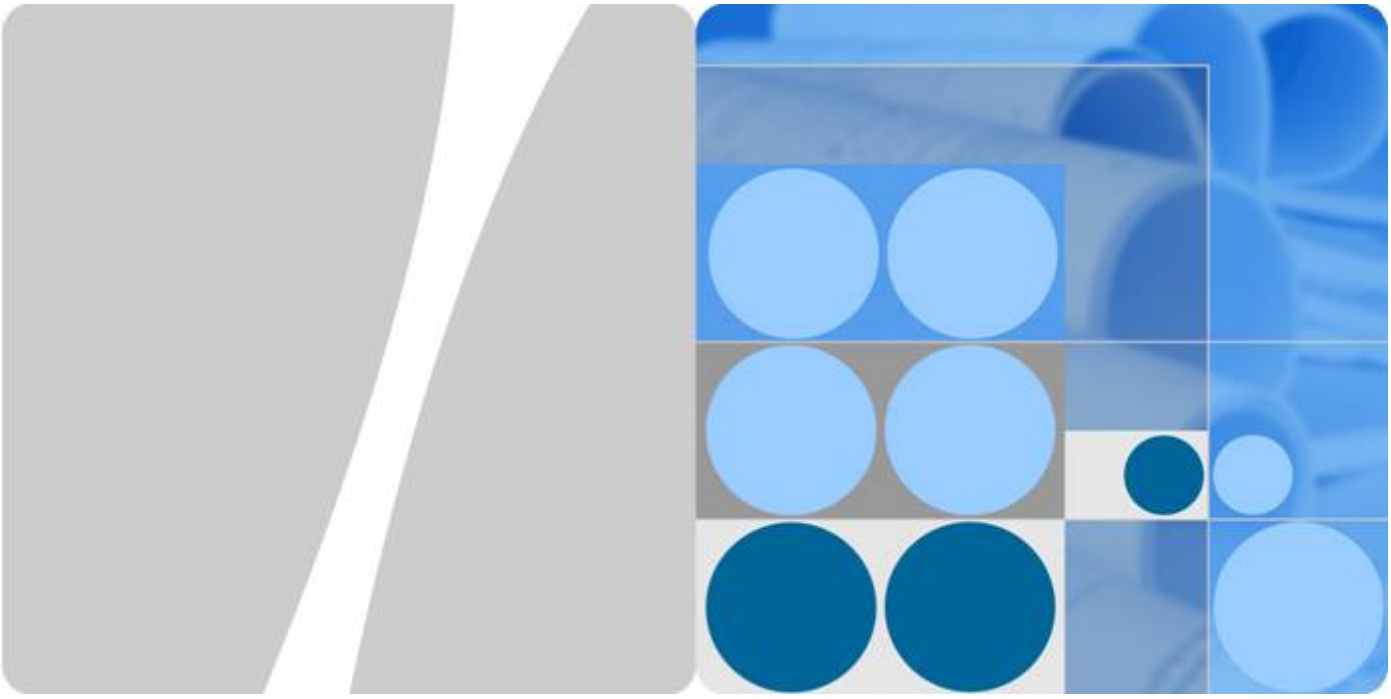


Huawei AR Series Access Routers

V200R010

Command Reference

Issue 14

Date 2025-10-30

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2023. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions

HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://e.huawei.com

About This Document

Intended Audience

This document provides the configuration commands of each feature supported by the device, including the syntax, view, default level, description, parameters, usage guideline, related commands, and example of each command.

This document together with the Configuration Guide provides intended readers with detailed usage of each command.

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
DANGER	Indicates a hazard with a high level of risk which, if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium level of risk which, if not avoided, could result in death or serious injury.
CAUTION	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.

Copyright © Huawei Technologies Co., Ltd.

Symbol	Description
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Supplements the important information in the main text. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

The command conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[ ]	Items (keywords or arguments) in brackets [ ] are optional.
{ x | y | ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x | y | ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x | y | ... }*	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x | y | ...]*	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

Copyright © Huawei Technologies Co., Ltd.

Interface Numbering Conventions

Interface numbers used in this manual are examples. In device configuration, use the existing interface numbers on devices.

Security Conventions

- Password setting
  - When configuring a password, the cipher text is recommended. To ensure device security, change the password periodically.
  - When you configure a password in plain text that starts and ends with %@%@, @%@%, %#%#, or %^%# (the password can be decrypted by the device), the password is displayed in the same manner as the configured one in the configuration file. Do not use this setting.
  - When you configure a password in cipher text, different features cannot use the same cipher-text password. For example, the cipher-text password set for the AAA feature cannot be used for other features.
- Encryption algorithm

  Currently, the device uses the following encryption algorithms: 3DES, AES, RSA, SHA1, SHA2, and MD5. 3DES, RSA and AES are reversible, while SHA1, SHA2, and MD5 are irreversible. The encryption algorithms DES, 3DES, RSA (RSA-1024 or lower), MD5 (in digital signature scenarios and password encryption), and SHA1 (in digital signature scenarios) have a low security, which may bring security risks. If protocols allowed, using more secure encryption algorithms, such as AES, RSA (RSA-2048 or higher), SHA2, and HMAC-SHA2, is recommended. The encryption algorithm depends on actual networking. The irreversible encryption algorithm must be used for the administrator password, SHA2 is recommended.
- Personal data

  Some personal data may be obtained or used during operation or fault location of your purchased products, services, features, so you have an obligation to make privacy policies and take measures according to the applicable law of the country to protect personal data.
- The terms mirrored port, port mirroring, traffic mirroring, and mirroring in this manual are mentioned only to describe the product's function of communication error or failure detection, and do not involve collection or processing of any personal information or communication data of users.

Reference Standards and Protocols

To obtain reference standards and protocols, log in to **Huawei official website**, search for "protocol compliance list", and download the *Huawei AR Series Standard and Protocol Comply Table*.

 Copyright © Huawei Technologies Co., Ltd.

Declaration

- This manual is only a reference for you to configure your devices. The contents in the manual, such as web pages, command line syntax, and command outputs, are based on the device conditions in the lab. The manual provides instructions for general scenarios, but do not cover all usage scenarios of all product models. The contents in the manual may be different from your actual device situations due to the differences in software versions, models, and configuration files. The manual will not list every possible difference. You should configure your devices according to actual situations.
- The specifications provided in this manual are tested in lab environment (for example, the tested device has been installed with a certain type of boards or only one protocol is run on the device). Results may differ from the listed specifications when you attempt to obtain the maximum values with multiple functions enabled on the device.
- In this document, public IP addresses may be used in feature introduction and configuration examples and are for reference only unless otherwise specified.
- In this document, AR series access routers include AR100&AR120&AR150&AR160&AR200&AR1200&AR2200&AR3200&AR3600 Series.

Mappings Between Product Software Versions and NMS Versions

The mappings between product software versions and NMS versions are as follows.

AR Product Software Version	eSight	iManager U2000
V200R010	V300R009C00	V200R018C50

 Copyright © Huawei Technologies Co., Ltd.

Contents

About This Document ii

1 Using the Command Query Tool to Query Product Command Information 1

2 Overview of CLIs 2

2.1 How to Use Command Lines 2

2.1.1 Entering Command Views 2

2.1.2 Setting Command Levels 4

2.1.3 Editing Command Lines 6

2.1.4 Using Command Line Online Help 8

2.1.5 Interpreting Command Line Error Messages 9

2.1.6 Using the **undo** Command Line 10

2.1.7 Displaying History Commands 11

2.1.8 Using Command Line Shortcut Keys 12

2.1.9 Executing Commands in a Batch 14

2.2 Displaying the Command Output 15

2.2.1 Verifying Command Line Configurations 15

2.2.2 Controlling the Display Mode of Commands 15

2.2.3 Filtering Command Outputs 16

2.3 Configuration Examples 20

2.3.1 Example for Using Tab 20

2.3.2 Example for Defining Shortcut Keys 21

3 Basic Configurations Commands 23

3.1 CLI Overview Commands 23

3.1.1 assistant task 23

3.1.2 cls 25

3.1.3 command-privilege level 25

3.1.4 diagnose 27

3.1.5 display assistant task history 28

3.1.6 display command-view 30

3.1.7 display history-command 31

3.1.8 display hotkey 32

3.1.9 display this 34

3.1.10 header 35

3.1.11 hotkey ... 37
3.1.12 if-match timer cron ... 40
3.1.13 perform batch-file ... 46
3.1.14 quit ... 47
3.1.15 return ... 48
3.1.16 set current-configuration display ... 49
3.1.17 system-view ... 51
3.2 Auto-Config Commands ... 52
3.2.1 autoconfig enable ... 52
3.2.2 autoconfig getting-file restart ... 54
3.2.3 display autoconfig activating-config delay ... 55
3.2.4 display autoconfig activating-config remanent-time ... 56
3.2.5 display autoconfig enable ... 57
3.2.6 display autoconfig-status ... 57
3.3 Auto-Start Configuration Commands ... 69
3.3.1 autostart ... 69
3.3.2 autostart enable ... 70
3.3.3 autostart run ... 71
3.3.4 display autostart config ... 71
3.3.5 display autostart status ... 72
3.3.6 ipaddress ... 79
3.3.7 servertype ... 80
3.3.8 username ... 81
3.4 USB-based Deployment Configuration Commands ... 82
3.4.1 autoupdate enable ... 82
3.4.2 clear usb autoupdate password ... 83
3.4.3 display autoupdate enable ... 84
3.4.4 display hmac enable ... 85
3.4.5 display usb autoupdate state ... 86
3.4.6 hmac enable ... 87
3.4.7 set usb autoupdate password ... 88
3.4.8 usb autoupdate generate encrypted boot-password ... 89
3.5 SMS-based Deployment Configuration Commands ... 90
3.5.1 sms config autodeploy enable ... 90
3.5.2 sms config caller ... 91
3.6 Fast Provisioning Configuration Commands ... 93
3.6.1 display fast provisioning record ... 93
3.6.2 display fast provisioning state ... 94
3.6.3 fast provisioning enable ... 95
3.6.4 fast-provisioning disable (sub-interface view) ... 96
3.6.5 fast-provisioning enable (interface view) ... 97
3.6.6 reset fast-provisioning ... 99

3.7 First Login Commands 100
3.7.1 clock datetime 100
3.7.2 clock daylight-saving-time 101
3.7.3 clock timezone 104
3.7.4 display clock 106
3.7.5 sysname 112
3.7.6 ip netbios-reply interface 113
3.8 UI Configuration Commands 115
3.8.1 acl (user interface view) 115
3.8.2 authentication-domain 116
3.8.3 authentication-mode (user interface view) 118
3.8.4 auto-execute command 119
3.8.5 databits 121
3.8.6 display mib-index interface 122
3.8.7 display user-interface 123
3.8.8 display user-interface maximum-vty 125
3.8.9 display users 126
3.8.10 display vty mode 127
3.8.11 display vty lines 128
3.8.12 flow-control 129
3.8.13 free user-interface 130
3.8.14 history-command max-size 131
3.8.15 idle-timeout 132
3.8.16 parity 133
3.8.17 protocol inbound 134
3.8.18 screen-length 136
3.8.19 screen-width 137
3.8.20 set authentication password 138
3.8.21 shell 139
3.8.22 speed (user interface view) 140
3.8.23 stopbits 142
3.8.24 user privilege 143
3.8.25 user-interface 145
3.8.26 user-interface current 148
3.8.27 user-interface maximum-vty 149
3.9 User Login Configuration Commands 150
3.9.1 connect 150
3.9.2 config lock 152
3.9.3 config unlock interval 153
3.9.4 display config lock 154
3.9.5 display ecc local-key-pair public 156
3.9.6 display ecc peer-public-key 158

3.9.7 display rsa local-key-pair public 160
3.9.8 display rsa peer-public-key 161
3.9.9 display ssh server 163
3.9.10 display ssh user-information 165
3.9.11 display telnet server status 167
3.9.12 display telnet-client 168
3.9.13 ecc local-key-pair 168
3.9.14 ecc peer-public-key 170
3.9.15 exline-breaker 172
3.9.16 language character-set 173
3.9.17 lock 174
3.9.18 matched upper-view 175
3.9.19 peer-public-key end 177
3.9.20 public-key-code begin 178
3.9.21 public-key-code end 179
3.9.22 redirect binding vpn-instance 181
3.9.23 redirect enable 182
3.9.24 redirect listen-port 183
3.9.25 rsa local-key-pair create 185
3.9.26 rsa local-key-pair destroy 186
3.9.27 rsa peer-public-key 187
3.9.28 send 189
3.9.29 set insecure-protocol enable 190
3.9.30 ssh client assign 192
3.9.31 ssh client first-time enable 193
3.9.32 ssh server authentication-retries 194
3.9.33 ssh server compatible-ssh1x enable 195
3.9.34 ssh server cipher 197
3.9.35 ssh server hmac 198
3.9.36 ssh server key-exchange 200
3.9.37 ssh server permit interface 202
3.9.38 ssh server port 203
3.9.39 ssh server rekey-interval 204
3.9.40 ssh server timeout 205
3.9.41 ssh server-source 206
3.9.42 ssh user assign 208
3.9.43 ssh user authentication-type 209
3.9.44 ssh user default-authentication-type 213
3.9.45 stelnet 213
3.9.46 stelnet server enable 217
3.9.47 super 218
3.9.48 super password 220

3.9.49 telnet 221
3.9.50 telnet client-source 223
3.9.51 telnet server-source 224
3.9.52 telnet server permit interface 226
3.9.53 telnet server enable 227
3.9.54 telnet server port 228
3.9.55 transparent-mode enable 229
3.10 HTTP Server Commands 230
3.10.1 display http server 231
3.10.2 display http user 233
3.10.3 display fast-configuration state 234
3.10.4 http acl 235
3.10.5 http client disable 236
3.10.6 http get 237
3.10.7 http server enable 239
3.10.8 http server load 240
3.10.9 http server max-online-users 241
3.10.10 http server permit interface 242
3.10.11 http server port 244
3.10.12 http server-source 245
3.10.13 http timeout 246
3.10.14 set fast-configuration state disable 247
3.10.15 set logo-path 248
3.10.16 set web login-style 250
3.11 File Management Commands 251
3.11.1 ascii 251
3.11.2 binary 252
3.11.3 bye 253
3.11.4 cd (FTP client view) 254
3.11.5 cd (SFTP client view) 255
3.11.6 cd (user view) 256
3.11.7 cdup (SFTP client view) 258
3.11.8 cdup (FTP client view) 259
3.11.9 close 260
3.11.10 copy 261
3.11.11 delete (FTP client view) 264
3.11.12 delete (user view) 265
3.11.13 dir (user view) 267
3.11.14 dir/ls (FTP client view) 271
3.11.15 dir/ls (SFTP client view) 273
3.11.16 disconnect 274
3.11.17 display ftp-client 275

3.11.18 display ftp-server ... 276
3.11.19 display ftp-users ... 278
3.11.20 display sftp-client ... 279
3.11.21 display tftp-client ... 281
3.11.22 display tftp-server status ... 282
3.11.23 execute ... 283
3.11.24 file prompt ... 285
3.11.25 format ... 286
3.11.26 ftp ... 287
3.11.27 ftp acl ... 291
3.11.28 ftp client-source ... 292
3.11.29 ftp server enable ... 293
3.11.30 ftp server permit interface ... 294
3.11.31 ftp server port ... 296
3.11.32 ftp server-source ... 297
3.11.33 ftp timeout ... 299
3.11.34 get (SFTP client view) ... 300
3.11.35 get (FTP client view) ... 301
3.11.36 help (SFTP client view) ... 302
3.11.37 lcd ... 303
3.11.38 mkdir (FTP client view) ... 304
3.11.39 mkdir (SFTP client view) ... 305
3.11.40 mkdir (User view) ... 306
3.11.41 more ... 308
3.11.42 move ... 311
3.11.43 open ... 314
3.11.44 passive ... 316
3.11.45 put (FTP client view) ... 317
3.11.46 put (SFTP client view) ... 319
3.11.47 pwd (FTP client view) ... 320
3.11.48 pwd (SFTP client view) ... 321
3.11.49 pwd (user view) ... 322
3.11.50 remotehelp ... 322
3.11.51 remove (SFTP client view) ... 324
3.11.52 remove (user view) ... 325
3.11.53 rename (SFTP client view) ... 325
3.11.54 rename (user view) ... 326
3.11.55 reset recycle-bin ... 329
3.11.56 rmdir (FTP client view) ... 331
3.11.57 rmdir (user view) ... 332
3.11.58 rmdir (SFTP client view) ... 333
3.11.59 set default ftp-directory ... 334

 Copyright © Huawei Technologies Co., Ltd.

3.11.60 set default tftp-directory ... 335
3.11.61 set net-manager vpn-instance ... 336
3.11.62 sftp ... 338
3.11.63 sftp client-source ... 343
3.11.64 sftp server enable ... 344
3.11.65 tftp ... 345
3.11.66 tftp client-source ... 348
3.11.67 tftp-server acl ... 350
3.11.68 tftp server enable ... 351
3.11.69 tftp server port ... 352
3.11.70 tftp server timeout ... 353
3.11.71 undelete ... 354
3.11.72 unzip ... 356
3.11.73 user ... 358
3.11.74 verbose ... 359
3.11.75 zip ... 361
3.12 Configuring System Startup Commands ... 363
3.12.1 autosave interval ... 363
3.12.2 autosave time ... 365
3.12.3 clear reset-reason ... 368
3.12.4 change default-password ... 369
3.12.5 compare configuration ... 371
3.12.6 diagnose verify enable ... 373
3.12.7 display autosave configuration ... 374
3.12.8 display current-configuration ... 375
3.12.9 display factory-configuration ... 377
3.12.10 display factory-configuration operate-mode ... 380
3.12.11 display reset-reason ... 381
3.12.12 display saved-configuration ... 384
3.12.13 display schedule reboot ... 385
3.12.14 display snmp-agent trap feature-name configuration all ... 386
3.12.15 display startup ... 388
3.12.16 display system ... 390
3.12.17 factory-configuration prohibit ... 392
3.12.18 factory-configuration reset ... 393
3.12.19 reboot ... 394
3.12.20 reset saved-configuration ... 395
3.12.21 save ... 396
3.12.22 schedule reboot ... 398
3.12.23 set factory-configuration ... 400
3.12.24 set factory-configuration operate-mode ... 402
3.12.25 snmp-agent trap enable feature-name configuration ... 404

3.12.26 startup saved-configuration 405
3.12.27 startup system-software 407
3.12.28 startup system-software backup 409
3.12.29 startup system-software check enable 411
3.12.30 startup patch 412
3.12.31 bootloader startup menu enable 413
3.12.32 display bootloader startup menu 414
3.13 Upgrade Commands 415
3.13.1 display license 416
3.13.2 display license accept agreement 421
3.13.3 display license esn 425
3.13.4 display license resource usage 426
3.13.5 display license revoke-ticket 427
3.13.6 display license state 428
3.13.7 display paf 429
3.13.8 display patch-information 430
3.13.9 display rollback state 432
3.13.10 license active 433
3.13.11 license active accept agreement 435
3.13.12 license emergency 436
3.13.13 license function 437
3.13.14 license resource 439
3.13.15 license revoke 440
3.13.16 patch delete all 441
3.13.17 patch load 442
3.13.18 rollback 443
3.13.19 set output slot 444
3.13.20 upgrade slot startup bootrom (User view) 446
3.14 Smart Upgrade Commands 447
3.14.1 display smart-upgrade information 447
3.14.2 smart-upgrade enable 451
3.14.3 smart-upgrade information 452
3.14.4 smart-upgrade right-now 454
3.14.5 smart-upgrade time 455

4 Device Management Commands 458

4.1 Device Status Checking Commands 458
4.1.1 display cpu-usage 458
4.1.2 display cpu-usage configuration 461
4.1.3 display device 463
4.1.4 display diagnostic-information 467
4.1.5 display elabel 470
4.1.6 display esn 474

4.1.7 display fan ... 475
4.1.8 display health ... 476
4.1.9 display memory-alloc mid ... 480
4.1.10 display memory-usage ... 481
4.1.11 display memory-usage process ... 482
4.1.12 display memory-usage process vrp ... 486
4.1.13 display memory-usage threshold ... 488
4.1.14 display power ... 490
4.1.15 display power system ... 491
4.1.16 display sn ... 493
4.1.17 display temperature ... 495
4.1.18 display transceiver ... 497
4.1.19 display version ... 501
4.1.20 display dyinggasp capacity ... 504
4.2 Hardware Configuration Commands ... 505
4.2.1 backup elabel ... 505
4.2.2 clear root-key ... 508
4.2.3 display root-key configuration ... 509
4.2.4 display rps elabel ... 510
4.2.5 display rps status ... 512
4.2.6 display rps temperature ... 513
4.2.7 display rps version ... 514
4.2.8 display slave default ... 515
4.2.9 display switchover state ... 516
4.2.10 display super-fast hardware state ... 517
4.2.11 osp-module memory-size ... 518
4.2.12 power ... 520
4.2.13 reset slot ... 521
4.2.14 set cpu-usage threshold ... 521
4.2.15 set memory-usage threshold ... 523
4.2.16 set operator-code ... 525
4.2.17 set output-mode osp ... 525
4.2.18 set root-key ... 527
4.2.19 set rps force ... 527
4.2.20 set transceiver ... 528
4.2.21 set transceiver-monitoring ... 530
4.2.22 set vendorname ... 531
4.2.23 slave default ... 532
4.2.24 slave restart ... 533
4.2.25 slave switchover ... 534
4.2.26 switchover enable ... 535
4.2.27 transceiver phony-alarm-disable ... 536

 Copyright © Huawei Technologies Co., Ltd.

4.2.28 upgrade osp-module software ... 537
4.2.29 set osp power uninterruptible ... 538
4.2.30 super-fast hardware enable ... 539
4.3 Information Center Configuration Commands ... 540
4.3.1 display actived-alarm highest-level ... 540
4.3.2 display channel ... 541
4.3.3 display debugging ... 545
4.3.4 display info-center ... 546
4.3.5 display info-center filter-id ... 550
4.3.6 display info-center logfile path ... 552
4.3.7 display info-center rate-limit record ... 552
4.3.8 display info-center rate-limit threshold ... 554
4.3.9 display info-center statistics ... 555
4.3.10 display log ... 557
4.3.11 display logbuffer ... 560
4.3.12 display logfile ... 565
4.3.13 display trapbuffer ... 568
4.3.14 info-center autosave logbuffer ... 571
4.3.15 info-center channel ... 572
4.3.16 info-center channel name ... 575
4.3.17 info-center enable ... 576
4.3.18 info-center filter-id ... 577
4.3.19 info-center logbuffer ... 579
4.3.20 info-center logbuffer size ... 580
4.3.21 info-center logfile path ... 581
4.3.22 info-center logfile size ... 583
4.3.23 info-center loghost ... 584
4.3.24 info-center loghost source ... 587
4.3.25 info-center max-logfile-number ... 588
4.3.26 info-center rate-limit except ... 590
4.3.27 info-center rate-limit global-threshold ... 591
4.3.28 info-center rate-limit monitor-period ... 592
4.3.29 info-center rate-limit threshold ... 593
4.3.30 info-center source channel ... 595
4.3.31 info-center statistic-suppress enable ... 600
4.3.32 info-center timestamp ... 601
4.3.33 info-center trapbuffer ... 603
4.3.34 info-center trapbuffer size ... 604
4.3.35 reset info-center statistics ... 606
4.3.36 reset logbuffer ... 607
4.3.37 reset trapbuffer ... 608
4.3.38 save logfile ... 608

4.3.39 terminal debugging 609
4.3.40 terminal logging 610
4.3.41 terminal monitor 611
4.3.42 terminal trapping 613
4.4 NTP Configuration Commands 614
4.4.1 display ntp-service sessions 614
4.4.2 display ntp-service status 619
4.4.3 display ntp-service trace 620
4.4.4 ntp-service access 622
4.4.5 ntp-service authentication complexity-check disable 625
4.4.6 ntp-service authentication enable 626
4.4.7 ntp-service authentication-keyid 627
4.4.8 ntp-service broadcast-client 629
4.4.9 ntp-service broadcast-server 630
4.4.10 ntp-service cwmp unicast-server 632
4.4.11 ntp-service discard 633
4.4.12 ntp-service enable 634
4.4.13 ntp-service in-interface disable 635
4.4.14 ntp-service kod-enable 636
4.4.15 ntp-service manycast-client 637
4.4.16 ntp-service manycast-server 638
4.4.17 ntp-service max-dynamic-sessions 639
4.4.18 ntp-service multicast-client 640
4.4.19 ntp-service multicast-server 642
4.4.20 ntp-service refclock-master 644
4.4.21 ntp-service reliable authentication-keyid 645
4.4.22 ntp-service source-interface 646
4.4.23 ntp-service unicast-peer 648
4.4.24 ntp-service unicast-server 651
4.5 Fault Management Commands 654
4.5.1 alarm (system view) 654
4.5.2 alarm correlation-suppress enable 655
4.5.3 alarm-name severity 656
4.5.4 clear alarm active 659
4.5.5 clear event all 660
4.5.6 correlation-analyze enable 661
4.5.7 delay-suppression enable 662
4.5.8 display alarm active 663
4.5.9 display alarm history 665
4.5.10 display alarm information 667
4.5.11 display event 668
4.5.12 display event information 670

4.5.13 event ... 671
4.5.14 mask interface ... 672
4.5.15 set said enable ... 673
4.5.16 suppression alarm-name ... 677
4.5.17 suppression event-name ... 678
4.6 Commands for Clock Source ... 680
4.6.1 clock source ... 680
4.6.2 display clock source ... 682
4.7 Energy-saving Configuration Commands ... 683
4.7.1 als ... 684
4.7.2 als restart ... 684
4.7.3 als restart mode ... 685
4.7.4 als restart pulse ... 687
4.7.5 display als ... 688
4.7.6 energy-efficient-ethernet enable ... 689
4.7.7 set fan-speed ... 691
4.8 PoE Configuration Commands ... 692
4.8.1 display poe device ... 692
4.8.2 display poe information ... 693
4.8.3 display poe power ... 695
4.8.4 display poe power-state ... 698
4.8.5 display poe-power ... 703
4.8.6 poe enable ... 704
4.8.7 poe force-power enable ... 705
4.8.8 poe { power-off | power-on } interface ... 706
4.8.9 poe legacy enable ... 708
4.8.10 poe max-power ... 708
4.8.11 poe power ... 710
4.8.12 poe power-management ... 711
4.8.13 poe power-off time-range ... 712
4.8.14 poe power-reserved ... 714
4.8.15 poe priority ... 715
4.8.16 poe-power utilization-threshold ... 716
4.9 OIDS Configuration Commands ... 718
4.9.1 collect oids database file to system-master ... 718
4.9.2 display oids current-event ... 719
4.9.3 display oids history-event ... 720
4.9.4 display oids monitor current-fault ... 723
4.9.5 display oids monitor kpi ... 725
4.9.6 display oids monitor status ... 729
4.9.7 display oids register-event ... 731
4.9.8 display oids register-status ... 733

4.9.9 oids monitor enable ... 734
4.10 OPS Configuration Commands ... 736
4.10.1 assistant scheduler suspend ... 736
4.10.2 clear ops running context ... 737
4.10.3 display ops assistant ... 738
4.10.4 display ops environment ... 742
4.10.5 display ops error ... 744
4.10.6 display ops running context ... 745
4.10.7 environment ... 746
4.10.8 ops ... 748
4.10.9 ops install file ... 748
4.10.10 ops uninstall file ... 751
4.10.11 script-assistant python ... 753
4.10.12 shutdown script-assistant ... 755
5 Interface Management Commands ... 757
5.1 Basic Interface Configuration Commands ... 758
5.1.1 bandwidth (Interface view) ... 758
5.1.2 description (interface view) ... 759
5.1.3 display default-parameter interface ... 760
5.1.4 display interface ... 763
5.1.5 display interface brief ... 775
5.1.6 display interface description ... 778
5.1.7 display ip interface description ... 781
5.1.8 display interface counters ... 785
5.1.9 display ip interface ... 787
5.1.10 display this interface ... 792
5.1.11 interface ... 796
5.1.12 reset counters if-mib interface ... 798
5.1.13 reset counters interface ... 799
5.1.14 restart (interface view) ... 800
5.1.15 set flow-stat interval ... 801
5.1.16 shutdown (interface view) ... 803
5.1.17 shutdown interval ... 804
5.2 Ethernet Interface Configuration Commands ... 805
5.2.1 am isolate ... 805
5.2.2 auto duplex ... 807
5.2.3 auto speed ... 809
5.2.4 clock (Ethernet interface view) ... 811
5.2.5 combo-port ... 812
5.2.6 display error-down recovery ... 816
5.2.7 display interface ethernet brief ... 817
5.2.8 display port-group ... 820

5.2.9 display port-isolate group ... 822
5.2.10 display snmp-agent trap feature-name error-down all ... 823
5.2.11 duplex ... 824
5.2.12 encapsulation priority-tagged ... 826
5.2.13 error-down auto-recovery ... 828
5.2.14 error-statistics threshold-event trigger error-down ... 831
5.2.15 flow-control (Ethernet interface view) ... 832
5.2.16 flow-control negotiation ... 833
5.2.17 group-member ... 834
5.2.18 interface (Ethernet interface) ... 836
5.2.19 interface range ... 837
5.2.20 ifg ... 839
5.2.21 log-threshold ... 840
5.2.22 loopback ... 842
5.2.23 mac-address (Ethernet interface view) ... 843
5.2.24 management-plane isolate enable ... 845
5.2.25 management-port isolate enable ... 846
5.2.26 mdi ... 847
5.2.27 mtu (Ethernet interface view) ... 849
5.2.28 negotiation auto ... 850
5.2.29 port-down holdoff-timer ... 851
5.2.30 port-group ... 852
5.2.31 port-group group-member ... 854
5.2.32 port-isolate enable ... 855
5.2.33 port-isolate mode ... 857
5.2.34 portswitch ... 858
5.2.35 set flow-statistics include-interframe ... 860
5.2.36 snmp-agent trap enable feature-name error-down ... 861
5.2.37 speed ... 862
5.2.38 trap-threshold ... 863
5.2.39 trap-threshold error-statistics ... 866
5.2.40 virtual-cable-test ... 867
5.3 Serial Interface Configuration Commands ... 868
5.3.1 async mode (serial) ... 869
5.3.2 baudrate ... 870
5.3.3 clock dce ... 872
5.3.4 clock dte ... 875
5.3.5 code (serial) ... 879
5.3.6 crc (serial) ... 880
5.3.7 detect dcd ... 881
5.3.8 detect dsr-dtr (serial) ... 883
5.3.9 display interface serial ... 884

5.3.10 display tdm statistic ... 887
5.3.11 idlecode (serial) ... 888
5.3.12 interface serial ... 890
5.3.13 invert receive-clock ... 891
5.3.14 invert receive-clock auto ... 892
5.3.15 invert transmit-clock ... 893
5.3.16 itf number (serial interface view) ... 895
5.3.17 link-protocol tdm ... 896
5.3.18 loopback ... 898
5.3.19 mtu (serial) ... 899
5.3.20 physical-mode ... 900
5.3.21 phy-mru (serial) ... 901
5.3.22 reverse-rts ... 903
5.3.23 virtualbaudrate ... 904
5.4 Async Interface Configuration Commands ... 906
5.4.1 async mode (async) ... 906
5.4.2 detect dsr-dtr (async) ... 907
5.4.3 display interface async ... 908
5.4.4 interface async ... 911
5.4.5 mtu (async) ... 912
5.4.6 phy-mru (async) ... 913
5.5 CE1/PRI Interface Configuration Commands ... 914
5.5.1 channel-set (CE1/PRI interface view) ... 914
5.5.2 clock (CE1/PRI interface view) ... 916
5.5.3 controller e1 ... 918
5.5.4 crc ... 919
5.5.5 data-coding (CE1/PRI interface view) ... 920
5.5.6 detect-ais (CE1/PRI interface view) ... 921
5.5.7 detect-rai (CE1/PRI interface view) ... 922
5.5.8 display controller e1 ... 923
5.5.9 display workmode ... 927
5.5.10 error-diffusion restraint config ... 931
5.5.11 error-diffusion restraint enable ... 932
5.5.12 error-diffusion restraint restart-channel ... 933
5.5.13 frame-format (CE1/PRI interface view) ... 934
5.5.14 idlecode (CE1/PRI interface view) ... 935
5.5.15 itf (CE1/PRI interface view) ... 936
5.5.16 line-termination ... 938
5.5.17 loopback (CE1/PRI interface view) ... 939
5.5.18 pri-set (CE1/PRI interface view) ... 940
5.5.19 sa (CE1/PRI interface view) ... 941
5.5.20 set workmode e1t1 ... 943

 Copyright © Huawei Technologies Co., Ltd.

5.5.21 using (CE1/PRI interface view) 944
5.6 CT1/PRI Interface Configuration Commands 946
5.6.1 alarm-threshold 946
5.6.2 cable 948
5.6.3 channel-set (CT1/PRI interface view) 949
5.6.4 clock (CT1/PRI interface view) 951
5.6.5 controller t1 952
5.6.6 crc 953
5.6.7 data-coding (CT1/PRI interface view) 955
5.6.8 detect-rai (CT1/PRI interface view) 956
5.6.9 display controller t1 956
5.6.10 display workmode 961
5.6.11 frame-format (CT1/PRI interface view) 965
5.6.12 idlecode (CT1/PRI interface view) 966
5.6.13 itf (CT1/PRI interface view) 967
5.6.14 loopback (CT1/PRI interface view) 969
5.6.15 pri-set (CT1/PRI interface view) 970
5.6.16 set workmode e1t1 971
5.7 CE3 Interface Configuration Commands 973
5.7.1 clock (CE3 interface view) 973
5.7.2 controller e3 974
5.7.3 crc 975
5.7.4 display controller e3 976
5.7.5 fe3 978
5.7.6 itf (CE3 interface view) 980
5.7.7 loopback (CE3 interface view) 981
5.7.8 national-bit (CE3 interface view) 982
5.7.9 using (CE3 interface view) 983
5.8 E1-F Interface Configuration Commands 984
5.8.1 crc 984
5.8.2 display fe1 985
5.8.3 display workmode 989
5.8.4 fe1 clock 993
5.8.5 fe1 data-coding 994
5.8.6 fe1 detect-ais 995
5.8.7 fe1 detect-rai 997
5.8.8 fe1 frame-format 998
5.8.9 fe1 idlecode 999
5.8.10 fe1 itf 1000
5.8.11 fe1 line-termination 1002
5.8.12 fe1 loopback 1003
5.8.13 fe1 sa 1004

 Copyright © Huawei Technologies Co., Ltd.

5.8.14 fe1 timeslot-list 1005
5.8.15 fe1 unframed 1007
5.8.16 reset framerstatics 1008
5.8.17 set workmode e1t1-f 1009
5.9 T1-F Interface Configuration Commands 1010
5.9.1 crc 1010
5.9.2 display ft1 1012
5.9.3 display workmode 1016
5.9.4 ft1 alarm-threshold 1020
5.9.5 ft1 cable 1023
5.9.6 ft1 clock 1024
5.9.7 ft1 data-coding 1025
5.9.8 ft1 detect-rai 1026
5.9.9 ft1 frame-format 1027
5.9.10 ft1 idlecode 1028
5.9.11 ft1 itf 1029
5.9.12 ft1 loopback 1030
5.9.13 ft1 timeslot-list 1032
5.9.14 set workmode e1t1-f 1033
5.10 E&M Interface Configuration Commands 1034
5.10.1 display em clock-mode 1035
5.10.2 em clock 1036
5.10.3 em passthrough enable 1037
5.10.4 em signal-mode 1038
5.10.5 em transmit gain 1040
5.10.6 em receive gain 1042
5.10.7 em pcm 1045
5.11 Cellular Interface Configuration Commands 1047
5.11.1 apn 1047
5.11.2 apn profile 1048
5.11.3 apn-profile 1049
5.11.4 apn user name catch-imsi-sn 1051
5.11.5 band gsm 1052
5.11.6 band gsm 1053
5.11.7 band wcdma 1055
5.11.8 band lte 1057
5.11.9 cellular log enable 1060
5.11.10 cellular log rssi-threshold 1061
5.11.11 cellular log sinr-threshold 1063
5.11.12 dialer mode ppp 1065
5.11.13 dialer timer probe-interval 1066
5.11.14 dialer-number (APN view) 1067

 Copyright © Huawei Technologies Co., Ltd.

5.11.15 display apn-profile configuration 1068
5.11.16 diagnostics-monitor-port on 1070
5.11.17 display cellular 1071
5.11.18 display interface cellular 1083
5.11.19 display cellular feature 1087
5.11.20 display sms interface cellular 1089
5.11.21 display sms interface cellular statistics 1091
5.11.22 display sms send-history 1092
5.11.23 display snmp-agent trap feature-name ifmtrap all 1093
5.11.24 imsi check 1095
5.11.25 interface cellular 1096
5.11.26 ip address negotiate 1098
5.11.27 mode cdma 1099
5.11.28 mode lte 1100
5.11.29 mode wcdma 1103
5.11.30 modem auto-recovery track nqa 1104
5.11.31 modem auto-recovery track action 1106
5.11.32 modem auto-recovery dial action modem-reboot fail-times 1108
5.11.33 modem auto-recovery services-unavailable 1109
5.11.34 modem encryption-algorithm 1111
5.11.35 modem peer network-route 1113
5.11.36 modem reboot 1114
5.11.37 mtu (3G) 1115
5.11.38 multi-apn enable 1116
5.11.39 packet-service recover 1117
5.11.40 pin modify 1118
5.11.41 pin unlock 1119
5.11.42 pin verification 1120
5.11.43 pin verify 1122
5.11.44 plmn search 1123
5.11.45 plmn select 1124
5.11.46 profile create 1126
5.11.47 profile delete 1127
5.11.48 profile create lte-default 1128
5.11.49 profile create lte-default sim-id 1131
5.11.50 profile delete lte-default 1135
5.11.51 profile delete lte-default sim-id 1136
5.11.52 reset counters cellular 1137
5.11.53 rssi-threshold 1138
5.11.54 service domain 1139
5.11.55 sim-card reboot 1140
5.11.56 sim-id 1141

5.11.57 sim switch to ... 1143
5.11.58 sim switch rssi-threshold ... 1144
5.11.59 sim switch-back enable ... 1146
5.11.60 sms delete interface cellular ... 1147
5.11.61 sms send interface cellular ... 1148
5.11.62 sms-pool ... 1150
5.11.63 sms item ... 1151
5.11.64 sms send-item ... 1153
5.11.65 sms service-center-address ... 1155
5.11.66 snmp-agent trap enable feature-name ifmtrap ... 1156
5.11.67 user ... 1157
5.12 ISDN BRI Interface Configuration Commands ... 1160
5.12.1 loopback (ISDN BRI interface view) ... 1160
5.12.2 display interface bri ... 1161
5.12.3 interface bri ... 1164
5.12.4 mtu (ISDN BRI interface view) ... 1165
5.12.5 set workmode bri ... 1167
5.12.6 shutdown (ISDN BRI interface view) ... 1168
5.13 POS Interface Commands ... 1169
5.13.1 clock (POS interface view) ... 1169
5.13.2 crc (POS interface view) ... 1170
5.13.3 display interface pos ... 1171
5.13.4 flag (POS interface view) ... 1176
5.13.5 frame-format (POS interface view) ... 1178
5.13.6 link-protocol (POS interface view) ... 1179
5.13.7 loopback (POS interface view) ... 1180
5.13.8 mtu (POS interface view) ... 1181
5.13.9 scramble (POS interface view) ... 1183
5.13.10 set workmode stm ... 1184
5.13.11 threshold (POS interface view) ... 1185
5.14 CPOS Interface Configuration Commands ... 1186
5.14.1 clock (CPOS interface view) ... 1186
5.14.2 controller cpos ... 1187
5.14.3 display controller cpos ... 1188
5.14.4 display controller cpos e1 ... 1193
5.14.5 display controller cpos t1 ... 1195
5.14.6 display cpos multi-channel ... 1198
5.14.7 e1 channel-set (CPOS interface view) ... 1200
5.14.8 e1 set clock (CPOS interface view) ... 1202
5.14.9 e1 set flag (CPOS interface view) ... 1203
5.14.10 e1 set frame-format (CPOS interface view) ... 1204
5.14.11 e1 set loopback (CPOS interface view) ... 1205

5.14.12 e1 shutdown (CPOS interface view) 1207
5.14.13 e1 unframed (CPOS interface view) 1208
5.14.14 flag (CPOS interface view) 1209
5.14.15 frame-format (CPOS interface view) 1211
5.14.16 itf (CPOS interface view) 1212
5.14.17 loopback (CPOS interface view) 1213
5.14.18 multi-channel align-mode 1214
5.14.19 multiplex mode 1215
5.14.20 set workmode cpos 1217
5.14.21 shutdown (CPOS interface view) 1218
5.14.22 t1 channel-set (CPOS interface view) 1219
5.14.23 t1 set clock (CPOS interface view) 1220
5.14.24 t1 set flag (CPOS interface view) 1221
5.14.25 t1 set frame-format (CPOS interface view) 1222
5.14.26 t1 set loopback (CPOS interface view) 1224
5.14.27 t1 shutdown (CPOS interface view) 1225
5.14.28 t1 unframed (CPOS interface view) 1226
5.14.29 threshold (CPOS interface view) 1228
5.15 ADSL Interface Configuration Commands 1229
5.15.1 adsl bitswap (adsl) 1229
5.15.2 adsl sra (adsl) 1230
5.15.3 adsl standard (adsl) 1232
5.15.4 adsl trellis (adsl) 1234
5.15.5 display dsl all interface 1236
5.15.6 display interface atm (adsl) 1238
5.15.7 display dsl interface atm (adsl) 1241
5.15.8 interface atm (adsl) 1247
5.15.9 mtu (adsl) 1248
5.15.10 xdsl auto return 1249
5.15.11 shutdown (adsl) 1250
5.16 VDSL Interface Configuration Commands 1251
5.16.1 adsl bitswap (vdsl) 1252
5.16.2 adsl sra (vdsl) 1253
5.16.3 adsl standard (vdsl) 1254
5.16.4 adsl trellis (vdsl) 1258
5.16.5 display dsl all interface 1259
5.16.6 display dsl interface atm (vdsl) 1262
5.16.7 display dsl hlog interface 1268
5.16.8 display dsl interface ethernet (vdsl) 1270
5.16.9 display dsl qln interface 1275
5.16.10 display interface atm (vdsl) 1277
5.16.11 display interface ethernet (vdsl) 1280

5.16.12 interface atm (vdsl) 1283
5.16.13 interface ethernet (vdsl) 1284
5.16.14 mtu (vdsl) 1285
5.16.15 set workmode vdsl 1287
5.16.16 shutdown (vdsl) 1288
5.16.17 vdsl anti-noise enable 1289
5.16.18 vdsl band 1290
5.16.19 vdsl bind 1292
5.16.20 vdsl downstream-retrans enable 1293
5.16.21 vdsl upstream-retrans enable 1294
5.16.22 vdsl standard 1295
5.17 G.SHDSL Interface Configuration Commands 1297
5.17.1 display dsl all interface 1297
5.17.2 display dsl interface (g.shdsl) 1299
5.17.3 display interface atm (g.shdsl) 1306
5.17.4 display interface ethernet (g.shdsl) 1309
5.17.5 interface atm (g.shdsl) 1312
5.17.6 interface ethernet (g.shdsl) 1313
5.17.7 mtu (g.shdsl) 1314
5.17.8 set workmode shdsl 1316
5.17.9 shdsl annex 1317
5.17.10 shdsl bind 1320
5.17.11 shdsl bind m-pair 2 pairs 1324
5.17.12 shdsl capability 1326
5.17.13 shdsl compatibility 1327
5.17.14 shdsl current target snr margin downstream 1329
5.17.15 shdsl current target snr margin upstream 1330
5.17.16 shdsl line-probing 1332
5.17.17 shdsl mode 1333
5.17.18 shdsl pam 1335
5.17.19 shdsl pbo 1336
5.17.20 shdsl psd 1338
5.17.21 shdsl rate auto 1339
5.17.22 shdsl rate maximum 1340
5.17.23 shdsl rate minimum 1342
5.17.24 shdsl tc mode 1343
5.17.25 shdsl worst case target snr margin upstream 1345
5.17.26 shdsl worst case target snr margin downstream 1346
5.17.27 shutdown (g.shdsl) 1347
5.18 IMA Commands 1349
5.18.1 clock (E1-IMA) 1349
5.18.2 differential-delay 1350

5.18.3 display interface atm (E1-IMA) 1351
5.18.4 display interface ima-group 1354
5.18.5 frame-format 1358
5.18.6 frame-length 1359
5.18.7 ima ima-group 1360
5.18.8 ima-clock 1362
5.18.9 ima-id 1363
5.18.10 ima-standard 1364
5.18.11 interface atm (E1-IMA) 1365
5.18.12 interface ima-group 1366
5.18.13 loopback 1367
5.18.14 min-active-links 1368
5.18.15 scramble 1369
5.19 PON Interface Configuration Commands 1370
5.19.1 display epon-info interface pon 1370
5.19.2 display gpon-info interface pon 1374
5.19.3 display pon-statistic interface pon 1377
5.19.4 display pon-transceiver interface pon 1381
5.19.5 epon compatibility 1386
5.19.6 epon-checkcode 1387
5.19.7 epon-loid 1388
5.19.8 epon-mac-address 1390
5.19.9 epon-password 1391
5.19.10 gpon-password 1392
5.19.11 interface pon 1396
5.19.12 laser 1397
5.19.13 optical-module threshold bias 1399
5.19.14 optical-module threshold rx-power 1400
5.19.15 optical-module threshold temperature 1401
5.19.16 optical-module threshold tx-power 1403
5.19.17 optical-module threshold voltage 1404
5.19.18 port mode 1406
5.19.19 reset pon-statistic interface pon 1408
5.19.20 undo optical-module threshold 1409
5.20 Logical Interface Configuration Commands 1409
5.20.1 broadcast-limit link 1410
5.20.2 display interface loopback 1411
5.20.3 display interface null 1413
5.20.4 display interface virtual-ethernet 1415
5.20.5 display virtual-access 1417
5.20.6 display interface virtual-template 1421
5.20.7 mac-address (Virtual-Ethernet interface view) 1424

 Copyright © Huawei Technologies Co., Ltd.

5.20.8 mtu ... 1425
5.20.9 interface (FR sub-interface) ... 1427
5.20.10 interface loopback ... 1428
5.20.11 interface null ... 1429
5.20.12 interface virtual-ethernet ... 1430
5.20.13 interface virtual-template ... 1431
5.20.14 statistic enable ... 1432
5.20.15 statistic ip enable ... 1434
5.20.16 statistic ipv6 enable ... 1435
5.20.17 trigger trap ... 1437
5.21 transparent transmission commands ... 1438
5.21.1 display transport info ... 1438
5.21.2 display transport mode ... 1441
5.21.3 display transport session ... 1442
5.21.4 display transport stat ... 1444
5.21.5 kick-out session ... 1447
5.21.6 mode (TTY user interface view) ... 1448
5.21.7 raw-transport server-port ... 1449
5.21.8 raw-transport best-effort ... 1452
5.21.9 raw-transport enable ... 1453
5.21.10 raw-transport packet-size ... 1454
5.21.11 raw-transport packet-timer ... 1455
5.21.12 raw-transport special-char ... 1456
5.21.13 raw-transport tcp idle-timeout ... 1457
5.21.14 raw-transport tty2-mode ... 1458
5.21.15 socket-transport enable ... 1460
5.21.16 undo parameter ... 1461

6 Ethernet Switching Commands ... 1463

6.1 MAC Address Table Configuration Commands ... 1463
6.1.1 display loop-detect eth-loop ... 1463
6.1.2 display bridge mac-address ... 1466
6.1.3 display mac-address ... 1467
6.1.4 display mac-address aging-time ... 1470
6.1.5 display mac-address blackhole ... 1472
6.1.6 display mac-address dynamic ... 1474
6.1.7 display mac-address mux ... 1476
6.1.8 display mac-address security ... 1478
6.1.9 display mac-address static ... 1480
6.1.10 display mac-address sticky ... 1483
6.1.11 display mac-address summary ... 1485
6.1.12 display mac-address total-number ... 1487
6.1.13 display mac-limit ... 1489

6.1.14 drop illegal-mac alarm....1491
6.1.15 drop illegal-mac enable....1492
6.1.16 loop-detect eth-loop....1493
6.1.17 loop-detect eth-loop alarm-only....1496
6.1.18 mac-address....1497
6.1.19 mac-address aging-time....1503
6.1.20 mac-address learning disable....1505
6.1.21 mac-limit....1508
6.1.22 port-security aging-time....1510
6.1.23 port-security enable....1512
6.1.24 port-security mac-address sticky....1513
6.1.25 port-security max-mac-num....1515
6.1.26 port-security protect-action....1517
6.1.27 reset loop-detect eth-loop....1519
6.1.28 undo mac-address temporary....1521
6.1.29 undo mac-limit all....1522
6.2 Link Aggregation Commands....1523
6.2.1 display eth-trunk....1523
6.2.2 display interface eth-trunk....1527
6.2.3 display lacp brief....1531
6.2.4 display lacp error packet....1532
6.2.5 display lacp statistics eth-trunk....1533
6.2.6 display snmp-agent trap feature-name lacp all....1535
6.2.7 display trunk index-map....1536
6.2.8 display trunk resource....1537
6.2.9 display trunkfwdtbl eth-trunk....1538
6.2.10 display trunkmembership eth-trunk....1540
6.2.11 eth-trunk....1542
6.2.12 interface eth-trunk....1544
6.2.13 lacp collector delay....1545
6.2.14 lacp preempt delay....1546
6.2.15 lacp preempt enable....1548
6.2.16 lacp priority....1549
6.2.17 lacp priority-command-mode....1550
6.2.18 lacp selected....1552
6.2.19 lacp src-mac....1553
6.2.20 lacp system-priority....1554
6.2.21 lacp timeout....1555
6.2.22 least active-linknumber....1557
6.2.23 load-balance....1559
6.2.24 mac-address (Eth-Trunk interface view)....1562
6.2.25 max active-linknumber....1563

 Copyright © Huawei Technologies Co., Ltd.

6.2.26 mode....1565
6.2.27 mtu (Eth-Trunk interface view)....1567
6.2.28 reset lacp error packet statistics....1569
6.2.29 reset lacp statistics eth-trunk....1569
6.2.30 snmp-agent trap enable feature-name lacp....1571
6.2.31 trunkport....1572
6.2.32 trunk member-port-inspect....1574
6.2.33 trunk-member trap....1575
6.3 VLAN Configuration Commands....1576
6.3.1 8021q protocol....1576
6.3.2 access-vlan....1578
6.3.3 aggregate-vlan....1581
6.3.4 arp broadcast....1582
6.3.5 bandwidth (VLANIF interface view)....1583
6.3.6 damping time....1584
6.3.7 description (VLAN view)....1586
6.3.8 description (VLANIF interface view)....1587
6.3.9 display dot1q information....1588
6.3.10 display qinq information....1590
6.3.11 display interface vlanif....1591
6.3.12 display mux-vlan....1594
6.3.13 display port vlan....1595
6.3.14 display sub-vlan....1597
6.3.15 display super-vlan....1598
6.3.16 display vlan....1599
6.3.17 display vlan priority....1604
6.3.18 display vlan-range....1605
6.3.19 dot1q termination vid....1606
6.3.20 dynamic-macvlan enable....1609
6.3.21 interface vlanif....1610
6.3.22 ip pool (VLAN view)....1611
6.3.23 management-vlan....1613
6.3.24 mtu (VLANIF interface view)....1614
6.3.25 mux-vlan....1615
6.3.26 name (VLAN view)....1617
6.3.27 port....1618
6.3.28 port default vlan....1620
6.3.29 port hybrid pvid vlan....1624
6.3.30 port hybrid tagged vlan....1626
6.3.31 port hybrid untagged vlan....1629
6.3.32 port link-type....1632
6.3.33 port mux-vlan enable....1634

6.3.34 port trunk allow-pass vlan....1635
6.3.35 port trunk pvid vlan....1638
6.3.36 qinq termination pe-vid ce-vid....1640
6.3.37 reset vlan statistics....1642
6.3.38 set vlan-range....1643
6.3.39 set reserved-vlan slot....1645
6.3.40 shutdown (VLANIF interface view)....1646
6.3.41 subordinate group....1647
6.3.42 subordinate separate....1649
6.3.43 vlan....1652
6.3.44 vlan priority....1653
6.3.45 vlan vlan-name....1655
6.3.46 termination-vid batch enable....1656
6.4 Voice VLAN Configuration Commands....1657
6.4.1 display voice-vlan oui....1658
6.4.2 display voice-vlan status....1659
6.4.3 voice-vlan aging-time....1661
6.4.4 voice-vlan enable....1662
6.4.5 voice-vlan legacy....1664
6.4.6 voice-vlan mac-address....1665
6.4.7 voice-vlan mode....1666
6.4.8 voice-vlan remark....1668
6.4.9 voice-vlan security enable....1670
6.5 QinQ Configuration Commands....1671
6.5.1 ce-vlan ignore....1671
6.5.2 qinq termination l2....1674
6.5.3 qinq protocol....1676
6.5.4 vlan allow-pass....1678
6.5.5 vlan dot1q-tunnel(Sub-interface)....1680
6.5.6 vlan dot1q-tunnel enable....1682
6.5.7 vlan stacking (Sub-interface)....1683
6.5.8 vlan stacking vid....1686
6.6 VLAN Mapping Configuration Commands....1688
6.6.1 vlan mapping 8021p....1688
6.6.2 vlan mapping vid(Sub-interface)....1690
6.6.3 vlan mapping vid....1692
6.7 GVRP Configuration Commands....1694
6.7.1 display garp statistics....1694
6.7.2 display garp timer....1695
6.7.3 display gvrp state....1697
6.7.4 display gvrp statistics....1700
6.7.5 display gvrp status....1701

6.7.6 display gvrp vlan-operation 1702
6.7.7 garp timer 1704
6.7.8 garp timer leaveall 1706
6.7.9 gvrp 1708
6.7.10 gvrp registration 1709
6.7.11 reset garp statistics 1710
6.8 STP/RSTP/MSTP Configuration Commands 1712
6.8.1 active region-configuration 1712
6.8.2 check region-configuration 1713
6.8.3 display snmp-agent trap feature-name mstp all 1714
6.8.4 display stp 1716
6.8.5 display stp abnormal-interface 1722
6.8.6 display stp active 1724
6.8.7 display stp bridge 1729
6.8.8 display stp error packet 1731
6.8.9 display stp global 1732
6.8.10 display stp region-configuration 1736
6.8.11 display stp tc-bpdu statistics 1737
6.8.12 display stp topology-change 1739
6.8.13 display stp vlan 1741
6.8.14 instance 1742
6.8.15 max bandwidth-affected-linknumber 1744
6.8.16 region-name 1745
6.8.17 reset stp error packet statistics 1746
6.8.18 reset stp statistics 1747
6.8.19 revision-level 1748
6.8.20 snmp-agent trap enable feature-name mstp 1749
6.8.21 stp bpdu-filter 1751
6.8.22 stp bpdu-filter default 1753
6.8.23 stp bpdu-protection 1754
6.8.24 stp bridge-diameter 1755
6.8.25 stp compliance 1757
6.8.26 stp config-digest-snoop 1758
6.8.27 stp converge 1759
6.8.28 stp cost 1760
6.8.29 stp edged-port 1762
6.8.30 stp edged-port default 1764
6.8.31 stp enable 1765
6.8.32 stp loop-protection 1767
6.8.33 stp max-hops 1768
6.8.34 stp mcheck 1770
6.8.35 stp mode (system view) 1771

6.8.36 stp no-agreement-check....1772
6.8.37 stp pathcost-standard....1774
6.8.38 stp point-to-point....1776
6.8.39 stp port priority....1778
6.8.40 stp priority....1779
6.8.41 stp region-configuration....1781
6.8.42 stp root....1782
6.8.43 stp root-protection....1784
6.8.44 stp tc-protection....1786
6.8.45 stp tc-protection interval....1787
6.8.46 stp tc-protection threshold....1788
6.8.47 stp timer forward-delay....1789
6.8.48 stp timer hello....1791
6.8.49 stp timer max-age....1792
6.8.50 stp timer-factor....1794
6.8.51 stp transmit-limit (interface view)....1795
6.8.52 stp transmit-limit (system view)....1796
6.8.53 vlan-mapping modulo....1798
6.9 SEP Configuration Commands....1799
6.9.1 block port....1799
6.9.2 control-vlan (SEP segment view)....1802
6.9.3 description (SEP segment view)....1804
6.9.4 display sep error packet....1805
6.9.5 display sep interface....1806
6.9.6 display sep segment....1810
6.9.7 display sep topology....1812
6.9.8 preempt (SEP segment view)....1815
6.9.9 protected-instance....1818
6.9.10 reset sep error packet statistics....1820
6.9.11 reset sep interface statistics....1820
6.9.12 sep segment....1821
6.9.13 sep segment (interface view)....1823
6.9.14 sep segment priority....1825
6.9.15 tc-notify....1827
6.9.16 tc-protection interval....1829
6.10 Layer 2 Protocol Transparent Transmission Commands....1830
6.10.1 l2protocol-tunnel....1830
6.10.2 l2protocol-tunnel group-mac....1832
6.10.3 l2protocol-tunnel user-defined-protocol....1834
6.11 Transparent Bridging (TB) Configuration Commands....1836
6.11.1 bpdu transmit enable....1836
6.11.2 bridge....1837

 Copyright © Huawei Technologies Co., Ltd.

6.11.3 bridge dhcp terminate enable 1839
6.11.4 bridge virtual-access forward-broadcast disable 1840
6.11.5 bridge vlan-transmit enable 1841
6.11.6 bridge (interface view) 1842
6.11.7 bridging disable 1844
6.11.8 display bridge information 1845
6.11.9 display bridge traffic 1848
6.11.10 display interface bridge-if 1851
6.11.11 display mac-address aging-time bridge 1855
6.11.12 display mac-address bridge 1856
6.11.13 fr map bridge 1860
6.11.14 interface bridge-if 1862
6.11.15 mac-address aging-time bridge 1863
6.11.16 mac-address blackhole bridge 1865
6.11.17 mac-address (Bridge-if interface view) 1866
6.11.18 mac-address static bridge 1868
6.11.19 map bridge broadcast 1870
6.11.20 reset bridge statistics 1871
6.11.21 reset counters interface bridge-if 1872
6.11.22 routing ip 1874
6.11.23 shutdown (bridge view) 1875
6.11.24 undo mac-address bridge 1876

7 WAN Commands 1878

7.1 DCC Configuration Commands 1878
7.1.1 dialer bundle 1878
7.1.2 dialer bundle-member 1880
7.1.3 dialer circular-group 1881
7.1.4 dialer disconnect 1883
7.1.5 dialer enable-circular 1884
7.1.6 dialer number 1885
7.1.7 dialer priority 1887
7.1.8 dialer queue-length 1889
7.1.9 dialer route 1890
7.1.10 dialer timer autodial 1892
7.1.11 dialer timer compete 1894
7.1.12 dialer timer enable 1895
7.1.13 dialer timer idle 1896
7.1.14 dialer timer wait-carrier 1897
7.1.15 dialer timer warmup 1899
7.1.16 dialer user 1900
7.1.17 dialer-group 1902
7.1.18 dialer retry limit 1903

7.1.19 dialer threshold 1905
7.1.20 dialer-rule (dialer-rule view) 1907
7.1.21 dialer-rule (system view) 1908
7.1.22 display dialer 1909
7.1.23 display interface dialer 1911
7.1.24 interface dialer 1914
7.1.25 standby routing-group 1915
7.1.26 standby routing-rule 1917
7.1.27 standby timer routing-disable 1918
7.2 PPP Configuration Commands 1919
7.2.1 display ppp compression iphc rtp 1920
7.2.2 display ppp compression iphc tcp 1921
7.2.3 display ppp compression stac-lzs 1923
7.2.4 display ppp information 1925
7.2.5 ip address ppp-negotiate 1931
7.2.6 ip tcp vjcompress 1932
7.2.7 link-protocol ppp 1934
7.2.8 ppp authentication-mode 1935
7.2.9 ppp chap password 1937
7.2.10 ppp chap user 1939
7.2.11 ppp compression iphc 1940
7.2.12 ppp compression iphc rtp-connections 1942
7.2.13 ppp compression iphc tcp-connections 1943
7.2.14 ppp compression stac-lzs 1945
7.2.15 ppp ipcp dns 1946
7.2.16 ppp ipcp dns admit-any 1947
7.2.17 ppp ipcp dns request 1949
7.2.18 ppp ipcp remote-address forced 1950
7.2.19 ppp ipcp default-route 1951
7.2.20 ppp keepalive retry-times 1952
7.2.21 ppp lcp remote-mru forced 1953
7.2.22 ppp pap local-user 1955
7.2.23 ppp peer hostroute-suppress 1957
7.2.24 ppp timer negotiate 1958
7.2.25 remote address 1959
7.2.26 reset ppp compression iphc 1961
7.2.27 reset ppp compression stac-lzs 1962
7.2.28 timer hold (PPP) 1963
7.3 MP Configuration Commands 1964
7.3.1 display interface mp-group 1964
7.3.2 display interface virtual-template 1967
7.3.3 display ppp mp 1970

7.3.4 discriminator ... 1973
7.3.5 interface mp-group ... 1974
7.3.6 interface virtual-template ... 1975
7.3.7 ppp mp ... 1976
7.3.8 ppp mp binding-mode ... 1978
7.3.9 ppp mp endpoint ... 1979
7.3.10 ppp mp fragment enable ... 1981
7.3.11 ppp multichassis-mp enable ... 1982
7.3.12 ppp mp least active-linknumber ... 1983
7.3.13 ppp mp lfi ... 1984
7.3.14 ppp mp lfi delay-per-frag ... 1985
7.3.15 ppp mp max-bind ... 1986
7.3.16 ppp mp min-fragment ... 1988
7.3.17 ppp mp reorder-window size ... 1989
7.3.18 ppp mp mp-group ... 1990
7.3.19 ppp mp user ... 1992
7.3.20 ppp mp virtual-template ... 1993
7.4 PPPoE Commands ... 1996
7.4.1 display pppoe-client session ... 1996
7.4.2 display pppoe-server session ... 1998
7.4.3 ppp keepalive in-traffic check ... 2000
7.4.4 pppoe-client dial-bundle-number ... 2000
7.4.5 ppp lcp sn accept ... 2003
7.4.6 ppp lcp imsi accept ... 2004
7.4.7 pppoe-server bind virtual-template ... 2005
7.4.8 pppoe-server max-sessions local-mac ... 2007
7.4.9 pppoe-server max-sessions total ... 2008
7.4.10 pppoe-server service-name ... 2009
7.4.11 pppoe-server log enable ... 2011
7.4.12 reset pppoe-client ... 2011
7.4.13 reset pppoe-server ... 2013
7.5 ATM Configuration Commands ... 2014
7.5.1 atm-cell qos enable ... 2014
7.5.2 atm-link check ... 2015
7.5.3 description (PVC view) ... 2016
7.5.4 display atm interface ... 2017
7.5.5 display atm map-info ... 2019
7.5.6 display atm pvc-group ... 2021
7.5.7 display atm pvc-info ... 2023
7.5.8 display atm pvc-info statistics ... 2026
7.5.9 encapsulation (PVC view) ... 2027
7.5.10 interface atm ... 2029

7.5.11 ip dscp 2031
7.5.12 ip precedence 2033
7.5.13 map bridge 2036
7.5.14 map bridge broadcast 2037
7.5.15 map ip 2039
7.5.16 map ppp 2041
7.5.17 oam ais-rdi 2043
7.5.18 oam cc end-to-end 2044
7.5.19 oam loopback 2045
7.5.20 oamping pvc 2046
7.5.21 pvc 2047
7.5.22 pvc-group 2050
7.5.23 pvc-protect 2052
7.5.24 pvc max-number 2053
7.5.25 pvp limit 2055
7.5.26 reset atm 2056
7.5.27 service cbr 2057
7.5.28 service ubr 2058
7.5.29 service vbr-nrt 2059
7.5.30 service vbr-rt 2061
7.6 Frame Relay Configuration Commands 2063
7.6.1 apply policy 2063
7.6.2 cbs outbound 2065
7.6.3 cir 2066
7.6.4 cir allow outbound 2067
7.6.5 display fr class 2068
7.6.6 display fr compression frf9 2070
7.6.7 display fr compression iphc 2072
7.6.8 display fr del 2075
7.6.9 display fr fragment-info 2076
7.6.10 display fr dlci-switch 2079
7.6.11 display fr inarp-info 2080
7.6.12 display fr interface 2081
7.6.13 display fr lmi-info 2083
7.6.14 display fr map-info 2085
7.6.15 display fr pvc-group 2087
7.6.16 display fr pvc-info 2090
7.6.17 display fr statistics 2092
7.6.18 display fr switch-table 2093
7.6.19 display interface mfr 2094
7.6.20 display mfr 2098
7.6.21 fr class 2101

7.6.22 fr compression frf9 2102
7.6.23 fr compression iphc 2104
7.6.24 fr de del 2106
7.6.25 fr del inbound-interface 2107
7.6.26 fr del protocol ip 2108
7.6.27 fr dlci 2111
7.6.28 fr dlci-switch 2112
7.6.29 fr inarp 2114
7.6.30 fr interface-type 2116
7.6.31 fr ip dscp 2117
7.6.32 fr ip precedence 2119
7.6.33 fr lmi n391dte 2121
7.6.34 fr lmi n392dce 2123
7.6.35 fr lmi n392dte 2124
7.6.36 fr lmi n393dce 2125
7.6.37 fr lmi n393dte 2127
7.6.38 fr lmi t392dce 2128
7.6.39 fr lmi type 2130
7.6.40 fr map bridge 2131
7.6.41 fr map ip 2133
7.6.42 fr map ppp 2137
7.6.43 fr pvc-group 2138
7.6.44 fr pvc-pq 2139
7.6.45 fr switch 2141
7.6.46 fr switching 2143
7.6.47 fr traffic-shaping 2144
7.6.48 fragment 2145
7.6.49 fr-class 2146
7.6.50 interface mfr 2147
7.6.51 link-protocol fr 2149
7.6.52 link-protocol fr mfr 2150
7.6.53 mfr bundle-name 2152
7.6.54 mfr fragment 2153
7.6.55 mfr fragment-size 2154
7.6.56 mfr link-name 2156
7.6.57 mfr retry 2157
7.6.58 mfr timer ack 2159
7.6.59 mfr timer hello 2160
7.6.60 mfr window-size 2162
7.6.61 pvc-pq 2164
7.6.62 reset fr inarp 2165
7.6.63 shutdown (FR interface view) 2166

 Copyright © Huawei Technologies Co., Ltd.

7.6.64 shutdown (FR switching view) 2167
7.6.65 timer hold (FR interface view) 2168
7.6.66 traffic-shaping adaptation 2170
7.7 HDLC Configuration Commands 2171
7.7.1 display hdlc error 2172
7.7.2 display hdlc statistics 2173
7.7.3 link-protocol hdlc 2174
7.7.4 timer hold (HDLC) 2175
7.8 LAPB Configuration Commands 2176
7.8.1 lapb max-frame 2176
7.8.2 lapb modulo 2178
7.8.3 lapb retry 2179
7.8.4 lapb timer 2180
7.8.5 lapb window-size 2182
7.8.6 link-protocol lapb 2183
7.8.7 display lapb status 2184
7.8.8 reset lapb statistics 2185
7.9 X.25 Configuration Commands 2186
7.9.1 display x25 alias-policy 2186
7.9.2 display x25 map 2187
7.9.3 display x25 switch-table pvc 2189
7.9.4 display x25 switch-table svc 2190
7.9.5 display x25 vc 2191
7.9.6 display x25 xot 2194
7.9.7 link-protocol x25 2195
7.9.8 reset x25 counters 2197
7.9.9 reset x25 vc 2198
7.9.10 reset xot 2199
7.9.11 x25 alias-policy 2200
7.9.12 x25 call-facility 2202
7.9.13 x25 default-protocol 2205
7.9.14 x25 facility packetsize-windowsize compatible enable 2206
7.9.15 x25 ignore called-address 2207
7.9.16 x25 ignore calling-address 2208
7.9.17 x25 map 2209
7.9.18 x25 modulo 2214
7.9.19 x25 packet-size 2215
7.9.20 x25 pvc 2217
7.9.21 x25 queue-length 2220
7.9.22 x25 receive-threshold 2222
7.9.23 x25 response called-address 2223
7.9.24 x25 response calling-address 2224

7.9.25 x25 reverse-charge-accept 2225
7.9.26 x25 roa-list 2226
7.9.27 x25 switch pvc 2227
7.9.28 x25 switch svc 2230
7.9.29 x25 switch svc xot 2232
7.9.30 x25 switching 2235
7.9.31 x25 timer hold 2236
7.9.32 x25 timer idle 2237
7.9.33 x25 timer tx0 2239
7.9.34 x25 timer tx1 2240
7.9.35 x25 timer tx2 2241
7.9.36 x25 timer tx3 2242
7.9.37 x25 vc-per-map 2244
7.9.38 x25 vc-range 2245
7.9.39 x25 window-size 2248
7.9.40 x25 x121-address 2251
7.9.41 x25 xot pvc 2252
7.10 IP-Trunk Commands 2255
7.10.1 display interface ip-trunk 2256
7.10.2 display trunkfwdtbl ip-trunk 2259
7.10.3 display trunkmembership ip-trunk 2260
7.10.4 display trunk resource 2261
7.10.5 interface ip-trunk 2262
7.10.6 ip-trunk 2263
7.10.7 least active-linknumber (IP-Trunk interface view) 2265
7.10.8 load-balance 2266
7.10.9 reset counters interface ip-trunk 2268
7.10.10 shutdown (IP-Trunk interface view) 2269
7.10.11 trunkport (IP-Trunk interface view) 2270
7.11 ISDN Configuration Commands 2271
7.11.1 dialer isdn-leased 2271
7.11.2 dialer isdn-leased 128k 2273
7.11.3 display isdn active-channel 2274
7.11.4 display isdn call-info 2276
7.11.5 display isdn call-record 2285
7.11.6 display isdn dss1-parameters 2287
7.11.7 isdn bch-assign 2290
7.11.8 isdn bch-local-manage 2292
7.11.9 isdn bch-select-way 2293
7.11.10 isdn caller-number 2294
7.11.11 isdn calling 2296
7.11.12 isdn check-called-number 2297

7.11.13 isdn check-time....2298
7.11.14 isdn crlength....2299
7.11.15 isdn ignore connect-ack....2301
7.11.16 isdn ignore sending-complete....2302
7.11.17 isdn l3-timer....2303
7.11.18 isdn link-mode....2308
7.11.19 isdn number-property....2309
7.11.20 isdn overlap-receiving....2312
7.11.21 isdn overlap-sending....2313
7.11.22 isdn pri-slipwnd-size....2314
7.11.23 isdn q921-permanent....2316
7.11.24 isdn send-restart....2317
7.11.25 isdn statistics....2317
7.11.26 permanent-active....2319
7.12 Modem Configuration Commands....2320
7.12.1 modem....2320
7.12.2 modem auto-answer....2321
7.12.3 modem timer answer....2322
7.12.4 sendat....2323
7.12.5 service modem-callback....2326
7.13 RTC Configuration Commands....2327
7.13.1 auto-close....2327
7.13.2 auto-link....2328
7.13.3 display rta....2330
7.13.4 reset rta statistics....2334
7.13.5 rta broadcast master-interface enable....2335
7.13.6 rta broadcast slave-interface....2337
7.13.7 rta rtc-server listen-port....2339
7.13.8 rta server enable....2340
7.13.9 rta template....2341
7.13.10 rta terminal....2342
7.13.11 tcp keepalive....2344
7.13.12 tcp nodelay....2345
7.13.13 tcp nodelay enhance....2346
7.13.14 tcp recvbuf-size....2348
7.13.15 tcp sendbuf-size....2349
7.13.16 vty rtc-client remote....2350
7.13.17 vty rtc-server remote....2352
7.14 CESoP Configuration Commands....2354
7.14.1 cesop connect....2354
7.14.2 cesop tdm-encapsulation-number....2355
7.14.3 cesop jitter-buffer....2357

 Copyright © Huawei Technologies Co., Ltd.

7.14.4 display cesop connect interface 2358

8 IP Service Commands 2360

8.1 IPv4 Configuration Commands 2360
8.1.1 ip address 2360
8.1.2 ip address unnumbered 2362
8.1.3 display ip interface 2364
8.1.4 display interface 2370
8.2 ARP Configuration Commands 2382
8.2.1 arp detect-mode unicast 2382
8.2.2 arp detect-times 2383
8.2.3 arp expire-time 2384
8.2.4 arp learning multicast enable (system view) 2386
8.2.5 arp-ping ip 2387
8.2.6 arp-ping mac 2388
8.2.7 arp-proxy enable 2390
8.2.8 arp-proxy inner-sub-vlan-proxy enable 2391
8.2.9 arp-proxy inter-sub-vlan-proxy enable 2392
8.2.10 arp regularly-refresh enable 2393
8.2.11 arp send-packet 2394
8.2.12 arp static 2395
8.2.13 arp-suppress enable 2398
8.2.14 display arp 2399
8.2.15 display arp error packet 2402
8.2.16 display arp interface 2404
8.2.17 display arp ip-conflict track 2407
8.2.18 display arp dynamic 2408
8.2.19 display arp dynamic vlan 2411
8.2.20 display arp network 2414
8.2.21 display arp packet statistics 2417
8.2.22 display arp static 2418
8.2.23 display arp statistics 2420
8.2.24 display arp track 2421
8.2.25 display arp vpn-instance 2423
8.2.26 display mac-address multiport 2425
8.2.27 display snmp-agent trap feature-name arp all 2427
8.2.28 l2-topology detect enable 2429
8.2.29 mac-address multiport 2429
8.2.30 mac-address multiport interface 2431
8.2.31 reset arp 2433
8.2.32 reset arp packet statistics 2435
8.2.33 snmp-agent trap enable feature-name arp 2435
8.3 DHCP Configuration Commands 2436

8.3.1 alarm ip-used percentage....2437
8.3.2 bootfile....2438
8.3.3 conflict auto-recycle interval....2439
8.3.4 dhcp alarm dhcp-rate enable....2441
8.3.5 dhcp alarm dhcp-rate threshold....2442
8.3.6 dhcp check dhcp-rate enable....2443
8.3.7 dhcp check dhcp-rate....2445
8.3.8 dhcp client class-id (interface view)....2447
8.3.9 dhcp client class-id (system view)....2448
8.3.10 dhcp client client-id....2449
8.3.11 dhcp client expected-lease....2450
8.3.12 dhcp client gateway-detect....2451
8.3.13 dhcp client default-route preference....2452
8.3.14 dhcp client hostname....2453
8.3.15 dhcp client renew....2454
8.3.16 dhcp client request option-list exclude....2455
8.3.17 dhcp client request option-list....2457
8.3.18 dhcp enable....2458
8.3.19 dhcp link arp....2459
8.3.20 dhcp option template....2460
8.3.21 dhcp relay release....2461
8.3.22 dhcp relay server-ip....2463
8.3.23 dhcp relay server-select....2465
8.3.24 dhcp relay trust option82....2466
8.3.25 dhcp select global....2467
8.3.26 dhcp select interface....2469
8.3.27 dhcp server alarm ip-used percentage....2470
8.3.28 dhcp select relay....2472
8.3.29 dhcp server bootfile....2473
8.3.30 dhcp server bootp....2475
8.3.31 dhcp server bootp automatic....2476
8.3.32 dhcp server conflict auto-recycle interval....2477
8.3.33 dhcp server database....2478
8.3.34 dhcp server dns-list....2480
8.3.35 dhcp server domain-name (interface view)....2482
8.3.36 dhcp server excluded-ip-address....2483
8.3.37 dhcp server gateway-list....2485
8.3.38 dhcp server force insert option....2486
8.3.39 dhcp server force response....2488
8.3.40 dhcp server group....2489
8.3.41 dhcp server import all....2491
8.3.42 dhcp server ip-range....2492

8.3.43 dhcp server lease 2493
8.3.44 dhcp server logging 2495
8.3.45 dhcp server mask 2497
8.3.46 dhcp server nbns-list 2498
8.3.47 dhcp server netbios-type 2500
8.3.48 dhcp server next-server 2502
8.3.49 dhcp server option 2503
8.3.50 dhcp server option121 2506
8.3.51 dhcp server option184 2508
8.3.52 dhcp server ping 2509
8.3.53 dhcp server sip-server 2510
8.3.54 dhcp server sname 2512
8.3.55 dhcp server static-bind 2513
8.3.56 dhcp server trust option82 2515
8.3.57 dhcp set ttl 2516
8.3.58 dhcp speed-limit auto 2518
8.3.59 dhcp-server 2519
8.3.60 display dhcp client 2520
8.3.61 display dhcp client statistics 2522
8.3.62 display dhcp server configuration 2524
8.3.63 display dhcp configuration 2526
8.3.64 display dhcp option template 2528
8.3.65 display dhcp relay 2531
8.3.66 display dhcp relay statistics 2533
8.3.67 display dhcp server database 2535
8.3.68 display dhcp server group 2537
8.3.69 display dhcp server statistics 2538
8.3.70 display dhcp statistics 2540
8.3.71 display ip pool 2544
8.3.72 display ip pool import all 2551
8.3.73 display snmp-agent trap feature-name dhcp all 2552
8.3.74 display snmp-agent trap feature-name mid_am all 2556
8.3.75 dns-list 2558
8.3.76 domain-name 2560
8.3.77 excluded-ip-address 2561
8.3.78 force insert option 2563
8.3.79 gateway (DHCP server group view) 2564
8.3.80 gateway-list 2565
8.3.81 ip address bootp-alloc 2567
8.3.82 ip address dhcp-alloc 2568
8.3.83 ip pool (system view) 2570
8.3.84 import all 2571

8.3.85 ip relay address cycle 2572
8.3.86 ip route dhcp 2573
8.3.87 lease 2575
8.3.88 lock (IP address pool view) 2576
8.3.89 logging (IP address pool view) 2579
8.3.90 nbns-list 2581
8.3.91 netbios-type 2583
8.3.92 network (IP address pool view) 2584
8.3.93 next-server 2586
8.3.94 option 2587
8.3.95 option121 2590
8.3.96 option184 2592
8.3.97 reset dhcp client statistics 2593
8.3.98 reset dhcp relay statistics 2594
8.3.99 reset dhcp server statistics 2596
8.3.100 reset dhcp statistics 2596
8.3.101 reset ip pool 2597
8.3.102 reset ip pool import 2599
8.3.103 section (IP address pool view) 2600
8.3.104 sip-server (IP address pool view) 2601
8.3.105 sname 2603
8.3.106 snmp-agent trap enable feature-name dhcp 2604
8.3.107 snmp-agent trap enable feature-name mid_am 2608
8.3.108 static-bind 2609
8.3.109 vpn-instance (DHCP server group view) 2612
8.3.110 vpn-instance (global address pool view) 2613
8.4 DNS Configuration Commands 2614
8.4.1 ddns apply policy 2615
8.4.2 display ddns interface 2616
8.4.3 display ddns policy 2618
8.4.4 display dns configuration 2619
8.4.5 display dns domain 2622
8.4.6 display dns dynamic-host 2623
8.4.7 display dns forward table 2626
8.4.8 display dns statistics 2627
8.4.9 display dns server 2629
8.4.10 display ip host 2631
8.4.11 ddns policy 2632
8.4.12 dns domain 2633
8.4.13 dns forward retry-number 2634
8.4.14 dns forward retry-timeout 2636
8.4.15 dns proxy enable 2637

8.4.16 dns proxy sip-info insert-mode decompression-domain-name....2638
8.4.17 dns relay enable....2639
8.4.18 dns resolve....2640
8.4.19 dns server....2641
8.4.20 dns server vpn-instance....2643
8.4.21 dns server source-ip....2644
8.4.22 dns-server-select-algorithm....2646
8.4.23 dns spoofing....2647
8.4.24 interval (DDNS policy view)....2648
8.4.25 ip host....2649
8.4.26 method (DDNS policy view)....2650
8.4.27 name-server (DDNS policy view)....2653
8.4.28 reset ddns policy....2655
8.4.29 reset dns dynamic-host....2655
8.4.30 reset dns forward table....2656
8.4.31 reset dns statistics....2657
8.4.32 ssl-policy (ddns-policy-view)....2658
8.4.33 url (DDNS policy view)....2659
8.4.34 dns resolve policy a....2663
8.4.35 rule (DNS resolution policy view)....2664
8.5 NAT Configuration Commands....2666
8.5.1 display firewall-nat session aging-time....2666
8.5.2 display nat address-group....2669
8.5.3 display nat alg....2670
8.5.4 display nat sip cac bandwidth information....2671
8.5.5 display nat dns-map....2673
8.5.6 display nat filter-mode....2674
8.5.7 display nat outbound....2675
8.5.8 display nat overlap-address....2677
8.5.9 display nat server....2678
8.5.10 display nat session....2680
8.5.11 display nat static....2682
8.5.12 display nat static interface enable....2684
8.5.13 display nat mapping-mode....2685
8.5.14 display nat mapping table....2686
8.5.15 firewall-nat session aging-time....2688
8.5.16 nat address-group....2691
8.5.17 nat alg....2693
8.5.18 nat sip cac enable....2694
8.5.19 nat dns-map....2696
8.5.20 nat filter-mode....2697
8.5.21 nat inside priority enable....2699

8.5.22 nat log-format elog....2700
8.5.23 nat miss forward deny....2701
8.5.24 nat outbound....2702
8.5.25 nat outbound (Easy-IP)....2704
8.5.26 nat overlap-address....2706
8.5.27 nat server....2709
8.5.28 nat session limit....2713
8.5.29 nat static (interface view)....2715
8.5.30 nat static (system view)....2720
8.5.31 nat static enable....2724
8.5.32 nat mapping-mode....2725
8.5.33 port-mapping....2727
8.5.34 reset nat session....2728
8.5.35 set nat-session self-healing enable....2731
8.5.36 tcp proxy....2731
8.5.37 tcp proxy aging-time....2733
8.6 UDP Helper Configuration Commands....2734
8.6.1 display udp-helper port....2734
8.6.2 display udp-helper server....2735
8.6.3 reset udp-helper packet....2737
8.6.4 udp-helper enable....2738
8.6.5 udp-helper port....2740
8.6.6 udp-helper server....2742
8.7 IP Performance Configuration Commands....2743
8.7.1 broadcast routing disable....2743
8.7.2 clear ip df....2744
8.7.3 control-packet output car bypass....2745
8.7.4 control-packet output filter bypass....2747
8.7.5 control-packet output queue bypass....2750
8.7.6 display forward pie counter....2752
8.7.7 discard { ra | rr | srr | ts }....2753
8.7.8 display icmp statistics....2754
8.7.9 display ip socket....2756
8.7.10 display ip socket register-port....2761
8.7.11 display ip statistics....2763
8.7.12 display load-sharing....2765
8.7.13 display network status....2767
8.7.14 display rawip statistics....2768
8.7.15 display tcp statistics....2770
8.7.16 display tcp status....2773
8.7.17 display udp statistics....2776
8.7.18 icmp blackhole unreachable send....2778

 Copyright © Huawei Technologies Co., Ltd.

8.7.19 icmp host-unreachable send 2779
8.7.20 icmp port-unreachable send 2780
8.7.21 icmp time-exceed 2781
8.7.22 icmp ttl-exceeded drop 2782
8.7.23 icmp ttl-exceeded send 2783
8.7.24 icmp unreachable drop 2784
8.7.25 icmp with-options drop 2785
8.7.26 icmp receive 2785
8.7.27 icmp-reply fast 2787
8.7.28 ip forward-broadcast 2788
8.7.29 ip soft-forward enhance enable 2790
8.7.30 ip verify source-address 2791
8.7.31 ip option-virtual-reassembly 2793
8.7.32 ip virtual-reassembly 2794
8.7.33 load-balance unequal-cost enable 2795
8.7.34 load-balance bandwidth 2797
8.7.35 reset forward pie counter 2798
8.7.36 reset ip socket monitor 2799
8.7.37 reset ip socket pktsort 2800
8.7.38 reset ip statistics 2800
8.7.39 reset rawip statistics 2801
8.7.40 reset tcp statistics 2802
8.7.41 reset udp statistics 2803
8.7.42 set priority dscp 2803
8.7.43 set priority dot1p 2805
8.7.44 set workmode lan-card l3centralize 2806
8.7.45 tcp adjust-mss 2808
8.7.46 tcp min-mss 2809
8.7.47 tcp timer fin-timeout 2811
8.7.48 tcp timer pathmtu-age 2812
8.7.49 tcp timer syn-timeout 2813
8.7.50 tcp window 2814
8.8 Basic IPv6 Configuration Commands 2815
8.8.1 control-packet-ipv6 output car bypass 2815
8.8.2 control-packet-ipv6 output filter bypass 2818
8.8.3 control-packet-ipv6 output queue bypass 2820
8.8.4 display default-parameter tcp6 2822
8.8.5 display icmpv6 statistics 2824
8.8.6 display ipv6 address-policy 2827
8.8.7 display ipv6 attack-source overlapping-fragment 2829
8.8.8 display ipv6 interface 2830
8.8.9 display ipv6 interface tunnel 2832

8.8.10 display ipv6 neighbors....2834
8.8.11 display ipv6 pathmtu....2838
8.8.12 display ipv6 socket....2840
8.8.13 display ipv6 statistics....2843
8.8.14 display rawip ipv6 statistics....2846
8.8.15 display tcp ipv6 authentication-statistics....2847
8.8.16 display tcp ipv6 statistics....2850
8.8.17 display tcp ipv6 status....2854
8.8.18 display this ipv6 interface....2858
8.8.19 display udp ipv6 statistics....2859
8.8.20 ipv6....2861
8.8.21 ipv6 address....2862
8.8.22 ipv6 address anycast....2864
8.8.23 ipv6 address auto global....2866
8.8.24 ipv6 address auto link-local....2867
8.8.25 ipv6 address eui-64....2868
8.8.26 ipv6 address link-local....2870
8.8.27 ipv6 address-policy....2872
8.8.28 ipv6 enable (interface view)....2874
8.8.29 ipv6 icmp blackhole unreachable send....2875
8.8.30 ipv6 icmp-error....2876
8.8.31 ipv6 icmp port-unreachable send....2877
8.8.32 ipv6 icmp hop-limit-exceeded send....2878
8.8.33 ipv6 icmp receive....2879
8.8.34 ipv6 icmp send....2881
8.8.35 ipv6 icmp too-big-rate-limit....2883
8.8.36 ipv6 mtu....2884
8.8.37 ipv6 nd autoconfig managed-address-flag....2885
8.8.38 ipv6 nd autoconfig other-flag....2887
8.8.39 ipv6 nd dad attempts....2888
8.8.40 ipv6 nd hop-limit....2890
8.8.41 ipv6 nd learning strict....2891
8.8.42 ipv6 nd neighbor-limit....2893
8.8.43 ipv6 nd ns multicast-enable....2894
8.8.44 ipv6 nd ns retrans-timer....2895
8.8.45 ipv6 nd nud reachable-time....2897
8.8.46 ipv6 nd ra....2898
8.8.47 ipv6 nd ra halt....2900
8.8.48 ipv6 nd ra hop-limit....2901
8.8.49 ipv6 nd ra preference....2902
8.8.50 ipv6 nd ra prefix....2904
8.8.51 ipv6 nd ra route-information....2906

8.8.52 ipv6 nd ra router-lifetime 2908
8.8.53 ipv6 nd stale-timeout 2910
8.8.54 ipv6 neighbor 2911
8.8.55 ipv6 pathmtu 2913
8.8.56 ipv6 pathmtu age 2915
8.8.57 ipv6 soft-forward enhance enable 2916
8.8.58 reset ipv6 address-policy 2917
8.8.59 reset ipv6 attack-source overlapping-fragment 2918
8.8.60 reset ipv6 neighbors 2918
8.8.61 reset ipv6 pathmtu 2920
8.8.62 reset ipv6 socket pktsort 2921
8.8.63 reset ipv6 statistics 2922
8.8.64 reset rawip ipv6 statistics 2923
8.8.65 reset tcp ipv6 authentication-statistics 2923
8.8.66 reset tcp ipv6 statistics 2924
8.8.67 reset udp ipv6 statistics 2925
8.8.68 set priority acl6 dscp 2926
8.8.69 set priority protocol-type-ipv6 dscp 2928
8.8.70 tcp ipv6 max-mss 2929
8.8.71 tcp ipv6 min-mss 2931
8.8.72 tcp ipv6 timer fin-timeout 2932
8.8.73 tcp ipv6 timer syn-timeout 2933
8.8.74 tcp ipv6 window 2934
8.9 DHCPv6 Configuration Commands 2935
8.9.1 address prefix 2935
8.9.2 capwap-ac (IPv6 address pool view) 2939
8.9.3 conflict-address expire-time 2940
8.9.4 dhcpv6 client information-request 2941
8.9.5 dhcpv6 client pd 2943
8.9.6 dhcpv6 duid 2945
8.9.7 dhcpv6 client renew 2947
8.9.8 renew-time-percent rebind-time-percent 2947
8.9.9 dhcpv6 interface-id format 2949
8.9.10 dhcpv6 interface-id insert enable 2952
8.9.11 dhcpv6 packet-rate 2953
8.9.12 dhcpv6 packet-rate drop-alarm enable 2954
8.9.13 dhcpv6 packet-rate drop-alarm threshold 2956
8.9.14 dhcpv6 pool 2957
8.9.15 dhcpv6 relay destination 2958
8.9.16 dhcpv6 relay server-select 2960
8.9.17 dhcpv6 relay source-interface 2961
8.9.18 dhcpv6 relay option79 insert enable 2963

 Copyright © Huawei Technologies Co., Ltd.

8.9.19 dhcpv6 remote-id format 2965
8.9.20 dhcpv6 remote-id insert enable 2970
8.9.21 dhcpv6 server (system view) 2971
8.9.22 dhcpv6 server (interface view) 2974
8.9.23 dhcpv6-server 2977
8.9.24 dhcpv6 server database 2978
8.9.25 dhcpv6 server group 2979
8.9.26 display dhcpv6 client 2981
8.9.27 display dhcpv6 client prefix 2983
8.9.28 display dhcpv6 client statistics 2984
8.9.29 display dhcpv6 duid 2986
8.9.30 display dhcpv6 relay configuration 2987
8.9.31 display dhcpv6 relay statistics 2988
8.9.32 display dhcpv6 pool 2990
8.9.33 display dhcpv6 relay 2994
8.9.34 display dhcpv6 server 2995
8.9.35 display dhcpv6 server group 2997
8.9.36 display dhcpv6 statistics 2998
8.9.37 display import all 3003
8.9.38 dns-domain-name 3004
8.9.39 dns-server (IPv6 address pool view) 3006
8.9.40 excluded-address 3007
8.9.41 information-refresh 3009
8.9.42 ipv6 address auto dhcp 3010
8.9.43 link-address 3012
8.9.44 lock (IPv6 address pool view) 3014
8.9.45 nis-domain-name 3015
8.9.46 nisp-domain-name 3016
8.9.47 nisp-server 3017
8.9.48 nis-server 3018
8.9.49 prefix-delegation 3020
8.9.50 reset dhcpv6 client statistics 3023
8.9.51 reset dhcpv6 pool 3024
8.9.52 reset dhcpv6 relay statistics 3026
8.9.53 reset dhcpv6 server statistics 3027
8.9.54 reset dhcpv6 statistics 3028
8.9.55 sip-domain-name 3029
8.9.56 sip-server (IPv6 address pool view) 3030
8.9.57 sntp-server 3031
8.9.58 static-bind address 3032
8.9.59 static-bind prefix 3034
8.9.60 suboption 3036

 Copyright © Huawei Technologies Co., Ltd.

8.9.61 vendor-specific ... 3038
8.9.62 import all (IPv6 address pool view) ... 3039
8.10 IPv6 DNS Configuration Commands ... 3040
8.10.1 dns proxy ipv6 enable ... 3040
8.10.2 dns relay ipv6 enable ... 3041
8.10.3 display dns ipv6 dynamic-host ... 3042
8.10.4 display dns ipv6 forward table ... 3043
8.10.5 display ipv6 host ... 3044
8.10.6 dns server ipv6 ... 3046
8.10.7 dns server ipv6 source-ip ... 3047
8.10.8 dns spoofing ipv6 ... 3048
8.10.9 ipv6 host ... 3050
8.10.10 reset dns ipv6 dynamic-host ... 3051
8.10.11 reset dns ipv6 forward table ... 3052
8.11 IPv6 over IPv4 Tunnel Configuration Commands ... 3052
8.11.1 destination ... 3053
8.11.2 interface tunnel ... 3054
8.11.3 source ... 3056
8.11.4 tunnel-protocol ... 3058
8.12 IPv4 over IPv6 Tunnel Configuration Commands ... 3060
8.12.1 display interface tunnel ... 3060
8.12.2 tunnel ipv4-ipv6 encapsulation-limit ... 3064
8.12.3 tunnel ipv4-ipv6 flow-label ... 3065
8.12.4 tunnel ipv4-ipv6 hop-limit ... 3066
8.12.5 tunnel ipv4-ipv6 traffic-class ... 3067

9 IP Unicast Routing Commands ... 3069

9.1 Static Route Configuration Commands ... 3069
9.1.1 ip route recursive-lookup bgp-vpnv4-route ... 3069
9.1.2 ip route recursive-lookup blackhole protocol static ... 3071
9.1.3 ip route-static ... 3072
9.1.4 ip route-static default-preference ... 3076
9.1.5 ip route-static selection-rule relay-depth ... 3077
9.1.6 ip route-static vpn-instance ... 3078
9.1.7 ip route-static track bfd-session admindown invalid ... 3082
9.1.8 ipv6 route-static ... 3083
9.1.9 ipv6 route-static default-preference ... 3086
9.1.10 ipv6 route-static track bfd-session admindown invalid ... 3087
9.1.11 ipv6 route-static vpn-instance ... 3089
9.1.12 routing-table download filter ... 3092
9.2 RIP Configuration Commands ... 3094
9.2.1 bfd all-interfaces enable (RIP) ... 3094
9.2.2 bfd all-interfaces (RIP) ... 3095

9.2.3 checkzero (RIP) 3096
9.2.4 default-cost (RIP) 3097
9.2.5 default-route originate 3098
9.2.6 description (RIP) 3100
9.2.7 display default-parameter rip 3101
9.2.8 display rip 3104
9.2.9 display rip bfd session 3107
9.2.10 display rip database 3109
9.2.11 display rip graceful-restart 3110
9.2.12 display rip interface 3112
9.2.13 display rip neighbor 3115
9.2.14 display rip neighbor last-nbr-down 3117
9.2.15 display rip route 3118
9.2.16 display snmp-agent trap feature-name rip all 3119
9.2.17 display rip statistics interface 3121
9.2.18 filter-policy export (RIP) 3123
9.2.19 filter-policy import (RIP) 3125
9.2.20 graceful-restart (RIP) 3127
9.2.21 host-route 3128
9.2.22 import-route (RIP) 3129
9.2.23 maximum load-balancing (RIP) 3131
9.2.24 network (RIP) 3132
9.2.25 peer (RIP) 3134
9.2.26 preference (RIP) 3135
9.2.27 reset rip configuration 3136
9.2.28 reset rip statistics 3137
9.2.29 rip 3138
9.2.30 rip authentication-mode 3139
9.2.31 rip bfd 3142
9.2.32 rip bfd block 3143
9.2.33 rip bfd enable 3144
9.2.34 rip bfd static 3145
9.2.35 rip input 3146
9.2.36 rip metricin 3147
9.2.37 rip metricout 3149
9.2.38 rip mib-binding 3150
9.2.39 rip output 3151
9.2.40 rip pkt-transmit 3152
9.2.41 rip poison-reverse 3153
9.2.42 rip replay-protect 3154
9.2.43 rip split-horizon 3155
9.2.44 rip summary-address 3156

9.2.45 rip valid-ttl-hops ... 3157
9.2.46 rip version ... 3159
9.2.47 silent-interface (RIP) ... 3160
9.2.48 summary (RIP) ... 3162
9.2.49 snmp-agent trap enable feature-name rip ... 3163
9.2.50 timers rip ... 3165
9.2.51 verify-source (RIP) ... 3166
9.2.52 version (RIP) ... 3167
9.3 RIPng Configuration Commands ... 3168
9.3.1 checkzero (RIPng) ... 3168
9.3.2 default-cost (RIPng) ... 3169
9.3.3 description (RIPng) ... 3170
9.3.4 display default-parameter ripng ... 3171
9.3.5 display ripng ... 3173
9.3.6 display ripng database ... 3175
9.3.7 display ripng interface ... 3176
9.3.8 display ripng neighbor ... 3178
9.3.9 display ripng neighbor last-nbr-down ... 3179
9.3.10 display ripng route ... 3180
9.3.11 display ripng statistics interface ... 3182
9.3.12 filter-policy export (RIPng) ... 3184
9.3.13 filter-policy import (RIPng) ... 3186
9.3.14 import-route (RIPng) ... 3187
9.3.15 maximum load-balancing (RIPng) ... 3189
9.3.16 preference (RIPng) ... 3190
9.3.17 reset ripng statistics ... 3191
9.3.18 ripng ... 3193
9.3.19 ripng default-route ... 3194
9.3.20 ripng input ... 3195
9.3.21 ripng enable ... 3196
9.3.22 ripng metricin ... 3197
9.3.23 ripng metricout ... 3198
9.3.24 ripng output ... 3199
9.3.25 ripng pkt-transmit ... 3200
9.3.26 ripng poison-reverse ... 3201
9.3.27 ripng split-horizon ... 3202
9.3.28 ripng summary-address ... 3204
9.3.29 timers ripng ... 3205
9.4 OSPF Configuration Commands ... 3206
9.4.1 abr-summary (OSPF area) ... 3206
9.4.2 area (OSPF) ... 3208
9.4.3 asbr-summary ... 3210

9.4.4 authentication-mode (OSPF area) 3212
9.4.5 bandwidth-reference (OSPF) 3215
9.4.6 bfd all-interfaces (OSPF) 3217
9.4.7 default (OSPF) 3219
9.4.8 default-cost (OSPF Aera) 3221
9.4.9 default-route-advertise (OSPF) 3222
9.4.10 description (OSPF) 3226
9.4.11 description (OSPF Area) 3227
9.4.12 display default-parameter ospf 3228
9.4.13 display gtsm statistics 3231
9.4.14 display ospf abr-asbr 3232
9.4.15 display ospf asbr-summary 3234
9.4.16 display ospf bfd session 3236
9.4.17 display ospf brief 3238
9.4.18 display ospf cumulative 3243
9.4.19 display ospf error 3246
9.4.20 display ospf global-statistics 3252
9.4.21 display ospf graceful-restart 3255
9.4.22 display ospf interface 3261
9.4.23 display ospf lsdb 3266
9.4.24 display ospf migp-routing 3274
9.4.25 display ospf mesh-group 3277
9.4.26 display ospf nexthop 3279
9.4.27 display ospf peer 3280
9.4.28 display ospf request-queue 3287
9.4.29 display ospf retrans-queue 3288
9.4.30 display ospf routing 3290
9.4.31 display ospf sham-link 3292
9.4.32 display ospf spf-statistics 3293
9.4.33 display ospf statistics updated-lsa 3296
9.4.34 display ospf vlink 3300
9.4.35 display snmp-agent trap feature-name ospf all 3301
9.4.36 dn-bit-set 3304
9.4.37 dn-bit-check 3306
9.4.38 domain-id (OSPF) 3308
9.4.39 eca-route-type compatible 3309
9.4.40 enable log 3311
9.4.41 filter export (OSPF Area) 3312
9.4.42 filter import (OSPF Area) 3313
9.4.43 filter-lsa-out peer 3315
9.4.44 filter-policy export (OSPF) 3317
9.4.45 filter-policy import (OSPF) 3319

9.4.46 flooding-control 3320
9.4.47 frr (OSPF) 3321
9.4.48 frr-policy route (OSPF FRR) 3323
9.4.49 frr-priority static low 3324
9.4.50 graceful-restart (OSPF) 3325
9.4.51 graceful-restart helper-role (OSPF) 3327
9.4.52 gtsm default-action 3329
9.4.53 gtsm log drop-packet 3331
9.4.54 import-route (OSPF) 3332
9.4.55 local-mt filter-policy (OSPF) 3336
9.4.56 local-mt enable (OSPF) 3338
9.4.57 loop-free-alternate (OSPF FRR) 3339
9.4.58 lsa-arrival-interval 3341
9.4.59 lsa-originate-interval 3343
9.4.60 lsdb-overflow-limit 3345
9.4.61 maxage-lsa route-calculate-delay (OSPF) 3346
9.4.62 maximum load-balancing (OSPF) 3347
9.4.63 maximum-routes 3349
9.4.64 mesh-group enable 3351
9.4.65 network (OSPF Area) 3352
9.4.66 nexthop (OSPF) 3354
9.4.67 nssa (OSPF Area) 3355
9.4.68 opaque-capability enable 3358
9.4.69 ospf 3359
9.4.70 ospf authentication-mode 3361
9.4.71 ospf bfd 3365
9.4.72 ospf bfd block 3367
9.4.73 ospf cost 3368
9.4.74 ospf dr-priority 3370
9.4.75 ospf enable 3371
9.4.76 ospf filter-lsa-out 3373
9.4.77 ospf frr block 3374
9.4.78 ospf maxage-lsa auto-protect disable 3375
9.4.79 ospf mib-binding 3376
9.4.80 ospf mtu-enable 3377
9.4.81 ospf network-type 3379
9.4.82 ospf p2mp-mask-ignore 3381
9.4.83 ospf router-id auto-recover disable 3382
9.4.84 ospf smart-discover 3383
9.4.85 ospf suppress-flapping peer 3384
9.4.86 ospf suppress-flapping peer disable 3386
9.4.87 ospf suppress-flapping peer hold-down 3387

9.4.88 ospf suppress-flapping peer hold-max-cost disable 3388
9.4.89 ospf timer dead 3390
9.4.90 ospf timer hello 3391
9.4.91 ospf timer poll 3393
9.4.92 ospf timer retransmit 3394
9.4.93 ospf trans-delay 3395
9.4.94 ospf valid-ttl-hops 3396
9.4.95 peer (OSPF) 3398
9.4.96 preference (OSPF) 3399
9.4.97 prefix-priority (OSPF) 3401
9.4.98 reset gtsm statistics 3402
9.4.99 reset ospf counters 3403
9.4.100 reset ospf counters maxage-lsa 3404
9.4.101 reset ospf process 3405
9.4.102 reset ospf redistribution 3407
9.4.103 reset ospf suppress-flapping peer 3408
9.4.104 retransmission-limit 3409
9.4.105 route-tag 3410
9.4.106 rfc1583 compatible 3412
9.4.107 sham-hello enable (OSPF) 3413
9.4.108 sham-link (OSPF Area) 3413
9.4.109 silent-interface (OSPF) 3418
9.4.110 snmp-agent trap enable feature-name ospf 3419
9.4.111 spf-schedule-interval 3423
9.4.112 stub (OSPF area) 3425
9.4.113 stub-router (OSPF) 3426
9.4.114 suppress-flapping peer disable (OSPF) 3428
9.4.115 vlink-peer (OSPF area) 3429
9.4.116 vpn-instance-capability simple (OSPF) 3433
9.5 OSPFv3 Configuration Commands 3435
9.5.1 abr-summary (OSPFv3 Area) 3435
9.5.2 area (OSPFv3) 3436
9.5.3 asbr-summary (OSPFv3) 3437
9.5.4 authentication-mode (OSPFv3) 3439
9.5.5 bandwidth-reference (OSPFv3) 3441
9.5.6 bfd all-interfaces (OSPFv3) 3442
9.5.7 default (OSPFv3) 3445
9.5.8 default-cost (OSPFv3 Area) 3446
9.5.9 default-route-advertise (OSPFv3) 3447
9.5.10 description (OSPFv3 Area) 3449
9.5.11 description (OSPFv3) 3450
9.5.12 display default-parameter ospfv3 3451

9.5.13 display ospfv3 ... 3455
9.5.14 display ospfv3 abr-summary-list ... 3457
9.5.15 display ospfv3 area ... 3459
9.5.16 display ospfv3 asbr-summary ... 3460
9.5.17 display ospfv3 black-box neighbor-down ... 3462
9.5.18 display ospfv3 bfd session ... 3464
9.5.19 display ospfv3 error ... 3467
9.5.20 display ospfv3 graceful-restart-information ... 3470
9.5.21 display ospfv3 interface ... 3473
9.5.22 display ospfv3 lsdb ... 3478
9.5.23 display ospfv3 next-hop ... 3482
9.5.24 display ospfv3 path ... 3483
9.5.25 display ospfv3 peer ... 3485
9.5.26 display ospfv3 request-list ... 3487
9.5.27 display ospfv3 retrans-list ... 3489
9.5.28 display ospfv3 routing ... 3490
9.5.29 display ospfv3 topology ... 3492
9.5.30 display ospfv3 vlink ... 3494
9.5.31 display ospfv3 statistics maxage-lsa ... 3496
9.5.32 display snmp-agent trap feature-name ospfv3 all ... 3497
9.5.33 domain-id (OSPFv3) ... 3500
9.5.34 filter export (OSPFv3) ... 3501
9.5.35 filter import (OSPFv3) ... 3503
9.5.36 filter-policy export (OSPFv3) ... 3504
9.5.37 filter-policy import (OSPFv3) ... 3506
9.5.38 graceful-restart (OSPFv3) ... 3507
9.5.39 helper-role (OSPFv3) ... 3508
9.5.40 import-route (OSPFv3) ... 3510
9.5.41 ipsec sa (OSPFv3) ... 3513
9.5.42 lsa-arrival-interval (OSPFv3) ... 3514
9.5.43 lsa-forwarding-address(OSPFv3) ... 3515
9.5.44 lsa-originate-interval (OSPFv3) ... 3516
9.5.45 maximum load-balancing (OSPFv3) ... 3517
9.5.46 maxage-lsa route-calculate-delay (OSPFv3) ... 3519
9.5.47 nexthop (OSPFv3) ... 3520
9.5.48 nssa (OSPFv3 Area) ... 3521
9.5.49 ospfv3 ... 3523
9.5.50 ospfv3 area ... 3524
9.5.51 ospfv3 authentication-mode ... 3525
9.5.52 ospfv3 bfd ... 3528
9.5.53 ospfv3 bfd block ... 3531
9.5.54 ospfv3 cost ... 3532

9.5.55 ospfv3 dr-priority....3533
9.5.56 ospfv3 ipsec sa....3534
9.5.57 ospfv3 mib-binding....3535
9.5.58 ospfv3 mtu-ignore....3536
9.5.59 ospfv3 network-type....3537
9.5.60 ospfv3 peer router-id....3538
9.5.61 ospfv3 router-id auto-recover disable....3540
9.5.62 ospfv3 suppress-flapping peer....3541
9.5.63 ospfv3 suppress-flapping peer disable....3543
9.5.64 ospfv3 suppress-flapping peer hold-down....3544
9.5.65 ospfv3 suppress-flapping peer hold-max-cost disable....3545
9.5.66 ospfv3 timer dead....3547
9.5.67 ospfv3 timer hello....3548
9.5.68 ospfv3 timer poll....3549
9.5.69 ospfv3 timer retransmit....3550
9.5.70 ospfv3 trans-delay....3551
9.5.71 ospfv3 valid-ttl-hops....3552
9.5.72 preference (OSPFv3)....3554
9.5.73 reset ospfv3....3555
9.5.74 router-id (OSPFv3)....3557
9.5.75 reset ospfv3 suppress-flapping peer....3558
9.5.76 sham-hello enable (OSPFv3)....3559
9.5.77 silent-interface (OSPFv3)....3560
9.5.78 snmp-agent trap enable feature-name ospfv3....3561
9.5.79 spf timers....3563
9.5.80 spf-schedule-interval (OSPFv3)....3564
9.5.81 stub (OSPFv3 Area)....3566
9.5.82 stub-router (OSPFv3)....3567
9.5.83 reset ospfv3 statistics maxage-lsa....3568
9.5.84 suppress-flapping peer disable (OSPFv3)....3569
9.5.85 vlink-peer (OSPFv3)....3570
9.6 IPv4 IS-IS Configuration Commands....3574
9.6.1 adjacency-strict-check enable....3574
9.6.2 area-authentication-mode....3575
9.6.3 attached-bit advertise....3579
9.6.4 attached-bit avoid-learning....3581
9.6.5 auto-cost enable....3582
9.6.6 bandwidth-reference (IS-IS)....3584
9.6.7 bfd all-interfaces (IS-IS)....3586
9.6.8 bfd all-interfaces enable....3588
9.6.9 circuit-cost....3589
9.6.10 circuit default-tag....3591

9.6.11 cost-style 3593
9.6.12 default-route-advertise (IS-IS) 3595
9.6.13 description (IS-IS) 3598
9.6.14 display default-parameter isis 3599
9.6.15 display isis cost interface 3603
9.6.16 display isis bfd interface 3605
9.6.17 display isis bfd session 3606
9.6.18 display isis brief 3608
9.6.19 display isis debug-switches 3612
9.6.20 display isis error 3613
9.6.21 display isis graceful-restart status 3617
9.6.22 display isis interface 3618
9.6.23 display isis last-peer-change 3623
9.6.24 display isis lsdb 3626
9.6.25 display isis migp-routing 3630
9.6.26 display isis mesh-group 3633
9.6.27 display isis name-table 3634
9.6.28 display isis peer 3636
9.6.29 display isis purge packet 3639
9.6.30 display isis route 3641
9.6.31 display isis spf-log 3647
9.6.32 display isis spf-tree 3652
9.6.33 display isis statistics 3658
9.6.34 display isis statistics purge-lsp 3663
9.6.35 display isis traffic-eng advertisements 3664
9.6.36 display isis traffic-eng link 3668
9.6.37 display isis traffic-eng network 3671
9.6.38 display isis traffic-eng statistics 3672
9.6.39 display isis traffic-eng sub-tlvs 3674
9.6.40 display snmp-agent trap feature-name isis all 3675
9.6.41 display snmp-agent trap feature-name isis-std all 3678
9.6.42 domain-authentication-mode 3681
9.6.43 filter-policy export (IS-IS) 3684
9.6.44 filter-policy import (IS-IS) 3686
9.6.45 flash-flood 3688
9.6.46 frr (IS-IS) 3689
9.6.47 frr-policy route 3690
9.6.48 graceful-restart (IS-IS) 3692
9.6.49 graceful-restart no-impact-holdtime 3693
9.6.50 graceful-restart interval 3694
9.6.51 graceful-restart suppress-sa 3696
9.6.52 graceful-restart t2-interval 3697

 Copyright © Huawei Technologies Co., Ltd.

9.6.53 import-route (IS-IS) 3698
9.6.54 import-route isis level-1 into level-2 3702
9.6.55 import-route isis level-2 into level-1 3704
9.6.56 isis 3707
9.6.57 isis authentication-mode 3708
9.6.58 isis bfd 3712
9.6.59 isis bfd block 3714
9.6.60 isis bfd enable 3715
9.6.61 isis bfd static 3716
9.6.62 isis circuit-level 3717
9.6.63 isis circuit-type 3719
9.6.64 isis cost 3720
9.6.65 isis delay-peer 3722
9.6.66 isis dis-name 3724
9.6.67 isis dis-priority 3725
9.6.68 isis enable 3727
9.6.69 isis lfa-backup 3728
9.6.70 isis lsp seq-overflow auto-recover disable 3729
9.6.71 isis mesh-group 3730
9.6.72 isis padding-hello 3732
9.6.73 isis peer-ip-ignore 3733
9.6.74 isis ppp-negotiation 3734
9.6.75 isis ppp-osicp-check 3735
9.6.76 isis purge-lsp auto-protect disable 3736
9.6.77 isis silent 3737
9.6.78 isis small-hello 3739
9.6.79 isis suppress-flapping peer 3740
9.6.80 isis suppress-flapping peer disable 3742
9.6.81 isis suppress-flapping peer hold-down 3743
9.6.82 isis suppress-flapping peer hold-max-cost disable 3745
9.6.83 isis suppress-reachability 3746
9.6.84 isis system-id auto-recover disable 3747
9.6.85 isis tag-value 3748
9.6.86 isis timer csnp 3750
9.6.87 isis timer hello 3752
9.6.88 isis timer holding-multiplier 3753
9.6.89 isis timer lsp-retransmit 3755
9.6.90 isis timer lsp-throttle 3757
9.6.91 is-level 3758
9.6.92 is-name 3760
9.6.93 is-name map 3761
9.6.94 log-peer-change 3762

9.6.95 local-mt enable (IS-IS) 3763
9.6.96 local-mt filter-policy (IS-IS) 3764
9.6.97 loop-free-alternate 3766
9.6.98 lsp-fragments-extend 3767
9.6.99 lsp-length 3768
9.6.100 maximum load-balancing (IS-IS) 3769
9.6.101 network-entity 3771
9.6.102 nexthop (IS-IS) 3772
9.6.103 optional-checksum enable 3773
9.6.104 preference (IS-IS) 3775
9.6.105 purge-originator-identification enable 3776
9.6.106 prefix-priority (IS-IS) 3778
9.6.107 reset isis all 3780
9.6.108 reset isis peer 3781
9.6.109 reset isis statistics packet 3782
9.6.110 reset isis statistics purge-lsp 3783
9.6.111 reset isis suppress-flapping peer 3784
9.6.112 set isis bfd delete delay-time 3785
9.6.113 set-overload 3786
9.6.114 snmp-agent trap enable feature-name isis 3789
9.6.115 snmp-agent trap enable feature-name isis-std 3792
9.6.116 spf-priority 3794
9.6.117 spf-slice-size 3795
9.6.118 summary (IS-IS) 3796
9.6.119 suppress-flapping lsp-flood 3798
9.6.120 suppress-flapping lsp-generation 3799
9.6.121 suppress-flapping peer disable (IS-IS) 3801
9.6.122 suppress-flapping route-calculate 3802
9.6.123 timer lsp-generation 3803
9.6.124 timer lsp-max-age 3805
9.6.125 timer lsp-refresh 3806
9.6.126 timer purge-zero-lsp route-calculate-delay 3808
9.6.127 timer spf 3809
9.6.128 virtual-system 3810
9.7 IPv6 IS-IS Configuration Commands 3811
9.7.1 ipv6 auto-cost enable 3811
9.7.2 ipv6 bandwidth-reference 3813
9.7.3 ipv6 circuit-cost 3815
9.7.4 ipv6 circuit default-tag 3816
9.7.5 ipv6 default-route-advertise 3818
9.7.6 ipv6 enable(IS-IS) 3820
9.7.7 ipv6 filter-policy export 3822

 Copyright © Huawei Technologies Co., Ltd.

9.7.8 ipv6 filter-policy import 3824
9.7.9 ipv6 import-route 3825
9.7.10 ipv6 import-route isis level-1 into level-2 3829
9.7.11 ipv6 import-route isis level-2 into level-1 3831
9.7.12 ipv6 maximum load-balancing 3834
9.7.13 ipv6 preference 3835
9.7.14 ipv6 prefix-priority (IS-IS) 3837
9.7.15 ipv6 spf-priority 3839
9.7.16 ipv6 summary 3840
9.7.17 isis ipv6 cost 3841
9.7.18 isis ipv6 enable 3844
9.7.19 isis ipv6 suppress-reachability 3845
9.7.20 isis ipv6 tag-value 3846
9.8 BGP Configuration Commands 3848
9.8.1 active-route-advertise 3848
9.8.2 aggregate (BGP) 3849
9.8.3 apply-label explicit-null 3852
9.8.4 as-notation plain 3853
9.8.5 as-path-limit 3855
9.8.6 bestroute as-path-ignore 3856
9.8.7 bestroute igp-metric-ignore 3857
9.8.8 bestroute med-confederation (BGP) 3858
9.8.9 bestroute med-none-as-maximum 3859
9.8.10 bestroute nexthop-resolved 3860
9.8.11 bestroute routerid-prior-clusterlist 3862
9.8.12 bgp 3863
9.8.13 bgp dynamic-session-limit 3864
9.8.14 check-first-as 3865
9.8.15 compare-different-as-med 3866
9.8.16 confederation id 3867
9.8.17 confederation nonstandard 3869
9.8.18 confederation peer-as 3870
9.8.19 confederation route unicast-to-label disable 3871
9.8.20 dampening 3872
9.8.21 default ipv4-unicast 3875
9.8.22 default local-preference 3876
9.8.23 default med 3877
9.8.24 default-route imported 3878
9.8.25 deterministic-med (BGP) 3879
9.8.26 display bgp bfd session 3881
9.8.27 display bgp error 3884
9.8.28 display bgp error discard 3886

9.8.29 display bgp group 3888
9.8.30 display bgp ipv6 bfd session 3895
9.8.31 display bgp ipv6 routing-table 3898
9.8.32 display bgp ipv6 routing-table statistics 3904
9.8.33 display bgp mdt routing-table 3907
9.8.34 display bgp mdt brief 3916
9.8.35 display bgp mdt routing-table statistics 3917
9.8.36 display bgp multicast group 3920
9.8.37 display bgp multicast network 3922
9.8.38 display bgp multicast paths 3924
9.8.39 display bgp multicast peer 3925
9.8.40 display bgp multicast routing-table 3926
9.8.41 display bgp multicast routing-table as-path-filter 3930
9.8.42 display bgp multicast routing-table cidr 3931
9.8.43 display bgp multicast routing-table community 3933
9.8.44 display bgp multicast routing-table community-filter 3935
9.8.45 display bgp multicast routing-table dampened 3936
9.8.46 display bgp multicast routing-table dampening parameter 3937
9.8.47 display bgp multicast routing-table different-origin-as 3938
9.8.48 display bgp multicast routing-table flap-info 3939
9.8.49 display bgp multicast routing-table peer 3941
9.8.50 display bgp multicast routing-table regular-expression 3943
9.8.51 display bgp multicast routing-table statistics 3944
9.8.52 display bgp multicast update-peer-group 3946
9.8.53 display bgp network 3947
9.8.54 display bgp paths 3950
9.8.55 display bgp peer 3953
9.8.56 display bgp peer orf ip-prefix 3971
9.8.57 display bgp resource 3972
9.8.58 display bgp routing-table 3973
9.8.59 display bgp routing-table dampened 3981
9.8.60 display bgp routing-table dampening parameter 3984
9.8.61 display bgp routing-table flap-info 3986
9.8.62 display bgp routing-table label 3989
9.8.63 display bgp routing-table peer no-advertise 3992
9.8.64 display bgp routing-table peer statistics 3997
9.8.65 display bgp routing-table statistics 3998
9.8.66 display bgp update-peer-group 4001
9.8.67 display bgp vpnv4 brief 4005
9.8.68 display bgp vpnv4 routing-table 4006
9.8.69 display bgp vpnv4 routing-table statistics 4019
9.8.70 display bgp vpnv6 brief 4024

9.8.71 display bgp vpnv6 routing-table 4026
9.8.72 display bgp vpnv6 routing-table statistics 4038
9.8.73 display default-parameter bgp 4044
9.8.74 display mbgp routing-table 4046
9.8.75 display mbgp routing-table statistics 4049
9.8.76 display snmp-agent trap feature-name bgp all 4050
9.8.77 ebgp-interface-sensitive 4053
9.8.78 ext-community-change enable 4054
9.8.79 filter-policy export (BGP) 4055
9.8.80 filter-policy import (BGP) 4058
9.8.81 graceful-restart (BGP) 4060
9.8.82 graceful-restart peer-reset 4061
9.8.83 graceful-restart timer restart 4062
9.8.84 graceful-restart timer wait-for-rib 4063
9.8.85 group 4064
9.8.86 import-route (BGP) 4066
9.8.87 ipv4-family 4067
9.8.88 ipv6-family 4069
9.8.89 keep-all-routes 4070
9.8.90 load-balancing as-path-ignore 4071
9.8.91 maximum load-balancing (BGP) 4073
9.8.92 maximum load-balancing eibgp 4075
9.8.93 network (BGP) 4077
9.8.94 nexthop recursive-lookup (BGP) 4079
9.8.95 nexthop recursive-lookup delay 4081
9.8.96 nexthop recursive-lookup non-critical-event delay 4082
9.8.97 out-delay 4084
9.8.98 peer advertise-community 4086
9.8.99 peer advertise-ext-community 4087
9.8.100 peer allow-as-loop 4089
9.8.101 peer as-number 4091
9.8.102 peer as-path-filter 4093
9.8.103 peer bfd 4095
9.8.104 peer bfd block 4097
9.8.105 peer bfd enable 4099
9.8.106 peer capability-advertise 4101
9.8.107 peer capability-advertise orf 4102
9.8.108 peer connect-interface 4104
9.8.109 peer connected-check-ignore 4107
9.8.110 peer default-route-advertise 4108
9.8.111 peer description (BGP) 4111
9.8.112 peer discard-ext-community (BGP) 4113

9.8.113 peer ebgp-max-hop 4114
9.8.114 peer enable (BGP) 4116
9.8.115 peer fake-as 4117
9.8.116 peer filter-policy 4119
9.8.117 peer group 4122
9.8.118 peer ignore 4124
9.8.119 peer ip-prefix 4125
9.8.120 peer keychain (BGP) 4128
9.8.121 peer keep-all-routes 4129
9.8.122 peer label-route-capability (BGP) 4131
9.8.123 peer listen-net 4133
9.8.124 peer listen-only 4134
9.8.125 peer log-change 4136
9.8.126 peer next-hop-invariable 4137
9.8.127 peer next-hop-local 4139
9.8.128 peer out-delay 4141
9.8.129 peer password 4143
9.8.130 peer path-mtu auto-discovery 4145
9.8.131 peer preferred-value 4146
9.8.132 peer public-as-only 4148
9.8.133 peer reflect-client 4150
9.8.134 peer route-limit 4152
9.8.135 peer route-policy 4155
9.8.136 peer route-update-interval 4157
9.8.137 peer timer 4159
9.8.138 peer timer connect-retry 4162
9.8.139 peer tracking 4164
9.8.140 peer tnl-policy 4166
9.8.141 peer valid-ttl-hops 4167
9.8.142 preference (BGP) 4169
9.8.143 qos-local-id behavior 4171
9.8.144 qppb local-policy 4173
9.8.145 qppb-policy enable 4174
9.8.146 reflect between-clients 4175
9.8.147 reflect change-path-attribute 4176
9.8.148 reflector cluster-id 4178
9.8.149 refresh bgp 4180
9.8.150 refresh bgp mdt 4182
9.8.151 refresh bgp multicast 4183
9.8.152 refresh bgp multicast external 4184
9.8.153 refresh bgp multicast internal 4185
9.8.154 reset bgp 4186

9.8.155 reset bgp dampening 4189
9.8.156 reset bgp flap-info 4191
9.8.157 reset bgp flapping-count 4194
9.8.158 reset bgp mdt 4195
9.8.159 reset bgp multicast 4197
9.8.160 reset bgp multicast dampening 4199
9.8.161 reset bgp multicast external 4199
9.8.162 reset bgp multicast flap-info 4200
9.8.163 reset bgp multicast internal 4201
9.8.164 router-id (BGP) 4202
9.8.165 router-id (BGP-VPN Instance IPv4 Address Family View) 4203
9.8.166 route-select delay 4205
9.8.167 routing-table limit threshold-alarm 4206
9.8.168 routing-table rib-only 4207
9.8.169 shutdown (BGP) 4209
9.8.170 slow-peer detection disable 4210
9.8.171 slow-peer detection threshold 4211
9.8.172 snmp-agent trap enable feature-name bgp 4212
9.8.173 summary automatic 4214
9.8.174 supernet unicast advertise 4215
9.8.175 timer (BGP) 4217
9.8.176 timer connect-retry 4219
9.8.177 undo synchronization (BGP) 4220
9.9 Routing Policy Configuration Commands 4221
9.9.1 apply as-path 4221
9.9.2 apply backup-interface 4223
9.9.3 apply backup-nexthop 4225
9.9.4 apply behavior 4227
9.9.5 apply comm-filter delete 4228
9.9.6 apply community 4230
9.9.7 apply cost 4233
9.9.8 apply cost-type 4234
9.9.9 apply dampening 4236
9.9.10 apply extcommunity 4237
9.9.11 apply ip-address next-hop (Route-Policy view) 4239
9.9.12 apply ipv6 next-hop 4241
9.9.13 apply ip-precedence 4242
9.9.14 apply isis 4244
9.9.15 apply local-preference 4245
9.9.16 apply mpls-label 4246
9.9.17 apply origin 4247
9.9.18 apply ospf 4249

9.9.19 apply preference....4250
9.9.20 apply preferred-value....4251
9.9.21 apply qos-local-id....4252
9.9.22 apply tag....4253
9.9.23 description (Route-Policy view)....4254
9.9.24 display ip as-path-filter....4255
9.9.25 display ip community-filter....4257
9.9.26 display ip extcommunity-filter....4259
9.9.27 display ip ip-prefix....4260
9.9.28 display ip ipv6-prefix....4262
9.9.29 display ip rd-filter....4264
9.9.30 display route-policy....4265
9.9.31 if-match acl (Route-Policy view)....4267
9.9.32 if-match as-path-filter....4268
9.9.33 if-match community-filter....4270
9.9.34 if-match cost....4272
9.9.35 if-match extcommunity-filter....4273
9.9.36 if-match interface....4275
9.9.37 if-match ip....4277
9.9.38 if-match ip-prefix....4279
9.9.39 if-match ipv6....4280
9.9.40 if-match mpls-label....4282
9.9.41 if-match rd-filter....4283
9.9.42 if-match route-type....4284
9.9.43 if-match tag....4286
9.9.44 ip as-path-filter....4287
9.9.45 ip community-filter....4289
9.9.46 ip extcommunity-filter....4294
9.9.47 ip ip-prefix....4297
9.9.48 ip ipv6-prefix....4302
9.9.49 ip rd-filter....4305
9.9.50 reset ip ip-prefix....4308
9.9.51 reset ip ipv6-prefix....4309
9.9.52 reset route-policy counters....4310
9.9.53 route-policy....4311
9.9.54 route-policy-change notify-delay....4314
9.10 IP Routing Basic Configuration Commands....4315
9.10.1 display fib....4315
9.10.2 display fib acl....4321
9.10.3 display fib interface....4323
9.10.4 display fib ip-prefix....4325
9.10.5 display fib longer....4326

 Copyright © Huawei Technologies Co., Ltd.

9.10.6 display fib next-hop....4329
9.10.7 display fib statistics....4331
9.10.8 display ip routing-table....4332
9.10.9 display ip routing-table limit....4340
9.10.10 display ip routing-table protocol....4342
9.10.11 display ip routing-table statistics....4347
9.10.12 display ip routing-table time-range....4349
9.10.13 display ipv6 fib....4354
9.10.14 display ipv6 fib statistics....4358
9.10.15 display ipv6 routing-table....4359
9.10.16 display ipv6 routing-table limit....4364
9.10.17 display ipv6 routing-table protocol....4366
9.10.18 display ipv6 routing-table statistics....4369
9.10.19 display ipv6 routing-table time-range....4371
9.10.20 display rm bfd-session....4377
9.10.21 display rm interface....4381
9.10.22 display rm ipv6 interface....4384
9.10.23 display rm ipv6 bfd-session....4387
9.10.24 display router id....4389
9.10.25 display route resource....4390
9.10.26 fib download all....4391
9.10.27 fib regularly-refresh....4392
9.10.28 fib regularly-refresh disable....4393
9.10.29 fib regularly-refresh start-time....4394
9.10.30 ip frr (system view)....4395
9.10.31 ip load-balance hash....4397
9.10.32 ip load-balance packet....4399
9.10.33 ip prefix-limit....4400
9.10.34 ip prefix-limit log-interval....4402
9.10.35 ip route prefix-priority-scheduler....4403
9.10.36 ip route recursive-lookup default-route....4405
9.10.37 ipv6 fib-loadbalance-type hash-based....4406
9.10.38 ipv6 fib regularly-refresh entry-number....4406
9.10.39 ipv6 fib regularly-refresh disable....4408
9.10.40 ipv6 fib regularly-refresh interval....4409
9.10.41 ipv6 fib regularly-refresh start-time....4410
9.10.42 ipv6 prefix-limit....4412
9.10.43 ipv6 prefix-limit log-interval....4414
9.10.44 ipv6 route prefix-priority-scheduler....4415
9.10.45 refresh fib....4417
9.10.46 refresh ipv6 fib....4418
9.10.47 reset ip routing-table statistics protocol....4418

9.10.48 reset ipv6 routing-table statistics protocol.... 4420
9.10.49 router id.... 4421
9.11 PBR Configuration Commands.... 4423
9.11.1 apply access-vpn.... 4423
9.11.2 apply default output-interface.... 4424
9.11.3 apply ip-address backup-nexthop.... 4425
9.11.4 apply ip-address default next-hop.... 4426
9.11.5 apply ip-address next-hop (policy-based route view).... 4427
9.11.6 apply ip-address next-hop track ip-route.... 4429
9.11.7 apply ip-precedence (policy-based route view).... 4430
9.11.8 apply output-interface.... 4432
9.11.9 backup-interface.... 4434
9.11.10 backup-ipv6-interface.... 4436
9.11.11 cmi-method.... 4438
9.11.12 description (service profile view).... 4440
9.11.13 display ip policy-based-route.... 4441
9.11.14 display ip policy-based-route setup.... 4442
9.11.15 display ip policy-based-route statistics local.... 4444
9.11.16 display ip policy-based-route statistics.... 4445
9.11.17 display policy-based-route.... 4447
9.11.18 display smart-policy-route.... 4449
9.11.19 display smart-policy-route link-state.... 4452
9.11.20 display smart-policy-route nqa-server link-state.... 4454
9.11.21 display smart-policy-route service-map.... 4455
9.11.22 display smart-policy-route redirect-link link-state.... 4458
9.11.23 if-match acl (policy-based route view).... 4459
9.11.24 if-match packet-length.... 4460
9.11.25 ip policy-based-route.... 4462
9.11.26 ip policy-based-route refresh-time.... 4462
9.11.27 ip local policy-based-route.... 4463
9.11.28 ip local route-based-source enable.... 4464
9.11.29 ip route re-search acl.... 4465
9.11.30 ipv6 route re-search acl.... 4467
9.11.31 link-group.... 4468
9.11.32 link-member.... 4469
9.11.33 link-path.... 4471
9.11.34 match.... 4472
9.11.35 match acl.... 4474
9.11.36 match acl ipv6.... 4476
9.11.37 nqa-client.... 4477
9.11.38 nqa-relay.... 4479
9.11.39 nqa-relay-group.... 4480

 Copyright © Huawei Technologies Co., Ltd.

9.11.40 nqa-relay-member....4481
9.11.41 nqa-server....4483
9.11.42 nqa-server port....4484
9.11.43 period....4485
9.11.44 policy-based-route....4486
9.11.45 prober....4487
9.11.46 redirect backup-nexthop....4489
9.11.47 redirect backup-interface....4491
9.11.48 redirect enhance enable....4492
9.11.49 redirect interface....4493
9.11.50 redirect ip-nexthop....4496
9.11.51 redirect ipv6-nexthop....4500
9.11.52 redirect-link....4502
9.11.53 redirect vpn-instance....4504
9.11.54 route flapping suppression....4506
9.11.55 route-policy nonexistent-config-check....4507
9.11.56 service-map....4508
9.11.57 service-map default-policy....4509
9.11.58 set cmi threshold....4510
9.11.59 set delay threshold....4512
9.11.60 set jitter threshold....4513
9.11.61 set link-group....4514
9.11.62 set loss threshold....4516
9.11.63 smart-policy-route....4517
9.11.64 standby-interface (smart-policy-route view)....4518
9.11.65 standby-limit-time (smart-policy-route view)....4521
9.11.66 wtr period....4523
9.12 Route Monitoring Group Configuration Commands....4524
9.12.1 ip route-monitor-group....4524
9.12.2 monitor enable (route monitoring group view)....4525
9.12.3 operator and....4526
9.12.4 track ip route....4527
9.12.5 trigger-down-delay (route monitoring group view)....4529
9.12.6 trigger-up-delay (route monitoring group view)....4530
9.12.7 display ip route-monitor-group....4532
9.12.8 display ip route-monitor-group track-route....4534

10 IP Multicast Commands....4536

10.1 IGMP Configuration Commands....4536
10.1.1 display default-parameter igmp....4536
10.1.2 display igmp control-message counters....4540
10.1.3 display igmp explicit-tracking....4543
10.1.4 display igmp group....4546

10.1.5 display igmp group ssm-mapping....4550
10.1.6 display igmp group static....4554
10.1.7 display igmp interface....4558
10.1.8 display igmp invalid-packet....4563
10.1.9 display igmp proxy group....4567
10.1.10 display igmp proxy interface....4570
10.1.11 display igmp proxy routing-table....4572
10.1.12 display igmp routing-table....4576
10.1.13 display igmp ssm-mapping....4579
10.1.14 igmp....4581
10.1.15 igmp enable....4582
10.1.16 igmp global limit....4583
10.1.17 igmp group-policy....4585
10.1.18 igmp ip-source-policy....4587
10.1.19 igmp lastmember-queryinterval....4589
10.1.20 igmp limit....4591
10.1.21 igmp max-response-time....4594
10.1.22 igmp on-demand....4595
10.1.23 igmp prompt-leave....4597
10.1.24 igmp proxy....4600
10.1.25 igmp proxy backup....4602
10.1.26 igmp proxy interface reroute....4603
10.1.27 igmp query ip-source-policy....4604
10.1.28 igmp require-router-alert....4606
10.1.29 igmp robust-count....4607
10.1.30 igmp send-router-alert....4609
10.1.31 igmp ssm-mapping enable....4610
10.1.32 igmp static-group....4611
10.1.33 igmp timer other-querier-present....4615
10.1.34 igmp timer query....4617
10.1.35 igmp ttl-check....4618
10.1.36 igmp version....4619
10.1.37 lastmember-queryinterval (IGMP)....4620
10.1.38 limit (IGMP)....4622
10.1.39 max-response-time (IGMP)....4625
10.1.40 proxy source-lifetime....4626
10.1.41 proxy source-policy....4627
10.1.42 proxy ssm-policy....4629
10.1.43 require-router-alert (IGMP)....4631
10.1.44 reset igmp control-message counters....4633
10.1.45 reset igmp explicit-tracking....4634
10.1.46 reset igmp group....4635

10.1.47 reset igmp group ssm-mapping....4637
10.1.48 robust-count (IGMP)....4639
10.1.49 send-router-alert (IGMP)....4641
10.1.50 ssm-mapping (IGMP)....4642
10.1.51 timer other-querier-present (IGMP)....4644
10.1.52 timer query (IGMP)....4646
10.1.53 ttl-check (IPv4)....4648
10.2 MLD Configuration Commands....4648
10.2.1 display default-parameter mld....4649
10.2.2 display mld control-message counters....4652
10.2.3 display mld explicit-tracking....4654
10.2.4 display mld group....4657
10.2.5 display mld group ssm-mapping....4660
10.2.6 display mld group static....4663
10.2.7 display mld interface....4667
10.2.8 display mld invalid-packet....4672
10.2.9 display mld routing-table....4676
10.2.10 display mld ssm-mapping....4678
10.2.11 display mld ssm-mapping interface....4680
10.2.12 lastlistener-queryinterval (MLD view)....4682
10.2.13 limit (MLD view)....4683
10.2.14 max-response-time (MLD view)....4685
10.2.15 mld....4687
10.2.16 mld enable....4688
10.2.17 mld global limit....4689
10.2.18 mld group-policy....4691
10.2.19 mld ip-source-policy....4693
10.2.20 mld lastlistener-queryinterval....4694
10.2.21 mld limit....4696
10.2.22 mld max-response-time....4699
10.2.23 mld on-demand....4701
10.2.24 mld prompt-leave....4702
10.2.25 mld query ip-source-policy....4705
10.2.26 mld require-router-alert....4706
10.2.27 mld robust-count....4708
10.2.28 mld send-router-alert....4710
10.2.29 mld ssm-mapping enable....4711
10.2.30 mld static-group....4712
10.2.31 mld timer other-querier-present....4715
10.2.32 mld timer query....4716
10.2.33 mld ttl-check....4718
10.2.34 mld version....4719

10.2.35 require-router-alert (MLD view) 4720
10.2.36 reset mld control-message counters 4721
10.2.37 reset mld explicit-tracking 4722
10.2.38 reset mld group 4724
10.2.39 reset mld group ssm-mapping 4726
10.2.40 robust-count (MLD view) 4727
10.2.41 send-router-alert (MLD view) 4729
10.2.42 ssm-mapping (MLD view) 4730
10.2.43 timer other-querier-present (MLD view) 4732
10.2.44 timer query (MLD view) 4733
10.2.45 ttl-check (IPv6) 4735
10.3 PIM (IPv4) Configuration Commands 4736
10.3.1 anycast-rp (IPv4) 4736
10.3.2 auto-rp listening enable 4738
10.3.3 bsm semantic fragmentation (IPv4) 4739
10.3.4 bsr-policy (IPv4) 4740
10.3.5 c-bsr (IPv4) 4742
10.3.6 c-bsr admin-scope 4744
10.3.7 c-bsr global 4745
10.3.8 c-bsr group 4747
10.3.9 c-bsr hash-length (IPv4) 4749
10.3.10 c-bsr holdtime (IPv4) 4750
10.3.11 c-bsr interval (IPv4) 4752
10.3.12 c-bsr priority (IPv4) 4753
10.3.13 c-rp (IPv4) 4755
10.3.14 c-rp advertisement-interval (IPv4) 4758
10.3.15 c-rp holdtime (IPv4) 4759
10.3.16 c-rp priority (IPv4) 4760
10.3.17 crp-policy (IPv4) 4761
10.3.18 display default-parameter pim-dm 4763
10.3.19 display default-parameter pim-sm 4768
10.3.20 display default-parameter pim-ssm 4774
10.3.21 display pim bfd session 4778
10.3.22 display pim bsr-info 4780
10.3.23 display pim claimed-route 4783
10.3.24 display pim control-message counters 4785
10.3.25 display pim grafts 4789
10.3.26 display pim interface 4790
10.3.27 display pim invalid-packet 4794
10.3.28 display pim neighbor 4800
10.3.29 display pim routing-table 4803
10.3.30 display pim rp-info 4810

10.3.31 graceful-restart (IPv4) 4812
10.3.32 graceful-restart period (IPv4) 4813
10.3.33 hello-option dr-priority (IPv4) 4814
10.3.34 hello-option holdtime (IPv4) 4816
10.3.35 hello-option lan-delay (IPv4) 4817
10.3.36 hello-option neighbor-tracking (IPv4) 4819
10.3.37 hello-option override-interval (IPv4) 4820
10.3.38 holdtime assert (IPv4) 4822
10.3.39 holdtime join-prune (IPv4) 4823
10.3.40 join-prune max-packet-length (IPv4) 4824
10.3.41 join-prune periodic-messages queue-size (IPv4) 4826
10.3.42 join-prune triggered-message-cache disable (IPv4) 4827
10.3.43 local-address (IPv4) 4828
10.3.44 neighbor-check (IPv4) 4829
10.3.45 peer (IPv4) 4830
10.3.46 pim 4832
10.3.47 pim bfd 4834
10.3.48 pim bfd enable 4835
10.3.49 pim bsr-boundary 4836
10.3.50 pim dm 4838
10.3.51 pim hello-option dr-priority 4839
10.3.52 pim hello-option holdtime 4840
10.3.53 pim hello-option lan-delay 4841
10.3.54 pim hello-option neighbor-tracking 4843
10.3.55 pim hello-option override-interval 4844
10.3.56 pim holdtime assert 4846
10.3.57 pim holdtime join-prune 4847
10.3.58 pim join-policy 4849
10.3.59 pim neighbor-policy 4850
10.3.60 pim require-genid 4852
10.3.61 pim silent 4853
10.3.62 pim sm 4854
10.3.63 pim state-refresh-capable 4855
10.3.64 pim timer dr-switch-delay 4856
10.3.65 pim timer graft-retry 4857
10.3.66 pim timer hello 4859
10.3.67 pim timer join-prune 4860
10.3.68 pim triggered-hello-delay 4861
10.3.69 probe-interval (IPv4) 4862
10.3.70 register-header-checksum 4863
10.3.71 register-policy (IPv4) 4865
10.3.72 register-source 4866

10.3.73 register-suppression-timeout (IPv4) 4867
10.3.74 reset pim control-message counters 4869
10.3.75 reset pim routing-table 4870
10.3.76 source-lifetime (IPv4) 4872
10.3.77 source-policy (IPv4) 4873
10.3.78 spt-switch-threshold (IPv4) 4874
10.3.79 ssm-policy (IPv4) 4877
10.3.80 state-refresh-interval (IPv4) 4878
10.3.81 state-refresh-rate-limit (IPv4) 4880
10.3.82 state-refresh-ttl (IPv4) 4881
10.3.83 static-rp (IPv4) 4882
10.3.84 timer hello (IPv4) 4885
10.3.85 timer join-prune (IPv4) 4886
10.3.86 timer spt-switch (IPv4) 4887
10.4 PIM (IPv6) Configuration Commands 4889
10.4.1 anycast-rp (IPv6) 4889
10.4.2 bsm semantic fragmentation (IPv6) 4890
10.4.3 bsr-policy (IPv6) 4892
10.4.4 c-bsr (IPv6) 4894
10.4.5 c-bsr admin-scope (IPv6) 4896
10.4.6 c-bsr global (IPv6) 4897
10.4.7 c-bsr hash-length (IPv6) 4898
10.4.8 c-bsr holdtime (IPv6) 4900
10.4.9 c-bsr interval (IPv6) 4901
10.4.10 c-bsr priority (IPv6) 4903
10.4.11 c-bsr scope 4904
10.4.12 c-rp (IPv6) 4905
10.4.13 c-rp advertisement-interval (IPv6) 4908
10.4.14 c-rp holdtime (IPv6) 4909
10.4.15 c-rp priority (IPv6) 4910
10.4.16 crp-policy (IPv6) 4912
10.4.17 display default-parameter pim-dm6 4914
10.4.18 display default-parameter pim-sm6 4918
10.4.19 display default-parameter pim-ssm6 4923
10.4.20 display pim ipv6 bsr-info 4927
10.4.21 display pim ipv6 claimed-route 4930
10.4.22 display pim ipv6 control-message counters 4931
10.4.23 display pim ipv6 grafts 4934
10.4.24 display pim ipv6 interface 4935
10.4.25 display pim ipv6 invalid-packet 4938
10.4.26 display pim ipv6 neighbor 4944
10.4.27 display pim ipv6 routing-table 4946

10.4.28 display pim ipv6 rp-info....4951
10.4.29 embedded-rp....4952
10.4.30 graceful-restart (IPv6)....4954
10.4.31 graceful-restart period (IPv6)....4955
10.4.32 hello-option dr-priority (IPv6)....4957
10.4.33 hello-option holdtime (IPv6)....4958
10.4.34 hello-option lan-delay (IPv6)....4959
10.4.35 hello-option neighbor-tracking (IPv6)....4961
10.4.36 hello-option override-interval (IPv6)....4962
10.4.37 holdtime assert (IPv6)....4964
10.4.38 holdtime join-prune (IPv6)....4965
10.4.39 join-prune max-packet-length (IPv6)....4966
10.4.40 join-prune periodic-messages queue-size (IPv6)....4968
10.4.41 join-prune triggered-message-cache disable (IPv6)....4969
10.4.42 local-address (IPv6)....4970
10.4.43 neighbor-check (IPv6)....4971
10.4.44 peer (IPv6)....4973
10.4.45 pim-ipv6....4974
10.4.46 pim ipv6 bsr-boundary....4975
10.4.47 pim ipv6 dm....4976
10.4.48 pim ipv6 hello-option dr-priority....4977
10.4.49 pim ipv6 hello-option holdtime....4979
10.4.50 pim ipv6 hello-option lan-delay....4980
10.4.51 pim ipv6 hello-option neighbor-tracking....4982
10.4.52 pim ipv6 hello-option override-interval....4983
10.4.53 pim ipv6 holdtime assert....4984
10.4.54 pim ipv6 holdtime join-prune....4986
10.4.55 pim ipv6 join-policy....4987
10.4.56 pim ipv6 neighbor-policy....4989
10.4.57 pim ipv6 require-genid....4990
10.4.58 pim ipv6 silent....4992
10.4.59 pim ipv6 sm....4993
10.4.60 pim ipv6 state-refresh-capable....4994
10.4.61 pim ipv6 timer dr-switch-delay....4995
10.4.62 pim ipv6 timer graft-retry....4996
10.4.63 pim ipv6 timer hello....4997
10.4.64 pim ipv6 timer join-prune....4999
10.4.65 pim ipv6 triggered-hello-delay....5000
10.4.66 probe-interval (IPv6)....5001
10.4.67 register-policy (IPv6)....5002
10.4.68 register-source (IPv6)....5004
10.4.69 register-suppression-timeout (IPv6)....5005

10.4.70 reset pim ipv6 control-message counters 5006
10.4.71 reset pim ipv6 routing-table 5007
10.4.72 source-lifetime (IPv6) 5009
10.4.73 source-policy (IPv6) 5010
10.4.74 spt-switch-threshold (IPv6) 5011
10.4.75 ssm-policy (IPv6) 5014
10.4.76 state-refresh-interval (IPv6) 5016
10.4.77 state-refresh-rate-limit (IPv6) 5017
10.4.78 state-refresh-ttl (IPv6) 5018
10.4.79 static-rp (IPv6) 5020
10.4.80 timer hello (IPv6) 5022
10.4.81 timer join-prune (IPv6) 5023
10.4.82 timer spt-switch (IPv6) 5024
10.5 MSDP Configuration Commands 5026
10.5.1 cache-sa-enable 5026
10.5.2 display default-parameter msdp 5027
10.5.3 display msdp brief 5030
10.5.4 display msdp control-message counters 5033
10.5.5 display msdp invalid-packet 5035
10.5.6 display msdp peer-status 5039
10.5.7 display msdp rpf-peer 5044
10.5.8 display msdp sa-cache 5047
10.5.9 display msdp sa-count 5049
10.5.10 encap-data-enable 5051
10.5.11 import-source 5053
10.5.12 msdp 5055
10.5.13 originating-rp 5056
10.5.14 peer connect-interface (MSDP) 5057
10.5.15 peer description (MSDP) 5059
10.5.16 peer keychain (MSDP) 5060
10.5.17 peer mesh-group 5062
10.5.18 peer minimum-ttl 5063
10.5.19 peer password (MSDP) 5065
10.5.20 peer request-sa-enable 5067
10.5.21 peer sa-cache-maximum 5068
10.5.22 peer sa-policy 5070
10.5.23 peer sa-request-policy 5072
10.5.24 reset msdp control-message counters 5074
10.5.25 reset msdp peer 5076
10.5.26 reset msdp sa-cache 5077
10.5.27 reset msdp statistics 5079
10.5.28 shutdown (MSDP) 5080

 Copyright © Huawei Technologies Co., Ltd.

10.5.29 static-rpf-peer 5081
10.5.30 timer retry 5083
10.6 Multicast VPN (IPv4) Configuration Commands in Rosen Mode 5084
10.6.1 auto-discovery 5084
10.6.2 display default-parameter mvpn 5087
10.6.3 display multicast-domain control-message counters 5089
10.6.4 display multicast-domain invalid-packet 5090
10.6.5 display multicast-domain vpn-instance share-group 5093
10.6.6 display multicast-domain vpn-instance switch-group receive 5095
10.6.7 display multicast-domain vpn-instance switch-group send 5098
10.6.8 mtu (MTI view) 5101
10.6.9 multicast extranet select-rpf 5102
10.6.10 multicast-domain holddown-time 5104
10.6.11 multicast-domain log switch-group-reuse 5105
10.6.12 multicast-domain share-group 5106
10.6.13 multicast-domain source-interface 5108
10.6.14 multicast-domain switch-delay 5109
10.6.15 multicast-domain switch-group-pool 5110
10.6.16 multicast-domain switch-without-register 5112
10.6.17 reset multicast-domain control-message counters 5114
10.6.18 multicast extranet traffic-forward type 5115
10.6.19 rpf-vector compatible standard 5116
10.6.20 rpf-vector 5117
10.7 Multicast Route Management (IPv4) Commands 5119
10.7.1 display default-parameter mrm 5119
10.7.2 display migp routing-table 5121
10.7.3 display migp routing-table statistics 5124
10.7.4 display mrt routing-table 5125
10.7.5 display mrt routing-table statistics 5128
10.7.6 display mrt routing-table vpn-instance 5130
10.7.7 display mtrace statistics 5131
10.7.8 display multicast boundary 5132
10.7.9 display multicast boundary policy 5134
10.7.10 display multicast forwarding-table 5137
10.7.11 display multicast routing-table 5142
10.7.12 display multicast routing-table static 5146
10.7.13 display multicast rpf-info 5148
10.7.14 ip rpf-route-static 5150
10.7.15 mtrace 5153
10.7.16 mtrace query-policy 5161
10.7.17 multicast boundary 5162
10.7.18 multicast boundary policy 5164

10.7.19 multicast boundary policy in 5165
10.7.20 multicast boundary policy out 5167
10.7.21 multicast forwarding-table downstream-limit 5169
10.7.22 multicast forwarding-table route-limit 5170
10.7.23 multicast invalid-packet 5173
10.7.24 multicast load-splitting 5174
10.7.25 multicast load-splitting weight 5176
10.7.26 multicast load-splitting-timer 5177
10.7.27 multicast longest-match 5178
10.7.28 multicast routing-enable 5179
10.7.29 ping multicast 5180
10.7.30 reset mtrace statistics 5185
10.7.31 reset multicast forwarding-table 5186
10.7.32 reset multicast routing-table 5188
10.8 Multicast Route Management (IPv6) Commands 5190
10.8.1 display multicast ipv6 boundary 5190
10.8.2 display multicast ipv6 boundary policy 5192
10.8.3 display multicast ipv6 forwarding-table 5194
10.8.4 display multicast ipv6 routing-table 5200
10.8.5 display multicast ipv6 rpf-info 5203
10.8.6 multicast ipv6 boundary 5204
10.8.7 multicast ipv6 boundary policy 5206
10.8.8 multicast ipv6 boundary policy in 5207
10.8.9 multicast ipv6 boundary policy out 5209
10.8.10 multicast ipv6 forwarding-table downstream-limit 5211
10.8.11 multicast ipv6 forwarding-table route-limit 5213
10.8.12 multicast ipv6 invalid-packet 5215
10.8.13 multicast ipv6 load-splitting 5216
10.8.14 multicast ipv6 load-splitting weight 5218
10.8.15 multicast ipv6 load-splitting-timer 5219
10.8.16 multicast ipv6 routing-enable 5221
10.8.17 reset multicast ipv6 forwarding-table 5222
10.8.18 reset multicast ipv6 routing-table 5223
10.9 IGMP Snooping Configuration Commands 5225
10.9.1 display igmp-snooping 5225
10.9.2 display igmp-snooping configuration 5229
10.9.3 display igmp-snooping port-info 5231
10.9.4 display igmp-snooping querier 5235
10.9.5 display igmp-snooping router-port 5237
10.9.6 display igmp-snooping statistics 5239
10.9.7 display l2-multicast forwarding-table 5242
10.9.8 igmp-snooping enable (system view) 5244

10.9.9 igmp-snooping enable (VLAN view) 5245
10.9.10 igmp-snooping group-limit 5246
10.9.11 igmp-snooping group-policy (interface view) 5250
10.9.12 igmp-snooping group-policy (VLAN view) 5252
10.9.13 igmp-snooping lastmember-queryinterval 5254
10.9.14 igmp-snooping learning 5256
10.9.15 igmp-snooping max-response-time 5258
10.9.16 igmp-snooping prompt-leave 5260
10.9.17 igmp-snooping querier enable 5262
10.9.18 igmp-snooping query-interval 5263
10.9.19 igmp-snooping report-suppress 5265
10.9.20 igmp-snooping require-router-alert 5267
10.9.21 igmp-snooping robust-count 5268
10.9.22 igmp-snooping router-aging-time 5270
10.9.23 igmp-snooping router-learning (VLAN view) 5272
10.9.24 igmp-snooping send-query enable 5273
10.9.25 igmp-snooping send-query source-address 5275
10.9.26 igmp-snooping send-router-alert 5276
10.9.27 igmp-snooping ssm-mapping 5277
10.9.28 igmp-snooping ssm-mapping enable 5279
10.9.29 igmp-snooping ssm-policy 5281
10.9.30 igmp-snooping static-router-port 5282
10.9.31 igmp-snooping suppress-time 5284
10.9.32 igmp-snooping version 5286
10.9.33 l2-multicast static-group 5287
10.9.34 multicast drop-unknown 5291
10.9.35 reset igmp-snooping group 5292
10.9.36 reset igmp-snooping statistics 5293
10.10 MLD Snooping Configuration Commands 5294
10.10.1 display mld-snooping 5295
10.10.2 display mld-snooping configuration 5298
10.10.3 display mld-snooping port-info 5299
10.10.4 display mld-snooping router-port 5301
10.10.5 display mld-snooping statistics 5303
10.10.6 mld-snooping enable 5306
10.10.7 mld-snooping group-policy (interface view) 5308
10.10.8 mld-snooping group-policy (VLAN view) 5310
10.10.9 mld-snooping last-listener-query-interval 5312
10.10.10 mld-snooping max-response-time 5314
10.10.11 mld-snooping prompt-leave 5316
10.10.12 mld-snooping querier enable 5318
10.10.13 mld-snooping query-interval 5319

10.10.14 mld-snooping require-router-alert 5321
10.10.15 mld-snooping robust-count 5322
10.10.16 mld-snooping router-aging-time 5324
10.10.17 mld-snooping send-query enable 5326
10.10.18 mld-snooping send-query source-address 5327
10.10.19 mld-snooping send-router-alert 5329
10.10.20 mld-snooping static-group 5330
10.10.21 mld-snooping static-router-port 5332
10.10.22 mld-snooping suppression-time 5333
10.10.23 mld-snooping table limit 5335
10.10.24 mld-snooping version 5337
10.10.25 multicast drop-unknown 5339
10.10.26 reset mld-snooping group 5340
10.10.27 reset mld-snooping statistics 5341
10.11 Multicast Network Management Commands 5342
10.11.1 display pim mib-control-message 5342
10.11.2 display pim mib-notification interval 5345
10.11.3 display snmp-agent trap feature-name igmp all 5346
10.11.4 display snmp-agent trap feature-name mld all 5350
10.11.5 display snmp-agent trap feature-name mrm all 5352
10.11.6 display snmp-agent trap feature-name msdp all 5353
10.11.7 display snmp-agent trap feature-name pim all 5355
10.11.8 display snmp-agent trap feature-name pim-std all 5358
10.11.9 igmp trap-interval limit 5360
10.11.10 mgmd total-number threshold-alarm 5361
10.11.11 mgmd host threshold-alarm 5362
10.11.12 multicast forwarding-table source-group-number threshold-alarm 5364
10.11.13 multicast mib-notification join-leave frequency 5366
10.11.14 multicast-mib 5367
10.11.15 pim mib-notification interval 5368
10.11.16 pim threshold-alarm 5370
10.11.17 snmp-agent trap enable feature-name igmp 5371
10.11.18 snmp-agent trap enable feature-name mld 5375
10.11.19 snmp-agent trap enable feature-name mrm 5376
10.11.20 snmp-agent trap enable feature-name msdp 5378
10.11.21 snmp-agent trap enable feature-name pim 5379
10.11.22 snmp-agent trap enable feature-name pim-std 5382

11 MPLS Commands 5384

11.1 Basic MPLS Configuration Commands 5384
11.1.1 apply lsp public 5384
11.1.2 authentication exclude 5386
11.1.3 authentication key-chain 5387

11.1.4 authentication key-chain all....5389
11.1.5 authentication key-chain peer-group....5390
11.1.6 auto-frr lsp-trigger....5392
11.1.7 backoff timer....5394
11.1.8 bfd bind ldp-lsp....5396
11.1.9 bfd bind static-lsp....5397
11.1.10 capability-announcement....5399
11.1.11 diffserv-mode....5400
11.1.12 display default-parameter mpls ldp....5402
11.1.13 display default-parameter mpls management....5406
11.1.14 display isis ldp-sync interface....5414
11.1.15 display lspv configuration....5416
11.1.16 display lspv statistics....5417
11.1.17 display mpls bfd session....5419
11.1.18 display mpls graceful-restart....5423
11.1.19 display mpls interface....5424
11.1.20 display mpls label static available....5426
11.1.21 display mpls label-stack ilm inlabel....5427
11.1.22 display mpls last-info lsp-down....5429
11.1.23 display mpls ldp....5432
11.1.24 display mpls ldp adjacency....5435
11.1.25 display mpls ldp adjacency statistics....5438
11.1.26 display mpls ldp error packet....5440
11.1.27 display mpls ldp error packet state....5441
11.1.28 display mpls ldp event adjacency-down....5443
11.1.29 display mpls ldp event gr-helper....5446
11.1.30 display mpls ldp event session-down....5448
11.1.31 display mpls ldp interface....5449
11.1.32 display mpls label all summary....5452
11.1.33 display mpls ldp lsp....5453
11.1.34 display mpls ldp lsp statistics....5455
11.1.35 display mpls ldp peer....5456
11.1.36 display mpls ldp peer statistics....5461
11.1.37 display mpls ldp remote-peer....5462
11.1.38 display mpls ldp session....5464
11.1.39 display mpls ldp session statistics....5470
11.1.40 display mpls lsp....5471
11.1.41 display mpls lsp statistics....5478
11.1.42 display mpls route-state....5480
11.1.43 display mpls static-lsp....5482
11.1.44 display ospf ldp-sync interface....5484
11.1.45 display snmp-agent trap feature-name ldp all....5486

11.1.46 display snmp-agent trap feature-name mpls_lspm all....5487
11.1.47 display static-route ldp-sync....5496
11.1.48 fec-list....5498
11.1.49 fec-node....5499
11.1.50 graceful-restart (MPLS-LDP view)....5500
11.1.51 graceful-restart timer neighbor-liveness....5501
11.1.52 graceful-restart timer reconnect....5502
11.1.53 graceful-restart timer recovery....5504
11.1.54 gtsm peer valid-ttl-hops....5505
11.1.55 inbound peer fec....5507
11.1.56 isis ldp-sync....5509
11.1.57 isis ldp-sync block....5511
11.1.58 isis timer ldp-sync hold-down....5512
11.1.59 isis timer ldp-sync hold-max-cost....5513
11.1.60 label advertise....5514
11.1.61 label distribution control-mode....5516
11.1.62 label-withdraw-delay....5517
11.1.63 label-withdraw-delay timer....5518
11.1.64 ldp-sync enable....5520
11.1.65 longest-match....5521
11.1.66 lsp-trigger bgp-label-route....5522
11.1.67 lsp-trigger....5524
11.1.68 lspv mpls-lsp-ping echo enable....5525
11.1.69 lspv packet-filter....5527
11.1.70 lsr-id....5528
11.1.71 maintain-session received-error-message....5529
11.1.72 md5-password....5530
11.1.73 md5-password all....5532
11.1.74 md5-password peer-group....5534
11.1.75 mpls (system view)....5536
11.1.76 mpls (interface view)....5537
11.1.77 mpls bfd enable....5538
11.1.78 mpls bfd....5539
11.1.79 mpls bfd-trigger....5541
11.1.80 mpls dynamic-label-number threshold-alarm....5542
11.1.81 mpls ldp advertisement....5544
11.1.82 mpls ldp (system view)....5545
11.1.83 mpls ldp (interface view)....5546
11.1.84 mpls ldp frr nexthop....5548
11.1.85 mpls ldp remote-peer....5550
11.1.86 mpls ldp timer hello-hold....5551
11.1.87 mpls ldp timer hello-send....5552

11.1.88 mpls ldp timer igp-sync-delay....5554
11.1.89 mpls ldp timer keepalive-hold....5555
11.1.90 mpls ldp timer keepalive-send....5557
11.1.91 mpls ldp transport-address....5558
11.1.92 mpls lsr-id....5560
11.1.93 mpls mtu....5561
11.1.94 mpls-passive....5562
11.1.95 mpls ping interval....5564
11.1.96 mtu-signalling....5565
11.1.97 no-renegotiate session-parameter-change graceful-restart....5566
11.1.98 ospf ldp-sync....5567
11.1.99 ospf timer ldp-sync hold-down....5569
11.1.100 ospf timer ldp-sync hold-max-cost....5570
11.1.101 outbound peer bgp-label-route....5571
11.1.102 outbound peer fec....5574
11.1.103 outbound peer split-horizon....5576
11.1.104 ping lsp....5578
11.1.105 propagate mapping....5585
11.1.106 proxy-egress disable....5586
11.1.107 remote-ip....5587
11.1.108 remote-ip auto-dod-request....5589
11.1.109 remote-peer auto-dod-request....5590
11.1.110 remote-peer pwe3....5592
11.1.111 reset mpls ldp....5593
11.1.112 reset mpls ldp error packet....5594
11.1.113 reset mpls ldp event adjacency-down....5595
11.1.114 reset mpls ldp event session-down....5595
11.1.115 route recursive-lookup tunnel....5596
11.1.116 snmp-agent trap enable feature-name ldp....5597
11.1.117 snmp-agent trap enable feature-name mpls_lspm....5599
11.1.118 snmp-agent trap suppress feature-name lsp....5605
11.1.119 static-lsp egress....5607
11.1.120 static-lsp ingress....5608
11.1.121 static-lsp transit....5610
11.1.122 static-route timer ldp-sync hold-down....5612
11.1.123 timer ldp-sync hold-down....5613
11.1.124 timer ldp-sync hold-max-cost....5614
11.1.125 tracert lsp....5616
11.1.126 ttl expiration pop....5621
11.1.127 ttl propagate....5622
11.1.128 ttl propagate public....5623
11.1.129 ttl propagate vpn....5624

11.1.130 undo outbound peer all.....5625
11.1.131 undo inbound peer all.....5626
11.2 MPLS TE Configuration Commands.....5627
11.2.1 add hop.....5627
11.2.2 bfd bind mpls-te.....5629
11.2.3 delete hop.....5631
11.2.4 display default-parameter mpls rsvp-te.....5632
11.2.5 display default-parameter mpls te cspf.....5634
11.2.6 display default-parameter mpls te management.....5635
11.2.7 display explicit-path.....5638
11.2.8 display mpls lsp attribute.....5640
11.2.9 display mpls rsvp-te.....5643
11.2.10 display mpls rsvp-te bfd session.....5646
11.2.11 display mpls rsvp-te established.....5648
11.2.12 display mpls rsvp-te graceful-restart.....5650
11.2.13 display mpls rsvp-te graceful-restart peer.....5652
11.2.14 display mpls rsvp-te interface.....5655
11.2.15 display mpls rsvp-te nsr status.....5657
11.2.16 display mpls rsvp-te peer.....5662
11.2.17 display mpls rsvp-te psb-content.....5664
11.2.18 display mpls rsvp-te request.....5667
11.2.19 display mpls rsvp-te reservation.....5669
11.2.20 display mpls rsvp-te rsb-content.....5671
11.2.21 display mpls rsvp-te sender.....5674
11.2.22 display mpls rsvp-te session.....5675
11.2.23 display mpls rsvp-te statistics.....5680
11.2.24 display mpls rsvp-te statistics fast-reroute.....5683
11.2.25 display mpls static-cr-lsp.....5685
11.2.26 display mpls stale-interface.....5687
11.2.27 display mpls te cspf destination.....5690
11.2.28 display mpls te cspf tedb.....5694
11.2.29 display mpls te ds-te.....5702
11.2.30 display mpls te hot-standby state.....5705
11.2.31 display mpls te link-administration admission-control.....5708
11.2.32 display mpls te link-administration bandwidth-allocation.....5709
11.2.33 display mpls te link-administration srlg-information.....5712
11.2.34 display mpls te session-entry.....5713
11.2.35 display mpls te srlg.....5715
11.2.36 display mpls te te-class-tunnel.....5716
11.2.37 display mpls te tunnel-interface.....5718
11.2.38 display mpls te tunnel-interface failed.....5721
11.2.39 display mpls te tunnel-interface last-error.....5722

11.2.40 display mpls te tunnel-interface traffic-state....5725
11.2.41 display mpls te tunnel....5727
11.2.42 display mpls te tunnel c-hop....5734
11.2.43 display mpls te tunnel path....5735
11.2.44 display mpls te tunnel statistics....5738
11.2.45 display ospf mpls-te....5740
11.2.46 display ospf traffic-adjustment....5744
11.2.47 display snmp-agent trap feature-name mpls_rsvp all....5746
11.2.48 display snmp-agent trap feature-name tunnel-te all....5748
11.2.49 enable traffic-adjustment....5750
11.2.50 explicit-path....5751
11.2.51 list hop....5752
11.2.52 modify hop....5753
11.2.53 mpls-te enable....5755
11.2.54 mpls rsvp-te....5756
11.2.55 mpls rsvp-te authentication....5757
11.2.56 mpls rsvp-te authentication handshake....5760
11.2.57 mpls rsvp-te authentication lifetime....5761
11.2.58 mpls rsvp-te authentication window-size....5763
11.2.59 mpls rsvp-te bfd....5764
11.2.60 mpls rsvp-te bfd all-interfaces....5766
11.2.61 mpls rsvp-te bfd all-interfaces enable....5767
11.2.62 mpls rsvp-te bfd block....5768
11.2.63 mpls rsvp-te bfd enable....5770
11.2.64 mpls rsvp-te challenge-lost....5771
11.2.65 mpls rsvp-te fast-reroute-bandwidth compatible....5772
11.2.66 mpls rsvp-te hello-lost....5773
11.2.67 mpls rsvp-te hello....5774
11.2.68 mpls rsvp-te hello basic-restart-time....5776
11.2.69 mpls rsvp-te hello full-gr....5777
11.2.70 mpls rsvp-te hello nodeid-session....5778
11.2.71 mpls rsvp-te hello support-peer-gr....5779
11.2.72 mpls rsvp-te keep-multiplier....5780
11.2.73 mpls rsvp-te peer....5781
11.2.74 mpls rsvp-te resv-rro....5783
11.2.75 mpls rsvp-te resvconfirm....5784
11.2.76 mpls rsvp-te retrans-timer challenge....5785
11.2.77 mpls rsvp-te send-message....5786
11.2.78 mpls rsvp-te srefresh....5788
11.2.79 mpls rsvp-te timer hello....5789
11.2.80 mpls rsvp-te timer refresh....5790
11.2.81 mpls rsvp-te timer retransmission....5791

11.2.82 mpls te 5792
11.2.83 mpls te affinity property 5793
11.2.84 mpls te auto-frr (MPLS view) 5795
11.2.85 mpls te auto-frr (interface view) 5796
11.2.86 mpls te auto-frr reoptimization 5798
11.2.87 mpls te backup 5799
11.2.88 mpls te backup frr-in-use 5802
11.2.89 mpls te backup hot-standby overlap-path 5803
11.2.90 mpls te bandwidth (interface view) 5804
11.2.91 mpls te bandwidth (tunnel interface view) 5806
11.2.92 mpls te bandwidth change thresholds 5808
11.2.93 mpls te bandwidth max-reservable-bandwidth 5810
11.2.94 mpls te bfd 5811
11.2.95 mpls te bfd block 5812
11.2.96 mpls te bfd enable 5813
11.2.97 mpls te bypass-attributes 5815
11.2.98 mpls te bypass-tunnel 5816
11.2.99 mpls te commit 5817
11.2.100 mpls te cspf 5818
11.2.101 mpls te cspf disable 5819
11.2.102 mpls te cspf preferred-igp 5820
11.2.103 mpls te cspf timer failed-link 5822
11.2.104 mpls te ds-te bcm 5823
11.2.105 mpls te ds-te mode 5824
11.2.106 mpls te fast-reroute 5825
11.2.107 mpls te hop-limit 5826
11.2.108 mpls te igp advertise 5827
11.2.109 mpls te igp metric 5828
11.2.110 mpls te igp shortcut 5829
11.2.111 mpls te link administrative group 5830
11.2.112 mpls te loop-detection 5831
11.2.113 mpls te metric 5832
11.2.114 mpls te path explicit-path 5833
11.2.115 mpls te path metric-type 5834
11.2.116 mpls te path-selection overload 5835
11.2.117 mpls te priority 5837
11.2.118 mpls te protected-interface 5838
11.2.119 mpls te record-route 5840
11.2.120 mpls te reoptimization (user view) 5841
11.2.121 mpls te reoptimization (tunnel interface view) 5842
11.2.122 mpls te resv-style 5844
11.2.123 mpls te route-pinning 5845

11.2.124 mpls te signal-protocol 5846
11.2.125 mpls te signaling-delay-trigger enable 5847
11.2.126 mpls te signalled tunnel-name 5848
11.2.127 mpls te srlg 5849
11.2.128 mpls te srlg path-calculation 5850
11.2.129 mpls te switch-delay 5852
11.2.130 mpls te tie-breaking 5854
11.2.131 mpls te timer fast-reroute 5855
11.2.132 mpls te timer retry 5856
11.2.133 mpls te tunnel-id 5858
11.2.134 next hop 5859
11.2.135 notify neighbor-down 5860
11.2.136 opaque-capability enable 5861
11.2.137 qos te queue-profile 5862
11.2.138 reset mpls rsvp-te 5863
11.2.139 reset mpls rsvp-te statistics 5864
11.2.140 reset mpls stale-interface 5865
11.2.141 reset mpls te auto-frr 5866
11.2.142 reset mpls te tunnel-interface tunnel 5867
11.2.143 snmp-agent trap enable feature-name mpls_rsvp 5868
11.2.144 snmp-agent trap enable feature-name tunnel-te 5870
11.2.145 static-cr-lsp egress 5872
11.2.146 static-cr-lsp ingress 5873
11.2.147 static-cr-lsp transit 5875
11.2.148 te-class 5877
11.2.149 te-class-mapping 5879
11.2.150 te-set-subtlv 5881
11.2.151 traffic-eng 5882
11.2.152 undo mpls te srlg all-config 5883

12 VPN Commands 5885

12.1 L2TP Configuration Commands 5885
12.1.1 allow l2tp 5886
12.1.2 display l2tp session 5887
12.1.3 display l2tp tunnel 5891
12.1.4 display l2tp-group 5894
12.1.5 display l2tp statistics tunnel 5897
12.1.6 l2tp aging 5900
12.1.7 l2tp enable 5900
12.1.8 l2tp-auto-client enable 5901
12.1.9 l2tp-group 5902
12.1.10 mandatory-chap 5904
12.1.11 mandatory-lcp 5905

12.1.12 multichassis-mp enable....5906
12.1.13 reset l2tp session....5908
12.1.14 reset l2tp tunnel....5909
12.1.15 reset l2tp statistics tunnel....5910
12.1.16 start l2tp....5912
12.1.17 tunnel authentication....5914
12.1.18 tunnel avp-hidden....5915
12.1.19 tunnel name....5917
12.1.20 tunnel password....5918
12.1.21 tunnel timer hello....5920
12.2 L2TPv3 Configuration Commands....5921
12.2.1 encapsulation l2tpv3....5921
12.2.2 l2tpv3 enable....5922
12.2.3 l2tpv3 local cookie....5923
12.2.4 l2tpv3 local session-id....5925
12.2.5 l2tpv3 remote cookie....5926
12.2.6 l2tpv3 remote session-id....5928
12.2.7 link-bridge....5929
12.2.8 tunnel-destination....5931
12.2.9 tunnel-source....5932
12.3 GRE Configuration Commands....5934
12.3.1 description (tunnel interface view)....5934
12.3.2 destination....5935
12.3.3 display interface tunnel....5937
12.3.4 display keepalive packets count....5940
12.3.5 display tunnel-info....5942
12.3.6 gre checksum....5945
12.3.7 gre df-bit....5946
12.3.8 gre key....5947
12.3.9 gre map virtual-ethernet forward-broadcast disable....5949
12.3.10 interface tunnel....5950
12.3.11 keepalive....5952
12.3.12 link-bridge....5954
12.3.13 map interface virtual-ethernet....5959
12.3.14 mtu (tunnel interface view)....5961
12.3.15 portswitch (VE interface view)....5963
12.3.16 qos pre-classify....5964
12.3.17 reset keepalive packets count....5965
12.3.18 source....5966
12.3.19 statistic enable (Tunnel interface view)....5968
12.3.20 tunnel route-via....5969
12.3.21 tunnel-protocol....5971

12.4 SVPN Configuration Commands 5974
12.4.1 authentication 5974
12.4.2 cmi-method (service view) 5975
12.4.3 cmi-threshold (service view) 5977
12.4.4 encapsulation (SVPN proposal view) 5979
12.4.5 destination (SVPN proposal view) 5980
12.4.6 svpn-proposal (system view) 5982
12.4.7 svpn-proposal (tunnel interface view) 5983
12.4.8 svpn-zone 5984
12.4.9 match (service view) 5986
12.4.10 recovery-delay 5987
12.4.11 reorder-window 5988
12.4.12 schedule-type (service view) 5989
12.4.13 service (SVPN proposal view) 5990
12.4.14 source (SVPN proposal view) 5992
12.4.15 source (service view) 5995
12.4.16 source index (service view) 5997
12.4.17 tunnel-protocol 5999
12.5 DSVPN Configuration Commands 6002
12.5.1 display nhrp peer 6002
12.5.2 display nhrp peer maximum-history 6004
12.5.3 display nhrp statistics 6006
12.5.4 nhrp authentication 6010
12.5.5 nhrp entry 6012
12.5.6 nhrp entry holdtime 6014
12.5.7 nhrp entry multicast dynamic 6016
12.5.8 nhrp network-id 6017
12.5.9 nhrp redirect 6019
12.5.10 nhrp registration interval 6020
12.5.11 nhrp registration no-unique 6022
12.5.12 nhrp shortcut 6024
12.5.13 nhrp tunnel-if-state related 6025
12.5.14 reset nhrp peer maximum-history 6026
12.5.15 reset nhrp statistics 6027
12.5.16 source 6028
12.5.17 tunnel-protocol 6030
12.5.18 undo nhrp peer 6032
12.6 IPSec Configuration Commands 6033
12.6.1 aaa authorization 6034
12.6.2 alias 6035
12.6.3 ah authentication-algorithm 6036
12.6.4 ah authentication-algorithm (ipsec-proto-protect-proposal view) 6038

12.6.5 anti-replay window....6039
12.6.6 authentication-algorithm....6040
12.6.7 authentication-method....6042
12.6.8 certificate peer-name....6043
12.6.9 certificate-check disable....6044
12.6.10 certificate-request empty-payload enable....6045
12.6.11 config-exchange....6046
12.6.12 connect track....6048
12.6.13 description....6051
12.6.14 dh....6052
12.6.15 disconnect track....6053
12.6.16 display ike error-info....6056
12.6.17 display ike global config....6064
12.6.18 display ike offline-info....6065
12.6.19 display ike identity....6068
12.6.20 display ike peer (all views)....6069
12.6.21 display ike peer ctrl-plane....6077
12.6.22 display ike proposal (All views)....6081
12.6.23 display ike proposal ctrl-plane....6085
12.6.24 display ike sa....6087
12.6.25 display ike statistics....6095
12.6.26 display ikev2 statistics....6098
12.6.27 display ike user-table (all views)....6109
12.6.28 display ike user-table ctrl-plane....6111
12.6.29 display interface tunnel-template....6112
12.6.30 display ipsec efficient-vpn....6115
12.6.31 display ipsec history record....6125
12.6.32 display ipsec global config....6128
12.6.33 display ipsec interface brief....6130
12.6.34 display ipsec policy (all views)....6131
12.6.35 display ipsec policy ctrl-plane....6137
12.6.36 display ipsec policy-template (all views)....6141
12.6.37 display ipsec policy-template ctrl-plane....6146
12.6.38 display ipsec profile (all views)....6149
12.6.39 display ipsec profile ctrl-plane....6153
12.6.40 display ipsec proposal (All views)....6156
12.6.41 display ipsec proposal ctrl-plane....6158
12.6.42 display ipsec proto-protect proposal....6160
12.6.43 display ipsec proposal (User view)....6161
12.6.44 display ipsec sa....6163
12.6.45 display ipsec proto-protect sa....6169
12.6.46 display ipsec statistics....6171

 Copyright © Huawei Technologies Co., Ltd.

12.6.47 display ipsec statistics route....6176
12.6.48 display ipsec proto-protect statistics....6178
12.6.49 dn....6181
12.6.50 dpd....6182
12.6.51 dpd msg....6183
12.6.52 dpd type....6185
12.6.53 dscp....6186
12.6.54 encapsulation-mode....6188
12.6.55 encapsulation-mode (ipsec-proto-protect-proposal view)....6189
12.6.56 encryption-algorithm....6190
12.6.57 esp authentication-algorithm....6191
12.6.58 esp authentication-algorithm (ipsec-proto-protect-proposal view)....6193
12.6.59 esp encryption-algorithm....6195
12.6.60 esp encryption-algorithm (ipsec-proto-protect-proposal view)....6196
12.6.61 exchange-mode....6198
12.6.62 fqdn....6199
12.6.63 id-type....6201
12.6.64 ike call admission limit in-negotiation-sa....6202
12.6.65 ike certificate-check disable....6203
12.6.66 ike dscp....6204
12.6.67 ike heartbeat....6205
12.6.68 ike heartbeat-timer interval....6207
12.6.69 ike heartbeat-timer timeout....6208
12.6.70 ike identity....6209
12.6.71 ike local-name....6210
12.6.72 ike nat-keepalive-timer interval....6211
12.6.73 ike sm-encryption-key-length enable....6212
12.6.74 ike user-table....6213
12.6.75 ike peer....6215
12.6.76 ike proposal....6216
12.6.77 ike-peer....6218
12.6.78 ike-proposal....6219
12.6.79 ikev1 phase1-phase2 sa dependent....6220
12.6.80 ikev2 authentication sign-hash....6221
12.6.81 ikev2 cookie-challenge....6223
12.6.82 ikev2 initial-contact enable....6224
12.6.83 ikev2 id-match-certificate enable....6225
12.6.84 ikev2 prf aes-xcbc-128 compatible....6226
12.6.85 inband crl....6227
12.6.86 inband ocsp....6228
12.6.87 integrity-algorithm....6229
12.6.88 interface-assign....6230

12.6.89 interface tunnel-template....6231
12.6.90 ip address....6233
12.6.91 ip address ike-negotiated....6234
12.6.92 ipsec anti-replay enable....6235
12.6.93 ipsec anti-replay window....6236
12.6.94 ipsec authentication sha2 compatible enable....6238
12.6.95 ipsec decrypt check....6239
12.6.96 ipsec df-bit....6240
12.6.97 ipsec efficient-vpn (interface view)....6241
12.6.98 ipsec efficient-vpn (system view)....6242
12.6.99 ipsec fragmentation before-encryption....6244
12.6.100 ipsec invalid-spi-recovery enable....6246
12.6.101 ipsec nat-traversal source-port....6247
12.6.102 ipsec netmask....6248
12.6.103 ipsec policy shared....6250
12.6.104 ipsec policy (interface view)....6251
12.6.105 ipsec policy (system view)....6253
12.6.106 ipsec policy-template....6256
12.6.107 ipsec profile (interface view)....6257
12.6.108 ipsec profile (system view)....6258
12.6.109 ipsec proposal....6260
12.6.110 ipsec proto-protect proposal....6261
12.6.111 ipsec remote traffic-identical accept....6262
12.6.112 ipsec sa....6264
12.6.113 ipsec sa global-duration....6265
12.6.114 ipsec sm4 version....6268
12.6.115 lifetime-notification-message enable....6269
12.6.116 local-address....6270
12.6.117 local-id-type....6272
12.6.118 local-id....6275
12.6.119 local-id-preference certificate enable....6276
12.6.120 local-id-reflect enable....6278
12.6.121 match ike-identity....6279
12.6.122 nat traversal....6280
12.6.123 pfs....6281
12.6.124 pki realm....6283
12.6.125 policy enable....6285
12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)....6285
12.6.127 pre-shared-key (IKE user view)....6288
12.6.128 prf....6290
12.6.129 proposal....6291
12.6.130 proposal (SA view)....6293

12.6.131 qos group 6294
12.6.132 qos pre-classify 6295
12.6.133 re-authentication interval 6296
12.6.134 remote-address (IKE peer view) 6297
12.6.135 remote-address (Efficient VPN policy view) 6302
12.6.136 remote-id 6303
12.6.137 remote-id-type 6305
12.6.138 reset ike error-info 6307
12.6.139 reset ike offline-info 6308
12.6.140 reset ike sa 6309
12.6.141 reset ike statistics 6310
12.6.142 reset ipsec history record 6311
12.6.143 reset ipsec sa 6312
12.6.144 reset ipsec statistics 6314
12.6.145 reset ipsec statistics route 6315
12.6.146 reset ipsec proto-protect statistics 6316
12.6.147 respond-only enable 6316
12.6.148 resource acl 6317
12.6.149 route accept 6319
12.6.150 route inject 6320
12.6.151 rsa encryption-padding 6322
12.6.152 rsa signature-padding 6323
12.6.153 sa authentication-hex 6324
12.6.154 sa authentication-hex (SA view) 6327
12.6.155 sa binding vpn-instance 6329
12.6.156 sa binding vpn-instance (Efficient VPN policy view) 6331
12.6.157 sa duration (IKE proposal view) 6332
12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view) 6334
12.6.159 sa encryption-hex 6337
12.6.160 sa encryption-hex (SA view) 6340
12.6.161 sa keep-holding-to hard-duration 6342
12.6.162 sa spi 6343
12.6.163 sa spi (SA view) 6345
12.6.164 sa string-key 6346
12.6.165 sa string-key (SA view) 6349
12.6.166 sa trigger-mode 6351
12.6.167 security acl 6352
12.6.168 service-scheme 6354
12.6.169 service-scheme (Efficient VPN policy view) 6355
12.6.170 sim-based-username 6356
12.6.171 switch-back enable 6358
12.6.172 transform 6359

12.6.173 transform (ipsec-proto-protect-proposal view) 6360
12.6.174 tunnel local 6361
12.6.175 tunnel remote 6363
12.6.176 tunnel pathmtu enable 6364
12.6.177 user (IKE user table view) 6365
12.6.178 user 6368
12.6.179 user-table 6369
12.6.180 version 6371
12.6.181 vpn-instance-traffic (IKE user view) 6371
12.6.182 user-fqdn 6373
12.7 A2A VPN Configuration Commands 6374
12.7.1 anti-replay time-based enable 6374
12.7.2 anti-replay time-based window 6375
12.7.3 display gdoi ks group 6377
12.7.4 display gdoi ks members 6381
12.7.5 display gdoi ks members history record 6383
12.7.6 display gdoi ks rekey statistics 6386
12.7.7 display gdoi ks sa 6387
12.7.8 display ipsec gdoi-policy 6390
12.7.9 display ipsec gdoi-sa 6395
12.7.10 gdoi ks group 6400
12.7.11 gdoi ks rekey 6401
12.7.12 gdoi sa direction receive-option 6402
12.7.13 group identity number 6403
12.7.14 ike-peer 6404
12.7.15 ipsec 6405
12.7.16 ipsec gdoi anti-replay force 32-bit enable 6407
12.7.17 ipsec gdoi multicast-rekey ip 6408
12.7.18 ipsec policy (system view) 6409
12.7.19 ipsec policy (interface view) 6410
12.7.20 local-id-type (GDOI Group View) 6412
12.7.21 local-id (GDOI Group View) 6413
12.7.22 proposal (GDOI group IPSec policy View) 6414
12.7.23 rekey authentication public-key rsa 6416
12.7.24 rekey destination address 6417
12.7.25 rekey encryption-algorithm 6418
12.7.26 rekey retry 6420
12.7.27 rekey sa duration time-based 6421
12.7.28 rekey sig-hash-algorithm 6423
12.7.29 rekey transport-type 6425
12.7.30 reset gdoi ks group 6426
12.7.31 reset gdoi ks members 6427

 Copyright © Huawei Technologies Co., Ltd.

12.7.32 reset gdoi ks members history record ... 6428
12.7.33 reset gdoi ks rekey statistics ... 6429
12.7.34 qos group ... 6430
12.7.35 qos pre-classify ... 6431
12.7.36 reset ipsec gdoi-sa ... 6432
12.7.37 sa duration time-based ... 6434
12.7.38 sa receive-only ... 6435
12.7.39 security acl ... 6437
12.7.40 source address (GDOI Group View) ... 6438
12.7.41 tunnel local ... 6440
12.7.42 user-table (GDOI Group View) ... 6441
12.8 SSL VPN Configuration Commands ... 6442
12.8.1 background-color ... 6443
12.8.2 banner-color ... 6444
12.8.3 bind acl ... 6445
12.8.4 bind domain ... 6446
12.8.5 bind ip-pool ... 6447
12.8.6 cut user ... 6449
12.8.7 description ... 6451
12.8.8 display sslvpn gateway ... 6452
12.8.9 display sslvpn gateway access-user ... 6454
12.8.10 display sslvpn gateway resource ... 6456
12.8.11 display sslvpn user statistics ... 6458
12.8.12 display sslvpn server port ... 6459
12.8.13 enable ... 6460
12.8.14 intranet interface ... 6461
12.8.15 link ... 6463
12.8.16 login-help ... 6465
12.8.17 login-message ... 6466
12.8.18 login-photo ... 6468
12.8.19 logo ... 6469
12.8.20 max-online-time ... 6470
12.8.21 max-user ... 6471
12.8.22 organization ... 6474
12.8.23 reset sslvpn user statistics ... 6475
12.8.24 route-mode ... 6476
12.8.25 route-split ... 6478
12.8.26 server ip-address ... 6479
12.8.27 server name ... 6481
12.8.28 service-type resource ... 6482
12.8.29 sslvpn gateway ... 6484
12.8.30 sslvpn server port ... 6485

12.8.31 table-color 6486
12.8.32 text-color 6488
12.9 BGP/MPLS IP VPN Configuration Commands 6489
12.9.1 apply tunnel-policy (tunnel-selector view) 6489
12.9.2 apply-label per-instance 6491
12.9.3 apply-label per-nexthop 6492
12.9.4 apply-label per-route 6494
12.9.5 apply lsp vpn 6495
12.9.6 as-number 6496
12.9.7 description (VPN instance view) 6498
12.9.8 description (tunnel interface view) 6499
12.9.9 description (tunnel-policy view) 6500
12.9.10 destination 6501
12.9.11 display default-parameter l3vpn 6503
12.9.12 display ip prefix-limit statistics 6504
12.9.13 display ipv6 prefix-limit statistics 6505
12.9.14 display ip vpn-instance 6507
12.9.15 display ip vpn-instance import-vt 6514
12.9.16 display interface tunnel 6516
12.9.17 display l3vpn vpn-list tunnel-policy 6519
12.9.18 display mpls label-stack vpn-instance 6520
12.9.19 display snmp-agent trap feature-name l3vpn all 6521
12.9.20 display traffic-statistics vpn-instance 6523
12.9.21 display tunnel-info 6525
12.9.22 display tunnel-policy 6528
12.9.23 display tunnel-policy-config 6530
12.9.24 display tunnel-policy subscriber statistics 6531
12.9.25 display tunnel-selector 6532
12.9.26 export route-policy 6534
12.9.27 if-match ip next-hop (tunnel-selector view) 6535
12.9.28 if-match ip-prefix (tunnel-selector view) 6537
12.9.29 if-match ipv6 next-hop (tunnel-selector view) 6539
12.9.30 import route-policy 6540
12.9.31 ingress-lsp trigger 6541
12.9.32 interface tunnel 6543
12.9.33 ip binding vpn-instance 6545
12.9.34 ip frr (VPN instance view) 6547
12.9.35 ip vpn-instance 6548
12.9.36 ipv4-family (VPN instance view) 6550
12.9.37 ipv6-family (VPN instance view) 6551
12.9.38 limit-log-interval 6552
12.9.39 lsp-trigger bgp-label-route 6554

 Copyright © Huawei Technologies Co., Ltd.

12.9.40 mpls te reserved-for-binding 6555
12.9.41 mtu (tunnel interface view) 6556
12.9.42 peer default-originate vpn-instance 6558
12.9.43 peer mpls-local-ifnet disable 6560
12.9.44 peer upe 6561
12.9.45 peer soo 6563
12.9.46 peer substitute-as 6566
12.9.47 policy vpn-target 6568
12.9.48 prefix limit 6569
12.9.49 reset traffic-statistics vpn-instance 6571
12.9.50 route-distinguisher 6572
12.9.51 routing-table limit 6574
12.9.52 rr-filter 6576
12.9.53 service-id (VPN instance view) 6578
12.9.54 snmp-agent trap enable feature-name l3vpn 6579
12.9.55 source 6581
12.9.56 supernet label-route advertise 6583
12.9.57 traffic-statistics enable 6584
12.9.58 tunnel binding 6585
12.9.59 tunnel-selector (system view) 6587
12.9.60 tunnel-selector (BGP view) 6589
12.9.61 tunnel select-seq 6591
12.9.62 tunnel-policy nonexistent-config-check 6593
12.9.63 tunnel-policy (system view) 6594
12.9.64 tunnel-protocol 6595
12.9.65 tnl-policy 6598
12.9.66 transit-vpn 6600
12.9.67 undo vpn frr all 6601
12.9.68 vpn-route cross multipath 6601
12.9.69 vpn-target 6603
12.9.70 vpn frr 6606
12.10 EVPN Configuration Commands 6607
12.10.1 advertise l2vpn evpn 6607
12.10.2 display bgp evpn routing-table 6608
12.10.3 display bgp evpn update-peer-group 6612
12.10.4 export route-policy evpn 6615
12.10.5 import route-policy evpn 6616
12.10.6 peer advertise 6617
12.10.7 peer advertise route-reoriginated 6619
12.10.8 peer import reoriginate 6620
12.10.9 l2vpn-family evpn 6622
12.10.10 peer mac-limit 6623

12.10.11 peer route-policy (BGP-EVPN address family view) 6624
12.10.12 policy vpn-target (BGP-EVPN address family view) 6626
12.10.13 refresh bgp evpn 6627
12.10.14 vpn-target evpn 6628
12.11 VLL Configuration Commands 6632
12.11.1 bfd bind pw 6632
12.11.2 ccc interface out-interface 6634
12.11.3 display l2vpn ccc-interface vc-type 6636
12.11.4 display mpls l2vc 6638
12.11.5 display mpls l2vc brief 6651
12.11.6 display mpls l2vc oam-mapping 6653
12.11.7 display mpls l2vpn forwarding-info 6657
12.11.8 display mpls l2vpn label-space 6659
12.11.9 display mpls l2vpn resource 6661
12.11.10 display mpls l2vpn vpws 6662
12.11.11 display mpls label-stack vll interface 6666
12.11.12 display mpls static-l2vc 6667
12.11.13 display mpls static-l2vc brief 6675
12.11.14 display snmp-agent trap feature-name l2vpn all 6677
12.11.15 display virtual-ethernet ve-group 6680
12.11.16 display vll ccc 6681
12.11.17 l3ve track oam-state 6683
12.11.18 l3ve track pw-state 6684
12.11.19 manual-set pw-ac-fault 6686
12.11.20 mpls l2vc 6687
12.11.21 mpls l2vpn 6690
12.11.22 mpls l2vpn default martini 6691
12.11.23 mpls l2vpn frag 6692
12.11.24 mpls l2vpn oam-mapping 6693
12.11.25 mpls l2vpn reroute 6694
12.11.26 mpls l2vpn service-name 6696
12.11.27 mpls l2vpn vccv bfd-cv-negotiation fault-detection-only 6698
12.11.28 mpls static-l2vc 6700
12.11.29 ping vc 6704
12.11.30 snmp-agent trap enable feature-name l2vpn 6708
12.11.31 tracert vc 6711
12.11.32 ve-group 6716
12.12 PWE3 Configuration Commands 6717
12.12.1 bfd bind pw 6717
12.12.2 control-word 6719
12.12.3 display mpls l2vc 6720
12.12.4 display mpls l2vc brief 6733

12.12.5 display mpls l2vc oam-mapping....6735
12.12.6 display mpls l2vpn interface performance....6739
12.12.7 display mpls static-l2vc....6741
12.12.8 display mpls static-l2vc brief....6749
12.12.9 display mpls switch-l2vc....6751
12.12.10 display mpls switch-l2vc brief....6756
12.12.11 display pw-template....6758
12.12.12 idle-code....6760
12.12.13 jitter-buffer depth....6762
12.12.14 manual-set pw-ac-fault....6763
12.12.15 mpls l2vc....6764
12.12.16 mpls l2vpn....6767
12.12.17 mpls l2vpn no-request-message....6768
12.12.18 mpls l2vpn oam-mapping....6769
12.12.19 mpls l2vpn pw performance disable....6771
12.12.20 mpls l2vpn reroute....6772
12.12.21 mpls l2vpn service-name....6774
12.12.22 mpls l2vpn stream-dual-receiving....6776
12.12.23 mpls l2vpn vccv bfd-cv-negotiation fault-detection-only....6777
12.12.24 mpls static-l2vc....6779
12.12.25 mpls switch-l2vc....6783
12.12.26 mtu (PW template view)....6788
12.12.27 peer-address....6790
12.12.28 ping vc....6791
12.12.29 pw-template....6795
12.12.30 reset pw....6797
12.12.31 snmp-agent trap enable feature-name l2vpn....6798
12.12.32 tdm-encapsulation-number....6801
12.12.33 tnl-policy (PW template view)....6802
12.12.34 tracert vc....6803
12.13 VPLS Configuration Commands....6808
12.13.1 description (VSI view)....6808
12.13.2 display l2vpn ccc-interface vc-type....6809
12.13.3 display mpls l2vpn resource....6811
12.13.4 display mpls label-stack vpls vsi....6813
12.13.5 display traffic-statistics vsi....6814
12.13.6 display traffic-statistics vsi peer....6816
12.13.7 display vpls connection....6818
12.13.8 display vpls forwarding-info....6820
12.13.9 display vpls-ping statistics....6824
12.13.10 display vpls-trace statistics....6825
12.13.11 display vsi....6826

12.13.12 display vsi mac-withdraw loop-detect 6834
12.13.13 display vsi pw out-interface 6836
12.13.14 display vsi remote 6837
12.13.15 display vsi services 6840
12.13.16 encapsulation (VSI view) 6842
12.13.17 ignore-ac-state 6843
12.13.18 interface-parameter-type vccv (VSI-LDP-PW view) 6844
12.13.19 interface-status-change mac-withdraw enable 6845
12.13.20 l2 binding 6846
12.13.21 mac-address blackhole vsi 6847
12.13.22 mac-address static vsi 6849
12.13.23 mac-learning 6852
12.13.24 mac-withdraw enable 6853
12.13.25 mpls l2vpn default vlan 6854
12.13.26 mpls l2vpn vsi-pw limit threshold-alarm 6855
12.13.27 mtu (VSI view) 6856
12.13.28 oam-detecting enable 6857
12.13.29 peer (VSI-LDP view) 6858
12.13.30 peer pw 6860
12.13.31 peer static-npe 6862
12.13.32 ping vpls 6863
12.13.33 ping vpls mac vsi 6866
12.13.34 pw 6869
12.13.35 pwsignal 6870
12.13.36 reset traffic-statistics vsi all 6871
12.13.37 reset traffic-statistics vsi name 6871
12.13.38 reset traffic-statistics vsi name peer 6873
12.13.39 reset vpls-ping statistics 6874
12.13.40 reset vpls-trace statistics 6875
12.13.41 shutdown (VSI view) 6875
12.13.42 trace vpls mac vsi 6876
12.13.43 tracert vpls 6880
12.13.44 traffic-statistics enable (VSI-LDP view) 6882
12.13.45 traffic-statistics peer enable 6883
12.13.46 vpls ignore-ac-state 6885
12.13.47 vpls mac-withdraw loop-detect enable 6886
12.13.48 vsi 6887
12.13.49 vsi-id 6888
12.14 VXLAN Configuration Commands 6889
12.14.1 arp static vni 6889
12.14.2 arp static vni interface 6891
12.14.3 bridge-domain (Layer 2 sub-interface view) 6893

12.14.4 bridge-domain (system view) 6895
12.14.5 description (BD view) 6896
12.14.6 display bridge-domain 6897
12.14.7 display interface nve 6899
12.14.8 display mac-address bridge-domain 6900
12.14.9 display vxlan encapsulation 6902
12.14.10 display vxlan peer 6905
12.14.11 display vxlan tunnel 6906
12.14.12 display vxlan vni 6908
12.14.13 encapsulation (Layer 2 sub-interface view) 6911
12.14.14 interface mode l2 6913
12.14.15 interface nve 6914
12.14.16 interface vbdif 6915
12.14.17 l2 binding vlan 6917
12.14.18 mac-address (VBDIF interface view) 6918
12.14.19 mac-address static bridge-domain 6920
12.14.20 mac-address static vni 6923
12.14.21 source (NVE interface view) 6925
12.14.22 vni head-end peer-list 6926
12.14.23 vxlan vni (BD view) 6928
12.14.24 vxlan vni (VPN instance view) 6929

13 WLAN-FAT AP Commands 6931

13.1 WLAN Service Configuration Commands 6931
13.1.1 80211n a-mpdu enable (for FAT AP) 6931
13.1.2 80211n a-mpdu (for FAT AP) 6932
13.1.3 80211bg basic-rate (for FAT AP) 6934
13.1.4 80211bg supported-rate (for FAT AP) 6935
13.1.5 ap-manufacturer-config (for FAT AP) 6937
13.1.6 ap-reset (for FAT AP) 6938
13.1.7 ap-sysname (for FAT AP) 6939
13.1.8 ap-threshold 6940
13.1.9 association-timeout (for FAT AP) 6941
13.1.10 auto-off service radio 6942
13.1.11 available-antenna-number (for Fat AP) 6944
13.1.12 beacon-interval (for FAT AP) 6945
13.1.13 channel (for FAT AP) 6947
13.1.14 channel-mode (for FAT AP) 6948
13.1.15 conflict-rate-threshold (for FAT AP) 6950
13.1.16 display actual channel-power (for FAT AP) 6951
13.1.17 display ap (for FAT AP) 6952
13.1.18 display ap configurable channel (for FAT AP) 6954
13.1.19 display ap-performance-statistic (for FAT AP) 6955

13.1.20 display ap-run-info (for FAT AP) 6956
13.1.21 display ap-threshold 6958
13.1.22 display ap around-ssid-list (for FAT AP) 6959
13.1.23 display binding radio-profile (for FAT AP) 6960
13.1.24 display channel country-code (for FAT AP) 6961
13.1.25 display power-level (for FAT AP) 6966
13.1.26 display radio config (for FAT AP) 6967
13.1.27 display radio-profile 6971
13.1.28 display radio status (for FAT AP) 6974
13.1.29 display service-set (for FAT AP) 6975
13.1.30 display station assoc-info (for FAT AP) 6977
13.1.31 display station assoc-num (for FAT AP) 6979
13.1.32 display station roam-track (for FAT AP) 6980
13.1.33 display station statistics (for FAT AP) 6981
13.1.34 display statistics sta (for FAT AP) 6985
13.1.35 display statistics radio (for FAT AP) 6988
13.1.36 display station online-fail-record (for FAT AP) 6991
13.1.37 display uncontrol ap (for FAT AP) 6995
13.1.38 display vap (for FAT AP) 6997
13.1.39 display wlan global 6998
13.1.40 display wlan record 7000
13.1.41 display workmode wlan 7002
13.1.42 dtim-interval (for FAT AP) 7003
13.1.43 forward-mode (for FAT AP) 7005
13.1.44 guard-interval-mode (for FAT AP) 7006
13.1.45 igmp-mode snooping (for FAT AP) 7007
13.1.46 interface wlan-bss 7008
13.1.47 interface wlan-radio 7010
13.1.48 legacy-station enable (for FAT AP) 7011
13.1.49 max-user-number (for FAT AP) 7012
13.1.50 multicast-rate (for FAT AP) 7013
13.1.51 per-threshold (for FAT AP) 7015
13.1.52 power-level (for FAT AP) 7016
13.1.53 power-mode (for FAT AP) 7017
13.1.54 radio enable (for FAT AP) 7018
13.1.55 radio-frequency (for FAT AP) 7019
13.1.56 radio-profile (WLAN view) (for FAT AP) 7020
13.1.57 radio-profile (Radio interface view) (for FAT AP) 7021
13.1.58 reset radio statistics (for FAT AP) 7022
13.1.59 reset station online-fail-record (for FAT AP) 7023
13.1.60 reset wlan record 7024
13.1.61 rts-cts-threshold (for FAT AP) 7025

13.1.62 set wlan collisionrate threshold....7026
13.1.63 set wlan record enable....7027
13.1.64 set wlan falsecca threshold....7029
13.1.65 set wlan utmost-power....7030
13.1.66 security-profile (service set view) (for FAT AP)....7031
13.1.67 service-set (for FAT AP)....7032
13.1.68 service-set (Radio interface view)....7034
13.1.69 set workmode wlan (for FAT AP)....7036
13.1.70 short-preamble (for FAT AP)....7037
13.1.71 smart-carrier-sense enable....7038
13.1.72 ssid (for FAT AP)....7039
13.1.73 ssid-hide (for FAT AP)....7040
13.1.74 ssid-catch (for FAT AP)....7041
13.1.75 traffic-profile (service set view) (for FAT AP)....7043
13.1.76 wlan (for FAT AP)....7044
13.1.77 wlan global country-code....7045
13.1.78 wlan record log timer....7049
13.1.79 wlan-bss (service set view)....7050
13.1.80 wmm-profile (WLAN view) (for FAT AP)....7052
13.1.81 wmm-profile (radio profile view) (for FAT AP)....7054
13.2 WLAN QoS Configuration Commands....7055
13.2.1 8021p (for FAT AP)....7056
13.2.2 8021p-map-up (for FAT AP)....7058
13.2.3 display traffic-profile (for FAT AP)....7061
13.2.4 display wmm-profile (for FAT AP)....7064
13.2.5 rate-limit vap (for FAT AP)....7069
13.2.6 rate-limit client (for FAT AP)....7070
13.2.7 traffic-profile (WLAN view) (for FAT AP)....7071
13.2.8 wmm edca ap (for FAT AP)....7073
13.2.9 wmm edca client (for FAT AP)....7076
13.2.10 wmm enable (for FAT AP)....7078
13.2.11 wmm mandatory enable (for FAT AP)....7079
13.3 WLAN Security Configuration Commands....7080
13.3.1 attack detection enable (for FAT AP)....7080
13.3.2 attack detection flood (for FAT AP)....7082
13.3.3 attack detection psk (for FAT AP)....7084
13.3.4 attack detection quiet-time (for FAT AP)....7085
13.3.5 display security-profile (for FAT AP)....7086
13.3.6 display sta-access-mode (for FAT AP)....7090
13.3.7 display sta-blacklist (for FAT AP)....7091
13.3.8 display sta-whitelist (for FAT AP)....7092
13.3.9 display wapi certificate (for FAT AP)....7093

13.3.10 display wlan ids attack-detected (for FAT AP) 7095
13.3.11 display wlan ids attack-detected statistics (for FAT AP) 7098
13.3.12 display wlan ids attack-history (for FAT AP) 7101
13.3.13 display wlan ids dynamic-blacklist (for FAT AP) 7103
13.3.14 dynamic-blacklist aging-duration (for FAT AP) 7105
13.3.15 dynamic-blacklist enable (for FAT AP) 7106
13.3.16 reset wlan ids attack-detected (for FAT AP) 7108
13.3.17 reset wlan ids attack-detected statistics (for FAT AP) 7109
13.3.18 reset wlan ids attack-history (for FAT AP) 7110
13.3.19 reset wlan ids dynamic-blacklist (for FAT AP) 7112
13.3.20 security-policy (for FAT AP) 7113
13.3.21 security-profile (for FAT AP) 7114
13.3.22 sta-access-mode (for FAT AP) 7116
13.3.23 sta-blacklist (for FAT AP) 7117
13.3.24 sta-whitelist (for FAT AP) 7118
13.3.25 user-isolate (for FAT AP) 7119
13.3.26 wapi asu (for FAT AP) 7120
13.3.27 wapi authentication-method (for FAT AP) 7121
13.3.28 wapi bk (for FAT AP) 7123
13.3.29 wapi import certificate (for FAT AP) 7124
13.3.30 wapi cert-retrans-count (for FAT AP) 7126
13.3.31 wapi msk (for FAT AP) 7127
13.3.32 wapi import private-key (for FAT AP) 7128
13.3.33 wapi sa-timeout (for FAT AP) 7130
13.3.34 wapi key-update (for FAT AP) 7131
13.3.35 wapi usk (for FAT AP) 7132
13.3.36 wep authentication-method (for FAT AP) 7134
13.3.37 wep default-key (for FAT AP) 7135
13.3.38 wep key (for FAT AP) 7136
13.3.39 authentication-method dot1x encryption-method (for FAT AP) 7139
13.3.40 authentication-method psk encryption-method (for FAT AP) 7140
13.4 WLAN Radio Resource Management Configuration Commands 7142
13.4.1 calibrate channel-set (for FAT AP) 7142
13.4.2 calibrate sensitivity (for FAT AP) 7144
13.4.3 calibrate enable { auto | manual | schedule time } (for FAT AP) 7145
13.4.4 calibrate manual startup (for FAT AP) 7147
13.4.5 display calibrate channel-set (for FAT AP) 7148
13.4.6 display neighbor (for FAT AP) 7149
13.4.7 display statistics calibrate (for FAT AP) 7150
13.4.8 reset statistics calibrate (Radio interface view) 7151

14 WLAN-AC Commands 7153

14.1 WLAN Service Configuration Commands 7153

14.1.1 ac sysnetid 7153
14.1.2 access-user syslog-restrain enable 7154
14.1.3 access-user syslog-restrain period 7155
14.1.4 active-dull-client enable 7156
14.1.5 alarm-restriction disable 7157
14.1.6 alarm-restriction period 7158
14.1.7 antenna-gain 7159
14.1.8 anti-attack broadcast-flood blacklist enable 7161
14.1.9 anti-attack broadcast-flood disable 7162
14.1.10 anti-attack broadcast-flood sta-rate-threshold 7163
14.1.11 ap auth-mode 7164
14.1.12 ap blacklist 7165
14.1.13 ap data-collection enable 7167
14.1.14 ap data-collection interval 7168
14.1.15 ap lldp enable 7169
14.1.16 ap manufacturer-config 7170
14.1.17 ap modify 7171
14.1.18 ap update ftp-server 7172
14.1.19 ap update ftp-server max-connect-number 7174
14.1.20 ap update load 7176
14.1.21 ap update mode 7177
14.1.22 ap update multi-load 7178
14.1.23 ap update multi-reset 7180
14.1.24 ap update reset 7182
14.1.25 ap update sftp-server 7183
14.1.26 ap update sftp-server max-connect-number 7185
14.1.27 ap update update-filename 7187
14.1.28 ap username 7188
14.1.29 ap whitelist 7190
14.1.30 ap-confirm 7192
14.1.31 ap-group 7193
14.1.32 ap-group (AP view) 7194
14.1.33 ap-id 7195
14.1.34 ap-mac 7197
14.1.35 ap-name 7199
14.1.36 ap-name (AP view) 7200
14.1.37 ap-ping 7201
14.1.38 ap-regroup 7202
14.1.39 ap-rename 7204
14.1.40 ap-reset 7205
14.1.41 ap-system-profile (WLAN view) 7206
14.1.42 ap-system-profile (AP group view and AP view) 7208

14.1.43 association-timeout ... 7209
14.1.44 beacon-2g-rate ... 7210
14.1.45 beacon-5g-rate ... 7212
14.1.46 beacon-interval ... 7213
14.1.47 capwap control-link-priority ... 7214
14.1.48 capwap dtls control-link encrypt ... 7216
14.1.49 capwap dtls psk ... 7217
14.1.50 capwap dtls psk-mandatory-match enable ... 7219
14.1.51 capwap echo ... 7220
14.1.52 capwap ipv6 enable ... 7222
14.1.53 capwap message-integrity psk ... 7223
14.1.54 capwap message-integrity psk-mandatory-match enable ... 7224
14.1.55 capwap sensitive-info psk ... 7225
14.1.56 capwap source interface ... 7227
14.1.57 channel ... 7228
14.1.58 channel-switch announcement disable ... 7230
14.1.59 commit (WLAN view) ... 7231
14.1.60 console disable ... 7232
14.1.61 country-code ... 7233
14.1.62 coverage distance ... 7238
14.1.63 cpu-usage threshold ... 7240
14.1.64 crc-alarm enable ... 7241
14.1.65 deny-broadcast-probe enable ... 7242
14.1.66 description (AP wired port profile view) ... 7243
14.1.67 dhcp trust port ... 7244
14.1.68 dai enable (AP wired port profile view) ... 7245
14.1.69 display ac global configuration ... 7246
14.1.70 display ap ... 7247
14.1.71 display ap around-ssid-list ... 7252
14.1.72 display ap asyn-message err-info ... 7253
14.1.73 display ap blacklist ... 7254
14.1.74 display ap config-info ... 7256
14.1.75 display ap configurable channel ... 7261
14.1.76 display ap elabel ... 7263
14.1.77 display ap global configuration ... 7265
14.1.78 display ap lldp neighbor ... 7266
14.1.79 display ap neighbor ... 7271
14.1.80 display ap offline-record ... 7273
14.1.81 display ap online-fail-record ... 7274
14.1.82 display ap optical-info ... 7276
14.1.83 display ap performance statistics ... 7280
14.1.84 display ap port ... 7282

14.1.85 display ap run-info 7284
14.1.86 display ap service-config acl 7287
14.1.87 display ap sta-signal strength 7288
14.1.88 display ap traffic statistics wireless 7289
14.1.89 display ap unauthorized record 7294
14.1.90 display ap uncontrol all 7295
14.1.91 display ap update configuration 7297
14.1.92 display ap update status 7299
14.1.93 display ap username 7304
14.1.94 display ap version 7305
14.1.95 display ap whitelist 7307
14.1.96 display ap wired-port 7309
14.1.97 display ap-group 7312
14.1.98 display ap-system-profile 7316
14.1.99 display ap-type 7322
14.1.100 display capwap configuration 7325
14.1.101 display channel switch-record 7327
14.1.102 display mac-address ap-all 7329
14.1.103 display mac-address { ap-id | ap-name } 7331
14.1.104 display port-link-profile 7332
14.1.105 display radio 7335
14.1.106 display radio-2g-profile 7337
14.1.107 display radio-5g-profile 7342
14.1.108 display references ap-system-profile 7349
14.1.109 display references port-link-profile 7350
14.1.110 display references radio-2g-profile 7351
14.1.111 display references radio-5g-profile 7352
14.1.112 display references regulatory-domain-profile 7353
14.1.113 display references ssid-profile 7354
14.1.114 display references traffic-profile 7355
14.1.115 display references vap-profile 7356
14.1.116 display references wired-port-profile 7357
14.1.117 display regulatory-domain-profile 7358
14.1.118 display ssid-profile 7360
14.1.119 display station 7364
14.1.120 display station assoc-info ap-offline-record 7369
14.1.121 display station online-fail-record 7371
14.1.122 display station offline-record 7374
14.1.123 display station statistics 7376
14.1.124 display traffic-profile 7381
14.1.125 display vap 7386
14.1.126 display vap create-fail-record 7388

14.1.127 display vap-profile....7390
14.1.128 display wired-port-profile....7393
14.1.129 display wlan config-errors....7396
14.1.130 display workmode wlan....7397
14.1.131 dot11a basic-rate....7398
14.1.132 dot11a supported-rate....7400
14.1.133 dot11bg basic-rate....7402
14.1.134 dot11bg supported-rate....7404
14.1.135 dtim-interval....7406
14.1.136 eapol-response dest-address transform-condition....7407
14.1.137 eapol-response dest-address transform-to....7408
14.1.138 eapol-start dest-address transform-condition....7410
14.1.139 eapol-start dest-address transform-to....7411
14.1.140 eirp....7413
14.1.141 eth-trunk (AP wired port profile view)....7414
14.1.142 forward-mode....7415
14.1.143 frequency....7416
14.1.144 guard-interval-mode....7418
14.1.145 high-temperature threshold....7419
14.1.146 ht a-mpdu disable....7420
14.1.147 ht a-mpdu max-length-exponent....7421
14.1.148 igmp-snooping enable (traffic profile view)....7423
14.1.149 igmp-snooping report-suppress....7424
14.1.150 ip source check user-bind enable....7425
14.1.151 ipsg enable (AP wired port profile view)....7426
14.1.152 keep-service enable....7428
14.1.153 keep-service enable allow new-access....7429
14.1.154 learn-client-address dhcp-strict....7430
14.1.155 learn-client-address disable....7431
14.1.156 learn-client-address enable (AP wired port profile view)....7432
14.1.157 led off....7433
14.1.158 legacy-station disable....7434
14.1.159 lldp admin-status....7435
14.1.160 lldp enable....7436
14.1.161 lldp message-transmission delay (AP system profile view)....7438
14.1.162 lldp message-transmission hold-multiplier (AP system profile view)....7440
14.1.163 lldp message-transmission interval (AP system profile view)....7441
14.1.164 lldp report-interval....7443
14.1.165 lldp restart-delay....7444
14.1.166 lldp tlv-enable (AP wired port link profile view)....7445
14.1.167 log-server....7447
14.1.168 low-temperature threshold....7448

14.1.169 management-vlan....7450
14.1.170 max-sta-number (SSID profile view)....7451
14.1.171 memory-usage threshold....7452
14.1.172 mtu....7453
14.1.173 multicast-rate....7455
14.1.174 port-link-profile (WLAN view)....7457
14.1.175 port-link-profile (AP wired port profile view)....7458
14.1.176 priority-map downstream dscp....7460
14.1.177 priority-map downstream trust....7462
14.1.178 priority-map tunnel-upstream dot11e....7463
14.1.179 priority-map tunnel-upstream dscp....7465
14.1.180 priority-map tunnel-upstream trust....7466
14.1.181 probe-response-retry....7467
14.1.182 radio....7469
14.1.183 radio disable....7470
14.1.184 radio-2g-profile (WLAN view)....7471
14.1.185 radio-2g-profile....7472
14.1.186 radio-5g-profile (WLAN view)....7474
14.1.187 radio-5g-profile....7475
14.1.188 radio-type (2G radio profile view)....7476
14.1.189 radio-type (5G radio profile view)....7478
14.1.190 rate-limit....7479
14.1.191 reach-max-sta hide-ssid disable....7481
14.1.192 regulatory-domain-profile (WLAN view)....7482
14.1.193 regulatory-domain-profile....7483
14.1.194 report-disassoc-request disable....7484
14.1.195 reset ap offline-record....7485
14.1.196 reset ap online-fail-record....7486
14.1.197 reset ap unauthorized record....7487
14.1.198 reset channel switch-record....7488
14.1.199 reset mac-address { ap-id | ap-name }....7489
14.1.200 reset station assoc-info ap-offline-record....7490
14.1.201 reset station offline-record....7491
14.1.202 reset station online-fail-record....7492
14.1.203 reset station statistics....7493
14.1.204 reset statistics....7494
14.1.205 rf-ping....7495
14.1.206 rts-cts-mode....7496
14.1.207 rts-cts-threshold....7497
14.1.208 service-vlan....7499
14.1.209 set workmode wlan....7500
14.1.210 sftp server disable....7501

14.1.211 short-preamble disable....7502
14.1.212 shutdown (AP wired port link profile view)....7503
14.1.213 snmp-agent trap enable feature-name wlan....7504
14.1.214 ssid....7505
14.1.215 ssid-hide enable....7506
14.1.216 ssid-profile (WLAN view)....7507
14.1.217 ssid-profile (VAP profile view)....7508
14.1.218 stelnet server disable....7510
14.1.219 telnet enable....7510
14.1.220 temporary-management enable (AP system profile view)....7511
14.1.221 temporary-management enable (VAP profile view)....7514
14.1.222 traffic-optimize (AP wired port profile view)....7515
14.1.223 traffic-optimize broadcast-suppression....7517
14.1.224 traffic-optimize multicast-suppression....7518
14.1.225 traffic-optimize multicast-unicast enable....7519
14.1.226 traffic-optimize sta-bridge-forward disable....7520
14.1.227 traffic-optimize unicast-suppression....7521
14.1.228 traffic-profile (VAP profile view)....7522
14.1.229 traffic-profile (WLAN view)....7523
14.1.230 type (VAP profile view)....7524
14.1.231 undo ap....7526
14.1.232 utmost-power disable....7527
14.1.233 vap-profile (WLAN view)....7528
14.1.234 vap-profile....7530
14.1.235 vht a-mpdu max-length-exponent....7531
14.1.236 vht a-msdu enable....7533
14.1.237 vht a-msdu max-frame-num....7534
14.1.238 vht mcs-map....7536
14.1.239 wifi-light....7537
14.1.240 wired-port-profile (WLAN view)....7539
14.1.241 wired-port-profile (AP group view and view)....7540
14.1.242 wlan....7542
14.1.243 wmm disable....7542
14.1.244 wmm edca-ap....7543
14.1.245 wmm edca-client (SSID profile view)....7546
14.1.246 wmm mandatory enable....7548
14.2 WLAN Radio Resource Management Configuration Commands....7549
14.2.1 amc-policy....7549
14.2.2 air-scan-profile....7550
14.2.3 air-scan-profile (radio profile view)....7552
14.2.4 band-steer balance gap-threshold....7553
14.2.5 band-steer balance start-threshold....7554

14.2.6 band-steer client-band-expire 7556
14.2.7 band-steer deny-threshold 7557
14.2.8 band-steer disable 7558
14.2.9 calibrate auto-channel-select disable 7560
14.2.10 calibrate auto-txpower-select disable 7561
14.2.11 calibrate enable { auto | manual | schedule time } 7562
14.2.12 calibrate error-rate-threshold 7564
14.2.13 calibrate manual startup 7565
14.2.14 calibrate sensitivity 7565
14.2.15 dca-channel bandwidth 7567
14.2.16 dca-channel channel-set 7568
14.2.17 display air-scan-profile 7570
14.2.18 display references air-scan-profile 7572
14.2.19 display references rrm-profile 7573
14.2.20 display rrm-profile 7574
14.2.21 display sta-load-balance static-group 7577
14.2.22 display station load-balance sta-mac 7580
14.2.23 display station rssi-rejected statistics 7581
14.2.24 display wlan calibrate channel-set 7582
14.2.25 display wlan calibrate statistics 7584
14.2.26 dynamic-edca enable 7585
14.2.27 gap-threshold 7586
14.2.28 interference adjacent-channel threshold 7588
14.2.29 interference co-channel threshold 7589
14.2.30 interference detect-enable 7590
14.2.31 interference station threshold 7591
14.2.32 member (static load balancing group view) 7592
14.2.33 power auto-adjust enable 7594
14.2.34 reset wlan calibrate statistics 7595
14.2.35 rrm-profile (WLAN view) 7596
14.2.36 rrm-profile (radio profile view) 7597
14.2.37 scan-channel-set 7598
14.2.38 scan-interval 7600
14.2.39 scan-period 7601
14.2.40 sta-load-balance dynamic enable 7602
14.2.41 sta-load-balance dynamic gap-threshold 7603
14.2.42 sta-load-balance dynamic start-threshold 7604
14.2.43 sta-load-balance static-group 7605
14.2.44 start-threshold 7606
14.3 WLAN Roaming Commands 7607
14.3.1 display station roam-track 7608
14.4 WLAN Security Configuration Commands 7609

14.4.1 brute-force-detect interval....7609
14.4.2 brute-force-detect quiet-time....7611
14.4.3 brute-force-detect threshold....7612
14.4.4 device report-interval....7614
14.4.5 device synchronization-interval....7615
14.4.6 display references wids-profile....7616
14.4.7 display references wids-spoof-profile....7617
14.4.8 display wids-profile....7618
14.4.9 display wids-spoof-profile....7621
14.4.10 display references security-profile....7623
14.4.11 display references sta-blacklist-profile....7624
14.4.12 display references sta-whitelist-profile....7625
14.4.13 display security-profile....7626
14.4.14 display sta-blacklist-profile....7631
14.4.15 display station dynamic-blacklist....7632
14.4.16 display sta-whitelist-profile....7634
14.4.17 display wlan ids attack-detected....7636
14.4.18 display wlan ids attack-detected statistics....7639
14.4.19 display wlan ids attack-history....7642
14.4.20 display wlan ids dynamic-blacklist....7644
14.4.21 display wlan wapi certificate....7647
14.4.22 dynamic-blacklist aging-time....7648
14.4.23 dynamic-blacklist enable....7649
14.4.24 flood-detect interval....7650
14.4.25 flood-detect quiet-time....7652
14.4.26 flood-detect threshold....7653
14.4.27 reset wlan ids attack-detected....7654
14.4.28 reset wlan ids attack-detected statistics....7656
14.4.29 reset wlan ids attack-history....7657
14.4.30 reset wlan ids dynamic-blacklist....7658
14.4.31 security dot1x....7659
14.4.32 security psk....7661
14.4.33 security wapi....7663
14.4.34 security wep....7665
14.4.35 security-profile....7667
14.4.36 security-profile (VAP profile view)....7668
14.4.37 spoof-detect quiet-time....7669
14.4.38 sta-access-mode....7670
14.4.39 sta-blacklist-profile....7671
14.4.40 sta-mac....7673
14.4.41 sta-whitelist-profile....7674
14.4.42 wapi asu....7675

14.4.43 wapi bk....7676
14.4.44 wapi cert-retrans-count....7677
14.4.45 wapi import certificate....7678
14.4.46 wapi import private-key....7680
14.4.47 wapi key-update....7682
14.4.48 wapi msk....7683
14.4.49 wapi sa-timeout....7684
14.4.50 wapi source interface....7685
14.4.51 wapi usk....7687
14.4.52 weak-iv-detect quiet-time....7688
14.4.53 wep default-key....7689
14.4.54 wep key....7690
14.4.55 wids attack detect enable....7693
14.4.56 wids-profile (WLAN view)....7695
14.4.57 wids-profile (AP group view and AP view)....7697
14.4.58 wids-spoof-profile (WLAN view)....7698
14.4.59 wids-spoof-profile (WIDS profile view)....7699
14.4.60 wpa ptk-update enable....7700
14.4.61 wpa ptk-update ptk-update-interval....7701
14.5 WLAN WDS Configuration Commands....7702
14.5.1 dhcp trust port (WDS profile view)....7702
14.5.2 display references wds-profile....7703
14.5.3 display references wds-whitelist-profile....7705
14.5.4 display wds-profile....7706
14.5.5 display wds-whitelist-profile....7709
14.5.6 display wds vap....7710
14.5.7 display wlan wds link....7712
14.5.8 mode (AP wired port profile view)....7714
14.5.9 peer-ap mac (WDS whitelist profile view)....7716
14.5.10 priority-map dscp (WDS profile view)....7717
14.5.11 priority-map trust (WDS profile view)....7719
14.5.12 security-profile (WDS profile view)....7720
14.5.13 user-isolate (AP wired port profile view)....7721
14.5.14 user-isolate (traffic profile view)....7722
14.5.15 vlan pvid (AP wired port profile view)....7723
14.5.16 vlan tagged (WDS profile view)....7725
14.5.17 vlan (AP wired port profile view)....7727
14.5.18 wds-mode....7729
14.5.19 wds-name....7730
14.5.20 wds-profile....7731
14.5.21 wds-profile radio....7733
14.5.22 wds-profile (AP group radio view or AP radio view)....7734

14.5.23 wds-whitelist-profile 7735
14.5.24 wds-whitelist-profile (AP group radio view or AP radio view) 7737
14.6 WLAN Reliability Commands 7738
14.6.1 ac protect cold-backup kickoff-station 7738
14.6.2 ac protect enable 7739
14.6.3 ac protect priority 7740
14.6.4 ac protect protect-ac 7741
14.6.5 ac protect restore disable 7742
14.6.6 display ac protect 7743
14.6.7 priority 7745
14.6.8 protect-ac 7747

15 Energy Efficiency Commands 7749

15.1 authentication mode 7751
15.2 authentication passwd 7752
15.3 authentication zigbee link-key 7753
15.4 display channel-type zigbee status 7754
15.5 display m2m-gateway configuration 7757
15.6 display m2m-gateway long-latitude 7759
15.7 display m2m-gateway statistics 7760
15.8 display m2m-gateway status 7762
15.9 display m2m-gateway task 7766
15.10 display m2m-gateway task list group-task 7775
15.11 display m2m-gateway task list optimal-task 7776
15.12 display m2m-gateway task list statistics 7777
15.13 display m2m-gateway task schedule 7779
15.14 display m2m-gateway tsvr-server status 7781
15.15 display m2m-gateway timer-join-network 7783
15.16 display m2m-gateway upgrade current 7785
15.17 display m2m-gateway upstream communication style 7786
15.18 display m2m-gateway upstream statistics 7787
15.19 display m2m-gateway whitelist 7789
15.20 display firmware process 7791
15.21 display zigbee link-key-using 7793
15.22 encrypt mode disable 7794
15.23 encrypt type 7795
15.24 firmware upgrade channel-type zigbee remote 7795
15.25 firmware upgrade channel-type zigbee local 7797
15.26 firmware upgrade channel-type zigbee erase flash 7798
15.27 firmware upgrade stop 7800
15.28 hes-bakserver 7801
15.29 hes-server 7802
15.30 longitude-latitude 7804

15.31 m2m-gateway 7805
15.32 reset m2m-gateway offline-device 7806
15.33 reset m2m-gateway statistics 7806
15.34 restore factory configuration 7807
15.35 task delete 7810
15.36 task update task-name 7811
15.37 tsvr-server 7812
15.38 upstream-cache cache-size wait-time 7814
15.39 upstream-cache mode 7815
15.40 upstream statistics threshold 7816
15.41 zigbee-network dismiss 7817
15.42 zigbee-network get-rssi 7818
15.43 zigbee-network permit-join 7820
15.44 zigbee-network permit-join whitelist 7821
15.45 zigbee-network status refresh 7822
15.46 zigbee-network timer-join-network 7823
15.47 zigbee-network timer-join-network enable 7825

16 Voice Commands 7827

16.1 Voice Configuration Commands 7827
16.1.1 Basic Voice Configuration Commands 7827
16.1.1.1 debugging voice logserver 7827
16.1.1.2 debugging voice module-name cmd 7828
16.1.1.3 debugging voice module-name debug-level-value 7831
16.1.1.4 display voice configuration 7834
16.1.1.5 display voice debugging 7835
16.1.1.6 display voice diagnostic-information 7837
16.1.1.7 display voice error 7838
16.1.1.8 display voice media-port 7839
16.1.1.9 display voice mix-info 7840
16.1.1.10 display voice online-info 7841
16.1.1.11 display voice run-stat 7844
16.1.1.12 display voice service-mode 7846
16.1.1.13 display voice sip-reg-count-per-second 7847
16.1.1.14 display voice trace 7848
16.1.1.15 display voice upgrade-info 7849
16.1.1.16 display voice voip-address 7849
16.1.1.17 eid-para signalling (PBX user view) 7851
16.1.1.18 flash-hook lower 7852
16.1.1.19 flash-hook upper 7853
16.1.1.20 load voice-package 7854
16.1.1.21 media-port 7856
16.1.1.22 mwi-mode 7857

16.1.1.23 pcm....7858
16.1.1.24 park-feed....7859
16.1.1.25 save tracelog....7860
16.1.1.26 service-mode....7860
16.1.1.27 sip-reg-count-per-second....7862
16.1.1.28 startup voice-package....7862
16.1.1.29 voice....7864
16.1.1.30 voip-address media....7865
16.1.1.31 voip-address signalling....7866
16.1.1.32 voip-vpn-instance....7867
16.1.1.33 undo logserver....7868
16.1.2 Clip Configuration Commands....7869
16.1.2.1 clip offhook ack-fsk-interval....7869
16.1.2.2 clip offhook dtas-ack-interval....7870
16.1.2.3 clip offhook dtas-duration....7871
16.1.2.4 clip offhook dtas-level....7872
16.1.2.5 clip offhook fsk-level....7873
16.1.2.6 clip offhook mark-signal-bit....7874
16.1.2.7 clip onhook channel-seize-bit....7875
16.1.2.8 clip onhook dtas-duration....7876
16.1.2.9 clip onhook dtas-fsk-interval....7877
16.1.2.10 clip onhook dtas-level....7878
16.1.2.11 clip onhook fsk-level....7879
16.1.2.12 clip onhook mark-signal-bit....7880
16.1.2.13 display voice clip....7881
16.1.3 Ring Configuration Commands....7883
16.1.3.1 display voice user-defined-ring....7883
16.1.3.2 ring frequency....7884
16.1.3.3 ring voltage....7885
16.1.3.4 stop-initial-ring enable....7886
16.1.3.5 user-defined-ring....7887
16.1.4 Upward-bandwidth Configuration Commands....7889
16.1.4.1 display voice media-bandwidth-control....7889
16.1.4.2 media-bandwidth-control enable....7890
16.1.4.3 media-bandwidth-control max-bandwidth....7891
16.1.5 Sip Stack Configuration Commands....7892
16.1.5.1 display voice sip....7892
16.1.5.2 entity-based-sessions-timer....7894
16.1.5.3 field-header max-forwards....7895
16.1.5.4 field-header organization....7896
16.1.5.5 field-header server....7897
16.1.5.6 field-header user-agent....7898

16.1.5.7 header-folding....7899
16.1.5.8 min-se....7900
16.1.5.9 session-progress....7901
16.1.5.10 session-rel-progress....7902
16.1.5.11 sip....7903
16.1.5.12 to-header-check-flag....7903
16.1.5.13 t1....7904
16.1.5.14 t2....7905
16.1.5.15 t4....7906
16.1.5.16 td....7907
16.1.6 Dsp Configuration Commands....7908
16.1.6.1 display voice dsp state....7908
16.1.6.2 display voice dsp statistic....7911
16.1.6.3 display voice dsp-attribute....7912
16.1.6.4 display voice tone....7916
16.1.6.5 dsp....7917
16.1.6.6 dsp-attribute....7918
16.1.6.7 dtmf-twist-value(dsp-attribute view)....7918
16.1.6.8 echo....7919
16.1.6.9 fax ecm....7920
16.1.6.10 fax redundancy-t30....7921
16.1.6.11 fax redundancy-t4....7922
16.1.6.12 fax training-mode....7923
16.1.6.13 fax training-rate....7924
16.1.6.14 fax v8negotiate....7925
16.1.6.15 jitter-buffer adapt-jb-threshold....7926
16.1.6.16 jitter-buffer init-adapt-jb....7927
16.1.6.17 jitter-buffer init-fixed-jb....7928
16.1.6.18 jitter-buffer max-adapt-jb....7929
16.1.6.19 jitter-buffer max-fixed-jb....7930
16.1.6.20 jitter-buffer min-adapt-jb....7932
16.1.6.21 jitter-buffer min-fixed-jb....7933
16.1.6.22 loop-back (DSP resource management view)....7934
16.1.6.23 nte2833-volume deviation....7936
16.1.6.24 nte2833-volume mode....7937
16.1.6.25 payload-type clear-mode....7939
16.1.6.26 payload-type g726-16k....7940
16.1.6.27 payload-type g726-24k....7941
16.1.6.28 payload-type g726-32k....7942
16.1.6.29 payload-type g726-40k....7943
16.1.6.30 payload-type nte....7944
16.1.6.31 payload-type redundancy....7945

16.1.6.32 payload-type vbd....7946
16.1.6.33 plc....7947
16.1.6.34 prohibit....7948
16.1.6.35 resource-threshold....7949
16.1.6.36 resource-threshold mode....7950
16.1.6.37 rtcp rtcp-interval....7951
16.1.6.38 rtcp rtcpxr....7952
16.1.6.39 rtcp sev-degrade-threshold....7953
16.1.6.40 rtcp vqm....7954
16.1.6.41 silence....7954
16.1.6.42 tone (Voice View)....7955
16.1.6.43 tone-frequency....7956
16.1.6.44 tone-cadence....7958
16.1.6.45 tone-detect-info....7959
16.1.6.46 traffic-policy (DSP attribute view)....7961
16.1.7 Voice Diagnose Commands....7963
16.1.7.1 clip port....7963
16.1.7.2 debugging voice-adapt....7965
16.1.7.3 diagnose....7966
16.1.7.4 digit-trace....7966
16.1.7.5 display fe slot fe-id table port-map dsp-port base-port....7967
16.1.7.6 display fe slot fe-id table voice-mr dest-ip port protocol....7968
16.1.7.7 display fe slot fe-id table voice-signal....7969
16.1.7.8 display pots loop-line-threshold....7971
16.1.7.9 display pots subcard-loopline-adjust....7972
16.1.7.10 display voice device state....7973
16.1.7.11 display voice statistics module at0....7973
16.1.7.12 display voice statistics module h323....7975
16.1.7.13 display voice statistics module pots....7979
16.1.7.14 display voice statistics module q931....7981
16.1.7.15 display voice statistics module r2....7985
16.1.7.16 display voice statistics module sip....7987
16.1.7.17 pots circuit-test....7989
16.1.7.18 pots loop-line-test....7991
16.1.7.19 pots loop-line-threshold....7992
16.1.7.20 pots path-test....7994
16.1.7.21 pots subcard-loopline-adjust get....7996
16.1.7.22 pots subcard-loopline-adjust restore....7997
16.1.7.23 pots subcard-loopline-adjust set....7998
16.1.7.24 reset voice statistics module....7999
16.1.7.25 ts6em....8000
16.2 Voice interface Commands....8001

16.2.1 Voice interface Configuration Commands....8001
16.2.1.1 access-mode....8001
16.2.1.2 access-mode (BRA Interface View)....8002
16.2.1.3 alarm....8003
16.2.1.4 crc4....8004
16.2.1.5 crc (VE1 interface view)....8005
16.2.1.6 crc-alarm-threshold....8006
16.2.1.7 display voice port bra....8008
16.2.1.8 display voice port fxo....8009
16.2.1.9 display voice port fxs....8011
16.2.1.10 display voice port ve1....8013
16.2.1.11 electric current....8016
16.2.1.12 electric impedance....8017
16.2.1.13 electric receive-gain....8019
16.2.1.14 electric send-gain....8021
16.2.1.15 feed....8025
16.2.1.16 gain....8026
16.2.1.17 impedance (FXO interface view)....8031
16.2.1.18 impedance (VE1 interface view)....8033
16.2.1.19 invert....8034
16.2.1.20 itf(VE1 interface view)....8035
16.2.1.21 l2-monitor....8036
16.2.1.22 l2-monitor (VE1 interface view)....8037
16.2.1.23 line-lock....8038
16.2.1.24 loop....8039
16.2.1.25 nlp-mode....8040
16.2.1.26 pcm-alarm....8041
16.2.1.27 port bra....8043
16.2.1.28 port fxo....8044
16.2.1.29 port fxs....8045
16.2.1.30 port ve1....8046
16.2.1.31 remote-power....8047
16.2.1.32 reset line-fault....8048
16.2.1.33 reverse-pole-pulse level....8049
16.2.1.34 ring....8050
16.2.1.35 sa....8052
16.2.1.36 shutdown....8053
16.2.1.37 signal(VE1 interface view)....8054
16.2.1.38 work-mode....8055
16.3 Voice Configuration Commands....8056
16.3.1 Basic Voice Configuration Commands....8056
16.3.1.1 debugging voice logserver....8056

16.3.1.2 debugging voice module-name cmd ... 8057
16.3.1.3 debugging voice module-name debug-level-value ... 8061
16.3.1.4 display voice configuration ... 8064
16.3.1.5 display voice debugging ... 8065
16.3.1.6 display voice diagnostic-information ... 8067
16.3.1.7 display voice error ... 8068
16.3.1.8 display voice media-port ... 8069
16.3.1.9 display voice mix-info ... 8070
16.3.1.10 display voice online-info ... 8071
16.3.1.11 display voice run-stat ... 8074
16.3.1.12 display voice service-mode ... 8076
16.3.1.13 display voice sip-reg-count-per-second ... 8077
16.3.1.14 display voice trace ... 8078
16.3.1.15 display voice upgrade-info ... 8079
16.3.1.16 display voice voip-address ... 8079
16.3.1.17 eid-para signalling (PBX user view) ... 8081
16.3.1.18 flash-hook lower ... 8082
16.3.1.19 flash-hook upper ... 8083
16.3.1.20 load voice-package ... 8084
16.3.1.21 media-port ... 8086
16.3.1.22 mwi-mode ... 8087
16.3.1.23 pcm ... 8088
16.3.1.24 park-feed ... 8089
16.3.1.25 save tracelog ... 8090
16.3.1.26 service-mode ... 8090
16.3.1.27 sip-reg-count-per-second ... 8092
16.3.1.28 startup voice-package ... 8092
16.3.1.29 voice ... 8094
16.3.1.30 voip-address media ... 8095
16.3.1.31 voip-address signalling ... 8096
16.3.1.32 voip-vpn-instance ... 8097
16.3.1.33 undo logserver ... 8098
16.3.2 Clip Configuration Commands ... 8099
16.3.2.1 clip offhook ack-fsk-interval ... 8099
16.3.2.2 clip offhook dtas-ack-interval ... 8100
16.3.2.3 clip offhook dtas-duration ... 8101
16.3.2.4 clip offhook dtas-level ... 8102
16.3.2.5 clip offhook fsk-level ... 8103
16.3.2.6 clip offhook mark-signal-bit ... 8104
16.3.2.7 clip onhook channel-seize-bit ... 8105
16.3.2.8 clip onhook dtas-duration ... 8106
16.3.2.9 clip onhook dtas-fsk-interval ... 8107

16.3.2.10 clip onhook dtas-level....8108
16.3.2.11 clip onhook fsk-level....8109
16.3.2.12 clip onhook mark-signal-bit....8110
16.3.2.13 display voice clip....8111
16.3.3 Ring Configuration Commands....8113
16.3.3.1 display voice user-defined-ring....8113
16.3.3.2 ring frequency....8114
16.3.3.3 ring voltage....8115
16.3.3.4 stop-initial-ring enable....8116
16.3.3.5 user-defined-ring....8117
16.3.4 Upward-bandwidth Configuration Commands....8119
16.3.4.1 display voice media-bandwidth-control....8119
16.3.4.2 media-bandwidth-control enable....8120
16.3.4.3 media-bandwidth-control max-bandwidth....8121
16.3.5 Sip Stack Configuration Commands....8122
16.3.5.1 display voice sip....8122
16.3.5.2 entity-based-sessions-timer....8124
16.3.5.3 field-header max-forwards....8125
16.3.5.4 field-header organization....8126
16.3.5.5 field-header server....8127
16.3.5.6 field-header user-agent....8128
16.3.5.7 header-folding....8129
16.3.5.8 min-se....8130
16.3.5.9 session-progress....8131
16.3.5.10 session-rel-progress....8132
16.3.5.11 sip....8133
16.3.5.12 to-header-check-flag....8133
16.3.5.13 t1....8134
16.3.5.14 t2....8135
16.3.5.15 t4....8136
16.3.5.16 td....8137
16.3.6 Dsp Configuration Commands....8138
16.3.6.1 display voice dsp state....8138
16.3.6.2 display voice dsp statistic....8141
16.3.6.3 display voice dsp-attribute....8142
16.3.6.4 display voice tone....8146
16.3.6.5 dsp....8147
16.3.6.6 dsp-attribute....8148
16.3.6.7 dtmf-twist-value(dsp-attribute view)....8148
16.3.6.8 echo....8149
16.3.6.9 fax ecm....8150
16.3.6.10 fax redundancy-t30....8151

16.3.6.11 fax redundancy-t4 8152
16.3.6.12 fax training-mode 8153
16.3.6.13 fax training-rate 8154
16.3.6.14 fax v8negotiate 8155
16.3.6.15 jitter-buffer adapt-jb-threshold 8156
16.3.6.16 jitter-buffer init-adapt-jb 8157
16.3.6.17 jitter-buffer init-fixed-jb 8158
16.3.6.18 jitter-buffer max-adapt-jb 8159
16.3.6.19 jitter-buffer max-fixed-jb 8160
16.3.6.20 jitter-buffer min-adapt-jb 8162
16.3.6.21 jitter-buffer min-fixed-jb 8163
16.3.6.22 loop-back (DSP resource management view) 8164
16.3.6.23 nte2833-volume deviation 8166
16.3.6.24 nte2833-volume mode 8167
16.3.6.25 payload-type clear-mode 8169
16.3.6.26 payload-type g726-16k 8170
16.3.6.27 payload-type g726-24k 8171
16.3.6.28 payload-type g726-32k 8172
16.3.6.29 payload-type g726-40k 8173
16.3.6.30 payload-type nte 8174
16.3.6.31 payload-type redundancy 8175
16.3.6.32 payload-type vbd 8176
16.3.6.33 plc 8177
16.3.6.34 prohibit 8178
16.3.6.35 resource-threshold 8179
16.3.6.36 resource-threshold mode 8180
16.3.6.37 rtcp rtcp-interval 8181
16.3.6.38 rtcp rtcpxr 8182
16.3.6.39 rtcp sev-degrade-threshold 8183
16.3.6.40 rtcp vqm 8184
16.3.6.41 silence 8184
16.3.6.42 tone (Voice View) 8185
16.3.6.43 tone-frequency 8186
16.3.6.44 tone-cadence 8188
16.3.6.45 tone-detect-info 8189
16.3.6.46 traffic-policy (DSP attribute view) 8191
16.3.7 Voice Diagnose Commands 8193
16.3.7.1 clip port 8193
16.3.7.2 debugging voice-adapt 8195
16.3.7.3 diagnose 8196
16.3.7.4 digit-trace 8196
16.3.7.5 display fe slot fe-id table port-map dsp-port base-port 8197

16.3.7.6 display fe slot fe-id table voice-mr dest-ip port protocol....8198
16.3.7.7 display fe slot fe-id table voice-signal....8199
16.3.7.8 display pots loop-line-threshold....8201
16.3.7.9 display pots subcard-loopline-adjust....8202
16.3.7.10 display voice device state....8203
16.3.7.11 display voice statistics module at0....8203
16.3.7.12 display voice statistics module h323....8205
16.3.7.13 display voice statistics module pots....8209
16.3.7.14 display voice statistics module q931....8211
16.3.7.15 display voice statistics module r2....8215
16.3.7.16 display voice statistics module sip....8217
16.3.7.17 pots circuit-test....8219
16.3.7.18 pots loop-line-test....8221
16.3.7.19 pots loop-line-threshold....8222
16.3.7.20 pots path-test....8224
16.3.7.21 pots subcard-loopline-adjust get....8226
16.3.7.22 pots subcard-loopline-adjust restore....8227
16.3.7.23 pots subcard-loopline-adjust set....8228
16.3.7.24 reset voice statistics module....8229
16.3.7.25 ts6em....8230
16.4 Voice interface Commands....8231
16.4.1 Voice interface Configuration Commands....8231
16.4.1.1 access-mode....8231
16.4.1.2 access-mode (BRA Interface View)....8232
16.4.1.3 alarm....8233
16.4.1.4 crc4....8234
16.4.1.5 crc (VE1 interface view)....8235
16.4.1.6 crc-alarm-threshold....8236
16.4.1.7 display voice port bra....8238
16.4.1.8 display voice port fxo....8239
16.4.1.9 display voice port fxs....8241
16.4.1.10 display voice port ve1....8243
16.4.1.11 electric current....8246
16.4.1.12 electric impedance....8247
16.4.1.13 electric receive-gain....8249
16.4.1.14 electric send-gain....8251
16.4.1.15 feed....8255
16.4.1.16 gain....8256
16.4.1.17 impedance (FXO interface view)....8261
16.4.1.18 impedance (VE1 interface view)....8263
16.4.1.19 invert....8264
16.4.1.20 itf(VE1 interface view)....8265

16.4.1.21 l2-monitor 8266
16.4.1.22 l2-monitor (VE1 interface view) 8267
16.4.1.23 line-lock 8268
16.4.1.24 loop 8269
16.4.1.25 nlp-mode 8270
16.4.1.26 pcm-alarm 8271
16.4.1.27 port bra 8273
16.4.1.28 port fxo 8274
16.4.1.29 port fxs 8275
16.4.1.30 port ve1 8276
16.4.1.31 remote-power 8277
16.4.1.32 reset line-fault 8278
16.4.1.33 reverse-pole-pulse level 8279
16.4.1.34 ring 8280
16.4.1.35 sa 8282
16.4.1.36 shutdown 8283
16.4.1.37 signal(VE1 interface view) 8284
16.4.1.38 work-mode 8285
16.5 PBX Configuration Commands 8287
16.5.1 PBX Basic Configuration Commands 8287
16.5.1.1 access-telno (disa view) 8287
16.5.1.2 account-set 8288
16.5.1.3 b2brouteadd 8289
16.5.1.4 cac 8290
16.5.1.5 call-type 8291
16.5.1.6 callprefix 8299
16.5.1.7 callroute (call prefix view) 8300
16.5.1.8 cause-mapping 8300
16.5.1.9 collectcall (call prefix view) 8301
16.5.1.10 country-code 8302
16.5.1.11 crbt (enterprise view) 8304
16.5.1.12 custom-right (call prefix view) 8305
16.5.1.13 description (enterprise view) 8305
16.5.1.14 digit-length 8306
16.5.1.15 disa 8307
16.5.1.16 display voice account-set 8308
16.5.1.17 display voice cac 8310
16.5.1.18 display voice callprefix 8311
16.5.1.19 display voice cause-mapping 8313
16.5.1.20 display voice country-code 8314
16.5.1.21 display voice disa 8315
16.5.1.22 display voice dss1 timer 8317

16.5.1.23 display voice enterprise....8318
16.5.1.24 display voice media-bandwidth-control (PBX)....8320
16.5.1.25 display voice pbx country-area-transform....8322
16.5.1.26 display voice pbx parameter....8323
16.5.1.27 display voice ring-mode....8327
16.5.1.28 display voice tone-set....8328
16.5.1.29 dn-set (disa view)....8329
16.5.1.30 dn-set (enterprise view)....8330
16.5.1.31 dss1 timer....8331
16.5.1.32 dst-enterprise (disa view)....8334
16.5.1.33 enterprise (account-set view)....8335
16.5.1.34 enterprise (call prefix view)....8336
16.5.1.35 enterprise (voice view)....8337
16.5.1.36 inter-only-call-source....8338
16.5.1.37 password cipher (account-set view)....8338
16.5.1.38 pbx default-country-code default-area-code....8339
16.5.1.39 pbx enable-country-area-transform....8340
16.5.1.40 pbx number-parameter....8341
16.5.1.41 prefix (call prefix view)....8374
16.5.1.42 pwdcalllimit....8375
16.5.1.43 re-route (call prefix view)....8376
16.5.1.44 ring-mode....8377
16.5.1.45 ssl-client-policy (SIP server view)....8380
16.5.1.46 ssl-client-policy (trunk group view)....8381
16.5.1.47 ssl-server-policy (SIP server view)....8383
16.5.1.48 ssl-server-policy (trunk group view)....8384
16.5.1.49 special-deal....8386
16.5.1.50 time....8387
16.5.1.51 tone-set....8389
16.5.1.52 user-account(account-set view)....8390
16.5.1.53 use-account-set (disa view)....8391
16.5.1.54 vu-custom-right (call prefix view)....8392
16.5.1.55 vuloopcount....8393
16.5.1.56 vuoutgoingright....8394
16.5.2 SIP Server Configuration Commands....8395
16.5.2.1 codec-priority....8395
16.5.2.2 cs-mode (SIP server view)....8397
16.5.2.3 ddns-client....8398
16.5.2.4 display voice sipserver....8399
16.5.2.5 display voice sipserver dtmf....8403
16.5.2.6 display voice sipserver fax-modem....8404
16.5.2.7 dtmf-transmission-mode....8406

16.5.2.8 fax-modem common negotiation-mode....8407
16.5.2.9 fax-modem common rtp-interval....8408
16.5.2.10 fax-modem common vbd-attribute-type....8409
16.5.2.11 fax-modem common vbd-codec....8410
16.5.2.12 fax-modem common vbd-payload-type....8411
16.5.2.13 fax-modem fax transmission-mode....8412
16.5.2.14 home-domain (SIP server view)....8413
16.5.2.15 media-bandwidth-control (SIP server view)....8414
16.5.2.16 media-bandwidth-control max-bandwidth (SIP server view)....8415
16.5.2.17 media-ip....8417
16.5.2.18 nte-fax-modem....8417
16.5.2.19 nte-negotiation-mode....8418
16.5.2.20 number-parameter (SIP server view)....8420
16.5.2.21 qos stream (SIP server view)....8428
16.5.2.22 redundancy-negotiation-mode....8429
16.5.2.23 redundancy-nte....8431
16.5.2.24 redundancy-start-mode....8432
16.5.2.25 redundancy-vbd....8433
16.5.2.26 reg-count-per-second....8434
16.5.2.27 register-uri....8435
16.5.2.28 reset (SIP server view)....8436
16.5.2.29 shutdown (SIP server view)....8437
16.5.2.30 signalling-address....8437
16.5.2.31 signalling-domain....8438
16.5.2.32 sipserver....8439
16.5.2.33 transfer(SIP server view)....8440
16.5.3 CDR Server Configuration Commands....8441
16.5.3.1 bill format....8441
16.5.3.2 bill textfield....8442
16.5.3.3 bill transfertype....8443
16.5.3.4 billpoolfull....8444
16.5.3.5 cdr-server....8445
16.5.3.6 display voice cdr-server....8446
16.5.3.7 server ip port....8448
16.5.3.8 username password....8449
16.5.4 PBX User Configuration Commands....8450
16.5.4.1 bind trunk-group (PBX user view)....8450
16.5.4.2 call-right....8451
16.5.4.3 custom-right (PBX user view)....8452
16.5.4.4 display voice pbxuser....8453
16.5.4.5 display voice pbxuser brief....8456
16.5.4.6 display voice pbxuser eid-para....8457

16.5.4.7 display voice pbxuser port ... 8459
16.5.4.8 display voice pbxuser sipue ... 8461
16.5.4.9 display voice pbxuser sipue-register-state ... 8463
16.5.4.10 display voice pbxuser start-telno ... 8464
16.5.4.11 display voice pbxuser state ... 8466
16.5.4.12 display voice priority-group ... 8467
16.5.4.13 dn-set (PBX user view) ... 8468
16.5.4.14 eid-para bell-ans-flag ... 8469
16.5.4.15 eid-para clip-format ... 8470
16.5.4.16 eid-para dc-time ... 8471
16.5.4.17 eid-para default-cli ... 8472
16.5.4.18 eid-para description (PBX user view) ... 8473
16.5.4.19 eid-para detect-ansbar-by-single-tone ... 8474
16.5.4.20 eid-para dsp-input-gain ... 8475
16.5.4.21 eid-para dsp-output-gain ... 8476
16.5.4.22 eid-para endservice ... 8477
16.5.4.23 eid-para fsk-mode ... 8478
16.5.4.24 eid-para fsk-time ... 8479
16.5.4.25 eid-para line-type ... 8479
16.5.4.26 eid-para password (PBX user view) ... 8481
16.5.4.27 eid-para priority (PBX user view) ... 8482
16.5.4.28 eid-para tas-pattern ... 8483
16.5.4.29 eid-para vqe-agc ... 8484
16.5.4.30 eid-para vqe-agc-level ... 8484
16.5.4.31 eid-para vqe-sns ... 8485
16.5.4.32 eid-para vqe-sns-level ... 8486
16.5.4.33 pbxuser (voice view) ... 8487
16.5.4.34 pbxuser-batch ... 8488
16.5.4.35 pickupgroup-name ... 8490
16.5.4.36 port (PBX user view) ... 8491
16.5.4.37 priority (PBX user view) ... 8492
16.5.4.38 priority-group (voice view) ... 8493
16.5.4.39 priority-group (PBX user view) ... 8494
16.5.4.40 proxyreg-id (PBX user view) ... 8496
16.5.4.41 sipue (PBX user view) ... 8497
16.5.4.42 telno (PBX user view) ... 8498
16.5.4.43 telno (priority-group view) ... 8499
16.5.4.44 telno service-password cipher (PBX user view) ... 8500
16.5.4.45 user-type (PBX user view) ... 8501
16.5.4.46 user-name ... 8502
16.5.4.47 web-password (PBX user view) ... 8503
16.5.5 SBC Proxy configuration commands ... 8504

16.5.5.1 display voice sbc media-relay 8504
16.5.5.2 media-bandwidth-control media-proxy enable 8505
16.5.5.3 media-bandwidth-control media-proxy max-bandwidth 8506
16.5.5.4 sbc mapped-media-ip 8507
16.5.5.5 sbc mapped-media-port-start 8508
16.5.5.6 sbc mapped-media-proxy-port-start 8509
16.5.5.7 sbc mapped-signalling-address 8510
16.5.5.8 sbc media-proxy 8511
16.5.5.9 sbc media-relay 8512
16.5.5.10 sbc signalling-proxy 8513
16.5.6 Trunk Group configuration commands 8514
16.5.6.1 auto-connect-controlchannel 8514
16.5.6.2 callproc-wait-response-timeout 8515
16.5.6.3 callroute (trunk group view) 8516
16.5.6.4 callsource (trunk group view) 8518
16.5.6.5 channels-timeout 8518
16.5.6.6 circuit-state-relate (trunk group view) 8519
16.5.6.7 codec-priority(trunk group view) 8521
16.5.6.8 cs-mode (trunk group view) 8523
16.5.6.9 custom-right (trunk group view) 8523
16.5.6.10 default-caller-telno (trunk view) 8525
16.5.6.11 del-techprefix 8525
16.5.6.12 description (trunk group view) 8526
16.5.6.13 digest-username 8527
16.5.6.14 display voice gatekeeper callprefix 8528
16.5.6.15 display voice gatekeeper endpoints 8530
16.5.6.16 display voice h323 app-time 8531
16.5.6.17 display voice h323 config 8533
16.5.6.18 display voice h323 running 8535
16.5.6.19 display voice r2 profile 8537
16.5.6.20 display voice r2 signalling-type 8541
16.5.6.21 display voice trunk-at0 8545
16.5.6.22 display voice trunk-e1r2 8547
16.5.6.23 display voice trunk-group 8548
16.5.6.24 display voice trunk-bra 8553
16.5.6.25 display voice trunk-pra 8555
16.5.6.26 display voice trunk-sipat0 8556
16.5.6.27 displayname 8557
16.5.6.28 dtmf-transmission-mode (trunk group view) 8559
16.5.6.29 earlyh245 8560
16.5.6.30 endservice trunk-sipat0(SIP AT0 trunk view) 8561
16.5.6.31 endsession-timeout 8562

16.5.6.32 enterprise dn-set (trunk group view) 8563
16.5.6.33 faststart-flag 8564
16.5.6.34 fax-modem common negotiation-mode 8564
16.5.6.35 fax-modem common rtp-interval 8565
16.5.6.36 fax-modem common vbd-attribute-type 8566
16.5.6.37 fax-modem common vbd-codec 8567
16.5.6.38 fax-modem common vbd-payload-type 8568
16.5.6.39 fax-modem fax transmission-mode 8569
16.5.6.40 gatekeeper-techprefix 8570
16.5.6.41 gkid 8572
16.5.6.42 gnr-number (trunk group view) 8573
16.5.6.43 gwid 8574
16.5.6.44 h245version 8575
16.5.6.45 h323-app-timer 8576
16.5.6.46 h323-attribute 8585
16.5.6.47 h323-number-parameter 8585
16.5.6.48 h323-systemname 8592
16.5.6.49 h323version 8593
16.5.6.50 heartbeat 8594
16.5.6.51 home-domain (trunk group view) 8595
16.5.6.52 line-signal-receive 8596
16.5.6.53 line-signal-send 8598
16.5.6.54 line-signalling 8599
16.5.6.55 localip 8600
16.5.6.56 maxcr (trunk group view) 8601
16.5.6.57 media-bandwidth-control enable (trunk-group) 8602
16.5.6.58 media-bandwidth-control max-bandwidth (trunk-group) 8603
16.5.6.59 media-ip (H323 Trunk group view) 8605
16.5.6.60 media-ip (SIP Trunk group view) 8606
16.5.6.61 medialoop-timeout 8607
16.5.6.62 nte-fax-modem 8608
16.5.6.63 nte-negotiation-mode 8609
16.5.6.64 num-plan-identify called 8610
16.5.6.65 num-plan-identify caller 8611
16.5.6.66 number-parameter (trunk group view) 8613
16.5.6.67 outgoing-right(trunk group view) 8632
16.5.6.68 peer-address 8633
16.5.6.69 peer-address static (H323 trunk group view) 8635
16.5.6.70 peer-address static (trunk group view) 8636
16.5.6.71 peer-address switchover 8638
16.5.6.72 pra-restart 8639
16.5.6.73 priority(trunk group view) 8639

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.74 productname....8640
16.5.6.75 q931-listenport....8641
16.5.6.76 qos stream (trunk group view)....8642
16.5.6.77 r2 profile....8643
16.5.6.78 r2 signalling-type....8644
16.5.6.79 r2-play-ringback....8645
16.5.6.80 r2-profile (trunk group view)....8646
16.5.6.81 r2-receive-earlymedia....8646
16.5.6.82 rasport....8647
16.5.6.83 reanswer....8648
16.5.6.84 recvalert-wait-response-timeout....8649
16.5.6.85 redundancy-negotiation-mode....8650
16.5.6.86 redundancy-nte (trunk group view)....8652
16.5.6.87 redundancy-start-mode (trunk group view)....8653
16.5.6.88 redundancy-vbd (trunk group view)....8654
16.5.6.89 register-E164-number (H323 trunk group view)....8655
16.5.6.90 register-address-receive....8656
16.5.6.91 register-address-send....8659
16.5.6.92 register-id (trunk group view)....8662
16.5.6.93 register-signal-receive....8663
16.5.6.94 register-signal-send....8664
16.5.6.95 register-signalling....8665
16.5.6.96 register-uri (trunk group view)....8668
16.5.6.97 request-channelclose-timeout....8669
16.5.6.98 requestmode-timeout....8670
16.5.6.99 reserved-circuit (trunk group view)....8671
16.5.6.100 reset (H323 attribute view)....8672
16.5.6.101 reset (trunk group view)....8672
16.5.6.102 roundtrip-delay-timeout....8673
16.5.6.103 select-mode (trunk group view)....8674
16.5.6.104 send-heartbeat....8676
16.5.6.105 send-techprefix....8677
16.5.6.106 setup-wait-response-timeout....8678
16.5.6.107 shutdown (H323 attribute view)....8678
16.5.6.108 shutdown (trunk group view)....8679
16.5.6.109 signalling-address....8680
16.5.6.110 signalling-type....8681
16.5.6.111 stable delay-time....8682
16.5.6.112 statuscode-toneid-mapping (trunk group view)....8683
16.5.6.113 support-cli-change....8684
16.5.6.114 support-h245tul....8685
16.5.6.115 tcp-connection-timeout....8686

16.5.6.116 tcp-keepalive-timerlen ... 8687
16.5.6.117 techprefix ... 8688
16.5.6.118 transfer (trunk group view) ... 8688
16.5.6.119 trunk-at0 ... 8690
16.5.6.120 trunk-bra ... 8692
16.5.6.121 trunk-bra typeofnumber ... 8694
16.5.6.122 trunk-group ... 8695
16.5.6.123 trunk-pra ... 8698
16.5.6.124 trunk-pra typeofnumber ... 8699
16.5.6.125 trunk-r2 ... 8701
16.5.6.126 trunk-sipat0 ... 8702
16.5.6.127 ttlrrq ... 8704
16.5.6.128 typeofnumber called ... 8705
16.5.6.129 typeofnumber caller ... 8707
16.5.6.130 use-rule-set ... 8708
16.5.6.131 workmode (H323 attribute view) ... 8709
16.5.7 Call Route configuration command ... 8710
16.5.7.1 callroute ... 8710
16.5.7.2 callroute (reroute view) ... 8711
16.5.7.3 callroute (route-analysis view) ... 8711
16.5.7.4 callsource ... 8712
16.5.7.5 callsource (route-analysis view) ... 8713
16.5.7.6 display voice callroute ... 8714
16.5.7.7 display voice callsource ... 8715
16.5.7.8 display voice reroute-deal ... 8716
16.5.7.9 display voice route-analysis ... 8717
16.5.7.10 failed-type (reroute view) ... 8718
16.5.7.11 re-callroute (reroute view) ... 8719
16.5.7.12 reroute-deal ... 8720
16.5.7.13 route-analysis ... 8721
16.5.7.14 selecttype ... 8721
16.5.7.15 trunk-group (route-analysis view) ... 8723
16.5.8 PBX Service Configuration Commands ... 8723
16.5.8.1 access-telno ... 8723
16.5.8.2 afterroute-change ... 8724
16.5.8.3 beforeroute-change ... 8725
16.5.8.4 bind (service user group view) ... 8726
16.5.8.5 bind main-eid (service view for the senior manager's secretary) ... 8727
16.5.8.6 busyselectmode (service user group view) ... 8728
16.5.8.7 call dual-dial-tone-flag (pre-routing number change plan view) ... 8729
16.5.8.8 call new-attribute (pre-routing number change plan view) ... 8730
16.5.8.9 call re-analyse (pre-routing number change plan view) ... 8731

16.5.8.10 call-right (user group view) 8732
16.5.8.11 called (calling number change view) 8734
16.5.8.12 called (post-routing number change plan view) 8735
16.5.8.13 called (pre-routing number change plan view) 8736
16.5.8.14 caller (calling number change view) 8738
16.5.8.15 caller (post-routing number change plan view) 8739
16.5.8.16 caller (pre-routing number change plan view) 8740
16.5.8.17 caller-change (voice view) 8741
16.5.8.18 callerprefix (calling number change view) 8742
16.5.8.19 callprefix (post-routing number change plan view) 8743
16.5.8.20 callprefix (pre-routing number change plan view) 8744
16.5.8.21 condition called-telno (pre-routing number change plan view) 8745
16.5.8.22 condition caller-telno (post-routing number change plan view) 8746
16.5.8.23 condition caller-telno (pre-routing number change plan view) 8747
16.5.8.24 config-dn (service view for the senior manager's secretary) 8748
16.5.8.25 country-code (trunk group view) 8749
16.5.8.26 cpu-flowcontrol 8750
16.5.8.27 crbt (user group view) 8751
16.5.8.28 crbt-file (user group view) 8752
16.5.8.29 crbt-file (enterprise view) 8753
16.5.8.30 custom-right (calling number change view) 8754
16.5.8.31 display voice afterroute-change 8756
16.5.8.32 display voice beforeroute-change 8757
16.5.8.33 display voice caller-change 8760
16.5.8.34 display voice cpu-flowcontrol 8761
16.5.8.35 display voice gnr-number 8762
16.5.8.36 display voice group-member 8763
16.5.8.37 display voice ivr-voice-file 8766
16.5.8.38 display voice number-map 8766
16.5.8.39 display voice pbxuser callback-info 8767
16.5.8.40 display voice pbxuser service-active 8768
16.5.8.41 display voice pbxuser service-right 8769
16.5.8.42 display voice pbxusergroup 8772
16.5.8.43 display voice pickup-group 8774
16.5.8.44 display voice ring-parallel-group 8775
16.5.8.45 display voice ring-serial-group 8776
16.5.8.46 display voice rule-set 8777
16.5.8.47 display voice service alert-ring 8779
16.5.8.48 display voice ssca-group 8780
16.5.8.49 display voice tone type 8781
16.5.8.50 display voice trunk-group trunk-circuit state brief 8794
16.5.8.51 display voice unicall-group 8795

16.5.8.52 display voice vms....8797
16.5.8.53 dn-set (PBX user group view)....8798
16.5.8.54 enterprise (calling number change view)....8799
16.5.8.55 enterprise (distinctive ringing service view)....8800
16.5.8.56 enterprise (number map view)....8801
16.5.8.57 enterprise (rule-set view)....8801
16.5.8.58 external-num....8802
16.5.8.59 forward-condition....8803
16.5.8.60 full-number (GNR view)....8805
16.5.8.61 gnr-number (voice view)....8806
16.5.8.62 group-member....8807
16.5.8.63 group-member (simultaneous ringing user group view and sequential ringing user group view)....8810
16.5.8.64 group-name....8811
16.5.8.65 If-encrypt....8812
16.5.8.66 internal-num....8813
16.5.8.67 ivr-voice-file....8813
16.5.8.68 line-share-mode (service view for the senior manager's secretary)....8814
16.5.8.69 master-first....8815
16.5.8.70 max-record-num....8816
16.5.8.71 max-record-time....8817
16.5.8.72 new-callsource (calling number change view)....8818
16.5.8.73 number-map....8819
16.5.8.74 out-ddd-ring-id....8820
16.5.8.75 out-idd-ring-id....8820
16.5.8.76 out-inter-ring-id....8821
16.5.8.77 out-local-ring-id....8822
16.5.8.78 outgoing-right (calling number change view)....8823
16.5.8.79 pbxusergroup....8824
16.5.8.80 prioritymode (service user group view)....8825
16.5.8.81 ring (user group view)....8826
16.5.8.82 ring-parallel-group....8827
16.5.8.83 ring-serial-group....8828
16.5.8.84 ringmode (service user group view)....8829
16.5.8.85 rule caller-telno called-telno....8830
16.5.8.86 rule disconnect-cause incoming....8832
16.5.8.87 rule-set....8833
16.5.8.88 selectinterval (ONLY group view)....8834
16.5.8.89 selectinterval (service group view)....8834
16.5.8.90 service abbdial....8835
16.5.8.91 service alert-ring....8836
16.5.8.92 service cba....8837
16.5.8.93 service cfb....8838

16.5.8.94 service cfc ... 8839
16.5.8.95 service cfnr ... 8840
16.5.8.96 service cfnr (user group view) ... 8841
16.5.8.97 service cfo ... 8842
16.5.8.98 service cfo (user group view) ... 8843
16.5.8.99 service cfu ... 8845
16.5.8.100 service crbt (enterprise view) ... 8845
16.5.8.101 service crbt (user group view) ... 8848
16.5.8.102 service dlc ... 8849
16.5.8.103 service dnd ... 8850
16.5.8.104 service hotline ... 8851
16.5.8.105 service rac ... 8853
16.5.8.106 service rcs ... 8854
16.5.8.107 service sca ... 8856
16.5.8.108 service scr ... 8859
16.5.8.109 service voicemailcfb ... 8860
16.5.8.110 service voicemailcfnr ... 8861
16.5.8.111 service voicemailcfo ... 8862
16.5.8.112 service voicemailcfu ... 8863
16.5.8.113 service wake-call ... 8864
16.5.8.114 service-active ... 8865
16.5.8.115 service-right ... 8866
16.5.8.116 space-waring-num-left ... 8869
16.5.8.117 ssca-group ... 8869
16.5.8.118 track vrrp ... 8870
16.5.8.119 triggertype (simultaneous or sequential ringing group view) ... 8872
16.5.8.120 trunk-group (post-routing number change plan view) ... 8873
16.5.8.121 unicall-group ... 8874
16.5.8.122 use-rule-set ... 8874
16.5.8.123 vms ... 8875
16.5.8.124 vmsdata-storage-path ... 8876
16.5.8.125 vmsno ... 8877
16.5.9 Local Survival Configuration Commands ... 8878
16.5.9.1 dataserver ... 8878
16.5.9.2 dataservertype ... 8878
16.5.9.3 display voice local-survival lefttime ... 8879
16.5.9.4 display voice local-survival status ... 8880
16.5.9.5 local-address ... 8882
16.5.9.6 local-bill ... 8883
16.5.9.7 local-survival ... 8883
16.5.9.8 password cipher ... 8884
16.5.9.9 primary-trunk-group ... 8885

16.5.9.10 reset ... 8886
16.5.9.11 ssl-server-policy ... 8887
16.5.9.12 sync-interval ... 8888
16.5.9.13 transfer ... 8889
16.5.10 Conference Configuration Commands ... 8890
16.5.10.1 attendee-password ... 8890
16.5.10.2 attendee-telno ... 8891
16.5.10.3 chairman-password ... 8892
16.5.10.4 conference ... 8893
16.5.10.5 conference-attribute ... 8894
16.5.10.6 conference-convoker ... 8895
16.5.10.7 conference-id-length ... 8896
16.5.10.8 conference-reconvoke-attempts ... 8897
16.5.10.9 custom-right (conference-attribute view) ... 8898
16.5.10.10 description ... 8900
16.5.10.11 display voice conference ... 8900
16.5.10.12 display voice conference-attribute ... 8901
16.5.10.13 display voice conference-convoker ... 8902
16.5.10.14 display voice conference-custom-right ... 8903
16.5.10.15 display voice conference-id-length ... 8903
16.5.10.16 display voice conference-out-right ... 8904
16.5.10.17 display voice conference-reconvoke-attempts ... 8905
16.5.10.18 dn-set ... 8905
16.5.10.19 out-right ... 8906
16.5.10.20 regnum ... 8908
16.5.10.21 schedule ... 8909
16.5.11 Self Service Http Server Commands ... 8910
16.5.11.1 display voice self-service-http-server ... 8910
16.5.11.2 self-service-http-server ... 8911
16.5.11.3 self-service http server enable ... 8911
16.5.11.4 self-service http server port ... 8912
16.5.11.5 self-service http secure-server enable ... 8913
16.5.11.6 self-service http secure-server port ... 8914
16.5.12 Group Registrar Configuration Commands ... 8915
16.5.12.1 bind trunk-group (group resistrar view) ... 8915
16.5.12.2 display voice groupreg ... 8916
16.5.12.3 display voice groupreg pbxuser brief ... 8917
16.5.12.4 groupreg ... 8918
16.5.12.5 home-domain (group resistrar view) ... 8919
16.5.12.6 impi ... 8920
16.5.12.7 pbxuser ... 8922
16.6 SIP AG Commands ... 8923

16.6.1 SIP AG Parameter Configuration Commands....8923
16.6.1.1 ag number-parameter....8924
16.6.1.2 ag string-parameter....8928
16.6.1.3 ag-domain....8933
16.6.1.4 auth mode....8934
16.6.1.5 auth (SIP AG view)....8935
16.6.1.6 conference-factory-uri....8937
16.6.1.7 description (SIP AG view)....8938
16.6.1.8 digitmap-timer....8939
16.6.1.9 display voice media-bandwidth-control (SIP AG)....8940
16.6.1.10 display voice local-digitmap....8942
16.6.1.11 display voice sctp-global-statistics....8943
16.6.1.12 display voice sip-profile....8945
16.6.1.13 display voice sip-reg-count-per-second....8947
16.6.1.14 display voice sip-service-logic....8947
16.6.1.15 display voice sipag....8949
16.6.1.16 display voice sipag auth....8952
16.6.1.17 display voice sipag dtmf....8954
16.6.1.18 display voice sipag fax-modem....8955
16.6.1.19 display voice sipag nte....8957
16.6.1.20 display voice sipag number-parameter....8958
16.6.1.21 display voice sipag ring-mode....8959
16.6.1.22 display voice sipag string-parameter....8961
16.6.1.23 display voice sipag redundancy....8963
16.6.1.24 display voice sipag sctp-association-info....8964
16.6.1.25 display voice sipag sctp-association-statistics....8967
16.6.1.26 display voice sipag sctp-protocol....8968
16.6.1.27 display voice sipag signal....8970
16.6.1.28 display voice sipag status-code-mapping....8972
16.6.1.29 display voice sipag user-defined-profile....8976
16.6.1.30 dtmf-transmission-mode....8982
16.6.1.31 fax-modem common negotiation-mode....8983
16.6.1.32 fax-modem common rtp-interval....8984
16.6.1.33 fax-modem common vbd-attribute-type....8985
16.6.1.34 fax-modem common vbd-codec....8986
16.6.1.35 fax-modem common vbd-pt-type....8987
16.6.1.36 fax-modem fax transmission-mode....8988
16.6.1.37 fax-modem modem transmission-mode....8990
16.6.1.38 home-domain....8991
16.6.1.39 local-digitmap....8992
16.6.1.40 loop (VE1 interface view)....8994
16.6.1.41 loop (bra interface view)....8995

16.6.1.42 loop (fxs interface view) 8995
16.6.1.43 media-addr 8996
16.6.1.44 media-bandwidth-control enable (SIPAG) 8998
16.6.1.45 media-bandwidth-control max-bandwidth (SIPAG) 8999
16.6.1.46 nte-dtmf 9000
16.6.1.47 nte-fax-modem 9001
16.6.1.48 nte-flash-hook 9002
16.6.1.49 nte-negotiation-mode 9003
16.6.1.50 phone-context 9005
16.6.1.51 primary-proxy-addr dns-a 9006
16.6.1.52 primary-proxy-addr dns-naptr 9007
16.6.1.53 primary-proxy-addr dns-srv 9008
16.6.1.54 primary-proxy-addr static 9009
16.6.1.55 profile 9010
16.6.1.56 proxy-detect-mode 9011
16.6.1.57 proxy-dhcp-option 9012
16.6.1.58 proxy-dual-home 9013
16.6.1.59 proxy-refresh-mode 9015
16.6.1.60 proxy-switchover 9016
16.6.1.61 redundancy-negotiation-mode 9017
16.6.1.62 redundancy-nte 9018
16.6.1.63 redundancy-start-mode 9019
16.6.1.64 redundancy-vbd 9021
16.6.1.65 redundancy-voice 9022
16.6.1.66 register-server-uri (SIP AG view) 9023
16.6.1.67 reset sctp-association-statistics 9024
16.6.1.68 reset sctp-global-statistics 9025
16.6.1.69 reset (SIP AG view) 9025
16.6.1.70 ring-mode 9026
16.6.1.71 scene 9028
16.6.1.72 sctp 9029
16.6.1.73 sdp-negotiation-mode 9034
16.6.1.74 secondary-proxy-addr dns-a 9035
16.6.1.75 secondary-proxy-addr dns-naptr 9036
16.6.1.76 secondary-proxy-addr dns-srv 9037
16.6.1.77 secondary-proxy-addr static 9038
16.6.1.78 service-logic 9039
16.6.1.79 signal 9041
16.6.1.80 signalling-addr 9042
16.6.1.81 sipag 9043
16.6.1.82 sip-reg-count-per-second 9044
16.6.1.83 status-code-mapping 9045

16.6.1.84 subscribe mwi....9048
16.6.1.85 subscribe reg....9049
16.6.1.86 subscribe ua-profile....9050
16.6.1.87 transfer (SIP AG view)....9051
16.6.1.88 unit....9052
16.6.1.89 user-defined-profile codec-priority....9055
16.6.1.90 user-defined-profile number-parameter....9056
16.6.1.91 user-defined-profile service-priority....9130
16.6.2 SIP AG User Configuration Commands....9131
16.6.2.1 active-mask time-slot config-status....9132
16.6.2.2 agid (SIP AG user view)....9133
16.6.2.3 auth (SIP service data profile view)....9133
16.6.2.4 auth (user group view)....9135
16.6.2.5 auto-resume-limit....9137
16.6.2.6 base-telno....9138
16.6.2.7 bell-ans-flag....9139
16.6.2.8 centrex-dial....9140
16.6.2.9 centrex-number....9141
16.6.2.10 centrex-prefix....9142
16.6.2.11 clip-format....9143
16.6.2.12 clip-transmission-sequence....9144
16.6.2.13 dc-time....9145
16.6.2.14 detect-ansbar-by-single-tone....9146
16.6.2.15 dial-tone....9147
16.6.2.16 display voice sipagusergroup....9148
16.6.2.17 display voice sipaguser....9151
16.6.2.18 display voice sipservicedata....9153
16.6.2.19 dsp-input-gain....9156
16.6.2.20 dsp-output-gain....9157
16.6.2.21 dsp-template....9158
16.6.2.22 endservice (SIP AG user view)....9159
16.6.2.23 endservice (User group view)....9160
16.6.2.24 extend-telno....9161
16.6.2.25 fsk-mode....9162
16.6.2.26 fsk-time....9163
16.6.2.27 group-name....9164
16.6.2.28 line-type....9165
16.6.2.29 mwi-mode....9166
16.6.2.30 precinct-mode....9167
16.6.2.31 priority....9168
16.6.2.32 register-uri-mode....9169
16.6.2.33 service cfb....9170

16.6.2.34 service cfnr....9171
16.6.2.35 service cfo....9172
16.6.2.36 service cfu....9173
16.6.2.37 service hotline....9174
16.6.2.38 service-right (SIP service data profile view)....9175
16.6.2.39 sipaguser (Voice View)....9177
16.6.2.40 sipagusergroup....9178
16.6.2.41 sipservicedata....9179
16.6.2.42 subscribe ua-profile....9180
16.6.2.43 tas-pattern....9182
16.6.2.44 uni-report....9183
16.6.2.45 uri....9184
16.6.2.46 vqe-agc....9185
16.6.2.47 vqe-agc-level....9186
16.6.2.48 vqe-sns....9187
16.6.2.49 vqe-sns-level....9188
16.7 H.248 AG Commands....9189
16.7.1 H.248 AG Parameter Setting Commands....9190
16.7.1.1 2833encrypt....9190
16.7.1.2 auth....9191
16.7.1.3 desc....9192
16.7.1.4 deviceName....9193
16.7.1.5 digitmap....9194
16.7.1.6 digitmap-timer....9196
16.7.1.7 display voice h248ag....9199
16.7.1.8 display voice h248ag h248stack....9204
16.7.1.9 display voice h248ag auth....9207
16.7.1.10 display voice h248ag digitmap....9208
16.7.1.11 display voice h248ag digitmap-timer....9210
16.7.1.12 display voice h248ag h248profile....9211
16.7.1.13 display voice h248ag h248statistics....9213
16.7.1.14 display voice h248ag mg-software....9215
16.7.1.15 display voice h248ag standalone....9230
16.7.1.16 display voice h248ag tid-format....9231
16.7.1.17 display voice h248ag mg-ringmode attribute....9233
16.7.1.18 display voice h248ag mg-ringmode default-mgcpara....9234
16.7.1.19 display voice h248ag sctp protocol....9235
16.7.1.20 display voice h248ag sctp association statistics....9238
16.7.1.21 display voice h248ag sctp association info....9239
16.7.1.22 display voice h248ag mg-ringmode default-ringpara....9241
16.7.1.23 display voice sctp version....9242
16.7.1.24 domainName....9243

16.7.1.25 h248profile....9244
16.7.1.26 h248stack format....9246
16.7.1.27 h248stack messagesegmentation....9247
16.7.1.28 h248stack MTU....9248
16.7.1.29 h248stack sdpencodetype....9249
16.7.1.30 h248stack securitytype....9249
16.7.1.31 h248stack tr....9250
16.7.1.32 heartBeat....9254
16.7.1.33 mgc switch....9256
16.7.1.34 mg-media-ip1....9257
16.7.1.35 mg-media-ip2....9258
16.7.1.36 mg-ringmode....9259
16.7.1.37 mg-ringmode default-mgcpara....9261
16.7.1.38 mg-ringmode default-ringpara....9262
16.7.1.39 mg-signal-ip....9263
16.7.1.40 mg-software parameter....9264
16.7.1.41 MIDType....9279
16.7.1.42 profile-negotiation....9281
16.7.1.43 profile-index....9283
16.7.1.44 primary-mgc-address1....9284
16.7.1.45 primary-mgc-address1 static....9285
16.7.1.46 reset....9287
16.7.1.47 retrans....9289
16.7.1.48 secondary-mgc-address1....9291
16.7.1.49 secondary-mgc-address1 static....9292
16.7.1.50 shutdown....9293
16.7.1.51 standalone parameters....9295
16.7.1.52 stand-alone-mgc-ip1....9297
16.7.1.53 start-negotiate-version....9298
16.7.1.54 transfer....9300
16.7.1.55 tid-format....9301
16.7.2 H.248 AG User Configuration Commands....9302
16.7.2.1 active-mask....9302
16.7.2.2 auto-resume-limit....9304
16.7.2.3 bell-ans-flag....9305
16.7.2.4 clip-format....9305
16.7.2.5 clip-transmission-sequence....9307
16.7.2.6 dc-time....9308
16.7.2.7 detect-ansbar-by-single-tone....9309
16.7.2.8 display voice h248aguser....9310
16.7.2.9 display voice h248aguser bra....9311
16.7.2.10 display voice h248aguser pots....9312

16.7.2.11 display voice h248aguser pra....9314
16.7.2.12 display voice iua-link....9315
16.7.2.13 display voice iua-linkset....9317
16.7.2.14 dsp-input-gain....9320
16.7.2.15 dsp-output-gain....9321
16.7.2.16 dsp-template....9322
16.7.2.17 endservice....9323
16.7.2.18 force-sendfsk....9325
16.7.2.19 fsk-mode....9326
16.7.2.20 fsk-time....9327
16.7.2.21 h248aguser....9328
16.7.2.22 line-type....9329
16.7.2.23 priority....9331
16.7.2.24 power-dialer....9332
16.7.2.25 tas-pattern....9333
16.7.2.26 telno....9334
16.7.2.27 uni-report....9334
16.7.2.28 vqe-agc....9335
16.7.2.29 vqe-agc-level....9336
16.7.2.30 vqe-sns....9337
16.7.2.31 vqe-sns-level....9338
16.7.3 H.248 AG Common Commands....9339
16.7.3.1 display voice fax-modem....9339
16.7.3.2 display voice media-bandwidth-control....9343
16.7.3.3 display voice rfc2198....9344
16.7.3.4 display voice tid-template....9346
16.7.3.5 h248ag....9347
16.7.3.6 fax-modem common....9348
16.7.3.7 fax-modem fax....9351
16.7.3.8 fax-modem modem....9352
16.7.3.9 iua-link....9355
16.7.3.10 iua-link clear sctp association statistics....9359
16.7.3.11 iua-link clear statistics....9360
16.7.3.12 iua-link lock....9361
16.7.3.13 iua-link reset....9362
16.7.3.14 iua-linkset....9363
16.7.3.15 iua-linkset-pendingtime....9367
16.7.3.16 local-digitmap....9368
16.7.3.17 rfc2198 smart-parameters....9370
16.7.3.18 sigtran....9371
16.7.3.19 tid-template....9372
16.7.3.20 tid-template-modify....9374

17 Virtualization Commands.....9376
17.1 attach disk.....9377
17.2 blank-disk name.....9378
17.3 cpu.....9379
17.4 delete package.....9381
17.5 display blank-disk name.....9381
17.6 display download-ratio package.....9383
17.7 display ovs bridge information.....9384
17.8 display ovs mac-address bridge.....9385
17.9 display ovs traffic-statistics bridge.....9386
17.10 display package information.....9387
17.11 display resource-usage.....9388
17.12 display veth information.....9389
17.13 display virtual-environment link.....9390
17.14 display virtual-environment reserve cpu-thread statistic.....9391
17.15 display virtual-environment resource.....9392
17.16 display vm.....9394
17.17 display vnc-server information.....9397
17.18 download package.....9398
17.19 exception-action.....9400
17.20 install vm.....9401
17.21 link.....9402
17.22 memory size.....9403
17.23 ova file.....9404
17.24 ovs bridge.....9409
17.25 port (vSwitch view).....9410
17.26 port default vlan (vSwitch view).....9411
17.27 port trunk allow-pass vlan (vSwitch view).....9413
17.28 reset cdrom file.....9414
17.29 reset ovs traffic-statistics bridge.....9415
17.30 set cdrom file.....9416
17.31 uninstall vm.....9417
17.32 veth.....9418
17.33 virtual-environment.....9419
17.34 virtual-environment reserve cpu-thread number.....9420
17.35 virtual-network-card number.....9421
17.36 vm.....9422
17.37 vm activate.....9423
17.38 vm deactivate.....9424
17.39 vm start.....9424
17.40 vm stop.....9425
17.41 vnc-server port.....9426

18 Reliability Commands.....9428
18.1 Interface Backup Configuration Commands.....9428
18.1.1 display standby state.....9428
18.1.2 standby bandwidth.....9431
18.1.3 standby interface.....9433
18.1.4 standby threshold.....9434
18.1.5 standby timer delay.....9436
18.1.6 standby track bfd-session.....9438
18.1.7 standby track nqa.....9439
18.1.8 standby track ip route.....9440
18.1.9 standby timer flow-check.....9441
18.2 Interface Monitoring Group Configuration Commands.....9443
18.2.1 binding interface.....9443
18.2.2 clear monitor-group.....9444
18.2.3 display monitor-group.....9446
18.2.4 monitor enable.....9449
18.2.5 monitor-group.....9450
18.2.6 track monitor-group.....9452
18.2.7 trigger-up-delay.....9454
18.3 NSR Configuration Commands.....9455
18.3.1 display switchover mode.....9455
18.3.2 switchover mode.....9456
18.4 HSB Configuration Commands.....9457
18.4.1 bind-service.....9457
18.4.2 display firewall hsb statistics event.....9458
18.4.3 display hsb statistics hsb-group.....9461
18.4.4 display hsb statistics hsb-service.....9467
18.4.5 display hsb-group.....9468
18.4.6 display hsb-service.....9470
18.4.7 display hsb-service-type firewall hsb-group.....9472
18.4.8 display hsb-service-type vpn-instance.....9473
18.4.9 display hsb-service-type vpn-instance information.....9474
18.4.10 hsb enable.....9475
18.4.11 hsb-group.....9476
18.4.12 hsb-service.....9477
18.4.13 hsb-service-type firewall.....9478
18.4.14 hsb-service-type vpn-instance.....9479
18.4.15 key.....9480
18.4.16 reset firewall hsb statistics event.....9482
18.4.17 reset hsb statistics hsb-group.....9482
18.4.18 reset hsb statistics hsb-service.....9483
18.4.19 service-ip-port.....9484

18.4.20 service-keep-alive detect....9486
18.4.21 track vrrp....9487
18.5 BFD Configuration Commands....9488
18.5.1 authentication-mode (BFD)....9488
18.5.2 bfd....9490
18.5.3 bfd bind peer-ip....9491
18.5.4 bfd bind peer-ip default-ip....9494
18.5.5 bfd bind peer-ip source-ip auto....9497
18.5.6 bfd bind peer-ipv6....9500
18.5.7 bfd bind peer-ipv6 source-ipv6 auto....9503
18.5.8 bfd one-arm-echo....9506
18.5.9 bfd session-name....9509
18.5.10 bfd session nonexistent-config-check....9510
18.5.11 bfd-group....9511
18.5.12 commit....9512
18.5.13 dampening timer-interval....9513
18.5.14 default-ip-address....9515
18.5.15 delay-up....9516
18.5.16 description (BFD session view)....9518
18.5.17 detect-multiplier....9519
18.5.18 discriminator....9520
18.5.19 display bfd configuration....9522
18.5.20 display bfd interface....9530
18.5.21 display bfd session....9531
18.5.22 display bfd statistics....9541
18.5.23 display bfd statistics session....9544
18.5.24 display bfd ttl....9549
18.5.25 display snmp-agent trap feature-name bfd all....9550
18.5.26 min-echo-rx-interval....9552
18.5.27 min-rx-interval....9553
18.5.28 min-tx-interval....9555
18.5.29 multi-hop destination-port....9556
18.5.30 peer-ip ttl....9558
18.5.31 process-interface-status....9560
18.5.32 process-pst....9562
18.5.33 reset bfd statistics....9564
18.5.34 shutdown (BFD session view)....9565
18.5.35 snmp-agent bfd trap-interval....9566
18.5.36 snmp-agent trap enable feature-name bfd....9567
18.5.37 tos-exp....9568
18.5.38 track bfd....9569
18.5.39 unlimited-negotiate....9570

 Copyright © Huawei Technologies Co., Ltd.

18.5.40 wtr....9571
18.5.41 lsp-path-check disable....9572
18.6 VRRP Configuration Commands....9573
18.6.1 direct-route track vrrp....9573
18.6.2 display snmp-agent trap feature-name vrrp all....9575
18.6.3 display vrrp....9577
18.6.4 display vrrp protocol-information....9582
18.6.5 display vrrp state-change interface vrid....9583
18.6.6 display vrrp statistics....9585
18.6.7 display vrrp6....9589
18.6.8 display vrrp6 state-change interface vrid....9593
18.6.9 display vrrp6 statistics....9595
18.6.10 dot1q vrrp....9598
18.6.11 qinq vrrp....9600
18.6.12 reset vrrp statistics....9601
18.6.13 reset vrrp6 statistics....9603
18.6.14 snmp-agent trap enable feature-name vrrp....9604
18.6.15 vrrp advertise send-mode....9606
18.6.16 vrrp arp send-mode simple....9607
18.6.17 vrrp gratuitous-arp timeout....9608
18.6.18 vrrp gratuitous-arp timeout disable....9610
18.6.19 vrrp recover-delay....9611
18.6.20 vrrp smooth-switching timer....9612
18.6.21 vrrp timer-advertise learning enable....9613
18.6.22 vrrp un-check ttl....9615
18.6.23 vrrp version....9616
18.6.24 vrrp version-3 send-packet-mode....9617
18.6.25 vrrp virtual-ip ping enable....9618
18.6.26 vrrp virtual-ip route-advertise disable....9619
18.6.27 vrrp vrid authentication-mode....9621
18.6.28 vrrp vrid preempt-mode disable....9623
18.6.29 vrrp vrid preempt-mode timer delay....9625
18.6.30 vrrp vrid priority....9626
18.6.31 vrrp vrid timer advertise....9628
18.6.32 vrrp vrid track bfd-session....9629
18.6.33 vrrp vrid track interface....9632
18.6.34 vrrp vrid track ip route....9634
18.6.35 vrrp vrid track nqa....9637
18.6.36 vrrp vrid version-3 send-packet-mode....9639
18.6.37 vrrp vrid virtual-ip....9640
18.6.38 vrrp6 nd send-mode simple....9642
18.6.39 vrrp6 un-check hop-limit....9643

18.6.40 vrrp6 vrid preempt-mode disable 9644
18.6.41 vrrp6 vrid preempt-mode timer delay 9645
18.6.42 vrrp6 vrid priority 9647
18.6.43 vrrp6 vrid timer advertise 9648
18.6.44 vrrp6 vrid track bfd-session 9650
18.6.45 vrrp6 vrid track interface 9652
18.6.46 vrrp6 vrid track interface ipv6-state 9654
18.6.47 vrrp6 vrid track ipv6 route 9656
18.6.48 vrrp6 vrid virtual-ip 9658
18.7 EFM Configuration Commands 9660
18.7.1 clear mgr inactive-configuration slot 9660
18.7.2 display efm 9661
18.7.3 display efm link-event local 9667
18.7.4 display efm session 9669
18.7.5 display snmp-agent trap feature-name efm all 9671
18.7.6 display test-packet result 9673
18.7.7 efm enable 9674
18.7.8 efm error-code notification enable 9675
18.7.9 efm error-code period 9677
18.7.10 efm error-code threshold 9678
18.7.11 efm error-frame notification enable 9679
18.7.12 efm error-frame period 9681
18.7.13 efm error-frame threshold 9682
18.7.14 efm error-frame-second notification enable 9683
18.7.15 efm error-frame-second period 9685
18.7.16 efm error-frame-second threshold 9686
18.7.17 efm holdup-timer 9687
18.7.18 efm loopback 9689
18.7.19 efm loopback ignore-request 9691
18.7.20 efm mode 9692
18.7.21 efm packet max-size 9694
18.7.22 efm timeout 9695
18.7.23 efm src-mac 9697
18.7.24 efm threshold-event trigger error-down 9697
18.7.25 efm trigger clear-arp vlan 9699
18.7.26 efm trigger error-down 9700
18.7.27 efm trigger if-down 9702
18.7.28 efm trigger mac-renew 9703
18.7.29 oam-bind efm interface bfd-session 9704
18.7.30 oam-bind efm interface trigger if-down interface 9707
18.7.31 oam-bind ingress bfd-session egress efm interface 9709
18.7.32 oam-bind ingress efm interface egress bfd-session 9712

 Copyright © Huawei Technologies Co., Ltd.

18.7.33 oam-bind ingress efm interface trigger if-down egress interface....9714
18.7.34 oam-bind ingress interface egress efm interface trigger if-down....9717
18.7.35 oam-bind interface efm interface trigger if-down....9720
18.7.36 oam-mgr....9723
18.7.37 snmp-agent trap enable feature-name efm....9724
18.7.38 test-packet start....9725
18.8 CFM Configuration Commands....9727
18.8.1 cfm enable (system view)....9727
18.8.2 active time....9728
18.8.3 alarm finish time....9729
18.8.4 alarm occur time....9730
18.8.5 alarm rdi track-action disable....9732
18.8.6 ccm-interval....9732
18.8.7 cfm md....9734
18.8.8 cfm default md....9737
18.8.9 cfm portid-tlv type....9738
18.8.10 display cfm ma....9739
18.8.11 display cfm md....9742
18.8.12 display cfm default md....9744
18.8.13 display cfm mep....9745
18.8.14 display cfm mp-info....9750
18.8.15 display cfm remote-mep....9753
18.8.16 display oam global configuration....9757
18.8.17 ma....9759
18.8.18 map....9761
18.8.19 mep mep-id....9763
18.8.20 mep alarm disable....9765
18.8.21 oam-bind cfm md ma efm interface....9766
18.8.22 oam-bind interface cfm md ma trigger if-down....9769
18.8.23 oam-bind ingress cfm md ma trigger egress interface....9772
18.8.24 oam-bind ingress cfm md ma egress efm interface....9775
18.8.25 oam-bind ingress efm interface egress cfm md ma....9777
18.8.26 oam-bind ingress interface egress cfm md ma trigger if-down....9780
18.8.27 packet-priority....9783
18.8.28 ping mac-8021ag....9784
18.8.29 remote-mep....9787
18.8.30 remote-mep ccm-receive enable....9788
18.8.31 senderid-tlv-type....9790
18.8.32 trace mac-8021ag....9791
18.8.33 mep ccm-send enable....9795
18.8.34 vlan (default MD view)....9796
18.9 Y.1731 Configuration Commands....9798

18.9.1 delay-measure two-way continual send test-id....9798
18.9.2 delay-measure two-way receive test-id....9800
18.9.3 delay-measure two-way send test-id....9802
18.9.4 display y1731 statistic-type....9805
18.9.5 display y1731 test-info....9809
18.9.6 loss-measure single-ended-synthetic continual send....9811
18.9.7 loss-measure single-ended-synthetic receive....9814
18.9.8 loss-measure single-ended-synthetic send....9816
18.9.9 reset y1731 statistic-type....9818
18.9.10 test-id....9819

19 Security Commands....9822

19.1 AAA Configuration Commands....9823
19.1.1 aaa....9823
19.1.2 aaa abnormal-offline-record....9824
19.1.3 aaa offline-record....9825
19.1.4 aaa online-fail-record....9825
19.1.5 aaa-authen-bypass....9826
19.1.6 aaa-author-bypass....9828
19.1.7 aaa-author-cmd-bypass....9829
19.1.8 aaa-quiet administrator except-list....9830
19.1.9 accounting interim-fail....9832
19.1.10 accounting realtime....9834
19.1.11 accounting start-fail....9836
19.1.12 accounting-copy radius-server....9837
19.1.13 accounting-mode....9838
19.1.14 accounting-scheme (AAA domain view)....9840
19.1.15 accounting-scheme (AAA view)....9841
19.1.16 admin-user privilege level....9843
19.1.17 authentication { roam-accounting | update-ip-accounting } * enable....9846
19.1.18 authentication roam-accounting update-session-mode....9847
19.1.19 authentication-mode (authentication scheme view)....9848
19.1.20 authentication-scheme (AAA domain view)....9850
19.1.21 authentication-scheme (AAA view)....9851
19.1.22 authentication-super....9853
19.1.23 authorization-cmd....9855
19.1.24 authorization-mode....9856
19.1.25 authorization-modify mode....9858
19.1.26 authorization-scheme (AAA domain view)....9860
19.1.27 authorization-scheme (AAA view)....9861
19.1.28 auto-update url (service scheme view)....9863
19.1.29 cmd recording-scheme....9864
19.1.30 cut access-user....9865

19.1.31 dhcp-server group (service scheme view) 9868
19.1.32 display aaa 9869
19.1.33 display aaa configuration 9875
19.1.34 display aaa-quiet administrator except-list 9878
19.1.35 display aaa statistics access-type-authenreq 9879
19.1.36 display aaa statistics offline-reason 9880
19.1.37 display access-user (All views) 9881
19.1.38 display accounting-scheme 9889
19.1.39 display authentication-scheme 9892
19.1.40 display authorization-scheme 9894
19.1.41 display domain 9896
19.1.42 display local-user 9899
19.1.43 display local-user expire-time 9904
19.1.44 display local-aaa-user password policy 9906
19.1.45 display recording-scheme 9908
19.1.46 display remote-user authen-fail 9909
19.1.47 display service-scheme 9912
19.1.48 dns (service scheme view) 9915
19.1.49 dns-name (service scheme view) 9916
19.1.50 domain (AAA view) 9917
19.1.51 domain (system view) 9919
19.1.52 domain-location 9920
19.1.53 domain-name-delimiter 9922
19.1.54 domainname-parse-direction 9923
19.1.55 idle-cut (service scheme view) 9925
19.1.56 ip-pool (service scheme view) 9926
19.1.57 local-aaa-user wrong-password 9928
19.1.58 local-aaa-user password policy access-user 9930
19.1.59 local-aaa-user password policy administrator 9931
19.1.60 local-user 9932
19.1.61 local-user account-type 9939
19.1.62 local-user bind-ip 9941
19.1.63 local-user change-password 9942
19.1.64 local-user expire-date 9943
19.1.65 local-user idle-cut 9944
19.1.66 local-user password 9945
19.1.67 local-user service-type 9947
19.1.68 local-user time-range 9949
19.1.69 outbound recording-scheme 9951
19.1.70 password alert before-expire 9952
19.1.71 password alert original 9953
19.1.72 password expire 9954

19.1.73 password history record number....9956
19.1.74 permit-domain....9957
19.1.75 qos-profile (service scheme view)....9958
19.1.76 recording-mode hwtacacs....9960
19.1.77 recording-scheme....9961
19.1.78 remote-aaa-user authen-fail....9963
19.1.79 remote-user authen-fail unblock....9964
19.1.80 reset aaa....9965
19.1.81 reset aaa statistics access-type-authenreq....9966
19.1.82 reset aaa statistics offline-reason....9967
19.1.83 reset access-user statistics....9968
19.1.84 reset local-user password history record....9968
19.1.85 route set acl....9969
19.1.86 route set interface....9971
19.1.87 security-name enable....9972
19.1.88 security-name-delimiter....9973
19.1.89 service-scheme (aaa domain view)....9974
19.1.90 service-scheme (AAA view)....9975
19.1.91 state (AAA domain view)....9977
19.1.92 statistic enable (AAA domain view)....9978
19.1.93 system recording-scheme....9979
19.1.94 user-group (AAA domain view)....9981
19.1.95 user-password complexity-check....9982
19.1.96 wins (service scheme view)....9983
19.1.97 aaa-author session-timeout invalid-value enable....9984
19.2 RADIUS Configuration Commands....9985
19.2.1 called-station-id mac-format....9985
19.2.2 calling-station-id mac-format....9986
19.2.3 display radius-attribute....9988
19.2.4 display radius-attribute check....9991
19.2.5 display radius-attribute disable....9992
19.2.6 display radius-attribute translate....9994
19.2.7 display radius-server accounting-stop-packet....9995
19.2.8 display radius-server authorization configuration....9997
19.2.9 display radius-server configuration....9999
19.2.10 display radius-server dead-interval dead-count....10004
19.2.11 display radius-server session-manage configuration....10005
19.2.12 display radius-server item....10006
19.2.13 display snmp-agent trap feature-name radius all....10009
19.2.14 radius-attribute check....10010
19.2.15 radius-attribute disable....10012
19.2.16 radius-attribute nas-ip....10013

19.2.17 radius-attribute nas-ipv6 ... 10015
19.2.18 radius-attribute set ... 10016
19.2.19 radius-attribute service-type with-authenonly-reauthen ... 10018
19.2.20 radius-attribute translate ... 10019
19.2.21 radius-server (aaa domain view) ... 10023
19.2.22 radius-server accounting ... 10024
19.2.23 radius-server accounting-stop-packet resend ... 10027
19.2.24 radius-server algorithm ... 10028
19.2.25 radius-server attribute message-authenticator access-request ... 10030
19.2.26 radius-server attribute translate ... 10031
19.2.27 radius-server authentication ... 10032
19.2.28 radius-server authorization ... 10035
19.2.29 radius-server authorization attribute-decode-sameastemplate ... 10038
19.2.30 radius-server authorization attribute-encode-sameastemplate ... 10039
19.2.31 radius-server authorization calling-station-id decode-mac-format ... 10041
19.2.32 radius-server authorization match-type ... 10043
19.2.33 radius-server dead-interval dead-count ... 10044
19.2.34 radius-server detect-server interval ... 10046
19.2.35 radius-server format-attribute ... 10047
19.2.36 radius-server hw-ap-info-format include-ap-ip ... 10050
19.2.37 radius-server nas-identifier-format ... 10051
19.2.38 radius-server nas-port-format ... 10052
19.2.39 radius-server nas-port-id-format ... 10054
19.2.40 radius-server retransmit timeout dead-time ... 10055
19.2.41 radius-server session-manage ... 10057
19.2.42 radius-server shared-key (RADIUS server template view) ... 10059
19.2.43 radius-server shared-key (system view) ... 10061
19.2.44 radius-server template ... 10062
19.2.45 radius-server testuser ... 10064
19.2.46 radius-server traffic-unit ... 10065
19.2.47 radius-server user-name domain-included ... 10066
19.2.48 reset radius-server accounting-stop-packet ... 10067
19.2.49 snmp-agent trap enable feature-name radius ... 10069
19.2.50 test-aaa ... 10070
19.2.51 radius-server dead-detect-condition by-server-ip ... 10073
19.3 HWTACACS Configuration Commands ... 10075
19.3.1 display hwtacacs-server accounting-stop-packet ... 10075
19.3.2 display hwtacacs-server template ... 10076
19.3.3 display hwtacacs-server template verbose ... 10079
19.3.4 hwtacacs enable ... 10087
19.3.5 hwtacacs-server ... 10088
19.3.6 hwtacacs-server accounting ... 10089

19.3.7 hwtacacs-server accounting-stop-packet resend....10092
19.3.8 hwtacacs-server authentication....10093
19.3.9 hwtacacs-server authorization....10096
19.3.10 hwtacacs-server shared-key....10099
19.3.11 hwtacacs-server shared-key (system view)....10101
19.3.12 hwtacacs-server source-ip....10103
19.3.13 hwtacacs-server source-ipv6....10104
19.3.14 hwtacacs-server template....10105
19.3.15 hwtacacs-server timer quiet....10106
19.3.16 hwtacacs-server timer response-timeout....10108
19.3.17 hwtacacs-server traffic-unit....10109
19.3.18 hwtacacs-server user-name domain-included....10110
19.3.19 hwtacacs-user change-password hwtacacs-server....10112
19.3.20 reset hwtacacs-server accounting-stop-packet....10113
19.3.21 reset hwtacacs-server statistics....10114
19.4 HACA Configuration Commands....10115
19.4.1 display haca-server accounting-stop-packet all....10115
19.4.2 display haca-server configuration....10116
19.4.3 display haca-server statistics....10120
19.4.4 haca enable....10126
19.4.5 haca-server (AAA domain view)....10127
19.4.6 haca-server accounting-stop-packet resend....10128
19.4.7 haca-server server-address....10129
19.4.8 haca-server source-ip....10131
19.4.9 haca-server template....10132
19.4.10 haca-server timer down-delay....10133
19.4.11 haca-server timer heart-beat....10134
19.4.12 haca-server timer reconnection....10135
19.4.13 haca-server timer response-timeout....10136
19.4.14 haca-server timer user-syn....10137
19.4.15 haca-server user-name....10138
19.4.16 reset haca-server statistics....10139
19.4.17 reset haca-server accounting-stop-packet all....10140
19.5 DAA Configuration Commands....10141
19.5.1 acl tariff-level....10141
19.5.2 display traffic-group....10143
19.5.3 tariff-level....10145
19.5.4 traffic-group....10146
19.5.5 traffic-group enable....10148
19.6 NAC Configuration Commands....10149
19.6.1 access-domain....10149
19.6.2 access-user arp-detect....10151

19.6.3 access-user arp-detect default ip-address 10153
19.6.4 access-user acl-priviledge-revert 10154
19.6.5 acl-id (user group view) 10155
19.6.6 authentication handshake 10156
19.6.7 authentication authen-fail fail-times 10158
19.6.8 authentication dot1x-mac-bypass 10159
19.6.9 authentication event action authorize 10160
19.6.10 authentication event authen-server-up action re-authen 10162
19.6.11 authentication event client-no-response action authorize 10164
19.6.12 authentication event portal-server-down action authorize 10165
19.6.13 authentication event portal-server-up action re-authen 10167
19.6.14 authentication ip-address in-accounting-start 10168
19.6.15 authentication single-access 10169
19.6.16 authentication timer handshake-period 10170
19.6.17 authentication timer authen-fail-aging 10172
19.6.18 authentication timer pre-authen-aging 10173
19.6.19 authentication timer re-authen 10174
19.6.20 authentication roam pre-authen mac-authen enable 10176
19.6.21 authentication mode 10177
19.6.22 authentication speed-limit auto 10179
19.6.23 authentication termination-action reauthenticate 10180
19.6.24 authentication trigger-condition (802.1X authentication) 10181
19.6.25 authentication trigger-condition (MAC address authentication) 10183
19.6.26 authentication-profile (Interface view or VAP profile view) 10184
19.6.27 authentication-profile (system view) 10186
19.6.28 cut web-authentication-user 10188
19.6.29 display access-user 10189
19.6.30 display authentication interface 10191
19.6.31 display authentication-profile configuration 10192
19.6.32 display dot1x 10200
19.6.33 display dot1x-access-profile configuration 10204
19.6.34 display dot1x quiet-user 10208
19.6.35 display free-rule-template configuration 10209
19.6.36 display mac-address authen 10210
19.6.37 display mac-address pre-authen 10212
19.6.38 display mac-access-profile configuration 10214
19.6.39 display mac-authen 10219
19.6.40 display mac-authen quiet-user 10225
19.6.41 display portal 10226
19.6.42 display portal local-server connect 10229
19.6.43 display portal local-server 10231
19.6.44 display portal local-server page-information 10235

 Copyright © Huawei Technologies Co., Ltd.

19.6.45 display portal-access-profile configuration 10236
19.6.46 display portal quiet-user 10239
19.6.47 display portal url-encode configuration 10240
19.6.48 display portal user-logout 10241
19.6.49 display server-detect state 10243
19.6.50 display url-template 10245
19.6.51 display user-group 10248
19.6.52 display web-auth-server configuration 10250
19.6.53 display snmp-agent trap feature-name mid_eapol all 10254
19.6.54 display snmp-agent trap feature-name mid_web all 10256
19.6.55 dot1x authentication-method 10257
19.6.56 dot1x eap-notify-packet 10260
19.6.57 dot1x handshake 10261
19.6.58 dot1x mc-trigger 10262
19.6.59 dot1x mc-trigger port-up-send enable 10263
19.6.60 dot1x quiet-period 10264
19.6.61 dot1x quiet-times 10265
19.6.62 dot1x reauthenticate mac-address 10266
19.6.63 dot1x reauthenticate 10267
19.6.64 dot1x retry 10268
19.6.65 dot1x timer 10270
19.6.66 dot1x timer quiet-period 10272
19.6.67 dot1x trigger dhcp-binding 10273
19.6.68 dot1x timer mac-bypass-delay 10275
19.6.69 dot1x timer tx-period 10276
19.6.70 dot1x unicast-trigger 10277
19.6.71 dot1x url 10278
19.6.72 dot1x-access-profile (authentication profile view) 10279
19.6.73 dot1x-access-profile (system view) 10281
19.6.74 dot1x port-control 10282
19.6.75 free-rule 10285
19.6.76 free-rule-template (authentication profile view) 10287
19.6.77 free-rule-template (system view) 10288
19.6.78 http get-method enable 10289
19.6.79 http-method post 10290
19.6.80 force-push 10295
19.6.81 link-down offline delay 10297
19.6.82 mac-access-profile (authentication profile view) 10298
19.6.83 mac-access-profile (system view) 10299
19.6.84 mac-authen authentication-method 10301
19.6.85 mac-authen domain 10302
19.6.86 mac-authen permit mac-address 10304

19.6.87 mac-authen quiet-times....10305
19.6.88 mac-authen reauthenticate mac-address....10306
19.6.89 mac-authen reauthenticate....10307
19.6.90 mac-authen timer quiet-period....10308
19.6.91 mac-authen timer reauthenticate-period....10310
19.6.92 mac-authen trigger dhcp-binding....10311
19.6.93 mac-authen username....10313
19.6.94 nginx proxy port....10317
19.6.95 nginx enable....10318
19.6.96 nginx load....10319
19.6.97 parameter....10321
19.6.98 port (Portal server profile view)....10322
19.6.99 portal auth-network....10324
19.6.100 portal captive-adaptive enable....10325
19.6.101 portal captive-bypass enable....10327
19.6.102 portal https-redirect enable....10328
19.6.103 portal local-server ad-image load....10329
19.6.104 portal local-server authentication-method....10331
19.6.105 portal local-server background-color....10332
19.6.106 portal local-server background-image load....10333
19.6.107 portal local-server enable....10335
19.6.108 portal local-server ip....10336
19.6.109 portal local-server keep-alive....10338
19.6.110 portal local-server load....10339
19.6.111 portal local-server logo load....10341
19.6.112 portal local-server....10343
19.6.113 portal local-server page-text load....10345
19.6.114 portal local-server policy-text load....10346
19.6.115 portal local-server syslog-limit enable....10348
19.6.116 portal local-server syslog-limit period....10349
19.6.117 portal local-server timer session-timeout....10350
19.6.118 portal logout different-server enable....10351
19.6.119 portal logout resend timeout....10352
19.6.120 portal max-user....10354
19.6.121 portal quiet-period....10354
19.6.122 portal quiet-times....10355
19.6.123 portal timer quiet-period....10356
19.6.124 portal timer offline-detect....10357
19.6.125 portal user-alarm percentage....10359
19.6.126 portal web-authen-server....10360
19.6.127 protocol....10362
19.6.128 portal url-encode enable....10363

19.6.129 portal-access-profile (authentication profile view) 10364
19.6.130 portal-access-profile (system view) 10366
19.6.131 redirect web-authentication-user 10367
19.6.132 remark 10369
19.6.133 reset dot1x statistics 10370
19.6.134 reset mac-authen statistics 10372
19.6.135 server-detect 10373
19.6.136 server-ip (Portal server profile view) 10375
19.6.137 shared-key (Portal server profile view) 10377
19.6.138 source-interface (Portal server template view) 10378
19.6.139 source-ip (Portal server profile view) 10379
19.6.140 snmp-agent trap enable feature-name mid_eapol 10380
19.6.141 snmp-agent trap enable feature-name mid_web 10382
19.6.142 url (URL template view) 10384
19.6.143 url (Portal server profile view) 10385
19.6.144 url-parameter mac-address format 10386
19.6.145 url-parameter 10387
19.6.146 url-parameter set 10391
19.6.147 url-template name 10393
19.6.148 url-template (Portal server profile view) 10394
19.6.149 user-sync 10395
19.6.150 user-group 10396
19.6.151 user-isolated 10398
19.6.152 user-vlan 10399
19.6.153 vpn-instance (Portal server template view) 10400
19.6.154 web-auth-server listening-port 10402
19.6.155 web-auth-server (Portal access profile view) 10403
19.6.156 web-auth-server reply-message 10405
19.6.157 web-auth-server (system view) 10406
19.6.158 web-auth-server version 10408
19.6.159 web-redirection disable (Portal server profile view) 10409
19.6.160 web-service aaa server 10410
19.6.161 web-service access enable 10412
19.6.162 web-service accounting enable 10413
19.6.163 web-service accounting interval 10414
19.7 ACL Configuration Commands 10415
19.7.1 acl ipv6 name 10415
19.7.2 acl ipv6 (system view) 10418
19.7.3 acl name 10420
19.7.4 acl (system view) 10423
19.7.5 acl logging 10426
19.7.6 description 10427

19.7.7 display acl....10429
19.7.8 display acl ipv6....10431
19.7.9 display acl resource....10433
19.7.10 display time-range....10435
19.7.11 ip port-set....10437
19.7.12 port (port set view)....10438
19.7.13 reset acl counter....10440
19.7.14 reset acl ipv6 counter....10441
19.7.15 reset acl logging....10443
19.7.16 rule (advanced ACL view)....10443
19.7.17 rule (advanced ACL6 view)....10456
19.7.18 rule (basic ACL view)....10465
19.7.19 rule (basic ACL6 view)....10469
19.7.20 rule (layer 2 ACL view)....10472
19.7.21 rule (user ACL view)....10477
19.7.22 rule description....10486
19.7.23 step....10488
19.7.24 time-range....10489
19.8 Firewall Configuration Commands....10494
19.8.1 bypass....10494
19.8.2 clear firewall statistics system....10495
19.8.3 clear firewall statistics zone....10496
19.8.4 detect aspf....10497
19.8.5 display firewall app session table....10498
19.8.6 display firewall app table statistics....10500
19.8.7 display firewall blacklist....10501
19.8.8 display firewall blacklist configuration....10503
19.8.9 display firewall defend....10504
19.8.10 display firewall interzone....10507
19.8.11 display firewall ipv6 session....10509
19.8.12 display firewall log configuration....10511
19.8.13 display firewall session....10513
19.8.14 display firewall statistics system....10515
19.8.15 display firewall statistics zone....10521
19.8.16 display firewall statistics zone-ip....10523
19.8.17 display firewall whitelist....10524
19.8.18 display firewall zone....10525
19.8.19 display firewall-nat session aging-time....10527
19.8.20 display port-mapping....10529
19.8.21 display session....10531
19.8.22 firewall blacklist....10534
19.8.23 firewall blacklist enable....10535

19.8.24 firewall black-white-list load configuration-file 10536
19.8.25 firewall black-white-list save configuration-file 10537
19.8.26 firewall defend all enable 10538
19.8.27 firewall defend fraggle enable 10539
19.8.28 firewall defend icmp-flood 10540
19.8.29 firewall defend icmp-flood enable 10542
19.8.30 firewall defend icmp-redirect enable 10543
19.8.31 firewall defend icmp-unreachable enable 10544
19.8.32 firewall defend ip-fragment enable 10544
19.8.33 firewall defend ip-sweep 10545
19.8.34 firewall defend ip-sweep enable 10547
19.8.35 firewall defend land enable 10548
19.8.36 firewall defend large-icmp 10549
19.8.37 firewall defend large-icmp enable 10550
19.8.38 firewall defend ping-of-death enable 10551
19.8.39 firewall defend port-scan 10552
19.8.40 firewall defend port-scan enable 10553
19.8.41 firewall defend smurf enable 10554
19.8.42 firewall defend syn-flood 10555
19.8.43 firewall defend syn-flood enable 10557
19.8.44 firewall defend tcp-flag enable 10558
19.8.45 firewall defend teardrop enable 10559
19.8.46 firewall defend tracert enable 10559
19.8.47 firewall defend udp-flood 10560
19.8.48 firewall defend udp-flood enable 10562
19.8.49 firewall defend winnuke enable 10563
19.8.50 firewall enable 10564
19.8.51 firewall interzone 10564
19.8.52 firewall log binary-log host 10566
19.8.53 firewall log enable 10567
19.8.54 firewall log log-interval 10569
19.8.55 firewall log session nat enable 10570
19.8.56 firewall statistics system connect-number 10571
19.8.57 firewall statistics system enable 10574
19.8.58 firewall whitelist 10575
19.8.59 firewall zone 10576
19.8.60 firewall-nat session aging-time 10577
19.8.61 packet-filter 10580
19.8.62 packet-filter ipv6 10582
19.8.63 packet-filter logging 10583
19.8.64 port-mapping 10585
19.8.65 priority (security zone view) 10587

19.8.66 reset firewall app table statistics 10589
19.8.67 reset firewall ipv6 session all 10590
19.8.68 reset firewall session 10591
19.8.69 reset session 10593
19.8.70 reset firewall statistics system defend 10595
19.8.71 session-log 10596
19.8.72 statistics connect-number ip 10597
19.8.73 statistics connect-number zone 10602
19.8.74 statistics ip enable 10606
19.8.75 statistics zone enable 10607
19.8.76 zone 10608
19.9 Deep Security Configuration Commands 10609
19.9.1 Security Policy Configuration Commands 10609
19.9.1.1 display engine information 10610
19.9.1.2 display security-policy 10611
19.9.1.3 display update configuration 10613
19.9.1.4 display update information all-sdb 10615
19.9.1.5 display update host source 10617
19.9.1.6 display update status 10618
19.9.1.7 display version (security policy) 10619
19.9.1.8 engine configuration commit 10621
19.9.1.9 engine enable 10622
19.9.1.10 engine enhanced-detection 10623
19.9.1.11 engine log enable 10623
19.9.1.12 engine log timeout 10624
19.9.1.13 engine pass-through enable 10625
19.9.1.14 profile (security policy view) 10626
19.9.1.15 security-policy 10629
19.9.1.16 security-policy (interzone view) 10631
19.9.1.17 update abort 10632
19.9.1.18 update apply 10633
19.9.1.19 update confirm 10633
19.9.1.20 update force apply 10634
19.9.1.21 update force local 10635
19.9.1.22 update force online 10637
19.9.1.23 update force restore sdb-default 10638
19.9.1.24 update force rollback 10639
19.9.1.25 update host source 10640
19.9.1.26 update local 10641
19.9.1.27 update online 10642
19.9.1.28 update online-mode 10643
19.9.1.29 update proxy 10644

19.9.1.30 update proxy enable 10646
19.9.1.31 update restore sdb-default 10647
19.9.1.32 update rollback 10648
19.9.1.33 update schedule 10648
19.9.1.34 update schedule enable 10650
19.9.1.35 update schedule retry-download interval 10651
19.9.1.36 update schedule retry-load interval 10652
19.9.1.37 update server 10653
19.9.2 Intrusion Prevention Configuration Commands 10654
19.9.2.1 action (IPS signature filter view) 10654
19.9.2.2 action (user-defined IPS signature view) 10655
19.9.2.3 application (IPS signature filter view) 10656
19.9.2.4 assoc-check enable 10657
19.9.2.5 category (IPS signature filter view) 10658
19.9.2.6 check (user-defined signature rule view) 10660
19.9.2.7 cnc domain-filter enable 10661
19.9.2.8 cnc domain-filter exception domain-name 10662
19.9.2.9 collect-attack-evidence enable (intrusion prevention profile view) 10663
19.9.2.10 condition (user-defined signature rule view) 10664
19.9.2.11 condition associated (user-defined signature rule view) 10668
19.9.2.12 condition move (user-defined signature rule view) 10670
19.9.2.13 context-awareness enable 10671
19.9.2.14 description (intrusion prevention profile view) 10672
19.9.2.15 description (user-defined IPS signature view) 10673
19.9.2.16 destination-ip (user-defined signature rule view) 10674
19.9.2.17 destination-port (user-defined signature rule view) 10675
19.9.2.18 display cnc domain-filter domain statistics 10676
19.9.2.19 display cnc domain-filter exception 10678
19.9.2.20 display cnc domain-filter statistics 10679
19.9.2.21 display context-awareness information statistics 10680
19.9.2.22 display context-awareness statistics 10681
19.9.2.23 display decoding statistics 10683
19.9.2.24 display ips signature-id rule 10684
19.9.2.25 display ips signature-state 10686
19.9.2.26 display ips statistics 10688
19.9.2.27 display ips-signature 10689
19.9.2.28 display ips-signature cve-id 10695
19.9.2.29 display ips-signature statistics 10697
19.9.2.30 display ips-signature vendor-id 10698
19.9.2.31 display profile type ips 10699
19.9.2.32 dns domain check 10707
19.9.2.33 dns domain length check 10708

19.9.2.34 dns malformed-packet check 10709
19.9.2.35 dns request-type check 10710
19.9.2.36 dns session request-times check 10711
19.9.2.37 exception ips-signature-id 10712
19.9.2.38 http multi-host check 10714
19.9.2.39 http ssh-over-http check 10715
19.9.2.40 http x-forwarded-for check 10716
19.9.2.41 http x-forwarded-for whitelist 10717
19.9.2.42 ips associated pre-defined 10718
19.9.2.43 ips collect-attack-evidence max-session-number 10719
19.9.2.44 http x-online-host blacklist 10721
19.9.2.45 http x-online-host check 10722
19.9.2.46 ips log based-on-session 10723
19.9.2.47 ips log merge enable 10724
19.9.2.48 ips signature-id 10724
19.9.2.49 ips signature-state 10725
19.9.2.50 name (user-defined IPS signature view) 10728
19.9.2.51 os (IPS signature filter view) 10729
19.9.2.52 profile type ips copy 10730
19.9.2.53 profile type ips name 10731
19.9.2.54 protocol (IPS signature filter view) 10732
19.9.2.55 protocol (user-defined IPS signature view) 10733
19.9.2.56 rename (IPS signature filter view) 10734
19.9.2.57 rename (user-defined signature rule view) 10735
19.9.2.58 rename (intrusion prevention profile view) 10736
19.9.2.59 reset cnc domain-filter statistics 10737
19.9.2.60 reset context-awareness information statistics 10738
19.9.2.61 reset context-awareness statistics 10739
19.9.2.62 reset decoding statistics 10740
19.9.2.63 reset ips statistic 10740
19.9.2.64 reset ips-signature statistics 10741
19.9.2.65 rule name (user-defined IPS signature view) 10742
19.9.2.66 scope (user-defined signature rule view) 10743
19.9.2.67 severity (IPS signature filter view) 10744
19.9.2.68 severity (user-defined IPS signature view) 10746
19.9.2.69 signature-set move 10747
19.9.2.70 signature-set name 10748
19.9.2.71 source-ip (user-defined signature rule view) 10749
19.9.2.72 source-port (user-defined signature rule view) 10750
19.9.2.73 target (IPS signature filter view) 10751
19.9.2.74 target (user-defined IPS signature view) 10752
19.9.3 URL Filtering Configuration Commands 10753

19.9.3.1 add { blacklist | whitelist } (URL filtering profile view) 10753
19.9.3.2 add { url | host } (predefined URL category view) 10757
19.9.3.3 add { url | host } (user-defined URL category view) 10763
19.9.3.4 add referer-host 10768
19.9.3.5 category action (URL filtering profile view) 10769
19.9.3.6 category action mode (URL filtering profile view) 10770
19.9.3.7 category pre-defined control-level (URL filtering profile view) 10771
19.9.3.8 default action (URL filtering profile view) 10772
19.9.3.9 description (URL filtering profile view) 10773
19.9.3.10 description (user-defined URL category view) 10774
19.9.3.11 display profile type url-filter 10775
19.9.3.12 display url-filter category 10779
19.9.3.13 display url-filter category pre-defined control-level 10785
19.9.3.14 display url-filter category statistics 10786
19.9.3.15 display url-filter statistics 10788
19.9.3.16 https-filter enable 10789
19.9.3.17 import url-sdb file 10790
19.9.3.18 profile type url-filter copy 10791
19.9.3.19 profile type url-filter name 10792
19.9.3.20 referer-filter whitelist-all enable 10793
19.9.3.21 rename (URL filtering profile view) 10794
19.9.3.22 rename (user-defined URL category view) 10795
19.9.3.23 reset url-filter category statistics 10796
19.9.3.24 reset url-filter statistics 10797
19.9.3.25 url-filter anti-bypass enable 10798
19.9.3.26 url-filter category pre-defined copy 10799
19.9.3.27 url-filter category pre-defined subcategory-id 10800
19.9.3.28 url-filter category user-defined copy 10801
19.9.3.29 url-filter category user-defined name 10802
19.9.3.30 url-filter https-filter consistency-check enable 10803
19.9.3.31 web-url-filter user-set 10804
19.9.3.32 enable web-url-filter user-set 10806
19.9.4 Deep Security Maintenance Commands 10808
19.9.4.1 display engine session statistic 10808
19.9.4.2 display engine session table 10809
19.9.4.3 display engine statistic 10811
19.9.4.4 display file-frame information 10812
19.9.4.5 display fragment-reassemble configuration 10814
19.9.4.6 display fragment-reassemble session table 10815
19.9.4.7 display profile 10817
19.9.4.8 display stream-reassemble configuration 10818
19.9.4.9 fragment-reassemble enable 10820

19.9.4.10 fragment-reassemble overflow-mode 10821
19.9.4.11 fragment-reassemble user-configure 10821
19.9.4.12 fragment-reassemble user-configure defense-check 10822
19.9.4.13 reset engine session statistic 10823
19.9.4.14 reset engine session table 10824
19.9.4.15 reset engine statistic 10825
19.9.4.16 reset fragment-reassemble statistic 10826
19.9.4.17 stream-reassemble enable 10826
19.9.4.18 stream-reassemble enhanced-mode 10827
19.9.4.19 stream-reassemble overflow-mode 10828
19.9.4.20 stream-reassemble overlap-mode 10829
19.9.4.21 stream-reassemble session-cache 10830
19.9.4.22 stream-reassemble session-timeout 10831
19.9.4.23 stream-reassemble tcp-option check 10831
19.9.4.24 stream-reassemble timestamp check 10832
19.9.4.25 stream-reassemble user-configure defense-check 10833
19.10 Local Attack Defense Configuration Commands 10834
19.10.1 application-apperceive 10834
19.10.2 auto-defend enable 10836
19.10.3 auto-defend action 10837
19.10.4 auto-defend alarm enable 10839
19.10.5 auto-defend alarm threshold 10840
19.10.6 auto-defend protocol 10841
19.10.7 auto-defend threshold 10844
19.10.8 auto-defend trace-type 10845
19.10.9 blacklist 10846
19.10.10 cpu-defend application-apperceive enable 10848
19.10.11 cpu-defend policy 10850
19.10.12 cpu-defend-policy 10851
19.10.13 deny 10853
19.10.14 description (attack defense policy view) 10854
19.10.15 display auto-defend attack-source 10855
19.10.16 display auto-defend configuration 10858
19.10.17 display cpu-defend configuration 10860
19.10.18 display cpu-defend policy 10861
19.10.19 display cpu-defend rate-adaption statistics 10864
19.10.20 display cpu-defend statistics 10865
19.10.21 packet-type 10867
19.10.22 packet-type priority 10869
19.10.23 rate-adaption adjust-period 10870
19.10.24 rate-adaption adjust-step 10871
19.10.25 rate-adaption cpu-usage threshold 10872

 Copyright © Huawei Technologies Co., Ltd.

19.10.26 rate-adaption enable 10874
19.10.27 rate-adaption exception packet-type 10875
19.10.28 rate-limit all-packets 10876
19.10.29 reset auto-defend attack-source 10877
19.10.30 reset cpu-defend statistics 10878
19.11 Attack Defense Configuration Commands 10879
19.11.1 anti-attack abnormal enable 10879
19.11.2 anti-attack enable 10881
19.11.3 anti-attack fragment enable 10882
19.11.4 anti-attack fragment car 10883
19.11.5 anti-attack icmp-flood enable 10884
19.11.6 anti-attack icmp-flood car 10885
19.11.7 anti-attack tcp-syn enable 10887
19.11.8 anti-attack tcp-syn car 10888
19.11.9 anti-attack udp-flood enable 10889
19.11.10 anti-attack urpf 10890
19.11.11 display anti-attack statistics 10891
19.11.12 reset anti-attack statistics 10893
19.12 Traffic Suppression Configuration Commands 10895
19.12.1 broadcast-suppression (interface view) 10895
19.12.2 broadcast-suppression (system view) 10897
19.12.3 display flow-suppression interface 10898
19.12.4 flood-suppression (interface view) 10899
19.12.5 icmp rate-limit 10901
19.12.6 icmp rate-limit enable 10902
19.12.7 multicast-suppression (interface view) 10903
19.12.8 multicast-suppression (system view) 10905
19.12.9 unicast-suppression (interface view) 10906
19.12.10 unicast-suppression (system view) 10908
19.13 ARP Security Configuration Commands 10909
19.13.1 arp anti-attack check user-bind alarm enable 10910
19.13.2 arp anti-attack check user-bind alarm threshold 10911
19.13.3 arp anti-attack check user-bind check-item (interface view) 10912
19.13.4 arp anti-attack check user-bind check-item (VLAN view) 10914
19.13.5 arp anti-attack check user-bind enable 10915
19.13.6 arp anti-attack entry-check enable 10916
19.13.7 arp anti-attack gateway-duplicate enable 10918
19.13.8 arp anti-attack log-trap-timer 10919
19.13.9 arp anti-attack packet-check sender-mac 10921
19.13.10 arp anti-attack rate-limit 10922
19.13.11 arp anti-attack rate-limit alarm enable 10924
19.13.12 arp anti-attack rate-limit alarm threshold 10925

19.13.13 arp anti-attack rate-limit enable....10926
19.13.14 arp gratuitous-arp send enable....10927
19.13.15 arp gratuitous-arp send interval....10928
19.13.16 arp learning dhcp-trigger....10929
19.13.17 arp learning strict (interface view)....10931
19.13.18 arp learning strict (system view)....10932
19.13.19 arp speed-limit flood-rate....10933
19.13.20 arp speed-limit source-mac....10935
19.13.21 arp speed-limit source-ip....10936
19.13.22 arp validate (interface view)....10938
19.13.23 arp-fake expire-time....10939
19.13.24 arp-limit....10941
19.13.25 arp-miss anti-attack rate-limit....10944
19.13.26 arp-miss anti-attack rate-limit alarm enable....10946
19.13.27 arp-miss anti-attack rate-limit alarm threshold....10947
19.13.28 arp-miss anti-attack rate-limit enable....10948
19.13.29 arp-miss speed-limit source-ip....10949
19.13.30 display arp anti-attack check user-bind interface....10951
19.13.31 display arp anti-attack configuration....10952
19.13.32 display arp anti-attack gateway-duplicate item....10957
19.13.33 display arp flood statistics....10958
19.13.34 display arp learning strict....10959
19.13.35 display arp packet statistics....10960
19.13.36 display arp-limit....10962
19.13.37 reset arp anti-attack statistics check user-bind....10963
19.13.38 reset arp anti-attack statistics rate-limit....10964
19.13.39 reset arp flood statistics....10965
19.13.40 reset arp packet statistics....10966
19.14 DHCP Snooping Configuration Commands....10967
19.14.1 arp dhcp-snooping-detect enable....10967
19.14.2 dhcp option82 enable....10968
19.14.3 dhcp option82 format....10970
19.14.4 dhcp server detect....10976
19.14.5 dhcp snooping alarm enable....10977
19.14.6 dhcp snooping alarm threshold....10979
19.14.7 dhcp snooping check dhcp-giaddr enable....10981
19.14.8 dhcp snooping check mac-address enable....10983
19.14.9 dhcp snooping check user-bind enable....10984
19.14.10 dhcp snooping disable....10986
19.14.11 dhcp snooping enable....10987
19.14.12 dhcp snooping enable no-user-binding....10989
19.14.13 dhcp snooping max-user-number....10991

 Copyright © Huawei Technologies Co., Ltd.

19.14.14 dhcp snooping trusted 10992
19.14.15 dhcp snooping user-alarm percentage 10994
19.14.16 dhcp snooping user-bind autosave 10995
19.14.17 dhcp snooping user-transfer enable 10997
19.14.18 dhcpv6 interface-id format 10998
19.14.19 dhcpv6 option18 format 11001
19.14.20 dhcpv6 option37 format 11005
19.14.21 dhcpv6 { option18 | option37 } enable 11009
19.14.22 dhcpv6 snooping relay-information enable 11010
19.14.23 display dhcp option82 configuration 11012
19.14.24 display dhcp snooping 11014
19.14.25 display dhcp snooping configuration 11019
19.14.26 display dhcp snooping statistics 11020
19.14.27 display dhcp snooping user-bind 11022
19.14.28 display dhcpv6 snooping user-bind 11025
19.14.29 reset dhcp snooping statistics 11028
19.14.30 reset dhcp snooping user-bind 11029
19.14.31 dhcp option82 encapsulation 11031
19.14.32 dhcp option82 subscriber-id format 11032
19.15 IP Source Guard Configuration Commands 11033
19.15.1 **display dhcp static user-bind** 11033
19.15.2 display dhcpv6 static user-bind 11036
19.15.3 display ip source check user-bind 11038
19.15.4 ip source check user-bind check-item (interface view) 11039
19.15.5 ip source check user-bind check-item (VLAN view) 11041
19.15.6 ip source check user-bind enable 11042
19.15.7 user-bind static 11043
19.16 URPF Configuration Commands 11045
19.16.1 ipv6 urpf 11045
19.16.2 urpf (interface view) 11047
19.17 PKI Configuration Commands 11049
19.17.1 auto-enroll 11049
19.17.2 ca-name 11051
19.17.3 ca id 11052
19.17.4 cdp-url 11053
19.17.5 certificate-check 11054
19.17.6 certificate auto-update enable 11057
19.17.7 certificate update expire-time 11058
19.17.8 cmp-request authentication-cert 11059
19.17.9 cmp-request ca-name 11060
19.17.10 cmp-request entity 11061
19.17.11 cmp-request message-authentication-code 11062

19.17.12 cmp-request origin-authentication-method....11063
19.17.13 cmp-request realm....11064
19.17.14 cmp-request rsa local-key-pair....11065
19.17.15 cmp-request server url....11067
19.17.16 cmp-request verification-cert....11068
19.17.17 common-name....11069
19.17.18 country (PKI entity view)....11070
19.17.19 crl auto-update enable....11072
19.17.20 crl cache....11072
19.17.21 crl http....11073
19.17.22 crl ldap....11074
19.17.23 crl scep....11075
19.17.24 crl update-period....11076
19.17.25 display ldap-server template....11077
19.17.26 display pki ca-capability....11078
19.17.27 display pki cert-req....11080
19.17.28 display pki certificate....11083
19.17.29 display pki certificate built-in-ca....11086
19.17.30 display pki certificate enroll-status....11090
19.17.31 display pki certificate filename....11092
19.17.32 display pki cmp statistics....11094
19.17.33 display pki credential-storage-path....11096
19.17.34 display pki crl....11097
19.17.35 display pki entity....11099
19.17.36 display pki ocsp cache detail....11101
19.17.37 display pki ocsp cache statistics....11103
19.17.38 display pki ocsp server down-information....11105
19.17.39 display pki peer-certificate....11106
19.17.40 display pki realm....11109
19.17.41 display pki rsa built-in-ca public....11113
19.17.42 display pki rsa local-key-pair....11115
19.17.43 display pki sm2 local-key-pair public (System view)....11117
19.17.44 email....11119
19.17.45 enrollment self-signed....11120
19.17.46 enrollment-request specific....11121
19.17.47 enrollment-request signature message-digest-method....11122
19.17.48 enrollment-url....11123
19.17.49 entity....11125
19.17.50 extension-request enterprise....11126
19.17.51 fingerprint....11127
19.17.52 fqdn....11129
19.17.53 ip-address....11130

19.17.54 key-usage....11132
19.17.55 ldap-server authentication....11133
19.17.56 ldap-server authentication manager....11134
19.17.57 ldap-server authentication manager-password....11136
19.17.58 ldap-server template....11138
19.17.59 ldap-server-template....11139
19.17.60 ldap-server (PKI realm view)....11140
19.17.61 locality....11142
19.17.62 ocsp nonce enable....11143
19.17.63 ocsp signature enable....11144
19.17.64 ocsp url....11145
19.17.65 ocsp-url from-ca....11146
19.17.66 organization-unit....11147
19.17.67 organization....11148
19.17.68 password (PKI realm view)....11149
19.17.69 pki built-in-ca match-rsa-key....11151
19.17.70 pki cmp certificate-request session....11152
19.17.71 pki cmp initial-request session....11153
19.17.72 pki cmp keyupdate-request session....11154
19.17.73 pki cmp session....11155
19.17.74 pki create-certificate....11156
19.17.75 pki delete-certificate....11158
19.17.76 pki delete-certificate built-in-ca....11158
19.17.77 pki delete-crl....11159
19.17.78 pki enroll-certificate....11160
19.17.79 pki entity....11162
19.17.80 pki export-certificate....11164
19.17.81 pki export-certificate default....11165
19.17.82 pki export built-in-ca rsa-key-pair....11166
19.17.83 pki export rsa-key-pair....11169
19.17.84 pki export sm2-key-pair....11171
19.17.85 pki file-format....11173
19.17.86 pki generate built-in-ca certificate....11174
19.17.87 pki get-certificate....11176
19.17.88 pki get-crl....11177
19.17.89 pki http....11178
19.17.90 pki import-certificate....11179
19.17.91 pki import-certificate built-in-ca....11184
19.17.92 pki import-certificate peer....11185
19.17.93 pki import-crl....11187
19.17.94 pki import built-in-ca rsa-key-pair....11189
19.17.95 pki import rsa-key-pair....11190

19.17.96 pki import sm2-key-pair 11192
19.17.97 pki ldap 11194
19.17.98 pki match-rsa-key 11195
19.17.99 pki match-sm2-key 11196
19.17.100 pki ocsp response cache enable 11197
19.17.101 pki ocsp response cache number 11198
19.17.102 pki ocsp response cache refresh interval 11199
19.17.103 pki realm (system view) 11200
19.17.104 pki release-certificate peer 11201
19.17.105 pki rsa built-in-ca 11202
19.17.106 pki rsa local-key-pair create 11204
19.17.107 pki rsa local-key-pair destroy 11206
19.17.108 pki set-certificate expire-prewarning 11207
19.17.109 pki sm2 local-key-pair create 11208
19.17.110 pki sm2 local-key-pair destroy 11209
19.17.111 pki validate ocsp-server-certificate enable 11210
19.17.112 pki validate-certificate 11211
19.17.113 reset pki cmp statistics 11212
19.17.114 reset pki ocsp response cache 11213
19.17.115 reset pki ocsp server down-information 11213
19.17.116 rsa local-key-pair 11215
19.17.117 serial-number 11216
19.17.118 sm2 local-key-pair 11217
19.17.119 source interface 11218
19.17.120 state (PKI entity view) 11219
19.17.121 undo pki cmp poll-request session 11221
19.17.122 validate time disable 11222
19.17.123 vpn-instance 11223
19.18 SSL Configuration Commands 11224
19.18.1 ciphersuite 11224
19.18.2 display ssl connection statistics 11228
19.18.3 display ssl policy 11229
19.18.4 pki-realm 11232
19.18.5 prefer-ciphersuite 11234
19.18.6 renegotiation enable 11237
19.18.7 reset ssl connection statistics 11239
19.18.8 server-verify enable 11239
19.18.9 session 11240
19.18.10 ssl policy 11242
19.18.11 ssl renegotiation-rate 11243
19.18.12 version (Client SSL policy view) 11244
19.18.13 version (server SSL policy view) 11246

19.19 HTTPS Configuration Commands.....11248
19.19.1 http secure-client ssl-policy.....11248
19.19.2 http secure-server enable.....11249
19.19.3 http secure-server manager-port.....11250
19.19.4 http secure-server ssl-policy.....11251
19.19.5 http secure-server port.....11252
19.20 Keychain Configuration Commands.....11253
19.20.1 algorithm.....11253
19.20.2 default send-key-id.....11256
19.20.3 display keychain.....11257
19.20.4 keychain.....11264
19.20.5 key-id.....11266
19.20.6 key-string.....11268
19.20.7 receive-time.....11270
19.20.8 receive-tolerance.....11273
19.20.9 send-time.....11274
19.20.10 tcp-algorithm-id.....11277
19.20.11 tcp-kind.....11279
19.20.12 time mode.....11281

20 QoS Commands.....11283

20.1 MQC Configuration Commands.....11283
20.1.1 classifier behavior.....11283
20.1.2 display traffic behavior.....11286
20.1.3 display traffic classifier.....11288
20.1.4 display traffic policy.....11290
20.1.5 display traffic policy statistics.....11293
20.1.6 display traffic policy statistics bridge-domain.....11300
20.1.7 display traffic policy statistics global.....11304
20.1.8 display traffic-policy applied-record.....11308
20.1.9 if-match 8021p.....11311
20.1.10 if-match acl.....11312
20.1.11 if-match any.....11314
20.1.12 if-match cvlan-8021p.....11315
20.1.13 if-match cvlan-id.....11317
20.1.14 if-match destination-mac.....11319
20.1.15 if-match dlci.....11321
20.1.16 if-match dscp.....11323
20.1.17 if-match fr-de.....11325
20.1.18 if-match inbound-interface.....11327
20.1.19 if-match ip-precedence.....11328
20.1.20 if-match l2-protocol.....11329
20.1.21 if-match mpls-exp.....11331

20.1.22 if-match outbound-interface....11333
20.1.23 if-match packet-length....11334
20.1.24 if-match protocol....11336
20.1.25 if-match qos-group....11337
20.1.26 if-match rtp....11338
20.1.27 if-match source-mac....11340
20.1.28 if-match tcp....11342
20.1.29 if-match user-set....11344
20.1.30 if-match vlan-id....11345
20.1.31 if-match pvc....11347
20.1.32 ip netstream sampler (traffic behavior view)....11348
20.1.33 qos pre-nat....11350
20.1.34 remark 8021p....11351
20.1.35 remark cvlan-8021p....11353
20.1.36 remark dscp....11354
20.1.37 remark fr-de....11355
20.1.38 remark local-precedence....11357
20.1.39 remark mpls-exp....11358
20.1.40 remark qos-group....11360
20.1.41 reset traffic policy statistics....11361
20.1.42 reset traffic policy statistics bridge-domain....11363
20.1.43 reset traffic policy statistics global....11365
20.1.44 traffic behavior....11366
20.1.45 traffic classifier....11367
20.1.46 traffic policy....11369
20.1.47 traffic-policy (BD view)....11372
20.1.48 traffic-policy (interzone view)....11374
20.1.49 traffic-policy (interface view)....11375
20.1.50 traffic-policy (traffic behavior view)....11377
20.1.51 traffic-policy global bind interface....11378
20.1.52 url-filter-profile....11380
20.2 Priority Mapping Commands....11382
20.2.1 display qos map-table....11382
20.2.2 input....11386
20.2.3 port priority....11394
20.2.4 qos map-table....11398
20.2.5 trust....11401
20.3 Traffic Policing and Traffic Shaping Commands....11403
20.3.1 bandwidth....11403
20.3.2 car (traffic behavior view)....11404
20.3.3 car (QoS profile view)....11411
20.3.4 display qos-profile....11413

20.3.5 display qos adaptation-profile 11414
20.3.6 display qos adaptation-profile applied-record 11417
20.3.7 display qos car statistics 11421
20.3.8 gts (traffic behavior view) 11423
20.3.9 gts adaptation-profile 11426
20.3.10 port-schedule high 11428
20.3.11 qos adaptation-profile 11429
20.3.12 qos car 11431
20.3.13 qos gts 11439
20.3.14 qos gts adaptation-profile 11442
20.3.15 qos lr (interface view) 11443
20.3.16 qos overhead 11445
20.3.17 queue gts 11446
20.3.18 qos-profile 11449
20.3.19 rate-adjust increase interval 11450
20.3.20 rate-adjust loss 11451
20.3.21 rate-adjust step 11453
20.3.22 rate-range 11455
20.3.23 reset qos car statistics 11456
20.3.24 track nqa 11458
20.4 Congestion Avoidance and Congestion Management Commands 11460
20.4.1 display drop-profile 11460
20.4.2 display qos queue statistics 11462
20.4.3 display qos queue-profile 11465
20.4.4 dscp discard-percentage 11467
20.4.5 ip-precedence discard-percentage 11472
20.4.6 drop-profile (system view) 11476
20.4.7 drop-profile (traffic behavior view) 11478
20.4.8 qos queue-profile (interface view) 11480
20.4.9 qos queue-profile (system view) 11481
20.4.10 queue af 11483
20.4.11 queue drop-profile 11486
20.4.12 queue ef 11488
20.4.13 queue length 11491
20.4.14 queue-length 11495
20.4.15 queue llq 11497
20.4.16 queue weight 11500
20.4.17 queue wfq 11502
20.4.18 reset qos queue statistics 11505
20.4.19 schedule 11506
20.4.20 wred 11511
20.5 Filtering Configuration Commands 11512

20.5.1 deny | permit ... 11513
20.6 Statistics Configuration Commands ... 11514
20.6.1 statistic enable (traffic behavior view) ... 11514
20.6.2 statistics enable (QoS profile view) ... 11515
20.7 ACL-based Simplified Traffic Policy Commands ... 11516
20.7.1 acl forward-algorithm hash ... 11516
20.7.2 display traffic-filter applied-record ... 11517
20.7.3 display traffic-filter statistics ... 11519
20.7.4 reset traffic-filter statistics ... 11521
20.7.5 traffic-filter (interface view) ... 11523
20.8 Bandwidth Management Configuration Commands ... 11526
20.8.1 bandlimit ... 11526
20.8.2 bandguarantee ... 11529
20.8.3 enable bandlimit ... 11531
20.8.4 enable bandguarantee ... 11534
20.8.5 user-ip ... 11537
20.8.6 user-set ... 11539
20.8.7 web ... 11540
20.9 Application Control Management Commands ... 11540
20.9.1 app-profile ... 11540
20.9.2 category ... 11542
20.9.3 application ... 11543
20.9.4 application-control ... 11544
20.9.5 enable application-control ... 11547
20.10 SAC Configuration Commands ... 11549
20.10.1 application name cache type aging-time ... 11549
20.10.2 category sub-category ... 11550
20.10.3 data-model ... 11555
20.10.4 description (user-defined application view) ... 11556
20.10.5 description (user-defined application rule view) ... 11557
20.10.6 detect max-bytes ... 11558
20.10.7 detect max-packets ... 11559
20.10.8 detect max-time ... 11559
20.10.9 detect uni-direction ... 11560
20.10.10 display application ... 11561
20.10.11 display application name aging-time ... 11566
20.10.12 display sa application-list ... 11567
20.10.13 display sa application-statistic ... 11569
20.10.14 display sa category ... 11572
20.10.15 display sa information ... 11574
20.10.16 if-match application ... 11575
20.10.17 if-match category ... 11577

 Copyright © Huawei Technologies Co., Ltd.

20.10.18 ip-address (user-defined application rule view) 11579
20.10.19 label (user-defined application view) 11580
20.10.20 port (user-defined application rule view) 11583
20.10.21 port-identification packet-number-threshold 11584
20.10.22 protocol (user-defined application rule view) 11585
20.10.23 rename (user-defined application rule view) 11586
20.10.24 rename (user-defined application view) 11587
20.10.25 reset sa application-statistic 11588
20.10.26 rule (user-defined application view) 11589
20.10.27 sa 11591
20.10.28 sa application-statistic enable 11592
20.10.29 signature (user-defined application rule view) 11593
20.10.30 user-defined-application 11595

21 Network Management and Monitoring Commands 11597

21.1 SNMP Configuration Commands 11597
21.1.1 display snmp-agent community 11598
21.1.2 display snmp-agent extend error-code status 11600
21.1.3 display snmp-agent group 11601
21.1.4 display snmp-agent local-engineid 11603
21.1.5 display snmp-agent mib-view 11604
21.1.6 display snmp-agent notify-filter-profile 11607
21.1.7 display snmp-agent statistics 11608
21.1.8 display snmp-agent sys-info 11611
21.1.9 display snmp-agent target-host 11612
21.1.10 display snmp-agent trap all 11614
21.1.11 display snmp-agent trap feature-name snmp all 11616
21.1.12 display snmp-agent trap-source 11617
21.1.13 display snmp-agent usm-user 11618
21.1.14 enable snmp trap updown 11620
21.1.15 snmp-agent 11621
21.1.16 snmp-agent bulk-fast enable 11622
21.1.17 snmp-agent community 11623
21.1.18 snmp-agent complexity-check disable 11626
21.1.19 snmp-agent community simple 11628
21.1.20 snmp-agent extend error-code enable 11631
21.1.21 snmp-agent group 11632
21.1.22 snmp-agent local-engineid 11636
21.1.23 snmp-agent mib-view 11637
21.1.24 snmp-agent notify-filter-profile 11640
21.1.25 snmp-agent permit interface 11641
21.1.26 snmp-agent sys-info 11643
21.1.27 snmp-agent target-host trap-hostname 11645

21.1.28 snmp-agent target-host trap-paramsname 11647
21.1.29 snmp-agent trap disable 11650
21.1.30 snmp-agent trap enable 11651
21.1.31 snmp-agent trap enable feature-name 11652
21.1.32 snmp-agent trap enable feature-name snmp 11653
21.1.33 snmp-agent trap enable syslog 11654
21.1.34 snmp-agent trap life 11655
21.1.35 snmp-agent trap queue-size 11656
21.1.36 snmp-agent trap source 11657
21.1.37 snmp-agent usm-user 11658
21.1.38 snmp-agent source loopback 11663
21.1.39 snmp-agent server-source 11664
21.2 RMON and RMON2 Configuration Commands 11665
21.2.1 display rmon alarm 11665
21.2.2 display rmon event 11668
21.2.3 display rmon eventlog 11670
21.2.4 display rmon history 11672
21.2.5 display rmon prialarm 11675
21.2.6 display rmon statistics 11677
21.2.7 display rmon2 hlhostcontroltable 11680
21.2.8 display rmon2 nlhosttable 11682
21.2.9 display rmon2 protocoldirtable 11683
21.2.10 display snmp-agent trap feature-name rmon all 11685
21.2.11 rmon alarm 11686
21.2.12 rmon event 11689
21.2.13 rmon history 11690
21.2.14 rmon prialarm 11691
21.2.15 rmon statistics 11694
21.2.16 rmon2 hlhostcontroltable 11696
21.2.17 rmon2 protocoldirtable 11698
21.2.18 rmon-statistics enable 11700
21.2.19 snmp-agent trap enable feature-name rmon 11701
21.3 TCP FPM Configuration Commands 11702
21.3.1 display tcp fpm session 11702
21.3.2 reset tcp fpm session all 11704
21.3.3 pm report tcp fpm enable 11705
21.3.4 tcp fpm enable 11706
21.3.5 tcp fpm report time 11706
21.4 IP FPM Configuration Commands 11707
21.4.1 authentication-mode (IPFPM-DCP view) 11707
21.4.2 authentication-mode (IPFPM-MCP view) 11709
21.4.3 authentication-mode (IPFPM-DCP instance view) 11711

21.4.4 color-flag....11712
21.4.5 dcp....11714
21.4.6 dcp id....11715
21.4.7 delay-measure enable two-way....11716
21.4.8 description (IPFPM-DCP instance view)....11718
21.4.9 description (IPFPM-MCP instance view)....11720
21.4.10 display ipfpm dcp....11721
21.4.11 display ipfpm mcp....11723
21.4.12 display ipfpm instance application....11725
21.4.13 display ipfpm statistic-type....11726
21.4.14 display snmp-agent trap feature-name ipfpm all....11729
21.4.15 flow (IPFPM-DCP instance view)....11730
21.4.16 instance (IPFPM-MCP view)....11733
21.4.17 instance (IPFPM-DCP view)....11735
21.4.18 interval....11736
21.4.19 ipfpm tlp (layer 3 interface)....11737
21.4.20 loss-measure enable....11738
21.4.21 mcp (IPFPM-DCP instance view)....11740
21.4.22 mcp (IPFPM-DCP view)....11742
21.4.23 mcp id....11744
21.4.24 measure disable (IPFPM-MCP instance view)....11745
21.4.25 nqa ipfpm dcp....11747
21.4.26 nqa ipfpm mcp....11748
21.4.27 protocol udp port....11749
21.4.28 snmp-agent trap enable feature-name ipfpm....11750
21.4.29 tlp....11751
21.5 CWMP Configuration Commands....11753
21.5.1 cwmp....11753
21.5.2 cwmp acs password....11754
21.5.3 cwmp acs url....11755
21.5.4 cwmp acs username....11757
21.5.5 cwmp cpe connect interface....11758
21.5.6 cwmp cpe connect retry....11759
21.5.7 cwmp cpe inform interval....11760
21.5.8 cwmp cpe inform interval enable....11762
21.5.9 cwmp cpe inform product-class device-type....11763
21.5.10 cwmp cpe inform time....11764
21.5.11 cwmp cpe password....11765
21.5.12 cwmp cpe username....11766
21.5.13 cwmp cpe wait timeout....11767
21.5.14 cwmp device-info serial-number system-mac....11769
21.5.15 cwmp enable....11770

21.5.16 cwmp escape-character 11771
21.5.17 cwmp escape-character enable 11772
21.5.18 cwmp password complexity-check disable 11773
21.5.19 cwmp permit interface 11774
21.5.20 cwmp request upload current-configuration 11776
21.5.21 cwmp ssl-client 11776
21.5.22 display cwmp configuration 11778
21.5.23 display cwmp password 11780
21.5.24 display cwmp request upload status 11781
21.5.25 display cwmp status 11782
21.5.26 cwmp ip-change inform disable 11784
21.5.27 cwmp ssl-server ssl-policy 11785
21.6 LLDP Configuration Commands 11786
21.6.1 display lldp local 11786
21.6.2 display lldp neighbor 11794
21.6.3 display lldp neighbor brief 11801
21.6.4 display lldp statistics 11802
21.6.5 display lldp tlv-config 11803
21.6.6 display snmp-agent trap feature-name lldptrap all 11806
21.6.7 lldp clear neighbor 11807
21.6.8 lldp dot3-tlv power 11809
21.6.9 lldp enable (interface view) 11810
21.6.10 lldp enable (system view) 11812
21.6.11 lldp management-address 11813
21.6.12 lldp message-transmission delay 11814
21.6.13 lldp message-transmission hold-multiplier 11816
21.6.14 lldp message-transmission interval 11818
21.6.15 lldp restart-delay 11820
21.6.16 lldp tlv-enable 11821
21.6.17 lldp tlv-enable private-tlv authentication 11826
21.6.18 lldp trap-interval 11828
21.6.19 reset lldp statistics 11830
21.6.20 snmp-agent trap enable feature-name lldptrap 11831
21.7 NQA Configuration Commands 11833
21.7.1 adv-factor 11833
21.7.2 agetime 11835
21.7.3 alarm 11836
21.7.4 clear-records 11839
21.7.5 community read cipher 11839
21.7.6 datafill 11841
21.7.7 datasize 11842
21.7.8 description (NQA view) 11844

21.7.9 destination-address 11845
21.7.10 destination-port 11847
21.7.11 display ip nqa-compatible responder statistics 11848
21.7.12 display nqa application 11850
21.7.13 display nqa alarm 11851
21.7.14 display nqa-alarm 11853
21.7.15 display nqa event 11854
21.7.16 display nqa-event 11855
21.7.17 display nqa-group 11856
21.7.18 display nqa history 11857
21.7.19 display nqa-parameter 11860
21.7.20 display nqa results 11864
21.7.21 display nqa support-server-type 11875
21.7.22 display nqa support-test-type 11876
21.7.23 display nqa-agent 11878
21.7.24 display nqa-ftp-record configuration 11879
21.7.25 display nqa-server 11881
21.7.26 display nqa-server session 11883
21.7.27 display snmp-agent trap feature-name nqa all 11884
21.7.28 dns-server 11886
21.7.29 fail-percent 11887
21.7.30 forwarding-simulation inbound-interface 11888
21.7.31 frequency 11890
21.7.32 ftp-filename 11891
21.7.33 ftp-filesize 11892
21.7.34 ftp-operation 11894
21.7.35 ftp-password 11895
21.7.36 ftp-username 11897
21.7.37 hardware-based enable 11898
21.7.38 http-operation 11899
21.7.39 http-url 11900
21.7.40 icmp-jitter-mode 11901
21.7.41 interval (NQA view) 11902
21.7.42 ip nqa-compatible responder enable 11904
21.7.43 ip nqa-compatible auto 11905
21.7.44 ip nqa-compatible udp 11906
21.7.45 ip-forwarding 11908
21.7.46 jitter-codec 11909
21.7.47 jitter-packetnum 11911
21.7.48 lsp-exp 11913
21.7.49 lsp-path full-display 11914
21.7.50 lsp-nexthop 11915

21.7.51 lsp-replymode 11916
21.7.52 lsp-tetunnel 11918
21.7.53 lsp-type 11919
21.7.54 lsp-version 11921
21.7.55 nexthop 11922
21.7.56 nqa 11924
21.7.57 nqa (NQA group view) 11925
21.7.58 nqa event 11927
21.7.59 nqa-ftp-record enable 11929
21.7.60 nqa-ftp-record filename 11930
21.7.61 nqa-ftp-record ip-address 11931
21.7.62 nqa-ftp-record item-num 11932
21.7.63 nqa-ftp-record password 11934
21.7.64 nqa-ftp-record time 11936
21.7.65 nqa-ftp-record trap-enable 11938
21.7.66 nqa-ftp-record source-address 11939
21.7.67 nqa-ftp-record username 11940
21.7.68 nqa-ftp-record vpn-instance 11941
21.7.69 nqa-group 11942
21.7.70 nqa-jitter tag-version 11943
21.7.71 nqa-server rtp-udp 11944
21.7.72 nqa-server session-record enable 11945
21.7.73 nqa-server tcpconnect 11946
21.7.74 nqa-server udpecho 11948
21.7.75 nqa upload statistics datetime-type 11950
21.7.76 probe-count 11951
21.7.77 probe-failtimes 11953
21.7.78 packet-rewrite-check 11954
21.7.79 records 11955
21.7.80 records history-filter 11957
21.7.81 remote-pw-id 11958
21.7.82 remote-address (NQA view) 11959
21.7.83 reset ip nqa-compatible responder statistics 11960
21.7.84 restart (NQA view) 11961
21.7.85 sendpacket passroute 11961
21.7.86 send-trap 11963
21.7.87 set-df 11965
21.7.88 snmp-agent trap enable feature-name nqa 11966
21.7.89 source-address 11970
21.7.90 source-interface 11971
21.7.91 source-port 11973
21.7.92 start 11974

21.7.93 stop....11977
21.7.94 test-failtimes....11978
21.7.95 test-type....11979
21.7.96 timestamp-unit....11980
21.7.97 threshold....11981
21.7.98 timeout....11983
21.7.99 tos....11984
21.7.100 tracert-hopfailtimes....11986
21.7.101 tracert-livetime....11987
21.7.102 ttl....11988
21.7.103 ttl-copymode....11989
21.7.104 vlan (NQA view)....11990
21.7.105 vpn-instance....11991
21.8 LSDP Configuration Commands....11992
21.8.1 lsdp....11993
21.8.2 lsdp trigger protocol ospf delay-up....11995
21.8.3 display lsdp....11996
21.9 Service Diagnosis Configuration Commands....11997
21.9.1 display trace information....11997
21.9.2 display trace instance....12000
21.9.3 display trace object....12002
21.9.4 reset trace instance....12005
21.9.5 save trace information....12006
21.9.6 trace enable....12007
21.9.7 trace object....12009
21.9.8 trace syslog source....12013
21.10 Mirroring Configuration Commands....12014
21.10.1 display mirror-port....12014
21.10.2 display observe-port....12016
21.10.3 mirror (interface view)....12017
21.10.4 mirror (traffic behavior view)....12018
21.10.5 observe-port....12020
21.11 Packet Capture Configuration Command....12021
21.11.1 capture-packet....12021
21.11.2 display voice-monitor....12024
21.11.3 voice-monitor....12026
21.12 NetStream Configuration Commands....12028
21.12.1 collect application....12029
21.12.2 collect category name....12030
21.12.3 collect counter....12031
21.12.4 collect interface....12032
21.12.5 display ip netstream....12034

21.12.6 display ip netstream cache....12037
21.12.7 display ip netstream record....12042
21.12.8 display ip netstream statistic....12043
21.12.9 display snmp-agent trap feature-name netstream all....12045
21.12.10 display snmp-agent trap feature-name sindex all....12047
21.12.11 enable....12048
21.12.12 export version....12049
21.12.13 ip netstream....12051
21.12.14 ip netstream aggregation....12052
21.12.15 ip netstream aggregation enable....12056
21.12.16 ip netstream aggregation timeout active....12057
21.12.17 ip netstream aggregation timeout inactive....12058
21.12.18 ip netstream as extend enable....12059
21.12.19 ip netstream cache log enable....12060
21.12.20 ip netstream cache log log-directory....12061
21.12.21 ip netstream export host....12063
21.12.22 ip netstream export index-switch....12065
21.12.23 ip netstream export source....12066
21.12.24 ip netstream export source interface....12067
21.12.25 ip netstream export template timeout-rate....12068
21.12.26 ip netstream export version....12069
21.12.27 ip netstream multicast....12071
21.12.28 ip netstream pre-classify enable....12072
21.12.29 ip netstream record....12073
21.12.30 ip netstream rpf-failure....12074
21.12.31 ip netstream sampler (interface view)....12075
21.12.32 ip netstream tcp-flag enable....12077
21.12.33 ip netstream tm-after enable....12078
21.12.34 ip netstream timeout active....12079
21.12.35 ip netstream timeout inactive....12080
21.12.36 ip-mpls netstream....12081
21.12.37 mpls netstream....12083
21.12.38 mask....12084
21.12.39 match ipv4....12086
21.12.40 match vxlan vni....12087
21.12.41 port ip netstream record....12088
21.12.42 reset ip netstream cache....12090
21.12.43 reset ip netstream statistic....12091
21.12.44 snmp-agent trap enable feature-name netstream....12092
21.12.45 snmp-agent trap enable feature-name sindex....12093
21.13 IP Accounting Configuration Commands....12094
21.13.1 display ip accounting input-packets....12094

21.13.2 display ip accounting output-packets 12096
21.13.3 display ip accounting precedence 12097
21.13.4 display ip accounting rule 12099
21.13.5 ip accounting 12100
21.13.6 ip accounting matched-threshold 12101
21.13.7 ip accounting mismatched-threshold 12103
21.13.8 ip accounting precedence 12105
21.13.9 ip accounting rule 12106
21.13.10 ip accounting timeout 12108
21.13.11 reset ip accounting 12109
21.14 TWAMP Light Configuration Commands 12110
21.14.1 client 12110
21.14.2 display twamp-light responder test-session 12111
21.14.3 display twamp-light statistic-type 12114
21.14.4 display twamp-light test-session 12118
21.14.5 nqa twamp-light 12123
21.14.6 responder 12124
21.14.7 sender 12125
21.14.8 test start 12126
21.14.9 test start-continual 12128
21.14.10 test stop 12131
21.14.11 test-session 12132
21.14.12 test-session (TWAMP-Light-Responder view) 12135
21.15 Ping and Tracert Configuration Commands 12138
21.15.1 ping 12138
21.15.2 ping ipv6 12149
21.15.3 tracert 12154
21.15.4 tracert ipv6 12159

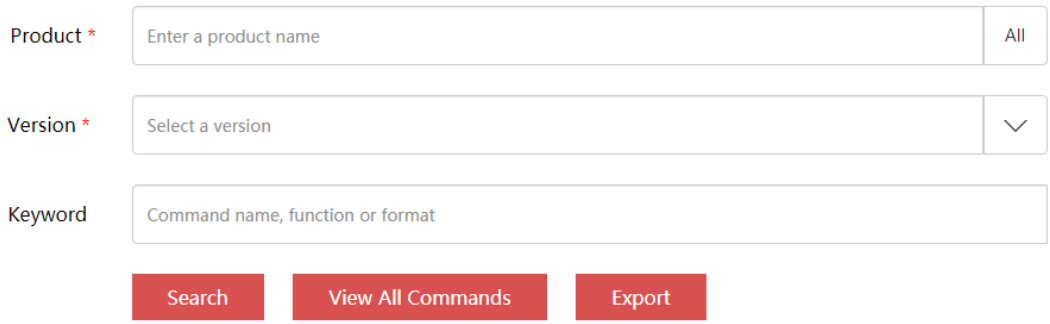
 Copyright © Huawei Technologies Co., Ltd.

1 Using the Command Query Tool to Query Product Command Information

This section describes how to use the command query tool to obtain detailed information about commands supported by different product models.

Figure 1-1 shows the **Command Query Tool** interface. You can use this tool to query information about commands supported by different product models, including the command format, function, level, and usage guidelines.

Figure 1-1 Interface of the command query tool



Copyright © Huawei Technologies Co., Ltd.

2 Overview of CLIs

About This Chapter

This chapter describes how to perform configuration and routine maintenance on devices by running commands.

2.1 How to Use Command Lines
This section describes how to use command lines and some techniques to improve operating efficiency.

2.2 Displaying the Command Output
This section describes how to query the configuration information about command lines, control the method in which command outputs are displayed, and filter the command outputs.

2.3 Configuration Examples
This section provides several examples that illustrate the use of command lines.

2.1 How to Use Command Lines

This section describes how to use command lines and some techniques to improve operating efficiency.

2.1.1 Entering Command Views

The device has many functions; therefore various configuration commands and query commands are provided to facilitate device management and maintenance. Huawei router registers commands to different command views based on the functions of the commands so that users can easily use them. To configure a function, enter the corresponding command view and then run corresponding commands.

The device provides various command views. For the methods of entering the command views except the following views, see the *Huawei AR Series Access Routers Command Reference*.

 Copyright © Huawei Technologies Co., Ltd.

Common Command Views

Name	How To Enter	Function
User view	When a user logs in to the device, the user enters the user view and the following prompt is displayed: `<Huawei>`	In the user view, you can view the running status and statistics of the device.

System view	Run the **system-view** command and press **Enter** in the user view. The system view is displayed.
	`<Huawei>` **`system-view`**
	`Enter system view, return user view with Ctrl+Z.`
	`[Huawei]`
		In the system view, you can set the system parameters of the device, and enter other function views from this view.

Interface view	Run the **interface** command and specify an interface type and number to enter the interface view. `[Huawei]` **`interface gigabitethernet`** *`X/Y/Z`* `[Huawei-GigabitEthernet`*`X/Y/Z`*`]` *X/Y/Z* indicates the number of an interface that needs to be specified. It is in the format of slot number/card number/interface sequence number. The interface GigabitEthernet is used as an example.	In the interface view, you can configure interface parameters including physical attributes, link layer protocols, and IP addresses.
Routing protocol view	Run a command to activate a routing protocol process in the system view. The corresponding routing protocol view is displayed. `[Huawei]` **`isis`** `[Huawei-isis-1]`	In routing protocol views, you can configure most routing protocol parameters. The routing protocol views include the IS-IS view, OSPF view, and RIP view.

The command line prompt Huawei is the default host name (sysname). The prompt indicates the current view. For example, <> indicates the user view and [] indicates all other views except the user view.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Some commands can be executed in multiple views, but they have different functions after being executed in different views. For example, you can run the **lldp enable** command in the system view to enable LLDP globally and in the interface view to enable LLDP on an interface.
- In the system view, you can run the **diagnose** command to enter the diagnostic view. Diagnostic commands are used for device fault diagnosis. If you run some commands in the diagnostic view, the device may fail to run properly or services may be interrupted. Contact technical support personnel and use these diagnostic commands with caution.

Exiting Command Views

You can run the **quit** command to return from the current view to an upper-level view.

For example, after you run the **quit** command to return from the AAA view to the system view, you can run the **quit** command again to return from the system view to the user view.

```
[Huawei-aaa] quit
[Huawei] quit
<Huawei>
```

To return from the AAA view directly to the user view, press **Ctrl+Z** or run the **return** command.

Press **Ctrl+Z** to return directly to the user view.

```
[Huawei-aaa]          // Enter Ctrl+Z
<Huawei>
```

Run the **return** command to return directly to the user view.

```
[Huawei-aaa] return
<Huawei>
```

2.1.2 Setting Command Levels

The system divides commands into four levels and sets the command level in the specified view. The device administrator can change the command level as required, so that a lower-level user can use some high-level commands. The device administrator can also change the command level to a larger value to improve device security.

Context

- The system grants users different access permissions based on their roles. User levels are classified into sixteen levels, which correspond to the command levels. Users can use only the commands at the same or lower level than their own levels. By default, there are four command levels 0 to 3 and sixteen user levels 0 to 15. **Table 2-1** describes the relationship between command levels and user levels.

Table 2-1 Relationship between command levels and user levels

User Level	Command Level	Name	Description
0	0	Visit level	Commands of this level include network diagnosis tool commands (such as ping and tracert), commands for accessing external devices from the local device (such as Telnet) and some display commands.
1	0, 1	Monitoring level	Commands of this level are used for system maintenance, including display commands. **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3. For details about command levels, see the *Huawei AR Series Access Routers Command Reference*.
2	0, 1, 2	Configuration level	Commands of this level are used for service configuration to provide direct network services, including routing commands and commands of each network layer.
3 to 15	0, 1, 2, 3	Management level	Commands of this level are used for basic system operations, including file system, FTP, TFTP download, user management, command level configuration, and debugging.

NOTICE

Changing the default command level without the guidance of technical personnel is not recommended. This may result in inconvenience for operation and maintenance and bring about security problems.

Procedure

Step 1 Run **system-view**

The system view is displayed.

Step 2 (Optional) Run **display command-view** *command-key*

The view of a specified command is displayed.

You can perform this step to check the view of the command whose level needs to be changed.

Step 3 Run **command-privilege level** *level* **view** *view-name command-key*

The command level is set in the specified view.

----End

2.1.3 Editing Command Lines

Editing Feature

You can edit commands in a CLI that supports multi-line edition. Each command can contain a maximum of 510 characters. The keywords in the commands are case insensitive. Whether a command parameter is case sensitive or not depends on what the parameter is.

Table 2-2 lists keys that are frequently used for command editing.

Table 2-2 Keys for command editing

Key	Function
Common key	Inserts a character at the current location of the cursor if the editing buffer is not full, and the cursor moves to the right. Otherwise, an alarm is generated.
Backspace	Deletes the character on the left of the cursor and the cursor moves to the left. When the cursor reaches the head of the command, an alarm is generated.
Left cursor key ← or Ctrl+B	Moves the cursor to the left by the space of a character. When the cursor reaches the head of the command, an alarm is generated.
Right cursor key → or Ctrl+F	Moves the cursor to the right by the space of a character. When the cursor reaches the end of the command, an alarm is generated.

Operating Techniques

Incomplete Keyword

You can enter incomplete keywords on the device. In the current view, you do not need to enter complete keywords if the entered characters can match a unique keyword. This function improves operating efficiency.

For example, to execute the **display current-configuration** command, you can enter **d cu**, **di cu**, or **dis cu**, but you cannot enter **d c** or **dis c** because they do not match unique keywords.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

The maximum length of a command (including the incomplete command) to be entered is 510 characters. If a command in incomplete form is configured, the system saves the command to the configuration file in its complete form, which may cause the command to have more than 510 characters. In this case, the command in incomplete form cannot be restored after the system restarts. Therefore, when you configure a command in incomplete form, pay attention to the length of the command.

Tab

Enter an incomplete keyword and press Tab to complete the keyword.

- When a unique keyword matches the input, the system replaces the incomplete input with the unique keyword and displays it in a new line with the cursor leaving a space behind. For example:

  a. Enter an incomplete keyword.

  ```
  [Huawei] info-
  ```

  b. Press **Tab**.

  The system replaces the entered keyword and displays it in a new line with the complete keyword followed by a space.

  ```
  [Huawei] info-center
  ```

- When the input has multiple matches, press Tab repeatedly to display the keywords beginning with the incomplete input in a circle until the desired keyword is displayed. In this case, the cursor closely follows the end of the keyword. For example:

  a. Enter an incomplete keyword.

  ```
  [Huawei] info-center log
  ```

  b. Press **Tab**.

  The system displays the prefixes of all the matched keywords. In this example, the prefix is **log**.

  ```
  [Huawei] info-center logbuffer
  ```

  Press **Tab** to switch from one matched keyword to another. In this case, the cursor closely follows the end of a word.

  ```
  [Huawei] info-center logfile
  [Huawei] info-center loghost
  ```

  Stop pressing **Tab** when the desired keyword is displayed.

- When an incorrect keyword is entered, press Tab and it is displayed in a new line without being changed. For example:

  a. Enter an incorrect keyword.

  ```
  [Huawei] info-center loglog
  ```

  b. Press **Tab**.

  ```
  [Huawei] info-center loglog
  ```

  The system displays information in a new line, but the keyword **loglog** remains unchanged and there is no space between the cursor and the keyword, indicating that this keyword does not exist.

 Copyright © Huawei Technologies Co., Ltd.

2.1.4 Using Command Line Online Help

When using a command line, you can use the online help to obtain real-time help without memorizing a large number of complex commands.

When entering command lines, you can enter a question mark (?) at any time to obtain online help. You can choose to obtain full help or partial help.

Full Help

When entering a command, you can use the full help function to obtain keywords and parameters for the command. Use any of the following methods to obtain full help from a command line.

- Enter a question mark (?) in any command view to obtain all the commands and their simple descriptions. For example:

```
<Huawei> ?
User view commands:
  arp-ping       ARP-ping
  autosave       <Group> autosave command group
  backup         Backup  information
  cd             Change current directory
  clear          Clear
  clock          Specify the system clock
  cls            Clear screen
  compare        Compare configuration file
  copy           Copy from one file to another
...
```

- Enter some keywords of a command and a question mark (?) separated by a space. All keywords associated with this command, as well as simple descriptions, are displayed. For example:

```
<Huawei> system-view
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode ?
  aaa       AAA authentication
  password  Authentication through the password of a user terminal interface
[Huawei-ui-vty0-4] authentication-mode aaa ?
  <cr>  Please press ENTER to execute command
[Huawei-ui-vty0-4] authentication-mode aaa
```

  – "aaa" and "password" are keywords. "AAA authentication" and "Authentication through the password of a user terminal interface" describe the keywords respectively.
  – <cr> indicates that there is no keyword or parameter in this position. You can press Enter to run this command.

- Enter some keywords of a command and a question mark (?) separated by a space. All parameters associated with this keyword, as well as simple descriptions, are listed. For example:

```
<Huawei> system-view
[Huawei] ftp timeout ?
  INTEGER<1-35791>  The value of FTP timeout (in minutes)
[Huawei] ftp timeout 35 ?
  <cr>  Please press ENTER to execute command
[Huawei] ftp timeout 35
```

  "INTEGER<1-35791>" describes the value range of the parameter. "The value of FTP timeout (in minutes)" briefly describes the function of this parameter.

 Copyright © Huawei Technologies Co., Ltd.

Partial Help

If you enter only the first or first several characters of a command keyword, partial help provides keywords that begin with this character or character string. Use any of the following methods to obtain partial help from a command line.

- Enter a character string followed directly by a question mark (?) to display all keywords that begin with this character string. For example:

```
<Huawei> d?
  debugging  <Group> debugging command group
  delete     Delete a file
  dialer     Dialer
  dir        List files on a filesystem
  display    Display information
<Huawei> d
```

- Enter a command and a string followed directly by a question mark (?) to display all the keywords that begin with this string. For example:

```
<Huawei> display b?
  bfd              Specify BFD(Bidirectional Forwarding Detection)
                  configuration information
  bgp              BGP information
  binding          Display binding relation of profile
  bridge           <Group> bridge command group
```

- Enter the first several letters of a keyword in a command and press **Tab** to display a complete keyword. The first several letters, however, must uniquely identify the keyword. If they do not identify a specific keyword, press **Tab** continuously to display different keywords and you can select one as required.

NOTE

The command output obtained through the online help function is used for reference only.

2.1.5 Interpreting Command Line Error Messages

If a command is entered and passes syntax check, the system executes it. Otherwise, the system reports an error message.

Table 2-3 lists the common error messages.

Table 2-3 Common error messages of the command line

Error Message	Cause of the Error
Error: Unrecognized command found at '^' position.	No command is found.
	No keyword is found.
Error: Wrong parameter found at '^' position.	The parameter type is incorrect.
	The parameter value exceeds the limit.
Error: Incomplete command found at '^' position.	The entered command is incomplete.
Error: Too many parameters found at '^' position.	Too many parameters are entered.

 Copyright © Huawei Technologies Co., Ltd.

Error Message	Cause of the Error
Error: Ambiguous command found at '^' position.	Indefinite command is entered.

2.1.6 Using the undo Command Line

If a command line begins with the keyword **undo**, it is an **undo** command line. The **undo** command lines restore default settings of parameters, disable functions, or delete configurations. Almost each configuration command line has a corresponding **undo** command.

Some examples of using the undo command are listed as follows:

- The **undo** command restores the default setting.

  The **sysname** command sets a device host name. For example:

```
<Huawei> system-view
[Huawei] sysname Server
[Server] undo sysname
[Huawei]
```

- The **undo** command disables a specified function.

  The **ftp server enable** command enables the FTP server function on the device. For example:

```
<Huawei> system-view
[Huawei] ftp server enable
Info: Succeeded in starting the FTP server
[Huawei] undo ftp server
Info: Succeeded in closing the FTP server.
```

- The **undo** command deletes a specified configuration.

  The **header** command configures the header information displayed on terminals when users log in. For example:

```
<Huawei> system-view
[Huawei] header login information "Hello,Welcome to Huawei!"
```

  Log out of the terminal and re-log in. A message "Hello, Welcome to Huawei!" is displayed before authentication. Run the **undo header login** command.

```
Hello,Welcome to Huawei!

Login authentication


Password:
<Huawei> system-view
[Huawei] undo header login
```

  Log out of the terminal and re-log in. No message is displayed before authentication.

```
Login authentication


Password:
<Huawei>
```

NOTE

The command output provided here is used for reference only. The actual output information may differ from the preceding information.

2.1.7 Displaying History Commands

The device automatically stores history commands entered by a user. To enter a command that has been executed, you can use this function to call up the history command.

By default, the system saves 10 history commands for each user. Run the **history-command max-size** *size-value* command to reset the number of history commands that can be saved in a specified user interface view. The maximum number is 256.

NOTE

If the value specified in the **history-command max-size** *size-value* command is large, it may take a long time to obtain a required history command. Therefore, a large value is not recommended.

Table 2-4 shows operations on history commands.

Table 2-4 Accessing history commands

Action	Command or Key	Result
Display history commands.	**display history-command**	The history commands entered by the current user are displayed.
Display the earlier history command.	Up arrow key ↑ or Ctrl+P	An earlier history command is displayed. If the current command is the first command, an alarm is generated when you attempt to display the earlier history command.
Display the later history command.	Down arrow key ↓ or Ctrl+N	A later history command is displayed. If the current command is the latest command, no output is displayed and an alarm is generated when you attempt to display the later history command.

When using history commands, note the following:

 Copyright © Huawei Technologies Co., Ltd.

- The saved history commands are the same as those entered by users. For example, if the user enters an incomplete command, the saved command also is incomplete.
- If the user runs the same command several times, only the latest command is saved. If the command is entered in different forms, they are considered as different commands.

  For example, if the **display current-configuration** command is run several times, only one history command is saved. If the **display current-configuration** command and the **dis curr** command are used, both of them are saved.

2.1.8 Using Command Line Shortcut Keys

You can use shortcut keys provided by the device to quickly enter commands.

There are two types of shortcut keys:

- User-defined shortcut keys: include Ctrl+G, Ctrl+L, Ctrl+O, and Ctrl+U. You can associate these shortcut keys with any commands. When a shortcut key is pressed, the system runs the corresponding command.
- System-defined shortcut keys: shortcut keys defined in the system that have fixed functions. Users cannot define these shortcut keys. **Table 2-5** lists the frequently used system-defined shortcut keys.

NOTE

The terminal in use may affect the functions of the shortcut keys. For example, if the shortcut keys defined by the terminal conflict with those defined in the system, the shortcut keys entered by the user are captured by the terminal program and the commands corresponding to the shortcut keys are not executed.

User-defined Shortcut Keys

When a user frequently uses a command or some commands, the user can use shortcut keys to define these commands. Only management-level users have the rights to define shortcut keys. The configurations are as follows:

1. Run the **system-view** command to enter the system view.
2. Run the **hotkey** { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_U** } *command-text* command to configure a shortcut key corresponding to a command.

The system supports four user-defined shortcut keys and the default values are as follows:

- Ctrl+G: **display current-configuration**
- Ctrl+L: **undo idle-timeout**
- Ctrl+O: **undo debugging all**
- Ctrl+U: Null

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- When defining shortcut keys, use double quotation marks to define the command if this command contains several keywords separated by spaces. For example, **hotkey ctrl_l "display tcp status"**. Do not use double quotation marks to define a command if the command contains only one keyword.
- Run the **display hotkey** command to view the status of the defined, undefined, and system-defined shortcut keys.
- Run the **undo hotkey** command to restore default values of the configured shortcut keys.
- Shortcut keys are executed in the same way as commands. The system can record commands in their original formats in the command buffer and logs to help query and locate the fault.
- The user-defined shortcut keys are available to all users. If a user does not have the rights to use the command defined by a shortcut key, the system displays an error message when this shortcut key is executed.

System-defined Shortcut Keys

Table 2-5 System-defined shortcut keys

Key	Function
Ctrl+A	Moves the cursor to the beginning of the current line.
Ctrl+B	Moves the cursor back one character.
Ctrl+C	Stops performing current functions.
Ctrl+D	Deletes the character where the cursor is located at.
Ctrl+E	Moves the cursor to the end of the last line.
Ctrl+F	Moves the cursor forward one character.
Ctrl+H	Deletes the character on the left side of the cursor.
Ctrl+K	Stops outgoing connections in the call establishment stage.
Ctrl+N	Displays the next command in the history command buffer.
Ctrl+P	Displays the previous command in the history command buffer.
Ctrl+T	Function as a question mark.
Ctrl+W	Deletes a character string on the left side of the cursor.
Ctrl+X	Deletes all the characters on the left side of the cursor.

 Copyright © Huawei Technologies Co., Ltd.

Key	Function
Ctrl+Y	Deletes all the characters on the right side of the cursor and the character where the cursor is located at.
Ctrl+Z	Returns to the user view.
Ctrl+]	Stops incoming connections or redirects the connections.
Esc+B	Moves the cursor back one word.
Esc+D	Deletes one word on the right side of the cursor.
Esc+F	Moves the cursor forward one word.

2.1.9 Executing Commands in a Batch

If multiple commands are frequently used consecutively, you can edit these commands to be executed in batches. This simplifies command input and improves efficiency.

Procedure

- Configure assistant tasks to automatically run commands in a batch at scheduled time.

  You can configure one or more scheduled tasks to realize automatic O&M. The device can then run one or a group of commands at specified time or after a certain delay. Assistant tasks enable the device to complete specified operations or configuration without human intervention. Assistant tasks are usually used for scheduled upgrading or configuration.

  a. Run the **system-view** command to enter system view.
  b. Run the **assistant task** *task-name* command to create an assistant task. You can create a maximum of five assistant tasks.
  c. Run the **if-match timer cron** *seconds minutes hours days-of-month months days-of-week* [*years*] command to specify the time when the assistant tasks work.
  d. Run the **perform** *priority* **batch-file** *filename* command to configure the operations of assistant tasks.

     NOTE

     By default, the commands listed in the batch file are executed in the system view.
  e. Run the **display assistant task history** [*task-name*] command to view the operation records of task assistants.

  This function promotes the automatic control and management abilities of the device, reducing power consumption.

----End

2.2 Displaying the Command Output

This section describes how to query the configuration information about command lines, control the method in which command outputs are displayed, and filter the command outputs.

2.2.1 Verifying Command Line Configurations

After the configurations are complete, you can run the **display** command to verify the configuration and running information on the device.

For example, after all configurations of the FTP service are complete, you can run the **display ftp-server** command to check parameters of the FTP server. For details on the usage and functions of the **display** command, see Checking the Configuration in each feature of the *Configuration Guide*.

You can also verify the current running configurations and configurations in the current view.

- Verify the current running configurations:

  display current-configuration

  This command does not display parameters that use default settings.
- Verify configurations in the current view:

  display this

  This command does not display parameters that use default settings.

  NOTE

  When a user runs the **display this** command to check configuration information, other users can run this same command only after all the command output is displayed.

2.2.2 Controlling the Display Mode of Commands

When running commands, you can specify the display mode.

- When the display output is more than one page, you can use **Pg Up** and **Pg Dn** to display information on the previous page and the next page.
- When the information cannot be completely displayed on one screen, the system will pause and you can view the information. You can use the function keys listed in **Table 2-6** to control the display mode of command lines.

  NOTE

  The **screen-length** *screen-length* **temporary** command sets the lines to be displayed temporarily on the terminal screen. If *screen-length* is 0, the split screen function is disabled. Therefore, the system will not pause when the information cannot be completely displayed on one screen.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-6 Display mode of commands

Key	Function
Ctrl+C or Ctrl+Z	Stops displaying information and running commands. **NOTE** You can also press any key (the number key or letter key) except space and Enter.
Space	Continues to display the next screen of information.
Enter	Continues to display the next line of information.

2.2.3 Filtering Command Outputs

When running the **display** command to check the command output, you can use the regular expression (specifying the rule to display) to filter the output information and locate needed information quickly.

Regular Expressions

A regular expression is a mode matching tool. It consists of common characters (such as letters) and special characters (called meta-characters). The regular expression is a template according to which you can search for the required string.

A regular expression provides the following functions:

- Searches for and obtains a sub-string that matches a rule in the string.
- Substitutes a string based on a certain matching rule.

The regular expression consists of common characters and special characters.

- Common characters

  Common characters are used to match themselves in a string, including all upper-case and lower-case letters, digits, punctuations, and special symbols. For example, a matches the letter "a" in "abc", 10 matches the digit "10" in "10.113.25.155", and @ matches the symbol "@" in "xxx@xxx.com".
- Special characters

  Special characters are used together with common characters to match the complex or special string combination. **Table 2-7** describes special characters and their syntax.

 Copyright © Huawei Technologies Co., Ltd.

Table 2-7 Description of special characters

Special Characters	Function	Example
\	Defines an escape character, which is used to mark the next character (common or special) as the common character.	* matches "*".
^	Matches the starting position of the string.	^10 matches "10.10.10.1" instead of "20.10.10.1".
$	Matches the ending position of the string.	1$ matches "10.10.10.1" instead of "10.10.10.2".
*	Matches the preceding element zero or more times.	10* matches "1", "10", "100", "1000", and so on. (10)* matches "null", "10", "1010", "101010", and so on.
+	Matches the preceding element one or more times.	10+ matches "10", "100", "1000", and so on. (10)+ matches "10", "1010", "101010", and so on.
?	Matches the preceding element zero or one time.	10? matches "1" or "10". (10)? matches "null" or "10".
.	Matches any single character.	0.0 matches "0x0", "020", and so on. .oo. matches "book", "look", "tool", and so on.
()	Defines a subexpression, which can be null. Both the expression and the subexpression should be matched.	100(200)+ matches "100200", "100200200", and so on.
x|y	Matches x or y.	100|200 matches "100" or "200". 1(2|3)4 matches "124" or "134", instead of "1234", "14", "1224", and "1334".
[xyz]	Matches any single character in the regular expression.	[123] matches the character 2 in "255".
[^xyz]	Matches any character that is not in the regular expression.	[^123] matches any character except for "1", "2", and "3".
[a-z]	Matches any character within the specified range.	[0-9] matches any character ranging from 0 to 9.

 Copyright © Huawei Technologies Co., Ltd.

Special Characters	Function	Example
[^a-z]	Matches any character beyond the specified range.	[^0-9] matches all non-numeric characters.
_	Matches a comma ",", left brace "{", right brace "}", left parenthesis "(", and right parenthesis ")". Matches the starting position of the input string. Matches the ending position of the input string. Matches a space.	_2008_ matches "2008", "space 2008 space", "space 2008", "2008 space", ",2008,", "{2008}", "(2008)", "{2008)", and "(2008}".

NOTE

Unless otherwise specified, all the characters in the preceding table must be printable characters.

- Degeneration of special characters

  Certain special characters, when placed at certain positions in a regular expression, degenerate to common characters.

  - The special characters following "\" match special characters themselves.
  - The special characters "*", "?", and "+" are placed at the starting position of the regular expression. For example, +45 matches "+45" and abc(*def) matches "abc*def".
  - The special character "^" is placed at any position except for the start of the regular expression. For example, abc^ matches "abc^".
  - The special character "$" is placed at any position except for the end of the regular expression. For example, 12$2 matches "12$2".
  - A right parenthesis ")" or right bracket "]" is not paired with a corresponding left parenthesis "(" or bracket "[". For example, abc) matches "abc)" and 0-9] matches "0-9]".

  NOTE

  Unless otherwise specified, degeneration rules also apply when the preceding regular expressions are subexpressions within parentheses.

- Combination of common and special characters

  In actual usage, regular expressions combine multiple common and special characters to match certain strings.

Specifying a Filtering Mode in a Command

NOTE

- The device uses a regular expression to implement the pipe character filtering function. A display command supports the pipe character only when there is excessive output information.
- When filtering conditions are set to query output information, the first line of the command output starts with the entire regular expression but not the string to be filtered.

The system allows you to use **| count** to display the number of lines and **| section** to display the command output by section after using filtering mode. **| count** and **| section** can work together with the following filtering modes.

Three filtering modes are provided for commands that support regular expressions.

- **| begin** *regular-expression*: displays all the lines beginning with the line that matches the regular expression.

  Filter the character strings to be entered until the specified case-sensitive character string is displayed. All the character strings following this specified character string are displayed on the screen.
- **| exclude** *regular-expression*: displays all the lines that do not match the regular expression.

  If the character strings to be entered do not contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.
- **| include** *regular-expression*: displays all the lines that match the regular expression.

  If the character strings to be entered contain the specified case-sensitive character string, they are displayed on the screen. Otherwise, they are filtered.

NOTE

The value of *regular-expression* is a string of 1 to 255 characters. *regular-expression* cannot contain underlines ([).

The following examples describe how to specify a filter mode in a command.

Example 1: Run the **display interface brief** command to display all the lines that do not match the regular expression Ethernet|NULL|Tunnel. Ethernet|NULL|Tunnel matches Ethernet, NULL or Tunnel.

```
<Huawei> display interface brief | exclude Ethernet|NULL|Tunnel
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
^down: standby
(e): ETHOAM down
(d): Dampening Suppressed
InUti/OutUti: input utility/output utility
Interface                 PHY   Protocol InUti OutUti   inErrors  outErrors
LoopBack1                   up    up(s)      0%     0%         0          0
Vlanif7                    up    up         --     --         0          0
Vlanif10                   up    up         --     --         0          0
Vlanif19                   up    up         --     --         0          0
```

```
Vlanif60                up    up         --     --         0         0
Vlanif66                down  down       --     --         0         0
Vlanif70                down  down       --     --         0         0
Vlanif77                up    up         --     --         0         0
Vlanif100               down  down       --     --         0         0
```

Example 2: Run the **display current-configuration** command to display all the lines that match the regular expression vlan.

```
<Huawei> display current-configuration | include vlan
vlan batch 7 10 18 to 19 30 60 66 70 77 100 105
vlan batch 200 1024
 port default vlan 77
 port default vlan 19
 port hybrid pvid vlan 10
 port hybrid untagged vlan 10
 port hybrid pvid vlan 60
 undo port hybrid vlan 1
 port hybrid tagged vlan 60
 port trunk allow-pass vlan 60
 port hybrid pvid vlan 10
 port hybrid tagged vlan 7
 port hybrid untagged vlan 10
```

NOTE

The preceding information is used for reference only.

2.3 Configuration Examples

This section provides several examples that illustrate the use of command lines.

2.3.1 Example for Using Tab

Networking Requirements

The user wants to enter commands in fast and convenient mode to facilitate completion of service configurations. The device supports the function that the user enters the first character or first several characters of the keyword and presses **Tab** to complete the keyword, which improves input efficiency.

Configuration Roadmap

The configuration roadmap is as follows:

1. If there is only one match for the incomplete keyword, enter the incomplete keyword and press **Tab**.
2. If there are several matches for the keyword, enter the incomplete keyword and press **Tab** repeatedly until the desired keyword is displayed.
3. Enter the incorrect keyword and press **Tab**. In this case, the incorrect keyword remains unchanged.

Use **Tab** if:

There Is Only One Match for an Incomplete Keyword

1. Enter an incomplete keyword.

   ```
   [Huawei] info-
   ```

2. Press **Tab**.

   The system replaces the entered keyword and displays it in a new line with the complete keyword followed by a space.

```
[Huawei] info-center
```

There Are Several Matches for an Incomplete Keyword

The keyword **info-center** can be followed by the following keywords. (The command output provided here is used for reference only. The actual output information may differ from the following information.)

```
[Huawei] info-center ?
  channel            Set the name of information channel
  console            Setting of console configuration
  enable             Enable the infomation center
  filter-id          Specify the configuration of the ID filtering table
  local
  logbuffer          Setting of log buffer configuration
  logfile            <Group> logfile command group
  loghost            Setting of logging host configuration
  max-logfile-number  Setting of logfile numbers
  monitor            Setting of monitor configuration
  snmp               Setting of snmp configuration
  source             Informational source setting
  timestamp          Set the time stamp type of information
  trapbuffer         Setting of trap buffer configuration
```

1. Enter an incomplete keyword.

```
[Huawei] info-center log
```

2. Press **Tab**.

   The system displays the prefixes of all the matched keywords. In this example, the prefix is **log**.

```
[Huawei] info-center logbuffer
```

   Press **Tab** to switch from one matched keyword to another. In this case, the cursor closely follows the end of a word.

```
[Huawei] info-center logfile
[Huawei] info-center loghost
```

   Stop pressing **Tab** when the desired keyword is displayed.

An Incorrect keyword Is Entered

1. Enter an incorrect keyword.

```
[Huawei] info-center loglog
```

2. Press **Tab**.

```
[Huawei] info-center loglog
```

   The system displays information in a new line, but the keyword **loglog** remains unchanged and there is no space between the cursor and the keyword, indicating that this keyword does not exist.

2.3.2 Example for Defining Shortcut Keys

Networking Requirements

The user always uses a command to configure services and query information on any device in a network. The frequent command input brings a low efficiency; therefore, the user requires fast command input and execution.

Configuration Roadmap

1. Define shortcut keys to improve the command input efficiency. For example, define the shortcut key **Ctrl+U** and associate it with the **display ip routing-table** command. To view information in the routing table, press the shortcut key **Ctrl+U**.
2. Enter **Ctrl+U** at the prompt [Huawei] to run the defined command and view the execution result.

Procedure

Step 1 Define the shortcut key **Ctrl+U**, associate it with the **display ip routing-table** command, and run the command.

```
<Huawei> system-view
[Huawei] hotkey ctrl_u "display ip routing-table"
```

Step 2 Press **Ctrl+U** at the prompt of [Huawei] to run the **display ip routing-table** command.

```
[Huawei] display ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 13        Routes : 13

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        0.0.0.0/0   Static  60   0           RD   192.168.200.100 GigabitEthernet1/0/0
        1.1.1.1/32  Direct  0    0           D    127.0.0.1       LoopBack0
    20.20.20.0/24   Direct  0    0           D    20.20.20.2      GigabitEthernet2/0/0
    20.20.20.2/32   Direct  0    0           D    127.0.0.1       GigabitEthernet2/0/0
  20.20.20.255/32   Direct  0    0           D    127.0.0.1       GigabitEthernet2/0/0
   101.101.1.0/24   OSPF    10   2           D    20.20.20.3      GigabitEthernet2/0/0
      127.0.0.0/8   Direct  0    0           D    127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D    127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D    127.0.0.1       InLoopBack0
  192.168.200.0/24  Direct  0    0           D    192.168.200.160 GigabitEthernet1/0/0
192.168.200.160/32  Direct  0    0           D    127.0.0.1       GigabitEthernet1/0/0
192.168.200.255/32  Direct  0    0           D    127.0.0.1       GigabitEthernet1/0/0
255.255.255.255/32  Direct  0    0           D    127.0.0.1       InLoopBack0
```

----End

3 Basic Configurations Commands

About This Chapter

3.1 CLI Overview Commands
3.2 Auto-Config Commands
3.3 Auto-Start Configuration Commands
3.4 USB-based Deployment Configuration Commands
3.5 SMS-based Deployment Configuration Commands
3.6 Fast Provisioning Configuration Commands
3.7 First Login Commands
3.8 UI Configuration Commands
3.9 User Login Configuration Commands
3.10 HTTP Server Commands
3.11 File Management Commands
3.12 Configuring System Startup Commands
3.13 Upgrade Commands
3.14 Smart Upgrade Commands

3.1 CLI Overview Commands

3.1.1 assistant task

Function

The **assistant task** command creates an assistant task.

The **undo assistant task** command deletes an assistant task.

By default, no assistant task is created.

Format

assistant task *task-name*

undo assistant task *task-name*

Parameters

Parameter	Description	Value
task-name	Specifies the name of an assistant task.	The value is a string of 1 to 15 characters. It can consist of underscores (_), letters, and digits only, and must start with a letter.

Views

System view

Default Level

3: Management level

Usage Guidelines

An assistant task is a virtual assistant on the device to realize automatic maintenance and management. After you create an assistant task and bind it to a batch of files to be processed, the device performs operations or configurations when it is unattended. Assistant tasks are mainly used for scheduled system upgrade or configuration.

NOTE

You can create a maximum of five assistant tasks on the device.

Example

Create an assistant task.

```
<Huawei> system-view
[Huawei] assistant task test
```

Related Topics

3.1.5 display assistant task history

3.1.12 if-match timer cron

3.1.13 perform batch-file

3.1.2 cls

Function

The **cls** command clears the current screen.

Format

cls

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

This command only clears the screen and does not clear the screen buffer.

Example

Clear screen.

```
<Huawei> cls
Info: Current terminal monitor is off.
Info: Current terminal debugging is off.
```

3.1.3 command-privilege level

Function

The **command-privilege level** command sets the command level in a specified view.

The **undo command-privilege** command restores the default command level.

By default, each command in each view has a default command level.

Format

command-privilege level *level* **view** *view-name command-key*

undo command-privilege view *view-name command-key*

Parameters

Parameter	Description	Value
level *level*	Specifies the command level.	The value is an integer that ranges from 0 to 15.
view *view-name*	Specifies the view name. You can enter a question mark (?) in the terminal GUI to obtain all view names in the command view.	-
command-key	Specifies a command. The command must be entered manually because automatic command line completion is not supported.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system divides commands into four levels and sets the command level in the specified view. The device administrator can change the command level as required, so that a lower-level user can use some high-level commands. The device administrator can also change the command level to a larger value to improve device security.

When using this command to change the level of a command, you can run the **display command-view** *command-key* command to check the view of the specified command. You can also check common views in **Table 3-1**.

Table 3-1 Common Views

View	View Name
cli_8f	All views
user	User view
system	System view
aaa	AAA view
async	Async interface view

 Copyright © Huawei Technologies Co., Ltd.

View	View Name
eth-trunk	Eth-Trunk interface view
gigabitethernet	GE interface view
loopBack	Loopback interface view
vlanif	VLANIF interface view
voice	Voice view

Precautions

You are not advised to change the default command level. If you need to change it, consult with professional personnel to ensure that routine operation and maintenance are not affected and security risk is avoided.

The rules for using this command to set the command level of a specified view are as follows:

- When you degrade the target command, all keywords in the command are degraded.
- When you upgrade the target command, only the last keyword in the command is upgraded.
- When you set a level for the target command, the levels of all commands (in the same view) starting with this command are changed.
- When you set a level for the target command, the keyword level in other commands having the same index as the keyword whose level is changed is also changed.
- If the level of keywords that have the same index is modified for multiple times, the latest configured level takes effect.
- This command is not supported in a dual-SRU scenario.

Example

Set the privilege level of the **save** command to 5.

```
<Huawei> system-view
[Huawei] command-privilege level 5 view cli_8f save
```

Related Topics

3.8.24 user privilege

3.1.4 diagnose

Function

The **diagnose** command enters the diagnostic view from the system view.

Format

diagnose

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Diagnostic commands are mainly used for fault diagnosis. However, running some commands may cause device faults or service interruptions. Therefore, use these commands under the instruction of Huawei technical engineers.

Example

Enter the diagnostic view.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose]
```

3.1.5 display assistant task history

Function

The **display assistant task history** command displays operation records of an assistant task.

Format

display assistant task history [*task-name*]

Parameters

Parameter	Description	Value
task-name	Specifies the name of an existing assistant task.	The value is a string of 1 to 15 characters consisting only of underscores (_), letters, and digits, and must start with a letter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The latest five operations of each assistant task are displayed in an earlier-to-later order.

Example

Displays operation records of an assistant task.

```
<Huawei> display assistant task history
-------------------------------------------------------------------------------
Assistant task name: nemo
-------------------------------------------------------------------------------
Assistant task name: song
 Action type    : Batch file
 Batch file name: sd1:/reboottest.bat
 Start time     : 2012-07-16 09:25:00
 End time       : 2012-07-16 09:25:00
 State          : Finished

 Action type    : Batch file
 Batch file name: sd1:/reboottest.bat
 Start time     : 2012-07-16 09:24:00
 End time       : 2012-07-16 09:24:00
 State          : Finished

-------------------------------------------------------------------------------
Assistant task name: xu
 Action type    : Batch file
 Batch file name: sd1:/reboottest.bat
 Start time     : 2012-07-16 09:25:00
 End time       : 2012-07-16 09:25:00
 State          : Finished

 Action type    : Batch file
 Batch file name: sd1:/reboottest.bat
 Start time     : 2012-07-16 09:24:00
 End time       : 2012-07-16 09:24:00
 State          : Finished

 Action type    : Batch file
 Batch file name: sd1:/reboottest.bat
 Start time     : 2012-07-16 09:23:00
 End time       : 2012-07-16 09:23:00
 State          : Finished

-------------------------------------------------------------------------------
```

Table 3-2 Description of the **display assistant task history** command output

Item	Description
Assistant task name	Task name. This parameter is configured using the **assistant task** command.
Action type	Operation that an assistant task performs.

Item	Description
Batch file name	Name of the batch file used by an assistant task. This parameter is configured using the **perform batch-file** command.
Start time	Operation start time of an assistant task.
End time	Operation end time of an assistant task.
State	Running status of an assistant task. • Running indicates that the assistant task is in operation. • Finished indicates that the assistant task has finished operation.

Related Topics

3.1.1 assistant task

3.1.12 if-match timer cron

3.1.13 perform batch-file

3.1.6 display command-view

Function

The **display command-view** command displays the view of a specified command.

Format

display command-view *command-key*

Parameters

Parameter	Description	Value
command-key	Specifies the command word of the command to be queried. Currently, the command word cannot be automatically displayed through the question mark help function, and needs to be entered manually.	The value is a string of 1 to 200 case-insensitive characters that can include spaces.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

You can run this command to check the view of a specified command. For example, if you need to run the **command-privilege level** command to change the level of a specified command, run the **display command-view** command to check the view of the specified command.

Example

Display the view of the **if-match timer cron** command.

```
<Huawei> system-view
[Huawei] display command-view if-match timer cron
 It will take several minutes, please wait.........

 Matching result(s):
 ----------------
 assistant-task
 ----------------
```

Table 3-3 Description of the **display command-view** command output

Item	Description
Matching result(s)	Query result. **NOTE** The return value **cli_8f** indicates all views.

Related Topics

3.1.3 command-privilege level

3.1.7 display history-command

Function

The **display history-command** command displays the historical commands stored on the current device.

Format

display history-command

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check historical commands the user has executed recently. This command facilitates information search. Historical commands are stored in the circular mode and a maximum of 200 historical commands can be displayed.

Precautions

All the historical commands entered by a user are automatically saved on the terminal, that is, any input that ends with **Enter** is saved as a historical command.

NOTE

- Historical commands are saved in the same format as that used in the input. If a command that is entered by a user is in an incomplete format, the saved historical command is also in the incomplete format.
- If a user runs a command several times, only the latest command is saved on the device. If the command is entered in different formats, they are considered as different commands.

You can view historical commands using the following methods:

- To view the previous historical command, press the Up arrow key or **Ctrl+P**.

  If there is an earlier historical command, the earlier historical command is displayed.
- To view the next historical command, press the Down arrow key or **Ctrl+N**.

  If there is a new historical command, the new historical command is displayed.

Example

Display the historical commands that have been executed on the current terminal.

```
<Huawei> display history-command
 quit
 user privilege level 15
 user-interface vty 0 4
 system-view
```

Related Topics

3.8.14 history-command max-size

3.1.8 display hotkey

Function

The **display hotkey** command displays the status of the defined, undefined, and system hotkeys.

Format

display hotkey

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you understand the defined, undefined, and system hotkeys in the system, you can use hotkeys to quickly enter commands. To redefine hotkeys for a command, run the **hotkey** command.

The system allows hotkeys in places where commands can be entered, and displays the commands corresponding to hotkeys. You can run the **display hotkey** command to view the commands corresponding to hotkeys.

Example

Display defined, undefined, and system hotkeys.

```
<Huawei> display hotkey
----------------- HOTKEY -----------------

           =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  undo idle-timeout
CTRL_O  undo debugging all

          =Undefined hotkeys=
Hotkeys Command
CTRL_U  NULL

           =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the first line
CTRL_B  Move the cursor one character left
CTRL_C  Stop current command function
CTRL_D  Erase current character
CTRL_E  Move the cursor to the end of the Last line
CTRL_F  Move the cursor one character right
CTRL_H  Erase the character left of the cursor
CTRL_K  Kill outgoing connection when connecting
CTRL_N  Display the next command from the history buffer
CTRL_P  Display the previous command from the history buffer
CTRL_T  Function as a question mark
CTRL_W  Delete the word left of the cursor
CTRL_X  Delete all characters up to the cursor
CTRL_Y  Delete all characters after the cursor
CTRL_Z  Return to the user view
CTRL_]  Kill incoming connection or redirect connection
```

 Copyright © Huawei Technologies Co., Ltd.

```
ESC_B   Move the cursor one word back
ESC_D   Delete remainder of word
ESC_F   Move the cursor forward one word
```

Table 3-4 Description of the display hotkey command output

Item	Description
Defined hotkeys	Defined hotkeys.
Undefined hotkeys	Undefined hotkeys.
System hotkeys	System hotkeys.

Related Topics

3.1.11 hotkey

3.1.9 display this

Function

The **display this** command displays the running configuration in the current view.

Format

display this

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the configurations are complete in a certain view, run the **display this** command to check the current configurations.

Precautions

If a configuration parameter uses the default value, this parameter is not displayed. The set parameters that do not be committed successfully are neither displayed.

If you run the **display this** command in an interface view, configuration of the interface view is displayed. If you run this command in a protocol view, configuration of the protocol view is displayed.

Example

Display the running configuration in the current view.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] display this
#
interface Ethernet2/0/0
 port link-type trunk
#
return
```

3.1.10 header

Function

The **header** command configures the header information displayed on a terminal when users log in to a connected device.

The **undo header** command deletes the header information displayed on a terminal when users log in to a connected device.

By default, no header information is displayed on terminals when users log in to a connected device.

Format

header { **login** | **shell** } { **information** *text* | **file** *file-name* }

undo header { **login** | **shell** }

Parameters

Parameter	Description	Value
login	Indicates header information displayed on a terminal when a user logs in to the device and a connection between the terminal and the device is activated.	-
shell	Indicates the header displayed on a terminal when the session is set up after the user logs in to the connected device.	-

Parameter	Description	Value
information *text*	Specifies the header and content.	The value is a string with spaces and carriage returns supported. The maximum length of the string that can be entered at one time is 220 characters, if a linefeed is contained in the first line. If no linefeed is contained in the first line, a maximum of 480 characters can be entered at one time, and the total string length ranges from 1 to 2000 characters.
file *file-name*	Specifies the file name that the header uses.	The value is a string of 5 to 64 characters. The maximum header file size is 128 KB. If the file size is greater than 128 KB, only the first 128 KB file information can be displayed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide some prompts or alarms to users, you can use the **header** command to configure a title on the device. If a user logs in to the device, the title is displayed.

Procedure

If **information** is specified, the header text starts and ends with the same character. You can set the header text in either of the following modes:

- Non-interactive: enter the header text behind the start character.

  Use the same character at the beginning and end of the header and press **Enter**. If the start and end characters are inconsistent, the system prompts an error message.
- Interactive: enter the start character and press **Enter**.

  The system displays a message prompting the correct header information. Then enter the required information and enter the same character at the beginning and end of the header, and press **Enter**. The system quits the interactive process.

  During interaction, you can press **Enter** at any time to enter information in the next line.

Precautions

- Before setting the **login** parameter, you must set login authentication parameters; otherwise, no header information about authentication is displayed.
- Before setting the **file** parameter, ensure that the file containing the header exists; otherwise, the file name cannot be obtained.
- If the **file** parameter is set, save the file containing the header in the root directory of the default storage media. To save the file to another directory, you must use a full path.
- If you use SSH1.X to log in to the device, the shell header rather than the login header is displayed.
- If you use SSH2.0 to log in to the device, both login and shell headers are displayed in the login process.
- If the header command is configured several times, only the latest configuration takes effect.
- After the login title is configured, any user that logs in to the system can view the title.
- The start and end characters in the header text can be double quotation marks ("). However, the header text content cannot contain double quotation marks ("").

Example

Configure a shell header. (non-interactive process)

```
<Huawei> system-view
[Huawei] header shell information &Hello! Welcome to system!&      # Enter the header text behind the start character '&' and enter '&' at the end of the header text, and press Enter.
```

Display the shell header if the login succeeds.

```
Hello! Welcome to system!
```

Configure a shell header (interactive process).

```
<Huawei> system-view
[Huawei] header shell information %      # Press Enter after entering the start character '%' to start the interactive process.
Info: Input banner text, and quit with the character '%'. Hello!
Welcome to system!%
[Huawei] quit
<Huawei> quit      // Log off.
```

Press **Enter**. The shell header is displayed when the user logs in again.

```
Hello!
Welcome to system!
<Huawei>
```

Specify the file that stores a login header.

```
<Huawei> system-view
[Huawei] header login file sd1:/header-file.txt
```

3.1.11 hotkey

Function

The **hotkey** command sets a shortcut key for a command.

The **undo hotkey** restores the system shortcut keys to the default values.

By default, the system sets the default values for three shortcut keys CTRL+G, CTRL+L, and CTRL+O, while does not set default value for CTRL+U.

Format

hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_U** } *command-text*

undo hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_U** }

Parameters

Parameter	Description	Value
CTRL_G	Specifies the shortcut key **Ctrl+G** for a command.	-
CTRL_L	Specifies the shortcut key **Ctrl+L** for a command.	-
CTRL_O	Specifies the shortcut key **Ctrl+O** for a command.	-
CTRL_U	Specifies the shortcut key **Ctrl+U** for a command.	-
command-text	Specifies the associated command line for shortcut keys.	The value is a string of 1 to 240 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set a shortcut key for a command that is often used; you can also change the default value of the shortcut key that is defined by the system according to your requirements.

Precautions

Four shortcut keys are customized by users: **CTRL+G**, **CTRL+L**, **CTRL+O**, and **CTRL +U**.

- By default, the shortcut key **CTRL+G** corresponds to the **display current-configuration** command which displays current configuration.
- By default, the shortcut key **CTRL+L** corresponds to the **undo idle-timeout** command which restores the default timeout period.

 Copyright © Huawei Technologies Co., Ltd.

- By default, the shortcut key **CTRL+O** corresponds to the **undo debugging all** command which stops the output of all debugging information.

After you use the **hotkey** command to set a shortcut key for a command, you can run the command by pressing the shortcut key or entering a command.

NOTE

One shortcut key can be set for only one command. If you set a shortcut key for multiple commands, only the latest configuration takes effect.

When assigning a command for a shortcut key, you need to mark the command with double quotation marks if the command consists of several words, that is, the command includes spaces. You do not need to mark the command with double quotation marks if the command consists of only one word.

Example

Assign the **display tcp status** command for the shortcut key **CTRL+L**.

```
<Huawei> system-view
[Huawei] hotkey ctrl_l "display tcp status"
[Huawei] commit
[Huawei] display hotkey
----------------- HOTKEY -----------------

          =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display tcp status
CTRL_O  undo debugging all

         =Undefined hotkeys=
Hotkeys Command
CTRL_U  NULL

          =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the first line
CTRL_B  Move the cursor one character left
CTRL_C  Stop current command function
CTRL_D  Erase current character
CTRL_E  Move the cursor to the end of the Last line
CTRL_F  Move the cursor one character right
CTRL_H  Erase the character left of the cursor
CTRL_K  Kill outgoing connection when connecting
CTRL_N  Display the next command from the history buffer
CTRL_P  Display the previous command from the history buffer
CTRL_T  Function as a question mark
CTRL_W  Delete the word left of the cursor
CTRL_X  Delete all characters up to the cursor
CTRL_Y  Delete all characters after the cursor
CTRL_Z  Return to the user view
CTRL_]  Kill incoming connection or redirect connection
ESC_B   Move the cursor one word back
ESC_D   Delete remainder of word
ESC_F   Move the cursor forward one word
```

Related Topics

3.1.8 display hotkey

3.1.12 if-match timer cron

Function

The **if-match timer cron** command sets the time to perform an assistant task.

The **undo if-match timer cron** command cancels the time configured for an assistant task.

By default, the time to perform an assistant task is not specified.

Format

if-match timer cron *seconds minutes hours days-of-month months days-of-week* [*years*]

undo if-match timer cron

Parameters

Parameter	Description	Value
seconds	Sets second.	The value is a string of characters in the cron format. A cron time string consists of digits (0 to 9) and special characters asterisk (*), hyphen (-), slash (/), and comma (,). The value ranges from 1 to 127. Currently, the device supports asterisk (*) only, indicating that the value is accurate to minute but not second.
minutes	Sets minute.	The value is a string of characters in the cron format. A cron time string consists of digits (0 to 9) and special characters asterisk (*), hyphen (-), slash (/), and comma (,). The value ranges from 1 to 127.
hours	Sets hour	The value is a string of characters in the cron format. A cron time string consists of digits (0 to 9) and special characters asterisk (*), hyphen (-), slash (/), and comma (,). The value ranges from 1 to 127.
days-of-month	Sets date.	The value is a string of characters in the cron format. A cron time string consists of digits (0 to 9) and special characters asterisk (*), hyphen (-), slash (/), and comma (,). The value ranges from 1 to 127. This parameter is exclusive with the *days-of-week* parameter. At least one of the two contains asterisk (*).
months	Sets month.	The value is a string of characters in the cron format. A cron time string consists of digits (0 to 9) and special characters asterisk (*), hyphen (-), slash (/), and comma (,). The value ranges from 1 to 127.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
days-of-week	Sets week.	The value is a string of characters in the cron format. A cron time string consists of digits (0 to 9) and special characters asterisk (*), hyphen (-), slash (/), and comma (,). The value ranges from 1 to 127. The parameter is exclusive with the *days-of-month* parameter. At least one of the two contains asterisk (*).
years	Sets year.	The value is a string of characters in the cron format. A cron time string consists of digits (0 to 9) and special characters asterisk (*), hyphen (-), slash (/), and comma (,). The value ranges from 1 to 127. If this parameter is not specified, it refers to all the years between 2000 to 2099.

Views

Assistant task view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **if-match timer cron** command is used to set the time to perform an assistant task. The time is expressed in the cron format defined in UNIX or Linux.

The commonly used time format (hh:mm:ss dd-mm-yyyy) can specify only one specific time value. The cron time format is more flexible and powerful and uses simple methods to display single or multiple time, duration, and period. The method is as follows:

- Valid characters include digits 0 to 9, and special characters asterisk (*), hyphen (-), slash (/), and comma (,).
- This table shows the syntax of cron format:

Expression Mode	Format	Description	Example
Single time point	<time>	<time>: The value is an integer that specifies a specific time value. The value range is dependent on specific parameter. The range of minutes is 0 to 59. The range of hours is 0 to 23. The range of days-of-month depends on the number of days in a specific month. The range of months is 1 to 12. The range of days-of-week is 0 to 7. The range of years is 2000 to 2099.	Command: if-match timer cron * 0 1 2 5 * 2012 Meaning: perform an assistant task at 1:00 on May 2, 2012.
Multiple time points	<time1>,<time2>,...,<timen>	<timen>: The value is an integer. The value range depends on specific parameter. Multiple time points are separated by a comma (,) with no space before or behind it. The time values in a list can be arranged at any sequence.	Command: if-match timer cron * 0 1,2,3 2 3 * 2012 Meaning: perform an assistant task at the following time points: ● 1:00, March 2, 2012 ● 2:00, March 2, 2012 ● 3:00, March 2, 2012

 Copyright © Huawei Technologies Co., Ltd.

Expression Mode	Format	Description	Example
Specific time point	<time>/<step>	<time>: The value is an integer that specifies a specific time value. <step>: The value is an integer that specifies the time incremental. The two values are separated by a slash (/) with no space before or behind it. The format: <time>,<time>+<step>,<time>+2*<step>,...,<time>+n*<step>. The maximum time (<time>+n*<step>) depends on specific parameter in the command line.	Command: if-match timer cron * 0 0/10 * 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 10:00, March 1, 2012 ● 20:00, March 1, 2012 ● 0:00, March 2, 2012 ● ... ● 10:00, March 2, 2012 ● 20:00, March 2, 2012

 Copyright © Huawei Technologies Co., Ltd.

Expression Mode	Format	Description	Example
Duration	<time1>-<time2>	<time1> and <time2>: The values are integers, specifying the start and end time respectively. <time2> must be later than or equal to <time1>. The two values are separated by a hyphen (—) with no space before or behind it. the <time1>-<time2> is same with <time1>,<time1>+1,<time1>+2, ……,<time2>. If <time1> and <time2> are the same, the two specify the same time point.	Command: if-match timer cron *0 0-3 1 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 1:00, March 1, 2012 ● 2:00, March 1, 2012 ● 3:00, March 1, 2012
Period	*	If the parameter in the command line is set to *, the parameter may refer to any time point. By setting the parameter to *, you can configure the system to periodically perform an assistant task every year, week, month, day, hour, or minute.	Command: if-match timer cron * 30 10 * 1 1 2012 Meaning: perform an assistant task at 10:30, Monday every week in January, 2012.

 Copyright © Huawei Technologies Co., Ltd.

Expression Mode	Format	Description	Example
Combination	Combination format	All the expression modes can be combined except "period". The expression modes are separated by a comma (,) with no space before or behind it.	Command: if-match timer cron * 0 0/10,2,4-5 1 3 * 2012 Meaning: perform an assistant task at the following time points: ● 0:00, March 1, 2012 ● 2:00, March 1, 2012 ● 4:00, March 1, 2012 ● 5:00, March 1, 2012 ● 10:00, March 1, 2012 ● 20:00, March 1, 2012

Precautions

- If you run this command multiple times in the same view, only the latest configuration takes effect.
- The *days-of-month* and *days-of-week* parameters are exclusive. Set one or both of them to "*". If one parameter is set to *, the other one specifies a specific date. If both parameters are set to *, they can refer to any date.
- The minimum unit supported is second, so set the second parameter to *. The specified assistant task can work only once every minute.
- Since the system can perform only one assistant task at a time, the time when one assistant task finished working may be later than the time when the next task is schedule to start. There may be a time span between the time when an assistant task is scheduled to work and the time when it actually starts to work. The **if-match timer cron** command specifies the time when an assistant task is scheduled to work.
- When you enter digits, such as 000002012, the numeric string means the same as 2012.

Example

Configure an assistant task to work at 20:00, 2012-05-04.

```
<Huawei> system-view
[Huawei] assistant task test
[Huawei-assistant-task-test] if-match timer cron * 0 20 4 5 * 2012
[Huawei-assistant-task-test] perform 1 batch-file sys.bat
```

Cancel the time for an assistant task to start to work.

```
<Huawei> system-view
[Huawei] assistant task test
[Huawei-assistant-task-test] undo if-match timer cron
```

Related Topics

3.1.1 assistant task
3.1.5 display assistant task history
3.1.13 perform batch-file

3.1.13 perform batch-file

Function

The **perform batch-file** command configures an assistant task to process a batch file.

The **undo perform** command disables the assistant task from processing a batch file.

By default, no batch file is configured for the assistant task.

Format

perform *priority* **batch-file** *filename*

undo perform *priority*

Parameters

Parameter	Description	Value
priority	Specifies the priority of an assistant task.	It has a fixed value of 1 at current because one assistant task can process only one batch file.
filename	Specifies the name of the batch file processed by the assistant task. The file name is in the *.bat format.	The value is a string of 5 to 64 case-insensitive characters without spaces.

Views

Assistant task template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After you successfully create an assistant task and specify the execution time, you can run this command to configure the device to process a batch file at the specified time.

Prerequisites

An assistant task has been created using the **assistant task** command and the time at which the task is executed has been specified using the **if-match timer cron** command.

Precautions

If an assistant task is being executed, stop the assistant task before you can delete it. If an assistant task is to be executed, directly delete it. The device will not execute the assistant task later.

By default, the commands listed in the batch file are executed in the system view.

Example

Configure the assistant task **huawei** to process the batch file **sys.bat** at 2012-05-04 20:00.

```
<Huawei> system-view
[Huawei] assistant task huawei
[Huawei-assistant-task-huawei] if-match timer cron * 0 20 4 5 * 2012
[Huawei-assistant-task-huawei] perform 1 batch-file sys.bat
```

Disable the assistant task to process the batch file.

```
<Huawei> system-view
[Huawei] assistant task huawei
[Huawei-assistant-task-huawei] undo perform 1
Info: Start to delete the action.
[Huawei-assistant-task-huawei] display this
#
assistant task huawei
 if-match timer cron * 0 20 4 5 * 2012
#
return
```

Related Topics

3.1.1 assistant task

3.1.5 display assistant task history

3.1.12 if-match timer cron

3.1.14 quit

Function

The **quit** command returns from the current view to a lower-level view. If the current view is the user view, this command exits from the system.

Format

quit

Parameters

None

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Three types of views are available and they are listed as follows from a lower level to a higher level:

- User view
- System view
- Service view, such as interface view

Run the **quit** command to return to a lower-level command view from the current view. If you are in the user view currently, after you run the **quit** command, you quit from the system.

Example

Return to the system view from the AAA view, and then return to the user view. After this, quit the system.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] quit
[Huawei] quit
<Huawei> quit
```

Related Topics

3.1.17 system-view

3.1.15 return

3.1.15 return

Function

The **return** command returns to the user view from other views except the user view.

Format

return

Parameters

None

Views

All views

Default Level

0: Visit level

Usage Guidelines

In other views, you can use the **return** command to return to the user view.

- Run this command to return to the user view if the current view is another view except the user view.
- If the current view is the user view, no change occurs after running this command.
- The shortcut keys<**Ctrl+Z**> have the same function as the **return** command.

Example

Return to the user view from the user interface view.

```
<Huawei> system-view
[Huawei] user-interface vty 0
[Huawei-ui-vty0] return
<Huawei>
```

Related Topics

3.1.17 system-view

3.1.16 set current-configuration display

Function

The **set current-configuration display** command sets the configurations that the user of a specified level can view.

The **undo set current-configuration display** command cancels the configuration.

By default, no configuration is specified for users.

Format

set current-configuration display [**all**] **level** *level command-key*

undo set current-configuration display [**all**] **level** *level command-key*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
all	Indicates that all configuration sub-items are displayed if the configuration contains sub-items.	-
level *level*	Specifies the user level.	The value is an integer ranging from 0 to 15.
command-key	Specifies the command of which the output will be displayed.	The value is a string of 1 to 255 case-sensitive characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

After the administrator runs the **command-privilege level** command to degrade the level of **display current-configuration**, low-level users can run the **display current-configuration** command to view all device configurations.

To allow the low-level users to view the specified configurations, the administrator can run the **set current-configuration display** command to specify the configurations to be displayed.

Precaution

- If you enter a part of a command in the *command-key* parameter, the system matches the commands starting with the characters you entered.
- If the command specified in *command-key* is executed in a sub-view, the **display current-configuration** command displays the configurations in the parent view.
- To view all configuration sub-items in a configuration item, use the **all** keyword.
- If you run the **set current-configuration display** command multiple times, multiple configurations can be specified. You can specify 128 configurations for the user of the certain level.

Example

Set the **display current-configuration** command level to 0 and specify the configurations that level-0 users can view.

```
<Huawei> system-view
[Huawei] command-privilege level 0 view cli_8f display current-configuration
```

```
[Huawei] set current-configuration display level 0 ip address
[Huawei] set current-configuration display level 0 aaa
[Huawei] set current-configuration display level 0 network
```

Display configurations as a level-0 user.

```
<Huawei> display current-configuration
#
aaa
#
interface GigabitEthernet0/0/0
 ip address 192.168.200.183 255.255.255.0
#
interface LoopBack0
 ip address 10.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
return
```

Specify other configurations that level-0 user can view.

```
<Huawei> system-view
[Huawei] set current-configuration display all level 0 aaa
```

Display configurations as a level-0 user.

```
<Huawei> display current-configuration
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user huawei password cipher %$%$^XcfPki5NVJ)ceVfc.;-f''Ei%$%$
 local-user huawei privilege level 3
#
interface GigabitEthernet0/0/0
 ip address 192.168.200.183 255.255.255.0
#
interface LoopBack0
 ip address 10.168.1.1 255.255.255.0
#
ospf 1
 area 0.0.0.0
  network 10.168.1.0 0.0.0.255
  network 172.16.1.0 0.0.0.255
#
return
```

3.1.17 system-view

Function

The **system-view** command enables you to enter the system view from the user view.

Format

system-view

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You must configure the device in the system view. Run this command in the user view to enter the system view.

Example

Enter the system view.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei]
```

Related Topics

3.1.14 quit

3.1.15 return

3.2 Auto-Config Commands

NOTE

- AR100 series, AR120 series (except AR129 and AR129GW-L), AR150 series (except AR156, AR156W, AR157, AR157G-HSPA+7, AR157VW, AR157W, AR158E, and AR158EVW), AR160 series (except AR161FW-P-M5), AR201, AR1200 series, AR2200 series, and AR3200 series support Auto-Config function.
- The management interfaces of the AR1200, AR2200, AR3200, and AR3600 series do not support the Auto-Config function.

3.2.1 autoconfig enable

Function

The **autoconfig enable** command enables Auto-Config.

The **undo autoconfig enable** command disables Auto-Config.

By default, Auto-Config is enabled on the device.

NOTE

Auto-Config is disabled on the device by default for AR169-P-M9, AR169W-P-M9, AR169RW-P-M9.

Format

autoconfig enable

undo autoconfig enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Auto-Config enables devices to be configured must be new devices or have no configuration files to automatically load version files including system software, patch files, configuration files when the device starts up.

You can configure the Auto-Config function only after it is enabled. The **autoconfig enable** command is used in the following scenarios:

- Auto-Config is disabled on the device (You can run the **3.2.5 display autoconfig enable** command to check whether Auto-Config is enabled). In such a case, you can use the **autoconfig enable** command to enable Auto-Config.
- If the Auto-Config function cannot be automatically recovered after an error occurs in the Auto-Config process, run the **undo autoconfig enable** command to disable the Auto-Config function. After Auto-Config stops, run the **autoconfig enable** command to enable Auto-Config again. You can use the **3.2.6 display autoconfig-status** command to check whether Auto-Config is enabled.

Example

Enable Auto-Config.

```
<Huawei> system-view
[Huawei] autoconfig enable
Info: Enable autoconfig successfully.
```

Related Topics

3.2.2 autoconfig getting-file restart

3.2.3 display autoconfig activating-config delay

3.2.4 display autoconfig activating-config remanent-time

3.2.5 display autoconfig enable

3.2.6 display autoconfig-status

 Copyright © Huawei Technologies Co., Ltd.

3.2.2 autoconfig getting-file restart

Function

The **autoconfig getting-file restart** command enables the device to re-obtain the intermediate file, the system software, patch file and configuration file from the file server.

Format

autoconfig getting-file restart

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the device fails to obtain the intermediate file, system software, patch file or configuration file, the Auto-Config process is suspended and needs to be restarted. The **autoconfig getting-file restart** command restarts the Auto-Config process, enabling the device to re-obtain the intermediate file, system software, patch file and configuration file. The **3.2.6 display autoconfig-status** command displays whether the Auto-Config process is suspended.

NOTE

This command can be executed only when obtaining files failed and the Auto-Config process is suspended.

Example

Configure the device to re-obtain files from the file server and continue the AutoConfig process.

```
<Huawei> system-view
[Huawei] autoconfig getting-file restart
```

Related Topics

3.2.1 autoconfig enable

3.2.5 display autoconfig enable

3.2.6 display autoconfig-status

 Copyright © Huawei Technologies Co., Ltd.

3.2.3 display autoconfig activating-config delay

Function

The **display autoconfig activating-config delay** command displays the delay in restarting a device after a configuration file is downloaded using Auto-Config.

Format

display autoconfig activating-config delay

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a user uses the Option 146 parameter to set the delay in restarting a device, there is a delay in restarting the device after the version file, patch file, and configuration file are downloaded using Auto-Config. After the device is restarted, loaded files can take effect. Run the **display autoconfig activating-config delay** command to check the configured delay in restarting a device.

Precautions

By default, the device is restarted immediately if no delay is set using the Option 146 parameter.

Example

Display the delay in restarting a device after a configuration file is downloaded using Auto-Config.

```
<Huawei> display autoconfig activating-config delay
The delay in activating configuration is 0 seconds.
```

Related Topics

3.2.4 display autoconfig activating-config remanent-time

3.2.4 display autoconfig activating-config remanent-time

Function

The **display autoconfig activating-config remanent-time** command displays the remaining delay in restarting a device after a configuration file is downloaded using Auto-Config.

Format

display autoconfig activating-config remanent-time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a user uses the Option 146 parameter to set the delay in restarting a device, there is a delay in restarting the device after the version file, patch file, and configuration file are downloaded using Auto-Config. After the device is restarted, loaded files can take effect. Run the **display autoconfig activating-config remanent-time** command to check the remaining delay in restarting a device.

Precautions

By default, the device is restarted immediately if no delay is set using the Option 146 parameter.

Example

Display the remaining delay in restarting a device after a configuration file is downloaded using Auto-Config.

```
<Huawei> display autoconfig activating-config remanent-time
The remanent time of activating configuration is 10 seconds.
```

Related Topics

3.2.3 display autoconfig activating-config delay

3.2.5 display autoconfig enable

Function

The **display autoconfig enable** command displays whether Auto-Config is enabled.

Format

display autoconfig enable

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Auto-Config runs only after it is enabled. You can run the **display autoconfig enable** command to check whether Auto-Config is enabled to ensure that Auto-Config runs properly.

Example

Check whether Auto-Config is enabled.

```
<Huawei> display autoconfig enable
Autoconfig is enabled.
```

Related Topics

3.2.1 autoconfig enable

3.2.6 display autoconfig-status

Function

The **display autoconfig-status** command displays the running status of Auto-Config.

Format

display autoconfig-status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the configuration and running status of Auto-Config.

```
<Huawei> display autoconfig-status

Running: No

Can deploy configurations with a USB disk: Yes

Stop   : Yes
Reason : Current startup configuration file already exists.

Suspend: No
Reason : --

The status of DHCP phase:
Operation result: --
Failed reason   : --

The status of setting ACS phase:
URL             : --
User name       : --
Password        : --
Operation result: --
Failed reason   : --

The status of getting middle file phase:
File name       : --
Operation result: --
Failed reason   : --

The status of getting system software phase:
File name       : --
Operation result: --
Failed reason   : --

The status of getting patch file phase:
File name       : --
Operation result: --
Failed reason   : --

The status of getting configuration file phase:
File name       : --
Operation result: --
Failed reason   : --

The status of activating configuration phase:
```

```
Remained time   : --
Operation result: --
Failed reason   : --
```

Table 3-5 Description of the display autoconfig-status command output

Item	Description
Running	Whether Auto-Config is running.
Can deploy configurations with a USB disk	Whether a USB disk can be used for deployment. **NOTE** The device can be configured using Auto-Config or USB deployment. However, two deployment methods cannot be used together.
Stop	Whether Auto-Config stops.
Reason	Reason that Auto-Config stops: ● AutoConfig is disabled. ● Current startup configuration file already exists.
Suspend	Whether Auto-Config is suspended.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Reason that Auto-Config is suspended: ● Autoconfig is completed. ● Connecting to file server failed. ● Deploying configurations with a USB disk. ● Failed to get the TFTP server address from the host. ● Getting file server information failed. ● Getting system MAC address and ESN failed. ● Getting system MAC address failed and the ESN is wrong. ● Getting system ESN failed and the MAC address is wrong. ● No file can be deleted. ● Option 147 check failed. ● Option 147 does not exist or check is successful, but check of other information fails. ● Option 141 is too long. ● Option 142 is too long. ● Option 67 is too long. ● Option 66 is too long. ● Option 15 is too long. ● Option 145 is too long. ● Option 146 is too long. ● Option 43 is too long. ● Space is not insufficient. ● Specifying startup patch file failed. ● Specifying startup system software failed. ● Specifying startup configuration file failed. ● Some ACS information is empty. ● Setting ACS URL failed. ● Setting ACS user name failed. ● Setting ACS password failed. ● The obtained version is different from the version in the system software name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• The system software already exists and is the current startup file. • The user name or password used to connect to the file server is wrong. • The file does not exist on the file server. • The extension name of the system software is wrong. • The extension name of the patch file is wrong. • The extension name of configuration file is wrong. • The configuration file already exists and is the current startup file. • The patch file already exists and is the current startup file. • The length of the middle file is incorrect. • The MAC address and ESN do not match. • The TFTP server cannot be found. • The length of some ACS information is wrong. • The format of ACS URL is wrong. • The format of ACS user name is wrong. • The format of ACS password is wrong. • The system software name or version is not received. • The system software name is too long. • The patch file name is too long. • The version is too long. • The configuration file name is too long. • The opervalue is too long. • The delaytime is too long. • The middle file does not have a configuration file name.
The status of DHCP phase	DHCP exchange phase.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Operation result	Result of interaction between the device and the DHCP server: ● --: The DHCP exchange phase is not started. ● Running: Auto-Config is running. ● Successful: Auto-Config is successful. ● Suspend: Auto-Config is suspended. ● Stop: Auto-Config stops.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Failed reason	Reason for interaction failure between the device and the DHCP server: ● AutoConfig is disabled. ● Current startup configuration file already exists. ● Deploying configurations with a USB disk. ● Failed to get the TFTP server address from the host. ● Getting file server information failed. ● Option 147 check failed. ● Option 147 does not exist or check is successful, but check of other information fails. ● Option 141 is too long. ● Option 142 is too long. ● Option 67 is too long. ● Option 66 is too long. ● Option 15 is too long. ● Option 145 is too long. ● Option 146 is too long. ● Option 43 is too long. ● The TFTP server cannot be found. ● The system software name is too long. ● The patch file name is too long. ● The version is too long. ● The configuration file name is too long. ● The opervalue is too long. ● The delaytime is too long. **NOTE** If Auto-Config keeps running during the interaction between the device and the DHCP server, **The last failed reason** is displayed, indicating the latest reason for failure.
The status of setting ACS phase	ACS configuration phase.
URL	ACS URL.
User name	ACS user name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Password	ACS password.
Operation result	Operation result: ● --: The ACS configuration phase is not started. ● Running: Auto-Config is running. ● Successful: Auto-Config is successful. ● Suspend: Auto-Config is suspended. ● Stop: Auto-Config stops.
Failed reason	Reason for a failure: ● Autoconfig is completed. ● AutoConfig is disabled. ● Current startup configuration file already exists. ● Some ACS information is empty. ● Setting ACS URL failed. ● Setting ACS user name failed. ● Setting ACS password failed. ● The length of some ACS information is wrong. ● The format of ACS URL is wrong. ● The format of ACS user name is wrong. ● The format of ACS password is wrong. **NOTE** If Auto-Config keeps running when ACS runs, **The last failed reason** is displayed, indicating the latest reason for failure.
The status of getting middle file phase	Phase of obtaining the intermediate file.
File name	Intermediate file name.
Operation result	Result of obtaining the intermediate file: ● --: The phase of obtaining the intermediate file is not started. ● Running: Auto-Config is running. ● Successful: Auto-Config is successful. ● Suspend: Auto-Config is suspended. ● Stop: Auto-Config stops.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Failed reason	Reason for failing to obtain the intermediate file: ● AutoConfig is disabled. ● Current startup configuration file already exists. ● Connecting to file server failed. ● Getting system MAC address and ESN failed. ● Getting system MAC address failed and the ESN is wrong. ● Getting system ESN failed and the MAC address is wrong. ● Space is not insufficient. ● The user name or password used to connect to the file server is wrong. ● The file does not exist on the file server. ● The length of the middle file is incorrect. ● The MAC address and ESN do not match. ● The middle file does not have a configuration file name. ● The system software name is too long. ● The patch file name is too long. ● The version is too long. ● The configuration file name is too long. **NOTE** If Auto-Config keeps running during the phase of obtaining the intermediate file, **The last failed reason** is displayed, indicating the latest reason for failure.
The status of getting system software phase	Phase of obtaining the system software.
File name	System software name.

Item	Description
Operation result	Result of obtaining system software: ● --: The phase of obtaining a version file is not started. ● Running: Auto-Config is running. ● Successful: Auto-Config is successful. ● Suspend: Auto-Config is suspended. ● Stop: Auto-Config stops.
Failed reason	Reason for failing to obtain the system software: ● AutoConfig is disabled. ● Current startup configuration file already exists. ● Connecting to file server failed. ● No file can be deleted. ● Specifying startup system software failed. ● Space is not insufficient. ● The file does not exist on the file server. ● The user name or password used to connect to the file server is wrong. ● The obtained version is different from the version in the system software name. ● The system software already exists and is the current startup file. ● The extension name of the system software is wrong. ● The system software name or version is not received. ● The system software already exists and is the rollback startup file. **NOTE** If Auto-Config keeps running during the phase of obtaining the system software, **The last failed reason** is displayed, indicating the latest reason for failure.
The status of getting patch file phase	Phase of obtaining a patch file.
File name	Patch file name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Operation result	Result of obtaining the patch file: ● --: The phase of obtaining a patch file is not started. ● Running: Auto-Config is running. ● Successful: Auto-Config is successful. ● Suspend: Auto-Config is suspended. ● Stop: Auto-Config stops.
Failed reason	Reason for failing to obtain the patch file: ● AutoConfig is disabled. ● Current startup configuration file already exists. ● Connecting to file server failed. ● Specifying startup patch file failed. ● Space is not insufficient. ● The file does not exist on the file server. ● The user name or password used to connect to the file server is wrong. ● The extension name of the patch file is wrong. ● The patch file already exists and is the current startup file. ● The patch file already exists and is the rollback startup file. **NOTE** If Auto-Config keeps running during the phase of obtaining the patch file, **The last failed reason** is displayed, indicating the latest reason for failure.
The status of getting configuration file phase	Phase of obtaining a configuration file.
File name	Configuration file name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Operation result	Result of obtaining the configuration file: ● --: The phase of obtaining a configuration file is not started. ● Running: Auto-Config is running. ● Successful: Auto-Config is successful. ● Suspend: Auto-Config is suspended. ● Stop: Auto-Config stops.
Failed reason	Reason for failing to obtain the configuration file: ● AutoConfig is disabled. ● Current startup configuration file already exists. ● Connecting to file server failed. ● Specifying startup configuration file failed. ● Space is not insufficient. ● The file does not exist on the file server. ● The user name or password used to connect to the file server is wrong. ● The extension name of configuration file is wrong. ● The configuration file already exists and is the current startup file. ● The configuration file already exists and is the rollback startup file. **NOTE** If Auto-Config keeps running during the phase of obtaining the configuration file, **The last failed reason** is displayed, indicating the latest reason for failure.
The status of activating configuration phase	Phase of activating the configuration.
Remained time	Remaining relay for restarting a device. The command output of this command is the same as that of the **3.2.4 display autoconfig activating-config remanent-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Operation result	Result of activating configurations: ● --: The phase of activating the configuration is not started. ● Running: Auto-Config is running. ● Successful: Auto-Config is successful. ● Suspend: Auto-Config is suspended. ● Stop: Auto-Config stops.
Failed reason	Reason for failing to activate configurations: ● AutoConfig is disabled. ● Current startup configuration file already exists.

Related Topics

3.2.1 autoconfig enable
3.2.2 autoconfig getting-file restart
3.2.4 display autoconfig activating-config remanent-time

3.3 Auto-Start Configuration Commands

3.3.1 autostart

Function

The **autostart** command displays the autostart view.

Format

autostart

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To perform configurations related to Auto-Start, enter the autostart view first. You can run this command in the system view to enter the autostart view.

Example

Display the autostart view.

```
<Huawei> system-view
[Huawei] autostart
[Huawei-autostart]
```

3.3.2 autostart enable

Function

The **autostart enable** command enables Auto-Start on a device.

The **undo autostart enable** command disables Auto-Start on a device.

By default, Auto-Start is disabled on a device.

Format

autostart enable

undo autostart enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run this command to enable Auto-Start. You can use Auto-Start to deploy or upgrade a device only after enabling Auto-Start.

Example

Enable Auto-Start.

```
[Huawei] autostart enable
Info: Enable autostart successfully.
```

 Copyright © Huawei Technologies Co., Ltd.

3.3.3 autostart run

Function

The **autostart run** command configures a device to immediately start the Auto-Start process.

Format

autostart run

Parameters

None

Views

Autostart view

Default Level

3: Management level

Usage Guidelines

When the Auto-Start process fails, you can modify file server parameters or reconfigure the intermediate file and file server, and run this command to configure the device to immediately start the Auto-Start process.

Example

Configure the device to immediately start the Auto-Start process.

```
<Huawei> system-view
[Huawei] autostart
[Huawei-autostart] autostart run
Are you sure to run autostart function? (Please set autostart config first.)[Y/N]:
y
Info: Autostart function run.
```

3.3.4 display autostart config

Function

The **display autostart config** command displays the file server configuration.

Format

display autostart config

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run this command to view the file server configuration on the device, including the type and IP address of the file server, and the user name and password for accessing the file server.

Example

Display the file server configuration.

```
[Huawei] display autostart config
Server type       :FTP
Server IP address :192.168.1.1
Username          :user1
Password          :***
```

Related Topics

3.3.1 autostart

3.3.7 servertype

3.3.6 ipaddress

3.3.8 username

3.3.5 display autostart status

Function

The **display autostart status** command displays the running status of Auto-Start.

Format

display autostart status

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the running status of Auto-Start.

```
[Huawei] display autostart status

Enable : Yes

Running: No

Can deploy configurations by USB disk or AutoConfig: Yes

Suspend: No
Reason : --

The status of getting middle file phase:
File name       : arstart.ini
Operation result: Suspend
Failed reason   : The unknown reason cause getting file from file server failed

The status of getting system software phase:
File name       : --
Operation result: --
Failed reason   : --

The status of getting patch file phase:
File name       : --
Operation result: --
Failed reason   : --

The status of getting configuration file phase:
File name       : --
Operation result: --
Failed reason   : --

The status of activating configuration phase:
Operation result: --
Failed reason   : --
```

Table 3-6 Description of the **display autostart status** command output

Item	Description
Enable	Whether Auto-Start is enabled: ● Yes: enabled ● No: disabled
Running	Whether Auto-Start is running: ● Yes: running ● No: not running

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Can deploy configurations by USB disk or AutoConfig	Whether site deployment using a USB flash drive or Auto-Config is available: ● Yes: available ● No: unavailable **NOTE** The device can be deployed using a USB flash drive, Auto-Config, or Auto-Start. The three deployment modes are mutually exclusive and only one of them can be used at a time.
Suspend	Whether Auto-Start is suspended: ● Yes: suspended ● No: not suspended

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Reason why Auto-Start is suspended. ● Autostart is completed. ● Connecting to file server failed. ● Getting file server information failed. ● Getting system MAC address and ESN failed. ● Getting system MAC address failed and the ESN is wrong. ● Getting system ESN failed and the MAC address is wrong. ● No file can be deleted. ● Space is not insufficient. ● Specifying startup patch file failed. ● Specifying startup system software failed. ● Specifying startup configuration file failed. ● The obtained version is different from the version in the system software name. ● The system software already exists and is the current startup file. ● The username or password used to connect to the file server is wrong. ● The file does not exist on the file server. ● The extension name of the system software is wrong. ● The extension name of the patch file is wrong. ● The extension name of configuration file is wrong. ● The configuration file already exists and is the current startup file. ● The patch file already exists and is the current startup file. ● The length of the middle file is incorrect. ● The MAC address and ESN do not match. ● The system software name or version is not received.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	● The system software name is too long. ● The patch file name is too long. ● The version is too long. ● The configuration file name is too long. ● The opervalue is too long. ● The middle file does not have a configuration file name.
The status of getting middle file phase	Phase of obtaining the intermediate file.
File name	Name of the intermediate file, system software, configuration file, or patch file.
Operation result	Result of the file obtaining phase. ● --: The phase is not started. ● Running: The phase is running. ● Successful: The phase is successful. ● Suspend: The phase is suspended. ● Stop: The phase stops.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Failed reason	Reason for failing to obtain a file. ● AutoStart is disabled. ● Current startup configuration file already exists. ● Connecting to file server failed. ● Getting system MAC address and ESN failed. ● Getting system MAC address failed and the ESN is wrong. ● Getting system ESN failed and the MAC address is wrong. ● Space is not insufficient. ● The username or password used to connect to the file server is wrong. ● The file does not exist on the file server. ● The length of the middle file is incorrect. ● The MAC address and ESN do not match. ● The middle file does not have a configuration file name. ● The system software name is too long. ● The patch file name is too long. ● The version is too long. ● The configuration file name is too long. ● Specifying startup system software failed. ● The obtained version is different from the version in the system software name. ● The system software already exists and is the current startup file. ● The extension name of the system software is wrong. ● The system software name or version is not received. ● The system software already exists and is the rollback startup file. ● Specifying startup patch file failed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• The extension name of the patch file is wrong. • The patch file already exists and is the current startup file. • The patch file already exists and is the rollback startup file. • Current startup configuration file already exists. • Specifying startup configuration file failed. • The extension name of configuration file is wrong. • The configuration file already exists and is the current startup file. • The configuration file already exists and is the rollback startup file.
The status of getting system software phase	Phase of obtaining the system software.
The status of getting patch file phase	Phase of obtaining the patch file.
The status of getting configuration file phase	Phase of obtaining the configuration file.
The status of activating configuration phase	Phase of activating the configuration.
Operation result	Result of the configuration activation phase. • --: The phase is not started. • Running: The phase is running. • Successful: The phase is successful. • Suspend: The phase is suspended. • Stop: The phase stops.
Failed reason	Reason for failing to activate the configuration. • AutoStart is disabled. • Current startup configuration file already exists.

Related Topics

3.3.2 autostart enable
3.3.3 autostart run

3.3.6 ipaddress

Function

The **ipaddress** command configures the IP address of the file server.

The **undo ipaddress** command deletes the IP address of the file server.

Format

ipaddress *ip*

undo ipaddress

Parameters

Parameter	Description	Value
ip	Specifies the IP address of the file server.	The value is in dotted decimal notation.

Views

Autostart view

Default Level

3: Management level

Usage Guidelines

Before using Auto-Start to deploy or upgrade a device, run this command to configure the IP address of the file server. After the IP address is configured, the device can connect to the corresponding file server based on the IP address and download site deployment files.

Example

Configure the IP address 192.168.1.20 for the file server.

```
<Huawei> system-view
[Huawei] autostart
[Huawei-autostart] ipaddress 192.168.1.20
Info: Set ip address successfully.
```

Related Topics

3.3.1 autostart

3.3.7 servertype

3.3.8 username

3.3.4 display autostart config

 Copyright © Huawei Technologies Co., Ltd.

3.3.7 servertype

Function

The **servertype** command configures the type of the file server.

The **undo servertype** command restores the default type of the file server.

By default, the file server is an FTP server.

Format

servertype { **FTP** | **SFTP** }

undo servertype

Parameters

Parameter	Description	Value
FTP	Sets the type of the file server to FTP.	-
SFTP	Sets the type of the file server to SFTP.	-

Views

Autostart view

Default Level

3: Management level

Usage Guidelines

Before using Auto-Start to deploy or upgrade a device, run this command to configure the type of the file server.

If the file server type is set to FTP, the device connects to the file server and downloads site deployment files using FTP. If the file server type is set to SFTP, the device connects to the file server and downloads site deployment files using SFTP.

Site deployment files contain the intermediate file and one or more of the system software, patch file, and configuration file.

Example

Set the type of the file server to SFTP.

```
<Huawei> system-view
[Huawei] autostart
[Huawei-autostart] servertype sftp
Info: Set server type successfully.
```

Related Topics

3.3.1 autostart

3.3.6 ipaddress
3.3.8 username
3.3.4 display autostart config

3.3.8 username

Function

The **username** command configures the user name and password for accessing the file server.

The **undo username** command deletes the user for accessing the file server.

By default, no user is configured for accessing the file server.

Format

username *username* **password** *password*

undo username *username*

Parameters

Parameter	Description	Value
username	Specifies the user name for accessing the file server.	The value is a string of 1 to 64 case-insensitive characters without spaces. It can contain special characters.
password	Specifies the password corresponding to the user name for accessing the file server.	The value is a string of case-sensitive characters without spaces. It can be a string of 1 to 32 characters in plain text, or a string of 80 characters in cipher text.

Views

Autostart view

Default Level

3: Management level

Usage Guidelines

Before using Auto-Start to deploy or upgrade a device, run this command to configure the user name and password for accessing the file server. After the user name and password are configured, the device can be authenticated by and connect to the file server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the user name and password for accessing the file server to **admin** and **huawei**, respectively.

```
<Huawei> system-view
[Huawei] autostart
[Huawei-autostart] username admin password huawei
Info: Set user name and password successfully.
```

Related Topics

3.3.1 autostart

3.3.7 servertype

3.3.6 ipaddress

3.3.4 display autostart config

3.4 USB-based Deployment Configuration Commands

3.4.1 autoupdate enable

Function

The **autoupdate enable** command enables the USB-based deployment function.

The **undo autoupdate enable** command disables the USB-based deployment function.

By default, the USB-based deployment function is disabled.

Format

autoupdate enable

undo autoupdate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

- If a device has the current configuration file (not an unconfigured device), you must run the **autoupdate enable** command to enable the USB-based deployment function before you can use a USB flash drive to upgrade the device.
- If a device has no current configuration file (unconfigured), the device can be upgraded using a flash drive regardless of whether the USB-based deployment function is enabled.

Prerequisites

This command can take effect only after an authentication password for USB-based deployment is configured by the **set usb autoupdate password** command.

Precautions

If the USB-based deployment is enabled, the **clear usb autoupdate password** command disables the USB-based deployment function while deleting the authentication password for USB-based deployment.

Example

Enable the USB-based deployment function.

```
<Huawei> system-view
[Huawei] set usb autoupdate password huawei123
[Huawei] autoupdate enable
Info: Enable Autoupdate successfully.
```

3.4.2 clear usb autoupdate password

Function

The **clear usb autoupdate password** command deletes the authentication password for USB-based deployment.

Format

clear usb autoupdate password

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To disable password authentication for USB-based deployment, run this command to delete the authentication password configured by the **set usb autoupdate password** command.

If the USB-based deployment and hash-based message authentication code (HMAC) check for USB-based deployment is enabled, the **clear usb autoupdate password** command also disables the USB-based deployment and the HMAC check. In this case, the device displays the following message "Info: Clear usb autoupdate password successfully, the hmac check and autoupdate are disabled."

If HMAC check is not enabled for USB-based deployment, the device displays the following information when you run the **clear usb autoupdate password** command "Info: Clear usb autoupdate password successfully."

Example

Delete the authentication password for USB-based deployment.

```
<Huawei> system-view
[Huawei] clear usb autoupdate password
```

Related Topics

3.4.7 set usb autoupdate password

3.4.3 display autoupdate enable

Function

The **display autoupdate enable** command displays whether the USB-based deployment function is enabled.

Format

display autoupdate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Check whether the USB-based deployment function is enabled.

```
<Huawei> system-view
[Huawei] display autoupdate enable
Autoupdate state: enabled.
```

Table 3-7 Description of the display autoupdate enable command output

Item	Description
Autoupdate state	• enabled: The USB-based deployment function is enabled. • disabled: The USB-based deployment function is not enabled.

3.4.4 display hmac enable

Function

The **display hmac enable** command displays whether the HMAC check function is enabled for USB-based deployment.

Format

display hmac enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Check whether the HMAC check function is enabled for USB-based deployment.

```
<Huawei> system-view
[Huawei] display hmac enable
Autoupdate hmac check state: enabled.
```

Table 3-8 Description of the display hmac enable command output

Item	Description
Autoupdate hmac check state	• enabled: The HMAC check function is enabled for USB-based deployment. • disabled: The HMAC check function is not enabled for USB-based deployment.

 Copyright © Huawei Technologies Co., Ltd.

3.4.5 display usb autoupdate state

Function

The **display usb autoupdate state** command displays the USB-based deployment status.

Format

display usb *usb-id* **autoupdate state**

Parameters

Parameter	Description	Value
usb-id	Specifies the USB interface ID.	The value is an integer ranging from 0 to 1.

Views

User view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the USB-based deployment status.

```
<Huawei> display usb 1 autoupdate state
Info: Deployment using the USB flash drive is completed successfully.
```

Table 3-9 Description of the display usb autoupdate state command output

Item	Description
Info: Deployment using the USB flash drive is completed successfully.	USB-based deployment is successful.
Info: Deployment using a USB flash drive is not performed.	USB-based deployment has not started.
Info: Deployment using a USB flash drive is in progress, please wait....	USB-based deployment is in progress.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Info: Deployment using the USB flash drive failed!	USB-based deployment fails.

Related Topics

3.4.7 set usb autoupdate password

3.4.6 hmac enable

Function

The **hmac enable** command enables the hash-based message authentication code (HMAC) check function for USB-based deployment.

The **undo hmac enable** command disables the HMAC check function for USB-based deployment.

By default, the HMAC check function is disabled.

Format

hmac enable

undo hmac enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

To improve security of USB-based deployment, you can run the **hmac enable** command to enable the HMAC check function for USB-based deployment.

After HMAC check is configured for USB-based deployment, the device uses the password configured by the **3.4.7 set usb autoupdate password** command as the key to calculate an HMAC based on the HMAC-SHA256 algorithm for a specific file. Then the device compares the calculated HMAC with the value of the HMAC field in the index file. If the two HMAC values are the same, the device considers the file to be downloaded valid.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

An authentication password has been configured using the **set usb autoupdate password** command.

Precautions

If HMAC check is enabled for USB-based deployment, the **clear usb autoupdate password** command disables the HMAC function while deleting the authentication password for USB-based deployment.

Example

Enable the HMAC check function for USB-based deployment.

```
<Huawei> system-view
[Huawei] set usb autoupdate password huawei123
[Huawei] hmac enable
Info: Enable Autoupdate hmac check successfully.
```

3.4.7 set usb autoupdate password

Function

The **set usb autoupdate password** command configures an authentication password for USB-based deployment.

Format

set usb autoupdate password *password*

Parameters

Parameter	Description	Value
password	Sets the authentication password used in USB-based deployment.	The value is a string of 8 to 64 characters in plain text without spaces, or a string of 8 to 108 characters in cipher text without spaces. The string must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

The authentication password configured by this command is used in the following scenarios:

 Copyright © Huawei Technologies Co., Ltd.

- When hash-based message authentication code (HMAC) check is enabled, the device uses this password as the key to calculate the HMAC.

  NOTE

  Currently, the HMAC can only be calculated using the HMAC-SHA256 algorithm.

- When downloading an encrypted configuration file from the USB flash drive, the device uses this password to decrypt the configuration file.

  NOTE

  Currently, configuration files can be encrypted only when they are being compressed into .zip format. The following encryption methods can be used:

  - Simple text encryption: For example, when you compress a .cfg configuration file into a .zip file, you can enter a password in the compression software to encrypt the configuration file.
  - AES256 encryption algorithm: For example, when you compress a .cfg configuration file into a .zip file, you can select the AES256 mode and enter a password in the compression software to encrypt the configuration file. This encryption method is recommended because it is more secure.

  The password used to encrypt the configuration file must be the same as the password configured by the **set usb autoupdate password** command.

Example

Set the authentication password used in USB-based deployment to huawei123.

```
<Huawei> system-view
[Huawei] set usb autoupdate password huawei123
```

Related Topics

3.4.5 display usb autoupdate state

3.4.8 usb autoupdate generate encrypted boot-password

Function

The **usb autoupdate generate encrypted boot-password** command encrypts a Boot password in plain text into one in cipher text.

Format

usb autoupdate generate encrypted boot-password

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In a scenario where USB-based deployment is performed and Boot passwords are set in a batch using configuration files, no password in plain text is allowed in the configuration files. Therefore, you can run the **usb autoupdate generate encrypted boot-password** command to generate an encrypted Boot password.

Precautions

You can run the **usb autoupdate generate encrypted boot-password** command on a device and then enter a password in plain text as prompted. The password is a string of 6 to 19 characters and must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters.

Example

Enter a Boot password in plain text and then a password in cipher text is generated.

```
<Huawei> system-view
[Huawei] usb autoupdate generate encrypted boot-password
Enter Password(<6-19>):
Confirm password:
Info:The encrypted boot password is:
%^%#NUWg5b|rB(.Z7'T5Yee:|3Z[Pl|32>)D,g8T8j5P%^%#
```

3.5 SMS-based Deployment Configuration Commands

NOTE

3G/LTE-supporting devices support SMS-based deployment. However, the AR109, AR109W, AR109GW-L, AR129CV, AR129CVW, and AR129CGVW-L do not support this function.

- Currently, 3G-supporting devices include:
  - 3G/LTE routers, which need to have 3G/LTE antennas installed before being used. For specific device models, see Licensing Requirements and Limitations for 3G Cellular Interfaces in "3G Cellular Interface Configuration".
  - Routers that can have 3G cards (except 3G-EVDO cards) installed in SIC slots. For specific device models, see Licensing Requirements and Limitations for 3G Cellular Interfaces in "3G Cellular Interface Configuration".
- Currently, the following routers support the LTE functions:
  - 3G/LTE routers, which need to have 3G/LTE antennas installed before being used. For specific device models, see Overview of LTE Cellular Interfaces in "LTE Cellular Interface Configuration".
  - Routers that can have LTE interface cards installed in slots. For specific device models, see Licensing Requirements and Limitations for LTE Cellular Interfaces in "LTE Cellular Interface Configuration".

3.5.1 sms config autodeploy enable

Function

The **sms config autodeploy enable** command enables the SMS-based deployment function.

The **undo sms config autodeploy enable** command disables the SMS-based deployment function.

By default, SMS-based deployment is enabled.

Format

sms config autodeploy enable

undo sms config autodeploy enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

As the enterprise network size expands, more branch devices need to be deployed. Some devices are geographically dispersed and difficult to obtain wired resources and have services deployed. SMS-based deployment function can solve this problem. For example, deployment personnel can send deployment short messages to devices through Short Message Service (SMS). Devices then receive and parse the short messages, activate 3G/LTE links, and access the file server through SFTP to obtain and load a configuration file for zero touch deployment in a batch. By default, SMS-based deployment is enabled. After devices are deployed successfully, you are advised to disable SMS-based deployment to prevent unauthorized users from modifying device configurations using forged deployment short messages.

Example

Enable SMS-based deployment.

```
<Huawei> system-view
[Huawei] sms config autodeploy enable
Info: Enable the SMS config function successfully.
```

Related Topics

3.5.2 sms config caller

3.5.2 sms config caller

Function

The **sms config caller** command configures a mobile phone number whitelist.

The **undo sms config caller** command deletes a mobile phone number whitelist.

By default, no mobile phone number whitelist is configured.

Format

sms config caller *tel-number*

undo sms config caller [*tel-number*]

Parameters

Parameter	Description	Value
tel-number	Specifies the mobile phone number segment in the whitelist.	The value is a string of 3 to 20 characters without spaces and can contain digits 0 to 9.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After devices are deployed successfully, you need to prevent device configurations from being modified according to short messages sent from unauthorized phone numbers. You can run the **sms config caller** command to configure a whitelist that contains mobile phone number segments. Only the mobile phone numbers that match all consecutive digits of any mobile phone number segment in the whitelist are allowed to send short messages for service configurations.

Precautions

Currently, a whitelist can contain a maximum of eight mobile phone number segments.

Example

Add the mobile phone number segment 13812345678 to a whitelist to allow the mobile phone number that matches this number segment to send short messages for SMS-based deployment.

```
<Huawei> system-view
[Huawei] sms config caller 13812345678
Info: Succeed in setting whitelist.
```

Related Topics

3.5.1 sms config autodeploy enable

3.6 Fast Provisioning Configuration Commands

3.6.1 display fast provisioning record

Function

The **display fast provisioning record** command displays the automatic learning record of an interface enabled with the fast provisioning function.

Format

display fast provisioning record [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the automatic learning records of interfaces enabled with the fast provisioning function.

```
<Huawei> system-view
[Huawei] display fast provisioning record
----------Fast Provisioning Record-----------
Ethernet1/0/0.1
   State : successful
   Vlan : 11
   IP : 172.16.0.1         Mask : 8
Fast provisioning num : 1
---------------------------------------------
```

Table 3-10 Description of the display fast provisioning record command output

Item	Description
State	State of a sub-interface. The value can be: ● successful: The sub-interface has learned and saved the configuration successfully. ● learning: The sub-interface is learning the configuration automatically.
Vlan/IP/Mask	Configuration information learned by the sub-interface.
Fast provisioning num	Number of sub-interfaces that have successfully learned configurations. Currently, a maximum of eight sub-interfaces are supported.

3.6.2 display fast provisioning state

Function

The **display fast provisioning state** command displays the status of the fast provisioning function on interfaces.

Format

display fast provisioning state

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the status of the fast provisioning function on interfaces.

```
<Huawei> system-view
[Huawei] display fast provisioning state
----------Fast Provisioning State----------
GigabitEthernet0/0/1
```

```
  GigabitEthernet0/0/1.1
      State : enable
  GigabitEthernet0/0/1.2
      State : disable
-------------------------------------------
```

Table 3-11 Description of the display fast provisioning state command output

Item	Description
State	Whether the fast provisioning function is enabled on a sub-interface. ● enable: The fast provisioning function is enabled on the sub-interface. ● disable: The fast provisioning function is disabled on the sub-interface. ● restart: The fast provisioning function is enabled on the sub-interface after the device restarts. ● inactive: The fast provisioning function is enabled on the sub-interface, but the physical state of the sub-interface is Down.

3.6.3 fast provisioning enable

Function

The **fast provisioning enable** command enables the fast provisioning function globally.

The **undo fast provisioning enable** command disables the fast provisioning function globally.

By default, the fast provisioning function is disabled globally.

Format

fast provisioning enable [**restart**]

undo fast provisioning enable

Parameters

Parameter	Description	Value
restart	Indicates that the fast provisioning function is enabled globally after the device restarts.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

To enable the fast provisioning function, run the **fast provisioning enable** in the system view.

Precautions

- After the fast provisioning function is disabled globally using the **undo fast provisioning enable** command, the fast provisioning function configured on interfaces also becomes invalid.
- After the fast provisioning function is enabled, the device starts a timer since the first time the automatic learning function is triggered. The fast provisioning function is automatically disabled globally and on interfaces 1 hour later. If the device restarts within 1 hour, the fast provisioning function will not be automatically disabled 1 hour later. In this case, the fast provisioning function can only be disabled using the **undo fast provisioning enable** command.
- The configuration takes effect immediately when the **fast provisioning enable** or **undo fast provisioning enable** command is used to enable or disable the fast provisioning function.
- The configuration takes effect after the device restarts when the **fast provisioning enable restart** command is used to enable the fast provisioning function.

Example

Enable the fast provisioning function globally.

```
<Huawei> system-view
[Huawei] fast provisioning enable
```

3.6.4 fast-provisioning disable (sub-interface view)

Function

The **fast-provisioning disable** command disables the fast provisioning function on a sub-interface.

The **undo fast-provisioning disable** command enables the fast provisioning function on a sub-interface.

By default, the fast provisioning function is disabled on a sub-interface. After the fast provisioning function is enabled on an interface, the function is automatically enabled on sub-interfaces of the interface.

Format

fast-provisioning disable

undo fast-provisioning disable

Parameters

None

Views

Ethernet sub-interface view, serial sub-interface view, ADSL sub-interface view, GE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

When the fast provisioning function is enabled on an interface using the **3.6.5 fast-provisioning enable (interface view)** command, all sub-interfaces of the interface have the function enabled. If the fast provisioning function only needs to be enabled on some sub-interfaces, run the **fast-provisioning disable** command to disable the fast provisioning function on specified sub-interfaces.

Prerequisite

The fast provisioning function has been enabled on the main interface using the **3.6.5 fast-provisioning enable (interface view)** command.

Example

Disable the fast provisioning function on the sub-interface GE1/0/0.1.

```
<Huawei> system-view
[Huawei] fast provisioning enable
[Huawei] interface gigabitEthernet 1/0/0
[Huawei-GigabitEthernet1/0/0] fast-provisioning enable
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] interface gigabitEthernet 1/0/0.1
[Huawei-GigabitEthernet1/0/0.1] fast-provisioning disable
```

3.6.5 fast-provisioning enable (interface view)

Function

The **fast-provisioning enable** command enables the fast provisioning function on an interface.

The **undo fast-provisioning enable** command disables the fast provisioning function on an interface.

By default, the fast provisioning function is disabled on an interface.

Format

fast-provisioning enable

undo fast-provisioning enable

Parameters

None

Views

Ethernet interface view, serial interface view, GE interface view, ADSL interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

You can run the **fast-provisioning enable** command to enable the fast provisioning function on an interface. After the fast provisioning function is enabled on an interface, sub-interfaces of the interface can automatically learn and save information such as the VLAN, IP address, and DLCI from the peer device.

Currently, the fast provisioning function is supported by the following three kinds of sub-interfaces:

- ADSL sub-interface: supports the fast provisioning function only when the sub-interface is used in an IPoA scenario.
- Serial sub-interface: supports the fast provisioning function only when the sub-interface is used in a synchronous or asynchronous sub-interface and the sub-interface type is P2P.
- Ethernet sub-interface: supports the fast provisioning function only in a scenario where packets carry one VLAN tag.

Prerequisite

The fast provisioning function has been enabled globally using the **3.6.3 fast provisioning enable** command.

Precautions

- After enabling the fast provisioning function on an interface, create a sub-interface for the interface. Only the sub-interface can automatically learn information such as the VLAN, IP address, and DLCI from the peer device.
- After the fast provisioning function is enabled, the device starts a timer since the first time the automatic learning function is triggered. The fast provisioning function is automatically disabled globally and on interfaces 1 hour later. If the device restarts within 1 hour, the fast provisioning function will not be automatically disabled 1 hour later. In this case, the fast provisioning function can only be disabled using the **undo fast provisioning enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the fast provisioning function on GE1/0/0.

```
<Huawei> system-view
[Huawei] fast provisioning enable
[Huawei] interface gigabitEthernet 1/0/0
[Huawei-GigabitEthernet1/0/0] fast-provisioning enable
```

3.6.6 reset fast-provisioning

Function

The **reset fast-provisioning** command clears configuration information automatically learned by an interface using the fast provisioning function.

Format

reset fast-provisioning

Parameters

None

Views

Ethernet interface view, serial interface view, ADSL interface view, Ethernet sub-interface view, serial sub-interface view, GE interface view, GE sub-interface view, ADSL sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

You can run the **reset fast-provisioning** command to clear configuration information automatically learned by an interface using the fast provisioning function. Sub-interfaces then can relearn configuration information automatically.

Precautions

- In the main interface view, run the **reset fast-provisioning** command to clear all the configuration information learned by sub-interfaces of the main interface.
- In the sub-interface view, run the **reset fast-provisioning** command to clear the IP address learned by the sub-interface.
- After the fast provisioning function is enabled, the device starts a timer since the first time the automatic learning function is triggered. The fast provisioning function is automatically disabled globally and on interfaces 1 hour later. If the device restarts within 1 hour, the fast provisioning function will not be automatically disabled 1 hour later. In this case, the fast

 Copyright © Huawei Technologies Co., Ltd.

provisioning function can only be disabled using the **undo fast provisioning enable** command.

Example

Reset the status of the fast provisioning function on the sub-interface GE1/0/0.1.

```
<Huawei> system-view
[Huawei] interface gigabitEthernet 1/0/0.1
[Huawei-GigabitEthernet1/0/0.1] reset fast-provisioning
```

3.7 First Login Commands

3.7.1 clock datetime

Function

The **clock datetime** command sets the current date and time on the router.

Format

clock datetime *HH:MM:SS YYYY-MM-DD*

Parameters

Parameter	Description	Value
HH:MM:SS	Specifies the current time on the router.	*HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. *SS* specifies the second, which is an integer ranging from 0 to 59.
YYYY-MM-DD	Specifies the current date (year, month, and day) on the router.	*YYYY* specifies the year, which is an integer ranging from 2000 to 2037. *MM* specifies the month, which is an integer ranging from 1 to 12. *DD* specifies the day, which is an integer ranging from 1 to 31.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the scenario where accurate absolute time is required, the current date and time must be set on the router.

Prerequisite

The time zone and daylight saving time have been configured using the **clock timezone** and **clock daylight-saving-time** commands. If the time zone and daylight saving time are not configured, the **clock datetime** command sets a UTC time.

Precautions

- The specified time must be in 24-hour format. If you do not specify *MM* and *SS*, their values are 0. You must enter at least one digit to specify *HH*. For example, when you enter 0, the time is 00:00:00.
- The specified year must be a four-digit number and the specified month and day can be a one-digit number. For example, when you enter 2012-9-1, the time is 2012-09-01.
- If the device is configured to restart at a specified time and if the system time is changed to be more than 10 minutes later than the specified restart time, the scheduled restart function will be disabled.

Example

Set the current time and date of the system to 0:0:0 2012-01-01.

```
<Huawei> clock datetime 0:0:0 2012-01-01
```

Related Topics

3.7.4 display clock

3.7.2 clock daylight-saving-time

Function

The **clock daylight-saving-time** command sets the name, start time, and end time of the daylight saving time (DST).

The **undo clock daylight-saving-time** command cancels the DST settings.

By default, DST is not used.

Format

clock daylight-saving-time *time-zone-name* **one-year** *start-time start-date end-time end-date offset*

clock daylight-saving-time *time-zone-name* **repeating** *start-time* { { **fifth** | **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *start-date1* } *end-time* { { **first** | **second** | **third** | **fourth** | **last** } *weekday month* | *end-date1* } *offset* [*start-year* [*end-year*]]

undo clock daylight-saving-time

Parameters

Parameter	Description	Value
time-zone-name	Specifies the name of the DST zone.	The value is a string of 1 to 32 characters.
one-year	Specifies absolute DST.	-
repeating	Specifies periodic DST.	-
start-time	Specifies the DST start time.	The start time is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, DST starts on the hour. You must enter at least one digit to specify *HH*. For example, when you enter 0, the start time is 00:00.
start-date	Specifies the DST start date.	The start date is in the format *YYYY-MM-DD*. *YYYY* specifies the year, which is an integer ranging from 2000 to 2037, *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
end-time	Specifies the DST end time.	The end time is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, DST starts on the hour. You must enter at least one digit to specify *HH*. For example, when you enter 0, the start time is 00:00.
end-date	Specifies the DST end date.	The end date is in the format *YYYY-MM-DD*. *YYYY* specifies the year, which is an integer ranging from 2000 to 2037, *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
fifth	Specifies the fifth week in a month.	-
first	Specifies the first week in a month.	-
second	Specifies the second week in a month.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
third	Specifies the third week in a month.	-
fourth	indicates the fourth week in a month.	-
last	Specifies the last week in a month.	-
weekday	Specifies a day of the week.	The value is **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, or **Sun**.
month	Specifies a month.	The value is **Jan**, **Feb**, **Mar**, **Apr**, **May**, **Jun**, **Jul**, **Aug**, **Sep**, **Oct**, **Nov**, or **Dec**.
start-date1	Specifies the DST start date.	The start date is in the format *MM-DD*. *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
end-date1	Specifies the DST end date.	The end date is in the format *MM-DD*. *MM* specifies the month, which is an integer ranging from 1 to 12, and *DD* specifies the day, which is an integer ranging from 1 to 31.
offset	Specifies the DST offset.	The offset is in 24-hour format *HH:MM*. *HH* specifies the hour, which is an integer ranging from 0 to 23. *MM* specifies the minute, which is an integer ranging from 0 to 59. If *MM* is not specified, the offset is the specified hours. You must enter at least one digit to specify *HH*.
start-year	Specifies the start year.	The start year is in the format *YYYY* and ranges from 2000 to 2037.
end-year	Specifies the end year.	The end year is in the format *YYYY* and ranges from 2000 to 2037.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

DST, also referred to as summer time, is a convention intended to save resources. In high latitude areas, sunrise time is earlier in summer than in winter. To reduce

use of incandescent lighting in the evenings and save energy, clocks are adjusted forward one hour.

Users can customize the DST zone according to their countries' or regions' convention. In addition, users can set how far ahead clocks are adjusted forward, usually an hour. With DST enabled, when it is time to start DST, the system time is adjusted according to the user-specified DST. When it is time to end DST, the system time automatically returns to the original time.

Configuration Impact

To configure DST, note the following:

- The time in logs and debugging information uses the local time adjusted based on the time zone and the configured DST.
- The time in the output of the **display** commands uses the local time adjusted based on the time zone and the configured DST.

To remove configurations for DST, note the following:

- If DST has already taken effect when you remove the configurations, the device will adjust its clock by subtracting the value of the *offset* parameter from the current time.
- If DST has not taken effect, removing the configurations will not affect the system time.

Precautions

- The DST is configured in the summer. The DST duration ranges from one day to one year.
- You can configure the start time and end time for periodic DST in one of the following modes: date+date, week+week, date+week, and week+date.

Example

Set periodic DST.

```
<Huawei> clock daylight-saving-time bj repeating 0 first sun jan 0 first sun apr 2 2009 2009
```

Set periodic DST by day.

```
<Huawei> clock daylight-saving-time bj repeating 12:11 1-1 1:0 3-4 1
```

Set absolute DST.

```
<Huawei> clock daylight-saving-time bj one-year 12:11 2010-10-2 1:00 2010-11-4 1
```

Related Topics

3.7.3 clock timezone

3.7.3 clock timezone

Function

The **clock timezone** command sets the local time zone.

The **undo clock timezone** command deletes the local time zone.

If you do not specify the time zone name, the system uses **Default Zone Name**.

Format

clock timezone *time-zone-name* { **add** | **minus** } *offset*

undo clock timezone

Parameters

Parameter	Description	Value
time-zone-name	Specifies the time zone name.	The name is a string of 1 to 32 case-sensitive characters without spaces.
add	Specifies the offset from the UTC for the time zone specified by *time-zone-name*. That is, the sum of the default UTC time zone and *offset* is equal to the time zone specified by *time-zone-name*.	-
minus	Specifies the offset from the UTC for the time zone specified by *time-zone-name*. That is, the remainder obtained by subtracting *offset* from the default UTC time zone is equal to the time zone specified by *time-zone-name*.	-
offset	Specifies the offset from the UTC.	Format: HH:MM:SS ● *HH* specifies the hour. – If the local time is earlier than the UTC, the value is an integer ranging from 0 to 14. – If the local time is later than the UTC, the value is an integer ranging from 0 to 12. ● *MM* and *SS* specify the minute and second respectively, and both range from 0 to 59. ● When *HH* is set to the maximum value, the *MM* and *SS* values must be 0.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system clock is the time indicated by the system timestamp. Because the rules governing local time differ in different regions, the system clock can be configured to comply with the rules of any given region.

System clock = UTC + Time zone offset + DST offset

To ensure normal communication between devices, set an accurate system clock. You can run the **clock timezone** and **clock daylight-saving-time** commands to set the time zone and DST offsets.

Precautions

- The specified time must be in 24-hour format. If you do not specify *MM* and *SS*, their values are 0. You must enter at least one digit to specify *HH*. For example, when you enter 0, the time is 00:00:00.
- After configuring the local time zone, run the **display clock** command to view the configuration. The time in logs and diagnostic information uses the local time adjusted based on the time zone and DST.

Example

Set the local time zone name for Beijing China to BJ.

If the default UTC is London time 2012-12-01 00:00:00, Beijing time is London time plus 08:00 because the offset from UTC is 8 hours.

```
<Huawei> clock datetime 0:0:0 2012-12-01
<Huawei> clock timezone BJ add 08:00:00
```

Related Topics

3.7.2 clock daylight-saving-time

3.7.4 display clock

Function

The **display clock** command displays the current date and clock setting.

Format

display clock

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display clock** command to view the system date and clock setting and adjust the setting if necessary.

Precautions

The system clock is set using the **clock datetime**, **clock timezone**, and **clock daylight-saving-time** commands.

- If the three commands are not used, the original system clock is displayed after you run the **display clock** command.
- You can use any combination of the three commands to configure the system time. **Table 3-12** lists the formats of the configured time.

The table assumes that the original system time is 08:00:00 on January 1, 2010.

- 1: indicates that the **clock datetime** command is used, in which the current time and date is *date-time*.
- 2: indicates that the **clock timezone** command is used, in which the time zone parameter is set and the time offset is *zone-offset*.
- 3: indicates that the **clock daylight-saving-time** command is used, in which the DST parameters are set and the time offset is *offset*.
- [1]: indicates that the **clock datetime** command is optional.

Table 3-12 System clock setting examples

Action	Configured System Time	Example
1	*date-time*	Command: **clock datetime 8:0:0 2011-11-12** Configured system time: 2011-11-12 08:00:02 Saturday Time Zone(Default Zone Name) : UTC+00:00
2	Original system time ± *zone-offset*	Command: **clock timezone BJ add 8** Configured system time: 2010-01-01 16:00:27 Friday Time Zone(BJ) : UTC+08:00
1, 2	*date-time* ± *zone-offset*	Commands: **clock datetime 8:0:0 2011-11-12** and **clock timezone BJ add 8** Configured system time: 2011-11-12 16:00:17 Saturday Time Zone(BJ) : UTC+08:00

 Copyright © Huawei Technologies Co., Ltd.

Action	Configured System Time	Example
[1], 2, 1	*date-time*	Commands: **clock timezone NJ add 8** and **clock datetime 9:0:0 2011-11-12** Configured system time: 2011-11-12 09:00:03 Saturday Time Zone(NJ) : UTC+08:00
3	If the original system time is not in the DST segment, the original system time is displayed.	Command: **clock daylight-saving-time BJ one-year 6:0 2011-8-1 6:0 2011-10-01 1** Configured system time: 2010-01-01 08:00:51 Friday Time Zone(Default Zone Name) : UTC+00:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00
	If the original system time is in the DST segment, the configured system time is the original system time plus *offset*.	Command: **clock daylight-saving-time BJ one-year 6:0 2010-1-1 6:0 2010-9-1 2** Configured system time: 2010-01-01 10:00:08 DST Friday Time Zone(BJ) : UTC+00:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2010 End year : 2010 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
1, 3	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock datetime 9:0:0 2011-11-12** and **clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1** Configured system time: 2011-11-12 09:00:26 Saturday Time Zone(Default Zone Name) : UTC+00:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00

 Copyright © Huawei Technologies Co., Ltd.

Action	Configured System Time	Example
	If *date-time* is in the DST segment, the configured system time is *date-time* +*offset*.	Commands: **clock datetime 9:0:0 2011-11-12** and **clock daylight-saving-time BJ one-year 9:0 2011-11-12 6:0 2011-12-01 2** Configured system time: 2011-11-12 11:02:21 DST Saturday Time Zone(BJ) : UTC+00:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 11-12 09:00:00 End time : 12-01 06:00:00 Saving time : 02:00:00
[1], 3, 1	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 6:0 2012-8-1 6:0 2012-10-01 1** and **clock datetime 9:0 2011-11-12** Configured system time: 2011-11-12 09:00:02 Saturday Time Zone(Default Zone Name) : UTC+00:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 08-01 06:00:00 End time : 10-01 06:00:00 Saving time : 01:00:00
	If *date-time* is in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2** and **clock datetime 3:0 2011-1-1** Configured system time: 2011-01-01 03:00:19 DST Saturday Time Zone(BJ) : UTC+00:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00

 Copyright © Huawei Technologies Co., Ltd.

Action	Configured System Time	Example
2, 3 or 3, 2	If the result of original system time ± *zone-offset* is not in the DST segment, the configured system time is equal to the original system time ± *zone-offset*.	Commands: **clock timezone BJ add 8** and **clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2** Configured system time: 2010-01-01 16:01:29 Friday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
	If the result of original system time ± *zone-offset* is in the DST segment, the configured system time is equal to the original system time ± *zone-offset* ± *offset*.	Commands: **clock daylight-saving-time BJ one-year 1:0 2010-1-1 1:0 2010-9-1 2** and **clock timezone BJ add 8** Configured system time: 2010-01-01 18:05:31 DST Friday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2010 End year : 2010 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00
1, 2, 3 or 1, 3, 2	If the value of *date-time* ± *zone-offset* is not in the DST segment, the configured system time is equal to *date-time* ± *zone-offset*.	Commands: **clock datetime 8:0:0 2011-11-12**, **clock timezone BJ add 8**, and **clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2** Configured system time: 2011-11-12 08:01:40 Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00

 Copyright © Huawei Technologies Co., Ltd.

Action	Configured System Time	Example
	If the value of *date-time* ± *zone-offset* is in the DST segment, the configured system time is equal to *date-time* ± *zone-offset* + *offset*.	Commands: **clock datetime 8:0:0 2011-1-1**, **clock daylight-saving-time BJ one-year 6:0 2011-1-1 6:0 2011-9-1 2** and **clock timezone BJ add 8** Configured system time: 2011-01-01 10:00:43 DST Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
[1], 2, 3, 1 or [1], 3, 2, 1	If *date-time* is not in the DST segment, the configured system time is *date-time*.	Commands: **clock daylight-saving-time BJ one-year 6:0 2012-1-1 6:0 2012-9-1 2**, **clock timezone BJ add 8**, and **clock datetime 8:0:0 2011-11-12** Configured system time: 2011-11-12 08:00:03 Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2012 End year : 2012 Start time : 01-01 06:00:00 End time : 09-01 06:00:00 Saving time : 02:00:00
	If *date-time* is in the DST segment, the configured system time is *date-time*.	Commands: **clock timezone BJ add 8**, **clock daylight-saving-time BJ one-year 1:0 2011-1-1 1:0 2011-9-1 2**, and **clock datetime 3:0:0 2011-1-1** Configured system time: 2011-01-01 03:00:03 DST Saturday Time Zone(BJ) : UTC+08:00 Daylight saving time : Name : BJ Repeat mode : one-year Start year : 2011 End year : 2011 Start time : 01-01 01:00:00 End time : 09-01 01:00:00 Saving time : 02:00:00

Example

Display the current system date and time.

```
<Huawei> display clock
```

```
2012-05-15 20:34:53
Tuesday
Time Zone(Default Zone Name) : UTC+00:00
Daylight saving time :
        Name        : BJ
        Repeat mode : one-year
        Start year  : 2012
        End year    : 2012
        Start time  : 08-01 06:00:00
        End time    : 10-01 06:00:00
        Saving time : 01:00:00
```

Table 3-13 Description of the display clock command output

Item	Description
Time Zone	Time zone.
Daylight saving time	DST.
Name	DST name.
Repeat mode	DST mode. ● one-year: absolute DST ● repeating: periodic DST
Start year	Year from which DST takes effect.
End year	Year when DST becomes ineffective.
Start time	Time when DST takes effect.
End time	Time when DST becomes ineffective.
Saving time	Storage time.

Related Topics

3.7.1 clock datetime

3.7.2 clock daylight-saving-time

3.7.5 sysname

Function

The **sysname** command sets the device host name.

The **undo sysname** command restores the default device host name.

By default, the device host name is Huawei.

Format

sysname *host-name*

undo sysname

Parameters

Parameter	Description	Value
host-name	Specifies the host name.	The value is a string of 1 to 246 case-sensitive characters with spaces, "?" not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Changing the host name affects the command interface prompt. For example, if the host name is Huawei, the user interface prompt is <Huawei>.

Example

Set the host name to HuaweiA.

```
<Huawei> system-view
[Huawei] sysname HuaweiA
[HuaweiA]
```

Related Topics

3.1.17 system-view

3.7.6 ip netbios-reply interface

Function

The **ip netbios-reply interface** command enables the query response processing function for the NETBIOS name service and specifies the type and number of the response interface.

The **undo ip netbios-reply interface** command disables the query response processing function for the NETBIOS name service.

By default, the query response processing function for the NETBIOS name service is disabled.

NOTE

Only the AR169W-P-M9 supports this command.

Format

ip netbios-reply interface *interface-type interface-number*

undo ip netbios-reply interface

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	• **interface-type** indicates the interface type. • **interface-number** indicates the interface number.	VLANIF, Layer 3 Ethernet, and Layer 3 GigabitEthernet interfaces are supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain a device's IP address by pinging the host name of the device, run the **ip netbios-reply interface** *interface-type interface-number* command to enable the query response processing function for the NETBIOS name service and specify the type and number of the response interface. The type and number of the response interface correspond to the device's IP address. In this case, the device's IP address can be obtained by pinging the host name of the device on the queried host.

Prerequisites

- An IP address has been configured for the virtual interface and the DHCP service function has been enabled on the interface.
- An IP address has been configured on the query response interface of the NETBIOS name service.

Follow-up Procedure

Run the **sysname** command to configure the host name required for the query.

NOTE

The host name required for the query is a character string. Rules of the host name are as follows:

- The host name is a string of 1 to 15 case-insensitive characters and can contain spaces.
- The host name cannot contain special characters % and @, contain quotation marks (") and | simultaneously, start with *, -, or /, or end with \.
- The host name cannot be an existing domain name, IP address, or part of an IP address.
- The host name cannot be a character string in decimal or hexadecimal notation.

Example

Enable the query response processing function for the NETBIOS name service and set the type and number of the response interface to GigabitEthernet 0/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip netbios-reply interface GigabitEthernet 0/0/0
```

3.8 UI Configuration Commands

3.8.1 acl (user interface view)

Function

The **acl** command uses an ACL to restrict login rights of users on a terminal.

The **undo acl** command cancels the configuration.

By default, login rights are not restricted.

Format

acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

undo acl [**ipv6**] { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
ipv6	Indicates an ACL6 number.	-
acl-number	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999. ● 2000-2999: restricts the source address using the basic ACL. ● 3000-3999: restricts the source and destination addresses using the advanced ACL.
inbound	Restricts users with an address or within an address segment to log in to the device.	-
outbound	Restricts users that have logged in to the device from logging in to other devices.	-

Views

User interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command restricts the login rights of a user interface based on the source IP address, destination IP address, source port, or destination port. You can use this command to permit or deny access to a destination or from a source.

Prerequisites

Before running this command, run the **acl (system view)** in the system view and run the **rule (basic ACL view)** or **rule (advanced ACL view)** command to configure an ACL.

If no rule is configured, login rights on the user interface are not restricted when the **acl** command is executed.

Precautions

After the configurations of the ACL take effect, all users on the user interface are restricted by the ACL.

You can configure all of the following ACL types: IPv4 inbound, IPv4 outbound, IPv6 inbound, and IPv6 outbound on a user interface. Only one ACL of each type can be configured on a user interface, and only the latest configuration of an ACL takes effect.

Example

Restrict the Telnet login rights on user interface VTY 0.

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule deny tcp source any destination-port eq telnet
[Huawei-acl-adv-3001] quit
[Huawei] user-interface vty 0
[Huawei-ui-vty0] acl 3001 outbound
```

Remove the restriction on the Telnet login rights on user interface VTY 0.

```
<Huawei> system-view
[Huawei] user-interface vty 0
[Huawei-ui-vty0] undo acl outbound
```

Related Topics

3.8.25 user-interface

3.8.2 authentication-domain

Function

The **authentication-domain** command configures an authentication domain for a type of users.

The **undo authentication-domain** command restores the default authentication domain configuration.

By default, the authentication domain is **default**.

Format

authentication-domain *domain-name*

undo authentication-domain

Parameters

Parameter	Description	Value
domain-name	Specifies the name of an authentication domain.	The name is a string of 1 to 64 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces. The string cannot contain the following characters: * " ? - --. **NOTE** The value must be the name of an existing authentication domain in AAA mode.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **authentication-domain** command to change the currently used authentication domain so that users of different access types can be authenticated in different authentication domains.

NOTE

Currently, the device supports console and virtual type terminal (VTY) user interfaces.

Prerequisites

An authentication domain must have been created in AAA mode and the authentication mode has been set to **AAA** using the **authentication-mode** command.

Precautions

If you change the authentication mode to a non-AAA mode using the **authentication-mode** command, the authentication domain configured using the **authentication-domain** command restores to **default**.

Example

Configure the authentication domain **domain1** for users on the console user interface.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain domain1
[Huawei-aaa] quit
[Huawei] user-interface console 0
[Huawei-ui-console0] authentication-mode aaa
[Huawei-ui-console0] authentication-domain domain1
```

3.8.3 authentication-mode (user interface view)

Function

The **authentication-mode** command configures the authentication mode for accessing the user interface.

The **undo authentication-mode** command deletes the authentication mode for accessing the user interface.

By default, no authentication mode for accessing the user interface is configured. For the users logging in to the interface, an authentication method must be configured; otherwise, users cannot log in.

Format

authentication-mode { **aaa** | **password** }

undo authentication-mode

Parameters

Parameter	Description	Value
aaa	Indicates the AAA authentication mode.	-
password	Indicates the password authentication mode.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a user logs in to the device using the console interface for the first time, the system prompts the user to set the login password. After the user logs in to the device, the user can run the **authentication-mode** command to change the authentication mode.

Before Telnet or SSH users log in to the device using VTY user interface, they must run the **authentication-mode** command to configure the authentication mode.

Precautions

To ensure that users can log in to the device successfully, configure the authentication mode.

- After you set the authentication mode for accessing a user interface to **password**, run the **set authentication password** command to configure an authentication password. Keep the password safe. You need to enter the password when logging in to the device. The levels of commands accessible to a user depend on the level configured for the user interface to which the user logs in.
- When the authentication mode is set to **aaa**, the authentication password is deleted at the same time. Users are required to enter the login user name and password to log in to the device. After login, the level of the commands the user can run depends on the level of the local user specified in AAA configuration.
- If the current login channel has a password, enter the password when you want to modify or delete the authentication mode of a VTY channel range that contains the current login channel.

Example

Configure the authentication mode for accessing the user interface.

```
<Huawei> system-view
[Huawei] user-interface vty 0
[Huawei-ui-vty0] authentication-mode aaa
```

3.8.4 auto-execute command

Function

The **auto-execute command** command configures auto-run commands.

The **undo auto-execute command** command cancels auto-run commands.

By default, the auto-run function is disabled.

Format

auto-execute command *command*

undo auto-execute command

Parameters

Parameter	Description	Value
command	Specifies an auto-run command.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **auto-execute command** command to make the device run a command automatically on the corresponding interface.

You can run the **auto-execute command** command to enable automatic execution for the **Telnet** command.

Precautions

- The **auto-execute command** command is applicable to the VTY user interface.
- When you log in to the device, the device automatically runs the commands that are configured by the **auto-execute command** command. The user's terminal disconnects from the device.
- Before saving the configuration of the **auto-execute command** command, ensure that you can log in to the device in other ways so that you can cancel the command configuration.
- If you use the **auto-execute command** command, you cannot configure the device in the user interface view. Therefore, use this command with caution.

Example

Configure the **telnet 10.110.100.1** command to automatically run after a user logs in to the device using the VTY0 interface.

```
<Huawei> system-view
[Huawei] user-interface vty 0
[Huawei-ui-vty0] auto-execute command telnet 10.110.100.1
Warning: The system will not be configured through ui-vty0.Continue? [Y/N]: y
```

3.8.5 databits

Function

The **databits** command sets the number of data bits of the user interface.

The **undo databits** command restores the default number of data bits.

By default, the number of data bits of the user interface is 8.

Format

databits { **5** | **6** | **7** | **8** }

undo databits

Parameters

Parameter	Description	Value
5	Indicates that the number of data bits is 5.	-
6	Indicates that the number of data bits is 6.	-
7	Indicates that the number of data bits is 7.	-
8	Indicates that the number of data bits is 8.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Use this command only when necessary. If the number of data bits of a device's user interface is changed, ensure that the same number of data bits is set on the Putty used for login.

The setting is valid only when the serial port is configured to work in asynchronous mode.

NOTE

The data bit of the console user interface does not support 5 and 6.

Example

Set the number of data bits to 7.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] databits 7
```

3.8.6 display mib-index interface

Function

The **display mib-index interface** command displays the index value of an interface in the MIB.

Format

display mib-index interface [*interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface for which the index value is displayed. ● *interface-type*: specifies the interface type, for example, Ethernet. If the interface type is not specified, the index values of all interfaces are displayed. ● *interface-number*: specifies the number of an interface. It is used with *interface-type* to specify an interface. If the interface number is not specified, the index values of all interfaces of the type are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mib-index interface** command as an NMS user to view the index values of interfaces.

Example

Display indexes of all interfaces.

```
<Huawei> display mib-index interface
IfName                    IfIndex   PortIndex
---------------------------------------------------
GigabitEthernet0/0/0        3         --
GigabitEthernet0/0/1        4         --
GigabitEthernet0/0/2        5         --
```

Table 3-14 Description of the display mib-index interface command output

Item	Description
IfName	Interface name.
IfIndex	Index value of an interface.
PortIndex	Index value of a port.

3.8.7 display user-interface

Function

The **display user-interface** command displays information about a user interface.

Format

display user-interface [*ui-type ui-number1* | *ui-number*] [**summary**]

Parameters

Parameter	Description	Value
ui-type	Displays information about a specified user interface.	The value can be Console, VTY, or TTY.
ui-number1	Displays information about a user interface with a specified relative number.	The minimum value is 0. The maximum value is smaller by 1 than the number of user interfaces the system supports.
ui-number	Displays information about a user interface with a specified absolute number.	The value is an integer ranging from 0 to 177. The value varies according to the device type.
summary	Displays the summary of a user interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display user-interface** command, you can view detailed configuration information about all user interfaces or a specified user interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display detailed information about the user interface with the absolute number 0.

```
<Huawei> display user-interface 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi      Auth  Int
  0    CON 0    9600        -     3     -                P     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
  A    : Authenticate use AAA.
  N    : Current UI need not authentication.
  P    : Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

Display detailed information about all user interfaces.

```
<Huawei> display user-interface
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi      Auth  Int
  0    CON 0    9600        -     3     -                P     -
+ 129  VTY 0                -     3     3                A     -
+ 130  VTY 1                -     1     2                A     -
+ 131  VTY 2                -     3     2                A     -
  132  VTY 3                -     1     -                P     -
  133  VTY 4                -     1     -                A     -
...
UI(s) not in async mode -or- with no hardware support:
1-128
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
  A    : Authenticate use AAA.
  N    : Current UI need not authentication.
  P    : Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

Table 3-15 Description of the display user-interface command output

Parameter	Description
+	Active user interface.
F	Active user interface in asynchronous mode.
Idx	Absolute number of a user interface.
Type	Type and relative number of a user interface.
Tx/Rx	Data transfer rate of the user interface.
Modem	Type of the modem.
Privi	Authority configured on a user interface.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
ActualPrivi	Actual permission of a user interface. In the case of the AAA authentication mode, the level of a local user in AAA configuration is the actual permission.
Auth	Authentication mode on a user interface.
Int	User interface.
A	AAA authentication.
N	No authentication on the current user interface.
P	Password authentication.

Related Topics

19.1.37 display access-user (All views)

3.8.8 display user-interface maximum-vty

Function

The **display user-interface maximum-vty** command displays the maximum number of VTY users.

Format

display user-interface maximum-vty

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display user-interface maximum-vty** command to view the maximum number of users who connect to the device using Telnet or SSH. By default, the total number of Telnet users and SSH users is five maximum.

Example

Display the maximum number of VTY users.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display user-interface maximum-vty
Maximum of VTY user : 5
```

Table 3-16 Description of the display user-interface maximum-vty command output

Parameter	Description
Maximum of VTY user	Maximum number of VTY users. The maximum number of VTY users can be configured using the **user-interface maximum-vty** command.

Related Topics

3.8.27 user-interface maximum-vty

3.8.9 display users

Function

The **display users** command displays login information for each user interface.

Format

display users [**all**]

Parameters

Parameter	Description	Value
all	Displays information about all users who log in to the device through user interfaces, including information about user interfaces that are not used. If the **all** parameter is not used, the command displays only information about user interfaces that have been connected.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about users who are connected to the device. The information includes the user name, IP address, and authentication and authorization information.

Example

Run the **display users** command to view information about users who log in to the device through the user interface.

```
<Huawei> display users
  User-Intf    Delay      Type    Network Address     AuthenStatus     AuthorcmdFlag
  129 VTY 0    00:00:00   TEL     10.164.6.10          pass
Username : user1
+ 130 VTY 1    00:00:00   TEL     10.164.6.15          pass
Username : user2
```

Table 3-17 Description of the **display users** command output

Item	Description
+	Terminal line in use.
User-Intf	The number in the first column indicates the absolute number of the user interface, and the number in the second column indicates the relative number of the user interface. User Interface type. ● Console: Users who log in through the console port ● VTY: Users who log in using VTY ● TTY: Users who log in using TTY ● WEB: Users who log in through Web system
Delay	Interval from the user's latest input to the current time, in seconds.
Type	Connection type. ● Console ● Telnet ● SSH ● Web
Network Address	IP address of the login user.
Username	User name for logging in to the device. If the user name is not specified, **Unspecified** is displayed.
AuthenStatus	Whether the authentication succeeds.
AuthorcmdFlag	Command line authorization status.

3.8.10 display vty mode

Function

The **display vty mode** command displays the current VTY mode.

Format

display vty mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

VTY modes are classified into the man-to-machine mode and machine-to-machine mode.

Example

Display the VTY mode.

```
<Huawei> display vty mode
current VTY mode is Human-Machine interface
```

3.8.11 display vty lines

Function

The **display vty lines** command lists the number of rows displayed on the VTY screen.

Format

display vty lines

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

List the number of lines displayed on the VTY screen.

```
<Huawei> display vty lines
Current VTY lines is 24.
```

Related Topics

3.8.18 screen-length

3.8.12 flow-control

Function

The **flow-control** command configures the flow control mode.

The **undo flow-control** command restores the default flow control mode.

The default flow control mode is **none**, that is, flow control is disabled.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series AR2220E, and AR2220L do not support this command.

Format

flow-control { **hardware** | **none** }

undo flow-control

Parameters

Parameter	Description	Value
hardware	Specifies that the flow control mode is hardware flow control, and it applies only to the console port.	-
none	Specifies that the flow control mode is no flow control.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The configuration is effective only when the serial interface works in asynchronous interaction mode.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the flow control mode to hardware flow control in the user view.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] flow-control hardware
```

3.8.13 free user-interface

Function

The **free user-interface** command disconnects the device from a specified user interface.

Format

free user-interface { *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
ui-number	Specifies the absolute number of a user interface.	The value is an integer ranging from 0 to 177. The value varies according to the device type.
ui-type	Specifies the type of a user interface.	The value can be TTY, Console, or VTY.
ui-number1	Specifies the relative number of a user interface.	The minimum value is 0. The maximum value is smaller by 1 than the number of user interfaces the system supports.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user logs in to the device and does not perform an operation or you want to forbid a user from performing operations on the device, you can run the **free user-interface** command to disconnect a specified user's terminal from the device. After the command is executed, the device logs out the user.

Precautions

The **free user-interface** command cannot be executed on the current user interface. For example, if the current user interface is VTY 2, the **free user-**

interface vty 2 command fails to be executed on VTY 2 and an error message is displayed.

Example

Disconnect the device from user-interface 0.

```
<Huawei> free user-interface 0
Warning: User interface Console1 will be freed. Continue? [Y/N]:y
```

Related Topics

3.1.14 quit

3.8.15 idle-timeout

3.8.14 history-command max-size

Function

The **history-command max-size** command sets the size of the historical command buffer.

The **undo history-command max-size** command restores the default size of the historical command buffer.

By default, a maximum of 10 previously-used commands can be saved in the buffer.

Format

history-command max-size *size-value*

undo history-command max-size

Parameters

Parameter	Description	Value
size-value	Specifies the size of the historical command buffer.	The value is an integer ranging from 0 to 256.

Views

User interface view

Default Level

2: Configuration level

Usage Guidelines

The CLI can automatically save the historical commands that you enter. This function is similar to that of Doskey. You can invoke and run the historical commands at any time.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the size of the historical command buffer to 20.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] history-command max-size 20
```

Related Topics

3.1.7 display history-command

3.8.15 idle-timeout

Function

The **idle-timeout** command sets the timeout duration for disconnection from a user interface.

The **undo idle-timeout** command restores the default timeout duration.

By default, the timeout duration is 5 minutes.

Format

idle-timeout *minutes* [*seconds*]

undo idle-timeout

Parameters

Parameter	Description	Value
minutes	Specifies the idle timeout duration, in minutes.	The value is an integer ranging from 0 to 35791, in minutes.
seconds	Specifies the idle timeout duration, in seconds.	The value is an integer ranging from 0 to 59, in seconds.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user logs in to the device and does not perform an operation, the user interface is occupied unnecessarily. You can run the **idle-timeout** command to disconnect the user's terminal from the device.

Precautions

- If you set the time to zero, then the line connection remains alive until you close it.
- If the user interface disconnection function is not configured, other users may fail to log in to the device.
- If the idle timeout interval is set to 0 or a large value, the terminal will remain in the login state, resulting in security risks. You are advised to run the **lock** command to lock the current connection.
- You are advised to set the timeout duration to 10-15 minutes.

NOTE

If AAA authentication is required for login users, the timeout duration configured by the **local-user idle-timeout** command takes effect. If no timeout duration is configured or the **undo local-user idle-timeout** command is executed in the AAA view, the timeout duration configured by the **idle-timeout** command on the user interface takes effect.

Example

Set the timeout duration to 1 minute and 30 seconds.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] idle-timeout 1 30
```

Related Topics

3.8.13 free user-interface

19.1.60 local-user

3.8.16 parity

Function

The **parity** command sets the parity bit of a user interface.

The **undo parity** command disables the parity check.

By default, no parity check is configured.

Format

parity { **even** [**soft**] | **none** | **odd** [**soft**] }

undo parity

Parameters

Parameter	Description	Value
even	Specifies even parity check.	-
none	Specifies no parity check.	-
odd	Specifies odd parity check.	-
soft	Specifies soft parity check.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- To improve data transmission security, you can configure the parity bit so that the device verifies the packets transmitted by the console port. If a packet fails the verification, the device discards the packet.
- The **parity** { **even** | **odd** } command sets the parity bit to an even or odd value based on whether the last bit of the data bit is an even or odd value. The **parity** { **even** [**soft**] | **odd** [**soft**]} command sets the parity bit based on whether the total number of 1s in the eight bits of the data bit is an even or odd value. You need to select the same verification mode as that of the peer end.
- After the parameter is configured, if the transparent transmission through the serial interface function is enabled, the device does not strip the first bit of the data in hexadecimal notation greater than 0x80.

Precautions

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the transmission parity bit on the console interface to odd parity.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] parity odd
```

3.8.17 protocol inbound

Function

The **protocol inbound** command specifies the protocols that the VTY user interface supports.

By default, the system supports SSH and Telnet.

Format

protocol inbound { **all** | **ssh** | **telnet** }

Parameters

Parameter	Description	Value
all	Indicates that all protocols including SSH and Telnet are supported.	-
ssh	Indicates that only SSH is supported.	-
telnet	Indicates that only Telnet is supported.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To manage and monitor login users, configure the VTY user interface for login users and run the **protocol inbound** command to configure the protocols that the VTY user interface supports.

Prerequisites

If SSH is configured for the user interface using the **protocol inbound** command, you must configure the **authentication-mode aaa** authentication mode to ensure successful logins. If the **password** authentication mode is configured, the **protocol inbound ssh** command cannot be executed.

Precautions

- The configuration takes effect at the next login.
- When SSH is specified for the VTY user interface, the SSH server function is enabled, and the RSA key is not configured, a user cannot log in to the SSH server using SSH.
- Telnet is an insecure protocol. Using SSH is recommended.

Example

Configure SSH for user interfaces VTY0 to VTY4.

```
<Huawei> system-view
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] authentication-mode aaa
[Huawei-ui-vty0-4] protocol inbound ssh
```

Related Topics

3.8.3 authentication-mode (user interface view)

3.8.18 screen-length

Function

The **screen-length** command sets the number of lines on each terminal screen after you run a command.

The **undo screen-length** command restores the default configuration.

By default, the number of lines to be displayed on a terminal screen is 24.

Format

In the user interface view:

screen-length *screen-length* [**temporary**]

undo screen-length [**temporary**]

In the user view:

screen-length *screen-length* **temporary**

undo screen-length temporary

Parameters

Parameter	Description	Value
screen-length	Specifies the number of lines displayed on a terminal screen.	The value is an integer that ranges from 0 to 512. The value 0 indicates that all command output is displayed on one screen.
temporary	Specifies the number of lines temporarily displayed on a terminal screen.	-

Views

User interface view, user view

Default Level

3: Management level

Usage Guidelines

If you run a command and its output is displayed in more lines than you can see on one screen, you can reduce the number of lines displayed on each screen.

In general, you do not need to change the number of lines displayed on each screen. Setting the number of lines to 0 is not recommended. The configuration takes effect after you log in to the system again.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In the user view, the **temporary** parameter is mandatory and this command is at the Monitoring level. The configured value takes effect only on the current VTY user interface but does not take effect on the next login on the same user interface or login on other VTY user interfaces.

Example

Set the number of lines on each screen of the terminal to 30.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] screen-length 30
```

3.8.19 screen-width

Function

The **screen-width** command sets the number of columns displayed on a terminal screen.

The **undo screen-width** command restores the default configuration.

By default, 80 columns are displayed on a terminal screen.

Format

screen-width *screen-width*

undo screen-width

Parameters

Parameter	Description	Value
screen-width	Specifies the width of a terminal screen.	The value is an integer ranging from 60 to 512.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you log in to the device from a console interface and run the **display interface description** [*interface-type* [*interface-number*]] command to view the interface information, output information does not automatically change to another line, resulting in wrong format of the output information.

To resolve this problem, run the **screen-width** command to adjust the information format. In general, you do not need to adjust the number of columns displayed on the terminal screen. Setting the number of columns displayed on a screen is not recommended.

Precautions

The number of columns set using the **screen-width** command is valid only for the current interface. The setting is not saved after you log out. When you log in to the device from the console interface and configure this command, the number of columns displayed on the terminal screen is valid only for the current console interface, which has no impact on other users who log in to the device from the VTY interface or other interfaces. If you log out of the console interface and log in to the device again, the default width is used for the terminal screen.

This command is valid only for information displayed by the **display interface description** [*interface-type* [*interface-number*]] command.

Example

Set the screen width to 100.

```
<Huawei> screen-width 100
Warning: This command will change the default screen width. Continue? [Y/N]:y
Info: Succeeded in setting the screen width to 100.
```

3.8.20 set authentication password

Function

The **set authentication password** command configures a local authentication password.

By default, the local authentication password is not configured for the device.

Format

set authentication password cipher

Parameters

Parameter	Description	Value
cipher	Indicates a password in cipher text.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If password authentication is configured for users, you can run the **set authentication password** command to change the password or set a password in cipher text.

Pre-configuration Tasks

Before running the **set authentication password** command, ensure that password authentication has been configured for the user interface.

Precautions

- The passwords must meet the following requirements:
  - The password is a string of 8 to 128 case-sensitive characters.
  - The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character.

    The special characters include spaces and the following:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Password entered in interactive mode is not displayed on the screen.
- Users can press **CTRL_C** to cancel password modification in the interaction mode.
- If the current login channel has a password, enter the password when you want to set an authentication password for a VTY channel range that contains the current login channel.
- If the password authentication is configured but the password is not configured for the user interface, the user cannot log in to the device.
- If the **set authentication password** command is executed multiple times, the latest configuration overrides the previous ones. You can run the **set authentication password** command to change the local authentication password. After the password is changed, a user who wants to log in to the device must enter the latest password for identity authentication.

Example

Set the local authentication password for the user interfaces VTY 0-4.

```
<Huawei> system-view
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] set authentication password cipher
Enter Password(<8-128>):
Confirm Password:
[Huawei-ui-vty0-4]
```

Related Topics

3.8.3 authentication-mode (user interface view)

3.8.21 shell

Function

The **shell** command enables terminal services on a user interface.

The **undo shell** command disables terminal services on a user interface.

By default, terminal services are enabled on Console user interface and a VTY user interface and disabled on a TTY user interface.

Format

shell

undo shell

Parameters

None

Views

User interface view

Default Level

3: Management level

Usage Guidelines

You can use the **shell** command on a user interface to enable terminal services. This command enables users to enter commands through this interface to query device information and configure the device.

You can use the **undo shell** command on the user interface to disable terminal services. This command does not allow users to perform any operations through this interface. After the **undo shell** command is configured on the console user interface view, the user interface does not provide access through the console interface and MiniUSB interface. After using the **undo shell** command in the VTY view and TTY view, this user interface does not provide Telnet, STelnet, and SFTP access.

Example

Disable terminal services on VTY 0 to VTY 4.

```
<Huawei> system-view
[Huawei] user-interface vty 0 4
[Huawei-ui-vty0-4] undo shell
```

3.8.22 speed (user interface view)

Function

The **speed** command sets the data transfer rate of a user interface.

The **undo speed** command restores the default data transfer rate of a user interface.

By default, the data transfer rate is 9600 bit/s.

Format

speed *speed-value*

undo speed

Parameters

Parameter	Description	Value
speed-value	Specifies the data transfer rate of a user interface.	The value is expressed in bit/s. The asynchronous serial interface supports the following data transfer rates: ● 600 bit/s ● 1200 bit/s ● 2400bit/s ● 4800 bit/s ● 9600 bit/s ● 19200 bit/s ● 38400 bit/s ● 57600 bit/s ● 115200 bit/s **NOTE** ● The console user interface does not support 600 bit/s and 1200 bit/s.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

The setting is valid only when the serial port is configured to work in asynchronous mode.

Example

Set the data transfer rate of a user interface to 115200 bit/s.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] speed 115200
```

3.8.23 stopbits

Function

The **stopbits** command sets the stop bit of a user interface.

The **undo stopbits** command restores the default stop bit of a user interface.

By default, the stop bit is 1.

Format

stopbits { **1.5** | **1** | **2** }

undo stopbits

Parameters

Parameter	Description	Value
1.5	Sets the stop bit to 1.5.	-
1	Sets the stop bit to 1.	-
2	Sets the stop bit to 2.	-

Views

User interface view

Default Level

3: Management level

Usage Guidelines

If the stop bit is 1, the corresponding data bit is 7 or 8.

If the stop bit is 1.5, the corresponding data bit is 5.

If the stop bit is 2, the corresponding data bit is 6, 7, or 8.

The setting is valid only when the serial port is configured to work in asynchronous mode.

NOTE

On the console user interface, the stop bit 1.5 is not supported.

Example

Set the stop bit of a user interface to 2.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0] stopbits 2
```

3.8.24 user privilege

Function

The **user privilege** command configures the user level.

The **undo user privilege** command restores the default user level.

By default, users who log in to the device using the console interface are at level 15 and other users are at level 0.

Format

user privilege level *level*

undo user privilege level

Parameters

Parameter	Description	Value
level *level*	Specifies the user level. **NOTE** The larger the value, the higher the priority.	The value is an integer ranging from 0 to 15.

Views

User interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system manages users at levels to control their access permissions. Users who log in to the device can use only commands at the same or lower level than their own levels.

Commands are classified into the visit level, monitoring level, configuration level, and management level that map levels 0, 1, 2, and 3, as listed in **Table 3-18**.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-18 Introduction to command levels

User Level	Command Level	Name	Description
0	0	Visit	Commands at this level are diagnosis commands such as ping and tracert commands and commands that are used to access a remote device such as Telnet clients.
1	0 and 1	Monitoring	Commands at this level are system maintenance commands such as display commands. **NOTE** Some display commands are not at this level. For example, the **display current-configuration** and **display saved-configuration** commands are at level 3.
2	0, 1, and 2	Configuration	Commands at this level are service configuration commands.
3-15	0, 1, 2, and 3	Management	Commands at this level are system basic operation commands that support services, including file system, FTP, TFTP, user management commands, command level configuration commands, and debugging commands.

Precautions

If refined right management is required, run the **command-privilege level** command to upgrade command levels.

Example

Set the user level on the VTY0 user interface to 2.

```
<Huawei> system-view
[Huawei] user-interface vty 0
[Huawei-ui-vty0] user privilege level 2
```

Log in to the device using Telnet and view detailed information about the VTY0 user interface.

```
<Huawei> display user-interface vty 0
  Idx  Type     Tx/Rx      Modem Privi ActualPrivi Auth  Int
+ 129   VTY 0              -     2     15          N     -
  +    : Current UI is active.
  F    : Current UI is active and work in async mode.
  Idx  : Absolute index of UIs.
  Type : Type and relative index of UIs.
  Privi: The privilege of UIs.
  ActualPrivi: The actual privilege of user-interface.
  Auth : The authentication mode of UIs.
  A: Authenticate use AAA.
  N: Current UI need not authentication.
  P: Authenticate use current UI's password.
  Int  : The physical location of UIs.
```

Table 3-19 Description of the user privilege level command output.

Item	Description
+	Current user interface is active.
F	Current user interface is active and work is in asynchronous mode.
Idx	Absolute index of user interface.
Type	Type and relative index of user interface.
Privi	The privilege of user interface.
ActualPrivi	The actual privilege of user interface.
Auth	The authentication mode of user interface.
Int	The physical location of UIs.
A	Authenticate use AAA.
N	The current user interface need not be authenticated.
P	Authenticates the user using the password configured on the current user interface.

Related Topics

3.12.8 display current-configuration
3.12.12 display saved-configuration
3.8.7 display user-interface

3.8.25 user-interface

Function

The **user-interface** command displays one or multiple user interface views.

Format

user-interface [*ui-type*] *first-ui-number* [*last-ui-number*]

Parameters

Parameter	Description	Value
ui-type	Specifies the type of a user interface. ● If the user interface is specified, the relative number is used. ● If the user interface is not specified, the absolute number is used.	The value can be console, tty, or vty.
first-ui-number	Specifies the number of the first user interface.	● If *ui-type* is set to **console**, the *first-ui-number* value is **0**. ● If *ui-type* is set to **vty**, the *first-ui-number* value ranges from 0 to the maximum number of VTY user interfaces. ● If *ui-type* is set to **tty**, the *first-ui-number* value ranges from 1 to the maximum number of TTY user interfaces.
last-ui-number	Specifies the number of the last user interface. When you select this parameter, you enter multiple user interface views at the same time. This parameter is valid only when *ui-type* is set to VTY or TTY. The *last-ui-number* value must be larger than the *first-ui-number* number.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the network administrator logs in to the device using the console interface, asynchronous serial interface, Telnet, or SSH, the system manages and monitors the session between the user and the device on the corresponding user interface. Each user interface corresponds a user interface view. The network administrator can set parameters such as authentication and user level to manage sessions in a unified manner.

Precautions

Only users at level 15 can use this command.

The user interface varies according to the login mode. The user interface views can be numbered using absolute numbers or relative numbers. **Table 3-20** describes absolute and relative numbers of user interfaces.

NOTE

- The relative numbering uniquely specifies a user interface or a group of user interfaces of the same type.
- The absolute numbering specifies a user interface or a group of user interfaces.

Table 3-20 Absolute and relative numbers of user interfaces

User Interface	Description	Absolute Number	Relative Number
Console user interface	Manages and controls users that log in to the device using the console interface.	0	0
TTY user interface	Manages and controls users that log in to the device using the asynchronous serial interface. **NOTE** The AR150&160&200 series do not support the TTY user interface.	1 to 128	The first one is TTY 1, the second one is TTY 2, and so on. Absolute numbers 1 to 128 map relative numbers TTY 1 to TTY 128.
VTY user interface	Manages and controls users that log in to the device using Telnet or SSH.	129 to 143	The first one is VTY 0, the second one is VTY 1, and so on. Absolute numbers 129 to 143 map relative numbers VTY 0 to VTY 14.

After you log in to the device, you can run the **display user-interface** command to view the supported user interfaces and the corresponding relative and absolute numbers.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enter the Console 0 user interface.

```
<Huawei> system-view
[Huawei] user-interface console 0
[Huawei-ui-console0]
```

Enter the VTY 1 user interface.

```
<Huawei> system-view
[Huawei] user-interface vty 1
[Huawei-ui-vty1]
```

Enter the VTY 1 to VTY 3 user interfaces.

```
<Huawei> system-view
[Huawei] user-interface vty 1 3
[Huawei-ui-vty1-3]
```

Related Topics

3.8.7 display user-interface

3.8.26 user-interface current

Function

The **user-interface current** command displays the current user interface view.

Format

user-interface current

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enter the current user interface view, run the **display user-interface** command without the user interface number.

Precautions

Only users at level 15 can use this command.

The user interface varies according to the login mode. The user interface views can be numbered using absolute numbers or relative numbers. **Table 3-20** describes absolute and relative numbers of user interfaces.

NOTE

- The relative numbering uniquely specifies a user interface or a group of user interfaces of the same type.
- The absolute numbering specifies a user interface or a group of user interfaces.

Example

Enter the current user view.

```
<Huawei> system-view
[Huawei] user-interface current
[Huawei-ui-vty1]
```

Related Topics

3.8.25 user-interface

3.8.7 display user-interface

3.8.27 user-interface maximum-vty

Function

The **user-interface maximum-vty** command configures the maximum number of login users.

The **undo user-interface maximum-vty** command restores the default maximum number of login users.

By default, the maximum number of Telnet and SSH users is 5.

Format

user-interface maximum-vty *number*

undo user-interface maximum-vty

Parameters

Parameter	Description	Value
number	Specifies the maximum number of Telnet and SSH users.	The value is an integer ranging from 0 to 15 or 16 to 20. **NOTE** The value range 16 to 20 is supported only after the maximum number of users is set to 15. In addition, the value range 16 to 20 is used only for emergent user escape.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **user-interface maximum-vty** command configures the maximum number of login users.

Precautions

- If the maximum number that you set is smaller than the number of current online users, the system displays a configuration failure message.
- The maximum number of login users set by the **user-interface maximum-vty** command is the total number of Telnet and SSH users.
- If the maximum number of login users is set to 0, no user is allowed to log in to the device using Telnet or SSH.

Example

Set the maximum number of Telnet users to 7.

```
<Huawei> system-view
[Huawei] user-interface maximum-vty 7
```

Related Topics

3.8.8 display user-interface maximum-vty

3.9 User Login Configuration Commands

3.9.1 connect

Function

The **connect** command establishes a control connection between a dumb terminal and a remote server.

The **undo connect** command closes a control connection between a dumb terminal and a remote server.

By default, a dumb terminal and a remote server do not establish a control connection.

Format

connect *host* [*port-number*] [**-a** *source-ip-address* | **-i** *interface-type interface-number*] [**-t** *interval*]

undo connect

Parameters

Parameter	Description	Value
host	Specifies the IP address or host name of the remote server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
port-number	Specifies the port number of a remote server.	The value is an integer that ranges from 1 to 55535. The default value 23 is the standard Telnet server port number.
-a *source-ip-address*	Specifies the source IP address of the local router.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the outbound interface of the local router.	-
-t *interval*	Specifies the interval at which the local router automatically establishes a connection to the remote server.	The value is an integer that ranges from 5 to 60, in seconds.

Views

TTY user interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a dumb terminal that has no IP address configured initiates a control connection setup request to a remote server through the router, run the **connect** command on the router to establish a control connection between the dumb terminal and remote server.

Precautions

The dumb terminal must connect to the asynchronous serial interface of the router.

If **-t** *interval* is not specified, the local router does not automatically establish a control connection to the remoter server.

Example

Establish a control connection between the dumb terminal and remote server.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] user-interface tty 41
[Huawei-ui-tty41] undo shell
[Huawei-ui-tty41] connect 1.1.1.2 1025 -a 1.1.1.1
```

3.9.2 config lock

Function

The **config lock** command locks the system configuration.

The **undo config lock** command unlocks the system configuration.

By default, the system configuration is unlocked.

Format

config lock

undo config lock

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent other users from modifying or deleting configured data, you can run the **config lock** command to lock the configuration management plane before data configuration. After completing data configuration, run the **undo config lock** command to unlock the configuration management plan so that other users can perform data configuration.

Precautions

The locked system configuration can be unlocked by only the user who locks it, the super administrator (run the **user privilege** command to set the user level to 15), or the network management system (NMS) user.

Example

Lock the system configuration.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] config lock
The system config is locked
```

Unlock the system configuration.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] undo config lock
The system config is unlocked
```

Related Topics

3.9.4 display config lock

3.9.3 config unlock interval

Function

The **config unlock interval** command configures the interval for unlocking a device.

The default interval is 5 minutes.

Format

config unlock interval *time*

Parameters

Parameter	Description	Value
time	Specifies the interval for unlocking a device.	The value is an integer ranging from 1 to 255, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the device configuration is clocked by the **config lock** command, other users cannot modify the configuration. In this case, the **config unlock interval** command can be used to configure the unlock interval, after which the device configuration is unlocked automatically.

Precautions

This command can be used by only the super administrator (run the **user privilege** command to set the user level to 15) and NMS user.

If you run the command multiple times, only the latest configuration takes effect.

The unlocking interval starts from the last time the current user configures the system.

Example

Set the unlock interval to 2 minutes.

```
<Huawei>system-view
[Huawei]config unlock interval 2
```

The following message is displayed when the configured unlock interval arrives.

```
[Huawei]
 The system config is unlocked
```

Related Topics

3.9.2 config lock

3.9.4 display config lock

3.9.4 display config lock

Function

The **display config lock** command displays lock information about the system configuration.

Format

display config lock

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

The information includes whether the system configuration is locked and the lock duration If you cannot configure the Router after login, run this command. The command output helps you locate faults. If the system configuration is locked, the command output includes the following: type, name, and IP address of the user who locks the configuration. If no IP address is available, **locked user IP address** is blank.

If the current system configuration is locks by a user (user A), only users at the same level as or higher level than user A can query user A information. If users at

a lower level queries user A information, the system displays a message indicating that the system configuration is locked by a user with a higher level.

Example

Display lock information about the system configuration (when configuration is not locked).

```
<Huawei> display config lock
  ------------------------------------------------------------------------------
  automatically unlocked interval(minute): 5
  locked state:                            unlocked
  ------------------------------------------------------------------------------
```

Table 3-21 Description of the display config lock command output

Item	Description
automatically unlocked interval(minute)	Interval after which the system automatically unlocks the configuration, in minutes.
locked state	Whether the system configuration is locked. The values are as follows: ● **locked**: indicates that the system configuration is locked. ● **unlocked**: indicates that the system configuration is not locked.

Display lock information about the system configuration (when configuration is locked).

```
<Huawei> display config lock
------------------------------------------------------------------------------
  automatically unlocked interval(minute): 5
  locked state:                            locked
  locked user type:                          telnet
  locked user name:                            huawei
  locked user IP address:                      192.168.0.1
------------------------------------------------------------------------------
```

Table 3-22 Description of the display config lock command output

Item	Description
automatically unlocked interval(minute)	Interval after which the system automatically unlocks the configuration, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
locked state	Whether the system configuration is locked. The values are as follows: • **locked**: indicates that the system configuration is locked. • **unlocked**: indicates that the system configuration is not locked.
locked user type	Type of the user who locks the system configuration. The user can be any of the following types: NMS user, serial port user, Telnet user, and web user.
locked user name	Name of the user who locks the system configuration.
locked user IP address	IP address of the user who locks the system configuration. If no IP address is available, **locked user IP address** is blank.

Related Topics

3.9.2 config lock

3.9.5 display ecc local-key-pair public

Function

The **display ecc local-key-pair public** command displays information about the public key in the local Elliptic Curves Cryptography (ECC) key pair.

Format

display ecc local-key-pair public

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **display ecc local-key-pair public** command to check information about the public key in the local ECC key pair on a client and then copy the public key to the server. The public key enables a server to authenticate users and ensures the login of authorized users.

Pre-configuration Tasks

You must run the **ecc local-key-pair create** command to generate a local ECC host key pair before using the command.

Example

Display information about the public key in the local ECC key pair on a client.

```
<Huawei> display ecc local-key-pair public
=====================================================
Time of Key pair created:2016-06-10 04:45:43+00:00
Key name : localhost_Host_ECC
Key modulus : 256
Key type : ECC encryption Key
Key fingerprint:
=====================================================
Key code:
04B8EC97 382591C6 BE764727 0B06F673 4E3FF3C9 C10F98F9 4D7D9B09 593DF604
D1465979 107F638D 59771BD1 C1C2D325 B7C3A331 9646B76F A9BACA98 4C0F19D2
BC

Host public key for PEM format code:
---- BEGIN SSH2 PUBLIC KEY ----
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLjslzglkca+
dkcnCwb2c04/88nBD5j5TX2bCVk99gTRRll5EH9jjVl3G9HBwtMlt8OjMZZGt2+p
usqYTA8Z0rw=
---- END SSH2 PUBLIC KEY ----

Public key code for pasting into OpenSSH authorized_keys file :
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBLjslzglkca
+dkcnCwb2c04/88nBD5j5TX2bCVk99gTRRll5EH9jjVl3G9HB
wtMlt8OjMZZGt2+pusqYTA8Z0rw= ecdsa-key
```

Table 3-23 Description of the display ecc local-key-pair public command output

Item	Description
Time of Key pair created	Time when the public key in the local ECC key pair is generated, in the format of YYYY-MM-DD HH:MM:SS.
Key Name	Name of the public key in the local ECC key pair.
Key modulus	Length of the public key in the local ECC key pair.
Key Type	Type of the public key in the local ECC key pair.
Key Code	Code of the public key in the local ECC key pair configured using the **ecc local-key-pair** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Host public key for PEM format code	PEM code of the public key in the local ECC key pair.
Public key code for pasting into OpenSSH authorized_keys file	Public key in the local ECC key pair used for OpenSSH authentication. Copy the public key to the **authorized_keys** file of OpenSSH to make the key effective.

Related Topics

3.9.13 ecc local-key-pair

3.9.6 display ecc peer-public-key

Function

The **display ecc peer-public-key** command displays information about the ECC public key configured on the remote end.

Format

display ecc peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays brief information about the ECC public key configured on the remote end.	-
name *key-name*	Displays the ECC public key with the specified name.	The value is a string of 1 to 30 case-sensitive characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **display ecc peer-public-key** command on a client to check information about the public key configured on the remote end. The public key enables a server to authenticate users and ensures the login of authorized users.

Example

Display brief information about all the ECC public keys.

```
<Huawei> display ecc peer-public-key brief
-----------------------------------------
      Bits      Name
-----------------------------------------
      256       testecc
-----------------------------------------
```

Display detailed information about the ECC public key named **testecc**.

```
<Huawei> display ecc peer-public-key name testecc
=====================================
   Key name: testecc
   Encoding type: OPENSSH
=====================================
Key Code:
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHYuJAsMAHPFT53pXNlXAE1YjXvjhdultL
zcDcrzJLqvPxhKALn1WXGPaNfQ
sAFQnsHzUYgICcBz/Cpxb5atVeg= ecdsa-key
```

Table 3-24 Description of the display ecc peer-public-key command output

Item	Description
Bits	Length of the ECC public key configured on the remote end.
Name	Name of the ECC public key configured on the remote end.
Key name	Name of the ECC public key configured on the remote end.
Encoding type	Encoding format of the ECC public key configured on the remote end. ● OPENSSH If OpenSSH is specified, data is Base64 encoded. OpenSSH is derived from PEM. ● PEM If PEM is specified, data is Base64 encoded. ● DER If DER is specified, data is Base16 encoded.
Key Code	Code of the public key in the local ECC key pair configured using the **ecc local-key-pair** command.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

3.9.14 ecc peer-public-key

3.9.7 display rsa local-key-pair public

Function

The **display rsa local-key-pair public** command displays the public key in the local key pair.

Format

display rsa local-key-pair public

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command on the client and configure the client public key in the command output to the SSH server, which ensures that the SSH client validity check by the SSH server is successful and enables the secure data exchange between the SSH server and client.

Example

Display the public key in the local key pair.

```
<Huawei> display rsa local-key-pair public
=====================================================

Time of Key pair created: 2011-10-06 16:26:37+00:00
Key name: Host
Key type: RSA encryption Key
=====================================================

Key code:
3047
  0240
    D538B7FC 3AFE1F5B F6C921F9 3D8C5322
905F623A
    F0123161 3DA61EEB F5E897CF DC126060
546CC84E
    B2AB7424 3EFF5D71 D84C5FE2 3E2BF5B3
D82DD979
    A22E4AA1
  0203
    010001
```

```
=====================================================

Time of Key pair created: 2011-10-06 16:26:53+00:00
Key name: Server
Key type: RSA encryption Key
=====================================================

Key code:
3067
  0260
    C51C2C01 56B06E6C EBF9055C F7AD9781
46B41A31
    5FC87282 E53CFE30 8E6321D3 AC74E948
0A010339
    E67C290E 2E0E8E40 BF5E1C97 F9C856EF
568DC159
    1A6D28ED AFFB474B 43EFB632 CFB0875F
85420EEA
    1919095B A5BC38D0 5FFF169E
0BDB3DC3
  0203
    010001
```

Table 3-25 Description of the **display rsa local-key-pair public** command output

Item	Description
Time of Key pair created	Time and date when the public key is created.
Key Name	The value can be the host or server public key. The server public key is saved only when the key type is RSA.
Key Type	Type of the public key.
Key Code	Code of the public key.

Related Topics

3.9.25 rsa local-key-pair create

3.9.8 display rsa peer-public-key

Function

The **display rsa peer-public-key** command displays the peer public key saved on the local host. If no parameter is specified, the command displays detailed information about all peer public keys.

Format

display rsa peer-public-key [**brief** | **name** *key-name*]

Parameters

Parameter	Description	Value
brief	Displays the brief information about all peer public keys.	-
name *key-name*	Specifies the key name.	The value is a string of 1 to 30 case-insensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check detailed information about the RSA public key and whether the local and peer public keys are the same.

Precautions

You must complete the RSA public key configuration before running this command.

Example

Display the brief information about all RSA public keys.

```
<Huawei> display rsa peer-public-key brief
Name                          Bits
-------------------------------------
rsakey001                      780
```

Table 3-26 Description of the display rsa peer-public-key brief command output

Item	Description
Bits	Bits in the public key.
Name	Name of the public key.

Display the detailed information about the RSA public key named **rsakey001**.

```
<Huawei> display rsa peer-public-key name rsakey001

=====================================
    Key name: rsakey001
=====================================
Key Code:
```

```
3067
  0260
    A3158E6C F252C039 135FFC45 F1E4BA9B 4AED2D88 D99B2463 3E42E13A 92A95A37
    45CDF037 1AF1A910 AAE3601C 2EB70589 91AF1BB5 BD66E31A A9150911 859CAB0E
    1E10548C D70D000C 55A1A217 F4EA2F06 E44BD438 DA472F14 3FB7087B 45E77C05
  0203
    010001
```

Table 3-27 Description of the display rsa peer-public-key name command output

Item	Description
Key name	Name of the public key.
Key Code	Code of the public key.

Related Topics

3.9.27 rsa peer-public-key

3.9.9 display ssh server

Function

The **display ssh server** command displays the SSH server information.

Format

display ssh server { **status** | **session** }

Parameters

Parameter	Description	Value
status	Displays the global configuration on the SSH server.	-
session	Displays the current session connection information on the SSH server.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the SSH attributes, you can run this command to view the configuration or session connection information on the SSH server to verify that the SSH connection has been established.

Example

Display the global configuration on the SSH server.

```
<Huawei> display ssh server status
 SSH version                        :1.99
 SSH connection timeout             :120 seconds
 SSH server key generating interval  :0 hours
 SSH Authentication retries         :3 times
 SFTP Server                        :Enable
 Stelnet server                     :Enable
```

Table 3-28 Description of the display ssh server status command output

Item	Description
SSH version	SSH protocol version. The value can be **1.99** or **2.0**.
SSH connection timeout	SSH connection timeout interval. The value ranges from **60** to **120**. The default value is **60**. The unit is second. Run the **ssh server timeout** command to set this item.
SSH server key generating interval	Key updating period of the SSH server. The default value is **0**. The unit is hour. Run the **ssh server rekey-interval** command to set this item.
SSH authentication retries	Number of times for retrying SSH authentication. The default value is **3**. Run the **ssh server authentication-retries** command to set this item.
SFTP Server	Status of the SFTP server. By default, it is disabled. Run the **sftp server enable** command to set this item.
Stelnet server	Status of the STelnet server. By default, it is disabled. Run the **stelnet server enable** command to set this item.

Display the current session connection information on the SSH server.

```
<Huawei> display ssh server session
 ------------------------------------------------------------------------
Conn    Ver   Encry     State  Auth-type        Username
------------------------------------------------------------------------
VTY 0  2     AES       run    password         john
------------------------------------------------------------------------
```

Table 3-29 Description of the display ssh server session command output

Item	Description
Conn	VTY connection.
Ver	Version number.
Encry	Encryption mode.
State	Session status on the SSH server.
Auth-type	Authentication mode for an SSH user. The options are as follows: • password • rsa • password-rsa (password and RSA) • all (password or RSA) Run the **ssh user authentication-type** command to set this item.
Username	User name for SSH server authentication.

Related Topics

3.11.64 sftp server enable
3.9.38 ssh server port
3.9.46 stelnet server enable

3.9.10 display ssh user-information

Function

The **display ssh user-information** command displays the configuration of all SSH users.

Format

display ssh user-information [*username*]

Parameters

Parameter	Description	Value
username	Displays the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the SSH user name, bound RSA public key name, and service type.

Example

Display the configuration of all SSH users.

```
<Huawei> display ssh user-information
 ---------------------------------------------------------------------------
 Username        Auth-type        User-public-key-name
 ---------------------------------------------------------------------------
 a               password         null
 ---------------------------------------------------------------------------
```

Table 3-30 Description of the display ssh user-information command output

Item	Description
Username	SSH user name.
Auth-type	Authentication mode for an SSH user. The options are as follows: ● password ● rsa ● password-rsa (password and RSA) ● all (password or RSA) Run the **ssh user authentication-type** command to set this item.
User-public-key-name	Peer RSA public key assigned to an SSH user. Run the **rsa peer-public-key** command to set this item.

Related Topics

3.9.27 rsa peer-public-key

3.9.43 ssh user authentication-type

 Copyright © Huawei Technologies Co., Ltd.

3.9.11 display telnet server status

Function

The **display telnet server status** command displays the status and configuration of the Telnet server.

Format

display telnet server status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

- You can run this command to check whether the device functions as a Telnet server.
- You can run this command to check the listening port number of the Telnet server if you have set the port number by running the **telnet server port** *port-number* command.

Example

Display the status and configuration of the Telnet server.

```
<Huawei> display telnet server status
 TELNET IPv4 server              :Enable
 TELNET IPv6 server              :Enable
 TELNET server port              :23
```

Table 3-31 Description of the display telnet server status command output

Item	Description
TELNET IPv4 server	IPv4 Telnet server.
TELNET IPv6 server	IPv6 Telnet server.
TELNET server port	Listening port number of the Telnet server.

 Copyright © Huawei Technologies Co., Ltd.

3.9.12 display telnet-client

Function

The **display telnet-client** command displays the source parameters when the device works as a Telnet client.

Format

display telnet-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After setting source parameters of the Telnet client, you can run this command to check the setting result. If you have not set **telnet client-source**, the default source IP address is 0.0.0.0.

Example

Display the source parameters for the device that works as a Telnet client.

```
<Huawei> display telnet-client
 The source address of telnet client is 10.1.1.1
```

Table 3-32 Description of the display telnet-client command output

Item	Description
The source address of telnet client is 10.1.1.1	The source IP address of the Telnet client is 10.1.1.1.

3.9.13 ecc local-key-pair

Function

The **ecc local-key-pair create** command generates a local ECC host key pair.

The **ecc local-key-pair destroy** command deletes the local ECC key.

 Copyright © Huawei Technologies Co., Ltd.

Format

ecc local-key-pair create

ecc local-key-pair destroy

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A local key pair is a prerequisite to a successful SSH login. Compared with the RSA algorithm used by the **rsa local-key-pair create** command, the ECC algorithm shortens the key length, accelerates the encryption, and improves the security. The length of the server key pair can be 256 bits, 384 bits and 521 bits. By default, the length of the key pair is 256 bits.

If you no longer need the local ECC key pairs, run the **ecc local-key-pair destroy** command to delete them.

Configuration Impact

The **ecc local-key-pair destroy** command deletes the local ECC host key pair, from the files on the master and slave main control boards. Exercise caution when you run this command.

Precautions

- The generated ECC host key pair is named in the format of the Router name_Host_ECC, such as HUAWEI_Host_ECC.
- The **ecc local-key-pair create** and **ecc local-key-pair destroy** commands are not saved in the configuration file. They only need to be run once and take effect even after the Router restarts.
- Do not delete the ECC key file from the Router. If the ECC key file is deleted, the ECC key pair cannot be restored after the Router is restarted.

Example

Generate a local ECC host key pair

```
<Huawei> system-view
[Huawei] ecc local-key-pair create
Info: The key name will be: HUAWEI_Host_ECC.
Info: The ECC host key named HUAWEI_Host_ECC already exists.
Warning: Do you want to replace it ? [Y/N]: Y
Info: The key modulus can be any one of the following : 256, 384, 521.
```

```
Info: If the key modulus is greater than 512, it may take a few minutes.
Please input the modulus [default=256]:256
Info: Generating keys...
Info: Succeeded in creating the ECC host keys.
```

Delete the local ECC host key pair.

```
<Huawei> system-view
[Huawei] ecc local-key-pair destroy
Info: The name of the key which will be destroyed is HUAWEI_Host_ECC.
Warning: These keys will be destroyed. Continue? [Y/N]:Y
Info: Succeeded in destroying the ECC host keys.
```

Related Topics

3.9.5 display ecc local-key-pair public

3.9.14 ecc peer-public-key

Function

The **ecc peer-public-key** command generates an ECC public key and enters the ECC public key view.

The **undo ecc peer-public-key** command deletes the ECC public key.

By default, no ECC public key is generated.

Format

ecc peer-public-key *key-name* **encoding-type** { **der** | **openssh** | **pem** }

undo ecc peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the ECC public key name.	The value is a string of 1 to 30 case-sensitive characters without spaces.
encoding-type	Specifies the encoding format of the ECC public key.	-
der	Sets the encoding format of the ECC public key to DER. DER uses hexadecimal notation to encode data.	-

Parameter	Description	Value
openssh	Sets the encoding format of the ECC public key to OpenSSH. OpenSSH uses base64 notation to encode data. OpenSSH is revised from PEM.	-
pem	Sets the encoding format of the ECC public key to PEM. PEM uses base64 notation to encode data.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you use an ECC public key for authentication, specify the public key on the server for the client of SSH users. When the client logs in to the server, the server uses the specified public key to authenticate the client.

After you enter the ECC public key view, run the **public-key-code begin** command, and copy the ECC public key to the server.

The public key on the client is randomly generated by the client software.

If an ECC public key has been assigned to an SSH user, delete the mapping between the ECC public key and the SSH user. If you do not delete the mapping, the **undo ecc peer-public-key** command cannot delete the ECC public key.

Follow-up Procedure

After you copy the ECC public key generated on the client to the server, perform the following operations to exit the ECC public key view:

1. Run the **public-key-code end** command to return to the ECC public key view.
2. Run the **peer-public-key end** command to exit the ECC public key view and return to the system view.

Precautions

A maximum of 20 ECC public keys can be configured.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an ECC public key and enter the ECC public key view.

```
<Huawei> system-view
[Huawei] ecc peer-public-key ecc-peer-key encoding-type pem
Info: Enter "ECC public key" view, return system view with "peer-public-key end".
[Huawei-ecc-public-key] public-key-code begin
Info: Enter "ECC key code" view, return the last view with "public-key-code end".
[Huawei-ecc-key-code] ---- BEGIN SSH2 PUBLIC KEY ----
[Huawei-ecc-key-code] AAAAE2VjZHNhLXNoYTItbmlzdHA1MjEAAAAIbmlzdHA1MjEAAACDBL5J4v3pqi5S
[Huawei-ecc-key-code] ALI9lvLw4cdvtpD2AC6sEJXg9GDCD5vGBnkXlKmnOy6d1TyrXx57ZPNnrSdqVkHC
[Huawei-ecc-key-code] sMBa63vSwg1XsVW2qZgx8H57+FJiTPY61b1Vfst9GUif1ymfpB7XrbdYZDownoh0
[Huawei-ecc-key-code] FZNadZtIf2CRc0OeiKXbCSPP25dfoT/DTcc=
[Huawei-ecc-key-code] ---- END SSH2 PUBLIC KEY ----
[Huawei-ecc-key-code] public-key-code end
[Huawei-ecc-public-key] peer-public-key end
```

Delete an ECC public key.

```
<Huawei> system-view
[Huawei] undo ecc peer-public-key ecc-peer-key
```

Related Topics

3.9.20 public-key-code begin

3.9.21 public-key-code end

3.9.19 peer-public-key end

3.9.15 exline-breaker

Function

The **exline-breaker enable** command enables the function of adding a line break.

The **exline-breaker disable** command disables the function of adding a line break.

By default, the function of adding a line break is disabled.

Format

exline-breaker { **enable** | **disable** }

Parameters

Parameter	Description	Value
enable	Enables the function of adding a line break.	-
disable	Disables the function of adding a line break.	-

Views

TTY user interface view

Default Level

3: Management level

Usage Guidelines

The device functions as a calling end to send a line break **\r\n**. When receiving the line break, the called end discards **\n** in the line break. As a result, data of the calling end differs from that of the called end. In this case, you can run the **exline-breaker enable** command to enable the function of adding a line break. After the function is enabled, the calling end adds a line break **\n** to **\r\n** when sending it. When the called end receives the data, it removes only one **\n** from the line break.

Example

Enable the function of adding a line break.

```
<Huawei> system-view
[Huawei] user-interface tty 41
[Huawei-ui-tty41] undo shell
[Huawei-ui-tty41] exline-breaker enable
```

3.9.16 language character-set

Function

The **language character-set** command configures the character set in the system.

The default character set in the system is ISO8859-1, that is, the system only supports English input.

Format

language character-set *character*

Parameters

Parameter	Description	Value
character	Specifies the character set in the system.	Currently, the system supports the following character sets: GBK, UTF-8, and ISO8859-1.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can configure the character set so that the system just supports Chinese or supports Chinese and English input. The character set facilitates device identification and management, for example, Chinese interface description can be configured.

Currently, the system supports the following character sets: GBK, UTF-8, and ISO8859-1. GBK and UTF-8 support both English and Chinese input, whereas ISO8859-1 supports only English input. GBK is a Chinese character set and UTF-8 is an international character set. To enter Chinese characters on the device, configure GBK or UTF-8 according to the character set supported on the terminal login software.

Precaution

The character set supported by the terminal login software affects the display of Chinese characters. If the character sets in the system and on the terminal login software are different, Chinese characters may be displayed as garbled characters.

After the character set function is configured, the device cannot work together with eSight or iManager U2000. The web system only displays the UTF-8 character set and does not support Chinese input.

Example

Configure GBK as the character set in the system.

```
<Huawei> system-view
[Huawei] language character-set GBK
```

3.9.17 lock

Function

The **lock** command locks the current user interface to prevent unauthorized users from operating the interface.

By default, the system does not automatically lock the current user interface.

Format

lock

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Lock the current user interface using this command to prevent other users from operating the interface. The user interfaces consist of console ports, and Virtual Type Terminals (VTYs).

After using the **lock** command, you are prompted to input the password twice. If you input the correct password for twice, the user interface is locked.

Precautions

- The passwords must meet the following requirements:
  - The password is a string of 8 to 128 case-sensitive characters.
  - The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character.

    The special characters include spaces and the following:

    `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Password entered in interactive mode is not displayed on the screen.
- When you run the **lock** command to lock the user interface and set a locking password, you can press **CTRL_C** to cancel the operation.
- To unlock the user interface, press **Enter**, and then input the correct password as prompted by the system.

Example

Lock the current user interface after logging in through the console port.

```
<Huawei> lock
Enter Password(<8-128>):
Confirm Password:
Info: The terminal is locked.
```

To log in to the system after the system is locked, you must press **Enter**. The following information is displayed:

```
Enter Password:
```

Enter the correct password and return to the user view.

```
<Huawei>
```

3.9.18 matched upper-view

Function

The **matched upper-view** command allows the system to search for the **undo** command in the upper view, and returns to the upper view.

The **undo matched upper-view** command prohibits the system from searching for the **undo** command in the upper view.

By default, the system does not search for the **undo** command in the upper view.

Format

matched upper-view

undo matched upper-view

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

When you run the **undo** command in a view, which is not registered in the current view, the system searches for the command in the upper view if the system is allowed to search for the **undo** command in the upper view. If the system finds the same **undo** command, the system executes this command in the upper view. If the system does not find the same **undo** command in the upper view, the system continues to search for this command in other upper views till the system view.

Running this command brings security risks. For example, if you run the **undo ftp server** command in the interface view, while this command is not registered in the interface view, the system automatically searches for it in the upper view, that is, the system view. In this manner, the system disables the FTP function.

The **matched upper-view** command is valid only for current login users who run this command.

Example

Allow the **undo** command to be searched for in the upper view.

```
<Huawei> system-view
[Huawei] matched upper-view
[Huawei] interface gigabitethernet1/0/1
[Huawei-GigabitEthernet1/0/1] undo ftp server
Info: Succeeded in closing the FTP server.
[Huawei]
```

Prohibit the **undo** command from being searched for in the upper view.

```
<Huawei> system-view
[Huawei] undo matched upper-view
[Huawei] interface gigabitethernet1/0/1
[Huawei-GigabitEthernet1/0/1] undo ftp server
                              ^
Error: Unrecognized command found at '^' position.
[Huawei-GigabitEthernet1/0/1]
```

Related Topics

3.1.14 quit

3.9.19 peer-public-key end

Function

The **peer-public-key end** command returns to the system view from the public key view and saves the configured public keys.

Format

peer-public-key end

Parameters

None

Views

Public key view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You must save the public key generated on the remote host to the local host, which ensures that the validity check on the remote end is successful. After editing a public key in the public key view, you can run this command to return to the system view.

Prerequisites

Before you run this command, the **rsa peer-public-key** command has been run to enter the RSA public key view or the **ecc peer-public-key** command has been run to enter the ECC public key view.

Example

Return to the system view from the public key view.

```
<Huawei> system-view
[Huawei] rsa peer-public-key rsakey001
[Huawei-rsa-public-key] public-key-code begin
[Huawei-rsa-key-code] 308188
[Huawei-rsa-key-code] 028180
[Huawei-rsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[Huawei-rsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[Huawei-rsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[Huawei-rsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[Huawei-rsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[Huawei-rsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[Huawei-rsa-key-code] 171896FB 1FFC38CD
[Huawei-rsa-key-code] 0203
[Huawei-rsa-key-code] 010001
[Huawei-rsa-key-code] public-key-code end
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-rsa-public-key] peer-public-key end
[Huawei]
```

Related Topics

3.9.20 public-key-code begin

3.9.21 public-key-code end

3.9.27 rsa peer-public-key

3.9.20 public-key-code begin

Function

The **public-key-code begin** command displays the public key editing view.

Format

public-key-code begin

Parameters

None

Views

Public key view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You must save the public key generated on the remote host to the local host, which ensures that the validity check on the remote end is successful. Run the **public-key-code begin** command to display the public key editing view, and enter the key data. The key characters can contain spaces. You can press **Enter** to enter data in another line.

Prerequisite

A key name has been specified by running the **rsa peer-public-key**, or **ecc peer-public-key** command.

Precautions

- The public key must be a hexadecimal character string in the public key encoding format, and generated by the client or server that supports SSH.
- The public keys displayed by running the **display rsa local-key-pair public**, or **display ecc local-key-pair public** command can be used as the key data to enter.

 Copyright © Huawei Technologies Co., Ltd.

- You can successfully edit the public key in a public key pair by entering the public key in the server key pair or client key pair. In SSH application, only the public key in the client key pair can be entered as key data. If you enter the public key in the server key pair, authentication fails during SSH login.

Example

Display the public key editing view and enter the key data.

```
<Huawei> system-view
[Huawei] rsa peer-public-key rsakey001
[Huawei-rsa-public-key] public-key-code begin
[Huawei-rsa-key-code] 308188
[Huawei-rsa-key-code] 028180
[Huawei-rsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[Huawei-rsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[Huawei-rsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[Huawei-rsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[Huawei-rsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[Huawei-rsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[Huawei-rsa-key-code] 171896FB 1FFC38CD
[Huawei-rsa-key-code] 0203
[Huawei-rsa-key-code] 010001
[Huawei-rsa-key-code] public-key-code end
[Huawei-rsa-public-key] peer-public-key end
[Huawei]
```

Related Topics

3.9.7 display rsa local-key-pair public
3.9.19 peer-public-key end
3.9.21 public-key-code end
3.9.27 rsa peer-public-key

3.9.21 public-key-code end

Function

The **public-key-code end** command returns to the public key view from the public key editing view and saves the configured public keys.

Format

public-key-code end

Parameters

None

Views

Public key editing view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After this command is run, the process of editing the public key ends. Before saving the public key, the system will check the validity of the key.

- If there are illegal characters in the public key character string configured by the user, the system will display a relevant error prompt. The public key previously configured by the user is discarded, thus the configuration fails.
- If the public key configured is valid, it is saved in the public key chain table of the client.

Prerequisites

Before you run this command, the **public-key-code begin** command has been run to enter the public key edit view.

Precautions

- Generally, in the public key view, only the **public-key-code end** command can be used to exit. Thus, in this instance the **quit** command cannot be used.
- If the legal key coding is not input, the key cannot be generated after the **public-key-code end** command is used. The system prompts that generating the incorrect key fails.
- If the key is deleted in another window, the system prompts that the key does not exist and returns to the system view directly after you run the **public-key-code end** command.

Example

Exit from the RSA public key editing view and saves the RSA key configuration.

```
<Huawei> system-view
[Huawei] rsa peer-public-key rsakey001
[Huawei-rsa-public-key] public-key-code begin
[Huawei-rsa-key-code] 308188
[Huawei-rsa-key-code] 028180
[Huawei-rsa-key-code] B21315DD 859AD7E4 A6D0D9B8 121F23F0 006BB1BB
[Huawei-rsa-key-code] A443130F 7CDB95D8 4A4AE2F3 D94A73D7 36FDFD5F
[Huawei-rsa-key-code] 411B8B73 3CDD494A 236F35AB 9BBFE19A 7336150B
[Huawei-rsa-key-code] 40A35DE6 2C6A82D7 5C5F2C36 67FBC275 2DF7E4C5
[Huawei-rsa-key-code] 1987178B 8C364D57 DD0AA24A A0C2F87F 474C7931
[Huawei-rsa-key-code] A9F7E8FE E0D5A1B5 092F7112 660BD153 7FB7D5B2
[Huawei-rsa-key-code] 171896FB 1FFC38CD
[Huawei-rsa-key-code] 0203
[Huawei-rsa-key-code] 010001
[Huawei-rsa-key-code] public-key-code end
[Huawei-rsa-public-key] peer-public-key end
[Huawei]
```

Related Topics

3.9.20 public-key-code begin
3.9.27 rsa peer-public-key

3.9.22 redirect binding vpn-instance

Function

The **redirect binding vpn-instance** command associates the redirection function with a VPN instance.

The **undo redirect binding vpn-instance** command cancels the association between the redirection function and a VPN instance.

By default, the redirection function is not associated with any VPN instance.

Format

redirect binding vpn-instance *vpn-instance-name*

undo redirect binding vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, all users on public and private networks can log in to remote devices after the redirection function is enabled. To allow only users in a VPN to log in to a remote device, associate the redirection function with the VPN instance on the device.

Prerequisite

A VPN instance has been created on the router, and the user-side interface of the router has been bound to the VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

The redirection function has been enabled by using the **redirect enable** command.

Precautions

After the redirection function is associated with a VPN instance, only users in the VPN instance can use the redirection function to log in to the device remotely. Users on the public network or other private networks connected to the router are prevented from logging in to the device remotely.

Example

Associate the redirection function with the VPN instance vpna.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] undo shell
[Huawei-ui-tty1] redirect enable
[Huawei-ui-tty1] redirect binding vpn-instance vpna
```

Related Topics

3.9.23 redirect enable

3.9.23 redirect enable

Function

The **redirect enable** command enables the redirection function on a TTY user interface.

The **undo redirect enable** command disables the redirection function on a TTY user interface.

By default, the redirection function is disabled.

Format

redirect [**ssh**] **enable**

undo redirect [**ssh**] **enable**

Parameters

Parameter	Description	Value
ssh	Enables the SSH-based redirection function on a serial port.	-

Views

User interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The redirection function is used in the following scenarios:

- An electricity system or finance system usually uses serial port terminals to collect data. These terminals are connected to asynchronous serial ports of a device. The device receives data flows from the terminals and encapsulates received data into Ethernet frames to transmit the data on an Ethernet network. With the redirection function, users can manage and maintain the terminals remotely.
- Some devices can be managed only through their console ports. In this scenario, connect their console ports to asynchronous serial ports of a device. The device can function as a serial port server to manage these devices.

Prerequisite

- There are reachable routes between the operation terminal and the device that provides the redirection function.
- The 8AS board on the device has registered successfully and asynchronous serial port corresponding to the TTY user interface on the board is in Up state.
- The asynchronous serial port corresponding to the TTY user interface has been configured to work in flow mode using the **async mode flow** command.

Precautions

If the modem function is enabled on a TTY user interface, the redirection function does not take effect.

Example

Enable the redirection function on a TTY user interface.

```
<Huawei> system-view
[Huawei] user-interface tty 9
[Huawei-ui-tty9] undo shell
[Huawei-ui-tty9] redirect enable
```

Related Topics

3.9.24 redirect listen-port

3.9.24 redirect listen-port

Function

The **redirect listen-port** command sets a port number for the redirection function on a TTY user interface.

The **undo redirect listen-port** command restores the default port number for the redirection function.

By default, the port number for the redirection function is 2000 plus the TTY user interface number.

Format

redirect [**ssh**] **listen-port** *port-number*

undo redirect [**ssh**] **listen-port**

Parameters

Parameter	Description	Value
ssh	Enables the SSH-based redirection function on a serial port.	-
port-number	Specifies the port number for the redirection function.	The value is an integer that ranges from 2129 to 3999.

Views

User interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the default port number for the redirection function is used by another service, run the **redirect listen-port** command to set a new port number.

Prerequisite

The redirection function has been enabled using the **redirect enable** command.

Example

Set the port number for the redirection function to 2500.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] undo shell
[Huawei-ui-tty1] redirect enable
[Huawei-ui-tty1] redirect listen-port 2500
```

Related Topics

3.9.23 redirect enable

3.9.25 rsa local-key-pair create

Function

The **rsa local-key-pair create** command generates the local RSA host and server key pairs.

By default, the local RSA host and server key pairs are not configured.

Format

rsa local-key-pair create

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement secure data exchange between the server and client, run this command to generate a local key pair.

Precautions

If the RSA key pair exists, the system prompts you to confirm whether to replace the original key pair.

After you run this command, the system prompts you to enter the number of bits in the host key. The difference between the bits in the server and host key pairs must be at least 128 bits. For a server or host key pair, the minimum length is 512 bits, the maximum length is 2048 bits, and the default length is 2048 bits.

NOTE

Because a longer key pair provides higher security, you are advised to use key pairs of the largest length.

After you run this command, the generated key pair is saved in the device and will not be lost after the device restarts.

This command is not saved in a configuration file.

Example

Generate the local RSA host and server key pairs.

```
<Huawei> system-view
[Huawei] rsa local-key-pair create
The key name will be: Host
RSA keys defined for Host already exist.
Confirm to replace them? (y/n)[n]:y
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is less than 2048,
       It will introduce potential security risks.
Input the bits in the modulus[default = 2048]:2048
Generating keys...
.......................................................................+++
....+++
.....................++++++++
.............++++++++
```

Related Topics

3.9.26 rsa local-key-pair destroy

3.9.26 rsa local-key-pair destroy

Function

The **rsa local-key-pair destroy** command deletes all local RSA host and server key pairs.

Format

rsa local-key-pair destroy

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To delete the local key pair, run **rsa local-key-pair destroy** command. If the host key pair and the service key pair of an SSH server are deleted, run the **rsa local-key-pair create** command to create the new host key pair and service key pair for the SSH server.

After you run this command, verify that all local RSA keys are deleted. This command is not saved in a configuration file.

Prerequisite

The local RSA keys that can be deleted exist.

Example

Delete all RSA server keys.

```
<Huawei> system-view
[Huawei] rsa local-key-pair destroy
% The name for the keys which will be destroyed is Host.
% Confirm to destroy these keys? (y/n)[n]:y
```

Related Topics

3.9.25 rsa local-key-pair create

3.9.27 rsa peer-public-key

Function

The **rsa peer-public-key** command configures an encoding format for an RSA public key and displays the RSA public key view.

The **undo rsa peer-public-key** command deletes a public key.

By default, the encoding format is distinguished encoding rules (DER) for an RSA public key.

Format

rsa peer-public-key *key-name* [**encoding-type** { **der** | **openssh** | **pem** }]

undo rsa peer-public-key *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the rsa public key name.	The value is a string of 1 to 30 case-insensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
encoding-type	Specifies an encoding format for an RSA public key.	-
der	Specifies the DER format for an RSA public key. DER encodes data in hexadecimal format.	-

Parameter	Description	Value
openssh	Specifies the OpenSSH format for an RSA public key. OpenSSH encodes data in base-64 format. OpenSSH is an encoding format based on PEM.	-
pem	Specifies the PEM format for an RSA public key. PEM encodes data in base-64 format.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you use an RSA public key for authentication, you must specify the public key of the corresponding client for an SSH user on the server. When the client logs in to the server, the server uses the specified public key to authenticate the client. You can also save the public key generated on the server to the client. Then the client can be successfully authenticated by the server when it logs in to the server for the first time.

Huawei data communications devices support the DER, OpenSSH and PEM formats for RSA keys. If you use an RSA key in non-DER/OpenSSH/PEM format, use a third-party tool to convert the key into a key in DER, OpenSSH or PEM format.

Because a third-party tool is not released with Huawei system software, RSA usability is unsatisfactory. In addition to DER, RSA keys need to support the privacy-enhanced mail (PEM) and OpenSSH formats to improve RSA usability.

Third-party software, such as PuTTY, OpenSSH, and OpenSSL, can be used to generate RSA keys in different formats. The details are as follows:

- The SecureCRT and PuTTY generate RSA keys in PEM format.
- The OpenSSH generates RSA keys in OpenSSH format.
- The OpenSSL generates RSA keys in DER format.

OpenSSL is an open source software. You can download related documents at http://www.openssl.org/.

After you configure an encoding format for an RSA public key, Huawei data communications device automatically generates an RSA public key in the

configured encoding format and enters the RSA public key view. Then you can run the **public-key-code begin** command and manually copy the RSA public key generated on the peer device to the local device.

Prerequisite

The public key on the remote host has been obtained and recorded.

Follow-up Procedure

After you copy the RSA public key generated on the peer device to the local device, perform the following operations to exit the RSA public key view:

1. Run the **public-key-code end** command to return to the RSA public key view.
2. Run the **peer-public-key end** command to exit the RSA public key view and return to the system view.

Precautions

The public key on the client is randomly generated by the client software.

If an RSA public key has assigned to an SSH client, release the binding relationship between the public key and the SSH client. If you do not release the binding relationship between them, the **undo rsa peer-public-key** command will fail to delete the RSA public key.

The peer public key supports only PKCS#1. Other PKCS versions are not supported.

Example

Configure the encoding format for an RSA public key and displays the RSA public key view.

```
<Huawei> system-view
[Huawei] rsa peer-public-key rsakey001
Enter "RSA public key" view, return system view with "peer-public-key end".
NOTE: The number of the bits of public key must be between 769 and 2048.
[Huawei-rsa-public-key]
```

Related Topics

3.9.8 display rsa peer-public-key

3.9.20 public-key-code begin

3.9.21 public-key-code end

3.9.19 peer-public-key end

3.9.28 send

Function

The **send** command sends messages to all user interfaces.

Format

send { **all** | *ui-number* | *ui-type ui-number1* }

Parameters

Parameter	Description	Value
all	Specifies that the system sends messages to all user interfaces.	-
ui-number	Specifies the absolute number of the user interface.	The minimum value is 0. The maximum value is smaller by 1 than the number of the user interfaces that the system supports.
ui-type	Specifies the type of the user interface.	-
ui-number1	Specifies the relative number of the user interface.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

After you run the **send** command, the system prompts you to enter the message to send. After you confirm to send this message, the user who logs in to the system from the specified user interface can receive this message.

Example

Send a message to the user interface VTY 0.

```
<Huawei> send vty 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:Hello, good morning!^Z
Warning: Send the message? [Y/N]: y
```

After you confirm to send the message, the user who logs in to the Huawei from VTY 0 can receive this message.

```
<Huawei>
Info: Receive a message from VTY2:Hello, good morning!
```

3.9.29 set insecure-protocol enable

Function

The **set insecure-protocol enable** command allows the usage of insecure management protocols HTTP and Telnet.

The **set insecure-protocol disable** command forbids the usage of insecure management protocols HTTP and Telnet.

By default, insecure management protocols HTTP and Telnet can be used except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR2204XE, and AR2204XE-DC. By default, insecure management protocols HTTP and Telnet cannot be used on the AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR2204XE, and AR2204XE-DC.

Format

set insecure-protocol enable

set insecure-protocol disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can log in to a device using HTTPS, Telnet, and STelnet, and HTTP and Telnet belong to insecure management protocols. For security purposes, you can run the **set insecure-protocol disable** command to forbid the usage of insecure management protocols HTTP and Telnet.

Precautions

Before running the **set insecure-protocol disable** command, you need to check whether the Telnet and HTTP service functions are enabled using the **display telnet server status** and **display http server** commands, respectively. If the Telnet and HTTP service functions are enabled, run the **undo telnet server enable** and **undo http server enable** commands to disable the two functions. The **set insecure-protocol disable** command then can be successfully run. If the Telnet and HTTP service functions are disabled, directly run the **set insecure-protocol disable** command to forbid the usage of insecure management protocols HTTP and Telnet.

Example

Forbid the usage of insecure management protocols HTTP and Telnet.

```
<Huawei> system-view
[Huawei] display telnet server status
 TELNET IPV4 server                    :Disable
 TELNET IPV6 server                    :Disable
 TELNET server port                    :23
 Error: insecure-protocol is disabled.
[Huawei] display http server
 HTTP server status            : Disabled       (default: disable)
```

```
 HTTP server port              : 80            (default: 80)
 HTTP timeout interval          : 10            (default: 10 minutes)
 Current online users          : 0
 Maximum users allowed          : 5
 HTTPS server status           : Enabled       (default: disable)
 HTTPS server port             : 443           (default: 443)
 HTTPS server manager port      :
 HTTPS SSL Policy              :
[Huawei] set insecure-protocol disable
```

Related Topics

3.9.45 stelnet

3.9.53 telnet server enable

3.10.7 http server enable

3.9.30 ssh client assign

Function

The **ssh client assign** command specifies the host public key of the SSH server to connect on the SSH client.

The **undo ssh client assign** command cancels the specified host public key of the SSH server to connect on the SSH client.

By default, the host public key of the server to connect is not specified on the client.

Format

ssh client *servername* **assign** { **rsa-key** | **ecc-key** } *keyname*

undo ssh client *servername* **assign** { **rsa-key** | **ecc-key** }

Parameters

Parameter	Description	Value
servername	Specifies the host name or IP address of the SSH server.	The value is a string of 1 to 64 characters without spaces.
rsa-key	Specifies the RSA public key.	-
ecc-key	Specifies the ECC public key.	-
keyname	Specifies the SSH server public key name that has been configured on the SSH client.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the SSH client connects to the SSH server for the first time and the first authentication is not enabled on the SSH client using the **ssh client first-time enable** command, the SSH client rejects the access from unauthorized SSH servers. You need to specify the host public key of the SSH server and the mapping between the key and SSH server on the SSH client. After that, the client will determine whether the server is reliable using the correct public key based on the mapping.

Precautions

The RSA or ECC public key to be assigned to the SSH server must have been configured on the SSH client using the **rsa peer-public-key** or **ecc peer-public-key** command. If the key has not been configured, the verification for the RSA or ECC public key of the SSH server on the SSH client fails.

Example

Assign the RSA public key to the SSH server.

```
<Huawei> system-view
[Huawei] ssh client 10.164.39.120 assign rsa-key sshrsakey01
```

Delete the RSA public key of the SSH server.

```
<Huawei> system-view
[Huawei] undo ssh client 10.164.39.120 assign rsa-key
```

Related Topics

3.9.31 ssh client first-time enable

3.9.31 ssh client first-time enable

Function

The **ssh client first-time enable** command enables the first authentication on the SSH client.

The **undo ssh client first-time enable** command disables the first authentication on the SSH client.

By default, first authentication is disabled on the SSH client.

Format

ssh client first-time enable

undo ssh client first-time enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the SSH client accesses the SSH server for the first time and the public key of the SSH server is not configured on the SSH client, you can enable the first authentication for the SSH client to access the SSH server and save the public key on the SSH client. When the SSH client accesses the SSH server next time, the saved public key is used to authenticate the SSH server.

Precautions

You can run the **ssh client assign** command to pre-assign a public key to the SSH server. In this manner, you can log in to the SSH server successfully at the first time.

Example

Enable the first authentication on the SSH client.

```
<Huawei> system-view
[Huawei] ssh client first-time enable
```

Related Topics

3.9.30 ssh client assign

3.9.32 ssh server authentication-retries

Function

The **ssh server authentication-retries** command sets the maximum number of authentication retries for an SSH connection.

The **undo ssh server authentication-retries** command restores the default maximum number of authentication retries for an SSH connection.

The default maximum number of authentication retries for an SSH connection is 3.

Format

ssh server authentication-retries *times*

undo ssh server authentication-retries

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
times	Specifies the maximum number of authentication retries for an SSH connection.	The value is an integer that ranges from 1 to 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to configure the maximum number of authentication retries for an SSH connection, which prevents server overload due to malicious access.

Precautions

The configured number of retries takes effect upon the next login.

The total number of RSA and password authentication retries on the SSH client cannot exceed the maximum number that is set using this command.

Example

Set the maximum number of times for retrying login authentication to 4.

```
<Huawei> system-view
[Huawei] ssh server authentication-retries 4
```

Related Topics

3.9.9 display ssh server

3.9.33 ssh server compatible-ssh1x enable

Function

The **ssh server compatible-ssh1x enable** command enables the SSH server's compatibility with earlier versions.

The **undo ssh server compatible-ssh1x enable** command disables the SSH server's compatibility with earlier versions.

By default, the server's compatibility with earlier versions is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

ssh server compatible-ssh1x enable

undo ssh server compatible-ssh1x enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH server needs to be configured with backward compatibility for the version negotiation between the client and the server. When a TCP connection is set up between the client and server, the client negotiates with the server on the version of which the client and the server can work together.

The server compares the version of its own with that sent by the client, and determines whether it can work with the client.

- If the protocol version on the client is earlier than 1.3 or later than 2.0, version negotiation fails and the server disconnects from the client.
- If the protocol version on the client is equal to or later than 1.3 and earlier than 1.99, the SSH1.5 server module is invoked and the SSH1.X process is performed when the SSH1.X-compatible mode is configured. When the SSH1.X-incompatible mode is configured, version negotiation fails and the server disconnects from the client.
- If the protocol version on the client is 1.99 or 2.0, the SSH2.0 server module is invoked and the SSH2.0 process is performed.

Precautions

- The configuration takes effect upon the next login.
- SSH2.0 has an extended structure and supports more authentication modes and key exchange methods than SSH1.X. SSH 2.0 can eliminate the security risks that SSH 1.X has. SSH 2.0 is more secure and therefore is recommended.

Example

Enable the SSH server's compatibility with earlier versions.

```
<Huawei> system-view
[Huawei] ssh server compatible-ssh1x enable
```

Related Topics

3.9.9 display ssh server

3.9.34 ssh server cipher

Function

The **ssh server cipher** command configures the encryption algorithm list of the SSH server.

The **undo ssh server cipher** command restores default encryption algorithms of the SSH server.

Earlier versions of V200R010C10:

By default, an SSH server supports the following encryption algorithms: **3des_cbc**, **aes128_cbc**, **aes128_ctr**, **aes192_ctr**, **aes256_ctr**, and **blowfish_cbc**.

V200R010C10 and later versions:

By default, an SSH server supports the following encryption algorithms: **aes128_ctr**, **aes192_ctr**, and **aes256_ctr**.

Format

ssh server cipher { **3des_cbc** | **aes128_cbc** | **aes128_ctr** | **aes192_ctr** | **aes256_ctr** | **blowfish_cbc** | **des_cbc** } *

undo ssh server cipher

Parameters

Parameter	Description	Value
3des_cbc	Adds the 3DES encryption algorithm in CBC encryption mode to the encryption algorithm list of the SSH server.	-
aes128_cbc	Adds the AES128 encryption algorithm in CBC encryption mode to the encryption algorithm list of the SSH server.	-
aes128_ctr	Adds the AES128 encryption algorithm in CTR encryption mode to the encryption algorithm list of the SSH server.	-
aes192_ctr	Adds the AES192 encryption algorithm in CTR encryption mode to the encryption algorithm list of the SSH server.	-
aes256_ctr	Adds the AES256 encryption algorithm in CTR encryption mode to the encryption algorithm list of the SSH server.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
blowfish_cbc	Adds the BLOWFISH encryption algorithm in CBC encryption mode to the encryption algorithm list of the SSH server.	-
des_cbc	Adds the DES encryption algorithm in CBC encryption mode to the encryption algorithm list of the SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The server and client negotiate the algorithm for encrypting packets transmitted between them. You can run the **ssh server cipher** command to configure the encryption algorithm list of the SSH server. The server compares the encryption algorithm list sent from the client with its own encryption algorithm list, and selects the first matched encryption algorithm for encrypting transmitted packets. If the encryption algorithm lists of the server and client have no common encryption algorithm, the encryption algorithm negotiation fails.

For example, run the **ssh server cipher** { **aes256_ctr** | **aes192_ctr** | **aes128_ctr** } * command to add the high-security **aes256_ctr**, **aes192_ctr**, and **aes128_ctr** encryption algorithms to the encryption algorithm list of the SSH server, improving device security.

Precautions

You are advised not to add the following encryption algorithms to the encryption algorithm list of the SSH server because they provide low security: **3des_cbc**, **aes128_cbc**, **blowfish_cbc**, and **des_cbc**.

Example

Add **aes256_ctr** to the encryption algorithm list of the SSH server.

```
<Huawei> system-view
[Huawei] ssh server cipher aes256_ctr
```

3.9.35 ssh server hmac

Function

The **ssh server hmac** command configures the check algorithm list of the SSH server.

The **undo ssh server hmac** command restores default check algorithms of the SSH server.

Earlier versions of V200R010C10:

By default, an SSH server supports all the check algorithms.

V200R010C10 and later versions:

By default, an SSH server supports the **sha2_256** encryption algorithms only.

Format

ssh server hmac { **md5** | **md5_96** | **sha1** | **sha1_96** | **sha2_256** | **sha2_256_96** } *

undo ssh server hmac

Parameters

Parameter	Description	Value
md5	Adds the MD5 check algorithm to the HMAC check algorithm list of the SSH server.	-
md5_96	Adds the MD5_96 check algorithm to the HMAC check algorithm list of the SSH server.	-
sha1	Adds the SHA1 check algorithm to the HMAC check algorithm list of the SSH server.	-
sha1_96	Adds the SHA1_96 check algorithm to the HMAC check algorithm list of the SSH server.	-
sha2_256	Adds the SHA2_256 check algorithm to the HMAC check algorithm list of the SSH server.	-
sha2_256_96	Adds the SHA2_256_96 check algorithm to the HMAC check algorithm list of the SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The server and client negotiate the algorithm for checking packets transmitted between them. You can run the **ssh server hmac** command to configure the check

algorithm list of the SSH server. The server compares the check algorithm list sent from the client with its own check algorithm list, and selects the first matched check algorithm for checking transmitted packets. If the check algorithm lists of the server and client have no common check algorithm, the check algorithm negotiation fails.

For example, run the **ssh server hmac sha2_256** command to add the high-security **sha2_256** check algorithm to the HMAC check algorithm list of the SSH server, improving device security.

Precautions

The check algorithms are arranged in descending order of priority as follows: **sha2_256**, **sha2_256_96**, **sha1**, **sha1_96**, **md5**, and **md5_96**.

You are advised not to add the following HMAC check algorithms to the HMAC check algorithm list of the SSH server because they provide low security: **sha2_256_96**, **sha1**, **sha1_96**, **md5**, and **md5_96**.

Example

Add **sha2_256** to the check algorithm list of the SSH server.

```
<Huawei> system-view
[Huawei] ssh server hmac sha2_256
```

3.9.36 ssh server key-exchange

Function

The **ssh server key-exchange** command configures a key exchange algorithm list for an SSH server.

The **undo ssh server key-exchange** command restores the default setting.

Earlier versions of V200R010C10:

By default, an SSH server supports all key exchange algorithms.

V200R010C10 and later versions:

By default, an SSH server supports the following key exchange algorithms: **dh_group_exchange_sha1** and **dh_group14_sha1**.

Format

ssh server key-exchange { **dh_group_exchange_sha1** | **dh_group14_sha1** | **dh_group1_sha1** } *

undo ssh server key-exchange

Parameters

Parameter	Description	Value
dh_group_exchange_sha1	Adds the Diffie-hellman-group-exchange-sha1 algorithm to the key exchange algorithm list of the SSH server.	-
dh_group14_sha1	Adds the Diffie-hellman-group14-sha1 algorithm to the key exchange algorithm list of the SSH server.	-
dh_group1_sha1	Adds the Diffie-hellman-group1-sha1 algorithm to the key exchange algorithm list of the SSH server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

An SSH user and a client need to negotiate a key exchange algorithm for the packets exchanged between them. You can run the **ssh server key-exchange** command to configure a key exchange algorithm list for the SSH server. After the server receives a packet from the client, the server matches the key exchange algorithm list of the client against its local list and selects the first matched key exchange algorithm. If no key exchange algorithm is matched, the negotiation fails.

Precautions

The key exchange algorithms are listed as follows in descending order of security levels: **dh_group_exchange_sha1**, **dh_group14_sha1**, and **dh_group1_sha1**. The **dh_group_exchange_sha1** algorithm is recommended.

You are advised not to add the **dh_group1_sha1** algorithm to the key exchange algorithm list of the SSH server because it provides low security.

Example

Configure a key exchange algorithm list containing **dh_group_exchange_sha1** for the SSH server.

```
<Huawei> system-view
[Huawei] ssh server key-exchange dh_group_exchange_sha1
```

3.9.37 ssh server permit interface

Function

The **ssh server permit interface** command specifies physical interfaces on the SSH server to which clients can connect.

The **undo ssh permit interface** command restores the default physical interfaces on the SSH server to which clients can connect.

By default, clients can connect to all the physical interfaces on the SSH server.

Format

ssh server permit interface { *interface-type interface-number* } &<1-5>

undo ssh server permit interface

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type*: specifies the interface type. *interface-number*: specifies the interface number. *interface-number* and *interface-type* specify an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent a client from connecting to the SSH server through an unauthorized physical interface, you can run the **ssh server permit interface** command to specify physical interfaces on the SSH server to which the client can connect.

Precautions

- By default, the client can connect to all the physical interfaces on the SSH server. When you run this command to specify one physical interface on the SSH server, the client cannot connect to the other physical interfaces on the SSH server.
- You can specify a maximum of five interfaces each time you run the **ssh server permit interface** command. The latest configuration overrides the previous one. For example, before you run the command, clients can connect

to three physical interfaces GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 on the SSH server. After you run the command to specify the interface GigabitEthernet 1/0/0, clients can only connect to the interface GigabitEthernet 1/0/0.

Example

Specify physical interfaces on the SSH server to which clients can connect.

```
<Huawei> system-view
[Huawei] ssh server permit interface gigabitethernet 1/0/0 gigabitethernet 2/0/0
Info: Succeeded in setting ssh permit interface.
```

Restore the default physical interfaces on the SSH server to which clients can connect.

```
<Huawei> system-view
[Huawei] undo ssh server permit interface
```

3.9.38 ssh server port

Function

The **ssh server port** command changes the listening port number of the SSH server.

The **undo ssh server port** command restores the default listening port number of the SSH server.

The default listening port number of the SSH server is 22.

Format

ssh server port *port-number*

undo ssh server port

Parameters

Parameter	Description	Value
port-number	Specifies the listening port number of the SSH server.	The value is 22 or an integer ranging from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Configure the listening port number of the SSH server to prevent from malicious access to the SSH service standard port and ensure security.

Precautions

The SSH client can log in successfully with no port specified only when the server is listening on port 22. If the server is listening on another port, the port number must be specified upon login.

Before changing the current port number, disconnect all devices from the port. After the port number is changed, the server starts to listen on the new port.

Example

Set the listening port number of the SSH server is 1025.

```
<Huawei> system-view
[Huawei] ssh server port 1025
```

Related Topics

3.9.9 display ssh server

3.11.62 sftp

3.9.45 stelnet

3.9.39 ssh server rekey-interval

Function

The **ssh server rekey-interval** command sets the interval for updating the SSH server key pair.

The **undo ssh server rekey-interval** command restores the default interval for updating the SSH server key pair.

The default interval for updating the SSH server key pair is 0, indicating that the key pair is never updated.

Format

ssh server rekey-interval *hours*

undo ssh server rekey-interval

Parameters

Parameter	Description	Value
hours	Specifies the interval for updating the server key pair.	The value is an integer that ranges from 1 to 24, in hours.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the server key pair is not updated for a long time, the key is easy to decrypt and the server is insecure. After the interval for updating the SSH server key pair is set using this command, the system will automatically update the key pair at intervals.

Precautions

If the client is connected to the server, the server public key on the client is not updated immediately. This key is updated only when the client is reconnected to the server.

Example

Set the interval for updating the SSH server key pair to 2 hours.

```
<Huawei> system-view
[Huawei] ssh server rekey-interval 2
```

Related Topics

3.9.9 display ssh server

3.9.40 ssh server timeout

Function

The **ssh server timeout** command sets the timeout interval for SSH connection authentication.

The **undo ssh server timeout** restores the default timeout interval for SSH connection authentication.

The default timeout interval for SSH connection authentication is 60 seconds.

Format

ssh server timeout *seconds*

undo ssh server timeout

Parameters

Parameter	Description	Value
seconds	Specifies the timeout interval for SSH connection authentication.	The value is an integer ranging from 60 to 120, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you have not logged in successfully at the timeout interval for SSH connection authentication, the current connection is terminated to ensure security. You can run the **display ssh server** command to query the current timeout interval.

Precautions

The setting for the timeout interval takes effect upon next login.

Example

Set the SSH connection authentication timeout interval to 90 seconds.

```
<Huawei> system-view
[Huawei] ssh server timeout 90
```

Related Topics

3.9.9 display ssh server

3.9.41 ssh server-source

Function

The **ssh server-source** command specifies a source IP address for an SSH server.

The **undo ssh server-source** command deletes the source IP address of an SSH server.

By default, the source IP address of an SSH server is not specified.

Format

ssh server-source { **-a** [**ipv6**] *source-ip-address* | **-i** [**ipv6**] *interface-type interface-number* }

undo ssh [**ipv6**] **server-source**

Parameters

Parameter	Description	Value
ipv6	Configures the SSH server to support an IPv6 source address.	-

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for the SSH server. The loopback IP address is recommended.	-
-i *interface-type interface-number*	Specifies the loopback interface of the SSH server as the source interface. If no loopback interface is configured or no IP address is configured for the source interface, the command fails to be executed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the SSH server uses the source IP address specified by routes to send and receive packets. The source IP address must be configured for an interface with stable performance, such as the loopback interface. Using the loopback interface as the source IP address simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Precautions

- After the source IP address is specified for the SSH server, you must use the specified IP address to log in to the SSH server.
- If the configured source IP address does not exist on the SSH server, configure this IP address on the device and then restart the SSH service. Then you can log in to the device.
- If the SSH service has been enabled, the SSH service restarts after the **ssh server-source** command is executed.
- If the specified source interface has been bound to a VPN instance, the SSH server is automatically bound to the same VPN instance.

Example

Set the source IP address of the SSH server to **LoopBack0**.

```
<Huawei> system-view
[Huawei] ssh server-source -i loopback 0
Warning: To make the server source configuration take effect, the ssh will be restarted. Continue? (y/n):y
Info: Succeeded in closing the STELNET server.
Info: Succeeded in setting the source interface of the ssh server to LoopBack0
Info: Succeeded in starting the STELNET server.
```

Related Topics

3.9.45 stelnet
3.9.46 stelnet server enable
3.9.38 ssh server port

3.9.42 ssh user assign

Function

The **ssh user assign** command assigns an existing public key to a user.

The **undo ssh user assign** command deletes the mapping between the user and public key.

By default, no public key is assigned to a user.

Format

ssh user *user-name* **assign** { **rsa-key** | **ecc-key** } *key-name*

undo ssh user *user-name* **assign** { **rsa-key** | **ecc-key** }

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces.
rsa-key	Specifies the RSA public key.	-
ecc-key	Specifies the ECC public key.	-
key-name	Specifies the client public key name.	The name is a string of 1 to 30 case-insensitive characters without a blank space.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSH client needs to log in to the SSH server in RSA or ECC mode, run this command to assign a public key to the client. If the client has been assigned keys, the latest assigned key takes effect.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The newly configured public key takes effect upon next login.

If the user named *user-name* to whom a public key is assigned does not exist, the system automatically creates an SSH user named *user-name* and performs the configured authentication for the SSH user.

Example

Assign key1 to a user named John.

```
<Huawei> system-view
[Huawei] ssh user john assign rsa-key key1
```

Related Topics

3.9.10 display ssh user-information

3.9.43 ssh user authentication-type

Function

The **ssh user authentication-type** command configures the authentication mode for an SSH user.

The **undo ssh user authentication-type** command restores the default authentication mode for an SSH user.

By default, the password authentication mode is configured for an SSH user.

Format

ssh user [*user-name*] **authentication-type** { **password** | **rsa** | **password-rsa** | **ecc** | **password-ecc** | **all** }

undo ssh user *user-name* **authentication-type**

Parameters

Parameter	Description	Value
user-name	Specifies the SSH user name.	The value is a string of 1 to 64 case-insensitive characters without spaces.
password	Specifies the password authentication mode.	-
rsa	Specifies the RSA authentication mode.	-
password-rsa	Specifies the password and RSA authentication mode.	-
ecc	Specifies the ECC authentication mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password-ecc	Specifies the password and ECC authentication mode.	-
all	Specifies the password, RSA or ECC authentication mode. **NOTE** In all authentication mode, the user priority depends on the authentication mode selected. ● If password authentication is selected, the user priority is the same as that specified on the AAA module. ● If RSA/ECC authentication is selected, the user priority depends on the priority of the VTY window used during user access. If all authentication is selected and an AAA user with the same name as the SSH user exists, user priorities may be different in password authentication and RSA/ECC authentication modes. Set relevant parameters as needed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you configure the authentication mode for an SSH user, the system automatically creates an SSH user named *user-name* if the *user-name* user does not exist.

Table 3-33 describes the usage scenarios for different authentication modes.

Table 3-33 Usage scenarios for authentication modes

Authentication Mode	Usage Scenario
RSA	It is a public key encryption architecture and an asymmetric encryption algorithm. Based on the problem of factoring large numbers, RSA is mainly used to transmit the keys of the symmetric encryption algorithm, which can improve encryption efficiency and simplify key management. The server checks whether the SSH user, public key, and digital user signature are valid. If all of them are valid, the user is permitted to access the server. If any of them is invalid, the authentication fails and the user is denied to access the server.
ECC	Like RSA authentication, the server first checks the validity of the SSH user and whether the public key and the numeric signature are valid. If all of them are consistent with those configured on the server, user authentication succeeds. If any of the three cannot pass authentication, the user access is denied. Compared with the RSA algorithm, the ECC authentication has the following advantages: ● Provides the same security with shorter key length. ● Features a shorter computing process and higher processing speed. ● Requires less storage space. ● Requires lower bandwidth.

 Copyright © Huawei Technologies Co., Ltd.

Authentication Mode	Usage Scenario
password	On the server, the AAA module assigns each authorized user a password for login. The server has the mapping between user names and passwords. When a user requests to access the server, the server authenticates the user name and password. If either of them fails to be authenticated, the access request of the user is denied. The account information of users who are configured with the password authentication mode can be configured on devices or remote authentication servers (for example, RADIUS servers).
password-rsa, or password-ecc	The SSH server authenticates a client by checking both the public key and password. The client can be authenticated only when both the public key and password meet the requirement.
all	In this authentication mode, the SSH server authenticates a client by checking the public key or password. The client can be authenticated when either the public key or password meets the requirement.

Precautions

A new SSH user cannot log in to the SSH server unless being configured with an authentication mode. The newly configured authentication mode takes effect upon next login.

Example

Configure the password authentication mode for an SSH user John.

```
<Huawei> system-view
[Huawei] ssh user john authentication-type password
```

Related Topics

3.9.10 display ssh user-information

3.9.44 ssh user default-authentication-type

Function

The **ssh user default-authentication-type** command sets the default authentication mode for SSH users.

By default, the default authentication mode for SSH users is password authentication except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR2204XE, and AR2204XE-DC. By default, the default authentication mode for SSH users of the AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR2204XE, and AR2204XE-DC is RSA authentication.

Format

ssh user default-authentication-type { **password** | **rsa** }

Parameters

Parameter	Description	Value
password	Sets the default authentication mode for SSH users to password authentication.	-
rsa	Sets the default authentication mode for SSH users to RSA authentication.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To change the default authentication mode for SSH users, run this command.

Example

Set the default authentication mode for SSH users to RSA authentication.

```
<Huawei> system-view
[Huawei] ssh user default-authentication-type rsa
```

3.9.45 stelnet

Function

The **stelnet** command enables you to use the STelnet protocol to log in to another device from the current device.

Format

IPv4 address

stelnet [**-a** *source-address*] *host-ip* [*port-number*] [[**-vpn-instance** *vpn-instance-name*] | [**identity-key** { **rsa** | **ecc** }] | [**user-identity-key** { **rsa** | **ecc** }] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_stoc_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | **sha2_256** | **sha2_256_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | **sha2_256** | **sha2_256_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

IPv6 address

stelnet ipv6 [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*] [[**-vpn6-instance** *vpn-instance-name*] | [**identity-key** { **rsa** | **ecc** }] | [**user-identity-key** { **rsa** | **ecc** }] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_stoc_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | sha2_256 | sha2_256_96 }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | **sha2_256** | **sha2_256_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

Parameters

Parameter	Description	Value
ipv6	Specifies an IPv6 address.	-
-a *source-address*	Specifies the STelnet source IP address.	-
host-ip	Specifies the IP address or host name of the remote IPv4 STelnet server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
host-ipv6	Specifies the IPv6 address or host name of the remote IPv6 STelnet server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
-oi *interface-type interface-number*	Specifies the outbound interface on the local device.	If the IPv6 address of the remote host is linked to a local address, the outbound interface must be specified.

Parameter	Description	Value
port-number	Specifies the port number that the SSH server is listening on.	The value is an integer that ranges from 1 to 65535. The default value 22 is the standard port number.
identity-key	Specifies the public key for server authentication.	The public key algorithm include RSA and ECC.
user-identity-key	Specifies the public key algorithm for the client authentication.	The public key algorithm include RSA and ECC. **NOTE** If the **user-identity-key** parameter is not used, RSA authentication is used by default. You can specify ECC authentication using the **user-identity-key** parameter.
prefer_kex	Specifies the preferred key exchange algorithm. The dh_group1 and dh_exchange_group algorithms are supported currently.	The default key exchange algorithm is dh_group1.
prefer_ctos_cipher	Specifies the preferred encryption algorithm from the client to the server.	Encryption algorithms **3des**, **aes128**, **aes128-ctr**, **aes192-ctr**, and **aes256-ctr** are supported currently. The default algorithm is aes128.
prefer_stoc_cipher	Specifies the preferred encryption algorithm from the server to the client. Encryption algorithms **3des**, **aes128**, **aes128-ctr**, **aes192-ctr**, and **aes256-ctr** are supported currently.	The default algorithm is aes128.
prefer_ctos_hmac	Specifies the preferred HMAC algorithm from the client to the server. The sha2_256, sha2_256_96, sha1, sha1_96, md5, and md5_96 algorithms are supported currently.	The default algorithm is sha1_96.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
prefer_stoc_hmac	Specifies the preferred HMAC algorithm from the server to the client. The sha2_256, sha2_256_96, sha1, sha1_96, md5, and md5_96 algorithms are supported currently.	The default algorithm is sha1_96.
-vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the IPv4 server belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
-vpn6-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the IPv6 server belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
-ki *aliveinterval*	Specifies the interval for sending keepalive packets when no packet is received.	The value is an integer that ranges from 1 to 3600, in seconds.
-kc *alivecountmax*	Specifies the number of times for no reply of keepalive packets.	The value is an integer that ranges from 3 to 10. The default value is 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Logins through Telnet bring security risks because Telnet does not provide any authentication mechanism and data is transmitted using TCP in plain text. Compared with Telnet, SSH guarantees secure file transfer on a traditional insecure network by authenticating clients and encrypting data in bidirectional mode. The SSH protocol supports STelnet. You can run this command to use STelnet to log in to another device from the current device.

STelnet is a secure Telnet service. SSH users can use the STelnet service in the same way as the Telnet service.

When a fault occurs in the connection between the client and server, the client needs to detect the fault in real time and proactively release the connection. You need to set the interval for sending keepalive packets and the maximum number of times on the client that logs in to the server through STelnet.

- Interval for sending keepalive packets: If a client does not receive any packet within the specified interval, the client sends a keepalive packet to the server.
- Maximum number of times the server has no response: If the number of times that the server does not respond exceeds the specified value, the client proactively releases the connection.

Precautions

- Enable the STelnet service on the SSH server by **stelnet server enable** command, before connecting the SSH server by using the STelnet command.
- The SSH client can log in to the SSH server with no port specified only when the server is listening on port 22. If the server is listening on another port, the port number must be specified upon login.
- 3DES, MD5, MD5_96, SHA1, and SHA1_96 encryption algorithm cannot ensure security. sha2_256, sha2_256_96, AES128, AES128-CTR, AES192-CTR or AES256-CTR encryption algorithm is recommended.

Example

Set keepalive parameters when the client logs in to the server through STelnet.

```
<Huawei> system-view
[Huawei] stelnet 10.164.39.209 -ki 10 -kc 4
```

Remotely connect to the STelnet server that uses an IPv6 address.

```
<Huawei> system-view
[Huawei] stelnet ipv6 fc00:2001:db8::1 prefer_ctos_cipher aes128
```

Related Topics

3.9.46 stelnet server enable

3.9.38 ssh server port

3.9.46 stelnet server enable

Function

The **stelnet server enable** command enables the STelnet service on the SSH server.

The **undo stelnet server enable** command disables the STelnet service on the SSH server.

By default, the STelnet service is disabled on the SSH server.

Format

stelnet server enable

undo stelnet server enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To connect a client to the SSH server through STelnet, you must enable the STelnet service on the SSH server.

Precautions

After you disable the STelnet service on the SSH server, all clients that have logged in through STelnet are disconnected.

Example

Enable the STelnet service.

```
<Huawei> system-view
[Huawei] stelnet server enable
```

Related Topics

3.9.45 stelnet

3.9.47 super

Function

The **super** command switches a user from the current level to a specified level.

Format

super [*level*]

Parameters

Parameter	Description	Value
level	Specifies the target user level.	The value is an integer that ranges from 0 to 15. By default, a user is switched to level 3.

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Users are assigned one of 16 levels, and these levels correspond to command levels. After logging in to the device, users can use only the commands whose levels are equal to or lower than their user levels.

When a user is switched from a lower level to a higher level, the device requires the user to enter the authentication password for the higher user level to authenticate the user identity, preventing unauthorized users from logging in to the device. You can run the **super password** command to set an authentication password used to switch a user from a lower level to a higher level.

If the entered target user level is lower than or equal to the current user level, the system directly sets the entered user level as the target user level, and displays a message. If the target level is higher than the current user level, the system asks the user to enter the authentication password.

The password entered by a user is not displayed on the screen. If the user enters the correct password within three times, the system switches the user to the higher user level; otherwise, the user level remains unchanged.

Precautions

- The configured target level takes effect only for the current user. The user level restores to the original level the next time the user logs in.
- AR3200 series routers do not support this command in active/standby switchover scenarios.
- The password is a string of 8 to 16 characters.
- The password must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

  Special characters include ` ~ ! @ # $ % ^ & * ( ) - _ = + \ | [{ }] ; : ' " , < . > / ? spaces.
- The password must be the same as the password set using the **super password** command.

Example

Switch a user to level 10.

```
<Huawei> super 10
  Password:
  Now user privilege is level 10, and only those commands whose level is
  equal to or less than this level can be used.
  Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

Related Topics

3.9.48 super password

3.9.48 super password

Function

The **super password** command sets an authentication password used to switch a user from a lower level to a higher level.

The **undo super password** command deletes an authentication password used to switch a user from a lower level to a higher level.

By default, no switching password is configured. You must set the authentication password before switching a user from a lower level to a higher level; otherwise, the switching fails.

Format

super password [**level** *user-level*] **cipher**

undo super password [**level** *user-level*]

Parameters

Parameter	Description	Value
level *user-level*	Specifies the target user level.	The value is an integer that ranges from 1 to 15. The target user level must be lower than or equal to the current user level. By default, the authentication password is set to switch a user to level 3.
cipher	Indicates that the configured password is displayed in cipher text.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If rights are reconfigured, you need to run the **super** command to switch a user from a lower level to a higher level. When a user is switched from a lower level to a higher level, the device authenticates the user identity to prevent unauthorized

 Copyright © Huawei Technologies Co., Ltd.

users from logging in to the device. Users at a higher level can run the **super password** command to set an authentication password used to switch a user from a lower level to a higher level, so that the device can authenticate the user identity.

Precautions

- AR3200 series routers do not support this command in active/standby switchover scenarios.
- The target user level must be lower than or equal to the current user level.
- The entered authentication password must meet the following requirements:
  - It is a string of 8 to 16 characters entered only in plain text.
  - It must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

    Special characters include ` ~ ! @ # $ % ^ & * ( ) - _ = + \ | [{ }] ; : ' " , < . > / ? spaces.
- The password entered in interactive mode is not displayed on the screen.
- When setting the password in interactive mode, you can press **CTRL+C** to cancel the password setting.
- If this command is run, passwords entered by users will be saved in cipher text in the configuration file. Therefore, a configured password cannot be retrieved from the system. Keep the password safe.

Example

Set an authentication password used to switch a user from a lower level to level 5.

```
<Huawei> system-view
[Huawei] super password level 5 cipher
Enter Password(<8-16>):
Confirm password:
```

Related Topics

3.9.47 super

3.9.49 telnet

Function

The **telnet** command enables you to use the Telnet protocol to log in to another device from the current device.

Format

Log in to another device through Telnet based on IPv4.

telnet [**vpn-instance** *vpn-instance-name*] [**-a** *source-ip-address*] *host-ip* [*port-number*]

Log in to another device through Telnet based on IPv6.

telnet ipv6 [**-a** *source-ip-address*] [**vpn6-instance** *vpn6-instance-name*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN4 instance name of the device to log in through Telnet.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
-a *source-ip-address*	By specifying a source IP address, you can use this address to communicate with the server for high network security. If no source address is specified, the system will use the IP address of the local outbound interface to initiate a Telnet connection.	-
vpn6-instance *vpn6-instance-name*	Specifies the VPN6 instance name of the device to log in through Telnet.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
host-ip	Specifies the IPv4 address or host name of the remote device.	The value is a string of 1 to 255 case-insensitive characters without spaces.
host-ipv6	Specifies the IPv6 address or host name of the remote device.	The value is a string of 1 to 255 case-insensitive characters without spaces.
-oi *interface-type interface-number*	Specifies the outbound interface on the local device.	If the IPv6 address of the remote host is linked to a local address, the outbound interface must be specified.
port-number	Specifies the number of the TCP port that is used by the remote device to provide the Telnet service.	The value is an integer that ranges from 1 to 65535. The default value is 23.

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If one or multiple devices on the network need to be configured and managed, you do not need to connect each device to your terminal for local maintenance. If you have learned the IP address of the device, you can run this command to log in to the device from your terminal for remote device configuration. By doing this, you can use one terminal to maintain multiple devices on the network.

You can press **Ctrl_]** to terminate an active connection between the local and remote devices.

Precautions

- Before you run the **telnet** command to connect to the Telnet server, the Telnet client and server must be able to communicate through Layer 3 and the Telnet service must be enabled on the Telnet server.
- Logins through Telnet bring security risks because Telnet does not provide any authentication mechanism and data is transmitted using TCP in plain text. The STelnet mode is recommended for the network that has the high security requirement.

Example

Connect to a remote device through Telnet.

```
<Huawei> telnet 192.168.1.6
```

Use the IPv6 address to connect to a remote device through Telnet.

```
<Huawei> telnet ipv6 fc00:0:0:11::158
```

Related Topics

3.9.53 telnet server enable

3.9.54 telnet server port

3.9.50 telnet client-source

Function

The **telnet client-source** command specifies the source IP address and interface for a Telnet client.

The **undo telnet client-source** command restores the default settings.

The default source IP address of the Telnet client is 0.0.0.0.

Format

telnet client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo telnet client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the IPv4 address of the local router.	-
-i *interface-type interface-number*	Specifies the outbound interface of the local router.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the source IP address and interface are not specified in the **telnet** command, use the default settings specified by **telnet client-source**. If the source IP address and interface are specified in the **telnet** command, use the specified settings. Check the current Telnet connection on the server. The IP address displayed is the specified source IP address or the primary IP address of the specified interface.

Precautions

If the specified source interface has been bound to a VPN instance, the client is automatically bound to the same VPN instance.

Example

Set the source IP address of the Telnet client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] telnet client-source -a 10.1.1.1
```

Related Topics

3.9.49 telnet

3.9.51 telnet server-source

Function

The **telnet server-source** command specifies a source IP address for a Telnet server.

The **undo telnet server-source** command deletes the source IP address of a Telnet server.

By default, the source interface of a Telnet server is not specified.

 Copyright © Huawei Technologies Co., Ltd.

Format

telnet server-source { **-a** [**ipv6**] *source-ip-address* | **-i** [**ipv6**] *interface-type interface-number* }

undo telnet [**ipv6**] **server-source**

Parameters

Parameter	Description	Value
ipv6	Configures the Telnet server to support an IPv6 source address.	-
-a *source-ip-address*	Specifies the source IP address for the Telnet server. The loopback IP address is recommended.	-
-i *interface-type interface-number*	Specifies the loopback interface of the Telnet server as the source interface. If no loopback interface is configured or no IP address is configured for the source interface, the command fails to be executed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the Telnet server uses the source IP address specified by routes to send packets. The source IP address must be configured for an interface with stable performance, such as the loopback interface. Using the loopback interface as the source IP address simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Precautions

- After the source IP address is specified for the Telnet server, you must use the specified IP address to log in to the Telnet server.
- If the Telnet service has been enabled, the Telnet service restarts after the **telnet server-source** command is executed.
- If the specified source interface has been bound to a VPN instance, the server is automatically bound to the same VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the source IP address of the Telnet server to **LoopBack0**.

```
<Huawei> system-view
[Huawei] telnet server-source -i loopback 0
Warning: To make the server source configuration take effect, the telnet server will be restarted. Continue?
[Y/N]: y
Info: Succeeded in setting the source interface of the telnet server to LoopBack0
Info: Telnet is insecure, recommended to use stelnet with encryption features.
```

Related Topics

3.9.49 telnet
3.9.53 telnet server enable
3.9.54 telnet server port

3.9.52 telnet server permit interface

Function

The **telnet server permit interface** command specifies physical interfaces on the Telnet server to which clients can connect.

The **undo telnet permit interface** command restores the default physical interfaces on the Telnet server to which clients can connect.

By default, clients can connect to all the physical interfaces on the Telnet server.

Format

telnet server permit interface { *interface-type interface-number* } &<1-5>

undo telnet server permit interface

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type*: specifies the interface type. *interface-number*: specifies the interface number. *interface-number* and *interface-type* specify an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent a client from connecting to the Telnet server through an unauthorized physical interface, you can run the **telnet server permit interface** command to specify physical interfaces on the Telnet server to which the client can connect.

Precautions

- By default, the client can connect to all the physical interfaces on the Telnet server. When you run this command to specify one physical interface on the Telnet server, the client cannot connect to the other physical interfaces on the Telnet server.
- You can specify a maximum of five interfaces each time you run the **telnet server permit interface** command. The latest configuration overrides the previous one. For example, before you run the command, clients can connect to three physical interfaces GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 on the Telnet server. After you run the command to specify the interface GigabitEthernet 1/0/0, clients can only connect to the interface GigabitEthernet 1/0/0.

Example

Specify physical interfaces on the Telnet server to which clients can connect.

```
<Huawei> system-view
[Huawei] telnet server permit interface gigabitethernet 1/0/0 gigabitethernet 2/0/0
Info: Succeeded in setting telnet permit interface.
```

Restore the default physical interfaces on the Telnet server to which clients can connect.

```
<Huawei> system-view
[Huawei] undo telnet server permit interface
```

3.9.53 telnet server enable

Function

The **telnet server enable** command enables the Telnet server.

The **undo telnet server enable** command disables the Telnet server.

By default, the Telnet server is disabled.

Format

telnet [**ipv6**] **server enable**

undo telnet [**ipv6**] **server enable**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6	Specifies a Telnet IPv6 server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run this command to enable and disable the Telnet server. A Telnet server can be connected only when it is enabled.

When the **undo telnet server enable** command is executed to disable the Telnet server, an online Telnet user goes offline because the Telnet service is disabled.

When a Telnet server stops, you can log in to the device only through the console port or SSH.

NOTICE

The Telnet protocol poses a security risk, and therefore the STelnet V2 mode is recommended.

Example

Enable a Telnet server.

```
<Huawei> system-view
[Huawei] telnet server enable
```

Disable a Telnet server.

```
<Huawei> system-view
[Huawei] undo telnet server enable
```

Enable an IPv6 Telnet server.

```
<Huawei> system-view
[Huawei] telnet ipv6 server enable
```

3.9.54 telnet server port

Function

The **telnet server port** command configures the listening port number of a Telnet server.

The default listening port of a Telnet server is 23.

 Copyright © Huawei Technologies Co., Ltd.

Format

telnet server port *port-number*

Parameters

Parameter	Description	Value
port-number	Specifies the listening port number of a Telnet server.	The value is an integer that is 23 or ranges from 1025 to 1999 or ranges from 5001 to 55535. The default value 23 is the standard Telnet server port number. **NOTE** If the port number of the Telnet server is set in versions earlier than V200R009C00 and the port number is in the range from 2000 to 5000, the original port number can still be used if system is upgraded to V200R009C00.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To protect the Telnet standard port against attacks and ensure network security, configure the listening port number of the Telnet server.

Precautions

A Telnet client can log in to the server with no port specified only when the server is listening on port 23. If the server is listening on another port, the port number must be specified upon login.

Before changing the current port number, disconnect all devices from the port. After the port number is changed, the server starts to listen on the new port.

Example

Configure the listening port number to 1026.

```
<Huawei> system-view
[Huawei] telnet server port 1026
```

3.9.55 transparent-mode enable

Function

The **transparent-mode enable** command enables the transparent transmission mode for redirection on a serial port.

The **undo transparent-mode enable** command disables the transparent transmission mode for redirection on a serial port.

By default, the transparent transmission mode for redirection on a serial port is disabled.

Format

transparent-mode enable

undo transparent-mode enable

Parameters

None

Views

TTY user interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device checks data redirected by a serial port and discards unidentifiable data, damaging the original data. You can run the **transparent-mode enable** command to ensure the original data integrity. The device will transparently transmit data without checking it.

Prerequisites

The redirection function has been enabled using the **redirect enable** command.

Example

Enable the transparent transmission mode for redirection on a serial port.

```
<Huawei> system-view
[Huawei] user-interface tty 44
[Huawei-ui-tty44] redirect enable
[Huawei-ui-tty44] transparent-mode enable
```

Related Topics

3.9.23 redirect enable

3.10 HTTP Server Commands

3.10.1 display http server

Function

The **display http server** command displays information about the current HTTP server.

Format

display http server

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can view the HTTP server information, including the status of common and security HTTP services, port number, maximum number of users allowed to access the HTTP server, and number of current online users.

Example

Display information about the current HTTP server.

```
<Huawei> display http server
  HTTP server status    : Enabled        (default: disable)
  HTTP server port              : 80             (default: 80)
  HTTP timeout interval           : 3              (default: 10 minutes)
  Current online users            : 0
  Maximum users allowed           : 5
  HTTPS server status             : Disabled       (default: disable)
  HTTPS server port               : 443            (default: 443)
  HTTPS server manager port       :
  HTTPS SSL Policy                :
```

Table 3-34 Description of the display http server command output

Item	Description
HTTP server status	Status of the common HTTP server. ● Enabled: The HTTP service is enabled. ● Disabled: The HTTP service is disabled. You can configure the common HTTP server status by running the **3.10.7 http server enable** command.

Item	Description
HTTP server port	Number of the listening port on the HTTP server. The default port number is 80. You can configure the HTTP server port number by running the **3.10.11 http server port** command.
HTTP timeout interval	Idle timeout duration of the HTTP server. The default value is 10 minutes. You can configure the idle timeout duration by running the **3.10.13 http timeout** command.
Current online users	Number of current online users.
Maximum users allowed	Maximum number of users allowed to access the HTTP server. You can configure the maximum number of users by running the **3.10.9 http server max-online-users** command.
HTTPS server status	Status of the security HTTP server. ● Enabled: The security HTTP service is enabled. ● Disabled: The security HTTP service is disabled. You can configure the security HTTP server status by running the **19.19.2 http secure-server enable** command.
HTTPS server port	Port number of the security HTTP server. The default value is 443. You can configure the security HTTP server port number by running the **19.19.5 http secure-server port** command.
HTTPS server manager port	Management port number of the HTTPS server. You can configure the security HTTPS server manager port by running the **19.19.3 http secure-server manager-port** command.
HTTPS SSL Policy	security HTTP SSL policy. You can configure the security HTTP SSL policy by running the **19.18.10 ssl policy** command.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

3.10.13 http timeout
3.10.7 http server enable
3.10.11 http server port

3.10.2 display http user

Function

The **display http user** command displays information about current online users.

Format

display http user [**username** *username*]

Parameters

Parameter	Description	Value
username *username*	Specifies the name of the current online user.	The value is a string of 1 to 64 case-insensitive characters, with no space or wildcard. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

If **username** is not specified, this command displays summary information about all online users.

If **username** is specified, this command displays detailed information about the specified online user.

Example

Display general information about the current online user.

```
<Huawei> display http user
-------------------------------------------------------------------------------
 User Name          IP Address          Login Date
-------------------------------------------------------------------------------
 admin              192.168.0.1         2011-10-13 11:11:12+00:00
-------------------------------------------------------------------------------
Total online users is 1
```

Display detailed information about the current online user **admin**.

```
<Huawei> display http user username admin
  Client IP Address : 192.168.0.1
  Login Date        : 2011-10-13 11:11:12+00:00
  User timeouts     : 3 minutes
```

Table 3-35 Description of the display http user command output

Item	Description
User Name	User name.
Client IP Address	IP address of the HTTP client.
Login Date	Login date and time.
User timeouts	Idle timeout duration of online users.

Related Topics

3.10.13 http timeout

3.10.3 display fast-configuration state

Function

The **display fast-configuration state** command displays the state of the Internet access wizard popup notification of the web system of the EasyOperation edition.

Format

display fast-configuration state

NOTE

Only the AR100&AR120&AR150&AR160&AR200 support this command.

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To check the state of the Internet access wizard popup notification of the web system of the EasyOperation edition, run this command.

Precautions

The models must support the web system of the EasyOperation edition.

Example

Display the state of the Internet access wizard popup notification of the web system of the EasyOperation edition.

```
<Huawei> display fast-configuration state
 Fast-configuration is enabled
```

3.10.4 http acl

Function

The **http acl** command configures an ACL on the HTTP server.

The **undo http acl** command deletes the ACL on the HTTP server.

By default, no ACL is configured on the HTTP server.

Format

http acl *acl-number*

undo http acl

Parameters

Parameter	Description	Value
acl-number	Specifies the ACL number.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure the security of an HTTP server, you need to configure an ACL for it to specify clients that can log in to the current HTTP server.

Precautions

- The HTTP supports the ACL whose number ranges from 2000 to 2999.
- The **http acl** command takes effect only after you run the **rule** command to configure the ACL rule.

- After an ACL rule is modified, the HTTP server does not forcibly log out an online user who matches the ACL rule until the user sends the next login request.
- If the **http acl** command is configured several times, only the latest configuration takes effect.

Example

Set the ACL number to 2000 for the HTTP server.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule 1 permit source any
[Huawei-acl-basic-2000] quit
[Huawei] http acl 2000
```

Related Topics

3.10.1 display http server

3.10.5 http client disable

Function

The **http client disable** command disabled the HTTP client function.

The **undo http client disable** command enables the HTTP client function.

By default, the HTTP client function is enabled.

Format

http client disable

undo http client disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

As the HTTP client, the device can upload and download files to the server through HTTP by default. After you run the **http client disable** command to disable the HTTP client function, you cannot upload or download files to the server through HTTP.

Example

Disable the HTTP client.

```
<Huawei> system-view
[Huawei] http client disable
Warning: The operation will stop HTTP client. Continue? [Y/N]:y
```

3.10.6 http get

Function

The **http get** command detects whether the URL server is reachable.

Format

http get [**-a** *source-ip-address* | **-c** *count* | **-t** *timeout* | **-v** *http-version*] * **url** *url*

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address of outgoing HTTP request packets. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address of outgoing HTTP request packets.	The value is in dotted decimal notation.
-c *count*	Specifies the transmission count of HTTP request packets. If the network works unstably, increase the transmission count to detect network quality based on the packet loss ratio.	The value is an integer ranging from 1 to 100. The default value is 5.
-t *timeout*	Specifies the timeout interval for an HTTP response packet. The **http get** command sends an HTTP request packet to an address and waits for a response. If the response is received within the timeout interval, the destination is reachable. If no response is received within the timeout interval, the sender displays a message indicating that the request packet times out. A response is received within 1 to 10 seconds after an HTTP request packet is sent. If the transmission speed is low, properly prolong the timeout interval.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 5000 ms.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-v *http-version*	Specifies the HTTP version number.	The HTTP version number is 1.0 or 1.1. The default value is 1.0.
url *url*	Specifies the destination URL.	The value is a string of 1 to 256 characters.

Views

System view

Default Level

1: Monitoring level

Usage Guidelines

The **http get** command detects whether the URL server is reachable. You can use HTTP request packets to detect the following items:

- Whether the HTTP service is enabled on the URL server
- Round-trip delay in communication
- Packet loss

Example

Check whether the HTTP service is enabled on the URL server with the URL of http://w3.huawei.com, and set the source IP address of outgoing HTTP packets to 10.137.147.142, the transmission count to 5, the period for waiting for a response packet to 100 ms, and the HTTP version number to 1.1.

```
<Huawei> system-view
[Huawei] http get -a 10.137.147.142 -c 5 -t 100 -v 1.1 url http://w3.huawei.com
  Http getting http://w3.huawei.com[10.82.55.199]:

   1:packets interaction time 90 ms,the link reachable
   2:packets interaction time 100 ms,the link reachable
   3:packets interaction time 100 ms,the link reachable
   4:packets interaction time 100 ms,the link reachable
   5:packets interaction time 90 ms,the link reachable
  --http get result statistics--
    Http Get 5 time(s),succeed 5 time(s),failed 0 time(s).
    round-trip min/avg/max = 90/96/100 ms
```

Table 3-36 Description of the http get command output

Item	Description
Http getting x.x.x	URL and IP address of the URL server.

Item	Description
x: packets interaction time x ms, the link reachable	Response to each HTTP packet. ● Round-trip delay in communication ● Link reachability If no response packet is received after the timeout period, the message "Connect times out" is displayed.
http get result statistics	HTTP test statistics: ● Http Get x time(s): number of outgoing HTTP packets ● succeed x time(s): number of HTTP request packets of which corresponding HTTP response packets are received ● failed x time(s): number of HTTP request packets of which corresponding HTTP response packets fail to be received ● round-trip min/avg/max: minimum, average, and maximum round-trip delay

Related Topics

21.15.1 ping
21.15.3 tracert

3.10.7 http server enable

Function

The **http server enable** command enables the HTTP server function.

The **undo http server enable** command disables the HTTP server function.

By default, the HTTP server function is enabled.

Format

http server enable

undo http server enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After running the **http server enable** command to enable the HTTP server, you can use the browser to access the web NMS to manage devices.

If the web page to load does not exist, the HTTP service cannot be enabled.

Example

Enable the HTTP server.

```
<Huawei> system-view
[Huawei] http server enable
```

Related Topics

3.10.1 display http server

3.10.8 http server load

3.10.8 http server load

Function

The **http server load** command loads a web page file.

The **undo http server load** command cancels loading of a specified web page file.

By default, the system loads the default web page file contained in the system software when the HTTP or HTTPS service is enabled.

Format

http server load *file-name*

undo http server load

Parameters

Parameter	Description	Settings
file-name	Specifies the name of the web page file to load.	The value is a string of 5 to 64 characters without spaces. The file name is in the *.sfs format or has no file name extension.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you need to manage and maintain devices on the graphical user interface (GUI), configure the Web network management function. When you need to update web page file when using the Web network management function, run this command to load web page file.

Prerequisites

Before loading the web page file using the **http server load** command, ensure that the web page file has been stored to the device; otherwise, file loading will fail.

Example

Load the web page file web_1.

```
<Huawei> system-view
[Huawei] http server load web_1
```

Related Topics

3.10.1 display http server

3.10.9 http server max-online-users

Function

The **http server max-online-users** command sets the maximum number of concurrent online users allowed by the web NMS.

The **undo http server max-online-users** command restores the number of concurrent online users allowed by the web NMS to the default value.

By default, the maximum number of concurrent online users allowed by the web NMS is 5.

Format

http server max-online-users *max-online-users*

undo http server max-online-users

Parameters

Parameter	Description	Value
max-online-users	Specifies the maximum number of concurrent online users allowed by the web NMS.	The value is an integer that ranges from 1 to 5. The default value is 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to set the maximum number of concurrent online users allowed by the web NMS. By doing so, the number of users allowed to simultaneously access the web NMS is limited.

Precautions

When the number of users that have logged in is larger than the value specified by this command, extra users will not be forced to go offline. For example, five users have logged in to the web NMS. If you run this command to set the maximum number of concurrent online users allowed by the web NMS to 3, two extra users will not be forced to go offline.

Example

Set the maximum number of concurrent online users allowed by the web NMS to 3.

```
<Huawei> system-view
[Huawei] http server max-online-users 3
```

3.10.10 http server permit interface

Function

The **http server permit interface** command configures interfaces through which users can access the web platform.

The **undo http server permit interface** command deletes the configured interfaces so that users can access the web platform using all interfaces on the device.

By default, all interfaces on the device allow clients to access the web system.

Format

http server permit interface { *interface-type interface-number* } &<1-5>

undo http server permit interface

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type* specifies the interface type. *interface-number* specifies the number of an interface. *interface-number* and *interface-type* specify an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from accessing the web platform through interfaces on the device, run the **http server permit interface** command to configure interfaces through which users can access the web platform.

Precautions

You can only run the **http server permit interface** command to configure physical interfaces and VLANIF interfaces.

In the factory default settings of the device, users can only access the web platform through management interfaces. For example, when the management interface of the device is GE0, the http server permit interface GigabitEthernet0/0/0 command is contained in the factory default settings of the device.

A maximum of five interfaces can be configured. If you run the **http server permit interface** command multiple times, only the latest configuration takes effect, For example, if GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 has been configured, and then run the **http server permit interface** command to configure GigabitEthernet 1/0/0, users can access the web platform only through GigabitEthernet 1/0/0.

Example

Configure the interfaces through which users can access the web platform.

```
<Huawei> system-view
[Huawei] http server permit interface GigabitEthernet 1/0/0 GigabitEthernet 2/0/0
 Info: Successed in setting web permit interface.
```

Delete the configured interfaces so that users can access the web platform using all interfaces on the device.

```
<Huawei> system-view
[Huawei] undo http server permit interface
```

3.10.11 http server port

Function

The **http server port** command sets the listening port number of the HTTP server.

The **undo http server port** command restores the default listening port number of the HTTP server.

By default, the listening port number of the HTTP server is 80.

Format

http server port *port-number*

undo http server port

Parameters

Parameter	Description	Value
port-number	Specifies the listening port number of the HTTP server.	The value is an integer that ranges from The value is 80, or an integer that ranges from 1025 to 51200. The default value is 80.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the listening port number of the security HTTP server is 80. Attackers may frequently access the default listening port, which wastes bandwidth, deteriorates server performance, and prevents authorized users from accessing the HTTP server through the listening port. You can run the **http server port** command to specify another listening port number to prevent attackers from accessing the listening port.

Precautions

If the **http server port** command is configured several times, only the latest configuration takes effect.

Example

Set the listening port number of the HTTP server to 1025.

```
<Huawei> system-view
[Huawei] http server port 1025
```

Related Topics

3.10.1 display http server

3.10.12 http server-source

Function

The **http server-source** command specifies a source IP address for an HTTP server.

The **undo http server-source** command deletes the source IP address of an HTTP server.

By default, the source IP address of an HTTP server is not specified.

Format

http server-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo http server-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for the HTTP server. The loopback IP address is recommended.	-
-i *interface-type interface-number*	Specifies the loopback interface of the HTTP server as the source interface. If no loopback interface is configured or no IP address is configured for the source interface, the command fails to be executed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the HTTP server uses the source IP address specified by routes to send and receive packets. The source IP address must be configured for an interface with stable performance, such as the loopback interface. Using the loopback interface as the source IP address simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Precautions

- After the source IP address is specified for the HTTP server, you must use the specified IP address to log in to the HTTP server.
- If the HTTP service has been enabled, the HTTP service restarts after the **http server-source** command is executed.

Example

Set the source IP address of the HTTP server to **LoopBack0**.

```
<Huawei> system-view
[Huawei] http server-source -i loopback 0
Warning: To make the server source configuration take effect, the HTTP server will be restarted. Continue?
(y/n)[n]:y
Info: Succeeded in setting the source IP or interface of the HTTP server
```

Related Topics

3.10.7 http server enable

3.10.11 http server port

3.10.13 http timeout

Function

The **http timeout** command sets the idle timeout duration of the web server.

The **undo http timeout** command restores the default idle timeout duration of the webHTTP server.

By default, the idle timeout duration of the web server is 10 minutes.

Format

http timeout *timeout*

undo http timeout

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
timeout	Specifies the idle timeout duration of the web server for online users.	The value is an integer that ranges from 1 to 35791, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A maximum of five web users are supported at present. When the fifth web user logs in to the web server, any other user cannot log in to the web server even if any of the five users does not perform operations for a long time. The idle timeout duration is configured to release web resources in time. To occupy web channels for a long time, you must set the idle timeout duration to the maximum value.

Precautions

- After you run the **http timeout** command, the idle timeout durations are the same for all web users who log in to the web server. If the idle timeout duration expires, a user is disconnected from the web server and the web server notifies the user only after the user sends the next login request.
- If the **http timeout** command is configured several times, only the latest configuration takes effect.

Example

Set the idle timeout duration of the webHTTP server to 6 minutes.

```
<Huawei> system-view
[Huawei] http timeout 6
```

Related Topics

3.10.1 display http server

3.10.14 set fast-configuration state disable

Function

The **set fast-configuration state disable** command disables the Internet access wizard popup notification of the web system of the EasyOperation edition.

The **undo set fast-configuration state disable** command enables the Internet access wizard popup notification of the web system of the EasyOperation edition.

 Copyright © Huawei Technologies Co., Ltd.

By default, the Internet access wizard popup notification of the web system of the EasyOperation edition is enabled.

Format

set fast-configuration state disable

undo set fast-configuration state disable

NOTE

Only the AR100&AR120&AR150&AR160&AR200 support this command.

Parameters

None

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user has configured the Internet access wizard function and logs in to the web system of the EasyOperation edition again, if the Internet access wizard popup notification is not required, run the **set fast-configuration state disable** to disable the Internet access wizard popup notification. If the Internet access wizard popup notification is required, run the **undo set fast-configuration state disable** command.

Precautions

The models must support the web system of the EasyOperation edition.

Example

Disable the Internet access wizard popup notification of the web system of the EasyOperation edition.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] set fast-configuration state disable
```

3.10.15 set logo-path

Function

The **set logo-path** command sets the storage directory of the logo image on the web page.

The **undo set logo-path** command cancels the configured storage directory of the logo image on the web page.

By default, the storage directory of the Huawei logo image is used.

Format

set logo-path *subpathname*

undo set logo-path

Parameters

Parameter	Description	Value
subpathname	Specifies the name of the subdirectory for storing the logo image.	The value is a string of 1 to 31 characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports customization of the logo image on the web page. You can create a subdirectory for storing the logo image under the directory **logo-path** of the default working directory on the device, and store the logo image to be displayed in the subdirectory. You can run the **set logo-path** command to configure the subdirectory as the storage directory of the logo image on the web page. The required logo image then can be displayed on the web page.

The default working directory on the AR2220–AC, AR2220–DC, AR2240, AR2240C, and AR3200 series is **sd1:**, and that on other models is **flash:**.

Prerequisites

When setting the storage directory of the logo image on the web page using the **set logo-path** command, ensure that a subdirectory for storing the logo image has been created using the **mkdir** command under the directory **logo-path** of the default working directory.

Precautions

- Store the logo image using the required file name and size in the created subdirectory. After the storage directory of the logo image on the web page is set using the **set logo-path** command, the device automatically reads the file under the directory and changes the logo image on the web page.

 Copyright © Huawei Technologies Co., Ltd.

- Store three files with different pixel sizes of the required logo image in the created subdirectory, and name them as required. Name the image with the pixel size 16x16 **logo1.png**, the image with the pixel size 21x22 **logo2.png**, and the image with the pixel size 44x44 **logo3.png**.

Configuration Impact

After the storage directory of the logo image on the web page is set using the **set logo-path** command, the logo image on the web page varies depending on the configuration.

Example

Set the storage directory of the logo image on the web page to the directory **example_path**.

```
<Huawei> system-view
[Huawei] set logo-path example_path
Info: Set the vendor picture directory: " example_path " successfully.
```

3.10.16 set web login-style

Function

The **set web login-style** command sets the edition for web platform login to a router.

By default, the EasyOperation edition is used for web platform login to a router.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series routers support this command.

Format

set web login-style { **professional** | **simple** }

Parameters

Parameter	Description	Value
professional	Sets the Classics edition for web platform login to the router.	-
simple	Sets the EasyOperation edition for web platform login to the router.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the EasyOperation edition is used for web platform login to the AR100&AR120&AR150&AR160&AR200 series routers. To log in to the Classics web platform, run the **set web login-style professional** command to set the web platform edition. To restore the EasyOperation edition, run the **set web login-style simple** command.

Example

Set the Classics edition for web platform login to the router.

```
<Huawei> system-view
[Huawei] set web login-style professional
```

3.11 File Management Commands

3.11.1 ascii

Function

The **ascii** command sets the file transfer mode to ASCII on an FTP client.

The default file transfer mode is ASCII.

Format

ascii

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Files can be transferred in ASCII or binary mode.

ASCII mode is used to transfer plain text files, and binary mode is used to transfer application files, such as system software, images, video files, compressed files, and database files.

Example

Set the file transfer mode to ASCII.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] ascii
200 Type set to A.
```

Related Topics

3.11.2 binary

3.11.2 binary

Function

The **binary** command sets the file transmission mode to binary on an FTP client.

The default file transfer mode is ASCII.

Format

binary

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Files can be transferred in ASCII or binary mode.

ASCII mode is used to transfer plain text files, and binary mode is used to transfer application files, such as system software, images, video files, compressed files, and database files.

Example

Set the file transmission mode to binary.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
```

```
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] binary
200 Type set to I.
```

Related Topics

3.11.1 ascii

3.11.3 bye

Function

The **bye** command terminates the connection with the remote FTP server and enters the user view.

Format

bye

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

This command is equivalent to the **quit** command.

You can use the **close** and **disconnect** commands to terminate the connection with the remote FTP server and retain the FTP client view.

Example

Terminate the connection with the remote FTP server and enter the user view.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
```

```
[Huawei-ftp] bye
221 Windows FTP Server (WFTPD, by Texas Imperial Software) says goodbye.
<Huawei>
```

Related Topics

3.11.9 close

3.11.16 disconnect

3.1.14 quit

3.11.4 cd (FTP client view)

Function

The **cd** command changes the working directory of the FTP server.

Format

cd *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a working directory on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

The FTP server authorizes users to access files in certain directories and their subdirectories.

Example

Change the working directory to **d:/temp**.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] cd d:/temp
250 "D:/temp" is current directory.
```

Related Topics

3.11.14 dir/ls (FTP client view)
3.11.47 pwd (FTP client view)

3.11.5 cd (SFTP client view)

Function

The **cd** command changes the working directory of the SFTP server.

Format

cd [*remote-directory*]

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a directory on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- The SFTP server authorizes users to access files in certain directories and their subdirectories.
- The specified working directory must exist on the SFTP server. If the *remote-directory* parameter is not included in the **cd** command, only the current working directory of an SSH user is displayed as the command output.

Example

Change the current working directory of the SFTP server to /bill.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> cd bill
Current directory is:
/bill
```

Related Topics

3.11.15 dir/ls (SFTP client view)

3.11.6 cd (user view)

Function

The **cd** command changes the current working directory of a user.

By default, the current working directory of only the AR2220–AC, AR2220–DC, AR2240, AR2240C, AR3260 series are sd1:.

Format

cd *directory*

Parameters

Parameter	Description	Value
directory	Specifies the current working directory of a user.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] path** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name. For example, a directory name is flash:/selftest/test/.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.

- slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
- slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

NOTE

Only the AR3200 series supports dual SRUs.

For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- The directory specified in the **cd** command must exist; otherwise, the error messages will displayed:

  You can perform the following operations to rectify faults:

  a. Run the **pwd** command to view the current working directory.

  b. Run the **dir** command to view the current working directory and verify that the directory specified in the **cd** command exists.

Example

Change the current working directory from flash:/temp to flash:.

```
<Huawei> pwd
flash:/temp
<Huawei> cd flash:
<Huawei> pwd
flash:
```

Change the current working directory from flash: to flash:/t1/t2.

```
<Huawei> pwd
flash:
<Huawei> cd flash:/t1/t2
<Huawei> pwd
flash:/t1/t2
```

Change the current working directory from flash:/selftest to flash:/logfile.

```
<Huawei> pwd
flash:/selftest
<Huawei> cd /logfile/
<Huawei> pwd
flash:/logfile
```

Change the current working directory from flash:/selftest to flash:/selftest/test.

```
<Huawei> pwd
flash:/selftest
<Huawei> cd test/
<Huawei> pwd
flash:/selftest/test
```

Related Topics

3.11.49 pwd (user view)

3.11.7 cdup (SFTP client view)

Function

The **cdup** command changes the current working directory of an SSH user to its parent directory.

Format

cdup

Parameters

None

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **cdup** command to change the current working directory to its parent directory.

Precautions

If the current working directory is the SFTP authorization directory, the command cannot change the current working directory.

Example

Change the current working directory to its parent directory.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> cd dhcp
Current directory is:
/dhcp
sftp-client> cdup
Current directory is:
/
sftp-client> cdup
Error: Failed to change the current directory.
sftp-client>
```

3.11.8 cdup (FTP client view)

Function

The **cdup** command enables you to return to the upper-level directory.

Format

cdup

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To exit from the current directory and return to the upper-level directory, run the **cdup** command.

Precautions

The directories accessible to an FTP user are restricted by the authorized directories configured for the user.

Example

Exit from the current directory and return to the upper-level directory.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] cd security
250 CWD command successful.
[Huawei-ftp] cdup
250 "C:/" is current directory .
```

Related Topics

3.11.14 dir/ls (FTP client view)

3.11.47 pwd (FTP client view)

 Copyright © Huawei Technologies Co., Ltd.

3.11.9 close

Function

The **close** command terminates the connection with the remote FTP server and retains the FTP client view.

Format

close

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is equivalent to the **disconnect** command.

You can run the **bye** and **quit** commands to terminate the connection with the remote FTP server and enter the user view.

Precautions

To enter the user view from the FTP client view, you can run the **bye** or **quit** command.

Example

Terminate the connection with the remote FTP server and enter the FTP client view.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] close
221 Windows FTP Server (WFTPD, by Texas Imperial Software) says goodbye.


[Huawei-ftp]
```

Related Topics

3.11.3 bye

3.11.10 copy

Function

The **copy** command copies a file.

Format

copy *source-filename destination-filename*

Parameters

Parameter	Description	Settings
source-filename	Specifies the path and the name of a source file.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Settings
destination-filename	Specifies the path and the name of a destination file.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

NOTE

Only the AR3200 series supports dual SRUs.

For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file name is not specified, the designation file and the source file have the same name. If the source file and the destination file are in the same directory, you must specify the destination file name. If the destination file name is not specified, you cannot copy the source file.
- If the destination file name is the same as that of an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**.
- When you use a USB drive, do not remove it during data transmission.

Example

Copy the file **config.cfg** from the root directory of the flash card to flash:/temp. The destination file name is **temp.cfg**.

```
<Huawei> copy flash:/config.cfg flash:/temp/temp.cfg
Info: Copy flash:/config.cfg to flash:/temp/temp.cfg?(y/n)[n]:y
100%  complete
Info: Copied file flash:/config.cfg to flash:/temp/temp.cfg...Done
```

If the current directory is the root directory of the flash card, you can perform the preceding configuration using the relative path.

```
<Huawei> pwd
flash:
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
   0   -rw-      6,721,804  Mar 19 2012 12:31:58   devicesoft.cc
   1   -rw-            910  Mar 19 2012 12:32:58   config.cfg
   2   drw-              -  Mar 05 2012 09:54:34   temp
...
468,560 KB total (197,728 KB free)
<Huawei> copy config.cfg temp/temp.cfg
Info: Copy flash:/config.cfg to flash:/temp/temp.cfg?(y/n)[n]:y
100%  complete
Info: Copied file flash:/config.cfg to flash:/temp/temp.cfg...Done
```

Copy the file **config.cfg** from the root directory of the flash card to flash:/temp. The destination file name is **config.cfg**.

```
<Huawei> pwd
flash:
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
   0   -rw-      6,721,804  Mar 19 2012 12:31:58   devicesoft.cc
   1   -rw-            910  Mar 19 2012 12:32:58   config.cfg
   2   drw-              -  Mar 05 2012 09:54:34   temp
...
468,560 KB total (197,728 KB free)
```

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> copy config.cfg temp
Info: Copy flash:/config.cfg to flash:/temp/config.cfg?(y/n)[n]:y
100%  complete
Info: Copied file flash:/config.cfg to flash:/temp/config.cfg...Done
```

Copy the file **backup.zip** to **backup1.zip** in the test directory from the current working directory flash:/test/.

```
<Huawei> pwd
flash:/test
<Huawei> copy backup.zip backup1.zip
Info: Copy flash:/test/backup.zip to flash:/test/backup1.zip?(y/n)[n]:y
100%  complete
Info: Copied file flash:/test/backup.zip to flash:/test/backup1.zip...Done
```

Related Topics

3.11.42 move

3.11.11 delete (FTP client view)

Function

The **delete** command deletes a file from the FTP server.

Format

delete *remote-filename*

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

A file deleted in the FTP client view cannot be restored.

Example

Delete the file **temp.c**.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
```

```
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] delete temp.c
Warning: The contents of file temp.c cannot be recycled. Continue? (y/n)[n]:y
250 File deleted from remote host.
```

Related Topics

3.11.14 dir/ls (FTP client view)

3.11.12 delete (user view)

Function

The **delete** command deletes a specified file in the storage device.

Format

delete [**/unreserved**] [**/force**] { *filename* | *devicename* }

Parameters

Parameter	Description	Value
/unreserved	Deletes a specified file. The deleted file cannot be restored.	-
/force	Deletes a file directly without any confirmation.	-
filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

Parameter	Description	Value
devicename	Deletes all the files in the storage device.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

  For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- The wildcard (*) character can be used in the **delete** command.
- If the parameter **/unreserved** is not included, the file is stored in the recycle bin. To display all files including deleted files that are displayed in square brackets ([ ]), run the **dir /all** command. To restore these files that are displayed in square brackets ([ ]), run the **undelete** command. To clear these files from the recycle bin, run the **reset recycle-bin** command.

NOTICE

If you delete a file using the **/unreserved** parameter, the file cannot be restored.

- If you delete a specified storage device, all files are deleted from the root directory of the storage device.
- If you delete two files with the same name from different directories, the last file deleted is kept in the recycle bin.
- If you attempt to delete a protected file, such as a configuration file, or patch file, a system prompt is displayed.
- You cannot delete a directory by running the **delete** command. To delete a directory, run the **rmdir (user view)** command.

Example

Delete the file **test.txt** from the **flash:/test/** directory.

```
<Huawei> delete flash:/test/test.txt
Info: Delete flash:/test/test.txt?(y/n)[n]:y
```

Delete the file **test.txt** from the current working directory **flash:/selftest**.

```
<Huawei> delete test.txt
Info: Delete flash:/selftest/test.txt?(y/n)[n]::y
```

Related Topics

3.11.55 reset recycle-bin

3.11.71 undelete

3.11.13 dir (user view)

Function

The **dir** command displays information about files and directories in the storage medium.

Format

dir [**/all**] [*filename* | *directory*]

Parameters

Parameter	Description	Value
/all	Displays information about all files and directories in the current directory, including files and directories moved to the recycle bin from the current directory.	-

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.
directory	Specifies the file directory.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] path** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The wildcard character (*) can be used in this command. If no parameter is specified, this command displays information about files and directories in the current directory.

The following describes the drive name:

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

  For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

You can run the **dir /all** command to view information about all files and directories of the storage medium, including those moved to the recycle bin. The name of a file in the recycle bin is placed in square brackets ([]), for example, [test.txt].

Precautions

The device can display information about a maximum of 2,000 files and directories.

Example

Display information about all files and directories in the current directory.

```
<Huawei> dir /all
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-          889  Feb 25 2012 10:00:58   private-data.txt
    1  -rw-        6,311  Feb 17 2012 14:05:04   backup.cfg
    2  -rw-          836  Jan 01 2012 18:06:20   rr.dat
    3  drw-            -  Jan 01 2012 18:08:20   syslogfile
    4  -rw-          836  Jan 01 2012 18:06:20   rr.bak
    5  drw-            -  Feb 27 2012 00:00:54   security
    6  -rw-      523,240  Mar 16 2011 11:21:36   bootrom_53hib66.bin
    7  -rw-        2,290  Feb 25 2012 16:46:06   vrpcfg.cfg
    8  -rw-          812  Dec 12 2011 15:43:10   hostkey
    9  drw-            -  Jan 01 2012 18:05:48   compatible
   10  -rw-   25,841,428  Nov 17 2011 09:48:10   basicsoft.cc
   11  -rw-          540  Dec 12 2011 15:43:12   serverkey
```

```
  12  -rw-     26,101,692  Dec 21 2011 11:44:52   devicesoft.cc
  13  -rw-          6,292  Feb 14 2012 11:14:32   1.cfg
  14  -rw-          6,311  Feb 17 2012 10:22:56   1234.cfg
  15  -rw-          6,311  Feb 25 2012 17:22:30   [11.cfg]

1,927,220 KB total (1,130,464 KB free)
```

Display information about the file vrpcfg.cfg in the current directory.

```
<Huawei> dir vrpcfg.cfg
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-          2,290  Feb 25 2012 16:46:06   vrpcfg.cfg

1,927,220 KB total (1,130,464 KB free)
```

Display information about all .txt files in the current directory.

```
<Huawei> dir *.txt
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-            889  Feb 25 2012 10:00:58   private-data.txt

1,927,220 KB total (1,130,464 KB free)
```

Table 3-37 Description of the **dir** command output

Item	Description
d	Directory. If this item is not displayed, the corresponding **FileName** field displays a file. For example, **devicesoft.cc** is a file and **security** is a directory.
r	The file or directory is readable.
w	The file or directory is writable.
[ ]	A file moved to the recycle bin.
FileName	• private-data.txt: The file saves service initialization data. Initialization data of some tasks is irrelevant to the configuration and is not recorded in the configuration file. The **private-data.txt** file records initialization data of these tasks, for example, the number of times the device restarts. • vrpcfg.cfg: configuration file. The file name extension of the configuration file must be .cfg or .zip. • basicsoft.cc: system software. The file name extension of the system software must be .cc. Some software sub-systems store necessary data in other files in the file system when the device is running properly.

3.11.14 dir/ls (FTP client view)

Function

The **dir** and **ls** commands display all files or specified files that are stored on the FTP server, and save them to a local disk.

Format

dir [*remote-filename* [*local-filename*]]

ls [*remote-filename* [*local-filename*]]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name and directory of a file stored on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of the local file that saves the FTP server file information.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes differences between the **dir** and **ls** commands.

- When you run the **dir** command, detailed file information is displayed, including the file size, date when the file was created, whether the file is a directory, and whether the file can be modified. When you run the **ls** command, only the file name is displayed.
- The **dir** command is used to save detailed file information, while the **ls** command is used to save only the file name even if the file is specified and saved in a local directory.

Precautions

The wildcard (*) character can be used in commands **dir** and **ls**.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the name or detailed information about a file that is saved in the test directory.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] cd test
250 CWD command successfully.

[Huawei-ftp] dir
200 Port command okay.
150 Opening ASCII mode data connection for *.
drwxrwxrwx   1 noone    nogroup         0 Mar 24 10:48 .
drwxrwxrwx   1 noone    nogroup         0 Mar 26 15:52 ..
drwxrwxrwx   1 noone    nogroup         0 Mar 23 16:04 yourtest
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 10:38 backup.txt
-rwxrwxrwx   1 noone    nogroup      5736 Mar 24 10:38 backup1.txt
226 Transfer complete.
[Huawei-ftp] ls
200 Port command okay.
150 Opening ASCII mode data connection for *.
.
..
yourtest
backup.txt
backup1.txt
226 Transfer complete.
```

Display the detailed information for the file **temp.c**, and save the displayed information in file **temp1**.

```
[Huawei-ftp] dir temp.c temp1
200 Port command okay.
150 Opening ASCII mode data connection for temp.c.

226 Transfer complete.

[Huawei-ftp] quit

221 Server closing.
<Huawei> more temp1
-rwxrwxrwx  1  noone   nogroup  3929  Apr 27 18:13  temp.c
```

Display the name of file **test.bat**, and save the displayed information in file **test**.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] ls test.bat test
200 Port command okay.
150 Opening ASCII mode data connection for test.bat.

226 Transfer complete.

[Huawei-ftp] quit
```

```
221 Server closing.
<Huawei> more test
test.bat
```

Table 3-38 Description of the dir/ls command output

Item	Description
d	Indicates a directory. If this parameter is not present, the command output indicates a file.
r	Indicates that the file or directory can be read.
w	Indicates that the file or directory can be modified.

3.11.15 dir/ls (SFTP client view)

Function

The **dir** and **ls** commands display a list of specified files that are stored on the SFTP server.

Format

dir [**-l** | **-a**] [*remote-directory*]

ls [**-l** | **-a**] [*remote-directory*]

Parameters

Parameter	Description	Value
-l	Displays detailed information about all files and directories in a specified directory.	-
-a	Displays names of all files and directories in a specified directory.	-
remote-directory	Specifies the name of a directory on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

The **dir** and **ls** commands are equivalent.

- If **-l** and **-a** parameters are not specified, detailed information about all files and directories in a specified directory is displayed when you run the **dir** or **ls** command. The effect is the same as the **dir -l** command output.
- By default, if the *remote-directory* parameter is not specified, the list of current directory files is displayed when you run the **dir** or **ls** command.

Example

Display a list of files in the **test** directory of the SFTP server.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> dir test
drwxrwxrwx   1 noone    nogroup        0 Mar 24 18:48 .
drwxrwxrwx   1 noone    nogroup        0 Mar 29 14:52 ..
-rwxrwxrwx   1 noone    nogroup        0 Mar 24 00:04 yourtest
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 18:38 backup.txt
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 18:38 backup1.txt
sftp-client> dir -a test
.
..
yourtest
backup.txt
backup1.txt
sftp-client> ls test
drwxrwxrwx   1 noone    nogroup        0 Mar 24 18:48 .
drwxrwxrwx   1 noone    nogroup        0 Mar 29 14:52 ..
-rwxrwxrwx   1 noone    nogroup        0 Mar 24 00:04 yourtest
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 18:38 backup.txt
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 18:38 backup1.txt
sftp-client> ls -a test
.
..
yourtest
backup.txt
backup1.txt
```

3.11.16 disconnect

Function

The **disconnect** command terminates the connection with the remote FTP server and displays the FTP client view.

Format

disconnect

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

This command is equivalent to the **close** command.

You can run the **bye** and **quit** commands to terminate the connection with the remote FTP server and enter the user view.

To enter the user view from the FTP client view, you can run the **bye** or **quit** command.

Example

Terminate the connection with the remote FTP server and enter the FTP client view.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] disconnect

221 Windows FTP Server (WFTPD, by Texas Imperial Software) says goodbye.

[Huawei-ftp]
```

Related Topics

3.11.3 bye

3.11.9 close

3.11.43 open

3.11.17 display ftp-client

Function

The **display ftp-client** command displays the source IP address configured for the FTP client.

Format

display ftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The default source IP address 0.0.0.0 is used if **ftp client-source** is not configured.

Example

Display the source IP address of the FTP client.

```
<Huawei> display ftp-client
Info: The source IP address of FTP client is 10.1.1.1.
```

Table 3-39 Description of the display ftp-client command output

Item	Description
Info: The source IP address of FTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the FTP client. You can run the **ftp client-source** command to configure the source IP address. If a source IP address has been configured by using the **ftp client-source** command, the message "The source interface of the FTP client is LoopBack0" is displayed.

Related Topics

3.11.26 ftp
3.11.28 ftp client-source

3.11.18 display ftp-server

Function

The **display ftp-server** command displays FTP server parameter settings.

Format

display [**ipv6**] **ftp-server**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to display FTP server parameter settings.

Example

Display FTP server parameter settings.

```
<Huawei> display ftp-server
  FTP server is running
  Max user number                5
  User count                     1
  Timeout value(in minute)       30
  Listening port                 21
  Acl number                     2010
  FTP server's source address    10.1.1.1
```

Table 3-40 Description of the display ftp-server command output

Item	Description
FTP server is running	The FTP server starts. You can run the **ftp** [**ipv6**] **server enable** command to start the FTP server.
Max user number	Maximum number of users who can access the FTP server.
User count	Number of users who are accessing the FTP server.
Timeout value(in minute)	Idle timeout duration of FTP users. You can run the **ftp** [**ipv6**] **timeout** command to set the idle timeout duration of FTP users.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Listening port	Number of the listening port on the FTP server. The default value is 21. If the value is not 21, you can run the **ftp** [**ipv6**] **server port** command to configure the listening port number.
Acl number	Number of the ACL of the FTP server. The default value is 0. You can run the **ftp** [**ipv6**] **acl** command to change the ACL number.
FTP server's source address	Source IP address for the FTP server to send packets. The default value is 0.0.0.0. You can run the **ftp server-source** command to configure the source IP address for the FTP server. Here, the source IP address 10.1.1.1 is displayed. If a source interface is configured, this field displays "FTP server's source interface LoopBack0." **NOTE** If you run the **display ipv6 ftp-server** command, the **FTP server's source interface LoopBack0** is not displayed.

Related Topics

3.11.27 ftp acl
3.11.29 ftp server enable
3.11.31 ftp server port
3.11.32 ftp server-source
3.11.33 ftp timeout

3.11.19 display ftp-users

Function

The **display ftp-users** command displays FTP user parameters on the FTP server.

Format

display ftp-users

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can check FTP user parameters on the FTP server, such as the FTP user name, IP address of the client host, port number, idle duration, and the authorized directories.

Example

Display FTP user parameters.

```
<Huawei> display ftp-users
  username  host                                  port  idle  topdir
  user      10.138.77.41                          4028  0     flash:/test
  huawei    10.137.217.159                          51156 0     flash:
```

The preceding information indicates that two users are connected to the FTP server.

Table 3-41 Description of the display ftp-users command output

Item	Description
username	FTP user name.
host	IP address of the client host.
port	Port number of the client host.
idle	Idle duration.
topdir	Authorized directory of a user. You can run the **local-user ftp-directory** command to configure the authorized directory.

Related Topics

3.11.33 ftp timeout

19.1.60 local-user

3.11.20 display sftp-client

Function

The **display sftp-client** command displays the source IP address configured for the SFTP client.

Format

display sftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display sftp client** command to display the source IP address of the SFTP client. The default source IP address 0.0.0.0 is used if **sftp client-source** is not configured.

Example

Display the source IP address configured for the SFTP client.

```
<Huawei> display sftp-client
Info: The source address of SFTP client is 10.1.1.1
```

Table 3-42 Description of the display sftp-client command output

Item	Description
Info: The source address of SFTP client is 10.1.1.1	10.1.1.1 is the source IP address of the SFTP client. You can run the **sftp client-source** command to configure the source IP address for the SFTP client. If an IP address has been configured for the source port, the message "The source interface of the SFTP client is LoopBack0" is displayed.

Related Topics

3.11.62 sftp

3.11.63 sftp client-source

3.11.21 display tftp-client

Function

The **display tftp-client** command displays the source IP address configured for the TFTP client.

Format

display tftp-client

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display tftp client** command to query source IP address of the TFTP client. The default source IP address is 0.0.0.0 if **tftp client-source** is not configured.

Example

Display the source IP address configured for the TFTP client.

```
<Huawei> display tftp-client
Info: The source address of TFTP client is 10.1.1.1.
```

Table 3-43 Description of the display tftp-client command output

Parameter	Description
Info: The source address of TFTP client is 10.1.1.1.	10.1.1.1 is the source IP address of the TFTP client. You can run the **tftp client-source** command to configure the source IP address for the TFTP client. If the IP address is configured for the source port, the message "The source interface of TFTP client is LoopBack0" is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

3.11.65 tftp

3.11.66 tftp client-source

3.11.22 display tftp-server status

Function

The **display tftp-server status** command displays the TFTP server information.

Format

display tftp-server status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check the TFTP server configuration and connections with the current TFTP clients.

Example

Display the TFTP server information.

```
<Huawei> display tftp-server status
TFTP Server is                    enabled
Listening port                    69
Timeout value(in second)              10
TFTP server's root path             flash:
There are 1 clients connected
      [1]: ip 10.137.217.163, port 23, op READ
```

Table 3-44 Description of the display tftp-server status command output

Item	Description
TFTP Server is	Status of the TFTP server. ● disabled ● enabled To enable or disable the TFTP server function, run the **tftp server enable** command.
Listening port	Port number of the TFTP server. To configure a port number for the TFTP server, run the **tftp server port** command.
Timeout value(in second)	Packet timeout period of the TFTP server, in seconds. To configure a packet timeout period for the TFTP server, run the **tftp server timeout** command.
TFTP server's root path	Working directory of the TFTP server. To configure a working directory for the TFTP server, run the **set default tftp-directory** command.
There are 1 clients connected	One client has connected to the TFTP server.
[1]: ip 10.137.217.163, port 23, op READ	Client information. The client sequence number is 1; IP address is 10.137.217.163; port number is 23; and operation type is Read.

3.11.23 execute

Function

The **execute** command executes a specified batch file.

Format

execute *batch-filename*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
batch-filename	Specifies the name of a batch file.	The value is a string of 5 to 64 case-insensitive characters without spaces. The file name extension is .bat.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a series of commands are frequently executed, write these commands in a batch file, and store this file in system. In this way, you can only execute this command to run multiple commands which were manually entered before. This command improves maintenance and management efficiency.

NOTE

- The batch file is edited in .txt format. When editing the file, ensure that one command occupies one line. After editing the file, save the file and change the file name extension to .bat.
- Transfer the batch file in file transmission mode to the device.

Prerequisites

Before running the **execute** command, ensure that the batch file to be processed is in the current directory; otherwise, the system cannot find the batch file.

Precautions

- The commands in a batch file are run one by one. A batch file cannot contain invisible characters (control characters or escape characters, such as \r, \n, and \b). If any invisible character is detected, the execute command exits from the current process and no rollback is performed.
- The **execute** command does not ensure that all commands can be run. If the system runs a wrong or immature command, it displays the error and goes to next command. The **execute** command does not perform the hot backup operation, and the command format or content is not restricted.
- In case of interactive commands, batch file execution waits the device to interact with users before continuing.

Example

Execute the **test.bat** file in the directory flash:/. The **test.bat** file contains three commands: **system-view**, **aaa**, and **local-user huawei password irreversible-cipher Helloworld@6789**.

```
<Huawei> system-view
[Huawei] execute test.bat
[Huawei] system-view
         ^
Error: Unrecognized command found at '^' position.
[Huawei] aaa
[Huawei-aaa] local-user huawei password irreversible-cipher Helloworld@6789
[Huawei-aaa]
```

When the system runs the first command **system-view** in current system view, it displays an error and continues to run the following commands.

The system displays the execution of a batch file in AAA view.

```
[Huawei-aaa] display this
 local-user huawei password irreversible-cipher %@%@HW=5%Mr;:2)/RX$FnU1HLO%-TBMp4wn%;~\#
%iAut}_~O%0L%@%@
```

3.11.24 file prompt

Function

The **file prompt** command changes the prompt mode when you perform operations on files.

The default prompt mode is alert.

Format

file prompt { **alert** | **quiet** }

Parameters

Parameter	Description	Value
alert	Display a prompt message before users perform an operation.	-
quiet	Do not display a prompt message before users perform an operation.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

If the prompt mode is set to quiet, the system does not provide prompt messages when operations leading to data loss are executed, such as deleting or overwriting files. Therefore, this prompt mode should be used with caution.

Example

Set the prompt mode to quiet. When you rename a copied file **test.txt** using an existing file name **test1.txt**, no prompt message is displayed.

```
<Huawei> system-view
[Huawei] file prompt quiet
[Huawei] quit
<Huawei> copy test.txt test1.txt
100%  complete
Info: Copied file flash:/test.txt to flash:/test1.txt...Done.
```

Set the prompt mode to alert.

```
<Huawei> system-view
[Huawei] file prompt alert
[Huawei] quit
<Huawei> copy test.txt test1.txt
Copy flash:/test.txt to flash:/test1.txt?[Y/N]:y
The file flash:/test1.txt exists. Overwrite it?[Y/N]:y
100%  complete
Info: Copied file flash:/test.txt to flash:/test1.txt...Done.
```

3.11.25 format

Function

The **format** command formats a storage device.

Format

format *drive*

Parameters

Parameter	Description	Value
drive	Specifies the name of the storage device to format. If a storage device contains the system software package, the storage device cannot be formatted using the **format** command. To format the storage device, perform the operation in the BootROM menu.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the storage device name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

When the file system fault cannot be rectified or the data on the storage device is unnecessary, the storage device can be formatted. When you run the **format** command, all files and directories are cleared from the storage device.

Configuration Impact

NOTICE

After a storage device is formatted, the data it saves is deleted. If the configuration file for the next startup is saved on the storage device, configurations are lost after the device is restarted. If the software package for the next startup is saved on the storage device, device restart is affected.

Precautions

NOTICE

After the **format** command is run, files and directories are cleared from the specified storage device and cannot be restored. Therefore, this command should be used with caution.

If the storage device is still unavailable after the **format** command is run, a physical exception may have occurred.

Example

Format the storage device.

```
<Huawei> format flash:
All data(include configuration and system startup file) on flash: will be lost , proceed with format? (y/n)
[n]:y
Info: Format flash: completed.
```

3.11.26 ftp

Function

The **ftp** command connects the FTP client to the FTP server and enters the FTP client view.

Format

Connect the FTP client to the FTP server based on the IPv4 address.

ftp [[**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]]

Connect the FTP client to the FTP server based on the IPv6 address.

ftp ipv6 *host-ipv6* [**vpn6-instance** *vpn6-instance-name*] [*port-number*]

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for connecting to the FTP client. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
port-number	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535. The default value is the standard port number 21.
public-net	Specifies the FTP server on the public network. You must set the **public-net** parameter when the FTP server IP address is a public network IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the IPv4 FTP server is located.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpn6-instance *vpn6-instance-name*	Specifies the name of the VPN instance where the IPv6 FTP server is located.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
host-ipv6	Specifies the IP address or host name of the remote IPv6 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before accessing the FTP server on the FTP client, you must first run the **ftp** command to connect the FTP client to the FTP server.

Precautions

- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified on the IPv4 network. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.

 Copyright © Huawei Technologies Co., Ltd.

  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If no parameter is set in the **ftp** command, only the FTP view is displayed, and no connection is set up between the FTP server and client.
- If the port number that the FTP server uses is non-standard, you must specify a standard port number; otherwise, the FTP server and client cannot be connected.
- When you run the **ftp** command, the system prompts you to enter the user name and password for logging in to the FTP server. You can log in to the FTP server if the user name and password are correct.
- If the number of login users exceeds the maximum value that the FTP server allows, other authorized users cannot log in to the FTP server. To allow news authorized users to log in to the FTP server, users who have performed FTP services must disconnect their clients from the FTP server. You can run the **bye** or **quit** command to disconnect the FTP client from the FTP server and return to the user view, or run the **close** or **disconnect** command to disconnect the FTP client from the FTP server and retain in the FTP client view.

Example

Connect to the FTP server whose IP address is 10.137.217.201.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp]
```

Connect to the remote IPv6 FTP server whose address is fc00:2001:db8::1.

```
<Huawei> ftp ipv6 fc00:2001:db8::1
Trying fc00:2001:db8::1
Press CTRL+K to abort
Connected to ftp fc00:2001:db8::1.
220 FTP service ready.
User(fc00:2001:db8::1:(none)):huawei
331 Password required for huawei
Enter Password:
230 User logged in.

[Huawei-ftp]
```

Related Topics

3.11.3 bye
3.11.16 disconnect

3.11.27 ftp acl

Function

The **ftp acl** command specifies an ACL number for the current FTP server so that the FTP client with the same ACL number can access the FTP server.

The **undo ftp acl** command deletes an ACL number of the current FTP server.

By default, no ACL is configured for FTP server.

Format

ftp [**ipv6**] **acl** *acl-number*

undo ftp [**ipv6**] **acl**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
acl-number	Specifies the number of the ACL.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure the security of an FTP server, you need to configure an ACL for it to specify FTP clients that can access the current FTP server.

Precautions

- The **ftp acl** command takes effect only after you run the **rule** command to configure the ACL rule.
- The FTP only supports the basic ACL whose number ranges from 2000 to 2999.

Example

Allow the client whose ACL number is 2000 to log in to the FTP server.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 10.10.10.1 0
```

```
[Huawei-acl-basic-2000] quit
[Huawei] ftp acl 2000
```

Related Topics

3.11.18 display ftp-server

3.11.28 ftp client-source

Function

The **ftp client-source** command specifies the source IP address for the FTP client to send packets.

The **undo ftp client-source** command restores the default source IP address for the FTP client to send packets.

The default source IP address for the FTP client to send packets is 0.0.0.0.

Format

ftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo ftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the source interface. You are advised to use the loopback interface. The IP address configured for the source interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Precautions

- You can also run the **ftp** command to configure the source IP address whose priority is higher than that of the source IP address specified by the **ftp client-source** command. If you specify the source IP addresses by running the **ftp client-source** and **ftp** commands, the source IP address specified by the **ftp** command is used for data communication and is available only for the current FTP connection, while the source IP address specified by the **ftp client-source** command is available for all FTP connections.
- The IP address that a user displays on the FTP server is the specified source IP address or source interface IP address.
- If the specified source interface has been bound to a VPN instance, the client is automatically bound to the same VPN instance.

Example

Set the source IP address of the FTP client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] ftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the FTP client to 10.1.1.1.
```

Related Topics

3.11.26 ftp

3.11.32 ftp server-source

3.11.17 display ftp-client

3.11.29 ftp server enable

Function

The **ftp server enable** command enables the FTP server function to allow FTP users to log in to the FTP server.

The **undo ftp server** command disables the FTP server function so that FTP users cannot log in to the FTP server.

By default, the FTP function is disabled.

Format

ftp [**ipv6**] **server enable**

undo ftp [**ipv6**] **server**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To manage FTP server files on a client, you must run the **ftp server enable** command to enable the FTP server function to allow FTP users to log in to the FTP server.

Precautions

If the FTP server function is disabled, no user can log in to the FTP server, and users who have logged in to the FTP server cannot perform any operation except logout.

NOTICE

The FTP protocol compromises device security. SFTP V2 mode is recommended.

Example

Enable the FTP server function.

```
<Huawei> system-view
[Huawei] ftp server enable
Info: Succeeded in starting the FTP server.
Info: FTP is insecure, recommended to use SFTP with encryption features.
```

Related Topics

3.11.18 display ftp-server

3.11.30 ftp server permit interface

Function

The **ftp server permit interface** command specifies physical interfaces on the FTP server to which clients can connect.

The **undo ftp permit interface** command restores the default physical interfaces on the FTP server to which clients can connect.

By default, clients can connect to all the physical interfaces on the FTP server.

Format

ftp server permit interface { *interface-type interface-number* } &<1-5>

undo ftp server permit interface

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type*: specifies the interface type. *interface-number*: specifies the interface number. *interface-number* and *interface-type* specify an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent a client from connecting to the FTP server through an unauthorized physical interface, you can run the **ftp server permit interface** command to specify physical interfaces on the FTP server to which the client can connect.

Precautions

- By default, the client can connect to all the physical interfaces on the FTP server. When you run this command to specify one physical interface on the FTP server, the client cannot connect to the other physical interfaces on the FTP server.
- You can specify a maximum of five interfaces each time you run the **ftp server permit interface** command. The latest configuration overrides the previous one. For example, before you run the command, clients can connect to three physical interfaces GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 on the FTP server. After you run the command to specify the interface GigabitEthernet 1/0/0, clients can only connect to the interface GigabitEthernet 1/0/0.

Example

Specify physical interfaces on the FTP server to which clients can connect.

```
<Huawei> system-view
[Huawei] ftp server permit interface gigabitethernet 1/0/0 gigabitethernet 2/0/0
```

```
Info: Succeeded in setting ftp permit interface.
```

Restore the default physical interfaces on the FTP server to which clients can connect.

```
<Huawei> system-view
[Huawei] undo ftp server permit interface
```

3.11.31 ftp server port

Function

The **ftp server port** command specifies the listening port number of the FTP server.

The default value is 21.

Format

ftp [**ipv6**] **server port** *port-number*

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
port *port-number*	Specifies the listening port number of the FTP server.	The value is 21 or an integer that ranges from 1025 to 55535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the listening port number of the FTP server is 21. Attackers may frequently access the default listening port, which wastes bandwidth, deteriorates server performance, and prevents authorized users from accessing the FTP server through the listening port. You can run the **ftp server port** command to specify another listening port number to prevent attackers from accessing the listening port.

Prerequisites

Before running the **ftp server port** command to specify the listening port number, you must first run the **undo ftp server** command to disable FTP services.

Precautions

- After the **ftp server port** command is executed, the FTP server disconnects all FTP connections and uses the new listening port.
- If the current listening port number is 21, FTP client users do not need to specify the port number for logging in to the FTP server. If the current listening port number is not 21, FTP client users must use the FTP server's listening port number to log in to the FTP server.
- After the listening port number is changed, you must run the **ftp server enable** command to enable FTP services to make the configuration take effect.

Example

Change the port number of the FTP server to 1028.

```
<Huawei> system-view
[Huawei] undo ftp server
[Huawei] ftp server port 1028
```

Related Topics

3.11.29 ftp server enable

3.11.32 ftp server-source

Function

The **ftp server-source** command specifies the source IP address for an FTP server to send packets.

The **undo ftp server-source** command restores the default source IP address for an FTP server to send packets.

The default source IP address for the FTP server to send packets is 0.0.0.0.

Format

ftp server-source { **-a** [**ipv6**] *source-ip-address* | **-i** [**ipv6**] *interface-type interface-number* }

undo ftp [**ipv6**] **server-source**

Parameters

Parameter	Description	Value
ipv6	Configures the FTP server to support an IPv6 source address.	-
-a *source-ip-address*	Specifies the source IP address for the FTP server to send packets. The loopback IP address is recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the loopback interface of the FTP server as the source interface. If no loopback interface is configured or no IP address is configured for the source interface, the command fails to be executed.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the FTP server uses the source IP address specified by routes to send packets. The source IP address must be configured for an interface with stable performance, such as the loopback interface. Using the loopback interface as the source IP address simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Precautions

- After the source IP address is specified for the FTP server, you must use the specified IP address to log in to the FTP server.
- If the FTP service has been enabled, the FTP service restarts after the **ftp server-source** command is executed.
- If the specified source interface has been bound to a VPN instance, the server is automatically bound to the same VPN instance.
- The source interface is not specified, which may cause security risks.

Example

Set the source IP address of the FTP server to **LoopBack0**.

```
<Huawei> system-view
[Huawei] ftp server-source -i loopback 0
Warning: To make the server source configuration take effect, the FTP server will be restarted. Continue?
[Y/N]: y
Info: Succeeded in setting the source interface of the FTP server to LoopBack0.
Info: Succeeded in starting the FTP server.
Info: FTP is insecure, recommended to use SFTP with encryption features.
```

Related Topics

3.11.26 ftp

3.11.29 ftp server enable
3.11.28 ftp client-source

3.11.33 ftp timeout

Function

The **ftp timeout** command configures the idle timeout duration of the FTP server.

The **undo ftp timeout** command restores the default idle timeout duration.

By default, the idle timeout duration of the FTP server is 30 minutes.

Format

ftp [**ipv6**] **timeout** *minutes*

undo ftp [**ipv6**] **timeout**

Parameters

Parameter	Description	Value
ipv6	Specifies the IPv6 FTP server.	-
minutes	Specifies idle timeout duration.	The value is an integer that ranges from 1 to 35791, in minutes. By default, the idle timeout duration is 30 minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

After a user logs in to the FTP server, a connection is set up between the FTP server and the user's client. The idle timeout duration is configured to release the connection when the connection is interrupted or when the user performs no operation for a specified time.

Example

Set the idle timeout duration to 36 minutes.

```
<Huawei> system-view
[Huawei] ftp timeout 36
```

Related Topics

3.11.18 display ftp-server

3.11.34 get (SFTP client view)

Function

The **get** command downloads a file from the SFTP server and saves the file to the local device.

Format

get *remote-filename* [*local-filename*]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be downloaded from the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of a downloaded file to be saved to the local device.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **get** command to download files from the FTP server to upgrade devices.

Precautions

- If *local-filename* is not specified on the local device, the original file name is used.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

Example

Download a file from the SFTP server.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
```

```
Connected to 10.137.217.201 ...
Enter password:
sftp-client> get test.txt
Remote file: / test.txt --->  Local file: test.txt
Info: Downloading file successfully ended.
```

Related Topics

3.11.46 put (SFTP client view)

3.11.35 get (FTP client view)

Function

The **get** command downloads a file from the FTP server and saves the file to the local device.

Format

get *remote-filename* [*local-filename*]

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be downloaded from the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.
local-filename	Specifies the name of a downloaded file to be saved to the local device.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **get** command to download system software, backup configuration files, and patch files from the FTP server to upgrade devices.

Precautions

- If the downloaded file name is not specified on the local device, the original file name is used.
- If the name of the downloaded file is the same as that of an existing local file, the system prompts you whether to overwrite the existing file.

 Copyright © Huawei Technologies Co., Ltd.

Example

Download the system software **devicesoft.cc** from the FTP server.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] get devicesoft.cc
200 Port command successful.
150 Opening data connection for devicesoft.cc.
226 File sent ok
FTP: 6482944 byte(s) received in 54.500 second(s) 1117.40byte(s)/sec.
```

Related Topics

3.11.45 put (FTP client view)

3.11.36 help (SFTP client view)

Function

The **help** command displays the help information in the SFTP client view.

Format

help [**all** | *command-name*]

Parameters

Parameter	Description	Value
all	Displays all commands in the SFTP client view.	-
command-name	Displays the format and parameters of a specified command in the SFTP client view.	-

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the SFTP view, you can only enter the question mark (?) to obtain all commands in the SFTP client view. If you enter a command keyword and the question mark (?) to query command parameters, an error message is displayed, as shown in the following:

```
sftp-client> dir ?
Error: Failed to list files.
```

You can run the **help** command to obtain the help information and display all commands or a command format in the SFTP client view.

Precautions

If you specify no parameter when running the **help** command, all commands in the SFTP client view are displayed. This has the same effect as the **help all** command or directly entering the question mark (?) in the SFTP client view.

Example

Display the format of the command **get**.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> help get
get Remote file name STRING<1-64>   [Local file name STRING<1-64>]  Download file
Default local file name is the same with remote file.
```

Display all commands in the SFTP client view.

```
sftp-client> help all
cd
cdup
dir
get
help
ls
mkdir
put
pwd
quit
rename
remove
rmdir
```

Related Topics

3.11.62 sftp

3.11.37 lcd

Function

The **lcd** command displays and changes the local working directory of the FTP client in the FTP client view.

Format

lcd [*local-directory*]

Parameters

Parameter	Description	Value
local-directory	Specifies the local working directory of the FTP client.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **lcd** command to display the local working directory of the FTP client when uploading or downloading files, and set the upload or download path to the path of the local working directory.

Precautions

The **lcd** command displays the local working directory of the FTP client, while the **pwd** command displays the working directory of the FTP server. If you specify the parameter *local-directory* in the **lcd** command, you can directly change the local working directory in the FTP client view.

Example

Change the local working directory to **flash:/test**.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] lcd
The current local directory is flash:.
[Huawei-ftp] lcd flash:/test
The current local directory is flash:/test.
```

Related Topics

3.11.47 pwd (FTP client view)

3.11.38 mkdir (FTP client view)

Function

The **mkdir** command creates a directory on the remote FTP server.

Format

mkdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the directory to be created.	The value is a string of case-insensitive characters without spaces. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

- You can run the **mkdir** command to create a subdirectory in a specified directory, and the subdirectory name must be unique.
- If no path is specified when you create a subdirectory, the subdirectory is created in the current directory.
- The created directory is stored on the FTP server.

Example

Create a directory **test** on the remote FTP server.

```
<Huawei> ftp 172.16.104.110
Trying 172.16.104.110 ...
Press CTRL+K to abort
Connected to 172.16.104.110.
220 FTP service ready.
User(172.16.104.110:(none)):huawei
331 Password required for huawei
Enter password:
230 User logged in.
[Huawei-ftp] mkdir test
257 "test" new directory created.
```

Related Topics

3.11.14 dir/ls (FTP client view)

3.11.56 rmdir (FTP client view)

3.11.39 mkdir (SFTP client view)

Function

The **mkdir** command creates a directory on the remote SFTP server.

Format

mkdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies the directory to be created.	The value is a string of case-insensitive characters without spaces. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can run the **mkdir** command to create a subdirectory in a specified directory, and the subdirectory name must be unique.
- If no path is specified when you create a subdirectory, the subdirectory is created in the current directory.
- The created directory is stored on the SFTP server.
- After a directory is created, you can run the **dir/ls (SFTP client view)** command to view the directory.

Example

Create a directory on the SFTP server.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> mkdir ssh
Info: Succeeded in creating a directory.
```

Related Topics

3.11.15 dir/ls (SFTP client view)
3.11.58 rmdir (SFTP client view)

3.11.40 mkdir (User view)

Function

The **mkdir** command creates a directory in the current storage device.

Format

mkdir *directory*

Parameters

Parameter	Description	Settings
directory	Specifies a directory or directory and its path.	The value is a string of case-insensitive characters in the **[drive] [path] directory** format. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. Characters such as ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only the AR3200 series supports dual SRUs.

For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

If you only the subdirectory name is specified, a subdirectory is created in the current working directory. You can run the **3.11.49 pwd (user view)** command to query the current working directory. If the subdirectory name and directory path are specified, the subdirectory is created in the specified directory.

Precautions

- The subdirectory name must be unique in a directory; otherwise, the message "Error: Directory already exists" is displayed.

Example

Create the subdirectory **new** in the flash card.

```
<Huawei> mkdir flash:/new
Info: Create directory flash:/new.....Done
```

Related Topics

3.11.13 dir (user view)

3.11.41 more

Function

The **more** command displays the content of a specified file.

Format

more [**/binary**] *filename* [*offset*] [**all**]

Parameters

Parameter	Description	Value
/binary	Displays the file content in binary mode.	-

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.
offset	Specifies the file offset.	The value is an integer that ranges from 0 to 2147483647, in bytes.
all	Displays all the file content on one screen.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **more** command to display the file content directly on a device.

- The following describes the drive name.
  - **drive** is the storage device and is named as follows:
    - sd1: root directory of the Micro SD card on the master SRU.
    - flash: root directory of the flash memory on the master SRU.
    - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
    - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

    NOTE

    Only the AR3200 series supports dual SRUs.

    For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

- The path can be an absolute path or relative path.
  - **flash:/my/test/** is an absolute path.
  - **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- You are not advised to use this command to display non-text files; otherwise, the terminal is shut down or displays garbled characters, which is harmless to the system.
- Files are displayed in text format.
- You can display the file content flexibly by specifying parameters before running the **more** command:
  - You can run the **more** *filename* command to view a specified text file. The content of the specified text file is displayed on multiple screens. You can press the spacebar consecutively on the current session GUI to display all content of the file.

    To display the file content on multiple screens, you must ensure that:

    - The number of lines that can be displayed on a terminal screen is greater than 0. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
    - The total number of file lines is greater than the number of lines that can be displayed on a terminal screen. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
  - You can run the **more** *filename offset* command to view a specified file. The content of the specified text file starting from *offset* is displayed on multiple screens. You can press the spacebar consecutively on the current session GUI to display all content of the file.

    To display the file content on multiple screens, you must ensure that:

    - The number of lines that can be displayed on a terminal screen is greater than 0. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
    - The number of lines starting from *offset* in the file is greater than the number of lines that can be displayed on a terminal screen. (The number of lines that can be displayed on a terminal screen is set by running the **screen-length** command.)
  - You can run the **more** *file-name* **all** command to view a specified file. The file content is displayed on one screen.

Example

Display the content of the file **test.bat**.

```
<Huawei> more test.bat
rsa local-key-pair create
user-interface vty 12 14
authentication-mode aaa
protocol inbound ssh
user privilege level 5
```

```
quit
ssh user sftpuser authentication-type password
sftp server enable
```

Display the content of the file **log.txt** and set the offset to 100.

```
<Huawei> more log.txt 100
:               CHINA HUAWEI TECHNOLOGY LIMITTED CO.,LTD
#   FILE NAME:                  Product Adapter File(PAF)
#   PURPOSE:                    MAKE VRPV5 SUITABLE FOR DIFFERENT PRODUCT IN LIB
#   SOFTWARE PLATFORM:          V6R2C00
#   DETAIL VERSION:             B283
#   DEVELOPING GROUP:           8090 SYSTEM MAINTAIN GROUP
#   HARDWARE PLATFORM:          8090 (512M Memory)
#   CREATED DATE:               2003/05/10
#   AUTH:                       RAINBOW
#   Updation History:           Kelvin dengqiulin update for 8090(2004.08.18)
#                               lmg update for R3(2006.11.7)
#                               fsr update for R5 (2008.1.18)
#                               qj update for R6 (2008.08.08)
#   COPYRIGHT:                  2003---2008
#-------------------------------------------------------------------------------


#BEGIN FOR RESOURCE DEFINATION
[RESOURCE]
FORMAT: SPECS RESOURCE NAME STRING = CONTROLLABLE(1 : ABLE , 0: NOT ABLE),DEFAUL
T VALUE , MAX VALUE , MIN VALUE
#BEGIN  SPECS RESOURCE FOR TE tunnel Nto1 PS MODULE
PAF_LCS_TUNNEL_SPECS_TE_PS_MAX_PROTECT_NUM = 1, 8, 16, 1
PAF_LCS_TUNNEL_SPECS_TE_PS_REBOOT_TIME     = 1, 180000, 3600000, 60000
  ---- More ----
```

Display the content of the file **paf.txt**.

```
<Huawei> more paf.txt all
PAF_LCS_588_IFC_FIFO_DEPTH_ASE = 222
#IFC_FIFO_DEPTH_ASE EXPLAIN (222: NORMAL, 102: DEEP)
PAF_LCS_588_IPE_FIFO_DEPTH_TCM = 659206
#IPE_FIFO_DEPTH_TCM EXPLAIN (659206: NORMAL, 655360: DEEP)
PAF_LCS_588_IFC_FIFO_DEPTH_TCM = 222
#IFC_FIFO_DEPTH_TCM EXPLAIN (222: NORMAL, 102: DEEP)
#END OF SPECS RESOURCE FOR 588 MODULE
#BEGIN  8090 MEM GATE  AND  ISSU MEM GATE
PAF_LCS_8090_BOARD_RESET_MEMORY_GATE           = 90
PAF_LCS_8090_512BOARD_RESET_MEMORY_GATE        = 85
PAF_LCS_8090_BOARD_RESET_MEMORY_GATE_ISSU      = 95
PAF_LCS_ISSU_CHECK_MEMORY_GATE                 = 40
#END  8090 MEM GATE  AND  ISSU MEM GATE
[END CONFIGURE]
```

3.11.42 move

Function

The **move** command moves the source file from a specified directory to a destination directory.

Format

move *source-filename destination-filename*

Parameters

Parameter	Description	Settings
source-filename	Specifies the directory and name of a source file.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.
destination-filename	Specifies the directory and name of a destination file.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

  For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**.
- This command cannot be used to move files between storage devices.
- The **move** and **copy** commands have different effects:
  - The **move** command moves the source file to the destination directory.
  - The **copy** command copies the source file to the destination directory.

Example

Move a file from **flash:/test/sample.txt** to **flash:/sample.txt**.

```
<Huawei> move flash:/test/sample.txt flash:/sample.txt
Info: Move flash:/test/sample.txt to flash:/sample.txt ?(y/n)[n]: y
Info: Moved file flash:/test/sample.txt to flash:/sample.txt.
```

Related Topics

3.11.10 copy

3.11.43 open

Function

The **open** command connects the FTP client and server.

Format

Connect the FTP client to the FTP server based on the IPv4 address.

open [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *host-ip* [*port-number*] [**public-net** | **vpn-instance** *vpn-instance-name*]

Connect the FTP client to the FTP server based on the IPv6 address.

open ipv6 *host-ipv6* [*port-number*]

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for connecting to the FTP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
port-number	Specifies the port number of the FTP server.	The value is an integer that ranges from 1 to 65535, or 21. The default value is the standard port number 21.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
public-net	Specifies the FTP server on the public network. You must set the **public-net** parameter when the FTP server IP address is a public network IP address.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance where the FTP server is located.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
host-ipv6	Specifies the IP address or host name of the remote IPv6 FTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **open** command in the FTP client view to connect the FTP client to the server to transmit files and manage files and directories of the FTP server.

Precautions

- You can run the **ftp** command in the user view to connect the FTP client and server and enter the FTP client view.
- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified on the IPv4 network. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.

 Copyright © Huawei Technologies Co., Ltd.

  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If the port number that the FTP server uses is non-standard, you must specify a standard port number; otherwise, the FTP server and client cannot be connected.
- When you run the **open** command, the system prompts you to enter the user name and password for logging in to the FTP server. You can log in to the FTP client and enter the FTP client view if the user name and password are correct.

Example

Connect the FTP client with the FTP server whose IP address is 10.137.217.204.

```
<Huawei> ftp
[Huawei-ftp] open 10.137.217.204
Trying 10.137.217.204 ...
Press CTRL+K to abort
Connected to 10.137.217.204.
220 FTP service ready.
User(10.137.217.204:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.

[Huawei-ftp]
```

Connect the FTP client with the FTP server whose IP address is fc00:2001:db8::1.

```
<Huawei> ftp
[Huawei-ftp] open ipv6 fc00:2001:db8::1
Trying fc00:2001:db8::1 ...
Press CTRL+K to abort
Connected to fc00:2001:db8::1
220 FTP service ready.
User(fc00:2001:db8::1:(none)):huawei
331 Password required for huawei
Enter Password:
230 User logged in.

[Huawei-ftp]
```

Related Topics

3.11.26 ftp

3.11.16 disconnect

3.11.44 passive

Function

The **passive** command sets the data transmission mode to passive.

The **undo passive** command sets the data transmission mode to active.

By default, the data transmission mode is active.

Format

passive

undo passive

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

The device supports the active and passive data transmission modes. In active mode, the server initiates a connection request, and the client and server need to enable and monitor a port to establish a connection. In passive mode, the client initiates a connection request, and only the server needs to monitor the corresponding port. This command is used together with the firewall function. When the client is configured with the firewall function, FTP connections are restricted between internal clients and external FTP servers if the FTP transmission mode is active. If the FTP transmission mode is passive, FTP connections between internal clients and external FTP servers are not restricted.

Example

Set the data transmission mode to passive.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] passive
Info: Succeeded in switching passive on.
```

3.11.45 put (FTP client view)

Function

The **put** command uploads a local file to the remote FTP server.

Format

put *local-filename* [*remote-filename*]

Parameters

Parameter	Description	Value
local-filename	Specifies the local file name of the FTP client.	The value is a string of 1 to 64 case-insensitive characters without spaces.
remote-filename	Specifies the name of the file to be uploaded to the remote FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **put** command to upload a local file to the remote FTP server for further check and backup. For example, you can upload the local log file to the FTP server for other users to check, and upload the configuration file to the FTP server as a backup before upgrading the device.

Precautions

- If the file name is not specified on the remote FTP server, the local file name is used.
- If the name of the uploaded file is the same as that of an existing file on the FTP server, the system overwrites the existing file.

Example

Upload the configuration file **vrpcfg.zip** to the remote FTP server as a backup, and save it as **backup.zip**.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] put vrpcfg.zip backup.zip
200 Port command successful.
150 Opening BINARY mode data connection for file transfer.
226 Transfer complete
FTP: 1098 byte(s) sent in 0.131 second(s) 8.38Kbyte(s)/sec.
```

Related Topics

3.11.35 get (FTP client view)

3.11.46 put (SFTP client view)

Function

The **put** command uploads a local file to a remote SFTP server.

Format

put *local-filename* [*remote-filename*]

Parameters

Parameter	Description	Value
local-filename	Specifies a local file name on the SFTP client.	The value is a case-insensitive character string without spaces. The file name (including the absolute path) contains 1 to 64 characters.
remote-filename	Specifies the name of the file uploaded to the remote SFTP server.	The value is a case-insensitive character string without spaces. The file name (including the absolute path) contains 1 to 64 characters.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command enables you to upload files from the local device to a remote SFTP server to view the file contents or back up the files. For example, you can upload log files of a device to an SFTP server and view the logs in the server. During an upgrade, you can upload the configuration file of the device to the SFTP server for backup.

Precautions

- If *remote-filename* is not specified, the uploaded file is saved on the remote SFTP server with the original file name.
- If the specified *remote-filename* is the same as an existing file name on the SFTP server, the uploaded file overwrites the existing file on the server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Upload a file to the SFTP server.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> put wm.cfg
local file: wm.cfg --->  Remote file: /wm.cfg
Info: Uploading file successfully ended.
```

Related Topics

3.11.34 get (SFTP client view)

3.11.47 pwd (FTP client view)

Function

The **pwd** command displays the FTP client's working directory on the remote FTP server.

Format

pwd

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

After logging in to the FTP server, you can run the **pwd** command to display the FTP client's working directory on the remote FTP server.

If the displayed working directory is incorrect, you can run the **cd** command to change the FTP client's working directory on the remote FTP server.

Example

Display the FTP client's working directory on the remote FTP server.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
```

```
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] pwd
257 "/" is current directory.
```

Related Topics

3.11.26 ftp

3.11.48 pwd (SFTP client view)

Function

The **pwd** command displays the SFTP client's working directory on the remote FTP server.

Format

pwd

Parameters

None

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

After logging in to the SFTP server, you can run the **pwd** command to display the SFTP client's working directory on the remote SFTP server.

If the displayed working directory is incorrect, you can run the **cd** command to change the SFTP client's working directory on the remote SFTP server.

Example

Display the SFTP client's working directory on the remote SFTP server.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> pwd
/
sftp-client> cd test
```

```
Current directory is:
/test
sftp-client> pwd
/test
```

Related Topics

3.11.5 cd (SFTP client view)

3.11.49 pwd (user view)

Function

The **pwd** command displays the current working directory.

Format

pwd

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **pwd** command in any directory to display the current working directory. To change the current working directory, you can run the **cd** command.

Example

Display the current working directory.

```
<Huawei> pwd
flash:/test
```

Related Topics

3.11.13 dir (user view)

3.11.6 cd (user view)

3.11.50 remotehelp

Function

The **remotehelp** command displays the help information about an FTP command when the FTP client and server are connected.

Format

remotehelp [*command*]

Parameters

Parameter	Description	Value
command	Specifies the FTP command.	The value is a string of 1 to 16 characters.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **remotehelp** command to display the help information about an FTP command.

- The help information is provided by the remote server. Different remote servers may provide different help information for an FTP command.
- The help information can be displayed for FTP commands **user**, **pass**, **cwd**, **cdup**, **quit**, **port**, **pasv**, **type**, **retr**, **stor**, **dele**, **rmd**, **mkd**, **pwd**, **list**, **nlst**, **syst**, **help**, **xcup**, **xcwd**, **xmkd**, **xpwd**, and **xrmd**.

Example

Display the syntax of the command **cdup**.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] remotehelp
214-The following commands are recognized (* =>'s unimplemented).
  USER   PORT   STOR   MSAM*   RNTO   NLST   MKD   CDUP
  PASS   PASV   APPE   MRSQ*   ABOR   SITE*  XMKD  XCUP
  ACCT   TYPE   MLFL*  MRCP*   DELE   SYST   RMD   STOU
  SMNT*  STRU   MAIL*  ALLO*   CWD    STAT   XRMD  SIZE*
  REIN   MODE   MSND*  REST*   XCWD   HELP   PWD   MDTM*
  QUIT   RETR   MSOM*  RNFR    LIST   NOOP   XPWD
214 Direct comments about WFTPD to alun@texis.com.

[Huawei-ftp] remotehelp cdup
214 Syntax: CDUP <change to parent directory>.
```

3.11.51 remove (SFTP client view)

Function

The **remove** command deletes specified files from the remote SFTP server.

Format

remove *remote-filename* &<1-10>

Parameters

Parameter	Description	Value
remote-filename	Specifies the name of the file to be deleted from the remote SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can configure a maximum of 10 file names in the command and separate them using spaces and delete them at one time.
- If the file to be deleted is not in the current directory, you must specify the file path.

Example

Delete the file **3.txt** from the server and **backup1.txt** from the **test** directory.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> remove 3.txt test/backup1.txt
Warning: Make sure to remove these files? [y/n][n]:y
Info: Succeeded in removing the file /3.txt.
Info: Succeeded in removing the file /test/backup1.txt.
```

Related Topics

3.11.15 dir/ls (SFTP client view)

3.11.52 remove (user view)

Function

The **remove** command removes a storage device safely.

Format

remove *drive*

Parameters

Parameter	Description	Value
drive	Specifies the name of the storage device to be removed.	The value can be **usb0:**, **usb1:**, **sd0:**, or **usbotg:**.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **remove** command to safely remove a USB disk or an SD card from the device to prevent files in the device from being damaged.

Example

Remove the storage device USB0.

```
<Huawei> remove usb0:
...
Info: remove device usb0: successfully
```

3.11.53 rename (SFTP client view)

Function

The **rename** command renames a file or directory stored on the SFTP server.

Format

rename *old-name new-name*

Parameters

Parameter	Description	Value
old-name	Specifies the name of a file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces.
new-name	Specifies the new name of the file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

You can run the **rename** command to rename a file or directory.

Example

Rename the directory **yourtest** on the SFTP server.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> rename test/yourtest test/test
Warning: Rename /test/yourtest to /test/test? [y/n][n]:y
Info: Succeeded in renaming file.
sftp-client> cd test
Current directory is:
/test
sftp-client> dir
drwxrwxrwx   1 noone    nogroup        0 Mar 29 22:44 .
drwxrwxrwx   1 noone    nogroup        0 Mar 29 22:39 ..
drwxrwxrwx   1 noone    nogroup        0 Mar 24 00:04 test
-rwxrwxrwx   1 noone    nogroup     5736 Mar 24 18:38 backup.txt
```

Related Topics

3.11.51 remove (SFTP client view)

3.11.54 rename (user view)

Function

The **rename** command renames a file or folder.

Format

rename *old-name new-name*

Parameters

Parameter	Description	Settings
old-name	Specifies the name of a file or folder.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] filename** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.
new-name	Specifies the new name of the file or directory.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] filename** format. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name:

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

  For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- You must rename a file or directory in its source directory.
- If the renamed file or directory has the same name as an existing file or directory, an error message is displayed.
- If you specify *old-name* or *new-name* without specifying the file path, the file must be saved in your current working directory.

Example

Rename the directory **mytest** to **yourtest** in the directory **flash:/test/**.

```
<Huawei> pwd
flash:/test
<Huawei> rename mytest yourtest
Info: Rename flash:/test/mytest to flash:/test/yourtest ?(y/n)[n]:y
Info: Rename file flash:/test/mytest to flash:/test/yourtest ......Done
```

Rename the file **sample.txt** to **sample.bak**.

```
<Huawei> rename sample.txt sample.bak
Info: Rename flash:/sample.txt to flash:/sample.bak ?(y/n)[n] :y
Info: Rename file flash:/sample.txt to flash:/sample.bak .......Done
```

Related Topics

3.11.49 pwd (user view)

3.11.55 reset recycle-bin

Function

The **reset recycle-bin** command permanently deletes files from the recycle bin.

Format

reset recycle-bin [*filename* | *devicename*]

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be deleted.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name. The wildcard (*) character is supported.
devicename	Specifies the storage device name.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you run the **delete** command without specifying the **/unreserved** parameter, the file is moved to the recycle bin and still occupies the memory. To free up the space, you can run the **reset recycle-bin** command to permanently delete the file from the recycle bin.

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

  For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- You can run the **dir /all** command to display all files that are moved to the recycle bin from the current directory, and file names are displayed in square brackets ([ ]).
- If you delete a specified storage device, all files in the root directory of the storage device are deleted.
- If you run the **reset recycle-bin** command directly, all files that are moved to the recycle bin from the current directory are permanently deleted.

Example

Delete the file **test.txt** that is moved to the recycle bin from the directory **test**.

```
<Huawei> reset recycle-bin flash:/test/test.txt
Info: Squeeze flash:/test/test.txt?(y/n)[n]:y
Info: Cleared file flash:/test/test.txt.
```

Delete files that are moved to the recycle bin from the current directory.

```
<Huawei> pwd
flash:/test
<Huawei> reset recycle-bin
Info: Squeeze flash:/test/backup.zip?(y/n)[n]:y
Info: Cleared file flash:/test/backup.zip.
Info: Squeeze flash:/test/backup1.zip?(y/n)[n]:y
Info: Cleared file flash:/test/backup1.zip.
```

Related Topics

3.11.12 delete (user view)
3.11.13 dir (user view)

3.11.56 rmdir (FTP client view)

Function

The **rmdir** command deletes a specified directory from the remote FTP server.

Format

rmdir *remote-directory*

Parameters

Parameter	Description	Value
remote-directory	Specifies a directory or path on the FTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **rmdir** command to delete a specified directory from the remote FTP server.

Precautions

- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- If no path is specified when you delete a subdirectory, the subdirectory is deleted from the current directory.
- The directory is deleted from the FTP server rather than the FTP client.

Example

Delete the directory **d:/temp1** from the remote FTP server.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] rmdir d:/temp1
250 'D:\temp1': directory removed.
```

Related Topics

3.11.14 dir/ls (FTP client view)
3.11.38 mkdir (FTP client view)

3.11.57 rmdir (user view)

Function

The **rmdir** command deletes a specified directory from the storage device.

Format

rmdir *directory*

Parameters

Parameter	Description	Value
directory	Specifies a directory or directory and its path.	The value is a string of case-insensitive characters in the **[drive] [path] directory** format. The absolute path length ranges from 1 to 64, while the directory name length ranges from 1 to 15. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. Characters such as ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only the AR3200 series supports dual SRUs.

For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- A deleted directory and its files cannot be restored from the recycle bin.

Example

Delete the directory **test** from the current directory.

```
<Huawei> rmdir test
Remove directory flash:/test?(y/n)[n]:y
Info: Removing directory flash:/test....Done!
```

Related Topics

3.11.40 mkdir (User view)

3.11.58 rmdir (SFTP client view)

Function

The **rmdir** command deletes a specified directory from the remote SFTP server.

Format

rmdir *remote-directory* &<1-10>

Parameters

Parameter	Description	Value
remote-directory	Specifies the name of a file on the SFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

SFTP client view

Default Level

3: Management level

Usage Guidelines

- You can configure a maximum of 10 file names in the command and separate them using spaces and delete them at one time.
- Before running the **rmdir** command to delete a directory, you must delete all files and subdirectories from the directory.
- If the directory to be deleted is not in the current directory, you must specify the file path.

Example

Delete the directory **1** from the current directory, and the directory **2** from the **test** directory.

```
<Huawei> system-view
[Huawei] sftp 10.137.217.201
Please input the username:admin
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201 ...
Enter password:
sftp-client> rmdir 1 test/2
Warning: Make sure to remove these directories? [Y/N]:y
Info: Succeeded in removing the directory /test/1.
Info: Succeeded in removing the directory /test/test/2.
```

Related Topics

3.11.51 remove (SFTP client view)

3.11.59 set default ftp-directory

Function

The **set default ftp-directory** command configures the default FTP working directory.

The **undo set default ftp-directory** command disables the default FTP working directory.

By default, no default FTP working directory is configured.

Format

set default ftp-directory *directory*

undo set default ftp-directory

Parameters

Parameter	Description	Value
directory	Specify the default FTP working directory.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **set default ftp-directory** command to configure a default FTP working directory for all FTP users at one time.

Precautions

- The **set default ftp-directory** command takes effect only when the device functions as an FTP server and the user function as an FTP client.
- You can run the **local-user ftp-directory** command to configure an authorized working directory for a local user.
- If you have configured the FTP working directory by running the **local-user ftp-directory** command, you must use this FTP working directory.
- You can run the **lcd** command to view the working directory of FTP users.
- If no FTP working directory is specified on the device, FTP users cannot log in to the device.

Example

Set the default FTP working directory to **flash:/**.

```
<Huawei> system-view
[Huawei] set default ftp-directory flash:/
```

3.11.60 set default tftp-directory

Function

The **set default tftp-directory** command configures a working directory for the TFTP server.

The **undo set default tftp-directory** command deletes the working directory of the TFTP server.

By default, no working directory is configured for the TFTP server.

Format

set default tftp-directory *directory*

undo set default tftp-directory

Parameters

Parameter	Description	Value
directory	Specifies the working directory for the TFTP server.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

You need to configure a working directory for the TFTP server on the device. After that, TFTP clients can obtain files from the specified working directory.

Example

Set the working directory of the TFTP server to flash:.

```
<Huawei> system-view
[Huawei] set default tftp-directory flash:
```

Related Topics

3.11.68 tftp server enable

3.11.61 set net-manager vpn-instance

Function

The **set net-manager vpn-instance** command configures the default VPN instance that the NMS uses on the device.

The **undo set net-manager vpn-instance** command deletes the default VPN instance from the device.

By default, no VPN instance is configured on the device.

Format

set net-manager vpn-instance *vpn-instance-name*

undo set net-manager vpn-instance

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the default VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the NMS manages devices on the VPN network, you need to send the device information to the NMS using the VPN instance.

You can run the **set net-manager vpn-instance** command to configure the default VPN instance for the NMS to manage the device so that the device can use this VPN instance to communicate with the NMS.

Precautions

- Before running the **set net-manager vpn-instance** command, you must create VPN instances.
- After running this command, you can successfully run file transfer commands that you have configured based on the FTP, SFTP commands only in the default VPN instance.
- If the host has been configured as a log host, the NMS can receive device logs from the default VPN instance.

Example

Set the default VPN instance to v1.

```
<Huawei> system-view
[Huawei] set net-manager vpn-instance v1
```

Related Topics

3.11.26 ftp

3.11.62 sftp

Function

The **sftp** command connects the device to the SSH server so that you can manage files that are stored on the SFTP server.

Format

Connect the SFTP client to the SFTP server based on IPv4.

sftp [**-a** *source-address* | **-i** *interface-type interface-number*] *host-ip* [*port*] [[**public-net** | **-vpn-instance** *vpn-instance-name*] | [**identity-key** { **rsa** | **ecc** }] | [**user-identity-key** { **rsa** | **ecc** }] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_stoc_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | **sha2_256** | **sha2_256_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | **sha2_256** | **sha2_256_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

Connect the SFTP client to the SFTP server based on IPv6.

sftp ipv6 [**-a** *source-address*] *host-ipv6* [**-oi** *interface-type interface-number*] [*port*] [[**-vpn6-instance** *vpn-instance-name*] | [**identity-key** { **rsa** | **ecc** }] | [**user-identity-key** { **rsa** | **ecc** }] | [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] | [**prefer_ctos_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_stoc_cipher** { **3des** | **aes128** | **aes128-ctr** | **aes192-ctr** | **aes256-ctr** }] | [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | **sha2_256** | **sha2_256_96** }] | [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** | **sha2_256** | **sha2_256_96** }]] * [**-ki** *aliveinterval* [**-kc** *alivecountmax*]]

Parameters

Parameter	Description	Value
ipv6	Specifies an IPv6 address.	-
-a *source-address*	Specifies the source IP address for connecting to the SFTP client. You are advised to use the loopback interface IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-i *interface-type interface-number*	Specifies the source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the SFTP connection cannot be set up.	-
host-ip	Specifies the IP address or host name of the remote IPv4 SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
host-ipv6	Specifies the IPv6 address or host name of the remote IPv6 SFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
-oi *interface-type interface-number*	Specifies an outbound interface on the local device. If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.	-
port	Specifies the port number of the SSH server.	The value is an integer that ranges from ranges from 1 to 65535. The default port number is 22.
public-net	Specifies the SFTP server on the public network. You must set the **public-net** parameter when the SFTP server IP address is a public network IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-vpn-instance *vpn-instance-name*	Name of the VPN instance where the IPv4 SFTP server is located.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
-vpn6-instance *vpn-instance-name*	Name of the VPN instance where the IPv6 SFTP server is located.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
identity-key	Specifies the public key for server authentication.	The public key algorithm include RSA and ECC.
user-identity-key	Specifies the public key algorithm for the client authentication.	The public key algorithm include RSA and ECC. **NOTE** If the **user-identity-key** parameter is not used, RSA authentication is used by default. You can specify ECC authentication using the **user-identity-key** parameter.
prefer_kex	Specifies the preferred key exchange algorithm. The dh_group1 and dh_exchange_group algorithms are supported currently.	The default key exchange algorithm is dh_group1.
prefer_ctos_cipher	Specify an encryption algorithm for transmitting data from the client to the server.	Encryption algorithms **3des**, **aes128**, **aes128-ctr**, **aes192-ctr**, and **aes256-ctr** are supported currently. The default encryption algorithm is aes128.
prefer_stoc_cipher	Specify an encryption algorithm for transmitting data from the server to the client.	Encryption algorithms **3des**, **aes128**, **aes128-ctr**, **aes192-ctr**, and **aes256-ctr** are supported currently. The default encryption algorithm is aes128.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
prefer_ctos_hmac	Specify an HMAC algorithm for transmitting data from the client to the server.	HMAC algorithms sha1, sha1_96, md5, sha2_256, sha2_256_96, and md5_96 are supported. The default HMAC algorithm is sha1_96.
prefer_stoc_hmac	Specify an HMAC algorithm for transmitting data from the server to the client.	HMAC algorithms sha1, sha1_96, md5, sha2_256, sha2_256_96, and md5_96 are supported. The default HMAC algorithm is sha1_96.
-ki *aliveinterval*	Specifies the interval for sending keepalive packets when no packet is received in reply.	The value is an integer that ranges from 1 to 3600, in seconds.
-kc *alivecountmax*	Specifies the times for sending keepalive packets when no packet is received in reply.	The value is an integer that ranges from 3 to 10. The default value is 5.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SFTP is short for SSH FTP that is a secure FTP protocol. SFTP is on the basis of SSH. It ensures that users can log in to a remote device securely for file management and transmission, and enhances the security in data transmission. In addition, you can log in to a remote SSH server from the device that functions as an SFTP client.

When the connection between the SFTP server and client fails, the SFTP client must detect the fault in time and disconnect from the SFTP server. To ensure this, before being connected to the server in SFTP mode, the client must be configured with the interval and times for sending the keepalive packet when no packet is received in reply. If the client receives no packet in reply within the specified interval, the client sends the keepalive packet to the server again. If the maximum number of times that the client sends keepalive packets exceeds the specified value, the client releases the connection. By default, when no packet is received, the function for sending keepalive packets is not enabled.

Precautions

- You can set the source IP address to the source or destination IP address in the ACL rule when the **-a** or **-i** parameter is specified. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.
- The SSH client can log in to the SSH server with no port number specified only when the port number of the SSH server is 22. If the SSH server uses another port, the port number must be specified when SSH clients log in to the SSH server.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.
- If you cannot run the **sftp** command successfully when you configured the ACL on the SFTP client, or when the TCP connection fails, an error message is displayed indicating that the SFTP client cannot be connected to the server.
- 3DES, MD5, MD5_96, SHA1, and SHA1_96 encryption algorithm cannot ensure security. AES128, AES128-CTR, AES192-CTR sha2_256, sha2_256_96 or AES256-CTR encryption algorithm is recommended.

Example

Set the current listening port number of the SSH server to 1025, and specify the SFTP client on the public network and the SSH server on the private network.

```
<Huawei> system-view
[Huawei] sftp 10.164.39.223 1025 -vpn-instance ssh
Please input the username: client001
Trying 10.164.39.223 ...
Press CTRL+K to abort
Enter password:
sftp-client>
```

Set keepalive parameters when the client is connected to the server in SFTP mode.

```
<Huawei> system-view
[Huawei] sftp 10.164.39.223 -ki 10 -kc 4
Please input the username: client001
Trying 10.164.39.223 ...
Press CTRL+K to abort
Enter password:
sftp-client>
```

Related Topics

3.11.64 sftp server enable

3.9.38 ssh server port

3.11.63 sftp client-source

Function

The **sftp client-source** command specifies the source IP address for the SFTP client to send packets.

The **undo sftp client-source** command restores the default source IP address for the SFTP client to send packets.

The default source IP address for the SFTP client to send packets is 0.0.0.0.

Format

sftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo sftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Specifies the source interface. You are advised to use the loopback interface. The IP address configured for the source interface is the source IP address for sending packets. If no IP address is configured for the source interface, the FTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status

impact, filters incoming and outgoing packets, and implements security authentication.

Precautions

- You can query the source IP address or primary IP address of the source interface for the SFTP connection on the SFTP server.
- The **sftp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **sftp client-source** command. If you specify source addresses in the **sftp client-source** and **sftp** commands, the source IP address specified in the **sftp** command is used for data communication. The source address specified in the **sftp client-source** command applies to all SFTP connections. The source address specified in the **sftp** command applies only to the current SFTP connection.
- If the specified source interface has been bound to a VPN instance, the client is automatically bound to the same VPN instance.

Example

Set the source IP address of the SFTP client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] sftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the SFTP client to 10.1.1.1.
```

Related Topics

3.11.62 sftp

3.11.20 display sftp-client

3.11.64 sftp server enable

Function

The **sftp server enable** command enables the SFTP service on the SSH server.

The **undo sftp server enable** command disables the SFTP service on the SSH server.

By default, the SFTP service is disabled.

Format

sftp server enable

undo sftp server enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To connect the client to the SSH server to transfer files in SFTP mode, you must first enable the SFTP server on the SSH server.

Example

Enable the SFTP service.

```
<Huawei> system-view
[Huawei] sftp server enable
Info: Succeeded in starting the SFTP server.
```

Disable the SFTP service.

```
<Huawei> system-view
[Huawei] undo sftp server enable
Info: Succeeded in closing the SFTP server.
```

Related Topics

3.11.62 sftp

3.11.65 tftp

Function

The **tftp** command uploads a file to the TFTP server or downloads a file to the local device.

Format

Upload a file to the TFTP server or download a file to the local device based on the IPv4 address

tftp [**-a** *source-ip-address* | **-i** *interface-type interface-number*] *tftp-server* [**public-net** | **vpn-instance** *vpn-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]

Upload a file to the TFTP server or download a file to the local device based on the IPv6 address

tftp ipv6 [**-a** *source-ip-address*] *tftp-server-ipv6* [**-oi** *interface-type interface-number*] [**vpn6-instance** *vpn6-instance-name*] { **get** | **put** } *source-filename* [*destination-filename*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address for connecting to the TFTP client. You are advised to use the loopback interface IP address.	-
-i *interface-type interface-number*	Specifies the source interface used by the TFTP client to set up connections. It consists of the interface type and number. It is recommended that you specify a loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the TFTP connection cannot be set up.	-
-oi *interface-type interface-number*	Specifies an outbound interface on the local device.	If the remote host uses an IPv6 address, you must specify the outbound interface on the local device.
tftp-server	Specifies the IPv4 address or host name for the TFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
tftp-server-ipv6	Specifies the IPv6 address of the IPv6 TFTP server.	The value is a string of 1 to 255 case-insensitive characters without spaces.
public-net	Specifies the TFTP server on the public network.	-
vpn-instance *vpn-instance-name*	Name of the VPN instance where the IPv4 TFTP server is located.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn6-instance *vpn6-instance-name*	Name of the VPN instance where the IPv6 TFTP server is located.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
get	Download a file.	-
put	Upload a file.	-
source-filename	Specifies the source file name.	The value is a string of 1 to 64 case-insensitive characters without spaces.
destination-filename	Specifies the directory and name of a destination file.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading the system, you can run the **tftp** command to upload an important file to the TFTP server or download a system software to the local device.

Precautions

- When you run the **tftp** command to upload a file to the TFTP server in TFTP mode, files are transferred in binary mode by default. The tftp does not support the ASCII mode for file transfer.
- After specifying a source IP address, you can use this IP address to communicate with the server and implement packet filtering to ensure data security.
- You can run the **set net-manager vpn-instance** command to configure the NMS management VPN instance before running the **open** command to connect the FTP client and server.
  - If **public-net** or **vpn-instance** is not specified, the FTP client accesses the FTP server in the VPN instance managed by the NMS.
  - If **public-net** is specified, the FTP client accesses the FTP server on the public network.
  - If **vpn-instance** *vpn-instance-name* is specified, the FTP client accesses the FTP server in a specified VPN instance.

Example

Download file **vrpcfg.txt** from the root directory of the TFTP server to the local device. The IP address of the TFTP server is 10.1.1.1. Save the downloaded file to the local device as file **vrpcfg.bak**.

```
<Huawei> tftp 10.1.1.1 get vrpcfg.txt flash:/vrpcfg.bak
```

Upload file **vrpcfg.txt** from the root directory of the storage device to the default directory of the TFTP server. The IP address of the TFTP server is 10.1.1.1. Save file **vrpcfg.txt** on the TFTP server as file **vrpcfg.bak**.

```
<Huawei> tftp 10.1.1.1 put flash:/vrpcfg.txt vrpcfg.bak
```

Obtain the link local IP address and interface name from the TFTP server.

```
<Huawei> tftp ipv6 fc00::1 -oi gigabitethernet 1/0/0 get file1 file2
```

Related Topics

3.11.67 tftp-server acl

3.11.66 tftp client-source

Function

The **tftp client-source** command specifies the source IP address for the TFTP client to send packets.

The **undo tftp client-source** command restores the default source IP address for the TFTP client to send packets.

The default source IP address for the TFTP client to send packets is 0.0.0.0.

Format

tftp client-source { **-a** *source-ip-address* | **-i** *interface-type interface-number* }

undo tftp client-source

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source IP address of the TFTP client. You are advised to use the loopback interface IP address.	The value is in dotted decimal notation.
-i *interface-type interface-number*	Source interface type and ID. You are advised to use the loopback interface. The IP address configured for this interface is the source IP address for sending packets. If no IP address is configured for the source interface, the TFTP connection cannot be set up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If no source IP address is specified, the client uses the source IP address that the router specifies to send packets. The source IP address must be configured for an interface with stable performance. The loopback interface is recommended. Using the loopback interface as the source interface simplifies the ACL rule and security policy configuration. This shields the IP address differences and interface status impact, filters incoming and outgoing packets, and implements security authentication.

Precautions

- The **tftp** command also configures the source IP address whose priority is higher than that of the source IP address specified in the **tftp client-source** command. If you specify source addresses in the **tftp client-source** and **tftp** commands, the source IP address specified in the **tftp** command is used for data communication. The source address specified in the **tftp client-source** command applies to all TFTP connections. The source address specified in the **tftp** command applies only to the current TFTP connection.
- You can query the source IP address or source interface IP address specified in the TFTP connection on the TFTP server.
- If the specified source interface has been bound to a VPN instance, the client is automatically bound to the same VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the source IP address of the TFTP client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] tftp client-source -a 10.1.1.1
Info: Succeeded in setting the source address of the TFTP client to 10.1.1.1.
```

Related Topics

3.11.65 tftp
3.11.21 display tftp-client

3.11.67 tftp-server acl

Function

The **tftp-server acl** command specifies the ACL number for the local device so that the device can access TFTP servers with the same ACL number.

The **undo tftp-server acl** command deletes the ACL number from the local device.

By default, no ACL number is specified on the local client.

Format

tftp-server acl *acl-number*

undo tftp-server acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure the security of the local device, you need to run the **tftp-server acl** command to specify an ACL to specify TFTP servers that the local device can access.

Precautions

- The **tftp-server acl** command takes effect only after you run the **rule** command to configure the ACL rule. If no ACL rule is configured, the local device can access a specified TFTP server in TFTP mode.
- The TFTP supports only the basic ACL whose number ranges from 2000 to 2999.

Example

Allow the local device to the access the TFTP server whose ACL number is 2000.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 10.10.10.1 0
[Huawei-acl-basic-2000] quit
[Huawei] tftp-server acl 2000
```

Related Topics

3.11.65 tftp

3.11.68 tftp server enable

Function

The **tftp server enable** command enables the TFTP server function on the device.

The **undo tftp server enable** command disables the TFTP server function on the device.

By default, the TFTP server function is disabled.

Format

tftp server enable

undo tftp server enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To allow a local client to remotely manage files on the device using TFTP, you must run this command to enable the TFTP server function on the device.

NOTE

The TFTP protocol has security risks; therefore, SFTPv2 is recommended for file management.

Prerequisite

The TFTP working directory has been configured by running the **set default tftp-directory** *directory* command.

Example

Enable the TFTP server function.

```
<Huawei> system-view
[Huawei] set default tftp-directory flash:
[Huawei] tftp server enable
```

Related Topics

3.11.60 set default tftp-directory

3.11.69 tftp server port

Function

The **tftp server port** command configures the port number of the TFTP server.

The **undo tftp server port** command restores the default port number of the TFTP server.

By default, the port number of the TFTP server is 69.

Format

tftp server port *port-number*

undo tftp server port

Parameters

Parameter	Description	Value
port-number	Specifies the port number of the TFTP server.	The value is an integer that ranges from 69 or 1025 to 55535. The default value is 69.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the port number of the TFTP server is 69. Users can directly log in to the device using the default port number. Attackers may access the default port, consuming bandwidth, deteriorating server performance, and causing authorized users unable to access the server. You can run this command to configure another port number for the TFTP server. This can prevent attacks to the TFTP server because attackers cannot obtain the newly configured port number.

Prerequisite

The TFTP service has been disabled by running the **undo tftp server enable** command.

Precautions

- When the port number of the TFTP server is 69, a TFTP client can connect to the TFTP server without the need to specify a port number. When the port number of the TFTP server is not 69, you need to specify a port number for the TFTP client before it can connect to the TFTP server, and the specified client port number must be the same as the server port number.
- After running this command to configure a new port number, you must run the **tftp server enable** command to enable the TFTP server before the modified port number takes effect.

Example

Set the port number of the TFTP server to 1028.

```
<Huawei> system-view
[Huawei] tftp server port 1028
```

Related Topics

3.11.68 tftp server enable

3.11.70 tftp server timeout

Function

The **tftp server timeout** command configures a packet timeout period for a TFTP server.

The **undo tftp server timeout** command restores the default packet timeout period for a TFTP server.

By default, the packet timeout period of a TFTP server is 5 seconds.

Format

tftp server timeout *timeout-second*

undo tftp server timeout

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
timeout-second	Specifies the packet timeout period of a TFTP server.	The value an integer that ranges from 1 to 300, in seconds. The default value is 5s.

Views

System view

Default Level

3: Management level

Usage Guidelines

If the server does not receive any response within 5 seconds after sending a packet to a client, it considers that the packet times out. The TFTP server will resend a packet twice. If the packet times out three times, the TFTP server disconnects the TFTP connection.

Example

Set the packet timeout period of a TFTP server to 10s.

```
<Huawei> system-view
[Huawei] tftp server timeout 10
```

Related Topics

3.11.68 tftp server enable

3.11.71 undelete

Function

The **undelete** command restores a file that has been has been temporally deleted and moved to the recycle bin.

Format

undelete { *filename* | *devicename* }

Parameters

Parameter	Description	Value
filename	Specifies the name of a file to be restored.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.
devicename	Specifies the storage device name.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **undelete** command to restore a file that has been temporally deleted and moved to the recycle bin. However, files that are permanently deleted by running the **delete** or **reset recycle-bin** command with the **/unreserved** parameter cannot be restored.

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Like *devicename*, **drive** specifies the storage device name.

Precautions

- To display information about a temporally deleted file, run the **dir /all** command. The file name is displayed in square brackets ([ ]).
- If the name of a file is the same as an existing directory, the file cannot be restored. If the destination file has the same name as an existing file, the system prompts you whether to overwrite the existing file. The system prompt is displayed only when **file prompt** is set to **alert**.

Example

Restore file **sample.bak** from the recycle bin.

```
<Huawei> undelete sample.bak
Info: Undelete flash:/sample.bak ?(y/n)[n]:y
Info: Undeleted file flash:/sample.bak.
```

Restore a file that has been moved from the root directory to the recycle bin.

```
<Huawei> undelete flash:
Info: Undelete flash:/test.txt?(y/n)[n]:y
Info: Undeleted file flash:/test.txt.
Info: Undelete flash:/rr.bak?(y/n)[n]:y
Info: Undeleted file flash:/rr.bak.
```

Related Topics

3.11.12 delete (user view)

3.11.13 dir (user view)

3.11.24 file prompt

3.11.55 reset recycle-bin

3.11.72 unzip

Function

The **unzip** command decompresses a file.

Format

unzip *source-filename destination-filename*

Parameters

Parameter	Description	Value
source-filename	Specifies the name of a source file to be decompressed.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.
destination-filename	Specifies the name of a destination file that is decompressed.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can decompress files, especially log files that are stored on the storage device and run the **more** command to query the file.

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.

- flash: root directory of the flash memory on the master SRU.
- slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
- slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

NOTE

Only the AR3200 series supports dual SRUs.

For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file path is specified while the file name is not specified, the designation file name is the same as the source file name.
- The source file persists after being decompressed.
- The compressed file must be a .zip file. If a file to be decompressed is not a zip file, the system displays an error message during decompression.
- The source file must be a single file. If you attempt to decompress a directory or multiple files, the decompression cannot succeed.

Example

Decompress log file **syslogfile-2012-02-27-17-47-50.zip** that are stored in the **syslogfile** directory and save it to the root directory as file **log.txt**.

```
<Huawei> pwd
flash:/syslogfile
<Huawei> unzip syslogfile-2012-02-27-17-47-50.zip flash:/log.txt
Info: Extract flash:/syslogfile/syslogfile-2012-02-27-17-47-50.zip to flash:/log.txt?(y/n)[n]:y
100%  complete
Info: Decompressed file flash:/syslogfile/syslogfile-2012-02-27-17-47-50.zip flash:/log.txt.
```

Related Topics

3.11.13 dir (user view)

3.11.49 pwd (user view)

3.11.73 user

Function

The **user** command changes the current FTP user when the local device is connected to the FTP server.

Format

user *user-name* [*password*]

Parameters

Parameter	Description	Value
user-name	Specifies the name of a login user.	The value is a string of 1 to 64 case-insensitive characters without space.
password	Specifies the login password.	The value is a string of 1 to 16 case-sensitive characters without space, single quotation mark, or question mark.

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **user** command to change the current user on the FTP server.

Precautions

After you run the **user** command to change the current user, a new FTP connection is set up, which is the same as that you specify in the **ftp** command.

Example

Log in to the FTP server using the user name **tom**.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] user tom
331 Password required for tom.
Enter password:
230 User logged in.
```

Related Topics

3.11.26 ftp

3.11.74 verbose

Function

The **verbose** command enables the verbose function on the FTP client.

The **undo verbose** command disables the verbose function.

By default, the verbose function is enabled.

Format

verbose

undo verbose

Parameters

None

Views

FTP client view

Default Level

3: Management level

Usage Guidelines

After the verbose function is enabled, all FTP response messages are displayed on the FTP client.

Example

Enable the verbose function.

```
<Huawei> ftp 10.137.217.201
Trying 10.137.217.201 ...
Press CTRL+K to abort
Connected to 10.137.217.201.
220 FTP service ready.
User(10.137.217.201:(none)):huawei
331 Password required for huawei.
Enter password:
230 User logged in.
[Huawei-ftp] verbose
Info: Succeeded in switching verbose on.
[Huawei-ftp] get h1.txt
200 Port command okay.
150 Opening ASCII mode data connection for h1.txt.

226 Transfer complete.
FTP: 69 byte(s) received in 0.160 second(s) 431.25byte(s)/sec.
```

Disable the verbose function.

```
[Huawei-ftp] undo verbose
Info: Succeeded in switching verbose off.
[Huawei-ftp] get h1.txt

FTP: 69 byte(s) received in 0.150 second(s) 460.00byte(s)/sec.
```

Related Topics

3.11.35 get (FTP client view)

3.11.45 put (FTP client view)

3.11.75 zip

Function

The **zip** command compresses a file.

Format

zip *source-filename destination-filename*

Parameters

Parameter	Description	Value
source-filename	Specifies the name of a source file to be compressed.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.
destination-filename	Specifies the name of a destination file that is compressed.	The value is a string of 1 to 64 case-insensitive characters without spaces in the **[drive] [path] file name** format. When quotation marks are used around the string, spaces are allowed in the string. In the preceding parameter, **drive** specifies the storage device name, and **path** specifies the directory and subdirectory. You are advised to add : and / between the storage device name and directory. Characters ~, *, /, \, :, ', " cannot be used in the directory name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The following describes the drive name.

- **drive** is the storage device and is named as follows:
  - sd1: root directory of the Micro SD card on the master SRU.
  - flash: root directory of the flash memory on the master SRU.
  - slave#sd1: root directory of the Micro SD card on the slave SRU. If the device has no slave SRU, this drive is unavailable.
  - slave#flash: root directory of the flash memory on the slave SRU. If the device has no slave SRU, this drive is unavailable.

  NOTE

  Only the AR3200 series supports dual SRUs.

  For the storage device type and specifications supported by the device, see "Technical Specifications" in the ***Hardware Description***.

The path can be an absolute path or relative path.

- **flash:/my/test/** is an absolute path.
- **selftest/** is a path relative to the current working directory and indicates the selftest directory in the current working directory.

Precautions

- If the destination file path is specified while the file name is not specified, the designation file name is the same as the source file name.
- The source file persists after being compressed.
- Directories cannot be compressed.

Example

Compress file **log.txt** that is stored in the root directory and save it to the **test** directory as file **log.zip**.

```
<Huawei> dir
Directory of flash:/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-           155  Dec 02 2011 01:28:48   log.txt
    1  -rw-         9,870  Oct 01 2011 00:22:46   patch.pat
    2  drw-             -  Mar 22 2012 00:00:48   test
    3  -rw-           836  Dec 22 2011 16:55:46   rr.dat
...

1,927,220 KB total (1,130,464 KB free)
<Huawei> zip log.txt flash:/test/log.zip
Info: Zip flash:/log.txt flash:/test/log.zip? (y/n)[n]:y
100%  complete
Info: Compressed file flash:/log.txt flash:/test/log.zip.
<Huawei> cd test
<Huawei> dir
Directory of flash:/test/

  Idx  Attr     Size(Byte)  Date        Time(LMT)  FileName
    0  -rw-           836  Mar 20 2012 19:49:14   test
    1  -rw-           239  Mar 22 2012 20:57:38   test.txt
```

```
  2  -rw-        1,056  Dec 02 2011 01:28:48   log.txt
  3  -rw-          240  Mar 22 2012 21:23:46   log.zip

1,927,220 KB total (1,130,463 KB free)
```

Related Topics

3.11.13 dir (user view)

3.12 Configuring System Startup Commands

3.12.1 autosave interval

Function

The **autosave interval** command sets the interval for automatically saving system configuration data.

Format

autosave interval { *value* | *time* | **configuration** *time* }

Parameters

Parameter	Description	Value
value	Configures the automatic save function. The automatic save function is classified into two types: saving configuration data automatically and saving modified data automatically. When the value is on, the two save functions are enabled. When the value is off, the two save functions are disabled and the data needs to be saved manually.	The value is an enumerated value that can be on or off. The default value is off.
time	Indicates the interval for automatically saving the configuration data. If an interval is configured, the configuration data is saved regardless of whether it is modified.	The value is an integer that ranges from 10 to 10080. The unit is minute. The default value is 1440 minutes.
configuration *time*	Indicates the interval for automatically saving the modified data. When the configuration data is modified, it is saved at the preset interval.	The value is an integer that ranges from 2 to 1440. The unit is minute. The default value is 30 minutes.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to set configuration data at preset intervals. When the interval is set, the system automatically saves the configuration data without requiring the command delivered by the network management system. The modified data can be saved in the storage device in real time and cannot be lost after system restart.

Precautions

- When the automatic save function is enabled, you can also run the **save** command to save the system configuration data manually. When the automatic save function is disabled, the system does not save data automatically and you need to run the **save** command to save the configured data.
- The automatic save function is disabled by default.
- After you run the **autosave interval** command, the frequent data save operation affects system performance. Do not set the automatic save interval to less than 1 hour. The automatic save interval of 24 hours or greater is recommended.
- The automatic save function specified by the **autosave interval** command cannot be enabled together with that specified by the **autosave time** command.

Example

Enable the automatic save function.

```
<Huawei> autosave interval on
  System autosave interval switch: on
  Autosave interval: 1440 minutes
  Autosave type: configuration file

  System autosave modified configuration switch: on
  Autosave interval: 30 minutes
  Autosave type: configuration file
```

Set the automatic save interval to 120 minutes.

```
<Huawei> autosave interval 120
  System autosave interval switch: on
  Autosave interval: 120 minutes
  Autosave type: configuration file
```

 Copyright © Huawei Technologies Co., Ltd.

Table 3-45 Description of the autosave interval command output

Item	Description
System autosave interval switch	Whether the device is enabled to automatically save system configuration data at the specified interval: ● on: The device is enabled to automatically save system configuration data at the specified interval. ● off: The device is disabled from automatically saving system configuration data at the specified interval.
Autosave interval	Specifies the interval for automatically saving configuration data. If an interval is configured, the configuration data is saved at intervals regardless of whether the data is changed.
Autosave type	Indicates that the type of file saved automatically is configuration file.
System autosave modified configuration switch	Indicates that the change to the configuration data is automatically saved. When the value is on, the function is enabled. When the value is off, the function is disabled.

Related Topics

3.12.2 autosave time

3.12.7 display autosave configuration

3.12.2 autosave time

Function

The **autosave time** command sets the automatic save time.

Format

autosave time { *value* | *time-value* }

Parameters

Parameter	Description	Value
value	Configures the device to save configuration data at a preset time.	Enumerated value. The options are as follows: ● on: The device is enabled to automatically save system configuration data at a preset time. ● off: The device is disabled from automatically saving system configuration data at a preset time. The default value is **off**.
time-value	Indicates the automatic save time after the device is enabled to automatically save system configuration data. After this parameter is configured, the system automatically saves the configuration data at intervals of the automatic save time.	The value ranges from 00:00:00 to 23:59:59. The default value is 00:00:00.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system can save configuration data at preset intervals or at the preset time. Run this command to set the automatic save time. When the time is set, the system automatically saves the configuration data without requiring the command delivered by the network management system. The modified data can be saved in the storage device in real time and cannot be lost after system restart.

Precautions

- When the device is enabled to automatically save system configuration data, the modified configuration is saved at the preset time. When the device is disabled from automatically saving system configuration data, the system does not save data automatically and you need to run the **save** command to save the configured data.
- The automatic save function specified by the **autosave time** command cannot be used with that specified by the **autosave interval** command.
- If data is frequently read from or written into the storage device, the lifespan of the storage medium is reduced. You are advised to disable the automatic save function immediately after the modified data is saved.

Example

Enable the device to automatically save system configuration data at intervals of the automatic save time.

```
<Huawei> autosave time on
  System autosave time switch: on
  Autosave time: 00:00:00
  Autosave type: configuration file
```

Set the automatic save time to 12:20:30.

```
<Huawei> autosave time 12:20:30
  System autosave time switch: on
  Autosave time: 12:20:30
  Autosave type: configuration file
```

Table 3-46 Description of the autosave time command output

Item	Description
System autosave time switch	Whether the device is enabled to automatically save system configuration data at the specified time: ● on: The device is enabled to automatically save system configuration data at the specified time. ● off: The device is disabled from automatically saving system configuration data at the specified time.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Autosave time	Automatic save time. The device saves system configuration data at intervals of the automatic save time no matter whether the configuration data changes.
Autosave type	Type of the file saved automatically.

Related Topics

3.12.1 autosave interval
3.12.7 display autosave configuration

3.12.3 clear reset-reason

Function

The **clear reset-reason** command clears the reset records of a device.

Format

clear reset-reason

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Clear the reset records of the device.

```
<Huawei> system-view
[Huawei] clear reset-reason
```

3.12.4 change default-password

Function

The **change default-password** command enables the function of changing AAA and Boot passwords when factory settings of a device are restored.

The **undo change default-password** command disables the function of changing AAA and Boot passwords when factory settings of a device are restored.

By default, the function of changing AAA and Boot passwords when factory settings of a device are restored is disabled,The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

Only the AR169EW, AR169EGW-L, AR161EW, AR161EW-M1, AR2204XE, and AR2204XE-DC support this command.

Format

change default-password

undo change default-password

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Prerequisites

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Usage Scenario

You can run the **change default-password** command to enable the function of changing AAA and Boot passwords when factory settings of a device are restored.

Precautions

The configuration takes effect immediately after the **change default-password** command is executed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the function of changing AAA and Boot passwords when factory settings of a device are restored.

```
<Huawei> system-view
[Huawei] change default-password
Info : The default password of boot has been changed.
Info : The default password of aaa has been changed.
Info : This operation can only be restored by command:undo change default-password.
```

Table 3-47 Description of the **change default-password** command output

Item	Description
Info : The default password of boot has been changed.	After the command is executed, the Boot password is changed. **NOTE** If the Boot password of the device is not set to the password in the prerequisite before the **change default-password** command is executed, the device does not display this information after you run this command.
Info : The default password of aaa has been changed.	After the command is executed, the AAA password is changed. **NOTE** If the AAA password of the device is not set to the password in the prerequisite before the **change default-password** command is executed, the device does not display this information after you run this command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Info : This operation can only be restored by command:undo change default-password.	After running the **change default-password** command, you can only run the **undo change default-password** command to disable the function of changing AAA and Boot passwords when factory settings of a device are restored. **NOTE** After running the **undo change default-password** command, you must restart the device using either of the following methods to make the configuration take effect. If the device enters the Boot mode after the **undo change default-password** command is executed and the device is restarted for the first time, the Boot password is still the password in the prerequisite. ● Run the **factory-configuration reset** command to restore the device to factory settings after the device is restarted, and then restart the device again. ● Hold down the RESET button to restart the device.

3.12.5 compare configuration

Function

The **compare configuration** compares whether the current configurations are identical with the next startup configuration file.

Format

compare configuration [*configuration-file* [*current-line-number save-line-number*]]

Parameters

Parameter	Description	Value
configuration-file	Specifies the name of the configuration file to be compared with the current configurations.	The value is a string of 5 to 64 case-insensitive characters without spaces.
current-line-number	Specifies the line number for comparison in the current configuration.	The value is an integer that ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
save-line-number	Specifies the line number for comparison in the saved configuration.	The value is an integer that ranges from 0 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If *current-line-number* and *save-line-number* are not specified, the configuration files are compared from the first lines. The two parameters can be specified to skip the differences that are found and continue the comparison.

When the difference is found using the **compare configuration** command, the different content in the current and saved configuration files is displayed. By default, 120 characters are displayed. If the different content from the start line to the end line contains less than 120 characters, only these characters are displayed.

Precautions

- The configuration file name extension must be .cfg or .zip.
- If *configuration-file* is not specified, the system compares whether the current configurations are identical with the next startup configuration file.
- If *configuration-file* is specified, the system compares whether the current configurations are identical with the specified startup configuration file.

Example

Compare whether the current configurations are identical with the next startup configuration file.

```
<Huawei> compare configuration
 The current configuration is not the same as the next startup configuration file.
 ====== configuration line 14 ======
 ftp server enable
#
 drop illegal-mac alarm
#
 vlan batch 10 to 11
#
 dot1x enable
#
set transceiver-monitoring disable
 ====== Configuration file line 14 ======
 drop illegal-mac alarm
#
 vlan batch 10 to 11
#
 dot1x enable
```

```
#
set transceiver-monitoring disable
```

Related Topics

3.12.21 save

3.12.6 diagnose verify enable

Function

The **diagnose verify enable** command enables the password authentication function for users who enter the diagnostic view.

The **diagnose verify disable** command disables the password authentication function for users who enter the diagnostic view.

By default, password authentication is not required for users who enter the diagnostic view.

NOTE

Only the AR161EW, AR169EGW-L, AR2204XE, and AR2204XE-DC support this command.

Format

diagnose verify enable

diagnose verify disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Password authentication is performed for users who enter the diagnostic view to ensure security. After the **diagnose verify enable** command is run in the system view, the system prompts you to enter the current Boot menu password. After the entered password is successfully verified, the password authentication function is successfully enabled for users who enter the diagnostic view. If password authentication is not required for users who enter the diagnostic view, after the **diagnose verify disable** command is run in the system view, the system prompts you to enter the current Boot menu password. After the entered password is successfully verified, the password authentication function is successfully disabled for users who enter the diagnostic view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the password authentication function for users who enter the diagnostic view.

```
<Huawei> system-view
[Huawei] diagnose verify enable
Please enter password:
Info: Set diagnose verify enable successfully.
```

3.12.7 display autosave configuration

Function

The **display autosave configuration** command displays the automatic save parameters of the configuration data.

Format

display autosave configuration

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command when you want to check whether the function for automatically saving configuration data is enabled, enable or disable the automatic save function, and modify the automatic save interval or time.

Precautions

- Run the **autosave time** command to set the time for automatically saving system configuration data.
- Run the **autosave interval** command to set the interval for automatically saving system configuration data.
- The frequent data save operation affects the lifespan of the system storage device. Do not set the automatic save interval to less than 1 hour. The automatic save interval of 24 hours or greater is recommended.

Example

Display the automatic save parameters configured in the system.

```
<Huawei> display autosave configuration
  System autosave interval switch: on
  Autosave interval: 120 minutes
  Autosave type: configuration file

  System autosave modified configuration switch: on
  Autosave interval: 30 minutes
  Autosave type: configuration file

  System autosave time switch: off
  Autosave time: 12:20:30
  Autosave type: configuration file
```

Table 3-48 Description of the display autosave configuration command output

Item	Description
System autosave interval switch	State of the automatic save function.
Autosave interval	Automatic save interval.
Autosave type	Type of the file that is automatically saved.
System autosave modified configuration switch	State of the function for automatically saving modified data.
System autosave time switch	State of the function for saving configuration data at the preset time.
Autosave time	Automatic save time.

Related Topics

3.12.21 save

3.12.2 autosave time

3.12.1 autosave interval

3.12.8 display current-configuration

Function

The **display current-configuration** command displays the currently running configuration.

This command does not display parameters that use default settings.

Format

display current-configuration [**configuration** [*configuration-type* [*configuration-instance*] **related**] | **controller** [*interface-type* [*interface-number*]] | **interface** [*interface-type* [*interface-number*]]] [**feature** *feature-name* [**filter** *filter-expression*] | **filter** *filter-expression*]

display current-configuration [**all** | **inactive** | [**simple**] [**section** *section*]]

Parameters

Parameter	Description	Value
configuration *configuration-type*	Specifies the configuration type.	The value is determined by the current system configurations. For example: ● system: system configuration ● user-interface: user interface configuration ● aaa: AAA configuration ● vpn-instance: VPN instance configuration ● ...
configuration-instance	Specifies a configuration instance.	The value is a string of 1 to 80 case-insensitive characters without spaces.
controller [*interface-type* [*interface-number*]]	Specifies a controller interface, for example, E1 control interface.	-
interface [*interface-type* [*interface-number*]]	Specifies an interface type.	-
feature *feature-name*	Specifies the configuration information about the specified feature.	-
filter *filter-expression*	Displays the configuration information that matches a regular expression.	The value is a string of 1 to 255 case-insensitive characters.
all	Displays all the configuration information.	-
inactive	Displays the offline configuration information.	-
simple	Displays the current simple configuration.	-
section *section*	Specifies the configurations to be obtained based on types.	The value is a string of 1 to 79 case-insensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

To check whether the configured parameters take effect, run the **display current-configuration** command. The parameters that do not take effect are not displayed.

The command output is relevant to user configuration. The command does not display the default configuration.

You can use a regular expression to filter the command output. For the regular expression rules, see "Filtering Command Outputs" in the *Huawei AR Series Access Routers Configuration Guide - Basic Configuration*.

If the configuration is in the offline state, the offline configuration is marked with * in the **display current-configuration all** and **display current-configuration inactive** command output.

Example

Display all configurations that include **vlan**.

```
<Huawei> display current-configuration | include vlan
vlan batch 10 77 88
 port trunk allow-pass vlan 10
```

Related Topics

3.12.21 save

3.12.20 reset saved-configuration

3.12.12 display saved-configuration

3.12.9 display factory-configuration

Function

The **display factory-configuration** command displays the factory configuration of the device.

Format

display factory-configuration

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the factory configuration of the device, including the HTTP and HTTPS server status, PKI domain name, SSL policy name and type, authorization scheme, accounting scheme, authentication mode, user priority, and allowed access type.

You can configure required basic information as the factory configuration and do not need to configure the basic information after restoring the factory configuration.

Factory settings of different devices may be different.

Example

Display the factory configuration of the Router.

```
<Huawei> display factory-configuration
#
vlan 1
#
 http server enable
 http secure-server ssl-policy default_policy
 http secure-server enable
#
ssl policy default_policy type server
 pki-realm default
#
aaa
 authentication-scheme default
 authorization-scheme default
 accounting-scheme default
 domain default
 domain default_admin
 local-user admin password cipher %^%#5d~9:M^ipCfL\iB)EQd>3Uwe%^%#
 local-user admin privilege level 15
 local-user admin service-type http telnet
#
interface Vlanif1
 ip address 192.168.1.1 255.255.255.0

#
user-interface con 0
user-interface vty 0
 authentication-mode aaa
 user privilege level 15
#
return
```

Table 3-49 Description of the **display factory-configuration** command output

Item	Description
vlan 1	The VLAN ID is 1.
http server enable	The HTTP server is enabled on the device.
http secure-server ssl-policy default_policy	The name of the server SSL policy applied to the HTTPS server is default_policy.
http secure-server enable	The HTTPS server is enabled on the device.
ssl policy default_policy type server	The name of the SSL policy is default_policy and the type is server.
pki-realm default	The name of the PKI domain on the device is default. The domain can be modified but cannot be deleted.
aaa	AAA view.
authentication-scheme default	The name of the system authentication scheme is default. The **default** authentication scheme can be modified but cannot be deleted. The **default** authentication scheme has the following policies: ● The authentication mode is local authentication. ● Users who fail to pass the authentication are forced to go offline.
authorization-scheme default	The name of the authorization scheme is default.
accounting-scheme default	The name of the accounting scheme is default.
domain default	The domain name is default. The device has two default domains named **default** and **default_admin**. The two domains can be modified but cannot be deleted.
domain default_admin	The domain name is default_admin. The device has two default domains named **default** and **default_admin**. The two domains can be modified but cannot be deleted.
local-user admin password cipher %@%@5d~9:M^ipCfL\iB)EQd>3Uwe%@%@	By default, the system has a local user whose user name is **admin** and the user password is in ciphertext.
local-user admin privilege level 15	The priority of the local user **admin** is 15.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
local-user admin service-type http telnet	The access types of the local user **admin** are HTTP and Telnet.
interface Vlanif1 ip address 192.168.1.1 255.255.255.0	The interface type is VLANIF and interface number is 1. The IP address and subnet mask of the interface are 192.168.1.1 and 255.255.255.0, respectively.
user-interface con 0	The user interface type is console and the relative number is 0.
user-interface vty 0	The user interface type is VTY and the relative number is 0.
authentication-mode aaa	The default authentication scheme use AAA authentication mode.
user privilege level 15	The user level is 15.

Related Topics

3.12.10 display factory-configuration operate-mode
3.12.23 set factory-configuration

3.12.10 display factory-configuration operate-mode

Function

The **display factory-configuration operate-mode** command displays the operation performed when the factory configuration is restored.

Format

display factory-configuration operate-mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the operation performed when the factory configuration is restored.

```
<Huawei> display factory-configuration operate-mode
OperaMode  Reserved.
```

Table 3-50 Description of the display factory-configuration operate-mode command output

Item	Description
OperaMode	Operation performed on the original factory configuration when the new factory configuration is restored. • **Delete**: deletes the original factory configuration. • **Reserved**: reserves the original factory configuration. • **Delete user config**: deletes all user configuration files including the files that are automatically generated by the system after the factory configuration is restored. **NOTE** Only the AR161EW, AR169EGW-L, AR2204XE, and AR2204XE-DC support this parameter.

Related Topics

3.12.9 display factory-configuration

3.12.11 display reset-reason

Function

The **display reset-reason** command displays the reason for board reset.

Format

display reset-reason [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a board.	The value is an integer and is dependent on the specific device.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

When no slot ID is specified, the **display reset-reason** command displays the reset reason for all boards.

Precautions

Currently, the restart causes of all LPUs are stored in the same storage space. The storage space can store a maximum of 200 restart causes. When the number of restart causes exceeds 200, new restart causes will overwrite the earliest restart causes. Each LPU can display the latest 10 restart causes.

Example

Displays the reset reason for all boards.

```
<Huawei> system view
[Huawei] display reset-reason
The LPU frame[0] board[1]'s reset total 10, detailed information:
--  1. 07/12   21:17:47, Reset No.: 10
      Reason: Reset for lpu version disaccord with mpu
--  2. 07/12   21:17:31, Reset No.: 9
      Reason: Reset for lpu version disaccord with mpu
--  3. 07/12   21:13:09, Reset No.: 8
      Reason: Reset for lpu version disaccord with mpu
--  4. 07/12   21:04:26, Reset No.: 7
      Reason: Reset by user command
--  5. 02/07   18:40:54, Reset No.: 6
      Reason: Reset for lpu version disaccord with mpu
--  6. 02/07   18:34:53, Reset No.: 5
      Reason: Reset by user command
--  7. 01/13   08:03:03, Reset No.: 4
      Reason: Reset by user command
--  8. 12/29   17:06:53, Reset No.: 3
      Reason: Reset by user command
--  9. 12/27   08:57:23, Reset No.: 2
      Reason: Reset by user command
-- 10. 12/26   20:26:26, Reset No.: 1
      Reason: Reset by user command
The LPU frame[0] board[2]'s reset total 10, detailed information:
--  1. 07/12   21:18:05, Reset No.: 10
      Reason: Reset for lpu version disaccord with mpu
--  2. 07/12   21:13:57, Reset No.: 9
      Reason: Reset for lpu version disaccord with mpu
--  3. 07/12   21:13:28, Reset No.: 8
      Reason: Reset for lpu version disaccord with mpu
--  4. 07/12   21:04:27, Reset No.: 7
      Reason: Reset by user command
--  5. 02/07   18:41:01, Reset No.: 6
      Reason: Reset for lpu version disaccord with mpu
--  6. 02/07   18:34:53, Reset No.: 5
      Reason: Reset by user command
--  7. 01/13   08:03:03, Reset No.: 4
      Reason: Reset by user command
--  8. 12/29   17:06:53, Reset No.: 3
      Reason: Reset by user command
```

 Copyright © Huawei Technologies Co., Ltd.

```
-- 9. 12/27   08:57:23, Reset No.: 2
      Reason: Reset by user command
-- 10. 12/26   20:26:27, Reset No.: 1
      Reason: Reset by user command
The LPU frame[0] board[3] has no reset records.
The LPU frame[0] board[4] has no reset records.
The LPU frame[0] board[5]'s reset total 10, detailed information:
--  1. 07/12   21:04:27, Reset No.: 10
      Reason: Reset by user command
--  2. 02/07   18:34:53, Reset No.: 9
      Reason: Reset by user command
--  3. 01/13   08:03:03, Reset No.: 8
      Reason: Reset by user command
--  4. 12/29   17:06:53, Reset No.: 7
      Reason: Reset by user command
--  5. 12/27   08:57:23, Reset No.: 6
      Reason: Reset by user command
--  6. 12/26   20:26:27, Reset No.: 5
      Reason: Reset by user command
--  7. 12/20   15:33:48, Reset No.: 4
      Reason: Reset by user command
--  8. 12/13   09:52:37, Reset No.: 3
      Reason: Reset by user command
--  9. 12/08   15:07:16, Reset No.: 2
      Reason: Reset by user command
-- 10. 11/25   19:58:09, Reset No.: 1
      Reason: Reset by user command
The LPU frame[0] board[6] has no reset records.
The LPU frame[0] board[7] has no reset records.
The LPU frame[0] board[8] has no reset records.
The LPU frame[0] board[9] has no reset records.
The LPU frame[0] board[10] has no reset records.
The MPU frame[0] board[14] has no reset records.
The MPU frame[0] board[15]'s reset total 10, detailed information:
--  1. 07/12   21:04:27, Reset No.: 10
      Reason: Reset by user command
--  2. 04/28   07:25:12, Reset No.: 9
      Reason: The MPU has been pulled out or has not been powered on
--  3. 04/28   06:32:27, Reset No.: 8
      Reason: The MPU has been pulled out or has not been powered on
--  4. 02/07   18:34:53, Reset No.: 7
      Reason: Reset by user command
--  5. 01/29   08:43:54, Reset No.: 6
      Reason: The MPU has been pulled out or has not been powered on
--  6. 01/13   08:03:03, Reset No.: 5
      Reason: Reset by user command
--  7. 01/01   18:13:34, Reset No.: 4
      Reason: The MPU has been pulled out or has not been powered on
--  8. 12/29   17:06:54, Reset No.: 3
      Reason: Reset by user command
--  9. 12/27   08:57:23, Reset No.: 2
      Reason: Reset by user command
-- 10. 12/26   20:26:27, Reset No.: 1
      Reason: Reset by user command
```

Displays the reset reason for a specific board.

```
<Huawei> system view
[Huawei] display reset-reason slot 1
The LPU frame[0] board[1]'s reset total 10, detailed information:
--  1. 07/12   21:17:47, Reset No.: 10
      Reason: Reset for lpu version disaccord with mpu
--  2. 07/12   21:17:31, Reset No.: 9
      Reason: Reset for lpu version disaccord with mpu
--  3. 07/12   21:13:09, Reset No.: 8
      Reason: Reset for lpu version disaccord with mpu
--  4. 07/12   21:04:26, Reset No.: 7
      Reason: Reset by user command
--  5. 02/07   18:40:54, Reset No.: 6
      Reason: Reset for lpu version disaccord with mpu
```

```
-- 6. 02/07   18:34:53, Reset No.: 5
      Reason: Reset by user command
-- 7. 01/13   08:03:03, Reset No.: 4
      Reason: Reset by user command
-- 8. 12/29   17:06:53, Reset No.: 3
      Reason: Reset by user command
-- 9. 12/27   08:57:23, Reset No.: 2
      Reason: Reset by user command
-- 10. 12/26   20:26:26, Reset No.: 1
      Reason: Reset by user command
```

Table 3-51 Description of the display reset-reason command output

Item	Description
LPU	Line Processing Unit.
frame	Frame ID of a board.
board	Slot ID of a board.
reset total	Number of times a board was reset.
detailed information	Detailed information about board resetting.
Reset No.	Number of a reset.
Reason	Reason for a reset.
MPU	Main Processing Unit.

3.12.12 display saved-configuration

Function

The **display saved-configuration** command displays the configuration file to be used for the next startup.

Format

display saved-configuration [**last** | **time**]

Parameters

Parameter	Description	Value
last	Displays the system configurations saved last time.	-
time	Displays the recent time when the configurations are saved manually or automatically.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

If the device has been started and is not working properly, run the **display saved-configuration** command to check the device startup configuration in the file specified by running the **startup saved-configuration** command.

Run the **display saved-configuration last** command to check the system configurations saved last time in the configuration file loaded during the current startup.

Run the **display saved-configuration time** command to check the last time when the system configurations are saved.

The command output is relevant to user configuration. The command does not display the default configuration.

Example

Display the configuration file for the next startup.

```
<Huawei> display saved-configuration
[V200R010]
#
 sysname Router
...
#
interface GigabitEthernet0/0/0
 ip address 192.168.200.182 255.255.255.0
...
#
user-interface maximum-vty 15
user-interface con 0
user-interface vty 0 14
 idle-timeout 0 0
#
return
```

Related Topics

3.12.26 startup saved-configuration

3.12.20 reset saved-configuration

3.12.8 display current-configuration

3.12.15 display startup

3.12.13 display schedule reboot

Function

The **display schedule reboot** command displays the configuration of the scheduled restart of the device.

Format

display schedule reboot

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After using the **schedule reboot** command to configure a scheduled restart, you can use this command to view the configuration of the scheduled restart.

Example

Display the configuration of the scheduled restart of the device.

```
<Huawei> display schedule reboot
Info:System will reboot at 22:00:00 2013/09/17 (in 1 hours and 43 minutes).
```

Table 3-52 Description of the display schedule reboot command output

Item	Description
System will reboot at	Specific restart time.
in hours and minutes	Time span between the restart time and the current time.

Related Topics

3.12.22 schedule reboot

3.12.14 display snmp-agent trap feature-name configuration all

Function

The **display snmp-agent trap feature-name configuration all** command displays all trap messages of the Configuration module.

Format

display snmp-agent trap feature-name configuration all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the alarm function is enabled, the **display snmp-agent trap feature-name configuration all** command can be used to display the status of all alarms about configuration management.

Example

Display all trap messages of the configuration module.

```
<Huawei> display snmp-agent trap feature-name configuration all
-----------------------------------------------------------------------------
Feature name: CONFIGURATION
Trap number : 1
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwCfgManEventlog                   off                      on
```

Table 3-53 Description of the display snmp-agent trap feature-name configuration all command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the Configuration module. hwCfgManEventlog: Trap message generated when the system configuration event is changed.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Current status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

3.12.25 snmp-agent trap enable feature-name configuration

3.12.15 display startup

Function

The **display startup** command displays the system software for the current and next startup, backup system software, configuration file, license file, and patch file, as well as voice file.

Format

display startup

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Before upgrading or degrading a device, run this command to check whether the files for next startup have been loaded. If the files have been loaded, the device can be upgraded or degraded successfully after it is restarted. You can also run the command to view the system software and files for current startup.

Precautions

Run this command to check whether the backup system software exists. If the backup system software and current startup system software are in the same storage device, save backup system software in another storage device to ensure that the system can still restart when the storage device is damaged.

Example

Display the names of system software for current and next startup.

```
<Huawei> display startup
MainBoard:
  Startup system software:                    sd1:/basicsoftware.cc
  Next startup system software:               sd1:/basicsoftware.cc
  Backup system software for next startup:    null
  Startup saved-configuration file:           sd1:/vrpcfg.zip
  Next startup saved-configuration file:      sd1:/vrpcfg.zip
  Startup license file:                       null
  Next startup license file:                  null
  Startup patch package:                      null
  Next startup patch package:                 null
  Startup voice-files:                        null
  Next startup voice-files:                   null
```

```
SlaveBoard:
  Startup system software:                    sd1:/basicsoftware.cc
  Next startup system software:               sd1:/basicsoftware.cc
  Backup system software for next startup:    null
  Startup saved-configuration file:           sd1:/vrpcfg.zip
  Next startup saved-configuration file:      sd1:/vrpcfg.zip
  Startup license file:                       null
  Next startup license file:                  null
  Startup patch package:                      null
  Next startup patch package:                 null
  Startup voice-files:                        null
  Next startup voice-files:                   null
```

Table 3-54 Description of the display startup command output

Item	Description
MainBoard	Master main control board.
SlaveBoard	Slave main control board. **NOTE** Only the AR3200 series supports dual SRUs.
Startup system software	System software that is used in the current startup.
Next startup system software	System software that is configured for the next startup by running the **startup system-software** command. If no system software for the next startup is configured, the system software used in the current startup is displayed.
Backup system software for next startup	Backup system software that is configured for the next startup by running the **startup system-software backup** command. **null** indicates that no backup system software exists on the device.
Startup saved-configuration file	Configuration file that is used in the current startup.
Next startup saved-configuration file	Configuration file that is configured for the next startup by running the **startup saved-configuration** command. If no configuration file for the next startup is configured, the configuration file used in the current startup is displayed.
Startup license file	License file that is used in the current startup. **default** indicates that no license file is specified or the license file does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Next startup license file	License file that is configured for the next startup. If no license file is configured, **default** is displayed.
Startup patch package	Patch package file that is used in the current startup. **null** indicates that no patch package file is specified or the patch package file does not take effect.
Next startup patch package	Patch package file that is configured for the next startup by running the **startup patch** command. If no patch package file is configured, **NULL** is displayed.
Startup voice-files	Voice file used in current startup. **null** indicates no voice file is specified.
Next startup voice-files	Voice file used in next startup. **null** indicates no voice file is specified.

Related Topics

3.12.26 startup saved-configuration
3.12.27 startup system-software
3.12.30 startup patch

3.12.16 display system

Function

The **display system** command displays the MD5 or SHA256 value of a file.

Format

display system { **file-md5** | **file-sha256** } *filename*

Parameters

Parameter	Description	Value
file-md5	Specifies the MD5 encryption mode.	-
file-sha256	Specifies the SHA256 encryption mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
filename	Specifies the name of the file whose MD5 or SHA256 value needs to be calculated.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After downloading a file from the server to the device, you can check whether the file is damaged during the download process, for example, whether the file is completely downloaded. You can use a piece of third-party software (for example, HashMyFiles) on the server to calculate the MD5 or SHA256 value of the file, run the **display system** command on the device to calculate the MD5 or SHA256 value of the downloaded file, and compare the two values calculated on the server and device. If the two values are the same, the file is not damaged. If the two values are different, the file is damaged, and you need to download the file again.

Precautions

If the size of a file exceeds 200 MB, the device displays the output of the **display system** command after a period of time. Wait until the command output is displayed.

Example

Display the MD5 value of the file **ar3600.cc**

```
<Huawei> system-view
[Huawei] display system file-md5 ar3600.cc
File Name:
ar3600.cc
MD5:
06d12eb350e428605e062a4392455dec
```

Display the SHA256 value of the file **ar3600.cc**.

```
<Huawei> system-view
[Huawei] display system file-sha256 ar3600.cc
File Name:
ar3600.cc
SHA256:
f6910519ab03ef1ecddd7db42784a28c8f32325f98866689df5431f94519165e
```

 Copyright © Huawei Technologies Co., Ltd.

Table 3-55 Description of the **display system** command output

Item	Description
File Name	Name of the file whose MD5 or SHA256 value needs to be calculated.
MD5	MD5 value of the file.
SHA256	SHA256 value of the file.

Related Topics

3.12.27 startup system-software

3.12.17 factory-configuration prohibit

Function

The **factory-configuration prohibit** command disables the function of restoring the factory settings of a device by holding down **reset**.

The **undo factory-configuration prohibit** command enables the function of restoring the factory settings of a device by holding down **reset**.

By default, you can hold down **reset** to restore the factory configuration.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series support this command.

Format

factory-configuration prohibit

undo factory-configuration prohibit

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If you hold down **reset** on a device for more than 5 seconds, the device restarts with the factory settings and all user-defined configurations are lost after the

restart. To retain user-defined configurations after you hold down **reset**, run the **factory-configuration prohibit** command to disable this function.

If you want to restore the factory settings of a device by holding down **reset**, run the **undo factory-configuration prohibit** command to enable this function.

Example

Disable the function of restoring the factory configuration of a device by holding down **reset**.

```
<Huawei> system-view
[Huawei] factory-configuration prohibit
```

Related Topics

3.12.23 set factory-configuration

3.12.24 set factory-configuration operate-mode

3.12.18 factory-configuration reset

Function

The **factory-configuration reset** command configures the device to restore factory settings after restart.

Format

factory-configuration reset

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If incorrect configurations cause exceptions of functions, run the **factory-configuration reset** command to configure the device to restore factory settings after restart.

Precautions

If the configuration file is not specified for factory settings, the device uses default configuration parameters for initialization after the **factory-configuration reset** command is executed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the device to restore factory settings after restart.

```
<Huawei> factory-configuration reset
Warning: It will clean the configuration which you have saved. If you have set the factory-configuration by hand, it will start from the modified factory-configuration, else it will start from the original one, when you restart the device. Continue? [y/n]:y
 Info: Successfully set factory config reset flag!
```

3.12.19 reboot

Function

The **reboot** command restarts the device.

Format

reboot [**fast**]

Parameters

Parameter	Description	Value
fast	Fast restarts the device. In fast restart mode, the configuration file is not saved.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command functions in the same way as a power recycle operation (power off and then restart the device). The command enables you to restart the device remotely.

- After the **reboot** command is run, the system displays a message asking you whether to save the configuration before restarting
- When the **reboot fast** command is run, the system restart quickly without displaying any message and the configuration is lost.

Precautions

- If you do not respond to the displayed message within the timeout period after running this command, the system will return to the user view and the device will not be restarted.
- This command interrupts services on the entire device. Therefore, do not use this command when the device is running properly.

- Before restarting the device, ensure that the configuration file has been saved.
- After this command is executed, the OSP daughter card on the AR161FW-P-M5, AR169-P-M9, AR169RW-P-M9, or AR169W-P-M9 is not affected.

Example

Restart the device.

```
<Huawei> reboot
```

Restart the device quickly.

```
<Huawei> reboot fast
```

3.12.20 reset saved-configuration

Function

The **reset saved-configuration** command clears the next startup configuration file and cancels the configuration file used for next startup.

Format

reset saved-configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- If the configuration file on the device is incompatible with the upgraded software, run the **reset saved-configuration** command to clear the configuration file and run the **startup saved-configuration** command to specify a new configuration file.
- If the device in use is applied to another scenario and the original configuration file of the device does not meet requirements in the scenario, run the **reset saved-configuration** command to clear the existing configuration file and restart the device to restore its factory configurations.

Precautions

- After you run the **reset saved-configuration** command, the next startup configuration file is cleared and the file is not used for next startup. If the

current startup configuration file is the same as the next startup configuration file, the current startup configuration file is also cleared.

- If you do not use the **startup saved-configuration** command to specify a new configuration file containing correct configurations or do not save the configuration file after running the **reset saved-configuration** command, the device uses factory configurations for startup. If the device does not have factory configurations, it uses default configurations for startup.
- If the next startup configuration file is empty, the device displays a message indicating that the file does not exist.
- Exercise caution when you run the **reset saved-configuration** command.

Example

Clear the next startup configuration file in the storage device and cancel the configuration file used for next startup.

```
<Huawei> reset saved-configuration
This will delete the configuration in the flash memory.
The device configurations will be erased to reconfigure.
Are you sure? (y/n)[n]:y
 Clear the configuration in the device successfully.
```

Related Topics

3.12.21 save

3.12.8 display current-configuration

3.12.12 display saved-configuration

3.12.21 save

Function

The **save** command saves the configurations to the default directory.

Format

save [**all**] [*configuration-file*]

Parameters

Parameter	Description	Value
all	Indicates that all configurations are saved, including the configurations of the boards that are not running.	-
configuration-file	Specifies the name of a configuration file.	The value is a string of 5 to 64 case-insensitive characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run commands to modify the current configuration of the device, but the modified configuration will be lost after the device restarts. To enable the new configuration to take effect after a restart, save the current configuration in the configuration file before restarting the device.

When a series of configurations are complete and take effect, you must save the current configuration file to the storage device.

The **save** *configuration-file* command saves the current configuration to a specific file on the storage device. Generally, running the **save** *configuration-file* command does not affect the current startup configuration file. If the configuration file specified by *configuration-file* has the same name with the current configuration file and the default directory is used, running the **save** *configuration-file* command is equivalent to running the **save** command.

Run the **save all** command to save all the current configurations, including the configurations of the boards that are not running, to the default directory.

The **save all** *configuration-file* command saves the current configuration to a specific file on the storage device. Generally, running the **save all** *configuration-file* command does not affect the current startup configuration file. If the configuration file specified by *configuration-file* has the same name with the current configuration file and the default directory is used, running the **save all** *configuration-file* command is equivalent to running the **save all** command.

If you do not specify *configuration-file* when saving the configuration file for the first time, the system asks you whether to save the configuration file as **vrpcfg.zip**.

Precautions

- If the configuration file to be saved using this command has the same name with the existing configuration file, the existing configuration file is rewritten.
- The configuration file name extension must be .zip or .cfg.
  - .cfg: The file is saved in plain text mode. After the file is specified as the configuration file, all commands in the file are recovered one by one during startup.
  - .zip: The .cfg file is compressed to a .zip file that occupies less space. After being specified as the configuration file, the .zip file is decompressed to the .cfg file and all commands in the .cfg file are recovered one by one during startup.

 Copyright © Huawei Technologies Co., Ltd.

Example

Save the current configuration file to the default directory.

```
<Huawei> save
 Warning: The current configuration will be written to the device.
 Are you sure to continue? (y/n):y
  It will take several minutes to save configuration file, please wait.........
 Configuration file had been saved successfully
 Note: The configuration file will take effect after being activated
```

Related Topics

3.12.20 reset saved-configuration

3.12.8 display current-configuration

3.12.12 display saved-configuration

3.12.26 startup saved-configuration

3.12.22 schedule reboot

Function

The **schedule reboot** command configures the scheduled restart of a device and set the specific time when the device restarts or the delay time before the device restarts.

The **undo schedule reboot** command disables the scheduled restart function.

By default, the scheduled restart is disabled.

Format

schedule reboot { **at** *time* | **delay** *interval* }

undo schedule reboot

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
at *time*	Specifies the device restart time.	The format of *time* is *hh:mm YYYY-MM-DD*. The restart time must be later than the current device time by less than 720 hours. *YYYY-MM-DD* indicates year, month, and date and is optional. ● *hh* indicates hour and the value ranges from 0 to 23. ● *mm* indicates minute and the value ranges from 0 to 59. ● *YYYY* indicates year and the value ranges from 2000 to 2099. ● *MM* indicates month and the value ranges from 1 to 12. ● *DD* indicates date and the value ranges from 1 to 31.
delay *interval*	Specifies the delay time before the device restarts.	The format of *interval* is *hh:mm* or *mm*. The delay time must be no more than 720 hours. ● In *hh:mm*, *hh* indicates hour and the value ranges from 0 to 720 and *mm* indicates minute and the value ranges from 0 to 59. ● *mm* indicates minute and the value ranges from 0 to 43200.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When upgrading or restarting the device, you can configure the device to restart at time when few services are running to minimize the impact on services.

Precautions

- If a specific date is set in the **schedule reboot** command and the date is a future date, the device will be restarted at the specified time and there may be a time difference within 1 minute. If no date is set, two situations may occur: If the specified time is later than the current time, the device is restarted at the specified time of the day. If the specified time is earlier than the current time, the device is restarted at the specified time of the next day.
- When **at** *time* or **delay** *interval* is used, the time difference between the specified date and the current date cannot be greater than 720 hours. If the

scheduled restart has been configured, the latest configuration overrides the previous one.

- The scheduled restart function becomes invalid when you use the **clock datetime** command to set the system time to over 10 minutes later than the restart time set by the **schedule reboot** command. If the time difference is equal to or less than ten minutes, the device immediately restarts and does not save the configuration.
- This command restarts the device at the specified time, interrupting all services on the device. Therefore, do not use this command when the device is running properly.
- Before restarting the device, ensure that the configuration file has been saved.

Example

Configure the device to restart at 22:00.

```
<Huawei> schedule reboot at 22:00
Info:Reboot system at 22:00:00 2012/07/25(in 10 hours and 10 minutes) confirm?[Y
/N]:y
```

Related Topics

3.12.13 display schedule reboot

3.12.23 set factory-configuration

Function

The **set factory-configuration** command configures the current configuration, existing configuration file, or default factory settings as the factory configuration.

Format

set factory-configuration from { **current-configuration** | *filename* | **default** }

Parameters

Parameter	Description	Value
current-configuration	Specifies the current configuration.	-

Parameter	Description	Value
filename	Specifies a configuration file name. **NOTE** Local configuration files with file name extension .cfg and .zip are supported.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive-name*] [*file-name*]. If *drive-name* is not specified, the value is the default storage medium name. The maximum length of the entered *file-name* is 64 minus the default storage medium name. **NOTE** If the length of the entered *configuration-file* is greater than 64, the system displays the following information: Error: The file name length is too long!
default	Specifies default factory settings.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you need to change the factory configuration based on requirements, an unknown problem occurs on the device, or the device operations are slow or unstable after the device has been running for a long time, you can run the **set factory-configuration** command to specify a new factory configuration.

Follow-up Procedure

After running the **set factory-configuration** command to specify a new factory configuration, you can use different methods on different device models to restore this factory configuration. On the AR100&AR120&AR150&AR160&AR200 series, hold down the **RESET** button at least 5s to restore the factory configuration. On the AR1200&AR2200&AR3200&AR3600 series, run the **factory-configuration reset** command to restore the factory configuration.

Precautions

The new configuration file is not greater than 100 KB. If the file is over 100 KB, the system fails to specify new factory configuration and displays the following information:

```
Error: Local file is too large!
```

After the **set factory-configuration** command is used, new factory configuration overrides the previous one.

Use the function that restores the factory configuration with caution. The user-defined configuration will be lost when you restore factory configuration.

NOTICE

Hold down the **RESET** button for more than 5s to restart the device. The device will use the new factory configuration after it restarts.

Press the **RESET** button to restart the device. The configuration is the latest one.

Example

Override the factory configuration with the current configuration.

```
<Huawei> set factory-configuration from current-configuration
 Warning: The current factory configuration will be replaced, and it's irreversible. Are you sure to set the factory configuration?[Y/N]:y
 Info: Successfully set factory config!
```

Override the factory configuration overrides the specified configuration.

```
<Huawei> set factory-configuration from factory.cfg
 Warning: The current factory configuration will be replaced, and it's irreversible. Are you sure to set the factory configuration?[Y/N]:y
 Info: Successfully set factory config!
```

Override the factory configuration with default factory settings.

```
<Huawei> set factory-configuration from default
 Warning: The current factory configuration will be replaced, and it's irreversible. Are you sure to set the factory configuration?[Y/N]:y
 Info: Successfully set factory config!
```

Related Topics

3.12.24 set factory-configuration operate-mode

3.12.24 set factory-configuration operate-mode

Function

The **set factory-configuration operate-mode** command sets the method for restoring the factory configuration.

By default, the system reserves the previous configuration file when restoring the factory configuration.

Format

set factory-configuration operate-mode { **reserve-configuration** | **delete-configuration** | **delete-user-configuration** }

Parameters

Parameter	Description	Value
reserve-configuration	Reserves current configuration file after factory settings are restored.	-
delete-configuration	Deletes current configuration file after factory settings are restored.	-
delete-user-configuration	Delete all user configuration files including the files that are automatically generated by the system after the factory configuration is restored. **NOTE** Only the AR161EW, AR169EGW-L, AR2204XE-DC, and AR2204XE support this parameter.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you use the **set factory-configuration** command to specify factory settings, run the **set factory-configuration operate-mode delete-configuration** command to specify the operation as **delete-configuration** for restoring factory settings. This prevents user information leak when the device is lost.

Follow-up Procedure

Run the **set factory-configuration operate-mode delete-user-configuration** command to delete all user configuration files and restart the device for restoring the factory configuration. Then run the **undo bootloader startup menu enable** command to hide the Boot main menu and restart the device. Press **Ctrl+B** to enter the Boot main menu as prompted, select **Password Manager** to enter the password management page. Enter Y as prompted, and then restart the device. All user configuration files are deleted and the default factory configuration is restored during the device startup.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the mode of restoring the factory configuration to **delete**.

```
<Huawei> set factory-configuration operate-mode delete-configuration
Warning: It may delete your configuration file when executing factory configur
ation,are you sure to set the operation mode?(Y/N)y
Successfully set factory operation mode
```

Related Topics

3.12.23 set factory-configuration

3.12.25 snmp-agent trap enable feature-name configuration

Function

The **snmp-agent trap enable feature-name configuration** command enables the trap function for the Configuration module.

The **undo snmp-agent trap enable feature-name configuration** command disables the trap function for the Configuration module.

By default, the trap function is disabled for the Configuration module.

Format

snmp-agent trap enable feature-name configuration [**trap-name hwcfgmaneventlog**]

undo snmp-agent trap enable feature-name configuration [**trap-name hwcfgmaneventlog**]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of Configuration events of specified types.	-
hwcfgmaneventlog	Enables the device to send a trap when the system event is changed.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The Configuration module is not configured with the function of excessive traps. To enable the trap function of one or more events, you can specify **trap-name**.

 Copyright © Huawei Technologies Co., Ltd.

You can run the **display snmp-agent trap feature-name configuration all** command to check the configuration result.

Example

Enables the device to send a trap when the system event is changed.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name configuration trap-name hwcfgmaneventlog
```

3.12.26 startup saved-configuration

Function

The **startup saved-configuration** command specifies the system configuration file for next startup.

Format

startup saved-configuration *configuration-file* [**slave-board** | **all**]

NOTE

Only the AR3200 series supports the **slave-board** and **all** parameters.

Parameters

Parameter	Description	Value
configuration-file	Specifies the name of a configuration file. Make sure that the file exists.	The value is a string of 1 to 64 case-insensitive characters in the format of [*drive-name*] [*file-name*]. It can contain the following special characters: [ ] @ ! # $ % ^ - = _ + { } , . : /. A string containing digits, letters, and underscores (_) is recommended. If *drive-name* is not specified, the value is the default storage medium name. The maximum length of the entered *file-name* is 64 minus the default storage medium name. **NOTE** If the length of the entered *configuration-file* is greater than 64, the system displays the following information: Error: The file name length is too long!
slave-board	Specifies the configuration file for next startup on the slave SRU.	-

Parameter	Description	Value
all	Specifies the configuration file for next startup on all SRUs.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the original configuration file cannot be used due to the software upgrade, run the **startup saved-configuration** command to specify another configuration file for next startup. The startup configuration file must be saved in the root directory of the storage device.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- The configuration file specified for the next startup must exist.
- The configuration file name extension must be .zip or .cfg.
  - A configuration file with the file name extension .cfg is a text file, and you can view the file content in the text file. After the file is specified as the configuration file for next startup, the system restores all commands in the file one by one during a startup.
  - A .cfg file is compressed to a .zip file that occupies less space. After being specified as the configuration file, the .zip file is decompressed to the .cfg file and the system restores all commands in the .cfg file one by one during startup.

Example

Specify the system configuration file for the next startup.

```
<Huawei> startup saved-configuration vrpcfg.cfg
```

Related Topics

3.12.15 display startup

3.12.22 schedule reboot

3.12.19 reboot

3.12.27 startup system-software

Function

The **startup system-software** command specifies the system software for next startup.

Format

startup system-software *system-file* [**slave-board** | **all**] [**verify** | **signature** *sign-filename*]

NOTE

- Only the AR3200 series supports the **slave-board** and **all** parameters.
- You cannot start the system software package in the system using an external hard disk.

Parameters

Parameter	Description	Value
system-file	Specifies the name of the system software file.	The value is a string of 1 to 64 case-insensitive characters in the format of [*drive-name*] [*file-name*]. It can contain the following special characters: [ ] @ ! # $ % ^ - = _ + { } , . : /. A string containing digits, letters, and underscores (_) is recommended. If *drive-name* is not specified, the value is the default storage medium name. The maximum length of the entered *file-name* is 64 minus the default storage medium name. **NOTE** If the length of the entered *configuration-file* is greater than 64, the system displays the following information: Error: The file name length is too long!
slave-board	Specifies the system software for next startup on the slave SRU.	-
all	Specifies the system software for next startup on all SRU.	-
verify	Checks validity of system software.	-

Parameter	Description	Value
signature *sign-filename*	Checks validity of the system software's digital signature file.	*sign-filename* is a character string in the format of [*drive-name*][*file-name*]. If *drive-name* is not specified, the name of the default storage device is used. The value is a string of 1 to 64 case-insensitive characters without spaces. The file name extension must be .asc.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In system software upgrade or downgrade, run this command to specify the system software for next startup.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- The system software package must use .cc as the file name extension and be saved to the root directory of the storage device.

The system software's digital signature file must use .asc as the file name extension and be saved to the root directory of the storage device.

If a slave SRU has been specified by **slave-board** or the system software for all SRUs has been specified by **all**, the device automatically copies the system software from the master SRU to the slave SRU and you do not need to run the **copy** *source-filename destination-filename* command. If the specified system software already exists on the slave SRU, the device displays a message asking whether you want to use the system software on the slave SRU. If not, the device displays a message asking whether you want to overwrite the existing system software. If the system software has been specified for next startup and cannot be overwritten, the device will cancel the automatic copy operation.

If the storage space of the slave SRU for which the system software is specified using the **startup system-software** command is insufficient, the device prompts that a failure occurs.

If the device has dual SRUs, specify the system software for next startup on both the master and slave SRUs.

The AR161G-L&AR161G-Lc&AR169G-L&AR169EGW-L support only the system software upgrade. If the version of the system software specified for next startup

using the **startup system-software** command is earlier than the current system software version, the system displays the following message:

```
Error: The version of the specified package file is too low.
```

Example

Specify the system software to be loaded for next startup.

```
<Huawei> startup system-software basicsoft.cc
```

Related Topics

3.12.15 display startup

3.12.26 startup saved-configuration

3.12.22 schedule reboot

3.12.19 reboot

3.12.28 startup system-software backup

Function

The **startup system-software backup** command specifies the backup system software for system startup.

By default, the device has no backup system software.

Format

startup system-software *filename* **backup**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
filename	Specifies the name of the backup system file.	The value is a string of 1 to 64 case-insensitive characters in the format of [*drive-name*] [*file-name*]. It can contain the following special characters: [ ] @ ! # $ % ^ - = _ + { } , . : /. A string containing digits, letters, and underscores (_) is recommended. The recommended format is **drive name:/file name**. For example, flash:/software.cc. If *drive-name* is not specified, the value is the default storage medium name. The maximum length of the entered *file-name* is 64 minus the default storage medium name. **NOTE** If the length of the entered *configuration-file* is greater than 64, the system displays the following information: Error: The file name length is too long!

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the specified startup software package is damaged, the system uses the backup software package to start.

Precautions

- The file name extension of the system software package must be .cc and the package must be stored in the root directory.
- The backup startup software package can be the same as or different from the current startup software package, but it must ensure a successful system start.

Example

Specify the backup system startup software for the system.

```
<Huawei> startup system-software basicsoft.cc backup
This operation will take several minutes, please wait.......
Info: Succeeded in setting the backup file for booting system
```

Related Topics

3.12.27 startup system-software

3.12.29 startup system-software check enable

Function

The **startup system-software check enable** command enables security check over the system software package.

The **undo startup system-software check enable** command disables security check over the system software package.

By default, security check over the system software package is disabled.

Format

startup system-software check enable

undo startup system-software check enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To prevent the system software package from being tampered during a system software upgrade, you can run the **startup system-software check enable** command to enable security check over the system software package. After this function is enabled, security check will be performed over the system software to be upgraded. If the system software package is tampered with, it cannot be loaded. You are advised to run the **save** command to save the configuration after security check over the system software package is enabled. The device then performs security check over the system software package to be loaded during each upgrade-triggered restart.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable security check over the system software package.

```
<Huawei> system-view
[Huawei] startup system-software check enable
 Info: This configuration will activate the startup system-software check functi
on, and the startup may take several minutes longer than usual. Continue? [y/n]:y
```

3.12.30 startup patch

Function

The **startup patch** command specifies the patch file for next startup.

Format

startup patch *patch-name* [**slave-board** | **all**]

NOTE

Only the AR3200&AR3600 series supports the **slave-board** and **all** parameters.

Parameters

Parameter	Description	Value
patch-name	Specifies the name of the patch file for next startup.	The value is a string of 1 to 64 case-insensitive characters in the format of [*drive-name*] [*file-name*]. It can contain the following special characters: [ ] @ ! # $ % ^ - = _ + { } , . : /. A string containing digits, letters, and underscores (_) is recommended. If *drive-name* is not specified, the value is the default storage medium name. The maximum length of the entered *file-name* is 64 minus the default storage medium name. **NOTE** If the length of the entered *configuration-file* is greater than 64, the system displays the following information: Error: The file name length is too long!
slave-board	Specifies the patch file for next startup on the slave SRU.	-
all	Specifies the patch file for next startup on all SRU.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To make the patch file take effect after the device restarts, run this command to specify the patch file for next startup.

Follow-up Procedure

Run the **reboot** or the **schedule reboot** command to restart the device.

Precautions

- A patch file uses .pat as the file name extension and must be saved in the root directory.
- If you use this command to specify another patch for next startup, the previous patch will be overridden.
- After the patch file is specified for next startup, run the **display patch-information** command to view the patch file.
  - If the patch file for next startup is not empty, the device load the patch automatically after next startup.
  - If the patch file for next startup is empty, the device cannot load the patch after next startup.
- After the device restarts, the system loads and runs the patch. If you do not want the system to load the patch file after startup, use the **patch delete all** command to delete the patch file.

Example

Specify the patch file for next startup.

```
<Huawei> startup patch patch.pat
```

Related Topics

3.12.15 display startup

3.12.22 schedule reboot

3.12.19 reboot

3.12.31 bootloader startup menu enable

Function

The **bootloader startup menu enable** command displays the Boot menu.

The **undo bootloader startup menu enable** command hides the Boot menu.

By default, the device displays the Boot menu.

NOTE

Only the AR161EGW-LM1, AR161EW, AR161EW-M1, AR169E, AR169EGW-L, AR169EW, AR2204XE and AR2204XE-DC support this command.

Format

bootloader startup menu enable

undo bootloader startup menu enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **bootloader startup menu enable** command to display the Boot menu on the device.

Example

Display the Boot menu.

```
<Huawei> system-view
[Huawei] bootloader startup menu enable
Warning: The operation will save all configuration to the next startup configuration.
And the WorkMode Change will be activated after board reboot. Continue? [y/n]:y
  It will take several minutes to save configuration file, please wait..........
...
Jun 14 2018 08:43:17+09:00 Huawei %%01LOAD/4/ENT_CONFIG_SET(l)[0]:Succeeded in setting
flash:/vrpcfg.zip for config file by device.
[Huawei]......
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
```

3.12.32 display bootloader startup menu

Function

The **display bootloader startup menu** command checks whether the Boot menu is hidden.

NOTE

Only the AR161EGW-LM1, AR161EW, AR161EW-M1, AR169E, AR169EGW-L, AR169EW, AR2204XE, and AR2204XE-DC support this command.

Format

display bootloader startup menu

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **display bootloader startup menu** command to check whether the Boot menu is hidden.

Example

Check whether the Boot menu is hidden.

```
<Huawei> system-view
[Huawei] display bootloader startup menue
BootLoader Startup Menu Config = Disable
```

Table 3-56 Description of the **display bootloader startup menu** command output

Item	Description
BootLoader Startup Menu Config	Whether the Boot menu is hidden. ● Disable: hides the Boot menu. ● Enable: displays the Boot menu.

3.13 Upgrade Commands

3.13.1 display license

Function

The **display license** command displays information about the license file in the system.

Format

display license

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

A license file dynamically controls the availability of some features. Only one license file is active in the system. Run this command to view detailed information about the active license in the system, including license file name, version, validity period, and control item. Based on the information, you can determine whether to upgrade the system version to support more features.

NOTE

In current version, the encoding format in displaying license information is the same as that of the license file used by the device. If different terminals are used for login, adjust the encoding formats of the terminals according to that of the license file to prevent garbled characters.

Example

Display information about the active license file of the MPU.

```
<Huawei> display license

 Active License on master board: flash:/LICAR2200all_2015070739W760.dat

 Active license    : flash:/LICAR2200all_2015070739W760.dat
 License state     : Normal
 Revoke ticket     : No ticket

 Product name      : AR
 Product version   : all
 License file ESN  : 2102310KFT10C8000117
 License Serial No : LIC2015070739W760
 Creator           : Huawei Technologies Co., Ltd.
 Created Time      : 2015-07-07 20:05:03
 Country           : China
 Custom            : No relevant customer information
```

```
Office           : UNKNOWN

Feature name      : ARLIC
Authorize type    : COMM
Expired date      : 2015-10-05
Trial days        : 60

Item name         : LAR0VOICEE03
Item type         : Function
Control value     : 1
Used value        : 1
Item state        : Normal
Item expired date : 2015-10-05
Item trial days   : 60
Description       : Value-Added Voice Package

Item name         : LAR0DATAE03
Item type         : Function
Control value     : 1
Used value        : 1
Item state        : Normal
Item expired date : 2015-10-05
Item trial days   : 60
Description       : Data Package

Item name         : LAR0SECE03
Item type         : Function
Control value     : 1
Used value        : 1
Item state        : Normal
Item expired date : 2015-10-05
Item trial days   : 60
Description       : Security Package

Item name         : LAR0DSVPN03
Item type         : Function
Control value     : 1
Used value        : 1
Item state        : Normal
Item expired date : 2015-10-05
Item trial days   : 60
Description       : DSVPN Function Controller

Item name         : LAR0AC03
Item type         : Function
Control value     : 1
Used value        : 1
Item state        : Normal
Item expired date : 2015-10-05
Item trial days   : 60
Description       : AC Cotroller

Item name         : LAR0ATC03
Item type         : Function
Control value     : 1
Used value        : 1
Item state        : Normal
Item expired date : 2015-10-05
Item trial days   : 60
Description       : Air Traffic Controller
```

Table 3-57 Description of the **display license** command output

Item	Description
Active License on master board	Name and path of the active license file on the MPU.

Item	Description
Active license	Name and path of the active license file.

Item	Description
License state	Status of a license file: ● Normal This state value indicates that a license file is working properly. If the status of the license file on the live network is not **Normal**, check the license file. ● Trial – A license file enters the Trial state if the ESN does not match the device. A license file in Trial state can be used only for 60 days. To continue to use a license file after the Trial state, apply for a new license file using the correct ESN. – A temporary license file expires and enters the Trial state. To continue to use a license file after the Trial state, apply for a new license file and activate it. – A license file is revoked and enters the Trial state. To continue to use a license file after the Trial state, apply for a new license file based on the revocation code and activate it. – If you replace the master main control board but the new ESN does not match the license file, the license file enters the Trial state. To continue to use a license file after the Trial state, apply for a new license file matching the new ESN and activate it. ● Demo When you activate a temporary license file, it enters the Demo state. The Demo state exists only for a demo license file used for test and deployment. A license file in Demo state allows you to use normal functions within a specified period. Before the

Item	Description
	expiration of the license file in Demo state, replace it with a commercial license file. ● Emergency A license file enters the Emergency state when a disaster occurs (commercial scenario). In the emergency conditions like earthquake, volcano explosion, and tsunami, you can run the **license emergency** command to trigger a license file to enter the Emergency state. The Emergency state stays for seven days, and a license file can enter the Emergency state three times. ● Default: No license file is activated or a license file expires. If a license file enters the Default state, services may be interrupted. If you want to use services after a license file expires or becomes invalid, apply for a new license file and activate it.
Revoke ticket	License revocation code.
Product name	Name of the product that runs the license. **NOTE** In version V200R010C00SPC500PWE, the value of **Product name** is **Router**.
Product version	Product version.
License file ESN	ESN in the license file.
License Serial No	Serial number of license file.
Creator	Creator of the file.
Created Time	Time when the file was created.
Country	Country of the authorized customer.
Custom	Authorized customer.
Office	Office of the authorized customer.
Feature name	Feature name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authorize type	Authorization type. ● demo: trial authorization. ● comm: commercial authorization.
Expired date	License expiration date. **PERMANENT** indicates that the license is permanently valid.
Trial days	Trial period.
Item name	Name of a control item.
Item type	Type of a control item.
Control value	Authorized count of a control item.
Used value	Used count of a control item.
Item state	Status of a control item.
Item expired date	Expiration date of a control item.
Item trial days	Trial period of a control item.
Description	Description of a control item.

3.13.2 display license accept agreement

Function

The **display license accept agreement** command displays information about functions activated through commands, including the functions that have been activated and time functions were used.

Format

display license accept agreement [**history**]

Parameters

Parameter	Description	Value
history	Displays details of each control item including the maximum activation count of a resource item, regardless of whether the ETU license is enabled.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

After the **display license accept agreement history** command is executed, either of the following situations occurs:

- If function licenses are activated, the **display license accept agreement history** command output is the same as the **display license accept agreement** command output.
- If resource licenses are activated, the message "Maximum control value" indicating the maximum activation count of a resource item is displayed.

If the control item is in **Enable** state, the function has been activated. The control item name corresponding to the same function on different product models may be different. Table 3-58 lists the mapping between authorized functions and control items.

Table 3-58 Mapping between authorized functions and control items

Authorization Function	Control Item
Data service (SPR and MPLS L2VPN) **NOTE** The AR150&AR160&AR200 series does not support MPLS L2VPN.	AR100&AR120&AR150&AR160&AR200: LAR0DATAE01 AR1200: LAR0DATAE02 AR2200: LAR0DATAE03 AR3200: LAR0DATAE04
Security service (SAC, Efficient VPN)	AR100&AR120&AR150&AR160&AR200: LAR0SECE01 AR1200: LAR0SECE02 AR2200: LAR0SECE03 AR3200: LAR0SECE04
WLAN AC Express	AR100&AR120&AR150&AR160&AR200: LAR0AC01 AR1200: LAR0AC02 AR2200: LAR0AC03 AR3200: LAR0AC04
DSVPN	AR100&AR120&AR150&AR160&AR200: LAR0DSVPN01 AR1200: LAR0DSVPN02 AR2200: LAR0DSVPN03 AR3200: LAR0DSVPN04

 Copyright © Huawei Technologies Co., Ltd.

Authorization Function	Control Item
XGE	AR100&AR120&AR150&AR160&AR200: LAR0XGE01 AR1200: LAR0XGE02 AR2200: LAR0XGE03 AR3200: LAR0XGE04

Example

Display information about functions activated through commands.

```
<Huawei> display license accept agreement history
 Active license Accept Agreement:     yes

 Item name            : LAR0DATAE04
 Item type            : Function
 Item state           : Disable, -
 Item left time       : -
 Item used time       : -
 Description          : Data GTLV2

 Item name            : LAR0SECE04
 Item type            : Function
 Item state           : Disable, -
 Item left time       : -
 Item used time       : -
 Description          : LAR0SECE04

 Item name            : LAR0AC04
 Item type            : Function
 Item state           : Disable, -
 Item left time       : -
 Item used time       : -
 Description          : LAR0AC04

 Item name            : LAR0SSLVPN00
 Item type            : Resource
 Control value        : 0
 Maximum control value : 0
 Item state           : Disable, -
 Item left time       : -
 Item used time       : -
 Description          : LAR0SSLVPN00

 Item name            : LAR0DSVPN04
 Item type            : Function
 Item state           : Disable, -
 Item left time       : -
 Item used time       : -
 Description          : LAR0DSVPN04

 Item name            : LAR0IVR00
 Item type            : Resource
 Control value        : 0
 Maximum control value : 0
 Item state           : Disable, -
 Item left time       : -
 Item used time       : -
 Description          : LAR0IVR00

 Item name            : LAR0CT00
 Item type            : Resource
```

```
Control value         : 0
Maximum control value : 0
Item state            : Disable, -
Item left time        : -
Item used time        : -
Description           : LAR0CT00

Item name             : LAR0CM00
Item type             : Resource
Control value         : 0
Maximum control value : 0
Item state            : Disable, -
Item left time        : -
Item used time        : -
Description           : LAR0CM00

Item name             : LAR0VOICEE04
Item type             : Function
Item state            : Disable, -
Item left time        : -
Item used time        : -
Description           : LAR0VOICEE04
```

Table 3-59 Description of the display license accept agreement history command output

Item	Description
Active license Accept Agreement	ETU license status: ● yes: The ETU license is activated. ● no: The ETU license is not activated.
Item name	Name of the control item.
Item type	Type of the control item: ● Function ● Resource
Item state	Status of the control item: ● Enable, Evaluate: This control item is activated and is in trial period. ● Enable, Permanent: This control item is activated and the trial period is reached. ● Disable, Evaluate: This control item is not activated and is in trial period. ● Disable, Permanent: This control item is not activated and the trial period is reached. ● Disable, -: This control item is not activated.
Item left time	Remaining time of the trial period after the control item is activated.

Item	Description
Item used time	Time elapsed since the control item has been used after the control item is activated.
Description	Description of the control item.
Control value	Value of the activated resource item.
Maximum control value	Maximum activation count of the resource item.

3.13.3 display license esn

Function

The **display license esn** command displays the equipment serial number (ESN) used for applying a license.

Format

display license esn

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When you need to use licensed resource items or function items, apply to Huawei for a license file. When applying for a license, you need to provide the device ESN.

ESN is the only identifier of device components (such as MPU and interface board), run the **display license esn** command to display the ESN of the current device, and then use the ESN to apply a license file for the device.

The ESN of the chassis must be the same as the ESN in the license to be activated. If they are different, the license file cannot be activated.

Example

Display the ESN used for applying a license.

```
<Huawei> display license esn
```

```
Master ESN is: 2102113374P0B4000046.
```

Table 3-60 Description of the **display license esn** command output

Item	Description
Master ESN is	ESN of the device.

3.13.4 display license resource usage

Function

The **display license resource usage** command displays the usage of the resource items defined in a license file.

Format

display license resource usage

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display license resource usage** command to check the usage of the resource items defined in the license file.

Resource usage refers to the percentage of resources used out of resources defined by the license file.

Example

Display the usage of licensed resources.

```
<Huawei> display license resource usage
 Activated License: flash:/LIC_ON179007_A1BB9D41960_all.dat
 FeatureName    | ConfigureItemName       | ResourceUsage

 CRFEA1         LARWLANAC00                 0/0
 CRFEA1         Test                    0/0
 CRFEA1         LAR0SSLVPN00              0/100
 CRFEA1         LAR0IVR00                 0/250
 CRFEA1         LAR0CT00                  0/250
 CRFEA1         LAR0CM00                   0/256
```

Table 3-61 Description of the display license resource usage command output

Item	Description
Activated License	File name and path of an active license name.
FeatureName	Name of the feature controlled by the license.
ConfigureItemName	Name of a control item.
ResourceUsage	Percentage of used resources.

3.13.5 display license revoke-ticket

Function

The **display license revoke-ticket** command displays the revocation code of the current license file of the device.

Format

display license revoke-ticket

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display license revoke-ticket** command enables you to check the revocation code of a license file that has become invalid on the device. This code proves that the current license file is invalid and is used to apply for a new license.

Precautions

This command displays information only when the license file in current device system is invalid. Otherwise, no command output is displayed.

Example

Display the revocation code of the current invalid license file.

```
<Huawei> display license revoke-ticket
 Info: The revoke ticket is: LIC20091103006100:27C1B773ED11D9F877855CDAEE74ABFE60E07126.
```

3.13.6 display license state

Function

The **display license state** command displays the license status on the MPU.

Format

display license state

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To check the status of the running license, run this command. The command displays the current status of the license and the number of days before the license in this status will expire.

The system supports the following license states:

- Normal: normal license
- Demo: demonstration license
- Trial: trial license that has expired but is still valid during the trial period
- Emergency: emergency license
- Default: default license

This command helps you locate license problems and verify the license status on the device.

Prerequisites

A license file has been stored on the main control board of the device and has been activated. This ensures that valid entries are displayed after the execution of the command. If the license file is not activated, no command output is displayed.

Example

Display the status of the license on the MPU.

```
<Huawei> display license state
```

```
Info: Master board license state: Trial. The remain days is 44.
```

3.13.7 display paf

Function

The **display paf** command displays information about the product adaptive file (PAF) in the system.

Format

display paf { **all** | { **resource** | **service** } *item-name* }

Parameters

Parameter	Description	Value
all	Displays all information about the PAF file.	-
resource	Specifies the value set for a resource item in the PAF file.	-
service	Specifies the value set for a service item in the PAF file.	-
item-name	Specifies the name of a resource item or a service item.	The value is a string of 1 to 64 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A PAF file provides only required resources and features. This command can display all the specification information about the PAF file.

Example

Display the value set for a resource item in the PAF file.

```
<Huawei> display paf resource PAF_LCS_NQA_SPECS_NUM_ENTRY
 PAF_LCS_NQA_SPECS_NUM_ENTRY = 0, 128, 128, 0
```

Display the value set for a service item in the PAF file.

```
<Huawei> display paf service PAF_LCS_BFD_BASIC_SPECS_ENABLED
 PAF_LCS_BFD_BASIC_SPECS_ENABLED = 0, 1
```

Table 3-62 Description of the display paf resource command output

Item	Description
PAF_LCS_NQA_SPECS_NUM_ENTRY	Resource item name in the PAF file.
0	Whether a resource item is controlled by a license. ● 1: yes ● 0: no
128	Default value of the resource item in the PAF file.
128	Maximum value of the resource item in the PAF file.
0	Minimum value of the resource item in the PAF file.

Table 3-63 Description of the display paf service command output

Item	Description
PAF_LCS_BFD_BASIC_SPECS_ENABLED	Service item name in the PAF file.
0	Whether a service item is controlled by a license. ● 1: yes ● 0: no
1	Service status. ● 1: enabled ● 0: disabled

3.13.8 display patch-information

Function

The **display patch-information** command displays information about the patch in the current system.

Format

display patch-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a patch is loaded or deleted, run this command to view information about the patch, including its version, name.

Example

Display information about the patch in the current system.

```
<Huawei> display patch-information
Patch version         :ARV200R009C00
Patch package name    :flash:/patch_ar650.pat
The state of the patch state file is:Running
The current state is:Running
*****************************************************************
*              The patch information,as follows                 *
*****************************************************************
Type        State         Count          Time(YYYY-MM-DD HH:MM:SS)
-----------------------------------------------------------------
exe         Running       1              2017-12-31 09:23:46+00:00
```

Table 3-64 Description of the display patch-information command output

Item	Description
Patch version	Version of the patch.
Patch package name	Name of the patch file.
The state of the patch state file is	Status of the patch file.
The current state is	Current status of the patch.
Type	Patch type. ● VRP: VRP patch for the MPU. ● CAP: CAP patch for the MPU. ● Kernel: Patch for the kernel. ● LPU: Patch for the LPU. ● soft: Patch for the software. ● exe: Patch for the file.
State	Running status of the patch. (**Running**: The patch is running.)

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Count	Number of patch units.
Time(YYYY-MM-DD HH:MM:SS)	Time when the patch takes effect.

Related Topics

3.13.16 patch delete all

3.13.17 patch load

3.13.9 display rollback state

Function

The **display rollback state** command displays the rollback status of the system.

Format

display rollback state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to:

- Check whether the rollback function is enabled.
- Preview the files used after a version rollback to avoid an unexpected rollback.
- The rollback status can be displayed only if the **rollback** command can be used. Therefore, the **display rollback state** command can display the rollback status only when the following conditions are met: the system software for rollback exists, the current software package is different from the previous system software package, and no new package is specified for next startup using the **startup system-software** command.
- If no rollback system software exists, a message "Rollback function is disabled in current state" will be displayed when you run the **display rollback state** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Preview the files used after a version rollback. The names and paths of various startup files used in the rollback version are displayed if the rollback function is enabled in the system.

```
<Huawei> display rollback state
Info: Rollback function is enabled in current state
The booting parameters for rollback are as follows:
  Rollback system software:                sd1:/software.cc
  Rollback saved-configuration file:         sd1:/iascf_autobackup.zip
  Rollback license file:                   null
  Rollback patch package:                    null
  Rollback voice-files:                    null
```

Table 3-65 Description of the display rollback state command output

Item	Description
Rollback system software	System software package used after the rollback.
Rollback saved-configuration file	Configuration file used after the rollback.
Rollback license file	License file used after the rollback.
Rollback patch package	Patch file used after the rollback.
Rollback voice-files	Voice file used after the rollback.

Related Topics

3.13.18 rollback

3.13.10 license active

Function

The **license active** command activates the license file saved in the storage of the device.

Format

license active *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of a license file.	The value is a string of 1 to 64 characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Change or upgrade the license file when the current license file is outdated or needs higher specifications and more features. The initial state of a license file is inactive and the license file does not take effect in the system. Run this command to activate the new or updated license file.

The **license active** command can be used to activate a license file in the following situations:

- The license needs to be activated for the first time.

  You can directly run this command to activate a license.
- The current license file needs to be updated.

  If the specifications of the new license file are lower than those of the current license file, the system displays a message asking you whether to continue. If you choose **No**, the system retains the current license file. If you choose **Yes**, the master MPU activates the current license file and the system uses the new license file.

Prerequisites

The new license file has been uploaded to the device.

Follow-up Procedure

When the system restarts, the system activates the license file that was activated last time to ensure the license files are the same before and after restart.

Precautions

- The license file must use .dat as file name extension and be saved to the default root directory in the storage of the device.
- If no path is specified, the license file in the working path is activated by default.
- If the specifications of the new license file are lower than those of the current license file (some functions are authorized in the current license file, but not in the new license file, or the new license file allows fewer resources than the current one), the system displays a message asking you whether to continue.
- When applying for a license, ensure that the ESN is case sensitive. If the case of the device ESN is different from that of the ESN in the license file, the license file cannot be activated.

Example

Activate **license.dat** in the storage of the device.

```
<Huawei> license active license.dat
```

3.13.11 license active accept agreement

Function

The **license active accept agreement** command activates the ETU license.

The **undo license active accept agreement** command deactivates the ETU license.

By default, the ETU license is deactivated.

Format

license active accept agreement

undo license active accept agreement

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After the **license active accept agreement** command is executed, the system asks you whether to sign the agreement:

- If you enter **yes**, the agreement is signed and this event is logged.
- If you enter **no**, the ETU license is deactivated.

Example

Activate the ETU license.

```
<Huawei> license active accept agreement
Dear Customer,

You will active the interim ETU (Easy to Use) license for featured functions of the AR, please read the
followings carefully.

After the activation of the interim ETU license for featured functions of the AR, you can conduct evaluation
of the featured functio
ns for a period of sixty (60) days.After the sixty (60) days evaluation period, the interim license will
automatically convert to th
e perpetual license. Continuing use of the featured functions of the product after the evaluation period
requires the perpetual lice
nse, together with the additional payment. Otherwise please close the ETU license for featured functions,
and stop using the feature
d functions.
```

```
Without purchasing the perpetual license from Huawei, the continuing use of the product will constitute
the inappropriate use beyond
 the interim license and infringement of rights of Huawei. The activation of the software command line
interface will be evidence of
 your acceptance of the perpetual license. Huawei will reserve all necessary rights to prosecute and to seek
all remedies at law and
 in equity.

ACCEPT? Yes or No[y/n]:y
 INFO: Succeeded in activating the ETU license.
```

Deactivate the ETU license.

```
<Huawei> undo license active accept agreement
 INFO: Succeeded in inactivating the ETU license.
```

3.13.12 license emergency

Function

The **license emergency** command enables the emergency state for the license.

Format

license emergency

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system configuration is classified into maximum configuration, authorized configuration, and minimum configuration.

- In maximum configuration, the maximum number of dynamic resource items are configured. Static resource items and function items are configured according to license configuration.
- Authorization configuration means the functions and resources of the software configured on the basis of contract or special authorization. Authorized configuration depends on feature authorization of license files.
- The minimum configuration is the default configuration when no activated license file exists in the system. The minimum configuration varies according to products.

Configurations are classified to limit the bearer capability of the system in different running status.

When you run the **license emergency** command to enable the emergency state for the license, the system is free from license control. In this case, the system can run with the maximum configuration of dynamic resources and the license-defined configuration of static resources and functions. When the validity period of the emergency state expires, dynamic resources are controlled by the license again. One version is provided with three validity periods of emergency state, each lasting for seven days.

The purpose for enabling the emergency state for the GTL license is disaster tolerance. If an earthquake takes place, for example, this mechanism protects users' services from being affected.

Precautions

- The emergency state cannot be disabled manually.
- The emergency state can only be enabled three times for each license, and the license can keep in emergency state for 7 days each time.
- The next emergency state can be enabled only on the last day when the last emergency state expires.

Example

Enable the license emergency state.

```
<Huawei> license emergency
Warning: This operation will cause LCS into the EMERGENCY state. Continue? [Y/N]:y
Info: Emergency started cannot be stopped.
```

Related Topics

3.13.10 license active

3.13.13 license function

Function

The **license function** command activates the license of a function item.

The **undo license function** command deactivates the license of a function item.

By default, the license of a function item is deactivated.

Format

license function *name*

undo license function *name*

Parameters

Parameter	Description	Value
name	Specifies the name of the activated ETU license function item.	Enumeration value. The options are as follows: • **ac**: WLAN AC Express • **datae**: data service • **dsvpn**: DSVPN • **sece**: security service • **voicee**: voice service

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **license function** command activates the license of a function item through the ETU license.

Prerequisites

The ETU license has been activated using the **license active accept agreement** command.

Precautions

- If the **license active accept agreement** command is not executed, an error message is displayed.
- You do not need to activate the license that has been activated.
- After the license is activated, there is a trial period of 60 days. After the trial period of 60 days, you use of the controlled function will be governed by Huawei license agreement. You must purchase the license or stop using the activated function after the trial period.

Example

Activate the data service.

```
<Huawei> license function datae
 INFO: Succeeded in activating the feature.
```

3.13.14 license resource

Function

The **license resource** command activates the license of a resource item.

The **undo license resource** command deactivates the license of a resource item.

By default, the license of a resource item is deactivated.

Format

license resource *name value*

undo license resource *name*

Parameters

Parameter	Description	Value
name	Specifies the name of the activated ETU license resource item.	Enumeration value. The options are as follows: • **cm**: number of phones that are calling
value	Specifies the value of a resource item.	The value is an integer. The value range depends on the resource license.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **license resource** command activates the license of a resource item.

Prerequisites

The ETU license has been activated using the **license active accept agreement** command.

Precautions

- If the **license active accept agreement** command is not executed, an error message is displayed.

 Copyright © Huawei Technologies Co., Ltd.

- You do not need to activate the license that has been activated.
- After the license is activated, there is a trial period of 60 days. After the trial period of 60 days, your use of the controlled function will be governed by Huawei license agreement. You must purchase the license or stop using the activated function after the trial period.

Example

Activate the license of a resource item.

```
<Huawei> license resource cm 10
 INFO: Succeeded in activating the feature.
```

3.13.15 license revoke

Function

The **license revoke** command revokes a license file.

Format

license revoke

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

License is an authorization file. You can apply for, upgrade, or activate the license file to get corresponding user rights.

If new devices are deployed, you can purchase new licenses as needed to enable license-controlled features and functions on the devices. This reduces purchase costs. If the capacities of the existing devices need to be expanded, you can update the licenses used on the devices to enable more license-controlled features and functions.

You can upgrade a license file to:

- Add new features.
- Optimizes device performance.
- Fix bugs in the current version.

Before updating a license file, run the **license revoke** command to revoke the existing license. The system then returns a license revocation code. This code is the evidence for license invalidation and is used to apply for a new license.

NOTE

A license revocation code is a character string generated after a license file becomes invalid. You can determine that a license file is invalid based on the corresponding revocation code.

Precautions

- When the existing license is going to expire, apply for a new license, upgrade, and activate the license. If the license has expired, the service modules are disabled and services are interrupted.
- After you run the **license revoke** command, the license file enters the Trial state and cannot be activated again regardless of how long the license file will expire.

Example

Revoke the current license file.

```
<Huawei> license revoke
```

Related Topics

3.13.10 license active

3.13.16 patch delete all

Function

The **patch delete all** command deletes patches on the current system.

Format

patch delete all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

- If you find errors in patches that have been loaded to the system, run this command to delete the patches to prevent patch errors from affecting system operating.

- Before loading a non-incremental patch, run this command to delete the existing patches (if any). Otherwise, the non-incremental patch cannot be loaded.

Example

Delete all patches.

```
<Huawei> patch delete all
```

Related Topics

3.13.8 display patch-information

3.13.17 patch load

Function

The **patch load** command loads the patches to the patch areas in the system.

Format

patch load *filename* **all run**

Parameters

Parameter	Description	Value
filename	Specifies the path and file name of a patch package. The path can be an absolute path or a relative path.	The value is a string of5 to 64 case-insensitive characters without spaces. The file name must have an extension of .pat.
all	Loads the patches of all boards.	-
run	Runs loaded patches of all boards.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When you load a patch to the current system, the system searches the patch package for a matching patch file according to the attributes of the patch file.

- If a matching patch file is found in the patch package, the system loads the patch.
- If no matching patch file is found in the patch package, the system does not load any patch.

Prerequisites

The patch package has been uploaded to the root directory of the storage device.

Before loading a patch, the system must resolve the patch package, check the validity of the patch files in the patch package, and obtain the attributes such as the patch type and version of the patch file.

Precautions

The patch file cannot be reloaded. When you reload a patch, the system displays an error message.

Example

Load the patches to the patch area of the device and run the patches directly.

```
<Huawei> patch load patch.pat all run
```

Related Topics

3.13.16 patch delete all

3.12.30 startup patch

3.13.8 display patch-information

3.13.18 rollback

Function

The **rollback** command rolls back the system to the previous version.

NOTE

Format

rollback

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an error occurs during an upgrade, cancel the current upgrade and run the **rollback** command to roll back the system to the previous version. After the rollback, the configuration of the device is the same as the previous configuration before upgrading.

You can delete the rollback software using the **delete (user view)** command. After the rollback software is deleted, a message will be displayed saying that the rollback function is unavailable if you run the **rollback** and **display rollback state** commands.

Prerequisites

The device has the rollback software. The current software package is different from the previous software package, and no new package is configured for next startup using the **startup system-software** *system-file* command.

Example

Roll back the system to the previous version. After you run the command, a message will be displayed ask you whether to continue. If you choose **y**, the system rolls back to its previous version. If you choose **n**, no operation will be performed.

```
<Huawei> rollback
After rollback, active board will reboot automatically. Please check if data has
 been saved
Are you sure to rollback? (y/n)[n]:y
```

Related Topics

3.13.9 display rollback state

3.13.19 set output slot

Function

The **set output slot** command redirects LPU information to the SRU.

The **undo set output slot** command cancels redirection of LPU information to the SRU.

Format

set output slot *slot-id*

undo set output slot *slot-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID.	The value varies with the device configuration.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can upgrade the system software through the BIOS menu of the SAE card.

Precautions

- You can run this command to redirect output information of the SAE card but not other cards to the SRU.
- You can perform the redirection operation using only the Telnet provided by a Windows operating system, Putty.
- The terminal modes supported include VTY100, Linux, and Xterm.
- When the message "Press <DEL> or <F2> to enter setup" is displayed on the screen, you must press **F2** to enter the BIOS page.
- The up, down, left, and right buttons on the keyboard are displayed as **^**, **V**, **<**, and **>** on the BIOS page.
- If you use the Hyper Terminal provided by the Windows operating system to redirect output information, the device responses slowly because the default transmission rate of a serial port is 9600 bit/s. You are advised to change the rate to 115,200 bit/s and then establish a connection again.

Example

Redirect output information about the SAE card to the SRU.

```
<Huawei> system-view
[Huawei] set output slot 2
****************************************************
*             Slot  2 output to mainboard          *
****************************************************
Press Ctrl+D to quit
```

3.13.20 upgrade slot startup bootrom (User view)

Function

The **upgrade slot startup bootrom** command updates the BootROM of a board to the BootROM version of the system software.

NOTE

- MPUs on the AR100, AR120, and AR3200 series routers support this command.
- MPUs on the AR161, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR169FVW-8S, AR169G-L, AR169W-P-M9, and AR169RW-P-M9 among the AR160 series routers support this command.
- MPUs on the AR1220-8GE and AR1220C among the AR1200 series routers support this command.
- MPUs on the AR2204E, AR2204E-D, AR2204-24GE, AR2204-27GE-P, AR2204-51GE, AR2204-51GE-P, and AR2204-51GE-R among the AR2200 series routers support this command.

Format

upgrade slot *slot-id* **startup bootrom**

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID of a registered LPU.	The value varies with the device configuration.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Boards do not support automatic loading of the corresponding BootROM. Generally, the BootROM does not need to be upgraded. However, if an exception occurs due to a fault in the BootROM, you need to run this command to manually upgrade the BootROM.

If the main control board cannot automatically upgrade the BootROM during a system software upgrade, you need to run this command to manually upgrade the BootROM.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The 9ES2, 24ES2GP, 4ES2G-S, 4ES2GP-S, 1GEC, 4GECS, 2X10GL, 3G-HSPA+7, 3G-EVDO, 1LTE-L, 1LTE-LV, 1LTEC, 1LTE-Lt, 1LTE-Lo, 1LTE-Lc, 1STM1, 1STM4, 4STM1, 16FXS, 32FXS, 1GBIS4W, 1NDE, SMXH, and DGP cards do not support this command.

NOTICE

Ensure normal power supply to the device when you are manually upgrading the BootROM. The component whose BootROM is upgraded may be permanently damaged once the device is powered off during manual upgrade of the BootROM.

Example

Upgrade the BootROM in slot 1 using the current system software package.

```
<Huawei> upgrade slot 1 startup bootrom
<Huawei> upgrade slot 1 startup bootrom
Warning: You can not reset, remove, or power off the board when upgrade is being
 performed, are you sure to continue?[Y/N]:y
Info: Please waiting..
Info: Online upgrade slot <1>, item <BootRom>,  ok.
Info: Please reset the board in slot 1 to take effect.
Warning: The operation will reset the board in slot 1. Continue? [y/
n]:n
```

3.14 Smart Upgrade Commands

3.14.1 display smart-upgrade information

Function

The **display smart-upgrade information** command displays details about smart upgrade.

Format

display smart-upgrade information

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After smart upgrade is enabled on an AR router, you can run the **display smart-upgrade information** command to check details about smart upgrade. When smart upgrade is enabled on an AR router, the router is not in the progress of requesting for the latest version information from the HOUP, and this command is run on the router, the router proactively requests for the latest version information.

Prerequisites

Smart upgrade has been enabled using the **smart-upgrade enable** command.

Precautions

After this command is run, the router is triggered to exchange information with the HOUP. If this command is run frequently to query upgrade information, smart upgrade will be affected.

Example

Display details about smart upgrade.

```
<Huawei> system-view
[Huawei] smart-upgrade enable
Info: Operation succeeded.
[Huawei] quit
<Huawei> display smart-upgrade information
Info:Loading the information.Please wait for a few minutes.
Scheduled upgrade:            Enable
Next upgrade time:            2019-07-17 23:00:00

Check for new version:        Upgrade required
Recommended software version:  V200R010C00SPC600
Recommended patch version:     None
Upgrade description:
Firmware and Patch Description in English:1)description:2)description:

Info update time:             2019-06-17 14:17:06

Cancellation status:          Initial
Upgrade status:               Initial
Software package size(B):     155945856
Patch package size(B):        0
Download progress(%):         0
Download speed(KB/s):         0.00
Download status:              notStart
Software package name:        AR160-V200R010C00SPC600.cc
Patch package name:           None
Patch type:                   None
Last upgrade type:            now
Last upgrade time:            2019-06-17 15:49
Last upgrade result:          None

Device name:                  AR169
ESN:                          21500102152SF5900070
SoftWare version:             V200R009C00SPC500
Patch version:                V200R009SPH012

Last startup software::       flash:/ar160_spc500.cc
Last startup patch:           flash:/patch_ar160a.pat
Backup configuration file:    vrpcfg_auto_backup.zip
Last startup voice package:   None
Last startup license:         None
```

Table 3-66 Description of the **display smart-upgrade information** command output

Item	Description
Scheduled upgrade	Status of the scheduled upgrade policy: ● Enable: Scheduled upgrade is enabled. ● Disable: Scheduled upgrade is disabled.
Next upgrade time	Next upgrade time. This item is displayed only when scheduled upgrade is enabled.
Check for new version	Checked new version information. ● Upgrade required: The router needs to be upgraded. ● Network error: A network error occurs. ● System error: A system error occurs. ● Querying: Version information is being queried. ● Initial: Version information check is initialized. ● Lastest version installed: The router version is the latest.
Recommended software version	Recommended system software version.
Recommended patch version	Recommended patch version.
Firmware and Patch Description in English	Hardware and patch description in English.
Info update time	Update time.
Cancellation status	Upgrade cancellation status: ● Initial: Upgrade cancellation is initialized. ● Cancelling: The upgrade is being canceled. ● Failed: The upgrade fails to be canceled. ● Successful: The upgrade is successfully canceled. ● None

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Upgrade status	Upgrade status: ● Initial: The upgrade is initialized. ● Upgrading: The router is being upgraded. ● Failed: The upgrade fails. ● Cancelled: The upgrade is canceled. ● Successful: The upgrade succeeds.
Software package size(B)	Software package size.
Patch package size(B)	Patch package size.
Download progress(%)	File download progress, in percentage.
Download speed(KB/s)	File download speed.
Download status	File download status: ● Initial: File download is initialized. ● downloadFailed: File download fails. ● downloadCancelled: File download is canceled. ● notStart: File download does not begin. ● downloadSucc: File download succeeds. ● downloading:%d: file download progress
Software package name	Software package name.
Patch package name	Patch package name.
Patch type	Patch type.
Last upgrade type	Last upgrade mode: ● timing: scheduled upgrade ● now: immediate upgrade ● None
Last upgrade time	Last upgrade time.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last upgrade result	Last upgrade result: ● cfgfailed: The configuration fails. ● rollback: The version is rolled back. ● successed: The upgrade succeeds. ● netError: A network error occurs. ● updating: The router is being upgraded. ● None
Device name	Device name.
ESN	ESN of the router.
SoftWare version	Software version.
Patch version	Patch version.
Last startup software	Software version for the last startup.
Last startup patch	Patch version for the last startup.
Backup configuration file	Backed up configuration file.
Last startup voice package	Voice package for the last startup.
Last startup license	License information for the last startup.

Related Topics

3.14.2 smart-upgrade enable
3.14.3 smart-upgrade information
3.14.4 smart-upgrade right-now
3.14.5 smart-upgrade time

3.14.2 smart-upgrade enable

Function

The **smart-upgrade enable** command enables smart upgrade.

The **undo smart-upgrade enable** command disables smart upgrade.

By default, smart upgrade is disabled.

Format

smart-upgrade enable

undo smart-upgrade enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To facilitate software upgrade management and reduce manual maintenance costs of routers, you can run the **smart-upgrade enable** command to enable smart upgrade. Smart upgrade achieves automatic new version detection, system file download, and router upgrade by connecting routers to the HOUP through the Internet.

Example

Enable smart upgrade.

```
<Huawei> system-view
[Huawei] smart-upgrade enable
Info: Operation succeeded.
```

3.14.3 smart-upgrade information

Function

The **smart-upgrade information** command sets the contact number and email address for smart upgrade.

The **undo smart-upgrade information** command cancels the contact number and email address for smart upgrade.

By default, no contact number or email address is set for smart upgrade.

Format

smart-upgrade information telephone *telephonenum* **email** *emailaddress*

undo smart-upgrade information telephone

Parameters

Parameter	Description	Value
telephone *telephonenum*	Specifies the contact number.	The value is a string of 1 to 21 characters. The value can contain the plus sign (+) and digits (0 to 9), and cannot contain spaces. The plus sign (+) can be used only at the beginning of a character string. If a character string starts with a plus sign (+), the maximum string length is 21. If a character string starts with a digit, the maximum string length is 20.
email *emailaddress*	Specifies the email address.	The value is a string of 1 to 128 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), and underscores (_).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **smart-upgrade information** command to set the contact number and email address for smart upgrade. If a smart upgrade-enabled router fails to be upgraded, the router can notify the user of the upgrade result based on the configured contact number and email address.

NOTE

The contact number and email address are used only for emergency contact upon an upgrade failure.

Prerequisites

Smart upgrade has been enabled using the **smart-upgrade enable** command.

Example

Set the contact number and email address for smart upgrade.

```
<Huawei> system-view
[Huawei] smart-upgrade enable
Info: Operation succeeded.
[Huawei] smart-upgrade information telephone 111111111 email test@huawei.comPrivacy Policy Your
privacy is important to us.
When enabling the automatic upgrade function for Huawei devices, you may, at your discretion, provide
```

```
your personal information such as the telephone number, mobile number, and email address on the
Command Line Interface (CLI).
This information will be used to notify you immediately of the upgrade result after the automatic upgrade
function is enabled.
By agreeing to these terms and conditions, you are authorizing Huawei to collect and process the
aforementioned personal information provided by you for the stated purpose.
Your information may be transferred to a third party of Huawei or affiliated company of Huawei for the
purpose of providing the aforementioned service for you.
The information you provide will be stored on the servers of Huawei and its affiliates.
The information may be transmitted outside your country or region and accessed, stored, and processed in
another country or region, including China.
Huawei is committed to protecting your personal information and preventing the information from being
used without authorization.
For more details, please refer to the full privacy policy at https://www.huawei.com/en/privacy-policy.
Do you agree to these terms and conditions? (Y/N)[N]:y Info: Operation succeeded.
```

Related Topics

3.14.2 smart-upgrade enable

3.14.4 smart-upgrade right-now

Function

The **smart-upgrade right-now** command performs smart upgrade on a router immediately.

Format

smart-upgrade right-now

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a router figures out that there is a new version available for upgrade on the HOUP, that is, the **Check for new version** field is displayed as **Upgrade required** in the **display smart-upgrade information** command output, you can run the **smart-upgrade right-now** command to perform smart upgrade on the router immediately. The router then obtains the new version file from the HOUP and starts an upgrade.

Prerequisites

Smart upgrade has been enabled using the **smart-upgrade enable** command.

Precautions

- After this command is run, the router automatically obtains the version file from the HOUP and starts an upgrade immediately. During the upgrade, original upgrade configurations will be deleted, and the current upgrade configurations are used. In addition, when a router restarts, it automatically saves and backs up configurations to the file named **vrpcfg_auto_backup.zip** or **vrpcfg_auto_backup.cfg**. However, to avoid unexpected configuration loss, you are advised to save the current configuration and export the configuration file in advance.
- After the device obtains the software version file, the system prompts the user whether to restart the device. By default, if the user does not perform any operation within 30 seconds, the device is automatically restarted.

Example

Perform smart upgrade on a router immediately.

```
<Huawei> system-view
[Huawei] smart-upgrade enable
Info: Operation succeeded.
[Huawei] smart-upgrade right-now
Info: Connecting to the smart upgrade platform...Please wait for a few minutes.
Info: Starting to download file AR120-V200R010C00SPC600.cc
100%
Info: Downloading file AR120-V200R010C00SPC600.cc succeeded.
smart-upgrade: 155944876 byte(s) received in 433 second(s) 355.71Kbyte(s)/sec.
Info: Starting to download file AR120-V200R010C00SPC600.cc.asc
Info: Verifying the system software package using the signature file ....................
........
Info: Verification succeeded.
Info: The device needs to be reboot to proceed with the upgrade. Continue? (Y will be selected by default
30 seconds later)(Y/N)[Y]:Y
```

3.14.5 smart-upgrade time

Function

The **smart-upgrade time** command sets the scheduled smart upgrade policy.

The **undo smart-upgrade time** command cancels the scheduled smart upgrade policy.

By default, the start time or interval for scheduled smart upgrade is not set.

Format

smart-upgrade time *HH:MM:SS* { **weekly** | **monthly** | **yearly** }

undo smart-upgrade time

Parameters

Parameter	Description	Value
HH:MM:SS	Specifies the upgrade start time.	In the parameter: • *HH* specifies the hour. The value is an integer that ranges from 0 to 23. • *MM* indicates the minute. The value is an integer that ranges from 0 to 59. • *SS* indicates the second. The value is an integer that ranges from 0 to 59.
weekly	Upgrades a router at an interval of seven days. The interval starts from the upgrade time specified by *HH:MM:SS*.	-
monthly	Upgrades a router at an interval of 30 days. The interval starts from the upgrade time specified by *HH:MM:SS*.	-
yearly	Upgrades a router at an interval of 365 days. The interval starts from the upgrade time specified by *HH:MM:SS*.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a router figures out that there is a new version available for upgrade on the HOUP, that is, the **Check for new version** field is displayed as **Upgrade required** in the **display smart-upgrade information** command output, you can run the **smart-upgrade time** command to set the start time and interval for smart upgrade. After the configuration is completed, once the specified time arrives, the

router is triggered to obtain the new version file from the HOUP and starts an upgrade.

Prerequisites

Smart upgrade has been enabled using the **smart-upgrade enable** command.

Precautions

- The *HH:MM:SS* parameter must be in 24-hour format. If you do not specify *MM:SS*, their values are 0. You must enter at least one digit to specify *HH*. For example, when you enter 0, the time is 00:00:00.
- After this operation is performed, once the specified time arrives, the router is triggered to obtain the new version file and starts an upgrade. During the upgrade, original upgrade configurations will be deleted, and the current upgrade configurations are used. In addition, when a router restarts, it automatically saves and backs up configurations to the file named **vrpcfg_auto_backup.zip** or **vrpcfg_auto_backup.cfg**. However, to avoid unexpected configuration loss, you are advised to save the current configuration and export the configuration file in advance.
- When an upgrade policy is configured, the time for triggering smart upgrade depends on the device time. If the configuration is completed, and the device time is changed and is later than the next automatic upgrade time, smart upgrade is triggered immediately on the device. During the upgrade, the device may be automatically restarted multiple times. Exercise caution when deciding to change the device time. In addition, remember to save the device configuration in a timely manner.

Example

Configure a router to be upgraded at an interval of seven days after an upgrade is triggered at 23:00:00.

```
<Huawei> system-view
[Huawei] smart-upgrade enable
Info: Operation succeeded.
[Huawei] smart-upgrade time 23:00:00 weekly
Info: Operation succeeded.
```

Related Topics

3.14.2 smart-upgrade enable

4 Device Management Commands

About This Chapter

4.1 Device Status Checking Commands
4.2 Hardware Configuration Commands
4.3 Information Center Configuration Commands
4.4 NTP Configuration Commands
4.5 Fault Management Commands
4.6 Commands for Clock Source
4.7 Energy-saving Configuration Commands
4.8 PoE Configuration Commands
4.9 OIDS Configuration Commands
4.10 OPS Configuration Commands

4.1 Device Status Checking Commands

4.1.1 display cpu-usage

Function

The **display cpu-usage** command displays CPU usage statistics.

Format

display cpu-usage [**slot** *slot-id*]

display cpu-usage [**process** *process-id*] [**slave**]

Parameters

Parameter	Description	Value
process *process-id*	Displays CPU usage statistics of a specified process.	The value is an integer and must be set according to the device configuration.
slot *slot-id*	Displays CPU usage statistics on the board in a specified slot. If the **slot** parameter is not specified, CPU usage of the MPU is displayed. **NOTE** The AR100&AR120&AR150&AR160&AR200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R do not support the **slot** *slot-id* parameter.	The value is an integer and must be set according to the device configuration.
slave	Displays the CPU usage statistics of a specified LPU. **NOTE** Only AR3200 series support this parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

CPU usage is an important indicator to evaluate device performance. A high CPU usage will cause service faults, for example, BGP route flapping, frequent VRRP active/standby switchover, and even failed device login. You can use the **display cpu-usage** command to view CPU usage in real time and check whether the device is working properly.

This command displays information about the CPU usage on the MPU or the specified interface board. If the **slave** or **slot** *slot-id* is not specified, the CPU usage of the master MPU is displayed.

Example

Display the CPU usage on the master MPU.

```
<Huawei> display cpu-usage
CPU   Usage Stat. Cycle: 10 (Second)
CPU   Usage Stat. Time : 2013-09-24  10:11:55
Control Plane
```

```
   CPU Usage: 23.3%   Max: 100%
   User: 10.7%   System:  6.9%   SoftIrq:  0.0%   HardIrq:  5.5%   Idle: 76.7%
   CPU utilization for ten seconds: 23.3%  one minute:  22.0%  five minutes:  2
3.0% .
Data    Plane
   CPU Usage:  1.7%   Max: 100%
   CPU utilization for ten seconds:  1.7%  one minute:   1.6%  five minutes:
1.6% .

PID   ProcessName         CPU%     CoreIndex      Runtime     State
194   cap32               1.7%      CPU1           26132042    R
193   vrp                20.0%      CPU0           11216335    S
191   monitor             0.0%      CPU0           2324        S
74    loop0               0.0%      CPU0           1913        S
13    bdi-default         0.0%      CPU0           977         S
7     events/0            0.0%      CPU0           708         S
138   k3gdevd             0.0%      CPU0           423         S
192   cap32               0.0%      CPU0           211         S
12    sync_supers         0.0%      CPU0           204         S
56    VFDS                0.0%      CPU0           166         S
1     init                0.0%      CPU0           90          S
19    kswapd0             0.0%      CPU0           63          S
30    mtdblockd           0.0%      CPU0           35          S
16    khubd               0.0%      CPU0           10          S
2     kthreadd            0.0%      CPU0           0           S
3     migration/0         0.0%      CPU0           0           S
4     ksoftirqd/0         0.0%      CPU0           0           S
5     migration/1         0.0%      CPU0           0           S
6     ksoftirqd/1         0.0%      CPU0           0           S
8     events/1            0.0%      CPU0           0           R
9     cpuset              0.0%      CPU0           0           S
10    khelper             0.0%      CPU0           0           S
11    async/mgr           0.0%      CPU0           0           S
14    kblockd/0           0.0%      CPU0           0           S
15    kblockd/1           0.0%      CPU0           0           S
20    aio/0               0.0%      CPU0           0           S
21    aio/1               0.0%      CPU0           0           S
22    crypto/0            0.0%      CPU0           0           S
23    crypto/1            0.0%      CPU0           0           S
29    sdcardqueue         0.0%      CPU0           0           S
139   k3gtxd              0.0%      CPU0           0           S
153   udpsvd              0.0%      CPU0           0           S
271   loop1               0.0%      CPU0           0           S
486   flush-mtd-unmap     0.0%      CPU0           0           S
```

Table 4-1 Description of the **display cpu-usage** command output

Item	Description
CPU Usage Stat. Cycle	Interval for collecting CPU usage statistics. The default interval is 10 seconds.
CPU Usage Stat. Time	Time when the latest CPU usage statistics are collected.
Control Plane	Latest CPU statistics on the control plane.
Data Plane	Latest CPU statistics on the forwarding plane.
CPU Usage	Current CPU usage
Max	Highest CPU usage in history.

Item	Description
User	User usage.
System	CPU usage.
SoftIrq	CPU usage when soft interruption is running.
HardIrq	CPU usage when hardware interruption is running.
Idle	CPU usage in idle.
CPU utilization for ten seconds	CPU usage in 10 seconds.
one minute	CPU usage in 1 minute.
five minutes	CPU usage in 5 minutes.
PID	Process ID.
ProcessName	Process name.
CPU%	CPU usage percent of each task to the total CPU usage.
CoreIndex	CPU index.
Runtime	System running time calculated based on CPU tick.
State	Status of a running process. The value is of the enumerated type: ● R: runnable state ● S: interruptible sleep state ● D: uninterruptible sleep state ● T: stopped or traced state ● Z: exiting state (zombie process) ● X: exiting state (the process is about to be destroyed)

4.1.2 display cpu-usage configuration

Function

The **display cpu-usage configuration** command displays CPU usage configuration.

Format

display cpu-usage configuration [**slave** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays CPU usage configuration of the board in a specified slot. If this parameter is not specified, CPU usage configuration of the main control board is displayed. **NOTE** The AR100&AR120&AR150&AR160&AR200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R do not support the **slot** *slot-id* parameter.	The value is an integer and must be set according to the device configuration.
slave	Displays CPU usage configuration of the slave control board. **NOTE** Only AR3200 series support this parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the alarm threshold and recovery threshold.

- When CPU usage reaches the alarm threshold, the system generates a CPU usage alarm.
- When CPU usage falls within the recovery threshold, the system generates a clear alarm.

Example

Display CPU usage configuration of the main control board.

```
<Huawei> display cpu-usage configuration
Master Board:
The CPU usage monitor is turned on.
The CPU thread usage monitor is turned on.
The current monitor cycle is 10 seconds.
The current monitor warning threshold is 80%.
The current monitor restore threshold is 75%.
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-2 Description of the display cpu-usage configuration command output

Item	Description
The CPU usage monitor	Whether the function of the CPU usage monitor is enabled or disabled.
The CPU thread usage monitor	Thread CPU usage monitoring switch of the device.
The current monitor cycle	Cycle for monitoring the CPU.
The current monitor warning threshold	Alarm threshold. To set the CPU usage alarm threshold, use the **set cpu-usage threshold** *threshold-value* [**slot** *slot-id*] command.
The current monitor restore threshold	Alarm recovery threshold. To set the CPU usage alarm recovery threshold, use the **set cpu-usage threshold** *threshold-value* **restore** *restore-threshold-value* [**slot** *slot-id*] command.

Related Topics

4.2.14 set cpu-usage threshold

4.1.3 display device

Function

The **display device** command displays the type and status of the components on a device.

Format

display device [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the type and status of components in a specified slot. If this parameter is not specified, the type and status of all components on the device are displayed.	The value is an integer and must be set according to the device configuration.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the working status of components on a device and check whether the device is working normally.

Example

Display information about the components on a device.

```
<Huawei> display device
AR2240's Device status:
Slot  Sub Type            Online   Power     Register      Alarm        Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1     -   2FE             Present  PowerOn   Registered    Normal       NA
2     -   1SA             Present  PowerOn   Registered    Normal       NA
3     -   1CPOS-155M       Present  PowerOn   Registered    Normal       NA
4     -   1ADSL-A/M        Present  PowerOn   Registered    Normal       NA
5     -   8FE1GE           Present  PowerOn   Registered    Normal       NA
6     -   -               Present  PowerOff  Unregistered  TimeOutReg   NA
8     -   1STM4            Present  PowerOn   Registered    Normal       NA
11    -   SRU40            Present  PowerOn   Registered    Normal       Master
9     -   PWR350A          Present  PowerOn   Registered    Normal       NA
12    -   FAN              Present  PowerOn   Registered    Normal       NA
```

Table 4-3 Description of the display device command output

Item	Description
Slot	Number of the slot where a component is installed.
Sub	Subcard number.
Type	Type of a component. **NOTE** In V200R005, the type of 1ADSL-B and 1ADSL-B/J cards is displayed as 1ADSL-B/J. In earlier versions, the type of the two cards is displayed as 1ADSL-B. You can check the PCB version to distinguish the two types of cards.
Online	Whether a component is installed. ● Present: indicates that the component is installed. ● Absent: indicates that the component is not installed.
Power	Whether a component is powered on. ● PowerOn: indicates that the component is powered on. ● PowerOff: indicates that the component is powered off. ● NA: indicates that the state is unknown. This value may be displayed after the device restarts.

Item	Description
Register	Whether a component is registered. ● Registered: indicates that the component is registered. ● Unregistered: indicates that the component is unregistered.
Alarm	Displays the reason why a component is powered off when a board is powered off: ● Normal: indicates that the component is running normally. ● PowerSetFail: indicates that the command-configured power-on fails. ● Nonsupport: indicates that the current version does not support the board or the current MPU does not the board in a specified slot. ● TimeOutReg: indicates that the board is not registered for a long period. ● UserSetOff: indicates that the power-off is configured by a command. ● LackPower: indicates that the power is insufficient. ● InfoGetFail: indicates that obtaining board information fails. **NOTE** The Alarm field may display either of the following values for a SAE card: ● Unconnected: The data link between the card and the device is disconnected. ● Normal: The data link between the card and the device is working normally.
Primary	Master/Slave status of a card. Slave indicates the slave card and Master indicates the master card. NA is displayed on other components.

Display component information in slot 1.

```
<Huawei> display device slot 1
AR2240's Device status:
Slot  Sub Type              Online   Power     Register      Alarm     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1     -   8FE1GE            Present  PowerOn   Registered    Normal    NA

-------------------------------------------------------------------------------
  Board Name        : 8FE1GE
  Board Description : 9-port 8FE/1GE  L2/L3 Ethernet Interface Card
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
  Port   Port     Optic    MDI     Speed    Duplex    Flow-    Port     POE
         Type     Status          (Mbps)            Ctrl     State    State
-------------------------------------------------------------------------------
   0     ETH(C)   -        auto    100      full      disable  up       -
   1     ETH(C)   -        auto    100      full      disable  up       -
```

```
 2    ETH(C)   -       auto    100     full     disable  up      -
 3    ETH(C)   -       auto    100     full     disable  down    -
 4    ETH(C)   -       auto    100     full     disable  down    -
 5    ETH(C)   -       auto    100     full     disable  down    -
 6    ETH(C)   -       auto    100     full     disable  down    -
 7    ETH(C)   -       auto    100     full     disable  down    -
 8    GE(C)    -       auto    1000    full     disable  up      -
-------------------------------------------------------------------------------
```

Table 4-4 Description of the display device slot command output

Item	Description
Slot	Number of the slot where a component is installed.
Sub	Subcard number.
Type	Type of a component. **NOTE** In V200R005, the type of 1ADSL-B and 1ADSL-B/J cards is displayed as 1ADSL-B/J. In earlier versions, the type of the two cards is displayed as 1ADSL-B. You can check the PCB version to distinguish the two types of cards.
Online	The component status is **Present**, indicating that the component is installed.
Power	The component status is **PowerOn**, indicating that the component is powered on.
Register	The component status is **Registered**, indicating that the component is registered.
Alarm	The component status is **Normal**, indicating that the component runs normally.
Primary	Master/Slave status of a card. Slave indicates the slave MPU; Master indicates the master MPU. NA is displayed on other components.
Board Name	Name of the card in the specified slot.
Board Description	Description of the card in the specified slot.
Port	Number of an interface in the specified slot.
Port Type	Type of an interface in the specified slot.
Optic Status	Whether the optical module on an interface is working.
MDI	Interface cable type: ● across: crossover cable ● auto: automatically identified cable ● normal: straight-through cable
Speed (Mbps)	Interface rate, in Mbit/s.

Item	Description
Duplex	Duplex mode of the interface: ● half: half-duplex mode ● full: full-duplex mode **NOTE** Only Ethernet interfaces support the full-duplex mode. You can configure an Ethernet interface to work in full-duplex mode using the **5.2.2 auto duplex** command. If a card is not an Ethernet interface card (such as the 1E1T1-M/2E1T1-M interface card), this field displays -.
Flow-Ctrl	Flow control status on the interface: ● enable: Flow control is enabled on the interface. ● disable: Flow control is disabled on the interface.
Port State	Interface status: ● up: The interface is Up. ● down: The interface is Down.
POE State	PoE status of the interface.

4.1.4 display diagnostic-information

Function

The **display diagnostic-information** command collects and displays current device diagnostic information or stores diagnostic information in the specified compressed package with one click.

NOTE

The specified compressed package contains the one-click diagnostic information file, user logs, diagnostic logs, and data dictionary file.

Format

display diagnostic-information [*file-name*]

Parameters

Parameter	Description	Value
file-name	Specifies the name of the file where diagnostic information is stored.	The value is a string of 5 to 64 characters. The file name extension must be .txt or .tar. The default directory where files are stored is as follows: • AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204E, AR2204E-D, AR2240C, AR2204, AR2220E, AR2204-51GE, AR2204-E, AR2204-51GE-R, AR2204-27GE-S: flash:/ • AR2220, AR2240, AR3200 series, AR3600 series: sd1:/

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a fault occurs in the system, you can use the **display diagnostic-information** command to collect diagnostic information for fault location.

The **display diagnostic-information** command output includes the output for multiple **display** commands, such as **3.7.4 display clock**, **4.1.19 display version**, and **3.12.8 display current-configuration**. Running the **display diagnostic-information** command is like running these **display** commands in batches.

Precautions

- If the *file-name* parameter is not specified, diagnostic information is only displayed on the screen. If the *file-name* parameter is specified, diagnostic information is only stored to a specified file but not displayed on the screen.
- If this command displays a long output, press **Ctrl+C** to abort this command.
- This command displays diagnostic information, which helps locate faults but may affect system performance. For example, CPU usage may become high. Therefore, do not use this command when the system is running properly.
- Running the **display diagnostic-information** command simultaneously on multiple terminals connected to the device is prohibited. This is because CPU usage of the device may obviously increase and the device performance may be degraded.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display diagnostic information about the device.

```
<Huawei> display diagnostic-information
==================================================
  ===============display version===============
==================================================
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.120 (AR2200 V200R003C00)
Copyright (C) 2011-2012 HUAWEI TECH CO., LTD
Huawei AR2240 Router uptime is 0 week, 1 day, 0 hour, 11 minutes
BKP 0 version information:
1. PCB      Version  : AR01BAK2B VER.A
2. If Supporting PoE : No
3. Board    Type     : AR2240
4. MPU Slot Quantity : 1
5. LPU Slot Quantity : 8

MPU 11(Master) : uptime is 0 week, 1 day, 0 hour, 11 minutes
SDRAM Memory Size    : 2048     M bytes
Flash Memory Size    : 16       M bytes
NVRAM Memory Size    : 512      K bytes
SD Card1 Memory Size : 1882     M bytes
MPU version information :
1. PCB      Version  : AR01SRU3A VER.B
2. MAB      Version  : 0
3. Board    Type     : SRU40
4. CPLD0    Version  : 104
5. CPLD1    Version  : 104
6. BootROM  Version  : 604

LPU 1 : uptime is 0 week, 1 day, 0 hour, 8 minutes
SDRAM Memory Size    : 96       K bytes
Flash Memory Size    : 384      K bytes
LPU version information :
1. PCB      Version  : AR01SEG1CA VER.B
2. MAB      Version  : 0
3. Board    Type     : 2FE
4. BootROM  Version  : cb

LPU 5 : uptime is 0 week, 1 day, 0 hour, 7 minutes
SDRAM Memory Size    : 256      M bytes
Flash Memory Size    : 16       M bytes
LPU version information :
1. PCB      Version  : AR01WMF9TTA VER.B
2. MAB      Version  : 0
3. Board    Type     : 8FE1GE
4. BootROM  Version  : 213
5. BootLoad Version  : 510

FAN version information :
1. PCB      Version  : AR01DF05A VER.A
2. Board    Type     : FAN
3. Software Version  : 103

==================================================
  ===============display clock===============
==================================================
2012-09-05 11:15:23
Wednesday
Time Zone(Default Zone Name) : UTC+00:00
==================================================
  ===============display device===============
==================================================
AR2240's Device status:
Slot  Sub Type              Online   Power     Register     Alarm     Primary
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1     -   2FE               Present  PowerOn   Registered   Normal    NA
```

```
5     -   8FE1GE            Present  PowerOn   Registered    Normal    NA
11    -   SRU40             Present  PowerOn   Registered    Normal    Master
9     -   PWR350A           Present  PowerOn   Registered    Normal    NA
12    -   FAN               Present  PowerOn   Registered    Normal    NA

ii
```

Table 4-5 Description of the **display diagnostic-information** command output

Item	Description
display version	System software version. For details, see **4.1.19 display version**.
display clock	Current date and time. For details, see **3.7.4 display clock**.
display device	Component information. For details, see **4.1.3 display device**.

Save diagnostic information to the file **aa.txt** in the flash memory.

```
<Huawei> display diagnostic-information flash:/aa.txt
  This operation will take several minutes, please wait.........................
.................................................................
Info: The diagnostic information was saved to the device successfully..
```

Related Topics

4.1.19 display version
3.7.4 display clock
3.12.8 display current-configuration
4.1.3 display device

4.1.5 display elabel

Function

The **display elabel** command displays the electronic label of the device.

Format

display elabel [*slot-id*] [**brief**]

display elabel backplane

Parameters

Parameter	Description	Value
backplane	Displays the electronic label of the backplane.	-

Parameter	Description	Value
slot-id	Displays the electronic label of the specified board. If this parameter is not specified, all electronic labels of the device are displayed.	The value is an integer and must be set according to the device configuration.
brief	Indicates that the electronic label of a board does not include optical module information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Electronic labels identify the hardware. You can use the **display elabel** command to view the electronic label information.

Example

Display brief information about the electronic label of the board in slot 1.

```
<Huawei> display elabel 1 brief
 It is executing, please wait...


[Slot_1]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0


[Main_Board]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=AR01SEF2TA
BarCode=020XTQ10BA000063
Item=03020XTQ
Description=AR,AR01SEF2TA,2-Port FE WAN Interface Card,1*2
Manufactured=2011-10-15
VendorName=Huawei
IssueNumber=00
CLEICode=56324
BOM=02352868
```

Display detailed information about electronic labels of the device.

```
<Huawei> display elabel
 It is executing, please wait...


/$[System Integration Version]
/$SystemIntegrationVersion=3.0


[Rack_1]
[SubRack_0]


[BackPlane_0]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=AR0B0024BA
BarCode=2102113373P0BA000130
Item=02113373
Description=AR2200,AR0B0024BA,AR2240 CHASSIS
Manufactured=2011-10-10
VendorName=Huawei
IssueNumber=00
CLEICode=56325
BOM=02352869



[Slot_0]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0


[Main_Board]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=AR01WMF9TTA
BarCode=020XTN10BA000044
Item=03020XTN
Description=AR,AR01WMF9TTA ,8-Port 10/100BASE(RJ45) and 1-Port 10/100/1000BASE(R
J45)-L2/L3 Ethernet Interface Card ,1*1
Manufactured=2011-10-11
VendorName=Huawei
IssueNumber=00
CLEICode=56326
BOM=02352870


[Slot_9]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0


[Main_Board]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=AR01PSAC35
BarCode=2102310CWN10B6000195
Item=02310CWN
Description=AR Series,AR01PSAC35,350W AC Power Module
Manufactured=2011-06-09
```

```
VendorName=Huawei
IssueNumber=00
CLEICode=56327
BOM=02352871



[Slot_12]
/$[Board Integration Version]
/$BoardIntegrationVersion=3.0


[Main_Board]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=AR01DF05A
BarCode=21021206134JB9000205
Item=02120613
Description=AR2200,AR01DF05A,Fan Box For AR2240
Manufactured=2011-09-21
VendorName=Huawei
IssueNumber=00
CLEICode=56328
BOM=02352872
```

Display the electronic label of the backplane.

```
<Huawei> display elabel backplane
 It is executing, please wait...


[BackPlane_0]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=AR0B0024BA
BarCode=2102113373P0BA000130
Item=02113373
Description=AR2200,AR0B0024BA,AR2240 CHASSIS
Manufactured=2011-10-10
VendorName=Huawei
IssueNumber=00
CLEICode=56329
BOM=02352873
```

Table 4-6 Description of the display elabel command output

Item	Description
BoardType	Board model of the specified component.
BarCode	Bar code of the specified component.
Item	BOM code of the specified component.
Description	English description of the specified component.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Manufactured	Production date of the specified component.
VendorName	Vendor name of the specified component.
IssueNumber	Issuing number of the specified component.
CLEICode	CLEI code of the specified component.
BOM	Sales BOM code of the specified component.

Related Topics

4.2.1 backup elabel

4.1.6 display esn

Function

The **display esn** command displays the Equipment Serial Number (ESN) of a device.

Format

display esn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ESN uniquely identifies a device. During the request for a license, the ESN is required. You can use the **display esn** command to view the ESN of the device.

Example

Display the ESN of the device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display esn
 ESN of device: 2102113374P0B4000046
```

4.1.7 display fan

Function

The **display fan** command displays the fan status.

NOTE

This command is not supported by the AR100&AR120&AR150&160&200 series.

Format

display fan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Devices can run properly when fans are working properly. If proper heat dissipation cannot be ensured for devices, devices may overheat, damaging the hardware. You can use the **display fan** command to view the fan status.

Example

Display the fan status of the device.

```
<Huawei> display fan
-------------------------------------------------------------------
        FanId  FanNum  Present  Register  Speed  Mode
-------------------------------------------------------------------
        12     [1-5]   YES      YES        34%  AUTO
                1                   2100
                2                   2040
                3                   2100
                4                   2130
                5                   2100
```

Table 4-7 Description of the display fan command output

Item	Description
FanId	ID of a fan.

Item	Description
FanNum	Number of fans.
Present	Whether a fan is installed properly: ● YES: The fan is installed properly. ● NO: The fan is not installed properly.
Register	Whether a fan is registered: ● YES: The fan is registered. ● NO: The fan is not registered.
Speed	Fan speed. This field refers to the percentage of the current fan speed to the full speed of the fan, or the actual fan speed, in Revolution(s) Per Minute (RPM). **NOTE** **NA** indicates a failure to obtain the fan speed.
Mode	Working mode of a fan: ● AUTO ● MANUAL

Related Topics

4.7.7 set fan-speed

4.1.8 display health

Function

The **display health** command displays the health status of the device.

Format

display health

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To learn about the device temperature, power supply, fan information, power, CPU usage, memory usage, and storage medium, use the **display health** command to view the health status.

Example

Display the health status of the device.

```
<Huawei> display health
-------------------------------------------------------------------------------
 Slot   Card   Sensor No.   SensorName          Status  Upper  Lower  Temp(C)
-------------------------------------------------------------------------------
 1      -      1            8FE1GE TEMP         NORMAL  85     0      45

 5      -      1            8FE1GE TEMP         NORMAL  85     0      45

 11     -      1            SRU40 TEMP          NORMAL  70     0      50

-------------------------------------------------------------------------
 PowerNo  Present  Mode   State      Current(A)   Voltage(V)   Power(W)
-------------------------------------------------------------------------
   9      YES     AC     Supply     N/A          12           350
   10     NO      N/A    N/A        N/A          N/A          N/A
-------------------------------------------------------------------
        FanId  FanNum  Present  Register  Speed  Mode
-------------------------------------------------------------------
        12     [1-5]   YES      YES        35%  AUTO
                1                    2100
                2                    2100
                3                    2100
                4                    2160
                5                    2130
 The total  power is : 350.000(W)
 The remain power is : 272.000(W)
 The system used power detail information :
-------------------------------------------------------------------------------
  SlotID  BoardType    Power-Used(W)  Power-Requested(W)
-------------------------------------------------------------------------------
  1       8FE1GE       3.010          4
  5       8FE1GE       9.530          13
  11      SRU40        42.000         61
System CPU Usage Information:
 System cpu usage at 2012-09-05  15:02:35 570 ms
-------------------------------------------------------------------------------
  SlotID  CPU Usage  Upper Limit
-------------------------------------------------------------------------------
  5       4 %        80%
  11      6 %        80%
System Memory Usage Information:
 System memory usage at 2012-09-05  15:02:35 640 ms
-------------------------------------------------------------------------------
  SlotID  Total Memory(MB)  Used Memory(MB)  Used Percentage  Upper Limit
-------------------------------------------------------------------------------
  5       176               20               11%              95%
  11      1257              194              15%              95%
System Disk Usage Information:
 System disk usage at 2012-09-05  15:02:35 710 ms
-------------------------------------------------------------------------------
  SlotID  Device        Total Available     Used Memory(MB)    Used Percentage
                        Memory(MB)
-------------------------------------------------------------------------------
  11      sd1:    1882.51              1000.51            53.15%
          flash:  2.00                 0.18               9.00%
```

Table 4-8 Description of the display health command output

Item	Description
Slot	Slot ID of a physical entity.
Card	Subcard where a physical entity is located.
Sensor No.	Serial number of the sensor on a physical entity.
SensorName	Name of the sensor on a physical entity. **NOTE** In V200R005, the type of 1ADSL-B and 1ADSL-B/J cards is displayed as 1ADSL-B/J. In earlier versions, the type of the two cards is displayed as 1ADSL-B. You can check the PCB version to distinguish the two types of cards.
Status	Status of a physical entity: ● NORMAL: The temperature of a physical entity is within the allowed range. ● ABNORMAL: The temperature of a physical entity is out of the allowed range. **NOTE** The 9ES2 and 4ES2G-S cards do not support this parameter.
Upper	Upper limit of the temperature of a physical entity. **NOTE** The 9ES2 and 4ES2G-S cards do not support this parameter.
Lower	Lower limit of the temperature of a physical entity. **NOTE** The 9ES2 and 4ES2G-S cards do not support this parameter.
Temperature.(C)	Temperature of a physical entity. **NOTE** The 9ES2 and 4ES2G-S cards do not support this parameter.
PowerNo	Number of a power supply.
Present	Whether a power supply is working: ● YES: The power supply is working. ● NO: The power supply is not working.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Power mode: ● DC ● AC
State	Status of a power supply: ● NotSupply: No power output. ● Supply: The power output is available.
Current(A)	Current of the power supply. It is displayed as N/A.
Voltage(V)	Rated voltage.
Power(W)	Rated power.
FanId	ID of a fan.
FanNum	Number of fans.
Present	Whether a fan is working: ● YES: A fan is working. ● NO: A fan is not working.
Register	Whether a fan is registered: ● YES: The fan is registered. ● NO: The fan is not registered.
Speed	Speed of a fan. This field refers to the percentage of the current fan speed to the full speed of the fan, or the actual fan speed, in Revolution(s) Per Minute (RPM).
Mode	Working mode of a fan: ● AUTO ● MANUAL
BoardType	Type of a board.
Power-Used(W)	Power supply of a board.
Power-Requested(W)	Maximum power of a board.
CPU Usage	CPU usage of a board.
Upper Limit	CPU usage alarm threshold. To set the CPU usage alarm threshold, use the **set cpu-usage threshold** *threshold-value* [**slot** *slot-id*] command.
Total Memory(MB)	Total memory of a board.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Used Memory(MB)	Used memory of a board.
Used Percentage	Memory usage of a board.
Device	Storage medium.

4.1.9 display memory-alloc mid

Function

The **display memory-alloc mid** command displays the memory allocated of a specified module.

Format

display memory-alloc mid *mid*

Parameters

Parameter	Description	Value
mid	Specifies the ID of a module.	The value is an integer, specify a module ID according to the Mapping between modules and IDs.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the memory allocated of the ACL module.

```
<Huawei> display memory-alloc mid
0XC06C0000


==================================================

*******************************************************************************
PtNo    UsedMemory(B)   UsedBlockNum    AllocTimes    FreeTimes
PtName
-------------------------------------------------------------------------------
```

```
1       1007552       15            17            2            USRPT
*****************************************************************************
```

Table 4-9 Description of the display memory-alloc mid command output

Item	Description
PtNo	Specifies the memory block number.
UsedMemory(B)	Specifies the size of the memory allocated, in bytes.
UsedBlockNum	Number of times memory is allocated.
AllocTimes	Number of times memory is allocated to a module.
FreeTimes	Number of times the remaining memory can be allocated to a module.
PtName	Specifies the memory block name.

4.1.10 display memory-usage

Function

The **display memory-usage** command displays the memory usage of the device.

Format

display memory-usage [**slave** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
slave	Displays memory usage of the slave control board. **NOTE** Only AR3200 series support this parameter.	-
slot *slot-id*	Displays memory usage of a specified board. If this parameter is not specified, memory usage of the main control board is displayed. **NOTE** The AR100&AR120&AR150&AR160&AR200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R do not support the **slot** *slot-id* parameter.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Memory usage is an important index to evaluate device performance. A high memory usage will cause service faults. You can use the **display memory-usage** command to view memory usage to check whether devices are working properly.

Example

Display memory usage of the current main control board.

```
<Huawei> display memory-usage
 Memory utilization statistics at 2008-12-15 15:17:42 746 ms
 System Total Memory Is: 394152720 bytes
 Total Memory Used Is: 130975664 bytes
 Memory Using Percentage Is: 33%
```

Display memory usage of the board in slot 2.

```
<Huawei> display memory-usage slot 2
 Slot 2/0 Memory utilization Info:
 Memory utilization statistics at 2008-12-15 15:08:58 532 ms
 System Total Memory Is: 59656976 bytes
 Total Memory Used Is: 16651852 bytes
 Memory Using Percentage Is: 27%
```

Table 4-10 Description of the **display memory-usage** command output

Item	Description
Memory utilization statistics	Statistics of the memory usage.
System Total Memory	Total memory of the device network operating system.
Total Memory Used	Total used memory of the device network operating system.
Memory Using Percentage	Memory usage.

4.1.11 display memory-usage process

Function

The **display memory-usage process** command displays the memory usage of a specific process.

NOTE

Only V200R010C10 and later versions support this command.

Format

display memory-usage process { *process-id* | **all** }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a process whose memory usage statistics are to be queried.	The value is an integer ranging from 0 to 4294967295.
all	Displays memory usage statistics of all processes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Memory usage is an important device performance indicator. High memory usage may cause service faults. You can use this command to check the memory usage of processes and verify that the device is running stably.

Example

Display memory usage statistics of all processes.

```
<Huawei> display memory-usage process all
PID   ProcessName        VmRSS(kB)    VmSize(kB)
1     init               1948         1288
1597  syslogd            3052         472
1601  moni               1856         1228
1608  monitor            244864       4508
1609  redis-server       21684        3796
1614  cap32              502448       7204
1615  main_task          957480       294792
1616  cap32              502504       6292
1617  cap32              502504       5928
1618  cap32              502504       5072
1619  confd              9004         5896
```

Display detailed information about the memory usage of process 1.

```
<Huawei> display memory-usage process 1
Name:   init
State:  S (sleeping)
Tgid:   1
Ngid:   0
Pid:    1
```

```
PPid:   0
TracerPid:      0
Uid:    0       0       0       0
Gid:    0       0       0       0
FDSize: 32
Groups:
NStgid: 1
NSpid:  1
NSpgid: 1
NSsid:  1
VmPeak:     1952 kB
VmSize:     1948 kB
VmLck:         0 kB
VmPin:         0 kB
VmHWM:      1288 kB
VmRSS:      1288 kB
VmData:      172 kB
VmStk:       136 kB
VmExe:       240 kB
VmLib:      1340 kB
VmPTE:        16 kB
VmPMD:         8 kB
VmSwap:        0 kB
HugetlbPages:          0 kB
Threads:        1
SigQ:   0/12248
SigPnd: 0000000000000000
ShdPnd: 0000000000000000
SigBlk: 0000000000000000
SigIgn: 0000000000000000
SigCgt: 0000000000084a07
CapInh: 0000000000000000
CapPrm: 0000003ffffffffff
CapEff: 0000003ffffffffff
CapBnd: 0000003ffffffffff
Seccomp:        0
Cpus_allowed:   1
Cpus_allowed_list:      0
Mems_allowed:   1
Mems_allowed_list:      0
voluntary_ctxt_switches:        137
nonvoluntary_ctxt_switches:     1324
```

Table 4-11 Description of the **display memory-usage process** command output

Item	Description
PID	Process ID.
ProcessName	Process name.
VmRSS(kB)	Size of the physical memory occupied by the process.
VmSize(kB)	Size of the virtual memory occupied by the process.
Name	Process name.
State	Process status: ● S: sleep ● R: running
Tgid	Thread group ID.

Item	Description
Ngid	NUMA group ID.
Pid	Thread ID.
PPid	Process ID of the parent process.
TracerPid	ID of the process tracing this process.
Uid	ID of the user who starts the process.
Gid	ID of the group to which the user ID belongs.
FDSize	Number of file descriptors currently allocated.
Groups	Supplementary group list.
NStgid	Thread group ID in each of the process ID namespaces of which the current process ID is a member.
NSpid	Thread ID in each of the process ID namespaces of which the current process ID is a member.
NSpgid	Process group ID in each of the process ID namespaces of which the current process ID is a member.
NSsid	Session ID in each of the process ID namespaces of which the current process ID is a member.
VmPeak	Peak memory usage during the running of the process.
VmSize	Size of the memory that is being used by the process.
VmLck	Size of the physical memory that is locked by the process.
VmPin	Size of the pinned memory allocated to the process.
VmHWM	Peak size of the physical memory allocated to the process.
VmRSS	Size of the physical memory currently used by the process.
VmData	Data segment size of the process.
VmStk	Stack segment size of the process.
VmExe	Code size of the process.
VmLib	Size of the library used by the process.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VmPTE	Size of the page tables occupied by the process.
VmPMD	Size of the second-level page tables occupied by the process.
VmSwap	Swap space used by the process.
HugetlbPages	Size of hugetlb memory portions.
Threads	Number of threads in the thread group containing this thread.
SigQ	Number of pending signals.
SigPnd	Mask of pending signals that are directed to the thread.
ShdPnd	Mask of pending signals that are directed to the thread group.
SigBlk	Signals that are blocked by the process.
SigIgn	Signals that are ignored by the process.
SigCgt	Signals that are caught by the process.
CapInh	Inherited capabilities of the process.
CapPrm	Permitted capabilities of the process.
CapEff	Effective capabilities of the process.
CapBnd	Set of bounding capabilities.
Seccomp	Secure computing mode.
Cpus_allowed	Affinity mask of CPUs on which this process can run.
Cpus_allowed_list	List of CPUs on which this process can run.
Mems_allowed	Affinity mask of memories allowed to use this process.
Mems_allowed_list	List of memories allowed to use this process.
voluntary_ctxt_switches	Number of voluntary process switching times.
nonvoluntary_ctxt_switches	Number of involuntary process switching times.

4.1.12 display memory-usage process vrp

 Copyright © Huawei Technologies Co., Ltd.

Function

The **display memory-usage process vrp** command displays the memory usage of the VRP process.

Format

display memory-usage process vrp [**slave**]

Parameters

Parameter	Description	Value
slave	Displays memory usage of the VRP process on the slave control board. **NOTE** Only AR3200 series support this parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Memory usage is an important performance indicator of a device. A high memory usage will cause service faults. You can use this command to check the memory usage of the VRP process and verify that the device is running stably.

Example

Display the memory usage of the VRP process.

```
<Huawei> display memory-usage process vrp
 Memory utilization statistics at 2013-07-10 09:55:20 729
ms
 The current memory of vrp process:
 Totalram : 253755392 bytes
 Total Memory Used Is : 212461632 bytes
 Memory Using Percentage Is: 83%
```

Table 4-12 Description of the display memory-usage process vrp command output

Item	Description
Memory utilization statistics at	Time when the memory usage information of the VRP process is collected.
The current memory of vrp process	Current memory usage of the VRP process.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Totalram	Total memory size allocated to the VRP process.
Total Memory Used Is	Memory size used by the VRP process.
Memory Using Percentage Is	Memory usage percentage of the VRP process.

4.1.13 display memory-usage threshold

Function

The **display memory-usage threshold** command displays the memory usage threshold on the device.

Format

display memory-usage threshold [**all** | **slot** *slot-id* | **slave**]

Parameters

Parameter	Description	Value
all	Displays memory usage thresholds of the main control board and all interface boards.	-
slot *slot-id*	Displays memory usage of a specified board. **NOTE** The AR100&AR120&AR150&AR160&AR200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, display_reset-snapshot_level.xmlAR2204-51GE-P, AR2204-51GE, AR2204-51GE-R do not support the **slot** *slot-id* parameter.	The value is an integer and must be set according to the device configuration.
slave	Displays memory usage of the slave control board. **NOTE** Only AR3200 series support this parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the memory usage alarm threshold to learn about the conditions for triggering alarms.

The default settings are as follows in versions earlier than V200R010C10:

- If the memory capacity of a card is smaller than or equal to 128 MB, the memory usage threshold is 90%.
- If the memory capacity of a card is larger than 128 MB, the memory usage threshold is 95%.

The default settings are as follows in V200R010C10 and later versions:

- If the memory capacity of a card is smaller than or equal to 256 MB, the memory usage threshold is 90%.
- If the memory capacity of a card is larger than 256 MB, the memory usage threshold is 95%.
- If the memory capacity of an SRU is equal to or less than 256 MB, the memory usage threshold is 88%.
- If the memory capacity of an SRU is greater than 256 MB but smaller than or equal to 512 MB, the memory usage threshold is 90%.
- If the memory capacity of an SRU is larger than 512 MB, the memory usage threshold is 95%.

When the memory capacity is less than or equal to 256 MB:

- If the memory usage reaches the value that equals the threshold minus 5%, the system generates a level-1 memory usage alarm, indicating that the memory usage is high.
- If the memory usage reaches the threshold, the system generates a level-2 memory usage alarm and triggers a device restart.
- When the memory usage is less than the value that equals the threshold minus 5%, the system generates a clear alarm.

When the memory capacity is more than 256 MB:

- If the memory usage reaches the value that equals the threshold minus 3%, the system generates a level-1 memory usage alarm, indicating that the memory usage is high.
- If the memory usage reaches the threshold, the system generates a level-2 memory usage alarm and triggers a device restart.
- When the memory usage is less than the value that equals the threshold minus 3%, the system generates a clear alarm.

Example

Display the memory usage threshold on the main control board.

```
<Huawei> display memory-usage threshold
 Current memory threshold of the main board is 95%.
```

Display memory usage thresholds of the main control board and all interface boards.

```
<Huawei> display memory-usage threshold all
 Current memory threshold of the main board is 95%.
 Current memory threshold of the slot 1 is 95%.
```

Table 4-13 Description of the display memory-usage threshold command output

Item	Description
Current memory threshold of the main board is 95%.	The memory usage threshold of the main control board is 95%. To set the memory usage threshold of the main control board, use the **set memory-usage threshold** *threshold-value* command.
Current memory threshold of the slot 1 is 95%.	The memory usage threshold of the board in slot 1 is 95%. To set the memory usage threshold of an interface board, use the **set memory-usage threshold** *threshold-value* **slot** *slot-id* command.

Related Topics

4.2.15 set memory-usage threshold

4.1.14 display power

Function

The **display power** command displays the information of all power supply units on the device.

NOTE

This command is not supported by the AR100&AR120&AR150&AR160 (except AR161EW, AR161EW-M1 and AR169EW) &AR200 series.

Format

display power

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the status of all power supply units, and their voltage, current and power.

Example

Display the power module status of the device.

```
<Huawei> display power
-----------------------------------------------------------------------------
 PowerNo  Present  Mode   State      Current(A)   Voltage(V)   Power(W)
-----------------------------------------------------------------------------
   9      NO       N/A    N/A        N/A          N/A          N/A
   10     YES      AC     Supply     N/A          12           350
```

Table 4-14 Description of the display power command output

Item	Description
PowerNo	Number of a power supply.
Present	Whether a power supply is working: ● YES: The power supply is working. ● NO: The power supply is not working.
Mode	Power mode: ● DC ● AC **NOTE** The current, voltage, and real-time power of DC power supply cannot be displayed.
State	Power supply status: ● NotSupply: No power is supplied. ● Supply: Power is supplied.
Current(A)	Current of the power supply, in Ampere. It is displayed as N/A.
Voltage(V)	Rated voltage, in V.
Power(W)	Rated power, in wattage.

4.1.15 display power system

Function

The **display power system** command displays power information on a device, including the system power and card power.

NOTE

This command is not supported by the AR100&AR120&AR150&AR160 (except AR161EW, AR161EW-M1 and AR169EW) &AR200 series.

Format

display power system

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the power of the device.

```
<Huawei> display power system
 The backup-mode  is : 1:0
 The total  power is : 350.000(W)
 The remain power is : 235.000(W)
 The system used power detail information :
-------------------------------------------------------------------------------
  SlotID  BoardType    Power-Used(W)  Power-Requested(W)
-------------------------------------------------------------------------------
  1       8FE1GE       9.476          13
  5       8FE1GE       9.476          13
  11       SRU40        42.000         61
  16       FAN          14.000         28
```

Table 4-15 Description of the display power system command output

Item	Description
The backup-mode is	Power module status: ● 1:0: A single power module is configured on the device. ● 1:1: Two power modules are configured on the device. **NOTE** This field is displayed only on the AR2204E-D, AR2204E, AR2204-27GE-P, AR2204E-D-27GE, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, and AR2204-51GE-R.
The total power is	Total power of the device.

Item	Description
The remain power is	Available power.
The system used power detail information	Details about system power.
SlotID	Slot ID of a component.
BoardType	Type of a component.
Power-Used(W)	Power consumed by a component.
Power-Requested(W)	Fixed power that the system provides to a component. **NOTE** Each fan module is provided fixed power of 28 W. When the power required by a fan module exceeds 28 W, the rest of power is allocated from the reserved power. If the power required by a fan module exceeds the fixed power but the reserved power is larger than the rest of required power, the fan module can still run normally.

4.1.16 display sn

Function

The **display sn** command displays the serial numbers (SNs) of components on a device.

Format

display sn [[**interface**] **abnormal** | **all** | **interface** *interface-type interface-number* | **license** | **slot** *slot-id*]

Parameters

Parameter	Description	Value
interface	Displays all abnormal interfaces. **NOTE** This command cannot display information about abnormal interfaces on an LPU.	-
abnormal	Displays all abnormal components.	-
all	Displays the SNs of all components.	-

Parameter	Description	Value
interface *interface-type interface-number*	Displays the SN of a specified interface: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
license	Displays the SN of a license.	-
slot *slot-id*	Displays the SN of the component in a specified slot.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the SNs of components on a device.

```
<Huawei> display sn
Equipment SN(ESN): AR00050123456789
License ESN: AR00050123456789
Slot  Sub Type          SN                  P/N
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1     -   2FE           020XTQ10C3000017        03020XTQ
2     -   1SA           020YNB10B5000151        03020YNB
3     -   1CPOS-155M       021AQU10C1000041         03021AQU
4     -   1ADSL-A/M       020XTT10B5000153        03020XTT
5     -   8FE1GE          020XTN10BA000044        03020XTN
8     -   1STM4           021XHD10E1000001        03021XHD
11    -   SRU40           AR00050123456789        02129615
9     -   PWR350A         2102310CWN10B6000195    02310CWN
12    -   FAN             21021206134JB9000205    02120613
```

Display the SN of the abnormal components.

```
<Huawei> display sn abnormal
Slot  Sub Type          SN                  P/N       State
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1     -   2FE           020XTQ10C3000017        03020XTQ   TimeOutReg
```

Table 4-16 Description of the **display sn** command output

Item	Description
Equipment SN(ESN)	Equipment serial number (ESN) of a device.
License ESN	ESN of a license.
Slot	Slot ID of a component.
Sub	Subcard ID.
Type	Type of a component.
SN	SN of a component.
P/N	Part number of a component.
State	State of a component.

4.1.17 display temperature

Function

The **display temperature** command displays the device temperature.

Format

display temperature { **all** | **slot** *slot-id* }

display temperature slot fan

Parameters

Parameter	Description	Value
all	Displays the temperature of all boards.	-
slot *slot-id*	Displays the temperature of the specified board.	The value is an integer and must be set according to the device configuration.
fan	Displays the temperature of the fan module. **NOTE** Before running this command, ensure that the fan module has been installed. Only AR2240, AR3670, and AR3260 support the **fan** parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A high or low device temperature may damage the hardware. This command displays the current device temperature. When the device temperature exceeds the upper threshold or falls below the lower threshold, the device generates an alarm to alert you that the device temperature is abnormal.

Example

Display the temperature of all boards.

```
<Huawei> display temperature all
-------------------------------------------------------------------------------
 Slot   Card   Sensor No.   SensorName          Status  Upper  Lower  Temp(C)
-------------------------------------------------------------------------------
 1      -      1            8FE1GE TEMP         NORMAL  85     0      45

 5      -      1            8FE1GE TEMP         NORMAL  85     0      45

 11     -      1            SRU40 TEMP          NORMAL  55     0      50
```

Display the temperature of the board in slot 1 of the device.

```
<Huawei> display temperature slot 1
-------------------------------------------------------------------------------
 Slot   Card   Sensor No.   SensorName          Status  Upper  Lower  Temp(C)
-------------------------------------------------------------------------------
 1      -      1            8FE1GE TEMP         NORMAL  85     0      45
```

Display the temperature of the fan module.

```
<Huawei> display temperature slot fan
-----------------------------------------------------------------------------
 Slot  Card  Sensor No.  SensorName         Status    Upper  Lower  Temp(C)
-----------------------------------------------------------------------------
 12    -     1           Hot Point          NORMAL    65     0      39
```

Table 4-17 Description of the display temperature command output

Item	Description
Slot	Slot ID of the board.
Card	Subcard number.
Sensor No.	Number of the sensor on the board.
SensorName	Name of the sensor on the board.

Item	Description
Status	Board temperature: ● NORMAL: The board temperature is within the allowed range. ● ABNORMAL: The board temperature is out of the allowed range.
Upper	Upper threshold of the temperature. **NOTE** When the temperature reaches the upper threshold, no alarm is generated immediately. The fan speed is adjusted first. If the temperature keeps increasing, an alarm is generated.
Lower	Lower threshold of the temperature. **NOTE** When the temperature reaches the lower threshold, no alarm is generated immediately. The fan speed is adjusted first. If the temperature keeps reducing, an alarm is generated.
Temperature.(C)	Current temperature of the board, in the centigrade scale (C).

4.1.18 display transceiver

Function

The **display transceiver** command displays information about the optical module on an interface.

NOTE

The command displays only information on optical interfaces.

Format

display transceiver [**interface** *interface-type interface-number* | **controller** *controller-type controller-number* | **slot** *slot-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	The interface type can be: ● Ethernet ● GigabitEthernet ● POS
controller *controller-type controller-number*	Specifies the type and number of a CPOS interface.	-
slot *slot-id*	Specifies a slot ID.	The value is an integer, and the value range depends on the device configuration.
verbose	Displays detailed information about the optical module on an interface, including the general information, manufacture information, alarm information, and diagnostic information.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to view general information, manufacture information, and alarm information about an optical module. If you specify the **verbose** keyword, diagnostic information is also displayed in addition to the preceding information.

Example

Display general information, manufacture information, and alarm information about the optical module on a specified interface.

```
<Huawei> display transceiver interface gigabitethernet 1/0/0

GigabitEthernet1/0/0 information:
-----------------------------------------------------------
Electronic label information:
  Description              :2100Mb/sec-850nm-LC-MM-500m(0.05mm)300m(0.0625mm)
  Type                     :PLRXPL-VI-S24-HW
  VendorSN                 :CA21QQ2Z8
  Manufacturing Date       :2010-05-25
  Manufacturer             :JDSU
-----------------------------------------------------------
Alarm information:
  RX power low
-----------------------------------------------------------
```

Display general information, manufacture information, alarm information and diagnostic information about the optical module on a specified interface.

```
<Huawei> display transceiver interface gigabitethernet 1/0/0 verbose

GigabitEthernet1/0/0 information:
-----------------------------------------------------------
Electronic label information:
  Description              :2100Mb/sec-850nm-LC-MM-500m(0.05mm)300m(0.0625mm)
  Type                     :PLRXPL-VI-S24-HW
  VendorSN                 :CA21QQ2Z8
  Manufacturing Date       :2010-05-25
  Manufacturer             :JDSU
-----------------------------------------------------------
Alarm information:
  RX power low
-----------------------------------------------------------
Realtime information:
  Temperature(°C)                    :35
  Voltage(V)                         :3.30
  Bias Current(mA)                   :4.08
  Bias High Threshold(mA)            :18.57
  Bias Low  Threshold(mA)            :1.07
  Current Rx Power(dBM)              :-31.54
  Default Rx Power High Threshold(dBM)     :0.00
  Default Rx Power Low  Threshold(dBM)     :-16.98
  Current Tx Power(dBM)              :-5.01
  Default Tx Power High Threshold(dBM)     :0.00
  Default Tx Power Low  Threshold(dBM)     :-9.50
  User Set Rx Power High Threshold(dBM)    :0.00
  User Set Rx Power Low Threshold(dBM)     :-16.98
  User Set Tx Power High Threshold(dBM)    :0.00
  User Set Tx Power Low Threshold(dBM)     :-9.50
  Default Temperature high  Threshold(°C)  :85
  Default Temperature low   Threshold(°C)  :-40
-----------------------------------------------------------
```

Table 4-18 Description of the **display transceiver** command output

Item	Description
Electronic label information	Electronic label of an optical module.
Description	Description of the optical module.
Type	Type of the optical module.
VendorSN	Serial number of the optical module.

Item	Description
Manufacturing Date	Manufacturing date of the optical module.
Manufacturer	Manufacturer of the optical module.
Alarm information	Alarm information about the optical module.
RX power low	Low receive power.
Realtime information	Real-time information about the optical module.
Temperature(°C)	Temperature of the optical module.
Voltage(V)	Voltage of the optical module.
Bias Current (mA)	Current bias of the optical module.
Bias High Threshold(mA)	Upper bias threshold for the optical module.
Bias Low Threshold(mA)	Lower bias threshold for the optical module.
Current RX Power(dBM)	Current receive power of the optical module.
Default RX Power High Threshold (dBM)	Default upper threshold for the receive power of the optical module.
Default RX Power Low Threshold (dBM)	Default lower threshold for the receive power of the optical module.
Current TX Power(dBM)	Current transmit power of the optical module.
Default TX Power High Threshold(dBM)	Default upper threshold for the transmit power of the optical module.
Default TX Power Low Threshold(dBM)	Default lower threshold for the transmit power of the optical module.
User Set Rx Power High Threshold(dBM)	Configured upper threshold for the receive power of the optical module.
User Set Rx Power Low Threshold(dBM)	Configured lower threshold for the receive power of the optical module.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
User Set Tx Power High Threshold(dBM)	Configured upper threshold for the transmit power of the optical module.
User Set Tx Power Low Threshold(dBM)	Configured lower threshold for the transmit power of the optical module.
Default Temperature high Threshold (°C)	Default upper threshold for temperature of the optical module.
Default Temperature low Threshold (°C)	Default lower threshold for temperature of the optical module.

4.1.19 display version

Function

The **display version** command displays the version of the device.

Format

display version [**slot** *slot-id*]

display version slot fan

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the version of the specified board.	The value is an integer and must be set according to the device configuration.
fan	Displays the version of the fan module. **NOTE** Before running this command, ensure that the fan module has been installed. Only AR2240, AR3670, and AR3260 support the **fan** parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display version** command to view the version of the device to determine whether the device needs to be upgraded.

Example

Display the version of the device.

```
<Huawei> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.120 (AR2200 V200R003C00)
Copyright (C) 2011-2012 HUAWEI TECH CO., LTD
Huawei AR2240 Router uptime is 0 week, 1 day, 5 hours, 10 minutes
BKP 0 version information:
1. PCB      Version  : AR01BAK2B VER.A
2. If Supporting PoE : No
3. Board    Type     : AR2240
4. MPU Slot Quantity : 1
5. LPU Slot Quantity : 8

MPU 11(Master) : uptime is 0 week, 1 day, 5 hours, 10 minutes
SDRAM Memory Size    : 2048    M bytes
Flash Memory Size    : 16      M bytes
NVRAM Memory Size    : 512     K bytes
SD Card1 Memory Size : 1882    M bytes
MPU version information :
1. PCB      Version  : AR01SRU3A VER.B
2. MAB      Version  : 0
3. Board    Type     : SRU40
4. CPLD0    Version  : 104
5. CPLD1    Version  : 104
6. BootROM  Version  : 604

LPU 1 : uptime is 0 week, 1 day, 5 hours, 7 minutes
SDRAM Memory Size    : 96      K bytes
Flash Memory Size    : 384     K bytes
LPU version information :
1. PCB      Version  : AR01SEG1CA VER.B
2. MAB      Version  : 0
3. Board    Type     : 2FE
4. BootROM  Version  : cb

LPU 5 : uptime is 0 week, 1 day, 5 hours, 6 minutes
SDRAM Memory Size    : 256     M bytes
Flash Memory Size    : 16      M bytes
LPU version information :
1. PCB      Version  : AR01WMF9TTA VER.B
2. MAB      Version  : 0
3. Board    Type     : 8FE1GE
4. BootROM  Version  : 213
5. BootLoad Version  : 510

FAN version information :
1. PCB      Version  : AR01DF05A VER.A
2. Board    Type     : FAN
3. Software Version  : 103
```

Display the version of the board in slot 1.

```
<Huawei> display version slot 1
LPU 1 : uptime is 0 week, 1 day, 5 hours, 15 minutes
SDRAM Memory Size    : 256      M bytes
Flash Memory Size    : 16       M bytes
LPU version information :
1. PCB       Version  : AR01WMF9TTA VER.B
2. MAB       Version  : 0
3. Board     Type     : 8FE1GE
4. BootROM   Version  : 213
5. BootLoad Version  : 510
```

Display the version of the fan module.

```
<Huawei> display version slot fan
FAN version information :
1. PCB       Version  : AR01DF05A VER.A
2. Board     Type     : FAN
3. Software Version  : 103
```

Table 4-19 Description of the display version command output

Item	Description
Huawei Versatile Routing Platform Software	-
VRP (R) software, Version	Versions of the VRP and the software of the device.
Copyright (C) 2011-2012 HUAWEI TECH CO., LTD	Copyright information.
uptime	System power-on time.
BKP 0 version information	Backplane version.
PCB Version	-
If Supporting PoE	Whether PoE is supported.
Board Type	- **NOTE** In V200R005, the type of 1ADSL-B and 1ADSL-B/J cards is displayed as 1ADSL-B/J. In earlier versions, the type of the two cards is displayed as 1ADSL-B. You can check the PCB version to distinguish the two types of cards.
MPU Slot Quantity	Number of MPU slots.
LPU Slot Quantity	Number of LPU slots.
MPU X (Master)	Master MPU slot ID.

Item	Description
SDRAM Memory Size	The **System Total Memory** field displayed in the **display memory-usage** command output is the memory assigned from the SDRAM memory. The value varies depending on the device model.
Flash Memory Size	-
NVRAM Memory Size	-
SD Card1 Memory Size	sd1 memory space.
USB Disk0 Memory Size	usb0 memory space.
MPU version information	MPU version.
LPU X	LPU in slot X.
LPU version information	LPU version.
FAN version information	Version of the fan module.

4.1.20 display dyinggasp capacity

Function

The **display dyinggasp capacity** command displays whether the battery capacity of the Dyinggasp capacitor card is full.

NOTE

Only the AR models that have the DGP cards installed support this command.

Format

display dyinggasp capacity [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the type and status of the card in a specified slot. If this parameter is not specified, this command displays the type and status of all components on the device.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dyinggasp capacity** command to check whether the battery capacity of the Dyinggasp capacitor card is full.

Example

Display whether the battery capacity of the Dyinggasp capacitor card is full.

```
<Huawei> display dyinggasp capacity
DyingGasp board capacity information:
Slot        Type          Capacity
-------------------------------------
1          AR-DGP-S       Full
-------------------------------------
```

Table 4-20 Description of the **display dyinggasp capacity** command output

Item	Description
Slot	Slot ID of a card.
Type	Type of a card.
Capacity	Capacitor capacity of a card: ● Full: The capacity is full. ● Charging: The capacitor card is charging. ● Fail: Failed to obtain the charging status.

4.2 Hardware Configuration Commands

4.2.1 backup elabel

Function

The **backup elabel** command backs up electronic labels of the device to the storage media.

The **backup elabel ftp** command backs up electronic labels of the device to a specified FTP server.

The **backup elabel tftp** command backs up electronic labels of the device to a specified TFTP server.

The **backup elabel backplane** command backs up electronic labels of the backplane to the storage media.

The **backup elabel backplane ftp** command backs up electronic labels of the backplane to a specified FTP server.

The **backup elabel backplane tftp** command backs up electronic labels of the backplane to a specified TFTP server.

NOTE

Only AR2240 and AR3200 series can back up electronic labels of the backplane.

Format

backup elabel *filename* [*slot-id*]

backup elabel ftp *ftp-server-address filename username password* [*slot-id*]

backup elabel tftp *tftp-server-address filename* [*slot-id*]

backup elabel backplane *filename*

backup elabel backplane ftp *ftp-server-address filename username password*

backup elabel backplane tftp *tftp-server-address filename*

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID of the board of which the electronic label needs to be saved. If this parameter is not specified, all electronic labels of the device are saved.	The value must be set according to the device configuration.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
filename	Specifies the name of the file that stores electronic labels.	The value is a string of 1 to 28 case-sensitive characters without spaces. The default directory where files are stored is as follows: ● AR100&AR120&AR150&AR160&AR200series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204E, AR2204E-D, AR2204-51GE-R, AR2240C, AR2204, AR2220L, AR2204-51GE, AR2220E: flash:/ ● AR2220, AR2240, AR3200 series, AR3600 series: sd1:/
ftp-server-address	Specifies the IP address of the FTP server that stores electronic labels.	The value is in dotted decimal notation.
username	Specifies the user name used to log in to the FTP server.	The value is a string of 1 to 20 case-sensitive characters without spaces.
password	Specifies the password used to log in to the FTP server.	The value is a string of 1 to 20 case-sensitive characters without spaces.
tftp-server-address	Specifies the IP address of the TFTP server that stores electronic labels.	The value is in dotted decimal notation.

Views

All views

Default Level

3: Management level

Usage Guidelines

When electronic labels are stored on a device, use the **backup elabel** command to save electronic labels to a file. This file can be saved to the storage media of the device, to the FTP server using FTP, or to the TFTP server using TFTP. FTP cannot ensure secure file transfer. SFTP is recommended on networks that require high security.

Precautions

If the name of the file is the same as that of an existing file in storage media of the device, the system prompts you whether to overwrite the existing file.

Example

Save electronic labels of the device to the **elabel.fls** file in the flash memory.

```
<Huawei> backup elabel flash:/elabel.fls
```

Save electronic labels of the device to FTP server 192.168.12.91. Set the FTP user name to **user** and password to **123**. Save electronic labels in the **elabel.fls** file.

```
<Huawei> backup elabel ftp 192.168.12.91 elabel.fls user 123
```

Save electronic labels of the device to the **elabel.fls** file on TFTP server 192.168.12.91.

```
<Huawei> backup elabel tftp 192.168.12.91 elabel.fls
```

Save electronic labels of the backplane to the **elabel.fls** file in the flash memory.

```
<Huawei> backup elabel backplane flash:/elabel.fls
```

Related Topics

4.1.5 display elabel

4.2.2 clear root-key

Function

The **clear root-key** command clears the configured root key.

Format

clear root-key

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

To improve service security and prevent encrypted packets from being decrypted, configure a root key again. To clear the configured root key, run the **clear root-key** command. After the device restarts, the device uses the system default root key.

Example

Clear the configured root key.

```
<Huawei> clear root-key
Warning: Clearing a root key takes effect only after the device is restarted. Are you sure you want to clear
it? [Y/N]:y
Info: Successed in setting next root-key on the master board.
```

Related Topics

4.2.18 set root-key

4.2.3 display root-key configuration

4.2.3 display root-key configuration

Function

The **display root-key configuration** command displays information about the currently used root key.

Format

display root-key configuration

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use the **display root-key configuration** command to check information about the currently used root key.

Example

Display information about the currently used root key.

```
<Huawei> display root-key configuration
Master:
```

```
Current root-key:  User-configured
Next root-key:     System default
```

Table 4-21 Description of the **display root-key configuration** command output

Item	Specification
Master	Information about the root key of the MPU.
Current root-key	Information about the currently used root key: ● User-configured: user-configured root key ● System default: system default root key
Next root-key	Information about the root key used after the device restarts: ● User-configured: user-configured root key ● System default: system default root key

Related Topics

4.2.18 set root-key

4.2.2 clear root-key

4.2.4 display rps elabel

Function

The **display rps elabel** command displays information about the electronic label of the redundant power system (RPS).

NOTE

Only the AR2201-48FE, AR2202-48FE, AR2204, AR2220E support this function.

Format

display rps elabel

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rps elabel** command to view information about the RPS electronic label.

Prerequisites

The device is connected to an external RPS and the RPS is working properly.

Example

Display information about the RPS electronic label.

```
<Huawei> display rps elabel
[Rps_Elabel]
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
BoardType=RPS1800
BarCode=21023538x710C3000028
Item=02353857
Description=RPS1800 Redundant Power System(6 DC Output Ports,12V Total Output Po
wer 140W,48V Total Output Power 1600W)
Manufactured=2012-03-29
VendorName=Huawei
IssueNumber=00
CLEICode=
BOM=
```

Table 4-22 Description of the display rps elabel command output

Item	Description
BoardType	Board type of the RPS.
BarCode	Board code of the RPS.
Item	BOM code of the RPS.
Description	Description about the RPS.
Manufactured	Production date of the RPS.
VendorName	Provider of the RPS.
IssueNumber	Issue number of the RPS.
CLEICode	Common language equipment identification (CLEI) of the RPS.
BOM	Sales BOM code of the RPS.

 Copyright © Huawei Technologies Co., Ltd.

4.2.5 display rps status

Function

The **display rps status** command displays the RPS status.

NOTE

Only the AR2201-48FE, AR2202-48FE, AR2204, AR2220E support this function.

Format

display rps status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rps status** command to view the RPS status.

Prerequisites

The device is connected to an external RPS and the RPS is working properly.

Example

Display the RPS status.

```
<Huawei> display rps status
-----------------------------------------------------------------
 RPS Module       Present        Status          WorkStatus
-----------------------------------------------------------------
 12V              YES            Normal          NotSupply
```

Table 4-23 Description of the display rps status command output

Item	Description
RPS Module	Name of the RPS module.

Item	Description
Present	Whether the RPS module is installed properly: ● YES ● NO
Status	Status of the RPS. ● Normal ● Abnormal
WorkStatus	Working status of the RPS: ● Supply: The RPS is supplying power. ● NotSupply: The RPS is in idle state. ● Upgrade: The RPS is being upgraded.

Related Topics

4.2.19 set rps force

4.2.6 display rps temperature

Function

The **display rps temperature** command displays the RPS temperature.

NOTE

Only the AR2201-48FE, AR2202-48FE, AR2204, AR2220E support this function.

Format

display rps temperature

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rps temperature** command to view the RPS temperature.

Prerequisites

The device is connected to an external RPS and the RPS is working properly.

Example

Display the RPS temperature.

```
<Huawei> display rps temperature
-------------------------------------------------------------------------------
  DeviceName          Status              Temperature(C)
-------------------------------------------------------------------------------
  RPS                 Normal              28
```

Table 4-24 Description of the display rps temperature command output

Item	Description
DeviceName	Name of the RPS.
Status	Status of the RPS. ● Normal ● Abnormal
Temperature(C)	Temperature of the RPS.

4.2.7 display rps version

Function

The **display rps version** command displays the RPS version information.

NOTE

Only the AR2201-48FE, AR2202-48FE, AR2204, AR2220E support this function.

Format

display rps version

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display rps version** command to view the hardware and software versions of the RPS.

Prerequisites

The device is connected to an external RPS and the RPS is working properly.

Example

Display the RPS version information.

```
<Huawei> display rps version
RPS Version Information :
1. Board     Type     : 7
2. PCB       Version  : LS521RPSA VER.C
3. SoftWare Version  : 212
4. BootROM  Version  : 112
```

Table 4-25 Description of the display rps version command output

Item	Description
Board Type	Board type of the RPS.
PCB Version	Version of the printed circuit board (PCB).
SoftWare Version	Software version.
BootROM Version	BootROM version.

4.2.8 display slave default

Function

The **display slave default** command displays the default slot ID of the slave MPU used after the next startup.

NOTE

Only AR3200 series supports this function.

Format

display slave default

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display slave default** command to view the slot ID of the default slave MPU used after the next startup.

Example

Display the slot ID of the default slave MPU used after the next startup.

```
<Huawei> display slave default
Info: Default slave slot is 14.
```

Related Topics

4.2.23 slave default

4.2.9 display switchover state

Function

The **display switchover state** command displays the current MPU status.

NOTE

Only AR3200 series supports this function.

Format

display switchover state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before performing a master/slave MPU switchover, use the **display switchover state** command to view the MPU status to determine whether to perform the MPU switchover. You can perform a master/slave switchover only when the MPU is in the real-time backup state.

Example

Display information about master and slave switchover, which helps check whether the stack meets switchover requirements.

```
<Huawei> display switchover state
Slot 15 HA FSM State(master): realtime or routine backup.
Slot 14 HA FSM State(slave): receiving realtime or routine data.
```

Table 4-26 Description of the display switchover state command output

Item	Description
HA FSM State(master)	Status of the master MPU: • waiting for the slave to be inserted: Only one MPU is installed and you need to install the slave MPU. • batch backup: The master MPU is backing up data to the slave MPU in batches. • realtime or routine backup: The master MPU is in real-time backup state.
HA FSM State(slave)	Status of the slave MPU: • receiving batch data: The slave MPU is receiving backup data from the master MPU in batches. • receiving realtime or routine data: The slave MPU is in the real-time state for receiving data.

Related Topics

4.2.25 slave switchover

4.2.26 switchover enable

4.2.10 display super-fast hardware state

Function

The **display super-fast hardware state** command displays the hardware acceleration function status.

NOTE

Only the AR161, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169RW-P-M9, and AR169W-P-M9 support this command.

Format

display super-fast hardware state

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to view the hardware acceleration function status of the device.

Example

Display the hardware acceleration function status.

```
<Huawei> display super-fast hardware state
Super-fast Hardware State : Enable
```

Table 4-27 Description of the **display super-fast hardware state** command output

Item	Description
Super-fast Hardware State	Hardware acceleration function status: • Enable • Disable

Related Topics

4.2.30 super-fast hardware enable

4.2.11 osp-module memory-size

Function

Run the **osp-module memory-size** command to configure the available memory space for VMs on the OSP daughter card.

By default, the available memory space for VMs on the OSP daughter card is 3 GB.

NOTE

Only the AR169RW-P-M9, AR169W-P-M9, and AR169-P-M9 support this command.

Format

osp-module memory-size *size-value*

Parameters

Parameter	Description	Value
size-value	Specifies the available memory space for VMs on the OSP daughter card.	The value is of the enumerated type: ● 3: indicates that 3 GB memory is available to VMs on the OSP daughter card. ● 6: indicates that 6 GB memory is available to VMs on the OSP daughter card. The default value is 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Certain memory space of an OSP daughter card is reserved for VMs. By default, VMs reserve certain memory space for audio and video functions. As a result, only 3 GB memory space is available to VMs. However, in some scenarios, audio and video functions are not required, causing a waste of memory space. If you want to increase the memory space of VMs, run the **osp-module memory-size** command to set the available memory space of VMs to 6 GB. The configured memory space takes effect after the OSP daughter card is restarted.

Example

Set the available memory space for VMs on the OSP daughter card to 6 GB.

```
<Huawei> system-view
[Huawei] osp-module memory-size 6
Info: This operation may affect voice functions on the OSP
card...
Info: Successfully allocated 6 GB memory to the OSP card, rebooting the OSP card to make it affects.
```

4.2.12 power

Function

The **power on** command powers on a specified board.

The **power off** command powers off a specified board.

NOTE

The AR100&AR120&AR150&160&200 series, and AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R do not support this command.

Format

power on slot *slot-id*

power off slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a board.	The value is an integer and must be set according to the device configuration.

Views

User view

Default Level

3: Management level

Usage Guidelines

When services are idle on the board, run the **power off** command to power off the board without affecting services. This ensures stable system operation and saves energy.

NOTE

Boards are hot swappable. Therefore, you do not need to power on or off boards before hot swapping them.

Example

Power off the board in slot 3.

```
<Huawei> power off slot 1
```

Power on the board in slot 1.

```
<Huawei> power on slot 1
```

Related Topics

4.1.3 display device

4.2.13 reset slot

Function

The **reset slot** command resets a specified card.

NOTE

The AR150&160&200 series, AR510 series, AR2201-48FE and AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204E, AR2240C, do not support this command.

Format

reset slot *slot-id*

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID of the card that needs to be reset.	The value is an integer and must be set according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can reset a specified card on the device. Resetting a card will interrupt services on the card.

Example

Reset the card in slot 1.

```
<Huawei> reset slot 1
Are you sure you want to reset board in slot 1 ? [y/n]:y
INFO: Resetting board[1] succeeded.
```

4.2.14 set cpu-usage threshold

Function

The **set cpu-usage threshold** command sets the CPU usage alarm threshold and CPU usage alarm recovery threshold.

The **undo set cpu-usage threshold** command restores the default CPU usage alarm threshold and CPU usage alarm recovery threshold.

By default, the CPU usage alarm threshold is 80% and the CPU usage alarm recovery threshold is 75%.

- When the CPU usage alarm threshold is lower than 60%, the default CPU usage alarm recovery threshold is 1% lower than the CPU usage alarm threshold.
- When the CPU usage alarm threshold is higher than or equal to 60%, the default CPU usage alarm recovery threshold is 5% lower than the CPU usage alarm threshold.

Format

set cpu-usage threshold *threshold-value* [**restore** *restore-threshold-value*]

undo set cpu-usage threshold

Parameters

Parameter	Description	Value
threshold *threshold-value*	Specifies the CPU usage alarm threshold.	The value is an integer that ranges from 2 to 100. The default value is 80.
restore *restore-threshold-value*	Specifies the CPU usage alarm recovery threshold.	The value is an integer that ranges from 1 to *threshold-value*-1. The default value is 75.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **set cpu-usage threshold** command to set the CPU usage alarm threshold and CPU usage alarm recovery threshold. Only when MPU's CPU usage exceeds the alarm threshold, the system logs the event and generates an alarm. By viewing log information, you can learn about CPU usage. When CPU usage falls within the recovery threshold, the system generates a clear alarm.

If the **slot** *slot-id* parameter is not specified, the CPU usage threshold of the MPU is set. If you specify the slot slot-id parameter, the alarm can be triggered only when an MPU is installed in the specified slot.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Default CPU usage alarm threshold and CPU usage alarm recovery threshold are recommended. If the CPU usage alarm threshold and CPU usage alarm recovery threshold are set too small, the system frequently generates alarms. If the CPU usage alarm threshold and CPU usage alarm recovery threshold are set too large, you cannot learn about CPU usage in a timely manner.

Example

Set the CPU usage alarm threshold of the MPU to 85%.

```
<Huawei> system-view
[Huawei] set cpu-usage threshold 85
```

Related Topics

4.1.2 display cpu-usage configuration

4.2.15 set memory-usage threshold

Function

The **set memory-usage threshold** command sets the memory usage threshold.

The **undo set memory-usage threshold** command restores the default memory usage threshold.

The default settings are as follows in versions earlier than V200R010C10:

- If the memory capacity of a card is smaller than or equal to 128 MB, the memory usage threshold is 90%.
- If the memory capacity of a card is larger than 128 MB, the memory usage threshold is 95%.

The default settings are as follows in V200R010C10 and later versions:

- If the memory capacity of a card is smaller than or equal to 256 MB, the memory usage threshold is 90%.
- If the memory capacity of a card is larger than 256 MB, the memory usage threshold is 95%.
- If the memory capacity of an SRU is equal to or less than 256 MB, the memory usage threshold is 88%.
- If the memory capacity of an SRU is greater than 256 MB but smaller than or equal to 512 MB, the memory usage threshold is 90%.
- If the memory capacity of an SRU is larger than 512 MB, the memory usage threshold is 95%.

Format

set memory-usage threshold *threshold-value* [**slot** *slot-id*]

undo set memory-usage threshold [**slot** *slot-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
threshold *threshold-value*	Specifies the memory usage threshold.	The value is an integer that ranges from 75 to 100.
slot *slot-id*	Specifies the slot ID of a board. **NOTE** The AR100&AR120&AR150&160&200 series, and AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204E, AR2204-51GE, AR2204-51GE-R do not support the **slot** *slot-id* parameter.	The value must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **set memory-usage threshold** command to set the memory usage threshold. When memory usage exceeds the threshold, the system logs the event and generates an alarm. By viewing log information, you can learn about memory usage.

If the **slot** *slot-id* parameter is not specified, the memory usage threshold of the MPU is set. If you specify the slot slot-id parameter, the alarm can be triggered only when an MPU is installed in the specified slot.

Precautions

You are advised to use the default threshold. If the memory usage threshold is set too low, the system generates alarms and restarts when memory usage exceeds the threshold. If the memory usage threshold is set too high, you cannot learn about memory usage in a timely manner.

Example

Set the memory usage threshold of the MPU to 85%.

```
<Huawei> system-view
[Huawei] set memory-usage threshold 85
```

Related Topics

4.1.13 display memory-usage threshold

4.2.16 set operator-code

Function

The **set operator-code** command configures a device to run in a user-defined state.

The **undo set operator-code** command cancels a device to run in a user-defined state.

By default, a device does not run in a user-defined state.

Format

set operator-code *user*

undo set operator-code *user*

Parameters

Parameter	Description	Value
user	Specifies a user type.	The value can only be CMCC, case-insensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command enables a device to run in a user-defined state, meeting special requirements of the user.

Currently, the system supports only one user-defined state: CMCC (China Mobile). In the CMCC state, the indexes of a device's entity MIBs and extended entity MIBs are fixed at 1. This ensures that main control units of different devices have the same index.

Example

Configure a device to run in the CMCC state.

```
<Huawei> system-view
[Huawei] set operator-code CMCC
```

4.2.17 set output-mode osp

Function

The **set output-mode osp** command redirects the serial port to the OSP daughter card.

NOTE

This command takes effect only on the AR161FW-P-M5, AR161G_L, AR161G_Lc, AR161G_U, AR169RW_P_M9, AR169W_P_M9, and AR169-P-M9 running a non-Android version.

Format

set output-mode osp

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After the OSP daughter card registers with the device, you can run this command to redirect the serial port to the OSP daughter card for secondary development of the OSP daughter card.

If the serial port is redirected to the OSP daughter card for the first time, the user name **huawei** must be entered but the password is not required. Only the user with user name **huawei** can redirect to the OSP daughter card through the serial port. The user name cannot be added, deleted, or modified.

Press **Ctrl+D** to exit from the serial port redirection page.

Example

Redirect the serial port to the OSP daughter card.

```
<Huawei> system-view
[Huawei] set output-mode osp
Warning: Now you enter a serial port redirection view for developer's testing, some commands may affect
operation by wrong use, plea
se carefully use it with HUAWEI engineer's direction. Are you sure to continue?[Y/
N]:Y
*****************************************************
*             OSP card output to mainboard          *
*****************************************************
Press Ctrl+D to quit

[Huawei]
root@Hi3716CV200:/ #
```

4.2.18 set root-key

Function

The **set root-key** command configures a root key.

By default, a device uses the system default root key.

Format

set root-key

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

A root key is located at the bottom of the key management infrastructure to protect confidentiality of upper-layer keys (such as key encryption key). Therefore, a root key is important to data security. A device's root key is often stored in the system. If attackers illegally obtain the root key, encrypted data will become insecure. To improve data security and prevent attackers from obtaining encrypted packets, reconfigure a root key on the device. The configured root key will take effect after the device restarts.

Example

Set the device root key to **huawei**.

```
<Huawei> set root-key
Warning: A new root key can take effect only after the device is restarted. Are you sure you want to
configure it? [Y/N]:y
Please enter a new key:huawei
Please enter the new key again:huawei
Info: Successed in setting next root-key on the master board.
```

Related Topics

4.2.2 clear root-key

4.2.19 set rps force

Function

The **set rps force** command forces the RPS to supply power for the device.

 Copyright © Huawei Technologies Co., Ltd.

The **undo set rps force** command disables the RPS from supplying power for the device.

By default, the system does not force the RPS to supply power for the device.

NOTE

Only the AR2201-48FE, AR2202-48FE, AR2204, AR2220E support this function.

Format

set rps force

undo set rps force

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RPS functions as the external backup power supply for the device. When a fault occurs in the internal power supply system, the RPS can supply power for the device in a timely manner to ensure normal device running. Before repairing the internal power supply, run the **set rps force** command to force the RPS to supply power for the device.

Prerequisites

The device is connected to an external RPS and the RPS is working properly.

Example

Force the RPS to supply power for the device.

```
<Huawei> system-view
[Huawei] set rps force
Info: Set the RPS force successfully.
```

Related Topics

4.2.5 display rps status

4.2.20 set transceiver

Function

Using the **set transceiver** command, you can set the alarm threshold of the optical power of the optical module.

Using the **undo set transceiver** command, restore the default power alarm thresholds of an optical module.

The default power alarm thresholds vary according to types of optical modules.

Format

set transceiver { **transmit-power** | **receive-power** } { **upper-threshold** | **lower-threshold** } *threshold*

undo set transceiver { **transmit-power** | **receive-power** } { **upper-threshold** | **lower-threshold** }

Parameters

Parameter	Description	Value
transmit-power	Indicates the transmission power.	-
receive-power	Indicates the receiving power.	-
upper-threshold	Indicates the upper alarm threshold of the optical power.	-
lower-threshold	Indicates the lower alarm threshold of the optical power.	-
threshold	Specifies the value of the alarm threshold.	The value varies according to optical module type. The alarm threshold is accurate to two digits after the decimal point.

Views

Ethernet interface view, GE interface view, XGE interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **set transceiver** command is invalid on electrical interfaces. This command is invalid for the interface without an optical module. It is recommended that you run the **4.1.18 display transceiver** command to view the upper and lower alarm thresholds of the optical power of the optical module before you set the alarm thresholds. Otherwise, the alarm thresholds you set may be invalid. In this case, error information is displayed.

An optical module has an original upper and lower alarm thresholds of the optical power. After you run the **set transceiver** command, the alarm threshold set by this command replaces the original alarm threshold.

The upper alarm threshold that you set must be greater than the original lower alarm threshold of the optical module and smaller than or equal to the original upper alarm threshold. If the upper alarm threshold is not set, the original upper alarm threshold of the optical module is used.

The lower alarm threshold that you set must be greater than or equal to the original lower alarm threshold of the optical module and smaller than the upper alarm threshold that you set. If the lower alarm threshold is not set, the original lower alarm threshold of the optical module is used.

Example

Set the lower alarm threshold of the receiving power of optical module on GE1/0/1 to -10 dBm and set the upper alarm threshold of the receiving power to -0.9 dBm. Then check the configuration.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/1
[Huawei-GigabitEthernet1/0/1] set transceiver receive-power lower-threshold -10
[Huawei-GigabitEthernet1/0/1] set transceiver transmit-power upper-threshold -0.9
```

Related Topics

4.1.18 display transceiver

4.2.21 set transceiver-monitoring

Function

The **set transceiver-monitoring** command enables or disables the alarm function for optical modules.

By default, the alarm function is disabled for optical modules.

Format

set transceiver-monitoring { **enable** | **disable** }

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the alarm function for optical modules.

```
<Huawei> system-view
[Huawei] set transceiver-monitoring enable
```

Related Topics

4.1.18 display transceiver

4.2.22 set vendorname

Function

The **set vendorname** command sets a Broadcom chip name.

The **undo set vendorname** command cancels the configured Broadcom chip name.

By default, a Broadcom chip is named BDCM.

Format

set vendorname *vendorname*

undo set vendorname

Parameters

Parameter	Description	Value
vendorname	Specifies a Broadcom chip name.	The value is a combination of four uppercase letters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To change the chip name reported to a DSLAM, run the **set vendorname** command to configure a chip name.

Precautions

- If the device has a daughter card with a Broadcom chip installed, after running the **set vendorname** command, you need to restart the corresponding interface by running the **shutdown** and **undo shutdown** commands or running the **restart** command to make the configuration take effect after running the **set vendorname** command.
- If the device does not have a daughter card with a Broadcom chip installed, you do not need to restart the corresponding interface after running the **set vendorname** command and then installing the daughter card. The command configuration automatically takes effect on the newly installed daughter card.
- If you run the **set vendorname** command multiple times, only the latest configuration takes effect.

Example

Set the Broadcom chip name to ABCD if the device has a daughter card with a Broadcom chip installed.

```
<Huawei> system-view
[Huawei] set vendorname ABCD
 Info: This operation takes effect after the interface shutdown and undo shutdown !
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] shutdown
[Huawei-Ethernet0/0/0] undo shutdown
```

Related Topics

5.1.16 shutdown (interface view)

5.1.14 restart (interface view)

4.2.23 slave default

Function

The **slave default** command sets the slot ID of the default slave MPU used after the next startup.

The **undo slave default** command cancels the configuration.

By default, the master MPU is in slot 15 and the slave MPU is in slot 14.

NOTE

Only AR3200 series supports this function.

Format

slave default *slot-id*

undo slave default

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID of the slave MPU after the next startup.	The slot ID is 14 or 15.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When both the master and slave MPUs on a device are properly installed, you can run the **slave default** command to configure the MPU in a specified slot as the slave MPU after the next startup.

Example

Configure the MPU in slot 14 as the slave MPU when the system restarts.

```
<Huawei> system-view
[Huawei] slave default 14
```

Related Topics

4.2.8 display slave default

4.2.24 slave restart

Function

The **slave restart** command resets the slave MPU.

NOTE

Only AR3200 series supports this function.

Format

slave restart

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To upgrade the system software in-service, first upgrade the software on the slave main control board when the master main control board works normally, and then restart the slave main control board. After the slave main control board is ready, perform active/standby switchover and upgrade the software on the master main control board.

Example

Restart the slave main control board.

```
<Huawei> system-view
[Huawei] slave restart
```

4.2.25 slave switchover

Function

The **slave switchover** command performs a master/slave switchover.

NOTE

Only AR3200 series supports this function.

Format

slave switchover

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During software upgrade or system maintenance, you can manually perform a master/slave switchover on MPUs. The master/slave switchover restarts the running master and slave MPUs. After the restart, the master MPU becomes the slave and the slave MPU becomes the master.

No master/slave main control board switchover can be performed before the patch on the registered slave main control board is restored.

Prerequisites

- The forcible master/slave switchover has been enabled on device.
- The **4.2.9 display switchover state** command output shows that system has met requirements for master/slave switchover.

Example

Perform a master/slave switchover.

```
<Huawei> system-view
[Huawei] switchover enable
[Huawei] slave switchover
Warning: Are you sure to switch over?[Y/N]:y
```

Related Topics

4.2.9 display switchover state

4.2.26 switchover enable

4.2.26 switchover enable

Function

The **switchover enable** command enables forcible master/slave switchover.

The **switchover disable** command disables forcible master/slave switchover.

By default, master/slave switchover is enabled.

NOTE

Only AR3200 series supports this function.

Format

switchover enable

switchover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **slave switchover** command takes effect only after forcible master/slave switchover is enabled. If forcible master/slave switchover is disabled, the **4.2.25 slave switchover** command does not take effect.

Example

Disable forcible master/slave switchover.

```
<Huawei> system-view
[Huawei] switchover disable
```

Related Topics

4.2.9 display switchover state

4.2.25 slave switchover

4.2.27 transceiver phony-alarm-disable

Function

The **transceiver phony-alarm-disable** command disables the alarm function for non-Huawei-certified optical modules.

The **undo transceiver phony-alarm-disable** command enables the alarm function for non-Huawei-certified optical modules.

By default, the alarm function for non-Huawei-certified optical modules is enabled.

Format

transceiver phony-alarm-disable

undo transceiver phony-alarm-disable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Non-Huawei-certified optical modules may fail to work normally. If non-Huawei-certified optical modules are used on devices produced since January 1, 2013, the devices generate a large number of alarms to prompt users to replace these optical modules with Huawei-certified optical modules. This facilitates optical module management and maintenance. Additionally, vendor information of optical modules early delivered from Huawei may not be recorded. When these optical modules are used on devices, the devices will also generate non-Huawei-certified optical module alarms. To protect user resources and ensure that these early delivered optical modules work properly, run the **transceiver phony-alarm-disable** command. This command will then disable the alarm function.

NOTE

If no such early delivered optical modules are used on devices, you are advised to enable the alarm function for non-Huawei-certified optical modules.

Example

Disable the alarm function for non-Huawei-certified optical modules.

```
<Huawei> system-view
[Huawei] transceiver phony-alarm-disable
```

4.2.28 upgrade osp-module software

Function

The **upgrade osp-module software** command upgrades the software version of an OSP daughter card.

NOTE

Only AR169-P-M9, AR169W-P-M9 and AR169RW-P-M9 support this command.

Format

upgrade osp-module software *filename*

Parameters

Parameter	Description	Value
filename	Specifies the upgrade file name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **upgrade osp-module software** command to upgrade an OSP daughter card without replacing the system software.

Example

Upgrade the software version of an OSP daughter card.

```
<Huawei> system-view
[Huawei] upgrade osp-module software osp_file.bin
```

4.2.29 set osp power uninterruptible

Function

The **set osp power uninterruptible** command configures automatic power-on for the OSP daughter card.

The **undo set osp power uninterruptible** command cancels automatic power-on for the OSP daughter card.

By default, automatic power-on is not configured for the OSP daughter card.

NOTE

This command is supported only by the AR169-P-M9, AR169W-P-M9, and AR169RW-P-M9.

Format

set osp power uninterruptible

undo set osp power uninterruptible

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

The Windows operating system installed on the OSP daughter card of the device cannot be powered on automatically after the device is restarted. To address this issue, you can configure automatic power-on for the OSP daughter card using the **set osp power uninterruptible** command.

Example

Configure automatic power-on for the OSP daughter card.

```
<Huawei> system-view
[Huawei] set osp power uninterruptible
```

4.2.30 super-fast hardware enable

Function

The **super-fast hardware enable** command enables hardware acceleration.

The **super-fast hardware disable** command disables hardware acceleration.

By default, hardware acceleration is disabled.

NOTE

Only the AR161, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169RW-P-M9, and AR169W-P-M9 support this command.

Format

super-fast hardware enable

super-fast hardware disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you require a high forwarding rate, run the **super-fast hardware enable** command to enable hardware acceleration. This configuration can increase the rate.

Precautions

After the **super-fast hardware enable** command is executed, the device supports only IPv4 service forwarding on Layer 3 interfaces excluding VLANIF interfaces and does not support other functions.

Example

Enable hardware acceleration.

```
<Huawei> system-view
[Huawei] super-fast hardware enable
```

Related Topics

4.2.10 display super-fast hardware state

4.3 Information Center Configuration Commands

4.3.1 display actived-alarm highest-level

Function

The **display actived-alarm highest-level** command displays the highest alarm severity levels of current active alarms.

Format

display actived-alarm highest-level

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the highest alarm severity levels of current active alarms.

```
<Huawei> display actived-alarm highest-level
 Info: The highest level of active alarm is critical.
```

Table 4-28 Description of the **display actived-alarm highest-level** command output

Item	Description
The highest level of active alarm is	Highest severity levels of current active alarms include: ● critical: indicates that a fault affects normal operation of the system. Effective measures must be taken immediately. For example, if a device or resources become unavailable, the fault needs to be rectified immediately even if the fault occurs during non-working hours. ● major: indicates that a fault decreases system quality. Effective measures must be taken immediately. For example, if service quality of a device or resources is reduced and needs to be restored, measures need to be taken immediately during working hours. ● minor: indicates that a fault has not affected service quality but needs to be processed or observed to prevent serious faults. ● warning: indicates that a fault may have potential errors that will affect services, requiring measures to be taken according to errors. ● indeterminate: indicates that the severity level is not determined. That is, impact of alarms depends on the environment. ● cleared: indicates the clearing of one or more previously reported alarms. This alarm clears all alarms for this managed object that have the same alarm type, possible causes and specific problems. Multiple associated notifications may be cleared using the correlated notifications parameter.

4.3.2 display channel

Function

The **display channel** command displays the channel configuration.

Format

display channel [*channel-number* | *channel-name*]

Parameters

Parameter	Description	Value
channel-number	Specifies the number of a channel.	The value is an integer than ranges from 0 to 9. That is, the system has 10 channels. Channels 0 to 5 have default names and the six channels map to six different output directions. **Table 4-29** shows the relationship between channels and output directions.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-sensitive characters. The value consists of letters or numbers and must start with a letter.

Table 4-29 Relationship between channel and output directions

Channel Number	Default Channel Name	Output Direction	Description
0	console	console	Console that can receive logs, traps, and debugging messages.
1	monitor	monitor	VTY terminal that can receive logs, traps, and debugging messages, which facilitates remote maintenance.
2	loghost	loghost	Log host that can receive logs, traps, and debugging messages. By default, information is saved on the log host in file format for easy reference.
3	trapbuffer	trapbuffer	Trap buffer that can receive traps.
4	logbuffer	logbuffer	Log buffer that can receive logs.
5	snmpagent	snmpagent	SNMP agent that can receive traps.
6	channel6	Unspecified	Reserved. You can specify to which destination this channel can output information.
7	channel7	Unspecified	Reserved. You can specify to which destination this channel can output information.
8	channel8	Unspecified	Reserved. You can specify to which destination this channel can output information.

 Copyright © Huawei Technologies Co., Ltd.

Channel Number	Default Channel Name	Output Direction	Description
9	channel9	logfile	Log file that can receive logs, traps, and debugging messages. Information is saved to the USB flash drive or SD card in file format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display channel** command displays the channel configuration.

When using this command, note the following points:

- When *channel-number* or *channel-name* is specified, the **display channel** command displays the specified channel that information passes through and information severity.
- When *channel-number* or *channel-name* is not specified, the **display channel** command displays all the channels that information passes through and information severity.

Example

Display the configuration of channel 0.

```
<Huawei> display channel 0
channel number: 0, channel name: console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging
```

Display the configuration of all channels.

```
<Huawei> display channel
channel number: 0, channel name: console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging

channel number: 1, channel name: monitor
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       Y      debugging     Y      debugging

channel number: 2, channel name: loghost
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      informational Y      debugging     N      debugging

channel number: 3, channel name: trapbuffer
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
```

```
ffff0000 default  N      informational Y      debugging     N      debugging

channel number: 4, channel name: logbuffer
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warning       N      debugging     N      debugging

channel number: 5, channel name: snmpagent
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  N      debugging     Y      debugging     N      debugging

channel number: 6, channel name: channel6
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number: 7, channel name: channel7
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number: 8, channel name: channel8
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging

channel number: 9, channel name: channel9
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      debugging     Y      debugging     N      debugging
```

Table 4-30 Description of the display channel command output

Item	Description
channel number	Channel number, which ranges from 0 to 9.
channel name	Channel name. **Table 4-29** lists default channel names. To set the channel name, run the **4.3.16 info-center channel name** command.
MODU_ID	Module ID. The default value is ffff0000.
NAME	Module name. The default value is **default**. To set the module name, run the **4.3.30 info-center source channel** command.
ENABLE	Whether logs/traps/debugging messages are allowed to pass through a channel: ● Y ● N To specify the channel, run the **4.3.30 info-center source channel** command.

Item	Description
LOG_LEVEL/ TRAP_LEVEL/ DEBUG_LEVEL	Lowest severity of output logs/traps/debugging messages. The following severities are listed in descending order of priority: • emergencies • alert • critical • error • warning • notification • informational • debugging To set the lowest severity of output logs, run the **4.3.30 info-center source channel** command.

Related Topics

4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.30 info-center source channel

4.3.3 display debugging

Function

The **display debugging** command displays debugging messages allowed to be sent by the device.

Format

display debugging [**interface** *interface-type interface-number*] [*module-name*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
module-name	Displays debugging messages sent by a specified module such as the DHCP module. If this parameter is not specified, all debugging messages allowed to be sent are displayed.	Enumerated type. The value depends on the registered module.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Debugging affects device performance. The **display debugging** command displays debugging messages allowed to be sent by the Router.

Prerequisites

By default, sending debugging messages is prohibited. The debugging of a specified module has been enabled.

Example

Display debugging messages allowed to be sent by the Router.

```
<Huawei> display debugging
ACL error debugging is on, on the slot 0
```

Display debugging messages allowed by the ARP module.

```
<Huawei> display debugging arp
slot[0]:ARP packet debugging is on
```

Related Topics

4.3.17 info-center enable

4.3.30 info-center source channel

4.3.39 terminal debugging

4.3.41 terminal monitor

4.3.4 display info-center

Function

The **display info-center** command displays the output configuration of the information center.

Format

display info-center

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display output configuration of the information center.

```
<Huawei> display info-center
Information Center: enabled
Log host:
        10.1.1.1, channel number: 2, channel name: loghost
        language: english, host facility: local7
Console:
        channel number: 0, channel name: console
Monitor:
        channel number: 1, channel name: monitor
SNMP Agent:
        channel number: 5, channel name: snmpagent
Log buffer:
        enabled
        max buffer size: 1024, current buffer size: 512
        current messages: 6, channel number: 4, channel name: logbuffer
        dropped messages: 0, overwritten messages: 0
Trap buffer:
        enabled
        max buffer size: 1024, current buffer size: 256
        current messages: 0, channel number: 3, channel name: trapbuffer
        dropped messages: 0, overwritten messages: 0
Logfile:
        channel number: 9, channel name: channel9, language: English
Information timestamp setting:
        log - date, trap - date, debug - date

 Sent messages = 25, Received messages = 25
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-31 Description of the display info-center command output

Item	Description
Information Center	Information center status: ● enabled ● disabled To enable the information center, run the **4.3.17 info-center enable** command.
Log host	Log host configuration.
10.1.1.1	Log host IP address. To set the log host IP address, run the **4.3.23 info-center loghost** command.
channel number	Number of a channel used to output information. To set the number of a channel used to output information, run the **4.3.15 info-center channel** command.
channel name	Name of a channel used to output information. To set the name of a channel used to output information, run the **4.3.16 info-center channel name** command.
language	Language mode in which information is output to a log host. To set the language mode in which information is output to a log host, run the **4.3.23 info-center loghost** command.
host facility	Logging tool. To configure the logging tool, run the **4.3.23 info-center loghost** command.
Console	Console configuration.
Monitor	Remote terminal configuration.
SNMP Agent	SNMP agent configuration.
Log buffer	Log buffer configuration.
enabled	Whether the Router is enabled to send logs/traps to the log/trap buffer. ● enabled ● disabled To enable the Router to send logs/traps to the log/trap buffer, run the **4.3.19 info-center logbuffer** or **4.3.33 info-center trapbuffer** command.
max buffer size	Maximum number of logs/traps in the log/trap buffer.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
current buffer size	Maximum number of logs/traps in the current log/trap buffer. To set the maximum number of logs/traps in the current log/trap buffer, run the **4.3.20 info-center logbuffer size** or **4.3.34 info-center trapbuffer size** command.
current messages	Number of messages recorded in the log/trap buffer.
dropped messages	Number of messages discarded by the log/trap buffer.
overwritten messages	Number of overwritten messages in the log/trap buffer.
Trap buffer	Trap buffer configuration.
logfile	Log file configuration.
Information timestamp setting	Timestamp format of logs, traps, and debugging messages: • boot: indicates that the timestamp is expressed in the format of relative time, a period of time since system start. • date: indicates the current system date and time. It is expressed in mm dd yyyy hh:mm:ss format. • short-date: indicates the short date. This timestamp differs from **date** is that the year is not displayed. • format-date: indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format. • none: indicates that the output information does not contain the timestamp. To configure the timestamp format, run the **4.3.32 info-center timestamp** command.
Sent messages	Number of sent messages output by information center modules.
Received messages	Number of messages sent to information center modules.

Related Topics

4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.19 info-center logbuffer
4.3.20 info-center logbuffer size
4.3.23 info-center loghost
4.3.32 info-center timestamp
4.3.33 info-center trapbuffer

 Copyright © Huawei Technologies Co., Ltd.

4.3.34 info-center trapbuffer size

4.3.5 display info-center filter-id

Function

The **display info-center filter-id** command displays information filtered by the information center.

Format

display info-center filter-id [*id* | **bymodule-alias** *modname alias*]

Parameters

Parameter	Description	Value
id	Displays filtered information with the specified ID.	The value is an integer that ranges from 0 to 4294967295.
bymodule-alias *modname alias*	Displays filtered information with the specified module name and mnemonic symbol. • *modname*: specifies the module name. • *alias* specifies the mnemonic symbol.	Enumerated type. Set the value according to the device configuration.

Views

All views

Default Level

3: Management level

Usage Guidelines

ID identifies each function module for log registration. An ID filter list is the aggregation of the shielded IDs.

If *id* or **bymodule-alias** is not specified, all information is filtered.

To prevent output of specified information, run the **4.3.18 info-center filter-id** command to add the ID to the filtering list, and then run the **display info-center filter-id** command to check whether information with this ID is filtered.

Example

Display filtered information with ID 3246215177.

```
<Huawei> display info-center filter-id 3246215177
ID            : 3246215177
Module          : 6OVER4
Alias          : DEL_UPTUNN_FAIL
Content         : Failed to delete the UPTUNNEL entry when processing ([STRING])
. (Interface=[STRING])
Filtered Number : 0
```

Display all the IDs in the filter list.

```
<Huawei> display info-center filter-id
ID            : 3246215177
Module          : 6OVER4
Alias          : DEL_UPTUNN_FAIL
Content         : Failed to delete the UPTUNNEL entry when processing ([STRING])
. (Interface=[STRING])
Filtered Number : 0

ID            : 3491254537
Module          : BGP
Alias          : ADD_DELETED_ROUTE
Content         : Add the route [STRING] that have other flags besides deleted f
lag [USHORT]
Filtered Number : 0
```

Table 4-32 Description of the display info-center filter-id command output

Item	Description
ID	Identifier to which each log corresponds. To configure the Router to filter a log or trap with a specified ID, run the **4.3.18 info-center filter-id** *id* command.
Module	Module name. To configure the Router to filter a log or trap with a specified module name or alias name, run the **4.3.18 info-center filter-id bymodule-alias** *modname alias* command.
Alias	Alias name. To configure the Router to filter a log or trap with a specified module name or alias name, run the **4.3.18 info-center filter-id bymodule-alias** *modname alias* command.
Content	Log message to which each log ID corresponds.
Filtered Number	Number of times that the log to which the log ID corresponds is filtered.

Related Topics

4.3.18 info-center filter-id

4.3.6 display info-center logfile path

Function

The **display info-center logfile path** command displays the path where log files are saved.

Format

display info-center logfile path

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display info-center logfile path** command displays the path where log files are saved. This command is used in the following scenarios:

- The information is output to the log file.
- The **save logfile** command is executed to save log files to the specified path.

Example

Display the path where log files are saved.

```
<Huawei> display info-center logfile path
Info: Logfile save path is usb0:/logfile
```

Related Topics

4.3.21 info-center logfile path

4.3.38 save logfile

4.3.7 display info-center rate-limit record

Function

The **display info-center rate-limit record** command displays the suppression of the log processing rate in the information center.

Format

display info-center rate-limit record

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the suppression of the log processing rate in the information center.

```
<Huawei> display info-center rate-limit record
Record No.1
 InfoID              : ff5ad009
 Module              : AAA
 Alias               : DESTFAILAUTHEN_ERR_EVENT
 Rate limit threshold : 50
 Total receive number : 1872
 Total drop number    : 922
 Total send number    : 950
 Begin timestamp      : 2014-11-18 11:41:28
```

Table 4-33 Description of the **display info-center rate-limit record** command output

Item	Description
InfoID	Log ID.
Module	Log module name.
Alias	Log mnemonic name.
Rate limit threshold	The maximum number of logs set for the information center to process every second.
Total receive number	The total number of logs that are generated during the latest suppression period.
Total drop number	The total number of logs that are discarded during the latest suppression period.
Total send number	The total number of logs that the information center process during the latest suppression period.
Begin timestamp	The timestamp signifying when the suppression function is enabled for the last time.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

4.3.29 info-center rate-limit threshold

4.3.8 display info-center rate-limit threshold

Function

The **display info-center rate-limit threshold** command displays the threshold of the log processing rate (maximum number of logs that the information center can process every second). The threshold information includes the default threshold contained in the released version, the default threshold for the specified log ID, and the threshold set through the command lines after the system startup.

Format

display info-center rate-limit threshold

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the threshold of the log processing rate set for the information center.

```
<Huawei> display info-center rate-limit threshold
Rate limit threshold(per second):
 Module        Alias                          Default  Config
 default                                  30       30
 IPC           IPCFRGTOOLARGE                    5        5
 IPC           IPCDUMPMEM                        5        5
 IPC           ALLOCINDEXERR                     5        5
 IPC           DRVNOTSTABLE                      2        2
 IPC           NOTIMODFALNOREASM                 2        2
 IPC           SYNRPCGETSMFAL                    5        5
 IPC           SYNRPCMODUNREG                    5        5
 IPC           SYNRPCRETNULL                     5        5
 IPC           MODULENOTREG                      5        5
 IPC           SENDRETURN                        5        5
 IPC           GETMTUFAL                         5        5
 IPC           ALLOCIPCFRGFAL                    5        5
 IPC           RECVINVALIDMSG                    5        5
 IPC           RCVNOTIQUEERR                     5        5
 IPC           NOTIFYQUEERR                      5        5
 IPC           SENDFINISHRETURN                  5        5
 IPC           RECVINVALIDMSGTYPE                5        5
 SOURCE        UMSGGETSRCOBJFAL                  1        1
```

Table 4-34 Description of the **display info-center rate-limit threshold** command output

Item	Description
Module	Log module name.
Alias	Log mnemonic name.
Default	The default threshold of the log processing rate.
Config	The threshold of the log processing rate set for the information center.

Related Topics

4.3.29 info-center rate-limit threshold

4.3.9 display info-center statistics

Function

The **display info-center statistics** command displays statistics in the information center.

Format

display info-center statistics

Parameters

Parameter	Description	Value
module-id *id*	Specify the displayed module ID.	It is a string of 8 characters in hex, including: 0 to 9, a to f, and A to F.
module-name *name*	Specify the displayed module name.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

The **display info-center statistics** command displays statistics in the information center.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics of shell in the information center.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] display info-center statistics module-name shell
Log & diag log information statistics data:
InfoID     level LogAlias                SendNum    DropNum
0x40391015   5     LOGIN                   15         0
0x40391016   5     LOGOUT                   9         0
0x4039101b   4     LOGINFAILED              0         0
0x4039101c   5     TIMEOUT                  0         0
0x40391020   4     OVERWRITE_EXEC           0         0
0x40391021   6     CMDCONFIRM_RECORD        0         0
0x40391022   6     CMDCONFIRM_UNIFORMRECORD 0         0
0x40391023   6     CMDCONFIRM_NOPROMPT      3         0
0x40391024   5     SETPASS_FAIL_FIRSTLOGIN  0         0
0x4039501d   4     CMDTIMEOUT               0         0
0x40395021   4     DISABLECMDFAIL           0         0
0x40395022   4     ENABLECMDFAIL            0         0
0x40395024   3     FAULT_USERINTERFACE      0         0
0x40399017   5     CMDRECORD             7314         2
0x40399018   6     DISPLAY_CMDRECORD       78         0

Debug information statistics data:
DebugID    level DebugAlias              SendNum    DropNum
0x40393000   7     AAARECEIVEOTHEREVT       0         0
0x40393001   7     AAARECEIVEOTHERMSG       0         0
0x40393002   7     AAAREADMSGFAIL           0         0
0x40393003   7     AAAREADEVTTIMEOUT        0         0
0x40393004   7     AAAREADEVTTIMEOUT10      0         0
0x40393005   7     AAAWRITECUTMSGFAIL       0         0
0x40393006   7     AUTHCMDSNDMSGFAIL        0         0
0x40393007   7     AUTHCMDTIMEOUT           0         0
0x40393008   7     AUTHCMDNONEED            0         0
0x40393009   7     NEEDAUTHCMD              0         0
0x4039300a   7     AUTHCMDFLAGCHG           0         0
0x4039300b   7     AUTHCMDFAIL              0         0
```

Table 4-35 Description of the display info-center statistics module-name shell command output

Item	Description
Log & diag log information statistics data	Statistics on message logs and diagnostic logs
InfoID	Information ID
level	Log level
LogAlias	Log analysis
SendNum	Number of send logs
DropNum	Number of discard logs
Debug information statistics data	Statistics on debug logs
DebugID	Debug log ID

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DebugAlias	Debug log analysis

4.3.10 display log

Function

Using the **display log** command, you can query all the logs or a specified log.

Format

display log [**cli** | **snmp**] **index** *index1* [*index2*]

display log [**cli** | **snmp**] { **all** | **name** *username* } [*start-date* [*start-time* [**–** *end-date* [*end-time*]]]]

Parameters

Parameter	Description	Value
cli	Queries specified logs.	-
snmp	Queries network management logs.	-
index *index1* [*index2*]	Indicates the index of the log to be queried. *index1* is the start index of the logs and *index2* is the end index of the logs. That is, the logs with the index starting from *index1* and ending with *index2* are displayed.	Numeral type. Range: 1-64.
name *username*	Queries logs by user name.	It is a string of 1-15 characters.
all	Queries logs of all users.	-
[*start-date* [*start-time* [**–** *end-date* [*end-time*]]]]	Sets the date and time when you query logs by user name or query logs of all users.	*start-date*: The real start date. Date format: yyyy-mm-dd. *start-time*: The real start time. Time format: hh:mm:ss. *end-date*: The real end date. Date format: yyyy-mm-dd. *end-time*: The real end time. Time format: hh:mm:ss.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

- When querying logs by **name** or by **all**, you can also query these logs by period.
- This command can be used to query logs of the user with the level the same as yours or lower than yours.
- Use parameters to display operation information about different users in different periods, for example, enter **all** to display the logs of all users.
- When a configuration is incorrect, a fault will occur. To locate the fault, run this command to query logs to learn about basic information, such as the name of the user who operates the system, the IP address of the user, the specific time when the user performs an operation, and the detailed operations.

Example

Query logs with indexes from 10 to 15.

```
<Huawei> display log index 10 15
  ------------------------------------------------------------------------------
  No.   UserName                    Domain          IP-Address
   15                          --              10.138.78.127
  Time: 2007-08-25 18:00:43+00:00
  Cmd:  traffic classifier cy
  ------------------------------------------------------------------------------
  No.   UserName                    Domain          IP-Address
   14                          --              10.138.78.127
  Time: 2007-08-25 17:59:51+00:00
  Cmd:  undo traffic behavior cy
  ------------------------------------------------------------------------------
  No.   UserName                    Domain          IP-Address
   13                          --              10.138.78.127
  Time: 2007-08-25 17:59:42+00:00
  Cmd:  undo traffic policy cy
  ------------------------------------------------------------------------------
  No.   UserName                    Domain          IP-Address
   12                          --              10.138.78.127
  Time: 2007-08-25 17:55:26+00:00
  Cmd:  quit
  ------------------------------------------------------------------------------
  No.   UserName                    Domain          IP-Address
   11                          --              10.138.78.127
  Time: 2007-08-25 17:54:05+00:00
  Cmd:  undo classifier cy
  No.   UserName                    Domain          IP-Address
   10                          --              10.138.78.127
  Time: 2007-08-25 17:54:05+00:00
  Cmd:  traffic policy cy
  ------------------------------------------------------------------------------
```

Query logs of all users within the period starting at 17:10:10 on 2007-08-25 and ending at 17:20:10 on 2007-08-25.

```
<Huawei> display log all 2007-08-25 17:10:10 - 2007-08-25 17:20:10
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   78                          --            10.138.78.127
 Time: 2007-08-25 17:19:59+00:00
 Cmd:  stp enable                  7
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   77                          --            10.138.78.127
 Time: 2007-08-25 17:19:47+00:00
 Cmd:  stp pathcost-standard legacy
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   76                          --            10.138.78.127
 Time: 2007-08-25 17:19:35+00:00
 Cmd:  stp root primary
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   75                          --            10.138.78.127
 Time: 2007-08-25 17:19:04+00:00
 Cmd:  log off
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   74                          --            10.138.78.127
 Time: 2007-08-25 17:18:54+00:00
 Cmd:  system-view
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   73                          --            10.138.78.127
 Time: 2007-08-25 17:18:49+00:00
 Cmd:  log on
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   72                          --            10.138.78.127
 Time: 2007-08-25 17:18:17+00:00
 Cmd:  stp root primary
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   71                          --            10.138.78.128
 Time: 2007-08-25 17:18:13+00:00
 Cmd:  info-center snmp channel snmpagent
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   70                          --            10.138.78.127
 Time: 2007-08-25 17:18:04+00:00
 Cmd:  stp mode stp
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   69                          --            10.138.78.127
 Time: 2007-08-25 17:17:58+00:00
 Cmd:  system-view
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   68                          --            10.138.78.127
 Time: 2007-08-25 17:17:35+00:00
 Cmd:  log on
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   67                          --            10.138.78.128
 Time: 2007-08-25 17:17:31+00:00
 Cmd:  info-center monitor channel monitor
 ------------------------------------------------------------------------------
 No.   UserName                    Domain          IP-Address
   66                          --            10.138.78.128
 Time: 2007-08-25 17:15:37+00:00
 Cmd:  info-center loghost source Ethernet 0/0/1
```

```
-------------------------------------------------------------------------------
No.   UserName                    Domain          IP-Address
  65                          --              10.138.78.128
Time: 2007-08-25 17:13:04+00:00
Cmd:  info-center loghost 10.1.1.2 language English
-------------------------------------------------------------------------------
No.   UserName                    Domain          IP-Address
  64                          --              10.138.78.128
Time: 2007-08-25 17:11:55+00:00
Cmd:  system-view
-------------------------------------------------------------------------------
No.   UserName                    Domain          IP-Address
  63                          --              10.138.78.128
Time: 2007-08-25 17:11:53+00:00
Cmd:  log on
-------------------------------------------------------------------------------
```

Table 4-36 Description of the **display log** command output

Item	Description
No.	Serial number of each log. The serial number is generated automatically by the system.
UserName	User name of the log
Time	Detailed operation time of the user
IP-Address	IP address of the user
Cmd	Detailed operations of the user
Domain	Domain name of the log

4.3.11 display logbuffer

Function

The **display logbuffer** command displays information recorded in the log buffer.

Format

display logbuffer [**size** *size* | **module** *module-name* | **level** *severity*] *

display logbuffer summary [**level** *severity*]

display logbuffer log-offset *offset-value* **size** *size*

Parameters

Parameter	Description	Value
size *size*	Displays the specified number of logs recently generated in the log buffer.	The value is an integer that ranges from 1 to 1024.
module *module-name*	Displays logs of a specified module in the log buffer.	Enumerated type. The value depends on the registered module.
level *severity*	Displays logs of specified severity in the log buffer.	Enumerated type. The value ranges from 0 to 7. ● 0: emergencies ● 1: alert ● 2: critical ● 3: error ● 4: warning ● 5: notification ● 6: informational ● 7: debugging
summary	Displays the summary of logs in the log buffer.	-
log-offset *offset-value*	Specifies logs of the specified offset in the log buffer.	The value is an integer that ranges from 0 to 1024.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- You can use the **display logbuffer log-offset** *offset-value* **size** *size* command to view specified logs in the log buffer. For example, the log buffer has 100 logs. TO view the 20th to 50th logs in the log buffer, run the **display logbuffer log-offset 20 size 30** command.
- Run the **display logbuffer** [**size** *size* | **module** *module-name* | **level** *severity*] * command to view logs of specified number, module, or severity in the log buffer. If **size**, **module**, or **level** is not specified, this command displays all logs in the log buffer.

- You can run the **display logbuffer summary** command to view logs of different severities in the log buffer.

Precautions

- When the number of logs in the log buffer is smaller than *value*, logs of the actual number are displayed.
- When the number of logs in the log buffer is smaller than *offset-value*, the system displays an error message.
- When the number of logs in the log buffer is larger than *offset-value*, the system displays logs starting from *offset-value* plus one. The log quantity is specified by *size*. If the log quantity is less than *size*, the system displays all the logs starting from *offset-value* plus one.

Example

Display all the logs in the log buffer.

```
<Huawei> display logbuffer
Logging buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 512
Channel number: 4, Channel name: logbuffer
Dropped messages: 0
Overwritten messages: 167
Current messages: 512

May 10 2012 13:42:59+00:00 huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[0]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=912)
May 10 2012 13:32:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[1]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 13:22:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[2]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 13:12:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[3]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=912)
May 10 2012 13:02:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[4]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 12:52:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[5]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 12:42:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[6]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=912)
May 10 2012 12:32:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[7]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 12:22:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[8]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 12:12:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[9]:Some packets a
re dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=912)
May 10 2012 12:02:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[10]:Some packet
s are dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 11:52:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[11]:Some packet
s are dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 11:42:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[12]:Some packet
s are dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
```

```
Count=912)
May 10 2012 11:32:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[13]:Some packet
s are dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 11:22:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[14]:Some packet
s are dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 11:12:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[15]:Some packet
s are dropped by cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 11:08:37+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[16]:Interface Ethern
et5/0/2 has turned into UP state.
May 10 2012 11:08:37+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[17]:Interface Ethern
et5/0/1 has turned into UP state.
May 10 2012 11:08:37+00:00 Huawei %%01IFNET/4/LINK_STATE(l)[18]:The line proto
col IP on the interface Vlanif20 has entered the UP state.
May 10 2012 11:08:37+00:00 Huawei %%01IFNET/4/IF_STATE(l)[19]:Interface Vlanif
20 has turned into UP state.
May 10 2012 11:08:37+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[20]:Interface Ether
net5/0/0 has turned into UP state.
May 10 2012 11:08:34+00:00 Huawei %%01IFNET/4/IF_ENABLE(l)[21]:Interface Gigab
itEthernet5/0/0 has been available.
May 10 2012 11:08:34+00:00 Huawei %%01IFNET/4/IF_ENABLE(l)[22]:Interface Ether
net5/0/7 has been available.
May 10 2012 11:08:34+00:00 Huawei %%01IFNET/4/IF_ENABLE(l)[23]:Interface Ether
net5/0/6 has been available.
```

Table 4-37 Description of the display logbuffer command output

Item	Description
Logging buffer configuration and contents	Whether the device is enabled to output logs to the log buffer: ● enabled ● disabled To configure the device to output logs to the log buffer, run the **4.3.19 info-center logbuffer** command.
Allowed max buffer size	Maximum size of the log buffer.
Actual buffer size	Actual size of the log buffer. To set the log buffer size, run the **4.3.20 info-center logbuffer size** command.
Channel number	Number of the channel used to send logs to the log buffer. To configure the number of a channel used to send logs to the log buffer, run the **4.3.15 info-center channel** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Channel name	Name of the channel used to send logs to the log buffer. To configure the name of a channel used to send logs to the log buffer, run the **4.3.16 info-center channel name** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

Display the summary of information in the log buffer.

```
<Huawei> display logbuffer summary
 EMERG ALERT  CRIT ERROR  WARN NOTIF  INFO DEBUG
     0     0     0    14   498     0     0     0
```

Table 4-38 Description of the display logbuffer summary command output

Item	Description
EMERG	Number of logs of emergencies.
ALERT	Number of logs of alert.
CRIT	Number of logs of critical.
ERROR	Number of logs of error.
WARN	Number of logs of warning.
NOTIF	Number of logs of notification.
INFO	Number of logs of informational.
DEBUG	Number of logs of debugging.

Display 10 logs starting from log 16.

```
<Huawei> display logbuffer log-offset 15 size 10
Logging buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 512
Channel number: 4, Channel name: logbuffer
Dropped messages: 0
Overwritten messages: 168
Current messages: 512

May 10 2012 11:12:59+00:00 Huawei %%01DEFD/4/CPCAR_DROP_MPU(l)[0]:Some packets are dropped by
cpcar on the MPU. (Packet-type=arp-request, Drop-
Count=684)
May 10 2012 11:08:37+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[1]:Interface Ethernet5/0/2 has turned into
UP state.
May 10 2012 11:08:37+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[2]:Interface Ethernet5/0/1 has turned into
```

```
UP state.
May 10 2012 11:08:37+00:00 Huawei %%01IFNET/4/LINK_STATE(l)[3]:The line protocol IP on the interface
Vlanif20 has entered the UP state.
May 10 2012 11:08:37+00:00 Huawei %%01IFNET/4/IF_STATE(l)[4]:Interface Vlanif20 has turned into UP
state.
May 10 2012 11:08:37+00:00 Huawei %%01IFPDT/4/IF_STATE(l)[5]:Interface Ethernet5/0/0 has turned into
UP state.
May 10 2012 11:08:34+00:00 Huawei %%01IFNET/4/IF_ENABLE(l)[6]:Interface GigabitEthernet5/0/0 has
been available.
May 10 2012 11:08:34+00:00 Huawei %%01IFNET/4/IF_ENABLE(l)[7]:Interface Ethernet5/0/7 has been
available.
May 10 2012 11:08:34+00:00 Huawei %%01IFNET/4/IF_ENABLE(l)[8]:Interface Ethernet5/0/6 has been
available.
May 10 2012 11:08:34+00:00 Huawei %%01IFNET/4/IF_ENABLE(l)[9]:Interface Ethernet5/0/5 has been
available.
```

Related Topics

4.3.4 display info-center
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.19 info-center logbuffer
4.3.20 info-center logbuffer size
4.3.36 reset logbuffer

4.3.12 display logfile

Function

The **display logfile** command displays information about a log file.

Format

display logfile *file-name* [*offset* | **hex**] *

Parameters

Parameter	Description	Value
file-name	Specifies the log file name, which can contain the drive and path.	The value is a string of 1 to 64 case-insensitive characters without spaces.
offset	Displays the log file with the specified offset or byte.	The value is an integer that ranges from 0 to 2147483647.
hex	Displays the log file in hexadecimal notation. If the parameter is not specified, the log file is displayed in text format.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

When encountering problems, you can query log information to know about what happened during device operation. This is helpful for fault location.

If the version saved in a log file and the version generated by the system are different, the log file is displayed in hexadecimal notation.

The file name is generated automatically by the system. The file name extension of the log file is *.log or *.dblg.

If the size of the current log file reaches the upper threshold, the system transfers the log file into a historical compressed file.

Precautions

If the files you filter based on the pipe character are large and no qualified log file is displayed, the command may fail to display any output for a long period of time until the command execution finishes.

When viewing the *.log.zip file, it is recommended that the length of the file name (including the driver and path) not exceed 62 bytes. Otherwise, the content of the file may fail to be viewed.

Example

Display log information saved in the log file in hexadecimal notation.

```
<Huawei> display logfile usb0:/logfile/log.log


#################################################################
#     This logfile is generated at slot 0
#################################################################

Apr 23 2011 11:06:51+00:00 huawei IFNET/1/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Int
erface 6 turned into DOWN state.(AdminStatus 1,OperStatus 2,InterfaceName Ethern
et0/0/1)
Apr 23 2011 11:06:51+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3487]:Interface Ethern
et0/0/1 has turned into DOWN state.
Apr 23 2011 11:06:53+00:00 huawei IFNET/6/IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Inter
face 6 turned into UP state.(AdminStatus 1,OperStatus 1,InterfaceName Ethernet0/
0/1)
Apr 23 2011 11:06:53+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3488]:Interface Ethern
et0/0/1 has turned into UP state.
Apr 23 2011 11:06:53+00:00 huawei IFNET/1/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Int
erface 6 turned into DOWN state.(AdminStatus 1,OperStatus 2,InterfaceName Ethern
et0/0/1)
Apr 23 2011 11:06:53+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3489]:Interface Ethern
et0/0/1 has turned into DOWN state.
Apr 23 2011 11:06:55+00:00 huawei IFNET/6/IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Inter
face 6 turned into UP state.(AdminStatus 1,OperStatus 1,InterfaceName Ethernet0/
0/1)
Apr 23 2011 11:06:55+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3490]:Interface Ethern
et0/0/1 has turned into UP state.
```

```
Apr 23 2011 11:06:56+00:00 huawei IFNET/1/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Int
erface 6 turned into DOWN state.(AdminStatus 1,OperStatus 2,InterfaceName Ethern
et0/0/1)
Apr 23 2011 11:06:56+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3491]:Interface Ethern
et0/0/1 has turned into DOWN state.
Apr 23 2011 11:06:58+00:00 huawei IFNET/6/IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Inter
face 6 turned into UP state.(AdminStatus 1,OperStatus 1,InterfaceName Ethernet0/
0/1)
Apr 23 2011 11:06:58+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3492]:Interface Ethern
et0/0/1 has turned into UP state.
Apr 23 2011 11:06:59+00:00 huawei IFNET/1/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Int
erface 6 turned into DOWN state.(AdminStatus 1,OperStatus 2,InterfaceName Ethern
et0/0/1)
Apr 23 2011 11:06:59+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3493]:Interface Ethern
et0/0/1 has turned into DOWN state.
Apr 23 2011 11:07:00+00:00 huawei IFNET/6/IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Inter
face 6 turned into UP state.(AdminStatus 1,OperStatus 1,InterfaceName Ethernet0/
0/1)
Apr 23 2011 11:07:00+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3494]:Interface Ethern
et0/0/1 has turned into UP state.
Apr 23 2011 11:07:01+00:00 huawei IFNET/1/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Int
erface 6 turned into DOWN state.(AdminStatus 1,OperStatus 2,InterfaceName Ethern
et0/0/1)
Apr 23 2011 11:07:01+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3495]:Interface Ethern
et0/0/1 has turned into DOWN state.
Apr 23 2011 11:07:03+00:00 huawei IFNET/6/IF_PVCUP:OID 1.3.6.1.6.3.1.1.5.4 Inter
face 6 turned into UP state.(AdminStatus 1,OperStatus 1,InterfaceName Ethernet0/
0/1)
Apr 23 2011 11:07:03+00:00 huawei %%01IFPDT/4/IF_STATE(l)[3496]:Interface Ethern
et0/0/1 has turned into UP state.
Apr 23 2011 11:07:03+00:00 huawei IFNET/1/IF_PVCDOWN:OID 1.3.6.1.6.3.1.1.5.3 Int
erface 6 turned into DOWN state.(AdminStatus 1,OperStatus 2,InterfaceName Ethern
et0/0/1)
```

Display log information saved in the log file in hexadecimal notation.

```
<Huawei> display logfile usb0:/logfile/log.log hex
0d  0a  0d  0a  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23
23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23
23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23
23  23  23  23  23  23  23  23  0d  0a  23  20  20  20  20  20  54  68  69  73
20  6c  6f  67  66  69  6c  65  20  69  73  20  67  65  6e  65  72  61  74  65
64  20  61  74  20  73  6c  6f  74  20  30  0d  0a  23  23  23  23  23  23  23
23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23
23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23
23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  23  0d  0a  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00  00
```

Related Topics

4.3.17 info-center enable

4.3.21 info-center logfile path

4.3.22 info-center logfile size

4.3.25 info-center max-logfile-number

4.3.38 save logfile

4.3.13 display trapbuffer

Function

The **display trapbuffer** command displays information recorded in the trap buffer.

Format

display trapbuffer [**size** *value*]

Parameters

Parameter	Description	Value
size *value*	Displays the specified number of traps recently generated in the trap buffer. If this parameter is not specified, all traps are displayed.	The value is an integer that ranges from 1 to 1024.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display trapbuffer** command displays the information of recent traps. If the number of traps in the trap buffer is smaller than *value*, traps of the actual number are displayed.

Example

Display all traps in the trap buffer.

```
<Huawei> display trapbuffer
Trapping buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 256
Channel number: 3, Channel name: trapbuffer
Dropped messages: 0
Overwritten messages: 0
Current messages: 29

#Sep 17 2012 17:09:47+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 17 2012 17:06:50+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=0, LldpStatsRemTables
Deletes=1, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 14 2012 20:03:40+00:00 huawei ENTITYTRAP/4/CPUUSAGERESUME:OID 1.3.6.1.4.1.2
011.5.25.219.2.14.2 CPU utilization resumed from exceeding the pre-alarm thresho
ld.(Index=9, HwEntityThresholdIndex=0, HwEntityPhysicalIndex=9, PhysicalName="SR
U Board 0", EntityThresholdType=1, EntityThresholdWarning=80, EntityThresholdCur
rent=23, EntityTrapFaultID=144896)
```

 Copyright © Huawei Technologies Co., Ltd.

```
#Sep 14 2012 18:15:27+00:00 huawei LLDP/4/ADDCHGTRAP:OID: 1.3.6.1.4.1.2011.5.25.
134.2.5 Local management address is changed. (LocManIPAddr=1.1.1.9)
#Sep 14 2012 18:13:40+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 14 2012 18:13:23+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=0, LldpStatsRemTables
Deletes=1, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 14 2012 17:16:05+00:00 huawei ENTITYTRAP/4/CPUUSAGERESUME:OID 1.3.6.1.4.1.2
011.5.25.219.2.14.2 CPU utilization resumed from exceeding the pre-alarm thresho
ld.(Index=9, HwEntityThresholdIndex=0, HwEntityPhysicalIndex=9, PhysicalName="SR
U Board 0", EntityThresholdType=1, EntityThresholdWarning=80, EntityThresholdCur
rent=9, EntityTrapFaultID=144896)
#Sep 14 2012 17:15:37+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 14 2012 17:15:37+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 14 2012 17:15:34+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 14 2012 17:15:33+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
#Sep 14 2012 17:15:33+00:00 huawei LLDP/4/NBRCHGTRAP:OID: 1.0.8802.1.1.2.0.0.1 N
eighbor information is changed. (LldpStatsRemTablesInserts=1, LldpStatsRemTables
Deletes=0, LldpStatsRemTablesDrops=0, LldpStatsRemTablesAgeouts=0)
```

Display the first 10 records in the trap buffer.

```
<Huawei> display trapbuffer size 10
Trapping buffer configuration and contents: enabled
Allowed max buffer size: 1024
Actual buffer size: 256
Channel number: 3, Channel name: trapbuffer
Dropped messages: 0
Overwritten messages: 600
Current messages: 256

#May  7 2012 15:12:40+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
#May  7 2012 15:07:35+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
#May  7 2012 15:02:19+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.217.150 exc
eeds the speed-limit value 5.
#May  7 2012 14:56:55+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
#May  7 2012 14:51:40+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
#May  7 2012 14:46:35+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
#May  7 2012 14:41:06+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.217.62 exce
eds the speed-limit value 5.
#May  7 2012 14:35:54+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
#May  7 2012 14:29:54+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
#May  7 2012 14:24:39+00:00 Huawei SECE/4/ARP_SIP_SPEEDLIMIT_ALARM:OID=1.3.6.1.4
.1.2011.5.25.165.2.2.2.11 The arp packet speed with source ip 10.137.216.1 excee
ds the speed-limit value 5.
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-39 Description of the display trapbuffer command output

Item	Description
Trapping buffer configuration and contents	Whether the device is enabled to output traps to the trap buffer: ● enabled ● disabled To enable the device to output traps to the trap buffer, run the **4.3.33 info-center trapbuffer** command.
Allowed max buffer size	Maximum size of the trap buffer.
Actual buffer size	Actual size of the trap buffer. To set the size of the trap buffer, run the **4.3.34 info-center trapbuffer size** command.
Channel number	Number of the channel used to send traps to the trap buffer. To set the channel number, run the **4.3.15 info-center channel** command.
Channel name	Name of the channel used to send traps to the trap buffer. To set the channel name, run the **4.3.16 info-center channel name** command.
Dropped messages	Number of dropped messages.
Overwritten messages	Number of overwritten messages.
Current messages	Number of current messages.

Related Topics

4.3.4 display info-center
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.33 info-center trapbuffer
4.3.34 info-center trapbuffer size
4.3.37 reset trapbuffer

 Copyright © Huawei Technologies Co., Ltd.

4.3.14 info-center autosave logbuffer

Function

The **info-center autosave logbuffer** command enables the function that automatically saves buffered logs.

The **undo info-center autosave logbuffer** command disables the function that automatically saves buffered logs.

By default, the function that automatically saves buffered logs is disabled.

Format

info-center autosave logbuffer interval *time-interval*

undo info-center autosave logbuffer

Parameters

Parameter	Description	Value
interval *time-interval*	Specifies the interval of automatically saving buffered logs. That is, buffered logs are saved at most one time within this specified interval.	The value is an integer that ranges from 0 to 72, in hours. If the interval is set to 0, buffered logs are automatically saved as long as the log buffer is full.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the path for storing log files is flash: on the switch, the log information generated on the switch is stored to the log buffer before being saved to log files. The buffered logs are saved to the flash memory only when the **save** command is executed to save the current configuration or the **reboot** command is executed to restart the switch. This operation may cause the loss of some logs.

To prevent logs from being lost, run the **info-center autosave logbuffer** command to enable the function that automatically saves buffered logs. When the log buffer is full, buffered logs are automatically saved to the flash memory.

To prevent buffered logs from being frequently written to the flash memory, set the interval for automatically saving buffered logs so that buffered logs are saved at most one time within this interval.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- The function that automatically saves buffered logs will write information to the flash memory. Excessive writes to the flash memory can reduce the life of the flash. Therefore, you are advised to disable this function if it is not required.
- The flash space is limited, so the switch does not automatically save buffered logs when the remaining flash space is less than 15 MB.
- The function that automatically saves buffered logs applies only when the default path for storing log files is flash: or the **info-center logfile path** command has been executed to set the path for storing log files to flash:. When log files are stored in the SD card or hard disk, this function does not take effect.

Example

Enable the function that automatically saves buffered logs and set the interval to 24 hours.

```
<Huawei> system-view
[Huawei] info-center autosave logbuffer interval 24
```

4.3.15 info-center channel

Function

The **info-center channel** command configures channels for outputting information in various directions.

The **undo info-center channel** command restores the default settings.

By default, the system outputs information in various directions through channels listed in the table below.

Table 4-40 Default association between the channel number, channel name, and output direction of information channels

Channel Number	Channel Name	Output Direction
0	console	Console
1	monitor	User terminal
2	loghost	Log host
3	trapbuffer	Trap buffer
4	logbuffer	Log buffer
5	snmpagent	SNMP agent
6	channel6	Unspecified
7	channel7	Unspecified
8	channel8	Unspecified

 Copyright © Huawei Technologies Co., Ltd.

Channel Number	Channel Name	Output Direction
9	channel9	Log file

Format

info-center { **console** | **logbuffer** | **logfile** | **monitor** | **snmp** | **trapbuffer** } **channel** { *channel-number* | *channel-name* }

undo info-center { **console** | **logbuffer** | **logfile** | **monitor** | **snmp** | **trapbuffer** } **channel**

Parameters

Parameter	Description	Value
console	Specifies the channel used to output information to the console.	-
logbuffer	Specifies the channel used to output information to the log buffer.	-
logfile	Specifies the channel used to output information to the log file.	-
monitor	Specifies the channel used to output information to the user terminal.	-
snmp	Specifies the channel used to output information to the SNMP agent.	-
trapbuffer	Specifies the channel used to output information to the trap buffer.	-
channel-number	Specifies the channel number.	The value is an integer ranging from 0 to 9.
channel-name	Specifies the name of a channel, which can be the default channel name or a user-defined name.	The value is a string of 1 to 30 case-sensitive characters. The value consists of letters or numbers and must start with a letter.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **info-center channel** command in the following scenarios: The same information is sent to different directions. For example, the log file and log host record the same content or the trap buffer and the SNMP agent record the same content.

NOTE

For details on how to configure a channel for outputting information to a log host, see **4.3.23 info-center loghost**.

Example

Configure the channel used to output information to a console.

```
<Huawei> system-view
[Huawei] info-center console channel console
```

Configure the channel used to output information to the log buffer.

```
<Huawei> system-view
[Huawei] info-center logbuffer channel logbuffer
```

Configure the channel used to output information to the log file.

```
<Huawei> system-view
[Huawei] info-center logfile channel 9
```

Configure the channel used to output information to the user terminal.

```
<Huawei> system-view
[Huawei] info-center monitor channel monitor
```

Configure the channel used to output information to an SNMP agent.

```
<Huawei> system-view
[Huawei] info-center snmp channel 5
```

Configure the channel used to output information to the trap buffer.

```
<Huawei> system-view
[Huawei] info-center trapbuffer channel trapbuffer
```

Related Topics

4.3.2 display channel
4.3.4 display info-center
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.19 info-center logbuffer
4.3.23 info-center loghost
4.3.30 info-center source channel
4.3.33 info-center trapbuffer

 Copyright © Huawei Technologies Co., Ltd.

4.3.16 info-center channel name

Function

The **info-center channel name** command names a channel with a specified number.

The **undo info-center channel** command restores the default channel name.

The following lists default channel names.

Table 4-41 Default channel names

Channel Number	Default Channel Name
0	console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent
6	channel6
7	channel7
8	channel8
9	channel9

Format

info-center channel *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

Parameters

Parameter	Description	Value
channel-number	Specifies the number of a channel.	The value is an integer than ranges from 0 to 9. That is, the system has 10 channels.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-sensitive characters. The value consists of letters or numbers and must start with a letter.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can rename channels, which facilitates memorization and usage.

Precautions

Channel names must be unique. It is recommended that channel names represent channel functions.

Example

Name channel 0 execconsole.

```
<Huawei> system-view
[Huawei] info-center channel 0 name execconsole
```

Related Topics

4.3.2 display channel
4.3.4 display info-center

4.3.17 info-center enable

Function

The **info-center enable** command enables the information center.

The **undo info-center enable** command disables the information center.

By default, the information center is enabled.

Format

info-center enable

undo info-center enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During device running, the information center records device operation. The system outputs system information to destinations such as the log host and the console only after the information center is enabled. Network administrators can store and query output information to monitor device running and locate faults.

Precautions

After the **undo info-center enable** command is executed, logs, traps, and debugging messages are not recorded. The log about running the **undo info-center enable** command is not recorded.

Follow-up Procedure

Configure a rule for outputting information to the terminal or remote server.

Example

Enable the information center.

```
<Huawei> system-view
[Huawei] info-center enable
Info: Information center is enabled.
```

Related Topics

4.3.4 display info-center
4.3.11 display logbuffer
4.3.12 display logfile
4.3.13 display trapbuffer
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.19 info-center logbuffer
4.3.30 info-center source channel
4.3.33 info-center trapbuffer

4.3.18 info-center filter-id

Function

The **info-center filter-id** command configures the Router to filter a specified log or trap.

The **undo info-center filter-id** command disables the Router from filtering a specified log or trap.

By default, no log or trap is filtered.

 Copyright © Huawei Technologies Co., Ltd.

Format

info-center filter-id { *id* | **bymodule-alias** *modname alias* } * &<1-50>

undo info-center filter-id { **all** | { *id* | **bymodule-alias** *modname alias* } * &<1-50> }

Parameters

Parameter	Description	Value
id	Specifies the ID of the log or trap to be filtered. **NOTE** The ID is the log or trap ID defined by the system.	The value is an integer that ranges from 0 to 4294967295.
bymodule-alias *modname alias*	Specifies the module name and alias name corresponding to the log or trap to be filtered.	The value is an enumerated value and must be set as prompted by the device.
all	Filters all logs or traps.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If some logs or traps are unnecessary, configure the Router not to output the logs and traps. When the filtering function is enabled, the information center does not send the traps with a specified ID that satisfy the filtering condition to any channel. As a result, the trap buffer, log file, console, terminal, or SNMP agent cannot receive the traps with the specified ID.

An ID filter list is the aggregation of the shielded IDs and is arranged in a specified order.

Precautions

- To add multiple IDs at a time, use a space to separate IDs. The result of each ID is displayed.
- Currently, the Router can filter traps with a maximum of 50 IDs. If there are more than 50 log IDs, the system displays a message indicating that the filtering table is full. To configure the filtering function, run the **undo info-center filter-id** { **all** | { *id* | **bymodule-alias** *modname alias* } * &<1-50> } command to delete original IDs and reconfigure the log ID.

- You cannot add the same ID or alias name repeatedly.
- When you add an unregistered or nonexistent ID or alias name, the system displays a message indicating that the system fails to filter the trap with the specified ID or alias name.

Example

Filter the log with the ID of 1098731530.

```
<Huawei> system-view
[Huawei] info-center filter-id 1098731530
Info: Succeeded in appending log ID 1098731530.
```

Filter information by module names and alias names.

```
<Huawei> system-view
[Huawei] info-center filter-id bymodule-alias CMD CLKCHGREBOOTCANCELED
Info: Succeeded in appending log ID 3225948163.
```

Cancel filtering for all logs.

```
<Huawei> system-view
[Huawei] undo info-center filter-id all
Info: Succeeded in deleting all IDs.
```

Related Topics

4.3.17 info-center enable

4.3.5 display info-center filter-id

4.3.19 info-center logbuffer

Function

The **info-center logbuffer** command enables the Router to send logs to the log buffer.

The **undo info-center logbuffer** command disables the Router from sending logs to the log buffer.

By default, the Router is enabled to send logs to the log buffer.

Format

info-center logbuffer

undo info-center logbuffer

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To view logs in the log buffer, run the **info-center logbuffer** command to enable the Router to send logs to the log buffer.

Example

Enable the Router to send logs to the log buffer.

```
<Huawei> system-view
[Huawei] info-center logbuffer
```

Related Topics

4.3.4 display info-center
4.3.11 display logbuffer
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.20 info-center logbuffer size
4.3.36 reset logbuffer

4.3.20 info-center logbuffer size

Function

The **info-center logbuffer size** command sets the maximum number of logs in the log buffer.

The **undo info-center logbuffer size** command restores the default maximum number of logs in the log buffer.

By default, a log buffer can store a maximum of 512 logs.

Format

info-center logbuffer size *logbuffer-size* [**channel** { *channel-number* | *channel-name* }]

undo info-center logbuffer size

Parameters

Parameter	Description	Value
logbuffer-size	Specifies the maximum number of logs in the log buffer.	The value is an integer that ranges from 0 to 1024. If *logbuffer-size* is 0, logs are not displayed.
channel-number	Specifies the channel number.	The value is an integer ranging from 0 to 9.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
channel-name	Specifies the name of a channel, which can be the default channel name or a user-defined name.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of logs in the log buffer reaches the maximum value, new logs will replace the existing logs that were placed earlier in the log buffer until all the new logs are stored. Logs are cleared only when the Router is restarted.

Precautions

When you run the **info-center logbuffer size** command multiple times, only the latest configuration takes effect.

Example

Set the maximum number of logs in the log buffer to 50.

```
<Huawei> system-view
[Huawei] info-center logbuffer size 50
```

Related Topics

4.3.4 display info-center
4.3.11 display logbuffer
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.19 info-center logbuffer
4.3.36 reset logbuffer

4.3.21 info-center logfile path

Function

The **info-center logfile path** command configures the path where log files are saved.

The **undo info-center logfile path** command cancels the path where log files are saved that are configured.

Format

info-center logfile path *path*

undo info-center logfile path

Parameters

Parameter	Description	Value
path	Specifies the path where log files are saved, which is in the format of storage medium name:/logfile, for example, usb0:/logfile.	Select the path according to device configuration. By default, The system selects a storage medium in descending order of priority: rom, hdd0, hdd1, hdd2, hdd3, sd0, sd1, usb0, usb1, and flash.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **info-center logfile path** command to set the path where log files are saved. Then log files are saved into the path and the file name is **log.log**. To view logs generated by the Router, run the **save logfile** command to save logs into a specified file or configure the Router to export information into a specified log file. Then run the **display logfile** command to view the log file.

Prerequisites

The information center has been enabled by using the **4.3.17 info-center enable** command.

Example

Configure the USB flash drive as the path where log files will be saved.

```
<Huawei> system-view
[Huawei] info-center logfile path usb0:/logfile
```

Related Topics

4.3.4 display info-center

4.3.6 display info-center logfile path
4.3.12 display logfile
4.3.22 info-center logfile size
4.3.38 save logfile

4.3.22 info-center logfile size

Function

The **info-center logfile size** command sets the log file size.

The **undo info-center logfile size** command restores the default log file size.

By default, the log file size is 8 MB.

Format

info-center logfile size *size*

undo info-center logfile size

Parameters

Parameter	Description	Value
size	Specifies the log file size.	The value is an integer that is 4, 8, 16, or 32, in MB. The default value is 8 MB.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the Router to export information to a log file, run the **info-center logfile size** command to set the log file size.

Precautions

If you configure the device to export information to a log file, exported information is saved in the **log.log** file. When the **log.log** file exceeds the specified size, the system compresses the file in to a zip package. When the storage space on the Router is smaller than 100 MB, the information center deletes the earliest log file.

Example

Set the log file size to 32 MB.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] info-center logfile size 32
```

Related Topics

4.3.4 display info-center

4.3.6 display info-center logfile path

4.3.12 display logfile

4.3.21 info-center logfile path

4.3.38 save logfile

4.3.23 info-center loghost

Function

The **info-center loghost** command configures the device to output information to a log host.

The **undo info-center loghost** command disables the device from outputting information to a log host.

By default, no information is output to the log host.

Format

info-center loghost *ip-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | **transport** { **udp** | **tcp ssl-policy** *policy-name* } | { **vpn-instance** *vpn-instance-name* | **public-net** } | **local-time** | **port** *port-id*] *

info-center loghost ipv6 *ipv6-address* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** *language-name* | **transport** { **udp** | **tcp ssl-policy** *policy-name* } | **local-time** | **port** *port-id*] *

undo info-center loghost *ip-address* [**vpn-instance** *vpn-instance-name*]

undo info-center loghost ipv6 *ipv6-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the log host.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
channel { *channel-number* | *channel-name* }	Specifies the channel used to send information to a log host. • *channel-number*: specifies the number of a channel. • *channel-name*: specifies the name of a channel. The name can be the default or user-defined channel name.	The value of *channel-number* is an integer that ranges from 0 to 9. The value of *channel-name* is a string of 1 to 30 case-sensitive characters. The value consists of letters or numbers and must start with a letter.
facility *local-number*	Specifies a syslog server facility that is used to identify the log information source. You can use this parameter to plan a local value for the log information of a specified device, so that the syslog server can handle received log information based on the parameter.	The value ranges from local0 to local7. The default value is local7.
language *language-name*	Displays the language in which logs are recorded.	Enumerated type. Currently, the value can only be English.
transport	Indicates the information transport mode.	-
udp	Indicates the UDP transport mode.	-
tcp	Indicates the TCP transport mode.	-
ssl-policy *policy-name*	Specifies a Secure Sockets Layer (SSL) policy in the TCP transport mode. This parameter is recommended to improve log transmission security.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain any space or question mark (?).
vpn-instance *vpn-instance-name*	VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
public-net	Indicates that the log host is connected in the public network.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
local-time	Indicates the local time when logs are sent to the log host.	By default, the system sends logs to the log host at the Coordinated Universal Time (UTC).
ipv6 *ipv6-address*	Specifies the IPv6 address of the log host.	The value is a 32-digit hexadecimal number.
port *port-id*	Specifies the IPv4 port of the log host.	The value is an integer that ranges from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To query information generated on the Router deployed remotely, configure the Router to export information to a log host so that you can view device information on the log host. Run the **info-center loghost** command to configure the Router to export information to a log host.

To configure the Router to output information to different log hosts using different channels, specify the channels used to send information to the log hosts. For example, you can configure the Router to output information to log hosts at 192.168.0.1 and 192.168.0.2 using channels 7 and 8 respectively.

Precautions

The Router can output information to eight log hosts including IPv4 and IPv6 hosts to implement backup among log hosts.

To transfer logs to the log hosts using TCP and encrypt logs using SSL, create an SSL policy first.

If the **set net-manager vpn-instance** command is run to configure the NMS to manage network elements through a VPN instance, either of the following situations occurs.

- If **vpn-instance** is configured, the system accesses the log host in the VPN instance.
- If **public-net** is configured, the system accesses the log host on the public network.

Example

Configure a device to use channel 16 to output information to the log host with the IPv4 address 10.1.1.1 and port at 6514.

```
<Huawei> system-view
[Huawei] info-center loghost 10.1.1.1 port 6514 channel channel6
```

Configure the Router to send information to the log host with the IPv6 address FC00:0:0:3001::1.

```
<Huawei> system-view
[Huawei] info-center loghost ipv6 fc00:0:0:3001::1
```

Configure the Router to send information to the host with the IPv4 address 192.168.2.2 and VPN instance name **vpn1**.

```
<Huawei> system-view
[Huawei] info-center loghost 192.168.2.2 vpn-instance vpn1
```

Configure a device to send information to the log host with the IPv4 address 192.168.2.2 in TCP mode, using the SSL policy **huawei123** that has been created in the system.

```
<Huawei> system-view
[Huawei] info-center loghost 192.168.2.2 transport tcp ssl-policy huawei123
```

Related Topics

4.3.4 display info-center
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.24 info-center loghost source

4.3.24 info-center loghost source

Function

The **info-center loghost source** command configures the source interface used by the Router to send information to a log host.

The **undo info-center loghost source** command restores the default source interface used by the Router to send information to a log host.

By default, the source interface for a device to send logs to a log host is the actual interface that sends the logs.

Format

info-center loghost source *interface-type interface-number*

undo info-center loghost source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple devices send log messages to the same log host, you can identify the devices by setting different source interfaces so as to index the received log messages.

The source interface specified in the **info-center loghost source** command for a device to send logs to a log host is not necessarily the actual interface that sends the logs, but the IP address of the specified source interface is carried in logs.

Prerequisites

There is a reachable route between the source interface and the log host.

Precautions

If you need to change the source interface configuration on the device, you must run the **undo info-center loghost** *ip-address* command and then reconfigure it.

Example

Specify Loopback0 IP address as the source interface address to send information to a log host.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.1.1.1 255.255.255.0
[Huawei-LoopBack0] quit
[Huawei] info-center loghost source loopback 0
```

Related Topics

4.3.4 display info-center

4.3.15 info-center channel

4.3.16 info-center channel name

4.3.17 info-center enable

4.3.23 info-center loghost

4.3.25 info-center max-logfile-number

Function

The **info-center max-logfile-number** command sets the maximum number of log files to be saved.

The **undo info-center max-logfile-number** command restores the default maximum number of log files to be saved.

By default, a maximum of 200 log files can be saved.

Format

info-center max-logfile-number *filenumbers*

undo info-center max-logfile-number

Parameters

Parameter	Description	Value
filenumbers	Specifies the maximum number of log files that can be saved.	The value is an integer that ranges from 2 to 500.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If too many log files are saved on the Router, many disk space resources are occupied. To view log files generated recently, run the **info-center max-logfile-number** command to set the maximum number of log files that can be saved.

Precautions

If the number of log files generated on the Router exceeds the limit, the system deletes the oldest log file so that the number of log files is not larger than the maximum value.

NOTICE

If the number of saved log files is greater than the default value, more system resources are consumed. The default value is recommended. Excess log files can be deleted manually or automatically. When the system deletes excess log files, high CPU usage may last for a short period.

Example

Set the maximum number of log files to be saved to 100.

```
<Huawei> system-view
[Huawei] info-center max-logfile-number 100
```

Related Topics

4.3.4 display info-center
4.3.21 info-center logfile path
4.3.22 info-center logfile size
4.3.12 display logfile
4.3.21 info-center logfile path
4.3.38 save logfile

4.3.26 info-center rate-limit except

Function

The **info-center rate-limit except** command cancels the log processing rate limit for logs.

The **undo info-center rate-limit except** command deletes the preceding configuration.

Format

info-center rate-limit except { **byinfoid** *infoID* | **bymodule-alias** *modname alias* }

undo info-center rate-limit except { **byinfoid** *infoID* | **bymodule-alias** *modname alias* }

Parameters

Parameter	Description	Value
byinfoid *infoID*	Specifies the log ID in hexadecimal notation.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to ffffffff.
bymodule-alias *modname*	Specifies the log module name.	The value is a string of 1 to 24 case-insensitive characters without spaces.
alias	Specifies the log mnemonic name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

When too many logs will never be generated under a specified ID, you can run the **info-center rate-limit except** command to avoid the impact of the suppression of

 Copyright © Huawei Technologies Co., Ltd.

the log processing rate. After this command is run, the configured log processing rate limit will not be effective for logs with the specified ID or module name.

Example

Prevent logs specified by the module name and mnemonic from being suppressed by the information center.

```
<Huawei> system-view
[Huawei] info-center rate-limit except bymodule-alias AAA AUTHEN_ERR_EVENT
```

Prevent logs specified by the log ID from being suppressed by the information center.

```
<Huawei> system-view
[Huawei] info-center rate-limit except byinfoid ff5ad009
```

Prevent logs with a specified log ID from being suppressed by the information center.

```
<Huawei> system-view
[Huawei] undo info-center rate-limit except bymodule-alias AAA AUTHEN_ERR_EVENT
```

Related Topics

4.3.8 display info-center rate-limit threshold

4.3.7 display info-center rate-limit record

4.3.27 info-center rate-limit global-threshold

Function

The **info-center rate-limit global-threshold** command sets the total number of logs that the information center can process every second.

The **undo info-center rate-limit global-threshold** command restores the default value.

By default, the information center processes a maximum of 400 logs in every second.

Format

info-center rate-limit global-threshold *value*

undo info-center rate-limit global-threshold

Parameters

Parameter	Description	Value
value	Specifies the maximum number of logs that the information center can process every second.	The value is an integer that ranges from 100 to 1000.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center rate-limit global-threshold** command to adjust the processing capability of the information center. If the number of logs to be processed exceeds the processing capability of the information center, the extra logs are discarded.

NOTE

- If the threshold is too low, some logs may be discarded.
- If the threshold is too high, the information center cannot identify the log ID under which too many logs are generated. The number of logs to be processed depends on the current processing capacity of the information center.

Example

Set the number of logs that the information center can process every second to 300.

```
<Huawei> system-view
[Huawei] info-center rate-limit global-threshold 300
```

Related Topics

4.3.8 display info-center rate-limit threshold

4.3.7 display info-center rate-limit record

4.3.28 info-center rate-limit monitor-period

Function

The **info-center rate-limit monitor-period** command sets the monitoring period for the information center to suppress the log processing rate.

The **undo info-center rate-limit monitor-period** command restores the default value.

By default, the monitoring period is 3 seconds.

Format

info-center rate-limit monitor-period *value*

undo info-center rate-limit monitor-period

Parameters

Parameter	Description	Value
value	Specifies the monitoring period for the information center to suppress the log processing rate.	The value is an integer ranging from 1 to 60, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

In the monitoring period specified by *value*, if the rate of sending a single log every second exceeds the threshold configured using the **info-center rate-limit threshold** command, the information center will limit the log processing rate. In this situation, the information center discards logs exceeding the threshold.

In the monitoring period that is five times *value*, if the number of a single type of logs that are sent every second is smaller than the threshold configured using the **info-center rate-limit threshold** command, the information center does not limit the log processing rate.

Example

Set the monitoring period for the information center to suppress the log processing rate to 5 seconds.

```
<Huawei> system-view
[Huawei] info-center rate-limit monitor-period 5
```

Related Topics

4.3.8 display info-center rate-limit threshold

4.3.7 display info-center rate-limit record

4.3.29 info-center rate-limit threshold

4.3.29 info-center rate-limit threshold

Function

The **info-center rate-limit threshold** command sets the maximum number of logs with the same log ID that the information center can process every second.

The **undo info-center rate-limit threshold** command restores the default setting.

By default, the information center processes a maximum of 30 logs with the same log ID in every second.

Format

info-center rate-limit threshold *value* [**byinfoid** *infoID* | **bymodule-alias** *modname alias*]

undo info-center rate-limit threshold [*value*] [**byinfoid** *infoID* | **bymodule-alias** *modname alias*]

Parameters

Parameter	Description	Value
value	Specifies the maximum number of logs with the same log ID that the information center can process every second.	The value is an integer that ranges from 1 to 500.
byinfoid *infoID*	Specifies the log ID.	The value is a 32-digit hexadecimal number in the format XXXXXXXX. It ranges from 0 to ffffffff.
bymodule-alias *modname*	Specifies the log of the module name.	The value is a string of 1 to 24 case-insensitive characters without spaces.
alias	Specifies the log of the mnemonic name.	The value is a string of 1 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **info-center rate-limit threshold** command to set the maximum number of logs with the same log ID that the information center can process every second. The information center monitors the number of logs that are generated every second under the same log ID. When the number of logs that are generated every second under the same log ID exceeds the threshold in the monitoring period, the information center decides that too many logs are generated and suppresses its log processing rate by processing only the conforming traffic (logs within the threshold) and discarding the non-conforming traffic (logs exceeding the threshold). When the number of logs that are generated every second under the same log ID falls below the threshold and remains below the threshold for five monitoring periods, the information center removes the suppression.

NOTE

If the threshold *value1* specified by the parameter **byinfoid** *infoID* or **bymodule-alias** *modname alias* differs from the threshold *value0* specified globally, *value1* takes effect.

By default, the information center processes a maximum of 30 logs with the same log ID in every second. In certain application scenarios, by default, the information center needs to process more than 50 logs with the same log ID in every second. You can set thresholds for logs with different log IDs.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Generally, the default threshold is recommended.

- If the threshold is too low, some logs may be discarded.
- If the threshold is too high, the information center cannot identify the log ID under which too many logs are generated.

Example

Set the maximum number of logs that the information center can process every second to 60.

```
<Huawei> system-view
[Huawei] info-center rate-limit threshold 60
```

Set the maximum number of logs identified by the same module name and mnemonic that the information center can process every second to 30.

```
<Huawei> system-view
[Huawei] info-center rate-limit threshold 30 bymodule-alias AAA AUTHEN_ERR_EVENT
```

Set the maximum number of logs with the same log ID that the information center can process every second to 20.

```
<Huawei> system-view
[Huawei] info-center rate-limit threshold 20 byinfoid ff5ad009
```

Restore the maximum number of logs that the information center can process every second to the default value.

```
<Huawei> system-view
[Huawei] undo info-center rate-limit threshold
```

Cancel the restriction on the maximum number of logs with a specified log ID that the information center can process every second.

```
<Huawei> system-view
[Huawei] undo info-center rate-limit threshold bymodule-alias AAA AUTHEN_ERR_EVENT
```

Related Topics

4.3.8 display info-center rate-limit threshold
4.3.7 display info-center rate-limit record

4.3.30 info-center source channel

Function

The **info-center source channel** command configures a rule for outputting information to a channel.

The **undo info-center source channel** command restores the default rule for outputting information to a channel.

The following lists the default rule for outputting information to a channel.

Table 4-42 Default rule for outputting information to a channel

Output Channel	Module Enabled to Output Information	Log		Trap		Debugging Message	
		Status	Lowest Output Severity	Status	Lowest Output Severity	Status	Lowest Output Severity
0 (console)	default	on	warning	on	debugging	on	debugging
1 (remote terminal)	default	on	warning	on	debugging	on	debugging
2 (log host)	default	on	debugging	on	debugging	off	debugging
3 (trap buffer)	default	off	informational	on	debugging	off	debugging
4 (log buffer)	default	on	warning	off	debugging	off	debugging
5 (SNMP agent)	default	off	debugging	on	debugging	off	debugging
6 (channel 6)	default	on	debugging	on	debugging	off	debugging
7 (channel 7)	default	on	debugging	on	debugging	off	debugging
8 (channel 8)	default	on	debugging	on	debugging	off	debugging
9 (channel 9)	default	on	debugging	on	debugging	off	debugging

Format

info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**log** { **state** { **off** | **on** } | **level** *severity* } * | **trap** { **state** { **off** | **on** } | **level** *severity* } * | **debug** { **state** { **off** | **on** } | **level** *severity* } *] *

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

Parameters

Parameter	Description	Value
module-name	Specifies the module name.	Enumerated type. The value depends on the registered module.
default	Indicates the default module.	-
channel-number	Specifies the number of a channel.	The value is an integer that ranges from 0 to 9.
channel-name	Specifies the name of a channel.	The value is a string of 1 to 30 case-sensitive characters. The value consists of letters or numbers and must start with a letter.
log { **state** { **off** | **on** } }	Specifies the log status. ● **off**: Logs are not sent. ● **on**: Logs are sent. **NOTE** This field does not take effect for diagnostic logs.	-
log { **level** *severity* }	Specifies the lowest severity of output logs. **NOTE** This field does not take effect for diagnostic logs.	Logs are classified into eight severities. The following severities are listed in descending order of priority: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging
trap { **state** { **off** | **on** } }	Specifies the trap status: ● **off**: Traps are not sent. ● **on**: Traps are sent.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
trap { **level** *severity* }	Specifies the lowest severity of output traps.	Logs are classified into eight severities. The following severities are listed in descending order of priority: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging
debug { **state** { **off** | **on** } }	Specifies the debugging message status. ● **off**: Debugging messages are not sent. ● **on**: Debugging messages are sent.	-
debug { **level** *severity* }	Specifies the lowest severity of output debugging messages.	Logs are classified into eight severities. The following severities are listed in descending order of priority: ● emergencies ● alert ● critical ● error ● warning ● notification ● informational ● debugging

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect and query information generated on the Router, define severities for various type of information that is output to different channels. You can run the **info-center source channel** command to configure a rule for outputting information to a channel.

The following lists information severities.

Table 4-43 Information severities

Value	Severity	Description
0	emergencies	A fault causes the device to fail to run normally unless it is restarted. For example, the device is restarted because of program exceptions or a memory error is detected.
1	alert	A fault needs to be rectified immediately. For example, memory usage of the system reaches the upper limit.
2	critical	A fault needs to be analyzed and processed. For example, the memory usage falls below the lower threshold; temperature falls below the alarm threshold; BFD detects that a device is unreachable or detects locally generated error messages.
3	error	An improper operation is performed or exceptions occur during service processing. The fault does not affect services but needs to be analyzed. For example, users enter incorrect commands or passwords; error protocol packets are received from other devices.
4	warning	Some events or operations may affect device running or cause service processing faults, which requires full attention. For example, a routing process is disabled; BFD detects packet loss; error protocol packets are detected.
5	notification	A key operation is performed to keep the device running normally. For example, the **shutdown** command is run; a neighbor is discovered; protocol status changes.
6	informationa l	A normal operation is performed. For example, a **display** command is run.
7	debugging	A normal operation is performed, which requires no attention.

Precautions

Each information channel has a default record with the module name **default**. The default configuration for logs, traps, and debugging messages in different channels may differ.

If a module generates a large number of logs, traps, or debugging messages in a short time, use the following methods to suppress this information:

- Specify **level** *severity* to adjust the channel level. Information with lower severity will be filtered.
- Specify **state off** to disable information sent by a specified module.

NOTICE

After the lowest severity of output information is specified, information lower than the severity will be filtered.

Example

Configure the device to send logs higher than or equal to warning of the CFM module.

```
<Huawei> system-view
[Huawei] info-center source CFM channel snmpagent log level warning
```

Related Topics

4.3.2 display channel
4.3.4 display info-center
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.19 info-center logbuffer
4.3.23 info-center loghost
4.3.33 info-center trapbuffer
4.3.39 terminal debugging
4.3.40 terminal logging
4.3.41 terminal monitor
4.3.42 terminal trapping

4.3.31 info-center statistic-suppress enable

Function

The **info-center statistic-suppress enable** command enables suppression of statistics about consecutive repeated logs.

The **undo info-center statistic-suppress enable** command disables suppression of statistics about consecutive repeated logs.

By default, suppression of statistics about consecutive repeated logs is enabled.

Format

info-center statistic-suppress enable

 Copyright © Huawei Technologies Co., Ltd.

undo info-center statistic-suppress enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A large number of repeated logs are generated in a short time in some scenarios, for example, when ARP and VRRP are enabled and an ARP attack or route link failure occurs. This wastes both the storage space and CPU resources. Generally, users do not want to view the repeated logs. You can run the **info-center statistic-suppress enable** command to suppress statistics on consecutive repeated logs so that the system can still record other logs.

NOTE

Logs that are generated consecutively and with the identical log ID and parameters can be regarded as repeatedly generated logs.

Precautions

Statistics about repeatedly generated logs are first output at the 30th seconds from the time the first log is output, and then statistics about repeatedly generated logs are output at the 120th seconds. After being output two times, statistics about repeatedly generated logs are output every 600 seconds.

Example

Disable suppression of statistics about consecutive repeated logs.

```
<Huawei> system-view
[Huawei] undo info-center statistic-suppress enable
```

4.3.32 info-center timestamp

Function

The **info-center timestamp** command sets the timestamp format of logs, traps, and debugging messages.

The **undo info-center timestamp** command restores the default timestamp format of logs, traps, and debugging messages.

By default, the timestamp format of logs, traps, and debugging messages is **date**. Debugging information is accurate to milliseconds, and alarm and log information is accurate to seconds.

Format

info-center timestamp debugging { { **date** | **short-date** | **format-date** } [**precision-time** { **tenth-second** | **second** }] | **boot** | **none**}

info-center timestamp log { { **date** | **short-date** | **format-date** } [**precision-time** { **tenth-second** | **millisecond** }] | **boot** | **none**}

info-center timestamp trap { { **date** | **short-date** | **format-date** } [**precision-time** { **tenth-second** | **millisecond** }] | **boot** | **none**}

undo info-center timestamp { **debugging** | **trap** | **log** }

Parameters

Parameter	Description	Value
debugging	Indicates debugging messages.	-
log	Indicates logs.	-
trap	Indicates traps.	-
boot	Indicates that the timestamp is expressed in the format of relative time, a period of time since the start of the system. The format is xxxxxx.yyyyyy. xxxxxx is the higher order 32 bits of the milliseconds elapsed since the start of the system; yyyyyy is the lower order 32 bits of the milliseconds elapsed since the start of the system.	-
none	Indicates that no timestamp information is specified.	-
date	Specifies the current date and time. It is expressed in mm dd yyyy hh:mm:ss format.	-
short-date	Indicates the short date. This timestamp differs from **date** is that the year is not displayed.	-
format-date	Indicates that the timestamp is expressed in YYYY-MM-DD hh:mm:ss format.	-
precision-time	Specifies the precision.	-
second	Indicates that the precision is accurate to seconds.	-
tenth-second	Indicates that the precision is accurate to 0.1 second.	-
millisecond	Indicates that the precision is accurate to milliseconds.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **info-center timestamp** command sets the timestamp format of logs, traps, and debugging messages.

The following describes the timestamp in **date** format.

Table 4-44 Description of fields of the timestamp in **date** format

Field	Description	Value
mm	Month	The value can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
dd	Date	1-31. If the date is smaller than 10, add a space in front of the date, For example, " 7".
yyyy	Year	4 digits
hh:mm:ss	Local time	hh ranges from 00 to 23, and mm or ss ranges from 00 to 59.

When the precision of the timestamp is accurate to 0.1 second or milliseconds, the system adds identifies to the logs generated at the same time based on the sequence.

Prerequisites

The information center has been enabled by using the **4.3.17 info-center enable** command.

Example

Set the timestamp format of traps to **boot**.

```
<Huawei> system-view
[Huawei] info-center timestamp trap boot
```

Set the timestamp precision of logs, traps, and debugging messages.

```
<Huawei> system-view
[Huawei] info-center timestamp log date precision-time millisecond
[Huawei] info-center timestamp debugging date precision-time tenth-second
[Huawei] info-center timestamp trap date precision-time millisecond
```

Related Topics

4.3.4 display info-center

4.3.33 info-center trapbuffer

Function

The **info-center trapbuffer** command enables the Router to send traps to the trap buffer.

The **undo info-center trapbuffer** command disables the Router from sending traps to the trap buffer.

By default, the Router is enabled to send traps to the trap buffer.

Format

info-center trapbuffer

undo info-center trapbuffer

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To view traps in the trap buffer, run the **info-center trapbuffer** command to enable the Router to send traps to the trap buffer.

Example

Enable the Router to send traps to the trap buffer.

```
<Huawei> system-view
[Huawei] info-center trapbuffer
```

Related Topics

4.3.4 display info-center
4.3.13 display trapbuffer
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.34 info-center trapbuffer size
4.3.37 reset trapbuffer

4.3.34 info-center trapbuffer size

Function

The **info-center trapbuffer size** command sets the maximum number of traps in the trap buffer.

The **undo info-center trapbuffer size** command restores the default maximum number of traps in the trap buffer.

By default, a trap buffer allows a maximum of 256 traps.

Format

info-center trapbuffer size *trapbuffer-size* [**channel** { *channel-number* | *channel-name* }]

undo info-center trapbuffer size

Parameters

Parameter	Description	Value
trapbuffer-size	Specifies the maximum number of traps in the trap buffer.	The value is an integer that ranges from 0 to 1024. If *trapbuffer-size* is 0, traps are not displayed.
channel-number	Specifies the channel number.	The value is an integer ranging from 0 to 9.
channel-name	Specifies the name of a channel, which can be the default channel name or a user-defined name.	The value is a string of 1 to 30 case-insensitive characters. The value consists of letters or numbers and must start with a letter.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **info-center trapbuffer size** command sets the maximum number of traps in the trap buffer.

Prerequisites

The Router has been enabled to output traps to the trap buffer by using the **4.3.33 info-center trapbuffer** command.

Precautions

When you run the **info-center trapbuffer size** command multiple times, only the latest configuration takes effect.

If a small value of *trapbuffer-size* is used, some traps may be not displayed. If a large value of *trapbuffer-size* is used, repeated traps may be displayed. The default value of *trapbuffer-size* is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum number of traps in the trap buffer to 30.

```
<Huawei> system-view
[Huawei] info-center trapbuffer size 30
```

Related Topics

4.3.4 display info-center
4.3.13 display trapbuffer
4.3.15 info-center channel
4.3.16 info-center channel name
4.3.17 info-center enable
4.3.33 info-center trapbuffer
4.3.37 reset trapbuffer

4.3.35 reset info-center statistics

Function

The **reset info-center statistics** command clears statistics on each module.

Format

reset info-center statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To recollect statistics on each module, run the **reset info-center statistics** command to clear all historical statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when you run the **reset info-center statistics** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics on each module.

```
<Huawei> reset info-center statistics
```

Related Topics

4.3.4 display info-center
4.3.9 display info-center statistics

4.3.36 reset logbuffer

Function

The **reset logbuffer** command clears logs in the log buffer.

Format

reset logbuffer

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To record logs in the log buffer again, run the **reset logbuffer** command to clear all the information in the log buffer.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the **reset logbuffer** command.

Example

Clear information in the log buffer.

```
<Huawei> reset logbuffer
Warning: This command will reset the log buffer. Logs in the buffer will be lost
. Continue? (y/n)[n]:y
```

Related Topics

4.3.11 display logbuffer

4.3.37 reset trapbuffer

Function

The **reset trapbuffer** command clears Trap information in the trap buffer.

Format

reset trapbuffer

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To record traps in the trap buffer again, run the **reset trapbuffer** command to clear all the information in the trap buffer.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the **reset trapbuffer** command.

Example

Clear information in the trap buffer.

```
<Huawei> reset trapbuffer
```

Related Topics

4.3.13 display trapbuffer

4.3.38 save logfile

Function

The **save logfile** command saves logs in the log file buffer to a log file.

Format

save logfile

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To reduce the number of times information is written into the storage device, information generated on the Router is saved into the log buffer before the information is saved into the log file. When the log file buffer is full, the system saves the logs in the log file buffer to the log file. You can also run the **save logfile** command to save the logs in the log file buffer to the log file. After the log file is generated, the system clears logs in the log file buffer to save new logs.

Prerequisites

The path to save log files has been set by using the **4.3.21 info-center logfile path** command.

Example

Save logs in the log file buffer to the log file.

```
<Huawei> save logfile
Info: It may take several seconds,please wait...
Save log file successfully.
```

Related Topics

4.3.4 display info-center

4.3.21 info-center logfile path

4.3.22 info-center logfile size

4.3.12 display logfile

4.3.21 info-center logfile path

4.3.25 info-center max-logfile-number

4.3.39 terminal debugging

Function

The **terminal debugging** command enables debugging message display on the user terminal.

The **undo terminal debugging** command disables debugging message display on the user terminal.

 Copyright © Huawei Technologies Co., Ltd.

By default, debugging message display is disabled on the user terminal.

Format

terminal debugging

undo terminal debugging

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **terminal debugging** command to enable debugging message display on the user terminal to view system debugging message and locate faults.

Prerequisites

The **4.3.41 terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Precautions

The output debugging information only includes protocol packets sent to hosts, excluding other forwarded packets.

Example

Enable debugging message display on the user terminal.

```
<Huawei> terminal debugging
Info: Current terminal debugging is on.
```

Related Topics

4.3.17 info-center enable

4.3.30 info-center source channel

4.3.41 terminal monitor

4.3.40 terminal logging

Function

The **terminal logging** command enables log display on the user terminal.

The **undo terminal logging** command disables log display on the user terminal.

By default, log display is enabled on the user terminal.

Format

terminal logging

undo terminal logging

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view logs on a terminal, run the **terminal logging** command to enable log display on the user terminal.

Prerequisites

The **4.3.41 terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Disable log display on the user terminal.

```
<Huawei> undo terminal logging
Info: Current terminal logging is off.
```

Related Topics

4.3.17 info-center enable

4.3.30 info-center source channel

4.3.41 terminal monitor

4.3.41 terminal monitor

Function

The **terminal monitor** command enables display of logs, traps, and debugging message output by the information center on the user terminal.

The **undo terminal monitor** command disables display of logs, traps, and debugging message output by the information center on the user terminal.

 Copyright © Huawei Technologies Co., Ltd.

By default, console display is enabled and terminal display is disabled.

Format

terminal monitor

undo terminal monitor

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Prerequisites

The information center has been enabled by using the **4.3.17 info-center enable** command.

Follow-up Procedure

Run the **terminal debugging**/**undo terminal debugging**, **terminal logging**/**undo terminal logging**, **terminal trapping**/**undo terminal trapping** command to enable or disable terminal debugging message, log, or trap display.

Precautions

Logs, traps, and debugging message are sent to the current terminal only when the **terminal monitor** command is used.

Running the **undo terminal monitor** command is equivalent to running the **undo terminal debugging**, **undo terminal logging**, **undo terminal trapping** command.

Example

Disable display of logs, traps, and debugging message output by the information center on the user terminal.

```
<Huawei> undo terminal monitor
Info: Current terminal monitor is off.
```

Related Topics

4.3.17 info-center enable

4.3.30 info-center source channel

4.3.39 terminal debugging

4.3.40 terminal logging

 Copyright © Huawei Technologies Co., Ltd.

4.3.42 terminal trapping

4.3.42 terminal trapping

Function

The **terminal trapping** command enables trap display on the user terminal.

The **undo terminal trapping** command disables trap display on the user terminal.

By default, trap display is enabled on the user terminal.

Format

terminal trapping

undo terminal trapping

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view traps on a terminal, run the **terminal trapping** command to enable trap display on the user terminal.

Prerequisites

The **4.3.41 terminal monitor** command has been executed to enable display of logs, traps, and debugging message output on the user terminal.

Example

Disable trap display on the user terminal.

```
<Huawei> undo terminal trapping
Info: Current terminal trapping is off.
```

Related Topics

4.3.17 info-center enable

4.3.30 info-center source channel

4.3.41 terminal monitor

 Copyright © Huawei Technologies Co., Ltd.

4.4 NTP Configuration Commands

4.4.1 display ntp-service sessions

Function

The **display ntp-service sessions** command displays all session information maintained by NTP on the local end.

Format

display ntp-service sessions [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about an NTP session. If **verbose** is not specified, only summary information about the NTP session is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display ntp-service sessions** command. If the **verbose** option is not specified, only summary information about a session is displayed.

Example

Display NTP session information of the local device.

```
<Huawei> display ntp-service sessions
 clock source: 127.127.1.0
 clock stratum: 1
 clock status:configured, insane, invalid
 reference clock ID: LOCAL(0)
 reach: 377
 poll: 64
 now: 2
 offset: 0.0000 ms
 delay: 0.00 ms
 disper: 0.94 ms
```

Table 4-45 Description of the display ntp-service sessions command output

Item	Description
clock source	Address of the clock source.
clock stratum	Stratum of the clock source. The clock stratum determines the precision of the clock, and its value ranges from 1 to 16. The higher the stratum value, the lower the clock precision. The value 1 indicates the highest precision, and the value 16 indicates the lowest precision. The clock with stratum16 is in the unsynchronized status, and cannot be used as a reference clock.
clock status	Status of a clock, where ● configured: indicates that the session is set up by a configuration command. ● master: indicates that the clock source corresponding to the session is the primary clock source of the current system. ● selected: indicates that the clock source corresponding to the session passes the clock selecting algorithm. ● candidate: indicates that the clock source corresponding to the session is a candidate clock source. ● sane: indicates that the clock source corresponding to the session passes the saneness test. ● insane: indicates that the clock source corresponding to the session does not pass the saneness test. ● valid: indicates that the clock source corresponding to the session is valid. The clock source corresponding to the session passes the test, is in a synchronized status and is of an effective stratum. The root delay and the root dispersion are within the normal range. ● invalid: indicates that the clock source corresponding to the session is invalid. ● unsynced: indicates that the clock source corresponding to the session is not yet synchronized or the stratum is invalid.
reference clock ID	When the local system has been synchronized to a remote NTP server or a clock source, the address of the remote server or the identifier of the clock source is displayed.
reach	Reachability count of the clock source. The value 0 indicates that the clock source is unreachable.
poll	Poll interval of NTP packets. The interval for sending two successive NTP packets, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
now	Interval between the last synchronization and the current time.
offset	Offset to the superior clock source.
delay	Delay to the superior clock source.
disper	Dispersion to the superior clock source.

Display detailed information about NTP sessions on the local device.

```
<Huawei> display ntp-service sessions verbose
 clock source: 127.127.1.0
 clock stratum: 1
 clock status:configured, master, sane, valid
 reference clock ID: LOCAL(0)
 local mode: client, local poll: 6
 peer mode: server, peer poll: 6
 offset: 0.0000 ms,delay: 0.00 ms,  disper: 0.88 ms
 root delay: 0.00 ms, root disper: 10.00 ms
 reach: 37, sync dist: 0.011, sync state: 3
 precision: 2^18, version: 3, peer interface: InLoopBack0
 reftime: 16:46:51.054 UTC Jul 28 2012(D3BE95FB.0DFB3FA6)
 orgtime: 16:46:51.054 UTC Jul 28 2012(D3BE95FB.0DFB3FA6)
 rcvtime: 16:46:51.054 UTC Jul 28 2012(D3BE95FB.0DFBF833)
 xmttime: 16:46:51.054 UTC Jul 28 2012(D3BE95FB.0DFADAFD)
 filter delay :  0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 filter offset:  0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 filter disper:  0.00   0.00   0.00   0.00   0.00   0.00   0.00   0.00
 reference clock status: working abnormally
 timecode:
```

Table 4-46 Description of the display ntp-service sessions verbose command output

Item	Description
clock source	Address of the clock source.
clock stratum	NTP stratum on which the local system is located.

Item	Description
clock status	Status of a clock, where ● configured: indicates that the session is set up by a configuration command. ● master: indicates that the clock source corresponding to the session is the primary clock source of the current system. ● selected: indicates that the clock source corresponding to the session passes the clock selecting algorithm. ● candidate: indicates that the clock source corresponding to the session is a candidate clock source. ● sane: indicates that the clock source corresponding to the session passes the saneness test. ● insane: indicates that the clock source corresponding to the session does not pass the saneness test. ● valid: indicates that the clock source corresponding to the session is valid. The clock source corresponding to the session passes the test, is in a synchronized status and is of an effective stratum. The root delay and the root dispersion are within the normal range. ● invalid: indicates that the clock source corresponding to the session is invalid. ● unsynced: indicates that the clock source corresponding to the session is not yet synchronized or the stratum is invalid.
reference clock ID	When the local system has been synchronized to a remote NTP server or a clock source, the address of the remote server or the identifier of the clock source is displayed. When the server is located on a certain VPN, the name of the VPN instance is displayed.
local mode	Local system mode.
peer mode	Peer system mode.
local poll	Local polling mode.
peer poll	Peer polling mode.
offset	Offset to the superior clock source.
delay	Delay to the superior clock source.
disper	Dispersion to the superior clock source.
root delay	Total system delay between the local end and the master reference clock. The default value is 0.
root disper	System dispersion of the local end to the master reference clock. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
reach	Reachability mark, indicating the reachability to the clock source.
sync dist	Synchronization distance to the superior clock source. This parameter evaluates and describes the clock source, and NTP chooses the clock source with the shortest synchronization distance.
sync state	Synchronization state: ● 0: The clock has never been synchronized. ● 1: Frequency information is obtained from configuration information. ● 2: The clock is set. ● 3: The clock is set, but the frequency is not yet determined. ● 4: The clock is synchronized. ● 5: An error is found.
precision	Precision of a peer clock.
version	NTP version.
peer interface	Peer interface.
reftime	Reference timestamp.
orgtime	Time when an NTP packet is sent for the last time.
rcvtime	Time when an NTP packet is received for the last time.
xmttime	Time when an NTP packet is forwarded for the last time.
filter delay	Filter delays of the 8 packets received for the last time.
filter offset	Filter offsets of the 8 packets received for the last time.
filter disper	Filter dispersions of the 8 packets received for the last time.
reference clock status	The status of the reference clock, including: ● working normally: normal status. ● working abnormally: abnormal status.
timecode	Indicates the time code.

Related Topics

4.4.23 ntp-service unicast-peer
4.4.24 ntp-service unicast-server
4.4.8 ntp-service broadcast-client
4.4.9 ntp-service broadcast-server

4.4.18 ntp-service multicast-client
4.4.19 ntp-service multicast-server

4.4.2 display ntp-service status

Function

The **display ntp-service status** command displays the status of NTP.

Format

display ntp-service status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Based on the displayed status of the NTP service, you can know the synchronization status and stratum of the local system clock.

Example

Display the status of the NTP service.

```
<Huawei> display ntp-service status
clock status: synchronized
clock stratum: 2
reference clock ID: LOCAL(0)
nominal frequency: 60.0002 Hz
actual frequency: 60.0002 Hz
clock precision: 2^18
clock offset: 0.0000 ms
root delay: 0.00 ms
root dispersion: 0.00 ms
peer dispersion: 10.00 ms
reference time: 15:51:36.259 UTC Apr 25 2012(C6179088.426490A3)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-47 Description of the display ntp-service status command output

Item	Description
clock status	Status of the clock: ● synchronized: indicates that the local system clock is synchronized with an NTP server or a reference clock. ● unsynchronized: indicates that the local system clock is not synchronized with any NTP server.
clock stratum	Stratum of the local system clock.
reference clock ID	Reference clock: ● If the local system clock has been synchronized with a remote NTP server or a reference clock, this field displays the IP address of the remote NTP server or the identifier of the reference clock. ● If the local system clock functions as a reference clock, this field displays "Local". ● If clock status is unsynchronized, this field displays "None".
nominal frequency	Nominal frequency of the local system clock.
actual frequency	Actual frequency of the local system clock.
clock precision	Precision of the local system clock.
clock offset	Offset between the local system clock and the NTP server.
root delay	Total delay between the local system clock and the master reference clock.
root dispersion	Total dispersion between the local system clock and the master reference clock.
peer dispersion	Dispersion between the local system clock and the remote NTP peer.
reference time	Reference timestamp.

4.4.3 display ntp-service trace

Function

The **display ntp-service trace** command displays the system to trace the path of reference clock source from the local device.

Format

display ntp-service trace

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display ntp-service trace** command, summary information of NTP servers for synchronizing time on the link from the local device to the reference clock source can be displayed.

NOTE

The **display ntp-service trace** command does not support an IPv6 clock source.

Example

Display the summary of each passing NTP server when you trace the reference clock source from the local device.

```
<Huawei> display ntp-service trace
server 10.0.0.1,stratum 5, offset 0.024099, synch distance 0.06337
server 172.16.1.1,stratum 4, offset 0.028786, synch distance 0.04575
server 192.168.1.1,stratum 3, offset 0.035199, synch distance 0.03075
server 192.168.20.1,stratum 2, offset 0.039855, synch distance 0.01096
refid 127.127.1.0
```

Table 4-48 Description of the display ntp-service trace command output

Item	Description
server	IP address of the NTP server.
stratum	Stratum of the clock on the NTP server.
offset	Offset to the superior reference clock.
synch distance	Synchronization distance to the superior reference clock. This parameter evaluates and describes the reference clock and NTP chooses the reference clock with the shortest synchronization distance.
refid	Reference clock source.

 Copyright © Huawei Technologies Co., Ltd.

4.4.4 ntp-service access

Function

The **ntp-service access** command sets the access control authority of the local NTP.

The **undo ntp-service access** command cancels the configured access control authority.

By default, no access control authority is set.

Format

ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } { *acl-number* | **ipv6** *acl6-number* } *

undo ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } [**ipv6** | **all**]

undo ntp-service access { **peer** | **query** | **server** | **synchronization** | **limited** } [*acl-number* | **ipv6** *acl6-number*] *

Parameters

Parameter	Description	Value
peer	Indicates maximum access authority. Both time request and control query can be performed on the local NTP service, and the local clock can be synchronized to the remote server.	-
query	Indicates minimum access. Only control query can be performed on the local NTP service.	-
server	Indicates that server access and query are permitted. Both time request and control query can be performed on the local NTP service, but the local clock cannot be synchronized to the remote server.	-
synchronization	Indicates that only server access is permitted. Only time request can be performed on the local NTP service.	-
limited	When the rate of NTP packets exceeds the upper limit, the incoming NTP packets are discarded, and a Kiss code is sent if the KOD function is enabled.	-
acl-number	Indicates the number of a basic ACL with IPv4 address specified.	The value is an integer that ranges from 2000 to 2999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6 *acl6-number*	Indicates the number of an ACL with IPv6 address specified.	The value is an integer that ranges from 2000 to 2999.
all	Indicates all access control authority.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with NTP authentication, **ntp-service access** is simpler to ensure the network security. When an access request reaches the local end, the access request is successively matched with the access authority from the highest one to the lowest one. The first successfully matched access authority takes effect. The matching order is: **peer**, **server**, **synchronization**, **query** and **limited**.

Depending on the access authority to be limited, run the command on different devices accordingly. For details, see the following table.

Table 4-49 Configuration of the NTP access control authority

NTP Operating Mode	Usage Scenario	Device Configured
Unicast NTP server/client mode	The client is restricted from being synchronized to a server, so that the client will not be synchronized to an unreliable unicast NTP server on the network.	Client
Unicast NTP server/client mode	The server is restricted from processing the synchronization time request of the client, so that the synchronization range of the server is controlled.	Server
NTP symmetric peer mode	The two ends are restricted from being synchronized with each other to prevent an unreliable symmetric passive peer on the network from synchronizing the client.	Symmetric active peer

 Copyright © Huawei Technologies Co., Ltd.

NTP Operating Mode	Usage Scenario	Device Configured
NTP symmetric peer mode	The symmetric passive peer is restricted from processing the time request, so that the synchronization range of the symmetric passive peer is controlled.	Symmetric passive peer
NTP multicast mode	The client is restricted from synchronizing to the server to prevent an unreliable multicast NTP server from synchronizing the client.	NTP multicast client
NTP broadcast mode	The client is restricted from being synchronized to a server, so that the client will not be synchronized to an unreliable broadcast NTP server on the network.	NTP broadcast client
NTP manycast client mode	The client is restricted from being synchronized to a server.	NTP manycast client
NTP manycast server mode	The server is restricted from processing the clock synchronization request sent by the client.	NTP manycast server

The **ntp-service access** command ensures the security to the minimal extent. A safer method is to perform identity authentication. See the **ntp-service authentication enable** command for relevant configuration.

Precautions

Check the configuration of the ACL rule before configuring the NTP access control authority in the ACL. When the ACL rule is **permit**, the peer device with the source IP address specified in this rule can access the NTP service on the local device. The access right of the peer device is configured using the **ntp-service access** command. When the ACL rule is **deny**, the peer device with the source IP address specified in this rule cannot access the NTP service on the local device.

Example

Enable the peer matching ACL 2000 to perform time request, query control and time synchronization on the local device.

```
<Huawei> system-view
[Huawei] ntp-service access peer 2000
```

Enable the server matching ACL 2002 to perform time request and query control on the local device.

```
<Huawei> system-view
[Huawei] ntp-service access server 2002
```

Related Topics

4.4.6 ntp-service authentication enable

4.4.5 ntp-service authentication complexity-check disable

Function

The **ntp-service authentication complexity-check disable** command disables NTP authentication key complexity check.

The **undo ntp-service authentication complexity-check disable** command enables NTP authentication key complexity check.

By default, NTP authentication key complexity check is enabled.

Format

ntp-service authentication complexity-check disable

undo ntp-service authentication complexity-check disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An NTP authentication key must meet the following requirements:

- The value is a string of 6-255 (plain text) or 20-392 (cipher text) case-sensitive characters without spaces.
- The community name must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters.
- If a key contains spaces, the key must be included in double quotation marks. A key can only have a pair of double quotation marks.

By default, the device performs complexity check on NTP authentication keys. If the check fails, the passwords cannot be configured. If you do not require this function, disable it. However, disabling this function has security risks.

The versions earlier than V200R006C10 do not support NTP authentication key complexity check. When a device running V200R006C10 or a later version connects to a device running an earlier version, run the **ntp-service authentication complexity-check disable** command to disable NTP authentication key complexity check on the device running V200R006C10 or a

 Copyright © Huawei Technologies Co., Ltd.

later version. If this command is not executed, clock synchronization will fail when the NTP authentication key cannot pass complexity check.

Example

Disable NTP authentication key complexity check.

```
<Huawei> system-view
[Huawei] ntp-service authentication complexity-check disable
```

Related Topics

4.4.7 ntp-service authentication-keyid
4.4.7 ntp-service authentication-keyid

4.4.6 ntp-service authentication enable

Function

The **ntp-service authentication enable** command enables identity authentication for NTP.

The **undo ntp-service authentication enable** command disables the identity authentication.

By default, identity authentication is disabled.

Format

ntp-service authentication enable

undo ntp-service authentication enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On networks requiring high security, authentication must be enabled for NTP. The NTP client authenticates NTP servers using a password and synchronizes time with only the authenticated server. This improves network security.

Example

Enable identity authentication for NTP.

```
<Huawei> system-view
[Huawei] ntp-service authentication enable
```

Related Topics

4.4.7 ntp-service authentication-keyid
4.4.21 ntp-service reliable authentication-keyid

4.4.7 ntp-service authentication-keyid

Function

The **ntp-service authentication-keyid** command sets NTP authentication key.

The **undo ntp-service authentication-keyid** command removes NTP authentication key.

By default, no authentication key is set.

Format

ntp-service authentication-keyid *key-id* **authentication-mode** { **md5** | **hmac-sha256** } [**cipher**] *password*

undo ntp-service authentication-keyid *key-id*

Parameters

Parameter	Description	Value
key-id	Indicates the key number.	Key ID is an integer and ranges from 1 to 4294967295.
authentication-mode md5	Indicates MD5 authentication mode.	-
authentication-mode hmac-sha256	Indicates HMAC-SHA256 authentication mode.	-
cipher	Indicates that the configured password is displayed in cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the authentication password in plain text or in cipher text.	When quotation marks are used around the string, spaces are allowed in the string. The keyword is a string of case sensitive characters without spaces. The string length range is: ● 6 to 255 characters in plain text. ● 48 to 348 characters in cipher text. **NOTE** To improve password security, the password must be a combination of at least two of the following: digits, lowercase letters, uppercase letters, and special characters, and the password length must be equal to or larger than 6. If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each password.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network that requires high security, the NTP authentication must be enabled. You can configure password authentication between client and server, which guarantee the client only to synchronize with server successfully authenticated, and improve network security. If the NTP authentication function is enabled, a reliable key should be configured at the same time. Keys configured on the client and the server must be identical.

NOTE

In NTP symmetric peer mode, the symmetric active peer functions as a client and the symmetric passive peer functions as a server.

Follow-up Procedure

You can configure multiple keys for each device. After the NTP authentication key is configured, you need to set the key to reliable using the **ntp-service reliable authentication-keyid** command. If you do not set the key to reliable, the NTP key does not take effect.

Precautions

Note that MD5 authentication algorithm cannot ensure security. HMAC-SHA256 authentication algorithm is recommended.

You can configure a maximum of 1024 keys for each device.

If the NTP authentication key is a reliable key, it automatically becomes unreliable when you delete the key. You do not need to run the **undo ntp-service reliable authentication-keyid** command.

Example

Set the HMAC-SHA256 identity authentication key. The key ID number is 10, and the key is **Betterkey**.

```
<Huawei> system-view
[Huawei] ntp-service authentication-keyid 10 authentication-mode hmac-sha256 BetterKey
```

Related Topics

4.4.6 ntp-service authentication enable

4.4.21 ntp-service reliable authentication-keyid

4.4.8 ntp-service broadcast-client

Function

The **ntp-service broadcast-client** command configures the device to work in NTP broadcast client mode.

The **undo ntp-service broadcast-client** command removes the device from the NTP broadcast client mode.

By default, the device is not configured in the NTP broadcast client mode.

Format

ntp-service broadcast-client

undo ntp-service broadcast-client

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

On a synchronization subnet, when the IP address of a server or a symmetric peer is not determined, or when the clocks on a large number of devices need to be synchronized on the network, you can implement clock synchronization by configuring the broadcast mode.

On a specified interface on the broadcast client, run the **ntp-service broadcast-client** command to configure an interface on the local device to receive NTP broadcast packets. When the local device automatically runs in the broadcast client mode, the device can receive the synchronization packets sent by a broadcast server. For the configuration of the broadcast server, see the **ntp-service broadcast-server** command.

When the configuration is complete, you can run the **display ntp-service sessions** command to obtain information about sessions between the broadcast server and the local device.

Example

Enable GE1/0/0 to receive NTP broadcast messages.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] ntp-service broadcast-client
```

Related Topics

4.4.9 ntp-service broadcast-server

4.4.9 ntp-service broadcast-server

Function

The **ntp-service broadcast-server** command configures the local device to work in NTP broadcast server mode.

The **undo ntp-service broadcast-server** command removes the device from the NTP broadcast server mode.

By default, the broadcast server mode is not configured.

Format

ntp-service broadcast-server [**version** *number* | **authentication-keyid** *key-id*] *

undo ntp-service broadcast-server

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
version *number*	Indicates the NTP version number. If this parameter is not specified, the version number is a default value.	The value is an integer that ranges from 1 to 4. The default value is 3.
authentication-keyid *key-id*	Indicates the authentication key number used to transmit a message to broadcast clients. If this parameter is not specified, authentication is not performed.	Key ID is an integer and ranges from 1 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

On a synchronization subnet, when the IP address of a server or a symmetric peer is not determined, or when the clocks on a large number of devices need to be synchronized on the network, you can implement clock synchronization by configuring the broadcast mode.

On a specified interface on the broadcast server, run the **ntp-service broadcast-server** command to configure an interface on the local device to send NTP broadcast packets. When the local device automatically runs in the broadcast server mode, the device can send synchronization packets to a broadcast client. For the configuration of the broadcast client, see the **ntp-service broadcast-client** command.

When the configuration is complete, you can run the **display ntp-service sessions** command to obtain information about sessions between the broadcast server and the client.

Example

Enable GE1/0/0 to send NTP broadcast packets, with the NTP version as 2 and the key number as 4.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] ntp-service broadcast-server version 2 authentication-keyid 4
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

4.4.8 ntp-service broadcast-client

4.4.10 ntp-service cwmp unicast-server

Function

The **ntp-service cwmp unicast-server** command configures the NTP server defined by CWMP.

The **undo ntp-service cwmp unicast-server** command deletes the NTP server defined by CWMP.

By default, the NTP server defined by CWMP is not configured.

Format

ntp-service cwmp unicast-server *unicast-server* { **first** | **second** }

undo ntp-service cwmp unicast-server *unicast-server*

Parameters

Parameter	Description	Value
unicast-server	Specifies the IPv4 address or host name of a remote server.	The value is a string of 1 to 32 case-insensitive characters without spaces.
first	Indicates that the current IPv4 address is the first NTP server defined by CWMP.	-
second	Indicates that the current IPv4 address is the second NTP server defined by CWMP.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

CWMP defines the first and second NTP servers. When an router device connects to an ACS by using CWMP, the IP addresses or host names of the first and the second NTP server can be specified using this command to implement time synchronization.

Example

Configure the server with the IP address 10.10.1.1 as the first NTP server.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ntp-service cwmp unicast-server 10.10.1.1 first
```

4.4.11 ntp-service discard

Function

The **ntp-service discard** command sets the minimum inter-packet interval and the average inter-packet interval of NTP.

The **undo ntp-service discard** command cancels the minimum inter-packet interval and the average inter-packet interval of NTP.

By default, the minimum inter-packet interval is set to the first power of 2 in seconds, namely, 2 seconds, and the average inter-packet interval is set to the fifth power of 2 in seconds, namely, 32 seconds.

Format

ntp-service discard { **min-interval** *min-interval-val* | **avg-interval** *avg-interval-val* } *

undo ntp-service discard

Parameters

Parameter	Description	Value
min-interval *min-interval-val*	Specifies the minimum inter-packet interval of NTP. The actual value of the minimum inter-packet interval of NTP is the value obtained by raising 2 to the power of *min-interval-val*, expressed in seconds.	The value of *min-interval-val* is an integer that ranges from 1 to 8.
avg-interval *avg-interval-val*	Specifies the average inter-packet interval of NTP. The actual value of the average inter-packet interval of NTP is the value obtained by raising 2 to the power of *avg-interval-val*, expressed in seconds.	The value of *avg-interval-val* is an integer that ranges from 1 to 8.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The minimum inter-packet interval and the average inter-packet interval of NTP are set using the **ntp-service discard** command. To generate kiss code RATE, we need to set the minimum inter-packet interval and the average inter-packet interval of NTP.

Example

Set both the minimum inter-packet interval and the average inter-packet interval of NTP to the fourth power of 2, expressed in seconds, namely, 16 seconds.

```
<Huawei> system-view
[Huawei] ntp-service discard min-interval 4 avg-interval 4
```

4.4.12 ntp-service enable

Function

The **ntp-service enable** command enables the NTP service function on the local device.

The **undo ntp-service enable** command disables the NTP service function on the local device.

By default, the NTP service function on the local device is enabled.

Format

ntp-service enable

undo ntp-service enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The NTP function can be used on a device only after the NTP service on the device is enabled.

Example

Enable the NTP service on the local device.

```
<Huawei> system-view
[Huawei] ntp-service enable
```

Related Topics

4.4.20 ntp-service refclock-master

4.4.13 ntp-service in-interface disable

Function

The **ntp-service in-interface disable** command disables an interface from receiving NTP packets.

The **undo ntp-service in-interface disable** command enables an interface to receive NTP packets.

By default, an interface is enabled to receive NTP packets.

Format

ntp-service [**ipv6**] **in-interface disable**

undo ntp-service [**ipv6**] **in-interface disable**

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **ntp-service** [**ipv6**] **in-interface disable** command provides a method for access control.

You can disable the interface connected to external devices from receiving NTP packets in either of the following situations:

- An unreliable clock server exists on the interface. By default, all the interfaces can receive NTP packets after NTP is enabled on the device. However, an unreliable clock source makes NTP clock data inaccurate.
- The NTP clock data is modified when the interface is attacked maliciously.

Example

Disable GE1/0/0 from receiving NTP packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ntp-service in-interface disable
```

4.4.14 ntp-service kod-enable

Function

The **ntp-service kod-enable** command enables the KOD function.

The **undo ntp-service kod-enable** command disables the KOD functions.

By default, the KOD function is disabled.

Format

ntp-service kod-enable

undo ntp-service kod-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Kiss-o'-Death (KOD) is a brand new access control technology put forward by NTPv4, and the KOD is mainly used for a server to provide information, such as a status report and access control, for a client. After the KOD function is enabled on the server, the server sends the kiss code DENY or RATE to the client according to the operating status of the system.

When the kiss code is generated in a specific situation, run the **ntp-service kod-enable** command.

Follow-up Procedure

After the KOD function is enabled on the server, you can run the **ntp-service access limited** command to enable control on the rate of incoming NTP packets. When the rate of incoming NTP packets reaches the upper threshold, the server sends the kiss code.

Example

Enable the KOD function.

```
<Huawei> system-view
[Huawei] ntp-service kod-enable
```

4.4.15 ntp-service manycast-client

Function

The **ntp-service manycast-client** command configures the NTP manycast client mode.

The **undo ntp-service manycast-client** command cancels the NTP manycast client mode.

By default, the NTP manycast client mode is disabled.

Format

ntp-service manycast-client [*ip-address* | **ipv6** [*ipv6-address*]] [**authentication-keyid** *key-id* | **ttl** *ttl-number*] *

undo ntp-service manycast-client [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a manycast IPv4 address, which is a class D address.	The default IPv4 address is 224.0.1.1.
ipv6 [*ipv6-address*]	Specifies a manycast IPv6 address.	The default IPv6 address is FF0E::0101.
authentication-keyid *key-id*	Specifies the ID of the authentication key used for sending packets to a manycast server.	The value ranges from 1 to 4294967295.
ttl *ttl-number*	Specifies the TTL value of a manycast packet.	The value is an integer ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The local device runs in the manycast client mode, and periodically sends manycast packets to manycast servers. After the local device receives the reply packet sent by a manycast server, the local device establishes dynamic C/S

 Copyright © Huawei Technologies Co., Ltd.

association with the server. The initial value of the automated key ranges from 65537 to 4294967295.

NOTE

In the configuration of the manycast client, if the server address is not specified, 224.0.1.1 or FF0E::0101 is adopted as the server address by default.

Example

Configure interface GE1/0/0 to receive NTP manycast packets. Assign the manycast address FF0E::111 to the manycast IPv6 packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ntp-service manycast-client ipv6 FF0E::111 authentication-keyid 6
```

Related Topics

4.4.19 ntp-service multicast-server

4.4.16 ntp-service manycast-server

Function

The **ntp-service manycast-server** command configures the NTP manycast server mode.

The **undo ntp-service manycast-server** command cancels the NTP manycast server mode.

By default, the NTP manycast server mode is not configured.

Format

ntp-service manycast-server [*ip-address* | **ipv6** [*ipv6-address*]]

undo ntp-service manycast-server [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a manycast IPv4 address, which is a class D address.	The default IPv4 address is 224.0.1.1.
ipv6 [*ipv6-address*]	Specifies a manycast IPv6 address.	The default IPv6 address is FF0E::0101.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The manycast server responds to the manycast packets sent by the client. After the manycast client receives the reply packet, the manycast client establishes temporary association with the server and enters C/S mode.

Precautions

If the manycast IP address is not specified when the **undo ntp-service manycast-server** command is run, the local device searches for the default IP address. In IPv4 networks, the default IP address of the manycast server is 224.0.1.1. In IPv6 networks, the default IP address of the manycast server is FF0E::0101. If the local device finds the default IP address, the **undo ntp-service manycast-server** command takes effect; otherwise, the **undo ntp-service manycast-server** does not take effect.

Example

Configure interface GE1/0/0 as an interface of the server. The interface is used for responding to the manycast client request from a manycast address.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ntp-service manycast-server ipv6 FF0E::111
```

Related Topics

4.4.15 ntp-service manycast-client

4.4.17 ntp-service max-dynamic-sessions

Function

The **ntp-service max-dynamic-sessions** command sets the maximum dynamic NTP sessions that can be set up.

The **undo ntp-service max-dynamic-sessions** command restores the maximum dynamic NTP sessions to the default value.

By default, up to 100 NTP dynamic sessions are allowed to be set up.

Format

ntp-service max-dynamic-sessions *number*

undo ntp-service max-dynamic-sessions

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Indicates the number of dynamic sessions allowed to be set up.	The number of dynamic NTP sessions is an integer that ranges from 0 to 100. The default value is 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A maximum of 128 sessions can be established on the same device running the NTP service in the same period, including static and dynamic sessions. In both unicast server/client mode and symmetric peer mode, command lines are used to establish static sessions. The dynamic sessions are established in broadcast mode, manycast mode, or multicast mode.

Excessive dynamic sessions directly affect the establishment of static sessions. A user can limit the number of local dynamic sessions solve this problem.

Precautions

When the number of local dynamic sessions on the device is limited,

- NTP dynamic sessions established are not affected. That is, when the number of the dynamic sessions exceeds the limit, the dynamic sessions established are not deleted, but a new dynamic session cannot be established.
- The limit on the number of local dynamic sessions allowed should be configured on the client because the server does not record the number of the established NTP sessions.

Example

Set the maximum NTP dynamic sessions allowed to be set up to 50.

```
<Huawei> system-view
[Huawei] ntp-service max-dynamic-sessions 50
```

4.4.18 ntp-service multicast-client

Function

The **ntp-service multicast-client** command configures the local device to work in NTP multicast client mode.

The **undo ntp-service multicast-client** command cancels the NTP multicast client mode.

By default, the NTP multicast client mode is not configured.

Format

ntp-service multicast-client [*ip-address* | **ipv6** [*ipv6-address*]]

undo ntp-service multicast-client [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Indicates the multicast IP address.	The default IP address is 224.0.1.1.
ipv6 [*ipv6-address*]	Indicates the multicast IPv6 address.	The default IPv6 address is FF0E::0101.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform clock synchronization in multicast mode, you can use the **ntp-service multicast-client** command to specify the current interface on the local device to receive NTP multicast packets. The local device runs in the multicast client mode.

If the valid multicast server is configured, the local device gets synchronized with the multicast server. The local device time is updated with the time of the server.

Follow-up Procedure

When the configuration is complete, run the **display ntp-service sessions** command to obtain session information about the multicast server and the local device.

NOTE

You can configure more than one multicast client with different multicast IP address on the same interface. When multiple multicast clients are configured, the device selects the optimal clock source by selecting a preferred clock.

You can configure a maximum of 1024 multicast clients on the local device, but a maximum of 128 multicast clients can work simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE1/0/0 to receive NTP multicast packets. The multicast address of the multicast packets is 224.0.1.2.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] ntp-service multicast-client 224.0.1.2
```

Related Topics

4.4.19 ntp-service multicast-server

4.4.1 display ntp-service sessions

4.4.19 ntp-service multicast-server

Function

The **ntp-service multicast-server** command specifies an interface on the local device to send NTP multicast packets. The local device runs in the multicast server mode.

The **undo ntp-service multicast-server** command cancels the NTP multicast server mode.

By default, the multicast server mode is not configured.

Format

ntp-service multicast-server [*ip-address*] [**version** *number* | **authentication-keyid** *key-id* | **ttl** *ttl-number*] *

ntp-service multicast-server [**ipv6** [*ipv6-address*]] [**authentication-keyid** *key-id* | **ttl** *ttl-number*] *

undo ntp-service multicast-server [*ip-address* | **ipv6** [*ipv6-address*]]

Parameters

Parameter	Description	Value
ip-address	Indicates the multicast IP address.	The default address is 224.0.1.1.
ipv6 [*ipv6-address*]	Indicates the multicast IPv6 address.	The default IPv6 address is FF0E::0101.
version *number*	Indicates the NTP version number. If this parameter is not specified, the version number is a default value.	The value is an integer that ranges from 1 to 4. The default value is 3.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
authentication-keyid *key-id*	Indicates the authentication key ID used when sending messages to the multicast clients. If this parameter is not specified, authentication is not performed.	The key ID is an integer that ranges from 1 to 4294967295.
ttl *ttl-number*	Indicates the life span of the multicast packet. If this parameter is not specified, the life span of the multicast packet is a default value.	The ttl number is an integer that ranges from 1 to 255. The default value is 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform clock synchronization in the multicast mode, run the **ntp-service multicast-server** command to specify the current interface on the local device to send NTP multicast packets. The local device runs in the multicast server mode, and functions as the multicast server to periodically send multicast packets to the multicast client.

Follow-up Procedure

When the configuration is complete, run the **display ntp-service sessions** command to obtain session information about the multicast server and the local device.

NOTE

You can configure a maximum of 128 multicast servers on the local device.

Example

Configure GE1/0/0 to send NTP multicast packets. The multicast IPv4 address is 224.0.1.1, the authentication key ID is 4 and the NTP version number is 3.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
```

```
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] ntp-service multicast-server 224.0.1.1 authentication-keyid 4 version 3
```

Related Topics

4.4.18 ntp-service multicast-client
4.4.1 display ntp-service sessions

4.4.20 ntp-service refclock-master

Function

The **ntp-service refclock-master** command sets the local clock to be the NTP primary clock that provides the synchronizing time for other devices.

The **undo ntp-service refclock-master** command cancels the configuration of the NTP primary clock.

By default, no NTP primary clock is specified.

Format

ntp-service refclock-master [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the local reference clock. When no IP address is assigned, the local clock whose IP address is 127.127.1.0 is set as the default NTP primary clock.	The value of *ip-address* is 127.127.1.u, and **u** ranges from 0 to 3, which represents the number of the selected local clock.
stratum	Specifies the stratum of the NTP primary clock. If this parameter is not specified, the stratum is a default value.	The value of the stratum is an integer that ranges from 1 to 15. The default value is 8. Timer is accurate if the stratum value is small.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local clock is the clock of the device itself. Run the **ntp-service refclock-master** command to set the local clock as the NTP primary clock that provides the synchronization time for other devices.

In NTP, the time synchronization in an NTP synchronization subnet is performed from a smaller level to a larger level, that is, from the 1st level to the 15th level. An authoritative clock is used as a reference time source for the synchronization subnet, and is located at the top of the synchronization subnet. The authoritative clock is stratum0. The current authoritative clock is mostly a Radio Clock or the Global Positioning System. The time of the authoritative clock is synchronized through the broadcast UTC time code other than NTP.

Precautions

A device on the network can perform clock synchronization in the following manners.

- Synchronizing with the local clock: The local clock is used as the reference clock.
- Synchronizing with another device on the network: This device is used as an NTP clock server to provide a reference clock for the local end.

If both manners are configured, the device selects an optimal clock source through selecting a preferred clock. That is, clocks determined in the two manners are compared to determine which clock is a lower stratum. The clock of a lower stratum is the preferred clock source.

The RTC precision of AR200, AR1220, AR2220, and AR3260 is low. You are not advised to configure these routers as NTP master clocks.

Example

Set the local clock to be the NTP primary clock, the stratum of which set to 3.

```
<Huawei> system-view
[Huawei] ntp-service refclock-master 3
```

4.4.21 ntp-service reliable authentication-keyid

Function

The **ntp-service reliable authentication-keyid** command specifies the authentication key to be reliable.

The **undo ntp-service reliable authentication-keyid** command cancels the current setting.

By default, no authentication key is specified to be reliable.

Format

ntp-service reliable authentication-keyid *key-id*

undo ntp-service reliable authentication-keyid *key-id*

Parameters

Parameter	Description	Value
key-id	Indicates the key number.	Key ID is an integer and ranges from 1 to 4294967295.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the identity authentication is enabled, this command is used to specify that one or more keys are reliable. That is, the client can only be synchronized with the server that provides the reliable key. The client cannot be synchronized with the server that provides unreliable keys.

Example

Enable the identity authentication in NTP and adopt the hmac-sha256 encryption mode with key number as 37 and the key as BetterKey. Specify the key to be reliable.

```
<Huawei> system-view
[Huawei] ntp-service authentication enable
[Huawei] ntp-service authentication-keyid 37 authentication-mode hmac-sha256 BetterKey
[Huawei] ntp-service reliable authentication-keyid 37
```

Related Topics

4.4.6 ntp-service authentication enable

4.4.7 ntp-service authentication-keyid

4.4.22 ntp-service source-interface

Function

The **ntp-service source-interface** command specifies the local source interface that sends NTP packets.

The **undo ntp-service source-interface** command cancels the current setting.

By default, the local source interface is not specified for sending NTP packets. The local source interface is automatically determined based on the route.

Format

ntp-service [**ipv6**] **source-interface** { *interface-type interface-number* | *interface-name* } [**vpn-instance** *vpn-instance-name*]

 Copyright © Huawei Technologies Co., Ltd.

undo ntp-service [**ipv6**] **source-interface** { *interface-type interface-number* | *interface-name* } [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6	Indicates that the network type of the local source interface is IPv6.	-
interface-type interface-number	Indicates the local interface type that sends the NTP packets.	-
interface-name	Indicates the local interface name that sends the NTP packets.	-
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configure the local source interface for sending/receiving NTP packets, so that the IP address of another interface on the device cannot be used as the destination address of a reply packet, which is convenient for a user to subsequently deploy a flow control policy. If the interface is not specified, the source IP address of the NTP packets is selected according to the route.

Precautions

For broadcast, multicast, and manycast modes, NTP service is implemented on the specified interface, and this interface is the source interface. Therefore, the **ntp-service source-interface** command is invalid for broadcast, multicast, and manycast modes.

Example

Specify GE1/0/0 as the source interface to send all the NTP packets.

```
<Huawei> system-view
[Huawei] ntp-service source-interface gigabitethernet 1/0/0
```

4.4.23 ntp-service unicast-peer

Function

The **ntp-service unicast-peer** command configures NTP peer mode.

The **undo ntp-service unicast-peer** command cancels the NTP peer mode.

By default, the NTP peer mode is not configured.

Format

ntp-service unicast-peer *server* [**version** *number* | **authentication-keyid** *key-id* | **maxpoll** *max-number* | **minpoll** *min-number* | **source-interface** { *interface-type interface-number* | *interface-name* } | **vpn-instance** *vpn-instance-name* | **preference**] *

ntp-service unicast-peer ipv6 *ipv6-address* [**authentication-keyid** *key-id* | **maxpoll** *max-number* | **minpoll** *min-number* | **source-interface** { *interface-type interface-number* | *interface-name* } | **vpn-instance** *vpn-instance-name* | **preference**] *

undo ntp-service unicast-peer { *server* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
server	Indicates the IPv4 address or domain name of the remote server.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation. **NOTE** If the IPv4 address and domain name are the same, only the command output of the domain name is displayed.
ipv6 *ipv6-address*	Indicates the IPv6 address of the remote server.	The value of *ipv6-address* is a unicast address, and cannot be the IPv6 address of the reference clock.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
version *number*	Indicates the NTP version number. If this parameter is not specified, the default version number is used.	The version number is an integer that ranges from 1 to 4. By default, it is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when transmitting messages to the remote peer. If this parameter is not specified, authentication is not performed.	The key ID is an integer that ranges from 1 to 4294967295.
maxpoll *max-number*	Indicates the maximum NTP poll interval.	The value is an integer that ranges from 10 to 17. The actual value of the maximum NTP poll interval is the value obtained by raising 2 to the power of max-number, expressed in seconds.
minpoll *min-number*	Indicates the minimum NTP poll interval.	The value is an integer that ranges from 3 to 6. The actual value of the minimum NTP poll interval is the value obtained by raising 2 to the power of min-number, expressed in seconds.
source-interface *interface-type interface-number* | *interface-name*	Indicates the source interface from which the symmetric active end sends NTP packets to the symmetric passive end. The source IP address of the NTP packets is the IP address of this interface.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preference	Indicates the remote peer as the preferred one. By default, the remote peer is not preferred. **NOTE** Generally, clocks are filtered based on the synchronization distance and dispersion. The clock is preferentially selected from the list of candidate clocks after filtering.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the clock of a device on the network needs to be synchronized in symmetric peer mode, you can run the **ntp-service unicast-peer** command to configure a remote node as the symmetric peer of the device. The local device runs in symmetric active peer mode. In this mode, the device and the remote peer can synchronize clock with each other.

Precautions

A maximum of 128 peers can be configured for the local device. The optimal symmetric peer is selected as the synchronization source.

When you run the **undo ntp-service unicast-peer** command with a specified **vpn-instance** *vpn-instance-name*, the configuration of the NTP symmetric passive peer with the IP address *server* on the VPN is canceled. If **vpn-instance** *vpn-instance-name* is not specified, the configuration of the NTP symmetric passive peer with the IP address *server* on the public network.

If the same server is specified in at least 2 commands that are run in sequence to configure the symmetric peer mode, during the configuration restoration, the last run command takes effect. For example, the **ntp-service unicast-peer 10.10.1.1 source-interface gigabitethernet 1/0/0** command and the **ntp-peer unicast-peer 10.10.1.1** command are run in sequence. During the configuration restoration, only the **ntp-service unicast-peer 10.10.1.1** command takes effect.

Example

Configure the peer 10.10.1.1 to provide the synchronizing time for the local device. The local device can also provide synchronizing time for the peer. The version number is 3. The IP address of the NTP packets is the address of GE1/0/0.

```
<Huawei> system-view
[Huawei] ntp-service unicast-peer 10.10.1.1 version 3 source-interface gigabitethernet 1/0/0
```

4.4.24 ntp-service unicast-server

Function

The **ntp-service unicast-server** command configures the NTP server mode.

The **undo ntp-service unicast-server** command cancels the NTP server mode.

By default, the NTP server mode is not configured.

Format

ntp-service unicast-server *server* [**version** *number* | **authentication-keyid** *key-id* | **maxpoll** *max-number* | **minpoll** *min-number* | **source-interface** { *interface-type interface-number* | *interface-name* } | **vpn-instance** *vpn-instance-name* | **preference**] *

ntp-service unicast-server ipv6 *ipv6-address* [**authentication-keyid** *key-id* | **maxpoll** *max-number* | **minpoll** *min-number* | **source-interface** { *interface-type interface-number* | *interface-name* } | **vpn-instance** *vpn-instance-name* | **preference**] *

undo ntp-service unicast-server { *server* | **ipv6** *ipv6-address* } [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
server	Indicates the IPv4 address or domain name of the remote server.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation. **NOTE** If the IPv4 address and domain name are the same, only the command output of the domain name is displayed.
ipv6 *ipv6-address*	Indicates the IPv6 address of the remote server.	The value of *ipv6-address* must be an IP address of a host, but cannot be a broadcast address, multicast address, or reference clock's IP address.

Parameter	Description	Value
version *number*	Indicates the NTP version number. If this parameter is not specified, the default version number is used.	The version number is an integer that ranges from 1 to 4. By default, the version number is 3.
authentication-keyid *key-id*	Indicates the authentication key ID used when messages are transmitted to the remote server. If this parameter is not specified, authentication is not performed.	The key ID is an integer that ranges from 1 to 4294967295.
maxpoll *max-number*	Indicates the maximum NTP poll interval. The NTP poll interval of the system floats between the minimum value and maximum value.	It is an integer ranging from 7 to 17, the actual value of the maximum NTP poll interval is the value obtained by raising 2 to the power of max-number, expressed in seconds. The default value is 7 seconds in NTPv1, NTPv2, NTPv3, and NTPv4.
minpoll *min-number*	Indicates the minimum NTP poll interval. The NTP poll interval of the system floats between the minimum value and maximum value.	It is an integer ranging from 3 to 6, the actual value of the minimum NTP poll interval is the value obtained by raising 2 to the power of min-number, expressed in seconds. The default value is 6 seconds.
source-interface *interface-type interface-number* | *interface-name*	Indicates the source interface from which the unicast client sends NTP packets to the unicast server. The source IP address of the NTP packets is the IP address of this interface.	-
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preference	Indicates the remote server as the preferred one. By default, the remote server is not preferred. **NOTE** Generally, clocks are filtered based on the synchronization distance and dispersion. The clock is preferentially selected from the list of candidate clocks after filtering.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the clock of a device on the network needs to be synchronized in unicast server/client mode, the command can be run, and the remote server specified by *server* is used as the local clock server. The local device runs in client mode. In this mode, the local client can be synchronized to the remote server, but the remote server cannot be synchronized to the local client.

If the client is enabled with the authentication function and configured with the corresponding authentication key, the server sends NTP packets with authentication to the client after receiving the synchronization request of the client. The received packets are authenticated by the client. After the authentication succeeds, the clock is synchronized. If the client is not enabled with the authentication function, the server sends NTP packets without authentication to the client after receiving the synchronization request of the client. The clock is synchronized after the client receives the packets.

Precautions

A maximum of 128 servers can be configured for the local device. The optimal symmetric peer is selected as the synchronization source.

If you need to delete a VPN instance, you must check whether the VPN instance is bound to the NTP server to ensure that the configuration can meet the requirements.

When the **undo ntp-service unicast-server** command is run, if the parameter **vpn-instance** *vpn-instance-name* is specified, cancel the configuration of the NTP server with the IP address *server* in the VPN. If the parameter **vpn-instance** *vpn-instance-name* is not specified, cancel the configuration of the NTP server with the IP address *server* in the public network.

 Copyright © Huawei Technologies Co., Ltd.

If the same server is specified in at least 2 commands that are run in sequence to configure the NTP server mode, during the configuration restoration, the last run command takes effect. For example, the **ntp-service unicast-server 10.10.1.1 source-interface gigabitethernet 1/0/0** command and the **ntp-service unicast-server 10.10.1.1** command are run in sequence. During the configuration restoration, only the **ntp-service unicast-server 10.10.1.1** command takes effect.

Example

Configure the server 10.10.1.1 to provide the synchronizing time for the local device. The NTP version number is 3.

```
<Huawei> system-view
[Huawei] ntp-service unicast-server 10.10.1.1 version 3
```

Configure the server 10.10.1.1 with VPN instance "abc" to provide the synchronizing time for the local device.

```
<Huawei> system-view
[Huawei] ntp-service unicast-server 10.10.1.1 vpn-instance abc
```

4.5 Fault Management Commands

4.5.1 alarm (system view)

Function

Using the **alarm** command, you can enter the alarm view.

Format

alarm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **alarm** command to enter the alarm view, you can configuration alarm management functions.

Example

Enter the alarm view.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm]
```

Related Topics

4.5.2 alarm correlation-suppress enable
4.5.3 alarm-name severity
4.5.4 clear alarm active
4.5.6 correlation-analyze enable
4.5.7 delay-suppression enable
4.5.14 mask interface
4.5.16 suppression alarm-name

4.5.2 alarm correlation-suppress enable

Function

The **alarm correlation-suppress enable** command enables NMS-based alarm correlation suppression.

The **undo alarm correlation-suppress enable** command disables NMS-based alarm correlation suppression.

By default, NMS-based alarm correlation suppression is enabled.

Format

alarm correlation-suppress enable target-host *ip-address* **securityname** *securityname* [**vpn-instance** *vpn-instance-name*]

alarm correlation-suppress enable target-host ipv6 *ipv6-address* **securityname** *securityname*

undo alarm correlation-suppress enable target-host *ip-address* **securityname** *securityname* [**vpn-instance** *vpn-instance-name*]

undo alarm correlation-suppress enable target-host ipv6 *ipv6-address* **securityname** *securityname*

Parameters

Parameter	Description	Value
target-host *ip-address*	Specifies the IPv4 address of an NMS host.	The value is in dotted decimal notation.
target-host ipv6 *ipv6-address*	Specifies the IPv6 address of an NMS host.	The value is a 32-digit hexadecimal number.
securityname *securityname*	Specifies the security name displayed on the NMS host.	The value is a string of 1 to 56 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 255 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A lot of alarms are generated and then reported on a running system. If non-root-cause alarms are unimportant, you can enable NMS-based alarm correlation suppression to filter out non-root-cause alarms.

Prerequisites

The alarm correlation analysis has been enabled using the **4.5.6 correlation-analyze enable** command.

Example

Enable the alarm correlation suppression of the NMS host whose security name is user123 and IP address is 192.168.3.1.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm] correlation-analyze enable
Info: Enable analyze correlation between alarms successfully
[Huawei-alarm] quit
[Huawei] alarm correlation-suppress enable target-host 192.168.3.1 securityname user123
```

Related Topics

4.5.1 alarm (system view)

4.5.6 correlation-analyze enable

4.5.3 alarm-name severity

Function

The **alarm-name severity** command sets the severity for an alarm.

The **undo alarm-name severity** command restores the default setting.

By default, each alarm has a default severity.

 Copyright © Huawei Technologies Co., Ltd.

Format

alarm-name *alarm-name* **severity** *severity*

undo alarm-name *alarm-name* **severity**

Parameters

Parameter	Description	Value
alarm-name	Specifies the registered alarm name.	The value is of enumerated type and varies according to the registered device type. To view registered alarm information, run the **4.5.10 display alarm information** command.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
severity *severity*	Specifies the alarm severity.	The value is of enumerated type. Alarms are classified into the following severities: ● **critical**: indicates that a fault affecting services has occurred and it must be rectified immediately. ● **major**: indicates that services are being affected and related measures need to be taken urgently. ● **minor**: indicates that a fault occurs but does not affect services. To avoid more serious faults that affect services, related measures must be taken. ● **warning**: indicates that a potential or impending service-affecting fault is detected before any significant effect has been felt. Take corrective actions to diagnose and rectify the fault. ● **indeterminate**: indicates that the alarm severity cannot be determined. ● **cleared**: indicates one or more previous alarm conditions have been cleared.

Views

Alarm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **alarm-name severity** command to change the alarm severity. However, the level of a clear alarm cannot be changed unless during the configuration restoration period. You can configure filtering conditions to allow the NMS to receive only alarms of specified alarm severity.

Precautions

The default severity of each alarm is different. To view the default severity of an alarm, run the **undo alarm-name severity** and **4.5.10 display alarm information** commands in sequence.

Example

Set the severity of the hwSysSlaveHDError alarm to warning.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm] alarm-name hwSysSlaveHDError severity warning
```

Related Topics

4.5.1 alarm (system view)
4.5.10 display alarm information

4.5.4 clear alarm active

Function

The **clear alarm active** command clears active alarms.

Format

clear alarm active { **all** | **sequence-number** *sequence-number* }

Parameters

Parameter	Description	Value
all	Clears all active alarms.	-
sequence-number *sequence-number*	Specifies the sequence number of an active alarm.	The value is an integer ranging from 1 to 2147483647.

Views

Alarm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting statistics on alarms generated on the device again, run the **clear alarm active** to clear active alarms.

Precautions

After the **clear alarm active** command is used, all active alarms on the device are deleted and cannot be restored.

Example

Clear all active alarms on the device.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm] clear alarm active all
```

Related Topics

4.5.1 alarm (system view)

4.5.8 display alarm active

4.5.5 clear event all

Function

The **clear event all** command clears events on the device.

Format

clear event all

Parameters

None

Views

Event view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting statistics on events generated on the device again, run the **clear event all** to clear events.

NOTICE

The **clear event all** command clears events on the device and cleared events cannot be restored.

Example

Clear events on the device.

```
<Huawei> system-view
[Huawei] event
[Huawei-event] clear event all
```

Related Topics

4.5.13 event

4.5.6 correlation-analyze enable

Function

The **correlation-analyze enable** command enables alarm correlation analysis.

The **undo correlation-analyze enable** command disables alarm correlation analysis.

By default, alarm correlation analysis is disabled.

Format

correlation-analyze enable

undo correlation-analyze enable

Parameters

None

Views

Alarm view

Default Level

2: Configuration level

Usage Guidelines

A lot of alarms are generated in a running system and reported to the NMS. If non-root-cause alarms are unimportant, you can run the **correlation-analyze enable** command to enable alarm correlation analysis to distinguish between root-cause alarms and non-root-cause alarms. After alarm correlation analysis is enabled, the system analyzes types of alarms. For a non-root-cause alarm, the

system marks the sequence number of its root-cause alarm on the non-root-cause alarm.

Example

Enable alarm correlation analysis.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm] correlation-analyze enable
Info: Enable analyze correlation between alarms successfully
```

Related Topics

4.5.1 alarm (system view)

4.5.7 delay-suppression enable

Function

The **delay-suppression enable** command enables the alarm or event reporting delay function.

The **undo delay-suppression enable** command disables the alarm or event reporting delay function.

By default, the reporting delay function is enabled.

Format

delay-suppression enable

undo delay-suppression enable

Parameters

None

Views

Alarm view or event view

Default Level

2: Configuration level

Usage Guidelines

If an alarm or an event is repeatedly generated, you can run the **delay-suppression enable** command to enable the reporting delay function to prevent a large number of repeated alarms or events from being reported to the NMS in a specified period.

Example

Enable the alarm reporting delay function.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm] delay-suppression enable
Info: Enable alarm delay suppression successfully
```

Related Topics

4.5.1 alarm (system view)

4.5.13 event

4.5.16 suppression alarm-name

4.5.17 suppression event-name

4.5.8 display alarm active

Function

The **display alarm active** command displays active alarms on the device.

Format

display alarm active

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display alarm active** command to view active alarms on the device to locate faults.

Example

Display active alarms on the device.

```
<Huawei> display alarm active
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  1/Independent/2011-08-22 15:27:38/-/0xff8c2028/hwFanInvalid/Warning/Start/OID
1.3.6.1.4.1.2011.5.25.219.2.6.5 Fan is invalid.(Index=16397, EntityPhysicalIndex
=16397, PhysicalName="FAN Card 0/1", EntityTrapFaultID=139264)
```

Table 4-50 Description of the display alarm active command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format
A=Sequence	Sequence number
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: • Independent: indicates an alarm for which alarm correlation analysis is not performed. • RootCause: indicates a root-cause alarm. • nonRootCause: indicates a non-root-cause alarm.
C=Generating time	Time when an alarm is generated
D=Clearing time	Time when an alarm is cleared
E=ID	Alarm ID
F=Name	Alarm name
G=Level	Alarm severity level You can run the **4.5.3 alarm-name severity** command to set this parameter.
H=State	Alarm status: • Start • End
I=Description information for locating(Para info, Reason info)	Alarm description including alarm parameters and causes for triggering alarms
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm (for non-root-cause alarms only)

Related Topics

4.5.1 alarm (system view)
4.5.2 alarm correlation-suppress enable
4.5.3 alarm-name severity
4.5.4 clear alarm active
4.5.6 correlation-analyze enable

 Copyright © Huawei Technologies Co., Ltd.

4.5.7 delay-suppression enable
4.5.14 mask interface
4.5.16 suppression alarm-name

4.5.9 display alarm history

Function

The **display alarm history** command displays historical alarms on the device.

Format

display alarm history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display alarm history** command to view the alarms that are cleared or generated on the device. The **display alarm history** command displays a maximum of 1024 alarm history records.

Example

Display historical alarms on the device.

```
<Huawei> display alarm history
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  1/Independent/2011-08-22 15:27:38/2011-08-22 15:42:51/0xff8c2028/hwFanInvalid/
Warning/End/OID 1.3.6.1.4.1.2011.5.25.219.2.6.5 Fan is invalid.(Index=16397, Ent
ityPhysicalIndex=16397, PhysicalName="FAN Card 0/1", EntityTrapFaultID=139264)
```

Table 4-51 Description of the display alarm history command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Alarm display format

Item	Description
A=Sequence	Sequence number
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm: ● Independent: indicates an alarm for which alarm correlation analysis is not performed. ● RootCause: indicates a root-cause alarm. ● nonRootCause: indicates a non-root-cause alarm.
C=Generating time	Time when an alarm is generated
D=Clearing time	Time when an alarm is cleared
E=ID	E=ID
F=Name	Alarm ID
G=Level	Alarm severity level You can run the **4.5.3 alarm-name severity** command to set this parameter.
H=State	Alarm status: ● Start ● End
I=Description information for locating(Para info, Reason info)	Alarm description including alarm parameters and causes for triggering alarms
J=RootCause alarm sequence(Only for nonRootCause alarm)	Sequence number of the root-cause alarm

Related Topics

4.5.1 alarm (system view)
4.5.8 display alarm active
4.5.2 alarm correlation-suppress enable
4.5.3 alarm-name severity
4.5.6 correlation-analyze enable
4.5.7 delay-suppression enable
4.5.14 mask interface
4.5.16 suppression alarm-name

 Copyright © Huawei Technologies Co., Ltd.

4.5.10 display alarm information

Function

The **display alarm information** command displays alarm configurations.

Format

display alarm information [**name** *alarm-name*]

Parameters

Parameter	Description	Value
name *alarm-name*	Displays the configuration of a specified alarm. If this parameter is not set, configurations of all alarms are displayed.	The value is of enumerated type and varies according to the registered device type.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view alarm configurations on the device, run the **display alarm information** command.

Example

Display the configuration of the alarm named hwFileError.

```
<Huawei> display alarm information name hwFileError
***********************************
  AlarmName: hwFileError
  AlarmType: Alarm
  AlarmLevel: Warning
  Suppress Period: 10s
  CauseAlarmName: NA
  Match VB Name: entPhysicalName hwStorageDevName
***********************************
```

Table 4-52 Description of the display alarm information command output

Item	Description
AlarmName	Name of an alarm.

Item	Description
AlarmType	Alarm type: ● Alarm: indicates a fault occurs. ● Resume Alarm: indicates a fault is rectified.
AlarmLevel	Alarm severity. You can run the **4.5.3 alarm-name severity** command to set this parameter.
Suppress Period	Alarm reporting delay. You can run the **4.5.16 suppression alarm-name** command to set this parameter.
CauseAlarmName	Name of the root-cause alarm.
Match VB Name	Matching content of paired alarms.

Related Topics

4.5.1 alarm (system view)
4.5.2 alarm correlation-suppress enable
4.5.3 alarm-name severity
4.5.6 correlation-analyze enable
4.5.7 delay-suppression enable
4.5.14 mask interface
4.5.16 suppression alarm-name

4.5.11 display event

Function

The **display event** command displays events on the device.

Format

display event

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display events on the device.

```
<Huawei> display event
A/B/C/D/E/F/G/H/I/J
A=Sequence, B=RootKindFlag(Independent|RootCause|nonRootCause)
C=Generating time, D=Clearing time
E=ID, F=Name, G=Level, H=State
I=Description information for locating(Para info, Reason info)
J=RootCause alarm sequence(Only for nonRootCause alarm)

  1/Independent/2011-08-29 16:36:55/-/0xc0dc2000/entConfigChange/Warning/Start/O
ID 1.3.6.1.2.1.47.2.0.1 Entity MIB change.
  2/Independent/2011-08-29 16:37:32/-/0xc0dc2000/entConfigChange/Warning/Start/O
ID 1.3.6.1.2.1.47.2.0.1 Entity MIB change.
```

Table 4-53 Description of the display event command output

Item	Description
A/B/C/D/E/F/G/H/I/J	Event display format
A=Sequence	Sequence number of an event
B=RootKindFlag(Independent|RootCause|nonRootCause)	Flag indicating a root-cause alarm or a non-root-cause alarm (The value of this field is **Independent** for any event.)
C=Generating time	Time when the event is generated
D=Clearing time	Time when the event is cleared (for non-root-cause alarms only)
E=ID	Event ID
F=Name	Event name
G=Level	Event level
H=State	Event status: ● Start ● End

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
I=Description information for locating(Para info, Reason info)	Description of an event, including parameters of the event and the reason why the event was triggered.
J=RootCause alarm sequence(Only for nonRootCause alarm)	This parameter is valid only for alarms.

Related Topics

4.5.5 clear event all
4.5.7 delay-suppression enable
4.5.12 display event information
4.5.13 event
4.5.17 suppression event-name

4.5.12 display event information

Function

The **display event information** command displays event configurations.

Format

display event information [**name** *event-name*]

Parameters

Parameter	Description	Value
name *event-name*	Displays the configuration of a specified event. If this parameter is not set, configurations of all events are displayed.	The value is of enumeration type and varies according to the registered device type.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view event configurations on the device, run the **display event information** command.

Example

Display registration information about the hwICLogfileNumberUpper event.

```
<Huawei> display event information name hwICLogfileNumberUpper
**********************************
  EventName: hwICLogfileNumberUpper
  EventType: Critical Event
  EventLevel: NA
  Suppress Period: 10s
  Match VB Name: hwICLogFileNumber
**********************************
```

Table 4-54 Description of the display event information command output

Item	Description
EventName	Event name.
EventType	Event type.
EventLevel	Event level.
Suppress Period	Event report delay period. You can run the **4.5.17 suppression event-name** command to set this parameter.
Match VB Name	Matching content of repeated events.

Related Topics

4.5.17 suppression event-name

4.5.13 event

Function

Using the **event** command, you can enter the event view.

Format

event

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **event** command to enter the event view, you can configure event management functions.

Example

Enter the event view.

```
<Huawei> system-view
[Huawei] event
[Huawei-event]
```

Related Topics

4.5.7 delay-suppression enable
4.5.11 display event
4.5.17 suppression event-name
4.5.12 display event information

4.5.14 mask interface

Function

The **mask interface** command enables interface-based alarm suppression.

The **undo mask interface** command disables interface-based alarm suppression.

By default, interface-based alarm suppression is disabled.

Format

mask interface *interface-type interface-number*

undo mask interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface on which alarm suppression is to be enabled.	-

Views

Alarm view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a large number of LinkDown alarms are generated on the interface, you can run the **mask interface** command to suppress LinkDown root-cause and non-root-cause alarms.

Prerequisites

The **4.5.6 correlation-analyze enable** command has been executed in the alarm view to enable alarm correlation analysis.

Example

Enable alarm suppression on the GE0/0/1 interface.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm] correlation-analyze enable
Info: Enable analyze correlation between alarms successfully
[Huawei-alarm] mask interface gigabitethernet0/0/1
```

Related Topics

4.5.1 alarm (system view)

4.5.6 correlation-analyze enable

4.5.15 set said enable

Function

The **set said enable** command enables System of Active Immunization and Diagnosis (SAID) for features.

The **undo set said enable** command disables SAID for features.

By default, the check function and diagnostic information collection function is enabled, and the self-healing function is disabled.

Format

set said { **all** | **module** *module-name* [**feature** *feature-name*] } **behavior** { **check-diagcollect** | **check-recovery** | **check-diagcollect-recovery** } **enable**

undo set said { **all** | **module** *module-name* [**feature** *feature-name*] } **enable**

Parameters

Parameter	Description	Value
all	Indicates all modules and features.	-

Parameter	Description	Value
module *module-name*	Specifies a module name.	Enumerated value. The values are as follows: ● IP ● DIAG ● IFM ● MAC (V200R010C10 and later versions support this value.) The value must be set according to the device configuration.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
feature *feature-name*	Specifies a feature name.	Enumerated value. The values are as follows: ● arp ● buf ● dsvpn (V200R010C10 and later versions support this value.) ● ipsec (V200R010C10 and later versions support this value.) ● l2tp ● mac (V200R010C10 and later versions support this value.) ● nat (V200R010C10 and later versions support this value.) ● nhp4 (V200R010C10 and later versions support this value.) ● nhp6 (V200R010C10 and later versions support this value.) ● VRRP ● LswRsc ● IfWarn ● MacFlap (V200R010C10 and later versions support this value.) The value must be set according to the device configuration.
behavior	Specifies the function for which SAID needs to be enabled.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
check-diagcollect	Enables the check function and diagnostic information collection function.	-
check-recovery	Enables the check function and self-healing function.	-
check-diagcollect-recovery	Enables the check function, diagnostic information collection function, and self-healing function.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SAID allows the device to automatically diagnose faults, identify typical service faults, and use service self-recovery methods for self-healing.

The automated fault diagnosis procedure consists of three phases, fault detection, fault diagnosis, and fault recovery. To enhance device maintainability, SAID supports the source tracing function to collect and store the information generated during fault diagnosis and recovery for fault location.

Precautions

Before enabling the SAID function for a feature, ensure that the device already has a feature module that has registered the self-healing function. Otherwise, the SAID function does not take effect.

Currently, the device supports only VRRP self-healing. VRRP will automatically identify and register the self-healing function.

Example

Enable the check function, diagnostic information collection function, and self-healing function for all modules.

```
<Huawei> system-view
[Huawei] set said all behavior check-diagcollect-recovery enable
Info:Operate succeed.
```

4.5.16 suppression alarm-name

Function

The **suppression alarm-name** command configures the period of delay in reporting alarms.

The **undo suppression alarm-name** command restores the period of delay in reporting alarms.

The system has defined a default period of delay in reporting alarms.

Format

suppression alarm-name *alarm-name* **cause-period** *cause-seconds*

undo suppression alarm-name *alarm-name* **cause-period**

Parameters

Parameter	Description	Value
alarm-name	Specifies the name of the alarm for which the period of delay in reporting alarms is to be configured.	The value is of enumeration type and varies according to the registered device type. To view registered alarm information, run the **4.5.10 display alarm information** command.
cause-period *cause-seconds*	Specifies the period of delay in reporting active alarms.	The value is an integer ranging from 0 to 600, in seconds. When the value is 0, the alarm is reported to the NMS without delay.

Views

Alarm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an alarm is reported repeatedly, users can use the reporting delay function to prevent the alarm from being reported to the NMS. The **suppression alarm-name** command configures the period of delay in reporting alarms.

 Copyright © Huawei Technologies Co., Ltd.

After the alarm reporting delay function is enabled,

- If no clear alarm is generated during the period, the alarm is reported to the NMS when the period expires.
- If a clear alarm is generated during this period, the alarm and its clear alarm are both deleted from the alarm queue and will not be reported to the NMS.

Prerequisites

The alarm reporting delay function has been enabled using the **4.5.7 delay-suppression enable** command.

Precautions

- Each active alarm has its own default period of delay. Run the **undo suppression alarm-name** and **4.5.10 display alarm information** commands in sequence to view the default period of reporting delay.
- If the delay is too short, alarm reporting is not efficiently postponed. If the delay is too long, alarm reporting is postponed and the time when the fault occurs cannot be correctly obtained. For most alarms, the default delay is recommended. For common alarms, such as alarms about hardware and environment, the period of delay in reporting alarms is set to 0.
- During alarm reporting, if you change the period of delay in reporting alarms, the new delay takes effect on the next alarm.

Example

Set the period of hwFileError alarm reporting delay to 5 seconds.

```
<Huawei> system-view
[Huawei] alarm
[Huawei-alarm] delay-suppression enable
[Huawei-alarm] suppression alarm-name hwFileError cause-period 5
```

Related Topics

4.5.1 alarm (system view)

4.5.7 delay-suppression enable

4.5.10 display alarm information

4.5.17 suppression event-name

Function

The **suppression event-name** command configures the period of delay in reporting events.

The **undo suppression event-name** command restores the period of delay in reporting events.

The system has defined a default period of delay in reporting events.

Format

suppression event-name *event-name* **period** *seconds*

undo suppression event-name *event-name* **period**

Parameters

Parameter	Description	Value
event-name	Specifies the name of the event for which the period of delay in reporting events is to be configured.	The value is of enumeration type and varies according to the registered device type. To view registered alarm information, run the **4.5.12 display event information** command.
period *seconds*	Specifies the period of delay in reporting events.	The value is an integer ranging from 0 to 600, in seconds. When the value is 0, the event is reported to the NMS without delay.

Views

Event view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an event is reported repeatedly, users can use the event reporting delay function to prevent the event from being reported to the NMS. The **suppression event-name** command configures the period of delay in reporting events.

After the event reporting delay function is enabled and the period of delay is configured, the system discards the event that is generated several times during the delay. When the delay expires, the system reports only the first event.

Prerequisites

The event reporting delay function has been enabled using the **4.5.7 delay-suppression enable** command.

Precautions

- Each event can be configured with a period of reporting different delay. Run the **undo suppression event-name** and **4.5.12 display event information** commands in sequence to view the default period of reporting delay.
- During event reporting, if you change the period of delay in reporting events, the new delay takes effect on the next alarm.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the period of delay in reporting the event named hwICLogfileNumberUpper to 5 seconds.

```
<Huawei> system-view
[Huawei] event
[Huawei-event] delay-suppression enable
[Huawei-event] suppression event-name hwICLogfileNumberUpper period 5
```

Related Topics

4.5.13 event

4.5.7 delay-suppression enable

4.5.12 display event information

4.6 Commands for Clock Source

4.6.1 clock source

Function

The **clock source** command configures an 8 kHz synchronous clock source.

The **undo clock source** command deletes the specified clock source.

NOTE

Only the AR161, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169RW-P-M9, AR169W-P-M9, AR2204C, AR2220, AR2220L, AR2220E, AR2240C, AR200 series, AR1200 series, AR3200 series, and AR3600 series support this command.

Format

clock source *sourceid slotid|cardid|portid*

clock source *sourceid* [*interface-type*] [*slotid|cardid|portid*] **priority** *priority*

undo clock source *sourceid*

Parameters

Parameter	Description	Value
sourceid	Specifies the index of a clock source.	The value is an integer that ranges from 0 to 9.

Parameter	Description	Value
interface-type	Specifies a clock source interface type. **NOTE** The interface type can only be ATM, serial, or Ethernet interface.	-
slotid|cardid|portid	*slotid* specifies the slot ID. *cardid* specifies the card ID. *portid* specifies the port number.	-
priority *priority*	Specifies the priority of a clock source.	The value is an integer that ranges from 0 to 9. The default value is 9. A smaller value indicates a higher priority of a clock source.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If LPUs have E1/T1 interfaces, an 8 kHz synchronous clock source needs to be configured.

The 8 kHz synchronous clock source recovered from an uplink voice interface needs to be sent to the SRU and LPUs as the transmit reference clock of each voice interface. If the SRU does not receive the 8 kHz synchronous clock source from LPUs, it sends clock signals generated by the local crystal oscillator to other cards as the transmit reference clock.

Configuration Impact

If clock signals recovered from multiple interfaces are used as system clock sources, the clock with highest priority is used as the master clock and other clocks are used as slave clocks. When the master clock is faulty, a slave clock is used.

Precautions

A maximum of 10 clock sources can be configured on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure port 0/0/5 as clock source 1 and set its priority to 5.

```
<Huawei> system-view
[Huawei] clock source 1 0/0/5
[Huawei] clock source 1 priority 5
```

Configure serial 0/0/0 as clock source 1 and set its priority to 1.

```
[Huawei] clock source 1 serial 0/0/0 priority 1
```

Configure serial 0/0/5 as clock source 5 and set its priority to 3. An error message indicating an invalid port number is displayed.

```
<Huawei> system-view
[Huawei] clock source 5 serial 0/0/5 priority 3
Error: Port invalid.
```

Related Topics

4.6.2 display clock source

4.6.2 display clock source

Function

The **display clock source** command displays information about all clock sources.

NOTE

Only the AR161, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169RW-P-M9, AR169W-P-M9, AR2204C, AR2220, AR2220L, AR2220E, AR2240C, AR200 series, AR1200 series, AR3200 series, and AR3600 series support this command.

Format

display clock source

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display clock source** command to view settings and statuses of clock sources. Based on the command output, you can determine whether to reconfigure a clock source.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about clock sources.

```
<Huawei> display clock source
-----------------------------------------------------------------------------
 Index  Config   Type   InterFace          Source      Priority   Output
  0     NO       ----   NA                -/-/-         -       ---
  1     YES      8KHz   Serial             0/0/0        1       FAILED
  2     NO       ----   NA                -/-/-         -       ---
  3     NO       ----   NA                -/-/-         -       ---
  4     NO       ----   NA                -/-/-         -       ---
  5     NO       ----   NA                -/-/-         -       ---
  6     NO       ----   NA                -/-/-         -       ---
  7     NO       ----   NA                -/-/-         -       ---
  8     NO       ----   NA                -/-/-         -       ---
  9     NO       ----   NA                -/-/-         -       ---
-----------------------------------------------------------------------------
```

Table 4-55 Description of the **display clock source** command output

Item	Description
Index	Index of a clock source.
Config	Whether a clock source is configured: ● YES: A clock source has been configured. ● NO: No clock source is configured.
Type	Frequency of the clock source. Currently, only the 8 kHz frequency is supported.
Interface	Clock source interface type. **NOTE** The interface type can only be ATM, serial, or Ethernet interface.
Source	Port number of the clock source. To configure a port number of a clock source, run the **clock source** command.
Priority	Priority of the clock source. To set the priority of a clock source, run the **clock source** command.
Output	Status of the clock source: ● SUCCESS: master clock source ● FAILED: slave clock source

4.7 Energy-saving Configuration Commands

4.7.1 als

Function

The **als** command enables ALS on an interface.

The **undo als** command disables ALS on an interface.

By default, ALS is disabled on an interface.

Format

als

undo als

Parameters

None

Views

GE interface view, XGE interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Only optical interfaces (except PON interfaces) support ALS, and electrical interfaces do not support ALS.

Example

Enable ALS on GigabitEthernet1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/1] als
```

Related Topics

4.7.5 display als

4.7.2 als restart

Function

The **als restart** command manually restarts the laser of an interface.

Format

als restart

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

GE interface view, XGE interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the laser of an optical module works in manual restart mode, if the faulty fiber link is recovered, you need to manually open the laser so that the laser sends one pulse to clear LOS of the optical interface. Then the data communication is recovered.

Prerequisites

ALS has been enabled on the interface using the **4.7.1 als** command and the restart mode of the laser has been set to manual restart mode using the **4.7.3 als restart mode** command.

Example

Restart lasers on GigabitEthernet1/0/0 manually.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/1] als
[Huawei-GigabitEthernet1/0/1] als restart mode manual
[Huawei-GigabitEthernet1/0/1] als restart
```

Related Topics

4.7.1 als

4.7.3 als restart mode

4.7.3 als restart mode

Function

The **als restart mode** command sets the mode of restarting the laser of the optical module.

By default, a laser works in automatic restart mode.

Format

als restart mode { **manual** | **automatic** }

Parameters

Parameter	Description	Value
manual	Sets the mode of restarting the laser of the optical module to manual.	-
automatic	Sets the mode of restarting the laser of the optical module to automatic.	-

Views

GE interface view, XGE interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The laser of an optical module works in automatic restart mode or manual restart mode.

- In automatic restart mode, the laser sends pulses at the interval set using the **4.7.4 als restart pulse interval** *pulse-interval* command to detect whether the link is recovered. The pulse width is set through the **4.7.4 als restart pulse width** *pulse-width* command.
- In manual restart mode, you must manually start the laser using the **4.7.2 als restart** command so that the laser can send a pulse. The ALS pulse width is set using the **4.7.4 als restart pulse width** *pulse-width* command.

If the fiber link recovery is detected in time, you can use the manual restart mode so that the laser can send pulses immediately. Therefore, data communication can be recovered rapidly.

Example

Configure lasers on GigabitEthernet1/0/1 to work in manual restart mode.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/1
[Huawei-GigabitEthernet1/0/1] als restart mode manual
```

Related Topics

4.7.1 als

4.7.2 als restart

4.7.4 als restart pulse

4.7.5 display als

4.7.4 als restart pulse

Function

The **als restart pulse** command sets the ALS pulse width or pulse interval for the laser of an optical module.

By default, the ALS pulse width of the laser is 2s, the ALS pulse interval of the laser is 100s.

Format

als restart pulse { **width** *pulse-width* | **interval** *pulse-interval* }

Parameters

Parameter	Description	Value
width *pulse-width*	Specifies the ALS pulse width of the laser.	The value is an integer that ranges from 2 to 200, in seconds.
interval *pulse-interval*	Specifies the ALS pulse interval of the laser.	The value is an integer that ranges from 100 to 20000, in seconds.

Views

GE interface view, XGE interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The ALS pulse width refers to the period between rising edges of pulses. A short ALS pulse width is beneficial for energy saving, but the fiber link recovery cannot be detected immediately. In contrary, a long ALS pulse width consumes more power but the fiber link recovery can be detected immediately.

In automatic restart mode, the ALS pulse interval affects the frequency of detecting the LOS on the interface. A long ALS pulse interval is beneficial for energy saving, but the fiber link recovery cannot be detected in a timely manner. In contrary, a short ALS pulse interval wastes power but the fiber link recovery can be detected immediately.

Example

Set the ALS pulse width on GigabitEthernet1/0/1 to 3s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/1
[Huawei-GigabitEthernet1/0/1] als restart pulse width 3
```

Set the ALS pulse interval of lasers on GigabitEthernet1/0/1 to 150s.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/1
[Huawei-GigabitEthernet1/0/1] als restart pulse interval 150
```

Related Topics

4.7.1 als
4.7.5 display als

4.7.5 display als

Function

The **display als** command displays ALS configuration.

Format

display als all

display als interface *interface-type interface-number*

display als controller cpos *cpos-number*

Parameters

Parameter	Description	Value
all	Displays ALS configuration on all interfaces.	-
interface *interface-type interface-number*	Displays ALS configuration on a specified interface (except a CPOS interface). ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
controller cpos *cpos-number*	Displays ALS configuration on a specified CPOS interface. *cpos-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display ALS configuration on GigabitEthernet1/0/0.

```
<Huawei> display als interface gigabitethernet 1/0/0
Interface                Mode     Pulse Interval Pulse Width
GigabitEthernet1/0/0     AUTO     100            2
```

Table 4-56 Description of the display als command output

Item	Description
Interface	Interface type and number.
Mode	ALS restart mode. ● AUTO: automatic restart mode. ● MANUAL: manual restart mode. The ALS restart mode is set to manual using the **4.7.3 als restart mode** command.
Pulse Interval	ALS pulse interval, expressed in seconds. The ALS pulse interval is set using the **4.7.4 als restart pulse interval** *pulse-interval* command.
Pulse Width	ALS pulse width, expressed in seconds. The ALS pulse width is set using the **4.7.4 als restart pulse width** *pulse-width* command.

Related Topics

4.7.1 als
4.7.3 als restart mode
4.7.4 als restart pulse

4.7.6 energy-efficient-ethernet enable

Function

The **energy-efficient-ethernet enable** command enables the Energy Efficient Ethernet (EEE) function on an electrical interface.

The **undo energy-efficient-ethernet enable** command disables the EEE function on an electrical interface.

By default, EEE is disabled on an electrical interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

energy-efficient-ethernet enable

undo energy-efficient-ethernet enable

Parameters

None

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system provides power for each interface. Even though an interface is idle, it consumes the same power as working interfaces. The **energy-efficient-ethernet enable** command enables the system to reduce the power on an interface when the interface is idle and restore the power when the interface starts to transmit data. This reduces system power consumption.

Prerequisites

If an electrical interface works in non-auto negotiation mode, run the **negotiation auto** command to enable auto-negotiation.

Precautions

The EEE function can be configured only on electrical interfaces. Optical interfaces or combo interfaces do not support the EEE function.

Ethernet electrical interfaces on AR160 series (except AR161, AR161W, AR161G-L, AR161G-Lc, AR161EW, AR161EW-M1, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169CVW-4B4S, AR169EGW-L, AR169G-L, and AR169-P-M), AR1220E, AR1220EV, AR1220EVW, AR1220F, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204E, AR2240C, AR2204-51GE, AR2204E-D, AR2204-51GE-R, and AR2204 support the EEE function.

Ethernet electrical interfaces on SRU400 of AR2240 and AR3260 support the EEE function.

GE electrical interfaces on the 4ES2G-S board support the EEE function.

Example

Enable the EEE function on electrical interface Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] energy-efficient-ethernet enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

5.2.3 auto speed
5.2.28 negotiation auto

4.7.7 set fan-speed

Function

The **set fan-speed** command sets the fan speed.

The **undo set fan-speed** command restores the default fan speed.

By default, the system automatically adjusts the fan speed.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

set fan-speed fan *slot-id* **percent** *percent*

undo set fan-speed fan *slot-id*

Parameters

Parameter	Description	Value
fan *slot-id*	Specifies the slot ID of a fan module.	The value is an integer and must be set according to the device configuration.
percent *percent*	Specifies the percentage of the current fan speed to the full fan speed. For example, if the value is set to 35, the current fan speed is 35% of the full fan speed.	The value is an integer that ranges from 30 to 100 on the AR1200 series, from 35 to 100 on the AR2200 series and AR3200 series.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fan speed affects the device temperature. When the device temperature is high, increase the fan speed to lower the device temperature. When the device temperature is low, reduce the fan speed to save energy. A proper fan speed ensures stable device operation.

Precautions

- By default, fans run in automatic mode. In this mode, the system adjusts the fan speed when detecting that the board temperature increases or decreases. The automatic mode reduces noises and saves energy without affecting system running. Therefore, exercise caution when setting the fan speed.
- If multiple fans are installed on a fan tray, all the fans run at the rate configured by this command.
- There is a 10% error between the fan speed set by the **set fan-speed** command and the actual fan speed. For example, if you set the fan speed to 50%, the actual fan speed displayed by the **4.1.7 display fan** command is between 45% and 55% of the full speed.

Example

Set the fan speed of the fan module in slot 0 to 60%.

```
<Huawei> system-view
[Huawei] set fan-speed fan 0 percent 60
 Info: Set FAN [0] speed successfully.
```

Related Topics

4.1.7 display fan

4.8 PoE Configuration Commands

NOTE

•Currently, the following models and interfaces support PoE function:

- Model: AR207V-P, AR201VW-P; Supporting interface: Ethernet0/0/0–Ethernet0/0/7
- Model: AR151W-P; Supporting interface: Ethernet0/0/0–Ethernet0/0/3
- Model: AR1220V, AR1220W, and AR1220VW; Supporting interface: Ethernet0/0/4–Ethernet0/0/7
- Model: AR1220EV, AR1220EVW; Supporting interface: GigabitEthernet0/0/4–GigabitEthernet0/0/7
- Model: AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161FW-P-M5; Supporting interface: GigabitEthernet0/0/0–GigabitEthernet0/0/3
- Model: AR2204-51GE-P, AR2204-48GE-P, AR2204XE and AR2204-27GE-P; Supporting interface: GigabitEthernet0/0/3–GigabitEthernet0/0/10

4.8.1 display poe device

Function

The **display poe device** command displays information about the device supporting Power over Ethernet (PoE).

 Copyright © Huawei Technologies Co., Ltd.

Format

display poe device

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before using the PoE function, run the **display poe device** command to check whether the device supports the PoE function. If the command output is displayed, the device supports the PoE function.

Example

Display information about the device supporting PoE.

```
<Huawei> display poe device
slot 0   : POE
```

Table 4-57 Description of the display poe device command output

Item	Description
Slot 0	The device supports PoE.

4.8.2 display poe information

Function

The **display poe information** command displays PoE running information about the device.

Format

display poe information [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the PoE running information in a specified slot.	The value must be set according to the device configuration.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information including the maximum output power set by the user, current power consumption, peak power consumption, and power management mode.

Example

Display the PoE running information about the device.

```
<Huawei> display poe information
 PSE information of slot : 0
     Power max        value(mW) : 148000
     Power peak       value(mW) : 0
     Power current    value(mW) : 0
     Total reference  power(mW) : 0
     Power high inrush     : Disable
     Power management mode : Auto

 PSE information of slot : 1
     Power max        value(mW) : 148000
     Power peak       value(mW) : 22896
     Power current    value(mW) : 21600
     Total reference  power(mW) : 53200
     Power high inrush     : Disable
     Power management mode : Auto
```

Table 4-58 Description of the display poe information command output

Item	Description
Power max value(mW)	Maximum power set for a board. To set the value, run the **4.8.10 poe max-power** command.
Power peak value(mW)	Peak power consumption of a board.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Power current value(mW)	Current power consumption of a board.
Total reference power(mW)	Total reference power of all PDs connected to a board.
Power High Inrush	State of power high inrush function, including enabled and disabled state. By default, the power high inrush function is in disabled state.
Power management mode	Power management mode, including auto and manual modes. To set the mode, run the **4.8.12 poe power-management** command.

Related Topics

4.8.10 poe max-power

4.8.12 poe power-management

4.8.3 display poe power

Function

The **display poe power** command displays current power information on interfaces.

Format

display poe power { **slot** *slot-id* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the power information about all interfaces supporting PoE in a specified slot.	The value is an integer, and the value range depends on the device configuration.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Displays the PoE power information about a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe power** command displays information including the current actual power, maximum output power set for an interface, and class, reference power, and average power of PDs on the interface.

Example

Display the output power of all the interfaces on the board in slot 0.

```
<Huawei> display poe power slot 0
Codes: REFPW(Reference power), USMPW(User set max power),
       CURPW(Current power), PKPW(Peak power),AVGPW(Average power)

PortName            Class  REFPW(mW) USMPW(mW) CURPW(mW) PKPW(mW)  AVGPW(mW)
-------------------------------------------------------------------------------
Ethernet0/0/4         -     -        37000     0         0         0
Ethernet0/0/5         -     -        37000     0         0         0
Ethernet0/0/6         -     -        37000     0         0         0
Ethernet0/0/7         -     -        37000     0         0         0
```

Table 4-59 Description of the display poe power slot command output

Item	Description
PortName	Name of an interface.
Class	Class of a PD on an interface. The system classifies PDs into five classes, namely, class 0 to class 4, according to their maximum power. If no PDs is connected to interface, "-" is displayed.

Item	Description
REFPW(mW)	Reference power of a PD. The system can identify the reference power of each PD. The value varies according to types of PDs. The mapping between PD classes and the reference power is as follows: ● 0: reference power 15.4 W ● 1: reference power 4 W ● 2: reference power 7 W ● 3: reference power 15.4 W ● 4: reference power 37 W
USMPW(mW)	Maximum output power set for an interface. To set the value, run the **4.8.11 poe power** command.
CURPW(mW)	Current power of the PDs on an interface.
PKPW(mW)	Peak power of the PDs on an interface. The value is a statistical value, which equals the current maximum power consumption of the PDs on the interface.
AVGPW(mW)	Average power of the PDs on an interface. The value is a statistical value, which equals the average power consumption from the power-on of the interface till now.

Display the output power of interface Eth0/0/4.

```
<Huawei> display poe power interface ethernet 0/0/4
Port PD          class     : -
Port PD          power(mW) : 200
Port PD peak      power(mW) : 0
Port PD average   power(mW) : 0
Port PD reference power(mW) : -
Port user set max power(mW) : 37000
```

Table 4-60 Description of the display poe power interface command output

Item	Description
Port PD power(mW)	Output power of an interface.
Port PD class	Class of a PD on an interface. The system classifies PDs into five classes, namely, class 0 to class 4, according to their maximum power.

Item	Description
Port PD reference power(mW)	Reference power of a PD. The system can identify the reference power of each PD. The value varies according to types of PDs. The mapping between PD classes and the reference power is as follows: ● 0: reference power 15.4 W ● 1: reference power 4 W ● 2: reference power 7 W ● 3: reference power 15.4 W ● 4: reference power 37 W
Port user set max power(mW)	Maximum output power set for an interface. To set the value, run the **4.8.11 poe power** command.
Port PD peak power(mW)	Peak power of the PDs on an interface. The value is a statistical value, which equals the current maximum power consumption of the PDs on the interface.
Port PD average power(mW)	Average power of the PDs on an interface. The value is a statistical value, which equals the average power consumption from the power-on of the interface till now.

Related Topics

4.8.1 display poe device
4.8.11 poe power
4.8.6 poe enable

4.8.4 display poe power-state

Function

The **display poe power-state** command displays the PoE power supply status of a device.

Format

display poe power-state { **slot** *slot-id* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the power supply status of interfaces supporting PoE in a specified slot.	The value is an integer, and the value range depends on the device configuration.
interface *interface-type interface-number*	Displays the PoE power supply status of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe power-state** command displays information including whether an interface is enabled to check compatibility of non-standard PDs, power supply status on of an interface, class of PDs on an interface, power supply priority, and maximum output power of an interface.

Example

Display the PoE power supply status of Ethernet 0/0/4.

```
<Huawei> display poe power-state interface ethernet 0/0/4
 Port legacy detect          : Disable
 Port power enabled          : Enable
 Port power ON/OFF           : Off
 Port power status           : Detecting
 Port PD class               : -
 Port reference power(mW)    : -
 Port power priority         : Low
 Port max power(mW)          : 30000
 Port current power(mW)      : 0
 Port peak power(mW)         : 0
 Port average power(mW)      : 0
 Port current(mA)            : 0.0
 Port voltage(V)             : 0.0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-61 Description of the display poe power-state interface command output

Item	Description
Port legacy detect	Whether an interface is enabled to check compatibility of non-standard PDs. To enable an interface to check compatibility of non-standard PDs, run the **poe legacy enable** command.
Port power enabled	Whether PoE is enabled on an interface. To enable PoE on an interface, run the **poe enable** command.
Port power ON/OFF	Whether the interface is powered on. ● On: indicates that the interface is powered on. ● Off: indicates that the interface is powered off.
Port power status	Power supply status of an interface. The status can be: ● Test mode: indicates the testing state. ● Detecting: indicates the detection state. ● Disabled: indicates that PoE is disabled on the interface. ● Chip fault: indicates that the chip of the interface fails. ● Power-deny: indicates that the reference power is greater than the maximum output power of an interface. ● Classification overcurrent: indicates that the current of the PDs on the interface exceeds the threshold. ● Unknown class: indicates that the class of the PD is unknown. ● Power overcurrent: indicates that the current of the PD on the interface exceeds the maximum current of the interface. ● Power-on failed: indicates that the interface fails to be powered on. ● Power-ready: indicates that the interface is ready to be powered on. ● Delivering-power: indicates that the PSE is powering on the interface. ● Over loaded: indicates that the power is overloaded. ● Power off time range: indicates that the interface is in the power-off time range.
Port PD class	Class of a PD connected to an interface. The system classifies PDs into five classes, namely, class 0 to class 4, according to their maximum power.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Port reference power(mW)	Reference power of an interface. The system can identify the maximum power of a PD, classify the PD into a certain level, and define the reference power of each level. The mappings between PD types and reference power values are: ● 0: reference power 15.4 W ● 1: reference power 4 W ● 2: reference power 7 W ● 3: reference power 15.4 W ● 4: reference power 30 W
Port power priority	Power supply priority of an interface. The priority is as follows: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **4.8.15 poe priority** command.
Port max power(mW)	Maximum output power of an interface. To set the value, run the **4.8.11 poe power** command.
Port current power(mW)	Current output power of an interface.
Port peak power(mW)	Peak output power of an interface.
Port average power(mW)	Average output power of an interface.
Port current(mA)	Output current of an interface.
Port voltage(V)	Output voltage of an interface.

Display the PoE power supply status of all the interfaces on the board in slot 0.

```
<Huawei> display poe power-state slot 0
PortName              PowerOn/Off  Enabled  Priority Status
-------------------------------------------------------------------------------
Ethernet0/0/4         Off          Enable   Low      Detecting
Ethernet0/0/5         Off          Enable   Low      Detecting
Ethernet0/0/6         Off          Enable   Low      Detecting
Ethernet0/0/7         Off          Enable   Low      Detecting
```

Table 4-62 Description of the display poe power-state slot command output

Item	Description
PortName	Name of an interface.

Item	Description
PowerOn/Off	Whether the interface is powered on. ● On: indicates that the interface is powered on. ● Off: indicates that the interface is powered off.
Enabled	Whether PoE is enabled on an interface. To enable PoE on an interface, run the **poe enable** command.
Priority	Power supply priority of an interface. The priority is as follows: ● Critical: indicates the highest priority. ● High: indicates the second highest priority. ● Low: indicates the lowest priority. To set the priority, run the **4.8.15 poe priority** command.
Status	Power supply status of an interface. The status is classified into following types: ● Test mode: indicates the testing state. ● Detecting: indicates the detection state. ● Disabled: indicates that PoE is disabled on the interface. ● Chip fault: indicates that the chip of the interface fails. ● Power-deny: indicates that the reference power is greater than the maximum output power of an interface. ● Classification overcurrent: indicates that the current of the PDs on the interface exceeds the threshold. ● Unknown class: indicates that the class of the PD is unknown. ● Power overcurrent: indicates that the current of the PD on the interface exceeds the maximum current of the interface. ● Power-on failed: indicates that the interface fails to be powered on. ● Power-ready: indicates that the interface is ready to be powered on. ● Delivering-power: indicates that the PSE starts to power on the interface. ● Over loaded: indicates that the power is overloaded. ● Power off time range: indicates that the interface is in the power-off time range.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

4.8.9 poe legacy enable
4.8.6 poe enable
4.8.15 poe priority
4.8.11 poe power

4.8.5 display poe-power

Function

The **display poe-power** command displays information about the PoE power supply.

Format

display poe-power

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display poe-power** displays information including the available total PoE power, percentage of the reserved power, power alarm threshold, PoE power backup mode, and PoE power module.

Example

Display PoE power information.

```
<Huawei> display poe-power
 Available power value(mW)    : 130000
 Power Utilization-threshold  : 90%
 Reserved power percent       : 20%
 Power backup-mode            : 1+1
 POE power :
    Power    value(mW) : 2928
    Voltage  value(V)  : 48.00
    Current  value(mA) : 61.00
```

 Copyright © Huawei Technologies Co., Ltd.

Table 4-63 Description of the display poe-power command output

Item	Description
Available power value(mW)	PoE power that the system can provide.
Power Utilization-threshold	Alarm threshold percentage of PoE power consumption. To set the threshold percentage, run the **4.8.16 poe-power utilization-threshold** command.
Reserved power percent	Reserved PoE power percentage. To set the percentage, run the **4.8.14 poe power-reserved** command.
Power backup-mode	Specifies the backup mode of PoE power supplies. Currently, only 1+0 mode is available. To set the 1+0 mode.
PoE Power	PoE power.
Power value(mW)	Power provided by one PoE power supply module.
Voltage value(V)	Current voltage of the PoE power supply. The unit is V.
Current value(mA)	Current of the PoE power supply. The unit is mA.

Related Topics

4.8.14 poe power-reserved
4.8.16 poe-power utilization-threshold

4.8.6 poe enable

Function

The **poe enable** command enables the PoE function on an interface.

The **undo poe enable** command disables the PoE function on an interface.

By default, the PoE function is enabled on an interface.

Format

poe enable

undo poe enable

Parameters

None

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

Before providing power for the PD connected to the interface, ensure the PoE function on the interface is enabled. IF the PoE function is not enabled, run the **poe enable** command to enable the PoE function on the interface.

In automatic mode, the power-on and power-off of interfaces is determined by the PoE power and interface power priority. When the PoE power is sufficient, the device does not power off one interface. To stop providing power for one PD, run the **undo poe enable** command.

Precautions

Interfaces supporting PoE include:

- Model: AR207V-P, AR201VW-P; Supporting interface: Ethernet0/0/0–Ethernet0/0/7
- Model: AR151W-P; Supporting interface: Ethernet0/0/0–Ethernet0/0/3
- Model: AR1220V, AR1220W, and AR1220VW; Supporting interface: Ethernet0/0/4–Ethernet0/0/7
- Model: AR1220EV, AR1220EVW; Supporting interface: GigabitEthernet0/0/4–GigabitEthernet0/0/7
- Model: AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161FW-P-M5; Supporting interface: GigabitEthernet0/0/0–GigabitEthernet0/0/3
- Model: AR2204-51GE-P, AR2204-48GE-P, AR2204XE and AR2204-27GE-P; Supporting interface: GigabitEthernet0/0/3–GigabitEthernet0/0/10

Example

Disable the PoE function on Ethernet0/0/4.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/4
[Huawei-Ethernet0/0/4] undo poe enable
Warning: This operation will power off PD of this port.Continue?[Y/N]:y
```

Related Topics

4.8.4 display poe power-state

4.8.7 poe force-power enable

Function

The **poe force-power enable** command enables forcible PoE power supply.

The **undo poe force-power enable** command disables forcible PoE power supply.

By default, forcible PoE power supply is disabled.

Format

poe force-power enable

undo poe force-power enable

Parameters

None

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

If the system power is sufficient and a non-standard PD is connected to the router, run the **poe force-power enable** command on the port connected to this PD to provide power to the PD when the router cannot detect the PD.

Example

Enable forcible PoE power supply.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] poe force-power enable
```

4.8.8 poe { power-off | power-on } interface

Function

The **poe** { **power-off** | **power-on** } **interface** command manually powers on or powers off the PD of an interface.

Format

poe { **power-off** | **power-on** } **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
power-off	Powers off an interface.	-
power-on	Powers on an interface.	-

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface that needs to be powered on or powered off manually.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

In manual power management mode, run the **poe** { **power-off** | **power-on** } **interface** command to power on or power off interfaces. To check whether the command runs successfully, run the **4.8.4 display poe power-state** command.

Precautions

When the available power of the device is insufficient and the device cannot provide power for a new PD, the **poe power-on interface** command is invalid.

Pre-configuration Tasks

Before powering on or powering off an interface, ensure that:

- The power management mode has been in manual mode through running the **4.8.12 poe power-management** command.
- PDs have been connected to the interface.
- The PoE function of the interface has been enabled.
- The classification of the PDs connected to the interface has finished and the PDs have been ready for being powered on.

Example

Manually power on Ethernet 0/0/4 interface.

```
<Huawei> system-view
[Huawei] poe power-on interface ethernet 0/0/4
Info: Succeeded in powering on the PD of port Ethernet0/0/4.
```

Related Topics

4.8.12 poe power-management

4.8.4 display poe power-state

4.8.3 display poe power

4.8.9 poe legacy enable

Function

The **poe legacy enable** command enables the power sourcing equipment (PSE) to check the compatibility of the power device (PD).

The **undo poe legacy enable** command disables the PSE from checking the compatibility of the PD.

By default, the PSE does not check the capability of the PD.

Format

poe legacy enable

undo poe legacy enable

Parameters

None

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

When compatibility check is enabled, the device can detect and provide power for the PD that does not comply with the 802.3af or 802.3at standard. If compatibility check is not enabled, the device cannot detect and provide power for the non-standard PD.

Example

Enable Ethernet0/0/4 to check the compatibility of the PD.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/4
[Huawei-Ethernet0/0/4] poe legacy enable
```

Related Topics

4.8.4 display poe power-state

4.8.10 poe max-power

Function

The **poe max-power** command sets the maximum output power of a device.

 Copyright © Huawei Technologies Co., Ltd.

The **undo poe max-power** command restores the maximum output power of a device to the default value.

By default, the maximum output power of a device depends on the power of the PoE power supply provided by the system.

Format

poe slot *slot-id* **max-power** *max-power*

undo poe max-power slot *slot-id*

Parameters

Parameter	Description	Value
max-power	Specifies the maximum output power of a device.	The value is an integer from 0 to X, in mW. X indicates the total sum of maximum power of all interfaces in the specified slot.
slot *slot-id*	Specifies the slot ID of a PoE card.	The value range depends on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

By default, the system automatically obtains the maximum PoE power supported by the device. You can run the **poe max-power** command to set the maximum output power to ensure stable PoE power supply when the total power of the device is insufficient.

Precautions

If the maximum output power that you set is smaller than the total power required by PDs, PDs with lower priority are powered off or cannot be powered on manually.

Example

Set the maximum output power of the device to 100000 mW.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] poe slot 0 max-power 100000
Warning: This operation may power off some PD. Continue?[Y/N]:y
```

Related Topics

4.8.5 display poe-power

4.8.11 poe power

4.8.11 poe power

Function

The **poe power** command sets the maximum output power of an interface.

The **undo poe power** command restores the default maximum output power of an interface.

By default, the maximum output power of an interface is 30000 mW.

Format

poe power *port-max-power*

undo poe power

Parameters

Parameter	Description	Value
port-max-power	Specifies the maximum output power of an interface.	The value is an integer that ranges from 0 to 60000, in mW.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The PD negotiation power may be different from the power required by some non-standard PDs or PDs that cannot be classified. You can run the **poe power** command to set the maximum output power of the interface, which prevents power overload for PDs and saves energy.

Prerequisites

The PoE function has been enabled on the interface using the **4.8.6 poe enable** command.

Example

Set the maximum output power of Ethernet0/0/4 to 20000 mW.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/4
[Huawei-Ethernet0/0/4] poe power 20000
Warning: This operation may power off the PD of this port.Continue?[Y/N]:y
Info: Succeed in setting maximum power of port.
```

Related Topics

4.8.4 display poe power-state

4.8.10 poe max-power

4.8.12 poe power-management

Function

The **poe power-management** command sets the power management mode of the device.

The **undo poe power-management** command restores the default power management mode of the device.

By default, the device uses the automatic power management mode.

Format

poe power-management { **auto** | **manual** } **slot** *slot-id*

undo poe power-management slot *slot-id*

Parameters

Parameter	Description	Value
auto	Specifies the power management mode to automatic mode.	-
manual	Specifies the power management mode to manual mode.	-
slot *slot-id*	Specifies the slot ID of a board.	The value is an integer, and the value range depends on the device configuration.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

In automatic power management mode, the device first provides power for the interfaces with higher priority and powers off the interfaces of lower priority when the power is insufficient. When the power is sufficient, all interfaces connected to PDs are powered on. To stop providing power for some interfaces, run the **undo poe enable** command to disable the PoE function on the interfaces. If the PoE function is enabled and disabled frequently, faults may occur on the interfaces. To prevent the faults, you can set the power management mode to manual mode. In manual mode, the power-on and power-off of an interface are controlled manually and not affected by the interface power priority.

Precautions

- If all the interfaces are of the same priority, the power supply priority of the interface with a smaller interface number is higher in automatic mode.
- You can view the power management mode by running the **4.8.2 display poe information** command.

Example

Set the power management mode of the board in slot 0 to manual mode.

```
<Huawei> system-view
[Huawei] poe power-management manual slot 0
```

Related Topics

4.8.2 display poe information

4.8.13 poe power-off time-range

Function

The **poe power-off time-range** command makes a configured PoE power-off time range effective on an interface.

The **undo poe power-off time-range** command cancels the configuration.

By default, a device is not configured with PoE power-off time range.

Format

poe power-off time-range *time-range-name*

undo poe power-off time-range

Parameters

Parameter	Description	Value
time-range-name	Specifies a name for a PoE power-off time range. The time unit is minutes.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word all cannot be specified as a time range name.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **poe power-off time-range** command makes a PoE power-off time range set in the system view effective on an interface. If the current time is within the specified time range, the PD connected to the interface cannot be powered on.

The **undo poe power-off time-range** command cancels the configuration. The time range does not take effect on the PD connected to the interface; however, the configuration of the time range is still saved.

NOTE

The **poe power-off time-range** command is only applied to automatic power management mode.

Pre-configuration Tasks

Before running the **poe power-off time-range** command, you must ensure a PoE power-off time range has been configured through running the **time-range** command in the system view.

Example

Configure a PoE power-off time range from 10:00 to 11:00 for PDs connected to Ethernet0/0/4.

```
<Huawei> system-view
[Huawei] time-range PoE 10:00 to 11:00 daily
[Huawei] interface ethernet 0/0/4
[Huawei-Ethernet0/0/4] poe power-off time-range PoE
Warning: Do you want to set the power off time range "PoE"?[Y/N]:y
```

Related Topics

19.7.24 time-range

4.8.14 poe power-reserved

Function

The **poe power-reserved** command sets the percentage of the reserved PoE power against the total PoE power.

The **undo poe power-reserved** command restores the default percentage of the reserved PoE power against the total PoE power.

By default, 20% of the total power is reserved.

Format

poe power-reserved *power-reserved*

undo poe power-reserved

Parameters

Parameter	Description	Value
power-reserved	Specifies the percentage of the reserved PoE power against the available PoE power.	The value is an integer that ranges from 0 to 100, in percentage. The default value is 20.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

The device can dynamically allocate power to each interface according to the power consumption of each interface. The power consumption of a PD keeps changing when the PD is running. The system periodically calculates the total power consumption of all the PDs. If the total power consumption exceeds the upper threshold of the device, the system cuts off the power of the PDs on the interfaces of low priority to ensure that other PDs can run normally.

Sometimes, however, the power consumption increases sharply and the available power of the system cannot support the burst increase of power. At this time, the

 Copyright © Huawei Technologies Co., Ltd.

system has not calculated and found that the total power consumption exceeded the upper threshold; therefore, the system does not cut off power low-priority interfaces in time. As a result, the PoE power supply is shut down for overload protection, and all PDs are powered off.

This problem can be solved by running the **poe power-reserved** command to set proper reserved power. When there is a burst increase in power consumption, the reserved power can support the system running. Then the system has time to power off interfaces of low priority to ensure stable running of other PDs.

Precautions

- The reserved power should not be set greater than 20%. If the reserved PoE power is greater than 20% of the total PoE power, the power capacity of the device is affected.

Example

Set the percentage of reserved PoE power to the total PoE power to 30%.

```
<Huawei> system-view
[Huawei] poe power-reserved 30
Warning: This operation may power off some PD.Continue?[Y/N]:y
```

Related Topics

4.8.10 poe max-power

4.8.5 display poe-power

4.8.15 poe priority

Function

The **poe priority** command sets the power priority of a PoE interface.

The **undo poe priority** command restores the default power priority of a PoE interface.

By default, the power supply priority of an interface is **low**.

Format

poe priority { **critical** | **high** | **low** }

undo poe priority

Parameters

Parameter	Description	Value
critical	Indicates the highest priority.	-
high	Indicates the second highest priority.	-

Parameter	Description	Value
low	Indicates the lowest priority.	-

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

When the output power of a device is insufficient, the device in automatic power management mode provides power for the interfaces of the higher power supply priorities first and cuts off power of the interfaces of the lower power supply priorities. If all the interfaces are of the same priority, the power supply priority of the interface with a smaller slot number is higher. If all the interfaces are of the same slot number, the power supply priority of the interface with a smaller interface number is higher.

Example

Set the power supply priority of Ethernet0/0/4 to critical.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/4
[Huawei-Ethernet0/0/4] poe priority critical
Warning: This operation may power off some PD with lower priority.Continue?[Y/N]:y
```

Related Topics

4.8.12 poe power-management

4.8.16 poe-power utilization-threshold

Function

The **poe-power utilization-threshold** command sets the alarm threshold of the PoE power consumption.

The **undo poe-power utilization-threshold** command restores the default alarm threshold of the PoE power consumption.

By default, the alarm threshold percentage is 90%.

Format

poe-power utilization-threshold *threshold-value*

undo poe-power utilization-threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the percentage of the PoE power consumption to the total PoE power.	The value is an integer, in percentage. It is limited by the percentage of the reserved PoE power to the total PoE power. The default value is 90.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

You can use the **poe-power utilization-threshold** command to set the alarm threshold of the PoE power consumption. When the total power consumed by PDs exceeds the configured upper limit, an alarm is generated to notify users of this event. If the total PoE power is 1600 W and the alarm threshold of the PoE power consumption is 90%, when the power consumption is greater than 1440 W, an alarm that the PoE power consumption exceeds the threshold is generated. When the power consumption is recovered to less than 1440 W, an alarm that the PoE power consumption is recovered is generated.

Precautions

Example

Set the alarm threshold of the PoE power consumption to 80%.

```
<Huawei> system-view
[Huawei] poe-power utilization-threshold 80
```

Related Topics

4.8.14 poe power-reserved

4.8.5 display poe-power

 Copyright © Huawei Technologies Co., Ltd.

4.9 OIDS Configuration Commands

NOTE

Only V200R010C10 and later versions support this function.

Only the AR3200 series, AR2220-AC, AR2220-DC, AR2240, and AR2240C support this function.

4.9.1 collect oids database file to system-master

Function

The **collect oids database file to system-master** command saves OIDS database files to the active MPU.

Format

collect oids database file to system-master

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Application Scenarios

After the OIDS function is enabled, the device saves the collected data and fault diagnosis results to database files on the active MPU. When you query OIDS data, the device reads the OIDS database files stored on the active MPU. For a dual-MPU, the device cannot read OIDS database files on the standby MPU. This means that, if an active/standby MPU switchover occurs, you cannot query the OIDS database files on the current standby MPU. In this case, you need to save the OIDS database files on the standby MPU to the active MPU, and then view OIDS data in the files. Otherwise, you may view incomplete OIDS data.

After the **collect oids database file to system-master** command is executed, the device deletes the previously collected OIDS database files saved on the active MPU, and then saves OIDS database files on all standby MPUs to the active MPU. If standby MPUs are not installed or registered, the device deletes only the previously collected OIDS database files saved on the active MPU.

Precautions

The contents of OIDS database files cannot be manually modified.

 Copyright © Huawei Technologies Co., Ltd.

Before running the **collect oids database file to system-master** command, ensure that the active MPU has sufficient space. To check the available storage space on the device, run the **dir** command. If the storage space is insufficient, run the **delete** command to delete unnecessary files.

Example

Save OIDS database files to the active MPU.

```
<Huawei> system-view
[Huawei] collect oids database file to system-master
Warning: After the command is run, the files in the directory sd1:/oids/gather will be deleted. Continue?
[Y/N]:y
```

4.9.2 display oids current-event

Function

The **display oids current-event** command displays information about OIDS events generated after the device starts.

Format

display oids current-event

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the OIDS monitoring function is enabled, the device periodically collects and saves diagnosis object attribute data to database files based on diagnosis types, diagnosis objects, and diagnosis object attributes. The OIDS module sends key performance indicator (KPI) data to each service module based on the collected diagnosis object attribute data. Service modules compare the KPI data with the defined threshold range to determine whether to generate an event. If a service module generates an event, it sends the event information to the OIDS module, which then records the information to database files. For details about OIDS events supported by the device, descriptions, and causes, see Appendix 2 OIDS Events Supported by the Device.

To check information about OIDS events generated after the device starts, run the **display oids current-event** command. To view OIDS events generated within a specified period or OIDS events of a specified type, run the **display oids history-event** command. To view OIDS event information registered on a device, run the **display oids register-event** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display OIDS event information generated on the MPU after the device starts.

```
<Huawei> display oids current-event
Slot: 0
-----------------------------------------------
Event name    : CPU Usage High
Object name   : CPU
Attribute name: CPU Usage
State value   : 95%
Begin time    : 2020-02-23 16:08:59
End time      : 2020-02-23 16:08:59
-----------------------------------------------

Info: At most 100 events that have been processed since each board starts can be displayed for this board.
All events that have not been processed will also be displayed.
```

Table 4-64 Output description of the **display oids current-event** command

Item	Description
Slot	Slot ID.
Event name	Event name.
Object name	Name of a diagnosis object.
Attribute name	Name of a diagnosis object attribute.
State value	Diagnosis object attribute value when an event occurs.
Begin time	Start time of an event.
End time	End time of an event.

4.9.3 display oids history-event

Function

The **display oids current-event** command displays information about OIDS events generated after the device starts.

Format

display oids history-event [**type** *type-name* [{ **object-index** *object-index* | **object-name** *object-name* } [{ **attribute-index** *attribute-index* | **attribute-name** *attribute-name* }]]] [**slot** *slot-id*] [{ **before** | **after** } **date-time** *time date*] [**period** { **1h** | **24h** }]

Parameters

Parameter	Description	Value
type *type-name*	Specifies a diagnosis type name.	The value is of the enumerated type: ● cpu: CPU diagnosis type. ● memory: memory diagnosis type.
object-index *object-index*	Specifies a diagnosis object index.	Run the **display oids register-status** command to view the diagnosis objects and diagnosis object attributes supported by the device. For details, see Appendix 1 OIDS Monitoring Items Supported by the Device.
object-name *object-name*	Specifies a diagnosis object name.	
attribute-index *attribute-index*	Specifies a diagnosis object attribute index.	
attribute-name *attribute-name*	Specifies a diagnosis object attribute name.	
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
before	Displays OIDS events generated before the specified time.	-
after	Displays OIDS events generated after the specified time.	-
date-time *time date*	Specifies a time value.	*time* is in HH:MM:SS format and ranges from 00:00:00 to 23:59:59. *date* is in YYYY-MM-DD format and ranges from 2000-1-1 to 2099-12-31.
period { **1h** | **24h** }	Specifies the period during which OIDS events need to be displayed.	If **period** is not specified, OIDS events generated within 1 hour before or after the current time are displayed by default.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Application Scenarios

After the OIDS monitoring function is enabled, the device periodically collects and saves diagnosis object attribute data to database files based on diagnosis types, diagnosis objects, and diagnosis object attributes. The OIDS module sends key performance indicator (KPI) data to each service module based on the collected diagnosis object attribute data. Service modules compare the KPI data with the defined threshold range to determine whether to generate an event. If a service module generates an event, it sends the event information to the OIDS module, which then records the information to database files. For details about OIDS events supported by the device, descriptions, and causes, see Appendix 2 OIDS Events Supported by the Device.

You can run the **display oids history-event** command to view OIDS events generated within a specified period or OIDS events of a specified type. To view OIDS events generated after the device starts, run the **display oids current-event** command. To view OIDS events registered on a device, run the **display oids history-event** command.

Precautions

If no time parameter is specified in the **display oids history-event** command, OIDS events generated within 1 hour before the current time are displayed by default.

For a dual-MPU, you are advised to run the **collect oids database file to system-master** command to collect OIDS database files to the active MPU before viewing OIDS monitoring and diagnosis results within a period of time.

Example

Display OIDS events generated within 1 hour before 17:00:00 on February 20, 2020.

```
<Huawei> display oids history-event before date-time 17:00:00 2020-02-20 period 1h
-----------------------------------------------------------------------
Slot       : 0
ObjectName : CPU
AttrName   : CPU Usage
Event      : CPU Usage High
Time       : 2020-02-20 16:35:11
State value: 93%
-----------------------------------------------------------------------
```

Table 4-65 Output description of the **display oids history-event** command

Item	Description
Slot	Slot ID.
ObjectName	Name of a diagnosis object.
AttrName	Name of a diagnosis object attribute.
Event	Event name.

Item	Description
Time	Time when an event occurs.
State value	Diagnosis object attribute value when an event occurs.

4.9.4 display oids monitor current-fault

Function

The **display oids monitor current-fault** command displays OIDS monitoring information that triggers abnormal events at the current time.

NOTE

When the OIDS monitoring function is disabled, run the **display oids monitor current-fault** command to display the latest OIDS monitoring information that triggers abnormal events previously.

Format

display oids monitor current-fault [**type** *type-name* [{ **object-index** *object-index* | **object-name** *object-name* } [{ **attribute-index** *attribute-index* | **attribute-name** *attribute-name* }]]]

Parameters

Parameter	Description	Value
type *type-name*	Specifies a diagnosis type name.	The value is of the enumerated type: • cpu: CPU diagnosis type. • memory: memory diagnosis type.
object-index *object-index*	Specifies a diagnosis object index.	Run the **display oids register-status** command to view the diagnosis objects and diagnosis object attributes supported by the device. For details, see Appendix 1 OIDS Monitoring Items Supported by the Device.
object-name *object-name*	Specifies a diagnosis object name.	
attribute-index *attribute-index*	Specifies a diagnosis object attribute index.	
attribute-name *attribute-name*	Specifies a diagnosis object attribute name.	

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the OIDS monitoring function is enabled, the device periodically collects and saves diagnosis object attribute data to database files based on diagnosis types, diagnosis objects, and diagnosis object attributes. The OIDS module sends key performance indicator (KPI) data to each service module based on the collected diagnosis object attribute data. The service module determines whether to generate an event for the KPI data based on the internal threshold range. If a service module generates an event, it sends the event information to the OIDS module. The OIDS module records the event in database files and sets diagnosis object attributes of abnormal events to Abnormal.

You can run the **display oids monitor current-fault** command to check attributes in the Abnormal state and the faulty services. To view detailed OIDS monitoring information recorded on the device, run the **display oids monitor status** command.

Example

Display OIDS monitoring information that triggers abnormal events at the current time.

```
<Huawei> display oids monitor current-fault
Slot Type-name  Object-name        Attribute-name      Status
-----------------------------------------------------------------
15   CPU        CPU                CPU_Usage           Abnormal
15   Memory     Memory             Memory_Usage        Abnormal
```

Table 4-66 Output description of the **display oids monitor current-fault** command

Item	Description
Slot	Slot ID.
Type-name	Diagnosis type.
Object-name	Name of a diagnosis object.
Attribute-name	Name of a diagnosis object attribute.
Status	Faulty state.

 Copyright © Huawei Technologies Co., Ltd.

4.9.5 display oids monitor kpi

Function

The **display oids monitor kpi** command displays KPI information generated within a certain period.

Format

display oids monitor kpi { **data** | **graph** } **type** *type-name* { **object-index** *object-index* | **object-name** *object-name* } { **attribute-index** *attribute-index* | **attribute-name** *attribute-name* } **slot** *slot-id* [**period** { **60min** | **24h** | **72h** } { **before** | **after** } **date-time** *time date*]

Parameters

Parameter	Description	Value
data	Displays KPI information in data format.	-
graph	Displays KPI information in graph format.	-
type *type-name*	Specifies a diagnosis type name.	The value is of the enumerated type: • cpu: CPU diagnosis type. • memory: memory diagnosis type.
object-index *object-index*	Specifies a diagnosis object index.	Run the **display oids register-status** command to view the diagnosis objects and diagnosis object attributes supported by the device. For details, see Appendix 1 OIDS Monitoring Items Supported by the Device.
object-name *object-name*	Specifies a diagnosis object name.	
attribute-index *attribute-index*	Specifies a diagnosis object attribute index.	
attribute-name *attribute-name*	Specifies a diagnosis object attribute name.	
slot *slot-id*	Specifies a slot ID.	The value depends on the device configuration.
period { **60min** | **24h** | **72h** }	Specifies the period during which KPI information needs to be displayed.	If **period** is not specified, KPI monitoring information generated 60 minutes before the current time is displayed by default.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
before	Displays KPI information generated before the specified time.	-
after	Displays KPI information generated after the specified time.	-
date-time *time date*	Specifies a time value.	*time* is in HH:MM:SS format and ranges from 00:00:00 to 23:59:59. *date* is in YYYY-MM-DD format and ranges from 2000-1-1 to 2099-12-31.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Application Scenarios

After the OIDS monitoring function is enabled, the device periodically collects and saves diagnosis object attribute data to database files based on diagnosis types, diagnosis objects, and diagnosis object attributes. The OIDS module sends key performance indicator (KPI) data to each service module based on the collected diagnosis object attribute data. The service module determines whether to generate an event for the KPI data based on the internal threshold range. If a service module generates an event, it sends the event information to the OIDS module. The OIDS module records the event in database files and sets diagnosis object attributes of abnormal events to Abnormal.

You can run the **display oids monitor kpi** command to query KPI information recorded on the device in data or graph format to quickly identify and rectify faults.

Precautions

For a dual-MPU, you are advised to run the **collect oids database file to system-master** command to collect OIDS database files to the active MPU before viewing OIDS monitoring and diagnosis results within a period of time.

The contents of OIDS database files cannot be manually modified.

Example

Display KPI information with Type set to CPU, Object index set to 0, and Attribute index set to 0 in slot 0 60 minutes after 07:47:12 on March 10, 2020.

```
<Huawei> display oids monitor kpi data type cpu object-index 0 attribute-index 0 slot 0 period 60min
after date-time 07:48:00 2020-03-10

Object name: CPU
Attribute name: CPU_Usage
Slot: 0

-----------------------------------------------------------------------------------------------------
Time                                    Average          Maximum          Status
-----------------------------------------------------------------------------------------------------
2020-03-10 07:47:12-2020-03-10 07:48:12 90%              90%              abnormal
2020-03-10 07:48:12-2020-03-10 07:49:12 90%              90%              abnormal
2020-03-10 07:49:12-2020-03-10 07:50:12 90%              90%              abnormal
2020-03-10 07:50:12-2020-03-10 07:51:12 90%              90%              abnormal
2020-03-10 07:51:12-2020-03-10 07:52:12 90%              90%              abnormal
2020-03-10 07:52:12-2020-03-10 07:53:12 90%              90%              abnormal
2020-03-10 07:53:12-2020-03-10 07:54:12 90%              90%              abnormal
2020-03-10 07:54:12-2020-03-10 07:55:12 85%              85%              abnormal
2020-03-10 07:55:12-2020-03-10 07:56:12 85%              85%              abnormal
2020-03-10 07:56:12-2020-03-10 07:57:12 85%              85%              abnormal
2020-03-10 07:57:12-2020-03-10 07:58:12 85%              85%              abnormal
2020-03-10 07:58:12-2020-03-10 07:59:12 85%              85%              abnormal
2020-03-10 07:59:12-2020-03-10 08:00:12 85%              85%              abnormal
2020-03-10 08:00:12-2020-03-10 08:01:12 85%              85%              abnormal
2020-03-10 08:01:12-2020-03-10 08:02:12 85%              85%              abnormal
2020-03-10 08:02:12-2020-03-10 08:03:12 85%              85%              abnormal
2020-03-10 08:03:12-2020-03-10 08:04:12 85%              85%              abnormal
2020-03-10 08:04:12-2020-03-10 08:05:12 85%              85%              abnormal
2020-03-10 08:05:12-2020-03-10 08:06:12 85%              85%              abnormal
2020-03-10 08:06:12-2020-03-10 08:07:12 85%              85%              abnormal
2020-03-10 08:07:12-2020-03-10 08:08:12 85%              85%              abnormal
2020-03-10 08:08:12-2020-03-10 08:09:12 85%              85%              abnormal
2020-03-10 08:09:12-2020-03-10 08:10:12 86%              86%              abnormal
2020-03-10 08:10:12-2020-03-10 08:11:12 86%              86%              abnormal
2020-03-10 08:11:12-2020-03-10 08:12:12 86%              86%              abnormal
2020-03-10 08:12:12-2020-03-10 08:13:12 86%              86%              abnormal
2020-03-10 08:13:12-2020-03-10 08:14:12 86%              86%              abnormal
2020-03-10 08:14:12-2020-03-10 08:15:12 86%              86%              abnormal
2020-03-10 08:15:12-2020-03-10 08:16:12 86%              86%              abnormal
2020-03-10 08:16:12-2020-03-10 08:17:12 86%              86%              abnormal
2020-03-10 08:17:12-2020-03-10 08:18:12 86%              86%              abnormal
2020-03-10 08:18:12-2020-03-10 08:19:12 86%              86%              abnormal
2020-03-10 08:19:12-2020-03-10 08:20:12 90%              90%              abnormal
2020-03-10 08:20:12-2020-03-10 08:21:12 90%              90%              abnormal
2020-03-10 08:21:12-2020-03-10 08:22:12 90%              90%              abnormal
2020-03-10 08:22:12-2020-03-10 08:23:12 90%              90%              abnormal
2020-03-10 08:23:12-2020-03-10 08:24:12 90%              90%              abnormal
2020-03-10 08:24:12-2020-03-10 08:25:12 23%              23%              normal
2020-03-10 08:25:12-2020-03-10 08:26:12 23%              23%              normal
2020-03-10 08:26:12-2020-03-10 08:27:12 23%              23%              normal
2020-03-10 08:27:12-2020-03-10 08:28:12 23%              23%              normal
2020-03-10 08:28:12-2020-03-10 08:29:12 23%              23%              normal
2020-03-10 08:29:12-2020-03-10 08:30:12 23%              23%              normal
2020-03-10 08:30:12-2020-03-10 08:31:12 23%              23%              normal
2020-03-10 08:31:12-2020-03-10 08:32:12 23%              23%              normal
2020-03-10 08:32:12-2020-03-10 08:33:12 23%              23%              normal
2020-03-10 08:33:12-2020-03-10 08:34:12 23%              23%              normal
2020-03-10 08:34:12-2020-03-10 08:35:12 91%              91%              abnormal
2020-03-10 08:35:12-2020-03-10 08:36:12 91%              91%              abnormal
2020-03-10 08:36:12-2020-03-10 08:37:12 91%              91%              abnormal
2020-03-10 08:37:12-2020-03-10 08:38:12 91%              91%              abnormal
2020-03-10 08:38:12-2020-03-10 08:39:12 91%              91%              abnormal
2020-03-10 08:39:12-2020-03-10 08:40:12 85%              85%              abnormal
2020-03-10 08:40:12-2020-03-10 08:41:12 85%              85%              abnormal
```

```
2020-03-10 08:41:12-2020-03-10 08:42:12 85%          85%          abnormal
2020-03-10 08:42:12-2020-03-10 08:43:12 85%          85%          abnormal
2020-03-10 08:43:12-2020-03-10 08:44:12 85%          85%          abnormal
2020-03-10 08:44:12-2020-03-10 08:45:12 -            -            NA
2020-03-10 08:45:12-2020-03-10 08:46:12 -            -            NA
2020-03-10 08:46:12-2020-03-10 08:47:12 -            -            NA
-----------------------------------------------------------------------------------------------

Abnormal Information:
---------------------------------------------
Time                Abnormal Value
---------------------------------------------
2020-03-10 07:50:00  90
2020-03-10 07:55:00  85
2020-03-10 08:00:00  85
2020-03-10 08:05:00  85
2020-03-10 08:10:00  86
2020-03-10 08:15:00  86
2020-03-10 08:20:00  90
2020-03-10 08:35:00  91
2020-03-10 08:40:00  85
```

Table 4-67 Output description of the **display oids monitor kpi** command

Item	Description
Object name	Name of a diagnosis object.
Attribute name	Name of a diagnosis object attribute.
Slot	Slot ID.
Time (first one)	Time range. ● If **period** is set to **60min**, **60min** is divided into 60 consecutive time ranges at the interval of 1 minute. ● If **period** is set to **24h**, **24h** is divided into 48 consecutive time ranges at the interval of 0.5 hour. ● If **period** is set to **72h**, **72h** is divided into 72 consecutive time ranges at the interval of 1 hour.
Average	Average value of diagnosis object attributes within a time range. "-" indicates that no data is available in the database during this period.
Maximum	Maximum value of diagnosis object attributes within a time range. "-" indicates that no data is available in the database during this period.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status	Status of a diagnosis object attribute: ● normal: The diagnosis object attribute is in normal state. ● abnormal: The diagnosis object attribute is in abnormal state. ● NA: The status is empty and no data is recorded in the database.
Abnormal Information	Information about the diagnosis object attribute in abnormal state.
Time (second one)	Record time.
Abnormal Value	Data of a diagnosis object attribute.

4.9.6 display oids monitor status

Function

The **display oids monitor status** command displays OIDS monitoring information at the current time.

Format

display oids monitor status [**type** *type-name* [{ **object-index** *object-index* | **object-name** *object-name* } [{ **attribute-index** *attribute-index* | **attribute-name** *attribute-name* }]]]

Parameters

Parameter	Description	Value
type *type-name*	Specifies a diagnosis type name.	The value is of the enumerated type: ● cpu: CPU diagnosis type. ● memory: memory diagnosis type.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
object-index *object-index*	Specifies a diagnosis object index.	Run the **display oids register-status** command to view the diagnosis objects and diagnosis object attributes supported by the device. For details, see Appendix 1 OIDS Monitoring Items Supported by the Device.
object-name *object-name*	Specifies a diagnosis object name.	
attribute-index *attribute-index*	Specifies a diagnosis object attribute index.	
attribute-name *attribute-name*	Specifies a diagnosis object attribute name.	

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the OIDS monitoring function is enabled, the device periodically collects and saves diagnosis object attribute data to database files based on diagnosis types, diagnosis objects, and diagnosis object attributes. The OIDS module sends key performance indicator (KPI) data to each service module based on the collected diagnosis object attribute data. The service module determines whether to generate an event for the KPI data based on the internal threshold range. If a service module generates an event, it sends the event information to the OIDS module. The OIDS module records the event in database files and sets diagnosis object attributes of abnormal events to Abnormal.

To check OIDS monitoring information recorded on the device, run the **display oids monitor status** command. The displayed information includes the current values, upper thresholds, and status of diagnosis object attributes. Based on the status of diagnosis object attributes, you can quickly detect service faults. To view information about attributes in the abnormal state, run the **display oids monitor current-fault** command.

Example

Display OIDS monitoring information related to the CPU diagnosis type at the current time.

```
<Huawei> display oids monitor status type cpu
Slot Type-name  Object          Attribute        Current          Upper   Status
             name            name             value            value
-----------------------------------------------------------------------------------------
15   CPU        CPU             CPU_Usage        8%               80%     Normal
15   CPU        CPU             CAP_CPU_Usage    0%               80%     Normal
```

Table 4-68 Output description of the **display oids monitor status** command

Item	Description
Slot	Slot ID.
Type-name	Diagnosis type.
Object name	Name of a diagnosis object.
Attribute name	Name of a diagnosis object attribute.
Current value	Current value of a diagnosis object attribute. "-" indicates that the OIDS monitoring function is disabled.
Upper value	Upper threshold of a diagnosis object attribute. Service modules compare the collected current diagnosis object attribute value with the defined upper threshold to determine whether to generate an event. "-" indicates that a diagnosis object attribute does not have the upper threshold.
Status	Status of a diagnosis object attribute: ● Init: The diagnosis object attribute is in initial state. ● Normal: The diagnosis object attribute is in normal state. ● Abnormal: The diagnosis object attribute is in abnormal state. ● Disable: The OIDS monitoring function is disabled.

4.9.7 display oids register-event

Function

The **display oids register-event** command displays information about OIDS events registered on the device.

Format

display oids register-event

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the OIDS monitoring function is enabled, the device periodically collects and saves diagnosis object attribute data to database files based on diagnosis types, diagnosis objects, and diagnosis object attributes. The OIDS module sends key performance indicator (KPI) data to each service module based on the collected diagnosis object attribute data. Service modules compare the KPI data with the defined threshold range to determine whether to generate an event. If a service module generates an event, it sends the event information to the OIDS module, which then records the information to database files. For details about OIDS events supported by the device, descriptions, and causes, see Appendix 2 OIDS Events Supported by the Device.

You can run the **display oids register-event** command to view all registered OIDS events on the device.

Example

Display OIDS event information registered on the MPU.

```
<Huawei> display oids register-event
Slot Event-name                    Event      Type-name  Occur      Restrain
                                 category            times      times
-----------------------------------------------------------------------------
15   CPU Usage High                Warning    CPU        0          0
15   CPU Usage Normal              Recovery   CPU        0          0
15   CAP CPU Usage High            Warning    CPU        0          0
15   CAP CPU Usage Normal          Recovery   CPU        0          0
15   Memory Usage High             Warning    Memory     0
0
15   Memory Usage Normal           Recovery   Memory     0          0
```

Table 4-69 Output description of the **display oids register-event** command

Item	Description
Slot	Slot ID.
Event-name	Event name.
Event category	Event type. ● Warning: warning event ● Recovery: recovery event ● Report: report event
Type-name	Diagnosis type.
Occur times	Number of times an event occurs.

Item	Description
Restrain times	Number of times an event is suppressed.

4.9.8 display oids register-status

Function

The **display oids register-status** command displays information about OIDS monitoring and diagnosis items registered on the device.

Format

display oids register-status [**type** *type-name*]

Parameters

Parameter	Description	Value
type *type-name*	Specifies a diagnosis type name.	The value is of the enumerated type: ● cpu: CPU diagnosis type. ● memory: memory diagnosis type.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display oids register-status** command to display information about the diagnosis types, diagnosis objects, and diagnosis object attributes registered on the device, and whether OIDS monitoring is enabled. For details about the diagnosis types, diagnosis objects, and diagnosis object attributes supported by the device, see Appendix 1 OIDS Monitoring Items Supported by the Device.

Example

Display information about OIDS monitoring and diagnosis items related to the CPU diagnosis type registered on the device.

```
<Huawei> display oids register-status type CPU
Slot Type-name  Object Object          Attribute Attribute       Monitor      Diagnose
```

```
            index  name            index    name            enable-status  enable-status
-----------------------------------------------------------------------------------------------
15   CPU      0     CPU             0       CPU_Usage         Enable        Disable
15   CPU      0     CPU             1       CAP_CPU_Usage      Enable        Disable
```

Table 4-70 Output description of the **display oids register-status** command

Item	Description
Slot	Slot ID.
Type-name	Diagnosis type.
Object index	Index of a diagnosis object.
Object name	Name of a diagnosis object.
Attribute index	Index of a diagnosis object attribute.
Attribute name	Name of a diagnosis object attribute.
Monitor enable-status	Status of the OIDS monitoring function: ● Enable: The OIDS monitoring function is enabled. ● Disable: The OIDS monitoring function is disabled.
Diagnose enable-status	Status of the OIDS diagnosis function: ● Enable: The OIDS diagnosis function is enabled. ● Disable: The OIDS diagnosis function is disabled.

4.9.9 oids monitor enable

Function

The **oids monitor enable** command enables the OIDS monitoring function.

The **undo oids monitor enable** command disables the OIDS monitoring function.

By default, the OIDS monitoring function is enabled.

Format

oids monitor enable { **type** *type-name* | **all** }

undo oids monitor enable { **type** *type-name* | **all** }

Parameters

Parameter	Description	Value
type *type-name*	Specifies a diagnosis type name.	The value is of the enumerated type: ● cpu: CPU diagnosis type. ● memory: memory diagnosis type.
all	Indicates all diagnosis types.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the OIDS monitoring function is enabled for all diagnosis types. The OIDS monitoring process is as follows:

1. The device periodically collects attribute data based on the type, object, and attribute, and records such data to the database files.
2. The OIDS module sends KPI data to each service module based on the collected diagnosis object attribute data. Service modules then determine whether the data is within the normal range.
3. Service modules compare the KPI data with the defined threshold range to determine whether to generate an event.
   - If a service module generates an event, it sends the event information to the OIDS module, and the process goes to Step 4.
   - If no service module generates any event, service modules perform no further operations and the process ends.
4. The OIDS module records the event in the database.

OIDS monitoring and event information enables you to learn about the device and service running status and to detect faults in a timely manner.

Example

Disable the OIDS monitoring function for the CPU diagnosis type.

```
<Huawei> system-view
[Huawei] undo oids monitor enable type CPU
```

Disable the OIDS monitoring function for all diagnosis types.

```
<Huawei> system-view
[Huawei] undo oids monitor enable all
```

4.10 OPS Configuration Commands

NOTE

The AR1220, AR1220V, AR1220W, AR1220VW and AR1220L do not support the OPS function.

4.10.1 assistant scheduler suspend

Function

The **assistant scheduler suspend** command disables the maintenance assistant function.

The **undo assistant scheduler suspend** command enables the maintenance assistant function.

By default, the maintenance assistant function is enabled.

Format

assistant scheduler suspend

undo assistant scheduler suspend

Parameters

None

Views

OPS view

Default Level

3: Management level

Usage Guidelines

If the maintenance assistant function is no longer needed, you can run the **assistant scheduler suspend** command to disable this function. After you run this command, none of assistants will run again.

This command applies to the following scenarios:

- Before deleting configured assistants one by one, run this command to disable the maintenance assistant function to prevent the assistants from running.
- If you do not need the functions provided by assistants, for example, preventive maintenance and upgrade functions, run this command to disable the maintenance assistant function.

 Copyright © Huawei Technologies Co., Ltd.

- During system maintenance, run this command to disable the maintenance assistant function temporarily.

Example

Disable the maintenance assistant function.

```
<Huawei> system-view
[Huawei] ops
[Huawei-ops] assistant scheduler suspend
Info: OPS function disable.
```

4.10.2 clear ops running context

Function

The **clear ops running context** command clears saved contexts.

Format

clear ops running context [*context-name*]

Parameters

Parameter	Description	Value
context-name	Specifies the context name. If *context-name* is not specified, all contexts will be cleared.	The value is a string of 1 to 16 case-sensitive characters without spaces.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

When a Python script uses an ops.context.save (varName, value) API, the device saves specified variables in the script as contexts. In another script, the device can use the ops.context.retrieve (varName) API to obtain the saved context variables and then clear the contexts to transmit variables between two scripts.

You can also run this command to clear context variables and unused contexts.

To check the contexts saved on the device, run the **display ops running context** command.

Example

Clear all the contexts on the device

```
<Huawei> system-view
[Huawei] ops
[Huawei-ops] clear ops running context
Info: All OPS context cleared.
```

Related Topics

4.10.6 display ops running context

4.10.3 display ops assistant

Function

The **display ops assistant** command displays information about OPS assistants.

Format

display ops assistant { **current** [**verbose**] | **history** } [**name** *assistant-name*]

Parameters

Parameter	Description	Value
current	Displays brief information about the current status of assistants.	-
verbose	Displays detailed information about the current status of assistants.	-
history	Displays historical operation records of assistants.	-
name *assistant-name*	Specifies an assistant name, namely, a Python script name for an assistant.	The value is a string of 1 to 118 case-sensitive characters without spaces. The file name extension of a Python script is .py.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

You can use this command to check the current status and historical operation record of an assistant, including the assistant name, running status, and execution result. The command can display a maximum of 100 latest assistant records.

Example

Display brief information about the current status of assistants.

```
<Huawei> display ops assistant current
-------------------------------------------------------
Assistant                    State        Condition
-------------------------------------------------------
subscribe_cli_sync_1.py      ready        cli
user-correlat-10.py          ready        multi
-------------------------------------------------------
```

Table 4-71 Description of the **display ops assistant current** command output

Item	Description
Assistant	Name of an assistant.
State	Current status of the assistant: ● ready: The assistant is waiting to be triggered. ● pending: The assistant is waiting to run. ● waiting: A resident script is waiting to be triggered the second time. ● running: The assistant is running. ● shutdown: The assistant is stopped. ● suspend: The maintenance assistant function is suspended.
Condition	Trigger condition for the assistant: ● cli: CLI event ● multimulti: complex event ● UAM: routing event ● timer: timer event ● trap: alarm event ● iclog: log event ● ADP_NQA: NQA test event ● IFM_IFPDT: interface status event

 Copyright © Huawei Technologies Co., Ltd.

Display detailed information about the current status of assistants.

```
<Huawei> display ops assistant current verbose
Assistant information
  Name                        :user-correlat-10.py
  State                       :ready
Running statistics
  Running times               :0
  Queue size/(free)           :5/(5)
  Skip for queue full         :0
  Skip for delay              :0
  Skip for suppression        :0
Condition information
  Condition tag               :cli1
    Condition type            :multi
    Threshold                 :1
    Period (s)                :0
    Hits in period            :0
  Condition tag               :cli2
    Condition type            :multi
    Threshold                 :1
    Period (s)                :0
    Hits in period            :0
  Condition tag               :cli3
    Condition type            :multi
    Threshold                 :1
    Period (s)                :0
    Hits in period            :0
  Condition tag               :cli4
    Condition type            :multi
    Threshold                 :1
    Period (s)                :0
    Hits in period            :0
  Correlate expression        :((cli1 andnot cli2) and (cli3 andnot cli4))
  Trigger control
    Threshold                 :1
    Period (s)                :30
    Delay (s)                 :0
    Suppress max              :0
    Hits in period            :0
```

Table 4-72 Description of the **display ops assistant current verbose** command output

Item	Description
Assistant information	Assistance task information.
Name	Name of an assistant.
State	Current status of the assistant: ● ready: The assistant is waiting to be triggered. ● pending: The assistant is waiting to run. ● waiting: A resident script is waiting to be triggered the second time. ● running: The assistant is running. ● shutdown: The assistant is stopped. ● suspend: The maintenance assistant function is suspended.

Item	Description
Running statistics	Detailed running information about the assistant.
Running times	Number of running times.
Queue size/(free)	Number of buffered assistants. If the number of buffered assistants reaches the maximum value, subsequent assistants will be discarded.
Skip for queue full	Number of tasks discarded because the queue is full.
Skip for delay	Number of tasks discarded within the delay.
Skip for suppression	Number of times the triggering of the assistant is suppressed.
Condition information	Condition information of the assistant. The **Condition information** field is displayed only for a complex event script.
Condition tag	Condition name.
Condition type	Trigger condition type. The value is multi.
Threshold	Maximum number of times tasks are executed. The default value is 1.
Period (s)	Detection period, in seconds. The default value is 30.
Hits in period	Number of times the trigger condition is met in the detection period.
Correlate expression	Condition combination mode.
Trigger control	Trigger control.
Delay (s)	Delay in triggering a working task. The default value is 0 seconds.
Suppress max	Maximum number of times working tasks are triggered within the delay. The default value is 0, indicating that working tasks will not be suppressed.

Display historical operation records of assistants.

```
<Huawei> display ops assistant history
Assistant history information
  Name                        :subscribe_cli_sync_1.py
```

```
Running information
  Trigger condition          :cli
  Trigger event name          :cli1
  Trigger time               :2015-06-25 19:48:51
  Execute start time          :2015-06-25 19:48:51
  Execute end time            :2015-06-25 19:48:53
  Execute result             :normal
```

Table 4-73 Description of the **display ops assistant history** command output

Item	Description
Assistant history information	Assistant task historical information.
Name	Name of an assistant.
Running information	Running information about the assistant.
Trigger condition	Task trigger condition for the assistant: ● cli: CLI event ● multi: complex event ● UAM: routing event ● timer: timer event ● trap: alarm event ● iclog: log event ● ADP_NQA: NQA test event ● IFM_IFPDT: interface status event
Trigger event name	Triggered task name for the assistant.
Trigger time	Trigger time of the assistant.
Execute start time	Execution start time of an assistant task.
Execute end time	Task execution end time of the assistant.
Execute result	Execution result of an assistant task.

4.10.4 display ops environment

Function

The **display ops environment** command displays information about OPS environment variables.

Format

display ops environment

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to check information about OPS environment variables after user-defined environment variables are configured using the **environment** command.

User-defined environment variables are displayed in alphabetical order.

Example

Display user-defined environment variables

```
<Huawei> display ops environment
No.  Name                    Value
1    user                    admin
```

Table 4-74 Description of the **display ops environment** command output

Item	Description
No.	Environment variable number. The value ranges from 1 to 100.
Name	Indicates an environment variable name. To configure this parameter, run the **environment** command.
Value	Indicates an environment variable value. To configure this parameter, run the **environment** command.

Related Topics

4.10.7 environment

 Copyright © Huawei Technologies Co., Ltd.

4.10.5 display ops error

Function

The **display ops error** command displays script execution errors.

Format

display ops error [**name** *assistant-name*]

Parameters

Parameter	Description	Value
name *assistant-name*	Specifies an assistant name, namely, a Python script name for an assistant.	The value is a string of 1 to 118 case-sensitive characters without spaces. The file name extension of a Python script is .py.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use this command to check execution errors of all scripts or a specified script. According to the command output, you can correct the errors.

Example

Display execution errors of all scripts.

```
<Huawei> display ops error
--------------------------------------------------------------------------------
test12.py:
Traceback (most recent call last):
  File ".lib/frame.py", line 114, in <module>
    ret = m.ops_execute(o)
  File "sd1:$_user/test12.py", line 7, in ops_execute
    status, err_context = o.context.save(varName, value)
NameError: global name 'varName' is not defined

--------------------------------------------------------------------------------
test13.py:
Traceback (most recent call last):
  File ".lib/frame.py", line 114, in <module>
    ret = m.ops_execute(o)
  File "sd1:$_user/test13.py", line 6, in ops_execute
    status, err_log = ops.syslog("Syslog: Hello, World..", ops.CRITICAL, "syslog
```

```
")
AttributeError: 'module' object has no attribute 'syslog'

-----------------------------------------------------------------------------
```

Table 4-75 Description of the **display ops error** command output

Item	Description
test12.py	Python script file name.
Traceback (most recent call last)	Last call error.
File "sd1:$_user/test12.py", line 7, in ops_execute	Location where an error occurs.
status, err_context = o.context.save(varName, value)	Invalid contents.
NameError	A variable error. The system is attempting to access a variable that is not declared.
AttributeError	An attribute error. The system is attempting to access an unknown object attribute.

4.10.6 display ops running context

Function

The **display ops running context** command displays existing contexts on the device.

Format

display ops running context

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When a Python script uses an ops.context.save(varName, value) API, the device saves specified variables in the script as contexts. In another script, the device can

use the ops.context.retrieve(varName) API to obtain the saved context variables and then clear the contexts to transmit variables between two scripts.

To check the contexts that are saved but not obtained by the device, run the **display ops running context** command.

To clear saved contexts, run the **clear ops running context** command.

Example

Display existing contexts on the device.

```
<Huawei> display ops running context
Name          Type     Value
varName1       digit    1234
varName2       string   5678
```

Table 4-76 Description of the **display ops running context** command output

Item	Description
Name	Indicates a variable name.
Type	Type of a variable value: • digit: an integer • string: a string
Value	Indicates a variable value.

Related Topics

4.10.2 clear ops running context

4.10.7 environment

Function

The **environment** command configures user-defined environment variables.

The **undo environment** command deletes user-defined environment variables.

By default, no environment variable is configured.

Format

environment *variable-name* [*variable-value*]

undo environment *variable-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
variable-name	Specifies the name of an environment variable.	The value is a string of 1 to 31 case-sensitive characters without spaces. It starts with a letter and contains only letters, digits, and underscores (_).
variable-value	Specifies the value of an environment variable.	The value is a string of 1 to 31 case-sensitive characters without spaces. **NOTE** If the string is enclosed within double quotation marks ("), the string can contain spaces.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Application Scenario

An environment variable consists of a name and a value. In a Python script, you can input an environment variable name in the location where a parameter needs to be input to indicate that an environment variable value needs to be referenced. When the system is running a Python script, it replaces an environment variable name with an environment variable value. To change the value, you can directly change it on the device without having to change and install the Python script. You can define and use environment variables to simplify the configuration and improve flexibility and feasibility of the Python script.

To define environment variables, run the **environment** command.

Precautions

- If *variable-name* is specified multiple times, the system will prompt that the configured environment variable already exists. You can choose whether to overwrite the existing variable value.
- The **environment** command can configure a maximum of 100 environment variables.

 Copyright © Huawei Technologies Co., Ltd.

- To check configured user-defined environment variables, run the **display ops environment** command.

Example

Set the value of the environment variable **user** to **admin**.

```
<Huawei> system-view
[Huawei] ops
[Huawei-ops] environment user admin
```

Related Topics

4.10.4 display ops environment

4.10.8 ops

Function

The **ops** command displays the OPS view.

Format

ops

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

You can configure assistants in the OPS view.

Example

Display the OPS view.

```
<Huawei> system-view
[Huawei] ops
[Huawei-ops]
```

4.10.9 ops install file

Function

The **ops install file** command installs a Python script.

Format

ops install file *file-name* [**destination** *directory*]

Parameters

Parameter	Description	Value
file-name	Specifies the directory and file name of the Python script to be installed. ● To save a Python script to the root directory of a device, you only need to specify the file name of the script. ● To save the Python script to a non-root directory, you need specify both the directory and file name of the script.	The value is a string of 1 to 64 case-sensitive characters without spaces. The file name extension of a Python script is .py. **NOTE** *file-name* cannot be set to the file name of a built-in Python script, such as cli.py, context.py, environment.py, farg.py, frame.py, iclog.py, interface.py, nqa.py, ops.py, route.py, snmp.py, spr.py, terminal.py, timer.py, trap.py, site.py, os.py, posixpath.py, stat.py, genericpath.py, warnings.py, linecache.py, types.py, UserDict.py, _abcoll.py, abc.py, _weakrefset.py, copy_reg.py, traceback.py, sysconfig.py, re.py, sre_compile.py, sre_parse.py, sre_constants.py, getopt.py, io.py, _pyio.py, __builtin__.py, __main__.py, _ast.py, _codecs.py, _ops.py, _sre.py, _symtable.py, _warnings.py, _weakref.py, errno.py, exceptions.py, gc.py, imp.py, marshal.py, posix.py, pwd.py, signal.py, sys.py, thread.py, xxsubtype.py, and zipimport.py.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination *directory*	Specifies the installation directory of a Python script.	The value is a string of 1 to 45 case-insensitive characters without spaces. If this parameter is not specified, the script will be installed in $_user. If this parameter is specified, the script will be installed in $_user/*directory*. If the directory name does not exist, a directory will be created. **NOTE** The total length of the file-name length and script installation directory cannot exceed 118. The total length is: storage path + $_user + directory name + file name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Application Scenario

OPS allows you to run the scripts you make. You can run the scripts after installing them. Before binding a Python script to an assistant, install the script.

To check information about the scripts installed in $_user, run the **dir (user view)** command.

Precautions

- Before installing a Python script, upload the script to the device.
- If the specified installation directory does not exist, a directory will be created. A maximum of seven levels of subdirectories can be created in $_user.
- To install Python scripts in $_user, you can only run the **ops install file** command. The scripts installed in this directory will be automatically backed up to the standby board.
- Before reinstalling a script, run the **ops uninstall file** command to uninstall the script.

- The maximum size of a script is 1 MB.
- It is recommended that the total size of files installed in $_user be smaller than 100 MB. If the total file size exceeds 100 MB, performance of data synchronization between the active and standby boards may deteriorate.

Example

Install the script **config.py** in the sd1: root directory to the default directory sd1:/$_user.

```
<Huawei> ops install file config.py
```

Install the script **config.py** in the sd1: root directory to the specific directory sd1:/$_user/user.

```
<Huawei> ops install file config.py destination user
```

Install the script **config.py** in the sd1:/admin directory to the default directory sd1:/$_user.

```
<Huawei> ops install file admin/config.py
```

Related Topics

4.10.10 ops uninstall file

4.10.10 ops uninstall file

Function

The **ops uninstall file** command uninstalls a Python script.

Format

ops uninstall file *file-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
file-name	Specifies the file name of the script to be uninstalled.	The value is a string of 1 to 64 case-sensitive characters without spaces and can contain a file directory. If a script in a specified installation directory *directory|file-name* needs to be deleted, *directory* specifies the installation directory of the script. **NOTE** The total length of the file-name length and script installation directory cannot exceed 118. The total length is: storage path + $_user + directory name + file name.

Views

User view

Default Level

3: Management level

Usage Guidelines

Application Scenario

You can uninstall unnecessary scripts to release storage space on a device. If an installed script needs to be modified, uninstall it first, and reinstall it after the modification.

Precautions

- This command cannot uninstall a script that has been bound to an assistant. To uninstall the script, unbind it from assistant first.
- If the script bound to an assistant calls other scripts, the called scripts can be uninstalled using this command. Therefore, it is recommended that you use one script to implement required functions.

Example

Uninstall the script **config.py** in the default directory sd1:/$_user.

```
<Huawei> ops uninstall file config.py
```

Uninstall the script **config.py** in the specific directory sd1:/$_user/user.

```
<Huawei> ops uninstall file user/config.py
```

Related Topics

4.10.9 ops install file

4.10.11 script-assistant python

Function

The **script-assistant python** command configures a Python script assistant.

The **undo script-assistant python** command deletes a Python script assistant.

By default, no Python script assistant is configured.

Format

script-assistant python *script-name*

undo script-assistant python *script-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
script-name	Specifies an assistant name, namely, a Python script name for an assistant.	The value is a string of 1 to 118 case-sensitive characters without spaces. The file name extension of a Python script is .py. **NOTE** *script-name* cannot be set to the file name of a built-in Python script, such as cli.py, context.py, environment.py, farg.py, frame.py, iclog.py, interface.py, nqa.py, ops.py, route.py, snmp.py, spr.py, terminal.py, timer.py, trap.py, site.py, os.py, posixpath.py, stat.py, genericpath.py, warnings.py, linecache.py, types.py, UserDict.py, _abcoll.py, abc.py, _weakrefset.py, copy_reg.py, traceback.py, sysconfig.py, re.py, sre_compile.py, sre_parse.py, sre_constants.py, getopt.py, io.py, _pyio.py, __builtin__.py, __main__.py, _ast.py, _codecs.py, _ops.py, _sre.py, _symtable.py, _warnings.py, _weakref.py, errno.py, exceptions.py, gc.py, imp.py, marshal.py, posix.py, pwd.py, signal.py, sys.py, thread.py, xxsubtype.py, and zipimport.py.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Application Scenario

Traditional network devices provide only limited functions and predefined services, failing to meet the requirements for diversified services as the network develops.

OPS allows you to run scripts to implement customized functions, meeting these requirements.

The device supports a built-in Python script interpreter. You can run the **script-assistant python** command to run a Python script and register the events defined in the script.

Pre-configuration Tasks

The Python script has been uploaded to the device and installed using the **ops install file** command in the user view.

Precautions

- Only one assistant can be configured for a Python script.
- The system does not check correctness of the Python script.

Example

Configure an assistant for the script **config.py**.

```
<Huawei> ops install file config.py
<Huawei> system-view
[Huawei] ops
[Huawei-ops] script-assistant python config.py
Info: Succeeded in installing script assistant config.py.
```

4.10.12 shutdown script-assistant

Function

The **shutdown script-assistant** command stops an assistant.

The **undo shutdown script-assistant** command starts an assistant.

By default, an assistant is started.

Format

shutdown script-assistant *script-name*

undo shutdown script-assistant *script-name*

Parameters

Parameter	Description	Value
script-name	Specifies an assistant name, namely, a Python script name for an assistant.	The value is a string of 1 to 118 case-sensitive characters without spaces. The file name extension of a Python script is .py.

 Copyright © Huawei Technologies Co., Ltd.

Views

OPS view

Default Level

3: Management level

Usage Guidelines

Application Scenario

To prevent a Python script of an assistant from running, run the **shutdown script-assistant** command to stop the assistant.

Precautions

Stopping a running assistant interrupts the task of the assistant. Exercise caution when performing this operation.

Example

Stop an assistant for the **script config.py**.

```
<Huawei> system-view
[Huawei] ops
[Huawei-ops] shutdown script-assistant config.py
Info: Succeeded in stopping script assistant config.py.
```

 Copyright © Huawei Technologies Co., Ltd.

5 Interface Management Commands

About This Chapter

NOTE

Async interface,Serial interface, PON interface, POS interface, CPOS interface, E&M interface, ADSL interface, VDSL interface, G.SHDSL interface, IMA interface, ISDN BRI interface, 3G/LTE Cellular interface, CE1/PRI interface, CT1/PRI interface, E1-F interface, T1-F interface, and CE3 interface demand for related cards. For the mapping between the device and interface card, see Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards.

5.1 Basic Interface Configuration Commands

5.2 Ethernet Interface Configuration Commands

5.3 Serial Interface Configuration Commands

5.4 Async Interface Configuration Commands

5.5 CE1/PRI Interface Configuration Commands

5.6 CT1/PRI Interface Configuration Commands

5.7 CE3 Interface Configuration Commands

5.8 E1-F Interface Configuration Commands

5.9 T1-F Interface Configuration Commands

5.10 E&M Interface Configuration Commands

5.11 Cellular Interface Configuration Commands

5.12 ISDN BRI Interface Configuration Commands

5.13 POS Interface Commands

5.14 CPOS Interface Configuration Commands

5.15 ADSL Interface Configuration Commands

5.16 VDSL Interface Configuration Commands

5.17 G.SHDSL Interface Configuration Commands

 Copyright © Huawei Technologies Co., Ltd.

5.18 IMA Commands

5.19 PON Interface Configuration Commands

5.20 Logical Interface Configuration Commands

5.21 transparent transmission commands

5.1 Basic Interface Configuration Commands

5.1.1 bandwidth (Interface view)

Function

The **bandwidth** command sets the interface bandwidth obtained by the NMS from the MIB.

The **undo bandwidth** command restores the default configuration.

By default, the interface bandwidth obtained by the NMS from the MIB depends on the interface type. For example, the bandwidth of a GE interface is 1000 Mbit/s.

Format

bandwidth *bandwidth* [**kbps**]

undo bandwidth

Parameters

Parameter	Description	Value
bandwidth	Specifies the bandwidth of an interface.	The value is an integer ranging from 1 to 1000000, and the default unit is Mbit/s.
kbps	Indicates the unit of an interface bandwidth is kbit/s. If **kbps** is not specified, the unit of an interface bandwidth is Mbit/s.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The bandwidth command mainly ensures that the network management station (NMS) can acquire the bandwidth of an interface. The NMS can check the interface bandwidth through the two objects **ifSpeed** and **ifHighSpeed** in **IF-MIB**.

- If the configured bandwidth is smaller than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as *bandwidth* x 1000 x 1000 and *bandwidth*.
- If the configured bandwidth is equal to or larger than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as 4294967295 (0XFFFFFFFF) and *bandwidth*.

Example

Set the bandwidth of Eth1/0/0 to 100 Mbit/s.

```
<Huawei> system-view
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0] bandwidth 100
```

5.1.2 description (interface view)

Function

The **description** command configures the description for an interface.

The **undo description** command restores the default description of an interface.

By default, the description of an interface is "HUAWEI, AR Series, *interface-type interface-number* Interface".

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the interface description.	The value is a string of 1 to 242 characters. The character string is case sensitive. It can contain blanks but cannot contain the question mark (?).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate device management and maintenance, you can configure descriptions for interfaces. An interface description can contain the device where the interface is located, interface type, and remote device. For example: To-[DeviceB]Eth-2/0/0 indicates that an interface of this device is connected to Eth2/0/0 of device B.

Precautions

The interface description is displayed from the first non-space character.

Example

Configure the description of Eth2/0/0 as To-[DeviceB]Eth-2/0/0, indicating that this device is connected to device B through Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] description To-[DeviceB]Eth-2/0/0
```

Related Topics

5.1.6 display interface description

5.1.3 display default-parameter interface

Function

The **display default-parameter interface** command displays the default interface configuration.

Format

display default-parameter interface *interface-type interface-number* [*.subinterface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the default configuration of a specified interface.	-
subinterface-number	Displays the running status of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Default configurations are not saved in the configuration file. To check the default configuration of an interface, run the **display default-parameter interface** command on the interface.

The displayed information varies according to interfaces.

Example

Display the default configuration of GE1/0/0.1.

```
<Huawei> display default-parameter interface gigabitethernet 1/0/0.1
 Interface state: undo shutdown
 MTU: 1500
 Flow-stat interval: 300s
 Trap-threshold: input-rate 100, output-rate 100
 Snmp trap updown: enable
 Description: HUAWEI, AR Series, GigabitEthernet1/0/0.1 Interface
```

Table 5-1 Description of the **display default-parameter interface gigabitethernet** command output

Item	Description
Interface state:	Default status of an interface: ● shutdown ● undo shutdown To change the interface status, run the **shutdown** command or the **undo shutdown** command in the interface view.
MTU:	Default MTU value of the interface. To set the MTU value for an interface, run the **mtu** command in the interface view.
Flow-stat interval:	Interval for collecting traffic statistics on the interface. To set the interval for collecting traffic statistics on an interface, run the **set flow-stat interval** command in the interface view.
Trap-threshold:	Alarm threshold for outbound and inbound bandwidth usage on the interface. To set the alarm threshold for outbound and inbound bandwidth usage on an interface, run the **trap-threshold** command in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Snmp trap updown:	Whether an alarm is sent to the NMS when the interface status changes: ● disable: No alarm is sent to the NMS when the interface status changes. ● enable: An alarm is sent to the NMS when the interface status changes. To configure an interface to send an alarm to the NMS when the interface status changes, run the **enable snmp trap updown** command in the interface view.
Description:	Interface description. To configure the description for an interface, run the **5.1.2 description (interface view)** command in the interface view.

Display the default configuration of Dialer1.

```
<Huawei> display default-parameter interface dialer 1
 MTU: 1500
 Timer hold: 10s
 Flow-stat interval: 300s
 Description: HUAWEI, AR Series, Dialer1 Interface
```

Table 5-2 Description of the **display default-parameter interface dialer** command output

Item	Description
MTU:	Default MTU value of the interface. To set the MTU value for an interface, run the **mtu** command in the interface view.
Timer hold:	Polling interval of the link layer protocol applied to the interface. To set the polling interval for an interface, run the **timer hold** command in the interface view.
Flow-stat interval:	Interval for collecting traffic statistics on the interface. To set the interval for collecting traffic statistics on an interface, run the **set flow-stat interval** command in the interface view.
Description:	Interface description. To configure the description for an interface, run the **5.1.2 description (interface view)** command in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

5.1.4 display interface

Function

The **display interface** command displays the interface running status and statistics.

Format

display interface [*interface-type* [*interface-number* [.*subinterface-number*] | **main**] | **main**]

display interface slot *slot-id* [**main**]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the running status of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.	-
subinterface-number	Displays the running status of a sub-interface.	The value is an integer that ranges from 1 to 4096.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
main	Displays running status and traffic statistics about an interface. ● If an interface has no sub-interfaces, status and traffic statistics about the interface are displayed whether you specify the **main** parameter or not. ● If an interface has sub-interfaces, status and traffic statistics about the interface and sub-interfaces are displayed if you do not specify the **main** parameter.	-
slot *slot-id*	Specifies the slot ID.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The running status and statistics of an interface includes the physical status, basic configuration, and packet forwarding of the interface. You can use the **display interface** command to collect traffic statistics or locate faults on an interface.

Precautions

If no interface type is specified, the running status and statistics of all the interfaces is displayed. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.

Example

Display the running status, basic configuration, and packet forwarding on Layer 2 Ethernet interface Ethernet2/0/0.

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
```

```
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Switch Port, PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
Last physical up time   : 2010-07-21 15:35:37
Last physical down time : 2010-07-20 01:06:25
Current system time: 2010-07-21 16:07:53-05:13
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO,  Clock   : -
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

Input:  126 packets, 34204 bytes
  Unicast:              0,  Multicast:              52
  Broadcast:           74,  Jumbo:                     0
  Discard:              0,  Total Error:             0

  CRC:                 0,  Giants:                 0
  Jabbers:              0,  Throttles:              0
  Runts:               0,  Symbols:                0
  Ignoreds:             0,  Frames:                 0

Output:  2398 packets, 799486 bytes
  Unicast:              0,  Multicast:            1461
  Broadcast:         1477,  Jumbo:                    0
  Discard:              0,  Total Error:            53

  Collisions:          32,  ExcessiveCollisions:      21
  Late Collisions:      0,  Deferreds:              0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-3 Description of the **display interface** command output

Item	Description
current state	Current interface status: ● DOWN: indicates that the interface is disabled. ● UP: indicates that the interface is enabled.
Line protocol current state	Link layer protocol status of the interface: ● DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
PVID	Default VLAN ID of the interface.
The Maximum Frame Length	Maximum frame length allowed by the interface.

Item	Description
IP Sending Frames' Format	Format of the frame contained in the sent IP packet, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the device.
Last physical up time	Last time the interface goes Up physically. If this field displays "-", the physical status of the interface does not change.
Last physical down time	Last time the interface goes Down physically. If this field displays "-", the physical status of the interface does not change.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH: MM: SS UTC±HH: MM DST format.
Port Mode	Working mode of the common interface: ● COMMON COPPER: The interface is an electrical interface. ● COMMON FIBER: The interface is an optical interface. Run **combo-port**. The working mode of the combo interface is configured. ● AUTO: The combo interface automatically select the working mode. ● AUTO FIBER: The combo interface automatically select optical working mode. ● AUTO COPPER: The combo interface automatically select electrical working mode. ● FORCE FIBER: The combo interface is configured as an optical interface. ● FORCE COPPER: The combo interface is configured as an electrical interface.
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto negotiation mode, the **speed** command configures the rate of an interface.
Loopback	Loopback configuration of the interface. The **loopback** command configures loopback on an interface.
Duplex	Duplex mode of the interface.
Negotiation	Auto-negotiation mode of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mdi	Network cable type of the interface.
Clock	Clock mode of the combo interface.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Jumbo	Number of jumbo frames received or sent by the interface.
Discard	Number of packets discarded by the interface during physical layer detection. These packets are discarded because the interface is congested. The device does not support the **Discard** field for Layer 2 Ethernet interfaces.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of CRC error packets received by the interface.
Giants	Number of jumbo frames with correct Frame Check Sequence (FCS) received by the interface. **NOTE** For the AR109, AR109W, AR109GW-L, AR121, AR121W, AR121GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, this item indicates the number of received packets with length exceeding the maximum jumbo frame size.
Jabbers	Number of jumbo frames with incorrect FCS received by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Throttles	Number of undersized frames with incorrect FCS received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Runts	Number of undersized frames with correct FCS values received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames with OpCode not being PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of frames that the interface stops sending when conflicts are detected during transmission.
ExcessiveCollisions	Number of frames that experience more than 16 consecutive conflict events and fail to be sent.
Late Collisions	Number of frames that experience conflict events and are delayed. The first 512 bits of these frames have been sent but these frames are delay because conflicts are detected.
Deferreds	Number of packets delayed because conflicts are detected before transmission.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Display the running status, basic configuration, and packet forwarding on Layer 3 Ethernet interface Ethernet2/0/0.

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.4.2/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
```

```
Last physical up time   : 2010-09-08 15:35:37
Last physical down time : 2010-09-08 01:06:25
Current system time: 2010-10-21 16:07:53
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO,  Clock   : -
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

Input:  126 packets, 34204 bytes
  Unicast:                0,  Multicast:                52
  Broadcast:             74,  Jumbo:                     0
  Discard:                0,  Total Error:               0

  CRC:                    0,  Giants:                    0
  Jabbers:                0,  Throttles:                 0
  Runts:                  0,  Symbols:                   0
  Ignoreds:               0,  Frames:                    0

Output:  2398 packets, 799486 bytes
  Unicast:                0,  Multicast:             1461
  Broadcast:           1477,  Jumbo:                     0
  Discard:                0,  Total Error:              53

  Collisions:            32,  ExcessiveCollisions:      21
  Late Collisions:        0,  Deferreds:                0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-4 Description of the **display interface** command output

Item	Description
current state	Current interface status: ● DOWN: indicates that the interface is disabled. ● UP: indicates that the interface is enabled.
Line protocol current state	Link layer protocol status of the interface: ● DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
The Maximum Transmit Unit is	MTU of the interface. For example, the default MTU of an Ethernet interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet Address is	IP address and mask length of the interface. The displayed information varies according to the IP address allocation mode: ● If the IP address is manually configured, the information is displayed as "Internet Address is 192.168.4.2/24." ● If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 192.168.4.2/24."
IP Sending Frames' Format	Format of the frame contained in the sent IP packet, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the device.
Last physical up time	Last time the interface goes Up physically. If this field displays "-", the physical status of the interface does not change.
Last physical down time	Last time the interface goes Down physically. If this field displays "-", the physical status of the interface does not change.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH: MM: SS UTC±HH: MM DST format.
Port Mode	Working mode of the interface: ● COMMON COPPER: The interface works as an electrical interface. ● COMMON FIBER: The interface works as an optical interface. If the interface is a combo interface: ● COMBO AUTO: The combo interface automatically selects the working mode. ● FORCE FIBER: The combo interface is configured as an optical interface. ● FORCE COPPER: The combo interface is configured as an electrical interface. To configure the working mode for an interface, run the **combo-port** command.
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto negotiation mode, the **speed** command configures the rate of an interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Loopback	Loopback configuration of the interface. To configure loopback on an interface, run the **loopback** command.
Duplex	Duplex mode of the interface.
Negotiation	Auto-negotiation mode of the interface.
Mdi	Network cable type of the interface.
Clock	Clock mode of the combo interface.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Jumbo	Number of jumbo frames received or sent by the interface. If the value is -, the number of jumbo frames cannot be collected on the device. **NOTE** Only interfaces of AR2220 MPUs support this statistical item.
Discard	Number of packets discarded by the interface during physical layer detection. These packets are discarded because the interface is congested. **NOTE** Only Layer 3 Ethernet interfaces of AR201, AR1220 and AR2220 MPUs support this statistical item.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of CRC error packets received by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Giants	Number of jumbo frames with correct FCS received by the interface. **NOTE** For the AR109, AR109W, AR109GW-L, AR121, AR121W, AR121GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, this item indicates the number of received packets with length exceeding the maximum jumbo frame size.
Jabbers	Number of jumbo frames with incorrect FCS received by the interface.
Throttles	Number of undersized frames with incorrect FCS received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Runts	Number of undersized frames with correct FCS values received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames with OpCode not being PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of frames that the interface stops sending when conflicts are detected during transmission.
ExcessiveCollisions	Number of frames that experience more than 16 consecutive conflict events and fail to be sent.
Late Collisions	Number of frames that experience conflict events and are delayed. The first 512 bits of these frames have been sent but these frames are delay because conflicts are detected.
Deferreds	Number of packets delayed because conflicts are detected before transmission.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Display the packet forwarding on dialer1 interface.

```
<Huawei> display interface dialer 1
Dialer1 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Dialer1 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 0(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is Dialer
Current system time: 2017-12-08 23:02:15
    Input: 8837 packets, 851857 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 11358 bits/sec, 14 packets/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 65350 bits/sec,Record time: 2017-12-06 04:16:23
Output peak rate 0 bits/sec,Record time: -


ipv4
    Input: 8837 packets, 851857 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 0 bits/sec, 0 packets/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 65350 bits/sec,Record time: 2017-12-06 04:16:23
Output peak rate 0 bits/sec,Record time: -


ipv6
    Input: 0 packets, 0 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 30744573456171227 bits/sec, 30744573456182571 packet
s/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-5 Description of the **display interface** command output

Item	Description
current state	Current interface status: ● DOWN: indicates that the interface is disabled. ● UP: indicates that the interface is enabled.

Item	Description
Line protocol current state	Link layer protocol status of the interface. ● DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
The Maximum Transmit Unit is	MTU of the interface. For example, the default MTU of an Ethernet interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
Internet Address is	IP address and mask length of the interface. The displayed information varies according to the IP address allocation mode: ● For a statically configured IP address: Internet Address is 192.168.4.2/24 If the IP address is statically configured, the information is displayed as "Internet Address is 192.168.4.2/24". ● If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 192.168.4.2/24".
IP Sending Frames' Format	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address	MAC address of the device.
Input	Total number of received packets.
Output	Total number of sent packets.
Last 600 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 600 seconds.
Last 600 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 600 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
ipv4	Number of IPv4 packets.
ipv6	Number of IPv6 packets.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Related Topics

5.1.2 description (interface view)

5.1.16 shutdown (interface view)

5.1.5 display interface brief

Function

The **display interface brief** command displays brief information about the status and configuration of interfaces.

Format

display interface brief [**main**]

Parameters

Parameter	Description	Value
main	Displays brief information about an Ethernet main interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface brief** command displays brief information about interfaces, including the physical status, link layer protocol status, inbound and outbound bandwidth usage within a certain period, and numbers of sent and received error packets. This information helps locate faults on interfaces.

Precautions

To clear statistics on an interface, run the **reset counters interface** command.

Example

Display brief information about the status and configuration of interfaces.

```
<Huawei> display interface brief
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
^down: standby
(e): ETHOAM down
InUti/OutUti: input utility/output utility
Interface                   PHY   Protocol InUti OutUti   inErrors  outErrors
Dialer1                     up    up(s)     0%     0%         0         0
Eth-Trunk18                 down  down      0%     0%         0         0
Ethernet1/0/0               up    up      0.01%  0.01%        0         0
Ethernet1/0/1               down  down      0%     0%         0         0
GigabitEthernet0/0/0        up    up      0.01%  0.01%        0         0
GigabitEthernet0/0/1        *down down      0%     0%         0         0
GigabitEthernet0/0/1.1      down  down      0%     0%         0         0
LoopBack0                   up    up(s)     0%     0%         0         0
NULL0                       up    up(s)     0%     0%         0         0
Tunnel0/0/0                 up    down      --     --         0         0
Tunnel0/0/1                 up    down      --     --         0         0
Virtual-Ethernet0/0/0       down  down      0%     0%         0         0
Virtual-Template0           up    down      0%     0%         0         0
Virtual-Template1           up    down      0%     0%         0         0
Virtual-Template2           up    down      0%     0%         0         0
Vlanif1                     down  down      --     --         0         0
Vlanif2                     down  down      --     --         0         0
Vlanif3                     up    up        --     --         0         0
Vlanif10                    down  down      --     --         0         0
```

Table 5-6 Description of the **display interface brief** command output

Item	Description
Interface	Type and number of an interface. If **(v)** is displayed behind an interface number, the interface is a virtual interface.

Item	Description
PHY	Physical status of an interface: ● up: indicates that the interface is working properly. ● down: indicates that the physical layer of the interface fails. ● *down: Administratively Down, indicating that the administrator has run the **shutdown** command on the interface. ● ^down: indicates that the interface is a backup interface. ● (l): indicates that the loopback function is enabled on the interface. ● (s): indicates that the spoofing function is enabled on the interface. ● (b): indicates that the link layer of the interface is in BFD Down state. ● (e): indicates that the link layer of the interface is in EFM Down state.
Protocol	Link layer protocol status of the interface: ● up: indicates that the interface is working properly. ● down: indicates that the link layer protocol of the interface fails. ● (s): indicates that the spoofing function is enabled on the interface. ● (b): indicates that the link layer of the interface is in BFD Down state. ● (e): indicates that the link layer of the interface is in EFM Down state. ● (d): indicates that the protocol module of the interface is suppressed. ● --: indicates that the link layer protocol status is not obtained.
InUti	Average inbound bandwidth usage of an interface within the last 300 seconds. Average inbound bandwidth usage within the last 300 seconds = Average inbound traffic rate within the last 300 seconds/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and greater than 0, the value 0.01% is displayed. When the interface bandwidth becomes lower, for example, the **speed** command is executed to reduce the bandwidth of an Ethernet interface, the bandwidth usage may be displayed as 100% because the traffic volume is not adjusted in time. "--" indicates that an interface does not support the display of bandwidth usage.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
OutUti	Average outbound bandwidth usage within the last 300 seconds. Average outbound bandwidth usage within the last 300 seconds = Average outbound traffic rate within the last 300 seconds/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and greater than 0, the value 0.01% is displayed. When the interface bandwidth becomes lower, for example, the **speed** command is executed to reduce the bandwidth of an Ethernet interface, the bandwidth usage may be displayed as 100% because the traffic volume is not adjusted in time. "--" indicates that an interface does not support the display of bandwidth usage.
inErrors	Number of error packets received by an interface. The value becomes 0 when you run the **reset counters interface** command in the user view or when the number of received packets reaches the maximum value 0xFFFFFFFF.
outErrors	Number of error packets sent by an interface. The value becomes 0 when you run the **reset counters interface** command in the user view or when the number of sent packets reaches the maximum value 0xFFFFFFFF.

Related Topics

5.1.4 display interface

5.1.13 reset counters interface

5.1.6 display interface description

Function

The **display interface description** command displays the description of an interface.

Format

display interface description [*interface-type* [*interface-number*]]

display interface description [*interface-type*] [**main**]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the description of a specified interface. If an interface type is specified but no interface number is specified, the description of all interfaces of the specified type is displayed.	-
main	Displays the description of the main interface. ● If an interface has no sub-interfaces, description about the interface are displayed whether you specify the **main** parameter or not. ● If an interface has sub-interfaces, description about the interface and sub-interfaces are displayed if you do not specify the **main** parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display interface** command can also display the description of an interface. To quickly view the description of an interface, you are advised to use the **display interface description** command.

If no interface type is specified, the description of all interfaces is displayed. If an interface type is specified but no interface number is specified, the description of all interfaces of the specified type is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the description of Eth2/0/0.

```
<Huawei> display interface description ethernet 2/0/0
PHY: Physical
*down: administratively down
(l): loopback
(s): spoofing
(b): BFD down
^down: standby
(e): ETHOAM down
(v): VirtualPort
Interface                 PHY     Protocol Description
Eth2/0/0                   *down   down     HUAWEI, AR Series, Ethernet2/0/0 Interface
```

Table 5-7 Description of the **display interface description** command output

Item	Description
Interface	Type and number of an interface. If **(v)** is displayed behind an interface number, the interface is a virtual interface.
PHY	Physical status of an interface: • up: indicates that the interface is working properly. • down: indicates that the physical layer of the interface fails. • *down: Administratively Down, indicating that the administrator has run the **shutdown** command on the interface. • ^down: indicates that the interface is a backup interface. • (l): indicates that the loopback function is enabled on the interface. • (b): indicates that the physical layer of the interface is in BFD Down state.
Protocol	Link layer protocol status of the interface: • up: indicates that the interface is working properly. • down: indicates that the link layer protocol of the interface fails. • (l): indicates that the loopback function is enabled on the interface. • (s): indicates that the spoofing function is enabled on the interface. • (b): indicates that the link layer of the interface is in BFD Down state. • (e): indicates that the link layer of the interface is in EFM Down state. • --: indicates that the link layer protocol status of the interface is not obtained.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Description	Interface description.

Related Topics

5.1.2 description (interface view)

5.1.7 display ip interface description

Function

The **display ip interface description** command displays IP-related information (such as the IP address, subnet mask, physical layer status, link layer protocol status, and number of interfaces in different states) and description of an interface.

Format

display ip interface description [*interface-type* [*interface-number*] | *interface-type* &<1-8>] | **slot** *slot-number*]

Parameters

Parameter	Description	Value
interface-type	Indicates the interface type. If no interface type is specified, IP-related configurations and statistics of all interfaces are displayed.	-
interface-number	Indicates the interface number, which is used together with *interface-type* to identify an interface. If no interface number is specified, IP-related configurations and statistics of interfaces in the same type are displayed.	-
interface-type	Indicates that the command can display IP-related information about interfaces of multiple types. The command can display IP-related information about interfaces in a maximum of eight types.	-
slot *slot-number*	Specifies the interface board number.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Instead of running the **display ip interface brief** and **display interface description** commands, you can run the **display ip interface description** command to view both IP-related information and description of an interface, which facilitates the user operation.

Example

View IP-related information and description of a specified interface.

```
<Huawei> display ip interface description
Codes:
     Ana(Analogmodem),       Asy(Async),             Cell(Cellular),
     Dia(Dialer),            Eth(Ethernet)           GE(GigabitEthernet),
     H(Hssi),                Ima(Ima-group),         Loop(LoopBack),
     MTun(MTunnel),          S(Serial),              Tun(Tunnel),
     VE(Virtual-Ethernet),   VT(Virtual-Template)

     d(dampened),            D(down),                *D(administratively down),
     ^D(standby),            l(loopback),            s(spoofing),
     U(up),                  E(E-Trunk down)
--------------------------------------------------------------------------------
Number of interfaces whose physical status is Up: 7
Number of interfaces whose physical status is Down: 4
Number of interfaces whose protocol status is Up: 4
Number of interfaces whose protocol status is Down: 7

Interface                    IP Address/Mask    Phy   Prot Description
Atm2/0/0                      unassigned         D     D
Eth1/0/0                      unassigned         U     D
Eth1/0/1                      10.1.1.2/24        U     U
GE0/0/0                       192.168.200.174/24 U     U
GE0/0/1                       unassigned         U     D
GE0/0/2                       unassigned         U     D
S6/0/0                        unassigned         U     U    NULL0
```

Table 5-8 Description of the **display ip interface description** command output

Item	Description
Codes:	The following information provides the full spelling and explanation of the abbreviated interface names, physical status, and link layer protocols. ● Full spelling of the abbreviated interface names is as follows: – Ana: Analog modem interfaces – Asy: Async interfaces – Cell: Cellular interfaces – Dia: Dialer interfaces – Eth: Ethernet interfaces – GE: Gigabit Ethernet interfaces – H: Hssi interfaces – Ima: IMA-Group interfaces – Loop: Loopback interfaces – MTun: MTunnel interfaces – S: Serial interfaces – Tun: Tunnel interfaces – VE: Virtual-Ethernet interfaces – VT: Virtual-Template interfaces ● Explanation of the abbreviated physical status of the interface is as follows: – U: indicates that the physical status of the interface is Up.U(l) indicates that the interface is enabled with the loopback function. – D: indicates that the physical status of the interface is Down. – *D: indicates that the network administrator has run the **shutdown** command on the interface. – ^D: indicates that the FIB module is in the standby state. – s: indicates that the interface is in spoofing status. – E: indicates the physical status of the Eth-Trunk. ● Explanation of the abbreviated link layer protocol status is as follows: – U: indicates that the status of the link layer protocol on the interface is Up.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	U(s) indicates that the link layer protocol of the interface is Up even though the interface is not configured with an IP address. (s) is an inherent attribute of the interface and will be displayed when the interface is configured with an IP address. (d) indicates that the protocol module of the interface is dampened. – D: indicates that the link layer protocol of the interface is Down or no IP address is assigned to the interface.
Number of interfaces whose physical status is Up:	Indicates the number of interfaces whose physical status is Up.
Number of interfaces whose physical status is Down:	Indicates the number of interfaces whose physical status is Down.
Number of interfaces whose protocol status is Up:	Indicates the number of interfaces whose link layer protocol is Up.
Number of interfaces whose protocol status is Down:	Indicates the number of interfaces whose link layer protocol is Down.
Interface	Indicates the name and number of an interface.
IP Address/Mask	Indicates the IP address and subnet mask of an interface.
Phy	Indicates the physical status of an interface.
Prot	Indicates the link layer protocol status of an interface.
Description	Indicates the description of an interface, expressed in characters. A maximum of 20 characters can be displayed. When the length of the description is greater than 20 characters, only the first 16 characters are displayed and the last 3 characters are replaced by ellipsis (...). If the description of an interface is the default setting, no information is displayed.

Related Topics

5.1.4 display interface

5.1.8 display interface counters

Function

The **display interface counters** command displays packet statistics on physical interfaces.

Format

display interface [*interface-type*] **counters** { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
interface-type	Displays statistics about packets sent and received by an interface.	-
inbound	Displays statistics about packets received by an interface.	-
outbound	Displays statistics about packets sent by an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface counters** command can be used when you need to:

- Check whether an interface is sending and receiving packets normally during interface fault diagnosis.
- Collect traffic statistics on an interface.
- Check whether an interface can send and receive multicast packets after the multicast function is configured.

If no interface type is specified, the statistics of packets sent and received by all interfaces are displayed. If an interface type is specified but no interface number is specified, the statistics about packets sent and received by all interfaces of this type are displayed.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

If you want to collect new traffic statistics, run the **reset counters interface** command to clear the current statistics.

Example

Display statistics about packets received by an interface.

```
<Huawei> display interface gigabitethernet counters inbound
Interface          Total      UniCast     MultiCast     BroadCast      Err
                 (pkts)       (pkts)       (pkts)       (pkts)   (pkts)
GE0/0/0            45403         8196        11094         26113       0
GE0/0/1                0            0            0             0       0
GE0/0/2             2778            0            0          2778       0
GE7/0/0                0            0            0             0       0
GE7/0/1                0            0            0             0       0
GE7/0/2                0            0            0             0       0
GE7/0/3                0            0            0             0       0
GE7/0/4                0            0            0             0       0
GE7/0/5            47182            1        47176             5       0
GE7/0/6                0            0            0             0       0
GE7/0/7                0            0            0             0       0
GE7/0/8                0            0            0             0       0
GE7/0/9                0            0            0             0       0
GE7/0/10               0            0            0             0       0
GE7/0/11               0            0            0             0       0
GE7/0/12               0            0            0             0       0
GE7/0/13               0            0            0             0       0
GE7/0/14               0            0            0             0       0
GE7/0/15               0            0            0             0       0
GE7/0/16               0            0            0             0       0
GE7/0/17               0            0            0             0       0
GE7/0/18               0            0            0             0       0
GE7/0/19               0            0            0             0       0
GE7/0/20               0            0            0             0       0
GE7/0/21               0            0            0             0       0
GE7/0/22               0            0            0             0       0
GE7/0/23               0            0            0             0       0

NOTICE
  OverFlow :more than 14 decimal digits (8 digits for column "Err").
       -- :not supported.
```

Table 5-9 Description of the **display interface counters** command output

Item	Description
Interface	Type and number of an interface.
Total	Total number of packets sent and received by an interface.
UniCast	Number of unicast packets sent or received by an interface.
MultiCast	Number of multicast packets sent or received by an interface.
BroadCast	Number of broadcast packets sent or received by an interface.
Err	Number of error packets sent or received by an interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

5.1.4 display interface

5.1.5 display interface brief

5.1.9 display ip interface

Function

The **display ip interface** command displays the IP configuration and statistics on interfaces. The statistics include the number of packets and bytes received and sent by interfaces, number of multicast packets sent and received by interfaces, and number of broadcast packets received, sent, forwarded, and discarded by interfaces.

The **display ip interface brief** command displays brief information about interface IP addresses, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.

Format

display ip interface [*interface-type interface-number*]

display ip interface brief [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]]

display ip interface brief [*interface-type*] &<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If no interface is specified, IP configuration and statistics about all interfaces are displayed.	-
brief	Displays brief information, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.	-
slot *slot-id*	Displays the IP configuration and statistics of interfaces on the specified slot. If the slot number is not specified, brief information related to the IP addresses of the interfaces on all interface boards and main control boards is displayed.	-
card *card-number*	Displays the IP configuration and statistics of interfaces on specified card.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip interface brief** command to view the following information:

- IP configurations of all interfaces
- IP configurations of interfaces of the specified type and a specified interface
- IP configurations of interfaces that have IP addresses

This command, however, cannot display the IP configurations of Layer 2 interfaces or Eth-Trunk member interfaces.

NOTE

- You can run the **display interface description** command to view the interface description.
- You can run the **display interface** command to view detailed information about the running status and statistics on the interface.

Example

Display the IP configuration and statistics on GE0/0/0.

```
<Huawei> display ip interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 1431, bytes : 97912, multicasts : 1426
output packets : 2716, bytes : 179760, multicasts : 2710
Directed-broadcast packets:
 received packets:          0, sent packets:          0
 forwarded packets:         0, dropped packets:          0
ARP packet input number:         11
  Request packet:                11
  Reply packet:                  0
  Unknown packet:                  0
Internet Address is 10.5.40.1/24
Broadcast address : 10.5.40.255
TTL being 1 packet number:        0
TTL invalid packet number:        0
ICMP packet input number:         0
  Echo reply:                    0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:                 0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
```

Table 5-10 Description of the **display ip interface** command output

Item	Description
GigabitEthernet1/0/0 current state	Physical status of GigabitEthernet1/0/0: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively DOWN: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: The link layer protocol of the interface is running properly. ● DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface.
The Maximum Transmit Unit	MTU of the interface. The default MTU of an Ethernet interface is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
input packets : 1431, bytes : 97912, multicasts : 1426	Total number of packets, bytes, and multicast packets received by the interface.
output packets : 2716, bytes : 179760, multicasts : 2710	Total number of packets, bytes, and multicast packets sent by the interface.
Directed-broadcast packets	Number of packets broadcast on the interface directly.
received packets	Total number of received packets.
sent packets	Total number of sent packets.
forwarded packets	Total number of forwarded packets.
dropped packets	Total number of discarded packets.
ARP packet input number	Number of received ARP packets.
Request packet	Number of request packets.
Reply packet	Number of response packets.
Unknown packet	Number of unknown packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet Address is	IP address and subnet mask of the interface. The displayed information varies according to the IP address allocation mode: ● If the IP address is manually configured, the information is displayed as "Internet Address is 10.5.40.1/24." ● If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 10.5.40.1/24."
Broadcast address	Broadcast address of an interface.
TTL being 1 packet number	Number of packets with TTL 1.
TTL invalid packet number	Number of packets with invalid TTL.
ICMP packet input number	Number of received ICMP packets.
Echo reply	Number of Echo Reply packets.
Unreachable	Number of Destination Unreachable packets.
Source quench	Number of Source Quench packets.
Routing redirect	Number of Redirect packets.
Echo request	Number of Echo Request packets.
Router advert	Number of Router Advertisement packets.
Router solicit	Number of Router Solicitation packets.
Time exceed	Number of Time Exceeded packets.
IP header bad	Number of IP header error packets.
Timestamp request	Number of Timestamp Request packets.
Timestamp reply	Number of Timestamp Reply packets.
Information request	Number of Information Request packets.
Information reply	Number of Information Reply packets.
Netmask request	Number of Address Mask Request packets.
Netmask reply	Number of Address Mask Reply packets.
Unknown type	Number of unknown packets.

Display brief IP information about all interfaces.

```
<Huawei> display ip interface brief
*down: administratively down
^down: standby
(l): loopback
```

```
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 3
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 3

Interface                   IP Address/Mask      Physical   Protocol
Atm0/0/0                      unassigned          down       down
Bridge-if10                   unassigned          down       down
MFR0/0/1                      unassigned          down       down
NULL0                         unassigned          up         up(s)
Vlanif1                     192.168.200.161/24   up         up
```

Table 5-11 Description of the **display ip interface brief** command output

Item	Description
*down:	Reason why an interface is physically Down. Administratively down indicates that the administrator has run the **shutdown** command on the interface.
^down: standby	Indicates that the interface is a backup interface.
(l): loopback	Indicates that the loopback function is enabled on the interface.
(s): spoofing	Indicates that the spoofing function is enabled on the interface.
(E): E-Trunk down	Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk.
The number of interface that is UP/DOWN in Physical is	Up or Down state of a physical link and number of interfaces in different states.
The number of interface that is UP/DOWN in Protocol is	Up or Down state of the protocol and number of interfaces in different states.
Interface	Interface type and number.
IP Address/ Mask	IP address and subnet mask of an interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Physical	Physical status of an interface: ● Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface. ● Down: indicates that the interface becomes faulty. ● *down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. (l) indicates that the loopback function is configured on the interface. ● !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down.
Protocol	Link protocol status of the interface: ● Up: indicates that the link protocol of the interface is running properly. (s) indicates that the link protocol status of the interface is Up when this interface is created and has no IP address configured. This is an inherent attribute of an interface. When this interface is configured with an IP address, (s) is still displayed. ● Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface. (l) indicates that the loopback function is configured on the interface.

Related Topics

5.1.4 display interface

5.1.10 display this interface

Function

The **display this interface** command displays interface information in the current interface view.

Format

display this interface

Parameters

None

Views

Interface view

Default Level

1: Monitoring level

Usage Guidelines

In the interface view, you can run the **display this interface** command to rapidly view the status of the interface and packet statistics on the interface.

Example

Display information about Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] display this interface
Ethernet2/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Switch Port, PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0819-a6cd-a894
Last physical up time   : 2012-09-10 10:26:36
Last physical down time : 2012-09-10 10:21:00
Current system time: 2012-09-12 16:56:03
Port Mode: COMMON COPPER
Speed : 1000,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO,  Clock   : -
Last 300 seconds input rate 152 bits/sec, 0 packets/sec
Last 300 seconds output rate 648 bits/sec, 0 packets/sec
Input peak rate 1872 bits/sec,Record time: 2012-09-12 10:21:53
Output peak rate 2248 bits/sec,Record time: 2012-09-10 10:26:42

Input:  793 packets, 463059 bytes
  Unicast:                0,  Multicast:              793
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Total Error:              0

  CRC:                    0,  Giants:                   0
  Jabbers:                0,  Throttles:                0
  Runts:                  0,  Symbols:                  0
  Ignoreds:               0,  Frames:                   0

Output:  104596 packets, 15863891 bytes
  Unicast:                0,  Multicast:           104596
  Broadcast:              0,  Jumbo:                    0
  Discard:                0,  Total Error:              0

  Collisions:             0,  ExcessiveCollisions:      0
  Late Collisions:        0,  Deferreds:                0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization : 0.01%
```

 Copyright © Huawei Technologies Co., Ltd.

Table 5-12 Description of the **display this interface** command output

Item	Description
current state	Current interface status: ● DOWN: indicates that the interface is disabled. ● UP: indicates that the interface is enabled. ● Administratively Down: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description.
PVID	Default VLAN ID of the interface.
TPID	Type of frames that are supported on the interface. By default, this field displays 0x8100, indicating an 802.1Q frame. If the device does not support 802.1Q frames, the interface discards the 802.1Q frames immediately after receiving them. This field is displayed only for a Layer 2 interface.
The Maximum Frame Length	Maximum frame length allowed by the interface.
IP Sending Frames' Format	Format of the frame contained in the sent IP packet, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the device.
Last physical up time	Last time the interface went Up physically. If this field displays "-", the physical status of the interface does not change.
Last physical down time	Last time the interface went Down physically. If this field displays "-", the physical status of the interface does not change.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Speed	Current rate of an interface.
Loopback	Loopback configuration of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Duplex	Duplex mode of the interface.
Negotiation	Auto-negotiation mode of the interface.
Mdi	Network cable type of the interface.
Clock	Clock mode of the combo interface.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Jumbo	Number of jumbo frames received or sent by the interface.
Discard	Number of packets discarded by the interface during physical layer detection.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of CRC error packets received by the interface.
Giants	Number of jumbo frames with the correct FCS received by the interface. **NOTE** For the AR109, AR109W, AR109GW-L, AR121, AR121W, AR121GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, this item indicates the number of received packets with length exceeding the maximum jumbo frame size.
Jabbers	Number of jumbo frames with incorrect FCS received by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Throttles	Number of undersized frames with incorrect FCS received by the interface.
Runts	Number of undersized frames with the correct FCS received by the interface.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames with OpCode not being PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of sent packets with 1 to 15 conflict events.
ExcessiveCollisions	Number of packets with 16 conflict events and failing to be sent.
Late Collisions	Number of packets with conflict and delayed.
Deferreds	Number of delayed packets without conflict.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Related Topics

5.1.4 display interface
5.1.5 display interface brief

5.1.11 interface

Function

The **interface** command displays the interface view or sub-interface view.

Format

interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. The interface type and number can be closely next to each other or separated by a space character. ● To create a sub-interface or enter a sub-interface view, specify *interface-number* in the format of main interface number.sub-interface number. For example, the number of sub-interface 1 on GE1/0/0 is GE1/0/0.1. ● To create a channelized interface or enter the view of a channelized interface, specify *interface-number* in the format of main interface number: channelized interface number. For example, the number of channelized interface 1 on E1 2/0/0 is Serial2/0/0:1.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the specified interface view is displayed, you can set attributes for the interface.

Precautions

- The **interface** command can display only the view of an existing physical interface and cannot create a physical interface.
- The **interface** command can create a logical interface and display the view of the logical interface.

Example

Display the view of Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0]
```

Display the view of MEth interface.

```
<Huawei> system-view
[Huawei] interface MEth 0/0/0
[Huawei-MEth0/0/0]
```

Related Topics

5.1.4 display interface

5.1.12 reset counters if-mib interface

Function

The **reset counters if-mib interface** command clears interface traffic statistics in the Network Management System (NMS).

Format

reset counters if-mib interface [*interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Clears traffic statistics on a specified interface in the NMS. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on a specific interface within a period in the NMS, clear existing traffic statistics on this interface in the NMS.

NOTE

For details on how to view interface traffic statistics in the NMS, see the NMS documentation.

Precautions

- If no interface type and number are specified, traffic statistics of all interfaces in the NMS are cleared.
- After you run the **reset counters if-mib interface** command, traffic statistics on all interfaces in the NMS are cleared. Therefore, confirm the action before you run this command.

 Copyright © Huawei Technologies Co., Ltd.

- Running the **reset counters if-mib interface** command does not affect the interface traffic statistics displayed by the **display interface** command. To clear the interface traffic statistics displayed by the **display interface** command, run the **reset counters interface** command.

Example

Clear traffic statistics on Eth2/0/0 in the NMS.

```
<Huawei> reset counters if-mib interface ethernet 2/0/0
```

Related Topics

5.1.13 reset counters interface

5.1.13 reset counters interface

Function

The **reset counters interface** command clears traffic statistics about a specified interface.

Format

reset counters interface [*interface-type* [*interface-number*]]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Clears traffic statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting traffic statistics on an interface within a certain period, run the **reset counters interface** command to clear existing traffic statistics.

Precautions

- Statistics cannot be restored after being cleared. Therefore, exercise caution before clearing the statistics.
- Traffic accounting is based on the packet statistics on an interface. The clearing of the packet statistics on an interface by using the **reset counters interface** command affects the traffic accounting result. Therefore, do not randomly clear the packet statistics on an interface in a normal application environment.
- If no interface type is specified, traffic statistics on all types of interfaces are cleared. If an interface type is specified but no interface number is specified, traffic statistics on all interfaces of the specified type are cleared.
- Running the **reset counters interface** command clears the statistics about received and transmitted packets on the interface in a certain period. The certain period is configured by using the **set flow-stat interval** *interval-time* command.

Example

Clear traffic statistics on all interfaces.

```
<Huawei> reset counters interface
```

Clear traffic statistics on VLANIF10.

```
<Huawei> reset counters interface vlanif 10
```

Related Topics

5.1.4 display interface
5.1.5 display interface brief

5.1.14 restart (interface view)

Function

The **restart** command restarts an interface.

Format

restart

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying parameters of an interface, run the **restart** command to make the modification take effect.

Precautions

- Restarting an interface during data transmission will cause data frame loss or service interruption. Exercise caution when you use the **restart** command.
- Running the **restart** command is equivalent to running the **shutdown** command and the **undo shutdown** command in sequence.

Example

Restart Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] restart
```

Related Topics

5.1.16 shutdown (interface view)

5.1.15 set flow-stat interval

Function

The **set flow-stat interval** command sets the interval for collecting the traffic statistics on interfaces.

The **undo set flow-stat interval** command restores the default interval for collecting traffic statistics on interfaces.

By default, the interval for collecting traffic statistics on interfaces is 300 seconds.

Format

set flow-stat interval *interval-time*

undo set flow-stat interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for collecting traffic statistics on interfaces.	The value is an integer that ranges from 10 to 600, in seconds. In addition, the value must be a multiple of 10. The default value is 300s.

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By using the **set flow-stat interval** command to set the interval for collecting traffic statistics on interfaces, you can collect and analyze traffic statistics according to your needs. You can also take traffic control measures based on the traffic statistics to prevent network congestion and service interruption.

- When congestion occurs, set the interval for collecting traffic statistics on an interface to less than 300 seconds, or 30 seconds if congestion worsens. Then observe the traffic distribution on the interface within a short period of time. If data packets cause congestion, take proper measures to control the rate of the packets.
- When the network bandwidth is sufficient and services are running properly, set the interval for collecting traffic statistics on an interface to more than 300 seconds. If the value of any traffic parameter is not within the specified range, change the interval for collecting traffic statistics to observe the traffic volume in real time.

Precautions

- The interval configured in the system view takes effect on all the interfaces that use the default interval.
- The interval configured in the interface view takes effect only on the current interface.
- The interval configured in the interface view takes precedence over the interval configured in the system view.
- The new interval takes effect after the original interval expires. Traffic statistics on logical interfaces are displayed in the second periodical update after the new interval takes effect. Traffic statistics on physical interfaces are displayed when the new interval takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval for collecting traffic statistics on Eth2/0/0 to 400s.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] set flow-stat interval 400
```

Related Topics

5.1.4 display interface

5.1.13 reset counters interface

5.1.13 reset counters interface

5.1.16 shutdown (interface view)

Function

The **shutdown** command disables an interface.

The **undo shutdown** command enables an interface.

By default, interfaces are enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying parameters of an interface, run the **shutdown** and **undo shutdown** commands to make the modification take effect.

When an interface is not connected to a cable or fiber, you can use the **shutdown** command to disable the interface to prevent exceptions caused by interference.

Precautions

- Disabling an interface during data transmission will cause data frame loss or service interruption. Exercise caution when you use the **shutdown** command.

 Copyright © Huawei Technologies Co., Ltd.

- Some logical interfaces, such as Virtual-Template and null interfaces, do not support the **shutdown** and **undo shutdown** commands.
- If you run the **shutdown** command in the Eth-Trunk interface view, all Eth-Trunk member interfaces are disabled.
- Running the **shutdown** and **undo shutdown** commands is equivalent to running the **restart** command.
- When an interface is configured with a sub-interface, the default interval for running the **shutdown** and **undo shutdown** commands on the main interface is 15 seconds. To change the interval, run the **shutdown interval** command.

Example

Shut down Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] shutdown
```

Related Topics

5.1.4 display interface

5.1.14 restart (interface view)

5.1.17 shutdown interval

Function

The **shutdown interval** command sets the minimum interval for re-enabling an interface.

The **undo shutdown interval** command restores the default minimum interval for re-enabling an interface.

By default, the minimum interval for re-enabling an interface is 0 seconds.

Format

shutdown interval *interval-value*

undo shutdown interval

Parameters

Parameter	Description	Value
interval-value	Specifies the minimum interval for re-enabling an interface.	The value is an integer that ranges from 5 to 15, in seconds.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some cases, for example, when parameters of an interface are modified but the modification does not take effect immediately, run the **shutdown** and **undo shutdown** commands to re-enable the interface. Then the modification can take effect. To shorten the waiting time, run the **shutdown interval** command to set the minimum interval for re-enabling an interface.

Precautions

- The minimum interval configured using this command also applies to the **restart** command.

Example

Set the minimum interval for re-enabling an interface to 5 seconds.

```
<Huawei> system-view
[Huawei] shutdown interval 5
```

Related Topics

5.1.16 shutdown (interface view)

5.1.14 restart (interface view)

5.2 Ethernet Interface Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2220E, AR2201-48FE, AR2202-48FE, AR2204-51GE-P, AR2204-51GE-R, AR2204-27GE-P, AR2204-27GE, AR2204E, AR2204E-D, and AR2204 only support isolation at Layer 2 and interworking at Layer 3. GE0/0/3 to GE0/0/26 on the AR2204-51GE-P and AR2204-51GE-R cannot be isolated from GE0/0/27 to GE0/0/50.

An interface on the 4GE-2S, 9ES2, 4ES2G-S or 4ES2GP-S card cannot be isolated from an interface on other cards.

The interface on 8FE1GE card support configuring the IFG and interface isolated.

The AR2200&AR3200 series support configuring the IFG and interface isolated.

5.2.1 am isolate

Function

The **am isolate** command isolates the current interface from a specified interface unidirectionally.

The **undo am isolate** command cancels unidirectional isolation between the current interface and a specified interface. If no interface is specified,

 Copyright © Huawei Technologies Co., Ltd.

unidirectional isolation between the current interface and all the other interfaces is canceled.

By default, no unidirectional isolation is configured between the current interface and a specified interface

Format

am isolate { *interface-type interface-number* }&<1-8>

undo am isolate [*interface-type interface-number*]&<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface from which the current interface is isolated unidirectionally. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **am isolate** command isolates interfaces unidirectionally. For example, if interface A is isolated from interface B unidirectionally, packets sent from interface A cannot reach interface B, but packets sent from interface B can reach interface A. Unidirectional isolation needs to be configured in the following scenarios:

- When multiple hosts connect to different interfaces of a device and a host sends many broadcast packets to the other hosts, isolate the interface connected to the host from other interfaces unidirectionally. Then the other hosts do not receive packets from the host.
- Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate. To isolate

interfaces in different port isolation groups, configure unidirectional isolation between these interfaces.

By default, only Layer 2 packets of the current interface are isolated from a specified interface, but Layer 3 packets are not isolated. To isolate both Layer 2 and Layer 3 packets on interfaces unidirectionally, run the **port-isolate mode all** command.

Precautions

An interface can be unidirectionally isolated from another type of interface. However, an interface cannot be unidirectionally isolated from itself or from the management interface. In addition, an Eth-Trunk cannot be unidirectionally isolated from its member interfaces.

An interface on the 4GE-2S, 9ES2, 4ES2G-S or 4ES2GP-S card cannot be unidirectionally isolated from an interface on other cards.

NOTE

An interface on the AR100&AR120&AR150&AR160 can be isolated from a maximum of 4 interfaces unidirectionally.

An interface on the AR200, AR1200, AR2200, AR3200 and AR3600 can be isolated from a maximum of 32 interfaces unidirectionally.

Example

Isolate Eth2/0/0 from Eth1/0/0 unidirectionally.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] am isolate ethernet 1/0/0
```

Related Topics

5.2.33 port-isolate mode

5.2.2 auto duplex

Function

The **auto duplex** command configures the duplex mode on an Ethernet electrical interface in auto-negotiation mode.

The **undo auto duplex** command restores the default duplex mode on an Ethernet electrical interface in auto-negotiation mode.

By default, the duplex mode on an Ethernet electrical interface is negotiated with the peer interface.

Format

auto duplex { **half** | **full** }*

undo auto duplex

Parameters

Parameter	Description	Value
half	Sets the duplex mode on an Ethernet electrical interface in auto-negotiation mode to half-duplex.	-
full	Sets the duplex mode on an Ethernet electrical interface in auto-negotiation mode to full-duplex.	-

Views

MEth interface view, Ethernet interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their duplex mode. If the negotiated duplex mode is not the required one, you can run the **auto duplex** command to set the required duplex mode in auto-negotiation mode. For example, two interfaces on both ends support full-duplex mode and half-duplex mode. If the two interfaces negotiate to work in half-duplex mode, but they are required to work in full-duplex mode, you can run the **auto duplex full** command to set the full-duplex mode for the two interfaces.

Prerequisites

The Ethernet interface works in auto-negotiation mode.

Precautions

- By default, an Ethernet interface works in auto-negotiation mode, which is recommended. If the negotiation succeeds, the two interfaces work at the same duplex mode and speed. The settings of the SPEED and DUPLEX parameters and auto-negotiation mode must be the same at the local and peer ends. Otherwise, negotiation may fail. The interface auto-negotiation mode, duplex mode and speed support depend on the device.
- In auto-negotiation mode, an FE electrical interface negotiates the duplex mode with the peer device on the link.
- In auto-negotiation mode, a GE electrical interface that works at a rate of 1000 Mbit/s supports the full-duplex mode. If the duplex mode is changed to

 Copyright © Huawei Technologies Co., Ltd.

half-duplex, the GE electrical interface works at a maximum rate of 100 Mbit/s.

Example

Configure Ethernet electrical interface Eth2/0/0 in auto-negotiation mode to work in half-duplex mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] auto duplex half
```

Related Topics

5.2.28 negotiation auto

5.2.3 auto speed

Function

The **auto speed** command configures the auto-negotiation rate of an Ethernet electrical interface.

The **undo auto speed** command restores the default auto-negotiation rate of an Ethernet electrical interface.

By default, Ethernet electrical interfaces on both ends can negotiate to any rate they support.

Format

auto speed { **10** | **100** | **1000** } *

undo auto speed

NOTE

GE optical interfaces do not support this command.

Parameters

Parameter	Description	Value
10	Sets the auto-negotiation rate of an Ethernet electrical interface to 10 Mbit/s.	-
100	Sets the auto-negotiation rate of an Ethernet electrical interface to 100 Mbit/s.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
1000	Sets the auto-negotiation rate of an Ethernet electrical interface to 1000 Mbit/s. **NOTE** FE electrical interfaces do not support this parameter.	-

Views

MEth interface view, Ethernet interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In auto-negotiation mode, interfaces on both ends of a link negotiate their rate. If the negotiated rate is not the required one, run the **auto speed** command to set the auto-negotiation rate range to limit the negotiated rate. For example, if two interfaces negotiate to work at a rate of 1000 Mbit/s, but they are required to work at a rate of 100 Mbit/s, you can run the **auto speed 100** command to set the rate of the interfaces to 100 Mbit/s.

By default, an Ethernet interface works in auto-negotiation mode, which is recommended. If the negotiation succeeds, the two interfaces work at the same duplex mode and speed. The settings of the SPEED and DUPLEX parameters and auto-negotiation mode must be the same at the local and peer ends. Otherwise, negotiation may fail. The interface auto-negotiation mode, duplex mode and speed support depend on the device.

Prerequisites

The Ethernet interface works in auto-negotiation mode. For details, see **negotiation auto**.

Example

Configure Ethernet electrical interface Eth2/0/0 to work at a rate of 100 Mbit/s in auto-negotiation mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] auto speed 100
```

Related Topics

5.2.28 negotiation auto

5.2.4 clock (Ethernet interface view)

Function

The **clock** command configures the clock mode of a combo interface.

The **undo clock** command restores the default setting.

By default, a combo interface automatically selects the clock mode, and preferentially works in slave clock mode to use line clock signals.

Format

clock [**auto perfer**] { **master** | **slave** }

undo clock

Parameters

Parameter	Description	Value
auto perfer	Allows a combo interface to automatically select the clock mode. If this parameter is not configured, you must manually specify the clock mode of a combo interface.	-
master	Configures a combo interface to work in master clock mode.	-
slave	Configures a combo interface to work in slave clock mode.	-

Views

GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A combo interface on a router is connected to an Ethernet interface that supports the clock function on the peer end. To exchange data successfully, interfaces on the two communicating parties must work in clock synchronization state.

A combo interface works in either of the following clock modes:

- Master: uses clock signals provided by the interface card.
- Slave: uses line clock signals.

 Copyright © Huawei Technologies Co., Ltd.

When a router is connected to an Ethernet interface on the peer end and both the connected interfaces support the clock function, you must configure the interfaces to work in master and slave clock modes respectively.

- When you manually specify the clock modes of the two interfaces, you must configure one interface to work in master clock mode and the other in slave clock mode.
- When you manually specify the clock mode of an interface and configure the other interface to automatically select the clock mode, the other interface will automatically select the clock mode opposite to the specified the clock mode of the peer interface.
- When you configure both the interfaces to automatically select the clock mode, the interfaces will select different clock modes.

Precautions

- When the peer Ethernet interface does not support the clock function, you do not need to configure the clock mode for the combo interface.

Example

Configure GE2/0/0 to work in master clock mode.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] clock master
```

Related Topics

5.2.5 combo-port

5.2.5 combo-port

Function

The **combo-port** command configures the working mode of a combo interface.

The **undo combo-port** command restores the default setting.

A combo interface works in auto mode and automatically works as an optical or electrical interface by default.

Format

combo-port { **auto** | **copper** | **fiber** }

undo combo-port

Parameters

Parameter	Description	Value
auto	Allows a combo interface to automatically select the working mode. The device checks the interface status and selects the working mode as follows: ● If the electrical interface becomes Up first, the combo interface works in electrical mode. ● If the optical interface becomes Up first, the combo interface works in optical mode. ● If the interface is in Down state, and an optical module is not installed, the combo interface works in electrical mode. ● If the interface is in Down state, and an optical module is installed, the combo interface works in optical mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	NOTE If the electrical interface is connected using a network cable and the combo interface goes Up: ● After the network cable is removed, the combo interface does not automatically switch to optical mode and remains in electrical mode even if an optical module is installed. In this case, you can run the **combo-port fiber** command to configure the combo interface to work in optical mode. ● If an optical module is installed and then the network cable is removed, the combo interface automatically switches to optical mode.	
copper	Configures a combo interface to work in electrical mode so that data is transmitted through network cables.	-
fiber	Configures a combo interface to work in optical mode so that data is transmitted through optical fibers.	-

Views

GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Combo interfaces are logic interfaces. One combo interface can work as a GE electrical interface or a GE optical interface. Each combo interface has only one internal forwarding interface. When the electrical interface is enabled, the optical

interface is disabled. When the optical interface is enabled, the electrical interface is disabled. Set the working mode of combo interfaces according to network requirements. The electrical and optical interfaces of a combo interface use the same interface view. You can enable the electrical or optical interface, and configure interface attributes such as the rate and duplex mode in the same interface view.

Precautions

This command takes effect only on combo interfaces.

If a combo interface is configured to work in a different mode from the remote interface, the two interfaces cannot communicate.

When a combo interface works in auto mode, to modify the configuration of the electrical or optical interface, you must forcibly configure the combo interface to work in electrical or optical mode.

If you have specified the interface attributes (such as auto-negotiation mode, rate, and duplex mode) on a combo interface, the system may automatically generate the **port media type fiber** and **port media type copper** configurations to determine whether an interface configuration item belongs to the optical interface or electrical interface. If the combo interface works in one mode (such as the electrical mode), the configuration for the other mode (such as the optical mode) will not be lost.

NOTE

When the combo interface of the AR531 series works in optical mode, the interface supports only the non-auto-negotiation mode, and the peer interface must also be configured to work in non-auto-negotiation mode.

For example, after you run the **display this** command on a combo interface, the interface configuration is as follows:

```
#
interface GigabitEthernet0/0/0
 ip address 192.168.1.10 255.255.255.0
 port media type fiber
  undo negotiation auto
  speed 100
 port media type copper
  undo negotiation auto
 combo-port fiber
#
```

The command output shows that there are two configuration items **undo negotiation auto** and **speed 100** when the combo interface works as an optical interface and one configuration item **undo negotiation auto** when the combo interface works as an electrical interface.

Example

Configure GE1/0/0 to work in electrical mode.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] combo-port copper
```

Related Topics

5.1.10 display this interface

5.2.6 display error-down recovery

Function

The **display error-down recovery** command displays information about the port in error-down state, including the interface name, cause of the error-down event, delay for the interface to change from Down to Up, and remaining time for the Up event.

NOTE

An interface enters the error-down state after being shut down due to an error. Currently, errors include BPDU protection.

Format

display error-down recovery [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the specified port in error-down state. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The auto recovery function is configured and the delay for the an interface to change from Down to Up is set using the **error-down auto-recovery** command. If the interface is in the error-down state, you can run the **display error-down recovery** command to view the remaining time for the Up event.

Prerequisites

The auto recovery function has been configured on an interface using the **error-down auto-recovery** command.

Precautions

If **interface** is not specified in this command, the system displays information about all interfaces in error-down state.

Example

Display the delay for the interface to change from Down to Up and the remaining time for the Up event.

```
<Huawei> display error-down recovery
interface                    error-down cause          recovery   remainder
                                                     time(sec)  time(sec)
--------------------------------------------------------------------------------
Ethernet2/0/0                bpdu-protection           30         10
```

Table 5-13 Description of the **display error-down recovery** command output

Item	Description
interface	Interface name.
error-down cause	Cause of the error-down event, including: ● efm-threshold-event ● bpdu-protection
recovery time(sec)	Delay for the interface to change from Down to Up, in seconds. If no automatic recovery time is configured, you need to run the **undo shutdown (interface view)** command to make the interface go Up and the recovery time is displayed as **--**.
remainder time(sec)	Remaining time for the Up event, in seconds. If no automatic recovery time is configured, you need to run the **undo shutdown (interface view)** command to make the interface go Up and the remaining time is displayed as **--**.

Related Topics

5.2.13 error-down auto-recovery

5.2.7 display interface ethernet brief

Function

The **display interface ethernet brief** command displays brief information about all Ethernet interfaces.

Format

display interface ethernet brief [**main**]

Parameters

Parameter	Description	Value
main	Displays brief information about all Ethernet main interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display interface ethernet brief** command to view brief information about Ethernet interfaces, including the physical status, auto-negotiation mode, duplex mode, bandwidth, and average inbound and outbound bandwidth usages within the last period of time. This information helps you locate and rectify faults.

Precautions

To clear statistics on an interface, run the **reset counters interface** command.

Example

Display brief information about all Ethernet interfaces.

```
<Huawei> display interface ethernet brief
PHY: Physical
*down: administratively down
(l): loopback
(b): BFD down
^down: standby
(v): VirtualPort
InUti/OutUti: input utility/output utility
Interface                 PHY   Auto-Neg Duplex Bandwidth  InUti OutUti Trunk
Ethernet1/0/0               up    disable  full       100M  0.01%  0.01%    --
Ethernet1/0/1               down  disable  full       100M     0%     0%    --
GigabitEthernet0/0/0        up    enable   full       100M  0.01%  0.01%    --
GigabitEthernet0/0/1        down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/1.1      down  enable   full       1000M     0%     0%    --
GigabitEthernet0/0/2        up    enable   full       1000M     0%     0%    --
GigabitEthernet0/0/3(v)     up    enable   full       1000M     0%     0%    --
GigabitEthernet0/0/3.1(v)   up    enable   full       1000M     0%     0%    --
```

Table 5-14 Description of the **display interface ethernet brief** command output

Item	Description
Interface	Type and number of an interface. All interfaces are displayed in alphabetical order. Information about the following interfaces can be displayed: ● Ethernet interface ● GE interface ● XGE interface If **(v)** is displayed behind an interface number, the interface is a virtual interface.
PHY	Physical status of an interface: ● up: indicates that the interface works properly. ● down: indicates that the physical layer of the interface fails. ● *down: refers to Administratively Down, indicating that the administrator has run the **shutdown (interface view)** command on the interface. ● ^down: refers to standby, indicating that this interface is a backup interface. ● (l): refers to loopback, indicating that the loopback function is enabled on the interface. ● (b): indicates that the physical layer of the interface is in BFD Down state.
Auto-Neg	Whether auto-negotiation is enabled on an interface: ● enable: indicates that auto-negotiation is enabled on the interface. ● disable: indicates that auto-negotiation is disabled on the interface. To configure the auto-negotiation mode for an interface, run the **negotiation auto** command.
Duplex	Duplex mode of an interface: ● full: indicates the full-duplex mode. ● half: indicates the half-duplex mode. ● In auto-negotiation mode, use the **auto duplex** command to configure the duplex mode of an interface. ● In non-auto negotiation mode, use the **duplex** command to configure the duplex mode of an interface.
Bandwidth	Bandwidth on the interface. If the bandwidth value is not 10, 100, or 1000, the value is accurate to three decimal places. For example, if the bandwidth of an interface is 5.696 Mbit/s, this field displays 5.696 Mbit/s. If the bandwidth value is 10, 100, or 1000, decimals are not displayed, and this field displays 10 Mbit/s, 100 Mbit/s, or 1000 Mbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
InUti	Average inbound bandwidth usage within the last 5 minutes. Average inbound bandwidth usage = Average inbound rate within the last 5 minutes/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and larger than 0, the value 0.01% is displayed. When the interface bandwidth becomes smaller, for example, the bandwidth is changed using the **speed** command, or when an Eth-Trunk member interface becomes Down or is removed from the Eth-Trunk, the bandwidth usage may be displayed as 100% because the communication traffic is not adjusted in time.
OutUti	Average outbound bandwidth usage within the last 5 minutes. Average outbound bandwidth usage = Average outbound rate within the last 5 minutes/Interface bandwidth When the average bandwidth usage is smaller than 0.01% and larger than 0, the value 0.01% is displayed. When the interface bandwidth becomes smaller, for example, the bandwidth is changed using the **speed** command, or when an Eth-Trunk member interface becomes Down or is removed from the Eth-Trunk, the bandwidth usage may be displayed as 100% because the communication traffic is not adjusted in time.
Trunk	Number of the Eth-Trunk to which an interface is added.

Related Topics

5.1.4 display interface
5.1.13 reset counters interface

5.2.8 display port-group

Function

The **display port-group** command displays information about permanent port groups and interfaces in these groups.

Format

display port-group [**all** | *port-group-name*]

Parameters

Parameter	Description	Value
all	Displays information about all permanent port groups and interfaces in these groups.	-
port-group-name	Displays information about a specified permanent port group and interfaces in the group.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When using the **display port-group** command, note that:

- If no parameter is configured, names of all permanent port groups are displayed.
- If **all** is configured, information about all permanent port groups and interfaces in these groups is displayed.
- If *port-group-name* is configured, information about a specified permanent port group and interfaces in the group is displayed.

Example

Display information about all port groups and interfaces in these groups.

```
<Huawei> display port-group all
Portgroup: port1
ethernet2/0/0
ethernet2/0/1
```

Table 5-15 Description of the **display port-group** command output

Item	Description
Portgroup	Name of a permanent port group.

Related Topics

5.2.30 port-group

5.2.17 group-member

5.2.9 display port-isolate group

Function

The **display port-isolate group** command displays the configuration of a port isolation group.

Format

display port-isolate group { *group-id* | **all** }

Parameters

Parameter	Description	Value
group-id	Displays the configuration of a specified port isolation group.	The value is an integer that ranges from 1 to 64.
all	Displays the configurations of all port isolation groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The port isolation feature isolates interfaces in a VLAN. By adding interfaces to a port isolation group, you can implement Layer 2 isolation between these interfaces. To view the configuration of the port isolation group, run the **display port-isolate group** command.

Example

Display the configurations of all port isolation groups.

```
<Huawei> display port-isolate group all
  The ports in isolate group 1:
Ethernet2/0/0
  The ports in isolate group 2:
Ethernet2/0/1
```

Related Topics

5.2.32 port-isolate enable

5.2.10 display snmp-agent trap feature-name error-down all

Function

The **display snmp-agent trap feature-name error-down all** command displays the status of all traps of the error-down module.

Format

display snmp-agent trap feature-name error-down all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The Simple Network Management Protocol (SNMP) is a network management standard widely used on the TCP/IP network. It uses a central computer (a network management station) that runs network management software to manage network elements. The SNMP agent reports trap messages to the network management station so that the network management station can obtain the network status in a timely manner, and the network administrator can take measures accordingly.

The **display snmp-agent trap feature-name error-down all** command displays the following information:

- Trap names supported by the error-down module. The trap names are the same as the trap names specified by the **snmp-agent trap enable feature-name error-down trap-name** *trap-name* command. Each trap name corresponds to a network element abnormality.
- Trap status of the error-down module. You can check whether the trap is reported based on the trap name.

Prerequisites

SNMP has been enabled. See **snmp-agent**.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display all traps of the error-down module.

```
<Huawei>display snmp-agent trap feature-name error-down all
-----------------------------------------------------------------------------
Feature name: ERROR-DOWN
Trap number : 2
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwErrordown                   on                      on
hwErrordownRecovery           on                      on
```

Table 5-16 Description of the display snmp-agent trap feature-name error-down all command output

Item	Description
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Name of the trap: ● hwErrordown: indicates an error-down alarm. ● hwErrordownRecovery: indicates an error-down clear alarm.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

5.2.36 snmp-agent trap enable feature-name error-down

5.2.11 duplex

Function

The **duplex** command configures the duplex mode on an Ethernet electrical interface in non-auto-negotiation mode.

The **undo duplex** command restores the default duplex mode on an Ethernet electrical interface in no-auto-negotiation mode.

By default, an Ethernet electrical interface works in full-duplex mode when auto-negotiation is disabled on the interface.

Format

duplex { **full** | **half** }

undo duplex

Parameters

Parameter	Description	Value
full	Configures the Ethernet interface to work in full-duplex mode when auto-negotiation is disabled on the interface.	-
half	Configures the Ethernet interface to work in half-duplex mode when auto-negotiation is disabled on the interface.	-

Views

Ethernet interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The duplex mode of an interface needs to be set in the following scenarios:

- To enable an interface to send and receive packets at the same time, set the full-duplex mode on the interface.
- To disable an interface from sending and receiving packets at the same time, set the half-duplex mode on the interface.

Prerequisites

The interface works in non-auto negotiation mode.

Precautions

A GE electrical interface that works at 1000 Mbit/s supports only the full-duplex mode. A GE electrical interface and its peer interface do not need to negotiate the duplex mode.

By default, an Ethernet interface works in auto-negotiation mode, which is recommended. If the negotiation succeeds, the two interfaces work at the same duplex mode and speed. The settings of the SPEED and DUPLEX parameters and auto-negotiation mode must be the same at the local and peer ends. Otherwise,

 Copyright © Huawei Technologies Co., Ltd.

negotiation may fail. The interface auto-negotiation mode, duplex mode and speed support depend on the device.

Example

Configure Ethernet electrical interface Eth2/0/0 to work in half-duplex mode when non-auto negotiation is disabled on the interface.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo negotiation auto
[Huawei-Ethernet2/0/0] duplex half
```

Related Topics

5.1.4 display interface

5.2.22 loopback

5.2.26 mdi

5.2.28 negotiation auto

5.2.37 speed

5.2.12 encapsulation priority-tagged

Function

The **encapsulation priority-tagged** command configures the outbound interface to add a VLAN tag of VLAN 0 to packets and sets the 802.1p priority of packets.

The **undo encapsulation priority-tagged** command disables the outbound interface from adding a VLAN tag of VLAN 0 to packets and deletes the 802.1p priority of packets.

By default, the outbound interface does not add any VLAN tag to packets and retains the original 802.1p priority of packets.

NOTE

Among AR2200 series routers, only the AR2220, AR2220L, AR2220E, AR2240, and AR2240C support this command.

Format

encapsulation priority-tagged [**dot1p** *priority-value* | **dot1p-transmit** *priority-value*]

undo encapsulation priority-tagged [**dot1p** | **dot1p-transmit**]

Parameters

Parameter	Description	Value
dot1p *priority-value*	Sets the 802.1p priority of protocol packets on the outbound interface.	The value is an integer that ranges from 0 to 7. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dot1p-transmit *priority-value*	Sets the 802.1p priority of data packets on the outbound interface.	The value is an integer that ranges from 0 to 7. The default value is 0.

Views

Ethernet interface view, GE interface view, XGE interface view, Layer 3 VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **encapsulation priority-tagged dot1p** *priority-value* command to configure the outbound interface to add a VLAN tag of VLAN 0 to packets and sets the 802.1p priority of protocol packets.

In the bridge scenario, you can run the **encapsulation priority-tagged dot1p-transmit** *priority-value* command to configure the outbound interface to add a VLAN tag of VLAN 0 to packets and sets the 802.1p priority of data packets.

Prerequisites

Run the **undo ip soft-forward enhance enable** command in the system view to disable the enhanced forwarding function for control packets generated by the device.

Precautions

The **encapsulation priority-tagged dot1p** *priority-value* command can be used only on Layer 3 Ethernet interfaces, GE interfaces, XGE interfaces, VE interfaces.

The **encapsulation priority-tagged dot1p-transmit** *priority-value* command can be used only on Layer 3 Ethernet interfaces, GE interfaces, XGE interfaces.

The **encapsulation priority-tagged dot1p-transmit** *priority-value* command takes effect only in bridge scenarios.

Example

Configure the outbound interface of the Eth2/0/0 to add a VLAN tag of VLAN 0 to packets and set the 802.1p priority of protocol packets to 3.

```
<Huawei> system-view
[Huawei] undo ip soft-forward enhance enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] encapsulation priority-tagged dot1p 3
```

Configure the outbound interface of the Eth2/0/0 to add a VLAN tag of VLAN 0 to packets and set the 802.1p priority of data packets to 3.

```
<Huawei> system-view
[Huawei] undo ip soft-forward enhance enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] encapsulation priority-tagged dot1p-transmit 3
```

5.2.13 error-down auto-recovery

Function

The **error-down auto-recovery** command enables an interface in error-down state to go Up and sets the auto recovery delay.

The **undo error-down auto-recovery** command disables an interface in error-down state from going Up automatically.

By default, an interface in error-down state is not enabled to go Up.

NOTE

An interface enters the error-down state after being shut down due to an error. Currently, errors include BPDU protection.

Format

error-down auto-recovery cause { **bpdu-protection** | **efm-remote-failure** | **efm-threshold-event** } **interval** *interval-value*

undo error-down auto-recovery cause { **bpdu-protection** | **efm-remote-failure** | **efm-threshold-event** } **interval** *interval-value*

Parameters

Parameter	Description	Value
cause	Indicates the cause for an interface in error-down state.	-
bpdu-protection	Indicates that STP BPDU protection is enabled.	-
efm-remote-failure	Indicates that an EFM remote failure event occurs.	-
efm-threshold-event	Indicates that a threshold crossing event occurs.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interval *interval-value*	Specifies the auto recovery delay.	The value is an integer that ranges from 30 to 86400, in seconds. • A smaller value indicates a higher frequency at which an interface alternates between Up and Down states. • A larger value indicates longer traffic interruption.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface enters the error-down state in the following scenarios.

Cause for an Interface in Error-down State	Scenario	Remarks
bpdu-protection	On an STP-enabled network where BPDU protection is configured on an edge port, if malicious attackers send bogus BPDUs to attack the switching device, the switching device sets the edge port to Down immediately after the edge port receives BPDUs. As a result, all services on the edge port are interrupted.	For details, see **stp bpdu-protection**.

 Copyright © Huawei Technologies Co., Ltd.

Cause for an Interface in Error-down State	Scenario	Remarks
efm-remote-failure	The **efm trigger error-down** command associates an error event with an interface. When EFM detects **critical-event**, **dying-gasp**, **link-fault**, or **timeout** faults, the protocol status of the interface becomes Down and all services on the interface are interrupted.	-
efm-threshold-event	When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. You can associate an EFM crossing event with an interface. Then the system sets the administrative status of the interface to Down. In this manner, all services on the interface are interrupted.	-

By default, an interface can only be resumed by a network administrator after being shut down. To configure the interface to restore to the Up state automatically, run the **error-down auto-recovery** command to set an auto recovery delay. After the delay, the interface goes Up automatically.

The restored interface is shut down again if the interface receives BPDUs again or the link is considered unavailable in a specified time.

Precautions

The **error-down auto-recovery** command is invalid for the interface that has been in error-down state. It takes effect for only the interface that enters the error-down state after the **error-down auto-recovery** command is executed.

BPDU protection has been enabled using the **stp bpdu-protection** command in the system view.

A threshold crossing event has been associated with an interface using the **efm threshold-event trigger error-down** command in the interface view. An error event has been associated with an interface using the **efm trigger error-down** command in the interface view.

Example

Set the delay for an interface changes from Down to Up to 50s after the edge port is enabled with BPDU protection on an STP-enabled network.

```
<Huawei> system-view
[Huawei] error-down auto-recovery cause bpdu-protection interval 50
```

Set the auto recovery delay to 50s after an EFM remote failure event is associated with an interface.

```
<Huawei> system-view
[Huawei] error-down auto-recovery cause efm-remote-failure interval 50
```

Related Topics

5.2.6 display error-down recovery

6.8.23 stp bpdu-protection

5.2.14 error-statistics threshold-event trigger error-down

Function

The **error-statistics threshold-event trigger error-down** command configures an interface to transit to the error-down state when the number of error packets received on the interface reaches the alarm threshold.

The **undo error-statistics threshold-event trigger error-down** command restores the default setting.

By default, an interface does not transit to the error-down state when the number of error packets received on the interface reaches the alarm threshold.

Format

error-statistics threshold-event trigger error-down

undo error-statistics threshold-event trigger error-down

Parameters

None

Views

Interface View

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an Ethernet interface that has the backup link configured receives error packets, packet loss occurs. To ensure that services are running properly, the interface transits to the error-down state and services are switched to the backup link when the number of error packets received on the interface reaches the alarm threshold.

Follow-up Procedure

By default, an interface that transits to the error-down state can only be restored manually using the **undo shutdown** command. To configure the interface to restore to the Up state automatically, run the **error-down auto-recovery cause error-statistics** command in the system view to set a recovery delay. After the delay, the interface goes Up automatically.

Example

Configure Eth2/0/0 to transit to the error-down state when the number of error packets received on the interface reaches the alarm threshold.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] error-statistics threshold-event trigger error-down
```

Related Topics

5.2.39 trap-threshold error-statistics

5.2.13 error-down auto-recovery

5.2.15 flow-control (Ethernet interface view)

Function

The **flow-control** command enables flow control on an Ethernet interface.

The **undo flow-control** command disables flow control on an Ethernet interface.

By default, flow control is disabled on an Ethernet interface.

Format

flow-control

undo flow-control

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion causes packet loss. Flow control is a method to prevent packet loss. If network congestion occurs on the local device, the local device sends a message to the remote device, instructing the remote device to reduce the packet sending rate. After receiving the message, the remote device reduces its packet sending rate, which prevents congestion.

Precautions

- If flow control is enabled on an interface, it must also be enabled on the peer interface.
- If the **flow-control negotiation** command has been executed on an Ethernet interface to enable flow control auto-negotiation, running the **flow-control** command on the interface will fail.

Example

Enable flow control on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] flow-control
```

Related Topics

5.2.16 flow-control negotiation

5.2.16 flow-control negotiation

Function

The **flow-control negotiation** command enables flow control auto-negotiation on an Ethernet interface.

The **undo flow-control negotiation** command disables flow control auto-negotiation on an Ethernet interface.

By default, flow control auto-negotiation is disabled on an Ethernet interface.

Format

flow-control negotiation

undo flow-control negotiation

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network congestion causes packet loss. Flow control can prevent packet loss. If congestion occurs on a device, the device sends a message to request the peer device to stop sending packets, which prevents packet loss. Flow control auto-negotiation enables a device to determine whether to enable flow control by negotiating with the peer device.

Prerequisites

The Ethernet interface works in auto-negotiation mode.

Precautions

- If flow control auto-negotiation is enabled on an interface, it must also be enabled on the peer interface.
- If flow control has been enabled on an Ethernet interface using the **flow-control** command, run the **undo flow-control** command to disable flow control before running the **flow-control negotiation** command. Otherwise, the **flow-control negotiation** command fails to be executed.

Example

Enable flow control auto-negotiation on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] negotiation auto
[Huawei-GigabitEthernet1/0/0] flow-control negotiation
```

Related Topics

5.2.15 flow-control (Ethernet interface view)

5.2.28 negotiation auto

5.2.17 group-member

Function

The **group-member** command adds specified Ethernet interfaces to a permanent port group.

The **undo group-member** command deletes specified Ethernet interfaces from a permanent port group.

By default, no Ethernet interface is added to a permanent port group.

 Copyright © Huawei Technologies Co., Ltd.

Format

group-member { { *interface-type interface-number1* | *interface-type1* } [**to** { *interface-type interface-number2* | *interface-type2* }] } &<1-10>

undo group-member { { *interface-type interface-number1* | *interface-type1* } [**to** { *interface-type interface-number2* | *interface-type2* }] } &<1-10>

undo group-member all-unavailable-interface

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Adds an Ethernet interface to a permanent port group. **to** specifies an interface range, indicating all the interfaces numbered between *interface-number1* and *interface-number2*.	*interface-number2* must be greater than *interface-number1*.
interface-type1 [**to** *interface-type2*]	Adds an Ethernet interface to a permanent port group. **to** specifies an interface range, indicating all the interfaces numbered between *interface-type1* and *interface-type2*.	*interface-type2* must be greater than *interface-type1*.

Views

Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To perform the same configuration on multiple Ethernet interfaces, add these Ethernet interfaces to a port group and run commands in the port group view to configure the Ethernet interfaces in batches.

Prerequisites

A permanent port group has been created using the **port-group** command in the system view.

Precautions

- The E1-F and CE1/PRI interfaces cannot be added to the same permanent port group.

- A maximum of 32 permanent port groups are supported by the system, and a maximum of 48 interfaces can be added to a permanent port group.
- This command has the same function as the **port-group group-member** command that is used in the system view. You can also run the **port-group group-member** command to add interfaces to a temporary port group to configure the interfaces in batches.
- When you specify the keyword **to** in the **group-member** command:
  - The interfaces specified before and after the keyword **to** must reside on the same interface card. To add consecutive interfaces on different interface cards to the same port group, run the **group-member** command or use **to** multiple times.
  - The interfaces specified before and after the keyword **to** must be of the same type such as Ethernet interfaces.
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not used, these limitations do not apply.

Example

Add Eth2/0/0 and Eth2/0/1 to port group **portgroup1**.

```
<Huawei> system-view
[Huawei] port-group portgroup1
[Huawei-port-group-portgroup1] group-member ethernet 2/0/0 to ethernet 2/0/1
```

Related Topics

5.2.30 port-group

5.2.8 display port-group

5.2.18 interface (Ethernet interface)

Function

Using the **interface** command, you can enter the specified interface view or sub-interface view.

Format

interface { **ethernet** | **gigabitethernet** | **xgigabitethernet** } *interface-number* [*.subinterface-number*]

Parameters

Parameter	Description	Value
ethernet	Enter the view of an FE interface.	-

Parameter	Description	Value
gigabitethernet	Enter the view of a GE interface.	-
xgigabitethernet	Enter the view of a 10GE interface.	-
interface-number	Specifies the number of an interface.	The value depends on the interface type and slot ID.
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After enter the specified Ethernet interface view, you can set attributes for the Ethernet interface.

You can run the **display device** command to view the slot ID of a card to determine the value range of *interface-number*. Only Layer 3 Ethernet interfaces support sub-interfaces.

Example

Enter the view of Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0]
```

Related Topics

5.1.4 display interface

5.2.19 interface range

Function

The **interface range** command creates a temporary interface group and adds specified interfaces to this temporary interface group. Commands configured for a temporary interface group then automatically run on all member interfaces.

By default, no temporary interface group is created.

Format

interface range { { *interface-type interface-number1* | *interface-type1* } [**to** { *interface-type interface-number2* | *interface-type2* }] } &<1-10>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	The value of *interface-number2* must be larger than the value of *interface-number1*.
interface-type1 [**to** *interface-type2*]	Specifies Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-type1* and *interface-type2* are added to the temporary port group.	The value of *interface-type2* must be larger than the value of *interface-type1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a device has many Ethernet interfaces and most of them have the same configuration. Configuring these Ethernet interfaces one by one increases the configuration workload and may result in incorrect configurations. Therefore, you can add the Ethernet interfaces to be configured with the same command to a port group. After a command is run in this port group, the system executes the command on all the member interfaces. This process allows Ethernet interfaces to be configured in batches.

Precautions

- The **interface range** and **port-group group-member** commands have the same functions. Therefore, use either of the commands for configuration.
- After exiting from the temporary port group view, the system deletes the temporary port group.

- The **interface range** command is equivalent to the **group-member** command executed in the permanent port group view. Multiple interfaces can be added to a permanent port group in batches using the **group-member** command.
- E1-F and CE1/PRI interfaces cannot be added to the same temporary port group.
- The system supports a maximum of 32 temporary port groups. If more than 32 users log in to the device through Telnet simultaneously, only 32 users can create temporary port groups.
- A temporary port group supports a maximum of 48 member interfaces.
- When you specify the keyword **to** in the **interface range** command:
  - The interfaces specified by *interface-number1* and *interface-number2* must reside on the same LPU. To add contiguous interfaces on different LPUs to the same port group, run this command several times or use the keyword **to** several times.
  - The interfaces specified by *interface-number1* and *interface-number2* must be of the same type, for example, both of the interfaces are Ethernet interfaces.
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not specified, the preceding limitations do not apply.

Example

Add Eth2/0/0 and 2/0/1 to a temporary port group.

```
<Huawei> system-view
[Huawei] interface range ethernet 2/0/0 to ethernet 2/0/1
[Huawei-port-group]
```

5.2.20 ifg

Function

The **ifg** command configures the inter-frame gap (IFG).

The **undo ifg** command restores the default IFG.

By default, the IFG is 12 bytes.

Format

ifg *ifg-value*

undo ifg

Parameters

Parameter	Description	Value
ifg-value	Specifies the IFG.	The value is an integer that ranges from 9 to 12, in bytes.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IFG is used to differentiate two data packets. The **ifg** command configures the IFG to adjust data packet forwarding efficiency.

NOTE

The packet forwarding rate, also called the throughput, is the data forwarding capability on an interface, expressed in packets per second. The packet forwarding rate is calculated based on the number of 64-byte data packets sent in a certain period. The payload of the frame header and IFG affects the packet forwarding rate.

Precautions

Changing the IFG on an interface is not recommended because this may cause packet loss on the interface.

Example

Set the IFG of Eth2/0/0 to 10 bytes.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ifg 10
```

5.2.21 log-threshold

Function

The **log-threshold** command sets the inbound and outbound bandwidth usage thresholds for generating a log.

The **undo log-threshold** command restores the default inbound and outbound bandwidth usage thresholds for generating a log.

The default inbound and outbound bandwidth usage thresholds for generating a log is 100.

 Copyright © Huawei Technologies Co., Ltd.

Format

log-threshold { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]

undo log-threshold { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Specifies the inbound bandwidth.	-
output-rate	Specifies the outbound bandwidth.	-
bandwidth-in-use	Specifies the bandwidth usage threshold for generating a log, prompting for a bandwidth increase request.	The value is an integer that ranges from 1 to 100.
resume-rate *resume-threshold*	Specifies the bandwidth usage threshold for generating a log, indicating that bandwidth usage has been restored.	The value is an integer that ranges from 1 to the value of *bandwidth-in-use*. The default value is the value of *bandwidth-in-use*.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Monitoring bandwidth usage helps you learn about current device load. If the bandwidth usage exceeds a configured threshold, a log or an alarm is generated, indicating that bandwidth resources become insufficient and need an increase. For example, if bandwidth usage exceeds 95% of total bandwidth, an alarm is generated, indicating that bandwidth is exhausted. Some services may be interrupted before the bandwidth increases. To help prevent service interruption, setting two bandwidth usage thresholds, one for generating a log and the other for generating an alarm helps you increase bandwidth in time.

NOTE

Outbound bandwidth usage = (Outbound interface rate/Outbound physical interface bandwidth) x 100

Inbound bandwidth usage = (Inbound interface rate/Inbound physical interface bandwidth) x 100

If the offset between the value of *bandwidth-in-use* and the value of *resume-threshold* is too small, log information may be frequently displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure Eth2/0/0 to generate a log when the outbound interface rate exceeds 80% of the bandwidth.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] log-threshold output-rate 80
```

Configure Eth2/0/0 to generate a log when the outbound interface rate exceeds 80% of the bandwidth and to generate a log indicating that bandwidth usage has been restored, when the outbound interface rate is lower than 60% of the bandwidth.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] log-threshold output-rate 80 resume-rate 60
```

Related Topics

5.2.38 trap-threshold

5.2.22 loopback

Function

The **loopback** command enables loopback detection on an interface.

The **undo loopback** command disables loopback detection on an interface.

By default, loopback detection is not configured.

Format

loopback internal

undo loopback

Parameters

Parameter	Description	Value
internal	Configures internal loopback detection on a specified interface.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Loopback detection can be enabled to test some special functions, for example, locating faults on the Ethernet. After loopback detection is enabled, the Ethernet interface works in full-duplex mode. After loopback detection is disabled, the original duplex mode of the Ethernet interface is restored.

After loopback detection is enabled on an interface, packets sent from the interface are sent back to this interface.

Follow-up Procedure

Run the **display interface** command to check whether the **current status** of the interface configured with internal loopback is Up. If the **current status** of the interface is Up, the internal forwarding function works well; otherwise, a fault occurs during internal forwarding.

Precautions

Loopback detection interrupts the operation of Ethernet interfaces and links. After loopback detection is performed, run the **undo loopback** command to disable loopback detection immediately.

Example

Configure loopback detection on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] loopback internal
```

Related Topics

5.1.4 display interface

5.2.23 mac-address (Ethernet interface view)

Function

The **mac-address** command configures a MAC address for an Ethernet interface.

The **undo mac-address** command restores the default MAC address of an Ethernet interface.

By default, the MAC address of an Ethernet interface is the system MAC address.

Format

mac-address *mac-address*

undo mac-address

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for an Ethernet interface.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number, such as 00e0 or fc01. The MAC address cannot be FFFF-FFFF-FFFF, all 0s, or a multicast MAC address.

Views

Ethernet interface view, GE interface view, XGE interface view,Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MAC address of an Ethernet interface is the system MAC address and may conflict with the MAC address of another interface. If the MAC address of an Ethernet interface conflicts with that of another interface, a loop may occur or traffic may fail to be forwarded.

You can run the **mac-address** command to change the MAC address of the Ethernet interface to ensure that service data flows are properly forwarded.

Configuration Impact

After the MAC address of an Ethernet interface is changed, the device proactively sends gratuitous ARP packets to update ARP entries on the remote device.

Precautions

This command can be configured only on Layer 3 Ethernet interfaces.

Example

Set the MAC address of GE1/0/0 to 0001-2345-abcd.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mac-address 0001-2345-abcd
```

Related Topics

5.1.4 display interface

5.2.24 management-plane isolate enable

Function

The **management-plane isolate enable** command disables the device from accessing the IP address of the management port from service ports.

The **undo management-plane isolate enable** command enables the device to access the IP address of the management port from service ports.

By default, the device is disabled from accessing the IP address of the management port from service ports.

NOTE

Only the AR2204EX, AR2240 (configured with the SRU100E, SRU200, SRU200E, and SRU400), AR3260 (configured with the SRU200, SRU200E, and SRU400) and AR3670 (configured with the SRUX5) support this command.

Format

management-plane isolate enable

undo management-plane isolate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **management-plane isolate enable** command on the device so that the service port will discard the packets whose destination address is the management port address. This improves network security and prevents attacks between the management port through the service ports. However, the device can access the IP address of service ports from the management port.

Precautions

The **management-port isolate enable** and **management-plane isolate enable** command functions are different. The **management-port isolate enable** command isolates traffic between the management port and service ports by marking the network segment routes with the outbound interface being the management port as the blackhole routes, whereas the **management-plane isolate enable** command isolates service ports from the management port by

marking the host and broadcast routes with the outbound interface being the management port as the blackhole routes.

Example

Enable the device to access the IP address of a management port from service ports.

```
<Huawei> system-view
[Huawei] undo management-plane isolate enable
```

Related Topics

5.2.25 management-port isolate enable

5.2.25 management-port isolate enable

Function

The **management-port isolate enable** command enables forwarding traffic isolation between the management port and service ports.

The **undo management-port isolate enable** command disables forwarding traffic isolation between the management port and service ports.

By default, forwarding traffic isolation is enabled between the management port and service ports.

NOTE

Only the AR2204EX, AR2240 (configured with the SRU100E, SRU200, SRU200E, and SRU400), AR3260 (configured with the SRU200, SRU200E, and SRU400) and AR3670 (configured with the SRUX5) support this command.

Format

management-port isolate enable

undo management-port isolate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **management-port isolate enable** command on the device to restrict packet traffic between the management port and service ports. That is, the packets received on the management port will not be forwarded from service ports; similarly, the packets received on service ports will not be forwarded from the management port. This improves network security and prevents attacks on the management port from service ports.

Precautions

The **management-port isolate enable** and **management-plane isolate enable** command functions are different. The **management-port isolate enable** command isolates traffic between the management port and service ports by marking the network segment routes with the outbound interface being the management port as the blackhole routes, whereas the **management-plane isolate enable** command isolates service ports from the management port by marking the host and broadcast routes with the outbound interface being the management port as the blackhole routes.

Example

Disable forwarding traffic isolation between the management port and service ports.

```
<Huawei> system-view
[Huawei] undo management-port isolate enable
```

Related Topics

5.2.24 management-plane isolate enable

5.2.26 mdi

Function

The **mdi** command configures the medium dependent interface (MDI) mode of an Ethernet electrical interface.

The **undo mdi** command restores the default MDI mode of an Ethernet electrical interface.

By default, an Ethernet electrical interface automatically identifies the network cable type.

Format

mdi { **across** | **auto** | **normal** }

undo mdi

Parameters

Parameter	Description	Value
across	Sets the MDI mode of an Ethernet electrical interface to **across**.	-

Parameter	Description	Value
auto	Sets the MDI mode of an Ethernet electrical interface to **auto**. An Ethernet electrical interface automatically identifies the network cable type.	-
normal	Sets the MDI mode of an Ethernet electrical interface to **normal**.	-

Views

Ethernet interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

An Ethernet interface consists of eight pins. Each pin has its functions. For example, pins 1 and 2 send signals, and pins 3 and 6 receive signals. By setting the MDI mode for an interface, you can change the roles of pins in communication so that the interface adapts to the actual network cable type.

Setting the MDI mode to **auto** is recommended because the auto mode applies to most scenarios. When the network cable type parameters cannot be obtained, set the MDI mode to **across** or **normal** manually.

The methods to set the MDI mode manually are as follows:

- When straight-through network cables are used, the MDI modes of the interfaces on the local and peer devices must be different. For example, you can set the MDI mode of the interface on the local device to **across** and the MDI mode of the interface on the peer device to **normal**.
- When crossover network cables are used, the MDI modes of the interfaces on the local and peer devices must be the same. For example, you can set the MDI modes of the interfaces on the local and peer devices to **across** or **normal**. Alternatively, the MDI type of the interface on a device is **auto** and the MDI type of the interface on the other device can be set to **across** or **normal**.

Example

Set the MDI mode of Eth2/0/0 to **across**.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mdi across
```

Related Topics

5.2.11 duplex
5.2.28 negotiation auto

5.2.27 mtu (Ethernet interface view)

Function

The **mtu** command sets the maximum transmission unit (MTU) for an Ethernet interface.

The **undo mtu** command restores the default MTU of an Ethernet interface.

By default, the MTU of an Ethernet interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of an Ethernet interface.	The value depends on the device.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data packets is limited at the network layer. Upon receiving an IP packet to be sent, the network layer checks to which local interface the packet needs to be sent and obtains the maximum transmission unit (MTU) configured on the interface. Then the network layer compares the MTU with the packet length. If the packet length is longer than the MTU, the network layer disassembles the packet to fragments, each no longer than the MTU.

- If the MTU is too small whereas the packet size is large, the packet is split into many fragments. Therefore, the packet may be discarded due to insufficient QoS queue length.
- If the MTU is too large, packets are transmitted slowly or even lost.

Precautions

- If you run the **mtu** command multiple times in the same Ethernet interface view, only the latest configuration takes effect.
- This command can only be used on Layer 3 Ethernet interfaces.

Example

Set the MTU of GE1/0/0 to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mtu 1200
```

Related Topics

5.1.4 display interface

5.2.28 negotiation auto

Function

The **negotiation auto** command configures an Ethernet interface to work in auto-negotiation mode.

The **undo negotiation auto** command configures an Ethernet interface to work in non-auto-negotiation mode.

By default, an Ethernet interface works in auto-negotiation mode.

Format

negotiation auto

undo negotiation auto

Parameters

None

Views

MEth interface view, Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Earlier Ethernet worked in 10M half-duplex mode and required mechanisms such as Carrier Sense Multiple Access (CSMA)/Collision Detection (CD) to ensure system stability. As Ethernet technology develops, full-duplex Ethernet and 100 Mbit/s Ethernet emerge. This greatly improves Ethernet performance. Auto-

negotiation technology allows new Ethernet to be compatible with earlier Ethernet. In auto-negotiation mode, interfaces on both ends of a link negotiate their operating parameters, including the duplex mode and rate. If the negotiation succeeds, the two interfaces work at the same operating parameters.

You can configure an interface to work in auto-negotiation mode only when interfaces on both ends support the auto-negotiation mode.

- If interfaces on both ends support auto-negotiation and are required to work in auto-negotiation mode, run the **negotiation auto** command.
- If one of the two interfaces does not support auto-negotiation or is not required to work in auto-negotiation mode, run the **undo negotiation auto** command.

Precautions

- By default, an Ethernet interface works in auto-negotiation mode, which is recommended. If the negotiation succeeds, the two interfaces work at the same duplex mode and speed. The settings of the SPEED and DUPLEX parameters and auto-negotiation mode must be the same at the local and peer ends. Otherwise, negotiation may fail. The interface auto-negotiation mode, duplex mode and speed support depend on the device.
- By default, GE interfaces do not support flow control auto-negotiation. You can run the **flow-control negotiation** command to configure flow control auto-negotiation.
- GE optical interfaces do not support auto-negotiation function after FE optical modules are installed on the interfaces.

Example

Configure Eth2/0/0 to work in non-auto-negotiation mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo negotiation auto
```

Related Topics

5.2.11 duplex

5.2.26 mdi

5.2.37 speed

5.2.29 port-down holdoff-timer

Function

The **port-down holdoff-timer** command sets the delay time for an interface to report the Down event.

The **undo port-down holdoff-timer** command configures an interface to report the Down event immediately.

By default, an interface reports the Down event immediately.

Format

port-down holdoff-timer *holdoff-timer*

undo port-down holdoff-timer

Parameters

Parameter	Description	Value
holdoff-timer	Specifies the delay time for an interface to report the Down event.	The value is an integer that ranges from 50 to 3000, in milliseconds.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

When an interface becomes Down, services on the interface are interrupted even if this interface becomes Up soon. To prevent services from being interrupted, set the delay in reporting a Down event on the interface so that the system still considers that this interface is in Up state within the delay time.

Example

Set the delay time for an interface to report the Down event to 100 ms.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port-down holdoff-timer 100
```

5.2.30 port-group

Function

The **port-group** command creates a permanent port group and displays the permanent port group view.

The **undo port-group** command deletes permanent port groups.

By default, no permanent port group is configured.

Format

port-group *port-group-name*

undo port-group { **all** | *port-group-name* }

Parameters

Parameter	Description	Value
port-group-name	Specifies the name of a permanent port group.	The value is a string of 1 to 32 case-insensitive characters without spaces. **NOTE** A permanent port group cannot be named **group**.
all	Deletes all port groups.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a device has many interfaces and most of them have the same configuration. Configuring these interfaces one by one increases the configuration workload and may result in incorrect configurations. You can add the interfaces to be configured with the same commands to a permanent port group. After a command is run in this port group, the system executes the command on all the member interfaces. This process allows interfaces to be configured in batches.

Follow-up Procedure

Run the **group-member** command to add Ethernet interfaces to the created permanent port group.

Precautions

- The *port-group-name* parameter cannot be set to **all**.
- The system supports a maximum of 32 permanent port groups and each port group supports a maximum of 48 member interfaces.

Example

Create port group **portgroup1** and enter the port group view.

```
<Huawei> system-view
[Huawei] port-group portgroup1
[Huawei-port-group-portgroup1]
```

Related Topics

5.2.8 display port-group

5.2.17 group-member

5.2.31 port-group group-member

Function

The **port-group group-member** command creates a temporary port group and adds specified Ethernet interfaces to the temporary port group. Commands configured for a temporary port group will be automatically run on all member interfaces.

By default, no temporary port group is created.

Format

port-group group-member { { *interface-type interface-number1* | *interface-type1* } [**to** { *interface-type interface-number2* | *interface-type2* }] } &<1-10>

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-number1* and *interface-number2* are added to the temporary port group.	The value of *interface-number2* must be larger than the value of *interface-number1*.
interface-type1 [**to** *interface-type2*]	Specifies Ethernet interfaces to be added to a temporary port group. **to** indicates an interface range. All interfaces numbered between *interface-type1* and *interface-type2* are added to the temporary port group.	The value of *interface-type2* must be larger than the value of *interface-type1*.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a device has many Ethernet interfaces and most of them have the same configuration. Configuring these Ethernet interfaces one by one increases the configuration workload and may result in incorrect configurations. Therefore, you

can add the Ethernet interfaces to be configured with the same command to a port group. After a command is run in this port group, the system executes the command on all the member interfaces. This process allows Ethernet interfaces to be configured in batches.

Precautions

- After exiting from the temporary port group view, the system deletes the temporary port group.
- The **port-group group-member** command is equivalent to the **group-member** command executed in the permanent port group view. Multiple interfaces can be added to a permanent port group in batches using the **group-member** command.
- E1-F and CE1/PRI interfaces cannot be added to the same temporary port group.
- The system supports a maximum of 32 temporary port groups. If more than 32 users log in to the device through Telnet simultaneously, only 32 users can create temporary port groups.
- A temporary port group supports a maximum of 48 member interfaces.
- When you specify the keyword **to** in the **port-group group-member** command:
  - The interfaces specified by *interface-number1* and *interface-number2* must reside on the same LPU. To add contiguous interfaces on different LPUs to the same port group, run this command several times or use the keyword **to** several times.
  - The interfaces specified by *interface-number1* and *interface-number2* must be of the same type, for example, both of the interfaces are Ethernet interfaces.
  - The interfaces specified before and after the keyword **to** must have the same attribute. For example, both of them are main interfaces or sub-interfaces. If they are sub-interfaces, they must belong to the same main interface.
  - If **to** is not specified, the preceding limitations do not apply.

Example

Add Eth2/0/0 and Eth2/0/1 to a temporary port group.

```
<Huawei> system-view
[Huawei] port-group group-member ethernet 2/0/0 to ethernet 2/0/1
[Huawei-port-group]
```

Related Topics

5.2.30 port-group

5.2.17 group-member

5.2.32 port-isolate enable

Function

The **port-isolate enable** command enables port isolation.

The **undo port-isolate enable** command disables port isolation.

By default, port isolation is disabled.

Format

port-isolate enable [**group** *group-id*]

undo port-isolate enable [**group** *group-id*]

Parameters

Parameter	Description	Value
group *group-id*	Specifies the ID of a port isolation group.	The value is an integer depending on the device.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement Layer 2 isolation between interfaces, add different interfaces to different VLANs. This, however, wastes VLAN resources. To save VLAN resources, enable port isolation to isolate interfaces in a VLAN. That is, you can add interfaces to a port isolation group to implement Layer 2 isolation between these interfaces. Port isolation provides secure and flexible networking schemes for customers.

Precautions

- After port isolation is configured, ports are isolated at Layer 2 but can communicate at Layer 3 by default. To configure both Layer 2 isolation and Layer 3 isolation, run the **port-isolate mode all** command.
- Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate. If *group-id* is not specified, interfaces are added to port isolation group 1 by default.
- Inter-board port isolation is not supported on the interfaces of the 4GE-2S, 9ES2, 4ES2G-S or 4ES2GP-S interface card.
- The AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2220E, AR2201-48FE, AR2202-48FE, AR2204-51GE-P, AR2204-51GE-R, AR2204-27GE-P, AR2204-27GE, AR2204E, AR2204E-D, and AR2204 only support isolation at Layer 2 and interworking at Layer 3. GE0/0/3 to GE0/0/26 on the AR2204-51GE-P and AR2204-51GE-R cannot be isolated from GE0/0/27 to GE0/0/50.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable port isolation on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port-isolate enable group 1
```

Related Topics

5.2.9 display port-isolate group

5.2.33 port-isolate mode

Function

The **port-isolate mode** command sets the port isolation mode.

By default, ports are isolated at Layer 2 but can communicate at Layer 3.

NOTE

The AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2220E, AR2201-48FE, AR2202-48FE, AR2204-51GE-P, AR2204-51GE-R, AR2204-27GE-P, AR2204-27GE, AR2204E, AR2204E-D, and AR2204 only support isolation at Layer 2 and interworking at Layer 3. GE0/0/3 to GE0/0/26 on the AR2204-51GE-P and AR2204-51GE-R cannot be isolated from GE0/0/27 to GE0/0/50.

Format

port-isolate mode { **l2** | **all** }

Parameters

Parameter	Description	Value
l2	Indicates that ports are isolated at Layer 2 but can communicate at Layer 3.	-
all	Indicates that ports are isolated at both Layer 2 and Layer 3.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To disable members in a port isolation group from communicating at Layer 2 but allow them to access public resources, such as printer and server, run the **port-isolate mode** command to set the port isolation mode to **l2**.

To disable members in a port isolation group from communicating at both Layer 2 and Layer 3, run the **port-isolate mode** command to set the port isolation mode to **all**.

Precautions

- To isolate ports at both Layer 2 and Layer 3, run the **port-isolate mode all** command.
- To isolate ports at Layer 2 but allow them to communicate at Layer 3, run the **port-isolate mode l2** command.

Example

Configure Layer 2 isolation and Layer 3 communication.

```
<Huawei> system-view
[Huawei] port-isolate mode l2
```

Related Topics

5.2.9 display port-isolate group

5.2.32 port-isolate enable

5.2.34 portswitch

Function

The **portswitch** command changes the working mode of Ethernet interfaces from Layer 3 mode to Layer 2 mode.

The **undo portswitch** command changes the working mode of Ethernet interfaces from Layer 2 mode to Layer 3 mode.

By default, an Ethernet interface works in Layer 2 mode.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Eth0/0/0 to Eth0/0/3 on the AR120 (except the AR129CV, AR129CVW, and AR129CGVW-L) and AR150 series can be changed from Layer 2 mode to Layer 3 mode.

GE0/0/0 to GE0/0/3 on the AR100 series, AR129CV, AR129CVW, AR129CGVW-L, and AR160 series can be changed from Layer 2 mode to Layer 3 mode.

Eth0/0/0 to Eth0/0/7 on the AR200 series, AR1220, AR1220V, AR1220W, AR1220VW, and AR1220F can be changed from Layer 2 mode to Layer 3 mode.

GE0/0/0 to GE0/0/7 on the AR1220C, AR1220E, AR1220EV, and AR1220EVW can be changed from Layer 2 mode to Layer 3 mode.

Eth0/0/0 and Eth0/0/47 on the AR2201-48FE and AR2202-48FE can be changed from Layer 2 mode to Layer 3 mode.

GE0/0/3 to GE0/0/50 on the AR2204-51GE-P, AR2204-51GE-R, and AR2204-51GE can be changed from Layer 2 mode to Layer 3 mode.

GE0/0/3 to GE0/0/26 on the AR2204-27GE-P, AR2204E-D-27GE, and AR2204-27GE can be changed from Layer 2 mode to Layer 3 mode.

The working modes of all interfaces on the 24GE Ethernet LAN cards can be changed from Layer 2 mode to Layer 3 mode. After the reserved VLAN ID of the 9ES2 Ethernet LAN card (excluding the 9ES2 Ethernet LAN card, 8FE1GE Ethernet electrical interface card, and 4ES2G-S Ethernet LAN card installed on the AR1200 series router) is delivered using the **set reserved-vlan** command, the working modes of all interfaces on the card can be changed from Layer 2 mode to Layer 3 mode.

AR2220E, AR2240, and AR3260 can run the **portswitch** command to change the working mode of all interfaces on the SRU200, SRU400, 4GECS, and 2X10GL from Layer 3 mode to Layer 2 mode. The interfaces that change the working mode to layer 2 only support VXLAN.

Format

portswitch

undo portswitch

Parameters

None

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an Ethernet interface on the device works in Layer 2 mode. To enable Layer 3 functions on the interface, run the **undo portswitch** command on the interface.

Precautions

The minimum interval between running the **portswitch** and **undo portswitch** commands must be 30s.

Example

Change the working mode of Eth0/0/0 from Layer 2 mode to Layer 3 mode.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/0
[Huawei-Ethernet0/0/0] undo portswitch
```

5.2.35 set flow-statistics include-interframe

Function

The **set flow-statistics include-interframe** command configures traffic statistics on an interface to contain the inter-frame gap and preamble.

The **undo set flow-statistics include-interframe** command configures traffic statistics on an interface not to contain the inter-frame gap and preamble.

By default, traffic statistics on an interface do not contain the inter-frame gap and preamble.

Format

set flow-statistics include-interframe

undo set flow-statistics include-interframe

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The QoS function counts the inter-frame gap when calculating the traffic rate on an interface, but the traffic statistics on the interface do not contain the inter-frame gap. Therefore, the traffic statistics collected on an interface are different from the traffic statistics of rate limit on the interface. To solve this problem, configure the traffic statistics on an interface to contain the inter-frame gap.

Precautions

The device counts bytes in the inter-frame gap when collecting traffic statistics on a sub-interface. By default, the device does not count bytes in the inter-frame gap when collecting traffic statistics on a main interface. Therefore, traffic statistics on a main interface differ from those on its sub-interface. You can run the **set flow-**

statistics include-interframe command on the main interface to configure the device to count bytes in the inter-frame gap and preamble when collecting traffic statistics on the main interface.

Example

Configure traffic statistics on Eth2/0/0 to contain the inter-frame gap and preamble.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] set flow-statistics include-interframe
```

Related Topics

5.1.4 display interface

5.2.36 snmp-agent trap enable feature-name error-down

Function

The **snmp-agent trap enable feature-name error-down** command enables the trap function for the errordown module.

The **undo snmp-agent trap enable feature-name error-down** command disables the trap function for the errordown module.

By default, the trap function is disabled for the errordown module.

Format

snmp-agent trap enable feature-name error-down [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name error-down [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Indicates the trap function for a specified type of trap messages of the errordown module: ● hwerrordown: indicates an errordown alarm. ● hwerrordownrecovery: indicates an errordown clear alarm.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can specify **trap-name** to enable the trap function for one or more events of the errordown module.

Example

Enable the trap function for errordown alarms.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name error-down trap-name hwerrordown
```

Related Topics

5.2.10 display snmp-agent trap feature-name error-down all

5.2.37 speed

Function

The **speed** command sets the rate for an Ethernet interface in non-auto negotiation mode.

By default, an Ethernet interface works at its highest rate when it works in non-auto negotiation mode. Specially, when a GE electrical interface works in non-auto-negotiation mode, its default rate is 100 Mbit/s, not the maximum rate 1000 Mbit/s supported by the GE interface.

NOTE

The rate range depends on the device.

Format

speed { **10** | **100** | **1000** | **10000** }

Parameters

Parameter	Description	Value
10	Indicates that the interface works at 10 Mbit/s.	-
100	Indicates that the interface works at 100 Mbit/s.	-
1000	Indicates that the interface works at 1000 Mbit/s.	-
10000	Indicates that the interface works at 10000 Mbit/s.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In non-auto negotiation mode, if interfaces on two connected devices work at different rates, use the **speed** command to change the rates of the interfaces to be the same so that the two devices can communicate.

Precautions

By default, an Ethernet interface works in auto-negotiation mode, which is recommended. If the negotiation succeeds, the two interfaces work at the same duplex mode and speed. The settings of the SPEED and DUPLEX parameters and auto-negotiation mode must be the same at the local and peer ends. Otherwise, negotiation may fail. The interface auto-negotiation mode, duplex mode and speed support depend on the device.

If the remote interface does not support the auto negotiation mode, run the **undo negotiation auto** command on the local interface to configure the interface to work in non-auto negotiation mode. You can then change the rate of the local interface to be the same as the rate of the remote interface to ensure proper communication.

Example

Configure GE2/0/0 to work at 100 Mbit/s in non-auto negotiation mode.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] undo negotiation auto
[Huawei-GigabitEthernet2/0/0] speed 100
```

Related Topics

5.2.28 negotiation auto

5.2.11 duplex

5.2.38 trap-threshold

Function

The **trap-threshold** command sets the inbound and outbound bandwidth usage thresholds for generating a trap.

The **undo trap-threshold** command restores the default inbound and outbound bandwidth usage thresholds for generating a trap.

The default inbound or outbound bandwidth usage threshold for generating a trap is 100.

 Copyright © Huawei Technologies Co., Ltd.

Format

trap-threshold { **input-rate** | **output-rate** } *bandwidth-in-use* [**resume-rate** *resume-threshold*]

undo trap-threshold { **input-rate** | **output-rate** }

Parameters

Parameter	Description	Value
input-rate	Indicates inbound bandwidth.	-
output-rate	Indicates outbound bandwidth.	-
bandwidth-in-use	Specifies the bandwidth usage threshold for generating a trap.	The value is an integer that ranges from 1 to 100.
resume-rate *resume-threshold*	Specifies the bandwidth usage threshold for clearing a trap.	The value is an integer that ranges from 1 to *bandwidth-in-use*. The default value is *bandwidth-in-use*.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The bandwidth usage represents the load on a device. If the bandwidth usage exceeds the threshold, bandwidth of the device is insufficient for services and needs expansion. For example, if the bandwidth usage exceeds 95%, an alarm is generated to indicate that bandwidth resources are used up. Services may be interrupted before system expansion. You can set the upper and lower thresholds for bandwidth usage. When the bandwidth usage exceeds the lower threshold, the system generates a log. When the bandwidth usage exceeds the upper threshold, the system triggers an alarm.

NOTE

Outbound bandwidth usage = (Outbound interface rate/Outbound physical interface bandwidth) x 100

Inbound bandwidth usage = (Inbound interface rate/Inbound physical interface bandwidth) x 100

The interface rate and bandwidth are expressed in bits per second.

The interval for collecting statistics on the traffic rate on an interface is the value configured using the **set flow-stat interval** command on the interface.

To set a lower threshold, run the **log-threshold** command.

The **trap-threshold** command sets the bandwidth usage threshold for generating a trap. The **trap-threshold** with the following parameters provides various functions:

- **trap-threshold input-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the inbound bandwidth usage threshold for generating a trap.
  - If inbound bandwidth usage exceeds the threshold specified in *bandwidth-in-use*, an hwIfMonitorInputRateRising trap is generated, indicating that inbound bandwidth usage exceeds the configured threshold.
  - If inbound bandwidth usage falls below the threshold specified in *resume-threshold*, an hwIfMonitorInputRateResume trap is generated, indicating that inbound bandwidth usage falls between the configured threshold for clearing a trap.
- **trap-threshold output-rate** *bandwidth-in-use* **resume-rate** *resume-threshold*: sets the outbound bandwidth usage threshold for generating a trap.
  - If outbound bandwidth usage exceeds the threshold specified in *bandwidth-in-use*, an hwIfMonitorOutputRateRising trap is generated, indicating that outbound bandwidth usage exceeds the configured threshold.
  - If outbound bandwidth usage falls below the threshold specified in *resume-threshold*, an hwIfMonitorOutputRateResume trap is generated, indicating that outbound bandwidth usage falls between the configured threshold for clearing a trap.

Precautions

- When the bandwidth usage exceeds the threshold for generating a trap, the system generates a trap. When the bandwidth usage falls below the threshold for clearing a trap, the system clears the trap.
- If the offset between the value of *bandwidth-in-use* and the value of *resume-threshold* is too small, trap information may be frequently displayed.
- The log threshold must be lower than the trap threshold, providing efficient protection for services. For example, when the inbound bandwidth usage reaches 80%, a log is generated. If the inbound bandwidth usage continues to increase and reaches 95%, a trap is generated. This ensures that a log is generated for inbound bandwidth usage of 80%, and a trap is generated for inbound bandwidth usage of 95%. Either the log or the trap prompts for a bandwidth increase, preventing service interruption.

Example

Configure Eth2/0/0 to generate a trap when the outbound bandwidth usage exceeds 60%.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] trap-threshold output-rate 60
```

Configure Eth2/0/0 to generate a trap when the outbound bandwidth usage exceeds 80% and clear the trap when the outbound bandwidth usage falls below 60%.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] trap-threshold output-rate 80 resume-rate 60
```

Related Topics

5.2.21 log-threshold

21.1.30 snmp-agent trap enable

5.2.39 trap-threshold error-statistics

Function

The **trap-threshold error-statistics** command sets the alarm threshold for error packets and alarm interval.

The **undo trap-threshold error-statistics** command restores the default alarm threshold for error packets and default alarm interval.

By default, the alarm threshold for error packets is 3 and the alarm interval is 10 seconds.

Format

trap-threshold error-statistics *threshold-value* **interval** *interval-value*

undo trap-threshold error-statistics

Parameters

Parameter	Description	Value
threshold-value	Sets the alarm threshold for error packets.	The value is an integer that ranges from 1 to 65535.
interval *interval-value*	Sets the interval for reporting alarms for error packets.	The value is an integer that ranges from 10 to 65530 and must be a multiple of 10, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

The system generates an alarm when the number of error packets received by an interface within an alarm interval exceeds the alarm threshold. If the number of

received error packets is 0 in the next alarm interval, the system displays an alarm clearance message.

Example

Set the alarm threshold for error packets on Eth2/0/0 to 10 and the alarm interval to 30 seconds.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] trap-threshold error-statistics 10 interval 30
```

5.2.40 virtual-cable-test

Function

The **virtual-cable-test** command tests the cable connected to an Ethernet electrical interface and displays the test result.

Format

virtual-cable-test

Parameters

None

Views

Ethernet interface view, GE interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **virtual-cable-test** command to check whether the cable works properly. According to the command output, you can locate and rectify cable faults.

- If the cable works properly, the total length of the cable is displayed.
- If the cable cannot work properly, the distance between the interface and the fault point is displayed.

Precautions

- The distance error generated during VCT detection is about 10 m. The test result is only for reference and may be inaccurate for cables of some vendors.
- Running the **virtual-cable-test** command may affect services on the interface in a short period of time.
- Combo electrical interfaces support cable tests.

 Copyright © Huawei Technologies Co., Ltd.

- Before performing a cable test, shut down the remote interface or remove the network cable from the remote interface. Otherwise, signals from the remote interface may make the test result inaccurate.

Example

Test the cable connected to Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] virtual-cable-test
Warning: The command will stop service for a while, continue[Y/N]?y
Pair A length: 189meter(s)
Pair B length: 189meter(s)
Pair C length: 189meter(s)
Pair D length: 189meter(s)
Pair A state: Ok
Pair B state: Ok
Pair C state: Ok
Pair D state: Ok
```

Table 5-17 Description of the virtual-cable-test command output

Item	Description
Pair A/B/C/D	Four pairs of circuits in a network cable.
Pair A length	Length of a network cable: ● The length is the distance between the interface and the fault point if a fault occurs. ● The length is the actual length of the cable when the cable works properly. ● The default length is 0 m if the interface is not connected to any network cable.
Pair A state	Network cable status: ● Ok: indicates that the circuit pair is terminated normally. ● Open: indicates that the circuit pair is not terminated. ● Short: indicates that the circuit pair is short-circuited. ● Crosstalk: indicates that the circuit pairs interfere with each other. ● Unknown: indicates that the circuit pair has an unknown fault.

5.3 Serial Interface Configuration Commands

5.3.1 async mode (serial)

Function

The **async mode** command sets the working mode for an asynchronous serial interface.

The **undo async mode** command restores the default setting.

By default, an asynchronous serial interface works in protocol mode.

Format

async mode { **flow** | **protocol** }

undo async mode

Parameters

Parameter	Description	Value
flow	Configures an asynchronous serial interface to work in flow mode.	-
protocol	Configures an asynchronous serial interface to work in protocol mode.	-

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two devices communicate by using asynchronous serial interfaces, the asynchronous serial interfaces work in protocol or flow mode. An asynchronous serial interface usually works in protocol mode. The flow mode is used for man-to-machine interactions such as dial-up.

- In protocol mode, serial interfaces on both ends establish a link based on the existing link layer protocol parameters after a physical connection is established between them.
- In flow mode, serial interfaces on both ends interact with each other, the local interface sends configuration information to the remote interface to set

 Copyright © Huawei Technologies Co., Ltd.

physical layer protocol parameters for the remote interface, and then the two interfaces establish a link based on the configured parameters.

Prerequisites

The serial interface has been configured to work in asynchronous mode by using the **physical-mode** command.

Precautions

- If you run the **async mode** command multiple times in the same serial interface view, only the latest configuration takes effect.
- After an asynchronous serial interface is configured to work in flow mode, the link layer protocol of this interface cannot be set to PPP.

Example

Configure an asynchronous serial interface to work in flow mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] physical-mode async
[Huawei-Serial1/0/0] async mode flow
```

Related Topics

5.3.20 physical-mode

5.3.21 phy-mru (serial)

5.3.2 baudrate

Function

The **baudrate** command sets the baud rate for a synchronous serial interface.

The **undo baudrate** command restores the default setting.

By default, the baud rate of a synchronous serial interface is 64000 bit/s.

Format

baudrate *baudrate*

undo baudrate

Parameters

Parameter	Description	Value
baudrate	Specifies the baud rate for a synchronous serial interface.	A synchronous serial interface supports the following baud rates, which are expressed in bit/s: ● 1200 ● 2400 ● 4800 ● 9600 ● 19200 ● 38400 ● 56000 ● 57600 ● 64000 ● 72000 ● 115200 ● 128000 ● 192000 ● 256000 ● 384000 ● 512000 ● 768000 ● 1024000 ● 2048000 ● 8192000

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Synchronous serial interfaces on both ends of a cable are of different types. One synchronous serial interface is a Data Terminal Equipment (DTE) interface, and the other is a Data Circuit-terminating Equipment (DCE) interface. A DTE refers to

 Copyright © Huawei Technologies Co., Ltd.

the device on which serial interfaces are connected to DTE cables; a DCE refers to the device on which serial interfaces are connected to DCE cables.

The baud rate determines the line transmission rate. You can set the baud rate on a DCE based on the cable type.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Precautions

If you run the **baudrate** command multiple times in the same serial interface view, only the latest configuration takes effect.

The **baudrate** command can be used only when the device functions as a DCE.

The baud rate range varies depending on the cable type.

- V.24DCE: 1200 bit/s to 64000 bit/s
- For the V.35DCE, RS449DCE, and RS530DCE, the baud rate range is as follows:
  - 1SA/2SA interface card: 1200 bit/s to 2048000 bit/s
  - 8SA interface card: 1200 bit/s to 8192000 bit/s
  - Serial interface on the AR2202-48FE: 1200 bit/s to 8192000 bit/s

NOTE

Ensure that the configured baud rate is the same as virtual baud rate (configured by the **virtualbaudrate** command) on the remote end (DTE). Otherwise, some packets will be discarded.

Example

Set the baud rate of a synchronous serial interface to 72000 bit/s.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] physical-mode sync
[Huawei-Serial2/0/0] baudrate 72000
```

Related Topics

5.3.20 physical-mode

5.3.23 virtualbaudrate

5.3.9 display interface serial

5.3.3 clock dce

Function

The **clock dce** command sets the clock mode for a synchronous serial interface on the DCE.

The **undo clock dce** command restores the default setting.

By default, the clock mode of a synchronous serial interface is **dceclk1** on the DCE.

Format

clock dce { **dceclk1** | **dceclk2** | **dceclk3** }

undo clock dce

Parameters

Parameter	Description	Setting
dceclk1	Sets the clock mode of a synchronous serial interface to **dceclk1** on the DCE.	-
dceclk2	Sets the clock mode of a synchronous serial interface to **dceclk2** on the DCE.	-
dceclk3	Sets the clock mode of a synchronous serial interface to **dceclk3** on the DCE. **NOTE** This parameter does not take effect for serial interfaces on 1SA/2SA interface cards.	-

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two communicating parties are connected through serial interfaces. One party functions as the DTE, and the other functions as the DCE. To exchange data successfully, communicating parties must work in clock synchronization state. For example, the DCE receive clock must be synchronized with the DTE transmit clock to ensure that the DCE can correctly receive data from the DTE.

Figure 5-1 shows the connections of clocks on synchronous serial interfaces. RD indicates a pin for receiving data. TD indicates a pin for sending data. RC, TC, and ETC indicate pins for sending or receiving clock signals.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-1 Connections of clocks on synchronous serial interfaces

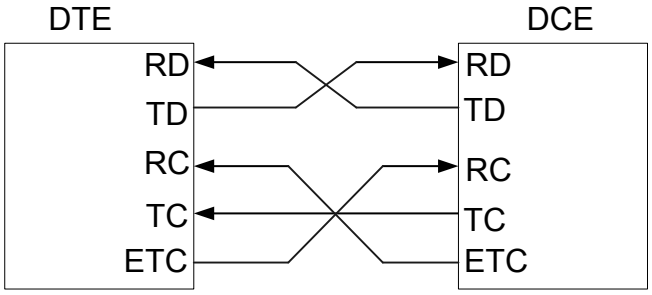


Table 5-18 describes the clock modes of a device functioning as a DCE. **TxClk** indicates the DCE send clock, and **RxClk** indicates the DCE receive clock. **RC** and **TC** indicate external clocks, and **Local** indicates a local clock.

Table 5-18 DCE clock modes

Clock Mode	Description	Precautions
dceclk1	TxClk = Local, RxClk = RC	• The DTE must use an RC clock as a receive clock. Otherwise, the DTE may receive error packets. • The DTE send clock must be synchronized with the ETC clock. Otherwise, the DCE may receive error packets.
dceclk2	TxClk = Local, RxClk = Local	The DTE must use RC clocks as its send and receive clocks. Otherwise, data transmission is abnormal.

 Copyright © Huawei Technologies Co., Ltd.

Clock Mode	Description	Precautions
dceclk3	TxClk = RC, RxClk = RC	• The DTE send clock must be synchronized with the ETC clock. Otherwise, the DCE may receive error packets. • The DTE receive clock must be synchronized with the ETC clock. Otherwise, the DTE may receive error packets.

Prerequisites

The serial interface has been configured to work in synchronous mode using the **physical-mode sync** command.

Precautions

If you run the **clock dce** command multiple times in the same serial interface view, only the latest configuration takes effect.

The **clock dce** command can be used only when the device functions as a DCE.

Example

Set the clock mode of Serial1/0/0 to **dceclk2** on the DCE.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] clock dce dceclk2
```

Related Topics

5.3.20 physical-mode

5.3.4 clock dte

Function

The **clock dte** command sets the clock mode for a synchronous serial interface on the DTE.

The **undo clock dte** command restores the default setting.

By default, the clock mode of a synchronous serial interface is **dteclk1** on the DTE.

Format

clock dte { **dteclk1** | **dteclk2** | **dteclk3** }

undo clock dte

Parameters

Parameter	Description	Setting
dteclk1	Sets the clock mode of a synchronous serial interface to **dteclk1** on the DTE. **NOTE** When the DTE uses an X.21 cable to connect to the DCE, the **dteclk2** mode is used even if you specify parameter **dteclk1** in the command.	-
dteclk2	Sets the clock mode of a synchronous serial interface to **dteclk2** on the DTE. **NOTE** When the DTE uses a V.24 cable to connect to the DCE, the DTE does not support parameter **dteclk2**.	-
dteclk3	Sets the clock mode of a synchronous serial interface to **dteclk3** on the DTE.	-

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Two communicating parties are connected through serial interfaces. One party functions as the DTE, and the other functions as the DCE. To exchange data successfully, communicating parties must work in clock synchronization state. For example, the DCE receive clock must be synchronized with the DTE transmit clock to ensure that the DCE can correctly receive data from the DTE.

Figure 5-2 shows the connections of clocks on synchronous serial interfaces. RD indicates a pin for receiving data. TD indicates a pin for sending data. RC, TC, and ETC indicate pins for sending or receiving clock signals.

 Copyright © Huawei Technologies Co., Ltd.

Figure 5-2 Connections of clocks on synchronous serial interfaces

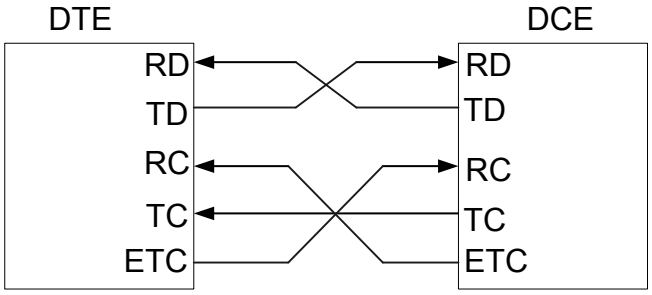


Table 5-19 describes the clock modes of a device functioning as a DTE. **TxClk** indicates the DTE send clock, and **RxClk** indicates the DTE receive clock. **RC** and **TC** indicate external clocks, and **Local** indicates a local clock.

Table 5-19 DTE clock modes

Clock Mode	Description	Precautions
dteclk1	TxClk = TC, RxClk = RC	The DTE uses clocks provided by the DCE. ● The DCE send clock must be synchronized with the ETC clock. Otherwise, the DTE may receive error packets. ● The DCE receive clock must be synchronized with the TC clock. Otherwise, the DCE may receive error packets.

 Copyright © Huawei Technologies Co., Ltd.

Clock Mode	Description	Precautions
dteclk2	TxClk = RC, RxClk = RC	The DTE uses clocks provided by the DCE. • The DCE send clock must be synchronized with the ETC clock. Otherwise, the DTE may receive error packets. • The DCE receive clock must be synchronized with the ETC clock. Otherwise, the DCE may receive error packets.
dteclk3	TxClk = Local, RxClk = RC	• The DCE send clock must be synchronized with the ETC clock. Otherwise, the DTE may receive error packets. • The DCE must use an RC clock as a receive clock. Otherwise, the DCE may receive error packets.

Prerequisites

The serial interface has been configured to work in synchronous mode using the **physical-mode sync** command.

Precautions

If you run the **clock dte** command multiple times in the same serial interface view, only the latest configuration takes effect.

The **clock dte** command can be used only when the device functions as a DTE.

Example

Set the clock mode of Serial1/0/0 to **dteclk2** on the DTE.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] clock dte dteclk2
```

Related Topics

5.3.20 physical-mode

5.3.5 code (serial)

Function

The **code** command sets the encoding and decoding mode for a synchronous serial interface.

The **undo code** command restores the default setting.

The default encoding and decoding mode of a synchronous serial interface is Non Return to Zero (NRZ).

Format

code { **nrz** | **nrzi** }

undo code

Parameters

Parameter	Description	Value
nrz	Sets the encoding and decoding mode to NRZ.	-
nrzi	Sets the encoding and decoding mode to Non Return to Zero Inverted (NRZI).	-

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NRZ and NRZI are encoding and decoding modes for synchronous serial interfaces.

- In NRZ, the positive level and negative level represent different logic values (1 or 0). The NRZ signal does not have a transition if the bit being transmitted is a logic 0.
- In NRZI, level inversion represents a logic value (1 or 0), and an unchanged level represents the other logic value (1 or 0). The NRZI signal does not have a transition if the bit being transmitted is a logic 0.

The default encoding and decoding mode of a synchronous serial interface is NRZ. When the encoding and decoding mode of the remote synchronous serial

 Copyright © Huawei Technologies Co., Ltd.

interface is NRZI, the encoding and decoding mode of the local synchronous serial interface needs to be changed to NRZI.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Precautions

If you run the **code** command multiple times in the same serial interface view, only the latest configuration takes effect.

If two devices communicate by using synchronous serial interfaces, the two devices must have the same encoding and decoding mode. Otherwise, received data frames will be decoded incorrectly and discarded as error frames.

Example

Set the encoding and decoding mode of a synchronous serial interface to NRZI.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] code nrzi
```

Related Topics

5.3.20 physical-mode

5.3.6 crc (serial)

Function

The **crc** command configures the cyclic redundancy check (CRC) mode of a synchronous serial interface.

The **undo crc** command restores the default CRC mode of a synchronous serial interface.

By default, the 16-bit CRC is used.

Format

crc { **16** | **32** | **none** }

undo crc

Parameters

Parameter	Description	Value
16	Indicates the 16-bit CRC.	-
32	Indicates the 32-bit CRC.	-

Parameter	Description	Value
none	Indicates that the synchronous serial interface does not perform CRC.	-

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CRC is a commonly used method to detect transmission errors in a communication system. It checks for transmission errors by adding redundancy codes to the original data. Transmission errors are more likely to be detected when more redundancy codes are added, but data is transmitted at a lower efficiency. Use the 16-bit or 32-bit CRC mode as required.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Configuration Impact

If you run the **crc** command multiple times in the same serial interface view, only the latest configuration takes effect.

Example

Set the CRC mode to 32-bit CRC on Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-serial1/0/0] ] physical-mode sync
[Huawei-Serial1/0/0] crc 32
```

5.3.7 detect dcd

Function

The **detect dcd** command enables Data Carrier Detect (DCD) signal detection on a synchronous serial interface.

The **undo detect dcd** command disables Data Carrier Detect (DCD) signal detection on a synchronous serial interface.

By default, DCD signal detection is enabled on a synchronous serial interface.

Format

detect dcd

undo detect dcd

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DCD signals monitor the working status of lines and DCEs. The **detect dcd** command enables DCD signal detection on a synchronous serial interface. DCD signal detection is used together with detection of Data Set Ready (DSR) and Data Terminal Ready (DTR) signals to determine the status of the synchronous serial interface.

The status of a synchronous serial interface is determined based on the following items:

- If detection of DSR and DTR signals is enabled on the interface, the device determines the status (Up or Down) of the interface by detecting DSR and DTR signals and checking whether the interface is connected to an external cable. The device considers the interface Up only when DSR and DCD signals are valid and the interface is connected to an external cable.
- If detection of DSR and DTR signals is disabled on the interface, the device considers that the interface is in Up state as long as it detects that the interface is connected to an external cable.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Example

Enable DCD signal detection on a synchronous serial interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] detect dcd
```

Related Topics

5.3.20 physical-mode

 Copyright © Huawei Technologies Co., Ltd.

5.3.9 display interface serial
5.3.8 detect dsr-dtr (serial)

5.3.8 detect dsr-dtr (serial)

Function

The **detect dsr-dtr** command enables detection of DSR and DTR signals on a serial interface.

The **undo detect dsr-dtr** command disables detection of DSR and DTR signals on a serial interface.

By default, detection of DSR and DTR signals is enabled on a serial interface.

Format

detect dsr-dtr

undo detect dsr-dtr

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

A DCE sends DSR signals to tell a DTE whether it is working, and a DTE sends DTR signals to tell a DCE whether it is working. The **detect dsr-dtr** command enables DSR and DTR signal detection on a serial interface, helping to determine the status of the serial interface.

The status of an asynchronous serial interface is determined based on the following items:

- If detection of DSR and DTR signals is enabled on the interface, the device considers the interface Up only when valid DSR signals are detected and the interface is connected to an external cable.
- If detection of DSR and DTR signals is disabled on the interface, the device automatically notifies users that the interface is in Up state without detecting whether the interface is connected to an external cable.

Example

Enable detection of DSR and DTR signals on a serial interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] detect dsr-dtr
```

Related Topics

5.3.20 physical-mode

5.3.9 display interface serial

5.3.7 detect dcd

5.3.9 display interface serial

Function

The **display interface serial** command displays the running status of and statistics about a serial interface.

Format

display interface serial [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a serial interface. If no interface number is specified, the running status of and statistics about all serial interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the serial interface status or locating faults on a serial interface, you can run the **display interface serial** command to view the running status of and statistics about the serial interface. You can collect traffic statistics and locate faults on the serial interface according to the command output.

Example

Display the status of Serial1/0/0.

```
<Huawei> display interface serial 1/0/0
Serial1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2011-02-25 16:00:49
Description:HUAWEI, AR Series, Serial1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 1.1.1.1/24
Link layer protocol is nonstandard HDLC
Last physical up time   : 2011-02-25 16:00:50
Last physical down time : 2011-02-25 16:00:49
Current system time: 2011-02-25 16:40:01
Last 300 seconds input rate 5210 bytes/sec 41680 bits/sec 100 packets/sec
Last 300 seconds output rate 5009 bytes/sec 40072 bits/sec 100 packets/sec
Input: 0 packets, 0 bytes
  Broadcast:            0,  Multicast:            0
  Errors:               0,  Runts:                0
  Giants:               0,  CRC:                  0

  Alignments:           0,  Overruns:             0
  Dribbles:             0,  Aborts:               0
  No Buffers:           0,  Frame Error:          0

Output: 0 packets, 0 bytes
  Total Error:          0,  Overruns:             0
  Collisions:           0,  Deferred:             0
  No Buffers:           0
    Input bandwidth utilization  : 0%
    Output bandwidth utilization : 0%
```

Table 5-20 Description of the display interface serial command output

Item	Description
Serial1/0/0 current state	Current physical status of the serial interface: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface. **damping** indicates that the interface is suppressed because of frequent flapping.
Last line protocol up time	Last time the link layer protocol of the interface goes Up.
Description	Description of the interface.

Item	Description
The Maximum Transmit Unit is	Maximum Transmission Unit (MTU) of the interface. The default MTU on a serial interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is enabled, the packets are discarded. To set the MTU, run the **mtu** command.
Internet Address is	IP address and subnet mask of the interface.
Last physical up time	Last time the link layer protocol of the interface goes Up.
Last physical down time	Last time the link layer protocol of the interface goes Down.
Hold timer	Lifecycle of a packet. If a packet is not sent out before the hold timer times out, the packet is discarded.
Internet Address	IP address of the interface. If no IP address is assigned to the interface, the system displays "Internet protocol processing: disabled."
Link layer protocol	Link layer protocol of the serial interface.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Interface is	Cable type of the serial interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Errors	Number of error packets detected at the physical layer.
Runts	Number of undersized frames with the correct FCS received by the interface.
Giants	Number of received jumbo frames with the correct FCS.
CRC	Number of CRC error packets received by the interface.
Alignments	Number of received packets with alignment errors.
Overruns	Number of received packets above the upper limit of the FIFO queue.
Aborts	Number of received packets aborted unexpectedly.
No Buffers	Number of received packets that cannot be buffered.
Frame Error	Number of received packets with frame errors.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Overruns	Number of sent packets below the upper limit of the FIFO queue.
Collisions	Number of sent packets with 1 to 15 conflict events.
Deferred	Number of delayed packets without conflict.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

Related Topics

5.3.19 mtu (serial)

5.3.10 display tdm statistic

Function

The **display tdm statistic** command displays service statistics of a TDM interface.

Format

display tdm statistic interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the number of a TDM interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring the TDM service, you can run this command to view service statistics of a TDM interface.

Precautions

- The service statistics of a TDM interface can be displayed only after the TDM service is configured.
- TDM interfaces include the synchronous/asynchronous serial interfaces that work in synchronous mode on the 8SA interface card, the interfaces formed by CE1/PRI or CT1/PRI interfaces (excluding ISDN PRI interfaces) on the 8E1T1-M interface card, and the interfaces formed by E1-F or T1-F interfaces on the 8E1T1-F interface card.

Example

Display service statistics of a TDM interface.

```
<Huawei> display tdm statistic interface serial 2/0/0
Serial2/0/0
  TxPkts  = 370066
  RxPkts  = 370858
  LosPkts  = 1064
  Overrun Count   = 308
  Underrun Count  = 83342
  MisOrderPkts    = 428
  MalformedPkts   = 328
```

Table 5-21 Description of the display tdm statistic command output

Item	Description
Serial2/0/0:0	TDM interface to be queried.
TxPkts	Number of packets that are sent.
RxPkts	Number of packets that are received.
LosPkts	Number of packets that are discarded.
Overrun Count	Number of packets that exceed the buffer upper limit.
Underrun Count	Number of packets that exceed the buffer lower limit.
MisOrderPkts	Number of packets not in sequence.
MalformedPkts	Number of malformed packets.

Related Topics

5.3.17 link-protocol tdm

5.3.11 idlecode (serial)

Function

The **idlecode** command sets the line idle code for a synchronous serial interface.

The **undo idlecode** command restores the default setting.

By default, a synchronous serial interface uses the line idle code 0x7e.

Format

idlecode { **7e** | **ff** }

undo idlecode

Parameters

Parameter	Description	Value
7e	Sets the line idle code to 0x7e for a synchronous serial interface.	-
ff	Sets the line idle code to 0xff for a synchronous serial interface.	-

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A synchronous serial interface transmits electrical signals, and therefore the interface line keeps transmitting data. When the interface line is idle, the line idle code is used to indicate that the line is idle.

NOTE

A synchronous serial interface supports two line idle codes: 0x7e and 0xff. The default line idle code 0x7e is recommended.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Precautions

If you run the **idlecode** command multiple times in the same serial interface view, only the latest configuration takes effect.

Two devices can communicate properly only when the same line idle code is set for serial interfaces on both devices.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the line idle code to 0xff for a synchronous serial interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] idlecode ff
```

Related Topics

5.3.20 physical-mode

5.3.12 interface serial

Function

The **interface serial** command displays the serial interface view.

Format

interface serial *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a serial interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To set attributes for a serial interface, run the **interface serial** command to enter the serial interface view.

Example

Enter the view of Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0]
```

Related Topics

5.3.9 display interface serial

 Copyright © Huawei Technologies Co., Ltd.

5.3.13 invert receive-clock

Function

The **invert receive-clock** command configures the device to invert clock signals received by a synchronous serial interface.

The **undo invert receive-clock** command restores the default setting.

By default, clock signals received by a synchronous serial interface are not inverted.

Format

invert receive-clock

undo invert receive-clock

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some special scenarios, clock delay occurs on a link. Then clocks on two ends are not synchronized or a large number of packets are discarded. To resolve this problem, configure the serial interface to invert clock signals that the serial interface sends and receives.

The procedure for determining clock signal inverting is as follows:

- By default, clock signals received by a synchronous serial interface are not inverted. If the protocol status of the synchronous serial interface can be Up, you do not need to modify the configuration of the synchronous serial interface. If the protocol status of the synchronous serial interface cannot be Up, check the packet statistics on the synchronous serial interface.
  - If the DTE receives error packets, for example, the packet count is not a multiple of the byte count, run the **invert receive-clock** command to configure the device to invert clock signals received by the synchronous serial interface.
  - If the DTE does not receive error packets but the DCE receives error packets, run the **invert transmit-clock** command to configure the device to invert clock signals transmitted by the synchronous serial interface.

 Copyright © Huawei Technologies Co., Ltd.

- If error packets are still increasing after the **invert receive-clock** and **invert transmit-clock** commands are executed, contact Huawei technical support personnel.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Precautions

NOTE

You can configure the device to invert clock signals received by a synchronous serial interface as required.

Example

Configure the device to invert clock signals received by a synchronous serial interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] invert receive-clock
```

Related Topics

5.3.20 physical-mode

5.3.15 invert transmit-clock

5.3.14 invert receive-clock auto

Function

The **invert receive-clock auto** command configures the device to automatically invert clock signals received by a synchronous serial interface.

The **undo invert receive-clock auto** command restores the default setting.

By default, clock signals received by a synchronous serial interface are not inverted.

Format

invert receive-clock auto

undo invert receive-clock auto

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When line signals are frequently interfered, clock delays may occur on the line from time to time. The device having the **invert receive-clock** command configured inverts clock signals received by a serial interface only once and does not invert clock signals for subsequent delays. In addition, when the delay disappears, the received clock signals are not automatically inverted back. As a result, clock signals are still not synchronized on the two interworking parties.

To resolve the problem, you can run the **invert receive-clock auto** command on the serial interface to configure the device to automatically invert clock signals. In this way, the received clock signals are automatically inverted upon clock delays on the line. When the delays disappear, the received clock signals are automatically inverted back, preventing impact of the delays and ensuring that clock signals are synchronized on the two interworking parties.

Prerequisites

The serial interface has been configured to work in synchronous mode using the **physical-mode sync** command.

Precautions

- The **invert receive-clock auto** command takes effect only on serial interfaces of the 1SA and 2SA interface cards.
- The **invert receive-clock auto** and **invert receive-clock** command cannot be configured simultaneously on the same interface.

Example

Configure the device to automatically invert clock signals received by the synchronous Serial1/0/0 interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] invert receive-clock auto
```

Related Topics

5.3.13 invert receive-clock

5.3.15 invert transmit-clock

Function

The **invert transmit-clock** command configures the device to invert clock signals transmitted by a synchronous serial interface.

The **undo invert transmit-clock** command restores the default setting.

By default, clock signals transmitted by a synchronous serial interface are not inverted.

Format

invert transmit-clock

undo invert transmit-clock

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some special scenarios, clock delay occurs on a link. Then clocks on two ends are not synchronized or a large number of packets are discarded. To resolve this problem, configure the serial interface to invert clock signals that the serial interface sends and receives.

The procedure for determining clock signal inverting is as follows:

- By default, clock signals received by a synchronous serial interface are not inverted. If the protocol status of the synchronous serial interface can be Up, you do not need to modify the configuration of the synchronous serial interface. If the protocol status of the synchronous serial interface cannot be Up, check the packet statistics on the synchronous serial interface.
  - If the DTE receives error packets, for example, the packet count is not a multiple of the byte count, run the **invert receive-clock** command to configure the device to invert clock signals received by the synchronous serial interface.
  - If the DTE does not receive error packets but the DCE receives error packets, run the **invert transmit-clock** command to configure the device to invert clock signals transmitted by the synchronous serial interface.
- If error packets are still increasing after the **invert receive-clock** and **invert transmit-clock** commands are executed, contact Huawei technical support personnel.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Precautions

NOTE

You can configure the device to invert clock signals transmitted by a synchronous serial interface as required.

Example

Configure the device to invert clock signals transmitted by a synchronous serial interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] invert transmit-clock
```

Related Topics

5.3.20 physical-mode

5.3.13 invert receive-clock

5.3.16 itf number (serial interface view)

Function

The **itf number** command sets the number of interframe filling tags of a synchronous serial interface.

The **undo itf number** command restores the default setting.

By default, the number of interframe filling tags of a synchronous serial interface is 4.

Format

itf number *number*

undo itf number

Parameters

Parameter	Description	Value
number	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 14. Each interframe filling tag occupies one byte.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interframe filling tag is a code sent when an interface does not send any service data, and allows the receiver to have a period of time for processing the received data frame and getting ready to receive the next frame.

Interframe filling tags generate extra costs and affect the transmission rate of the interface. You can use the **itf number** command to manually set a proper number of interframe filling tags between two neighboring frames, ensuring a proper transmission rate.

- When you increase the number of interframe filling tags, the rate of sending valid data packets decreases.
- When you decrease the number of interframe filling tags, the rate of sending valid data packets increases.

  NOTE

  Since interframe filling tags bring extra costs, the transmission rate of a serial interface usually does not reach the bandwidth requirement. To increase the transmission rate of the serial interface, set a small number of interframe filling tags using the **itf number** command.

Prerequisites

The serial interface has been configured to work in synchronous mode using the **physical-mode sync** command.

Precautions

- Interfaces on both ends can communicate only when the same number of interframe filling tags is set for them.
- The number of interframe filling tags cannot be set to 2 on the 1SA and 2SA interface cards.
- Serial interfaces formed by E1/T1 interfaces do not support the **itf number** command.

Example

Set the number of interframe filling tags to 1 on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] itf number 1
```

5.3.17 link-protocol tdm

Function

The **link-protocol tdm** command sets the encapsulation protocol to TDM for a serial interface.

The **undo link-protocol tdm** command restores the default setting.

By default, PPP is used as the encapsulation protocol on a serial interface.

NOTE

The serial interface formed by the 6E&M card supports only TDM as the encapsulation protocol.

Format

link-protocol tdm

undo link-protocol tdm

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a serial interface to send and receive TDM data, run the **link-protocol tdm** command to set the encapsulation protocol to TDM for the serial interface.

NOTE

- When changing the encapsulation protocol to TDM, you can directly enable TDM without disabling the original encapsulation protocol.
- After the encapsulation protocol is set to TDM, the interface does not support subinterface creation.

Precautions

- The configuration of the **link-protocol tdm** command overrides the configurations of previous link-layer protocols, interrupts services of the protocols, and releases resources occupied by the protocols.
- The following serial interfaces support this command: synchronous/asynchronous serial interfaces on the 8SA interface card, interfaces formed by CE1/PRI, CT1/PRI interfaces (excluding ISDN PRI interfaces) on the 8E1T1-M interface card, interfaces formed by E1-F or T1-F interfaces on the 8E1T1-F interface card and E&M interfaces.

  NOTE

  The encapsulation protocol can be set to TDM on the 8SA, 8E1T1-M, and 8E1T1-F interface cards of the device only when the device MPU can deliver the 8KHZ clock to the 8SA, 8E1T1-M, and 8E1T1-F interface cards. The MPU can be: SRU40, SRU60, SRU80, or SRU100.

  The encapsulation protocol can be set to TDM only on the VB interface cards among 8E1T1-M and 8E1T1-F interface cards. You can run the **display version slot** *slot-id* command in the diagnosis view to check the version number of the 8E1T1-M or 8E1T1-F interface card on the specified slot. If the **PCB** field value is **VER.B**, the 8E1T1-M or 8E1T1-F interface card is the VB interface card.

Example

Set the encapsulation protocol to TDM on Serial2/0/0.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol tdm
```

5.3.18 loopback

Function

Using the **loopback** command, you can enable loopback detection and set the loopback detection mode on a serial interface.

Using the **undo loopback** command, you can restore the default setting.

By default, internal loopback detection is disabled.

Format

loopback { **local** | **remote** }

undo loopback

Parameters

Parameter	Description	Value
local	Sets internal loopback.	-
remote	Sets external loopback.	-

Views

Serial interface view, async interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function detects the interface status or cable status and must be disabled when devices work properly.

- In internal loopback mode, the local device loops back outgoing packets to itself to test whether it works properly.
- In external loopback mode, the local device loops back the packets received from its peer device to the peer device to test whether the link between the two devices works properly.

Example

Enable internal loopback detection on Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] loopback local
```

5.3.19 mtu (serial)

Function

The **mtu** command sets the MTU for a serial interface.

The **undo mtu** command restores the default MTU.

By default, the MTU of a serial interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a serial interface.	The value is an integer and the value depends on the device.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than the MTU.

If forcible unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. Therefore, large packets must be forcibly

 Copyright © Huawei Technologies Co., Ltd.

fragmented to prevent packet loss on the network. In this case, you can run the **mtu** command to set the size of a fragment.

Configuration Impact

If you run the **mtu** command multiple times in the same serial interface view, only the latest configuration takes effect.

Follow-up Procedure

Run the **shutdown** and **undo shutdown**/**restart** commands to restart the related physical interface to make the configuration take effect.

Example

Set the MTU of a serial interface to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] mtu 1200
[Huawei-Serial1/0/0] restart
```

Related Topics

5.3.9 display interface serial

5.3.20 physical-mode

Function

The **physical-mode** command sets the working mode for a serial interface.

By default, a serial interface works in synchronous mode.

Format

physical-mode { **async** | **sync** }

Parameters

Parameter	Description	Value
async	Configures a serial interface to work in asynchronous mode.	-
sync	Configures a serial interface to work in synchronous mode.	-

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A serial interface works in synchronous or asynchronous mode. When a serial interface is used to establish a Digital Data Network (DDN) leased line or connects to a terminal, the serial interface works in synchronous mode. When a serial interface is used to establish an asynchronous leased line or is used for modem dial-up, data backup, or terminal access, the serial interface works in asynchronous mode.

Precautions

If you run the **physical-mode** command multiple times in the same serial interface view, only the latest configuration takes effect.

Serial interfaces on both ends must work in the same mode.

Synchronous serial interfaces on both ends of a cable are of different types. One synchronous serial interface is a Data Terminal Equipment (DTE) interface, and the other is a Data Circuit-terminating Equipment (DCE) interface. The device where a DTE interface is located is a DTE, and the device where a DCE interface is located is a DCE. The device functions as a DTE or DCE.

The serial interface on the main control board of AR2202-48FE can work only in synchronous mode. Therefore, the AR2202 does not support this command.

When changing the working mode of a serial interface, run the **reset counters interface serial** *interface-number* command to clear the statistics on the interface to ensure the statistics accuracy.

Example

Configure a serial interface to work in asynchronous mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] physical-mode async
```

Related Topics

5.3.9 display interface serial

5.3.21 phy-mru (serial)

Function

The **phy-mru** command sets the maximum receive unit (MRU) for an asynchronous serial interface.

The **undo phy-mru** command restores the default MRU.

By default, the MRU of an asynchronous serial interface is 1700 bytes.

Format

phy-mru *mrusize*

undo phy-mru

Parameters

Parameter	Description	Value
mrusize	Specifies the MRU for an asynchronous serial interface.	The value is an integer that ranges from 4 to 1700, in bytes.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MRU is the maximum size of a packet that can be received by an interface. The MTU of a serial interface cannot be greater than the MRU of the interface, ensuring that both ends are capable of receiving packets from each other.

Prerequisites

The serial interface has been configured to work in asynchronous mode by using the **physical-mode** command.

Configuration Impact

If you run the **phy-mru** command multiple times in the same serial interface view, only the latest configuration takes effect.

Example

Set the MRU to 1200 bytes for an asynchronous serial interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] phy-mru 1200
```

Related Topics

5.3.20 physical-mode

5.3.1 async mode (serial)

 Copyright © Huawei Technologies Co., Ltd.

5.3.22 reverse-rts

Function

The **reverse-rts** command configures the device to invert Request To Send (RTS) signals of a synchronous serial interface.

The **undo reverse-rts** command restores the default setting.

By default, RTS signals of a synchronous serial interface are not inverted.

Format

reverse-rts

undo reverse-rts

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A synchronous serial interface works in full duplex mode by default. To make the device compatible with devices working in half duplex mode, run the **reverse-rts** command to configure the device to invert RTS signals of a synchronous serial interface so that RTS signals become invalid. Then the remote interface does not send data when the local interface is sending data.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Example

Configure the device to invert RTS signals of a synchronous serial interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] reverse-rts
```

Related Topics

5.3.20 physical-mode

5.3.9 display interface serial

 Copyright © Huawei Technologies Co., Ltd.

5.3.23 virtualbaudrate

Function

The **virtualbaudrate** command sets the virtual baud rate for a synchronous serial interface.

The **undo virtualbaudrate** command restores the default setting.

The default virtual baud rate of a synchronous serial interface is 64000 bit/s.

Format

virtualbaudrate *virtualbaudrate*

undo virtualbaudrate

Parameters

Parameter	Description	Value
virtualbaudrate	Specifies the virtual baud rate for a synchronous serial interface.	A synchronous serial interface supports the following baud rates, which are expressed in bit/s: ● 1200 ● 2400 ● 4800 ● 9600 ● 19200 ● 38400 ● 56000 ● 57600 ● 64000 ● 72000 ● 115200 ● 128000 ● 192000 ● 256000 ● 384000 ● 512000 ● 768000 ● 1024000 ● 2048000 ● 8192000

 Copyright © Huawei Technologies Co., Ltd.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **virtualbaudrate** command sets the baud rate for a serial interface of a DTE.

Prerequisites

The serial interface has been configured to work in synchronous mode by using the **physical-mode** command.

Precautions

If you run the **virtualbaudrate** command multiple times in the same serial interface view, only the latest configuration takes effect.

The **virtualbaudrate** command can be used only on a DTE.

The virtual baud rate range varies depending on the cable type.

- V.24DTE: 1200 bit/s to 64000 bit/s
- For the V.35DTE, X.21DTE, RS449DTE, and RS530DTE, the virtual baud rate range is as follows:
  - 1SA/2SA interface card: 1200 bit/s to 2048000 bit/s
  - 8SA interface card: 1200 bit/s to 8192000 bit/s
  - Serial interface on the AR2202-48FE: 1200 bit/s to 8192000 bit/s

NOTE

Ensure that the configured virtual baud rate is the same as baud rate (configured by the **baudrate** command) on the remote end (DCE). Otherwise, some packets will be discarded.

Example

Set the virtual baud rate of a synchronous serial interface to 72000 bit/s.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] physical-mode sync
[Huawei-Serial1/0/0] virtualbaudrate 72000
```

Related Topics

5.3.20 physical-mode

5.3.2 baudrate

5.3.9 display interface serial

 Copyright © Huawei Technologies Co., Ltd.

5.4 Async Interface Configuration Commands

5.4.1 async mode (async)

Function

The **async mode** command sets the working mode for an async interface.

The **undo async mode** command restores the default setting.

By default, an async interface works in protocol mode.

Format

async mode { **flow** | **protocol** }

undo async mode

Parameters

Parameter	Description	Value
flow	Configures an async interface to work in flow mode.	-
protocol	Configures an async interface to work in protocol mode.	-

Views

Async interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two devices communicate by using async interfaces, the async interfaces work in protocol or flow mode. An async interface usually works in protocol mode. The flow mode is used for man-to-machine interactions such as dial-up.

- In protocol mode, async interfaces on both ends establish a link based on the existing link layer protocol parameters after a physical connection is established between them.

 Copyright © Huawei Technologies Co., Ltd.

- In flow mode, async interfaces on both ends interact with each other, the local interface sends configuration information to the remote interface to set physical layer protocol parameters for the remote interface, and then the two interfaces establish a link based on the configured parameters.

Precautions

If you run the **async mode** command multiple times in the same async interface view, only the latest configuration takes effect.

After an async interface is configured to work in flow mode, the link layer protocol of this interface cannot be set to PPP, and mirroring and packet capturing cannot be configured on this interface.

After run the **async mode flow** command to set the working mode of the Async interface to flow mode, the physical layer status of the Async interface is Up by default.

Example

Configure an async interface to work in flow mode.

```
<Huawei> system-view
[Huawei] interface async 2/0/0
[Huawei-Async2/0/0] async mode flow
```

Related Topics

5.4.6 phy-mru (async)

5.4.2 detect dsr-dtr (async)

Function

The **detect dsr-dtr** command enables detection of DSR and DTR signals on an async interface.

The **undo detect dsr-dtr** command disables detection of DSR and DTR signals on an async interface.

By default, detection of DSR and DTR signals is enabled on an async interface.

Format

detect dsr-dtr

undo detect dsr-dtr

Parameters

None

Views

Async interface view

Default Level

2: Configuration level

Usage Guidelines

The **detect dsr-dtr** command enables DSR and DTR signal detection on an async interface, helping to determine the status of the async interface.

The status of an async interface is determined based on the following items:

- If detection of DSR and DTR signals is enabled on the interface, the device considers the interface Up only when valid DSR signals are detected and the interface is connected to an external cable.
- If detection of DSR and DTR signals is disabled on the interface, the device automatically notifies users that the interface is in Up state without detecting whether the interface is connected to an external cable.

Example

Enable detection of DSR and DTR signals on an async interface.

```
<Huawei> system-view
[Huawei] interface async 2/0/0
[Huawei-Async2/0/0] detect dsr-dtr
```

Related Topics

5.4.3 display interface async

5.4.3 display interface async

Function

The **display interface async** command displays the running status of and statistics about an async interface.

Format

display interface async [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an async interface. If no interface number is specified, the running status of and statistics about all serial interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the async interface status or locating faults on an async interface, you can run the **display interface async** command to view the running status of and statistics about the async interface. You can collect traffic statistics and locate faults on the async interface according to the command output.

Example

Display the status of Async 2/0/0.

```
<Huawei> display interface async 2/0/0
Async2/0/0 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, Huawei Series, Async2/0/0 Interface
Route Port,The Maximum Transmit Unit is 1200, Hold timer is 10(sec)
Internet Address is 10.137.77.69/24
Last physical up time   : 2011-01-16 21:09:21
Last physical down time : 2011-01-16 21:08:31
Current system time: 2011-01-16 21:09:37
Physical layer is asynchronous, Baudrate is 9600 bps
Last 300 seconds input rate 0 bytes/sec 0 bits/sec 0 packets/sec
Last 300 seconds output rate 0 bytes/sec 0 bits/sec 0 packets/sec
Input: 0 packets, 0 bytes
  Broadcast:            0,  Multicast:            0
  Errors:               0,  Runts:                0
  Giants:               0,  CRC:                  0

  Alignments:           0,  Overruns:             0
  Dribbles:             0,  Aborts:               0
  No Buffers:           0,  Frame Error:          0

Output: 3 packets, 9 bytes
  Total Error:          0,  Overruns:             0
  Collisions:           0,  Deferred:             0

DCD=DOWN DTR=UP DSR=DOWN RTS=UP CTS=DOWN
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-22 Description of the display interface async command output

Item	Description
Async2/0/0 current state	Current physical status of the async interface: • UP: indicates that the interface is physically Up. • DOWN: indicates that the interface is physically Down. • Administratively down: indicates that the administrator has run the **shutdown** command on the interface.

Item	Description
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface. **damping** indicates that the interface is suppressed because of frequent flapping.
Description	Description of the interface.
The Maximum Transmit Unit is	Maximum transmit unit (MTU) of the interface. By default, the MTU is 1488 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded. You can run the **mtu** command to set the MTU.
Internet Address is	IP address and subnet mask of the interface.
Last physical up time	Last time the link layer protocol of the interface goes Up.
Last physical down time	Last time the link layer protocol of the interface goes Down.
Hold timer	Lifecycle of a packet. If a packet is not sent out before the hold timer times out, the packet is discarded.
Internet Address	IP address of the interface. If no IP address is assigned to the interface, the system displays "Internet protocol processing: disabled."
Link layer protocol	Link layer protocol of the serial interface.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Interface is	Cable type of the serial interface.
Broadcasts	Number of broadcast packets received or sent by the interface.
Multicasts	Number of multicast packets received or sent by the interface.
Errors	Number of error packets detected at the physical layer.
Runts	Number of undersized frames with the correct FCS received by the interface.
Giants	Number of received jumbo frames with the correct FCS.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CRC	Number of CRC error packets received by the interface.
Align errors	Number of received packets with alignment errors.
Overruns	Number of received packets above the upper limit of the FIFO queue.
Aborts	Number of received packets aborted unexpectedly.
No Buffers	Number of received packets that cannot be buffered.
Frame Errors	Number of received packets with frame errors.
Underruns	Number of sent packets below the lower limit of the FIFO queue.
Collisions	Number of sent packets with 1 to 15 conflict events.
Deferreds	Number of delayed packets without conflict.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

Related Topics

5.4.5 mtu (async)

5.4.4 interface async

Function

The **interface async** command displays the async interface view.

Format

interface async *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an async interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To set attributes for an async interface, run the **interface async** command to enter the async interface view.

Example

Enter the view of Async 2/0/0.

```
<Huawei> system-view
[Huawei] interface async 2/0/0
[Huawei-Async2/0/0]
```

Related Topics

5.4.3 display interface async

5.4.5 mtu (async)

Function

The **mtu** command sets the MTU for an async interface.

The **undo mtu** command restores the default MTU.

By default, the MTU of an async interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of an async interface.	The value is an integer that ranges from 128 to 1500, in bytes.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than the MTU.

If forcible unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. Therefore, large packets must be forcibly fragmented to prevent packet loss on the network. In this case, you can run the **mtu** command to set the size of a fragment.

Configuration Impact

If you run the **mtu** command multiple times in the same async interface view, only the latest configuration takes effect.

Follow-up Procedure

Run the **shutdown** and **undo shutdown**/**restart** commands to restart the related physical interface to make the configuration take effect.

Example

Set the MTU of an async interface to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface async 2/0/0
[Huawei-Async2/0/0] mtu 1200
[Huawei-Async2/0/0] restart
```

Related Topics

5.4.3 display interface async

5.4.6 phy-mru (async)

Function

The **phy-mru** command sets the maximum receive unit (MRU) for an async interface.

The **undo phy-mru** command restores the default MRU.

By default, the MRU of an async interface is 1700 bytes.

Format

phy-mru *mrusize*

undo phy-mru

Parameters

Parameter	Description	Value
mrusize	Specifies the MRU of an async interface.	The value is an integer that ranges from 4 to 1700, in bytes.

Views

Async interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MRU is the maximum size of a packet that can be received by an interface. The MTU of an async interface cannot be greater than the MRU of the interface, ensuring that both ends are capable of receiving packets from each other.

Configuration Impact

If you run the **phy-mru** command multiple times in the same async interface view, only the latest configuration takes effect.

Example

Set the MRU to 1200 bytes for an async interface.

```
<Huawei> system-view
[Huawei] interface async 2/0/0
[Huawei-Async2/0/0] phy-mru 1200
```

Related Topics

5.4.1 async mode (async)

5.5 CE1/PRI Interface Configuration Commands

5.5.1 channel-set (CE1/PRI interface view)

Function

Using the **channel-set** command, you can bundle timeslots of a CE1/PRI interface to form a channel set.

Using the **undo channel-set** command, you can cancel the configuration.

By default, no timeslot of a CE1/PRI interface is bundled to form a channel set.

Format

channel-set *set-number* **timeslot-list** *list*

undo channel-set [*set-number*]

Parameters

Parameter	Description	Value
set-number	Specifies the number of the channel set.	The value is an integer that ranges from 0 to 30.
timeslot-list *list*	Specifies the timeslot to be bundled.	*list* specifies the number of a timeslot, and its value ranges from 1 to 31. You can specify a single timeslot by using *number*, specify a timeslot range by using *number1-number2*, or specify multiple timeslots by using *number1,number2-number3*.

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a family or a small enterprise, multiple terminals (such as telephones, fax machines, and computers) may share the same E1 link. In this situation, timeslots of the E1 link need to be bundled to form channel sets. Each channel set transmits a type of service. For example, 2 timeslots are used for voice transmission, and 16 timeslots are used for Internet access.

When a CE1/PRI interface works in CE1 mode, its 2 Mbit/s transmission line is divided into 32 timeslots at a rate of 64 kbit/s. Timeslot 0 transmits synchronization signals, and the remaining 31 timeslots can be bundled randomly to form multiple channel sets. Each channel set transmits a type of service.

After the **channel-set** command is run, a serial interface is created automatically. It has the same logical features as a synchronous serial interface. The number format of a serial interface is "serial *interface-number.set-number*". *interface-number* specifies the number of a CE1/PRI interface, and *set-number* specifies the number of a channel set.

Prerequisites

A CE1/PRI interface has been configured to work in CE1/PRI mode by using the **using ce1** command.

Precautions

- The **channel-set** and **pri-set (CE1/PRI interface view)** commands cannot be used on the same CE1/PRI interface. That is, you can configure only one timeslot bundling mode on a CE1/PRI interface.
- Timeslots of a CE1 interface can be bundled to form a maximum of 31 channel sets and a minimum of 1 channel set. That is, a single timeslot can form a channel set, and 31 timeslots can be bundled to form one channel set.

  NOTE

  If you run the **channel-set** command in the same CE1/PRI interface view multiple times, multiple channel sets can be formed by bundling timeslots. One timeslot can be bundled to only one channel set.
- Channel sets on the local and remote CE1/PRI interfaces must contain the same timeslots; otherwise, errors will occur in communication.

Example

Bundle timeslots 1, 10 to 16, and 18 of CE1 1/0/0 to form channel set 0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] using ce1
[Huawei-E1 1/0/0] channel-set 0 timeslot-list 1,10-16,18
```

Related Topics

5.5.18 pri-set (CE1/PRI interface view)

5.5.21 using (CE1/PRI interface view)

5.5.2 clock (CE1/PRI interface view)

Function

Using the **clock** command, you can set the clock mode for a CE1/PRI interface.

Using the **undo clock** command, you can restore the default setting.

By default, a CE1/PRI interface works in slave clock mode.

Format

clock { **master** | **slave** | **system** }

undo clock

Parameters

Parameter	Description	Value
master	Configures a CE1/PRI interface to work in master clock mode and use internal clock signals. When a CE1/PRI interface functions as a Data Circuit-terminating Equipment (DCE), it must work in master clock mode and provide clock signals for a Data Terminal Equipment (DTE).	-
slave	Configures a CE1/PRI interface to work in slave clock mode and use line clock signals. When a CE1/PRI interface functions as a DTE, it must work in slave clock mode and obtain clock signals from a DCE.	-
system	Configures a CE1/PRI interface to work in system clock mode and use MPU clock signals. **NOTE** This parameter takes effect only when it is configured on interfaces of the 4E1T1-M/8E1T1-M interface card.	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To exchange data correctly, communicating parties must work in clock synchronization state.

A CE1/PRI interface supports the following clock modes:

- master: uses the internal clock signal.
- slave: uses the line clock signal.
- system: uses the MPU clock signal.

Precautions

When the router and a remote device are directly connected by using two CE1/PRI interfaces, the two CE1/PRI interfaces must work in master clock mode and slave clock mode.

When the MPU on the router obtains the clock with high accuracy from the upstream device and the router needs to synchronize the clock to downstream device, the interface on the router must be configured to work in system clock mode. Moreover, the interface on the downstream device must be configured to work in slave clock mode.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure CE1/PRI 1/0/0 to work in master clock mode.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] clock master
```

5.5.3 controller e1

Function

Using the **controller e1** command, you can enter the view of a CE1/PRI interface.

Format

controller e1 *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a CE1/PRI interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enter the CE1/PRI interface view, run the **controller e1** command.

Prerequisites

The 1E1T1-M/2E1T1-M/4E1T1-M/8E1T1-M interface card is configured to work in CE1/PRI mode, run the **set workmode slot** *slot-id* **e1t1 e1-data** command.

Example

Enter the view of CE1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0]
```

5.5.4 crc

Function

The **crc** command configures the cyclic redundancy check (CRC) mode of a synchronous serial interface.

The **undo crc** command restores the default CRC mode of a synchronous serial interface.

By default, the 16-bit CRC is used.

Format

crc { **16** | **32** | **none** }

undo crc

Parameters

Parameter	Description	Value
16	Indicates the 16-bit CRC.	-
32	Indicates the 32-bit CRC.	-
none	Indicates that the synchronous serial interface does not perform CRC.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CRC is a commonly used method to detect transmission errors in a communication system. It checks for transmission errors by adding redundancy codes to the original data. Transmission errors are more likely to be detected when more redundancy codes are added, but data is transmitted at a lower efficiency. Use the 16-bit or 32-bit CRC mode as required.

Precautions

- Interfaces that support CRC include:
  - Synchronous/asynchronous serial interfaces that work in synchronous mode. The interface name is Serial.

 Copyright © Huawei Technologies Co., Ltd.

  - Interfaces formed by CE1/PRI and CT1/PRI interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by CE3 interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1-F and T1-F interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1/T1 interfaces that are channelized from CPOS interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
- The synchronous serial interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.

Example

Set the CRC mode to 32-bit CRC on Serial 1/0/0/0:0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0/0:0
[Huawei-Serial1/0/0/0:0] crc 32
```

5.5.5 data-coding (CE1/PRI interface view)

Function

Using the **data-coding** command, you can determine whether data is inverted by a CE1/PRI interface.

Using the **undo data-coding** command, you can restore the default setting.

By default, a CE1/PRI interface does not invert data.

Format

data-coding { **inverted** | **normal** }

undo data-coding

Parameters

Parameter	Description	Value
inverted	Configures a CE1/PRI interface to invert data.	-
normal	Configures a CE1/PRI interface not to invert data.	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Data inversion indicates that every "1" bit in the data stream becomes a "0" bit and every "0" bit becomes a "1" bit.

Two devices can communicate only when the same data inversion configuration is performed on CE1/PRI interfaces on both devices.

Example

Configure CE1/PRI 1/0/0 to invert data.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] data-coding inverted
```

5.5.6 detect-ais (CE1/PRI interface view)

Function

Using the **detect-ais** command, you can enable alarm indication signal (AIS) detection on a CE1/PRI interface.

Using the **undo detect-ais** command, you can disable AIS detection.

By default, AIS detection is enabled on a CE1/PRI interface.

Format

detect-ais

undo detect-ais

Parameters

None

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AIS alarms are also called upstream alarms, indicating that the peer device or the receive link of the local device becomes faulty.

If the number of 0s in 512 consecutive bits (two consecutive frames) of a received signal is smaller than 3, an AIS alarm is generated. If the number of 0s in 512 consecutive bits of a received signal is greater than or equal to 3, an AIS alarm is cleared.

If AIS detection is enabled, the local device sends a message carrying the remote alarm indication (RAI) bit to the peer device after detecting AIS alarms.

Prerequisites

The CE1/PRI interface has been configured to work in E1 mode by using the **using e1** command.

Example

Enable AIS detection on CE1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] using e1
[Huawei-E1 1/0/0] detect-ais
```

5.5.7 detect-rai (CE1/PRI interface view)

Function

Using the **detect-rai** command, you can enable remote alarm indication (RAI) detection on a CE1/PRI interface.

Using the **undo detect-rai** command, you can disable RAI detection.

By default, RAI detection is enabled on a CE1/PRI interface.

Format

detect-rai

undo detect-rai

Parameters

None

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If RAI detection is enabled, a device sends an RAI alarm to its peer device after detecting loss of frame (LoF) caused by clock asynchronization or loss of signal (LOS).

Prerequisites

The CE1/PRI interface has been configured to work in CE1/PRI mode by using the **using ce1** command.

Example

Disable RAI detection on CE1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] undo detect-rai
```

5.5.8 display controller e1

Function

Using the **display controller e1** command, you can view information about a CE1/PRI interface.

Format

display controller [**e1** [*interface-number*]]

Parameters

Parameter	Description	Value
interface-number	Displays information about a specified CE1/PRI interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the interface status or locating faults on an interface, run the **display controller e1** command to obtain the configuration information and alarm state of the interface. You can locate faults on the interface according to the command output.

Example

Display information about CE1/PRI 1/0/0.

```
<Huawei> display controller e1 1/0/0
E1 1/0/0 current state : UP
Description : HUAWEI, AR Series, E1 1/0/0 Interface
Basic Configuration:
  Work Mode is E1 Framed, Cable type is 120 Ohm balanced.
  Frame-format is NO-CRC4, Line Code is Hdb3.
  Source Clock is Slave, Data-coding is Normal.
  Idle code is 7E, Itf type is 7E, Itf number is 4.
  Loopback is Not Set.
Alarm State:
  Receiver alarm state is Loss-of-Frame.
  Transmitter is sending remote alarm.
Historical Statistics:
  Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
```

Table 5-23 Description of the display controller e1 command output

Item	Sub-Item	Description
current state	-	Physical status of the interface. ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down.
Description	-	Description of the interface.
Basic Configuration	Work Mode	Working mode of the interface. ● E1 UNFRAMED: indicates that the interface works in E1 mode. ● E1 FRAMED: indicates that the interface works in CE1/PRI mode. To configure the working mode for a CE1/PRI interface, run the **using (CE1/PRI interface view)** command.
Basic Configuration	Cable type	Type of the cable connected to the CE1/PRI interface. The value can be: ● 120 Ohm: indicates a balanced cable (twisted pair). ● 75 Ohm: indicates a non-balanced cable (coaxial cable).

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-Item	Description
Basic Configuration	Frame-format	Frame format of the interface, which can be CRC4 or NO-CRC4. To configure the frame format for a CE1/PRI interface, run the **frame-format (CE1/PRI interface view)** command. • CRC4: indicates that the frame format is a multi-frame. • NO-CRC4: indicates that the frame format is a basic frame, which is also called a dual-frame or an odd-even frame.
Basic Configuration	Line Code	Encoding and decoding mode of the interface.
Basic Configuration	Source Clock	Clock mode of the interface, which can be master or slave. To configure the clock mode for a CE1/PRI interface, run the **clock (CE1/PRI interface view)** command. • MASTER: indicates that the interface works in master clock mode and uses the internal clock signal. • SLAVE: indicates that the interface works in slave clock mode and uses the line clock signal.
Basic Configuration	Idle code	Line idle code of the interface, which can be 7E or FF. To configure the line idle code for a CE1/PRI interface, run the **idlecode (CE1/PRI interface view)** command.
Basic Configuration	Itf type	Interframe filling tag of the interface, which can be 7E or FF. To configure the interframe filling tag for a CE1/PRI interface, run the **itf (CE1/PRI interface view)** command.
Basic Configuration	Itf number	Number of interframe filling tags, which ranges from 0 to 14. To configure the number of interframe filling tags on a CE1/PRI interface, run the **itf (CE1/PRI interface view)** command.
Basic Configuration	Loopback	Whether loopback detection is enabled on the interface. If loopback detection has been enabled, the loopback detection mode is displayed. To configure loopback detection on a CE1/PRI interface, run the **loopback (CE1/PRI interface view)** command. **NOTE** The loopback detection function detects the interface status or cable status and must be disabled when devices work properly.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-Item	Description
Alarm State	Receiver alarm state is Loss-of-Frame.	No alarm is received. If an alarm is generated, the specific alarm type is displayed. The following alarms may be generated: ● Loss-of-Signal (LOS): This alarm is generated when data transmission is interrupted or frames are lost because of severe problems, for example, the cable is broken or is not well connected. ● Alarm-Indication-Signal (AIS): This alarm is generated when the remote end fails to receive the frame alignment signals. This alarm generally indicates a fault on the remote device and is also called the upstream alarm. ● Loss-of-Frame (LOF): This alarm is generated when signals cannot be encapsulated in frames. It is usually generated with a LOS alarm and is cleared when frame alignment succeeds. ● Remote-Alarm-Indication (RAI): This alarm is generated when the remote end does not receive frames from the local end for some reasons, for example, the local end fails to send frames, the transmission line of the local end fails, or the remote end fails to receive frames. When a LOS, AIS, or LOF alarm is generated, the local end needs to send the RAI bit to the remote end. In addition, "Transmitter is sending remote alarm." is displayed.
Historical Statistics	Data in current interval	The current accumulation period.
Historical Statistics	Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) occurring over the accumulation period.
Historical Statistics	Path Code Violations	Frame synchronization bit error in the E1-noCRC formats or a CRC error in the E1-CRC formats.
Historical Statistics	Slip Secs	A second with one or more out of frame defects or a detected incoming AIS.
Historical Statistics	Fr Loss Secs	Number of seconds an Out Of Frame (OOF) error is detected.
Historical Statistics	Line Err Secs	A second in which one or more code violations occurred or one or more LOS defects.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-Item	Description
Historical Statistics	Degraded Mins	One in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Historical Statistics	Errored Secs	A second with one or more path coding violations, one or more Out of Frame defects, or one or more controlled slip events or a detected AIS defect.
Historical Statistics	Bursty Err Secs	A second with fewer than 320 and more than one path coding violation error events, no Severely Errored Frame defects, and no detected incoming AIS defects.
Historical Statistics	Severely Err Secs	A second with 320 or more path code violation errors events, one or more Out of Frame defects, or a detected AIS defect.
Historical Statistics	Unavail Secs	Number of seconds that the interface is unavailable.
Historical Statistics	Total Data	Displays total accumulated data for all intervals.

5.5.9 display workmode

Function

The **display workmode** command displays the working modes of interface cards.

Format

display workmode { **slot** *slot-id* | **all** }

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the working mode of an interface card in a specified slot.	The value must be the slot ID of an interface card with a configurable working mode. The working mode of the following interface cards can be changed: 1E1T1-M/2E1T1-M, 1E1T1-F/2E1T1-F, 4G.SHDSL, VDSL2, 1CPOS-155M, 4STM1 and 2BST.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Displays the working mode of all interface cards with configurable working modes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command applies to only the interface cards with configurable working mode. To configure the working mode of an interface card, run the **set workmode e1t1**, **set workmode e1t1-f**, **set workmode shdsl**, **set workmode vdsl**, **set workmode cpos**, **set workmode stm** or **set workmode bri** command.

Example

Display the working mode of the interface card in slot 2.

```
<Huawei> display workmode slot 2
-----------------------------------------------------------------------
Slot  Type              config-workmode     active-workmode
-----------------------------------------------------------------------
2     1CPOS-155M-W        e1-data          e1-data
```

Table 5-24 Description of the display workmode command output

Item	Description
Slot	Slot ID of the interface card.

Item	Description
Type	Interface card type: ● 1E1/T1-M ● 2E1/T1-M ● 4E1/T1-M ● 8E1/T1-M ● 1E1/T1-F ● 2E1/T1-F ● 4E1/T1-F ● 8E1/T1-F ● 4G.SHDSL ● VDSL2 ● 1CPOS-155M ● 4STM1 ● 2BST

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
config-workmode	config working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
active-workmode	active working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

5.5.10 error-diffusion restraint config

Function

The **error-diffusion restraint config** command configures the error packet diffusion restraint parameters.

The **undo error-diffusion restraint config** command restores the default settings of the error packet diffusion restraint parameters.

By default, the detection time is 30 seconds, the renewal time is 600 seconds, and the error packet threshold percentage is 20%.

Format

error-diffusion restraint config *detect-timer renew-timer threshold*

undo error-diffusion restraint config

Parameters

Parameter	Description	Value
detect-timer	Configures the detection timer.	The value is an integer that ranges from 30 to 600, in seconds. The default value is 30.
renew-timer	Configures the renewal timer.	The value is an integer that ranges from 120 to 2400, in seconds. The default value is 600.
threshold	Configures the error packet threshold percentage.	The value is an integer that ranges from 5 to 100. The default value is 20.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After error packet diffusion restraint is enabled, the device considers that an interface is faulty and forcibly disables the interface when the error packet rate on the interface exceeds the value of *threshold* within the time specified by *detect-timer*. After the time specified by *renew-timer*, the interface is restored to the normal state.

The value of *renew-timer* cannot be smaller than four times the value of *detect-timer*.

Example

Configure the detection timer to 100 seconds, renewal timer to 2400 seconds, and error packet threshold to 15% for error packet diffusion restraint.

```
<Huawei> system-view
[Huawei] error-diffusion restraint config 100 2400 15
```

5.5.11 error-diffusion restraint enable

Function

The **error-diffusion restraint enable** command enables the error packet diffusion restraint function.

The **undo error-diffusion restraint enable** command disables the error packet diffusion restraint function.

 Copyright © Huawei Technologies Co., Ltd.

By default, the error packet diffusion restraint function is disabled.

Format

error-diffusion restraint enable

undo error-diffusion restraint enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a timeslot receives specified error packets, other timeslots will receive error packets consecutively. This is called error packet diffusion. You can configure the error packet diffusion restraint function to reduce the error packet diffusion probability.

Example

Disable the error packet diffusion restraint function.

```
<Huawei> system-view
[Huawei] undo error-diffusion restraint enable
```

5.5.12 error-diffusion restraint restart-channel

Function

The **error-diffusion restraint restart-channel** command restarts the interface that is disabled because of the error packet diffusion restraint function.

By default, this function is disabled.

Format

error-diffusion restraint restart-channel serial *interface-number*

Parameters

Parameter	Description	Value
serial *interface-number*	Specifies the number of an interface.	Only a CE1/PRI interface is supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After error packet diffusion restraint is enabled, the device considers that an interface is faulty and forcibly disables the interface when the error packet rate on the interface exceeds the value of *threshold* within the time specified by *detect-timer*. After the time (in seconds) specified by *renew-timer*, the interface is restored to the normal state. You can run this command to enable the disabled interface before the time specified by *renew-timer*.

Example

Restart the interface Serial 1/0/0:10 that is disabled because of the error packet diffusion restraint function.

```
<Huawei> system-view
[Huawei] error-diffusion restraint restart-channel serial 1/0/0:10
```

5.5.13 frame-format (CE1/PRI interface view)

Function

Using the **frame-format** command, you can set the frame format for a CE1/PRI interface.

Using the **undo frame-format** command, you can restore the default setting.

By default, the frame format of a CE1/PRI interface is non-CRC4.

Format

frame-format { **crc4** | **no-crc4** }

undo frame-format

Parameters

Parameter	Description	Value
crc4	Sets the frame format to CRC4.	-
no-crc4	Sets the frame format to non-CRC4.	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A CE1/PRI interface functioning as a CE1 interface supports both CRC4 and non-CRC4.

- CRC4: indicates that the frame format is a multi-frame. A multi-frame is formed by using the first bit of timeslot 0 and contains 16 consecutive PCM frames.
- Non-CRC4: indicates that the frame format is a basic frame. A basic frame is also called a dual-frame or an odd-even frame.

The multi-frame format supports CRC4, whereas the basic frame format does not support CRC4.

Prerequisites

The CE1/PRI interface has been configured to work in CE1/PRI mode by using the **using ce1** command.

Precautions

Two devices can communicate properly only when the same frame format is set for CE1/PRI interfaces on both devices. Otherwise, a CRC4 alarm is generated.

Example

Set the frame format to CRC4 for CE1 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] frame-format crc4
```

5.5.14 idlecode (CE1/PRI interface view)

Function

Using the **idlecode** command, you can set the line idle code for a CE1/PRI interface.

Using the **undo idlecode** command, you can restore the default setting.

By default, the line idle code of a CE1/PRI interface is 0x7e.

Format

idlecode { **7e** | **ff** }

undo idlecode

Parameters

Parameter	Description	Value
7e	Sets the line idle code to 0x7e.	-
ff	Sets the line idle code to 0xff.	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A CE1/PRI interface transmits electrical signals, and therefore the interface line keeps transmitting data. When no data is being transmitted, a line idle code needs to be filled.

The line idle code is the code sent over the timeslot that is not bundled to form a logical channel.

A CE1/PRI interface supports two line idle codes: 0x7e and 0xff. The default line idle code 0x7e is recommended.

Precautions

- If you run the **idlecode** command multiple times in the same CE1/PRI interface view, only the latest configuration takes effect.
- Two devices can communicate properly only when the same line idle code is set for CE1/PRI interfaces on both devices.

Example

Set the line idle code to 0xff for CE1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] idlecode ff
```

5.5.15 itf (CE1/PRI interface view)

Function

The **itf** command sets the interframe filling tag and the number of interframe filling tags on a CE1/PRI interface.

The **undo itf** command restores the default setting.

By default, a CE1/PRI interface uses the interframe filling tag 0x7e and four interframe filling tags.

Format

itf { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 14.
type	Specifies the interframe filling tag.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag is the code sent when the timeslot bundled to form a logical channel does not send any service data.

A CE1/PRI interface supports two interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

Precautions

- Two devices can communicate properly only when the same interframe filling tag and the same number of interframe filling tags are set on CE1/PRI interfaces on both devices.
- A CE1/PRI interface cannot achieve the bandwidth because of extra costs of interframe filling tags. To improve the transmission rate of the CE1/PRI interface, run the **itf number** command to set the number of interframe filling tags to 0.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interframe filling tag to 0xff on CE1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] itf type ff
```

5.5.16 line-termination

Function

Using the **line-termination** command, you can set the cable type for a CE1/PRI interface.

Using the **undo line-termination** command, you can restore the default setting.

By default, a CE1/PRI interface connects to a 120 ohm balanced cable (twisted pair).

Format

line-termination { **75-ohm** | **120-ohm** }

undo line-termination

Parameters

Parameter	Description	Value
75-ohm	Indicates that the CE1/PRI interface connects to a 75 ohm non-balanced cable (coaxial cable).	-
120-ohm	Indicates that the CE1/PRI interface connects to a 120 ohm balanced cable (twisted pair).	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

A CE1/PRI interface can connect to a twisted pair or coaxial cable. The resistance of a twisted pair is 120 ohm, and the resistance of a coaxial cable is 75 ohm.

If the type of the cable connected to a CE1/PRI interface changes, use this command to change the cable type.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the cable type to coaxial cable for CE1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] line-termination 75-ohm
```

5.5.17 loopback (CE1/PRI interface view)

Function

Using the **loopback** command, you can enable loopback detection and set the loopback detection mode on a CE1/PRI interface.

Using the **undo loopback** command, you can restore the default setting.

By default, loopback detection is disabled.

Format

loopback { **local** | **payload** | **remote** }

undo loopback

Parameters

Parameter	Description	Value
local	Sets internal loopback.	-
payload	Sets payload loopback.	-
remote	Sets external loopback.	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function detects the interface status or cable status and must be disabled when devices work properly.

- In internal loopback mode, the local device loops back outgoing packets to itself to test whether it works properly.
- In payload loopback mode, the local device loops back the valid payload of outgoing packets to itself. Generally, the synchronization signals transmitted by timeslot 0 are not looped back to the local device.

 Copyright © Huawei Technologies Co., Ltd.

- In external loopback mode, the local device loops back the packets received from its peer device to the peer device to test whether the link between the two devices works properly.

Example

Enable internal loopback detection on CE1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] loopback local
```

5.5.18 pri-set (CE1/PRI interface view)

Function

Using the **pri-set** command, you can bundle timeslots of a CE1/PRI interface to form a PRI set.

Using the **undo pri-set** command, you can cancel the configuration.

By default, no timeslot of a CE1/PRI interface is bundled to form a PRI set.

NOTE

Timeslots of a CE1/PRI interface on the 1E1T1-M/2E1T1-M/4E1T1-M/8E1T1-M interface card can be bundled to form a PRI set.

Format

pri-set [**timeslot-list** *list*]

undo pri-set

Parameters

Parameter	Description	Value
timeslot-list *list*	Specifies the timeslot to be bundled. If this parameter is not specified, all timeslots except timeslot 0 are bundled to form an ISDN PRI interface at a rate of 30B+D.	*list* specifies the number of a timeslot, and its value ranges from 1 to 31. Timeslot 16 alone cannot be bundled to form an ISDN PRI interface. You can specify a single timeslot by using *number*, specify a timeslot range by using *number1-number2*, or specify multiple timeslots by using *number1,number2-number3*.

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use a CE1/PRI interface to transmit voice service data and ISDN signals, run the **pri-set** command to bundle timeslots of the CE1/PRI interface to form an ISDN PRI interface.

When a CE1/PRI interface functions as a PRI interface, timeslot 16 functions as the D channel to transmit signals. Therefore, only one group of timeslots except timeslots 0 and 16 can be randomly selected to function as B channels, and then these B channels are bundled with timeslot 16 to form a PRI set. The PRI set functions as a PRI interface.

After the **pri-set** command is run, a serial interface is created automatically. It has the same logical features as an ISDN PRI interface. The number format of a serial interface is "serial *interface-number*:15". *interface-number* specifies the number of a CE1/PRI interface.

Prerequisites

A CE1/PRI interface has been configured to work in CE1/PRI mode by using the **using ce1** command.

Precautions

- The **pri-set** and **channel-set** commands cannot be used on the same CE1/PRI interface. That is, you can configure only one timeslot bundling mode on a CE1/PRI interface.
- Before running the **undo pri-set** command, run the **shutdown** command to disable the specified serial interface.
- Channel sets on the local and remote CE1/PRI interfaces must contain the same timeslots; otherwise, errors will occur in communication.

Example

Bundle timeslots 1, 5 to 8, and 16 of CE1/PRI 1/0/0 to form a PRI set.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] pri-set timeslot-list 1,5-8,16
```

Related Topics

5.5.1 channel-set (CE1/PRI interface view)

5.5.21 using (CE1/PRI interface view)

5.5.19 sa (CE1/PRI interface view)

Function

The **sa** command sets the content of the five outgoing sa bits.

The **undo sa** command restores the default setting.

By default, the content of the five outgoing sa bits is 0.

Format

sa *sa4 sa5 sa6 sa7 sa8*

undo sa

Parameters

Parameter	Description	Value
sa4	Specifies the content of the outgoing sa4 bit.	The value is an integer that ranges from 0 to 255.
sa5	Specifies the content of the outgoing sa5 bit.	The value is an integer that ranges from 0 to 255.
sa6	Specifies the content of the outgoing sa6 bit.	The value is an integer that ranges from 0 to 255.
sa7	Specifies the content of the outgoing sa7 bit.	The value is an integer that ranges from 0 to 255.
sa8	Specifies the content of the outgoing sa8 bit.	The value is an integer that ranges from 0 to 255.

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the CE1/PRI interface works in CE1/PRI mode, SA4 to SA8 in the E1 frame can be used for transmitting low-speed data. By default, the values of SA4 to SA8 are 0. In some scenarios, the remote device will check received SA fields. Therefore, SA fields must be configurable on the router to ensure normal connection of the CE1/PRI interface.

Prerequisites

The CE1/PRI interface has been configured to work in CE1/PRI mode by using the **using ce1** command.

Precautions

By default, the SA field value is 0. Before configuring the SA field, collect configuration information on the remote device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the content of five outgoing sa bits to 1, 2, 3, 4, and 5 respectively.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] sa 1 2 3 4 5
```

5.5.20 set workmode e1t1

Function

The **set workmode e1t1** command sets the working mode of a 1E1T1-M/2E1T1-M interface card.

By default, a 1E1T1-M/2E1T1-M interface card works in CE1/PRI mode (e1-data).

NOTE

The 4E1T1-M/8E1T1-M interface card only works in CE1/PRI mode (e1-data) and does not support working mode switching.

Format

set workmode slot *slot-id* **e1t1** { **e1-data** | **t1-data** | **e1-voice** | **t1-voice** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a 1E1T1-M/2E1T1-M interface card.	Run the **display device** command to view slot IDs and types of interface cards and find the slot ID with E1/T1-M displayed. Then run the **display workmode** command to view the interface card work mode on the device.
e1-data	Indicates a 1E1T1-M/2E1T1-M interface card works in CE1/PRI mode and functions as an E1 data card.	-
t1-data	Indicates a 1E1T1-M/2E1T1-M interface card works in CT1/PRI mode and functions as a T1 data card.	-
e1-voice	Indicates a 1E1T1-M/2E1T1-M interface card functions as a E1 voice card.	-
t1-voice	Indicates a 1E1T1-M/2E1T1-M interface card functions as a T1 voice card.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A 1E1T1-M interface card provides one E1/T1/PRI/VE1/VT1 interface and a 2E1T1-M interface card provides two E1/T1/PRI/VE1/VT1interfaces. The **set workmode e1t1** command sets the working mode of a 1E1T1-M/2E1T1-M interface card.

Precautions

After this command is used, the system prompts you to reset the 1E1T1-M/2E1T1-M interface card to make the new working mode take effect. If you select **Yes**, the system resets the interface card. Otherwise, you need to run the **reset slot** command to manually reset the interface card to make the new working mode take effect.

Example

Configure the 2E1T1-M interface card in slot 1 to functions as a T1 data card.

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1 t1-data
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

Configure the 2E1T1-M interface card in slot 1 to functions as an E1 voice card.

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1 e1-voice
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

Related Topics

4.1.3 display device

5.5.9 display workmode

4.2.13 reset slot

5.5.21 using (CE1/PRI interface view)

Function

Using the **using** command, you can set the working mode for a CE1/PRI interface.

Using the **undo using** command, you can restore the default setting.

By default, a CE1/PRI interface works in CE1/PRI mode.

Format

using { **ce1** | **e1** }

undo using

Parameters

Parameter	Description	Value
ce1	Sets the working mode to CE1/PRI.	-
e1	Sets the working mode to E1.	-

Views

CE1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

A CE1/PRI interface works in either E1 mode or CE1/PRI mode.

- In E1 mode, a CE1/PRI interface works at a rate of 2.048 Mbit/s without timeslot division. Similar to a synchronous serial interface, a CE1/PRI interface supports link layer protocols (such as PPP and FR) and network protocols (such as IP).
- In CE1/PRI mode, the 2 Mbit/s transmission line of a CE1/PRI interface is divided into 32 timeslots at a rate of 64 kbit/s. The 32 timeslots are numbered 0 to 31, and timeslot 0 transmits synchronization signals.

  The CE1/PRI interface working in CE1/PRI mode functions as either a CE1 interface or a PRI interface.

  - When the CE1/PRI interface functions as a CE1 interface, timeslots except timeslot 0 can be randomly bundled to form multiple channel sets. Each channel set corresponds to a channel. Each group of bundled timeslots functions as an interface, which has the same logical features as a synchronous serial interface and supports link layer protocols (such as PPP, HDLC, and FR) and network protocols (such as IP).

    To bundle timeslots to form a channel set, run the **channel-set (CE1/PRI interface view)** command.
  - When the CE1/PRI interface functions as a PRI interface, timeslot 16 functions as the D channel to transmit signals. Therefore, only one group of timeslots except timeslots 0 and 16 can be randomly selected to function as B channels, and then these B channels are bundled with timeslot 16 to form a PRI set. The PRI set functions as an ISDN PRI interface, which supports link layer protocols such as PPP and network protocols such as IP, and can be configured with DCC parameters.

 Copyright © Huawei Technologies Co., Ltd.

To bundle timeslots to form a PRI set, run the **pri-set (CE1/PRI interface view)** command.

To use a dedicated E1 line (with the 2 Mbit/s bandwidth) to transmit data, configure a CE1/PRI interface to work in E1 mode. To use multiple low-rate (128 kbit/s or 256 kbit/s) channels to transmit different services or use a CE1/PRI interface as a PRI interface, configure the CE1/PRI interface to work in CE1/PRI mode.

Example

Configure CE1/PRI 1/0/0 to work in E1 mode.

```
<Huawei> system-view
[Huawei] controller e1 1/0/0
[Huawei-E1 1/0/0] using e1
```

Related Topics

5.5.1 channel-set (CE1/PRI interface view)

5.5.18 pri-set (CE1/PRI interface view)

5.6 CT1/PRI Interface Configuration Commands

5.6.1 alarm-threshold

Function

Using the **alarm-threshold** command, you can configure alarm thresholds for a CT1/PRI interface.

Using the **undo alarm-threshold** command, you can restore the default alarm thresholds for a CT1/PRI interface.

The default alarm thresholds are as follows:

- Alarm indication signal (AIS) alarm: level-1.
- Loss of frame alignment (LFA) alarm: level-1.
- Loss of signal (LOS) alarm: The value of pulse-detection is 176 and the value of pulse-recovery is 22, indicating that a LOS alarm is generated if less than 22 pulses are detected within 176 pulse intervals.

Format

alarm-threshold { **ais** { **level-1** | **level-2** } | **lfa** { **level-1** | **level-2** | **level-3** | **level-4** } | **los** { **pulse-detection** *value* | **pulse-recovery** *value* } }

undo alarm-threshold { **ais** | **lfa** | **los** { **pulse-detection** | **pulse-recovery** } }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ais { **level-1** | **level-2** }	Sets the AIS alarm threshold. ● **level-1**: indicates that an AIS alarm is generated when there are less than two 0s in the bit stream of a super frame (SF) or extended super frame (ESF). ● **level-2**: indicates that an AIS is generated when there is less than three 0s in the code stream of an SF or less than five 0s in the code stream of an ESF.	The default AIS alarm threshold is **level-1**.
lfa { **level-1** | **level-2** | **level-3** | **level-4** }	Sets the loss of frame alignment (LFA) alarm threshold. ● **level-1**: indicates that an LFA alarm is generated when two of four frame alignment bits are lost.**level-2**: indicates that an LFA alarm is generated when two of five frame alignment bits are lost. ● **level-3**: indicates that an LFA alarm is generated when two of six frame alignment bits are lost.**level-4**: indicates that an LFA alarm is generated when errors occur in four consecutive ESF frames. This keyword is valid only for the ESF format.	The default LFA alarm threshold is **level-1**.
los { **pulse-detection** *value* | **pulse-recovery** *value* }	Sets the LOS alarm threshold. ● **pulse-detection** specifies the LOS detection period, expressed by the number of pulse intervals. ● **pulse-recovery** specifies the pulse threshold. A LOS alarm is generated when the number of pulses detected within the specified number of pulse intervals is less than the value of **pulse-recovery**.	The value of **pulse-detection** ranges from 16 to 4096, and the value of **pulse-recovery** ranges from 1 to 256. By default, the value of **pulse-detection** is 176 and the value of **pulse-recovery** is 22, indicating that a LOS alarm is generated if less than 22 pulses are detected within 176 pulse intervals.

 Copyright © Huawei Technologies Co., Ltd.

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the LOS detection period to 300 pulse intervals.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] alarm-threshold los pulse-detection 300
```

5.6.2 cable

Function

Using the **cable** command, you can set the attenuation or length of the transmission line matching a CT1/PRI interface.

Using the **undo cable** command, you can restore the default transmission line configuration.

The default attenuation of the transmission line on a CT1/PRI interface is -7.5 db.

Format

cable { **long** { **-7.5db** | **-15db** | **-22.5db** } | **short** { **133ft** | **266ft** | **399ft** | **533ft** | **655ft** } }

undo cable

Parameters

Parameter	Description	Value
long { **-7.5db** | **-15db** | **-22.5db** }	Sets the attenuation of the transmission line matching the CT1/PRI interface. This parameter is applicable to transmission lines longer than 655 feet. The attenuation of such transmission lines can be -7.5 db, -15 db, or -22.5 db. Set the attenuation based on quality of received signals. Transmission lines with a lower quality have a larger attenuation. When received signals are of low quality, set this parameter to offset the attenuation.	-

Parameter	Description	Value
short { **133ft** | **266ft** | **399ft** | **533ft** | **655ft** }	Sets the length of the transmission line matching the CT1/PRI interface. This parameter is applicable to transmission lines not longer than 665 feet. The length can be 133 feet, 266 feet, 399 feet, 533 feet, or 655 feet.	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

This command is required only when received signals are of a low quality. The command determines the waveform of transmitted signals.

When signals that the device receives are of a good quality, use the default configuration.

Example

Set the length of the transmission line matching CT1/PRI 1/0/0 to 133 feet.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] cable short 133ft
```

5.6.3 channel-set (CT1/PRI interface view)

Function

Using the **channel-set** command, you can bundle timeslots of a CT1/PRI interface to form a channel set.

Using the **undo channel-set** command, you can cancel the configuration.

By default, no timeslot of a CT1/PRI interface is bundled to form a channel set.

Format

channel-set *set-number* **timeslot-list** *list* [**speed** { **56k** | **64k** }]

undo channel-set *set-number*

Parameters

Parameter	Description	Value
set-number	Specifies the number of the channel set.	The value is an integer that ranges from 0 to 23.
timeslot-list *list*	Specifies the timeslot to be bundled.	*list* specifies the number of a timeslot, and its value ranges from 1 to 24. You can specify a single timeslot by using *number*, specify a timeslot range by using *number1-number2*, or specify multiple timeslots by using *number1,number2-number3*.
speed { **56k** | **64k** }	Specifies the speed of each timeslot, in kbit/s. When **56k** is specified, the speed of a channel set is *n* x 56 kbit/s. When **64k** is specified, the speed of a channel set is *n* x 64 kbit/s. *n* is the number of timeslots in a channel set. By default, the speed of each timeslot in a channel set is 64 kbit/s. **NOTE** The speed of timeslots at both ends must be the same; otherwise, errors will occur in communication.	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a family or a small enterprise, multiple terminals (such as telephones, fax machines, and computers) may share the same T1 link. In this situation, timeslots of the T1 link need to be bundled to form channel sets. Each channel set transmits a type of service. For example, 2 timeslots are used for voice transmission, and 16 timeslots are used for Internet access.

A CT1/PRI interface has 24 timeslots, numbered from 1 to 24. The timeslots can be bundled into multiple channel sets, and each channel set transmits a type of service.

 Copyright © Huawei Technologies Co., Ltd.

The **channel-set** command bundles timeslots of a CT1/PRI interface to form a channel set. After the **channel-set** command is run, a serial interface is created automatically. It has the same logical features as a synchronous serial interface. The number format of a serial interface is "serial *interface-number.set-number*". *interface-number* specifies the number of a CT1/PRI interface, and *set-number* specifies the number of a channel set.

Precautions

- The **channel-set** and **pri-set (CT1/PRI interface view)** commands cannot be used on the same CT1/PRI interface. That is, you can configure only one timeslot bundling mode on a CT1/PRI interface.
- Timeslots of a CT1 interface can be bundled to form a maximum of 24 channel sets and a minimum of 1 channel set. That is, a single timeslot can form a channel set, and 24 timeslots can be bundled to form one channel set.

  NOTE

  If you run the **channel-set** command in the same CT1/PRI interface view multiple times, multiple channel sets can be formed by bundling timeslots. One timeslot can be bundled to only one channel set.
- Channel sets on the local and remote CT1/PRI interfaces must contain the same timeslots; otherwise, errors will occur in communication.

Example

Bundle timeslots 1, 10 to 16, and 18 of CT1 1/0/0 to form channel set 0.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] channel-set 0 timeslot-list 1,10-16,18
```

Related Topics

5.6.15 pri-set (CT1/PRI interface view)

5.6.4 clock (CT1/PRI interface view)

Function

Using the **clock** command, you can set the clock mode for a CT1/PRI interface.

Using the **undo clock** command, you can restore the default setting.

By default, a CT1/PRI interface works in slave clock mode and uses line clock signals.

Format

clock { **master** | **slave** }

undo clock

Parameters

Parameter	Description	Value
master	Configures a CT1/PRI interface to work in master clock mode and use internal clock signals. When a CT1/PRI interface functions as a Data Circuit-terminating Equipment (DCE), it must work in master clock mode and provide clock signals for a Data Terminal Equipment (DTE).	-
slave	Configures a CT1/PRI interface to work in slave clock mode and use line clock signals. When a CT1/PRI interface functions as a DTE, it must work in slave clock mode and obtain clock signals from a DCE.	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To exchange data correctly, communicating parties must work in clock synchronization state.

A CT1/PRI interface supports the following clock modes:

- master: uses the internal clock signal.
- slave: uses the line clock signal.

Precautions

When two routers are directly connected by using two CT1/PRI interfaces, the two CT1/PRI interfaces must work in master clock mode and slave clock mode.

Example

Configure CT1/PRI 1/0/0 to work in master clock mode.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] clock master
```

5.6.5 controller t1

Function

Using the **controller t1** command, you can enter the view of a CT1/PRI interface.

Format

controller t1 *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a CT1/PRI interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enter the CT1/PRI interface view, run the **controller t1** command.

Prerequisites

The 1E1T1-M/2E1T1-M interface card is configured to work in CT1/PRI mode, run the **set workmode slot** *slot-id* **e1t1 t1-data**.

Example

Enter the view of CT1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0]
```

5.6.6 crc

Function

The **crc** command configures the cyclic redundancy check (CRC) mode of a synchronous serial interface.

The **undo crc** command restores the default CRC mode of a synchronous serial interface.

By default, the 16-bit CRC is used.

Format

crc { **16** | **32** | **none** }

undo crc

Parameters

Parameter	Description	Value
16	Indicates the 16-bit CRC.	-
32	Indicates the 32-bit CRC.	-
none	Indicates that the synchronous serial interface does not perform CRC.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CRC is a commonly used method to detect transmission errors in a communication system. It checks for transmission errors by adding redundancy codes to the original data. Transmission errors are more likely to be detected when more redundancy codes are added, but data is transmitted at a lower efficiency. Use the 16-bit or 32-bit CRC mode as required.

Precautions

- Interfaces that support CRC include:
  - Synchronous/asynchronous serial interfaces that work in synchronous mode. The interface name is Serial.
  - Interfaces formed by CE1/PRI and CT1/PRI interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by CE3 interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1-F and T1-F interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1/T1 interfaces that are channelized from CPOS interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
- The synchronous serial interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the CRC mode to 32-bit CRC on Serial 1/0/0/0:0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0/0:0
[Huawei-Serial1/0/0/0:0] crc 32
```

5.6.7 data-coding (CT1/PRI interface view)

Function

Using the **data-coding** command, you can determine whether data is inverted by a CT1/PRI interface.

Using the **undo data-coding** command, you can restore the default setting.

By default, a CT1/PRI interface does not invert data.

Format

data-coding { **inverted** | **normal** }

undo data-coding

Parameters

Parameter	Description	Value
inverted	Configures a CT1/PRI interface to invert data.	-
normal	Configures a CT1/PRI interface not to invert data.	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Two devices can communicate only when the same data inversion configuration is performed on CT1/PRI interfaces on both devices.

Example

Configure CT1/PRI 1/0/0 to invert data.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] data-coding inverted
```

5.6.8 detect-rai (CT1/PRI interface view)

Function

Using the **detect-rai** command, you can enable remote alarm indication (RAI) detection on a CT1/PRI interface.

Using the **undo detect-rai** command, you can disable RAI detection.

By default, RAI detection is enabled on a CT1/PRI interface.

Format

detect-rai

undo detect-rai

Parameters

None

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If RAI detection is enabled, a device sends an RAI alarm to its peer device after detecting loss of frame (LoF) caused by clock asynchronization or loss of signal (LOS).

Prerequisites

The frame format has been set to extended super frame (ESF) by using the **frame-format esf** command.

Example

Disable RAI detection on CT1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] undo detect-rai
```

5.6.9 display controller t1

Function

Using the **display controller t1** command, you can view information about a CT1/PRI interface.

Format

display controller [**t1** [*interface-number*]]

Parameters

Parameter	Description	Value
interface-number	Displays information about a specified CT1/PRI interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the interface status or locating faults on an interface, run the **display controller t1** command to obtain the configuration information and alarm state of the interface. You can locate faults on the interface according to the command output.

Example

Display information about CT1/PRI 1/0/0.

```
<Huawei> display controller t1 1/0/0
T1 1/0/0 current state : DOWN
Description : HUAWEI, AR Series, T1 1/0/0 Interface
Basic Configuration:
  Work Mode is T1 Framed, Cable type is 100 Ohm balanced.
  Frame-format is ESF, Line Code is B8zs.
  Source Clock is Slave, Data-coding is Normal.
  Idle code is 7E, Itf type is 7E, Itf number is 4.
  Loopback is Not Set.
Alarm State:
  Receiver alarm state is Loss-of-Frame.
  Transmitter is sending remote alarm.
Historical Statistics:
  Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Sec
```

 Copyright © Huawei Technologies Co., Ltd.

Table 5-25 Description of the display controller t1 command output

Item	Sub-item	Description
current state	-	Physical status of the interface. ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down.
Description	-	Description of the interface.
Basic Configuration	Work Mode is T1 Framed	The interface works in T1 framed mode, namely, the channelized mode.
Basic Configuration	Cable type is 100 Ohm balanced	The cable is connected to a 100 ohm balanced cable.
Basic Configuration	Frame-format	Frame format of the interface, which can be ESF or SF. To configure the frame format for a CT1/PRI interface, run the **frame-format (CT1/PR interface view)** command. ● ESF: extended super frame format ● SF: super frame format
Basic Configuration	Line Code	Encoding and decoding mode of the interface.
Basic Configuration	Source Clock	Clock mode of the interface, which can be master or slave. To configure the clock mode for a CT1/PRI interface, run the **clock (CT1/PRI interface view)** command. ● MASTER: indicates that the interface works in master clock mode and uses the internal clock signal. ● SLAVE: indicates that the interface works in slave clock mode and uses the line clock signal.
Basic Configuration	Data-coding	Whether to invert data. The value can be **inverted** or **normal**. To configure a CT1/PRI interface to invert data, run the **data-coding (CT1/PRI interface view)** command. ● inverted: indicates that the interface inverts data. ● normal: indicates that the interface does not invert data.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Basic Configuration	Idle code	Line idle code of the interface, which can be 7E or FF. To configure the line idle code for a CT1/PRI interface, run the **idlecode (CT1/PRI interface view)** command.
Basic Configuration	Itf type	Interframe filling tag of the interface, which can be 7E or FF. To configure the interframe filling tag for a CT1/PRI interface, run the **itf (CT1/PRI interface view)** command.
Basic Configuration	Itf number	Number of interframe filling tags, which ranges from 0 to 14. To configure the number of interframe filling tags on a CT1/PRI interface, run the **itf (CT1/PRI interface view)** command.
Basic Configuration	Loopback	Whether loopback detection is enabled on the interface. If loopback detection has been enabled, the loopback detection mode is displayed. To configure loopback detection on a CT1/PRI interface, run the **loopback (CT1/PRI interface view)** command. **NOTE** The loopback detection function detects the interface status or cable status and must be disabled when devices work properly.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Alarm State	Receiver alarm state is	Type of a received alarm. If no alarm is received, the message "Receiver alarm state is None." is displayed. If an alarm is generated, the specific alarm type is displayed. The following alarms may be generated: ● Loss-of-Signal (LOS): This alarm is generated when data transmission is interrupted or frames are lost because of severe problems, for example, the cable is broken or is not well connected. ● Alarm-Indication-Signal (AIS): This alarm is generated when the remote end fails to receive the frame alignment signals. This alarm generally indicates a fault on the remote device and is also called the upstream alarm. ● Loss-of-Frame (LOF): This alarm is generated when signals cannot be encapsulated in frames. It is usually generated with a LOS alarm and is cleared when frame alignment succeeds. ● Remote-Alarm-Indication (RAI): This alarm is generated when the remote end does not receive frames from the local end for some reasons, for example, the local end fails to send frames, the transmission line of the local end fails, or the remote end fails to receive frames. When a LOS, AIS, or LOF alarm is generated, the local end needs to send the RAI bit to the remote end. In addition, "Transmitter is sending remote alarm." is displayed.
Historical Statistics	Data in current interval	The current accumulation period.
Historical Statistics	Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) occurring over the accumulation period.
Historical Statistics	Path Code Violations	Frame synchronization bit error in the E1-noCRC formats or a CRC error in the E1-CRC formats.
Historical Statistics	Slip Secs	A second with one or more out of frame defects or a detected incoming AIS.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Historical Statistics	Fr Loss Secs	Number of seconds an Out Of Frame (OOF) error is detected.
Historical Statistics	Line Err Secs	A second in which one or more code violations occurred or one or more LOS defects.
Historical Statistics	Degraded Mins	One in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Historical Statistics	Errored Secs	A second with one or more path coding violations, one or more Out of Frame defects, or one or more controlled slip events or a detected AIS defect.
Historical Statistics	Bursty Err Secs	A second with fewer than 320 and more than one path coding violation error events, no Severely Errored Frame defects, and no detected incoming AIS defects.
Historical Statistics	Severely Err Secs	A second with 320 or more path code violation errors events, one or more Out of Frame defects, or a detected AIS defect.
Historical Statistics	Unavail Secs	Number of seconds that the interface is unavailable.
Historical Statistics	Total Data	Displays total accumulated data for all intervals.

5.6.10 display workmode

Function

The **display workmode** command displays the working modes of interface cards.

Format

display workmode { **slot** *slot-id* | **all** }

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the working mode of an interface card in a specified slot.	The value must be the slot ID of an interface card with a configurable working mode. The working mode of the following interface cards can be changed: 1E1T1-M/2E1T1-M, 1E1T1-F/2E1T1-F, 4G.SHDSL, VDSL2, 1CPOS-155M, 4STM1 and 2BST.
all	Displays the working mode of all interface cards with configurable working modes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command applies to only the interface cards with configurable working mode. To configure the working mode of an interface card, run the **set workmode e1t1**, **set workmode e1t1-f**, **set workmode shdsl**, **set workmode vdsl**, **set workmode cpos**, **set workmode stm** or **set workmode bri** command.

Example

Display the working mode of the interface card in slot 2.

```
<Huawei> display workmode slot 2
-----------------------------------------------------------------------
Slot  Type              config-workmode     active-workmode
-----------------------------------------------------------------------
2     1CPOS-155M-W        e1-data          e1-data
```

Table 5-26 Description of the display workmode command output

Item	Description
Slot	Slot ID of the interface card.

Item	Description
Type	Interface card type: ● 1E1/T1-M ● 2E1/T1-M ● 4E1/T1-M ● 8E1/T1-M ● 1E1/T1-F ● 2E1/T1-F ● 4E1/T1-F ● 8E1/T1-F ● 4G.SHDSL ● VDSL2 ● 1CPOS-155M ● 4STM1 ● 2BST

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
config-workmode	config working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
active-workmode	active working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

5.6.11 frame-format (CT1/PRI interface view)

Function

Using the **frame-format** command, you can set the frame format for a CT1/PRI interface.

Using the **undo frame-format** command, you can restore the default setting.

By default, a CT1/PRI interface uses the extended super frame (ESF) format.

Format

frame-format { **esf** | **sf** }

undo frame-format

Parameters

Parameter	Description	Value
esf	Sets the frame format to ESF.	-
sf	Sets the frame format to super frame (SF).	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

A CT1/PRI interface supports the SF format and ESF format. The two formats enable multiple frames to share the frame alignment information and signaling information so that more bits can be used to transmit data.

- SF: consists of 12 frames that share the frame alignment information and signaling information. Frame 6 and frame 12 are signaling frames.
- ESF: consists of 24 frames that share the frame alignment information and signaling information. Frames 6, 12, 18, and 24 are signaling frames.

Example

Set the frame format on CT1/PRI 1/0/0 to SF.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] frame-format sf
```

5.6.12 idlecode (CT1/PRI interface view)

Function

Using the **idlecode** command, you can set the line idle code for a CT1/PRI interface.

Using the **undo idlecode** command, you can restore the default setting.

By default, the line idle code of a CT1/PRI interface is 0x7e.

Format

idlecode { **7e** | **ff** }

undo idlecode

Parameters

Parameter	Description	Value
7e	Sets the line idle code to 0x7e.	-
ff	Sets the line idle code to 0xff.	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A CT1/PRI interface transmits electrical signals, and therefore the interface line keeps transmitting data. When no data is being transmitted, a line idle code needs to be filled.

The line idle code is the code sent over the timeslot that is not bundled to form a logical channel.

A CT1/PRI interface supports two line idle codes: 0x7e and 0xff. The default line idle code 0x7e is recommended.

Precautions

- If you run the **idlecode** command multiple times in the same CT1/PRI interface view, only the latest configuration takes effect.
- Two devices can communicate properly only when the same line idle code is set for CT1/PRI interfaces on both devices.

Example

Set the line idle code to 0xff for CT1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] idlecode ff
```

5.6.13 itf (CT1/PRI interface view)

Function

Using the **itf** command, you can set the interframe filling tag and the number of interframe filling tags on a CT1/PRI interface.

Using the **undo itf** command, you can restore the default setting.

By default, a CT1/PRI interface uses the interframe filling tag 0x7e and four interframe filling tags.

Format

itf { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 14.
type	Specifies the interframe filling tag.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag is the code sent when the timeslot bundled to form a logical channel does not send any service data.

A CT1/PRI interface supports two interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

Precautions

- Two devices can communicate properly only when the same interframe filling tag and the same number of interframe filling tags are set on CT1/PRI interfaces on both devices.
- A CT1/PRI interface cannot achieve the bandwidth because of extra costs of interframe filling tags. To improve the transmission rate of the CT1/PRI interface, run the **itf number** command to set the number of interframe filling tags to 0.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interframe filling tag to 0xff on CT1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] itf type ff
```

5.6.14 loopback (CT1/PRI interface view)

Function

Using the **loopback** command, you can enable loopback detection and set the loopback detection mode on a CT1/PRI interface.

Using the **undo loopback** command, you can restore the default setting.

By default, loopback detection is disabled.

Format

loopback { **local** | **payload** | **remote** }

undo loopback

Parameters

Parameter	Description	Value
local	Sets internal loopback.	-
payload	Sets payload loopback.	-
remote	Sets external loopback.	-

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function detects the interface status or cable status and must be disabled when devices work properly.

- In internal loopback mode, the local device loops back outgoing packets to itself to test whether it works properly.
- In payload loopback mode, the local device loops back the valid payload of outgoing packets to itself. Generally, the synchronization signals transmitted by timeslot 0 are not looped back to the local device.

 Copyright © Huawei Technologies Co., Ltd.

- In external loopback mode, the local device loops back the packets received from its peer device to the peer device to test whether the link between the two devices works properly.

Example

Enable internal loopback detection on CT1/PRI 1/0/0.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] loopback local
```

5.6.15 pri-set (CT1/PRI interface view)

Function

Using the **pri-set** command, you can bundle timeslots of a CT1/PRI interface to form a PRI set.

Using the **undo pri-set** command, you can cancel the configuration.

By default, no timeslot of a CT1/PRI interface is bundled to form a PRI set.

Format

pri-set [**timeslot-list** *list*]

undo pri-set

Parameters

Parameter	Description	Value
timeslot-list *list*	Specifies the timeslot to be bundled. If this parameter is not specified, all timeslots except timeslot 0 are bundled to form an ISDN PRI interface at a rate of 23B+D.	*list* specifies the number of a timeslot, and its value ranges from 1 to 24. Timeslot 24 functions as the D channel and must be bundled to other timeslots to form a PRI set. You can specify a single timeslot by using *number*, specify a timeslot range by using *number1-number2*, or specify multiple timeslots by using *number1,number2-number3*.

Views

CT1/PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use a CT1/PRI interface to transmit voice service data and ISDN signals, run the **pri-set** command to bundle timeslots of the CT1/PRI interface to form a PRI interface.

When a CT1/PRI interface works as a PRI interface, timeslot 24 functions as the D channel to transmit signals. You can bundle any of timeslots 1 to 23 with timeslot 24 to form a PRI set. The PRI set contains *n* B channels and one D channel. Here, *n* is the number of timeslots in the PRI set except timeslot 24.

After the **pri-set** command is run, a serial interface is created automatically. It has the same logical features as an ISDN PRI interface. The number format of a serial interface is "serial *interface-number*:15". *interface-number* specifies the number of a CT1/PRI interface.

Precautions

- The **pri-set** and **channel-set** commands cannot be used on the same CT1/PRI interface. That is, you can configure only one timeslot bundling mode on a CT1/PRI interface.
- Before running the **undo pri-set** command, run the **shutdown** command to disable the specified serial interface.
- Channel sets on the local and remote CT1/PRI interfaces must contain the same timeslots; otherwise, errors will occur in communication.

Example

Bundle timeslots 1, 5 to 8, and 24 of CT1/PRI 1/0/0 to form a PRI set.

```
<Huawei> system-view
[Huawei] controller t1 1/0/0
[Huawei-T1 1/0/0] pri-set timeslot-list 1,5-8,24
```

Related Topics

5.6.3 channel-set (CT1/PRI interface view)

5.6.16 set workmode e1t1

Function

The **set workmode e1t1** command sets the working mode of a 1E1T1-M/2E1T1-M interface card.

By default, a 1E1T1-M/2E1T1-M interface card works in CE1/PRI mode (e1-data).

NOTE

The 4E1T1-M/8E1T1-M interface card only works in CE1/PRI mode (e1-data) and does not support working mode switching.

Format

set workmode slot *slot-id* **e1t1** { **e1-data** | **t1-data** | **e1-voice** | **t1-voice** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a 1E1T1-M/2E1T1-M interface card.	Run the **display device** command to view slot IDs and types of interface cards and find the slot ID with E1/T1-M displayed. Then run the **display workmode** command to view the interface card work mode on the device.
e1-data	Indicates a 1E1T1-M/2E1T1-M interface card works in CE1/PRI mode and functions as an E1 data card.	-
t1-data	Indicates a 1E1T1-M/2E1T1-M interface card works in CT1/PRI mode and functions as a T1 data card.	-
e1-voice	Indicates a 1E1T1-M/2E1T1-M interface card functions as a E1 voice card.	-
t1-voice	Indicates a 1E1T1-M/2E1T1-M interface card functions as a T1 voice card.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A 1E1T1-M interface card provides one E1/T1/PRI/VE1/VT1 interface and a 2E1T1-M interface card provides two E1/T1/PRI/VE1/VT1interfaces. The **set workmode e1t1** command sets the working mode of a 1E1T1-M/2E1T1-M interface card.

Precautions

After this command is used, the system prompts you to reset the 1E1T1-M/2E1T1-M interface card to make the new working mode take effect. If you select **Yes**, the system resets the interface card. Otherwise, you need to run the **reset slot** command to manually reset the interface card to make the new working mode take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the 2E1T1-M interface card in slot 1 to functions as a T1 data card.

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1 t1-data
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

Configure the 2E1T1-M interface card in slot 1 to functions as an E1 voice card.

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1 e1-voice
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

Related Topics

4.1.3 display device

5.6.10 display workmode

4.2.13 reset slot

5.7 CE3 Interface Configuration Commands

5.7.1 clock (CE3 interface view)

Function

The **clock** command sets the clock mode of a CE3 interface.

The **undo clock** command restores the default settings.

By default, a CE3 interface works in slave clock mode.

Format

clock { **master** | **slave** }

undo clock

Parameters

Parameter	Description	Value
master	Configures a CE3 interface to work in master clock mode. When the device functions as a Data Circuit-terminating Equipment (DCE), the CE3 interface of the device must work in master clock mode and provide clock signals for a Data Terminal Equipment (DTE).	-

Parameter	Description	Value
slave	Configures a CE3 interface to work in slave clock mode. When the device functions as a DTE, the CE3 interface of the device must work in slave clock mode and obtain clock signals from a DCE.	-

Views

CE3 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To exchange data successfully, communicating parties must work in clock synchronization state.

Precautions

When two routers are directly connected using two CE3 interfaces, one CE3 interface must work in master clock mode and the other must work in slave clock mode.

Example

Configure CE3 1/0/0 to work in master clock mode.

```
<Huawei> system-view
[Huawei] controller e3 1/0/0
[Huawei-E3 1/0/0] clock master
```

5.7.2 controller e3

Function

The **controller e3** command enters the CE3 interface view.

Format

controller e3 *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a CE3 interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enter the CE3 interface view, run the **controller e3** command.

Example

Enter the view of CE3 1/0/0.

```
<Huawei> system-view
[Huawei] controller e3 1/0/0
[Huawei-E3 1/0/0]
```

5.7.3 crc

Function

The **crc** command configures the cyclic redundancy check (CRC) mode of a synchronous serial interface.

The **undo crc** command restores the default CRC mode of a synchronous serial interface.

By default, the 16-bit CRC is used.

Format

crc { **16** | **32** | **none** }

undo crc

Parameters

Parameter	Description	Value
16	Indicates the 16-bit CRC.	-
32	Indicates the 32-bit CRC.	-
none	Indicates that the synchronous serial interface does not perform CRC.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CRC is a commonly used method to detect transmission errors in a communication system. It checks for transmission errors by adding redundancy codes to the original data. Transmission errors are more likely to be detected when more redundancy codes are added, but data is transmitted at a lower efficiency. Use the 16-bit or 32-bit CRC mode as required.

Precautions

- Interfaces that support CRC include:
  - Synchronous/asynchronous serial interfaces that work in synchronous mode. The interface name is Serial.
  - Interfaces formed by CE1/PRI and CT1/PRI interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by CE3 interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1-F and T1-F interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1/T1 interfaces that are channelized from CPOS interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
- The synchronous serial interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.

Example

Set the CRC mode to 32-bit CRC on Serial 1/0/0/0:0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0/0:0
[Huawei-Serial1/0/0/0:0] crc 32
```

5.7.4 display controller e3

Function

The **display controller e3** command displays information about a CE3 interface.

Format

display controller [**e3** [*interface-number*]]

Parameters

Parameter	Description	Value
interface-number	Specifies a CE3 interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the status or locate faults on a CE3 interface, run the **display controller e3** command to view the interface configuration and alarm information. You can locate faults on the interface according to the command output.

Example

Display information about CE3 1/0/0.

```
<Huawei> display controller e3 1/0/0
E3 1/0/0 current state : UP
Description : HUAWEI, AR Series, E3 1/0/0 Interface
  Frame-format G751, line code HDB3, clock slave, national-bit 1, loopback not set
  Receiver alarm state is None.
```

Table 5-27 Description of the display controller e3 command output

Item	Description
E3 1/0/0 current state	Current physical status of the CE3 interface: ● UP: The physical status is normal. ● DOWN: The physical status is abnormal.
Description	Description of the CE3 interface. The value is a maximum of 242 case-sensitive characters with spaces. The description helps users learn about the functions of the CE3 interface.
Frame-format	Frame format of the CE3 interface.
line code	Line coding and decoding format of the CE3 interface.
clock	Clock mode: ● slave ● master
national-bit	National bit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
loopback not set	The loopback function is disabled on the CE3 interface. The loopback function is enabled on the CE3 interface only when some special functions are tested.
Receiver alarm state is None	No alarm is received. If an alarm is generated, the specific alarm type is displayed. The following alarms may be generated: ● Loss-of-Signal (LOS): This alarm is generated when data transmission is interrupted or frames are lost because of severe problems, for example, the cable is broken or is not well connected. ● Alarm-Indication-Signal (AIS): This alarm is generated when the remote device fails to receive frame alignment signals. This alarm generally indicates a fault on the remote device and is also called the upstream alarm. ● Loss-of-Frame (LOF): This alarm is generated when signals cannot be encapsulated in frames. It is usually generated with a LOS alarm and is cleared when frame alignment succeeds. ● Remote-Alarm-Indication (RAI): This alarm is generated when the remote device does not receive frames from the local device for some reasons, for example, the local device fails to send frames, the transmission line of the local device fails, or the remote device fails to receive frames.

5.7.5 fe3

Function

The **fe3** command configures a CE3 interface to work in Fractional E3 (FE3) mode and sets the DSU mode or subrate.

The **undo fe3** command restores the default settings.

By default, the DSU mode is 1, that is, Kentrox mode. The default subrate is 34010 kbit/s.

Format

fe3 { **dsu-mode** { **0** | **1** } | **subrate** *number* }

undo fe3 { **dsu-mode** | **subrate** }

Parameters

Parameter	Description	Value
dsu-mode	Specifies the DSU mode for FE3.	-
0	Sets the DSU mode to 0, that is, Digital Link mode. In this mode, a CE3 interface supports a subrate that ranges from 358 kbit/s to 34010 kbit/s. There are 95 rate levels with the differential 358 kbit/s between each two rate levels.	-
1	Sets the DSU mode to 1, that is, Kentrox mode. In this mode, a CE3 interface supports a subrate of 34010 kbit/s or a subrate that ranges from 500 kbit/s to 24500 kbit/s. There are 50 rate levels with the differential 500 kbit/s between each two rate levels.	-
subrate *number*	Specifies the subrate of the CE3 interface in FE3 mode.	The value is an integer that ranges from 1 to 34010, in kbit/s.

Views

CE3 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FE3, Fractional E3 or Subrate E3, is an E3 non-standard application mode. Devices of other vendors support different rate levels. You can run the **fe3** command to configure Huawei devices to be compatible with FE3 DSU modes on devices of other vendors so that Huawei devices can communicate with devices of other vendors.

Precautions

The rate set using the **fe3 subrate** command is an approximate rate. Subrates of each DSU mode that is set using the **fe3 dsu-mode** command are dispersed. Therefore, after a subrate is specified using the **fe3 subrate** command, a CE3 interface calculates the most accurate rate (in bit/s) matching the specified subrate based on the current DSU mode and enables the hardware circuit to support the calculated rate.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure CE3 1/0/0 to work in FE3 mode, set the DSU mode to 1, and set the subrate to 3000 kbit/s

```
<Huawei> system-view
[Huawei] controller e3 1/0/0
[Huawei-E3 1/0/0] using e3
[Huawei-E3 1/0/0] fe3 dsu-mode 1
[Huawei-E3 1/0/0] fe3 subrate 3000
```

Related Topics

5.7.4 display controller e3

5.7.6 itf (CE3 interface view)

Function

The **itf** command sets the interframe filling tag and the number of interframe filling tags on a CE3 interface.

The **undo itf** command restores the default setting.

By default, a CE3 interface uses the interframe filling tag 0x7e and four interframe filling tags.

Format

itf { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 14.
type	Specifies the interframe filling tag.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

CE3 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag is the code sent when the timeslot bundled to form a logical channel does not send any service data.

A CE3 interface supports two interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

Precautions

- Two devices can communicate properly only when the same interframe filling tag and the same number of interframe filling tags are set on CE3 interfaces on both devices.
- A CE3 interface cannot achieve the bandwidth because of extra costs of interframe filling tags. To improve the transmission rate of the CE3 interface, run the **itf number** command to set the number of interframe filling tags to 0.

Example

Set the interframe filling tag to 0xff on CE3 1/0/0.

```
<Huawei> system-view
[Huawei] controller e3 1/0/0
[Huawei-E3 1/0/0] itf type ff
```

5.7.7 loopback (CE3 interface view)

Function

The **loopback** command enables loopback detection and sets the loopback detection mode on a CE3 interface.

The **undo loopback** command restores the default settings.

By default, loopback detection is disabled.

Format

loopback { **local** | **remote** }

undo loopback

Parameters

Parameter	Description	Value
local	Sets internal loopback detection.	-
remote	Sets external loopback detection.	-

Views

CE3 interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function monitors the interface status or cable status and must be disabled when devices are working properly.

- In internal loopback mode, the local device loops back outgoing packets to itself to test whether it works properly.
- In external loopback mode, the local device loops back the packets received from the remote device to the remote device to test whether the link between the two devices works properly.

Example

Enable internal loopback detection on CE3 1/0/0.

```
<Huawei> system-view
[Huawei] controller e3 1/0/0
[Huawei-E3 1/0/0] loopback local
```

5.7.8 national-bit (CE3 interface view)

Function

The **national-bit** command sets the national bit on a CE3 interface.

The **undo national-bit** command restores the default settings.

By default, the national bit is 1 on a CE3 interface.

Format

national-bit { **0** | **1** }

undo national-bit

Parameters

Parameter	Description	Value
0	Sets the national bit to 0. This interface can only be used in communication within a country.	-
1	Sets the national bit to 1. This interface can be used in international communication.	-

Views

CE3 interface view

Default Level

2: Configuration level

Usage Guidelines

You are advised to set the national bit to 1. The national bit is set to 0 on a CE3 interface only in some special situations.

Example

Set the national bit on CE3 1/0/0 to 0.

```
<Huawei> system-view
[Huawei] controller e3 1/0/0
[Huawei-E3 1/0/0] national-bit 0
```

Related Topics

5.7.4 display controller e3

5.7.9 using (CE3 interface view)

Function

The **using** command configures a CE3 interface to work in E3 mode.

The **undo using** command disables a CE3 interface from working in E3 mode.

Format

using e3

undo using

Parameters

Parameter	Description	Value
e3	Configures a CE3 interface to work in E3 mode.	-

Views

CE3 interface view

Default Level

2: Configuration level

Usage Guidelines

A CE3 interface is a physical interface in the E3 system, which can work in E3 mode (unchannelized mode). To use an E3 leased line (with 34 Mbit/s bandwidth) to transmit data, configure a CE3 interface to work in E3 mode.

 Copyright © Huawei Technologies Co., Ltd.

- In E3 mode, a CE3 interface works at a rate of 34.368 Mbit/s without timeslot division. Similar to a synchronous serial interface, a CE3 interface supports IP network protocol and data link layer protocols such as PPP and FR.

Example

Configure CE3 1/0/0 to work in E3 mode.

```
<Huawei> system-view
[Huawei] controller e3 1/0/0
[Huawei-E3 1/0/0] using e3
```

5.8 E1-F Interface Configuration Commands

5.8.1 crc

Function

The **crc** command configures the cyclic redundancy check (CRC) mode of a synchronous serial interface.

The **undo crc** command restores the default CRC mode of a synchronous serial interface.

By default, the 16-bit CRC is used.

Format

crc { **16** | **32** | **none** }

undo crc

Parameters

Parameter	Description	Value
16	Indicates the 16-bit CRC.	-
32	Indicates the 32-bit CRC.	-
none	Indicates that the synchronous serial interface does not perform CRC.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CRC is a commonly used method to detect transmission errors in a communication system. It checks for transmission errors by adding redundancy codes to the original data. Transmission errors are more likely to be detected when more redundancy codes are added, but data is transmitted at a lower efficiency. Use the 16-bit or 32-bit CRC mode as required.

Precautions

- Interfaces that support CRC include:
  - Synchronous/asynchronous serial interfaces that work in synchronous mode. The interface name is Serial.
  - Interfaces formed by CE1/PRI and CT1/PRI interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by CE3 interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1-F and T1-F interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1/T1 interfaces that are channelized from CPOS interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
- The synchronous serial interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.

Example

Set the CRC mode to 32-bit CRC on Serial 1/0/0/0:0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0/0:0
[Huawei-Serial1/0/0/0:0] crc 32
```

5.8.2 display fe1

Function

Using the **display fe1** command, you can view the configuration and alarm information about a specified E1-F interface.

Format

display fe1 serial *interface-number*

Parameters

Item	Description	Value
serial *interface-number*	Displays the configuration and alarm information about a specified E1-F interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

E1-F interfaces on both ends can communicate only when they have the same parameter settings except for the clock mode.

The **display fe1** command displays the E1-F interface configuration. If the local E1-F interface configuration is different from the remote E1-F interface configuration, modify relevant parameters. This command also displays the E1-F interface alarm information, which helps you check whether the link is working properly.

NOTE

This command is applicable only to E1-F interfaces.

Example

Display the configuration and alarm information about E1-F 1/0/0.

```
<Huawei> display fe1 serial 1/0/0
Serial1/0/0
Basic Configuration:
  Work Mode is E1 Fractional Framed, Cable type is 120 Ohm balanced.
  Frame-format is NO-CRC4, Line Code is Hdb3.
  Source Clock is Slave, Data-coding is Normal.
  Idle code is 7E, Itf type is 7E, Itf number is 4.
  Loopback is Not Set.
Alarm State:
  Receiver alarm state is None.
Historical Statistics:
  Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours):
  5604553200 Line Code Violations, 0 Path Code Violations
  85520 Slip Secs, 85520 Fr Loss Secs, 85520 Line Err Secs, 0 Degraded Mins
  85520 Errored Secs, 0 Bursty Err Secs, 85520 Severely Err Secs, 85520 Unavail
Secs
```

Table 5-28 Description of the display fe1 serial command output

Item	Sub-item	Description
Basic Configuration	Work Mode	Working mode of an E1-F interface: • E1 FRACTIONAL FRAMED: The interface works in framed mode. • E1 UNFRAMED: The interface works in unframed mode. To set the working mode for an E1-F interface, run the **fe1 unframed** command.
Basic Configuration	Cable type	Type of the cable connected to an E1-F interface: • 120 Ohm: balanced cable (twisted pair). • 75 Ohm: non-balanced cable (coaxial cable).
Basic Configuration	Frame-format	Frame format of an E1-F interface, which can be **CRC4** or **NO-CRC4**. To configure the frame format for an E1-F interface, run the **fe1 frame-format** command. • CRC4: multiframe format. • NO-CRC4: basic frame format, which is also called dual-frame format or odd-even frame format.
Basic Configuration	Line Code	Line code used by an E1-F interface. The value is **HDB3**.
Basic Configuration	Source Clock	Clock mode of an E1-F interface, which can be master, slave, or system. To set the clock mode for an E1-F interface, run the **fe1 clock** command. • MASTER: The interface works in master clock mode and uses the local clock. • SLAVE: The interface works in slave clock mode and uses the line clock. • SYSTEM: The interface works in system clock mode and uses the line clock.
Basic Configuration	Data-coding	Whether to invert data: • inverted: The interface inverts data. • normal: The interface does not invert data. To configure data inversion, run the **fe1 data-coding** command.
Basic Configuration	Idle code	Line idle code used by an E1-F interface, which can be 7E or FF. To set the line idle code for an E1-F interface, run the **fe1 idlecode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Basic Configuration	Itf type	Interframe filling tag used by an E1-F interface, which can be 7E or FF. To set the minimum number of interframe filling tags for an E1-F interface, run the **fe1 itf** command.
Basic Configuration	Itf number	Minimum number of interframe filling tags, which ranges from 0 to 14. To set the minimum number of interframe filling tags for an E1-F interface, run the **fe1 itf** command.
Basic Configuration	Loopback	Whether loopback detection is enabled on an E1-F interface. If loopback detection has been enabled, the loopback detection mode is displayed. To enable loopback detection on an E1-F interface, run the **fe1 loopback** command. **NOTE** The loopback detection function monitors the interface status or cable status and must be disabled when devices are working properly.
Alarm State	Receiver alarm state is None.	No alarm is received. If an alarm is generated, the specific alarm type is displayed. The following alarms may be generated: ● Loss-of-Signal (LoS): This alarm is generated when data transmission is interrupted or frames are lost because of severe problems, for example, the cable is broken or is not connected properly. ● Alarm-Indication-Signal (AIS): This alarm is generated when the remote end fails to receive frame alignment signals. This alarm generally indicates a fault on the remote device and is also called the upstream alarm. ● Loss-of-Frame (LoF): This alarm is generated when signals cannot be encapsulated in frames. It is generated with a LoS alarm and is cleared when frame alignment succeeds. ● Remote-Alarm-Indication (RAI): This alarm is generated when the remote end does not receive frames from the local end for some reasons, for example, the local end fails to send frames, the transmission line of the local end fails, or the remote end fails to receive frames. When a LoS, AIS, or LoF alarm is generated, the local end needs to send the RAI bit to the remote end. This field will be displayed as "Transmitter is sending remote alarm."

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Historical Statistics	Data in current interval	The current accumulation period.
Historical Statistics	Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) occurring over the accumulation period.
Historical Statistics	Path Code Violations	Frame synchronization bit error in the E1-noCRC formats or a CRC error in the E1-CRC formats.
Historical Statistics	Slip Secs	A second with one or more out of frame defects or a detected incoming AIS.
Historical Statistics	Fr Loss Secs	Number of seconds an Out Of Frame (OOF) error is detected.
Historical Statistics	Line Err Secs	A second in which one or more code violations occurred or one or more LOS defects.
Historical Statistics	Degraded Mins	One in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Historical Statistics	Errored Secs	A second with one or more path coding violations, one or more Out of Frame defects, or one or more controlled slip events or a detected AIS defect.
Historical Statistics	Bursty Err Secs	A second with fewer than 320 and more than one path coding violation error events, no Severely Errored Frame defects, and no detected incoming AIS defects.
Historical Statistics	Severely Err Secs	A second with 320 or more path code violation errors events, one or more Out of Frame defects, or a detected AIS defect.
Historical Statistics	Unavail Secs	Number of seconds that the interface is unavailable.
Historical Statistics	Total Data	Displays total accumulated data for all intervals.

5.8.3 display workmode

Function

The **display workmode** command displays the working modes of interface cards.

Format

display workmode { **slot** *slot-id* | **all** }

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the working mode of an interface card in a specified slot.	The value must be the slot ID of an interface card with a configurable working mode. The working mode of the following interface cards can be changed: 1E1T1-M/2E1T1-M, 1E1T1-F/2E1T1-F, 4G.SHDSL, VDSL2, 1CPOS-155M, 4STM1 and 2BST.
all	Displays the working mode of all interface cards with configurable working modes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command applies to only the interface cards with configurable working mode. To configure the working mode of an interface card, run the **set workmode e1t1**, **set workmode e1t1-f**, **set workmode shdsl**, **set workmode vdsl**, **set workmode cpos**, **set workmode stm** or **set workmode bri** command.

Example

Display the working mode of the interface card in slot 2.

```
<Huawei> display workmode slot 2
-----------------------------------------------------------------------
Slot  Type              config-workmode     active-workmode
-----------------------------------------------------------------------
2     1CPOS-155M-W        e1-data         e1-data
```

Table 5-29 Description of the display workmode command output

Item	Description
Slot	Slot ID of the interface card.
Type	Interface card type: ● 1E1/T1-M ● 2E1/T1-M ● 4E1/T1-M ● 8E1/T1-M ● 1E1/T1-F ● 2E1/T1-F ● 4E1/T1-F ● 8E1/T1-F ● 4G.SHDSL ● VDSL2 ● 1CPOS-155M ● 4STM1 ● 2BST

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
config-workmode	config working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
active-workmode	active working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

5.8.4 fe1 clock

Function

Using the **fe1 clock** command, you can set the clock mode of an E1-F interface.

Using the **undo fe1 clock** command, you can restore the default clock mode of an E1-F interface.

By default, an E1-F interface works in slave clock mode and uses the line clock.

Format

fe1 clock { **master** | **slave** | **system** }

undo fe1 clock

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
master	Configures an E1-F interface to work in master clock mode and use the local clock. When an E1-F interface functions as the data circuit-terminating equipment (DCE), it must work in master clock mode and provide clock signals for the data terminal equipment (DTE).	-
slave	Configures an E1-F interface to work in slave clock mode and use the line clock. When an E1-F interface functions as the DTE, it must work in slave clock mode and obtain clock signals from the DCE.	-
system	Configures an E1-F interface to work in system clock mode and use the line clock.	-

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To exchange data successfully, communicating parties must work in clock synchronization state.

Precautions

When E1-F interfaces of two devices are directly connected, one E1-F interface must work in master clock mode and the other must work slave clock mode.

Example

Configure E1-F 1/0/0 to work in master clock mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 clock master
```

5.8.5 fe1 data-coding

Function

Using the **fe1 data-coding** command, you can determine whether an E1-F interface inverts data.

Using the **undo fe1 data-coding** command, you can restore the default setting.

By default, an E1-F interface does not invert data.

Format

fe1 data-coding { **inverted** | **normal** }

undo fe1 data-coding

Parameters

Parameter	Description	Value
inverted	Configures an E1-F interface to invert data.	-
normal	Configures an E1-F interface not to invert data.	-

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

When data inversion is enabled on an E1-F interface, the E1-F interface inverts every one bit in a data stream into a zero bit and every zero bit into a one bit.

E1-F interfaces on both ends can communicate only when they have the same data inversion configuration.

Example

Configure E1-F 1/0/0 to invert data.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 data-coding inverted
```

5.8.6 fe1 detect-ais

Function

Using the **fe1 detect-ais** command, you can enable alarm indication signal (AIS) detection on an E1-F interface.

Using the **undo fe1 detect-ais** command, you can disable AIS detection.

By default, AIS detection is enabled on an E1-F interface.

Format

fe1 detect-ais

undo fe1 detect-ais

Parameters

None

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AIS alarms are also called upstream alarms, indicating that the peer device or the receive link of the local device becomes faulty.

An AIS alarm is generated when the number of 0s in 512 consecutive bits (two consecutive frames) of a received signal is smaller than 3. An AIS alarm is cleared when the number of 0s in 512 consecutive bits of a received signal is greater than or equal to 3.

When AIS detection is enabled on an E1-F interface, the local device sends the RAI bit to the peer device after detecting AIS alarms.

Prerequisite

The E1-F interface has been configured to work in unframed mode using the **fe1 unframed** command.

Precautions

In framed mode, AIS detection is enabled for frame alignment detection by default. Therefore, this command cannot be used on an E1-F interface working in framed mode.

Example

Disable AIS detection on E1-F 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] undo fe1 detect-ais
```

Related Topics

5.8.15 fe1 unframed

 Copyright © Huawei Technologies Co., Ltd.

5.8.7 fe1 detect-rai

Function

Using the **fe1 detect-rai** command, you can enable remote alarm indication (RAI) detection on an E1-F interface.

Using the **undo fe1 detect-rai** command, you can disable RAI detection.

By default, RAI detection is enabled on an E1-F interface.

Format

fe1 detect-rai

undo fe1 detect-rai

Parameters

None

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If RAI detection is enabled, a device sends an RAI alarm to its peer device after detecting loss of frame (LoF) caused by clock asynchronization or loss of signal (LoS).

Prerequisite

The E1-F interface must work in framed mode.

If an E1-F interface works in unframed mode, run the **undo fe1 unframed** command to configure the E1-F interface to work in framed mode. To view the working mode of an E1-F interface, run the **display fe1** command.

Example

Disable RAI detection on E1-F 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] undo fe1 detect-rai
```

Related Topics

5.8.2 display fe1

 Copyright © Huawei Technologies Co., Ltd.

5.8.15 fe1 unframed

5.8.8 fe1 frame-format

Function

Using the **fe1 frame-format** command, you can set the frame format for an E1-F interface.

Using the **undo fe1 frame-format** command, you can restore the default frame format.

By default, an E1-F interface uses the basic frame format (non-CRC4).

Format

fe1 frame-format { **crc4** | **no-crc4** }

undo fe1 frame-format

Parameters

Parameter	Description	Value
crc4	Sets the frame format to CRC4 (multiframe format).	-
no-crc4	Sets the frame format to non-CRC4 (basic frame format).	-

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In framed mode, an E1-F interface supports two frame formats:

- CRC4: indicates the multiframe format. A multiframe is formed by the first bit in each frame transmitted over timeslot 0. It contains 16 consecutive pulse code modulation (PCM) frames.
- Non-CRC4: indicates the basic frame format, which is also called the dual-frame format or odd-even frame format.

The multiframe format supports Cyclic Redundancy Check 4-bit (CRC4), whereas the basic frame format does not support CRC4.

Prerequisite

The E1-F interface must work in framed mode.

 Copyright © Huawei Technologies Co., Ltd.

If an E1-F interface works in unframed mode, run the **undo fe1 unframed** command to configure the E1-F interface to work in framed mode. To view the working mode of an E1-F interface, run the **display fe1** command.

Precautions

Interfaces on both ends can communicate only when they use the same frame format. If two E1-F interfaces use different frame formats, a CRC4 alarm is generated.

Example

Set the frame format to CRC4 for E1-F 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 frame-format crc4
```

Related Topics

5.8.2 display fe1

5.8.15 fe1 unframed

5.8.9 fe1 idlecode

Function

Using the **fe1 idlecode** command, you can set the line idle code for an E1 interface.

Using the **undo fe1 idlecode** command, you can restore the default line idle code.

By default, an E1-F interface uses the line idle code 0x7e.

Format

fe1 idlecode { **7e** | **ff** }

undo fe1 idlecode

Parameters

Parameter	Description	Value
7e	Sets the line idle code to 0x7e.	-
ff	Sets the line idle code to 0xff.	-

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An E1-F interface transmits electrical signals, and therefore the interface line keeps transmitting data. When no data is being transmitted, the line idle code needs to be filled.

The line idle code is the code sent over a timeslot that is not bundled into a channel.

An E1-F interface supports two types of line idle codes: 0x7e and 0xff. The default line idle code 0x7e is recommended.

Precautions

Interfaces on both ends can communicate only when they use the same line idle code.

Example

Set the line idle code to 0xff for E1-F 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 idlecode ff
```

5.8.10 fe1 itf

Function

Using the **fe1 itf** command, you can set the interframe filling tag and the number of interframe filling tags on an E1-F interface.

Using the **undo fe1 itf** command, you can restore the default setting.

By default, an E1-F interface uses the interframe filling tag 0x7e and sends four filling tags between two frames.

Format

fe1 itf { **number** *number* | **type** { **7e** | **ff** } }

undo fe1 itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value ranges from 0 to 14. Specially, the value ranges from 0 to 7 for the E1-F interface on the AR2204-FE.
type	Specifies the interframe filling tag.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag is the code sent when a timeslot in a logical channel does not send any service data.

An E1-F interface supports two interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

Precautions

- Interfaces on both ends can communicate only when the same interframe filling tag and the same number of interframe filling tags are set for them.
- An E1-F interface cannot achieve the bandwidth because of extra costs of interframe filling tags. To improve the transmission rate of the E1-F interface, run the **fe1 itf number** command to set the number of interframe filling tags to 0.

Example

Set the interframe filling tag to 0xff on E1-F 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 itf type ff
```

5.8.11 fe1 line-termination

Function

Using the **fe1 line-termination** command, you can set the cable type for an E1-F interface.

Using the **undo fe1 line-termination** command, you can restore the default cable type.

By default, the cable type applicable to an E1-F interface is 120 ohm balanced cable (twisted pair).

Format

fe1 line-termination { **75-ohm** | **120-ohm** }

undo fe1 line-termination

Parameters

Parameter	Description	Value
75-ohm	Indicates that an E1-F interface connects to a 75 ohm non-balanced cable (coaxial cable).	-
120-ohm	Indicates that an E1-F interface connects to a 120 ohm balanced cable (twisted pair).	-

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

An E1-F interface can connect to a twisted pair or coaxial cable. The resistance of a twisted pair is 120 ohm, and the resistance of a coaxial cable is 75 ohm.

This command is required when the type of the cable connected to an E1-F interface changes.

Example

Set the cable type to coaxial cable for E1-F 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 line-termination 75-ohm
```

5.8.12 fe1 loopback

Function

Using the **fe1 loopback** command, you can enable loopback detection on an E1-F interface.

Using the **undo fe1 loopback** command, you can disable loopback detection on an E1-F interface.

By default, loopback detection is disabled on an E1-F interface.

Format

fe1 loopback { **local** | **payload** | **remote** }

undo fe1 loopback

Parameters

Parameter	Description	Value
local	Indicates internal loopback.	-
payload	Indicates payload loopback.	-
remote	Indicates external loopback.	-

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function monitors the interface status or cable status and must be disabled when devices are working properly.

- Internal loopback tests whether the local device works properly by looping back outgoing packets to the local device.
- Payload loopback tests whether the local device works properly by looping back the valid payload of outgoing packets. Generally, frames transmitted by timeslot 0 are not looped back.
- External loopback tests whether the link between the local and remote devices works properly by looping back the packets received from the remote device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable internal loopback detection on E1-F 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 loopback local
```

5.8.13 fe1 sa

Function

The **fe1 sa** command sets the content of the five outgoing sa bits.

The **undo fe1 sa** command restores the default setting.

By default, the content of the five outgoing sa bits is 0.

Format

fe1 sa *sa4 sa5 sa6 sa7 sa8*

undo fe1 sa

Parameters

Parameter	Description	Value
sa4	Specifies the content of the outgoing sa4 bit.	The value is an integer that ranges from 0 to 255.
sa5	Specifies the content of the outgoing sa5 bit.	The value is an integer that ranges from 0 to 255.
sa6	Specifies the content of the outgoing sa6 bit.	The value is an integer that ranges from 0 to 255.
sa7	Specifies the content of the outgoing sa7 bit.	The value is an integer that ranges from 0 to 255.
sa8	Specifies the content of the outgoing sa8 bit.	The value is an integer that ranges from 0 to 255.

Views

E1-F interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When an E1-F interface works in framed mode, SA4 to SA8 in the E1 frame can be used for transmitting low-speed data. By default, the values of SA4 to SA8 are 0. In some scenarios, the remote device will check received SA fields. Therefore, SA fields must be configurable on the router to ensure normal connection of the E1-F interface.

Prerequisites

The E1-F interface must work in framed mode.

By default, an E1-F interface works in framed mode. If an E1-F interface works in unframed mode, run the **undo fe1 unframed** command to configure the E1-F interface to work in framed mode. To view the working mode of an E1-F interface, run the **display fe1** command.

Precautions

By default, the SA field value is 0. Before configuring the SA field, collect configuration information on the remote device.

Example

Set the content of five outgoing sa bits to 1, 2, 3, 4, and 5 respectively.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 sa 1 2 3 4 5
```

5.8.14 fe1 timeslot-list

Function

Using the **fe1 timeslot-list** command, you can bundle timeslots on an E1-F interface into a channel.

Using the **undo fe1 timeslot-list** command, you can restore the default setting.

By default, all timeslots of an E1-F interface are bundled, and the rate of the E1-F interface is 1984 kbit/s.

Format

fe1 timeslot-list *list*

undo fe1 timeslot-list

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
list	Specifies the numbers of timeslots to be bundled.	The value is an integer that ranges from 1 to 31. You can specify a single timeslot by using *number*, specify a timeslot range by using *number1-number2*, or specify multiple timeslots by using *number1, number2-number3*.

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an E1-F interface works in framed mode, its 2 Mbit/s transmission line is divided into 32 timeslots (64 kbit/s in each timeslot). Timeslot 0 transmits frame alignment signals, and any of timeslots 1 to 31 can be bundled into a channel. The rate of an E1-F interface is *n* x 64 kbit/s, in which *n* is the number of timeslots bundled into a channel. An E1-F interface working in framed mode supports link layer protocols such as Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), and Frame Relay (FR) and network protocols such as IP.

Prerequisite

The E1-F interface must work in framed mode.

By default, an E1-F interface works in framed mode. If an E1-F interface works in unframed mode, run the **undo fe1 unframed** command to configure the E1-F interface to work in framed mode. To view the working mode of an E1-F interface, run the **display fe1** command.

Example

Bundle timeslots 1, 2, 3, 8, and 10 of E1-F 1/0/0 into a channel.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 timeslot-list 1-3,8,10
```

Related Topics

5.8.2 display fe1

5.8.15 fe1 unframed

5.8.15 fe1 unframed

Function

Using the **fe1 unframed** command, you can configure an E1-F interface to work in unframed mode.

Using the **undo fe1 unframed** command, you can configure an E1-F interface to work in framed mode.

By default, an E1-F interface works in framed mode.

Format

fe1 unframed

undo fe1 unframed

Parameters

None

Views

E1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An E1-F interface works in either of the following modes:

- In unframed mode, an E1-F interface works at a rate of 2.048 Mbit/s without timeslot division. Similar to a synchronous serial interface, an E1-F interface supports link layer protocols such as PPP, HDLC, FR, and IP.
- In framed mode, an E1-F interface is divided into 32 timeslots, which are numbered 0 to 31. Timeslot 0 transmits frame alignment signals. Any random group of timeslots 1 to 31 can be bundled into a channel. The rate of an E1-F interface is *n* x 64 kbit/s, in which *n* is the number of timeslots bundled into a channel.

In either unframed mode or framed mode, an E1-F interface is similar to a synchronous serial interface and supports link layer protocols such as the Point-to-Point Protocol (PPP), High-Level Data Link Control (HDLC), and Frame Relay (FR) and network protocols such as IP.

If an E1-F interface is connected to an E1 leased line (2 Mbit/s), configure the E1-F interface to work in unframed mode. If an E1-F interface is connected to a low-rate (1 Mbit/s or 512 kbit/s) line, configure the E1-F interface to work in framed mode.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

If an E1-F interface works in framed mode, you can run the **fe1 timeslot-list** command to specify the timeslots to be bundled.

Example

Configure E1-F 1/0/0 to work in unframed mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fe1 unframed
```

Related Topics

5.8.14 fe1 timeslot-list

5.8.16 reset framerstatics

Function

The **reset framerstatics** command clears error frame statistics on an interface.

Format

reset framerstatics [**fe1 interface** *interface-type interface-number* | **ft1 interface** *interface-type interface-number* | **controller e1** *interface-number*]

Parameters

Parameter	Description	Value
fe1 interface *interface-type interface-number*	Clears error frame statistics on a specified E1-F interface.	-
ft1 interface *interface-type interface-number*	Clears error frame statistics on a specified T1-F interface.	-
controller e1 *interface-number*	Clears error frame statistics on a specified CE1/PRI interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **reset framerstatics** command to clear error frame statistics on an interface. The statistics cannot be restored after being cleared.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear error frame statistics on the interface E13/0/0.

```
<Huawei> reset framerstatics controller e1 3/0/0
```

5.8.17 set workmode e1t1-f

Function

The **set workmode e1t1-f** command sets the working mode of a 1E1T1-F/2E1T1-F interface card.

By default, a 1E1T1-F/2E1T1-F interface card works in E1-F mode.

NOTE

The 4E1T1-F/8E1T1-F interface card only works in E1-F mode and does not support working mode switching.

Format

set workmode slot *slot-id* **e1t1-f** { **e1-f** | **t1-f** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a 1E1T1-F/2E1T1-F interface card.	Run the **display device** command to view slot IDs and types of interface cards and find the slot ID with E1/T1-F displayed. Then run the **display workmode** command to view the interface card work mode on the device.
e1-f	Indicates a 1E1T1-F/2E1T1-F interface card works in fractional channelized E1 (E1-F) mode.	-
t1-f	Indicates a 1E1T1-F/2E1T1-F interface card works in fractional channelized T1 (T1-F) mode.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A 1E1T1-F interface card provides one fractional channelized E1/T1 interface and a 2E1T1-F interface card provides two fractional channelized E1/T1 interfaces. A 1E1T1-F/2E1T1-F interface card cannot both provide E1-F and T1-F interfaces. The **set workmode e1t1-f** command sets the working mode of a 1E1T1-F/2E1T1-F interface card.

Precautions

After this command is used, the system prompts you to reset the 1E1T1-F/2E1T1-F interface card to make the new working mode take effect. If you select **Yes**, the system resets the interface card. Otherwise, you need to run the **reset slot** command to manually reset the interface card to make the new working mode take effect.

Example

Configure the 2E1T1-F interface card in slot 1 to work in T1-F mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1-f t1-f
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

Related Topics

4.1.3 display device

5.8.3 display workmode

4.2.13 reset slot

5.9 T1-F Interface Configuration Commands

5.9.1 crc

Function

The **crc** command configures the cyclic redundancy check (CRC) mode of a synchronous serial interface.

The **undo crc** command restores the default CRC mode of a synchronous serial interface.

By default, the 16-bit CRC is used.

Format

crc { **16** | **32** | **none** }

undo crc

Parameters

Parameter	Description	Value
16	Indicates the 16-bit CRC.	-
32	Indicates the 32-bit CRC.	-
none	Indicates that the synchronous serial interface does not perform CRC.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CRC is a commonly used method to detect transmission errors in a communication system. It checks for transmission errors by adding redundancy codes to the original data. Transmission errors are more likely to be detected when more redundancy codes are added, but data is transmitted at a lower efficiency. Use the 16-bit or 32-bit CRC mode as required.

Precautions

- Interfaces that support CRC include:
  - Synchronous/asynchronous serial interfaces that work in synchronous mode. The interface name is Serial.
  - Interfaces formed by CE1/PRI and CT1/PRI interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by CE3 interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1-F and T1-F interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
  - Interfaces formed by E1/T1 interfaces that are channelized from CPOS interfaces. The interface name is Serial and the interface logic is the same as that of synchronous serial interfaces.
- The synchronous serial interfaces on both ends of a link must use the CRC of the same length. If lengths of the CRCs used on two ends are different, the two devices cannot communicate with each other.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the CRC mode to 32-bit CRC on Serial 1/0/0/0:0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0/0:0
[Huawei-Serial1/0/0/0:0] crc 32
```

5.9.2 display ft1

Function

Using the **display ft1** command, you can view the configuration and alarm information about a specified T1-F interface.

Format

display ft1 serial *interface-number*

Parameters

Parameter	Description	Value
serial *interface-number*	Displays the configuration and alarm information about a specified T1-F interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To ensure that devices on both ends communicate, T1-F interfaces on both ends must be configured with the same parameters except for the clock mode.

You can run the **display ft1** command to view the configuration of a specified T1-F interface. If the local configuration conflicts with the remote configuration, change the local configuration. You can also run the **display ft1** command to view the alarm information about the T1-F interface for fault location.

NOTE

This command is applicable only to T1-F interfaces.

Example

Display the configuration and alarm information about T1-F 1/0/0.

```
<Huawei> display ft1 serial 1/0/0
Serial1/0/0
Basic Configuration:
  Work Mode is T1 Fractional Framed, Cable type is 100 Ohm balanced.
  Frame-format is ESF, Line Code is B8zs.
  Source Clock is Slave, Data-coding is Normal.
  Idle code is 7E, Itf type is 7E, Itf number is 4.
  Loopback is Not Set.
Alarm State:
  Receiver alarm state is None.
Historical Statistics:
  Data in current interval (0 seconds elapsed):
  0 Line Code Violations, 0 Path Code Violations
  0 Slip Secs, 0 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
  0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 0 Unavail Secs
  Total Data (last 24 hours):
  5604553200 Line Code Violations, 0 Path Code Violations
  85520 Slip Secs, 85520 Fr Loss Secs, 85520 Line Err Secs, 0 Degraded Mins
  85520 Errored Secs, 0 Bursty Err Secs, 85520 Severely Err Secs, 85520 Unavail
Secs
```

Table 5-30 Description of the display ft1 command output

Item	Sub-item	Description
Basic Configuration	Work Mode is T1 Fractional Framed	The interface works in framed mode.
Basic Configuration	Cable type is 100 Ohm balanced.	The cable is connected to a 100 ohm balanced cable.
Basic Configuration	Frame-format	Frame format of the interface, which can be ESF or SF. To configure the frame format for a T1-F interface, run the **ft1 frame-format** command. ● ESF: extended super frame format ● SF: super frame format
Basic Configuration	Line Code	Encoding and decoding mode of the interface, which can be **B8ZS**.
Basic Configuration	Source Clock	Clock mode of the interface, which can be master or slave. To set the clock mode for a T1-F interface, run the **ft1 clock** command. ● MASTER: indicates that the interface works in master clock mode and uses internal clock signals. ● SLAVE: indicates that the interface works in slave clock mode and uses line clock signals.

Item	Sub-item	Description
Basic Configuration	Data-coding	Whether to invert data. The value can be **inverted** or **normal**: ● inverted: The interface inverts data. ● normal: The interface does not invert data. To configure data inversion, run the **ft1 data-coding** command.
Basic Configuration	Idle code	Line idle code of the interface, which can be 7E or FF. To set the line idle code for a T1-F interface, run the **ft1 idlecode** command.
Basic Configuration	Itf type	Interframe filling tag of the interface, which can be 7E or FF. To set the interframe filling tag for a T1-F interface, run the **ft1 itf** command.
Basic Configuration	Itf number	Number of interframe filling tags, which ranges from 0 to 14. To set the number of interframe filling tags for a T1-F interface, run the **ft1 itf** command.
Basic Configuration	Loopback	Whether loopback detection is enabled on the interface. If loopback detection has been enabled, the loopback detection mode is displayed. To enable loopback detection on a T1-F interface, run the **ft1 loopback** command. **NOTE** The loopback detection function detects the interface status or cable status and must be disabled when devices work properly.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Alarm State	Receiver alarm state is None.	No alarm is received. If an alarm is generated, the specific alarm type is displayed. The following alarms may be generated: ● Loss-of-Signal (LOS): This alarm is generated when data transmission is interrupted or frames are lost because of severe problems, for example, the cable is broken or is not well connected. ● Alarm-Indication-Signal (AIS): This alarm is generated when the remote end fails to receive the frame alignment signals. This alarm generally indicates a fault on the remote device and is also called the upstream alarm. ● Loss-of-Frame (LOF): This alarm is generated when signals cannot be encapsulated in frames. It is usually generated with a LOS alarm and is cleared when frame alignment succeeds. ● Remote-Alarm-Indication (RAI): This alarm is generated when the remote end does not receive frames from the local end for some reasons, for example, the local end fails to send frames, the transmission line of the local end fails, or the remote end fails to receive frames. When a LOS, AIS, or LOF alarm is generated, the local end needs to send the RAI bit to the remote end. In addition, "Transmitter is sending remote alarm." is displayed.
Historical Statistics	Data in current interval	The current accumulation period.
Historical Statistics	Line Code Violations	Count of both Bipolar Violations (BPVs) and Excessive Zeros (EXZs) occurring over the accumulation period.
Historical Statistics	Path Code Violations	Frame synchronization bit error in the E1-noCRC formats or a CRC error in the E1-CRC formats.
Historical Statistics	Slip Secs	A second with one or more out of frame defects or a detected incoming AIS.
Historical Statistics	Fr Loss Secs	Number of seconds an Out Of Frame (OOF) error is detected.
Historical Statistics	Line Err Secs	A second in which one or more code violations occurred or one or more LOS defects.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Historical Statistics	Degraded Mins	One in which the estimated error rate exceeds 1E-6 but does not exceed 1E-3.
Historical Statistics	Errored Secs	A second with one or more path coding violations, one or more Out of Frame defects, or one or more controlled slip events or a detected AIS defect.
Historical Statistics	Bursty Err Secs	A second with fewer than 320 and more than one path coding violation error events, no Severely Errored Frame defects, and no detected incoming AIS defects.
Historical Statistics	Severely Err Secs	A second with 320 or more path code violation errors events, one or more Out of Frame defects, or a detected AIS defect.
Historical Statistics	Unavail Secs	Number of seconds that the interface is unavailable.
Historical Statistics	Total Data	Displays total accumulated data for all intervals.

5.9.3 display workmode

Function

The **display workmode** command displays the working modes of interface cards.

Format

display workmode { **slot** *slot-id* | **all** }

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the working mode of an interface card in a specified slot.	The value must be the slot ID of an interface card with a configurable working mode. The working mode of the following interface cards can be changed: 1E1T1-M/2E1T1-M, 1E1T1-F/2E1T1-F, 4G.SHDSL, VDSL2, 1CPOS-155M, 4STM1 and 2BST.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Displays the working mode of all interface cards with configurable working modes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command applies to only the interface cards with configurable working mode. To configure the working mode of an interface card, run the **set workmode e1t1**, **set workmode e1t1-f**, **set workmode shdsl**, **set workmode vdsl**, **set workmode cpos**, **set workmode stm** or **set workmode bri** command.

Example

Display the working mode of the interface card in slot 2.

```
<Huawei> display workmode slot 2
-----------------------------------------------------------------------------
Slot  Type                 config-workmode     active-workmode
-----------------------------------------------------------------------------
2     1CPOS-155M-W         e1-data             e1-data
```

Table 5-31 Description of the display workmode command output

Item	Description
Slot	Slot ID of the interface card.

Item	Description
Type	Interface card type: ● 1E1/T1-M ● 2E1/T1-M ● 4E1/T1-M ● 8E1/T1-M ● 1E1/T1-F ● 2E1/T1-F ● 4E1/T1-F ● 8E1/T1-F ● 4G.SHDSL ● VDSL2 ● 1CPOS-155M ● 4STM1 ● 2BST

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
config-workmode	config working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
active-workmode	active working mode: ● e1-data: The interface card works in CE1/PRI mode. ● e1-voice: The interface card is configured as an E1 voice card. ● t1-data: The interface card works in CT1/PRI mode. ● t1-voice: The interface card is configured as an T1 voice card. ● stm1: The interface card works in 4stm mode, that is, it provides four interfaces working at the rate of 155 Mbit/s. ● stm4: The interface card works in 1stm mode, that is, it provides one interface working at the rate of 622 Mbit/s. ● e1-f: The interface card works in E1-F mode. ● t1-f: The interface card works in T1-F mode. ● atm: The 4G.SHDSL interface card works in ATM mode. ● ptm: The 4G.SHDSL interface card works in PTM mode. ● bri-voice-nt: The voice interface card works in NT mode. ● bri-voice-te: The voice interface card works in TE mode.

5.9.4 ft1 alarm-threshold

Function

Using the **ft1 alarm-threshold** command, you can configure alarm thresholds for a T1-F interface.

Using the **undo ft1 alarm-threshold** command, you can restore the default alarm thresholds for a T1-F interface.

The default alarm thresholds are as follows:

- Loss of signal (LOS) alarm: The value of pulse-detection is 176 and the value of pulse-recovery is 22, indicating that a LOS alarm is generated if less than 22 pulses are detected within 176 pulse intervals.

 Copyright © Huawei Technologies Co., Ltd.

- Alarm indication signal (AIS) alarm: level-1.
- Loss of frame alignment (LFA) alarm: level-1.

Format

ft1 alarm-threshold { **ais** { **level-1** | **level-2** } | **lfa** { **level-1** | **level-2** | **level-3** | **level-4** } | **los** { **pulse-detection** *value* | **pulse-recovery** *value* } }

undo ft1 alarm-threshold { **ais** | **lfa** | **los** { **pulse-detection** | **pulse-recovery** } }

Parameters

Parameter	Description	Value
ais { **level-1** | **level-2** }	Sets the AIS alarm threshold. ● **level-1**: indicates that an AIS alarm is generated when there are less than two 0s in the bit stream of a super frame (SF) or extended super frame (ESF). ● **level-2**: indicates that an AIS is generated when there is less than three 0s in the code stream of an SF or less than five 0s in the code stream of an ESF.	The default AIS alarm threshold is **level-1**.
lfa { **level-1** | **level-2** | **level-3** | **level-4** }	Sets the loss of frame alignment (LFA) alarm threshold. ● **level-1**: indicates that an LFA alarm is generated when two of four frame alignment bits are lost. ● **level-2**: indicates that an LFA alarm is generated when two of five frame alignment bits are lost. ● **level-3**: indicates that an LFA alarm is generated when two of six frame alignment bits are lost. ● **level-4**: indicates that an LFA alarm is generated when errors occur in four consecutive ESF frames. This keyword is valid only for the ESF format.	The default LFA alarm threshold is **level-1**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
los { **pulse-detection** *value* | **pulse-recovery** *value*	Sets the LOS alarm threshold. • **pulse-detection** specifies the LOS detection period, expressed by the number of pulse intervals. • **pulse-recovery** specifies the pulse threshold. A LOS alarm is generated when the number of pulses detected within the specified number of pulse intervals is less than the value of **pulse-recovery**.	The value of **pulse-detection** ranges from 16 to 4096, and the value of **pulse-recovery** ranges from 1 to 256. By default, the value of **pulse-detection** is 176 and the value of **pulse-recovery** is 22, indicating that a LOS alarm is generated if less than 22 pulses are detected within 176 pulse intervals. The value of **pulse-detection** ranges from 16 to 4096, and the value of **pulse-recovery** ranges from 1 to 256. By default, the value of **pulse-detection** is 176 and the value of **pulse-recovery** is 22, indicating that a LOS alarm is generated if less than 22 pulses are detected within 176 pulse intervals.

Views

T1-F interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the LOS detection period to 300 pulse intervals.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 alarm-threshold los pulse-detection 300
```

5.9.5 ft1 cable

Function

Using the **ft1 cable** command, you can set the attenuation or length of the transmission line matching a T1-F interface.

Using the **undo ft1 cable** command, you can restore the default transmission line configuration.

The default attenuation of the transmission line on a T1-F interface is -7.5 db.

Format

ft1 cable { **long** { **-7.5db** | **-15db** | **-22.5db** } | **short** { **133ft** | **266ft** | **399ft** | **533ft** | **655ft** } }

undo ft1 cable

Parameters

Parameter	Description	Value
long { **-7.5db** | **-15db** | **-22.5db**	Sets the attenuation of the transmission line matching the T1-F interface. This parameter is applicable to transmission lines longer than 655 feet. The attenuation of such transmission lines can be -7.5 db, -15 db, or -22.5 db. Set the attenuation based on quality of received signals. Transmission lines with a lower quality have a larger attenuation. When received signals are of low quality, set this parameter to offset the attenuation.	-
short { **133ft** | **266ft** | **399ft** | **533ft** | **655ft** }	Sets the length of the transmission line matching the T1-F interface. This parameter is applicable to transmission lines not longer than 665 feet. The length can be 133 feet, 266 feet, 399 feet, 533 feet, or 655 feet.	-

Views

T1-F interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command is required only when received signals are of a low quality. The command determines the waveform of transmitted signals.

When signals that the device receives are of a good quality, use the default configuration.

Example

Set the length of the transmission line matching T1-F interface Serial 1/0/0 to 133 feet.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 cable short 133ft
```

5.9.6 ft1 clock

Function

Using the **ft1 clock** command, you can set the clock mode for a T1-F interface.

Using the **undo ft1 clock** command, you can restore the default setting.

By default, a T1-F interface works in slave clock mode and uses line clock signals.

Format

ft1 clock { **master** | **slave** | **system** }

undo ft1 clock

Parameters

Parameter	Description	Value
master	Configures a T1-F interface to work in master clock mode and use internal clock signals. When a T1-F interface functions as a Data Circuit-terminating Equipment (DCE), it must work in master clock mode and provide clock signals for a Data Terminal Equipment (DTE).	-
slave	Configures a T1-F interface to work in slave clock mode and use line clock signals. When a T1-F interface functions as a DTE, it must work in slave clock mode and obtain clock signals from a DCE.	-
system	Configures a T1-F interface to work in system clock mode and use line clock signals.	-

Views

T1-F interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To exchange data correctly, communicating parties must work in clock synchronization state.

Precautions

When T1-F interfaces of two devices are directly connected, one T1-F interface must work in master clock mode and the other in slave clock mode.

Example

Configure T1-F interface Serial 1/0/0 to work in master clock mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 clock master
```

5.9.7 ft1 data-coding

Function

Using the **ft1 data-coding** command, you can determine whether data is inverted by a T1-F interface.

Using the **undo ft1 data-coding** command, you can restore the default setting.

By default, a T1-F interface does not invert data.

Format

ft1 data-coding { **inverted** | **normal** }

undo ft1 data-coding

Parameters

Parameter	Description	Value
inverted	Configures a T1-F interface to invert data.	-
normal	Configures a T1-F interface not to invert data.	-

Views

T1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Data inversion indicates that every "1" bit in the data stream becomes a "0" bit and every "0" bit becomes a "1" bit.

Devices on both ends can communicate only when the same data inversion configuration is performed on T1-F interfaces on both devices.

Example

Configure T1-F interface Serial 1/0/0 to invert data.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 data-coding inverted
```

5.9.8 ft1 detect-rai

Function

Using the **ft1 detect-rai** command, you can enable remote alarm indication (RAI) detection on a T1-F interface.

Using the **undo ft1 detect-rai** command, you can disable RAI detection.

By default, RAI detection is enabled on a T1-F interface.

Format

ft1 detect-rai

undo ft1 detect-rai

Parameters

None

Views

T1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If RAI detection is enabled, a device sends an RAI alarm to its peer device after detecting loss of frame (LoF) caused by clock asynchronization or loss of signal (LoS).

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The frame format has been set to extended super frame (ESF) by using the **ft1 frame-format esf** command.

Example

Disable RAI detection on T1-F interface Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] undo ft1 detect-rai
```

Related Topics

5.9.2 display ft1

5.9.9 ft1 frame-format

Function

Using the **ft1 frame-format** command, you can set the frame format for a T1-F interface.

Using the **undo ft1 frame-format** command, you can restore the default setting.

By default, a T1-F interface uses the extended super frame (ESF) format.

Format

ft1 frame-format { **esf** | **sf** }

undo ft1 frame-format

Parameters

Parameter	Description	Value
esf	Sets the frame format to ESF.	-
sf	Sets the frame format to super frame (SF).	-

Views

T1-F interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

A T1-F interface supports the SF format and ESF format. The two formats enable multiple frames to share the frame alignment information and signaling information so that more bits can be used to transmit data.

- SF: consists of 12 frames that share the frame alignment information and signaling information. Frame 6 and frame 12 are signaling frames.
- ESF: consists of 24 frames that share the frame alignment information and signaling information. Frames 6, 12, 18, and 24 are signaling frames.

Example

Set the frame format on T1-F interface Serial 1/0/0 to SF.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 frame-format sf
```

5.9.10 ft1 idlecode

Function

Using the **ft1 idlecode** command, you can set the line idle code for a T1-F interface.

Using the **undo ft1 idlecode** command, you can restore the default setting.

By default, the line idle code of a T1-F interface is 0x7e.

Format

ft1 idlecode { **7e** | **ff** }

undo ft1 idlecode

Parameters

Parameter	Description	Value
7e	Sets the line idle code to 0x7e.	-
ff	Sets the line idle code to 0xff.	-

Views

T1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A T1-F interface transmits electrical signals, and therefore the interface line keeps transmitting data. When no data is being transmitted, a line idle code needs to be filled.

The line idle code is the code sent over the timeslot that is not bundled to form any logical channel.

A T1-F interface supports two line idle codes: 0x7e and 0xff. The default line idle code 0x7e is recommended.

Precautions

Devices on both ends can communicate properly only when the same line idle code is set for T1-F interfaces on both devices.

Example

Set the line idle code to 0xff for T1-F interface Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 idlecode ff
```

5.9.11 ft1 itf

Function

Using the **ft1 itf** command, you can set the interframe filling tag and the number of interframe filling tags on a T1-F interface.

Using the **undo ft1 itf** command, you can restore the default setting.

By default, a T1-F interface uses the interframe filling tag 0x7e and four interframe filling tags.

Format

ft1 itf { **number** *number* | **type** { **7e** | **ff** } }

undo ft1 itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 14. Specially, the value ranges from 0 to 7 for the T1-F interface on the AR2204-FE.

Parameter	Description	Value
type	Specifies the interframe filling tag.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

T1-F interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag is the code sent when the timeslot bundled to form a logical channel does not send any service data.

A T1-F interface supports two interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

Precautions

- Devices on both ends can communicate properly only when the same interframe filling tag and the same number of interframe filling tags are set on T1-F interfaces of both devices.
- A T1-F interface cannot achieve the bandwidth because of extra costs of interframe filling tags. To improve the transmission rate of the T1-F interface, run the **ft1 itf number** command to set the number of interframe filling tags to 0.

Example

Set the interframe filling tag to 0xff on T1-F interface Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 itf type ff
```

5.9.12 ft1 loopback

Function

Using the **ft1 loopback** command, you can enable loopback detection on a T1-F interface.

Using the **undo ft1 loopback** command, you can restore the default setting.

By default, loopback detection is disabled.

Format

ft1 loopback { **local** | **payload** | **remote** }

undo ft1 loopback

Parameters

Parameter	Description	Value
local	Sets internal loopback.	-
payload	Sets payload loopback.	-
remote	Sets external loopback.	-

Views

T1-F interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function detects the interface status or cable status and must be disabled when devices work properly.

- In internal loopback mode, the local device loops back outgoing packets to itself to test whether it works properly.
- In payload loopback mode, the local device loops back the valid payload of outgoing packets to itself. Generally, the synchronization signals transmitted by timeslot 0 are not looped back to the local device.
- In external loopback mode, the local device loops back the packets received from its peer device to the peer device to test whether the link between the two devices works properly.

Example

Enable internal loopback detection on T1-F interface Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 loopback local
```

 Copyright © Huawei Technologies Co., Ltd.

5.9.13 ft1 timeslot-list

Function

Using the **ft1 timeslot-list** command, you can configure timeslot bundling on a T1-F interface.

Using the **undo ft1 timeslot-list** command, you can restore the default configuration.

By default, all timeslots of a T1-F interface are bundled. The default rate of a T1-F interface is 1536 kbit/s.

Format

ft1 timeslot-list *list* [**speed** { **56k** | **64k** }]

undo ft1 timeslot-list

Parameters

Parameter	Description	Value
list	Specifies the timeslot to be bundled.	*list* specifies the number of a timeslot, and its value ranges from 1 to 24. You can specify a single timeslot by using *number*, specify a timeslot range by using *number1-number2*, or specify multiple timeslots by using *number1,number2-number3*.
speed { **56k** | **64k** }	Specifies the speed of each timeslot, in kbit/s. When **56k** is specified, the speed of a channel set is *n* x 56 kbit/s. When **64k** is specified, the speed of a channel set is *n* x 64 kbit/s. *n* is the number of timeslots in a channel set. By default, the speed of each timeslot in a channel set is 64 kbit/s.	-

Views

T1-F Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After timeslots of a T1-F interface are bundled, the interface rate changes accordingly. For example, when 10 timeslots 1 through 10 of a T1-F interface are bundled, the interface rate changes to 10 x 64 kbit/s or 10 x 56 kbit/s. Timeslots of a T1-F interface can be bundled into only one channel, which is the synchronous serial interface of this T1-F interface.

Example

Bundle timeslots 1, 2, 3, 8, and 10 of T1-F 1/0/0 into a channel.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ft1 timeslot-list 1-3,8,10
```

Related Topics

5.9.2 display ft1

5.9.14 set workmode e1t1-f

Function

The **set workmode e1t1-f** command sets the working mode of a 1E1T1-F/2E1T1-F interface card.

By default, a 1E1T1-F/2E1T1-F interface card works in E1-F mode.

NOTE

The 4E1T1-F/8E1T1-F interface card only works in E1-F mode and does not support working mode switching.

Format

set workmode slot *slot-id* **e1t1-f** { **e1-f** | **t1-f** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a 1E1T1-F/2E1T1-F interface card.	Run the **display device** command to view slot IDs and types of interface cards and find the slot ID with E1/T1-F displayed. Then run the **display workmode** command to view the interface card work mode on the device.
e1-f	Indicates a 1E1T1-F/2E1T1-F interface card works in fractional channelized E1 (E1-F) mode.	-

Parameter	Description	Value
t1-f	Indicates a 1E1T1-F/2E1T1-F interface card works in fractional channelized T1 (T1-F) mode.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A 1E1T1-F interface card provides one fractional channelized E1/T1 interface and a 2E1T1-F interface card provides two fractional channelized E1/T1 interfaces. A 1E1T1-F/2E1T1-F interface card cannot both provide E1-F and T1-F interfaces. The **set workmode e1t1-f** command sets the working mode of a 1E1T1-F/2E1T1-F interface card.

Precautions

After this command is used, the system prompts you to reset the 1E1T1-F/2E1T1-F interface card to make the new working mode take effect. If you select **Yes**, the system resets the interface card. Otherwise, you need to run the **reset slot** command to manually reset the interface card to make the new working mode take effect.

Example

Configure the 2E1T1-F interface card in slot 1 to work in T1-F mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 e1t1-f t1-f
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

Related Topics

4.1.3 display device

5.5.9 display workmode

4.2.13 reset slot

5.10 E&M Interface Configuration Commands

5.10.1 display em clock-mode

Function

The **display em clock-mode** command displays the clock source mode of the 6E&M card.

Format

display em clock-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The 6E&M card is typically used for Very High Frequency (VHF) data transmission and uses the Time-Division Multiplexing (TDM) protocol. By default, the card uses the built-in clock as the clock source. When the card works in transparent transmission mode, bit errors occur in TDM transmission when the frequency offset exists between the clock of the card and the system clock of the device. By checking the working mode of the card's clock source, you can determine whether to configure the clock working mode for the card.

Example

Display the clock mode of the 6E&M card.

```
<Huawei> display em clock-mode
  Info: The 6E&M boards work in BOARD mode.
```

Table 5-32 Description of the **display em clock-mode** command output

Item	Description
Info: The 6E&M boards work in BOARD mode.	Clock mode of the 6E&M card. ● BOARD: uses the built-in clock source of the 6E&M card. ● SYSTEM: uses the system clock.

 Copyright © Huawei Technologies Co., Ltd.

5.10.2 em clock

Function

The **em clock** command sets the clock mode of a 6E&M card.

The **undo em clock** command restores the default setting.

By default, the clock mode of the 6E&M card is **board**.

Format

em clock { **system** | **board** }

undo em clock

Parameters

Parameter	Description	Value
system	Sets the clock mode of the 6E&M card to system clock mode.	-
board	Sets the clock mode of the 6E&M card to built-in clock mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 6E&M card is typically used for Very High Frequency (VHF) data transmission and uses the Time-Division Multiplexing (TDM) protocol. By default, the card uses the built-in clock as the clock source. When the card works in transparent transmission mode, bit errors occur in TDM transmission when the frequency offset exists between the clock of the card and the system clock of the device. To solve this problem, you need to configure the card to work in the system clock mode to eliminate the bit errors caused by the frequency offset of the clock source.

Precautions

If a router is directly connected to the 6E&M card of the peer device, you need to run the **em clock** command on both ends.

Clock synchronization channels (for example, connecting through E1 interfaces) are available between devices. Run the **fe1 clock system** command on the main E1 interface for clock synchronization to configure the interface to use the system clock mode. Run the **clock source** command on the peer device to configure the

 Copyright © Huawei Technologies Co., Ltd.

interface type of the clock source. Ensure that the clock sources of the devices at both ends are synchronized.

Example

Configure the 6E&M card to work in system clock mode. The main E1 interface for clock synchronization is Serial 4/0/0.

```
<Huawei> system-view
[Huawei] interface serial 4/0/0
[Huawei-Serial1/0/0] fe1 clock system
[Huawei-Serial1/0/0] quit
[Huawei] em clock system
```

5.10.3 em passthrough enable

Function

The **em passthrough enable** command enables data transparent transmission on an E&M interface.

The **undo em passthrough enable** command restores the default setting.

By default, data transparent transmission is disabled on an E&M interface.

Format

em passthrough enable

undo em passthrough enable

Parameters

None

Views

E&M interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before the data processing center and E&M terminal transmit E&M data, you must enable data transparent transmission on E&M interfaces so that routers can transparently transmit E&M data through the MPLS tunnel.

Prerequisites

TDM has been configured as the link-layer protocol of the E&M interface using the **link-protocol tdm** command.

Example

Enable data transparent transmission on E&M interface 2/0/0.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol tdm
[Huawei-Serial2/0/0] em passthrough enable
```

Related Topics

5.3.17 link-protocol tdm

5.10.4 em signal-mode

Function

The **em signal-mode** command sets the signaling mode of an E&M interface.

The **undo em signal-mode** command restores the default setting.

By default, the signaling mode of an E&M interface is Bell-5.

Format

em signal-mode { **bell-1** | **bell-2** | **bell-3** | **bell-4** | **bell-5** }

undo em signal-mode

Parameters

Parameter	Description	Setting
bell-1	Sets the signaling mode of an E&M interface to Bell-1. **NOTE** Currently, the device does not support the Bell-1 signaling mode.	-
bell-2	Sets the signaling mode of an E&M interface to Bell-2. **NOTE** Currently, the device does not support the Bell-2 signaling mode.	-
bell-3	Sets the signaling mode of an E&M interface to Bell-3. **NOTE** Currently, the device does not support the Bell-3 signaling mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Setting
bell-4	Sets the signaling mode of an E&M interface to Bell-4. **NOTE** Currently, the device does not support the Bell-4 signaling mode.	-
bell-5	Sets the signaling mode of an E&M interface to Bell-5.	-

Views

E&M interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a router connects to a device through an E&M interface, the signaling modes on the router and the device must be same so that data can be transmitted between them. You can configure the signaling mode of the E&M interface on the router based on that of the connected interface of the device.

Prerequisites

TDM has been configured as the link-layer protocol of the E&M interface using the **link-protocol tdm** command.

Example

Set the signaling mode of E&M interface 2/0/0 to Bell-5.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol tdm
[Huawei-Serial2/0/0] em signal-mode bell-5
```

Related Topics

5.3.17 link-protocol tdm

 Copyright © Huawei Technologies Co., Ltd.

5.10.5 em transmit gain

Function

The **em transmit gain** command configures the transmit signal gain level of an E&M interface.

The **undo em transmit gain** command restores the default configuration.

By default, the transmit signal gain level of an E&M interface is 14.

Format

em transmit gain *gain-level*

undo em transmit gain

Parameters

Parameter	Description	Value
gain-level	Specifies the transmit signal gain level of the E&M interface.	The value is an integer that ranges from 0 to 41. Different signal gain levels correspond to different signal gains. **Table 5-33** describes the mapping between the signal gain level and signal gain value.

Table 5-33 Mapping between the signal gain level and signal gain value

Gain Level	Gain Value
0	-7 dB
1	-6.5 dB
2	-6 dB
3	-5.5 dB
4	-5 dB
5	-4.5 dB
6	-4 dB
7	-3.5 dB
8	-3 dB
9	-2.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Gain Level	Gain Value
10	-2 dB
11	-1.5 dB
12	-1 dB
13	-0.5 dB
14	0 dB
15	0.5 dB
16	1 dB
17	1.5 dB
18	2 dB
19	2.5 dB
20	3 dB
21	3.5 dB
22	4 dB
23	4.5 dB
24	5 dB
25	5.5 dB
26	6 dB
27	6.5 dB
28	7 dB
29	7.5 dB
30	8 dB
31	8.5 dB
32	9 dB
33	9.5 dB
34	10 dB
35	10.5 dB
36	11 dB
37	11.5 dB
38	12 dB
39	12.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Gain Level	Gain Value
40	13 dB
41	13.5 dB

Views

E&M interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a local user and a remote user are on a call, you can run the **em transmit gain** command to configure the transmit signal gain level of the E&M interface to adjust the call volume.

- When the remote user feels that the call volume is low and the call quality is poor, you can run the **em transmit gain** command on the local E&M interface to increase the transmit signal gain level.
- When the remote user feels that the call volume is high and the call quality is good, you can run the **em transmit gain** command on the local E&M interface to reduce the transmit signal gain level.

Prerequisite

The TDM protocol has been configured as the data link layer protocol of the E&M interface using the **link-protocol tdm** command.

Example

Set the transmit signal gain level of the E&M interface to 20.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol tdm
[Huawei-Serial2/0/0] em transmit gain 20
```

Related Topics

5.3.17 link-protocol tdm

5.10.6 em receive gain

Function

The **em receive gain** command configures the receive signal gain level of an E&M interface.

The **undo em receive gain** command restores the default configuration.

By default, the receive signal gain level of an E&M interface is 40.

Format

em receive gain *gain-value*

undo em receive gain

Parameters

Parameter	Description	Value
gain-value	Specifies the receive signal gain level of the E&M interface.	The value is an integer that ranges from 0 to 43. Different signal gain levels correspond to different signal gains. **Table 5-34** describes the mapping between the signal gain level and signal gain value.

Table 5-34 Mapping between the signal gain level and signal gain value

Gain Level	Gain Value
0	-20 dB
1	-19.5 dB
2	-19 dB
3	-18.5 dB
4	-18 dB
5	-17.5 dB
6	-17 dB
7	-16.5 dB
8	-16 dB
9	-15.5 dB
10	-15 dB
11	-14.5 dB
12	-14 dB
13	-13.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Gain Level	Gain Value
14	-13 dB
15	-12.5 dB
16	-12 dB
17	-11.5 dB
18	-11 dB
19	-10.5 dB
20	-10 dB
21	-9.5 dB
22	-9 dB
23	-8.5 dB
24	-8 dB
25	-7.5 dB
26	-7 dB
27	-6.5 dB
28	-6 dB
29	-5.5 dB
30	-5 dB
31	-4.5 dB
32	-4 dB
33	-3.5 dB
34	-3 dB
35	-2.5 dB
36	-2 dB
37	-1.5 dB
38	-1 dB
39	-0.5 dB
40	0 dB
41	0.5 dB
42	1 dB
43	1.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Views

E&M interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a local user and a remote user are on a call, you can run the **em receive gain** command to configure the receive signal gain level of the E&M interface to adjust the call volume.

- When the local user feels that the call volume is low and the call quality is poor, you can run the **em receive gain** command on the local E&M interface to increase the receive signal gain level.
- When the local user feels that the call volume is high and the call quality is good, you can run the **em receive gain** command on the local E&M interface to reduce the receive signal gain level.

Prerequisite

The TDM protocol has been configured as the data link layer protocol of the E&M interface using the **link-protocol tdm** command.

Example

Set the receive signal gain level of the E&M interface to 20.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol tdm
[Huawei-Serial2/0/0] em receive gain 20
```

Related Topics

5.3.17 link-protocol tdm

5.10.7 em pcm

Function

The **em pcm** command configures the companding algorithm of pulse code modulation (PCM).

The **undo em pcm** command restores the default configuration.

By default, the PCM companding algorithm is A-law algorithm.

 Copyright © Huawei Technologies Co., Ltd.

Format

em pcm { **a-law** | **u-law** }

undo em pcm

Parameters

Parameter	Description	Value
a-law	Specifies the A-law algorithm.	-
u-law	Specifies the u-law algorithm.	-

Views

E&M interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are two pulse code modulation (PCM) companding algorithms: A-law algorithm and u-law algorithm. The A-law algorithm is mainly used in digital communication systems of Europe and China. The u-law algorithm is mainly used in digital communication systems of North America and Japan.

Choose the PCM companding algorithm based on the standard used locally.

Prerequisite

The TDM protocol has been configured as the data link layer protocol of the E&M interface using the **link-protocol tdm** command.

Example

Set the PCM companding algorithm to the u-law algorithm.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol tdm
[Huawei-Serial2/0/0] em pcm u-law
```

Related Topics

5.3.17 link-protocol tdm

5.11 Cellular Interface Configuration Commands

NOTE

Cellular interfaces are classified into 3G cellular interfaces and LTE cellular interfaces.

Cellular channel interfaces are classified into 3G channel interfaces and LTE channel interfaces.

5.11.1 apn

Function

The **apn** command configures an APN in the APN profile.

The **undo apn** command deletes the configured APN from the APN profile.

By default, no APN is configured in the APN profile. During LTE dial-up, apn profile name specifies an access point name (APN) user name.

Format

apn *apn-name*

undo apn

Parameters

Parameter	Description	Value
apn-name	Specifies the name of the APN.	The value is a string of 1 to 99 case-sensitive characters without spaces.

Views

APN profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An access point name (APN) identifies an external PDN network (for example, the Internet or IMS network) that users want to access.

You can run the **apn** command to configure an APN in the APN profile.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- APNs are provided by the carrier.
- After an APN is configured, it is permanently recorded in a 3G or LTE modem. If the APN changes, reconfigure it.
- If the **apn** command is run repeatedly in the same APN profile view, the latest configuration overwrites the earlier ones.

Example

Configure an APN named **3gnet** in the APN profile.

```
<Huawei> system-view
[Huawei] apn profile 3gprofile
[Huawei-apn-profile-3gprofile] apn 3gnet
```

Related Topics

5.11.2 apn profile

5.11.2 apn profile

Function

The **apn profile** command creates an APN profile and displays the APN profile view.

The **undo apn profile** command deletes the created APN profile.

By default, no APN profile is created.

Format

apn profile *profile-name*

undo apn profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the APN profile.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can create an APN profile and configure an APN in the profile so that you can access external PDN networks using the configured APN.

If no APN profile is created, the device dynamically configures an APN.

Example

Configure the APN profile named **3gprofile** and enter the APN profile view.

```
<Huawei> system-view
[Huawei] apn profile 3gprofile
[Huawei-apn-profile-3gprofile]
```

Related Topics

5.11.3 apn-profile

5.11.67 user

5.11.3 apn-profile

Function

The **apn-profile** command binds an APN profile to a cellular interface or cellular channel interface.

The **undo apn-profile** command deletes the APN profile bound to a cellular interface or cellular channel interface.

By default, no APN profile is bound to a cellular interface or cellular channel interface.

Format

apn-profile *profile-name* [**priority** *priority*] [**track nqa** { *admin-name test-name* } &<1-2>]

undo apn-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the APN profile.	The value is a string of 1 to 64 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
priority *priority*	Specifies the priority of the APN profile.	The value is an integer that ranges from 1 to 255. The default value is 100. A larger value indicates a higher priority. When dual SIM cards are available, two APN profiles can be bound to an LTE cellular interface or LTE channel interface. The APN profile with a higher priority can access the LTE network first. You are advised to set the priority of the APN profile bound to the master SIM card to higher than that of the APN profile bound to the backup SIM card.
track nqa *admin-name test-name*	Specifies the administrator and name of an NQA test instance. If this parameter is specified, the device performs an NQA probe on the 3G or LTE network when the dial-up initiated through a cellular interface or cellular channel interface succeeds. The device terminates the 3G or LTE link after three consecutive NQA probe failures. Additionally, you can run the **dialer timer probe-interval** command to set the NQA probe interval. **NOTE** The NQA test instance type must be ICMP test. To specify this parameter, configure an NQA test instance and ensure that the route from the NQA test instance to the destination is reachable.	The value is a string of 1 to 32 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view, Cellular channel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring an APN profile, you must bind the APN profile to a cellular interface or cellular channel interface so that the APN profile configuration takes effect on the cellular interface or cellular channel interface.

Prerequisites

Run the **dialer enable-circular** command to enable the circular DCC (C-DCC) function.

Precautions

After an APN profile is bound to a cellular interface or cellular channel interface, run the **shutdown** and **undo shutdown** commands or the **restart** command to restart the interface so that the configurations can take effect.

Example

Bind the APN profile 3Gnet to the cellular interface.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] dialer enable-circular
[Huawei-Cellular0/0/0] apn-profile 3Gnet
[Huawei-Cellular0/0/0] shutdown
[Huawei-Cellular0/0/0] undo shutdown
```

Related Topics

5.11.2 apn profile

5.11.4 apn user name catch-imsi-sn

Function

The **apn user name catch-imsi-sn** command enables the function of carrying the IMSI and SN in an APN user name.

The **undo apn user name catch-imsi-sn** command disables the function of carrying the IMSI and SN in an APN user name.

By default, the function of carrying the IMSI and SN in an APN user name is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

apn user name catch-imsi-sn

undo apn user name catch-imsi-sn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a device connects to the Agile Controller-Campus, the Agile Controller-Campus allocates an IP address to the device based on the IMSI of the SIM card and the SN of the device. You can run the **apn user name catch-imsi-sn** command to enable the function of carrying the IMSI and SN in an APN user name, so that the device uses the APN user name carrying the IMSI and SN for LTE dialup to obtain an IP address from the Agile Controller-Campus.

Example

Enable the function of carrying the IMSI and SN in an APN user name.

```
<Huawei> system-view
[Huawei] apn user name catch-imsi-sn
```

Related Topics

5.11.24 imsi check

5.11.5 band gsm

Function

The **band auto** command deletes the configured frequency band of the GSM/WCDMA network and then LTE cellular interfaces can automatically select a frequency band to connect to the GSM/WCDMA network.

Format

band auto

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The networks of network carriers can provide multiple frequency bands for user access. To delete the configured frequency band of the network so that cellular interfaces can automatically select a frequency band, run the **band auto** command.

Precautions

- This command is valid only when the 3G modem is installed.
- When the network signal is weak, a modem is automatically migrated to another network for normal operation..

Example

Delete the configured frequency band of the network.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] band auto
```

5.11.6 band gsm

Function

The **band gsm** command sets the frequency band of the GSM network that 3G cellular interfaces are connected to.

By default, 3G cellular interfaces automatically select a frequency band to connect to the GSM network.

Format

band gsm { **gsm1800** | **gsm1900** | **gsm850** | **gsm900** }*

Parameters

Parameter	Description	Value
gsm1800	Indicates that the GSM network that 3G cellular interfaces are connected to works at the 1800 MHz frequency.	-

Parameter	Description	Value
gsm1900	Indicates that the GSM network that 3G cellular interfaces are connected to works at the 1900 MHz frequency.	-
gsm850	Indicates that the GSM network that 3G cellular interfaces are connected to works at the 850 MHz frequency.	-
gsm900	Indicates that the GSM network that 3G cellular interfaces are connected to works at the 900 MHz frequency.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

GSM networks of network carriers can provide multiple frequency bands for user access. When the frequency band of a GSM network changes after 3G cellular interfaces are connected to the GSM network, the 3G modem automatically adjusts the frequency band accordingly, which affects stability of 3G links.

When the frequency band of a GSM network that you access is fixed, you can run the **band gsm** command to set the frequency band of the GSM network that 3G cellular interfaces are connected to. This prevents frequency band changes caused by frequency interference and ensures 3G link stability.

Precautions

- This command is valid only when the 3G modem is installed.
- Run the **display cellular** *interface-number* **network** command to view the **Current Network Connection** field and check whether 3G cellular interfaces are connected to the GSM network.
- Confirm the frequency band of the GSM network in your location with the GSM network carrier to set the optimal frequency band.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the GSM network to which 3G cellular interfaces are connected to work at the 1800 MHz frequency and 900 MHz frequency.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] band gsm gsm1800 gsm900
```

Related Topics

5.11.17 display cellular

5.11.7 band wcdma

5.11.7 band wcdma

Function

The **band wcdma** command sets the frequency band of the WCDMA network that 3G cellular interfaces are connected to.

By default, 3G cellular interfaces automatically select a frequency band to connect to the WCDMA network.

Format

band wcdma { **wcdma1900** | **wcdma2100** | **wcdma850** | **wcdma900** | **AWS** | **wcdma1700** }*

Parameters

Parameter	Description	Value
wcdma1700	Indicates that the WCDMA network that 3G cellular interfaces are connected to works at the 1700 MHz frequency.	-
wcdma1900	Indicates that the WCDMA network that 3G cellular interfaces are connected to works at the 1900 MHz frequency.	-
wcdma2100	Indicates that the WCDMA network that 3G cellular interfaces are connected to works at the 2100 MHz frequency.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wcdma850	Indicates that the WCDMA network that 3G cellular interfaces are connected to works at the 850 MHz frequency.	-
wcdma900	Indicates that the WCDMA network that 3G cellular interfaces are connected to works at the 900 MHz frequency.	-
AWS	Indicates that the WCDMA network that 3G cellular interfaces are connected to works at the 1700/2100 (US) MHz frequency.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WCDMA networks of network carriers can provide multiple frequency bands for user access. When the frequency band of a WCDMA network changes after 3G cellular interfaces are connected to the WCDMA network, the 3G modem automatically adjusts the frequency band accordingly, which affects stability of 3G links.

When the frequency band of a WCDMA network that you access is fixed, you can run the **band wcdma** command to set the frequency band of the WCDMA network that 3G cellular interfaces are connected to. This prevents frequency band changes caused by frequency interference and ensures 3G link stability.

Precautions

- This command is valid only when the 3G modem is installed.
- Run the **display cellular** *interface-number* **network** command to view the **Current Network Connection** field and check whether 3G cellular interfaces are connected to the WCDMA network.
- Confirm the frequency band of the WCDMA network in your location with the WCDMA network carrier to set the optimal frequency band.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the WCDMA network to which 3G cellular interfaces are connected to work at the 1900 MHz frequency and 900 MHz frequency.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] band wcdma wcdma1900 wcdma900
```

Related Topics

5.11.17 display cellular

5.11.6 band gsm

5.11.8 band lte

Function

The **band lte** command allows you to manually set the frequency band of the LTE network that LTE cellular interfaces are connected to.

By default, LTE cellular interfaces automatically select a frequency band to connect to the LTE network.

Format

band lte { **band1** | **band2** | **band3** | **band4** | **band5** | **band7** | **band8** | **band12** | **band13** | **band17** | **band18** | **band19** | **band20** | **band26** | **band28** | **band34** | **band38** | **band39** | **band40** | **band41** }*

Parameters

Parameter	Description	Value
band1	Indicates that the frequency band of the LTE network is Band 1 (transmit: 1920 MHz to 1980 MHz; receive: 2110 MHz to 2170 MHz).	-
band2	Indicates that the frequency band of the LTE network is Band 2 (transmit: 1850 MHz to 1910 MHz; receive: 1930 MHz to 1990 MHz).	-
band3	Indicates that the frequency band of the LTE network is Band 3 (transmit: 1710 MHz to 1785 MHz; receive: 1805 MHz to 1880 MHz).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
band4	Indicates that the frequency band of the LTE network is Band 4 (transmit: 1710 MHz to 1755 MHz; receive: 2110 MHz to 2155 MHz).	-
band5	Indicates that the frequency band of the LTE network is Band 5 (transmit: 824 MHz to 849 MHz; receive: 869 MHz to 894 MHz).	-
band7	Indicates that the frequency band of the LTE network is Band 7 (transmit: 2500 MHz to 2570 MHz; receive: 2620 MHz to 2690 MHz).	-
band8	Indicates that the frequency band of the LTE network is Band 8 (transmit: 880 MHz to 915 MHz; receive: 925 MHz to 960 MHz).	-
band13	Indicates that the frequency band of the LTE network is Band 13 (transmit: 777 MHz to 787 MHz; receive: 746 MHz to 756 MHz).	-
band17	Indicates that the frequency band of the LTE network is Band 17 (transmit: 704 MHz to 716 MHz; receive: 734 MHz to 746 MHz).	-
band18	Indicates that the frequency band of the LTE network is Band 8 (transmit: 815 MHz to 830 MHz; receive: 860 MHz to 875 MHz).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
band19	Indicates that the frequency band of the LTE network is Band 17 (transmit: 830 MHz to 845 MHz; receive: 860 MHz to 875 MHz).	-
band20	Indicates that the frequency band of the LTE network is Band 20 (transmit: 832 MHz to 862 MHz; receive: 791 MHz to 821 MHz).	-
band26	Indicates that the frequency band of the LTE network is Band 28 (transmit: 816 MHz to 849 MHz; receive: 859 MHz to 894 MHz).	-
band28	Indicates that the frequency band of the LTE network is Band 28 (transmit: 703 MHz to 748 MHz; receive: 758 MHz to 803 MHz).	-
band38	Indicates that the frequency band of the LTE network ranges from 2570 MHz to 2620 MHz.	-
band39	Indicates that the frequency band of the LTE network ranges from 1880 MHz to 1920 MHz.	-
band40	Indicates that the frequency band of the LTE network ranges from 2300 MHz to 2400 MHz.	-
band41	Indicates that the frequency band of the LTE network ranges from 2496 MHz to 2690 MHz.	-

Views

Cellular interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LTE networks of network carriers can provide multiple frequency bands for user access. When the frequency band of an LTE network changes after LTE cellular interfaces are connected to the LTE network, the LTE modem automatically adjusts the frequency band accordingly, which affects stability of LTE links.

When the frequency band of an LTE network that you access is fixed, you can manually run the **band lte** command to set the frequency band of the LTE network that LTE cellular interfaces are connected to. This prevents frequency band changes caused by frequency interference and ensures LTE link stability.

Precautions

- This command is valid only when the LTE modem is installed.
- Run the **display cellular** *interface-number* **network** command to view the **Current Network Connection** field and check whether LTE cellular interfaces are connected to the LTE network.
- Confirm the frequency band of the LTE network in your location with the LTE network carrier to set the optimal frequency band.

Example

Manually configure the LTE network to which LTE cellular interfaces are connected to work at the Band 1 frequency.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] band lte band1
```

Related Topics

5.11.17 display cellular

5.11.6 band gsm

5.11.7 band wcdma

5.11.9 cellular log enable

Function

The **cellular log enable** command enables the WWAN log function.

The **undo cellular log enable** command disables the WWAN log function.

By default, the WWAN log function is disabled.

Format

cellular log enable

undo cellular log enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To view changes of the signal strength, cell ID, or network type in WWAN logs, you can run the **cellular log enable** command to enable the WWAN log function.

- When the 3G signal strength changes, the device records the WWAN/5/WWAN_RSSI_NORMAL log or the WWAN/5/WWAN_RSSI_WEAK log.
- When the 3G signal strength changes, the device records the WWAN/5/WWAN_SINR_NORMAL log or WWAN/5/WWAN_SINR_WEAK log.
- When the cell ID changes, the device records the WWAN/5/WWAN_CELLID log.
- When the network type changes, the device records the WWAN/5/WWAN_NETWORK log.
- When Cellular interface received a network reject code, the device records the WWAN/5/WWAN_NETWORK_REJECT_CAUSE log.

Example

Enable the WWAN log function.

```
<Huawei> system-view
[Huawei] cellular log enable
```

5.11.10 cellular log rssi-threshold

Function

The **cellular log rssi-threshold** command configures the received signal strength indicator (RSSI) threshold used for determining the 3G signal strength.

The **undo cellular log rssi-threshold** command restores the RSSI threshold used for determining the 3G signal strength to the default value.

By default, the RSSI threshold used for determining the 3G signal strength is -89 dBm.

Format

cellular log rssi-threshold *rssi-threshold*

undo cellular log rssi-threshold

Parameters

Parameter	Description	Value
rssi-threshold	Specifies the RSSI threshold used for determining the 3G signal strength. ● If the strength of received 3G signals is greater than the RSSI threshold 10 consecutive times, and the signal strength becomes normal, the device records the **WWAN/5/WWAN_RSSI_NORMAL** log. ● If the strength of received 3G signals is not greater than the RSSI threshold 10 consecutive times, and the signal strength becomes weak, the device records the **WWAN/5/WWAN_RSSI_WEAK** log.	The value is a negative integer that ranges from -110 to -60, in dBm.

Views

System View

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

You can run the **cellular log enable** command to enable the WWAN log function and view the 3G signal strength change in WWAN logs. You can run the **cellular log rssi-threshold** command to configure the RSSI threshold used for determining the 3G signal strength. The device records the signal strength change in logs based on the RSSI threshold.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After enabling the WWAN log function using the **cellular log enable** command, run the **cellular log rssi-threshold** command to configure the device to record logs based on the configured RSSI threshold.

Example

Set the RSSI threshold of the 3G signal strength to -80 dBm.

```
<Huawei> system-view
[Huawei] cellular log enable
[Huawei] cellular log rssi-threshold 80
```

Related Topics

5.11.9 cellular log enable

5.11.11 cellular log sinr-threshold

Function

The **cellular log sinr-threshold** command sets the signal to interference plus noise ratio (SINR) threshold used to determine the LTE signal strength.

The **undo cellular log sinr-threshold** command restores the default SINR threshold used to determine the LTE signal strength.

By default, the SINR threshold used to determine the LTE signal strength is 10 dB.

Format

cellular log sinr-threshold *sinr-threshold*

undo cellular log sinr-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
sinr-threshold	Sets the SINR threshold used to determine the LTE signal strength. • If the strength of received LTE signals is greater than the SINR threshold 10 consecutive times, and the signal strength becomes normal, the device records the **WWAN/5/WWAN_SINR_NORMAL** log. • If the strength of received LTE signals is not greater than the SINR threshold 10 consecutive times, and the signal strength becomes weak, the device records the **WWAN/5/WWAN_SINR_WEAK** log.	The value is an integer that ranges from 0 to 30, in dB.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the LTE signal strength change in logs, run the **cellular log enable** command to enable the WWAN log function first. You can then run the **cellular log sinr-threshold** command to set the SINR threshold used to determine the LTE signal strength. The device then records signal strength change logs based on the configured threshold.

Precautions

After the WWAN log function is enabled using the **cellular log enable** command, the device records logs based on the SINR threshold configured using the **cellular log sinr-threshold** command.

Example

Set the SINR threshold used to determine the LTE signal strength to 15 dB.

```
<Huawei> system-view
[Huawei] cellular log enable
[Huawei] cellular log sinr-threshold 15
```

Related Topics

5.11.9 cellular log enable

5.11.12 dialer mode ppp

Function

The **dialer mode ppp** command configures the PPP dial-up mode for the LTE modem to connect to a 3G or an LTE network.

The **undo dialer mode** command restores the default dial-up mode for the LTE modem to connect to a 3G or an LTE network.

By default, the LTE modem uses the standard interface defined in the network diver interface specification to connect to a 3G or an LTE network.

NOTE

Only routers with the built-in ME906E and ME909s-120 modules support this command.

Format

dialer mode ppp

undo dialer mode

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

By default, the LTE modem uses the standard interface defined in the network diver interface specification to connect to a 3G or an LTE network. If the carrier's

device only supports the PPP dial-up mode for 3G/LTE network access, you must run the **dialer mode ppp** command to set the dial-up mode to PPP.

Example

Configure the PPP dial-up mode for the LTE modem to connect to a 3G or an LTE network.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] dialer mode ppp
modem reboot for changing modem dialer mode
```

5.11.13 dialer timer probe-interval

Function

The **dialer timer probe-interval** command sets the NQA probe interval for a cellular interface or cellular channel interface.

The **undo dialer timer probe-interval** command restores the default NQA probe interval.

By default, the NQA probe interval of a cellular interface or cellular channel interface is 60 seconds.

Format

dialer timer probe-interval *interval*

undo dialer timer probe-interval

Parameters

Parameter	Description	Value
interval	Specifies the NQA probe interval for a cellular interface or cellular channel interface.	The value is an integer that ranges from 1 to 60, in seconds.

Views

Cellular interface view, Cellular channel interface view

Default Level

2: Configuration level

Usage Guidelines

You are advised to set the NQA probe interval to be the same as the interval for automatically performing an NQA test instance. The later interval is set using the **frequency** command.

Example

Set the NQA probe interval of a cellular interface to 50 seconds.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] dialer enable-circular
[Huawei-Cellular0/0/0] dialer timer probe-interval 50
```

Related Topics

5.11.3 apn-profile

5.11.14 dialer-number (APN view)

Function

The **dialer-number** command configures a dialer number for the APN to dial up the remote device.

The **undo dialer-number** command deletes the dialer number for the APN to dial up the remote device.

By default, the dialer number for dialing up the remote device is not configured.

Format

dialer-number *dial-number*

undo dialer-number *dial-number*

Parameters

Parameter	Description	Value
dial-number	Specifies the dialer number.	The value is a string of 1 to 32 case-insensitive characters.

Views

APN view

Default Level

2: Configuration level

Usage Guidelines

When a device performs LTE dialup and the APN needs to dial up a destination address, you can run the dialer-number command to configure a dialer number.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a dialer number for an APN.

```
<Huawei> system-view
[Huawei] apn profile me906
[Huawei-apn-profile-me906] dialer-number *99#
```

5.11.15 display apn-profile configuration

Function

The **display apn-profile configuration** command displays the APN profile configurations.

Format

display apn-profile configuration [*apn-profile-number*]

Parameters

Parameter	Description	Value
apn-profile-number	Specifies the number of APN profiles. ● If this parameter is specified, the APN profile configurations are displayed according to the sequence in which the APN profiles are configured. ● If this parameter is not specified, the configurations of all APN profiles are displayed.	The value is an integer that ranges from 1 to 128.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to check the configurations of the existing APN profiles on the device.

Example

Display configurations of all APN profiles.

```
<Huawei> display apn-profile configuration
--------------------------------------------------------------------------------
profile-name       :unicom
apn               :ltenet1
user-name          :user1
authentication-mode:chap
sim-id            :1
--------------------------------------------------------------------------------
profile-name       :telcom
apn               :ltenet2
user-name          :user2
authentication-mode:auto
sim-id            :2
```

Table 5-35 Description of the display apn-profile configuration command output

Item	Description
profile-name	Name of an APN profile. To create an APN profile and enter the APN profile view, run the **apn profile** command.
apn	Name of an APN. To configure an APN in the APN profile, run the **apn** command.
user-name	User name for accessing an external PDN network. To configure the user name for accessing an external PDN network, run the **user** command.
authentication-mode	Authentication mode for accessing an external PDN network. ● **auto**: PAP or CHAP authentication ● **pap**: PAP authentication ● **chap**: CHAP authentication To configure the authentication mode for accessing an external PDN network, run the **user** command and specify the **authentication-mode** parameter. When the **authentication-mode** parameter is not specified, the **auto** mode is used by default.
sim-id	ID of a SIM card. To configure a SIM card ID in the APN profile, run the **sim-id** command. **NOTE** The dual-SIM functions can be configured only on the LTE cellular interface (Cellular 0/0/0) supported by the AR109GW-L, AR121GW-L, AR129GW-L, AR129CGVW-L, AR161FG-Lc, AR161FG-L, AR169FGW-L, AR169FGVW-L, AR169G-L, AR169EGW-L, AR161G-L, AR161G-Lc, AR161FGW-La, AR161FGW-Lc, and AR161FGW-L.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

5.11.2 apn profile
5.11.1 apn
5.11.67 user
5.11.56 sim-id

5.11.16 diagnostics-monitor-port on

Function

The **diagnostics-monitor-port on** command enables the MiniUSB interface on the 3G/LTE card.

The **undo diagnostics-monitor-port on** command disables the MiniUSB interface on the 3G/LTE card.

By default, the MiniUSB interface on the 3G/LTE card is disabled.

Format

diagnostics-monitor-port on

undo diagnostics-monitor-port on

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **diagnostics-monitor-port on** command enables the MiniUSB interface on the 3G/LTE card, you can use the PC to implement Internet access through dialup or upgrade the 3G/LTE module. The PC can connect to the MiniUSB interface on the 3G/LTE card through the USB line.

Precautions

- The original 3G/LTE service is interrupted after the **diagnostics-monitor-port on** command is run.
- The firmware version of the 3G/LTE modem cannot be upgraded after the **diagnostics-monitor-port on** command is run.
- If the device or 3G/LTE card is reset, the **diagnostics-monitor-port on** command cannot take effect. You must reconfigure the command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the MiniUSB interface on the 3G/LTE card.

```
<Huawei> system-view
[Huawei] interface cellular 1/0/0
[Huawei-Cellular1/0/0] diagnostics-monitor-port on
```

5.11.17 display cellular

Function

The **display cellular** command displays information about call sessions on a 3G or an LTE modem.

Format

display cellular *interface-number* { **all** | **hardware** | **security** | **network** | **profile** | **radio** }

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface.	-
all	Displays all information about call sessions on a 3G or an LTE modem. The information involves hardware, parameter description profile, network, radio, and security.	-
hardware	Displays hardware information about a 3G or an LTE modem.	-
security	Displays security information about a 3G or an LTE modem.	-
network	Displays network information about a 3G or an LTE modem.	-
profile	Displays parameter profile information about a 3G or an LTE modem.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
radio	Displays radio information about a 3G or an LTE modem.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display cellular** command displays information about call sessions on a 3G or an LTE modem, including the 3G or LTE modem's hardware information, parameter profile information, network information, radio information, security information or all the preceding information.

Example

Display all information about call sessions on a 3G modem.

```
<Huawei> display cellular 0/0/0 all
Modem State:
Hardware Information.
=====================
Model = E372
Modem Type = WCDMA modem
Modem Firmware Version = 11.870.02.10.11
Hardware Version = CP12TCPU
Integrate circuit card identity (ICCID) = 98681011274300909893
International Mobile Subscriber Identity (IMSI) = 460016002707237
Mobile Station International ISDN Number (MSISDN) = 86013987654321
International Mobile Equipment Identity (IMEI) = 354661034412719
Factory Serial Number (FSN) = MLA7NA1093003693
Modem Status = Online
Profile Information.
====================
Profile 1 = ACTIVE
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = 3GNET
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = Combined
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Home
Network Selection Mode = Automatic
Network Connection Mode = WCDMA precedence
Current Network Connection = WCDMA(WCDMA)
Mobile Country Code (MCC) = 460
```

```
Mobile Network Code (MNC) = 01
Mobile Operator Information = "CHN-CUGSM"
Location Area Code (LAC) = 53505
Cell ID = 6012
Upstream Bandwidth = 54kbps
Downstream Bandwidth = 384kbps
Radio Information.
==================
Current Bands : AUTO
Current RSSI = -55 dBm (good)

Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

Display all information about call sessions (connected to the LTE network) on an LTE modem.

```
<Huawei> display cellular 0/0/0 all
Modem State:
Hardware Information.
=====================
Model = ME906E
Modem Type = LTE module
Modem Firmware Version =  11.833.15.00.000
Hardware Version = CD2E392UM
Integrate circuit card identity (ICCID) = 98681011274300909893
International Mobile Subscriber Identity (IMSI) = 460016002731442
Mobile Station International ISDN Number (MSISDN) = 86013987654321
International Mobile Equipment Identity (IMEI) = 861230010006485
Factory Serial Number (FSN) = T2Y01A9211900298
Modem Status = Online
Profile Information.
====================
Profile 1 = ACTIVE
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = LTENET
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = Combined
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Home
Network Selection Mode = Automatic
Network Connection Mode =  LTE only
Current Network Connection = LTE(LTE)
Mobile Country Code (MCC) = 460
Mobile Network Code (MNC) = 07
Mobile Operator Information = CHINA  MOBILE
Cell ID = 55924
Upstream Bandwidth = 50mbps
Downstream Bandwidth = 100mbps
Radio Information.
==================
Current Bands :
  GSM: GSM1800
  WCDMA: AUTO
  LTE: AUTO
Current RSSI = -55 dBm
Current RSRP = -86 dBm (strong)
```

```
Current RSRQ = -6 dB
Current SINR = 29 dB
Bands supported :
  GSM: GSM850 GSM900 GSM1800 GSM1900
  WCDMA: WCDMA850 WCDMA900 WCDMA2100 WCDMA1900
  LTE: LTE900 LTE2100
Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

Display all information about call sessions (connected to the WCDMA network) on an LTE modem.

```
<Huawei> display cellular 0/0/0 all
Modem State:
Hardware Information.
=====================
Model = ME906E
Modem Type = LTE module
Modem Firmware Version =  11.833.15.00.000
Hardware Version = CD2E392UM
Integrate circuit card identity (ICCID) = 98681011274300909893
International Mobile Subscriber Identity (IMSI) = 460016002731442
Mobile Station International ISDN Number (MSISDN) = 86013987654321
International Mobile Equipment Identity (IMEI) = 861230010006485
Factory Serial Number (FSN) = T2Y01A9211900298
Modem Status = Online
Profile Information.
====================
Profile 1 = ACTIVE
--------
PDP Type = IPv4, Header Compression = OFF
Data Compression = OFF
Access Point Name (APN) = LTENET
Packet Session Status = Active
* - Default profile
Network Information.
====================
Current Service Status = Service available
Service Domain = PS-only
Current Service =  PS
Packet Service = Attached
Packet Session Status = Active
Current Roaming Status = Home
Network Selection Mode = Automatic
Network Connection Mode = WCDMA only
Current Network Connection = WCDMA(WCDMA)
Mobile Country Code (MCC) = 460
Mobile Network Code (MNC) = 07
Mobile Operator Information = CHINA  MOBILE
Location Area Code (LAC) = 53515
Cell ID = 55924
Upstream Bandwidth = 50kbps
Downstream Bandwidth = 384kbps
Radio Information.
==================
Current Bands :
  GSM: GSM1800
  WCDMA: AUTO
  LTE: AUTO
Current RSSI = -55 dBm (good)
Current RSCP = -47 dBm
Current ECIO = 0 dB
Bands supported :
  GSM: GSM850 GSM900 GSM1800 GSM1900
  WCDMA: WCDMA850 WCDMA900 WCDMA2100 WCDMA1900
```

```
 LTE: LTE900 LTE2100
Modem Security Information.
===========================
SIM ID = 1
PIN Verification = Disabled
PIN Status = Ready
Number of Retries remaining = 3
SIM Status = OK
```

Display network information about a 3G or an LTE modem.

```
<Huawei> display cellular 0/0/0 network
Modem State:
Network Information.
====================
Current Service Status = Service available
Service Domain = Combined
Current Service = Combined
Packet Service = Attached
Packet Session Status = Inactive
Current Roaming Status = Home
Network Selection Mode = Automatic
Network Connection Mode = WCDMA precedence
Current Network Connection = WCDMA(WCDMA)
Mobile Country Code (MCC) = 460
Mobile Network Code (MNC) = 01
Mobile Operator Information = CHN-UNICOM
Location Area Code (LAC) = 53515
Cell ID = 55924
Upstream Bandwidth = 54kbps
Downstream Bandwidth = 384kbps
```

Table 5-36 Description of the **display cellular** command output

Item	Description
Modem State	Status of the 3G or LTE modem.
Hardware Information	Information about the 3G or LTE modem hardware.
Model	Model of the 3G or LTE modem.
Modem Type	Modular type of the 3G or LTE modem. The displayed modular type consists of the modular standard type and modular physical type. The modular standard types are as follows: ● WCDMA: indicates the WCDMA standard. ● CDMA2000: indicates the CDMA2000 standard. ● LTE: indicates the LTE standard.
Modem Firmware Version	Firmware version of the 3G or LTE modem.
Hardware Version	Hardware version of the 3G or LTE modem.
Integrate circuit card identity (ICCID)	Integrate circuit card identity of the 3G or LTE modem.
International Mobile Subscriber Identity (IMSI)	International Mobile Subscriber Identity (IMSI) allocated to the user.

Item	Description
Mobile Station International ISDN Number (MSISDN)	Mobile Station International ISDN Number (MSISDN).
International Mobile Equipment Identity (IMEI)	International Mobile Equipment Identity (IMEI) of the 3G or LTE modem.
Factory Serial Number (FSN)	Factory serial number (FSN) of the 3G or LTE modem.
Modem Status	Whether the 3G or LTE modem is online: ● Online: indicates that the modem is online. ● Offline: indicates that the modem is offline.
Profile Information	Information about the parameter profile configured for the 3G or LTE modem.
Profile 1	Status of profile 1: ● Active: indicate the active status. ● Inactive: indicate the inactive status.
PDP Type	Packet data protocol (PDP) type: ● IPv4: indicates IPv4 packets. ● PPP: indicates PPP packets.
Header Compression	Whether IP header compression is enabled: ● On: IP header compression is enabled. ● OFF: IP header compression is disabled.
Data Compression	Whether IP packet data compression is enabled: ● On: IP packet data compression is enabled. ● OFF: IP packet data compression is disabled.
Access Point Name (APN)	APN that the carrier allocated to the 3G or LTE modem. To set an APN, run the **apn** command in the APN profile view.
Packet Session Status	Session status: ● Active: indicates that data is transmitted properly. ● Inactive: indicates that data transmission is interrupted.
Default profile	Default parameter profile, profile 1.
Network Information	Information about the network connected to the 3G or LTE modem.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current Service Status	Service status of the 3G or LTE modem: ● Service available: The 3G or LTE modem is providing services. ● No service: No service is available on the 3G or LTE modem. ● Emergency: The 3G or LTE modem provides services only for emergency use. ● Region emergency: The 3G or LTE modem provides services only for emergency use in a region. ● Saving status: The 3G or LTE modem is working in power-saving mode.
Service Domain	Configured PS or CS domain: ● PS-only: The modem works only in the PS domain. ● Combined: The modem works in both the CS domain and PS domain. This parameter can be configured using the **service domain** command.
Current Service	Service type: ● CS: Only the circuit switching (CS) service is available. ● PS: Only the packet switching (PS) service is available. ● Combined: Both the PS and CS services are available. ● Not support CDMA: CDMA does not support the service. ● Invalid: Neither the CS service nor the PS service has been registered.
Packet Service	Relationship between the 3G or LTE modem and the PS domain: ● Attached: The 3G or LTE modem is attached to the PS domain. ● Detached: The 3G or LTE modem is detached from the PS domain.
Current Roaming Status	Roaming status of the user: ● Home: The user is in the home location. ● Roaming: The user is roaming.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Network Selection Mode	Method used to select a public land mobile network (PLMN): ● Automatic: indicates automatic network selection. ● Manual: indicates manual network selection. This parameter can be configured using the **plmn select** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Network Connection Mode	Connection mode that the 3G modem used on a WCDMA or CDMA network, or connection mode that the LTE modem used on an LTE network. The following connection modes are available for a WCDMA network: ● GSM only: Only the GSM mode can be used. ● GSM precedence: The GSM mode is used preferentially. ● WCDMA only: Only the WCDMA mode can be used. ● WCDMA precedence: The WCDMA mode is used preferentially. This parameter can be configured using the **mode wcdma** command. The following connection modes are available for a CDMA network: ● 1xrtt only: Only the CDMA2000 1X (1xRTT) mode can be used. ● Evdo only: Only the CDMA2000 1xEV-DO mode can be used. ● HYBRID: The CDMA2000 1X and CDMA2000 1xEV-DO combined mode can be used. This parameter can be configured using the **mode cdma** command. The following connection modes are available for an LTE network: ● Automatic: indicates that the LTE modem automatically selects a network. ● GSM only: indicates that the LTE modem can only select the GSM network. ● WCDMA only: indicates that the LTE modem can only select the WCDMA network. ● LTE only: indicates that the LTE modem can only select the LTE network. ● UMTS only: indicates that the LTE modem selects the WCDMA or TD-SCDMA network. ● WCDMA-GSM: indicates that the LTE modem selects the WCDMA or GSM network. The WCDMA mode is used preferentially. ● UMTS-GSM: indicates that the LTE modem selects the UMTS or GSM network. The UMTS mode is used preferentially. This parameter can be configured using the **mode lte** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current Network Connection	Type of the network connected to the 3G or LTE modem.
Mobile Country Code (MCC)	Mobile country code of the network. This parameter can be configured using the **plmn select** command.
Mobile Network Code (MNC)	Mobile network code of the network. This parameter can be configured using the **plmn select** command.
Mobile Operator Information	Carrier information.
Location Area Code (LAC)	Location area code of the network.
Cell ID	Cell ID of the network.
Upstream Bandwidth	Upstream bandwidth of the 3G or LTE modem.
Downstream Bandwidth	Downstream bandwidth of the 3G or LTE modem.
Radio Information	Information about the radio used by the 3G or LTE modem.
Current Bands	Frequency band used by the 3G or LTE modem. The option **AUTO** indicates that the 3G or LTE modem automatically selects the frequency band of the carrier network to be connected to. To set the frequency band, run the **band gsm**, **band wcdma** or **band lte** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current RSSI	Received signal strength indicator. On a WCDMA network, the relationship between the signal strength and RSSI is as follows: ● good: The RSSI is higher than or equal to -70 dBm. ● normal: The RSSI is higher than -85 dBm and lower than -70 dBm. ● weak: The RSSI is higher than -113 dBm and lower than or equal to -85 dBm. ● no service: The RSSI is lower than or equal to -113 dBm. On a CDMA2000 network, the relationship between the signal strength and RSSI is as follows: ● good: The RSSI is higher than or equal to -80 dBm. ● normal: The RSSI is higher than -90 dBm and lower than -80 dBm. ● weak: The RSSI is higher than -125 dBm and lower than or equal to -90 dBm. ● no service: The RSSI is lower than or equal to -125 dBm.
Current RSRP	Reference signal received power. On a 4G/LTE network, the relationship between the signal strength and RSRP is as follows: ● strong: The RSRP is higher than or equal to -90 dBm. ● good: The RSRP is higher than -105 dBm and lower than or equal to -90 dBm. ● normal: The RSRP is higher than -112 dBm and lower than or equal to -105 dBm. ● slow: The RSRP is higher than -125 dBm and lower than or equal to -112 dBm. ● weak: The RSRP is higher than -136 dBm and lower than or equal to -125 dBm. ● no service: The RSRP is lower than or equal to -136 dBm.
Current RSRQ	Reference signal received quality.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current SINR	Signal to interference plus noise ratio. By default, the SINR threshold is used for the LTE signal strength The relationship between the signal strength and SINR is as follows: ● good: The SINR is higher than or equal to 15 dB. ● normal: The SINR is higher than 10 dB and lower than 15 dB. ● weak: The SINR is lower than or equal to 10 dB and is higher than or equal to -20 dB. ● no service: The SINR is lower than -20 dB.
Current RSCP	Received signal code power.
Current ECIO	Energy per chip to interference of other cell ratio.
Bands supported	Frequency band supported by the 3G or LTE modem.
Modem Security Information.	3G or LTE modem's security information.
SIM ID	The ID of SIM card.
PIN Verification	Whether PIN authentication is enabled: ● Enabled: PIN authentication is enabled. ● Disabled: PIN authentication is disabled. This parameter can be configured using the **pin verification** command.
PIN Status	Status of the PIN: ● Unknown: indicates that the status of PIN authentication is unknown. ● Ready: indicates that the PIN is unlocked successfully. ● PIN Requirement: indicates that users need to enter the PIN for authentication. ● PUK Requirement: indicates that users need to enter the PUK to unlock the PIN.
Number of Retries remaining	Number of PIN authentication attempts allowed. By default, the PIN is locked after the user enters incorrect PINs consecutively 3 times.
SIM Status	Status of the SIM card: ● Invalid: indicates that the SIM card is not functioning properly for some reason. For example, the PIN is not unlocked. ● Not insert: indicates that the SIM card is not installed. ● OK: indicates that the SIM card works normally.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

5.11.46 profile create
5.11.45 plmn select
5.11.29 mode wcdma
5.11.27 mode cdma
5.11.42 pin verification

5.11.18 display interface cellular

Function

The **display interface cellular** command displays the status of and traffic statistics on a cellular interface or cellular channel interface.

Format

display interface cellular [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface. If this parameter is not specified, the status of and traffic statistics on all cellular interfaces or cellular channel interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display interface cellular** command displays the status of and traffic statistics on a cellular interface or cellular channel interface. You can collect traffic statistics and locate faults on the serial interface according to the command output.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the status of and traffic statistics on cellular interface 0/0/0.

```
<Huawei> display interface cellular 0/0/0
Cellular0/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Cellular0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is negotiated, 10.1.1.2/24
Link layer protocol is PPP
LCP opened, IPCP opened
Current system time: 2011-06-08 11:35:23
Modem State: Present
Model = ME906E
Current Network Connection = LTE(LTE)
Current RSSI = -91 dBm
Current SINR = 6 dB (weak)
Last 300 seconds input rate 555 bytes/sec 4440 bits/sec 12 packets/sec
Last 300 seconds output rate 11230 bytes/sec 89840 bits/sec 311 packets/sec
   Input: 210 packets, 87205 bytes
     Unicast:                 200,       Ununicast:                 10
   Output:225340 packets, 6760917 bytes
     Unicast:                 225300,    Ununicast:                 40
   Input bandwidth utilization  : 0.01%
   Output bandwidth utilization : 0.01%
```

Table 5-37 Description of the **display interface cellular** command output

Item	Description
Cellular0/0/0 current state	Status of the cellular interface: ● UP: The interface is physically Up. ● DOWN: The interface is physically Down. ● Administratively down: The administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the cellular interface: ● UP: The link layer protocol of the interface is Up. ● DOWN: The link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Description	Interface description.
The Maximum Transmit Unit is	Maximum Transmission Unit (MTU) of the interface. Run the **5.20.8 mtu** command to set the maximum transmission unit (MTU) of an interface.
Hold timer is 10(sec)	Lifecycle of a packet. If a packet is not sent out before the hold timer times out, the packet is discarded.
Internet Address	IP address of the cellular interface. If no IP address is assigned to the interface, the system displays "Internet protocol processing : disabled".
Link layer protocol	Link layer protocol used by the cellular interface.
LCP opened	Status of the Link Control Protocol (LCP).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPCP opened	Internet Protocol Control Protocol (IPCP) status of the MP link.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Modem State	Whether a 3G or LTE modem has been connected to the cellular interface.
Model	Model of the 3G or LTE modem.
Current Network Connection	Type of the network connected to the 3G or LTE modem.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current RSSI/RSRP	Received signal strength indicator or reference signal receiving power. On a WCDMA network, the relationship between the signal strength and RSSI is as follows: ● good: The RSSI is higher than or equal to -70 dBm. ● normal: The RSSI is higher than -85 dBm and lower than -70 dBm. ● weak: The RSSI is higher than -113 dBm and lower than or equal to -85 dBm. ● no service: The RSSI is lower than or equal to -113 dBm. On a CDMA2000 network, the relationship between the signal strength and RSSI is as follows: ● good: The RSSI is higher than or equal to -80 dBm. ● normal: The RSSI is higher than -90 dBm and lower than -80 dBm. ● weak: The RSSI is higher than -125 dBm and lower than or equal to -90 dBm. ● no service: The RSSI is lower than or equal to -125 dBm. On a 4G/LTE network, the relationship between the signal strength and RSRP is as follows: ● strong: The RSRP is higher than or equal to -90 dBm. ● good: The RSRP is higher than -105 dBm and lower than or equal to -90 dBm. ● normal: The RSRP is higher than -112 dBm and lower than or equal to -105 dBm. ● slow: The RSRP is higher than -125 dBm and lower than or equal to -112 dBm. ● weak: The RSRP is higher than -136 dBm and lower than or equal to -125 dBm. ● no service: The RSRP is lower than or equal to -136 dBm.
Current SINR	Signal to interference plus noise ratio. By default, the SINR threshold is used for the LTE signal strength The relationship between the signal strength and SINR is as follows: ● good: The SINR is higher than or equal to 15 dB. ● normal: The SINR is higher than 10 dB and lower than 15 dB. ● weak: The SINR is lower than or equal to 10 dB and is higher than or equal to -20 dB. ● no service: The SINR is lower than -20 dB.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input	Number of packets received by the cellular interface.
Output	Number of packets sent by the cellular interface.
Unicast	Number of unicast packets received or sent by the cellular interface.
Ununicast	Number of non-unicast packets received or sent by the cellular interface.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

5.11.19 display cellular feature

Function

The **display cellular feature** command displays the status of the source address verification, LTE QoS flow control, and DHCP transparent transmission functions of the modem.

NOTE

Only routers with built-in ME909s modules support this command.

Format

display cellular *interface-number* **feature**

Parameters

Parameter	Description	Value
interface-number	Displays the status of the source address verification, LTE QoS flow control, and DHCP transparent transmission functions of the modem on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cellular feature** command to check the status of the source address verification, LTE QoS flow control, and DHCP transparent transmission functions of the modem. If the modem's firmware version is correct, the status of source address verification function is disabled, and the status of the LTE QoS flow control and DHCP transparent transmission functions is enabled according to customization. If the modem feature status does not meet the customized status, run the **module-upgrade** command in the diagnostic view to upgrade the modem version.

Example

Display the status of the source address verification, LTE QoS flow control, and DHCP transparent transmission functions of the modem on Cellular0/0/0.

```
<Huawei> display Cellular 0/0/0 feature
Modem feature status:
  Source address check: disabled
  LTE QoS control: enabled
  DHCP transfer packet: enabled
  Audio optimize: enabled
  Discontinuous Reception: disabled
  Encryption algorithm: gea1 gea2
  Modem log status: locked
```

Table 5-38 Description of the **display cellular feature** command output

Item	Description
Modem feature status	Status of the source address verification, LTE QoS flow control, and DHCP transparent transmission functions of the modem.
Source address check	Status of source MAC address verification.
LTE QoS control	Status of the LTE QoS flow control feature.
DHCP transfer packet	Status of the DHCP transparent transmission function.
Audio optimize	Status of the audio optimization function.
Discontinuous Reception	Status of the Discontinuous Reception (DRX) function.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Encryption algorithm	GPRS encryption algorithm supported by the 3G/LTE modem. You can run the **modem encryption-algorithm** command to change the GPRS encryption algorithm.
Modem log status	Log status of the current modem: ● locked: The modem is locked. ● unlocked: The modem is unlocked. **NOTE** Only V200R010C10 and later versions support this command.

5.11.20 display sms interface cellular

Function

The **display sms interface cellular** command displays information about received SMS messages.

Format

display sms interface cellular *interface-number* { **brief** | **id** *sms-id* | **verbose** }

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface.	-
brief	Displays brief information about all SMS messages.	-
id *sms-id*	Displays information about the SMS message with a specified ID. *sms-id* specifies the SMS message ID.	The value is an integer that ranges from 0 to 255.
verbose	Displays detailed information about all SMS messages.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to view information about SMS messages received by the device, including the source number, sending date and time, and size of the messages.

Example

Display brief information about all SMS messages received by Cellular2/0/0.

```
<Huawei> display sms interface cellular 2/0/0 brief
  ID   FROM         DATE      TIME      SIZE
   1  ****1111  13/02/14  10:38:36    20
   2  ****2222  13/02/14  15:40:41     5
   3  ****3333  13/02/14  16:19:04     6
 USED: 3  TOTAL: 3
```

Display detailed information about all SMS messages received by Cellular2/0/0.

```
<Huawei> display sms interface cellular 2/0/0 verbose
[ ID:  1 TIME: 13/02/14 10:38:36 FROM: ****1111 ]
[ ID:  2 TIME: 13/02/14 15:40:41 FROM: ****2222 ]
[ ID:  3 TIME: 13/02/14 16:19:04 FROM: ****3333 ]
```

Display information about the SMS message with the ID 1 received by Cellular2/0/0.

```
<Huawei> display sms interface cellular 2/0/0 id 1
ID:  1
FROM: ****1111
DATE: 13/02/14
TIME: 10:38:36
SIZE: 20
```

Table 5-39 Description of the **display sms interface cellular** command output

Item	Description
ID	ID of a received SMS message.
FROM	Source number of a received SMS message.
DATE	Date when an SMS message is received.
TIME	Time when an SMS message is received.
SIZE	Size of a received SMS message.

 Copyright © Huawei Technologies Co., Ltd.

5.11.21 display sms interface cellular statistics

Function

The **display sms interface cellular statistics** command displays statistics about SMS messages.

Format

display sms interface cellular *interface-number* **statistics**

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to check statistics about SMS messages, including the number of received SMS messages, number of SMS messages sent successfully, number of SMS messages failed to be sent, and number of deleted SMS messages.

Example

Display statistics about SMS messages received or sent by Cellular2/0/0.

```
<Huawei> display sms interface cellular 2/0/0 statistics
Total SMS received = 8
Total SMS sent successfully = 3
Total SMS sent failure = 0
Total SMS deleted = 3
```

Table 5-40 Description of the **display sms interface cellular statistics** command output

Item	Description
Total SMS received	Number of received SMS messages.

Item	Description
Total SMS sent successfully	Number of SMS messages sent successfully.
Total SMS sent failure	Number of SMS messages failed to be sent.
Total SMS deleted	Number of deleted SMS messages.

5.11.22 display sms send-history

Function

The **display sms send-history** command displays records of sent short messages saved in the memory.

Format

display sms send-history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check records of sent short messages.

Precautions

A maximum of 20 records of recently sent short messages can be displayed. The new record overrides the old ones.

After the device restarts, the historical records of sent short messages disappear.

Example

Display records of sent short messages saved in the memory.

```
<Huawei> display sms send-history
ID RECEIVER          YYYY/MM/DD  HH:MM:SS    INTERFACE        RESULT
0  ****5678          2015/03/04  17:15:54                     FAIL
```

Table 5-41 Description of the **display sms send-history** command output

Item	Description
ID	ID of a short message record. The ID ranges from 0 to 19.
RECEIVER	User phone number for receiving short messages. To configure the user phone number, run the **sms item** command.
YYYY/MM/DD	Date when short messages are sent.
HH:MM:SS	Time when short messages are sent.
INTERFACE	Cellular interface that successfully sends short messages.
RESULT	Result of sending short messages. • SUCCESS: indicates that short messages are sent successfully. • FAIL: indicates that short messages fail to be sent. • UNSENT: indicates that all cellular interfaces cannot send short messages. • INVALID: indicates that the SMS service referenced by the **sms send-item** command does not exist. Short messages cannot be sent.

Related Topics

5.11.63 sms item

5.11.23 display snmp-agent trap feature-name ifmtrap all

Function

The **display snmp-agent trap feature-name ifmtrap all** command displays the status of all traps on the IFM module.

Format

display snmp-agent trap feature-name ifmtrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name ifmtrap all** command to check the status of all traps on the IFM module. The status of a trap is configured using the **snmp-agent trap enable feature-name ifmtrap** command.

Example

Display the status of all traps on the IFM module.

```
<Huawei> display snmp-agent trap feature-name ifmtrap all
-----------------------------------------------------------------------------
Feature name: IFMTRAP
Trap number : 5
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hw3GPinModify                  on                      on
hwPortPhysicalEthHalfDuplexAlarm
                             off                     off
hwPortPhysicalEthFullDuplexClear
                             off                     off
hw3GMIBTrapCellIdChange        off                     off
hwPortSpeedChangeTrap          off                     off
```

Table 5-42 Description of the **display snmp-agent trap feature-name ifmtrap all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Name of a trap. Traps on the IFM module include: • hw3GPinModify: enables the trap function for the PIN change. • hwPortPhysicalEthHalfDuplexAlarm: enables the trap function for the interface duplex mode change from full-duplex to half-duplex. • hwPortPhysicalEthFullDuplexClear: enables the trap function for the interface duplex mode change from half-duplex to full-duplex. • hw3GMIBTrapCellIdChange: enables the trap function for the cell ID change. • hwPortSpeedChangeTrap: enables the trap function for the interface rate change.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default switch status	Default trap status: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Current trap status: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

5.11.66 snmp-agent trap enable feature-name ifmtrap

5.11.24 imsi check

Function

The **imsi check** command enables IMSI check before LTE dialup.

The **undo imsi check** command disables IMSI check before LTE dialup.

By default, IMSI check before LTE dialup is disabled.

Format

imsi check *imsi*

undo imsi check

Parameters

Parameter	Description	Value
imsi	Specifies the IMSI of a SIM card.	The value is a string of 1 to 15 characters. It can only contain digits 0 to 9.

Views

LTE cellular interface view

Default Level

2: Configuration level

Usage Guidelines

To prevent a rogue SIM card from establishing a connection with the Agile Controller-Campus through LTE dialup, you can enable IMSI check before dialup to check whether the configured IMSI is the same as the IMSI of the current SIM card. If the IMSIs are the same, the device continues the dialup. If the IMSIs are different, the device does not trigger the dialup.

Example

Enable IMSI check before LTE dialup. The IMSI is 666.

```
<Huawei> system-view
[Huawei] interface Cellular 0/0/0
[Huawei-Cellular0/0/0] imsi check 666
```

Related Topics

5.11.4 apn user name catch-imsi-sn

5.11.25 interface cellular

Function

Using the **interface cellular** command, you can enter the cellular interface view or cellular channel interface view.

Format

interface cellular *interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface. ● To enter the cellular interface view, specify *interface-number* in the format of slot number/card number/interface number. ● To enter the cellular channel interface view, specify *interface-number* in the format of chassis number/slot number/card number/main interface number:channel interface number (the value can be 1 or 2). For example, channel interface 1 of Cellular0/0/0 is numbered Cellular0/0/0:1.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the 3G or LTE function on a cellular interface or cellular channel interface, run the **interface cellular** command to enter the cellular interface view or cellular channel interface view.

Cellular channel interfaces only apply to the multi-APN scenario.

Prerequisites

The multi-APN function has been enabled on the cellular interface before you enter the cellular channel interface view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enter the view of cellular interface 0/0/0.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0]
```

Display the view of cellular channel interface 1.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] multi-apn enable
[Huawei-Cellular0/0/0] quit
[Huawei] interface cellular 0/0/0:1
[Huawei-Cellular0/0/0:1]
```

Related Topics

5.11.18 display interface cellular
5.11.38 multi-apn enable

5.11.26 ip address negotiate

Function

The **ip address negotiate** command enables a cellular interface or cellular channel interface to dynamically obtain an IP address.

The **undo ip address negotiate** command disables a cellular interface or cellular channel interface from dynamically obtaining an IP address.

By default, a cellular interface or cellular channel interface cannot dynamically obtain an IP address.

Format

ip address negotiate

undo ip address negotiate

Parameters

None

Views

Cellular interface view, Cellular channel interface view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ip address negotiate** command to enable a cellular interface or cellular channel interface to dynamically obtain an IP address from the carrier.

Example

Enable the cellular interface to dynamically obtain an IP address.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] ip address negotiate
```

5.11.27 mode cdma

Function

Using the **mode cdma** command, you can configure a CDMA2000 network connection mode for a 3G modem.

Format

mode cdma { **1xrtt-only** | **evdo-only** | **hybrid** }

Parameters

Parameter	Description	Value
1xrtt-only	Indicates that a 3G modem connects to a 1x radio transmission technology (1xRTT) network.	-
evdo-only	Indicates that a 3G modem connects to an evolution-data optimized (EV-DO) network.	-
hybrid	Indicates that a 3G modem connects to a 1xRTT and EV-DO combined network.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 3G modem has various types. By default, each type of the 3G modem has a unique CDMA2000 network connection mode. After a CDMA2000 network

connection mode is configured, it is recorded in the 3G modem and permanently valid.

Configure a correct CDMA2000 network connection mode for the 3G modem based on the type of the network provided by the carrier. If the CDMA2000 network connection mode is incorrect, you need to run the **mode cdma** command to change the CDMA2000 network connection mode for the 3G modem.

Precautions

- This command is valid only when a 3G modem with a UIM card is connected to a 3G cellular interface.
- If you run the **mode cdma** command multiple times in the same 3G cellular interface view, only the latest configuration takes effect.

Example

Configure the 3G modem to connect to a 1xRTT and EV-DO combined network.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] mode cdma hybrid
```

Related Topics

5.11.29 mode wcdma

5.11.28 mode lte

Function

The **mode lte** command configures the 3G or LTE network connection mode for an LTE modem.

By default, the 3G or LTE network connection mode is auto for an LTE modem.

Format

mode lte { **auto** | **gsm-only** | **1xrtt-only** | **evdo-only** | **hybrid** | **lte-only** | **tdscdma-only** | **umts-gsm** | **umts-only** | **wcdma-gsm** | **wcdma-only** }

Parameters

Parameter	Description	Value
auto	Indicates that an LTE modem automatically connects to a network.	-
gsm-only	Indicates that an LTE modem can only connect to a GSM network.	-

Parameter	Description	Value
1xrtt-only	Indicates that an LTE modem can only connect to a 1xRTT network. **NOTE** The 1LTE-Lt interface card support this parameter.	-
evdo-only	Indicates that an LTE modem can only connect to a EV-DO network. **NOTE** The 1LTE-Lt interface card and 1LTE-Lt-7 interface card support this parameter.	-
hybrid	Indicates that an LTE modem connects to a 1xRTT and EV-DO combined network. **NOTE** The 1LTE-Lt interface card support this parameter.	-
lte-only	Indicates that an LTE modem can only connect to a LTE network.	-
tdscdma-only	Indicates that an LTE modem can only connect to a TD-SCDMA network. **NOTE** The 1LTE-Lt and 1LTEC interface card support this parameter.	-
umts-gsm	Indicates that an LTE modem connects to either a UMTS or GSM network and preferentially connects to the UMTS network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card supports this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
umts-only	Indicates that an LTE modem can only connect to either a WCDMA or TD-SCDMA network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card supports this parameter.	-
wcdma-gsm	Indicates that an LTE modem connects to either a WCDMA or GSM network and preferentially connects to the WCDMA network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card does not support this parameter.	-
wcdma-only	Indicates that an LTE modem can only connect to a WCDMA network. **NOTE** The 1LTEC interface card and 1LTE-Lt-7 interface card does not support this parameter.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LTE cellular interfaces can connect to the 3G or LTE network only when the 3G or LTE network connection mode is configured for an LTE modem based on the type of the network provided by the carrier. If the connection mode is inconsistent with the network type, run the **mode lte** command to modify the 3G or LTE network connection mode for the LTE modem.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- This command is valid only when the LTE modem is working.
- If you run the **mode lte** command multiple times in the same LTE cellular interface view, only the latest configuration takes effect.

Example

Configure the LTE modem to select the LTE network.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] mode lte lte-only
```

5.11.29 mode wcdma

Function

Using the **mode wcdma** command, you can configure a WCDMA network connection mode for a 3G modem.

Format

mode wcdma { **gsm-only** | **gsm-precedence** | **wcdma-only** | **wcdma-precedence** }

Parameters

Parameter	Description	Value
gsm-only	Indicates that a 3G modem connects to a GSM network.	-
gsm-precedence	Indicates that a 3G modem preferentially connects to a GSM network.	-
wcdma-only	Indicates that a 3G modem connects to a WCDMA network.	-
wcdma-precedence	Indicates that a 3G modem preferentially connects to a WCDMA network.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 3G modem has various types. By default, each type of the 3G modem has a unique WCDMA network connection mode. After a WCDMA network connection mode is configured, it is recorded in the 3G modem and permanently valid.

Configure a correct WCDMA network connection mode for the 3G modem based on the type of the network provided by the carrier. If the WCDMA network connection mode is incorrect, you need to run the **mode wcdma** command to change the WCDMA network connection mode for the 3G modem.

Precautions

- This command is valid only when a 3G modem is connected to a 3G cellular interface.
- If you run the **mode wcdma** command multiple times in the same 3G cellular interface view, only the latest configuration takes effect.

Example

Configure the 3G modem to select only WCDMA networks to connect to.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] mode wcdma wcdma-only
```

5.11.30 modem auto-recovery track nqa

Function

The **modem auto-recovery track nqa** command configures the device to use an NQA test instance to detect the 3G or LTE link status.

The **undo modem auto-recovery track nqa** command restores the default setting.

By default, the device does not use an NQA test instance to detect a 3G or LTE link.

Format

modem auto-recovery track { **nqa** *admin-name test-name* | **nqa-group** *nqa-group-name* } [**probe-cycle** *period* | **probe-cycle seconds** *period-s*]

undo modem auto-recovery track { **nqa** | **nqa-group** }

NOTE

Only V200R010C10 and later versions support the **nqa-group** *nqa-group-name* parameter.

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces.
nqa-group *nqa-group-name*	Indicates the name of an NQA group for an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces.
probe-cycle *period*	Specifies the interval for querying NQA test results.	The value is an integer that ranges from 1 to 30, in minutes. The default value is 5.
probe-cycle seconds *period-s*	Specifies the interval for querying NQA test results, in seconds.	The value is an integer that ranges from 1 to 1800, in seconds. The default value is 300.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a 3G/LTE link becomes unstable because of weak 3G/LTE signals or noises, you may fail to access external networks through the 3G/LTE link even if the dialup succeeds. To prevent this problem, configure the device to use NQA test instances (multiple NQA test instances can be added to an NQA group) to detect the 3G/LTE link status. When the 3G/LTE link is unstable, the device triggers the corresponding action to restore the link.

Prerequisites

ICMP NQA test instances have been configured.

If you need multiple NQA test instances, configure these test instances, add these test instances to an NQA group, and set the test instance type to ICMP.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **modem auto-recovery track action** command to set the maximum number of 3G/LTE link detection failures in an NQA test instance. When the number of consecutive 3G/LTE link detection failures in an NQA test instance reaches the maximum value, the device triggers an action to recover the link.

Example

Configure the device to use an NQA test instance **user user1** to detect a 3G or LTE link.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] modem auto-recovery track nqa user user1
```

Related Topics

5.11.31 modem auto-recovery track action

5.11.31 modem auto-recovery track action

Function

The **modem auto-recovery track action** command sets the maximum number of 3G or LTE link detection failures in an NQA test instance. When the number of consecutive 3G or LTE link detection failures in an NQA test instance reaches the maximum value, the device triggers an action to recover the 3G or LTE link.

The **undo modem auto-recovery** command restores the default setting.

By default, the maximum number of 3G or LTE link detection failures in an NQA test instance is not configured. That is, the device does not trigger an action to recover a 3G or LTE link when 3G or LTE link detection fails for several consecutive times.

Format

modem auto-recovery track action { **plmn-search** | **redial** } **fail-times** *times*

modem auto-recovery track action modem-reboot fail-times *times* [**mandatory**]

undo modem auto-recovery track action { **plmn-search** | **modem-reboot** | **redial** }

Parameters

Parameter	Description	Value
plmn-search	Configures the device to search the PLMN again when the number of consecutive 3G or LTE link detection failures reaches the maximum value.	-
modem-reboot	Configures the device to restart the 3G or LTE modem when the number of consecutive 3G or LTE link detection failures reaches the maximum value.	-
redial	Configures the device to reconfigure a dial-up connection when the number of consecutive 3G or LTE link detection failures reaches the maximum value.	-
fail-times *times*	Specifies the maximum number of 3G or LTE link detection failures in an NQA test instance.	The value is an integer that ranges from 1 to 128.
mandatory	Configures the device to perform operations based on the NQA detection result without considering the interface status. **NOTE** This parameter is supported in V200R010C10 and later versions.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **modem auto-recovery track nqa** command is executed to use an NQA test instance to test the 3G or LTE link status, run the **modem auto-recovery track action** command to set the maximum number of 3G or LTE link detection failures in an NQA test instance if the 3G or LTE link is unreachable for a long period. When the number of consecutive 3G or LTE link detection failures in an NQA test instance reaches the maximum value, the device triggers an action (reconfigure a dial-up connection, search the PLMN again or restart the 3G or LTE modem) to recover the 3G or LTE link.

Precautions

When **mandatory** is not specified, the number of link detection failures increases by one if the cellular main interface is Up and there is no incoming traffic on the interface in case of an NQA test failure. When **mandatory** is specified, the number of link detection failures increases by one if NQA tests fail. When the number of link detection failures reaches the threshold, the system restarts the LTE module.

Example

Configure the device to search the PLMN again when the number of consecutive 3G or LTE link detection in an NQA test instance reaches 10.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] modem auto-recovery track action plmn-search fail-times 10
```

Related Topics

5.11.30 modem auto-recovery track nqa

5.11.32 modem auto-recovery dial action modem-reboot fail-times

Function

The **modem auto-recovery dial action modem-reboot fail-times** command sets the maximum number of dial-up failures. When the number of consecutive dial-up failures reaches the maximum value, the device restarts a 3G or LTE modem.

The **undo modem auto-recovery dial action modem-reboot** command deletes the maximum number of dial-up failures.

By default, the maximum number of of dial-up failures is not configured. That is, the device does not restart the 3G modem or restart itself in consecutive dial-up failures

Format

modem auto-recovery dial action modem-reboot fail-times *times*

undo modem auto-recovery dial action modem-reboot

Parameters

Parameter	Description	Value
times	Specifies the maximum number of dial-up failures.	The value is an integer that ranges from 1 to 128. The value less than 8 is recommended.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

When the dial-up initiated through a cellular interface fails multiple times, you can run the **modem auto-recovery dial action modem-reboot fail-times** command to set the maximum number of dial-up failures. When the number of consecutive dial-up failures reaches the maximum value, the device restarts the 3G or LTE modem so that the fault can be rectified automatically.

Example

Set the maximum number of dial-up failures to 5.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] modem auto-recovery dial action modem-reboot fail-times 5
```

5.11.33 modem auto-recovery services-unavailable

Function

The **modem auto-recovery services-unavailable** command sets the out-of-service state detection interval and the maximum number of times the 3G/LTE modem automatically restarts.

The **undo modem auto-recovery services-unavailable** command disables the function of automatically restarting the 3G/LTE modem or automatically switching the active and standby SIM cards upon the out-of-service state.

By default, the maximum number of times the 3G/LTE modem automatically restarts and the out-of-service state detection interval are not set on the device. That is, the 3G/LTE modem does not automatically restart or the active and standby SIM cards are not automatically switched upon the out-of-service state.

 Copyright © Huawei Technologies Co., Ltd.

Format

modem auto-recovery services-unavailable action modem-reboot test-times *times* **interval** *interval*

modem auto-recovery services-unavailable action sim-switch [**interval** *interval*]

undo modem auto-recovery services-unavailable

Parameters

Parameter	Description	Value
action modem-reboot	Restarts the 3G/LTE modem automatically upon the out-of-service state.	-
action sim-switch	Switches the active and standby SIM cards automatically upon the out-of-service state.	-
test-times *times*	Specifies the maximum number of times the 3G/LTE modem automatically restarts.	The value is an integer that ranges from 0 to 10. You are not advised to set the value greater than 8. The value 0 indicates that the number of times the 3G/LTE modem automatically restarts is infinite.
interval *interval*	Specifies the out-of-service state detection interval.	The value is an integer that ranges from 60 to 3600, in 5 seconds. The default detection interval is 600 seconds when the active and standby SIM cards are automatically switched upon the out-of-service state.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

When the 3G cellular or LTE cellular interface is in out-of-service state because of a network exception, you can run the **modem auto-recovery services-unavailable action modem-reboot test-times** command to set the out-of-service state detection interval and the maximum number of times the 3G/LTE modem automatically restarts. When the period of time the 3G/LTE modem remains in out-of-service state reaches the detection interval, the 3G/LTE modem automatically restarts or the active and standby SIM cards are switched.

When the interface recovers from the out-of-service state within the detection interval or the number of times the 3G/LTE modem automatically restarts reaches the upper limit, the 3G/LTE modem no longer restarts. You can run the **display cellular** *interface-number* **network** command to view the current status of the 3G/LTE modem. When **Current Service Status** is displayed as **Service available** in the command output, the 3G/LTE modem recovers from the out-of-service state.

Example

Set the out-of-service state detection interval of the 3G/LTE modem to 300s (60*5s) and the maximum number of times the 3G/LTE modem automatically restarts to 5.

```
<Huawei> system-view
[Huawei] interface cellular 1/0/0
[Huawei-Cellular1/0/0] modem auto-recovery services-unavailable action modem-reboot test-times 5 interval 60
```

Set the out-of-service state detection interval of the 3G/LTE modem to 400s. Within the detection interval, the active and standby SIM cards are automatically switched.

```
<Huawei> system-view
[Huawei] interface cellular 1/0/0
[Huawei-Cellular1/0/0] modem auto-recovery services-unavailable action sim-switch interval 400
```

5.11.34 modem encryption-algorithm

Function

The **modem encryption-algorithm** command configures the GPRS encryption algorithm for the 3G/LTE modem.

By default, the 3G/LTE modem supports the GEA1.0 and GEA2.0 encryption algorithms, and does not support the GEA3.0 encryption algorithm.

NOTE

Only routers with built-in ME909s modules support this command.

Format

modem encryption-algorithm { **gea1** | **gea3** }

Parameters

Parameter	Description	Value
gea1	Sets the GPRS encryption algorithm of the 3G/LTE modem to GEA1.0 and GEA2.0.	-
gea3	Sets the GPRS encryption algorithm of the 3G/LTE modem to GEA3.0 and GEA2.0.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the 3G/LTE modem registers and accesses the network, it uses the GPRS encryption algorithms GEA1.0 and GEA2.0 to initiate a registration with the core network by default. The core network then selects the encryption mode based on the encryption capability of itself. The device can access the network only when the encryption mode matches the device.

If the encryption mode supported by the core network does not match the current device, you can run the **modem encryption-algorithm gea3** command to set the GPRS encryption algorithm of the 3G/LTE modem to GEA2.0 and GEA3.0.

Precautions

This command can be run only when the 3G/LTE modem is in position.

To ensure the configured GPRS encryption algorithm still takes effect when the device accesses the network for the next time, you can restart the modem immediately.

If you choose not to restart the modem immediately, you can run the **modem reboot** command to restart the 3G/LTE modem.

Example

Set the GPRS encryption algorithm of the 3G/LTE modem to GEA1.0 and GEA2.0, and choose not to restart the modem immediately.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] modem encryption-algorithm gea1
```

```
Warning: The modified GPRS encryption algorithm can take effect only after the m
odem reboot. The LTE modem will reboot. Continue? [Y/N]:n
Info: The encryption algorithm takes effect next time after the modem reboot.
[Huawei-Cellular0/0/0]
Apr  9 2000 09:16:16+00:00 Huawei 0.0.0.0 %%01IFPDT/4/MODEM_REBOOT(l)[1]:The use
r choose NO when there is a selection about whether to reboot modem.
```

Set the GPRS encryption algorithm of the 3G/LTE modem to GEA3.0 and GEA2.0, and choose to restart the modem immediately.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] modem encryption-algorithm gea3
Warning: The modified GPRS encryption algorithm can take effect only after the m
odem reboot. The LTE modem will reboot. Continue? [Y/N]:y
Apr  9 2000 09:18:01+00:00 Huawei 0.0.0.0 %%01IFPDT/4/MODEM_REBOOT(l)[2]:The use
r choose YES when there is a selection about whether to reboot modem.
```

5.11.35 modem peer network-route

Function

The **modem peer network-route** command enables the function of installing the peer's routes in the local routing table.

The **undo modem peer network-route** command disables the function of installing the peer's routes in the local routing table.

By default, a device is disabled from installing the peer's routes in the local routing table.

NOTE

This function is supported in V200R010C10 and later versions.

Format

modem peer network-route

undo modem peer network-route

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to install the peer's routes in the local routing table, run the **modem peer network-route** command.

Precautions

After the **modem peer network-route** command is run, the local routing table contains the peer's routes.

After the **undo modem peer network-route** command is run, the local routing table does not contain the peer's routes.

Example

Enable the function of installing the peer's routes in the local routing table.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] modem peer network-route
```

5.11.36 modem reboot

Function

The **modem reboot** command restarts a 3G/LTE modem.

Format

modem reboot [**fast**]

NOTE

Only the models with built-in ME909s terminal modules in V200R010C10 and later versions support the **fast** parameter.

Parameters

Parameter	Description	Value
fast	Restarts the LTE modem fast.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 3G/LTE modem restarts automatically when it detects an exception. If the 3G/LTE modem cannot restart automatically, you can run this command to restart it manually.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- When this command is executed to manually restart a 3G/LTE modem, services on the specified cellular interface will be interrupted.
- SIM, USIM, and UIM cards are not hot swappable.

  To ensure that the installed SIM, USIM, and UIM cards work properly, run the **modem reboot** command to manually restart the 3G/LTE modem after hot swapping these cards.

  To check whether SIM, USIM, and UIM cards are working properly, run the **display cellular** command to view the **SIM Status** or **UIM Status** field.

Example

Restart a 3G/LTE modem.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] modem reboot
Warning: The 3G/LTE module will reboot. Continue? [Y/N]:y
```

Related Topics

5.11.17 display cellular

5.11.37 mtu (3G)

Function

Using the **mtu** command, you can set the maximum transmission unit (MTU) for a cellular interface or cellular channel interface.

Using the **undo mtu** command, you can restore the default MTU.

By default, the MTU of a cellular interface or cellular channel interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a cellular interface.	The value is an integer that ranges from 128 to 1500, in bytes.

Views

Cellular interface view, Cellular channel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IP layer limits the size of a packet sent each time. Any time the IP layer receives an IP packet, it checks to which local interface the packet needs to be sent and obtains the MTU of the interface. Then, the IP layer compares the MTU with the packet size. If the packet size is larger than the MTU, the IP layer disassembles the packet to fragments smaller than the MTU.

If forcible unfragmentation is configured, oversized packets are discarded at the IP layer. To prevent packet loss on the network, large packets must be forcibly fragmented. Run the **mtu** command to set the size of a fragment.

Precautions

If you run the **mtu** command multiple times in the same cellular interface view or cellular channel interface, only the latest configuration takes effect.

Follow-up Procedure

Run the **shutdown** and **undo shutdown**/**restart** commands to restart the related physical interface to make the configuration take effect.

Example

Set the MTU of cellular interface 0/0/0 to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] mtu 1200
[Huawei-Cellular0/0/0] restart
```

Related Topics

5.11.18 display interface cellular

5.11.38 multi-apn enable

Function

The **multi-apn enable** command enables the multi-APN function on a cellular interface.

The **undo multi-apn enable** command disables the multi-APN function on a cellular interface.

By default, the multi-APN function is disabled on a cellular interface.

Format

multi-apn enable

undo multi-apn enable

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A cellular interface can be configured with two cellular channel interfaces. After the multi-APN function is configured, you can create two APN profiles and bind the APN profiles respectively to the two cellular channel interfaces. One APN connects to the Internet for data communication, and the other connects to the IMS network for VoIP communication.

Precautions

The multi-APN functions can be configured only on the LTE cellular interface (Cellular 0/0/0) supported by the AR109GW-L, AR121GW-L, AR129CGVW-L, AR161FG-Lc, AR161FG-L, AR169FGW-L, AR169FGVW-L, AR169G-L, AR169EGW-L, AR161G-L, AR161G-Lc, AR161FGW-Lc, and AR161FGW-L.

LTE interface cards (except 1LTE-Lt and 1LTE-Lt-7) support the multi-APN configuration. LTE interface cards support the dual-SIM configuration.

Example

Enable the multi-APN function on the cellular interface.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] multi-apn enable
```

5.11.39 packet-service recover

Function

The **packet-service recover** command configures a 3G or LTE modem to automatically restart and sets the interval at which a 3G or LTE modem automatically restarts.

The **undo packet-service recover** command cancels the configuration.

By default, a 3G or LTE modem does not automatically restart.

Format

packet-service recover *interval*

undo packet-service recover

Parameters

Specification	Description	Value
interval	Specifies the interval at which a 3G or LTE modem automatically restarts.	The value is an integer that ranges from 10 to 86400, in seconds.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

When a 3G or LTE modem is not attached to a PS domain, you can run the **packet-service recover** command to configure a 3G or LTE modem to automatically restart and set the interval at which the 3G or LTE modem automatically restarts. Then the 3G or LTE modem automatically restarts and starts dialing until it is attached to a PS domain.

Example

Set the interval at which a 3G or LTE modem automatically restarts to 200s.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] packet-service recover 200
```

Related Topics

5.11.17 display cellular

5.11.40 pin modify

Function

The **pin modify** command changes the personal identification number (PIN) of a SIM, USIM or UIM card.

Format

pin modify

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set a new PIN for the SIM, USIM or UIM card. The new PIN is saved on the SIM, USIM or UIM card.

Precautions

- This command is valid only when a 3G or LTE modem with a SIM, USIM or UIM card is connected to a cellular interface.
- The PIN of a SIM, USIM or UIM card can be changed only when PIN authentication is enabled on the 3G modem.

Example

Change the PIN.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] pin modify
Enter Current Pin Code:
Enter Pin Code:
Confirm Pin Code:
Warning: PIN will be changed. Continue? [Y/N]:y
PIN has been changed successfully.
```

Related Topics

5.11.41 pin unlock

5.11.42 pin verification

5.11.43 pin verify

5.11.41 pin unlock

Function

The **pin unlock** command unlocks the SIM, USIM or UIM card using the personal identification number unlocked key (PUK) and sets a new PIN.

Format

pin unlock

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PIN unblocking key (PUK) is allocated by the carrier. If a user enters incorrect PINs three consecutive times, the SIM, USIM or UIM card is locked to ensure security of the card. To unlock the card, enter the PUK.

Precautions

This command is valid only when a 3G or LTE modem with a SIM, USIM or UIM card is connected to a cellular interface.

NOTE

If a user enters incorrect PUKs ten consecutive times, the SIM, USIM or UIM card is permanently locked and the user needs to obtain a new one from the carrier.

Example

Unlock the SIM, USIM or UIM card using the PUK and sets a new PIN.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] pin unlock
Enter Current Puk Code:
Enter Pin Code:
Confirm Pin Code:
Warning: PIN will be unlocked and changed. Continue? [Y/N]:y
Unlocking PIN...Please wait...
PIN has been unlocked and changed successfully.
```

Related Topics

5.11.40 pin modify
5.11.42 pin verification
5.11.43 pin verify

5.11.42 pin verification

Function

The **pin verification** command enables or disables PIN authentication on a 3G or LTE modem.

By default, PIN authentication is disabled.

Format

pin verification enable [**auto**]

pin verification disable

Parameters

Parameter	Description	Value
enable	Enables PIN authentication.	-
disable	Disables PIN authentication.	-
auto	Indicates automatic PIN authentication. This parameter can be specified if you do not require high security of the SIM, USIM or UIM card. After this parameter is specified, you do not need to enter the PIN every time you use the SIM, USIM or UIM card.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PIN identifies the user of a SIM, USIM or UIM card.

PIN authentication prevents unauthorized users from using a SIM, USIM or UIM card. You can use a 3G or LTE modem only after the PIN is authenticated.

Precautions

- This command is valid only when a 3G or LTE modem with a SIM, USIM or UIM card is connected to a cellular interface.
- If PIN authentication in auto mode fails, you must manually enter the PIN for authentication.

Example

Enable PIN authentication on the 3G or LTE modem.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] pin verification enable auto
Enter Current Pin Code:
```

Related Topics

5.11.40 pin modify

5.11.41 pin unlock

5.11.43 pin verify

5.11.43 pin verify

Function

The **pin verify** command authenticates a PIN.

Format

pin verify [**auto**]

Parameters

Parameter	Description	Value
auto	Indicates automatic PIN authentication. This parameter can be specified if you do not require high security of the SIM, USIM or UIM card. After this parameter is specified, you do not need to enter the PIN every time you use the SIM, USIM or UIM card.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIN authentication is enabled, you are required to enter the correct PIN every time you use the SIM, USIM or UIM card. If the PIN authentication fails, data communication is unavailable on the 3G or LTE modem.

Precautions

- If you enter incorrect PINs three consecutive times, the PIN of the SIM, USIM or UIM card is locked.
- This command is valid only when a 3G or LTE modem with a SIM, USIM or UIM card is connected to a cellular interface.

NOTE

A PIN is a decimal integer of 4 to 8 digits. Obtain the initial PIN from the carrier.

Example

Authenticate the PIN.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] pin verify
Enter Current Pin Code:
 Verifying PIN...Please wait...
 PIN has been verified successfully.
```

Related Topics

5.11.40 pin modify

5.11.41 pin unlock

5.11.42 pin verification

5.11.44 plmn search

Function

Using the **plmn search** command, you can configure a 3G or LTE modem to search for available public land mobile networks (PLMNs).

Format

plmn search

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **plmn search** command is a network detection command.

Precautions

- This command applies only to WCDMA or LTE networks. This command is valid only when a 3G or LTE modem with a SIM or USIM card is connected to a cellular interface.
- It takes several minutes for a 3G or LTE modem to complete the search after this command is executed.

  NOTE

  If the 3G or LTE modem fails to search PLMNs after executing this command, the possible causes include poor signal quality, coverage hole, and signal interference. Wait for a period and run the command again.

Follow-up Procedure

After PLMNs are found, the system shows the searching results. Users can run the **plmn select** command to select a PLMN manually.

Example

Search for PLMNs.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] plmn search
```

Related Topics

5.11.45 plmn select

5.11.45 plmn select

Function

The **plmn select** command allows you to manually select a PLMN for a 3G or an LTE modem or configure the 3G or LTE modem to automatically select a PLMN.

By default, a 3G or an LTE modem automatically selects a PLMN.

Format

Manually selecting a PLMN:

plmn select manual *mcc mnc* [**fail-over-auto**]

undo plmn select manual

Automatically selecting a PLMN:

plmn auto

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
manual	Manually selects a PLMN for a 3G or an LTE modem. When this keyword is used, set the *mcc* and *mnc* parameter.	-
mcc	Specifies the mobile country code (MCC) of a PLMN.	The value is an integer that ranges from 0 to 999.
mnc	Specifies the mobile network code (MNC) of a PLMN.	The value is an integer that ranges from 0 to 999.
fail-over-auto	Indicates that a 3G or an LTE modem automatically selects a PLMN when manual selection of a PLMN fails.	-
auto	Automatically selects a PLMN.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a WCDMA or an LTE network, you can manually select a PLMN for a 3G or an LTE modem or configure the 3G or LTE modem to automatically select a PLMN.

By default, a 3G or an LTE modem automatically selects a PLMN. If you have subscribed to WCDMA or LTE services and obtained the mobile country code (MCC) and mobile network code (MNC), you can manually select a PLMN.

Precautions

This command applies only to WCDMA or LTE networks. This command is valid only when a 3G or an LTE modem with a SIM or USIM card is connected to a cellular interface.

When the manual PLMN selection mode is use, the automatic PLMN selection mode is restored after you run the **undo plmn select manual** command. When

the automatic PLMN selection mode is used, there is no change after you run this command.

NOTE

If the manually selected PLMN is invalid, the 3G or LTE modem cannot connect to the network. Run the **undo plmn select manual** or **plmn auto** command to configure the 3G or LTE modem to automatically select a PLMN, and run the **modem reboot** command to manually restart the modem.

Follow-up Procedure

Run the **display cellular** command to view information about the selected PLMN.

Example

Manually select a PLMN for the 3G or LTE modem.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] plmn select manual 460 03
```

Related Topics

5.11.44 plmn search

5.11.17 display cellular

5.11.46 profile create

Function

Using the **profile create** command, you can create a parameter profile for a 3G or LTE modem and configure an APN in the parameter profile.

Format

profile create *profile-number* { **dynamic** | **static** *apn* }

Parameters

Parameter	Description	Value
profile-number	Specifies the number of a description profile.	The value is 1.
dynamic	Indicates that the 3G modem dynamically sets the access point name (APN).	-
static *apn*	Configures a static APN.	The value is a string of 1 to 99 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An APN identifies a service type on a WCDMA or LTE network. The WCDMA or LTE system provides services for users according to APNs configured for the users.

Precautions

This command applies only to WCDMA or LTE networks. This command is valid only when a 3G or LTE modem with a SIM or USIM card is connected to a cellular interface.

NOTE

APNs vary according to different WCDMA or LTE network carriers. Obtain the APN from the local carrier.

Example

Create a parameter profile for the 3G or LTE modem connected to cellular interface 0/0/0 and configure an APN as 3GNET.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] profile create 1 static 3GNET
```

Related Topics

5.11.47 profile delete

5.11.47 profile delete

Function

Using the **profile delete** command, you can delete the parameter profile of a 3G or LTE modem.

Format

profile delete *profile-number*

Parameters

Parameter	Description	Value
profile-number	Specifies the number of a description profile.	The value is 1.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

This command applies only to WCDMA or LTE networks. This command is valid only when a 3G or LTE modem with a SIM or USIM card is connected to a cellular interface.

Example

Delete the parameter profile of the 3G or LTE modem connected to cellular interface 0/0/0.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] profile delete 1
```

Related Topics

5.11.46 profile create

5.11.48 profile create lte-default

Function

The **profile create lte-default** command configures the default APN for an LTE network.

NOTE

The 1ELTE-L-S card does not support this command.

Format

profile create lte-default *apn* [**user** *username* **password** { **cipher** | **simple** } *password* **authentication-mode** { **chap** | **pap** }]

Parameters

Parameter	Description	Value
apn	Specifies the default APN for an LTE network.	The value is a string of 1 to 99 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user *username*	Specifies the user name provided by the carrier for accessing an external PDN network.	The value is a string of 1 to 127 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password { **cipher** | **simple** } *password*	Specifies the password provided by the carrier for accessing an external PDN network. There are two types of passwords. ● **cipher**: indicates the ciphertext password. You can enter either an explicit or ciphertext password, but the password is displayed in ciphertext in the configuration file. By default, passwords are in ciphertext. ● **simple**: indicates the plaintext password. You can enter a plaintext password, and the password is displayed in plaintext in the configuration file. **NOTICE** If you select **simple**, the password is saved in the configuration file in plaintext, posing security risks. You are advised to use the **cipher** option, which means that the passwords are encrypted before being stored.	The value is a string of 1 to 127 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
authentication-mode { **chap** | **pap** }	Specifies the authentication mode. ● **chap**: CHAP authentication ● **pap**: PAP authentication	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some carriers require that devices connect to LTE networks through the default APN, whereas other carriers do not have such requirements. If users are required to connect to a carrier's LTE network through the default APN, you can run the **profile create lte-default** command to configure the default APN for the LTE network.

You can run the **profile delete lte-default** command to delete the default APN configured for an LTE network.

Precautions

This command applies only to LTE networks. This command takes effect only when the LTE modem and SIM/USIM card are installed.

APNs vary depending on LTE network carriers. Obtain the APN from the local carrier.

For the 1LTE-Lt interface cards, the APN configured using the **profile create lte-default** command and the APN configured using the **apn** command overwrite each other. The two commands cannot be configured together.

Example

Set the default APN of an LTE network to CMNET.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] profile create lte-default CMNET
```

Related Topics

5.11.50 profile delete lte-default

5.11.49 profile create lte-default sim-id

Function

The **profile create lte-default sim-id** command configures the default APN for an LTE network.

By default, no default APN is configured for an LTE network.

Format

profile create lte-default *apn* [**user** *username* **password** { **cipher** | **simple** } *password***authentication-mode** { **chap** | **pap** }] **sim-id** *sim-id*

Parameters

Parameter	Description	Value
apn	Specifies the default APN for an LTE network.	The value is a string of 1 to 99 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user *username*	Specifies the user name provided by the carrier for accessing an external PDN network.	The value is a string of 1 to 127 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password { **cipher** | **simple** } *password*	Specifies the password provided by the carrier for accessing an external PDN network. There are two types of password type. ● **cipher**: Indicates the cipher text password type. The options are as follows: You can enter either explicit or ciphertext password, but is used to query the configuration file are displayed in ciphertext mode password, The default value is cipher type. ● **simple**: Indicates the type of a passwords in plaintext. You can enter passwords in plaintext, the configuration file, the password is displayed in plaintext mode. **NOTICE** If you select simple option, the password is saved in the configuration file in plaintext, causing security risks. You are advised to use the cipher option, the passwords are encrypted before being stored.	The value is a string of 1 to 127 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
authentication-mode { **chap** | **pap** }	Specifies the authentication mode. ● **chap**: CHAP authentication ● **pap**: PAP authentication	-
sim-id	Specifies the ID of the SIM card to which the default APN is bound.	The value is 1 or 2, corresponding to the device ID.

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some carriers require that devices connect to LTE networks through the default APN. In dual-card single-standby scenarios, if the two SIM cards need to connect to different carriers' LTE networks through different default APNs, you can run the **profile create lte-default sim-id** command to bind different default APNs to the IDs of the SIM cards, so that the corresponding default APN is delivered to the LTE module during a SIM card switchover.

You can run the **profile delete lte-default sim-id** command to delete the default APN configured for an LTE network.

Precautions

- This command only applies to LTE networks. This command takes effect only when the LTE modem and SIM/USIM card are installed.
- APNs vary depending on LTE network carriers. Obtain the APN from the local carrier.
- If two SIM cards connect to a carrier's LTE network through the same default APN, it is recommended that you run the **profile create lte-default** command to configure the default APN.
- If the **profile create lte-default** command has been configured, an error message will be displayed when the **profile create lte-default sim-id** command is configured. To run the **profile create lte-default sim-id** command, delete the original configuration first. Similarly, if the **profile create lte-default sim-id** command has been configured, you need to delete the command configuration first before running the **profile create lte-default** command.
- If the **profile create lte-default** command has been used to configure two SIM cards to connect to a carrier's LTE network through the same default APN, you can only delete the default APN configured for the LTE network using the **profile delete lte-default** command.

Example

Set the default APN for SIM card 1 to connect to an LTE network to CMNET.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] profile create lte-default CMNET sim-id 1
```

Related Topics

5.11.51 profile delete lte-default sim-id

5.11.50 profile delete lte-default

Function

The **profile delete lte-default** command deletes the default APN configured for an LTE network.

NOTE

The LTE data card E8278 does not support this command.

Format

profile delete lte-default

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some carriers require that devices connect to LTE networks through the default APN, whereas other carriers do not have such requirements. To delete the default APN configured using the **profile create lte-default** command for an LTE network, run the **profile delete lte-default** command.

Precautions

This command applies only to LTE networks. This command takes effect only when the LTE modem and SIM/USIM card are installed.

Example

Delete the default APN configured for an LTE network.

```
<Huawei> system-view
[Huawei] interface cellular 2/0/0
[Huawei-Cellular2/0/0] profile delete lte-default
```

Related Topics

5.11.48 profile create lte-default

 Copyright © Huawei Technologies Co., Ltd.

5.11.51 profile delete lte-default sim-id

Function

The **profile delete lte-default sim-id** command deletes the default APN configured for an LTE network.

Format

profile delete lte-default sim-id *sim-id*

Parameters

Parameter	Description	Value
sim-id	Specifies the ID of the SIM card to which the default APN to be deleted is bound.	The value is 1 or 2, corresponding to the device ID.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some carriers require that devices connect to LTE networks through the default APN, whereas other carriers do not have such requirements. To delete the default APN configured for an LTE network using the **profile create lte-default sim-id** command, run the **profile delete lte-default sim-id** command.

Precautions

- This command only applies to LTE networks. This command takes effect only when the LTE modem and SIM/USIM card are installed.
- If the default APN for the SIM card to connect to a carrier's LTE network has been configured using the **profile create lte-default sim-id** command, you can only delete the default APN configured for the LTE network using the **profile delete lte-default_sim-id** command.

Example

Delete the default APN for SIM card 1 to connect to an LTE network.

```
<Huawei> system-view
[Huawei] interface cellular 2/0/0
[Huawei-Cellular2/0/0] profile delete lte-default sim-id 1
```

Related Topics

5.11.49 profile create lte-default sim-id

5.11.52 reset counters cellular

Function

Using the **reset counters cellular** command, you can clear traffic statistics on a cellular interface or cellular channel interface.

Format

reset counters interface cellular [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting traffic statistics on a cellular interface or cellular channel interface, run the **reset counters cellular** command to clear the existing traffic statistics.

Example

Clear traffic statistics on cellular interface 0/0/0.

```
<Huawei> reset counters interface cellular 0/0/0
```

Related Topics

5.11.18 display interface cellular

 Copyright © Huawei Technologies Co., Ltd.

5.11.53 rssi-threshold

Function

The **rssi-threshold** command sets the RSSI threshold for successfully establishing a 3G/LTE link. Only when the RSSI is greater than the threshold, a 3G/LTE modem can establish a 3G/LTE link successfully.

The **undo rssi-threshold** restores the default setting.

By default, a 3G/LTE modem does not establish a 3G/LTElink based on the RSSI threshold.

Format

rssi-threshold *rssi-threshold*

undo rssi-threshold

Parameters

Parameter	Description	Setting
rssi-threshold	Specifies the RSSI threshold for successfully establishing a 3G/LTE link.	The value is an integer that ranges from -120 to -60, in dBm.

Views

Cellular interface view, Cellular channel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Usually, signal quality does not affect 3G/LTE link establishment by a 3G/LTE modem in dialup mode. You can use the **rssi-threshold** command to configure signal quality to affect establishment and disconnection of 3G/LTE links. When the RSSI is less than or equal to the threshold, the 3G/LTE modem cannot establish 3G/LTE link in dialup mode, and the established 3G/LTE links will be disconnected.

- When services have high 3G/LTE link quality requirements and will be greatly affected by poor link quality, set a large RSSI threshold to detect link quality and take measures in a timely manner.
- When services have low 3G/LTE link quality requirements and will be slightly affected by poor link quality, set a small RSSI threshold to prevent establishment failures and disconnection of 3G/LTE links.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- When you run the **rssi-threshold** *rssi-threshold* command multiple times on a cellular interface or cellular channel interface, only the latest configuration takes effect.
- When you run the **rssi-threshold** command on both the cellular interface and cellular channel interface, only the configuration on the cellular channel interface takes effect.

Example

Set the RSSI threshold for successfully establishing a 3G/LTE link to -100 dBm.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] rssi-threshold 100
```

5.11.54 service domain

Function

The **service domain** command configures the service domain of a 3G or an LTE modem.

By default, a 3G or an LTE modem works in both the CS domain and PS domain.

Format

service domain { **ps-only** | **combined** }

Parameters

Parameter	Description	Value
ps-only	Configures a 3G or an LTE modem to work only in the PS domain.	-
combined	Configures a 3G or an LTE modem to work in both the CS domain and PS domain.	-

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 3G network supports both the CS domain and PS domain. The LTE network supports only the PS domain. To prevent services in the CS domain from changing the network from an LTE network to a 3G network, you can run the **service domain ps-only** command to configure an LTE modem to work only in the PS domain when it connects to an LTE network.

Precautions

You can run the **display cellular** command to view the configured service domain of a 3G or an LTE modem.

After configuring the service domain of a 3G or an LTE modem, run the **modem reboot** command to restart the 3G or an LTE modem to make the configuration take effect.

Example

Configure an LTE modem to work only in the PS domain.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] service domain ps-only
Info: The service domain will take effect after modem reboot.
```

Related Topics

5.11.17 display cellular

5.11.55 sim-card reboot

Function

The **sim-card reboot** command restarts a SIM, USIM, or UIM card.

NOTE

Only the models with built-in ME909s terminal modules in V200R010C10 and later versions support this command.

Format

sim-card reboot

Parameters

None

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 3G/LTE modem can automatically detect whether a SIM, USIM, or UIM card is properly installed. To restart a SIM, USIM, or UIM card, run the **sim-card reboot** command.

Precautions

- When this command is executed to manually restart a SIM, USIM, or UIM card, services on the specified cellular interface will be interrupted.
- SIM, USIM, and UIM cards are not hot swappable.

  To ensure that the installed SIM, USIM, and UIM cards work properly, run the **sim-card reboot** command to manually restart the cards after hot swapping these cards.

  To check whether SIM, USIM, and UIM cards are working properly, run the **display cellular** command to view the **SIM Status** or **UIM Status** field.

Example

Restart a SIM, USIM, or UIM card.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] sim-card reboot
Warning: The 3G/LTE SIM/USIM card will reset. Continue? [Y/N]:y
```

Related Topics

5.11.17 display cellular

5.11.56 sim-id

Function

The **sim-id** command sets the ID of a SIM card on an APN profile to determine the master or backup SIM card to be bound to the APN profile.

The **undo sim-id** command restores the default setting.

The default ID of a SIM card is 1.

Format

sim-id *sim-id*

undo sim-id

Parameters

Parameter	Description	Value
sim-id	Specifies the ID of the SIM card bound to an APN profile.	The value is 1 or 2. ● The value 1 indicates that the APN profile is bound to the master SIM card. ● The value 2 indicates that the APN profile is bound to the backup SIM card.

Views

APN profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve data transmission reliability of the 3G or LTE link, you can use two 3G cellular interfaces One cellular interface functions as the master link to connect to a 3G or LTE network, the other cellular interface functions as the backup link to connect to another 3G or LTE network. When the master 3G or LTE link is faulty, traffic is automatically switched to the backup 3G or LTE link, improving reliability of access to the Internet.

However, some devices do not support two cellular interfaces or the costs of two cellular interfaces are high for users. Users can use a cellular interface supporting dual SIM cards. One SIM card functions as the master SIM card, the other SIM card functions as the backup SIM card. The master and backup SIM cards connect to different 3G or LTE networks. If dial-up fails because the account balance of the master SIM card is insufficient, the master SIM card is faulty, the 3G or LTE link signal quality is poor, or the connected 3G or LTE network is faulty, traffic is automatically switched to the backup SIM card, ensuring uninterrupted enterprise services.

You can run the **sim-id** command on an APN profile to set the ID of a SIM card to determine the master or backup SIM card to be bound to the APN profile.

- When the APN profile is bound to the master SIM card, the cellular interface can connect to the 3G or LTE network through the master SIM card.
- When the APN profile is bound to the backup SIM card, the cellular interface can connect to the 3G or LTE network through the backup SIM card.
- When the cellular interface are bound both to the APN profiles, the master SIM card is preferentially used to connect to the 3G or LTE network. Only if

dial-up fails because the account balance of the master SIM card is insufficient, the master SIM card is faulty, the 3G or LTE link signal quality is poor, or the connected 3G or LTE network is faulty, traffic is automatically switched to the backup SIM card.

Precautions

If you run the **sim-id** command in the same APN profile view multiple times, only the latest configuration takes effect.

The master and backup SIM cards cannot simultaneously work. Upon a SIM card switchover, traffic is interrupted for a short period.

Example

Set the ID of the SIM card bound to the APN profile **ltenet** to 2, indicating that **ltenet** is bound to the backup SIM card.

```
<Huawei> system-view
[Huawei] apn profile ltenet
[Huawei-apn-profile-ltenet] sim-id 2
```

Related Topics

5.11.2 apn profile

5.11.3 apn-profile

5.11.57 sim switch to

5.11.58 sim switch rssi-threshold

5.11.57 sim switch to

Function

The **sim switch to** command enables manual switchover between SIM cards.

Format

sim switch to *sim-id*

Parameters

Parameter	Description	Value
sim-id	Specifies the ID of the SIM card to which 3G services are switched.	The value is 1 or 2. • The value 1 indicates that 3G services are manually switched to the master SIM card. • The value 2 indicates that 3G services are manually switched to the backup SIM card.

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view, Cellular channel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When automatic SIM card switchover is not configured or the switchover condition is not met, you can run the **sim switch to** command to manually switch between SIM cards.

Precautions

Manual switchover between SIM cards leads to service interruption for a short period and affects service transmission. Exercise caution when performing this operation.

Example

Manually switch 3G or LTE services to the backup SIM card.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] sim switch to 2
```

Related Topics

5.11.3 apn-profile

5.11.56 sim-id

5.11.58 sim switch rssi-threshold

5.11.58 sim switch rssi-threshold

Function

The **sim switch rssi-threshold** command enables automatic switchover between SIM cards based on the received signal strength indicator (RSSI) threshold.

The **undo sim switch rssi-threshold** command disables automatic switchover between SIM cards based on the RSSI threshold.

By default, a cellular interface does not switch between SIM cards based on the RSSI threshold.

Format

sim switch rssi-threshold *rssi-threshold*

undo sim switch rssi-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rssi-threshold	Specifies the RSSI threshold for switching between SIM cards. When the received signal strength is lower than the RSSI threshold, the cellular interface automatically switches between SIM cards. For example, if the RSSI threshold is -105 dBm, the SIM cards are switched when the received signal strength is lower than -105 dBm.	The value is an integer that ranges from -120 to -60, in dBm. The recommended RSSI threshold is -105 dBm.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two SIM cards are available, if the 3G or LTE link signal quality on one SIM card is poor and affects data transmission, the other SIM card needs to provide 3G or LTE services in time.

The RSSI indicates the strength of signals received on a cellular interface. You can run the **sim switch rssi-threshold** command to configure automatic switchover between SIM cards based on the RSSI threshold. When the received signal strength is lower than the RSSI threshold, the cellular interface automatically switches between SIM cards.

Precautions

Set a proper RSSI threshold based on the 3G or LTE link signal quality.

- A large RSSI threshold (such as -70 dBm) results in frequent switchovers between SIM cards. Traffic is frequently interrupted.
- A small RSSI threshold (such as -110 dBm) results in no switchover between SIM cards even if the 3G or LTE link signal quality is poor. The SIM card providing poor-quality 3G or LTE services is always in use.

If you run the **sim switch rssi-threshold** *rssi-threshold* command in the same cellular interface view multiple times, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure automatic switchover between SIM cards when the signal strength is lower than -105 dBm.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] sim switch rssi-threshold 105
```

Related Topics

5.11.56 sim-id

5.11.57 sim switch to

5.11.59 sim switch-back enable

Function

The **sim switch-back enable** command enables automatic switchback to the master SIM card.

The **undo sim switch-back enable** command disables automatic switchback to the master SIM card.

By default, traffic on the backup SIM card is not automatically switched back to the master SIM card.

Format

sim switch-back enable [**timer** *time*]

undo sim switch-back enable

Parameters

Parameter	Description	Value
timer *time*	Indicates the specified period of time after which traffic on the backup SIM card is automatically switched back to the master SIM card. When this parameter is not specified, traffic on the backup SIM card is switched back to the master SIM card after 60 minutes.	The value is an integer that ranges from 1 to 65535, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When 3G or LTE link signal quality is poor on the master SIM card or the connected carrier network is faulty, traffic is automatically switched to the backup SIM card. After a period of time, 3G or LTE link signal quality on the master SIM card becomes good or the connected carrier network is recovered. You can run the **sim switch-back enable** command to automatically switch traffic back to the master SIM card.

Precautions

If you run the **sim switch-back enable timer** *time* command in the same cellular interface view multiple times, only the latest configuration takes effect.

After the **sim switch-back enable** [**timer** *time*] command is executed to enable switchback from the backup SIM card to the master SIM card, you need to verify that the 3G or LTE link on the master SIM card is normal after the period specified by **timer** *time*. Otherwise, traffic is frequently switched between the master and backup SIM cards, affecting service transmission.

Example

Enable automatic traffic switchback from the backup SIM card to the master SIM card.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] sim switch-back enable
```

Related Topics

5.11.56 sim-id

5.11.57 sim switch to

5.11.58 sim switch rssi-threshold

5.11.60 sms delete interface cellular

Function

The **sms delete interface cellular** command deletes SMS messages saved in the SIM card.

Format

sms delete interface cellular *interface-number* { *sms-id* | **all** }

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface.	-
sms-id	Specifies the ID of an SMS message to be deleted.	The value is an integer that ranges from 0 to 255.
all	Deletes all SMS messages.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can receive SMS messages sent by user mobile phones and save the SMS messages in the SIM card. If the number of SMS messages saved in the SIM card exceeds the maximum number, you can run this command to delete the SMS messages.

Example

Delete all SMS messages saved in the SIM card.

```
<Huawei> system-view
[Huawei] sms delete interface cellular 2/0/0 all
Info: SMS delete success.
```

5.11.61 sms send interface cellular

Function

The **sms send interface cellular** command sends an SMS message to a specified destination number.

Format

sms send interface cellular *interface-number destination-telephone-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a cellular interface or cellular channel interface.	-
destination-telephone-number	Specifies the destination number that receives the SMS message.	The value is a string of 1 to 21 characters without spaces. It can contain an asterisk (*), a plus sign (+), a number sign (#), and digits 0 to 9. The plus sign (+) can be used only at the start of a character string. If a character string starts with a plus sign (+), the maximum string length is 21. If a character string starts with other characters, the maximum string length is 20.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To send an SMS message to a specified mobile number, you can run this command and write the SMS message to send it to the destination number.

Precautions

This command is an interactive command. After running the command, you can press **Enter** and enter the SMS message as prompted. Currently, the device can only send English SMS messages.

The content of an SMS message is a string of 0 to 160 case-sensitive characters with spaces. An SMS message uses a percent sign (%) as the terminator. The percent sign (%) is not included in the SMS message content.

A line feed in the SMS message content is considered as two characters, and cannot be deleted after being entered.

 Copyright © Huawei Technologies Co., Ltd.

The 1LTE-Lt and 1LTE-Lt-7 cards do not support the function of sending SMS messages using China Telecom SIM cards.

Example

Configure the device to send the SMS message "I have received your message." to the user with the mobile number 13812345678.

```
<Huawei> system-view
[Huawei] sms send interface cellular 2/0/0 +8613812345678
Info: Please input sms content within 160 characters, end with character '%':
I have received your message.%
Info: SMS send success.
```

5.11.62 sms-pool

Function

The **sms-pool** command displays the SMS service pool view.

The **undo sms-pool** command deletes all configurations in the SMS service pool view.

By default, there is no configuration in the SMS service pool view.

Format

sms-pool

undo sms-pool

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before running the **sms item** command to configure an SMS service, run the **sms-pool** command to enter the SMS service pool view.

Precautions

If an SMS service in the SMS service pool has been referenced by the **sms send-item** command, short messages cannot be sent after the **undo sms-pool** command is run to delete the configuration from the SMS service pool.

Example

Display the SMS service pool view.

```
<Huawei> system-view
[Huawei] sms-pool
[Huawei-sms-pool]
```

Related Topics

5.11.63 sms item

5.11.64 sms send-item

5.11.63 sms item

Function

The **sms item** command configures the phone numbers for receiving short messages, and short message content in the SMS service pool.

The **undo sms item** command deletes the configured SMS services.

By default, no SMS service is configured in the SMS service pool.

Format

sms item *item-id* **telephone-number** *tel-number* &<1-3> **content**

undo sms item *item-id*

Parameters

Parameter	Description	Value
item-id	Specifies the ID of an SMS service.	The value is an integer that ranges from 1 to 20.
telephone-number *tel-number*	User phone number for receiving short messages. A maximum of three phone numbers can be specified. **NOTE** A user's phone number must be valid; otherwise, the user cannot receive short messages.	The value is a string of 1 to 21 characters. The value can contain the digits 0-9 and plus sign (+), and does not support spaces. In addition, the plus sign (+) can only be the first character in the value. When the first character is the plus sign (+), the maximum value length is 21. When the first character is a digit, the maximum value length is 20.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
content	Specifies the short message content. **NOTE** This command is an interactive command. After running the command, press **Enter** and enter the short message content as prompted.	The value is a string of 1 to 160 case-sensitive characters with spaces. The value ends with %.

Views

SMS service pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the SMS service is configured in the SMS service pool, run the **sms send-item** command on a service interface to reference the SMS service with a specified ID. When the service interface status changes, the short message preset in the SMS service is sent to the specified user phone number.

Precautions

A maximum of 20 SMS services can be configured in an SMS service pool. Each SMS service can be preset with 3 phone numbers. Each short message can contain at most 160 characters. The short message content is configured to end with %.

When the SMS service with a specified ID is referenced, it can be modified and can be deleted. If the SMS service is deleted, short messages cannot be sent.

Example

Configure the SMS service with ID 1 to send the short message "The interface is in Up state." to the phone number +8613812345678.

```
<Huawei> system-view
[Huawei] sms-pool
[Huawei-sms-pool] sms item 1 telephone-number +8613812345678 content
Info: Please input the sms content within 160 characters, end with '%':
The interface is in Up state.%
```

Related Topics

5.11.62 sms-pool

5.11.64 sms send-item

5.11.64 sms send-item

Function

The **sms send-item** command configures the SMS alarm function on an interface to send a specified short message alarm to specific users when the interface status changes.

The **undo sms send-item** command deletes the configured SMS alarm function.

By default, the SMS alarm function is not configured on an interface.

Format

sms send-item *item-id* **track-interface** { **up** | **down** } [**after** *time*]

undo sms send-item *item-id*

Parameters

Parameter	Description	Value
item-id	Specifies the ID of the SMS service to be referenced. **NOTE** The value of *item-id* must have been configured using the **sms item** command; otherwise, the command cannot be run.	The value is an integer that ranges from 1 to 20.
track-interface { **up** | **down** }	Sends a short message alarm when detecting that the link status changes.	-
after *time*	Specifies the delay for sending a short message alarm. If **after** *time* is not specified, a short message alarm is sent immediately. After this parameter is specified, a short message alarm is sent only when the link status remains unchanged within the value of *time*. If the link status changes within the time, no short message alarm is sent.	The value is an integer that ranges from 1 to 65535, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Views

Cellular interface view, ATM interface view, serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario of active/standby interface backup, when the active and standby links are switched, the active/standby interface status changes. Users can view the alarm on the device to know the interface status change. If users want to sense the interface status change anytime and anywhere, run this command to configure the SMS alarm function on the interface. After the function is configured, the alarm with the interface status change is sent to users in a short message.

Prerequisites

The SMS service with a specified ID has been configured using the **sms item** command.

Precautions

Currently, the SMS alarm function can be configured on interfaces only when cellular, ATM, and serial interfaces are used as the active and standby interfaces.

This command can be run on each interface at most four times, and the latest configuration does not override the previous ones.

Example

Configure the SMS alarm function on Cellular2/0/0 to send the short message "The interface is in Up state." to the phone number +8613812345678 when the link on the interface goes Up. Send the short message "The interface is still in Up state." to the phone number if services are not switched back to the active link after 120 minutes.

```
<Huawei> system-view
[Huawei] sms-pool
[Huawei-sms-pool] sms item 1 telephone-number +8613812345678 content
Info: Please input the sms content within 160 characters, end with '%':
The interface is in Up state.%
[Huawei-sms-pool] sms item 2 telephone-number +8613812345678 content
Info: Please input the sms content within 160 characters, end with '%':
The interface is still in Up state.%
[Huawei-sms-pool] quit
[Huawei] interface cellular 2/0/0
[Huawei-Cellular2/0/0] sms send-item 1 track-interface up
[Huawei-Cellular2/0/0] sms send-item 2 track-interface up after 120
```

Related Topics

5.11.63 sms item

5.11.65 sms service-center-address

Function

The **sms service-center-address** command configures the SMS center number on a cellular interface.

The **undo sms service-center-address** command deletes the configured SMS center number.

By default, no SMS center number is configured on a cellular interface.

Format

sms service-center-address *service-center-number*

undo sms service-center-address

Parameters

Parameter	Description	Value
service-center-number	Specifies the SMS center number.	The value is a string of 1 to 21 characters. The value can contain the digits 0-9 and plus sign (+). It does not support spaces. In addition, the plus sign (+) can only be the first character in the value. When the first character is the plus sign (+), the maximum value length is 21. When the first character is a digit, the maximum value length is 20.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command on a cellular interface to configure the SMS center number used for the interface to send short messages.

Precautions

Only one SMS center number can be configured on each cellular interface.

Example

Configure the SMS center number +8613800000000 on Cellular2/0/0.

```
<Huawei> system-view
[Huawei] interface cellular 2/0/0
[Huawei-Cellular2/0/0] sms service-center-address +8613800000000
```

5.11.66 snmp-agent trap enable feature-name ifmtrap

Function

The **snmp-agent trap enable feature-name ifmtrap** command enables the trap function for the IFM module.

The **undo snmp-agent trap enable feature-name ifmtrap** command disables the trap function for the IFM module.

By default, the **hw3GPinModify** trap function is enabled and other trap functions for the IFM module are disabled.

Format

snmp-agent trap enable feature-name ifmtrap [**trap-name** { **hw3gmibtrapcellidchange** | **hw3gpinmodify** | **hwportphysicalethfullduplexclear** | **hwportphysicalethhalfduplexalarm** | **hwportspeedchangetrap** }]

undo snmp-agent trap enable feature-name ifmtrap [**trap-name** { **hw3gmibtrapcellidchange** | **hw3gpinmodify** | **hwportphysicalethfullduplexclear** | **hwportphysicalethhalfduplexalarm** | **hwportspeedchangetrap** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for a specified event. If this parameter is not specified, all trap functions for the IFM module are enabled.	-
hw3gmibtrapcellidchange	Enables the trap function for the cell ID change.	-

Parameter	Description	Value
hw3gpinmodify	Enables the trap function for the PIN change.	-
hwportphysicalethfullduplexclear	Enables the trap function for the interface duplex mode change from half-duplex to full-duplex.	-
hwportphysicalethhalfduplexalarm	Enables the trap function for the interface duplex mode change from full-duplex to half-duplex.	-
hwportspeedchangetrap	Enables the trap function for the interface rate change.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can specify **trap-name** to enable the trap function for a specified event.

Example

Enable the trap function for the interface duplex mode change from full-duplex to half-duplex.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name ifmtrap trap-name
hwportphysicalethhalfduplexalarm
```

Related Topics

5.11.23 display snmp-agent trap feature-name ifmtrap all

5.11.67 user

Function

The **user** command configures the user name, password, and authentication mode for accessing an external PDN network.

The **undo user** command deletes the user configured for accessing an external PDN network.

By default, the user name, password, and authentication mode for accessing an external PDN network are not configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

user name *username* **password** { **cipher** | **simple** } *password* [**authentication-mode** { **auto** | **pap** | **chap** }]

undo user name *username*

Parameters

Parameter	Description	Value
name *username*	Specifies the user name for accessing an external PDN network, which is provided by the carrier.	The value is a string of 1 to 64 case-sensitive characters without spaces.
cipher	Displays the password in cipher text.	-
simple	Displays the password in plain text. **NOTE** When you specify **simple**, the password is saved in plain text in the configuration, which brings potential security risks. You are advised to specify **cipher** to save the password in the cipher text.	-
password	Specifies the user password for accessing an external PDN network, which is provided by the carrier.	The value is a case-sensitive character string without spaces. If **simple** is specified, the password is in plain text and contains 1 to 32 characters. If **cipher** is specified, the password is either in cipher text containing 24 to 68 characters, for example, %^%#k5bf>8df@:_;Na'+R"U,#L#w88HE1M.L4YY2~W2u0%RDL#z#%^%#, or in plain text containing 1 to 32 characters, for example, 214357.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
authentication-mode { **auto** | **pap** | **chap** }	Specifies the authentication mode. ● **auto**: PAP or CHAP authentication ● **pap**: PAP authentication ● **chap**: CHAP authentication When the **authentication-mode** parameter is not specified, the **auto** mode is used by default. **NOTE** Select a proper authentication mode based on the carrier network. PAP authentication provides lower security. When you specify **auto** or **pap** to enable the device to use PAP authentication, the password is transmitted in plain text on the network. This brings potential security risks.	-

Views

APN profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user uses a cellular interface to access an external PDN network through a 3G or LTE network. To ensure information security, the external PDN network authenticates the access user. The user can use the cellular interface to perform data communication with the external PDN network through a 3G or LTE network only after the user passes the authentication.

Precautions

Contact the carrier when configuring the user name, password, and authentication mode.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the user name, password, and authentication mode for accessing the external PDN network.

```
<Huawei> system-view
[Huawei] apn profile 3gnet
[Huawei-apn-profile-3gnet] user name jack password cipher huawei@123 authentication-mode chap
```

Related Topics

5.11.2 apn profile

5.12 ISDN BRI Interface Configuration Commands

5.12.1 loopback (ISDN BRI interface view)

Function

Using the **loopback** command, you can configure loopback detection on an ISDN BRI interface.

Using the **undo loopback** command, you can disable loopback detection on an ISDN BRI interface.

By default, loopback detection is disabled on an ISDN BRI interface.

Format

loopback { **local** | **remote** } [**b1** | **b2** | **both**]

undo loopback

Parameters

Parameter	Description	Value
local	Configures local loopback on an ISDN BRI interface.	-
remote	Configures remote loopback on an ISDN BRI interface.	-
b1	Configures loopback detection on the B1 channel.	-
b2	Configures loopback detection on the B2 channel.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
both	Configures loopback detection on both the B1 channel and B2 channel.	-

Views

ISDN BRI interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function monitors the interface status or cable status and must be disabled when devices are working properly.

- In local loopback mode, the local device loops back outgoing packets to itself to test whether it is working properly.
- In remote loopback mode, the local device loops back the packets received from its peer device to the peer device to test whether the link between the two devices is working properly.

Example

Configure loopback detection on an ISDN BRI interface.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] loopback remote b1
```

Related Topics

5.12.2 display interface bri

5.12.2 display interface bri

Function

Using the **display interface bri** command, you can view information about an ISDN BRI interface, including the running status and statistics.

Format

display interface bri [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an ISDN BRI interface.	If no interface number is specified, information about all ISDN BRI interfaces including B channels and D channels is displayed. **NOTE** • The interface number of a signaling channel (D channel) is in the format of *interface-number*. • In a data channel (B channel), the interface number of the B1 channel is in the format of *interface-number*.1 and that of the B2 channel is in the format of *interface-number*.2.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the ISDN BRI interface status or locating faults on an ISDN BRI interface, run the **display interface bri** command to obtain the interface information, including the running status and traffic statistics. You can collect traffic statistics and locate faults on the interface according to the command output.

Example

Display information about BRI 1/0/0.

```
<Huawei> display interface bri 1/0/0
Bri1/0/0 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Bri1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
baudrate is 192000 bps,  Timeslot(s) Used: 1, 2
Internet Address is 2.2.2.1/24
Encapsulation is ISDN
Current system time: 2011-06-28 17:12:30
Last 300 seconds input rate 0 bytes/sec 0 bits/sec 0 packets/sec
```

```
Last 300 seconds output rate 0 bytes/sec 0 bits/sec 0 packets/sec

Input: 0 packets, 0 bytes
  No Buffers:            0
Output: 0 packets, 0 bytes
  No Buffers:            0,  Underruns:            0

    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

Display information about BRI 1/0/0:1.

```
<Huawei> display interface bri 1/0/0:1
Bri1/0/0:1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Bri1/0/0:1 Interface
Route Port,The Maximum Transmit Unit is 1500
baudrate is 64000 bps,  Timeslot(s) Used: 1
Link layer protocol is PPP
LCP initial
Last physical up time   : 2011-06-22 13:07:41
Last physical down time : 2011-06-22 13:06:11
Current system time: 2011-06-28 17:15:12
Last 300 seconds input rate 0 bytes/sec 0 bits/sec 0 packets/sec
Last 300 seconds output rate 0 bytes/sec 0 bits/sec 0 packets/sec

Input: 0 packets, 0 bytes
  No Buffers:            0
Output: 0 packets, 0 bytes
  No Buffers:            0,  Underruns:            0

    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

Table 5-43 Description of the display interface bri command output

Item	Description
Bri1/0/0 current state	Current physical status of the ISDN BRI interface: • UP: indicates that the interface is physically Up. • DOWN: indicates that the interface is physically Down. • Administratively down: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: • UP: indicates that the link layer-protocol status of the interface is Up. • DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Description	Interface description.
baudrate	Interface baud rate.
Timeslot(s) Used	Timeslots used in a data channel.

Item	Description
Internet Address is	IP address and mask length configured on the interface. According to different assignment modes of IP addresses, this parameter is displayed in the following ways: ● If IP address is configured manually, the parameter is displayed as **Internet Address is 1.1.1.1/24.** ● If IP address is assigned by DHCP, the parameter is displayed as **Internet Address is allocated by DHCP, 1.1.1.1/24.** If no IP address is configured on the interface, the parameter is displayed as **Internet protocol processing : disabled.**
Encapsulation is ISDN	The packet encapsulation format is ISDN.
Link layer protocol	Link layer protocol of the ISDN BRI interface.
LCP initial	A PPP connection is established successfully.
Last physical up time	Last time the link layer protocol of the interface goes Up.
Last physical down time	Last time the link layer protocol of the interface goes Down.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH: MM: SS UTC±HH: MM DST format.
No Buffers	Number of received packets that cannot be buffered.
Underruns	Number of sent packets below the lower limit of the FIFO queue.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

5.12.3 interface bri

Function

Using the **interface bri** command, you can enter the signaling channel (D channel) of an ISDN BRI interface.

Format

interface bri *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an ISDN BRI interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting attributes for an ISDN BRI interface, run the **interface bri** command to enter the signaling channel (D channel) of an ISDN BRI interface.

Example

Enter the signaling channel (D channel) of an ISDN BRI interface.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0]
```

Related Topics

5.12.2 display interface bri

5.12.4 mtu (ISDN BRI interface view)

Function

Using the **mtu** command, you can set the maximum transmission unit (MTU) for an ISDN BRI interface.

Using the **undo mtu** command, you can restore the default MTU.

By default, the MTU of an ISDN BRI interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of an ISDN BRI interface.	The value is an integer, in bytes. The value depends on the device.

Views

ISDN BRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Whenever receiving an IP packet, the IP layer determines the next-hop interface for the packet and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU.

If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To prevent packet loss on the network, large packets must be forcibly fragmented. The **mtu** command is used to set the size of a fragment.

Precautions

If you run the **mtu** command multiple times in the same ISDN BRI interface view, only the latest configuration takes effect.

Follow-up Procedure

Run the **shutdown** and **undo shutdown**/**restart** commands to restart the related physical interface to make the configuration take effect.

Example

Set the MTU of an ISDN BRI interface to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] mtu 1200
[Huawei-Bri1/0/0] restart
```

 Copyright © Huawei Technologies Co., Ltd.

5.12.5 set workmode bri

Function

The **set workmode bri** command sets the working mode of a 2BST voice card.

By default, a 2BST voice card works in Network Termination (NT) mode.

Format

set workmode slot *slot-id* **bri bri-voice** { **nt-mode** | **te-mode** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a 2BST voice card.	Run the **display device** command to view slot IDs and types of interface cards and find the slot ID with 2BST displayed. Then run the **display workmode** command to view the interface card work mode on the device.
bri-voice { **nt-mode** | **te-mode** }	Indicates the working mode of a 2BST voice card. ● **nt-mode**: The 2BST voice card works in NT mode. ● **te-mode**: The 2BST voice card works in Terminal Equipment (TE) mode.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device can function as the ISDN user-side or network-side device.

- When the device functions as the ISDN user-side device, configure the 2BST voice card to work in TE mode.
- When the device functions as the ISDN network-side device, configure the 2BST voice card to work in NT mode.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After this command is executed, the configured service takes no effect.

After this command is used, the system prompts you to reset the 2BST voice card to make the new working mode take effect. If you select **Yes**, the system resets the interface card. Otherwise, you need to run the **reset slot** command to manually reset the interface card to make the new working mode take effect.

Example

Configure the 2BST voice card in slot 2 to work in TE mode.

```
<Huawei> system-view
[Huawei] set workmode slot 2 bri bri-voice te-mode
Warning: Changing the working mode will reset the board in slot 2. Continue? [y/
n]:y
INFO: Resetting board[2] succeeded.
```

Related Topics

4.1.3 display device

5.5.9 display workmode

4.2.13 reset slot

5.12.6 shutdown (ISDN BRI interface view)

Function

Using the **shutdown** command, you can shut down an ISDN BRI interface.

Using the **undo shutdown** command, you can enable an ISDN BRI interface.

By default, an ISDN BRI interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

ISDN BRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying parameters of an ISDN BRI interface, run the **shutdown** and **undo shutdown** commands on the interface for the modifications to take effect.

When an ISDN BRI interface is not connected to a cable, run the **shutdown** command to shut down the interface to prevent interference.

Precautions

- Data frames may be lost if you disable an interface during data transmission. Exercise caution when you use the **shutdown** command.
- Running the **shutdown** and **undo shutdown** commands is equivalent to running the **restart** command.

Example

Shut down an ISDN BRI interface.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] shutdown
```

Related Topics

5.12.2 display interface bri

5.13 POS Interface Commands

5.13.1 clock (POS interface view)

Function

The **clock** command sets the clock mode of a POS interface.

The **undo lock** command restores the default setting.

By default, a POS interface works in slave clock mode.

Format

clock { **master** | **slave** | **system** }

undo clock

Parameters

Parameter	Description	Value
master	Configures a POS interface to work in master clock mode.	-
slave	Configures a POS interface to work in slave clock mode.	-
system	Configures a POS interface to work in system clock mode.	-

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To exchange data correctly, communicating parties must work in clock synchronization state.

A POS interface supports the following clock modes:

- master: uses the internal clock signal.
- slave: uses the line clock signal.
- system: uses the MPU clock signal.

Precautions

When the POS interfaces of the router and a remote device are directly connected, set the clock mode of one end to master and that of the peer end to slave.

When the POS interface of the router is connected to the SONET or SDH network, set the clock mode of the POS interface to slave because the SONET or SDH network clock has a higher accuracy than the POS interface.

When the MPU on the router obtains the clock with high accuracy from the upstream device and the router needs to synchronize the clock to downstream device, the interface on the router must be configured to work in system clock mode. Moreover, the interface on the downstream device must be configured to work in slave clock mode.

Example

Sets the clock mode to master on POS 2/0/0.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] clock master
```

Related Topics

5.13.3 display interface pos

5.13.2 crc (POS interface view)

Function

The **crc** command sets the CRC field length of a POS interface.

The **undo crc** restores the default setting.

By default, the CRC field length is 32 bits.

Format

crc { **16** | **32** }

undo crc

Parameters

Parameter	Description	Value
16	Sets the CRC field length to 16 bits.	-
32	Sets the CRC field length to 32 bits.	-

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A POS interface supports 16-bit and 32-bit CRC fields. CRC checks the data consistency and uses a complex calculation with high accuracy. A 32-bit field can achieve higher accuracy than a 16-bit field but uses more resources.

Precautions

Ensure that the same CCR field length is configured for both devices on the link. Otherwise, the two devices cannot be connected.

Example

Set the CRC field length to 16 bits on POS 2/0/0.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] crc 16
```

Related Topics

5.13.3 display interface pos

5.13.3 display interface pos

Function

The **display interface pos** command displays the configuration and status of a POS interface.

Format

display interface pos [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Specifies the POS interface ID. If no interface ID is specified, the configuration and status of all POS interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the interface status or locate faults on an interface, run the **display interface pos** command to obtain the status of the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Example

Display the configuration and status of POS 2/0/0.

```
<Huawei> display interface pos 2/0/0
Pos2/0/0current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Pos2/0/0Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 10.1.1.1/24
Link layer protocol is PPP
LCP opened, IPCP opened
Last physical up time   : 2012-08-09 17:25:11
Last physical down time : 2012-08-09 17:25:09
Current system time: 2012-08-09 19:33:13
  Frame-format is Sonet,
  Source Clock is Slave,
  Source Loopback is Not Set.
  Tx: J0: 25, J1: NULL, C2: 0x16
  Rx: J0: 25, J1: NULL, C2: 0x16
Regenerator section:
  Alarm: none
  Error: 0 BIP
Multiplex section:
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path(VC-4-1):
  Alarm: none
  Error: 65532 BIP, 0 REI
Last 300 seconds input rate 16 bits/sec 0 packets/sec
Last 300 seconds output rate 97888600 bits/sec 8223 packets/sec
```

 Copyright © Huawei Technologies Co., Ltd.

```
Input: 145902099 packets, 119450564927 bytes
  Total error:            0,    CRC:                  0
  Giants:                 0,    Runts:                0
Output: 218481195 packets, 115763190175 bytes
  Total error:            0
    Input bandwidth utilization  : 0.01%
    Output bandwidth utilization :   63%
```

Table 5-44 Description of the display interface pos command output

Item	Description
Pos2/0/0 current state	Physical status of POS 2/0/0 ● UP: The interface is physically Up. ● DOWN: The interface has a fault. ● Administratively DOWN: The administrator uses the **shutdown** command on the interface.
Line protocol current state	Link-layer protocol status of the interface ● UP: The link-layer protocol of the interface is in the Up state. ● DOWN: The link-layer protocol of the interface is in the Down state or no IP address is assigned to the interface.
Description	Description of the interface The description contains a maximum of 242 case-sensitive characters, with spaces supported.
The Maximum Transmit Unit	MTU of the interface
Hold timer	Polling interval of the interface
Internet Address is	IP address and mask of the interface The value is displayed in either of the following formats: ● For a statically configured IP address: Internet Address is 1.1.1.1/24 ● For an IP address allocated by DHCP: Internet Address is allocated by DHCP, 1.1.1.1/24
Link layer protocol is	Link-layer protocol of the interface ● FR ● PPP ● HDLC
LCP reqsent	LCP negotiation being request for sending
Last physical up time	Last time the interface went Up physically If the value of this field is displayed as "-", the physical status of the interface does not change.

Item	Description
Last physical down time	Last time the interface went Down physically If the value of this field is displayed as "-", the physical status of the interface does not change.
Frame-format	Frame format
Source Clock	Clock mode
Source Loopback	Whether to configure loopback detection
Tx: J0: NULL, J1: NULL, C2: 0x16	Sent overhead bytes
Rx: J0: NULL, J1: NULL, C2: 0x0	Received overhead bytes

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm	Traps. ● Loss of Signal (LOS): The LOS state is declared when the bit error rate (BER) is larger than 10e-3 because the input optical power is zero, too low, or too high. LOS is also detected when an all-0s or an all-1s pattern on the incoming SONET signal lasts 20 (+/-3) microseconds or longer. The LOS alarm is removed when two consecutive valid framing patterns (A1, A2) are received within the specified period. ● Out of Frame (OOF): The OOF alarm is generated when five or more consecutive received frames (625 microseconds) contain no correct A1 and A2 bytes. ● Loss of Frame (LOF): The LOF alarm is generated when an OOF defect on the incoming SONET signal persists for 3 milliseconds. The LOF alarm is cleared when frames received by the receiving terminal contain correct A1 and A2 bytes within 1 millisecond. ● Trace Identifier Mismatch (TIM): The TIM alarm is generated on the receiving terminal when the values of J0 and J1 bytes in received frames differ from the expected values. After a TIM alarm is generated, the receiving terminal sends an RDI trap to the receiving terminal to indicate the defect on the remote end. The TIM alarm is cleared when the values are the same as the expected values. ● Alarm Indication Signal (AIS): The line AIS (LAIS) alarm is received on the local terminal when it receives three or five consecutive frames whose K2 byte (bit 6 to bit 8) is 111. After receiving an LAIS alarm, the local terminal must send an LRDI trap to the remote terminal. The LAIS alarm is cleared when the local terminal receives three or five consecutive frames whose K2 byte (bit 6 to bit 8) is not 111. When the local terminal receives three consecutive frames containing AIS_ind, a path AIS (PAIS) is generated. When an AIS alarm is generated, the protocol status changes to Down, causing packet transmission interruption.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Remote Defect Indication (RDI): The receiving terminal sends an RDI trap to the sending terminal to inform it of signal degrade. • Loss of Pointer (LOP): The LOP alarm is generated when the receiving terminal receives eight consecutive frames containing invalid pointers or new data flags (NDFs). After receiving the LOP alarm, the receiving terminal sends an RDI trap to the sending terminal to inform it of the defect. • Payload Label Mismatch (PLM): The PLM alarm is generated on the receiving terminal when the values of C2 byte in the received frame differs from the expected value. After receiving a PLM alarm, the receiving terminal sends an RDI trap to the sending terminal to indicate the defect on the peer end. • Unequipped (UNEQ): The UNEQ alarm is generated when C2 bytes in the received five consecutive frames are all 0s.
Last 300 seconds input rate	Packet receiving rate (bits per second and packets per second) in the last 300 seconds
Last 300 seconds output rate	Packet sending rate (bits per second and packets per second) in the last 300 seconds
Input	Total number of received packets
Output	Total number of sent packets
Input bandwidth utilization	Inbound bandwidth usage
Output bandwidth utilization	Outbound bandwidth usage

Related Topics

5.13.6 link-protocol (POS interface view)

5.13.4 flag (POS interface view)

Function

The **flag** command sets the overhead bytes for a SONET/SDH frame.

The **undo flag** command restores the default setting.

The default overhead bytes for the SDH are used: The C2 overhead byte is 0x16; J0 and J1 overhead bytes are blank.

Format

flag c2 *c2-value*

flag j0 { **1byte-mode** *value* | **16byte-mode** *value* | **64byte-mode** *value* }

flag j1 { **1byte-mode** *value* | **16byte-mode** *value* | **64byte-mode** *value* }

undo flag { **c2** | **j0** | **j1** }

Parameters

Parameter	Description	Value
c2 *c2-value*	Specifies the path signal label byte. It is contained in the higher-order path overhead and is used to specify the multiplexing structure and the attribute of the information payload in a Virtual Container (VC) frame.	The value is an integer that ranges from 0 to 255.
j0	Specifies the regeneration section trace byte. It is contained in the RSOH and is used to detect the continuity of a connection between two interfaces on the section.	-
j1	Specifies the Higher-Order VC-N path trace byte. It is carried in the higher-order path overhead and is used to detect the continuity of the connection between two interfaces on a channel.	-
1byte-mode *value*	Indicates that the J0/J1 overhead byte mode is 1byte-mode.	The value is a string of 1 character.
16byte-mode *value*	Indicates that the J0/J1 overhead byte mode is 16byte-mode.	The value is a string of 1 to 15 characters.
64byte-mode *value*	Indicates that the J0/J1 overhead byte mode is 64byte-mode	The value is a string of 1 to 62 characters.

Views

POS interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SDH frames contain various overhead bytes that are used to implement operation and maintenance functions such as layered management of SDH transport networks. J1, J0, and C2 are used for interoperatability between devices of different countries, areas, or manufacturers.

Precautions

C2, J0, and J1 at the receive and transmit ends should be the same; otherwise, the two ends fail to communicate.

Example

Set the overhead byte J0.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] flag j0 16byte-mode aabb
```

Related Topics

5.13.3 display interface pos

5.13.5 frame-format (POS interface view)

Function

The **frame-format** command sets the frame format for a POS interface.

The **undo frame-format** command restores the default setting.

By default, the frame format is SDH.

Format

frame-format { **sdh** | **sonet** }

undo frame-format

Parameters

Parameter	Description	Value
sdh	Sets the frame format to SDH.	-
sonet	Sets the frame format to SONET.	-

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SDH and SONET are different standards defined by different organizations, but their content and functions are similar. SDH is mainly used in Europe and China and SONET is mainly used in North America and Japan. Different device manufacturers provide different default configurations for them.

Configure the POS interface frame format based on the standard used locally.

Precautions

Ensure that the frame format is the same on both ends.

There is a fixed 4-byte interframe gap (IFG) on a POS interface.

Example

Set the frame format to SONET on POS 2/0/0.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] frame-format sonet
```

Related Topics

5.13.3 display interface pos

5.13.6 link-protocol (POS interface view)

Function

The **link-protocol** command sets the link-layer protocol for a POS interface.

The **undo link-protocol** command restores the default setting.

By default, the link-layer protocol of a POS interface is PPP.

Format

link-protocol { **fr** | **hdlc** | **ppp** }

undo link-protocol { **fr** | **hdlc** }

Parameters

Parameter	Description	Value
fr	Sets the link-layer protocol of the interface to FR.	-
hdlc	Sets the link-layer protocol of the interface to HDLC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ppp	Sets the link-layer protocol of the interface to PPP.	-

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

The link-layer protocol of a POS interface can be FR, PPP or HDLC. The protocol parameters can be set only after the link-layer protocol is set correctly.

Example

Set the link-layer protocol of POS 2/0/0 to HDLC.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] link-protocol hdlc
Warning: The encapsulation protocol of the link will be changed.
Continue? [Y/N]:y
```

Related Topics

5.13.3 display interface pos

5.13.7 loopback (POS interface view)

Function

The **loopback** command enables loopback detection on a POS interface and sets the detection mode.

The **undo loopback** command restores the default setting.

By default, loopback detection is disabled on a POS interface.

Format

loopback { **local** | **remote** }

undo loopback

Parameters

Parameter	Description	Value
local	Specifies internal loopback.	-
remote	Specifies remote loopback.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

POS provides different loopback functions to diagnose faults on the interface or connection cable. Normally, the loopback function should not be enabled.

Precautions

- Loopback can be enabled only for POS interfaces using the master clock mode. Otherwise, the POS interface cannot be connected.
- When loopback is enabled for a POS interface, the physical status is Up and the link-layer protocol status is Down if the link-layer protocol is PPP or FR, and the physical status and link-layer protocol status are both Up if the link-layer protocol is HDLC.

Example

Enable internal loopback on POS 2/0/0.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] loopback local
```

Related Topics

5.13.3 display interface pos

5.13.8 mtu (POS interface view)

Function

The **mtu** command sets the maximum transmission unit (MTU) for a POS interface.

The **undo mtu** command restores the default setting.

By default, the MTU of a POS interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mtu	Sets the MTU for a POS interface.	The value is an integer and the value depends on the device, in bytes.

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then, the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer disassembles the packet to fragments, each not longer than the MTU.

If forcible unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. Therefore, large packets must be forcibly fragmented to prevent packet loss on the network. The **mtu** command sets the size of a fragment.

Precautions

- If you run the **mtu** command multiple times in the same POS interface view, only the latest configuration takes effect.
- After changing the MTU on an interface using the **mtu** command, run the **shutdown** and **undo shutdown**/**restart** command in the interface view to restart the interface for the configuration to take effect.

Example

Set the MTU of POS 2/0/0 to 1200.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] mtu 1200
[Huawei-Pos2/0/0] restart
```

Related Topics

5.13.3 display interface pos

5.13.9 scramble (POS interface view)

Function

The **scramble** command enables a POS interface to scramble payload data.

The **undo scramble** command disables the scrambling function.

By default, the scrambling function is enabled.

Format

scramble

undo scramble

Parameters

None

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To avoid long consecutive 1 and 0 and allow the receiver to extract clock signals, a POS interface supports scrambling of payload data.

Precautions

NOTICE

Ensure that the same scrambling function is configured for both devices on the link. Otherwise, the two devices cannot be connected.

Example

Disable a POS interface from scrambling payload data.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] undo scramble
```

Related Topics

5.13.3 display interface pos

 Copyright © Huawei Technologies Co., Ltd.

5.13.10 set workmode stm

Function

The **set workmode stm** command sets the working mode of a 4STM1 interface card.

By default, a 4STM1 interface card works in **stm1** mode, that is, it provides four interfaces working at the rate of 155 Mbit/s.

Format

set workmode slot *slot-id* **stm** { **stm4** | **stm1** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a 4STM1 interface card.	Run the **display device** command to view slot IDs and types of interface cards, find the slot ID with 4STM1 displayed.
stm4	Sets the working mode to **stm4**, that is, only the POS optical interface numbered 0 and working at the rate of 622 Mbit/s is available. The other interfaces numbered 1 to 3 are unavailable.	-
stm1	Sets the working mode to **stm1**, that is, four POS optical interfaces working at the rate of 155 Mbit/s are available.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a 4STM1 interface card connects to an SDH network, the 4STM1 interface card provides four interfaces working at the rate of 155 Mbit/s or one interface working at the rate of 622 Mbit/s. You can run this command to set the working mode of a 4STM1 interface card.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After running this command, reset the card to make the configuration take effect. You can reset the card as prompted or run the **reset slot** command to manually reset the card.

You can run the **display workmode** command to view the working mode of a 4STM1 interface card.

Example

Configure the 4STM1 interface card in slot 2 to work in stm1 mode.

```
<Huawei> system-view
[Huawei] set workmode slot 2 stm stm4
Warning: Changing the working mode will reset the board in slot 2. Continue? [y/
n]:y
INFO: Resetting board[2] succeeded.
```

Related Topics

4.1.3 display device

5.5.9 display workmode

5.13.11 threshold (POS interface view)

Function

The **threshold** command sets SD and SF alarm thresholds for a POS interface.

The **undo threshold** command restores the default setting.

The default Signal Degrade (SD) log threshold is 10e-6 and the default SF log threshold is 10e-3.

Format

threshold { **sd** | **sf** } *value*

undo threshold { **sd** | **sf** }

Parameters

Parameter	Description	Value
sd *value*	Specifies the SD alarm threshold.	The threshold is in the format 10e-*value* and *value* is an integer ranging from 3 to 9.
sf *value*	Specifies the SF alarm threshold.	The threshold is in the format 10e-*value* and *value* is an integer ranging from 3 to 9.

Views

POS interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When link performance deteriorates, set the alarm thresholds on POS interfaces to learn link status.

- When link performance deteriorates a little, an SD alarm is reported.
- When link performance deteriorates greatly, an SF alarm is reported.

Precautions

The SD alarm threshold must be smaller than the SF alarm threshold.

Example

Set the SD alarm threshold to 10e-8 on POS 2/0/0.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] threshold sd 8
```

Related Topics

5.13.3 display interface pos

5.14 CPOS Interface Configuration Commands

5.14.1 clock (CPOS interface view)

Function

The **clock** command sets the clock mode of a CPOS interface.

The **undo clock** command restores the default setting.

By default, a CPOS interface works in slave clock mode.

Format

clock { **master** | **slave** | **system** }

undo clock

Parameters

Parameter	Description	Value
master	Configures a CPOS interface to work in master clock mode.	-
slave	Configures a CPOS interface to work in slave clock mode.	-
system	Configures a CPOS interface to work in system clock mode.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To exchange data correctly, communicating parties must work in clock synchronization state.

A CPOS interface supports the following clock modes:

- master: uses the internal clock signal.
- slave: uses the line clock signal.
- system: uses the MPU clock signal.

Precautions

When CPOS interfaces of the route and a remote device are connected directly or connected using WDM, one CPOS interface should work in master clock mode and use internal clock signals, and the other CPOS interface should work in slave clock mode and use line clock signals.

When connecting to a SONET/SDH device, a CPOS interface must be configured with the slave clock mode because the clock on a SONET/SDH network is more accurate than the internal clock source on a CPOS interface.

When the MPU on the router obtains the clock with high accuracy from the upstream device and the router needs to synchronize the clock to downstream device, the interface on the router must be configured to work in system clock mode. Moreover, the interface on the downstream device must be configured to work in slave clock mode.

Example

Configure CPOS 1/0/0 to work in master clock mode.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] clock master
```

Related Topics

5.14.3 display controller cpos

5.14.2 controller cpos

Function

The **controller cpos** command displays the CPOS interface view.

Format

controller cpos *cpos-number*

Parameters

Parameter	Description	Value
cpos-number	Specifies the number of a CPOS interface. The value is in the format of slot ID/subcard ID/interface sequence number.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring parameters such as frame formats and overhead bytes for a CPOS interface, you must enter the CPOS interface view.

Example

Enter the interface view of CPOS 1/0/0.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0]
```

Related Topics

5.14.3 display controller cpos

5.14.3 display controller cpos

Function

The **display controller cpos** command displays the physical layer configuration of the CPOS interface and all E1/T1 channels.

Format

display controller [**cpos** [*cpos-number*]]

Parameters

Parameter	Description	Value
cpos-number	Displays the physical layer configuration of the CPOS interface with a specified number and all E1/T1 channels. The value is in the format of slot ID/subcard ID/interface sequence number. If the *cpos-number* parameter is not specified, physical layer configurations of all CPOS interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the interface status or identifying the cause of the interface faults, you can run the **display controller cpos** command to obtain the status and statistics of the interface. According to the information, you can measure the traffic and identify the fault.

Example

Display the physical layer configuration of CPOS1/0/0 and all E1/T1 channels.

```
<Huawei> display controller cpos 1/0/0
Cpos1/0/0 current state : UP
Description : HUAWEI, AR Series, Cpos1/0/0 Interface
  Frame-format SDH, multiplex AU-3, clock master, loopback not set
  Tx: J0: 0x1, J1: "NetEngine", C2: 0x2
  Rx: J0: 0x1, J1: "NetEngine", C2: 0x2
Regenerator section:
  Alarm: none
  Error: 0 BIP
Multiplex section:
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path (VC-3-1):
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path (VC-3-2):
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path (VC-3-3):
  Alarm: none
  Error: 0 BIP, 0 REI
Cpos1/0/0  CT1 1  is up
  Frame-format ESF, clock master, loopback not set
Cpos1/0/0  CT1 2  is up
  Frame-format ESF, clock master, loopback not set
Cpos1/0/0  CT1 3  is up
  Frame-format ESF, clock master, loopback not set
 (here omitted some output information)
```

```
Cpos1/0/0  CT1 83  is up
  Frame-format ESF, clock master, loopback not set
Cpos1/0/0  CT1 84  is up
  Frame-format ESF, clock master, loopback not set
```

Table 5-45 Description of the **display controller cpos** command output

Item	Description
Cpos1/0/0 current state:	Indicates the current physical status of the CPOS interface.
Description	Description of the CPOS interface. The value is a maximum of 242 case-sensitive characters with spaces. The description helps users learn about the functions of the CPOS interface.
Frame-format SDH, multiplex AU-3, clock master, loopback not set	Indicates the physical layer information of the CPOS interface: ● The format of frames is SDH. To set the frame format, run the **frame-format** command. ● AU-3 multiplexing path is adopted. To set the multiplexing mode, run the **multiplex mode** command. ● The master clock mode is adopted, that is, internal clock signals are used. To set the clock mode, run the **clock** command. ● The loopback function is disabled. To configure the loopback function, run the **loopback** command.
Tx: J0: 0x1, J1: "NetEngine", C2: 0x2	Indicates the sent overhead bytes. To set the overhead byte, run the **flag** command.
Rx: J0: 0x1, J1: "NetEngine", C2: 0x2	Indicates the received overhead bytes.
Regenerator section	Indicates the alarm and error statistics of the regenerator section.
Multiplex section	Indicates the alarm and error statistics of the multiplexing section.
Higher order path (VC-3-x)	Indicates the alarm and error statistics of the higher-order path. VC-3-x indicates VC-3 numbered x. When AU-3 multiplexing path is adopted, three VC-3s are multiplexed into one STM-1. Therefore, there are three higher-order paths. When AU-4 multiplexing path is adopted, there is only one higher-order path VC-4.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm	Indicates the alarm statistics. ● Loss of Signal (LOS): The LOS alarm is generated when data transmission is interrupted or frames are lost because of severe problems, for example, there is no transmit optical power, the transmit optical power is too high or too low, the cable is broken, or the cable is not properly connected. ● Out of Frame (OOF): The OOF alarm is generated when five or more consecutive received frames (625 microseconds) contain no correct A1 and A2 bytes. ● Loss of Frame (LOF): The LOF alarm is generated when an OOF defect on the incoming SONET signal persists for 3 milliseconds. ● Trace Identifier Mismatch (TIM): The TIM alarm is generated on the receiving terminal when the values of J0 and J1 bytes in received frames differ from the expected values. After a TIM alarm is generated, the receiving terminal sends an RDI trap to the receiving terminal to indicate the defect on the remote end. The TIM alarm is cleared when the values are the same as the expected values. ● Alarm Indication Signal (AIS): The line AIS (LAIS) alarm is received on the local terminal when it receives three or five consecutive frames whose K2 byte (bit 6 to bit 8) is 111. After receiving an LAIS alarm, the local terminal must send an LRDI trap to the remote terminal. The LAIS alarm is cleared when the local terminal receives three or five consecutive frames whose K2 byte (bit 6 to bit 8) is not 111. When the local terminal receives three consecutive frames containing AIS_ind, a path AIS (PAIS) is generated. When an AIS alarm is generated, the protocol status changes to Down, causing packet transmission interruption.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Remote Defect Indication (RDI): The receiving terminal sends an RDI trap to the sending terminal to inform it of signal degrade. • Loss of Pointer (LOP): The LOP alarm is generated when the receiving terminal receives eight consecutive frames containing invalid pointers or new data flags (NDFs). After receiving the LOP alarm, the receiving terminal sends an RDI trap to the sending terminal to inform it of the defect. • Payload Label Mismatch (PLM): The PLM alarm is generated on the receiving terminal when the value of C2 byte in the received frame differs from the expected value. After receiving a PLM alarm, the receiving terminal sends an RDI trap to the sending terminal to indicate the defect on the peer end. • Unequipped (UNEQ): The UNEQ alarm is generated when C2 bytes in the received five consecutive frames are all 0s.
Error	Indicates the error statistics. Possible error types are as follows: • BIP: is short for bit-interleaved parity • REI: is short for remote error indication
Cpos1/0/0 CT1 1 is up	Indicates the status of T1 channel 1 of CPOS 1/0/0.
Frame-format ESF, clock master, loopback not set	Indicates the physical layer information of the T1 channel: • The format of frames is ESF. • The master clock mode is adopted, that is, internal clock signals are used. • The loopback function is disabled.

Related Topics

5.14.4 display controller cpos e1
5.14.5 display controller cpos t1

5.14.4 display controller cpos e1

Function

The **display controller cpos e1** command displays the physical layer configuration of the specified E1 channel of the specified CPOS interface.

Format

display controller cpos *cpos-number* **e1** *e1-number*

Parameters

Parameter	Description	Value
cpos-number	Displays the physical layer configuration of a specified CPOS interface. The value is in the format of slot ID/subcard ID/interface sequence number.	-
e1-number	Displays the physical layer configuration of a specified E1 channel of a specified CPOS interface.	The value is an integer that ranges from 1 to 63.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Compared with the **display controller cpos** command, the **display controller cpos e1** command displays the error and alarm information of the lower-order path, the multiplexing path of the E1 channel, and E1 channel multiplexing path.

Example

Display the status of E1 channel 1 of CPOS 1/0/0.

```
<Huawei> display controller cpos 1/0/0 e1 1
Cpos1/0/0 current state : UP
Description : HUAWEI, AR Series, Cpos1/0/0 Interface
  Frame-format SDH, multiplex AU-4, clock master, loopback not set
  Tx: J0: 0x1, J1: NULL, C2: 0x2
  Rx: J0: NULL, J1: NULL, C2: 0x0
Regenerator section:
  Alarm: none
  Error: 0 BIP
Multiplex section:
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path (VC-4-1):
```

```
  Alarm: none
  Error: 0 BIP, 0 REI
Lower order path:
  Alarm: none
  Error: 0 BIP, 0 REI
Cpos1/0/0  CE1 1 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E1 framer (1-1-1-1):
  Alarm: none
  Error: 0 CEC, 0 FEBC, 0 REC
```

Table 5-46 Description of the **display controller cpos e1** command output

Item	Description
Cpos1/0/0 current state	Indicates the current physical status of the CPOS interface.
Description	Indicates the description of the interface, which is case sensitive and support blank spaces. A maximum of 242 characters can be entered.
Frame-format SDH, multiplex AU-4, clock master, loopback not set	Indicates the physical layer information of the CPOS interface: • The format of frames is SDH. To set the frame format, run the **frame-format** command. • AU-3 multiplexing path is adopted. To set the multiplexing mode, run the **multiplex mode** command. • The master clock mode is adopted, that is, internal clock signals are used. To set the clock mode, run the **clock** command. • The loopback function is disabled. To configure the loopback function, run the **loopback** command.
Tx: J0: 0x1, J1: NULL, C2: 0x2	Indicates the sent overhead bytes. To set the overhead byte, run the **flag** command.
Rx: J0: NULL, J1: NULL, C2: 0x0	Indicates the received overhead bytes.
Regenerator section	Indicates the alarm and error statistics of the regenerator section.
Multiplex section	Indicates the alarm and error statistics of the multiplexing section.
Higher order path (VC-3-x)	Indicates the alarm and error statistics of the higher-order path. VC-4-1 indicates that AU-4 multiplexing path is adopted, and there is only one higher-order path VC-4.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm:Error	Indicates the alarm and error statistics. Possible error types are as follows: ● BIP: is short for bit-interleaved parity. ● REI: is short for remote error indication. ● CEC: is short for cyclic redundancy check error counter. ● FEBC: is short for frame bit error counter. ● REC: is short for receive E-Bit counter.
Cpos1/0/0 CE1 1 is up	Indicates the current status of E1 channel 1 of CPOS 1/0/0.
E1 framer (1-1-1-1)	Indicates the process of multiplexing the E1 channel. 1-1-1-1 indicates the following respectively: ● Number of VC-4 to which the E1 channel belongs ● Number of TUG-3 to which the E1 channel belongs ● Number of TUG-2 to which the E1 channel belongs ● Number of TU-12 to which the E1 channel belongs

Related Topics

5.14.3 display controller cpos
5.14.5 display controller cpos t1

5.14.5 display controller cpos t1

Function

The **display controller cpos t1** command displays the physical layer configuration of the specified T1 channel of the specified CPOS interface.

Format

display controller cpos *cpos-number* **t1** *t1-number*

Parameters

Parameter	Description	Value
cpos-number	Displays the physical layer configuration of a specified CPOS interface. The value is in the format of slot ID/subcard ID/interface sequence number.	-
t1-number	Displays the physical layer configuration of a specified T1 channel of a specified CPOS interface.	The value is an integer that ranges from 1 to 84.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Compared with the **display controller cpos** command, the **display controller cpos t1** command displays the error and alarm information of the lower-order path, the multiplexing path of the E1 channel, and T1 multiplexing path.

Example

Display the status of T1 channel 2 of CPOS 1/0/0.

```
<Huawei> display controller cpos 1/0/0 t1 2
Cpos1/0/0 current state : UP
Description : HUAWEI, AR Series, Cpos1/0/0 Interface
  Frame-format SDH, multiplex AU-3, clock master, loopback not set
  Tx: J0: 0x1, J1: NULL, C2: 0x2
  Rx: J0: NULL, J1: NULL, C2: 0x0
Regenerator section:
  Alarm: none
  Error: 0 BIP
Multiplex section:
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path (VC-3-2):
  Alarm: none
  Error: 0 BIP, 0 REI
Lower order path:
  Alarm: none
  Error: 4095 BIP, 2047 REI
Cpos1/0/0  CT1 2 is up
  Frame-format ESF, clock master, loopback not set
T1 framer (2-1-1):
  Alarm: none
  Error: 0 CEC, 0 FEBC, 0 REC
```

 Copyright © Huawei Technologies Co., Ltd.

Table 5-47 Description of the **display controller cpos t1** command output

Item	Description
Cpos1/0/0 current state:	Indicates the current physical status of the CPOS interface.
Description	Description of the CPOS interface. The value is a maximum of 242 case-sensitive characters with spaces. The description helps users learn about the functions of the CPOS interface.
Frame-format SDH, multiplex AU-3, clock master, loopback not set	Indicates the physical layer information of the CPOS interface: ● The format of frames is SDH. To set the frame format, run the **frame-format** command. ● AU-3 multiplexing path is adopted. To set the multiplexing mode, run the **multiplex mode** command. ● The master clock mode is adopted, that is, internal clock signals are used. To set the clock mode, run the **clock** command. ● The loopback function is disabled. To configure the loopback function, run the **loopback** command.
Tx: J0: 0x1, J1: NULL, C2: 0x2	Indicates the sent overhead bytes. To set the overhead byte, run the **flag** command.
Rx: J0: NULL, J1: NULL, C2: 0x0	Indicates the received overhead bytes.
Regenerator section	Indicates the alarm and error statistics of the regenerator section.
Multiplex section	Indicates the alarm and error statistics of the multiplexing section.
Higher order path (VC-3-2)	Indicates the alarm and error statistics of the higher-order path. VC-3-2 indicates the VC-3 numbered 2.
Lower order path:	Indicates the alarm and error statistics of the lower-order path.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm:Error	Indicates the alarm statistics and error statistics. Possible error types are as follows: • BIP: is short for bit-interleaved parity. • REI: is short for remote error indication. • CEC: is short for cyclic redundancy check error counter. • FEBC: is short for frame bit error counter. • REC: is short for receive E-Bit counter.
Cpos1/0/0 CT1 2 is up	Indicates the current status of T1 channel 1 of CPOS 1/0/0.
Frame-format ESF, clock master, loopback not set	Indicates the physical layer information of the T1 channel: • The format of frames is ESF. • The master clock mode is adopted, that is, internal clock signals are used. • The loopback function is disabled.
T1 framer (2-1-1)	Indicates the process of multiplexing the T1 channel. 2-1-1 indicates the following respectively: • Number of VC-3 to which the T1 channel belongs • Number of TUG-2 to which the T1 channel belongs • Number of TU-11 to which the T1 channel belongs

Related Topics

5.14.3 display controller cpos
5.14.4 display controller cpos e1

5.14.6 display cpos multi-channel

Function

The **display cpos multi-channel** command displays the multiplexing path tributary unit groups (TUGs) of an E1 or a T1 channel.

Format

display cpos { **e1-data** | **t1-data** } **multi-channel align-mode**

Parameters

Parameter	Description	Value
e1-data	Displays the multiplexing path tributary unit groups (TUGs) of an E1 channel.	-
t1-data	Displays the TUGs of a T1 channel.	-
multi-channel align-mode	Sets the connection mode in which a CPOS interface connects to a remote device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display cpos multi-channel** command displays the multiplexing path TUGs of an E1 or a T1 channel.

Example

Display the multiplexing path TUGs of an E1 channel.

```
<Huawei> display cpos e1-data multi-channel align-mode
TUG-3  TUG-2  TU-12  Huawei  Lucent  Alcatel
  1      1      1      1      1       1
  2      1      1      2     22      22
  3      1      1      3     43      43
  1      2      1      4      4       2
  2      2      1      5     25      23
  3      2      1      6     46      44
  1      3      1      7      7       3
  2      3      1      8     28      24
  3      3      1      9     49      45
  1      4      1     10     10       4
  2      4      1     11     31      25
  3      4      1     12     52      46
  1      5      1     13     13       5
  2      5      1     14     34      26
  3      5      1     15     55      47
  1      6      1     16     16       6
  2      6      1     17     37      27
  3      6      1     18     58      48
  1      7      1     19     19       7
  2      7      1     20     40      28
  3      7      1     21     61      49
  1      1      2     22      2       8
  2      1      2     23     23      29
  3      1      2     24     44      50
  1      2      2     25      5       9
  2      2      2     26     26      30
  3      2      2     27     47      51
  1      3      2     28      8      10
  2      3      2     29     29      31
  3      3      2     30     50      52
  1      4      2     31     11      11
```

```
2    4    2    32    32    32
3    4    2    33    53    53
1    5    2    34    14    12
2    5    2    35    35    33
3    5    2    36    56    54
1    6    2    37    17    13
2    6    2    38    38    34
3    6    2    39    59    55
1    7    2    40    20    14
2    7    2    41    41    35
3    7    2    42    62    56
1    1    3    43    3    15
2    1    3    44    24    36
3    1    3    45    45    57
1    2    3    46    6    16
2    2    3    47    27    37
3    2    3    48    48    58
1    3    3    49    9    17
2    3    3    50    30    38
3    3    3    51    51    59
1    4    3    52    12    18
2    4    3    53    33    39
3    4    3    54    54    60
1    5    3    55    15    19
2    5    3    56    36    40
3    5    3    57    57    61
1    6    3    58    18    20
2    6    3    59    39    41
3    6    3    60    60    62
1    7    3    61    21    21
2    7    3    62    42    42
3    7    3    63    63    63
```

Table 5-48 Description of the display cpos multi-channel command output

Item	Description
TUG-3	Tributary unit group type 3.
TUG-2	Tributary unit group type 2.
TU-12	Tributary unit type 12.
Huawei	CPOS connection mode: Huawei mode.
Lucent	CPOS connection mode: Lucent mode.
Alcatel	CPOS connection mode: Alcatel mode.

Related Topics

5.14.18 multi-channel align-mode

5.14.7 e1 channel-set (CPOS interface view)

Function

The **e1 channel-set** command configures an E1 channel to work in channelized mode and bundles timeslots of E1 channel together.

The **undo e1 channel-set** command unbinds the timeslots.

By default, the device does not bundle timeslots of E1 channel.

Format

e1 *e1-number* **channel-set** *set-number* **timeslot-list** *slot-list*

undo e1 *e1-number* **channel-set** *set-number*

Parameters

Parameter	Description	Value
e1-number	Specifies the E1 channel number of CPOS.	The value ranges from 1 to 63.
set-number	Specifies the number of the channel-set.	The value ranges from 0 to 30.
timeslot-list *slot-list*	Specifies the timeslot number or the timeslot range.	The value ranges from 1 to 31. It can be separate timeslot or time ranges. Time slots are separated by ","; while the range is expressed by "-".

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The E1 channel of a CPOS interface can work in unchannelized or channelized mode.

- In unchannelized mode, an E1 channel works at a rate of 2 Mbit/s without timeslot division. The logical features of an E1 channel are the same as those of a synchronous serial interface.
- When an E1 channel works in channelized mode, the 2 Mbit/s transmission line is divided into 32 timeslots at a rate of 64 kbit/s. The 32 timeslots are numbered 0 to 31, and timeslot 0 transmits synchronization signals. Timeslots except timeslot 0 can be randomly bundled into a channel set that functions as an interface. The rate of the interface is N x 64 kbit/s, in which N is the number of timeslots bundled into a channel set. The interface has the same logical features as a synchronous serial interface.

In channelized mode, the name and number of an E1 channel is **serial** *interface-number*|*e1-number.set-number*. *interface-number* specifies the number of the CPOS interface, *e1-number* specifies the E1 channel number, and *set-number* specifies the number of the channel set.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To sure the system's processing capability, one CPOS interface can be bound with 512 logical channels at most.

Example

Configure E1 channel 63 to work in channelized mode and bundles timeslots of E1 channel 3 together.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] e1 63 channel-set 1 timeslot-list 1-31
```

Enter the serial port (generated after the binding) view.

```
[Huawei-Cpos1/0/0] quit
[Huawei] interface serial 1/0/0/63:1
[Huawei-Serial1/0/0/63:1]
```

Related Topics

5.14.13 e1 unframed (CPOS interface view)

5.14.8 e1 set clock (CPOS interface view)

Function

The **e1 set clock** command sets the clock mode of E1.

The **undo e1 set clock** command restores the default setting.

By default, the clock mode of an E1 channel is slave.

Format

e1 *e1-number* **set clock** { **master** | **slave** }

undo e1 *e1-number* **set clock**

Parameters

Parameter	Description	Value
e1-number	Specifies the E1 channel number of CPOS.	The value ranges from 1 to 63 in integer.
master	Indicates the master clock.	-
slave	Indicates the slave clock.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The clock modes of different E1 channels on the same CPOS port are independent of each other. The clock mode of the E1 channel must be different on both ends.

Example

Set the clock mode of the E1 channel 1 to master.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] e1 1 set clock master
```

Related Topics

5.14.4 display controller cpos e1

5.14.9 e1 set flag (CPOS interface view)

Function

The **e1 set flag** command sets the overhead byte of an E1 channel.

The **undo e1 set flag** command restores the default setting.

By default, J2 repeatedly transmits a string of null characters, and the V5 byte value is 2.

Format

e1 *e1-number* **set flag** { **j2** { **1byte-mode** *1byte-string* | **16byte-mode** *16byte-string* } | **v5** *v5-string* }

undo e1 *e1-number* **set flag** { **j2** | **v5** }

Parameters

Parameter	Description	Value
e1-number	Specifies the E1 channel number of a CPOS interface.	The value is an integer that ranges from 1 to 63.
j2 1byte-mode *1byte-string*	Sets the 1-byte length trace format for the low-order path trace byte J2.	The value is a string of 1 character.
j2 16byte-mode *16byte-string*	Sets the 16-byte length trace format for the low-order path trace byte J2.	The value is a string of 1 to 15 characters.
v5 *v5-string*	Sets the low-order path signal label byte V5.	The value is an integer that ranges from 2 to 4.

Views

CPOS interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The pathoverhead (POH) of E1 channels must be the same on both ends; otherwise, devices on both ends may not communicate properly.

Example

Set the V5 byte of E1 channel 1 on a CPOS interface to 3.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] e1 1 set flag v5 3
```

Related Topics

5.14.4 display controller cpos e1

5.14.10 e1 set frame-format (CPOS interface view)

Function

The **e1 set frame-format** command configures the frame format of an E1 channel.

The **undo e1 set frame-format** command restores the default setting.

By default, no-CRC4 is used.

Format

e1 *e1-number* **set frame-format** { **crc4** | **no-crc4** }

undo e1 *e1-number* **set frame-format**

Parameters

Parameter	Description	Value
e1-number	Specifies the E1 channel number of CPOS.	The value ranges from 1 to 63 in integer.
crc4	Sets the frame format of the E1 channel to CRC4.	-
no-crc4	Sets the frame format of the E1 channel to no-CRC4.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The E1 channel channelized from CPOS interfaces supports frame formats: CRC4 and no-CRC4.

- CRC4: indicates that the frame format is a multi-frame. A multi-frame is formed by using the first bit of timeslot 0 and contains 16 consecutive PCM frames.
- Non-CRC4: indicates that the frame format is a basic frame. A basic frame is also called a dual-frame or an odd-even frame.

The multi-frame format supports CRC4, whereas the basic frame format does not support CRC4.

Precautions

The frame format on the local end must be the same as that on the remote end.

NOTE

If the **e1 unframed** command has been used, run the **undo e1 unframed** command to disable the E1 channel from working in unframed mode before running the **e1 set frame-format** command to configure the frame format for the E1 channel.

Example

Set the frame format of the E1 channel 1 to CRC4.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] e1 1 set frame-format crc4
```

Related Topics

5.14.4 display controller cpos e1

5.14.11 e1 set loopback (CPOS interface view)

Function

The **e1 set loopback** command enables loopback detection of an E1 channel and sets the detection mode.

The **undo e1 set loopback** command disables the loopback detection of an E1 channel.

By default, the loopback detection of an E1 channel is disabled.

Format

e1 *e1-number* **set loopback** { **local** | **remote** }

undo e1 *e1-number* **set loopback**

Parameters

Parameter	Description	Value
e1-number	Specifies the E1 channel number of CPOS.	The value ranges from 1 to 63 in integer.
local	Sets an E1 channel to implement local loopback.	-
remote	Sets an E1 channel to implement remote loopback.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The E1 channel provides a variety of loopback functions for tests on different levels.

- In the internal loopback, data at the sending end is looped back to the receiving end.
- In the external remote loopback, the received data is looped back without passing through the E1 framer and generating the payload.

When a loopback is enabled on an E1 channel, the loopback is valid for the synchronous serial interface formed by the E1 channel.

- When the link layer protocol of the synchronous serial interface is PPP, the physical status of the synchronous serial interface is Up; whereas the link layer protocol is Down.
- When the link layer protocol used by the synchronous serial interface is HDLC, the physical status and link layer status at both ends depend on the loopback mode:
  - In the internal loopback, the physical status of interfaces at both ends is Up. The link layer status of the sending end is Up, and that of the receiving end is Down.
  - In the external remote loopback, the physical status of interfaces at both ends is Up. The link layer status of the sending end is Down, and that of the receiving end is Up.

Example

Set the E1 channel 1 to perform the external remote loopback.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] e1 1 set loopback remote
```

Related Topics

5.14.4 display controller cpos e1

5.14.12 e1 shutdown (CPOS interface view)

Function

The **e1 shutdown** command disables an E1 channel.

The **undo e1 shutdown** command enables an E1 channel.

By default, an E1 channel is enabled.

Format

e1 *e1-number* **shutdown**

undo e1 *e1-number* **shutdown**

Parameters

Parameter	Description	Value
e1-number	Specifies the E1 channel number of CPOS.	The value ranges from 1 to 63 in integer.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **e1 shutdown** command disables an idle E1 channel.

Precautions

- After the **e1 shutdown** command is run on an E1 channel, the E1 channel and interfaces that timeslots are bound into are shut down and stop receiving and sending data. Data may be lost if you disable the E1 channel during data transmission. Exercise caution when you use the **shutdown** command.
- After the **undo shutdown** command is run on an E1 channel, the E1 channel and interfaces that timeslots are bound into go Up.

Example

Disable the E1 channel 1.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
```

```
[Huawei-Cpos1/0/0] e1 1 shutdown
```

Related Topics

5.14.4 display controller cpos e1

5.14.13 e1 unframed (CPOS interface view)

Function

The **e1 unframed** command configures an E1 channel to work in unchannelized mode and generates an interface working at a rate of 2 Mbit/s without timeslot division.

The **undo e1 unframed** command restores the default configuration.

By default, an E1 channel works in channelized mode.

Format

e1 *e1-number* **unframed**

undo e1 *e1-number* **unframed**

Parameters

Parameter	Description	Value
e1-number	Specifies the E1 channel number of CPOS.	The value is an integer that ranges from 1 to 63.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The E1 channel of a CPOS interface can work in unchannelized or channelized mode.

- In unchannelized mode, an E1 channel works at a rate of 2 Mbit/s without timeslot division. The logical features of an E1 channel are the same as those of a synchronous serial interface.
- When an E1 channel works in channelized mode, the 2 Mbit/s transmission line is divided into 32 timeslots at a rate of 64 kbit/s. The 32 timeslots are numbered 0 to 31, and timeslot 0 transmits synchronization signals. Timeslots except timeslot 0 can be randomly bundled into a channel set that functions as an interface. The rate of the interface is N x 64 kbit/s. The interface has the same logical features as a synchronous serial interface.

 Copyright © Huawei Technologies Co., Ltd.

In channelized mode, the name and number of interfaces formed by the E1 channel are **serial** *interface-number*|*e1-number*.**0**. *interface-number* specifies the number of the CPOS interface, and *e1-number* specifies the E1 channel number.

Example

Configure E1 channel 3 of CPOS 1/0/0 to operate in unframed mode.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] e1 3 unframed
```

Display the E1 channel 3 interface view.

```
[Huawei]interface serial 1/0/0/3:0
[Huawei-Serial1/0/0/3:0]
```

Related Topics

5.14.3 display controller cpos

5.14.14 flag (CPOS interface view)

Function

The **flag** command sets the overhead byte of a SONET or SDH frame.

The **undo flag** command restores the default setting.

By default, the overhead byte C2 is 2, and the overhead byte S1 is 15.

Format

flag { **c2** *c2-value* | { **j0** | **j1** } { **1byte-mode** *1byte-string* | **16byte-mode** *16byte-string* | **64byte-mode** *64byte-string* } | **s1** *s1-string* }

undo flag { **c2** | **j0** | **j1** | **s1** }

Parameters

Parameter	Description	Value
c2 *c2-value*	Specifies the path signal label byte. It is contained in the higher-order path overhead and is used to specify the multiplexing structure and the attribute of the information payload in a Virtual Container (VC) frame.	The value is a decimal integer that ranges from 0 to 255. The default value is 2.
j0	Specifies the regeneration section trace byte. It is contained in the RSOH and is used to detect the continuity of a connection between two interfaces on the section.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
j1	Specifies the Higher-Order VC-N path trace byte. It is carried in the higher-order path overhead and is used to detect the continuity of the connection between two interfaces on a channel.	-
1byte-mode *1byte-string*	Indicates that the J0/J1 overhead byte mode is 1-byte-mode.	The value is a string of 1 character.
16byte-mode *16byte-string*	Indicates that the J0/J1 overhead byte mode is 16-byte-mode.	The value is a string of 1 to 15 characters.
64byte-mode *64byte-string*	Indicates that the J0/J1 overhead byte mode is 64-byte-mode.	The value is a string of 1 to 62 characters.
s1 *s1-string*	Specifies the synchronization status byte S1.	The value is a decimal integer that ranges from 0 to 15.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A SONET or SDH frame has a variety of overhead bytes and can implement Operation and Maintenance (OAM) such as management of layers on the transmission network. C2, J1, J0 and S1 help devices from different countries, areas or manufacturers to communicate with each other.

Precautions

The values of C2, J0, J1, and S1 at the receive and transmit ends must be the same; otherwise, the two ends fail to communicate.

Example

Set the S1 byte of CPOS 1/0/0 to 10.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] flag s1 10
```

Related Topics

5.14.3 display controller cpos

5.14.15 frame-format (CPOS interface view)

Function

Using the **frame-format** command, you can set the frame type used by CPOS.

Using the **undo frame-format** command, you can restore the default setting.

By default, SDH is used.

Format

frame-format { **sdh** | **sonet** }

undo frame-format

Parameters

Parameter	Description	Value
sdh	Sets the frame format of a CPOS interface to SDH.	-
sonet	Sets the frame format of a CPOS interface to SONET.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SDH and SONET are different standards defined by different organizations, but their content and functions are similar. SDH is mainly used in Europe and China and SONET is mainly used in North America and Japan. Different device manufacturers provide different default configurations for them.

Configure the CPOS interface frame format based on the standard used locally.

Precautions

The frame format of the CPOS interface must be the same on both ends.

Example

Set the frame format of CPOS1/0/0 to SONET.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] frame-format sonet
```

Related Topics

5.14.3 display controller cpos

5.14.16 itf (CPOS interface view)

Function

The **itf** command sets the interframe filling tag and the number of interframe filling tags on a CPOS interface.

The **undo itf** command restores the default setting.

By default, a CPOS interface uses the interframe filling tag 0x7e and four interframe filling tags.

Format

itf { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 14.
type	Specifies the interframe filling tag.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag is the code sent when the timeslot bundled to form a logical channel that belongs to an E1 or T1 Channel channelized by a CPOS interface does not send any service data.

A CPOS interface supports two interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- Two devices can communicate properly only when the same interframe filling tag and the same number of interframe filling tags are set on CPOS interfaces on both devices.
- E1/T1 Channels channelized by a CPOS interface cannot achieve the bandwidth because of extra costs of interframe filling tags. To improve the transmission rate of the CPOS interface, run the **itf number** command to set the number of interframe filling tags to 0.

Example

Set the interframe filling tag to 0xff on CPOS 1/0/0.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] itf type ff
```

5.14.17 loopback (CPOS interface view)

Function

The **loopback** command enables loopback detection on a CPOS interface and sets the detection mode.

The **undo loopback** command restores the default setting.

By default, loopback detection is disabled on a CPOS interface.

Format

loopback { **local** | **remote** }

undo loopback

Parameters

Parameter	Description	Value
local	Specifies local loopback on a CPOS interface.	-
remote	Specifies remote loopback on a CPOS interface.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

CPOS provides loopback on different levels. The various loopback functions can be used to troubleshoot the ports or cables. In normal conditions, the loopback should be disabled.

NOTE

After the serial interface formed by the CPOS interface is encapsulated with the PPP protocol and the loopback is configured, the status of the link layer protocol is Down, which belongs to the normal case.

Example

Enable the remote loopback on CPOS 1/0/0.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] loopback remote
```

Related Topics

5.14.3 display controller cpos

5.14.18 multi-channel align-mode

Function

The **multi-channel align-mode** command sets the connection mode in which a CPOS interface connects to a remote device.

The **undo multi-channel align-mode** command restores the default setting.

By default, the connection mode of a CPOS interface is Huawei.

Format

multi-channel align-mode { **alcatel** | **huawei** | **lucent** }

undo multi-channel align-mode

Parameters

Parameter	Description	Value
alcatel	Sets the connection mode to Alcatel. Select this mode when a CPOS interface needs to connect to an Alcatel device.	-
huawei	Sets the connection mode to Huawei. Select this mode when a CPOS interface needs to connect to a Huawei device.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
lucent	Sets the connection mode to Lucent. Select this mode when a CPOS interface needs to connect to a Lucent device.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When CPOS interfaces of a Huawei device and a non-Huawei device are connected through optical fibers or using WDM, configure the connection mode for the CPOS interface.

A router provides three connection modes: Alcatel mode, Huawei mode, and Lucent mode. Configure the mode to suit the device connected to the CPOS interface.

NOTE

When the E1/T1 links on all low-end devices are aggregated to the device's CPOS interface through an SDH/SONET network, you do not need to configure the connection mode for the CPOS interface.

Precautions

After running the **multi-channel align-mode** command, you need to run the **reset slot** command or run both the **power off slot** and **power on slot** commands to restart the corresponding interface board for the configuration to take effect.

Example

Set the connection mode of a CPOS interface to Lucent.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] multi-channel align-mode align-mode lucent
```

Related Topics

5.14.6 display cpos multi-channel

5.14.19 multiplex mode

Function

Using the **multiplex mode** command, you can set the AUG multiplexing mode.

Using the **undo multiplex mode** command, you can restore the default setting.

By default, **au-4** is used.

Format

multiplex mode { **au-4** | **au-3** }

undo multiplex mode

Parameters

Parameter	Description	Value
au-4	Indicates AUG multiplexes to AU-4.	-
au-3	Indicates AUG multiplexes to AU-3.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Choose a proper AUG multiplexing mode and ensure that the AUG multiplexing mode of the CPOS interface is the same on both ends.

NOTE

When CPOS is applied in the SDH mode, using the **multiplex mode** command, you can configure AUG to multiplex to either AU-4 or AU-3.

When CPOS is applied in the SONET mode, AUG can multiplex only to AU-3. The **multiplex mode** command does not take effect.

Example

Configure AUG to multiplex to AU-3 in the SDH mode.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] frame-format sdh
[Huawei-Cpos1/0/0] multiplex mode au-3
```

Related Topics

5.14.15 frame-format (CPOS interface view)

 Copyright © Huawei Technologies Co., Ltd.

5.14.20 set workmode cpos

Function

The **set workmode cpos** command sets the working mode of a 1CPOS-155M/1CPOS-155M-WM interface card.

By default, a 1CPOS-155M/1CPOS-155M-W interface card works in E1 mode (e1-data).

Format

set workmode slot *slot-id* **cpos** { **e1-data** | **t1-data** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a 1CPOS-155M/1CPOS-155M-W interface card.	Run the **display device** command to view slot IDs and types of interface cards and find the slot ID of the CPOS interface card.
e1-data	Indicates a 1CPOS-155M/1CPOS-155M-W interface card works in E1 mode and functions as a channelized E1 data card (CE1).	-
t1-data	Indicates a 1CPOS-155M/1CPOS-155M-W interface card works in T1 mode and functions as a channelized T1 data card (CT1).	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After this command is used, the system prompts you to reset the CPOS interface card to make the new working mode take effect. If you select **Yes**, the system resets the interface card. Otherwise, you need to run the **reset slot** command to manually reset the interface card to make the new working mode take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the 1CPOS-155M-W interface card in slot 2 to work in T1 mode.

```
<Huawei> system-view
[Huawei] set workmode slot 2 cpos t1-data
Warning: Changing the working mode will reset the board in slot 2. Continue? [y/
n]:y
INFO: Resetting board[2] succeeded.
```

Related Topics

4.1.3 display device

5.14.21 shutdown (CPOS interface view)

Function

The **shutdown** command shuts down the current CPOS physical interface.

The **undo shutdown** command enables a CPOS physical interface.

By default, a CPOS physical interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **shutdown** command to shut down an idle interface that is not connected to a cable.

Precautions

- After the **shutdown** command is run on a CPOS physical interface, all E1/T1 channels of the CPOS interface and interfaces that timeslots are bound into are shut down and stop receiving and sending data. Data may be lost if you disable an interface during data transmission. Exercise caution when you use the **shutdown** command.
- After the **undo shutdown** command is run on a COS interface, the CPOS physical interface and interfaces that timeslots are bound into go Up.

Example

Disable the physical port CPOS 1/0/0.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] shutdown
```

Related Topics

5.14.27 t1 shutdown (CPOS interface view)

5.14.22 t1 channel-set (CPOS interface view)

Function

The **t1 channel-set** command configures a T1 channel to work in channelized mode and bundles timeslots of T1 channel together.

The **undo t1 channel-set** command unbinds the timeslots.

By default, the device does not bundle timeslots of T1 channel.

Format

t1 *t1-number* **channel-set** *set-number* **timeslot-list** *slots-list* [**speed** { **56k** | **64k** }]

undo t1 *t1-number* **channel-set** *set-number*

Parameters

Parameter	Description	Value
t1-number	Specifies the T1 channel number of a CPOS interface.	The value ranges from 1 to 84 in integer.
set-number	Specifies the number of the channel set.	The value ranges from 0 to 23 in integer.
timeslot-list *slot-list*	Specifies the number or range of bound timeslots.	It is an integer in the range of 1 to 24. Time slots are separated by ","; while the range is expressed by "-".
speed { **56k** | **64k** }	Specifies the timeslot binding mode. • If **56k** is selected, binding mode is N x 56 kbit/s. • If **64k** is selected, binding mode is N x 64 kbit/s. If **speed** is not specified, the default 64 kbit/s is used.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The T1 channel of a CPOS interface can work in unchannelized or channelized mode.

- In unchannelized mode, a T1 interface works at a rate of 1.544 Mbit/s without timeslot division. The logical features of a T1 channel are the same as those of a synchronous serial interface.
- When a T1 channel works in channelized mode, timeslots numbered 1 to 24 can be randomly bundled into a channel set that functions as an interface. The rate of the interface is N x 56 kbit/s or N x 64 kbit/s, in which N is the number of timeslots bundled into a channel set. The interface has the same logical features as a synchronous serial interface.

In channelized mode, the name and number of a T1 channel is **serial** *interface-number*/*t1-number*.*set-number*. *interface-number* specifies the number of the CPOS interface, *t1-number* specifies the T1 channel number, and *set-number* specifies the number of the channel set.

Example

Configure T1 channel 1 to work in channelized mode and bundle timeslots of T1 channel 1.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] t1 1 channel-set 1 timeslot-list 1-24
```

Enter the view of the serial interface generated after binding.

```
[Huawei-Cpos1/0/0] quit
[Huawei] interface serial 1/0/0/1:1
[Huawei-Serial1/0/0/1:1]
```

Related Topics

5.14.28 t1 unframed (CPOS interface view)

5.14.23 t1 set clock (CPOS interface view)

Function

The **t1 set clock** command sets the clock mode of a T1 channel.

The **undo t1 set clock** command restores the default setting.

By default, the clock mode of a T1 channel is slave.

 Copyright © Huawei Technologies Co., Ltd.

Format

t1 *t1-number* **set clock** { **master** | **slave** }

undo t1 *t1-number* **set clock**

Parameters

Parameter	Description	Value
t1-number	Specifies the T1 channel number of a CPOS interface.	The value ranges from 1 to 84 in integer.
master	Sets the clock mode of a T1 channel to master.	-
slave	Sets the clock mode of a T1 channel to slave.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The clock modes of the different T1 channels of the same CPOS interface are independent from each other. The clock mode of the T1 channel must be different on both ends.

Example

Configure T1 channel 1 to use the master clock mode.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] t1 1 set clock master
```

Related Topics

5.14.5 display controller cpos t1

5.14.24 t1 set flag (CPOS interface view)

Function

The **t1 set flag** command sets the overhead byte of a T1 channel.

The **undo t1 set flag** command restores the default setting.

By default, J2 repeatedly transmits a string of null characters, and the V5 byte value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Format

t1 *t1-number* **set flag** { **j2** { **1byte-mode** *1byte-string* | **16byte-mode** *16byte-string* } | **v5** *v5-string* }

undo t1 *t1-number* **set flag** { **j2** | **v5** }

Parameters

Parameter	Description	Value
t1-number	Specifies the T1 channel number of a CPOS interface.	The value is an integer that ranges from 1 to 84.
j2 1byte-mode *1byte-string*	Sets the 1-byte length trace format for the low-order path trace byte J2.	The value is a string of 1 character.
j2 16byte-mode *16byte-string*	Sets the 16-byte length trace format for the low-order path trace byte J2.	The value is a string of 1 to 15 characters.
v5 *v5-string*	Sets the low-order path signal label byte V5.	The value is an integer that ranges from 2 to 4.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The pathoverhead (POH) of T1 channels must be the same on both ends; otherwise, devices on both ends may not communicate properly.

Example

Set the V5 byte of T1 channel 1 on a CPOS interface to 4.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] t1 1 set flag v5 4
```

Related Topics

5.14.5 display controller cpos t1

5.14.25 t1 set frame-format (CPOS interface view)

Function

The **t1 set frame-format** command configures the frame format of a T1 channel.

The **undo t1 set frame-format** command restores the default setting.

By default, the frame format of a T1 channel is ESF.

Format

t1 *t1-number* **set frame-format** { **esf** | **sf** }

undo t1 *t1-number* **set frame-format**

Parameters

Parameter	Description	Value
t1-number	Specifies the T1 channel number of a CPOS interface.	The value ranges from 1 to 84 in integer.
esf	Sets the frame format of the T1 channel to extended super frame (ESF).	-
sf	Sets the frame format of the T1 channel to super frame (SF).	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The T1 channel channelized by CPOS interfaces supports the SF format and ESF format. The two formats enable multiple frames to share the frame alignment information and signaling information so that more bits can be used to transmit data.

- SF: consists of 12 frames that share the frame alignment information and signaling information. Frame 6 and frame 12 are signaling frames.
- ESF: consists of 24 frames that share the frame alignment information and signaling information. Frames 6, 12, 18, and 24 are signaling frames.

Precautions

The frame format of the T1 channel must be the same on both ends.

NOTE

If the **t1 unframed** command has been used, run the **undo t1 unframed** command to disable the T1 channel from working in unframed mode before running the **t1 set frame-format** command to configure the frame format for the T1 channel.

Example

Set the frame format of T1 channel 1 to SF.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] t1 1 set frame-format sf
```

Related Topics

5.14.5 display controller cpos t1

5.14.26 t1 set loopback (CPOS interface view)

Function

The **t1 set loopback** command enables loopback detection of a T1 channel and sets the detection mode.

The **undo t1 set loopback** command disables the loopback detection of a T1 channel.

By default, the loopback detection of a T1 channel is disabled.

Format

t1 *t1-number* **set loopback** { **local** | **remote** }

undo t1 *t1-number* **set loopback**

Parameters

Parameter	Description	Value
t1-number	Specifies the T1 channel number of a CPOS interface.	The value ranges from 1 to 84 in integer.
local	Sets a T1 channel to implement local loopback.	-
remote	Sets a T1 channel to implement remote loopback.	-

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback is generally used to perform some special tests. In the normal situation, the loopback should be disabled.

 Copyright © Huawei Technologies Co., Ltd.

- In the internal loopback, data at the sending end is looped back to the receiving end.
- In the external remote loopback, the received data is looped back without passing through the E1 framer and generating the payload.

When a loopback is enabled on an T1 channel, the loopback is valid for the synchronous serial interface formed by the T1 channel.

- When the link layer protocol of the synchronous serial interface is PPP, the physical status of the synchronous serial interface is Up; whereas the link layer protocol is Down.
- When the link layer protocol used by the synchronous serial interface is HDLC, the physical status and link layer status at both ends depend on the loopback mode:
  - In the internal loopback, the physical status of interfaces at both ends is Up. The link layer status of the sending end is Up, and that of the receiving end is Down.
  - In the external remote loopback, the physical status of interfaces at both ends is Up. The link layer status of the sending end is Down, and that of the receiving end is Up.

Example

Configure the T1 channel 1 to perform the remote loopback.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] t1 1 set loopback remote
```

Related Topics

5.14.5 display controller cpos t1

5.14.27 t1 shutdown (CPOS interface view)

Function

The **t1 shutdown** command disables a T1 channel.

The **undo t1 shutdown** command enables a T1 channel.

By default, a T1 channel is enabled.

Format

t1 *t1-number* **shutdown**

undo t1 *t1-number* **shutdown**

Parameters

Parameter	Description	Value
t1-number	Specifies the T1 channel number of a CPOS interface.	The value ranges from 1 to 84 in integer.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **t1 shutdown** command to disable an idle T1 channel.

Precautions

- After the **t1 shutdown** command is run on a T1 channel, the T1 channel and interfaces that timeslots are bound into are shut down and stop receiving and sending data. Data may be lost if you disable the T1 channel during data transmission. Exercise caution when you use the **shutdown** command.
- After the **undo shutdown** command is run on a T1 channel, the T1 channel and interfaces that timeslots are bound into go Up.

Example

Disable the T1 channel 1.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] t1 1 shutdown
```

Related Topics

5.14.21 shutdown (CPOS interface view)

5.14.28 t1 unframed (CPOS interface view)

Function

The **t1 unframed** command configures a T1 channel to work in unchannelized mode and generates an interface working at a rate of 1.544 Mbit/s without timeslot division.

The **undo t1 unframed** command restores the default configuration.

By default, a T1 channel works in channelized mode.

Format

t1 *t1-number* **unframed**

undo t1 *t1-number* **unframed**

Parameters

Parameter	Description	Value
t1-number	Specifies the T1 channel number of a CPOS interface.	The value ranges from 1 to 84 in integer.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

The T1 channel of a CPOS interface can work in unchannelized or channelized mode.

- In unchannelized mode, a T1 interface works at a rate of 1.544 Mbit/s without timeslot division. The logical features of a T1 channel are the same as those of a synchronous serial interface.
- When a T1 channel works in channelized mode, timeslots numbered 1 to 24 can be randomly bundled into a channel set that functions as an interface. The rate of the interface is N x 56 kbit/s or N x 64 kbit/s. The interface has the same logical features as a synchronous serial interface.

In channelized mode, the name and number of interfaces formed by the T1 channel are **serial** *interface-number*|*t1-number*.**0**. *interface-number* specifies the number of the CPOS interface, and *t1-number* specifies the T1 channel number.

Example

Configure the T1 channel 3 of the CPOS 1/0/0 to work in the unframed mode.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] t1 3 unframed
```

Display the T1 channel 3 interface view.

```
[Huawei] interface serial 1/0/0/3:0
[Huawei-Serial1/0/0/3:0]
```

Related Topics

5.14.5 display controller cpos t1

5.14.29 threshold (CPOS interface view)

Function

The **threshold** command sets alarm thresholds for a CPOS interface.

The **undo threshold** command restores the default alarm thresholds.

The default SD (signal degrade) alarm threshold is 10e-6 and the default SF alarm threshold is 10e-3.

Format

threshold { **sd** | **sf** } *value*

undo threshold { **sd** | **sf** }

Parameters

Parameter	Description	Value
sd *value*	Specifies the SD alarm threshold.	The value is an integer that ranges from 3 to 9. The alarm threshold is 10e-*value*.
sf *value*	Specifies the SF (signal failure) alarm threshold.	The value is an integer that ranges from 3 to 9. The alarm threshold is 10e-*value*.

Views

CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When link performance deteriorates, set the alarm thresholds on CPOS interfaces to learn link status.

- When link performance deteriorates a little, an SD alarm is reported.
- When link performance deteriorates greatly, an SF alarm is reported.

Precautions

The SD alarm threshold must be smaller than the SF alarm threshold.

Example

Set the SD alarm threshold of CPOS 1/0/0 to 10e-8.

```
<Huawei> system-view
[Huawei] controller cpos 1/0/0
[Huawei-Cpos1/0/0] threshold sd 8
```

Related Topics

5.14.27 t1 shutdown (CPOS interface view)

5.15 ADSL Interface Configuration Commands

NOTE

Among the AR150&AR160&AR200 series, only the AR156, AR156W, AR157 series, AR206, and AR207 series support ADSL interfaces.

Among the AR150&AR160&AR200, only the AR157, AR157W, AR157VW, AR157G-HSPA+7, AR207, AR207V, AR207VW, AR207V-P, and AR207G-HSPA+7 support AnnexM. Among the AR150&AR160&AR200, only the AR156, AR156W, and AR206 support AnnexJ.

AR1200, AR2200 (except AR2201-48FE and AR2202-48FE), AR3200, and AR3600 series provide ADSL-A/M and ADSL-B/J boards. Only the ADSL-A/M boards support AnnexM. Only the ADSL-B/J boards support AnnexJ.

5.15.1 adsl bitswap (adsl)

Function

The **adsl bitswap** command enables or disables bit exchange on an ADSL interface.

By default, bit exchange is enabled on an ADSL interface.

Format

adsl bitswap { **off** | **on** }

Parameters

Parameter	Description	Value
off	Disables bit exchange on an ADSL interface.	-
on	Enables bit exchange on an ADSL interface.	-

Views

ADSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During line activation, every sub-channel calculates the signal-to-noise ratio (SNR) and the number of bits to be transmitted. After the line is activated, the SNR may change because the external environment changes. For example, the SNRs of some sub-channels reduce, whereas the SNRs of some other sub-channels increase. After a long period of time, the line may be disconnected.

The bit exchange function has the following advantages:

- Allows sub-channels failing to transmit the specified number of bits to switch some bits to sub-channels with higher SNRs.
- Reduces the transmit power of sub-channels with higher SNRs to increase the sending rate and SNRs of sub-channels with lower SNRs.

  This reduces the bit error rate without triggering line negotiation.

Prerequisites

The ADSL interface has been deactivated by using the **shutdown** command.

Follow-up Procedure

To make bit exchange take effect immediately on an ADSL interface, run the **undo shutdown** command to activate the ADSL interface.

Precautions

Bit exchange must be enabled on devices on both ends of a line and takes effect only after the line is activated.

Example

Disable bit exchange on ADSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl bitswap off
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.15.8 interface atm (adsl)

5.15.11 shutdown (adsl)

5.15.2 adsl sra (adsl)

Function

The **adsl sra** command enables or disables seamless rate adaptation on an ADSL interface.

By default, seamless rate adaptation is disabled on an ADSL interface.

Format

adsl sra { **off** | **on** }

Parameters

Parameter	Description	Value
off	Disables seamless rate adaptation on an ADSL interface.	-
on	Enables seamless rate adaptation on an ADSL interface.	-

Views

ADSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the external environment changes, to prevent the line disconnection, use the bit exchange function to adjust bit distribution or the power among sub-channels without deactivating the line. The bit exchange function, however, cannot change the line rate. When the line environment becomes worse, the bit exchange function cannot meet the requirement for the bit error rate. The bit exchange function just allows the line to be activated at a smaller rate. When the line environment becomes better, the bit exchange function cannot adjust the rate, wasting line resources.

Seamless rate adaptation solves the preceding problem. It dynamically adjusts the line rate without reactivating the line.

Prerequisites

The ADSL interface has been deactivated by using the **shutdown** command.

Follow-up Procedure

To make seamless rate adaptation take effect immediately on an ADSL interface, run the **undo shutdown** command to activate the ADSL interface.

Precautions

Seamless rate adaptation must be enabled on devices on both ends of a line and takes effect only after the line is activated.

Example

Enable seamless rate adaptation on ADSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl sra on
[Huawei-Atm1/0/0] undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

5.15.8 interface atm (adsl)

5.15.11 shutdown (adsl)

5.15.3 adsl standard (adsl)

Function

The **adsl standard** command configures a transmission standard for an ADSL interface.

The **undo adsl standard** command restores the default setting.

By default, an ADSL interface transmission standard is **auto**.

Format

adsl standard { **adsl2** [**annexm** | **annexj** | **annexl**] | **adsl2+** [**annexm** | **annexj**] | **auto** | **gdmt** | **t1413** }

undo adsl standard

Parameters

Parameter	Description	Value
adsl2	Configures ADSL2 (G.992.3) for an ADSL interface. ADSL2 provides fast transmission rates by improving the modulation rate, coding gain, and initialization state machine, reducing the frame overhead, and using enhanced signal processing methods. ADSL2 can provide a maximum of 1 Mbit/s upstream transmission rate and 12 Mbit/s downstream transmission rate.	-
adsl2+	Configures ADSL2+ (G.992.5) for an ADSL interface. ADSL2+ expands the frequency band to 2.208 MHz and provides a maximum of 1 Mbit/s upstream transmission rate and 24 Mbit/s downstream transmission rate.	-
annexm	Supports the expansion of upstream frequency band of ADSL2 or ADSL2+ and provides a maximum of 2 Mbit/s upstream transmission rate. **NOTE** ADSL boards on the device include ADSL-A/M and ADSL-B/J boards. Only ADSL-A/M boards support this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
annexj	Supports the expansion of upstream frequency band of ADSL2 or ADSL2+ and provides a maximum of 3.078 Mbit/s upstream transmission rate. **NOTE** ADSL boards on the device include ADSL-A/M and ADSL-B/J boards. Only ADSL-B/J boards support this parameter.	-
annexl	Configures reach extended ADSL2 (AnnexL for short) for an ADSL interface. AnnexL is defined in ADSL2 recommendation. It uses a narrower frequency band and optimizes the power spectral density (PSD) mask to provide long-distance transmission of high performance. **NOTE** ADSL boards on the device include ADSL-A/M and ADSL-B/J boards. Only ADSL-A/M boards support this parameter.	-
auto	Configures an ADSL interface to automatically adapt to the transmission standard of the remote ADSL interface. If this parameter is specified, the device selects the same transmission standard as a DSLAM from G.DMT, ADSL2, AnnexL, ADSL2+, AnnexM, and T1.413.	-
gdmt	Configures G.DMT (G.992.1) for an ADSL interface. G.DMT provides an upstream frequency band from 25 kHz to 138 kHz, a downstream frequency band from 138 kHz to 1.104 MHz, a maximum of 1 Mbit/s upstream transmission rate, and a maximum of 8 Mbit/s downstream transmission rate.	-
t1413	Configures T1.413 for an ADSL interface. When an ADSL interface uses T1.413, the ADSL interface works in full rate mode, and provides a maximum of 1 Mbit/s upstream transmission rate and 8 Mbit/s downstream transmission rate. **NOTE** ADSL boards on the device include ADSL-A/M and ADSL-B/J boards. Only ADSL-A/M boards support this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

ADSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to transmit services on an ADSL line, run the **adsl standard** command to configure the device to use the same transmission standard as a DSLAM. You are advised to configure the device to automatically adapt to the transmission standard of the DSLAM.

Prerequisites

The ADSL interface has been deactivated by using the **shutdown** command.

Follow-up Procedure

To make the transmission standard configured for an ADSL interface take effect, run the **undo shutdown** command on the interface to activate the interface.

Example

Configure T1.413 for ADSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl standard t1413
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.15.8 interface atm (adsl)

5.15.11 shutdown (adsl)

5.15.4 adsl trellis (adsl)

Function

The **adsl trellis** command enables or disables trellis coding on an ADSL interface.

By default, trellis coding is enabled on an ADSL interface.

Format

adsl trellis { **off** | **on** }

Parameters

Parameter	Description	Value
off	Disables trellis coding on an ADSL interface.	-
on	Enables trellis coding on an ADSL interface.	-

Views

ADSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Trellis coding increases the signal noise ratio (SNR) by using a coding algorithm with a high coding efficiency. After trellis coding is enabled, the line activation rate is greatly increased.

Prerequisites

The ADSL interface has been deactivated by using the **shutdown** command.

Follow-up Procedure

To make trellis coding take effect immediately on an ADSL interface, run the **undo shutdown** command to activate the ADSL interface.

Precautions

Trellis coding must be enabled on devices on both ends of a line and takes effect only after the line is activated.

As specified in ADSL2 (G.992.3) and ADSL2+ (G.992.5) standards, trellis coding must be enabled. Under normal circumstances, it is recommended that you do not disable trellis coding; otherwise, interface connection problems may occur.

Example

Disable trellis coding on ADSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl trellis off
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.15.8 interface atm (adsl)

5.15.11 shutdown (adsl)

5.15.5 display dsl all interface

Function

The **display dsl all interface** command displays status information about all xDSL interfaces.

Format

display dsl all interface

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dsl all interface** command to check the negotiation status with xDSL interfaces at the central office, transmission standard, line status, performance statistics, bit exchange status, seamless rate adaptation status, trellis coding status, and card version of the ADSL interface and VDSL interface (in ATM or PTM mode), and check the link status, vendor, and performance statistics of the G.SHDSL interface.

Precautions

This command cannot display information about xDSL sub-interfaces.

Example

Display status information about all xDSL interfaces.

```
<Huawei> display dsl all interface
 Atm1/0/0 information:
 ------------------------------------------------------------
 DSL driver and PHY status
     Line0:
     Training status                    : Showtime
     Transmission mode                      : VDSL2
     VDSL2 profile                      : Profile 17a
     Line status                       : No Defect
     Downstream max. attainable rate(Kbps): 142372
     Upstream max. attainable rate(Kbps)  : 63853
     Downstream actual net data rate(Kbps): 60016
     Upstream actual net data rate(Kbps)  : 20013
     Downstream SNR margin(dB)            : 28.8
```

```
    Upstream SNR margin(dB)              : 31.9
    Downstream attenuation(dB)           : 0.0
    Upstream attenuation(dB)             : 0.0
    Downstream output power(dBm)         : 14.5
    Upstream output power(dBm)           : -6.4
    Downstream total cells               : 1348781845
    Upstream total cells                 : 0
    Downstream data cells                : 0
    Upstream data cells                  : 0
    Downstream bit errors                : 0
    Upstream bit errors                  : 0
    Total drop cells                     : 0
    Downstream total ES count            : 60
    Upstream total ES count              : 0
    Downstream total SES count           : 59
    Upstream total SES count             : 0
    Downstream total UAS count           : 849
    Upstream total UAS count             : 849
    Total AS count                       : 86128

    Line1:
    Training status                      : Showtime
    Transmission mode                    : VDSL2
    VDSL2 profile                        : Profile 17a
    Line status                          : No Defect
    Downstream max. attainable rate(Kbps): 145984
    Upstream max. attainable rate(Kbps)  : 64009
    Downstream actual net data rate(Kbps): 60016
    Upstream actual net data rate(Kbps)  : 20013
    Downstream SNR margin(dB)            : 28.0
    Upstream SNR margin(dB)              : 32.4
    Downstream attenuation(dB)           : 0.0
    Upstream attenuation(dB)             : 0.0
    Downstream output power(dBm)         : 13.1
    Upstream output power(dBm)           : -6.5
    Downstream total cells               : 1360438742
    Upstream total cells                 : 0
    Downstream data cells                : 0
    Upstream data cells                  : 0
    Downstream bit errors                : 0
    Upstream bit errors                  : 0
    Total drop cells                     : 0
    Downstream total ES count            : 59
    Upstream total ES count              : 0
    Downstream total SES count           : 56
    Upstream total SES count             : 0
    Downstream total UAS count           : 683
    Upstream total UAS count             : 683
    Total AS count                       : 86230

Line capability
    Bitswap                              : On
    SRA                                  : Off
    Trellis coding                       : On

Board version
    vendor ID                            : 0xB5 0 "BDCM" 0 0
    vendor serial                        : 10000000000000000000000000000000
    Board ID                             : 963168MBV_17A
    Software version                     : 4.12L.08
    Bootloader (CFE) version             : 1.0.38-112.118
    DSL PHY and driver version           : A2pvbF038j.d24h
    Build timestamp                      : 20170706_1814

ATU-C version
    vendor ID                            : BDCM:0x938f
    vendor number                        : 0x938f
-------------------------------------------------------------
```

```
Atm2/0/1 information:
-----------------------------------------------------------------
 Operating mode                          :CPE
 Port admin status                       :Active
 Port running status                     :Activated
 Port admin bind status                  :EFM-2
 Bind group master port                  :0
 Bind group running port                 :1;
 LOSWS Defect alarm                      :none
 SNR Margin alarm                        :none
 Loop Attenuation alarm                  :none
 Modem status                            :DOWN_READY
 Condition                               :NO_COND_
 Reason                                  :ERR_UNUSED_
 Port transmission mode                  :G.991.2 Annex A&B&F&G
 Port power spectral density             :Symmetric
 Port line probe                         :Enable
 Inventory of SHDSL port 0
 Vendor ID                               :Infineon
 Vendor mode                             :SOCRATES
 Vendor serial                           :4e_2e_1e
 EOC version                             :0
 Standard version                        :8
 Vendor list                             :-
 Vendor issue                            :1
 Software code                           :1.7.2
 Equipment code                          :-
 Information of other vendor             :V200R008
 Transmission mode capability            :G.991.2 Annex A&B&F&G
-----------------------------------------------------------------
```

Table 5-49 Description of the **display dsl all interface** command output

Item	Description
Atm1/0/0 information	Information about ATM1/0/0. ATM1/0/0 in this example is a VDSL interface. For detailed command output descriptions, see **display dsl interface atm (vdsl)** and **display dsl interface ethernet (vdsl)**. For detailed command output description of an ADSL interface, see **display dsl interface atm (adsl)**.
Atm2/0/1 information	Information about ATM2/0/1. ATM2/0/1 in this example is a G.SHDSL interface. For detailed command output description, see **display dsl interface (g.shdsl)**.

5.15.6 display interface atm (adsl)

Function

The **display interface atm** command displays the configuration and status of an ADSL interface.

Format

display interface atm [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Specifies the ADSL interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the interface status or locating faults on an ADSL interface, run the **display interface atm** command on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Example

Display the configuration and status of ADSL interface 1/0/0.

```
<Huawei> display interface atm 1/0/0
Atm1/0/0 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Atm1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1488
Internet Address is 1.1.1.1/24
AAL enabled: AAL5, Maximum PVCs: 16
PVCs on main-interface: 2 (Total PVCs: 6)
Last physical up time   : 2012-12-31 17:46:03
Last physical down time : 2013-01-04 16:56:30
Current system time: 2013-01-06 14:06:16

Port PHY type    : ADSL
CRC anomaly count: 0
The physical up times since the board startup  : 1
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec

Input correct packet:  264237922 packets, Input total data:  38232948935 bytes
  OAM Cells:            2398245,  ASM Cells:                  0
  Packet Errors:              1,  Packet Discards:            1
  Cell Errors:              888

Output:  261837042 packets, 38967726112 bytes
  OAM Cells:            2398272,  ASM Cells:                  0
  Packet Errors:              0,  Packet Discards:            0
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-50 Description of the display interface atm command output

Item	Description
Atm1/0/0 current state	Physical status of ATM1/0/0: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the network administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Description	Interface description. The description contains a maximum of 242 case-sensitive characters, with spaces supported. This field describes functions of the ADSL interface.
The Maximum Transmit Unit is	Maximum transmit unit (MTU) of the interface. By default, the MTU is 1488 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded.
Internet Address is	IP address of the interface. If no IP address is assigned to the interface, the system displays "Internet protocol processing : disabled".
AAL enabled	ATM Adaptation Layer (AAL). **NOTE** The device supports only AAL5.
Maximum PVCs	Maximum number of permanent virtual circuits (PVCs).
PVCs on main-interface: (Total PVCs:)	Number of PVCs on the main interface (total number of PVCs on both the main interface and sub-interfaces).
Last physical up time	Last time the interface went Up physically. If the value of this field is displayed as "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last physical down time	Last time the interface went Down physically. If the value of this field is displayed as "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Port PHY type	Physical type of the interface.
CRC anomaly count	Number of abnormal CRC packets.
The physical uptimes since the system startup	Number of times that interface becomes Up after the system starts.
OAM Cells	Number of OAM cells.
ASM Cells	Number of incoming autonomous status message (ASM) cells.
Packet Errors	Number of error packets.
Packet Discards	Number of discard packets.
Cell Errors	Number of error cells.
Input bandwidth utilization	Percentage of the incoming packet rate to the total bandwidth.
Output bandwidth utilization	Percentage of the outgoing packet rate to the total bandwidth.

Related Topics

5.15.8 interface atm (adsl)

5.15.7 display dsl interface atm (adsl)

Function

The **display dsl interface atm** command displays information about an ADSL interface.

Format

display dsl interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the ADSL interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

According to the **display dsl interface atm** command output, you can check the training status, transmission standard, line status, performance statistics, bit exchange status, seamless rate adaptation status, trellis coding status, and board version of the ADSL interface.

Example

Display information about ADSL interface 1/0/0.

```
<Huawei> display dsl interface atm 1/0/0
 ------------------------------------------------------------
 DSL driver and PHY status
     Training Status                    : Showtime
     Transmission mode                  : ADSL2+
     Line Status                        : No Defect
     Downstream max. attainable rate(Kbps): 28184
     Upstream max. attainable rate(Kbps)  : 2529
     Downstream actual net data rate(Kbps): 24538
     Upstream actual net data rate(Kbps)  : 1021
     Downstream SNR margin(dB)            : 13.1
     Upstream SNR margin(dB)              : 18.9
     Downstream attenuation(dB)           : 0.0
     Upstream attenuation(dB)             : 4.8
     Downstream output power(dB)          : 7.2
     Upstream output power(dB)            : -8.3
     Downstream total cells               : 3305378
     Upstream total cells                 : 74443
     Downstream data cells                : 36545
     Upstream data cells                  : 5447
     Downstream bit errors                : 124
     Upstream bit errors                  : 365
     Total drop cells                     : 241
     Downstream total ES count            : 0
     Upstream total ES count              : 0
     Downstream total SES count           : 0
     Upstream total SES count             : 0
     Downstream total UAS count           : 72
     Upstream total UAS count             : 72
     Total AS count                       : 36

 Line modulations
     G.Dmt                                : Disabled
     T1.413                               : Disabled
```

```
    ADSL2                          : Disabled
    AnnexL                         : Disabled
    ADSL2+                          : Enabled
    AnnexM                           : Disabled

Line capability
    Bitswap                        : On
    SRA                           : Off
    Trellis coding                  : On

Board version
    vendor ID                       : BDCM:0x938f
    vendor serial                   : 0x938f
    Board ID:                      : 963281TAN
    Software version                  : 4.06L.03
    Bootloader (CFE) version            : 1.0.37-106.24
    DSL PHY and driver version           : A2pD033a.d23c
    Build timestamp                   : 20110221_2122

ATU-C version
    vendor ID                       : BDCM:0x938f
    vendor number                     : 0x938f
-------------------------------------------------------------
```

Table 5-51 Description of the display dsl interface atm 1/0/0 command output

Item	Sub-item	Description
DSL driver and PHY status	Training Status	Training status of the ADSL interface: ● Idle: indicates that the ADSL interface is idle. ● Training: indicates that the ADSL interface is negotiating with the remote ADSL interface. ● Showtime: indicates that negotiation between the two ADSL interfaces succeeds. **NOTE** Other sub-items of **DSL driver and PHY status** can be displayed only after negotiation between the local and remote ADSL interfaces succeeds.

Item	Sub-item	Description
	Transmission mode	Transmission standard of the ADSL interface: ● ADSL2: provides a maximum of 1 Mbit/s upstream transmission rate and 12 Mbit/s downstream transmission rate. ● ADSL2 AnnexM: expands the upstream frequency band of ADSL2 and provides a maximum of 2 Mbit/s upstream transmission rate. ● RE-ADSL2: is defined in ADSL2 recommendation. It uses a narrower frequency band and optimizes the power spectral density (PSD) mask to provide long-distance transmission of high performance. ● ADSL2+: provides a maximum of 1 Mbit/s upstream transmission rate and 24 Mbit/s downstream transmission rate. ● ADSL2+ AnnexM: expands the upstream frequency band of ADSL2+ and provides a maximum of 2 Mbit/s upstream transmission rate. ● G.DMT: provides a maximum of 1 Mbit/s upstream transmission rate and 8 Mbit/s downstream transmission rate. ● T1.413: provides a maximum of 1 Mbit/s upstream transmission rate and 8 Mbit/s downstream transmission rate. To configure the transmission standard, run the **adsl standard (adsl)** command.
	Line Status	Line status of the ADSL interface: ● No Defect: indicates that the ADSL interface has been activated. ● Loss of Frame: indicates that frames are lost. ● Loss of Signal: indicates that signals are lost. ● Loss of Power: indicates that the device is powered off. ● Loss of Signal Quality: indicates that the signal quality is low.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Downstream max. attainable rate(Kbps)	Maximum downstream transmission rate (in kbit/s).
	Upstream max. attainable rate(Kbps)	Maximum upstream transmission rate (in kbit/s).
	Downstream actual net data rate(Kbps)	Actual downstream transmission rate (in kbit/s).
	Upstream actual net data rate(Kbps)	Actual upstream transmission rate (in kbit/s).
	Downstream SNR margin(dB)	Downstream noise margin (dB).
	Upstream SNR margin(dB)	Upstream noise margin (dB).
	Downstream attenuation(dB)	Downstream attenuation (dB).
	Upstream attenuation(dB)	Upstream attenuation (dB).
	Downstream output power(dB)	Downstream output power (dB).
	Upstream output power(dB)	Upstream output power (dB).
	Downstream total cells	Total number of downstream cells.
	Upstream total cells	Total number of upstream cells.
	Downstream data cells	Number of downstream data cells.
	Upstream data cells	Number of upstream data cells.
	Downstream bit errors	Downstream bit errors.
	Upstream bit errors	Upstream bit errors.
	Total drop cells	Total number of dropped cells.
	Downstream total ES count	Total number of downstream errored seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Upstream total ES count	Total number of upstream errored seconds.
	Downstream total SES count	Total number of downstream severely errored seconds.
	Upstream total SES count	Total number of upstream severely errored seconds.
	Downstream total UAS count	Total number of downstream unavailable seconds.
	Upstream total UAS count	Total number of upstream unavailable seconds.
	Total AS count	Total number of available seconds.
Line modulations	G.Dmt	Status of the transmission standards supported by the ADSL interface: ● If the device is configured to automatically adapt to the transmission standard of the DSLAM, G.Dmt, T1.413, ADSL2, AnnexL, ADSL2+, and AnnexM are enabled. The device then selects the same transmission standard as the DSLAM from the preceding transmission standards. You can know which transmission standard is selected by viewing the **Transmission mode** field. ● If a transmission standard is specified for the ADSL interface, only this transmission standard is enabled.
	T1.413	
	ADSL2	
	AnnexL	
	ADSL2+	
	AnnexM	
Line capability	Bitswap	Bit exchange status: ● On: enabled ● Off: disabled To configure bit exchange, run the **adsl bitswap (adsl)** command.
	SRA	Seamless rate adaptation status: ● On: enabled ● Off: disabled To configure seamless rate adaptation, run the **adsl sra (adsl)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Trellis coding	Trellis coding status: ● On: enabled ● Off: disabled To configure trellis coding, run the **adsl trellis (adsl)** command.
Board version	vendor ID	ID of the peer-side chip vendor.
	vendor serial	Sequence number of the peer-side chip vendor.
	Board ID	Board ID.
	Software version	System software version.
	Bootloader (CFE) version	BootRom version.
	DSL PHY and driver version	Board driver version.
	Build timestamp	Time the board is registered.
ATU-C version	vendor ID	ID of the peer-side chip vendor.
	vendor number	Sequence number of the peer-side chip vendor.

Related Topics

5.15.8 interface atm (adsl)

5.15.8 interface atm (adsl)

Function

The **interface atm** command displays the ADSL interface view.

Format

interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an ADSL interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **interface atm** command displays the ADSL interface view.

Example

Enter the view of ADSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0]
```

Related Topics

5.15.6 display interface atm (adsl)

5.15.7 display dsl interface atm (adsl)

5.15.9 mtu (adsl)

Function

The **mtu** command sets the maximum transmission unit (MTU) for a ADSL interface.

The **undo mtu** command restores the default MTU.

By default, the MTU of a ADSL interface is 1488 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a ADSL interface.	The value is an integer that ranges from 128 to 1510, in bytes.

Views

ADSL interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than the MTU.

If forcible unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. Therefore, large packets must be forcibly fragmented to prevent packet loss on the network. In this case, you can run the **mtu** command to set the size of a fragment.

Follow-up Procedure

Run the **shutdown** and **undo shutdown** commands to restart the related physical interface to make the configuration take effect.

Precautions

If you run the **mtu** command multiple times in the same ADSL interface view, only the latest configuration takes effect.

After the transparent bridge is enabled on the device and the ADSL interface is added to the bridge group, the MTU cannot be greater than 1470 bytes.

Example

Set the MTU of a ADSL interface to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] mtu 1200
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] undo shutdown
```

5.15.10 xdsl auto return

Function

The **xdsl auto return** command enables the auto return function.

By default, the auto return function is disabled.

Format

xdsl auto return { **disable** | **enable** }

Parameters

Parameter	Description	Value
disable	Disables the auto return function.	-
enable	Enables the auto return function.	-

Views

User view

Default Level

0: Visit level

Usage Guidelines

This command is not supported currently, and is used for future expansion.

Example

Enable the auto return function.

```
<Huawei> xdsl auto return enable
```

5.15.11 shutdown (adsl)

Function

The **shutdown** command deactivates an ADSL interface.

The **undo shutdown** command activates an ADSL interface.

By default, an ADSL interface is activated.

Format

shutdown

undo shutdown

Parameters

None

Views

ADSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ADSL interfaces must be activated before transmitting services. Activation of an ADSL interface refers to the training between a DSLAM and a CPE. During the training, the two devices check the line distance and status based on parameters such as the transmission standard, upstream and downstream line rates, and specified noise margin to determine whether they can work properly under the existing conditions. If the training succeeds, the ADSL interface on the CPE is activated and can transmit services between the two devices.

The device functions as a CPE and aggregates services to a DSLAM by using an ADSL interface.

After a device starts, its ADSL interface is automatically activated. The ADSL interface remains activated as long as its ADSL line works properly. To enable the device to communicate with a DSLAM, run the **shutdown** command to deactivate the ADSL interface on the device, set parameters for the interface, and then run the **undo shutdown** command to reactivate this interface to make configurations take effect.

Follow-up Procedure

After an ADSL interface is deactivated, it is disconnected from a DSLAM. To enable the ADSL interface to transmit services, reactivate this ADSL interface.

Example

Activate ADSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.15.8 interface atm (adsl)

5.16 VDSL Interface Configuration Commands

NOTE

The AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR129W, AR169, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR169F, AR169BF, AR169FVW, AR169FVW-8S, AR169FGW-L, AR169G-L, AR169JFVW-4B4S, AR169JFVW-2S, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, and AR169FGVW-L support VDSL interfaces.

AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR129W, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, and AR169RW-P-M9 do not support T1.413.AR169EW, AR169EGW-L, AR169F, AR169BF, AR169FVW, AR169FVW-8S, AR169FGW-L, AR169JFVW-4B4S, AR169JFVW-2S, and AR169FGVW-L only support AnnexA and AnnexM. AR169BF only supports AnnexB and AnnexJ.

 Copyright © Huawei Technologies Co., Ltd.

5.16.1 adsl bitswap (vdsl)

Function

The **adsl bitswap** command enables or disables bit exchange on a VDSL interface.

By default, bit exchange is enabled on a VDSL interface.

Format

adsl bitswap { **off** | **on** }

Parameters

Parameter	Description	Value
off	Disables bit exchange on a VDSL interface.	-
on	Enables bit exchange on a VDSL interface.	-

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During line activation, every sub-channel calculates the signal-to-noise ratio (SNR) and the number of bits to be transmitted. After the line is activated, the SNR may change because the external environment changes. For example, the SNRs of some sub-channels reduce, whereas the SNRs of some other sub-channels increase. After a long period of time, the line may be disconnected.

The bit exchange function has the following advantages:

- Allows sub-channels failing to transmit the specified number of bits to switch some bits to sub-channels with higher SNRs.
- Reduces the transmit power of sub-channels with higher SNRs to increase the sending rate and SNRs of sub-channels with lower SNRs.

  This reduces the bit error rate without triggering line negotiation.

Prerequisites

The VDSL interface has been deactivated by using the **shutdown** command.

Follow-up Procedure

To make bit exchange take effect immediately on a VDSL interface, run the **undo shutdown** command to activate the VDSL interface.

Precautions

Bit exchange must be enabled on devices on both ends of a line and takes effect only after the line is activated.

Example

Disable bit exchange on VDSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl bitswap off
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.16.12 interface atm (vdsl)

5.16.16 shutdown (vdsl)

5.16.2 adsl sra (vdsl)

Function

The **adsl sra** command enables or disables seamless rate adaptation on a VDSL interface.

By default, seamless rate adaptation is disabled on a VDSL interface.

Format

adsl sra { **off** | **on** }

Parameters

Parameter	Description	Value
off	Disables seamless rate adaptation on a VDSL interface.	-
on	Enables seamless rate adaptation on a VDSL interface.	-

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the external environment changes, to prevent the line disconnection, use the bit exchange function to adjust bit distribution or the power among sub-channels without deactivating the line. The bit exchange function, however, cannot change the line rate. When the line environment becomes worse, the bit exchange function cannot meet the requirement for the bit error rate. The bit exchange function just allows the line to be activated at a smaller rate. When the line environment becomes better, the bit exchange function cannot adjust the rate, wasting line resources.

Seamless rate adaptation solves the preceding problem. It dynamically adjusts the line rate without reactivating the line.

Prerequisites

The VDSL interface has been deactivated by using the **shutdown** command.

Follow-up Procedure

To make seamless rate adaptation take effect immediately on a VDSL interface, run the **undo shutdown** command to activate the VDSL interface.

Precautions

Seamless rate adaptation must be enabled on devices on both ends of a line and takes effect only after the line is activated.

Example

Enable seamless rate adaptation on VDSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl sra on
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.16.12 interface atm (vdsl)

5.16.16 shutdown (vdsl)

5.16.3 adsl standard (vdsl)

Function

The **adsl standard** command configures a transmission standard for a VDSL interface in ATM mode.

The **undo adsl standard** command restores the default setting.

By default, the transmission standard of a VDSL interface in ATM mode is **auto**.

Format

adsl standard { **adsl2** [**annexa** | **annexm** | **annexb** | **annexj** | **annexl**] | **adsl2+** [**annexa** | **annexm** | **annexb** | **annexj**] | **auto** [**over-pots** | **over-isdn**] | **gdmt** [**annexa** | **annexb**] | **t1413** }

undo adsl standard

Parameters

Parameter	Description	Value
adsl2	Specifies ADSL2 (G.992.3) as the transmission standard of a VDSL interface. ADSL2 provides faster transmission rates on the same frequency band as ADSL by improving the modulation rate, coding gain, and initialization state machine, reducing the frame head overhead, and using the enhanced signal processing algorithm. ADSL2 can provide a maximum of 1 Mbit/s upstream transmission rate and 12 Mbit/s downstream transmission rate.	-
adsl2+	Specifies ADSL2+ (G.992.5) as the transmission standard of a VDSL interface. The frequency band that ADSL2+ uses is expanded to 2.208 MHz. ADSL2+ provides a maximum of 1 Mbit/s upstream transmission rate and 24 Mbit/s downstream transmission rate.	-
annexa	Indicates that POTS services of the G.DMT, ADSL2, or ADSL2+ standard are compatible.	-
annexm	Indicates that the upstream frequency band of ADSL2 or ADSL2+ can be expanded and a maximum of 2 Mbit/s upstream transmission rate is provided.	-
annexb	Indicates that ISDN services of the G.DMT, ADSL2, or ADSL2+ standard are compatible.	-
annexj	Indicates that the upstream frequency band of ADSL2 or ADSL2+ can be expanded and ADSL2 or ADSL2+ can provide a maximum of 2.9 Mbit/s upstream transmission rate.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
annexl	Specifies AnnexL as the transmission standard of a VDSL interface. Reach extended ADSL2 (AnnexL for short) is defined in ADSL2 recommendation. AnnexL uses a narrower frequency band and optimizes the transmit power spectrum profile to provide long-distance transmission with high performance.	-
auto	Configures a VDSL interface to automatically use the transmission standard of the remote VDSL interface. If this parameter is specified, the device selects the same transmission standard as a DSLAM from G.DMT, ADSL2, AnnexL, ADSL2+, AnnexM, and T1.413.	-
over-pots	Specifies AnnexA as the automatic transmission standard of a VDSL interface. AnnexA is also called ADSL over POTS; the low frequency band carries voice services.	-
over-isdn	Specifies AnnexB as the automatic transmission standard of a VDSL interface. AnnexB is also called ADSL over ISDN; the low frequency band carries ISDN services.	-
gdmt	Specifies G.DMT (G.992.1) as the transmission standard of a VDSL interface. G.DMT provides an upstream frequency band from 25 kHz to 138 kHz, a downstream frequency band from 138 kHz to 1.104 MHz, a maximum of 1 Mbit/s upstream transmission rate, and a maximum of 8 Mbit/s downstream transmission rate.	-
t1413	Specifies T1.413 as the transmission standard of a VDSL interface. T1.413 is a full-rate ADSL protocol, and provides a maximum of 800 kbit/s upstream transmission rate and 8 Mbit/s downstream transmission rate.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that service flows are properly transmitted on a VDSL, run the **adsl standard** command to configure the transmission standard of a VDSL interface in ATM mode to be the same as that of the remote interface. You are advised to configure a VDSL interface to automatically use the transmission standard of the remote interface.

Precautions

AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR129W, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, and AR169RW-P-M9 do not support T1.413.AR169EW, AR169EGW-L, AR169F, AR169BF, AR169FVW, AR169FVW-8S, AR169FGW-L, AR169JFVW-4B4S, AR169JFVW-2S, and AR169FGVW-L only support AnnexA and AnnexM. AR169BF only supports AnnexB and AnnexJ.

When a VDSL line carries voice or ISDN services and the VDSL interface is configured to work in auto mode, the interface cannot go Up. In this case, specify the **over-pots** and **over-isdn** parameters in the command, respectively.

Prerequisites

The VDSL interface has been deactivated using the **shutdown** command.

Follow-up Procedure

To make the transmission standard configured for a VDSL interface take effect, run the **undo shutdown** command on the interface to activate the interface.

Example

Configure VDSL interface 1/0/0 to use the transmission standard T1.413.

```
<Huawei> system-view
[Huawei] set workmode slot 1 vdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl standard t1413
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.16.12 interface atm (vdsl)

5.16.16 shutdown (vdsl)

5.16.4 adsl trellis (vdsl)

Function

The **adsl trellis** command enables or disables trellis coding on a VDSL interface in ATM mode.

By default, trellis coding is enabled on a VDSL interface in ATM mode.

Format

adsl trellis { **off** | **on** }

Parameters

Parameter	Description	Value
off	Disables trellis coding on a VDSL interface.	-
on	Enables trellis coding on a VDSL interface.	-

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Trellis coding increases the signal noise ratio (SNR) by using a coding algorithm with a high coding efficiency. After trellis coding is enabled, the line activation rate is greatly increased.

Prerequisites

The VDSL interface has been deactivated by using the **shutdown** command.

Follow-up Procedure

To make trellis coding take effect immediately on a VDSL interface, run the **undo shutdown** command to activate the VDSL interface.

Precautions

Trellis coding must be enabled on devices on both ends of a line and takes effect only after the line is activated.

 Copyright © Huawei Technologies Co., Ltd.

As specified in ADSL2 (G.992.3) and ADSL2+ (G.992.5) standards, trellis coding must be enabled. Under normal circumstances, it is recommended that you do not disable trellis coding; otherwise, interface connection problems may occur.

Example

Disable trellis coding on VDSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] adsl trellis off
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.16.16 shutdown (vdsl)

5.16.5 display dsl all interface

Function

The **display dsl all interface** command displays status information about all xDSL interfaces.

Format

display dsl all interface

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dsl all interface** command to check the negotiation status with xDSL interfaces at the central office, transmission standard, line status, performance statistics, bit exchange status, seamless rate adaptation status, trellis coding status, and card version of the ADSL interface and VDSL interface (in ATM or PTM mode), and check the link status, vendor, and performance statistics of the G.SHDSL interface.

Precautions

This command cannot display information about xDSL sub-interfaces.

Example

Display status information about all xDSL interfaces.

```
<Huawei> display dsl all interface
 Atm1/0/0 information:
 ------------------------------------------------------------
 DSL driver and PHY status
     Line0:
     Training status                    : Showtime
     Transmission mode                  : VDSL2
     VDSL2 profile                      : Profile 17a
     Line status                        : No Defect
     Downstream max. attainable rate(Kbps): 142372
     Upstream max. attainable rate(Kbps)  : 63853
     Downstream actual net data rate(Kbps): 60016
     Upstream actual net data rate(Kbps)  : 20013
     Downstream SNR margin(dB)            : 28.8
     Upstream SNR margin(dB)              : 31.9
     Downstream attenuation(dB)           : 0.0
     Upstream attenuation(dB)             : 0.0
     Downstream output power(dBm)         : 14.5
     Upstream output power(dBm)           : -6.4
     Downstream total cells               : 1348781845
     Upstream total cells                 : 0
     Downstream data cells                : 0
     Upstream data cells                  : 0
     Downstream bit errors                : 0
     Upstream bit errors                  : 0
     Total drop cells                     : 0
     Downstream total ES count            : 60
     Upstream total ES count              : 0
     Downstream total SES count           : 59
     Upstream total SES count             : 0
     Downstream total UAS count           : 849
     Upstream total UAS count             : 849
     Total AS count                       : 86128

     Line1:
     Training status                    : Showtime
     Transmission mode                  : VDSL2
     VDSL2 profile                      : Profile 17a
     Line status                        : No Defect
     Downstream max. attainable rate(Kbps): 145984
     Upstream max. attainable rate(Kbps)  : 64009
     Downstream actual net data rate(Kbps): 60016
     Upstream actual net data rate(Kbps)  : 20013
     Downstream SNR margin(dB)            : 28.0
     Upstream SNR margin(dB)              : 32.4
     Downstream attenuation(dB)           : 0.0
     Upstream attenuation(dB)             : 0.0
     Downstream output power(dBm)         : 13.1
     Upstream output power(dBm)           : -6.5
     Downstream total cells               : 1360438742
     Upstream total cells                 : 0
     Downstream data cells                : 0
     Upstream data cells                  : 0
     Downstream bit errors                : 0
     Upstream bit errors                  : 0
     Total drop cells                     : 0
     Downstream total ES count            : 59
     Upstream total ES count              : 0
     Downstream total SES count           : 56
     Upstream total SES count             : 0
     Downstream total UAS count           : 683
     Upstream total UAS count             : 683
     Total AS count                       : 86230

 Line capability
```

```
    Bitswap                        : On
    SRA                            : Off
    Trellis coding                 : On

Board version
    vendor ID                      : 0xB5 0 "BDCM" 0 0
    vendor serial                  : 10000000000000000000000000000000
    Board ID                       : 963168MBV_17A
    Software version               : 4.12L.08
    Bootloader (CFE) version       : 1.0.38-112.118
    DSL PHY and driver version     : A2pvbF038j.d24h
    Build timestamp                : 20170706_1814

ATU-C version
    vendor ID                      : BDCM:0x938f
    vendor number                  : 0x938f
-------------------------------------------------------------
Atm2/0/1 information:
-------------------------------------------------------------------
 Operating mode                          :CPE
 Port admin status                       :Active
 Port running status                     :Activated
 Port admin bind status                  :EFM-2
 Bind group master port                  :0
 Bind group running port                 :1;
 LOSWS Defect alarm                      :none
 SNR Margin alarm                        :none
 Loop Attenuation alarm                  :none
 Modem status                            :DOWN_READY
 Condition                               :NO_COND_
 Reason                                  :ERR_UNUSED_
 Port transmission mode                  :G.991.2 Annex A&B&F&G
 Port power spectral density             :Symmetric
 Port line probe                         :Enable
 Inventory of SHDSL port 0
 Vendor ID                               :Infineon
 Vendor mode                             :SOCRATES
 Vendor serial                           :4e_2e_1e
 EOC version                             :0
 Standard version                        :8
 Vendor list                             :-
 Vendor issue                            :1
 Software code                           :1.7.2
 Equipment code                          :-
 Information of other vendor             :V200R008
 Transmission mode capability            :G.991.2 Annex A&B&F&G
-------------------------------------------------------------
```

Table 5-52 Description of the **display dsl all interface** command output

Item	Description
Atm1/0/0 information	Information about ATM1/0/0. ATM1/0/0 in this example is a VDSL interface. For detailed command output descriptions, see **display dsl interface atm (vdsl)** and **display dsl interface ethernet (vdsl)**. For detailed command output description of an ADSL interface, see **display dsl interface atm (adsl)**.
Atm2/0/1 information	Information about ATM2/0/1. ATM2/0/1 in this example is a G.SHDSL interface. For detailed command output description, see **display dsl interface (g.shdsl)**.

5.16.6 display dsl interface atm (vdsl)

Function

The **display dsl interface atm** command displays information about a VDSL interface in ATM mode.

Format

display dsl interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the interface number of the VDSL interface in ATM mode.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dsl interface atm** command displays the training status, transmission standard, line status, performance statistics, bit exchange status, seamless rate adaptation status, trellis coding status, and board version of the VDSL interface.

Example

Display information about VDSL interface 1/0/0 in ATM mode.

```
<Huawei> display dsl interface atm 1/0/0
 ------------------------------------------------------------
 DSL Connection Status
     DSL sync count                      : 1
     DSL up time: 0 day(s) 0 hour(s)
                  2 minute(s) 1 second(s)
 DSL driver and PHY status
     Training Status                     : Showtime
     Transmission Mode                   : ADSL2
     Line Status                         : No Defect
     Downstream max. attainable rate(Kbps): 132740
     Upstream max. attainable rate(Kbps)  : 44503
     Downstream actual net data rate(Kbps): 51399
     Upstream actual net data rate(Kbps)  : 25708
     Downstream SNR margin(dB)            : 28.8
     Upstream SNR margin(dB)              : 27.0
     Downstream attenuation(dB)           : 0.0
     Upstream attenuation(dB)             : 0.0
```

```
    Downstream output power(dBm)          : 7.5
    Upstream output power(dBm)            : -4.8
    Downstream total cells                : 826623466
    Upstream total cells                  : 413437274
    Downstream data cells                 : 672651340
    Upstream data cells                   : 246036145
    Downstream bit errors                 : 0
    Upstream bit errors                   : 0
    Total drop cells                      : 0
    Downstream total ES count             : 0
    Upstream total ES count               : 0
    Downstream total SES count            : 0
    Upstream total SES count              : 0
    Downstream total UAS count            : 31
    Upstream total UAS count              : 31
    Total AS count                        : 6820
    Downstream CRC errors                 : 0
    Upstream CRC errors                   : 0
    Downstream FEC count                  : 0
    Upstream FEC count                    : 0

Line modulations
    G.Dmt                                 : Enabled
    T1.413                                : Enabled
    ADSL2                                 : Enabled
    AnnexL                                : Enabled
    ADSL2+                                : Enabled
    AnnexM                                : Enabled

Line capability
    Bitswap                               : On
    SRA                                   : Off
    Trellis coding                        : On

Board version
    vendor ID                             : BDCM:0x938f
    vendor number                         : 0x938f
    Board ID:                             : 963281TAN
    Software version                      : 4.06L.03
    Bootloader (CFE) version              : 1.0.37-106.24
    DSL PHY and driver version            : A2pD033a.d23c
    Build timestamp                       : 20110221_2122

ATU-C version
    vendor ID                             : BDCM:0x938f
    vendor number                         : 0x938f
-------------------------------------------------------------
```

Table 5-53 Description of the **display dsl interface atm** command output

Item	Sub-item	Description
DSL Connection Status	DSL sync count	Total number of times that the DSL link synchronization.
	DSL up time	The total time of consecutive times that the DSL link up.

Item	Sub-item	Description
DSL driver and PHY status	Training Status	Training status of the VDSL interface: ● Idle: indicates that the VDSL interface is idle. ● Training: indicates that the VDSL interface is negotiating with the remote VDSL interface. ● Showtime: indicates that negotiation between the two VDSL interfaces succeeds. ● NoSignal: indicates that there is no signal. ● Disabled: indicates that the **shutdown (vdsl)** command is executed on the VDSL interface. **NOTE** Other sub-items of **DSL driver and PHY status** can be displayed only after negotiation between the local and remote VDSL interfaces succeeds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Transmission mode	Transmission standard of the VDSL interface: ● ADSL2: provides a maximum of 1 Mbit/s upstream transmission rate and 12 Mbit/s downstream transmission rate. ● ADSL2 AnnexM: expands the upstream frequency band of ADSL2 and provides a maximum of 2 Mbit/s upstream transmission rate. ● RE-ADSL2: is defined in ADSL2 recommendation. It uses a narrower frequency band and optimizes the power spectral density (PSD) mask to provide long-distance transmission of high performance. ● ADSL2+: provides a maximum of 1 Mbit/s upstream transmission rate and 24 Mbit/s downstream transmission rate. ● ADSL2+ AnnexM: expands the upstream frequency band of ADSL2+ and provides a maximum of 2 Mbit/s upstream transmission rate. ● G.DMT: provides a maximum of 1 Mbit/s upstream transmission rate and 8 Mbit/s downstream transmission rate. ● T1.413: provides a maximum of 800 kbit/s upstream transmission rate and 8 Mbit/s downstream transmission rate. To configure the transmission standard, run the **adsl standard (vdsl)** command.
	Line Status	Line status of the VDSL interface: ● No Defect: indicates that the VDSL interface has been activated. ● Loss of Frame: indicates that frames are lost. ● Loss of Signal: indicates that signals are lost. ● Loss of Power: indicates that the device is powered off. ● Loss of Signal Quality: indicates that the signal quality is low.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Downstream max. attainable rate(Kbps)	Maximum downstream transmission rate (in kbit/s).
	Upstream max. attainable rate(Kbps)	Maximum upstream transmission rate (in kbit/s).
	Downstream actual net data rate(Kbps)	Actual downstream transmission rate (in kbit/s).
	Upstream actual net data rate(Kbps)	Actual upstream transmission rate (in kbit/s).
	Downstream SNR margin(dB)	Downstream noise margin (dB).
	Upstream SNR margin(dB)	Upstream noise margin (dB).
	Downstream attenuation(dB)	Downstream attenuation (dB).
	Upstream attenuation(dB)	Upstream attenuation (dB).
	Downstream output power(dBm)	Downstream output power (dBm).
	Upstream output power(dBm)	Upstream output power (dBm).
	Downstream total cells	Total number of downstream cells.
	Upstream total cells	Total number of upstream cells.
	Downstream data cells	Number of downstream data cells.
	Upstream data cells	Number of upstream data cells.
	Downstream bit errors	Downstream bit errors.
	Upstream bit errors	Upstream bit errors.
	Total drop cells	Total number of dropped cells.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Downstream total ES count	Total number of downstream errored seconds.
	Upstream total ES count	Total number of upstream errored seconds.
	Downstream total SES count	Total number of downstream severely errored seconds.
	Upstream total SES count	Total number of upstream severely errored seconds.
	Downstream total UAS count	Total number of downstream unavailable seconds.
	Upstream total UAS count	Total number of upstream unavailable seconds.
	Total AS count	Total number of available seconds.
	Downstream CRC errors	Total number of downstream CRC errors.
	Upstream CRC errors	Total number of upstream CRC errors.
	Downstream FEC count	Total number of downstream FEC errors.
	Upstream FEC count	Total number of upstream FEC errors.
Line modulations	G.Dmt	Status of the transmission standards supported by the VDSL interface: ● If the device is configured to automatically adapt to the transmission standard of the DSLAM, G.Dmt, T1.413, ADSL2, AnnexL, ADSL2+, and AnnexM are enabled. The device then selects the same transmission standard as the DSLAM from the preceding transmission standards. You can know which transmission standard is selected by viewing the **Transmission mode** field. ● If a transmission standard is specified for the VDSL interface, only this transmission standard is enabled.
	T1.413	
	ADSL2	
	AnnexL	
	ADSL2+	
	AnnexM	

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Line capability	Bitswap	Bit exchange status: ● On: enabled ● Off: disabled To configure bit exchange, run the **adsl bitswap (vdsl)** command.
	SRA	Seamless rate adaptation status: ● On: enabled ● Off: disabled To configure seamless rate adaptation, run the **adsl sra (vdsl)** command.
	Trellis coding	Trellis coding status: ● On: enabled ● Off: disabled To configure trellis coding, run the **adsl trellis (vdsl)** command.
Board version	vendor ID	ID of the peer-side chip vendor.
	vendor number	Sequence number of the peer-side chip vendor.
	Board ID	Board ID.
	Software version	System software version.
	Bootloader (CFE) version	BootRom version.
	DSL PHY and driver version	Board driver version.
	Build timestamp	Time the board is registered.
ATU-C version	vendor ID	ID of the peer-side chip vendor.
	vendor number	Sequence number of the peer-side chip vendor.

Related Topics

5.16.12 interface atm (vdsl)

5.16.7 display dsl hlog interface

Function

The **display dsl hlog interface** command displays information about the HLog parameter of a VDSL interface.

Format

display dsl hlog interface { **atm** | **ethernet** } *interface-number* [**from** *tone-num* **to** *tone-num*]

Parameters

Parameter	Description	Value
{ **atm** | **ethernet** } *interface-number*	Specifies the number of a DSL interface working in the ATM or PTM mode.	-
from *tone-num* **to** *tone-num*	Specifies the tone start number of a DSL interface that needs to be displayed. A maximum number of 50 tone records can be displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Viewing information about the HLog parameter of an interface helps users to determine the quality of DSL links based on the actual link requirement and take corresponding measures to improve the quality of DSL links. The measures include restarting the DSL interface links and replacing the DSL cables.

Example

Display information about the HLog parameter of the VDSL interface ATM 1/0/0.

```
<Huawei> display dsl hlog interface atm 1/0/0 from 0 to 19
Showing up to 50 records.
Tone number      HLog
  0          -96.0000
  1          -96.0000
  2          -96.0000
  3          -96.0000
  4          -96.0000
  5          -96.0000
  6          -96.0000
  7          -96.2500
  8          -4.0625
  9          -4.0625
```

```
10        -4.0625
11        -4.0625
12        -4.0625
13        -4.0625
14        -4.0625
15        -4.0625
16        -0.1875
17        -0.1875
18        -0.1875
19        -0.1875
```

Table 5-54 Description of the **display dsl hlog interface** command output

Item	Description
Showing up to 50 records.	Displays a maximum number of 50 records about the HLog parameter of an interface.
Tone number HLog	Displays information about the HLog parameter corresponding to the tone number of an interface.

Related Topics

5.16.9 display dsl qln interface

5.16.8 display dsl interface ethernet (vdsl)

Function

The **display dsl interface ethernet** command displays information about a VDSL interface in PTM mode.

Format

display dsl interface ethernet *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the interface number of the VDSL interface in PTM mode.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dsl interface ethernet** command displays the training status, transmission standard, line status, performance statistics, bit exchange status, seamless rate adaptation status, trellis coding status, and board version of the VDSL interface.

Example

Display information about VDSL interface 0/0/0 in PTM mode. The following uses the VDSL interface on the AR169F as an example.

```
<Huawei> display dsl interface ethernet 0/0/0
 ------------------------------------------------------------
 DSL driver and PHY status
     Training status                    : Showtime
     Transmission mode                  : VDSL2 AnnexA
     VDSL2 profile                      : Profile 17a
     Line status                        : No Defect
     Downstream max. attainable rate(Kbps): 142372
     Upstream max. attainable rate(Kbps)  : 63853
     Downstream actual net data rate(Kbps): 60016
     Upstream actual net data rate(Kbps)  : 20013
     Downstream SNR margin(dB)            : 28.8
     Upstream SNR margin(dB)              : 31.9
     Downstream attenuation(dB)           : 0.0
     Upstream attenuation(dB)             : 0.0
     Downstream output power(dBm)         : 14.5
     Upstream output power(dBm)           : -6.4
     Downstream total cells               : 1348781845
     Upstream total cells                 : 0
     Downstream data cells                : 0
     Upstream data cells                  : 0
     Downstream bit errors                : 0
     Upstream bit errors                  : 0
     Total drop cells                     : 0
     Downstream total ES count            : 60
     Upstream total ES count              : 0
     Downstream total SES count           : 59
     Upstream total SES count             : 0
     Downstream total UAS count           : 849
     Upstream total UAS count             : 849
     Total AS count                       : 86128

 Line modulations
     VDSL2                                : Enabled
     AnnexA                               : Enabled
     AnnexB                               : Enabled

 Line capability
     Bitswap                              : On
     SRA                                  : Off
     Trellis coding                       : On

 Board version
     vendor ID                            : 0xB5 0 "BDCM" 0 0
     vendor serial                        : 10000000000000000000000000000000
     Board ID                             : 963168MBV_17A
     Software version                     : 4.12L.08
     Bootloader (CFE) version             : 1.0.38-112.118
     DSL PHY and driver version           : A2pvbF038j.d24h

 ATU-C version
     vendor ID                            : BDCM:0x938f
     vendor number                        : 0x938f
 ------------------------------------------------------------
```

Table 5-55 Description of the display dsl interface ethernet 0/0/0 command output

Item	Sub-item	Description
DSL driver and PHY status	Line0	One of two lines of the VDSL interface in PTM mode, Line0.
	Training Status	Training status of the VDSL interface: • Idle: indicates that the VDSL interface is idle. • Training: indicates that the VDSL interface is negotiating with the remote VDSL interface. • Showtime: indicates that negotiation between the two VDSL interfaces succeeds. • NoSignal: indicates that there is no signal. • Disabled: indicates that the **shutdown (vdsl)** command is executed on the VDSL interface. **NOTE** Other sub-items of **DSL driver and PHY status** can be displayed only after negotiation between the local and remote VDSL interfaces succeeds.
	Transmission mode	Transmission standard of the VDSL interface: • VDSL2: provides a maximum of 100 Mbit/s upstream transmission rate and 100 Mbit/s downstream transmission rate. • VDSL2 AnnexA: provides a maximum of 100 Mbit/s upstream transmission rate and 100 Mbit/s downstream transmission rate, supports VDSL2, and is compatible with POTS services. • VDSL2 AnnexB: provides a maximum of 100 Mbit/s upstream transmission rate and 100 Mbit/s downstream transmission rate, supports VDSL2, and is compatible with ISDN services. To configure the transmission standard, run the **vdsl standard** command.
	VDSL2 profile	Spectrum distribution profile.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Line Status	Line status of the VDSL interface: ● No Defect: indicates that the VDSL interface has been activated. ● Loss of Frame: indicates that frames are lost. ● Loss of Signal: indicates that signals are lost. ● Loss of Power: indicates that the device is powered off. ● Loss of Signal Quality: indicates that the signal quality is low.
	Downstream max. attainable rate(Kbps)	Maximum downstream transmission rate (in kbit/s).
	Upstream max. attainable rate(Kbps)	Maximum upstream transmission rate (in kbit/s).
	Downstream actual net data rate(Kbps)	Actual downstream transmission rate (in kbit/s).
	Upstream actual net data rate(Kbps)	Actual upstream transmission rate (in kbit/s).
	Downstream SNR margin(dB)	Downstream noise margin (dB).
	Upstream SNR margin(dB)	Upstream noise margin (dB).
	Downstream attenuation(dB)	Downstream attenuation (dB).
	Upstream attenuation(dB)	Upstream attenuation (dB).
	Downstream output power(dBm)	Downstream output power (dB).
	Upstream output power(dBm)	Upstream output power (dB).
	Downstream total cells	Total number of downstream cells.
	Upstream total cells	Total number of upstream cells.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Downstream data cells	Number of downstream data cells.
	Upstream data cells	Number of upstream data cells.
	Downstream bit errors	Downstream bit errors.
	Upstream bit errors	Upstream bit errors.
	Total drop cells	Total number of dropped cells.
	Downstream total ES count	Total number of downstream errored seconds.
	Upstream total ES count	Total number of upstream errored seconds.
	Downstream total SES count	Total number of downstream severely errored seconds.
	Upstream total SES count	Total number of upstream severely errored seconds.
	Downstream total UAS count	Total number of downstream unavailable seconds.
	Upstream total UAS count	Total number of upstream unavailable seconds.
	Total AS count	Total number of available seconds.
	Line1	One of two lines of the VDSL interface in PTM mode, Line1.
Line modulations	VDSL2	Status of the transmission standards supported by the VDSL interface: ● If the device is configured to automatically adapt to the transmission standard of the VDSL2, AnnexA, and AnnexB are enabled. The device then selects the same transmission standard as the DSLAM from the preceding transmission standards. You can know which transmission standard is selected by viewing the **Transmission mode** field. ● If a transmission standard is specified for the VDSL interface, only this transmission standard is enabled.
	AnnexA	
	AnnexB	

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Line capability	Bitswap	Bit exchange status: • On: enabled • Off: disabled To configure bit exchange, run the **adsl bitswap (vdsl)** command.
	SRA	Seamless rate adaptation status: • On: enabled • Off: disabled To configure seamless rate adaptation, run the **adsl sra (vdsl)** command.
	Trellis coding	Trellis coding status: • On: enabled • Off: disabled To configure trellis coding, run the **adsl trellis (vdsl)** command.
Board version	vendor ID	Vendor ID.
	vendor serial	Device serial number.
	Board ID	Board ID.
	Software version	System software version.
	Bootloader (CFE) version	BootROM version.
	DSL PHY and driver version	Board driver version.
	Build timestamp	Time the board is registered.
ATU-C version	vendor ID	ID of the peer-side chip vendor.
	vendor number	Sequence number of the peer-side chip vendor.

Related Topics

5.16.13 interface ethernet (vdsl)

5.16.9 display dsl qln interface

Function

The **display dsl qln interface** command displays information about the QLN parameter of a DSL interface.

Format

display dsl qln interface { **atm** | **ethernet** } *interface-number* [**from** *tone-num* **to** *tone-num*]

Parameters

Parameter	Description	Value
{ **atm** | **ethernet** } *interface-number*	Specifies the number of a DSL interface working in the ATM or PTM mode.	-
from *tone-num* **to** *tone-num*	Specifies the tone start number of a DSL interface that needs to be displayed. A maximum number of 50 tone records can be displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Viewing information about the QLN parameter of an interface helps users to determine the quality of DSL links based on the actual link requirement and take corresponding measures to improve the quality of DSL links. The measures include restarting the DSL interface links and replacing the DSL cables.

Example

Display information about the QLN parameter of the VDSL interface Ethernet 0/0/0.

```
<Huawei> display dsl qln interface Ethernet 0/0/0 from 4045 to 4095
Showing up to 50 records.
Tone number      QLN
  4045        -160.0000
  4046        -160.0000
  4047        -160.0000
  4048        -160.0000
  4049        -160.0000
  4050        -160.0000
  4051        -160.0000
  4052        -160.0000
  4053        -160.0000
  4054        -160.0000
```

```
4055      -160.0000
4056      -160.0000
4057      -160.0000
4058      -160.0000
4059      -160.0000
4060      -160.0000
4061      -160.0000
4062      -160.0000
4063      -160.0000
4064      -160.0000
4065      -160.0000
4066      -160.0000
4067      -160.0000
4068      -160.0000
4069      -160.0000
4070      -160.0000
4071      -160.0000
4072      -160.0000
4073      -160.0000
4074      -160.0000
4075      -160.0000
4076      -160.0000
4077      -160.0000
4078      -160.0000
4079      -160.0000
4080      -160.0000
4081      -160.0000
4082      -160.0000
4083      -160.0000
4084      -160.0000
4085      -160.0000
4086      -160.0000
4087      -160.0000
4088      -160.0000
4089      -160.0000
4090      -160.0000
4091      -160.0000
4092      -160.0000
4093      -160.0000
4094      -160.0000
```

Table 5-56 Description of the **display dsl qln interface** command output

Item	Description
Showing up to 50 records.	Displays a maximum number of 50 records about the QLN parameter of an interface.
Tone number QLN	Displays information about the QLN parameter corresponding to the tone number of an interface.

Related Topics

5.16.7 display dsl hlog interface

5.16.10 display interface atm (vdsl)

Function

The **display interface atm** command displays the configuration and status of a VDSL interface.

Format

display interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a VDSL interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When monitoring the interface status or locating faults on a VDSL interface, run the **display interface atm** command on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Prerequisites

The VDSL interface is working in ATM mode.

Example

Display the configuration and status of VDSL interface 1/0/0.

```
<Huawei> display interface atm 1/0/0
Atm1/0/0 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Atm1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.1/24
AAL enabled: AAL5, Maximum PVCs: 16
PVCs on main-interface: 1 (Total PVCs: 4)
Last physical up time   : 2012-12-31 17:46:27
Last physical down time : 2013-01-04 16:56:29
Current system time: 2013-01-06 14:06:26

Port PHY type    : VDSL
The physical up times since the system startup : 1
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec

Input:  211359250 packets, 30040764364 bytes
  OAM Cells:            1918511,  ASM Cells:                  0
  Packet Errors:              4,  Packet Discards:            4
  Cell Errors:              636

Output:  211353924 packets, 30617567900 bytes
  OAM Cells:            1918502,  ASM Cells:                  0
```

```
Packet Errors:            0,  Packet Discards:            0
  Input bandwidth utilization  :    0%
  Output bandwidth utilization :    0%
```

Table 5-57 Description of the display interface atm command output

Item	Description
Atm1/0/0 current state	Physical status of ATM1/0/0: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the network administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Description	Interface description. The description contains a maximum of 242 case-sensitive characters, with spaces supported. This field describes functions of the VDSL interface.
The Maximum Transmit Unit is	Maximum transmit unit (MTU) of the interface. By default, the MTU is 1488 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded.
Internet Address is	IP address of the interface. If no IP address is assigned to the interface, the system displays "Internet protocol processing : disabled".
AAL enabled	ATM Adaptation Layer (AAL). **NOTE** The device supports only AAL5.
Maximum PVCs	Maximum number of virtual circuits (PVCs).
PVCs on main-interface: (Total PVCs:)	Number of PVCs on the main interface (total number of PVCs on both the main interface and sub-interfaces).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last physical up time	Last time the interface went Up physically. If the value of this field is displayed as "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Last physical down time	Last time the interface went Down physically. If the value of this field is displayed as "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Port PHY type	Physical type of the interface.
The physical uptimes since the system startup	Number of times that interface becomes Up after the system starts.
OAM Cells	Number of OAM cells.
ASM Cells	Number of incoming autonomous status message (ASM) cells.
Packet Errors	Number of error packets.
Packet Discards	Number of discard packets.
Cell Errors	Number of error cells.
Input bandwidth utilization	Percentage of the incoming packet rate to the total bandwidth.
Output bandwidth utilization	Percentage of the outgoing packet rate to the total bandwidth.

Related Topics

5.16.12 interface atm (vdsl)

5.16.11 display interface ethernet (vdsl)

Function

The **display interface ethernet** command displays the configuration and status of a VDSL interface working in PTM mode.

Format

display interface ethernet *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a VDSL interface working in PTM mode.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When monitoring the interface status or locating faults on a VDSL interface, run the **display interface ethernet** command on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Prerequisites

The VDSL interface is working in PTM mode.

Example

Display the configuration and status of VDSL interface 1/0/0 working in PTM mode.

```
<Huawei> display interface ethernet 1/0/0
Ethernet1/0/0 current state : UP
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Ethernet1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 5678-9876-2345
Last physical up time   : 2011-01-03 17:40:01
Last physical down time : 2011-01-03 17:39:33
Current system time: 2011-01-03 18:24:47

Port PHY type    : VDSL
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec

Input:  0 packets, 0 bytes
  OAM Cells:                0,  ASM Cells:                0
  Packet Errors:            0,  Cell Errors:              0

Output:  0 packets, 0 bytes
  OAM Cells:                0,  ASM Cells:                0
```

```
Input bandwidth utilization  :    0%
Output bandwidth utilization :    0%
```

Table 5-58 Description of the **display interface ethernet** command output

Item	Description
Ethernet1/0/0 current state	Physical status of Ethernet1/0/0: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the network administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Description	Interface description.
The Maximum Transmit Unit is	Maximum transmit unit (MTU) of the interface. By default, the MTU is 1488 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded.
Internet protocol processing	● If no IP address is assigned to the interface, the system displays "disable." ● If an IP address is assigned to the interface, the IP address and subnet mask are displayed.
IP Sending Frames' Format is	Format of the frame contained in the sent IP packet.
Last physical up time	Last time the interface went Up physically. If the value of this field is displayed as "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Last physical down time	Last time the interface went Down physically. If the value of this field is displayed as "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY-MM-DD HH:MM:SS UTC±HH:MM DST format.
Port PHY type	Physical port type.
OAM Cells	Number of OAM cells.
ASM Cells	Number of incoming autonomous status message (ASM) cells.
Packet Errors	Number of error packets.
Cell Errors	Number of error cells.
Input bandwidth utilization	Percentage of the incoming packet rate to the total bandwidth.
Output bandwidth utilization	Percentage of the outgoing packet rate to the total bandwidth.

Related Topics

5.16.13 interface ethernet (vdsl)

5.16.12 interface atm (vdsl)

Function

The **interface atm** command displays the view of a VDSL interface working in ATM mode.

Format

interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a VDSL interface working in ATM mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **interface atm** command displays the view of a VDSL interface working in ATM mode.

Prerequisites

The VDSL interface has been configured to work in ATM mode by using the **5.16.15 set workmode vdsl** command.

By default, VDSL interfaces on a VDSL board work in ATM mode.

Example

Enter the view of VDSL interface 1/0/0 working in ATM mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 vdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0]
```

Related Topics

5.16.15 set workmode vdsl

5.16.13 interface ethernet (vdsl)

Function

The **interface ethernet** command displays the view of a VDSL interface working in PTM mode.

Format

interface ethernet *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a VDSL interface working in PTM mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **interface ethernet** command displays the view of a VDSL interface working in PTM mode.

Prerequisites

The VDSL interface has been configured to work in PTM mode by using the **5.16.15 set workmode vdsl** command.

By default, VDSL interfaces on a VDSL board work in PTM mode.

Example

Enter the view of VDSL interface 1/0/0 working in PTM mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 vdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0]
```

Related Topics

5.16.15 set workmode vdsl

5.16.14 mtu (vdsl)

Function

The **mtu** command sets the maximum transmission unit (MTU) for a VDSL interface.

The **undo mtu** command restores the default MTU.

By default, the MTU of a VDSL interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a VDSL interface.	The value is an integer, in bytes. The value depends on the device.

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than the MTU.

If forcible unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. Therefore, large packets must be forcibly fragmented to prevent packet loss on the network. In this case, you can run the **mtu** command to set the size of a fragment.

Follow-up Procedure

Run the **shutdown** and **undo shutdown** commands to restart the related physical interface to make the configuration take effect.

Precautions

If you run the **mtu** command multiple times in the same VDSL interface view, only the latest configuration takes effect.

Example

Set the MTU of a VDSL interface to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] mtu 1200
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

5.16.15 set workmode vdsl

Function

The **set workmode vdsl** command configures the working mode for a VDSL interface.

By default, a VDSL interface works in PTM mode.

Format

set workmode slot *slot-id* **vdsl** { **atm** | **ptm** }

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID of the VDSL interface.	-
{ **atm** | **ptm** }	Specifies the working mode of the VDSL interface. ● If **atm** is specified, the VDSL interface works in ATM mode. To transmit ATM cells on a VDSL interface, configure the interface to work in ATM mode. ● If **ptm** is specified, the VDSL interface works in PTM mode. To transmit Ethernet frames on a VDSL interface, configure the interface to work in PTM mode.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device aggregates service traffic to a DSLAM by using VDSL interfaces. To enable the device to transmit services on a VDSL line, run the **set workmode vdsl** command to configure the same working mode as the DSLAM for the device.

Follow-up Procedure

- Run the **interface atm** command to enter the interface view if the VDSL interface works in ATM mode.
- Run the **interface ethernet** command to enter the interface view if the VDSL interface works in PTM mode.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After running the **set workmode vdsl** command, you need to restart the card or device (except the AR129CGVW-L and AR169FGW-L) and wait for a period of time to make the configuration take effect.

The AR129CGVW-L and AR169FGW-L support mode switching only when the interfaces are not configured and in the shutdown state.

ni

Example

Set the working mode to PTM for the VDSL interface in slot 1.

```
<Huawei> system-view
[Huawei] set workmode slot 1 vdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

5.16.16 shutdown (vdsl)

Function

The **shutdown** command deactivates a VDSL interface.

The **undo shutdown** command activates a VDSL interface.

By default, a VDSL interface is activated.

Format

shutdown

undo shutdown

Parameters

None

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VDSL interfaces must be activated before transmitting services. Activation of a VDSL interface refers to the training between a DSLAM and a CPE. During the training, the two devices check the line distance and status based on parameters such as the transmission standard, upstream and downstream line rates, and specified noise margin to determine whether they can work properly under the existing conditions. If the training succeeds, the VDSL interface on the CPE is activated and can transmit services between the two devices.

The device functions as a CPE and aggregates services to a DSLAM by using a VDSL interface.

After the device starts, its VDSL interface is automatically activated. The VDSL interface remains activated as long as its VDSL line works properly. To enable the device to communicate with a DSLAM, run the **shutdown** command to deactivate the VDSL interface on the device, set parameters for the interface, and then reactivate this interface to make configurations take effect.

Follow-up Procedure

After a VDSL interface is deactivated, it is disconnected from a DSLAM. To enable the VDSL interface to transmit services, reactivate this VDSL interface.

Example

Activate VDSL interface 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] undo shutdown
```

Related Topics

5.16.12 interface atm (vdsl)

5.16.17 vdsl anti-noise enable

Function

The **vdsl anti-noise enable** command enables enhanced noise resistance on a VDSL interface.

The **undo vdsl anti-noise enable** command disables enhanced noise resistance on a VDSL interface.

By default, enhanced noise resistance is disabled on a VDSL interface.

NOTE

Only the AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169W-P-M9, AR169RW-P-M9, and AR169-P-M9 devices support this configuration.

Format

vdsl anti-noise enable

undo vdsl anti-noise enable

Parameters

None

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device functions as a CPE, enhanced noise resistance is disabled on the VDSL interface by default. High line noise will cause packet loss and line disconnection on the device. To avoid such issues, you can run the **vdsl anti-noise enable** command to enable enhanced noise resistance on the VDSL interface.

Precautions

This command will cause an interface to restart, resulting in data frame loss or service interruption.

After enhanced noise resistance is enabled, the negotiated VDSL link bandwidth may reduce. Therefore, configure this command based on the actual link effect.

Example

Enable enhanced noise resistance on a VDSL interface.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/0
[Huawei-Ethernet0/0/0] vdsl anti-noise enable
Warning: This operation may cause the interface to restart and work in lower bandwidth than befor. Are
you sure to continue? [Y/N]:y
```

5.16.18 vdsl band

Function

The **vdsl band** command enables or disables a specified carrier band on a VDSL interface.

By default, carrier bands are enabled on a VDSL interface.

Format

vdsl band { **a43** | **b43** | **v43** } { **off** | **on** }

Parameters

Parameter	Description	Value
a43	Specifies the a43 carrier band on a VDSL interface.	-
b43	Specifies the b43 carrier band on a VDSL interface.	-
v43	Specifies the v43 carrier band on a VDSL interface.	-

Parameter	Description	Value
off	Disables a specified carrier band on a VDSL interface.	-
on	Enables a specified carrier band on a VDSL interface.	-

Views

VDSL interface view, Ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Carrier bands a43, b43, and v43 on a VDSL interface allow the local device to connect to and negotiate with a digital subscriber line access multiplexer (DSLAM). By default, carrier bands are enabled on the VDSL interface and the local device selects a carrier band through auto-negotiation with the DSLAM. If the DSLAM does not support a carrier band, run the **vdsl band** { **a43** | **b43** | **v43** } **off** command to disable the carrier band.

Prerequisites

- The transmission mode has been set to ATM or PTM using the **set workmode** command on the VDSL interface.
- The VDSL interface has been deactivated using the **shutdown** command.

Precautions

The **vdsl band** command only enables or disables a specified carrier band on a VDSL interface. To make the configuration take effect immediately, run the **undo shutdown** command on the VDSL interface to activate the interface.

Example

Disable the v43 carrier band on the VDSL interface Ethernet0/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet0/0/0
[Huawei-Ethernet0/0/0] shutdown
[Huawei-Ethernet0/0/0] vdsl band v43 off
[Huawei-Ethernet0/0/0] undo shutdown
```

Related Topics

5.16.16 shutdown (vdsl)

5.16.19 vdsl bind

Function

The **vdsl bind** command binds two lines of a VDSL interface in PTM mode.

The **undo vdsl bind** command unbinds two lines of a VDSL interface in PTM mode.

By default, two lines of a VDSL interface in PTM mode are bound.

NOTE

Only the 2VDSL2 interface card, AR169EW, AR169EGW-L, AR169F, AR169FVW, AR169FVW-8S, AR169FGW-L, and AR169FGVW-L support this command.

Format

vdsl bind

undo vdsl bind

Parameters

None

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device is deployed as a CPE, a VDSL interface in PTM mode has two lines (Line0 and Line1). By default, the two lines are bound to increase bandwidth. When the DSLAM requires the CPE to use one line for access, run the **undo vdsl bind** command to unbind the two lines of the VDSL interface in PTM mode.

Prerequisites

1. The VDSL interface has been configured to work in PTM mode using the **set workmode slot** *slot-id* **vdsl ptm** command.
2. The VDSL interface has been deactivated using the **shutdown** command.

Follow-up Procedures

To make the configuration take effect immediately, run the **undo shutdown** command on the VDSL interface to activate the interface.

Example

Unbind two lines of a VDSL interface in PTM mode.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/0
[Huawei-Ethernet0/0/0] undo vdsl bind
```

5.16.20 vdsl downstream-retrans enable

Function

The **vdsl downstream-retrans enable** command enables the downstream retransmission function on a VDSL interface.

The **undo vdsl downstream-retrans enable** command disables the downstream retransmission function on a VDSL interface.

By default, the downstream retransmission function is enabled on a VDSL interface.

NOTE

Only the AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169W-P-M9, AR169RW-P-M9, and AR169-P-M9 devices support this configuration.

Format

vdsl downstream-retrans enable

undo vdsl downstream-retrans enable

Parameters

None

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device functions as a CPE, the downstream retransmission function is enabled on the VDSL interface by default. This enhances link reliability. When the device restarts, it sends a Dying Gasp message to the remote device. If the remote device that does not support the downstream retransmission function receives a Dying Gasp message, you can run the **undo vdsl downstream-retrans enable** command to disable the downstream retransmission function on the VDSL interface. In this case, the remote device can properly respond the Dying Gasp message.

Precautions

This command will cause an interface to restart, resulting in data frame loss or service interruption.

Example

Disable the downstream retransmission function on a VDSL interface.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/0
[Huawei-Ethernet0/0/0] undo vdsl downstream-retrans enable
Warning: This operation may cause the interface to restart. Are you sure to continue? [Y/N]:y
```

5.16.21 vdsl upstream-retrans enable

Function

The **vdsl upstream-retrans enable** command enables the upstream retransmission function on a VDSL interface.

The **undo vdsl upstream-retrans enable** command disables the upstream retransmission function on a VDSL interface.

By default, the upstream retransmission function is enabled on a VDSL interface.

NOTE

Only the AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169W-P-M9, AR169RW-P-M9, and AR169-P-M9 devices support this configuration.

Format

vdsl upstream-retrans enable

undo vdsl upstream-retrans enable

Parameters

None

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device functions as a CPE, the upstream retransmission function is enabled on the VDSL interface by default. This enhances link reliability. When the device restarts, it sends a Dying Gasp message to the remote device. If the remote device that does not support the upstream retransmission function receives a Dying Gasp message, you can run the **undo vdsl upstream-retrans enable**

command to disable the upstream retransmission function on the VDSL interface. In this case, the remote device can properly respond the Dying Gasp message.

Precautions

This command will cause an interface to restart, resulting in data frame loss or service interruption.

Example

Disable the upstream retransmission function on a VDSL interface.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/0
[Huawei-Ethernet0/0/0] undo vdsl upstream-retrans enable
Warning: This operation may cause the interface to restart. Are you sure to continue? [Y/N]:y
```

5.16.22 vdsl standard

Function

The **vdsl standard** command configures a transmission standard for a VDSL interface in PTM mode.

The **undo vdsl standard** command restores the default setting.

By default, a VDSL interface in PTM mode automatically uses the transmission standard of the peer interface.

Format

vdsl standard vdsl2 { **annexa** | **annexb** }

undo vdsl standard

Parameters

Parameter	Description	Value
vdsl2	Configures VDSL2 (G993.2) for a VDSL interface in PTM mode. VDSL2 provides a maximum of 50 Mbit/s upstream transmission rate and 100 Mbit/s downstream transmission rate.	-
annexa	Supports VDSL2 and is compatible with POTS services.	-
annexb	Supports VDSL2 and is compatible with ISDN services.	-

Views

VDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to transmit services on a VDSL line, run the **vdsl standard** command to configure the device to use the same transmission standard as a DSLAM.

Precautions

AR109, AR109W, AR109GW-L, AR129, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR129W, AR169, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, and AR169RW-P-M9 do not support T1.413.AR169EW, AR169EGW-L, AR169F, AR169BF, AR169FVW, AR169FVW-8S, AR169FGW-L, AR169JFVW-4B4S, AR169JFVW-2S, and AR169FGVW-L only support AnnexA and AnnexM. AR169BF only supports AnnexB and AnnexJ.

Prerequisites

The VDSL interface has been deactivated using the **shutdown** command.

Follow-up Procedure

To make the transmission standard configured for a VDSL interface take effect, run the **undo shutdown** command on the interface to activate the interface.

Example

Configure AnnexA for VDSL interface Eth0/0/0.

```
<Huawei> system-view
[Huawei] set workmode slot 0 vdsl ptm
Warning: All the configuration will be saved to the next startup configuration.
Continue? [y/n]: y
  It will take several minutes to save configuration file, please wait.........
...
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
Warning: Changing the working mode will reset the board in slot 0. Continue? [y/
n]:y
INFO: Resetting board[0] succeeded.
[Huawei] interface ethernet 0/0/0
[Huawei-Ethernet0/0/0] shutdown
[Huawei-Ethernet0/0/0] vdsl standard vdsl2 annexa
[Huawei-Ethernet0/0/0] undo shutdown
```

Related Topics

5.16.13 interface ethernet (vdsl)

5.16.16 shutdown (vdsl)

5.17 G.SHDSL Interface Configuration Commands

5.17.1 display dsl all interface

Function

The **display dsl all interface** command displays status information about all xDSL interfaces.

Format

display dsl all interface

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dsl all interface** command to check the negotiation status with xDSL interfaces at the central office, transmission standard, line status, performance statistics, bit exchange status, seamless rate adaptation status, trellis coding status, and card version of the ADSL interface and VDSL interface (in ATM or PTM mode), and check the link status, vendor, and performance statistics of the G.SHDSL interface.

Precautions

This command cannot display information about xDSL sub-interfaces.

Example

Display status information about all xDSL interfaces.

```
<Huawei> display dsl all interface
 Atm1/0/0 information:
 ------------------------------------------------------------
 DSL driver and PHY status
     Line0:
     Training status                    : Showtime
     Transmission mode                      : VDSL2
     VDSL2 profile                      : Profile 17a
     Line status                       : No Defect
     Downstream max. attainable rate(Kbps): 142372
     Upstream max. attainable rate(Kbps)  : 63853
```

```
    Downstream actual net data rate(Kbps): 60016
    Upstream actual net data rate(Kbps)  : 20013
    Downstream SNR margin(dB)            : 28.8
    Upstream SNR margin(dB)              : 31.9
    Downstream attenuation(dB)           : 0.0
    Upstream attenuation(dB)             : 0.0
    Downstream output power(dBm)         : 14.5
    Upstream output power(dBm)           : -6.4
    Downstream total cells               : 1348781845
    Upstream total cells                 : 0
    Downstream data cells                : 0
    Upstream data cells                  : 0
    Downstream bit errors                : 0
    Upstream bit errors                  : 0
    Total drop cells                     : 0
    Downstream total ES count            : 60
    Upstream total ES count              : 0
    Downstream total SES count           : 59
    Upstream total SES count             : 0
    Downstream total UAS count           : 849
    Upstream total UAS count             : 849
    Total AS count                       : 86128

    Line1:
    Training status                      : Showtime
    Transmission mode                    : VDSL2
    VDSL2 profile                        : Profile 17a
    Line status                          : No Defect
    Downstream max. attainable rate(Kbps): 145984
    Upstream max. attainable rate(Kbps)  : 64009
    Downstream actual net data rate(Kbps): 60016
    Upstream actual net data rate(Kbps)  : 20013
    Downstream SNR margin(dB)            : 28.0
    Upstream SNR margin(dB)              : 32.4
    Downstream attenuation(dB)           : 0.0
    Upstream attenuation(dB)             : 0.0
    Downstream output power(dBm)         : 13.1
    Upstream output power(dBm)           : -6.5
    Downstream total cells               : 1360438742
    Upstream total cells                 : 0
    Downstream data cells                : 0
    Upstream data cells                  : 0
    Downstream bit errors                : 0
    Upstream bit errors                  : 0
    Total drop cells                     : 0
    Downstream total ES count            : 59
    Upstream total ES count              : 0
    Downstream total SES count           : 56
    Upstream total SES count             : 0
    Downstream total UAS count           : 683
    Upstream total UAS count             : 683
    Total AS count                       : 86230

Line capability
    Bitswap                              : On
    SRA                                  : Off
    Trellis coding                       : On

Board version
    vendor ID                            : 0xB5 0 "BDCM" 0 0
    vendor serial                        : 10000000000000000000000000000000
    Board ID                             : 963168MBV_17A
    Software version                     : 4.12L.08
    Bootloader (CFE) version             : 1.0.38-112.118
    DSL PHY and driver version           : A2pvbF038j.d24h
    Build timestamp                      : 20170706_1814

ATU-C version
    vendor ID                            : BDCM:0x938f
```

```
    vendor number                    : 0x938f
-------------------------------------------------------------
Atm2/0/1 information:
-------------------------------------------------------------------
 Operating mode                          :CPE
 Port admin status                       :Active
 Port running status                     :Activated
 Port admin bind status                  :EFM-2
 Bind group master port                  :0
 Bind group running port                 :1;
 LOSWS Defect alarm                      :none
 SNR Margin alarm                        :none
 Loop Attenuation alarm                  :none
 Modem status                            :DOWN_READY
 Condition                               :NO_COND_
 Reason                                  :ERR_UNUSED_
 Port transmission mode                  :G.991.2 Annex A&B&F&G
 Port power spectral density             :Symmetric
 Port line probe                         :Enable
 Inventory of SHDSL port 0
 Vendor ID                               :Infineon
 Vendor mode                             :SOCRATES
 Vendor serial                           :4e_2e_1e
 EOC version                             :0
 Standard version                        :8
 Vendor list                             :-
 Vendor issue                            :1
 Software code                           :1.7.2
 Equipment code                          :-
 Information of other vendor             :V200R008
 Transmission mode capability            :G.991.2 Annex A&B&F&G
-------------------------------------------------------------
```

Table 5-59 Description of the **display dsl all interface** command output

Item	Description
Atm1/0/0 information	Information about ATM1/0/0. ATM1/0/0 in this example is a VDSL interface. For detailed command output descriptions, see **display dsl interface atm (vdsl)** and **display dsl interface ethernet (vdsl)**. For detailed command output description of an ADSL interface, see **display dsl interface atm (adsl)**.
Atm2/0/1 information	Information about ATM2/0/1. ATM2/0/1 in this example is a G.SHDSL interface. For detailed command output description, see **display dsl interface (g.shdsl)**.

5.17.2 display dsl interface (g.shdsl)

Function

The **display dsl interface** command displays information about a G.SHDSL interface.

Format

display dsl interface { **atm** | **ethernet** } *interface-number*

Parameters

Parameter	Description	Value
atm	Displays information about a G.SHDSL interface working in ATM transmission mode.	-
ethernet	Displays information about a G.SHDSL interface working in PTM transmission mode.	-
interface-number	Specifies the number of a G.SHDSL interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dsl interface** command displays information about a G.SHDSL interface, including the link layer status, vendor information, and performance statistics.

NOTE

The fields displayed in the command output are the same for G.SHDSL interfaces working in ATM or PTM transmission mode.

Example

Display information about G.SHDSL interface 1/0/0 working in ATM transmission mode.

```
<Huawei> display dsl interface atm 1/0/0
-------------------------------------------------------------------
  Operating mode                          :CPE
  Port admin status                       :Active
  Port running status                     :Activated
  Port admin bind status                  :MPair-2
  Bind group master port                  :0
  LOSWS Defect alarm                      :none
  SNR Margin alarm                        :none
  Loop Attenuation alarm                  :none
  Modem status                            :UP_DATA_MODE
  Condition                               :GHS_TRANSFER_
  Reason                                  :ERR_UNUSED_
  Port transmission mode                  :G.991.2 Annex A&B&F&G
  Port power spectral density             :Symmetric
  Port line probe                         :Enable
```

```
 Line Status of SHDSL port 0
 Current line rate(unit:kbps)                    :5704
 Current transmission mode                       :G.991.2 Annex G
 Actual attainable payload line rate(unit:kbps)  :11392
 Current modulation mode                         :TCPAM-32
 Current PBO downstream(unit:dB)                 :6.0
 Current PBO upstream(unit:dB)                   :0.0
 Current loop attenuation downstream(unit:dB)    :0
 Current loop attenuation upstream(unit:dB)      :0
 Current SNR margin downstream(unit:dB)          :19
 Current SNR margin upstream(unit:dB)            :0
 Inventory of SHDSL port 0
 Vendor ID                                       :Infineon
 Vendor mode                                     :SOCRATES
 Vendor serial                                   :4e_2e_1e
 EOC version                                     :0
 Standard version                                :8
 Vendor list                                     :-
 Vendor issue                                    :1
 Software code                                   :1.6.3
 Equipment code                                  :-
 Information of other vendor                     :B01D01
 Transmission mode capability                    :G.991.2 Annex A&B&F&G
 Current 15 minute statistics (Time elapsed 260 seconds)
  ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
 Previous 15 minute statistics
  ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
 Current 24 hr statistics
  ES:0, SES:0, CRC:0, LOSWS:0, UAS:0
 Previous 24 hr statistics
  ES:0, SES:0, CRC:0, LOSWS:0, UAS:1
-------------------------------------------------------------------------
```

Display information about G.SHDSL interface 1/0/0 working in PTM transmission mode.

```
<Huawei> display dsl interface ethernet 1/0/0
-------------------------------------------------------------------------
 Operating mode                                  :CPE
 Port admin status                               :Active
 Port running status                             :Activated
 Port admin bind status                          :EFM-2
 Bind group master port                          :0
 Bind group running port                         :1;
 LOSWS Defect alarm                              :none
 SNR Margin alarm                                :none
 Loop Attenuation alarm                          :none
 Modem status                                    :DOWN_READY
 Condition                                       :NO_COND_
 Reason                                          :ERR_UNUSED_
 Port transmission mode                          :G.991.2 Annex A&B&F&G
 Port power spectral density                     :Symmetric
 Port line probe                                 :Enable
 Inventory of SHDSL port 0
 Vendor ID                                       :Infineon
 Vendor mode                                     :SOCRATES
 Vendor serial                                   :4e_2e_1e
 EOC version                                     :0
 Standard version                                :8
 Vendor list                                     :-
 Vendor issue                                    :1
 Software code                                   :1.7.2
 Equipment code                                  :-
 Information of other vendor                     :V200R008
 Transmission mode capability                    :G.991.2 Annex A&B&F&G
-------------------------------------------------------------------------
```

Table 5-60 Description of the display dsl interface atm 1/0/0 command output

Item	Description
Operating mode	Working mode of the G.SHDSL interface: ● CO: Central Office. ● CPE: Customer Premises Equipment.
Port admin status	Administrative status of the G.SHDSL interface: ● Active: indicates that the interface is activated. ● Deactive: indicates that the interface is deactivated.
Port running status	Running status of the G.SHDSL interface: ● Activated: indicates that the interface has been activated. ● Activating: indicates that the interface is being activated. ● Deactivated: indicates that the interface has been deactivated. ● Deactivating: indicates that the interface is being deactivated.
Port admin bind status	Interface binding mode: ● Normal: indicates that the G.SHDSL interface is not bound to any other interface. ● MPair-X: indicates M-Pair binding. X specifies the number of bound interfaces. ● EFM-X: indicates EFM binding. X specifies the number of bound interfaces. To configure the interface binding mode, run the **shdsl bind** { **efm** | **m-pair** } *link-number* command.
Bind group master port	Number of the main interface. This field is displayed only when M-Pair binding or EFM binding is configured.
Bind group running port	Number of the slave interface activated in the bind group. This field is displayed only when a main interface configured with EFM binding is configured.

Item	Description
LOSWS Defect alarm	Loss of signal (LOS) alarm.
SNR Margin alarm	SNR margin alarm.
Loop Attenuation alarm	Loop attenuation alarm.
Modem status	Link modulation status. • DOWN_NOT_READY • DOWN_READY • STOP_DOWN_READY • INITIALIZING • UP_DATA_MODE
Condition	Condition for the modulation status.
Reason	Reason for the modulation status.
Port transmission mode	Transmission standard: • G.991.2 Annex A&B • G.991.2 Annex A • G.991.2 Annex B To configure the transmission standard, run the **shdsl annex** { **a** | **all** | **b** } command.
Port power spectral density	Power spectral density (PSD) mode: • Asymmetric: indicates asymmetric PSD. • Symmetric: indicates symmetric PSD. To configure the PSD mode, run the **shdsl psd** { **asymmetry** | **symmetry** } command.
Port line probe	Line probing status: • Enable: indicates that the line probing function is enabled. • Disable: indicates that the line probing function is disabled. To configure the line probing function, run the **shdsl line-probing** { **disable** | **enable** } command.
Current line rate(unit:kbps)	Actual line rate, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current transmission mode	Current transmission mode. The device displays the actual transmission mode negotiated by the two ends based on the output of the **shdsl capability** { **auto** | **g-shdsl** | **g-shdsl.bis** } command. ● If **g-shdsl** is specified, the device displays **Annex A** or **Annex B**. ● If **g-shdsl.bis** is specified, the device displays **Annex F** or **Annex G**. ● If **auto** is specified, the device displays the transmission mode obtained from the CO side when functioning as a CPE and displays **Annex F** or **Annex G** (the same as the g-shdsl.bis mode) when functioning as a CO.
Actual attainable payload line rate(unit:kbps)	Actual line payload rate, in kbit/s.
Current modulation mode	Current modulation mode: ● TCPAM-16 ● TCPAM-32
Current PBO downstream(unit:dB)	Current downstream power back-off, in dB.
Current PBO upstream(unit:dB)	Current upstream power back-off, in dB.
Current loop attenuation downstream(unit:dB)	Current downstream loop attenuation, in dB.
Current loop attenuation upstream(unit:dB)	Current upstream loop attenuation, in dB.
Current SNR margin downstream(unit:dB)	Current downstream SNR margin, in dB.
Current SNR margin upstream(unit:dB)	Current upstream SNR margin, in dB.
Vendor ID	ID of a vendor.
Vendor mode	Model of the vendor equipment.
Vendor serial	Serial number of the vendor equipment.
EOC version	Embedded operations channel (EOC) software version.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Standard version	G.SHDSL standard version.
Vendor list	If the system displays "-", there is no vendor list.
Vendor issue	Vendor software issue.
Software code	Vendor software version.
Equipment code	Vendor equipment code.
Information of other vendor	Information about other vendors.
Transmission mode capability	Supported transmission standard.
Current 15 minute statistics	Statistics in the current 15 minutes.
Time elapsed 260 seconds	Total number of seconds in which errors are detected within 15 minutes.
ES	Number of errored seconds recorded within 15 minutes. An errored second is a second in which at least one CRC error occurs or at least one Loss of Sync Word (LOSW) is set to 1.
SES	Number of severely errored seconds recorded within 15 minutes. A severely errored second is a second in which at least 50 CRC errors occur or at least one LOSW is set to 1.
CRC	Number of CRC errors detected within 15 minutes.
LOSWS	Number of LOSW seconds recorded within 15 minutes.
UAS	Number of seconds in which a G.SHDSL line remains unavailable within 15 minutes. If 10 consecutive severely errored seconds are detected on a G.SHDSL line, the G.SHDSL line becomes unavailable.
Previous 15 minute statistics	Statistics in the previous 15 minutes.
Current 24 hr statistics	Statistics in the current 24 hours.
Previous 24 hr statistics	Statistics in the previous 24 hours.

Related Topics

5.17.5 interface atm (g.shdsl)
5.17.6 interface ethernet (g.shdsl)

5.17.3 display interface atm (g.shdsl)

Function

The **display interface atm** command displays the configuration and status of a G.SHDSL interface working in ATM transmission mode.

Format

display interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a G.SHDSL interface working in ATM transmission mode.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When monitoring the interface status or locating faults on a G.SHDSL interface, run the **display interface atm** command on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Prerequisites

The G.SHDSL interface is working in ATM transmission mode.

Example

Display the configuration and status of G.SHDSL interface 1/0/0 working in ATM transmission mode.

```
<Huawei> display interface atm 1/0/0
Atm1/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-12-31 17:46:13
Description:HUAWEI, AR Series, Atm1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.1/24
AAL enabled: AAL5, Maximum PVCs: 8
PVCs on main-interface: 8 (Total PVCs: 8)
Last physical up time   : 2012-12-31 17:46:13
```

```
Last physical down time : 2012-12-31 17:43:48
Current system time: 2013-01-06 14:06:38

Port PHY type : G.SHDSL
Total seconds counted in 15 minutes            :400
ES count in 15 minutes (unit:Second)           :0
SES count in 15 minutes (unit:Second)          :0
CRC anomaly count in 15 minutes                :0
LOSW count in 15 minutes (unit:Second)         :0
UAS count in 15 minutes (unit:Second)          :0

Last 300 seconds input rate 1059904 bits/sec, 1232 packets/sec
Last 300 seconds output rate 1016080 bits/sec, 1221 packets/sec

Input:  622961422 packets, 66968337586 bytes
        0 error, 0 discard, 0 crc
Output:  617299079 packets, 64198983080 bytes
        0 error, 0 discard
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
```

Table 5-61 Description of the display interface atm command output

Item	Description
Atm1/0/0 current state	Physical status of ATM1/0/0: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the network administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Last line protocol up time	Last time the link layer protocol of the interface goes Up.
Description	Interface description.
The Maximum Transmit Unit is	Maximum transmit unit (MTU) of the interface. By default, the MTU is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded.
Internet Address is	IP address of the interface. If no IP address is assigned to the interface, the system displays "Internet protocol processing : disabled".
AAL enabled	ATM Adaptation Layer (AAL).

Item	Description
Maximum PVCs	Maximum number of virtual circuits (PVCs).
PVCs on main-interface: (Total PVCs:)	Number of PVCs on the main interface (total number of PVCs on both the main interface and sub-interfaces).
Last physical up time	Last time the interface went Up physically. If the system displays "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last physical down time	Last time the interface went Down physically. If the system displays "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Port PHY type	Physical port type.
Total seconds counted in 15 minutes	Total number of seconds in which errors are detected within 15 minutes.
ES count in 15 minutes (unit:Second)	Number of errored seconds recorded within 15 minutes. An errored second is a second in which at least one CRC error occurs or at least one LOSW is set to 1.
SES count in 15 minutes (unit:Second)	Number of severely errored seconds recorded within 15 minutes. A severely errored second is a second in which at least 50 CRC errors occur or at least one LOSW is set to 1.
CRC anomaly count in 15 minutes	Number of CRC errors detected within 15 minutes.
LOSW count in 15 minutes (unit:Second)	Number of LOSW seconds recorded within 15 minutes.
UAS count in 15 minutes (unit:Second)	Number of seconds in which a G.SHDSL line remains unavailable within 15 minutes. If 10 consecutive severely errored seconds are detected on a G.SHDSL line, the G.SHDSL line becomes unavailable.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last 300 seconds input rate	Incoming packet rate (bit/s and pps) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bit/s and pps) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization	Percentage of the incoming packet rate to the total bandwidth.
Output bandwidth utilization	Percentage of the outgoing packet rate to the total bandwidth.

Related Topics

5.17.5 interface atm (g.shdsl)

5.17.4 display interface ethernet (g.shdsl)

Function

The **display interface ethernet** command displays the configuration and status of a G.SHDSL interface working in PTM transmission mode.

Format

display interface ethernet *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a G.SHDSL interface working in PTM transmission mode.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When monitoring the interface status or locating faults on a G.SHDSL interface, run the **display interface ethernet** command on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Prerequisites

The G.SHDSL interface is working in PTM transmission mode.

Example

Display the configuration and status of G.SHDSL interface 1/0/0 working in PTM transmission mode.

```
<Huawei> display interface ethernet 1/0/0
Ethernet1/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Ethernet1/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : 10.1.1.2/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc01-0003
Last physical up time   : 2010-06-21 14:56:32
Last physical down time : 2010-06-21 14:56:31
Current system time: 2010-06-29 20:26:18

  Port PHY type : G.SHDSL
  Total seconds counted in 15 minutes            :286
  ES count in 15 minutes (unit:Second)           :0
  SES count in 15 minutes (unit:Second)          :0
  CRC anomaly count in 15 minutes                :0
  LOSW count in 15 minutes (unit:Second)         :0
  UAS count in 15 minutes (unit:Second)          :286

  Last 300 seconds input rate 24 bits/sec, 0 packets/sec
  Last 300 seconds output rate 24 bits/sec, 0 packets/sec

  Input:  13 packets, 1160 bytes
          0 error, 0 discard,
  Output:  10 packets, 980 bytes
          0 error, 0 discard

    Input bandwidth utilization  : 0.01%
    Output bandwidth utilization : 0.01%
```

Table 5-62 Description of the display interface ethernet command output

Item	Description
Ethernet1/0/0 current state	Physical status of Ethernet1/0/0: ● UP: indicates that the interface is physically Up. ● DOWN: indicates that the interface is physically Down. ● Administratively down: indicates that the network administrator has run the **shutdown** command on the interface.

Item	Description
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Description	Interface description.
Internet protocol processing : disabled	No IP address is assigned to the interface. If an IP address is assigned to the interface, the IP address and subnet mask are displayed.
IP Sending Frames' Format is	Format of the frame contained in the sent IP packet.
Last physical up time	Last time the interface went Up physically. If the system displays "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last physical down time	Last time the interface went Down physically. If the system displays "-", the physical status of the interface does not change. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Port PHY type	Physical port type.
Total seconds counted in 15 minutes	Total number of seconds in which errors are detected within 15 minutes.
ES count in 15 minutes (unit:Second)	Number of errored seconds recorded within 15 minutes. An errored second is a second in which at least one CRC error occurs or at least one LOSW is set to 1.
SES count in 15 minutes (unit:Second)	Number of severely errored seconds recorded within 15 minutes. A severely errored second is a second in which at least 50 CRC errors occur or at least one LOSW is set to 1.
CRC anomaly count in 15 minutes	Number of CRC errors detected within 15 minutes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
LOSW count in 15 minutes (unit:Second)	Number of LOSW seconds recorded within 15 minutes.
UAS count in 15 minutes (unit:Second)	Number of seconds in which a G.SHDSL line remains unavailable within 15 minutes. If 10 consecutive severely errored seconds are detected on a G.SHDSL line, the G.SHDSL line becomes unavailable.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

Related Topics

5.17.6 interface ethernet (g.shdsl)

5.17.5 interface atm (g.shdsl)

Function

The **interface atm** command displays the view of a G.SHDSL interface working in ATM transmission mode.

Format

interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a G.SHDSL interface working in ATM transmission mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **interface atm** command displays the view of a G.SHDSL interface working in ATM transmission mode.

Prerequisites

The G.SHDSL interface has been configured to work in ATM mode by using the **set workmode (shdsl)** command.

Example

Enter the view of G.SHDSL interface 1/0/0 working in ATM transmission mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0]
```

Related Topics

5.17.8 set workmode shdsl

5.17.6 interface ethernet (g.shdsl)

Function

The **interface ethernet** command displays the view of a G.SHDSL interface working in PTM transmission mode.

Format

interface ethernet *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a G.SHDSL interface working in PTM transmission mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **interface ethernet** command displays the view of a G.SHDSL interface working in PTM transmission mode.

Prerequisites

The G.SHDSL interface has been configured to work in PTM mode by using the **set workmode (shdsl)** command.

Example

Enter the view of G.SHDSL interface 1/0/0 working in PTM transmission mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0]
```

Related Topics

5.17.8 set workmode shdsl

5.17.7 mtu (g.shdsl)

Function

The **mtu** command sets the maximum transmission unit (MTU) for a G.SHDSL interface.

The **undo mtu** command restores the default MTU.

By default, the MTU of a G.SHDSL interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a G.SHDSL interface.	The value is an integer, in bytes. If G.SHDSL interfaces work in ATM transmission mode, the value range is as follows: ● AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2220E and AR2204: 128 to 1606. ● AR2220, AR2240, AR2240C, AR3260, and AR3670: 128 to 1978. If G.SHDSL interfaces work in PTM transmission mode, the value is ranging from 46 to 1572.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than the MTU.

If forcible unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. Therefore, large packets must be forcibly fragmented to prevent packet loss on the network. In this case, you can run the **mtu** command to set the size of a fragment.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Run the **shutdown** and **undo shutdown** commands to restart the related physical interface to make the configuration take effect.

Precautions

If you run the **mtu** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

Example

Set the MTU of a G.SHDSL interface to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] mtu 1200
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] undo shutdown
```

5.17.8 set workmode shdsl

Function

The **set workmode shdsl** command sets the transmission mode for a G.SHDSL interface.

By default, G.SHDSL interfaces work in ATM mode.

Format

set workmode slot *slot-id* **shdsl** { **atm** | **ptm** }

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a G.SHDSL interface.	-
atm	Indicates a G.SHDSL interface works in ATM transmission mode. To transmit ATM cells on a G.SHDSL interface, configure the interface to work in ATM transmission mode.	-
ptm	Indicates a G.SHDSL interface works in PTM transmission mode. To transmit Ethernet frames on a G.SHDSL interface, configure the interface to work in PTM transmission mode.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device aggregates service traffic to a DSLAM by using G.SHDSL interfaces. To enable the device to transmit services on a G.SHDSL line, run the **set workmode shdsl** command to configure the same transmission mode as the DSLAM for the device.

Prerequisites

All G.SHDSL interfaces have been deactivated and unbound from each other.

Follow-up Procedure

- Run the **interface atm** command to enter the interface view if the G.SHDSL interface works in ATM mode.
- Run the **interface ethernet** command to enter the interface view if the G.SHDSL interface works in PTM mode.

Precautions

- The SRU of AR158E, AR158EVW, AR168F, AR168F-4P and AR208E has only one WAN physical interface. After the transmission mode is set for the G.SHDSL interface card, four G.SHDSL interfaces all work in the configured mode. The AR168F and AR168F-4P interfaces are numbered from 0 to 3. In ATM mode, the AR158E, AR158EVW and AR208E interfaces are numbered from 0 to 3; in PTM mode, the AR158E and AR158EVW interfaces are numbered from 4 to 7, and AR208E interfaces are numbered from 8 to 11.
- Each 4G.SHDSL board on the AR1200, AR2204, AR2204-51GE-P, AR2204-51GE-R, AR2204-27GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204E, AR2204E-D, AR2220E, AR2220, AR2240, AR2240C, AR3200, and AR3600 has only one physical interface. This physical interface can be virtualized into four G.SHDSL upstream interfaces numbered from 0 to 3. After the transmission mode is set for the G.SHDSL interface card, four G.SHDSL interfaces all work in the configured mode.

Example

Set the transmission mode to PTM for the G.SHDSL interface in slot 1.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
```

5.17.9 shdsl annex

Function

The **shdsl annex** command configures a transmission standard for a G.SHDSL interface.

By default, a G.SHDSL interface supports G.991.2 Annex A, G.991.2 Annex F, and G.991.2 Annex B, and G.991.2 Annex G.

Format

shdsl annex { **a** | **all** | **b** }

Parameters

Parameter	Description	Value
a	Configures a G.SHDSL interface to support G.991.2 Annex A and G.991.2 Annex F. If **a** is specified: ● When payload rate on G.SHDSL interface channels is smaller than 2304 kbit/s, the router applies the G.991.2 Annex A standard on the interface. ● When payload rate on G.SHDSL interface channels between 2304 kbit/s and 5696 kbit/s, the router applies the G.991.2 Annex F standard on the interface.	-
all	Configures a G.SHDSL interface to support G.991.2 Annex A, G.991.2 Annex F, and G.991.2 Annex B, and G.991.2 Annex G. G.SHDSL interfaces on both ends negotiate the transmission standard.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
b	Configures a G.SHDSL interface to support G.991.2 Annex B and G.991.2 Annex G. If **b** is specified: ● When payload rate on G.SHDSL interface channels is smaller than 2304 kbit/s, the router applies the G.991.2 Annex B standard on the interface. ● When payload rate on G.SHDSL interface channels between 2304 kbit/s and 5696 kbit/s, the router applies the G.991.2 Annex G standard on the interface.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the router works as customer premises equipment (CPE), it can adapt the transmission standard according to the standard used on the central office (CO). For example, if the CO uses the G.991.2 Annex B standard while the CPE uses another standard, the CPE automatically changes the standard to G.991.2 Annex B. To enable services to be transmitted on an SHDSL line, run the **shdsl annex** command to specify the same transmission standard as that used on the CO. The default configuration is recommended.

Prerequisites

The G.SHDSL interface has been deactivated using the **shutdown** command.

Precautions

The transmission standard can be configured on G.SHDSL interfaces working in ATM or PTM transmission mode. If the transmission mode is set to ATM and the

interface binding mode is set to M-Pair binding, the transmission standard must be configured on the main interface.

Example

Set the transmission standard of G.SHDSL interface 1/0/0 working in PTM transmission mode to G.991.2 Annex A.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0] shutdown
[Huawei-Ethernet1/0/0] shdsl annex a
```

Related Topics

5.17.8 set workmode shdsl

5.17.10 shdsl bind

Function

The **shdsl bind** command binds a G.SHDSL interface.

The **undo shdsl bind** command unbinds a G.SHDSL interface.

By default, G.SHDSL interfaces are not bound together.

Format

shdsl bind { **efm** *link-number* | **m-pair** { *link-number* | **auto** } }

undo shdsl bind

Parameters

Parameter	Description	Value
efm	Sets the interface binding mode to EFM binding. When G.SHDSL interfaces work in PTM mode, they can be bound in EFM mode. In EFM binding mode, a maximum of four interfaces can be bound together. The rate after interface binding equals the sum of rates of all the bound interfaces.	-

Parameter	Description	Value
m-pair	Sets the interface binding mode to M-Pair binding. When G.SHDSL interfaces work in ATM mode, they can be bound in M-Pair mode. In M-Pair binding mode, two G.SHDSL interfaces, three G.SHDSL interfaces, or four G.SHDSL interfaces can be bound together to provide twice, three times, or four times the rate of a single G.SHDSL interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
link-number	Specifies the number of interfaces to be bound.	The value can be 2, 3, or 4. **NOTE** ● The SRU of AR158E, AR158EVW, AR168F, AR168F-4P and AR208E has only one WAN physical interface. After the transmission mode is set for the G.SHDSL interface card, four G.SHDSL interfaces all work in the configured mode. The AR168F and AR168F-4P interfaces are numbered from 0 to 3. In ATM mode, the AR158E, AR158EVW and AR208E interfaces are numbered from 0 to 3; in PTM mode, the AR158E and AR158EVW interfaces are numbered from 4 to 7, and AR208E interfaces are numbered from 8 to 11. ● Each 4G.SHDSL board on the AR1200, AR2204, AR2204-51GE-P, AR2204-51GE-R, AR2204-27GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204E, AR2204E-D, AR2220E, AR2220, AR2240, AR2240C, AR3200, and AR3600 has only one physical interface. This physical interface can be virtualized into four G.SHDSL upstream interfaces numbered from 0 to 3. After the transmission mode is set for the G.SHDSL interface card, four G.SHDSL interfaces all work in the configured mode. ● If the value is 2, two interfaces (Port 0 and Port 1, or Port 2 and Port 3) can be bound together.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		● If the value is 3, three interfaces (Port 0, Port 1, and Port 2) can be bound together. ● If the value is 4, four interfaces (Port 0, Port 1, Port 2, and Port 3) can be bound together.
auto	Indicates the automatic binding mode. After this parameter is specified, the local device automatically adjusts its binding mode to be the same as the binding mode of the peer device through negotiation. **NOTE** ● This parameter is configured only when the device functions as a CPE and the transmission mode is ATM.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To increase link bandwidth, run the **shdsl bind** command to bind G.SHDSL interfaces.

Prerequisites

- Only contiguous interfaces on the same 4G.SHDSL board can be bound together. The number of the first interface to be bound must be 0 or 2, and the first bound interface is the main interface, and the remaining bound interfaces are slave interfaces.
- Before binding interfaces, ensure that these interfaces have been deactivated and that slave interfaces are not configured with any service.

- You can run the **shdsl bind m-pair auto** command only when the G.SHDSL interface works in CPE mode and the transmission mode is ATM.

Precautions

- After G.SHDSL interfaces are bound together in M-Pair mode, the transmission standard, PSD mode, and line probing status of these interfaces are restored to the default settings. To activate all the bound interfaces or set parameters for these interfaces, you just need to activate the main interface or set parameters for the main interface. Other bound interfaces inherit the configurations from the main interface. For example, if the main interface is activated, other interfaces in the same binding group are also activated.
- After G.SHDSL interfaces are bound together in EFM mode, you can set different parameters for these interfaces. For example, you can set different transmission standards for these interfaces.

  NOTE

  To activate G.SHDSL interfaces bound in EFM mode, activate the main and slave interfaces in sequence.
- When G.SHDSL interfaces are bound together in EFM mode, these G.SHDSL interfaces cannot be bound to other interfaces. For example, when G.SHDSL interfaces 1/0/0 and 1/0/1 are bound in EFM mode, G.SHDSL interface 1/0/2 cannot be bound to G.SHDSL interface 1/0/0 or 1/0/1.

Example

Bind G.SHDSL interfaces 1/0/0, 1/0/1, and 1/0/2 working in PTM transmission mode in EFM mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0] shutdown
[Huawei-Ethernet1/0/0] quit
[Huawei] interface ethernet 1/0/1
[Huawei-Ethernet1/0/1] shutdown
[Huawei-Ethernet1/0/1] quit
[Huawei] interface ethernet 1/0/2
[Huawei-Ethernet1/0/2] shutdown
[Huawei-Ethernet1/0/2] quit
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0] shdsl bind efm 3
```

Related Topics

5.17.8 set workmode shdsl
5.17.27 shutdown (g.shdsl)

5.17.11 shdsl bind m-pair 2 pairs

Function

The **shdsl bind m-pair 2 pairs** command configures a binding mode for a G.SHDSL interface.

The **undo shdsl bind** command unbinds a G.SHDSL interface.

By default, the auto-enhanced binding mode is used.

Format

shdsl bind m-pair 2 [**pairs** { **auto-enhanced** | **enhanced** | **standard** }]

undo shdsl bind

Parameters

Parameter	Description	Value
auto-enhanced	Indicates the auto-enhanced mode.	-
enhanced	Indicates the enhanced mode.	-
standard	Indicates the standard mode.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to connect to the peer device, run the **shdsl bind m-pair 2 pairs** command to configure a binding mode based on the chip type of the peer device.

Prerequisites

- The G.SHDSL interface has been configured to work in ATM transmission mode.
- Only contiguous interfaces on the same 4G.SHDSL board can be bound together. The number of the first interface to be bound must be 0 or 2, and the first bound interface is the main interface, and the remaining bound interfaces are slave interfaces.
- Before binding interfaces, ensure that these interfaces have been deactivated and that slave interfaces are not configured with any service.

Precautions

- When the g-shdsl mode is configured, G.SHDSL interface supports only the enhanced mode.
- When the g-shdsl.bisl mode is configured, G.SHDSL interface supports auto-enhanced, standard, and enhanced modes. By default, when the g-shdsl.bisl mode is configured, G.SHDSL interface uses the auto-enhanced mode.

 Copyright © Huawei Technologies Co., Ltd.

- This command can only be executed on interface 0 or 2.

Example

Set the binding mode to enhanced.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl bind m-pair 2 pairs enhanced
[Huawei] interface atm 1/0/1
[Huawei-Atm1/0/1] shutdown
[Huawei-Atm1/0/1] quit
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.12 shdsl capability

Function

The **shdsl capability** command configures the capability for the G.SHDSL interface card.

The **undo shdsl capability** command restores the default setting.

By default, the G.SHDSL interface card uses the auto mode.

Format

shdsl capability { **auto** | **g-shdsl** | **g-shdsl.bis** }

undo shdsl capability

Parameters

Parameter	Description	Value
auto	Indicates the auto mode.	-
g-shdsl	Indicates the g-shdsl mode.	-
g-shdsl.bis	Indicates the g-shdsl.bis mode.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to connect to the peer device, run the **shdsl capability** command to configure the capability for the G.SHDSL interface card based on the chip type of the peer device. When the peer device uses the g-shdsl mode, you must configure the g-shdsl mode on the device.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Precautions

If you run the **shdsl capability** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

Example

Configure the capability in g-shdsl mode for the G.SHDSL interface card working in ATM transmission mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl capability g-shdsl
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.13 shdsl compatibility

Function

The **shdsl compatibility** command sets the compatibility mode for a G.SHDSL interface.

The **undo shdsl compatibility** command restores the default setting.

By default, a G.SHDSL interface uses the **normal** compatibility mode.

Format

shdsl compatibility pmms { **normal** | **long** } **vendor** { **normal** | **gs** [**enhanced**] } **filter** { **normal** | **specific** }

undo shdsl compatibility

Parameters

Parameter	Description	Value
pmms { **normal** | **long** }	Specifies the probe mode of the G.SHDSL interface. ● **normal** indicates the standard probe mode. ● **long** indicates the probe mode that is compatible with the receiver equipped with Globespan chip 2.5.x or 3.0.x.	-
vendor { **normal** | **gs** [**enhanced**] }	Specifies the vendor ID of the G.SHDSL interface. ● **normal** indicates the device vendor ID. ● **gs** indicates Globespan vendor ID. **gs enhanced** indicates enhanced Globespan vendor ID. The peer device with Globespan vendor ID will disconnect from the router that has an ID different from Globespan vendor ID. To solve the problem, set the vendor ID to Globespan vendor ID. **NOTE** If the router configured with Globespan vendor ID cannot communicate with the peer device, configure enhanced Globespan vendor ID.	-
filter { **normal** | **specific** }	Specifies the interoperatability mode of the G.SHDSL interface. ● **normal** indicates the default mode. ● **specific** indicates the mode in which the device can identify signals sent by the peer device when the device connects to the peer device equipped with Globespan chip of earlier version and the rate is less than 512 kbit/s, and the power spectral density (PSD) mode does not comply with standards.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to connect to the peer device, run the **shdsl compatibility** command to configure the capability for the G.SHDSL interface based on the chip type of the peer device.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Example

Set the compatibility mode for ATM 1/0/0.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl compatibility pmms long vendor gs filter specific
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.14 shdsl current target snr margin downstream

Function

The **shdsl current target snr margin downstream** command sets the downlink signal to noise ratio (SNR) on a G.SHDSL interface.

The **undo shdsl current target snr margin downstream** command restores the default setting.

By default, the downlink SNR on a G.SHDSL interface is 6 dB.

Format

shdsl current target snr margin downstream *value*

undo shdsl current target snr margin downstream

Parameters

Parameter	Description	Value
value	Specifies the downlink SNR on a G.SHDSL interface.	The value is an integer that ranges from 0 to 10, in dB.

 Copyright © Huawei Technologies Co., Ltd.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the downlink SNR for a G.SHDSL interface to manage the device.

When the actual SNR of the device is greater than the configured SNR, the device is activated successfully.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Configuration Impact

If you run the **shdsl current target snr margin downstream** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

Example

Set the downlink SNR on a G.SHDSL interface to 4 dB.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl current target snr margin downstream 4
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.15 shdsl current target snr margin upstream

Function

The **shdsl current target snr margin upstream** command sets the uplink signal to noise ratio (SNR) on a G.SHDSL interface.

The **undo shdsl current target snr margin upstream** command restores the default setting.

By default, the uplink SNR on a G.SHDSL interface is 6 dB.

Format

shdsl current target snr margin upstream *value*

undo shdsl current target snr margin upstream

Parameters

Parameter	Description	Value
value	Specifies the uplink SNR on a G.SHDSL interface.	The value is an integer that ranges from 0 to 10, in dB.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the uplink SNR for a G.SHDSL interface to manage the device.

When the actual SNR of the device is greater than the configured SNR, the device is activated successfully.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Configuration Impact

If you run the **shdsl current target snr margin upstream** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

Example

Set the uplink SNR on a G.SHDSL interface to 4 dB.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl current target snr margin upstream 4
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.16 shdsl line-probing

Function

The **shdsl line-probing** command enables or disables the line probing function on a G.SHDSL interface.

By default, the line probing function is enabled on a G.SHDSL interface.

Format

shdsl line-probing { **disable** | **enable** }

Parameters

Parameter	Description	Value
disable	Disables the line probing function on a G.SHDSL interface.	-
enable	Enables the line probing function on a G.SHDSL interface.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **shdsl line-probing** command is used in the following scenarios:

- If the remote DSLAM is configured with the maximum and minimum G.SHDSL line rates, the local G.SHDSL interface must be activated at a rate within the specified range. By enabling the line probing function on the G.SHDSL interface, configure the G.SHDSL interface to be activated at the rate that is within the specified range and matches the actual line rate.
- If the remote DSLAM is configured with a fixed G.SHDSL line rate, the local G.SHDSL interface must be activated at the fixed G.SHDSL line rate. By disabling the line probing function on the G.SHDSL interface, enable the G.SHDSL interface to be activated at the fixed G.SHDSL line rate.

Prerequisites

The G.SHDSL interface has been deactivated using the **shutdown** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Enabling the line probing function prolongs interface activation, and disabling the line probing function shortens interface activation.

If a G.SHDSL interface fails to be activated, the maximum and minimum line rates need to be reconfigured on the remote DSLAM to ensure successful interface activation, regardless of whether the line probing function is enabled.

The line probing function can be enabled or disabled on G.SHDSL interfaces working in ATM or PTM transmission mode. If the transmission mode is set to ATM and the interface binding mode is set to M-Pair binding, the line probing function must be enabled or disabled on the main interface.

Example

Disable the line probing function on G.SHDSL interface 1/0/0 working in PTM transmission mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0] shutdown
[Huawei-Ethernet1/0/0] shdsl line-probing disable
```

Related Topics

5.17.8 set workmode shdsl

5.17.17 shdsl mode

Function

The **shdsl mode** command configures a working mode for a G.SHDSL interface.

The **undo shdsl mode** command restores the default working mode of a G.SHDSL interface.

By default, a G.SHDSL interface works in CPE mode.

Format

shdsl mode { **co** | **cpe** }

undo shdsl mode

Parameters

Parameter	Description	Value
co	Indicates that a G.SHDSL interface works in CO mode.	-
cpe	Indicates that a G.SHDSL interface works in CPE mode.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two devices establish a back-to-back connection, one device must work in CO mode and the other device must work in CPE mode.

Prerequisites

1. All the G.SHDSL interfaces on the same board (4G.SHDSL interface card or SRU) have been deactivated using the **shutdown** command.
2. All the G.SHDSL interfaces on the same board (4G.SHDSL interface card or SRU) are not bound together.

Precautions

This command can be configured only on the G.SHDSL interface with the smallest interface number among all the G.SHDSL interfaces on the same board (4G.SHDSL interface card or SRU).

Example

Configure the G.SHDSL interface using ATM to work in CO mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/1
[Huawei-Atm1/0/1] shutdown
[Huawei-Atm1/0/1] quit
[Huawei] interface atm 1/0/2
[Huawei-Atm1/0/2] shutdown
[Huawei-Atm1/0/2] quit
[Huawei] interface atm 1/0/3
[Huawei-Atm1/0/3] shutdown
[Huawei-Atm1/0/3] quit
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl mode co
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.18 shdsl pam

Function

The **shdsl pam** command sets the modulation mode on a G.SHDSL interface.

The **undo shdsl pam** command restores the default setting.

By default, a G.SHDSL interface uses the auto mode.

Format

shdsl pam { **16** | **32** | **64** | **128** | **auto** }

undo shdsl pam

Parameters

Parameter	Description	Value
16	Indicates 16 PAM mode.	-
32	Indicates 32 PAM mode.	-
64	Indicates 64 PAM mode.	-
128	Indicates 128 PAM mode.	-
auto	Indicates the auto mode. **NOTE** If a G.SHDSL interface uses the auto mode, only the 16 PAM mode and 32 PAM mode can be configured automatically, the 64 PAM mode and 128 PAM mode must be configured manually.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to connect to the peer device, run the **shdsl pam** command to set the modulation mode for a G.SHDSL interface based on the chip type of the peer device.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Precautions

If you run the **shdsl pam** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

- When the g-shdsl mode is configured, G.SHDSL interface only supports 16 PAM mode.
- When the g-shdsl.bis mode is configured, G.SHDSL interface supports 16 PAM, 32 PAM, 64 PAM, 128 PAM, and auto modes. By default, when the g-shdsl.bis mode is configured, G.SHDSL interface uses the auto mode.

Example

Configure 32 PAM mode for the G.SHDSL interface card working in ATM transmission mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl pam 32
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.19 shdsl pbo

Function

The **shdsl pbo** command adjusts the transmit power of a G.SHDSL interface.

The **undo shdsl pbo** command restores the default mode for the transmit power of a G.SHDSL interface.

By default, the auto mode is used.

Format

shdsl pbo { *value* | **auto** }

undo shdsl pbo

Parameters

Parameter	Description	Value
value	Specifies the adjusted transmit power.	The value is an integer that ranges from 1 to 31, in dB.
auto	Indicates that the transmit power is adjusted automatically.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Normally, an interface adjusts its transmit power based on the line noise to achieve a proper SNR. When the noise is known or the rate automatically adjusted by the interface is inaccurate, you can manually adjust the transmit power.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Example

Set the transmit power of the G.SHDSL interface in ATM mode to 20 dB.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl pbo 20
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

 Copyright © Huawei Technologies Co., Ltd.

5.17.20 shdsl psd

Function

The **shdsl psd** command sets the Power Spectral Density (PSD) mode for a G.SHDSL interface.

By default, the PSD mode of a G.SHDSL interface is symmetric PSD.

Format

shdsl psd { **asymmetry** | **symmetry** }

Parameters

Parameter	Description	Value
asymmetry	Indicates asymmetric PSD. In asymmetric PSD mode, the device uses a high output power for better transmission performance and is suitable for long-distance transmission.	-
symmetry	Indicates symmetric PSD. In symmetric PSD mode, the device is spectral-compatible with other services, uses less power, and is suitable for short-distance transmission.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to transmit services on a G.SHDSL line, run the **shdsl psd** command to set the same PSD mode as the DSLAM for the device.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The PSD describes how the power of a signal or time series is distributed with frequency.

Prerequisites

The G.SHDSL interface has been deactivated using the **shutdown** command.

Precautions

The PSD mode can be configured on G.SHDSL interfaces working in ATM or PTM transmission mode. If the transmission mode is set to ATM and the interface binding mode is set to M-Pair binding, the PSD mode must be configured on the main interface.

Example

Set asymmetric PSD on G.SHDSL interface 1/0/0 working in PTM transmission mode.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl ptm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface ethernet 1/0/0
[Huawei-Ethernet1/0/0] shutdown
[Huawei-Ethernet1/0/0] shdsl psd asymmetry
```

Related Topics

5.17.8 set workmode shdsl

5.17.21 shdsl rate auto

Function

The **shdsl rate auto** command sets the default rate of a G.SHDSL interface.

Format

shdsl rate auto

Parameters

None.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default minimum rate of a G.SHDSL interface is 192 kbit/s, and the default maximum rate of a G.SHDSL interface is 15296 kbit/s.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Example

Set the default rate of a G.SHDSL interface.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl rate auto
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.22 shdsl rate maximum

Function

The **shdsl rate maximum** command sets the maximum rate on a G.SHDSL interface.

The **undo shdsl rate maximum** command restores the default maximum rate of a G.SHDSL interface.

By default, the maximum rate on a G.SHDSL interface is 15296 kbit/s.

Format

shdsl rate maximum *maximum*

undo shdsl rate maximum

Parameters

Parameter	Description	Value
maximum	Specifies the maximum rate of a G.SHDSL interface.	The value is an integer that ranges from 192 to 15296, in kbit/s. The configured maximum rate must be greater than or equal to the configured minimum rate.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To meet requirements for the transmission rate, run the **shdsl rate maximum** command to set the maximum rate on a G.SHDSL interface.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Precautions

If you run the **shdsl rate maximum** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

- In g-shdsl mode, the value must range from 192 to 2304, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 16 PAM, the value must range from 192 to 2304, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 32 PAM, the value must range from 192 to 5696, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 64 PAM, the value must range from 192 to 12736, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 128 PAM, the value must range from 192 to 15296, in kbit/s.

NOTE

The value of *maximum* is a multiple of 64 except 2312 kbit/s and 3848 kbit/s. For example, when *maximum* is set to 650 kbit/s, the value 640 kbit/s takes effect. When *maximum* is set to 2312 kbit/s, the value 2312 kbit/s takes effect.

Example

Set the maximum rate of a G.SHDSL interface to 3840 kbit/s.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl rate maximum 3840
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.23 shdsl rate minimum

Function

The **shdsl rate minimum** command sets the minimum rate on a G.SHDSL interface.

The **undo shdsl rate minimum** command restores the default minimum rate of a G.SHDSL interface.

By default, the minimum rate on a G.SHDSL interface is 192 kbit/s.

Format

shdsl rate minimum *minimum*

undo shdsl rate minimum

Parameters

Parameter	Description	Value
minimum	Specifies the minimum rate of a G.SHDSL interface.	The value is an integer that ranges from 192 to 15296, in kbit/s. The configured minimum rate must be smaller than or equal to the configured maximum rate.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To meet requirements for the transmission rate, run the **shdsl rate minimum** command to set the minimum rate on a G.SHDSL interface.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Precautions

If you run the **shdsl rate minimum** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

- In g-shdsl mode, the value must range from 192 to 2304, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 16 PAM, the value must range from 192 to 2304, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 32 PAM, the value must range from 192 to 5696, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 64 PAM, the value must range from 192 to 12736, in kbit/s.
- In g-shdsl.bis mode, when the modulation mode is 128 PAM, the value must range from 192 to 15296, in kbit/s.

NOTE

The value of *minimum* is a multiple of 64 except 2312 kbit/s and 3848 kbit/s. For example, when *minimum* is set to 650 kbit/s, the value 640 kbit/s takes effect. When *minimum* is set to 2312 kbit/s, the value 2312 kbit/s takes effect.

Example

Set the minimum rate of a G.SHDSL interface to 320 kbit/s.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl rate minimum 320
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.24 shdsl tc mode

Function

The **shdsl tc mode** command configures the extended compatibility mode at the transport layer of a G.SHDSL interface. A G.SHDSL interface supports IEEE and ITU-T handshake modes.

The **undo shdsl tc mode** command restores the default setting.

By default, the extended compatibility mode at the transport layer of a G.SHDSL interface is **efm**.

Format

shdsl tc mode { **efm** | **ptm_6465o** | **efm_6465o** }

undo shdsl tc mode

Parameters

Parameter	Description	Value
efm	Configures a G.SHDSL interface to work in efm mode. The efm mode only applies to the IEEE handshake mode.	-
ptm_6465o	Configures a G.SHDSL interface to work in ptm_6465o mode. The ptm_6465o mode only applies to the ITU-T handshake mode.	-
efm_6465o	Configures a G.SHDSL interface to work in efm_6465o mode. The efm_6465o mode applies to IEEE and ITU-T handshake modes.	-

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The handshake mode varies according to the chip type on the DSLAM. You need to configure the extended compatibility mode at the transport layer of the local interface so that the local device can communicate with the DSLAM using IEEE and ITU-T handshake modes.

Prerequisites

Before configuring the extended compatibility mode at the transport layer of a G.SHDSL interface, complete the following configurations:

1. Run the **set workmode** command to set the transmission mode to PTM.
2. Run the **shutdown** command to deactivate all PTM interfaces.
3. Run the **shdsl mode** command to set the working mode of the G.SHDSL interface to CPE (client) mode.

Precautions

Only the PTM main interface supports this command. The configured extended compatibility mode at the transport layer takes effect for all PTM interfaces.

Example

Set the extended compatibility mode at the transport layer of Ethernet0/0/0 to efm_6465o.

```
<Huawei> system-view
[Huawei] set workmode slot 0 shdsl ptm
```

```
Warning: Changing the working mode will reset the board in slot 0. Continue? [y/
n]:y
INFO: Resetting board[0] succeeded.
[Huawei] interface ethernet0/0/0
[Huawei-Ethernet0/0/0] shutdown
[Huawei-Ethernet0/0/0] shdsl mode cpe
[Huawei-Ethernet0/0/0] shdsl tc mode efm_6465o
```

Related Topics

5.17.8 set workmode shdsl

5.17.13 shdsl compatibility

5.17.27 shutdown (g.shdsl)

5.17.25 shdsl worst case target snr margin upstream

Function

The **shdsl worst case target snr margin upstream** command sets the lowest uplink signal to noise ratio (SNR) on a G.SHDSL interface.

The **undo shdsl worst case target snr margin upstream** command restores the default setting.

By default, the lowest uplink SNR on a G.SHDSL interface is 0 dB.

Format

shdsl worst case target snr margin upstream *value*

undo shdsl worst case target snr margin upstream

Parameters

Parameter	Description	Value
value	Specifies the lowest uplink SNR on a G.SHDSL interface.	The value is an integer that ranges from 0 to 6, in dB.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the lowest uplink SNR for a G.SHDSL interface to manage the device.

If the actual lowest SNR of the device is smaller than the configured lowest uplink SNR, the device is disconnected.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Precautions

If you run the **shdsl worst case target snr margin upstream** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

Example

Set the lowest uplink SNR on a G.SHDSL interface to 6 dB.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl worst case target snr margin upstream 6
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.26 shdsl worst case target snr margin downstream

Function

The **shdsl worst case target snr margin downstream** command sets the lowest downlink signal to noise ratio (SNR) on a G.SHDSL interface.

The **undo shdsl worst case target snr margin downstream** command restores the default setting.

By default, the lowest downlink SNR on a G.SHDSL interface is 0 dB.

Format

shdsl worst case target snr margin downstream *value*

undo shdsl worst case target snr margin downstream

Parameters

Parameter	Description	Value
value	Specifies the lowest downlink SNR on a G.SHDSL interface.	The value is an integer that ranges from 0 to 6, in dB.

 Copyright © Huawei Technologies Co., Ltd.

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the lowest downlink SNR for a G.SHDSL interface to manage the device.

If the actual lowest SNR of the device is smaller than the configured lowest downlink SNR, the device is disconnected.

Prerequisites

The **shutdown** command has been executed on the G.SHDSL interface.

Precautions

If you run the **shdsl worst case target snr margin downstream** command multiple times in the same G.SHDSL interface view, only the latest configuration takes effect.

Example

Set the lowest downlink SNR on a G.SHDSL interface to 6 dB.

```
<Huawei> system-view
[Huawei] set workmode slot 1 shdsl atm
Warning: Changing the working mode will reset the board in slot 1. Continue? [y/
n]:y
INFO: Resetting board[1] succeeded.
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] shutdown
[Huawei-Atm1/0/0] shdsl worst case target snr margin downstream 6
```

Related Topics

5.17.8 set workmode shdsl

5.17.27 shutdown (g.shdsl)

5.17.27 shutdown (g.shdsl)

Function

The **shutdown** command deactivates a G.Single-pair high-speed Digital Subscriber Line (G.SHDSL) interface.

The **undo shutdown** command activates a G.SHDSL interface.

By default, a G.SHDSL interface is activated.

Format

shutdown

undo shutdown

Parameters

None

Views

G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

G.SHDSL interfaces must be activated before transmitting services. Activation of a G.SHDSL interface refers to the training between a Digital Subscriber Line Access Multiplexer (DSLAM) and a Customer Premises Equipment (CPE). During the training, the two devices check the line distance and status based on parameters such as the transmission standard, upstream and downstream line rates, and specified noise margin to determine whether they can work properly under the existing conditions. If the training succeeds, the G.SHDSL interface on the CPE is activated and can transmit services between the two devices.

The device functions as a CPE and aggregates services to a DSLAM by using a G.SHDSL interface.

After the device starts, its G.SHDSL interface is automatically activated. The G.SHDSL interface remains activated as long as its G.SHDSL line works properly. To enable the device to communicate with a DSLAM, run the **undo activate** command to deactivate the G.SHDSL interface on the device, set parameters such as the transmission standard, interface binding mode, power spectral density (PSD) mode, and line probing function for the interface, and then reactivate the interface to make the configured parameters take effect.

Precautions

After a G.SHDSL interface is deactivated, the device is disconnected from a DSLAM. To enable the G.SHDSL interface to transmit services, reactivate this G.SHDSL interface.

Example

Activate G.SHDSL interface 1/0/0 working in ATM transmission mode.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

5.17.5 interface atm (g.shdsl)

5.18 IMA Commands

NOTE

AR1200 series, AR2204, AR2220E, AR2220, AR2240, AR3260 and AR3670 support E1-IMA interfaces.

5.18.1 clock (E1-IMA)

Function

The **clock** command configures the clock mode of an E1-IMA interface.

The **undo clock** command restores the default clock mode of an E1-IMA interface.

By default, the clock mode of an E1-IMA interface is slave (**slave**).

Format

clock { **master** | **slave** }

undo clock

Parameters

Parameter	Description	Value
master	Indicates that the clock mode of an E1-IMA interface is master.	-
slave	Indicates that the clock mode of an E1-IMA interface is slave.	-

Views

E1-IMA interface view

Default Level

2: Configuration level

Usage Guidelines

When the router is connected to the peer device through E1-IMA interfaces, one E1-IMA interface must work in master clock mode and the other must work in slave clock mode.

Example

Set the clock mode to master on the interface ATM 2/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] clock master
```

5.18.2 differential-delay

Function

The **differential-delay** command configures the maximum differential delay of member links in an IMA group.

The **undo differential-delay** command restores the default maximum differential delay of member links in an IMA group.

By default, the maximum differential delay of member links in an IMA group is 25 ms.

Format

differential-delay *interval*

undo differential-delay

Parameters

Parameter	Description	Value
interval	Specifies the maximum differential delay of member links in an IMA group.	The value is an integer that ranges from 25 to 100, in milliseconds.

Views

IMA group view

Default Level

2: Configuration level

Usage Guidelines

The local device sends data over the member links in an IMA group at the same time. However, there is a delay when the data reaches the peer device. The **differential-delay** command configures the maximum differential delay of member links in an IMA group.

If the maximum differential delay of member links in an IMA group exceeds the set *interval*, the link-layer protocol of the IMA link becomes Down.

Example

Set the maximum differential delay of member links in an IMA group to 25 ms.

```
<Huawei> system-view
[Huawei] interface ima-group 2/0/0
```

```
[Huawei-Ima-group2/0/0] differential-delay 25
```

Related Topics

5.18.12 interface ima-group

5.18.3 display interface atm (E1-IMA)

Function

The **display interface atm** command displays information about E1-IMA interfaces.

Format

display interface atm [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Displays information about a specified E1-IMA interface. If no interface number is specified, information about all the interfaces of this type is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display interface atm** command to obtain the status of and statistics on an interface when you monitor the interface status or locate faults on the interface. You can collect traffic statistics and diagnose faults on the interface according to the command output.

Example

Display information about the E1-IMA interface ATM 2/0/0.

```
<Huawei> display interface atm 2/0/0
Atm2/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-07-24 14:13:49
```

```
Description:HUAWEI, AR Series, Atm2/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
AAL enabled: AAL5, Maximum PVCs: 8
PVCs on main-interface: 0 (Total PVCs: 0)
Last physical up time   : 2012-07-24 14:13:49
Last physical down time : 2012-07-24 14:07:06
Current system time: 2012-07-25 15:29:46
  ATM over E1, Scramble is Enabled, baudrate is 1920000 bps
  Frame-format is NO-Crc4-Adm, Line Code is Hdb3.
  Source Clock is Slave, Loopback is Not Set.
Last 300 seconds input rate 0 bytes/sec 0 bits/sec 0 packets/sec
Last 300 seconds output rate 0 bytes/sec 0 bits/sec 0 packets/sec

Input: 0 packets, 0 bytes
  Total Error: 0
  CRC: 0
Output: 0 packets, 0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-63 Description of the display interface atm command output

Item	Description
Atm2/0/0 current state	Physical status of ATM 2/0/0: ● UP: indicates that the physical status of the interface is Up. ● DOWN: indicates that the interface has a fault. ● Administratively down: indicates that the administrator has run the **shutdown** command on the interface.
Current state of the line protocol	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol of the interface is Down or no IP address is assigned to the interface.
Last line protocol up time	Last time when the link layer protocol of the interface goes Up.
Description	Interface description. The description contains a maximum of 242 case-sensitive characters, with spaces supported. This field describes functions of the interface.
The Maximum Transmit Unit is	MTU of the interface. By default, the MTU is 1488 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet protocol processing	If no IP address is assigned to the interface, Internet protocol processing: disabled is displayed. If an IP address is assigned to the interface, the IP address and subnet mask are displayed.
AAL enabled	ATM adaptation layer. **NOTE** The device supports only ATM Adaptation Layer Type 5 (AAL5).
Maximum PVCs	Maximum number of virtual circuits (VCs).
PVCs on main-interface: (Total PVCs:)	Number of PVCs on the main interface (total number of VCs on both the main interface and sub-interfaces).
Last physical up time	Last time when the interface went Up physically. If the value of this field is displayed as "-", the physical status of the interface has not changed. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last physical down time	Last time when the interface went Down physically. If the value of this field is displayed as "-", the physical status of the interface has not changed. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Scramble is	Payload scramble enabling on the E1-IMA interface. The scramble function can be configured by using the **5.18.15 scramble** command.
Frame-format is	Frame format of the E1-IMA interface. The frame-format can be configured by using the **5.18.5 frame-format** command.
Line Code is	Line code of the E1-IMA interface.
Source Clock is	Clock mode of the E1-IMA interface. The clock mode can be configured by using the **5.18.1 clock (E1-IMA)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Loopback is	Loopback mode of the E1-IMA interface. The loopback mode can be configured by using the **5.18.13 loopback** command.
Last 300 seconds input rate	Incoming packet rate (bit/s and pps) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bit/s and pps) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization	Percentage of the incoming packet rate to the total bandwidth.
Output bandwidth utilization	Percentage of the outgoing packet rate to the total bandwidth.

Related Topics

5.1.16 shutdown (interface view)
5.18.15 scramble
5.18.5 frame-format
5.18.1 clock (E1-IMA)
5.18.13 loopback

5.18.4 display interface ima-group

Function

The **display interface ima-group** command displays information about IMA groups.

Format

display interface ima-group [*interface-number*]

Parameters

Parameter	Description	Value
interface-number	Displays information about a specified IMA group. If no IMA group number is specified, information about all IMA groups is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display interface ima-group** command to obtain the status of and statistics on the IMA group when you monitor the interface status or locate faults on an interface. You can collect traffic statistics and diagnose faults on the interface according to the command output.

Example

Display information about the IMA group 2/0/0.

```
<Huawei> display interface ima-group 2/0/0
Ima-group2/0/0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2013-01-08 16:28:55
Description:HUAWEI, AR Series, Ima-group2/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.1/24
AAL enabled: AAL5, Maximum PVCs: 8
PVCs on main-interface: 4 (Total PVCs: 4)
Current system time: 2013-01-08 17:55:53
Physical layer is ATM over IMA
 Maximum allowed differential delay is: 25ms, Minimum required active links num:
 1
 Tx frame length: 32, symmetry: symmetrical configuration and operation
 Ne Tx clock mode CTC
 Ima protocol version: Version 1.0(standard implementation)
 Ima group near-end state is: operational
 Ima group far-end state is: operational
  LinkName Atm2/0/0
   NeLink TxLid 1, Tx Link state is active
   NeLink RxLid 1, Rx link state is active
   FeLink TxLid 1, Tx Link state is active
   FeLink RxLid 1, Rx link state is active
   Defect: NONE
  LinkName Atm2/0/1
   NeLink TxLid 2, Tx Link state is active
   NeLink RxLid 2, Rx link state is active
```

```
  FeLink TxLid 2, Tx Link state is active
  FeLink RxLid 2, Rx link state is active
  Defect: NONE
Last 300 seconds input rate 58701 bytes/sec 469608 bits/sec 611 packets/sec
Last 300 seconds output rate 58634 bytes/sec 469072 bits/sec 611 packets/sec

Input: 3317314 packets, 318312108 bytes
Output: 3317257 packets, 318305028 bytes
   Input bandwidth utilization  : 6.38%
   Output bandwidth utilization : 6.38%
```

Table 5-64 Description of the display interface ima-group command output

Item	Description
Ima-group2/0/0 current state	Status of IMA-group 2/0/0: ● UP: indicates that the physical status of the interface is Up. ● DOWN: indicates that the interface has a fault. ● Administratively down: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates the link layer protocol status of the interface is Down.
Last line protocol up time	Last time when the link layer protocol of the interface goes Up.
Description	Interface description. The description contains a maximum of 242 case-sensitive characters, with spaces supported. This field describes functions of the interface.
The Maximum Transmit Unit is	MTU of the interface. By default, the MTU is 1488 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is configured, these packets are discarded.
Internet protocol processing	If no IP address is assigned to the interface, Internet protocol processing: disabled is displayed. If an IP address is assigned to the interface, the IP address and subnet mask are displayed.
AAL enabled	ATM adaptation layer. **NOTE** The device supports only AAL5.
Maximum PVCs	Maximum number of VCs.

Item	Description
PVCs on main-interface: (Total PVCs:)	Number of PVCs on the main interface (total number of VCs on both the main interface and sub-interfaces).
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Physical layer is	Type of the physical layer.
Maximum allowed differential delay is	Maximum differential delay of member links in the IMA group. Maximum differential delay of member links in an IMA group can be configured by using the **5.18.2 differential-delay** command.
Minimum required active links num	Minimum number of available member links in the IMA group. Minimum number of available member links in an IMA group can be configured by using the **5.18.14 min-active-links** command.
Tx frame length	Number of the cells contained in the IMA frame. Number of the cells contained in an IMA frame can be configured by using the **5.18.6 frame-length** command.
symmetry: symmetrical configuration and operation	Power spectral density (PSD) mode of the interface.
Ne Tx clock mode CTC	Clock mode of the IMA group. The clock mode can be configured by using the **5.18.8 ima-clock** command.
Ima protocol version	Standard used by the IMA group. The standard used by an IMA group can be configured by using the **5.18.10 ima-standard** command.
Ima group near-end state is	State of the local IMA group.
Ima group far-end state is	State of the remote IMA group.
NeLink TxLid 1, Tx Link state is active	LID of the transmit link at the local end. The transmit link status is active.
NeLink RxLid 1, Rx link state is active	LID of the receive link at the local end. The receive link status is active.
FeLink TxLid 1, Tx Link state is active	LID of the transmit link at the remote end. The transmit link status is active.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FeLink RxLid 1, Rx link state is active	LID of the receive link at the remote end. The receive link status is active.
Defect	Link fault.
Last 300 seconds input rate	Incoming packet rate (bit/s and pps) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bit/s and pps) within the last 300 seconds.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization	Percentage of the incoming packet rate to the total bandwidth.
Output bandwidth utilization	Percentage of the outgoing packet rate to the total bandwidth.

Related Topics

5.1.16 shutdown (interface view)
5.18.2 differential-delay
5.18.6 frame-length
5.18.10 ima-standard
5.18.14 min-active-links

5.18.5 frame-format

Function

The **frame-format** command configures the frame format for an E1-IMA interface.

The **undo frame-format** command restores the default frame format for an E1-IMA interface.

By default, the frame format of an E1-IMA interface is No-CRC4 ADM.

Format

frame-format { **crc4-adm** | **no-crc4-adm** }

undo frame-format

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
crc4-adm	Indicates that the frame format of the E1-IMA interface is CRC4 ADM.	-
no-crc4-adm	Indicates that the frame format of the E1-IMA interface is No-CRC4 ADM.	-

Views

E1-IMA interface view

Default Level

2: Configuration level

Usage Guidelines

ATM direct mapping (ADM) technology maps ATM sells transmitted over the E1 lines to E1 frames.

To ensure the normal service transmission on the links, run the **frame-format** command to configure the E1-IMA interface to use the same frame format as the peer device.

Example

Set the frame format to No-CRC4 ADM on the interface ATM 2/0/0.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] frame-format no-crc4-adm
```

5.18.6 frame-length

Function

The **frame-length** command configures the number of the ATM cells contained in an IMA frame.

The **undo frame-length** command restores the default number of the ATM cells contained in an IMA frame.

By default, an IMA frame contains 128 ATM cells.

Format

frame-length { **32** | **64** | **128** | **256** }

undo frame-length

Parameters

Parameter	Description	Value
32	Indicates that an IMA frame contains 32 ATM cells.	-
64	Indicates that an IMA frame contains 64 ATM cells.	-
128	Indicates that an IMA frame contains 128 ATM cells.	-
256	Indicates that an IMA frame contains 256 ATM cells.	-

Views

IMA group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You must configure the same number of the ATM cells contained in an IMA frame as the peer device; otherwise, the IMA protocol negotiation fails.

Precautions

After the **frame-length** command is executed, run the **shutdown** and **undo shutdown** commands in the IMA group view to make the configuration take effect.

Example

Set the number of the cells contained in an IMA frame to 64.

```
<Huawei> system-view
[Huawei] interface ima-group 2/0/0
[Huawei-Ima-group2/0/0] frame-length 64
```

Related Topics

5.18.12 interface ima-group

5.18.7 ima ima-group

Function

The **ima ima-group** command adds an interface to a specified IMA group.

The **undo ima ima-group** command removes an interface from an IMA group.

Format

ima ima-group *interface-number*

undo ima ima-group

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an IMA group. The value is in slot ID/subcard ID/interface serial number format.	The slot ID of the IMA group must be same as that of the E1-IMA interface. The interface serial number ranges from 0 to 3.

Views

E1-IMA interface view, G.SHDSL interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you require high bandwidth that a single E1-IMA link or G.SHDSL link cannot provide, you can bind multiple E1-IMA links or G.SHDSL links to an IMA group to increase the bandwidth.

Precautions

Before adding an E1-IMA or G.SHDSL interface to the IMA group, delete all network-layer configurations on the E1-IMA or G.SHDSL interface. For example, before running the **ima ima-group** command, you must run the **undo ip address** command to delete the IP address.

When removing a link from the original IMA group to a new IMA group, you need to remove two interfaces of the link from the original IMA group, and then add the two interfaces of the link to the new IMA group.

If two devices on both ends of a link cannot communicate after the link is removed from an original IMA group to a new IMA group, run the **shutdown** and **undo shutdown** commands in the IMA group view on the two devices.

Example

Add the E1-IMA interface 2/0/0 to the IMA group 2/0/0.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] ima ima-group 2/0/0
```

Related Topics

5.18.11 interface atm (E1-IMA)

5.18.8 ima-clock

Function

The **ima-clock** command configures the clock mode of an IMA group.

The **undo ima-clock** command restores the default clock mode of an IMA group.

By default, the clock mode of an IMA group is the common transmit clock (**CTC**).

Format

ima-clock { **ctc** [**link-number** *number*] | **itc** }

undo ima-clock

Parameters

Parameter	Description	Value
ctc	Indicates that the clock mode of an IMA group is CTC.	-
link-number *number*	Specifies the E1-IMA link number, which is the link number of a clock source.	The value is an integer that ranges from 0 to 3.
itc	Indicates that the clock mode of an IMA group is independent transmit clock (ITC).	-

Views

IMA group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IMA group supports the following clock modes:

- CTC: In this mode, all member links of an IMA group share a clock source, that is either an external clock or a clock of a member link.
- ITC: In this mode, the member links of an IMA group use at least two different clock sources.

Precautions

- If an IMA group uses the ITC clock mode, the clock mode of its member interfaces, namely, E1-IMA interfaces, must be set to slave.
- If an IMA group uses the CTC clock mode, E1-IMA interfaces must be set to master.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the ITC clock mode for an IMA group.

```
<Huawei> system-view
[Huawei] interface ima-group 2/0/0
[Huawei-Ima-group2/0/0] ima-clock itc
```

Related Topics

5.18.12 interface ima-group

5.18.9 ima-id

Function

The **ima-id** command sets the IMA ID of an IMA group.

The **undo ima-id** command restores the default IMA ID of an IMA group.

By default, the interface sequence number is used as the IMA ID of an IMA group.

Format

ima-id *ima-id*

undo ima-id

Parameters

Parameter	Description	Value
ima-id	Specifies the IMA ID of an IMA group.	The value is an integer that ranges from 0 to 255.

Views

IMA group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **ima-id** command to set the IMA ID of an IMA group.

Precautions

This command can be used only when no E1-IMA link or G.SHDSL link joins an IMA group.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the IMA ID of an IMA group to 1.

```
<Huawei> system-view
[Huawei] interface ima-group 2/0/0
[Huawei-Ima-group2/0/0] ima-id 1
```

Related Topics

5.18.12 interface ima-group

5.18.10 ima-standard

Function

The **ima-standard** command configures the standard used by an IMA group.

The **undo ima-standard** command restores the default standard used by an IMA group.

By default, the standard used by an IMA group is set to **normal**.

Format

ima-standard { **normal** | **standard-v10** | **standard-v11** | **alternate-v10** }

undo ima-standard

Parameters

Parameter	Description	Value
normal	The **normal** parameter has different meanings for IMA groups with different member interfaces: ● For an IMA group with G.SHDSL member interfaces, it indicates that the standard used by the IMA group is set to V1.1 (standard implementation). ● For an IMA group with E1-IMA member interfaces, it indicates that the IMA group automatically uses the same standard as the peer IMA group. **NOTE** If the peer IMA group uses V1.0 (other implementation), the local IMA group cannot automatically use the same standard as the peer IMA group.	-
standard-v10	Indicates that the standard used by the current IMA group is set to V1.0 (standard implementation).	-
standard-v11	Indicates that the standard used by the current IMA group is set to V1.1 (standard implementation). **NOTE** An IMA group with G.SHDSL member interfaces does not support this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
alternate-v10	Indicates that the standard used by the current IMA group is set to V1.0 (other implementation).	-

Views

IMA group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure the normal service transmission on links, run the **ima-standard** command to configure the IMA group to use the same standard as the peer device.

For a local IMA group with E1-IMA member interfaces, if the standard used by the peer IMA group is unknown, specify the **normal** parameter to configure the local IMA group to automatically use the same standard as the peer IMA group.

Precautions

After the **ima-standard** command is executed, run the **shutdown** and **undo shutdown** commands in the IMA group view to make the configuration take effect.

If there are multiple IMA groups composed of G.SHDSL interfaces on the device, these IMA groups must be configured with the same standard.

If the **normal** parameter is specified on both the local and remote devices, the standard used by the current IMA group is set to V1.1 (standard implementation).

Example

Set the standard to V1.0 for the current IMA group 2/0/0.

```
<Huawei> system-view
[Huawei] interface ima-group 2/0/0
[Huawei-Ima-group2/0/0] ima-standard standard-v10
[Huawei-Ima-group2/0/0] shutdown
[Huawei-Ima-group2/0/0] undo shutdown
```

Related Topics

5.18.12 interface ima-group

5.18.11 interface atm (E1-IMA)

Function

The **interface atm** command enters the E1-IMA interface view.

Format

interface atm *interface-number*

Parameters

Parameter	Description	Value
interface-number	Indicates the number of the E1-IMA interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **interface atm** command to enter the E1-IMA interface view and configure attributes for the E1-IMA interface.

Example

Enter the E1-IMA 2/0/0 view.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0]
```

Related Topics

5.18.3 display interface atm (E1-IMA)

5.18.12 interface ima-group

Function

The **interface ima-group** command creates an IMA group and enters the IMA group view.

The **undo interface ima-group** command deletes a created IMA group.

Format

interface ima-group *interface-number*

undo interface ima-group *interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the interface number of the IMA group.	The value is in slot ID/0/serial number format. The value of the serial number ranges from 0 to 3.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before binding multiple E1-IMA links or G.SHDSL links into an IMA group, you need to create an IMA group.

Example

Create an IMA group and enter the IMA group 2/0/0 view.

```
<Huawei> system-view
[Huawei] interface ima-group 2/0/0
[Huawei-Ima-group2/0/0]
```

Related Topics

5.18.11 interface atm (E1-IMA)

5.18.13 loopback

Function

The **loopback** command configures the loopback mode on an E1-IMA interface.

The **undo loopback** command cancels the loopback mode of an E1-IMA interface.

By default, loopback detection is disabled.

Format

loopback { **local** | **payload** | **remote** }

undo loopback

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
local	Indicates that the loopback mode of the E1-IMA interface is set to local.	-
payload	Indicates that the loopback mode of the E1-IMA interface is set to payload.	-
remote	Indicates that the loopback mode of the E1-IMA interface is set to remote.	-

Views

E1-IMA interface view

Default Level

2: Configuration level

Usage Guidelines

The loopback detection function monitors the interface status or cable status. This function must be disabled when devices are working properly.

- The **local** loopback tests whether the local device works properly by looping back outgoing packets to itself.
- The **payload** loopback tests whether the local device works properly by looping back the valid payload of outgoing packets. Generally, frames transmitted by timeslot 0 are not looped back.
- The **remote** loopback tests whether the link between the two devices works properly by looping back the packets received from its peer device to the peer device.

Example

Set the loopback mode to payload on the interface ATM 2/0/0.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] loopback payload
```

5.18.14 min-active-links

Function

The **min-active-links** command configures the minimum number of available member links in an IMA group.

The **undo min-active-links** command restores the default minimum number of available member links in an IMA group.

By default, the minimum number of available member links in an IMA group is 1.

Format

min-active-links *number*

undo min-active-links

Parameters

Parameter	Description	Value
number	Specifies the minimum number of available member links in an IMA group.	The value is an integer that ranges from 1 to 4.

Views

IMA group view

Default Level

2: Configuration level

Usage Guidelines

The bandwidth for an IMA group is determined by the minimum number of available member links in the group.

By default, the minimum number of available member links in an IMA group is 1. An IMA group can work as long as one member link is available.

Example

Set the minimum number of available member links in the IMA group 2/0/0 to 2.

```
<Huawei> system-view
[Huawei] interface ima-group 2/0/0
[Huawei-Ima-group2/0/0] min-active-links 2
```

Related Topics

5.18.12 interface ima-group

5.18.15 scramble

Function

The **scramble** command enables the scramble function on an E1-IMA interface.

The **undo scramble** command disables the scramble function on an E1-IMA interface.

By default, the payload scramble function is enabled on an E1-IMA interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

scramble

undo scramble

Parameters

None

Views

E1-IMA interface view

Default Level

2: Configuration level

Usage Guidelines

In the digital communication system, the scramble function is used to convert digital signals into pseudo random digital signals with the same meaning and same bit rate for easy transmission and storage.

The **scramble** command takes effect only on the payload rather than cell header.

- The scramble function can effectively prevent successive 0 and 1 in the sent data.
- The disabled scramble function does not convert the signals in sent data and not restore the signals in received data.

Example

Enable the payload scramble function on the E1-IMA interface ATM 2/0/0.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] scramble
```

5.19 PON Interface Configuration Commands

5.19.1 display epon-info interface pon

Function

The **display epon-info interface pon** command displays information about an Ethernet passive optical network (EPON) interface.

Format

display epon-info interface pon *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an EPON interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the attributes of an EPON interface, including the laser working mode, signal status, logical link identifier (LLID), encryption function status (enabled or disabled), encryption mode, loopback mode, and MAC address, password, or logical identifier and check code for authentication.

Example

Display information about EPON interface PON1/0/0.

```
<Huawei> display epon-info interface pon 1/0/0
 -----------------------------------------------------------------
  Mac-address        : 00E1-6600-0000
  Password           : %@%@GlX%9DYkb@mWA.Xsq}U7$RAuesDv~ix|CA/e>|<EVZS:RAx$%@%@
  Loid               : hwloid
  Check code         : eponcode
  Laser state        : Auto
  Signal state       : Up
  Loopback state     : No loopback
  Encryption state   : Off
  Encryption mode    : Triple Churning
  Rogue ONT state    : No
  Port role          : Protect
  Active state       : Standby
 -----------------------------------------------------------------
 ---------------------------------------------------
  LLID                    Register state
 ---------------------------------------------------
  -                       Unregistered
 ---------------------------------------------------
```

Table 5-65 Description of the display epon-info interface pon command output

Item	Description
Mac-address	MAC address that the EPON interface uses for authentication.
Password	Password that the EPON interface uses for authentication.

Item	Description
Loid	Logical identifier that the EPON interface uses for authentication.
Check code	Check code that the EPON interface uses for authentication.
Laser state	Laser working status of the optical module on the EPON interface. ● Auto: indicates that the optical module generates optical signals when data needs to be transmitted and stops generating optical signals when no data needs to be transmitted. ● On: indicates that the optical module continuously generates optical signals. ● Off: indicates that the optical module does not generate optical signals.
Signal state	Optical signal status on the EPON interface. ● Up: indicates that the optical signal is received. ● Down: indicates that the optical signal is not received or the optical power is beyond the normal range.
Loopback state	Loopback status on the EPON interface. ● No loopback: indicates that loopback is not configured on the interface. ● GE-PHY internal loopback: indicates internal loopback at the GE physical layer. ● GE-PHY line loopback: indicates line loopback at the GE physical layer. ● Unknown loopback state: indicates that the hardware does not support the loopback function.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Encryption state	Whether the encryption function is enabled. ● Off: indicates that the encryption function is disabled. ● Downstream encryption: indicates that encryption is enabled for downstream data. ● Down & Up stream encryption: indicates that encryption is enabled for both upstream data and downstream data.
Encryption mode	Encryption mode used on the EPON interface. Currently, the device supports only the triple churning encryption mode.
Rogue ONT state	Whether the optical network unit (ONT) is a rogue ONT. The value is Yes or No.
Port role	Role of the EPON interface. ● Work: working port ● Protect: protecting port
Active state	Active/standby status of the EPON interface.
LLID	Logical link identifier (LLID) of the EPON interface. ● -: indicates that the ONU does not have an LLID because it has not been registered. ● Value: indicates the LLID allocated to the ONU by the optical line terminal (OLT).
Register state	Registration status of the ONU. ● EXT-OAM-registered: indicates that the ONU has registered with the OLT successfully. ● Unregistered: indicates that the ONU has not registered.

Related Topics

5.19.8 epon-mac-address
5.19.9 epon-password

5.19.7 epon-loid
5.19.6 epon-checkcode

5.19.2 display gpon-info interface pon

Function

The **display gpon-info interface pon** command displays information about a gigabit passive optical network (GPON) interface.

Format

display gpon-info interface pon *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a GPON interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view attributes of a GPON interface, including the optical network unit (ONU) ID, serial number (SN), password, link status, registration status, Physical Layer Operations, Administration and Maintenance (PLOAM) status, port role, and active/standby status.

Example

Display information about GPON interface PON1/0/0.

```
<Huawei> display gpon-info interface pon 1/0/0
-----------------------------------------------------------------------------------------
  ONU-ID                  : 1
  SN                      : 6877687700111747 (hwhw-00111747)
  Password                : %@%@Hn5wW{:%FRZy7;6lp[NB,#o:%@%@
  Link state              : Up
  Register state          : Registered
  Ploam state             : Operation-State
  Laser switch            : Auto
  OMCI PortID             : 1
  Rogue ONT state         : No
  Port role               : Work
  Active state            : Active
-----------------------------------------------------------------------------------------
```

```
 -------------------------------------------------------------------------------
TCONT-INDEX  AllocID  GEM-PortID   Car-Index  Encrypt
-------------------------------------------------------------------------------
       0       0          -         -         -
       1     256          -         -         -
 -------------------------------------------------------------------------------
```

Table 5-66 Description of the display gpon-info interface pon command output

Item	Description
ONU-ID	ID of the ONU where the GPON interface is located. An ONU ID is a unique identifier allocated by the optical line terminal (OLT)
SN	SN of the ONU. The SN of each ONU is a globally unique string of 13 characters. The first four characters represent the manufacturer. The SN of a Huawei ONU starts with hwhw.
Password	Password that the GPON interface uses for authentication.
Link state	Link status of the GPON interface. The value is Up or Down.
Register state	Registration status of the ONU. ● Registered: indicates that the ONU has registered with the OLT successfully. ● Unregistered: indicates that the ONU has not registered.

Item	Description
PLOAM state	PLOAM status of the GPON interface. ● Initial-State: indicates that the ONU was just powered on or detected a loss of signal (LOS) or loss of frame (LOF). ● Standby-State: indicates that the ONU has received downstream frames and is waiting for network parameters. ● Serial-Number-State: indicates that the ONU is reporting its SN to the OLT. ● Ranging-State: indicates that the OLT is measuring the distance to the ONU. ● Operation-State: indicates that the ONU is working. ● POPUP-State: indicates that the ONU detects a LOS or LOF. ● Emergency-Stop-State: indicates that the ONU was stopped due an emergency.
Laser switch	Optical signal status on the GPON interface. ● Auto: indicates that the GPON interface is in auto state. ● Up: indicates that the GPON interface continuously generates optical signals. ● Off: indicates that the GPON interface does not generate optical signals.
OMCI portID	The GPON encapsulation mode (GEM) port ID used by the ONT Management Control Interface (OMCI). ONT stands for the optical network terminal.
Rogue ONT state	Whether the ONT is a rogue ONT. The value is Yes or No.
Port role	Role of the GPON interface. ● Work: working port ● Protect: protecting port
Active state	Active/standby status of the GPON interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TCONT-INDEX	T-CONT index used by the ONU.
AllocID	ID allocated by the OLT to identify a T-CONT.
GEM-PortID	GEM port ID that identifies a service flow.
Car-Index	Index of CAR applied to a GEM port.
Encrypt	Status of the encryption function on the GEM port. ● On: indicates that encryption is enabled on the GEM port. ● Off: indicates that encryption is disabled on the GEM port.

Related Topics

5.19.10 gpon-password

5.19.3 display pon-statistic interface pon

Function

The **display pon-statistic interface pon** command displays traffic statistics on a passive optical network (PON) interface.

Format

display pon-statistic interface pon *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a PON interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display pon-statistic interface pon** command displays traffic statistics on a PON interface, including the number of frames received, number of bytes received, numbers of uplink and downlink Ethernet frames, and real-time uplink and downlink traffic volumes.

To view the traffic statistics collected in a certain period, run the **reset pon-statistic interface pon** command to clear existing traffic statistics, and then run the **display pon-statistic interface pon** command.

NOTE

EPON and GPON interfaces use different packet encapsulation modes; therefore, the command outputs for EPON and GPON interfaces are different.

Example

Display traffic statistics on EPON interface PON1/0/0.

```
<Huawei> display pon-statistic interface pon 1/0/0
 ----------------------------------------------------------------
  Received frames                : 58032
  Received bytes                 : 2389
  Received unicast frames        : 0
  Received multicast frames      : 37
  Received broadcast frames      : 0
  Received 64-byte frames        : 33
  Received 65~127-byte frames    : 4
  Received 128~255-byte frames   : 0
  Received 256~511-byte frames   : 0
  Received 512~1023-byte frames  : 0
  Received 1024~1518-byte frames : 0
  Received over 1518-byte frames : 0
  Received undersize frames      : 0
  Received oversize frames       : 0
  Received CRC error frames      : 0
  Sent frames                    : 58005
  Sent bytes                     : 2523
  Sent unicast frames            : 0
  Sent multicast frames          : 37
  Sent broadcast frames          : 0
  Sent 64-byte frames            : 32
  Sent 65~127-byte frames        : 5
  Sent 128~255-byte frames       : 0
  Sent 256~511-byte frames       : 0
  Sent 512~1023-byte frames      : 0
  Sent 1024~1518-byte frames     : 0
  Sent over 1518-byte frames     : 0
  PON Rx FEC error frames        : 0
  PON Tx MPCP frames             : 57968
  PON Rx MPCP frames             : 57995
  PON Tx OAM frames              : 37
  PON Rx OAM frames              : 37
  Up traffic (kbps)              : 0
  Down traffic (kbps)            : 0
 ----------------------------------------------------------------
```

Table 5-67 Description of the display pon-statistic interface pon command output (EPON interface)

Item	Description
Received frames	Number of frames received by the EPON interface.
Received bytes	Number of bytes received by the EPON interface.
Received unicast frames	Number of unicast frames received by the EPON interface.
Received multicast frames	Number of multicast frames received by the EPON interface.
Received broadcast frames	Number of broadcast frames received by the EPON interface.
Received 64-byte frames	Number of 64-byte frames received by the EPON interface.
Received 65~127-byte frames	Number of frames of 65 to 127 bytes received by the EPON interface.
Received 128~255-byte frames	Number of frames of 128 to 255 bytes received by the EPON interface.
Received 256~511-byte frames	Number of frames of 256 to 511 bytes received by the EPON interface.
Received 512~1023-byte frames	Number of frames of 512 to 1023 bytes received by the EPON interface.
Received 1024~1518-byte frames	Number of frames of 1024 to 1518 bytes received by the EPON interface.
Received over 1518-byte frames	Number of frames of more than 1518 bytes received by the EPON interface.
Received undersize frames	Number of undersized frames received by the EPON interface.
Received oversize frames	Number of oversized frames received by the EPON interface.
Received CRC error frames	Number of frames with cyclic redundancy check (CRC) errors received by the EPON interface.
Sent frames	Number of frames sent by the EPON interface.
Sent bytes	Number of bytes sent by the EPON interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Sent unicast frames	Number of unicast frames sent by the EPON interface.
Sent multicast frames	Number of multicast frames sent by the EPON interface.
Sent broadcast frames	Number of broadcast frames sent by the EPON interface.
Sent 64-byte frames	Number of 64-byte frames sent by the EPON interface.
Sent 65~127-byte frames	Number of frames of 65 to 127 bytes sent by the EPON interface.
Sent 128~255-byte frames	Number of frames of 128 to 255 bytes sent by the EPON interface.
Sent 256~511-byte frames	Number of frames of 256 to 511 bytes sent by the EPON interface.
Sent 512~1023-byte frames	Number of frames of 512 to 1023 bytes sent by the EPON interface.
Sent 1024~1518-byte frames	Number of frames of 1024 to 1518 bytes sent by the EPON interface.
Sent over 1518-byte frames	Number of frames of more than 1518 bytes sent by the EPON interface.
PON Rx FEC error frames	Number of frames with forward error correction (FEC) errors received by the EPON interface.
PON Tx MPCP frames	Number of Multipoint Control Protocol (MPCP) frames sent by the EPON interface.
PON Rx MPCP frames	Number of MPCP frames received by the EPON interface.
PON Tx OAM frames	Number of OAM frames sent by the EPON interface.
PON Rx OAM frames	Number of OAM frames received by the EPON interface.
Up traffic	Real-time upstream traffic rate on the EPON interface.
Down traffic	Real-time downstream traffic rate on the EPON interface.

Display traffic statistics on GPON interface PON1/0/0.

```
<Huawei> display pon-statistic interface pon 1/0/0
 ----------------------------------------------------------------
  Up OMCI cells statistics                : 0
  Down OMCI cells statistics              : 0
  Up Ethernet frames statistics           : 224
  Down Ethernet frames statistics         : 134
  Up PLOAM messages statistics            : 0
  Down PLOAM messages statistics          : 12
 ----------------------------------------------------------------
```

Table 5-68 Description of the display pon-statistic interface pon command output (GPON interface)

Item	Description
Up OMCI Cells statistics	Number of upstream ONT Management Control Interface (OMCI) cells. ONT stands for the optical network terminal.
Down OMCI Cells statistics	Number of downstream OMCI cells.
Up Ethernet frames statistics	Number of upstream Ethernet frames.
Down Ethernet frames statistics	Number of downstream Ethernet frames.
Up PLOAM Messages statistics	Number of upstream Physical Layer Operations, Administration and Maintenance (PLOAM) messages. PLOAM messages are used for maintain optical network units (ONUs).
Down PLOAM Messages statistics	Number of downstream PLOAM messages.

Related Topics

5.19.19 reset pon-statistic interface pon

5.19.4 display pon-transceiver interface pon

Function

The **display pon-transceiver interface pon** command displays information about the optical module on a passive optical network (PON) interface.

Format

display pon-transceiver interface pon *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a PON interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pon-transceiver interface pon** command output includes the optical wavelength, identifier, transmission distance, version, bias current, voltage, and various alarm thresholds of an optical module.

Example

Display information about the optical module on PON1/0/0.

```
<Huawei> display pon-transceiver interface pon 1/0/0
 ---------------------------------------------------------------------------
 Optical Module status          : Online
 Wave Length(nm)                : 1310
 Identifier                     : SFP
 Ext.Identifier                 : GBIC/SFP function is defined by serial ID only
 Connector                      : SC
 Encoding                       : NRZ
 BR,Nominal(100Mbps)            : 13
 Length(9um)(km)                : 20.0
 Length(50um)                   : Not support
 Length(62.5um)                 : Not support
 Length(Copper)                 : Not support
 Cc_base                        : 0x1a
 CC_EXT                         : 0xf3
 BR,max                         : Unspecified
 BR,min                         : Unspecified
 SFF-8472 Compliance            : Invalid
 Options                        : TX_DISABLE,and disables the serial output
                                : TX_FAULT
                                : LOS(signal inverted from standard definition)
 Vendor Rev                     : Unspecified
 Vendor PN                      : HPSP2120
 Vendor SN                      : 030KMF1107501261
 Vendor OUI                     : 000000
 Manufactured                   : 10-07-08
 Vendor name                    : HUAWEI
 RX power(dBm)                  : -11.82
 TX power(dBm)                  : 2.49
 Temperature(C)                 : 53.87
 TX Bias current(mA)            : 10.54
 Supply Voltage(V)              : 3.25
 RX power Alarm Threshold(dBm) : [-,-]
 TX power Alarm Threshold(dBm) : [-,-]
 Temperature Alarm Threshold(C): [-,-]
```

```
TX Bias Alarm Threshold(mA)   : [10,20]
Voltage Alarm Threshold(V)    : [-,-]
-------------------------------------------------------------------------------
```

Table 5-69 Description of the display pon-transceiver interface pon command output

Optical Module status	Description
Optical Module status	Status of the optical module. The value is Online or Offline.
Wave Length(nm)	Optical wavelength of the optical module.
Identifier	Identifier of the optical module. ● Unknown ● GBIC ● Module/connector soldered to motherboard ● SFP
Ext.Identifier	Extended identifier of the optical module. ● Not specified or not compliant with a defined MOD_DEF. ● GBIC is compliant with MOD_DEF 1 ● GBIC is compliant with MOD_DEF 2 ● GBIC is compliant with MOD_DEF 3 ● GBIC/SFP function is defined by serial ID only ● GBIC is compliant with MOD_DEF 5 ● GBIC is compliant with MOD_DEF 6 ● GBIC is compliant with MOD_DEF 7

 Copyright © Huawei Technologies Co., Ltd.

Optical Module status	Description
Connector	Connector type used by the optical module. ● Unknown ● SC ● Fibre Channel Style 1 copper connector ● Fibre Channel Style 2 copper connector ● BNC/TNC ● Fibre Channel coaxial headers ● FiberJack ● LC ● MT-RJ ● MU ● SG ● Optical pigtail ● HSSDC II ● Copper Pigtail
Encoding	Encoding format used by the optical module. ● Unspecified ● 8B10B ● 4B5B ● NRZ ● Manchester ● SONET Scrambled
BR,Nominal(100Mbps)	Default bit rate.
Length(9um)(km)	Transmission distance of a 9/125 μm optical fiber.
Length(50um)	Transmission distance of a 50/125 μm optical fiber.
Length(62.5um)	Transmission distance of a 62.5/125 μm optical fiber.
Length(Copper)	Transmission distance of a copper network cable.
Cc_base	Check code for the basic ID.
CC_EXT	Check code for the extended ID.
BR,max	Maximum bit rate.

 Copyright © Huawei Technologies Co., Ltd.

Optical Module status	Description
BR,min	Minimum bit rate.
SFF-8472 Compliance	Whether the optical module complies with SFF-8472.
Options	Options.
Vendor Rev	Version of the optical module.
Vendor PN	Product number used by the manufacturer.
Vendor SN	Product number used by the manufacturer.
Vendor OUI	Organizationally Unique Identifier (OUI) of the manufacturer.
Manufactured	Production date of the optical module.
Vendor name	Name of the manufacturer.
RX power(dBm)	Receiving optical power.
TX power(dBm)	Sending optical power.
Temperature(C)	Operating temperature.
TX Bias current(mA)	Bias current of the optical module.
Supply Voltage(V)	Voltage provided for the optical module.
RX power Alarm Threshold(dBm)	Alarm threshold of the receiving optical power. To set the alarm threshold, run the **optical-module threshold rx-power** command.
TX power Alarm Threshold(dBm)	Alarm threshold of the transmitting optical power. To set the alarm threshold, run the **optical-module threshold tx-power** command.
Temperature Alarm Threshold(C)	Alarm threshold of the operating temperature. To set the alarm threshold, run the **optical-module threshold temperature** command.
TX Bias Alarm Threshold(mA)	Alarm threshold of the bias current. To set the alarm threshold, run the **optical-module threshold bias** command.
Voltage Alarm Threshold(V)	Alarm threshold of the voltage. To set the alarm threshold, run the **optical-module threshold voltage** command.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

5.19.11 interface pon
5.19.14 optical-module threshold rx-power
5.19.16 optical-module threshold tx-power
5.19.13 optical-module threshold bias
5.19.17 optical-module threshold voltage
5.19.15 optical-module threshold temperature

5.19.5 epon compatibility

Function

The **epon compatibility** command configures the compatibility mode of an EPON interface.

The **undo epon compatibility** command restores the default setting.

By default, the compatibility mode of an EPON interface is not configured.

Format

epon compatibility dba

undo epon compatibility

Parameters

Parameter	Description	Value
dba	Configures an EPON interface to work in dynamic bandwidth assignment (DBA) mode.	-

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device connects to an optical line terminal (OLT) through an EPON interface and the remote OLT sends non-standard DBA packets, you can run this command

 Copyright © Huawei Technologies Co., Ltd.

to set the compatibility mode of the EPON interface to DBA so that the device can process non-standard DBA packets from the remote OLT and transmit services.

Prerequisites

A PON interface has been configured to work in EPON mode.

Precautions

After running the **epon compatibility** command on a device, restart the device to make the configuration take effect.

Example

Set the compatibility mode of an EPON interface to DBA.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] port mode epon
 After you set the work mode of port to a fixed type, you need to interrupt the
service of the up-link port to change the work mode.
 Are you sure to proceed? (y/n)[n]:y
[Huawei-Pon1/0/0] epon compatibility dba
```

Related Topics

5.19.11 interface pon

5.19.18 port mode

5.19.6 epon-checkcode

Function

The **epon-checkcode** command configures an authentication check code on an Ethernet passive optical network (EPON) interface.

Format

epon-checkcode *checkcode*

Parameters

Parameter	Description	Value
checkcode	Specifies a check code used for authentication.	The value is a string of 1 to 12 characters without spaces.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical line terminal (OLT) authenticates validity and identity of each optical network unit (ONU) to prevent unauthorized ONUs.

The **epon-checkcode** command configures logical identifier authentication: The OLT authenticates an ONU by checking the logical identifier (LOID) and check code of the ONU. You can configure the OLT to check only the LOID, or check both the LOID and check code. Logical identifier authentication is applicable to networks requiring flexible access.

NOTE

When logical identifier authentication is used, run the **epon-checkcode** command to configure an LOID for the ONU.

Configuration Impact

If you run the **epon-checkcode** command multiple times in the same view, only the latest configuration takes effect.

Follow-up Procedure

Run the **epon-loid** command to configure an LOID for the ONU when the OLT is configured to check both the LOID and check code.

Precautions

All the authentication parameters are pre-configured on the OLT and cannot be modified on the ONU. Otherwise, the ONU cannot be authenticated.

Example

Set the authentication check code to eponcode on EPON interface PON1/0/0.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] port mode epon
 After you set the work mode of port to a fixed type, you need to interrupt the
service of the up-link port to change the work mode. Are you sure to proceed? (
y/n)[n]:y
[Huawei-Pon1/0/0] epon-checkcode eponcode
```

Related Topics

5.19.11 interface pon

5.19.18 port mode

5.19.7 epon-loid

5.19.1 display epon-info interface pon

5.19.7 epon-loid

Function

Using the **epon-loid** command, you can configure the authentication logical identifier (LOID) on an Ethernet passive optical network (EPON) interface.

Format

epon-loid *loid*

Parameters

Parameter	Description	Value
loid	Specifies the LOID used for authentication.	The value is a string of 1 to 24 characters without spaces.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical line terminal (OLT) authenticates validity and identity of each optical network unit (ONU) to prevent unauthorized ONUs.

The **epon-loid** command configures logical identifier authentication: The OLT authenticates an ONU by checking the logical identifier (LOID) and check code of the ONU. You can configure the OLT to check only the LOID or check both the LOID and check code. Logical identifier authentication is applicable to networks requiring flexible access.

NOTE

When logical identifier authentication is used, run the **epon-loid** command to configure an LOID for the ONU no matter whether the OLT checks only the LOID or checks both the LOID and check code.

Follow-up Procedure

Run the **epon-checkcode** command to configure a check code for the device if the OLT checks both the LOID and check code in authentication.

Precautions

If you run the **epon-loid** command multiple times in the same view, only the latest configuration takes effect.

All the authentication parameters are pre-configured on the OLT and cannot be modified on the ONU. Otherwise, the ONU cannot be authenticated.

Example

Set the LOID to hwloid on EPON interface PON1/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] port mode epon
 After you set the work mode of port to a fixed type, you need to interrupt the
service of the up-link port to change the work mode. Are you sure to proceed? (
y/n)[n]:y
[Huawei-Pon1/0/0] epon-loid hwloid
```

Related Topics

5.19.11 interface pon

5.19.18 port mode

5.19.6 epon-checkcode

5.19.1 display epon-info interface pon

5.19.8 epon-mac-address

Function

Using the **epon-mac-address** command, you can configure the authentication MAC address on an Ethernet passive optical network (EPON) interface.

Format

epon-mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address used for authentication.	The value is in the H-H-H format. H is a hexadecimal number of 4 digits.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical line terminal (OLT) authenticates validity and identity of each optical network unit (ONU) to prevent unauthorized ONUs.

When the OLT uses MAC address authentication, run the **epon-mac-address** command to configure a MAC address for the device. MAC address authentication is applicable to networks requiring high security.

Precautions

All the authentication parameters are pre-configured on the OLT and cannot be modified on the ONU. Otherwise, the ONU cannot be authenticated.

NOTE

The MAC address cannot be changed after the ONU passes the authentication.

Example

Set the configuration MAC address to 0018-8232-6518 on EPON interface PON1/0/0.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] port mode epon
 After you set the work mode of port to a fixed type, you need to interrupt the
service of the up-link port to change the work mode. Are you sure to proceed? (
y/n)[n]:y
[Huawei-Pon1/0/0] epon-mac-address 0018-8232-6518
```

Related Topics

5.19.11 interface pon

5.19.18 port mode

5.19.1 display epon-info interface pon

5.19.9 epon-password

Function

Using the **epon-password** command, you can configure the authentication password on an Ethernet passive optical network (EPON) interface.

Format

epon-password cipher *password*

Parameters

Parameter	Description	Value
password	Specifies the password used for authentication.	The value is a string of 1 to 68 case-sensitive characters without spaces. • The length of a plaintext password ranges from 1 to 32. • The length of a ciphertext password ranges from 32 to 68.

 Copyright © Huawei Technologies Co., Ltd.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical line terminal (OLT) authenticates validity and identity of each optical network unit (ONU) to prevent unauthorized ONUs.

When the OLT uses password authentication, run the **epon-password** command to configure a password for the switch. Password authentication is applicable to networks requiring flexible access.

NOTE

Password authentication is a Huawei proprietary authentication mode. When this mode is used, the OLT must be a Huawei device.

Precautions

If you run the **epon-password** command multiple times in the same view, only the latest configuration takes effect.

All the authentication parameters are pre-configured on the OLT and cannot be modified on the ONU. Otherwise, the ONU cannot be authenticated.

Example

Set the authentication password to hwpwd on EPON interface PON1/0/0.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] port mode epon
 After you set the work mode of port to a fixed type, you need to interrupt the
service of the up-link port to change the work mode. Are you sure to proceed? (
y/n)[n]:y
[Huawei-Pon1/0/0] epon-password cipher hwpwd
```

Related Topics

5.19.11 interface pon

5.19.18 port mode

5.19.1 display epon-info interface pon

5.19.10 gpon-password

Function

Using the **gpon-password** command, you can configure the authentication password on a gigabit passive optical network (GPON) interface.

Format

gpon-password cipher *password*

Parameters

Parameter	Description	Value
password	Specifies the password used for authentication.	The value is a string of 1 to 48 case-sensitive characters without spaces. • The length of a plaintext password ranges from 1 to 10. • The length of a ciphertext password is 48.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical line terminal (OLT) authenticates validity and identity of each optical network unit (ONU) to prevent unauthorized ONUs. A GPON system supports the following ONU authentication modes:

The device supports the SN authentication mode by default.

Table 5-70 lists the comparison of ONU authentication modes in a GPON system.

 Copyright © Huawei Technologies Co., Ltd.

Table 5-70 Comparison of ONU authentication modes in a GPON system

Authentication Mode	Description	Advantage	Disadvantage	Usage Scenario
SN authentication	The OLT authenticates an ONU by checking the SN of the ONU. The SN of each ONU is a globally unique string of 13 characters. The first four characters represent the manufacturer. The SN of a Huawei ONU starts with hwhw.	This mode does not require any manual configuration and has a high reliability.	When an ONU fails and needs to be replaced by a new one, the SN of the new ONU must be added to the OLT, so this mode is not flexible.	It is applicable to all scenarios because the device supports this mode by default.

 Copyright © Huawei Technologies Co., Ltd.

Authentication Mode	Description	Advantage	Disadvantage	Usage Scenario
Password authentication	The OLT authenticates an ONU by checking whether the password sent by the ONU is the same as that configured locally.	It is simple to configure and you do not need to configure new passwords when users change their physical locations. This mode implements flexible access.	When two ONUs use the same password, the OLT allows the one that passes the authentication earlier to go online. Therefore, if an unauthorized ONU has gone online by using the password of an authorized ONU, the authorized ONU cannot go online.	It is applicable to networks requiring flexible access.

A GPON system supports the following ONU authentication modes: only by serial number (SN), only by password, or by SN and password. When a GPON system authenticates the ONU by checking the password or checking the SN and password, you must run this command to configure a password for the GPON.

Configuration Impact

If you run the **gpon-password** command multiple times in the same view, only the latest configuration takes effect.

Precautions

All the authentication parameters are pre-configured on the OLT and cannot be modified on the ONU. Otherwise, the ONU cannot be authenticated.

Example

Set the authentication password to huawei on GPON interface PON1/0/0.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] port mode gpon
 After you set the work mode of port to a fixed type, you need to interrupt the
service of the up-link port to change the work mode. Are you sure to proceed? (
y/n)[n]:y
[Huawei-Pon1/0/0] gpon-password cipher huawei
```

Related Topics

5.19.11 interface pon

5.19.18 port mode

5.19.2 display gpon-info interface pon

5.19.11 interface pon

Function

Using the **interface pon** command, you can enter the passive optical network (PON) interface view and create a PON sub-interface.

Format

interface pon *interface-number*

interface pon *interface-number.subinterface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a PON interface. The value is in slot ID/subcard ID/interface sequence number format.	Values of the fields are: • The subcard ID is 0. • The interface sequence number is 0 or 1. **NOTE** • When the sequence number of a PON interface is 0, services are configured on this interface. • When the sequence number of a PON interface is 1, this interface functions as a backup interface. In most cases, no service is configured on this interface.
subinterface-number	Specifies the number of a PON sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To configure attributes of a PON interface or a PON sub-interface, you need to use this command to enter the PON interface view or PON sub-interface view.

Example

Enter the view of PON1/0/0.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0]
```

Create and enter PON1/0/0.1

```
<Huawei> system-view
[Huawei] interface pon 1/0/0.1
[Huawei-Pon1/0/0.1]
```

Related Topics

5.19.4 display pon-transceiver interface pon

5.19.12 laser

Function

Using the **laser** command, you can configure the laser working mode of the optical module on a passive optical network (PON) interface.

The default laser working mode is **auto**.

Format

laser { **auto** | **off** | **on** [*time-value*] }

Parameters

Parameter	Description	Value
auto	Indicates that the optical module generates optical signals when data needs to be transmitted and stops generating optical signals when no data needs to be transmitted.	-
off	Indicates that the optical module does not generate optical signals.	-
on	Indicates that the optical module continuously generates optical signals.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-value	Specifies the period during which the optical module generates optical signals.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 20.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- The auto mode is used when a PON interface needs to transmit data.
- The off mode is used when a PON interface does not need to transmit data in a long time.
- The on mode is used when the transmit power of the optical module needs to be tested.

Precautions

- If you run the **laser** command multiple times in the same view, only the latest configuration takes effect.
- Before setting the laser working mode on a PON interface to off, ensure that the PON interface does not need to transmit any service data. Otherwise, services on the interface will be interrupted.
- When setting the laser working mode to on, you can set the *time-value* parameter. The optical module generates optical signals within the specified period. After this period, the optical module works in auto mode. If this parameter is not set, the optical module starts to work in auto mode after 20 seconds.
- When a PON interface works in GPON mode, the laser working mode cannot be directly changed from off to on. You must change the laser working mode to auto, and then change it to on.

Example

Configure the optical module on PON1/0/0 to continuously generate optical modules for 30 seconds.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] laser on 30
```

Related Topics

5.19.11 interface pon

5.19.4 display pon-transceiver interface pon

5.19.13 optical-module threshold bias

Function

Using the **optical-module threshold bias** command, you can set the lower and upper alarm thresholds of the bias current for the optical module on a passive optical network (PON) interface.

Format

optical-module threshold bias { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }*

Parameters

Parameter	Description	Value
lower-limit *lower-limit*	Specifies the lower alarm threshold of the bias current.	The value is an integer that ranges from 0 mA to 10000 mA. The recommended value is 2.
upper-limit *upper-limit*	Specifies the upper alarm threshold of the bias current.	The value is an integer that ranges from 0 mA to 10000 mA. The recommended value is 70.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical module can work properly when the bias current is in the range of 0 mA to 10000 mA. If the bias current is out of this range, the optical module may fail to receive optical signals. As a result, the optical network unit (ONU) is forced offline and services on the ONU are interrupted. The **optical-module threshold bias** command sets the lower and upper alarm thresholds of the bias current. When the bias current is out of the specified range, the ONU sends a trap to the NMS.

Precautions

If you run the **optical-module threshold bias** command multiple times in the same view, only the latest configuration takes effect.

The lower alarm threshold must be smaller than or equal to the upper alarm threshold.

Example

Set the lower alarm threshold of the bias current to 5 mA and the upper alarm threshold to 50 mA.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] optical-module threshold bias lower-limit 5 upper-limit 50
```

Related Topics

5.19.11 interface pon

5.19.4 display pon-transceiver interface pon

5.19.14 optical-module threshold rx-power

Function

Using the **optical-module threshold rx-power** command, you can set the lower and upper alarm thresholds of the receiving optical power for the optical module on a passive optical network (PON) interface.

Format

optical-module threshold rx-power { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }*

Parameters

Parameter	Description	Value
lower-limit	Specifies the lower alarm threshold of the receiving optical power.	The value is a floating point number, accurate to the second decimal place. The value ranges from -99.00 dBm to 100.00 dBm. The recommended value is -35.00.
upper-limit	Specifies the upper alarm threshold of the receiving optical power.	The value is a floating point number, accurate to the second decimal place. The value ranges from -99.00 dBm to 100.00 dBm. The recommended value is 1.00.

 Copyright © Huawei Technologies Co., Ltd.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical module can work properly when the receiving optical power is in the range of -99.00 dBm to 100.00 dBm. If the receiving optical power is out of this range, the optical module may fail to receive optical signals. As a result, the optical network unit (ONU) is forced offline and services on the ONU are interrupted. The **optical-module threshold rx-power** command sets the lower and upper alarm thresholds of the receiving optical power. When the receiving optical power is out of the specified range, the ONU sends a trap to the NMS.

Precautions

If you run the **optical-module threshold rx-power** command multiple times in the same view, only the latest configuration takes effect.

The lower alarm threshold must be smaller than or equal to the upper alarm threshold.

Example

Set the lower alarm threshold of the receiving optical power to -25 dBm and set the upper alarm threshold to 50 dBm.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] optical-module threshold rx-power lower-limit -25 upper-limit 50
```

Related Topics

5.19.11 interface pon

5.19.4 display pon-transceiver interface pon

5.19.15 optical-module threshold temperature

Function

The **optical-module threshold temperature** command sets the lower and upper alarm thresholds of the temperature for the optical module on a passive optical network (PON) interface.

Format

optical-module threshold temperature { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }*

Parameters

Parameter	Description	Value
lower-limit	Specifies the lower alarm threshold of the temperature.	The value is a floating point number, accurate to the second decimal place. The value ranges from -99.00°C to 300.00°C. The recommended value is -10.
upper-limit	Specifies the upper alarm threshold of the temperature.	The value is a floating point number, accurate to the second decimal place. The value ranges from -99.00°C to 300.00°C. The recommended value is 100.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical module can work properly when the temperature is in the range of -99.00°C to 300.00°C. If the temperature is out of this range, the optical module may fail to receive optical signals. As a result, the optical network unit (ONU) is forced offline and services on the ONU are interrupted. The **optical-module threshold temperature** command sets the lower and upper alarm thresholds of the temperature. When the temperature is out of the specified range, the ONU sends a trap to the NMS.

Precautions

If you run the **optical-module threshold temperature** command multiple times in the same view, only the latest configuration takes effect.

The lower alarm threshold must be smaller than or equal to the upper alarm threshold.

Example

Set the lower alarm threshold of the temperature to 5°C and the upper alarm threshold to 25°C.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] optical-module threshold temperature lower-limit 5 upper-limit 25
```

Related Topics

5.19.11 interface pon

5.19.4 display pon-transceiver interface pon

5.19.16 optical-module threshold tx-power

Function

Using the **optical-module threshold tx-power** command, you can set the lower and upper alarm thresholds of the transmitting optical power for the optical module on a passive optical network (PON) interface.

Format

optical-module threshold tx-power { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }*

Parameters

Parameter	Description	Value
lower-limit	Specifies the lower threshold of the transmitting optical power.	The value is a floating point number, accurate to the second decimal place. The value ranges from -99.00 dBm to 100.00 dBm. The recommended value is -1.00.
upper-limit	Specifies the upper threshold of the transmitting optical power.	The value is a floating point number, accurate to the second decimal place. The value ranges from -99.00 dBm to 100.00 dBm. The recommended value is 7.00.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical module can work properly when the transmitting optical power is in the range of -99.00 dBm to 100.00 dBm. If the transmitting optical power is out of this range, the optical module may fail to receive optical signals. As a result, the optical network unit (ONU) is forced offline and services on the ONU are interrupted. The **optical-module threshold tx-power** command sets the lower and upper alarm thresholds of the transmitting optical power. When the transmitting optical power is out of the specified range, the ONU sends a trap to the NMS.

Precautions

If you run the **optical-module threshold tx-power** command multiple times in the same view, only the latest configuration takes effect.

The lower alarm threshold must be smaller than or equal to the upper alarm threshold.

Example

Set the lower alarm threshold of the transmitting optical power to -25 dBm and set the upper alarm threshold to 50 dBm.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] optical-module threshold tx-power lower-limit -25 upper-limit 50
```

Related Topics

5.19.11 interface pon

5.19.4 display pon-transceiver interface pon

5.19.17 optical-module threshold voltage

Function

Using the **optical-module threshold voltage** command, you can set the lower and upper alarm thresholds of the voltage for the optical module on a passive optical network (PON) interface.

Format

optical-module threshold voltage { **lower-limit** *lower-limit* | **upper-limit** *upper-limit* }*

Parameters

Parameter	Description	Value
lower-limit	Specifies the lower alarm threshold of the voltage.	The value is a floating point number, accurate to the second decimal place. The value ranges from 0 V to 100.00 V. The recommended value is 2.97.
upper-limit	Specifies the upper alarm threshold of the voltage.	The value is a floating point number, accurate to the second decimal place. The value ranges from 0 V to 100.00 V. The recommended value is 3.63.

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An optical module can work properly when the voltage is in the range of 0 V to 100.00 V. If the voltage is out of this range, the optical module may fail to receive optical signals. As a result, the optical network unit (ONU) is forced offline and services on the ONU are interrupted. The **optical-module threshold voltage** command sets the lower and upper alarm thresholds of the voltage. When the voltage is out of the specified range, the ONU sends a trap to the NMS.

Precautions

If you run the **optical-module threshold voltage** command multiple times in the same view, only the latest configuration takes effect.

The lower alarm threshold must be smaller than or equal to the upper alarm threshold.

Example

Set the lower alarm threshold of the voltage to 5 V and the upper alarm threshold to 25 V.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] optical-module threshold voltage lower-limit 5 upper-limit 25
```

Related Topics

5.19.11 interface pon

5.19.4 display pon-transceiver interface pon

5.19.18 port mode

Function

Using the **port mode** command, you can configure the working mode of an Ethernet passive optical network (PON) interface.

By default, a PON interface works in auto-sensing mode.

Format

port mode { **adapt** | **gpon** | **epon** }

Parameters

Parameter	Description	Value
adapt	Indicates that the PON interface automatically determines the working mode according to the received optical signals. **NOTE** In auto-negotiation mode, the PON interface of the device can work in EPON or GPON mode automatically according to the received optical signal. You are advised to configure a PON interface to work in auto-negotiation mode. To trigger another negotiation after a successful negotiation, reset the PON board. For example, if a PON interface of the device has automatically negotiated to work in EPON mode, you need to reset the PON board so that this interface can automatically negotiate to work in GPON mode when this interface connects to an OLT's PON interface that works in GPON mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
gpon	Indicates that the PON interface works in gigabit PON (GPON) mode.	-
epon	Indicates that the PON interface works in Ethernet PON (EPON) mode.	-

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PON interface of the device is connected to an optical line terminal (OLT), the PON interface must work in the same mode as the remote PON interface of the OLT. You can configure the PON interface to work in EPON or GPON mode according to the working mode of the remote PON interface. Alternatively, you can configure the PON interface to work in auto-sensing mode so that it determines the working mode according to the received optical signals.

Precautions

If you run the **port mode** command multiple times in the same view, only the latest configuration takes effect.

If a PON interface is transmitting service data, changing the working mode will interrupt services on the PON interface. Run this command with caution.

A PON interface does not support switching between the EPON and GPON modes. You must change the a PON interface to the auto-negotiation mode, and then switch it to EPON or GPON.

NOTE

The interval between two mode switches cannot be less than 30 seconds. If it is less than 30 seconds, the device will generate incorrect information.

Example

Configure PON1/0/0 to work in GPON mode.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] port mode gpon
```

```
 After you set the work mode of port to a fixed type, you need to interrupt the
service of the up-link port to change the work mode. Are you sure to proceed? (
y/n)[n]:y
```

Related Topics

5.19.11 interface pon

5.19.19 reset pon-statistic interface pon

Function

Using the **reset pon-statistic interface pon** command, you can clear traffic statistics on a passive optical network (PON) interface.

Format

reset pon-statistic interface pon *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a PON interface.	-

Views

User view, System view

Default Level

2: Configuration level

Usage Guidelines

Before collecting traffic statistics on a PON interface in a certain period, you must run the **reset pon-statistic interface pon** command to clear the previous statistics.

Example

Clear traffic statistics on PON1/0/0.

```
<Huawei> system-view
[Huawei] reset pon-statistic interface pon 1/0/0
```

Related Topics

5.19.3 display pon-statistic interface pon

5.19.20 undo optical-module threshold

Function

Using the **undo optical-module threshold** command, you can remove all configured alarm thresholds for the optical module.

Format

undo optical-module threshold

Parameters

N/A

Views

PON interface view

Default Level

2: Configuration level

Usage Guidelines

To remove all lower and upper alarm thresholds of the bias current, receiving optical power, transmitting optical power, voltage, or temperature are configured, you can use this command. After all configured alarm thresholds of the device are removed, the ONU will not send alarms to network management devices when the bias current, receiving optical power, transmitting optical power, voltage, or temperature is too high or too low.

Example

Remove all configured alarm thresholds.

```
<Huawei> system-view
[Huawei] interface pon 1/0/0
[Huawei-Pon1/0/0] undo optical-module threshold
```

Related Topics

5.19.11 interface pon

5.20 Logical Interface Configuration Commands

5.20.1 broadcast-limit link

Function

Using the **broadcast-limit link** command, you can set the maximum number of links for sending multicast or broadcast packets supported by a virtual template interface.

Using the **undo broadcast-limit link** command, you can restore the default setting.

By default, the maximum number of links for sending multicast or broadcast packets supported by a virtual template interface is 30.

Format

broadcast-limit link *number*

undo broadcast-limit link

Parameters

Parameter	Description	Value
number	Specifies the maximum number of links for sending multicast or broadcast packets supported by a virtual template interface.	The value ranges from 0 to 128. You are advised to use the default value.

Views

VT interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the number of links configured on a virtual template interface is large, system performance deteriorates when multicast or broadcast packets need to be sent over each link. To solve the problem, you can run the **broadcast-limit link** command to set the maximum number of links supported by the virtual template interface.

Precautions

When the number of links exceeds the maximum value, multicast or broadcast packets are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum number of links for sending multicast or broadcast packets supported by the virtual template interface 1 to 30.

```
<Huawei> system-view
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] broadcast-limit link 30
```

Related Topics

5.20.6 display interface virtual-template

5.20.2 display interface loopback

Function

Using the **display interface loopback** command, you can view the status of a loopback interface.

Format

display interface loopback [*loopback-number*]

Parameters

Parameter	Description	Value
loopback-number	Specifies the number of a loopback interface. If *loopback-number* is not specified, the status of all loopback interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where you need to monitor the status of an interface or locate an interface fault, you can use the **display interface loopback** command to collect the statistics on the interface including the status. Through the displayed information, you can collect the traffic statistics and troubleshoot the interface.

Example

Display the status of a specified loopback interface.

```
<Huawei> display interface loopback 6
LoopBack6 current state : UP
Line protocol current state : UP (spoofing)
```

 Copyright © Huawei Technologies Co., Ltd.

```
Description:HUAWEI, AR Series, LoopBack6 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.10.1.1/32
Physical is Loopback
Current system time: 2012-05-28 11:20:08
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 0 bytes
   Output:0 bytes
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
```

Table 5-71 Description of the display interface loopback command output

Item	Description
LoopBack6 current state	Physical status of the loopback interface. After a loopback interface is created, the physical status keeps Up.
Line protocol current state	Link layer protocol status of the interface. After a loopback interface is created, the status of the link layer protocol keeps Up.
Description	Description of the interface. Up to 242 case-sensitive characters (including spaces) can be entered. The description helps you to know the functions of the interface.
The Maximum Transmit Unit is	Maximum transmission unit (MTU). The default MTU is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
Internet Address is	IP address of the interface.
Physical is Loopback	Information about the link at the physical layer.
Current system time	Current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Last 300 seconds input rate Last 300 seconds output rate	Average rates at which the interface sends and receives packets and bytes in the last five minutes. You can run the **set flow-stat interval** command to change the interval at which traffic statistics are collected.

Item	Description
Realtime 2 seconds input rate Realtime 2 seconds output rate	Real-time rates at which the interface sends and receives packets and bytes within 2 seconds. It refers to the interval between two **display** commands that are run on the same interface. The maximum value is the statistical interval displayed in the previous piece of information. This entry is displayed only when information about a logical interface is viewed.
Input	Total number of packets and the total number of bytes received by the interface.
Output	Total number of packets and the total number of bytes sent by the interface.
Input bandwidth utilization	Percentage of the packet receiving to the total bandwidth.
Output bandwidth utilization	Percentage of the packet sending rate to the total bandwidth.

Related Topics

5.20.10 interface loopback

5.20.3 display interface null

Function

Using the **display interface null** command, you can view the status of a null interface.

Format

display interface null [**0**]

Parameters

Parameter	Description	Value
0	Specifies the number of the null interface.	The value can be 0 only.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display interface null** command displays the status of a null interface. The interface status information includes: the physical status, link layer protocol status, description, MTU, IP address, current system time, last time statistics about the null interface are cleared, incoming and outgoing packet rates in bit/s and pps, total numbers of packets and bytes received and sent by the null interface, and percentages of the rates for receiving and sending packets to the total bandwidth.

Precautions

There is only one null interface, namely, NULL 0.

Example

Display the status of Null 0 interface.

```
<Huawei> display interface null 0
NULL0 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, NULL0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Physical is NULL DEV
Current system time: 2012-08-28 15:09:56
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 2 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 2 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 bytes
    Output:0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-72 Description of the display interface null command output

Item	Description
NULL0 current state	Physical status of the null interface. The physical status of the null interface remains Up.
Line protocol current state	Link layer protocol status of the null interface. The link layer protocol status of the null interface remains Up.
Description	Description of the interface. Up to 242 case-sensitive characters (including spaces) can be entered. The description helps know the functions of the interface.
The Maximum Transmit Unit is	Maximum transmission unit (MTU). The value is 1500 bytes.
Internet protocol processing : disabled	No IP address is assigned to the interface.
Physical is NULL DEV	The interface does not exist physically.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current system time	Current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Last 300 seconds input rate Last 300 seconds output rate	Rates for sending and receiving the bytes and the packets by the interface in the last five minutes.
Realtime 2 seconds input rate Realtime 2 seconds output rate	Real-time rates of sending and receiving the bytes and the packets within 2 seconds. It refers to the interval between two **display** commands that are run on the same interface. The maximum value is the statistical interval displayed in the previous piece of information. This entry is displayed only when information about a logical interface is viewed.
Input	Total number of packets and total number of bytes received by the interface.
Output	Total number of packets and total number of bytes sent by the interface.
Input bandwidth utilization	Percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Percentage of the rate for sending packets to the total bandwidth.

Related Topics

5.20.11 interface null

5.20.4 display interface virtual-ethernet

Function

The **display interface virtual-ethernet** command displays the status of a virtual Ethernet (VE) interface.

If no interface number is specified, information about all VE interfaces is displayed.

Format

display interface virtual-ethernet [*ve-number*]

Parameters

Parameter	Description	Value
ve-number	Specifies the number of a VE interface. The interface number consists of the slot ID, card number, and sequence number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display interface virtual-ethernet** command displays the status of a VE interface, including the current physical status, link layer protocol status, last time the link layer protocol status goes Up, description, MTU, IP address, frame format, maximum QoS bandwidth, output queue status, and current system time.

Example

Display the status of VE 0/0/0.

```
<Huawei> display interface virtual-ethernet 0/0/0
Virtual-Ethernet0/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Virtual-Ethernet0/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing: 10.1.1.1/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0000-0000-0000
Current system time: 2010-09-07 15:27:28
    Input bandwidth utilization  : 0%
    Output bandwidth utilization : 0%
```

Table 5-73 Description of the display interface virtual-Ethernet command output

Item	Description
Virtual-Ethernet0/0/0 current state	Physical status of the VE interface: • UP: indicates that the interface works properly. • DOWN: indicates that the physical connection of the interface is Down. • Administratively down: indicates that the administrator has run the **shutdown** command on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol on the interface is Up. ● DOWN: indicates that the link layer protocol on the interface is Down or no IP address is assigned to the interface.
Description	Description of the interface. A maximum of 242 case-sensitive characters (including spaces) can be entered. The description helps know the functions of the interface.
The Maximum Transmit Unit is	MTU of the interface. The default value of the MTU is 1500 bytes on a serial interface. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
Internet protocol processing : disabled	No IP address is assigned to the interface, the information is displayed as "Internet protocol processing : disabled ". If an IP address is assigned to the interface, the IP address and subnet mask are displayed.
IP Sending Frames' Format is	Frame format of the sent IP packets.
Current system time:	Current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Input bandwidth utilization	Percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Percentage of the rate for sending packets to the total bandwidth.

Related Topics

5.20.12 interface virtual-ethernet

5.20.5 display virtual-access

Function

The **display virtual-access** command displays the virtual access interface status.

Format

display virtual-access [**vt** *vt-number* | **dialer** *dialer-interface-number* | **user** *user-name* | **peer** *peer-address* | *va-number*]*

Parameters

Parameter	Description	Value
vt *vt-number*	Specifies the number of the VT interface bound to the VA interface.	The value is an integer that ranges from 0 to 1023.
dialer *dialer-interface-number*	Specifies the number of the dialer interface bound to the VA interface.	The value is an integer and the value depend on the device.
user *user-name*	Specifies the user name for logging in to the VA interface.	The value is a string of 1 to 64 case-sensitive characters without spaces.
peer *peer-address*	Specifies the IP address of the peer device connected to the VA interface.	The value is in dotted decimal notation.
va-number	Specifies the number of the VA interface.	The value is an integer that ranges from 0 to 1023.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A VA interface is generated after the VT interface is instantiated. A VA interface is generated for one PPP connection. For example, a VA interface is generated for a PPPoE session or a PPPoFR connection.

Whether multiple VA interfaces can be generated on a VT interface depends on the MP binding mode. For details, see the **ppp mp binding-mode** command.

When monitoring the interface status or locating faults on an interface, you can run the **display virtual-access** command to obtain the status of and statistics on the interface.

If no parameter is specified, the status of all VT interfaces are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the status of all VA interfaces when a VA interface is generated on a VT interface.

```
<Huawei> display virtual-access
Virtual-Template1:0 current state : UP
Line protocol current state : UP
Last line protocol up time : 2012-07-18 10:54:39
Description:HUAWEI, AR Series, Virtual-Template1:0 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened
Physical is IPCP
Current system time: 2012-07-18 10:56:28
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 bytes
    Output:0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 5-74 Description of the display virtual-access command output

Item	Description
Virtual-Template1:0 current state	Virtual-Template interface status: ● UP: indicates that the physical status of the interface is Up. ● DOWN: indicates that the physical status of the interface is Down. In this field, the number following Virtual-Template indicates "VT interface number:VA interface number". For example, 1:0 indicates that the VT interface number is 1 and VA interface number is 0.
Line protocol current state	Link layer protocol status of the interface: ● UP: indicates that the link layer protocol status of the interface is Up. ● DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface.
Last line protocol up time	Last time the link layer protocol of the interface goes Up.
Description	Interface description.
The Maximum Transmit Unit is	Maximum Transmission Unit (MTU) of the interface. The default MTU on a serial interface is 1480 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is enabled, the packets are discarded.
Hold timer is	Lifecycle of a packet. If a packet is not sent out before the hold timer times out, the packet is discarded.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Link layer protocol is	Link layer protocol type.
LCP	Status of the Link Control Protocol (LCP). The LCP status is as follows: ● Initial: indicates that the physical layer is unavailable. ● Starting: indicates that the physical layer is starting. The device retains in Starting state for a short time. ● Closed: indicates that the device sends a Terminate-Ack packet to terminate the connection after receiving the Configure-Request packet. ● Stopped: indicates that the device receives the Configure-Request packet, but does not receive a Configure-Ack packet from the peer device. In this case, the device sends a Terminate-Ack packet. ● Closing: indicates that the connection is being closed. The device enters the Closed state if the device receives a Configure-Ack packet from the peer device or the timer expires. The device retains in Closing state for a short time. ● Stopping: indicates that the connection is being closed to prevent subsequent traffic transmission. The device retains in Stopping state for a short time. ● Req-Sent: indicates an attempt to establish a connection. The device sends a Configure-Request packet, but does not receive a Configure-Ack packet from the peer device. ● Ack-Rcvd: indicates that the device sends a Configure-Request packet and receives a Configure-Ack packet from the peer device but does not receive a Configure-Ack packet to the peer device. ● Ack-Sent: indicates that the device sends a Configure-Request packet and a Configure-Ack packet to the peer device and receives a Configure-Ack packet from the peer device. ● Opened: indicates that the device sends a Configure-Ack packet to the peer device and receives a Configure-Ack packet from the peer device. The link layer works properly.
MP	MP link status. If the MP link is in Opened state, the MP link works properly. The MP link is in Opened state only when the LCP status of all member links in the MP link is Opened.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPCP	Internet Protocol Control Protocol (IPCP) status of the MP link. If IPCP is in Opened state, the MP link works properly. The IPCP status of the MP link is Opened only when the IPCP status of the primary link in the MP link is Opened.
Current system time	Current system time. If the time zone is configured and system time uses the daylight-saving-time (DST). The time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Realtime 0 seconds input rate	Rate of packets received when this command is being executed.
Realtime 0 seconds output rate	Rate of packets sent when this command is being executed.
Input	Total number of received packets.
Output	Total number of sent packets.
Input bandwidth utilization	Inbound bandwidth usage.
Output bandwidth utilization	Outbound bandwidth usage.

Related Topics

7.3.8 ppp mp binding-mode

5.20.6 display interface virtual-template

Function

Using the **display interface virtual-template** command, you can view the status of a virtual template (VT) interface.

Format

display interface virtual-template [*vt-number*]

Parameters

Parameter	Description	Value
vt-number	Displays the status of the specified VT interface. If no VT number is specified, the status of all VT interfaces is displayed.	The value is an integer that ranges from 0 to 1023.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display interface virtual-template** command displays the status of a VT interface, including the current physical status, link layer protocol and its status, IP address, description, output queue status, incoming and outgoing packet rates in bit/s and pps, total numbers of packets and bytes received and sent by the VT interface, and percentages of the rates for receiving and sending packets to the total bandwidth.

Example

Display the status of a specified VT interface.

```
<Huawei> display interface virtual-template 1
Virtual-Template1 current state : UP
Line protocol current state :UP (spoofing)Description:HUAWEI, AR Series, Virtual-Template1 InterfaceRoute
Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.1/24
Link layer protocol is PPP
LCP initial, MP opened
Physical is None, baudrate is 64000 bps
Current system time: 2007-09-06 20:57:31
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 0 bytes
   Output:0 bytes
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
```

Table 5-75 Description of the display interface virtual-template command output

Item	Description
Virtual-Template1 current state	Physical status of the VT interface: ● UP: indicates that the interface works properly.

Item	Description
Line protocol current state	Link layer protocol status of the interface: ● UP (spoofing): indicates that the link layer protocol of the interface is always Up with the spoofing feature enabled.
Link layer protocol is	Link layer protocol.
Internet Address is	IP address assigned to the interface. If no IP address is assigned to the interface, "Internet protocol processing : disabled" is displayed.
LCP initial,, MP opened	Indicates the status of LCP.
Description	Description of the interface. A maximum of 242 case-sensitive characters (including spaces) can be entered. The description helps you to know the functions of the interface.
The Maximum Transmit Unit is	MTU of the interface. The default value of the MTU is 1500 bytes on a serial interface. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
Physical is None	No physical interface exists. Logical interfaces do not exist physically.
Current system time	Current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Last 300 seconds input rate Last 300 seconds output rate	Rates of the bytes and the packets that the interface sends and receives in the last 300 seconds.
Realtime 2 seconds input rate Realtime 2 seconds output rate	Real-time rates of sending and receiving the bytes and the packets within 2 seconds. It refers to the interval between two **display** commands that are run on the same interface. The maximum value is the statistical interval displayed in the previous piece of information. This entry is displayed only when information about a logical interface is viewed.
Input	Total number of packets and total number of bytes received by the interface.
Output	Total number of packets and total number of bytes sent by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input bandwidth utilization	Percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Percentage of the rate for sending packets to the total bandwidth.

Related Topics

5.20.13 interface virtual-template

5.20.7 mac-address (Virtual-Ethernet interface view)

Function

The **mac-address** command configures a MAC address for the Virtual-Ethernet interface.

The **undo mac-address** command deletes the MAC address that is configured for the Virtual-Ethernet interface.

By default, the MAC address of the Virtual-Ethernet interface is the system MAC address.

NOTE

Only Layer 3 VE interfaces support this command.

Format

mac-address *mac-address*

undo mac-address

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address of a Virtual-Ethernet interface.	The MAC address is in the format of H-H-H. H is a hexadecimal number that contains one to four digits, such as 00e0 and fc01. If an H contains less than four digits, 0s are padded ahead. For example, if you specify an H as e0, it is displayed as 00e0. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.

Views

Virtual-Ethernet interface view, Virtual-Ethernet sub-interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MAC address of a Virtual-Ethernet interface is the system MAC address, and may conflict with the MAC address of another interface (a physical or logical interface). If the MAC address of the Virtual-Ethernet interface conflicts with that of another interface, a loop probably occurs or traffic forwarding on the Virtual-Ethernet interface may fail.

In this case, you must run the **mac-address** command to configure a MAC address for the Virtual-Ethernet interface to guarantee the normal transmission of service data flows.

Configuration Impact

After the MAC address of the Virtual-Ethernet interface is changed, the device sends gratuitous ARP packets to the remote device so that the remote device can refresh its ARP entries.

Example

Configure a MAC address for VE 0/0/1.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] mac-address 0001-2345-abcd
```

Related Topics

5.20.4 display interface virtual-ethernet

5.20.8 mtu

Function

The **mtu** command sets the maximum transmission unit (MTU) of an interface.

The **undo mtu** command restores the default MTU of an interface.

By default, the MTU of an interface is 1500 bytes.

Format

mtu *size*

undo mtu

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
size	Specifies the MTU of an interface.	The value is an integer that ranges from 128 to 1500, in bytes.

Views

Virtual template interface view, dialer interface view, MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IP layer limits the size of a packet sent each time. Any time the IP layer receives an IP packet, it checks to which local interface the packet needs to be sent and obtains the MTU of the interface. Then, the IP layer compares the MTU with the packet size. If the packet size is larger than the MTU, the IP layer disassembles the packet to fragments smaller than the MTU.

If forcible unfragmentation is configured, oversized packets are discarded at the IP layer. To prevent packet loss on the network, oversized packets must be forcibly fragmented. You can run the **mtu** command to set the size of a fragment.

Precautions

After running the **mtu** command on an interface, restart the interface to make the configured MTU take effect.

You can restart an interface by using the following methods:

- Run the **shutdown** command and then the **undo shutdown** command.
- Run the **restart** command.

NOTE

The device does not support restart of a virtual template interface.

Example

Set the MTU of Virtual-template 10 to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface virtual-template 10
[Huawei-Virtual-Template10] mtu 1200
[Huawei-Virtual-Template10] restart
```

5.20.9 interface (FR sub-interface)

Function

Using the **interface** command, you can create a sub-interface on the interface whose link layer protocol is FR.

Using the **undo interface** command, you can delete a sub-interface from the interface whose link layer protocol is FR.

Format

interface *interface-type interface-number.subinterface-number* [**p2mp** | **p2p**]

undo interface *interface-type interface-number.subinterface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface whose link layer protocol is FR. **NOTE** The E1, T1, CE1/PRI, CT1/PRI, E1–F, T1–F, CPOS, ISDN BRI, or SA interface can configure the link layer protocol as frame relay.	-
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 1024.
p2mp	Sets the network type of a sub-interface to P2MP. P2MP is the default sub-interface network type when the link layer protocol of a main interface is FR.	-
p2p	Sets the network type of a sub-interface to P2P.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Sub-interfaces are logical (virtual) interfaces configured on a main interface. Sub-interfaces can share physical parameters of their main interface or be configured

with their respective link layer parameters and network layer parameters. The sub-interface status change does not affect the main interface status, but the main interface status change affects the status of sub-interfaces. Sub-interfaces work properly only when their main interface is in the Up state.

To implement various services such as MPLS and VPN services on an interface whose link layer protocol is FR, you can configure these services on different sub-interfaces of the interface.

Prerequisites

The link layer protocol of the main interface is FR.

Precautions

When a main interface is configured with a sub-interface, the interval between running the **shutdown** and **undo shutdown** commands on the main interface must be at least 15 seconds.

Example

Create sub-interface Serial2/0/0.1.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0.1
[Huawei-Serial2/0/0.1]
```

Related Topics

5.1.16 shutdown (interface view)

5.20.10 interface loopback

Function

The **interface loopback** command creates a loopback interface.

The **undo interface loopback** command deletes a loopback interface.

Format

interface loopback *loopback-number*

undo interface loopback *loopback-number*

Parameters

Parameter	Description	Value
loopback-number	Specifies the number of a loopback interface.	The VE sequence number range depends on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A loopback interface is always Up at the physical layer and link layer unless it is manually shut down.

The IP address of a loopback interface is usually specified as the source address of packets.

Example

Create loopback interface 5.

```
<Huawei> system-view
[Huawei] interface loopback 5
[Huawei-LoopBack5]
```

Related Topics

5.20.2 display interface loopback

5.20.11 interface null

Function

Using the **interface null** command, you can enter the null interface view.

Format

interface null 0

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Null0 interface never forwards or accepts any traffic. All traffic sent to this interface is directly discarded. Unnecessary traffic can be sent to the Null0 interface to avoid using ACLs.

Precautions

There is only one null interface, named null0. This interface is always Up and cannot be shut down or deleted.

Example

Enter the view of the Null0 interface.

```
<Huawei> system-view
[Huawei] interface null 0
[Huawei-NULL0]
```

Related Topics

5.20.3 display interface null

5.20.12 interface virtual-ethernet

Function

Using the **interface virtual-ethernet** command, you can create a virtual Ethernet (VE) interface.

Using the **undo interface virtual-ethernet** command, you can delete a VE interface.

Format

interface virtual-ethernet *ve-number*

undo interface virtual-ethernet *ve-number*

Parameters

Parameter	Description	Value
ve-number	Specifies the number of a VE interface, in the format of slot number/card number/sequence number. The card number can be the number of an absent card.	The VE sequence number range depends on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VE interface is a logical interface that has Ethernet features. When PPPoE packets or IPoE packets need to be transmitted over an ATM network, a VE

interface is required to implement interworking between PPPoE and ATM, or between IPoE and ATM.

Precautions

VE sub-interfaces can be created only after the VE main interface is created. The value of the VE sub-interface number ranges from 1 to 1024.

If a VE interface is bound to a physical interface, you must unbind the VE interface from the physical interface before deleting the VE interface.

Example

Create a VE interface 0/0/12.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/12
[Huawei-Virtual-Ethernet0/0/12]
```

Create a VE sub-interface 0/0/12.1.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/12
[Huawei-Virtual-Ethernet0/0/12] quit
[Huawei] interface virtual-ethernet 0/0/12.1
[Huawei-Virtual-Ethernet0/0/12.1]
```

Related Topics

5.20.4 display interface virtual-ethernet

5.20.13 interface virtual-template

Function

Using the **interface virtual-template** command, you can create a virtual template (VT) interface and enter the VT interface view.

Using the **undo interface virtual-template** command, you can delete a VT interface.

Format

interface virtual-template *vt-number*

undo interface virtual-template *vt-number*

Parameters

Parameter	Description	Value
vt-number	Specifies the number of a VT interface.	The VE sequence number range depends on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocols such as PPP and ATM cannot transmit packets of each other, and need to communicate by using virtual access (VA) interfaces. When Layer 2 protocols need to communicate, the system automatically creates a VA interface. You can configure a VA interface only by setting attributes for a VT interface. A VT interface is used by the system to configure VA interfaces.

Prerequisites

A VT interface has been created before the system creates a VA interface.

Precautions

After a VT interface is deleted, all of its derived VA interfaces are deleted automatically.

The link layer protocol of a VT interface is Up only when VA interfaces in Up state exist on the VT interface.

Example

Create VT interface 10.

```
<Huawei> system-view
[Huawei] interface virtual-template 10
[Huawei-Virtual-Template10]
```

Related Topics

5.20.6 display interface virtual-template

5.20.14 statistic enable

Function

Using the **statistic enable** command, you can enable the traffic statistics collection function on an interface.

Using the **undo statistic enable** command, you can restore the default setting.

By default, the traffic statistics collection function is disabled on an interface.

Format

statistic enable { **inbound** | **outbound** }

undo statistic enable { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables the traffic statistics collection function for incoming traffic on an interface.	-
outbound	Enables the traffic statistics collection function for outgoing traffic on an interface.	-

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view, MFR interface view, Layer 3 Virtual Ethernet interface view, Dialer interface view, VLANIF interface view, MP-group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the traffic statistics collection function is enabled on an interface, you can collect statistics about incoming and outgoing traffic on the interface.

Precautions

If the traffic statistics collection function has been configured on the maximum interfaces, running the **statistic enable** command will fail.

If you run the **statistic enable inbound** command to enable traffic statistics collection for incoming traffic on an interface, statistics about incoming traffic on the interface will be cleared.

When the traffic statistics collection function is enabled on a VLANIF interface using this command, the number of error packets on the interface will not be collected. If interfaces on the 8FE1GE, 24GE, and 24ES2GP cards are added to VLANs, statistics on traffic forwarded on the VLANIF interfaces are not collected.

Follow-up Procedure

Run the **display interface** command to view traffic statistics.

Example

Enable the traffic statistics collection function for incoming traffic on Ethernet2/0/0.1.

```
<Huawei> system-view
```

```
[Huawei] interface ethernet2/0/0.1
[Huawei-Ethernet2/0/0.1] statistic enable inbound
```

Related Topics

5.1.4 display interface

5.20.15 statistic ip enable

Function

Using the **statistic ip enable** command, you can enable the IPv4 traffic statistics collection function on an interface.

Using the **undo statistic ip enable** command, you can restore the default setting.

By default, the IP traffic statistics collection function is disabled on an interface.

NOTE

The SRU80, SRU100, SRU200, SRU400, and SRUX5 do not support this command.

Format

statistic ip enable { **inbound** | **outbound** }

undo statistic ip enable { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables the IP traffic statistics collection function for incoming traffic on an interface.	-
outbound	Enables the IP traffic statistics collection function for outgoing traffic on an interface.	-

Views

Dialer interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IPv4 traffic statistics collection function is enabled on an interface, you can collect statistics about incoming and outgoing IP traffic on the interface.

Precautions

You can configure the IPv4 traffic statistics collection function on a maximum of 4096 interfaces. If the IP traffic statistics collection function has been configured on 4096 interfaces, running the **statistic ip enable** command will fail.

When the IPv4 traffic statistics collection function is enabled on a VLANIF interface using this command, the number of error packets on the interface will not be collected. If interfaces on the 8FE1GE, 24GE, and 24ES2GP cards are added to VLANs, statistics on traffic forwarded on the VLANIF interfaces are not collected.

Follow-up Procedure

Run the **display interface** command to view IP traffic statistics.

Example

Enable the IPv4 traffic statistics collection function for incoming traffic on VLANIF100.

```
<Huawei> system-view
[Huawei] interface vlanif 100
[Huawei-Vlanif100] statistic ip enable inbound
```

Related Topics

5.1.4 display interface

5.20.16 statistic ipv6 enable

Function

Using the **statistic ipv6 enable** command, you can enable the IPv6 traffic statistics collection function on an interface.

Using the **undo statistic ipv6 enable** command, you can restore the default setting.

By default, the IPv6 traffic statistics collection function is disabled on an interface.

NOTE

The SRU80, SRU100, SRU200, SRU400, and SRUX5 do not support this command.

Format

statistic ipv6 enable { **inbound** | **outbound** }

undo statistic ipv6 enable { **inbound** | **outbound** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Descripv6tion	Value
inbound	Enables the IPv6 traffic statistics collection function for incoming traffic on an interface.	-
outbound	Enables the IPv6 traffic statistics collection function for outgoing traffic on an interface.	-

Views

Dialer interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IPv6 traffic statistics collection function is enabled on an interface, you can collect statistics about incoming and outgoing IPv6 traffic on the interface.

Precautions

You can configure the IPv6 traffic statistics collection function on a maximum of 4096 interfaces. If the IPv6 traffic statistics collection function has been configured on 4096 interfaces, running the **statistic ipv6 enable** command will fail.

When the IPv6 traffic statistics collection function is enabled on a VLANIF interface using this command, the number of error packets on the interface will not be collected. If interfaces on the 8FE1GE, 24GE, and 24ES2GP cards are added to VLANs, statistics on traffic forwarded on the VLANIF interfaces are not collected.

Follow-up Procedure

Run the **display interface** command to view IPv6 traffic statistics.

Example

Enable the IPv6 traffic statistics collection function for incoming traffic on VLANIF100.

```
<Huawei> system-view
[Huawei] interface vlanif 100
[Huawei-Vlanif100] statistic ipv6 enable inbound
```

Related Topics

5.1.4 display interface

5.20.17 trigger trap

Function

Using the **trigger trap** command, you can configure an interface to send traps to the NMS.

Format

trigger trap { **linkup** | **linkdown** }

Parameters

Parameter	Description	Value
linkup	Sends the LinkUp trap to the NMS.	-
linkdown	Sends the LinkDown trap to the NMS.	-

Views

Loopback interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traps configured by **trigger trap** are used to check whether the network between the NMS and device functions properly. If the NMS receives a trap sent from the interface, the network between the NMS and device functions properly; otherwise, a fault may occur on the network.

Prerequisites

Run the **snmp-agent trap enable feature-name** command to enable the LinkUp and LinkDown traps.

Precautions

The **trigger trap** command is used on loopback interfaces to check the network between the NMS and device. The interface status does not change according to the meaning of the trap. For example, if the **trigger trap linkdown** command is used, the loopback interface sends a LinkDown trap to the NMS but does not change its status to Down. If you have used the **trigger trap linkdown** command, you must run the **trigger trap linkup** command to clear the LinkDown trap on the NMS.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a loopback interface to send the LinkUp trap to the NMS.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] trigger trap linkup
```

5.21 transparent transmission commands

5.21.1 display transport info

Function

The **display transport info** command displays the service configuration of the current serial interface.

Format

display transport info

Parameters

None

Views

TTY user interface view

Default Level

1: Monitoring level

Usage Guidelines

A router can function as a server or client to transparently transmit data through the serial interface in TCP or UDP mode. You can run the **display transport info** command to check information, such as the transmission mode, connection type, IP address of the remote device, interface number, about the router in TCP server, TCP client, and UDP client modes of transparent transmission through the serial interface, respectively.

Example

Display the service configuration of the current serial interface when the router functions as a TCP server.

```
<Huawei> system-view
[Huawei] user-interface tty 9
[Huawei-ui-tty9] display transport info
*******************************************************************************
 TTYIndex                    9      IsTransEnable              Enabled
 TransMode                   RAW      ConnectType                TCP Server
 MaxClientNum                4      TcpIdleTimeOut                   0
```

```
PacketTimer                    100      PacketSize                    0
SpecialChar                         best-effort              Disabled
RS232Mode                  Disabled      TTY2Mode                   RS485
Server Port                 60000      IsSetClientIp                 No
*****************************************************************************
```

Display the service configuration of the current serial interface when the router functions as a TCP client.

```
<Huawei> system-view
[Huawei] user-interface tty 9
[Huawei-ui-tty9] display transport info
*****************************************************************************
TTYIndex                       9      IsTransEnable              Enabled
TransMode                    RAW      ConnectType             TCP Client
MaxServerNum                   100      TcpServerCount                 0
TcpIdleTimeOut                   0      PacketSize                     0
PacketTimer                    100      best-effort              Disabled
SpecialChar                         TTY2Mode                   RS485
RS232Mode                  Disabled
Server IP            1.1.2.1      Server Port                 60000
Server IP            1.1.2.1      Server Port                 60001
*****************************************************************************
```

Table 5-76 Description of the **display transport info** command output

Item	Description
TTYIndex	Index of the user interface view.
IsTransEnable	Whether the RAW service function is enabled. To enable the RAW service function, run the **raw-transport enable** command.
TransMode	Transmission mode for transparent data transmission through the serial interface. ● None: no service mode ● RAW: transparent transmission mode To configure the transmission mode, run the **mode (TTY user interface view)** command.
ConnectType	Connection type for transparent data transmission through the serial interface. ● TCP server ● TCP client ● UDP client To configure the connection type, run the **raw-transport server-port** command.

Item	Description
MaxClientNum	Maximum number of clients that the router functioning as a server can be connected to. The value is 4.
MaxServerNum	Maximum number of servers that the router functioning as a client can be connected to. The value is 100.
TcpClientCount	Current number of clients that the router functioning as a server is connected to.
TcpServerCount	Current number of servers that the router functioning as a client is connected to.
TcpIdleTimeOut	Timeout interval for TCP connections. To configure the timeout interval for TCP connections, run the **raw-transport tcp idle-timeout** command.
PacketSize	Size of an encapsulated packet. To configure the size of an encapsulated packet, run the **raw-transport packet-size** command.
PacketTimer	Packet encapsulation timer. To configure the packet encapsulation timer, run the **raw-transport packet-timer** command.
best-effort	Whether the best-effort function is enabled. To enable the best-effort function, run the **raw-transport best-effort** command.
SpecialChar	Special character of an encapsulated packet. To configure the special character of an encapsulated packet, run the **raw-transport special-char** command.
TTY2Mode	TTY2 mode. ● RS485 ● RS422 To configure the TTY2 mode, run the **raw-transport tty2-mode** command.
RS232Mode	Whether the RS232 serial interface mode is enabled. To configure the RS232 serial interface mode, run the **raw-transport server-port** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Server IP	IP address of the server. To configure the IP address of the server, run the **raw-transport server-port** command.
Server Port	Interface number of the server. To configure the interface number of the server, run the **raw-transport server-port** command.
IsSetClientIp	Whether the IP address of the client is configured. To configure the IP address of the client, run the **raw-transport server-port** command.

Related Topics

5.21.2 display transport mode
5.21.3 display transport session
5.21.4 display transport stat

5.21.2 display transport mode

Function

The **display transport mode** command displays the service mode of the current serial interface.

Format

display transport mode

Parameters

None

Views

TTY user interface view

Default Level

1: Monitoring level

Usage Guidelines

After checking the service mode of the current serial interface using the **display transport mode** command, you can run the **mode** command to enter the service mode of the current serial interface or switch to another service mode of the serial interface base on actual requirements.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the service mode of the current serial interface.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] display transport mode
Info: Current TTY mode is RAW.
```

Table 5-77 Description of the **display transport mode** command output

Item	Description
Current TTY mode	Service mode of the current serial interface. ● none ● raw To configure the service mode of the current serial interface, run the **mode (TTY user interface view)** command.

Related Topics

6.2.26 mode

5.21.3 display transport session

Function

The **display transport session** command displays session information about the current serial interface.

Format

display transport session

Parameters

None

Views

TTY user interface view

Default Level

1: Monitoring level

Usage Guidelines

A router can function as a server or client to transparently transmit data through the serial interface in TCP or UDP mode. You can run the **display transport**

session command to check the session ID, establishment time of the session, and the IP address and interface number of the client or server for which the session is established.

Example

Display session information about the current serial interface when the router functions as a TCP server.

```
<Huawei> system-view
[Huawei] user-interface tty 9
[Huawei-ui-tty9] display transport session
 ******************************************************************************
 TTYIndex                    9      IsTransEnable              Enabled
 TransMode                   RAW      ConnectType                TCP Server
 Server Port               60000
 Session                     1      Time            2017-12-11 12:07:53
 Client IP           1.1.2.1      Client Port                53094
 Session                     2      Time            2017-12-11 12:08:04
 Client IP           1.1.2.1      Client Port                53122

 ******************************************************************************
```

Display session information about the current serial interface when the router functions as a TCP client.

```
<Huawei> system-view
[Huawei] user-interface tty 9
[Huawei-ui-tty9] display transport session
 ******************************************************************************
 TTYIndex                    9      IsTransEnable              Enabled
 TransMode                   RAW      ConnectType                TCP Client
 MaxServerNum                  100      TcpIdleTimeOut                  0
 PacketTimer                 100      PacketSize                    0
 SpecialChar                        best-effort              Disabled
 RS232Mode               Disabled      TTY2Mode                     RS485
 Server IP           1.1.2.1      Server Port                60000
 Server IP           1.1.2.1      Server Port                60001
 ******************************************************************************
```

Table 5-78 Description of the **display transport session** command output

Item	Description
TTYIndex	Index of the user interface view.
IsTransEnable	Whether the RAW service function is enabled. To configure the RAW service function, run the **raw-transport enable** command.
TransMode	Transmission mode for transparent data transmission through the serial interface. ● None: no service mode ● RAW: transparent transmission mode To configure the transmission mode, run the **mode (TTY user interface view)** command.

Item	Description
ConnectType	Connection type for transparent data transmission through the serial interface. ● TCP server ● TCP client ● UDP client To configure the connection type, run the **raw-transport server-port** command.
Session	Session ID. To delete a specified session, run the **kick-out session** command.
Time	Connection time of a session.
ServerPort	Interface number of the server. To configure the interface number of the server, run the **raw-transport server-port** command.
Server IP	IP address of the server. To configure the IP address of the server, run the **raw-transport server-port** command.
Client IP	IP address of the client. To configure the IP address of the client, run the **raw-transport server-port** command.
Client Port	Interface number of the client. To configure the interface number of the client, run the **raw-transport server-port** command.

Related Topics

5.21.5 kick-out session
5.21.2 display transport mode
5.21.4 display transport stat
5.21.1 display transport info

5.21.4 display transport stat

Function

The **display transport stat** command displays packet statistics of the current serial interface.

Format

display transport stat

Parameters

None

Views

TTY user interface view

Default Level

1: Monitoring level

Usage Guidelines

A router can function as a server or client to transparently transmit data through the serial interface in TCP or UDP mode. You can run the **display transport stat** command to check packet statistics information of the current serial interface, including the number of times sessions are established, number of times sessions are rejected, number of received packets, and number of sent packets.

Example

Display status information about the current serial interface when the router functions as a TCP server.

```
<Huawei> system-view
[Huawei] user-interface tty 9
[Huawei-ui-tty9] display transport stat
 ******************************************************************************
 TTYIndex                    9      IsTransEnable              Enabled
 TransMode                   RAW      ConnectType                TCP Server
 Serial Tx                  0      Serial Rx                   0
 Session                    1
 Client IP            1.1.2.1      Client Port                53094
 Socket Tx                   0      Socket Rx                    0
 Session                    2
 Client IP            1.1.2.1      Client Port                53122
 Socket Tx                   0      Socket Rx                    0

 ******************************************************************************
```

Display status information about the current serial interface when the router functions as a TCP client.

```
<Huawei> system-view
[Huawei] user-interface tty 9
[Huawei-ui-tty9] display transport stat
 ******************************************************************************
 TTYIndex                    9      IsTransEnable              Enabled
 TransMode                   RAW      ConnectType                TCP Client
 Serial Tx                  0      Serial Rx                   0
 Session                    3
 Server IP            1.1.2.1      Server Port                60000
 TTYIndex                    9      IsTransEnable              Enabled
 TransMode                   RAW      ConnectType                TCP Client
 Serial Tx                  0      Serial Rx                   0
 Session                    3
```

```
Server IP          1.1.2.1     Server Port          60000

******************************************************************************
```

Table 5-79 Description of the **display transport stat** command output

Item	Description
TTYIndex	Index of the user interface view.
IsTransEnable	Whether the RAW service function is enabled. To configure the RAW service function, run the **raw-transport enable** command.
TransMode	Transmission mode for transparent data transmission through the serial interface. ● None: no service mode ● RAW: transparent transmission mode To configure the transmission mode, run the **mode (TTY user interface view)** command.
ConnectType	Connection type for transparent data transmission through the serial interface. ● TCP server ● TCP client ● UDP client To configure the connection type, run the **raw-transport server-port** command.
Serial Tx	Number of packets sent through the serial interface.
Serial Rx	Number of packets received through the serial interface.
Session	Session ID. To delete a specified session, run the **kick-out session** command.
ServerPort	Interface number of the server. To configure the interface number of the server, run the **raw-transport server-port** command.
Server IP	IP address of the server. To configure the IP address of the server, run the **raw-transport server-port** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Client IP	IP address of the client. To configure the IP address of the client, run the **raw-transport server-port** command.
Client Port	Interface number of the client. To configure the interface number of the client, run the **raw-transport server-port** command.
Socket Tx	Number of sent packets on the TCP or UDP layer.
Socket Rx	Number of received packets on the TCP or UDP layer.

Related Topics

5.21.2 display transport mode
5.21.3 display transport session
5.21.1 display transport info

5.21.5 kick-out session

Function

The **kick-out session** command deletes the specified session connection.

Format

kick-out session *session-id*

Parameters

Parameter	Description	Value
session-id	Specifies the session ID.	The value is an integer that ranges from 1 to 4294967290.

Views

TTY user interface view

Default Level

2: Configuration level

Usage Guidelines

A unique session ID (*session-id*) is allocated to each connection in the TTY user interface view. You can check session information of the current serial interface

using the **display transport session** command. Deleting the session connection corresponding to the value of *session-id* using the **kick-out session** command is similar to disabling the RAW service using the **undo raw-transport enable** command in the RAW service view.

Example

Delete the session connection with the ID 100.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] kick-out session 100
```

Related Topics

5.21.3 display transport session

5.21.9 raw-transport enable

5.21.6 mode (TTY user interface view)

Function

The **mode** command configures the service mode of the serial interface, and displays the corresponding service view or an existing service view.

By default, the service mode of the serial interface is none.

Format

mode { **none** | **raw** | **scada** | **modbus-transport** }

Parameters

Parameter	Description	Value
none	Sets the service mode of the serial interface to none.	-
raw	Sets the service mode of the serial interface to RAW.	-
scada	Sets the service mode of the serial interface to SCADA. This is a reserved parameter.	-
modbus-transport	Sets the service mode of the serial interface to modbus-transport. This is a reserved parameter.	-

Views

TTY user interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After running the **mode** command, you can enter the corresponding service view and configure corresponding service functions. You can configure the following modes based on actual requirements:

- None: no service mode
- RAW: transparent transmission mode

Prerequisites

Transparent transmission through the serial interface has been enabled using the **socket-transport enable** command before the **mode raw** command is run on the RS232 serial interface.

Example

Set the service mode of the serial interface to the RAW mode and display the RAW service view.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] socket-transport enable
Info : RS232 has been changed to service mode.
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw]
```

5.21.7 raw-transport server-port

Function

The **raw-transport server-port** command configures transmission parameters for transparent transmission through the serial interface.

The **undo raw-transport** { **tcp** | **udp** } **client server-port** *server-port* **server-ip** *server-ip* command deletes transmission parameters specified in the RAW service view.

The **undo** { **tcp** | **udp** } command deletes all transmission parameters in the RAW service view.

By default, the working mode of the router for transparent transmission through the serial interface is not configured.

Format

raw-transport tcp server server-port *server-port* [**client-ip** *client-ip*] [**vpn-instance** *vpn-instance-name*]

raw-transport tcp client server-port *server-port* **server-ip** *server-ip* [**vpn-instance** *vpn-instance-name*]

raw-transport udp client server-port *server-port* **server-ip** *server-ip*

undo raw-transport tcp client server-port *server-port* **server-ip** *server-ip* [**vpn-instance** *vpn-instance-name*]

 Copyright © Huawei Technologies Co., Ltd.

undo raw-transport udp client server-port *server-port* **server-ip** *server-ip*

undo { **tcp** | **udp** }

NOTE

Only V200R010C10 and later versions support the **vpn-instance** *vpn-instance-name* parameter.

Parameters

Parameter	Description	Value
tcp server	Configures the router as a server to transparently transmit data through the serial interface in TCP mode.	-
tcp client	Configures the router as a client to transparently transmit data through the serial interface in TCP mode.	-
udp client	Configures the router as a client to transparently transmit data through the serial interface in UDP mode.	-
server-port *server-port*	Specifies the listening interface number of the server.	The value is an integer that ranges from 1 to 65534.
server-ip *server-ip*	Specifies the IP address of the server to which the listened router is connected.	The value is in dotted decimal notation, and must be a valid IP address of class A, B, or C. A maximum of 100 different IP addresses of servers can be configured.
client-ip *client-ip*	Specifies the IP address of the client that needs to be listened and is connected to the router.	The value is in dotted decimal notation, and must be a valid IP address of class A, B, or C. If the **client-ip** *client-ip* parameter is not specified, the router can randomly connect to a maximum of four clients. If the **client-ip** *client-ip* is specified, the client has occupied a connection and the router can randomly connect to a maximum of three clients.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the transparent transmission service of a serial port is bound.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

RAW service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Major differences between transparent transmission through the serial interface in TCP and UDP modes are as follows:

- TCP is connection-oriented and provides a data retransmission mechanism. It has high requirements for the network quality and real-time data transmission. When the network quality is poor, packet loss may occur.
- UDP is connectionless and does not provide a data retransmission mechanism. It has low requirements for the network quality and real-time data transmission.

You can choose an appropriate mode based on data integrity, network quality, and real-time data transmission requirements.

Precautions

If the RAW service has been enabled, run the **undo raw-transport enable** command to disable the RAW service before running the **raw-transport server-port** command. Otherwise, an error message is displayed.

For the same TTY, you can select only one mode from the TCP client, TCP server, and UDP client modes. The latest configured mode takes effect. A router functioning as a client can be connected to a maximum of 100 servers. A router functioning as a server can be connected to a maximum of four clients.

The system verifies the configured IP address and interface number.

- The following IP addresses are invalid:
  - Addresses with all 0s or 1s
  - Multicast addresses (class D addresses)
  - Loopback addresses (in the 127.x.x.x format)
  - Broadcast addresses of classes A, B, and C
- When the router functions as a server, values of *server-port* configured in different TTYs cannot be the same at the same time.

 Copyright © Huawei Technologies Co., Ltd.

- When the router functions as a client, values of *server-ip* configured in different TTYs cannot be the same at the same time.

Example

Configure the router as a server to transparently transmit data through the serial interface in TCP mode.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport tcp server server-port 1111 client-ip 10.1.1.100
```

Configure the router as a client to transparently transmit data through the serial interface in TCP mode.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport tcp client server-port 1111 server-ip 10.1.1.100
```

Configure the router as a client to transparently transmit data through the serial interface in UDP mode.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport udp client server-port 1111 server-ip 10.1.1.100
```

Related Topics

5.21.16 undo parameter

5.21.8 raw-transport best-effort

Function

The **raw-transport best-effort** command enables the best effort mode, so that the router discards old data from the cache first.

undo best-effort command disables the best effort mode.

By default, the best effort mode is disabled, so that the router discards new data from the cache first.

Format

raw-transport best-effort

undo best-effort

Parameters

None

Views

RAW service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the router discards new data from the cache first. After the **raw-transport best-effort** command is run, the router discards old data from the cache first.

Precautions

If the RAW service has been enabled, run the **undo raw-transport enable** command to disable the RAW service before running the **raw-transport best-effort** command. Otherwise, an error message is displayed.

Example

Configure the best effort mode, so that the router discards old data from the cache first.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport best-effort
```

Related Topics

5.21.9 raw-transport enable

5.21.1 display transport info

5.21.9 raw-transport enable

Function

The **raw-transport enable** command enables the RAW service function.

The **undo raw-transport enable** command disables the RAW service function.

By default, the RAW service function is disabled.

Format

raw-transport enable

undo raw-transport enable

Parameters

None

Views

RAW service view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Configuration commands run in the RAW service view take effect only after the RAW service function is enabled.

Example

Enable the RAW service function.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport enable
```

Related Topics

5.21.11 raw-transport packet-timer

5.21.1 display transport info

5.21.10 raw-transport packet-size

Function

The **raw-transport packet-size** command configures the size of an encapsulated packet.

The **undo packet-size** command cancels the configured size of an encapsulated packet.

By default, the size of an encapsulated packet is not configured. The router does not encapsulate received packets and sends them without changing their sizes (not greater than 2000 bytes).

Format

raw-transport packet-size *size*

undo packet-size

Parameters

Parameter	Description	Value
size	Specifies the size of an encapsulated packet.	The value is an integer that ranges from 16 to 1400, in bytes.

Views

RAW service view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the size of an encapsulated packet is configured, the router only sends packets whose sizes reach the specified size.

Precautions

If the RAW service has been enabled, run the **undo raw-transport enable** command to disable the RAW service before running the **raw-transport packet-size** command. Otherwise, an error message is displayed.

Example

Set the size of an encapsulated packet to 100 bytes.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport packet-size 100
```

Related Topics

5.21.1 display transport info

5.21.11 raw-transport packet-timer

Function

The **raw-transport packet-timer** command configures the packet encapsulation timer.

The **undo packet-timer** command restores the default interval of the packet encapsulation timer.

By default, the interval of the packet encapsulation timer is 100 ms.

Format

raw-transport packet-timer *time*

undo packet-timer

Parameters

Parameter	Description	Value
time	Specifies the periodic packet sending time.	The value is an integer that ranges from 20 to 100000, in milliseconds. The value must be an integer multiple of 20, for example, 40, 60, or 80.

 Copyright © Huawei Technologies Co., Ltd.

Views

RAW service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the packet encapsulation timer is configured and a router does not obtain packets within a specified period, the router sends received packets.

Precautions

If the RAW service has been enabled, run the **undo raw-transport enable** command to disable the RAW service before running the **raw-transport packet-timer** command. Otherwise, an error message is displayed.

Example

Set the interval of the packet encapsulation timer to 200 ms.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport packet-timer 200
```

Related Topics

5.21.9 raw-transport enable

5.21.1 display transport info

5.21.12 raw-transport special-char

Function

The **raw-transport special-char** command enables the special character filtering function.

The **undo special-char** command disables the special character filtering function.

By default, the special character filtering function is disabled.

Format

raw-transport special-char *char-value*

undo special-char

Parameters

Parameter	Description	Value
char-value	Specifies the special character to be filtered.	The value is an integer that ranges from 0 to 255.

Views

RAW service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the special character filtering function is enabled and a router receives a packet containing a special character, the router immediately sends the packet.

Precautions

If the RAW service has been enabled, run the **undo raw-transport enable** command to disable the RAW service before running the **raw-transport special-char** command. Otherwise, an error message is displayed.

Example

Enable the special character filtering function and set the special character to be filtered to 3.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport special-char 3
```

5.21.13 raw-transport tcp idle-timeout

Function

The **raw-transport tcp idle-timeout** command configures the timeout interval for TCP connections.

The **undo idle-timeout** command restores the default timeout interval for TCP connections.

By default, the timeout interval for TCP connections is 0 minutes.

Format

raw-transport tcp idle-timeout *time*

undo idle-timeout

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time	Specifies the timeout interval for TCP connections.	The value is an integer that ranges from 0 to 60, in minutes.

Views

RAW service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the timeout interval for TCP connections is 0 minutes, indicating that TCP connections are not automatically disconnected. For security purposes, you can disconnect TCP connections if the router does not receive or send any data within a specified period. If a router functions a server and the TCP connection is disconnected, the router re-enters the listening status and waits from the next connection. If a router functions as a client and the TCP connection is disconnected, the TCP connection is automatically re-established when data needs to be sent.

Precautions

If the RAW service has been enabled, run the **undo raw-transport enable** command to disable the RAW service before running the **raw-transport tcp idle-timeout** command. Otherwise, an error message is displayed.

Example

Set the timeout interval for TCP connections to 2 minutes.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
[Huawei-ui-tty1-raw] raw-transport tcp idle-timeout 2
```

Related Topics

5.21.9 raw-transport enable

5.21.1 display transport info

5.21.14 raw-transport tty2-mode

Function

The **raw-transport tty2-mode** command configures the working mode of the TTY2.

 Copyright © Huawei Technologies Co., Ltd.

By default, the working mode of the TTY2 is RS485.

Format

raw-transport tty2-mode *mode*

Parameters

Parameter	Description	Value
mode	Specifies the working mode of the TTY2.	The value is a character string and can be: • RS485 • RS422

Views

RAW service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the working mode of the TTY2 to RS485 or RS422 using the **raw-transport tty2-mode** command. This command takes effect only for the TTY2.

Precautions

If the RAW service has been enabled, run the **undo raw-transport enable** command to disable the RAW service before running the **raw-transport tty2-mode** command. Otherwise, an error message is displayed.

Example

Set the working mode of the TTY2 to RS422.

```
<Huawei> system-view
[Huawei] user-interface tty 2
[Huawei-ui-tty2] mode raw
[Huawei-ui-tty2] raw-transport tty2-mode rs422
```

Related Topics

5.21.9 raw-transport enable

5.21.1 display transport info

5.21.15 socket-transport enable

Function

The **socket-transport enable** command switches the RS232 serial interface of a router from the management mode to the service mode.

The **undo socket-transport enable** command switches the RS232 serial interface of a router from the service mode back to the management mode.

By default, the RS232 serial interface is a management interface.

NOTE

The 8AS interface board does not support the **socket-transport enable** command.

Format

socket-transport enable

undo socket-transport enable

Parameters

None

Views

TTY user interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the RS232 serial interface of a router functions as a management interface and users can perform configuration management using this interface. After the **socket-transport enable** command is run, the RS232 serial interface of a router is switched from a management interface to a service interface for transparent transmission through the serial interface. In this case, the local router can receive data of the remote device when interconnected with the remote device.

The RJ45 and RS485 serial interfaces are service interfaces, and the serial interface modes do not need to be switched.

Precautions

The RS232 serial interface cannot receive data from a management interface after being switched to a service interface. To switch a serial interface back to a management interface, run the **undo socket-transport enable** command. You need to log in to the router and be authenticated again after a switchover.

 Copyright © Huawei Technologies Co., Ltd.

Only the TTY1 interface supports the **socket-transport enable** command.

Example

Enable the function of transparent transmission through the serial interface.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] socket-transport enable
Info : RS232 has been changed to service mode.
```

Related Topics

5.21.1 display transport info

5.21.16 undo parameter

Function

The **undo parameter** command deletes all RAW service configurations.

Format

undo parameter

Parameters

None

Views

RAW service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To delete all RAW service configurations in the RAW service view, run the **undo parameter** command.

Prerequisites

The RAW service function has been disabled using the **undo raw-transport enable** command.

Example

Delete all RAW service configurations.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] mode raw
```

```
[Huawei-ui-tty1-raw] undo raw-transport enable
[Huawei-ui-tty1-raw] undo parameter
```

6 Ethernet Switching Commands

About This Chapter

6.1 MAC Address Table Configuration Commands
6.2 Link Aggregation Commands
6.3 VLAN Configuration Commands
6.4 Voice VLAN Configuration Commands
6.5 QinQ Configuration Commands
6.6 VLAN Mapping Configuration Commands
6.7 GVRP Configuration Commands
6.8 STP/RSTP/MSTP Configuration Commands
6.9 SEP Configuration Commands
6.10 Layer 2 Protocol Transparent Transmission Commands
6.11 Transparent Bridging (TB) Configuration Commands

6.1 MAC Address Table Configuration Commands

6.1.1 display loop-detect eth-loop

Function

The **display loop-detect eth-loop** command displays the result of MAC address flapping detection.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support MAC address flapping detection.

The AR100, AR120, AR161, AR161G-L, AR161W, AR169, AR169-P-M9, AR169G-L, AR169W, AR161EW, AR161EW-M1, AR161G-Lc, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR161G-U, AR169W-P-M9, AR169RW-P-M9, AR2204-24GE, AR2204-48GE-P, AR2204E, AR2204E-D, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE, AR2204-51GE-R, AR2204-51GE-P, AR2220E, AR2204XE-DC, and AR2204XE do not support MAC address flapping detection.

Format

display loop-detect eth-loop [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the result of MAC address flapping detection in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring MAC address flapping detection, you can use the **display loop-detect eth-loop** command to verify the configuration.

The **display loop-detect eth-loop** command displays the blocked interfaces, blocked MAC addresses, and VLANs that the blocked interfaces and MAC addresses belong to.

Precautions

If **vlan** *vlan-id* is not specified, the result of MAC address flapping detection in all VLANs is displayed.

Example

Display the result of MAC address flapping detection in all VLANs.

```
<Huawei> display loop-detect eth-loop
VLAN          Block-time      RetryTimes      Block-action
```

```
--------------- --------------- --------------- ---------------
100             0               0               alarm-only

Total items:1

Blocked ports:

Total items:0

PortName                 Vlan     Status         Expire(s)      Leave times
------------------------ --------  -------------  -------------  -------------

Blocked Mac Address:

Total items:0

Mac Address              Vlan     Status         Expire(s)      Leave times
------------------------ --------  -------------  -------------  -------------
```

Table 6-1 Description of the display loop-detect eth-loop command output

Item	Description
VLAN	ID of a VLAN where MAC address flapping detection is configured.
Block-time	Blocking time of an interface or a MAC address.
RetryTimes	Number of detection attempts before an interface or a MAC address is permanently blocked.
Total items	Total number of VLANs where MAC address flapping detection is configured.
Block-action	Action performed when MAC address flapping occurs. ● alarm-only: only sends a trap. ● block-mac: blocks the flapping MAC address. ● block-port: blocks the interface where MAC address flapping occurs.
Blocked ports	Interfaces that are blocked.
PortName	Name of a blocked interface.
Total items	Number of blocked interfaces.
Blocked Mac Address	MAC addresses that are blocked.
Mac Address	Blocked MAC address.
Total items	Number of blocked MAC addresses.
Status	Status of a blocked interface or MAC address.
Expire(s)	How soon will a blocked interface or MAC address be unblocked, in seconds.

Item	Description
Leave times	Number of MAC address flapping events allowed after an interface or a MAC address is unblocked. When this number is exceeded, the interface or MAC address will be permanently blocked.

Related Topics

6.1.16 loop-detect eth-loop

6.1.2 display bridge mac-address

Function

The **display bridge mac-address** command displays the bridge MAC address of a device.

Format

display bridge mac-address

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you need to view the bridge MAC address of a device, run the **display bridge mac-address** command.

Example

Display the bridge MAC address of a device.

```
<Huawei> display bridge mac-address
System bridge MAC address: 00e0-f74b-6d00
```

 Copyright © Huawei Technologies Co., Ltd.

Table 6-2 Description of the display bridge mac-address command output

Item	Description
System bridge MAC address	Indicates the bridge MAC address of a device.

6.1.3 display mac-address

Function

The **display mac-address** command displays the MAC address table of the router. A MAC address entry contains the destination MAC address, VLAN ID, outbound interface, and entry type.

Format

display mac-address *mac-address* [**vlan** *vlan-id* | **vsi** *vsi-name* | **verbose**]

display mac-address [**vlan** *vlan-id* | **vsi** *vsi-name* | *interface-type interface-number*] *

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address in an entry.	The value is in H-H-H format. H is a hexadecimal number of 4 digits, for example, 00e0 and fc01. If you enter less than four digits, 0s are prefixed to the input digits. For example, if you enter e0, the system changes e0 to 00e0. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
vlan *vlan-id*	Displays MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vsi *vsi-name*	Displays the MAC address entries of a specified Virtual Switching Instance (VSI). **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Displays the MAC address entries with a specified outbound interface. • *interface-type* specifies the type of the outbound interface. • *interface-number* specifies the number of the outbound interface.	-
verbose	Displays detailed information about MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the router stores MAC addresses of other devices. When forwarding an Ethernet frame, the router searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The **display mac-address** command displays all MAC address entries, such as dynamic MAC address entries, static MAC address entries, and blackhole MAC address entries. A MAC address entry contains the destination MAC address, VLAN ID, outbound interface, and entry type.

Follow-up Procedure

If any MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address static** command to add a correct one.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If you run the **display mac-address** command without parameters, all MAC address entries are displayed.

When the router has a large number of MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all MAC address entries.

```
<Huawei> display mac-address
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge/VSI/BD      Learned-From              Type
--------------------------------------------------------------------------------
0000-0000-0033       100/-                Eth0/0/5                  dynamic
0003-0002-0003    -/-/-/10                Eth0/0/1.1                static
0004-0003-0004    -/-/-/20                2.2.2.2                   static

--------------------------------------------------------------------------------
Total items displayed = 3
```

Display detailed information about all MAC address entries in VLAN 100.

```
<Huawei> display mac-address vlan 100
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge/VSI/BD      Learned-From              Type
--------------------------------------------------------------------------------
0000-0000-0033       100/-                Eth0/0/5                  dynamic

--------------------------------------------------------------------------------
Total items displayed = 1
```

Table 6-3 Description of the **display mac-address** command output

Item	Description
MAC Address	Destination MAC address in a MAC address entry.
VLAN/ Bridge/VSI/BD	● VLAN: VLAN associated with the interface ● Bridge: bridge that the interface belongs to ● VSI: VSI associated with the interface ● BD: BD associated with the interface **NOTE** BD information is displayed only on the VXLAN-enabled device.
Learned-From	Interface that learns a MAC address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Type of a MAC address entry. • static: indicates a static MAC address entry, which is manually configured and will not be aged out. • blackhole: indicates a blackhole MAC address entry, which is manually configured and will not be aged out. • dynamic: indicates a MAC address entry learned by the router, which will be aged out when the aging time expires. • security: indicates a MAC address entry that an interface learns after port security is enabled. • sticky: indicates a MAC address entry that an interface learns after the sticky MAC function is enabled. • mux: indicates a MAC address entry learned by a MUX VLAN enabled interface. • snooping: indicates a static MAC address entry generated based on the dynamic DHCP snooping binding table.
Total items displayed	Specifies the total number of MAC address entries that can be displayed.

Related Topics

6.1.11 display mac-address summary
6.1.12 display mac-address total-number

6.1.4 display mac-address aging-time

Function

The **display mac-address aging-time** command displays the aging time of dynamic MAC address entries in the MAC address table.

Format

display mac-address aging-time [**vsi** [**name** *name*]

Parameters

Parameter	Description	Value
vsi [**name** *name*]	Displays the aging time with the specified Virtual Switching Instance (VSI) name of the address table entries. **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	The value is a string of 1 to 31 case-insensitive characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays the aging time of dynamic MAC address entries on the router. You can check whether the aging time is suitable for network requirements and device performance.

Follow-up Procedure

If the aging time is unsuitable for requirements or device performance, run the **mac-address aging-time** command to set the aging time properly.

Precautions

If the aging time is 0, dynamic MAC addresses will not be aged out. In this case, MAC address entries increase sharply and the MAC address table will be full quickly.

Example

Display the aging time of dynamic MAC address entries.

```
<Huawei> display mac-address aging-time
  Aging time: 300 second(s)
```

Table 6-4 Description of the display mac-address aging-time command output

Item	Description
Aging time	Aging time of dynamic MAC address entries, in seconds. To set the aging time, run the **mac-address aging-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

6.1.19 mac-address aging-time

6.1.5 display mac-address blackhole

Function

The **display mac-address blackhole** command displays blackhole MAC address entries.

Format

display mac-address blackhole [**vlan** *vlan-id* | **vsi** *vsi-name*] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays blackhole MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
vsi *vsi-name*	Displays the blackhole MAC address entries in a specified Virtual Switching Instance (VSI). **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about specified blackhole MAC address entries. **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the router stores MAC addresses of other devices. When forwarding an Ethernet frame, the router searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The MAC address table contains the following MAC address entries:

- Blackhole MAC address entries that are used to discard packets with the specified MAC addresses or destination MAC addresses. Blackhole MAC address entries are manually configured and will not be aged out.
- Static MAC entries that are manually configured and will not be aged out.
- Dynamic MAC address entries that are learned by the router and will be aged out when the aging time expires.

To check whether blackhole MAC address entries are configured correctly, run this command. These entries ensure communication between authorized users.

Follow-up Procedure

If any blackhole MAC address entry in the command output is incorrect, run the **undo mac-address** command to delete the entry or run the **mac-address blackhole** command to add a correct one.

Precautions

If you run the **display mac-address blackhole** command without parameters, all blackhole MAC address entries are displayed.

If the MAC address table does not contain any blackhole MAC address, no information is displayed.

Example

Display all blackhole MAC address entries.

```
<Huawei> display mac-address blackhole
--------------------------------------------------------------------------------
MAC Address         VLAN/Bridge/VSI/BD                Learned-From        Type
--------------------------------------------------------------------------------
0022-0022-0033      100/-                    -                blackhole
0000-0000-0001      101/-                    -                blackhole


--------------------------------------------------------------------------------
Total items displayed = 2
```

Table 6-5 Description of the display mac-address blackhole command output

Item	Description
MAC Address	Destination MAC address in a blackhole MAC address entry.
VLAN/ Bridge/VSI/BD	ID of the VLAN, Bridge, BD or name of the VSI that a MAC address belongs to.
Learned-From	When the type of a MAC address entry is blackhole, "-" is displayed.
Type	Type of a MAC address entry.

Related Topics

6.1.11 display mac-address summary
6.1.12 display mac-address total-number
6.1.18 mac-address

6.1.6 display mac-address dynamic

Function

The **display mac-address dynamic** command displays dynamic MAC address entries.

Format

display mac-address dynamic [**vlan** *vlan-id* | *interface-type interface-number* | **verbose**]

display mac-address dynamic [[**slot**] *slot-id*] { **vsi** *vsi-name* | *interface-type interface-number* } * [**verbose**]

display mac-address dynamic [[**slot**] *slot-id*] **vsi** *vsi-name* [**peer** *peer-ip* **pw-id** *pw-id*] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays dynamic MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays dynamic MAC address entries with a specified outbound interface. • *interface-type* specifies the type of the outbound interface. • *interface-number* specifies the number of the outbound interface.	-
slot *slot-id*	Displays the dynamic MAC address entries on a board in a specified slot.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Displays detailed information about dynamic MAC address entries.	-
vsi *vsi-name*	Displays the blackhole MAC address entries in a specified Virtual Switching Instance (VSI). **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *peer-ip*	Displays the number of MAC address entries on the device with the specified IP address at the other end of the Pseudo Wire (PW).	The value is in dotted decimal notation.
pw-id *pw-id*	Displays the number of MAC address entries on the device with the specified PW ID at the other end of the PW.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table needs to be updated constantly because the network topology always changes. You can use this command to view learned MAC addresses in real time.

Follow-up Procedure

If the displayed dynamic MAC address entries are invalid, run the **undo mac-address** command to delete dynamic MAC address entries.

Precautions

If you run the **display mac-address dynamic** command without parameters, all dynamic MAC address entries are displayed.

If the MAC address table does not contain any dynamic MAC address entry, no information is displayed.

When the router has a large number of dynamic MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all dynamic MAC address entries.

```
<Huawei> display mac-address dynamic
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge/VSI/BD          Learned-From       Type
--------------------------------------------------------------------------------
0022-0022-0033    100/-                 Eth2/0/1          dynamic
0000-0000-0001    -/HUAWEI                Eth2/0/1          dynamic
--------------------------------------------------------------------------------
Total items displayed = 2
```

Table 6-6 Description of the display mac-address dynamic command output

Item	Description
MAC Address	Destination MAC address in a dynamic MAC address entry.
VLAN/ Bridge/VSI/BD	ID of the VLAN, name of the bridge, BD or name of the virtual switch instance (VSI) that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry.

Related Topics

6.1.11 display mac-address summary
6.1.12 display mac-address total-number
6.1.18 mac-address

6.1.7 display mac-address mux

Function

The **display mac-address mux** command displays MUX MAC address entries.

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220, AR2220L, AR2220E, AR2240, AR2240C, AR3260, and AR3670 support MUX VLAN.

Only the 8FE1GE, 24ES2GP, and 24GE cards support MUX VLAN.

Format

display mac-address mux [**vlan** *vlan-id* | *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MUX MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MUX MAC address entries with a specified outbound interface. • *interface-type* specifies the type of the outbound interface. • *interface-number* specifies the number of the outbound interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. A MUX MAC address entry is learned by a MUX VLAN enabled interface. The learned MUX MAC address entries are deleted after the router restarts.

After configuring the MUX VLAN function, you can run the **display mac-address mux** command to check whether the learned MUX MAC address entries are correct.

Follow-up Procedure

If the displayed MUX MAC address entries are invalid, run the **undo mac-address** command to delete MUX MAC address entries.

Precautions

If you run the **display mac-address mux** command without parameters, all MUX MAC address entries are displayed.

 Copyright © Huawei Technologies Co., Ltd.

If the MAC address table does not contain any MUX MAC address entry, no information is displayed.

When the router has a large number of MUX MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all MUX MAC address entries.

```
<Huawei> display mac-address mux
--------------------------------------------------------------------------------
MAC Address         VLAN/Bridge/VSI/BD                  Learned-From        Type
--------------------------------------------------------------------------------
0022-0022-0033      100/-                    Eth1/0/2          mux

--------------------------------------------------------------------------------
Total items displayed = 1
```

Table 6-7 Description of the display mac-address mux command output

Item	Description
MAC Address	Destination MAC address in a MUX MAC address entry.
VLAN/ Bridge/VSI/BD	ID of the VLAN, name of the bridge, BD or name of the virtual switch instance (VSI) that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry.

Related Topics

6.1.11 display mac-address summary

6.1.12 display mac-address total-number

6.1.8 display mac-address security

Function

The **display mac-address security** command displays secure dynamic MAC address entries.

Format

display mac-address security [**vlan** *vlan-id* | *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays secure dynamic MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays secure dynamic MAC address entries with a specified outbound interface. • *interface-type* specifies the type of the outbound interface. • *interface-number* specifies the number of the outbound interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface by using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. The learned secure dynamic MAC address entries are deleted after the device restarts.

After configuring the port security function, you can run the **display mac-address security** command to check whether the learned secure dynamic MAC address entries are correct.

Follow-up Procedure

If the displayed secure dynamic MAC address entries are invalid, run the **undo mac-address** command to delete secure dynamic MAC address entries.

Precautions

If you run the **display mac-address security** command without parameters, all secure dynamic MAC address entries are displayed.

If the MAC address table does not contain any secure dynamic MAC address entry, no information is displayed.

 Copyright © Huawei Technologies Co., Ltd.

When the device has a large number of secure dynamic MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all secure dynamic MAC address entries.

```
<Huawei> display mac-address security
--------------------------------------------------------------------------------
MAC Address         VLAN/Bridge/VSI/BD              Learned-From        Type
--------------------------------------------------------------------------------
0022-0022-0033      100/-                Eth2/0/1          security
0000-0000-0001      200/-                Eth2/0/2          security

--------------------------------------------------------------------------------
Total items displayed = 2
```

Table 6-8 Description of the display mac-address security command output

Item	Description
MAC Address	Destination MAC address in a secure dynamic MAC address entry.
VLAN/ Bridge/VSI/BD	ID of the VLAN, name of the bridge, BD or name of the virtual switch instance (VSI) that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry.

Related Topics

6.1.11 display mac-address summary
6.1.12 display mac-address total-number
6.1.23 port-security enable

6.1.9 display mac-address static

Function

The **display mac-address static** command displays static MAC address entries.

Format

display mac-address static [**vlan** *vlan-id* | *interface-type interface-number*]

display mac-address static [**vsi** *vsi-name* | *interface-type interface-number*] * [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays static MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays the static MAC address entries on a specified interface.	-
vsi *vsi-name*	Displays the static MAC address entries of a specified Virtual Switching Instance (VSI). **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about specified static MAC address entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the router stores MAC addresses of other devices. When forwarding an Ethernet frame, the router searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

The MAC address table contains the following MAC address entries:

- Static MAC entries that are manually configured and will not be aged out.
- Blackhole MAC address entries that are used to discard packets with the specified source MAC addresses or destination MAC addresses. Blackhole MAC address entries are manually configured and will not be aged out.

- Dynamic MAC address entries that are learned by the router and will be aged out when the aging time expires.

To improve network security, configure static MAC address entries to ensure that packets destined for specified MAC addresses are forwarded by the specified interfaces. This prevents attack packets with bogus MAC addresses and guarantees communication between the router and the upstream device or server. After configuring static MAC address entries, you can run the **display mac-address static** command to verify the configuration.

Follow-up Procedure

If any static MAC address entry is incorrect, run the **undo mac-address** command to delete it.

Precautions

If you run the **display mac-address static** command without parameters, all static MAC address entries are displayed.

If the MAC address table does not contain any static MAC address entry, no information is displayed.

Example

Display all static MAC address entries.

```
<Huawei> display mac-address static
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge/VSI/BD            Learned-From       Type
--------------------------------------------------------------------------------
0022-0022-0033    100/-                 Eth2/0/0          static
0000-0000-0001    101/-                 Eth2/0/2          static

--------------------------------------------------------------------------------
Total items displayed = 2
```

Table 6-9 Description of the display mac-address static command output

Item	Description
MAC Address	Destination MAC address in a static MAC address entry.
VLAN/ Bridge/VSI/BD	ID of the VLAN, name of the bridge, name of the virtual switch instance (VSI) or name of bridge domain that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry.

Related Topics

6.1.11 display mac-address summary

6.1.12 display mac-address total-number

6.1.18 mac-address

6.1.10 display mac-address sticky

Function

The **display mac-address sticky** command displays sticky VLAN MAC address entries.

Format

display mac-address sticky [**vlan** *vlan-id* | *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays sticky MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays sticky MAC address entries with a specified outbound interface. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the router stores MAC addresses of other devices. When forwarding an Ethernet frame, the router searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

After port security is enabled on an interface by using the **port-security enable** command, MAC address entries learned by the interface are stored in the MAC

address table as secure dynamic MAC address entries. The learned secure dynamic MAC address entries are deleted after the router restarts. If the sticky MAC function is also enabled on the interface by using the **port-security mac-address sticky** command, secure dynamic MAC address entries change to sticky MAC address entries. Sticky MAC address entries are not deleted after the router restarts.

To check the sticky MAC configuration or the learned sticky MAC address entries, run the **display mac-address sticky** command.

Follow-up Procedure

If the displayed sticky MAC address entries are invalid, run the **undo mac-address** command to delete sticky MAC address entries.

Precautions

If you run the **display mac-address sticky** command without parameters, all sticky MAC address entries are displayed.

If the MAC address table does not contain any sticky MAC address, no information is displayed.

When the router has a large number of sticky MAC address entries, it is recommended that you specify parameters in the command to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, so you cannot find the required information.
- The system traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all sticky MAC address entries.

```
<Huawei> display mac-address sticky
--------------------------------------------------------------------------------
MAC Address         VLAN/Bridge/VSI/BD              Learned-From        Type
--------------------------------------------------------------------------------
0022-0022-0033      100/-                           Eth2/0/1            sticky
0000-0000-0001      200/-                           Eth2/0/2            sticky

--------------------------------------------------------------------------------
Total items displayed = 2
```

Table 6-10 Description of the display mac-address sticky command output

Item	Description
MAC Address	MAC address in a sticky MAC address entry.
VLAN/ Bridge/VSI/BD	ID of the VLAN, name of the bridge, BD or name of the virtual switch instance (VSI) that a MAC address belongs to.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry.

Related Topics

6.1.11 display mac-address summary
6.1.12 display mac-address total-number
6.1.23 port-security enable
6.1.24 port-security mac-address sticky

6.1.11 display mac-address summary

Function

The **display mac-address summary** command displays statistics on MAC address entries.

Format

display mac-address summary

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the device stores MAC addresses of other devices. When forwarding an Ethernet frame, the router searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

When the router has many MAC address entries of different types, you can use the **display mac-address summary** command to view the summary of MAC address entries in the system. In the command output, Local and Remote identify the MAC address entries learned by the local board and MAC address entries synchronized from other boards.

Precautions

This command does not display the MAC address of interfaces on the 4GE-2S interface card.

 Copyright © Huawei Technologies Co., Ltd.

Example

View statistics on all MAC address entries in the system.

```
<Huawei> display mac-address summary
Mac Item of Lan Switch
-----------------------------------------------------------------------
Slot Total Blackhole Static DynLoc DynRmt Secure Sticky Block Authen
-----------------------------------------------------------------------
0      1       1     0     0     0     0     0     0     0
-----------------------------------------------------------------------
sum:   1       1     0     0     0     0     0     0     0

Mac Item of Transparent Bridge
---------------------------------
Total  Blackhole  Static  Dynamic
---------------------------------
1          0       1       0
```

Table 6-11 Description of the display mac-address summary command output

Item	Description
Mac Item of Lan Switch	Statistics about MAC address entries at the LAN side.
Mac Item of Transparent Bridge	Statistics about MAC address entries on the transparent bridge.
Slot	Slot ID of a board.
Total	Total number of MAC address entries.
Blackhole	Number of blackhole MAC address entries.
Static	Number of static MAC address entries.
Dynamic	Number of dynamic MAC address entries.
DynLoc	Number of MAC address entries learned by the local board.
DynRmt	Number of MAC address entries synchronized from other boards.
Secure	Number of secure dynamic MAC address entries.
Sticky	Number of sticky MAC address entries.
Block	Number of blocked MAC addresses.
Authen	Number of MAC addresses that have been authenticated.
sum	Total number of MAC address entries on all boards.

Related Topics

6.1.3 display mac-address
6.1.12 display mac-address total-number

6.1.12 display mac-address total-number

Function

The **display mac-address total-number** command displays the number of MAC address entries of a specified type.

Format

display mac-address total-number [**slot** *slot-id*]

display mac-address total-number [**vlan** *vlan-id* | *interface-type interface-number*]

display mac-address total-number blackhole [**vsi** *vsi-name*]

display mac-address total-number dynamic [**vlan** *vlan-id* | *interface-type interface-number*]

display mac-address total-number dynamic [**slot** *slot-id*] [**vsi** *vsi-name* | *interface-type interface-number*] *

display mac-address total-number dynamic [**slot** *slot-id*] **vsi** *vsi-name* **peer** *peer-ip* **pw-id** *pw-id*

display mac-address total-number static [**vlan** *vlan-id* | *interface-type interface-number*]

display mac-address total-number static [**vsi** *vsi-name* | *interface-type interface-number*] *

Parameters

Parameter	Description	Value
slot *slot-id*	Displays the number of MAC address entries on a specified board.	The value is an integer and must be the slot ID of a running board.
dynamic	Displays the number of dynamic MAC address entries.	-
blackhole	Displays the number of blackhole MAC address entries.	-
static	Displays the number of static MAC address entries.	-
vlan *vlan-id*	Displays the number of MAC address entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vsi *vsi-name*	Displays the blackhole MAC address entries in a specified Virtual Switching Instance (VSI). **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Displays the number of MAC address entries learned by a specified interface.	-
peer *peer-ip*	Displays the number of MAC address entries on the device with the specified IP address at the other end of the Pseudo Wire (PW).	The value is in dotted decimal notation.
pw-id *pw-id*	Displays the number of MAC address entries on the device with the specified PW ID at the other end of the PW.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The MAC address table of the router stores MAC addresses of other devices. When forwarding an Ethernet frame, the router searches the MAC address table for the outbound interface according to the destination MAC address and VLAN ID in the Ethernet frame.

When the router has many MAC address entries of different types, you can use the **display mac-address total-number** command to view statistics on MAC address entries of a specified type.

Precautions

If no parameter is specified, the total number of MAC address entries in the system is displayed.

If *interface-type interface-number* is not specified, the total number of MAC addresses learned by all interfaces is displayed.

If **vlan** *vlan-id* is not specified, the total number of MAC addresses in all VLANs is displayed.

Example

Display the number of dynamic MAC address entries.

```
<Huawei> display mac-address total-number dynamic
Info: total number of mac-address is : 20
```

Table 6-12 Description of the display mac-address total-number command output

Item	Description
Info: total number of mac-address	Total number of MAC address entries in the system.

Related Topics

6.1.11 display mac-address summary

6.1.3 display mac-address

6.1.13 display mac-limit

Function

The **display mac-limit** command displays the rules that limit the number of learned MAC addresses.

Format

display mac-limit [*interface-type interface-number* | **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the MAC address limiting rule on a specified interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan *vlan-id*	Displays the MAC address limiting rules in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether MAC address limiting rules are configured correctly, run the **display mac-limit** command. If a rule is incorrect, run the **mac-limit** command to modify the rule or run the **undo mac-limit all** command to delete it.

Precautions

If no parameter is specified, MAC address learning limit rules of all interfaces and VLANs are displayed.

vlan is not supported by AR200 and AR1200.

Example

Display all the MAC address limiting rules.

```
<Huawei> display mac-limit
-----------------------------------------------------------------------
PORT                VLAN     Maximum     Action     Alarm
-----------------------------------------------------------------------
Eth2/0/2            -        100         discard    enable

-----------------------------------------------------------------------
```

Table 6-13 Description of the display mac-limit command output

Item	Description
PORT	Name of an interface.
VLAN	ID of a VLAN.
Maximum	Maximum number of MAC addresses that can be learned. To set the maximum number of MAC addresses, run the **mac-limit** command.

Item	Description
Action	Action performed on packets when the number of learned MAC addresses exceeds the maximum number. ● discard: discards packets with new source MAC addresses. ● forward: forwards packets with new source MAC addresses.
Alarm	Whether an alarm is generated when the number of learned MAC addresses exceeds the maximum. ● enable: indicates that an alarm is generated. ● disable: indicates that an alarm is not generated.

Related Topics

6.1.21 mac-limit

6.1.14 drop illegal-mac alarm

Function

The **drop illegal-mac alarm** command configures the router to send a trap to the network management system (NMS) when receiving a packet with an all-0 MAC address.

By default, the router sends an alarm to the NMS when receiving a packet with an all-0 MAC address.

Format

drop illegal-mac alarm

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some legacy computers or network devices may send packets with an all-0 source or destination MAC address when their network adapters fail. The **drop illegal-**

mac alarm command configures the router to send a trap to the NMS when receiving a packet with an all-0 MAC address. You can locate the faulty network adapter according to the trap message.

Precautions

If the alarm function is disabled on the router, the NMS cannot receive any trap message.

After you run the **drop illegal-mac alarm** command, the router sends a trap only once after receiving packets with an all 0 MAC address. To configure the router to send traps continuously, run the **drop illegal-mac alarm** command repeatedly.

Example

Configure the router to send a trap to the NMS when receiving a packet with an all-0 MAC address.

```
<Huawei> system-view
[Huawei] drop illegal-mac alarm
```

Related Topics

6.1.15 drop illegal-mac enable

6.1.15 drop illegal-mac enable

Function

The **drop illegal-mac enable** command enables the router to discard packets with an all-0 invalid MAC address.

The **undo drop illegal-mac enable** command disables the router from discarding packets with an all-0 invalid MAC address.

By default, the router does not discard packets with an all-0 MAC address.

NOTE

The AR100&AR120&AR150&AR160 (except AR161EW-M1, AR169EGW-L, AR161EW, and AR169EW) &AR200&AR1200&AR3600 series, AR2204-24GE, AR2204-51GE, AR2204-48GE-P, AR2204E, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2220L, AR2220E, and AR2240C do not support discarding packets with an all-0 MAC address.

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support discarding packets with an all-0 MAC address.

Format

drop illegal-mac enable

undo drop illegal-mac enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some legacy computers or network devices may send packets with an all-0 source or destination MAC address when their network adapters fail. You can run the **drop illegal-mac enable** command to configure the router to discard such packets. After receiving the packets with an all-0 source or destination MAC address, the router discards the packets.

This command reduces incorrect MAC address entries on the device.

Example

Configure the router to discard packets with an all-0 invalid MAC address.

```
<Huawei> system-view
[Huawei] drop illegal-mac enable
```

Related Topics

6.1.14 drop illegal-mac alarm

6.1.16 loop-detect eth-loop

Function

The **loop-detect eth-loop** command enables MAC address flapping detection in a VLAN.

The **undo loop-detect eth-loop** command disables MAC address flapping detection in a VLAN.

By default, MAC address flapping detection is disabled in a VLAN.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support MAC address flapping detection.

The AR100, AR120, AR161, AR161G-L, AR161W, AR169, AR169-P-M9, AR169G-L, AR169W, AR161EW, AR161EW-M1, AR161G-Lc, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR161G-U, AR169W-P-M9, AR169RW-P-M9, AR2204-24GE, AR2204-48GE-P, AR2204E, AR2204E-D, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE, AR2204-51GE-R, AR2204-51GE-P, AR2220E, AR2204XE-DC, and AR2204XE do not support MAC address flapping detection.

 Copyright © Huawei Technologies Co., Ltd.

Format

loop-detect eth-loop { [**block-mac**] **block-time** *block-time* **retry-times** *retry-times* | **alarm-only** }

undo loop-detect eth-loop

Parameters

Parameter	Description	Value
block-mac	Blocks traffic from the flapping MAC address. If this parameter is not specified, the system blocks the interface where MAC address flapping occurs. When **block-mac** is specified, the *block-time* and *retry-times* parameters refer to the blocking time and number of retries for the blocked MAC address.	-
block-time *block-time*	Specifies the period during which an interface or a MAC address is blocked.	The value is an integer that ranges from 10 to 65535, in seconds.
retry-times *retry-times*	Specifies the number of detection attempts before an interface or a MAC address is permanently blocked.	The value is an integer that ranges from 1 to 5.
alarm-only	Indicates that the system only sends a trap message to the NMS but does not block an interface when detecting MAC address flapping on the interface.	-

Views

VLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

MAC address flapping occurs when a MAC address is learned by two interfaces in the same VLAN. The MAC address entry learned later replaces the earlier one. The **loop-detect eth-loop** command is used to check whether MAC address flapping occurs in a VLAN. When MAC address flapping occurs, the router performs the configured action.

You can use this command to enable MAC address flapping detection in the following scenarios:

- Loops in a VLAN cause MAC address flapping.
- Unauthorized users simulate MAC addresses of valid network devices to attack the router. This may cause MAC address flapping.

You can configure the router to block the MAC address or interface or only send a trap when MAC address flapping occurs. This function reduces impact on the router when MAC address flapping occurs.

If the router is configured to block the MAC address or interface, it performs the following action:

When detecting MAC address flapping in a VLAN, the router blocks the interface or MAC address for *block-time* seconds, and then checks for MAC address flapping again. If no MAC address flapping occurs within 20 seconds, the router unblocks the interface or MAC address and starts a new round of detection. If MAC address flapping is detected again within 20 seconds, the router repeats the MAC address flapping detection process for a certain number of times (specified by *retry-times*). If the MAC address flapping persists, the interface or MAC address is permanently blocked.

Precautions

After you run the command in a VLAN view, MAC address flapping is prevented only on the interfaces in this VLAN.

After an interface is permanently blocked, it no longer forwards packets or learns MAC addresses. To unblock the interface, run the **reset loop-detect eth-loop** command.

If you run the **loop-detect eth-loop** command multiple times in the same VLAN view, only the latest configuration takes effect.

Example

Enable MAC address flapping detection in VLAN 10 and configure the system to block the interface where MAC address flapping occurs. Set the interface blocking time to 10s and the number of detection attempts before the interface is permanently blocked to 3.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] loop-detect eth-loop block-time 10 retry-times 3
```

Related Topics

6.1.1 display loop-detect eth-loop

6.1.17 loop-detect eth-loop alarm-only

Function

The **loop-detect eth-loop alarm-only** command enables global MAC address flapping detection.

The **undo loop-detect eth-loop alarm-only** command disables global MAC address flapping detection.

By default, global MAC address flapping detection is disabled.

NOTE

AR2204-27GE-P, AR2204-51GE-R, AR2204-51GE-P and AR2204-51GE do not support the configuration.

Format

loop-detect eth-loop alarm-only

undo loop-detect eth-loop alarm-only

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MAC address flapping occurs when a loop occurs on a network or when unauthorized users send packets with bogus MAC addresses to attack the AR.

To prevent MAC address flapping, run the **loop-detect eth-loop alarm-only** command to enable global MAC address flapping detection. When the AR detects MAC address flapping, it sends a trap to the network management system (NMS). You can locate faults according to the trap messages.

Precautions

If the alarm function is disabled on the AR, the NMS cannot receive any trap message.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable global MAC address flapping detection on the AR.

```
<Huawei> system-view
[Huawei] undo loop-detect eth-loop alarm-only
```

Related Topics

6.1.1 display loop-detect eth-loop

6.1.18 mac-address

Function

The **mac-address** command adds a static MAC address entry or a blackhole MAC address entry.

The **undo mac-address** command deletes MAC address entries of a specified type.

NOTE

For the AR100 series, AR120 series, AR161, AR169, AR161G-L, AR161G-Lc, AR169CVW, AR169CVW-4B4S, AR161G-U, AR169W-P-M9, AR169RW-P-M9, AR169G-L, AR169EGW-L, AR169EW, AR169-P-M9, and AR1220E, when the source MAC addresses of packets are blackhole MAC addresses, the device forwards packets and does not discard them.

The WAN-side Interface of the AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204-27GE-P, AR2204E-D-27GE and AR2204-27GE, when the source MAC addresses of packets are blackhole MAC addresses, the device forwards packets and does not discard them.

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards forward packets with the source MAC address as the blackhole MAC address.

Format

mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id*

mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name* [**pe-vid** *pe-vid* [**ce-vid** { *ce-vid* | **any** }]]

mac-address static *mac-address* **virtual-ethernet** *interface-number* **atm** *interface-number* **pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } **vlan** *vlan-id*

mac-address blackhole *mac-address* { **vlan** *vlan-id* | **vsi** *vsi-name* }

undo mac-address blackhole [{ *mac-address* { **vlan** *vlan-id* | **vsi** *vsi-name* } } | **vlan** *vlan-id* | **vsi** *vsi-name*]

undo mac-address [*mac-address*] [**vlan** *vlan-id*]

undo mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name* [**pe-vid** *pe-vid* [**ce-vid** { *ce-vid* | **any** }]]

undo mac-address { **all** | **dynamic** | **static** | **security** | **sticky** } [*interface-type interface-number* | **vlan** *vlan-id*] *

undo mac-address { *interface-type interface-number* | **vlan** *vlan-id* } *

undo mac-address static *mac-address* **virtual-ethernet** *interface-number* **atm** *interface-number* **pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } **vlan** *vlan-id*

undo mac-address { **static** | **dynamic** | **all** } **virtual-ethernet** *interface-number* **atm** *interface-number* **pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } [**vlan** *vlan-id*]

undo mac-address { **static** | **dynamic** |**all** } [*interface-type interface-number* | **vsi** *vsi-name*] *

Parameters

Parameter	Description	Value
blackhole	Indicates blackhole MAC address entries.	-
static	Indicates static MAC address entries, that is, MAC address entries configured manually.	-
mac-address	Specifies the source or destination MAC address in a MAC address entry.	The value is in H-H-H format. H is a hexadecimal number of 4 digits. The MAC address cannot be FFFF-FFFF-FFFF, 0000-0000-0000, or a multicast MAC address.
interface-type interface-number	Specifies the outbound interface in a MAC address entry. ● *interface-type* specifies the type of the outbound interface. ● *interface-number* specifies the number of the outbound interface.	-
vlan *vlan-id*	Specifies the ID of the VLAN that the outbound interface belongs to.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a specified VSI instance. If the user device is connected to a PE by using a VSI, *vsi-name* can be specified in the **mac-address blackhole** command. The VSI specified by *vsi-name* must be existing. **NOTE** AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
pe-vid *pe-vid*	Specifies the outer VLAN tag.	The value is a decimal integer ranging from 1 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN tag. If **pe-vid** *pe-vid* or **ce-vid** *ce-vid* is configured, the corresponding interface must be a sub-interface that is bound to the VSI and configured with QinQ termination.	The value is a decimal integer ranging from 1 to 4094.
any	Indicates that the VLAN tag in an inner tag can be any value. If **any** is configured, the inner tag is not concerned. This reduces user configuration workload and system resource consumption.	-
peer *peer-ip*	Specifies the IP address of the device on the other end of the PW that corresponds to the MAC address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pw-id *pw-id*	Specifies the PW ID of the device on the other end of the PW that corresponds to the MAC address. Virtual Private LAN Service (VPLS) is a point-to-multipoint Layer 2 virtual private network (L2VPN) technology. A VPLS network consists of multiple VSIs connecting PEs. VSIs can map the physical links on a VPLS network to Pseudo Wires (PWs). To correctly delete the MAC addresses learned on a VPLS network, you need to specify **peer** *peer-ip* and **pw-id** *pw-id*.	The value is a decimal integer ranging from 1 to 4294967295.
virtual-ethernet *interface-number*	Specifies the number of the VE interface. When configuring a VE interface, you must configure an ATM PVC associated with the VE interface. The VE interface in this command must be a Layer 2 interface in a specified VLAN.	-
atm *interface-number*	Indicates the number of an Asynchronous Transfer Mode (ATM) interface. The Permanent Virtual Channel (PVC) of the ATM interface must be mapped to the VE interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pvc-name	Specifies the name of the PVC. The PVC name should be unique on the ATM interface.	The name is a string of 16 case-insensitive characters at most. Moreover, the value is an invalid VPI and VCI value pair, for example, "1/20".
vpi	Specifies the value of the Virtual Path Identifier (VPI) of an ATM network.	The value is an integer ranging from 0 to 4095.
vci	Specifies the value of the Virtual Channel Identifier (VCI) of an ATM network.	The value is an integer ranging from 0 to 2 or 5 to 65535. Generally, values from 0 to 31 for the VCI are reserved for special use. Not using them in the configuration is recommended. The VPI and VCI cannot both be 0.
all	Deletes all MAC address entries.	-
dynamic	Deletes dynamic MAC address entries, that is, the MAC address entries learned by an interface.	-
security	Deletes secure dynamic MAC address entries, that is, MAC addresses that an interface learns after port security is enabled.	-
sticky	Deletes sticky dynamic MAC address entries, that is, MAC addresses that an interface learns after the sticky MAC function is enabled.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MAC address entries are classified into the following types:

- Dynamic MAC address entries that are learned by an interface after MAC address learning is enabled.
- Static MAC address entries that are manually configured. They take precedence over dynamic MAC address entries.
- Blackhole MAC address entries that are manually configured. A data frame is discarded if the source or destination MAC address matches a blackhole MAC address entry.
- Secure dynamic MAC address entries that are learned by an interface after port security is enabled.
- Sticky MAC address entries that are learned by an interface after the sticky MAC function is enabled.

Functions of static and blackhole MAC address entries are:

- Static MAC address entries prevent bogus packets with trusted device MAC addresses sent from attackers and guarantee communication between the router and the upstream device or server.
- Blackhole MAC address entries prevent untrusted devices from attacking the router.

The **undo mac-address** command is used in the following scenarios:

- The upstream device or server has changed or the untrusted device has been removed, and the corresponding static MAC address entry or blackhole MAC address entry needs to be deleted.
- When the learned dynamic MAC address entries, secure dynamic MAC address entries, and sticky MAC address entries are not required, delete them and configure the device to learn them again.

Prerequisites

The interface has been added to a VLAN.

Precautions

You can configure multiple static MAC address entries or blackhole MAC address entries by running the mac-address command multiple times.

When the **undo mac-address blackhole** command is run and no parameter is specified, all the blackhole MAC address entry are deleted.

If you configure a static or blackhole MAC address entry when the MAC table is full, the router processes the MAC address entry as follows:

- If a dynamic MAC address entry with the same MAC address exists in the MAC address table, the router replaces the dynamic MAC address entry with the configured entry.
- If no dynamic MAC address entry with the same MAC address exists in the MAC address table, the MAC address entries cannot be added to the MAC address table.

 Copyright © Huawei Technologies Co., Ltd.

When using the **undo mac-address** command, pay attention to the following points:

- If *interface-type interface-number* is not specified, MAC address entries of a specified type on all interfaces are deleted.
- If **vlan** *vlan-id* is not specified, MAC address entries of a specified type in all VLANs are deleted.

Example

Add a static MAC address entry to the MAC address table. The destination MAC address is 0003-0003-0003. The outbound interface is ethernet2/0/0, which belongs to VLAN 4.

```
<Huawei> system-view
[Huawei] mac-address static 0003-0003-0003 ethernet 2/0/0 vlan 4
```

Configure a blackhole MAC address entry to discard the Ethernet frames whose destination MAC address is 0004-0004-0004 and VLAN ID is VLAN 5.

```
<Huawei> system-view
[Huawei] mac-address blackhole 0004-0004-0004 vlan 5
```

Related Topics

6.1.3 display mac-address

6.1.11 display mac-address summary

6.1.20 mac-address learning disable

6.1.19 mac-address aging-time

Function

The **mac-address aging-time** command sets the aging time of dynamic MAC address entries.

The **undo mac-address aging-time** command restores the default aging time of dynamic MAC address entries.

By default, the aging time of dynamic MAC address entries is 300 seconds.

Format

mac-address aging-time *aging-time*

undo mac-address aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of dynamic MAC address entries.	The value is an integer and its range depends on product models. ● On the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value can be 0 or in the range of 60 to 3825. ● On the AR2220, AR2220E, AR2240C, AR2240 and AR3200&AR3600 series, the value can be 0 or in the range of 60 to 1000000. **NOTE** The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards, the value can be 0 or in the range of 60 to 3825. The value is expressed in seconds. The default value is 300. The value 0 indicates that dynamic MAC address entries will not be aged out.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The network topology changes frequently, and the router will learn many MAC addresses. You can run the **mac-address aging-time** command to set a proper

aging time for dynamic MAC address entries so that aged MAC address entries are deleted from the MAC address table. This reduces MAC address entries in the MAC address table.

The system starts an aging timer for each dynamic MAC address entry. If a dynamic MAC address entry is not updated within a certain period (twice the aging time), the entry is deleted. If the entry is updated within this period, the aging timer of this entry is reset. If the aging time is short, the router is sensitive to network changes.

When setting the aging time of dynamic MAC address entries, follow these rules:

- Set a longer aging time on a stable network and a shorter aging time on an unstable network.
- The capacity of the MAC address table on a low end device is small; therefore, set a relatively short aging time on low end devices to save the MAC address table space.

Precautions

Dynamic MAC address entries are lost after system restart. Static MAC address entries and blackhole MAC address entries are not aged or lost.

If the aging time is 0, dynamic MAC addresses will not be aged out. In this case, MAC address entries increase sharply and the MAC address table will be full quickly.

If you run the **mac-address aging-time** command multiple times, only the latest configuration takes effect.

Example

Set the aging time of dynamic MAC address entries to 500 seconds.

```
<Huawei> system-view
[Huawei] mac-address aging-time 500
```

Related Topics

6.1.4 display mac-address aging-time

6.1.20 mac-address learning disable

Function

The **mac-address learning disable** command disables MAC address learning.

The **undo mac-address learning disable** command enables MAC address learning.

By default, MAC address learning is enabled.

NOTE

Only the AR2200&AR3200&AR3600 series support disable MAC address learning in a VLAN.

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support disable MAC address learning in a VLAN.

 Copyright © Huawei Technologies Co., Ltd.

Format

mac-address learning disable [**action** { **discard** | **forward** }]

undo mac-address learning disable

Parameters

Parameter	Description	Value
action	Indicates the action that the interface takes after MAC address learning is disabled. ● This parameter takes effect only in the interface view and port group view, and the specified interface must be a Layer 2 interface. ● You can use this parameter to determine whether packets are forwarded when the specified interface does not need to learn MAC addresses. By default, an interface forwards the packets carrying new MAC addresses after MAC address learning is disabled.	-
discard	Discards the packets whose source MAC addresses do not match the MAC address table.	-
forward	Forwards the packets according to the MAC address table.	-

Views

VLAN view, Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, bridge group view, Virtual-Ethernet interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want an interface to forward only packets with certain MAC addresses, use this command. For example, if an interface is connected to a server, configure a static MAC address entry with the MAC address of the server, and then disable MAC address learning and set the action to discard on the interface. The configuration prevents other servers or terminals from accessing the interface and improves network stability and security.

When a router with MAC address learning enabled receives an Ethernet frame, it records the source MAC address and inbound interface of the Ethernet frame in a MAC address entry. When receiving other Ethernet frames destined for this MAC address, the router forwards the frames through the corresponding outbound interface according to the MAC address entry. MAC address learning reduces broadcast packets on a network.

You can use the **mac-address learning disable** command to disable MAC address learning on an interface. The action performed on received packets can be set to **discard** or **forward**.

- When the action is set to **forward**, the router forwards packets according to the MAC address table. If a packet does not match any MAC address entry, the router broadcasts the packet.
- When the action is set to **discard**, the router searches for the source MAC address of the packet in the MAC address table. If the source MAC address is found in the MAC address table, the router forwards the packet according to the MAC address entry. If the source MAC address is not found, the router discards the packet. The default action is **forward**.

Prerequisites

Running the **portswitch** command in the VE interface view switches the VE interface from Layer 3 to Layer 2.

Precautions

The action cannot be configured in the VLAN view and bridge group view.

After MAC address learning is disabled on an interface, the device does not learn new MAC addresses on the interface, but untrusted terminals can still access the network.

Example

Disable MAC address learning in Eth0/0/2 interface.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/2
[Huawei-Ethernet0/0/2] mac-address learning disable
```

 Copyright © Huawei Technologies Co., Ltd.

6.1.21 mac-limit

Function

The **mac-limit** command configures a rule to limit the number of MAC addresses that can be learned.

The **undo mac-limit** command deletes the rule.

By default, the number of learned MAC addresses is not limited.

NOTE

The AR200, AR1200 do not support limiting the number of MAC addresses learned in a VLAN.

The 4GE-2S, 4ES2G-S, 4ES2GP-S and 9ES2 cards do not support limiting the number of MAC addresses learned.

The AR2204-51GE and AR120&AR160 series do not support limiting the number of MAC addresses learned.

Format

mac-limit { **action** { **discard** | **forward** } | **alarm** { **disable** | **enable** } | **maximum** *max-num* } *

undo mac-limit

Parameters

Parameter	Description	Value
action { **discard** | **forward** }	Indicates the action performed when the number of learned MAC address entries reaches the limit. • **discard**: discards packets with new source MAC addresses. • **forward**: forwards packets with new source MAC addresses but does not add the new MAC addresses to the MAC address table. **NOTE** This parameter cannot be specified in the VLAN view.	If no action is specified in the command, the default action **discard** is used.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
alarm { **disable** | **enable** }	Indicates whether the system generates an alarm when the number of learned MAC address entries reaches the limit. ● **disable**: indicates that no alarm is generated when the number of learned MAC addresses reaches the limit. ● **enable**: indicates that an alarm is generated when the number of learned MAC addresses reaches the limit.	If you do not set this parameter in the command, the alarm function is enabled by default.
maximum *max-num*	Sets the maximum number of MAC addresses that can be learned. **NOTE** If **maximum** is not set, you must run the **mac-limit** command with **maximum** specified. If you have run the **mac-limit** command to set the maximum number of MAC addresses that can be learned, you do not need to set **maximum** *max-num* when running this command again.	The value is a decimal integer and its range depends on product models. ● On the AR120&AR150&AR160&AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 0 to 2048. ● On the AR2220, AR2220E, AR2240C and AR2240 the value ranges from 0 to 4096. ● On the AR3200&AR3600 series the value ranges from 0 to 8192. The value 0 indicates that the highest rate of MAC address learning is not limited.

 Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view, Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mac-limit** command limits the number of access users and prevents attacks to the MAC address tables. You can enable the function to improve network security.

Precautions

The action cannot be set in the VLAN view.

The **mac-limit** and **port-security enable** commands cannot be used on the same interface.

Example

Configure the following MAC address learning rule on Ethernet2/0/0:

- The maximum number of learned MAC addresses is 30.
- When the number of learned MAC addresses exceeds the maximum, and an alarm is generated.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mac-limit maximum 30 alarm enable
```

6.1.22 port-security aging-time

Function

The **port-security aging-time** command sets the aging time of secure dynamic MAC addresses on an interface.

The **undo port-security aging-time** command restores the default configuration.

By default, secure dynamic MAC addresses will not be aged out.

NOTE

- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support port security.
- The AR100&AR120 series, AR161G-L, AR169-P-M9, AR161, AR161W, AR169, AR169G-L, AR169W, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR161G-U, AR169RW-P-M9, AR169W-P-M9, AR2204-24GE, AR2204-51GE, AR2204-48GE-P, AR169CVW, AR161EW-M1, AR169EGW-L, AR161G-Lc, AR169CVW-4B4S, AR161EW, AR169EW do not support port security.

 Copyright © Huawei Technologies Co., Ltd.

Format

port-security aging-time *time*

undo port-security aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time of secure dynamic MAC addresses.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **port-security enable** command to enable port security on an interface, MAC address entries learned by the interface are saved in the MAC address table as secure dynamic MAC addresses. The learned secure dynamic MAC addresses will not be aged by default. When the number of learned MAC addresses reaches the limit, the interface cannot learn new MAC addresses.

If MAC addresses learned by an interface can be trusted only for a certain period, run the **port-security aging-time** command to set the aging time of secure dynamic MAC addresses on the interface. Then secure dynamic MAC addresses can be aged out and the interface can learn new MAC addresses.

Prerequisites

Port security is enabled on the interface.

Precautions

If the aging time of secure dynamic MAC addresses on an interface is shorter than the global aging time of dynamic MAC addresses, secure dynamic MAC addresses are aged out when the global aging time expires.

If you run the **port-security aging-time** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the aging time of secure dynamic MAC addresses on Eth2/0/0 to 30 minutes.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port-security enable
[Huawei-Ethernet2/0/0] port-security aging-time 30
```

Related Topics

6.1.23 port-security enable

6.1.23 port-security enable

Function

The **port-security enable** command enables the port security function on an interface.

The **undo port-security enable** command disables the port security function on an interface.

By default, port security is disabled on an interface.

NOTE

- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support port security.
- The AR100&AR120 series, AR161G-L, AR169-P-M9, AR161, AR161W, AR169, AR169G-L, AR169W, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR161G-U, AR169RW-P-M9, AR169W-P-M9, AR2204-24GE, AR2204-51GE, AR2204-48GE-P, AR169CVW, AR161EW-M1, AR169EGW-L, AR161G-Lc, AR169CVW-4B4S, AR161EW, AR169EW do not support port security.

Format

port-security enable

undo port-security enable

Parameters

None

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After port security is enabled on an interface, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries. By default, secure dynamic MAC addresses will not be aged out. After the

device restarts, secure dynamic MAC address entries are lost and need to be relearned.

Port security has the following functions:

- Prevent unauthorized guests from using their computers to connect to an enterprise network.
- Prevent employees of a company from moving their computers without permission.

Precautions

The protection action, maximum number of learned secure MAC address entries, and sticky MAC function can be configured only after port security is enabled.

The **port-security enable** and **mac-limit maximum** cannot be used on the same interface.

The MUX VLAN and port security functions conflict on an interface. That is, the **port mux-vlan enable** and **port-security enable** commands cannot be used on the same interface.

Port security and MAC address authentication conflict on an interface; therefore, the **port-security enable** command cannot be used on the same interface.

Port security and 802.1x authentication conflict on an interface.

If port security is enabled after MAC address learning is disabled using the **mac-address learning disable** command, the port security function does not take effect. If port security is enabled before MAC address learning is disabled on an interface, the device no longer learns MAC addresses on the interface, but secure MAC addresses that have been learned are reserved.

Example

Enable port security on Ethernet2/0/1.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port-security enable
```

Related Topics

6.1.26 port-security protect-action

6.1.25 port-security max-mac-num

6.1.24 port-security mac-address sticky

6.1.24 port-security mac-address sticky

Function

The **port-security mac-address sticky** enables the sticky MAC function on an interface.

The **undo port-security mac-address sticky** disables the sticky MAC function on an interface.

By default, the sticky MAC function is disabled on an interface.

NOTE

- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support port security.
- The AR100&AR120 series, AR161G-L, AR169-P-M9, AR161, AR161W, AR169, AR169G-L, AR169W, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR161G-U, AR169RW-P-M9, AR169W-P-M9, AR2204-24GE, AR2204-51GE, AR2204-48GE-P, AR169CVW, AR161EW-M1, AR169EGW-L, AR161G-Lc, AR169CVW-4B4S, AR161EW, AR169EW do not support port security.

Format

port-security mac-address sticky [*mac-address* **vlan** *vlan-id*]

undo port-security mac-address sticky [*mac-address* **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a sticky MAC address entry.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. A MAC address cannot be FFFF-FFFF-FFFF.
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **port-security enable** command to enable port security on an interface, MAC address entries learned by the interface are stored in the MAC address table as secure dynamic MAC address entries.

After the sticky MAC function is enabled on an interface, the dynamic MAC addresses learned by the interface change to sticky MAC addresses. If the number of sticky MAC addresses does not reach the limit, the MAC addresses learned subsequently change to sticky MAC addresses. When the number of sticky MAC addresses reaches the limit, packets whose source MAC addresses do not match sticky MAC address entries are discarded. In addition, the system determines whether to send a trap message or shut down the interface according to the configured security protection action.

 Copyright © Huawei Technologies Co., Ltd.

After enabling the sticky MAC function on an interface, you can run the **port-security mac-address sticky** *mac-address* **vlan** *vlan-id* command to manually configure a sticky MAC address entry.

The sticky MAC function has the following functions:

- Prevent non-employees from using their own computers to access the company intranet without the permission of the network administrator.
- Prevent employees from moving network devices or computers of the company without the permission of the network administrator.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

If you run the **port-security mac-address sticky** [*mac-address* **vlan** *vlan-id*] command multiple times, multiple sticky MAC address entries are configured.

Example

Enable the sticky MAC function on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port-security enable
[Huawei-Ethernet2/0/0] port-security mac-address sticky
```

Related Topics

6.1.23 port-security enable
6.1.25 port-security max-mac-num

6.1.25 port-security max-mac-num

Function

The **port-security max-mac-num** command sets the maximum number of secure MAC addresses that can be learned on an interface.

By default, only one MAC addresses can be learned on an interface.

NOTE

- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support port security.
- The AR100&AR120 series, AR161G-L, AR169-P-M9, AR161, AR161W, AR169, AR169G-L, AR169W, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR161G-U, AR169RW-P-M9, AR169W-P-M9, AR2204-24GE, AR2204-51GE, AR2204-48GE-P, AR169CVW, AR161EW-M1, AR169EGW-L, AR161G-Lc, AR169CVW-4B4S, AR161EW, AR169EW do not support port security.

Format

port-security max-mac-num *max-number*

Parameters

Parameter	Description	Value
max-number	Specifies the maximum number of secure MAC addresses that can be learned by an interface.	The value is an integer and its range depends of product models. • On the AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204E-D-27GE, AR2204E, AR2204E-D, AR2202-48FE and AR2204 the value ranges from 1 to 1024. • On the AR2220, AR2220E, AR2240C, AR2240 and AR3200&AR3600 series, the value ranges from 1 to 4096.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security on an interface, you can run the **port-security max-mac-num** command to limit the number of MAC addresses that the interface can learn.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

If the sticky MAC function is disabled, *max-number* limits the number of secure dynamic MAC addresses learned by the interface and secure static MAC addresses configured manually.

 Copyright © Huawei Technologies Co., Ltd.

If the sticky MAC function is enabled, *max-number* limits the number of sticky MAC addresses learned by the interface, and sticky MAC addresses and secure static MAC addresses configured manually.

If you run the **port-security max-mac-num** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the maximum number of MAC addresses that can be learned by Ethernet2/0/0 to 5.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port-security enable
[Huawei-Ethernet2/0/0] port-security max-mac-num 5
```

Related Topics

6.1.23 port-security enable

6.1.24 port-security mac-address sticky

6.1.26 port-security protect-action

Function

The **port-security protect-action** command configures a protection action for the system to perform when the number of learned MAC addresses reaches the limit.

The **undo port-security protect-action** command restores the default protection action.

The default action is **restrict**.

NOTE

- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support port security.
- The AR100&AR120 series, AR161G-L, AR169-P-M9, AR161, AR161W, AR169, AR169G-L, AR169W, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR161G-U, AR169RW-P-M9, AR169W-P-M9, AR2204-24GE, AR2204-51GE, AR2204-48GE-P, AR169CVW, AR161EW-M1, AR169EGW-L, AR161G-Lc, AR169CVW-4B4S, AR161EW, AR169EW do not support port security.

Format

port-security protect-action { **protect** | **restrict** | **shutdown** }

undo port-security protect-action

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
protect	Discards packets with new source MAC addresses when the number of learned MAC addresses reaches the limit.	-
restrict	Discards packets with new source MAC addresses and sends a trap message when the number of learned MAC addresses reaches the limit.	-
shutdown	Set the interface status to error down and sends a trap message when the number of learned MAC addresses reaches the limit.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling port security, you can run the **port-security protect-action** command to configure the action performed on the interface when the number of learned MAC addresses reaches the limit.

The default action **restrict** is recommended. If the action is set to **shutdown** on an interface connected to a downstream device, the interface discards packets from trusted MAC addresses. Select the **shutdown** action only when the interface is directly connected to a user terminal.

Prerequisites

Port security has been enabled by using the **port-security enable** command on the interface.

Precautions

If the action is set to **shutdown**, the interface is shut down when the number of learned MAC addresses exceeds the limit.

If you run the **port-security protect-action** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the protection action on Ethernet2/0/0 to **protect**.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port-security enable
[Huawei-Ethernet2/0/0] port-security protect-action protect
```

Related Topics

6.1.23 port-security enable

6.1.24 port-security mac-address sticky

6.1.27 reset loop-detect eth-loop

Function

The **reset loop-detect eth-loop** command unblocks a blocked interface or MAC address in a specified VLAN.

NOTE

AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-R, AR2204-51GE-P and AR2204-51GE do not support the command.

Format

reset loop-detect eth-loop vlan *vlan-id* { **all** | **interface** *interface-type interface-number* | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Unblocks all the permanently blocked interfaces in the specified VLAN. If **all** is specified, the system unblocks all permanently blocked interfaces and MAC addresses in the specified VLAN, and then starts MAC address detection on the interfaces and MAC addresses.	-
interface *interface-type interface-number*	Specifies an interface in the specified VLAN. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface. If **interface** *interface-type interface-number* is specified, the system unblocks the specified interface, and then starts MAC address detection on the interface.	-
mac-address *mac-address*	Specifies a permanently blocked MAC address in the specified VLAN. If **mac-address** *mac-address* is specified, the system unblocks the specified MAC address, and then starts MAC address detection for the MAC address.	The value is in the H-H-H format. H is a hexadecimal number of 1 to 4 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is configured to block the MAC address or interface, it performs the following action:

When detecting MAC address flapping in a VLAN, the router blocks the interface or MAC address for *block-time* seconds, and then checks for MAC address flapping again. If no MAC address flapping occurs within 20 seconds, the router unblocks the interface or MAC address and starts a new round of detection. If MAC address flapping is detected again within 20 seconds, the router repeats the MAC address flapping detection process for a certain number of times (specified by *retry-times*). If the MAC address flapping persists, the interface or MAC address is permanently blocked.

After an interface is permanently blocked, it no longer forwards packets or learns MAC addresses. After MAC address flapping is removed, you can run the **reset loop-detect eth-loop** command to unblock the interface so that the interface can forward traffic and learn MAC addresses again.

Precautions

Before running the **reset loop-detect eth-loop** command, you can run the **display loop-detect eth-loop** command to view the result of MAC address flapping detection. According to the command output, you can find which interface or MAC address to unblock.

Example

Unblock all permanently blocked interfaces in VLAN 10.

```
<Huawei> system-view
[Huawei] reset loop-detect eth-loop vlan 10 all
```

Related Topics

6.1.1 display loop-detect eth-loop

6.1.16 loop-detect eth-loop

6.1.28 undo mac-address temporary

Function

The **undo mac-address temporary** command deletes all the temporary MAC address entries in the system.

Format

undo mac-address temporary

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the LPU or interface card is pulled out, the static MAC address entries configured on the interfaces are reserved as temporary MAC address entries. After the LPU or interface card is plugged again, the static MAC address entries are restored.

If the LPU or interface card is not plugged after being pulled out, the temporary MAC address entries become unnecessary and occupy the system resources. In this case, you can run the **undo mac-address temporary** command to delete all the temporary MAC address entries in the system.

Example

Delete all the temporary MAC address entries in the system.

```
<Huawei> system-view
[Huawei] undo mac-address temporary
```

6.1.29 undo mac-limit all

Function

The **undo mac-limit all** command deletes all MAC address limiting rules.

Format

undo mac-limit all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command deletes all the rules configured by the **mac-limit** command.

Precautions

Before using this command, run the **display mac-limit** command to check the MAC address limiting rules and confirm your operation.

Example

Delete all MAC address limiting rules.

```
<Huawei> system-view
[Huawei] undo mac-limit all
```

Related Topics

6.1.21 mac-limit

6.2 Link Aggregation Commands

NOTE

- AR100&AR120 series do not support link aggregation.
- Among the AR160 series routers, AR161, AR161G-L, AR161W, AR169, AR169G-L, AR169-P-M9, AR161G-U, AR169W-P-M9, AR169RW-P-M9, AR161EW, AR161EW-M1, AR161G-Lc, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L do not support link aggregation.

6.2.1 display eth-trunk

Function

The **display eth-trunk** command displays the Eth-Trunk configuration.

Format

display eth-trunk [*trunk-id* [**interface** *interface-type interface-number* | **verbose**]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	Set the value according to existing Eth-Trunk interfaces.
interface *interface-type interface-number*	Specifies a member interface. *interface-type* specifies the type of the member interface. *interface-number* specifies the number of the member interface.	-

Parameter	Description	Value
verbose	Displays the detailed configuration of a specified Eth-Trunk, including the Eth-Trunk traffic statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring an Eth-Trunk on a device, you can run the **display eth-trunk** command to check whether the Eth-Trunk configuration is correct.

When using the **display eth-trunk** command, pay attention to the following points:

- If no parameter is specified, the **display eth-trunk** command displays the configurations of all Eth-Trunks.
- If only *trunk-id* is specified, the **display eth-trunk** command displays the configuration of a specified Eth-Trunk.
- If *trunk-id* and **interface** *interface-type interface-number* are specified, the configuration of member interfaces of the specified Eth-Trunk is displayed.
- If *trunk-id* is specified and **verbose** is configured, the **display eth-trunk** command displays detailed configuration of a specified Eth-Trunk, including the Eth-Trunk traffic statistics.

Prerequisites

The Eth-Trunk has been correctly configured. If no Eth-Trunk is configured, when you run this command, the system displays an error message.

Precautions

If there are traffic statistics about many Eth-Trunks, you are advised to specify *trunk-id* or **interface** *interface-type interface-number* to filter output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly updated, and required information cannot be located.
- The system does not respond because of long-time information traverse and search.

Example

Display the configuration of Eth-Trunk 1 in manual load balancing mode.

```
<Huawei> display eth-trunk 1
Eth-Trunk1's state information is:
 WorkingMode: NORMAL            Hash arithmetic: According to SA-XOR-DA
 Least Active-linknumber:2      Max Bandwidth-affected-linknumber:8
 Operate Status: up             Number Of Up Port In Trunk:2
 --------------------------------------------------------------------------------
 PortName                  Status       Weight
 Ethernet2/0/1              Up           1
 Ethernet2/0/2              Up           1
```

Display the configuration of Eth-Trunk 1 in LACP mode.

```
<Huawei> display eth-trunk 1
Eth-Trunk1's state information is:
Local:
LAG ID: 1                  WorkingMode: STATIC
Preempt Delay: Disabled     Hash arithmetic: According to SA-XOR-
DA
System Priority: 32768      System ID: 781d-bacd-75fc
Least Active-linknumber: 1  Max Active-linknumber: 8
Operate status: up          Number Of Up Port In Trunk: 2
--------------------------------------------------------------------------------
ActorPortName   Status   PortType PortPri PortNo PortKey PortState
Weight
Ethernet2/0/1   Selected 100M     32768   9217   289     10111100  1
Ethernet2/0/2   Selected 100M     32768   9218   289     10111100  1

Partner:
--------------------------------------------------------------------------------
ActorPortName   SysPri   SystemID        PortPri PortNo PortKey PortState
Ethernet2/0/1   32768    781d-bacc-ac50  32768   5121   289
10111100
Ethernet2/0/2   32768    781d-bacc-ac50  32768   5122   289     10111100
```

Table 6-14 Description of the **display eth-trunk** command output

Item	Description
Local	Configuration of the local Eth-Trunk.
LAG ID	ID of the Eth-Trunk.
WorkingMode	Working mode of the Eth-Trunk: ● NORMAL: manual load balancing mode ● STATIC: LACP mode
Preempt Delay Time	Preemption delay: ● If LACP preemption is enabled, the value is displayed. ● If LACP preemption is disabled, the value is displayed as Disabled.
Hash arithmetic	Hash algorithm used for load balancing among member interfaces of the Eth-Trunk. The hash algorithm is configured by using the **load-balance** command.
System Priority/SysPri	System LACP priority.
System ID/SystemID	System ID.

Item	Description
Least Active-linknumber	Minimum number of active member links in Up state.
Max Active-linknumber	Maximum number of active member links in Up state.
Max Bandwidth-affected-linknumber	Maximum number of connections that affect the Eth-Trunk bandwidth.
Operate status	Eth-Trunk status: ● up ● down
Number Of Up Port In Trunk	Number of member interfaces in Up state in the Eth-Trunk.
ActorPortName/PortName	Name of a member interface.
Status	Status of the local member interface in LACP mode: ● Selected: A member interface in Selected state is active. ● Unselect: A member interface in Unselected state is inactive. Status of the local member interface in manual load balancing mode: ● Up: indicates that the interface is properly started. ● Down: indicates that the interface is faulty.
PortType	Type of the local member interface.
PortPri	LACP priority of the member interface.
PortNo	Number of the member interface in LACP mode.
PortKey	Key value of the member interface in LACP mode.
PortState	Status variable of the member interface.
Weight	Weight of the member interface.

Related Topics

6.2.11 eth-trunk
6.2.22 least active-linknumber
6.2.23 load-balance

6.2.2 display interface eth-trunk

Function

The **display interface eth-trunk** command displays Eth-Trunk status information.

Format

display interface eth-trunk [*trunk-id* | **main**]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer and varies according to device model: ● AR150&AR160 series: 0 to 3. ● AR200 series, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D and AR2202-48FE: 0 to 7. ● AR2204, AR2220E: 0 to 14. ● AR2220, AR2240C, AR2240 and AR3200&AR3600 series: 0 to 63. ● The value range on the 4GE-2S, 4ES2G-S, 4ES2GP-S and 9ES2 cards is 0 to 7.
main	Displays the status of and traffic statistics about an Eth-Trunk main interface. If **main** is not specified, the status of and traffic statistics about both an Eth-Trunk main interface and Eth-Trunk sub-interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display interface eth-trunk** command to view the status and weight of each Eth-Trunk member interface.

To monitor the status of an interface or locate an interface fault, you can use the **display interface eth-trunk** command to collect the status of and traffic statistics on the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Example

Display status information about Eth-Trunk 10.

```
<Huawei> display interface Eth-Trunk 10
Eth-Trunk10 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Eth-Trunk1 Interface
Switch Port, PVID :    1, TPID : 8100(Hex), Hash arithmetic : According to SA-XO
R-DA,The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 80fb-0635-45b3
Current system time: 2011-09-22 10:27:18
Input: 0 packets, 0 bytes
  Unicast:              0,  Multicast:              0
  Broadcast:             0,  Discard:                0
  Total Error:           0

Output: 0 packets, 0 bytes
  Unicast:              0,  Multicast:              0
  Broadcast:             0,  Discard:                0
  Total Error:           0

    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
-----------------------------------------------------
PortName                    Status      Weight
-----------------------------------------------------
-----------------------------------------------------
The Number of Ports in Trunk : 0
The Number of UP Ports in Trunk : 0
```

Table 6-15 Description of the **display interface eth-trunk** command output

Item	Description
Eth-Trunk10 current state	Status of Eth-Trunk 10: • UP: The interface is properly started. • DOWN: The interface is faulty. • Administratively Down: If the administrator uses the **shutdown (interface view)** command on the interface, the interface is Administratively Down.

Item	Description
Line protocol current state	Link layer protocol status of the interface: ● DOWN: The link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: The link layer protocol of the interface is running properly.
Description	Description of the interface.
Switch Port	Layer 2 interface.
PVID	ID of the VLAN to which the interface belongs
TPID	Type of frames that are supported on the interface. By default, this field displays 0x8100, indicating an 802.1Q frame. This field is valid only for a Layer 2 interface.
Hash arithmetic	Hash algorithm used for load balancing among Eth-Trunk member interfaces. The hash algorithm depends on the load balancing mode configured by using the **load-balance** command.
The Maximum Frame Length	MTU of the Eth-Trunk.
IP Sending Frames' Format	Format of Ethernet frames sent by the interface. The default frame format is Ethernet_II. An Ethernet interface supports the following frame formats: ● Ethernet_II ● Ethernet_SNAP ● 802.2 ● 802.3
Hardware address	MAC address of the Eth-Trunk.
Current system time	Last time when the Eth-Trunk became Down or Up. If a time zone is configured and the daylight saving time is used, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input	Statistics about packets received on the interface. • Unicast: Total number of unicast packets. • Multicast: Total number of multicast packets. • Broadcast: Total number of broadcast packets. • Discard: Number of discard packets. • Total Error: Number of error packets.
Output	Statistics about packets sent on the interface. • Unicast: Total number of unicast packets. • Multicast: Total number of multicast packets. • Broadcast: Total number of broadcast packets. • Discard: Number of discard packets. • Total Error: Number of error packets.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.
PortName	Name of the Eth-Trunk member interface.
Status	Status of the Eth-Trunk member interface.
Weight	Weight of the Eth-Trunk member interface in load balancing.
The Number of Ports in Trunk	Number of Eth-Trunk member interfaces.
The Number of UP Ports in Trunk	Number of Eth-Trunk member interfaces in Up state.

Related Topics

6.2.11 eth-trunk
5.1.13 reset counters interface

6.2.3 display lacp brief

Function

The **display lacp brief** command displays brief LACP information, including the LACP system priority and system ID.

Format

display lacp brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Devices at both ends of an Eth-Trunk compare LACP system priorities and system IDs to determine the Actor during LACP negotiation.

- By default, the LACP system priority is 32768, and the device with the smaller LACP system ID is used as the Actor.
- If LACP system priorities are changed using the **lacp priority** command, the device with the smaller LACP system priority is used as the Actor.

The **display eth-trunk** command can be used to check the LACP system priority and system ID only after an Eth-Trunk in LACP mode has been configured. This is inconvenient for network planning. To facilitate network planning, you can run the **display lacp brief** command to check the LACP system priority and system ID when no Eth-Trunk in LACP mode is configured.

Example

Display brief LACP information.

```
<Huawei> display lacp brief
System Priority:32768
System ID      :00e0-5958-ef00
```

 Copyright © Huawei Technologies Co., Ltd.

Table 6-16 Description of the **display lacp brief** command output

Item	Description
System Priority	LACP system priority. To configure the LACP system priority, run the **lacp priority** command.
System ID	System ID, which is the bridge MAC address of the device.

6.2.4 display lacp error packet

Function

The **display lacp error packet** command displays the content of recently received error packets.

Format

display lacp error packet

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

On a Layer 2 network running LACP, if a device is attacked by LACP error packets, you can run the **display lacp error packet** command to view the content of recently received. The command output helps locate faults and maintain devices.

Example

Display the content of recently received error packets.

```
<Huawei> display lacp error packet
-------------------------------------------------------
[Eth-Trunk 2, interface: Ethernet2/0/0, time: Feb 17 2012 12:03:08]:
0080c200    00020000    00000000    89020300    120000e0
00000000    00000000    00000000    01640c21    e3760100
0c020202    00000000    00000000    00000000    00000000
00000000    00000000    00000000    00000000    00000000
00000000    00000000    00000000    00000000    00000000
-------------------------------------------------------
```

Table 6-17 Description of the **display lacp error packet** command output

Item	Description
interface	Name of an interface that receives error packets.
time	Time when error packets were received.
<HHHHHHHH>&<1-n>	Details about error packets, in hexadecimal notation.

Related Topics

6.2.29 reset lacp statistics eth-trunk

6.2.5 display lacp statistics eth-trunk

Function

The **display lacp statistics eth-trunk** command displays statistics on received and sent Link Aggregation Control Protocol Data Units (LACPDUs) about an Eth-Trunk in LACP mode.

Format

display lacp statistics eth-trunk [*trunk-id* [**interface** *interface-type interface-number*]]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	Set the value according to existing Eth-Trunk interfaces.
interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be used only when the Eth-Trunk works in LACP mode. To change the working mode of an Eth-Trunk to the LACP mode, run the **mode lacp-static** command in the Eth-Trunk interface view.

To view the statistics on a specific Eth-Trunk, ensure that the Eth-Trunk has been created. To view the statistics on a specified Eth-Trunk member interface, ensure that the interface is added to the Eth-Trunk.

Example

Display the statistics on LACPDUs sent and received by member interfaces of Eth-Trunk 4.

```
<Huawei> display lacp statistics eth-trunk 4
 Eth-Trunk4's PDU statistic is:
 --------------------------------------------------------------------------------
 Port                LacpRevPdu   LacpSentPdu  MarkerRevPdu  MarkerSentPdu
 Ethernet2/0/1          7213         7213         0             0
 Ethernet2/0/2         20683         830          0             0
 Ethernet2/0/3         16356         677          0             0
```

Display the statistics on LACPDUs sent and received by member interface Ethernet2/0/1 of Eth-Trunk 4.

```
<Huawei> display lacp statistics eth-trunk 4 interface ethernet 2/0/1
 Ethernet2/0/1's PDU statistic is:
 --------------------------------------------------------------------------------
 Port                LacpRevPdu   LacpSentPdu  MarkerRevPdu MarkerSentPdu
 Ethernet2/0/1          7673         7673         0            0
```

Table 6-18 Description of the **display lacp statistics eth-trunk** command output

Item	Description
Port	Current member interface of the Eth-Trunk.
LacpRevPdu	Number of received LACPDUs.
LacpSentPdu	Number of sent LACPDUs.
MarkerRevPdu	Number of received MARKER packets.
MarkerSentPdu	Number of sent MARKER packets.

Related Topics

6.2.29 reset lacp statistics eth-trunk

6.2.6 display snmp-agent trap feature-name lacp all

Function

The **display snmp-agent trap feature-name lacp all** command displays all trap messages of the LACP module.

Format

display snmp-agent trap feature-name lacp all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The SNMP agent reports trap messages to the network management station so that the network management station can obtain the network status in a timely manner, and the network administrator can take measures accordingly.

The **display snmp-agent trap feature-name lacp all** command displays whether all trap functions of the LACP module are enabled.

Example

Display all trap messages of the LACP module.

```
<Huawei> display snmp-agent trap feature-name lacp all
-------------------------------------------------------------------------------
Feature name: LACP
Trap number : 3
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwLacpPartnerExpiredLoss        off                     on
hwLacpPDUChange                 off                     on
hwLacpPDUChangeResume           off                     on
```

Table 6-19 Description of the **display snmp-agent trap feature-name lacp all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the LACP module: ● hwLacpPartnerExpiredLoss: The local end receives a timeout packet from the remote end. ● hwLacpPDUChange: indicates that the status of a member interface of an Eth-Trunk interface in static LACP mode changed from selected to not selected due to an LACPDU change. ● hwLacpPDUChangeResume: indicates that the status of a member interface of an Eth-Trunk interface in static LACP mode changed from unselected to selected.
Default switch status	Whether the default trap function is enabled: ● on: The trap function is enabled. ● off: The trap function is disabled.
Current switch status	Whether the current trap function is enabled: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

6.2.30 snmp-agent trap enable feature-name lacp

6.2.7 display trunk index-map

Function

The **display trunk index-map** command displays the mapping between Eth-Trunk IDs and internal indexes and mapping between IP-Trunk IDs and internal indexes.

Format

display trunk index-map

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An ID is manually allocated to an Eth-Trunk or IP-Trunk during Eth-Trunk or IP-Trunk creation. For example, the ID of Eth-Trunk 1 is 1. In addition, the device also allocates an internal number, also called the index, to each Eth-Trunk. When allocating indexes, the device traverses indexes in ascending order. The unallocated index is used as the index of an Eth-Trunk; therefore, the mapping between Eth-Trunk IDs and indexes is unordered.

Example

Display the mapping between Eth-Trunk IDs and internal indexes and mapping between IP-Trunk IDs and internal indexes.

```
<Huawei> display trunk index-map
Index   Interface Name

-----------------------------
1       Eth-Trunk10
2       Eth-Trunk20
3       Eth-Trunk5
```

Table 6-20 Description of the **display trunk index-map** command output

Item	Description
Index	Index of the Eth-Trunk.
Interface Name	Name of the Eth-Trunk.

6.2.8 display trunk resource

Function

The **display trunk resource** command displays trunk resources that have been used on a device.

Format

display trunk resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To learn about used trunk resources, run the **display trunk resource** command to check the number of created trunks and the number of interfaces added to the trunk interface.

Example

Display trunk resources used on a device.

```
<Huawei> display trunk resource
Number of configured trunk interfaces is : 4
Interface          Member Count
------------------------------------------------------------
Eth-Trunk1          2
Eth-Trunk10         0
Eth-Trunk30         0
Eth-Trunk55         0
```

Table 6-21 Description of the **display trunk resource** command output

Item	Description
Number of configured trunk interfaces is	Number of configured trunk interfaces.
Interface	Trunk interface type: ● Eth-Trunk ● IP-Trunk
Member Count	Number of member interfaces added to a trunk interface.

6.2.9 display trunkfwdtbl eth-trunk

Function

The **display trunkfwdtbl eth-trunk** command displays the forwarding table of an Eth-Trunk.

Format

display trunkfwdtbl eth-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	Set the value according to existing Eth-Trunk interfaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An Eth-Trunk supports a maximum of eight physical member interfaces, which correspond to eight entries in the forwarding table. The eight entries correspond to hash key values 0 to 7. The system searches for outbound interfaces among active links based on HASH-KEY values.

Example

Display the forwarding table of an Eth-Trunk.

```
<Huawei> display trunkfwdtbl eth-trunk 1
 Eth-Trunk1's forwarding table is:
Ethernet2/0/0
Ethernet2/0/0
Ethernet2/0/0
Ethernet2/0/0
Ethernet2/0/0
Ethernet2/0/0
Ethernet2/0/0
Ethernet2/0/0
```

Table 6-22 Description of the **display trunkfwdtbl eth-trunk** command output

Item	Description
Eth-Trunk1's forwarding table	Forwarding entry of an Eth-Trunk.

Related Topics

6.2.11 eth-trunk

 Copyright © Huawei Technologies Co., Ltd.

6.2.10 display trunkmembership eth-trunk

Function

The **display trunkmembership eth-trunk** command displays information about Eth-Trunk member interfaces.

Format

display trunkmembership eth-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	Set the value according to existing Eth-Trunk interfaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an Eth-Trunk is successfully configured, you can run the **display trunkmembership eth-trunk** command to view the configuration of the Eth-Trunk and its member interfaces.

To monitor the status of an interface or locate an interface fault, you can use the **display trunkmembership eth-trunk** command to view detailed information about an Eth-Trunk and its member interfaces. The command output helps you can troubleshoot faults and check the member interface configuration.

Prerequisites

An Eth-Trunk has been correctly configured. If the Eth-Trunk is not created, the system displays an error when you run the **display trunkmembership eth-trunk** command.

Precautions

Before running the **display trunkmembership eth-trunk** command to view the configuration of the Eth-Trunk in LACP mode, ensure that the Eth-Trunk has been configured to work in LACP mode using the **mode lacp-static** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about member interfaces of Eth-Trunk 2.

```
<Huawei> display trunkmembership eth-trunk 2
Trunk ID: 2
Used status: VALID
TYPE: ethernet
Working Mode : Normal
Number Of Ports in Trunk = 2
Number Of Up Ports in Trunk = 2
Operate status: up

Interface Ethernet2/0/1, valid, operate up, weight=1
Interface Ethernet2/0/2, valid, operate up, weight=1
```

Table 6-23 Description of the display trunkmembership eth-trunk command output

Item	Description
Trunk ID	ID of the Eth-Trunk.
Used status	Whether the Eth-Trunk is available: ● VALID: The Eth-Trunk is available. ● INVALID: The Eth-Trunk is unavailable.
TYPE	Type of an Eth-Trunk.
Working Mode	Working mode of an Eth-Trunk. ● Normal: manual load balancing mode ● Static: LACP mode
Number Of Ports in Trunk	Number of interfaces that are added to the Eth-Trunk.
Number Of Up Ports in Trunk	Number of Up interfaces that are added to the Eth-Trunk.
Operate status	Eth-Trunk status: ● up ● down
Interface,valid,operate, weight	Detailed information about a member interface: ● Interface: indicates the interface type and number. ● valid: indicates that the interface is available. ● operate: indicates the status of the interface. ● weight: indicates the weight of the interface for load balancing.

Related Topics

6.2.11 eth-trunk
6.2.12 interface eth-trunk

 Copyright © Huawei Technologies Co., Ltd.

6.2.11 eth-trunk

Function

The **eth-trunk** command adds an interface to an Eth-Trunk.

The **undo eth-trunk** command removes an interface from an Eth-Trunk.

By default, an interface does not belong to any Eth-Trunk.

Format

eth-trunk *trunk-id*

undo eth-trunk

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer and varies according to device model: ● AR150&AR160 series: 0 to 3. ● AR200 series, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D and AR2202-48FE: 0 to 7. ● AR2204, AR2220E: 0 to 14. ● AR2220, AR2240C, AR2240 and AR3200&AR3600 series: 0 to 63. ● The value range on the 4GE-2S, 4ES2G-S, 4ES2GP-S and 9ES2 cards is 0 to 7.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

To improve the connection reliability and increase the bandwidth, you can use the **eth-trunk** command to bind multiple interfaces into an Eth-Trunk.

You can add an interface to an Eth-Trunk only after you run the **interface Eth-Trunk** command to create the Eth-Trunk.

 Copyright © Huawei Technologies Co., Ltd.

When you add an Ethernet interface to an Eth-Trunk, the interface must use default settings of some attributes. Otherwise, the interface cannot be added to the Eth-Trunk. The attributes include:

- Link type
- Maximum percentage of broadcast traffic
- Maximum percentage of multicast traffic
- Maximum percentage of unknown unicast traffic
- VLAN that the interface belongs to
- Interface priority
- Whether the interface allows BPDUs to pass through
- MAC address learning
- Adding the interface to a multicast group statically
- Discarding broadcast packets
- Discarding unknown multicast packets
- Discarding unknown unicast packets

The attributes on all member interfaces of an Eth-Trunk must be consistent and cannot be changed separately. If the preceding attributes of an Eth-Trunk are changed, the attributes of all the member interfaces are changed accordingly.

It is recommended that you run the **shutdown (interface view)** command to disable an interface before adding the interface to an Eth-Trunk. After adding interfaces at both ends of a link to an Eth-Trunk, run the **undo shutdown (interface view)** command to enable the interfaces. Otherwise, traffic interruption or broadcast storms may occur.

It is recommended that you run the **shutdown (interface view)** command to disable a member interface before running the **undo eth-trunk** command to remove the member interface from an Eth-Trunk.

The number of member interfaces of the Eth-Trunk on devices at both ends must be the same. The interfaces at both ends must be connected with straight-through cables.

NOTE

Only interfaces of the same type can be added to an Eth-Trunk.

Example

Add Ethernet2/0/0 to Eth-Trunk 2.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] eth-trunk 2
```

Related Topics

6.2.1 display eth-trunk

6.2.10 display trunkmembership eth-trunk

6.2.12 interface eth-trunk

5.1.16 shutdown (interface view)

 Copyright © Huawei Technologies Co., Ltd.

6.2.12 interface eth-trunk

Function

The **interface eth-trunk** command displays the view of an existing Eth-Trunk or creates an Eth-Trunk and displays its view.

The **undo interface eth-trunk** command deletes an Eth-Trunk.

By default, no Eth-Trunk is created.

Format

interface eth-trunk *trunk-id*[.*subnumber*]

undo interface eth-trunk *trunk-id*[.*subnumber*]

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer and varies according to device model: ● AR150&AR160 series: 0 to 3. ● AR200 series, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D and AR2202-48FE: 0 to 7. ● AR2204, AR2220E: 0 to 14. ● AR2220, AR2240C, AR2240 and AR3200&AR3600 series: 0 to 63. ● The value range on the 4GE-2S, 4ES2G-S, 4ES2GP-S and 9ES2 cards is 0 to 7.
subnumber	Specifies the ID of an Eth-Trunk sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If the specified Eth-Trunk already exists, the **interface eth-trunk** command directly displays the view of the specified Eth-Trunk.

You can delete an Eth-Trunk only when the Eth-Trunk does not contain any member interface.

NOTE

Eth-Trunk sub-interfaces can be created only when you run the **undo portswitch** command to switch the Eth-Trunk in Layer 3 mode.

Example

Create Eth-Trunk 2.

```
<Huawei> system-view
[Huawei] interface eth-trunk 2
[Huawei-Eth-Trunk2]
```

Related Topics

5.1.4 display interface

6.2.10 display trunkmembership eth-trunk

6.2.11 eth-trunk

5.1.11 interface

6.2.13 lacp collector delay

Function

The **lacp collector delay** command configures the value of the **CollectorMaxDelay** field in an LACPDU.

The **undo lacp collector delay** command restores the default value of the **CollectorMaxDelay** field in an LACPDU.

The default value of the **CollectorMaxDelay** field is 0 in an LACPDU.

Format

lacp collector delay *delay-time*

undo lacp collector delay

Parameters

Parameter	Description	Value
delay-time	Specifies the value of the **CollectorMaxDelay** field in an LACPDU.	The value is an integer that ranges from 0 to 65535, in 10 microseconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default value of the **CollectorMaxDelay** field in LACPDUs sent by the device of different versions to the connected non-Huawei device is different. This may cause high CPU usage. You can run the **lacp collector delay** command to set the value of the **CollectorMaxDelay** field in LACPDUs.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp-static** command.

Precautions

For a Huawei device, the valid value range of the **CollectorMaxDelay** field is 0 to 65535. Even though the member interfaces of the same Eth-Trunk receive LACPDUs with different **CollectorMaxDelay** values, the device can process the LACPDUs without deteriorating its CPU performance.

Example

Set the value of the **CollectorMaxDelay** field to 65535.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] mode lacp-static
[Huawei-Eth-Trunk1] lacp collector delay 65535
```

6.2.14 lacp preempt delay

Function

The **lacp preempt delay** command sets the LACP preemption delay.

The **undo lacp preempt delay** command restores the default LACP preemption delay.

By default, the LACP preemption delay is 30 seconds.

Format

lacp preempt delay *delay-time*

undo lacp preempt delay

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delay-time	Specifies the LACP preemption delay.	The value is an integer that ranges from 10 to 180, in seconds.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

To use this command, ensure that the following conditions are met:

- The Eth-Trunk has been configured to work in LACP mode using the **mode lacp-static** command in the Eth-Trunk interface view.
- Priority preemption has been enabled on the Eth-Trunk using the **lacp preempt enable** command in the Eth-Trunk interface view.

Link A replaces link B and becomes active after the preemption delay in the following situation:

1. LACP priority preemption is enabled and the **lacp preempt delay** command is used.
2. The faulty link (link A) with higher priority than that of the current active link (link B) recovers.
3. The number of current active links reaches the upper threshold.

If priority preemption is enabled but the preemption delay is not set, the interface with a higher priority preempts the interface with a lower priority according to the default preemption delay.

Example

Set the LACP preemption delay of Eth-Trunk 1 to 20 seconds.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] mode lacp-static
[Huawei-Eth-Trunk1] lacp preempt delay 20
```

Related Topics

6.2.15 lacp preempt enable

6.2.26 mode

 Copyright © Huawei Technologies Co., Ltd.

6.2.15 lacp preempt enable

Function

The **lacp preempt enable** command enables priority preemption for an Eth-Trunk in LACP mode.

The **undo lacp preempt enable** command disables priority preemption for an Eth-Trunk in LACP mode.

By default, priority preemption is disabled.

Format

lacp preempt enable

undo lacp preempt enable

Parameters

None

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

In LACP mode, when one of the active links fails, the system selects the link with the highest priority from backup links to replace the faulty one. When the faulty link recovers, the priority of this link is higher than the priority of the link that replaces itself, and priority preemption is enabled, the link becomes active again.

If priority preemption is disabled, the system does not re-select any active interface. The recovered link functions as the backup one.

When priority preemption is enabled, the system selects an active interface based on the LACP interface priority on the Actor.

Prerequisites

The LACP mode must have been configured using the **mode lacp-static** command in the Eth-Trunk interface view.

Precautions

To ensure that an Eth-Trunk works properly, enable or disable LACP preemption on both ends of the Eth-Trunk.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable priority preemption on Eth-Trunk 1.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] mode lacp-static
[Huawei-Eth-Trunk1] lacp preempt enable
```

Related Topics

6.2.14 lacp preempt delay

6.2.16 lacp priority

Function

The **lacp priority** command sets the LACP system or interface priority.

The **undo lacp priority** command restores the default LACP system or interface priority.

By default, the LACP system or interface priority is 32768.

Format

lacp priority *priority*

undo lacp priority

Parameters

Parameter	Description	Value
priority	Specifies the LACP priority. A smaller value indicates a higher LACP priority.	The value is an integer that ranges from 0 to 65535.

Views

System view, Ethernet interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LACP system priority is used to differentiate the local device and the remote device. The device of a higher LACP system priority is selected as the Actor of the

link aggregate group (LAG), and active interfaces are selected according to interfaces of the Actor.

The LACP interface priority is used to differentiate interfaces on a device. The interface of a higher priority is selected as the active interface.

If devices at both ends of an Eth-Trunk are not configured with LACP system priorities, the devices use the default LACP system priority 32768 and the device with a smaller MAC address is selected as the Actor.

Prerequisites

The interface has been added to the Eth-Trunk in LACP mode.

You can run the **mode lacp-static** command in the Eth-Trunk interface view to change the working mode of an Eth-Trunk to LACP.

Precautions

If the **max active-linknumber** command is executed in LACP mode to set the upper threshold for the number of active interfaces, you need to determine the active interfaces when the number of interfaces manually added to an LAG exceeds the upper threshold. Setting the LACP interface priority ensures that interfaces with higher priorities become active ones in LACP mode.

If the **max active-linknumber** command is not used, the upper threshold for the number of active interfaces is 8. When the number of interfaces manually added to an LAG is smaller than 8, you do not need to select active interfaces because all interfaces are active.

Example

Set the LACP system priority to 1.

```
<Huawei> system-view
[Huawei] lacp priority 1
```

Set the LACP priority of Ethernet2/0/0 to 1.

```
<Huawei> system-view
[Huawei] interface ethernet2/0/0
[Huawei-Ethernet2/0/0] lacp priority 1
```

Related Topics

6.2.25 max active-linknumber

6.2.17 lacp priority-command-mode

Function

The **lacp priority-command-mode** command sets a Link Aggregation Control Protocol (LACP) system priority configuration mode.

The **undo lacp priority-command-mode** command restores the default LACP system priority configuration mode.

By default, the LACP system priority configuration mode is **default**.

Format

lacp priority-command-mode { **default** | **system-priority** }

undo lacp priority-command-mode

Parameters

Parameter	Description	Value
default	Sets the LACP system priority configuration mode to **default**. In **default** mode, the LACP system priority is configured using the **lacp priority** command in the system view.	-
system-priority	Sets the LACP system priority configuration mode to **system-priority**. In **system-priority** mode, the LACP system priority is configured using the **lacp system-priority** command in the system view.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In versions earlier than V200R005C32, the LACP system priority is configured using the **lacp priority** command in the system view, and the LACP interface priority is configured using the same command but in the interface view.

A change in the LACP system priority will cause LACP renegotiation. During the renegotiation process, Eth-Trunk interfaces in LACP mode will go Down until the renegotiation succeeds, which may interrupt services. If the **lacp priority** command used to set the LACP interface priority is executed in the system view, the Eth-Trunk in LACP mode may alternate between Up and Down. To prevent this situation, run the **lacp priority-command-mode** command in the system view to set the configuration mode of the LACP system priority to **system-priority**. This mode can be used to differentiate the LACP system priority and LACP interface priority.

Precautions

- If you specify **default** in the command, the LACP system priority and LACP interface priority configurations still use the same command (**lacp priority** *priority*).

 Copyright © Huawei Technologies Co., Ltd.

- If you specify **system-priority** in the command, run the **lacp system-priority** *priority* command to configure the LACP system priority and run the **lacp priority** *priority* command to configure the LACP interface priority.

Example

Set the LACP system priority configuration mode to **system-priority**.

```
<Huawei> system-view
[Huawei] lacp priority-command-mode system-priority
```

6.2.18 lacp selected

Function

The **lacp selected** command configures a mode for selecting active interfaces of an Eth-Trunk in LACP mode.

The **undo lacp selected** command restores the default mode for selecting active interfaces of an Eth-Trunk in LACP mode.

By default, active interfaces are selected based on the LACP interface priority.

Format

lacp selected { **priority** | **speed** }

undo lacp selected

Parameters

Parameter	Description	Value
priority	Indicates that active interfaces are selected based on the LACP interface priority. The interfaces with high priorities are preferentially selected as active interfaces.	-
speed	Indicates that active interfaces are selected based on the interface rate. High-speed interfaces are preferentially selected as active interfaces.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined in LACP, active interfaces are selected based on the LACP interface priority by default. If member interfaces of an Eth-Trunk in LACP mode work at

different rates, low-speed interfaces may be selected as active interfaces. To enable the device to select high-speed interfaces as active interfaces, run the **lacp selected** command to set the mode of selecting active interfaces to **speed**.

To enable the device to select active interface based on the LACP interface priority, run the **lacp selected priority** command to set the mode of selecting active interfaces to **priority**.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp-static** command in the Eth-Trunk interface view.

Precautions

Active interfaces are selected based on the LACP interface priority by default. Changing the mode for selecting active interfaces may cause service interruptions for a short time. You are advised not to change the mode for selecting active interfaces during service transmission.

You are advised not to bundle interfaces working at different rates into an Eth-Trunk in LACP mode because the priority preemption function may become ineffective.

Example

Configure Eth-Trunk 1 in LACP mode and configure the device to select active interfaces based on the interface rate.

```
<Huawei> system-view
[Huawei] interface Eth-Trunk 1
[Huawei-Eth-Trunk1] mode lacp-static
[Huawei-Eth-Trunk1] lacp selected speed
```

Related Topics

6.2.26 mode

6.2.19 lacp src-mac

Function

The **lacp src-mac** command configures an interface or system MAC address as an LACPDU's source MAC address.

The **undo lacp src-mac** command restores the default source MAC address.

By default, the system MAC address is used as an LACPDU's source MAC address.

Format

lacp src-mac { **bridge** | **port** }

undo lacp src-mac

Parameters

Parameter	Description	Value
bridge	Configures the system MAC address as an LACPDU's source MAC address.	-
port	Configures an interface MAC address as an LACPDU's source MAC address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a Huawei device connects to a non-Huawei device through Eth-Trunk interfaces in static LACP mode, if the Huawei device uses the default system MAC address, whereas the non-Huawei device uses the MAC addresses of the Eth-Trunk member interfaces as LACPDUs' source MAC addresses, the non-Huawei device may consider the received LACPDUs with the same MAC address invalid and therefore discard them, leading to an LACP negotiation failure.

To ensure a successful LACP negotiation, run the **lacp src-mac port** command to configure the Huawei device to use interface MAC addresses as LACPDUs' source MAC addresses.

Example

Configure interface MAC addresses as LACPDUs' source MAC addresses.

```
<Huawei> system-view
[Huawei] lacp src-mac port
```

6.2.20 lacp system-priority

Function

The **lacp system-priority** command configures a Link Aggregation Control Protocol (LACP) system priority.

The **undo lacp system-priority** command restores the default LACP system priority.

The default LACP system priority is 32768.

Format

lacp system-priority *priority*

undo lacp system-priority

Parameters

Parameter	Description	Value
priority	Specifies an LACP system priority.	The value is an integer ranging from 0 to 65535. A smaller value indicates a higher LACP priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system priority is set to differentiate the priority of the local device and the peer device. The system of a higher priority is selected as the Actor of the link aggregate group (LAG), and active interfaces are selected according to interfaces of the Actor.

If the devices on both ends of the Eth-Trunk are not configured with system priorities, the devices use the default priority 32768. In this case, the Actor is selected according to the system MAC. The system with a smaller MAC is selected as the Actor.

Prerequisites

The **lacp priority-command-mode system-priority** command has been executed in the system view to set the configuration mode of the LACP system priority to **system-priority**.

Example

Set the LACP system priority to 10.

```
<Huawei> system-view
[Huawei] lacp priority-command-mode system-priority
[Huawei] lacp system-priority 10
```

6.2.21 lacp timeout

Function

The **lacp timeout** command configures the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs.

The **undo lacp timeout** command restores the default timeout interval.

By default, the timeout interval for an Eth-Trunk to receive LACPDUs is 90s.

 Copyright © Huawei Technologies Co., Ltd.

Format

lacp timeout { **fast** [**user-defined** *user-defined*] | **slow** }

undo lacp timeout

Parameters

Parameter	Description	Value
fast	Indicates that the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs is 3 seconds. If **fast** is specified, the remote device sends an LACPDU every 1 second. In this mode, the local device can quickly respond to LACPDUs from the remote device but consumes more system resources compared with the **slow** mode.	-
user-defined *user-defined*	Specifies the timeout interval for an Eth-Trunk to receive LACPDUs when **fast** is specified.	The value is an integer that ranges from 3 to 90, in seconds. The default value is 3.
slow	Indicates that the timeout interval for an Eth-Trunk in LACP mode to receive LACPDUs is 90 seconds. If **slow** is specified, the remote device sends an LACPDU every 30 seconds. In this mode, the local device responds to LACPDUs from the remote device slowly but consumes fewer system resources compared with the **fast** mode. The timeout interval on the two ends can be different. To facilitate maintenance, you are advised to set the same timeout interval at both ends.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two devices are connected through three GE interfaces at each end and the three GE interfaces are bundled into an Eth-Trunk, you can run the **mode lacp-**

static command to configure the Eth-Trunk to work in LACP mode and run the **least active-linknumber** *link-number* command to set the lower threshold for the number of active interfaces to 2.

If the Eth-Trunk on the local device cannot detect a self-loop or fault that occurred on a member interface in the LAG on the remote device, the local Eth-Trunk still has three member interfaces in Up state and the three member interfaces still load balance data, causing packet loss. To ensure reliable data transmission, run the **lacp timeout** command to set the timeout interval for the Eth-Trunk to receive LACPDUs. If a local member interface does not receive any LACPDU within the configured timeout interval, it becomes Down immediately and no longer forwards data.

The number of Up member interfaces does not fall below the configured lower threshold for the number of active interfaces, so the Eth-Trunk is still Up. In this case, data is load balanced between the two member interfaces in Up state and reliably transmitted to the remote end.

Prerequisites

The Eth-Trunk has been configured to work in LACP mode using the **mode lacp-static** command in the Eth-Trunk interface view.

Precautions

After the timeout interval is successfully configured, pay attention to the following points:

- If **fast** is specified, the remote device sends an LACPDU every 1 second.
- If **slow** is specified, the remote device sends an LACPDU every 30 seconds.

The timeout interval configured on an Eth-Trunk takes effect on all its member interfaces.

Example

Set the timeout interval for Eth-Trunk 1 to receive LACPDUs to 3 seconds.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] mode lacp-static
[Huawei-Eth-Trunk1] lacp timeout fast
```

Related Topics

6.2.26 mode

6.2.22 least active-linknumber

6.2.22 least active-linknumber

Function

The **least active-linknumber** command sets the lower threshold for the number of active interfaces in an Eth-Trunk.

The **undo least active-linknumber** command restores the default lower threshold for the number of active interfaces in an Eth-Trunk.

 Copyright © Huawei Technologies Co., Ltd.

By default, the lower threshold for the number of active interfaces in an Eth-Trunk is 1.

Format

least active-linknumber *link-number*

undo least active-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the lower threshold for the number of active interfaces in an Eth-Trunk.	The value is an integer that ranges from 1 to 8.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of active interfaces in an Eth-Trunk affects the status and bandwidth of the Eth-Trunk. The bandwidth of an Eth-Trunk is equal to the total bandwidth of all member interfaces in Up state.

The number of Up member links affects the status and bandwidth of an Eth-Trunk. To ensure that the Eth-Trunk functions properly and is less affected by member link status changes, set the following thresholds.

- Lower threshold for the number of active interfaces

  When the number of active interfaces falls below this threshold, the Eth-Trunk goes Down. This guarantees the Eth-Trunk a minimum available bandwidth.

  For example, if the Eth-Trunk is required to provide a minimum bandwidth of 2 Gbit/s and each member link's bandwidth is 1 Gbit/s, the lower threshold for the number of active interfaces must be set to 2 or larger.
- Upper threshold for the number of active interfaces

  When the number of active interfaces reaches this threshold, the bandwidth of the Eth-Trunk will not increase even if more member links go Up. This guarantees higher network reliability.

  To set the upper threshold for the number of active interfaces, use the **max active-linknumber** command.

To delete the configured lower threshold or restore the default lower threshold, use the **undo least active-linknumber** or **least active-linknumber 1** command.

Prerequisites

The Eth-Trunk has been correctly configured.

Precautions

If you run the **least active-linknumber** command multiple times, only the latest configuration takes effect.

After the upper threshold for the number of active interfaces is configured, the following situations may occur:

- The Eth-Trunk goes Down when the number of active interfaces falls below the configured lower threshold.
- The Eth-Trunk goes Up when the number of active interfaces reaches the configured lower threshold.

If the **max active-linknumber** command has been configured before you run the **least active-linknumber** command, ensure that the lower threshold for the number of active interface is smaller than or equal to the upper threshold for the number of active interfaces.

Example

Set the lower threshold for the number of active interfaces to 3.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] least active-linknumber 3
```

Related Topics

6.2.1 display eth-trunk

6.2.25 max active-linknumber

6.2.23 load-balance

Function

The **load-balance** command sets a load balancing mode of an Eth-Trunk.

The **undo load-balance** command restores the default load balancing mode of an Eth-Trunk.

By default, a Layer 2 Eth-Trunk uses the load balancing mode of **src-dst-mac**, and a Layer 3 Eth-Trunk uses the load balancing mode of **src-dst-ip**.

Format

load-balance { **dst-ip** | **dst-mac** | **src-ip** | **src-mac** | **src-dst-ip** | **src-dst-mac** }

undo load-balance

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dst-ip	Indicates load balancing based on destination IP addresses.	-
dst-mac	Indicates load balancing based on destination MAC addresses.	-
src-ip	Indicates load balancing based on source IP addresses.	-
src-mac	Indicates load balancing based on source MAC addresses.	-
src-dst-ip	Indicates load balancing based on source and destination IP addresses.	-
src-dst-mac	Indicates load balancing based on source and destination MAC addresses.	-

Views

System view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure proper load balancing between physical links of an Eth-Trunk and avoid link congestion, use the **load-balance** command to set the load balancing mode of the Eth-Trunk.

Load balancing is valid only for outgoing traffic; therefore, the load balancing modes for the interfaces at both ends of the link can be different and do not affect each other.

 Copyright © Huawei Technologies Co., Ltd.

You can set the load balancing mode based on traffic models. When a parameter of traffic changes frequently, you can set the load balancing mode based on this parameter to ensure that the traffic is load balanced evenly. For example, if IP addresses in packets change frequently, use the load balancing mode based on **dst-ip**, **src-ip**, or **src-dst-ip** so that traffic can be properly load balanced among physical links. If MAC addresses in packets change frequently and IP addresses are fixed, use the load balancing mode based on **dst-mac**, **src-mac**, or **src-dst-mac** so that traffic can be properly load balanced among physical links.

The device supports the following load balancing modes:

- dst-ip: load balancing based on destination IP address. In this mode, the system obtains the specified three bits from each of the destination IP address and the TCP or UDP port number in outgoing packets to perform the Exclusive-OR calculation, and then selects the outgoing interface from the Eth-Trunk table according to the calculation result.
- dst-mac: load balancing based on destination MAC address. In this mode, the system obtains the specified three bits from each of the destination MAC address, VLAN ID, Ethernet type, and incoming interface information to perform the Exclusive-OR calculation, and then selects the outgoing interface from the Eth-Trunk table according to the calculation result.
- src-ip: load balancing based on source IP address. In this mode, the system obtains the specified three bits from each of the source IP address and the TCP or UDP port number in incoming packets to perform the Exclusive-OR calculation, and then selects the outgoing interface from the Eth-Trunk table according to the calculation result.
- src-mac: load balancing based on source MAC address. In this mode, the system obtains the specified three bits from each of the source MAC address, VLAN ID, Ethernet type, and incoming interface information to perform the Exclusive-OR calculation, and then selects the outgoing interface from the Eth-Trunk table according to the calculation result.
- src-dst-ip: load balancing based on the Exclusive-OR result of the source IP address and destination IP address. In this mode, the system performs the Exclusive-OR calculation between the Exclusive-OR results of the source IP and destination IP modes, and then selects the outgoing interface from the Eth-Trunk table according to the calculation result.
- src-dst-mac: load balancing based on the Exclusive-OR result of the source MAC address and destination MAC address. In this mode, the system obtains three bits from each of the source MAC address, destination MAC address, VLAN ID, Ethernet type, and incoming interface information to perform the Exclusive-OR calculation, and then selects the outgoing interface from the Eth-Trunk table according to the calculation result.

Precautions

If you run the **load-balance** command multiple times, only the latest configuration takes effect.

On a Layer 2 Eth-Trunk, the **load-balance** command must be configured in the system view to configure a load balancing mode, do not support the **dst-ip**, **src-ip** and **src-dst-ip** parameters. On a Layer 3 Eth-Trunk, the **load-balance** command must be configured in the Eth-Trunk interface view to configure a load balancing mode.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160 series, AR1220C, AR1220-8GE, AR1220E, AR1220EVW, AR1220EV, AR2200 series (except AR2201-48FE, AR2202-48FE, AR2204, AR2220) do not support the load balancing mode configuration.

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support the load balancing mode configuration.

Example

Set the load balancing mode of Eth-Trunk 1 to **dst-mac**.

```
<Huawei> system-view
[Huawei] interface Eth-Trunk 1
[Huawei-Eth-Trunk1] load-balance dst-mac
```

Related Topics

6.2.2 display interface eth-trunk

6.2.24 mac-address (Eth-Trunk interface view)

Function

The **mac-address** command configures a MAC address for an Eth-Trunk interface.

The **undo mac-address** command restores the default MAC address of an Eth-Trunk interface.

By default, the MAC address of an Eth-Trunk interface is the system MAC address.

Format

mac-address *mac-address*

undo mac-address

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for an Eth-Trunk interface.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number, such as 00e0 or fc01. The MAC address cannot be FFFF-FFFF-FFFF, all 0s, or a multicast MAC address.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

By default, the MAC address of an Eth-Trunk interface is the system MAC address and may conflict with the MAC address of another interface.

If the MAC address of an Eth-Trunk interface conflicts with that of another interface, a loop may occur or traffic may fail to be forwarded. You can run the **mac-address** command to change the MAC address of the Eth-Trunk interface to prevent MAC address conflicts.

Precautions

This command can be configured only on Layer 3 Eth-Trunk interfaces.

After the MAC address of an Eth-Trunk interface is changed, the device proactively sends gratuitous ARP packets to update ARP entries on the remote device.

Example

Set the MAC address of Eth-Trunk1 to 0001-2345-abcd.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] undo portswitch
[Huawei-Eth-Trunk1] mac-address 0001-2345-abcd
```

Related Topics

6.2.2 display interface eth-trunk

6.2.25 max active-linknumber

Function

The **max active-linknumber** command sets the upper threshold for the number of active interfaces in an Eth-Trunk.

The **undo max active-linknumber** command restores the default upper threshold for the number of active interfaces in an Eth-Trunk.

By default, the upper threshold for the number of active interfaces in an Eth-Trunk is 8.

Format

max active-linknumber *link-number*

undo max active-linknumber

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
link-number	Specifies the upper threshold for the number of active interfaces.	The value is an integer that ranges from 1 to 8.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of active interfaces in an Eth-Trunk affects the status and bandwidth of the Eth-Trunk. The bandwidth of an Eth-Trunk is equal to the total bandwidth of all member interfaces in Up state.

The number of Up member links affects the status and bandwidth of an Eth-Trunk. To ensure that the Eth-Trunk functions properly and is less affected by member link status changes, set the following thresholds.

- Lower threshold for the number of active interfaces

  When the number of active interfaces falls below this threshold, the Eth-Trunk goes Down. This guarantees the Eth-Trunk a minimum available bandwidth.

  For example, if the Eth-Trunk is required to provide a minimum bandwidth of 2 Gbit/s and each member link's bandwidth is 1 Gbit/s, the minimum number of Up member links must be set to 2 or larger.

  To set the lower threshold for the number of active interfaces, run the **least active-linknumber** command.
- Upper threshold for the number of active interfaces

  When the number of active interfaces reaches this threshold, the bandwidth of the Eth-Trunk will not increase even if more member links go Up. The upper threshold is used to improve network reliability with assured bandwidth.

Prerequisites

The Eth-Trunk has been correctly configured.

Precautions

- If you run the **max active-linknumber** command multiple times, only the latest configuration takes effect.
- The **max active-linknumber** command is valid only in LACP mode.

 Copyright © Huawei Technologies Co., Ltd.

- If the number of member interfaces added to an Eth-Trunk is less than the upper threshold, there is no backup interface.
- After you run this command, if the number of current active interfaces reaches the upper threshold, new member interfaces function as the backup interfaces.
- If the **least active-linknumber** command has been configured before you run the **max active-linknumber** command, ensure that the maximum number of active member links is larger than or equal to the minimum number of active member links.
- In 1:1 static LACP mode, when an Eth-Trunk interface has only one active member link, if the master link becomes Down, the Down event is reported to the Eth-Trunk interface when any of the following occurs:
  - The timeout period (60s) for reporting the Down state elapses.
  - The backup link goes Up and becomes the master link.
  - The backup link fails and cannot go Up.
- When a Huawei switch connects to a non-Huawei device, if the maximum number of active links at both ends is smaller than the number of all active interfaces of the Eth-Trunk, a link is interrupted suddenly especially in 1:1 mode. As a result, LACP negotiation results at both ends are different and the Eth-Trunk in Down state cannot be restored. It is recommended that LACP preemption be enabled and the same preemption delay be set at both ends or the maximum number of active links be not set at both ends.

  NOTE

  The 1:1 mode indicates that the maximum number of active links at both ends of an Eth-Trunk is 1 and two member interfaces join an Eth-Trunk at both ends.

Example

Set the upper threshold for the number of active interfaces in Eth-Trunk 1 to 3.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] mode lacp-static
[Huawei-Eth-Trunk1] max active-linknumber 3
```

Related Topics

6.2.1 display eth-trunk

6.2.22 least active-linknumber

6.2.26 mode

Function

The **mode** command configures a working mode of an Eth-Trunk.

The **undo mode** command restores the default working mode of an Eth-Trunk.

By default, an Eth-Trunk works in manual load balancing mode.

Format

mode { **lacp-static** | **manual load-balance** }

undo mode

Parameters

Parameter	Description	Value
lacp-static	Indicates the LACP mode.	-
manual load-balance	Indicates the manual load balancing mode.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenarios

An Eth-Trunk can use the following working modes:

- LACP mode

  When the devices that are directly connected through an Eth-Trunk support LACP, you can run the **mode lacp-static** command to configure the Eth-Trunk to work in LACP mode. This mode can implement both load balancing and redundancy.

  In LACP mode, you must manually create an Eth-Trunk and add member interfaces to the Eth-Trunk. The difference between the LACP mode and manual load balancing mode is that active member interfaces are selected by sending LACP data units (LACPDUs). That is, when a group of interfaces are added to an Eth-Trunk, devices at both ends determine active and inactive interfaces by sending LACPDUs to each other.

- Manual load balancing mode

  When one of the devices at the two ends of an Eth-Trunk does not support LACP, run the **mode manual load-balance** command to configure the Eth-Trunk to work in manual load balancing mode. In addition, you can add multiple member interfaces to the Eth-Trunk to increase the bandwidth between the two devices and improve reliability.

  The manual load balancing mode is a basic link aggregation mode. In this mode, you must manually create an Eth-Trunk and add interfaces to the Eth-Trunk. LACP is not used.

  In manual load balancing mode, all active interfaces of the Eth-Trunk forward data and load balance traffic.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If you run the **mode** command multiple times, only the latest configuration takes effect.

Before changing the working mode of an Eth-Trunk, ensure that the Eth-Trunk contains no member interface.

When an Eth-Trunk changes from manual load balancing mode to LACP mode, the Eth-Trunk can contain member interfaces. When an Eth-Trunk changes from LACP mode to manual load balancing mode, ensure that the Eth-Trunk has no member interface.

Example

Configure Eth-Trunk 1 to work in manual load-balance mode.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] trunkport Ethernet 5/0/0 to 5/0/1
Info: This operation may take a few seconds. Please wait for a moment.........don
e.
[Huawei-Eth-Trunk1] mode manual load-balance
Warning: This command will interrupt services. The peer Eth-Trunk interface must
 also work in manual load balancing mode. All LACP configurations on this Eth-Tr
unk interface and its member interfaces have been deleted.
```

Related Topics

6.2.1 display eth-trunk

6.2.27 mtu (Eth-Trunk interface view)

Function

The **mtu** command sets the maximum transmission unit (MTU) for an Eth-Trunk.

The **undo mtu** command restores the default MTU of an Eth-Trunk.

By default, the MTU of an Eth-Trunk is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of an Eth-Trunk.	The value is an integer that ranges from 46 to 9202, in bytes.

Views

Eth-Trunk interface view, Eth-Trunk sub-interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IP layer controls the maximum length of outgoing packets each time. Any time the IP layer receives an outgoing IP packet, it checks which local interface the packet needs to be sent to and queries the MTU of the interface. Then the IP layer compares the MTU with the length of the outgoing packet. If the packet length is larger than the MTU, the IP layer fragments the packet to ensure that the length of each fragment is smaller or equal to the MTU.

If forcible unfragmentation is configured, some packets are lost during data transmission at the IP layer. To ensure that jumbo packets are not dropped during transmission, configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Prerequisites

The Eth-Trunk has been correctly configured.

Configuration Impact

If a small MTU is used and the size of packets is large, packets may be fragmented into many fragments and discarded by QoS queues.

Precautions

- You need to run the **mtu** command in the view of an Eth-Trunk to change its MTU. Do not run the **mtu** command on the Eth-Trunk member interfaces.
- After using the **mtu** command to change the MTU of an Eth-Trunk, change the MTU of the remote Eth-Trunk to ensure that the MTUs of both interfaces are the same. Otherwise, services may be interrupted.
- The MTU cannot be configured on a Layer 2 Eth-Trunk.
- The minimum MTU of an Eth-Trunk member interface is used as the MTU of the Eth-Trunk.

Example

Set the MTU of an Eth-Trunk to 1400 bytes.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] undo portswitch
[Huawei-Eth-Trunk1] mtu 1400
```

Related Topics

6.2.2 display interface eth-trunk

 Copyright © Huawei Technologies Co., Ltd.

6.2.28 reset lacp error packet statistics

Function

The **reset lacp error packet statistics** command clears statistics on error LACPDUs.

Format

reset lacp error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Applicable Scenario

To check statistics on error LACPDUs in a given period of time, run the **reset lacp error packet statistics** command to clear the existing statistics.

Precautions

The **reset lacp error packet statistics** command clears statistics on error LACPDUs. The cleared statistics cannot be restored. Exercise caution when you run this command.

Example

Clear the statistics about error LACPDUs.

```
<Huawei> reset lacp error packet statistics
```

6.2.29 reset lacp statistics eth-trunk

Function

The **reset lacp statistics eth-trunk** command clears statistics about LACPDUs on all Eth-Trunks in LACP mode, a specified Eth-Trunk in LACP mode, or a specified member interface.

Format

reset lacp statistics eth-trunk [*trunk-id* [**interface** *interface-type interface-number*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	Set the value according to existing Eth-Trunk interfaces.
interface *interface-type interface-number*	Specifies an Eth-Trunk member interface. *interface-type*: specifies the type of the interface. *interface-number*: specifies the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics about LACPDUs on a specific interface within a given period of time, you need to run the **reset lacp statistics eth-trunk** command to clear the existing statistics about LACPDUs on the interface.

When using the **reset lacp statistics eth-trunk** command, pay attention to the following points:

- If no parameter is specified, statistics about LACPDUs on all Eth-Trunks in LACP mode are cleared.
- If only *trunk-id* is specified, statistics about LACPDUs on the specified Eth-Trunk in LACP mode are cleared.
- If both *trunk-id* and **interface** *interface-type interface-number* are specified, statistics about LACPDUs on the specified member interface of the specified Eth-Trunk in LACP mode are cleared.

Prerequisites

- The Eth-Trunk has been created and configured to work in LACP mode.
- Member interfaces have been added to the Eth-Trunk.

Precautions

The **reset lacp statistics eth-trunk** command clears statistics about sent and received LACPDUs on all Eth-Trunks in LACP mode, a specified Eth-Trunk in LACP mode, or a specified member interface. The cleared statistics cannot be restored. Exercise caution when you run this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics about LACPDUs on all Eth-Trunks in LACP mode.

```
<Huawei> reset lacp statistics eth-trunk
```

Clear the statistics about LACPDUs on the member interface Ethernet2/0/0 of Eth-Trunk 1 in LACP mode.

```
<Huawei> reset lacp statistics eth-trunk 1 interface ethernet 2/0/0
```

6.2.30 snmp-agent trap enable feature-name lacp

Function

The **snmp-agent trap enable feature-name lacp** command enables the trap function for the LACP module.

The **undo snmp-agent trap enable feature-name lacp** command disables the trap function for the LACP module.

By default, the trap function is disabled for the LACP module.

Format

snmp-agent trap enable feature-name lacp [**trap-name** { **hwlacppartnerexpiredloss** | **hwLacpPDUChange** | **hwLacpPDUChangeResume** }]

undo snmp-agent trap enable feature-name lacp [**trap-name** { **hwlacppartnerexpiredloss** | **hwLacpPDUChange** | **hwLacpPDUChangeResume** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of LACP events of specified types.	-
hwLacpPartnerExpiredLoss	Enables the device to send a trap when the local end received a timeout packet from the remote end.	-
hwLacpPDUChange	Enables the device to send a trap when the status of a member interface of an Eth-Trunk interface in static LACP mode changed from selected to not selected.	-
hwLacpPDUChangeResume	Enables the device to send a trap when the status of a member interface of an Eth-Trunk interface in static LACP mode changed from unselected to selected.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

No parameter is available to enable all LACP traps. To enable the trap function of one or more events, specify **trap-name**.

Example

Enable the device to send traps when the local end received a timeout packet from the remote end.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name lacp trap-name hwLacpPartnerExpiredLoss
```

Related Topics

6.2.6 display snmp-agent trap feature-name lacp all

6.2.31 trunkport

Function

The **trunkport** command adds a member interface in the Eth-Trunk interface view.

The **undo trunkport** command deletes a member interface in the Eth-Trunk interface view.

By default, no member interface is added to an Eth-Trunk.

Format

trunkport *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>

undo trunkport *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-8>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-number2*]	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be larger than the value of *interface-number1*. *interface-number1* and *interface-number2* specify the range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified.	-

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

An Eth-Trunk contains a maximum of 8 member interfaces. The member interfaces in an Eth-Trunk must have the same type.

Example

Add Ethernet2/0/0 to Eth-Trunk 1.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] trunkport ethernet 2/0/0
```

Related Topics

6.2.1 display eth-trunk

6.2.11 eth-trunk

6.2.32 trunk member-port-inspect

Function

The **trunk member-port-inspect** command enables the detection of Eth-Trunk member interfaces.

The **undo trunk member-port-inspect** command disables the detection of Eth-Trunk member interfaces.

By default, the detection of Eth-Trunk member interfaces is disabled.

Format

trunk member-port-inspect

undo trunk member-port-inspect

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Each Eth-Trunk member interface transmits services through a separate path. Therefore, the delay, jitter, and packet loss ratio on each path is different. When the quality of services on Eth-Trunk member links deteriorates, run the **trunk member-port-inspect** command to enable the detection of member interfaces and then run the **ping** command to detect whether the network connectivity of each member interface is normal.

NOTE

The **trunk member-port-inspect** command detects all Layer 3 Eth-Trunk member interfaces. Therefore, to save system resources, you must disable the command immediately after the detection.

Example

Enable the detection of Eth-Trunk member interfaces.

```
<Huawei> system-view
[Huawei] trunk member-port-inspect
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.15.1 ping

6.2.33 trunk-member trap

Function

The **trunk-member trap in private-mib enable** command configures Eth-Trunk member interfaces to send traps through the proprietary MIB.

The **undo trunk-member trap in private-mib enable** command configures Eth-Trunk member interfaces to send traps through the public MIB.

By default, traps of Eth-Trunk member interfaces are sent through the public MIB.

Format

trunk-member trap in private-mib enable

undo trunk-member trap in private-mib enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an Eth-Trunk member interface changes from Up to Down or from Down to Up, the status change needs to be notified to users through traps so that the users can determine whether the device fault causes the status change.

To determine the Eth-Trunk that the member interface belongs to, you can run the **trunk-member trap in private-mib enable** command to configure Eth-Trunk member interfaces to send traps through the proprietary MIB. This is because the trap sent through a proprietary MIB carries information about the Eth-Trunk with the specified ID, whereas the trap sent through the public MIB does not carry information about the Eth-Trunk with specified ID.

Prerequisites

The Eth-Trunk has been correctly configured.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After the **trunk-member trap in private-mib enable** command is configured, traps are sent only through the proprietary MIB. That is, you need to view the sent traps through Huawei proprietary MIB.

Example

Configure Eth-Trunk member interfaces to send traps through the proprietary MIB.

```
<Huawei> system-view
[Huawei] trunk-member trap in private-mib enable
```

Related Topics

6.2.10 display trunkmembership eth-trunk

6.3 VLAN Configuration Commands

NOTE

- Among the AR160 series routers, only the AR161EW, AR161EW-M1, AR169EW, and AR169EGW-L do not support Super VLAN.
- Only the AR2204XE, AR2204XE-DC, AR2220, AR2220L, AR2220E, AR2240, AR2240C, AR3260, and AR3670 support MUX VLAN.
- Only the 8FE1GE, 24ES2GP, and 24GE cards support MUX VLAN.

6.3.1 8021q protocol

Function

The **8021q protocol** command changes the Tag Protocol Identifier (TPID) in an 802.1Q frame. The TPID specifies the protocol type in a VLAN tag.

The **undo 8021q protocol** command restores the default TPID in an 802.1Q frame.

By default, the TPID in an 802.1Q frame is 0x8100.

Format

8021q protocol *protocol-id*

undo 8021q protocol

Parameters

Parameter	Description	Value
protocol-id	Specifies the TPID in an 802.1Q frame.	The value is a hexadecimal integer that ranges from 0x600 to 0xFFFF.

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Devices from different vendors or in different network plans may use different values of TPID fields in VLAN tags of VLAN packets. When the TPID on the remote device is not 0x8100 and devices need to communicate, run the **8021q protocol** command to change the TPID to be the same as that on the remote device. The TPID in VLAN packets received and sent by a device interface is changed to be the configured TPID so that devices can communicate.

Precautions

The **8021q protocol** command can be executed on only Layer 3 Ethernet and GE interfaces.

The **8021q protocol** command is valid for only tagged VLAN packets.

The TPID value specified by the **8021q protocol** command must be different from TPID values of specific protocols. Otherwise, the interface cannot correctly classify protocol packets. The TPID value cannot be any of the values in the following table.

Table 6-24 Description of protocol types and values

Protocol Type	Value
ARP	0x0806
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
HGMP	0x88A7
Reserved	0xFFFD/0xFFFE/0xFFFF

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the TPID in a VLAN tag on GE1/0/0 to 0x9100.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] 8021q protocol 9100
```

6.3.2 access-vlan

Function

The **access-vlan** command adds one or more sub-VLANs to a super-VLAN.

The **undo access-vlan** command removes one or more sub-VLANs from a super-VLAN.

By default, no sub-VLAN is added to the super-VLAN.

Format

access-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo access-vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies a range of sub-VLAN IDs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only one VLAN is added to the super-VLAN. You can specify a maximum of 10 VLAN ID ranges at a time. The ranges cannot overlap.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094. Number of Sub-VLAN each Super-VLAN supports according to the different machines The value range varies according to devices: ● AR100&AR120&AR150&AR160&AR200&AR1200: 8. ● AR2200 series (except AR2220-AC, AR2220-DC, AR2220E and AR2240C): 8. ● AR2220-AC, AR2220-DC, AR2220E and AR2240C: 16. ● AR2204XE, AR2204XE-DC, AR3600: 32. ● Models equipped with the SRU40: 16. ● Models equipped with the SRU80/SRU200/SRU100E/SRU200E/SRU400: 32.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VLAN technology is widely applied to packet switching networks because it controls broadcast domains flexibly and is easy to deploy. Generally, a Layer 3 switch usually uses a Layer 3 logical interface in each VLAN to allow user hosts in different broadcast domains to communicate. This wastes IP addresses. The VLAN aggregation function is introduced to save IP addresses while implementing communication between VLANs.

The VLAN aggregation function associates a super-VLAN with multiple sub-VLANs. A VLANIF interface can be created in the super-VLAN and be configured with an IP address. Interfaces in all the sub-VLANs use this IP address as the gateway address to communicate with interfaces in other VLANs. This reduces subnet IDs, subnet default gateway addresses, and subnet broadcast IP addresses. In a word, the VLAN aggregation function allows different broadcast domains to use the same subnet address, implements flexible addressing, and saves IP addresses.

Prerequisites

The sub-VLANs to be added to the super-VLAN have been created.

The super-VLAN has been configured using the **aggregate vlan** command.

Before running the **access-vlan** command, delete VLANIF interfaces from all the sub-VLANs.

Follow-up Procedure

Configure the sub-VLANs to implement Layer 2 communication between them.

Precautions

The super-VLAN must be different from all its sub-VLANs.

A VLAN can be added to only one super-VLAN.

If you run the **access-vlan** command multiple times in the same VLAN view, all the specified VLANs are added to the super-VLAN.

Example

Add sub-VLAN20 and sub-VLAN30 to super-VLAN2.

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] aggregate-vlan
[Huawei-vlan2] access-vlan 20 30
```

Related Topics

6.3.3 aggregate-vlan
6.3.43 vlan
6.3.16 display vlan

6.3.21 interface vlanif
8.1.1 ip address
8.2.9 arp-proxy inter-sub-vlan-proxy enable

6.3.3 aggregate-vlan

Function

The **aggregate-vlan** command configures a VLAN as a super-VLAN.

The **undo aggregate-vlan** command cancels the configuration.

By default, no VLAN is configured as a super-VLAN.

Format

aggregate-vlan

undo aggregate-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VLAN technology is widely applied to packet switching networks because it controls broadcast domains flexibly and is easy to deploy. Generally, a Layer 3 switch usually uses a Layer 3 logical interface in each VLAN to allow user hosts in different broadcast domains to communicate. This wastes IP addresses. The VLAN aggregation function is introduced to save IP addresses while implementing communication between VLANs.

The VLAN aggregation function associates a super-VLAN with multiple sub-VLANs. A VLANIF interface can be created in the super-VLAN and be configured with an IP address. Interfaces in all the sub-VLANs use this IP address as the gateway address to communicate with interfaces in other VLANs. This reduces subnet IDs, subnet default gateway addresses, and subnet broadcast IP addresses. In a word, the VLAN aggregation function allows different broadcast domains to use the same subnet address, implements flexible addressing, and saves IP addresses.

Prerequisites

Before configuring a VLAN as a super-VLAN, delete all physical interfaces from the VLAN.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

VLAN 1 cannot be configured as a super-VLAN.

If a VLAN has been configured as a guest VLAN, it cannot be configured as a super-VLAN.

The super-VLAN must be different from all its sub-VLANs.

After a VLAN is configured as a super-VLAN, no physical interface can be added to the VLAN.

Example

Configure VLAN 2 as a Super-VLAN.

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] aggregate-vlan
```

Related Topics

6.3.16 display vlan

6.3.4 arp broadcast

Function

The **arp broadcast** command enables ARP broadcast on a VLAN tag termination sub-interface.

The **undo arp broadcast** command disables ARP broadcast on a VLAN tag termination sub-interface.

By default, ARP broadcast is enabled on a VLAN tag termination sub-interface.

Format

arp broadcast enable

undo arp broadcast enable

arp broadcast disable

undo arp broadcast disable

Parameters

None

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VLAN tag termination sub-interfaces discard broadcast packets after receiving the packets. To permit a VLAN tag termination sub-interface to forward broadcast packets, run the **arp broadcast enable** command on the sub-interface to enable ARP broadcast.

You can also use the **arp broadcast disable** command to disable ARP broadcast on a VLAN tag termination sub-interface, and run the **undo arp broadcast disable** command to enable ARP broadcast on a VLAN tag termination sub-interface.

Configuration Impact

When IP packets need to be sent from a VLAN tag termination sub-interface:

- The system discards IP packets when ARP broadcast is not enabled on the VLAN tag termination sub-interface.
- The system tags an ARP broadcast packet and forwards it through the VLAN tag termination sub-interface when ARP broadcast is enabled run on the VLAN tag termination sub-interface.

Precautions

When you enable or disable ARP broadcast on a VLAN tag termination sub-interface, the routing status of the sub-interface becomes Down and then Up. This may result in route flapping on the entire network, affecting services.

After the ARP broadcast function is enabled using the **arp broadcast enable** command, if a service packet is sent from a termination sub-interface but does not have an ARP entry, an ARP request is copied and sent in all VLANs of the sub-interface. If a large number of VLANs are configured, the number of ARP requests to be copied and sent is large, which may bring a heavy burden on the peer devices that receive the ARP requests. Consequently, the peer devices may encounter exceptions, such as high CPU usage and broadcast suppression. The local device may also fail to immediately send ARP requests as it is busy in processing packet copying, leading to ARP learning failures. To prevent this issue, you are advised to reduce the number of VLANs configured on sub-interfaces.

Example

Enable ARP broadcast on Ethernet2/0/0.1.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0.1
[Huawei-Ethernet2/0/0.1] dot1q termination vid 10
[Huawei-Ethernet2/0/0.1] arp broadcast enable
```

6.3.5 bandwidth (VLANIF interface view)

Function

The **bandwidth** command sets the bandwidth of a VLANIF interface.

The **undo bandwidth** command deletes the configured bandwidth of a VLANIF interface.

By default, the bandwidth of a VLANIF interface is not configured.

Format

bandwidth *bandwidth*

undo bandwidth

Parameters

Parameter	Description	Value
bandwidth	Specifies the bandwidth of a VLANIF interface.	The value is an integer ranges from 1 to 1000000, in Mbit/s.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

The **bandwidth** command ensures that the network management station (NMS) can obtain the bandwidth of a VLANIF interface. The NMS can check the interface bandwidth through **ifSpeed** and **ifHighSpeed** in **IF-MIB**.

- If the configured bandwidth is smaller than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as *bandwidth* x 1000 x 1000 and *bandwidth*.
- If the configured bandwidth is equal to or larger than 4000 Mbit/s, **ifSpeed** and **ifHighSpeed** are respectively displayed as 4294967295 (0XFFFFFFFF) and *bandwidth*.

Example

Set the bandwidth of VLANIF 2 to 10000 Mbit/s.

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] quit
[Huawei] interface vlanif 2
[Huawei-Vlanif2] bandwidth 10000
```

6.3.6 damping time

Function

The **damping time** command sets the VLAN damping time on a VLANIF interface, that is, the delay before reporting a VLAN Down event to the VLANIF interface.

The **undo damping time** command restores the default dumping time.

The default damping time on a VLANIF interface is 0 seconds. That is, the VLANIF interface is notified immediately after the VLAN becomes Down.

Format

damping time *delay-time*

undo damping time

Parameters

Parameter	Description	Value
delay-time	Specifies the delay before reporting the VLAN Down event to a VLANIF interface.	The value ranges from 0 to 20, in seconds. The default value is 0.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Software upgrade or active/standby switchover on the router may cause frequent status changes on VLANIF interfaces. To prevent network flapping, run the **damping time** command on VLANIF interfaces to configure the VLAN damping function.

When all interfaces in a VLAN become Down, the router waits for a period specified by *delay-time* and then reports the VLAN Down event to the VLANIF interface.

Precautions

If any interface in the VLAN becomes Up within the delay time, the VLANIF interface remains Up.

You can use the **display interface vlanif** command to view the VLAN damping time.

If you run the **damping time** command multiple times in the same VLANIF interface view, only the latest configuration takes effect.

Example

Set the VLAN damping time on VLANIF 10 to 10 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] interface vlanif 10
[Huawei-Vlanif10] damping time 10
```

Related Topics

6.3.11 display interface vlanif

6.3.7 description (VLAN view)

Function

The **description** command sets the description of a VLAN.

The **undo description** command restores the default description of a VLAN.

By default, the description of a VLAN shows the VLAN ID. For example, the description of VLAN 2 is "VLAN 0002".

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VLAN.	It is a string of 1 to 80 characters. The characters are case sensitive. Spaces are allowed.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command is used to set the description of a VLAN, which is convenient for identifying, memorizing, and maintaining the VLAN.

The **display vlan** *vlan-id* **verbose** command can display the description of a specified VLAN.

Precautions

Set different descriptions for VLANs to distinguish.

If you run the **description** command multiple times in the same VLAN view, only the last configuration takes effect.

Example

Set the description of VLAN 2 as "Huawei".

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] description Huawei
```

Related Topics

6.3.16 display vlan

6.3.8 description (VLANIF interface view)

Function

The **description** command set the description of a VLANIF interface.

The **undo description** command restores the default description of a VLANIF interface.

By default, the description of a VLANIF interface is in "HUAWEI, AR Series, Vlanif2 Interface" format.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VLANIF interface.	It is a string of 1 to 242 characters. The characters are case sensitive. Spaces are allowed.

Views

VLANIF interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To manage VLANIF interfaces conveniently, use the **description** command to set VLANIF interface descriptions. The description of a VLANIF interface helps you identify the VLANIF interface and know its functions.

You can use the **display interface vlanif** command to view the description of a VLANIF interface.

Precautions

The description of a VLANIF interface should provide useful information.

Set different descriptions for VLANIF interfaces to distinguish VLANIF interfaces.

If you run the **description** command multiple times in the same VLANIF interface view, only the latest configuration takes effect.

Example

Set the description of VLANIF 2 to Huawei.

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] quit
[Huawei] interface vlanif 2
[Huawei-Vlanif2] description Huawei
```

Related Topics

6.3.11 display interface vlanif

6.3.21 interface vlanif

6.3.9 display dot1q information

Function

The **display dot1q information termination** command displays the configuration of a dot1q sub-interface.

Format

display dot1q information termination [**interface** *interface-type interface-number* [.*subinterface-number*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Parameter	Description	Value
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring dot1q termination on sub-interfaces, run the **display dot1q information termination** command to view the sub-interfaces where dot1q termination is configured and configuration of the dot1q sub-interfaces.

Example

Display the configuration of all dot1q sub-interfaces.

```
<Huawei> display dot1q information termination
 Ethernet2/0/0.3
   Total QinQ Num: 1
   dot1q  termination vid 3
   Total vlan-group Num: 0
```

Table 6-25 Description of the display dot1q information command output

Item	Description
Ethernet2/0/0.3	Sub-interface name.
Total QinQ Num	Number of QinQ entries configured for user packets on a sub-interface.
dot1q termination vid 3	VLAN allowed by a sub-interface.
Total vlan-group Num	Number of VLAN groups configured on a sub-interface.

Related Topics

6.3.19 dot1q termination vid

 Copyright © Huawei Technologies Co., Ltd.

6.3.10 display qinq information

Function

Using the **display qinq information** command, you can view the names of all the interfaces configured with QinQ termination and the number of QinqQ on the interfaces.

Format

display qinq information termination [**interface** *interface-type interface-number* [.*subinterface-number*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
subinterface-number	Specifies the number of a sub-interface.	The value is an integer that ranges from 1 to 4096.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the qinq termination, you can run the **display qinq information** command to view the interfaces configured with qinq termination and the related configuration of qinq termination.

Example

Display all the sub-interfaces configured with QinQ termination.

```
<Huawei> display dot1q information termination
 Ethernet2/0/0.30
   Total QinQ Num: 1
   qinq termination pe-vid 300 ce-vid 200
   Total vlan-group Num: 0
```

Table 6-26 Description of the display qinq information command output

Item	Description
Ethernet2/0/0.30	Sub-interface name.

Item	Description
Total QinQ Num	Number of QinQ entries configured for user packets on a sub-interface.
qinq termination pe-vid 300 ce-vid 200	Set the encapsulation mode on Ethernet2/0/0.1 to QinQ and allow the packets with the outer VLAN tag 100 and inner VLAN tag 200 to pass through.
Total vlan-group Num	Number of VLAN groups configured on a sub-interface.

6.3.11 display interface vlanif

Function

The **display interface vlanif** command displays the status and configuration of a VLANIF interface.

Format

display interface vlanif [*vlan-id* | **main**]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer and the value range depends on the range of existing VLANIF interfaces. You can enter the question mark (?) to obtain the range of VLAN IDs.
main	Displays status and traffic statistics about a VLANIF interface. A VLANIF interface has no sub-interfaces. Status and traffic statistics about a VLANIF interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor an interface or locate an interface fault, you can use the **display interface vlanif** command to view the interface status, interface configuration, and traffic statistics on the interface.

Prerequisites

The specified VLANIF interface has been created.

Precautions

If *vlan-id* is not specified, the **display interface vlanif** command displays information about all VLANIF interfaces in the system.

Example

Display the status and configuration of VLANIF 3.

```
<Huawei> display interface vlanif 3
Vlanif3 current state : DOWN
Line protocol current state : DOWN
Description:HUAWEI, AR Series, Vlanif3 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-fc01-00e1
Current system time: 2007-09-12 20:21:13
    Input: 0 packets, 0 bytes
    Output: 0 packets, 0 bytes
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -


    Input bandwidth utilization  : --
    Output bandwidth utilization : --
```

Table 6-27 Description of the display interface vlanif command output

Item	Description
current state	Status of a VLANIF interface. The value is UP or Down.
Line protocol current state	Status of the link-layer protocol on a VLANIF interface. The value is UP or Down.
Description	Description of a VLANIF interface.
Route Port	Indicates that the interface is a Layer 3 interface.
The Maximum Transmit Unit	Specifies the MTU of a VLANIF interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet Address	IP address of a VLANIF interface. If the VLANIF interface does not have an IP address, the system displays "Internet protocol processing: disabled."
IP Sending Frames' Format	Encapsulation format of IP packets, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the VLANIF interface.
Current system time	Indicates the current system time. If a time zone is configured and the daylight saving time is used, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Input/Output	Number of packets and bytes received and sent by the VLANIF interface. **NOTE** This field is displayed only when the traffic statistics function is enabled on the VLANIF interface using the **statistic enable** command.
Last 300 seconds input/output rate	Rates of incoming and outgoing packets in the last 300 seconds, expressed in bytes per second and packets per second. **NOTE** This field is displayed only when the traffic statistics function is enabled on the VLANIF interface using the **statistic enable** command.
Input/Output peak rate/Record time	Maximum rate of incoming and outgoing packets and time when the maximum rate is reached. **NOTE** This field is displayed only when the traffic statistics function is enabled on the VLANIF interface using the **statistic enable** command.
Input/Output bandwidth utilization	Inbound/outbound bandwidth utilization on an interface.

Related Topics

6.3.8 description (VLANIF interface view)
6.3.21 interface vlanif
8.1.1 ip address
6.3.24 mtu (VLANIF interface view)

6.3.12 display mux-vlan

Function

Using the **display mux-vlan** command, you can view the MUX VLAN configuration.

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220, AR2220L, AR2220E, AR2240, AR2240C, AR3260, and AR3670 support MUX VLAN.

Only the 8FE1GE, 24ES2GP, and 24GE cards support MUX VLAN.

Format

display mux-vlan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring the MUX VLAN function, you can use the **display mux-vlan** command to verify the configuration. This command displays the principal VLAN ID, subordinate VLAN ID, VLAN type, and interfaces in each VLAN.

Precautions

If no MUX VLAN is configured by using the **mux-vlan** command, the **display mux-vlan** command does not display any information.

Example

Display the MUX VLAN configuration.

```
<Huawei> display mux-vlan
Principal Subordinate Type        Interface
-------------------------------------------------------------------------------
100       -          principal
100       120          separate     Ethernet2/0/0
100       130          group        Ethernet1/0/2
100       140          group        Ethernet1/0/3
-------------------------------------------------------------------------------
```

Table 6-28 Description of the display mux-vlan command output

Item	Description
Principal	ID of a principal VLAN.
Subordinate	ID of a subordinate VLAN
Type	Type of a VLAN. ● principal: indicates a principal VLAN. ● group: indicates a subordinate group VLAN. ● separate: indicates a subordinate separate VLAN.
Interface	Interfaces in a VLAN.

Related Topics

6.3.25 mux-vlan
6.3.43 vlan
6.3.42 subordinate separate
6.3.41 subordinate group

6.3.13 display port vlan

Function

The **display port vlan** command displays information about interfaces of the VLAN.

Format

display port vlan [*interface-type interface-number* | **active**] *

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface in the VLAN. If this parameter is not specified, information about all interfaces in the VLAN is displayed.	-
active	Indicates the interface information of dynamic entries in the VLAN.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display port vlan** command to view information about interfaces of the VLAN and check whether the VLAN is assigned by the command, protocols, or services. If a fault occurs on an interface, you can locate the fault based on the information about the interface and VLAN.

Prerequisite

A VLAN has been created and the Layer 2 interface has joined the VLAN.

Precautions

If a large number of mappings between interfaces and VLANs exist on the device, you are advised to specify the interface or **active** to filter the command output. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is repeatedly refreshed, causing required information to fail to be obtained.
- The system does not respond because of long-time information traverse and search.

Example

Display information about interfaces that belong to each VLAN on the device.

```
<Huawei> display port vlan
Port                Link Type    PVID  Trunk VLAN List
--------------------------------------------------------------------------------
Ethernet2/0/0          hybrid       1     -
Ethernet2/0/1          hybrid       1     -
Ethernet2/0/2          hybrid       1     -
Ethernet2/0/3          hybrid       1     -
Ethernet2/0/4          hybrid       1     -
Ethernet2/0/5          access       3     -
Ethernet2/0/6          hybrid       1     -
Ethernet2/0/7          hybrid       1     -
```

Table 6-29 Description of the display port vlan command output

Item	Description
Port	Indicates the type and number of the interface.
Link Type	Indicates the types of the interface link.
PVID	Indicates the default VLAN ID of the interface. By default, VLAN 1 is the default VLAN of all interfaces.

Item	Description
Trunk VLAN List	• Indicates the VLAN IDs that are dynamically added by an interface. • Indicates the VLAN IDs of packets that are statically configured to pass through an interface.

Related Topics

6.3.32 port link-type

6.3.14 display sub-vlan

Function

The **display sub-vlan** command displays information about sub-VLAN entries.

Format

display sub-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a sub-VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VLAN aggregation is configured on a device, you can determine whether VLAN aggregation has been correctly configured by running the **display sub-vlan** command to check information about sub-VLANs and check which sub-VLANs are contained in a super-VLAN.

When using the **display sub-vlan** command, note the following issues:

- If *vlan-id* is not specified, information about all sub-VLANs on the device is displayed.
- If *vlan-id* is specified, information about a specific sub-VLAN is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Before running the **display sub-vlan** command, ensure that the device is configured with sub-VLANs. Otherwise, no command output is displayed.

Example

Display information about all sub-VLANs.

```
<Huawei> display sub-vlan
VLAN ID   Super-VLAN
--------------------------------------------------------------------------------
10        40
20        40
30        40
```

Table 6-30 Description of the **display sub-vlan** command output

Item	Description
VLAN ID	Existing sub-VLAN on the device.
Super-VLAN	Super-VLAN that the sub-VLAN belongs to.

Related Topics

6.3.43 vlan

6.3.15 display super-vlan

Function

The **display super-vlan** command displays information about super-VLAN entries.

Format

display super-vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID of a super-VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VLAN aggregation is configured on a device, you can determine whether VLAN aggregation has been correctly configured by running the **display super-vlan** command to check information about super-VLANs and check which sub-VLANs are contained in a super-VLAN.

When using the **display super-vlan** command, note the following issues:

- If *vlan-id* is not specified, information about all super-VLANs on the device is displayed.
- If *vlan-id* is specified, information about a specific super-VLAN is displayed.

Before running the **display super-vlan** command, ensure that the device is configured with super-VLANs. Otherwise, no command output is displayed.

Example

Display information about all super-VLANs.

```
<Huawei> display super-vlan
VLAN ID   Sub-VLAN
-------------------------------------------------------------------------------
40        10 20 30
```

Table 6-31 Description of the **display super-vlan** command output

Item	Description
VLAN ID	Existing super-VLAN on the device.
Sub-VLAN	Sub-VLAN in the super-VLAN.

Related Topics

6.3.43 vlan

6.3.16 display vlan

Function

The **display vlan** command displays information about VLANs.

Format

display vlan [{ *vlan-id* | **vlan-name** *vlan-name* } [**verbose**]]

display vlan [*vlan-id1* [**to** *vlan-id2*] | **brief** | **summary**]

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
vlan-id1 [**to** *vlan-id2*]	Specifies a range of VLAN IDs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*. If **to** *vlan-id2* is not specified, only information about the VLAN specified by *vlan-id1* is displayed.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.
summary	Displays summary of all VLANs.	-
verbose	Displays detailed information about a specified VLAN. If **verbose** is not specified, only brief information about the VLAN is displayed.	-
vlan-name *vlan-name*	Specifies a VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
brief	Indicates brief information about VLANs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display vlan** command displays VLAN configuration or packet statistics on interfaces in a VLAN.

Precautions

If no parameter is specified, brief information about all VLANs is displayed.

Example

Display brief information about all VLANs.

```
<Huawei> display vlan
* : management-vlan
--------------------
The total number of vlans is : 6
VLAN ID Type         Status   MAC Learning Broadcast/Multicast/Unicast Property
--------------------------------------------------------------------------------
1       common       enable   enable       forward   forward   forward default
10      common       enable   enable       forward   forward   forward default
100     common       enable   enable       forward   forward   forward default
199     common       enable   enable       forward   forward   forward default
900     common       enable   enable       forward   forward   forward default
4094    common       enable   enable       forward   forward   forward default
```

Display detailed information about VLAN 100.

```
<Huawei> display vlan 100 verbose
* : Management-VLAN
--------------------
  VLAN ID                     : 100
  VLAN Name                   :
  VLAN Type                   : Common
  Description                 : VLAN 0100
  Status                      : Enable
  Broadcast                   : Enable
  MAC Learning                : Enable
  Smart MAC Learning          : Disable
  Current MAC Learning Result : Enable
  Statistics                  : Disable
  Property                    : Default
  VLAN State                  : Down
  ----------------
  Tagged        Port: Ethernet2/0/0
  ----------------
  Active  Tag   Port: Ethernet2/0/0
--------------------
Interface                   Physical
Ethernet2/0/0                    DOWN
```

Display summary of all VLANs.

```
<Huawei> display vlan summary
static vlan:
Total 7 static vlan exist(s).
1 to 2 10 45 56 100 111
dynamic vlan:
Total 0 dynamic vlan exist(s).
reserved vlan:
Total 0 reserved vlan exist(s).
```

Display brief of all VLANs.

```
<Huawei> display vlan brief
U:Up;D:Down;TG:Tagged;UT:Untagged;

VID  Name            Status  Ports
--------------------------------------------------------------------------------
1                  enable  UT: Eth2/0/3(U) Eth2/0/5(D) Eth2/0/6(D)
                           Eth2/0/7(D) Eth-Trunk1(D) Eth-Trunk2(D)
                           Eth-Trunk3(D) Eth-Trunk6(D) Eth-Trunk7(D)
10                 enable  UT: Eth2/0/0(U) Eth2/0/4(D)
11                 enable  UT: Eth-Trunk5(D)
                       TG: Eth2/0/7(D)
12                 enable
20                 enable
100                 enable  UT: Eth2/0/1(U)
200                 enable  UT: Eth2/0/2(U)
470                 enable
```

Table 6-32 Description of the display vlan command output

Item	Description
: management-vlan/ : Management-VLAN	Management VLAN.
The total number of vlans is	Total number of VLANs.
VLAN ID/VID	ID of a VLAN.
VLAN Type/Type	Type of a VLAN: ● Mux: principal VLAN used in the MUX VLAN function ● Mux-sub: subordinate VLAN used in the MUX VLAN function ● Common: common VLAN ● *Common: management VLAN
Status	Status of a VLAN. The value is always **Enable**.
Broadcast	Whether the broadcast function is enabled in a VLAN: ● Disable: The broadcast function is disabled. ● Enable: The broadcast function is enabled.
MAC Learning	Whether MAC address learning is enabled: ● disable: MAC address learning is disabled. ● enable: MAC addresses learning is enabled.
Broadcast/Multicast/Unicast	Whether Broadcast/Multicast/Unicast message is retransmitted.

Item	Description
Property	Property of a VLAN: ● Default: default VLAN ● MulticastVlan: multicast VLAN ● UserVlan: user VLAN
VLAN Name/Name	Name of a VLAN.
Description	Description of a VLAN.
Smart MAC Learning	Whether smart MAC address learning is enabled: ● disable: Smart MAC address learning is disabled. ● enable: Smart MAC addresses learning is enabled.
Current MAC Learning Result	MAC address learning result.
Statistics	Whether the traffic statistics function is enabled in a VLAN: ● disable: Traffic statistics function is disabled. ● enable: Traffic statistics function is enabled.
VLAN State	Status of the VLAN: ● Up ● Down The status of a VLAN is determined by the status of member interfaces in the VLAN. A VLAN is Up only when at least one member interface in the VLAN is Up.
Tagged Port	(Untagged Port). Interfaces that are manually added to a VLAN in tagged or untagged mode.
Active Tag Port	(Active Untag Port). Active interfaces that join a VLAN in tagged or untagged mode.
static vlan	VLANs that are created manually.
dynamic vlan	VLANs that are learned dynamically.
reserved vlan	VLANs that are reserved for certain functions.
U: Up	The interface is Up.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
D: Down	The interface is Down.
TG: Tagged	Tagged packets.
UT: Untagged	Untagged packets.
Ports	Interfaces in a VLAN.

Related Topics

6.3.7 description (VLAN view)
6.3.37 reset vlan statistics
6.3.43 vlan

6.3.17 display vlan priority

Function

Using the **display vlan priority** command, you can view the 802.1p priorities of VLANs.

Format

display vlan { *vlan-id* | **all** } **priority**

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID. If this parameter is specified, the 802.1p priority of the specified VLAN is displayed.	The value is an integer that ranges from 1 to 4094.
all	Displays 802.1p priorities of all VLANs.	-

Views

All views

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **display vlan priority** command displays the 802.1p priority of a specified VLAN or 802.1p priorities of all VLANs.

Example

Display 802.1p priorities of all VLANs.

```
<Huawei> display vlan all priority

------------------------------
 VLAN ID       Priority
------------------------------
    11          3
------------------------------
Total items displayed = 1
```

Table 6-33 Description of the display vlan priority command output

Item	Description
VLAN ID	ID of a VLAN.
Priority	802.1p priority of a VLAN.
Total items displayed	Number of VLAN-priority items displayed.

Related Topics

6.3.44 vlan priority

6.3.18 display vlan-range

Function

The **display vlan-range** command displays the range of VLANs that can be created on the 4GE-2S interface card.

Format

display vlan-range slot *slot-id*

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID. The 4GE-2S interface card must be in the slot.	The value is an integer that ranges from 1 to 15.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **display vlan-range** command to view the range of VLANs that can be created on the 4GE-2S interface card.

Example

Display the range of VLANs that can be created on the 4GE-2S interface card in slot 6.

```
<Huawei> system-view
[Huawei] display vlan-range slot 6
 ----------------The board supports the following VLAN group----------------
 0001 0100 0101 0102 0103 0104 0105 0106 0107 0108 0109 0110 0111 0112 0113
 0114 0115 0116 0117 0118 0119 0120 0121 0122 0123 0124 0125 0126 0127 0128
 0129 0130 0131 0132 0133 0134 0135 0136 0137 0138 0139 0140 0141 0142 0143
 0144 0145 0146 0147 0148 0149 0150 0151 0152 0153 0154 0155 0156 0157 0158
 0159 0160 0161 0162 0163 0164 0165 0166 0167 0168 0169 0170 0171 0172 0173
 0174 0175 0176 0177 0178 0179 0180 0181 0182 0183 0184 0185 0186 0187 0188
 0189 0190 0191 0192 0193 0194 0195 0196 0197 0198 0199 0200 0201 0202 0203
 0204 0205 0206 0207 0208 0209 0210 0211 0212 0213 0214 0215 0216 0217 0218
 0219 0220 0221 0222 0223 0224 0225 0226
```

Related Topics

6.3.38 set vlan-range

6.3.19 dot1q termination vid

Function

The **dot1q termination vid** command sets the single VLAN ID for Dot1q termination on a sub-interface.

The **undo dot1q termination vid** command deletes the single VLAN ID for Dot1q termination on a sub-interface.

By default, the single VLAN ID for Dot1q termination is not set on a sub-interface.

Format

dot1q termination vid *low-pe-vid* [**to** *high-pe-vid*]

undo dot1q termination vid *low-pe-vid* [**to** *high-pe-vid*]

Parameters

Parameter	Description	Value
low-pe-vid	Specifies the lower limit of the VLAN ID in the user packet.	The value is an integer that ranges from 1 to 4094.
to *high-pe-vid*	Specifies the upper limit of the VLAN ID in the user packet.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- Communication between VLANs

  VLANs are widely used because they can separate Layer 2 packets. A physical LAN is divided into multiple logical broadcast domains. Hosts in the same VLAN can communicate with each other but the hosts of different VLANs cannot. The Layer 3 routing technology is used for communication between hosts of different VLANs in the following two methods:

  – Through the VLANIF interface on the device.

  – Through the Layer 3 Ethernet interface on the device.

    However, when a traditional Layer 3 Ethernet interface receives VLAN packets, the VLAN packets are discarded. To enable communication between hosts of different VLANs, you can create an Ethernet sub-interface on the Layer 3 Ethernet interface and enable QinQ termination on the sub-interface to remove the tag from the VLAN packet.

- Communication between a LAN and a WAN

  Most packets on a LAN have VLAN tags, but some WAN protocols such as ATM, FR, and PPP, cannot identify VLAN packets. To send a VLAN packet from LAN to WAN, the device records VLAN information in the packet, removes the VLAN tag, and forwards the packet.

Based on the number of tags, VLAN packets can be classified into Dot1q packets and QinQ packets. A Dot1q packet carries a single-layer VLAN tag and a QinQ packet carries a double-layer VLAN tag. Accordingly, there are two VLAN tag termination modes:

- Dot1q termination, which terminates tags carried in Dot1q packets

  To configure Dot1q termination, run the **dot1q termination vid** command.

- QinQ termination, which terminates tags carried in QinQ packets.

  To configure QinQ termination, run the **qinq termination pe-vid ce-vid** command in the sub-interface view.

After the **dot1q termination vid** command is run, the sub-interface for VLAN tag termination processes the packet in the following procedures:

- The sub-interface removes the tag in the VLAN packet when receiving the packet and forwards the packet on Layer 3. The outbound interface determines whether the forwarded VLAN packet carries tags.
- The sub-interface adds VLAN information to the packet and then sends the packet.

NOTE

Batch VLAN termination applies to the Terminal access scenario only.

Precautions

- *high-pe-vid* is supported by only the AR3200&AR3600 series.
- You can specify *high-pe-vid* only after the **termination-vid batch enable** command is used to enable a sub-interface to batch terminate VLAN tags.
- The value of *high-pe-vid* must be greater than or equal to the value of *low-pe-vid*.
- When this command is executed on an Eth-Trunk sub-interface, you cannot specify *high-pe-vid*.
- The tag values of the user packet received by the sub-interface must be in the range of *pe-vid*s specified in the command; otherwise, the packet is discarded.
- When you run the **undo dot1q termination vid** command to delete the single VLAN ID for Dot1q termination on a sub-interface, the VLAN ID must be the same as that specified in the **dot1q termination vid** command.
- If the **dot1q termination vid** command is run more than once, all configurations take effect.

Configuration Impact

After you run this command to enable batch VLAN termination on a sub-interface, the sub-interface can only connect to an L2VPN but cannot be used for Layer 3 forwarding.

Example

Set the encapsulation mode on Ethernet2/0/0.1 to Dot1q and allow the packets with the VLAN tag 100 to pass through.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0.1
[Huawei-Ethernet2/0/0.1] dot1q termination vid 100
```

Related Topics

6.3.36 qinq termination pe-vid ce-vid

6.3.20 dynamic-macvlan enable

Function

The **dynamic-macvlan enable** command enables MAC address-based dynamic VLAN assignment.

The **undo dynamic-macvlan enable** command disables MAC address-based dynamic VLAN assignment.

By default, MAC address-based dynamic VLAN assignment is disabled.

NOTE

Only the AR1220E, AR1220EV, AR1220EVW, and AR1220F support this function.

Format

dynamic-macvlan enable

undo dynamic-macvlan enable

Parameters

N/A

Views

GE interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

After you run the **dynamic-macvlan enable** command on a port and 802.1X or MAC address authentication is completed, the VLAN attribute assigned by the RADIUS server is added to the packets sent to the CPU regardless of the port from which users access the network. In this manner, a MAC address-to-VLAN mapping is created and packets are not directed based on the PVID.

Precautions

- This command can be run only on Layer 2 ports of the device panel.
- The ports must be of the hybrid untagged type.
- The ports enabled with MAC address-based dynamic VLAN assignment support Layer 3 services only.
- If a port has an authentication profile applied, you need to unbind the authentication profile from the port before running the **dynamic-macvlan enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable MAC address-based dynamic VLAN assignment on GE0/0/3.

```
<Huawei> system-view
[Huawei] interface GigabitEthernet 0/0/3
[Huawei-GigabitEthernet0/0/3] dynamic-macvlan enable
```

6.3.21 interface vlanif

Function

The **interface vlanif** command creates a VLANIF interface and displays the VLANIF interface view.

The **undo interface vlanif** command deletes a VLANIF interface.

By default, VLANIF interfaces are not created.

Format

interface vlanif *vlan-id*

undo interface vlanif *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the VLAN that a VLANIF interface belongs to.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device needs to communicate with devices at the network layer, you can create a logical interface based on a VLAN on the device, namely, a VLANIF interface. A VLANIF interface is a network layer interface and can be configured with an IP address. The device then users the VLANIF interface to communicate with devices at the network layer.

Prerequisites

The specified VLAN has been created using the **vlan** command before you create a VLANIF interface.

Follow-up Procedure

Run the **ip address** to assign an IP address to the VLANIF interface.

Precautions

If the specified VLANIF interface exists, the **interface vlanif** command displays the VLANIF interface view directly.

After a VLANIF interface is configured, the corresponding VLAN cannot be configured as a sub-VLAN or principal VLAN.

When a VLANIF interface is used as a management VLANIF interface where you can telnet to the device, the user VLAN ID cannot be the same as the management VLAN ID; otherwise, you will fail to telnet to the device.

Example

Create VLANIF 2 and enter the VLANIF interface view.

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] quit
[Huawei] interface vlanif 2
[Huawei-Vlanif2]
```

Related Topics

6.3.11 display interface vlanif

6.3.43 vlan

6.3.22 ip pool (VLAN view)

Function

The **ip pool** command configures an IP address pool for a sub-VLAN.

The **undo ip pool** command deletes the IP address pool of a sub-VLAN.

By default, no IP address pool is configured for sub-VLANs.

Format

ip pool *start-address* [**to** *end-address*]

undo ip pool

Parameters

Parameter	Description	Value
start-address	Specifies the start IP address in an IP address pool.	It is in dotted decimal notation.

Parameter	Description	Value
to *end-address*	Specifies the end IP address in an IP address pool. If *end-address* is not specified, only one IP address, that is, *start-address*, exists in the IP address pool.	It is in dotted decimal notation.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After assigning an IP address to the super-VLAN by assigning the IP address to a VLANIF interface, you can specify the IP address range for users in the VLAN. In this manner, the ARP module filters out packets with IP addresses beyond the IP address range so that the number of ARP packets can be exactly controlled.

If the super VLAN is enabled with proxy ARP, the system directly sends an ARP Request packet from a user in the sub-VLAN to the destination sub-VLAN based on the IP address carried in the packet, which reduces broadcast traffic.

The **ip pool** command can be used to set an IP address pool for the sub-VLAN. In the IP address pool, a single IP address or a consecutive IP address segment can be configured, but inconsecutive IP address segments cannot be configured.

Prerequisites

After the preceding configuration is complete, run the **aggregate-vlan** command in the view of a VLAN to set the VLAN to the super-VLAN, and run the **access-vlan** command to set the VLANs that need IP address pools configured to be sub-VLANs of the super-VLAN.

Configuration Impact

After the **ip pool** command is run for a sub-VLAN, only ARP packets, including ARP request, ARP response, and proxy ARP, with the IP addresses in the IP address pool can be processed in the sub-VLAN.

Precautions

Before updating the IP address pool configured for a sub-VLAN, run the **undo ip pool** command to delete the existing one.

Example

Configure an IP address pool for VLAN 20, with IP addresses ranging from 10.10.10.10 to 10.10.10.20.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] vlan 20
[Huawei-vlan20] ip pool 10.10.10.10 to 10.10.10.20
```

Related Topics

6.3.3 aggregate-vlan

6.3.2 access-vlan

6.3.23 management-vlan

Function

Using the **management-vlan** command, you can configure a VLAN as a management VLAN.

Using the **undo management-vlan** command, you can cancel the configuration.

By default, no VLAN is configured as a management VLAN.

Format

management-vlan

undo management-vlan

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use a network management system to manage multiple devices, create a VLANIF interface on each device and configure a management IP address for the VLANIF interface. You can then log in to a device and manage it using its management IP address. If a user-side interface is added to the VLAN, users connected to the interface can also log in to the device. This brings security risks to the device.

After a VLAN is configured as a management VLAN, no access interface can be added to the VLAN. An access interface is connected to users. The management VLAN forbids users connected to access interfaces to log in to the device, improving device performance.

Follow-up Procedure

Create a VLANIF interface corresponding to the VLAN and configure a management IP address on the VLANIF interface.

Precautions

VLAN 1 cannot be configured as an mVLAN.

You can run the **display vlan** command to view the management VLAN configuration. In the command output, the VLAN marked with a * is the management VLAN.

After a VLAN is configured as a management VLAN, only trunk and hybrid interfaces can be added to the VLAN.

Example

Configure VLAN 100 as a management VLAN.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] management-vlan
```

Related Topics

6.3.16 display vlan

6.3.43 vlan

6.3.24 mtu (VLANIF interface view)

Function

Using the **mtu** command, you can set the maximum transmission unit (MTU) of a VLANIF interface.

Using the **undo mtu** command, you can restore the default MTU of a VLAN interface.

By default, the MTU of a VLAN interface is 1500 bytes.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a VLANIF interface.	The value is an integer that ranges from 46 to 1600, in bytes.

 Copyright © Huawei Technologies Co., Ltd.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MTU is short for maximum transmission unit. An MTU value determines the maximum number of bytes each time a sender can send. If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, aggravating the network transmission load. To avoid this problem, set the MTU value of the VLANIF interface.

Example

Set the MTU of the VLANIF 100 interface to 1492 bytes.

```
<Huawei> system-view
[Huawei] interface Vlanif 100
[Huawei-Vlanif100] mtu 1492
```

Related Topics

6.3.40 shutdown (VLANIF interface view)

6.3.25 mux-vlan

Function

The **mux-vlan** command configures a VLAN as a principal VLAN.

The **undo mux-vlan** command cancels the configuration.

By default, no VLAN is configured as a principal VLAN.

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220, AR2220L, AR2220E, AR2240, AR2240C, AR3260, and AR3670 support MUX VLAN.

Only the 8FE1GE, 24ES2GP, and 24GE cards support MUX VLAN.

Format

mux-vlan

undo mux-vlan

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.
  - Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

Prerequisites

The VLAN does not have a VLANIF interface.

Follow-up Procedure

Configure subordinate VLANs for the principal VLAN and enable the MUX VLAN function on interfaces.

Precautions

If a VLAN has been configured as a principal VLAN, it cannot be used to configure the VLANIF interface, Super VLAN, Sub VLAN.

If a VLAN has been configured as a principal VLAN, it cannot be configured as a subordinate VLAN of another principal VLAN.

 Copyright © Huawei Technologies Co., Ltd.

The device supports a maximum of 128 principal VLANs. The maximum number of subordinate VLANs in a principal VLAN is as follows:

- AR2200: 16
- AR3200&AR3600: 32

Example

Configure VLAN 5 as a principal VLAN.

```
<Huawei> system-view
[Huawei] vlan 5
[Huawei-vlan5] mux-vlan
```

Related Topics

6.3.12 display mux-vlan

6.3.33 port mux-vlan enable

6.3.42 subordinate separate

6.3.41 subordinate group

6.3.26 name (VLAN view)

Function

The **name** command configures a name for a VLAN.

The **undo name** command deletes a configured VLAN name.

By default, a VLAN does not have a name.

Format

name *vlan-name*

undo name

Parameters

Parameter	Description	Value
vlan-name	Specifies the VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

If a device is configured with multiple VLANs for transmitting different services, you can name the VLANs in their corresponding VLAN views to facilitate service management. In this manner, you can check the deployed services of a VLAN by the VLAN name.

After VLANs are named, you can run the **vlan vlan-name** command in the system view to enter the view of a specific VLAN, and then check or modify the configuration of the VLAN.

Example

Create VLAN 2, which is used to transmit data services, and name it as data.

```
<Huawei> system-view
[Huawei] vlan 2
[Huawei-vlan2] name data
```

Related Topics

6.3.43 vlan

6.3.27 port

Function

The **port** command configures a VLAN as the default VLAN of an interface and adds the interface to the VLAN.

The **undo port** command restores the default VLAN of an interface to the default setting.

By default, VLAN 1 is the default VLAN of all interfaces.

Format

port *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

undo port *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type { *interface-number1* [**to** *interface-number2*] }	Configures the default VLAN for multiple interfaces. ● *interface-type* specifies the type of interfaces. ● *interface-number1* specifies the number of the first interface. ● *interface-number2* specifies the number of the last interface. The value of *interface-number2* must be greater than the value of *interface-number1*. The *interface-number1* and *interface-number2* parameters identify a range of interfaces. If **to** *interface-number2* is not specified, only one interface is specified. You can specify 10 interface ranges at one time.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from a user device are untagged, and frames sent from a remote device may also be untagged. However, the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

 Copyright © Huawei Technologies Co., Ltd.

After the default VLAN is specified for an access interface, packets passing through the interface are processed as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN ID.
- When the interface receives a tagged packet:
  - If the interface is an access interface, it compares the VLAN ID of the packet with the default VLAN ID. If they are the same, the interface forwards the packets; otherwise, the interface discards the packets.
- Before forwarding tagged packets, access interfaces remove VLAN tags from the packets.

Prerequisites

The link-type of specified interfaces cannot be access or trunk before you run the **port** command.

Precautions

A super VLAN cannot be configured as the default VLAN of interfaces.

The **undo port** command deletes the default VLAN of the specified interfaces only if the current VLAN is the default VLAN of these interfaces.

If you run the **port** command multiple times in the same VLAN view, the VLAN is configured as the default VLAN of all the specified interfaces.

You can also run the **port default vlan** command in the interface view to configure the default VLAN for an interface. The two commands have the same function.

Example

Configure VLAN 3 as the default VLAN of interfaces Eth2/0/0 to Eth2/0/4.

```
<Huawei> system-view
[Huawei] vlan 3
[Huawei-vlan3] port ethernet 2/0/0 to 2/0/4
```

Related Topics

6.3.16 display vlan

6.3.32 port link-type

6.3.28 port default vlan

6.3.28 port default vlan

Function

The **port default vlan** command configures the default VLAN of an interface and adds the interface to the VLAN.

The **undo port default vlan** command restores the default VLAN of an interface to the default setting.

By default, VLAN 1 is the default VLAN of all interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Format

port default vlan *vlan-id* [**step** *step-number* [**increased** | **decreased**]]

undo port default vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the default VLAN.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
step *step-number* [**increased** | **decreased**]	Specifies that the interface added to an interface group can be bound to VLANs starting from the one identified by *vlan-id* in an ascending or descending order at a step specified by *step-number*. **increased** specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id* at a step specified by *step-number* to add the interfaces to the VLANs. Whereas **decreased** specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id* at a step specified by *step-number* to add the interfaces to the VLANs. For example, you can configure **increased**, and set *vlan-id* to 10 and *step-number* to 20 in the **port default vlan** command. After this configuration, interface 1 joins VLAN 10; interface 2 joins VLAN 30... By analogy, interface 10 joins VLAN 190. **NOTE** ● This parameter can only be used in the port group view. ● When using **step** and *vlan-id* in the command, ensure that all interfaces added to the VLAN are available. ● If this parameter is not specified, all interfaces in an interface group are added into the same VLAN, that is, VLAN *vlan-id*.	The value is an integer that ranges from 1 to 4093.

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, Virtual-Ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All frames sent from a user device are untagged, and frames sent from a remote device may also be untagged. However, the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

After the default VLAN is specified for an access interface, packets passing through the interface are processed as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN tag.
- When the interface receives a tagged packet:
  - If the interface is an access interface, it compares the VLAN ID of the packet with the default VLAN ID. If they are the same, the interface forwards the packets; otherwise, the interface discards the packets.
- Before forwarding tagged packets, access interfaces remove VLAN tags from the packets.

Prerequisites

Running the **portswitch** command in the VE interface view switches the VE interface from Layer 3 to Layer 2.

The VLAN to be configured as the default VLAN has been created.

The interface type is access. If not, run the **port link-type** command to change the interface type.

Precautions

- You can also run the **port** command in the VLAN view to configure the default VLAN of an interface. The two commands have the same function.
- A super VLAN cannot be configured as the default VLAN of interfaces.
- This command is invalid on a member interface of an Eth-Trunk.
- If you run the **port default vlan** command multiple times in the same interface view, only the latest configuration takes effect.
- This configuration will be deleted automatically if the default VLAN is deleted in system view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure VLAN 3 (an existing VLAN) as the default VLAN of Eth2/0/0 (an access interface).

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] port default vlan 3
```

Configure VLAN 4 (an existing VLAN) as the default VLAN of VE0/0/1 (an access interface).

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type access
[Huawei-Virtual-Ethernet0/0/1] port default vlan 4
```

Related Topics

6.3.16 display vlan

6.3.27 port

6.3.32 port link-type

6.3.29 port hybrid pvid vlan

Function

The **port hybrid pvid vlan** command specifies the default VLAN ID of a hybrid interface.

The **undo port hybrid pvid vlan** command restores the default VLAN ID of a hybrid interface to the default setting.

By default, VLAN 1 is the default VLAN ID of all interfaces.

Format

port hybrid pvid vlan *vlan-id*

undo port hybrid pvid vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a hybrid interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, WLAN-ESS interface view, Virtual-Ethernet interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface may receive untagged and tagged frames, but the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

A hybrid interface processes Ethernet frames as follows:

- When the interface receives an untagged frame, it tags the frame with the default VLAN ID. If the default VLAN ID is allowed by the interface, the interface accepts the frame. Otherwise, the interface discards the frame.
- When the interface receives a tagged frame, it accepts the frame if the VLAN ID of the frame is in the list of allowed VLAN IDs. Otherwise, the interface discards the frame.
- If the VLAN ID of a frame is allowed by the interface, the interface forwards the frame.

Prerequisites

The VLAN to be specified as the default VLAN has been created.

Running the **portswitch** command in the VE interface view switches the VE interface from Layer 3 to Layer 2.

Precautions

This command is invalid on a member interface of an Eth-Trunk.

The **port hybrid pvid vlan** command only specifies the default VLAN for an interface but does not add the interface to the default VLAN.

If you run the **port hybrid pvid vlan** command multiple times in the same interface view, only the latest configuration takes effect.

This configuration will be deleted automatically if the default VLAN is deleted in system view.

Example

Specify VLAN 5 as the default VLAN of Eth2/0/0.

```
<Huawei> system-view
[Huawei] vlan 5
[Huawei-vlan5] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type hybrid
[Huawei-Ethernet2/0/0] port hybrid pvid vlan 5
```

Specify VLAN 5 as the default VLAN of the VE0/0/1 interface.

```
<Huawei> system-view
[Huawei] vlan 5
[Huawei] quit
[Huawei] interface virtual-ethernet 0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type hybrid
[Huawei-Virtual-Ethernet0/0/1] port hybrid pvid vlan 5
```

Related Topics

6.3.35 port trunk pvid vlan

6.3.30 port hybrid tagged vlan

Function

The **port hybrid tagged vlan** command adds a hybrid interface to the specified VLANs. Frames of the VLANs then pass through the hybrid interface in tagged mode.

The **undo port hybrid vlan** command removes a hybrid interface from the specified VLANs.

By default, a hybrid interface is added to VLAN 1 in untagged mode.

Format

port hybrid tagged vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port hybrid vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view)**port hybrid tagged vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view)**undo port hybrid vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a hybrid interface to specified VLANs. • *vlan-id1* specifies the start VLAN ID. • **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a hybrid interface to all VLANs.	-
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port hybrid tagged vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, WLAN-BSS interface view, WLAN-ESS interface view, Virtual-Ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hybrid interface can connect to either a user device or a router. This command adds a hybrid interface to VLANs in tagged mode so that the hybrid interface allows frames from the VLANs to pass.

After a hybrid interface is added to VLANs in tagged mode, the interface forwards frames without removing VLAN tags of frames.

Prerequisites

Running the **portswitch** command in the VE interface view switches the VE interface from Layer 3 to Layer 2.

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

- This command is invalid on a member interface of an Eth-Trunk.
- A super VLAN cannot be specified in the command.
- If you run the **port hybrid tagged vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.

 Copyright © Huawei Technologies Co., Ltd.

Example

Add Eth2/0/0 to VLAN 3 to VLAN 5 in tagged mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type hybrid
[Huawei-Ethernet2/0/0] port hybrid tagged vlan 3 to 5
```

Add VE0/0/1 to VLAN 6 to VLAN 8 in tagged mode.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type hybrid
[Huawei-Virtual-Ethernet0/0/1] port hybrid tagged vlan 6 to 8
```

Related Topics

6.3.32 port link-type

6.3.31 port hybrid untagged vlan

6.3.31 port hybrid untagged vlan

Function

The **port hybrid untagged vlan** command adds a hybrid interface to the specified VLANs. Frames of the VLANs then pass through the hybrid interface in untagged mode.

The **undo port hybrid vlan** command removes a hybrid interface from the specified VLANs.

By default, a hybrid interface is added to VLAN 1 in untagged mode.

Format

port hybrid untagged vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port hybrid vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view)**port hybrid untagged vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view)**undo port hybrid vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a hybrid interface to specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a hybrid interface to all VLANs.	-
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port hybrid untagged vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, WLAN-ESS interface view, Virtual-Ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hybrid interface can connect to either a user device or a router. When a hybrid interface is connected to a user device, it must be added to VLANs in untagged mode so that it sends untagged frames.

After a hybrid interface is added to VLANs in untagged mode, the interface removes VLAN tags of frames before sending frames.

Prerequisites

Running the **portswitch** command in the VE interface view switches the VE interface from Layer 3 to Layer 2.

If an interface is not a hybrid interface, run the **port link-type hybrid** command to change the interface type to hybrid.

Precautions

- This command is invalid on a member interface of an Eth-Trunk.
- A super VLAN cannot be specified in the command.
- If you run the **port hybrid untagged vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.

Example

Add Eth2/0/0 to VLAN 3 to VLAN 5 in untagged mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type hybrid
[Huawei-Ethernet2/0/0] port hybrid untagged vlan 3 to 5
```

Add VE0/0/1 to VLAN 6 to VLAN 8 in untagged mode.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type hybrid
[Huawei-Virtual-Ethernet0/0/1] port hybrid untagged vlan 6 to 8
```

Related Topics

6.3.32 port link-type

6.3.30 port hybrid tagged vlan

6.3.32 port link-type

Function

The **port link-type** command sets the link type of an interface.

The **undo port link-type** command restores the default link type of an interface.

By default, the link type of an interface is hybrid.

Format

port link-type { **access** | **hybrid** | **trunk** }

undo port link-type

Parameters

Parameter	Description	Value
access	Sets the link type of an interface to access.	-
hybrid	Sets the link type of an interface to hybrid.	-
trunk	Sets the link type of an interface to trunk.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, WLAN-ESS interface view, Virtual-Ethernet interface view

NOTE

A Wlan-ESS interface can only be set as a hybrid interface.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Characteristics of different interfaces are:

- An access interface connects to a user device. It can connect only to an access link, and Ethernet frames transmitted on the access link are untagged. An access interface adds a VLAN tag to packets and sets the VID field in the VLAN tag to the default VLAN ID. The access link transmits only the packets with the default VLAN ID.
- A trunk interface connects to a router and can connect only to a trunk link. A trunk interface allows frames from multiple VLANs to pass.
- A hybrid interface can connect to either a user device or a router, and it can connect to an access link or a trunk link. A hybrid interface allows frames from multiple VLANs to pass and can remove VLAN tags of outgoing frames.

Prerequisites

The interface must work in Layer 2 mode. If the interface works in Layer 3 mode, run the **portswitch** command to switch to Layer 2 mode.

Before changing the interface type, restore the default VLAN configuration of the interface so that the interface belongs to only VLAN 1.

Follow-up Procedure

Add the interface to VLANs.

Precautions

This command is invalid on a member interface of an Eth-Trunk.

If you run the **port link-type** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the link type of Eth2/0/0 to trunk.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
```

Set the link type of VE 0/0/1 to trunk.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type trunk
```

Related Topics

3.1.9 display this

6.3.33 port mux-vlan enable

Function

The **port mux-vlan enable** command enables the MUX VLAN function on an interface.

The **undo port mux-vlan enable** command disables the MUX VLAN function on an interface.

By default, the MUX VLAN function is disabled on an interface.

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220, AR2220L, AR2220E, AR2240, AR2240C, AR3260, and AR3670 support MUX VLAN.

Only the 8FE1GE, 24ES2GP, and 24GE cards support MUX VLAN.

Format

port mux-vlan enable

undo port mux-vlan enable

Parameters

None

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves a MUX VLAN and several subordinate VLANs. Subordinate VLANs are classified into subordinate group VLANs and subordinate separate VLANs. Subordinate VLANs can communicate with the principal VLAN but cannot communicate with each other. Interfaces in a subordinate group VLAN can

 Copyright © Huawei Technologies Co., Ltd.

communicate with each other, and interfaces in a subordinate separate VLAN are isolated from each other.

The MUX VLAN function takes effect only after it is enabled on an interface.

Prerequisites

Before enable MUX VLAN function, complete the following task:

- The port has been added to only a VLAN. If the port has been added to multiple VLANs, the MUX VLAN function cannot be enabled on this port.
- The port has been added to a principal or subordinate VLAN in untagged mode as an access or hybrid interface.

Precautions

- Disabling MAC address learning or limiting the number of learned MAC addresses on an interface affects the MUX VLAN function on the interface.
- The MUX VLAN and port security functions conflict on an interface. That is, the **port-security enable** and **port mux-vlan enable** commands cannot be used on the same interface.

Example

Enable the MUX VLAN function on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port mux-vlan enable
```

Related Topics

6.3.12 display mux-vlan

6.3.25 mux-vlan

6.3.34 port trunk allow-pass vlan

Function

The **port trunk allow-pass vlan** command adds a trunk interface to the specified VLANs.

The **undo port trunk allow-pass vlan** command deletes a trunk interface from the specified VLANs.

By default, a trunk interface is in VLAN 1.

Format

port trunk allow-pass vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

undo port trunk allow-pass vlan { { *vlan-id1* [**to** *vlan-id2*] }&<1-10> | **all** }

(Port group view)**port trunk allow-pass vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

(Port group view)**undo port trunk allow-pass vlan** *vlan-id3* [**step** *step-number* [**increased** | **decreased**]]

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Adds a trunk interface to specified VLANs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value of *vlan-id1* is an integer that ranges from 1 to 4094. The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Adds a trunk interface to all VLANs.	-
vlan-id3	Specifies the ID of the start VLAN to be bound to the member port of a port group.	The value is an integer that ranges from 1 to 4094.
step *step-number*	Specifies the step for the increase or decrease in the value of the VLAN ID. With this parameter specified, the member ports in a port group can be bound to VLANs starting from the one identified by *vlan-id3* in an ascending or descending order at a step specified by *step-number*. This facilitates the subsequent user configuration. For example: A port group has 10 member ports. You can configure **increased**, and set *vlan-id3* to 1 and *step-number* to 1 in the **port trunk allow-pass vlan** command. After this configuration, member port 1 joins VLAN 1; member port 2 joins VLAN 2... By analogy, member port 10 joins VLAN 10.	The value is an integer that ranges from 1 to 4093.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
increased	Specifies an increase in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group.	By default, Layer 2 ports are bound to the VLANs in an ascending order.
decreased	Specifies a decrease in the values of VLAN IDs starting from the one identified by *vlan-id3* at a step specified by *step-number* to bind the VLANs to the member ports of a port group. When setting **decreased**, ensure that the value of *vlan-id3* is greater than or equal to the number of the member ports of the port group.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, Virtual-Ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A trunk interface can join multiple VLANs and connects to a network device. To allow all packets from one or multiple VLANs to pass through a trunk interface, the trunk interface must be added to the VLANs using the **port trunk allow-pass vlan** command.

Prerequisites

Running the **portswitch** command in the VE interface view switches the VE interface from Layer 3 to Layer 2.

The link-type of the interface is configured to trunk.

Precautions

The command cannot be used on a member interface of an Eth-Trunk.

If you run the **port trunk allow-pass vlan** command multiple times in the same interface view, the interface is added to all the specified VLANs.

Example

Add Eth2/0/0 to VLANs 10 to 30.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 10 to 30
```

Add VE0/0/1 to VLANs 6 to 8.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type trunk
[Huawei-Virtual-Ethernet0/0/1] port trunk allow-pass vlan 6 to 8
```

Related Topics

6.3.16 display vlan

6.3.35 port trunk pvid vlan

6.3.35 port trunk pvid vlan

Function

The **port trunk pvid vlan** command specifies the default VLAN for a trunk interface.

The **undo port trunk pvid vlan** command restores the default VLAN of a trunk interface to the default setting.

By default, VLAN 1 is the default VLAN of trunk interfaces.

Format

port trunk pvid vlan *vlan-id*

undo port trunk pvid vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the default VLAN ID of a trunk interface.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view, Virtual-Ethernet interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An interface may receive untagged and tagged frames, but the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by an interface. The default VLAN ID of the interface can be added to untagged frames so that these frames are forwarded in the default VLAN.

Prerequisites

Running the **portswitch** command in the VE interface view switches the VE interface from Layer 3 to Layer 2.

The VLAN to be specified as the default VLAN has been created.

Follow-up Procedure

Add the trunk interface to the default VLAN.

Precautions

The **port trunk pvid vlan** command only specifies the default VLAN of a trunk interface but does not add the trunk interface to the default VLAN. A trunk interface forwards frames with the default VLAN ID only after it is added to the default VLAN using the **port trunk allow-pass vlan** command.

If you run the **port trunk pvid vlan** command multiple times in the same interface view, only the latest configuration takes effect.

This configuration will be deleted automatically if the default VLAN is deleted in system view.

Example

Specify VLAN 5 as the default VLAN of Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk pvid vlan 5
```

Specify VLAN 5 as the default VLAN of the VE0/0/1 interface.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type trunk
[Huawei-Virtual-Ethernet0/0/1] port trunk pvid vlan 5
```

Related Topics

6.3.32 port link-type

6.3.34 port trunk allow-pass vlan

6.3.36 qinq termination pe-vid ce-vid

Function

The **qinq termination pe-vid ce-vid** command configures QinQ termination on a sub-interface.

The **undo qinq termination pe-vid ce-vid** command cancels QinQ termination on a sub-interface.

By default, QinQ termination is disabled on a sub-interface.

Format

qinq termination pe-vid *pe-vid* **ce-vid** *ce-vid1* [**to** *ce-vid2*]

undo qinq termination pe-vid *pe-vid* **ce-vid** *ce-vid1* [**to** *ce-vid2*]

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.
ce-vid *ce-vid1* [**to** *ce-vid2*]	Specifies the inner VLAN ID. ● *ce-vid1*: specifies the lower threshold of the inner VLAN tag in the user packet. ● *ce-vid2*: specifies the upper threshold of the outer VLAN tag in the user packet. **NOTE** You can specify *ce-vid2* only after the **termination-vid batch enable** command is used to enable a sub-interface to batch terminate VLAN tags.	The value of *ce-vid1* is an integer that ranges from 1 to 4094. The value of *ce-vid2* is an integer that ranges from 1 to 4094. The value of *ce-vid2* must be larger than or equal to the value of *ce-vid1*.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

- Communication between VLANs

  The VLAN technology is widely used because it helps Layer 2 packets of different users to be separately transmitted. With the VLAN technology, a physical LAN is divided into multiple logical broadcast domains, that is, VLANs. In this manner, hosts in a VLAN can communicate with each other, but hosts in different VLANs cannot communicate at Layer 2. The Layer 3 routing technology is required for communication of hosts in different VLANs.
- Communication between a LAN and a WAN

  Most packets on a LAN have VLAN tags, but some WAN protocols such as ATM, FR, and PPP, cannot identify VLAN packets. To send a VLAN packet from LAN to WAN, the device records VLAN information in the packet, removes the VLAN tag, and forwards the packet.

Based on the number of tags, VLAN packets can be classified into Dot1q packets and QinQ packets. A Dot1q packet carries a single-layer VLAN tag and a QinQ packet carries a double-layer VLAN tag. Accordingly, there are two VLAN tag termination modes:

- Dot1q termination, which terminates tags carried in Dot1q packets

  To configure Dot1q termination, run the **dot1q termination vid** command in the sub-interface view.
- QinQ termination, which terminates tags carried in QinQ packets.

  To configure Dot1q termination, run the **qinq termination pe-vid ce-vid** command.

After the **qinq termination pe-vid ce-vid** command is run, the sub-interface for VLAN tag termination processes the packet in the following procedures:

- The sub-interface removes the tag in the VLAN packet when receiving the packet and forwards the packet on Layer 3. Whether the forwarded VLAN packet carries tags is determined by the outbound interface.
- The sub-interface adds VLAN information to the packet and then sends the packet.

NOTE

Batch VLAN termination applies to the Terminal access scenario only.

Precautions

The MTU of a sub-interface must be at least 4 bytes smaller than the MTU of its primary interface. Especially, the MTU of a QinQ sub-interface must be at least 8 bytes smaller than the MTU of its primary interface.

Ethernet sub-interfaces of VDSL interfaces in PTM mode do not support QinQ commands.

Configuration Impact

After you run this command to enable batch VLAN termination on a sub-interface, the sub-interface can only connect to an L2VPN but cannot be used for Layer 3 forwarding.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the encapsulation mode on Ethernet2/0/0.1 to QinQ and allow the packets with the outer VLAN tag 100 and inner VLAN tag 200 to pass through.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0.1
[Huawei-Ethernet2/0/0.1] qinq termination pe-vid 100 ce-vid 200
```

Related Topics

6.3.46 termination-vid batch enable

6.3.19 dot1q termination vid

6.3.37 reset vlan statistics

Function

Using the **reset vlan statistics** command, you can clear traffic statistics in a specified VLAN.

Format

reset vlan statistics *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command is used when you need to collect new packet statistics in a VLAN. After this command is executed, the packet count in the VLAN becomes 0.

Precautions

NOTICE

Traffic statistics cannot be restored after they are cleared. Exercise caution when you use the command.

Example

Clear traffic statistics in VLAN 3.

```
<Huawei> reset vlan statistics 3
```

Related Topics

6.3.16 display vlan

6.3.38 set vlan-range

Function

The **set vlan-range** command configures a range of VLANs that can be created on the 4GE-2S interface card.

The **undo set vlan-range** command deletes a range of VLANs that can be created on the 4GE-2S interface card.

Format

set vlan-range slot *slot-id* **vlan batch** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo set vlan-range slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID. The 4GE-2S interface card must be installed in the slot.	The value is an integer that ranges from 1 to 15.
vlan batch	Indicates that VLANs are created in a batch.	-
vlan-id1 **to** *vlan-id2*	Specifies IDs of the VLANs that are created in a batch. • *vlan-id1* specifies the first VLAN ID. • *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be greater than *vlan-id1*. *vlan-id2* and *vlan-id1* specify the range of VLANs. • If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is created.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **set vlan-range** command to configure a range of VLANs that can be created on the 4GE-2S interface card. Only VLANs in the range can be created on the 4GE-2S interface card.

Precautions

- Before the **set vlan-range** command is used:
  - VLANs are delivered according to the sequence in which the VLANs were created on the 4GE-2S interface card. The system allows a maximum of 252 VLANs. Excess VLANs are not delivered.
  - If VLANs are created in a batch, VLANs are delivered in ascending order of VLAN ID. The system allows a maximum of 252 VLANs. Excess VLANs are not delivered.
  - If more than 252 VLANs are created, the **set vlan-range** command is recommended.
- After the **set vlan-range** command is used:
  - VLANs in a specified range are delivered to the 4GE-2S interface card. Ensure that the VLAN ID range is within 252. After the **set vlan-range** or **undo set vlan-range** command is executed, you must restart the 4GE-2S interface card to make the configuration take effect.
  - The 4GE-2S interface card must allow VLAN 1. You cannot use the **set vlan-range** command to set VLAN 1.
  - The VLAN ID range allowed on the 4GE-2S interface card is 1-252. Except for VLAN 1, the **set vlan-range** command allows a maximum of 251 VLANs.
  - After the VLAN ID range is set on the 4GE-2S interface card, interfaces on the 4GE-2S interface card allow only these VLANs in the range.
- If interfaces on the 4GE-2S card installed on a device are added to a VLAN and the **set vlan-range** command is not configured, the device automatically delivers the **set vlan-range** command and proactively restarts the 4GE-2S card after the **save** command is run to save configurations and the device or the 4GE-2S card is restarted. After the 4GE-2S card is restarted, you are advised to run the **save** command again to save configurations. This ensures that VLAN services on the 4GE-2S card can run properly.
- If you do not want the device to deliver the **set vlan-range** command after the device or the 4GE-2S card is restarted, run the **undo set vlan-range** command and then the **save** command on the device. The device then will not automatically deliver the **set vlan-range** command for the card in the corresponding slot. However, VLAN services may fail to take effect on the 4GE-2S card. Exercise caution when performing this operation.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create VLANs 100 to 200 on the 4GE-2S interface card in slot 6.

```
<Huawei> system-view
[Huawei] set vlan-range slot 6 vlan batch 100 to 200
Warning: This configuration takes effect after the board is reset. Otherwise, services may be affected. You
need to manually reset the board.
```

Related Topics

6.3.18 display vlan-range

6.3.39 set reserved-vlan slot

Function

The **set reserved-vlan slot** command configures the reserved VLAN ID on the interface card.

The **undo set reserved-vlan slot** command deletes the reserved VLAN ID configured on the interface card.

By default, no reserved VLAN ID is configured on the interface card.

Format

set reserved-vlan *vlan-id* **slot** *slot-id*

undo set reserved-vlan slot *slot-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the reserved VLAN ID, which cannot conflict with the service VLAN ID.	The value is an integer that ranges from 1 to 4094.
slot-id	Specifies the slot ID. The value must be the ID of the slot where the interface card is installed.	The value is an integer that ranges from 1 to 15.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **set reserved-vlan slot** command configures the reserved VLAN ID on the interface card. The working mode of the interface on the interface card can be changed from Layer 2 mode to Layer 3 mode only after the reserved VLAN ID is configured.

Precautions

The reserved VLAN ID cannot conflict with the service VLAN ID. You can change or delete the reserved VLAN ID only when all interfaces on the interface card in the corresponding slot work in Layer 2 mode.

The working modes of all interfaces on the 24GE Ethernet LAN cards can be changed from Layer 2 mode to Layer 3 mode. After the reserved VLAN ID of the 9ES2 Ethernet LAN card (excluding the 9ES2 Ethernet LAN card, 8FE1GE Ethernet electrical interface card, and 4ES2G-S Ethernet LAN card installed on the AR1200 series router) is delivered using the **set reserved-vlan** command, the working modes of all interfaces on the card can be changed from Layer 2 mode to Layer 3 mode.

Example

Configure the reserved VLAN 100 on the interface card in slot 6.

```
<Huawei> system-view
[Huawei] set reserved-vlan 100 slot 6
```

6.3.40 shutdown (VLANIF interface view)

Function

Using the **shutdown** command, you can shut down a VLANIF interface.

Using the **undo shutdown** command, you can enable a VLANIF interface.

By default, a VLANIF interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VLANIF interface fails or is not needed, you can run the **shutdown** command on the VLANIF interface.

Precautions

A VLANIF interface is Up as long as an interface in the corresponding VLAN is Up.

After the VLANIF interface is shut down, the interface status changes to Down even if physical interfaces in the corresponding VLAN are Up.

After a VLANIF interface is shut down, none of the users that use the VLANIF interface address as the gateway address can communicate at Layer 3. In addition, the VLANIF interface address cannot be used in route calculation.

After a VLANIF interface is shut down, the dynamic ARP entry corresponding to the VLANIF interface starts aging in the ARP table. If the VLANIF interface address is in a static ARP entry, the ARP entry is not deleted.

Example

Enable VLANIF 2.

```
<Huawei> system-view
[Huawei] interface vlanif 2
[Huawei-Vlanif2] undo shutdown
```

Related Topics

6.3.11 display interface vlanif

6.3.41 subordinate group

Function

The **subordinate group** command configures subordinate group VLANs for a principal VLAN.

The **undo subordinate group** command removes subordinate group VLANs from a principal VLAN.

By default, a principal VLAN does not have any subordinate group VLAN.

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220, AR2220L, AR2220E, AR2240, AR2240C, AR3260, and AR3670 support MUX VLAN.

Only the 8FE1GE, 24ES2GP, and 24GE cards support MUX VLAN.

Format

subordinate group { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo subordinate group { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies a range of VLAN IDs. ● *vlan-id1* specifies the start VLAN ID. ● **to** *vlan-id2* specifies the end VLAN ID. If **to** *vlan-id2* is not specified, only one subordinate group VLAN is configured.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094 and must be greater than or equal to the value of *vlan-id1*.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.
  - Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add

customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

After interfaces using by employees are added to the subordinate group VLAN, employees can access servers of the enterprise and communicate with one another.

Prerequisites

The specified subordinate group VLANs have been created. The principal VLAN has been created.

The specified subordinate group VLANs are not super-VLANs and do not have any VLANIF interface.

The specified subordinate group VLANs do not have any VLANIF interface.

Before configuring a VLAN as a subordinate group VLAN, run the **undo subordinate group** command to delete all its member interfaces.

Follow-up Procedure

Add interfaces to subordinate group VLANs and enable the MUX VLAN function on the interfaces.

Precautions

Subordinate VLANs must be different from the principal VLAN.

A VLAN cannot be configured as a subordinate group VLAN and a subordinate separate VLAN simultaneously.

If you run the **subordinate group** command multiple times in the same VLAN view, all the specified VLANs are configured as subordinate group VLANs. A principal VLAN can be configured with a maximum of 32 subordinate group VLANs.

A subordinate group VLAN cannot be used to configure the VLANIF interface, Super-VLAN, Sub-VLAN.

Example

Configure VLAN 7 as the subordinate group VLAN of VLAN 5.

```
<Huawei> system-view
[Huawei] vlan 5
[Huawei-vlan5] subordinate group 7
```

Related Topics

6.3.42 subordinate separate

6.3.42 subordinate separate

Function

The **subordinate separate** command configures a subordinate separate VLAN for a principal VLAN.

The **undo subordinate separate** command removes the subordinate separate VLAN from a principal VLAN.

By default, a principal VLAN does not have any subordinate separate VLAN.

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220, AR2220L, AR2220E, AR2240, AR2240C, AR3260, and AR3670 support MUX VLAN.

Only the 8FE1GE, 24ES2GP, and 24GE cards support MUX VLAN.

Format

subordinate separate *vlan-id*

undo subordinate separate

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of an existing VLAN.	The value is an integer that ranges from 1 to 4094.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All employees and customers of an enterprise can access servers on the enterprise network. The enterprise allows employees to communicate but expects to isolate customers from one another. To meet this requirement, the enterprise can add the servers to a VLAN, add employees to another VLAN, and add each customer to a different VLAN. This wastes VLAN IDs and increases workload on VLAN configuration.

The MUX VLAN function is introduced to solve this problem. The MUX VLAN function isolates Layer 2 traffic between interfaces in a VLAN. This function involves the following VLANs:

- Principal VLAN: allows member interfaces to communicate with each other and with interfaces in subordinate VLANs.
- Subordinate VLAN
  - Subordinate separate VLAN: allows member interfaces to communicate with only interfaces in the principal VLAN. An interface in a subordinate

separate VLAN cannot communicate with interfaces in the same VLAN or other subordinate VLANs.

- Subordinate group VLAN: allows member interfaces to communicate with interfaces in the same VLAN and interfaces in the principal VLAN. An interface in a subordinate group VLAN cannot communicate with interfaces in other subordinate VLANs.

According to features of the preceding VLANs, the enterprise can add the servers to the principal VLAN, add employees to a subordinate group VLAN, and add customers to a subordinate separate VLAN. Customers are then allowed to access the servers but isolated from one another. This saves VLAN IDs on the enterprise network and facilitates network management.

After interfaces using by customers are added to the subordinate separate VLAN, customers can neither communicate with each other nor access servers of the enterprise.

Prerequisites

The specified subordinate separate VLAN has been created. The principal VLAN has been created.

The specified subordinate group VLANs are not super-VLANs and do not have any VLANIF interface.

The specified subordinate separate VLANs do not have any VLANIF interface.

Before configuring a VLAN as a subordinate separate VLAN, run the **undo subordinate separate** command to delete all its member interfaces.

Follow-up Procedure

Add interfaces to the subordinate separate VLAN and enable the MUX VLAN function on the interfaces.

Precautions

Subordinate VLANs must be different from the principal VLAN.

A VLAN cannot be configured as a subordinate group VLAN and a subordinate separate VLAN simultaneously.

A principal VLAN can be configured with only one subordinate separate VLAN. Before configuring another VLAN as the subordinate separate VLAN, run the **undo subordinate separate** command to delete the previous one.

A subordinate separate VLAN cannot be used to configure the VLANIF interface, Super-VLAN, or Sub-VLAN.

Example

Configure VLAN 6 as the subordinate separate VLAN of VLAN 5.

```
<Huawei> system-view
[Huawei] vlan 5
[Huawei-vlan5] subordinate separate 6
```

Related Topics

6.3.41 subordinate group

6.3.43 vlan

Function

The **vlan** command creates a VLAN and displays the VLAN view. If the VLAN exists, the VLAN view is displayed.

The **undo vlan** command deletes a VLAN.

By default, all interfaces belong to the default VLAN, named VLAN 1.

Format

vlan *vlan-id*

vlan batch { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan *vlan-id*

undo vlan batch { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID.	The value is an integer ranging from 1 to 4094.
batch	Configures VLANs in batches.	-
vlan-id1 **to** *vlan-id2*	Specifies range of VLANs to be configured in batches: ● *vlan-id1* specifies the start VLAN ID. ● *vlan-id2* specifies the end VLAN ID. *vlan-id2* must be greater than or equal to *vlan-id1*. *vlan-id1* and *vlan-id2* define a range together. ● If the parameter **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is created.	The *vlan-id1* and *vlan-id2* are integers ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce broadcast domains and enhance security on a complex network, VLANs can be created on the network to isolate the devices that do not need to communicate each other. The **vlan batch** command creates multiple VLANs at one time, simplifying VLAN configuration.

Follow-up Procedure

Assign VLANs according to network requirements.

Precautions

VLAN 1 is the default VLAN, which cannot be deleted and does not need to be created.

The **vlan** command can be used to create a VLAN and enter the VLAN view. If a VLAN has been created, the VLAN view is displayed after this command is used. The **vlan** command multiple times creates multiple VLANs. If a VLAN has been created, using this command cannot be used to create the same VLAN or modify the configurations of the VLAN.

The **vlan batch** command can be used to create multiple VLANs in batches. If a VLAN has been created, using this command cannot be used to create the same VLAN or modify the configurations of the VLAN. The **vlan batch** commands multiple times creates VLANs in multiple batches.

Before deleting a VLAN, run the **undo interface vlanif** command to delete the corresponding VLANIF interface.

Currently, the AR150 support a maximum of 64 VLANs; the AR100, AR120, AR160, AR200, AR1200, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204 support a maximum of 128 VLANs; the 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards support a maximum of 128 VLANs; other modes support a maximum of 4094 VLANs.

Example

Create VLAN 100 and enter the VLAN 100 view. If VLAN 100 exists, the VLAN 100 view is displayed directly.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100]
```

Related Topics

6.3.16 display vlan

6.3.44 vlan priority

Function

Using the **vlan priority** command, you can configure the 802.1p priority for a VLAN.

Using the **undo vlan priority** command, you can cancel the configuration.

By default, the system retains the original 802.1p priority of packets.

NOTE

The AR2201-48FE, AR2202-48FE, AR2240C, 8FE1GE card, and 24GE card do not support this command.

Format

vlan *vlan-id* **priority** *new-priority-value*

vlan batch *vlan-id1* **to** *vlan-id2* **priority** *new-priority-value*

undo vlan *vlan-id* **priority**

undo vlan batch *vlan-id1* **to** *vlan-id2* **priority**

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
new-priority-value	Specifies the 802.1p priority of a VLAN.	The value is an integer that ranges from 0 to 7.
batch	Configures VLANs in batches.	-
vlan-id1 **to** *vlan-id2*	Specifies range of VLANs to be configured in batches.	The *vlan-id1* and *vlan-id2* are integers ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring 802.1p priorities for VLANs, you can ensure that packets from the VLAN with the highest priority are transmitted first when congestion occurs.

Prerequisites

The specified VLAN has been created.

Configuration Impact

This command changes the 802.1p priority of packets from the specified VLAN. When congestion occurs, packets from the VLAN with the highest priority are transmitted first.

Precautions

The **vlan priority** command takes effect only for VLANs containing interfaces on the main control board of the devices.

Example

Set the priority of VLAN 11 to 3.

```
<Huawei> system-view
[Huawei] vlan 11 priority 3
```

Related Topics

6.3.17 display vlan priority

6.3.45 vlan vlan-name

Function

The **vlan vlan-name** command displays the view of a VLAN with the specified VLAN name.

The **undo vlan vlan-name** command deletes a VLAN with the specified VLAN name. After the command is used, the VLAN name is also deleted.

Format

vlan vlan-name *vlan-name*

undo vlan vlan-name *vlan-name*

Parameters

Parameter	Description	Value
vlan-name	Specifies the VLAN name.	The name is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **name** command is run to set a VLAN name, you can run the **vlan vlan-name** command in the system view to enter the corresponding VLAN view.

Assume that a device has multiple VLANs and each VLAN has a name. If you need to delete the VLAN that is used to transmit voice services but cannot remember the ID of the VLAN, you can run the **undo vlan vlan-name** command to delete the VLAN by inputting the VLAN name.

Prerequisites

Before running the **vlan vlan-name** command, ensure that the **name** command is run to set the VLAN name.

Precautions

When you run the **undo vlan vlan-name** command to delete a VLAN, services configured for the VLAN are deleted at the same time. The deleted services cannot be restored even if you recreate the VLAN. Therefore, exercise caution when running the **undo vlan vlan-name** command.

Example

Enter the view of the VLAN named **user1**.

```
<Huawei> system-view
[Huawei] vlan vlan-name user1
[Huawei-vlan2]
```

Related Topics

6.3.26 name (VLAN view)

6.3.46 termination-vid batch enable

Function

The **termination-vid batch enable** command enables a sub-interface to batch terminate VLAN tags.

The **undo termination-vid batch enable** command disables a sub-interface from batch terminating VLAN tags.

By default, a sub-interface is enabled to batch terminate VLAN tags.

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220E, AR2240, AR3200 series, and AR3600 series support this command.

Format

termination-vid batch enable

undo termination-vid batch enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where the device functions as the Terminal access and downstream users of the Terminal access belong to different VLANs, packets from each VLAN need to be terminated.

You can run this command to enable a sub-interface to batch terminate VLAN tags and run the **dot1q termination vid** or **qinq termination pe-vid ce-vid** command to specify multiple VLANs for termination.

NOTE

This command can be only executed on the Terminal access.

Precautions

If VLANs for termination have been configured on a sub-interface, run the **undo dot1q termination vid** or **undo qinq termination pe-vid ce-vid** command to cancel the configuration.

Example

Enable Eth2/0/0.1 to batch terminate VLAN tags.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0.1
[Huawei-Ethernet2/0/0.1] termination-vid batch enable
Info: This command applies to only Terminal access scenarios.
```

Related Topics

6.3.19 dot1q termination vid
6.3.36 qinq termination pe-vid ce-vid

6.4 Voice VLAN Configuration Commands

NOTE

Among the AR series routers, only the AR161EW-M1, AR161EW, AR169EW, and AR169EGW-L do not support Voice VLAN.

 Copyright © Huawei Technologies Co., Ltd.

6.4.1 display voice-vlan oui

Function

The **display voice-vlan oui** command displays the OUI address and OUI attributes of a voice VLAN.

Format

display voice-vlan oui

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the OUI address, OUI mask, and OUI description of the voice VLAN.

Example

Display the OUI address of the voice VLAN.

```
<Huawei> display voice-vlan oui
-----------------------------------------------
OuiAddress       Mask            Description
-----------------------------------------------
0022-3300-0000   ffff-ff00-0000   PhoneA
0011-2200-0000   ffff-ff00-0000   PhoneB
```

Table 6-34 Description of the display voice-vlan oui command output

Item	Description
OuiAddress	OUI address of the packets that can pass through the device. You can run the **voice-vlan mac-address** command to configure the OUI address.
Mask	OUI mask of the packets that can pass through the device.
Description	Description of the OUI address.

Related Topics

6.4.6 voice-vlan mac-address

6.4.2 display voice-vlan status

Function

The **display voice-vlan status** command displays information about the current voice VLAN.

Format

display voice-vlan [*vlan-id*] **status**

Parameters

Parameter	Description	Value
vlan-id	Displays information about a specified voice VLAN. If *vlan-id* is not specified, information about all voice VLANs is displayed.	The value is an integer that ranges from 2 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display voice-vlan status** command to view the following information:

- VLAN ID of the voice VLAN
- Working status of the voice VLAN
- Aging time of the voice VLAN
- 802.1p priority of the voice VLAN
- DSCP value of the voice VLAN
- Interface enabled with the voice VLAN
- The mode in Which an Interface Is Added to a Voice VLAN
- Secure mode of the voice VLAN on an interface
- Voice VLAN legacy

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about the current voice VLAN, such as the working status, secure mode, aging time, the 802.1p priority, DSCP value, and information about an interface that is enabled with voice VLAN.

```
<Huawei> display voice-vlan status
Voice VLAN Configurations:
--------------------------------------------------
Voice VLAN ID           :  2
Voice VLAN status       : Enable
Voice VLAN 8021p remark  : 6
Voice VLAN dscp remark   : 46
-----------------------------------------------------------
Port Information:
-----------------------------------------------------------
Port                    Add-Mode  Security-Mode  Legacy
-----------------------------------------------------------
Ethernet2/0/0           Manual    Security       Disable
```

Table 6-35 Description of the display voice-vlan status command output

Item	Description
Voice VLAN ID	ID of the voice VLAN.
Voice VLAN status	Status of the voice VLAN function. The value can be: ● Enable ● Disable You can run the **voice-vlan enable** command to configure the voice VLAN status.
Voice VLAN 8021p remark	802.1p priority of the voice VLAN. You can run the **voice-vlan remark** command to configure the 802.1p priority of the voice VLAN.
Voice VLAN dscp remark	DSCP value of the voice VLAN. You can run the **voice-vlan remark** command to configure the DSCP value of the voice VLAN.
Port	Number of the interface on which the voice VLAN function is enabled.
Add-Mode	Working mode of the voice VLAN. The value can be: ● Manual: indicates the manual mode. ● Auto: indicates the automatic mode. You can run the **voice-vlan mode** command to configure the working mode of the voice VLAN.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Security-Mode	Security mode of the voice VLAN on the interface. The value can be: ● Security: indicates the secure mode. ● Normal: indicates the normal mode. You can run the **voice-vlan security enable** command to configure the secure mode of the voice VLAN.
Legacy	Whether the interface can communicate with voice devices of other vendors. The value can be: ● Enable: indicates that the interface can communicate with voice devices of other vendors. ● Disable: indicates that the interface cannot communicate with voice devices of other vendors. You can run the **voice-vlan legacy enable** command to enable an interface to communicate with voice devices of other vendors.

Related Topics

6.4.4 voice-vlan enable
6.4.9 voice-vlan security enable
6.4.7 voice-vlan mode

6.4.3 voice-vlan aging-time

Function

The **voice-vlan aging-time** command sets the aging time of the voice VLAN.

The **undo voice-vlan aging-time** command restores the default aging time of the voice VLAN.

The default aging time is 1440 minutes.

Format

voice-vlan aging-time *minutes*

undo voice-vlan aging-time

Parameters

Parameter	Description	Value
minutes	Specifies the aging time of the voice VLAN.	The value ranges from 5 to 43200, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In auto mode, the device determines whether to add an interface to the voice VLAN based on the source MAC address of the voice packets received by the interface and changes the priority of the voice packets.

The system starts an aging timer for each MAC address entry of the voice VLAN. Before the aging timer expires:

- If the interface does not receive any voice packets, the device automatically deletes the interface from the voice VLAN and stops changing the priority of received packets.
- If the interface receives voice packets again, the device adds the interface to the voice VLAN and changes the priority of voice VLANs.

Precautions

In manual mode, you can add an interface to or delete an interface from the voice VLAN regardless of the aging time of the voice VLAN.

Example

Set the aging time of the voice VLAN to 100 minutes.

```
<Huawei> system-view
[Huawei] voice-vlan aging-time 100
```

Related Topics

6.4.2 display voice-vlan status

6.4.4 voice-vlan enable

Function

The **voice-vlan enable** command configures the specified VLAN as a voice VLAN and enables the voice VLAN function.

The **undo voice-vlan enable** command disables the voice VLAN function.

By default, the voice VLAN function is disabled on an interface.

Format

voice-vlan *vlan-id* **enable**

undo voice-vlan enable (port group view)

undo voice-vlan [*vlan-id*] **enable** (other interface views except the port group view)

Parameters

Parameter	Description	Value
vlan-id	Configures a specified VLAN as a voice VLAN.	The value is an integer that ranges from 2 to 4094.

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After being enabled with the voice VLAN function, a device is able to identify voice data based on source MAC addresses of received frames.

Precautions

If the voice VLAN configured on an interface works in automatic mode, you need to run the **port link-type** command to set the interface type to trunk, or hybrid.

To ensure normal transmission of different services, assign different VLAN IDs to the voice VLAN and default VLAN on the interface.

At a time, only one VLAN can be configured as the voice VLAN on an interface.

Example

Configure VLAN 2 as a voice VLAN and enable the voice VLAN function on Ethernet 2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] voice-vlan 2 enable
```

Related Topics

6.4.2 display voice-vlan status

6.4.5 voice-vlan legacy

Function

The **voice-vlan legacy** command enables CDP-compatible Voice VLAN function so that the switch encapsulates voice VLAN information in CDP packets and sends them to connected IP phones.

The **voice-vlan legacy** command disables CDP-compatible Voice VLAN function.

By default, CDP-compatible function is disabled.

Format

voice-vlan legacy enable

undo voice-vlan legacy enable

Parameters

None

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The switch can encapsulate voice VLAN information into LLDPDUs and send them to connected IP phones. However, IP phones of some vendors send Cisco Discovery Protocol (CDP) packets. You can run the **voice-vlan legacy enable** command to enable CDP-compatible function so that the switch encapsulates voice VLAN information in CDP packets and sends them to connected IP phones.

Prerequisites

The voice VLAN function has been enabled using the **voice-vlan enable** command.

Example

Enable CDP-compatible Voice VLAN function on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] voice-vlan 10 enable
[Huawei-Ethernet2/0/0] voice-vlan legacy enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

6.4.2 display voice-vlan status

6.4.6 voice-vlan mac-address

Function

The **voice-vlan mac-address** command sets the OUI address of the voice VLAN.

The **undo voice-vlan mac-address** command cancels the setting of the OUI address.

By default, no OUI address is set.

Format

voice-vlan mac-address *mac-address* **mask** *oui-mask* [**description** *text*]

undo voice-vlan mac-address { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Specifies the OUI address of voice packets that can be transmitted in the voice VLAN.	The value is in the format of H-H-H. H is a hexadecimal number that contains 4 digits, such as 00e0 and fc01. The address cannot be all 0s, multicast address, or broadcast address.
mask *oui-mask*	Specifies the mask of the OUI address.	The value is in the format of H-H-H. H is a 4-digit hexadecimal number that can be f or 0. The value in binary notation must start with consecutive 1s and end with consecutive 0s.
description *text*	Indicates the description of the OUI address.	The value is a string of 1 to 80 case-sensitive characters.
all	Specifies all the OUI address.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An OUI is the first 24 bits of a 48-bit MAC address assigned to each vendor by the Institute of Electrical and Electronics Engineers (IEEE). Voice packets sent by IP phones can be identified by the MAC address ranges requested by IP phone vendors.

In voice VLAN, the OUI is user-defined and not necessarily 24 bits long. The OUI is the result of the AND operation between the MAC address and mask in the **voice-vlan mac-address** command. The mask of the OUI cannot be all 0s.

Precautions

- The *mac-address* value cannot be all 0s or a multicast or broadcast address.
- A device can be configured with a maximum of 16 OUIs. When the device is configured with 16 OUIs, subsequent configurations will not take effect.

When you run the **undo voice-vlan mac-address** command to delete an OUI MAC address, set *mac-address* to the result of the logical AND operation between the OUI and the OUI mask that you set.

Example

Allow the voice packets coming from Phone A, an IP phone, to be identified by the voice VLAN. The MAC address of Phone A is 1234-1234-1234 and the OUI mask address is ffff-ff00-0000.

```
<Huawei> system-view
[Huawei] voice-vlan mac-address 1234-1234-1234 mask ffff-ff00-0000 description PhoneA
```

Related Topics

6.4.1 display voice-vlan oui

6.4.7 voice-vlan mode

Function

The **voice-vlan mode** command sets the working mode of the voice VLAN on an interface.

The **undo voice-vlan mode** command restores the mode in which an interface is added to a voice VLAN to the default.

By default, the voice VLAN of an interface works in automatic mode.

Format

voice-vlan mode { **auto** | **manual** }

undo voice-vlan mode manual

Parameters

Parameter	Description	Value
auto	Indicates the automatic mode of the voice VLAN.	-
manual	Indicates the manual mode of the voice VLAN.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ports can be added to a voice VLAN in either of the following modes:

- Automatic mode

  A voice VLAN-enabled port learns source MAC addresses of frames from voice devices, adds ports connecting the device to voice devices to a voice VLAN, and uses the voice VLAN aging timer to control the number of ports in the voice VLAN. If a voice VLAN-enabled port does not receive voice data from a voice device before the aging timer expires, the port will be automatically deleted from the voice VLAN. If the port receives voice data from the voice device again, the port will be automatically added to the voice VLAN.

  In auto mode, you cannot manually add ports to a voice VLAN.

- Manual mode

  After the voice VLAN function is enabled, ports connected to voice devices must be manually added to a voice VLAN. Otherwise, the voice VLAN function does not take effect.

Pre-configuration Tasks

Voice VLAN has been enabled using the **voice-vlan enable** command.

In auto mode, access interfaces cannot be added to a voice VLAN. To add the interface to the voice VLAN, run the **port link-type** command to change the link type of the interface to trunk or hybrid.

Precautions

The working mode of the voice VLAN on an interface does not affect the working mode of the voice VLAN on another interface. That is, voice VLANs on different interfaces can adopt different working modes.

 Copyright © Huawei Technologies Co., Ltd.

Example

On Eth2/0/0, configure the voice VLAN to work in manual mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] voice-vlan 10 enable
[Huawei-Ethernet2/0/0] voice-vlan mode manual
```

Related Topics

6.4.4 voice-vlan enable

6.4.2 display voice-vlan status

6.4.8 voice-vlan remark

Function

The **voice-vlan remark** command changes the 802.1p priority and DSCP value for a voice VLAN.

The **undo voice-vlan remark** command restores the 802.1p priority and DSCP value to their default values for a voice VLAN.

By default, the 802.1p priority and DSCP value for a voice VLAN are 6 and 46 respectively.

Format

voice-vlan remark { **8021p** *8021p-value* | **dscp** *dscp-value* } *

undo voice-vlan remark { **8021p** | **dscp** } *

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the 802.1p priority. The 802.1p priority is indicated by the value in the 3-bit PRI field in each 802.1Q VLAN frame. This field determines the transmission priority for data packets when a switching device is congested.	The value is an integer that ranges from 0 to 7. The default value 6. The larger the value, the higher the priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dscp *dscp-value*	Specify the DSCP value. The DSCP value is indicated by the 6 bits in the ToS field in the IPv4 packet header. DSCP, as the signaling for DiffServ, is used for QoS guarantee on IP networks. The traffic controller on the network gateway takes actions merely based on the information carried by the 6 bits. **NOTE** AR2204-27GE-P, AR2204-51GE-R, AR2204-51GE-P and AR2204-51GE do not support this parameter.	The value is an integer that ranges from 0 to 63. The default value is 46.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When voice VLAN is deployed on a network, voice service must be transmitted with a shorter delay than data service. Therefore, voice data packets need to be transmitted with a higher priority than other service data packets to reduce the transmission delay. You can run the **voice-vlan remark** command to change the 802.1p and DSCP priorities of a voice VLAN to allow voice data packets to be transmitted with a high priority.

Precautions

The **voice-vlan** *vlan-id* **enable** command has been run on an interface to specify a VLAN as a voice VLAN, and the voice VLAN function has been enabled on the interface.

If the **voice-vlan remark** command has been run multiple times, the last configuration overrides the previous configurations.

Example

Set the DSCP value for a voice VLAN to 20.

```
<Huawei> system-view
[Huawei] voice-vlan remark dscp 20
```

 Copyright © Huawei Technologies Co., Ltd.

6.4.9 voice-vlan security enable

Function

The **voice-vlan security enable** command enables the secure mode of the voice VLAN.

The **undo voice-vlan security enable** command disables the secure mode of the voice VLAN.

By default, the secure mode of the voice VLAN is disabled.

Format

voice-vlan security enable

undo voice-vlan security enable

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the data filtering mechanism, a voice VLAN works in either secure or normal mode:

- Secure mode

  A voice VLAN-enabled inbound port transmits only frames of which the source MAC addresses match OUIs configured on the device, discards the voice data not belong to the current voice VLAN and the other data can be forwarded normally.

  The secure mode prevents a voice VLAN from being attacked by malicious data flows, but consumes system resources to check frames.

- Normal mode

  A voice VLAN-enabled inbound port transmits both voice and non-voice data. The port does not compare source MAC addresses in received frames with configured OUIs, exposing a voice VLAN to malicious attacks.

Pre-configuration Tasks

Voice VLAN has been enabled using the **voice-vlan enable** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

When a voice VLAN works in secure mode, only voice packets in the VLAN can be transmitted in the voice VLAN.

To allow both voice packets and data packets to be transmitted in the voice VLAN, configure the voice VLAN to work in normal mode.

The AR100&AR120&AR150&AR160&AR200&AR1200 series devices do not support the secure mode.

Example

Disable the secure mode of the voice VLAN on Ethernet 2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo voice-vlan security enable
```

Related Topics

6.4.1 display voice-vlan oui
6.4.2 display voice-vlan status

6.5 QinQ Configuration Commands

NOTE

Only the AR100, AR120, AR150, AR160, AR200 series routers support QinQ tunneling.

AR1220F, AR1220E, AR1220EV, and AR1220EVW support QinQ tunneling.

Only the AR1200, AR2200, AR3200, AR3600 series routers support termination sub-interface access to the VPN.

6.5.1 ce-vlan ignore

Function

The **ce-vlan ignore** command enables a Dot1q termination sub-interface on an L2VPN network to ignore the inner tag in a QinQ packet and terminate the outer tag.

The **undo ce-vlan ignore** command disables a Dot1q termination sub-interface on an L2VPN network from forwarding QinQ packets.

By default, a Dot1q termination sub-interface on an L2VPN network discards QinQ packets.

NOTE

The AR200 series do not supports this command.

Format

ce-vlan ignore

undo ce-vlan ignore

Parameters

None

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

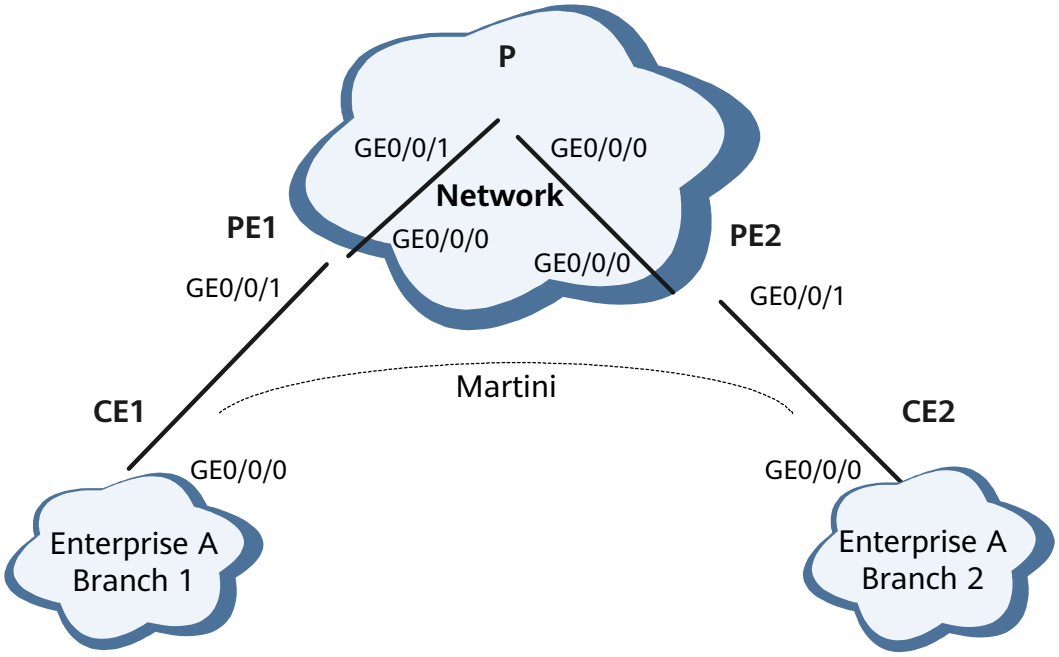
When users communicate over an L2VPN (including VLL), a Dot1q termination sub-interface processes only single-tagged Dot1q packets and discards double-tagged QinQ packets.

When VLANs are assigned on a VPN and CEs connect to the ISP network through PEs, whether user packets carry VLAN tags and types of VLAN tags are unknown. After a CE interface connected to a PE adds the outer VLAN tag allocated by the ISP to user packets, the Dot1q termination sub-interface on the PE interface connected to the CE receives both Dot1q and QinQ packets. By default, a Dot1q termination sub-interface cannot forward QinQ packets. You need to configure the Dot1q termination sub-interface to ignore the inner tag in QinQ packets and terminate the outer tag so that the Dot1q termination sub-interface can forward QinQ packets.

When a Dot1q sub-interface functions as the ingress or egress of a Martini VLL, run this command to implement transparent transmission of user packets over the ISP network.

 Copyright © Huawei Technologies Co., Ltd.

Figure 6-1 Networking diagram of connecting the Dot1q termination sub-interface to the VLL



Prerequisites

- The encapsulation mode of the sub-interface has been set to Dot1q termination by running the **dot1q termination vid** command in the sub-interface view.
- L2VPN (including VLL) has been deployed.

  For details on how to configure VLL, see "VLL Configuration" in the *AR Configuration Guide - VPN*.

Precautions

When the L2VPN configuration is deleted, the **ce-vlan ignore** command on the sub-interface is also deleted.

Example

On PE1, enable the Dot1q termination sub-interface GE0/0/1.1 connected to the VLL to ignore the inner tag in a QinQ packet and terminate the outer tag.

```
<Huawei> system-view
[Huawei] mpls lsr-id 10.1.1.9
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls l2vpn
[Huawei-l2vpn] quit
[Huawei] interface gigabitethernet0/0/1.1
[Huawei-GigabitEthernet0/0/1.1] dot1q termination vid 10
[Huawei-GigabitEthernet0/0/1.1] mpls l2vc 10.3.3.9 101
[Huawei-GigabitEthernet0/0/1.1] ce-vlan ignore
```

Related Topics

6.3.19 dot1q termination vid

6.5.2 qinq termination l2

Function

The **qinq termination l2** command configures the mode in which a sub-interface for QinQ VLAN tag termination connects to a PWE3/VLL network.

The **undo qinq termination l2** command deletes the mode configured for a sub-interface for QinQ VLAN tag termination in which the sub-interface connects to a PWE3/VLL network.

By default, a sub-interface for QinQ VLAN tag termination connects to a PWE3/VLL network in asymmetry mode.

Format

qinq termination l2 { **symmetry** | **asymmetry** }

undo qinq termination l2

Parameters

Parameter	Description	Value
symmetry	Configures the sub-interface for QinQ VLAN tag termination to connect to a PWE3/VLL network in symmetry mode.	-
asymmetry	Configures the sub-interface for QinQ VLAN tag termination to connect to a PWE3/VLL network in asymmetry mode. In asymmetry mode, a sub-interface does not send inner tags as part of data to the peer. Inner tags cannot be used to identify users, and therefore cannot be specified with a range of VLAN IDs. **NOTE** Generally, of the two tags carried by a packet sent by a Huawei device, the inner tag specifies the user, and the outer tag specifies the service.	-

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

More QinQ encapsulation and termination modes are provided to differentiate users and services and save VLAN resources. These modes are widely used for refined operation.

If users communicate over an L2VPN (a PWE3, VLL network), you can run the **qinq termination l2** command on the sub-interfaces for QinQ VLAN tag termination of L2VPN edge devices to configure the mode in which the sub-interfaces connect to the L2VPN.

Prerequisites

The following configurations are required before the **qinq termination l2** command is used on a sub-interface:

- The encapsulation type of the sub-interface is set to QinQ termination.

  The **qinq termination pe-vid ce-vid** command is used in the sub-interface view to set the encapsulation type of the sub-interface to QinQ termination.
- A PWE3, VLL network is deployed.

  For PWE3, VLL configurations, see the chapter "PWE3 Configuration", "VLL Configuration" in the *AR Configuration Guide - VPN*.

Configuration Impact

- If the **qinq termination l2 symmetry** command is used on a sub-interface for QinQ VLAN tag termination, the sub-interface connects to the L2VPN in symmetry mode. MAC address learning is performed only for outer tags carried in packets. The sub-interface sends inner tags as part of data to the peer.
- If the **qinq termination l2 asymmetry** command is used on a sub-interface for QinQ VLAN tag termination, the sub-interface connects to the L2VPN in asymmetry mode. MAC address learning is performed for both inner and outer tags carried in packets. The sub-interface does not send inner tags as part of data to the peer.

The edge device on an L2VPN searches the MAC address table based on the destination MAC address carried in a packet to obtain the outbound interface. Then, the device encapsulates the packet based on the mode in which its sub-interface connects to the L2VPN. **Table 6-36** and **Table 6-37** show the modes in which a sub-interface connects to an L2VPN.

Table 6-36 Packet processing on an inbound interface

Inbound Interface Type	PWE3/VLL	
	Ethernet Encapsulation	VLAN Encapsulation
Symmetry mode	Removes the outer tag.	Keeps both inner and outer tags unchanged.
Asymmetry mode	Removes both the inner and outer tags.	Removes both inner and outer tags, and then adds another tag.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-37 Packet processing on an outbound interface

Outbound Interface Type	PWE3/VLL	
	Ethernet Encapsulation	VLAN Encapsulation
Symmetry mode	Adds an outer tag.	Replaces the outer tag.
Asymmetry mode	Adds two tags.	Remove the existing tag, and then add two tags.

Example

Configure the sub-interface for QinQ VLAN tag termination GE1/0/0.2 to connect to an L2VPN in asymmetry mode.

```
[Huawei] interface gigabitethernet1/0/0.2
[Huawei-GigabitEthernet1/0/0.2] qinq termination l2 asymmetry
[Huawei-GigabitEthernet1/0/0.2] qinq termination pe-vid 1 ce-vid 1
```

Related Topics

6.3.36 qinq termination pe-vid ce-vid

6.5.3 qinq protocol

Function

The **qinq protocol** command sets the TPID value in the outer VLAN tag of an interface.

The **undo qinq protocol** command restores the default TPID value in the outer VLAN tag.

By default, the TPID value in the outer VLAN tag is 0x8100.

Format

qinq protocol *protocol-id*

undo qinq protocol

Parameters

Parameter	Description	Value
protocol-id	Specifies the TPID value in the outer VLAN tag.	The value is a 4-digit hexadecimal integer that ranges from 0x0600 to 0xFFFF. The default TPID value is 0x8100.

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, VE interface view, XGE interface view, PON interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Devices from different vendors or in different network plans may use different TPID values in VLAN tags of VLAN packets. To adapt to an existing network plan, the device supports TPID value configuration. You can set the TPID value on the device to be the same as the TPID value in the network plan to ensure compatibility with the current network.

Precautions

The **portswitch** command has been executed in the VE interface view to switch the VE interface from Layer 3 to Layer 2.

The device directly connected to an interface must be able to identify the TPID value in the outer VLAN tag on the interface.

The **qinq protocol** command identifies incoming frames, and adds or changes the TPID value of outgoing frames.

The TPID value specified by the **qinq protocol** command must be different from TPID values of specific protocols. Otherwise, the interface cannot correctly classify protocol packets. The TPID value cannot be any of the values in the following table.

Table 6-38 Description of protocol types and values

Protocol Type	Value
ARP	0x0806
RARP	0x8035
IP	0x0800
IPv6	0x86DD
PPPoE	0x8863/0x8864
MPLS	0x8847/0x8848
IPX/SPX	0x8137
LACP	0x8809
802.1x	0x888E
HGMP	0x88A7

 Copyright © Huawei Technologies Co., Ltd.

Protocol Type	Value
Reserved	0xFFFD/0xFFFE/0xFFFF

Example

Set the TPID value in the outer VLAN tag of QinQ frames to 0x9100 on GE0/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-GigabitEthernet0/0/0] qinq protocol 9100
```

Set the TPID value in the outer VLAN tag of QinQ frames to 0x9100 on VE0/0/1.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] qinq protocol 9100
```

6.5.4 vlan allow-pass

Function

The **vlan allow-pass** command configures a VLAN allowed by a sub-interface.

The **undo vlan allow-pass** command cancels the configuration.

By default, no allowed VLAN is configured on a sub-interface.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series, AR1220E, AR1220EV, AR1220EVW, and AR1220F support this command.

The 4G.SHDSL and VDSL2 cards in PTM mode support this command.

Format

vlan allow-pass vid { { *vlan-id1* } [**to** *vlan-id2*] } &<1–8>

vlan allow-pass default

undo vlan allow-pass vid { { *vlan-id1* } [**to** *vlan-id2*] } &<1–8>

undo vlan allow-pass default

Parameters

Parameter	Description	Value
vid *vlan-id1* [**to** *vlan-id2*]	Specifies VLANs from which packets are allowed to pass through. • *vlan-id1* specifies the start VLAN ID. • *vlan-id2* specifies the end VLAN ID.	*vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be greater than *vlan-id1*. *vlan-id2* and *vlan-id1* specify a range of VLANs. If **to** *vlan-id2* is not specified, the system allows only the VLAN specified by *vlan-id1*.
default	Indicates that packets are forwarded through the default sub-interface when the packets do not match other QinQ or VLAN mapping entries on a sub-interface.	-

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring other QinQ functions except VLAN-ID-based VLAN Stacking, run the **vlan allow-pass** { **vid** *vlan-id1* [**to** *vlan-id2*] | **default** } command to configure the VLAN allowed by a sub-interface.

Prerequisites

The sub-interface has been added to a bridge group.

Precautions

When you run the **vlan allow-pass** command on a sub-interface multiple times, multiple VLANs are specified.

Both **vlan stacking** and **vlan allow-pass** can configure VLANs allowed by sub-interfaces. The VLANs allowed by all sub-interfaces of a main interface cannot overlap.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE0/0/0.1 to allow VLANs 10 to 30 and 40 to 50.

```
<Huawei> system-view
[Huawei] bridge 1
[Huawei-bridge1] quit
[Huawei] interface gigabitethernet 0/0/0.1
[Huawei-GigabitEthernet0/0/0.1] bridge 1
[Huawei-GigabitEthernet0/0/0.1] bridge vlan-transmit enable
[Huawei-GigabitEthernet0/0/0.1] vlan allow-pass vid 10 to 30 40 to 50
```

6.5.5 vlan dot1q-tunnel(Sub-interface)

Function

The **vlan dot1q-tunnel** command configures the dotlq tunnel function on a sub-interface.

The **undo vlan dot1q-tunnel** command cancels the dotlq tunnel function on a sub-interface.

By default, the dotlq tunnel function is disabled on a sub-interface.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series, AR1220E, AR1220EV, AR1220EVW, and AR1220F support this command.

The 4G.SHDSL and VDSL2 cards in PTM mode support this command.

Format

vlan dot1q-tunnel *tunnel-vlan-id* [**native vid** *native-vlan-id*]

undo vlan dot1q-tunnel

Parameters

Parameter	Description	Value
tunnel-vlan-id	Specifies the VLAN ID in the (outer) VLAN tag to be added to a packet.	The value is an integer that ranges from 1 to 4094.
native vid *native-vlan-id*	Specifies the VLAN ID in the inner VLAN tag to be added to the received untagged VLAN packets.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Dot1q tunnel isolates a carrier network from a user network and is widely used when users connect to a carrier network. When private networks connect to a carrier network through CEs and PEs, run the **vlan dot1q-tunnel** command on CE interfaces connected to PEs so that the CE interfaces add the outer VLAN tag allocated by the carrier to user packets. This implementation saves VLAN IDs and allows user packets to be transparently transmitted on the carrier network.

After the **vlan dot1q-tunnel** command is used, a packet sent from the CE to the PE is processed as follows:

- If the packet carries a tag, the CE adds the outer VLAN tag (tunnel tag) specified by *tunnel-vlan-id* to the packet.
- If the packet does not carry any tag, the CE adds the inner VLAN tag (native tag) specified by *native-vlan-id* and the outer VLAN tag specified by *tunnel-vlan-id* to the packet.

A packet sent from the PE to the CE is processed as follows:

- If the outer VLAN ID of the packet is the same as the tunnel tag specified by *tunnel-vlan-id* but the inner VLAN ID differs from the inner VLAN tag specified by *native-vlan-id*, the CE removes the outer VLAN tag.
- If the outer VLAN ID of the packet is the same as the tunnel tag specified by *tunnel-vlan-id* and the inner VLAN ID is the same as the inner VLAN tag specified by *native-vlan-id*, the CE removes both the inner and outer VLAN tags.

Prerequisites

The sub-interface has been added to a bridge group and the VLANs allowed by the sub-interface has been configured using the **vlan allow-pass** command.

The VLANs allowed by the sub-interface include user VLANs and the VLAN specified by *tunnel-vlan-id*.

Precautions

The **vlan dot1q-tunnel** command can be only executed at one time on a sub-interface and the VLAN specified by *tunnel-vlan-id* must be allowed by the sub-interface.

You can configure only dot1q tunnel function, vlan stacking, or vlan mapping on a sub-interface.

Example

User packets contain packets with VLAN 30 and untagged packets. Enable the dotlq tunnel function on GE0/0/0.1. When received packets carry VLAN tags, the outer VLAN tag with VLAN 10 is added to the packets. When received packets are untagged packets, the inner VLAN tag with VLAN 20 and the outer VLAN tag with VLAN 10 are added to the packets.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] bridge 1
[Huawei-bridge1] quit
[Huawei] interface gigabitethernet 0/0/0.1
[Huawei-GigabitEthernet0/0/0.1] bridge 1
[Huawei-GigabitEthernet0/0/0.1] bridge vlan-transmit enable
[Huawei-GigabitEthernet0/0/0.1] vlan allow-pass vid 10
[Huawei-GigabitEthernet0/0/0.1] vlan allow-pass vid 30
[Huawei-GigabitEthernet0/0/0.1] vlan dot1q-tunnel 10 native vid 20
```

6.5.6 vlan dot1q-tunnel enable

Function

The **vlan dot1q-tunnel enable** command enables basic QinQ on a Layer 2 Ethernet interface.

The **undo vlan dot1q-tunnel enable** command disables basic QinQ on a Layer 2 Ethernet interface.

By default, basic QinQ is disabled on a Layer 2 Ethernet interface.

Format

vlan dot1q-tunnel enable

undo vlan dot1q-tunnel enable

Parameters

None

Views

Virtual-Ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Basic QinQ is performed based on interfaces. Basic QinQ can be configured to expand VLAN space when multiple VLANs are required. Basic QinQ expands VLAN space by adding an additional 802.1Q tag to 802.1Q tagged packets, solving the problem of insufficient VLAN resources.

To implement basic QinQ on a Layer 3 sub-interface, add the sub-interface to the bridge and run the **vlan allow-pass** command to configure the VLAN allowed by the sub-interface. You only need to run the **vlan dot1q-tunnel enable** command on the Layer 2 Ethernet interface to enable basic QinQ, simplifying the configuration.

Prerequisites

The **portswitch** command has been executed in the VE interface view to switch the VE interface from Layer 3 to Layer 2.

The **port link-type access** command has been executed to set the link type of the Layer 2 Ethernet interface to access.

Precautions

Example

Enable basic QinQ on Layer 2 VE0/0/1.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type access
[Huawei-Virtual-Ethernet0/0/1] vlan dot1q-tunnel enable
```

6.5.7 vlan stacking (Sub-interface)

Function

The **vlan stacking** command configures VLAN stacking on a sub-interface.

The **undo vlan stacking** command cancels VLAN stacking on a sub-interface.

By default, VLAN stacking is disabled on a sub-interface.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series, AR1220E, AR1220EV, AR1220EVW, and AR1220F support this command.

The 4G.SHDSL and VDSL2 cards in PTM mode support this command.

Format

vlan stacking { **default** | **vid** *low-ce-vid* [**to** *high-ce-vid*] } **pe-vid** *pe-vid* [**remark-8021p** *8021p-value2*]

vlan stacking 8021p *8021p-value1* **pe-vid** *pe-vid* [**remark-8021p** *8021p-value2*]

undo vlan stacking { **default** | **vid** *low-ce-vid* [**to** *high-ce-vid*] | **8021p** *8021p-value1* }

Parameters

Parameter	Description	Value
default	Indicates that packets are forwarded through the default sub-interface when the packets do not match other VLAN stacking entries on a sub-interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vid *low-ce-vid* [**to** *high-ce-vid*]	Specifies VLANs from which packets are allowed to pass through. ● *low-ce-vid* specifies the start VLAN ID. ● *high-ce-vid* specifies the end VLAN ID.	*low-ce-vid* and *high-ce-vid* are integers that range from 1 to 4094. *high-ce-vid* must be greater than *low-ce-vid*. *high-ce-vid* and *low-ce-vid* specify a range of VLANs.
pe-vid *pe-vid*	Specifies the VLAN ID in the outer S-VLAN tag. The outer VLAN tag is added to packets matching **default**, **vid** *low-ce-vid* [**to** *high-ce-vid*], or **8021p** *8021p-value1*.	The value is an integer that ranges from 1 to 4094.
remark-8021p *8021p-value2*	Specifies the re-marked 802.1p priority in the stacked outer tag.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. By default, the 802.1p priority in the stacked outer VLAN tag is the same as the 802.1p priority in the inner VLAN tag.
8021p *8021p-value1*	Specifies the 802.1p priority in a VLAN frame. The 802.1p priority is represented by a three-bit PRI (priority) field in an 802.1Q frame, and is used when high-priority packets need to be first forwarded.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When private networks connect to a carrier network through CEs and PEs, run the **vlan stacking** command on CE interfaces connected to PEs so that the CE interfaces add the outer VLAN tag allocated by the carrier to user packets. This implementation saves VLAN IDs and allows user packets to be transparently transmitted on the carrier network.

An 802.1p priority indicates a packet priority. Generally, different services of a user use different priorities. A carrier can establish different data transmission networks for different services based on 802.1p priorities so that services on the carrier network can be differentiated.

Unlike the **vlan dot1q-tunnel** used to add outer VLAN tags based on interfaces, the **vlan stacking** command adds outer VLAN tags based on 802.1p priorities or VLAN IDs. VLAN stacking is also called selective QinQ.

After the **vlan stacking** command is used, packets are processed as follows:

- After the **vlan stacking 8021p** *8021p-value1* **pe-vid** *pe-vid* [**remark-8021p** *8021p-value2*] command is used on an interface, the VLAN tag specified by *pe-vid* is added to packets with the 802.1p priority specified by *8021p-value1* and the 802.1p priority specified by *8021p-value2* in the stacked tag can be modified.
- After the **vlan stacking vid** *low-ce-vid* [**to** *high-ce-vid*] **pe-vid** *pe-vid* [**remark-8021p** *8021p-value2*] command is used on an interface, packets with VLAN IDs specified by *low-ce-vid* [**to** *high-ce-vid*] are allowed to pass through, the outer S-VLAN tag specified by *pe-vid* can be added to packets, and the 802.1p priority specified by *8021p-value2* in the stacked tag can be modified.
- After the **vlan stacking default pe-vid** *pe-vid* [**remark-8021p** *8021p-value2*] command is used on an interface, packets that do not match other VLAN stacking entries on the interface are forwarded by the default sub-interface, the outer S-VLAN tag specified by *pe-vid* can be added to packets, and the 802.1p priority specified by *8021p-value2* in the stacked tag can be modified.

The outer VLAN tag of packets are removed before the packets are sent.

Prerequisites

The sub-interface has been added to a bridge group.

Precautions

You can run this command multiple times on each sub-interface:

- When you run the **vlan stacking vid** *low-ce-vid* [**to** *high-ce-vid*] **pe-vid** *pe-vid* [**remark-8021p** *8021p-value2*] command multiple times to configure VLAN ID-based VLAN stacking, ensure that values of *pe-vid* are the same and values of **remark-8021p** *8021p-value2* are the same.
- When you run the **vlan stacking 8021p** *8021p-value1* **pe-vid** *pe-vid* [**remark-8021p** *8021p-value2*] command multiple times to configure 802.1p priority-based VLAN stacking, values of both *pe-vid* and **remark-8021p** *8021p-value2* can be different.

The **vlan stacking default** command can be executed only on a sub-interface among all sub-interfaces of each main interface.

 Copyright © Huawei Technologies Co., Ltd.

You can configure only dot1q tunnel function, vlan stacking, or vlan mapping on a sub-interface.

When canceling VLAN stacking on a sub-interface, the VLAN range should be totally the same as configuring VLAN stacking.

Both **VLAN stacking** and **VLAN allow-pass** can configure VLANs allowed by sub-interfaces. The VLANs allowed by all sub-interfaces of a main interface cannot overlap.

Example

Configure VLAN stacking on GE0/0/0.1. When received packets use the VLAN tag with VLAN IDs 10 to 13, outer VLAN 100 is added to the packet.

```
<Huawei> system-view
[Huawei] bridge 1
[Huawei-bridge1] quit
[Huawei] interface gigabitethernet 0/0/0.1
[Huawei-GigabitEthernet0/0/0.1] bridge 1
[Huawei-GigabitEthernet0/0/0.1] bridge vlan-transmit enable
[Huawei-GigabitEthernet0/0/0.1] vlan stacking vid 10 to 13 pe-vid 100
```

6.5.8 vlan stacking vid

Function

The **vlan-stacking vid** command configures VLAN stacking on a Layer 2 Ethernet interface.

The **undo vlan stacking vid** command cancels the configuration.

By default, VLAN stacking is not configured on a Layer 2 Ethernet interface.

Format

vlan stacking vid *low-ce-vid* [**to** *high-ce-vid*] **pe-vid** *pe-vid-value* [**remark-8021p** *8021p-val*]

undo vlan stacking vid *low-ce-vid* [**to** *high-ce-vid*]

Parameters

Parameter	Description	Value
low-ce-vid [**to** *high-ce-vid*]	Specifies VLANs from which packets are allowed to pass through. • *low-ce-vid* specifies the start VLAN ID. • *high-ce-vid* specifies the end VLAN ID.	*low-ce-vid* and *high-ce-vid* are integers that range from 1 to 4094. *high-ce-vid* must be greater than *low-ce-vid*. *high-ce-vid* and *low-ce-vid* specify a range of VLANs.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pe-vid *pe-vid-value*	Specifies the VLAN ID in the outer S-VLAN tag. The device adds the outer VLAN tag to packets matching **vid** *low-ce-vid* [**to** *high-ce-vid*] or *8021p* **8021p-value1**.	The value is an integer that ranges from 1 to 4094.
remark-8021p *8021p-val*	Specifies the re-marked 802.1p priority in the stacked outer tag.	The value is an integer that ranges from 0 to 7. A greater value indicates a higher priority. By default, the 802.1p priority in the stacked outer VLAN tag is the same as the 802.1p priority in the inner VLAN tag.

Views

Virtual-Ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When different private networks connect to a carrier network by connecting CEs to PEs, the CEs need to identify users and use different QoS scheduling policies or distribute services. You can run the **vlan stacking** command on a CE interface connected to a PE to configure the VLAN allowed by the interface and add the outer VLAN tag allocated by the carrier to user packets. This implementation saves VLAN IDs and allows user packets to be transparently transmitted on the carrier network.

An 802.1p priority indicates a packet priority. Generally, different services of users use different priorities. A carrier can establish different data transmission networks for different services based on 802.1p priorities so that services on the carrier network can be differentiated.

Unlike the **vlan dot1q-tunnel** command used to add outer VLAN tags based on interfaces, the **vlan stacking** command adds outer VLAN tags based on VLAN IDs. QinQ stacking is also called selective QinQ.

After the **vlan stacking vid** *low-ce-vid* [**to** *high-ce-vid*] **pe-vid** *pe-vid-value* [**remark-8021p** *8021p-val*] command is used on an interface, packets with VLAN

IDs specified by *low-ce-vid* **to** *high-ce-vid* are allowed to pass through, the outer S-VLAN tag specified by *pe-vid* can be added to the packets, and the 802.1p priority in the stacked tag is changed to *8021p-val*.

Prerequisites

The **portswitch** command has been executed in the VE interface view to switch the VE interface from Layer 3 to Layer 2.

The **port link-type hybrid** command has been executed to set the link type of the Layer 2 Ethernet interface to hybrid.

Precautions

- VLAN stacking and VLAN mapping can take effect, but VLAN IDs of multiple CEs must be unique, VLAN IDs in the original and mapped tags must be different, and VLAN IDs of multiple PEs must be unique.
- Layer 2 Ethernet interfaces support only VLAN ID-based VLAN stacking, and do not support VLAN stacking based on 802.1p priorities or VLAN IDs and 802.1p priorities.
- When VLAN stacking is canceled on a Layer 2 Ethernet interface, the VLAN ID range allowed must be the same as the configured VLAN ID range.
- This command can be configured on an interface multiple times, and a maximum of 128 VLAN stacking entries can be configured on all interfaces.

Example

Configure VLAN stacking on Layer 2 VE0/0/1 to add VLAN 200 to received packets tagged with VLAN 20 to VLAN 23 and re-mark the 802.1p priority with 2.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type hybrid
[Huawei-Virtual-Ethernet0/0/1] port hybrid tagged vlan 100
[Huawei-Virtual-Ethernet0/0/1] vlan stacking vid 20 to 23 pe-vid 200 remark-8021p 2
```

6.6 VLAN Mapping Configuration Commands

NOTE

Only the AR100&AR120&AR150&AR160&AR200, AR1220F, AR1220E, AR1220EV, and AR1220EVW support VLAN mapping.

6.6.1 vlan mapping 8021p

Function

The **vlan mapping 8021p** command configures 802.1p priority-based VLAN mapping on a sub-interface.

The **undo vlan mapping 8021p** command cancels 802.1p priority-based VLAN mapping on a sub-interface.

By default, 802.1p priority-based VLAN mapping is not configured on a sub-interface.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series, AR1220E, AR1220EV, AR1220EVW, and AR1220F support this command.

The 4G.SHDSL and VDSL2 cards in PTM mode support this command.

Format

vlan mapping 8021p *8021p-value1* **map-8021p** *8021p-value2*

undo vlan mapping 8021p *8021p-value1*

Parameters

Parameter	Description	Value
8021p-value1	Specifies the 802.1p priority in frames received by a sub-interface.	The value is an integer that ranges from 0 to 7.
map-8021p *8021p-value2*	Specifies the mapped 802.1p priority.	The value is an integer that ranges from 0 to 7.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If some packets sent from one LAN to another need to be first forwarded, their 802.1p priorities in the packets need to be changed. You can run the **vlan mapping 8021p** command on the LAN edge device to enable 802.1p priority-based VLAN mapping. 802.1p priority-based VLAN mapping maps *8021p-value1* to *8021p-value2* in the inbound direction and then forwards packets based on mapped 802.1p priorities. In the outbound direction, packets are not processed.

Pre-configuration Tasks

The sub-interface has been added to a bridge group and the VLANs allowed by the sub-interface has been configured using the **vlan allow-pass** command.

Precautions

You can configure only dot1q tunnel function, vlan stacking, or vlan mapping on a sub-interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure VLAN mapping on the sub-interface GE0/0/0.1 to map the 802.1p priority of data frames of VLAN 10 from 1 to 6.

```
<Huawei> system-view
[Huawei] bridge 1
[Huawei-bridge1] quit
[Huawei] interface gigabitethernet 0/0/0.1
[Huawei-GigabitEthernet0/0/0.1] bridge 1
[Huawei-GigabitEthernet0/0/0.1] bridge vlan-transmit enable
[Huawei-GigabitEthernet0/0/0.1] vlan allow-pass vid 10
[Huawei-GigabitEthernet0/0/0.1] vlan mapping 8021p 1 map-8021p 6
```

Related Topics

6.6.2 vlan mapping vid(Sub-interface)

6.6.2 vlan mapping vid(Sub-interface)

Function

The **vlan mapping vid** command configures VLAN ID-based VLAN mapping on a sub-interface.

The **undo vlan mapping vid** command cancels VLAN ID-based VLAN mapping on a sub-interface.

By default, VLAN ID-based VLAN mapping is not configured on a sub-interface.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series, AR1220E, AR1220EV, AR1220EVW, and AR1220F support this command.

The 4G.SHDSL and VDSL2 cards in PTM mode support this command.

Format

vlan mapping vid *vlan-id1* **map-vlan** *vlan-id2*

undo vlan mapping vid *vlan-id1* **map-vlan** *vlan-id2*

Parameters

Parameter	Description	Value
vlan-id1	Specifies the VLAN ID in the VLAN tag carried in a frame received by a sub-interface.	The value is an integer that ranges from 1 to 4094.
map-vlan *vlan-id2*	Specifies the VLAN ID in the mapped VLAN tag.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets are sent from one LAN to another, their VLAN IDs need to be changed in the following scenarios:

- The VLAN IDs deployed in new sites and old sites conflict, but new sites need to communicate with old sites.
- The sites connecting to the public network have conflicting VLAN IDs because of improper planning. These sites do not need to communicate.
- The VLAN IDs on both ends of the private network are different.

You can run the **vlan mapping vid** command on the LAN edge device to configure VLAN ID-based VLAN mapping. On the sub-interface, VLAN ID-based VLAN mapping maps *vlan-id1* to *vlan-id2* in the inbound direction and *vlan-id2* to *vlan-id1* in the outbound direction, and then forwards packets.

Pre-configuration Tasks

The sub-interface has been added to a bridge group and the VLANs allowed by the sub-interface has been configured using the **vlan allow-pass** command.

The VLANs allowed by the sub-interface include VLANs specified by *vlan-id1* in **vlan mapping vid** *vlan-id1* **map-vlan** *vlan-id2*.

Precautions

When the **vlan mapping vid** command is executed multiple times, *vlan-id2* in the **vlan mapping vid** command on a sub-interface must be different from *vlan-id1* and *vlan-id2* in the **vlan mapping vid** command on other sub-interfaces of the same main interface.

You can configure only dot1q tunnel function, vlan stacking, or vlan mapping on a sub-interface.

Example

Configure VLAN mapping on GE0/0/0.1 to map VLAN 100 in received packets to VLAN 200.

```
<Huawei> system-view
[Huawei] bridge 1
[Huawei-bridge1] quit
[Huawei] interface gigabitethernet 0/0/0.1
[Huawei-GigabitEthernet0/0/0.1] bridge 1
[Huawei-GigabitEthernet0/0/0.1] bridge vlan-transmit enable
[Huawei-GigabitEthernet0/0/0.1] vlan allow-pass vid 100
[Huawei-GigabitEthernet0/0/0.1] vlan mapping vid 100 map-vlan 200
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

6.6.1 vlan mapping 8021p

6.6.3 vlan mapping vid

Function

The **vlan mapping vid** command configures VLAN ID-based VLAN mapping on a Layer 2 Ethernet interface.

The **undo vlan mapping vid** command cancels the configuration of VLAN ID-based VLAN mapping on a Layer 2 Ethernet interface.

By default, VLAN ID-based VLAN mapping is not configured on a Layer 2 Ethernet interface.

Format

vlan mapping vid *vid-value1* **map-vlan** *vid-value2* [**remark-8021p** *8021p-val*] [**inbound**]

undo vlan mapping vid *vid-value1*

Parameters

Parameter	Description	Value
vid-value1	Specifies the VLAN ID in the VLAN tag carried in a frame received by a Layer 2 Ethernet interface.	The value is an integer that ranges from 1 to 4094.
map-vlan *vid-value2*	Specifies the VLAN ID in the mapped VLAN tag.	The value is an integer that ranges from 1 to 4094.
remark-8021p *8021p-val*	Specifies the mapped 802.1p priority.	The value is an integer that ranges from 0 to 7.
inbound	Maps tags in packets on an interface in the inbound direction. If this parameter is not specified, the device maps tags in packets on an interface in the inbound and outbound directions. **NOTE** Layer 2 VE interfaces do not support this parameter.	-

Views

, Virtual-Ethernet interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets are sent from one LAN to another, their VLAN IDs need to be changed. For example, VLAN IDs need to be changed in the following scenarios:

- The VLAN IDs deployed in new sites and old sites conflict, but new sites need to communicate with old sites.
- The VLAN ID planning of each site on the public network is different. As a result, the VLAN IDs conflict. The sites, however, do not need to communicate.
- The VLAN IDs on both ends of the private network are different.

You can run the **vlan mapping vid** command on the LAN edge device to configure VLAN ID-based VLAN mapping. VLAN ID-based VLAN mapping enables the device to map *vlan-id1* in received packets to *vlan-id2* in the inbound direction and *vlan-id2* to *vlan-id1* in the outbound direction. Then the device forwards packets.

Prerequisites

The **portswitch** command has been executed in the VE interface view to switch the VE interface from Layer 3 to Layer 2.

The **port link-type** { **hybrid** | **trunk** } command has been executed to set the link type of the Layer 2 Ethernet interface to trunk or hybrid.

Precautions

- The VLAN ID in the tag of the received frame on an interface must be different from the mapped VLAN ID.
- The mapped outer VLAN must exist and the interface must join the original and mapped VLANs in tagged mode.
- VLAN stacking and VLAN mapping can take effect, but VLAN IDs of multiple CEs must be unique, VLAN IDs in the original and mapped tags must be different, and VLAN IDs of multiple PEs must be unique.
- Layer 2 Ethernet interfaces support only VLAN ID-based VLAN mapping, and do not support VLAN mapping based on 802.1p priorities or VLAN IDs and 802.1p priorities.
- This command can be configured on an interface multiple times, and a maximum of 128 VLAN mapping entries can be configured on all interfaces.

Example

Configure VLAN mapping on Layer 2 VE0/0/1 to map VLAN 1 in received packets to VLAN 2 and re-mark the 802.1p priority with 3.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] port link-type trunk
[Huawei-Virtual-Ethernet0/0/1] vlan mapping vid 1 map-vlan 2 remark-8021p 3
```

 Copyright © Huawei Technologies Co., Ltd.

6.7 GVRP Configuration Commands

NOTE

- AR100&AR120 series routers do not support GVRP.
- Among the AR160 series routers, only AR161, AR161G-L, AR161W, AR169, AR169G-L, AR169-P-M9, AR161G-L, AR169CVW, AR169CVW-4B4S, AR161G-U, AR169W-P-M9, and AR169RW-P-M9 do not support GVRP.
- Among the AR1200 series routers, only AR1220E, AR1220EV, and AR1220EVW do not support GVRP.
- The 9ES2, 4GE-2S, 4ES2G-S, and 4ES2GP-S cards do not support GVRP.

6.7.1 display garp statistics

Function

The **display garp statistics** command displays statistics about the Generic Attribute Registration Protocol (GARP) on an interface.

Format

display garp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about GARP on the specified interface. • *interface-type* specifies the type of an interface. • *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the GARP VLAN Registration Protocol (GVRP) is enabled on an interface, the system collects statistics about GVRP packets sent, received, and discarded on the

interface. You can view the statistics to check whether the GVRP function on the interface is normal.

When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system displays statistics about GARP packets on all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system displays statistics about GARP packets on the specified interface.

Example

Display statistics about GARP packets on a specified interface.

```
<Huawei> display garp statistics interface ethernet 2/0/0

 GARP statistics on port Ethernet2/0/0
   Number of GVRP frames received       : 0
   Number of GVRP frames transmitted    : 0
   Number of frames discarded           : 0
```

Table 6-39 Description of the display garp statistics command output

Item	Description
Number of GVRP frames received	Number of GVRP packets received by an interface.
Number of GVRP frames transmitted	Number of GVRP packets sent by an interface.
Number of frames discarded	Number of packets discarded by an interface.

Related Topics

6.7.9 gvrp

6.7.2 display garp timer

Function

The **display garp timer** command displays the values of GARP timers.

Format

display garp timer [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the GARP timers of the specified interface. • *interface-type* specifies the type of an interface. • *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display garp timer** command displays the values of GARP timers. When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system displays GARP timers of all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system displays GARP timers of the specified interface.

Example

Display the values of the GARP timers of the specified interface.

```
<Huawei> display garp timer interface ethernet 2/0/0

 GARP timers on port Ethernet2/0/0
   GARP JoinTime              : 80 centiseconds
   GARP LeaveTime             : 240 centiseconds
   GARP LeaveAllTime          : 1000 centiseconds
   GARP HoldTime              : 40 centiseconds
```

Table 6-40 Description of the display garp timer command output

Item	Description
GARP JoinTime	Value of the Join timer. You can run the **garp timer** command to set the Join timer.
GARP LeaveTime	Value of the Leave timer. You can run the **garp timer** command to set the Leave timer.

Item	Description
GARP LeaveAllTime	Value of the LeaveAll timer. You can run the **garp timer leaveall** command to set the LeaveAll timer.
GARP HoldTime	Value of the Hold timer. You can run the **garp timer** command to set the Hold timer.

Related Topics

6.7.7 garp timer

6.7.3 display gvrp state

Function

The **display gvrp state** command displays information about the GVRP state machine.

Format

display gvrp state interface *interface-type interface-number* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the GVRP state machine of the specified interface. • *interface-type* specifies the type of an interface. • *interface-number* specifies the number of an interface.	-
vlan *vlan-id*	Displays information about the state machine of the specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The GVRP function has two types of state machines: Applicant state machine and Registrar state machine.

An applicant implements declaration of attributes. If no message is lost during transmission, an applicant can ensure that all registrars have registered an attribute after it sends a Join message or receives a JoinIn message. To ensure reliable transmission of messages, the applicant needs to send two Join messages or send a Join message and receive a JoinIn message to confirm that all registrars have registered an attribute. Therefore, a simple counter is used. The counter starts from 0 and increases by 1 every time the applicant sends a Join message or receives a JoinIn message. The maximum value of the counter is 2. If the applicant receives a JoinEmpty, Empty, Leave, or LeaveAll message, the counter is reset to 0. This indicates that the applicant can send PDUs only when the value of the counter is smaller than 2.

The Join timer controls the interval for sending Join messages, but not every attribute has its own Join timer. A GVRP participant uses a Join timer. The value of the Join timer must be long enough to ensure that all the attributes can be packaged in a message and transmitted in a declaration.

- Anxious applicants

  Depending on the value of the applicant counter, an applicant may be in either of the following states:

  - V (very anxious): The value of the counter is 0, indicating that the applicant does not send a Join message or receive a JoinIn message.
  - A (anxious): The value of the counter is 1, indicating that no message is lost and all the registrars have registered the attribute.
  - Q (quiet): The value of the counter is 2, indicating that the applicant does not need to send Join messages.

- Members and observers

  The preceding states are applicable to normal situations. In special cases, for example, when some terminals do not need to send registration messages and only need to retain all the GARP state machines, these terminals must be separated from other entities. Therefore, the concept of member and observer is introduced. A member refers to an entity that tries to declare or retain an attribute value or an entity that has not sent a Leave message yet. An observer refers to an entity that traces the states of attributes but does not declare attributes.

  Multiple entities may actively join or leave the same attribute. To minimize the number of Join or Leave messages in this situation, members are classified into active members and passive members. Therefore, the following states are introduced:

  - A: Active member
  - P: Passive member
  - O: Observer

In addition, when an active member must send a Leave message to cancel a declaration, the active member enters the leaving state. Considering all these states, the state machine of an applicant has multiple state combinations, as shown in the following table.

State Combination	Very Anxious	Anxious	Quiet	Leaving
Active Member	VA	AA	QA	LA
Passive Member	VP	AP	QP	-
Observer	VO	AO	QO	LO

When a passive member needs to cancel a declaration, it can switch to the observer state. Therefore, the leaving passive member state does not exist.

A registrar has a Leave timer and three states: IN (attribute registered), MTR (attribute deregistered), and LV (attribute being deregistered). If a registrar in LV state does not receive the declaration of an attribute within the timeout interval of the Leave timer, the registrar enters the MTR state.

A registrar changes to different states depending on the received message:

- When receiving a Join message, the registrar changes to the IN state.
- When receiving a Leave or LeaveAll message, the registrar changes from the IN state to the LV state and starts the Leave timer. If the registrar is not in IN state, it does not change its state after receiving a Leave or LeaveAll message.
- The registrar does not change its state after receiving an Empty message.

Example

Display information about the GVRP state machine.

```
<Huawei> display gvrp state interface ethernet 2/0/0 vlan 100
  GVRP state of VLAN 100 on port Ethernet2/0/0

      Applicant state machine :    VP
      Registrar state machine :    MTR
```

Table 6-41 Description of the display gvrp state command output

Item	Description
Applicant state machine	State machine of the applicant.
Registrar state machine	State machine of the registrar.

Related Topics

6.7.9 gvrp

6.7.4 display gvrp statistics

Function

The **display gvrp statistics** command displays statistics about GVRP on an interface.

Format

display gvrp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the statistics about GVRP on the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface. If no interface is specified, the system displays statistics about GVRP on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display gvrp statistics** command displays statistics about GVRP on an interface, including the GVRP status, number of GVRP registration failures, source MAC address of the last GVRP PDU, and registration mode of the interface.

Example

Display the statistics about GVRP on an interface.

```
<Huawei> display gvrp statistics interface ethernet 2/0/0

 GVRP statistics on port Ethernet2/0/0
   GVRP status                  : Enabled
   GVRP registrations failed      : 0
   GVRP last PDU origin           : 0000-0000-0000
   GVRP registration type         : Normal
```

Table 6-42 Description of the display gvrp statistics command output

Item	Description
GVRP status	GVRP state. The value can be: ● Enabled ● Disabled
GVRP registrations failed	Number of GVRP registration failures.
GVRP last PDU origin	Source MAC address of the last GVRP PDU.
GVRP registration type	GVRP registration type of an interface, which is configured by the **gvrp registration** command. The registration type can be: ● Fixed ● Forbidden ● Normal

Related Topics

6.7.9 gvrp
6.7.10 gvrp registration

6.7.5 display gvrp status

Function

The **display gvrp status** command displays whether global GVRP is enabled.

Format

display gvrp status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device with GVRP enabled can dynamically register VLANs or deregister VLANs from an interface. You can run the **display gvrp status** command to check whether GVRP is enabled.

Example

Display the enabling status of global GVRP.

```
<Huawei> display gvrp status
Info:  GVRP is enabled.
```

Table 6-43 Description of the display gvrp status command output

Item	Description
GVRP is enabled	Global GVRP is enabled.

Related Topics

6.7.9 gvrp

6.7.6 display gvrp vlan-operation

Function

The **display gvrp vlan-operation** command displays the operation of adding a specified interface to dynamic VLANs.

Format

display gvrp vlan-operation interface *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays operations related to dynamic VLANs performed on the specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display gvrp vlan-operation** command displays the dynamic VLANs to which an interface is added.

Example

Display the operation of adding an interface to dynamic VLANs.

```
<Huawei> display gvrp vlan-operation interface Ethernet 2/0/0
  Dynamic VLAN operations on port Ethernet2/0/0

      Operations of adding VLAN to TRUNK          : none
```

Table 6-44 Description of the display gvrp vlan-operation command output

Item	Description
Operations of adding VLAN to TRUNK	Operation of adding a trunk interface to dynamic VLANs.

Related Topics

6.7.9 gvrp

6.7.7 garp timer

Function

The **garp timer** command sets GARP timers.

The **undo garp timer** command restores the default values of GARP timers.

By default, the value of the Hold timer is 40 centiseconds, the value of the Join timer is 80 centiseconds, and the value of the Leave timer is 240 centiseconds.

Format

garp timer { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** }

Parameters

Parameter	Description	Value
hold *timer-value*	Sets the value of the GARP Hold timer.	• Lower limit: 40 centiseconds • Upper limit: smaller than or equal to half the value of the Join timer, changing with the value of the Join timer • The value can be exactly divided by 20, in centiseconds.
join *timer-value*	Sets the value of the GARP Join timer.	• Lower limit: greater than or equal to two times the value of the Hold timer, changing with the value of the Hold timer • Upper limit: smaller than half the value of the Leave timer, changing with the value of the Leave timer • The value can be exactly divided by 20, in centiseconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
leave *timer-value*	Sets the value of the GARP Leave timer.	• Lower limit: greater than two times the value of the Join timer, changing with the value of the Join timer • Upper limit: smaller than the value of the LeaveAll timer, changing with the value of the LeaveAll timer • The value can be exactly divided by 20, in centiseconds.

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can set the following GARP timers:

- Join timer: controls sending of Join messages including JoinIn messages and JoinEmpty messages.
- Hold timer: controls sending of Join messages (JoinIn messages and JoinEmpty messages) and Leave messages (LeaveIn messages and LeaveEmpty messages).
- Leave timer: controls attribute deregistration.

You can set the GARP timers to control sending of GARP protocol packets.

Prerequisite

The physical port has been added to the port group before running the **garp timer** command in the port group view.

Precautions

When using the **garp timer** command to set the GARP timers, pay attention to the following points:

- The **garp timer** can be used only on trunk interfaces.
- The **undo garp timer** command restores the default values of GARP timers. If the default value of a timer is out of the valid range, the **undo garp timer** command does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

- The value range of each timer changes with the values of the other timers. If a value you set for a timer is not in the allowed range, you can change the value of the timer that determines the value range of this timer.
- To restore the default values of all the GARP timers, restore the Hold timer to the default value, and then restore the Join timer, Leave timer, and LeaveAll timer to the default values in sequence.

NOTE

In actual application, it is recommended that you use the following values of the GVRP timers:

- GARP Hold timer: 100 centiseconds (1 second)
- GARP Join timer: 600 centiseconds (6 seconds)
- GARP Leave timer: 3000 centiseconds (30 seconds)
- GARP LeaveAll timer: 12000 centiseconds (2 minutes)

When more than 100 dynamic VLANs are created, use the preceding recommended values. When the number of dynamic VLANs increases, lengths of the GARP timers need to be increased.

Example

Set the LeaveALL timer of Ethernet2/0/0 to 2000 centiseconds.

```
<Huawei> system-view
[Huawei] garp timer leaveall 2000
```

Set the Leave timer of Ethernet 2/0/0 to 800 centiseconds.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] garp timer leave 800
```

Set the Join timer of Ethernet 2/0/0 to 300 centiseconds.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] garp timer join 300
```

Set the Hold timer of Ethernet 2/0/0 to 100 centiseconds.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] garp timer hold 100
```

Related Topics

6.7.2 display garp timer
6.7.8 garp timer leaveall

6.7.8 garp timer leaveall

Function

The **garp timer leaveall** command sets the GARP LeaveAll timer.

The **undo garp timer leaveall** command restores the default value of the GARP LeaveAll timer.

The default value of the LeaveAll timer is 1000 centiseconds (10 seconds).

Format

garp timer leaveall *timer-value*

undo garp timer leaveall

Parameters

Parameter	Description	Value
timer-value	Specifies the value of the GARP LeaveAll timer.	The value is an integer that ranges from 260 to 32000 and that can be exactly divided by 20, in centiseconds. The value of the LeaveAll timer must be greater than the values of Leave timers on all the interfaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GARP participant is enabled, the LeaveAll timer is started. When the LeaveAll timer expires, the GARP participant sends LeaveAll messages to request other GARP participants to re-register all its attributes. Then the LeaveAll timer restarts.

Devices on a network may have different settings for the LeaveAll timer. In this case, all the devices use the smallest LeaveAll timer value on the network. When the LeaveAll timer of a device expires, the device sends LeaveAll messages to other devices. After other devices receive the LeaveAll messages, they reset their LeaveAll timers. Therefore, only the LeaveAll timer with the smallest value takes effect even if devices have different settings for the LeaveAll timer.

Prerequisites

Before setting GARP timers on an interface, you must enable GVRP globally.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The Leave timer length on an interface is restricted by the global LeaveAll timer length. When configuring the global LeaveAll timer, ensure that all the interfaces that have a GARP Leave timer configured are working properly.

Example

Set the LeaveAll timer to 2000 centiseconds.

```
<Huawei> system-view
[Huawei] garp timer leaveall 2000
```

Related Topics

6.7.7 garp timer

6.7.2 display garp timer

6.7.9 gvrp

Function

The **gvrp** command enables GVRP globally or on an interface.

The **undo gvrp** command disables GVRP globally or on an interface.

By default, GVRP is disabled globally and on each interface.

Format

gvrp

undo gvrp

Parameters

None

Views

System view, Ethernet interface view, GE interface view,port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device with GVRP enabled can dynamically register VLANs or deregister VLANs from an interface. To make GVRP take effect, run the **gvrp** command both in the system view and interface view.

Precautions

When configuring GVRP, pay attention to the following points:

- If you run the **gvrp** command in the system view, GVRP is enabled globally. If you run this command in the interface view, GVRP is enabled on the interface.
- Before enabling GVRP on an interface, you must enable GVRP globally.
- Before enabling GVRP on an interface, you must set the link type of the interface to trunk.

Example

Enable GVRP globally.

```
<Huawei> system-view
[Huawei] gvrp
```

Enable GVRP on Ethernet 2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] gvrp
```

Related Topics

6.7.5 display gvrp status

6.7.4 display gvrp statistics

6.7.10 gvrp registration

Function

The **gvrp registration** command sets the registration mode of a GVRP interface.

The **undo gvrp registration** command restores the default registration mode of a GVRP interface.

By default, the registration mode of a GVRP interface is **normal**.

Format

gvrp registration { **fixed** | **forbidden** | **normal** }

undo gvrp registration

Parameters

Parameter	Description	Value
fixed	Indicates the fixed registration mode.	-
forbidden	Indicates the forbidden registration mode.	-
normal	Indicates the normal registration mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A GVRP interface supports three registration modes:

- Normal: In this mode, the GVRP interface can dynamically register and deregister VLANs, and transmit dynamic VLAN registration information and static VLAN registration information.
- Fixed: In this mode, the GVRP interface is disabled from dynamically registering and deregistering VLANs and can transmit only the static VLAN registration information. If the registration mode of a trunk interface is set to **fixed**, the interface allows only the manually configured VLANs to pass even if it is configured to allow all the VLANs to pass.
- Forbidden: In this mode, the GVRP interface is disabled from dynamically registering and deregistering VLANs and can transmit only information about VLAN 1. If the registration mode of a trunk interface is set to **forbidden**, the interface allows only VLAN 1 to pass even if it is configured to allow all the VLANs.

Pre-configuration Tasks

Before setting the registration mode of an interface, you must enable GVRP globally and configure the interface as a trunk interface.

Example

Set the registration mode of Eth2/0/0 to **fixed**.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] gvrp
[Huawei-Ethernet2/0/0] gvrp registration fixed
```

Related Topics

6.7.9 gvrp

6.7.4 display gvrp statistics

6.7.11 reset garp statistics

Function

The **reset garp statistics** command clears statistics about GARP packets on an interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset garp statistics [**interface** { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-5>]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears the statistics about GARP packets on a specified interface. ● *interface-type* specifies the type of an interface. ● *interface-number* specifies the number of an interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before collecting GARP traffic statistics on a specific interface within a certain period, you need to clear the existing GARP traffic statistics on this interface.

When using this command, pay attention to the following points:

- If **interface** *interface-type interface-number* is not specified, the system clears statistics about GARP packets on all the interfaces.
- If **interface** *interface-type interface-number* is specified, the system clears statistics about GARP packets on the specified interface.

Precautions

GARP statistics cannot be restored after being cleared. Confirm your action before using this command.

Example

Clear statistics about GARP packets on Eth2/0/0.

```
<Huawei> reset garp statistics interface ethernet 2/0/0
```

Related Topics

6.7.9 gvrp

6.8 STP/RSTP/MSTP Configuration Commands

NOTE

AR120 series, AR161, AR161G-L, AR161W, AR169, AR169-P-M9, AR169G-L, AR169W, AR161EW, AR161EW-M1, AR161G-Lc, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L do not support MSTP.

6.8.1 active region-configuration

Function

The **active region-configuration** command activates the configuration of a multiple spanning tree (MST) region.

Format

active region-configuration

Parameters

None

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring MST region parameters, especially VLAN mapping tables for MST regions, is likely to cause network topology flapping. To reduce network flapping, make sure that newly configured MST region parameters take effect only after the **active region-configuration** command is run.

Precautions

After the **active region-configuration** command is run, configured MST region parameters will take effect and the spanning tree will be recalculated.

Example

Map VLAN 5 to the spanning tree instance 2 and activate the configuration.

```
<Huawei> system-view
```

```
[Huawei] stp region-configuration
[Huawei-mst-region] instance 2 vlan 5
[Huawei-mst-region] active region-configuration
```

Related Topics

6.8.2 check region-configuration

6.8.10 display stp region-configuration

6.8.2 check region-configuration

Function

The **check region-configuration** command displays the configuration of an MST region such as the region name, revision level, and VLAN mapping table.

Format

check region-configuration

Parameters

None

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each region is called an MST region and each spanning tree is called a multiple spanning tree instance (MSTI).

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- MST region revision level
- Mappings between MSTIs and VLANs

To ensure that MST region configurations on each switching device are correct, you are recommended to run the **check region-configuration** command to check the MST region configurations before running the **active region-configuration** command. If the MST region configurations are correct, run the **active region-configuration** command to activate them.

Precautions

By default, VLANs that are not mapped to any instances with non-zero IDs using the **instance** command are mapped to instance 0.

Example

Display the configuration of an MST region.

```
<Huawei> system-view
[Huawei] stp region-configuration
[Huawei-mst-region] check region-configuration
 Admin configuration
   Format selector    :0
   Region name        :00b010000001
   Revision level     :0

   Instance   VLANs Mapped
     0       1 to 9, 11 to 4094
    16       10
```

Table 6-45 Description of the check region-configuration command output

Item	Description
Format selector	Selection factor defined by MSTP
Region name	Name of the MST region. To configure the name for an MST region, run the **region-name** command.
Revision level	Revision level of the MST region. To set the revision level of the MST region, run the **revision-level** command.
Instance VLANs Mapped	Mapping between MSTIs and VLANs. To configure the mapping between MSTIs and VLANs, run the **instance** or **vlan-mapping modulo**.

Related Topics

6.8.1 active region-configuration

6.8.3 display snmp-agent trap feature-name mstp all

Function

The **display snmp-agent trap feature-name mstp all** command displays all trap messages of the MSTP module.

Format

display snmp-agent trap feature-name mstp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

The **display snmp-agent trap feature-name mstp all** command displays whether all trap functions of the MSTP module are enabled.

Example

Display all trap messages of the MSTP module.

```
<Huawei>display snmp-agent trap feature-name mstp all
-------------------------------------------------------------------------------
Feature name: MSTP
Trap number : 8
-------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwMstpiPortStateForwarding       off                      off
hwMstpiPortStateDiscarding       off                      off
hwMstpiBridgeLostRootPrimary     off                      off
hwMstpiPortBpduGuarded           off                      off
hwMstpiPortRootGuarded           off                      off
hwMstpiPortLoopGuarded           off                      off
hwMstpiEdgePortChanged           off                      off
hwMstpProLoopbackDetected        off                      off
```

Table 6-46 Description of the **display snmp-agent trap feature-name mstp all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.

Item	Description
Trap name	Name of a trap message of the MSTP module: • **hwMstpiPortStateForwarding**: indicates that the port status changes to Forwarding. • **hwMstpiPortStateDiscarding**: indicates that the port status changes to Discarding. • **hwMstpiBridgeLostRootPrimary**: indicates that the current device is no longer the root bridge. • **hwMstpiPortBpduGuarded**: indicates that the edge port enabled with the BPDU guard function can receive BPDUs. • **hwMstpiPortRootGuarded**: indicates that the port enabled with the root guard function receives BPDUs with higher priorities. • **hwMstpiPortLoopGuarded**: indicates that the port enabled with the loop guard function does not receive any BPDU in a specified period. • **hwMstpiEdgePortChanged**: indicates that the edge port that is not enabled with the BPDU guard function is no longer the edge port after receiving BPDUs. • **hwMstpProLoopbackDetected**: indicates that the port is blocked with the port detects loopback.
Default switch status	Whether the default trap function is enabled: • on: The trap function is enabled. • off: The trap function is disabled.
Current switch status	Whether the current trap function is enabled: • on: The trap function is enabled. • off: The trap function is disabled.

Related Topics

6.8.20 snmp-agent trap enable feature-name mstp

6.8.4 display stp

Function

The **display stp** command displays the status of and statistics on a spanning tree instance.

Format

display stp [**instance** *instance-id*] [**interface** *interface-type interface-number*] [**brief**]

Parameters

Parameter	Description	Value
instance *instance-id*	Displays the status and statistics of a spanning tree instance. If **instance** *instance-id* is not specified, the status and statistics of all spanning tree instances will be displayed in the sequence of the interface numbers.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: ● AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. ● AR2220, AR2240, and AR3200 series: 49.
interface *interface-type interface-number*	Displays the information of a spanning tree on a specified interface. If **interface** *interface-type interface-number* is not specified, the status and statistics of all interfaces will be displayed in the sequence of the interface numbers.	-
brief	Displays the brief status.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display stp** command is used to check whether STP/RSTP/MSTP is run in the existing switching device or specified interface.

- If the **Protocol Status** field value is **Disabled**, STP/RSTP/MSTP is not run.
- If STP/RSTP/MSTP has been run, information such as the working mode of STP/RSTP/MSTPT will be displayed.

When the network planner has deployed STP/RSTP/MSTP on the network, you can run the **display stp** command to check whether the configurations and calculation result.

 Copyright © Huawei Technologies Co., Ltd.

Example

When the **stp enable** command does not run, the status and statistics of STP are displayed.

```
<Huawei> display stp
 Protocol Status       :Disabled
 Protocol Standard     :IEEE 802.1s
 Version               :3
 CIST Bridge Priority  :32768
 MAC address           :00e0-6343-6800
 Max age(s)            :20
 Forward delay(s)      :15
 Hello time(s)         :2
 Max hops              :20
```

Table 6-47 Description table of the display stp command output

Item	Description
Protocol Status	Status of the protocol. ● Disabled ● Enabled
Protocol Standard	Standards of the protocol.
Version	Protocol version: ● 0: STP ● 2: RSTP ● 3: MSTP To set the protocol version, run the **stp mode** command.
CIST Bridge Priority	Priority of the switch in the CIST. To set the STP priority, run the **stp priority** command.
MAC address	MAC address of the switch.
Max age (s)	Maximum TTL of BPDU. To set the value of Max Age, run the **stp timer max-age** command.
Forward delay (s)	Time taken by interface status transition. To set the value of Forward Delay, run the **stp timer forward-delay** command.
Hello time (s)	Interval for sending BPDUs from the root switch. To set the hello time, run the **stp timer hello** command.
Max hops	Maximum number of hops in an MST region. To set the maximum number of hops, run the **stp max-hops** command.

Display the status of and statistics on the spanning tree instance 0 on Eth2/0/0.

```
<Huawei> display stp instance 0 interface ethernet 2/0/0
-------[CIST Global Info][Mode MSTP]-------
```

```
CIST Bridge         :32768.00e0-fc0e-a421
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :32768.00e0-fc0e-a421 / 0
CIST RegRoot/IRPC   :32768.00e0-fc0e-a421 / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :0
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 23h:9m:30s
Number of TC        :1
----[Port3(Ethernet2/0/0)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T)    :Config=auto / Active=19
 Designated Bridge/Port   :32768.00e0-fc0e-a421 / 128.1229
 Port Edged          :Config=disabled / Active=disabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :3 packets/hello-time
 Protection Type     :None
 Config-digest-snoop :snooped=false
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 0
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :147
         TCN: 0, Config: 0, RST: 0, MST: 147
 BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
```

Table 6-48 Description of the display stp instance command output

Item	Description
CIST Global Info	CIST global information.
Mode MSTP	The operation mode is MSTP. By default, the mode is MSTP. To set the operation mode, run the **stp mode** command.
CIST Bridge	ID of the CIST bridge. ● The previous 16 bits are the priority of the switch in CIST. ● The latter 48 bits is the MAC address of the switch.
Config Times	Configured bridge protocol parameters: ● **Hello**: interval at which Bridge Protocol Data Units (BPDUs) are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region

Item	Description
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region
CIST Root/ERPC	CIST root bridge ID/External path cost (the path cost from the switch to the CIST root bridge.)
CIST RegRoot/IRPC	Region root bridge ID/Internal path cost (the path cost from the switch to region root bridge.)
CIST RootPortId	CIST root port ID. "0.0" indicates the switch is a root bridge and has no root port.
BPDU-Protection	BPDU protection function: ● Disabled ● Enabled
TC or TCN received	Number of the received TC or TCN packets.
TC count per hello	Number of TC packets received within a hello interval.
STP Converge Mode	STP converge mode
Time since last TC	Period from the last topology change to now.
Number of TC	Topology change count.
Port Protocol	The status of the port protocol is as follows: ● Enable: STP is enabled on the port. ● disable: STP is disabled on the port.
Port Role	In CIST area, the four port roles are as follows: ● Root Port ● Designated Port ● Alternate Port ● Backup Port
Port Priority	Priority of the port. To set the priority for a port, run the **stp port priority** command.
Port Cost(Dot1T)	Path cost of the port. It is calculated by dot1t algorithm. ● config: refers to the path cost that is configure manually. ● active: refers to the path cost actually.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Designated Bridge/ Port	ID of the designated switch and port. The first 16 bits of the switch ID represent the priority of the switch in the CIST region; the last 48 bits represent the MAC address of the switch. The first 4 bits of the port ID represent the priority and the last 12 bits represent the port number.
Port Edged	Edged port that is specified by the administrator: ● enabled ● disabled **Config** indicates that the value is configured by using the **stp edged-port** command. **Active** indicates the actual value.
Point-to-point	Link type of the port. **Config** indicates that the link type is configured by running the **stp point-to-point** command. **Active** indicates the actual link type.
Transit Limit	Limit of the BPDUs sent by the current port during each Hello time. To set the limit of the BPDUs sent by the current port during each Hello time, run the **stp transmit-limit (interface view)** command.
Protection Type	The protection type is as follows: ● root-protection: valid only on a designed port. ● loop-protection: valid only on a root port or an alternate one.
Port STP Mode	STP mode on an interface.
Config-digest-snoop	The configuration digest snooping function. The command output is displayed only after the **stp config-digest-snoop** command is configured and the configuration digest snooping function is enabled on the port. If the port is not enabled with the function, the command output is not displayed: ● snooped=false: The configuration digest of the packets on the remote end is the same as that on the local end. ● snooped=true: The configuration digest of the packets on the remote end is different from that on the local end.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Port Protocol Type	Format of the packets that the interface receives and sends. The formats are as follows: ● auto ● legacy ● dot1s The default value is **auto**. **Config** indicates that the packet format is configured by running the **stp compliance** command. **Active** indicates the actual packet format.
PortTimes	Values in the bridge protocol information of the interface: ● Hello: the period of sending BPDUs. ● MaxAge: the maximum life cycle of BPDU. ● FwDly: deferred time of the change of the port status. ● MaxHop: the maximum hops in the MST region.
TC or TCN send	Number of BPDUs with TC flags or TCN BPDUs sent by the port.
TC or TCN received	Number of BPDUs with TC flags or TCN BPDUs received by the port.
BPDU Sent	Statistics about the packets sent by BPDU is as follows: ● TCN: topology change notification ● Config: STP packets ● RST: RSTP packets ● MST: MSTP packets
BPDU Received	Statistics about the packets received by BPDU.

Related Topics

6.8.18 reset stp statistics
6.8.31 stp enable

6.8.5 display stp abnormal-interface

Function

The **display stp abnormal-interface** command displays information about abnormal interfaces running the Spanning Tree Protocol (STP).

Format

display stp [**instance** *instance-id*] **abnormal-interface**

Parameters

Parameter	Description	Value
instance *instance-id*	Displays the status and statistics of a specified spanning tree instance. If **instance** *instance-id* is not specified, the status and statistics of all spanning tree instances will be displayed in the sequence of the interface numbers.	The value is an integer in the range 0 to 4094. The value **0** indicates a common and internal spanning tree (CIST) instance. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: • AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. • AR2220, AR2240, and AR3200 series: 49.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a device has many interfaces and the **display stp** command output displays vast information, viewing information about abnormal interfaces running STP is difficult.

You can use the **display stp abnormal-interface** command to view information about abnormal interfaces running STP.

Example

Display information about abnormal interfaces in process 0 running STP

```
<Huawei> display stp instance 0 abnormal-interface
MSTID    Interface              Status        Reason
   0    Ethernet0/0/0       DISCARDING     LOOP-Protected
   0    Ethernet0/0/1       DOWN          BPDU-Protected
   0    Ethernet0/0/2       DISCARDING     ROOT-Protected
   0    Ethernet0/0/3       DISCARDING     LOOP-Detected
```

Table 6-49 Description of the **display stp abnormal-interface** command output

Item	Description
MSTID	MSTP instance ID

Item	Description
Interface	Interface type
Status	Status of an interface after the STP protection takes effect • **DOWN**: indicates that the physical status of the interface is Down (including error-down). • **DISCARDING**: indicates the blocked interface after the topology of the spanning tree becomes stable.
Reason	An interface running STP becomes abnormal due to one of the following: • **Root-Protected**: indicates that the root protection takes effect. • **Loop-Protected**: indicates that the loop protection takes effect. • **BPDU-Protected**: indicates that the BPDU protection takes effect. • **Loop-Detected**: indicates that the loop detection takes effect.

Related Topics

6.8.4 display stp

6.8.6 display stp active

Function

The **display stp active** command displays the status of and statistics on spanning trees of all Up interfaces.

Format

display stp active

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **display stp active** command displays information about spanning trees of Up interfaces only.

Example

Display information about spanning trees of all Up interfaces.

```
<Huawei> display stp active
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :61440.781d-ba56-f06c
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :61440.781d-ba56-f06c / 0
CIST RegRoot/IRPC   :61440.781d-ba56-f06c / 0
CIST RootPortId     :0.0
BPDU-Protection     :Disabled
TC or TCN received  :85
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 9h:10m:8s
Number of TC        :13
Last TC occurred    :GigabitEthernet1/0/4
----[Port18(GigabitEthernet1/0/10)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :61440.781d-ba56-f06c / 128.18
 Port Edged          :Config=default / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :10 packets/s
 Protection Type     :None
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :5
 TC or TCN received  :0
 BPDU Sent           :178445
         TCN: 0, Config: 0, RST: 0, MST: 178445
 BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
 Last forwarding time: 2012/04/19 16:58:37 UTC+08:00
----[Port19(GigabitEthernet2/1/17)][FORWARDING]----
 Port Protocol       :Enabled
 Port Role           :Designated Port
 Port Priority       :128
 Port Cost(Dot1T )   :Config=auto / Active=20000
 Designated Bridge/Port   :61440.781d-ba56-f06c / 128.19
 Port Edged          :Config=default / Active=enabled
 Point-to-point      :Config=auto / Active=true
 Transit Limit       :10 packets/s
 Protection Type     :None
 Port STP Mode       :MSTP
 Port Protocol Type  :Config=auto / Active=dot1s
 PortTimes           :Hello 2s MaxAge 20s FwDly 15s RemHop 20
 TC or TCN send      :0
 TC or TCN received  :0
 BPDU Sent           :5
         TCN: 0, Config: 0, RST: 0, MST: 5
 BPDU Received       :0
         TCN: 0, Config: 0, RST: 0, MST: 0
 Last forwarding time: 2012/04/23 20:06:08 UTC+08:00

-------[MSTI 1 Global Info]-------
```

```
MSTI Bridge ID      :61440.781d-ba56-f06c
MSTI RegRoot/IRPC   :61440.781d-ba56-f06c / 0
MSTI RootPortId     :0.0
Master Bridge       :61440.781d-ba56-f06c
Cost to Master      :0
TC received         :2
TC count per hello  :0
Time since last TC  :0 days 9h:10m:8s
Number of TC        :9
Last TC occurred    :GigabitEthernet1/0/4
```

Table 6-50 Description of the **display stp active** command output

Item	Description
CIST Bridge	● The 16 leftmost bits are the switch's priority in the CIST. ● The 48 rightmost bits are the switch's MAC address.
Config Times	Configured bridge protocol parameters: ● **Hello**: interval at which Bridge Protocol Data Units (BPDUs) are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region
Active Times	Bridge protocol parameters that are being used: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **MaxHop**: maximum number of hops in the MST region
CIST Root/ERPC	CIST root bridge ID/external path cost from the switch to the root bridge.
CIST RegRoot/IRPC	ID of the CIST region root bridge/Cost of the internal path (path from the switch to the CIST region root switch)
CIST RootPortId	CIST root port ID. "0.0" indicates that the switch is the root switch without the root port.
BPDU-Protection	Whether BPDU protection is enabled: ● **Disabled**: BPDU protection is disabled. ● **Enabled**: BPDU protection is enabled.
TC or TCN received	Number of received topology change (TC) or topology change notification (TCN) packets
TC count per hello	Number of TC packets received per Hello time

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
STP Converge Mode	Convergence mode of the Spanning Tree Protocol (SPT), which can be **fast** or **normal**. For details, see **stp converge**.
Time since last TC	Time since the last topology change
Number of TC	Number of topology changes
Last TC occurred	Interface which causes the last topology change **NOTE** This parameter does not appear when **Number of TC** is **0**.
Port Protocol	STP status on the interface: • **Enabled**: STP is enabled on the interface. • **Disabled**: STP is disabled on the interface.
Port Role	Role of an interface. In the CIST region, the roles of interfaces are as follows: • Root Port • Designated Port • Alternate Port • Backup Port
Port Priority	Interface priority. For details, see **stp port priority**.
Port Cost(Dot1T)	Path cost (calculated by dot1t) of an interface: • **Config**: configured path cost • **Active**: path cost that is being used
Designated Bridge/ Port	Switch ID/Port ID The first 16 bits represent the switch's priority in the CIST region, and the last 48 bits represent the switch's MAC address. The first 4 bits of the port ID represent the port's priority, and the last 12 bits represent the port number.
Port Edged	Whether the edge interface (specified by the administrator) is enabled: • **enabled**: The edge interface is enabled. • **disabled**: The edge interface is disabled. **Config** indicates the value that is specified in the **stp edged-port** command, and **Active** indicates the value in use.
Point-to-point	Link type of the interface. **Config** indicates the link type that is specified in the **stp point-to-point** command, and **Active** indicates the link type that is being used.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Transit Limit	Maximum number of BPDUs that the current interface can send per second. For details, see **stp transmit-limit**.
Protection Type	Protection type, which can be: ● **root-protection**: Protection takes effect only on the specified interface. ● **loop-protection**: Protection takes effect only on the root interface or alternate interface.
Port STP Mode	STP mode of the interface
Port Protocol Type	Format of packets sent and received on the interface, which can be: ● auto ● legacy ● dot1s The default value is **auto**. **Config** indicates the packet format that is specified in the **stp compliance** command, and **Active** indicates the packet format in use.
PortTimes	Bridge protocol parameters of the interface: ● **Hello**: interval at which BPDUs are sent ● **MaxAge**: maximum TTL of a BPDU ● **FwDly**: delay in interface status transition ● **RemHop**: maximum number of hops in the MST region
TC or TCN send	Number of TC or TCN packets sent on the interface
TC or TCN received	Number of TC or TCN packets received on the interface
BPDU Sent	Statistics on sent BPDUs, including: ● **TCN**: TCN BPDUs ● **Config**: STP BPDUs ● **RST**: Rapid Spanning Tree Protocol (RSTP) BPDUs ● **MST**: MSTP BPDUs
BPDU Received	Statistics on received BPDUs
Last forwarding time	Time when the interface last entered the forwarding state
MSTI Bridge ID	Multiple Spanning Tree instance (MSTI) bridge ID
MSTI RegRoot/IRPC	MSTI root bridge ID/Cost of the internal path (path from the switch to the MSTI root switch)

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MSTI RootPortId	ID of the MSTI root interface. **0.0** indicates that the switch is the root switch and does not provide any root interface.
Master Bridge	ID of the bridge where the master interface is located. ● The first 16 bits represent the switch's priority in the CIST. ● The last 48 bits represent the switch's MAC address.
Cost to Master	Cost of the path from the switch to the bridge where the master interface is located. **0** indicates that the master interface is located at the current bridge.
TC received	Number of received TC packets

Related Topics

6.8.4 display stp
6.8.7 display stp bridge
6.8.9 display stp global

6.8.7 display stp bridge

Function

The **display stp bridge** command displays details about the spanning tree of a bridge.

Format

display stp bridge { **root** | **local** }

Parameters

Parameter	Description	Value
root	Displays details about the spanning tree of the root bridge.	-
local	Displays details about the spanning tree of the local bridge.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a device provides many interfaces, running the **display stp** command displays a large amount of information, and it is difficult to find information about the spanning trees of the root and local bridges.

Using the **display stp bridge** command, you can easily view details about the spanning trees of the root and local bridges.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.

Example

Display details about the spanning tree of the root bridge of MSTP process 0.

```
<Huawei> display stp bridge root
MSTID            Root ID  Root Cost Hello Max Forward Root Port
                                   Time Age   Delay
----- -------------------- ---------- ----- --- ------- ------------------
    0 61440.781d-ba56-f06c         0     2  20      15
    1 61440.781d-ba56-f06c         0     2  20      15
```

Table 6-51 Description of the **display stp bridge** command output

Item	Description
MSTID	MSTP instance ID
Root ID	MSTP root bridge ID
Root Cost	MSTP root path cost
Hello Time	Interval at which Bridge Protocol Data Units (BPDUs) are sent from the root switch
Max Age	Maximum TTL of a BPDU
Forward Delay	Delay in interface status transition
Root Port	Root interface

Related Topics

6.8.4 display stp

6.8.6 display stp active

6.8.9 display stp global

 Copyright © Huawei Technologies Co., Ltd.

6.8.8 display stp error packet

Function

The **display stp error packet** command displays the statistics about error packets received by MSTP and the contents of recently received packets.

Format

display stp error packet

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device on a Layer 2 network runs MSTP is attacked by MSTP error packets, the **display stp error packet** command can be used to view recently received MSTP error packets.

Example

Display the statistics about error packets received by MSTP and the contents of recently received packets.

```
<Huawei> display stp error packet
 4 error-packet(s) have been received and the last one is received at 2011/05/02 12:45:31.
01 80 C2 00 00 00 38 AA D2 11 11 10 00 69 42 42
03 00 00 03 02 7C 00 00 38 AA D2 11 11 10 00 00
00 00 00 00 38 AA D2 11 11 10 80 01 00 00 14 00
02 00 0F 00 00 00 40 00 33 38 61 61 64 32 31 31
31 31 31 30 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 AC 36 17 7F 50 28
3C D4 B8 38 21 D8 AB 26 DE 62 00 00 00 00 00 00
38 AA D2 11 11 10 14
```

 Copyright © Huawei Technologies Co., Ltd.

Table 6-52 Description of the display stp error packet command output

Item	Description
<n> error-packet(s) have been received and the last one is received at <time>	n error packets are received and the time when the last error packet is received is recorded. <n>: number of error packets <time>: time when the last error packet is received

Related Topics

6.8.18 reset stp statistics

6.8.31 stp enable

6.8.9 display stp global

Function

The **display stp global** command displays global Spanning Tree Protocol (STP) information.

Format

display stp global

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a device provides many interfaces, the **display stp** command output contains a large amount of information, and it is difficult to find the desired information quickly and view global information at a glance. The **display stp brief** command output, by comparison, displays information about spanning trees on interfaces, but not global information.

Using the **display stp global** command, you can view global STP information conveniently.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- If you run this command in the system view without specifying an MSTP process ID, information about MSTP process 0 is displayed by default.
- If you run this command in the MSTP process view without specifying an MSTP process ID, information about the MSTP process in this view is displayed by default.

Example

Display brief STP information about MSTP process 0.

```
<Huawei> display stp global
Protocol Status            : Enabled
Bpdu-filter default        : Disabled
Tc-protection              : Enabled
Tc-protection threshold    : 1
Tc-protection interval     : 2s
Edged port default         : Enabled
Pathcost-standard          : Dot1t
Timer-factor               : 3
Transmit-limit             : 10
Bridge-diameter            : 7
-------[CIST Global Info][Mode MSTP]-------
CIST Bridge         :61440.781d-ba56-f06c
Config Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
Active Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20
CIST Root/ERPC      :61440.781d-ba56-f06c / 0
CIST RegRoot/IRPC   :61440.781d-ba56-f06c / 0 (This bridge is the root)
CIST RootPortId     :128.3 (Ethernet5/0/0)
BPDU-Protection     :Disabled
TC or TCN received  :85
TC count per hello  :0
STP Converge Mode   :Normal
Time since last TC  :0 days 9h:12m:34s
Number of TC        :13
Last TC occurred    :Ethernet5/0/0
```

Table 6-53 Description of the **display stp global** command output

Item	Description
Protocol Status	Spanning Tree Protocol (STP) status: ● **Enabled**: STP is enabled. ● **Disabled**: STP is disabled.
Bpdu-filter default	Whether the function of configuring device interfaces as Bridge Protocol Data Unit (BPDU) filter interfaces is enabled: ● **Enabled**: The function is enabled. ● **Disabled**: The function is disabled.
Tc-protection	Topology change (TC) protection status.
Tc-protection threshold	Threshold of TC packets that the device can handle and immediately refresh forwarding entries in a given period

<table>
<tr><th>Item</th><th>Description</th></tr>
<tr><td>Tc-protection interval</td><td>Time the MSTP takes to handle a given number of TC packets and immediately refresh forwarding entries</td></tr>
<tr><td>Edged port default</td><td>Whether the function of configuring all ports of the switch as edge ports is enabled:
● Enabled: The function is enabled.
● Disabled: The function is disabled.</td></tr>
<tr><td>Pathcost-standard</td><td>Method of calculating the MSTP path cost</td></tr>
<tr><td>Timer-factor</td><td>Multiplier of Hello time</td></tr>
<tr><td>Transmit-limit</td><td>Maximum number of BPDUs that the current interface can send per Hello time. For details, see stp transmit-limit.</td></tr>
<tr><td>Bridge-diameter</td><td>Network diameter of the MSTP
For details, see stp bridge-diameter.
The value of this field depends on the mappings between the IEEE-recommended network diameter and STP time parameters (Hello Time, Forward Delay, and Max Age). If the mapping fails, default value 7 takes effect. Figure 6-2 shows the mappings between the IEEE-recommended network diameter and STP time parameters.

Figure 6-2 Mappings between the IEEE-recommended network diameter and STP time parameters
<table>
<tr><th>Max Age</th><th>Hello Time</th><th>Forward Delay</th><th>Briage-diameter</th></tr>
<tr><td>10</td><td>2</td><td>7</td><td>2</td></tr>
<tr><td>12</td><td>2</td><td>9</td><td>3</td></tr>
<tr><td>14</td><td>2</td><td>10</td><td>4</td></tr>
<tr><td>16</td><td>2</td><td>12</td><td>5</td></tr>
<tr><td>18</td><td>2</td><td>13</td><td>6</td></tr>
<tr><td>20</td><td>2</td><td>15</td><td>7</td></tr>
</table></td></tr>
</table>

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CIST Bridge	Common and internal spanning tree (CIST) bridge ID • The first 16 bits represent the switch's priority in the CIST. • The last 48 bits represent the switch's MAC address.
Config Times	Configured bridge protocol parameters: • **Hello**: interval at which BPDUs are sent • **MaxAge**: maximum TTL of a BPDU • **FwDly**: delay in interface status transition • **MaxHop**: maximum number of hops in the MST region
Active Times	Bridge protocol parameters that are being used: • **Hello**: interval at which BPDUs are sent • **MaxAge**: maximum TTL of a BPDU • **FwDly**: delay in interface status transition • **MaxHop**: maximum number of hops in the MST region
CIST Root/ERPC	CIST root switch ID/Cost of the external path (path from the switch to the CIST root switch)
CIST RegRoot/IRPC	ID of the CIST region root bridge/Cost of the internal path (path from the switch to the CIST region root switch)
CIST RootPortId	ID of the CIST root interface. **0.0** indicates that the switch is the root switch and does not provide any root interface.
BPDU-Protection	Whether BPDU protection is enabled: • **Disabled**: BPDU protection is disabled. • **Enabled**: BPDU protection is enabled.
TC or TCN received	Number of received TC or topology change notification (TCN) packets
TC count per hello	Number of TC packets received per Hello time
STP Converge Mode	Convergence mode of the Spanning Tree Protocol (SPT), which can be **fast** or **normal**. For details, see **stp converge**.
Time since last TC	Time since the last topology change
Number of TC	Number of topology changes
Last TC occurred	Interface which causes the last topology change **NOTE** This parameter does not appear when **Number of TC** is **0**.

Related Topics

6.8.4 display stp
6.8.6 display stp active
6.8.7 display stp bridge

6.8.10 display stp region-configuration

Function

The **display stp region-configuration** command displays the effective configuration of the MST region on the switching device. The configuration includes the region name, revision level and mapping relationship between VLANs and spanning tree instances.

Format

display stp region-configuration [**digest**]

Parameters

Parameter	Description	Value
digest	Displays brief information about the effective MST region.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an MST region is configured and takes effect on the network running MSTP, you can run the **display stp region-configuration** command to view the name, revision level, STP instance, and inter-VLAN mapping of the MST region.

Example

Display the configuration of MST regions.

```
<Huawei> display stp region-configuration
Oper configuration
  Format selector :0
  Region name     :huawei
  Revision level  :0
  Instance   VLANs Mapped
    0       21 to 4094
```

```
  1      1 to 10
  2      11 to 20
```

Display brief information about the effective MST region.

```
<Huawei> display stp region-configuration digest
 Oper configuration
   Format selector    :0
   Region name        :huawei
   Revision level     :0
   Digest             :0xAC36177F50283CD4B83821D8AB26DE62
```

Table 6-54 Description of the display stp region-configuration command output

Item	Description
Format selector	Selection factors defined by the MSTP protocol.
Region name	Name of the MST region. For the related commands, see **region-name**.
Revision level	Revision level of the MST region. For the related commands, see **revision-level**.
Instance VLANs Mapped	Mapping between the spanning tree instance and VLANs of the MST region. For the related commands, see **instance** or **vlan-mapping modulo**. If the mapping is incorrect, run the **instance** command to re-map the specified VLAN to the specified MSTI and run the **active region-configuration** command to activate the mapping.
Digest	Brief information about the MST region.

Related Topics

6.8.14 instance

6.8.16 region-name

6.8.19 revision-level

6.8.11 display stp tc-bpdu statistics

Function

The **display stp tc-bpdu statistics** command displays statistics of sent and received topology change (TC) and topology change notification (TCN) BPDUs on interfaces.

Format

display stp [**instance** *instance-id*] [**interface** *interface-type interface-number*] **tc-bpdu statistics**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of an MSTP instance of which statistics of TC and TCN BPDUs are displayed. If the parameter **instance** *instance-id* is not specified, statistics of TC and TCN BPDUs on all interfaces are displayed in the sequence of the interface numbers.	The value is an integer that ranges from 0 to 4094. The value 0 indicates a CIST instance. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: ● AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. ● AR2220, AR2240, and AR3200 series: 49.
interface *interface-type interface-number*	Specifies the interface on which statistics of TC and TCN BPDUs are displayed. If the parameter **interface** *interface-type interface-number* is not specified, statistics of TC and TCN BPDUs on all interfaces are displayed in the sequence of the interface numbers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you need to know whether a fault has occurred on interfaces that send and receive TC/TCN BPDUs, you can run this command to view statistics of these BPDUs and locate the fault.

Example

Display the statistics of TC/TCN BPDUs on interfaces of an MSTP instance.

```
<Huawei> display stp tc-bpdu statistics
 ------------------------- STP TC/TCN information -------------------------
 MSTID Port                    TC(Send/Receive)      TCN(Send/Receive)
 0     GigabitEthernet1/0/9          3/2                  0/0
 0     GigabitEthernet1/0/10         1/0                  0/0
 1     GigabitEthernet1/0/9         14/9                  -/-
 1     GigabitEthernet1/0/10         8/10                 -/-
```

```
2    GigabitEthernet1/0/9          3/2              -/-
2    GigabitEthernet1/0/10          1/0              -/-
```

Table 6-55 Description of the **display stp tc-bpdu statistics** command output

Item	Description
MSTID	ID of an MSTP instance
Port	Interface name
TC(Send/Receive)	Statistics of send and received TC BPDUs
TCN(Send/Receive)	Statistics of send and received TCN BPDUs ("-" indicates that MSTP instances except MSTP instance 0 do not have TCN BPDUs sent and received)

Related Topics

6.8.18 reset stp statistics

6.8.12 display stp topology-change

Function

The **display stp topology-change** command displays the statistics about topology changes.

Format

display stp [**instance** *instance-id*] **topology-change**

Parameters

Parameter	Description	Value
instance *instance-id*	Displays statistics about the topology changes of a specified STP instance. If this parameter is not specified, the statistics about the topology changes of a CIST instance are displayed.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: • AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. • AR2220, AR2240, and AR3200 series: 49.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

On a Layer 2 network running MSTP, a device clears ARP entries and MAC entries after receiving topology change packets. If a device receives too many topology change packets, the device will frequently clear ARP entries and MAC entries, causing high CPU usage. As a result, network traffic is instable.

The **display stp topology-change** command can be used to display the statistics about MSTP topology changes. If the statistics increase, network flapping occurs.

Example

Display statistics about MSTP topology changes.

```
<Huawei> display stp topology-change
 CIST topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(detected)    :Ethernet2/0/0
   Topology change last received from     :00e0-5b3c-c100
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 1 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(detected)    :GigabitEthernet1/0/2
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 2 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
   Topology change initiator(notified)    :GigabitEthernet1/0/3
   Number of generated topologychange traps :   5
   Number of suppressed topologychange traps:   3

 MSTI 3 topology change information
   Number of topology changes             :5
   Time since last topology change        :0 days 0h:23m:19s
```

Table 6-56 Description of the display stp topology-change command output

Item	Description
Number of topology changes	Total number of topology changes since initialization. **NOTE** The number of received and sent TC BPDUs in each VLAN may be different during topology convergence, so the number of topology changes in each VLAN may be different.
Time since last topology change	Time since the last topology change

Item	Description
Topology change initiator(detected)	Interface that initiates a topology change because the interface status changes to detected
Topology change initiator(notified)	Interface that initiates a topology change after receiving a topology change packet
Topology change last received from	Source bridge MAC address contained in a topology change packet
Number of generated topologychange traps	Total number of generated topology-change traps.
Number of suppressed topologychange traps	Total number of suppressed topology-change traps.

Related Topics

6.8.18 reset stp statistics
6.8.31 stp enable

6.8.13 display stp vlan

Function

The **display stp vlan** command displays the STP status on an interface added to a specified VLAN.

Format

display stp vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Displays the STP status on an interface added to a specified VLAN.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After an interface is added to a VLAN, the **display stp vlan** command can be used to the display the STP status on the interface. In this case, the mapping between VLANs and instances does not need to be concerned with.

Example

Display the STP status on an interface added to a specified VLAN.

```
<Huawei> display stp vlan 1
 InstanceId   Port                    Role  State
 ------------------------------------------------------------
    0       Ethernet1/0/0            ROOT  FORWARDING
    0       Ethernet2/0/0            DESI  FORWARDING
```

Table 6-57 Description of the **display stp vlan** command output

Item	Description
InstanceId.	Instance ID
Port	Interface
Role	Interface role
State	Interface status

Related Topics

6.8.18 reset stp statistics

6.8.31 stp enable

6.8.14 instance

Function

The **instance** command maps a VLAN to a spanning tree instance.

The **undo instance** command deletes the mapping between a VLAN and a spanning tree instance.

By default, all VLANs are mapped to CIST, that is, instance 0.

NOTE

The AR100 series, AR120 series (except AR129CGVW-L), among the AR160 series, the AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc. AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169CVW-4B4S, AR169EGW-L, AR169G-L, AR169W-P-M9, AR169RW-P-M9, AR169-P-M9 do not support this command.

Format

instance *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo instance *instance-id* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

Parameters

Parameter	Description	Value
instance-id	Specifies the number of a spanning tree instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: ● AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. ● AR2220, AR2240, and AR3200 series: 49. The value of *instance-id* specified in the **undo instance** command cannot be 0. This means that instance 0 cannot be deleted.
vlan *vlan-id1*	Specifies a start VLAN ID.	The value is an integer ranging from 1 to 4094. The start VLAN ID must be smaller than the end VLAN ID.
to *vlan-id2*	Specifies an end VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **instance** command is used to set mappings between spanning tree instances and VLANs.

Precautions

When using the **undo instance** command, note the following points:

- After the mapping between specified VLANs and a specified spanning tree instance is deleted, these VLANs will be mapped to a CIST, namely, instance 0.

- If no VLAN is specified, all VLANs that have established mappings with the spanning tree instance will be mapped to a CIST.

If the **instance** command is run more than once, all configurations take effect.

A VLAN cannot be mapped to different spanning tree instances. If the **instance** command is run several times, the latest configuration overrides the previous one.

Example

Map VLAN 2 to spanning tree instance 1.

```
<Huawei> system-view
[Huawei] stp region-configuration
[Huawei-mst-region] instance 1 vlan 2
```

Related Topics

6.8.10 display stp region-configuration

6.8.15 max bandwidth-affected-linknumber

Function

The **max bandwidth-affected-linknumber** command sets the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.

The **undo max bandwidth-affected-linknumber** command restores the default upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.

By default, the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk is 8.

Format

max bandwidth-affected-linknumber *link-number*

undo max bandwidth-affected-linknumber

Parameters

Parameter	Description	Value
link-number	Specifies the upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk.	The value is an integer ranging from 1 to 8.

Views

Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The upper threshold for the number of interfaces that determine the bandwidth of an Eth-Trunk is used for STP calculation.

For example, device A and device B are connected by two Eth-Trunks. Eth-Trunk1 has three member links that are Up; the Eth-Trunk2 has two member links that are Up. The bandwidth of each member link is 1 Gbit/s, so the bandwidth of Eth-Trunk1 is 3 Gbit/s and the bandwidth of Eth-Trunk2 is 2 Gbit/s. If device A is the root bridge during STP calculation, Eth-Trunk1 on device B is the root port and Eth-Trunk2 is the alternate port. You can run this command to set the upper threshold to 1. Then the bandwidth of Eth-Trunk1 becomes 1 Gbit/s during STP calculation. Bandwidth decrease affects the interface cost, causing STP recalculation. The **max bandwidth-affected-linknumber** command does not affect traffic forwarding on the Eth-Trunk. The bandwidth used to forward traffic is still 3 Gbit/s.

Example

Set the upper threshold to 3.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] max bandwidth-affected-linknumber 3
```

Related Topics

6.2.1 display eth-trunk

6.2.22 least active-linknumber

6.8.16 region-name

Function

The **region-name** command configures the MST region name of the switching device.

The **undo region-name** command restores the default name.

By default, the MST region name is the MAC address of the management network interface on the MPU of the switching device.

Format

region-name *name*

undo region-name

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name	Specifies the region name of the switching device.	The value is a case-sensitive text of 1 to 32 characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

The **region-name** command is used to configure MST region names in order to identify different regions.

Example

Set the MST region name of the switch to "huawei".

```
<Huawei> system-view
[Huawei] stp region-configuration
[Huawei-mst-region] region-name huawei
```

Related Topics

6.8.10 display stp region-configuration

6.8.17 reset stp error packet statistics

Function

The **reset stp error packet statistics** command clears the statistics of error STP packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset stp error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Applicable Scenario

You can use the **reset stp error packet statistics** command to clear the history statistics when you need to observe the statistics of error STP packets in a period from the current time.

Precautions

The **reset stp error packet statistics** command clears the statistics about error STP packets are cleared and cannot be restored. Therefore, confirm the action before you use the command.

Example

Clear the statistics about error STP packets.

```
<Huawei> reset stp error packet statistics
```

6.8.18 reset stp statistics

Function

The **reset stp statistics** command clears the statistics of a spanning tree.

Format

reset stp [**interface** *interface-type interface-number*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface type and the number of the interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Sometimes, traffic statistics within a certain period is needed. In this situation, clear the existing statistics before restarting the count.

When you run the **reset stp statistics** command:

- If you specify an interface, you can clear the statistics of a spanning tree on the interface.
- If you do not specify an interface, you can clear the statistics of spanning trees on all interfaces.

Example

Clear the statistics of spanning trees on Eth2/0/0.

```
<Huawei> reset stp interface ethernet 2/0/0 statistics
```

Related Topics

6.8.4 display stp

6.8.19 revision-level

Function

The **revision-level** command configures the revision level of MST region of a switching device.

The **undo revision-level** command restores the default level.

By default, the revision level of MST region is 0.

Format

revision-level *level*

undo revision-level

Parameters

Parameter	Description	Value
level	Specifies the revision level of the MST region.	The value is an integer ranging from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each region is called an MST region and each spanning tree is called a multiple spanning tree instance (MSTI).

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs
- MST region revision level

If two switching devices have the same region name and VLAN mapping table, the **revision-level** command can be used to set different revision levels for the two devices so that the two devices belong to different MST regions.

Example

Set the MSTP revision level of the switching device to 5.

```
<Huawei> system-view
[Huawei] stp region-configuration
[Huawei-mst-region] revision-level 5
```

Related Topics

6.8.10 display stp region-configuration

6.8.20 snmp-agent trap enable feature-name mstp

Function

The **snmp-agent trap enable feature-name mstp** command enables the trap function for the MSTP module.

The **undo snmp-agent trap enable feature-name mstp** command disables the trap function for the MSTP module.

By default, the trap function is disabled for the MSTP module.

Format

snmp-agent trap enable feature-name mstp [**trap-name** { **hwmstpibridgelostrootprimary** | **hwmstpiedgeportchanged** | **hwmstpiportbpduguarded** | **hwmstpiportloopguarded** |

hwmstpiportrootguarded | **hwmstpiportstatediscarding** | **hwmstpiportstateforwarding** | **hwmstpproloopbackdetected** }]

undo snmp-agent trap enable feature-name mstp [**trap-name** { **hwmstpibridgelostrootprimary** | **hwmstpiedgeportchanged** | **hwmstpiportbpduguarded** | **hwmstpiportloopguarded** | **hwmstpiportrootguarded** | **hwmstpiportstatediscarding** | **hwmstpiportstateforwarding** | **hwmstpproloopbackdetected** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of MSTP events of specified types.	-
hwmstpibridgelostrootprimary	Enables the device to send trap when the current device is no longer the root bridge.	-
hwmstpiedgeportchanged	Enables the device to send trap when the edge port that is not enabled with the BPDU guard function is no longer the edge port after receiving BPDUs.	-
hwmstpiportbpduguarded	Enables the device to send trap when the edge port enabled with the BPDU guard function can receive BPDUs.	-
hwmstpiportloopguarded	Enables the device to send trap when the port enabled with the loop guard function does not receive any BPDU in a specified period.	-
hwmstpiportrootguarded	Enables the device to send trap when the port enabled with the root guard function receives BPDUs with higher priorities.	-
hwmstpiportstatediscarding	Enables the device to send trap when the port status changes to Discarding.	-
hwmstpiportstateforwarding	Enables the device to send trap when the port status changes to Forwarding.	-
hwmstpproloopbackdetected	Enables the device to send trap when port detected loopback, block the port.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The MSTP module is not configured with the function of excessive traps. To enable the traps of one or more events, you can specify **trap-name**.

Example

Enables the device to send trap when the current device is no longer the root bridge.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mstp trap-name hwmstpibridgelostrootprimary
```

Related Topics

6.8.3 display snmp-agent trap feature-name mstp all

6.8.21 stp bpdu-filter

Function

The **stp bpdu-filter enable** command specifies a port as a BPDU-filter port.

The **stp bpdu-filter disable** command specifies a port as a non-BPDU-filter port.

The **undo stp bpdu-filter** command restores the default attribute of a BPDU-filter port.

By default, a port is a non-BPDU-filter port.

Format

stp bpdu-filter { **enable** | **disable** }

undo stp bpdu-filter

Parameters

None

Views

Eth-Trunk interface view, Ethernet interface view, GE interface view, Port-group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, if the **stp edged-port enable** command is used to configure a port as an edge port, the port will not participate in the spanning tree calculation. This speeds up network convergence and

improves network stability. This port, however, will still send BPDUs. This may cause BPDUs to be sent to other networks. As a result, these networks flap.

The **stp bpdu-filter enable** command can be used on the port to address this problem. After the **stp bpdu-filter enable** command is used on the port, the port will become a BPDU-filter port, and will not process BPDUs.

NOTICE

If the **stp bpdu-filter enable** command is run on a port, the port will not transmit or process BPDUs. The port cannot negotiate the STP status with the directly connected port on the remote device. Therefore, exercise cautions when using the **stp bpdu-filter enable** command. Running the **stp bpdu-filter enable** command only on edge ports is recommended.

Running the **stp bpdu-filter enable** command in the interface view configures only the current port as a BPDU-filter port. If multiple BPDU-filter ports are required on a device, the **stp bpdu-filter default** command can be used in the system view to configure all the ports as BPDU-filter ports. If some ports need to participate in spanning tree calculation but do not need to be configured as BPDU-filter ports, the **stp bpdu-filter disable** command can be used in the view of these ports to configure them as non-BPDU-filter ports. Similarly, if the **stp bpdu-filter disable** command has been run on a port, the non-BPDU filter port attributes of the port will not change after the **stp bpdu-filter default** command is run.

Precautions

After the **stp bpdu-filter disable** command is run on a port, the port becomes a non-BPDU-filter port. The port is still a non-BPDU-filter port even if the **stp bpdu-filter default** command is run in the system view. After the **undo stp bpdu-filter** command is run on the port, the BPDU-filter attributes of the port restore to the default ones.

Example

On a network edge device, specify Eth2/0/0 as a non-BPDU-filter port.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] portswitch
[Huawei-Ethernet2/0/0] stp bpdu-filter disable
```

On a network edge device, specify Eth2/0/0 as a BPDU-filter port.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] portswitch
[Huawei-Ethernet2/0/0] stp bpdu-filter enable
```

Related Topics

6.8.22 stp bpdu-filter default

6.8.29 stp edged-port

6.8.22 stp bpdu-filter default

Function

The **stp bpdu-filter default** command specifies all ports of a device as BPDU-filter ports.

The **undo stp bpdu-filter default** command specifies all ports of a device as non-BPDU-filter ports.

By default, a port is a non-BPDU-filter port.

Format

stp bpdu-filter default

undo stp bpdu-filter default

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, if the **stp edged-port enable** command is used to configure a port as an edge port, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability. This port, however, will still send BPDUs. This may cause BPDUs to be sent to other networks. As a result, these networks flap.

The **stp bpdu-filter enable** command can be used on the port to address this problem. After the **stp bpdu-filter enable** command is used on the port, the port will become a BPDU-filter port, and will not process BPDUs.

Running the **stp bpdu-filter enable** command in the interface view configures only the current port as a BPDU-filter port. If multiple BPDU-filter ports are required on a device, the **stp bpdu-filter default** command can be used in the system view to configure all ports as BPDU-filter ports. Then run the **stp bpdu-filter disable** command in the interface view to change the interfaces that need not to be configured as BPDU filter interfaces into non-BPDU filter interfaces.

Precautions

After the **stp bpdu-filter default** command is run, a port that has been configured with the **undo stp bpdu-filter** command will become a BPDU-filter

 Copyright © Huawei Technologies Co., Ltd.

port. After the **stp bpdu-filter disable** command is run, the port that has been configured with the **undo stp bpdu-filter** command, however, will still serve as a non-BPDU-filter port.

NOTICE

After the **stp bpdu-filter default** and **stp edged-port default** commands are run in the system view, none of the ports on the device will initiate any BPDUs or initiate a negotiation with the remote device, and all the ports are in the forwarding state. This may lead to a loop and cause a broadcast storm. Exercise cautions when using the **stp bpdu-filter default** and **stp edged-port default** commands in the system view.

Example

On a network edge device, specify all ports as BPDU-filter ports.

```
<Huawei> system-view
[Huawei] stp bpdu-filter default
```

Related Topics

6.8.21 stp bpdu-filter

6.8.29 stp edged-port

6.8.23 stp bpdu-protection

Function

The **stp bpdu-protection** command enables BPDU protection on a switching device.

The **undo stp bpdu-protection** command disables BPDU protection on a switching device.

By default, the BPDU protection is disabled.

Format

stp bpdu-protection

undo stp bpdu-protection

Parameters

None.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

An edge port will lose edge port attributes after receiving BPDUs. To prevent attackers from forging BPDUs to change edge ports to non-edge ports, you can run the **stp bpdu-protection** command to configure BPDU protection on a switching device.

Precautions

After BPDU protection is enabled, a switching device sets an edge port to error down state if the edge port receives a BPDU and retains the port as an edge port. To configure the edge port in error-down state to automatically restore to the Up state, run the **error-down auto-recovery cause bpdu-protection interval** *interval-value* command in the system view.

Example

Enable the BPDU protection on the switching device.

```
<Huawei> system-view
[Huawei] stp bpdu-protection
```

Related Topics

6.8.4 display stp

6.8.29 stp edged-port

6.8.24 stp bridge-diameter

Function

The **stp bridge-diameter** command configures the diameter of the spanning tree.

The **undo stp bridge-diameter** command restores the default diameter.

By default, the diameter of the spanning tree is 7.

Format

stp bridge-diameter *diameter*

undo stp bridge-diameter

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
diameter	Specifies the diameter.	The value is an integer ranging from 2 to 7.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, the network diameter is the maximum number of devices between two switching devices. If the network diameter is improperly set, network converge may slow down, affecting users' normal communication.

The **stp bridge-diameter** command can be used to set a proper network diameter based on the network scale. This helps to accelerate network convergence.

The following time parameters are related to the network scale:

- Hello Time
- Forward Delay
- Max Age

Precautions

After the **stp bridge-diameter** command is used on a switching device, the switching device will automatically set proper values for Hello Time, Forward Delay, and Max Age based on the configured network diameter.

On an MSTP network, the network diameter configured using the **stp bridge-diameter** command is valid only for CISTs.

Example

Set the network diameter to 5.

```
<Huawei> system-view
[Huawei] stp bridge-diameter 5
```

Related Topics

6.8.47 stp timer forward-delay
6.8.48 stp timer hello
6.8.49 stp timer max-age

6.8.25 stp compliance

Function

The **stp compliance** command configures the format for the MSTP packets that are received and sent on the switching device.

The **undo stp compliance** command restores the default format for the MSTP packets that are received and sent on the switching device.

By default, the MSTP packet format is **auto**.

Format

stp compliance { **auto** | **dot1s** | **legacy** }

undo stp compliance

Parameters

Parameter	Description	Value
auto	Indicates that the protocol format is self-adaptive.	-
dot1s	Indicates that the format is standard IEEE 802.1s.	-
legacy	Indicates the private packet format.	-

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP protocol packets have two formats: dot1s (IEEE 802.1s standard packets) and legacy (proprietary protocol packets). The **stp compliance** command can be used on a device to set an MSTP packet format based on the format of the MSTP packet received from a remote device so that this device can better communicate with the remote device.

The auto mode is set to allow a port to automatically switch to the MSTP protocol packet format used by the remote end based on the MSTP protocol packet format received from the remote end. This enables the two interfaces to use the same MSTP protocol packet format.

Example

Set the format of the MSTP packets to the standard format of the interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp compliance dot1s
```

Restore the self-adaptive format of the MSTP packets that are received and sent by the switching device.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo stp compliance
```

Related Topics

6.8.4 display stp

6.8.26 stp config-digest-snoop

Function

The **stp config-digest-snoop** command enables digest snooping.

The **undo stp config-digest-snoop** command disables digest snooping.

By default, the digest snooping is disabled.

Format

stp config-digest-snoop

undo stp config-digest-snoop

Parameters

None

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

On an MSTP network where Huawei and non-Huawei devices are interconnected, if the Huawei and non-Huawei devices have the same region name, revision level, and VLAN mapping table but different BPDU keys, the **stp config-digest-snoop** command can be used to enable the Huawei and non-Huawei devices to exchange BPDUs.

Example

Enable digest snooping on Eth2/0/0.

```
<Huawei> system-view
```

```
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp config-digest-snoop
```

Related Topics

6.8.4 display stp

6.8.27 stp converge

Function

The **stp converge** command sets the converging mode of a spanning tree protocol.

The **undo stp converge** command restores the default mode.

By default, the converging mode of the spanning tree protocol is **normal**.

Format

stp converge { **fast** | **normal** }

undo stp converge

Parameters

Parameter	Description	Value
fast	Indicates ARP entries that will be directly deleted.	-
normal	Indicates ARP entries that will age quickly.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, if the topology of a spanning tree instance changes, the forwarding paths of VLANs that are mapped to this instance change. As a result, ARP entries related to these VLANs need to be updated. Based on methods for processing ARP entries, the converging modes of a spanning tree protocol are classified into fast and normal:

- In fast mode, entries that need to be updated in an ARP table are directly deleted.
- In normal mode, entries that need to be updated in an ARP table quickly age. A switching device sets the EXPIRE time of these ARP entries to 0 in order to age them. If the number of detection times for aging out ARP entries is

greater than 0, the switching device detects these ARP entries before deleting them.

The **stp converge** command can be used to set a converging mode based on the method for processing ARP entries.

Precautions

If the **stp converge fast** command is run on a switching device and the topology of a spanning tree instance changes, the switching device will directly delete the ARP entries that need to be updated in the ARP table.

If the **stp converge normal** command is run on a switching device and the topology of a spanning tree instance changes, the switching device will age the ARP entries that need to be updated in the ARP table.

Setting the converging mode of a spanning tree protocol to **normal** is recommended. If the fast mode is used, frequent ARP entry deletion will affect services and even may cause the CPU usage of the device to reach 100%. As a result, packet processing will time out, causing network flapping.

Example

Set the converging mode of the spanning tree protocol on the Ethernet switch as normal.

```
<Huawei> system-view
[Huawei] stp converge normal
```

Related Topics

6.8.4 display stp

6.8.28 stp cost

Function

The **stp cost** command sets the path cost of a port in a spanning tree.

The **undo stp cost** command restores the default path cost.

By default, the path cost of a port in a spanning tree is the path cost corresponding to the port rate.

Format

stp [**instance** *instance-id*] **cost** *cost*

undo stp [**instance** *instance-id*] **cost**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the number of a spanning tree instance. If **instance** *instance-id* is not specified, it indicates the path cost of an interface in CIST.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: ● AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. ● AR2220, AR2240, and AR3200 series: 49.
cost	Specifies the path cost of an interface.	According to different calculation standards, the value ranges are as follows: ● Huawei legacy standard: 1 to 200,000 ● IEEE 802.1d-1998 standard: 1 to 65535 ● IEEE 802.1t standard: 1 to 200,000,000

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The path cost of a port is an important basis for calculating a spanning tree. Path costs determine root port selection. In a spanning tree, the port with the lowest path cost to the root bridge is selected as a root port.

If different path costs are set for a port on an MSTP device in different spanning tree instances, traffic of different VLANs will be forwarded along different physical links and VLAN-based load balancing can be carried out.

Path costs depend on path cost calculation standards. After the path cost calculation standard is determined, set a relatively small path cost within a specified range for a port that has a high link rate. In the Huawei legacy standard, default path costs for ports with different link rates are different, as shown in the following table.

 Copyright © Huawei Technologies Co., Ltd.

Table 6-58 Mappings between link rates and path costs (Huawei legacy standard)

Link Rate	Recommended Value Default, Value	Recommended Value Range	Value Range
10 Mbit/s	2000	200-20000	1-200,000
100 Mbit/s	200	20-2000	1-200,000
1 Gbit/s	20	2-200	1-200,000
10 Gbit/s	2	2-20	1-200,000
Over 10 Gbit/s	1	1-2	1-200,000

Prerequisites

A path cost calculation standard has been set using the **stp pathcost-standard** command.

Precautions

If the path cost of a port, the spanning tree where the port resides needs to be recalculated.

If the **stp pathcost-standard** command is used to change the path cost calculation standard, the path cost set using the **stp cost** command for a port will be restored to the default value.

Example

Set the path cost of Eth2/0/0 in spanning tree instance 2 to 200.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp instance 2 cost 200
```

Related Topics

6.8.4 display stp

6.8.37 stp pathcost-standard

6.8.29 stp edged-port

Function

The **stp edged-port enable** command sets the current port as an edge port.

The **stp edged-port disable** command sets the current port as a non-edge port.

The **undo stp edged-port** command restores the default attribute of an edge port.

By default, all the ports on the switching device are non-edge ports.

Format

stp edged-port { **enable** | **disable** }

undo stp edged-port

Parameters

Parameter	Description	Value
enable	Sets the current port as an edge port.	-
disable	Sets the current port as a non-edge port.	-

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

Precautions

If a port of a switching device receives a BPDU after being configured as an edge port, the switching device will automatically set the port as a non-edge port and recalculate the spanning tree.

Example

Configure Eth2/0/0 as an edge port.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp edged-port enable
```

Related Topics

6.8.23 stp bpdu-protection
6.8.30 stp edged-port default

6.8.30 stp edged-port default

Function

The **stp edged-port default** command configures the ports on a switching device as edge ports.

The **undo stp edged-port default** command restores the default setting.

By default, the ports on a switching device are non-edge ports.

Format

stp edged-port default

undo stp edged-port default

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a port connected to terminals does not need to participate in spanning tree calculation. If the port participates in spanning tree calculation, the network convergence speed will be affected. In addition, status changes of the port may cause network flapping, interrupting user traffic. To address this problem, you can run the **stp edged-port enable** command to configure the port as an edge port. Then, the port will not participate in the spanning tree calculation. This speeds up network convergence and improves network stability.

NOTICE

After the **stp edged-port default** command is run on a device, all ports of the device will be become edge ports. During network topology calculation, running the **stp edged-port default** command may cause a loop. Exercise caution when using this command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If a port of a switching device receives a BPDU after being configured as an edge port, the switching device will automatically set the port as a non-edge port and recalculate the spanning tree.

To prevent attackers from forging BPDUs to change edge ports on a switching device to non-edge ports, you can run the **stp bpdu-protection** command in the system view to configure BPDU protection on the switching device. After BPDU protection is enabled on a switching device, the switching device shuts down the edge port if the edge port receives a BPDU. The attributes of the edge port are not changed.

Example

Configure all ports on an edge device as edge ports.

```
<Huawei> system-view
[Huawei] stp edged-port default
```

Related Topics

6.8.23 stp bpdu-protection

6.8.29 stp edged-port

6.8.31 stp enable

Function

The **stp enable** command enables STP/RSTP/MSTP on a switching device or an interface.

The **undo stp enable** command disables STP/RSTP/MSTP on a switching device or an interface.

The **stp disable** command disables STP/RSTP/MSTP on a switching device or an interface.

The **undo stp disable** command enables STP/RSTP/MSTP on a switching device or an interface.

By default, STP/RSTP/MSTP is enabled on a switching device.

Format

stp enable

undo stp enable

stp disable

undo stp disable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view, Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a complex Layer 2 network, to prevent loops or break loops, STP/RSTP/MSTP can be configured on switching devices.

Running the **stp enable** command enables STP/RSTP/MSTP. The devices running STP/RSTP/MSTP discover loops on the network by exchanging information with each other and trim the ring topology into a loop-free tree topology by blocking a certain interface. In this manner, replication and circular propagation of packets are prevented on the network. In addition, the processing performance of devices is prevented from deteriorating.

Enabling STP/RSTP/MSTP consumes system resources so that you can run the **stp disable** command to disable STP/RSTP/MSTP on devices or interfaces that do not participate in the spanning tree calculation.

Pre-configuration Tasks

After STP/RSTP/MSTP is enabled on a ring network, STP/RSTP/MSTP immediately calculates spanning trees on the network. Configurations on a switching device, such as, the switching device priority and port priority, will affect spanning tree calculation. Any change of the configurations may cause network flapping. Therefore, to ensure rapid and stable spanning tree calculation, before enabling STP/RSTP/MSTP, perform basic configurations on the switching device and its interfaces. For example:

- Run the **stp** [**instance** *instance-id*] **priority** *priority* command to set the priority of the switching device in the spanning tree.
- Run the **stp** [**instance** *instance-id*] **root primary** command to set the switching device as the primary root bridge of the spanning tree.
- Run the **stp** [**instance** *instance-id*] **root secondary** command to set the switching device as the secondary root bridge of the spanning tree.
- If the spanning tree protocol is MSTP, run the **region-name** *name*, **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] } &<1-10>, **vlan-mapping modulo**, and **revision-level** *level* commands to configure the MST region.

Other configurations are needed based on real-world situations.

Precautions

- If STP/RSTP/MSTP is enabled on an interface, the interface participates in the spanning tree calculation and determine whether it is in the forwarding state according to the calculation result.

 Copyright © Huawei Technologies Co., Ltd.

- If STP/RSTP/MSTP is disabled on an interface, the interface does not participate in the spanning tree calculation and it is always in the forwarding state.
- STP/RSTP/MSTP must be enabled on all interfaces that participate in the spanning tree calculation. Otherwise, a loop may occur.
- Spanning tree calculation may result in network flapping. Before network convergence, packets cannot be correctly forwarded. In this case, if the DHCP server is configured on a VLANIF interface, DHCP clients obtain IP addresses slowly. To solve the problem, disable STP or configure the device interface connected to a terminal as the edge interface.

Example

Enable STP/RSTP/MSTP on a switching device.

```
<Huawei> system-view
[Huawei] stp enable
```

Disable STP/RSTP/MSTP on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp disable
```

Related Topics

6.8.4 display stp

6.8.32 stp loop-protection

Function

The **stp loop-protection** command enables loop protection on the current port.

The **undo stp loop-protection** command disables loop protection on the current port.

By default, loop protection on ports is disabled.

Format

stp loop-protection

undo stp loop-protection

Parameters

None.

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree protocol, a switching device maintains the status of the root port and blocked port by continually receiving BPDUs from the upstream switching device. If ports cannot receive BPDUs from the upstream switching device due to link congestion or unidirectional link failures, the switching device will re-select a root port. Then, the previous root port becomes a designated port and the previous blocked port enters the Forwarding state. As a result, loops may occur on the network.

To prevent the preceding problems, deploy loop protection. If the root port or alternate port does not receive BPDUs from the upstream device for a long time, the switch enabled with loop protection sends a notification to the NMS. If the root port is used, the root port enters the Discarding state and becomes the designated port. If the alternate port is used, the alternate port keeps blocked and becomes the designated port. In this case, loops will not occur. After the link is not congested or unidirectional link failures are rectified, the port receives BPDUs for negotiation and restores its original role and status.

NOTE

- An Alternate port is the backup of the root port. When the root port can normally send and receive BPDUs, the Alternate port is in the blocked state.
- Between two interconnected switching devices in a spanning tree, the switching device nearer to the root bridge is the upstream device of the other devices.

Precautions

Loop protection and root protection cannot be configured on the same interface simultaneously.

Example

Enable loop protection on the Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp loop-protection
```

Related Topics

6.8.4 display stp

6.8.33 stp max-hops

Function

The **stp max-hops** command sets the maximum hops of a spanning tree in an MST region.

The **undo stp max-hops** command restores the default value of the maximum hops of a spanning tree.

By default, the maximum hops in an MST region is 20.

Format

stp max-hops *hop*

undo stp max-hops

Parameters

Parameter	Description	Value
hop	Specifies the maximum hops.	The value ranges from 1 to 40.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Switching devices on a Layer 2 network running MSTP communicate with each other by exchanging MST BPDUs. An MST BPDU has a field that indicates the number of remaining hops.

- The number of remaining hops in a BPDU sent by the root switching device equals the maximum number of hops.
- The number of remaining hops in a BPDU sent by a non-root switching device equals the maximum number of hops minus the number of hops from the non-root switching device to the root switching device.
- If a switching device receives a BPDU in which the number of remaining hops is 0, the switching device will discard the BPDU.

Therefore, the maximum number of hops of a spanning tree in an MST region determines the network scale. The **stp max-hops** command can be used to set the maximum number of hops in an MST domain so that the network scale of a spanning tree can be controlled.

Precautions

In an MST region, the maximum number of hops set on the root switching device in a CIST or an MSTI is the maximum number of hops in the CIST or MSTI.

Example

Set the maximum hops in the MST region to 35.

```
<Huawei> system-view
[Huawei] stp max-hops 35
```

Related Topics

6.8.4 display stp

6.8.34 stp mcheck

Function

The **stp mcheck** command configures a port to automatically switch from the STP mode back to the RSTP/MSTP mode.

By default, a port transitions from the STP mode to the RSTP/MSTP mode by receiving BPDUs. A port that does not receive BPDUs cannot transition from the STP mode to the RSTP/MSTP mode.

Format

stp mcheck

Parameters

None

Views

System view, Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a port of an RSTP/MSTP switching device is directly connected to an STP switching device, the port automatically switches to the STP mode and then sends BPDUs. This ensures that the two switching devices properly communicate with each other. If the STP switching device is powered off or removed, the port on the RSTP/MSTP switching device cannot switch back to the RSTP/MSTP mode. As a result, the RSTP/MSTP device cannot communicate with other RSTP/MSTP switching devices.

When the interface goes Up, you can run the **stp mcheck** command. After this command is run on a port, the port will automatically switch from the STP mode back to the RSTP/MSTP mode.

Precautions

This command does not take effect on a port in Down state.

Running the **stp mcheck** command in the system view configures all ports on the current switching device to automatically switch back to the RSTP/MSTP mode.

 Copyright © Huawei Technologies Co., Ltd.

Running the **stp mcheck** command in the MSTP process view configures all ports bound to the current MSTP process to automatically switch back to the RSTP/MSTP mode.

Running the **stp mcheck** command in the interface view configures only the current port to automatically switch back to the RSTP/MSTP mode.

Example

Perform MCheck on Eth2/0/0 and switch it to the MSTP mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp mcheck
```

6.8.35 stp mode (system view)

Function

The **stp mode** command sets the operation mode of the spanning tree protocol on a switching device.

The **undo stp mode** command restores the default operation mode of the spanning tree protocol.

By default, the switching device operates in MSTP mode.

Format

stp mode { **mstp** | **rstp** | **stp** }

undo stp mode

Parameters

Parameter	Description	Value
mstp	Indicates the MSTP mode.	-
rstp	Indicates the RSTP mode.	-
stp	Indicates the STP mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an STP/RSTP/MSTP network, switching devices running different spanning tree protocols cannot communicate with each other. As a result, spanning trees cannot

be properly calculated. A switching device has three operation modes: MSTP, RSTP, and STP.

The **stp mode** command can be used to set a proper operation mode for a spanning tree protocol on a switching device and enables the switching device to identify BPDUs sent by a switching device that runs a different spanning tree protocol during communication.

By default, all ports on a switching device operate in MSTP mode. When a switching device finds that it is directly connected to an STP switching device, it automatically switch the operation mode the port directly connected to the STP switching device to STP.

Configuration Impact

- After the **stp mode mstp** command is run on a switching device, all ports running MSTP on the switching device, excluding the ports directly connected to STP switching devices, operate in MSTP mode and can send MSTP BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode rstp** command is run on a switching device, all ports running RSTP on the switching device, excluding the ports directly connected to STP switching devices, operate in RSTP mode and can send RSTP BPDUs. The ports directly connected to STP switching devices operate in STP mode.
- After the **stp mode stp** command is run on a switching device, all ports of the switching device operate in STP mode and send configured BPDUs.

Precautions

- A port operating in MSTP mode can communicate with a port operating in RSTP mode.
- The **stp mode rstp** command can be used to enable a switch that does not support MSTP to communicate with an STP switch.

Example

Set the operation mode of the switching device to the STP mode.

```
<Huawei> system-view
[Huawei] stp mode stp
```

Related Topics

6.8.4 display stp

6.8.36 stp no-agreement-check

Function

The **stp no-agreement-check** command configures the common fast transition mechanism on an interface.

The **undo stp no-agreement-check** command restores the default fast transition mechanism on an interface.

By default, the enhanced transition mechanism is configured on an interface.

Format

stp no-agreement-check

undo stp no-agreement-check

Parameters

None

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If Huawei and non-Huawei data communication devices are deployed on a network running a spanning tree protocol, the Huawei devices and non-Huawei devices may fail to communicate with each other, because they have different Proposal/Agreement mechanisms. To address this problem, the **stp no-agreement-check** command can be used to set a common fast transition mechanism or an enhanced transition mechanism on a port.

- Running the **stp no-agreement-check** command configures a common fast transition mechanism on a port.
- Running the **undo stp no-agreement-check** command configures an enhanced fast transition mechanism on a port.

Precautions

The fast transition mechanism is also called the Proposal/Agreement mechanism. The device currently supports the following modes:

- Enhanced mode: The current interface counts a root port when it calculates the synchronization flag bit.
  a. An upstream device sends a Proposal message to a downstream device requesting fast status transition. After receiving the message, the downstream device sets the port connected to the upstream device as the root port and blocks all non-edge ports.
  b. The upstream device then sends an Agreement message to the downstream device. After the downstream device receives the message, the root port transitions to the Forwarding state.
  c. The downstream device then responds with an Agreement message. After receiving the message, the upstream device sets the port connected to the downstream device as the designated port, and then the status of the designated port changes to Forwarding.
- Common mode: The current interface ignores the root port when it calculates the synchronization flag bit.

 Copyright © Huawei Technologies Co., Ltd.

a. An upstream device sends a Proposal message to a downstream device requesting fast transition. After receiving the message, the downstream device sets the port connected to the upstream device as the root port and blocks all non-edge ports. Then, the status of the root port changes to Forwarding.
b. The downstream device then responds with an Agreement message. After receiving the message, the upstream device sets the port connected to the downstream device as the designated port, and then the status of the designated port changes to Forwarding.

NOTE

Between two interconnected switching devices in a spanning tree, the switching device nearer to the root bridge is the upstream device of the other devices.

Example

Configure the common fast transition mechanism for the Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp no-agreement-check
```

6.8.37 stp pathcost-standard

Function

The **stp pathcost-standard** command sets the standard used to calculate the path cost.

The **undo stp pathcost-standard** command restores the default standard used to calculate the path cost.

By default, the IEEE 802.1T is used to calculate the path cost.

Format

stp pathcost-standard { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

Parameters

Parameter	Description	Value
dot1d-1998	Indicates IEEE 802.1D standard that used to calculate the path cost.	-
dot1t	Indicates IEEE 802.1T standard that used to calculate the path cost.	-
legacy	Indicates Huawei legacy standard that used to calculate the path cost.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A path cost is a port parameter, and is used by a spanning tree protocol to select a link. By calculating path costs, a spanning tree protocol selects stable links, blocks redundant paths, and trims a network into a loop-free network. The path cost range is determined by the path cost calculation standard.

Table 6-59 lists path costs defined by the IEEE 802.1D-1998 standard, IEEE 802.1T standard, and Huawei legacy standard. Different vendors use different standards.

Table 6-59 Path cost list

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1T Standard	Huawei Legacy Standard
0	-	65535	200,000,000	200,000
10 Mbps	Half-Duplex	100	2,000,000	2000
	Full-Duplex	99	1,999,999	1999
	Aggregated Link 2 Ports	95	1,000,000	1800
	Aggregated Link 3 Ports	95	666,666	1600
	Aggregated Link 4 Ports	95	500,000	1400
100 Mbps	Half-Duplex	19	200,000	200
	Full-Duplex	18	199,999	199
	Aggregated Link 2 Ports	15	100,000	180
	Aggregated Link 3 Ports	15	66,666	160
	Aggregated Link 4 Ports	15	50,000	140
1000 Mbps	Full-Duplex	4	20,000	20
	Aggregated Link 2 Ports	3	10,000	18

 Copyright © Huawei Technologies Co., Ltd.

Interface Rate	Interface Mode	Recommended STP Path Cost		
		IEEE 802.1D-1998 Standard	IEEE 802.1T Standard	Huawei Legacy Standard
	Aggregated Link 3 Ports	3	6666	16
	Aggregated Link 4 Ports	3	5000	14
10 Gbps	Full-Duplex	2	2000	2
	Aggregated Link 2 Ports	1	1000	1
	Aggregated Link 3 Ports	1	666	1
	Aggregated Link 4 Ports	1	500	1

Precautions

If the path cost calculation standard is changed on a port, the path cost of the port is restored to the default value. The **stp cost** command can be used to set a path cost for a port.

Usually, all switching devices on the same network use the same path cost calculation standard.

Example

Use the IEEE 802.1d-1998 to calculate the path cost.

```
<Huawei> system-view
[Huawei] stp pathcost-standard dot1d-1998
```

Related Topics

6.8.4 display stp

6.8.38 stp point-to-point

Function

The **stp point-to-point** command sets the link type of a port.

The **undo stp point-to-point** command restores the default link type.

By default, the link type of the ports on the switching device is **auto**. That is, the spanning tree protocol detects whether a port is connected to a P2P link.

Format

stp point-to-point { **auto** | **force-false** | **force-true** }

undo stp point-to-point

Parameters

Parameter	Description	Value
force-true	Indicates the link type is P2P.	-
force-false	Indicates the link type is non-P2P.	-
auto	Indicates that the spanning tree protocol detects automatically whether the port is connected to a P2P link.	-

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, if a port of a switching device is connected to a non-P2P link, the port cannot perform fast status transition.

If a port works in full-duplex mode, the port is connected to a P2P link, and **force-true** can be set in the **stp point-to-point** command.

If a port works in half-duplex mode, the **stp point-to-point force-true** command can be used to forcibly set the type of the link to which the port is connected to P2P, implementing rapid network convergence.

Precautions

The **stp point-to-point** command configuration on a port takes effect in all spanning tree instances where the port resides.

Example

Set the link type of Eth2/0/0 as P2P.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp point-to-point force-true
```

6.8.39 stp port priority

Function

The **stp port priority** command sets the priority of a port in a spanning tree.

The **undo stp port priority** command restores the default priority.

By default, the priority of a port in a spanning tree is 128.

Format

stp [**instance** *instance-id*] **port priority** *priority*

undo stp [**instance** *instance-id*] **port priority**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the spanning tree instance. If this parameter is not specified, the statistics about the topology changes of a CIST are displayed.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: ● AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. ● AR2220, AR2240, and AR3200 series: 49.
priority	Specifies the priority of a port.	The priority ranks from 0 to 240 in descending order. The value is an integer multiple of 16, such as, 0, 16, and 32.

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When ports participate in spanning tree calculation, the PIDs of these ports on switching devices may affect the designated port election result. During spanning tree calculation, the port with the smallest PID is elected as the designated port.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

A PID is the ID of a port, and consists of a 4-bit priority and a 12-bit port number.

The **stp port priority** command can be used to change the priority of a port. This affects the PID of the port and determines whether the port can be elected as the designated port.

Precautions

When the priority of a port changes, a spanning tree protocol recalculates the role of the port and performs status transition for the port.

The priority of a port determines the role of the port in a specified spanning tree instance and process. You can set different priorities for a port in different spanning tree instances or processes so that user traffic can be forwarded along different links and traffic load balancing can be implemented.

Example

Set the priority of Eth2/0/0 to 16 in the spanning tree instance 2.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp instance 2 port priority 16
```

Related Topics

6.8.40 stp priority

6.8.4 display stp

6.8.40 stp priority

Function

The **stp priority** command sets the priority of the switching device in a spanning tree.

The **undo stp priority** command restores the default priority.

By default, the priority of the switching device in a spanning tree is 32768.

Format

stp [**instance** *instance-id*] **priority** *priority*

undo stp [**instance** *instance-id*] **priority**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of a spanning tree instance. If the parameter **instance** *instance-id* is not specified, the configuration takes effect on a CIST instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: ● AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. ● AR2220, AR2240, and AR3200 series: 49.
priority	Specifies the priority of the switching device in a spanning tree. The smaller the value is, the higher the switch priority is.	The priority ranks from 0 to 61440. The value is an integer multiple of 4096, such as 0, 4096 and 8192. The default is 32768.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Priorities of switching devices are an important factor to calculate a spanning tree and determine the selection of the root bridge.

On an STP/RSTP/MSTP network, each spanning tree has only one root bridge, which is responsible for sending BPDUs. Owning to the importance of the root bridge, the switching device with high performance and network hierarchy is generally chosen as the root bridge. The priority of such a switching device, however, may not be that high. Therefore, setting a high priority for the switching device is necessary so that the device can function as a root bridge.

Other devices with low performance and network hierarchy are not fit to be a root bridge. Therefore, set low priorities for these devices.

On an MSTP network, each switching device can be set with a distinct priority in each spanning tree instance.

Precautions

The smaller the priority value of a switching device is, the higher the possibility that the switching device is selected as the root bridge.

 Copyright © Huawei Technologies Co., Ltd.

If a switching device has been configured as the primary or secondary root bridge, before changing the priority of the switching device, run the **undo stp** [**instance** *instance-id*] **root** command to disable the root bridge or secondary root bridge function.

If the **stp root primary** command is run to set a switching device as the primary root bridge, the priority value of the switching device is 0.

If the **stp root secondary** command is run to set a switching device as the secondary root bridge, the priority value of the switching device is 4096.

Example

Set the priority of the switching device in spanning tree instance 1 to 4096.

```
<Huawei> system-view
[Huawei] stp instance 1 priority 4096
```

Related Topics

6.8.4 display stp

6.8.41 stp region-configuration

Function

The **stp region-configuration** command displays the MST region view.

The **undo stp region-configuration** command restores the default configuration of the MST region.

The default parameters of the MST regions are as follows:

- MST region name: MAC address of the main processing unit of the switching device.
- MSTP revision level 0.
- VLAN mapping table: all VLANs are mapped to CIST.

Format

stp region-configuration

undo stp region-configuration

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees and these spanning trees are independent of each other. Each spanning tree is called a multiple spanning tree instance (MSTI) and each region is called a multiple spanning tree (MST) region.

Two switching devices belong to the same MST region if they have the following parameters the same:

- MST region name
- Mappings between VLANs and MSTIs
- Revision level of the MST region

If the preceding parameters need to be set for the current switching device or the current process, run the **stp region-configuration** command to enter the MST region view first.

Follow-up Procedure

After the **stp region-configuration** command is run to enter the MST region view, run the following commands:

- Run the **region-name** command to set the MST region name.
- Run the **instance** or the **vlan-mapping modulo** command to set the mappings between VLANs and MSTIs.
- Run the **revision-level** name command to set the revision level of the MST region.

Example

Enter the MST region view.

```
<Huawei> system-view
[Huawei] stp region-configuration
[Huawei-mst-region]
```

Related Topics

6.8.10 display stp region-configuration

6.8.42 stp root

Function

The **stp root** command configures a switching device as a root bridge or secondary root bridge of a spanning tree.

The **undo stp root** command cancels the configuration.

By default, a switching device does not function as the root bridge or secondary root bridge of a spanning tree.

 Copyright © Huawei Technologies Co., Ltd.

Format

stp [**instance** *instance-id*] **root** { **primary** | **secondary** }

undo stp [**instance** *instance-id*] **root**

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of a spanning tree instance. If the parameter **instance** *instance-id* is not specified, the configuration takes effect on a CIST instance.	The value is an integer ranging from 0 to 4094. Value 0 refers to CIST. **NOTE** *instance-id* ranges from 0 to 4094. Different models support different numbers of instances: ● AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, and AR2204: 17. ● AR2220, AR2240, and AR3200 series: 49.
primary	Indicates that the switching device functions as the root bridge of a spanning tree.	-
secondary	Indicates that the switching device functions as the secondary root bridge of a spanning tree.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an STP/RSTP/MSTP network, each spanning tree has only one root bridge, which is responsible for sending BPDUs. Owning to the importance of the root bridge, the switching device with high performance and network hierarchy is generally chosen as a root bridge. The priority of such a device, however, may be not that high. Therefore, setting a high priority for the switching device is necessary so that the device can function as a root bridge.

To ensure nonstop traffic transmission, run the **stp root** command to configure the switching device as the secondary root bridge. When the root bridge is faulty or is powered off, the secondary root bridge becomes the root bridge during spanning tree calculation.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

After the **stp root primary** command is run to set a switching device to be the primary root bridge, the priority value of the switching device is 0 in the spanning tree and the priority cannot be modified.

The secondary root bridge specified using the **stp root secondary** command has the priority value of 4096 and the priority cannot be modified.

Precautions

A spanning tree has only one root bridge.

A switching device in a spanning tree cannot function both as the primary root bridge and as the secondary root bridge.

If multiple secondary root bridges are set in a spanning tree, the one with the smallest MAC address functions as the secondary root bridge of the spanning tree.

Example

Set the switching device as the root bridge of spanning tree instance 1.

```
<Huawei> system-view
[Huawei] stp instance 1 root primary
```

Set the switching device as the secondary root bridge of spanning tree instance 4.

```
<Huawei> system-view
[Huawei] stp instance 4 root secondary
```

Related Topics

6.8.4 display stp

6.8.43 stp root-protection

Function

The **stp root-protection** command enables root protection at the current port.

The **undo stp root-protection** command restores the default setting of root protection.

By default, root protection is disabled at all ports.

Format

stp root-protection

undo stp root-protection

Parameters

None

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Owning to incorrect configurations or malicious attacks on the network, a root bridge may receive BPDUs with a higher priority. Consequently, the root bridge is no longer able to serve as the root bridge, and the network topology is changed, triggering a spanning tree recalculation. This spanning tree recalculation may transfer traffic from high-speed links to low-speed links, causing traffic congestion.

If a designated port is enabled with the root protection function, the port role cannot be changed. Once a designated port that is enabled with root protection receives BPDUs with a higher priority, the port enters the Discarding state and does not forward packets. If the port does not receive any BPDUs with a higher priority before a period (generally two Forward Delay periods) expires, the port automatically enters the Forwarding state.

NOTE

You can run the **stp timer forward-delay** command to set the Forward Delay period.

Precautions

The root protection function takes effect only on a designated port. In addition, configuring the root protection function on a port that functions as the designated port in all instances is recommended.

If the **stp root-protection** command is run on other types of ports, the root protection function does not take effect.

Loop protection and root protection cannot be configured on the same interface simultaneously.

Example

Enable the root protection function on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp root-protection
```

Related Topics

6.8.42 stp root

6.8.42 stp root

6.8.4 display stp

6.8.44 stp tc-protection

Function

The **stp tc-protection** command enables TC BPDU protection.

The **undo stp tc-protection** command disables TC BPDU protection.

By default, TC BPDU protection is disabled.

Format

stp tc-protection

undo stp tc-protection

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network where spanning tree protocol is running, a switching device that receives TC BPDUs will delete the corresponding MAC entries and ARP entries. Frequent deletion operations will greatly affect the CPU, leading to a high CPU usage. In this case, you can run the **stp tc-protection** command to enable the TC BPDU attack defense function.

After the **stp tc-protection** command is run to enable the TC BPDU attack defense function, the number of times that TC BPDUs are processed by the switching device within a unit time is configurable (the default unit time is 2s, and the default number of times is 1). If the number of TC BPDUs that the switching device receives within a unit time exceeds the specified threshold, the switching device handles TC BPDUs only for the specified number of times. Additional TC BPDUs are processed by the switching device as a whole for once after the timer (that is, the specified time period) expires. In this manner, the switching device is prevented from frequently deleting its MAC entries and ARP entries so that the CPU is protected against overburden.

NOTE

The value of the unit time is consistent with the spanning tree protocol's Hello time and can be set using the **stp timer hello** command.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

After the **stp tc-protection** command is run, run the **stp tc-protection threshold** command to set the number of times that TC BPDUs are processed by the switching device within a unit time.

Example

Enable the TC BPDU protection function.

```
<Huawei> system-view
[Huawei] stp tc-protection
```

Related Topics

6.8.46 stp tc-protection threshold

6.8.45 stp tc-protection interval

Function

The **stp tc-protection interval** command sets the time for a device to process the maximum number of TC BPDUs.

The **undo stp tc-protection interval** command restores the default value.

By default, the time is the Hello timer length.

Format

stp tc-protection interval *interval-value*

undo stp tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the time for a device to process the maximum number of TC BPDUs.	The value is an integer ranging from 1 to 600, in seconds.

Views

System view or MST process region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network running a spanning tree protocol, a device deletes MAC address entries and ARP entries after receiving TC packets. Frequent entry deletion may cause high CPU usage.

 Copyright © Huawei Technologies Co., Ltd.

The TC attack defense function is enabled by default, you can configure the time, which the device takes to handle a given number of TC packets and immediately refresh forwarding entries, by running the **stp tc-protection interval** command. Within the time specified by *interval-value*, the device handles a given number of TC packets. Excess TC packets are processed by the device at once after the timer (whose length is the configured time) expires. This mechanism ensures that the device does not frequently delete its MAC entries and ARP entries, and therefore does not have excessive CPU usage.

NOTE

You can specify the maximum number of TC packets that the device processes can handle in the specified time by running the **stp tc-protection threshold** command.

Example

Configure the amount of time, which MSTP process 0 and MSTP process 1 take to handle a given number of TC packets and immediately refreshes forwarding entries, to 10 seconds.

```
<Huawei> system-view
[Huawei] stp tc-protection interval 10
[Huawei] stp process 1
[Huawei-mst-process-1] stp tc-protection interval 10
```

Related Topics

6.8.46 stp tc-protection threshold

6.8.46 stp tc-protection threshold

Function

The **stp tc-protection threshold** command sets the number of times that a device handles received TC BPDUs and updates forwarding entries within a unit time.

The **undo stp tc-protection threshold** command restores the default setting.

By default, after a device receives TC BPDUs, the default number of times that the device handles the TC BPDUs and updates forwarding entries is 1 within a unit time.

Format

stp tc-protection threshold *threshold*

undo stp tc-protection threshold

Parameters

Parameter	Description	Value
threshold	Indicates the number of times that a device handles the TC BPUD and updates forwarding entries per unit of time.	The value is an integer ranging from 1 to 255.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view or MST process region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a Layer 2 network where MSTP is run, a switching device that receives TC BPDUs will delete the corresponding MAC entries and ARP entries. Frequent deletion operations will greatly affect the CPU, leading to a high CPU usage.

The TC attack defense function is enabled by default, the number of times that TC BPDUs are processed by the switching device within a unit time is configurable (the default unit time is 2s, and the default number of times is 1). If the number of TC BPDUs that the switching device receives within a unit time exceeds the specified threshold, the switching device handles TC BPDUs only for the specified number of times. Additional TC BPDUs are processed by the switching device as a whole for once after the timer (that is, the specified time period) expires. In this manner, the switching device is prevented from frequently deleting its MAC entries and ARP entries so that the CPU is protected against overburden.

NOTE

The value of the unit time is consistent with the Hello time and can be set using the **stp timer hello** command.

Example

Set the threshold update forwarding entries to 5.

```
<Huawei> system-view
[Huawei] stp tc-protection threshold 5
```

Related Topics

6.8.45 stp tc-protection interval

6.8.47 stp timer forward-delay

Function

The **stp timer forward-delay** command sets the value of the Forward Delay of a switching device.

The **undo stp timer forward-delay** command restores the default value of the Forward Delay.

By default, the value of the Forward Delay of a switching device is 1500 centiseconds (15 seconds).

 Copyright © Huawei Technologies Co., Ltd.

Format

stp timer forward-delay *forward-delay*

undo stp timer forward-delay

Parameters

Parameter	Description	Value
forward-delay	Specifies the value of the Forward Delay.	The value ranges from 400 to 3000 centiseconds by a step of 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running a spanning tree algorithm, if the network topology is changed, it takes time to advertise new BPDU configuration messages on the network. During this period, interfaces to be blocked may not be blocked in time and interface ever blocked may not be blocked. As a result, a temporary loop may be formed. To prevent this problem, you can use the Forward Delay timer to set a delay time. During the delay time, all interfaces are blocked temporarily.

The **stp timer forward-delay** command is used to set the Forward Delay timer.

Precautions

The value of the Forward Delay timer set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the value of the Forward Delay timer of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and MaxAge are as follows. The spanning tree functions properly only if the correct relationships are established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) >= Max Age
- Max Age >= 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

Set the Forward Delay to 2000 centiseconds (20 seconds).

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] stp timer forward-delay 2000
```

Related Topics

6.8.48 stp timer hello

6.8.49 stp timer max-age

6.8.24 stp bridge-diameter

6.8.48 stp timer hello

Function

The **stp timer hello** command sets the interval of the switching device to send BPDUs, that is, the value of the Hello Time.

The **undo stp timer hello** command restores the default setting.

By default, the interval of the switch to send BPDUs is 200 centiseconds (2 seconds).

Format

stp timer hello *hello-time*

undo stp timer hello

Parameters

Parameter	Description	Value
hello-time	Specifies the interval of the switch to send BPDUs.	The value ranges from 100 to 1000, in centiseconds by a step of 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device periodically sends BPDUs to other devices in the same spanning tree at the interval of the Hello Time. Sending BPDUs periodically ensures that the spanning tree is stable. The **stp timer hello** command can be used to set the BPDU sending interval, that is, the Hello Time.

 Copyright © Huawei Technologies Co., Ltd.

If no BPDUs are received by the switching device within the timeout period (timeout period = Hello Time x 3 x Timer Factor), the spanning tree is calculated again.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

The value of the Hello Time set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the value of the Hello Time of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree works properly only if the relationships are correctly established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) >= Max Age
- Max Age >= 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

Set the Hello Time to 400 centiseconds (4 seconds).

```
<Huawei> system-view
[Huawei] stp timer hello 400
```

Related Topics

6.8.47 stp timer forward-delay

6.8.49 stp timer max-age

6.8.24 stp bridge-diameter

6.8.49 stp timer max-age

Function

The **stp timer max-age** command sets the Max Age of a switching device, that is, the BPDU aging time on a port of the switching device.

The **undo stp timer max-age** command restores the default setting.

By default, the Max Age of a switching device is 2000 centiseconds (20 seconds).

Format

stp timer max-age *max-age*

undo stp timer max-age

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-age	Specifies the BPDU aging time on a port of the switch.	The value ranges from 600 to 4000 in centiseconds with a step of 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device checks whether the BPDUs received from an upstream switching device time out based on the set Max Age value. If the received BPDUs time out, the switching device ages the BPDUs and blocks the port that receives the BPDUs. Then, the switching device sends the BPDUs with the switching device as the root bridge. This aging mechanism effectively controls the diameter of the spanning tree. After the **stp timer max-age** command is run, the Max Age value is set to control the timeout period of received BPDUs.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

The value of the Max Age set on the root bridge is advertised to other devices of the same spanning tree using BPDUs. Then it becomes the MaxAge value of all devices in the spanning tree.

The relationships between the Hello Time, Forward Delay, and Max Age are as follows. The spanning tree functions properly only if the relationships are correctly established. Otherwise, frequent network flapping occurs.

- 2 x (Forward Delay - 1.0 second) >= Max Age
- Max Age >= 2 x (Hello Time + 1.0 second)

Running the **stp bridge-diameter** command to set the network diameter is recommended. After the **stp bridge-diameter** command is run, the switching device sets optimum values for the three parameters, Hello Time, Forward Delay, and Max Age.

Example

Set the Max Age to 1000 centiseconds (10 seconds).

```
<Huawei> system-view
```

```
[Huawei] stp timer max-age 1000
```

Related Topics

6.8.4 display stp
6.8.47 stp timer forward-delay
6.8.48 stp timer hello
6.8.24 stp bridge-diameter

6.8.50 stp timer-factor

Function

The **stp timer-factor** command sets the timer factor of the timeout period of a switching device to the Hello Time.

The **undo stp timer-factor** command restores the default setting.

By default, the timer factor is 3.

NOTE

If a switching device does not receive BPDUs from an upstream device within the timeout period (timeout period = Hello Time × 3 × Timer Factor), the spanning tree is calculated again.

Format

stp timer-factor *factor*

undo stp timer-factor

Parameters

Parameter	Description	Value
factor	Specifies the timer factor.	The value ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, if a switching device does not receive BPDUs from an upstream device within the timeout period, it considers that the upstream device becomes faulty, and will recalculate the spanning tree.

 Copyright © Huawei Technologies Co., Ltd.

Sometimes, however, the failure of the upstream device to send BPDUs within the timeout period is only because it is busy processing services. In this case, the spanning tree cannot be calculated. Therefore, you can set a long timeout period on a stable network to avoid the waste of network resources.

NOTE

In a spanning tree, the device closer to the root bridge is the upstream device of another connected device.

Precautions

If the parameter *factor* is set smaller, the timeout period of the switching device to re-calculate the spanning tree is shorter. In this case, there is a higher probability that the switching device incorrectly considers the upstream device as being faulty.

If the parameter *factor* is set larger, the timeout period of the switching device to re-calculate the spanning tree is longer. In this case, there is a higher probability that the traffic becomes interrupted because the upstream device has become faulty.

Example

Set the Timer-Factor of the switching device to 6.

```
<Huawei> system-view
[Huawei] stp timer-factor 6
```

Related Topics

6.8.48 stp timer hello

6.8.51 stp transmit-limit (interface view)

Function

The **stp transmit-limit** command sets the maximum number of BPDUs that the current port can send in a specified period.

The **undo stp transmit-limit** command restores the default maximum BPDUs.

By default, the maximum number of BPDUs that a port sends is 6 per second.

Format

stp transmit-limit *packet-number*

undo stp transmit-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum number of BPDUs that a port can send in a specified period.	The value is an integer that ranges from 1 to 255.

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where a spanning tree protocol is enabled, a switching device periodically sends BPDUs to other devices in the same spanning tree with the interval of the Hello Time. Sending BPDUs periodically ensures that the spanning tree is stable. If the number of sent BPDUs are great in a specified period, excessive system and bandwidth resources will be consumed.

To prevent this problem from occurring, run the **stp transmit-limit** command to set the maximum number of BPDUs that can be sent by an interface in a specified period. In this manner, the BPDU sending speed is controlled, preventing excessive use of system and bandwidth resources by MSTP when the network topology flaps.

Precautions

After the **stp transmit-limit** command is configured, the maximum number of BPDUs sent in a specified period by the interface is determined by the set value.

Example

Set the maximum BPDUs that Eth2/0/0 can send in a specified period to 5.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] stp transmit-limit 5
```

6.8.52 stp transmit-limit (system view)

Function

The **stp transmit-limit** command configures the maximum number of Bridge Protocol Data Units (BPDUs) that each interface of the local device can send per second.

The **undo stp transmit-limit** command restores the maximum number of BPDUs, which can be sent by each interface of the local device per second, to the default value.

By default, each interface can send a maximum of 6 BPDUs per second.

Format

stp transmit-limit *packet-number*

undo stp transmit-limit

Parameters

Parameter	Description	Value
packet-number	Maximum number of BPDUs that each interface of the local device can send per second	The value is an integer ranging from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network running the Spanning Tree Protocol (STP), a switch sends BPDUs to other devices in the same spanning tree at the interval of the Hello time, to maintain the spanning tree stability. If a number of BPDUs are sent every second, system and bandwidth resources will be greatly consumed.

NOTE

You can configure the Hello time by using the **stp timer hello** command. The Hello time is the length of the Hello timer and specifies the interval at which the switch sends BPDUs.

To prevent excessive usage of system and bandwidth resources, you can run the **stp transmit-limit** command to configure the maximum number of BPDUs that each interface of the local device can send per second. This configuration controls the BPDU sending rate and prevents the Multiple Spanning Tree Protocol (MSTP) from consuming too many system and bandwidth resources when topology flapping occurs.

Precautions

After the **stp transmit-limit** command is executed, *packet-number* controls the maximum number of BPDUs that each interface can send per second.

You can also configure the maximum number of BPDUs that a specific interface can send per second by running the **stp transmit-limit (interface view)** command in the view of this interface. The **stp transmit-limit (interface view)** command configuration in the interface view takes precedence over the **stp transmit-limit** command configuration in the system view. That is, if the **stp transmit-limit (interface view)** command is configured in the view of an interface, the **stp transmit-limit** command configuration in the system view does not take effect for this interface.

Example

Configure the maximum number of BPDUs that each interface of the local device can send per second to **5**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] stp transmit-limit 5
```

Related Topics

6.8.48 stp timer hello

6.8.51 stp transmit-limit (interface view)

6.8.53 vlan-mapping modulo

Function

The **vlan-mapping modulo** command enables VLAN-to-instance mapping assignment based on a default algorithm.

The **undo vlan-mapping modulo** command restores the default mapping.

By default, all VLANs are mapped to CIST, namely, spanning tree instance 0.

Format

vlan-mapping modulo *modulo*

undo vlan-mapping modulo

Parameters

Parameter	Description	Value
modulo	Specifies the value of a module.	The value is an integer ranging from 1 to 16.

Views

MST region view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSTP divides a switching network into multiple regions, each of which has multiple spanning trees that are independent of each other. Each spanning tree is called an MSTI and each region is called an MST region.

Two switching devices belong to the same MST region only when they have the following same configurations:

- MST region name
- Mappings between MSTIs and VLANs

 Copyright © Huawei Technologies Co., Ltd.

- MST region revision level

The **vlan-mapping modulo** command is used to enable VLAN-to-instance mapping assignment based on a default algorithm.

NOTE

In the command, **vlan-mapping modulo** indicates that the formula (VLAN ID-1)%modulo +1 is used. In the formula, (VLAN ID-1)%modulo means the remainder of (VLAN ID-1) divided by the value of modulo. This formula is used to map a VLAN to the corresponding MSTI. The calculation result of the formula is ID of the mapping MSTI. For example, if the modulus is 16, the switch maps VLAN 1 to MSTI 1, VLAN 2 to MSTI 2 VLAN 16 to MSTI 16, VLAN 17 to MSTI 1, and so on.

Precautions

The **instance** *instance-id* **vlan** { *vlan-id* [**to** *vlan-id*] }&<1-10> command is recommended because VLAN-to-instance mapping assignments cannot meet actual mapping requirements.

Example

Map all VLANs to spanning tree instances modulo 16.

```
<Huawei> system-view
[Huawei] stp region-configuration
[Huawei-mst-region] vlan-mapping modulo 16
```

Related Topics

6.8.10 display stp region-configuration

6.9 SEP Configuration Commands

NOTE

The AR100 series, AR120 series, AR161, AR161G-L, AR161W, AR169, AR169-P-M9, AR169G-L, AR169W, AR161EW, AR161EW-M1, AR161G-Lc, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR161G-U, AR169W-P-M9, AR169RW-P-M9 do not support SEP.

6.9.1 block port

Function

The **block port** command configures the mode in which an interface is blocked on the device where the primary edge interface resides.

The **undo block port** command restores the default mode in which an interface is blocked on the device where the primary edge interface resides.

By default, the system selects a blocked interface from the interfaces on both ends of the link that is established last or the link that recovers from a fault last.

Format

block port { **sysname** *sysname* **interface** { *interface-type interface-number* | *interface-name* } | **hop** *hop-id* | **optimal** | **middle** }

undo block port

Parameters

Parameter	Description	Value
sysname *sysname*	Specifies the name of the device where the interface to be blocked resides.	The value is a string of 1 to 20 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
interface { *interface-type interface-number* | *interface-name* }	Specifies the interface to be blocked. *interface-type* indicates the type of the interface to be blocked. After SEP is enabled, **sysname** *sysname* and **interface** { *interface-type interface-number* | *interface-name* } specify the interface to be blocked. Before configuring the mode in which an interface is blocked, run the **display sep topology verbose** command to view detailed information about the topology of the current ring and obtain information about all the interfaces in the topology. Then, you can specify the device and interface names.	*interface-name* specifies the user-defined interface name in the format of interface type+interface number. The value of *interface-name* is a string of 1 to 63 case-sensitive characters without spaces. The interface type can be: 40GE, 100GE, Eth-Trunk, Ethernet, GigabitEthernet, MultiGE, XGigabitEthernet.
hop *hop-id*	Specifies the interface with the specified hop count from the primary edge interface as the blocked interface. *hop-id* specifies the hop count. If *hop-id* is set to 1, the primary edge interface is blocked. If *hop-id* is set to 2, the neighboring interface of the primary edge interface is blocked. The hop count increases by steps of 1 in the downstream direction of the primary edge interface.	The value is an integer that ranges from 1 to 128.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
optimal	Specifies the interface with the highest priority as the blocked interface. SEP compares interface priorities as follows: 1. A larger value set using the **sep segment priority** command indicates a higher priority. 2. If interfaces have the same priority value, a smaller bridge MAC address indicates a higher priority. 3. If interfaces have the same priority value and the same bridge MAC address, a smaller interface number indicates a higher priority.	-
middle	Specifies the interface in the middle of the SEP segment as the blocked interface.	-

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some interfaces are blocked to prevent loops. Any interface in a SEP segment may be blocked if no interface is specified for blocking. A complete SEP segment contains only one blocked interface.

You can specify the blocked interface according to network requirements or your reference. The specified interface is not blocked immediately. Normally, the blocked interface is one of the two interfaces that complete neighbor negotiations last. The specified interface preempts to be the blocked interface only after the preemption mechanism takes effect.

The SEP segment must have been created before the **block port** command is used.

To make the **block port** command configuration take effect, complete the following tasks before using the **block port** command.

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **control-vlan (SEP segment view)** command to configure the control VLAN of the SEP segment.

- Run the **sep segment (interface view)** command to add the interface to the SEP segment and configure the interface as the primary edge interface.

Example

On the device where the primary edge interface is located, specify the device and interface names to block the specified interface.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] block port sysname Huawei interface ethernet 2/0/0
```

On the device where the primary edge interface is located, specify the interface with the specified hop count from the primary edge interface as the interface to be blocked.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] block port hop 3
```

On the device where the primary edge interface is located, specify the interface with the highest priority as the interface to be blocked.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] block port optimal
```

On the device where the primary edge interface is located, specify the interface in the middle of the SEP segment as the interface to be blocked.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] block port middle
```

Related Topics

6.9.12 sep segment
6.9.13 sep segment (interface view)
6.9.2 control-vlan (SEP segment view)
6.9.5 display sep interface

6.9.2 control-vlan (SEP segment view)

Function

The **control-vlan** command configures the control VLAN of a SEP segment for SEP packet transmission.

The **undo control-vlan** command deletes the configured control VLAN.

By default, no control VLAN is configured in a SEP segment.

Format

control-vlan *vlan-id*

undo control-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the control VLAN in a SEP segment.	The value is an integer that ranges from 1 to 4094.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

After a SEP segment is created, run the **control-vlan** command to create a control VLAN for the SEP segment.

Compared with a data VLAN, a control VLAN forwards only SEP packets but not service packets in a SEP segment, which improves SEP security.

Devices in the same SEP segment must be configured with the same control VLAN to fast forward SEP packets. Different SEP segments can use the same control VLAN.

NOTE

In the absence of neighbors, devices that are not in a SEP segment cannot be added to the control VLAN of the SEP segment. Otherwise, network loops occur.

The control VLAN must be not created, and is not used by, VLAN mapping, and VLAN stacking. In addition, no interface is added to the control VLAN.

You must configure the control VLAN of a SEP segment before adding interfaces to the SEP segment.

- If the SEP segment contains an interface, the control VLAN cannot be deleted. To delete the configured control VLAN, run the **undo sep segment** command in the interface view to remove the interface from the SEP segment, and then run the **undo control-vlan** command.
- If the SEP segment contains no interface, you can configure the control VLAN multiple times. Only the latest configuration takes effect.
- After the control VLAN is created, the configuration file automatically displays the command for creating the VLAN.

  Each SEP segment must have a control VLAN. After an interface is added to a SEP segment that has a control VLAN, the interface is automatically added to the control VLAN.

  - If the interface type is trunk, in the configuration file, the **port trunk allow-pass vlan** command is displayed in the view of the interface added to the SEP segment.

- If the interface type is hybrid, in the configuration file, the **port hybrid tagged vlan** command is displayed in the view of the interface added to the SEP segment.

To check whether the control VLAN is created or view the control VLAN where SEP packets are transmitted, run the **display sep interface** command and specify the **verbose** parameter.

Example

Configure control VLAN 5 for SEP segment 1.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] control-vlan 5
```

Related Topics

6.9.12 sep segment

6.9.5 display sep interface

6.9.3 description (SEP segment view)

Function

The **description** command configures the description of the SEP segment.

The **undo description** command restores the default setting.

By default, the description of an SEP segment is null.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an SEP segment	The value is a string of 1 to 255 case-sensitive characters. When double quotation marks are used around the string, spaces are allowed in the string.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a device running SEP, you can run the **description** command to configure the description of the SEP segment, such as the SEP segment ID. Configuring the description of an SEP segment facilitates the maintenance of the SEP segment.

Precautions

After being configured in the SEP-Segment view, the description command takes effect only on the local device.

Example

Configure the description **It's segment 10** for SEP segment 10.

```
<Huawei> system-view
[Huawei] sep segment 10
[Huawei-sep-segment10] description It's segment 10
```

Related Topics

6.9.12 sep segment

6.9.4 display sep error packet

Function

The **display sep error packet** command displays the statistics about error packets received by SEP and the contents of recently received packets.

Format

display sep error packet

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device on a Layer 2 network runs SEP is attacked by SEP error packets, the **display sep error packet** command can be used to view recently received MSTP error packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the statistics about error packets received by SEP and the contents of recently received packets.

```
<Huawei> display sep error packet
4 error-packets have been recieved and the last

one is recieved at 2012/05/02 12:45:31 UTC+08:00 :


01 80 c2 00 00 02 00 e0 fc 8e 0b 34 88 09 01 01
01 14 80 00 00 e0 fc 8e 0b 34 01 21 80 00 09 06
47 00 00 00 02 14 00 00 00 00 00 00 00 00 00 00
00 00 00 00 c7 00 00 00 03 10 ff ff 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00
```

Related Topics

6.9.10 reset sep error packet statistics

6.9.5 display sep interface

Function

The **display sep interface** command displays information about the interfaces in a SEP segment.

Format

display sep interface [*interface-type interface-number* | **segment** *segment-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays SEP information on a specified interface. *interface-type* specifies the type of an interface. *interface-number* specifies the number of an interface.	-
segment *segment-id*	Displays information about the interfaces in a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
verbose	Displays detailed SEP information on a specified interface, including traffic statistics.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

To monitor the status of an interface or locate an interface fault, use this command to collect statistics and the status of the interface. Then you can locate the interface fault according to the statistics.

When using the **display sep interface** command,

- If no parameter is specified, this command displays information about all the interfaces in SEP segments.
- If only *interface-type interface-number* is specified, this command displays information about a specified interface in SEP segments.
- If only **segment** *segment-id* is specified, this command displays information about all the interfaces in a specified SEP segment.
- If only **verbose** is specified, this command displays detailed information about all the interfaces in SEP segments.
- If *interface-type interface-number* and **verbose** are specified, this command displays detailed information about a specified interface in SEP segments.
- If **segment** *segment-id* and **verbose** are specified, this command displays detailed information about a specified interface in a specified SEP segment.

NOTE

Before running this command, complete the following tasks:

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **sep segment (interface view)** command in the Ethernet interface view to add an interface to a SEP segment and set the role of the interface as required.

Example

Display information about all the interfaces in SEP segments.

```
<Huawei> display sep interface
SEP segment 1
-----------------------------------------------------------------
Interface       Port Role      Neighbor Status          Port Status
-----------------------------------------------------------------
Eth1/0/1          *secondary    up                 forwarding
Eth1/0/2          common        up                 forwarding
```

Display information about a specified interface in SEP segments.

```
<Huawei> display sep interface ethernet 2/0/0
SEP segment 1
-----------------------------------------------------------------
Interface         Port Role     Neighbor Status     Port Status
-----------------------------------------------------------------
Eth2/0/0          common        up                 forwarding
```

Display detailed information about a specified interface in a specified SEP segment.

```
<Huawei> display sep interface segment 1 verbose
SEP segment 1
Control-vlan          :3
```

```
Preempt Delay Timer    :0
TC-Notify Propagate to :stp
-----------------------------------------------------------------
Interface              :Eth1/0/1
Port Role              :Config = *primary / Active =  *secondary
Port Priority          :64
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :NULL
NBR TLV             rx :0                tx :0
LSP INFO TLV        rx :0                tx :0
LSP ACK TLV         rx :0                tx :0
PREEMPT REQ TLV     rx :0                tx :0
PREEMPT ACK TLV     rx :0                tx :0
TC Notify           rx :0                tx :0
EPA                 rx :0                tx :0
Interface              :Eth1/0/2
Port Role              :Config = common / Active =  common
Port Priority          :64
Port Status            :forwarding
Neighbor Status        :up
Neighbor Port          :LSW3 - Eth1/0/1 (00e0-ff7c-6400.0000)
NBR TLV             rx :51820            tx :51882
LSP INFO TLV        rx :50380            tx :5776
LSP ACK TLV         rx :5749             tx :50296
PREEMPT REQ TLV     rx :0                tx :1
PREEMPT ACK TLV     rx :4                tx :0
TC Notify           rx :22               tx :3
EPA                 rx :0                tx :0
```

Table 6-60 Description of the **display sep interface** command output

Item	Description
SEP segment	ID of a SEP segment.
Interface	Interface name.
Port Role	Role of an interface in a SEP segment: ● common: common interface ● primary: primary edge interface ● secondary: secondary edge interface ● *primary: no-neighbor primary edge interface ● *secondary: no-neighbor secondary edge interface
Neighbor Status	Status of the neighbor state machine: ● up: Neighbor negotiations succeed and the protocol status of the interface is Up. ● down: Neighbor negotiations fail and no neighbor relationship is established between the local interface and its peer interface. ● init: The local interface receives packets from the peer interface and neighbor negotiations start. ● conflict: The local interface receives packets from multiple peer interfaces and the protocol status of the interface is Conflict.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Port Status	Current status of the interface: ● discarding: The interface is blocked and can forward SEP packets but not data packets. ● forwarding: The interface is in Forwarding state and can forward both data packets and SEP packets.
Port Priority	Interface priority. It is an integer that ranges from 1 to 128. By default, the interface priority is 64.
Control-vlan	ID of a control VLAN. A control VLAN is used to forward SEP packets in the local SEP segment.
Preempt Delay Timer	Delay in preempting the blocked interface after the faulty link recovers, in seconds.
TC-Notify Propagate to	Object to be notified of a topology change.
Neighbor Port	Neighbor interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no neighbor, the value is NULL.
NBR TLV	Neighbor information packet: ● rx: indicates the number of received neighbor information packets. ● tx: indicates the number of sent neighbor information packets.
LSP INFO TLV	LSA packets: ● rx: indicates the number of received LSA packets. ● tx: indicates the number of sent LSA packets.
LSP ACK TLV	ACK packets in response to LSA packets: ● rx: indicates the number of received ACK packets in response to LSA packets. ● tx: indicates the number of sent ACK packets in response to LSA packets.
PREEMPT REQ TLV	Preemption packets: ● rx: indicates the number of received preemption packets. ● tx: indicates the number of sent preemption packets.
PREEMPT ACK TLV	ACK packets in response to preemption packets: ● rx: indicates the number of received ACK packets in response to preemption packets. ● tx: indicates the number of sent ACK packets in response to preemption packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TC Notify	Packets reporting topology changes: ● rx: indicates the number of received packets reporting topology changes. ● tx: indicates the number of sent packets reporting topology changes.
EPA	Packets reporting edge port selection: ● rx: indicates the number of received packets reporting edge port selection. ● tx: indicates the number of sent packets reporting edge port selection.

Related Topics

6.9.12 sep segment
6.9.13 sep segment (interface view)

6.9.6 display sep segment

Function

The **display sep segment** command displays the configurations of SEP segments.

Format

display sep segment {*segment-id* | **all** }

Parameters

Parameter	Description	Value
segment-id	Displays the configuration of a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
all	Displays the configurations of all SEP segments.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After SEP is configured, you can run the **display sep segment** command to view the configuration of a specified SEP segment or all SEP segments on the network.

Example

Display the configuration of SEP segment 2.

```
<Huawei> display sep segment 2
-----------------------------------------------------------------
SEP Segment ID         :2
SEP Control-vlan       :3
Protected-instance     :0 to 5 9 12 to 13 16 to 17 20 to 21
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected    :Eth-Trunk2
Name of Port Member    :Eth-Trunk3
TC-Notify Propagate to :segment 6
```

Display the configurations of all SEP segments.

```
<Huawei> display sep segment all
-----------------------------------------------------------------
SEP Segment ID         :1
SEP Control-vlan       :10
Protected-instance     :0 to 48
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected    :Eth-Trunk2
Name of Port Member    :
TC-Notify Propagate to :segment 6
-----------------------------------------------------------------
SEP Segment ID         :2
SEP Control-vlan       :3
Protected-instance     :0 to 5 9 12 to 13 16 to 17 20 to 21
Preempt Delay Timer(s) :20/0 (Configured/Remaining)
Block Port Expected    :Eth-Trunk2
Name of Port Member    :Eth-Trunk3
TC-Notify Propagate to :segment 6
-----------------------------------------------------------------
Total number of segment configured = 2
```

Table 6-61 Description of the **display sep segment** command output

Item	Description
SEP Segment ID	ID of a SEP segment.
SEP Control-vlan	Control VLAN for transmitting SEP packets.
Protected-instance	ID of a protected instance.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Preempt Delay Timer(s)	Delay in preemption. ● Configured: configured value of the Preempt Delay Timer (s). ● Remaining: remaining value of the Preempt Delay Timer (s). If the timer does not start, 0 is displayed. If preemption is not configured for an SEP segment, one of the two interfaces that complete neighbor negotiation last remains to be blocked even though a network fault is rectified. Consequently, the interface specified to be blocked is not blocked.
Block Port Expected	Specified blocked interface.
Name of Port Member	Name of a member interface.
TC-Notify Propagate to	Object to which topology changes are reported.

6.9.7 display sep topology

Function

The **display sep topology** command displays the topologies of SEP segments.

Format

display sep topology [**segment** *segment-id*] [**verbose**]

Parameters

Parameter	Description	Value
segment *segment-id*	Displays the topology of a specified SEP segment.	The value is an integer that ranges from 1 to 1024.
verbose	Displays detailed information about the topology of a SEP segment.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After SEP is configured, you can run the **display sep topology** command to view the topologies of SEP segments, including device names, names of the interfaces added to SEP segments, and roles of the interfaces in a SEP segment.

When running the **display sep topology** command:

- If no parameter is specified, this command displays brief information about the topologies of all the SEP segments on the device.
- If only **segment** *segment-id* is specified, this command displays brief information about the topology of a specified SEP segment.
- If only **verbose** is specified, this command displays detailed information about the topologies of all SEP segments on the device.
- If **segment** *segment-id* and **verbose** are specified, this command displays detailed information about the topology of a specified SEP segment on the device.

NOTE

Before running this command, complete the following tasks:

- Run the **sep segment** command in the system view to create a SEP segment.
- Run the **sep segment (interface view)** command in the Ethernet interface view to add an interface to the SEP segment and set the role of the interface as required.

  Edge interfaces must be configured in the SEP segment; otherwise, the SEP topology is incomplete and the system displays an error message.

Example

Display the topologies of all SEP segments on the device.

```
<Huawei> display sep topology
SEP segment 1
-----------------------------------------------------------------
System Name      Port Name          Port Role       Port Status
-----------------------------------------------------------------
ROUTER1          GE1/0/1            primary         forwarding
ROUTER2          GE1/0/1            common          forwarding
ROUTER2          GE1/0/2            common          forwarding
ROUTER3          GE1/0/1            common          forwarding
ROUTER3          GE1/0/2            common          discarding
ROUTER4          GE1/0/1            common          forwarding
ROUTER4          GE1/0/2            common          forwarding
ROUTER5          GE1/0/1            common          forwarding
ROUTER5          GE1/0/3            common          forwarding
ROUTER1          GE1/0/3            secondary       forwarding
```

Display detailed topology information in SEP segment 1.

```
<Huawei> display sep topology segment 1 verbose
SEP segment 1
SEP detects a segment failure that may be caused by an incomplete topology
-----------------------------------------------------------------
System Name     :224-Router
Port Name       :Eth0/0/2
Port Role       :Config = *primary / Active =  *secondary
PortID          :00e0-fc03-2240.0000
Port Priority   :41024
Port Status     :discarding
Link Status     :down
Neighbor Status :down
```

```
Age Time        :60(s)
Sequence Number :0x80000003
Neighbor Port   :NULL
Brother Port    :224-Router - Eth0/0/1 (00e0-fc03-2240.0001)
```

Table 6-62 Description of the **display sep topology** command output

Item	Description
SEP segment	ID of a SEP segment.
System Name	Device name.
Port Name	Name of an interface added to the SEP segment.
Port Role	Role of an interface in the SEP segment: ● common: common interface ● primary: primary edge interface ● secondary: secondary edge interface ● *primary: no-neighbor primary edge interface ● *secondary: no-neighbor secondary edge interface Config: indicates the configured role of an interface in a SEP segment. Active: indicates the running role of an interface in a SEP segment. **NOTE** In normal situations, an SEP segment has a primary edge interface, a secondary edge interface, and common interfaces.
Port Status	Current status of an interface: ● discarding: The interface is blocked and can forward SEP packets but not data packets. ● forwarding: The interface is in Forwarding state and can forward both data packets and SEP packets.
PortID	Interface ID. It is in the format of 6-byte system MAC address +2-byte interface number.
Port Priority	Interface priority. It is an integer that ranges from 1 to 128. By default, the interface priority is 64.
Link Status	Link status: ● up: The link is Up. ● down: The link is Down.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Neighbor Status	Status of the neighbor state machine: ● up: Neighbor negotiations succeed and the protocol status of the interface is Up. ● down: Neighbor negotiations fail and no neighbor relationship is established between the local interface and its peer interface. ● init: The local interface receives packets from the peer interface and neighbor negotiations start. ● conflict: The local interface receives packets from multiple peer interfaces and the protocol status of the interface is Conflict.
Age Time	Aging time of the LSA.
Sequence Number	Sequence number of the LSA.
Neighbor Port	Neighbor interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no neighbor, the value is NULL.
Brother Port	Brother interface. It is in the format of system name +interface name (system MAC address or interface ID). If there is no brother, the value is NULL.

Related Topics

6.9.12 sep segment

6.9.13 sep segment (interface view)

6.9.8 preempt (SEP segment view)

Function

The **preempt** command configures the blocked interface preemption mode on the device where the primary edge interface is located.

The **undo preempt delay** command cancels the configuration of delayed preemption on the primary edge interface.

By default, the SEP preemption mode is not configured.

Format

preempt { **manual** | **delay** *seconds* }

undo preempt delay

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
manual	Indicates the manual preemption mode.	-
delay	Indicates the delayed preemption mode.	-
seconds	Specifies the preemption delay. You can configure a preemption delay to prevent network flapping. When link faults are rectified, the specified interface waits until the delay timer expires, and then preempts to be the blocked interface.	The value is an integer that ranges from 15 to 600, in seconds.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some ports are blocked to prevent loops.

When a link in the SEP segment fails, the blocked interface in Up state changes to the Forwarding state after receiving a fault notification packet. If the preemption mode is not configured, when all link faults are rectified or the last two interfaces enabled with SEP complete neighbor negotiations, interfaces send blocking status packets to each other. The interface with the highest priority is then blocked, and the other interfaces enter the Forwarding state.

NOTE

The blocked interface is determined by the administrative priority and user-defined priority of each interface. The priority value of an interface contains 16 bits. The higher 8 bits are defined by the system, and the lower 8 bits are set by the user. The value of the lower 8 bits ranges from 1 to 128, and the default value is 64. The interface with the highest priority is blocked.

If the preemption mode is configured on the device where the primary edge interface is located, the specified interface transitions to the Blocking state and sends blocking status packets to other ports.

SEP supports the following preemption modes:

- Delayed preemption

  After all interface faults are rectified, the faulty interface does not send any fault notification packet. If the primary edge interface does not receive any fault notification packet within 3 seconds, it starts the delay timer. When the delay timer expires, the devices in the SEP segment initiate blocked interface preemption.

NOTE

You must set the preemption delay when delayed preemption is used because there is no default delay time.

After delay preemption is configured, you can run the **undo preempt delay** command in the SEP segment view to delete the configuration of delay preemption.

- Manual preemption

  In this mode, if the link status databases of the primary and secondary edge interfaces are complete, the primary edge interface sends preemption packets to block the specified interface. Then the specified interface sends blocking status packets to request the original blocked interface to transition to the Forwarding state.

  NOTE

  - Manual preemption is a one-off operation and will not take effect again after the preemption is complete on the SEP segment. To change the blocked interface, run the **preempt** command and specify the **delay** parameter to configure delayed preemption.
  - Manual preemption causes a short link disconnection in the SEP segment.

Blocked interface preemption is triggered when the following conditions are met:

- The primary edge interface in the SEP segment is selected.

  To configure interface roles, run the **sep segment** *segment-id* [**edge** [**no-neighbour**] { **primary** | **secondary** }] command in the interface view.
- The method of selecting the interface to block is configured on the device where the primary edge interface is located.

  To configure the method of selecting the interface to block, run the **block port** { **sysname** *sysname* **interface** *interface-type interface-number* | **hop** *hop-id* | **optimal** | **middle** } command in the SEP segment view.
- The topology of the SEP segment must be complete.

Example

Configure manual preemption on the device where the primary edge port is located.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] preempt manual
```

Configure delayed preemption on the device where the primary edge port is located.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] preempt delay 100
```

Related Topics

6.9.12 sep segment

6.9.13 sep segment (interface view)

6.9.1 block port

6.9.5 display sep interface

6.9.9 protected-instance

Function

The **protected-instance** command configures protected instances in a SEP segment.

The **undo protected-instance** command deletes the protected instances in a SEP segment.

By default, no protected instance is configured in a SEP segment.

Format

protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> }

undo protected-instance { **all** | { *instance-id1* [**to** *instance-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
all	Indicates all protected instances in a SEP segment.	-
instance-id1 [**to** *instance-id2*]	Specifies the IDs of protected instances in a SEP segment. The keyword **to** connecting two instance IDs, indicating an ID range from *instance-id1* to *instance-id2*. The value of *instance-id2* must be greater than the value of *instance-id1*. **&<1-10>** indicates that the parameter before the sign (&) can be repeated 1 to 10 times. Instance IDs must be listed in ascending order; otherwise, the system displays the message "Error: The protected instance list is invalid."	The value is an integer in the range 0 to 4094. Each device supports a maximum of 65 instances.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In common SEP networking, a physical ring can be configured with only one SEP segment in which only one interface can be blocked. If an interface in a complete SEP segment is blocked, all service data is transmitted only along the path where the primary edge interface is located. The path where the secondary edge interface is located remains idle, wasting bandwidth.

SEP multi-instance is used to improve bandwidth efficiency, allowing each physical interface on a ring network to be added to two SEP segments. A physical ring can be configured with two logical rings, allowing packets carrying different VLAN IDs to pass through. Load balancing is then implemented between the two logical rings. This implementation requires logical rings to be configured with different protected instances and mappings between protected instances and VLANs to be configured. The **protected-instance** command can be used to configure protected instances for a SEP segment.

Prerequisites

The protected instance IDs configured for SEP segments do not overlap. If different SEP segments have duplicate protected instance IDs, replan protected instance IDs.

Follow-up Procedure

Complete the following tasks to configure mappings between protected instances and VLANs:

1. Run the **stp region-configuration** command to enter the MST region view.
2. Run the **instance** *instance-id* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command to configure mappings between protected instances and VLANs.

   The value of *instance-id* specified in this command must be the same as the value of *instance-id* specified in the **protected-instance** command.
3. Run the **active region-configuration** command to activate the configured mappings between protected instances and VLANs.

Precautions

If you run the **protected-instance** command multiple times in the same SEP segment, multiple instances are configured.

After the **protected-instance** command is run to configure different protected instances for SEP segments and mappings between protected instances and VLANs are set, topology changes affect only corresponding VLANs. This ensures reliable data transmission.

Before adding an interface to a SEP segment, ensure that the SEP segment has been configured with protected instances; otherwise, the interface cannot be added to the SEP segment.

Example

Configure protected instances for SEP segment 1.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] protected-instance all
```

Related Topics

6.9.12 sep segment

6.9.10 reset sep error packet statistics

Function

The **reset sep error packet statistics** command clears the statistics of error sep packets.

Format

reset sep error packet statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Applicable Scenario

You can use the **reset sep error packet statistics** command to clear the history statistics when you need to observe the statistics of error sep packets in a period from the current time.

Precautions

The **reset sep error packet statistics** command clears the statistics about error sep packets are cleared and cannot be restored. Therefore, confirm the action before you use the command.

Example

Clear the statistics about error sep packets.

```
<Huawei> reset sep error packet statistics
```

6.9.11 reset sep interface statistics

Function

The **reset sep interface statistics** command clears SEP packet statistics on a specified interface in a SEP segment.

Format

reset sep interface *interface-type interface-number* **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears SEP packet statistics on a specified interface in a SEP segment. *interface-type* specifies the type of the interface in a SEP segment. *interface-number* specifies the number of the interface in a SEP segment.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Before collecting SEP packet statistics on an interface within a certain period, clear existing traffic statistics on this interface. In such a situation, you can run the **reset sep interface statistics** command.

NOTE

- Before the **reset sep interface statistics** command is run, the SEP segment must be created and the interface must be added to the SEP segment.
- After the **reset sep interface statistics** command is run, SEP packet statistics on the specified interface in the SEP segment are cleared and cannot be restored. Confirm your action before you use this command.

Example

Clear SEP packet statistics on Eth 2/0/0 in the SEP segment.

```
<Huawei> reset sep interface ethernet 2/0/0 statistics
```

Related Topics

6.9.12 sep segment
6.9.13 sep segment (interface view)
6.9.5 display sep interface
6.9.7 display sep topology

6.9.12 sep segment

Function

The **sep segment** command creates a SEP segment and displays the SEP segment view. If the specified SEP segment has been created, you can directly enter the SEP segment view.

The **undo sep segment** command deletes the existing SEP segment.

Format

sep segment *segment-id*

undo sep segment *segment-id*

Parameters

Parameter	Description	Value
segment *segment-id*	Specifies the ID of a SEP segment.	The value is an integer that ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

On a Layer 2 switching network, packets will be transmitted infinitely once a loop occurs, causing a broadcast storm. The broadcast storm occupies all the bandwidth on the network, causing network congestion or even breakdown of the entire network. To prevent loops on a Layer 2 switching network, Huawei develops the Smart Ethernet Protection (SEP) protocol.

SEP is a ring network protocol specially used for the Ethernet link layer. It blocks redundant links to prevent loops. It can run on a network together with STP, RSTP, MSTP and supports display of the network topology. When the devices of other vendors are used on the network, SEP can also prevent loops, but does not need to be configured on these devices.

A SEP segment consists of interconnected Layer 2 switching devices configured with the same SEP segment ID and control VLAN ID. A SEP segment is the basic unit for SEP.

Before enabling SEP, run the **sep segment** command to create a SEP segment. Then run the **control-vlan (SEP segment view)** command in the SEP segment view to configure a control VLAN.

A SEP segment can be deleted only when it does not contain any interface. If the SEP segment contains interfaces, run the **undo sep segment** *segment-id* command in the corresponding interface views to delete the interfaces from the SEP segment one by one.

Example

Create SEP segment 1.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

6.9.2 control-vlan (SEP segment view)
6.9.13 sep segment (interface view)
6.9.7 display sep topology

6.9.13 sep segment (interface view)

Function

The **sep segment** command adds an Ethernet interface to a specified SEP segment and configures the role of the Ethernet interface.

The **undo sep segment** command removes an Ethernet interface from a specified SEP segment and deletes the interface role configuration.

By default, an Ethernet interface is not added to a specified SEP segment and is not configured with a role.

Format

sep segment *segment-id* [**edge** [**no-neighbor**] { **primary** | **secondary** }]

undo sep segment *segment-id*

Parameters

Parameter	Description	Value
segment *segment-id*	Specifies the ID of the SEP segment to which an Ethernet interface is added.	The value is an integer that ranges from 1 to 1024.
edge	Specifies the Ethernet interface added to the SEP segment as an edge interface.	-
no-neighbor	Specifies the Ethernet interface as a no-neighbor edge interface.	-
primary	Specifies the Ethernet interface as a primary edge interface.	-
secondary	Specifies the Ethernet interface as a secondary edge interface.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

A Layer 2 interface can forward SEP packets only after being added to a SEP segment. Each Layer 2 switching device in a SEP segment is a node. Each node can have at most two Layer 2 interfaces added to the same SEP segment.

When using the **sep segment** command:

- If no parameter is specified, this command adds an Ethernet interface to a specified SEP segment and configures the interface as a common interface.

  In a SEP segment, all interfaces except edge interfaces and blocked interfaces are common interfaces.

  A common interface monitors the status of the directly-connected SEP link. When the link status changes, the interface sends a topology change notification message to notify its neighbors. Then the topology change notification message is flooded on the link until it finally reaches the primary edge interface. The primary edge interface determines how to process the link change.
- If **edge** and **primary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the primary edge interface.

  A SEP segment has only one primary edge interface, which is determined by the configuration and primary edge interface election. The primary edge interface initiates blocked interface preemption, terminates packets, and sends topology change notification messages to other networks.
- If **edge** and **secondary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the secondary edge interface.

  A SEP segment has only one secondary edge interface, which is determined by the configuration and secondary edge interface election. The secondary edge interface terminates packets and sends topology change notification messages to other networks.
- If **edge**, **no-neighbor**, and **primary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the no-neighbor primary edge interface.

  An interface at the edge of a SEP segment is a no-neighbor edge interface. There are two types of no-neighbor edge interface: no-neighbor primary edge interface and no-neighbor secondary edge interface. You can configure the role of a no-neighbor edge interface. A no-neighbor edge interface terminates packets and sends topology change notification messages to other networks. It is commonly used to interconnect Huawei devices and non-Huawei devices or interconnect Huawei devices and devices that do not support SEP.
- If **edge**, **no-neighbor**, and **secondary** are specified, this command adds an Ethernet interface to the specified SEP segment and configures the interface as the no-neighbor secondary edge interface.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To make the **sep segment** command take effect, ensure that:

- You have created a SEP segment and configured a control VLAN and protected instances.
- To add an interface to a SEP segment, configure the interface as a hybrid or trunk interface.
- If **no-neighbor** is not specified, the interface to be added to the SEP segment is not an STP interface.
- Two interfaces at the edge of a SEP segment must be configured as edge interfaces. The roles of the interfaces are defined by users.
- All the interfaces on the network are Up so that the SEP segment is complete and the displayed topology information is correct.

To view the role of an interface added to a SEP segment, run the **display sep topology** or **display sep interface** command.

Example

Add Eth 2/0/0 to SEP segment 1 and configure the interface as the no-neighbor secondary edge interface.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] sep segment 1 edge no-neighbor secondary
```

Related Topics

6.9.12 sep segment

6.9.2 control-vlan (SEP segment view)

6.9.7 display sep topology

6.9.5 display sep interface

6.9.14 sep segment priority

Function

The **sep segment priority** command configures the priority of an Ethernet interface in a specified SEP segment.

The **undo sep segment priority** command restores the default priority of an Ethernet interface in a specified SEP segment.

By default, the priority of an Ethernet interface in a specified SEP segment is 64.

Format

sep segment *segment-id* **priority** *priority*

undo sep segment *segment-id* **priority**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
segment *segment-id*	Specifies the ID of the SEP segment to which an Ethernet interface is added.	The value is an integer that ranges from 1 to 1024.
priority *priority*	Specifies the priority of an Ethernet interface in a specified SEP segment. A larger value indicates a higher priority. When the link fault is rectified, the interface with the highest priority is likely to become the blocked interface.	The value is an integer that ranges from 1 to 128. The default value is 64.

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

In a SEP segment, some interfaces are blocked to prevent loops. Any interface in a SEP segment may be blocked if no interface is specified for blocking. A complete SEP segment contains only one blocked interface.

If you run the **block port optimal** command to select the blocked interface according to the port priority, the interface priority set using the **sep segment priority** command determines whether the interface will be blocked when an interface fault is rectified.

The blocked interface is determined by the administrative priority and user-defined priority of each interface. The priority value of an interface contains 16 bits. The higher 8 bits are defined by the system, and the lower 8 bits are set by the user. A higher interface priority indicates a higher probability that the interface is blocked.

SEP compares interface priorities as follows:

1. Compares configured interface priority values. A larger value indicates a higher priority.
2. Compares bridge MAC addresses of interfaces with same priority values. A smaller bridge MAC address indicates a higher priority.
3. Compares interface numbers of interfaces with identical bridge MAC addresses. A smaller interface number indicates a higher priority.

Before using the **sep segment priority** command, ensure that the SEP segment is created using the **sep segment** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the priority of Eth 2/0/0 added to SEP segment 1 to 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] sep segment 1 priority 10
```

Related Topics

6.9.12 sep segment
6.9.7 display sep topology
6.9.5 display sep interface

6.9.15 tc-notify

Function

The **tc-notify** command configures a SEP segment to report topology changes to other SEP segments or networks running other ring network protocols.

The **undo tc-notify** command disables a SEP segment from reporting topology changes to other SEP segments or networks running other ring network protocols.

By default, a SEP segment does not send topology change notifications.

Format

tc-notify { **segment** { *segment-id1* [**to** *segment-id2*] } &<1-10> | **stp** }

undo tc-notify { **segment** { *segment-id1* [**to** *segment-id2*] } &<1-10> | **stp** }

Parameters

Parameter	Description	Value
segment *segment-id1* [**to** *segment-id2*]	Specifies the SEP segments to which topology changes of the local SEP segment need to be reported. Topology changes of the local SEP segment are reported to other SEP segments, but not the local SEP segment. The keyword **to** connecting two segment IDs, indicating an ID range from *segment-id1* to *segment-id2*. The value of *segment-id2* must be greater than the value of *segment-id1*.	The value is an integer that ranges from 1 to 1024.
stp	Indicates that the local SEP segment reports topology changes to STP networks.	-

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If topology changes in a SEP segment are not reported to the upper-layer Layer 2 network in time, devices on the upper-layer network retain the original MAC address entries, causing traffic interruption. To ensure uninterrupted traffic transmission, run the **tc-notify** command to configure the local SEP segment to report topology changes to other SEP segments or networks running other ring network protocols.

Prerequisites

The **sep segment** command has been used to create SEP segments.

Precautions

If the **tc-notify** command is run more than once, all configurations take effect.

When the topology of a SEP segment changes, the SEP segment sends topology change notification messages to other SEP segments or networks running other ring network protocols. If the specified segment or network does not exist, the **tc-notify** command configuration does not take effect.

After receiving topology change notification messages from a SEP segment, devices on the upper layer network send Flush FDB packets on the network. Then, all the devices on the upper-layer network delete the original MAC addresses and learn new MAC addresses to ensure normal traffic transmission.

The **tc-notify** command is used on the device connecting a lower-layer network and an upper-layer network.

Example

Configure SEP segment 1 to report topology changes to SEP segments 10 to 20.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] tc-notify segment 10 to 20
```

Configure SEP segment 1 to report topology changes to STP networks.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] tc-notify stp
```

Related Topics

6.9.7 display sep topology

6.9.5 display sep interface

 Copyright © Huawei Technologies Co., Ltd.

6.9.16 tc-protection interval

Function

The **tc-protection interval** command sets the interval for suppressing topology change (TC) notification packets.

The **undo tc-protection interval** command restores the default interval for suppressing TC notification packets.

By default, the interval for suppressing TC notification packets is 2s.

Format

tc-protection interval *interval-value*

undo tc-protection interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval for suppressing TC notification packets. A longer interval ensures stable SEP operating but deteriorates convergence performance.	The value is an integer that ranges from 1 to 10, in seconds.

Views

SEP segment view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Assume that a host is connected to an upstream network through three or more SEP networks. If the topology of the SEP network nearest to the host changes, doubled TC notification packets are flooded on the upper-layer SEP network. Each time TC notification packets pass through a SEP segment, TC notification packets will be doubled. The upstream network will receive multiple duplicate TC notification packets.

Frequent topology change notifications reduce the CPU packet processing capability, and cause devices in the SEP segments to frequently refresh MAC address entries, which consumes bandwidth resources. To address the problem, run the **tc-protection interval** command to suppress TC notification packets.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **sep segment** command has been used to create SEP segments.

Precautions

After this command is used, the upstream network only needs to process one TC notification packet but not multiple duplicate TC notification packets. In addition, this function protects devices on the SEP segment against TC attacks.

Example

Set the interval for suppressing TC notification packets to 3s in SEP segment 1.

```
<Huawei> system-view
[Huawei] sep segment 1
[Huawei-sep-segment1] tc-protection interval 3
```

Related Topics

6.9.12 sep segment

6.10 Layer 2 Protocol Transparent Transmission Commands

6.10.1 l2protocol-tunnel

Function

The **l2protocol-tunnel enable** command enables Layer 2 protocol transparent transmission on an interface.

The **undo l2protocol-tunnel enable** command disables Layer 2 protocol transparent transmission on an interface.

By default, Layer 2 protocol transparent transmission is disabled on an interface.

NOTE

Only Layer 3 interfaces support this command.

Format

l2protocol-tunnel { *protocol-type* | **user-defined-protocol** *protocol-name* } **enable**

undo l2protocol-tunnel { *protocol-type* | **user-defined-protocol** *protocol-name* } **enable**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol.	Enumerated value. The values are as follows: ● STP: Spanning Tree Protocol ● LACP: Link Aggregation Control Protocol ● LLDP: Link Layer Discovery Protocol ● CDP: Cisco Discovery Protocol You can run this command with different values of *protocol-type* specified, and the commands are not overridden.
user-defined-protocol *protocol-name*	Specifies the name of a user-defined Layer 2 protocol.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocols running between user networks, such as MSTP and LACP, must traverse a backbone network to perform Layer 2 protocol calculation.

Generally, the destination MAC addresses in Layer 2 protocol packets of the same Layer 2 protocol are the same. For example, the MSTP PDUs are BPDUs with the destination MAC address 0180-C200-0000. Therefore, when a Layer 2 protocol packet reaches an edge device on a backbone network, the edge device cannot identify whether the Layer 2 protocol packet comes from a user network or the

 Copyright © Huawei Technologies Co., Ltd.

backbone network and sends the Layer 2 protocol packet to the CPU to calculate a spanning tree. As a result, the user network devices calculate a spanning tree with backbone network edge devices but not with user network devices.

You can configure Layer 2 protocol transparent transmission and run the **l2protocol-tunnel group-mac** or **l2protocol-tunnel user-defined-protocol** command to replace the destination MAC address of Layer 2 protocol packets with a specified MAC address. Then run the **l2protocol-tunnel enable** command on the PE interface connected to the public network so that the Layer 2 protocol packets with the specified MAC address can be forwarded from this interface and traverse the public network.

To transparently transmit LACPDUs, you need to run both the **l2protocol-tunnel lacp enable** and **bpdu transmit enable** commands.

Precautions

You must add the interface where the **l2protocol-tunnel enable** command is configured to the network bridge group so that Layer 2 protocol transparent transmission can take effect. You can run the **bridge** *bridge-id* command to add the interface to the network bridge group.

Example

Configure GE1/0/0 to transparently transmit STP BPDUs.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] l2protocol-tunnel stp enable
```

Related Topics

6.10.2 l2protocol-tunnel group-mac

6.10.3 l2protocol-tunnel user-defined-protocol

6.11.6 bridge (interface view)

6.10.2 l2protocol-tunnel group-mac

Function

The **l2protocol-tunnel group-mac** command enables the device to replace the multicast destination MAC address of Layer 2 protocol packets with a specified multicast MAC address.

The **undo l2protocol-tunnel** command cancels the configuration.

By default, the device is not enabled to replace the multicast destination MAC address of Layer 2 protocol packets with a specified multicast MAC address.

Format

l2protocol-tunnel *protocol-type* **group-mac** *group-mac*

undo l2protocol-tunnel *protocol-type*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
protocol-type	Specifies the type of a Layer 2 protocol.	Enumerated value. The values are as follows: ● STP: Spanning Tree Protocol ● LACP: Link Aggregation Control Protocol ● LLDP: Link Layer Discovery Protocol ● CDP: Cisco Discovery Protocol **NOTE** You can run this command with different values of *protocol-type* specified, and the commands are not overridden.
group-mac	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits. The value ranges from 0100-0ccd-0000 to 0100-0ccd-ffff.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocols running between user networks, such as MSTP and LACP, must traverse a backbone network to perform Layer 2 protocol calculation.

Generally, the destination MAC addresses in Layer 2 protocol packets of the same Layer 2 protocol are the same. For example, the MSTP PDUs are BPDUs with the destination MAC address 0180-C200-0000. Therefore, when a Layer 2 protocol packet reaches an edge device on a backbone network, the edge device cannot identify whether the Layer 2 protocol packet comes from a user network or the backbone network and sends the Layer 2 protocol packet to the CPU to calculate

 Copyright © Huawei Technologies Co., Ltd.

a spanning tree. As a result, the user network devices calculate a spanning tree with backbone network edge devices but not with user network devices.

To resolve this problem, run the **l2protocol-tunnel group-mac** command on backbone network edge devices to replace the multicast destination MAC addresses in Layer 2 protocol packets with a specified multicast MAC address (group MAC address). This configuration allows Layer 2 protocol packets to be tunneled so that user network devices can calculate a spanning tree.

Precautions

When configuring Layer 2 protocol transparent transmission, do not use multicast MAC addresses that have been used on the device.

Example

Configure a device to replace the destination MAC address of STP packets with 0100-0ccd-eeee before tunneling the STP BPDUs.

```
<Huawei> system-view
[Huawei] l2protocol-tunnel stp group-mac 0100-0ccd-eeee
Info: Please make sure the input multicast MAC address doesn't conflict with other protocols.
```

Related Topics

6.10.1 l2protocol-tunnel

6.10.3 l2protocol-tunnel user-defined-protocol

Function

The **l2protocol-tunnel user-defined-protocol** command customizes Layer 2 protocol packets, including the protocol name, multicast destination MAC address, and MAC address that replaces the destination MAC address of Layer 2 protocol packets.

The **undo l2protocol-tunnel user-defined-protocol** command cancels the configuration.

By default, Layer 2 protocol packets are not customized.

Format

l2protocol-tunnel user-defined-protocol *protocol-name* **protocol-mac** *protocol-mac* **group-mac** *group-mac*

undo l2protocol-tunnel user-defined-protocol *protocol-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
protocol-name	Specifies the name of a user-defined Layer 2 protocol.	The value is a string of 1 to 31 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
protocol-mac *protocol-mac*	Specifies the multicast destination MAC address of the user-defined protocol packets.	The value is in the format of H-H-H. An H is a hexadecimal number of 4 digits. The value ranges from 0180-c200-0000 to 0180-c200-0013, 0180-c200-0016 to 0180-c200-002f and 0100-0ccc-cccc to 0100-0ccc-cccd.
group-mac *group-mac*	Specifies the multicast MAC address that replaces the destination MAC address of Layer 2 protocol packets.	The value is in the format of H-H-H. An H is a hexadecimal number of 4 digits. The value ranges from 0100-0ccd-0000 to 0100-0ccd-ffff.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When Layer 2 protocol packets with a specified multicast destination MAC address need to be transparently transmitted on an ISP network, you can define characteristic information about the Layer 2 protocol on devices on the ISP network.

Before running the **l2protocol-tunnel enable** command to enable transparent transmission of user-defined Layer 2 protocol packets, run the **l2protocol-tunnel**

user-defined-protocol command to define characteristic information about the Layer 2 protocol.

Precautions

When Layer 2 protocol transparent transmission is configured, the destination MAC address of user-defined protocol packets must be different from that of STP BPDUs, LACPDUs, LLDPDUs, and CDP packets, and the replaced multicast MAC address must be different from the used multicast MAC address.

Example

Define a Layer 2 protocol named **huawei**. Set the destination MAC address of its packets to 0180-c200-0020 and use multicast MAC address 0100-0ccd-eeee to replace the destination MAC address of its packets.

```
<Huawei> system-view
[Huawei] l2protocol-tunnel user-defined-protocol huawei protocol-mac 0180-c200-0020 group-mac
0100-0ccd-eeee
Info: Please make sure the input multicast MAC address doesn't conflict with other protocols.
```

Related Topics

6.10.1 l2protocol-tunnel

6.11 Transparent Bridging (TB) Configuration Commands

6.11.1 bpdu transmit enable

Function

The **bpdu transmit enable** command enables an interface of a bridge group or an interface connected to a VLL to transparently transmit BPDUs.

The **undo bpdu transmit enable** command cancels the configuration.

By default, an interface of a bridge group or an interface connected to a VLL is disabled from transparently transmitting BPDUs.

Format

bpdu transmit enable

undo bpdu transmit enable

Parameters

None

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When BPDUs are transmitted between interfaces of a bridge group or L2VPNs, to prevent BPDUs from being discarded, run the **bpdu transmit enable** command on the interface of the bridge group or interface connected to a VLL.

Prerequisites

The interface has been added to the bridge group or VLL.

Precautions

The command can only be used on Layer 3 interfaces.

Example

Enable transparent transmission of BPDUs of bridge group 1.

```
<Huawei> system-view
[Huawei] interface Ethernet 0/0/0
[Huawei-Ethernet0/0/0] undo portswitch
[Huawei-Ethernet0/0/0] bridge 1
[Huawei-Ethernet0/0/0] bpdu transmit enable
```

Enable transparent transmission of BPDUs of a VLL.

```
<Huawei> system-view
[Huawei] interface Vlanif 1
[Huawei-Vlanif1] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100 receive-vpn-label 100
[Huawei-Vlanif1] bpdu transmit enable
```

6.11.2 bridge

Function

The **bridge** command creates a bridge group and enter the bridge group view. If a bridge group has been created, you can directly enter the bridge group view.

The **undo bridge** command deletes a bridge group.

By default, no bridge group is created in the system.

Format

bridge *bridge-id*

undo bridge *bridge-id*

Parameters

Parameter	Description	Value
bridge-id	Specifies the number of a bridge group.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Bridges transmit data at the link layer.

On small-scale networks (especially on distributed networks), bridges can reduce costs for network maintenance. Bridges allow end users to construct large-scale networks and expand the network scale without any special configurations.

Transparent bridges connect different LANs. The configuration of transparent bridges is easy and will not affect the existing LAN. You must create a bridge group by using the **bridge** command before adding interfaces to it.

Precautions

After a bridge group has been created by using the **bridge** command adds an interface to the bridge group.

- The **undo bridge** *bridge-id* command is used to delete a bridge group. If the bridge group to be deleted has a Bridge-if interface, you need to delete the Bridge-if interface first. Otherwise, the **undo bridge** *bridge-id* command will not take effect.
- After a bridge group has been deleted by using the **undo bridge** *bridge-id* command, the system deletes attribute configurations and static MAC entries of the bridge group, and removes member interfaces from the bridge group.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The same bridge group number can be used by multiple devices.

Example

Create bridge group 3.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3]
```

Related Topics

6.11.8 display bridge information

6.11.3 bridge dhcp terminate enable

Function

The **bridge dhcp terminate enable** command terminates DHCP packets on the interface of a bridge group.

The **undo bridge dhcp terminate enable** command cancels the configuration.

By default, the function of terminating DHCP packets on the interface of a bridge group is disabled.

Format

bridge dhcp terminate enable

undo bridge dhcp terminate enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

- To prevent the interface of a bridge group from transparently transmitting DHCP packets that are identified to the bridge, run the **bridge dhcp terminate enable** command to terminate DHCP packets on the interface of the bridge group.
- To enable the interface of a bridge group to transparently transmit DHCP packets that are identified to the bridge, run the **undo bridge dhcp terminate enable** command to disable the DHCP packet termination function.

 Copyright © Huawei Technologies Co., Ltd.

Example

Terminate DHCP packets on the interface of a bridge group.

```
<Huawei> system-view
[Huawei] bridge dhcp terminate enable
```

Related Topics

6.11.2 bridge

6.11.4 bridge virtual-access forward-broadcast disable

Function

The **bridge virtual-access forward-broadcast disable** command disables a virtual access (VA) interface from forwarding broadcast packets.

The **undo bridge virtual-access forward-broadcast disable** command enables a VA interface to forward broadcast packets.

By default, a VA interface is enabled to forward broadcast packets.

Format

bridge virtual-access forward-broadcast disable

undo bridge virtual-access forward-broadcast disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple L2TP users on the LNS join the same network bridge and the LAC sends packets to the LNS, if the LAC cannot obtain the destination address, the LAC sends broadcast packets to all users of the network bridge. Much network bandwidth is occupied, the burden of the LNS is increased, and normal packets are discarded.

To address the issues, run the **bridge virtual-access forward-broadcast disable** command on the LNS to disable the VA interface from forwarding broadcast packets.

Precautions

After a VA interface is disabled from forwarding broadcast packets, branch users may fail to communicate.

Example

Disable a VA interface from forwarding broadcast packets.

```
<Huawei> system-view
[Huawei] bridge virtual-access forward-broadcast disable
```

6.11.5 bridge vlan-transmit enable

Function

The **bridge vlan-transmit enable** command enables an interface in a bridge group to transparently transmit VLAN IDs.

The **undo bridge vlan-transmit enable** command disables an interface in a bridge group from transparently transmitting VLAN IDs.

By default, an interface in a bridge group is disabled from transparently transmitting VLAN IDs.

Format

bridge vlan-transmit enable

undo bridge vlan-transmit enable

Parameters

None

Views

ATM interface view, GE interface view, XGE interface view, PON interface view, Dialer interface view, MP-Group interface view, Serial interface view, Ethernet interface view (WAN side)

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario where transparent bridges connect different LANs, and VLAN IDs of packets are exchanged between LANs to isolate VLANs and enable communication within a VLAN, you can enable an interface in a bridge group to transparently transmit VLAN IDs. This prevents VLAN IDs to be discarded in the case that VLAN ID transmission is not supported.

After being enabled to transparently transmit VLAN IDs, the interface in a bridge group does not perform any operation on VLAN IDs in packets.

Prerequisites

Before enabling an interface to transparently transmit VLAN IDs, ensure that the interface has been added to a bridge group.

Precautions

If a bridge group is deleted or the interface enabled to transparently transmit VLAN IDs is removed from the bridge group, the system will delete the configuration of this command automatically.

VLANIF interfaces do not support VLAN ID transparent transmission.

Example

Enable a specified interface in bridge group 3 to transparently transmit VLAN IDs.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] bridge 3
[Huawei-GigabitEthernet1/0/0] bridge vlan-transmit enable
```

Related Topics

6.11.2 bridge

6.11.6 bridge (interface view)

Function

The **bridge** command adds an interface to a bridge group.

The **undo bridge** command removes an interface from a bridge group.

By default, an interface is not added to any bridge group.

Format

bridge *bridge-id*

undo bridge

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bridge-id	Specifies the number of the bridge group to which an interface is added.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a transparent bridge connects different LANs, you can run the **bridge** command to add an interface to a bridge group.

Prerequisites

The **bridge** command has been used to create a bridge group.

Precautions

After the **bridge (interface view)** command is run, an interface is added to a bridge group; after the **undo bridge (interface view)** command is run, an interface is removed from a bridge group.

- The number of interfaces that can be added to a bridge group depends on device models:
  - AR100&AR120& AR150& AR160& AR200& AR1200 series: 20
  - AR2200 and AR3600 series: 128

  Interfaces of different types can be added to the same bridge group, but Layer 2 interfaces cannot be added to a bridge group.
- VLANIF interfaces in a super VLAN cannot be added to a bridge group.

 Copyright © Huawei Technologies Co., Ltd.

- QinQ termination Ethernet sub-interfaces, QinQ termination XGE sub-interfaces and QinQ termination GE sub-interfaces do not support the transparent bridge function.

Example

Create bridge group 2 and add a specified interface to bridge group 2.

```
<Huawei> system-view
[Huawei] bridge 2
[Huawei-bridge2] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] bridge 2
```

Create bridge group 3 and add a specified sub-interface to bridge group 3.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3] quit
[Huawei] interface gigabitethernet 2/0/0.1
[Huawei-GigabitEthernet2/0/0.1] bridge 3
```

Related Topics

6.11.8 display bridge information

6.11.7 bridging disable

Function

The **bridging disable** command disables a bridge group from bridging protocol packets.

The **undo bridging disable** command enables a bridge group to bridge protocol packets.

By default, a bridge group is disabled from bridging all protocol packets.

Format

bridging { **ip** | **others** } **disable**

undo bridging { **ip** | **others** } **disable**

Parameters

Parameter	Description	Value
ip	Enables a bridge group to bridge or disables a bridge group from bridging IP packets.	-
others	Enables a bridge group to bridge or disables a bridge group from bridging non-IP packets.	-

Views

Bridge group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A bridge group is enabled to bridge all protocol packets by default. The **bridging disable** command can be used to disable a bridge group from bridging packets of a specified protocol, which can thus close upper layer applications, such as ARP.

Prerequisites

Before disabling a bridge group from bridging packets of a specified protocol, ensure that the bridge has been created.

Configuration Impact

You can run the **bridging disable** command to disable a bridge group from bridging function packets of a specified protocol.

Example

Disable bridge group 3 from bridging IP packets.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3] bridging ip disable
```

Related Topics

6.11.8 display bridge information

6.11.8 display bridge information

Function

The **display bridge information** command displays information about all bridge groups or a specified bridge group.

Format

display bridge [*bridge-id*] **information**

Parameters

Parameter	Description	Value
bridge-id	Specifies the number of a bridge group.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bridge information** command can display information about a specified bridge group, including the management status, types of protocols for which the bridging function is enabled, whether the IP routing function is enabled, and whether the MAC address learning function is enabled.

The **display bridge information** command can display the configurations of the bridge-related command.

Precautions

When using this command, note the following points:

- If *bridge-id* is not specified, the command output displays the configurations of all bridge groups.
- If *bridge-id* is specified, the command output displays the configurations of a specified bridge group.

Example

Display information about all bridge groups.

```
<Huawei> display bridge information

Bridge 1 :
```

```
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 6 interface(s) in the bridge
    Ethernet0/0/1 : Down
    Ethernet1/0/0 : Down
    Serial1/0/0 : Down
    Vlanif1 : Down
    Vlanif2 : Down
    Vlanif10 : Down
Bridge 2 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : IP
    MAC learning : Enable
  interface :total 1 interface(s) in the bridge
    MFR0/0/2 : Down
```

Display information about bridge group 1.

```
<Huawei> display bridge 1 information

Bridge 1 :
    Status       : Undo Shutdown
    Bridging     : IP, Others
    Routing      : -
    MAC learning : Enable
  interface :total 6 interface(s) in the bridge
    Ethernet0/0/1 : Down
    Ethernet1/0/0 : Down
    Serial1/0/0 : Down
    Vlanif1 : Down
    Vlanif2 : Down
    Vlanif10 : Down
```

Table 6-63 Description of the **display bridge information** command output

Item	Description
Bridge 1	Displays information about a bridge group. ● If *bridge-id* is not specified, the command output displays information about all bridge groups. ● If the specified interface is added to a bridge group, the command output displays the number of the bridge group. ● If the specified bridge group number does not exist or the specified interface does not belong to any bridge group, no information is displayed.
Status	Specifies the management status of the bridge group, which can be either of the following: ● Shutdown ● Undo Shutdown
Bridging	Specifies types of protocols (IP and Others) for which the bridging function can be enabled. "-" indicates that the bridging function is disabled for both protocol types.

Item	Description
Routing	Indicates whether the IP routing function can be enabled in a bridge group. ● IP: indicates that the IP routing function can be enabled in a bridge group. ● -: indicates that the IP routing function cannot be enabled in a bridge group.
MAC learning	Indicates whether the MAC address learning function can be enabled in a bridge group. ● Enable ● Disable
interface	Specifies the interface added to a bridge group.

Related Topics

6.11.2 bridge

6.11.9 display bridge traffic

Function

The **display bridge traffic** command displays traffic statistics about interfaces in a bridge group.

Format

display bridge traffic [**bridge** *bridge-id* | **interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bridge *bridge-id*	Specifies the number of a bridge group.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.
interface-type	Specifies the interface type. If the interface type is not specified, traffic statistics about all interfaces in a bridge group are displayed.	-
interface-number	Specifies the number of an interface. If the interface number is not specified, traffic statistics about interfaces of a specified type in a bridge group are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bridge traffic** command can display traffic statistics of an interface or all interfaces in a bridge group, or about all interfaces in all bridge groups.

 Copyright © Huawei Technologies Co., Ltd.

If no parameter is specified in this command, the command output displays traffic statistics on all interfaces in all bridge groups.

Example

Display traffic statistics on all interfaces in all bridge groups.

```
<Huawei> display bridge traffic

Bridge 1 :
 Input  :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
 Output :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
Bridge 2 :
 Input  :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
 Output :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
```

Display traffic statistics on all interfaces in a specified bridge group.

```
<Huawei> display bridge traffic bridge 1

Bridge 1 :
 Input  :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
 Output :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
```

Displays traffic statistics on a specified interface in a bridge group.

```
<Huawei> display bridge traffic interface ethernet 1/0/0

Bridge 1 :
 Input  :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
 Output :
        0 total, 0 bpdu, 0 single,
        0 multi, 0 broadcast,
```

Table 6-64 Description of the **display bridge traffic** command output

Item	Description
Bridge 1	Displays information about the bridge group. ● If no bridge group number is specified, the command output displays information about all bridges group. ● If the specified interface belongs to a bridge group, the command output displays the number of the bridge group. ● If the specified bridge group number does not exist or the specified interface does not belong to any bridge group, no information is displayed.

Item	Description
Input	Specifies statistics about incoming packets, including the total number of incoming packets, transparently-transmitted packets, unicast packets, multicast packets, and broadcast packets.
Output	Specifies statistics about outgoing packets, including the total number of outgoing packets, transparently-transmitted packets, unicast packets, multicast packets, and broadcast packets.

Related Topics

6.11.2 bridge

6.11.10 display interface bridge-if

Function

The **display interface bridge-if** command displays the status of and statistics about Bridge-if interfaces.

Format

display interface bridge-if [*bridge-id* | **main**]

Parameters

Parameter	Description	Value
bridge-id	Displays status and statistics about a bridge-if interface with an interface number. If no Bridge-if interface number is specified, status and statistics about all Bridge-if interfaces are displayed.	The value is an integer. • On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. • On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. • On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. • On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
main	Displays status and traffic statistics about a bridge-if interface. A bridge-if interface has no sub-interfaces. Status and traffic statistics about a bridge-if interface are displayed whether you specify the **main** parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you need to monitor the status of a Bridge-if interface or locate the fault on a Bridge-if interface, you can run the **display interface bridge-if** command to view the status and traffic statistics of the interface. Based on the command output, you can collect traffic statistics and troubleshoot the interface.

Prerequisites

The Bridge-if interface specified in this command must be an existing one; otherwise, the system prompts an error.

Example

Display information about a specified Bridge-if interface.

```
<Huawei> display interface bridge-if 1
Bridge-if1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Bridge-if1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 1.1.1.3/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 00e0-1419-3000
Physical is BRIDGE-IF
Current system time: 2010-10-13 08:43:04-08:00
   Last 300 seconds input rate 0 bits/sec, 0 packets/sec
   Last 300 seconds output rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds input rate 0 bits/sec, 0 packets/sec
   Realtime 2 seconds output rate 0 bits/sec, 0 packets/sec
   Input: 8 packets,0 bytes,
         6 unicast,2 broadcast,0 multicast
   Output:9 packets,0 bytes,
         7 unicast,2 broadcast,0 multicast
```

```
Input bandwidth utilization  :    0%
Output bandwidth utilization :    0%
```

Table 6-65 Description of the display interface bridge-if command output

Item	Description
Bridge-if1 current state	Specifies the current physical status of the Bridge-if interface. ● UP: indicates that the physical connection of the interface is normal. ● DOWN: indicates that the physical connection of the interface is abnormal. ● Administratively down: This state is displayed after the network administrator has run the **shutdown** command on the interface.
Line protocol current state	Specifies the link layer protocol status of the Bridge-if interface. ● UP: indicates that the link layer protocol of the interface is Up. ● DOWN: indicates that the link layer protocol of the interface is Down or no IP address is assigned to the interface.
Description	Indicates the description of an interface. The information allows users to know about functions of the interface and is used to identify the current interface. The **description** command is used to configure or modify the description of an interface.
Route Port	Indicates the Layer 3 interface.
The Maximum Transmit Unit is	Indicates the MTU of the interface. By default, the MTU is 1500 bytes. Packets larger than the MTU are fragmented before being sent. If fragmentation is disabled, packets will be discarded. The **mtu** command is used to configure or modify the MTU of an interface.
Internet Address is	Indicates the IP address of an interface. If no IP address is configured on the current interface, the system displays "Internet protocol processing: disabled".

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IP Sending Frames' Format is	Format of the Ethernet frame sent by the Bridge-if interface. The default frame format is PKTFMT_ETHNT_2. When receiving frames, the Ethernet protocol can identify the following formats: ● PKTFMT_ETHNT_2 ● Ethernet_SNAP ● 802.2 ● 802.3
Hardware address is	MAC address of the Bridge-if interface.
Physical is	Specifies the interface type.
Current system time	Specifies the current time of the system. If the time zone is configured and the daylight saving time is used, the system time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Last 300 seconds input rate Last 300 seconds output rate	Indicates the rates at which bytes and packets are sent and received by the interface in the last 300 seconds. Each time this command is run, the value of this field is re-counted. The rates at which bytes or packets are sent 300s before this command is run is displayed, in the number of bytes or packets per 300s. The **set flow-stat interval** command is used to configure or modify the interval at which traffic statistics are collected.
Realtime 2 seconds input rate Realtime 2 seconds output rate	Indicates the real-time rates at which packets are sent and received within 2 seconds. It refers to the interval between two **display interface** commands that are run on the same interface. The maximum value is the statistical interval displayed in the previous piece of information. **NOTE** This field is displayed only when you view statistics about a logical interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input	Total number of packets and bytes received on the interface ● packets: indicates the total number of packets. ● bytes: indicates the total number of bytes. ● unicast: indicates the number of unicast packets. ● broadcast: indicates the number of broadcast packets. ● multicast: indicates the number of multicast packets. **NOTE** Total number of packets received on the interface = Number of unicast packets + Number of broadcast packets + Number of multicast packets.
Output	Total number of packets and bytes sent by the interface ● packets: indicates the total number of packets. ● bytes: indicates the total number of bytes. ● unicast: indicates the number of unicast packets. ● broadcast: indicates the number of broadcast packets. ● multicast: indicates the number of multicast packets. **NOTE** Total number of packets sent by the interface = Number of unicast packets + Number of broadcast packets + Number of multicast packets.
Input bandwidth utilization	Indicates the percentage of the rate at which packets are received to the total bandwidth.
Output bandwidth utilization	Indicates the percentage of the rate at which packets are sent to the total bandwidth.

Related Topics

6.11.14 interface bridge-if

6.11.11 display mac-address aging-time bridge

Function

The **display mac-address aging-time bridge** command displays the aging time for dynamic MAC address entries in the bridge group.

Format

display mac-address aging-time bridge

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the bridge group is configured on a device, to view the aging time for dynamic MAC address entries in the bridge group, run the **display mac-address aging-time bridge** command all view. To set the aging time, run the **mac-address aging-time** command in the system view. The command output helps verify the configuration and analyze faults.

Precautions

If a MAC address entry does not age, the aging time in the command output is 0s.

Example

Display the aging time of dynamic MAC address entries.

```
<Huawei> display mac-address aging-time bridge
  Aging time: 300 seconds
```

Table 6-66 Description of the **display mac-address aging-time bridge** command output

Item	Description
Aging time:	Aging time (in seconds) for dynamic MAC entries in the bridge group, in seconds. The aging time can be configured using the **mac-address aging-time bridge** command in the system view.

6.11.12 display mac-address bridge

Function

The **display mac-address bridge** command displays MAC address entries of a bridge group.

Format

display mac-address [*mac-address* | *interface-type interface-number*] **bridge** *bridge-id* [**verbose**]

display mac-address [**static** | **dynamic**] *interface-type interface-number* **bridge** *bridge-id* [**verbose**]

display mac-address [**static** | **dynamic** | **blackhole**] **bridge** *bridge-id*

Parameters

Parameter	Description	Value
mac-address	Displays the MAC address entries of a bridge group with a specified unicast MAC address.	The value is in the format of H-H-H. H is a hexadecimal number that contains four digits, such as 00e0 and fc01. A MAC address cannot be FFFF-FFFF-FFFF or any multicast MAC addresses. -
blackhole	Displays the MAC address blackhole entries of a bridge group. Specifies a blackhole entry, which will not be aged. After being configured and saved, the entries are not lost after the system is reset or the I/O interface board is hot swapped.	-
static	Displays the MAC address static entries of a bridge group. Specifies a static entry, which will not be aged. After being configured and saved, the entries are not lost after the reset or hot plug of the I/O interface board.	-
dynamic	Displays the MAC address dynamic entries of a bridge group. Specifies a dynamic entry, which will be aged. Dynamic entries will lose after the system is reset or the I/O interface board is hot swapped.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bridge *bridge-id*	Displays the MAC address entries of a bridge group with a specified bridge ID.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.
verbose	Displays the detailed MAC address entries of a bridge group.	-
interface-type interface-number	Displays the MAC address entries of a bridge group with a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display mac-address bridge** command can display the MAC address entry of a specific bridge group. You can display MAC address entries about a MAC address or MAC address type (**blackhole**, **static**, and **dynamic**).

Example

Display static MAC entries of bridge group 2.

```
<Huawei> display mac-address 0001-0001-0001 bridge 2
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge/VSI/BD          Learned-From            Type
--------------------------------------------------------------------------------
0001-0001-0001       -/2              Eth0/0/1                  static
```

```
--------------------------------------------------------------------------------
Total items displayed = 1
```

Display the details of the MAC address entries with a specified interface and a bridge id.

```
[Huawei] display mac-address Ethernet 0/0/1 bridge 10 verbose
--------------------------------------------------------------------------------
MAC Address : 0001-0002-0002            VLAN/Bridge/VSI/BD :    -/10
Learned-From: Eth0/0/1                  Type : static

--------------------------------------------------------------------------------
Total items displayed = 1
```

Display the static MAC address entries on a specified interface and a specified Bridge.

```
[Huawei] display mac-address static Ethernet 0/0/1 bridge 10 verbose
--------------------------------------------------------------------------------
MAC Address : 0001-0002-0002            VLAN/Bridge/VSI/BD :    -/10
Learned-From: Eth0/0/1                  Type : static

--------------------------------------------------------------------------------
Total items displayed = 1
```

Table 6-67 Description of the **display mac-address** Command Output

Item	Description
MAC Address	Specifies a MAC address.
VLAN/ Bridge/VSI/BD	Specifies the VLAN, Bridge, BD or Virtual Switch Instance (VSI) to which the outbound interface belongs.
Learned-From	● static: Indicates an interface on which the MAC addresses of the static type are configured. ● dynamic: Indicates an interface from which the MAC addresses of the dynamic type are learned. ● blackhole: The value is always displayed as "-"

Item	Description
Type	Specifies a type of MAC addresses entry. • **static**: indicates static MAC address entries, which are configured by users and delivered to I/O interface boards. Static MAC address entries will not age. In addition, they will not lose even if the system is reset or the I/O interface board is hot swapped. • **blackhole**: indicates blackhole MAC address entries, which are configured by users and delivered to I/O interface boards. Blackhole entries are used to discard frames carrying specified destination MAC addresses. Blackhole MAC address entries will not age. In addition, they will not lose even if the system is reset or the I/O interface board is hot swapped. • **dynamic**: indicates dynamic MAC address entries, which are learned and stored by I/O interface boards. Dynamic MAC address entries will age. They will be removed from the forwarding table if the system is reset or the I/O interface board is hot swapped.
Total items displayed	Specifies the total number of MAC address entries that can be displayed.

Related Topics

6.11.18 mac-address static bridge

6.11.13 fr map bridge

Function

The **fr map bridge** command adds a bridge mapping entry on a frame relay (FR) interface.

The **undo fr map bridge** command deletes a bridge mapping entry from an FR interface.

By default, no bridge mapping entry is configured.

Format

fr map bridge *dlci-number* **broadcast**

undo fr map bridge *dlci-number* **broadcast**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dlci-number	Specifies the Data Link Connection Identifier (DCLI) of a local virtual circuit.	The value is an integer ranging from 16 to 1022.
broadcast	Indicates whether the bridge mapping entry can be used to send broadcast packets.	-

Views

Frame relay serial interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **fr map bridge** *dlci-number* **broadcast** command can be used to enable an interface added to a bridge group to send broadcast packets based on the bridge mapping entry.

Prerequisites

Run the **bridge** *bridge-id* command in the interface view to add the interface to a bridge group.

Precautions

If the DLCI specified in the **fr map bridge** *dlci-number* **broadcast** command does not exist, the system will create a DLCI as specified. The created DLCI will be deleted when the **undo fr map bridge** *dlci-number* **broadcast** command is run.

Each FR interface can be configured with only one bridge mapping entry.

If a bridge is deleted or the FR interface quits the bridge group, the corresponding bridge mapping entry will be deleted from the FR interface.

Example

Configure a bridge mapping entry with the DLCI being 50 on MFR0/0/0.

```
<Huawei> system-view
[Huawei] interface mfr 0/0/0
[Huawei-MFR0/0/0] bridge 5
[Huawei-MFR0/0/0] fr map bridge 50 broadcast
```

 Copyright © Huawei Technologies Co., Ltd.

6.11.14 interface bridge-if

Function

The **interface bridge-if** command creates a Bridge-if interface and enter the Bridge-if interface view.

The **undo interface bridge-if** command deletes a Bridge-if interface.

By default, no Bridge-if interface is created in a bridge group.

Format

interface bridge-if *bridge-id*

undo interface bridge-if *bridge-id*

Parameters

Parameter	Description	Value
bridge-id	Specifies the number of a bridge group.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, Local Area Network (LAN) users that need to be interconnected belong to the same network segment or aggregated network segment. A bridge connects multiple LANs at the link layer. If users in a bridge group need to access another network, link-layer bridging cannot meet the requirement. Transparent Bridging integrated with routing can meet the requirement.

 Copyright © Huawei Technologies Co., Ltd.

Integrated routing has the ability to route between different networks by using Bridge-if interfaces.

After configuring a Bridge-if interface, you must run the **routing ip** command on the bridge group to enable the IP packet routing function.

Prerequisites

A bridge group has been configured before you create a Bridge-if interface in the bridge group.

Precautions

A bridge group where a Bridge-if interface has been created can be deleted only after the created Bridge-if interface is deleted.

- A Bridge-if interface uniquely identifies a bridge group and a bridge group can be configured with only one Bridge-if interface.
- Currently, a Bridge-if interface can be configured with an MTU, descriptions, an IP address, a MAC address, static routes, Domain Name Service (DNS), and IP security (IPSec).

Example

Create a Bridge-if interface.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3] quit
[Huawei] interface bridge-if 3
[Huawei-Bridge-if3]
```

Related Topics

6.11.2 bridge

6.11.22 routing ip

6.11.15 mac-address aging-time bridge

Function

The **mac-address aging-time bridge** command sets the aging time for MAC address entries of bridge groups.

The **undo mac-address aging-time bridge** command restores the default aging time for MAC address entries of bridge groups.

By default, the aging time for MAC address entries of bridge groups is 300s.

Format

mac-address aging-time *seconds* **bridge**

undo mac-address aging-time bridge

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
seconds	Specifies the aging time for MAC address entries of bridge groups.	The value is an integer and its range depends on product models. ● On the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value can be 0 or in the range of 60 to 3825. ● On the AR2220, AR2220E, AR2240C, AR2240 and AR3200&AR3600 series, the value can be 0 or in the range of 60 to 1000000. **NOTE** The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards, the value can be 0 or in the range of 60 to 3825. The value is expressed in seconds. The default value is 300. The value 0 indicates that dynamic MAC address entries will not be aged out.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mac-address aging-time bridge** command can be used to set the aging time for MAC address entries of bridge groups.

After the aging time has been set, only dynamic MAC address entries will age, and non-dynamic MAC address entries will not. If the aging time is set to 0, none of dynamic MAC address entries will age.

Configuration Impact

The configured aging time takes effect on the dynamic MAC address entries of all bridge groups that are configured on a device. After the **mac-address aging-time bridge** command is run, the dynamic MAC address entries learned by bridge groups will age when the configured aging time expires.

Example

Set the aging time for MAC address entries of bridge groups to 500s.

```
<Huawei> system-view
```

```
[Huawei] mac-address aging-time 500 bridge
```

Related Topics

6.11.12 display mac-address bridge

6.11.16 mac-address blackhole bridge

Function

The **mac-address blackhole bridge** command configures a blackhole MAC address entry for a bridge group.

The **undo mac-address blackhole bridge** command deletes the blackhole MAC address entry that is configured for a bridge group.

By default, no blackhole MAC address entry is configured for any bridge group.

Format

mac-address blackhole *mac-address* **bridge** *bridge-id*

undo mac-address blackhole [*mac-address*] **bridge** *bridge-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a unicast MAC address for a bridge group.	The value is in the format of H-H-H. H is a hexadecimal number that contains four digits, such as 00e0 and fc01. A MAC address cannot be FFFF-FFFF-FFFF or any multicast MAC addresses.
bridge *bridge-id*	Specifies the number of a bridge group.	The value is an integer. • On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. • On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. • On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. • On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security on a stable network, the **mac-address blackhole bridge** command can be run to configure a blackhole MAC address entry for a bridge group. When configuring a blackhole MAC address entry, no outbound interface needs to be specified.

Precautions

If the source or destination MAC address of a packet is a blackhole MAC address, the device discards the packet.

A blackhole MAC address entry configured using the **mac-address blackhole bridge** command is not associated with blackhole entries in a VLAN.

Example

Configure a blackhole MAC address entry for a bridge group.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] bridge 3
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] mac-address blackhole 0002-0002-0002 bridge 3
```

Related Topics

6.11.12 display mac-address bridge

6.11.17 mac-address (Bridge-if interface view)

Function

The **mac-address** command configures a MAC address for the Bridge-if interface of the current bridge group.

The **undo mac-address** command deletes the MAC address that is configured for the Bridge-if interface of the current bridge group.

By default, the MAC address of the Bridge-if interface is the system MAC address.

Format

mac-address *mac-address*

undo mac-address

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address of a Bridge-if interface.	The MAC address is in the format of H-H-H. H is a hexadecimal number that contains four digits, such as 00e0 and fc01. A MAC address cannot be FFFF-FFFF-FFFF or any multicast MAC addresses.

Views

Bridge-if interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MAC address of a Bridge-if interface is the system MAC address, and may conflict with the MAC address of another interface (a physical or logical interface). If the MAC address of the Bridge-if interface conflicts with that of a member interface in the bridge group, Layer 3 traffic forwarding on the Bridge-if interface may fail.

In this case, you must run the **mac-address** command to reconfigure a MAC address for the Bridge-if interface.

Configuration Impact

After the MAC address of the Bridge-if interface is changed, the device sends gratuitous ARP packets to the remote device so that the remote device can refresh its ARP entries.

Example

Configure a MAC address for Bridge-if 1.

```
<Huawei> system-view
[Huawei] interface bridge-if 1
[Huawei-Bridge-if1] mac-address 0001-2345-abcd
```

Related Topics

6.11.10 display interface bridge-if

6.11.18 mac-address static bridge

Function

The **mac-address static bridge** command configures a static MAC address entry for a bridge group. The outbound interface of the configured static entry belongs to a specific bridge group.

The **undo mac-address bridge** command deletes the static MAC address entry that is configured for a bridge group.

By default, no static MAC address entry is configured for a bridge group.

Format

mac-address static *mac-address interface-type interface-number* [**vlan** *vlan-id*] **bridge** *bridge-id*

undo mac-address static *mac-address interface-type interface-number* **vlan** *vlan-id* **bridge** *bridge-id*

undo mac-address [**static** | **dynamic** | **all**] [*interface-type interface-number*] [**vlan** *vlan-id* | **bridge** *bridge-id*]

undo mac-address *mac-address* **bridge** *bridge-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a unicast MAC address for a bridge group.	The value is in the format of H-H-H. H is a hexadecimal number that contains four digits, such as 00e0 and fc01. A MAC address cannot be FFFF-FFFF-FFFF or any multicast MAC addresses.
interface-type interface-number	Specifies the type and number of an interface.	-
vlan *vlan-id*	indicates the VLAN ID.	The value can be 1 or 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bridge *bridge-id*	Specifies the number of a bridge group.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.
all	Indicates all MAC address entries.	-
dynamic	Specifies a dynamic entry, which will be aged. Dynamic entries will be lost after the system is reset or the I/O interface board is hot swapped.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security on a stable network, the **mac-address static bridge** command can be run to configure a static MAC address entry for a bridge group.

Prerequisites

Interfaces must have been added to the bridge group. The interface can be a Layer 3 interface or a Layer 2 interface that has been added to a VLAN (and the VLANIF interface has been added to the bridge group).

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After a static MAC address entry has been configured for a bridge group, the bridge group forwards packets based on the configured static MAC address entry.

Example

Configure a static MAC address entry for a bridge group.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] bridge 3
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] mac-address static 0001-0001-0001 gigabitethernet 1/0/0 bridge 3
```

Related Topics

6.11.12 display mac-address bridge

6.11.19 map bridge broadcast

Function

The **map bridge broadcast** command configures a PVC to send and receive bridge packets.

The **undo map bridge broadcast** command prohibits a PVC from sending and receiving bridge packets.

By default, a PVC on an ATM interface is not configured to send and receive bridge packets.

Format

map bridge broadcast

undo map bridge broadcast

Parameters

None

Views

ATM-PVC view, IMA-PVC view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two Ethernet networks communicate with each other by using ATM links or IMA group links, the Ethernet frames need to be transmitted by means

transparent bridging (TB). The **map bridge broadcast** command can be run to allow a PVC to send and receive bridge packets.

Prerequisites

Interfaces have been added to a bridge group.

Precautions

On an ATM interface, only one PVC is allowed to send and receive bridge packets.

If a PVC is deleted, the configuration (sending and receiving bridge packets) of the PVC will also be automatically deleted.

Example

Configure PVC 1/102 to send and receive bridge packets.

```
<Huawei> system-view
[Huawei] interface atm 1/0/1
[Huawei-Atm1/0/1] bridge 2
[Huawei-Atm1/0/1] pvc 1/102
[Huawei-atm-pvc-Atm1/0/1-1/102] map bridge broadcast
```

6.11.20 reset bridge statistics

Function

The **reset bridge statistics** command clears the traffic statistics in a bridge group.

Format

reset bridge *bridge-id* **statistics**

Parameters

Parameter	Description	Value
bridge-id	Specifies the number of a bridge group.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **reset bridge statistics** command can be used to clear the traffic statistics in the current bridge group.

Precautions

After the **reset bridge statistics** command is run, the traffic statistics in a bridge group will be cleared.

The traffic statistics cannot be restored after being cleared. Exercise caution when running the **reset bridge statistics** command.

Example

Clear the traffic statistics in bridge group 10.

```
<Huawei> system-view
[Huawei] bridge 10
[Huawei-bridge10] quit
[Huawei] quit
<Huawei> reset bridge 10 statistics
```

Related Topics

6.11.2 bridge

6.11.21 reset counters interface bridge-if

Function

The **reset counters interface bridge-if** command clears the traffic statistics on a Bridge-if interface.

Format

reset counters interface bridge-if [*bridge-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bridge-id	Specifies the number of a bridge group.	The value is an integer. • On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. • On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. • On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. • On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To locate faults in a bridge group, the **reset counters interface bridge-if** command can be used to clear the original traffic statistics.

Precautions

After the **reset counters interface bridge-if** command is run, the traffic statistics on the Bridge-if interface of a bridge group will be cleared.

The traffic statistics cannot be restored after being cleared. Exercise caution when running the **reset counters interface bridge-if** command.

Example

Clear the traffic statistics on Bridge-if 1.

```
<Huawei> reset counters interface bridge-if 1
```

Related Topics

6.11.10 display interface bridge-if

6.11.22 routing ip

Function

The **routing ip** command enables a bridge group to route IP protocol packets.

The **undo routing ip** command disables a bridge group from routing IP protocol packets.

By default, a bridge group is disabled from routing IP protocol packets.

Format

routing ip

undo routing ip

Parameters

None

Views

Bridge group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, LAN users who need to be interconnected belong to the same network segment or aggregated network. A bridge connects multiple LANs at the link layer. If users in a bridge group need to access another network, link-layer bridging cannot meet the requirement.

Integrated routing and bridging can meet the requirement. In the integrated bridging and routing function, a Bridge-if interface can be created and the **routing ip** command can be run on the bridge group to configure the IP protocol packet routing function. This allows interconnection between different network segments.

Prerequisites

The **bridge** command has been run to create bridge groups.

The IP routing function cannot be configured if any member interface in the bridge group is configured with an IP address. Before configuring the IP routing function, make sure that none of the member interfaces has an IP address.

Precautions

A Bridge-if interface can forward IP protocol packets only when the **routing ip** command is run.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the IP routing function for bridge group 3.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3] routing ip
```

Related Topics

6.11.8 display bridge information

6.11.14 interface bridge-if

6.11.23 shutdown (bridge view)

Function

The **shutdown** command shuts down a specified bridge group.

The **undo shutdown** command starts a specified bridge group.

By default, a bridge group is started.

Format

shutdown

undo shutdown

Parameters

None

Views

Bridge group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To shut down traffic in a bridge group, the **shutdown** command can be used to shut down the bridge group.

Precautions

After the **shutdown** command is run, the traffic in a specified bridge group is shut down. If the bridge group has a Bridge-if interface, running the **shutdown** command makes the physical status of the interface to go Down, disables the forwarding function of the Bridge-if interface, shuts down traffic in the bridge group, and interrupts services.

 Copyright © Huawei Technologies Co., Ltd.

The **shutdown** command is used to shut down only the traffic being forwarded in a bridge group and on the Bridge-if interface, and the member interfaces in the bridge group will not be shut down. If the member interfaces in the bridge group are also forwarding the traffic that does not belong to any bridge group, the traffic will not be affected by the **shutdown** command.

Example

Shut down bridge group 3.

```
<Huawei> system-view
[Huawei] bridge 3
[Huawei-bridge3] shutdown
```

Related Topics

6.11.8 display bridge information

6.11.24 undo mac-address bridge

Function

The **undo mac-address bridge** command deletes MAC address entries of a bridge group.

Format

undo mac-address *mac-address* **bridge** *bridge-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address.	The value is in the format of H-H-H. H is a 4-digit hexadecimal number, such as 00e0 and fc01. If an H contains less than four hexadecimal digits, the first digits contained in the H are 0s. For example, if an H is e0, it is equal to 00e0. FFFF-FFFF-FFFF is invalid for a MAC address.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bridge-id	Specifies the number of a bridge group.	The value is an integer. ● On the AR100&AR120&AR150&AR160, the value ranges from 1 to 16. ● On the AR200, AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, and AR2204, the value ranges from 1 to 16. ● On the AR2220, AR2220E, AR2240C, the value ranges from 1 to 255. ● On the AR2204XE, AR2204XE-DC, AR2240, AR3200 and AR3600 series, the value ranges from 1 to 1024.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo mac-address bridge** command can be used to delete MAC address entries of a bridge group.

Configuration Impact

Dynamic MAC address entries of a specified bridge group or an interface in a bridge group are deleted.

Precautions

MAC address entries of a bridge group cannot be restored after being deleted. Therefore, exercise caution when running the **undo mac-address bridge** command.

Example

Delete MAC address entries of a specified bridge group.

```
<Huawei> system-view
[Huawei] undo mac-address bridge 200
```

 Copyright © Huawei Technologies Co., Ltd.

7 WAN Commands

About This Chapter

7.1 DCC Configuration Commands
7.2 PPP Configuration Commands
7.3 MP Configuration Commands
7.4 PPPoE Commands
7.5 ATM Configuration Commands
7.6 Frame Relay Configuration Commands
7.7 HDLC Configuration Commands
7.8 LAPB Configuration Commands
7.9 X.25 Configuration Commands
7.10 IP-Trunk Commands
7.11 ISDN Configuration Commands
7.12 Modem Configuration Commands
7.13 RTC Configuration Commands
7.14 CESoP Configuration Commands

7.1 DCC Configuration Commands

7.1.1 dialer bundle

Function

The **dialer bundle** command specifies a dialer bundle for a dialer interface in the resource-shared dial control center (RS-DCC).

 Copyright © Huawei Technologies Co., Ltd.

The **undo dialer bundle** command deletes the dialer bundle from a dialer interface for in the RS-DCC.

By default, a dialer interface does not have a dialer bundle.

Format

dialer bundle *number*

undo dialer bundle

Parameters

Parameter	Description	Value
number	Specifies the dialer bundle used by a dialer interface.	The value is an integer, and the value range varies depending on the device model.

Views

Dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RS-DCC separates the logical dialing configurations from physical configurations on an interface, which cannot be supported by the circular DCC (C-DCC). In the RS-DCC, dialing parameters are configured on a dialer interface, and then the physical interface is dynamically associated with the dialer interface. The device uses the dialer bundle to bind a physical interface and a dialer interface.

The **dialer bundle** command specifies a dialer bundle for the dialer interface, and the **dialer bundle-member** command specifies physical interfaces in the dialer bundle. This command is used when you need to specify the physical interface that serves the dialer interface.

Prerequisites

The RS-DCC function has been enabled using the **dialer user** command before the **dialer bundle** command is run; otherwise, the **dialer bundle** command cannot take effect.

Precautions

Only one dialer bundle can be specified for a dialer interface.

Example

Specify dialer bundle 3 for dialer interface 1.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface dialer 1
[Huawei-Dialer1] dialer user userb
[Huawei-Dialer1] dialer bundle 3
```

Related Topics

7.1.2 dialer bundle-member

7.1.16 dialer user

7.1.2 dialer bundle-member

Function

Using the **dialer bundle-member** command, for details about how to configure the resource-shared DCC mode, you can add a physical interface to a dialer bundle.

Using the **undo dialer bundle-member** command, you can delete a physical interface from a dialer bundle.

By default, a physical interface does not belong to any dialer bundle.

Format

dialer bundle-member *number* [**priority** *priority*]

undo dialer bundle-member *number*

Parameters

Parameter	Description	Value
number	Specifies a dialer bundle for the physical interface.	The value is an integer, and the value range varies depending on the device model.
priority *priority*	Specifies the priority of the interface in the dialer bundle. A larger value indicates a higher priority. The interface with the highest priority is selected for dialing.	It is an integer that ranges from 1 to 255. The default value is 1.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenarios

After the RS-DCC is configured to implement dial-on-demand function, the system chooses physical interfaces from a dialer bundle according to the interface priorities to initiate calls; therefore, the dialer bundle must contain physical interfaces. The **dialer bundle-member** command adds physical interfaces to dialer bundles.

Precautions

- This command must be used in physical interface views. A physical interface can belong to multiple dialer bundles.
- If you run the **dialer bundle-member** command in the same interface view multiple times, the interface is added to multiple dialer bundles.

Example

Add interface Serial1/0/0:15 to dialer bundle 1 and dialer bundle 2, and set the interface priority to 50.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer bundle-member 1 priority 50
[Huawei-Serial1/0/0:15] dialer bundle-member 2 priority 50
```

Related Topics

7.1.1 dialer bundle

7.1.3 dialer circular-group

Function

Using the **dialer circular-group** command, you can add a physical interface to a dialer circular group.

Using the **undo dialer circular-group** command, you can remove a physical interface from the dialer circular group.

By default, a physical interface does not belong to any dialer circular group.

Format

dialer circular-group *number*

undo dialer circular-group

Parameters

Parameter	Description	Value
number	Specifies the dialer circular group number of the physical interface.	The dialer circular group number is set by the **interface dialer** command.

 Copyright © Huawei Technologies Co., Ltd.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dialer circular-group** command adds physical interfaces to a dialer circular group if multiple local interfaces need to call one or multiple remote ends in C-DCC. When a dialer interface needs to initiate a call, it chooses the physical interface with the highest priority (set by **dialer priority**) from the local circular group to initiate the call.

Prerequisites

The C-DCC function has been enabled by the **dialer enable-circular** command.

Follow-up Procedure

After this command is executed, use the **dialer priority** command to set the priorities for physical interfaces in the dialer circular group.

Precautions

- A physical interface belongs to only one dialer circular group, but a dialer circular group can contain multiple physical interfaces.
- If you run the **dialer circular-group** command multiple times in the same view, only the latest configuration takes effect.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Add Serial1/0/0:15 and Serial1/0/1:15 to dialer circular group 1.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer enable-circular
[Huawei-Serial1/0/0:15] dialer circular-group 1
[Huawei-Serial1/0/0:15] quit
[Huawei] interface serial 1/0/1:15
[Huawei-Serial1/0/1:15] dialer enable-circular
[Huawei-Serial1/0/1:15] dialer circular-group 1
```

Related Topics

7.1.5 dialer enable-circular

7.1.24 interface dialer

 Copyright © Huawei Technologies Co., Ltd.

7.1.4 dialer disconnect

Function

Using the **dialer disconnect** command, you can tear down a dial-up link temporarily.

Format

dialer disconnect [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the interface where the dial-up link needs to be torn down. If no interface is specified, the dial-up links on all interfaces are torn down.	The interface type can be ISDN BRI, ISDN PRI, cellular, or dialer.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To reduce network load or modify dial-up settings, you may need to tear down a dial-up link temporarily.

Precautions

This command only temporarily tears down dial-up links.

- If a disconnected link is enabled with the auto-dial function, it will be re-established when the dialer timer expires.
- If the link is not enabled with the auto-dial function, it will be re-established when transmitting data.

NOTE

After a dial-up link is torn down, all services on the link are interrupted; therefore, ensure that the link is not in use before you tear down the link.

Example

Tear down the dial-up link on interface Dialer0.

```
<Huawei> dialer disconnect interface dialer 0
```

7.1.5 dialer enable-circular

Function

Using the **dialer enable-circular** command, you can enable the circular DCC (C-DCC) function, the dialer number and IP address assigns automatically.

Using the **undo dialer enable-circular** command, you can disable the C-DCC function.

By default, the DCC function is disabled on an interface.

Format

dialer enable-circular

undo dialer enable-circular

Parameters

None

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the data to be transmitted is delay-insensitive, bursting, and has a small volume, the routers can use the dial control center (DCC) mode to reduce costs. DCC sets up a call connection only when there is data to be transmitted. DCC is a flexible, cost-effective, and efficient solution. After DCC is used on the routers connected with the PSTN, the routers set up a connection by dialing only when there is data to be transmitted between them. That is, they start the DCC process to transmit signal, and tear down the connection when no data is transmitted on the link.

DCC supports extensible dial-on-demand functions to meet various application requirements. It is applicable to the following major scenarios:

- DCC uses link backup to ensure normal communication. When communication fails because of a link error or other reasons, the backup link is used to continue the communication.

  Generally, a network of a different type is used for link backup. For example, an ISDN or a 3G network can be used for the link backup of an IP network. The device implements link backup by:

  – Using the interface backup mode

  - Using the dynamic routing standby mode
- DCC on a PPPoE/PPPoEoA client saves costs for users.

The device supports two DCC modes: Circular DCC (C-DCC) and resource-shared DCC (RS-DCC). The two modes are applicable to different scenarios. The two ends in communication can adopt different modes. You can choose the DCC modes according to the following table.

DCC Mode	Usage Scenario
C-DCC	C-DCC is applicable to the medium- or large-scale sites that have many physical links.
RS-DCC	RS-DCC is applicable to the small- or medium-scale sites that have a few physical links but many connected interfaces.

To enable the C-DCC function, use the **dialer enable-circular** command.

Precautions

If C-DCC is enabled on a physical interface, only this interface can initiate calls to remote ends. If C-DCC is enabled on a dialer interface, one interface or multiple interfaces can initiate calls to remote ends.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Run the **dialer enable-circular** command to view detailed information about the cellular interfaces, the device will set the DCC automatic dial-up interval to 10 seconds to prevent long automatic dial-up.

Example

Enable C-DCC on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer enable-circular
```

Related Topics

7.1.3 dialer circular-group

7.1.6 dialer number

Function

The **dialer number** command configures a dialer number for calling the remote end.

The **undo dialer number** command deletes a dialer number.

By default, no dialer number is configured.

Format

dialer number *dial-number* [**autodial**] [**exponent**]

undo dialer number *dial-number*

Parameters

Parameter	Description	Value
dial-number	Specifies the dialer number on an interface for calling the remote end.	It is a string of 1 to 30 case-sensitive characters without any space. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
autodial	Configures an interface to automatically initiate a call according to the configured dialer number. By default, the auto-dial interval is 300 seconds. You can run the **dialer timer autodial** command to set the auto-dial interval.	-

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a dialer interface of C-DCC dials only one destination, the dialer number needs to be configured.

In RS-DCC, if PPP encapsulation is enabled on the dialer interface, you can choose to use the **dialer number** command or not. If FR encapsulation is enabled on the dialer interface, you must use the **dialer number** command on the calling and called ends. The calling end then chooses an interface to initiate a call according to the configured dialer number, and the called end determines whether to respond to the call according to the dialer number.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

Before using the **dialer number** command, ensure that either of the following conditions is met:

- The **dialer user** command has been used to enable the RS-DCC function.
- The **dialer enable-circular** command has been used to enable the C-DCC function.
- The **dialer route** command is not used on the interface.

Precautions

In RS-DCC, the dialer interfaces of the calling end can have same dialer number, but the dialer interfaces of the called end cannot; otherwise, calls will be failed. In C-DCC, the dialer interfaces of both the calling end and called end can have same dialer number.

You can run the **dialer number** command multiple times on the same dialer interface to configure multiple dialer numbers for calling the remote end, except in the following situations:

- If **autodial** is specified in the **dialer number** command, you can run the **dialer number** command only once on the dialer interface to configure a dialer number for calling the remote end.

The ISDN leased line and dialing functions cannot be configured on the same interface.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in PRI mode.

Example

Set the dialer number on dialer interface 1 to 11111.

```
<Huawei> system-view
[Huawei] interface dialer 1
[Huawei-Dialer1] dialer user userb
[Huawei-Dialer1] dialer number 11111
```

Related Topics

7.1.5 dialer enable-circular

7.1.16 dialer user

7.1.7 dialer priority

Function

Using the **dialer priority** command, you can set the priorities of physical interfaces in a dialer circular group.

Using the **undo dialer priority** command, you can restore the default interface priorities.

By default, the priorities of physical interfaces in a dialer circular group are 1.

 Copyright © Huawei Technologies Co., Ltd.

Format

dialer priority *priority*

undo dialer priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the physical interface in the dialer circular group.	The value is an integer that ranges from 1 to 127. A larger value indicates a higher priority. The default value is 1.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A dialer circular group of C-DCC may contain multiple physical interfaces. When a dialer interface needs to initiate a call, it chooses the physical interface with the highest priority from the local circular group to initiate the call. The **dialer priority** command sets the interface priorities in the dialer circular group.

Prerequisites

The physical interface has been added to the dialer circular group by the **dialer circular-group** command.

Precautions

If you run the **dialer priority** command multiple times in the same view, only the latest configuration takes effect.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Set the priority of Serial1/0/0:15 in dialer circular group 0 to 5.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer circular-group 0
[Huawei-Serial1/0/0:15] dialer priority 5
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.1.3 dialer circular-group

7.1.8 dialer queue-length

Function

Using the **dialer queue-length** command, you can set the buffer queue length on a dial interface.

Using the **undo dialer queue-length** command, you can restore the default queue length.

By default, packets are not buffered on a dialer interface.

Format

dialer queue-length *packets*

undo dialer queue-length

Parameters

Parameter	Description	Value
packets	Indicates the number of packets allowed in the buffer queue.	The value is an integer that ranges from 1 to 100.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a dialer interface receives a packet but the call connection is not established, the dialer interface discards the packet. However, if a buffer queue is configured on the dialer interface, the dialer interface stores the packet in the buffer, and sends the packet after the call connection is established.

Precautions

- If you run the **dialer queue-length** command multiple times in the same view, only the latest configuration takes effect.
- If the buffer queue is long, the interface discards less packets, but a lot of system resources will be occupied. It is recommended that the queue length value be equal to or smaller than 20.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Set the buffer queue length on Dialer0 to 10.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] dialer queue-length 10
```

7.1.9 dialer route

Function

Using the **dialer route** command, you can configure a dialer interface to dial the specified destinations or to receive the calls from multiple remote ends.

Using the **undo dialer route** command, you can delete the settings.

By default, no dialer route exists in the system.

Format

Dialer interface view

dialer route ip *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string* [**autodial** | **interface** *interface-type interface-number*] *]

undo dialer route ip *next-hop-address* [**user** *hostname*] [*dial-string*] [**interface** *interface-type interface-number*]

ISDN BRI interface view, ISDN PRI interface view

dialer route ip *next-hop-address* [**user** *hostname* | **broadcast**] * [*dial-string* [**autodial**]]

undo dialer route ip *next-hop-address* [**user** *hostname*] [*dial-string*]

Parameters

Parameter	Description	Value
ip *next-hop-address*	Specifies the destination address, which is the address of the directly connected next hop.	The value is in dotted decimal notation.
user *hostname*	Specifies the remote end user name for incoming call authentication. If the user name is specified, you must configure PPP authentication.	The value is a string of 1 to 32 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
broadcast	Indicates that broadcast packets (such as OSPF and RIP packets) can be sent through the dialer route.	-
dial-string	Specifies the dialer number used to call the remote end. The dialer number is used only when the interface initiates a call to the remote end. **NOTE** This parameter must be specified to ensure that a call is successfully initiated to the remote end.	The value is a string of 1 to 30 case-sensitive characters. Spaces are allowed.
autodial	Indicates that the interface will automatically initiate calls. If this parameter is specified, the router dials using the local **dialer route** at an interval (the interval is set by **dialer timer autodial**).	-
interface *interface-type interface-number*	Specifies the physical interface where the dialer route is configured.	-

Views

ISDN BRI interface view, ISDN PRI interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a dialer interface in C-DCC needs to dial multiple destinations or receive calls from multiple remote ends, the data of the destinations or remote ends must be configured on the router by using the **dialer route** command.

Prerequisites

The C-DCC function has been enabled by the **dialer enable-circular** command.

Precautions

- The **dialer route** command cannot be used on the interface enabled with RS-DCC. That is, the **dialer route** and **dialer user** commands cannot be used on the same interface.
- When the link layer protocol of an interface is FR, you can only run the **dialer number** command but not the **dialer route** command to configure a dialer number.

 Copyright © Huawei Technologies Co., Ltd.

- When a dialup interface is a 3G cellular interface or the physical interface of a dialer interface is a 3G cellular interface, you can only use the **dialer number** command to configure a dialer number but cannot use the **dialer route** command. This is true for an Async interface.
- Multiple **dialer routes** can be configured on a dialer interface. A destination address can be specified in multiple dialer routes, and the dialer routes to the same destination are the backup of each other.

  NOTE

  This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in PRI mode.
- The **dialer route** command specifies only one destination. To specify multiple destinations for a dialer interface, run this command multiple times.

  NOTE

  When the **standby routing-group** command is used to specify a standby routing group for a dialer interface, the **dialer route** command specifies only one destination.

Example

Configure Serial1/0/0:15 to initiate a call to the remote end with the IP address 10.10.10.5 and user name user1, and set the dialer number to 12345678.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer enable-circular
[Huawei-Serial1/0/0:15] dialer route ip 10.10.10.5 user user1 12345678
```

Related Topics

7.1.5 dialer enable-circular

7.1.10 dialer timer autodial

7.1.10 dialer timer autodial

Function

Using the **dialer timer autodial** command, you can set the auto-dial interval.

Using the **undo dialer timer autodial** command, you can restore the default auto-dial interval.

By default, the auto-dial interval is 300 seconds.

Format

dialer timer autodial *seconds*

undo dialer timer autodial

Parameters

Parameter	Description	Value
seconds	Specifies the auto-dial interval.	The value is an integer that ranges from 1 to 604800, in seconds. The default value is 300.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is only applied to C-DCC.

A DCC router immediately attempts to dial the remote end after starting. The dialing process is not triggered by data packets. If a connection cannot be established with the remote end, the router retries at an interval set by the **dialer timer autodial** command.

Prerequisites

The C-DCC function has been enabled by the **dialer enable-circular** command.

Precautions

- The DCC router attempts to dial the remote end at the interval of ***seconds*** until the call connection is established.
- The **dialer timer autodial** command may be used together with the **dialer route** command or the **dialer number** command that contains the **autodial** keyword. The auto-dial function is not triggered by packets, and the call connection established by auto-dial will not age out. That is, the **dialer timer idle** command is invalid for the call connection established by auto-dial.

  NOTE

  This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Set the auto-dial interval to 90 seconds on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer enable-circular
[Huawei-Serial1/0/0:15] dialer timer autodial 90
```

Related Topics

7.1.5 dialer enable-circular
7.1.13 dialer timer idle
7.1.22 display dialer

7.1.11 dialer timer compete

Function

Using the **dialer timer compete** command, you can set the compete-idle timer after a competition occurs among interfaces.

Using the **undo dialer timer compete** command, you can restore the default compete-idle timer.

By default, the compete-idle timer is 20 seconds.

Format

dialer timer compete *seconds*

undo dialer timer compete

Parameters

Parameter	Description	Value
seconds	Specifies the compete-idle timer on an interface after a competition occurs among interfaces.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 20.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A competition occurs when all channels are occupied. The compete-idle timer takes effect when the competition occurs.

If the compete-idle timer is not set, the idle-timer takes effect for an established link. When a call to another destination needs to be established, the system replaces the idle timer with the compete-idle timer to control the ongoing call. When the idle time of the ongoing call reaches the compete-idle timer, the call is disconnected.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The compete-idle timer must be smaller than the idle timer set by **dialer timer idle**.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Set the timer idle to 50 seconds and timer compete to 10 seconds on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer timer idle 50
[Huawei-Serial1/0/0:15] dialer timer compete 10
```

Related Topics

7.1.13 dialer timer idle

7.1.22 display dialer

7.1.12 dialer timer enable

Function

Using the **dialer timer enable** command, you can set the delay in initiating a new call after the previous call is disconnected.

Using the **undo timer enable** command, you can restore the default setting.

By default, a new call is initiated 5 seconds after the previous call is disconnected.

Format

dialer timer enable *seconds*

undo dialer timer enable

Parameters

Parameter	Description	Value
seconds	Specifies the delay in initiating a new call after the previous call is disconnected.	The value is an integer that ranges from 5 to 65535, in seconds. The default value is 5.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a DCC line is disconnected due to a fault or hang-up, the link is established again only after a certain period of time. This prevents PBX overloading. The **dialer timer enable** command sets this period of time.

Prerequisites

Before using this command for an RS-DCC, run the **dialer user** command to set the remote end user name. Before using this command for a C-DCC, run the **dialer enable-circular** command to enable the C-DCC function.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in PRI mode.

Precautions

If you run the **dialer timer enable** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the delay to 10 seconds on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer enable-circular
[Huawei-Serial1/0/0:15] dialer timer enable 10
```

Related Topics

7.1.22 display dialer

7.1.13 dialer timer idle

Function

Using the **dialer timer idle** command, you can set the maximum link idle time on an interface. During this period of time, no Interesting packet is transmitted over the link.

Using the **undo dialer timer idle** command, you can restore the default link idle time.

By default, the maximum link idle time is 120 seconds.

Format

dialer timer idle *seconds*

undo dialer timer idle

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
seconds	Specifies the maximum link idle time.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 120.*0*, indicating that the idle time is infinite. A link is always connected even if no Interesting packet transmitted.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dialer timer idle** command sets the maximum idle time for links. If no data is transmitted over a link within the idle time, the link is disconnected. This saves resources and costs.

Precautions

- If you run the **dialer timer idle** command multiple times in the same view, only the latest configuration takes effect.
- This command affects only new calls but not the established calls.

  NOTE

  This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Set the maximum link idle time on Dialer0 to 100 seconds.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] dialer timer idle 100
```

Related Topics

7.1.22 display dialer

7.1.14 dialer timer wait-carrier

Function

Using the **dialer timer wait-carrier** command, you can set the wait-carrier timer.

Using the **undo dialer timer wait-carrier** command, you can restore the default wait-carrier timer.

By default, the wait-carrier timer is 60 seconds.

Format

dialer timer wait-carrier *seconds*

undo dialer timer wait-carrier

Parameters

Parameter	Description	Value
seconds	Specifies the wait-carrier timer of calls.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 60.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The wait-carrier timer controls the call setup time.

The wait-carrier timer starts when a call is initiated. If the call cannot be set up before the wait-carrier timer expires, the DCC aborts the call setup process.

Precautions

If you run the **dialer timer wait-carrier** command in the same view multiple times, only the latest configuration takes effect.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Set the wait-carrier timer on Serial1/0/0:15 to 80 seconds.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer timer wait-carrier 80
```

Related Topics

7.1.22 display dialer

7.1.15 dialer timer warmup

Function

Using the **dialer timer warmup** command, you can set the warmup timer on the router configured with the dial-up backup function, that is, the delay for this function to take effect after the system starts.

Using the **undo dialer timer warmup** command, you can restore the default warmup timer.

By default, the warmup timer is 30 seconds.

Format

dialer timer warmup *seconds*

undo dialer timer warmup

Parameters

Parameter	Description	Value
seconds	Specifies the warmup timer for the dial-up backup function.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The warmup timer starts when the system is started, and the system enables the dial-up backup function after the warmup timer expires. The warmup timer reduces the impact of route flapping. Before the warmup timer expires, the system does not use the backup link to initiate calls.

Configuration Impact

After a router configured with the dial-up backup function starts, it does use the backup link within the warmup time even if the active link is not Up.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the warmup timer to 20 seconds.

```
<Huawei> system-view
[Huawei] dialer timer warmup 20
```

Related Topics

7.1.26 standby routing-rule

7.1.16 dialer user

Function

Using the **dialer user** command, you can enable the resource-share DCC (RS-DCC) function and set the remote end user name.

Using the **undo dialer user** command, you can disable the RS-DCC function and delete the remote user name.

By default, the RS-DCC function is disabled and the remote user name is not set.

Format

dialer user *user-name*

undo dialer user [*user-name*]

Parameters

Parameter	Description	Value
user-name	Indicates the remote end user name. If this parameter is not specified when you run the **undo dialer user** command, the RS-DCC function is disabled and all the remote user names are deleted. If this parameter is specified, the specified user name is deleted.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

Dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the data to be transmitted is delay-insensitive, bursting, and has a small volume, the routers can use the dial control center (DCC) mode to reduce costs. DCC sets up a call connection only when there is data to be transmitted. DCC is a

flexible, cost-effective, and efficient solution. After DCC is used on the routers connected with the PSTN, the routers set up a connection by dialing only when there is data to be transmitted between them. That is, they start the DCC process to transmit signal, and tear down the connection when no data is transmitted on the link.

DCC supports extensible dial-on-demand functions to meet various application requirements. It is applicable to the following major scenarios:

- DCC uses link backup to ensure normal communication. When communication fails because of a link error or other reasons, the backup link is used to continue the communication.

  Generally, a network of a different type is used for link backup. For example, an ISDN or a 3G network can be used for the link backup of an IP network. The device implements link backup by:

  – Using the interface backup mode
  – Using the dynamic routing standby mode
- DCC on a PPPoE/PPPoEoA client saves costs for users.

  In this scenario, the user-name parameter will not be carried to the remote end for authentication, and it is only used to identify the local user and enable the RS-DCC mode.

The device supports two DCC modes: C-DCC and resource-shared DCC (RS-DCC). The two modes are applicable to different scenarios. The two ends in communication can adopt different modes. You can choose the DCC modes according to the following table.

DCC Mode	Usage Scenario
C-DCC	C-DCC is applicable to the medium- or large-scale sites that have many physical links.
RS-DCC	RS-DCC is applicable to the small- or medium-scale sites that have a few physical links but many connected interfaces.

To enable the RS-DCC function, use the **dialer user** command.

If PPP encapsulation is configured on dialer interfaces of RS-DCC, the system chooses a dialer interface to receive a call according to the remote user name negotiated by PPP.

Follow-up Procedure

After using the **dialer user** command, set other RS-DCC parameters, such as the dialer bundle and dialer number for the dialer interface.

Precautions

- This command is applied only to RS-DCC.
- If you run the **dialer user** command multiple times in the dialer interface view, multiple remote end user names are mapped to the dialer interface.

Example

Enable RS-DCC on interface dialer 3 and set the remote end user names to RouterA and RouterB.

```
<Huawei> system-view
[Huawei] interface dialer 3
[Huawei-Dialer3] dialer user RouterA
[Huawei-Dialer3] dialer user RouterB
```

Related Topics

7.1.6 dialer number

7.1.17 dialer-group

Function

Using the **dialer-group** command, you can add an interface to a dialer access group.

Using the **undo dialer-group** command, you can delete an interface from a dialer access group.

By default, an interface does not belong to any dialer access group.

Format

dialer-group *group-number*

undo dialer-group

Parameters

Parameter	Description	Value
group-number	Specifies the dialer access group for an interface. The dialer access group is configured by the **dialer-rule** command.	The value of *group-number* must be the same as the value of *dialer-rule-number* in the **dialer-rule** command.

Views

ISDN BRI interface view, ISDN PRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The DCC dialer ACL must be configured correctly and associated to interfaces (physical interfaces and dialer interfaces) by using the **dialer-group** command; otherwise, DCC packets cannot be sent. The **dialer-group** command adds interfaces to dialer access groups to control packet sending on the interfaces.

Prerequisites

Before running the **dialer-group** command, run the **dialer user** command to enable the RS-DCC function or the **dialer enable-circular** command to enable the Circular DCC function; otherwise, the **dialer-group** command cannot take effect.

Precautions

An interface belongs to only one dialer access group. If you run the **dialer-group** command in the same interface view multiple times, only the latest configuration takes effect.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Add Dialer0 to dialer access group 1.

```
<Huawei> system-view
[Huawei] dialer-rule
[Huawei-dialer-rule] dialer-rule 1 acl 3001
[Huawei-dialer-rule] quit
[Huawei] interface dialer 0
[Huawei-Dialer0] dialer user userb
[Huawei-Dialer0] dialer-group 1
```

Related Topics

7.1.20 dialer-rule (dialer-rule view)

7.1.18 dialer retry limit

Function

The **dialer retry limit** command sets the quiet duration and retransmission times in the quiet duration.

The **undo dialer retry limit** command restores the default settings.

By default, the quiet duration and retransmission times in the quiet duration are not set on a router.

Format

dialer retry limit *counts* **quiet-period** *period*

undo dialer retry limit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
counts	Specifies retransmission times in the quiet duration.	The value is an integer that ranges from 1 to 65535.
quiet-period *period*	Specifies the quiet duration.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

Dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device of other vendors functions as the PPPoE or PPPoEoA server, it limits the number of connection attempts of a client in a specified period (quiet duration). When the number of connection attempts exceeds the threshold, the device no longer receives connection requests from the client.

When a router functions as a PPPoE or PPPoEoA client, it continuously sends connection requests to the PPPoE or PPPoEoA server until a connection is established. When the number of connection attempts in the quiet duration exceeds the maximum value allowed on the PPPoE or PPPoEoA server, the PPPoE or PPPoEoA server no longer receives connection requests from the client until the quiet duration times out. However, the client still sends connection requests to the PPPoE or PPPoEoA server in the quiet duration, wasting resources.

To address this problem, set the quiet duration and retransmission times in the quiet duration. When the number of retransmission times in the quiet duration exceeds the threshold, the client stops sending connection requests to the server until the quiet duration times out.

Prerequisites

You have run the **dialer user** command to enable RS-DCC function. Otherwise, the **dialer retry limit** command cannot take effect.

Precautions

If you run the **dialer retry limit** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the quiet duration to 10s and retransmission times in the quiet duration to 20.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface dialer 1
[Huawei-Dialer1] dialer user userb
[Huawei-Dialer1] dialer retry limit 20 quiet-period 10
```

Related Topics

7.1.16 dialer user

7.1.19 dialer threshold

Function

The **dialer threshold** command sets the load threshold of a DCC link. When the percentage of traffic in available bandwidth of all DCC links exceeds the configured percentage, another link is initiated to call the same destination.

The **undo dialer threshold** command restores the default setting.

By default, flow control is disabled.

Format

dialer threshold *traffic-percentage* [**in** | **in-out** | **out**]

undo dialer threshold

Parameters

Parameter	Description	Value
traffic-percentage	Specifies the percentage of traffic in available bandwidth.	The value is an integer that ranges from 0 to 99. A value no larger than 90 is recommended.
in	Indicates that only incoming traffic is calculated during actual load calculation.	-
in-out	Indicates that only the higher of incoming traffic and outgoing traffic is calculated during actual load calculation.	-
out	Indicates that only outgoing traffic is calculated during actual load calculation.	-

Views

ISDN BRI interface view, ISDN PRI interface view, Async interface view, dialer interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In DCC applications, you can configure the load threshold of links.

- When the load threshold ranges from 1 to 99, you can adjust the allocated bandwidth for MP bundle according to the percentage of actual traffic in available bandwidth.
  - When the percentage of traffic in bandwidth of a DCC link exceeds the configured load threshold, a second DCC link is initiated to work with the first DCC link for MP bundle. When the percentage of traffic in bandwidth of the two DCC links exceeds the configured load threshold, a third DCC link is initiated to work with the two DCC links for MP bundle. The rest may be deduced by analogy. This implementation ensures that DCC links have proper loaded traffic.
  - When the percentage of traffic of N links (N is an integer that is larger than 1) in bandwidth of N-1 links is smaller than the configured load threshold, the system shuts down a link. The rest may be deduced by analogy. This implementation ensures that DCC link usage efficiency is in the proper range.
- When the load threshold is 0, all available links are initiated to call the destination without traffic detection during auto-dial or traffic-triggered dialup. The links on which calls have been set up are not terminated because of timeout.

Prerequisites

The remote user name has been configured using the **dialer user** command or C-DCC has been enabled using the **dialer enable-circular** command.

Precautions

- In C-DCC, this command is used on the interfaces in a dialer circular group. In RS-DCC, this command can only be used on dialer interfaces.
- This command can be used only when the **dialer number** command is used for dialup.
- This command only takes effect in the outgoing call scenario, not the incoming call scenario.
- This command must be used together with the **ppp mp** command.
- When the **dialer threshold** *traffic-percentage* command (*traffic-percentage* is not 0) is used together with the **ppp mp max-bind** *max-bind-number* command, a link is initiated first. If the percentage of traffic in available bandwidth still exceeds the value of *traffic-percentage*, the next idle link is initiated until the number of bundled links reaches the value of *max-bind-number* or the percentage of traffic in available bandwidth is smaller than the value of *traffic-percentage*.

  If you configure **dialer threshold** *0*, DCC initiates all available links and the **dialer timer idle** command configuration becomes ineffective.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the load threshold of Dialer1 to 80%.

```
<Huawei> system-view
[Huawei] interface dialer 1
[Huawei-Dialer1] dialer threshold 80
```

7.1.20 dialer-rule (dialer-rule view)

Function

Using the **dialer-rule** command, you can specify a dialer access control list (ACL) for a dialer access group. The dialer ACL defines conditions to initiate calls.

Using the **undo dialer-rule** command, you can delete a dialer ACL.

By default, no dialer ACL is configured.

Format

dialer-rule *dialer-rule-number* { **acl** { *acl-number* | **name** *acl-name* } | **ip** { **deny** | **permit** } | **ipv6** { **deny** | **permit** } }

undo dialer-rule *dialer-rule-number* [**acl** | **ip** | **ipv6**]

Parameters

Parameter	Description	Value
dialer-rule-number	Specifies the number of a dialer access group.	The value is the same as the value of *group-number* in the **dialer-group** command.
acl { *acl-number* | **name** *acl-name* }	Indicates the number or name of the dialer ACL.	The value of *acl-number* is an integer that ranges from 2000 to 3999. The value of *acl-name* is a string of 1 to 32 case-sensitive characters without space. The name must start with an English letter and can be a mixture of English letters, digits, hyphens (-), or underlines (_).
ip { **deny** | **permit** }	Indicates whether the dialer ACL allows or forbids IPv4 packets.	-
ipv6 { **deny** | **permit** }	Indicates whether the dialer ACL allows or forbids IPv6 packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Dialer-rule view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A dialer ACL filters all the packets passing a dialer interface.

The DCC dialer ACL must be configured and associated to the interfaces (physical interfaces and dialer interfaces) by using the dialer-group command; otherwise, DCC packets cannot be sent. You can configure filtering rules for a dialer ACL or associate an existing ACL to the dialer ACL.

Prerequisites

The ACL to be associated to the dialer ACL has been created.

Precautions

To control packet sending on a DCC dialer interface, run the **dialer-rule** command to configure a dialer ACL for the interface, and then run the **dialer-group** command to add the interface to a dialer access group.

If the **dialer-group** of a dialer interface does not have a **dialer-rule**, the packets from the interface are considered as Uninteresting packets and are discarded.

Example

Create dialer ACL 1, which permits all IPv4 packets and rejects all IPv6 packets.

```
<Huawei> system-view
[Huawei] dialer-rule
[Huawei-dialer-rule] dialer-rule 1 ip permit
```

Create dialer ACL 1, which permits all IPv4 and IPv6 packets.

```
<Huawei> system-view
[Huawei] dialer-rule
[Huawei-dialer-rule] dialer-rule 1 ip permit
[Huawei-dialer-rule] dialer-rule 1 ipv6 permit
```

Related Topics

7.1.17 dialer-group

7.1.21 dialer-rule (system view)

Function

Using the **dialer-rule** command, you can enter the dialer rule view.

Format

dialer-rule

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you use the **dialer-rule (dialer rule view)** command to configure the dialer access control list (ACL), you must run this command to enter the dialer rule view.

Follow-up Procedure

Configure the dialer ACL by using the **dialer-rule (dialer rule view)** command.

Precautions

The dialer rule view cannot be deleted.

Example

Enter the dialer rule view.

```
<Huawei> system-view
[Huawei] dialer-rule
[Huawei-dialer-rule]
```

Related Topics

7.1.20 dialer-rule (dialer-rule view)

7.1.22 display dialer

Function

Using the **display dialer** command, you can view the DCC information on an interface.

Format

display dialer [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the DCC information on an interface. If this parameter is not specified, the DCC information on all interfaces is displayed.	The interface can be a physical interface or a dialer interface.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a DCC fault occurs, you can use the command to view the configuration information on the dialer interface. The configuration information helps you analyze the DCC dialing process to locate the fault.

Example

Display configuration information on interface dialer 1.

```
<Huawei> display dialer interface dialer 1
Dial Interface:Dialer1
  Dialer Route:
  NextHop_address Dialer_Numbers
        2.2.2.2

  Dialer Timers(Secs):
  Auto-dial:4800    Compete:20    Enable:5
  Idle:120    Wait-for-Carrier:60
```

Table 7-1 Description of the display dialer command output

Item	Sub-item	Description
Dialer Route	NextHop_address	Destination address set by **dialer route**.
	Dialer_Numbers	Dialer number set by **dialer number**.
Dialer Timers(Secs)	Auto-dial	Auto-dial interval set by **dialer timer autodial**.
	Compete	Compete-idle timer set by **dialer timer compete**.
	Enable	Link disconnection time set by **dialer timer enable**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
	Idle	Maximum link idle time set by **dialer timer idle**.
	Wait-for-Carrier	Wait-carrier timer set by **dialer timer wait-carrier**.

Related Topics

7.1.9 dialer route
7.1.10 dialer timer autodial
7.1.11 dialer timer compete
7.1.12 dialer timer enable
7.1.13 dialer timer idle
7.1.14 dialer timer wait-carrier

7.1.23 display interface dialer

Function

Using the **display interface dialer** command, you can view information about dialer interfaces.

Format

display interface dialer [*number*]

Parameters

Parameter	Description	Value
number	Displays information about a dialer interface. If this parameter is not specified, information about all dialer interfaces is displayed.	The value range of *number* depends on the number range of dialer interfaces. Only the numbers of created dialer interfaces are displayed.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When monitoring the interface status or locating faults on a dialer interface, run the **display interface dialer** command on the interface. According to the output information, you can collect traffic statistics and locate faults on the interface.

Example

Display information about interface dialer 1.

```
<Huawei> display interface dialer 1
Dialer1 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Dialer1 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 1.1.1.1/24
Link layer protocol is PPP
LCP opened
Physical is Dialer
Current system time: 2010-08-24 22:57:27-05:13
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 bytes
    Output:0 bytes
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

Table 7-2 Description of the display interface dialer command output

Item	Description
Dialer1 current state	Physical status of the dialer interface: ● UP: indicates that the physical status of the interface is Up. ● DOWN: indicates that the interface has a fault. ● Administratively down: indicates that the network administrator has run the **shutdown** command on the interface.
Line protocol current state	Link-layer protocol status of the dialer interface: ● UP (spoofing): indicates that the link-layer protocol status of the interface is Up. **spoofing** indicates that the link-layer protocol of the dialer interface is logically Up and dial-up can be performed. ● DOWN: indicates that the link-layer protocol status of the interface is Down or no IP address is assigned to the interface. **damping** indicates that the interface is suppressed because of frequent flapping.
Description	Interface description.
The Maximum Transmit Unit	Maximum transmit unit (MTU) of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hold timer	Heartbeat interval after the PPP LCP negotiation status becomes Opened.
Internet Address	Interface IP address. If no IP address is assigned to the dialer interface, the system displays "Internet protocol processing: disabled."
Link layer protocol is PPP	The link-layer protocol is PPP.
LCP	LCP negotiation status: ● Initial: indicates that the physical layer is faulty. ● Starting: indicates that the physical layer is starting. This state lasts for a short time. ● Closed: indicates that the system has sent a Terminate-Ack packet to terminate the connection after receiving the Configure-Request packet. ● Stopped: indicates that the system receives the Configure-Request packet, but does not receive a Configure-Ack packet from the peer device. The system then sends a Terminate-Ack packet. ● Closing: indicates that the connection is being closed. The system enters the Closed state if it receives a Configure-Ack packet from the peer device or the timer expires. This state lasts for a short time. ● Stopping: indicates that the connection is being closed to prevent subsequent traffic. This state lasts for a short time. ● Req-Sent: indicates an attempt to establish a connection. The system has sent a Configure-Request packet, but does not receive a Configure-Ack packet. ● Ack-Rcvd: indicates that the system has sent a Configure-Request packet and receives a Configure-Ack packet from the peer device, but does not send a Configure-Ack packet to the peer device. ● Ack-Sent: indicates that the system has sent a Configure-Request packet and a Configure-Ack packet to the peer device, and receives a Configure-Ack packet from the peer device. ● Opened: indicates that the system has sent a Configure-Ack packet to the peer device and receives a Configure-Ack packet from the peer device. This indicates that the link layer works properly.
Physical is Dialer	The interface is a dialer interface.
Current system time	Current system time.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last 300 seconds input rate 0 bits/sec, 0 packets/sec Last 300 seconds output rate 0 bits/sec, 0 packets/sec	Rates of packets sent and received in the last 300 seconds, expressed in bits per second and packets per second.
Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec	Rates of packets sent and received when the **display interface dialer** command is being executed.
Input: 0 bytes Output:0 bytes	Total number of bytes sent and received by the interface.
Input bandwidth utilization : 0.00% Output bandwidth utilization : 0.00%	Upstream bandwidth usage and downstream bandwidth usage on the interface.

7.1.24 interface dialer

Function

Using the **interface dialer** command, you can create a dialer interface and enter the dialer interface view.

Using the **undo interface dialer** command, you can delete the dialer interface.

By default, no dialer interface exists.

Format

interface dialer *number*

undo interface dialer *number*

Parameters

Parameter	Description	Value
number	Specifies the number of a dialer interface.	The value is an integer and the value depend on the device.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

DCC allows routers to communicate by using the Public Switched Telephone Network (PSTN) and provides on-demand dialup services. The device supports two DCC modes: circular DCC (C-DCC) and resource-shared DCC (RS-DCC).

A dialer interface is a logical interface that is used to implement DCC. After a physical interface is bound to a dialer interface, the physical interface inherits the configurations of the dialer interface.

This command is applied to C-DCC and RS-DCC. When you create a dialer interface for C-DCC, a dialer circular group with the same number as the dialer interface is also created. When you create a dialer interface for RS-DCC, only the dialer interface will be created.

NOTICE

If DCC dialing is triggered or the ISDN link is Up, when you run the **undo interface dialer** command to delete a dialer interface, the device may be reset unexpectedly. To solve the problem, run the **undo dialer user** command to disable RS-DCC or the **undo dialer enable-circular** command to disable C-DCC.

Example

Create interface dialer 1.

```
<Huawei> system-view
[Huawei] interface dialer 1
```

Related Topics

7.1.23 display interface dialer

7.1.25 standby routing-group

Function

Using the **standby routing-group** command, you can specify a standby routing group for a dialer interface. This dialer interface is then used as a standby dialer interface.

Using the **undo standby routing-group** command, you can cancel the setting.

By default, the standby routing function is disabled.

Format

standby routing-group *group-number*

undo standby routing-group *group-number*

Parameters

Parameter	Description	Value
group-number	Specifies the standby routing group for a dialer interface.	The value is an integer that ranges from 1 to 255.

Views

ISDN PRI interface view, ISDN BRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A standby routing group contains some monitored network segments. If the system detects that a monitored network segment does not have a reachable route, it uses the standby dialer interface for dialing. The **standby routing-group** command specifies the standby dialer interface.

For example, standby routing group 1 that monitors 10.0.0.0/8 is specified for Serial1/0/0:15. When the system detects that network segment 10.0.0.0/8 does not have a reachable route, it uses Serial1/0/0 as the standby dialer interface for dialing.

Prerequisites

The basic DCC function has been enabled on the standby dialer interface and the standby routing group has been created by the **standby routing-rule** command.

Precautions

After the route in the monitored network segment is recovered, the system can disconnect the standby dialer interface immediately or after a specified timer expires. This timer is set by the **standby timer routing-disable** command.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Specify a standby routing group for Dialer 0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] standby routing-group 1
```

Related Topics

7.1.26 standby routing-rule

7.1.27 standby timer routing-disable

7.1.26 standby routing-rule

Function

Using the **standby routing-rule** command, you can create a standby routing group and add the network segments to be monitored to the group.

Using the **undo standby routing-rule** command, you can delete a standby routing group or delete network segments from the standby routing group.

By default, no standby routing group exists.

Format

standby routing-rule *group-number* **ip** *ip-address* { *mask* | *mask-length* }

undo standby routing-rule *group-number* [**ip** *ip-address* { *mask* | *mask-length* }]

Parameters

Parameter	Description	Value
group-number	Specifies the number of the standby routing group.	The value is an integer that ranges from 1 to 255.
ip *ip-address*	Specifies the network segment to be monitored.	The value of *ip-address* is in dotted decimal notation.
mask	Specifies the mask of the network segment to be monitored.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the network segment to be monitored.	The value is an integer that ranges from 0 to 32.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A standby routing group contains some monitored network segments. When there is no reachable route to any of the monitored network segments, the standby dialer interface is used for dialing.

Configuration Impact

Follow-up Procedure

After creating a standby routing group, use the **standby routing-group** command to specify this group for a dialer interface.

Precautions

You can add multiple network segments to a standby routing group. The system uses the standby dialer interface only when no network segment has a reachable route.

Example

Create standby routing group 1 and add network segment 10.0.0.0/8 to the group.

```
<Huawei> system-view
[Huawei] standby routing-rule 1 ip 10.0.0.0 255.0.0.0
```

Related Topics

7.1.9 dialer route

7.1.25 standby routing-group

7.1.27 standby timer routing-disable

Function

Using the **standby timer routing-disable** command, you can set the delay to disconnect the standby dialer interface after the routes in the monitored network segment are recovered.

Using the **undo standby timer routing-disable** command, you can restore the default delay.

By default, when the routes in a network segment are recovered, the system disconnects the standby dialer interface after a 30-second delay.

Format

standby timer routing-disable *seconds*

undo standby timer routing-disable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
seconds	Specifies the delay to disconnect the standby dialer interface. If this parameter is set to 0, the system immediately disconnects the standby dialer interface when the routes in a network segment are recovered.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.

Views

ISDN PRI interface view, ISDN BRI interface view, cellular interface view, Async interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **standby timer routing-disable** command sets a delay to disconnect the standby dialer interface. This delay prevents route flapping after the routes in the network segment are recovered.

Configuration Impact

If you run the **standby timer routing-disable** command in the same view multiple times, only the latest configuration takes effect.

NOTE

This command can be used in the ISDN PRI interface view. A PRI interface can be a CE1 or CT1 interface working in the PRI mode.

Example

Set the delay to disconnect the standby dialer interface to 15 seconds on Dialer 0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] standby timer routing-disable 15
```

7.2 PPP Configuration Commands

7.2.1 display ppp compression iphc rtp

Function

The **display ppp compression iphc rtp** command displays RTP/UDP/IP header compression statistics in IPHC.

Format

display ppp compression iphc rtp [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays RTP/UDP/IP header compression statistics on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the following information:

- Statistics on received packets, including the number of compressed packets, number of error packets, number of discarded packets, and total number of all received packets
- Statistics on sent packets, including the number of compressed packets, number of all packets, number of sent bytes, number of saved bytes, and total number of all sent bytes

Example

Display RTP/UDP/IP header compression statistics on Serial 1/0/0:0 in IPHC.

```
<Huawei> display ppp compression iphc rtp interface serial 1/0/0:0
IPHC: RTP/UDP/IP header compression

  Interface: Serial 1/0/0:0
    Received:
      Compress/Error/Discard/Total: 0/0/0/0 (Packets)
    Sent:
      Compress/Total: 0/0 (Packets)
      Send/Save/Total: 0/0/0 (Bytes)
Connect:
  Rx/Tx: 16/16
      Long-search/Miss: 0/0
```

Table 7-3 Description of the display ppp compression iphc rtp command output

Item	Description
IPHC	IP header compression statistics.
Interface	Interface to which header compression is applied.
Received	Statistics on received packets.
Compress/Error/Discard/Total	Number of compressed packets/Number of error packets/Number of discarded packets/Total number of all received IPHC RTP packets (including full header packets and compressed packets).
Sent	Statistics on sent packets.
Compress/Total	Number of compressed packets/Total number of all IPHC RTP packets sent (including full header packets and compressed packets).
Send/Save/Total	Number of sent bytes/Number of saved bytes/Total number of all sent bytes.
Connect	Statistics on compression entry queries.
Rx	Maximum number of data connections that can be decompressed when the device functions as the receiver.
Tx	Maximum number of data connections that can be compressed when the device functions as the transmitter.
Long-search/Miss	Number of compression entry queries/Number of compression entry query failures.

Related Topics

7.2.11 ppp compression iphc

7.2.2 display ppp compression iphc tcp

Function

The **display ppp compression iphc tcp** command displays TCP/IP header compression statistics in IPHC.

Format

display ppp compression iphc tcp [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays TCP/IP header compression statistics on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the following information:

- Statistics on received packets, including the number of compressed packets, number of error packets, number of discarded packets, and total number of all received packets.
- Statistics on sent packets, including the number of compressed packets, number of all packets, number of sent bytes, number of saved bytes, and total number of all sent bytes.
- Number of compression entry queries and number of compression entry query failures.

Example

Display TCP/IP header compression statistics on Serial 1/0/0:0 in IPHC.

```
<Huawei> display ppp compression iphc tcp interface serial 1/0/0:0
IPHC: TCP/IP header compression
  Interface: Serial 1/0/0:0
    Received:
      Compress/Error/Discard/Total: 0/0/0/0 (Packets)
    Sent:
      Compress/Total: 0/0 (Packets)
      Send/Save/Total: 0/0/0 (Bytes)
    Connect:
        Rx/Tx: 16/16
        Long-search/Miss: 0/0
```

Table 7-4 Description of the display ppp compression iphc tcp command output

Item	Description
IPHC	IP header compression statistics.
Interface	Interface to which header compression is applied.
Received	Statistics on received packets.

Item	Description
Compress/Error/Discard/Total	Number of compressed packets/Number of error packets/Number of discarded packets/Total number of all received IPHC TCP packets (including full header packets and compressed packets).
Sent	Statistics on sent packets.
Compress/Total	Number of compressed packets/Total number of all IPHC TCP packets sent (including full header packets and compressed packets).
Send/Save/Total	Number of sent bytes/Number of saved bytes/Total number of all sent bytes.
Connect	Statistics on compression entry queries.
Rx	Maximum number of data connections that can be decompressed when the device functions as the receiver.
Tx	Maximum number of data connections that can be compressed when the device functions as the transmitter.
Long-search/Miss	Number of compression entry queries/Number of compression entry query failures.

Related Topics

7.2.11 ppp compression iphc

7.2.3 display ppp compression stac-lzs

Function

The **display ppp compression stac-lzs** command displays Stac LZS compression statistics.

Format

display ppp compression stac-lzs [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays Stac LZS compression statistics on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display Stac LZS compression statistics on Serial 1/0/0:0.

```
<Huawei> display ppp compression stac-lzs interface serial 1/0/0:0
Serial 1/0/0:0
  sent:
    CompressedPackets  = 0,  UnCompressedPackets  = 0
    CompressedOctets    = 0,  UnCompressedOctets    = 0
  receive:
    CompressedPackets  = 0,  UnCompressedPackets  = 0
    CompressedOctets    = 0,  UnCompressedOctets     = 0
    DeCompressedPackets = 0, DeCompressedOctets = 0
```

Table 7-5 Description of the display ppp compression stac-lzs command output

Item	Description
sent	Statistics on packets sent from the local device.
receive	Statistics on packets received by the local device.
CompressedPackets	Number of compressed packets.
UnCompressedPackets	Number of uncompressed packets.
CompressedOctets	Number of compressed bytes.
UnCompressedOctets	Number of uncompressed bytes.
DeCompressedPackets	Number of received compressed packets that are successfully decompressed and not discarded by the local device.
DeCompressedOctets	Number of received compressed bytes that are successfully decompressed and not discarded by the local device.

Related Topics

7.2.14 ppp compression stac-lzs

7.2.4 display ppp information

Function

The **display ppp information** command displays PPP link parameters.

Format

display ppp information { *ifIndex* | **all** | **ppp-index** *ppp-index* }

Parameters

Parameter	Description	Value
ifIndex	Displays the parameters of the PPP link with the specified interface index. You can use the **display ifnet index-map** command in the Diagnostic view to view the interface indexes of all ports.	The value is an integer that ranges from 0 to 4294967294.
all	Displays the parameters of all PPP links.	-
ppp-index	Displays the parameters of the PPP link with the specified PPP index.	The value is an integer that ranges from 0 to 4294967294.

Views

All view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the parameters of the PPP link with the specified interface index.

```
<Huawei> display ppp information 0x27
 ================= PPP Info Begin =================
 IfIndex    = 0x27;
 PPPIndex   = 0x70000000;
 PPPType    = 0;
 MTU        = 0;
```

```
MpType     = 0;
IsDialer   = 0;
IsCallIn   = 0;
IsCallBack = 0;
VLinkIndex = 0;
BridgeID   = 0;
RouteIf    = 0x27;
Phase      = 0;
UserId     = -1;
AuthServer = 0;
AuthClient = 0;
VlanId     = 0;
PvcId      = 0x0;
PeerIp     = 0x0;
PeerPubIP  = ;
RemAddrUse = 0;
FrameIP    = 0x0;
VrfIndex   = 0x0;
Gateway    = 0xffffffff;
Mask       = 0xffffffff;
PriDNS     = 0x0;
SecDNS     = 0x0;
PriNBNS    = 0x0;
SecNBNS    = 0x0;
PoolNO     = 65535;
MagicNo    = 0x50505021;
TraceID    = 0xffffffff;
IPHCFormat = 0;
UserMac    = 0000-0000-0000;
VirUserMac = 02e0-0000-0027;
Terminate_Cause        = 1;
Terminate_InsideCause = 19;
FirstIfID  = 1;
IfIDType   = 0;
IfID       = 0000:0000:0000:0000;
IfIDAuto   = 0000:0000:0000:0000;
LoginUsrName   = ;
CallBackString = ;
CalledNumber   = ;
CallingNumber  = ;
------------------------------
PPPInfo  Addr  = 0x3bbf8598;
LcpInfo  Addr  = 0x6e24feb4;
PapInfo  Addr  = 0x0;
ChapInfo Addr  = 0x0;
IpcpInfo Addr  = 0x0;
Ip6cpInfo Addr = 0x0;
BcpInfo  Addr  = 0x0;
MpInfo   Addr  = 0x0;
------------------------------
ConfigInfo     Addr  = 0x3f30c324;
UsedConfigInfo Addr  = 0x3f30c984;
=================== PPP Info End ===================
```

Table 7-6 Description of the **display ppp information** command output

Item	Description
IfIndex	Interface index.

Item	Description
PPPType	PPP protocol type: ● 0: common PPP link ● 1: PPPoE server ● 2: PPPoEoA ● 3: PPPoA ● 4: PPPoFR ● 5: PPPoE client ● 6: MP ● 7: L2TP
MTU	Maximum Transmission Unit (MTU).
MpType	MP channel type: ● 0: non-MP channel ● 1: MP sub-channel ● 2: MP channel ● 3: MP template
IsDialer	Whether the interface is a dialer interface: ● 0: The interface is not a dialer interface. ● 1: The interface is a dialer interface for PPP callback link.
IsCallIn	Whether the local end is the calling end: ● 0: The local end is not the calling end. ● 1: The local end is the calling end .
IsCallBack	Whether the user is a callback user: ● 0: The user is not a callback user. ● 1: The user is the callback user .
VLinkIndex	VLink index.
BridgeID	Bridge ID.
RouteIf	Route interface index.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Phase	PPP negotiation phase: ● 0: Dead Phase (link dead phase) ● 1: Establish Phase (link establishment phase) ● 2: Authenticate Phase (authentication phase) ● 3: CBCP Phase (CBCP negotiation phase) ● 4: Network Phase (network negotiation phase) ● 5: Terminate Phase (link termination phase)
UserId	User ID.
AuthServer	Whether the local end is the authenticating end.
AuthClient	Whether the local end is the authenticated end.
VlanId	VLAN ID.
PvcId	PVC ID.
PeerIp	Peer IP address.
PeerPubIP	Peer LAC IP address.
RemAddrUse	Usage flag of the remote IP address.
FrameIP	Frame IP address delivered by the RADIUS server.
VrfIndex	VPN index delivered by the RADIUS server.
Gateway	User gateway.
Mask	User mask.
PriDNS	Primary DNS address allocated to an authenticated user.
SecDNS	Secondary DNS address allocated to an authenticated user.
PriNBNS	Primary NBNS address allocated to an authenticated user.
SecNBNS	Secondary NBNS address allocated to an authenticated user.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PoolNO	Address pool index delivered by the RADIUS server.
MagicNo	Magic number.
TraceID	Service tracing ID.
IPHCFormat	IPHC compression format.
UserMac	User MAC address.
VirUserMac	User virtual MAC address.
Terminate_Cause	Termination cause: ● 0: initial value ● 1: A user requests to go offline. ● 2: Data services are interrupted.
Terminate_InsideCause	Internal termination cause: ● 0: initial value ● 1: A user requests to go offline. ● 10: The NAS requests the user to go offline. ● 19: The remote user requests to go offline. ● 22: Echo handshake fails. ● 25: PPPoE users go offline after the Ethernet interface goes Down.
FirstIfID	First obtained interface ID.
IfIDType	Interface ID type.
IfID	Interface ID.
IfIDAuto	Interface ID.
LoginUsrName	Login user name.
CallBackString	Callback dial string.
CalledNumber	Called number .
CallingNumber	Calling number.
PPPInfo Addr	Memory address of the PPP control module.
LcpInfo Addr	Memory address of the LCP control module.
PapInfo Addr	Memory address of the PAP control module.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ChapInfo Addr	Memory address of the CHAP control module.
IpcpInfo Addr	Memory address of the IPCP control module.
Ip6cpInfo Addr	Memory address of the IP6CP control module.
BcpInfo Addr	Memory address of the BCP control module.
MpInfo Addr	Memory address of the MP control module.
ConfigInfo Addr	Memory address of the configuration control module input by the user on the current interface.
UsedConfigInfo Addr	Memory address of the configuration control module used for negotiation.
Ouraddr	Local IP address.
Hisaddr	Peer IP address.
dnsaddr0	Primary DNS IP address.
dnsaddr1	Secondary DNS IP address.
GotOption	Negotiated local option.
HisOption	Negotiated remote option.
WantOption	Local option to be negotiated with the remote end.
AllowOption	Local option that can be negotiated with the remote end.

Display the parameters of all PPP links.

```
[Huawei-diagnose] display ppp information all
PPP INFO ALL :
 Interface              IfIndex  MTU   LocalIP         PeerIP
PeerPublicIP
 Dialer16:0             0x231    1492  192.168.100.2   192.168.100.1
 Virtual-Template3:0    0x21d    1500  10.1.1.11       10.1.1.10
 Virtual-Template2:0    0x21c    1500  10.2.1.11       10.2.1.10
 Virtual-Template33:0   0x28b    1500  10.3.33.2       10.3.33.1
 Virtual-Template1:0    0x217    1500  10.2.1.11       10.2.1.10
 Serial3/0/0/16:0       0x29b    1500
 Serial3/0/0/13:1       0x289    1500
 Serial3/0/0/13:0       0x288    1500
 Serial3/0/0/8:0        0x272    1500  10.0.0.1        10.0.0.2
```

Table 7-7 Description of the **display ppp information all** command output

Item	Description
Interface	Interface name.
IfIndex	Interface index.
MTU	Maximum Transmission Unit.
LocalIP	Local IP address.
PeerIP	Peer IP address.
PeerPublicIP	IP address of the peer public network.

7.2.5 ip address ppp-negotiate

Function

The **ip address ppp-negotiate** command configures IP address negotiation on an interface to allow the interface to obtain an IP address from the remote device.

The **undo ip address ppp-negotiate** command cancels IP address negotiation.

By default, an interface does not obtain an IP address through PPP negotiation.

Format

ip address ppp-negotiate

undo ip address ppp-negotiate

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the local interface runs PPP at the link layer but is not assigned an IP address, and the remote device has IP addresses, you can configure IP address negotiation

on the local interface so that it can obtain an IP address from the remote device. For example, when the client accesses the Internet through an Internet Server Provider (ISP) network, it can obtain an IP address from the ISP.

Prerequisites

- PPP has been configured as the link layer protocol of the interface.
- The address assignment function has been enabled on the remote device.

Example

Configure IP address negotiation on Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ip address ppp-negotiate
```

Related Topics

7.2.7 link-protocol ppp

7.2.25 remote address

7.2.6 ip tcp vjcompress

Function

The **ip tcp vjcompress** command configures Van Jacobson Header Compression (VJHC) on an interface of a PPP link.

The **undo ip tcp vjcompress** command cancels the configuration.

By default, VJHC is not configured on an interface of a PPP link.

Format

ip tcp vjcompress

undo ip tcp vjcompress

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

VJHC complies with RFC 1144 and is an algorithm for compressing TCP/IP packet headers on PPP links. The two devices on a PPP link use IP Control Protocol (IPCP) to negotiate with each other for VJHC capability, which improves transmission efficiency over PPP links. The two devices must negotiate with each other twice if packets sent on both directions of the PPP link need compression. The PPP field in an IP packet can be set to one of the following values:

- 0021: IP packets.
- 002d: compressed TCP packets. The original TCP/IP header of a packet is replaced by the compressed TCP/IP header.
- 002f: uncompressed TCP packets.

A device does not compress a data packet if the packet header is not in the compression status list; instead, the device directly sends the packet with the PPP field **002f** to the peer device and adds the packet header to the compression status list of the local device. When receiving the packet, the peer device adds the packet header to its compression status list.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Precautions

VJHC compresses TCP/IP headers, while IPHC compresses TCP/IP headers or RTP/UDP/IP headers.

After running the **ip tcp vjcompress** command on an interface, restart the interface to make the configuration take effect.

You can restart an interface by using the following methods:

- Run the **shutdown** command and then the **undo shutdown** command.
- Run the **restart** command.

NOTE

Ensure that the PPP link VJHC function is configured on the peer device; otherwise, the PPP compression negotiation between the two ends fails.

Example

Configure VJHC on Serial2/0/0.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol ppp
[Huawei-Serial2/0/0] ip tcp vjcompress
```

Related Topics

7.2.7 link-protocol ppp

7.2.7 link-protocol ppp

Function

The **link-protocol ppp** command configures PPP as the link layer protocol of an interface.

The **undo link-protocol ppp** command deletes the PPP protocol of an interface.

By default, all interfaces except Ethernet interfaces and LTE Cellular interfaces run PPP at the link layer.

NOTE

Only the Cellular interfaces support the **undo link-protocol ppp** command.

Format

link-protocol ppp

undo link-protocol ppp

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

The **link-protocol ppp** command configures PPP as the link layer protocol of an interface.

Example

Configure PPP as the link layer protocol of Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] link-protocol ppp
```

 Copyright © Huawei Technologies Co., Ltd.

7.2.8 ppp authentication-mode

Function

The **ppp authentication-mode** command configures the PPP authentication mode in which the local device authenticates the remote device.

The **undo ppp authentication-mode** command restores the default configuration.

By default, PPP authentication is not performed.

Format

ppp authentication-mode { **chap** | **pap** } [[**call-in**] **domain** *domain-name*]

undo ppp authentication-mode

Parameters

Parameter	Description	Value
chap	Sets the PPP authentication mode to Challenge Handshake Authentication Protocol (CHAP) authentication.	-
pap	Sets the PPP authentication mode to Password Authentication Protocol (PAP) authentication. **NOTE** In PAP authentication, passwords are transmitted in plain text on the network, bringing potential security risks. CHAP authentication is recommended.	-
call-in	Indicates that the local device authenticates users only when these users call in.	-
domain *domain-name*	Specifies the domain name used for user authentication. **NOTE** The specified domain must have been created using the **domain (AAA view)** command.	The value is a string of 1 to 64 case-sensitive characters without any space, asterisk (*), question mark (?), or quotation mark ('').

 Copyright © Huawei Technologies Co., Ltd.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PPP link, the local device authenticates the remote device to improve security. Two PPP authentication modes are available:

- PAP: It is a two-way handshake authentication protocol that transmits passwords in plain text.

  PAP is used on networks that do not require high security.
- CHAP: It is a three-way handshake authentication protocol that transmits passwords in cipher text.

  On networks requiring high security, CHAP authentication is used to establish a PPP connection. In practice, CHAP authentication is widely used.

Prerequisites

PPP has been configured as the link layer protocol of the interface.

Configuration Impact

The local device performs PPP authentication on the remote device by using the authentication mode configured by the command. If PPP authentication fails, the two devices cannot communicate.

- If a domain is specified, the domain is used as the user authentication domain.
- If no domain is specified, and the user name sent from the remote device contains a domain name, this domain is used as the authentication domain. If the user name sent from the remote device does not contain any domain name, the default domain is used as the authentication domain.

Example

Configure CHAP authentication on Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp authentication-mode chap
```

Related Topics

7.2.7 link-protocol ppp
7.2.10 ppp chap user
7.2.22 ppp pap local-user

7.2.9 ppp chap password

7.2.9 ppp chap password

Function

The **ppp chap password** command configures a password for CHAP authentication.

The **undo ppp chap password** command deletes the password of CHAP authentication.

By default, no password is configured for CHAP authentication.

Format

ppp chap password { **cipher** | **simple** } *password*

undo ppp chap password

Parameters

Parameter	Description	Value
cipher	Displays the password in cipher text.	-
simple	Displays the password in plain text. **NOTE** When you specify **simple**, the password is saved in plain text in the configuration, which brings potential security risks. You are advised to specify **cipher** to save the password in the cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the password for CHAP authentication.	The value is a case-sensitive character string without spaces. If **simple** is specified, the password is in plain text and contains 1 to 32 characters. If **cipher** is specified, the password is either in cipher text containing 24 to 68 characters, for example, %^%#k5bf>8df@:_;Na'+R"U,#L#w88HE1M.L4YY2~W2u0%RDL#z#%^%#, or in plain text containing 1 to 32 characters, for example, 214357.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the PPP authentication mode is set to CHAP authentication on the authenticator by using the **ppp authentication-mode** command, you must configure the user name and password for CHAP authentication on the authenticated party.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Precautions

After the **ppp chap password** and **ppp chap user** commands are used, the device sends the configured password and user name to the remote device for authentication.

 Copyright © Huawei Technologies Co., Ltd.

The **ppp chap password** command must be used on the authenticated device, and the configured password must be the same as that configured on the authenticating device.

Example

Configure password **huawei** for CHAP authentication on Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp chap password cipher huawei@123
```

Related Topics

7.2.10 ppp chap user

7.2.8 ppp authentication-mode

7.2.10 ppp chap user

Function

The **ppp chap user** command configures a user name for CHAP authentication.

The **undo ppp chap user** command deletes the user name of CHAP authentication.

By default, no user name is configured for CHAP authentication.

Format

ppp chap user *username*

undo ppp chap user

Parameters

Parameter	Description	Value
username	Specifies a user name for CHAP authentication.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the PPP authentication mode is set to CHAP authentication by using the **ppp authentication-mode** command, you must configure the user name and password for CHAP authentication.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Precautions

After the **ppp chap password** and **ppp chap user** commands are used, the device sends the configured password and user name to the remote device for authentication.

The **ppp chap user** command must be used on the authenticated device, and the configured user name must be the same as that configured on the authenticating device.

Example

Configure user name **huawei** for CHAP authentication on Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp chap user huawei
```

Related Topics

7.2.9 ppp chap password

7.2.8 ppp authentication-mode

7.2.11 ppp compression iphc

Function

The **ppp compression iphc** command configures IP Header Compression (IPHC) on an interface of a PPP link.

The **undo ppp compression iphc** command cancels the configuration.

By default, IPHC is not configured on an interface of a PPP link.

Format

ppp compression iphc [**nonstandard**]

undo ppp compression iphc

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
nonstandard	Uses the nonstandard mode to compress RTP/UDP/IP headers. **NOTE** If this parameter is not specified, the standard mode is used to compress RTP/UDP/IP headers.	-

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPHC is an algorithm for compressing IP headers on PPP links. This algorithm compresses TCP/IP headers or RTP/IP headers to reduce the packet length and improve transmission efficiency over PPP links.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Precautions

VJHC compresses TCP/IP headers, while IPHC compresses TCP/IP headers or RTP/UDP/IP headers.

After running the **ppp compression iphc** command on an interface, restart the interface to make the configuration take effect.

You can restart an interface by using the following methods:

- Run the **shutdown** command and then the **undo shutdown** command.
- Run the **restart** command.

NOTE

Ensure that the PPP link IPHC function is configured on the peer device; otherwise, the PPP compression negotiation between the two ends fails.

Example

Configure IPHC on Serial2/0/0.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol ppp
[Huawei-Serial2/0/0] ppp compression iphc
```

Related Topics

7.2.7 link-protocol ppp

7.2.12 ppp compression iphc rtp-connections

Function

The **ppp compression iphc rtp-connections** command sets the maximum number of connections for RTP/UDP/IP header compression on an interface of a PPP link.

The **undo ppp compression iphc rtp-connections** command restores the default configuration.

By default, RTP/UDP/IP header compression is allowed on a maximum of 16 connections on an interface of a PPP link.

Format

ppp compression iphc rtp-connections *number*

undo ppp compression iphc rtp-connections

Parameters

Parameter	Description	Value
number	Sets the maximum number of connections for RTP/UDP/IP header compression.	The value is an integer that ranges from 3 to 1000.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view MP-Group interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets with the same source and destination addresses are transmitted on the same PPP link. You can run the **ppp compression iphc rtp-connections** *number* command to set the maximum number of connections for RTP/UDP/IP header compression over a PPP link. This configuration limits the number of packets that the device processes concurrently.

If the maximum numbers of connections for RTP/UDP/IP header compression are different on the compressing and decompressing ends, the smaller number takes effect after the negotiation using IP Control Protocol (IPCP).

Prerequisites

1. The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.
2. IPHC compression has been enabled on the interface of a PPP link using the **ppp compression iphc** command.

Precautions

RTP header compression is performed for the packets sent by multiple users when the packets pass through the PPP link. When the number of connections for RTP header compression exceeds the packet rate, the RTP header compression function may not take effect due to the compression aging mechanism. It is recommended that the number of connections for RTP header compression should be configured to be less than the packet rate (unit: pps).

NOTE

If the compression aging mechanism is used, the device checks compression connections once every second and ages the compression connections that are not used recently.

Example

Set the maximum number of connections for RTP/UDP/IP header compression on Serial1/0/0 to 20 in IPHC.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol ppp
[Huawei-Serial1/0/0] ppp compression iphc
[Huawei-Serial1/0/0] ppp compression iphc rtp-connections 20
```

Related Topics

7.2.7 link-protocol ppp

7.2.13 ppp compression iphc tcp-connections

Function

The **ppp compression iphc tcp-connections** command sets the maximum number of connections for TCP/IP header compression on an interface of a PPP link.

The **undo ppp compression iphc tcp-connections** command restores the default configuration.

By default, TCP/IP header compression is allowed on a maximum of 16 connections on an interface of a PPP link.

Format

ppp compression iphc tcp-connections *number*

undo ppp compression iphc tcp-connections

Parameters

Parameter	Description	Value
number	Sets the maximum number of connections for TCP/IP header compression.	The value is an integer that ranges from 3 to 256.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view MP-Group interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets with the same source and destination addresses are transmitted on the same PPP link. You can run the **ppp compression iphc tcp-connections** *number* command to set the maximum number of connections for TCP/IP header compression over a PPP link. This configuration limits the number of packets that the device processes concurrently.

If the maximum numbers of connections for TCP/IP header compression are different on the compressing and decompressing ends, the smaller number takes effect after the negotiation using IP Control Protocol (IPCP).

Prerequisites

1. The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.
2. IPHC compression has been enabled on the interface of a PPP link using the **ppp compression iphc** command.

Example

Set the maximum number of connections for TCP/IP header compression on Serial1/0/0 to 20 in IPHC.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol ppp
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Serial1/0/0] ppp compression iphc
[Huawei-Serial1/0/0] ppp compression iphc tcp-connections 20
```

Related Topics

7.2.7 link-protocol ppp

7.2.14 ppp compression stac-lzs

Function

The **ppp compression stac-lzs** command configures Stac Lempel Ziv Standard (Stac LZS) compression on an interface of a PPP link.

The **undo ppp compression stac-lzs** command cancels the configuration.

By default, Stac LZS compression is not configured on an interface of a PPP link.

Format

ppp compression stac-lzs

undo ppp compression stac-lzs

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view MP-Group interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Stac Lempel Ziv Standard (Stac LZS) compression, developed by Stac Electronics, is a standard of data compression at the link layer. Stac LZS compression compresses only the payload in a packet.

Before using Stac LZS compression, the two devices on a PPP link use the Compression Control Protocol (CCP) to negotiate with each other for a data compression algorithm. After the devices at both ends of a PPP link (an LCP link before authentication) complete authentication, the two devices check whether Stac LZS compression is enabled on the connected interfaces. If Stac LZS compression is enabled, the two devices start CCP negotiation. After CCP negotiation succeeds, the two devices transmit compressed data packets.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Precautions

After running the **ppp compression stac-lzs** command on an interface, restart the interface to make the configuration take effect.

You can restart an interface by using the following methods:

- Run the **shutdown** command and then the **undo shutdown** command.
- Run the **restart** command.

NOTE

Ensure that the PPP link STAC-LZS function is configured on the peer device; otherwise, the PPP compression negotiation between the two ends fails.

Example

Configure Stac LZS compression on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol ppp
[Huawei-Serial1/0/0] ppp compression stac-lzs
```

Related Topics

7.2.7 link-protocol ppp

7.2.15 ppp ipcp dns

Function

The **ppp ipcp dns** command enables the device to specify a DNS server address for the remote device.

The **undo ppp ipcp dns** command disables the device from specifying a DNS server address for the remote device.

By default, the device does not specify any DNS server address for the remote device.

Format

ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

undo ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

Parameters

Parameter	Description	Value
primary-dns-address	Specifies the IP address of a primary DNS server.	The value is in dotted decimal notation.

Parameter	Description	Value
secondary-dns-address	Specifies the IP address of a secondary DNS server.	The value is in dotted decimal notation.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a host connects to the device by using PPP and needs to use a domain name to access the Internet, the device must specify a DNS server address for the host.

Prerequisites

PPP has been configured as the link layer protocol of the interface.

Precautions

The **ppp ipcp dns** command cannot be used together with **ppp ipcp dns admit-any** or **ppp ipcp dns request**.

Example

Specify a DNS server address for the remote device of Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp ipcp dns 10.10.10.10 10.10.10.11
```

Related Topics

7.2.7 link-protocol ppp
7.2.16 ppp ipcp dns admit-any
7.2.17 ppp ipcp dns request

7.2.16 ppp ipcp dns admit-any

Function

The **ppp ipcp dns admit-any** command configures the device to accept the DNS server address specified by the remote device.

The **undo ppp ipcp dns admit-any** command cancels the configuration.

By default, the device cannot obtain the DNS server address specified by the remote device.

Format

ppp ipcp dns admit-any

undo ppp ipcp dns admit-any

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device connects to a remote device by using PPP and needs to use a domain name to access the Internet, you must configure the remote device to specify a DNS server address for the device.

To configure the remote device to specify a DNS server address for the device, run the **ppp ipcp dns admit-any** command to configure the device to accept the DNS server address specified by the remote device or run the **ppp ipcp dns request** command to configure the device to request a DNS server address from the remote device.

Prerequisites

PPP has been configured as the link layer protocol of the interface.

Precautions

If the device obtains a valid DNS server address from the remote device, run the **display dns server** command to view the negotiated DNS server address.

The **ppp ipcp dns admit-any** command cannot be used together with **ppp ipcp dns**.

Example

Configure Dialer0 to accept the DNS server address specified by the remote device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp ipcp dns admit-any
```

Related Topics

7.2.7 link-protocol ppp

7.2.17 ppp ipcp dns request

7.2.17 ppp ipcp dns request

Function

The **ppp ipcp dns request** command configures the device to request a DNS server address from the remote device.

The **undo ppp ipcp dns request** command restores the default configuration.

By default, the device is disabled from requesting a DNS server address from the remote device.

Format

ppp ipcp dns request

undo ppp ipcp dns request

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device connects to a remote device by using PPP and needs to use a domain name to access the Internet, you must configure the remote device to specify a DNS server address for the device.

To configure the remote device to specify a DNS server address for the device, run the **ppp ipcp dns request** command to configure the device to request a DNS server address from the remote device or run the **ppp ipcp dns admit-any** command to configure the device to accept the DNS server address specified by the remote device.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

PPP has been configured as the link layer protocol of the interface.

Precautions

If the device obtains a valid DNS server address from the remote device, run the **display dns server** command to view the negotiated DNS server address.

The **ppp ipcp dns request** command cannot be used together with **ppp ipcp dns**.

Example

Configure Dialer0 to request a DNS server address from the remote device.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp ipcp dns request
```

Related Topics

7.2.7 link-protocol ppp

7.2.16 ppp ipcp dns admit-any

7.2.18 ppp ipcp remote-address forced

Function

The **ppp ipcp remote-address forced** command configures the device to assign an IP address to the remote device. This prevents the remote device from using its configured IP address.

The **undo ppp ipcp remote-address forced** command cancels the configuration. The remote device can use its configured IP address.

By default, the remote device can use its configured IP address during IP address negotiation with the local device in the IPCP negotiation phase.

Format

ppp ipcp remote-address forced

undo ppp ipcp remote-address forced

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ppp ipcp remote-address forced** command enables the device to assign an IP address to the remote device, preventing the remote device from using its configured IP address. The **ppp ipcp remote-address forced** command must be used together with the **remote address** command.

Prerequisites

PPP has been configured as the link layer protocol of the interface.

Example

Configure Dialer0 to assign IP address 10.0.0.1 to the remote device. In this situation, the remote device can accept or reject the assigned IP address.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] remote address 10.0.0.1
```

Configure Dialer0 to forcibly assign IP address 10.0.0.1 to the remote device. In this situation, the remote device must accept the assigned IP address, and cannot accept or reject the assigned IP address.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] remote address 10.0.0.1
[Huawei-Dialer0] ppp ipcp remote-address forced
```

Related Topics

7.2.25 remote address

7.2.19 ppp ipcp default-route

Function

The **ppp ipcp default-route** command generates a default route with both the destination IP address and mask as all 0s when IPCP negotiation succeeds.

The **undo ppp ipcp default-route** deletes the default route with both the destination IP address and mask as all 0s.

Format

ppp ipcp default-route

undo ppp ipcp default-route

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure a default route to specify the default outbound interface, run the **ppp ipcp default-route** command.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Example

Generate a default route with both the destination IP address and mask as all 0s when IPCP negotiation succeeds.

```
<Huawei> system-view
[Huawei] interface serial 3/0/0
[Huawei-Serial3/0/0] ppp ipcp default-route
```

7.2.20 ppp keepalive retry-times

Function

The **ppp keepalive retry-times** command sets the number of times for retransmitting PPP heartbeat packets.

The **undo ppp keepalive retry-times** command restores the default setting.

By default, the number of times for retransmitting PPP heartbeat packets is 4.

Format

ppp keepalive retry-times *retry-times*

undo ppp keepalive retry-times

Parameters

Parameter	Description	Setting
retry-times	Specifies the number of times for retransmitting PPP heartbeat packets.	The value is an integer that ranges from 1 to 10.

 Copyright © Huawei Technologies Co., Ltd.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends PPP heartbeat packets to detect PPP link quality. When the link quality is low and the number of times for retransmitting PPP heartbeat packets reaches the upper limit, the device tears down the PPP connection.

- When services have high PPP link quality requirements and will be greatly affected by poor link quality, decrease the number of times for retransmitting PPP heartbeat packets to detect link quality and take measures in a timely manner.
- When services have low PPP link quality requirements and will be slightly affected by poor link quality, increase the number of times for retransmitting PPP heartbeat packets to prevent frequent disconnection of PPP links.

Prerequisites

PPP has been configured as the link-layer protocol of the interface.

Precautions

The command configuration on a PPP link takes effect on new online users, but not existing online users.

Example

Set the number of times for retransmitting PPP heartbeat packets to 5.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp keepalive retry-times 5
```

Related Topics

7.2.7 link-protocol ppp

7.2.21 ppp lcp remote-mru forced

Function

The **ppp lcp remote-mru forced** configures the router to force the peer to use a larger MRU in LCP negotiation. MRU stands for maximum receive unit.

The **undo ppp lcp remote-mru forced** command disables the router from forcing the peer to use a larger MRU in LCP negotiation.

 Copyright © Huawei Technologies Co., Ltd.

By default, when a router functions as a PPPoE or PPPoA client, it forces the peer to use a larger MRU in LCP negotiation; otherwise, the peer is not forced to use a larger MRU in LCP negotiation.

Format

ppp lcp remote-mru forced

undo ppp lcp remote-mru forced

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the L2TP scenario, the router functions as a LAC and other vendors' device functions as a LNS. When a PPPoE client attempts to go online in dial-up mode, it performs LCP negotiation with the LAC. After establishing an L2TP tunnel with the LNS, the LAC sends the result of LCP negotiation with the PPPoE client to the LNS. If the MRU value negotiated with the PPPoE client is smaller than the MTU value on the LNS end, the LNS sends the PPP link disconnection request and therefore the client fails to go online. In this case, you can run the **ppp lcp remote-mru forced** command on the LAC PPP interface to force the PPPoE client to use a greater MRU in LCP negotiation.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Example

Configure the router force the peer to use a larger MRU in LCP negotiation.

```
<Huawei> system-view
[Huawei] interface virtual-template 10
[Huawei-Virtual-Template10] ppp lcp remote-mru forced
```

7.2.22 ppp pap local-user

Function

The **ppp pap local-user** command configures the user name and password to be sent from the local device to the remote device in PAP authentication.

The **undo ppp pap local-user** command deletes the configured user name and password.

By default, the local device sends a request to the remote device without the user name and password in PAP authentication.

Format

ppp pap local-user *username* **password** { **cipher** | **simple** } *password*

undo ppp pap local-user

Parameters

Parameter	Description	Value
username	Specifies the user name sent from the local device to the remote device in PAP authentication.	The value is a string of 1 to 64 case-sensitive characters without spaces.
cipher	Displays the password in cipher text.	-
simple	Displays the password in plain text. **NOTE** When you specify **simple**, the password is saved in plain text in the configuration, which brings potential security risks. You are advised to specify **cipher** to save the password in the cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the password sent from the local device to the remote device in PAP authentication.	The value is a case-sensitive character string without spaces. If **simple** is specified, the password is in plain text and contains 1 to 32 characters. If **cipher** is specified, the password is either in cipher text containing 24 to 68 characters, for example, %^%#k5bf>8df@:_;Na'+R"U,#L#w88HE1M.L4YY2~W2u0%RDL#z#%^%#, or in plain text containing 1 to 32 characters, for example, 214357.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the PPP authentication mode is set to PAP authentication on the authenticator by using the **ppp authentication-mode** command, you must configure the user name and password for PAP authentication on the authenticated party.

In PAP authentication, the local device needs to send the user name and password to the remote device. The remote device checks its user table to determine whether the local device passes the authentication or sends the user name and password to the remote authentication server.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Precautions

The user name and password configured by using the **ppp pap local-user** command must be the same as those configured on the remote device.

NOTE

In PAP authentication, the password is transmitted in plain text on the network no matter whether you specify **cipher** or **simple**, which brings potential security risks.

Example

Configure user name **papuser1** and password **huawei** on Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp pap local-user papuser1 password cipher huawei@123
```

Related Topics

7.2.8 ppp authentication-mode

7.2.23 ppp peer hostroute-suppress

Function

The **ppp peer hostroute-suppress** command enables the suppression of adding the peer host route to the local routing table of direct routes.

The **undo ppp peer hostroute-suppress** command disables the suppression of adding the peer host route to the local routing table of direct routes.

By default, the local routing table of direct routes contains the peer host route.

Format

ppp peer hostroute-suppress

undo ppp peer hostroute-suppress

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PPP link does not strictly require that the peer and local IP addresses exist at the same network segment. Two ends of a PPP link with IP addresses at different

network segments can communicate with each other. In addition, one end automatically adds the host route of the other end at a different network segment to the local routing table of direct routes.

However, when one end is configured with an incorrect IP address, the other end automatically adds the incorrect peer host route to the local routing table of direct routes. As a result, the incorrect routing information is advertised across the network.

You can run the **ppp peer hostroute-suppress** or **undo ppp peer hostroute-suppress** command to enable or disable the suppression of adding the peer host route to the local routing table of direct routes.

- After you run the **ppp peer hostroute-suppress** command, the local routing table of direct routes no longer contains the peer host route.
- After you run the **undo ppp peer hostroute-suppress** command, the local routing table of direct routes contains the peer host route.

Prerequisites

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

Follow-up Procedure

Run the **shutdown** and **undo shutdown** or **restart** commands to restart the interface to make the configuration take effect.

Example

Enable the suppression of adding the peer host route to the local routing table of direct routes, and restart the interface.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp peer hostroute-suppress
[Huawei-Dialer0] shutdown
[Huawei-Dialer0] undo shutdown
```

Related Topics

7.2.7 link-protocol ppp

7.2.24 ppp timer negotiate

Function

The **ppp timer negotiate** command sets the timeout period of PPP negotiation.

The **undo ppp timer negotiate** command restores the default setting.

By default, the timeout period of PPP negotiation is 3 seconds.

Format

ppp timer negotiate *seconds*

undo ppp timer negotiate

Parameters

Parameter	Description	Value
seconds	Specifies the timeout period of PPP negotiation.	The value is an integer that ranges from 1 to 10, in seconds.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PPP negotiation, if the local end does not receive any response from the remote end within the specified timeout period, the local end retransmits the last packet until it receives a response from the remote end.

Prerequisites

PPP has been configured as the link layer protocol of the interface.

Example

Set the timeout period of PPP negotiation to 4 seconds on Dialer1.

```
<Huawei> system-view
[Huawei] interface dialer 1
[Huawei-Dialer1] ppp timer negotiate 4
```

Related Topics

7.2.7 link-protocol ppp

7.2.25 remote address

Function

The **remote address** command configures the local device to assign an IP address to or specify an IP address pool for the remote device.

The **undo remote address** command restores the default configuration.

By default, the local device does not assign any IP address to the remote device.

Format

remote address { *ip-address* | **pool** *pool-name* }

undo remote address

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address to be assigned to the remote device. **NOTE** This parameter does not take effect when the PPPoE server assigns an IP address to a PPPoE client on the VT interface.	The value is in dotted decimal notation. **NOTE** The IP address to be assigned to the remote device cannot be 0.0.0.0 or 255.255.255.255.
pool *pool-name*	Specifies the name of the IP address pool, from which an IP address is assigned to the remote device.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the remote interface is not assigned an IP address but the local device has IP addresses, you can run the **remote address** command to configure the local device to assign an IP address to or specify an IP address pool for the remote interface.

Prerequisites

The remote interface has been shut down to release its IP address.

The **ip address ppp-negotiate** command has been used to enable the remote interface to accept the IP address assigned in PPP negotiation.

The link layer protocol on the interface has been set to PPP using the **link-protocol ppp**.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If you run the **remote address** *ip-address* command multiple times in the same interface view, only the latest configuration takes effect.

To configure the local device to assign an IP address to the remote device, run the **ppp ipcp remote-address forced** command in the interface view.

Example

Specify IP address pool **pool_a** for the remote interface connecting to VT interface 10.

```
<Huawei> system-view
[Huawei] interface virtual-template 10
[Huawei-Virtual-Template10] remote address pool pool_a
```

Related Topics

7.2.5 ip address ppp-negotiate

7.2.7 link-protocol ppp

7.2.26 reset ppp compression iphc

Function

The **reset ppp compression iphc** command clears IPHC compression statistics.

Format

reset ppp compression iphc [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears IPHC compression statistics on a specified interface. If this parameter is not specified, the command clears IPHC statistics on all interfaces.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

None

Example

Clear IPHC compression statistics on Serial1/0/0.

```
<Huawei> reset ppp compression iphc interface serial 1/0/0
```

Related Topics

7.2.11 ppp compression iphc

7.2.27 reset ppp compression stac-lzs

Function

The **reset ppp compression stac-lzs** command clears Stac LZS compression statistics on an interface of a PPP link.

Format

reset ppp compression stac-lzs [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If this parameter is not specified, the command clears Stac LZS compression statistics on all interfaces.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Clear Stac LZS compression statistics on all interfaces of a PPP link.

```
<Huawei> reset ppp compression stac-lzs
```

Related Topics

7.2.11 ppp compression iphc

 Copyright © Huawei Technologies Co., Ltd.

7.2.28 timer hold (PPP)

Function

The **timer hold** command sets the interval for sending Keepalive packets.

The **undo timer hold** command restores the default setting.

By default, the interval for sending Keepalive packets is 10s.

Format

timer hold *seconds*

undo timer hold

Parameters

Parameter	Description	Value
seconds	Specifies the polling interval for an interface.	The value is an integer that ranges from 0 to 32767, in seconds. If the interval is set to 0 seconds, no Keepalive packet is sent.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, POS interface view, CPOS interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, cellular interface view, dialer interface view, virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The polling interval of an interface is the interval at which the interface sends Keepalive packets.

Keepalive packets are used to monitor and maintain the link status. If an interface does not receive any Keepalive packet after five Keepalive intervals, it considers that the link fails.

Prerequisites

PPP has been configured as the link layer protocol of the interface.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

On a low-speed link, the *seconds* parameter cannot be set to a small value because it may take a long time to transmit oversized packets on the link. If the interval for sending Keepalive packets is set to a small value, transmission of Keepalive packets is delayed. If an interface does not receive any Keepalive packet from the remote interface after five Keepalive intervals, the interface considers that the link fails.

Example

Set the interval for sending Keepalive packets to 15 seconds on Dialer0.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] link-protocol ppp
[Huawei-Dialer0] timer hold 15
```

Related Topics

7.2.7 link-protocol ppp

7.3 MP Configuration Commands

7.3.1 display interface mp-group

Function

The **display interface mp-group** command displays the MP-Group interface status.

Format

display interface mp-group [*number*]

Parameters

Parameter	Description	Value
number	Specifies the number of an MP-Group interface. If no interface number is specified, the status of all MP-Group interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the interface status or locating faults on an interface, you can run the **display interface mp-group** command to obtain the status of and statistics on the interface.

Example

Display the MP-Group interface status.

```
<Huawei> display interface mp-group
Mp-group0/0/1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Mp-group0/0/1 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 10.10.10.10/24
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened
Physical is MP, baudrate is 64000 bps
Current system time: 2011-02-09 10:21:48
   Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
   Last 300 seconds output rate 0 bytes/sec, 0 packets/sec
   Realtime 0 seconds input rate 0 bytes/sec, 0 packets/sec
   Realtime 0 seconds output rate 0 bytes/sec, 0 packets/sec
   6 packets input, 84 bytes, 0 drops
   6 packets output, 84 bytes, 0 drops
   Input bandwidth utilization  :    0%
   Output bandwidth utilization :    0%
```

Table 7-8 Description of the display interface mp-group command output

Item	Description
Mp-group0/0/1 current state	Status of MP-Group0/0/1: • UP: indicates that the interface is Up. • DOWN: indicates that the interface is Down. • Administratively down: indicates that the network administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: • UP: indicates that the link layer protocol status of the interface is Up. • DOWN: indicates that the link layer protocol status of the interface is Down or no IP address is assigned to the interface. **damping** indicates that the interface is suppressed because of frequent flapping.
Description	Description of the interface.
The Maximum Transmit Unit is	Maximum Transmission Unit (MTU) of the interface. The default MTU on a serial interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If non-fragmentation is enabled, the packets are discarded.
Internet Address is	IP address and subnet mask of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Link layer protocol is	Link layer protocol type. The link layer protocol on an MP-Group interface can only be the Point-to-Point Protocol (PPP).
LCP	Status of the Link Control Protocol (LCP). The LCP status is as follows: ● Initial: indicates that the physical layer is unavailable. ● Starting: indicates that the physical layer is starting. The device retains in Starting state for a short time. ● Closed: indicates that the device sends a Terminate-Ack packet to terminate the connection after receiving the Configure-Request packet. ● Stopped: indicates that the device receives the Configure-Request packet, but does not receive a Configure-Ack packet from the peer device. In this case, the device sends a Terminate-Ack packet. ● Closing: indicates that the connection is being closed. The device enters the Closed state if the device receives a Configure-Ack packet from the peer device or the timer expires. The device retains in Closing state for a short time. ● Stopping: indicates that the connection is being closed to prevent subsequent traffic transmission. The device retains in Stopping state for a short time. ● Req-Sent: indicates an attempt to establish a connection. The device sends a Configure-Request packet, but does not receive a Configure-Ack packet from the peer device. ● Ack-Rcvd: indicates that the device sends a Configure-Request packet and receives a Configure-Ack packet from the peer device but does not receive a Configure-Ack packet to the peer device. ● Ack-Sent: indicates that the device sends a Configure-Request packet and a Configure-Ack packet to the peer device and receives a Configure-Ack packet from the peer device. ● Opened: indicates that the device sends a Configure-Ack packet to the peer device and receives a Configure-Ack packet from the peer device. The link layer works properly.
MP	MP link status. If the MP link is in Opened state, the MP link works properly. The MP link is in Opened state only when the LCP status of all member links in the MP link is Opened.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPCP	Internet Protocol Control Protocol (IPCP) status of the MP link. If IPCP is in Opened state, the MP link works properly. The IPCP status of the MP link is Opened only when the IPCP status of the primary link in the MP link is Opened.
Physical is MP, baudrate is	The link belongs to an MP link and the interface baud is displayed.
Current system time	Current system time. If the time zone is configured and system time uses the daylight-saving-time (DST). The time is in YYYY/MM/DD HH:MM:SS UTC±HH:MM DST format.
Last 300 seconds input rate Last 300 seconds output rate	Rates of sending and receiving bytes and packets on the interface in the last 300 seconds.
packets input, bytes, drops packets output, bytes, drops	Total number of packets and bytes sent and received on the interface, and total number of packets discarded because of insufficient buffer space.

Related Topics

7.3.5 interface mp-group

7.3.2 display interface virtual-template

Function

Using the **display interface virtual-template** command, you can view the status of a virtual template (VT) interface.

Format

display interface virtual-template [*vt-number*]

Parameters

Parameter	Description	Value
vt-number	Displays the status of the specified VT interface. If no VT number is specified, the status of all VT interfaces is displayed.	The value is an integer that ranges from 0 to 1023.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display interface virtual-template** command displays the status of a VT interface, including the current physical status, link layer protocol and its status, IP address, description, output queue status, incoming and outgoing packet rates in bit/s and pps, total numbers of packets and bytes received and sent by the VT interface, and percentages of the rates for receiving and sending packets to the total bandwidth.

Example

Display the status of a specified VT interface.

```
<Huawei> display interface virtual-template 1
Virtual-Template1 current state : UP
Line protocol current state :UP (spoofing)Description:HUAWEI, AR Series, Virtual-Template1 InterfaceRoute
Port,The Maximum Transmit Unit is 1500
Internet Address is 10.1.1.1/24
Link layer protocol is PPP
LCP initial, MP opened
Physical is None, baudrate is 64000 bps
Current system time: 2007-09-06 20:57:31
    Last 300 seconds input rate 0 bits/sec, 0 packets/sec
    Last 300 seconds output rate 0 bits/sec, 0 packets/sec
    Realtime 2 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 2 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 0 bytes
    Output:0 bytes
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 7-9 Description of the display interface virtual-template command output

Item	Description
Virtual-Template1 current state	Physical status of the VT interface: ● UP: indicates that the interface works properly.
Line protocol current state	Link layer protocol status of the interface: ● UP (spoofing): indicates that the link layer protocol of the interface is always Up with the spoofing feature enabled.
Link layer protocol is	Link layer protocol.
Internet Address is	IP address assigned to the interface. If no IP address is assigned to the interface, "Internet protocol processing : disabled" is displayed.

Item	Description
LCP initial,, MP opened	Indicates the status of LCP.
Description	Description of the interface. A maximum of 242 case-sensitive characters (including spaces) can be entered. The description helps you to know the functions of the interface.
The Maximum Transmit Unit is	MTU of the interface. The default value of the MTU is 1500 bytes on a serial interface. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
Physical is None	No physical interface exists. Logical interfaces do not exist physically.
Current system time	Current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Last 300 seconds input rate Last 300 seconds output rate	Rates of the bytes and the packets that the interface sends and receives in the last 300 seconds.
Realtime 2 seconds input rate Realtime 2 seconds output rate	Real-time rates of sending and receiving the bytes and the packets within 2 seconds. It refers to the interval between two **display** commands that are run on the same interface. The maximum value is the statistical interval displayed in the previous piece of information. This entry is displayed only when information about a logical interface is viewed.
Input	Total number of packets and total number of bytes received by the interface.
Output	Total number of packets and total number of bytes sent by the interface.
Input bandwidth utilization	Percentage of the rate for receiving packets to the total bandwidth.
Output bandwidth utilization	Percentage of the rate for sending packets to the total bandwidth.

Related Topics

7.3.6 interface virtual-template

7.3.3 display ppp mp

Function

The **display ppp mp** command displays binding information and the statistics on links in an MP link.

Format

display ppp mp [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface where the MP binding information and the statistics on links in an MP link need to be displayed. If you do not specify the interface type and number, information and statistics about all the interfaces of the MP are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

- When monitoring the interface status or locating faults on an interface, you can run the **display ppp mp** command to view the status of and statistics on the interface.
- You can run the **display ppp mp** command to check whether physical interfaces are bound to the specified virtual template interface, check whether the binding mode is direct binding or authentication binding, and check whether physical interfaces are bound to the MP-Group interface.

Prerequisites

The MP configurations at both ends are complete and member interfaces have been restarted at both ends.

Example

Display the MP binding information and the statistics about links in an MP link on the virtual template interface **virtual template 1**.

```
<Huawei> display ppp mp interface virtual-template 1
Template is Virtual-Template1
 Bundle quid0, 2 member, slot 0, Master link is Virtual-Template1:0
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The bundled son channels are:
     Serial1/0/0
     Serial1/0/1
```

Table 7-10 Description of the display ppp mp interface virtual-template command output

Item	Description
Template is Virtual-Template1	Used virtual template interface is Virtual-Template1.
Bundle	Remote user name of the bound link is quid0. Information following Bundle varies according to the MP binding mode: ● If the MP binding condition is **authentication**, the remote user name is displayed. ● If the MP binding condition is **descriptor**, the remote endpoint discriminator is displayed. ● If the MP binding condition is **both**, the remote user name or remote endpoint discriminator is displayed. **NOTE** An endpoint discriminator is represented in ASCII format. For example, the value 733000000000 indicates that the endpoint discriminator is s0. A user name is a string of characters. For example, the value s0 indicates that the user name is s0.
member	Number of bound links is two.
slot	Slot ID.
Master link is Virtual-Template1	Virtual template interface number and virtual access interface number of the primary link.
lost fragments	Number of fragments discarded in the inbound direction.
reordered	Number of reassembled packets in the inbound direction.
unassigned	Number of packets to be reassembled in the inbound direction.
interleaved	Number of sent Link Fragmentation and Interleaving (LFI) fragments.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
sequence 0/0 rcvd/sent	Receiving or transmitting sequence number.
The bundled son channels are	Local interfaces corresponding to PPP links in an MP link.

Display the MP binding information and bound links on the MP-Group interface.

```
<Huawei> display ppp mp interface mp-group 0/0/1
Mp-group is Mp-group0/0/1
 ===========Sublinks status begin======
 Serial1/0/0 physical UP,protocol UP
 Serial2/0/0 physical UP,protocol UP
 ===========Sublinks status end========
 Bundle Multilink, 2 members, slot 0, Master link is Mp-group0/0/1
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The bundled sub channels are:
      Serial1/0/0
      Serial2/0/0
```

Table 7-11 Description of the display ppp mp interface mp-group command output

Item	Description
Mp-group is Mp-group0/0/1	Used MP-Group interface is MP-Group 0/0/1.
Serial physical, protocol	Name of the physical interface and its physical status and link layer protocol status. ● Up: The physical layer or the link layer of the interface is Up. ● Down: The physical layer or the link layer of the interface is Down. **damping** indicates that the interface is suppressed because of frequent flapping.
Bundle Multilink, member, slot, Master link is	Number of valid bound links, slot ID, and bound interface.
lost fragments	Number of fragments discarded in the inbound direction.
reordered	Number of reassembled packets in the inbound direction.
unassigned	Number of packets to be reassembled in the inbound direction.
sequence rcvd/sent	Receiving or transmitting sequence number.
The bundled sub channels are	Local interfaces corresponding to PPP links in an MP link.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.2.7 link-protocol ppp
7.3.7 ppp mp
7.3.20 ppp mp virtual-template

7.3.4 discriminator

Function

The **discriminator** command enables the terminal discriminator negotiation function.

The **undo discriminator** command disables the terminal discriminator negotiation function.

By default, the terminal discriminator negotiation function is enabled.

Format

discriminator

undo discriminator

Parameters

None

Views

MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device performs MP connections with other vendors' devices using MP-Group links, if other vendors' devices cannot identify the device's terminal discriminator, the connection fails. You can run the **undo discriminator** command in the MP-Group interface view to disable the terminal discriminator negotiation function.

Precautions

Run the **shutdown** and **undo shutdown** or **restart** command to restart the physical interface to make the configuration take effect.

Example

Disable the terminal discriminator negotiation function on the interface MP-Group0/0/1.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface mp-group 0/0/1
[Huawei-Mp-group0/0/1] undo discriminator
```

7.3.5 interface mp-group

Function

The **interface mp-group** command creates an MP-Group interface and enters the MP-Group interface view.

The **undo interface mp-group** command deletes a specified MP-Group interface.

By default, no MP-Group interface is created.

Format

interface mp-group *number*

undo interface mp-group *number*

Parameters

Parameter	Description	Value
number	Specifies the number of an MP-Group interface.	The value is in the 0/0/*sequence number* format. The sequence number range varies according to the device types.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MP binding by using an MP-Group interface, you need to first create an MP-Group interface.

Follow-up Procedure

Run the **ppp mp mp-group** command to bind an interface to the MP-Group interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create MP-Group interface 0/0/1.

```
<Huawei> system-view
[Huawei] interface mp-group 0/0/1
[Huawei-Mp-group0/0/1]
```

Related Topics

7.3.18 ppp mp mp-group

7.3.6 interface virtual-template

Function

Using the **interface virtual-template** command, you can create a virtual template (VT) interface and enter the VT interface view.

Using the **undo interface virtual-template** command, you can delete a VT interface.

Format

interface virtual-template *vt-number*

undo interface virtual-template *vt-number*

Parameters

Parameter	Description	Value
vt-number	Specifies the number of a VT interface.	The VE sequence number range depends on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Layer 2 protocols such as PPP and ATM cannot transmit packets of each other, and need to communicate by using virtual access (VA) interfaces. When Layer 2 protocols need to communicate, the system automatically creates a VA interface. You can configure a VA interface only by setting attributes for a VT interface. A VT interface is used by the system to configure VA interfaces.

Prerequisites

A VT interface has been created before the system creates a VA interface.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After a VT interface is deleted, all of its derived VA interfaces are deleted automatically.

The link layer protocol of a VT interface is Up only when VA interfaces in Up state exist on the VT interface.

Example

Create VT interface 10.

```
<Huawei> system-view
[Huawei] interface virtual-template 10
[Huawei-Virtual-Template10]
```

Related Topics

7.3.2 display interface virtual-template

7.3.7 ppp mp

Function

The **ppp mp** command configures a PPP interface to work in MP mode.

The **undo ppp mp** command configures a PPP interface to work in PPP mode.

By default, a PPP interface works in PPP mode.

Format

ppp mp

undo ppp mp

Parameters

None

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, 3G Cellular interface view, dialer interface view, virtual template interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To increase link bandwidth, you can bind multiple PPP links into an MP link. To implement MP binding, interfaces must work in MP mode.

 Copyright © Huawei Technologies Co., Ltd.

The following table lists the MP implementation types and principles.

Type	Subtype	Characteristic
Using a VT	Binding PPP links to a VT	Multiple interfaces are bound to a VT. This method is simple but does not ensure high security.
	Searching for a VT using the user name of the PPP link	The system searches for the bound VT using the authenticated remote user name. Links with the same user name are bound to the same VT. This method is flexible but the configuration is complex.
Using an MP-Group	Adding PPP links to an MP-Group	An MP-Group interface is dedicated to MP applications. MP is implemented by binding multiple interfaces to an MP-Group interface. This method is efficient and the configuration is simple. It is widely used on networks.

When configuring MP implemented by searching for a VT using the user name of the PPP link, run this command.

Prerequisites

The user name has been associated with the VT interface by using the **ppp mp user** command.

Precautions

- You must configure bidirectional PPP authentication on the interface.
- Interfaces must be bound to one VT interface in the same mode.
- The **ppp mp** command and the **ppp mp virtual-template** command are exclusive. That is, you can configure only MP direct binding or MP authentication binding by using a VT interface.

Example

Configure Dialer0 to work in MP mode.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp mp
```

Related Topics

7.3.19 ppp mp user

7.3.8 ppp mp binding-mode

Function

The **ppp mp binding-mode** command configures a PPP binding mode.

The **undo ppp mp binding-mode** command restores the default PPP binding mode.

By default, PPP binding is performed based on the remote user name and remote endpoint discriminator. That is, the PPP binding mode is **both**.

Format

ppp mp binding-mode { **authentication** | **descriptor** | **both** }

undo ppp mp binding-mode

Parameters

Parameter	Description	Value
authentication	Indicates that the remote user name is used for PPP binding.	-
descriptor	Indicates that the remote endpoint discriminator is used for PPP binding.	-
both	Indicates that the remote user name and remote endpoint discriminator are used for MP binding.	-

Views

Virtual template interface view, Dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a virtual template interface is used to implement MP, multiple MP bundles can be formed and each MP bundle corresponds to one MP link, regardless of how MP

 Copyright © Huawei Technologies Co., Ltd.

binding is implemented. To differentiate MP bundles formed by using a virtual template interface, specify the binding mode using the **ppp mp binding-mode** command in the virtual template interface view. The command supports three binding modes: **authentication**, **descriptor**, and **both**. The default binding mode is **both**.

- If the MP binding mode is **authentication**, links with the same remote user name are bound to the same MP bundle.
- If the MP binding condition is **descriptor**, links with the same remote endpoint discriminator through LCP negotiation are bound to the same MP bundle.
- If the MP binding mode is **both**, links with the same remote user name and remote endpoint discriminator are bound to the same MP bundle.

Follow-up Procedure

Run the **shutdown** and **undo shutdown** or **restart** commands to restart the related physical interface to make the configuration take effect.

Precautions

The local and remote devices must have the same MP binding mode; otherwise, errors occur in MP negotiation.

Example

Configure MP binding by using VT interface 1 according to the remote user name.

```
<Huawei> system-view
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] ppp mp binding-mode authentication
```

7.3.9 ppp mp endpoint

Function

The **ppp mp endpoint** command configures the Endpoint option content for LCP negotiation when an interface works in MP mode.

The **undo ppp mp endpoint** command configures the default Endpoint option content for LCP negotiation when an interface works in MP mode.

By default, the Endpoint option content for LCP negotiation is a random number.

Format

ppp mp endpoint *endpoint-name*

undo ppp mp endpoint

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
endpoint-name	Specifies the Endpoint option content for LCP negotiation.	The value is a string of 1 to 20 case-sensitive characters without spaces.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, 3G Cellular interface view, dialer interface view, virtual template interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Endpoint option content (the endpoint discriminator) is an MP negotiation option. The Endpoint option is negotiated in LCP negotiation.

If multiple MP links are created on a device, you can use the **ppp mp endpoint** command to modify the Endpoint option content to distinguish different MP links.

You can choose to use the **ppp mp endpoint** command when running the **ppp mp binding-mode** command to set the binding mode to **both** or **descriptor**.

Follow-up Procedure

Run the **shutdown** and **undo shutdown** or **restart** commands to restart the related physical interface to make the configuration take effect.

Precautions

The maximum length of the Endpoint option content is 20 characters. If the length of the Endpoint option content exceeds 20 characters, the first 20 characters are used as the Endpoint option content.

Example

Configure the Endpoint option content of Dialer0 as **Router1**.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp mp endpoint Router1
```

Related Topics

7.3.8 ppp mp binding-mode

7.3.10 ppp mp fragment enable

Function

The **ppp mp fragment enable** command enables MP packet fragmentation.

The **undo ppp mp fragment enable** command disables MP packet fragmentation.

By default, MP packet fragmentation is disabled.

Format

ppp mp fragment enable

undo ppp mp fragment enable

Parameters

None

Views

Virtual template interface view, Dialer interface view, MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Large-sized packets require a longer transmission time and occupy a link for a long time. If subsequent packets need to be forwarded in real time, there may be a delay and user experience is low. To solve the problem, run the **ppp mp fragment enable** command to enable MP packet fragmentation so that fragments of small-sized packets and large-sized packets are sent to a queue.

If MP packet fragmentation is not required, run the **undo ppp mp fragment enable** command.

Precautions

MP packet fragmentation is not required on a link with bandwidth greater than 768 kbit/s.

Example

Disable MP packet fragmentation.

```
<Huawei> system-view
[Huawei] interface Virtual-Template 1
[Huawei-Virtual-Template1] undo ppp mp fragment enable
```

7.3.11 ppp multichassis-mp enable

Function

The **ppp multichassis-mp enable** command enables Multi-Chassis Multilink PPP (MMP) on an MP member interface.

The **undo ppp multichassis-mp enable** command disables MMP on an MP member interface.

By default, MMP is disabled on an MP member interface.

Format

ppp multichassis-mp enable

undo ppp multichassis-mp enable

Parameters

None

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow MP member interfaces of different access servers to receive multiple dialup requests sent by the same branch device and terminate the requests in the same MP bundle, run the **ppp multichassis-mp enable** command on MP member interfaces. In this case, the MP member interfaces are bound to the same MP bundle.

Precautions

The MP member interfaces bound to the same MP bundle must be configured with the same endpoint discriminator or user name so that the branch device can bind the PPP links.

Example

Enable MMP on the ISDN PRI interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] ppp multichassis-mp enable
```

 Copyright © Huawei Technologies Co., Ltd.

7.3.12 ppp mp least active-linknumber

Function

The **ppp mp least active-linknumber** command sets the lower threshold for the number of links bundled into an MP-Group interface.

The **undo ppp mp least active-linknumber** command restores the lower threshold for the number of links bundled into an MP-Group interface.

By default, the lower threshold for the number of links bundled into an MP-Group interface is 1.

Format

ppp mp least active-linknumber *value*

undo ppp mp least active-linknumber

Parameters

Parameter	Description	Value
value	Specifies the lower threshold for the number of links bundled into an MP-Group interface.	The value is an integer that ranges from 1 to 32.

Views

MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an MP-Group interface is used to implement MP, the MP bandwidth is the sum of the bandwidths of all the PPP links that are in Up state and bundled into the MP-Group interface. To meet the bandwidth requirements of user services, you can run this command to set the lower threshold for the number of bundled links in the MP-Group interface to ensure the minimum available MP bandwidth.

After LCP negotiation succeeds, NCP negotiation is performed only when the number of MP bundled links reaches the lower threshold. If NCP negotiation succeeds, MP becomes available.

If a bundled PPP link goes Down when the MP is available, the number of bundled PPP links in an MP-Group interface falls below the lower threshold, the MP-Group interface goes Down accordingly.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

- When the number of available PPP links in an MP-Group interface is less than the lower threshold configured using the **ppp mp threshold-least number** command, the MP-Group interface goes Down immediately.
- When the number of available PPP links in an MP-Group interface is more than or equal to the lower threshold configured using the **ppp mp threshold-least number** command, the MP-Group interface goes Up immediately.

Example

Set the lower threshold for the number of links bundled into an MP-Group interface to 2.

```
<Huawei> system-view
[Huawei] interface Mp-group 0/0/1
[Huawei-Mp-group0/0/1] ppp mp least active-linknumber 2
```

7.3.13 ppp mp lfi

Function

The **ppp mp lfi** command, enables LFI.

The **undo ppp mp lfi** command disables LFI.

By default, LFI is disabled on an interface.

Format

ppp mp lfi

undo ppp mp lfi

Parameters

None

Views

Virtual template interface view, Dialer interface view, MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Large packets require a longer transmission period of time and occupy a link for a long period. If subsequent packets such as voice packets need to be forwarded in real time, there may be a delay and user experience. To solve the problem, fragment packets and place fragments of small packets and large packets to the queue.

 Copyright © Huawei Technologies Co., Ltd.

To fragment and reassemble packets, enable LFI.

Configuration Impact

- After the **ppp mp lfi** command is used, LFI is enabled. LFI divides large frames into small frames. Then the small frames and other small fragments are sent together. The delay and jitter on a link at a slow rate are reduced. The divided frames are reassembled at the destination.
- After the **ppp mp lfi** command is run, the fragment size is not determined by the **ppp mp min-fragment** command. Instead, the fragment size is determined by both the maximum delay of an LFI fragment and the interface committed information rate (CIR).
- After LFI is enabled, the formula for calculating the LFI fragment size is as follows: LFI fragment size = (maximum fragment delay x interface CIR)/8 The maximum delay of an LFI fragment is set by using the **ppp mp lfi delay-per-frag** command, and the interface CIR is set by using the **qos gts** command. If the interface CIR is not set, the LFI fragment size is fixed to 500 bytes.
- After LFI is enabled on an interface, voice packets sent from the interface are placed into a protocol queue. Packets in a protocol queue are scheduled in Strict Priority (SP) mode. Packets in other queues can be scheduled only after packets in protocol queues are scheduled.

Example

Enable LFI on the interface **Virtual-Template1**.

```
<Huawei> system-view
[Huawei] interface Virtual-Template 1
[Huawei-Virtual-Template1] ppp mp lfi
```

Related Topics

7.3.14 ppp mp lfi delay-per-frag

7.3.14 ppp mp lfi delay-per-frag

Function

The **ppp mp lfi delay-per-frag** command sets the maximum delay of an LFI fragment.

The **undo ppp mp lfi delay-per-frag** command restores the default maximum delay of an LFI fragment.

By default, the maximum delay of an LFI fragment is 10 ms.

Format

ppp mp lfi delay-per-frag *max-delay*

undo ppp mp lfi delay-per-frag

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-delay	Specifies the maximum delay of an LFI fragment.	The value is an integer that ranges from 1 to 1000, in ms.

Views

Virtual template interface view, Dialer interface view, MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

If an LFI fragment does not reach the destination within the maximum delay, it is discarded. A packet may fail to be reassembled if its fragments are lost. Therefore, set the maximum delay of an LFI fragment properly.

Example

Enable LFI on Virtual-Template1 and set the maximum delay of an LFI fragment to 20 ms.

```
<Huawei> system-view
[Huawei] interface Virtual-Template 1
[Huawei-Virtual-Template1] ppp mp lfi
[Huawei-Virtual-Template1] ppp mp lfi delay-per-frag 20
```

Related Topics

7.3.13 ppp mp lfi

7.3.15 ppp mp max-bind

Function

The **ppp mp max-bind** command sets the maximum number of links in an MP link.

The **undo ppp mp max-bind** command restores the default maximum number of links in an MP link.

By default, the maximum number of links in an MP link is 16.

Format

ppp mp max-bind *max-bind-number*

undo ppp mp max-bind

Parameters

Parameter	Description	Value
max-bind-number	Specifies the maximum number of links in an MP link.	The value ranges from 1 to 32. You are advised to use the default maximum number of links in an MP link.

Views

Virtual template interface view, Dialer interface view, MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the sum of bandwidth of PPP links from exceeding the specified bandwidth, configure the maximum number of PPP links in an MP link.

Follow-up Procedure

Run the **shutdown** and **undo shutdown** commands or the **restart** command to restart member interfaces to make the configuration take effect.

NOTE

After the **ppp mp max-bind** command is executed on the synchronous serial interface formed by bundling timeslots on the CE1, CT1, or CPOS interface, you only need to run the **shutdown** and **undo shutdown** commands or the **restart** command on the CE1, CT1, or CPOS interface.

Precautions

- A maximum of 32 member interfaces can be added to an MP link. If more than 32 member interfaces join an MP link, excess MP member interfaces that fail to be bundled become Down after LCP negotiation and enter the LCP negotiation state again. In this case, the excess MP member interfaces alternate between Up and Down.
- The **ppp mp max-bind** command is not recommended because PPP performance may be deteriorated after the **ppp mp max-bind** command is used. Use the **ppp mp max-bind** command under the instruction of Huawei technical personnel.
- If the number of links in an MP link reaches the maximum value, new available PPP links cannot join the MP.
- To make this command take effect, ensure that there is no member link in the MP-Group. Before bundling MP member links, run the **ppp mp max-bind** command to set the maximum number of links in an MP link.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum number of links in an MP link to 20 on Virtual-Template 1.

```
<Huawei> system-view
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] ppp mp max-bind 20
```

7.3.16 ppp mp min-fragment

Function

The **ppp mp min-fragment** command sets the minimum length of outgoing MP packets to be fragmented.

The **undo ppp mp min-fragment** command restores the default minimum length of outgoing MP packets to be fragmented.

By default, the minimum length of outgoing MP packets to be fragmented is 500 bytes.

Format

ppp mp min-fragment *size*

undo ppp mp min-fragment

Parameters

Parameter	Description	Value
size	Specifies the minimum length of outgoing MP packets to be fragmented. Only the outgoing MP packets whose length is greater than the value are fragmented.	The value is an integer that ranges from 128 to 1500, in bytes. You are advised to use the default minimum length of outgoing MP packets to be fragmented.

Views

Virtual template interface view, dialer interface view, MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Oversized packets require a longer transmission period and occupy a link for a long period. If subsequent packets need to be forwarded in real time, a delay may

occur, affecting user experience. To address this problem, fragment oversized packets into small-sized packets for transmission.

You can use the **ppp mp min-fragment** command to set the minimum length of outgoing MP packets to be fragmented.

NOTE

The outgoing MP packet fragment length depends on the number of links and the minimum length of outgoing MP packets to be fragmented. If the number of bundled links is *N* and the minimum length of outgoing MP packets to be fragmented is *size*, the formula is as follows:

n = Original packet size/*size*

Actual fragment size = Packet size/Smaller value between *N* and *n*

Example:

- When four links are bundled, the original packet size is 1000 bytes, *size* is set to 500 bytes, and the packet is divided into two fragments, the actual fragment size is 500 bytes.
- When four links are bundled, the original packet size is 1000 bytes, *size* is set to 150 bytes, and the packet is divided into four fragments, the actual fragment size is 250 bytes.

NOTE

The **ppp mp min-fragment** command takes effect only when LFI is disabled. After LFI is enabled, the minimum length of outgoing MP packets to be fragmented is determined by both the delay and bandwidth. For details, see **ppp mp lfi**.

Example

Set the minimum length of outgoing MP packets to be fragmented to 256 bytes on the interface **Virtual-Template1**.

```
<Huawei> system-view
[Huawei] interface Virtual-Template 1
[Huawei-Virtual-Template1] ppp mp fragment enable
[Huawei-Virtual-Template1] ppp mp min-fragment 256
```

7.3.17 ppp mp reorder-window size

Function

The **ppp mp reorder-window size** command configures the sliding window size when MP reassembles received fragments.

The **undo ppp mp reorder-window size** command restores the default setting.

By default, the MP sliding window size is 64.

Format

ppp mp reorder-window size *size*

undo ppp mp reorder-window size

Parameters

Parameter	Description	Value
size	Specifies the sliding window size, or the number of fragments allowed in the MP sliding window.	The value ranges from 64 to 1024.

Views

Virtual template interface view, Dialer interface view, MP-Group interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device receives traffic containing large-sized packets and exceeding the physical bandwidth of the MP binding, the device fails to reassemble the fragmented packets. This command adjusts the number of fragments allowed in the MP sliding window on the device, reducing failures to reassemble fragments.

Configuration Impact

If you run the **ppp mp reorder-window size** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the sliding window size to 200.

```
<Huawei> system-view
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] ppp mp reorder-window size 200
```

7.3.18 ppp mp mp-group

Function

The **ppp mp mp-group** command binds an interface to the MP-Group interface so that the interface works in MP mode.

The **undo ppp mp** command configures an interface to work in PPP mode.

By default, an interface works in PPP mode.

Format

ppp mp mp-group *number*

undo ppp mp

Parameters

Parameter	Description	Value
number	Specifies the number of an MP-Group interface.	An MP-Group interface has been created by using the **interface mp-group** command.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, POS interface view, CPOS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To increase link bandwidth, you can bind multiple PPP links into an MP link. To implement MP binding, interfaces must work in MP mode.

The following table describes the MP binding modes.

Type	Subtype	Characteristic
Using a VT	Binding PPP links to a VT	Multiple interfaces are bound to a VT. This method is simple but does not ensure high security.
	Searching for a VT using the user name of the PPP link	The system searches for the bound VT using the authenticated remote user name. Links with the same user name are bound to the same VT. This method is flexible but the configuration is complex.

 Copyright © Huawei Technologies Co., Ltd.

Type	Subtype	Characteristic
Using an MP-Group interface	Adding PPP links to an MP-Group	An MP-Group interface is dedicated to MP applications. MP is implemented by binding multiple interfaces to an MP-Group interface. This method is efficient and the configuration is simple. It is widely used on networks.

When configuring MP implemented by binding PPP links to an MP-Group interface, run this command.

Prerequisites

An MP-Group interface has been created by using the **interface mp-group** command.

Example

Bind Serail2/0/0 to MP-Group0/0/1.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] ppp mp mp-group 0/0/1
```

Related Topics

7.3.5 interface mp-group

7.3.19 ppp mp user

Function

The **ppp mp user** command associates the user name with a virtual template interface.

The **undo ppp mp user** command unbinds the user name from a virtual template interface.

Format

ppp mp user *username* **bind virtual-template** *vt-number*

undo ppp mp user *username*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
username	Specifies the user name of the remote device, which is obtained in PAP or CHAP authentication on a PPP link.	The value is a string of 1 to 64 characters.
bind virtual-template *vt-number*	Specifies the number of the virtual template interface bound to the user name of the remote device.	The value is an integer that ranges from 0 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MP authentication binding by using a virtual template interface, run the **ppp mp user** command. The device searches for the associated virtual template interface according to the user name of the remote device obtained in authentication.

Follow-up Procedure

Run the **ppp mp** command on the bound interface and configure bidirectional PPP authentication.

Run the **shutdown** and **undo shutdown** or **restart** commands to restart member interfaces to make the configuration take effect.

Example

Associate the user **user1** with virtual template interface 1.

```
<Huawei> system-view
[Huawei] ppp mp user user1 bind virtual-template 1
```

7.3.20 ppp mp virtual-template

Function

The **ppp mp virtual-template** command sets the number of the VT interface bound to an interface so that the interface works in MP mode.

The **undo ppp mp** command unbinds an interface from a VT interface so that the interface works in PPP mode.

By default, an interface works in PPP mode.

Format

ppp mp virtual-template *vt-number*

undo ppp mp

Parameters

Parameter	Description	Value
vt-number	Specifies the number of the VT interface.	The value is an integer that ranges from 0 to 1023.

Views

Serial interface view, Async interface view, ISDN BRI interface view, E1-F interface view, CE1/PRI interface view, CE3 interface view, T1-F interface view, CT1/PRI interface view, virtual template interface view, CPOS interface view, POS interface view, dialer interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To increase link bandwidth, you can bind multiple PPP links into an MP link. To implement MP binding, interfaces must work in MP mode.

The following table describes the MP binding modes.

Type	Subtype	Characteristic
Using a VT	Binding PPP links to a VT	Multiple interfaces are bound to a VT. This method is simple but does not ensure high security.

 Copyright © Huawei Technologies Co., Ltd.

Type	Subtype	Characteristic
	Searching for a VT using the user name of the PPP link	The system searches for the bound VT using the authenticated remote user name. Links with the same user name are bound to the same VT. This method is flexible but the configuration is complex.
Using an MP-Group interface	Adding PPP links to an MP-Group	An MP-Group interface is dedicated to MP applications. MP is implemented by binding multiple interfaces to an MP-Group interface. This method is efficient and the configuration is simple. It is widely used on networks.

When configuring MP implemented by binding PPP links to a VT, run this command.

Precautions

- Interfaces must be bound to one VT interface in the same mode.
- The **ppp mp virtual-template** command and the **ppp mp** command are exclusive. That is, you can configure only MP direct binding or MP authentication binding by using a VT interface. The configuration of ppp mp virtual-template limitations is 200 on the device.
- The VT interface specified in this command can be a VT interface that has been created or is not created. If the specified VT interface is not created, run the **interface virtual-template** command after running the **ppp mp virtual-template** command to create a VT interface.
- When PPP links are bound to a VT in the VT interface view, services directly configured in the VT interface view do not take effect. For example, in Example 2, if VT interface 0 is bound to VT interface 1, services (such as IP address and QoS) configured on VT interface 0 do not take effect. The services take effect only when you configure them on VT interface 1.

Example

Bind Serial1/0/0 to VT interface 1 so that Serial1/0/0 works in MP mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ppp mp virtual-template 1
```

Bind VT interface 0 to VT interface 1 so that VT interface 0 works in MP mode.

```
<Huawei> system-view
[Huawei] interface virtual-template 0
[Huawei-Virtual-Template0] ppp mp virtual-template 1
```

7.4 PPPoE Commands

7.4.1 display pppoe-client session

Function

The **display pppoe-client session** command displays information about PPPoE sessions on the PPPoE client, including the session status and statistics.

Format

display pppoe-client session { **packet** | **summary** } [**dial-bundle-number** *number*]

Parameters

Parameter	Description	Value
packet	Displays the packet statistics of PPPoE sessions.	-
summary	Displays summary of PPPoE sessions.	-
dial-bundle-number *number*	Displays statistics about a specified PPPoE session.	The value of *number* is an integer that ranges from 1 to 255. If this parameter is not specified, statistics about all PPPoE sessions are displayed.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor PPPoE sessions on the PPPoE client, use this command to obtain the session status and statistics. You can locate PPPoE faults according to the command output.

Example

Display the summary of all PPPoE sessions on the PPPoE client.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display pppoe-client session summary
PPPoE Client Session:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
1    1       1       GE1/0/0       00e0fc030201  0819a6cd0680  UP
```

Table 7-12 Description of the display pppoe-client session summary command output

Item	Description
ID	ID of a PPPoE session.
Bundle	Dialer bundle of the PPPoE session.
Dialer	Number of the dialer interface.
Intf	Physical interface to which the dialer interface is bound.
Client-MAC	MAC address of the PPPoE client.
Server-MAC	MAC address of the PPPoE server.
State	Status of the PPPoE session. ● IDLE: indicates that the PPPoE session is idle. ● PADI: indicates that the PPPoE session is at the Discovery stage and a PPPoE Active Discovery Initiation (PADI) packet has been sent. ● PADR: indicates that the PPPoE session is at the Discovery stage and a PPPoE Active Discovery Request (PADR) packet has been sent. ● UP: indicates that the PPPoE session has been established successfully.

Display packet statistics of all PPPoE sessions on the PPPoE client.

```
<Huawei> display pppoe-client session packet
PPPoE Client Session:
ID     InP       InO       InD       OutP      OutO      OutD
1      36        758       0         50        1222      0
```

Table 7-13 Description of the display pppoe-client session packet command output

Item	Description
ID	ID of a PPPoE session.
InP	Number of received packets.
InO	Number of received bytes.
InD	Number of incoming packets that are discarded.
OutP	Number of sent packets.

Item	Description
OutO	Number of sent bytes.
OutD	Number of outgoing packets that are discarded.

7.4.2 display pppoe-server session

Function

The **display pppoe-server session** command displays information about PPPoE sessions on the PPPoE server, including the session status and statistics.

Format

display pppoe-server session { **all** | **packet** }

Parameters

Parameter	Description	Value
all	Displays information about all PPPoE sessions.	-
packet	Displays the packet statistics of PPPoE sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor PPPoE sessions on the PPPoE server, use this command to obtain the session status and statistics. You can locate PPPoE faults according to the command output.

Example

Display information about all PPPoE sessions on the PPPoE server.

```
<Huawei> display pppoe-server session all
Total Session: 1
SID      Intf                  State   OIntf          RemMAC         LocMAC
1        Virtual-Template1        UP     GE1/0/0        00e0.fc03.0201 0819.a6cd.0680
```

Table 7-14 Description of the display pppoe-server session all command output

Item	Description
Total Session	Total number of PPPoE sessions.
SID	ID of a PPPoE session.
Intf	Number of the virtual template interface corresponding to the PPPoE session.
State	Status of the PPPoE session.
OIntf	Ethernet interface on which the PPPoE session is established.
RemMAC	MAC address of the PPPoE client.
LocMAC	MAC address of the PPPoE server.

Display the statistics about PPPoE sessions.

```
<Huawei> display pppoe-server session packet
SID     RemMAC        LocMAC          InP      InO   InD     OutP     OutO  OutD
1    00e0fc030201 0819a6cd0680       34      738     0       34      738     0
```

Table 7-15 Description of the display pppoe-server session packet all command output

Item	Description
SID	ID of a PPPoE session.
RemMAC	MAC address of the PPPoE client.
LocMAC	MAC address of the PPPoE server.
InP	Number of received packets.
InO	Number of received bytes.
InD	Number of incoming packets that are discarded.
OutP	Number of sent packets.
OutO	Number of sent bytes.
OutD	Number of outgoing packets that are discarded.

Related Topics

7.4.7 pppoe-server bind virtual-template

7.4.3 ppp keepalive in-traffic check

Function

The **ppp keepalive in-traffic check** command disables the device functioning as a PPPoE server from sending heartbeat packets when it receives packets.

The **undo ppp keepalive in-traffic check** command enables the virtual template interface to send heartbeat packets when it receives packets.

By default, the device functioning as a PPPoE server periodically sends heartbeat packets.

Format

ppp keepalive in-traffic check

undo ppp keepalive in-traffic check

Parameters

None

Views

Virtual template view

Default Level

2: Configuration level

Usage Guidelines

When a large number of users access the device functioning as a PPPoE server to decrease occupation of network resources by heartbeat packets, you can run the **ppp keepalive in-traffic check** command to disable the device from sending heartbeat packets when it receives packets.

Example

Disable the device functioning as a PPPoE server from sending heartbeat packets when it receives packets.

```
<Huawei> system-view
[Huawei] interface virtual-template 10
[Huawei-Virtual-Template10] ppp keepalive in-traffic check
```

7.4.4 pppoe-client dial-bundle-number

Function

The **pppoe-client dial-bundle-number** command specifies a dialer bundle of a PPPoE session on an interface.

The **undo pppoe-client dial-bundle-number** command unbinds the dialer bundle from the PPPoE session.

By default, no dialer bundle is specified.

Format

pppoe-client dial-bundle-number *number* [**on-demand**] [**no-hostuniq**] [**ppp-max-payload** *value*] [**service-name** *name*]

undo pppoe-client dial-bundle-number *number*

Parameters

Parameter	Description	Value
number	Specifies the dialer bundle of a PPPoE session.	The value is an integer that ranges from 1 to 255. This parameter uniquely identifies a PPPoE session and can be used as the ID of a PPPoE session.
on-demand	Configures on-demand dialing on the PPPoE client.	-
no-hostuniq	Indicates that the session initiated by the PPPoE client does not contain the Host-Uniq field. By default, the session initiated by the PPPoE client contains the Host-Uniq field.	-
ppp-max-payload *value*	Specifies the maximum value of the MTU of PPP negotiation during the establishment of a PPPoE session.	The value is an integer that ranges from 64 to 1976. The default value is 1500.
service-name *name*	Specifies the value of the **Service-Name** field in packets sent by a PPPoE client in the Discovery stage. When users want to establish sessions with the PPPoE server providing specific services, specify **service-name** in this command.	The value is a string of 1 to 128 case-sensitive characters without spaces and special characters such as asterisk (*), question mask (?), and quotation mask ('').

Views

Ethernet interface view, Ethernet sub-interface view, GE interface view, GE sub-interface view, XGE interface view, XGE sub-interface view, Layer 3 virtual Ethernet interface view, virtual Ethernet sub-interface view, PON interface view, PON sub-interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PPPoE session can be created on a physical Ethernet interface, a PON interface, or a virtual Ethernet interface bound to an ADSL interface. When the device uses an ADSL interface to connect to the Internet directly, run the **pppoe-client dial-bundle-number** command on the virtual Ethernet interface bound to the ADSL interface. When the device uses an Ethernet interface to connect to an ADSL modem, run the **pppoe-client dial-bundle-number** command on the Ethernet interface.

NOTE

The Ethernet interface must be a WAN-side Ethernet interface. LAN-side Ethernet interfaces do not support PPPoE.

Prerequisites

A dialer interface has been configured and the dialer bundle has been specified for the dialer interface.

Precautions

- If **on-demand** is not specified, the PPPoE session works in permanent online mode. If this parameter is specified, the PPPoE session works in on-demand dialing mode. The device supports the packet triggering mode for on-demand dialing.
  - In permanent online mode, the device initiates a PPPoE session immediately after the physical link becomes Up. The PPPoE session persists until you use the **undo pppoe-client dial-bundle-number** command to delete it.
  - In triggered online mode, the device does not initiate a PPPoE session immediately after the physical link becomes Up. Instead, the device initiates a PPPoE session only when data needs to be transmitted on the link. If no data is transmitted on the PPPoE link within the interval specified by **dialer timer idle** *seconds*, the device terminates the PPPoE session. When data needs to be transmitted on the PPPoE link, the device sets up the PPPoE session again.

    NOTE

    - The **undo pppoe-client dial-bundle-number** command deletes a PPPoE session permanently regardless of the working mode of the session. To establish the session again, run the **pppoe-client dial-bundle-number** command.
    - Multiple PPPoE sessions can be established on an Ethernet interface or a PON interface. That is, an Ethernet interface or a PON interface can belong to multiple dialer bundles. A dialer bundle can contain only one Ethernet interface. One dialer bundle maps one PPPoE session. If the dialer bundle of a dialer interface already has an Ethernet interface or a PON interface used for PPPoE, no interface can be added to the dialer bundle. If the dialer bundle contains other interfaces, no Ethernet interface or PON interface can be added to the dialer bundle to establish PPPoE sessions on the PPPoE client.

 Copyright © Huawei Technologies Co., Ltd.

- If **no-hostuniq** is not specified, the PPPoE session initiated by the PPPoE client contains the Host-Uniq field. The PPPoE client uses this field to associate an access server response with a particular host request, which ensures strict check.

Example

Specify dialer bundle 1 for the PPPoE session on GE0/0/1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] pppoe-client dial-bundle-number 1
```

Related Topics

7.1.1 dialer bundle

7.1.13 dialer timer idle

7.1.16 dialer user

7.1.24 interface dialer

7.4.5 ppp lcp sn accept

Function

The **ppp lcp sn accept** command configures a PPPoE client to allow for serial number (SN) negotiation during the LCP negotiation.

The **undo ppp lcp sn accept** command restores the default setting.

By default, a PPPoE client is not allowed to perform SN negotiation during the LCP negotiation.

Format

ppp lcp sn accept

undo ppp lcp sn accept

Parameters

None

Views

Dialer interface view

Default Level

2: Configuration level

Usage Guidelines

To enhance access security for PPPoE users, a PPPoE server can authenticate the SNs of PPPoE clients by actively requesting SNs from PPPoE clients during LCP the

negotiation. When the device functioning as a PPPoE client receives such a request from the PPPoE server, the device does not return its SN during LCP negotiation. As a result, the PPPoE server cannot authenticate the SN of the PPPoE client.

To resolve this problem, you can run the **ppp lcp sn accept** command to configure the PPPoE client to allow for SN negotiation.

Example

Configure a PPPoE client to allow for SN negotiation during the LCP negotiation.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp lcp sn accept
```

Related Topics

7.4.6 ppp lcp imsi accept

7.4.6 ppp lcp imsi accept

Function

The **ppp lcp imsi accept** command configures a PPPoE client to allow for international mobile subscriber identity (IMSI) negotiation during the LCP negotiation.

The **undo ppp lcp imsi accept** command restores the default setting.

By default, a PPPoE client is not allowed to perform IMSI negotiation during the LCP negotiation.

Format

ppp lcp imsi accept

undo ppp lcp imsi accept

Parameters

None

Views

Dialer interface view

Default Level

2: Configuration level

Usage Guidelines

To enhance access security for PPPoE users, a PPPoE server can authenticate the IMSIs of PPPoE clients by actively requesting IMSIs from PPPoE clients during LCP the negotiation. When the device functioning as a PPPoE client receives such a

request from the PPPoE server, the device does not return its IMSI during LCP negotiation. As a result, the PPPoE server cannot authenticate the IMSI of the PPPoE client.

To resolve this problem, you can run the **ppp lcp imsi accept** command to configure the PPPoE client to allow for IMSI negotiation.

Example

Configure a PPPoE client to allow for IMSI negotiation during the LCP negotiation.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] ppp lcp imsi accept
```

Related Topics

7.4.5 ppp lcp sn accept

7.4.7 pppoe-server bind virtual-template

Function

The **pppoe-server bind virtual-template** command binds a virtual template interface to an Ethernet interface and enables PPPoE on the Ethernet interface.

The **undo pppoe-server bind virtual-template** command disables PPPoE on an interface.

By default, PPPoE is disabled.

Format

pppoe-server bind virtual-template *vt-number*

undo pppoe-server bind

Parameters

Parameter	Description	Value
vt-number	Specifies the number of a virtual template interface.	The value is an integer that ranges from 0 to 1023.

Views

Ethernet interface view, Ethernet sub-interface view, GE interface view, GE sub-interface view, XGE interface view, XGE sub-interface view, Layer 3 virtual Ethernet interface view, virtual Ethernet sub-interface view, PON interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as the PPPoE server, it authenticates PPPoE clients and allocates IP addresses to PPPoE clients. The **pppoe-server bind virtual-template** command binds a virtual template interface to an Ethernet interface or a PON interface. The virtual template specifies the authentication mode and IP addresses.

NOTE

The Ethernet interface must be a WAN-side Ethernet interface. LAN-side Ethernet interfaces do not support PPP.

Prerequisites

The virtual template interface has been created.

Precautions

- A physical interface can bind only one VT.
- This command specifies a physical link for the virtual template interface.
- When configuring a static route passing through a virtual interface, specify the next hop IP address but not the outbound interface. To specify the outbound interface, ensure that the virtual template interface is bound to a physical interface in Up state; otherwise, packets cannot be transmitted using this route.

After binding a specified virtual template to an interface, the device sets the negotiation polling interval in the virtual template to 30 seconds, and number of times for retransmitting heartbeat packets to 2, that is, the heartbeat timeout period is 60 seconds to 90 seconds. This configuration prevents frequent heartbeat packet transmission from affecting the device performance.

NOTE

Restarting a card or removing and reinstalling a card will cause interruption of PPPoE services. Therefore, exercise caution when performing these operations. Before you restart a card or remove and reinstall a card, run the **shutdown** command to shut down interfaces on the card.

Example

Bind virtual template interface 1 to GE1/0/0 and enable PPPoE.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pppoe-server bind virtual-template 1
```

Related Topics

5.20.13 interface virtual-template

7.4.8 pppoe-server max-sessions local-mac

Function

The **pppoe-server max-sessions local-mac** command sets the maximum number of PPPoE sessions that can be created on a MAC address of the device that functions as the PPPoE server.

The **undo pppoe-server max-sessions local-mac** command restores the default setting.

By default,

- A maximum of 128 PPPoE sessions can be created on a MAC address of the AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-51GE-P, AR2204-51GE-R, AR2204-48GE-P, AR2204-24GE, AR2204-27GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204E, AR2204E-D, and AR2204 that function as the PPPoE server.
- A maximum of 512 PPPoE sessions can be created on a MAC address of the AR2220E, AR2240C, AR2220 that functions as the PPPoE server.
- A maximum of 6144 PPPoE sessions can be created on the AR2204XE and AR2204XE-DC.
- For the AR2240 and AR3260, the number of PPPoE sessions varies depending on different SRUs.
  - SRU40 and SRU60: 512
  - SRU80: 1024
  - SRU100E, SRU200E, and SRU200: 6144
  - SRU400: 10240
- A maximum of 6144 PPPoE sessions can be created on the AR3670 (SRUX5).

Format

pppoe-server max-sessions local-mac *number*

undo pppoe-server max-sessions local-mac

Parameters

Parameter	Description	Value
number	Specifies the maximum number of PPPoE sessions that can be created on a MAC address of the device.	The value is an integer and varies according to the device types.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command limits the maximum number of PPPoE sessions that can be created on a MAC address of the device that functions as the PPPoE server.

Example

Set the maximum number of PPPoE sessions that can be created on a MAC address of the device to 15.

```
<Huawei> system-view
[Huawei] pppoe-server max-sessions local-mac 15
```

Related Topics

7.4.9 pppoe-server max-sessions total

7.4.9 pppoe-server max-sessions total

Function

The **pppoe-server max-sessions total** command sets the maximum number of PPPoE sessions that can be created on the device.

The **undo pppoe-server max-sessions total** command restores the default setting.

By default,

- A maximum of 128 PPPoE sessions can be created on the AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-51GE-P, AR2204-51GE-R, AR2204-48GE-P, AR2204-24GE, AR2204-27GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204E, AR2204E-D, and AR2204.
- A maximum of 512 PPPoE sessions can be created on the AR2220E, AR2240C, AR2220.
- A maximum of 6144 PPPoE sessions can be created on the AR2204XE and AR2204XE-DC.
- For the AR2240 and AR3260, the number of PPPoE sessions varies depending on different SRUs.
  - SRU40 and SRU60: 512
  - SRU80: 1024
  - SRU100E, SRU200E, and SRU200: 6144
  - SRU400: 10240
- A maximum of 6144 PPPoE sessions can be created on the AR3670 (SRUX5).

Format

pppoe-server max-sessions total *number*

undo pppoe-server max-sessions total

Parameters

Parameter	Description	Value
number	Specifies the maximum number of PPPoE sessions that can be created on the device.	The value is an integer and varies according to the device types.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

This command limits the number of access users on the device.

Example

Set the maximum number of PPPoE sessions that can be created on the device to 15.

```
<Huawei> system-view
[Huawei] pppoe-server max-sessions total 15
```

Related Topics

7.4.8 pppoe-server max-sessions local-mac

7.4.10 pppoe-server service-name

Function

The **pppoe-server service-name** command sets the name of the server that starts the PPPoE service on an interface.

The **undo pppoe-server service-name** command restores the default setting.

By default, the name of the server that starts the PPPoE service on an interface is an empty character string.

Format

pppoe-server service-name *name*

undo pppoe-server service-name

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name	Specifies the name of the server that starts the PPPoE service on an interface.	The value is a string of 1 to 128 case-sensitive characters without any space, asterisk (*), question mark (?), or quotation mark ('').

Views

Ethernet interface view, Ethernet sub-interface view, GE interface view, GE sub-interface view, XGE interface view, XGE sub-interface view, Layer 3 virtual Ethernet interface view, virtual Ethernet sub-interface view, PON interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish sessions between users and the specified PPPoE server, you can run the **pppoe-server service-name** command to specify the name of the server that starts the PPPoE service on an interface.

Pre-configuration Task

The PPPoE service is started on the interface using the **pppoe-server bind virtual-template** command.

Example

Set **IP-Service** as the name of the server that starts the PPPoE service on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pppoe-server bind virtual-template 1
[Huawei-GigabitEthernet1/0/0] pppoe-server service-name IP-Service
```

Related Topics

7.4.7 pppoe-server bind virtual-template

 Copyright © Huawei Technologies Co., Ltd.

7.4.11 pppoe-server log enable

Function

The **pppoe-server log enable** command enables logging of PPPoE user state changes.

The **undo pppoe-server log enable** command disables logging of PPPoE user state changes.

By default, logging of PPPoE user state changes is disabled.

Format

pppoe-server log enable

undo pppoe-server log enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **pppoe-server log enable** command to enable logging of PPPoE user state changes. The PPPoE server then records information about the Up/Down protocol state during user access, and you can check the user state changes.

Example

Enable logging of PPPoE user state changes.

```
<Huawei> system-view
[Huawei] pppoe-server log enable
```

7.4.12 reset pppoe-client

Function

The **reset pppoe-client** command resets all PPPoE sessions or a specified PPPoE session on the PPPoE client. After a PPPoE session is reset, the PPPoE client will establish the session later.

Format

reset pppoe-client { **all** | **dial-bundle-number** *number* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
all	Resets all PPPoE sessions on the PPPoE client.	-
dial-bundle-number *number*	Resets the specified PPPoE session.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PPP parameters of a PPPoE session set after a PPP link is created do not take effect immediately. To make the parameter settings effective, run the **reset pppoe-client** command to reset the PPPoE session. The parameter settings take effect after the PPPoE session is established again.

Configuration Impact

If **all** is specified, all the online PPPoE users are disconnected. If **dial-bundle-number** is specified, the PPPoE users who dial up from the specified dialer interface are disconnected.

If a PPPoE session in permanent online mode is reset, the device will establish the session again after 16 seconds. If a PPPoE session in packet triggered mode is reset, the device will establish the session again when data needs to be transmitted using the session.

NOTE

The **reset pppoe-client** command terminates PPPoE sessions temporarily, and the sessions will be established later; the **undo pppoe-client dial-bundle-number** command deletes PPPoE sessions permanently.

Example

Reset the PPPoE session created on dialer bundle 1.

```
<Huawei> reset pppoe-client dial-bundle-number 1
```

Related Topics

7.4.4 pppoe-client dial-bundle-number

7.4.13 reset pppoe-server

Function

The **reset pppoe-server** command terminates all PPPoE sessions or a specified PPPoE session on the PPPoE server.

Format

reset pppoe-server { **all** | **interface** *interface-type interface-number* | **virtual-template** *number* }

Parameters

Parameter	Description	Value
all	Terminates all PPPoE sessions on the PPPoE server.	-
interface *interface-type interface-number*	Terminates the PPPoE session on the specified physical interface.	-
virtual-template *number*	Terminates the PPPoE session on the specified virtual template interface.	The value of *number* is an integer that ranges from 0 to 1023.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To disconnect users from the device or trigger re-negotiation, terminate PPPoE sessions.

Configuration Impact

If **all** is specified, all the online PPPoE users are disconnected. If **interface** *interface-type interface-number* is specified, the PPPoE users who dial up from this interface are disconnected. If **virtual-template** *number* is specified, the PPPoE users who dial up from the physical interface bound to this virtual template interface are disconnected.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

User services are interrupted when PPPoE sessions are terminated; therefore, use the **reset pppoe-server** command with caution.

Example

Terminate PPPoE sessions on GE1/0/0.

```
<Huawei> reset pppoe-server interface gigabitethernet 1/0/0
```

Related Topics

7.4.2 display pppoe-server session

7.5 ATM Configuration Commands

7.5.1 atm-cell qos enable

Function

The **atm-cell qos enable** command enables ATM cell rate limiting on an interface card.

The **undo atm-cell qos enable** command disables ATM cell rate limiting on an interface card.

By default, ATM cell rate limiting is disabled on an interface card.

Format

atm-cell qos enable

undo atm-cell qos enable

Parameters

None

Views

ATM-PVC view, ATM-PVC-Group-PVC view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, ATM cell rate limiting is disabled. The **service cbr**, **service ubr**, **service vbr-nrt**, or **service vbr-rt** command enables ATM cell rate limiting on the main

control card. The **atm-cell qos enable** command enables ATM cell rate limiting on an interface card.

Prerequisite

The service type of a PVC and related rate parameters have been configured using the **service cbr**, **service ubr**, **service vbr-nrt**, or **service vbr-rt** command.

Precautions

If the configured service type of a PVC is deleted using the **undo service** command, ATM cell rate limiting enabled on an interface card using the **atm-cell qos enable** command is also disabled.

Example

Set the PVC name to huawei, VPI/VCI to 1/101, PVC service type to CBR, and peak forwarding rate of ATM cells to 1000 kbit/s, and enable ATM cell rate limiting on an interface card.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc huawei 1/101
[Huawei-atm-pvc-Atm1/0/0-1/101-huawei] service cbr 1000
[Huawei-atm-pvc-Atm1/0/0-1/101-huawei] atm-cell qos enable
```

Related Topics

7.5.27 service cbr

7.5.28 service ubr

7.5.29 service vbr-nrt

7.5.30 service vbr-rt

7.5.2 atm-link check

Function

The **atm-link check** command enables the connection of a link on an ATM sub-interface. When all the PVCs or PVPs go Down, the protocol status of the ATM sub-interface is also set to Down.

The **undo atm-link check** command disables the function.

By default, the connection of the link of an ATM sub-interface is enabled.

Format

atm-link check

undo atm-link check

Parameters

None

Views

ATM sub-interface view, IMA group sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an ATM sub-interface goes Up but all its PVCs or PVPs go Down, traffic is discarded and fails to be forwarded on this sub-interface. To allow the network layer to obtain the PVC and PVP status, run the **atm-link check** command to enable the connection of a link on the ATM sub-interface. If all the PVCs or PVPs go Down, the protocol status on the ATM sub-interface is set to Down, preventing data loss.

NOTE

ATM sub-interfaces are classified into P2P and P2MP. The default type is P2MP.

- P2P sub-interface: connects to a single remote device. A P2P sub-interface is configured with a single PVC, which allows the system to identify uniquely a remote device without being configured with a static address mapping.
- P2MP sub-interface: connects to multiple remote devices. A P2MP sub-interface is configured with multiple PVCs. An address mapping is established for each PVC and its connected remote protocol address. This allows traffic to travel through a specified PVC and successfully reach the destination. The address mappings can be configured manually or established dynamically using RARP.

Precautions

After the **atm-link check** command is run, the protocol status of an ATM sub-interface is set to Down after all the PVCs or PVPs on the sub-interface go Down.

Example

Disable the ATM link check on an ATM P2P sub-interface.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0.1 p2p
[Huawei-Atm1/0/0.1] undo atm-link check
```

Related Topics

7.5.10 interface atm

7.5.3 description (PVC view)

Function

The **description** command configures the description for a PVC.

The **undo description** command deletes the configured description for a PVC.

By default, there is no description for a PVC.

 Copyright © Huawei Technologies Co., Ltd.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description for a PVC.	The value is a string of 1 to 128 case-sensitive characters, spaces supported.

Views

ATM-PVC view, IMA-PVC view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To describe a configured PVC, you can run the **description** command to configure the description for a PVC.

Prerequisites

A PVC has been created using the **pvc** command.

Example

Configure the description for a PVC.

```
<Huawei> system-view
[Huawei] interface atm1/0/0
[Huawei-Atm1/0/0] pvc 100/100
[Huawei-atm-pvc-Atm1/0/0-100/100] description abc
```

7.5.4 display atm interface

Function

The **display atm interface** command displays detailed information about ATM interfaces.

If sub-interfaces exist, detailed information about sub-interfaces is also displayed.

Format

display atm interface [**atm** *interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
atm	Indicates an ATM interface.	-
interface-number	Specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Currently, ATM is mainly used at the data link layer. Based on packet switching, ATM inherits high-speed circuit switching to provide a universal connection-oriented transfer mode suitable for various services. This allows ATM to carry multiple upper-layer protocols, such as IP, IPoE, PPP, and PPPoE. Their applications are called IPoA, IPoEoA, PPPoA, and PPPoEoA.

To monitor the interface status and locate an interface fault, run the **display atm interface** command to obtain the interface status and statistics.

Example

Display information about ATM 2/0/0.

```
<Huawei> display atm interface atm 2/0/0
ATM interface Atm2/0/0, State UP
  Port Information:
    Maximum VCs: 16
    PVCs: 2, MAPs: 1
    input pkts: 0, input bytes: 0, input pkt errors: 0
    output pkts: 5915, output bytes: 141960, output pkt errors: 0
 information of this Interface
    PVCs: 1, MAPs: 1
    input pkts: 0, input bytes: 0, input pkt errors: 0
    output pkts: 5915, output bytes: 141960, output pkt errors: 0
ATM interface Atm2/0/0.1, multi-point, State UP
 information of this Interface
    PVCs: 0, MAPs: 0
    input pkts: 0, input bytes: 0, input pkt errors: 0
    output pkts: 0, output bytes: 0, output pkt errors: 0
ATM interface Atm2/0/0.10, point-to-point, State UP
 information of this Interface
    PVCs: 1, MAPs: 0
    input pkts: 0, input bytes: 0, input pkt errors: 0
    output pkts: 0, output bytes: 0, output pkt errors: 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 7-16 Description of the **display atm interface** command output

Item	Description
ATM interface, State	Indicates the number and status of the ATM interface.
Port Information:	Indicates information about a port.
Maximum VCs: 16	Indicates that the maximum number of PVCs on the ATM interface is 16. **NOTE** The maximum number of PVCs on ADSL interface is 16, the maximum number of PVCs on G.SHDSL interface is 8.
PVCs: 2, MAPs: 1	Indicates that there are two PVCs and one MAP on the main interface.
input pkts: 0, input bytes: 0, input pkt errors: 0	Indicates that the numbers of input packets, input bytes, and input packet errors are all 0.
output pkts: 5915, output bytes: 141960, output pkt errors: 0	Indicates that the number of output packets is 5915; the number of output bytes is 141960; the number of output packet errors is 0.
ATM interface Atm2/0/0.1, multi-point, State UP	Indicates a sub-interface ATM 2/0/0.1 whose type is P2MP and status is Up.

Related Topics

7.5.10 interface atm

7.5.5 display atm map-info

Function

The **display atm map-info** command displays information about the upper layer protocol mapping table of ATM.

Format

display atm map-info [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }]]

Parameters

Parameter	Description	Value
interface	Indicates an interface.	-

Parameter	Description	Value
atm	Indicates an ATM interface.	-
pvc	Specifies the Permanent Virtual Circuit (PVC).	-
pvc-name	Specifies the PVC name. The value is created by the **pvc** command. The value of *vpi*/*vci* for each PVC must be unique on an ATM interface (including its sub-interfaces).	The value is a string of 1-16 case-insensitive characters.
vpi	Specifies the VPI. The PVC identified by *vpi* must have been created.	The value is an integer. It is ranging from 0 to 255.
vci	Specifies the VCI. The PVC identified by *vci* must have been created.	The value is an integer ranging from 0 to 2 and 5 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In the scenario where you need to monitor the status of an interface or locate an interface fault, you can run the **display atm map-info** command to view the status and statistics of the interface. According to the information, you can measure traffic and locate the interface fault.

Example

Display information about the upper layer protocol mapping table of all ATM interfaces.

```
<Huawei> display atm map-info
Atm1/0/0, PVC 1/33, IP, State UP
1.2.1.1, vlink 1
Atm1/0/0, PVC 1/32, PPP, Virtual-Template10, UP
Atm1/0/0, PVC 2/101, ETH, Virtual-Ethernet0/0/1, UP
```

 Copyright © Huawei Technologies Co., Ltd.

Table 7-17 Description of the **display atm map-info** command output

Item	Description
Atm1/0/0, PVC 1/33, IP, State UP 1.2.1.1, vlink 1	Indicates that: • PVC 1/33 of ATM 1/0/0 is configured with IPoA mapping. • The configured mapping static IP address is 1.2.1.1. • The Vlink numbered 1 is used. • The status of Vlink 1 is activated (Up).
Atm1/0/0, PVC 1/32, PPP, Virtual-Template10, UP	Indicates that: • PVC 1/32 of ATM 1/0/0 is configured with PPPoA mapping. • The VT interface numbered 10 is used. • The status of the VT interface is activated (Up).
Atm1/0/0, PVC 2/101, ETH, Virtual-Ethernet0/0/1, UP	Indicates that: • PVC 2/101 of ATM 1/0/0 is configured with PPPoEoA mapping or IPoEoA mapping. • The VE interface numbered 0/0/1 is used. • The status of the VE interface is activated (Up).

Related Topics

7.5.15 map ip

7.5.16 map ppp

7.5.6 display atm pvc-group

Function

The **display atm pvc-group** command displays information about PVC groups.

Format

display atm pvc-group [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }]]

Parameters

Parameter	Description	Value
interface	Indicates an interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
atm	Indicates an ATM interface.	-
pvc-name	Specifies the PVC name. The value is created by the **pvc** command. The value of *vpi*/*vci* for each PVC must be unique on an ATM interface (including its sub-interfaces).	The value is a string of 1-16 case-insensitive characters.
interface-number	Specifies the interface number.	-
vpi	Specifies the VPI. The PVC identified by *vpi* must have been created.	The value is an integer. It is ranging from 0 to 255.
vci	Specifies the VCI. The PVC identified by *vci* must have been created.	The value is an integer ranging from 0 to 2 and 5 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If no PVC group is configured, all PVCs evenly share bandwidth resources and transmit packets to destinations. This does not ensure reliable transmission and may cause transmission delays. To address this problem, you can configure a PVC group and specify PVCs in the group to separately transmit IP packets with different priorities. In addition, the PVCs can be configured to provide Differential QoS assurance based on application requirements.

If a PVC group has been configured on an interface, run the **display atm pvc-group** command to view the configuration and statistics about the PVC group.

When using the **display atm pvc-group** command, note the following points:

- If no parameter is specified, the configuration and statistics about PVC groups on all interfaces are displayed.
- If only the parameter **interface** is specified, the configuration and statistics about PVC groups on the specific interface are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The configuration about ATM PVC groups is complete.

Example

Display information about all PVC groups on ATM interfaces of the device.

```
<Huawei> display atm pvc-group
PVC-GROUP-NAME    VPI/VCI    STATE ENCAP PROTOCOL INTERFACE
aaa               3/35       Down  SNAP  None     Atm1/0/0(DOWN)
```

Table 7-18 Description of the display atm pvc-group command output

Item	Description
PVC-GROUP-NAME	Indicates the name of a PVC-Group.
VPI/VCI	Indicates the VPI/VCI values of a PVC.
STATE	Indicates the status of a PVC, either Up or Down.
ENCAP	Indicates the AAL encapsulation type.
PROTOCOL	Indicates the application mode: ● IP indicates IPoA. ● ETH indicates PPPoEoA or IPoEoA. ● PPP indicates PPPoA.
INTERFACE	Indicates an ATM interface, which is named in the slot number/card number/interface number format, for example, ATM 1/0/0.

Related Topics

7.5.22 pvc-group

7.5.7 display atm pvc-info

Function

The **display atm pvc-info** command displays information about PVCs.

Format

display atm pvc-info [**interface atm** *interface-number* [**pvc** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface atm *interface-number*	Specifies the ATM interface number.	-
pvc	Specifies the PVC.	-
pvc-name	Specifies the PVC name. The value is created by the **pvc** command. The value of *vpi/vci* for each PVC must be unique on an ATM interface (including its sub-interfaces).	The value is a string of 1-16 case-insensitive characters.
vpi/vci	Specifies the virtual path identifier (VPI) and virtual channel identifier (VCI) on an ATM network. The PVC specified by *vpi/vci* must have been created.	The *vpi* value is an integer ranging from 0 to 255. The *vci* value is an integer ranging from 0 to 2 and 5 to 65534.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

ATM is connection-oriented. ATM connections are logical connections, called virtual circuits (VCs). Each VC is identified by a virtual path identifier (VPI) and a virtual channel identifier (VCI). A pair of VPI/VCI takes effect only on one link between two ATM nodes. Each ATM node maps the VPI/VCI values into a specific address. When an ATM connection is released, the VPI/VCI values for the connection are also reclaimed and put into a resource table. Then, the VPI/VCI can be used again.

If a PVC has been configured on an interface, run the **display atm pvc-info** command to view the configuration and statistics about the PVC.

When using the **display atm pvc-info** command, note the following points:

- If no parameter is specified, the configuration and statistics about PVCs on all interfaces are displayed.

 Copyright © Huawei Technologies Co., Ltd.

- If only the parameter **interface** is specified, the configuration and statistics about PVCs on the specific interface are displayed.

Prerequisites

The configuration about ATM PVCs is complete.

Example

Display information about PVCs of all ATM interfaces.

```
<Huawei> display atm pvc-info
Atm1/0/0, VPI: 33, VCI: 44, INDEX: 19
  AAL5 Encaps: SNAP, Protocol: IP
  Service-type:UBR
  input pkts: 1357852279, input bytes: 4294967295, input pkt errors: 0
  output pkts: 1511, output bytes: 66964, output pkt errors: 0
  Interface State: UP, PVC State: UP
  OAM Statistics:
  input pkts: 0, input bytes: 0
  output pkts: 0, output bytes: 0
```

Display information about the PVC of the specified interface.

```
<Huawei> display atm pvc-info interface atm 2/0/0 pvc 1/100
Atm2/0/0, VPI: 1, VCI: 100, INDEX: 1
  AAL5 Encaps: SNAP, Protocol: IP
  Service-type:UBR
  input pkts: 0, input bytes: 0, input pkt errors: 0
  output pkts: 8959, output bytes: 215016, output pkt errors: 0
  Interface State: UP, PVC State: UP
  OAM Statistics:
  input pkts: 0, input bytes: 0
  output pkts: 0, output bytes: 0
```

Table 7-19 Description of the **display atm pvc-info** command output

Item	Description
VPI, VCI	Values of VPI and VCI in the VPI/VCI pair.
INDEX	Index number of the PVC.
AAL5 Encaps	The encapsulation type is AAL5.
Protocol	Type of the network layer protocol.
Service-type	Service type, including: ● CBR: Constant Bit Rate ● UBR: Unspecified Bit Rate ● VBR-NRT: Variable Bit Rate-Non Real Time ● VBR-RT: Variable Bit Rate-Real Time
input pkts, input bytes, input pkt errors	Numbers of input packets, input bytes, and input packet errors.
output pkts, output bytes, output pkt errors	Numbers of output packets; output bytes; and output packet errors.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface State	Interface status. • UP • DOWN
PVC State	PVC status. • UP • DOWN
OAM Statistics	OAM statistics.

Related Topics

7.5.21 pvc

7.5.8 display atm pvc-info statistics

Function

The **display atm pvc-info statistics** command displays statistics about PVC number.

Format

display atm pvc-info statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about PVC number on a specified interface. If **interface** *interface-type interface-number* is not specified in the command, statistics about PVC number on all interfaces on which PVC has been configured are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

If PVCs are configured on multiple interfaces, to check statistics about PVC number on each interface, you need to run the **display this** command on each interface, which is time-consuming. To address issue, run the **display atm pvc-info statistics** command to check statistics about PVC number on all interfaces.

Precautions

If a PVC has not been configured on an interface, no information is displayed.

Example

Display statistics about PVC number on all interfaces.

```
<Huawei> display atm pvc-info statistics
Atm pvc-info statistics for interface Atm1/0/0:
Maximum VCs: 2048
Total VCs : 2
UP VCs    : 2  DOWN VCs   : 0
Atm pvc-info statistics for interface Atm2/0/0:
Maximum VCs: 2048
Total VCs : 1
UP VCs    : 1  DOWN VCs   : 0
```

Display statistics about PVC number on ATM 1/0/0.

```
<Huawei> display atm pvc-info statistics interface atm 1/0/0
Atm pvc-info statistics for interface Atm1/0/0:
Maximum VCs: 2048
Total VCs : 2
UP VCs    : 2  DOWN VCs   : 0
```

Table 7-20 Description of the **display atm pvc-info statistics** command output

Item	Description
Maximum VCs	Maximum number of PVCs that can be configured on the interface, which can be configured using the **pvc max-number** command.
Total VCs	Number of PVCs configured on the interface.
UP VCs	Number of PVCs with the link layer protocol Up.
DOWN VCs	Number of PVCs with the link layer protocol Down.

7.5.9 encapsulation (PVC view)

Function

The **encapsulation** command specifies the ATM AAL5 as the encapsulation type for PVC.

The **undo encapsulation** command restores the default setting.

By default, **aal5snap** is adopted.

Format

encapsulation { **aal5snap** | **aal5mux** }

undo encapsulation

Parameters

Parameter	Description	Value
aal5snap	Indicates the **aal5snap** encapsulation type.	-
aal5mux	Indicates the **aal5mux** encapsulation type, that is, the multiplexing encapsulation type.	-

Views

ATM-PVC view, IMA-PVC view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ATM supports multi-protocol encapsulation. It defines a standard technique that transmits multi-protocol datagrams using AAL5 frames on an ATM network. The ATM Adaptation Layer (AAL) isolates the ATM layer from a higher layer. It transforms data packets into 48-byte ATM cells. Running the **encapsulation** command can configure an ATM AAL5 encapsulation type. The parameters of the **encapsulation** command are applied to different encapsulation scenarios:

- **aal5snap**

  The **aal5snap** encapsulation type can be used to transmit multiple protocols over the same PVC. If the **aal5snap** is configured, PVCs support Inverse Address Resolution Protocol (InARP), LLC encapsulation, and Subnetwork Access Protocol (SNAP) encapsulation.

  LLC/SNAP is a default encapsulation technology. It allows multiplexing of multiple protocols over a single ATM VC. A protocol adds a different IEEE 802.2 logical link control (LLC) header to PDUs that are transmitted using the protocol.

- **aal5mux**

  This encapsulation type allows a specified PVC between two ATM sites to transmit a single type of protocol packets. If the two ATM sites change, another type of protocol packets will be transmitted over the PVC. Therefore, a PVC can be used to transmit different types of protocol packets. PVCs must be configured with the **aal5mux** encapsulation type.

aal5snap and **aal5mux** are two common encapsulation types. They are selected based on real-world situations, such as network types and costs. If network costs

depend on the number of established PVCs, **aal5snap** is preferred. If network costs depend on transmission volume, **aal5mux** is preferred because packets encapsulated based on **aal5mux** have smaller packet headers.

Precautions

Running the **encapsulation** command will change the encapsulation type of PVCs. Therefore, verify that PVCs are not transmitting services before running the command.

Some encapsulation types may not support one or more of the following service modes: IPoA, IPoEoA, PPPoA, and PPPoEoA. If a service mode is configured with an encapsulation type that does not support the service mode, the system will display a prompt.

Only **aal5snap** supports InARP. InARP cannot be configured when **aal5mux** is adopted.

To change the AAL5 encapsulation type of PVC to **aal5mux**, InARP must be deleted first if it has been configured.

Example

The first method is as follows (Specify the AAL5 encapsulation type of the PVC 2/45 as aal5snap):.

```
<Huawei>system-view
[Huawei]interface atm 1/0/0
[Huawei-Atm1/0/0]pvc 2/45
[Huawei-atm-pvc-Atm1/0/0-2/45] encapsulation aal5snap
```

Related Topics

7.5.21 pvc

7.5.10 interface atm

Function

The **interface atm** command creates an ATM sub-interface and displays the ATM interface view.

The **undo interface atm** command deletes an ATM sub-interface.

By default, the type of a sub-interface is P2MP.

Format

interface atm *interface-number*

interface atm *interface-number.subinterface-number* [**p2mp** | **p2p**]

undo interface atm *interface-number*

undo interface atm *interface-number.subinterface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of an ATM interface.	-
subinterface-number	Specifies the number of an ATM sub-interface.	The value is an integer that ranges from 1 to 1024.
p2mp	Specifies the type of a sub-interface of p2mp.	-
p2p	Specifies the type of a sub-interface of p2p.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, ATM is mainly used at the data link layer. Based on packet switching, ATM inherits high-speed circuit switching to provide a universal connection-oriented transfer mode suitable for various services. This allows ATM to carry multiple upper-layer protocols, such as IP, IPoE, PPP, and PPPoE. Their applications are called IPoA, IPoEoA, PPPoA, and PPPoEoA.

- Run the **interface atm** *interface-number* command to enter the ATM interface view and configure PVCs.
- Run the **interface atm** *interface-number.subinterface-number* [**p2mp** | **p2p**] command to enter the ATM sub-interface view and configure PVCs.

  The type of an ATM sub-interface can be P2MP or P2P. Multiple PVCs can be created on a P2MP sub-interface, whereas only one PVC can be created on a P2P sub-interface.

Precautions

Before changing the sub-interface type, run the **undo interface atm** *interface-number.subinterface-number* command on the sub-interface.

Example

Enter the ATM 1/0/0 interface view.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0]
```

Create and enter ATM 1/0/0.1, and set its type to P2P.

```
<Huawei> system-view
[Huawei] undo interface atm 1/0/0.1
[Huawei] interface atm 1/0/0.1 p2p
[Huawei-Atm1/0/0.1]
```

Related Topics

7.5.4 display atm interface

7.5.11 ip dscp

Function

The **ip dscp** command maps a range of DSCP values of IP packets to a PVC.

The **undo ip dscp** command deletes the mapping between a range of DSCP values and a PVC.

By default, IP packets carrying DSCP identifier on a PVC have not precedences

Format

ip dscp { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } { *min* [*max*] | **default** }

undo ip dscp [*pvc-name* [*vpi*/*vci*] | *vpi*/*vci*]

Parameters

Parameter	Description	Value
pvc-name	Specifies a PVC name. This parameter is used in the **pvc** command line. The *vpi*/*vci* values of each PVC on an ATM interface (main interface or sub-interface) is unique.	The value is a string of 1 to 16 case-insensitive characters.
vpi	Specifies *vpi* to be the virtual path identifier (VPI) for a virtual path on an ATM network. The PVC specified by *vpi* must have been created.	The value is an integer. It is ranging from 0 to 255.
vci	Specifies *vci* to be the virtual channel identifier (VCI) for a virtual channel on an ATM network. The PVC specified by *vci* must have been created.	The value is an integer ranging from 0 to 2 and 5 to 65534.
min	Specifies the minimum IP precedence value of IP packets to be transmitted along the PVC.	The value is an integer ranging from 0 to 63.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
max	Specifies the maximum IP Precedence value of IP packets to be transmitted along the PVC.	The value is an integer ranging from 0 to 63.
default	Indicates that the PVC transmits IP packets with default precedence.	-

Views

ATM-PVC group view, IMA-Group-PVC-Group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring PVC groups can classify service data based on precedence values. IP packets that are transmitted over ATM links can be classified based on the ToS field of packets.

The ToS field in an IP packet contains a DSCP or precedence value. Perform the following operations to map DSCP or precedence values to PVCs:

- If the ToS field contains a DSCP value, run the **ip dscp** command to map a DSCP value to a PVC.

  The DSCP value uses 6 bits of the ToS field, ranging from 0 to 63. The greater the value, the higher the precedence. After precedence values are mapped to PVCs, IP packets with different precedence values are transmitted along specified PVCs. This allows services with different precedence values to be transmitted separately.

  The parameters of the **ip dscp** command can be selected as required.

  - Running the **ip dscp** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } *min* [*max*] command can configure IP packets with DSCP values between *min* and *max* to be transmitted along a PVC with the specified *vpi*/*vci* values.
  - Running the **ip dscp** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } **default** command can configure all IP packets without specified PVCs to be transmitted along the PVC with the specified *vpi*/*vci* values.
- If the ToS field contains a precedence value, run the **ip precedence** command to configure a PVC to transmit IP packets with the precedence value.

Prerequisites

Create the PVC for transmitting IP packets.

Precautions

DSCP values can be mapped only to PVCs in the PVC group. The *min* value must be smaller than or equal to the *max* value. If the PVC to which a specific DSCP

value is mapped goes Down or the PVC is not mapped to a specific DSCP value, IP packets with this DSCP value will be transmitted along the default PVC. If the default PVC is also Down, the packets will be transmitted along a PVC to which a smaller DSCP value is mapped. The following PVC forwarding modes are recommended:

- Forward unicast packets over PVCs to which IP priorities of these packets are mapped.
- Forward IS-IS, multicast, and broadcast packets over the PVC to which the DSCP value of 63 is mapped.

The **ip dscp** command takes effect only for the ATM PVC group containing the PVCs transmitting IPoA packets.

Example

Configure PVC with the name of **mypvc** and VPI/VCI of 2/45 to transmit IP packets with DSCP values of 0 to 3.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-ATM1/0/0] pvc mypvc 2/45
[Huawei-atm-pvc-Atm1/0/0-2/45-mypvc] quit
[Huawei-ATM1/0/0] pvc-group mypvc 2/45
[Huawei-Atm1/0/0-atm-pvc-group-2/45-mypvc] ip dscp mypvc 2/45 0 3
```

Related Topics

7.5.22 pvc-group

7.5.21 pvc

7.5.12 ip precedence

Function

The **ip precedence** command maps a range of IP precedence values to a PVC.

The **undo ip precedence** command deletes the mapping between a range of IP precedence values and a PVC.

By default, a PVC is not configured with a precedence.

Format

ip precedence { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } { *min* [*max*] | **default** }

undo ip precedence [*pvc-name* [*vpi*/*vci*] | *vpi*/*vci*]

Parameters

Parameter	Description	Value
pvc-name	Specifies a PVC name. This parameter is used in the **pvc** command line. The *vpi*/*vci* values of each PVC on an ATM interface (main interface or sub-interface) are unique.	The value is a string of 1 to 16 case-insensitive characters.
vpi	Specifies *vpi* to be the virtual path identifier (VPI) for a virtual path on an ATM network. The PVC specified by *vpi* must have been created.	The value is an integer. It is ranging from 0 to 255.
vci	Specifies *vci* to be the virtual channel identifier (VCI) for a virtual channel on an ATM network. The PVC specified by *vci* must have been created.	The value is an integer ranging from 0 to 2 and 5 to 65534.
min	Specifies the minimum IP precedence value of IP packets to be transmitted along the PVC.	The value is an integer ranging from 0 to 7.
max	Specifies the maximum IP precedence value of IP packets to be transmitted along the PVC.	The value is an integer ranging from 0 to 7.
default	Indicates that the PVC transmits IP packets with the default precedence value.	-

Views

ATM-PVC group view, IMA-Group-PVC-Group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring PVC groups can classify service data based on precedence values IP packets that are transmitted over FR links can be classified based on the ToS fields of packets.

 Copyright © Huawei Technologies Co., Ltd.

The ToS field in an IP packet contains a DiffServ Code Point (DSCP) or precedence value. Perform the following operations to map DSCP or precedence values to PVCs:

- If ToS fields of packets contain precedence values, run the **ip precedence** command to map precedence values of packets to a PVC.

  The 3-bit precedence value in the ToS field ranges from 0 to 7. It can identify 8 precedence values. The larger the value, the higher the precedence. After IP precedence values are mapped to PVCs, IP packets with different IP precedence values are transmitted along separate PVCs. This allows services with different precedence values to be transmitted separately.

  The parameters of the **ip precedence** command can be selected as required.

  - Running the **ip precedence** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } *min* [*max*] command, you can configure IP packets with DSCP values ranging from *min* to *max* to be transmitted along a PVC with a specified *vpi*/*vci* value.
  - Running the **ip precedence** { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } **default** command configures all IP packets without specified PVCs to be transmitted along the PVC with the specified *vpi*/*vci* value.
- If ToS fields of packets contain DSCP values, run the **ip dscp** command to map DSCP values of packets to a PVC.

Prerequisites

Create the PVC to which the DSCP values of packets are mapped.

Precautions

DSCP values can be mapped only to PVCs in the PVC group. The *min* value must be smaller than the *max* value. If the PVC to which a specific DSCP value is mapped goes Down or the PVC is not mapped to a specific DSCP value, IP packets with this DSCP value will be transmitted along the default PVC. If the default PVC is also Down, the packets will be transmitted along a PVC to which a smaller DSCP value is mapped. By default, the device forwards IS-IS, multicast, and broadcast packets along the PVC to which DSCP value 6 is mapped. Sufficient bandwidth resources must be reserved for a PVC carrying protocol packets to ensure that the protocol packets are transmitted properly. If traffic congestion on the PVC causes the protocol packets to fail to be transmitted, service interruption may occur. The following PVC forwarding modes are recommended:

- Forward unicast packets over PVCs to which IP precedence values of these packets are mapped.
- Forward IS-IS, multicast, and broadcast packets over the PVC to which the DSCP value of 7 is mapped.

The VPI/VCI values configured for the primary and secondary ATM PVCs in an ATM PVC group must be the same on the local and remote ends. The IP precedence value configured for each ATM PVC must also be the same on the local and remote ends. If ATM PVCs on the local and remote ends are configured with different IP precedence values, services provided by the ATM PVC group will be interrupted.

The **ip precedence** command takes effect only for the ATM PVC group containing the PVCs transmitting IPoA packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure PVC with the name of **huawei** and VPI/VCI of 2/45 to transmit IP packets with IP precedence values of 0 to 3.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-ATM1/0/0] pvc huawei 2/45
[Huawei-atm-pvc-Atm1/0/0-2/45-huawei] quit
[Huawei-ATM1/0/0] pvc-group huawei 2/45
[Huawei-Atm1/0/0-atm-pvc-group-2/45-huawei] ip precedence huawei 2/45 0 3
```

Related Topics

7.5.22 pvc-group

7.5.21 pvc

7.5.13 map bridge

Function

The **map bridge** command sets up the IPoEoA mapping or PPPoEoA mapping on the PVC.

The **undo map bridge** command deletes the IPoEoA mapping or PPPoEoA mapping on the PVC.

By default, no mapping is configured on the PVC.

Format

map bridge virtual-ethernet *interface-number*

undo map bridge

Parameters

Parameter	Description	Value
virtual-ethernet*interface-number*	Specifies the interface number of a VE interface. The format is slot number/module number/sequence number.	The value depends on the device. The VE interface has been created.

Views

ATM-PVC view, IMA-PVC view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

NOTE

Because the upper layer of the link layer of the VE interface is Ethernet and the lower layer is AAL5, the MAC address of the VE interface is not the actual one and it cannot be obtained from the hardware. You must manually configure the correct MAC address.

IPoE over ATM (IPoEoA) means that IPoE packets are encapsulated into ATM cells and transmitted on ATM networks. IPoEoA is applicable to the scenario where a device is connected to the remote server to access an external server at a high speed. An ATM PVC can be used to bear traffic between the device and the server that is far away from the device. In addition, the server must provide an ATM interface to bear Ethernet packets.

PPPoE over ATM (PPPoEoA) is used to bear PPP over Ethernet (PPPoE) packets on an ATM network. This means that Ethernet packets are encapsulated in ATM cells. A PVC can be used to provide all Ethernet functions.

Running the **map bridge virtual-ethernet** *interface-number* command can configure IPoEoA or PPPoEoA mapping.

Precautions

The command can be configured only on a Layer 3 VE interface. If this command is configured on a Layer 2 VE interface, the configuration does not take effect.

Example

The following examples display a complete process of the IPoEoA configuration.

Create VE 0/0/2.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/2
```

Configure IP address 10.1.1.1/16 for the interface.

```
[Huawei-Virtual-Ethernet0/0/2] ip address 10.1.1.1 255.255.0.0
[Huawei-Virtual-Ethernet0/0/2] quit
```

Create PVC 1/102 at ATM 0/0/2

```
[Huawei] interface atm 0/0/2
[Huawei-Atm0/0/2] pvc 1/102
```

Use the VE interface to set up the IPoE mapping in the PVC view.

```
[Huawei-atm-pvc-Atm0/0/2-1/102] map bridge virtual-ethernet 0/0/2
```

Related Topics

7.5.15 map ip

7.5.14 map bridge broadcast

Function

The **map bridge broadcast** command configures a PVC to send and receive bridge packets.

The **undo map bridge broadcast** command prohibits a PVC from sending and receiving bridge packets.

By default, a PVC on an ATM interface is not configured to send and receive bridge packets.

Format

map bridge broadcast

undo map bridge broadcast

Parameters

None

Views

ATM-PVC view, IMA-PVC view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two Ethernet networks communicate with each other by using ATM links or IMA group links, the Ethernet frames need to be transmitted by means transparent bridging (TB). The **map bridge broadcast** command can be run to allow a PVC to send and receive bridge packets.

Prerequisites

Interfaces have been added to a bridge group.

Precautions

On an ATM interface, only one PVC is allowed to send and receive bridge packets.

If a PVC is deleted, the configuration (sending and receiving bridge packets) of the PVC will also be automatically deleted.

Example

Configure PVC 1/102 to send and receive bridge packets.

```
<Huawei> system-view
[Huawei] interface atm 1/0/1
[Huawei-Atm1/0/1] bridge 2
[Huawei-Atm1/0/1] pvc 1/102
[Huawei-atm-pvc-Atm1/0/1-1/102] map bridge broadcast
```

 Copyright © Huawei Technologies Co., Ltd.

7.5.15 map ip

Function

The **map ip** command creates the IPoA mapping for the PVC.

The **undo map ip** command deletes the mapping.

By default, no mapping is configured.

Format

map ip { *ip-address* | **default** | **inarp** [*minutes*] } [**broadcast**]

undo map ip [*ip-address* | **default** | **inarp**]

Parameters

Parameter	Description	Value
ip-address	Specifies the peer IP address mapping to PVC.	-
default	Configures a mapping with the default route property. If a packet cannot find a mapping of the next hop at the interface, and a certain PVC has the default mapping, the packet can be sent over the PVC.	-
inarp	Enables InARP at a PVC.	-
minutes	Specifies the interval of sending InARP packets in minutes.	The value ranges from 1 to 600. The default is 1.
broadcast	Indicates the pseudo broadcast. If a mapping with such property is configured at PVC, the broadcast packets of a PVC interface are sent at the PVC.	-

Views

ATM-PVC view, IMA-PVC view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPoA means that IP packets are encapsulated into ATM cells and transmitted on ATM networks. As bearer networks for IP services, ATM networks provide good network performance and mature QoS assurance. Running the **map ip** command to create IPoA mapping is to associate the protocol address of a remote device

 Copyright © Huawei Technologies Co., Ltd.

with a local PVC. This helps upper-layer protocols locate the remote device based on its protocol address.

Running the **map ip** *ip-address* command configures a mapping between a PVC and a destination IP address. Every IP packet to be transmitted on an IPoA network must be mapped to a PVC. You can perform the following operations to configure mappings in batches:

- To map all the IP packets destined for the same network segment to one PVC, run the **map ip** *ip-address* command.
- To map all the IP packets that have not been mapped to any PVCs to one PVC, run the **map ip default** command.
- If the local device is the DTE, run the **map ip inarp** [*minutes*] command to use InARP for automatic mapping. In this case, you do not need to configure mappings between IP addresses and PVCs.

  NOTE

  minutes must be set to a proper value based on the network topology stability. If the network topology changes frequently, set a small *minutes* value. If the network topology is stable, set a large *minutes* value.

  The AR109, AR109W, AR109GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169W-P-M9, AR169RW-P-M9, and AR169-P-M9 do not support **map ip inarp** [*minutes*] command.

If the upper-layer protocol, such as OSPF, transmits packets in broadcast mode on an ATM network, configure **broadcast** for the PVC. If a PVC is configured with **broadcast**, all broadcast packets on the PVC's interface are sent along the PVC.

Prerequisites

The **aal5snap** encapsulation type has been configured.

Precautions

The IP address specified in this command must be the IP address of the peer interface. Otherwise, data cannot be correctly forwarded.

One IP address cannot be mapped to multiple ATM interfaces or sub-interfaces on the same device. Otherwise, traffic cannot be properly forwarded.

Example

Create a static mapping on PVC 2/45. Configure the peer IP address to 10.1.1.1 and configure the address to support pseudo broadcast.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc 2/45
[Huawei-atm-pvc-Atm1/0/0-2/45] map ip 10.1.1.1 broadcast
```

Enable InARP at PVC 2/45 to make the interface automatically obtain the peer address and send InARP packets every 10 minutes.

```
[Huawei-atm-pvc-Atm1/0/0-2/45] map ip inarp 10
```

Related Topics

7.5.13 map bridge

7.5.16 map ppp

7.5.16 map ppp

Function

The **map ppp** command creates a mapping between PPPoA and a PVC.

The **undo map ppp** command deletes the mapping between PPPoA and a PVC.

By default, PPPoA is not configured.

Format

map ppp { **virtual-template** *vt-number* [**server**] | **dialer** *dialer-number* }

undo map ppp

Parameters

Parameter	Description	Value
virtual-template *vt-number*	Specifies the number of the VT interface for PPPoA. The *vt-number* must have been created by **interface virtual-template** command.	The value is an integer ranging from 0 to 1023.
server	Configures the device as a PPPoA server.	-
dialer *dialer-number*	Specifies the number of the Dialer interface for PPPoA. The interface must have been created by **interface dialer** command.	The value is an integer and the value depend on the device.

Views

ATM-PVC view, IMA-PVC view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ATM has short communication delays and high network throughput, but does not support authentication. This means that unauthorized users can use ATM to

access enterprise networks. Point-to-Point Protocol (PPP) is a data link layer protocol used to transmit network layer packets on P2P links. It supports authentication and is extensible. PPPoA allows devices to check validity of users that attempt to log in. This improves ATM network security.

NOTE

PPPoA means that PPP packets are encapsulated into ATM cells and transmitted over the ATM network. IP or other protocol packets are encapsulated into PPP packets. PPP provides flexible and various applications for PPPoA.

PPPoA links are classified into the following types:

- Permanent-online PPPoA: You can run the **map ppp virtual-template** *vt-number* command to configure permanent-online PPPoA.
- On-demand PPPoA: You can run the **map ppp virtual-template** *vt-number* or **map ppp dialer** *dialer-number* command to configure on-demand PPPoA.

Prerequisites

A virtual template (VT) interface or a dialer interface has been created.

Precautions

If on-demand PPPoA is configured, a PPP connection will be automatically terminated after a period of time that is set in the dial control center (DCC). Therefore, the **undo map ppp** command does not need to be run.

The Dialer interface to be specified in the **map ppp dialer** *dialer-number* command must be the one that is not used and is configured with the PPP encapsulation mode. If the Dialer interface is used or configured with another encapsulation mode, the system displays an error.

Example

The following example describes a complete process for configuring PPPoA.

Create VT interface 10 and assign an IP address to this interface.

```
<Huawei> system-view
[Huawei] interface virtual-template 10
[Huawei-Virtual-Template10] ip address 10.1.1.1 255.255.255.0
[Huawei-Virtual-Template10] quit
```

Create PVC 1/101 on ATM 1/0/0.

```
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc 1/101
```

Configure PPPoA on VT interface 10.

```
[Huawei-atm-pvc-Atm1/0/0-1/101] map ppp virtual-template 10
```

Related Topics

7.5.13 map bridge
7.5.15 map ip

7.5.17 oam ais-rdi

Function

Using the **oam ais-rdi** command, you can enable Alarm Indication Signal (AIS) or Remote Defect Indication (RDI) cell detection.

Using the **undo oam ais-rdi** command, you can disable AIS or RDI cell detection.

By default, AIS or RDI cell detection is disabled.

Format

oam ais-rdi [**up** *up-count* **down** *down-count*]

undo oam ais-rdi

Parameters

Parameter	Description	Value
up *up-count*	Specifies the number of consecutive seconds during which AIS/RDI cells are not received before the PVC becomes Up.	The value is an integer that ranges from 1 to 10, in seconds. The default value is 2.
down *down-count*	Specifies the number of consecutively received AIS/RDI cells before the PVC becomes Down.	The value is an integer that ranges from 1 to 5. The default value is 2.

Views

ATM-PVC view, IMA-PVC view, IMA-Group-PVC-Group-PVC view, ATM-PVC-Group-PVC view

Default Level

2: Configuration level

Usage Guidelines

An AIS cell is sent to notify the downstream device that the upstream device is faulty. An RDI cell is sent to notify the upstream device that the downstream device is unreachable. After AIS or RDI cell detection is enabled, if the device receives AIS/RDI cells of a number specified by *down-count*, the PVC becomes Down. If the device does not receive AIS/RDI cells within the specified number of consecutive seconds specified by *up-count*, the PVC becomes Up.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set *up-count* to 5s and *down-count* to 5 on PVC2/45.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] pvc 2/45
[Huawei-atm-pvc-Atm2/0/0-2/45] oam ais-rdi up 5 down 5
```

7.5.18 oam cc end-to-end

Function

Using the **oam cc end-to-end** command, you can enable the OAM Continuity Check (CC) function.

Using the **undo oam cc end-to-end** command, you can disable the OAM CC function.

By default, OAM CC is disabled.

Format

oam cc end-to-end { **both** | **sink** | **source** }

undo oam cc end-to-end { **both** | **sink** | **source** }

Parameters

Parameter	Description	Value
both	Indicates that the PVC receives CC cells when it functions as the receive end and the PVC encapsulates CC cells into cell flows when it functions as the transmit end.	-
sink	Indicates that the PVC receives CC cells when it functions as the receive end.	-
source	Indicates that the PVC encapsulates CC cells into cell flows when it functions as the transmit end.	-

Views

ATM-PVC view, IMA-PVC view, IMA-Group-PVC-Group-PVC view, ATM-PVC-Group-PVC view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

OAM CC allows the device to encapsulate CC cells into cell flows periodically. If CC cells are transmitted successfully, connectivity is normal. This detection mode occupies certain bandwidth on each link.

After CC is enabled, if the device does not receive CC cells in 3s, the PVC becomes Down. After the device receives CC cells, the PVC becomes Up.

NOTE

When you configure CC, if **source** or **both** is configured on one end, **sink** or **both** must be configured on the other end.

Example

Enable CC on PVC2/45.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] pvc 2/45
[Huawei-atm-pvc-Atm2/0/0-2/45] oam cc end-to-end sink
```

7.5.19 oam loopback

Function

Using the **oam loopback** command, you can enable OAM F5 loopback cell transmission and retransmission detection.

Using the **undo oam loopback** command, you can disable OAM F5 loopback cell transmission and retransmission detection.

By default, the device does not send OAM F5 loopback cells, but the device must respond to the received OAM F5 loopback cells.

Format

oam loopback [**up** *up-count* **down** *down-count* **retry-frequency** *retry-frequency*]

undo oam loopback

Parameters

Parameter	Description	Value
up *up-count*	Specifies the number of consecutive OAM F5 loopback cells received before the PVC changes from Down to Up.	The value is an integer that ranges from 1 to 10. The default value is 5.

Parameter	Description	Value
down *down-count*	Specifies the number of consecutive OAM F5 loopback cells not received before the PVC changes from Up to Down.	The value is an integer that ranges from 1 to 10. The default value is 5.
retry-frequency *retry-frequency*	Specifies the interval at which OAM F5 loopback cells are sent during retransmission detection before the PVC status changes.	The value is an integer that ranges from 1 to 10, in seconds. The default value is 5.

Views

ATM-PVC view, IMA-PVC view, IMA-Group-PVC-Group-PVC view, ATM-PVC-Group-PVC view

Default Level

2: Configuration level

Usage Guidelines

OAM F5 loopback cells are sent to detect connectivity on the ATM network. After OAM F5 loopback cell transmission and retransmission detection are enabled, the PVC status changes only when a certain number of OAM F5 loopback cells are received.

Example

Enable OAM F5 loopback cell detection on PVC2/45, and set *up-count* to 4, *down-count* to 4, and the interval at which OAM F5 loopback cells are sent during retransmission detection to 2s.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] pvc 2/45
[Huawei-atm-pvc-Atm2/0/0-2/45] oam loopback up 4 down 4 retry-frequency 2
```

7.5.20 oamping pvc

Function

Using the **oamping pvc** command, you can test connectivity of an ATM link on a specified ATM interface.

Format

oamping pvc { *pvc-name* | *vpi/vci* } [*number timeout*]

Parameters

Parameter	Description	Value
pvc-name	Specifies the name of the PVC on which OAM cells are sent.	The value is a string of 1 to 16 case-insensitive characters without spaces.
vpi/vci	Specifies the VPI/VCI pair of the PVC on which OAM cells are sent.	The VPI value ranges from 0 to 255 and the VCI value ranges from 0 to 2 and 5 to 65534.
number	Specifies the number of OAM cells sent consecutively.	The value is an integer that ranges from 1 to 1000. The default value is 4.
timeout	Specifies the timeout interval during which no OAM response message is received.	The value is an integer that ranges from 1 to 30, in seconds. The default value is 2.

Views

ATM interface view

Default Level

2: Configuration level

Usage Guidelines

The device can send OAM cells on a PVC of a specified ATM interface to determine connectivity of the ATM link. If no ATM response message is received within the timeout interval, packets are lost on the ATM link because the ATM link is unreachable or busy.

Example

On PVC2/45 of ATM2/0/0, set *number* to 3 and *timeout* to 1s.

```
<Huawei> system-view
[Huawei] interface atm 2/0/0
[Huawei-Atm2/0/0] oamping pvc 2/45 3 1
```

7.5.21 pvc

Function

The **pvc** command creates a PVC of the specified VPI/VCI or PVCs of the specified VPI/VCI in batches and displays the PVC view or the PVC batch view.

The **undo pvc** command deletes the specified PVC.

By default, no PVC is created.

Format

pvc { { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* } | { *start-vpi*/*start-vci end-vpi*/*end-vci* } }

undo pvc { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }

Parameters

Parameter	Description	Value
pvc-name	Specifies a PVC name. This parameter is used in the **pvc** command line. The *vpi*/*vci* values of each PVC on an ATM interface (main interface or sub-interface) is unique.	The value is a string of 1 to 16 case-insensitive characters. It cannot contain a space or question mark (?).
vpi	Specifies *vpi* to be the virtual path identifier (VPI) for a virtual path on an ATM network. The PVC specified by *vpi* must have been created.	The value is an integer. It is ranging from 0 to 255.
vci	Specifies *vci* to be the virtual channel identifier (VCI) for a virtual channel on an ATM network. The PVC specified by *vci* must have been created.	The value is an integer ranging from 0 to 2 and 5 to 65534.
start-vpi/*start-vci*	Specifies the start *vpi*/*vci* in PVCs configured in batches.	The *start-vpi* value is an integer. It is ranging from 0 to 255. The *start-vci* value is an integer ranging from 0 to 2 and 5 to 65534.
end-vpi/*end-vci*	Specifies the start *vpi*/*vci* in PVCs configured in batches.	The *start-vpi* value is an integer. It is ranging from 0 to 255. The *start-vci* value is an integer ranging from 0 to 2 and 5 to 65534.

 Copyright © Huawei Technologies Co., Ltd.

Views

Atm sub-interface view, ATM-PVC group view, IMA group view, IMA group sub-interface view, IMA-Group-PVC-Group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ATM is mainly used at the data link layer. ATM works based on packet switching and inherits high-speed circuit switching to provide a universal connection-oriented transfer mode. This transfer mode is applicable to various services. It allows multiple upper-layer protocols (such as the IPoA, IPoEoA, PPPoA, and PPPoEoA) to be carried on the ATM network.

ATM is connection-oriented. ATM connections are logical connections, called virtual circuits (VCs). Each VC is identified by a virtual path identifier (VPI) and a virtual channel identifier (VCI). A pair of VPI/VCI takes effect only on one link between two ATM nodes. Each ATM node maps the VPI/VCI values into a specific address. When an ATM connection is released, the VPI/VCI values for the connection are also reclaimed and put into a resource table. Then, the VPI/VCI values can be used again.

If *pvc-name* is configured to create a PVC, *vpi*/*vci* values must be specified for the PVC. After a PVC is configured with a PVC name, run the **pvc** *pvc-name* command to display the PVC view. To delete this PVC, run the **undo pvc** command with either the PVC name or the VPI/VCI values of the PVC.

Precautions

PVCs with the same attributes can be created or deleted in batches. The principles for deleting PVCs in batches are as follows:

- Run the **pvc** command to create PVCs with the same attributes in batches in one of the following situations:
  - PVCs to be created have the same VPI value and consecutive VCI values.
  - PVCs to be created have the same VCI value and consecutive VPI values.
  - PVCs to be created have consecutive VPI values and are in the same VCI range.
  - If PVCs to be created have consecutive VPI values and are in different VCI ranges, create PVCs in batches based on VPIs.
  - If PVCs to be created have inconsecutive VPI values, check whether the PVCs can be created in batches based on their VPI values.

  PVCs with different attributes cannot be displayed in batches.

  The IMA group interfaces do not support the batch PVC creation function.
- Running the **undo pvc** command can delete PVCs with different attributes in batches as long as these PVCs are within the specified VPI/VCI range.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a PVC named "huawei" with VPI/VCI being 1/101.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc huawei 1/101
```

Related Topics

7.5.7 display atm pvc-info

7.5.22 pvc-group

Function

The **pvc-group** command creates a PVC group on an interface or displays the PVC group view.

The **undo pvc-group** command deletes a specified PVC group.

By default, a PVC group on an interface is not created.

Format

pvc-group { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }

undo pvc-group { *pvc-name* [*vpi*/*vci*] | *vpi*/*vci* }

Parameters

Parameter	Description	Value
pvc-name	Specifies a PVC name. This parameter is used in the **pvc** command line. The *vpi*/*vci* values of each PVC on an ATM interface (main interface or sub-interface) are unique.	The value is a string of 1 to 16 case-insensitive characters. It cannot contain a space or question mark (?).
vpi	Specifies *vpi* to be the virtual path identifier (VPI) for a virtual path on an ATM network. The PVC specified by *vpi* must have been created.	The value is an integer. It is ranging from 0 to 255.
vci	Specifies *vci* to be the virtual channel identifier (VCI) for a virtual channel on an ATM network. The PVC specified by *vci* must have been created.	The value is an integer ranging from 0 to 2 and 5 to 65534.

 Copyright © Huawei Technologies Co., Ltd.

Views

ATM interface view, ATM sub-interface view, IMA group view, IMA group sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a PVC group is not configured, each PVC can be mapped only to one IP address. That is, a subscriber's traffic flow can occupy only one PVC. The traffic flows of different types of the subscriber evenly share the PVC's bandwidth. This processing cannot meet various services' different requirements for reliability and transmission delays. After a PVC group is configured, a subscriber's traffic flow can occupy multiple PVCs. You can specify PVCs in the PVC group to separately transmit IP packets with different precedence values. This transmission mechanism provides different QoSs for different services.

If a *pvc-name* value (such as "huawei") has been specified for a PVC, running the **pvc-group** *pvc-name* command with the *pvc-name* value of "huawei" can display a PVC group view. This upgrades the PVC named *pvc-name* to a PVC group.

To delete a PVC group, you can run the **undo pvc-group** *pvc-name* command. If the name of the PVC group is "huawei", you can run the **undo pvc-group** *huawei* command. Alternatively, you can run the **undo pvc-group** *vpi/vci* command. If the VPI/VCI values of the PVC group are 2/45, you can run the **undo pvc-group** *vpi/vci* command.

Prerequisites

Check that the PVC with the same name or VPI/VCI value has been created.

Precautions

The virtual path identifier (VPI)/virtual channel identifier (VCI) values configured for the primary and secondary ATM PVCs in an ATM PVC group must be the same on the local and remote ends. The IP precedence value or the DSCP value carried by the IP packet on each ATM PVC must also be the same on the local and remote ends. If the IP packets on ATM PVCs on the local and remote ends are configured with different IP precedence values (**ip precedence**) or DSCP values (**ip dscp**), services provided by the ATM PVC group will be interrupted.

If a PVC link is unstable, you must configure ATM OAM on the PVC interface of the local end to sense the PVC status change on the remote end.

Example

Create a PVC group based on the PVC named **huawei** and with the VPI or VCI value of 2 or 45.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc huawei 2/45
```

```
[Huawei-atm-pvc-Atm1/0/0-2/45-huawei] quit
[Huawei-Atm1/0/0] pvc-group huawei 2/45
```

Related Topics

7.5.12 ip precedence

7.5.21 pvc

7.5.23 pvc-protect

Function

The **pvc-protect** command configures protection for member permanent virtual channels (PVCs) in a PVC group.

The **undo pvc-protect** command disables protection for member PVCs in a PVC group.

By default, protection for member PVCs in a PVC group is disabled.

Format

pvc-protect { *pvc-name* [*vpi/vci*] | *vpi/vci* } **individual**

undo pvc-protect { *pvc-name* [*vpi/vci*] | *vpi/vci* }

Parameters

Parameter	Description	Value
pvc-name	Specifies a PVC name. This parameter is used in the **pvc** command line. The *vpi/vci* values of each PVC on an asynchronous transfer mode (ATM) interface (main interface or sub-interface) are unique.	The value is a string of 1 to 16 case-insensitive characters.
vpi/vci	Specifies the virtual path identifier (VPI) and virtual channel identifier (VCI) on an ATM network. The PVC specified by *vpi/vci* must have been created.	The *vpi* value is an integer ranging from 0 to 255. The *vci* value is an integer ranging from 0 to 2 and 5 to 65534.
individual	Specifies the Individual mode in which PVCs are protected separately.	-

Views

ATM-PVC group view, IMA-Group-PVC-Group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring a PVC group, users can specify PVCs in the group to separately transmit IP packets with different priorities. In addition, the PVCs can be configured to provide differential QoS assurance based on application requirements. If a PVC with a high priority goes Down, the device automatically searches for a PVC with a low priority to take over user traffic. This mechanism prevents a service interruption, but a user cannot detect the link fault.

To configure protection for member PVCs in a PVC group, run the **pvc-protect** command. If the link goes faulty on a protected member PVC, the PVC group becomes unavailable so that traffic cannot be forwarded. This way helps detect the link fault promptly and locate the cause.

Precautions

If the **pvc-protect** command is configured on a member PVC on which no service is running in the PVC group, the PVC group goes Down when the member PVC goes Down. If the PVC group goes Down, all member PVCs go Down, which causes the services running on other member PVCs to be interrupted.

Example

Configure protection for member PVCs named **huawei** in a PVC group.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-ATM1/0/0] pvc huawei 2/45
[Huawei-atm-pvc-Atm1/0/0-2/45-huawei] quit
[Huawei-ATM1/0/0] pvc-group huawei 2/45
[Huawei-atm-pvc-group-Atm1/0/0-2/45-huawei] pvc-protect huawei 2/45 individual
```

Related Topics

7.5.22 pvc-group

7.5.21 pvc

7.5.24 pvc max-number

Function

The **pvc max-number** command sets the maximum number of VCs on an ATM interface.

The **undo pvc max-number** command restores the default maximum number of VCs on an ATM interface.

By default, G.SHDSL interfaces, E1-IMA interfaces, and IMA groups support a maximum of eight VCs on an ATM interface; ADSL and VDSL interfaces support a maximum of 16 VCs on an ATM interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

pvc max-number *max-number*

undo pvc max-number

Parameters

Parameter	Description	Value
max-number	Specifies the supported maximum VC number.	The value is an integer. The value range is as follows: ● G.SHDSL interfaces, E1-IMA interfaces, and IMA groups: 1-8 ● ADSL and VDSL interfaces: 1-16

Views

ATM interface view, IMA-Group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent device resources from being exhausted, run the **pvc max-number** command to configure the maximum number of VCs on an ATM interface. If the number of PVCs configured on an ATM interface reaches the upper limit, no PVC can be created again.

Precautions

Running the **pvc max-number** command can configure the maximum number of VCs that are shared by the ATM main interface and sub-interfaces.

If an ATM main or sub-interface has PVCs, the number of PVCs configured using the **pvc max-number** command must be greater than the number of existing PVCs.

This command can be executed only in the view of an ATM main interface.

Example

Sets the maximum number of VCs to 8 on ATM 1/0/0.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc max-number 8
```

Related Topics

7.5.4 display atm interface

7.5.25 pvp limit

Function

The **pvp limit** command sets the parameters for the VP policing.

The **undo pvp limit** command deletes the VP policing.

By default, the VP policing is not performed.

Format

pvp limit *vpi peak-rate*

undo pvp limit *vpi*

Parameters

Parameter	Description	Value
vpi	Specifies the ATM network VPI.	It ranges from 0 to 255 in integer.
peak-rate	Specifies the normal traffic.	The value ranges from 8 to 4294967295, in Kbit/s. Set the value of *peak-rate* within the actual bandwidth of an ATM interface.

Views

ATM interface view, IMA group view

Default Level

2: Configuration level

Usage Guidelines

In the VP policing, the parameters of PVC are still valid.

The packets are transmitted only when the packets meet requirements of PVC and VP policing.

The traffic statistics include the LLC/SNAP, MUX and NLPID encapsulation headers except for the ATM cell header.

Example

Set the traffic of VP with VPI being 1 to 2 M.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvp limit 1 2000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.5.21 pvc
7.5.27 service cbr
7.5.29 service vbr-nrt
7.5.30 service vbr-rt
7.5.28 service ubr

7.5.26 reset atm

Function

The **reset atm** command clears the ATM interface statistics.

Format

reset atm interface [**atm** *interface-number*]

Parameters

Parameter	Description	Value
atm *interface-number*	Specifies the ATM interface index.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the status and statistics of an interface displayed by the **display atm interface** command, you can measure traffic and locate faults.

Before collecting traffic information about a specific interface within a period, clear the existing traffic statistics on this interface.

Precautions

The **reset atm** command clears statistics on all ATM interfaces. To clear statistics on a specific ATM interface and its sub-interfaces, specify the parameter **atm** *interface-number* in the **reset atm** command.

Example

Clear the statistics on all interfaces.

```
<Huawei> reset atm interface
```

Related Topics

7.5.4 display atm interface

7.5.27 service cbr

Function

The **service cbr** command specifies the PVC service type as Constant Bit Rate (CBR).

The **undo service** command restores the PVC service type to the default value.

By default, the service type is Unspecified Bit Rate (UBR) after a PVC is created.

Format

service cbr *output-pcr*

undo service

Parameters

Parameter	Description	Value
output-pcr	Specifies the peak rate of outputting ATM cells in kbit/s.	The value is an integer in kbit/s and varies according to the interface types. • E1-IMA interface: 64 to 1984 • ADSL interface: 64 to 2048 • G.SHDSL interface: 64 to 22784 • VDSL interface: 64 to 34000

Views

ATM-PVC view, IMA-PVC view, IMA-Group-PVC-Group-PVC view, ATM-PVC-Group-PVC view

Default Level

2: Configuration level

Usage Guidelines

This command and the **service ubr**, **service vbr-rt** and **service vbr-nrt** commands can be used to set the service type.

The newly specified PVC service type covers the existing service type.

The CBR can be configured on a maximum of eight PVCs of an ATM interface.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM main interface simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM sub-interface simultaneously.

Example

Create a PVC named "huawei" with VPI/VCI being 1/101.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc huawei 1/101
```

Specify the PVC service type as CBR. Set the peak rate of outputting ATM cells to 1,000 kbit/s.

```
[Huawei-atm-pvc-Atm1/0/0-1/101-huawei] service cbr 1000
```

Related Topics

7.5.25 pvp limit

7.5.29 service vbr-nrt

7.5.30 service vbr-rt

7.5.28 service ubr

7.5.28 service ubr

Function

The **service ubr** command specifies the service type of a PVC as UBR and specifies the rate parameters.

The **undo service** command restores the PVC service type to the default value.

By default, the service type is UBR after a PVC is created.

Format

service ubr [*output-pcr*]

undo service

Parameters

Parameter	Description	Value
output-pcr	Specifies the peak rate of outputting ATM cells in kbit/s.	The value is an integer in kbit/s and varies according to the interface types. • E1-IMA interface: 64 to 1984 • ADSL interface: 64 to 2048 • G.SHDSL interface: 64 to 22784 • VDSL interface: 64 to 34000

 Copyright © Huawei Technologies Co., Ltd.

Views

ATM-PVC view, IMA-PVC view, IMA-Group-PVC-Group-PVC view, ATM-PVC-Group-PVC view

Default Level

2: Configuration level

Usage Guidelines

This command as well as the **service vbr-nrt**, **service vbr-rt** and the **service cbr** commands can be used to set the service type and service parameters of a PVC.

The newly specified PVC service type covers the existing service type.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM main interface simultaneously.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM sub-interface simultaneously.

Example

Create a PVC named "huawei" with VPI/VCI being 1/101.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc huawei 1/101
```

Specify the service type of the PVC as UBR.

```
[Huawei-atm-pvc-Atm1/0/0-1/101-huawei] service ubr
```

Specify the service type of the PVC as UBR and set the peak rate of ATM cells to 1,000 kbit/s.

```
[Huawei-atm-pvc-Atm1/0/0-1/101-huawei] service ubr 1000
```

Related Topics

7.5.27 service cbr

7.5.29 service vbr-nrt

7.5.30 service vbr-rt

7.5.29 service vbr-nrt

Function

The **service vbr-nrt** command specifies the service type of a PVC as Variable Bit Rate-Non Real Time (VBR-NRT) and specifies the rate parameters.

The **undo service** command restores the PVC service type to the default value.

By default, the service type is UBR when a PVC is created.

Format

service vbr-nrt *output-pcr output-scr output-mbs*

 Copyright © Huawei Technologies Co., Ltd.

undo service

Parameters

Parameter	Description	Value
output-pcr	Specifies the peak rate of outputting ATM cells in kbit/s.	The value is an integer in kbit/s and varies according to the interface types. • E1-IMA interface: 64 to 1984 • ADSL interface: 64 to 2048 • G.SHDSL interface: 64 to 22784 • VDSL interface: 64 to 34000
output-scr	Specifies the sustainable rate of outputting ATM cells in kbit/s.	The value is an integer in kbit/s and varies according to the interface types. • E1-IMA interface: 64 to 1984 • ADSL interface: 64 to 2048 • G.SHDSL interface: 64 to 22784 • VDSL interface: 64 to 34000 *output-scr* must be no larger than *output-pcr*.
output-mbs	Specifies the maximum burst size of the sent ATM cells, namely the maximum cache number of sent ATM cells.	The value ranges from 1 to 512 in cells.

Views

ATM-PVC view, IMA-PVC view, IMA-Group-PVC-Group-PVC view, ATM-PVC-Group-PVC view

Default Level

2: Configuration level

Usage Guidelines

This command and the **service cbr**, **service vbr-rt**, and **service ubr** commands can be used to set the PVC service type and service parameters of Variable Bit Rate-Real Time (VBR-RT) and CBR.

The newly specified PVC service type covers the existing service type.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM main interface simultaneously.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM sub-interface simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a PVC named "huawei" with VPI/VCI being 1/101.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc huawei 1/101
```

Specify the service type of the PVC as VBR-NRT. Set the peak rate of outputting ATM cells to 1,000 kbit/s, sustainable cell output rate to 1,000 kbit/s and the maximum burst size to 320 cells.

```
[Huawei-atm-pvc-Atm1/0/0-1/101-huawei] service vbr-nrt 1000 1000 320
```

Related Topics

7.5.27 service cbr

7.5.30 service vbr-rt

7.5.28 service ubr

7.5.30 service vbr-rt

Function

The **service vbr-rt** command sets the service type of a PVC to Variable Bit Rate-Real Time (VBR-RT) and specifies the rate parameters.

The **undo service** command restores the PVC service type to the default value.

By default, the service type is UBR when a PVC is created.

Format

service vbr-rt *output-pcr output-scr output-mbs*

undo service

Parameters

Parameter	Description	Value
output-pcr	Specifies the peak rate of outputting ATM cells in kbit/s.	The value is an integer in kbit/s and varies according to the interface types. • E1-IMA interface: 64 to 1984 • ADSL interface: 64 to 2048 • G.SHDSL interface: 64 to 22784 • VDSL interface: 64 to 34000

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
output-scr	Specifies the sustainable rate of outputting ATM cells in kbit/s.	The value is an integer in kbit/s and varies according to the interface types. ● E1-IMA interface: 64 to 1984 ● ADSL interface: 64 to 2048 ● G.SHDSL interface: 64 to 22784 ● VDSL interface: 64 to 34000 *output-scr* must be no larger than *output-pcr*
output-mbs	Specifies the maximum burst size of sent ATM cells, namely the maximum cache number of sent ATM cells at the interface.	The value ranges from 1 to 512 cells.

Views

ATM-PVC view, IMA-PVC view, IMA-Group-PVC-Group-PVC view, ATM-PVC-Group-PVC view

Default Level

2: Configuration level

Usage Guidelines

This command and the **service ubr**, **service cbr** and **service vbr-nrt** commands can be used to set the service type.

The newly specified PVC service type covers the existing service type.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM main interface simultaneously.

Services, and queue profiles and traffic policies containing CBQ cannot be configured on the ATM sub-interface simultaneously.

Example

Create a PVC named "huawei" with VPI/VCI being 1/101.

```
<Huawei> system-view
[Huawei] interface atm 1/0/0
[Huawei-Atm1/0/0] pvc huawei 1/101
```

Specify the service type of the PVC as VBR-RT. Configure the peak rate of outputting ATM cells to 1,000 kbit/s, sustainable output rate to 1,000 kbit/s, the maximum burst size to 320 cells.

```
[Huawei-atm-pvc-Atm1/0/0-1/101-huawei] service vbr-rt 1000 1000 320
```

Related Topics

7.5.25 pvp limit
7.5.27 service cbr
7.5.29 service vbr-nrt
7.5.28 service ubr

7.6 Frame Relay Configuration Commands

NOTE

AR100&AR120&AR150&AR160&AR200 series (except AR162 and AR168F-4P) AR2201-48FE do not support HDLC.

7.6.1 apply policy

Function

Using the **apply policy** command, you can apply a QoS policy to an FR class.

Using the **undo apply policy** command, you can unbind a QoS policy from an FR class.

By default, no QoS policy is applied to an FR class.

Format

apply policy *policy-name* { **inbound** | **outbound** }

undo apply policy { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a QoS policy to be applied to a specified FR class.	The value is a string of 1 to 31 case-insensitive characters. Before applying a QoS policy, ensure that the QoS policy has been created.
inbound	Indicates that the specified QoS policy is applied to the incoming packets on a PVC.	-
outbound	Indicates that the specified QoS policy is applied to the outgoing packets on a PVC.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

FR class view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement FR QoS, create a traffic policy and apply it in the FR class view. You can run the **apply policy** command to apply a traffic policy to an FR class to provide differentiated services for various packets forwarded by using FR.

Prerequisites

The QoS policy to be applied has been created by using the **traffic policy** command.

Precautions

If an FR class is applied to an FR virtual circuit (VC), the traffic policy applied to the FR class is also applied to the FR VC.

NOTE

- Before running the **apply policy** command, ensure that no traffic policy is applied to the sub-interface and interface where the FR VC is established. If a class-based queue (CBQ) has been configured in the traffic policy and PVC priority queuing (PVC PQ) has been configured on the interface, running this command is prohibited.
- FR class does not support traffic policy nesting.

Example

Create a traffic behavior named **b1** and set the assured bandwidth to 56 kbit/s.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] queue af bandwidth 56
[Huawei-behavior-b1] quit
```

Create a traffic classifier named **c1** and configure matching rules for traffic classification based on the DE bit in FR packets.

```
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match fr-de
[Huawei-classifier-c1] quit
```

Create a traffic policy named **p1** and associate the traffic policy with the traffic classifier and traffic behavior.

```
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
```

Create an FR class named **huawei** and apply traffic policy **p1** to the FR class.

```
[Huawei] fr class huawei
[Huawei-fr-class-huawei] apply policy p1 inbound
[Huawei-fr-class-huawei] apply policy p1 outbound
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.6.21 fr class
20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy

7.6.2 cbs outbound

Function

Using the **cbs outbound** command, you can set the committed burst size (CBS) in the outbound direction of FR VCs.

Using the **undo cbs outbound** command, you can restore the default CBS.

By default, the CBS of FR VCs is 1500 bytes.

Format

cbs outbound *committed-burst-size*

undo cbs outbound

Parameters

Parameter	Description	Value
committed-burst-size	Specifies the CBS in the outbound direction of FR VCs.	The value is an integer that ranges from 1500 to 4294967295, in bytes.

Views

FR class view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CBS is the volume of traffic that an FR network is committed to transmit within the interval of Tc. When network congestion occurs, the FR network can transmit this volume of traffic successfully.

Precautions

Before running the **cbs** command, run the **fr traffic-shaping** command to enable FR traffic shaping. Otherwise, the **cbs** command does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

If an FR class is applied to an FR VC by using the **fr-class** command, the CBS set in the FR class is also applied to the FR VC.

Example

Set the CBS in the outbound direction of FR VCs to 2000 bytes.

```
<Huawei> system-view
[Huawei] fr class huawei
[Huawei-fr-class-huawei] cbs outbound 2000
```

Related Topics

7.6.21 fr class

7.6.47 fr traffic-shaping

7.6.49 fr-class

7.6.3 cir

Function

Using the **cir** command, you can set the committed information rate (CIR) for FR VCs.

Using the **undo cir** command, you can restore the default CIR.

By default, the CIR of FR VCs is 56 kbit/s.

Format

cir *committed-information-rate*

undo cir

Parameters

Parameter	Description	Value
committed-information-rate	Specifies the CIR of FR VCs.	The value is an integer that ranges from 8 to 45000, in kbit/s.

Views

FR class view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CIR is the minimum transmission rate that a VC is committed to provide. Users can send data at the CIR even when network congestion occurs.

Precautions

Before running the **cir** command, run the **fr traffic-shaping** command to enable FR traffic shaping. Otherwise, the **cir** command does not take effect.

If an FR class is applied to an FR VC by using the **fr-class** command, the CIR set in the FR class is also applied to the FR VC.

NOTE

The CIR set by using the **cir** command cannot be greater than the allowed CIR set by using the **cir allow** command.

Example

Set the CIR of FR VCs to 100 kbit/s.

```
<Huawei> system-view
[Huawei] fr class huawei
[Huawei-fr-class-huawei] cir 100
```

Related Topics

7.6.4 cir allow outbound

7.6.47 fr traffic-shaping

7.6.49 fr-class

7.6.4 cir allow outbound

Function

Using the **cir allow outbound** command, you can set the CIR allowed by FR VCs.

Using the **undo cir allow outbound** command, you can restore the default CIR allowed by FR VCs.

By default, the CIR allowed by FR VCs is 56 kbit/s.

Format

cir allow outbound *committed-information-rate*

undo cir allow outbound

Parameters

Parameter	Description	Value
committed-information-rate	Specifies the CIR allowed FR VCs in the outbound direction.	The value is an integer that ranges from 8 to 45000, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Views

FR class view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The allowed CIR is the transmission rate that an FR network can provide in normal situations. When no network congestion occurs, users can send data at the allowed CIR.

Precautions

Before running the **cir allow** command, run the **fr traffic-shaping** command to enable FR traffic shaping. Otherwise, the **cir allow** command does not take effect.

If an FR class is applied to an FR VC by using the **fr-class** command, the allowed CIR set in the FR class is also applied to the FR VC.

NOTE

The allowed CIR set by using the command cannot be smaller than the CIR set by using the **cir** command.

Example

Set the CIR allowed by FR VCs in the outbound direction to 200 kbit/s.

```
<Huawei> system-view
[Huawei] fr class huawei
[Huawei-fr-class-huawei] cir allow outbound 200
```

Related Topics

7.6.3 cir

7.6.47 fr traffic-shaping

7.6.49 fr-class

7.6.5 display fr class

Function

Using the **display fr class** command, you can view the FR class configuration.

Format

display fr class [*class-name*]

Parameters

Parameter	Description	Value
class-name	Displays the configuration of a specified FR class. If no FR class name is specified, all FR class configurations are displayed.	To create an FR class, run the **fr class** command.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display fr class** command displays the FR class configuration and helps to locate FR QoS faults.

Example

Display all FR class configurations.

```
<Huawei> display fr class
fr class c1
 General Traffic Shape Info:
  CIR allow outbound 45000(Kbps), CIR 100(Kbps), CBS outbound 15000(byte)
 Fragment Size Info:
  fragment 80(byte)
 Traffic Shaping Adaptation Info:
  traffic-shaping adaptation becn 30(percentage)
  traffic-shaping adaptation interface-congestion 40(packet number)
 PVC-PQ Queue Info:
  pvc-pq top
 Traffic Policy Info:
  apply policy p1 inbound
  apply policy p1 outbound

fr class q1
 General Traffic Shape Info:
  CIR allow outbound 56(Kbps), CIR 56(Kbps), CBS outbound 1500(byte)
 Traffic Shaping Adaptation Info:
  traffic-shaping adaptation becn 30(percentage)
  traffic-shaping adaptation interface-congestion 25(packet number)
 PVC-PQ Queue Info:
  pvc-pq normal
```

Table 7-21 Description of the display fr class command output

Item	Description
General Traffic Shape Info	Traffic shaping information about the FR class. To configure traffic shaping, run the **cir allow**, **cir**, and **cbs** commands.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Fragment Size Info	Fragment size information about the FR class. To configure the fragment size, run the **fragment** command.
Traffic Shaping Adaptation Info	Traffic shaping adaptation information. To configure traffic shaping adaptation, run the **traffic-shaping adaptation** command.
PVC-PQ Queue Info	PVC PQ queue information. To configure a PVC PQ queue, run the **pvc-pq** command.
Traffic Policy Info	Traffic policy applied to the FR class. To configure a traffic policy, run the **apply policy** command.

Related Topics

7.6.21 fr class

7.6.6 display fr compression frf9

Function

The **display fr compression frf9** command displays information about FRF.9 STAC compression.

Format

display fr compression frf9 [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about FRF.9 STAC compression on a specified interface. **NOTE** The interface must be a main interface and cannot be a sub-interface. If a main interface number is specified, FRF.9 compression information about all its sub-interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

FRF.9 STAC compression, as a cost-effective bandwidth saving function provided for Frame Relay (FR) users, saves network bandwidth resources, reduces network loads, and improves the transmission efficiency.

NOTE

Generally, links working at rates lower than 768 kbps are considered low-speed links.

To monitor interface status or locate faults on an interface, run the **display fr compression frf9** command to view statistics about the interface. The command output can provide information for troubleshooting the interface.

NOTE

If no interface is specified, information about FRF.9 compression on all interfaces is displayed.

Prerequisites

FR compression configurations must be completed before the **display fr compression frf9** command is run to view information about FRF.9 STAC compression.

Example

Display information about FR compression.

```
<Huawei> display fr compression frf9
  Serial1/0/0:0   -DLCI = 22
  sent:
    CompressedPackets  = 10103,  UnCompressedPackets  = 0
    CompressedOctets    = 337695,  OriginalOctets    = 838549
  receive:
    CompressedPackets  = 10101,  UnCompressedPackets  = 0
    CompressedOctets    = 60681,  UnCompressedOctets     = 0
    NotDroppedCompressedPackets = 10101, NotDroppedUnCompressedPackets = 0
    DeCompressedPackets = 10101, DeCompressedOctets = 838383
```

Table 7-22 Description of the display fr compression frf9 command output

Item	Description
Serial1/0/0:0 -DLCI = 22	An FR interface number and the DCLI on the interface
sent	Information of sent packets
CompressedPackets	Number of compressed packets among sent packets
UncompressedPackets	Number of uncompressed packets among sent packets
CompressedOctets	Number of compressed bytes among sent packets
OriginalOctets	Number of original bytes among sent packets

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
receive	Information of received bytes
CompressedPackets	Number of compressed packets among received packets
UnCompressedPackets	Number of uncompressed packets among received packets
CompressedOctets	Number of compressed bytes among received packets
UnCompressedOctets	Number of uncompressed bytes among received packets
NotDroppedCompressedPackets	Number of undropped packets among compressed packets
NotDroppedUnCompressedPackets	Number of undropped packets among uncompressed packets
DeCompressedPackets	Number of decompressed packets
DeCompressedOctets	Number of decompressed bytes

Related Topics

7.6.22 fr compression frf9
7.6.23 fr compression iphc

7.6.7 display fr compression iphc

Function

The **display fr compression iphc** command displays information about IP header compression (IPHC) on an FR interface.

Format

display fr compression iphc [**interface** *interface-type interface-number*[*.subnumber*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about IPHC on a specified FR interface.	-
subnumber	Displays information about IPHC on a specified FR sub-interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

IPHC compression, as a cost-effective bandwidth saving function provided for FR users, saves network bandwidth, reduces network workload, and improves the transmission efficiency.

NOTE

Generally, links working at rates lower than 768 kbps are considered low-speed links.

To monitor the status of an interface or locate an interface fault, run the **display fr compression iphc** command to view statistics about the interface. The command output can provide information for troubleshooting the interface.

NOTE

If no interface is specified, information about FRF.9 compression on all interfaces is displayed.

Prerequisites

IPHC configurations must be completed before the **display fr compression iphc** command is run to view information about IPHC.

Example

Display information about IPHC.

```
<Huawei> display fr compression iphc
Serial1/0/0:0 -DLCI:22
  RTP header compression information:
    Compression:
        RtpTotal      :              0 , RtpCompressed :              0
        RtpLongSearch :              0 , RtpMiss       :              0
        RtpSavedbytes :              0 , RtpSentBytes  :              0
    Decompression:
        RtpTotal      :              0 , RtpCompressed :              0
        RtpError      :              0
    Compression-connections: 256 , Decompression-connections: 256

  Information of TCP header compression:
    Compression:
        TcpTotal      :           9230 , TcpCompressed :           9229
        TcpLongSearch :              0 , TcpMiss       :              1
        TcpSavedbytes :         304557 , TcpSentBytes  :         452303
    Decompression:
        TcpTotal      :              0 , TcpCompressed :              0
        TcpError      :              0
    Compression-connections: 256 , Decompression-connections: 256
```

Table 7-23 Description of the **display fr compression iphc** command output

Item	Description
Serial1/0/0:0 -DLCI:22	An FR interface number and the DCLI value on the interface
RTP header compression information	Statistics about the compressed RTP headers
Compression	Statistics about compressed packets
RtpTotal	Total number of received IPHC RTP packets including full header packets and compressed packets
RtpCompressed	Total number of compressed RTP packets
RtpLongSearch	Ranking of a node in the link table. If the value is 0, the first node is the desired node. If the value is n, the n+1 node is the desired node.
RtpMiss	Total number of uncompressed RTP packets
RtpSavedbytes	Number of saved RTP bytes
RtpSentBytes	Number of sent RTP bytes
Decompression	Statistics about the uncompressed RTP headers
RtpError	Number of received error RTP packets
Information of TCP header compression	Statistics about the compressed TCP headers
TcpTotal	Total number of received IPHC TCP packets including full header packets and compressed packets
TcpCompressed	Total number of compressed TCP packets
TcpLongSearch	Ranking of a node in the link table. If the value is 0, the first node is the desired node. If the value is n, the n+1 node is the desired node.
TcpMiss	Total number of uncompressed TCP packets
TcpSavedbytes	Number of saved TCP bytes
TcpSentBytes	Number of sent TCP bytes
TcpError	Number of received error TCP packets
Compression-connections	Maximum number of compressed connections

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Decompression-connections	Maximum number of decompressed connections

Related Topics

7.6.22 fr compression frf9
7.6.23 fr compression iphc

7.6.8 display fr del

Function

Using the **display fr del** command, you can view detailed information about DE rule lists.

Format

display fr del [*list-number*]

Parameters

Parameter	Description	Value
list-number	Displays information about a specified DE rule list. If no rule list number is specified, all DE rule list information is displayed.	The value is an integer that ranges from 1 to 10.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display fr del** command displays detailed information about DE rule lists, including the rule list number and DE rules.

DE rule lists include interface-based and IP-based DE rule lists. To configure an interface-based DE rule list and an IP-based DE rule list, run the **fr del inbound-interface** and **fr del protocol ip** commands.

Example

Display detailed information about all DE rule lists.

```
<Huawei> display fr del
List      Rule
```

```
1        protocol ip greater-than 1
1        protocol ip
1        protocol ip acl 2000
1        protocol ip fragment
1        protocol ip greater-than 2
1        protocol ip less-than 50
1        protocol ip source-port tcp domain
1        protocol ip source-port udp domain
1        protocol ip  estination-port tcp dom
1        protocol ip  estination-port udp dom

List     Rule
2        protocol ip fragment
```

Table 7-24 Description of the display fr del command output

Item	Description
List	DE rule list number.
Rule	Rule in a DE rule list.

Related Topics

7.6.25 fr del inbound-interface

7.6.26 fr del protocol ip

7.6.9 display fr fragment-info

Function

The **display fr fragment-info** command displays information about FR fragments.

Format

display fr fragment-info [**interface** *interface-type interface-number* [*.subinterface-number*]] [**dlci** *dlci-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about FR fragments on the interface with a specified interface type and number.	-
.subinterface-number	Displays information about FR fragments with a specified sub-interface number.	-
dlci *dlci-number*	Displays information about FR fragments with a specified DLCI.	The value is an integer that ranges from 16 to 1022.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

On a low-speed FR link, large data packets increase the transmission delay. The FR fragmentation mechanism fragments a large data packet into several smaller packets, enabling low-speed FR links to transmit packets with low delay.

When voice and data packets are sent simultaneously, sending large data packets occupies bandwidth for a long period of time. This causes the delay in voice packet transmission or even packet loss. As a result, the voice quality deteriorates. FR fragmentation aims to minimize the voice delay and ensure real-time voice transmission. After FR fragmentation is configured, a large data packet is fragmented into smaller data packets. Subsequently, voice packets and the smaller data packets are sent alternately to ensure that voice packets are processed in a timely manner. This shortens the voice delay.

If FR fragmentation is configured on the device, you can run the **display fr fragment-info** command to view the FR fragmentation configuration and statistics.

When using this command, note the following:

- When no parameter is specified, this command displays the FR fragmentation configuration and statistics of all DLCIs on the device.
- When only **interface** is specified, this command displays the FR fragmentation configuration and statistics of all DLCIs on the specified interface.
- When both **interface** and **dlci** are specified, this command displays the FR fragmentation configuration and statistics of the specified DLCI on the specified interface.

Prerequisites

FR fragmentation has been configured.

Example

Display the FR fragmentation configuration and statistics of all DLCIs on the specified interface.

```
<Huawei> display fr fragment-info interface serial 1/0/0
 interface Serial1/0/0 :
 interface        dlci        type                  size        in/out/drop
 Serial1/0/0      22          FRF12(End to End)     100         4215/5625/0
```

Table 7-25 Description of the display fr fragment-info command output

Item	Description
interface	Interface name.
dlci	Data link connection identifier that identifies a virtual circuit (VC).
type	Fragment type: ● FRF.12
size	Fragment size, in bytes.
in/out/drop	Number of received, send, and dropped fragments.

Display the FR fragmentation configuration and statistics of the specified DLCI on the specified interface.

```
<Huawei> display fr fragment-info interface Serial 3/0/0:0 dlci 22
Type : FRF12(End to End)
 Size : 100
 Pre-fragment:
   out packets:              0,  out bytes  :              0
 Fragmented:
   in packets :              0,  out packets:              0
   in bytes   :              0,  out bytes  :              0
 Assembled  :
   in packets :              0,  in bytes   :              0
 Dropped    :
   in packets :              0,  out packets:              0
   in bytes   :              0,  out bytes  :              0
  Out-of-sequence pkts:              0
```

Table 7-26 Description of the display fr fragment-info command output

Item	Description
Type	Fragment type: ● FRF.12
Size	Fragment size, in bytes.
Pre-fragment	Number of packets to be fragmented.
Fragmented	Number of fragments to be sent.
Assembled	Number of reassembled fragments.
Dropped	Number of dropped fragments.
Out-of-sequence pkts	Number of out-of-sequence fragments.
out pkts / out bytes	Number of outgoing packets or bytes.
in pkts / in bytes	Number of incoming packets or bytes.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.6.48 fragment

7.6.10 display fr dlci-switch

Function

The **display fr dlci-switch** command displays information about FR switching.

Format

display fr dlci-switch [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about an FR switching route on a specified interface. The specified interface can only be a serial, an MFR, or a tunnel interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor the status of an interface or locate an interface fault, run the **display fr dlci-switch** command to view statistics about the interface. The command output can provide information for troubleshooting the interface.

Precautions

If the link layer protocol of the specified interface is not configured to FR, no command output is displayed after the **display fr dlci-switch** command is run on the interface.

Example

Display information about FR switching.

```
<Huawei> display fr dlci-switch
Frame relay switch statistics for board 0
Status   Interface(DLCI)    ---------->   Interface(DLCI)
Inactive Serial1/0/0(110)                Tunnel0/0/1(220)
Active   Tunnel0/0/1(220)                 Serial1/0/0(110)
```

Table 7-27 Description of the **display fr dlci-switch** command output

Item	Description
Frame relay switch statistics for board 0	Statistics about FR switching on board 0
Status	Interface status
Interface(In DLCI) ----------> Interface(Out DLCI)	Inbound interface and DLCI value, and outbound interface and DLCI value."<----->" indicates the mapping relationship between the inbound interface and the outbound interface.

Related Topics

7.6.28 fr dlci-switch

7.6.11 display fr inarp-info

Function

The **display fr inarp-info** command displays statistics about FR InARP packets.

Format

display fr inarp-info [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface. **NOTE** The interface must be a main interface. If no interface is specified, statistics about FR InARP packets on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Inverse ARP is used to parse the protocol address (IP address and IPX address) of the peer device connected to the local device through a VC.

Inverse ARP packets include InARP request packets and InARP response packets. The **display fr inarp-info** command output shows whether InARP works properly.

Prerequisites

InARP is enabled using the **fr inarp** command.

Example

Display the statistics of FR InARP packets.

```
<Huawei> display fr inarp-info
Frame relay InverseARP statistics for interface Serial1/0/0:0 (DTE)
In ARP request    Out ARP reply    Out ARP request    In ARP reply
0                 0                1                  1
```

Table 7-28 Description of the **display fr inarp-info** command output

Item	Description
Frame relay InverseARP statistics for interface Serial1/0/0:0 (DTE)	Indicates the statistics of the FR InARP packets on Serial 1/0/0 with the interface type being DTE.
In ARP request	Indicates the number of received ARP Request packets.
Out ARP reply	Indicates the number of sent ARP Reply packets.
Out ARP request	Indicates the number of sent ARP Request packets.
In ARP reply	Indicates the number of received ARP Reply packets.

Related Topics

7.6.29 fr inarp

7.6.12 display fr interface

Function

The **display fr interface** command displays information about an FR interface.

Format

display fr interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If *interface-type interface-number* is not specified, information about all FR interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Based on the function of the interface on the network, the type of an FR interfaces can be DTE or DCE. In real world situations, an DTE interface can be connected to a DCE interface only. The type of the FR interface on the device that functions as an FR switch must be DCE. The **display fr interface** command can be used to display information about an FR interface, including the type, physical status, and link layer protocol status of the interface.

Prerequisites

To view information about FR sub-interface, you must have successfully created a FR sub-interface.

Configuration Impact

To monitor interface status or locate an interface fault, run the **display fr interface** command to view information about the interface. This information provides a basis for fault location.

Example

Display the status of all FR interfaces.

```
<Huawei> display fr interface
MFR0/0/15, DTE, physical up, protocol up
Serial1/0/0, DTE, physical up, protocol up
Serial2/0/0:1, DTE, physical up, protocol up
Serial2/0/0:2, DTE, physical up, protocol up
```

 Copyright © Huawei Technologies Co., Ltd.

Table 7-29 Description of the **display fr interface** command output

Item	Description
MFR0/0/15	Indicates the interface type and number.
DTE	Indicates the working mode of the interface: • DTE: indicates the working mode of the interface on the user side. • DCE: indicates the working mode of the interface on the network side.
physical up	Indicates that the physical link is Up.
protocol up	Indicates that the link protocol is Up.

Related Topics

7.6.19 display interface mfr

7.6.13 display fr lmi-info

Function

The **display fr lmi-info** command displays the statistics of LMI frames.

Format

display fr lmi-info [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If *interface-type interface-number* is not specified, statistics about LMI frames on all FR interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a PVC is set up, both the DCE and DTE need to be aware of the PVC status. The LMI protocol is used to monitor the PVC status.

The LMI module manages PVCs by adding PVCs, deleting PVCs, and detecting PVC status and integrity of PVC links. LMI packets can be classified into the following:

- Status enquiry packet: sent from the DTE to the DCE to request the PVC status or detect the link integrity.
- Status packet: sent from the DCE to the DTE to respond to a status enquiry packet with the PVC status or link integrity information.

The **display fr lmi-info** command can be used to display statistics about LMI packets on an FR interface.

Prerequisites

The LMI protocol and relevant parameters have been configured.

Precautions

The parameter **interface** in the **display fr lmi-info** command is valid only for a main interface.

Example

Display the statistics of LMI frames.

```
<Huawei> display fr lmi-info
Frame relay LMI statistics for interface MFR0/0/0 (DTE, Q933)
  T391DTE = 10 (hold timer 10)
  N391DTE = 5, N392DTE = 3, N393DTE = 4
  out status enquiry = 0, in status = 0
  status timeout = 0, discarded messages = 0
Frame relay LMI statistics for interface Serial6/0/0 (DCE, Q933)
  T392DCE = 15, N392DCE = 3, N393DCE = 4
  in status enquiry = 250, out status = 250
  status enquiry timeout = 0, discarded messages = 15
```

Table 7-30 Description of the **display fr lmi-info** command output

Item	Description
T391DTE	Indicates the polling timer on the DTE side. It defines the interval for the DTE to send Status Enquiry messages.
N391DTE	Indicates the interval for sending Full Status Enquiry messages. That is, when the counter reaches N391, the Full Status Enquiry messages is sent.
N392DTE	Indicates the error threshold, that is, the maximum number of errors occurring in the observed events.
N393DTE	Indicates the event counter, that is, the total number of the observed events.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
out status enquiry	Indicates the number of sent Status Enquiry messages.
in status	Indicates the number of received Status Reply messages.
status timeout	Indicates the number of times that Status Enquiry messages expire.
discarded messages	Indicates the number of discarded messages.
T392DCE	Indicates a time variable. It defines the longest time for DCE to wait for a status request packet.
N392DCE	N392DCE refers to the above N392DTE. Note that DCE requires T392 rather than T391 to determine the fixed time interval at which DTE sends a status request packet. The time interval of a status request packet sent by DTE is determined by T391.
N393DCE	N393DCE refers to the above N393DTE. Note that DCE requires T392 rather than T391 to determine the fixed time interval at which DTE sends a status request packet. The time interval of a status request packet sent by DTE is determined by T391.

Related Topics

7.6.30 fr interface-type

7.6.14 display fr map-info

Function

The **display fr map-info** command displays mappings between IP addresses and DLCI values.

Format

display fr map-info [**interface** *interface-type interface-number*] [**dlci** *dlci-number*]

display fr map-info pvc-group [[*pvc-group-name*] **interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface.	The interface can also be a sub-interface. If no interface is specified, information about all interfaces will be displayed.
dlci *dlci-number*	Specifies the DLCI value.	The value is an integer ranging from 16 to 1022.
pvc-group *pvc-group-name*	Specifies the PVC group name.	The value is a string of 1 to 16 characters. If no PVC name is specified, information about all PVCs of specified FR interfaces will be displayed.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

As a statistics multiplexing protocol, the FR protocol provides multiple VCs over a single physical link. VCs are differentiated by DLCIs. A PVC is valid only on an interface and its directly connected interface. The same DLCI values on different physical interfaces of an FR network do not indicate the same PVC.

A maximum of 1024 VCs are supported on an FR interface. The FR address mapping is defined to associate the protocol address of the remote device with the FR address (the local DLCI) of the remote device. After that, the higher-layer protocol can discover the remote device based on the protocol address of the remote device.

The **display fr map-info** command can be used to display the mapping between the destination IP address and DLCI.

Prerequisites

The mapping between the destination IP address and DLCI is defined manually or using InARP.

- For manual mapping configuration, see **fr map ip**.
- For mapping configuration using InARP, see **fr inarp**.

Example

Display mappings between IP addresses and DLCI values.

```
<Huawei> display fr map-info
Map Statistics for interface Serial1/0/0:0 (DCE)
```

```
DLCI = 200, IP 2.2.2.2, Serial1/0/0:0
  create time = 2010/12/02 00:08:29, status = INACTIVE
  encapsulation = ietf, vlink = 3
```

Table 7-31 Description of the display fr map-info command output

Item	Description
Map Statistics for interface Serial1/0/0:0 (DCE)	Indicates mappings between IP addresses and DLCI values on Serial 1/0/2:0 in DCE mode.
DLCI	Indicates the Data-Link Connection Identifier.
Serial1/0/0:0	Indicates the type and number of the interface to which the DLCI values and dynamically-learned IP addresses belong.
create time	Indicates the time a mapping between an IP address and a DLCI value is created.
status	Indicates the address mapping status.
encapsulation	Indicates the protocol encapsulation type for the interface. To change the encapsulation type, run the **link-protocol fr** command.
vlink	Indicates the index of vlink.
broadcast	Indicates that broadcast is enabled. If broadcast is not enabled, this field is not displayed.

Related Topics

7.6.41 fr map ip
7.6.29 fr inarp

7.6.15 display fr pvc-group

Function

The **display fr pvc-group** command displays information about a specific PVC group or all PVC groups.

Format

display fr pvc-group [[*pvc-group-name* [**verbose**]] **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
pvc-group-name	Specifies the PVC group name. The value is created by the **fr pvc-group** command. If no PVC group name is specified, information about all PVC groups on the specific interface is displayed.	The value is a string of 1 to 16 characters.
verbose	Displays detailed information.	-
interface *interface-type interface-number*	Specifies the interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Configuring a PVC group allows PVCs with the same destination address to forward packets at the same time and packets with different priorities to be transmitted along separate PVCs. If IP packets need to be transmitted along FR PVCs in a PVC group, map the ToS fields of IP packets to FR PVCs so that IP packets with different priorities are transmitted along separate PVCs. In addition, each PVC in the group can be configured with a different QoS policy for transmitting a specific type of services.

To monitor the status of an interface or locate an interface fault, run the **display fr pvc-group** command to view status of the interface and statistics on the interface. The command output provides a basis for statistics collection and interface troubleshooting.

Prerequisites

A PVC group is created and PVCs are added to the PVC group.

Example

Display information about all PVC groups.

```
<Huawei> display fr pvc-group
PVC-GROUP-name    State     TosType     INARP   Interface        Type PhyStatus
abc             Inactive  PRECEDENCE  Enable  Serial1/0/0      DTE  Down
def             Inactive  PRECEDENCE  Enable  Serial1/0/0      DTE  Down
```

Display information about the PVC group named **abc**.

```
<Huawei> display fr pvc-group abc verbose interface serial 1/0/0
PVC-GROUP-name: abc
  state: Inactive, TosType: PRECEDENCE, INARP: Enable
  Interface: Serial1/0/0, Type: DTE, PhyStatus: Down
  Grade   ForwardDLCI  ConfigDLCI
  0       -            200
  1       -            200
  2       -            100
  3       -            -
  4       -            -
  5       -            -
  6       -            -
  7       -            -
```

Table 7-32 Description of the display fr pvc-group command output

Item	Description
PVC-GROUP-name	Indicates the name of a PVC group.
State	Indicates the PVC group status: ● ACTIVE ● INACTIVE
TosType	Indicates the ToS type: ● PRECEDENCE ● DSCP ● NONE
INARP	Indicates whether or not InARP is enabled: ● ENABLE ● DISABLE
Interface	Indicates the interface number.
Type	Indicates the interface type.
PhyStatus	Indicates the physical status of the interface: ● Up ● Down
Grade	Indicates the priority value: ● The IP Precedence value ranges from 0 to 7. ● The DSCP value ranges from 0 to 63.
ForwardDLCI	Indicates the DLCI of a PVC that forwards packets with a specific IP Precedence or DSCP value.
ConfigDLCI	Indicates the DLCI of a PVC that is configured to forward packets with a specific IP Precedence or DSCP value.

Related Topics

7.5.22 pvc-group

7.6.16 display fr pvc-info

Function

The **display fr pvc-info** command displays configurations and statistics about FR PVCs.

Format

display fr pvc-info [**interface** *interface-type interface-number*[*.subinterface-number*]] [**dlci** *dlci-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
.subinterface-number	Specifies the sub-interface number.	-
dlci *dlci-number*	Specifies the DLCI.	The value ranges from 16 to 1022.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

As a cost-effective solution provided for FR users, FRF.9 compression saves network bandwidth resources, reduces network loads, and improves the transmission efficiency.

If FRF.9 compression has been configured, the **display fr pvc-info** command can be used to view configurations and statistics about FRF.9 compression.

When using the **display fr pvc-info** command, note the following points:

- If no parameter is specified, the configuration and statistics about PVCs on all interfaces are displayed.
- If only the parameter **interface** is specified, the configuration and statistics about PVCs on the specific interface are displayed.
- If both **interface** and **dlci** are specified, information about the specified PVC on the specified interface is displayed, including configurations and statistics about the PVC and FR QoS.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The configurations of FR interfaces and DLCIs are complete.

Example

Display configurations and statistics about FR PVCs.

```
<Huawei> display fr pvc-info
PVC statistics for interface MFR0/0/15 (DTE, physical UP)
    DLCI = 1007, USAGE = LOCAL (00000010), MFR0/0/15
    create time = 2011/03/23 15:11:28, status = ACTIVE
    InARP = Enable, PVC-GROUP = NONE
    in packets = 146122, in bytes = 7672736
    out packets = 1443, out bytes = 423664

PVC statistics for interface Serial1/0/0 (DTE, physical UP)
    DLCI = 16, USAGE = LOCAL (00000010), Serial1/0/0
    create time = 2011/03/22 16:48:49, status = ACTIVE
    InARP = Enable, PVC-GROUP = NONE
    in packets = 53796932, in bytes = 2922267712
    out packets = 602423292, out bytes = 30121124060
```

Table 7-33 Description of the display fr pvc-info command output

Item	Description
DLCI	Indicates the data link connection identifier.
USAGE	Indicates how the PVC is obtained. LOCAL indicates that the PVC is configured locally; UNUSED indicates that the PVC is learned from the DCE side.
create time	Indicates the creation time of the PVC.
status	Indicates the PVC status. The values are: ● active ● inactive
InARP	Indicates whether the InARP function is enabled.
PVC-GROUP	Indicates the PVC group to which the PVC belongs. NONE indicates that the PVC does not belong to any PVC group.
in packets	Indicates the number of packets received by the PVC.
in bytes	Indicates the number of bytes received by the PVC.
out packets	Indicates the number of packets sent by the PVC.
out bytes	Indicates the number of bytes sent by the PVC.

 Copyright © Huawei Technologies Co., Ltd.

7.6.17 display fr statistics

Function

The **display fr statistics** command displays the statistics of currently received and sent data on the FR interface.

Format

display fr statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and the number of an interface. **NOTE** You can specify only main interfaces by using *interface-type interface-number*. If no interface is specified, the statistics of all FR interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor interface status or locate an interface fault, run the **display fr statistics** command to view interface status and statistics. The command output provides a basis for statistics collection and interface troubleshooting.

Example

Display the statistics of currently received and sent data on the FR interface.

```
<Huawei> display fr statistics interface mfr 0/0/3
Frame relay packet statistics for interface MFR0/0/3 (DTE)
  in packets = 2132202, in bytes = 25592466
  out packets = 2132208, out bytes = 25592426
```

Table 7-34 Description of the **display fr statistics** command output

Item	Description
in packets	Number of received packets
in bytes	Number of received bytes
out packets	Number of sent packets

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
out bytes	Number of sent bytes

Related Topics

7.6.12 display fr interface

7.6.18 display fr switch-table

Function

The **display fr switch-table** command displays information about the switching table of the router.

Format

display fr switch-table [**name** *name*]

Parameters

Parameter	Description	Value
name *name*	Displays information about an FR switching table with a specified FR switch name.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor interface status or locate an interface fault, run the **display fr switch-table** command to view interface status and statistics. The command output helps users troubleshoot the interface.

Example

View information in the current switching table of the router.

```
<Huawei> display fr switch-table
Total PVC switch records:1
PVC-Name                    Status   Interface(DLCI) <-----> Interface(DLCI)
pvc1                      Active   Serial1/0/0(300)        Tunnel0/0/2(500)
```

Table 7-35 Description of the **display fr switch-table** command output

Item	Description
PVC-Name	Name of a PVC
Status	Status of a PVC
Interface(DLCI) <-----> Interface(DLCI)	Inbound interface and DLCI value, and outbound interface and DLCI value

Related Topics

7.6.45 fr switch

7.6.19 display interface mfr

Function

The **display interface mfr** command displays the configuration, status, and packet statistics of an MFR interface.

Format

display interface mfr [*interface-number* [*.subnumber*]]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a bound interface.	-
.subnumber	Specifies the sub-interface number of a bound interface.	The number is an integer ranging from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor the status of an interface or locate an interface fault, run the **display interface mfr** command to view status of the interface and statistics on the interface. The command output provides a basis for statistics collection and interface troubleshooting.

 Copyright © Huawei Technologies Co., Ltd.

The **display mfr** command can also be used to view the status of the MFR interface and statistics on the MFR interface. The **display interface mfr** and **display mfr** commands are used in different scenarios:

- The **display interface mfr** command is used to obtain basic configuration of an MFR interface (including the link layer protocol and link status).
- The **display mfr** command is used to obtain detailed statistics about packets on an MFR interface (including hello packets and ACK packets).

Precautions

If no interface is specified, information about all interfaces is displayed.

Example

Display the configuration and status of MFR 0/0/3.

```
<Huawei> display interface mfr 0/0/3
MFR0/0/3 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, MFR0/0/3 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : UP
Link layer protocol is FR IETF
  LMI DLCI is 0, LMI type is Q.933a, frame relay DTE
  LMI status enquiry sent 0, LMI status received 0
  LMI status timeout 0, LMI message discarded 0
Physical is MFR, baudrate: 0 bps
Current system time: 2011-02-23 16:14:09-08:00
    Last 300 seconds input rate 0 bytes/sec, 0 packets/sec
    Last 300 seconds output rate 0 bytes/sec, 0 packets/sec
    Realtime 206 seconds input rate 0 bytes/sec, 0 packets/sec
    Realtime 206 seconds output rate 0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
    0 packets output, 0 bytes, 0 drops
    Input bandwidth utilization  : 0.00%
    Output bandwidth utilization : 0.00%
```

Table 7-36 Description of the **display interface mfr** command output

Item	Description
MFR0/0/3 current state	Indicates the physical status of MFR 0/0/3: ● UP: indicates that the physical status of the interface is Up. ● DOWN: indicates that the physical status of the interface is Down. ● Administratively Down: indicates that the administrator runs the **shutdown** command on the interface.
Line protocol current state	Indicates the status of the link protocol of the interface: ● UP: indicates that the link protocol status of the interface is Up. ● DOWN: indicates that the link protocol status of the interface is Down.

Item	Description
Last line protocol up time	Indicates the last time when the link protocol of the interface goes Up.
Description	Indicates the description of the interface, which are case sensitive and support blank spaces. A maximum of characters can be entered. The description can help you to learn about the functions of the interface.
The Maximum Transmit Unit is	Indicates the MTU. By default, it is 1500 bytes. The packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet Address is	Indicates the IP address and the subnet mask of the interface.
Link layer protocol is	Indicates the link layer protocol.
LMI DLCI is 0, LMI type is Q.933a, frame relay DTE	Indicates that the DLCI used by LMI is 0, the LMI type is Q.933A on the FR DTE side.
LMI status enquiry sent, LMI status received	Indicates the number of sent Status Enquiry messages and the number of received Status messages.
LMI status timeout, LMI message discarded	Indicates the number of times that the LMI Status Enquiry message times out and the number of discarded LMI messages.
Physical is MFR, baudrate	Indicates the baud rate and that the physical link is MFR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output queue : (Urgent queue : Size/Length/Discards)Output queue : (Protocol queue : Size/Length/Discards)Output queue : (FIFO queuing : Size/Length/Discards)	Indicates the current status of the output queue, including: ● Urgent queue: The protocol packets at the link layer, such as the PPP negotiation packets and Keepalive packets, enter this queue. ● Protocol queue: The packets with the priority being 6 enter this queue. ● Common queue: The queue may be First In First Out queue (FIFO queue), Priority Queue (PQ), Custom Queue (CQ), or Class-based Queue (CBQ) according to the queue type applied to the interface. When congestion occurs, the interface first sends the packets in the urgent queue, then the packets in the protocol queue, and last the packets in the common queue. The fields of each output queue are described as follows: ● Size: indicates the number of packets in the queue. ● Length: indicates the maximum number of packets in the queue. ● Discards: indicates the number of packets discarded because the queue is full. According to the value of Discards, you can determine whether the interface capacity meets the forwarding requirements. For example, when the value of Discards is greater than the other two values, it indicates that the router may be busy with other tasks and cannot process the packets in the queue. If this situation lasts for a long period, it indicates that the router of higher performance is required.
Current system time	Indicates the current system time. If the system is configured with a time zone and is in the summer time, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.
Statistics last cleared	Indicates the last time when interface statistics are cleared.
Last 300 seconds input rate Last 300 seconds output rate	Indicates the rates for sending and receiving bytes and packets on the interface in the last 300 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
8 packets input, 206 bytes, 0 drops8 packets output, 222 bytes, 0 drops	The field indicates the following: • Total number of packets and bytes received and sent on the interface • Number of packets discarded because of insufficient buffer space

Related Topics

7.6.12 display fr interface

7.6.20 display mfr

Function

The **display mfr** command displays configuration and statistics of the MFR bundle and bundle link.

Format

display mfr [**interface** *interface-type interface-number* | **verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies an interface.	-
verbose	Displays detailed information, including the number of sent and received control packets.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To monitor the status of an interface or locate an interface fault, run the **display mfr** command to view status of the interface and statistics on the interface. The command output provides a basis for statistics collection and interface troubleshooting.

 Copyright © Huawei Technologies Co., Ltd.

The **display interface mfr** command can also be used to view the status of the MFR interface and statistics on the MFR interface. The **display mfr** and **display interface mfr** commands are used in different scenarios:

- The **display interface mfr** command is used to obtain basic configuration of an MFR interface (including the link layer protocol and link status).
- The **display mfr** command is used to obtain detailed statistics about packets on an MFR bundle link (including hello packets and ACK packets).

Precautions

If no bundle or bundle link is specified, information about all bundles and bundle links is displayed.

Example

View the configuration and status of all FR bundles and FR bundle links.

```
<Huawei> display mfr
Bundle interface:MFR0/0/0, Bundle state = up,  Bundle class = A,
   Fragment disabled
   Bundle name = bundle
   Bundle links:
   Serial1/0/0, PHY state = Administratively up, link state = up  Link name
 : linkname
```

View the detailed status of all FR bundle links.

```
<Huawei> display mfr verbose
Bundle interface:MFR0/0/0, Bundle state = up,  Bundle class = A,
   Fragment disabled, Bundle fragment size = 300
   Bundle name = MFR0/0/3, Bundle links up number = 1
   Bundle links:
   LID : Serial1/0/0 Peer LID:
   Bound to MFR0/0/0(BID:bundle) Peer BID:
   Physical state: Administratively up, link state: up
   Bundle Link statistics:
      Hello(TX/RX):        0/0    Hello_ack(TX/RX):       0/0
      Add_link(TX/RX):     0/0    Add_link_ack(TX/RX):    0/0
      Add_link_rej(TX/RX):  0/0
      Remove_link(TX/RX):   0/0    Remove_link_ack(TX/RX):  0/0
      Pkts dropped(in/out): 0/0
      Timer: ACK  2, Hello  3
      Retry: Max  3, Current 0
      Cause code: none
```

Table 7-37 Description of the **display mfr** command output

Item	Description
Bundle interface	Bundle interface.
Bundle state	Running state of bundle interface.
Bundle class	Class A indicates if there is one bundle link is in the Up status, the bundle is flagged as Up. The bundle is Down only after all bundle links are Down.
Bundle fragment size	Maximum fragment size allowed on an FR bundle link.
Bundle links	Physical interface information of each bundle link.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Bundle links up number	Number of member links in Up state.
LID	Bundle link identifier. By default, it is the interface name of the current bound link.
Peer LID	Bundle link identifier of the peer end. By default, it is the interface name of the peer bound link.
Physical state	Operating status of the physical interface.
Link state	Operating status of the bundle link protocol.
Bundle Link statistics	Packet statistics of the bundle link.
Hello (TX/RX)	Number of "Hello" packets sent and received. The "Hello" packet maintains link status.
Hello_ack (TX/RX)	Number of "Hello" acknowledgement packets sent and received. The "Hello_ack" packet notifies the peer that a "Hello" packet has been received.
Add_link (TX/RX)	Number of "Add_link" packets sent and received. The "Add_link" packet notifies the peer that the local node has prepared for processing frames.
Add_link_ack (TX/RX)	Number of "Add_link" acknowledgement packets transmitted and received. The "Add_link_ack" packet notifies the peer that an "Add_link" packet has been received.
Add_link_rej (TX/RX)	Number of "Add_link" reject packets transmitted and received. The "Add_link_rej" packet is used to notify the peer that an "Add_link" packet has been rejected.
Remove_link (TX/RX)	Number of "Remove_link" packets transmitted and received. The "Remove_link" packet notifies the peer that the local node is removing a bundle link from the bundle.
Remove_link_ack (TX/RX)	Number of "Remove_link" acknowledgement packets transmitted and received. The "Remove_link_ack" packet notifies the peer that a "Remove_link" packet has been received.
Pkts dropped (in/out)	Number of discarded packets that are sent and received.
Timer	The time of waiting for Hello acknowledgement message before the bundle link retransmits a Hello message or retransmits an "Add_link" message used for initial synchronization.
Hello 10	Interval for the bundle link to send a Hello message.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Retry	Maximum retry times for the bundle link to retransmit a Hello message or retransmit an "Add_link" packet that is used for initial synchronization before the bundle link waits for the Hello acknowledgement message.
Current 0	Current retried times.
Cause code	The reason for the bundle link to be in the current status.

Related Topics

7.6.52 link-protocol fr mfr
7.6.50 interface mfr

7.6.21 fr class

Function

Using the **fr class** command, you can create an FR class and enter the FR class view.

Using the **undo fr class** command, you can delete an FR class.

By default, no FR class is created.

Format

fr class *name*

undo fr class *name*

Parameters

Parameter	Description	Value
name	Specifies the name of an FR class to be created or the FR class view to be displayed.	The value is a string of 1 to 31 case-insensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the configured FR class parameters take effect, run the **fr-class** command to associate the FR class with an interface or a VC and enable FR QoS on the interface.

Follow-up Procedure

Set parameters such as queue parameters and traffic shaping parameters for FR VCs in the created FR class view.

Example

Create an FR class named **huawei**.

```
<Huawei> system-view
[Huawei] fr class huawei
[Huawei-fr-class-huawei]
```

Related Topics

7.6.49 fr-class

7.6.22 fr compression frf9

Function

The **fr compression frf9** command enables FRF.9 STAC compression.

The **undo fr compression frf9** command disables FRF.9 STAC compression.

By default, FR compression is disabled.

Format

fr compression frf9

undo fr compression frf9

Parameters

None

Views

Serial sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FRF.9 STAC compression, as a cost-effective bandwidth saving function provided for Frame Relay (FR) users, saves network bandwidth resources, reduces network loads, and improves the transmission efficiency.

NOTE

Generally, links working at rates lower than 768 kbps are considered low-speed links.

The procedure for configuring FRF.9 STAC compression is described below:

1. Run the **fr compression frf9** command on P2P FR sub-interfaces to enable FR compression.

   NOTE

   The FR encapsulation format must be IETF.

2. Run the **fr map ip** command on FR main interfaces or P2MP FR sub-interfaces to enable FR compression.

Prerequisites

Before using the **fr compression frf9** command, run the **fr dlci** command to configure a DLCI on an interface.

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Precautions

FRF.9 compression must be enabled on both ends of an FR link.

FRF.9 compression includes a synchronization process. If packet mis-sequence occurs during synchronization, compression may fail.

FR compression takes effect after the **shutdown** and **undo shutdown** commands are executed in sequence to restart the FR interface.

If the **fr map ip** command is run on an interface and the **nonstandard** parameter is configured in the command to set the packet format supported by the FR interface to nonstandard, the **fr compression frf9** command is unavailable on the interface.

Example

Enable FR compression on the P2P sub-interface serial 1/0/0.1.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] quit
[Huawei] interface serial 1/0/0.1 p2p
[Huawei-Serial1/0/0.1] fr dlci 100
[Huawei-fr-dlci-Serial1/0/0.1-100] quit
[Huawei-Serial1/0/0.1] fr compression frf9
```

Related Topics

7.6.41 fr map ip

7.6.23 fr compression iphc

Function

The **fr compression iphc** command enables IPHC compression on an FR interface.

The **undo fr compression iphc** command disables IPHC compression on an FR interface.

By default, IPHC compression is disabled on an FR interface.

Format

fr compression iphc [**nonstandard** | **rtp-connections** *number1* | **tcp-connections** *number2* | **tcp-include**]

undo fr compression iphc [**nonstandard** | **rtp-connections** | **tcp-connections** | **tcp-include**]

Parameters

Parameter	Description	Value
nonstandard	Sets the packet format supported by the FR interface to nonstandard. If the remote devices are Huawei devices, configure the encapsulation format to **nonstandard.**	-
rtp-connections *number1*	Specifies the maximum number of connections for RTP header compression.	The value is an integer and the default value is 256. For the AR2240 and AR3260, the number of RTP connections varies depending on different SRUs. ● SRU40, SRU80, SRU100E, SRU200, SRU200E, and SRU60: 3-256 ● SRU400: 3-1000 For the AR3670 (SRUX5), the value ranges from 3 to 1000. For other models, the value ranges from 3 to 256.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tcp-connections *number2*	Specifies the maximum number of connections for TCP header compression.	The value ranges from 3 to 256, and the initial number is 256.
tcp-include	Indicates that RTP compression includes TCP header compression.	-

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPHC compression provides a cost-effective solution for FR users by compressing IP headers to save network bandwidth, reduce network workload, and improve transmission efficiency on the FR network.

NOTE

Generally, links working at rates lower than 768 kbps are considered low-speed links.

Prerequisites

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Configuration Impact

When the **undo fr compression iphc** command is used to cancel IPHC compression, the **fr compression iphc** command configuration is automatically deleted.

Precautions

- IPHC compression must be enabled on both ends of an FR link.
- RTP header compression is performed for the packets sent by multiple users when the packets pass through the FR link. When the number of connections for RTP header compression exceeds the packet rate, the RTP header compression function may not take effect due to the compression aging mechanism. It is recommended that the number of connections for RTP header compression should be configured to be less than the packet rate (unit: pps).

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If the compression aging mechanism is used, the device checks compression connections once every second and ages the compression connections that are not used recently.

- FR compression takes effect after the **shutdown** and **undo shutdown** commands are executed in sequence to restart the FR interface or MFR interface.

Example

Configure IP header compression on serial 1/0/0, and configure the number of RTP compression connections is 200.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr compression iphc
[Huawei-Serial1/0/0] fr compression iphc rtp-connections 200
```

7.6.24 fr de del

Function

Using the **fr de del** command, you can apply a Discard Eligibility (DE) rule list to a specified FR VC.

Using the **undo fr de del** command, you can delete a DE rule list from an FR VC.

By default, no DE rule list is applied to an FR VC.

Format

fr de del *list-number* **dlci** *dlci-number*

undo fr de del *list-number* **dlci** *dlci-number*

Parameters

Parameter	Description	Value
list-number	Specifies the number of the DE rule list to be applied.	The value is an integer that ranges from 1 to 10.
dlci *dlci-number*	Specifies the FR VC to which a DE rule list is applied.	The value is an integer that ranges from 16 to 1022.

Views

FR interface view, FR sub-interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

When network congestion occurs, a Data Circuit-terminating Equipment (DCE) first discards packets with the DE bit 1 to relieve network congestion.

If a DE rule list is applied to an FR VC, and packets transmitted over the VC match rules in the DE rule list, the DE bit of the packets is set to 1.

Example

Apply DE rule list 3 to a VC with DLCI 100 on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr dlci 100
[Huawei-fr-dlci-Serial1/0/0-100] quit
[Huawei-Serial1/0/0] fr de del 3 dlci 100
```

Related Topics

7.6.25 fr del inbound-interface

7.6.26 fr del protocol ip

7.6.25 fr del inbound-interface

Function

Using the **fr del inbound-interface** command, you can configure an interface-based Discard Eligibility (DE) rule list.

Using the **undo fr del inbound-interface** command, you can delete a specified DE rule from an interface-based DE rule list.

By default, no interface-based DE rule list is configured.

Format

fr del *list-number* **inbound-interface** *interface-type interface-number*

undo fr del *list-number* **inbound-interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
list-number	Specifies the number of the interface-based DE rule list to be configured.	The value is an integer that ranges from 1 to 10.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the number of the inbound interface to which DE rules are applied.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When network congestion occurs, a Data Circuit-terminating Equipment (DCE) first discards packets with the DE bit 1 to relieve network congestion.

After an interface-based DE rule list is configured, a router sets the DE bit of packets received from a specified interface to 1 before forwarding them as FR packets. When network congestion occurs, packets with the DE bit 1 are discarded first.

Precautions

If you run the **fr del inbound-interface** command repeatedly, you can add new rules into a DE rule list. A DE rule list contains a maximum of 100 DE rules.

Before deleting a DE rule list, delete all DE rules from the DE rule list.

Example

Add a rule into DE rule list 3 to set the DE bit of packets received from Serial1/0/0 to 1 before these packets are forwarded as FR packets.

```
<Huawei> system-view
[Huawei] fr del 3 inbound-interface serial 1/0/0
```

Related Topics

7.6.24 fr de del

7.6.26 fr del protocol ip

7.6.26 fr del protocol ip

Function

Using the **fr del protocol ip** command, you can configure an IP-based Discard Eligibility (DE) rule list.

Using the **undo fr del protocol ip** command, you can delete a specified DE rule from an IP-based DE rule list.

By default, no IP-based DE rule list is configured.

Format

fr del *list-number* **protocol ip** [**fragments** | **acl** *acl-number* | **less-than** *bytes* | **greater-than** *bytes* | **source-port** { **tcp** *ports* | **udp** *ports* } | **destination-port** { **tcp** *ports* | **udp** *ports* }]

undo fr del *list-number* **protocol ip** [**fragments** | **acl** *acl-number* | **less-than** *bytes* | **greater-than** *bytes* | **source-port** { **tcp** *ports* | **udp** *ports* } | **destination-port** { **tcp** *ports* | **udp** *ports* }]

Parameters

Parameter	Description	Value
list-number	Specifies the number of the IP-based DE rule list to be configured.	The value is an integer that ranges from 1 to 10.
fragments	Indicates that DE rules will be applied to all fragmented IP packets.	-
acl *acl-number*	Indicates that DE rules will be applied to IP packets matching a specified ACL rule.	The value of *acl-number* is an integer that ranges from 2000 to 3999.
less-than *bytes*	Indicates that DE rules will be applied to IP packets smaller than the specified number of bytes.	The value of *bytes* is an integer that ranges from 0 to 65535, in bytes.
greater-than *bytes*	Indicates that DE rules will be applied to IP packets greater than the specified number of bytes.	The value of *bytes* is an integer that ranges from 0 to 65535, in bytes.
source-port	Indicates that DE rules will be applied based on the source port number.	-
destination-port	Indicates that DE rules will be applied based on the destination port number.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tcp *ports*	Indicates that DE rules will be applied to IP packets with the specified TCP port number.	The value of *ports* is a string of characters and varies according to devices.
udp *ports*	Indicates that DE rules will be applied to IP packets with the specified UDP port number.	The value of *ports* is a string of characters and varies according to devices.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When network congestion occurs, a Data Circuit-terminating Equipment (DCE) first discards packets with the DE bit 1 to relieve network congestion.

After an IP-based DE rule list is configured, a router identifies the IP packets that need to be marked based on the configure DE rules and sets the DE bit of these packets to 1 before forwarding them as FR packets. When network congestion occurs, packets with the DE bit 1 are discarded first.

Precautions

If no parameter is specified in the **fr del protocol ip** command, DE rules will be applied to all IP packets.

If you run the **fr del protocol ip** command repeatedly, you can add new rules into a DE rule list. A DE rule list contains a maximum of 100 DE rules.

Before deleting a DE rule list, delete all DE rules from the DE rule list.

Example

Add a rule into DE rule list 3 to set the DE bit of all FR packets into which IP packets are encapsulated to 1.

```
<Huawei> system-view
[Huawei] fr del 3 protocol ip
```

Related Topics

7.6.24 fr de del

7.6.25 fr del inbound-interface

7.6.27 fr dlci

Function

The **fr dlci** command configures a PVC for an FR interface.

The **undo fr dlci** command deletes a PVC configured on an FR interface.

Format

fr dlci *dlci-number*

undo fr dlci [*dlci-number*]

Parameters

Parameter	Description	Value
dlci-number	Specifies the DLCI number. • If *dlci-number* is not specified in the **undo fr dlci** command, all DLCI configurations on the interface will be deleted. • If the **undo fr dlci** command is configured on an FR interface, the DLCI configurations on the FR sub-interfaces will not be deleted.	The value is an integer ranging from 16 to 1022 among which DLCIs 1008 to 1022 are reserved.

Views

FR interface view, FR sub-interface view, MFR interface view or FR PVC group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a statistics multiplexing protocol, the FR protocol provides multiple VCs over a single physical link. VCs are identified by DLCIs. The **fr dlci** command can be used to configure VCs for an FR interface.

- When the type of an FR interface is DCE, manually configure VCs on the FR interface or its sub-interfaces.
- When the type of an FR interface is DTE, the system automatically specifies VCs based on the peer device if the interface is an FR interface; you need to manually specify VCs on the DCE and DTE if the interface is an FR sub-interface.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The **fr interface-type** command can be used to set the type of an FR interface.

Prerequisites

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Configuration Impact

A DLCI is valid only on the local interface and its directly connected interface. The same DLCI values on different physical interfaces of an FR network do not indicate the same PVC.

If you run the **fr dlci** command several times, the latest configuration overrides the previous one.

Precautions

The DLCI on the DTE must be the same as that on the DCE.

Example

Assign a PVC with the DLCI value of 100 to the FR sub-interface Serial1/0/0.1.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] quit
[Huawei] interface serial 1/0/0.1
[Huawei-Serial1/0/0.1] fr dlci 100
[Huawei-fr-dlci-Serial1/0/0.1-100]
```

Related Topics

7.6.30 fr interface-type

7.6.28 fr dlci-switch

Function

The **fr dlci-switch** command configures FR switching route.

The **undo fr dlci-switch** command deletes the configured FR switching route.

By default, no FR switching route is configured.

Format

fr dlci-switch *dlci-number* **interface** *interface-type interface-number* **dlci** *dlci-number*

undo fr dlci-switch *dlci-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dlci *dlci-number*	Specifies the inbound and outbound DLCI value.	The value is an integer ranging from 16 to 1022.
interface *interface-type interface-number*	Specifies the outbound interface. Only a tunnel interface can be specified as the outbound interface.	-

Views

FR interface view, MFR interface view, POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The FR protocol, as a statistics multiplexing protocol, can provide multiple VCs over a single physical line. FR switching is a typical FR application. In an FR switching scenario, DCE devices exchange and forward IP packets at the data link layer through PVCs. FR switching can be implemented in the following modes:

- FR switching route: The **fr dlci-switch** *in-dlci* **interface** *interface-type interface-number* **dlci** *out-dlci* command is used to specify the outbound interface and DLCI of a forwarded packet to create a switching route.

  The interface on which the packet is forwarded can be an FR interface or an MFR interface. If a tunnel interface is specified as the outbound interface, FR packets can be transmitted over an IP network.
- FR switching PVCs: A switching route is created on two interfaces of a device to forward packets. For details, see description of the **fr switch** command.

Prerequisites

The link layer protocol of interfaces must be FR. The **link-protocol fr** command can be used to configure the link layer protocol as FR.

Before configuring FR switching routes, run the **fr switching** command to enable the FR switching function.

Configuration Impact

After the **fr dlci-switch** is run, Inverse ARP packets cannot be sent on the PVC enabled with FR switching and dynamic MAP entries cannot be created. The dynamic MAP entries on the DLCI will be automatically deleted.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- The interface enabled with FR switching must be a DCE interface. The FR switching function takes effect only after the **fr interface-type** command is used to set the FR interface type.
- Only the DLCI that is configured on the interface can be specified in the command.
- The DLCI that is configured in the FR PVC group view cannot be specified in the **fr dlci-switch** command.
- The DLCI that is configured in the **fr map ppp**, **fr map ip**, or **fr map bridge** command cannot be specified in the **fr dlci-switch** command.
- Different interfaces cannot be configured with the same FR switching route. To be specific, do not specify the same DLCI and outbound interface in the **fr dlci-switch** command for different interfaces.

Example

Configure a static route on which packets on serial 1/0/0 with the DLCI value of 200 can be forwarded through the tunnel interface 0/0/1 with the DLCI value of 300.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] fr dlci-switch 200 interface tunnel0/0/1 dlci 300
```

Related Topics

7.6.46 fr switching

7.6.29 fr inarp

Function

The **fr inarp** command enables FR InARP.

The **undo fr inarp** command disables FR InARP.

By default, FR InARP is enabled.

Format

FR interface view:

fr inarp [**ip** [*dlci-number* | **pvc-group** *pvc-group-name*]]

undo fr inarp [**ip** [*dlci-number* | **pvc-group** *pvc-group-name*]]

MFR interface view:

fr inarp [**ip** [*dlci-number*]]

undo fr inarp [**ip** [*dlci-number*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip	Indicates that InARP is performed for IP protocols.	-
dlci-number	Specifies the DLCI number.	The value is an integer ranging from 16 to 1022.
pvc-group *pvc-group-name*	Specifies the PVC group name.	The value is a string of 1 to 16 case-insensitive characters.

Views

FR interface view, MFR interface view, or POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Inverse ARP is used to parse the protocol address (including the IP address and IPX address) of the peer device connected to the local device through a VC.

After the **fr inarp** command is used to enable FR InARP, the mapping between the peer IP address and the DLCI is automatically defined on the local device. You do not need to manually configure the mapping.

Prerequisites

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Configuration Impact

If you run the **fr inarp** command several times, the latest configuration overrides the previous one.

Precautions

If the static mapping or dynamic mapping has been created, the local device does not send Inverse ARP request packets to the peer device regardless of whether the peer address in the static mapping is correct. The local device sends Inverse ARP packets to the peer device only when no mapping is defined.

After the device receives Inverse ARP request packets, no dynamic mapping will be defined if the protocol address of the peer device is the same as that in the mapping configured on the device.

Example

Enable InARP on all PVCs of the FR interface Serial 1/0/0:0.

```
<Huawei> system-view
```

```
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr inarp
```

Related Topics

7.6.62 reset fr inarp

7.6.14 display fr map-info

7.6.30 fr interface-type

Function

The **fr interface-type** command sets the FR interface type.

The **undo fr interface-type** command restores the default type.

By default, the FR interface type is DTE.

Format

fr interface-type { **dce** | **dte** }

undo fr interface-type

Parameters

Parameter	Description	Value
dce	Indicates the type of FR interface as DCE.	-
dte	Indicates the type of FR interface as DTE.	-

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FR networks allow devices to exchange data. Devices and interfaces on FR networks play the following roles:

- Data Terminal Equipment (DTE): a user-side device. The interface on the user-side device is a DTE interface.
- Data Circuit-terminating Equipment (DCE): a network device, providing an access for user devices, and it is generally known as data circuit termination equipment interfaces.

 Copyright © Huawei Technologies Co., Ltd.

In real world situations, an DTE interface can be connected to a DCE interface only. The type of the FR interface on the device that functions as an FR switch must be DCE.

Prerequisites

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Configuration Impact

If you run the **fr interface-type** command several times, the latest configuration overrides the previous one.

Precautions

The **fr interface-type** command configuration will change the FR interface type, and then affect the LMI negotiation.

Example

Set the type of the FR interface Serial 1/0/0:0 as DCE.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dce
```

Related Topics

7.6.51 link-protocol fr

7.6.31 fr ip dscp

Function

The **fr ip dscp** command maps a range of DSCP values of IP packets to a PVC.

The **undo fr ip dscp** command deletes the mapping between a range of DSCP values of IP packets and a PVC.

By default, no DSCP value is mapped to a PVC.

Format

fr ip dscp *dlci-number* { *min* [*max*] | **default** }

undo fr ip dscp [*dlci-number*]

Parameters

Parameter	Description	Value
dlci-number	Specifies the DLCI value of a PVC.	The value is an integer ranging from 16 to 1022.

Parameter	Description	Value
min	Specifies the minimum DSCP value of IP packets to be transmitted along the PVC.	The value is an integer ranging from 0 to 63.
max	Specifies the maximum DSCP value of IP packets to be transmitted along the PVC.	The value is an integer ranging from *min* to 63.
default	Configure the PVC to transmit IP packets, DSCP values in which are not mapped to any PVC.	-

Views

Serial FR PVC group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Services with different precedence values can be transmitted separately after a PVC group is configured. IP packets that are transmitted over FR links can be classified based on the Type of Service (ToS) field of packets.

Tos field in an IP header contains a DiffServ Code Point (DSCP) or Precedence value. Perform the following operations to map DSCP or Precedence values to PVCs:

- If the ToS field contains a DSCP value, run the **fr ip dscp** command to map a DSCP value to a PVC.

  A DSCP value uses 6 bits of the ToS field, ranging from 0 to 63. The greater the value, the higher the precedence. After precedence values are mapped to PVCs, IP packets with different precedence values are transmitted along specified PVCs. This allows services with different precedence values to be transmitted separately.

  The parameters of the **fr ip dscp** command can be selected as required.

  - The **fr ip dscp** *dlci-number min max* command can be used to allow IP packets with the DSCP value ranging from *min* to *max* to be transmitted along the PVC with the DLCI number of *dlci-number*.
  - The **fr ip dscp** *dlci-number* **default** command can be used to allow all IP packets with the DSCP values not mapped to a PVC to be transmitted along the PVC with the DLCI number of *dlci-number*.

    If a specific DSCP value is not mapped to any PVCs in a group, the entire group will become unavailable. Therefore, configuring a default PVC is recommended if there is a possibility that some DSCP values are not mapped to PVCs.
- If the ToS field contains a Precedence value, run the **fr ip precedence** command to map a Precedence value to a PVC.

Prerequisites

The PVC with the DLCI number specified in the **fr ip dscp** command must be configured.

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Precautions

DSCP values can be mapped only to PVCs in the PVC group. The *min* value must be smaller than or equal to the *max* value. If the PVC to which a specific DSCP value is mapped to goes Down, IP packets with this DSCP value will be transmitted along the default PVC. If the default PVC is also Down, the packets will be transmitted along a PVC to which a smaller DSCP value is mapped. The following PVC forwarding modes are recommended:

- Forward unicast packets along PVCs to which DSCP values of these packets are mapped.
- Forward IS-IS, multicast, and broadcast packets along the PVC to which the DSCP value of 63 is mapped.

Example

Configure the PVC with the DLCI value of 100 in the PVC group named **abc** to transmit IP packets with DSCP values of 0 to 20, and with the DLCI value of 101 to transmit other IP packets.

```
<Huawei> system-view
[Huawei] interface serial1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr pvc-group abc
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr dlci 100
[Huawei-Serial1/0/0-fr-pvc-group-dlci-abc-100] quit
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr dlci 101
[Huawei-Serial1/0/0-fr-pvc-group-dlci-abc-101] quit
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr ip dscp 100 0 20
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr ip dscp 101 default
```

Related Topics

7.6.43 fr pvc-group

7.6.32 fr ip precedence

Function

The **fr ip precedence** command maps IP Precedence values to PVCs.

The **undo fr ip precedence** command deletes mappings between IP Precedence values and PVCs.

By default, no IP precedence value is mapped to a PVC.

Format

fr ip precedence *dlci-number* { *min* [*max*] | **default** }

undo fr ip precedence [*dlci-number*]

Parameters

Parameter	Description	Value
dlci-number	Specifies the DLCI value of a PVC.	The value is an integer ranging from 16 to 1022.
min	Specifies the minimum IP Precedence value of IP packets to be transmitted along the PVC.	The value is an integer ranging from 0 to 7.
max	Specifies the maximum IP Precedence value of IP packets to be transmitted along the PVC.	The value is an integer ranging from *min* to 7.
default	Configures the PVC to transmit IP packets, IP Precedence values in which are not mapped to any PVC.	-

Views

Serial FR PVC group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Services with different precedence values can be transmitted separately after a PVC group is configured. IP packets that are transmitted over FR links can be classified based on the ToS field of packets.

The Type of Service (ToS) field in an IP header contains a DiffServ Code Point (DSCP) or Precedence value. Do as follows to map DSCP or Precedence values to PVCs:

- If the ToS field contains a Precedence value, run the **fr ip precedence** command to map a Precedence value to a PVC.

  An IP Precedence value uses 3 bits of the ToS field in an IP packet, ranging from 0 to 7. The greater the value, the higher the precedence. After precedence values are mapped to PVCs, IP packets with different precedence values are transmitted along specified PVCs. This allows services with different precedence values to be transmitted separately.

  The parameters of the **fr ip precedence** command can be selected as required.

  - The **fr ip precedence** *dlci-number min max* command can be used to allow IP packets with the Precedence value ranging from *min* to *max* to be transmitted along the PVC with the DLCI number of *dlci-number*.
  - The **fr ip precedence** *dlci-number* **default** command can be used to allow all IP packets with the Precedence values not mapped to a PVC to be transmitted along the PVC with the DLCI number of *dlci-number*.

 Copyright © Huawei Technologies Co., Ltd.

If a specific Precedence value is not mapped to any PVCs in a group, the entire group will become unavailable. Therefore, configuring a default PVC is recommended if there is a possibility that some Precedence values are not mapped to PVCs.

- If the ToS field contain a DSCP value, run the **fr ip dscp** command to map a DSCP value to a PVC.

Prerequisites

The PVC with the DLCI number specified in the **fr ip precedence** command must be configured.

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Precautions

Precedence values can be mapped only to PVCs in the PVC group. The *min* value must be smaller than or equal to the *max* value. If the PVC to which a specific Precedence value is mapped to goes Down, IP packets with this Precedence value will be transmitted along the default PVC. If the default PVC is also Down, the packets will be transmitted along a PVC to which a smaller Precedence value is mapped. The following PVC forwarding modes are recommended:

- Forward unicast packets along PVCs to which Precedence values of these packets are mapped.
- Forward IS-IS, multicast, and broadcast packets along the PVC to which the Precedence value of 7 is mapped.

Example

Configure the PVC with the DLCI value of 100 in the PVC group named **abc** to transmit IP packets with IP Precedence values of 0 to 2, and with the DLCI value of 101 to transmit other IP packets.

```
<Huawei> system-view
[Huawei] interface serial1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr pvc-group abc
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr dlci 100
[Huawei-Serial1/0/0-fr-pvc-group-dlci-abc-100] quit
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr dlci 101
[Huawei-Serial1/0/0-fr-pvc-group-dlci-abc-101] quit
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr ip precedence 100 0 2
[Huawei-Serial1/0/0-fr-pvc-group-abc] fr ip precedence 101 default
```

Related Topics

7.6.43 fr pvc-group

7.6.33 fr lmi n391dte

Function

The **fr lmi n391dte** command configures the parameter N391 at the DTE side.

The **undo fr lmi n391dte** command restores the default setting.

By default, the value of the parameter N391 at the DTE side is 6.

Format

fr lmi n391dte *n391-value*

undo fr lmi n391dte

Parameters

Parameter	Description	Value
n391-value	Specifies the counts of sending a status enquiry packet. N391 defines an interval (a week) at which the DTE sends a status enquiry packet.	The value is an integer ranging from 1 to 255. The default value is 6.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LMI protocol is used to exchange status information to maintain FR link and PVC status.

The DTE sends a Status enquiry packet at an interval to query the status of a VC. N391 defines the ratio of the integrity authentication packet number to the status enquiry packet number, (N391 - 1):1. The **fr lmi n391dte** command can be used to modify the interval at which status enquiry packets are sent.

Prerequisites

The type of the FR interface must be DTE. The **fr interface-type** command can be used to configure the type of an FR interface.

Configuration Impact

The **fr lmi n391dte** command can be used to modify the interval at which status enquiry packets are sent. The DTE sends a status enquiry packet to query the link status at an interval. After receiving the status enquiry packet, the DCE immediately replies with a status response packet. If the DTE does not receive the response within a specific period, a fault is counted. If the number of faults exceeds the upper limit, the DTE considers the physical link and all VCs on it unavailable. This will lead to an FR negotiation failure.

If you run the **fr lmi n391dte** command several times, the latest configuration overrides the previous one.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the FR interface Serial 1/0/0:0 to operate in the DTE mode. Set the counter value of the PVC status-enquiry to 10.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dte
[Huawei-Serial1/0/0:0] fr lmi n391dte 10
```

Related Topics

7.6.30 fr interface-type
7.6.65 timer hold (FR interface view)

7.6.34 fr lmi n392dce

Function

The **fr lmi n392dce** command configures the parameter N392 at the DCE side.

The **undo fr lmi n392dce** command restores the default configuration.

By default, the value of the parameter N392 at the DCE side is 3.

Format

fr lmi n392dce *n392-value*

undo fr lmi n392dce

Parameters

Parameter	Description	Value
n392-value	Specifies the upper limit of faults on the DCE.	The value is an integer ranging from 1 to 10. The default value is 3.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCE requires the DTE to send a status enquiry packet at an interval that is determined by T392. If the DCE does not receive any status enquiry packet within a specific period, a fault is counted and the number of faults increases by 1. If the number of faults exceeds the upper limit, the DCE considers the physical link and all VCs on it unavailable.

 Copyright © Huawei Technologies Co., Ltd.

The **fr lmi n392dce** command can be used to set the upper limit of faults.

Prerequisites

The type of the FR interface must be DTE. The **fr interface-type** command can be used to configure the type of an FR interface.

Configuration Impact

The upper limit will determine the FR link negotiation rate.

If you run the **fr lmi n392dce** command several times, the latest configuration overrides the previous one.

Precautions

N392 on the DCE must be smaller than N393 on the DCE.

Example

Configure the FR interface Serial 1/0/0:0 to operate in the DCE mode and configure N392 and N393 to 5 and 6 respectively.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dce
[Huawei-Serial1/0/0:0] fr lmi n392dce 5
[Huawei-Serial1/0/0:0] fr lmi n393dce 6
```

Related Topics

7.6.30 fr interface-type
7.6.36 fr lmi n393dce

7.6.35 fr lmi n392dte

Function

The **fr lmi n392dte** command configures N392 at the DTE side.

The **undo fr lmi n392dte** command restores the default configuration.

By default, the value value is 3.

Format

fr lmi n392dte *n392-value*

undo fr lmi n392dte

Parameters

Parameter	Description	Value
n392-value	Specifies the error threshold.	The value is an integer that ranges from 1 to 10. The default value is 3.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DTE sends a status enquiry packet to query the link status at an interval. After receiving the status enquiry packet, the DCE immediately replies with a status response packet. If the DTE does not receive the response within a specific period, a fault is counted and the number of faults increases by 1. If the number of faults exceeds the upper limit, the DTE considers the physical link and all VCs on it unavailable. The **fr lmi n392dte** command can be used to set the upper limit of faults.

Prerequisites

The type of the FR interface must be DTE. The **fr interface-type** command can be used to configure the type of an FR interface.

Configuration Impact

The upper limit will determine the FR link negotiation rate.

If you run the **fr lmi n392dte** command several times, the latest configuration overrides the previous one.

Precautions

N392 on the DTE must be smaller than N393 on the DTE.

Example

Set the FR interface Serial 1/0/0:0 to operate in the DTE mode. Set N392 and N393 to 5 and 6 respectively.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dte
[Huawei-Serial1/0/0:0] fr lmi n392dte 5
[Huawei-Serial1/0/0:0] fr lmi n393dte 6
```

Related Topics

7.6.30 fr interface-type

7.6.37 fr lmi n393dte

7.6.36 fr lmi n393dce

Function

The **fr lmi n393dce** command sets the N393 at the DCE side.

 Copyright © Huawei Technologies Co., Ltd.

The **undo fr lmi n393dce** command restores the default configuration.

By default, the default value is 4.

Format

fr lmi n393dce *n393-value*

undo fr lmi n393dce

Parameters

Parameter	Description	Value
n393-value	Specifies the event counter.	The value is an integer that ranges from 1 to 10. The default value is 4.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DCE requires the DTE to send a status enquiry packet at an interval that is determined by T392. If the DCE does not receive any status enquiry packet within a specific period, a fault is counted and the number of faults increases by 1. If the number of faults exceeds the upper limit, the DCE considers the physical link and all VCs on it unavailable.

N392 and N393 together define the upper limit of faults. N393 indicates the number of observed events; N392 indicates the upper limit of faults in the observed events. If the number of faults reaches N392 in N393 events on the DCE, the DCE determines that the upper limit is reached and considers the physical link and all VCs on it unavailable.

The **fr lmi n393dce** command can be used to modify N393.

Prerequisites

The type of the FR interface must be DCE. The **fr interface-type** command can be used to configure the type of an FR interface.

Configuration Impact

The upper limit will determine the FR link negotiation rate.

If you run the **fr lmi n393dce** command several times, the latest configuration overrides the previous one.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

N392 on the DCE must be smaller than N393 on the DCE.

Example

Configure the FR interface Serial 1/0/0:0 to operate in the DCE mode. Set N392 to 5 and N393 to 6.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dce
[Huawei-Serial1/0/0:0] fr lmi n392dce 5
[Huawei-Serial1/0/0:0] fr lmi n393dce 6
```

Related Topics

7.6.30 fr interface-type
7.6.34 fr lmi n392dce

7.6.37 fr lmi n393dte

Function

The **fr lmi n393dte** command configures the N393 at the DTE side.

The **undo fr lmi n393dte** command restores the default configuration.

By default, the default value is 4.

Format

fr lmi n393dte *n393-value*

undo fr lmi n393dte

Parameters

Parameter	Description	Value
n393-value	Specifies the event counter.	The value is an integer that ranges from 1 to 10. The default value is 4.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DTE sends a status enquiry packet to query the link status at an interval. After receiving the status enquiry packet, the DCE immediately replies with a status

response packet. If the DTE does not receive the response within a specific period, a fault is counted and the number of faults increases by 1. If the number of faults exceeds the upper limit, the DTE considers the physical link and all VCs on it unavailable. The **fr lmi n393dte** command can be used to set the upper limit of faults.

N392 and N393 together define the upper limit of faults. N393 indicates the number of observed events; N392 indicates the upper limit of faults in the observed events. If the number of faults reaches N392 in N393 events on the DTE, the DTE determines that the upper limit is reached and considers the physical link and all VCs on it unavailable.

The **fr lmi n393dte** command can be used to modify N393.

Prerequisites

The type of the FR interface must be DTE. The **fr interface-type** command can be used to configure the type of an FR interface.

Configuration Impact

The upper limit will determine the FR link negotiation rate.

If you run the **fr lmi n393dte** command several times, the latest configuration overrides the previous one.

Precautions

The DCE requires the DTE to send a status enquiry packet at an interval that is determined by T392. If the DCE does not receive any status enquiry packet within a specific period, a fault is counted and the number of faults increases by 1. If the number of faults exceeds the upper limit, the DCE considers the physical link and all VCs on it unavailable.

Example

Configure the FR interface Serial 1/0/0:0 to operate in the DTE mode. Set N392 and N393 to 5 and 6 respectively.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dte
[Huawei-Serial1/0/0:0] fr lmi n392dte 5
[Huawei-Serial1/0/0:0] fr lmi n393dte 6
```

Related Topics

7.6.30 fr interface-type
7.6.35 fr lmi n392dte

7.6.38 fr lmi t392dce

Function

The **fr lmi t392dce** command sets T392 on the DCE.

The **undo fr lmi t392dce** command restores the default setting.

The default T392 value is 15s on the DCE.

Format

fr lmi t392dce *t392-value*

undo fr lmi t392dce

Parameters

Parameter	Description	Value
t392-value	Specifies the value of the polling timer.	The value is an integer that ranges from 5 to 32 in seconds.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

T392 defines the maximum time during which the DCE waits for a status response packet. T392 must be larger than T391.

After receiving a status enquiry packet, the DCE replies with a status packet, and the polling timer starts on the DCE for another status enquiry packet. If the DCE does not receive another status enquiry packet within the period determined by T392, a fault is counted and the number of faults increases by 1.

Prerequisites

The type of the FR interface must be DCE. The **fr interface-type** command can be used to configure the type of an FR interface.

Configuration Impact

The upper limit of faults will determine the FR link negotiation rate.

If you run the **fr lmi t392dce** command several times, the latest configuration overrides the previous one.

Example

Configure the FR interface Serial 1/0/0:0 to operate in the DCE mode. Set T392 to 10.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dce
[Huawei-Serial1/0/0:0] fr lmi t392dce 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.6.30 fr interface-type

7.6.65 timer hold (FR interface view)

7.6.39 fr lmi type

Function

The **fr lmi type** command configures the Local Management Interface (LMI) protocol type of FR.

The **undo fr lmi type** command restores the default type.

By default, the LMI protocol type of FR is **q933a**.

Format

fr lmi type { **ansi** | **nonstandard** | **q933a** }

undo fr lmi type

Parameters

Parameter	Description	Value
ansi	Specifies the standard LMI protocol type defined in ANSI T1.617 Appendix D.	-
nonstandard	Specifies the nonstandard compatible LMI protocol.	-
q933a	Specifies the LMI protocol of Q.933 Appendix A.	-

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PVC is used, both the DCE and DTE need to be aware of the PVC status. The LMI protocol is used to monitor the PVC status.

The LMI protocol is used to exchange status information to maintain FR link and PVC status. The LMI module manages PVCs by adding PVCs, deleting PVCs, and detecting PVC status and integrity of PVC links.

Currently, three standard LMI protocol types are supported:

- **fr lmi type ansi**: configures the LMI protocol type as ANSI T1.617.

 Copyright © Huawei Technologies Co., Ltd.

- **fr lmi type nonstandard**: configures the LMI protocol type as nonstandard.

  NOTE

  Only Huawei devices support **nonstandard**, and thus this parameter cannot be used when Huawei and non-Huawei devices communicate with each other.

- **fr lmi type q933a**: configures the LMI protocol type as ITU-T Q.933.

Prerequisites

The **link-protocol fr** command can be used to configure the link layer protocol as FR, and the LMI protocol types of both ends must be the same.

Configuration Impact

If you run the **fr lmi type** command several times, the latest configuration overrides the previous one. After the configuration is complete, the FR negotiation will be performed based on the new LMI protocol type.

Precautions

The **fr lmi type** command configuration will affect the FR negotiation. Confirm whether to modify the LMI protocol type before running the **fr lmi type** command.

Example

Configure the FR LMI protocol of Serial 1/0/0:0 as the nonstandard compatible protocol.

```
<Huawei> system-view
[Huawei] interface Serial1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr lmi type nonstandard
```

Related Topics

7.6.13 display fr lmi-info

7.6.40 fr map bridge

Function

The **fr map bridge** command adds a bridge mapping entry on a frame relay (FR) interface.

The **undo fr map bridge** command deletes a bridge mapping entry from an FR interface.

By default, no bridge mapping entry is configured.

Format

fr map bridge *dlci-number* **broadcast**

undo fr map bridge *dlci-number* **broadcast**

Parameters

Parameter	Description	Value
dlci-number	Specifies the Data Link Connection Identifier (DCLI) of a local virtual circuit.	The value is an integer ranging from 16 to 1022.
broadcast	Indicates whether the bridge mapping entry can be used to send broadcast packets.	-

Views

Frame relay serial interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **fr map bridge** *dlci-number* **broadcast** command can be used to enable an interface added to a bridge group to send broadcast packets based on the bridge mapping entry.

Prerequisites

Run the **bridge** *bridge-id* command in the interface view to add the interface to a bridge group.

Precautions

If the DLCI specified in the **fr map bridge** *dlci-number* **broadcast** command does not exist, the system will create a DLCI as specified. The created DLCI will be deleted when the **undo fr map bridge** *dlci-number* **broadcast** command is run.

Each FR interface can be configured with only one bridge mapping entry.

If a bridge is deleted or the FR interface quits the bridge group, the corresponding bridge mapping entry will be deleted from the FR interface.

Example

Configure a bridge mapping entry with the DLCI being 50 on MFR0/0/0.

```
<Huawei> system-view
[Huawei] interface mfr 0/0/0
[Huawei-MFR0/0/0] bridge 5
[Huawei-MFR0/0/0] fr map bridge 50 broadcast
```

 Copyright © Huawei Technologies Co., Ltd.

7.6.41 fr map ip

Function

The **fr map ip** command configures a static mapping between destination IP address and a specified DLCI value.

The **undo fr map ip** command deletes a static mapping between an IP address and a specified DLCI value.

By default, no IP address is mapped to any DLCI value.

Format

fr map ip { *destination-address* [*mask*] | **default** } *dlci-number* [[**ietf** | **nonstandard**] [**broadcast**]] [**compression** { **frf9** | **iphc rtp-connections** *rtp-connections-number* [**tcp-connections** *tcp-connections-number*] }]

fr map ip { *destination-address* [*mask*] | **default** } **pvc-group** *pvc-group-name* [[**ietf** | **nonstandard**] [**broadcast**]]

undo fr map ip { *destination-address* [*mask*] | **default** } { *dlci-number* | **pvc-group** *pvc-group-name* }

Parameters

Parameter	Description	Value
destination-address mask	Specifies the destination address and subnet mask.	The subnet mask format must be X.X.X.X. Each X is an integer ranging from 0 to 255.
default	Specifies a default mapping, all IP addresses will be mapped to the specified DLCI.	-
dlci-number	Specifies the local DLCI.	The value is an integer ranging from 16 to 1022.
pvc-group *pvc-group-name*	Specifies the PVC group name. The PVC group name must be unique on the ATM interface and cannot be a pair of valid VPI/VCI values. For example, 1/20 cannot be used as a PVC group name. The MFR interface does not support this parameter.	The value is a string of 1 to 16 case-insensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ietf	Sets the packet format of the FR interface to IETF. If the remote devices are non-Huawei devices, configure the encapsulation format to **ietf**.	-
nonstandard	Sets the packet format supported by the FR interface to nonstandard. If the remote devices are Huawei devices, configure the encapsulation format to **nonstandard**.	-
broadcast	Allows the PVC indicated by the DLCI to send broadcast packets.	-
compression	Specifies FR compression. **NOTE** The POS interface does not support FR compression. FR compression takes effect after the **shutdown** and **undo shutdown** commands are executed in sequence to restart the FR interface.	-
frf9	Enables FRF.9 compression to compress packets by using FRF.9 standard and Lempel-Ziv-Stac (LZS) algorithms. This parameter is unavailable for P2P interfaces.	-
iphc	Sets the maximum number of RTP headers that can be compressed. • **iphc** in the **fr map ip** command specifies the maximum number of RTP headers that can be compressed over the PVC indicated by the DLCI. • If the maximum number of RTP headers that can be compressed is not configured on the FR interface, a maximum of 256 RTP headers can be compressed over the PVC indicated by the DLCI.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rtp-connections *rtp-connections-number*	Sets the maximum number of RTP headers that can be compressed.	The value is an integer and the default value is 256. For the AR2240 and AR3260, the number of RTP connections varies depending on different SRUs. ● SRU40, SRU80, SRU100E, SRU200, SRU200E, and SRU60: 3-256 ● SRU400: 3-1000 For the AR3670 (SRUX5), the value ranges from 3 to 1000. For other models, the value ranges from 3 to 256.
tcp-connections *tcp-connections-number*	Sets the maximum number of TCP headers that can be compressed.	The value is an integer ranging from 3 to 256. The default value is 256.

Views

FR interface view, FR sub-interface view, MFR interface view, or POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FR, as a statistics multiplexing protocol, can provide multiple VCs over a single physical transmission line.

A VC is identified by a DLCI. The DLCI is local to the interface and its directly connected interface. Therefore, the same DLCI on different physical interfaces of an FR network do not indicate the same PVC.

The **fr map ip** command associates the protocol address of a peer device with the FR address (DLCI value) of the local device. This configuration helps upper-layer protocols locate a peer device based on the protocol address of the peer device.

Prerequisites

The link layer protocol of interfaces must be FR. The **link-protocol fr** command can be used to configure the link layer protocol as FR.

The **fr compression frf9** command is run to enable FRF.9 compression before configuring FRF.9 compression on a P2P FR interface.

The **fr compression iphc** command is run to enable IPHC compression before configuring RTP compression on a P2P FR interface.

Configuration Impact

If the DCE is configured with static address mapping and the DTE is enabled with the dynamic address mapping function, the DTE can communicate with the DCE without being configured with static address mapping. If the DTE is configured with a static address mapping and the DCE is enabled with the dynamic address mapping function, the DTE and DCE cannot communicate with each other.

Precautions

If interconnected DTE and DCE interfaces meet the following conditions:

- The interfaces are configured with FRF.9 compression.

  NOTE

  - FRF.9 compression applies to only low-speed links.
  - FRF.9 compression includes a synchronization process. If packet mis-sequence occurs during synchronization, compression may fail.
- The DTE interface learns the DLCI value using the dynamic address mapping function.

Restart these two interfaces after running the **undo fr map ip** { *ip-address* | **default** } *dlci-number* command on the DTE interface. After that, the DTE and DCE can communicate with each other.

When configuring **broadcast**, pay attention to the following points:

- The **fr map ip default** *dlci-number* **broadcast** and **fr map ip** *destination-address dlci-number* **broadcast** commands cannot be configured on the same interface.
- On an interface, you cannot specify the same DLCI but different destination addresses in the **fr map ip** *destination-address dlci-number* **broadcast** command.

When configuring *mask*, pay attention to the following points:

- The **fr map ip** *destination-address mask dlci-number* and **fr map ip default** *dlci-number* commands cannot be configured on the same interface for the same DLCI.
- The **fr map ip** *destination-address mask dlci-number* and **fr map ip** *destination-address dlci-number* commands cannot be configured on the same interface for the same DLCI with the same *destination-address* value.

Example

Configure a static mapping between the IP address of the peer router (10.1.2.1) and the DLCI value (50) of a PVC that connects the router on serial 1/0/0:0.

```
<Huawei> system-view
```

```
[Huawei] interface Serial1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr map ip 10.1.2.1 50
```

Related Topics

7.6.14 display fr map-info

7.6.29 fr inarp

7.6.42 fr map ppp

Function

The **fr map ppp** command maps an FR PVC to a PPP link.

The **undo fr map ppp** command deletes the mapping between FR PVC and PPP link.

By default, no FR PVC is mapped to any PPP link.

Format

fr map ppp interface *interface-type interface-number dlci-number*

undo fr map ppp [**interface** *interface-type interface-number dlci-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of a VT interface.	-
dlci-number	Specifies the DLCI value of a local PVC.	The value is an integer ranging from 16 to 1022.

Views

FR interface view, FR sub-interface view, MFR interface view, or POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FR simplifies frame encapsulation. It features lower communication delays and higher network throughput, compared with other data link layer protocols. FR, however, does not provide authentication functions, and thus cannot guarantee that only valid users accessing enterprise networks. PPP is a data link layer protocol used to transmit network layer packets on P2P links. It provides effective

authentication functions and is extensible. Configuring PPPoFR allows devices to check validity of login users, ensuring FR network security.

After the **fr map ppp** command is used, the DTE device maps a PVC to a PPP link to establish a PPPoFR link. This allows PPP packets to be transmitted along the FR PVC.

Prerequisites

The link layer protocol of interfaces must be FR. The **link-protocol fr** command can be used to configure the link layer protocol as FR.

Example

Map the PVC with the DLCI value of 100 on Serial 1/0/0 to a PPP link to establish a PPPoFR link.

```
<Huawei> system-view
[Huawei] interface Serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr map ppp interface virtual-template 1 100
```

Related Topics

7.6.14 display fr map-info

7.6.29 fr inarp

7.6.43 fr pvc-group

Function

The **fr pvc-group** command creates a PVC group and displays the PVC group view.

The **undo fr pvc-group** command deletes a specified PVC group.

By default, no PVC group is created.

Format

fr pvc-group *pvc-group-name*

undo fr pvc-group [*pvc-group-name*]

Parameters

Parameter	Description	Value
pvc-group-name	Specifies the PVC group name. The PVC group name must be unique on the FR interface and cannot be a pair of valid VPI/VCI values. For example, 1/20 cannot be used as a PVC group name.	The name is a string of 1 to 16 case-insensitive characters.

Views

FR serial interface view, FR serial sub-interface view, POS interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a conventional FR network, only one PVC forwards packets even though multiple PVCs have been configured with the same destination address. If this PVC becomes unavailable, another PVC will be used to forward packets. This results in low bandwidth usage and a failure in providing sufficient bandwidth for packets with high priorities.

Configuring a PVC group allows PVCs with the same destination address to forward packets at the same time and packets with different priorities to be transmitted along separate PVCs. If IP packets need to be transmitted along FR PVCs in a PVC group, map the ToS fields of IP packets to FR PVCs so that IP packets with different priorities are transmitted along separate PVCs. In addition, each PVC in the group can be configured with a different QoS policy for transmitting a specific type of services.

Prerequisites

The link layer protocol of the interface must be FR. The **link-protocol fr** command can be used to configure FR.

Precautions

A maximum of eight PVCs can be added to one PVC group.

Example

Create a PVC group named **abc**.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr pvc-group abc
```

Related Topics

7.6.14 display fr map-info

7.6.44 fr pvc-pq

Function

Using the **fr pvc-pq** command, you can set the queue type to PVC priority queuing (PVC PQ) for an FR interface and set the queue length, namely, the maximum number of packets in a queue.

Using the **undo fr pvc-pq** command, you can restore the queue type of an FR interface to First In First Out (FIFO).

By default, the queue type of an FR interface is FIFO.

Format

fr pvc-pq [*top-limit middle-limit normal-limit bottom-limit*]

undo fr pvc-pq

Parameters

Parameter	Description	Value
top-limit	Specifies the length of a top-priority queue.	The value is an integer that ranges from 1 to 1024, in packets. The default value is 20.
middle-limit	Specifies the length of a middle-priority queue.	The value is an integer that ranges from 1 to 1024, in packets. The default value is 40.
normal-limit	Specifies the length of a normal-priority queue.	The value is an integer that ranges from 1 to 1024, in packets. The default value is 60.
bottom-limit	Specifies the length of a bottom-priority queue.	The value is an integer that ranges from 1 to 1024, in packets. The default value is 80.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PVC PQ is an FR queue mechanism. Similar to PQ, PVC PQ has four queue types: top, middle, normal, and bottom, which are listed in descending order of priority. In an FR class, PVC PQ queues are specified for packets transmitted over VCs. When congestion occurs on the interface, packets transmitted over different VCs are placed into different PVC PQ queues. Packets are sent based on their queue priorities. For example, packets in the highest priority queue are sent first, and packets in lower priority queues are sent only when the queues with higher priorities are emptied.

Prerequisites

FR traffic shaping has been enabled by using the **fr traffic-shaping** command.

Example

Set the queue type of Serial 1/0/0 to PVC PQ.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr traffic-shaping
[Huawei-Serial1/0/0] fr pvc-pq
```

7.6.45 fr switch

Function

The **fr switch** command configures an FR switching PVC.

The **undo fr switch** command deletes an FR switching PVC.

By default, no FR switching PVC is configured.

Format

fr switch *name* [**interface** *interface-type in-interface-number* **dlci** *in-dlci* **interface** *interface-type out-interface-number* **dlci** *out-dlci*]

undo fr switch *name*

Parameters

Parameter	Description	Value
name	Specifies the name of an FR switching PVC.	The value is a string of 1 to 16 case-sensitive characters.
interface *interface-type in-interface-number*	Specifies the inbound interface for a PVC. An FR interface or an MFR interface can be specified as the inbound interface of a PVC.	-
dlci *in-dlci*	Specifies the inbound DLCI value.	The value is an integer ranging from 16 to 1022.
interface *interface-type out-interface-number*	Specifies the outbound interface for a PVC. Only a tunnel interface can be specified as the outbound interface of a PVC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dlci *out-dlci*	Specifies the outbound DLCI value.	The value is an integer ranging from 16 to 1022.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The FR protocol, as a statistics multiplexing protocol, can provide multiple VCs over a single physical link. FR switching is a typical FR application. In an FR switching scenario, DCE devices exchange and forward IP packets at the data link layer through PVCs. FR switching can be implemented in the following modes:

- FR switching routes: A forwarding route is configured by specifying the outbound interface and the DLCI value of forwarded packets. For details, see description of the **fr dlci-switch** command.
- FR switching PVCs: A switching route is created on two interfaces of a device to forward packets. The interface on which the packet is forwarded can be an FR interface or an MFR interface. If a tunnel interface is specified as the outbound interface, FR packets can be transmitted over an IP network.

If you run the **fr switch** *name* command without specifying any parameters, the FR switching PVC view is displayed.

Prerequisites

The link layer protocol of interfaces must be FR. The **link-protocol fr** command can be used to configure the link layer protocol as FR.

Before configuring an FR switching PVC, run the **fr switching** command to enable the FR switching function.

Configuration Impact

After the **fr switch** is run, Inverse ARP packets cannot be sent on the PVC enabled with FR switching and dynamic MAP entries cannot be created. The dynamic MAP entries on the DLCI will be automatically deleted.

Precautions

A PVC configured with the static mapping between the DLCI and FR address cannot be configured with FR switching.

The type of the interface enabled with FR switching must be DCE. The FR switching function takes effect only after the **fr interface-type** command is used to set the FR interface type.

 Copyright © Huawei Technologies Co., Ltd.

The specified inbound and outbound interfaces for a PVC must have been created.

Example

Create a switching PVC named pvc2.

```
<Huawei> system-view
[Huawei] fr switch pvc2 interface serial 1/0/0 dlci 100 interface tunnel 0/0/1 dlci 200
```

Related Topics

7.6.46 fr switching

7.6.46 fr switching

Function

The **fr switching** command enables the FR switching function.

The **undo fr switching** command disables the FR switching function.

By default, the FR switching function is disabled.

Format

fr switching

undo fr switching

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The FR protocol, as a statistics multiplexing protocol, can provide multiple VCs over a single physical line. FR switching is a typical FR application. FR switching entries can be generated by creating an FR switching route or an FR switching PVC after the **fr switching** command is run to activate entries first.

Prerequisites

The type of the interface enabled with FR switching must be DCE. The FR switching function takes effect only after the **fr interface-type** command is used to set the FR interface type.

Configuration Impact

After the **undo fr switching** command is run, the PVC switching function will be disabled and all FR switching entries will be deleted.

Example

Enable the FR switching function.

```
<Huawei> system-view
[Huawei] fr switching
```

Related Topics

7.6.28 fr dlci-switch

7.6.45 fr switch

7.6.47 fr traffic-shaping

Function

Using the **fr traffic-shaping** command, you can enable FR traffic shaping.

Using the **undo fr traffic-shaping** command, you can disable FR traffic shaping.

By default, FR traffic shaping is disabled.

Format

fr traffic-shaping

undo fr traffic-shaping

Parameters

None

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

FR traffic shaping is applied to an outbound interface of a router on an FR network to control outgoing traffic. Each permanent virtual circuit (PVC) of the outbound interface can transmit traffic based on parameters in the FR class applied to the interface.

When network congestion occurs, the transmission rate reduces from the current rate by a specified percentage. If the new transmission rate is smaller than the CIR, the CIR is used as the actual transmission rate. When network congestion is relieved, the transmission rate increases from the current rate by a specified

 Copyright © Huawei Technologies Co., Ltd.

percentage. If the new transmission rate is greater than the allowed CIR, the allowed CIR is used as the actual transmission rate.

Example

Enable FR traffic shaping on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr traffic-shaping
```

7.6.48 fragment

Function

Using the **fragment** command, you can enable packet fragmentation on FR VCs.

Using the **undo fragment** command, you can disable packet fragmentation on FR VCs.

By default, packet fragmentation is disabled on FR VCs.

Format

fragment [*fragment-size*]

undo fragment

Parameters

Parameter	Description	Value
fragment-size	Specifies the fragment size for FR VCs.	The value is an integer that ranges from 64 to 1600, in bytes. The default value is 64 bytes.

Views

FR class view

Default Level

2: Configuration level

Usage Guidelines

On a low-speed FR link, large data packets increase the transmission delay. The FR fragmentation mechanism fragments a large data packet into several smaller packets, enabling low-speed FR links to transmit packets with low delay.

When voice and data packets are sent simultaneously, sending large data packets occupies bandwidth for a long period of time. This causes the delay in voice

packet transmission or even packet loss. As a result, the voice quality deteriorates. FR fragmentation aims to minimize the voice delay and ensure real-time voice transmission. After FR fragmentation is configured, a large data packet is fragmented into smaller data packets. Subsequently, voice packets and the smaller data packets are sent alternately to ensure that voice packets are processed in a timely manner. This shortens the voice delay.

The fragment function on the FR VC takes effect when the following conditions are met:

- The **mfr fragment** command is used on the MFR interface.
- The **fragment** command is used in the FR class view and the FR class is associated with the MFR interface.

Example

Set the fragment size to 128 bytes in an FR class named **huawei**.

```
<Huawei> system-view
[Huawei] fr class huawei
[Huawei-fr-class-huawei] fragment 128
```

7.6.49 fr-class

Function

Using the **fr-class** command, you can associate an FR class with an FR VC or FR interface.

Using the **undo fr-class** command, you disassociate an FR class from an FR VC or FR interface.

By default, no FR class is associated with any FR VC or FR interface.

Format

fr-class *class-name*

undo fr-class *class-name*

Parameters

Parameter	Description	Value
class-name	Specifies the name of an FR class to be associated with an FR VC or FR interface.	The value is a string of 1 to 31 case-insensitive characters.

Views

FR DLCI view, FR interface view, FR sub-interface view, MFR interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

To apply QoS parameters in an FR class to an FR VC, run the **fr-class** command to associate the FR class with the FR VC or FR interface.

If the specified FR class does not exist, the **fr-class** command creates an FR class and associates the FR class with an FR VC or FR interface. If the specified FR class already exists, the **fr-class** command associates the existing FR class with an FR VC or FR interface.

After an FR class is associated with an FR interface, QoS parameters in the FR class are applied to all VCs on the interface.

Example

Associate FR class **huawei** with an FR VC with the DLCI 200.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr
[Huawei-Serial1/0/0] fr dlci 200
[Huawei-fr-dlci-Serial1/0/0-200] fr-class huawei
```

Related Topics

7.6.21 fr class

7.6.27 fr dlci

7.6.50 interface mfr

Function

The **interface mfr** command creates a MFR bundle interface or sub-interface and displays the corresponding interface view.

The **undo interface mfr** command deletes a specified MFR bundle interface or sub-interface.

By default, there is no MFR interface or sub-interface.

Format

interface mfr *interface-number* [.*subnumber* [**p2mp** | **p2p**]]

undo interface mfr *interface-number* [.*subnumber*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the interface number of a MFR bundle. The format is slot number/card number/port number.	The slot number and card number are fixed at 0. The port number ranges from 0 to 15.
subnumber	Specifies the sub-interface number of a MFR bundle.	The value ranges from 1 to 1024.
p2mp	Indicates the type of a sub-interface is P2MP.	It is the default FR sub-interface type.
p2p	Indicates the type of a sub-interface is P2P.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a cost-effective solution, MFR bundles multiple physical links to increase bandwidth on FR networks.

NOTE

The status of every physical interface added to an MFR interface determines the status of the MFR interface. As long as one physical interface of the MFR interface is available, the MFR interface is available for upper-layer FR applications. If all physical interfaces of the MFR interface are unavailable, the MFR interface is unavailable for upper-layer FR applications.

Run either of the following commands on an MFR sub-interface:

- To create an MFR sub-interface on a P2P link on which IP addresses of the local and remote interfaces belong to the same network segment, run the **interface mfr** *interface-number.subnumber* **p2p** command.
- To create an MFR sub-interface on a P2MP link on which IP addresses of the local and remote interfaces belong to different network segments, run the **interface mfr** *interface-number.subnumber* **p2mp** command.

Follow-up Procedure

The MFR interface that is created using the **interface mfr** command is a logical interface. You can run the **link-protocol fr mfr** command to add physical interfaces to a created MFR interface.

Precautions

- An MFR interface must be created before its sub-interfaces are configured.
- All physical interfaces must be deleted from an MFR interface before the **undo interface mfr** command is used to delete the MFR interface.

Example

Create a MFR bundle interface with a P2MP sub-interface.

```
<Huawei> system-view
[Huawei] interface mfr 0/0/3
[Huawei-MFR0/0/3] quit
[Huawei] interface mfr 0/0/3.1 p2mp
```

Related Topics

7.6.52 link-protocol fr mfr

7.6.53 mfr bundle-name

7.6.51 link-protocol fr

Function

The **link-protocol fr** command indicates the FR encapsulation format.

The **undo link-protocol fr** command restores the default setting.

By default, the data link layer protocol of an interface is PPP. When the data link layer protocol of an interface is FR, the FR encapsulation format is IETF by default.

Format

link-protocol fr [**ietf** | **nonstandard**]

undo link-protocol fr

Parameters

Parameter	Description	Value
ietf	Indicates that the FR encapsulation format is IETF.	-
nonstandard	Indicates that the FR encapsulation format is nonstandard.	-

Views

Serial interface view, POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

FR provides transmission at a fixed rate and packet switching, facilitating accounting. To configure FR networks, configure FR as the link layer protocol on interfaces.

The **link-protocol fr** command can be used to configure FR as the link layer protocol for an interface. There are two FR encapsulation formats:

- IETF: encapsulates frames complying with RFC 1490.
- nonstandard: used for communication between Huawei and non-Huawei devices.

Precautions

- Two connected interfaces send packets only in locally set formats. If they can recognize both formats, they can receive packets in both formats even though they are configured with different FR encapsulation formats. If one device cannot automatically recognize both formats, configure both devices with the same FR encapsulation format.
- To modify the FR encapsulation format on an interface, delete its sub-interfaces if there are any.
- If the FR encapsulation format configured for an interface is changed, the system will automatically delete all FR configurations on this interface. FR must be reconfigured for this interface.
- After changing the link layer configuration of an FR interface, run the **shutdown** command and then the **undo shutdown** command to restart the interface and make the configuration take effect.
- If you run the **link-protocol fr** command several times, the latest configuration overrides the previous one.

Example

Configure the FR encapsulation on Serial 1/0/0:0 and select the nonstandard encapsulation.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr nonstandard
```

Related Topics

7.6.52 link-protocol fr mfr

7.6.52 link-protocol fr mfr

Function

The **link-protocol fr mfr** command configures an MFR bundle link on a physical interface and adds it to a specified MFR link.

By default, there is no MFR bundle link.

Format

link-protocol fr mfr *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the interface number. The value is specified by the **interface mfr** command.	-

Views

FR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a cost-effective solution, MFR bundles multiple physical links to increase bandwidth on FR networks.

An MFR link is called a bundle, and physical member links are called bundle links. The **link-protocol fr mfr** command configures an MFR bundle link on a physical interface and adds it to a specified MFR link. The bandwidth of an MFR link equals the sum bandwidth of its member links.

NOTE

One MFR interface corresponds to one bundle. One bundle may contain multiple bundle links, each of which corresponds to one physical interface. Bundle links are visible at the physical layer, and bundles are visible at the data link layer.

To delete a physical interface from an MFR interface, run the **link-protocol** command to configure a non-FR protocol as the link layer protocol.

Prerequisites

The specified MFR interface must have been created.

- Before adding a physical interface to an MFR interface, create the MFR interface and run the **shutdown** command to shut down the MFR interface.
- After adding a physical interface to an MFR interface, run the **undo shutdown** command to start the MFR interface.

Configuration Impact

The function and configuration of an MFR interface are the same as those of an ordinary FR interface. After a physical interface is bundled into an MFR interface, the originally configured parameters for the physical interface at the physical layer and the FR link layer no longer take effect. Instead, the parameters of this MFR interface are used for the physical interface.

Precautions

A maximum of 16 physical interfaces can be added to an MFR interface on the device.

 Copyright © Huawei Technologies Co., Ltd.

The status of every physical interface added to an MFR interface determines the status of the MFR interface. As long as one physical interface of the MFR interface is available, the MFR interface is available for upper-layer FR applications. If all physical interfaces of the MFR interface are unavailable, the MFR interface is unavailable for upper-layer FR applications.

Example

Configure Serial 1/0/0:0 as a bundle link and add it to the FR bundle interface MFR 0/0/3.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr mfr 0/0/3
```

Related Topics

7.6.50 interface mfr

7.6.56 mfr link-name

7.6.53 mfr bundle-name

Function

The **mfr bundle-name** command sets the BID for an MFR interface.

The **undo mfr bundle-name** command restores the default setting.

By default, the BID is in the form of "MFR + FR bundle number" such as MFR 0/0/3.

Format

mfr bundle-name [*name*]

undo mfr bundle-name

Parameters

Parameter	Description	Value
name	Specifies the name of a BID.	It is a string of 1 to 49 case-sensitive characters without blank spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To simplify interface management, you can run the **mfr bundle-name** command on an MFR interface to identify the interface and describe the function of the interface.

Follow-up Procedure

After running the **mfr bundle-name** command to configure the description of an interface, you can run the **display interface mfr** command to view the description.

Precautions

After the BID of an interface is modified, the new BID takes effect only after the **shutdown** and **undo shutdown** commands are used to restart the interface.

Example

Set the BID of the FR link as bundle1.

```
<Huawei> system-view
[Huawei] interface MFR 0/0/3
[Huawei-MFR0/0/3] mfr bundle-name bundle1
```

Related Topics

7.6.56 mfr link-name

7.6.54 mfr fragment

Function

The **mfr fragment** command enables fragmentation for an MFR bundle.

The **undo mfr fragment** command disables fragmentation for an MFR bundle.

By default, the function is disabled.

Format

mfr fragment

undo mfr fragment

Parameters

None

Views

MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If low-speed links transmit a large volume of network traffic, set the maximum MFR fragment size to reduce transmission delays.

NOTE

Generally, links whose bandwidth is lower than 768 kbit/s are considered low-speed links.

Follow-up Procedure

After fragmentation is enabled for an MFR bundle, run the **mfr fragment-size** command to set the maximum MFR fragment size.

Example

Enable the fragmentation on MFR 0/0/3.

```
<Huawei> system-view
[Huawei] interface mfr 0/0/3
[Huawei-MFR0/0/3] mfr fragment
```

Related Topics

7.6.55 mfr fragment-size

7.6.60 mfr window-size

7.6.55 mfr fragment-size

Function

The **mfr fragment-size** command configures the maximum fragment size allowed on an FR bundle link.

The **undo mfr fragment-size** command restores the default setting.

By default, the maximum fragment size allowed on an FR bundle link is 300 bytes.

Format

mfr fragment-size *size*

undo mfr fragment-size

Parameters

Parameter	Description	Value
size	Specifies the fragment size, including the FR header.	The value is an integer ranging from 60 to 1500, in bytes.

 Copyright © Huawei Technologies Co., Ltd.

Views

MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If low-speed links transmit a large volume of network traffic, set the maximum MFR fragment size to reduce transmission delays.

NOTE

Generally, links whose bandwidth is lower than 768 kbit/s are considered low-speed links.

The maximum MFR fragment size is determined by the member interface working at the lowest speed. For example, if T1 interfaces are bundled on one end and 64 kbit/s interfaces are bundled on the other end, both devices are configured with the maximum MFR fragment size based on the remote interfaces.

Table 7-38 Recommended fragmentation for less than 10 ms link transmission delays

Lowest Link Rate (in kbps)	Recommended Maximum Fragment Size (in bytes)
56	70
64	80
128	160
256	320
512	640
768	1000
1536	1600

Prerequisites

The **mfr fragment** command is used to enable fragmentation for an MFR bundle.

Configuration Impact

After the **mfr fragment-size** *size* command is run, the size of each fragment excluding the last one is equal to *size*. The size of the last fragment is smaller than or equal to *size*.

Precautions

Configuring the same maximum fragment size for both ends of an MFR link is recommended to improve transmission efficiency.

Example

Configure the maximum fragment size allowed on the MFR bundle link to 60 bytes.

```
<Huawei> system-view
[Huawei] interface mfr 0/0/1
[Huawei-MFR0/0/1] mfr fragment
[Huawei-MFR0/0/1] mfr fragment-size 60
```

Related Topics

7.6.54 mfr fragment

7.6.60 mfr window-size

7.6.56 mfr link-name

Function

The **mfr link-name** command sets the FR bundle link identifier (LID).

The **undo mfr link-name** command restores the default setting.

By default, LID is the name of the corresponding physical interface.

Format

mfr link-name [*name*]

undo mfr link-name

Parameters

Parameter	Description	Value
name	Specifies the name of a bundle LID.	It is a string of 1 to 49 characters.

Views

FR interface view

Default Level

2: Configuration level

Usage Guidelines

The peer identifies an FR bundle link through LID or associates the bundle link with an FR bundle by using LID.

LID is locally valid. Therefore, the LIDs at both ends of a link can be the same.

 Copyright © Huawei Technologies Co., Ltd.

If a bundle LID on an interface is changed, the modification takes effect only the **shutdown** and the **undo shutdown** commands are run on the interface.

Example

Set the bundle LID of the MFR bundle link Serial 1/0/0:0 to bl1.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr mfr 0/0/3
[Huawei-Serial1/0/0:0] mfr link-name bl1
```

Related Topics

7.6.53 mfr bundle-name

7.6.57 mfr retry

Function

The **mfr retry** command sets the maximum times that an FR bundle link can retransmit the Hello message while waiting for a Hello acknowledgement.

The **undo mfr retry** command restores the default setting.

By default, an MFR bundle link is allowed to retransmit Hello packets for two times.

Format

mfr retry *retry-number*

undo mfr retry

Parameters

Parameter	Description	Value
retry-number	Specifies the maximum number of times an MFR bundle link is allowed to retransmit Hello packets.	The value is an integer ranging from 1 to 5.

Views

FR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a cost-effective solution, MFR bundles multiple physical links to increase bandwidth on FR networks.

 Copyright © Huawei Technologies Co., Ltd.

The two ends of an MFR link communicate with each as follows:

1. The sender sends a Hello packet to the receiver along the MFR link. The interval at which Hello packets are sent can be specified by using the **mfr timer hello** *hello-interval* command.
2. There are two results as the sender receives or does not receive the Hello packet:
   - The sender receives the Hello packet before the timeout period expires, and the MFR link is successfully established. The timeout period can be specified by using the **mfr timer ack** *ack-timeout* command.
   - The sender does not receive any Hello packet before the timeout period expires, and the MFR link fails to be established. The sender will send a Hello packet again, expecting to receive an ACK packet. The maximum times for resending a Hello packet can be specified by using the **mfr retry** *retry-number* command.

     NOTE

     If the sender does not receive an ACK packet after the maximum number of times is reached, the system considers that the data link layer protocol of the FR link fails.

Prerequisites

The **mfr retry** command can be configured only after a physical interface is added to an MFR interface using the **link-protocol fr mfr** command.

Configuration Impact

The interval specified by **mfr timer hello** *hello-interval* must be larger than the timeout period specified by **mfr timer ack** *ack-timeout*. Otherwise, the configured timeout period will be invalid.

Precautions

The status of every physical interface added to an MFR interface determines the status of the MFR interface. As long as one physical interface of the MFR interface is available, the MFR interface is available for upper-layer FR applications. If all physical interfaces of the MFR interface are unavailable, the MFR interface is unavailable for upper-layer FR applications. An MFR interface is a logical interface working at the data link layer, and its member interfaces are physical interfaces working at the physical layer.

Example

Set the maximum retransmission times of the Hello message to 3 on the bundle link Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol fr mfr 0/0/3
[Huawei-Serial1/0/0] mfr retry 3
```

Related Topics

7.6.58 mfr timer ack
7.6.59 mfr timer hello

7.6.58 mfr timer ack

Function

The **mfr timer ack** command sets the time of waiting for an ACK packet before the FR bundle link retransmits the Hello packet.

The **undo mfr timer ack** command restores the default setting.

By default, the time of waiting for an ACK packet before the FR bundle link retransmits the Hello packet is 4s.

Format

mfr timer ack *ack-timeout*

undo mfr timer ack

Parameters

Parameter	Description	Value
ack-timeout	Specifies the time of waiting for an ACK packet before the Hello packet is retransmitted.	The value is an integer ranging from 1 to 10, in seconds.

Views

FR interface view, POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a cost-effective solution, MFR bundles multiple physical links to increase bandwidth on FR networks.

The two ends of an MFR link communicate with each as follows:

1. The sender sends a Hello packet to the receiver along the MFR link. The interval at which Hello packets are sent can be specified by using the **mfr timer hello** *hello-interval* command.
2. There are two results as the sender receives or does not receive the Hello packet:
   - The sender receives the Hello packet before the timeout period expires, and the MFR link is successfully established. The timeout period can be specified by using the **mfr timer ack** *ack-timeout* command.
   - The sender does not receive any Hello packet before the timeout period expires, and the MFR link fails to be established. The sender will send a

 Copyright © Huawei Technologies Co., Ltd.

Hello packet again, expecting to receive an ACK packet. The maximum times for resending a Hello packet can be specified by using the **mfr retry** *retry-number* command.

NOTE

If the sender does not receive an ACK packet after the maximum number of times is reached, the system considers that the data link layer protocol of the FR link fails.

Prerequisites

The **mfr timer ack** command can be configured only after a physical interface is added to an MFR interface using the **link-protocol fr mfr** command.

Configuration Impact

The interval specified by **mfr timer hello** *hello-interval* must be larger than the timeout period specified by **mfr timer ack** *ack-timeout*. Otherwise, the configured timeout period will be invalid.

Precautions

The status of every physical interface added to an MFR interface determines the status of the MFR interface. As long as one physical interface of the MFR interface is available, the MFR interface is available for upper-layer FR applications. If all physical interfaces of the MFR interface are unavailable, the MFR interface is unavailable for upper-layer FR applications. An MFR interface is a logical interface working at the data link layer, and its member interfaces are physical interfaces working at the physical layer.

Example

Set the FR bundle link Serial 1/0/0:0 to wait for 6 seconds before retransmitting the Hello message.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr mfr 0/0/3
[Huawei-Serial1/0/0:0] mfr timer ack 6
```

Related Topics

7.6.59 mfr timer hello

7.6.57 mfr retry

7.6.59 mfr timer hello

Function

The **mfr timer hello** command sets the interval of transmitting a Hello message for an FR bundle link.

The **undo mfr timer hello** command restores the default setting.

By default, a Hello packet is sent at an interval of 10 seconds on the MFR bundle link.

Format

mfr timer hello *hello-interval*

undo mfr timer hello

Parameters

Parameter	Description	Value
hello-interval	Specifies the interval at which the MFR bundle link transmits Hello packets.	The value is an integer ranging from 1 to 180, in seconds.

Views

FR interface view, POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a cost-effective solution, MFR bundles multiple physical links to increase bandwidth on FR networks.

The two ends of an MFR link communicate with each as follows:

1. The sender sends a Hello packet to the receiver along the MFR link. The interval at which Hello packets are sent can be specified by using the **mfr timer hello** *hello-interval* command.
2. There are two results as the sender receives or does not receive the Hello packet:
   - The sender receives the Hello packet before the timeout period expires, and the MFR link is successfully established. The timeout period can be specified by using the **mfr timer ack** *ack-timeout* command.
   - The sender does not receive any Hello packet before the timeout period expires, and the MFR link fails to be established. The sender will send a Hello packet again, expecting to receive an ACK packet. The maximum times for resending a Hello packet can be specified by using the **mfr retry** *retry-number* command.

     NOTE

     If the sender does not receive an ACK packet after the maximum number of times is reached, the system considers that the data link layer protocol of the FR link fails.

Prerequisites

The **mfr timer hello** command can be configured only after a physical interface is added to an MFR interface using the **link-protocol fr mfr** command.

Configuration Impact

The interval specified by **mfr timer hello** *hello-interval* must be larger than the timeout period specified by **mfr timer ack** *ack-timeout*. Otherwise, the configured timeout period will be invalid.

Precautions

The status of every physical interface added to an MFR interface determines the status of the MFR interface. As long as one physical interface of the MFR interface is available, the MFR interface is available for upper-layer FR applications. If all physical interfaces of the MFR interface are unavailable, the MFR interface is unavailable for upper-layer FR applications. An MFR interface is a logical interface working at the data link layer, and its member interfaces are physical interfaces working at the physical layer.

Example

Configure the bundle link Serial 1/0/0:0 to transmit the Hello message every 15 seconds.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr mfr 0/0/3
[Huawei-Serial1/0/0:0] mfr timer hello 15
```

Related Topics

7.6.58 mfr timer ack

7.6.57 mfr retry

7.6.60 mfr window-size

Function

The **mfr window-size** command configures the number of fragments held by the window when MFR reassembles fragments.

The **undo mfr window-size** command configures the number of fragments held by the window when MFR reassembles fragments to as the default value.

By default, the size of a sliding window equals the number of physical interfaces of an MFR bundle.

Format

mfr window-size *number*

undo mfr window-size

Parameters

Parameter	Description	Value
number	Specifies the number of fragments.	The value is an integer ranging from 1 to 16.

Views

MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If low-speed links transmit a large volume of network traffic, set the maximum MFR fragment size to reduce transmission delays.

NOTE

Generally, links whose bandwidth is lower than 768 kbit/s are considered low-speed links.

The sender sends fragments based on the receiving capability of the receiver and the current network status. The **mfr window-size** command can be used to configure the number of fragments held by the slide window when MFR reassembles fragments.

The slide window size determines the speed at which fragments are reassembled. You need to find the trade-off between the number of MFR member links and the slide window size. The default value is recommended.

Prerequisite

The **mfr fragment** command is used to enable fragmentation for an MFR bundle.

Configuration Impact

The fragmentation rate will be affected if the slide window size is greatly different from the number of physical interfaces in an MFR interface.

Precautions

Ensure that the slide window size and the number of physical interfaces in an MFR interface are the same to improve fragment resembling efficiency.

Example

Set the size of the sliding window of MFR 0/0/3 to 8.

```
<Huawei> system-view
[Huawei] interface mfr 0/0/3
[Huawei-MFR0/0/3] mfr window-size 8
```

Related Topics

7.6.50 interface mfr

7.6.54 mfr fragment

7.6.55 mfr fragment-size

 Copyright © Huawei Technologies Co., Ltd.

7.6.61 pvc-pq

Function

Using the **pvc-pq** command, you can specify a PVC PQ queue for packets transmitted over FR VCs.

Using the **undo pvc-pq** command, you can restore the default setting.

By default, packets transmitted over FR VC are placed into the normal-priority queue of PVC PQ.

Format

pvc-pq { **top** | **middle** | **normal** | **bottom** }

undo pvc-pq

Parameters

Parameter	Description	Value
top	Places packets transmitted over FR VCs into a top-priority queue.	-
middle	Places packets transmitted over FR VCs into a middle-priority queue.	-
normal	Places packets transmitted over FR VCs into a normal-priority queue.	-
bottom	Places packets transmitted over FR VCs into a bottom-priority queue.	-

Views

FR class view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

PVC PQ has four queue types: top, middle, normal, and bottom, which are listed in descending order of priority. Packets are placed into the four types of queues based on their VCs. After the queue type of an interface is set to PVC PQ, packets transmitted over the same VC are placed into the same PVC PQ queue.

Prerequisites

The queue type of an FR interface has been set to PVC PQ by using the **fr pvc-pq** command.

Example

Configure packets transmitted over the FR VC associated with FR class **huawei** to enter the high-priority queue.

```
<Huawei> system-view
[Huawei] fr class huawei
[Huawei-fr-class-huawei] pvc-pq top
```

Related Topics

7.6.44 fr pvc-pq

7.6.62 reset fr inarp

Function

The **reset fr inarp** command clears the address mapping of FR established by InARP.

Format

reset fr inarp

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before re-collecting traffic statistics on a specific interface within a certain period, clear the existing traffic statistics of this interface.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

The **reset fr inarp** command can be used to delete all dynamic mapping entries on the router. The execution of this command may result in service interruption. Exercise caution when running this command.

Example

Clear all the FR dynamic address mapping.

```
<Huawei> reset fr inarp
```

Related Topics

7.6.29 fr inarp

7.6.11 display fr inarp-info

7.6.63 shutdown (FR interface view)

Function

The **shutdown** command disables the FR interface or MFR interface.

The **undo shutdown** command enables the FR interface or MFR interface.

By default, the FR interface or MFR interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent a specific interface from forwarding data, run the **shutdown** command in the interface view to shut down the interface.

To enable a specific interface to work, run the **undo shutdown** command in the interface view to start the interface.

Configuration Impact

After the **shutdown** command is run on an MFR interface, all interfaces in the MFR interface are shut down.

Precautions

When a physical interface of the device is idle and not connected to any cable, run the **shutdown** command to shut down the interface to avoid interference.

Example

Shut down the current interface.

```
<Huawei> system-view
[Huawei] interface mfr 0/0/3
[Huawei-MFR0/0/3] shutdown
```

Related Topics

7.6.12 display fr interface

7.6.19 display interface mfr

7.6.64 shutdown (FR switching view)

Function

The **shutdown** command disables the current FR switching PVC.

The **undo shutdown** command enables the current FR switching PVC.

By default, the current FR switching PVC is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

FR switching view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device must be enabled with the FR switching function when the device functions as an FR switch or needs to implement data exchange on an FR network.

 Copyright © Huawei Technologies Co., Ltd.

The router implements the FR switching function using switching PVCs and controls the status of each PVC using the **shutdown** command.

When sub-interfaces are configured on an interface, a minimum interval of 15 seconds is required between the executions of the **shutdown** and **undo shutdown** commands on the main interface.

Prerequisites

The **shutdown** command can take effect only when switching PVC configurations are complete and the specified PVCs are in the Up state.

Example

Disable a switching PVC named pvc2.

```
<Huawei> system-view
[Huawei] fr switch pvc2 interface serial 1/0/0 dlci 100 interface tunnel 0/0/1 dlci 200
[Huawei-fr-switching-pvc2] shutdown
```

Related Topics

7.6.12 display fr interface

7.6.65 timer hold (FR interface view)

Function

The **timer hold** command sets the interval at which status enquiry packets are sent on the DTE.

The **undo timer hold** command restores the default setting.

By default, the DTE sends state enquiry packets at an interval of 10s.

Format

timer hold *interval-time*

undo timer hold

Parameters

Parameter	Description	Value
interval-time	Specifies the polling timer value.	The value is an integer ranging from 0 to 32767, in seconds. When *interval-time* is set to 0, the LMI protocol is disabled.

Views

FR interface view, MFR interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a PVC is used, both the DCE and DTE need to be aware of the PVC status. The LMI protocol is used to monitor the PVC status.

The LMI protocol is used to exchange status information to maintain FR link and PVC status. The DTE sends a status enquiry packet to query the link status at an interval (T391). After receiving the status enquiry packet, the DCE immediately replies with a status response packet. If the DTE does not receive the response within a specific period, a fault is counted. If the number of faults exceeds the upper limit, the DTE considers the physical link and all VCs on it unavailable. In this manner, the status of the link and PVC between the DTE and DCE is maintained.

NOTE

T391, as a variable, defines the interval at which the DTE sends state enquiry packets.

The **timer hold** command sets the interval (T391) at which status enquiry packets are sent on the DTE.

Prerequisites

The type of the FR interface must be DTE. The **fr interface-type** command can be used to configure the type of an FR interface.

Configuration Impact

If you run the **timer hold** command several times, the latest configuration overrides the previous one. After the configuration is complete, the FR negotiation will be performed based on the new LMI protocol type.

Precautions

If the network delay is too long or the congestion is severe, you can increase the polling interval value to reduce network flapping.

Example

Configure the FR interface Serial 1/0/0:0 to operate in the DTE mode. Set the value of polling timer to 15 seconds.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:0
[Huawei-Serial1/0/0:0] link-protocol fr
[Huawei-Serial1/0/0:0] fr interface-type dte
[Huawei-Serial1/0/0:0] timer hold 15
```

Related Topics

7.6.30 fr interface-type

7.6.38 fr lmi t392dce

7.6.66 traffic-shaping adaptation

Function

Using the **traffic-shaping adaptation** command, you can enable traffic shaping adaptation.

Using the **undo traffic-shaping adaptation** command, you can disable traffic shaping adaptation.

By default, traffic shaping adaptation is enabled. Traffic is adjusted based on the backward explicit congestion notification (BECN) bit by 25% of the transmission rate.

Format

traffic-shaping adaptation { **becn** *percentage* | **interface-congestion** *number* }

undo traffic-shaping adaptation { **becn** | **interface-congestion** }

Parameters

Parameter	Description	Value
becn	Adjusts the transmission rate of packets with the BECN bit.	-
percentage	Specifies the percentage of the transmission rate to be adjusted for packets with the BECN bit.	The value is an integer that ranges from 1 to 30, in percentage. The default value is 25%.
interface-congestion	Adjusts the transmission rate based on the packet count of an interface's output queue.	-
number	Specifies the maximum number of packets in an interface's output queue.	The value is an integer that ranges from 1 to 40.

Views

FR class view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To enable FR VCs to automatically adapt to traffic, run the **traffic-shaping adaptation** command to configure FR VCs to automatically adjust the transmission rate. FR VCs determine whether to change the transmission rate based on the following items:

- BECN bit: When network congestion occurs, a DCE sends a packet with the BECN bit set to 1 to a DTE. After receiving this packet, the DTE reduces the transmission rate of VCs from the allowed CIR by a specified percentage each time until the transmission rate reduces to the CIR. If the DTE does not receive any packet with the BECN bit set to 1 within a specified period, it restores the transmission rate of VCs to the allowed CIR.
- Packet count of an interface's output queue: When the interface's output queue reaches the specified length, the transmission rate of VCs begins to reduce. When the interface's output queue is smaller than the specified length, the transmission rate of VCs increases.

Prerequisites

FR traffic shaping has been enabled by using the **fr traffic-shaping** command.

Precautions

NOTE

The AR3260 and AR3670 do not support adjustment of the transmission rate according to the packet count of an interface's output queue.

Example

Configure FR VCs associated with FR class **huawei** to automatically adjust the transmission rate of packets with the BECN bit set to 1 by 20%.

```
<Huawei> system-view
[Huawei] fr class huawei
[Huawei-fr-class-huawei] traffic-shaping adaptation becn 20
```

Related Topics

7.6.3 cir

7.6.4 cir allow outbound

7.6.47 fr traffic-shaping

7.7 HDLC Configuration Commands

NOTE

AR100&AR120&AR150&AR160&AR200 series (except AR162 and AR168F-4P) AR2201-48FE do not support HDLC.

 Copyright © Huawei Technologies Co., Ltd.

7.7.1 display hdlc error

Function

The **display hdlc error** command displays the statistics and details about error packets received by HDLC.

Format

display hdlc error { **statistics** | **packet** *packet-number* } [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
statistics	Displays the error packet statistics.	-
packet *packet-number*	Specifies the number of latest received error packets.	The value is an integer ranging from 1 to 10. The default value is 1.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the interface status or locate faults on an interface, run the **display hdlc error** command to view the status of the interface. You can collect traffic statistics and locate faults on the interface according to the command output.

Example

Display statistics about error packets on Serial1/0/0.

```
<Huawei> display hdlc error statistics interface Serial 1/0/0
HDLC error packet statistics for interface Serial1/0/0:
 Packet too small :          0
 Bad interface    :          0
 Bad packet       :          0
 Sequence mismatch:          0
 Interface down   :          0
 Unknown packet   :          0
```

Table 7-39 Description of the display hdlc error command output

Item	Description
Packet too small	Number of received short packets.
Bad interface	Number of error packets indicating interface errors.
Bad packet	Total number of received error packets.
Sequence mismatch	Number of packets whose sequence numbers are not matched.
Interface down	Number of error packets indicating interface Down.
Unknown packet	Number of error packets indicating unknown errors.

7.7.2 display hdlc statistics

Function

The **display hdlc statistics** command displays statistics about packets on an HDLC interface.

Format

display hdlc statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface number is specified, the statistics about HDLC packets on all interface boards are displayed. If the interface number is specified, the statistics about HDLC packets on the specified interface board are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics about packets on Serial1/0/0.

```
<Huawei> display hdlc statistics interface serial 1/0/0
HDLC packet statistics for interface Serial1/0/0:
 IPv4 Input      :        165      IPv4 Output      :        165
 ISIS Input      :          0      ISIS Output      :          0
 Keepalive Input :       1743      Keepalive Output :       1782
 Invalid Input   :          0
```

Table 7-40 Description of the display hdlc statistics command output

Item	Description
IPv4 Input	Number of received IPv4 packets
IPv4 Output	Number of sent IPv4 packets
ISIS Input	Number of received ISIS packets
ISIS Output	Number of sent ISIS packets
Keepalive Input	Number of received keepalive packets
Keepalive Output	Number of sent keepalive packets
Invalid Input	Number of received invalid packets

7.7.3 link-protocol hdlc

Function

The **link-protocol hdlc** command sets the link layer protocol of an interface to HDLC.

The **undo link-protocol hdlc** command restores the default setting.

By default, the link layer protocol is PPP.

Format

link-protocol hdlc

undo link-protocol hdlc

Parameters

None

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

When you encapsulate an interface with HDLC, ensure that the IP address of the interface must be at the same network segment with that of the peer.

Example

Set HDLC for Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol hdlc
```

Related Topics

7.7.4 timer hold (HDLC)

7.7.4 timer hold (HDLC)

Function

The **timer hold** command sets the polling interval for sending keepalive packets.

The **undo timer hold** command restores the default setting.

By default, the interface polling interval is 10 seconds.

Format

timer hold *seconds*

undo timer hold

Parameters

Parameter	Description	Value
seconds	Sets a polling interval.	The value is an integer ranging from 0 to 32767, in seconds. Value 0 indicates that link check is disabled.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

HDLC uses keepalive packets to check the link status. You can set the polling interval to specify the interval for sending keepalive packets.

- If the network delay is too long or the congestion is severe, you can increase the polling interval to prevent network flapping.
- If the polling interval is too long, the link check will be slow. If the polling interval is too short, device load will increase and more network bandwidth will be occupied.

Precautions

When setting the polling interval, ensure that configurations on both ends are the same. Otherwise, the link-layer protocol cannot be Up.

Example

Set the polling interval to 20 seconds on Serial 1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] timer hold 20
```

Related Topics

7.7.3 link-protocol hdlc

7.8 LAPB Configuration Commands

NOTE

Only the AR2204XE, AR2204XE-DC AR2240C and the router which using SRU40 support LAPB and X.25.

7.8.1 lapb max-frame

Function

The **lapb max-frame** command sets LAPB parameter N1.

The **undo lapb max-frame** command restores the default value of LAPB parameter N1.

The default N1 value is 12032.

Format

lapb max-frame *n1-value*

undo lapb max-frame

Parameters

Parameter	Description	Setting
n1-value	Specifies the value of LAPB parameter N1.	The value is an integer, in bits. Set parameter N1 based on the following scenarios: ● When the data link layer protocol of an interface is LAPB, the N1 value is fixed at 12032. ● When the data link layer protocol of an interface is X.25, the N1 value ranges from 1096 to 12104 and must be a multiple of 8. By default, the N1 value is eight times the total number of bytes of the MTU plus the protocol header.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LAPB parameter N1 indicates the maximum number of bits in sent or received I frames on the interface. When the interface accesses an X.25 network, X.25 packets are encapsulated in LAPB I frames. LAPB parameter N1 also indicates the maximum number of bits in transmitted X.25 packets on the link.

Prerequisites

LAPB has been configured as the data link layer protocol of an interface using the **link-protocol lapb** command, or X.25 has been configured as the data link layer protocol of an interface using the **link-protocol x25** command.

Example

Set LAPB parameter N1 to 12032 on Serial1/0/0.

```
<Huawei> system-view
```

```
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol lapb
[Huawei-Serial1/0/0] lapb max-frame 12032
```

Related Topics

7.8.6 link-protocol lapb

7.8.2 lapb modulo

Function

The **lapb modulo** command sets the LAPB frame numbering mode (also called modulo).

The **undo lapb modulo** command restores the default LAPB frame numbering mode.

By default, the LAPB frame numbering mode is modulo 8.

Format

lapb modulo { **128** | **8** }

undo lapb modulo

Parameters

Parameter	Description	Setting
128	Sets the LAPB frame numbering mode to modulo 128.	-
8	Sets the LAPB frame numbering mode to modulo 8.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LAPB frame numbering mode is used to define the number range of information frames (I frames). I frames are numbered in sequence and the cycle range of I frame numbers is 0 to modulo minus 1.

 Copyright © Huawei Technologies Co., Ltd.

Two LAPB frame numbering modes are available: modulo 8 and modulo 128. Modulo 8 is the basic mode supported by all standard LAPB versions and applies to most links. Modulo 128 is the extended mode and supports larger throughput when applied to links with low error rates and high speeds, for example, satellite links.

Prerequisites

LAPB has been configured as the data link layer protocol of an interface using the **link-protocol lapb** command, or X.25 has been configured as the data link layer protocol of an interface using the **link-protocol x25** command.

Precautions

Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

Example

Set the LAPB frame numbering mode to modulo 8 on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol lapb
[Huawei-Serial1/0/0] lapb modulo 8
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.8.6 link-protocol lapb

7.8.3 lapb retry

Function

The **lapb retry** command sets LAPB parameter N2.

The **undo lapb retry** command restores the default value of LAPB parameter N2.

The default N2 value is 10.

Format

lapb retry *n2-value*

undo lapb retry

Parameters

Parameter	Description	Setting
n2-value	Specifies the value of LAPB parameter N2.	The value is an integer that ranges from 1 to 255.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LAPB parameter N2 indicates the maximum number of times the DCE or DTE successfully sends a frame to the remote DTE or DCE. If the number of times the DCE or DTE sends a frame exceeds the N2 value, the frame fails to be sent and LAPB link becomes Down.

Prerequisites

LAPB has been configured as the data link layer protocol of an interface using the **link-protocol lapb** command, or X.25 has been configured as the data link layer protocol of an interface using the **link-protocol x25** command.

Example

Set LAPB parameter N2 to 20 on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol lapb
[Huawei-Serial1/0/0] lapb retry 20
```

Related Topics

7.8.6 link-protocol lapb

7.8.4 lapb timer

Function

The **lapb timer** command sets the values of LAPB system timers T1, T2, and T3.

The **undo lapb timer** command restores the default values of timers T1, T2, and T3.

By default, the T1 value is 3000 ms, the T2 value is 1500 ms, and the T3 value is 0s.

Format

lapb timer { **t1** *t1-value* | **t2** *t2-value* | **t3** *t3-value* }

undo lapb timer { **t1** | **t2** | **t3** }

Parameters

Parameter	Description	Setting
t1-value	Specifies the value of LAPB system timer T1.	The value is an integer that ranges from 1 to 64000, in milliseconds.
t2-value	Specifies the value of LAPB system timer T2.	The value is an integer that ranges from 1 to 32000, in milliseconds.
t3-value	Specifies the value of LAPB system timer T3.	The value is an integer that ranges from 0 to 255, in seconds. When the value of T3 is 0, the T3 timer does not take effect.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help monitor LAPB data transmission, LAPB defines the following timers:

- T1 timer: send timer. When the T1 timer expires, the DTE or DCE starts retransmission.
- T2 timer: receive timer. When the T2 timer expires, the DTE or DCE must send an acknowledgement frame so that the remote DCE or DTE can receive the acknowledgement frame before its T1 timer expires. The T2 value must be smaller than or equal to a half of the T1 value.
- T3 timer: idle channel timer. When the T3 timer expires, the DCE reports to the packet layer that the channel of the link has been idle for a long period of time. The T3 value must be larger than the T1 value of the DCE.

Prerequisites

LAPB has been configured as the data link layer protocol of an interface using the **link-protocol lapb** command, or X.25 has been configured as the data link layer protocol of an interface using the **link-protocol x25** command.

Example

Set the LAPB system timer T1 to 1000 ms on Serial1/0/0.

```
<Huawei> system-view
```

```
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol lapb
[Huawei-Serial1/0/0] lapb timer t1 1000
```

Related Topics

7.8.6 link-protocol lapb

7.8.5 lapb window-size

Function

The **lapb window-size** command sets LAPB window parameter K.

The **undo lapb window-size** command restores the default value of LAPB window parameter K.

The default value of LAPB window parameter K is 7.

Format

lapb window-size *k-value*

undo lapb window-size

Parameters

Parameter	Description	Setting
k-value	Specifies the value of LAPB window parameter K.	The value is an integer and varies with the LAPB frame numbering mode (also called modulo). • If modulo 8 is used, the value of LAPB window parameter K ranges from 1 to 7. • If modulo 128 is used, the value of LAPB window parameter K ranges from 1 to 127.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Window parameter K defines the LAPB window size, indicating the maximum number of I frames with numbers to be acknowledged that the DTE or DCE can send.

Prerequisites

LAPB has been configured as the data link layer protocol of an interface using the **link-protocol lapb** command, or X.25 has been configured as the data link layer protocol of an interface using the **link-protocol x25** command.

Precautions

Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

Example

Set LAPB window parameter K to 5 on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol lapb
[Huawei-Serial1/0/0] lapb window-size 5
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.8.6 link-protocol lapb

7.8.2 lapb modulo

7.8.6 link-protocol lapb

Function

The **link-protocol lapb** command sets the data link layer protocol to LAPB on an interface.

The **undo link-protocol lapb** command restores the default configuration.

By default, the data link layer protocol of an interface is PPP. When LAPB is used as the data link layer protocol on an interface, the interface works as a DTE interface and transmits IP traffic by default.

Format

link-protocol lapb [**dce** | **dte**] [**ip** | **multi-protocol**]

undo link-protocol lapb

Parameters

Parameter	Description	Setting
dce	Configures an interface as a DCE interface.	-

Parameter	Description	Setting
dte	Configures an interface as a DTE interface.	-
ip	Configures LAPB to transmit IP traffic.	-
multi-protocol	Configures LAPB to transmit traffic of multiple network-layer protocols.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

LAPB is a bit-oriented data link layer that defines the process of exchanging frames between the data terminal equipment (DTE) and data circuit-terminating equipment (DCE). It ensures that frames are transmitted in the right sequence without errors.

In addition to the second layer of X.25, LAPB can function as an independent data link layer protocol to transmit non-X.25 data of upper-layer protocols. LAPB can be configured on synchronous serial interfaces for simple local data transmission.

Example

Set the data link layer protocol to LAPB on Serial1/0/0 and configure Serial1/0/0 as a DCE interface.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol lapb dce
```

7.8.7 display lapb status

Function

The **display lapb status** command displays information about the LAPB status.

Format

display lapb status

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display information about the LAPB status.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] display lapb status
  Lapb Current Status:
  linkSetup--SABM sent.
  the times of state changes: 1
  state change reason:
  initial state.
  T1 timer out: 0
```

Table 7-41 Description of the display lapb status command output

Item	Description
Lapb Current Status	Current LAPB status.
the times of state changes	Number of LAPB status changes.
state change reason	Cause for an LAPB status change.
T1 timer out	Number of times that the T1 timer expires.

Related Topics

7.8.6 link-protocol lapb

7.8.8 reset lapb statistics

Function

The **reset lapb statistics** command clears statistics about LAPB packets on an interface.

Format

reset lapb statistics

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before collecting traffic statistics about an interface within a period of time, clear the existing statistics about this interface.

Example

Clear statistics about LAPB packets on Serial1/0/0.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] reset lapb statistics
```

7.9 X.25 Configuration Commands

NOTE

Only the AR2204XE, AR2204XE-DC AR2240C and the router which using SRU40 support LAPB and X.25.

7.9.1 display x25 alias-policy

Function

The **display x25 alias-policy** command displays the X.25 alias list.

Format

display x25 alias-policy [**interface serial** *interface-number*]

Parameters

Parameter	Description	Value
interface serial *interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating an interface fault, you can run this command to view alias information about the interface.

Example

Display the X.25 alias list.

```
<Huawei> display x25 alias-policy
Alias for interface Serial2/0/0:
   Alias-1  : $20112450          left
   Alias-2  : $20112405$          strict
   Alias-3  : 20112450$          right
```

Table 7-42 Description of the display x25 alias-policy command output

Item	Description
Alias for interface Serial2/0/0	Aliases of Serial2/0/0: • $20112450: alias 1, which is in left-aligned matching mode. • 20112405: alias 2, which is in strict matching mode. • 20112450$: alias 3, which is in right-aligned matching mode.

Related Topics

7.9.11 x25 alias-policy

7.9.2 display x25 map

Function

The **display x25 map** command displays the X.25 address mapping table.

Format

display x25 map

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

X.25 address mapping can be configured using the **x25 map** command (direct configuration) or the **x25 pvc** command (indirect configuration). You can run the **display x25 map** command to view all address mapping entries.

Example

Display the X.25 address mapping table.

```
<Huawei> display x25 map
Interface:Serial2/0/0(protocol status is up):
ip address:1.1.1.1   X.121 address: 22
   map-type: SVC_MAP  VC-number: 0
   Facility:
     ACCEPT_REVERSE;
     BROADCAST;
     PACKET_SIZE: I 512  O 512 ;
```

Table 7-43 Description of the display x25 map command output

Item	Description
Interface	Type and number of the interface where an address mapping table exists.
ip address	IP address of the interface.
X.121 address	X.121 address of the interface.
map-type	Virtual circuit (VC) type of address mapping.
VC-number	Total number of VC connections.
Facility	User facility configured for the interface.

Related Topics

7.9.17 x25 map
7.9.20 x25 pvc
7.9.27 x25 switch pvc
7.9.41 x25 xot pvc

 Copyright © Huawei Technologies Co., Ltd.

7.9.3 display x25 switch-table pvc

Function

The **display x25 switch-table pvc** command displays the X.25 PVC routing table.

Format

display x25 switch-table pvc

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring interface status or locating an interface fault, you can run this command to view information about the X.25 PVC routing table.

Example

Display the X.25 PVC routing table.

```
<Huawei> display x25 switch-table pvc
#1     (In: Serial1/0/0  - PVC1024   ) <--> (Out: Serial2/0/0  - PVC1   )
#2     (In: Serial2/0/0  - PVC1024   ) <--> (Out: Serial1/0/0  - PVC1   )
```

Table 7-44 Description of the display x25 switch-table pvc command output

Item	Description
#1	Sequence number of a route in the X.25 PVC routing table.
In	Type, number, and VC number of an interface that receives packets.
Out	Type, number, and VC number of an interface that forwards packets.

Related Topics

7.9.20 x25 pvc

7.9.27 x25 switch pvc

7.9.41 x25 xot pvc

7.9.4 display x25 switch-table svc

Function

The **display x25 switch-table svc** command displays the X.25 SVC routing table.

Format

display x25 switch-table svc { **dynamic** | **static** }

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When monitoring interface status or locating an interface fault, you can run this command to view information about the X.25 SVC routing table.

Example

Display the X.25 SVC routing table.

```
<Huawei> display x25 switch-table svc static
Number Destination Substitute-src Substitute-dst CUD   SwitchTo(type/name)
1      11                                          I/Serial2/0/0
2      22                                          I/Serial2/1/0
3      132                                          T/1.1.1.123
4      133                                          T/1.1.1.123
5      111            222            333                T/4.4.4.4
Total of static svc is 5.
The item type of SwitchTo meaning:
I: interface   H: hunt-group   T: xot
```

Table 7-45 Description of the display x25 switch-table svc command output

Item	Description
Number	Sequence number of a route in the X.25 SVC routing table.
Substitute-src	Source X.121 address after substitution. If the value is empty, the address substitution is not required.

Item	Description
Substitute-dst	Destination X.121 address after substitution. If the value is empty, the address substitution is not required.
CUD	Call user data.
SwitchTo	Forwarding address of a route, including the interface, XOT channel, and hunt group.

Related Topics

7.9.27 x25 switch pvc

7.9.5 display x25 vc

Function

The **display x25 vc** command displays X.25 VCs.

Format

display x25 vc [*vcn*]

Parameters

Parameter	Description	Value
vcn	Specifies the number of an X.25 VC.	The value is an integer that ranges from 1 to 4095. If no X.25 VC number is specified, all VCs are displayed.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device functions as a DCE and X.25 switching is enabled, set up VCs to transmit data. VCs are classified into the following types:

- Switched virtual circuit (SVC): An SVC is a temporary connection for transmitting scattered data. When there is data to be transmitted, DTEs set up an SVC. When data transmission is complete, DTEs tear down the SVC. SVCs apply to transmission of intermittent and burst traffic.
- Permanent virtual circuit (PVC): After a PVC is set up, devices enter the data transmission phase, in which calls are not established or cleared. Once a PVC

is set up, it permanently takes effect unless you tear down it manually. PVCs apply to transmission of frequent and stable traffic.

You can run the **display x25 vc** command to view information about both SVCs and PVCs. Some fields in the command output are different for the SVCs and PVCs.

Example

Display X.25 VCs.

```
<Huawei> display x25 vc
Interface: Serial2/0/0
  SVC 1
    State: P4
    Map: ip 10.1.1.2 to 130
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 5  Local PR: 5  Remote PS: 5  Remote PR: 4
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 5/5  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 420/420
    Snd Queue(Current/Max): 0/200
Interface: Serial2/0/0
  SVC 10
    State: P4
    SVC <--> Serial2/0/0 SVC 60
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 0  Local PR: 0  Remote PS: 0  Remote PR: 0
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 5/5  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 420/420
    Snd Queue(Current/Max): 0/200
Interface: Serial2/0/0-1.1.1.1
  PVC 1
    State: P/Inactive
    XOT PVC <--> Serial2/0/0 PVC 1 connected
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 0  Local PR: 0  Remote PS: 0  Remote PR: 0
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 0/0  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 0/0
    Snd Queue(Current/Max): 1/200
Interface: Serial2/0/0
  PVC 1
    State: D3
    PVC <--> XOT Serial2/0/0-1.1.1.1 PVC 1 connected
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 0  Local PR: 0  Remote PS: 0  Remote PR: 0
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 0/0  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 0/0
    Snd Queue(Current/Max): 0/200
Interface: Serial2/0/0
  SVC 59
    State: P4
```

```
  PAD: UI-130 From remote 130 connected to local 220
  Window size: input 2  output 2
  Packet Size: input 128  output 128
  Local PS: 3  Local PR: 1  Remote PS: 1  Remote PR: 2
  Local Busy: FALSE  Reset times: 0
  Input/Output:
    DATA 9/11  INTERRUPT 0/0
    RR 6/2  RNR 0/0  REJ 0/0
    Bytes 53/363
Snd Queue(Current/Max): 0/200
```

Table 7-46 Description of the display x25 vc command output

Item	Description
Interface	Type and number of an interface of a VC.
SVC 1	Type and number of the VC.
State	Status of the VC.
Map	Mapping between the IP address and VC number.
Window size	Size of windows.
Packet Size	Size of packets.
Local PS	Sequence number of an X.25 packet to be sent on the local end.
Local PR	Sequence number of the next desired X.25 packet to be received on the local end.
Remote PS	Sequence number of an X.25 packet to be sent on the remote end.
Remote PR	Sequence number of the next desired X.25 packet to be received on the remote end.
Local Busy	Indicates whether the local end is busy. The options are as follows: ● TRUE: busy ● FALSE: not busy
Reset times	Number of VC reset times.
SVC <--> Serial2/0/0 SVC 60	Remote interface and VC number of an SVC.
XOT PVC <--> Serial2/0/0 PVC 1 connected	Remote interface, VC number, and VC status of an XOT connection.
Input/Output	Input and output information.
Snd Queue(Current/Max)	Send queue (number of current packets in the queue/maximum number of packets in the queue).

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.9.20 x25 pvc
7.9.27 x25 switch pvc
7.9.41 x25 xot pvc

7.9.6 display x25 xot

Function

The **display x25 xot** command displays information about XOT connections.

Format

display x25 xot

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display x25 xot** command to view detailed information about all XOT connections, including the remote IP address, remote port number, local IP address, local port number, keepalive attribute settings of the socket, inbound interface name, and outbound interface name.

Example

Display information about XOT connections.

```
<Huawei> display x25 xot
SVC 1024:  ( ESTAB )
  tcp peer ip: 10.1.1.1, peer port: 1998
  tcp local ip: 10.1.1.2, local port: 1024
  socket keepalive period: 5, keepalive tries: 3
  come interface name: Serial1/0/0-10.1.1.1
  go interface name: Serial1/0/0
```

Table 7-47 Description of the display x25 xot command output

Item	Description
SVC 1024: (ESTAB)	An XOT link has been set up through an SVC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
tcp peer ip: 10.1.1.1, peer port: 1998	The remote IP address is 10.1.1.1, and the remote port number is 1998.
tcp local ip: 10.1.1.2, local port: 1024	The local IP address is 10.1.1.2, and the remote port number is 1024.
socket keepalive period: 5, keepalive tries: 3	The delay for sending keepalive packets is 5s for the XOT connection, and the maximum number of failures to send a keepalive packet is 3. When the number of failures to send a keepalive packet exceeds 3, the XOT connection is torn down.
come interface name	The inbound interface name is Serial1/0/0-10.1.1.1 (XOT interface).
go interface name	The outbound interface name is Serial1/0/0.

Related Topics

7.9.29 x25 switch svc xot

7.9.41 x25 xot pvc

7.9.7 link-protocol x25

Function

The **link-protocol x25** command configures X.25 as the data link layer protocol of an interface.

The **undo link-protocol x25** command restores the default configuration.

By default, the data link layer protocol of an interface is PPP. When the data link layer protocol of an interface is X.25, the interface works in DTE mode by default and data packets are encapsulated in IETF format.

Format

link-protocol x25 [**dce** | **dte**] [**ietf** | **nonstandard**]

undo link-protocol x25

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dce	Indicates that the interface works in DCE mode.	-
dte	Indicates that the interface works in DTE mode.	-
letf	Indicates that data packets are encapsulated in IETF format. IP packets or other network protocol packets on the X.25 network are encapsulated in IETF RFC 1356 standard encapsulation format.	-
nonstandard	Indicates that data packets are encapsulated in nonstandard encapsulation formats. IP packets or other network protocol packets on the X.25 network are encapsulated in nonstandard encapsulation formats.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The X.25 protocol stack defines the interfaces between the DTE and DCE on public data networks (PDNs). The protocol stack has three layers, physical layer, data link layer, and packet layer. LAPB is used on the data link layer.

An X.25 network is deployed on a WAN that allows for low transmission costs and does not have high requirements for the remote transmission speed or delay. Currently, X.25 networks are still used as dedicated networks in some countries or regions. As IP networks are widely applied, X.25 data is transmitted on IP

 Copyright © Huawei Technologies Co., Ltd.

networks. X.25 over TCP (XOT) technology is introduced to connect X.25 networks over IP networks. This technology encapsulates X.25 packets in TCP packets to transmit X.25 packets across an IP network.

Precautions

Use the IETF data packet encapsulation format if there is no special requirement.

When configuring X.25 as the data link layer protocol of an interface, use different configuration methods in different scenarios.

- If two devices are connected through an X.25 network, they should work in DTE mode.
- If the X.25 switching function is enabled on a device, the device generally works in DCE mode.
- If two devices are directly connected in back-to-back mode using the X.25 protocol, configure one device to work in DTE mode and the other device in DCE mode, and ensure that connected interfaces on the two devices use the same data packet encapsulation format.

Example

Set the data link layer protocol of Serial1/0/0 to X.25, operation mode to DCE, and data packet encapsulation format to IETF.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25 dce ietf
```

7.9.8 reset x25 counters

Function

The **reset x25 counters** command clears statistics about X.25 packets on an interface.

Format

reset x25 counters interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Before collecting traffic statistics about an interface within a period of time, clear the existing statistics about this interface.

Example

Clear statistics about X.25 packets on Serial1/0/0.

```
<Huawei> reset x25 counters interface serial 1/0/0
```

7.9.9 reset x25 vc

Function

The **reset x25 vc** command resets an X.25 VC.

Format

reset x25 vc interface *interface-type interface-number* [*vc-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
vc-number	Specifies a VC number.	The value is an integer that ranges from 1 to 4095.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Resetting a VC will interrupt existing services. Therefore, exercise caution when running the **reset x25 vc** command.

Example

Reset all VCs on Serial1/0/0.

```
<Huawei> reset x25 vc interface serial 1/0/0
```

Related Topics

7.9.5 display x25 vc

7.9.10 reset xot

Function

The **reset xot** command automatically deletes an XOT link for an SVC.

The **reset xot** command automatically resets an XOT link for a PVC.

Format

reset xot local *local-ip-address local-port* **remote** *remote-ip-address remote-port*

Parameters

Parameter	Description	Value
local-ip-address	Specifies the local IP address of the XOT link.	The value is in dotted decimal notation.
local-port	Specifies the local port number of the XOT link.	The value is an integer that ranges from 1 to 65535.
remote-ip-address	Specifies the remote IP address of the XOT link.	The value is in dotted decimal notation.
remote-port	Specifies the remote port number of the XOT link.	The value is an integer that ranges from 1 to 65535.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **reset xot** to delete or reset an XOT link. You can run the **display x25 xot** command to obtain the IP addresses and port numbers required to delete or reset an XOT link.

Example

Delete or reset an XOT link.

```
<Huawei> reset xot local 10.1.1.1 1998 remote 10.1.1.2 1024
```

Related Topics

7.9.6 display x25 xot

7.9.5 display x25 vc

7.9.30 x25 switching

 Copyright © Huawei Technologies Co., Ltd.

7.9.11 x25 alias-policy

Function

The **x25 alias-policy** command specifies an alias for the X.121 address of an X.25 interface.

The **undo x25 alias-policy** command deletes the alias for the X.121 address of an X.25 interface.

By default, the X.121 address of an X.25 interface has no alias.

Format

x25 alias-policy *match-type alias-string*

undo x25 alias-policy *match-type alias-string*

Parameters

Parameter	Description	Value
match-type	Specifies the matching mode of an alias. **Table 7-48** describes available matching modes.	-
alias-string	Specifies the alias of an X.121 address.	-

Table 7-48 Alias matching modes and meanings

Matching Mode	Meaning	Example
free	Indicates free matching. The alias is similar to "1234".	For example, the alias 1234 successfully matches 561234, 12345677, and 956123478, but fails to match 12354.
free-ext	Indicates extended free matching. The alias is similar to "...1234..".	For example, the alias ...1234.. successfully matches 678123459, but fails to match 68123459, 67812345, and 6781234591.

 Copyright © Huawei Technologies Co., Ltd.

Matching Mode	Meaning	Example
left	Indicates left alignment matching. The alias is similar to "$1234".	For example, the alias $1234 successfully matches 1234567 and 12346790, but fails to match 3123478 and 123784.
left-ext	Indicates extended left alignment matching. The alias is similar to "$1234...".	For example, the alias $1234... successfully matches 1234679 and 1234872, but fails to match 123468 and 12346890.
right	Indicates right alignment matching. The alias is similar to "1234$".	For example, the alias 1234$ successfully matches 791234 and 6901234, but fails to match 7912345 and 6212534.
right-ext	Indicates extended right alignment matching. The alias is similar to "....1234$".	For example, the alias ....1234$ successfully matches 79001234 and 86901234, but fails to match 7912345 and 506212534.
strict	Indicates strict matching. The alias is similar to "1234".	For example, the alias 1234 only matches 1234.
whole	Indicates whole matching. The alias is similar to ".....".	For example, the alias ..... successfully matches all valid X.121 addresses whose length is 8.
whole-ext	Indicates extended whole matching. The alias can only be "*".	The alias * successfully matches all valid X.121 addresses.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an X.25 call is forwarded over different X.25 networks, the X.25 networks may process the destination address (called DTE's address) carried in the call packet. For example, the X.25 networks regularly add or remove the prefix or suffix. You need to configure an alias for the X.121 address to adapt to the changes.

Prerequisites

The interface has been configured to use X.25 as the data link layer protocol and work in DCE mode using the **link-protocol x25 dce** [**ietf** | **nonstandard**] command.

Precautions

NOTE

Consult the X.25 service provider about whether the alias function is enabled and which matching method can be selected.

Example

Configure X.25 as the data link layer protocol of Serial1/0/0, assign the X.121 address 20112451 to Serial1/0/0, and configure two aliases with different matching modes for the X.121 address.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25 dce
[Huawei-Serial1/0/0] x25 x121-address 20112451
[Huawei-Serial1/0/0] x25 alias-policy right 20112451$
[Huawei-Serial1/0/0] x25 alias-policy left $20112451
```

After the configuration, a call with the destination address 20112451 can be accepted as long as the call can reach the local X.25 interface Serial1/0/0 no matter whether the network adds a prefix or suffix to the address.

Related Topics

7.9.1 display x25 alias-policy
7.9.40 x25 x121-address

7.9.12 x25 call-facility

Function

The **x25 call-facility** command configures user facility options for an X.25 interface. If an option is configured, all calls originated from the X.25 interface carry corresponding information fields in call packets.

The **undo x25 call-facility** command deletes configured user facility options.

By default, no user facility option is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

x25 call-facility *facility-option*

undo x25 call-facility *facility-option*

Parameters

Parameter	Description	Value
facility-option	Specifies a user facility option. **Table 7-49** describes optional user facility options.	-

Table 7-49 Description of user facility options

Option	Description	Value
packet-size *input-size output-size*	Indicates that the maximum packet size negotiation is performed for a call originated from the X.25 interface. The maximum packet size negotiation is a part of the flow control parameter negotiation. It involves two parameters: the maximum input packet size and maximum output packet size.	The value is an integer that ranges from 16 to 4096, in bytes. It must be an integral power of 2.
reverse-charge-request	Indicates that a call originated from the X.25 interface carries the reverse charging request.	-
roa-list *name*	Specifies a recognized operating agency (ROA) list name for the X.25 interface. The ROA list is defined by running the **x25 roa-list** command in the system view.	The value is a string of 1 to 19 characters.
send-delay *value*	Indicates that a call originated from the X.25 interface carries the maximum transit delay request.	The value is an integer that ranges from 0 to 65534, in milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Option	Description	Value
threshold *in out*	Indicates that the throughput class negotiation is performed for a call originated from the X.25 interface.	The value is an integer that can only be 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, and 48000, which are expressed in bit/s.
window-size *input-window-size output-window-size*	Indicates that the window size negotiation is performed for a call originated from the X.25 interface. The window size negotiation is a part of the flow control parameter negotiation. It involves two parameters: the input window size and output window size.	The value is an integer and varies with the X.25 packet sequence numbering mode (also called modulo). ● When the X.25 packet sequence numbering mode is the modulo 8 mode, the value of the window size ranges from 1 to 7. ● When the X.25 packet sequence numbering mode is the modulo 128 mode, the value of the window size ranges from 1 to 127.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Various user facility options are defined in the X.25 protocol. By default, no user facility is configured on the device. You can select and configure user facilities using the following methods:

- Run the **x25 call-facility** *facility-option* command to configure user facility options based on an X.25 interface.
- Run the **x25 map** command to configure user facility options based on an address mapping.

The X.25 interface-based configuration is effective for every call originated from the X.25 interface. The address mapping-based configuration is effective only for calls originated from the address mapping. If both X.25 interface-based

configuration and address mapping-based configuration are configured, the address mapping-based configuration has a higher priority.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Configure all calls originated from Serial1/0/0 to negotiate the maximum packet size and window size with the peer end, set the maximum packet size negotiation value to 512 bytes, and set the window size negotiation value to 5.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 call-facility packet-size 512 512
[Huawei-Serial1/0/0] x25 call-facility window-size 5 5
```

Related Topics

7.9.17 x25 map

7.9.13 x25 default-protocol

Function

The **x25 default-protocol** command configures the default upper-layer protocol for X.25.

The **undo x25 default-protocol** command restores the default configuration.

By default, the upper-layer protocol for X.25 is the Internet Protocol (IP).

Format

x25 default-protocol ip

undo x25 default-protocol

Parameters

Parameter	Description	Value
ip	Sets the default upper-layer protocol for X.25 to the IP protocol. Currently, it can only be set to the IP protocol.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An X.25 Call Request packet contains a Call User Data (CUD) field that specifies the upper-layer protocol. During setup of an X.25 switched virtual circuit (SVC), the called DTE checks the CUD field in the X.25 Call Request packet. If the CUD field is unrecognizable, the called DTE refuses the setup of the call connection, and the call cannot be set up. You can configure the default upper-layer protocol for X.25 on an X.25 interface. Currently, the default upper-layer protocol can only be set to the Internet Protocol (IP). After receiving a Call Request packet with an unknown CUD field, the X.25 interface processes the packet based on the specified default upper-layer protocol.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Set the default upper-layer protocol for X.25 on Serial1/0/0 to the IP protocol.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 default-protocol ip
```

Related Topics

7.9.17 x25 map

7.9.14 x25 facility packetsize-windowsize compatible enable

Function

The **x25 facility packetsize-windowsize compatible enable** command enables the compatible option for X.25 user facility. If this option is enabled, the window size and packet size carried in call packets of all the calls originated from the X.25 interface will be consistent with those of the remote end.

The **undo x25 facility packetsize-windowsize compatible enable** command disables the compatible option for X.25 user facility.

By default, the compatible option is disabled for X.25 user facility.

Format

x25 facility packetsize-windowsize compatible enable

undo x25 facility packetsize-windowsize compatible enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device functioning as a DTE or DCE connects to non-Huawei devices using X.25, inconsistent window sizes and packet sizes will cause Clear or Reset events. To ensure that X.25 performs flow control effectively and correctly, you need to configure the compatible option for X.25 user facility.

Example

Enable the compatible option for X.25 user facility.

```
<Huawei> system-view
[Huawei] x25 facility packetsize-windowsize compatible enable
```

7.9.15 x25 ignore called-address

Function

The **x25 ignore called-address** command configures an X.25 interface to send a Call Request packet without the X.121 address of the called DTE.

The **undo x25 ignore called-address** command restores the default configuration.

By default, the Call Request packet sent by an X.25 interface contains the X.121 address of the called DTE.

Format

x25 ignore called-address

undo x25 ignore called-address

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

As specified in X.25, a Call Request packet must contain the calling DTE address and called DTE address. However, some Call Request packets do not contain the called DTE address or calling DTE address in actual network environments. You can configure the Call Request packet based on actual network requirements to adapt to differences between networks.

You can run the **x25 ignore called-address** command to configure an X.25 interface to send a Call Request packet without the X.121 address of the called DTE.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Configure Serial1/0/0 to send a Call Request packet that does not contain the X.121 address of the called DTE.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 ignore called-address
```

Related Topics

7.9.23 x25 response called-address

7.9.16 x25 ignore calling-address

7.9.24 x25 response calling-address

7.9.16 x25 ignore calling-address

Function

The **x25 ignore calling-address** command configures an X.25 interface to send a Call Request packet without the X.121 address of the calling DTE.

The **undo x25 ignore calling-address** command restores the default configuration.

By default, the Call Request packet sent by an X.25 interface contains the X.121 address of the calling DTE.

Format

x25 ignore calling-address

undo x25 ignore calling-address

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As specified in X.25, a Call Request packet must contain the calling DTE address and called DTE address. However, some Call Request packets do not contain the called DTE address or calling DTE address in actual network environments. You can configure the Call Request packet based on actual network requirements to adapt to differences between networks.

You can run the **x25 ignore calling-address** command to configure an X.25 interface to send a Call Request packet without the X.121 address of the calling DTE.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Configure Serial1/0/0 to send a Call Request packet that does not contain the X.121 address of the calling DTE.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 ignore calling-address
```

Related Topics

7.9.23 x25 response called-address

7.9.15 x25 ignore called-address

7.9.24 x25 response calling-address

7.9.17 x25 map

Function

The **x25 map** command creates a mapping between the IP address and X.121 address of a destination device on an X.25 interface.

The **undo x25 map** command deletes a configured mapping.

By default, no mapping between the IP address and X.121 address of a destination device is configured on an X.25 interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

x25 map ip *ip-address* **x121-address** *x.121-address* [*option*]

undo x25 map ip *ip-address*

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IP protocol of the destination device.	The value is in dotted decimal notation.
x121-address *x.121-address*	Specifies the X.121 address of the destination device.	The value is a string of 1 to 15 characters. It can only contain digits 0 to 9.
option	Specifies the options in an X.25 address mapping. For descriptions of the options, see **Table 7-50**.	-

Table 7-50 Descriptions of options in an X.25 address mapping

Parameter	Meaning	Value
broadcast	Indicates that the device sends broadcast data packets to the remote end of the SVC associated with the address mapping. This option supports some routing protocols (for example, RIP).	-
encapsulation-type	Specifies the data packet encapsulation format. The value can be **nonstandard**, **ietf**, **multi-protocol**, or **snap**.	-
idle-timer *minutes*	Specifies the maximum idle time for the SVC associated with the address mapping.	The value is an integer that ranges from 0 to 255, in minutes. *0* indicates that the idle time is infinite. An SVC is always connected even if no data is transmitted over it.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Meaning	Value
no-callin	Prohibits the device from using the address mapping to accept a call.	-
no-callout	Prohibits the device from using the address mapping to initiate a call.	-
packet-size *input-packet output-packet*	Indicates that the device negotiates the maximum packet size with the peer end when it uses the address mapping to initiate a call. The maximum packet size negotiation is a part of the flow control parameter negotiation. It involves two parameters: the maximum input packet size and maximum output packet size. **NOTE** If this parameter is not specified, the maximum input packet size and maximum output packet size on the X.25 main interface are configured using the **x25 packet-size** command. The maximum input packet size and maximum output packet size on an X.25 sub-interface are the same as these on the X.25 main interface when the X.25 sub-interface is created.	The value is an integer that ranges from 16 to 4096, in bytes. It must be an integral power of 2.
reverse-charge-accept	Allows an address mapping to accept a call with the reverse charging request.	-
reverse-charge-request	Indicates that a call originated from the address mapping carries the reverse charging request.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Meaning	Value
roa-list *roa-name*	Specifies a recognized operating agency (ROA) list name for the address mapping. The ROA list is defined by running the **x25 roa-list** command in the system view.	The value is a string of 1 to 19 characters.
send-delay *time*	Indicates that a call originated from the address mapping carries a maximum transit delay request.	The value is an integer that ranges from 0 to 65534, in milliseconds.
threshold *in out*	Indicates that the device negotiates the throughput class with the peer end when it uses the address mapping to initiate a call.	The value is an integer that can only be 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, and 48000, which are expressed in bit/s.
vc-per-map	Configures the maximum number of SVCs associated with the address mapping.	The value is an integer that ranges from 1 to 8.
window-size *input-window-size output-window-size*	Indicates that the device negotiates the window size with the peer end when it uses the address mapping to initiate a call. **NOTE** If this parameter is not specified, the input window size and output window size on the X.25 main interface are configured using the **x25 window-size** command. The input window size and output window size on an X.25 sub-interface are the same as these on the X.25 main interface when the X.25 sub-interface is created.	The value is an integer and varies with the X.25 packet sequence numbering mode (also called modulo). • When the X.25 packet sequence numbering mode is the modulo 8 mode, the value of the window size ranges from 1 to 7. • When the X.25 packet sequence numbering mode is the modulo 128 mode, the value of the window size ranges from 1 to 127.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enterprises A and B communicate through an X.25 network. The address in a data packet is an IP address. However, the X.25 network uses X.121 addresses for internal communication. Both the source host that initiates a call and the destination host of the call have IP addresses and X.121 addresses. A mapping between the IP address and X.121 address of the destination host must be configured on the X.25 interface or X.25 sub-interface of the source host. The source host can use the mapping to find the X.121 address of the destination host according to its IP address. The source host then can successfully initiate a call to the destination host.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

- Two or more address mappings with the same IP address cannot exist on the same X.25 interface.
- After an address mapping is configured, all contents of the address mapping cannot be changed, including the IP address, X.121 address, and all options. To change the contents, run the **undo x25 map** command to delete the existing address mapping first, and create an address mapping.

Example

Configure two address mappings on Serial1/0/0 and Serial2/0/0 respectively, and set different attributes for the four address mappings.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 map ip 1.1.1.1 x121-address 20112451 reverse-charge-request reverse-charge-
accept
[Huawei-Serial1/0/0] x25 map ip 1.1.1.2 x121-address 20112450 packet-size 512 512 idle-timer 10
[Huawei-Serial1/0/0] quit
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol x25
[Huawei-Serial2/0/0] x25 map ip 2.1.1.1 x121-address 25112451 window-size 4 4 broadcast
[Huawei-Serial2/0/0] x25 map ip 2.1.1.2 x121-address 25112450 no-callin
```

Related Topics

7.9.2 display x25 map

7.9.25 x25 reverse-charge-accept

7.9.12 x25 call-facility

7.9.32 x25 timer idle

7.9.37 x25 vc-per-map

7.9.18 x25 modulo

 Copyright © Huawei Technologies Co., Ltd.

7.9.18 x25 modulo

Function

The **x25 modulo** command configures the X.25 packet sequence numbering mode for an interface. The X.25 packet sequence numbering mode is also called the modulo.

The **undo x25 modulo** command restores the default X.25 packet sequence numbering mode.

By default, the modulo 8 mode is used.

Format

x25 modulo { **8** | **128** }

undo x25 modulo

Parameters

Parameter	Description	Value
8	Specifies the modulo 8 mode, which is also called the basic numbering mode.	-
128	Specifies the modulo 128 mode, which is also called the extended numbering mode.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The X.25 packet sequence numbering mode defines the numbering range of X.25 data packets. X.25 data packets are numbered from 0 to modulo minus 1. The sequence number circulates within the range. For example, if the modulo 8 mode is used, the number ranges from 0 to 7 (8 minus 1).

X.25 supports modulo 8 and modulo 128 packet sequence numbering modes. The modulo 8 mode is the default mode. To improve the communication efficiency between DTEs, you can set the X.25 packet sequence numbering mode to the

 Copyright © Huawei Technologies Co., Ltd.

modulo 128 mode if the end-to-end link rate, link quality, and X.25 network performance are high.

NOTE

The X.25 packet sequence numbering mode is different from the LAPB frame sequence numbering mode. When the modulo 128 mode is applied to a DTE/DCE interface with a high throughput rate, LAPB modulo 128 mode only improves the communication rate (point-to-point rate) between a local DTE interface and a local DCE interface, while X.25 modulo 128 mode improves the end-to-end communication rate between a local DTE and a remote DTE.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

Example

Set the X.25 packet sequence numbering mode of Serial1/0/0 to the modulo 128 mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 modulo 128
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.12 x25 call-facility

7.9.17 x25 map

7.9.20 x25 pvc

7.9.27 x25 switch pvc

7.9.41 x25 xot pvc

7.9.39 x25 window-size

7.9.19 x25 packet-size

Function

The **x25 packet-size** command configures the maximum input packet size and maximum output packet size on an X.25 interface.

The **undo x25 packet-size** command restores the default values of the maximum input and output packet sizes on an X.25 interface.

By default, both the maximum input packet size and maximum output packet size on an X.25 interface are 128 bytes.

Format

x25 packet-size *input-packet output-packet*

undo x25 packet-size

Parameters

Parameter	Description	Value
input-packet	Specifies the maximum input packet size on the X.25 interface.	The value is an integer that ranges from 16 to 4096, in bytes. It must be an integral power of 2.
output-packet	Specifies the maximum output packet size on the X.25 interface.	The value is an integer that ranges from 16 to 4096, in bytes. It must be an integral power of 2.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, an X.25 packet switched network has a maximum transmission unit (MTU) size. The size of data packets sent by a data terminal equipment (DTE) cannot exceed the MTU size. Otherwise, virtual circuits may be reset. Therefore, the sending and receiving DTE devices must support packet fragmentation and reassembly.

If the size of a data packet exceeds the MTU size, the sending DTE fragments the data packet according to the MTU size, and sets the M bit to 1 in all fragments except the last fragment. After receiving the fragments, the receiving DTE device reassembles the fragments into a data packet based on the M bit, and sends the data packet to the upper-layer protocol.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

- Consult the access service provider about the maximum input packet size. Generally, the maximum input packet size and maximum output packet size are the same. Do not set different values for the two parameters unless the network supports the setting.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.
- When an X.25 sub-interface is created, the maximum packet size configuration on the X.25 sub-interface is the same as that on the X.25 main interface. However, the maximum packet size on the X.25 sub-interface remains unchanged if the maximum packet size on the X.25 main interface is modified using the **x25 packet-size** command.
- When device functions as the data circuit-terminating equipment (DCE) in the SVC XOT scenario, the maximum input packet size and maximum output packet size on the X.25 interface of the downstream data terminal equipment (DTE) can only be negotiated to 1024 bytes at most.

Example

Set the maximum input packet size and maximum output packet size on the X.25 interface Serial1/0/0 to 256 bytes.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 packet-size 256 256
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.12 x25 call-facility
7.9.20 x25 pvc
7.9.27 x25 switch pvc
7.9.41 x25 xot pvc

7.9.20 x25 pvc

Function

The **x25 pvc** command creates a PVC.

The **undo x25 pvc** command deletes an existing PVC.

By default, no PVC is created.

Format

x25 pvc *pvc-number* **ip** *ip-address* **x121-address** *x.121-address* [*option*]

undo x25 pvc *pvc-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
pvc-number	Specifies the number of a local PVC.	The value is an integer that ranges from 1 to 4095 and must be in the range of PVC channel numbers.
ip *ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.
x.121-address	Specifies the destination X.121 address.	The value is a string of 1 to 15 characters. It can only contain digits 0 to 9.
option	Specifies attributes of the PVC. For details about the attributes, see **Table 7-51**.	-

Table 7-51 Details about the PVC attributes

Parameter	Description	Setting
broadcast	Sends broadcast data packets to the remote end of the PVC. This parameter supports some configured routing protocols such as Routing Information Protocol (RIP).	-
encapsulation-type	Specifies the data packet encapsulation format. The value can be **nonstandard**, **ietf**, **multi-protocol**, or **snap**.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Setting
packet-size *input-packet output-packet*	Specifies the maximum lengths of X.25 packets to be sent and received for the PVC. The negotiation of the maximum length of X.25 packets is a part of flow control parameter negotiation and involves parameters *input-packet* and *output-packet*. **NOTE** If this parameter is not specified, the maximum input packet size and maximum output packet size on the X.25 main interface are configured using the **x25 packet-size** command. The maximum input packet size and maximum output packet size on an X.25 sub-interface are the same as these on the X.25 main interface when the X.25 sub-interface is created.	The value is an integer that ranges from 16 to 4096, in bytes. It must be an integral power of 2.
window-size *input-window-size output-window-size*	Specifies the sizes of PVC input and output windows. **NOTE** If this parameter is not specified, the input window size and output window size on the X.25 main interface are configured using the **x25 window-size** command. The input window size and output window size on an X.25 sub-interface are the same as these on the X.25 main interface when the X.25 sub-interface is created.	The value is an integer and varies with the X.25 packet sequence numbering mode (also called modulo). • When the X.25 packet sequence numbering mode is the modulo 8 mode, the value of the window size ranges from 1 to 7. • When the X.25 packet sequence numbering mode is the modulo 128 mode, the value of the window size ranges from 1 to 127.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Similar to SVCs, data transmission through PVCs requires the mapping between the protocol address and X.121 address of the destination. However, you do not need to run the **x25 map** command to create an address mapping before configuring a PVC. One address mapping is created when you run the **x25 pvc** command to configure a PVC.

Prerequisites

1. X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.
2. The range of PVC numbers has been configured using the **x25 vc-range** command.

Example

Set the data link layer protocol to X.25 on Serial1/0/0, set the range of PVC channel numbers, and create two PVCs.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 vc-range bi-channel 8 1024
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
[Huawei-Serial1/0/0] x25 pvc 2 ip 1.1.1.1 x121-address 20112451 broadcast packet-size 512 512
[Huawei-Serial1/0/0] x25 pvc 6 ip 1.1.1.2 x121-address 20112453 broadcast window-size 5 5
```

Related Topics

7.9.38 x25 vc-range

7.9.17 x25 map

7.9.21 x25 queue-length

Function

The **x25 queue-length** command sets the length of data queues on an X.25 virtual circuit (VC).

The **undo x25 queue-length** command restores the default configuration.

By default, a data queue on an X.25 VC can contain a maximum of 200 data packets.

Format

x25 queue-length *queue-length*

undo x25 queue-length

Parameters

Parameter	Description	Value
queue-length	Specifies the data queue length on an X.25 VC.	The value ranges from 0 to 9999, indicating the number of data packets in a queue.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to adapt to different networks, you can specify the length of sending and receiving data queues for X.25 VCs on the device. By default, a data queue can contain 200 data packets. If the data traffic is high or the X.25 network has a low transmission rate, you can increase the data queue length to prevent accidental loss of data packets.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

- Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.
- The data queue length on an X.25 VC is determined when the X.25 VC is created. The **x25 queue-length** command does not affect the data queue length on a created X.25 VC.

Example

Set the VC data queue length on Serial1/0/0 to 300 data packets.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 queue-length 300
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.19 x25 packet-size

7.9.22 x25 receive-threshold

Function

The **x25 receive-threshold** command sets the value for advance packet acknowledgement.

The **undo x25 receive-threshold** command restores the default configuration.

By default, the value for advance packet acknowledgement is 0. That is, the advance packet acknowledgement function is disabled.

Format

x25 receive-threshold *count*

undo x25 receive-threshold

Parameters

Parameter	Description	Value
count	Specifies the value for advance packet acknowledgement.	The value is an integer that ranges from 1 to 127.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

According to the X.25 protocol, the receiver sends an acknowledgement packet only when the input window is full, that is, the number of received packets is the same as the value of the input window size. However, some X.25 networks have a long delay, reducing the sending and receiving efficiency. To improve the sending and receiving efficiency, you can specify a value for packet acknowledgement. When the number of received packets is the same as the specified value, the receiver sends an acknowledgement packet to the peer end. This value is called the receive-threshold. It ranges from 0 to the value of the input window size. If the value is set to 1, the receiver sends an acknowledgement for each received data packet. If the value is set to the value of the input window size, the receiver sends an acknowledgement packet after the input window is full. This function is important to applications with a high requirement on the response speed.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

Example

Set the value for advance packet acknowledgement on Serial1/0/0 to 2.

```
<Huawei> system-view
[Huawei]interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 receive-threshold 2
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.39 x25 window-size

7.9.23 x25 response called-address

Function

The **x25 response called-address** command configures an X.25 interface to send a Call Accepted packet with the called DTE address.

The **undo x25 response called-address** command restores the default configuration.

By default, the Call Accepted packet sent by an X.25 interface does not contain the called DTE address.

Format

x25 response called-address

undo x25 response called-address

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different X.25 networks have different requirements on whether the Call Accepted packet contains the calling DTE address and called DTE address. Some X.25

networks require that the Call Accepted packet should contain both addresses, some require one of the two addresses, and some require neither of the two addresses in the Call Accepted packet. You can configure the Call Accepted packet based on actual network requirements to adapt to differences between networks.

You can run the **x25 response called-address** command to configure an X.25 interface to send a Call Accepted packet with the called DTE address.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Configure Serial1/0/0 to send a Call Accepted packet that contains the called DTE address.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 response called-address
```

Related Topics

7.9.24 x25 response calling-address

7.9.15 x25 ignore called-address

7.9.16 x25 ignore calling-address

7.9.24 x25 response calling-address

Function

The **x25 response calling-address** command configures an X.25 interface to send a Call Accepted packet with the calling DTE address.

The **undo x25 response calling-address** command restores the default configuration.

By default, the Call Accepted packet sent by an X.25 interface does not contain the calling DTE address.

Format

x25 response calling-address

undo x25 response calling-address

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different X.25 networks have different requirements on whether the Call Accepted packet contains the calling DTE address and called DTE address. Some X.25 networks require that the Call Accepted packet should contain both addresses, some require one of the two addresses, and some require neither of the two addresses in the Call Accepted packet. You can configure the Call Accepted packet based on actual network requirements to adapt to differences between networks.

You can run the **x25 response calling-address** command to configure an X.25 interface to send a Call Accepted packet with the calling DTE address.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Configure Serial1/0/0 to send a Call Accepted packet that contains the calling DTE address.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 response calling-address
```

Related Topics

7.9.23 x25 response called-address

7.9.15 x25 ignore called-address

7.9.16 x25 ignore calling-address

7.9.25 x25 reverse-charge-accept

Function

The **x25 reverse-charge-accept** command allows an X.25 interface to accept a call with the reverse charging request.

The **undo x25 reverse-charge-accept** command prohibits an X.25 interface from accepting a call with the reverse charging request.

By default, an X.25 interface cannot accept a call with the reverse charging request.

Format

x25 reverse-charge-accept

undo x25 reverse-charge-accept

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an X.25 interface cannot accept a call with the reverse charging request. If you run the **x25 reverse-charge-accept** command to allow an X.25 interface to accept a call with the reverse charging request, the X.25 interface accepts all calls with the reverse charging request.

If you allow an address mapping to accept a call with the reverse charging request by specifying the **reverse-charge-accept** option in the **x25 map** command, the X.25 interface only accepts calls with the reverse charging request that aim at the address mapping, but rejects other calls with the reverse charging request that do not aim at the address mapping.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Configure Serial1/0/0 to accept a call with the reverse charging request.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 reverse-charge-accept
```

Related Topics

7.9.17 x25 map

7.9.26 x25 roa-list

Function

The **x25 roa-list** command defines the ROA list.

The **undo x25 roa-list** deletes ROAs from the ROA list.

By default, no ROA list is defined.

 Copyright © Huawei Technologies Co., Ltd.

Format

x25 roa-list *roa-name roa-id* &<1-10>

undo x25 roa-list *roa-name*

Parameters

Parameter	Description	Value
roa-name	Specifies the name of an ROA.	The value is a string of 1 to 19 characters.
roa-id	Specifies the ID associated with the ROA.	The value is an integer that ranges from 0 to 9999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An ROA list can contain multiple ROAs, and multiple IDs can be specified for each ROA. After an ROA list is defined, you can run the **x25 call-facility** or **x25 map** command to reference ROAs in the list based on ROA names.

Example

Define an ROA list, and reference ROAs in the list on Serial1/0/0.

```
<Huawei> system-view
[Huawei] x25 roa-list list1 11 23 45
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 call-facility roa-list list1
```

Related Topics

7.9.12 x25 call-facility

7.9.17 x25 map

7.9.27 x25 switch pvc

Function

The **x25 switch pvc** command configures an X.25 PVC route.

The **undo x25 switch pvc** command deletes the X.25 PVC route of a specified PVC.

By default, no X.25 PVC route is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

x25 switch pvc *pvc-number1* **interface serial** *number* **pvc** *pvc-number2* [*option*]

undo x25 switch pvc *pvc-number1*

Parameters

Parameter	Description	Value
pvc-number1	Specifies the PVC number on the input interface.	The value is an integer that ranges from 1 to 4095 and must be in the range of PVC channel numbers.
pvc-number2	Specifies the PVC number on the output interface.	The value is an integer that ranges from 1 to 4095 and must be in the range of PVC channel numbers.
interface serial *number*	Specifies the type and number of the output interface.	-
option	Specifies attributes of the PVC. For details about the attributes, see **Table 7-52**.	-

Table 7-52 Details about the PVC attributes

Parameter	Description	Setting
packet-size *input-packet output-packet*	Specifies the maximum lengths of X.25 packets to be sent and received for the PVC. The negotiation of the maximum length of X.25 packets is a part of flow control parameter negotiation and involves parameters *input-packet* and *output-packet*. **NOTE** If the parameter **packet-size** is not specified, run the **x25 packet-size** command to set the maximum lengths of X.25 packets to be sent and received on an X.25 interface.	The value is an integer that ranges from 16 to 4096, in bytes. It must be an integral power of 2.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Setting
window-size *input-window-size output-window-size*	Specifies the sizes of PVC input and output windows. **NOTE** If this parameter is not specified, the sizes of the input and output windows configured using the **x25 window-size** command on an X.25 interface is used.	The value is an integer and varies with the X.25 packet sequence numbering mode (also called modulo). • When the X.25 packet sequence numbering mode is the modulo 8 mode, the value of the window size ranges from 1 to 7. • When the X.25 packet sequence numbering mode is the modulo 128 mode, the value of the window size ranges from 1 to 127.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an X.25 PVC route having its forwarding interface specified is configured, the device forwards X.25 packets transmitted through the PVC on the local interface to the PVC on the specified interface. In this way, the device can address and forward X.25 data transmitted through PVCs.

Prerequisites

1. X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.
2. The range of PVC numbers has been configured using the **x25 vc-range** command.

Example

Configure a route between PVC 1 on Serial1/0/0 and PVC 2 on Serial2/0/0 for X.25 packet switching.

```
<Huawei>system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25 dce
```

```
[Huawei-Serial1/0/0] x25 vc-range bi-channel 8 1024
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
[Huawei-Serial1/0/0] x25 switch pvc 1 interface serial 2/0/0 pvc 2
[Huawei-Serial1/0/0] quit
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] link-protocol x25 dce
[Huawei-Serial2/0/0] x25 vc-range bi-channel 8 1024
[Huawei-Serial2/0/0] shutdown
[Huawei-Serial2/0/0] undo shutdown
[Huawei-Serial2/0/0] x25 switch pvc 2 interface serial 1/0/0 pvc 1
```

Related Topics

7.9.5 display x25 vc
7.9.30 x25 switching
7.9.18 x25 modulo

7.9.28 x25 switch svc

Function

The **x25 switch svc** command configures an X.25 SVC route.

The **undo x25 switch svc** command deletes a specified X.25 SVC route.

By default, no X.25 SVC route is configured.

Format

x25 switch svc [*-number*] *x.121-address* **interface** *interface-type interface-number*

undo x25 switch svc *x.121-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
-number	Specifies the number of an X.25 SVC route.	The value of *number* is an integer that ranges from 1 to 4096.
x.121-address	Specifies the destination X.121 address.	The value is a string of 1 to 15 mode matching characters. For details about mode matching, see **Table 7-53** and **Table 7-54**.
interface *interface-type interface-number*	Specifies the type and number of the forwarding interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Table 7-53 X.121 mode matching rule

Wildcard	Matching Rule	Example	Matching String of Characters
*	Matching zero or more characters before the wildcard	fo*	fo, foo, or fooo
+	Matching zero or more characters before the wildcard	fo+	fo, foo, or fooo
^	Matching the start of the input string	^hell	hell, hello, or hellaaa
$	Matching the end of the input string	ar$	ar, car, or hear
\char	Matching the single character specified by char	b\+	b+
.	Matching any single character	l.st	last, lbst, or lost
.*	Matching any zero or more characters	fo.*	fo, foo, or fot
.+	Matching any one or more characters	fo.+	foo, fot, or foot

Table 7-54 Input rules of X.121 address mode matching string of characters

Character	Input Rule
*	It cannot be at the beginning of a string of characters, after ^, or before and after + or *.
+	It cannot be at the beginning of a string of characters, after ^, or before and after + or *.
\	It cannot be at the end of a string of characters.
^	It cannot be before + or *.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an X.25 SVC route whose destination address is the X.121 address and whose forwarding interface is specified, the device forwards the received X.25 packets

whose destination addresses are the specified X.121 address to the specified interface. In this way, the device can address and forward X.25 data transmitted through SVCs.

Example

Add an X.25 SVC route with the destination address as 8888 and forwarding interface as Serial1/0/0.

```
<Huawei> system-view
[Huawei] x25 switch svc 8888 interface serial 1/0/0
```

Related Topics

7.9.4 display x25 switch-table svc

7.9.29 x25 switch svc xot

Function

The **x25 switch svc xot** command configures an SVC XOT route.

The **undo x25 switch svc xot** command deletes a specified SVC XOT route.

By default, no SVC XOT route is configured.

Format

x25 switch svc [*-number*] *x.121-address* **xot** *ip-address* [*xot-option*]

undo x25 switch svc *x.121-address* [**xot** *ip-address*]

Parameters

Parameter	Description	Value
-number	Specifies the number of an X.25 SVC route.	The value of *number* is an integer that ranges from 1 to 4096.
x.121-address	Specifies the destination X.121 address.	The value is a string of 1 to 15 mode matching characters. For details about mode matching, see **Table 7-55** and **Table 7-56**.
ip-address	Specifies the remote IP address of the XOT connection.	The value is in dotted decimal notation.
xot-option	Specifies XOT connection parameter options. For details, see **Table 7-57**.	-

 Copyright © Huawei Technologies Co., Ltd.

Table 7-55 X.121 mode matching rule

Wildcard	Matching Rule	Example	Matching String of Characters
*	Matching zero or more characters before the wildcard	fo*	fo, foo, or fooo
+	Matching zero or more characters before the wildcard	fo+	fo, foo, or fooo
^	Matching the start of the input string	^hell	hell, hello, or hellaaa
$	Matching the end of the input string	ar$	ar, car, or hear
\char	Matching the single character specified by char	b\+	b+
.	Matching any single character	l.st	last, lbst, or lost
.*	Matching any zero or more characters	fo.*	fo, foo, or fot
.+	Matching any one or more characters	fo.+	foo, fot, or foot

Table 7-56 Input rules of X.121 address mode matching string of characters

Character	Input Rule
*	It cannot be at the beginning of a string of characters, after ^, or before and after + or *.
+	It cannot be at the beginning of a string of characters, after ^, or before and after + or *.
\	It cannot be at the end of a string of characters.
^	It cannot be before + or *.

Table 7-57 XOT connection parameter options

Option	Description	Setting
timer *seconds*	Specifies the keepalive timer of the XOT connection. When the timer expires, the device sends keepalive packets to detect availability of the XOT connection.	The value is an integer that ranges from 1 to 3600, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Option	Description	Setting
retry *times*	Specifies the maximum number of failures to send a keepalive packet. When the number of failures to send a keepalive packet exceeds the *times* value, the XOT connection is torn down.	The value is an integer that ranges from 3 to 3600.
source *interface-type interface-number*	Specifies the type and number of the interface that initiates the XOT connection.	-
vpn-instance *vpn-instance-name* **NOTE** Only V200R010C10 and later versions support this parameter.	Specifies the name of the VPN instance to which the XOT connection is bound.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An SVC XOT route determines how a device forwards received X.25 packets through an IP network. After an SVC XOT route is configured, the local X.25 network can communicate with the remote X.25 network through SVCs across an IP network.

Example

Forward X.25 data of SVC 1 to the remote interface with IP address 10.1.1.1 across the IP network.

```
<Huawei> system-view
[Huawei] x25 switch svc 1 xot 10.1.1.1
```

Related Topics

7.9.4 display x25 switch-table svc

7.9.30 x25 switching

7.9.30 x25 switching

Function

The **x25 switching** command enables X.25 switching.

The **undo x25 switching** command disables X.25 switching.

By default, X.25 switching is disabled.

Format

x25 switching

undo x25 switching

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When X.25 switching is enabled, the device can receive X.25 packets on an X.25 interface and forwards the X.25 packet through another interface based on the destination address information in the X.25 packets. Only after X.25 switching is enabled, configurations of X.25 routes can take effect.

Precautions

Enabling or disabling X.25 switching only affects call establishment, but does not affect established links.

If X.25 switching is enabled and various X.25 routes are configured, you can run the **undo x25 switching** command to disable X.25 switching. If you run the **display current-configuration** command to view configurations of X.25 routes, the command output contains different configuration in the following situations:

- If SVC routes are configured, the **display current-configuration** command output does not contain SVC route configuration.
- If PVC routes are configured, the **display current-configuration** command output contains PVC route configuration.
- If you do not restart the device and run the **x25 switching** command to enable X.25 switching again, the **display current-configuration** command output contains SVC route configuration.

 Copyright © Huawei Technologies Co., Ltd.

- If you restart the device, the configurations of SVC and PVC routes are lost.

Example

Enable X.25 switching.

```
<Huawei> system-view
[Huawei] x25 switching
```

Related Topics

7.9.20 x25 pvc

7.9.27 x25 switch pvc

7.9.41 x25 xot pvc

7.9.5 display x25 vc

7.9.4 display x25 switch-table svc

7.9.31 x25 timer hold

Function

The **x25 timer hold** command configures the device not to resend a call request to a destination within a specified delay if the device fails to establish a call to the destination.

The **undo x25 timer hold** command restores the default setting.

The default delay is 0; that is, the function is disabled.

Format

x25 timer hold *minutes*

undo x25 timer hold

Parameters

Parameter	Description	Value
minutes	Specifies the delay.	The value is an integer that ranges from 0 to 1000, in minutes.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device frequently sends call requests to a destination that does not exist or is faulty, working efficiency of the device is lowered. You can run the **x25 timer hold** command to configure an X.25-enabled device to delay sending a call request within a specified period of time to the destination with which the device failed to establish a call.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

This function takes effect only on outgoing calls.

Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

Example

Configure Serial1/0/0 to delay sending a call request within 5 minutes to the destination with which Serial1/0/ failed to establish a call.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 timer hold 5
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

7.9.32 x25 timer idle

Function

The **x25 timer idle** command sets the maximum idle time for switched virtual circuits (SVCs) on an interface.

The **undo x25 timer idle** command restores the default value of the maximum idle time for SVCs on an interface.

By default, the maximum idle time for SVCs on an interface is 0 minutes. An SVC is always connected even if no data is transmitted over it.

Format

x25 timer idle *minutes*

undo x25 timer idle

Parameters

Parameter	Description	Value
minutes	Specifies the maximum idle time of SVCs.	The value is an integer that ranges from 0 to 255, in minutes.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an SVC is always connected even when no data packet is transmitted over it. This wastes network resources and increases expenses. You can set a maximum SVC idle time. An SVC is in the idle state when no data packet is transmitted over it. When some SVCs are in the idle state for a time longer than the maximum idle time, X.25 automatically disconnects these SVCs, saving unnecessary expenses for users. These SVCs are set up again when data packets need to be transmitted.

You can specify the maximum idle time for an SVC using the following methods:

- Run the **x25 timer idle** command to set the maximum idle time for SVCs based on an X.25 interface.
- Run the **x25 map** command to set the maximum idle time for SVCs based on an address mapping.

The X.25 interface-based configuration is effective for every call originated from the X.25 interface. The address mapping-based configuration is effective only for calls originated from the address mapping. If both X.25 interface-based configuration and address mapping-based configuration are configured, the address mapping-based configuration has a higher priority.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface.

Precautions

Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

Example

Set the maximum idle time for SVCs on Serial1/0/0 to 10 minutes.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 timer idle 10
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.17 x25 map

7.9.33 x25 timer tx0

Function

The **x25 timer tx0** command configures the DTE T20 Restart Request timer or DCE T10 Restart Indication timer.

The **undo x25 timer tx0** command restores the default configuration.

By default, the values of the DTE T20 Restart Request timer and DCE T10 Restart Indication timer are 180s and 60s respectively.

Format

x25 timer tx0 *seconds*

undo x25 timer tx0

Parameters

Parameter	Description	Value
seconds	Specifies the value of the restart timer.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The restart procedure deletes all switched virtual circuits (SVCs) and resets all permanent virtual circuits (PVCs) between a DTE interface and a DCE interface. It is often used when network faults occur.

There are two types of restart timers: T10 and T20 timers. As specified in X.25, the local DTE sends a Restart Request packet to the local DCE and starts the T20 timer. The local DCE sends a Restart Indication packet to the local DTE and starts the T10 timer. If no response is received from the peer end after the timer expires, the sender takes measures to ensure the normal operation of the local procedure.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the restart timer on Serial1/0/0 to 120s.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 timer tx0 120
```

Related Topics

7.9.34 x25 timer tx1
7.9.35 x25 timer tx2
7.9.36 x25 timer tx3

7.9.34 x25 timer tx1

Function

The **x25 timer tx1** command configures the DTE T21 Call Request timer or DCE T11 Incoming Call timer.

The **undo x25 timer tx1** command restores the default configuration.

By default, the values of the DTE T21 Call Request timer and DCE T11 Incoming Call timer are 200s and 180s respectively.

Format

x25 timer tx1 *seconds*

undo x25 timer tx1

Parameters

Parameter	Description	Value
seconds	Specifies the value of the call timer.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As specified in X.25, there are two timers in the call setup phase.

- The calling DTE starts the T21 timer after sending a Call Request packet. If no response (Call Connected or Clear Indication packet) is received from the local

DCE after the timer expires, the calling DTE sends a Clear Request packet to set logical channels to the Ready state.

- The remote DCE starts the T11 timer after sending an Incoming Call packet. After receiving the Incoming Call packet, the called DTE responds with a Call Accepted or Clear Request packet within 90s. If the called DTE does not respond, the remote DCE sends a Clear Indication packet to both the calling DTE and called DTE after the T11 timer expires.

If no response is received from the peer end after the timer expires, the sender takes measures to ensure the normal operation of the local procedure.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Set the value of the call timer on Serial1/0/0 to 100s.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 timer tx1 100
```

Related Topics

7.9.33 x25 timer tx0

7.9.35 x25 timer tx2

7.9.36 x25 timer tx3

7.9.35 x25 timer tx2

Function

The **x25 timer tx2** command configures the DTE T22 Reset Request timer or DCE T12 Reset Indication timer.

The **undo x25 timer tx2** command restores the default configuration.

By default, the values of the DTE T22 Reset Request timer and DCE T12 Reset Indication timer are 180s and 60s respectively.

Format

x25 timer tx2 *seconds*

undo x25 timer tx2

Parameters

Parameter	Description	Value
seconds	Specifies the value of the reset timer.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Call Request packet is used to restore a call or permanent virtual circuit (PVC) to the original state.

As specified in X.25, the local DTE sends a Reset Request packet to the local DCE and starts the T22 timer. When the Reset Request packet is sent to the remote DCE over an X.25 network, the remote DCE sends a Reset Indication packet to the remote DTE and starts the T12 timer. If no response is received from the peer end after the timer expires, the sender takes measures to ensure the normal operation of the local procedure.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Set the value of the reset timer on Serial1/0/0 to 120s.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 timer tx2 120
```

Related Topics

7.9.33 x25 timer tx0

7.9.34 x25 timer tx1

7.9.36 x25 timer tx3

7.9.36 x25 timer tx3

Function

The **x25 timer tx3** command configures the DTE T23 Clear Request timer or DCE T13 Clear Indication timer.

The **undo x25 timer tx3** command restores the default configuration.

By default, the values of the DTE T23 Clear Request timer and DCE T13 Clear Indication timer are 180s and 60s respectively.

 Copyright © Huawei Technologies Co., Ltd.

Format

x25 timer tx3 *seconds*

undo x25 timer tx3

Parameters

Parameter	Description	Value
seconds	Specifies the value of the clear timer.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The call clearing procedure clears all network information related to a call and releases all network resources. The logical channel for the call on an X.25 interface returns to the Ready state.

As specified in X.25, the calling DTE starts the T23 timer after sending a Clear Request packet. The remote DCE starts the T13 timer after sending a Call Indication packet to the called DTE. If no response is received from the peer end after the timer expires, the sender takes measures to ensure the normal operation of the local procedure.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Example

Set the value of the clear timer on Serial1/0/0 to 100s.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 timer tx3 100
```

Related Topics

7.9.33 x25 timer tx0

7.9.34 x25 timer tx1

7.9.35 x25 timer tx2

 Copyright © Huawei Technologies Co., Ltd.

7.9.37 x25 vc-per-map

Function

The **x25 vc-per-map** command configures the maximum number of SVCs associated with an address mapping on an X.25 interface.

The **undo x25 vc-per-map** command restores the default configuration.

By default, one address mapping can only be associated with one SVC.

Format

x25 vc-per-map *count*

undo x25 vc-per-map

Parameters

Parameter	Description	Value
count	Specifies the maximum number of SVCs associated with an address mapping on the X.25 interface.	The value is an integer that ranges from 1 to 8.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, one address mapping can only be associated with one SVC. If a large amount of data needs to be transmitted but the SVC transmission rate is low, you can associate the address mapping with more SVCs to reduce data loss.

You can modify the maximum number of SVCs associated with an address mapping using the following methods:

- Run the **x25 vc-per-map** command to configure the maximum number of SVCs associated with an address mapping based on an X.25 interface.
- Run the **x25 map** command to configure the maximum number of SVCs associated with an address mapping based on an address mapping.

The X.25 interface-based configuration is effective for every call originated from the X.25 interface. The address mapping-based configuration is effective only for calls originated from the address mapping. If both X.25 interface-based configuration and address mapping-based configuration are configured, the address mapping-based configuration has a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

Example

Set the maximum number of SVCs associated with an address mapping on Serial1/0/0 to 3.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 vc-per-map 3
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.17 x25 map

7.9.38 x25 vc-range

Function

The **x25 vc-range** command sets the lower and upper thresholds of an X.25 VC range.

The **undo x25 vc-range** command restores the default configuration.

The default configuration is as follows:

- Both the lower and upper thresholds of the incoming-only channel range are 0.
- The lower and upper thresholds of the two-way channel range are 1 and 1024 respectively.
- Both the lower and upper thresholds of the outgoing-only channel range are 0.

Format

x25 vc-range [**in-channel** *lic hic*] [**bi-channel** *ltc htc*] [**out-channel** *loc hoc*]

undo x25 vc-range

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
in-channel *lic hic*	Specifies the lower and upper thresholds of the incoming-only channel range.	The value is an integer that ranges from 0 to 4095. **NOTE** If *hic* (the upper threshold of the incoming-only channel range) is set to 0, *lic* (the lower threshold of the incoming-only channel range) must also be set to 0, indicating that the incoming-only channel range cannot be used.
bi-channel *ltc htc*	Specifies the lower and upper thresholds of the two-way channel range.	The value is an integer that ranges from 0 to 4095. **NOTE** If *htc* (the upper threshold of the two-way channel range) is set to 0, *ltc* (the lower threshold of the two-way channel range) must also be set to 0, indicating that the two-way channel range cannot be used.
out-channel *loc hoc*	Specifies the lower and upper thresholds of the outgoing-only channel range.	The value is an integer that ranges from 0 to 4095. **NOTE** If *hoc* (the upper threshold of the outgoing-only channel range) is set to 0, *loc* (the lower threshold of the outgoing-only channel range) must also be set to 0, indicating that the outgoing-only channel range cannot be used.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

- By default, the device prohibits the use of the incoming-only channel range and outgoing-only channel range, and permits the use of the two-way channel range (1 to 1024). The VC range must be correctly configured based on requirements of the access service provider.
- The *lic*, *hic*, *ltc*, *htc*, *loc*, and *hoc* parameter settings must be the same on both sides of a physical connection between a DTE and a DCE. Otherwise, X.25 procedures may be interrupted, causing data transmission failures.
- The preceding parameters must meet the following requirement: 1 ≤ *lic* ≤ *hic* < *ltc* ≤ *htc* < *loc* ≤ *hoc* < 4095. If the requirement is not met, the device displays an error message.
- If either threshold of a range is 0, the other threshold must be 0. A range cannot be used when its upper and lower thresholds are both 0.
- Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

NOTE

The lower threshold of the permanent virtual circuit (PVC) channel range is 1. The upper threshold of the PVC channel range is determined by the nearest channel range that is not prohibited. If the lower threshold of the nearest channel range is X, the upper threshold of the PVC channel range is X minus 1. If the lower threshold of the nearest channel range is 1, the PVC channel range cannot be used. By default, the incoming-only and outgoing-only channel ranges cannot be used. The number of two-way channels ranges from 1 to 1024. (The *ltc* and *htc* parameters are set to 1 and 1024 respectively.) Therefore, the PVC channel range cannot be used by default. PVCs cannot be configured. Before configuring a PVC or an X.25 PVC route, you must configure a proper PVC channel range.

Table 7-58 lists the PVC channel ranges in several typical configuration scenarios.

Table 7-58 PVC channel ranges in several typical configuration scenarios

No.	Incoming-only Channel Range	Two-way Channel Range	Outgoing-only Channel Range	PVC Channel Range
1	[0, 0]	[1, 1024]	[0, 0]	Prohibited
2	[0, 0]	[10, 24]	[0, 0]	[1, 9]
3	[1, 10]	[15, 30]	[0, 0]	Prohibited
4	[5, 10]	[15, 25]	[30, 32]	[1, 4]
5	[0, 0]	[0, 0]	[20, 45]	[1, 19]
6	[0, 0]	[0, 0]	[0, 0]	[1, 4095]

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure X.25 as the data link layer protocol of Serial 1/0/0, permit the use of the incoming-only and two-way channel ranges, and prohibit the use of the outgoing-only channel range. The lower and upper thresholds of the three channel ranges are 1 and 7, 8 and 1024, and 0 and 0 respectively.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 vc-range in-channel 1 7 bi-channel 8 1024
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.5 display x25 vc

7.9.39 x25 window-size

Function

The **x25 window-size** command configures the input window size and output window size of an X.25 interface.

The **undo x25 window-size** command restores the default configuration.

By default, both the input window size and output window size of an X.25 interface are 2.

Format

x25 window-size *input-window-size output-window-size*

undo x25 window-size

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
input-window-size	Specifies the input window size of an X.25 interface.	The value is an integer and varies with the X.25 packet sequence numbering mode (also called modulo). ● When the X.25 packet sequence numbering mode is the modulo 8 mode, the value of the input window size ranges from 1 to 7. ● When the X.25 packet sequence numbering mode is the modulo 128 mode, the value of the input window size ranges from 1 to 127.
output-window-size	Specifies the output window size of an X.25 interface.	The value is an integer and varies with the X.25 packet sequence numbering mode (also called modulo). ● When the X.25 packet sequence numbering mode is the modulo 8 mode, the value of the output window size ranges from 1 to 7. ● When the X.25 packet sequence numbering mode is the modulo 128 mode, the value of the output window size ranges from 1 to 127.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The input window size and output window size of an X.25 interface have the following functions:

- The input window size of an X.25 interface determines the maximum number of correct data packets that can be received by the X.25 interface before it sends the acknowledgement information. When the bandwidth is high, a larger window size indicates a higher transmission rate.
- The output window size of an X.25 interface determines the maximum number of data packets that can be sent by the X.25 interface before it receives correct acknowledgement information. When the bandwidth is high, a larger window size indicates a higher transmission rate.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

- Consult the access service provider about the input window size and output window size of an X.25 interface. Generally, the input window size and output window size of an X.25 interface are the same. Do not set different values for the two parameters unless the network supports the setting.
- Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.
- When an X.25 sub-interface is created, the window size configuration on the X.25 sub-interface is the same as that on the X.25 main interface. However, the window size on the X.25 sub-interface remains unchanged if the window size on the X.25 main interface is modified using the **x25 window-size** command.

Example

Set both the input window size and output window size of Serial1/0/0 to 5.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 window-size 5 5
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

Related Topics

7.9.17 x25 map

7.9.20 x25 pvc

7.9.27 x25 switch pvc

7.9.41 x25 xot pvc

7.9.22 x25 receive-threshold

 Copyright © Huawei Technologies Co., Ltd.

7.9.40 x25 x121-address

Function

The **x25 x121-address** command configures an X.121 address for an X.25 interface.

The **undo x25 x121-address** command deletes an X.121 address.

By default, no X.121 address is configured for an X.25 interface.

Format

x25 x121-address *x.121-address*

undo x25 x121-address

Parameters

Parameter	Description	Value
x.121-address	Specifies the X.121 address of the X.25 interface.	An X.121 address is a string of 1 to 15 characters. It can only contain digits 0 to 9.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring an X.121 address for an X.25 interface, use different configuration methods in different scenarios.

- If a device connects to an X.25 public packet network, the access service provider must assign a valid X.121 address to the device.
- If two devices are directly connected in back-to-back mode, you can randomly specify valid X.121 addresses for the devices.
- If a device works in switching mode, an X.121 address is not necessary.

Prerequisites

X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- If you run the **x25 x121-address** command multiple times in the same X.25 interface view, only the latest configuration takes effect.
- Run the **shutdown** and **undo shutdown** commands or run the **restart** command to restart the physical interface to make the configuration take effect.

NOTE

For the X.121 address format and dynamic conversion between the IP address and X.121 address, see *ITU-T Recommendation X.121* and related RFCs.

Example

Set the data link layer protocol of Serial1/0/0 to X.25 and X.121 address to 20112451.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol x25
[Huawei-Serial1/0/0] x25 x121-address 20112451
[Huawei-Serial1/0/0] shutdown
[Huawei-Serial1/0/0] undo shutdown
```

7.9.41 x25 xot pvc

Function

The **x25 xot pvc** command adds a PVC XOT route.

The **undo x25 pvc** command deletes the specified PVC XOT route.

By default, no PVC XOT route is configured.

Format

x25 xot pvc *pvc-number1 ip-address* **interface serial** *interface-number* **pvc** *pvc-number2* [*xot-option*]

undo x25 pvc *pvc-number1*

Parameters

Parameter	Description	Value
pvc-number1	Specifies the PVC number on the local interface.	The value is an integer that ranges from 1 to 4095 and must be in the range of PVC channel numbers.
ip-address	Specifies the remote IP address of the XOT link.	The value is in dotted decimal notation.
interface serial *interface-number*	Specifies the type and number of the remote interface.	-

Parameter	Description	Value
pvc-number2	Specifies the PVC number on the remote interface.	The value is an integer that ranges from 1 to 4095 and must be in the range of PVC channel numbers.
xot-option	Specifies an XOT channel parameter option. For details, see **Table 7-59**.	-

Table 7-59 XOT channel parameter options

Option	Description	Value
packet-size *input-packet output-packet*	Specifies the maximum lengths of X.25 packets to be sent and received for the PVC. The negotiation of the maximum length of X.25 packets is a part of flow control parameter negotiation and involves parameters *input-packet* and *output-packet*. **NOTE** If the parameter **packet-size** is not specified, run the **x25 packet-size** command to set the maximum lengths of X.25 packets to be sent and received on an X.25 interface.	The value is an integer that ranges from 16 to 4096, in bytes. It must be an integral power of 2.
window-size *input-window-size output-window-size*	Specifies the sizes of PVC input and output windows. **NOTE** If this parameter is not specified, the sizes of the input and output windows configured using the **x25 window-size** command on an X.25 interface is used.	The value is an integer and varies with the X.25 packet sequence numbering mode (also called modulo). • When the X.25 packet sequence numbering mode is the modulo 8 mode, the value of the window size ranges from 1 to 7. • When the X.25 packet sequence numbering mode is the modulo 128 mode, the value of the window size ranges from 1 to 127.

 Copyright © Huawei Technologies Co., Ltd.

Option	Description	Value
timer *seconds*	Specifies the keepalive timer of the XOT connection. When the timer expires, the device sends keepalive packets to detect availability of the XOT connection.	The value is an integer that ranges from 1 to 3600, in seconds.
retry *times*	Specifies the maximum number of failures to send a keepalive packet. When the number of failures to send a keepalive packet exceeds the *times* value, the XOT connection is torn down.	The value is an integer that ranges from 3 to 3600.
source *interface-type interface-number*	Specifies the type and number of the interface that initiates the XOT connection.	-
vpn-instance *vpn-instance-name* **NOTE** Only V200R010C10 and later versions support this parameter.	Specifies the name of the VPN instance to which the XOT connection is bound.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PVC XOT route determines how a device forwards received X.25 packets through an IP network. After a PVC XOT route is configured, the local X.25 network can communicate with the remote X.25 network through PVCs across an IP network.

Prerequisites

1. X.25 has been configured as the data link layer protocol of the interface using the **link-protocol x25** command.

2. The range of PVC numbers has been configured using the **x25 vc-range** command.

Precautions

In the PVC XOT scenario, the device functions as the data circuit-terminating equipment (DCE) and communicates with non-Huawei devices through an IP network. To modify the X.25 packet sequence numbering mode (also called modulo) on the X.25 interface, you must delete the PVC XOT route first and reconfigure the PVC XOT route. Traffic can then be successfully forwarded.

Example

When the range of X.25 VC numbers is configured, configure a route between PVC 1 of local interface Serial1/0/0 and PVC 2 of remote interface Serial2/0/0 across the IP network for X.25 packet switching.

Configuration on the local device is as follows:

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ip address 10.1.1.1 255.255.255.0
[Huawei-Serial1/0/0] link-protocol x25 dce ietf
[Huawei-Serial1/0/0] x25 vc-range in-channel 10 20 bi-channel 30 1024
[Huawei-Serial1/0/0] x25 xot pvc 1 10.1.1.2 interface serial 2/0/0 pvc 2
```

Configuration on the remote device is as follows:

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] ip address 10.1.1.2 255.255.255.0
[Huawei-Serial1/0/0] link-protocol x25 dce ietf
[Huawei-Serial1/0/0] x25 vc-range in-channel 10 20 bi-channel 30 1024
[Huawei-Serial1/0/0] x25 xot pvc 2 10.1.1.1 interface serial 1/0/0 pvc 1
```

Related Topics

7.9.5 display x25 vc
7.9.30 x25 switching

7.10 IP-Trunk Commands

NOTE

The 1STM1, 1STM4, and 4STM1 interface cards support POS interfaces. For the mapping between the device and interface card, see 1STM1 (1-Port 155M Packet over SDH/SONET Optical Interface Card), 1STM4 (1-Port 622M Packet over SDH/SONET Optical Interface Card) or 4STM1 (4-Port 155M Packet over SDH/SONET Optical Interface Card) in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Cards-POS/CPOS Card*.

7.10.1 display interface ip-trunk

Function

The **display interface ip-trunk** command displays the status of an IP-Trunk interface.

Format

display interface ip-trunk [*trunk-id* | **main**]

Parameters

Parameter	Description	Value
trunk-id	Displays the status of an IP-Trunk interface.	The value is an integer and varies according to device model, the value depend on the device.
main	Displays status and traffic statistics about an IP-Trunk interface. An IP-Trunk interface has no sub-interfaces. Status and traffic statistics about an IP-Trunk interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the interface status or locate faults on an interface, run the **display interface ip-trunk** command to view the status of the interface.

Example

Display the status of IP-Trunk 1.

```
<Huawei> display interface ip-trunk 1
Ip-Trunk1 current state : UP
Line protocol current state : UP
Last line protocol up time : 2013-09-17 21:42:47
Description:HUAWEI, AR Series, Ip-Trunk1 Interface
Route Port,Hash arithmetic : According to SIP-XOR-DIP,Maximal BW: 155M, Current
BW: 155M, The Maximum Transmit Unit is 1500
```

```
Internet Address is 1.1.1.1/24  Link layer protocol is nonstandard HDLC
Physical is IP_TRUNK
Current system time: 2013-09-18 10:09:08
    Last 10 seconds input rate 160 bits/sec, 0 packets/sec
    Last 10 seconds output rate 160 bits/sec, 0 packets/sec
    Realtime 0 seconds input rate 0 bits/sec, 0 packets/sec
    Realtime 0 seconds output rate 0 bits/sec, 0 packets/sec
    Input: 199810 packets,23190749 bytes
           2 errors,2 drops
    Output:990962 packets,92902320 bytes
           0 drops
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
-----------------------------------------------------
PortName                    Status      Weight
-----------------------------------------------------
Pos2/0/0                    UP          1
-----------------------------------------------------
The Number of Ports in Trunk : 1
The Number of UP Ports in Trunk : 1
```

Table 7-60 Description of the display interface ip-trunk command output

Item	Description
IP-Trunk1 current state	Status of the IP-Trunk1 interface ● UP: The physical layer of the interface is in the Up state. ● DOWN: The physical layer of the interface is in the Down state. ● Administratively DOWN: The administrator uses the **shutdown** command on the interface.
Line protocol current state	Link status of the interface ● UP: The link-layer protocol of the interface is in the Up state. ● DOWN: The link-layer protocol of the interface is in the Down state.
Last line protocol up time	Last time when the interface link protocol is Up.
Description	Description of the interface The value can be configured using the **description** command.
Route Port	Layer-3 interface An IP-Trunk interface works only as a layer-3 interface.
Hash arithmetic	Hash algorithm of the interface Hash calculation is performed based on the "Exclusive-OR" result of the source and destination IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximal BW	Maximum bandwidth of the IP-Trunk interface, that is, the sum of maximum bandwidth supported by each POS interface added to the IP-Trunk interface.
Current BW	Actual bandwidth of the IP-Trunk interface After POS interfaces of different rates are added to the same IP-Trunk, all the interfaces adopt the smallest rate among them. For example, when you add a 10 Gbit/s POS interface and a 2.5 Gbit/s POS interface to an IP-Trunk, the 10 Gbit/s POS interface can forward data only at the rate of 2.5 Gbit/s, and the IP-Trunk interface can forward data at the rate of 5 Gbit/s, instead of 12.5 Gbit/s.
Current system time	Current system time.
Last 10 seconds input/output rate	Rate of bytes and packets received on the interface in the last 10 seconds.
Realtime 0 seconds input/output rate	Rate of bytes and packets received on the interface currently.
Input	Number of packets received by the interface
Output	Number of packets sent by the interface
Input bandwidth utilization	Input bandwidth usage of the IP-Trunk interface
Output bandwidth utilization	Output bandwidth usage of the IP-Trunk interface
PortName	Name of the IP-Trunk member interface
Status	Status of the member interface
Weight	Weight of the member interface
The Number of Ports in Trunk	Number of IP-Trunk member interfaces
The Number of UP Ports in Trunk	Number of IP-Trunk member interfaces in the Up state

Related Topics

7.10.9 reset counters interface ip-trunk

7.10.2 display trunkfwdtbl ip-trunk

Function

The **display trunkfwdtbl ip-trunk** command displays the forwarding table of an IP-Trunk interface.

Format

display trunkfwdtbl ip-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Displays the status of an IP-Trunk interface.	The value is an integer and varies according to device model, the value depend on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An IP-Trunk supports a maximum of eight physical member interfaces, which correspond to eight entries in the forwarding table. The eight entries correspond to hash key values 0 to 7. The system searches for outbound interfaces among active links based on hash key values.

When data forwarded by an IP-Trunk interface is abnormal, run the **display trunkfwdtbl ip-trunk** command to view the forwarding table of the interface.

Precautions

An IP-Trunk contains a maximum of eight POS interfaces. Therefore, the forwarding table contains eight entries.

Example

Display the forwarding table of IP-Trunk 1.

```
<Huawei> display trunkfwdtbl ip-trunk 1
Ip-Trunk1's forwarding table is:
Pos2/0/0
Pos2/0/0
Pos2/0/0
Pos2/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Pos2/0/0
Pos2/0/0
Pos2/0/0
Pos2/0/0
```

Related Topics

7.10.6 ip-trunk

7.10.3 display trunkmembership ip-trunk

Function

The **display trunkmembership ip-trunk** command displays information about member interfaces of an IP-Trunk interface.

Format

display trunkmembership ip-trunk *trunk-id*

Parameters

Parameter	Description	Value
trunk-id	Displays the status of an IP-Trunk interface.	The value is an integer and varies according to device model, the value depend on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display trunkmembership ip-trunk** command to view the status and weight of each member interface of the IP-Trunk.

Example

Display member interfaces of an IP-Trunk interface.

```
<Huawei> display trunkmembership ip-trunk 3
Trunk ID: 3
TYPE: pos
Number Of Ports in Trunk = 1
Number Of Up Ports in Trunk = 1
Operate status: up
Interface Pos2/0/0, valid, operate up, weight=1
```

Table 7-61 Description of the display trunkmembership ip-trunk command output

Item	Description
Trunk ID	IP-Trunk interface ID
TYPE	IP-Trunk type (POS)
Number Of Ports in Trunk	Number of POS interfaces that are added to the IP-Trunk interface
Number Of Up Ports in Trunk	Number of Up interfaces that are added to the IP-Trunk interface
Operate status	Running status • up • down
Interface Pos2/0/0, valid, operate up, weight=1	Status and weight of a member interface • Whether the interface is valid (valid or invalid) • Whether the interface is Up or Down (operate down or operate up). • weight=1

Related Topics

7.10.6 ip-trunk

7.10.4 display trunk resource

Function

The **display trunk resource** command displays trunk resources that have been used on a device.

Format

display trunk resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To learn about used trunk resources, run the **display trunk resource** command to check the number of created trunks and the number of interfaces added to the trunk interface.

Example

Display trunk resources used on a device.

```
<Huawei> display trunk resource
Number of configured trunk interfaces is : 4
Interface          Member Count
-------------------------------------------------------------
Eth-Trunk1          2
Eth-Trunk10         0
Eth-Trunk30         0
Eth-Trunk55         0
```

Table 7-62 Description of the **display trunk resource** command output

Item	Description
Number of configured trunk interfaces is	Number of configured trunk interfaces.
Interface	Trunk interface type: ● Eth-Trunk ● IP-Trunk
Member Count	Number of member interfaces added to a trunk interface.

7.10.5 interface ip-trunk

Function

The **interface ip-trunk** command creates an IP-Trunk interface and enters the IP-Trunk interface view.

The **undo interface ip-trunk** command deletes an existent IP-Trunk interface.

Format

interface ip-trunk *trunk-id*

undo interface ip-trunk *trunk-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trunk-id	Specifies the IP-Trunk interface ID.	The value is an integer and varies according to device model, the value depend on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You need to create an IP-Trunk interface, and then set parameters in the IP-Trunk interface view.

Example

Create an IP-Trunk interface numbered 1.

```
<Huawei> system-view
[Huawei] interface ip-trunk 1
[Huawei-Ip-Trunk1]
```

Related Topics

7.10.6 ip-trunk

7.10.6 ip-trunk

Function

The **ip-trunk** command adds a POS interface to an IP-Trunk.

The **undo ip-trunk** command removes a POS interface from an IP-Trunk.

By default, a POS interface is not added to any IP-Trunk interfaces.

Format

ip-trunk *trunk-id*

undo ip-trunk

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trunk-id	Specifies the IP-Trunk interface ID.	The value is an integer and varies according to device model, the value depend on the device.

Views

POS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip-trunk** command adds a POS interface to a specified IP-Trunk.

Precautions

- The link-layer protocol of the POS interface that is added to the IP-Trunk interface must be HDLC. After a POS interface is added to the IP-Trunk interface, the link-layer protocol cannot be changed.
- A member interface can neither have Layer 3 features such as the IP address nor configure any services when being added to the IP-Trunk interface.
- A POS interface can be added to only one IP-Trunk interface. The POS interface must be deleted from the original IP-Trunk interface before joining another IP-Trunk interface.
- IP-Trunk interfaces cannot be added to IP-Trunk interfaces.
- POS interfaces on different interface boards can be added to the same IP-Trunk interface.
- POS interfaces of different rates can be added to the same IP-Trunk, but all the interfaces adopt the smallest rate among them. For example, when you add a 622 Mbit/s POS interface and a 155 MB POS interface to an IP-Trunk, the 622 Mbit/s POS interface can forward data only at the rate of 155 Mbit/s, and the IP-Trunk interface can forward data at the rate of 310 Mbit/s, instead of 777 Mbit/s.
- If a member interface of an IP-Trunk interface is connected to the peer, the directly connected interface on the peer must also be a member interface of an IP-Trunk interface.

Example

Add POS 2/0/0 to IP-Trunk 1.

```
<Huawei> system-view
[Huawei] interface pos 2/0/0
[Huawei-Pos2/0/0] ip-trunk 1
```

Related Topics

7.10.5 interface ip-trunk

7.10.7 least active-linknumber (IP-Trunk interface view)

Function

The **least active-linknumber** command sets the minimum number of IP-Trunk member interfaces in the Up state.

The **undo least active-linknumber** command restores the default setting.

By default, the minimum number of IP-Trunk member interfaces in the Up state is 1.

Format

least active-linknumber *link-number*

undo least active-linknumber

Parameters

Parameter	Description	Value
link-number	Sets the minimum number of IP-Trunk member interfaces in the Up state.	The value is an integer ranging from 1 to 8.

Views

IP-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The minimum number is configured to ensure the minimum bandwidth and prevent packet loss caused by a small number of active links and high load. For example, each member link can provide a bandwidth of 155 Mbit/s, and the trunk interface should provide a minimum bandwidth of 310 Mbit/s. In this case, the minimum number should be set to 2 or a larger value.

- When the number of IP-Trunk member interfaces in the Up state is smaller than the minimum number, the trunk becomes Down.
- When the number of IP-Trunk member interfaces in the Up state increases to the minimum number, the trunk becomes Up.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

To ensure normal forwarding, you are advised to configure the two ends of an IP-Trunk link with the same minimum number.

Example

Set the minimum number of IP-Trunk 1 member interfaces in the Up state to 3.

```
<Huawei> system-view
[Huawei] interface ip-trunk 1
[Huawei-Ip-Trunk1] least active-linknumber 3
```

7.10.8 load-balance

Function

The **load-balance** command sets a load balancing mode of an IP-Trunk.

The **undo load-balance** command restores the default load balancing mode of an IP-Trunk.

By default, the load balancing mode is **src-dst-ip**.

Format

load-balance { **dst-ip** | **src-dst-ip** | **src-ip** }

undo load-balance

Parameters

Parameter	Description	Value
dst-ip	Indicates load balancing based on destination IP addresses.	-
src-ip	Indicates load balancing based on source IP addresses.	-
src-dst-ip	Indicates load balancing based on source and destination IP addresses.	-

Views

IP-Trunk interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A data flow is a group of datagrams with the same source IP address and destination IP address.

When trunk interfaces are not used, Layer 2 frames of the same data flow can reach the destination in sequence because only one physical connection exists between the two devices. After trunk interfaces are used, multiple physical links exist between two devices. If the first and second frames are transmitted over different physical links, the second frame may reach the destination earlier than the first frame.

To prevent the disorder of frames, a data forwarding mechanism is introduced into the trunking technology to ensure that the frames of the same data flow are sent to the destination in sequence. This mechanism categorizes data flows based on MAC addresses or IP addresses. Datagrams that belong to the same data flow are transmitted over the same physical link.

If IP addresses are used for categorizing data flows, packets with the same source and same destination IP addresses are transmitted over the same physical link.

You can set the load balancing mode based on traffic models. When a parameter of traffic changes frequently, you can set the load balancing mode based on this parameter to ensure that the traffic is load balanced evenly. For example, if IP addresses in packets change frequently, use the load balancing mode based on **dst-ip**, **src-ip**, or **src-dst-ip** so that traffic can be properly load balanced among physical links.

The device supports the following load balancing modes:

- **dst-ip**: load balancing based on destination IP address. In this mode, the system obtains the specified three bits from each of the destination IP address and the TCP or UDP port number of outgoing interfaces to perform the Exclusive-OR calculation, and then selects the outgoing interface from the IP-Trunk table according to the calculation result.

  If the packet destination IP address in the data flow changes frequently but the source IP address has a smaller change, you can use this load balancing mode.
- **src-ip**: load balancing based on source IP address. In this mode, the system obtains the specified three bits from each of the source IP address and the TCP or UDP port number of incoming interfaces to perform the Exclusive-OR calculation, and then selects the outgoing interface from the IP-Trunk table according to the calculation result.

  If the packet source IP address in the data flow changes frequently but the destination IP address has a smaller change, you can use this load balancing mode.
- **src-dst-ip**: load balancing based on the Exclusive-OR result of the source IP address and destination IP address. In this mode, the system performs the Exclusive-OR calculation between the Exclusive-OR results of the **dst-ip** and **src-ip** modes, and then selects the outgoing interface from the IP-Trunk table according to the calculation result.

  If the packet source and destination IP addresses in the data flow change frequently, you can use this load balancing mode.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- If you run the **load-balance** command multiple times, only the latest configuration takes effect.
- Load balancing is valid only for outgoing traffic; therefore, the load balancing modes for the interfaces at both ends of the link can be different and do not affect each other.

Example

Set the load balancing mode of an IP-Trunk to **dst-ip**.

```
<Huawei> system-view
[Huawei] interface IP-Trunk 1
[Huawei-IP-Trunk1] load-balance dst-ip
```

7.10.9 reset counters interface ip-trunk

Function

The **reset counters interface ip-trunk** command deletes statistics on an IP-Trunk interface.

Format

reset counters interface ip-trunk [*trunk-id*]

Parameters

Parameter	Description	Value
trunk-id	Specifies the IP-Trunk interface ID.	The value is an integer and varies according to device model, the value depend on the device.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before re-collecting traffic statistics on a specific interface within a certain period, you need to delete the existing statistics on this interface.

The **reset counters interface ip-trunk** command deletes the output of the **display interface ip-trunk** command.

Precautions

Once statistics are deleted, they cannot be restored. Confirm the action before you perform it.

Example

Delete statistics on IP-Trunk1.

```
<Huawei> reset counters interface ip-trunk 1
```

Related Topics

7.10.1 display interface ip-trunk

7.10.10 shutdown (IP-Trunk interface view)

Function

The **shutdown** command disables an IP-Trunk interface.

The **undo shutdown** command enables the current IP-Trunk interface.

By default, an IP-Trunk is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

IP-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **shutdown** command is executed for an IP-Trunk interface, all its member interfaces are automatically disabled, and the **undo shutdown** command becomes invalid for a member interface.

- When the administrator uses the **shutdown** command on an IP-Trunk interface, the interface is in the Administratively DOWN state and:
  - A new member interface that is added to the IP-Trunk interface automatically enters the Administratively DOWN state.
  - A member interface that is removed from the IP-Trunk interface remains in the Administratively DOWN state.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Data frames may be lost if you disable an interface during data transmission. Exercise caution when you use the **shutdown** command.

Example

Disable the IP-Trunk1 interface.

```
<Huawei> system-view
[Huawei] interface ip-trunk 1
[Huawei-Ip-Trunk1] shutdown
```

Related Topics

7.10.5 interface ip-trunk

7.10.11 trunkport (IP-Trunk interface view)

Function

The **trunkport** command adds member interfaces in batches in the IP-Trunk interface view.

The **undo trunkport** command deletes member interfaces in batches in the IP-Trunk interface view.

By default, an interface does not belong to any IP-Trunk.

Format

trunkport pos { *interface-number1* [**to** *interface-number2*] }

undo trunkport pos { *interface-number1* [**to** *interface-number2*] }

Parameters

Parameter	Description	Value
pos { *interface-number1* [**to** *interface-number2*] }	Specifies a POS interface. • *interface-number1* specifies the ID of the first POS interface. • *interface-number2* specifies the ID of the last POS interface.	The *interface-number2* value must be greater than the *interface-number1* value and values between *interface-number2* and *interface-number1* are IDs of existing interfaces.

Views

IP-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users can use the **trunkport** command to add member interfaces in batches in the IP-Trunk interface view.

Precautions

- The link-layer protocol of the POS interface that is added to the IP-Trunk interface must be HDLC. After a POS interface is added to the IP-Trunk interface, the link-layer protocol cannot be changed.
- A member interface can neither have Layer 3 features such as the IP address nor configure any services when being added to the IP-Trunk interface.
- A POS interface can be added to only one IP-Trunk interface. The POS interface must be deleted from the original IP-Trunk interface before joining another IP-Trunk interface.
- IP-Trunk interfaces cannot be added to IP-Trunk interfaces.
- POS interfaces on different interface boards can be added to the same IP-Trunk interface.
- POS interfaces of different rates can be added to the same IP-Trunk, but all the interfaces adopt the smallest rate among them. For example, when you add a 622 Mbit/s POS interface and a 155 MB POS interface to an IP-Trunk, the 622 Mbit/s POS interface can forward data only at the rate of 155 Mbit/s, and the IP-Trunk interface can forward data at the rate of 310 Mbit/s, instead of 777 Mbit/s.
- If a member interface of an IP-Trunk interface is connected to the peer, the directly connected interface on the peer must also be a member interface of an IP-Trunk interface.

Example

Add member interfaces POS 2/0/0 and 4/0/0 to IP-Trunk1.

```
<Huawei> system-view
[Huawei] interface ip-trunk 1
[Huawei-Ip-Trunk1] trunkport pos 2/0/0 4/0/0
```

Related Topics

7.10.1 display interface ip-trunk
7.10.6 ip-trunk

7.11 ISDN Configuration Commands

7.11.1 dialer isdn-leased

Function

The **dialer isdn-leased** command configures a 64 kbit/s ISDN leased line.

The **undo dialer isdn-leased** command deletes a 64 kbit/s ISDN leased line.

By default, the 64 kbit/s ISDN leased line is not configured on the device.

Format

dialer isdn-leased *number*

undo dialer isdn-leased *number*

Parameters

Parameter	Description	Value
number	Specifies the ID of the timeslot or the B channel used as a 64 kbit/s ISDN leased line.	The value is an integer. ● For ISDN BRI interfaces, the value ranges from 1 to 2. The values 1 and 2 correspond to B1 and B2 channel respectively. ● For CE1/PRI interfaces, the value ranges from 1 to 31. Values 1 to 31 correspond to timeslots 1 to 31 respectively. Timeslot 16 functions as the D channel. ● For CT1/PRI interfaces, the value ranges from 1 to 24. Values 1 to 24 correspond to timeslots 1 to 24 respectively. Timeslot 24 functions as the D channel.

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enterprise branches and the headquarters connect to the ISP-provided ISDN network through ISDN interfaces. When a branch company needs to exchange a large amount of data with the headquarters or other branch companies for a long period of time, establish an ISDN leased line between them to ensure timely, high-speed, and reliable data transmission.

B channels on ISDN BRI interfaces or timeslots of PRI interfaces can be configured as leased lines to provide 64 kbit/s bandwidth. The leased lines are called 64 kbit/s ISDN leased lines.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

- The circular DCC has been configured. For the configuration procedure, see Configuring C-DCC.
- Network-side ISDN switches provide an ISDN leased line.

Precautions

- If the B channel on an ISDN BRI interface or the timeslot of an ISDN PRI interface is used as the ISDN leased line, the interface cannot be used for dialing. That is, the ISDN leased line and dialing functions cannot be configured on the same interface.
- Before switching between the 64 kbit/s ISDN leased line and 128 kbit/s ISDN leased line, delete the configuration of the original leased line.

Example

Configure B1 channel on BRI1/0/0 as the leased line.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-BRI 1/0/0] dialer isdn-leased 1
```

Configure timeslot 1 of Serial 1/0/0:15 on CE1/PRI interface as the leased line.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] dialer isdn-leased 1
```

Related Topics

7.11.2 dialer isdn-leased 128k
7.1.22 display dialer

7.11.2 dialer isdn-leased 128k

Function

The **dialer isdn-leased 128k** command configures a 128 kbit/s ISDN leased line.

The **undo dialer isdn-leased 128k** command deletes a 128 kbit/s ISDN leased line.

By default, the 128 kbit/s ISDN leased line is not configured on the device.

Format

dialer isdn-leased 128k

undo dialer isdn-leased 128k

Parameters

None

Views

ISDN BRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enterprise branches and the headquarters connect to the ISP-provided ISDN network through ISDN interfaces. When a branch company needs to exchange a large amount of data with the headquarters or other branch companies for a long period of time, establish an ISDN leased line between them to ensure timely, high-speed, and reliable data transmission.

The 64 kbit/s and 128 kbit/s leased lines can be configured on ISDN BRI interfaces. The **dialer isdn-leased 128k** command configures a 128 kbit/s leased line.

Prerequisites

- The circular DCC has been configured. For the configuration procedure, see Configuring C-DCC.
- Network-side ISDN switches provide an ISDN leased line.

Precautions

- If the B channel on an ISDN BRI interface is used as the ISDN leased line, the interface cannot be used for dialing. That is, the ISDN leased line and dialing functions cannot be configured on the same interface.
- Before switching between the 64 kbit/s ISDN leased line and 128 kbit/s leased line, delete the configuration of the original leased line.

Example

Configure a 128 kbit/s ISDN leased line on BRI 1/0/0.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-BRI 1/0/0] dialer isdn-leased 128k
```

Related Topics

7.11.1 dialer isdn-leased

7.11.3 display isdn active-channel

Function

Using the **display isdn active-channel** command, you can view active call information on ISDN interfaces.

Format

display isdn active-channel [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays active call information on the specified ISDN interface. If no interface is specified, active call information on all the ISDN interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display isdn active-channel** command displays active call information on ISDN interfaces. You can locate ISDN call faults according to the command output.

Precautions

If there is no active call information, the **display isdn active-channel** command output is empty.

Example

Display active call information on Serial1/0/0:15.

```
<Huawei> display isdn active-channel interface serial 1/0/0:15
Serial1/0/0:15
--------------------------------------------------------------------------------
Channel  Call     Call     Calling        Calling     Called         Called
Info     Property Type     Number         Subaddress  Number
Subaddress
--------------------------------------------------------------------------------
B3       Digital  Out      7654321        -           1234567        -
```

Display active call information on BRI1/0/0

```
<Huawei> display isdn active-channel interface bri 1/0/0
BRI 1/0/0
--------------------------------------------------------------------------------
Channel  Call     Call     Calling        Calling     Called         Called
Info     Property Type     Number         Subaddress  Number
Subaddress
--------------------------------------------------------------------------------
B1       Digital  Out      -              -           88888204       -
```

 Copyright © Huawei Technologies Co., Ltd.

Table 7-63 Description of the display isdn active-channel command output

Item	Description
Channel Info	Channel where the active call resides. • For ISDN BRI interfaces, channels can be B1 and B2. • For CE1/PRI interfaces, channels can be B1 to B15 or B17 to B31. • For CT1/PRI interfaces, channels can be B1 to B23.
Call Property	Property of the active call: • Digital: indicates a digital call. • Analog: indicates an analog call.
Call Type	Type of the active call: • In: indicates an incoming call. • Out: indicates an outgoing call.
Calling Number	Calling number of the active call.
Calling Subaddress	Calling sub-address of the active call.
Called Number	Called number of the active call.
Called Subaddress	Called sub-address of the active call.

Related Topics

7.11.10 isdn caller-number
7.11.11 isdn calling
7.11.12 isdn check-called-number

7.11.4 display isdn call-info

Function

Using the **display isdn call-info** command, you can view call information on ISDN interfaces.

Format

display isdn call-info [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays call information on the specified ISDN interface. If no interface is specified, call information on all the ISDN interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display isdn call-info** command displays call information on ISDN interfaces, including the status of each layer (Q.921 and Q.931) of the ISDN protocol. You can locate ISDN call faults according to the command output.

Example

Display call information on Serial1/0/0:15.

```
<Huawei> display isdn call-info interface serial 1/0/0:15
Serial1/0/0:15 :
  Link Layer: TEI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
  Network Layer: 1 connection(s)
    Connection 1 :
      CCIndex:0x0002 , State: Active , CES:1 ,
Channel:0x00000008
      Calling_Num[:Sub]: 7654321
      Called_Num[:Sub]: 1234567
```

Table 7-64 Description of the display isdn call-info interface serial command output

Item	Sub-item	Description
Link Layer	TEI	Terminal equipment identifier (TEI) of the link layer.
Link Layer	State	Link layer protocol status: ● TEI_ASSIGNED ● AWAITING_ESTABLISHMENT ● AWAITING_RELEASE ● MULTIPLE_FRAME_ESTABLISHED ● TIMER_RECOVER

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Network Layer	CCIndex	Index of the call at the call control (CC) layer.

Item	Sub-item	Description
Network Layer	State	Network layer status: ● NULL: No call exists. ● CALL_INITIATED: This state exists for an outgoing call when the user requests call establishment to the network. ● OVERLAP_SENDING: This state exists for an outgoing call when the user has received an acknowledgement of the call establishment request and is permitted to send additional call information to the network in overlap mode. ● OUTGOING_CALL_PROCEEDING: This state exists for an outgoing call when the user has received the acknowledgement that the network has received all call information required for call establishment. ● CALL_DELIVERED: This state exists for an outgoing call when the calling user has received an indication that remote user alerting has been initiated. ● CALL_PRESENT: This state exists for an incoming call when the user has received a call establishment request but has not yet responded. ● OVERLAP_RECEIVING: This state exists for an incoming call when the user has confirmed a call establishment request and is ready to receive call information in overlap mode. ● CALL_RECEIVED: This state exists for an incoming call when the user has initiated an alert but has not yet answered. ● CONNECT_REQUEST: This state exists for an incoming call when the user has answered the call and is waiting to be awarded the call. ● INCOMING_CALL_PROCEEDING: This state exists for an incoming call when the user has sent an acknowledgement that all call information required for call establishment has been received. ● ACTIVE: This state exists for an incoming call when the user has received an acknowledgement from the network that the user has been awarded the call. This state exists for an outgoing call when the user has received an indication that the remote user has answered the call. ● DISCONNECT_REQUEST: This state exists when the user has requested the network to clear the end-to-end connection and is waiting for a response. ● DISCONNECT_INDICATION: This state exists when the user has received a disconnection request

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
		because the network has disconnected the end-to-end connection. ● SUSPEND_REQUEST: This state exists when the user has requested the network to suspend the call and is waiting for a response. ● RESUME_REQUEST: This state exists when the user has requested the network to resume a previously suspended call and is waiting for a response. ● RELEASE_REQUEST: This state exists when the user has requested the network to release the call and is waiting for a response. ● OVERLAP_RECEIVING: This state exists for an incoming call when the user has acknowledged the call establishment request from the network and prepares to receive additional call information in overlap mode. After a call has been established, the network layer status is ACTIVE.
Network Layer	CES	Connection endpoint suffix (CES), which is specified by a Layer 3 or management entity to identify a Layer 2 link connected to Layer 3. The value is always 1.
Network Layer	Channel	ISDN B channel used by a call. This field is displayed as a hexadecimal number. After it is converted into a binary number, bits of the binary number indicate whether corresponding B channels are used. If the value of a bit is 1, the B channel specified by the bit is used. If the value of a bit is 0, the B channel specified by the bit is not used. For example, after a hexadecimal number 0x00000008 is converted into a binary number, only bit 3 is 1, so B3 channel is used.
Network Layer	Calling_Num[:Sub]	Calling number and calling sub-address.
Network Layer	Called_Num[:Sub]	Called number and called sub-address.

Display call information on BRI1/0/0.

- When a BRI interface works in point-to-point (P2P) mode, the following command output is displayed.

```
<Huawei> display isdn call-info interface bri 1/0/0
Bri1/0/0 :
  Link Layer 1:  TEI = 0, State =
MULTIPLE_FRAME_ESTABLISHED
  Link Layer 2:  TEI = 0, State =
TEI_ASSIGNED
  Link Layer 3:  TEI = 0, State =
```

```
TEI_ASSIGNED
  Link Layer 4:  TEI = 0, State =
TEI_ASSIGNED
  Link Layer 5:  TEI = 0, State =
TEI_ASSIGNED
  Link Layer 6:  TEI = 0, State =
TEI_ASSIGNED
  Link Layer 7:  TEI = 0, State =
TEI_ASSIGNED
  Link Layer 8:  TEI = 0, State =
TEI_ASSIGNED
  Network Layer: 1 connection(s)
    Connection 1 :
      CCIndex:0x0002 , State: Active , CES:1 ,
Channel:0x00000001
      Calling_Num[:Sub]: 7654321
      Called_Num[:Sub]: 1234567
```

- When a BRI interface works in point-to-multipoint (P2MP) mode, the following command output is displayed.

```
<Huawei> display isdn call-info interface bri 1/0/0
Bri1/0/0 :
  Link Layer 1:  TEI = 65, State =
MULTIPLE_FRAME_ESTABLISHED
  Link Layer 2:  TEI = NONE, State =
TEI_UNASSIGNED
  Link Layer 3:  TEI = NONE, State =
TEI_UNASSIGNED
  Link Layer 4:  TEI = NONE, State =
TEI_UNASSIGNED
  Link Layer 5:  TEI = NONE, State =
TEI_UNASSIGNED
  Link Layer 6:  TEI = NONE, State =
TEI_UNASSIGNED
  Link Layer 7:  TEI = NONE, State =
TEI_UNASSIGNED
  Link Layer 8:  TEI = NONE, State =
TEI_UNASSIGNED
  Network Layer: 1 connection(s)
    Connection 1 :
      CCIndex:0x0002 , State: Active , CES:1 ,
Channel:0x00000001
      Calling_Num[:Sub]: 7654321
      Called_Num[:Sub]: 1234567
```

Table 7-65 Description of the display isdn call-info interface bri command output

Item	Sub-item	Description
Link Layer	-	Link layer status. A BRI interface connects to a network-side device by using network terminal 1 (NT1) and works in either P2P or P2MP mode. When a BRI interface works in P2MP mode, a maximum of eight devices can be connected to NT1, and each device has its own link layer status.

Item	Sub-item	Description
TEI	-	Terminal equipment identifier (TEI). When a BRI interface works in P2P mode, the TEI is always 0. When a BRI interface works in P2MP mode, the TEI ranges from 64 to 126 or is NONE. The value NONE indicates that there is no TEI.
State	-	Link layer protocol status: ● TEI_UNASSIGNED ● ASSIGN_AWAITING_TEI ● ESTABLISH_AWAITING_TEI ● TEI_ASSIGNED ● AWAITING_ESTABLISHMENT ● AWAITING_RELEASE ● MULTIPLE_FRAME_ESTABLISHED ● TIMER_RECOVER ● TEI_ASSIGNED_EXT1 ● TEI_ASSIGNED_EXT2
Network Layer	CCIndex	Index of the call at the CC layer.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Network Layer	State	Network layer status: ● NULL: No call exists. ● CALL_INITIATED: This state exists for an outgoing call when the user requests call establishment to the network. ● OVERLAP_SENDING: This state exists for an outgoing call when the user has received an acknowledgement of the call establishment request and is permitted to send additional call information to the network in overlap mode. ● OUTGOING_CALL_PROCEEDING: This state exists for an outgoing call when the user has received the acknowledgement that the network has received all call information required for call establishment. ● CALL_DELIVERED: This state exists for an outgoing call when the calling user has received an indication that remote user alerting has been initiated. ● CALL_PRESENT: This state exists for an incoming call when the user has received a call establishment request but has not yet responded. ● OVERLAP_RECEIVING: This state exists for an incoming call when the user has confirmed a call establishment request and is ready to receive call information in overlap mode. ● CALL_RECEIVED: This state exists for an incoming call when the user has initiated an alert but has not yet answered. ● CONNECT_REQUEST: This state exists for an incoming call when the user has answered the call and is waiting to be awarded the call. ● INCOMING_CALL_PROCEEDING: This state exists for an incoming call when the user has sent an acknowledgement that all call

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
		information required for call establishment has been received. ● ACTIVE: This state exists for an incoming call when the user has received an acknowledgement from the network that the user has been awarded the call. This state exists for an outgoing call when the user has received an indication that the remote user has answered the call. ● DISCONNECT_REQUEST: This state exists when the user has requested the network to clear the end-to-end connection and is waiting for a response. ● DISCONNECT_INDICATION: This state exists when the user has received a disconnection request because the network has disconnected the end-to-end connection. ● SUSPEND_REQUEST: This state exists when the user has requested the network to suspend the call and is waiting for a response. ● RESUME_REQUEST: This state exists when the user has requested the network to resume a previously suspended call and is waiting for a response. ● RELEASE_REQUEST: This state exists when the user has requested the network to release the call and is waiting for a response. ● OVERLAP_RECEIVING: This state exists for an incoming call when the user has acknowledged the call establishment request from the network and prepares to receive additional call information in overlap mode. After a call has been established, the network layer status is ACTIVE.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
Network Layer	CES	Connection endpoint suffix (CES), which is specified by a Layer 3 or management entity to identify a Layer 2 link connected to Layer 3. When a BRI interface works in P2P mode, the CES is always 1. When a BRI interface works in P2MP mode, the CES ranges from 1 to 8.
Network Layer	Channel	ISDN B channel used by a call. This field is displayed as a hexadecimal number. After it is converted into a binary number, bits of the binary number indicate whether corresponding B channels are used. If the value of a bit is 1, the B channel specified by the bit is used. If the value of a bit is 0, the B channel specified by the bit is not used. For example, after a hexadecimal number 0x00000001 is converted into a binary number, only bit 1 is 1, so B1 channel is used.
Network Layer	Calling_Num[:Sub]	Calling number and calling sub-address.
Network Layer	Called_Num[:Sub]	Called number and called sub-address.

Related Topics

7.11.10 isdn caller-number
7.11.11 isdn calling
7.11.12 isdn check-called-number

7.11.5 display isdn call-record

Function

Using the **display isdn call-record** command, you can view historical call statistics on ISDN interfaces.

Format

display isdn call-record [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays historical call statistics on the specified ISDN interface. If no interface is specified, historical call statistics on all the ISDN interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display isdn call-record** command displays historical call statistics on ISDN interfaces. You can check the correctness of time-based accounting according to the command output.

Historical call statistics record calls established since system startup. The system stores a maximum of 200 call history records.

Example

Display historical call statistics on Serial1/0/0:15.

```
<Huawei> display isdn call-record interface serial 1/0/0:15
Serial1/0/0:15
-------------------------------------------------------------------------------
Call Calling       Called        Start           Stop            Seconds
Type Number        Number        Time            Time            Used
-------------------------------------------------------------------------------
In   6666666       7777777       10-11-24 14:50:39 -               14
Out  7654321       1234567       10-11-24 14:48:48 10-11-24 14:49:43 55
```

Display historical call statistics on BRI1/0/0.

```
<Huawei> display isdn call-record interface bri 1/0/0
Bri1/0/0
-------------------------------------------------------------------------------
Call Calling       Called        Start           Stop            Seconds
Type Number        Number        Time            Time            Used
-------------------------------------------------------------------------------
Out  -             88888204      10-12-07 11:58:39 -               92
```

 Copyright © Huawei Technologies Co., Ltd.

Table 7-66 Description of the display isdn call-record command output

Item	Description
Call Type	Call type: ● In: indicates an incoming call. ● Out: indicates an outgoing call.
Calling Number	Calling number.
Called Number	Called number.
Start Time	Call start time.
Stop Time	Call end time.
Seconds Used	Duration of a historical call or elapsed time of an in-progress call, in seconds.

7.11.6 display isdn dss1-parameters

Function

Using the **display isdn dss1-parameters** command, you can view ISDN Layer 2 and Layer 3 parameters.

Format

display isdn dss1-parameters [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays ISDN Layer 2 and Layer 3 parameters on the specified ISDN interface. If no interface is specified, default ISDN Layer 2 and Layer 3 parameters are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display isdn dss1-parameters** command displays ISDN Layer 2 and Layer 3 parameters. You can locate ISDN faults according to the command output.

Example

Display default ISDN Layer 2 and Layer 3 parameters.

```
<Huawei> display isdn dss1-parameters
ISDN Q921 system parameters:
  T200(sec)  T202(sec)  T203(sec)  N200  K(BRI)
K1(PRI)
  1          2          10         3     1        7

ISDN Q931 system timers:
  Timer-Number         Value(sec)
      T301             240
      T302             15
      T303             4
      T304             30
      T305             30
      T308             4
      T309             90
      T310             40
      T313             4
      T314             4
      T316             120
      T317             10
      T318             4
      T319             4
      T321             30
      T322             4
```

Display ISDN Layer 2 and Layer 3 parameters on BRI1/0/0.

```
<Huawei> display isdn dss1-parameters interface bri 1/0/0
ISDN Q921 system parameters:
  T200(sec)  T202(sec)  T203(sec)  N200  K(BRI)
  1          2          10         3     1

ISDN Q931 system timers:
  Timer-Number         Value(sec)
      T301             240
      T302             15
      T303             4
      T304             30
      T305             30
      T308             4
      T309             90
      T310             40
      T313             4
      T314             4
      T316             120
      T317             10
      T318             4
      T319             4
      T321             30
      T322             4
```

 Copyright © Huawei Technologies Co., Ltd.

Table 7-67 Description of the display isdn dss1-parameters command output

Item	Sub-item	Description
ISDN Q921 system parameters	T200(sec)	Retransmission timer of the ISDN layer 2 protocol, in seconds. The value is always 1.
ISDN Q921 system parameters	T202(sec)	Retransmission timer of TEI Request messages of the ISDN layer 2 protocol, in seconds. The value is always 2.
ISDN Q921 system parameters	T203(sec)	Maximum link idle time of the ISDN Layer 2 protocol, in seconds. The value is always 10.
ISDN Q921 system parameters	N200	Maximum number of retransmissions. The value is always 3.
ISDN Q921 system parameters	K(BRI)	Sliding window size of an ISDN BRI interface. The value is always 1. This field is displayed only when a BRI interface card is inserted.
ISDN Q921 system parameters	K1(PRI)	Sliding window size of an ISDN PRI interface. The value can be set by using the **isdn pri-slipwnd-size** command. This field is displayed only when a CE1/PRI or CT1/PRI interface card is inserted.

 Copyright © Huawei Technologies Co., Ltd.

Item	Sub-item	Description
ISDN Q931 system timers	Timer-Number	Timers of the ISDN Layer 3 protocol: • T301 • T302 • T303 • T304 • T305 • T308 • T309 • T310 • T313 • T314 • T316 • T317 • T318 • T319 • T321 • T322 For functions of these timers, see the Usage Scenario of the **isdn l3-timer** command.
ISDN Q931 system timers	Value(sec)	Timer values of the ISDN Layer 3 protocol. Values of T301, T302, T303, T304, T305, T308, T309, T310, T313, T316, and T322 can be set by using the **isdn l3-timer** command. Values of other timers are default values and cannot be set.

Related Topics

7.11.17 isdn l3-timer

7.11.22 isdn pri-slipwnd-size

7.11.7 isdn bch-assign

Function

The **isdn bch-assign** command enables the router to ignore the option indicating that only the indicated channel is acceptable sent from the ISDN-side device.

The **undo isdn bch-assign** command disables the router from ignoring the option indicating that only the indicated channel is acceptable sent from the ISDN-side device.

By default, the router does not ignore the option indicating that only the indicated channel is acceptable sent from the ISDN-side device.

Format

isdn bch-assign

undo isdn bch-assign

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The router connects to an integrated services digital network (ISDN) through the ISDN-side device. When the router receives a channel identification message from the ISDN-side device and the message contains the option indicating that only the indicated channel is acceptable, if B channel that the ISDN-side device assigns to the router is occupied, the router notifies the ISDN-side device that there is no available B channel on the local end. In this case, the ISDN link fails to be established.

To solve the problem, run the **isdn bch-assign** command on the router to enable the router to ignore the option indicating that only the indicated channel is acceptable sent from the ISDN-side device. After the command is configured, the router ignores the option and selects another B channel to establish the ISDN link when the identification message sent from the ISDN-side device contains the option and the assigned B channel is occupied.

Precautions

When the router can connect to the ISDN through the ISDN-side device, you do not need to configure the **isdn bch-assign** command.

Example

Enable the router to ignore the option indicating that only the indicated channel is acceptable sent from the ISDN-side device.

```
<Huawei> system-view
[Huawei] isdn bch-assign
```

7.11.8 isdn bch-local-manage

Function

Using the **isdn bch-local-manage** command, you can enable the device to manage ISDN B channels.

Using the **undo isdn bch-local-manage** command, you can disable the device from managing ISDN B channels.

By default, B channels are managed by ISDN switches.

Format

isdn bch-local-manage [**exclusive**]

undo isdn bch-local-manage

Parameters

Parameter	Description	Value
exclusive	Configures exclusive local B channel management.	-

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the process of a call, properly management of B channels that the call is using can improve call efficiency and reduce call loss.

In practice, ISDN switches are recommended for B channel management.

Precautions

- After the **isdn bch-local-manage** command is used, B channels are managed and selected by the device. The B channel selected by the device is used for communication if the ISDN switch also has an idle B channel with the same number. If the B channel with the same number as that selected by the device has been used, the ISDN switch specifies another idle B channel for communication.

 Copyright © Huawei Technologies Co., Ltd.

- The **isdn bch-local-manage exclusive** command configures exclusive local B channel management on an interface. If the B channel specified by an ISDN switch is different from that selected by the device, a call failure occurs.

Example

Configure exclusive local B channel management on BRI1/0/0.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn bch-local-manage exclusive
```

Configure exclusive local B channel management on CE1/PRI interface Serial 1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn bch-local-manage exclusive
```

Related Topics

7.11.9 isdn bch-select-way

7.11.9 isdn bch-select-way

Function

Using the **isdn bch-select-way** command, you can configure the order in which B channels will be selected.

By default, B channels are selected in ascending order of channel numbers.

Format

isdn bch-select-way { **ascending** | **descending** }

Parameters

Parameter	Description	Value
ascending	Configures B channels to be selected in ascending order of channel numbers.	-
descending	Configures B channels to be selected in descending order of channel numbers.	-

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After local B channel management or exclusive local B channel management is configured, B channels must be selected on the local end. The **isdn bch-select-way** command configures the order in which B channels will be selected on the local end.

Prerequisites

Local B channel management or exclusive local B channel management has been configured by using the **isdn bch-local-manage** [**exclusive**] command.

Example

Configure exclusive local B channel management on BRI1/0/0 and configure B channels to be selected in descending order of channel numbers.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn bch-local-manage exclusive
[Huawei-Bri1/0/0] isdn bch-select-way descending
```

Configure exclusive local B channel management on CE1/PRI interface Serial 1/0/0:15 and configure B channels to be selected in descending order of channel numbers.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn bch-local-manage exclusive
[Huawei-Serial1/0/0:15] isdn bch-select-way descending
```

Related Topics

7.11.8 isdn bch-local-manage

7.11.10 isdn caller-number

Function

The **isdn caller-number** command specifies an allowed calling number.

The **undo isdn caller-number** command restores the default setting.

By default, all calling numbers are allowed.

Format

isdn caller-number *caller-number*

undo isdn caller-number *caller-number*

Parameters

Parameter	Description	Value
caller-number	Specifies an allowed calling number.	The value is a string of 1 to 24 case-insensitive characters without spaces or question mark (?).

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For security purposes, you can configure allowed calling numbers. In this way, the device only receives calls from specified calling parties.

Precautions

If you run the **isdn caller-number** command multiple times (up to 32) in the same interface view, multiple calling numbers are allowed.

Example

Specify allowed calling numbers 66666 and 77777 on BRI1/0/0.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-BRI1/0/0] isdn caller-number 66666
[Huawei-BRI1/0/0] isdn caller-number 77777
```

Specify allowed calling numbers 66666 and 77777 on CE1/PRI interface Serial 1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn caller-number 66666
[Huawei-Serial1/0/0:15] isdn caller-number 77777
```

Related Topics

7.11.11 isdn calling
7.11.12 isdn check-called-number

7.11.11 isdn calling

Function

The **isdn calling** command configures the calling number in an outgoing call.

The **undo isdn calling** command restores the default configuration.

By default, an outgoing call does not contain the calling number.

Format

isdn calling *calling-number*

undo isdn calling

Parameters

Parameter	Description	Value
calling-number	Specifies the calling number in an outgoing call.	The value is a string of 1 to 24 case-insensitive characters without spaces or question mark (?).

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On networks where charging is performed based on calling numbers, a user can send a specific calling number that enjoys a preferential tariff to reduce the expense.

Precautions

If you run the **isdn calling** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Configure BRI1/0/0 to add a calling number 88888 in a message to be sent to the called party.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn calling 88888
```

Configure CE1/PRI interface Serial 1/0/0:15 to add a calling number 88888 in a message to be sent to the called party.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn calling 88888
```

Related Topics

7.11.10 isdn caller-number
7.11.12 isdn check-called-number

7.11.12 isdn check-called-number

Function

Using the **isdn check-called-number** command, you can specify a called number or called sub-address to be checked in an incoming call.

Using the **undo isdn check-called-number** command, you can restore the default configuration.

By default, the called number or called sub-address in an incoming call is not checked.

Format

isdn check-called-number *called-party-number* [**:** *subaddress*]

undo isdn check-called-number

Parameters

Parameter	Description	Value
called-party-number	Specifies the called number to be checked in an incoming call.	The value is a string of 1 to 30 case-insensitive characters. It cannot contain a space or question mark (?).
: *subaddress*	Specifies the called sub-address to be checked in an incoming call.	The value is a string of 1 to 40 case-insensitive characters. It cannot contain a space or question mark (?).

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For security purposes, configure the device to check called numbers or called sub-addresses. The device will reject a call if the call contains an incorrect called number or called sub-address.

Precautions

If you run the **isdn check-called-number** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Configure BRI1/0/0 to check called number 666888 and called sub-address 1 in an incoming call.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn check-called-number 666888:1
```

Configure CE1/PRI interface Serial 1/0/0:15 to check called number 666888 and called sub-address 1 in an incoming call.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn check-called-number 666888:1
```

Related Topics

7.11.10 isdn caller-number
7.11.11 isdn calling

7.11.13 isdn check-time

Function

Using the **isdn check-time** command, you can configure ISDN call check.

Using the **undo isdn check-time** command, you can restore the default configuration.

By default, ISDN call check is not configured.

Format

isdn check-time *time*

undo isdn check-time

Parameters

Parameter	Description	Value
time	Specifies the time ISDN call check is started.	This parameter is in HH:MM format. HH indicates the hour and the value ranges from 00 to 23. MM indicates the minute and the value ranges from 00 to 59.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If communication is interrupted because of physical link faults, the call status of the ISDN call control (CC) module may be unsynchronized with the call status of the Q.931 module. When this occurs, run the **isdn check-time** command to configure ISDN call check. After ISDN call check is performed, the call status of the ISDN CC module is synchronized with the call status of the Q.931 module.

Precautions

If you run the **isdn check-time** command multiple times, only the latest configuration takes effect.

Example

Configure the device to perform ISDN call check at 2 a.m. every day.

```
<Huawei> system-view
[Huawei] isdn check-time 02:00
```

7.11.14 isdn crlength

Function

Using the **isdn crlength** command, you can set the call reference length on an ISDN interface.

Using the **undo isdn crlength** command, you can restore the default call reference length.

By default, the call reference length is 1 bytes on a Basic Rate Interface (BRI) and 2 byte on a Primary Rate Interface (PRI).

 Copyright © Huawei Technologies Co., Ltd.

Format

isdn crlength *call-reference-length*

undo isdn crlength

Parameters

Parameter	Description	Value
call-reference-length	Specifies the call reference length on an ISDN interface.	The value is an integer that ranges from 1 to 2, in bytes.

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The call reference is a 1- or -2 byte sequence number that ISDN assigns to a call to identify the call. Where,

- The 1-byte call reference ranges from 0 to 127 to differentiate 128 calls.
- The 2-byte call reference ranges from 0 to 255 to differentiate 256 calls.

When a call ends, its call reference is released immediately and can be assigned to a new call.

The router can automatically identify the call reference length after receiving a call from a remote device. Some devices on networks, however, cannot automatically identify the call reference length. To enable the router to communicate with such a device and initiate a call, run the **isdn crlength** command to configure the router with the same call reference length as that of the remote device.

Precautions

If you run the **isdn crlength** command multiple times in the same interface view, only the latest configuration takes effect.

NOTE

Before running the **isdn crlength** command on an ISDN interface, ensure that there is no call on the interface. Otherwise, this command does not take effect. Alternatively, run the **shutdown**, **isdn crlength**, and **undo shutdown** commands on the ISDN interface to make the configuration take effect. Such operations, however, will disconnect existing calls on the ISDN interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the call reference length to 1 byte on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn crlength 1
```

7.11.15 isdn ignore connect-ack

Function

Using the **isdn ignore connect-ack** command, you can configure the device to transition to the ACTIVE state without sending or receiving any CONNECT ACK message.

Using the **undo isdn ignore connect-ack** command, you can restore the default configuration.

By default, the device transitions to the ACTIVE state only after sending or receiving a CONNECT ACK message.

Format

isdn ignore connect-ack [**incoming** | **outgoing**]

undo isdn ignore connect-ack [**incoming** | **outgoing**]

Parameters

Parameter	Description	Value
incoming	Configures the device to transition to the ACTIVE state without waiting to receive a CONNECT ACK message from an ISDN switch when the device receives a call.	-
outgoing	Configures the device to transition to the ACTIVE state without having to send a CONNECT ACK message to an ISDN switch when the device initiates a call.	-

Views

ISDN BRI interface view, ISDN PRI interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device switches to the ACTIVE state only after sending or receiving a CONNECT ACK message. In practice, some ISDN switches do not reply with CONNECT ACK messages. Run the **isdn ignore connect-ack** command to configure the device to ignore CONNECT ACK messages.

Precautions

- If the **incoming** or **outgoing** parameter is not specified, the device ignores CONNECT ACK messages when initiating and receiving calls.
- When the device communicates with an ISDN switch, the configuration about whether to ignore CONNECT ACK messages on the device must be the same as the configuration on the ISDN switch.

NOTE

Before running the **isdn ignore connect-ack** command on an ISDN interface, ensure that there is no call on the interface. Otherwise, this command does not take effect. Alternatively, run the **shutdown**, **isdn ignore connect-ack**, and **undo shutdown** commands on the ISDN interface to make the configuration take effect. Such operations, however, will disconnect existing calls on the ISDN interface.

Example

Configure the device to transition to the ACTIVE state without sending any CONNECT ACK message when it initiates a call on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn ignore connect-ack outgoing
```

7.11.16 isdn ignore sending-complete

Function

The **isdn ignore sending-complete** command enables the device configured with ISDN services to process messages without the complete field.

The **undo isdn ignore sending-complete** command disables the device configured with ISDN services from processing messages without the complete field.

By default, a device configured with ISDN services processes only messages with the complete field.

Format

isdn ignore sending-complete

undo isdn ignore sending-complete

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When messages without the complete field are sent for ISDN connection negotiation between a satellite terminal and a device, the device cannot process such messages and the negotiation fails. You can run the **isdn ignore sending-complete** command to enable the device configured with ISDN services to process messages without the complete field, implementing the successful interconnection.

Example

Enable a device configured with ISDN services to process messages without the complete field.

```
<Huawei> system-view
[Huawei] isdn ignore sending-complete
```

7.11.17 isdn l3-timer

Function

Using the **isdn l3-timer** command, you can configure ISDN Layer 3 timers.

Using the **undo isdn l3-timer** command, you can restore the default settings of ISDN Layer 3 timers.

The following table lists default values of ISDN Layer 3 timers.

Table 7-68 Default values of ISDN layer 3 timers

ISDN Layer 3 Timer	Default Value (Seconds)
T301	240
T302	15
T303	4
T304	30
T305	30
T308	4

 Copyright © Huawei Technologies Co., Ltd.

ISDN Layer 3 Timer	Default Value (Seconds)
T309	90
T310	40
T313	4
T316	120
T322	4

Format

isdn l3-timer *timer-name timer-value*

undo isdn l3-timer { *timer-name* | **all** }

Parameters

Parameter	Description	Value
timer-name timer-value	Specifies values of ISDN Layer 3 timers.	All timer values are integers expressed in seconds and the value ranges are as follows: ● T301: 30 to 1200 ● T302: 1 to 60 ● T303: 2 to 10 ● T304: 10 to 60 ● T305: 4 to 30 ● T308: 2 to 10 ● T309: 10 to 180 ● T310: 10 to 180 ● T313: 2 to 10 ● T316: 20 to 180 ● T322: 2 to 10
all	Restore default values of all Layer 3 timers.	-

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Table 7-69 lists functions of ISDN Layer 3 timers. For details, see the Q.931 protocol. You can set values of T301, T302, T303, T304, T305, T308, T309, T310, T313, T316, and T322.

Table 7-69 Functions of ISDN Layer 3 timers

Timer Number	Call State	Cause for Start	When to Stop	At the First Expiry	At the Second Expiry
T301	Call Delivered	An ALERT message is received.	A CONNECT message is received.	The call is deleted.	The timer is not restarted.
T302	Overlap receiving	An INFO message is received after a SETUP ACK message is sent.	An INFO message sending complete indication is received; or an acknowledgement that sufficient call information is received.	The call is cleared if call information is incomplete. Otherwise, a CALL PROCEEDING message is sent.	The timer is not restarted.
T303	Call Initiated	A SETUP message is sent.	A SETUP ACK, CALL PROC or RELEASE COMPLETE message is received.	A SETUP message is retransmitted, and T303 is restarted.	The internal connection is cleared; a RELEASE COMPLETE message is sent; the ISDN Layer 3 protocol enters the NULL state.

 Copyright © Huawei Technologies Co., Ltd.

Timer Number	Call State	Cause for Start	When to Stop	At the First Expiry	At the Second Expiry
T304	Overlap Sending	An INFO message is sent, and T304 is restarted when the INFO message is retransmitted.	A CALL PROC ALERT, CONNECT, or DISC message is received.	A DISC message is sent.	The timer is not restarted.
T305	Disconnect Request	A DISC message is sent.	An REL or a DISC message is received.	An REL message is sent.	The timer is not restarted.
T308	Release request	An REL message is sent.	An REL or REL COMPLETE message is received.	The REL message is retransmitted, and T308 is restarted.	The B channel enters the maintenance mode, and the call reference is released.
T309	Any stable state	The data link is disconnected, and calls in stable state are not lost.	The data link is reconnected.	The internal connection is cleared, and the B channel and call reference are released.	The timer is not restarted.
T310	Outgoing Call Proceeding	A CALL PROCEEDING message is received.	An ALERT, CONNECT, DISC, or PROGRESS message is received.	A DISC message is sent.	The timer is not restarted.
T313	Connect request	A CONNECT message is sent.	A CONNECT ACK message is received.	A DISC message is sent.	The timer is not restarted.

 Copyright © Huawei Technologies Co., Ltd.

Timer Number	Call State	Cause for Start	When to Stop	At the First Expiry	At the Second Expiry
T314	Receiving Segmented Message	The message segment is received.	The last message segment is received.	The message is discarded.	The timer is not restarted.
T316	Restart Request	A RESTART message is sent.	A RESTART ACK message is received.	The RESTART message can be retransmitted several times.	The RESTART message can be retransmitted several times.
T317	Restart	A RESTART message is received.	The call reference is internally cleared.	A maintenance notification is sent.	The timer is not restarted.
T318	Resume Request	An RES message is sent.	An RES ACK or RES REJ message is received.	The internal connection is cleared; the call reference is released; the NULL state is displayed.	The timer is not restarted.
T319	Suspend Request	A SUSPEND message is sent.	A SUSPEND ACK or SUSP REJ message is received.	The ISDN Layer 3 protocol enters the ACTIVE state and notifies the user application.	The timer is not restarted.
T321	Any call state	A fault occurs on the D channel.	Response to the Layer 3 message is received.	DL-ESTABLISH-REQ messages are sent on both D channels.	The timer is not restarted.

 Copyright © Huawei Technologies Co., Ltd.

Timer Number	Call State	Cause for Start	When to Stop	At the First Expiry	At the Second Expiry
T322	Any call state	A STATUS ENQ message is sent.	A STATUS, DISC, REL, or REL COM message is received.	The STATUS ENQ message can be retransmitted several times.	The STATUS ENQ message can be retransmitted several times.

Precautions

Values of ISDN Layer 3 timers on the device must be the same as those on an ISDN switch.

Example

Set the T301 timer to 180s on BRI1/0/0.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn l3-timer t301 180
```

Set the T301 timer to 180s on CE1/PRI interface Serial 1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn l3-timer t301 180
```

Related Topics

7.11.6 display isdn dss1-parameters

7.11.18 isdn link-mode

Function

The **isdn link-mode** command configures a BRI interface to work in point-to-point (P2P) mode.

The **undo isdn link-mode** command restores the default configuration.

By default, a BRI interface on a device works in point-to-multipoint (P2MP) mode.

Format

isdn link-mode p2p

undo isdn link-mode

Parameters

Parameter	Description	Value
p2p	Configures a BRI interface to work in P2P mode.	-

Views

ISDN BRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ISDN BRI interface on an ISDN user-side device is connected to an ISDN switch by using network terminal 1 (NT1). NT1 can provide multiple S/T interfaces so that an ISDN switch can connect to multiple ISDN user-side devices.

A device can function as an ISDN user-side device.

- To enable only one device to communicate with an ISDN switch, configure a BRI interface on the device to work in P2P mode.
- To enable multiple devices to communicate with an ISDN switch, configure each BRI interface to work in P2MP mode.

Precautions

An ISDN BRI interface on a device must work in the same mode as an ISDN BRI interface on an ISDN switch.

Example

Configure BRI1/0/0 to work in P2P mode.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn link-mode p2p
```

7.11.19 isdn number-property

Function

Using the **isdn number-property** command, you can set the type and encoding scheme of calling or called numbers in outgoing ISDN calls.

Using the **undo isdn number-property** command, you can restore the default configuration.

By default, the device selects the ISDN number type and encoding scheme depending on upper layer services.

Format

isdn number-property *number-property* [**calling** | **called**] [**out**]

undo isdn number-property [**calling** | **called**] [**out**]

Parameters

Parameter	Description	Value
number-property	Specifies the number type and encoding scheme.	The value ranges from 0x0 to 0x7F. If the value is in binary format, bits 1 to 4 specify the encoding scheme, bits 5 to 7 specify the number type, and bit 8 is the reserved bit. **Table 7-70** lists number types and encoding schemes. For details, see the related protocol.
calling	Specifies the fixed number type and encoding scheme for a calling number.	-
called	Specifies the fixed number type and encoding scheme for a called number.	-
out	Specifies the fixed number type and encoding scheme for a calling or called number in an outgoing call.	-

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

ISDN features supported by the device comply with Digital Subscriber Signaling System No.1 (DSS1). **Table 7-70** lists the ISDN number types and encoding schemes defined in DSS1.

Table 7-70 ISDN number types and encoding schemes

Protocol	Field (Bit) Value								Definition
	-	Number Type			Encoding Scheme				
	8	7	6	5	4	3	2	1	
DSS1	-	0	0	0	-	-	-	-	Unknown
	-	0	0	1	-	-	-	-	International number
	-	0	1	0	-	-	-	-	National number
	-	0	1	1	-	-	-	-	Network specific number
	-	1	0	0	-	-	-	-	Subscriber number
	-	1	1	0	-	-	-	-	Abbreviated number
	-	1	1	1	-	-	-	-	Reserved for extension
	-	-	-	-	0	0	0	0	Unknown
	-	-	-	-	0	0	0	1	ISDN/telephony numbering plan (Recommendation E.164)
	-	-	-	-	0	0	1	1	Data numbering plan (Recommendation X.121)
	-	-	-	-	0	1	0	0	Telex numbering plan (Recommendation F.69)
	-	-	-	-	1	0	0	0	National standard numbering plan
	-	-	-	-	1	0	0	1	Private numbering plan
	-	-	-	-	1	1	1	1	Reserved for extension

NOTE

Undefined bits in DSS1 are reserved.

Example

Set the type and encoding scheme of called numbers in outgoing ISDN calls to unknown on BRI1/0/0.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn number-property 0 called out
```

Set the type and encoding scheme of called numbers in outgoing ISDN calls to unknown on CE1/PRI interface Serial 1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serail1/0/0:15] isdn number-property 0 called out
```

7.11.20 isdn overlap-receiving

Function

Using the **isdn overlap-receiving** command, you can configure an ISDN interface to work in overlap receiving mode. In this mode, the called party starts establishing a connection only after it receives all the digits of the called number.

Using the **undo isdn overlap-receiving** command, you can restore the default configuration.

By default, an ISDN interface work in non-overlap receiving mode. The called party starts establishing a connection immediately after it receives some digits of the called number without waiting to receive all the digits of the called number.

Format

isdn overlap-receiving

undo isdn overlap-receiving

Parameters

None

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

In overlap receiving mode, the device, functioning as the called party, starts establishing a connection only after it receives all the digits of the called number.

- If the network-side device sends a message carrying the sending complete information element, the device supports the overlap receiving mode by default.
- If the network-side device sends a message that does not carry the sending complete information element, run the **isdn overlap-receiving** command so that the device can support the overlap receiving mode.

  In this situation, the time during which the device waits to receive the sending complete information element is determined by the T302 timer. The default value of the T302 timer is 15 seconds. You can run the **isdn l3-timer** command to set the T302 timer value.

Example

Configure Serial 1/0/0:15 to work in overlap receiving mode.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn overlap-receiving
```

Related Topics

7.11.21 isdn overlap-sending

7.11.21 isdn overlap-sending

Function

Using the **isdn overlap-sending** command, you can configure an ISDN interface to send a called number in overlap mode.

Using the **undo isdn overlap-sending** command, you can restore the default configuration.

By default, an ISDN interface sends a complete called number at a time.

Format

isdn overlap-sending [*digits*]

undo isdn overlap-sending

Parameters

Parameter	Description	Value
digits	Specifies the maximum number of digits to be sent in overlap mode at a time. If this parameter is not configured, a maximum of 10 digits of a called number can be sent at a time by default.	The value is an integer that ranges from 1 to 15.

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a remote ISDN switch cannot receive a complete called number or the maximum number of digits the ISDN switch allows is less than the number of digits of a called number, configure the device to send the called number in overlap mode. Otherwise, the device cannot establish a call with the ISDN switch.

When an ISDN interface is configured to send a called number in overlap mode, it sends the configured maximum number of bits at a time until all digits of the called number are sent.

Precautions

If you run the **isdn overlap-sending** command multiple times in the same interface view, only the latest configuration takes effect.

NOTE

Before running the **isdn overlap-sending** command on an ISDN interface, ensure that there is no call on the interface. Otherwise, this command does not take effect. Alternatively, run the **shutdown**, **isdn overlap-sending**, and **undo shutdown** commands on the ISDN interface to make the configuration take effect. Such operations, however, will disconnect existing calls on the ISDN interface.

Example

Configure Serial1/0/0:15 to send a maximum of five digits of a called number in overlap mode at a time.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn overlap-sending 5
```

Related Topics

7.11.20 isdn overlap-receiving

7.11.22 isdn pri-slipwnd-size

Function

Using the **isdn pri-slipwnd-size** command, you can set the sliding window size on an ISDN PRI interface.

By default, the sliding window size on an ISDN PRI interface is 7.

Format

isdn pri-slipwnd-size { *window-size* | **default** }

Parameters

Parameter	Description	Value
window-size	Specifies the sliding window size on an ISDN PRI interface.	The value ranges from 5 to 14.
default	Restores the sliding window size on an ISDN PRI interface to default value 7.	-

Views

ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The sliding window mechanism is used for flow control. In earlier network communication mechanisms, two communicating devices send data without checking whether network congestion occurs. If too many packets are sent at a time, the intermediate nodes are congested and packets are lost, causing a communication failure between the two devices. The sliding window mechanism is introduced to solve this problem.

The sliding window size specifies the maximum number of unacknowledged frames allowed on an interface that sends packets.

Precautions

- If you run the **isdn pri-slipwnd-size** command multiple times in the same interface view, only the latest configuration takes effect.
- A small sliding window size increases the packet loss ratio. Therefore, the default sliding window size is recommended.

Example

Set the sliding window size to 8 on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn pri-slipwnd-size 8
```

 Copyright © Huawei Technologies Co., Ltd.

7.11.23 isdn q921-permanent

Function

Using the **isdn q921-permanent** command, you can enable Q.921 automatic link establishment on an ISDN BRI interface.

Using the **undo isdn q921-permanent** command, you can restore the default configuration.

By default, Q.921 automatic link establishment is disabled on an ISDN BRI interface.

Format

isdn q921-permanent

undo isdn q921-permanent

Parameters

None

Views

ISDN BRI interface view

Default Level

2: Configuration level

Usage Guidelines

This command enables the link between two correctly connected interfaces to enter the MULTIPLE_FRAME_ESTABLISHED state without being triggered by any call.

After two ISDN PRI interfaces are correctly connected, the Q.921 layer performs negotiation and enters the MULTIPLE_FRAME_ESTABLISHED state without being triggered by any call. The Q.921 layer of an ISDN BRI interface enters the MULTIPLE_FRAME_ESTABLISHED state only when there is a call triggered.

To enable an ISDN BRI interface to enter the MULTIPLE_FRAME_ESTABLISHED state immediately after being correctly connected, run the **isdn q921-permanent** command on the interface.

Example

Enable BRI1/0/0 to enter the MULTIPLE_FRAME_ESTABLISHED state without being triggered by any call.

```
<Huawei> system-view
[Huawei] interface bri 1/0/0
[Huawei-Bri1/0/0] isdn q921-permanent
```

 Copyright © Huawei Technologies Co., Ltd.

7.11.24 isdn send-restart

Function

Using the **isdn send-restart** command, you can enable ISDN PRI interfaces to actively send RESTART messages.

Using the **undo isdn send-restart** command, you can disable ISDN PRI interfaces from actively sending RESTART messages.

By default, ISDN PRI interfaces actively send RESTART messages.

Format

isdn send-restart

undo isdn send-restart

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Faults may occur during the release of a call, causing a call release failure. If an ISDN PRI interface is configured to actively send RESTART messages to a network-side device, the network-side device sets all calls to the NULL state and all B channels to the IDLE state after receiving a RESTART message from the PRI interface.

Example

Disable ISDN PRI interfaces to actively send RESTART messages to a remote device.

```
<Huawei> system-view
[Huawei] undo isdn send-restart
```

7.11.25 isdn statistics

Function

Using the **isdn statistics** command, you can configure the statistics function on an ISDN interface.

By default, message statistics on an ISDN interface are not collected.

 Copyright © Huawei Technologies Co., Ltd.

Format

isdn statistics { **clear** | **continue** | **display** [**flow**] | **start** | **stop** }

Parameters

Parameter	Description	Value
clear	Clears message statistics on an ISDN interface.	-
continue	Continues collecting message statistics on an ISDN interface.	-
display [**flow**]	Displays statistics on an ISDN interface. If the **flow** parameter is specified, statistics on an ISDN interface are displayed in flow format.	-
start	Starts collecting message statistics on an ISDN interface.	-
stop	Stops collecting message statistics on an ISDN interface.	-

Views

ISDN BRI interface view, ISDN PRI interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can view the message exchange process to locate ISDN faults.

The usage of this command is as follows:

- Before collecting message statistics on an interface, run the **isdn statistics start** command in the ISDN interface view.
- To stop collecting message statistics, run the **isdn statistics stop** command.
- To view message statistics, run the **isdn statistics display** command.
- To view message statistics in flow format, run the **isdn statistics display flow** command.

 Copyright © Huawei Technologies Co., Ltd.

- To continue collecting message statistics after stopping collecting message statistics, run the **isdn statistics continue** command.
- To clear message statistics, run the **isdn statistics clear** command.

Precautions

Message statistics must be collected on the link where a call has been established.

Example

Start collecting message statistics on Serial1/0/0:15.

```
<Huawei> system-view
[Huawei] interface serial 1/0/0:15
[Huawei-Serial1/0/0:15] isdn statistics start
```

After a period of time, stop collecting message statistics on Serial1/0/0:15.

```
[Huawei-Serial1/0/0:15] isdn statistics stop
```

Display message statistics on Serial1/0/0:15.

```
[Huawei-Serial1/0/0:15] isdn statistics display
Q.931 message received and sent out on current port:
CALL_PROC        Send(0)          Recv(1)
SETUP            Send(1)          Recv(0)
CONN             Send(0)          Recv(1)
CONNECT_ACK      Send(1)          Recv(0)
DISCONNECT       Send(1)          Recv(0)
RELEASE          Send(0)          Recv(1)
RELEASE_COM      Send(1)          Recv(0)
```

NOTE

The displayed message statistics include message types and the numbers of messages sent and received on the ISDN interface. Numbers in round brackets specify the number of times that the interface sends or receives a specific message.

Clear message statistics on Serial1/0/0:15.

```
[Huawei-Serial1/0/0:15] isdn statistics clear
[Huawei-Serial1/0/0:15] isdn statistics display
No statistic information
```

7.11.26 permanent-active

Function

The **permanent-active** command sets the physical layer status of an ISDN BRI interface to permanently active.

The **undo permanent-active** command restores the default physical layer status of an ISDN BRI interface.

By default, the physical layer status of an ISDN BRI interface stays inactive.

Format

permanent-active

undo permanent-active

Parameters

None

Views

ISDN BRI interface view

Default Level

2: Configuration level

Usage Guidelines

The physical layer status of an ISDN BRI interface can stay permanently active or inactive.

- If the physical layer status of an ISDN BRI interface is permanently active, the physical layer automatically becomes Up.
- If the physical layer status of an ISDN BRI interface is inactive, the physical layer becomes Up only when services are forwarded on the ISDN BRI interface. In other cases, the physical layer becomes Up or Down according to the activation or deactivation operations on the ISDN network-side device.

The physical layer status of an ISDN BRI interface must be the same as that of the ISDN network-side device.

Example

Set the physical layer status of an ISDN BRI interface to permanently active.

```
<Huawei> system-view
[Huawei] interface bri 2/0/0
[Huawei-Bri2/0/0] permanent-active
```

7.12 Modem Configuration Commands

NOTE

Currently, only the asynchronous serial interfaces on the 8AS board support the modem function.

7.12.1 modem

Function

The **modem** command sets modem call-in and call-out permissions.

The **undo modem** command restores the default setting.

By default, the device does not allow modem call-in or call-out.

Format

modem [**both** | **call-in**]

undo modem [**both** | **call-in**]

Parameters

Parameter	Description	Value
both	Allows both modem call-in and call-out.	-
call-in	Allows only modem call-in.	-

Views

TTY user interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable the routers communicate with each other over the PSTN through a modem, set modem call-in and call-out permissions in the user interface view. Generally, configure the calling router to allow modem call-in and call-out and the called router to allow only modem call-in.

Precautions

This command is valid only for async interfaces.

When no parameter is specified in the **modem** command, both modem call-in and call-out are allowed.

Example

Configure the device to allow only modem call-in.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] modem call-in
```

7.12.2 modem auto-answer

Function

The **modem auto-answer** command configures a modem to work in auto-answer mode.

The **undo modem auto-answer** command restores the default configuration.

By default, a modem works in non-auto answer mode. In this case, the device sends AT commands to enable a modem to answer calls.

Format

modem auto-answer

undo modem auto-answer

Parameters

None

Views

TTY user interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- You are advised to set the modem answer mode on the device to be the same as the answer mode of the modem connecting to the device. If the modem works in auto-answer mode (the AA indicator of the modem is on), run the modem auto-answer command to prevent a router from sending response instructions after the auto-answer mode is configured. If the modem works in non-auto answer mode, run the **undo modem auto-answer** command.
- The modem answer mode configured on a router must be the same as the answer mode of the modem connected to the router. If the two answer modes are different, the modem may fail to function properly.

Precautions

This command is valid only for async interfaces.

Example

Configure a modem to work in auto-answer mode.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] modem auto-answer
```

Related Topics

7.12.1 modem

7.12.3 modem timer answer

Function

The **modem timer answer** command sets the modem answer timeout period.

The **undo modem timer answer** command restores the default modem answer timeout period.

 Copyright © Huawei Technologies Co., Ltd.

By default, the modem answer timeout period is 30s.

Format

modem timer answer *seconds*

undo modem timer answer

Parameters

Parameter	Description	Value
seconds	Specifies the modem answer timeout period.	The value is an integer that ranges from 1 to 60, in seconds.

Views

TTY user interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The modem answer timeout period refers to the period between picking up a phone and dialing a number.

Precautions

This command is valid only for async interfaces.

Example

Set the modem answer timeout period to 40 seconds.

```
<Huawei> system-view
[Huawei] user-interface tty 1
[Huawei-ui-tty1] modem timer answer 40
```

7.12.4 sendat

Function

The **sendat** command configures the device to send an AT command to a modem.

Format

sendat *at-string*

Parameters

Parameter	Description	Value
at-string	Specifies an AT command string.	The value is a string of 1 to 127 case-insensitive characters with spaces. The value can be **+++**, **A/**, or any string starting with AT.

Views

Async interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device sends entered strings to a modem as AT commands without checking the validity of these commands. In the strings, lowercase letters are automatically converted to uppercase letters. If the modem debugging of an Async interface is enabled, the result codes returned from the modem are displayed. If the modem is configured to return AT commands, the executed AT commands are displayed too.

Table 7-71 Common AT commands

Command	Description
A	Answer command, which enables a modem to answer an incoming call without waiting for the ringing. Use this command when a modem is configured to work in non-auto answer mode or to connect to another modem actively. All the commands following the A command in the same command line will be ignored.
Bn	Communication standards (ITU or Bell): ● B0: The communication standard is ITU V.22 and the transmission rate is 1200 bps. ● B1: The communication standard is Bell 212 and the transmission rate is 1200 bps. ● B2 or B3: The ITU V.23 reverse path is disabled. ● B15: The communication standard is ITU V.21 and the transmission rate is 300 bps. ● B16: The communication standard is 103J and the transmission rate is 300 bps.

 Copyright © Huawei Technologies Co., Ltd.

Command	Description
En	Echo command, indicating whether to display the entered strings locally. ● E0: The entered strings are not displayed locally. ● E1: The entered strings are displayed locally.
Dn	Dial command, instructing a modem to dial the number following D in the command line. In pulse dialing mode, only digits are allowed.
Hn	Mode in which a modem hangs up a call. ● H0: A modem disconnects a call to hang up the call. ● H1: A modem picks up the phone and occupies the telephone line to hang up a call. By default, a modem disconnects a call to hang up the call.
Ln	Speaker volume for fax and data communication. ● L0 or L1: low volume ● L2: medium volume ● L3: high volume By default, medium volume is used.
Mn	Speaker options for fax and data communication. ● M0: The speaker is always turned off. ● M1: After a number is dialed, the speaker is always on until the carrier signal is detected. ● M2: The speaker is always on when the modem is off-hook. ● M3: The speaker is always on after a number is dialed until the carrier signal is detected. By default, M1 is used.
Nn	Whether to perform negotiation when the local modem tries to establish a connection with a remote modem operating at a different transmission rate. ● N0: The communication standard specified by the S37 register and the ATB commands is used when a call is initiated or answered. ● N1: The transmission rate specified by the S37 register and ATB commands is used for negotiation when a call is initiated or answered. During the negotiation, the transmission rate may reduce. By default, N1 is used.

 Copyright © Huawei Technologies Co., Ltd.

Command	Description
On	Forces a modem to enter the connect state. ● O0: The modem enters the connect state. ● O1: A retrain sequence begins before the modem returns to the connect state. ● O3: The transmission rate is negotiated again before the modem returns to the connect state. **NOTE** This command causes a modem to return to the connect state after you switch to the command mode by executing the +++ command.
R	Enables a modem to enter the answer mode after a number is dialed.
Sr=n	Writes data n into the S register numbered r. ● r: register ID, which can be 0 through 27, 29, 31 through 33, 35, 37, and 89 ● n: value to be assigned to the register, which ranges from 0 to 255.
T	Tone dialing. By default, tone dialing is used.

Precautions

- Using AT commands to configure a modem may cause the incorrect modem status, affecting the dialing function. Therefore, use this command under instruction of technical personnel.
- The **sendat** command can specify only one AT command at a time. If you specify more than one AT command, the configuration will fail.

Example

Configure the device to send the **ATD152** command to the modem, enabling the modem to call number 152.

```
<Huawei> system-view
[Huawei] interface async 2/0/0
[Huawei-Async2/0/0] sendat ATD152
```

7.12.5 service modem-callback

Function

The **service modem-callback** command enables the user callback function.

The **undo service modem-callback** command disables the user callback function.

By default, the user callback function is disabled.

Format

service modem-callback

undo service modem-callback

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the user callback function.

```
<Huawei> system-view
[Huawei] service modem-callback
```

7.13 RTC Configuration Commands

NOTE

Only the AR2204XE, AR2204XE-DC, AR2220L, AR2220E, AR2240C, and routers using SRU40, SRU100, SRU100E, and SRU400 support the RTC.

7.13.1 auto-close

Function

The **auto-close** command sets an interval for automatically closing a TCP connection in a terminal template view.

The **undo auto-close** restores the default interval for automatically closing a TCP connection.

By default, the interval for automatically closing a TCP connection is 0 seconds, that is, the system is not configured to automatically close a TCP connection.

Format

auto-close *time*

undo auto-close

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time	Specifies the interval for automatically closing a TCP connection.	The value is an integer that ranges from 5 to 240, in seconds. The default value is 0. That is, the system is not configured to automatically close a TCP connection.

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

RTC supports the automatic TCP connection close function. You can run the **auto-close** *time* command to set an interval for automatically closing a TCP connection in the terminal template view.

- After the interval is set, when no data is exchanged between the monitoring terminal and the RTC client, the RTC client automatically disconnects the TCP connection with the RTC server after the specified interval, which saves bandwidth.
- When the interval is 0 seconds, the TCP connection between the RTC client and server is always remained even if no data is exchanged between the monitoring terminal and the RTC client.

Example

Set the interval for automatically closing a TCP connection in **template1** to 10s.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] auto-close 10
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.2 auto-link

7.13.2 auto-link

Function

The **auto-link** command sets an interval for automatically setting up a TCP connection in a terminal template view.

 Copyright © Huawei Technologies Co., Ltd.

The **undo auto-link** command restores the default interval for automatically setting up a TCP connection.

By default, the interval for automatically setting up a TCP connection is 0 seconds, that is, the system is not configured to automatically set up a TCP connection.

Format

auto-link *time*

undo auto-link

Parameters

Parameter	Description	Value
time	Specifies the interval for automatically setting up a TCP connection.	The value is an integer that ranges from 5 to 240, in seconds. The default value is 0. That is, the system is not configured to automatically set up a TCP connection.

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

RTC supports the automatic TCP connection setup function. You can run the **auto-link** *time* command to set an interval for automatically setting up a TCP connection in the terminal template view.

- After the interval is set and the physical link between routers is working properly, a router automatically sets up a TCP connection with the peer router after the specified interval even if no data traffic is exchanged.
- If the interval is 0 seconds, the RTC client sets up a TCP connection with the RTC server only when the monitoring terminal sends a data exchange request to the RTC client.

Example

Set the interval for automatically setting up a TCP connection in **template1** to 10s.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] auto-link 10
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template
7.13.1 auto-close

7.13.3 display rta

Function

The **display rta** command displays RTC information.

Format

display rta { **all** | **statistics** | *terminal-number* { **brief** | **statistics** | *vty-number* } }

Parameters

Parameter	Description	Value
all	Displays information about all terminal connections.	-
statistics	Displays terminal statistics.	-
terminal-number	Displays information about a terminal with a specified number.	The value is an integer that ranges from 1 to 255.
brief	Displays brief information about a terminal with a specified number.	-
vty-number	Displays information about a VTY with a specified number.	The value is an integer that ranges from 0 to 7.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display brief information about TTY 1.

```
<Huawei> display rta 1 brief
 TTY 1
 ---------------------------------------
```

```
 Interface Used: Serial1/0/0
 Interface IfIndex: 69
 Current State: OK
 Total VTY Number: 1
 Current VTY: 0
 Socket RecvBuf Size: 16384
 Socket SendBuf Size: 16384
 KeepAliveTime: 10
 KeepAliveCount: 2
 Nodelay: 0
 AutoCloseTime: 10
 AutoLinkTime: 10
 AutoLinkTimerID: 572
 AutoCloseTimerID: 4294967295
--------------------------------------
```

Table 7-72 Description of the display rta 1 brief command output

Item	Description
TTY	TTY number.
Interface Used	Name of the synchronous serial port bound to the RTC terminal template.
Interface IfIndex	Interface index.
Current State	Current status of the connection: ● Down: The physical link is Down. ● OK: The terminal connection is normal. ● Menu: The terminal connection is in Menu state.
Total VTY Number	Total number of VTYs.
Current VTY	Number of the current VTY.
Socket RecvBuf Size	Buffer size for receiving TCP packets. To set the buffer size for receiving TCP packets, run the **tcp recvbuf-size** command.
Socket SendBuf Size	Buffer size for sending TCP packets. To set the buffer size for sending TCP packets, run the **tcp sendbuf-size** command.
KeepAliveTime	Interval for sending TCP keepalive packets. To set the interval for sending TCP keepalive packets, run the **tcp keepalive** command.
KeepAliveCount	Number of times TCP keepalive packets are retransmitted. To set the number of times the TCP keepalive packets are retransmitted, run the **tcp keepalive** command.
Nodelay	Status of the TCP_NODELAY option. To set the status of the TCP_NODELAY option, run the **tcp nodelay** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AutoCloseTime	Interval for automatically closing a TCP connection. To set the interval for automatically closing a TCP connection, run the **auto-close** command.
AutoLinkTime	Interval for automatically setting up a TCP connection. To set the interval for automatically setting up a TCP connection, run the **auto-link** command.
AutoLinkTimerID	Timer for automatically setting up a TCP connection.
AutoCloseTimerID	Timer for automatically closing a TCP connection.

Display terminal statistics.

```
<Huawei> display rta statistics
 RTA Template Number: 1
 RTA TTY Number: 1
 RTA APP Number: 1
 RTA Listen Port Number: 0
```

Table 7-73 Description of the display rta statistics command output

Item	Description
RTA Template Number	Number of RTC terminal templates.
RTA TTY Number	Number of RTC TTYs.
RTA APP Number	Number of applications generated on terminals.
RTA Listen Port Number	Number of ports setting up TCP connections.

Display information about VTY 0 on TTY 1.

```
<Huawei> display rta 1 0
 TTY 1  VTY 0
 -----------------------------------
   APP Index: 1
   APP Type: RTC-Client
   APP Name: <null>
   APP State: Linked
   Remote IP: 1.1.1.2
   Local IP: 1.1.1.1
   Source IP: 0.0.0.0
   Remote Port: 9000
   Local Port: 58863
   SndQueLength: 0
   RcvQueLength: 0
   CurrentRcvDateLen: 0
 -----------------------------------
```

Table 7-74 Description of the display rta 1 0 command output

Item	Description
TTY 1	TTY number.
VTY 0	VTY number.
APP Index	Application index.
APP Type	Application type: ● RTC-Client ● RTC-Server
APP Name	Application name. If the application name is not set, <null> is displayed.
APP State	Application status: ● Kept: The TCP connection is not set up. ● Linking: The TCP connection is being set up. ● Linked: The TCP connection is set up.
Remote IP	IP address of the peer end on the TCP connection.
Local IP	IP address of the local end on the TCP connection.
Source IP	Source IP address.
Remote Port	Number of the remote port on the TCP connection.
Local Port	Number of the local port on the TCP connection.
SndQueLength	Length of the current sending queue.
RcvQueLength	Length of the current receiving queue.
CurrentRcvDateLen	Length of the current buffer for receiving remote data.

Display statistics on TTY 1.

```
<Huawei> display rta 1 statistics
 TTY 1
   Receive from terminal: 429324 packets, 38639160 bytes
   Send to terminal: 429323 packets, 52377406 bytes
   Receive from remote: 429323 packets, 40356362 bytes
   Send to remote: 429324 packets, 40356456 bytes


   VTY 0
     Receive from terminal: 429324 packets, 38639160 bytes
     Send to terminal: 429323 packets, 52377406 bytes
     Receive from remote: 429323 packets, 40356362 bytes
     Send to remote: 429324 packets, 40356456 bytes
```

Table 7-75 Description of the display rta 1 statistics command output

Item	Description
Receive from terminal	Size of the data received from the terminal.
Send to terminal	Size of the data sent to the terminal.
Receive from remote	Size of the data received from the remote end.
Send to remote	Size of the data sent to the remote end.

Related Topics

7.13.14 tcp recvbuf-size
7.13.15 tcp sendbuf-size
7.13.11 tcp keepalive
7.13.12 tcp nodelay
7.13.1 auto-close
7.13.2 auto-link

7.13.4 reset rta statistics

Function

The **reset rta statistics** command deletes statistics on an RTC terminal.

Format

reset rta statistics *terminal-number*

Parameters

Parameter	Description	Value
terminal-number	Deletes statistics on the RTC terminal with a specified number.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

During routine maintenance, before recollecting statistics about an RTC terminal, run this command to delete existing terminal statistics.

NOTICE

RTC terminal statistics cannot be restored after being deleted. Confirm the action before running this command.

Example

Delete statistics on RTC terminal 1.

```
<Huawei> reset rta statistics 1
```

7.13.5 rta broadcast master-interface enable

Function

The **rta broadcast master-interface enable** command configures an interface on an RTC client as an interface-level broadcast master interface.

The **undo rta broadcast master-interface enable** command restores default settings of an interface on an RTC client.

By default, an interface is not configured as an interface-level broadcast master interface.

Format

rta broadcast master-interface enable

undo rta broadcast master-interface enable

Parameters

None

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

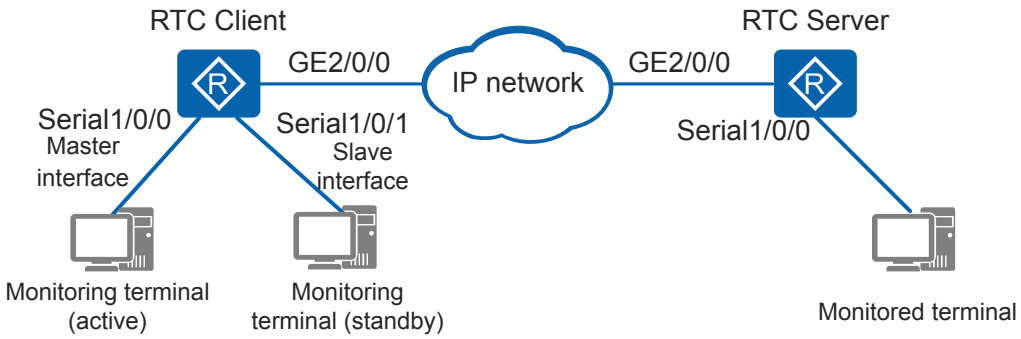
Usage Scenario

This command applies to an RTC client. As shown in the RTC scenario in **Figure 7-1**, monitoring terminals and a remote monitored terminal connect to routers through synchronous serial interfaces. The routers exchange data through an IP

network. The monitored terminal collects data in real time, responds promptly to data requests from monitoring terminals, and sends monitoring data to the monitoring terminals.

To back up monitoring data received by monitoring terminals, you can configure the interface-level broadcast function on the RTC client, run the **rta broadcast master-interface enable** command to configure a master interface, and run the **rta broadcast slave-interface** command to configure a slave interface. Monitoring data received by the monitoring terminal connected to the master interface is backed up to the monitoring terminal connected to the slave interface.

Figure 7-1 Networking diagram for configuring interface-level broadcast on the RTC client



Prerequisites

The following operations must have been performed before this command is run:

- Run the **vty** *vty-number* **rtc-client remote** *ip-address port-number* [**source** *source-ip*] command in an RTC terminal template to configure RTC client VTYs.
- Run the **rta terminal** *template-name terminal-number* command on the router's synchronous serial interface to bind the RTC terminal template to the interface.

Example

Configure Serial1/0/0 as an interface-level broadcast master interface.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] vty 1 rtc-client remote 10.10.10.10 9010
[Huawei-rta-template-template1] quit
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol hdlc
[Huawei-Serial1/0/0] rta terminal template1 1
[Huawei-Serial1/0/0] rta broadcast master-interface enable
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.16 vty rtc-client remote

7.13.10 rta terminal

7.13.6 rta broadcast slave-interface

7.13.6 rta broadcast slave-interface

Function

The **rta broadcast slave-interface** command configures an interface on an RTC client as an interface-level broadcast slave interface.

The **undo rta broadcast slave-interface** command restores default settings of an interface on an RTC client.

By default, an interface is not configured as an interface-level broadcast slave interface.

Format

rta broadcast slave-interface *terminal-number*

undo rta broadcast slave-interface *terminal-number*

Parameters

Parameter	Description	Value
terminal-number	Specifies the RTC terminal number configured on the interface-level broadcast master interface. **NOTE** The value of this parameter must be the same as the RTC terminal number in the RTC terminal template bound to the master interface using the **rta terminal** *template-name terminal-number* command.	The value is an integer that ranges from 1 to 255.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

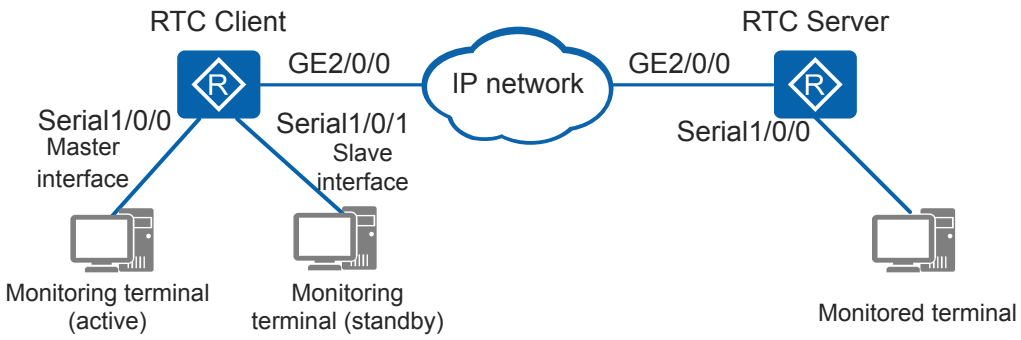
Usage Scenario

This command applies to an RTC client. As shown in the RTC scenario in **Figure 7-2**, monitoring terminals and a remote monitored terminal connect to routers through synchronous serial interfaces. The routers exchange data through an IP network. The monitored terminal collects data in real time, responds promptly to data requests from monitoring terminals, and sends monitoring data to the monitoring terminals.

To back up monitoring data received by monitoring terminals, you can configure the interface-level broadcast function on the RTC client, run the **rta broadcast**

master-interface enable command to configure a master interface, and run the **rta broadcast slave-interface** command to configure a slave interface. Monitoring data received by the monitoring terminal connected to the master interface is backed up to the monitoring terminal connected to the slave interface.

Figure 7-2 Networking diagram for configuring interface-level broadcast on the RTC client



Prerequisites

The following operations must have been performed before this command is run:

- Run the **rta terminal** *template-name terminal-number* command on the router's master interface to bind an RTC terminal template to the interface.
- Run the **link-protocol hdlc** command on the router's slave interface to configure HDLC as the link layer protocol.

Precautions

Before this command is run, no terminal template can be bound to an interface configured as an interface-level broadcast slave interface.

An RTC terminal template supports a maximum of eight interface-level broadcast slave interfaces, that is, you can configure a maximum of eight interface-level broadcast slave interfaces for an interface-level broadcast master interface.

Example

Configure Serial1/0/1 as an interface-level broadcast slave interface.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] vty 1 rtc-client remote 10.10.10.10 9010
[Huawei-rta-template-template1] quit
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol hdlc
[Huawei-Serial1/0/0] rta terminal template1 1
[Huawei-Serial1/0/0] rta broadcast master-interface enable
[Huawei-Serial1/0/0] quit
[Huawei] interface serial 1/0/1
[Huawei-Serial1/0/1] link-protocol hdlc
[Huawei-Serial1/0/1] rta broadcast slave-interface 1
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template
7.13.16 vty rtc-client remote
7.13.17 vty rtc-server remote
7.13.5 rta broadcast master-interface enable

7.13.7 rta rtc-server listen-port

Function

The **rta rtc-server listen-port** command sets the TCP port number on an RTC server.

The **undo rta rtc-server listen-port** command deletes the TCP port number on an RTC server.

By default, the TCP port number is not set on an RTC server.

Format

rta rtc-server listen-port *port-number*

undo rta rtc-server listen-port *port-number*

Parameters

Parameter	Description	Value
port-number	Specifies the TCP port number on an RTC server.	The value is an integer that ranges from 1024 to 50000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the RTC server. After you run this command to set the TCP port number on an RTC server, the RTC server can receive all TCP connection requests destined for this port from an RTC client. The RTC server can receive TCP connection requests only when the port specified by the RTC client exists on the RTC server. After a TCP connection is set up, the RTC server sends the monitored data to the RTC client.

Prerequisites

The RTC function has been enabled using the **rta server enable** command.

Precautions

As an RTC server, a router supports only one port for setting up a TCP connection.

Example

Set TCP port number on an RTC server to 9010.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta rtc-server listen-port 9010
```

Related Topics

7.13.8 rta server enable

7.13.8 rta server enable

Function

The **rta server enable** command enables the RTC function on a router.

The **undo rta server enable** command disables the RTC function on a router.

By default, RTC is disabled on a router.

Format

rta server enable

undo rta server enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Many enterprises, such as the civil aviation system and banks, require real-time monitoring and unified management on terminal data (such as data on radars and front end processors). This requires data exchange between monitoring terminals and monitored terminals.

Terminals exchange data using HDLC packets, which cannot be transmitted on IP networks. After routers are configured with RTC, HDLC packets from the monitored terminal (such as the front end processor or radar) are encapsulated into TCP packets by the connected router. The router sets up a TCP connection

with the peer router across the IP network and transmits the TCP packets to the peer router. The peer router decapsulates the TCP packets into HDLC packets and sends them to the monitoring terminal. HDLC packets are transparently transmitted across the IP network.

Subsequent configurations such as the RTC terminal template can take effect only after RTC is enabled.

Precautions

After the **undo rta server enable** command is executed, RTC is disabled on all terminals, but configurations such as the RTC terminal template are kept.

Example

Enable RTC on the router.

```
<Huawei> system-view
[Huawei] rta server enable
```

7.13.9 rta template

Function

The **rta template** command creates an RTC terminal template and enters the RTC terminal template view. If the specified RTC terminal template exists, the RTC terminal template view is displayed.

The **undo rta template** command deletes an RTC terminal template.

By default, no RTC terminal template is configured.

Format

rta template *template-name*

undo rta template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an RTC terminal template.	The value is a string of 1 to 15 case-sensitive characters without spaces. The value contains digits, letters, underlines (_), and dots (.).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TCP connection is set up between an RTC client and an RTC server, the RTC server can send data on the monitored terminal to the RTC client. After creating an RTC terminal template on the RTC client or server, you can set TCP connection parameters in the RTC terminal template.

Prerequisites

The RTC function has been enabled using the **rta server enable** command.

Follow-up Procedure

- Run the **vty rtc-client remote** command on the RTC client to configure VTYs.
- Run the **vty rtc-server remote** command on the RTC server to configure VTYs.

Example

Create an RTC terminal template **template1** and enter the RTC terminal template view.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1]
```

Related Topics

7.13.8 rta server enable

7.13.16 vty rtc-client remote

7.13.17 vty rtc-server remote

7.13.10 rta terminal

Function

The **rta terminal** command binds an RTC terminal template to a serial interface.

The **undo rta terminal** command deletes an RTC terminal template bound to a serial interface.

By default, no RTC terminal template is bound to a serial interface.

Format

rta terminal *template-name terminal-number*

undo rta terminal

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
template-name	Specifies the name of an RTC terminal template.	The value is a string of 1 to 15 case-sensitive characters without spaces. The value contains digits, letters, underlines (_), and dots (.).
terminal-number	Specifies the RTC terminal number.	The value is an integer that ranges from 1 to 255.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A monitoring terminal and a monitored terminal connect to routers both through synchronous serial interfaces. Routers exchange data across an IP network. To allow the IP network to transparently transmit HDLC packets, run the **rta terminal** *template-name terminal-number* command on a synchronous serial interface to bind an RTC terminal template to the port.

Prerequisites

The following operations must have been performed before this command is used:

- Run the **rta template** *template-name* command on the RTC client or server to create an RTC terminal template and set TCP connection parameters.
- Run the **link-protocol hdlc** command on the synchronous serial interface to configure HDLC encapsulation.

Precautions

An RTC terminal template can be bound to the following interfaces on a router:

- Synchronous or asynchronous serial interface. The interface name is **Serial**. An RTC terminal template can be bound to only a synchronous serial interface. You need to run the **physical-mode sync** command to specify the serial interface to work in synchronous mode.
- Interfaces formed by CE1/CT1 and CE3 interfaces. The interface name is **Serial** and the interface logic is the same as that of synchronous serial interfaces.
- Interfaces formed by E1-F and T1-F interfaces. The interface name is **Serial** and the interface logic is the same as that of synchronous serial interfaces.
- Interfaces formed by E1/T1 interfaces that are channelized from CPOS interfaces. The interface name is **Serial** and the interface logic is the same as that of synchronous serial interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure an RTC terminal template **template1** on Serial 1/0/0 and set the RTC terminal number to 1.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] quit
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol hdlc
[Huawei-Serial1/0/0] rta terminal template1 1
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.16 vty rtc-client remote

7.13.17 vty rtc-server remote

7.13.11 tcp keepalive

Function

The **tcp keepalive** command sets the interval for and the number of times for sending TCP keepalive packets.

The **undo tcp keepalive** command restores the default parameters for sending TCP keepalive packets.

By default, TCP keepalive packets are sent every 50s, and the number of retransmissions is 3.

Format

tcp keepalive *time count*

undo tcp keepalive

Parameters

Parameter	Description	Value
keepalive *time*	Specifies the interval for sending TCP keepalive packets.	The value is an integer that ranges from 10 to 7200, in seconds. The default value is 50.
count	Specifies the number of times the TCP keepalive packets are retransmitted.	The value is an integer that ranges from 1 to 100. The default value is 3.

Views

Terminal template view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TCP connection is set up between an RTC client and an RTC server, the RTC server can send data on the monitored terminal to the RTC client. The two ends of the TCP connection must send TCP keepalive packets to check reliability of the TCP connection.

- If one end receives a response from the peer end after sending a TCP keepalive packet, the TCP connection is normal.
- If one end receives no response from the peer end after the specified interval, the end resends a TCP keepalive packet. If no response is received after the specified number of retransmissions, the TCP connection is closed. The two ends need to reestablish a TCP connection.

Precautions

After setting TCP connection parameters, you must reestablish a TCP connection (in automatic mode or triggered by traffic) to make the settings take effect.

Example

Set the interval for sending TCP keepalive packets to 60s and the number of retransmissions to 6 in the RTC terminal template **template1**.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] tcp keepalive 60 6
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.17 vty rtc-server remote

7.13.12 tcp nodelay

Function

The **tcp nodelay** command disables a TCP connection from using the Nagle's algorithm.

The **undo tcp nodelay** command enables a TCP connection to use the Nagle's algorithm.

By default, a TCP connection uses the Nagle's algorithm.

Format

tcp nodelay

 Copyright © Huawei Technologies Co., Ltd.

undo tcp nodelay

Parameters

None

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TCP connection is set up between an RTC client and an RTC server, the RTC server can send data on the monitored terminal to the RTC client. During the TCP connection setup, the Nagle's algorithm complying with RFC 896 is used to prevent network congestion caused by a large number of TCP packets on the network. However, the Nagle's algorithm causes delays in receiving and sending TCP packets, which are unbearable during data exchange. When the number of TCP packets cannot cause network congestion, you can run the **tcp nodelay** command to disable TCP connections from using the Nagle's algorithm to reduce delays in receiving and sending TCP packets.

Precautions

After setting TCP connection parameters, you must reestablish a TCP connection (in automatic mode or triggered by traffic) to make the settings take effect.

Example

Disable TCP connections in the RTC terminal template **template1** from using the Nagle's algorithm.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] tcp nodelay
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.17 vty rtc-server remote

7.13.13 tcp nodelay enhance

Function

The **tcp nodelay enhance** command enables the low-latency enhancement function of TCP connections.

 Copyright © Huawei Technologies Co., Ltd.

The **undo tcp nodelay enhance** command disables the low-latency enhancement function of TCP connections.

By default, the low-latency enhancement function of TCP connections is disabled.

Format

tcp nodelay enhance

undo tcp nodelay enhance

Parameters

None

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an RTC terminal access scenario, an RTC client exchanges information with an RTC server through a TCP connection. When a low packet latency or jitter is required, the low-latency enhancement function of TCP connections needs to be enabled.

Precautions

The low-latency enhancement function of TCP connections takes effect only when the **tcp nodelay enhance** command is configured on both the RTC client and RTC server.

Prerequisites

The interval for automatically setting up a TCP connection has been configured using the **auto-link** *time* command.

Example

Enable the low-latency enhancement function of TCP connections.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] auto-link 10
[Huawei-rta-template-template1] tcp nodelay enhance
Warning: This command must be configured on both the client and server. continue? [y/n]:y
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.17 vty rtc-server remote

7.13.14 tcp recvbuf-size

Function

The **tcp recvbuf-size** command sets the buffer size for receiving TCP packets.

The **undo tcp recvbuf-size** command restores the default buffer size for receiving TCP packets.

By default, the buffer size for receiving TCP packets is 20480 bytes.

Format

tcp recvbuf-size *recvsize*

undo tcp recvbuf-size

Parameters

Parameter	Description	Value
recvbuf-size *recvsize*	Specifies the buffer size for receiving TCP packets.	The value is an integer that ranges from 2048 to 40960, in bytes. The default value is 20480.

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TCP connection is set up between an RTC client and an RTC server, the RTC server can send data on the monitored terminal to the RTC client. You can run the **tcp recvbuf-size** command to set the buffer size for receiving TCP packets based on the device performance and delay requirement.

- If the device has good performance and requires low-delay transmission of data packets, use a small buffer size so that the device forwards data in real time.
- If the device has common performance and does not require low-delay transmission of data packets, use a large buffer size. TCP packets are stored in the buffer and are not sent until the buffer is full.

Precautions

After setting TCP connection parameters, you must reestablish a TCP connection (in automatic mode or triggered by traffic) to make the settings take effect.

Example

Set the buffer size for receiving TCP packets in **template1** to 5120 bytes.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] tcp recvbuf-size 5120
```

Related Topics

7.13.8 rta server enable
7.13.9 rta template
7.13.17 vty rtc-server remote

7.13.15 tcp sendbuf-size

Function

The **tcp sendbuf-size** command sets the buffer size for sending TCP packets.

The **undo tcp sendbuf-size** command restores the default buffer size for sending TCP packets.

By default, the buffer size for sending TCP packets is 20480 bytes.

Format

tcp sendbuf-size *sendsize*

undo tcp sendbuf-size

Parameters

Parameter	Description	Value
sendbuf-size *sendsize*	Specifies the buffer size for sending TCP packets.	The value is an integer that ranges from 2048 to 40960, in bytes. The default value is 20480.

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TCP connection is set up between an RTC client and an RTC server, the RTC server can send data on the monitored terminal to the RTC client. You can run the **tcp sendbuf-size** command to set the buffer size for sending TCP packets based on the device performance and delay requirement.

- If the device has good performance and requires low-delay transmission of data packets, use a small buffer size so that the device forwards data in real time.
- If the device has common performance and does not require low-delay transmission of data packets, use a large buffer size. TCP packets are stored in the buffer and are not sent until the buffer is full.

Precautions

After setting TCP connection parameters, you must reestablish a TCP connection (in automatic mode or triggered by traffic) to make the settings take effect.

Example

Set the buffer size for sending TCP packets in **template1** to 5120 bytes.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] tcp sendbuf-size 5120
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.17 vty rtc-server remote

7.13.16 vty rtc-client remote

Function

The **vty rtc-client remote** command configures RTC client VTYs.

The **undo vty** command deletes information about VTYs in an RTC terminal template.

By default, no RTC client VTY is configured.

Format

vty *vty-number* **rtc-client remote** *ip-address port-number* [**source** *source-ip*]

undo vty *vty-number*

Parameters

Parameter	Description	Value
vty-number	Specifies the number of an RTC client VTY.	The value is an integer that ranges from 0 to 7.
ip-address	Specifies the IP address of an RTC server.	The value is in dotted decimal notation.
port-number	Specifies the TCP port number on the RTC client. The RTC server can receive TCP connection requests only when the port specified by the RTC client exists on the RTC server.	The value is an integer that ranges from 1024 to 50000.
source *source-ip*	Specifies the source IP address for the RTC client to communicate with the RTC server. An RTC client uses the IP address of a fixed port as the source IP address to communicate with an RTC server, to ensure a stable TCP connection. ● If this parameter is specified, there must be a reachable route between the specified source IP address and the RTC server. ● If this parameter is not specified, the system selects a source IP address based on the routing table.	The value is in dotted decimal notation.

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the RTC client. An RTC client may exchange service data with multiple RTC servers. For example, the monitoring center of a bank needs to monitor savings service data in multiple banking branches. To meet this requirement, the user can configure RTC client VTYs so that a monitoring terminal

can exchange data with multiple monitored terminals. An RTC client supports multiple VTYs, each of which maps an RTC server.

Precautions

- In an RTC terminal template, RTC client and RTC server VTYs cannot be configured simultaneously.
- In an RTC terminal template, a maximum of eight types of RTC client VTYs can be configured.

Example

In the RTC terminal template **template1**, set RTC client VTY1, and specify TCP port 9010 on the RTC client for setting up TCP connections with the RTC server 10.10.10.10.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] vty 1 rtc-client remote 10.10.10.10 9010
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.17 vty rtc-server remote

7.13.17 vty rtc-server remote

Function

The **vty rtc-server remote** command configures RTC server VTYs.

The **undo vty** command deletes information about VTYs in an RTC terminal template.

By default, no RTC server VTY is configured.

Format

vty *vty-number* **rtc-server remote** *ip-address terminal-number*

undo vty *vty-number*

Parameters

Parameter	Description	Value
vty-number	Specifies the number of an RTC server VTY.	The value is an integer that ranges from 0 to 7.
ip-address	Specifies the IP address of an RTC client.	The value is in dotted decimal notation.

Parameter	Description	Value
terminal-number	Specifies the terminal number on the RTC client for setting up a TCP connection with the RTC server. **NOTE** This terminal number must be the same as that specified using the **rta terminal** command when the RTC terminal template is bound to an RTC client port.	The value is an integer that ranges from 1 to 255.

Views

Terminal template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the RTC server. An RTC server may exchange service data with multiple RTC clients. For example, multiple ground monitoring centers in the civil aviation system need to collect detection data on a radar. You can configure RTC server VTYs so that the monitored radar can exchange data with multiple monitoring devices. An RTC server supports multiple VTYs, each of which maps an RTC client.

Precautions

- In an RTC terminal template, RTC client and RTC server VTYs cannot be configured simultaneously.
- In an RTC terminal template, a maximum of eight types of RTC server VTYs can be configured.

Example

In the RTC terminal template **template1**, set RTC server VTY1, and specify terminal 1 for setting up TCP connections with the RTC client 10.20.20.20.

```
<Huawei> system-view
[Huawei] rta server enable
[Huawei] rta template template1
[Huawei-rta-template-template1] vty 1 rtc-server remote 10.20.20.20 1
```

Related Topics

7.13.8 rta server enable

7.13.9 rta template

7.13.16 vty rtc-client remote

7.14 CESoP Configuration Commands

NOTE

Only the AR168F-4P supports this feature.

7.14.1 cesop connect

Function

The **cesop connect** command establishes a CESoP connection.

The **undo cesop connect** command tears down a CESoP connection.

By default, no CESoP connection is established.

Format

cesop connect local-ip *local-ip-address* **local-udp** *local-udp-port* **remote-ip** *remote-ip-address* **remote-udp** *remote-udp-port* **remote-mac** *mac-address* [**vlan** *vlan* **8021p** *8021p-value*]

undo cesop connect

Parameters

Parameter	Description	Value
local-ip *local-ip-address*	Specifies the local IP address of the CESoP connection.	The value is in dotted decimal notation and must be a valid Class A, B, or C IP address. It cannot be a broadcast address or loopback address (in the format of 127.x.x.x).
local-udp *local-udp-port*	Specifies the local UDP port number of the CESoP connection.	The value is an integer that ranges from 1 to 65535.
remote-ip *remote-ip-address*	Specifies the remote IP address of the CESoP connection.	The value is in dotted decimal notation and must be a valid Class A, B, or C IP address. It cannot be a broadcast address or loopback address (in the format of 127.x.x.x).
remote-udp *remote-udp-port*	Specifies the remote UDP port number of the CESoP connection.	The value is an integer that ranges from 1 to 65535.
remote-mac *mac-address*	Specifies the remote MAC address of the CESoP connection.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan *vlan*	Specifies the VLAN ID of service flows transmitted over the CESoP connection.	The value is an integer that ranges from 1 to 4094.
8021p *8021p-value*	Specifies the 802.1p priority of service flows transmitted over the CESoP connection. The 802.1p priority is represented by a three-bit PRI (priority) field in an 802.1Q frame, and is used when high-priority packets need to be forwarded preferentially.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

CESoP uses UDP to transmit TDM data packets. You can run the **cesop connect** command to specify the local and remote IP addresses and UDP port numbers on the two devices to establish a CESoP connection respectively. To ensure connection security, you must specify the MAC address of the remote device.

Example

Establish a CESoP connection. Set the local IP address to 10.10.10.1, local UDP port number to 50048, remote IP address to 10.10.10.2, remote UDP port number to 65535, remote MAC address to 00e0-fc00-1010, VLAN ID to 10, and 802.1p priority to 5.

```
<Huawei> system-view
[Huawei] interface serial 0/0/0
[Huawei-Serial0/0/0] cesop connect local-ip 10.10.10.1 local-udp 50048 remote-ip 10.10.10.2 remote-udp 65535 remote-mac 00e0-fc00-1010 vlan 10 8021p 5
```

7.14.2 cesop tdm-encapsulation-number

Function

The **cesop tdm-encapsulation-number** command configures the number of TDM frames encapsulated in a CESoP packet.

The **undo cesop tdm-encapsulation-number** command restores the default number of TDM frames encapsulated in a CESoP packet.

By default, the number of TDM frames encapsulated in a CESoP packet is 8.

 Copyright © Huawei Technologies Co., Ltd.

Format

cesop tdm-encapsulation-number *number*

undo cesop tdm-encapsulation-number

Parameters

Parameter	Description	Value
number	Specifies the number of TDM frames encapsulated in a CESoP packet.	The value is an integer that ranges from 8 to 16. The default value is 8.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A small number of TDM frames encapsulated in a packet shortens network delay, but causes a high encapsulation overhead. A large number of TDM frames encapsulated in a packet reduces encapsulation overhead, but causes a long network delay. Configure the number of TDM frames encapsulated in a CESoP packet based on actual requirements.

Configuration Impact

After the **cesop tdm-encapsulation-number** command is run, CESoP negotiates the number of encapsulated frames based on the configuration. If the numbers of encapsulated frames configured on the local and remote devices are different, the serial interface cannot go Up.

Precautions

If the CESoP connection has been established, changing the number of encapsulated TDM frames using the **cesop tdm-encapsulation-number** command may cause a service interruption.

Example

Set the number of TDM frames encapsulated in a CESoP packet to 16.

```
<Huawei> system-view
[Huawei] interface serial 0/0/0
[Huawei-Serial0/0/0] cesop tdm-encapsulation-num 16
Warning:This operation will set the tdm encapsulation number and re-enable cesop on the interface
Serial0/0/0.
Are you sure to continue?[Y/N]y
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

7.14.3 cesop jitter-buffer

7.14.3 cesop jitter-buffer

Function

The **cesop jitter-buffer** command configures the jitter buffer depth in CESoPSN application.

The **undo cesop jitter-buffer** command restores the default jitter buffer depth of TDM.

The default jitter buffer depth is 8 milliseconds.

Format

cesop jitter-buffer *depth*

undo cesop jitter-buffer

Parameters

Parameter	Description	Value
depth	Specifies the jitter buffer depth, that is, the allowed maximum jitter delay.	The value is an integer that ranges from 4 to 64, in milliseconds. The default value is 8.

Views

Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A jitter buffer is designed to smooth the jitter in packet transmission over a link. The device stores frames of TDM services received at different rates in the jitter buffer, and then sends the frames to the next hop at a constant rate, smoothing the transmission jitter.

A smaller jitter buffer depth indicates a weaker jitter resistance capability. A larger jitter buffer depth indicates a stronger jitter resistance capability, but causes a long transmission delay during data flow reconstruction. A too small or large jitter buffer adversely affects service transmission.

Therefore, configure a proper jitter buffer depth based on the delay sensitivity of services, bandwidth, and jitter on the live network.

 Copyright © Huawei Technologies Co., Ltd.

- It is recommended that you set the jitter buffer depth to about 8 ms for voice services because they are very sensitive to delay. You can appropriately increase the jitter buffer depth for video and data services.
- If the network topology is complex and link transmission jitter is large, it is recommended that you appropriately increase the jitter buffer depth. Otherwise, appropriately decrease the jitter buffer depth.
- If the initial wait jitter is long, appropriately decrease the jitter buffer depth.

In addition to pre-configuring a proper jitter buffer depth on a packet switched network, you need to monitor the jitter resistance effects of different jitter buffer depths promptly, and gradually adjust the jitter buffer depth based on services.

Precautions

If the CESoP connection has been established, changing the jitter buffer depth using the **cesop jitter-buffer** command may cause a service interruption.

Example

Set the jitter buffer depth to 4 milliseconds.

```
<Huawei> system-view
[Huawei] interface serial 0/0/0
[Huawei-Serial0/0/0] cesop jitter-buffer 4
Warning:This operation will set the jitter buffer and re-enable cesop on the interface Serial0/0/0.
Are you sure to continue?[Y/N]y
```

Related Topics

7.14.2 cesop tdm-encapsulation-number

7.14.4 display cesop connect interface

Function

The **display cesop connect interface** command displays CESoP connection information of an interface.

Format

display cesop connect interface *interface-type* [*interface-number*]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays CESoP connection information of an interface with the specified type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display CESoP connection information of a specified interface.

```
<Huawei> display cesop connect interface serial 0/0/0
  Remote MAC address : 00e0-fc00-2222
  Local MAC address  : 00e0-fc00-1111
  VLAN ID            : 10
  Priority           : 7
  Remote IP          : 192.168.1.2
  Local IP           : 192.168.1.1
  Remote UDP         : 65535
  Local UDP          : 50048
```

Table 7-76 Description of the **display cesop connect interface** command output

Item	Description
Remote MAC address	Remote MAC address of the CESoP connection.
Local MAC address	Local MAC address of the CESoP connection.
VLAN ID	VLAN ID of service flows transmitted over the CESoP connection.
Priority	802.1p priority of service flows transmitted over the CESoP connection.
Remote IP	Remote IP address of the CESoP connection.
Local IP	Local IP address of the CESoP connection.
Remote UDP	Remote UDP port number of the CESoP connection.
Local UDP	Local UDP port number of the CESoP connection.

Related Topics

7.14.1 cesop connect

8 IP Service Commands

About This Chapter

8.1 IPv4 Configuration Commands
8.2 ARP Configuration Commands
8.3 DHCP Configuration Commands
8.4 DNS Configuration Commands
8.5 NAT Configuration Commands
8.6 UDP Helper Configuration Commands
8.7 IP Performance Configuration Commands
8.8 Basic IPv6 Configuration Commands
8.9 DHCPv6 Configuration Commands
8.10 IPv6 DNS Configuration Commands
8.11 IPv6 over IPv4 Tunnel Configuration Commands
8.12 IPv4 over IPv6 Tunnel Configuration Commands

8.1 IPv4 Configuration Commands

8.1.1 ip address

Function

The **ip address** command configures an IP address for an interface.

The **undo ip address** command deletes an IP address from an interface.

By default, no IP address is configured for an interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip address *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

Parameters

Parameter	Description	Value
ip-address { *mask* | *mask-length* }	Specifies the IP address of an interface. ● *ip-address* specifies the IP address. ● *mask* specifies the mask of the IP address. ● *mask-length* specifies the mask length of IP address.	● The value of *ip-address* is in dotted decimal notation. ● The value of *mask* is in dotted decimal notation. ● The value of *mask-length* is an integer that ranges from 0 to 32.
sub	Configures a secondary IP address for an interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip address** command configures IP addresses for interfaces on the router so that the router can communicate with different network segments. To connect an interface to multiple network segments, configure multiple IP addresses for the interface. Among these IP addresses, one is the primary IP address and the others are secondary IP addresses. If you configure a new primary IP address for the interface, the new IP address overrides the original one.

- The **undo ip address** command deletes all IP addresses from an interface.
- The **undo ip address** *ip-address* { *mask* | *mask-length* } command deletes the primary IP address of an interface.
- The **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command deletes a secondary IP address.

Precautions

The following conditions are prohibited for different interfaces on the same device:

- The IP addresses are the same.
- The broadcast addresses (with the host number field containing all 1s in the binary mode) corresponding to the IP addresses are the same. For example, if the IP address of interface A is 10.1.1.1/16 and its corresponding broadcast address is 10.1.255.255 and the IP address of interface B is 10.1.1.2/24 and its corresponding broadcast address is 10.1.1.255, the configuration is successful. However, if the IP address of interface B is also 10.1.1.2/16 and its corresponding broadcast address is also 10.1.255.255, the configuration fails.
- The IP address of an interface is the same as the broadcast address of another interface. For example, if the IP address of interface A is 1.1.1.1/28 and its broadcast address is 1.1.1.15 and the IP address of interface B is 1.1.1.15/26, the configuration fails.

You can configure a secondary IP address only after configuring a primary IP address on the interface. You must delete all secondary IP addresses before deleting the primary IP address.

You can configure multiple IP address for a Layer 3 interface on the device, one as the primary IP address, and the others as secondary IP addresses. Each Layer 3 interface can have a maximum of 31 secondary IP addresses.

NOTE

IP addresses of different interfaces on the router cannot be located on the same network segment.

Example

Configure a primary IP address 10.1.0.1 and a secondary IP address 10.2.0.1 for GE1/0/0, with subnet mask 255.255.255.0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.0.1 255.255.255.0
[Huawei-GigabitEthernet1/0/0] ip address 10.2.0.1 255.255.255.0 sub
```

Related Topics

5.1.9 display ip interface

8.1.2 ip address unnumbered

Function

The **ip address unnumbered** command configures IP unnumbered on an interface so that the interface can borrow the IP address from another interface.

The **undo ip address unnumbered** command cancels the IP unnumbered configuration on an interface.

By default, an interface does not borrow the IP address from another interface.

Format

ip address unnumbered interface *interface-type interface-number*

undo ip address unnumbered

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the numbered interface from which the IP address will be borrowed. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

- You can run the **ip address unnumbered** command to configure certain interfaces, including the ATM interface, dialer interface, tunnel interface, tunnel-template interface, and interface encapsulated with PPP, HDLC, or frame relay to borrow an IP address from an Ethernet interface, loopback interface, or another type of interface. The Ethernet interfaces and Ethernet sub-interfaces only can borrow the IP address from loopback interface.
- Sub-interfaces using FR as the link layer protocol can borrow IP addresses from other interfaces.
- An IP unnumbered interface cannot run dynamic routing protocols because it does not have an IP address itself. To enable the interface to communicate with a peer network segment, configure a static route to the network segment.

When dialer interfaces borrow 32-bit-mask IP addresses from loopback interfaces, pay attention to the following points:

- In automatic dialup mode, after a dialer interface borrows the IP address from a loopback interface, a link is automatically established. No static route needs to be configured.
- In traffic-triggered dialup mode, if a dialer number used to call the remote end is configured using the **dialer number** *dial-number* command, a route to the loopback interface is generated after the dialer interface borrows the IP address of the loopback interface. To enable packets to reach the dialer interface and trigger dialup, configure a static route and specify the dialer interface as the outbound interface.

 Copyright © Huawei Technologies Co., Ltd.

For example, the local dialer interface (dialer1) borrows IP address 1.1.1.1/32 from a loopback interface, the remote IP address is 1.1.1.16, and the destination IP address of dialup packets is 2.1.1.1. To enable traffic to reach dialer1 and trigger dialup, run the **ip route-static 2.1.1.1 255.255.255.255 Dialer1** command to configure a static route and specify dialer1 as the outbound interface.

- In traffic-triggered dialup mode, if the next hop of dialup packets is configured using the **dialer route** *next-hop-address* command, a route to the loopback interface is generated after the dialer interface borrows the IP address of the loopback interface. To trigger dialup, configure a static route, specify the dialer interface as the outbound interface, and specify the next hop.

  For example, the local dialer interface (dialer1) borrows IP address 1.1.1.1/32 from a loopback interface, the remote IP address is 1.1.1.16, and the destination IP address of dialup packets is 2.1.1.1. To enable traffic to reach dialer1 and trigger dialup, run the **ip route-static 2.1.1.1 255.255.255.255 Dialer1 1.1.1.16** command to configure a static route, specify dialer1 as the outbound interface, and specify the next hop.

NOTE

The numbered interface cannot borrow the interface from another interface. Other interfaces cannot borrow the IP address from the unnumbered interface.

The **ip address unnumbered** command can be used only on Layer 3 interfaces.

Example

Configure Tunnel0/0/1 to borrow the IP address from LoopBack0.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] ip address unnumbered interface loopback 0
```

Related Topics

8.1.1 ip address

8.1.3 display ip interface

Function

The **display ip interface** command displays the IP configuration and statistics on interfaces. The statistics include the number of packets and bytes received and sent by interfaces, number of multicast packets sent and received by interfaces, and number of broadcast packets received, sent, forwarded, and discarded by interfaces.

The **display ip interface brief** command displays brief information about interface IP addresses, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.

Format

display ip interface [*interface-type interface-number*]

display ip interface brief [*interface-type* [*interface-number*] | **slot** *slot-id* [**card** *card-number*]]

display ip interface brief [*interface-type*] &<1-8>

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If no interface is specified, IP configuration and statistics about all interfaces are displayed.	-
brief	Displays brief information, including the IP address, subnet mask, physical status, link-layer protocol status, and number of interfaces in different states.	-
slot *slot-id*	Displays the IP configuration and statistics of interfaces on the specified slot. If the slot number is not specified, brief information related to the IP addresses of the interfaces on all interface boards and main control boards is displayed.	-
card *card-number*	Displays the IP configuration and statistics of interfaces on specified card.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip interface brief** command to view the following information:

- IP configurations of all interfaces
- IP configurations of interfaces of the specified type and a specified interface
- IP configurations of interfaces that have IP addresses

This command, however, cannot display the IP configurations of Layer 2 interfaces or Eth-Trunk member interfaces.

NOTE

- You can run the **display interface description** command to view the interface description.
- You can run the **display interface** command to view detailed information about the running status and statistics on the interface.

Example

Display the IP configuration and statistics on GE0/0/0.

```
<Huawei> display ip interface gigabitethernet 0/0/0
GigabitEthernet0/0/0 current state : UP
Line protocol current state : UP
The Maximum Transmit Unit : 1500 bytes
input packets : 1431, bytes : 97912, multicasts : 1426
output packets : 2716, bytes : 179760, multicasts : 2710
Directed-broadcast packets:
 received packets:          0, sent packets:          0
 forwarded packets:         0, dropped packets:       0
ARP packet input number:        11
  Request packet:               11
  Reply packet:                 0
  Unknown packet:               0
Internet Address is 10.5.40.1/24
Broadcast address : 10.5.40.255
TTL being 1 packet number:      0
TTL invalid packet number:      0
ICMP packet input number:       0
  Echo reply:                   0
  Unreachable:                  0
  Source quench:                0
  Routing redirect:             0
  Echo request:                 0
  Router advert:                0
  Router solicit:               0
  Time exceed:                  0
  IP header bad:                0
  Timestamp request:            0
  Timestamp reply:              0
  Information request:          0
  Information reply:            0
  Netmask request:              0
  Netmask reply:                0
  Unknown type:                 0
```

Table 8-1 Description of the **display ip interface** command output

Item	Description
GigabitEthernet1/0/0 current state	Physical status of GigabitEthernet1/0/0: • UP: indicates that the interface is physically Up. • DOWN: indicates that the interface is physically Down. • Administratively DOWN: indicates that the administrator has run the **shutdown** command on the interface.
Line protocol current state	Link layer protocol status of the interface: • UP: The link layer protocol of the interface is running properly. • DOWN: The link layer protocol of the interface is Down or no IP address is configured on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
The Maximum Transmit Unit	MTU of the interface. The default MTU of an Ethernet interface is 1500 bytes. Packets longer than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
input packets : 1431, bytes : 97912, multicasts : 1426	Total number of packets, bytes, and multicast packets received by the interface.
output packets : 2716, bytes : 179760, multicasts : 2710	Total number of packets, bytes, and multicast packets sent by the interface.
Directed-broadcast packets	Number of packets broadcast on the interface directly.
received packets	Total number of received packets.
sent packets	Total number of sent packets.
forwarded packets	Total number of forwarded packets.
dropped packets	Total number of discarded packets.
ARP packet input number	Number of received ARP packets.
Request packet	Number of request packets.
Reply packet	Number of response packets.
Unknown packet	Number of unknown packets.
Internet Address is	IP address and subnet mask of the interface. The displayed information varies according to the IP address allocation mode: ● If the IP address is manually configured, the information is displayed as "Internet Address is 10.5.40.1/24." ● If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 10.5.40.1/24."
Broadcast address	Broadcast address of an interface.
TTL being 1 packet number	Number of packets with TTL 1.
TTL invalid packet number	Number of packets with invalid TTL.
ICMP packet input number	Number of received ICMP packets.
Echo reply	Number of Echo Reply packets.
Unreachable	Number of Destination Unreachable packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Source quench	Number of Source Quench packets.
Routing redirect	Number of Redirect packets.
Echo request	Number of Echo Request packets.
Router advert	Number of Router Advertisement packets.
Router solicit	Number of Router Solicitation packets.
Time exceed	Number of Time Exceeded packets.
IP header bad	Number of IP header error packets.
Timestamp request	Number of Timestamp Request packets.
Timestamp reply	Number of Timestamp Reply packets.
Information request	Number of Information Request packets.
Information reply	Number of Information Reply packets.
Netmask request	Number of Address Mask Request packets.
Netmask reply	Number of Address Mask Reply packets.
Unknown type	Number of unknown packets.

Display brief IP information about all interfaces.

```
<Huawei> display ip interface brief
*down: administratively down
^down: standby
(l): loopback
(s): spoofing
(E): E-Trunk down
The number of interface that is UP in Physical is 2
The number of interface that is DOWN in Physical is 3
The number of interface that is UP in Protocol is 2
The number of interface that is DOWN in Protocol is 3

Interface                     IP Address/Mask      Physical   Protocol
Atm0/0/0                        unassigned          down       down
Bridge-if10                     unassigned          down       down
MFR0/0/1                        unassigned          down       down
NULL0                           unassigned          up         up(s)
Vlanif1                       192.168.200.161/24   up         up
```

Table 8-2 Description of the **display ip interface brief** command output

Item	Description
*down:	Reason why an interface is physically Down. Administratively down indicates that the administrator has run the **shutdown** command on the interface.
^down: standby	Indicates that the interface is a backup interface.

Item	Description
(l): loopback	Indicates that the loopback function is enabled on the interface.
(s): spoofing	Indicates that the spoofing function is enabled on the interface.
(E): E-Trunk down	Indicates that the Eth-Trunk is Down because of the protocol negotiation on the E-Trunk.
The number of interface that is UP/DOWN in Physical is	Up or Down state of a physical link and number of interfaces in different states.
The number of interface that is UP/DOWN in Protocol is	Up or Down state of the protocol and number of interfaces in different states.
Interface	Interface type and number.
IP Address/ Mask	IP address and subnet mask of an interface.
Physical	Physical status of an interface: ● Up: indicates that the interface is physically Up. (l) indicates that the loopback function is configured on the interface. ● Down: indicates that the interface becomes faulty. ● *down: indicates that the administrator has run the **shutdown (interface view)** command on the interface. (l) indicates that the loopback function is configured on the interface. ● !down: indicates that the FIB module is suspended. In this case, the link protocol status of the interface is Down.
Protocol	Link protocol status of the interface: ● Up: indicates that the link protocol of the interface is running properly. (s) indicates that the link protocol status of the interface is Up when this interface is created and has no IP address configured. This is an inherent attribute of an interface. When this interface is configured with an IP address, (s) is still displayed. ● Down: indicates that the link protocol of the interface fails or no IP address is configured on the interface. (l) indicates that the loopback function is configured on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.1.4 display interface

8.1.4 display interface

Function

The **display interface** command displays the interface running status and statistics.

Format

display interface [*interface-type* [*interface-number* [.*subinterface-number*] | **main**] | **main**]

display interface slot *slot-id* [**main**]

Parameters

Parameter	Description	Value
interface-type [*interface-number*]	Displays the running status of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.	-
subinterface-number	Displays the running status of a sub-interface.	The value is an integer that ranges from 1 to 4096.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
main	Displays running status and traffic statistics about an interface. ● If an interface has no sub-interfaces, status and traffic statistics about the interface are displayed whether you specify the **main** parameter or not. ● If an interface has sub-interfaces, status and traffic statistics about the interface and sub-interfaces are displayed if you do not specify the **main** parameter.	-
slot *slot-id*	Specifies the slot ID.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The running status and statistics of an interface includes the physical status, basic configuration, and packet forwarding of the interface. You can use the **display interface** command to collect traffic statistics or locate faults on an interface.

Precautions

If no interface type is specified, the running status and statistics of all the interfaces is displayed. If the interface type is specified but no interface number is specified, the running status of all the interfaces of this type is displayed.

Example

Display the running status, basic configuration, and packet forwarding on Layer 2 Ethernet interface Ethernet2/0/0.

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
```

```
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Switch Port, PVID :    1, TPID : 8100(Hex), The Maximum Frame Length is 9216
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
Last physical up time   : 2010-07-21 15:35:37
Last physical down time : 2010-07-20 01:06:25
Current system time: 2010-07-21 16:07:53-05:13
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO,  Clock   : -
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

Input:  126 packets, 34204 bytes
  Unicast:              0,  Multicast:              52
  Broadcast:           74,  Jumbo:                     0
  Discard:              0,  Total Error:             0

  CRC:                 0,  Giants:                 0
  Jabbers:              0,  Throttles:              0
  Runts:               0,  Symbols:                0
  Ignoreds:             0,  Frames:                 0

Output:  2398 packets, 799486 bytes
  Unicast:              0,  Multicast:            1461
  Broadcast:         1477,  Jumbo:                    0
  Discard:              0,  Total Error:            53

  Collisions:          32,  ExcessiveCollisions:      21
  Late Collisions:      0,  Deferreds:               0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 8-3 Description of the **display interface** command output

Item	Description
current state	Current interface status: ● DOWN: indicates that the interface is disabled. ● UP: indicates that the interface is enabled.
Line protocol current state	Link layer protocol status of the interface: ● DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
PVID	Default VLAN ID of the interface.
The Maximum Frame Length	Maximum frame length allowed by the interface.

Item	Description
IP Sending Frames' Format	Format of the frame contained in the sent IP packet, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the device.
Last physical up time	Last time the interface goes Up physically. If this field displays "-", the physical status of the interface does not change.
Last physical down time	Last time the interface goes Down physically. If this field displays "-", the physical status of the interface does not change.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH: MM: SS UTC±HH: MM DST format.
Port Mode	Working mode of the common interface: ● COMMON COPPER: The interface is an electrical interface. ● COMMON FIBER: The interface is an optical interface. Run **combo-port**. The working mode of the combo interface is configured. ● AUTO: The combo interface automatically select the working mode. ● AUTO FIBER: The combo interface automatically select optical working mode. ● AUTO COPPER: The combo interface automatically select electrical working mode. ● FORCE FIBER: The combo interface is configured as an optical interface. ● FORCE COPPER: The combo interface is configured as an electrical interface.
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto negotiation mode, the **speed** command configures the rate of an interface.
Loopback	Loopback configuration of the interface. The **loopback** command configures loopback on an interface.
Duplex	Duplex mode of the interface.
Negotiation	Auto-negotiation mode of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mdi	Network cable type of the interface.
Clock	Clock mode of the combo interface.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Jumbo	Number of jumbo frames received or sent by the interface.
Discard	Number of packets discarded by the interface during physical layer detection. These packets are discarded because the interface is congested. The device does not support the **Discard** field for Layer 2 Ethernet interfaces.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of CRC error packets received by the interface.
Giants	Number of jumbo frames with correct Frame Check Sequence (FCS) received by the interface. **NOTE** For the AR109, AR109W, AR109GW-L, AR121, AR121W, AR121GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, this item indicates the number of received packets with length exceeding the maximum jumbo frame size.
Jabbers	Number of jumbo frames with incorrect FCS received by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Throttles	Number of undersized frames with incorrect FCS received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Runts	Number of undersized frames with correct FCS values received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames with OpCode not being PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of frames that the interface stops sending when conflicts are detected during transmission.
ExcessiveCollisions	Number of frames that experience more than 16 consecutive conflict events and fail to be sent.
Late Collisions	Number of frames that experience conflict events and are delayed. The first 512 bits of these frames have been sent but these frames are delay because conflicts are detected.
Deferreds	Number of packets delayed because conflicts are detected before transmission.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Display the running status, basic configuration, and packet forwarding on Layer 3 Ethernet interface Ethernet2/0/0.

```
<Huawei> display interface ethernet 2/0/0
Ethernet2/0/0 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Ethernet2/0/0 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet Address is 192.168.4.2/24
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 0018-2000-0083
```

```
Last physical up time   : 2010-09-08 15:35:37
Last physical down time : 2010-09-08 01:06:25
Current system time: 2010-10-21 16:07:53
Port Mode: COMMON COPPER
Speed :  100,  Loopback: NONE
Duplex: FULL,  Negotiation: ENABLE
Mdi   : AUTO,  Clock   : -
Last 300 seconds input rate 0 bits/sec, 0 packets/sec
Last 300 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

Input:  126 packets, 34204 bytes
  Unicast:                0,  Multicast:                52
  Broadcast:             74,  Jumbo:                     0
  Discard:                0,  Total Error:               0

  CRC:                    0,  Giants:                    0
  Jabbers:                0,  Throttles:                 0
  Runts:                  0,  Symbols:                   0
  Ignoreds:               0,  Frames:                    0

Output:  2398 packets, 799486 bytes
  Unicast:                0,  Multicast:              1461
  Broadcast:           1477,  Jumbo:                     0
  Discard:                0,  Total Error:              53

  Collisions:            32,  ExcessiveCollisions:      21
  Late Collisions:        0,  Deferreds:                0

    Input bandwidth utilization threshold : 100.00%
    Output bandwidth utilization threshold: 100.00%
    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 8-4 Description of the **display interface** command output

Item	Description
current state	Current interface status: ● DOWN: indicates that the interface is disabled. ● UP: indicates that the interface is enabled.
Line protocol current state	Link layer protocol status of the interface: ● DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
The Maximum Transmit Unit is	MTU of the interface. For example, the default MTU of an Ethernet interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.

Item	Description
Internet Address is	IP address and mask length of the interface. The displayed information varies according to the IP address allocation mode: ● If the IP address is manually configured, the information is displayed as "Internet Address is 192.168.4.2/24." ● If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 192.168.4.2/24."
IP Sending Frames' Format	Format of the frame contained in the sent IP packet, which can be PKTFMT_ETHNT_2, Ethernet_802.3, or Ethernet_SNAP.
Hardware address	MAC address of the device.
Last physical up time	Last time the interface goes Up physically. If this field displays "-", the physical status of the interface does not change.
Last physical down time	Last time the interface goes Down physically. If this field displays "-", the physical status of the interface does not change.
Current system time	Current system time. If the time zone is configured and the daylight saving time is used, the time is in YYYY/MM/DD HH: MM: SS UTC±HH: MM DST format.
Port Mode	Working mode of the interface: ● COMMON COPPER: The interface works as an electrical interface. ● COMMON FIBER: The interface works as an optical interface. If the interface is a combo interface: ● COMBO AUTO: The combo interface automatically selects the working mode. ● FORCE FIBER: The combo interface is configured as an optical interface. ● FORCE COPPER: The combo interface is configured as an electrical interface. To configure the working mode for an interface, run the **combo-port** command.
Speed	Current rate of the interface. ● In auto-negotiation mode, the **auto speed** command configures the rate of an interface. ● In non-auto negotiation mode, the **speed** command configures the rate of an interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Loopback	Loopback configuration of the interface. To configure loopback on an interface, run the **loopback** command.
Duplex	Duplex mode of the interface.
Negotiation	Auto-negotiation mode of the interface.
Mdi	Network cable type of the interface.
Clock	Clock mode of the combo interface.
Last 300 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 300 seconds.
Last 300 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 300 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
Input	Total number of received packets.
Output	Total number of sent packets.
Unicast	Number of unicast packets received or sent by the interface.
Multicast	Number of multicast packets received or sent by the interface.
Broadcast	Number of broadcast packets received or sent by the interface.
Jumbo	Number of jumbo frames received or sent by the interface. If the value is -, the number of jumbo frames cannot be collected on the device. **NOTE** Only interfaces of AR2220 MPUs support this statistical item.
Discard	Number of packets discarded by the interface during physical layer detection. These packets are discarded because the interface is congested. **NOTE** Only Layer 3 Ethernet interfaces of AR201, AR1220 and AR2220 MPUs support this statistical item.
Total Error	Number of error packets found during physical layer detection.
CRC	Number of CRC error packets received by the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Giants	Number of jumbo frames with correct FCS received by the interface. **NOTE** For the AR109, AR109W, AR109GW-L, AR121, AR121W, AR121GW-L, AR129, AR129W, AR129CVW, AR129CV, AR129GW-L, AR129CGVW-L, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, this item indicates the number of received packets with length exceeding the maximum jumbo frame size.
Jabbers	Number of jumbo frames with incorrect FCS received by the interface.
Throttles	Number of undersized frames with incorrect FCS received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Runts	Number of undersized frames with correct FCS values received by the interface. Undersized frames are the frames that are shorter than 64 bytes and have the correct format and valid CRC field.
Symbols	Number of received frames with coding errors.
Ignoreds	Number of received MAC control frames with OpCode not being PAUSE.
Frames	Number of packets with incorrect 802.3 length.
Collisions	Number of frames that the interface stops sending when conflicts are detected during transmission.
ExcessiveCollisions	Number of frames that experience more than 16 consecutive conflict events and fail to be sent.
Late Collisions	Number of frames that experience conflict events and are delayed. The first 512 bits of these frames have been sent but these frames are delay because conflicts are detected.
Deferreds	Number of packets delayed because conflicts are detected before transmission.
Input bandwidth utilization threshold	Threshold for inbound bandwidth usage.
Output bandwidth utilization threshold	Threshold for outbound bandwidth usage.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Display the packet forwarding on dialer1 interface.

```
<Huawei> display interface dialer 1
Dialer1 current state : UP
Line protocol current state : UP (spoofing)
Description:HUAWEI, AR Series, Dialer1 Interface
Route Port,The Maximum Transmit Unit is 1500, Hold timer is 0(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is Dialer
Current system time: 2017-12-08 23:02:15
    Input: 8837 packets, 851857 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 11358 bits/sec, 14 packets/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 65350 bits/sec,Record time: 2017-12-06 04:16:23
Output peak rate 0 bits/sec,Record time: -


ipv4
    Input: 8837 packets, 851857 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 0 bits/sec, 0 packets/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 65350 bits/sec,Record time: 2017-12-06 04:16:23
Output peak rate 0 bits/sec,Record time: -


ipv6
    Input: 0 packets, 0 bytes
    Output: 0 packets, 0 bytes
Last 600 seconds input rate 30744573456171227 bits/sec, 30744573456182571 packet
s/sec
Last 600 seconds output rate 0 bits/sec, 0 packets/sec
Input peak rate 0 bits/sec,Record time: -
Output peak rate 0 bits/sec,Record time: -

    Input bandwidth utilization  :    0%
    Output bandwidth utilization :    0%
```

Table 8-5 Description of the **display interface** command output

Item	Description
current state	Current interface status: ● DOWN: indicates that the interface is disabled. ● UP: indicates that the interface is enabled.

Item	Description
Line protocol current state	Link layer protocol status of the interface. ● DOWN: indicates that the link layer protocol of the interface fails or no IP address is assigned to the interface. ● UP: indicates that the link layer protocol of the interface is running properly.
Description	Interface description. To configure the description for an interface, run the **description** command.
The Maximum Transmit Unit is	MTU of the interface. For example, the default MTU of an Ethernet interface is 1500 bytes. Packets whose size is greater than the MTU are fragmented before being transmitted. If fragmentation is not allowed, the packets are discarded.
Internet Address is	IP address and mask length of the interface. The displayed information varies according to the IP address allocation mode: ● For a statically configured IP address: Internet Address is 192.168.4.2/24 If the IP address is statically configured, the information is displayed as "Internet Address is 192.168.4.2/24". ● If the IP address is obtained using DHCP, the information is displayed as "Internet Address is allocated by DHCP, 192.168.4.2/24".
IP Sending Frames' Format	Format of frames sent by the IP protocol, including PKTFMT_ETHNT_2, Ethernet_802.3, and Ethernet_SNAP.
Hardware address	MAC address of the device.
Input	Total number of received packets.
Output	Total number of sent packets.
Last 600 seconds input rate	Incoming packet rate (bits per second and packets per second) within the last 600 seconds.
Last 600 seconds output rate	Outgoing packet rate (bits per second and packets per second) within the last 600 seconds.
Input peak rate	Maximum incoming packet rate.
Output peak rate	Maximum outgoing packet rate.
ipv4	Number of IPv4 packets.
ipv6	Number of IPv6 packets.
Input bandwidth utilization	Inbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output bandwidth utilization	Outbound bandwidth usage. This parameter is not collected on interfaces that do not support statistics collection, and the value is fixed at 0% or --.

Related Topics

5.1.2 description (interface view)

5.1.16 shutdown (interface view)

8.2 ARP Configuration Commands

8.2.1 arp detect-mode unicast

Function

The **arp detect-mode unicast** command configures an interface to send ARP aging probe packets in unicast mode.

The **undo arp detect-mode unicast** command restores the default configuration of detection modes on an interface.

By default, an interface sends the last ARP aging probe packet in broadcast mode, and the rest ARP aging probe packets are sent in unicast mode.

Format

arp detect-mode unicast

undo arp detect-mode unicast

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before an ARP entry is aged, the interface periodically sends ARP aging probe packets at a set interval to update ARP entries. The device deletes an ARP entry if

 Copyright © Huawei Technologies Co., Ltd.

it does not receive a reply after a specified number of probes. The aging probe packet can be a unicast or broadcast packet.

When a non-Huawei device connected to a Huawei router receives an ARP aging probe packet whose destination MAC address is a broadcast address, the non-Huawei device checks the ARP table. If the mapping between the IP address and the MAC address of the Huawei router exists in the ARP table, the non-Huawei device discards the ARP aging probe packet. Then the Huawei router cannot receive a response and deletes the corresponding ARP entry. As a result, traffic from the non-Huawei device cannot be forwarded. Therefore, when a non-Huawei device is connected to a Huawei router, configure the Huawei switch to send ARP aging probe packets in unicast mode. The non-Huawei device needs to respond to the ARP aging probe packet.

Precautions

If the IP address of the peer device remains the same but the MAC address changes frequently, it is recommended that you configure ARP aging probe packets to be broadcast.

When the MAC address of the peer device remains the same, and the bandwidth of the network is insufficient, it is recommended that you set the interface to send ARP aging probe packets in unicast mode.

Example

Configure an interface to send ARP aging probe packets in unicast mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp detect-mode unicast
```

Related Topics

8.2.2 arp detect-times

8.2.3 arp expire-time

8.2.2 arp detect-times

Function

The **arp detect-times** command sets the number of ARP probes for aging dynamic ARP entries.

The **undo arp detect-times** command restores the default number of ARP probes for aging dynamic ARP entries.

By default, the number of ARP probes for aging dynamic ARP entries is 3.

Format

arp detect-times *detect-times*

undo arp detect-times

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
detect-times	Specifies the number of ARP probes for aging dynamic ARP entries.	The value is an integer ranging from 0 to 10. The default value is 3.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **arp detect-times** command sets the number of ARP probes for aging dynamic ARP entries to reduce address resolution errors. Before aging a dynamic ARP entry, the system first performs probes. If no response is received after the number of probes reaches the upper limit, the ARP entry is deleted.

Precautions

If the number of ARP probes is set to 0, the system directly deletes expired ARP entries.

Example

Set the number of ARP probes to 5 on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp detect-times 5
```

Related Topics

8.2.3 arp expire-time

8.2.1 arp detect-mode unicast

8.2.3 arp expire-time

Function

The **arp expire-time** command sets the aging time of dynamic ARP entries.

The **undo arp expire-time** command restores the default aging time of dynamic ARP entries.

By default, the aging time of dynamic ARP entries is 1200 seconds, that is, 20 minutes.

 Copyright © Huawei Technologies Co., Ltd.

Format

arp expire-time *expire-time*

undo arp expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of dynamic ARP entries.	The value is an integer ranging from 60 to 62640, in seconds. The default value is 1200 seconds, that is, 20 minutes.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **arp expire-time** command sets the aging time of dynamic ARP entries to reduce address resolution errors.

Precautions

After proxy ARP is enabled, the aging time of ARP entries on hosts should be shortened so that invalid ARP entries can be deleted as soon as possible. Then IP packet forwarding failures decrease on the router.

The command can be configured globally or on the specified interface. If the command is not configured on the interface, the aging expiry time of a dynamic ARP entry will be the one configured globally. If the command is both configured globally and on the specified interface, the aging expiry time of a dynamic ARP entry will be the one configured on the interface.

Example

Set the aging time of dynamic ARP entries to 600s on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp expire-time 600
```

Related Topics

8.2.2 arp detect-times

8.2.1 arp detect-mode unicast

 Copyright © Huawei Technologies Co., Ltd.

8.2.4 arp learning multicast enable (system view)

Function

The **arp learning multicast enable** command globally enables a device to learn multicast MAC addresses and generate dynamic ARP entries.

The **undo arp learning multicast enable** command globally disables a device from learning multicast MAC addresses and generate dynamic ARP entries.

By default, a device is globally disabled from learning multicast MAC addresses.

Format

arp learning multicast enable

undo arp learning multicast enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A MAC address corresponding to an IP address may be a multicast MAC address. In this case, a network administrator has to configure a static ARP entry. A device can generate dynamic ARP entries if enabled to learn multicast MAC addresses. This way reduces a network administrator's workload of configuring static ARP entries and reduces network operation and maintenance costs.

Precautions

After a device is enabled to learn multicast MAC addresses, the device may be attacked by ARP attack packets carrying multicast MAC addresses as source MAC addresses.

Example

Globally enable a device to learn multicast MAC addresses and generate dynamic ARP entries.

```
<Huawei> system-view
[Huawei] arp learning multicast enable
```

8.2.5 arp-ping ip

Function

The **arp-ping ip** command checks whether an IP address on a LAN is in use by sending ARP packets.

Format

arp-ping ip *ip-address* [**timeout** *time-out-value*] [**interface** *interface-type interface-number* [**vlan-id** *vlan-id*]]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Specifies the type and number of the interface that sends ARP packets. Where, ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. You must configure an outbound interface through which ARP packets are sent if you monitor the local IP address.	By default, you can search the FIB table for an outbound interface through which ARP packets are sent if you monitor a non-local IP address.
timeout *time-out-value*	Specifies the timeout period for an ARP-ping test. You are advised to specify the parameter if you monitor the local IP address.	The value is an integer in the range 1 to 10, in seconds. The default value is 3s.
vlan-id *vlan-id*	Specifies the ID of a VLAN.	The ID is an integer ranging from 1 to 4094. If this parameter is not specified, the VLAN ID is considered as 0. When the specified outbound interface is a Layer 2 interface, you need to configure *vlan-id*; when the specified outbound interface is a Layer 3 interface, you cannot configure *vlan-id*.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **arp-ping ip** command checks whether an IP address on a LAN is in use by sending ARP packets.

The **ping** command can also check whether an IP address is in use. If the destination host or the router configured with the firewall function are configured not to reply to ping packets, there is no response to the ping packet. Consequently, the IP address is considered unused. ARP is a Layer 2 protocol; therefore, ARP packets can pass through the firewall that is configured not to reply to ping packets. In this way, the preceding situation does not occur.

In addition, the length of an ARP Request packet is smaller than that of an Internet Control Message Protocol (ICMP) packet used in the **ping** command, occupying fewer network resources. You are advised to use the **arp-ping ip** command.

Precautions

ARP has been enabled and the device can send and receive ARP packets.

If the IP address specified in the **arp-ping ip** command is the IP address of the local device or a loopback address, the detection fails.

Example

Run the **arp-ping ip** command to check whether the IP address 10.1.1.1 is used.

```
<Huawei> arp-ping ip 10.1.1.1
ARP-Pinging 10.1.1.1:

10.1.1.1 is used by 00e0-fc91-8d70
```

Related Topics

8.2.6 arp-ping mac

8.2.6 arp-ping mac

Function

The **arp-ping mac** command checks whether a MAC address is used by another device on a LAN by sending ICMP packets or checks the IP address corresponding to the MAC address.

Format

arp-ping mac *mac-address* { *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in the H-H-H format. Each H contains one to four hexadecimal numbers, such as 00e0 and fc01. If you enter fewer than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be a multicast, broadcast, or virtual MAC address.
ip-address	Specifies the network segment to be queried.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance.
interface *interface-type interface-number*	Specifies the type and number of the interface that sends and receives ICMP packets. Where, ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you know a specific MAC address but not the corresponding IP address on a network segment, you can run the **arp-ping mac** command to send ICMP packets.

ICMP has been enabled and the device can send and receive ICMP packets.

Example

Run the **arp-ping mac** command on VLANIF2 to check whether the MAC address 00e0-fca6-a45d is used on a LAN.

```
<Huawei> arp-ping mac 00e0-fca6-a45d interface vlanif 2
  OutInterface: VLANIF2 MAC[00-E0-FC-A6-A4-5D], press CTRL_C to break
```

 Copyright © Huawei Technologies Co., Ltd.

```
----- ARP-Ping MAC statistics -----
1 packet(s) transmitted
1 packet(s) received

IP ADDRESS          MAC ADDRESS
192.168.1.122       00-E0-FC-A6-A4-5D
```

Table 8-6 Description of the arp-ping mac command output

Item	Description
IP ADDRESS	IP address mapping the specified MAC address.
MAC ADDRESS	MAC address to be checked.

Related Topics

8.2.5 arp-ping ip

8.2.7 arp-proxy enable

Function

The **arp-proxy enable** command enables routed proxy ARP on an interface.

The **undo arp-proxy enable** command disables routed proxy ARP on an interface.

By default, routed proxy ARP is disabled on an interface.

Format

arp-proxy enable

undo arp-proxy enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two hosts on different physical networks of the same logical network segment are not configured with the default gateways, you can use the **arp-proxy enable**

command to enable routed proxy ARP on a device between the two hosts to resolve IP addresses of the hosts.

Precautions

Routed ARP proxy allows hosts on different physical networks of the same logical network segment to communicate. The IP addresses of the hosts on a subnet have the same network ID; therefore, the default gateway address does not need to be configured on the hosts.

Example

Enable routed proxy ARP on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp-proxy enable
```

Related Topics

8.2.8 arp-proxy inner-sub-vlan-proxy enable

8.2.9 arp-proxy inter-sub-vlan-proxy enable

8.2.8 arp-proxy inner-sub-vlan-proxy enable

Function

The **arp-proxy inner-sub-vlan-proxy enable** command enables intra-VLAN proxy ARP.

The **undo arp-proxy inner-sub-vlan-proxy enable** command disables intra-VLAN proxy ARP.

By default, intra-VLAN proxy ARP is disabled.

Format

arp-proxy inner-sub-vlan-proxy enable

undo arp-proxy inner-sub-vlan-proxy enable

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If host isolation is configured on the router, you need to configure intra-VLAN proxy ARP to allow hosts to communicate in a VLAN.

Precautions

QinQ sub-interfaces, Dot1q sub-interfaces, QinQ Stacking sub-interfaces and QinQ Mapping sub-interfaces do not support proxy ARP within a VLAN.

Example

Enable intra-VLAN proxy ARP on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-proxy inner-sub-vlan-proxy enable
```

Related Topics

8.2.7 arp-proxy enable
8.2.9 arp-proxy inter-sub-vlan-proxy enable

8.2.9 arp-proxy inter-sub-vlan-proxy enable

Function

The **arp-proxy inter-sub-vlan-proxy enable** command enables inter-VLAN proxy ARP or proxy ARP on termination sub-interfaces.

The **undo arp-proxy inter-sub-vlan-proxy enable** command disables inter-VLAN proxy ARP or proxy ARP on termination sub-interfaces.

By default, inter-VLAN proxy ARP or proxy ARP on termination sub-interfaces is disabled.

Format

arp-proxy inter-sub-vlan-proxy enable

undo arp-proxy inter-sub-vlan-proxy enable

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement communication between different VLANs, you must enable inter-VLAN proxy ARP on the interface.

In a super-VLAN, hosts of different sub-VLANs cannot communicate. To implement communication between them, you must enable inter-VLAN proxy ARP on the VLANIF interface of the super-VLAN.

Precautions

After inter-VLAN proxy ARP is enabled and packets are sent from different VLANs but do not have the corresponding ARP entries, ARP packets are replicated in all VLANs on the involved sub-interface. If a lot of VLANs are configured, a large number of ARP packets need to be replicated, causing heavy burden on the peer device and abnormalities (such as high CPU usage and broadcast suppression) on downstream devices. In addition, the local device may fail to send ARP packets in time due to the replication of a large number of packets, which may lead to ARP learning failures. Therefore, do not configure too many VLANs on an interface.

Example

Enable inter-VLAN proxy ARP on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-proxy inter-sub-vlan-proxy enable
```

Related Topics

8.2.7 arp-proxy enable

8.2.8 arp-proxy inner-sub-vlan-proxy enable

8.2.10 arp regularly-refresh enable

Function

The **arp regularly-refresh enable** command enables the scheduled ARP refresh function.

The **undo arp regularly-refresh enable** command disables the scheduled ARP refresh function.

By default, the scheduled ARP refresh function is enabled.

Format

arp regularly-refresh enable

undo arp regularly-refresh enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the scheduled ARP refresh function is enabled on the device, and the device updates ARP entries every 10 hours.

Example

Disable the scheduled ARP refresh function.

```
<Huawei> system-view
[Huawei] undo arp regularly-refresh enable
```

8.2.11 arp send-packet

Function

The **arp send-packet** command configures the ARP unicast detection function.

Format

arp send-packet *ip-address mac-address* **interface** *interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address for a unicast ARP request packet to be sent.	This value is in dotted decimal notation.
mac-address	Specifies a destination MAC address for a unicast ARP request packet to be sent.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits. *mac-address* cannot be FFFF-FFFF-FFFF.
interface *interface-type interface-number*	Specifies the type and number of an interface for sending out a unicast ARP request packet.	-
vid *vid*	Specifies an outer tag value for a unicast ARP request packet to be sent.	The value is an integer ranging from 1 to 4094.
cevid *cevid*	Specifies an inner tag value for a unicast ARP request packet to be sent.	The value is an integer ranging from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether a peer device is reachable, run the **arp send-packet** command to configure a local interface to send a unicast ARP request packet that carries the peer device's IP and MAC addresses as the destination addresses.

- If the peer is reachable, the peer sends an ARP reply packet to the local device. Then, the local device uses information carried in the ARP reply packet to create or update an ARP entry for the peer.
- If the peer is unreachable, the peer device does not send an ARP reply packet. The local device does not generate an ARP entry.

The ARP entries learned or updated by the local device will be deleted after their aging time expires and can be updated again after the local device receives ARP request packets from the peer device.

Example

Configure GE1/0/0 to send a unicast ARP request packet that carries the destination IP address 2.2.2.3 and destination MAC address 5489-98f4-786e.

```
<Huawei> arp send-packet 2.2.2.3 5489-98f4-786e interface gigabitethernet 1/0/0
```

8.2.12 arp static

Function

The **arp static** command configures static ARP entries.

The **undo arp static** command deletes static ARP entries.

By default, the ARP mapping table is empty and address mappings are obtained using dynamic ARP.

Format

arp static *ip-address mac-address* [**vpn-instance** *vpn-instance-name*]

arp static *ip-address mac-address* **vid** *vlan-id* [**cevid** *ce-vid*] **interface** *interface-type interface-number*

undo arp static *ip-address* [*mac-address*] [**vpn-instance** *vpn-instance-name* | **vid** *vlan-id* [**cevid** *ce-vid*] **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address in a static ARP entry.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address of a static ARP entry.	The value is in H-H-H format. An H contains one to four hexadecimal numbers.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. The parameter is used for the MPLS VPN feature. When this parameter is set, it indicates that the ARP entry is of the VPN instance. **NOTE** After the name of a VPN instance is specified, the device can automatically learn the outbound interface, with no need for specifying it.	The value must be an existing VPN instance.
interface *interface-type interface-number*	Specifies the outbound interface of a static ARP packet. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** If the IP address corresponding to the specified ARP entry belongs to the VPN, an outbound interface cannot be specified.	-
vid *vlan-id*	Specifies the ID of the VLAN to which a static ARP entry belongs.	The value is an integer ranging from 1 to 4094.
cevid *ce-vid*	Specifies the inner VLAN ID.	The value is a decimal integer ranging from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security and facilitate management, you may need to configure mappings between IP addresses and MAC addresses. In this case, run the **arp**

static command to configure a fixed ARP mapping entry that maps an IP address to a MAC address.

A static ARP entry cannot be dynamically modified.

A static ARP entry is used in the following situations:

- Direct the packets whose destination IP addresses are not on the local network segment to a gateway on the local network segment so that the packets can be forwarded by the gateway.
- Bind the destination IP addresses of invalid packets to a nonexistent MAC address so that the invalid packets are filtered out.

Precautions

If a static ARP entry to be created exists, the system updates the entry.

After a static ARP entry is configured, it cannot be dynamically updated.

The IP address specified by *ip-address* and the IP address of the outbound interface specified by **interface** must be on the same network segment.

- For Layer 3 physical interfaces and Layer 3 Eth-Trunk interfaces, run the **arp static** *ip-address mac-address* command to configure static ARPentries.
- For VLANIF interfaces and Dot1q termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries.
- For QinQ termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **cevid** *ce-vid* **interface** *interface-type interface-number* command to configure static ARP mapping entries with double tags. *vid* specified in this command must be the same as *pe-vid* in the **qinq termination pe-vid ce-vid** command, and *ce-vid* must be within the value range of *ce-vid* in the **qinq termination pe-vid ce-vid** command.
- For interfaces bound to a VPN instance:
  - For Layer 3 physical interfaces and Layer 3 Eth-Trunk interfaces, run the **arp static** *ip-address mac-address* **vpn-instance** *vpn-instance-name* command to configure static ARP entries.
  - For VLANIF interfaces and Dot1q termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries.
  - For QinQ termination sub-interfaces, run the **arp static** *ip-address mac-address* **vid** *vlan-id* **cevid** *ce-vid* **interface** *interface-type interface-number* command to configure static ARP mapping entries with double tags. *vid* specified in this command must be the same as *pe-vid* in the **qinq termination pe-vid ce-vid** command, and *ce-vid* must be within the value range of *ce-vid* in the **qinq termination pe-vid ce-vid** command.

Example

Configure a static ARP entry that maps the IP address 10.0.0.1 to the MAC address aaaa-fccc-1212.

```
<Huawei> system-view
[Huawei] arp static 10.0.0.1 aaaa-fccc-1212
```

Configure a static ARP entry that maps the IP address 10.1.1.1 to MAC address 0efc-0505-86e3. This entry belongs to VLAN 10. The outbound interface is Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] arp static 10.1.1.1 0efc-0505-86e3 vid 10 interface ethernet 2/0/0
```

Configure a static ARP entry that maps the IP address 10.1.1.1 to MAC address 0efc-0505-86e3. This ARP entry belongs to the VPN instance **vpn1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] arp static 10.1.1.1 0efc-0505-86e3 vpn-instance vpn1
```

Configure an ARP entry that maps the IP address 10.1.1.1 to the MAC address 00e0-fc01-0000. The VLAN ID in the outer VLAN tag is 10 and the VLAN ID in the inner VLAN tag is 100. The outbound interface is GE1/0/0.1.

```
<Huawei> system-view
[Huawei] arp static 10.1.1.1 00e0-fc01-0000 vid 10 cevid 100 interface gigabitethernet 1/0/0.1
```

Related Topics

8.2.16 display arp interface
8.2.31 reset arp

8.2.13 arp-suppress enable

Function

Using the **arp-suppress enable** command, you can enable ARP suppression.

Using the **undo arp-suppress** command, you can disable ARP suppression.

By default, ARP suppression is disabled but is enabled on VLANIF interfaces.

Format

arp-suppress enable

undo arp-suppress

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the system receives a great number of ARP packets from the same source at a time, it needs to update ARP entries repeatedly, causing performance deterioration. To ensure system performance, you can enable ARP suppression. The system then only responds to ARP Request packets but does not update ARP entries.

If ARP suppression is enabled for all interfaces, ARP entries on some interfaces cannot be updated temporarily. ARP suppression is applicable to only VLANIF and Eth-Trunk interfaces. By default, it always takes effect on VLANIF interfaces. It can be configured on other logical interfaces.

After the **undo arp-suppress** command is executed, ARP suppression is enabled only on VLANIF interfaces.

Example

Enable ARP suppression.

```
<Huawei> system-view
[Huawei] arp-suppress enable
```

8.2.14 display arp

Function

The **display arp** command displays all ARP mapping entries.

Format

display arp [**all** | **brief**]

Parameters

Parameter	Description	Value
all	Displays all ARP mapping entries.	-
brief	Displays brief information about ARP mapping entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays all ARP mapping entries, including the aging time of ARP entries, ARP entry type, and VPN instance to which ARP entries belong.

NOTE

If Layer 3 VXLAN is configured on the device, you can query dynamic ARP entries through BDIF interfaces, but not through physical interfaces.

If Layer 3 VXLAN is configured on the device, you cannot query static ARP entries through physical and BDIF interfaces.

Example

Display all ARP mapping entries.

```
<Huawei> display arp all
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN(SIP/DIP)       PVC
--------------------------------------------------------------------------------
192.168.0.1     00e0-fc01-0000             S--
192.168.118.1   0018-2000-0083             I -         Vlanif11
10.1.1.1        0018-2000-0083             I -         Vlanif10
10.1.1.116      0018-2000-0083             I -         GE2/0/0
10.1.1.118      0001-0c01-3401  14         D-0         GE2/0/0
10.1.1.4        0016-ecb7-a879  18         D-0         GE2/0/0
192.168.10.1    0018-8267-7f7d             D-0         GE1/0/4
                                      10/-
192.168.10.1    0018-8267-7f7d             S--         vbdif10
                                      1.1.1.1/2.2.2.2
192.168.10.1    0018-8267-7f7d             D-0         vbdif10
                                      1.1.1.1/2.2.2.3
--------------------------------------------------------------------------------
Total:9         Dynamic:4       Static:1     Interface:6
```

Display brief information about all ARP mapping entries.

```
<Huawei> display arp brief
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE  INTERFACE
                                VLAN/CEVLAN(SIP/DIP)       PVC
--------------------------------------------------------------------------------
192.168.200.176 5489-9876-2c5c             I -   Eth1/0/0
192.168.200.100 5489-98f4-5a8e 18          D-0   Eth1/0/1
10.1.1.2        5489-9876-2c5e             I -   Eth1/0/2
192.168.10.1    0018-8267-7f7d             S--   vbdif10
                                      1.1.1.1/2.2.2.2
--------------------------------------------------------------------------------
Total:4         Dynamic:1       Static:0     Interface:3
```

Table 8-7 Description of the display arp command output

Item	Description
IP ADDRESS	IP address in the ARP entry.

Item	Description
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of ARP entries, in minutes.
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating the dynamic entry obtained through the ARP packet ● S: Static, indicating the static entry obtained through static configuration If the second bit is F, the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
SIP/DIP	Source IP address and destination IP address of a VXLAN tunnel.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

Related Topics

8.2.12 arp static
8.2.18 display arp dynamic
8.2.16 display arp interface
8.2.20 display arp network
8.2.22 display arp static
8.2.23 display arp statistics
8.2.31 reset arp

8.2.15 display arp error packet

Function

The **display arp error packet** command displays the latest ten ARP error packets.

Format

display arp error packet

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device cannot learn ARP entries, you can run this command to check the latest received ARP error packets. The ARP error packets help locate the fault.

Example

Display the latest ten ARP error packets.

```
<Huawei> display arp error packet
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:53]:
 00 01 08 00 06 04 00 01 00 25 9E 4B 1F 75 0A 8A
 4E 02 00 00 00 00 00 00 0A 8A 4E FF 00 00 00 00
 00 00 00 00 00 00 FF FF FF FF FF FF 00 25
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:54]:
 00 01 08 00 06 04 00 01 00 13 72 FD E7 1C 0A 8A
 4E 98 00 00 00 00 00 00 0A 8A 4E 30 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:34:55]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:05]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:05]:
 00 01 08 00 06 04 00 01 00 E0 FC 8F B2 DD 0A 8A
 4E 01 00 00 00 00 00 00 0A 8A 4F FA 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:08]:
 00 01 08 00 06 04 00 01 00 0F E2 5C 8C EA AC 12
 3E FE 00 00 00 00 00 00 AC 12 3E FE 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:11]:
 00 01 08 00 06 04 00 01 00 1B B9 78 25 2E 0A 8A
 4E A5 00 00 00 00 00 00 0A 8A 4E 2D 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:15]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:19]:
 00 01 08 00 06 04 00 01 00 13 72 9B 21 A7 0A 8A
 4E 82 00 00 00 00 00 00 0A 8A 4E 01 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
-----------------------------------------------------
 [interface = Vlanif10, time = 2010-05-24 20:35:22]:
 00 01 08 00 06 04 00 01 00 E0 FC 8F B2 DD 0A 8A
 4E 01 00 00 00 00 00 00 0A 8A 4F FA 00 00 00 00
 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```

Table 8-8 Description of the display arp error packet command output

Item	Description
interface	Interface name.
time	Time when an ARP error packet is received.

Related Topics

8.2.16 display arp interface

8.2.31 reset arp

8.2.16 display arp interface

Function

The **display arp interface** command displays ARP mapping entries of a specified interface.

Format

display arp interface *interface-type interface-number* [**vid** *vlan-id* [**cevid** *cevlan-id*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
vid *vlan-id*	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.
cevid *cevlan-id*	Specifies the CE VLAN ID.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor dynamic ARP entries or locate the faults in ARP, you can run this command to check the ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display all the ARP entries of Ethernet2/0/0.

```
<Huawei> display arp interface ethernet 2/0/0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
-------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201            I -         Ethernet1/0/1       r1
192.168.1.1     0000-0a41-0200  15        D-6         Ethernet1/0/1       r1
-------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

Table 8-9 Description of the display arp interface command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating the dynamic entry obtained through the ARP packet ● S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the entry is reported to the routing module, the route to this IP address is calculated, and entries in the FIB are correspondingly updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
INTERFACE	Type and number of the interface that has learnt ARP entries.
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries of the local interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.2.12 arp static

8.2.31 reset arp

6.3.43 vlan

8.2.17 display arp ip-conflict track

Function

The **display arp ip-conflict track** command displays recorded information about the detected IP address conflict.

Format

display arp ip-conflict track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Route flapping caused by IP address conflicts affects user services. To help users quickly locate IP conflicts to better manage IP addresses of network devices, run the **display arp ip-conflict track** command to view the recorded information about the detected IP address conflict.

NOTE

The maximum number of IP conflict information that can be recorded by the system is 200, and the oldest recorded information will be covered by newly added if the conflicted IP address is more than 200.

Example

Display the information of the detected IP address conflict.

```
<Huawei> display arp ip-conflict track
  Conflict type       : Remote IP Conflict
  IP address          : 10.1.1.1
  System time         : 2011-04-10 06:59:43
  Conflict count      : 1
  Suppress count      : 0
  Old interface       : GE1/0/1
  Receive interface   : GE1/0/2
```

```
Old VLAN/CEVLAN     : 100/0
Receive VLAN/CEVLAN : 100/0
Old MAC             : 00e0-ca63-8141
Receive MAC         : 00e0-ca63-8142
```

Table 8-10 Description of the display arp ip-conflict track command output

Item	Description
Conflict type	IP address conflict type
IP address	Conflicting IP address
System time	System time when an IP conflict occurred
Conflict count	Total number of the IP conflict times **NOTE** The field is displayed as 0 if the ARP entry corresponding to the IP address expires or is deleted.
Suppress count	Number of the suppressed IP conflicts **NOTE** The field is displayed as 0 if the ARP entry corresponding to the IP address expires or is deleted.
Old interface	Interface recorded in the ARP entry of the IP address
Receive interface	Interface that receives the ARP packet with duplicate IP address
Old VLAN/CEVLAN	VLAN and CEVLAN recorded in the ARP entry of the IP address
Receive VLAN/CEVLAN	VLAN and CEVLAN configured on the interface that receives the ARP packet with duplicate IP address
Old MAC	Source MAC address recorded in the ARP entry of the IP address
Receive MAC	Source MAC address of the second ARP packet with duplicate IP address

8.2.18 display arp dynamic

Function

The **display arp dynamic** command displays all dynamic ARP entries.

Format

display arp dynamic

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all dynamic ARP mapping entries.

```
<Huawei> display arp dynamic
IP ADDRESS       MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                           VLAN/CEVLAN
-------------------------------------------------------------------------------
10.137.217.210   00e0-fc01-0203            I -         Ethernet1/0/0
10.137.216.1     0025-9e38-a09e  20        D-0         Ethernet1/0/0
10.137.217.208   00e0-fc01-0205  16        D-0         Ethernet1/0/0
10.2.2.1         00e0-fc99-9999            I -         Eth-Trunk0
10.6.3.34        00e0-fc01-0204            I -         Ethernet2/0/0.1
192.168.20.1     00e0-fc99-9999            I -         Vlanif100
10.0.0.1         00e0-fc99-9999            I -         Vlanif200
-------------------------------------------------------------------------------
Total:7          Dynamic:2       Static:0     Interface:5
```

Table 8-11 Description of the display arp dynamic command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of ARP entries, in minutes.

Item	Description
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating the dynamic entry obtained through the ARP packet ● S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.

Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.2.14 display arp
8.2.16 display arp interface
8.2.20 display arp network
8.2.22 display arp static
8.2.23 display arp statistics
8.2.31 reset arp

8.2.19 display arp dynamic vlan

Function

The **display arp dynamic vlan** command displays dynamic Address Resolution Protocol (ARP) entries that a device has generated on a specified VLAN.

Format

display arp dynamic [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the dynamic ARP entries that a device has generated on a specified VLAN. If this parameter is not specified, all dynamic ARP entries that a device has generated are displayed.	The value is an integer ranging from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor dynamic ARP or locate a fault if dynamic ARP goes faulty on a device, run the **display arp dynamic vlan** command to view dynamic ARP entries. The **display arp dynamic vlan** command displays dynamic ARP entries that a device has generated. You can locate the fault based on the command output.

Example

Display dynamic ARP entries that a device has generated on VLAN 10.

```
<Huawei> display arp dynamic vlan 10
```

```
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN
--------------------------------------------------------------------------------
172.16.1.1      0000-c10b-5f77          I -         Vlanif10
172.16.1.2      00e0-4c77-5e3c  20        D-0           GE1/0/1
                                10/-
172.16.1.3      0025-9e36-e8a6  14        D-0           GE1/0/2
                                10/-
172.16.1.4      00e0-fcd5-c860  19        D-0           GE1/0/3
                                10/-
--------------------------------------------------------------------------------
Total:4         Dynamic:3       Static:0     Interface:1     Remote:0
```

Table 8-12 Description of the **display arp dynamic vlan** command output

Item	Description
IP ADDRESS	IP address in an ARP entry.
MAC ADDRESS	MAC address in an ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of an ARP entry, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TYPE	Entry type and number of the slot that obtains the entry. The entry type contains 3 bits. ● The first bit can be as follows: – I: Interface, indicating the MAC address of the interface – D: Dynamic, indicating the dynamic entry obtained through the ARP packet – S: Static, indicating the static entry obtained through static configuration – R: Remote, indicating the ARP entry obtained through remote backup ● The second bit can only be F, indicating that the entry is reported to the routing module, the route to this IP address is calculated, and the entries in the FIB are correspondingly updated. If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. **NOTE** VLANIF interface and sub-interfaces for VLAN tag termination (including QinQ termination sub-interfaces and Dolt1q termination sub-interfaces) on devices report learned ARP entries to the routing module to generate 32-bit host routes (routes destined for complete host addresses). The host routes are accurate and can be used for packet forwarding. Because the forwarding model of the two types of interfaces requires accurate forwarding paths. However, the outbound interfaces of VLANIF interface routes are VLANIF interfaces. VLANIF interfaces are virtual interfaces that may correspond to multiple physical interfaces, and as a result, such routes cannot be used for packet forwarding. Therefore, the VLANIF interfaces report learned ARP entries to the routing module to generate host routes. As for sub-interfaces for VLAN tag termination, they may correspond to multiple VLANs, and the forwarding model requires that packets be sent to a specified VLAN. Therefore, the sub-interfaces for VLAN tag termination also report learned ARP entries to the routing module to generate host routes. ● The third bit indicates the number of the slot that obtains this entry.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	NOTE For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs.
INTERFACE	Type and number of the interface on which the ARP entry is generated.
VLAN	ID of the VLAN to which the ARP entry belongs.
Total	Total number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries on the interface.
Remote	Number of remote backup ARP entries.

8.2.20 display arp network

Function

The **display arp network** command displays ARP mapping entries of a specified network segment.

Format

display arp network *net-number* [*net-mask*] [**dynamic** | **static**]

Parameters

Parameter	Description	Value
net-number	Specifies the network ID.	The value is in dotted decimal notation.
net-mask	Specifies the subnet mask.	The value is in dotted decimal notation or a decimal number ranging from 1 to 32.
dynamic	Displays dynamic ARP entries of a specified network segment.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
static	Displays static ARP entries of a specified network segment.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all ARP entries of the network segment with network ID 10.10.0.0 and subnet mask 255.255.0.0.

```
<Huawei> display arp network 10.10.0.0 255.255.0.0
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
                                VLAN/CEVLAN PVC
-------------------------------------------------------------------------------
10.10.20.9      0018-2000-0083          I -         Vlanif10
10.10.10.6      0018-2000-0083          I -         Vlanif20
-------------------------------------------------------------------------------
Total:2         Dynamic:0       Static:0        Interface:2
```

Table 8-13 Description of the display arp network command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes.

Item	Description
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating the dynamic entry obtained through the ARP packet ● S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.2.12 arp static
8.2.18 display arp dynamic
8.2.16 display arp interface
8.2.22 display arp static
8.2.23 display arp statistics
8.2.31 reset arp

8.2.21 display arp packet statistics

Function

The **display arp packet statistics** command displays the statistics on ARP packets.

Format

display arp packet statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate and rectify ARP faults, you can run this command to the statistics on ARP packets.

Example

Display the statistics on ARP packets.

```
<Huawei> display arp packet statistics
ARP Pkt Received:   sum  10088
ARP Learnt Count:   sum     52
ARP Pkt Discard For Limit:   sum      0
ARP Pkt Discard For SpeedLimit:   sum     31
ARP Pkt Discard For Proxy Suppress:   sum    307
ARP Pkt Discard For Other:   sum   9274
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-14 Description of the display arp packet statistics command output

Item	Description
ARP Pkt Received	Number of the received ARP packets.
ARP Learnt Count	Times of ARP learning.
ARP Pkt Discard For Limit	Number of ARP packets discarded due to the ARP entry limit.
ARP Pkt Discard For SpeedLimit	Number of ARP packets discarded when the number of ARP packets from a specified source IP address exceeds the limit.
ARP Pkt Discard For Proxy Suppress	Number of packets discarded for the speed limit.
ARP Pkt Discard For Other	Number of the packets discarded due to other causes.

8.2.22 display arp static

Function

The **display arp static** command displays all static ARP mapping entries.

Format

display arp static

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all static ARP entries.

```
<Huawei> display arp static
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE       INTERFACE   VPN-INSTANCE
```

```
                                    VLAN/CEVLAN PVC
--------------------------------------------------------------------------------
10.1.2.1        0023-0045-0067          S--
--------------------------------------------------------------------------------
Total:1         Dynamic:0       Static:1     Interface:0
```

Table 8-15 Description of the display arp static command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry.
EXPIRE(M)	Remaining lifetime of ARP entries, in minutes.
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating the dynamic entry obtained through the ARP packet ● S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the ARP entry has been reported to the routing module, the route to this IP address has been calculated, and the entry in the FIB has been updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.

Item	Description
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Total number of ARP entries in the ARP mapping table.
Dynamic	Number of dynamic ARP entries in the ARP mapping table.
Static	Number of static ARP entries in the ARP mapping table.
Interface	Number of ARP entries in the ARP mapping table on the local interface.

Related Topics

8.2.12 arp static
8.2.18 display arp dynamic
8.2.16 display arp interface
8.2.20 display arp network
8.2.23 display arp statistics
8.2.31 reset arp

8.2.23 display arp statistics

Function

The **display arp statistics** command displays ARP entry statistics.

Format

display arp statistics { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays ARP entry statistics of the system.	-
interface *interface-type interface-number*	Displays ARP entry statistics of a specified interface.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

To monitor ARP entries or locate the faults in ARP, you can run this command to check ARP entry statistics.

Example

Display ARP entry statistics.

```
<Huawei> display arp statistics all
Dynamic:1        Static:0
```

Table 8-16 Description of the display arp statistics all command output

Item	Description
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.

8.2.24 display arp track

Function

The **display arp track** command displays changes of outbound interfaces in ARP entries learned by a VLANIF interface.

Format

display arp track

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If the outbound interfaces change in ARP entries learned by a VLANIF interface, traffic may be interrupted. In this case, run the **display arp track** command to check changes of outbound interfaces and time of changes.

Precautions

After the **display arp track** command is executed, changes of ARP entries are displayed in the following situations:

- Outbound interfaces in dynamic ARP entries learnt by the VLANIF interface change to other interfaces.
- No outbound interface is specified in the static ARP entries. The outbound interface changes to other interfaces.
- Dynamic ARP entries or static ARP entries in which no VLAN ID or outbound interface is specified are deleted.

Changes of ARP entries cannot be displayed in the following situations:

- ARP entries change on a non-VLANIF interface.
- New ARP entries are learnt.
- The VLAN ID and outbound interface are manually specified in static ARP entries.

Example

Display changes of ARP entries.

```
<Huawei> display arp track
Operate Flags: M - Modify, D - Delete
-----------------------------------------------------------------------------
Op IP-Address  MAC-Address     VLAN   Old-Port   New-Port   System-Time
-----------------------------------------------------------------------------
M  10.1.1.1    0001-0001-0001  1000   Ethernet2/0/0  Ethernet1/0/2  2017-08-19 12:10:12
D  10.2.1.100  0003-0003-0003  300                   Ethernet1/0/3  2017-08-19 12:12:12
```

Table 8-17 Description of the display arp track command output

Item	Description
Op	Operation identifier. ● M: Modify, indicating that the outbound interface changes. ● D: Delete, indicating that the ARP entry is deleted.
IP-Address	IP address in the ARP entry.
MAC-Address	MAC address in the ARP entry.
VLAN	ID of the VLAN to which the VLANIF interface belongs.
Old-Port	Original outbound interface in the ARP entry.
New-Port	New outbound interface in the ARP entry.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
System-Time	System time when the outbound interface changes.

8.2.25 display arp vpn-instance

Function

The **display arp vpn-instance** command displays ARP entries of a specified VPN instance.

Format

display arp vpn-instance *vpn-instance-name* [**dynamic** | **static**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance name.	The value must be an existing VPN instance.
dynamic	Displays dynamic ARP entries.	-
static	Displays static ARP entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor dynamic ARP entries or locate the faults in ARP, you can run this command to check the ARP entries.

Example

Display all the ARP entries of VPN r1.

```
<Huawei> display arp vpn-instance r1
IP ADDRESS      MAC ADDRESS     EXPIRE(M) TYPE        INTERFACE   VPN-INSTANCE
                                          VLAN/CEVLAN PVC
-------------------------------------------------------------------------------
192.168.1.11    0000-0a41-0201            I -         Eth1/0/0       r1
192.168.1.1     0000-0a41-0200  12        D-6         Eth1/0/0       r1
-------------------------------------------------------------------------------
Total:2         Dynamic:1       Static:0    Interface:1
```

Table 8-18 Description of the display arp vpn-instance command output

Item	Description
IP ADDRESS	IP address in the ARP entry.
MAC ADDRESS	MAC address in the ARP entry. If the field is Incomplete, the entry is a fake ARP entry. If a large number of ARP Miss messages are sent to the upper-layer software, the system resources will be exhausted in processing the ARP Miss messages. To resolve this problem, the system automatically generates ARP fake entries instead of ARP entries. You can run the **arp-fake expire-time** command to configure the aging time of fake ARP entries.
EXPIRE(M)	Remaining lifetime of the ARP entry, in minutes.
TYPE	ARP entry type and slot ID of the LPU that obtains the entry. The entry type contains 3 bits. The first bit can be any of the following: ● I: Interface, indicating the MAC address of the interface ● D: Dynamic, indicating the dynamic entry obtained through the ARP packet ● S: Static, indicating the static entry obtained through static configuration The second bit can only be F, indicating that the entry is reported to the routing module, the route to this IP address is calculated, and entries in the FIB are correspondingly updated. **NOTE** If the entry is not reported to the routing module, this field displays "-". For the ARP entry with the type as "I", this flag bit does not exist. The third bit indicates the slot ID of the LPU that obtains the entry. **NOTE** For the ARP entry with the type as "I" or "S", this field displays "-".
VPN-INSTANCE	Name of the VPN instance to which the ARP entry belongs. The value is set using the **ip vpn-instance** command.
INTERFACE	Type and number of the interface that has learnt ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN/CEVLAN	ID of the VLAN to which the ARP entry belongs. The value is set using the **vlan** command.
PVC	Interface where the PVC exists and the corresponding VPI/VCI.
Total	Number of ARP entries.
Dynamic	Number of dynamic ARP entries.
Static	Number of static ARP entries.
Interface	Number of ARP entries of the local interface.

Related Topics

8.2.12 arp static
8.2.16 display arp interface
8.2.31 reset arp

8.2.26 display mac-address multiport

Function

The **display mac-address multiport** command displays the configured multi-interface MAC address entries.

Format

display mac-address multiport [[*mac-address*] **vlan** *vlan-id*] [**total-number**]

Parameters

Parameter	Description	Value
mac-address	Displays the specified multi-interface MAC address entry.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Displays multi-interface MAC address entries in the specified VLAN.	The value is an integer that ranges from 1 to 4094.
total-number	Displays the total number of multi-interface MAC address entries.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the configured multi-interface MAC address entries. If no MAC address or VLAN is specified, the system displays all multi-interface MAC address entries. You can configure multi-interface MAC address entries using the **8.2.30 mac-address multiport interface** or **8.2.29 mac-address multiport** command.

Example

Display multi-interface MAC address entries in VLAN 100.

```
<Huawei> display mac-address multiport vlan 100
--------------------------------------------------------------------------------
MAC Address       VLANID    Out-Interface
--------------------------------------------------------------------------------
03bf-2100-2200    100       Ethernet5/0/1
                            Ethernet5/0/2
                                        2 port(s)
--------------------------------------------------------------------------------
 Total Group(s) : 1
```

Display the multi-interface MAC address entry matching MAC address 03bf-0a80-f6fc in VLAN 100.

```
<Huawei> display mac-address multiport 03bf-0a80-f6fc vlan 100
--------------------------------------------------------------------------------
MAC Address       VLANID    Out-Interface
--------------------------------------------------------------------------------
03bf-2100-2200    100       Ethernet5/0/1
                            Ethernet5/0/2
                                        2 port(s)
--------------------------------------------------------------------------------
 Total Group(s) : 1
```

Display the number of configured multi-interface MAC address entries.

```
<Huawei> display mac-address multiport total-number
Total number of mac-address : 1
```

Table 8-19 Description of the display mac-address multiport command output

Item	Description
MAC Address	Destination MAC address.
VLANID	VLAN to which the outbound interface belongs.
Out-Interface	Outbound interface.
Total Group(s)	Total number of multi-interface MAC address entries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total number of mac-address	Total number of multi-interface MAC address entries.

Related Topics

8.2.29 mac-address multiport

8.2.30 mac-address multiport interface

8.2.27 display snmp-agent trap feature-name arp all

Function

The **display snmp-agent trap feature-name arp all** command displays all trap messages of the ARP module.

Format

display snmp-agent trap feature-name arp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

After running the **snmp-agent trap enable feature-name arp** command to enable or disable a trap function of the ARP module, run the **display snmp-agent trap feature-name arp all** command to check the status of all trap functions of the ARP module.

Example

Display all trap messages of the ARP module.

```
<Huawei>display snmp-agent trap feature-name arp all
-----------------------------------------------------------------------------
```

```
Feature name: ARP
Trap number : 6
--------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwEthernetARPSpeedLimitAlarm    on                      on
hwEthernetARPThresholdExceedAlarm
                             on                      on
hwEthernetARPThresholdResumeAlarm
                             on                      on
hwEthernetARPIPConflictEvent    on                      on
hwEthernetARPLearnStopAlarm     on                      on
hwEthernetARPLearnResumeAlarm   on                      on
```

Table 8-20 Description of the **display snmp-agent trap feature-name arp all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the ARP module: ● hwEthernetARPSpeedLimitAlarm: alarm of ARP speed limit. It is a non-excessive trap. ● hwEthernetARPThresholdExceedAlarm: alarm of the number of ARP entries exceeding the upper threshold. ● hwEthernetARPThresholdResumeAlarm: alarm of the number of ARP entries falling below the upper threshold. ● hwEthernetARPIPConflictEvent: alarm of the IP address conflict. ● hwEthernetARPLearnStopAlarm: alarm of stopping learning ARP entries because the board memory usage reaches the threshold. ● hwEthernetARPLearnResumeAlarm: clear alarm of stopping learning ARPpackets because the board memory usage falls below the threshold.
Default switch status	Status of the default trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Status of the current trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

8.2.33 snmp-agent trap enable feature-name arp

8.2.28 l2-topology detect enable

Function

The **l2-topology detect enable** command enables Layer 2 topology detection.

The **undo l2-topology detect enable** command disables Layer 2 topology detection.

By default, Layer 2 topology detection is disabled.

Format

l2-topology detect enable

undo l2-topology detect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **l2-topology detect enable** command is run, all ARP entries in the VLAN are updated if the Layer 2 interface changes from Down to Up.

Example

Enable Layer 2 topology detection.

```
<Huawei> system-view
[Huawei] l2-topology detect enable
```

8.2.29 mac-address multiport

Function

The **mac-address multiport** command configures a multi-interface MAC address entry in the interface view.

The **undo mac-address multiport** command deletes a multi-interface MAC address entry in the interface view.

By default, no multi-interface MAC address entry is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

mac-address multiport *mac-address* **vlan** *vlan-id*

undo mac-address multiport *mac-address* **vlan** *vlan-id*

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.
vlan *vlan-id*	Specifies a VLAN to which an interface belongs.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All servers in an NLB group share a virtual IP address and a virtual MAC address. When a device functions as the access gateway and directly connects to the NLB group, the device needs to forward packets destined for the virtual IP address to all servers in the NLB group. You can run the **mac-address multiport** or **8.2.30 mac-address multiport interface** command to configure a multi-interface MAC address entry, and run the **8.2.12 arp static** command to configure a short static ARP entry. After the configurations, the device determines the virtual MAC address matching the virtual IP address and the VLAN to which the NLB servers belong. Then the device determines the outbound interfaces by searching the MAC address table based on the virtual MAC address and VLAN. The device can communicate with the NLB servers.

Prerequisites

A VLAN has been created, and the interface has been added to the VLAN.

Precautions

The VLAN cannot be a super-VLAN, sub-VLAN, MUX VLAN, or control VLAN of a SEP segment.

When you run the **mac-address multiport** command to configure a multi-interface MAC address entry, ensure that the specified MAC address and VLAN ID are simultaneously different from those in a static MAC address entry or a blackhole MAC address entry.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a multi-interface MAC address entry with the destination MAC address being 03bf-2100-2200 on Ethernet2/0/0 in VLAN 100.

```
<Huawei> system-view
[Huawei] vlan batch 100
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] port default vlan 100
[Huawei-Ethernet2/0/0] mac-address multiport 03bf-2100-2200 vlan 100
```

Related Topics

8.2.30 mac-address multiport interface
8.2.26 display mac-address multiport

8.2.30 mac-address multiport interface

Function

The **mac-address multiport interface** command configures a multi-interface MAC address entry in the system view.

The **undo mac-address multiport interface** command deletes a multi-interface MAC address entry in the system view.

By default, no multi-interface MAC address entry is configured on a device.

Format

mac-address multiport *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-5> **vlan** *vlan-id*

undo mac-address multiport *mac-address* **interface** { *interface-type interface-number1* [**to** *interface-type interface-number2*] } &<1-5> **vlan** *vlan-id*

undo mac-address multiport { **all** | [*mac-address*] **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address.	The value is in H-H-H format. An H contains 1 to 4 hexadecimal digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number1 [**to** *interface-type interface-number2*]	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number1* specifies the number of the first interface for which a multi-interface MAC address entry needs to be configured. • *interface-number2* specifies the number of the last interface for which a multi-interface MAC address entry needs to be configured. The value of *interface-number2* must be greater than that of *interface-number1*, and the two values determine an interface range. On AR1200, AR2200 AR3600, and AR3200, the specified interfaces must be located on the same card.	-
vlan *vlan-id*	Specifies a VLAN to which interfaces belong.	The value is an integer that ranges from 1 to 4094.
all	Specifies all multi-interface MAC address entries.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All servers in an NLB group share a virtual IP address and a virtual MAC address. When a device functions as the access gateway and directly connects to the NLB group, the device needs to forward packets destined for the virtual IP address to all servers in the NLB group. You can run the **mac-address multiport interface** or **8.2.29 mac-address multiport** command to configure a multi-interface MAC address entry, and run the **8.2.12 arp static** command to configure a short static ARP entry. After the configurations, the device determines the virtual MAC address matching the virtual IP address and the VLAN to which the NLB servers belong. Then the device determines the outbound interfaces by searching the MAC address table based on the virtual MAC address and VLAN. The device can communicate with the NLB servers.

Prerequisites

A VLAN has been created, and the interfaces have been added to the VLAN.

Precautions

The VLAN cannot be a super-VLAN, sub-VLAN, MUX VLAN, or control VLAN of a SEP segment.

When you run the **mac-address multiport interface** command to configure a multi-interface MAC address entry, ensure that the specified MAC address and VLAN ID are simultaneously different from those in a static MAC address entry or a blackhole MAC address entry.

Example

Configure a multi-interface MAC address entry with the destination MAC address being 03bf-2100-2200 and outbound interfaces being Ethernet2/0/0 and Ethernet2/0/1 in VLAN 100.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type access
[Huawei-Ethernet2/0/0] quit
[Huawei] interface ethernet 2/0/1
[Huawei-Ethernet2/0/1] port link-type access
[Huawei-Ethernet2/0/1] quit
[Huawei] vlan 100
[Huawei-vlan100] port ethernet 2/0/0 to 2/0/1
[Huawei-vlan100] quit
[Huawei] mac-address multiport 03bf-2100-2200 interface ethernet 2/0/0 to ethernet 2/0/1 vlan 100
```

Related Topics

8.2.29 mac-address multiport
8.2.26 display mac-address multiport

8.2.31 reset arp

Function

The **reset arp** command deletes ARP entries in the ARP mapping table.

Format

reset arp { **dynamic** [**ip** *ip-address* [**vpn-instance** *vpn-instance-name*]] | **interface** *interface-type interface-number* [**ip** *ip-address*] | **static** }

Parameters

Parameter	Description	Value
dynamic	Deletes dynamic ARP entries.	-

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
ip *ip-address*	Deletes dynamic ARP entries of a specified interface and with a specified IP address. If an interface learns excessive ARP entries, you can specify this parameter to delete a specified ARP entry.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specify the vpn-instance name.	The value must be an existing VPN instance.
static	Deletes static ARP entries.Static ARP entries cannot be restored after being cleared. Exercise caution when you clear static ARP entries.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device is attacked, it learns a large number of invalid ARP entries. In this case, you can use this command to delete ARP entries.

Precautions

- The **reset arp** command deletes mappings between IP addresses and MAC addresses. As a result, users may fail to access some nodes.

Example

Delete dynamic ARP entries in the ARP mapping table.

```
<Huawei> reset arp dynamic
```

Delete ARP entries of Ethernet2/0/0 with the IP address 10.1.1.1 in the ARP mapping table.

```
<Huawei> reset arp interface ethernet 2/0/0 ip 10.1.1.1
```

Related Topics

8.2.16 display arp interface

8.2.32 reset arp packet statistics

Function

The **reset arp packet statistics** command clears the statistics on ARP packets.

Format

reset arp packet statistics

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp packet statistics** command to display the statistics on ARP packets. To obtain correct statistics, run the **reset arp packet statistics** command to clear existing statistics first.

The **reset arp packet statistics** command clears the ARP packet statistics only on the main control board.

Example

Clear the statistics on all ARP packets.

```
<Huawei> reset arp packet statistics
```

8.2.33 snmp-agent trap enable feature-name arp

Function

The **snmp-agent trap enable feature-name arp** command enables the trap function for the ARP module.

The **undo snmp-agent trap enable feature-name arp** command disables the trap function for the ARP module.

By default, the trap function is enabled for the ARP module.

 Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent trap enable feature-name arp [**trap-name** { **hwethernetarpspeedlimitalarm** | **hwethernetarpthresholdexceedalarm** | **hwethernetarpthresholdresumealarm** | **hwethernetarpipconflictevent** }]

undo snmp-agent trap enable feature-name arp [**trap-name** { **hwethernetarpspeedlimitalarm** | **hwethernetarpthresholdexceedalarm** | **hwethernetarpthresholdresumealarm** | **hwethernetarpipconflictevent** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of ARP events of specified types.	-
hwethernetarpspeedlimitalarm	Enables the alarm of ARP speed limit. It is a non-excessive trap.	-
hwethernetarpthresholdexceedalarm	Enables the alarm of the number of ARP entries exceeding the upper threshold.	-
hwethernetarpthresholdresumealarm	Enables the alarm of the number of ARP entries falling below the upper threshold.	-
hwethernetarpipconflictevent	Enables the alarm of IP address conflict.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If you do not specify **trap-name**, all traps of the ARP module will be enabled.

Example

Enables the trap function of ARP speed limit.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name arp trap-name hwethernetarpspeedlimitalarm
```

8.3 DHCP Configuration Commands

NOTE

Wireless interfaces cannot function as DHCP clients or BOOTP clients.

8.3.1 alarm ip-used percentage

Function

The **alarm ip-used percentage** command configures the percentage of the alarms indicating that the addresses in an address pool are used up, and the percentage of the clear alarms.

The **undo alarm ip-used percentage** command restores the default percentages of the alarms and clear alarms.

By default, the percentage of the alarms indicating that the addresses in an IP address pool are used up is 100%, and the percentage of the clear alarms is 50%.

Format

alarm ip-used percentage *alarm-resume-percentage alarm-percentage*

undo alarm ip-used percentage

Parameters

Parameter	Description	Value
alarm-resume-percentage	Specifies the percentage of the clear alarms.	The value is an integer that ranges from 1 to 100. The default value is **50**. **NOTE** The percentage of the clear alarms cannot exceed that of the alarms.
alarm-percentage	Specifies the percentage of the alarms indicating that the addresses in an address pool are used up.	The value is an integer that ranges from 1 to 100. The default value is **100**.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the addresses in an IP address pool are used up, alarms are sent to notify the administrator.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The percentage of the clear alarms cannot exceed that of the alarms.

Example

Configure the percentage of the alarms indicating that the addresses in an address pool are used up, and the percentage of the clear alarms in the IP address pool view.

```
<Huawei> system-view
[Huawei] ip pool p1
[Huawei-ip-pool-p1] alarm ip-used percentage 80 90
```

8.3.2 bootfile

Function

The **bootfile** command configures the name of the startup configuration file for a DHCP client.

The **undo bootfile** command deletes the configured name of the startup configuration file for a DHCP client.

By default, the startup configuration file name is not configured for a DHCP client.

Format

bootfile *bootfile*

undo bootfile

Parameters

Parameter	Description	Value
bootfile	Specifies the name of the startup configuration file for a DHCP client.	The value is a string of 1 to 127 case-sensitive characters without spaces.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as

the startup configuration file name for the DHCP clients. After the startup configuration file name is configured using the **bootfile** command, the Offer and ACK packets sent from the DHCP server carry this file name. The DHCP client can acquire the startup configuration file from the specified server based on the file name.

Precautions

Usually, the startup configuration file is saved on a specified file server. Therefore, the route between the DHCP client and the file server must be reachable and the ip address or name of the file server must be specified.

Example

In the IP address pool view, configure the name of the startup configuration file as **start.ini** for the DHCP client.

```
<Huawei> system-view
[Huawei] ip pool p1
[Huawei-ip-pool-p1] bootfile start.ini
```

In the DHCP Option template view, configure the name of the startup configuration file as **start.ini** for the DHCP client.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] bootfile start.ini
```

Related Topics

8.3.83 ip pool (system view)

8.3.20 dhcp option template

8.3.3 conflict auto-recycle interval

Function

The **conflict auto-recycle interval** command enables automatic reclaim of conflicting IP addresses in the global address pool and configures the interval for the automatic reclaim.

The **undo conflict auto-recycle interval** command disables automatic reclaim of conflicting IP addresses in the global address pool and deletes the configured interval for the automatic reclaim.

By default, automatic reclaim of conflicting IP addresses in the global address pool is disabled.

Format

conflict auto-recycle interval day *day* [**hour** *hour* [**minute** *minute*]]

undo conflict auto-recycle interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
day *day*	Specifies the interval for the automatic reclaim, in days.	The value is an integer that ranges from 0 to 999, in days. The default value is 0.
hour *hour*	Specifies the interval for the automatic reclaim, in hours.	The value is an integer that ranges from 0 to 23, in hours. The default value is 0.
minute *minute*	Specifies the interval for the automatic reclaim, in minutes.	The value is an integer that ranges from 0 to 59, in minutes. The default value is 0.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When a DHCP server allocates IP addresses to clients, IP address conflict may occur because IP addresses of some hosts have been manually configured. In this case, the DHCP server considers these IP addresses as conflicting IP addresses, and allocates available IP addresses from the conflicting IP addresses to clients only after available IP addresses in the address pool are used up. To reclaim conflicting IP addresses promptly, the administrator can run the **conflict auto-recycle interval** command to enable automatic reclaim and specify the reclaim interval.

Prerequisites

The global address pool has been created using the **8.3.83 ip pool (system view)** command.

Example

Enable automatic reclaim for conflicting IP addresses in the global address pool **global1**, and set the interval for automatic reclaim to one day.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] conflict auto-recycle interval day 1
```

8.3.4 dhcp alarm dhcp-rate enable

Function

Using the **dhcp alarm dhcp-rate enable** command, you can enable the DHCP message checking alarm.

Using the **undo dhcp alarm dhcp-rate enable** command, you can disable the DHCP message checking alarm.

By default, the DHCP message checking alarm is disabled.

Format

dhcp alarm dhcp-rate enable

undo dhcp alarm dhcp-rate enable

Parameters

None

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP message checking is enabled, configure the DHCP message checking alarm on an interface. An alarm is generated if the number of discarded DHCP messages on the interface reaches the alarm threshold.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Prerequisites

The following configurations have been performed in sequence:

1. DHCP has been enabled globally by using the **dhcp enable** command.
2. DHCP message checking has been enabled by using the **dhcp check dhcp-rate enable** command.

Follow-up Procedure

Run the **dhcp alarm dhcp-rate threshold** command to set the alarm threshold.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the DHCP message checking alarm on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp check dhcp-rate enable
[Huawei-Ethernet2/0/0] dhcp alarm dhcp-rate enable
```

Related Topics

8.3.5 dhcp alarm dhcp-rate threshold

8.3.5 dhcp alarm dhcp-rate threshold

Function

The **dhcp alarm dhcp-rate threshold** command sets the alarm threshold for DHCP message checking on an interface.

The **undo dhcp alarm dhcp-rate threshold** command restores the default alarm threshold.

The **dhcp alarm dhcp-rate enable threshold** command enables a device to generate an alarm when the number of discarded DHCP messages reaches the threshold and sets the corresponding alarm threshold.

The **undo dhcp alarm dhcp-rate enable threshold** command disables a device from generating an alarm when the number of discarded DHCP messages reaches the threshold.

By default, a device is not enabled to generate an alarm when the number of discarded DHCP messages reaches the threshold, and the alarm threshold is 100 packets.

Format

dhcp alarm dhcp-rate threshold *threshold*

undo dhcp alarm dhcp-rate threshold

dhcp alarm dhcp-rate enable threshold *threshold*

undo dhcp alarm dhcp-rate enable threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for DHCP message checking on an interface.	The value is an integer ranging from 1 to 1000.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DHCP message checking alarm is enabled on an interface, set the alarm threshold for DHCP message checking on an interface. An alarm is generated when the number of discarded DHCP messages reaches the alarm threshold on an interface.

Prerequisites

Before running the **dhcp alarm dhcp-rate threshold** command, you must run the **dhcp alarm dhcp-rate enable** command to enable the DHCP message checking alarm.

Precautions

If you set the alarm threshold for DHCP message checking in both the system view and interface view, the alarm threshold configured in the interface view takes effect.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Example

Set the alarm threshold for DHCP message checking to 150 on interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp alarm dhcp-rate threshold 150
```

Related Topics

8.3.4 dhcp alarm dhcp-rate enable

8.3.6 dhcp check dhcp-rate enable

Function

The **dhcp check dhcp-rate enable** command enables DHCP packet rate checking.

The **undo dhcp check dhcp-rate enable** command disables DHCP packet rate checking.

By default, DHCP packet rate checking is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

In the system view:

dhcp check dhcp-rate enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp check dhcp-rate enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the interface view or VLAN view:

dhcp check dhcp-rate enable

undo dhcp check dhcp-rate enable

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables DHCP packet rate checking in specified VLANs. • *vlan-id1* specifies the ID of the first VLAN. • *vlan-id2* specifies the ID of the last VLAN. *vlan-id2* and *vlan-id1* determine a VLAN ID range.	• *vlan-id1* is an integer that ranges from 1 to 4094. • *vlan-id2* is an integer that ranges from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.

Views

System view, VLAN view, Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If attackers send DHCP packets continuously, the protocol stack of the router is affected.

To prevent attackers from sending a large number of DHCP packets, enable DHCP message checking on the router. The router checks the rate of sending DHCP packets including DHCP request and DHCP response packets. Only a certain number of DHCP packets can be sent to the DHCP protocol stack in a certain period of time and excess messages are discarded.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Follow-up Procedure

Run the **dhcp check dhcp-rate** command to set the rate of sending DHCP packets.

Example

Enable DHCP packet rate checking in the system view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp check dhcp-rate enable
```

Enable DHCP packet rate checking in VLAN 100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp check dhcp-rate enable
```

Related Topics

8.3.18 dhcp enable

8.3.7 dhcp check dhcp-rate

8.3.7 dhcp check dhcp-rate

Function

The **dhcp check dhcp-rate** command sets the checking rate of DHCP messages sent to the DHCP protocol stack.

The **undo dhcp check dhcp-rate** command restores the default checking rate of DHCP messages sent to the DHCP protocol stack.

By default, the checking rate of DHCP messages sent to the DHCP protocol stack is 100 pps.

Format

In the system view:

dhcp check dhcp-rate *rate* [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp check dhcp-rate

In the interface view or VLAN view:

dhcp check dhcp-rate *rate*

undo dhcp check dhcp-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rate	Specifies the checking rate of DHCP messages sent to the DHCP protocol stack.	The value ranges from 1 to 100, in pps.
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the checking rate of DHCP messages sent from the specified VLAN to the DHCP protocol stack. • *vlan-id1*: specifies the ID of the first VLAN. • *vlan-id2*: specifies the ID of the last VLAN. *vlan-id2* and *vlan-id1* determine a VLAN ID range.	• *vlan-id1* is an integer that ranges from 1 to 4094. • *vlan-id2* is an integer that ranges from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.

Views

System view, VLAN view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DHCP message checking is enabled, set the checking rate of DHCP messages sent to the DHCP protocol stack. In a period of time, only a certain number of DHCP messages can be sent to the DHCP protocol stack. The DHCP messages that exceed the rate are discarded.

Prerequisites

DHCP message checking has been enabled by using the **dhcp check dhcp-rate enable** command.

Precautions

You can set the checking rate of DHCP messages sent to the DHCP protocol stack in the system view, interface view, or VLAN view. The checking rates configured in the interface view, VLAN view, and system view take effect in descending order of priority.

If you run the **dhcp check dhcp-rate** *rate* command only in the system view, the checking rate of DHCP messages sent to the DHCP protocol stack in the VLAN view and interface view is the same as that configured in the system view.

 Copyright © Huawei Technologies Co., Ltd.

The interfaces supporting this command include Layer 2 GE interfaces, Layer 2 Ethernet interfaces, Layer 2 Eth-Trunk interfaces, Layer 2 port group, Layer 3 GE interfaces, and Layer 3 Ethernet interfaces.

Example

Set the checking rate of DHCP messages to 50 pps.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp check dhcp-rate 50
```

Related Topics

8.3.6 dhcp check dhcp-rate enable

8.3.8 dhcp client class-id (interface view)

Function

The **dhcp client class-id** command sets the Option60 field in the DHCP request packet sent by the DHCP client.

The **undo dhcp client class-id** command deletes the configured Option60 field in the DHCP request packet sent by the DHCP client.

By default, no Option60 field is configured.

Format

dhcp client class-id *class-id*

undo dhcp client class-id

Parameters

Parameter	Description	Value
class-id	Indicates the value of the Option60 field.	The value is a string of 1 to 64 case-sensitive characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The DHCP server identifies the devices according to the Option60 field in the DHCP request packet. You can run the **dhcp client class-id** *class-id* command to

customize the Option60 field in the DHCP request packet sent from the DHCP client.

After you run the **dhcp client class-id** *class-id* command in the VLANIF interface view, the device that functions as the DHCP client fills the set Option60 in the DHCP request packet on the VLANIF interface.

Example

Set the class-id of a DHCP client to **huawei** on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client class-id huawei
```

8.3.9 dhcp client class-id (system view)

Function

The **dhcp client class-id** command is used to set the Option60 field in the DHCP request packet sent by the DHCP client.

The **undo dhcp client class-id** command is used to restore the default value of the Option60 field.

By default, the default value of the Option60 field depends on the device type, which is " huawei *Device Model*".

Format

dhcp client class-id *class-id*

undo dhcp client class-id

Parameters

Parameter	Description	Value
class-id	Indicates the value of the Option60 field.	The value is a string of 1 to 64 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The DHCP server identifies the devices according to the Option60 field in the DHCP request packet. You can run the **dhcp client class-id** *class-id* command to

customize the Option60 field in the DHCP request packet sent from the DHCP client.

Configuration information of the Option60 field is saved in the *storage device*:/dhcp/dhcp-client.options file. By default, the storage device needs to provide more than 80-byte storage space. You can run the **more dhcp/dhcp-client.options** command in the user view to check configuration information of the Option60 field.

After you run the **dhcp client class-id** *class-id* command in the system view, the device that functions as the DHCP client fills the set Option60 in the DHCP request packet sent from all of the interfaces.

Example

Set the class-ID of a DHCP client to **huawei**.

```
<Huawei> system-view
[Huawei] dhcp client class-id huawei
```

8.3.10 dhcp client client-id

Function

The **dhcp client client-id** command configures an identifier for a DHCP client.

The **undo dhcp client client-id** command restores the default identifier of a DHCP client.

By default, the identifier of a DHCP client is the client's MAC address.

Format

dhcp client client-id *client-id*

undo dhcp client client-id

Parameters

Parameter	Description	Value
client-id	Specifies the identifier of a DHCP client.	The value is a string of 2 to 64 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp client client-id** command configures an identifier for a DHCP client. The identifier is encapsulated into a DHCP Request message. When a DHCP client requests an IP address from a DHCP server, the DHCP server obtains the identifier of the DHCP client and assigns an IP address to the DHCP client with the specified identifier.

Example

Set the identifier of the DHCP client to **huawei_client** on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client client-id huawei_client
```

8.3.11 dhcp client expected-lease

Function

The **dhcp client expected-lease** command enables expected lease on a DHCP client.

The **undo dhcp client expected-lease** command disables expected lease on a DHCP client.

By default, expected lease is disabled on the DHCP client.

Format

dhcp client expected-lease *time*

undo dhcp client expected-lease

Parameters

Parameter	Description	Value
time	Specifies an expected lease for a DHCP client.	The value is an integer that ranges from 60 to 864000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcp client expected-lease** command applies to DHCP clients. An expected lease can be contained in Option 51 of a DHCP Request message sent to the

server. The server compares the expected lease with the lease in the address pool and assigns a shorter lease to the client.

NOTE

When the device functions as the DHCP client, the lease cannot be shorter than 8 seconds. Otherwise, some packets are discarded. Therefore, the lease configured on the peer end DHCP server cannot be shorter than 8 seconds.

Example

Set the expected lease to 7200s on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client expected-lease 7200
```

8.3.12 dhcp client gateway-detect

Function

The **dhcp client gateway-detect** command enables gateway detection on a DHCP client.

The **undo dhcp client gateway-detect** command disables gateway detection on a DHCP client.

By default, gateway detection is disabled on a DHCP client.

Format

dhcp client gateway-detect period *period* **retransmit** *retransmit* **timeout** *time*

undo dhcp client gateway-detect

Parameters

Parameter	Description	Value
period *period*	Specifies an interval for gateway detection on a DHCP client.	The value is an integer that ranges from 1 to 86400, in seconds.
retransmit *retransmit*	Specifies the retransmission count of gateway detection on a DHCP client.	The value is an integer that ranges from 1 to 10.
timeout *time*	Specifies the timeout period of gateway detection on a DHCP client.	It is an integer that ranges from 300 to 2000, in milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp client gateway-detect** command applies to DHCP clients. After a DHCP client obtains an IP address, the **dhcp client gateway-detect** command enables the DHCP client to detect the status of the gateway being used. If the gateway has an incorrect address or the gateway device fails, the DHCP client requests a new IP address from the DHCP server.

Precautions

Gateway detection applies to dual-homed scenarios.

Example

Enable gateway detection on GE1/0/0 of the DHCP client. Set the detection interval to 3600s, retransmission count to 3, and timeout period to 500 ms.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client gateway-detect period 3600 retransmit 3 timeout 500
```

8.3.13 dhcp client default-route preference

Function

The **dhcp client default-route preference** command configures the default route preference that a DHCP server delivers to a DHCP client.

The **undo dhcp client default-route preference** command restores the default value of the default route preference that a DHCP server delivers to a DHCP client.

By default, the default route preference that a DHCP server delivers to a DHCP client is 60.

Format

dhcp client default-route preference *preference-value*

undo dhcp client default-route preference

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
preference-value	Specifies the default route preference.	The value is an integer that ranges from 1 to 255. A smaller value indicates a higher preference.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

A DHCP client can obtain the default route through the DHCP server to dynamically update the routing table. The next-hop address of the default route is the DHCP client's gateway address carried in Option3.

The default route that a DHCP server delivers is the user network router (UNR) route with the default preference 60. You can run the **dhcp client default-route preference** command to change the default route preference.

Example

In the view of VLANIF100, set the default route preference that a DHCP server delivers to a DHCP client to 30.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client default-route preference 30
```

8.3.14 dhcp client hostname

Function

The **dhcp client hostname** command configures a host name for a DHCP/BOOTP client.

The **undo dhcp client hostname** command deletes the configured host name of a DHCP/BOOTP client.

By default, no host name is configured for a DHCP/BOOTP client.

Format

dhcp client hostname *hostname*

undo dhcp client hostname

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hostname	Specifies the name of a DHCP/BOOTP client.	The value is a string of 1 to 64 case-sensitive characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A DHCP server must obtain the host name of a client before assigning an IP address to the client. To configure a host name for a DHCP/BOOTP client, run the **dhcp client hostname** command. The host name is used to match the local domain name of the DHCP/BOOTP client.

Follow-up Procedure

After DHCP/BOOTP client is enabled, the device can use DHCP to obtain an IP address.

Example

Set the host name of a DHCP/BOOTP client to **huawei gateway** on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client hostname huawei gateway
```

8.3.15 dhcp client renew

Function

The **dhcp client renew** command renews the lease of the IP address obtained by a DHCP client.

Format

dhcp client renew

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command applies to the following scenarios:

- Manually renewing the lease

  If a DHCP server assigns the original IP address to the client, only the lease is renewed. If another DHCP server assigns an IP address to the client, the client obtains a new IP address and related network parameters.
- Updating the IP address

  When the DHCP client is migrated from a network segment to another network segment and the original IP address lease does not expire, the client needs to update the IP address.

After the **dhcp client renew** command is run, the DHCP client sends a lease renewal request to the DHCP server.

- If the DHCP client receives a positive reply from the server, the client updates the parameters such as the lease duration.
- If the DHCP client receives a negative reply from the server, the client releases the applied parameters and re-applies to the DHCP server for an IP address and other network parameters.
- If no reply is received, the client does not perform any operation.

The **dhcp client renew** command can be normally run only after the DHCP client function is enabled on the interface and an IP address is obtained.

Example

Renew the IP address lease on VLANIF100.

```
<Huawei> system-view
[Huawei] interface vlanif 100
[Huawei-Vlanif100] dhcp client renew
```

8.3.16 dhcp client request option-list exclude

Function

The **dhcp client request option-list exclude** command configures a list of default request options that are not carried in the Option55 field of DHCP Request messages.

The **undo dhcp client request option-list exclude** command deletes the list of default request options that are not carried in the Option55 field of DHCP Request messages.

 Copyright © Huawei Technologies Co., Ltd.

By default, the Option55 field in DHCP Request messages carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default.

Format

dhcp client request option-list exclude *option-code* &<1-8>

undo dhcp client request option-list exclude *option-code* &<1-8>

Parameters

Parameter	Description	Value
option-code	Specifies a list of default request options that are excluded from the Option55 field.	The value is of enumerated type and can be 3, 6, 15, 28, 33, 44, 121, and 184.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The Option55 field in DHCP Request messages is used to set the request option list. DHCP clients use this option to specify network configuration parameters that need to be obtained from the DHCP server. By default, the Option55 field carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default. You can run the **dhcp client request option-list exclude** command to configure a list of default options that are excluded from the Option55 field based on network requirements.

For option meanings, see *DHCP Options* in *CLI-based Configuration - IP Service Configuration Guide - DHCP Configuration*.

Example

Configure the default request option 3 to be excluded from the Option55 field in DHCP Request messages on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client request option-list exclude 3
```

 Copyright © Huawei Technologies Co., Ltd.

8.3.17 dhcp client request option-list

Function

The **dhcp client request option-list** command configures a list of request options that the Option55 field in DHCP Request packets carries besides the default options.

The **undo dhcp client request option-list** command deletes a list of request options that the Option55 field in DHCP Request packets carries besides the default options.

By default, the Option55 field in DHCP Request packets carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default.

Format

dhcp client request option-list *option-code* &<1-9>

undo dhcp client request option-list *option-code* &<1-9>

Parameters

Parameter	Description	Value
option-code	Specifies a list of request options that the Option55 field carries besides the default options.	The value is of enumerated type and can be 4, 7, 17, 42, 43, 66, 67, 120, and 129.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The Option55 field in DHCP Request packets is used to set the request option list. DHCP clients use this option to specify network configuration parameters that need to be obtained from the DHCP server. By default, the Option55 field carries request options 3, 6, 15, 28, 33, 44, 121, and 184 by default. Besides the default options, you can run the **dhcp client request option-list option-code** command to set a list of other request options that the Option55 field carries.

For option meanings, see *DHCP Options* in *CLI-based Configuration - IP Service Configuration Guide - DHCP Configuration*.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the Option55 field in DHCP Request packets to carry option 4 on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp client request option-list 4
```

8.3.18 dhcp enable

Function

The **dhcp enable** command enables the DHCP function.

The **undo dhcp enable** command disables the DHCP function.

By default, the DHCP function is disabled.

Format

dhcp enable

undo dhcp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network scale and complexity increase makes network configurations complex. For example, computers frequently change their locations, and IP addresses are insufficient for these computers. The DHCP protocol is developed to address these problems. The **dhcp enable** command enables the DHCP function on the device.

Precautions

The **dhcp enable** command is the prerequisite for configuring DHCP-related functions, including DHCP relay, DHCP snooping, and DHCP server. These functions take effect only after the **dhcp enable** command is run. After the **undo dhcp enable** command is run, all DHCP-related configurations of the device are deleted. After DHCP is enabled again using the **dhcp enable** command, all DHCP-related configurations of the device are restored to the default configurations.

Follow-up Procedure

Configure DHCP relay, DHCP Client, and DHCP server functions.

Example

Enable the DHCP function on the device.

```
<Huawei> system-view
[Huawei] dhcp enable
```

Related Topics

8.3.26 dhcp select interface

8.3.75 dns-list

8.3.19 dhcp link arp

Function

The **dhcp link arp** command configures an interface of a DHCP client to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

The **undo dhcp link arp** command configures an interface of a DHCP client not to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

By default, an interface of a DHCP client does not deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

Format

dhcp link arp

undo dhcp link arp

Parameters

None

Views

Ethernet interface view, Eth-Trunk interface view, GE interface view, VE interface view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to configure a DHCP client to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure an interface of a DHCP client to deliver a static ARP entry after it receives a DHCP ACK packet from the DHCP server.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp link arp
```

8.3.20 dhcp option template

Function

The **dhcp option template** command creates a DHCP Option template and enters the DHCP Option template view.

The **undo dhcp option template** command deletes a configured DHCP Option template.

By default, no DHCP Option template is created on the device.

Format

dhcp option template *template-name*

undo dhcp option template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of the DHCP Option template.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value can contain digits, letters, underscores (_), hyphens (-), and dots (.), but cannot be set to **-** or **--**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. During network deployment, a DHCP server dynamically allocates IP addresses with leases to clients or allocates fixed IP

addresses to some clients. For example, laptops or terminals are often moved to different places in enterprises, and they can obtain IP addresses using the dynamic allocation mode. However, IP addresses obtained dynamically are randomly allocated, and cannot be set to specified IP addresses. To allocate fixed IP addresses to some fixed terminals (such as IP phones), run the **8.3.108 static-bind** command in the global address view to bind IP addresses to MAC addresses of the clients so that the clients are allocated fixed IP addresses.

In some cases, you need to allocate other network configuration parameters except IP addresses to fixed static terminals. For example, besides obtaining an IP address, an IP phone needs information such as the startup configuration file to register normally. In this case, you can configure a DHCP Option template and configure network configuration parameters except the IP address required by the client in the DHCP Option template. Then bind the DHCP Option template to the fixed terminal in the global address pool. The DHCP server then allocates the IP address and other parameters to the terminal.

Precautions

Network parameters configured in the DHCP Option template view take effect only for static clients. A DHCP Option template can be bound to multiple clients. Run the **static-bind ip-address** *ip-address* **mac-address** *mac-address* [**option-template** *template-name*] command to configure a DHCP Option template that is bound to static clients.

Example

Create a DHCP Option template named **test**.

```
<Huawei> system-view
[Huawei] dhcp option template test
```

Related Topics

8.3.64 display dhcp option template

8.3.108 static-bind

8.3.21 dhcp relay release

Function

The **dhcp relay release** command configures a DHCP relay agent to send a release message to a DHCP server for releasing the IP address assigned to a DHCP client.

Format

In the system view:

dhcp relay release *client-ip-address mac-address* [**vpn-instance** *vpn-instance-name*] [*server-ip-address*]

In the interface view:

dhcp relay release *client-ip-address mac-address* [*server-ip-address*]

Parameters

Parameter	Description	Value
client-ip-address	Specifies the IP address of a DHCP client.	The value is in dotted decimal notation.
mac-address	Specifies the MAC address of a DHCP client.	The value is in H-H-H format. H is a hexadecimal number of 1 to 4 digits.
server-ip-address	Specifies the IP address of a DHCP server. If this parameter is specified, a DHCP relay agent sends a release message to the specified DHCP server for releasing the IP address assigned to a DHCP client.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified DHCP server releasing IP addresses belongs.	The value must an existing VPN name.

Views

Interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. In some situations, for example, a user is forced to go offline, the user's IP address is no longer used. However, the user cannot access the network, and will not send a DHCP release message to the DHCP server to release the IP address assigned by the DHCP server. Before the IP address lease expires, the DHCP server will not assign the user's IP address to another client, wasting IP addresses. In this case, you can run the **dhcp relay release** command to configure a DHCP relay agent to send a DHCP release message to the DHCP server. After receiving the message, the DHCP server sets the status of the IP address to idle. The DHCP server then can assign the released IP address to another client.

If a DHCP server address is specified, the DHCP relay agent sends an address release request only to the specified DHCP server. If no DHCP server address is specified, the following situations occur:

 Copyright © Huawei Technologies Co., Ltd.

- When the **dhcp relay release** command is run in the system view, the DHCP relay agent sends an address release request to DHCP servers on all the interfaces working in DHCP relay mode.
- When the **dhcp relay release** command is run in the interface view, the DHCP relay agent sends an address release request to all DHCP servers on the VLANIF interface.

Precautions

The **dhcp relay release** command only releases the IP addresses dynamically assigned by DHCP servers.

Example

Configure a DHCP relay agent to send a release message to the DHCP server at 10.1.1.1 for releasing the IP address 192.168.1.1 assigned to the DHCP client whose MAC address is 0050-ba34-2000.

```
<Huawei> system-view
[Huawei] dhcp relay release 192.168.1.1 0050-ba34-2000 10.1.1.1
```

8.3.22 dhcp relay server-ip

Function

The **dhcp relay server-ip** command configures a DHCP server address on an interface enabled with DHCP relay.

The **undo dhcp relay server-ip** command deletes the configured DHCP server addresses on an interface enabled with DHCP relay.

By default, no DHCP server address on an interface enabled with DHCP relay is configured.

Format

dhcp relay server-ip *ip-address*

undo dhcp relay server-ip { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.
all	Deletes all the DHCP server addresses configured on an interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. When a DHCP client needs to send a DHCP Discover message to a DHCP server on a different network segment through a DHCP relay agent, you must configure the DHCP server address on the DHCP relay agent.

When a DHCP relay agent forwards a DHCP Discover message, it does not check whether the DHCP server status is Down. If multiple DHCP server addresses are configured on an interface, multiple DHCP servers respond with DHCP Offer messages to the DHCP client. However, the DHCP client uses the first received DHCP Offer message. As a result, IP addresses in the IP address pool on the first DHCP server are insufficient, but available IP addresses in the IP address pools on the other DHCP servers are not allocated. To make each DHCP server allocate the same number of IP addresses, a DHCP relay agent changes the forwarding order each time it forwards a DHCP Discover message, so that load balancing is implemented among DHCP servers. A DHCP relay agent forwards a DHCP Discover message as follows:

- The DHCP relay agent forwards the message to all DHCP servers by default, and changes the forwarding order each time it forwards a DHCP Discover message.
- You can configure the **8.3.85 ip relay address cycle** command to reduce the number of packets received by a DHCP server and lessen the load of a DHCP server. After this command is configured, the DHCP relay agent forwards a received DHCP Discover message to one DHCP server at a time, and forwards the DHCP Discover message to a different DHCP server each time it receives the message.

Prerequisites

DHCP relay has been enabled on the interface using the **dhcp select relay** command.

Precautions

If you run the **dhcp relay server-ip** command for multiple times, multiple DHCP server addresses are configured.

Each interface that is enabled with DHCP relay can be configured with a maximum of 8 DHCP server addresses.

Example

Configure DHCP relay on GE1/0/0 and add two DHCP server addresses.

```
<Huawei> system-view
[Huawei] dhcp enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select relay
[Huawei-GigabitEthernet1/0/0] dhcp relay server-ip 10.1.1.2
[Huawei-GigabitEthernet1/0/0] dhcp relay server-ip 10.1.1.3
```

Related Topics

8.3.28 dhcp select relay

8.3.23 dhcp relay server-select

Function

The **dhcp relay server-select** command configures a DHCP server group for a DHCP relay agent.

The **undo dhcp relay server-select** command deletes the configured DHCP server group of a DHCP relay agent.

By default, no DHCP server group is configured.

Format

dhcp relay server-select *group-name*

undo dhcp relay server-select

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp relay server-select** command applies to DHCP relay agents. When a DHCP client needs to send DHCP requests to a DHCP server using a DHCP relay agent, you can run the **dhcp relay server-select** command to specify a DHCP server group for the DHCP relay agent and configure the DHCP server address.

Prerequisites

1. A DHCP server group has been created using the **dhcp server group** command.
2. The DHCP relay function has been enabled using the **dhcp select relay** command so that the system can forward DHCP packets to the specified DHCP server.

Precautions

- Multiple interfaces can be configured with the same DHCP server group, and one interface can be configured with only one DHCP server group.
- Addresses of DHCP servers in a DHCP server group cannot be on the same network segment with addresses of interfaces enabled with DHCP relay.
- If you run the **dhcp relay server-select** command in the same interface view for multiple times, only the latest configuration takes effect. If a specified DHCP server group does not exist, the configuration fails; however, the latest configured DHCP server group still takes effect.
- The **dhcp relay server-select** command can only be used on Layer 3 interfaces, including Layer 3 GE interfaces, Layer 3 Ethernet interfaces, and Layer 3 Eth-Trunk interfaces.

Example

Configure the DHCP server group of a DHCP relay agent as **group1** on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server group group1
[Huawei-dhcp-server-group-group1] dhcp-server 10.10.10.10
[Huawei-dhcp-server-group-group1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select relay
[Huawei-GigabitEthernet1/0/0] dhcp relay server-select group1
```

Related Topics

8.3.40 dhcp server group
8.3.59 dhcp-server
8.3.65 display dhcp relay

8.3.24 dhcp relay trust option82

Function

The **dhcp relay trust option82** command enables Option 82 on the DHCP relay agent.

The **undo dhcp relay trust option82** command disables Option 82 on the DHCP relay agent.

By default, Option 82 is enabled on the DHCP relay agent.

Format

dhcp relay trust option82

undo dhcp relay trust option82

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP relay agent to enable the Option 82 function. After receiving a DHCP packet that carries the Option 82 field but the giaddr field of the packet is 0, the DHCP relay agent processes the packet by default. Using the **undo dhcp relay trust option82** command, the DHCP relay agent discards the packet.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Example

Enable Option 82 trusted of the DHCP relay agent.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp relay trust option82
```

8.3.25 dhcp select global

Function

The **dhcp select global** command enables an interface to use the global address pool.

The **undo dhcp select global** command disables an interface from using the global address pool.

By default, an interface is disabled from using the global address pool.

Format

dhcp select global

undo dhcp select global

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select global** command applies to DHCP servers. After receiving a DHCP Request message from a DHCP client, a DHCP server assigns an IP address from the local address pool to the client. Run the **dhcp select global** command to configure the device to assign IP addresses from the global address pool. When no interface address pool is created for the DHCP server, the DHCP server assigns an IP address from the global address pool to an online user.

The device can also assign IP addresses from an interface address pool using the **dhcp select interface** command in the interface view.

Prerequisites

- DHCP has been enabled using the **dhcp enable** command in the system view.
- Before running the **dhcp select global** command, you need to run the **ip address** command to configure the interface IP address.

Precautions

- When the device is configured as a DHCP server, if the server's real IP address is configured as the DHCP server IP address on a DHCP relay agent, the server's Layer 3 interface that receives relayed DHCP messages can process these messages, without the need of running the **dhcp select global** command on the interface.
- When the device is configured as a DHCP server, if the VRRP virtual IP address of the server's Layer 3 interface that does not receive DHCP messages is configured as the DHCP server IP address on the DHCP relay agent, the DHCP server cannot process messages relayed by the DHCP relay agent. The DHCP server can process messages relayed by the DHCP relay agent only if the VRRP virtual IP address of the server's Layer 3 interface that receives DHCP messages is configured as the DHCP server IP address on the DHCP relay agent and the **dhcp select global** command is configured on this Layer 3 interface.
- In IPoEoA scenarios, the DHCP server function for the global address pool cannot be enabled on a VE interface of a device. That is, the **dhcp select global** and **map bridge virtual-ethernet** *interface-number* commands cannot be configured on the same VE interface. Otherwise, the DHCP server function does not take effect.

Example

Enable GE1/0/0 to use the global address pool.

```
<Huawei> system-view
[Huawei] dhcp enable
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select global
```

Related Topics

8.3.18 dhcp enable

8.3.83 ip pool (system view)

8.3.26 dhcp select interface

7.5.13 map bridge

8.3.26 dhcp select interface

Function

The **dhcp select interface** command enables an interface to use the interface address pool.

The **undo dhcp select interface** command disables an interface from using the interface address pool.

By default, the DHCP server function using the interface address pool is disabled on an interface.

Format

dhcp select interface

undo dhcp select interface

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select interface** command applies to DHCP servers. After receiving a DHCP Request message from a DHCP client, a DHCP server assigns an IP address from the local address pool to the client. Run the **dhcp select interface** command to configure a DHCP server to assign IP addresses from the interface address pool to clients.

The device can also assign IP addresses from a global address pool using the **dhcp select global** command.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This command is not supported in the tunnel interface view.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

An IP address has been configured for an interface using the **ip address** command. The IP addresses assigned by the address pool and configured on the interface are on the same network segment.

Precautions

- By default, an management interface is disabled from the DHCP server function using the interface address pool. However, the **dhcp select interface** command is added to the factory settings of an management interface. In this way, when a device is started based on the factory settings, the DHCP server function of the management interface is enabled.
- In IPoEoA scenarios, the DHCP server function for the interface address pool cannot be enabled on a VE interface of a device. That is, the **dhcp select interface** and **map bridge virtual-ethernet** *interface-number* commands cannot be configured on the same VE interface. Otherwise, the DHCP server function does not take effect.

Example

Enable GE1/0/0 to use the interface address pool.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.2 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
```

Related Topics

7.5.13 map bridge

8.3.27 dhcp server alarm ip-used percentage

Function

The **dhcp server alarm ip-used percentage** command configures the percentage of the alarms indicating that the addresses in an interface address pool are used up, and the percentage of the clear alarms.

The **undo dhcp server alarm ip-used percentage** command restores the default percentages of the alarms and clear alarms.

By default, the percentage of the alarms indicating that the addresses in an interface address pool are used up is 100%, and the percentage of the clear alarms is 50%.

Format

dhcp server alarm ip-used percentage *alarm-resume-percentage alarm-percentage*

undo dhcp server alarm ip-used percentage

Parameters

Parameter	Description	Value
alarm-resume-percentage	Specifies the percentage of the clear alarms.	The value is an integer that ranges from 1 to 100. The default value is **50**. **NOTE** The percentage of the clear alarms cannot exceed that of the alarms.
alarm-percentage	Specifies the percentage of the alarms indicating that the addresses in an address pool are used up.	The value is an integer that ranges from 1 to 100. The default value is **100**.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the addresses in an interface address pool are used up, alarms are sent to notify the administrator.

Precautions

The percentage of the clear alarms cannot exceed that of the alarms.

Example

Configure the percentage of the alarms indicating that the addresses in an interface address pool are used up, and the percentage of the clear alarms in the interface address pool of the VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.10.10.10 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server alarm ip-used percentage 80 90
```

Related Topics

8.3.18 dhcp enable
8.3.26 dhcp select interface

8.3.28 dhcp select relay

Function

The **dhcp select relay** command enables the DHCP relay function.

The **undo dhcp select relay** command disables the DHCP relay function.

By default, the DHCP relay function is disabled.

Format

dhcp select relay

undo dhcp select relay

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp select relay** command applies to DHCP relay agents. If the DHCP server and client are on the same network segment, they can directly communicate with each other using DHCP. In this case, no DHCP relay agent is needed. If the DHCP server and client are on different network segments, the DHCP relay function must be enabled to forward DHCP messages.

Prerequisites

The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.

Follow-up Tasks

- To ensure that a DHCP relay agent can forward DHCP packets to a DHCP server, run the **8.3.23 dhcp relay server-select** or **dhcp relay server-ip** command on the DHCP relay-enabled interface to configure the correct IP address of the DHCP server.

 Copyright © Huawei Technologies Co., Ltd.

- To ensure that a DHCP server can forward DHCP packets to a DHCP relay agent, you must configure a route to the DHCP relay agent on the DHCP server.

Precautions

- The DHCP server must select an IP address in the same network segment with the DHCP relay agent from the global address pool to ensure that the DHCP client obtains an IP address on the local network segment. No interface address pool can be configured on the interface that connects the DHCP server and relay agent.
- Before using the **dhcp select relay** command on a G.SHDSL or VDSL interface, ensure that the interface works in PTM mode.
- If DHCP relay is enabled in a super-VLAN, DHCP snooping cannot be enabled in this super-VLAN.

Example

Enable the DHCP relay function on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select relay
```

Related Topics

8.3.23 dhcp relay server-select

8.3.22 dhcp relay server-ip

8.3.29 dhcp server bootfile

Function

The **dhcp server bootfile** command configures the name of the startup configuration file for a DHCP client.

The **undo dhcp server bootfile** command deletes the configured name of the startup configuration file for a DHCP client.

By default, the startup configuration file name is not configured for a DHCP client.

Format

dhcp server bootfile *bootfile*

undo dhcp server bootfile

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bootfile	Specifies the name of the startup configuration file for a DHCP client.	The value is a string of 1 to 127 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP clients. After the name of the startup configuration file is configured using the **dhcp server bootfile** command, the Offer and ACK packets sent from the DHCP server carry this file name. The DHCP client can acquire the startup configuration file from the specified server based on the file name.

Prerequisites

1. The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.
2. The DHCP server has been enabled on the interface using the **8.3.26 dhcp select interface** command.

Example

Configure the name of the startup configuration file as **start.ini** for the DHCP client on the Vlanif100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.1.1 255.255.255.0
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server bootfile start.ini
```

Related Topics

8.3.18 dhcp enable

8.3.26 dhcp select interface

 Copyright © Huawei Technologies Co., Ltd.

8.3.30 dhcp server bootp

Function

Using the **dhcp server bootp** command, you can enable a DHCP server to respond to a Bootstrap Protocol (BOOTP) request.

Using the **undo dhcp server bootp** command, you can disable a DHCP server from responding to a BOOTP request.

By default, a DHCP server responds to a BOOTP request.

Format

dhcp server bootp

undo dhcp server bootp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A DHCP server and a BOOTP server may reside on the same network segment. The BOOTP server assigns static IP addresses to BOOTP clients. As defined in the DHCP protocol, a DHCP server can also respond to BOOTP requests to assign IP addresses to BOOTP clients. BOOTP clients may obtain IP addresses from the DHCP server but not the BOOTP server.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command in the system view.

Follow-up Procedure

Using the **dhcp server bootp automatic** command in the system view, you can enable the DHCP server to allocate IP addresses to BOOTP clients.

Example

Enable a DHCP server to respond to a BOOTP request.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server bootp
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.18 dhcp enable

8.3.31 dhcp server bootp automatic

Function

The **dhcp server bootp automatic** command enables the DHCP server to dynamically allocate IP addresses to BOOTP clients.

The **undo dhcp server bootp automatic** command disables the DHCP server from dynamically allocating IP addresses to BOOTP clients.

By default, a DHCP server does not dynamically allocate IP addresses to BOOTP clients.

Format

dhcp server bootp automatic

undo dhcp server bootp automatic

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When BOOTP clients need to obtain their IP addresses, DNS server's IP address, and gateway IP address from a DHCP server, you need to run the **dhcp server bootp automatic** command to enable the DHCP server to dynamically allocate IP addresses to BOOTP clients.

Prerequisites

- DHCP has been enabled globally using the **dhcp enable** command in the system view.
- The DHCP server has been enabled to respond to BOOTP requests by using the **dhcp server bootp** command, or **dhcp server bootp automatic** cannot take effect.

Precautions

When the device functions as the DHCP server, the device can allocate IP addresses to BOOTP clients if the BOOTP clients reside on the same network as

 Copyright © Huawei Technologies Co., Ltd.

the DHCP server. You can run the **dhcp server bootp automatic** command to dynamically allocate IP addresses. You can also run the **static-bind** command or the **dhcp server static-bind** command to allocate IP addresses to BOOTP clients in the static binding mode.

Example

Enable the DHCP server to allocate IP addresses to BOOTP clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server bootp
[Huawei] dhcp server bootp automatic
```

Related Topics

8.3.18 dhcp enable

8.3.30 dhcp server bootp

8.3.32 dhcp server conflict auto-recycle interval

Function

The **dhcp server conflict auto-recycle interval** command enables automatic reclaim of conflicting IP addresses in the interface address pool and configures the interval for the automatic reclaim.

The **undo dhcp server conflict auto-recycle interval** command disables automatic reclaim of conflicting IP addresses in the interface address pool and deletes the configured interval for the automatic reclaim.

By default, automatic reclaim of conflicting IP addresses in the interface address pool is disabled.

Format

dhcp server conflict auto-recycle interval day *day* [**hour** *hour* [**minute** *minute*]]

undo dhcp server conflict auto-recycle interval

Parameters

Parameter	Description	Value
day *day*	Specifies the interval for the automatic reclaim, in days.	The value is an integer that ranges from 0 to 999, in days. The default value is 0.
hour *hour*	Specifies the interval for the automatic reclaim, in hours.	The value is an integer that ranges from 0 to 23, in hours. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
minute *minute*	Specifies the interval for the automatic reclaim, in minutes.	The value is an integer that ranges from 0 to 59, in minutes. The default value is 0.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When a DHCP server allocates IP addresses to clients, IP address conflict may occur because IP addresses of some hosts have been manually configured. In this case, the DHCP server considers these IP addresses as conflicting IP addresses, and allocates available IP addresses from the conflicting IP addresses to clients only after available IP addresses in the address pool are used up. To reclaim conflicting IP addresses promptly, the administrator can run this command to enable automatic reclaim and specify the reclaim interval.

Prerequisites

1. IP addresses in the interface address pool have been configured using the **ip address** command.
2. The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Example

Enable automatic reclaim for conflicting IP addresses in the address pool on VLANIF 100, and set the interval for automatic reclaim to one day.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.1.1 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server conflict auto-recycle interval day 1
```

8.3.33 dhcp server database

Function

The **dhcp server database** command enables the function to save the current DHCP data to storage devices.

 Copyright © Huawei Technologies Co., Ltd.

The **undo dhcp server database** command disables the function to save the DHCP data to storage devices.

By default, DHCP data is not saved to storage devices.

Format

dhcp server database { **enable** | **recover** | **write-delay** *interval* }

undo dhcp server database { **enable** | **recover** | **write-delay** }

Parameters

Parameter	Description	Value
enable	Enables the function to save DHCP data to storage devices.	-
recover	Recovers DHCP configurations using DHCP data in storage device.	-
write-delay *interval*	Specifies the interval at which DHCP data is saved.	The value is an integer ranging from 300 to 86400, in seconds. The default value is 3600 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCP server, run the **dhcp server database enable** command to enable the device to save DHCP data to storage devices. This avoids data loss caused by device faults. Then the system generates **lease.txt** and **conflict.txt** files in the storage device. The two files save address lease information and address conflict information respectively. Run the **8.3.67 display dhcp server database** command to check the storage device for saving DHCP data. After the **dhcp server database enable** command is run, current DHCP data is automatically saved at the specified interval, and previous data files are overwritten. The interval can be set using the **dhcp server database write-delay** *interval* command.

 Copyright © Huawei Technologies Co., Ltd.

If a fault occurs on the device, run the **dhcp server database recover** command to recover DHCP data from storage devices during the system restarts.

Prerequisites

The **dhcp server database enable** command has been run to enable the device to save DHCP data to storage devices, and ensure that the storage devices work properly.

Precautions

- The lease.txt and conflict.txt files are overwritten periodically; therefore, you are advised to back up and save the two files to other locations.
- The time displayed in the lease.txt and conflict.txt files is the UTC time rather than the system time, and you do not need to pay attention to time zone information.

Example

Enable the device to save the current DHCP data to storage devices and set the interval at which DHCP data is saved to 2000s.

```
<Huawei> system-view
[Huawei] dhcp server database enable
[Huawei] dhcp server database write-delay 2000
```

Recover DHCP configuration using the DHCP data saved on storage devices.

```
<Huawei> system-view
[Huawei] dhcp server database recover
```

Related Topics

8.3.67 display dhcp server database

8.3.34 dhcp server dns-list

Function

The **dhcp server dns-list** command configures DNS server addresses for an interface address pool.

The **undo dhcp server dns-list** command deletes the specified DNS server addresses of an interface address pool.

By default, no DNS server address is configured in an interface address pool.

Format

dhcp server dns-list { *ip-address* &<1-8> | **unnumbered interface** *interface-type interface-number* }

undo dhcp server dns-list { **all** | *ip-address* | **unnumbered interface** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the DNS server. You can configure up to eight IP addresses for the DNS servers and separate two IP addresses with a space.	The value is in dotted decimal notation.
unnumbered interface *interface-type interface-number*	Borrows the DNS server address obtained by the interface as the DNS server IP address.	-
all	Deletes all IP addresses of DNS servers specified for the client.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If user hosts access hosts on the network through the domain name, user hosts need to send DNS Request messages to the DNS server and resolve the domain name. To enable DNS services on the DHCP client, specify the DNS server address for the interface address pool on the DHCP server. The DHCP server can assign both the specified DHCP server address and an IP address to the client. To configure DNS server addresses for a global address pool, run the **dns-list** command.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- Each address pool can be configured with a maximum of eight DNS server addresses. If multiple DNS server addresses are configured, the first DNS server address assigned to the DHCP client functions as the primary address and other addresses are secondary addresses.
- To specify multiple DNS servers, enter multiple DNS server addresses in the **dhcp server dns-list** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify a DNS server at 10.10.1.254 for domain name resolution when IP addresses in the interface address pool on GE1/0/0 are assigned to clients.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server dns-list 10.10.1.254
```

Related Topics

8.3.26 dhcp select interface

8.3.75 dns-list

8.3.35 dhcp server domain-name (interface view)

8.3.35 dhcp server domain-name (interface view)

Function

The **dhcp server domain-name** command configures a DNS domain name assigned to a DHCP client.

The **undo dhcp server domain-name** command deletes a specified domain name.

By default, no domain name is configured for the DHCP client.

Format

dhcp server domain-name *domain-name*

undo dhcp server domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name that the DHCP server assigns to the client.	The value is a string of 1 to 63 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Run the **dhcp server domain-name** command on a DHCP server to specify a domain name for each interface address pool. When allocating IP addresses to clients, the DHCP server also sends the domain names to the clients.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

To configure a domain name for the global address pool, run the **domain-name** command.

Example

Set the domain name assigned by the DHCP address pool on the interface to **example.com**.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server domain-name example.com
```

Related Topics

8.3.76 domain-name

8.3.26 dhcp select interface

8.3.36 dhcp server excluded-ip-address

Function

The **dhcp server excluded-ip-address** command specifies the range of IP addresses that cannot be automatically assigned to clients from an interface address pool.

The **undo dhcp server excluded-ip-address** command deletes the specified range of IP addresses that cannot be automatically assigned to clients from the interface address pool.

By default, all IP addresses in the address pool can be automatically assigned to clients.

Format

dhcp server excluded-ip-address *start-ip-address* [*end-ip-address*]

undo dhcp server excluded-ip-address *start-ip-address* [*end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address that cannot be automatically assigned.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address that cannot be automatically assigned. If *end-ip-address* is not specified, only *start-ip-address* cannot be automatically assigned.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server excluded-ip-address** command applies to DHCP servers. Fixed IP addresses are allocated to some specific hosts (such as the WWW server) on the network for a long time. If these hosts' IP addresses are overlapped with IP addresses in the address pool and the DHCP server allocates these overlapped IP addresses to other hosts, IP address conflicts may occur. To prevent the IP address conflict, you need to exclude these IP addresses from being automatically allocated in the address pool.

You can run the **dhcp server excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the interface address pool.

You can run the **excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the global address pool.

Prerequisites

- An address segment in the interface address pool is configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- IP addresses that cannot be automatically assigned must be in the address pool. If the range of IP addresses in the address pool is changed using the **dhcp server ip-range** command, IP addresses that are configured not to be automatically assigned must be within the changed IP address range.
- You do not need to exclude the gateway address configured using the **8.3.37 dhcp server gateway-list** command from being automatically allocated. The device automatically adds the gateway address into the list of IP addresses that cannot be automatically allocated.

  You do not need to exclude the IP address of a server's interface connecting to a client from being automatically allocated. The device automatically sets the interface IP address to the Conflict status during address allocation.
- If you run this command multiple times, you can specify multiple IP addresses or IP address segments that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check used IP addresses in the current address pool, and then specify unused IP addresses that cannot be automatically assigned. To exclude used IP addresses from being automatically assigned, run the **reset ip pool** command to reclaim used IP addresses first.

Example

Specify that IP addresses 192.168.1.1 to 192.168.1.20 cannot be automatically assigned to clients from the address pool on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server excluded-ip-address 192.168.1.1 192.168.1.20
```

Related Topics

8.3.26 dhcp select interface

8.3.77 excluded-ip-address

8.3.37 dhcp server gateway-list

Function

The **dhcp server gateway-list** command sets the default gateway IP address that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server gateway-list** command deletes the configured default gateway IP address.

By default, the default gateway IP address that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server gateway-list *ip-address* &<1-8>

undo dhcp server gateway-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address. You can configure a maximum of eight gateway addresses, which are separated by spaces.	The value is in decimal dotted notation.
all	Indicates all IP addresses.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

To load balance traffic and improve network reliability, you can configure multiple default gateway addresses.

NOTICE

Do not configure the default gateway address allocated to DHCP clients as a broadcast address.

If the VRRP virtual IP address is configured on the interface and no gateway address is pre-allocated to the DHCP client using the **dhcp server gateway-list** command, the DHCP server uses the first VRRP virtual IP address as the gateway address to be allocated to the client. If no VRRP virtual IP address is configured on the interface, the DHCP server uses the physical IP address of the interface as the gateway address to be allocated to the client.

If the **dhcp server gateway-list** command is not configured, the gateway address allocated by the DHCP server to the DHCP client may fail to be displayed in trace information during fault diagnosis. Therefore, you are advised to configure this command if the DHCP server function based on an interface address pool is used.

Example

Enable a DHCP server on a GE1/0/0 to pre-allocate default gateway address 10.1.1.1 to DHCP clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server gateway-list 10.1.1.1
```

8.3.38 dhcp server force insert option

Function

The **dhcp server force insert option** command configures a DHCP server to forcibly insert an Option field specified in the interface address pool to a DHCP Response packet that it sends to a DHCP client.

The **undo dhcp server force insert option** command deletes the Option field forcibly inserted to a DHCP Response packet that a DHCP server sends to a DHCP client.

By default, a DHCP server does not forcibly insert an Option field to a DHCP Response packet that it sends to a DHCP client.

Format

dhcp server force insert option *code* &<1-254>

undo dhcp server force insert option *code* &<1-254>

Parameters

Parameter	Description	Value
code	Specifies the code for a forcibly replied option. You can configure a DHCP server to forcibly reply one or more options.	The value is an integer that ranges from 1 to 254.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In general, when a DHCP client applies for an IP address from a DHCP server, parameters contained in the DHCP Request packet specify the options the client requires. The DHCP server inserts the required options to a DHCP Response packet.

Sometimes, a device, functioning as a DHCP server, receives a DHCP Request packet that contains no parameter specifying the options the client requires. However, the client still wants to obtain the options configured on the interface address pool. You can run the **dhcp server force insert option** *code* &<1-254> command to configure the DHCP server to forcibly insert an Option field to the DHCP Response packet.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

1. The device has been configured to assign IP addresses in the interface address pool using the **dhcp select interface** command.
2. The Option field has been configured in the interface address pool using the **dhcp server option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command in the interface view.

Example

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server option 4 hex 11 22
[Huawei-GigabitEthernet1/0/0] dhcp server force insert option 4
```

Related Topics

8.3.26 dhcp select interface

8.3.49 dhcp server option

8.3.39 dhcp server force response

Function

The **dhcp server force response** command forces a DHCP server to reply with a DHCP NAK message.

The **undo dhcp server force response** command restores the default settings.

By default, a DHCP server is not forced to reply with a DHCP NAK message.

Format

dhcp server force response

undo dhcp server force response

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Scenario

When a DHCP client goes online in two steps, the IP address requested by the DHCP client is in the IP address pool, but no lease record of the DHCP client is found in the address pool. For example, after obtaining an IP address from another DHCP server, a wireless user roams to the current DHCP server and the original IP address is in the address pool of the current DHCP server. Alternatively, the address pool is reset and the original user needs to go online again. In this case, when receiving a DHCP Request message from the DHCP client, the DHCP server keeps silent and does not reply the DHCP client with a DHCP NAK message. The DHCP client can apply for an IP address to go online again in four steps only after the two steps for the client to go online time out. As a result, the DHCP client is slow in obtaining an IP address. To force the DHCP server to reply with a DHCP NAK message, you can run the **dhcp server force response** command, so that the DHCP client can quickly enter the four-step process for going online and apply for an IP address again.

Prerequisites

DHCP has been enabled on the device using the **dhcp enable** command.

Example

Force a DHCP server to reply with a DHCP NAK message.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server force response
```

8.3.40 dhcp server group

Function

The **dhcp server group** command creates a DHCP server group and displays the DHCP server group view or directly displays the view of the existing DHCP server group.

The **undo dhcp server group** command deletes an existing DHCP server group.

By default, no DHCP server group is configured.

Format

dhcp server group *group-name*

undo dhcp server group *group-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. Generally, a DHCP relay agent serves multiple DHCP servers. To manage these DHCP servers in a unified manner, run the **dhcp server group** command to create a DHCP server group. The DHCP server group then assigns IP addresses to users using the DHCP relay agent.

Follow-up Procedure

- Run the **dhcp-server** command to add DHCP servers to the DHCP server group.
- Run the **8.3.23 dhcp relay server-select** command in the interface view to specify a DHCP server group for the DHCP relay agent.

Precautions

You can configure a maximum of 64 DHCP server groups in the system, and a maximum of 8 DHCP servers in a DHCP server group.

Example

Create a DHCP server group named **dhcp-srv1**.

```
<Huawei> system-view
[Huawei] dhcp server group dhcp-srv1
```

Related Topics

8.3.59 dhcp-server

8.3.68 display dhcp server group

8.3.23 dhcp relay server-select

8.3.41 dhcp server import all

Function

The **dhcp server import all** command enables the device to automatically obtain the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from an interface address pool.

The **undo dhcp server import all** command disables the device from automatically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from an interface address pool.

By default, the device is disabled from automatically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from an interface address pool.

Format

dhcp server import all

undo dhcp server import all

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP server. Run the **dhcp server import all** command on the DHCP server to automatically allocate the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the carrier to the DHCP client.

Prerequisites

The DHCP server has been enabled on the interface using the **8.3.26 dhcp select interface** command.

Precautions

The **dhcp server import all** command can only be used on Layer 3 interfaces, including Layer 3 GE interfaces, Layer 3 Ethernet interfaces, and Layer 3 Eth-Trunk interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the device to automatically obtain configurations of the DNS server and NetBIOS server from an interface address pool.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server import all
```

Related Topics

8.3.72 display ip pool import all
8.3.102 reset ip pool import

8.3.42 dhcp server ip-range

Function

The **dhcp server ip-range** command sets the range of IP addresses that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server ip-range** command deletes the configured IP address range.

By default, the range of IP addresses that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server ip-range *start-ip-address end-ip-address*

undo dhcp server ip-range

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address.	The value is in decimal dotted notation.
end-ip-address	Specifies the end IP address.	The value is in decimal dotted notation.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Prerequisites

Usage Scenario

You can run the **dhcp server ip-range** *start-ip-address end-ip-address* command to change the range of IP addresses in an address pool based on actual usage of IP addresses.

Prerequisites

The DHCP server function of the interface address pool has been enabled on interfaces using the **dhcp select interface** command.

Example

Enable a DHCP server on a GE1/0/0 to pre-allocate IP addresses 192.168.1.2 to 192.168.1.100 to DHCP clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 192.168.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server ip-range 192.168.1.2 192.168.1.100
```

8.3.43 dhcp server lease

Function

The **dhcp server lease** command specifies the IP address lease for addresses in an interface address pool.

The **undo dhcp server lease** command restores the default IP address lease of addresses in an interface address pool.

By default, the IP address lease of addresses in an interface address pool is one day.

Format

dhcp server lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo dhcp server lease

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer that ranges from 0 to 999. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer that ranges from 0 to 23. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer that ranges from 0 to 59. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment.

DHCP clients require different IP address leases.

- If a host (such as the DNS server) needs to use a fixed IP address for a long time, run the **dhcp server lease unlimited** command to configure the IP address lease as unlimited.
- If a host (such as a portable computer) needs to use a temporary IP address, run the **dhcp server lease** command to specify an IP address lease. After the lease expires, the DHCP server withdraws the IP address and assigns the address to other clients.

When a DHCP client starts and 50% or 87.5% of its IP address lease has passed, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease.

- If the IP address can still be assigned to the client, the DHCP server informs the client of a renewed IP address lease.
- If the IP address can no longer be assigned to the client, the DHCP server informs the client that the IP address lease cannot be renewed.

You can run the **8.3.71 display ip pool** command to view information about the IP address lease. The values of the **lease** and **left** fields in the command output indicate the configured lease time and remaining lease time, respectively.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

Different IP address leases can be specified for different interface address pools on a DHCP server. All IP addresses in an interface address pool have the same lease.

If the IP address lease of an address pool is changed using this command, newly assigned IP addresses use the new IP address lease. IP addresses assigned before the change still use the original IP address lease before the lease is updated, and use the new lease after the lease is updated.

Example

Set the IP address lease of the address pool on GE1/0/0 to 2 days 2 hours and 30 minutes.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server lease day 2 hour 2 minute 30
```

Related Topics

8.3.26 dhcp select interface

8.3.87 lease

8.3.44 dhcp server logging

Function

The **dhcp server logging** command enables the logging function during IP address allocation of the DHCP server in the interface view.

The **undo dhcp server logging** command disables the logging function during IP address allocation of the DHCP server in the interface view.

By default, the logging function during IP address allocation of the DHCP server is disabled.

Format

dhcp server logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

undo dhcp server logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

Parameters

Parameter	Description	Value
allocation-fail	Displays logs when address allocation fails.	-
allocation-success	Displays logs when address allocation succeeds.	-
release	Displays logs when addresses are released.	-
renew-fail	Displays logs when address lease renewal fails.	-
renew-success	Displays logs when address lease renewal succeeds.	-
detect-conflict	Displays logs when address conflict occurs.	-
recycle-conflict	Displays logs when conflicting addresses are reclaimed.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When the DHCP server allocates IP addresses to clients, it records address allocation information to facilitate routine maintenance and fault location. After the logging function during IP address allocation of the DHCP server is configured using the **dhcp server logging** command, the DHCP server records logs about address allocation, conflict, lease renewal, and release.

Run the **display ip pool interface** *interface-pool-name* command to check the status of the logging function during IP allocation of the DHCP server.

Prerequisites

The DHCP server function of the interface address pool has been enabled on interfaces using the **dhcp select interface** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- With this logging function enabled, if a large number of DHCP clients request IP addresses from the DHCP server, the server frequently records logs. The server performance may therefore be affected.
- IP address allocation logs are recorded in the AM module. To view log information, the information center must be enabled. In addition, default settings for log output vary depending on various factors including the log level and output direction. For details, see Information Center Configuration.

  For example, the level of logs indicating that an IP address is successfully allocated, an IP address is successfully renewed, and an IP address is successfully released is informational, and these logs are not recorded in the log buffer by default. You can run the **info-center source AM channel 4 log level informational** command to change the level of the logs to be recorded in the log buffer. You can then run the **display logbuffer** command to check the preceding logs.

Example

Enable the logging function during IP address allocation of the DHCP server on the interface VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.1.1 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server logging
```

Related Topics

8.3.71 display ip pool

8.3.45 dhcp server mask

Function

The **dhcp server mask** command sets the subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients.

The **undo dhcp server mask** command deletes the configured subnet mask.

By default, the subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients is not configured.

Format

dhcp server mask { *mask* | *mask-length* }

undo dhcp server mask

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mask	Specifies a subnet mask.	The value is in decimal dotted notation.
mask-length	Specifies the length of the subnet.	The value is an integer ranging from 0 to 32.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the DHCP server function on an interface, you can configure the range and subnet mask of IP addresses that a DHCP server pre-allocates to DHCP clients. Run the **dhcp server ip-range** command to configure the IP address range and run the **dhcp server mask** command to configure the subnet mask of the IP addresses.

Prerequisites

The DHCP server function of the interface address pool has been enabled on interfaces using the **dhcp select interface** command.

Example

Set the subnet mask of IP addresses that a DHCP server on a GE1/0/0 pre-allocates to DHCP clients to 255.255.255.0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server mask 255.255.255.0
```

8.3.46 dhcp server nbns-list

Function

The **dhcp server nbns-list** command configures Network Basic Input Output System (NetBIOS) server addresses for an interface address pool.

The **undo dhcp server nbns-list** command deletes the NetBIOS server address from an interface address pool.

By default, no NetBIOS server address is configured for an interface address pool.

Format

dhcp server nbns-list *ip-address* &<1-8>

undo dhcp server nbns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the NetBIOS server address.	The value is in dotted decimal notation.
all	Deletes all NetBIOS server addresses.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before hosts communicate with each other, a NetBIOS server needs to resolve the accessed NetBIOS hostname to an IP address. To enable hosts to communicate with each other, run the **dhcp server nbns-list** command to configure NetBIOS server addresses for an interface address pool. When assigning IP addresses to clients, a DHCP server also assigns the configured NetBIOS server addresses to clients. To configure NetBIOS server addresses for a global address pool, run the **nbns-list** command.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

Each interface can be configured with a maximum of eight NetBIOS server addresses. The first assigned address functions as the primary address, and other addresses function as secondary addresses.

Example

Specify a NetBIOS server at 192.168.1.99 for domain name resolution when IP addresses in the interface address pool on GE1/0/0 are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcp enable
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server nbns-list 192.168.1.99
```

Related Topics

8.3.26 dhcp select interface

8.3.47 dhcp server netbios-type

8.3.90 nbns-list

8.3.91 netbios-type

8.3.47 dhcp server netbios-type

Function

The **dhcp server netbios-type** command specifies the NetBIOS node type for a DHCP client connecting to an interface.

The **undo dhcp server netbios-type** command deletes the specified NetBIOS node type of a DHCP client connecting to an interface.

By default, no NetBIOS node type is specified for a DHCP client connecting to an interface.

Format

dhcp server netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo dhcp server netbios-type

Parameters

Parameter	Description	Value
b-node	Indicates a node in broadcast mode. A b-node obtains the mapping in broadcast mode.	-
h-node	Indicates a node in hybrid mode. An h-node is a b-type node enabled with the end-to-end communication mechanism.	-
m-node	Indicates a node in mixed mode. An m-node is a p-type node with some broadcast features.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
p-node	Indicates a node in peer-to-peer mode. This node obtains mappings by communicating with the NetBIOS server.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When DHCP clients use NetBIOS on the WAN to communicate, their host names and IP addresses need to be mapped. You can run the **dhcp server netbios-type** command to configure the NetBIOS node type for an interface address pool. When assigning an IP address to the client, the DHCP server also sends the specified NetBIOS node type to the client.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

To specify the NetBIOS node type for a client in the global address pool, run the **netbios-type** command.

Example

Set the NetBIOS node type for a client in the address pool on GE1/0/0 to **p-node**.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server netbios-type p-node
```

Related Topics

8.3.26 dhcp select interface

8.3.46 dhcp server nbns-list

8.3.90 nbns-list

8.3.91 netbios-type

8.3.48 dhcp server next-server

Function

The **dhcp server next-server** command specifies a server IP address for DHCP clients.

The **undo dhcp server next-server** command cancels the configuration.

By default, no server IP address is specified by the DHCP Server for DHCP clients.

Format

dhcp server next-server *ip-address*

undo dhcp server next-server

Parameters

Parameter	Description	Value
ip-address	Specifies a server IP address.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server next-server** command is used on DHCP servers. When assigning a DHCP client an IP address, a DHCP server can also assign the DHCP client an IP address of the server that provides network services for the client. For example, some clients like IP phones still need other configuration parameters after automatically obtaining IP addresses. You can run the **dhcp server next-server** command to specify the server address used after a client obtains an IP address. The client then requests the configuration parameters from the specified server after obtaining an IP address.

If users use addresses in the interface address pool, run the **dhcp server next-server** command to specify the DHCP server IP address. If users use addresses in the global address pool, run the **next-server** command to specify the DHCP server IP address.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

- The address of an interface address pool has been configured using the **ip address** command.
- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- The **dhcp server next-server** command takes effect for only users that use addresses in the interface address pool.
- If you run the **dhcp server next-server** command multiple times, only the latest configuration takes effect.

Example

Specify the server IP address 192.168.1.2 in the interface address pool on VLANIF100 used to provide services for terminal users.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.1.1.2 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server next-server 192.168.1.2
```

Related Topics

8.3.93 next-server

8.3.49 dhcp server option

Function

The **dhcp server option** command sets user-defined option for an interface address pool.

The **undo dhcp server option** command deletes user-defined option from an interface address pool.

By default, no user-defined option is configured in an interface address pool.

Format

dhcp server option *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }

undo dhcp server option [*code* [**sub-option** *sub-code*]]

Parameters

Parameter	Description	Value
code	Specifies the code for a user-defined option.	The value is an integer that ranges from 1 to 254, except values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 120, 121 and 184. **NOTE** ● The format of option82, Option121 and Option184 are different from the other codes of a customized option. ● There are well-known options and customized options. For details about well-known options, see RFC 2132.
sub-option *sub-code*	Specifies the code of a user-defined sub-option.	The value is an integer that ranges from 1 to 254. For details about well-known options, see RFC 2132.
ascii *ascii-string*	Specifies the user-defined option code as an ASCII character string.	The value is a string of 1 to 255 characters when **sub-option** is not specified, or a string of 1 to 253 characters when **sub-option** is specified.
hex *hex-string*	Specifies the user-defined option code as a hexadecimal string.	The value is a hexadecimal string with an even number of digits, for example, hh or hhhh. If **sub-option** is not specified, the even number is in the range of 2 to 254. If **sub-option** is specified, the even number is in the range of 2 to 252. The value can be a combination of digits (0-9) and letters (A-F and a-f).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-string*	Specifies the user-defined option code as a ciphertext character string.	The value is a string, you can enter a character string in explicit text or cipher text. ● The character string in explicit text is a string of 1 to 64 characters. ● The character string in cipher text is a string of 48 to 108 characters. No matter whether the character string is entered in explicit or cipher text, the character string is displayed in cipher text in the configuration file and in explicit text in packets.
ip-address *ip-address*	Specifies the user-defined option code as an IP address.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. The Option field in a DHCP packet carries control information and parameters, including basic information such as the DNS service, NetBIOS service, and IP address lease. If a DHCP server is configured with option, when a DHCP client applies for an IP address from an interface address pool, the client can obtain configurations in the Option field of the DHCP response packet from the DHCP server without having to configure the DNS service, NetBIOS service, or IP address lease separately.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.

- The DHCP server function has been enabled on the interface using the **dhcp select interface** command.

Precautions

- When the password is contained in option, the **ascii** or **hex** type is insecure. Set the option type to **cipher**. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, number, and special characters. In addition, the password must consist of six or more than six characters.
- The **dhcp server option** command configures basic functions, such as the NetBIOS service and IP address lease. The system also provides commands to configure these functions separately. These commands take precedence over the **dhcp server option** command.
- To set user-defined option for a global address pool, run the **option** command.

Example

Set Option64 to 0x11 (a hexadecimal number) for the interface address pool on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server option 64 hex 11
```

Related Topics

8.3.26 dhcp select interface

8.3.94 option

8.3.50 dhcp server option121

Function

The **dhcp server option121** command configures a classless static route allocated by a DHCP server to a client.

The **undo dhcp server option121** command deletes a classless static route allocated by a DHCP server to a client.

By default, the classless static route allocated to a client is not configured.

Format

dhcp server option121 ip-address { *ip-address mask-length gateway-address* } &<1-8>

undo dhcp server option121 [**ip-address** *ip-address mask-length gateway-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
gateway-address	Specifies the gateway address of a route.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server option121 ip-address** command applies to only the DHCP server. The **dhcp server option121 ip-address** command configures Option 121 that defines a classless static route allocated to a client from an interface address pool.

mask-length and *gateway-address* specify a classless static route. The **dhcp server option121 ip-address** command configures a maximum of eight classless static routes.

Precautions

- To configure multiple classless static routes, run the **dhcp server option121 ip-address** command repeatedly.
- The **undo dhcp server option121** command will delete all classless static routes. To delete one classless static route, run the **undo dhcp server option121 ip-address** *ip-address mask-length gateway-address* command.

Example

Configure a classless static route allocated by a DHCP server to a client in the interface address pool on VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.1.1.2 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server option121 ip-address 10.10.10.10 24 192.168.11.11
```

Related Topics

8.3.83 ip pool (system view)

8.3.49 dhcp server option

8.3.51 dhcp server option184

Function

The **dhcp server option184** command configures Option 184 allocated by a DHCP server to a client.

The **undo dhcp server option184** command deletes Option 184 allocated by a DHCP server to a client.

By default, Option 184 allocated by a DHCP server to a client is not configured.

Format

dhcp server option184 { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* }

undo dhcp server option184 [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

NOTE

AR109, AR109W, AR109GW-L, AR129CGVW-L do not support **voice-vlan** *vlan-id* parameter.

Parameters

Parameter	Description	Value
ncp-ip *ip-address*	Specifies the IP address of the network call processor (NCP).	The value is in dotted decimal notation.
as-ip *ip-address*	Specifies the IP address of the backup NCP.	The value is in dotted decimal notation.
fail-over *ip-address*	Specifies the IP address in the failover route.	The value is in dotted decimal notation.
dialer-string	Specifies the dialer string.	The value is a string of 1 to 64 characters.
voice-vlan *vlan-id*	Specifies the ID of a voice VLAN.	The value is an integer that ranges from 1 to 4094.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **dhcp server option184** command applies to only the DHCP server and configures Option 184 allocated by a DHCP server to a client in an interface address pool.

Example

Configure Option 184 allocated by a DHCP server to a client in the interface address pool on VLANIF100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 10.1.1.2 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] dhcp server option184 as-ip 10.10.10.10
```

Related Topics

8.3.83 ip pool (system view)

8.3.49 dhcp server option

8.3.52 dhcp server ping

Function

The **dhcp server ping** command sets the maximum number of ping packets to be sent and the maximum response time of a ping packet.

The **undo dhcp server ping** command restores the default setting.

By default, the DHCP server sends 2 ping packets and the maximum response time is 500 ms.

Format

dhcp server ping { **packet** *number* | **timeout** *milliseconds* } *

undo dhcp server ping { **packet** | **timeout** }

Parameters

Parameter	Description	Value
packet *number*	Specifies the maximum number of ping packets to be sent.	The value is an integer ranging from 0 to 10. The value 0 indicates that no ping operation is performed.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
timeout *milliseconds*	Specifies the maximum response time of a ping packet.	The value is an integer that ranges from 0 to 10000, in milliseconds. The value 0 indicates that no ping operation is performed.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Repetitive IP address assignment will cause IP address conflicts. To solve this problem, before assigning an IP address to a client, the DHCP server needs to send ping packets using the **dhcp server ping** command to check whether the IP address is in use. Address detection checks whether the DHCP server receives any response within a certain period of time. If there is no response within a certain period of time, the DHCP server continues to send ping packets to this address until the number of ping packets reaches the maximum value. If there is still no response, it indicates that the IP address is not in use. This ensures that the IP address assigned to the client is unique.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Set the maximum number of ping packets to 3 and the maximum response time to 400 ms.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server ping packet 3
[Huawei] dhcp server ping timeout 400
```

Related Topics

8.3.18 dhcp enable

8.3.53 dhcp server sip-server

Function

The **dhcp server sip-server** command configures the SIP server IP address assigned to a DHCP client on an interface address pool.

The **undo dhcp server sip-server** command deletes the configured SIP server IP address assigned to a DHCP client on an interface address pool.

By default, the SIP server IP address assigned to a DHCP client on an interface address pool is not configured.

Format

dhcp server sip-server { **ip-address** *ip-address* &<1-2> | **list** *domain-name* &<1-2> }

undo dhcp server sip-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IP address for the SIP server.	The value is in dotted decimal notation.
list *domain-name*	Specifies the domain name of the SIP server.	The value is a string of 1 to 63 characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP server. To enable DHCP clients to normally access the Internet, the DHCP server needs to specify the SIP server IP address in the interface address pool when assigning IP addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured in each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- Before specifying the IP address or name for a SIP server, ensure that the SIP server exists.
- If you run this command repeatedly, the latest configuration overrides the previous ones.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify 10.1.1.1 as the IP address of the SIP server when addresses in the interface VLANIF100 address pool are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server sip-server ip-address 10.1.1.1
```

8.3.54 dhcp server sname

Function

The **dhcp server sname** command configures the name of the server where the DHCP client obtains the startup configuration file.

The **undo dhcp server sname** command deletes the configured name of the server where the DHCP client obtains the startup configuration file.

By default, the name of the server where the DHCP client obtains the startup configuration file is not configured.

Format

dhcp server sname *sname*

undo dhcp server sname

Parameters

Parameter	Description	Value
sname	Specifies the name of the server where the DHCP client obtains the startup configuration file.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for

the DHCP clients. After the name of the server where the DHCP client obtains the startup configuration file is configured using the **dhcp server sname** command, the DHCP client obtains the startup configuration file from this server.

Prerequisites

1. The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.
2. The DHCP server has been enabled on the interface using the **8.3.26 dhcp select interface** command.
3. The startup configuration file name has been configured for the DHCP client using the **8.3.29 dhcp server bootfile**.

Follow-up Procedures

Ensure that the route between the DHCP client and the file server where the DHCP client obtains the startup configuration file is reachable.

Example

Configure the name of the server where the DHCP client obtains the startup configuration file as **Huawei** in the interface address pool on GE1/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 255.255.255.0
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server bootfile start.ini
[Huawei-GigabitEthernet1/0/0] dhcp server sname Huawei
```

Related Topics

8.3.18 dhcp enable

8.3.26 dhcp select interface

8.3.29 dhcp server bootfile

8.3.55 dhcp server static-bind

Function

The **dhcp server static-bind** command binds an IP address in an interface address pool to a MAC address.

The **undo dhcp server static-bind** command unbinds the IP address in an interface address pool from a MAC address.

By default, an IP address in an interface address pool is not bound to any MAC address.

Format

dhcp server static-bind ip-address *ip-address* **mac-address** *mac-address* [**description** *description*]

undo dhcp server static-bind [**ip-address** *ip-address* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address to be bound. The IP address must be valid in an interface address pool.	The value is in dotted decimal notation.
mac-address *mac-address*	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
description *description*	Specifies the user description.	The value is a string of 1 to 256 case-sensitive characters. It can contain spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp server static-bind** command applies to DHCP servers. When planning a network, you need to allocate fixed IP addresses to some important hosts to ensure reliability. In this case, you can bind IP addresses in the address pool to the MAC addresses of these hosts. After the preceding configuration is complete, if the host of the MAC address to which the IP address is bound request an IP address from the DHCP server, the DHCP server finds the bound IP address based on the host's MAC address and allocates this IP address to the host, ensuring that the IP address obtained by the host is fixed.

You can run the **dhcp server static-bind** command to bind an IP address in an interface address pool to a MAC address.

You can run the **static-bind** command to bind an IP address in a global address pool to a MAC address.

Prerequisites

- The address of an interface address pool has been configured using the **ip address** command.
- Enable the DHCP server function based on the interface address pool on the interface using the **dhcp select interface** command.

Precautions

- Ensure that the bound IP address is not configured as the IP address that cannot be allocated using the **8.3.36 dhcp server excluded-ip-address** command and is not allocated by the DHCP server.
- You can run the **display ip pool** command to view the used IP addresses in the current address pool and select an available IP address to be bound to the MAC address. To bind used IP addresses to MAC addresses, run the **reset ip pool** command to reclaim used IP addresses first. IP addresses that are used can also be statically bound to MAC addresses or unbound from MAC addresses. When an IP address is statically bound to a MAC address, ensure that the MAC address to be bound is the same as the MAC address of the user who actually uses the IP address.
- The DHCP server preferentially allocates the IP address that has been statically bound to the client's MAC address.
- After an IP address is bound to a MAC address, the IP address does not expire; the binding between the IP and MAC addresses cannot be deleted when the IP address is in use. After an IP address is bound to a MAC address, the IP address does not expire. After an automatically allocated IP address is statically bound to a MAC address, the lease time of the IP address becomes unlimited. After the static binding between the IP address and the MAC address is deleted, the lease time of the IP address becomes the same as that configured in the address pool.

Example

Configure a DHCP server to assign a fixed IP address 10.10.10.20 in the interface address pool on gigabitethernet 1/0/0 to a host with the MAC address 2020-e2f3-2a3b.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.10.10.10 24
[Huawei-GigabitEthernet1/0/0] dhcp select interface
[Huawei-GigabitEthernet1/0/0] dhcp server static-bind ip-address 10.10.10.20 mac-address 2020-e2f3-2a3b
```

8.3.56 dhcp server trust option82

Function

The **dhcp server trust option82** command enables Option 82 on the DHCP server.

The **undo dhcp server trust option82** command disables Option 82 on the DHCP server.

By default, the DHCP server trusts Option 82.

Format

dhcp server trust option82

undo dhcp server trust option82

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP server to enable the Option 82 function. After receiving a DHCP packet that carries the Option 82 field but the giaddr is 0, the DHCP server processes the packet by default. Using the **undo dhcp server trust option82** command, the DHCP server discards the packet.

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Example

Enable Option 82 of the DHCP server.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp server trust option82
```

8.3.57 dhcp set ttl

Function

The **dhcp set ttl** command sets the TTL value for DHCP Discover messages after they are forwarded by the DHCP relay agent at Layer 3.

The **undo dhcp set ttl** command restores the default setting.

By default, the TTL value of DHCP Discovery messages decreases by 1 after they are forwarded by the DHCP relay agent at Layer 3.

Format

dhcp set ttl { **unvaried** | *ttl-value* }

undo dhcp set ttl

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
unvaried	Indicates that the TTL value of DHCP Discovery messages remains unchanged after the messages are forwarded by the DHCP relay agent at Layer 3. That is, the device does not reduce the TTL value by 1.	-
ttl-value	Specifies a fixed TTL value for DHCP Discovery messages after they are forwarded by the DHCP relay agent at Layer 3.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp set ttl** command is used on DHCP relay agents. When a DHCP relay agent forwards DHCP Discovery messages at Layer 3, it reduces the TTL value of the messages by 1 by default. Assume that the TTL value of a DHCP Discovery message received by the DHCP relay agent is 1. If the DHCP relay agent reduces the TTL value by 1, the TTL value changes to 0. The next-hop routing device will discard the message as its TTL value is 0. As a result, the DHCP server cannot receive the DHCP Discovery message forwarded by the DHCP relay agent. To ensure that the DHCP server can receive the DHCP Discovery message sent from the client, run the **dhcp set ttl** command to set the TTL value of the DHCP Discovery message to a non-zero value after the message is forwarded at Layer 3.

NOTE

If the DHCP relay agent connects to a special client whose TTL value of DHCP Discovery messages is 1, and if there are routing devices between the DHCP relay agent and DHCP server, run the **dhcp set ttl** *ttl-value* command to specify a fixed TTL value (16 is recommended) for DHCP Discovery messages after they are forwarded by the DHCP relay agent at Layer 3.

Prerequisites

The DHCP function has been enabled globally using the **dhcp enable** command.

Example

Set the TTL value of DHCP Discovery messages to 16 after the messages are forwarded by the DHCP relay agent at Layer 3.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp set ttl 16
```

8.3.58 dhcp speed-limit auto

Function

The **dhcp speed-limit auto** command enables dynamic rate limiting on DHCP packets.

The **undo dhcp speed-limit auto** command disables dynamic rate limiting on DHCP packets.

By default, dynamic rate limiting is disabled on DHCP packets.

Format

dhcp speed-limit auto

undo dhcp speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security or facilitate management, users may require that the DHCP packet processing rate should be limited. If the rate is not limited, CPU and memory resources can be used up due to malicious attacks.

Table 8-21 and Table 8-22 list the mapping between the DHCP packet rate and CPU/memory usage after dynamic rate limiting on DHCP packets is enabled.

Table 8-21 DHCP packet rate and CPU usage

CPU Usage (%)	DHCP Packet Rate (packets/second)
(70–85)	100
[85–100)	50
100	10

Table 8-22 DHCP packet rate and memory usage

Memory Usage (%)	DHCP Packet Rate (packets/second)
(65–75)	100
[75–85)	50
[85–100)	10

Prerequisites

DHCP has been enabled globally by using the **dhcp enable** command.

Precautions

- When the CPU usage is higher than 70% or the memory usage is higher than 65%, the DHCP packet processing rate is limited.
- The DHCP packet processing rate is the same as the smaller rate among the rates corresponding to the CPU or memory usage. For example, when the CPU usage is 80% and the memory usage is 80%, the DHCP packet rate is 50.

Example

Enable dynamic rate limiting on DHCP packets.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp speed-limit auto
```

8.3.59 dhcp-server

Function

The **dhcp-server** command adds DHCP servers to a DHCP server group.

The **undo dhcp-server** command deletes DHCP servers from a DHCP server group.

By default, no DHCP server is configured in a DHCP server group.

Format

dhcp-server *ip-address* [*ip-address-index*]

undo dhcp-server { *ip-address* | *ip-address-index* }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DHCP server.	The value is in dotted decimal notation.

Parameter	Description	Value
ip-address-index	When you specify the IP address for a DHCP server, you can specify *ip-address-index* for the IP address. If you do not specify the server index, the system assigns an idle index to the server.	The value is an integer that ranges from 0 to 7.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp-server** command applies to DHCP relay agents. To ensure that the DHCP relay agent can forward messages to multiple DHCP servers, configure multiple DHCP servers in a DHCP server group.

Precautions

- Each DHCP server group can be configured with a maximum of eight DHCP servers. You can delete a DHCP server by specifying *ip-address-index*.
- If a VPN instance is bound to an interface of the router, the DHCP server group must be bound to this VPN instance.

Example

Add the DHCP server at 10.10.78.56 to a DHCP server group **dhcp-srv1**.

```
<Huawei> system-view
[Huawei] dhcp server group dhcp-srv1
[Huawei-dhcp-server-group-dhcp-srv1] dhcp-server 10.10.78.56
```

Related Topics

8.3.40 dhcp server group
8.3.68 display dhcp server group
8.3.23 dhcp relay server-select

8.3.60 display dhcp client

Function

The **display dhcp client** command displays DHCP/BOOTP client lease information.

Format

display dhcp client [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCP/BOOTP client lease information on a specified interface: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device functions as the DHCP/BOOTP client, this command displays DHCP/BOOTP client lease information.

Example

Display DHCP client lease information.

```
<Huawei> display dhcp client
DHCP client lease information on interface GigabitEthernet0/0/1 :
 Current machine state          : Bound
 Internet address assigned via : DHCP
 Physical address               : 0819-a6cd-a896
 IP address                     : 192.168.1.254
 Subnet mask                    : 255.255.255.0
 Gateway ip address             : 192.168.1.2
 DHCP server                    : 192.168.1.2
 Lease obtained at              : 2013-06-26 07:40:22
 Lease expires at               : 2013-06-27 07:40:22
 Lease renews at                : 2013-06-26 19:40:22
 Lease rebinds at               : 2013-06-27 04:40:22
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-23 Description of the **display dhcp client** command output

Item	Description
DHCP client lease information on interface *if1*	DHCP client lease information on the interface *if1*.
Current machine state	Current device status.
Internet address assigned via	IP address obtained using DHCP or BOOTP.
Physical address	Device MAC address.
IP address	Device IP address.
Subnet mask	Mask of the device IP address.
Gateway ip address	Gateway address of the DHCP or BOOTP server.
DHCP server	DHCP server address (no value for a BOOTP client).
Lease obtained at	Time the lease is obtained.
Lease expires at	Time the lease expires (no value for a BOOTP client).
Lease renews at	Time the lease needs to be renewed (no value for a BOOTP client). The lease of an IP address needs to be renewed when half of the lease expires.
Lease rebinds at	Time the lease is renewed (no value for a BOOTP client). The lease of an IP address is renewed when 87.5% of the lease expires.

8.3.61 display dhcp client statistics

Function

The **display dhcp client statistics** command displays message statistics on a DHCP/BOOTP client.

Format

display dhcp client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays message statistics on a specified interface: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device functions as the DHCP client, the **display dhcp client statistics** command displays message statistics.

Example

Display message statistics on a DHCP/BOOTP client.

```
<Huawei> display dhcp client statistics
DHCP message statistics on interface Ethernet2/0/0 :
Input: total 0 packets
  Bootp reply            :          0
  Offer                  :          0
  Ack                    :          0
  Nak                    :          0
Output: total 0 packets
  Bootp request          :          0
  Discover               :          0
  Request                :          0
    Request of init-reboot:          0
    Request of selecting  :          0
    Request of renewing   :          0
    Request of rebinding  :          0
  Decline                :          0
  Release                :          0
```

Table 8-24 Description of the **display dhcp client statistics** command output

Item	Description
Input	Total number of DHCP messages received by the client.

Item	Description
Bootp reply	Number of BOOTP replies received by the client from the server.
Offer	Number of Offer messages received by the client from the server.
Ack	Number of ACK messages received by the client from the server.
Nak	Number of NAK messages received by the client from the server.
Output	Total number of messages forwarded by the client.
Bootp request	Number of BOOTP requests received by the server from the client.
Discover	Number of Discover messages received by the server from the client.
Request	Number of Request messages received by the server from the client.
Request of init-reboot	Number of Request of init-reboot messages received by the server from the client.
Request of selecting	Number of Request of selecting messages received by the server from the client.
Request of renewing	Number of Request of renewing messages received by the server from the client.
Request of rebinding	Number of Request of rebinding messages received by the server from the client.
Decline	Number of Decline messages received by the server from the client.
Release	Number of Release messages received by the server from the client.

8.3.62 display dhcp server configuration

Function

The **display dhcp server configuration** command displays configurations about a DHCP server.

 Copyright © Huawei Technologies Co., Ltd.

Format

display dhcp server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the Router functions as a DHCP server, you can run the **display dhcp server configuration** command to display configurations about the DHCP server.

Example

Display configurations about a DHCP server.

```
<Huawei> display dhcp server configuration
  DHCP server global running information :
  DHCP server bootp                : Disable (default)
  DHCP server bootp automatic      : Disable (default)
  DHCP server ping packet          : 2       (default)
  DHCP server ping timeout         : 500     (default)
  DHCP server trust option82       : Enable  (default)
  DHCP server force response       : Disable (default)

  DHCP server running information for interface Vlanif10 :
  DHCP server mode                 : Interface

  DHCP server running information for interface
Vlanif20 :
  DHCP server mode                 : Global
```

Table 8-25 Description of the **display dhcp server configuration** command output

Item	Description
DHCP server global running information	Global configurations about the DHCP server.
DHCP server bootp	Whether the DHCP server is enabled to respond to BOOTP requests. To configure this item, run the **8.3.30 dhcp server bootp** command.

Item	Description
DHCP server bootp automatic	Whether the DHCP server is enabled to dynamically allocate IP addresses to BOOTP clients. To configure this item, run the **8.3.31 dhcp server bootp automatic** command.
DHCP server ping packet	Maximum number of ping packets sent by the DHCP server. To configure this item, run the **8.3.52 dhcp server ping** command.
DHCP server ping timeout	Maximum response time of a ping packet sent by the DHCP server. To configure this item, run the **8.3.52 dhcp server ping** command.
DHCP server trust option82	Whether the DHCP server is enabled to trust the Option82 field. To configure this item, run the **8.3.56 dhcp server trust option82** command.
DHCP server force response	Whether the DHCP server is enabled to reply with DHCP NAK messages. To configure this item, run the **8.3.39 dhcp server force response** command.
DHCP server running information for interface *ifn*	Configurations about the DHCP server on an interface.
DHCP server mode	DHCP server mode. The value can be: • Interface: DHCP server based on an interface address pool. To configure this item, run the **8.3.26 dhcp select interface** command. • Global: DHCP server based on the global address pool. To configure this item, run the **8.3.25 dhcp select global** command.

8.3.63 display dhcp configuration

Function

The **display dhcp configuration** command displays configuration information about the DHCP public module.

Format

display dhcp configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to query configuration information about the DHCP public module.

Example

Display configuration information about the DHCP public module.

```
<Huawei> display dhcp configuration
  DHCP global running information :
  DHCP                                  : Enable
  DHCP speed limit                          : Disable  (default)
```

Table 8-26 Description of the **display dhcp configuration** command output

Item	Description
DHCP global running information	Configuration information about the DHCP public module in the system view.
DHCP	Indicates whether DHCP is enabled. The value can be: ● Enable: DHCP is enabled. ● Disable (default): DHCP is disabled. By default, DHCP is disabled. You can configure this parameter using the **8.3.18 dhcp enable** command.

Item	Description
DHCP speed limit	Indicates whether dynamic DHCP message rate limiting is enabled. The value can be: ● Enable: Dynamic DHCP message rate limiting is enabled. ● Disable (default): Dynamic DHCP message rate limiting is disabled. By default, dynamic DHCP message rate limiting is disabled. You can configure this parameter using the **8.3.58 dhcp speed-limit auto** command.

8.3.64 display dhcp option template

Function

The **display dhcp option template** command displays the configuration of a DHCP Option template.

Format

display dhcp option template [**name** *template-name*]

Parameters

Parameter	Description	Value
name *template-name*	Displays the configuration of a specified DHCP Option template.	The template must be an existing DHCP Option template.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a DHCP Option template, you can run the **display dhcp option template** command to view the configuration of the DHCP Option template,

 Copyright © Huawei Technologies Co., Ltd.

including the template name, number, IP address of a server configured for the client after the client automatically obtains the IP address, domain name, and values of customized options.

Example

Display the configuration of the DHCP Option template named **test**.

```
<Huawei> display dhcp option template name test
 ---------------------------------------------------------------------------
  Template-Name  : test
  Template-No    : 1
  Next-server    : 192.168.1.5
  Domain-name    : huawei.com
  DNS-server0    : 192.168.2.7
  DNS-server1    : 192.168.2.8
  NBNS-server0   : 192.168.1.7
  NBNS-server1   : 192.168.1.8
  Netbios-type   : b-node
  Gateway-0      : 192.168.1.10
```

Display the configurations of all DHCP Option templates.

```
<Huawei> display dhcp option template
 ---------------------------------------------------------------------------
  Template-Name  : template1
  Template-No    : 0
  Next-server    : 10.1.1.4
  Domain-name    : -
  DNS-server0    : -
  NBNS-server0   : -
  Netbios-type   : -
  Gateway-0      : -

 ---------------------------------------------------------------------------
  Template-Name  : template2
  Template-No    : 1
  Next-server    : 192.168.1.5
  Domain-name    : huawei.com
  Option-code      : 64
    Option-subcode : 3
      Option-type  : hex
      Option-value : 11
  DNS-server0    : 192.168.2.7
  DNS-server1    : 192.168.2.8
  NBNS-server0   : 192.168.2.7
  NBNS-server1   : 192.168.2.8
  Netbios-type   : b-node
  Gateway-0      : 192.168.1.10
```

Table 8-27 Description of the **display dhcp option template** command output

Item	Description
Template-Name	Name of the DHCP Option template. To specify the parameter, run the **8.3.20 dhcp option template** command.
Template-No	Index value of the DHCP Option template.

Item	Description
Next-server	IP address of a server configured for the client after the client automatically obtains the IP address. To specify the parameter, run the **8.3.93 next-server** command in the DHCP Option template view.
Domain-name	Name of a domain. To specify the parameter, run the **8.3.76 domain-name** command in the DHCP Option template view.
Option-code	Code for a customized option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
Option-subcode	Code for a customized sub-option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
Option-type	Character string type for a customized option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
Option-value	Character string value for a customized option. To specify the parameter, run the **8.3.94 option** command in the DHCP Option template view.
DNS-server0	Address of the DNS server. Currently, a maximum of eight DNS server addresses can be configured. Values 0 and 1 indicate the first and second DNS server addresses respectively. To specify the parameter, run the **8.3.75 dns-list** command in the DHCP Option template view.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
NBNS-server0	Address of the NetBIOS server. Currently, a maximum of eight NetBIOS server addresses can be configured in a DHCP Option template. Values 0 and 1 indicate the first and second NetBIOS server addresses respectively. To specify the parameter, run the **8.3.90 nbns-list** command in the DHCP Option template view.
Netbios-type	NetBIOS node type. To specify the parameter, run the **8.3.91 netbios-type** command in the DHCP Option template view.
Gateway-0	Gateway address. Currently, a maximum of eight gateway addresses can be configured. The value 0 indicates the first gateway address. To specify the parameter, run the **8.3.80 gateway-list** command in the DHCP Option template view.

Related Topics

8.3.20 dhcp option template

8.3.65 display dhcp relay

Function

The **display dhcp relay** command displays configuration information about a DHCP relay agent.

Format

display dhcp relay { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays configuration information about DHCP relay agents configured on all interfaces.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Displays configuration information about a DHCP relay agent configured on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check configuration information about DHCP relay agents configured on interfaces.

Example

Display configuration information about DHCP relay agents on all interfaces.

```
<Huawei> display dhcp relay all
 DHCP relay agent running information of interface Vlanif5 :
 Server group name      : group1
 Gateway address in use : 10.100.100.1

 DHCP relay agent running information of interface Vlanif100 :
 Server IP address [00] : 10.2.2.3
 Gateway address in use : 10.2.2.2
```

Table 8-28 Description of the **display dhcp relay all** command output

Item	Description
DHCP relay agent running information of interface *if*	DHCP relay agent configuration of the *if* interface.
Server group name	Group name of the DHCP Server. To specify the parameter, run the **8.3.23 dhcp relay server-select** command.

Item	Description
Server IP address [x]	IP address of a DHCP server in the DHCP server group. The value x is the index of a DHCP server. To specify the parameter, run the **8.3.59 dhcp-server** command.
Gateway address in use	IP address of the DHCP gateway. To specify the parameter, run the **8.3.79 gateway (DHCP server group view)** command.

8.3.66 display dhcp relay statistics

Function

The **display dhcp relay statistics** command displays message statistics on a DHCP relay agent.

Format

display dhcp relay statistics [**server-group** *group-name*]

Parameters

Parameter	Description	Value
server-group *group-name*	Displays message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. If this parameter is not specified, message statistics on DHCP relay agents connected to all DHCP servers are displayed.	The value must be an existing DHCP server group on the device.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Run the **display dhcp relay statistics** command to check whether the client is correctly configured or the network is connected.

- Run the **display dhcp relay statistics server-group** *group-name* command to check message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. The DHCP server group name needs to be specified.
- Run the **display dhcp relay statistics** command to check message statistics on all DHCP relay agents besides DHCP relay agents connected to DHCP servers in the DHCP server group.

Follow-up Procedure

After detecting incorrect message statistics on a DHCP relay agent, run the **reset dhcp relay statistics** [**server-group** *group-name*] command to clear message statistics on the DHCP relay agent.

Example

Display message statistics on a DHCP relay agent.

```
<Huawei> display dhcp relay statistics
 The statistics of DHCP RELAY:
   DHCP packets received from clients        : 0
       DHCP DISCOVER packets received        : 0
       DHCP REQUEST packets received         : 0
       DHCP RELEASE packets received         : 0
       DHCP INFORM packets received          : 0
       DHCP DECLINE packets received         : 0
   DHCP packets sent to clients              : 0
       Unicast packets sent to clients       : 0
       Broadcast packets sent to clients     : 0
   DHCP packets received from servers        : 0
       DHCP OFFER packets received           : 0
       DHCP ACK packets received             : 0
       DHCP NAK packets received             : 0
   DHCP packets sent to servers              : 0
   DHCP Bad packets received                 : 0
```

Table 8-29 Description of the **display dhcp relay statistics** command output

Item	Description
DHCP packets received from clients	DHCP messages received from clients.
DHCP DISCOVER packets received	DHCP Discover messages received from clients.
DHCP REQUEST packets received	DHCP Request messages received from clients.
DHCP RELEASE packets received	DHCP Release messages received from clients.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCP INFORM packets received	DHCP Inform messages received from clients.
DHCP DECLINE packets received	DHCP Decline messages received from clients.
DHCP packets sent to clients	DHCP messages sent to clients.
Unicast packets sent to clients	Unicast packets sent to clients.
Broadcast packets sent to clients	Broadcast packets sent to clients.
DHCP packets received from servers	DHCP messages received from servers.
DHCP OFFER packets received	DHCP Offer messages received from servers.
DHCP ACK packets received	DHCP ACK messages received from servers.
DHCP NAK packets received	DHCP NAK messages received from servers.
DHCP packets sent to servers	DHCP messages sent to servers.
DHCP Bad packets received	DHCP error messages received.

Related Topics

8.3.98 reset dhcp relay statistics
8.3.69 display dhcp server statistics

8.3.67 display dhcp server database

Function

The **display dhcp server database** command displays information about the DHCP database.

Format

display dhcp server database

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display dhcp server database** command displays the storage path and file name of DHCP data on a DHCP server. This information helps to check:

- Whether the function that saves DHCP data to the storage device is enabled. If this function is not enabled, run the **dhcp server database** command to enable it.
- Whether the interval at which DHCP data is saved is proper.
- Whether the function that recovers DHCP data from the storage device after the system restarts is enabled.

Precautions

The function that saves DHCP data to storage devices and the function that recovers DHCP data from storage devices can be enabled in any sequence.

Example

Display information about the DHCP database.

```
<Huawei> display dhcp server database
 Status: disable
 Recover from files after reboot: disable
 File saving lease items: flash:/dhcp/lease.txt
 File saving conflict items: flash:/dhcp/conflict.txt
 Save Interval: 300 (seconds)
```

Table 8-30 Description of the **display dhcp server database** command output

Item	Description
Status	Whether to save the data to the storage device: ● disable ● enable The value is set using the **dhcp server database** command.
Recover from files after reboot	Whether to recover data from the file on the storage device after the system restarts: ● disable ● enable The value is set using the **dhcp server database** command.
File saving lease items	File name and path of the file for storing address lease information.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
File saving conflict items	File name and path of the file for storing address conflict information.
Save Interval	Interval at which DHCP data is saved, in seconds. The value is set using the **dhcp server database** command.

8.3.68 display dhcp server group

Function

The **display dhcp server group** command displays the configuration of a DHCP server group.

Format

display dhcp server group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified DHCP server group.	The value must be an existing DHCP server group on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. The **display dhcp server group** command displays information about all the DHCP server groups of a DHCP relay agent and the number of DHCP servers in the DHCP server groups. If *group-name* is specified, the **display dhcp server group** *group-name* command displays DHCP server addresses and the number of DHCP servers in a specified DHCP server group.

Prerequisites

A DHCP server group has been created on a DHCP relay agent using the **dhcp server group** command.

Example

Display the configuration of the DHCP server group **myServers**.

```
<Huawei> display dhcp server group myServers
 Group-name          : myServers
   (0)  Server-IP    : 10.1.1.1
   Gateway           : 10.10.10.1
   VPN instance      : --
```

Table 8-31 Description of the **display dhcp server group** command output

Item	Description
Group-name	Name of a DHCP server group. To specify the parameter, run the **8.3.40 dhcp server group** command.
Gateway	Gateway address of the DHCP server in the DHCP server group. To specify the parameter, run the **8.3.79 gateway (DHCP server group view)** command.
VPN instance	VPN instance to which the DHCP server group belongs. To specify the parameter, run the **8.3.109 vpn-instance (DHCP server group view)** command.

8.3.69 display dhcp server statistics

Function

The **display dhcp server statistics** command displays statistics on a DHCP server.

Format

display dhcp server statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the display dhcp server statistics command to check whether the client is correctly configured or the network is connected.

Follow-up Procedure

After detecting incorrect message statistics on a DHCP server, run the **reset dhcp server statistics** command to clear message statistics on the DHCP server.

Example

Display statistics on the DHCP server.

```
<Huawei> display dhcp server statistics
 DHCP Server Statistics:

 Client Request:          6
  Dhcp Discover:           1
  Dhcp Request:            4
  Dhcp Decline:            0
  Dhcp Release:            1
  Dhcp Inform:             0
 Server Reply:             4
  Dhcp Offer:              1
  Dhcp Ack:                3
  Dhcp Nak:                0
 Bad Messages:             0
```

Table 8-32 Description of the **display dhcp server statistics** command output

Item	Description
DHCP Server Statistics	Statistics on the DHCP server.
Client Request	Number of DHCP messages sent from the DHCP client to the DHCP server.
Dhcp Discover, Dhcp Request, Dhcp Decline, Dhcp Release, Dhcp Inform	Numbers of different types of DHCP messages sent from the DHCP client to the DHCP server.
Server Reply	Number of DHCP messages sent from the DHCP server to the DHCP client.
Dhcp Offer, Dhcp Ack, Dhcp Nak	Numbers of different types of DHCP messages sent from the DHCP server to the DHCP client.
Bad Messages	Number of unknown messages.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.99 reset dhcp server statistics

8.3.70 display dhcp statistics

Function

The **display dhcp statistics** command displays DHCP message statistics.

Format

display dhcp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcp statistics** command displays statistics about sent and received DHCP messages.

Example

Display DHCP message statistics.

```
<Huawei> display dhcp statistics
Input: total 172 packets, discarded 0 packets
  Bootp request          :        0,  Bootp reply          :        0
  Discover               :        0,  Offer                :      172
  Request                :        0,  Ack                  :        0
  Release                :        0,  Nak                  :        0
  Decline                :        0,  Inform               :        0

  Rx buffers full        :     2978,  L2fdb lookup failed  :       38

Output: total 172 packets, discarded 0 packets
```

Table 8-33 Description of the **display dhcp statistics** command output

Item	Description
Bootp request	Number of BOOTP requests sent by the device that functions as the client.
Bootp reply	Number of BOOTP replies received by the client from the server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Discover	Number of Discover messages received by the server from the client.
Offer	Number of Offer messages received by the client from the server.
Request	Number of BOOTP requests received by the server from the client.
Ack	Number of ACK messages received by the client from the server.
Release	Number of Release messages received by the server from the client.
Nak	Number of NAK messages received by the client from the server.
Decline	Number of Decline messages sent by the client.
Inform	Number of Inform messages sent by the client.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rx buffers full or L2fdb lookup failed	Information displayed when the DHCP service is abnormal. The displayed information includes: ● Rx buffers full: Total number of DHCP packets discarded because the remaining queue length is shorter than the reserved threshold. ● L2fdb lookup failed: Total number of DHCP packets discarded because entries fail to be queried. ● High cpu occupancy: Total number of DHCP packets discarded because the CPU usage is excessively high. ● Port blocked: Total number of DHCP packets discarded because the inbound interface is blocked. ● Bad vlan id: Total number of DHCP packets discarded because the VLAN ID is incorrect. ● Memory exhausted: Total number of DHCP packets discarded because the memory is exhausted. ● L3if protocol down: Total number of DHCP packets discarded because the Layer 3 protocol of the source interface goes Down. ● Rate limit: Total number of DHCP packets discarded because rates of the packets exceed the limit. ● Bad packet length: Total number of DHCP packets discarded because the packet length is incorrect. ● Bad ip header length: Total number of DHCP packets discarded because the IP header length is incorrect. ● Bad ip header checksum: Total number of DHCP packets discarded because the checksum of the IP header is incorrect. ● Bad udp checksum: Total number of DHCP packets discarded because the checksum of the UDP header is incorrect. ● Hops exceeded: Total number of DHCP packets discarded because the number of next hops is incorrect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Bad magic cookie: Total number of DHCP packets discarded because the magic-cookie field is incorrect. • Duplicate option: Total number of DHCP packets discarded because the option fields are duplicate. • Bad option length: Total number of DHCP packets discarded because the option field length is incorrect. • End option absent: Total number of DHCP packets discarded because of the incorrect end option. • Dest-port equals source: Total number of DHCP packets discarded because the source interface is also the outbound interface. • Bad chaddr: Total number of DHCP packets discarded because the MAC address of the client is incorrect. • Bad giaddr: Total number of DHCP packets discarded because the relay gateway is incorrect. • Bad request: Total number of DHCP packets discarded because the request packets are incorrect. • Bad reply: Total number of DHCP packets discarded because the response packets are incorrect. • Bad dest udp-port: Total number of DHCP packets discarded because the destination interface is incorrect. • Bad message type: Total number of DHCP packets discarded because of incorrect destination interfaces. • L2fdb lookup failed: Total number of incoming DHCP packets discarded because entries fail to be queried. • Max-user limit: Total number of DHCP packets discarded because the maximum number of users is exceeded. • Add bindtable failed: Total number of DHCP packets discarded because dynamic binding entries are added.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Client transferred: Total number of DHCP packets discarded due to interface flapping. • Bad original interface: Total number of DHCP packets discarded because dynamic binding entries are added. • Bad client-id: Total number of DHCP packets discarded because the client ID is incorrect. • Bad server-id: Total number of DHCP packets discarded because the server ID is incorrect. • Bad dest-ip: Total number of DHCP packets discarded because the destination IP address is incorrect. • Other error: Total number of DHCP packets discarded due to other reasons.

8.3.71 display ip pool

Function

The **display ip pool** command displays the configurations of an address pool.

Format

display ip pool

display ip pool interface *interface-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used**]

display ip pool name *ip-pool-name* [*start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used** [**user-type** { **dhcp** | **pppoe** | **l2tp** | **ipsec** | **ssl-vpn** | **ppp** }]]

display ip pool vpn-instance *vpn-instance-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-pool-name*	Displays the configuration of the specified interface address pool. **NOTE** An interface address pool is specified using the type and number of an interface without spaces between them.	The interface address pool must exist on the device.
name *ip-pool-name*	Displays the configuration of the specified global address pool.	The global address pool must exist on the device.
start-ip-address [*end-ip-address*]	Displays the IP addresses within the range specified by the start IP address in the address pool. If *end-ip-address* is set, the end IP address is also specified.	The value is in dotted decimal notation.
all	Displays all IP addresses in the address pool.	-
conflict	Displays the conflicting IP addresses in the address pool. (If an IP address that the DHCP server prepares to allocate to a user exists on the network, the IP address will be added to the conflict list. This problem occurs when a static IP address is configured or an active/standby switchover occurs in a VRRP group if the range of IP addresses in the address pools on the master and backup devices overlap.)	-
expired	Displays the expired and idle IP addresses in the address pool.	-
used [**user-type** { **dhcp** | **pppoe** | **l2tp** | **ipsec** | **ssl-vpn** | **ppp** }]	Display the IP addresses used in the address pool by the specific type of users. ● Select **dhcp**, to specify the users who obtain IP addresses by DHCP. ● Select **pppoe**, to specify the users who obtain IP addresses by PPPoE dial-up. ● Select **l2tp**, to specify the L2TP users. ● Select **ipsec**, to specify the IPSec users. ● Select **ssl-vpn**, to specify the SSL VPN users. ● Select **ppp**, to specify the PPP users.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the address pool in a specified VPN instance.	The value must be an existing VPN instance on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip pool** command to view information about a configured address pool and IP addresses in the address pool, including the address pool name, lease, lock status, and status of IP addresses in the address pool.

Example

Display information about conflicting IP addresses in the address pool **huawei**.

```
<Huawei> display ip pool name huawei conflict
  Pool-name        : huawei
  Pool-No          : 1
  Lease            : 1 Days 0 Hours 0 Minutes
  Domain-name      : -
  Option-code      : 60
    Option-subcode : --
    Option-type    : cipher
    Option-value   : %^%#5g)NPN1M,$M;pQ-lT\P>Al6QN4#ldIVVjD69XlCN%^%#
  DNS-server0      : -
  NBNS-server0     : -
  Netbios-type     : -
  Position         : Local
  Status           : Unlocked
  Gateway-0        : -
  Network          : 192.168.0.0
  Mask             : 255.255.255.0
  VPN instance     : --
  Bootfile         : 43534
  Logging          : Enable
  Conflicted address recycle interval: 1 Days 0 Hours 0 Minutes
  Address Statistic: Total       :254       Used        :1
                     Idle        :252       Expired     :2
                     Conflict    :1         Disabled    :0

 -----------------------------------------------------------------------------
  Network section
        Start           End       Total    Used Idle(Expired) Conflict Disabled
 -----------------------------------------------------------------------------
     192.168.0.1   192.168.0.254     254       1        252(2)       1     0
 -----------------------------------------------------------------------------
 Client-ID format as follows:
   DHCP  : mac-address                PPPoE   : mac-address
   IPSec : user-id/portnumber/vrf     PPP     : interface index
   L2TP  : cpu-slot/session-id        SSL-VPN : user-id/session-id
```

```
-----------------------------------------------------------------------------
Index          IP          Client-ID   Type     Left   Status
-----------------------------------------------------------------------------
  109   192.168.0.110                -      -        -   Conflict
-----------------------------------------------------------------------------
```

Table 8-34 Description of the **display ip pool** command output

Item	Description
Pool-name	Name of an IP address pool. To configure the IP address pool name, run the **ip pool (system view)** command.
Pool-No	Index of the IP address pool.
Lease	Lease of the IP address pool. To configure the lease of the IP address pool, run the **lease** command.
Domain-name	Name of a domain. To configure the domain name, run the **domain-name** command.
Option-code	Value of a customized option. To configure the value, run the **option** command.
Option-subcode	Value of a customized sub-option. To configure the value, run the **option** command.
Option-type	Type of a customized option code: ● ascii: indicates that the customized option code is an ASCII character string. ● hex: indicates that the customized option code is a hexadecimal string. ● cipher: indicates that the customized option code is a ciphertext character string. To configure the type, run the **option** command.
Option-value	Content of a customized option. To configure the content, run the **option** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DNS-server0	Address of the DNS server. Currently, an IP address pool can be configured with up to eight DNS servers. The value 0 indicates the first DNS server address and the value 1 indicates the second DNS server address. To configure the DNS server address, run the **dns-list** command.
NBNS-server0	Address of the NetBIOS server. Currently, an address pool can be configured with up to eight NetBIOS server addresses. The value 0 indicates the first NetBIOS server address. To configure the NetBIOS server address, run the **nbns-list** command.
Netbios-type	NetBIOS type. To configure the NetBIOS type, run the **netbios-type** command.
Position	Location of the IP address pool.
Status (First)	Status of the address pool. To configure the address pool status, run the **lock (IP address pool view)** command.
Gateway-0	Gateway address. Currently, a maximum of eight gateway addresses can be configured in an IP address pool. The value 0 indicates the first gateway address. To configure the gateway address, run the **gateway-list** command.
Network	Network segment of the address pool.
Mask	Subnet mask of the address pool. To configure the subnet mask of the address pool, run the **network (IP address pool view)** command.
Bootfile	Name of the startup configuration file configured for the DHCP client. To configure the name, run the **bootfile** command.
VPN instance	Name of a VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Logging	Status of the logging function when the DHCP server allocates IP addresses. ● Enable ● Disable To configure the status of the logging function, run the **logging** or **dhcp server logging** command.
Conflicted address recycle interval	The interval for the automatic reclaim of conflicting IP addresses in the address pool. To configure the status of the logging function, run the **conflict auto-recycle interval day** *day* [**hour** *hour* [**minute** *minute*]] command.
Address Statistic	Statistics about IP addresses in the address pool.
Start	Start IP address of the IP address pool.
End	End IP address of the IP address pool.
Total	Total number of IP addresses in the address pool. Total = Used + Idle(Expired) + Conflict + Disable
Used	Number of used IP addresses in the address pool.
Idle(Expired)	Number of idle(expired) IP addresses in the address pool.
Conflict	Number of conflicting IP addresses in the address pool.
Disabled	Number of disabled IP addresses in the address pool.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Client-ID format as follows	Client ID format: ● DHCP: mac-address. The client ID format of DHCP users is a MAC address. ● PPPoE: mac-address. The client ID format of PPPoE users is a MAC address. ● IPSec: user-id/portnumber/vrf. The client ID format of IPSec users is a user ID, port number, or VPN index. ● PPP: interface index. The client ID format of PPP users is an interface index. ● L2TP: cpu-slot/session-id. The client ID format of L2TP users is a CPU ID-slot ID or session ID. ● SSL-VPN: user-id/session-id. The client ID format of SSL-VPN users is a user ID or session ID.
Index	Index.
IP	IP address.
Client-ID	DHCP client ID.
Type	DHCP client type. The types include DHCP, PPPoE, IPSec, PPP, L2TP, and SSL-VPN.
Left	Remaining lease of an IP address. When the result of the calculation formula ([**Lease** - **Left**]/**Lease**) is 50% or 87.5%, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease. If the renewal succeeds, the value of the **Left** field is recounted. If the renewal fails, the DHCP client requests an IP address again and the status of its original IP address is set to **Expired**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status (Second)	Status of an IP address: ● Used: indicates that the IP address is used. ● Idle: indicates that the IP address is idle. ● Expired: indicates that the lease of the IP address expires and the IP address is idle. ● Conflict: indicates that the IP address conflicts with another IP address on the network. ● Disable: indicates that the IP address cannot be used. ● Static-bind: indicates that the IP address is bound to a MAC address. ● Static-bind used: indicates that the IP address is bound to a MAC address and used.

8.3.72 display ip pool import all

Function

The **display ip pool import all** commands displays DNS and NetBIOS configurations that a DHCP server automatically assigns to a DHCP client.

Format

display ip pool import all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **8.3.84 import all** command on the DHCP server to enable the DHCP server to automatically assign configurations of DNS server and NetBIOS server to

DHCP clients. The **display ip pool import all** command displays configurations of DNS server and NetBIOS server that the DHCP server automatically assigns to DHCP clients.

Example

Display DNS and NetBIOS configurations that the DHCP server automatically assigns to the DHCP client.

```
<Huawei> display ip pool import all
 ---------------------------------------------------------------------------
 Parameter      Update time          Protocol  Value
 ---------------------------------------------------------------------------
 domain-name     -                    -        -
 dns-server      -                    -        -
 nbns-server     -                    -        -
 ---------------------------------------------------------------------------
```

Table 8-35 Description of **display ip pool import all** command output

Item	Description
Parameter	Dynamically assigned information type: ● domain-name: domain name information ● dns-server: DNS server information ● nbns-server: NetBIOS server information To set the dynamically assigned information type, run the **8.3.84 import all** command.
Update time	Update time of dynamically assigned information.
Protocol	Protocol type of dynamically assigned information.
Value	Contents of dynamically assigned information.

Related Topics

8.3.84 import all

8.3.41 dhcp server import all

8.3.73 display snmp-agent trap feature-name dhcp all

Function

The **display snmp-agent trap feature-name dhcp all** command displays the status of all traps on the DHCP module.

Format

display snmp-agent trap feature-name dhcp all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the DHCP module, you can run this command to check the status of all traps on the DHCP module. To enable the trap function for the DHCP module, run the **snmp-agent trap enable feature-name dhcp** command.

Prerequisites

The SNMP function has been enabled on the device. For details, see **snmp-agent**.

Example

Display the status of all traps on the DHCP module.

```
<Huawei>display snmp-agent trap feature-name dhcp all
-------------------------------------------------------------------------------
Feature name: dhcp
Trap number : 15
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwNomatchSnpBindTblDhcpPktAlarm
                             off                     off
hwDhcpSnpChaddrAlarm         off                     off
hwDhcpV6PktPrefixAlarm       off                     on
hwUntrustedReplyPktAlarm     off                     off
hwDhcpPktRateAlarm           off                     on
hwSnpUserNumberAlarmIf       on                      off
hwSnpUserNumberAlarmIfResume on                      off
hwSnpUserNumberAlarmVlan     on                      off
hwSnpUserNumberAlarmVlanResume on
off
hwSnpUserNumberAlarmGlobal   on                      off
hwSnpUserNumberAlarmGlobalResume
                             on                      off
hwNdSnpUserNumberAlarmIf     on                      off
hwNdSnpUserNumberAlarmIfResume on
off
hwNdSnpUserNumberAlarmGlobal on                      off
hwNdSnpUserNumberAlarmGlobalResume

                             on                      off
```

Table 8-36 Description of the **display snmp-agent trap feature-name dhcp all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Name of a trap. Traps on the DHCP module include: ● hwNomatchSnpBindTblDhcpPktAlarm: The device sends a Huawei proprietary trap when the number of DHCP Request packets that do not match DHCP snooping binding entries and are discarded on an interface exceeds the threshold. ● hwDhcpSnpChaddrAlarm: The device sends a Huawei proprietary trap when the number of discarded DHCP packets whose CHADDR field differs from the source MAC address exceeds the threshold. ● hwDhcpV6PktPrefixAlarm: The device sends a Huawei proprietary trap message when the DHCPv6 prefix length exceeds the threshold. ● hwUntrustedReplyPktAlarm: The device sends a Huawei proprietary trap message when the number of DHCP Reply packets discarded on an untrusted interface exceeds the threshold. ● hwDhcpPktRateAlarm: The device sends a Huawei proprietary trap message when the number of discarded DHCP packets whose rate exceeds the limit exceeds the threshold. ● hwSnpUserNumberAlarmIf: The device sends a Huawei proprietary trap message when the number of DHCP access users on an interface exceeds the upper threshold. ● hwSnpUserNumberAlarmIfResume: The device sends a Huawei proprietary trap message when the number of DHCP access users on an interface falls below the lower threshold. ● hwSnpUserNumberAlarmVlan: The device sends a Huawei proprietary trap message when the number of DHCP access users in a VLAN exceeds the upper threshold. ● hwSnpUserNumberAlarmVlanResume: The device sends a Huawei proprietary trap message when the number of DHCP access users in a VLAN falls below the lower threshold. ● hwSnpUserNumberAlarmGlobal: The device sends a Huawei proprietary trap message when the number of DHCP access users on the device exceeds the upper threshold. ● hwSnpUserNumberAlarmGlobalResume: The device sends a Huawei proprietary trap message when the number of DHCP access users on the device falls below the lower threshold.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• hwNdSnpUserNumberAlarmIf: The device sends a Huawei proprietary trap message when the number of ND access users on an interface exceeds the upper threshold. • hwNdSnpUserNumberAlarmIfResume: The device sends a Huawei proprietary trap message when the number of ND access users on an interface falls below the lower threshold. • hwNdSnpUserNumberAlarmGlobal: The device sends a Huawei proprietary trap message when the number of ND access users on the device exceeds the upper threshold. • hwNdSnpUserNumberAlarmGlobalResume: The device sends a Huawei proprietary trap message when the number of ND access users on the device falls below the lower threshold.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.
Current switch status	Trap status: • on: The trap is enabled. • off: The trap is disabled.

Related Topics

8.3.106 snmp-agent trap enable feature-name dhcp

8.3.74 display snmp-agent trap feature-name mid_am all

Function

The **display snmp-agent trap feature-name mid_am all** command displays the status of all traps for the AM module.

Format

display snmp-agent trap feature-name mid_am all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the AM module, you can run this command to check the status of all traps for the AM module. You can run the **snmp-agent trap enable feature-name mib_am** command to enable the trap function for the AM module.

Prerequisites

SNMP has been enabled on the device. You can enable SNMP using the **snmp-agent** command.

Example

Display the status of all traps for the AM module.

```
<Huawei>display snmp-agent trap feature-name mid_am all
-----------------------------------------------------------------------------
Feature name: MID_AM
Trap number : 2
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwUsedIPReachThreshold          on                      on
hwUsedIPReachThresholdResume    on                      on
```

Table 8-37 Description of the **display snmp-agent trap feature-name mid_am all** command output

Item	Description
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Names of the traps related to the AM module, including: • hwUsedIPReachThreshold: When the number of used IP addresses in an IP address pool exceeds the upper trap threshold, the device sends a Huawei proprietary trap. • hwUsedIPReachThresholdResume: When the number of used IP addresses in an IP address pool falls below the lower trap threshold, the device sends a Huawei proprietary trap.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Status of the trap function: • on: The trap function is enabled. • off: The trap function is disabled.

Related Topics

8.3.107 snmp-agent trap enable feature-name mid_am

8.3.75 dns-list

Function

The **dns-list** command configures the DNS server address for the DHCP client.

The **undo dns-list** command deletes a configured DNS server address.

By default, no DNS server address is configured.

Format

IP address pool view

dns-list { *ip-address* &<1-8> | **unnumbered interface** *interface-type interface-number* }

undo dns-list { *ip-address* | **unnumbered interface** | **all** }

DHCP Option template view

dns-list *ip-address* &<1-8>

undo dns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the DNS server address.	The value is in dotted decimal notation. A maximum of eight DNS server addresses can be configured. These IP addresses are separated by spaces.
unnumbered interface *interface-type interface-number*	Borrows the DNS server address obtained by the interface as the DNS server IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Deletes all DNS server addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If user hosts access hosts on the network by domain names, user hosts need to send DNS requests to the DNS server and resolve the domain name to access for communication. To connect a DHCP client to the network, configure a DHCP server address so that the DHCP server can assign both the specified DNS server address and an IP address to the client. To configure DNS server addresses for an interface address pool, run the **dhcp server dns-list** command.

Precautions

In the IP address pool view and DHCP Option template view, a device can be configured with a maximum of eight DNS server addresses respectively. The address first assigned to the clients functions as the primary address, and the other seven addresses function as secondary addresses.

Example

In the IP address pool view, set the IP address of the DNS server to 10.10.10.10.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] dns-list 10.10.10.10
```

In the DHCP Option template view, set the IP address of the DNS server to 10.10.10.10.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] dns-list 10.10.10.10
```

Related Topics

8.3.83 ip pool (system view)
8.3.34 dhcp server dns-list

8.3.76 domain-name

Function

The **domain-name** command configures the domain name suffix for the DHCP client.

The **undo domain-name** command deletes a configured domain name suffix.

By default, no domain name suffix is configured.

Format

domain-name *domain-name*

undo domain-name

Parameters

Parameter	Description	Value
domain-name	Specifies a domain name to be assigned to a DHCP client.	The value is a string of 1 to 63 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

This command applies to DHCP servers. When allocating IP addresses to the client, the DHCP server also specifies domain names for clients. Run the **domain-name** command on the DHCP server to specify a domain name. When allocating IP addresses to clients, the DHCP server also sends the domain names to the clients.

To configure a domain name for an interface address pool, run the **dhcp server domain-name (interface view)** command.

Example

In the IP address pool view, configure the domain name suffix assigned to the DHCP client as **example.com**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip pool test
[Huawei-ip-pool-test] domain-name example.com
```

In the DHCP Option template, configure the domain name suffix assigned to the DHCP client as **huawei.com**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] domain-name huawei.com
```

Related Topics

8.3.83 ip pool (system view)

8.3.35 dhcp server domain-name (interface view)

8.3.77 excluded-ip-address

Function

The **excluded-ip-address** command specifies the range of IP addresses that cannot be automatically assigned to clients from the address pool.

The **undo excluded-ip-address** command deletes the specified range of IP addresses that cannot be automatically assigned to clients from the address pool.

By default, all IP addresses in the address pool can be automatically assigned to clients.

Format

excluded-ip-address *start-ip-address* [*end-ip-address*]

undo excluded-ip-address *start-ip-address* [*end-ip-address*]

Parameters

Parameter	Description	Value
start-ip-address	Specifies the start IP address that cannot be automatically assigned.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address that cannot be automatically assigned. If *end-ip-address* is not specified, only *start-ip-address* cannot be automatically assigned.	The value is in dotted decimal notation. *end-ip-address* and *start-ip-address* must be on the same network segment and *end-ip-address* must be larger than *start-ip-address*.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **excluded-ip-address** command applies to DHCP servers. Fixed IP addresses are allocated to some specific hosts (such as the WWW server) on the network for a long time. If these hosts' IP addresses are overlapped with IP addresses in the address pool and the DHCP server allocates these overlapped IP addresses to other hosts, IP address conflicts may occur. To prevent the IP address conflict, you need to exclude these IP addresses from being automatically allocated in the address pool.

You can run the **excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the global address pool.

You can run the **dhcp server excluded-ip-address** command to specify the IP addresses or the range of IP addresses that cannot be automatically assigned to clients in the interface address pool.

Prerequisites

Network segment addresses that can be assigned from the global address pool have been configured using the **network (address pool view)** command.

Precautions

- The excluded IP address or IP address segment must be in the local address pool.
- You do not need to exclude the gateway address configured using the **8.3.80 gateway-list** command from being automatically allocated. The device automatically adds the gateway address into the list of IP addresses that cannot be automatically allocated.

  You do not need to exclude the IP address of a server's interface connecting to a client from being automatically allocated. The device automatically sets the interface IP address to the Conflict status during address allocation.
- If you run the **excluded-ip-address** command multiple times, you can specify multiple IP addresses or IP address segments that cannot be automatically assigned to clients from the specified address pool.
- You can run the **display ip pool** command to check used IP addresses in the current address pool, and then specify unused IP addresses that cannot be automatically assigned. To exclude used IP addresses from being automatically assigned, run the **reset ip pool** command to reclaim used IP addresses first.

Example

Specify that IP addresses 10.10.10.10 to 10.10.10.20 cannot be automatically assigned to clients from the address pool **global1**.

```
<Huawei> system-view
[Huawei] ip pool global1
```

```
[Huawei-ip-pool-global1] network 10.10.10.0 mask 24
[Huawei-ip-pool-global1] excluded-ip-address 10.10.10.10 10.10.10.20
```

Related Topics

8.3.83 ip pool (system view)

8.3.92 network (IP address pool view)

8.3.36 dhcp server excluded-ip-address

8.3.78 force insert option

Function

The **force insert option** command configures a DHCP server to forcibly insert an Option field specified in the global address pool or DHCP Option template to a DHCP Response packet that it sends to a DHCP client.

The **undo force insert option** command deletes the Option field forcibly inserted to a DHCP Response packet that a DHCP server sends to a DHCP client.

By default, a DHCP server does not forcibly insert an Option field to a DHCP Response packet that it sends to a DHCP client.

Format

force insert option *code* &<1-254>

undo force insert option *code* &<1-254>

Parameters

Parameter	Description	Value
code	Specifies the code for a forcibly replied option. You can configure a DHCP server to forcibly reply one or more options.	The value is an integer that ranges from 1 to 254.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a DHCP client applies for an IP address from a DHCP server, parameters contained in the DHCP Request packet specify the options the client requires. The DHCP server inserts the required options to a DHCP Response packet.

Sometimes, the DHCP server on the existing network receives a DHCP Request packet that contains no parameter specifying the options the client requires. However, the client still wants to obtain the options configured on the global address pool. You can run the **force insert option** *code* &<1-254> command to configure the DHCP server to forcibly insert an Option field to the DHCP Response packet.

Prerequisites

The Option field has been configured in the global address pool by running the **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command in the global address pool view.

Example

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet in the address pool **pool1**.

```
<Huawei> system-view
[Huawei] ip pool pool1
[Huawei-ip-pool-pool1] option 4 hex 11 22
[Huawei-ip-pool-pool1] force insert option 4
```

Configure a DHCP server to forcibly insert Option 4 to a DHCP Response packet in the DHCP Option template **template1**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option 4 hex 11 22
[Huawei-dhcp-option-template-template1] force insert option 4
```

Related Topics

8.3.83 ip pool (system view)

8.3.94 option

8.3.20 dhcp option template

8.3.79 gateway (DHCP server group view)

Function

The **gateway** command specifies an egress gateway address of the DHCP server in the DHCP server group view.

The **undo gateway** command restores the default setting.

By default, no egress gateway address is specified.

Format

gateway *ip-address*

undo gateway

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an egress gateway.	The value is in dotted decimal notation.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. If a DHCP server and its DHCP relay agent are on different network segments, you can run the **gateway** command to specify an egress gateway address for the DHCP relay agent. In this way, the DHCP relay agent can communicate with the DHCP server. Run the **gateway-list** command to configure an egress gateway for the DHCP server.

Precautions

- If an egress gateway is not configured for a DHCP relay agent using the **gateway** command, the DHCP relay agent uses the interface address as the gateway address to communicate with the DHCP server.
- When two router devices function as the DHCP server and DHCP relay agent respectively, they must use the same egress gateway address.

Example

Specify the egress gateway address of the server group **myServers** as 10.10.10.1.

```
<Huawei> system-view
[Huawei] dhcp server group myServers
[Huawei-dhcp-server-group-myServers] gateway 10.10.10.1
```

8.3.80 gateway-list

Function

The **gateway-list** command configures the egress gateway address for the DHCP client.

The **undo gateway-list** command deletes a configured egress gateway address.

By default, no egress gateway address is configured.

Format

gateway-list *ip-address* &<1-8>

undo gateway-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies an egress gateway address.	The value is in dotted decimal notation.
all	Deletes all gateway addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. If a DHCP server and its client are on different network segments, you can run the **gateway-list** command to specify an egress gateway address. In this way, the DHCP server and client can communicate with each other. Then the DHCP server can assign both an IP address and the specified egress gateway address to the client. You can configure multiple gateways in a global address pool to load balance traffic and improve network reliability.

Run the **8.3.79 gateway (DHCP server group view)** command to configure an egress gateway for a DHCP relay agent.

Configuration Impact

If a gateway address is configured on the DHCP server, a DHCP client obtains the gateway address from the DHCP server and automatically generates a default route to the gateway address. If you run the **option121** command on the DHCP server to allocate classless static routes to DHCP clients, the DHCP client uses an allocated classless static route and does not automatically generate a default route to the gateway address.

Precautions

In the IP address pool view and DHCP Option template view, the Router can be configured with a maximum of eight egress gateway addresses respectively. These gateway addresses cannot be subnet broadcast addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the IP address pool view, set the egress gateway address for the DHCP client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] gateway-list 10.1.1.1
```

In the DHCP Option template, set the egress gateway address for the DHCP client to 10.1.1.1.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] gateway-list 10.1.1.1
```

Related Topics

8.3.83 ip pool (system view)

8.3.20 dhcp option template

8.3.81 ip address bootp-alloc

Function

The **ip address bootp-alloc** command enables the BOOTP client function on an interface.

The **undo ip address bootp-alloc** command disables the BOOTP client function from an interface.

By default, the BOOTP client function is disabled on an interface.

Format

ip address bootp-alloc [**unicast**]

undo ip address bootp-alloc

Parameters

None

Parameter	Description	Value
unicast	Indicates that the client requests the server to unicast response packets to the client.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCP is developed based on the BOOTP protocol. The device supports both DHCP and BOOTP and allows hosts to obtain IP addresses by BOOTP.

To enable an interface to obtain IP addresses using BOOTP, you can enable the BOOTP client function on the interface. A BOOTP client requests for an IP address from the server using BOOTP. The BOOTP client has two functions:

- Sends BOOTP Request messages to the server.
- Processes BOOTP Reply messages from the server.

To obtain an IP address, the BOOTP client sends a BOOTP Request message to the server. When the server receives the BOOTP Request message, it sends a BOOTP response message to the BOOTP client. The BOOTP client obtains the assigned IP address from the response message.

Precautions

Interfaces of the Router can have IP addresses statically configured using the **ip address** command or dynamically obtain IP addresses using the **ip address bootp-alloc** command. A static IP address takes precedence over a dynamic IP address. If the interface has dynamically obtained an IP address after the **ip address bootp-alloc** command is executed, running the **undo ip address** command deletes the IP address and the **ip address bootp-alloc** command. If the interface does not obtain an IP address after the **ip address bootp-alloc** command is executed, running the **undo ip address** command does not delete the **ip address bootp-alloc** command.

Example

Enable the BOOTP client function on GE1/0/0 to obtain an IP address.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address bootp-alloc
```

8.3.82 ip address dhcp-alloc

Function

The **ip address dhcp-alloc** command enables the DHCP client function on an interface.

The **undo ip address dhcp-alloc** command disables the DHCP client function on an interface.

By default, the DHCP client function is disabled on an interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip address dhcp-alloc [**unicast**]

undo ip address dhcp-alloc

Parameters

Parameter	Description	Value
unicast	Indicates that the client requests the server to unicast response packets.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable an interface of the Router to obtain IP addresses using DHCP, enable the DHCP client function on the interface. A BOOTP client applies for an IP address from the server using DHCP. The DHCP client has two functions:

- Sends DHCP Request messages to the server.
- Processes DHCP Reply messages from the server.

To obtain an IP address, the DHCP client sends a DHCP Request message to the server. After the server receives the DHCP Request message, it sends a DHCP response message to the DHCP client. The DHCP client obtains the assigned IP address from the response message.

Precautions

Interfaces of the device can have IP addresses statically configured using the **ip address** command or dynamically obtain IP addresses using the **ip address dhcp-alloc** command. A static IP address takes precedence over a dynamic IP address. If the interface has dynamically obtained an IP address after the **ip address dhcp-alloc** command is executed, running the **undo ip address** command deletes the IP address and the **ip address dhcp-alloc** command. If the interface does not obtain an IP address after the **ip address dhcp-alloc** command is executed, running the **undo ip address** command does not delete the **ip address dhcp-alloc** command.

Example

Enable the DHCP client function on GE1/0/0 to obtain an IP address.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address dhcp-alloc
```

8.3.83 ip pool (system view)

Function

The **ip pool** command creates a global address pool.

The **undo ip pool** command deletes a global address pool.

By default, no global address pool is created.

Format

ip pool *ip-pool-name*

undo ip pool *ip-pool-name*

Parameters

Parameter	Description	Value
ip-pool-name	Specifies the name for an IP address pool.	The value is a string of 1 to 64 characters without spaces. It can contain digits, letters, and special characters such as underscores (_), hyphens (-), and periods (.). It cannot be set to **-** or **--**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When configuring a DHCP server, run the **ip pool (system view)** command in the system view to create a global IP address pool and set parameters for the global IP address pool, including a gateway address, the IP address lease, and a VPN instance. Then the configured DHCP server can assign IP addresses in the IP address pool to clients.

Follow-up Procedure

Run the **8.3.92 network (IP address pool view)** command to specify the range of the IP addresses in the pool.

Example

Create a global address pool named **global1**.

```
<Huawei> system-view
[Huawei] ip pool global1
```

Related Topics

8.3.92 network (IP address pool view)

8.3.84 import all

Function

The **import all** command enables the device to dynamically obtain the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the global address pool.

The **undo import all** command disables the device from dynamically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the global address pool.

By default, the local is disabled from dynamically obtaining the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the global address pool.

Format

import all

undo import all

Parameters

None

Views

Global address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on the DHCP server. Run the **import all** command on the DHCP server to automatically allocate the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the carrier to the DHCP client.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The global address pool has been created using the **ip pool (system view)** command.

Precautions

The device functions as a DHCP client to obtain the DNS server IP address, DNS domain name suffix, and NetBIOS server IP address from the carrier, and then functions as the DHCP server to allocate obtained information to DHCP clients using this command. The device cannot allocate information obtained from the carrier using other methods to clients.

Example

Enable the device to dynamically obtain configurations of DNS server and NetBIOS server from global address pool **global**.

```
<Huawei> system-view
[Huawei] ip pool global
[Huawei-ip-pool-global] import all
```

Related Topics

8.3.72 display ip pool import all

8.3.102 reset ip pool import

8.3.85 ip relay address cycle

Function

The **ip relay address cycle** command enables the DHCP server polling function on a DHCP relay agent.

The **undo ip relay address cycle** command disables the DHCP server polling function on a DHCP relay agent.

By default, DHCP server polling is disabled on a DHCP relay agent.

Format

ip relay address cycle

undo ip relay address cycle

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. When multiple DHCP server addresses are configured on a DHCP relay agent, the DHCP relay agent forwards DHCP Discover messages to all servers by default. As a result, DHCP servers need to process a large number of messages, leading to heavy loads of servers. To solve this problem, configure the **ip relay address cycle** command. After this command is configured, the DHCP relay agent forwards a received DHCP Discover message to one DHCP server at a time, and forwards the DHCP Discover message to a different DHCP server each time it receives the message. Multiple DHCP servers then can allocate the same number of IP addresses, implementing load balancing among DHCP servers.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Example

Enable DHCP server polling on the router in the system view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ip relay address cycle
```

Related Topics

8.3.18 dhcp enable

8.3.86 ip route dhcp

Function

The **ip route dhcp** command configures a routing entry delivered by the DHCP server to a DHCP client.

The **undo ip route dhcp** command cancels the configuration.

By default, no routing entry is delivered by the DHCP server to a DHCP client.

Format

ip route *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*]

undo ip route *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length. The 32-bit mask is represented by consecutive 1s, and the mask in dotted decimal notation can be replaced by the mask length.	The value is an integer that ranges from 0 to 32.
interface-type interface-number	Specifies the type and number of the interface that forwards packets.	-
dhcp	Indicates that the DHCP client obtains routing entries using DHCP.	-
preference-value	Specifies the priority of the routing protocol.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **ip route dhcp** command is used on DHCP clients. After the **ip route** *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [*preference-value*] command is run, a route with the gateway address as the next-hop IP address is automatically generated when a DHCP client obtains an IP address from the DHCP server through a DHCP request.

Example

Configure a routing entry to be obtained in DHCP mode on the DHCP client, and specify GE1/0/0 as the outbound interface for forwarding packets and 30 as the routing protocol priority.

```
<Huawei> system-view
[Huawei] ip route 10.1.1.1 24 gigabitethernet 1/0/0 dhcp 30
```

8.3.87 lease

Function

The **lease** command sets the lease for IP addresses in a global IP address pool.

The **undo lease** command restores the default lease of IP addresses in a global IP address pool.

By default, the lease of IP addresses is one day.

Format

lease { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo lease

Parameters

Parameter	Description	Value
day *day*	Specifies the number of days in the IP address lease.	The value is an integer that ranges from 0 to 999. The default value is 1.
hour *hour*	Specifies the number of hours in the IP address lease.	The value is an integer that ranges from 0 to 23. The default value is 0.
minute *minute*	Specifies the number of minutes in the IP address lease.	The value is an integer that ranges from 0 to 59. The default value is 0.
unlimited	Indicates that the IP address lease is unlimited.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To meet different client requirements, DHCP supports dynamic, automatic, and static address assignment.

Different hosts require different IP address leases. For example, if some hosts such as a DNS server need to use certain IP addresses for a long time, run the **lease**

command to set the IP address lease of the current global address pool to **unlimited**. If some hosts such as a portable computer just need to use temporary IP addresses, run the **lease** command to set the IP address lease of the current global address pool to the required time so that the expired IP addresses can be released and assigned to other clients.

When a DHCP client starts and 50% or 87.5% of its IP address lease has passed, the DHCP client sends a DHCP Request message to the DHCP server to renew the lease.

- If the IP address can be assigned to the client, the DHCP server informs the client that the IP address lease can be renewed.
- If the IP address can no longer be assigned to the client, the DHCP server informs the client that the IP address lease cannot be renewed. The client needs to request for another IP address.

You can run the **8.3.71 display ip pool** command to view information about the IP address lease. The values of the **lease** and **left** fields in the command output indicate the configured lease time and remaining lease time, respectively.

Prerequisites

A global IP address pool has been created using the **8.3.83 ip pool (system view)** command and the DHCP server function is enabled using the **dhcp enable** command.

Precautions

Different IP address leases can be specified for different global address pools on a DHCP server. In a global address pool, all addresses have the same lease.

To specify the IP address lease for an interface address pool, run the **dhcp server lease** command.

If the IP address lease of an address pool is changed using this command, newly assigned IP addresses use the new IP address lease. IP addresses assigned before the change still use the original IP address lease before the lease is updated, and use the new lease after the lease is updated.

Example

Set the lease of a global address pool **global1** to 2 days 2 hours and 30 minutes.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] lease day 2 hour 2 minute 30
```

Related Topics

8.3.83 ip pool (system view)

8.3.88 lock (IP address pool view)

Function

The **lock** command locks an IP address pool.

The **undo lock** restores the default configuration.

By default, no IP address pool is locked.

Format

lock [**track nqa** *admin-name test-name*]

undo lock

Parameters

Parameter	Description	Value
track nqa *admin-name test-name*	Specifies the NQA test instance to be associated with the IP address pool. ● *admin-name*: specifies the name of the administrator for the NQA test instance. ● *test-name*: specifies the name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without any space.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **lock** command is run, the specified IP address pool is locked and IP addresses in this address pool cannot be assigned to clients. When a DHCP server needs to be redeployed, you need to migrate address pools on the DHCP server to another DHCP server on the live network. To retain the addresses that have been assigned to clients from a global address pool, run the **lock** command to lock the global address pool. When new users get online after the address pool migration, they apply for IP addresses from a new address pool.

After **track nqa** *admin-name test-name* is specified, the device can function as the backup DHCP server, and its IP address pool is associated with NQA test instances to check the DHCP server status (including the link and DHCP server function). This improves network reliability. When the DHCP server is working properly, the IP address pool is locked, and users obtain IP addresses through the DHCP server. When NQA detects that the DHCP server is faulty, the IP address pool is unlocked and assigns IP addresses to newly online users. When NQA detects that the DHCP

server fault is rectified, the IP address pool is locked again, and newly online users obtain IP addresses through the DHCP server.

An IP address pool can be associated with NQA test instances of the DHCP and ICMP types. According to the test mechanism, NQA test instances of the DHCP type are used to test whether the DHCP server function is normal; those of the ICMP type are used to test whether routes to the DHCP server are reachable. You can select one NQA test instance type based on the site requirements.

Prerequisites

Before specifying the NQA test instance to be associated with the IP address pool using **track nqa** *admin-name test-name*, perform the following operations and start the NQA test instance.

- Configuring and starting an NQA test instance of the DHCP type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type dhcp** command to configure the test type to DHCP.
  d. Run the **source-interface** *interface-type interface-number* command to specify the source interface for sending DHCP packets.
  e. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  f. Run the **start** command to start the NQA test instance.

     An NQA test instance can be started immediately, at a specified time, or after a specified delay.

     - Run the **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance immediately.
     - Run the **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance at a specified time.
     - Run the **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance after a specified delay.
- Configuring and starting an NQA test instance of the ICMP type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type icmp** command to configure the test type to ICMP.
  d. Run the **destination-address ipv4** *ipv4-address* command to configure the destination IP address.
  e. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  f. Run the **start** command to start the NQA test instance.

An NQA test instance can be started immediately, at a specified time, or after a specified delay.

- Run the **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance immediately.
- Run the **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance at a specified time.
- Run the **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance after a specified delay.

Precautions

An IP address pool can be associated to only one NQA test instance. If you run the **lock** [**track nqa** *admin-name test-name*] command multiple times, the last configuration takes effect.

When the NQA test instance type is not DHCP and ICMP, the association between the IP address pool and NQA do not take effect. In this case, the IP address pool is locked.

Example

Lock the IP address pool **global1**.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] lock
```

Configure an NQA test instance of the DHCP type and check whether the IP address pool **global1** is locked according to the NQA detection result.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type dhcp
[Huawei-nqa-admin-test] source-interface gigabitethernet 1/0/0
[Huawei-nqa-admin-test] start now
[Huawei-nqa-admin-test] quit
[Huawei] ip pool global1
[Huawei-ip-pool-global1] lock track nqa admin test
```

Related Topics

8.3.83 ip pool (system view)

8.3.89 logging (IP address pool view)

Function

The **logging** command enables the logging function during IP address allocation of the DHCP server in the IP address pool view.

The **undo logging** command disables the logging function during IP address allocation of the DHCP server in the IP address pool view.

By default, the logging function during IP address allocation of the DHCP server is disabled.

Format

logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

undo logging [**allocation-fail** | **allocation-success** | **release** | **renew-fail** | **renew-success** | **detect-conflict** | **recycle-conflict**] *

Parameters

Parameter	Description	Value
allocation-fail	Displays logs when address allocation fails.	-
allocation-success	Displays logs when address allocation succeeds.	-
release	Displays logs when addresses are released.	-
renew-fail	Displays logs when address lease renewal fails.	-
renew-success	Displays logs when address lease renewal succeeds.	-
detect-conflict	Displays logs when address conflict occurs.	-
recycle-conflict	Displays logs when conflicting addresses are reclaimed.	-

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a DHCP server. When the DHCP server allocates IP addresses to clients, it records address allocation information to facilitate routine maintenance and fault location. After the logging function during IP address allocation of the DHCP server is configured using the **logging** command, the DHCP server records logs about address allocation, conflict, lease renewal, and release.

Run the **display ip pool name** *ip-pool-name* command to check the status of the logging function during IP address allocation of the DHCP server.

Prerequisites

The global address pool has been created using the **ip pool (system view)** command.

Precautions

- With this logging function enabled, if a large number of DHCP clients request IP addresses from the DHCP server, the server frequently records logs. The server performance may therefore be affected.
- IP address allocation logs are recorded in the AM module. To view log information, the information center must be enabled. In addition, default settings for log output vary depending on various factors including the log level and output direction. For details, see Information Center Configuration.

  For example, the level of logs indicating that an IP address is successfully allocated, an IP address is successfully renewed, and an IP address is successfully released is informational, and these logs are not recorded in the log buffer by default. You can run the **info-center source AM channel 4 log level informational** command to change the level of the logs to be recorded in the log buffer. You can then run the **display logbuffer** command to check the preceding logs.

Example

Enable the logging function during IP address allocation of the DHCP server in the IP address pool **pool1**.

```
<Huawei> system-view
[Huawei] ip pool pool1
[Huawei-ip-pool-pool1] logging
```

8.3.90 nbns-list

Function

The **nbns-list** command configures the NetBIOS server address for the DHCP client.

The **undo nbns-list** command deletes a configured NetBIOS server address.

By default, no NetBIOS server address is configured.

Format

nbns-list *ip-address* &<1-8>

undo nbns-list { *ip-address* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a NetBIOS server.	The value is in dotted decimal notation. A maximum of eight NetBIOS server addresses can be configured. These IP addresses are separated by spaces.

Parameter	Description	Value
all	Deletes all NetBIOS server addresses.	-

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before hosts communicate with each other, a NetBIOS server needs to resolve the accessedNetBIOS hostname to an IP address. To enable hosts to communicate with each other, run the **nbns-list** command to configure NetBIOS server addresses. When assigning IP addresses to clients, a DHCP server also assigns the configured NetBIOS server addresses to clients. To configure NetBIOS server addresses for an interface address pool, run the **dhcp server nbns-list** command.

Precautions

In the IP address pool view and DHCP Option template view, a device can be configured with a maximum of eight NetBIOS server addresses respectively. The first assigned address functions as the primary address, and the other seven addresses function as secondary addresses.

Example

In the IP address pool view, set the IP address of the NetBIOS server to 192.168.1.1.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] nbns-list 192.168.1.1
```

In the DHCP Option template view, set the IP address of the NetBIOS server to 10.1.1.1.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] nbns-list 10.1.1.1
```

Related Topics

8.3.83 ip pool (system view)
8.3.46 dhcp server nbns-list
8.3.20 dhcp option template

8.3.91 netbios-type

Function

The **netbios-type** command configures the NetBIOS node type for the DHCP client.

The **undo netbios-type** command deletes a configured NetBIOS node type.

By default, no NetBIOS node type for the DHCP client is configured.

Format

netbios-type { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

Parameters

Parameter	Description	Value
b-node	Indicates a node in broadcast mode. A b-node obtains the mapping between host names and IP addresses in broadcast mode.	-
h-node	Indicates a node in hybrid mode. An h-node is a b-type node enabled with the end-to-end communication mechanism.	-
m-node	Indicates a node in mixed mode. An m-node is a p-type node with some broadcast features.	-
p-node	Indicates a node in peer-to-peer mode. A p-node obtains the mapping between host names and IP addresses by communicating with a NetBIOS server.	-

Views

IP address pool view, DHCP Option template view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. When a DHCP client uses NetBIOS for communication, its host name needs to be mapped to an IP address, and the NetBIOS node type needs to be specified for it using the **netbios-type** command. When a DHCP server assigns an IP address to clients, it also sends the specified NetBIOS node type to clients.

Prerequisites

To specify the NetBIOS node type for a client in the interface address pool, run the **dhcp server netbios-type** command.

Example

In the IP address pool view, set the NetBIOS node type for the DHCP client to **b-node**.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] netbios-type b-node
```

In the DHCP Option template view, set the NetBIOS node type for the DHCP client to **b-node**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] netbios-type b-node
```

Related Topics

8.3.83 ip pool (system view)

8.3.90 nbns-list

8.3.47 dhcp server netbios-type

8.3.92 network (IP address pool view)

Function

The **network** command sets a network segment address for a global address pool.

The **undo network** command restores the default network segment address.

By default, no network segment address is specified.

Format

network *ip-address* [**mask** { *mask* | *mask-length* }]

undo network

Parameters

Parameter	Description	Value
ip-address	Specifies a network segment address.	The value is in dotted decimal notation.
mask	Specifies the mask of the network segment address. If this parameter is not specified, the natural mask is used.	-
mask	Specifies the mask of the network segment address.	The value is in dotted decimal notation.
mask-length	Specifies the network mask length of the DHCP server.	The value is an integer that ranges from 0 to 32.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Before a DHCP server assigns IP addresses to clients from a global address pool, run the **network** command to set a network segment address for the global address pool so that the DHCP server can select and assign IP addresses on this network segment to clients. When a DHCP server assigns an IP address to the client from the interface address pool, the network segment of the interface IP address is that of the interface address pool.

Precautions

Each IP address pool can be configured with only one network segment. If the system needs multiple address segments, multiple IP address pools are required.

The size of an address pool can be controlled by setting the mask length. The mask length is in reverse proportion to the address pool size.

When configuring an address pool, ensure that IP addresses on the network address segment must be class A, B, or C IP addresses, and the mask cannot be set to 0, 1, 31, or 32.

The size of the IP address pool cannot be larger than 64K.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the network segment address of the IP address pool **global1** to 192.168.1.0 and mask length to 24.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] network 192.168.1.0 mask 24
```

Related Topics

8.3.83 ip pool (system view)

8.3.93 next-server

Function

The **next-server** command configures the IP address of a server for the DHCP client after the client automatically obtains the IP address.

The **undo next-server** command deletes a configured IP address of a server for the DHCP client after the client automatically obtains the IP address.

By default, no IP address of a server is configured for the DHCP client after the client automatically obtains the IP address.

Format

next-server *ip-address*

undo next-server

Parameters

Parameter	Description	Value
ip-address	Specifies a server IP address.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **next-server** command is used on DHCP servers. When assigning a client an IP address, a DHCP server can also assign the client an IP address of the server that provides network services for the client. For example, after obtaining IP addresses,

clients such as IP phones need parameters such as the startup configuration file to work normally. You can run the **next-server** command to specify the server address used after a client obtains an IP address. The client then requests the configuration parameters from the specified server after obtaining an IP address.

If users use addresses in the interface address pool, run the **dhcp server next-server** command to specify the DHCP server IP address. If users use addresses in the global address pool, run the **next-server** command to specify the DHCP server IP address.

Precautions

- Only one IP address of a server that provides network services can be configured in each IP address pool view or DHCP Option template view. If the system needs multiple IP addresses of servers that provide network services, configure multiple IP address pools or DHCP Option templates.
- If you run the **next-server** command multiple times, only the latest configuration takes effect.

Example

In the IP address pool view, set the IP address of a server for the DHCP client after the client automatically obtains the IP address to 10.1.2.2.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] next-server 10.1.2.2
```

In the DHCP Option template view, set the IP address of a server for the DHCP client after the client automatically obtains the IP address to 10.1.2.2.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] next-server 10.1.2.2
```

Related Topics

8.3.48 dhcp server next-server

8.3.20 dhcp option template

8.3.94 option

Function

The **option** command configures the user-defined option that a DHCP server assigns to a DHCP client.

The **undo option** command deletes the user-defined option that a DHCP server assigns to a DHCP client.

By default, no user-defined option that a DHCP server assigns to a DHCP client is configured.

Format

option *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> }

undo option [*code* [**sub-option** *sub-code*]]

Parameters

Parameter	Description	Value
code	Specifies the code for a user-defined option.	The value is an integer that ranges from 1 to 254, except values 1, 3, 6, 15, 44, 46, 50, 51, 52, 53, 54, 55, 57, 58, 59, 61, 82, 121 and 184. **NOTE** There are well-known options and customized options. For details about well-known options, see RFC 2132.
sub-option *sub-code*	Specifies the code of a user-defined sub-option.	The value is an integer that ranges from 1 to 254. For details about well-known options, see RFC 2132.
ascii *ascii-string*	Specifies the user-defined option code as an ASCII character string.	The value is a string of characters case-sensitive characters with spaces supported. If **sub-option** is not specified, the value is a string of 1 to 255 characters. If **sub-option** is specified, the value is a string of 1 to 253 characters.
hex *hex-string*	Specifies the user-defined option code as a hexadecimal string.	The value is a hexadecimal string with an even number of characters, for example, hh or hhhh. If **sub-option** is not specified, the value without spaces ranges from 1 to 254; if **sub-option** is specified, the value without spaces ranges from 1 to 252. The value can be a combination of digits (0-9) and letters (A-F and a-f).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-string*	Specifies the user-defined option code as a ciphertext character string.	The value is a string, you can enter a character string in plain text or cipher text. ● The character string in plain text is a string of 1 to 64 characters. ● The character string in cipher text is a string of 32 to 104. No matter whether the character string is entered in plain or cipher text, the character string is displayed in cipher text in the configuration file and in plain text in packets.
ip-address *ip-address*	Specifies the user-defined option code as an IP address.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. The option field in a DHCP packet carries control information and parameters. If a DHCP server is configured with options, when a DHCP client applies for an IP address, the client can obtain the configurations in the option field of the DHCP response packet from the DHCP server. To configure user-defined options for an interface address pool, run the **dhcp server option** command.

Precautions

- To ensure accuracy, read the Request For Comments (RFC) before configuring options.
- When the password is contained in option, the **ascii** or **hex** type is insecure. Set the option type to **cipher**. A secure password should contain at least two types of the following: lowercase letters, uppercase letters, number, and

special characters. In addition, the password must consist of six or more than six characters.

- Note the following if the **option** *code* [**sub-option** *sub-code*] { **ascii** *ascii-string* | **hex** *hex-string* | **cipher** *cipher-string* | **ip-address** *ip-address* &<1-8> } command is not executed for the first time:
  - If the new *code* is different from the existing *code*, both new and existing configurations take effect.
  - If the new *code* is the same as the existing *code*, the following situations may occur:
    - When a *sub-code* is specified in the existing command, the new configuration overrides the existing configuration if the new and existing *sub-code*s are the same, and both the new and existing configurations take effect if the new and existing *sub-code*s are different. If no *sub-code* is specified in the new command, the new configuration overrides the existing configuration.
    - When no *sub-code* is specified in the existing command, the new configuration overrides the existing configuration.

Example

In the global address pool **global1**, configure Option64 to 0x11 (a hexadecimal number).

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] option 64 hex 11
```

In the DHCP Option template **template1**, configure Option64 to 0x11 (a hexadecimal number).

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option 64 hex 11
```

Related Topics

8.3.83 ip pool (system view)

8.3.49 dhcp server option

8.3.20 dhcp option template

8.3.95 option121

Function

The **option121** command configures the classless static route for the DHCP client.

The **undo option121** command deletes a configured classless static route.

By default, no classless static route is configured.

Format

option121 ip-address { *ip-address mask-length gateway-address* } &<1-8>

undo option121 [**ip-address** *ip-address mask-length gateway-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
gateway-address	Specifies the gateway address of a route.	The value is in dotted decimal notation.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **option121** command applies to only the DHCP server. The **option121** command configures Option 121 that defines a classless static route allocated to a client.

mask-length and *gateway-address* specify a classless static route. The **option121** command configures a maximum of eight classless static routes.

Precautions

- To configure multiple classless static routes, run the **option121** command repeatedly.
- The **undo option121** command will delete all classless static routes. To delete one classless static route, run the **undo option121 ip-address** *ip-address mask-length gateway-address* command.

Example

In the IP address pool view, configure classless static routes delivered by the DHCP server.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] option121 ip-address 10.10.10.10 24 10.11.11.11
```

In the DHCP Option template view, configure classless static routes delivered by the DHCP server.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option121 ip-address 10.10.10.10 24 10.11.11.11
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.83 ip pool (system view)
8.3.49 dhcp server option
8.3.20 dhcp option template

8.3.96 option184

Function

The **option184** command configures the Option 184 field for the DHCP client.

The **undo option184** command deletes a configuration in the Option 184 field.

By default, no content in the Option 184 field is configured.

Format

option184 { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* }

undo option184 [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

NOTE

AR109, AR109W, AR109GW-L, AR129CGVW-L do not support **voice-vlan** *vlan-id* parameter.

Parameters

Parameter	Description	Value
ncp-ip *ip-address*	Specifies the IP address of the network call processor (NCP).	The value is in dotted decimal notation.
as-ip *ip-address*	Specifies the IP address of the backup NCP.	The value is in dotted decimal notation.
fail-over *ip-address*	Specifies the IP address in the failover route.	The value is in dotted decimal notation.
dialer-string	Specifies the dialer string.	The value is a string of 1 to 64 characters.
voice-vlan *vlan-id*	Specifies the ID of a voice VLAN.	The value is an integer that ranges from 1 to 4094.

Views

IP address pool view, DHCP Option template view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **option184** command applies to only the DHCP server and configures Option 184 allocated by a DHCP server to a client in a global address pool.

Example

In the IP address pool view, configure the Option 184 field.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] option184 as-ip 192.168.1.10
```

In the DHCP Option template view, configure the Option 184 field.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] option184 as-ip 10.10.10.10
```

Related Topics

8.3.83 ip pool (system view)

8.3.49 dhcp server option

8.3.20 dhcp option template

8.3.97 reset dhcp client statistics

Function

The **reset dhcp client statistics** command clears packet statistics about a DHCP client.

Format

reset dhcp client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clear packet statistics about the DHCP client of the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset dhcp client statistics** command is applicable to DHCP client. During DHCP troubleshooting, statistics about the packets sent and received within a specified period need to be checked. Therefore, before collecting packet statistics, run the **reset dhcp client statistics** command to clear the existing packet statistics. Then you can run the **display dhcp client statistics** command to check packet statistics about the DHCP client.

Precautions

The **reset dhcp client statistics** command can be run multiple times at any interval.

Example

Clear packet statistics about the DHCP client.

```
<Huawei> reset dhcp client statistics
```

Related Topics

8.3.61 display dhcp client statistics

8.3.98 reset dhcp relay statistics

Function

The **reset dhcp relay statistics** command clears message statistics on a DHCP relay agent.

Format

reset dhcp relay statistics [**server-group** *group-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
server-group *group-name*	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. Collecting statistics on the DHCP messages sent and received within a specified period helps you locate DHCP faults. Run the **reset dhcp relay statistics** [**server-group** *group-name*] command to clear original statistics on DHCP messages, and run the **display dhcp relay statistics** [**server-group** *group-name*] command to view packet statistics about the DHCP relay agent.

- Run the **reset dhcp relay statistics server-group** *group-name* command to clear message statistics on DHCP relay agents connected to DHCP servers in a specified DHCP server group. The DHCP server group name needs to be specified.
- Run the **reset dhcp relay statistics** command to clear message statistics on all DHCP relay agents besides DHCP relay agents connected to DHCP servers in the DHCP server group.

Precautions

The **reset dhcp relay statistics** command can be run multiple times at any interval.

Example

Clear message statistics on the DHCP relay agent.

```
<Huawei> reset dhcp relay statistics
```

Related Topics

8.3.66 display dhcp relay statistics

 Copyright © Huawei Technologies Co., Ltd.

8.3.99 reset dhcp server statistics

Function

The **reset dhcp server statistics** command clears statistics on the DHCP server.

Format

reset dhcp server statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. Collecting statistics on the DHCP messages sent and received within a specified period helps you locate DHCP faults. Run the **reset dhcp server statistics** command to clear original statistics on DHCP messages and then run the **display dhcp server statistics** to view message statistics on the DHCP server.

Precautions

The **reset dhcp server statistics** command can be run multiple times at any interval.

Example

Clear message statistics on the DHCP server.

```
<Huawei> reset dhcp server statistics
```

Related Topics

8.3.69 display dhcp server statistics

8.3.100 reset dhcp statistics

Function

The **reset dhcp statistics** command clears packet statistics about a DHCP.

Format

reset dhcp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

During DHCP troubleshooting, statistics about the packets sent and received within a specified period need to be checked. Therefore, before collecting packet statistics, run the **reset dhcp statistics** command to clear the existing packet statistics. Then you can run the **display dhcp statistics** command to view DHCP message statistics.

Example

Clear packet statistics about the DHCP.

```
<Huawei> reset dhcp statistics
```

Related Topics

8.3.70 display dhcp statistics

8.3.101 reset ip pool

Function

The **reset ip pool** command resets the IP address pool configured on the device.

Format

reset ip pool { **interface** *interface-name* | **name** *ip-pool-name* } { *start-ip-address* [*end-ip-address*] | **all** | **conflict** | **expired** | **used** }

Parameters

Parameter	Description	Value
interface *interface-name*	Specifies the name of the interface address pool to be reset, which is represented by the type and number of an interface.	The value is a string of 1 to 64 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.
name *ip-pool-name*	Specifies the name of the global address pool to be reset.	The value is a string of 1 to 64 characters without spaces. A combination of digits, letters, underscores (_), and dots (.) is allowed.
start-ip-address	Specifies the start IP address of the IP address pool to be reset.	The value is in dotted decimal notation.
end-ip-address	Specifies the end IP address of the IP address pool to be reset.	The value is in dotted decimal notation.
all	Indicates that all the IP addresses need to be reset.	-
conflict	Indicates that the conflicting IP addresses need to be reset.	-
expired	Indicates that the expired IP addresses need to be reset.	-
used	Indicates that the used IP addresses need to be reset.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset ip pool** command resets the IP addresses that cannot be released in an IP address pool. If an IP address conflict occurs because two clients use the same IP address, run the **reset ip pool** command to reset the specified IP address pool.

Precautions

If a user's IP address is within the IP address range specified when this command is run, the user cannot continue to use the IP address after this command is run, and needs to send an IP address application request again.

The address pool status cannot be restored after this command is run. Therefore, exercise caution when deciding to run this command.

Follow-up Procedure

After the address pool is set to idle, the client can obtain an IP address from the global address pool.

Example

Reset the conflicting IP addresses in the IP address pool **mypool**.

```
<Huawei> reset ip pool name mypool conflict
```

Related Topics

8.3.71 display ip pool

8.3.102 reset ip pool import

Function

The **reset ip pool import** command clears the DNS and NetBIOS configurations dynamically obtained by an address pool.

Format

reset ip pool import { **all** | **dns** | **domain-name** | **nbns** }

Parameters

Parameter	Description	Value
all	Indicates that all the configurations dynamically obtained by the address pool need to be reset.	-
dns	Indicates that the DNS configurations dynamically obtained by the address pool need to be reset.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
domain-name	Indicates that the domain-name configurations dynamically obtained by the address pool need to be reset.	-
nbns	Indicates that the NBNS configurations dynamically obtained by the address pool need to be reset.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

This command applies to DHCP servers. When the DNS and NetBIOS configurations dynamically obtained by an address pool are incorrect, run the **reset ip pool import all** command to clear the obtained configurations before recollecting the DNS and NetBIOS configurations.

Example

Clear the DNS and NetBIOS configurations dynamically obtained by an address pool.

```
<Huawei> reset ip pool import all
Warning: The network configuration parameters imported from center server will
be clean up. Continue? [Y/N]y
```

Related Topics

8.3.84 import all

8.3.41 dhcp server import all

8.3.103 section (IP address pool view)

Function

The **section** command configures the IP address segment in an IP address pool.

The **undo section** command deletes the configured IP address segment in an IP address pool.

By default, the IP address segment in an IP address pool is not configured.

Format

section *section-id start-address* [*end-address*]

undo section *section-id*

Parameters

Parameter	Description	Value
section-id	Specifies the ID of the address segment in the IP address pool.	The value is an integer that ranges from 0 to 255.
start-address	Specifies the start IP address of the address segment.	The value is in dotted decimal notation.
end-address	Specifies the end IP address of the address segment. **NOTE** The end IP address must be larger than the start IP address. If the end IP address is not entered, there is only one address in the address segment.	The value is in dotted decimal notation.

Views

IP address pool view

Default Level

2: Configuration level

Usage Guidelines

An IP address pool consists of one or more IP address segments. The IP addresses on each address segment cannot overlap.

Example

Configure an IP address segment 10.1.1.10-10.1.1.15 with the ID 0 for the IP address pool **abc**.

```
<Huawei> system-view
[Huawei] ip pool abc
[Huawei-ip-pool-abc] section 0 10.1.1.10 10.1.1.15
```

8.3.104 sip-server (IP address pool view)

Function

The **sip-server** command configures the SIP server IP address assigned to a DHCP client in a global address pool.

The **undo sip-server** command deletes the configured SIP server IP address assigned to a DHCP client in a global address pool.

By default, the SIP server IP address assigned to a DHCP client in a global address pool is not configured.

Format

sip-server { **ip-address** *ip-address* &<1-2> | **list** *domain-name* &<1-2> }

undo sip-server

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IP address for the SIP server.	The value is in dotted decimal notation.
list *domain-name*	Specifies the domain name of the SIP server.	The value is a string of 1 to 63 characters.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to the DHCP server. To enable DHCP clients to normally access the Internet, the DHCP server needs to specify the SIP server IP address in the address pool when assigning IP addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured in each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- Before specifying the IP address or name for a SIP server, ensure that the SIP server exists.
- If you run this command repeatedly, the latest configuration overrides the previous ones.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify 192.168.1.1 as the IP address of the SIP server when addresses in the global address pool **global1** are assigned to clients.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] sip-server ip-address 192.168.1.1
```

8.3.105 sname

Function

The **sname** command configures the name of the server from which the DHCP client obtains the startup configuration file.

The **undo sname** command deletes the configured name of the server from which the DHCP client obtains the startup configuration file.

By default, no name is configured for the server from which the DHCP client obtains the startup configuration file.

Format

sname *sname*

undo sname

Parameters

Parameter	Description	Value
sname	Specifies the name of the server where the DHCP client obtains the startup configuration file.	The value is a string of 1 to 63 case-sensitive characters without spaces.

Views

IP address pool view, DHCP Option template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Besides assigning IP addresses, a DHCP server can also provide the required network configuration parameters, such as the startup configuration file name for the DHCP client. After the name of the server from which the DHCP client obtains the startup configuration file is configured using the **sname** command, the DHCP client obtains the startup configuration file from this server.

Precautions

Ensure that the route between the DHCP client and the file server from which the DHCP client obtains the startup configuration file is reachable.

Example

In the IP address pool view, configure the name of the server from which the DHCP client obtains the startup configuration file as **example**.

```
<Huawei> system-view
[Huawei] ip pool p1
[Huawei-ip-pool-p1] sname example
```

In the DHCP Option template view, configure the name of the server from which the DHCP client obtains the startup configuration file as **Huawei**.

```
<Huawei> system-view
[Huawei] dhcp option template template1
[Huawei-dhcp-option-template-template1] sname Huawei
```

Related Topics

8.3.83 ip pool (system view)

8.3.20 dhcp option template

8.3.106 snmp-agent trap enable feature-name dhcp

Function

The **snmp-agent trap enable feature-name dhcp** command enables the trap function for the DHCP module.

The **undo snmp-agent trap enable feature-name dhcp** command disables the trap function for the DHCP module.

For details about whether the trap function for the DHCP module is enabled or disabled by default, see **8.3.73 display snmp-agent trap feature-name dhcp all**.

Format

snmp-agent trap enable feature-name dhcp [**trap-name** { **hwdhcppktratealarm** | **hwdhcpsnpchaddralarm** | **hwdhcpv6pktprefixalarm** | **hwndsnpusernumberalarmglobal** | **hwndsnpusernumberalarmglobalresume** | **hwndsnpusernumberalarmif** | **hwndsnpusernumberalarmifresume** | **hwnomatchsnpbindtbldhcppktalarm** | **hwsnpusernumberalarmglobal** | **hwsnpusernumberalarmglobalresume** | **hwsnpusernumberalarmif** | **hwsnpusernumberalarmifresume** | **hwsnpusernumberalarmvlan** | **hwsnpusernumberalarmvlanresume** | **hwuntrustedreplypktalarm** }]

undo snmp-agent trap enable feature-name dhcp [**trap-name** { **hwdhcppktratealarm** | **hwdhcpsnpchaddralarm** | **hwdhcpv6pktprefixalarm** | **hwndsnpusernumberalarmglobal** | **hwndsnpusernumberalarmglobalresume** | **hwndsnpusernumberalarmif** | **hwndsnpusernumberalarmifresume** | **hwnomatchsnpbindtbldhcppktalarm** | **hwsnpusernumberalarmglobal** | **hwsnpusernumberalarmglobalresume** | **hwsnpusernumberalarmif** | **hwsnpusernumberalarmifresume** | **hwsnpusernumberalarmvlan** | **hwsnpusernumberalarmvlanresume** | **hwuntrustedreplypktalarm** }]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the DHCP module.	-
hwdhcppktratealarm	Enables the device to send a Huawei proprietary trap when the number of discarded DHCP packets whose rate exceeds the limit exceeds the threshold.	-
hwdhcpsnpchaddra-larm	Enables the device to send a Huawei proprietary trap when the number of discarded DHCP packets whose CHADDR field differs from the source MAC address exceeds the threshold.	-
hwdhcpv6pktprefixalarm	Enables the device to send a Huawei proprietary trap when the DHCPv6 prefix length exceeds the threshold.	-
hwndsnpusernumbera-larmglobal	Enables the device to send a Huawei proprietary trap when the number of ND access users on the device exceeds the upper threshold.	-
hwndsnpusernumbera-larmglobalresume	Enables the device to send a Huawei proprietary trap when the number of ND access users on the device falls below the lower threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwndsnpusernumberalarmif	Enables the device to send a Huawei proprietary trap when the number of ND access users on an interface exceeds the upper threshold.	-
hwndsnpusernumberalarmifresume	Enables the device to send a Huawei proprietary trap when the number of ND access users on an interface falls below the lower threshold.	-
hwnomatchsnpbindtbldhcppktalarm	Enables the device to send a Huawei proprietary trap when the number of DHCP Request packets that do not match DHCP snooping binding entries and are discarded on an interface exceeds the threshold.	-
hwsnpusernumberalarmglobal	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on the device exceeds the upper threshold.	-
hwsnpusernumberalarmglobalresume	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on the device falls below the lower threshold.	-
hwsnpusernumberalarmif	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on an interface exceeds the upper threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwsnpusernumberalarmifresume	Enables the device to send a Huawei proprietary trap when the number of DHCP access users on an interface falls below the lower threshold.	-
hwsnpusernumberalarmvlan	Enables the device to send a Huawei proprietary trap when the number of DHCP access users in a VLAN exceeds the upper threshold.	-
hwsnpusernumberalarmvlanresume	Enables the device to send a Huawei proprietary trap when the number of DHCP access users in a VLAN falls below the lower threshold.	-
hwuntrustedreplypktalarm	Enables the device to send a Huawei proprietary trap when the number of DHCP Reply packets discarded on an untrusted interface exceeds the threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **snmp-agent** to enable the trap function for one or more events.

NOTE

For traps that are enabled by default, the device has the trap suppression function configured and does not report traps within 10 minutes.

Example

Enable the trap function for hwdhcppktratealarm of the DHCP module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name dhcp trap-name hwdhcppktratealarm
```

Related Topics

8.3.73 display snmp-agent trap feature-name dhcp all

8.3.107 snmp-agent trap enable feature-name mid_am

Function

The **snmp-agent trap enable feature-name mid_am** command enables the trap function for the AM module.

The **undo snmp-agent trap enable feature-name mid_am** command disables the trap function for the AM module.

By default, the trap function is enabled for the AM module.

Format

snmp-agent trap enable feature-name mid_am [**trap-name** { **hwusedipreachthreshold** | **hwusedipreachthresholdresume** }]

undo snmp-agent trap enable feature-name mid_am [**trap-name** { **hwusedipreachthreshold** | **hwusedipreachthresholdresume** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event of the AM module.	-
hwusedipreachthres-hold	Enables the function of sending Huawei proprietary traps when the number of used IP addresses in an IP address pool exceeds the upper trap threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwusedipreachthre-sholdresume	Enables the function of sending Huawei proprietary traps when the number of used IP addresses in an IP address pool falls below the lower trap threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** as required to enable the trap function for one or more events.

NOTE

The device has the trap suppression function configured and does not report traps within 10 minutes.

Example

Enable all traps of the AM module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mid_am
```

Related Topics

8.3.74 display snmp-agent trap feature-name mid_am all

8.3.108 static-bind

Function

The **static-bind** command binds an IP address in a global address pool to a MAC address of a client.

The **undo static-bind** command unbinds the IP address in a global address pool from a MAC address.

By default, the IP address in a global address pool is not bound to any MAC address.

Format

static-bind ip-address *ip-address* **mac-address** *mac-address* [**option-template** *template-name* | **description** *description*]

undo static-bind [**ip-address** *ip-address* | **mac-address** *mac-address*]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies the IP address to be bound. The IP address must be a valid IP address in the global address pool.	The value is in dotted decimal notation.
mac-address *mac-address*	Specifies the user MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
option-template *template-name*	Specifies the name of the DHCP Option template. To allocate network configuration parameters except IP addresses to static clients, specify the parameter. Before specifying the parameter, run the **dhcp option template** command to create a DHCP option template, and configure network parameters for static clients in the DHCP Option template view.	The name is a string of 1 to 31 case-sensitive characters without spaces.
description *description*	Specifies the user description.	The value is a string of 1 to 256 case-sensitive characters. It can contain spaces.

Views

IP address pool view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind** command applies to DHCP servers. When planning a network, you need to allocate fixed IP addresses to some important hosts to ensure reliability. In this case, you can bind IP addresses in the address pool to the MAC addresses of these hosts. After the preceding configuration is complete, if the host of the MAC address to which the IP address is bound request an IP address from the DHCP server, the DHCP server finds the bound IP address based on the host's MAC address and allocates this IP address to the host, ensuring that the IP address obtained by the host is fixed.

You can run the **static-bind** command to bind an IP address in a global address pool to a MAC address.

You can run the **dhcp server static-bind** command to bind an IP address in an interface address pool to a MAC address.

Prerequisites

Network segment addresses that can be assigned from the global address pool have been configured using the **network (IP address pool view)** command.

Precautions

- Ensure that the bound IP address is not configured as the IP address that cannot be allocated using the **8.3.77 excluded-ip-address** command and is not allocated by the DHCP server.
- You can run the **display ip pool** command to view the used IP addresses in the current address pool and select an available IP address to be bound to the MAC address. To bind used IP addresses to MAC addresses, run the **reset ip pool** command to reclaim used IP addresses first. IP addresses that are used can also be statically bound to MAC addresses or unbound from MAC addresses. When an IP address is statically bound to a MAC address, ensure that the MAC address to be bound is the same as the MAC address of the user who actually uses the IP address.
- The DHCP server preferentially allocates the IP address that has been statically bound to the client's MAC address.
- After an IP address is bound to a MAC address, the IP address does not expire; the binding between the IP and MAC addresses cannot be deleted when the IP address is in use. After an IP address is bound to a MAC address, the IP address does not expire. After an automatically allocated IP address is statically bound to a MAC address, the lease time of the IP address becomes unlimited. After the static binding between the IP address and the MAC address is deleted, the lease time of the IP address becomes the same as that configured in the address pool.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a DHCP server to assign a fixed IP address 192.168.1.10 in the global address pool **global1** to a host with the MAC address dcd2-fc96-e4c0.

```
<Huawei> system-view
[Huawei] ip pool global1
[Huawei-ip-pool-global1] network 192.168.1.10 mask 24
[Huawei-ip-pool-global1] static-bind ip-address 192.168.1.10 mac-address dcd2-fc96-e4c0
```

Related Topics

8.3.83 ip pool (system view)

8.3.55 dhcp server static-bind

8.3.20 dhcp option template

8.3.109 vpn-instance (DHCP server group view)

Function

The **vpn-instance** command binds a DHCP server group to a VPN instance.

The **undo vpn-instance** command unbinds the VPN instance from a DHCP server group.

By default, no DHCP server is bound to a VPN instance.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance on the device.

Views

DHCP server group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP relay agents. To apply DHCP services in a VPN instance, you need to run the **vpn-instance** command to bind the created DHCP server group to the VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

The VPN instance bound to the DHCP server group on the DHCP relay agent must be the same as the VPN instance bound to the IP address pool on the DHCP server; otherwise, users in the IP address pool cannot go online.

Example

Bind DHCP server group **dhcp-srv1** to VPN instance **huawei**.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] ipv4-family
[Huawei-vpn-instance-huawei-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] dhcp server group dhcp-srv1
[Huawei-dhcp-server-group-dhcp-srv1] vpn-instance huawei
```

Related Topics

8.3.40 dhcp server group

8.3.110 vpn-instance (global address pool view)

Function

The **vpn-instance** command binds an IP address pool to a VPN instance.

The **undo vpn-instance** command restores the default setting.

By default, an IP address pool is not bound to any VPN instance.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance on the device.

 Copyright © Huawei Technologies Co., Ltd.

Views

Global address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to DHCP servers. To apply DHCP services in a VPN instance, you need to run the **vpn-instance** command to bind the created IP address pool to the VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

- The VPN instance bound to the IP address pool on the DHCP server must be the same as the VPN instance bound to the DHCP server group on the DHCP relay agent; otherwise, users in the IP address pool cannot go online using this DHCP server group.
- If an IP address pool is bound to a VPN instance, IP addresses assigned from this address pool are VPN addresses.
- To bind an interface address pool to a VPN instance, run the **ip binding vpn-instance** command in the interface view.

Example

Bind the address pool **global1** to the VPN instance **huawei**.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] ipv4-family
[Huawei-vpn-instance-huawei-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] ip pool global1
[Huawei-ip-pool-global1] vpn-instance huawei
```

Related Topics

8.3.83 ip pool (system view)

12.9.33 ip binding vpn-instance

8.4 DNS Configuration Commands

8.4.1 ddns apply policy

Function

The **ddns apply policy** command allows you to apply DDNS policies on interfaces.

The **undo ddns apply policy** command deletes the configuration.

By default, no DDNS policy is bound to an interface.

Format

ddns apply policy *policy-name* [**fqdn** *domain-name*]

undo ddns apply policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Specifies a DDNS policy name.	The value must be the name of an existing DDNS policy.
fqdn *domain-name*	Specifies domain name updated by the DDNS.	The value is a string of 1 to 128 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DNS provides static mappings between domain names and IP addresses. When IP addresses of interfaces change, DNS cannot dynamically update mappings. After the specified DDNS policy is applied on an interface, if the IP address of the interface changes, the DDNS policy updates mapping between the specified Fully Qualified Domain Name (FQDN) and the IP address.

If a DDNS policy with the same name is bound to an interface repeatedly and different FQDNs are specified, only the latest configuration takes effect and a DDNS update is initiated.

Prerequisites

To apply the policy on an interface, you need to create the DDNS policy first, also the DDNS policy, including DDNS Server domain-name, DDNS Client domain-name, username and password, must be completely configured.

 Copyright © Huawei Technologies Co., Ltd.

Example

Apply the DDNS policy "test "on the Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ddns apply policy test
```

Related Topics

8.4.11 ddns policy

8.4.2 display ddns interface

Function

The **display ddns interface** command displays information about the interfaces to which DDNS policies are applied.

Format

display ddns interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Indicates all interfaces.	-
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about the interfaces to which DDNS policies are applied, run the **display ddns interface** command.

Example

Display the configuration of DDNS policies applied to Eth2/0/0.

```
<Huawei> display ddns interface ethernet 2/0/0
 Policies applied on interface Ethernet2/0/0 :
 ------------------------------------------------------------------------------
 Policy name          : 123
 Server             : ns.huawwei.com
 User name            : -
 Password             : -
```

```
Update method        : ddns
Update interval      : 3600 seconds
Current status       : START
Client FQDN          : 123
Client IP            : 0.0.0.0
Server IP            : -
Last update time     : 2015-10-27 10:30:28
Last update result   : Update failed
```

Table 8-38 Description of the **display ddns interface** command output

Item	Description
Policy name	DDNS policy name.
Server	Domain name of a DDN service provider.
User name	User name used for access to a DDNS service provider.
Password	Password used for access to a DDNS service provider.
Update method	DDNS update method: ● **http**: common HTTP update method ● **vendor-specific**: vendor-defined update method ● **ddns**: update method compliant with RFC 2136, which updates only A records. ● **ddns both**: update method compliant with RFC 2136, which updates A and PTR records.
Update interval	Interval at which a DDNS client initiates a DDNS update, in seconds.
Current status	Status of an applied DDNS policy: ● INIT: Initial state. ● ESTABLISH: Update is successful. ● AUTHENTICATION FAILED: Authentication failed. ● START: Update starts.
Client FQDN	Domain name of a DDNS client.
Client IP	IP address of a DDNS client.
Server IP	IP address of a DDNS server.
Last update time	Last update time.

Item	Description
Last update result	Last update result: ● Success: The update is successful. ● Resolve ddns server domain name fail: Failed to parse the domain name of the DDNS server. ● Authentication fail: Authentication failed. ● Update failed: The update failed. ● Updating: The update is ongoing.

8.4.3 display ddns policy

Function

The **display ddns policy** command displays DDNS policy information.

Format

display ddns policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays information about a specified DDNS policy	The DDNS policy name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ddns policy** command to view DDNS policy information. If no *policy-name* is specified, all DDNS policies information is displayed.

Example

Display current DDNS policy information.

```
<Huawei> display ddns policy test
 Policy name          : test
```

```
Server          : oray://username:password@phddnsdev.oray.net
User name       : -
Password        : -
Update method   : vendor-specific
Update interval : 3600 seconds
Apply interface : Ethernet2/0/0
```

Table 8-39 Description of the **display ddns policy** command output

Item	Description
Policy name	DDNS policy name.
Server	Domain-name of a DDNS service provider
User name	User name for accessing a DDNS service provider
Password	Password for accessing a DDNS service provider
Update method	Update mode of the DDNS Client. ● **http**: indicates the update mode of common http. ● **vendor-specific**: indicates the update mode defined by the vendors. ● **ddns**: indicates the update mode defined by RFC2136, which only updates Class-A records. ● **ddns both**: indicates the update mode defined by RFC2136, which updates Class-A records and PTR records.
Update interval	Interval for which the DDNS client initiates DDNS updates, in second.
Apply interface	Interface that applies this policy

8.4.4 display dns configuration

Function

The **display dns configuration** command displays the global DNS configurations.

Format

display dns configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global DNS configurations.

```
<Huawei> display dns configuration
 ------------------------------------------------------------------------------
 Dns resolve                      :  Disabled
 DNS-server-select-algorithm      :  Auto
 Dns server source ip address     :  -
 Dns server source ipv6 address   :  -
 Dns proxy                        :  Disabled
 Dns IPv6 proxy                   :  Disabled
 Dns relay                        :  Disabled
 Dns IPv6 relay                   :  Disabled
 Dns spoofing                     :  -
 Dns IPv6 spoofing                :  -
 Dns forward retry-number         :  2
 Dns forward retry-timeout        :  3
 Dns server vpn-instance          :  vpn1
 ------------------------------------------------------------------------------
```

Table 8-40 Description of the **display dns configuration** command output

Item	Description
Dns resolve	Whether dynamic DNS resolution is enabled. The value can be: ● Enabled: Dynamic DNS resolution is enabled. ● Disabled: Dynamic DNS resolution is disabled. To enable dynamic DNS resolution, run the **dns resolve** command.
DNS-server-select-algorithm	Algorithm for selecting a destination DNS server. The value can be: ● Fixed: The destination DNS server is selected in fixed order. ● Auto: The destination DNS server is selected in auto order. To specify an algorithm for selecting a destination DNS server, run the **dns-server-select-algorithm** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dns server source ip address	Source IP address of the local device for communication. To set the source IP address of the local device, run the **dns server source-ip** command.
Dns server source ipv6 address	Source IPv6 address of the local device for communication. To set the source IPv6 address of the local device, run the **dns server ipv6 source-ip** command.
Dns proxy	Whether DNS proxy is enabled. The value can be: ● Enabled: DNS proxy is enabled. ● Disabled: DNS proxy is disabled. To enable DNS proxy, run the **dns proxy enable** command.
Dns IPv6 proxy	Whether IPv6 DNS proxy is enabled. The value can be: ● Enabled: IPv6 DNS proxy is enabled. ● Disabled: IPv6 DNS proxy is disabled. To enable DNS proxy, run the **dns proxy ipv6 enable** command.
Dns relay	Whether DNS relay is enabled. The value can be: ● Enabled: DNS relay is enabled. ● Disabled: DNS relay is disabled. To enable DNS relay, run the **dns relay enable** command.
Dns IPv6 relay	Whether IPv6 DNS relay is enabled. The value can be: ● Enabled: IPv6 DNS relay is enabled. ● Disabled: IPv6 DNS relay is disabled. To enable IPv6 DNS relay, run the **dns relay ipv6 enable** command.
Dns spoofing	IP address that spoofs Reply packets. To enable DNS spoofing and specify the IP address that spoofs Reply packets, run the **dns spoofing** command.
Dns IPv6 spoofing	IPv6 address that spoofs Reply packets. To enable DNS spoofing and specify the IPv6 address that spoofs Reply packets, run the **dns spoofing ipv6** command.
Dns forward retry-number	Number of times for retransmitting query messages to the destination DNS server. To set the number of times for retransmitting query messages to the destination DNS server, run the **dns forward retry-number** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dns forward retry-timeout	Retransmission timeout period that the device sends query messages to the destination DNS server. To set the retransmission timeout period that the device sends query messages to the destination DNS server, run the **dns forward retry-timeout** command.
Dns server vpn-instance	Name of the VPN instance that the DNS server belongs to. If the VPN instance that the DNS server belongs to is not specified, this parameter is not displayed. To configure the name of the VPN instance that the DNS server belongs to, run the **dns server vpn-instance** command.

8.4.5 display dns domain

Function

The **display dns domain** command displays the configuration and sequence of domain name suffixes.

Format

display dns domain [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays the detail information of domain name suffixes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dns domain** command to view the configuration and sequence of domain name suffixes.

Example

Display the list of domain name suffixes.

```
<Huawei> display dns domain
Type:
```

```
D:Dynamic     S:Static

NO.  Type    Domain name                    TTL
1     S      com                          -
2     S      net                          -
```

Table 8-41 Description of the **display dns domain** command output

Item	Description
NO.	Domain name suffix numbers, that is, the configuration sequence of domain name suffixes.
Type	Domain name suffixes type, including dynamic and static domain name suffix.
Domain name	Configured domain name suffix. In this example, two domain name suffixes are displayed. During DNS resolution, the first suffix "com" is added and sent to the DNS server. If the DNS server gives no response, the query message is resent. If the DNS server still gives no response, the query message is resent for a third time. If the DNS server still does not respond, the second suffix "net" is added and sent to the DNS server for searching for the mapped address.
TTL	Domain name suffix TTL.

Related Topics

8.4.12 dns domain

8.4.6 display dns dynamic-host

Function

The **display dns dynamic-host** command displays dynamic DNS entries saved in the domain name cache.

Format

display dns dynamic-host [**ip** | **naptr** | **srv**] [*domain-name*]

Parameters

Parameter	Description	Value
ip	Specifies the Class-A and PTR query dynamic DNS entries.	-
naptr	Specifies the NAPTR query dynamic DNS entries.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
srv	Specifies the SRV query dynamic DNS entries.	-
domain-name	Specifies the dynamic DNS entries of a domain name.	The value must be an existing domain name suffix.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dns dynamic-host** command to view dynamic DNS entries saved in the domain name cache and check whether domain names match the mapping entries.

Example

Display the dynamic DNS entries saved in the domain name cache.

```
<Huawei> display dns dynamic-host
Host                          TTL      Type   Address
sipx.autosrv.com                114       IP    192.168.1.1
sip.autosrv.com                 237       IP    192.168.1.2
sip.autonaptr.com               117       IP    192.168.1.3
_sip._tcp.autosrv.com            55       SRV   0 0 0 sipx.autosrv.com
                                          0 0 0 sip.autosrv.com
autonaptr.com                    0        NAPTR 101 10 A SIP+D2T  sip.autona

Total  :  5
```

Table 8-42 Description of the **display dns dynamic-host** command output

Item	Description
Host	Domain name. ● sipx.autosrv.com: indicates the domain name of the server providing the SIP service. ● _sip._tcp.autosrv.com: indicates the domain name of the server providing the SIP service through TCP in autosrv.com. ● autonaptr.com: indicates the domain name in the NAPTR resource record.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TTL	Time left before dynamic DNS entries saved in the cache age out, in seconds.
Type	Query type: ● IP: Class-A query, which is used to request the IP address corresponding to a domain name, or Pointer (PTR) query, which is used to request the domain name corresponding to an IP address. ● SRV: Service Record (SRV) query, which is used to obtain information about a server based on the protocol running on the server, including the domain name and port number. ● NAPTR: Naming Authority Pointer (NAPTR) query, which is used to obtain information about a server based on the server's domain name, including the IP address, and the transmission protocol.
Address	IP address mapping the domain name. ● 192.168.1.1: indicates the IPv4 address. ● 0 0 0 sipx.autosrv.com: indicates the SRV query result. In the SRV query result, **0 0 0** indicates the priority, weight, and port number respectively, and **sipx.autosrv.com** indicates the domain name of the server providing the SIP service. ● 101 10 A SIP+D2T sip.autona: indicates the NAPTR query result. In the NAPTR query result, **101 10** indicates the NAPTR resource record sequence and priority; **A** indicates that the IP address to be queried; **SIP+D2T** indicates that SIP and TCP are used; **sip.autona** indicates the domain name to be queried.

Related Topics

8.4.29 reset dns dynamic-host

8.4.7 display dns forward table

Function

The **display dns forward table** command displays the DNS forwarding table, including the mapping entry of the source IP address in a specified DNS query message.

Format

display dns forward table [**source-ip** *ip-address*]

Parameters

Parameter	Description	Value
source-ip *ip-address*	Specifies the source IP address in query messages.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DNS proxy or DNS relay is enabled, you can run the **display dns forward table** command to view the DNS table of IP addresses.

NOTE

When the device receives DNS request packets from the client but does not receive DNS reply packets from the server, you need to run the **display dns forward table** command to view the DNS forwarding table.

Example

Display the DNS table on the DNS proxy or DNS relay.

```
<Huawei> display dns forward table
Domain name          : www.domain.com
Source IP            : 10.136.128.53
Source port          : 2055
Source packet id     : 3562
Forward packet id    : 60669
Query type           : 1
VPN-Instance         : vpna
```

Table 8-43 Description of the display dns forward table command output

Item	Description
Domain name	Domain name.
Source IP	IP address of the client.
Source port	Port number of the client.
Source packet id	ID of the request packet from the client.
Forward packet id	ID of the forwarded packet, which corresponds to the ID of the request packet from the client.
Query type	Query type: ● 1: Class-A query ● 12: Pointer Record (PTR) query ● 33: SRV query ● 35: NAPTR query
VPN-Instance	Name of the VPN instance that the DNS client belongs to.

8.4.8 display dns statistics

Function

The **display dns statistics** command displays statistics on DNS packets.

Format

display dns statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check statistics on DNS packets, including the DNS IPv4 and IPv6 addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics on DNS packets.

```
<Huawei> display dns statistics

SumFromDNSv4Client          : 0
SumToDNSv4Client            : 0
SumFromDNSv4Server          : 0
SumToDNSv4Server            : 0

SumFromDNSv6Client          : 0
SumToDNSv6Client            : 0
SumFromDNSv6Server          : 0
SumToDNSv6Server            : 0

RetryFromClient             : 0
NotQueryFromClient          : 0
ParseFailFromClient         : 0
TooLongFromClient           : 0
LocalQueryFromClient        : 0
NotStandardQueryFromClient  : 0

NotRespFromServer           : 0
NoAnswerFromServer          : 0
ParseFailFromServer         : 0
TooLongFromServer           : 0
ErrorRespFromServer         : 0
NotStandardQueryFromServer  : 0

ResolvePolicyRuleDeny       : 0
```

Table 8-44 Description of the **display dns statistics** command output

Item	Description
SumFromDNSv4Client	Total number of packets sent from IPv4 DNS clients.
SumToDNSv4Client	Total number of packets sent to IPv4 DNS clients.
SumFromDNSv4Server	Total number of packets sent from IPv4 DNS servers.
SumToDNSv4Server	Total number of packets sent to IPv4 DNS servers.
SumFromDNSv6Client	Total number of packets sent from IPv6 DNS clients.
SumToDNSv6Client	Total number of packets sent to IPv6 DNS clients.
SumFromDNSv6Server	Total number of packets sent from IPv6 DNS servers.
SumToDNSv6Server	Total number of packets sent to IPv6 DNS servers.
RetryFromClient	Number of packets retransmitted from clients.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
NotQueryFromClient	Number of non-query packets sent from clients.
ParseFailFromClient	Number of packets that failed to be parsed and are sent from clients.
TooLongFromClient	Number of packets longer than 512 bytes sent from clients.
LocalQueryFromClient	Number of query packets of which the source address is a local address and sent from clients.
NotStandardQueryFromClient	Number of nonstandard query packets sent from clients.
NotRespFromServer	Number of non-response packets sent from servers.
NoAnswerFromServer	Number of response packets of which the ANCOUNT field is 0 and sent from servers.
ParseFailFromServer	Number of packets that failed to be parsed and are sent from servers.
TooLongFromServer	Number of packets longer than 512 bytes sent from servers.
ErrorRespFromServer	Number of error response packets sent from servers.
NotStandardQueryFromServer	Number of nonstandard query packets sent from servers.
ResolvePolicyRuleDeny	Times of resolve policy rule deny.

8.4.9 display dns server

Function

The **display dns server** command displays the configuration and sequence of the current DNS server.

Format

display dns server [**verbose**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
verbose	Displays detailed information about the DNS server.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring DNS, run the **display dns server** command to view the configuration and sequence of current DNS servers.

Example

Display configurations of a DNS server.

```
<Huawei> display dns server
Type:
D:Dynamic     S:Static

IPv4 DNS server :
NO. Type Status Used IP Address
0   S    -      Yes  10.1.1.1
1   S    -      Yes  10.1.1.2
2   D    Up     Yes  10.1.1.2
3   D    Up     Yes  10.1.1.3

IPv6 DNS servers :
NO. Type Status Used IPv6 Address                        Interface
0   S    -      Yes  FC00:1::1                          -
1   D    -      Yes  FC00:1::1                          -
2   D    -      Yes  FC00:1::2                          -
```

Table 8-45 Description of the **display dns server** command output

Item	Description
Type	Configuration type of the DNS server IP address, including dynamic and static.
IPv4 DNS server	IPv4 DNS server configuration.
NO.	DNS server number, indicating the order in which they were configured.
Status	DNS server status.
Used	Indicates whether the DNS server is used.
IP Address	IPv4 address of the DNS server.

Item	Description
IPv6 Address	IPv6 address of the DNS server.
IPv6 DNS servers	IPv6 DNS server configuration.
Interface	Name of the outbound interface communicating with the DNS server.

Related Topics

8.4.19 dns server

8.4.10 display ip host

Function

The **display ip host** command displays mappings between hosts and IP addresses.

Format

display ip host

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring static DNS entries, you can run the **display ip host** command to view the mapping between hosts and IP addresses.

Example

Display mappings between hosts and IP addresses.

```
<Huawei> display ip host
Host                Age       Flags  Address
example               0        static 10.2.2.2
```

Table 8-46 Description of the **display ip host** output of the command

Item	Description
Host	Host name.
Age	Aging time. The value 0 indicates that the static DNS entry need not be aged.
Flags	Status of the domain name. "Static" indicates the static domain name.
Address	IP address matching the host.

8.4.11 ddns policy

Function

The **ddns policy** command creates a DDNS policy and enters the DDNS policy view.

The **undo ddns policy** command deletes a DDNS policy.

By default, no DDNS policy is created in the system.

Format

ddns policy *policy-name*

undo ddns policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the DDNS policy.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

DNS provides static mappings between domain names and IP addresses. When IP addresses of nodes change, DNS cannot dynamically update mappings. If a DNS

client uses the original domain name to access the node, the DNS client will fail to access the node because the IP address mapping the domain name is incorrect. The DDNS updates the mappings between the domain name and the IP address on the DNS server to ensure that the IP address can be resolved correctly. The device can function as a DDNS client. When the IP address of the interface that provides services changes, the device sends a request of updating the domain name entry to the DDNS server. After receiving the request, the DDNS server updates the domain name entry.

Example

Create a DDNS policy "test ".

```
<Huawei> system-view
[Huawei] ddns policy test
[Huawei-ddns-policy-test]
```

8.4.12 dns domain

Function

The **dns domain** command configures a domain name suffix of a server or a host on a DNS client that the DNS client wants to access.

The **undo dns domain** command deletes a configured domain name suffix from a DNS client.

By default, no domain name suffix is configured on a DNS client.

Format

dns domain *domain-name*

undo dns domain [*domain-name*]

Parameters

Parameter	Description	Value
domain-name	Specifies a domain name suffix on a DNS Client.	The value is a string of 1 to 64 characters, spaces not supported. The string is a combination of digits, letters, underscores (_), dots (.), and hyphen (-).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

Generally, the domain name suffixes of some servers or hosts that a DNS client accesses are the same, for example, com.cn. In this case, you can set the domain name suffixes. When a DNS client accesses a host:

- If the entered domain name does not carry dots (.), for example, "huawei", the system first adds the suffix com.cn to the domain name and sends a domain name request of "huawei.com.cn" to the DNS server to find the IP address corresponding to the domain name. If the DNS client does not receive any response from the server, it sends a domain name request of "huawei" to the DNS server to find the IP address corresponding to the domain name.
- If the entered domain name carries dots (.), for example, "ilite.huawei", the system first sends a domain name request of "ilite.huawei" to the DNS server to find the IP address corresponding to the domain name. If the DNS client does not receive any response from the server, it adds the suffix com.cn to the domain name and sends a domain name request of "ilite.huawei.com.cn" to the DNS server to find the IP address corresponding to the domain name.

Precautions

A DNS client supports a maximum of 10 domain name suffixes. To configure multiple domain name suffixes, you can run the **dns domain** command repeatedly.

If the name of the suffix to be deleted is specified, the specified suffix is deleted. Otherwise, all the suffixes are deleted.

Example

Configure a domain name suffix as com.cn.

```
<Huawei> system-view
[Huawei] dns domain com.cn
```

Related Topics

8.4.5 display dns domain

8.4.13 dns forward retry-number

Function

The **dns forward retry-number** command sets the number of times for the device to retransmit query requests to the destination DNS server.

The **undo dns forward retry-number** command restores the default retransmission count.

By default, the retransmission count is 2.

Format

dns forward retry-number *number*

undo dns forward retry-number

Parameters

Parameter	Description	Value
number	Specifies the number of times for the device to retransmit query requests to the destination DNS server.	The value is an integer from 0 to 15.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The mode for a device to select the destination DNS server can be **auto** and **fixed**. For how a device sends DNS request packets to the destination DNS server in each mode and the corresponding precautions, see **8.4.22 dns-server-select-algorithm**.

If the number of times for the device to retransmit DNS request packets to each destination DNS server is relatively large and the packet retransmission timeout period is relatively long, the time for the DNS client to wait for the response from the DNS server is too long. However, the request timeout period of the DNS client is shorter, so that the DNS client fails to properly receive response packets from the server. To enable the DNS server to rapidly respond DNS request packets, you can run the **dns forward retry-number** and **dns forward retry-timeout** commands to adjust the number of times for the device to retransmit DNS request packets to each DNS server and the packet retransmission timeout period for ensuring that the DNS client can properly receive response packets from the server.

You need to consider the number of times for the device to retransmit DNS query requests to the destination DNS server, retransmission timeout period, and mode for the device to select the DNS server into consideration before configuring the query timeout period on a device.

- When the mode for a device to select the destination DNS server is **auto**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period
- When the mode for a device to select the destination DNS server is **fixed**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period x Number of DNS servers

Example

Set the retransmission count that the device sends query packets to the destination DNS server to 1.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dns forward retry-number 1
```

8.4.14 dns forward retry-timeout

Function

The **dns forward retry-timeout** command sets the retransmission timeout period that the device sends Query packets to the destination DNS server.

The **undo dns forward retry-timeout** command restores the default retransmission timeout period.

By default, the retransmission timeout period for which the device sends DNS query requests to the destination DNS server is 3 seconds.

Format

dns forward retry-timeout *time*

undo dns forward retry-timeout

Parameters

Parameter	Description	Value
time	Specifies the retransmission timeout period that the device sends Query packets to the destination DNS server.	The value is an integer that ranges from 1 to 15, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The mode for a device to select the destination DNS server can be **auto** and **fixed**. For how a device sends DNS request packets to the destination DNS server in each mode and the corresponding precautions, see **8.4.22 dns-server-select-algorithm**.

If the number of times for the device to retransmit DNS request packets to each destination DNS server is relatively large and the packet retransmission timeout period is relatively long, the time for the DNS client to wait for the response from the DNS server is too long. However, the request timeout period of the DNS client is shorter, so that the DNS client fails to properly receive response packets from the server. To enable the DNS server to rapidly respond DNS request packets, you

 Copyright © Huawei Technologies Co., Ltd.

can run the **dns forward retry-number** and **dns forward retry-timeout** commands to adjust the number of times for the device to retransmit DNS request packets to each DNS server and the packet retransmission timeout period for ensuring that the DNS client can properly receive response packets from the server.

You need to consider the number of times for the device to retransmit DNS query requests to the destination DNS server, retransmission timeout period, and mode for the device to select the DNS server into consideration before configuring the query timeout period on a device.

- When the mode for a device to select the destination DNS server is **auto**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period
- When the mode for a device to select the destination DNS server is **fixed**, the query timeout period of a DNS device is calculated as follows: (Number of retransmission times + 1) x Retransmission timeout period x Number of DNS servers

Example

Set the retransmission timeout period that the device sends Query packets to the destination DNS server to 2 seconds.

```
<Huawei> system-view
[Huawei] dns forward retry-timeout 2
```

8.4.15 dns proxy enable

Function

The **dns proxy enable** command enables DNS proxy.

The **undo dns proxy enable** command disables DNS proxy.

By default, DNS proxy is disabled.

Format

dns proxy enable

undo dns proxy enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

DNS proxy is used to forward DNS requests and reply packets between the DNS client and DNS server. The DNS client sends a DNS request packet to the device on which DNS proxy is enabled. The device sends the request packet to the DNS server and sends the reply packet to the DNS client. The device functions as the DNS proxy to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable DNS proxy.

```
<Huawei> system-view
[Huawei] dns proxy enable
```

Disable DNS proxy.

```
<Huawei> system-view
[Huawei] undo dns proxy enable
```

Related Topics

8.4.17 dns relay enable

8.4.7 display dns forward table

8.4.30 reset dns forward table

8.4.16 dns proxy sip-info insert-mode decompression-domain-name

Function

The **dns proxy sip-info insert-mode decompression-domain-name** command inserts SIP server information to DNS response packets in domain name decompression mode when the device functions as a DNS proxy.

The **undo dns proxy sip-info insert-mode decompression-domain-name** command restores the default insert mode.

By default, the domain name decompression mode is not used.

Format

dns proxy sip-info insert-mode decompression-domain-name

undo dns proxy sip-info insert-mode decompression-domain-name

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command applies only to the Branch Exchange Survivable Telephony (BEST) solution. In the BEST solution, the phone functions as the DNS client and the device functions as the DNS proxy. When the DNS client initiates an SRV query, the device inserts SIP server information to the DNS response packet. For example, when a Cisco phone is used and the **dns proxy sip-info insert-mode decompression-domain-name** command is not used to insert SIP server information to DNS response packets in domain name decompression mode, the phone cannot resolve DNS response packets that have SIP server information inserted.

Example

Insert SIP server information to DNS response packets in domain name decompression mode in the BEST solution.

```
<Huawei> system-view
[Huawei] dns resolve
[Huawei] dns proxy enable
[Huawei] dns proxy sip-info insert-mode decompression-domain-name
```

8.4.17 dns relay enable

Function

The **dns relay enable** command enables DNS relay.

The **undo dns relay enable** command disables DNS relay.

By default, DNS relay is disabled.

Format

dns relay enable

undo dns relay enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

DNS relay is used to forward DNS requests and reply packets between the DNS client and DNS server. The DNS client sends a DNS request packet to the device on which DNS relay is enabled. The device sends the request packet to the DNS server and sends the reply packet to the DNS client. The device functions as the DNS relay to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable DNS relay.

```
<Huawei> system-view
[Huawei] dns relay enable
```

Disable DNS relay.

```
<Huawei> system-view
[Huawei] undo dns relay enable
```

Related Topics

8.4.15 dns proxy enable

8.4.7 display dns forward table

8.4.30 reset dns forward table

8.4.18 dns resolve

Function

The **dns resolve** command enables dynamic DNS resolution.

The **undo dns resolve** command disables dynamic DNS resolution.

By default, the dynamic DNS resolution is disabled.

Format

dns resolve

undo dns resolve

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To obtain IP addresses mapping domain names using the DNS server, run the **dns resolve** command to enable dynamic DNS resolution on the device.

Example

Enable dynamic DNS resolution.

```
<Huawei> system-view
[Huawei] dns resolve
```

Related Topics

8.4.19 dns server

8.4.19 dns server

Function

The **dns server** command configures an IP address for a DNS server.

The **undo dns server** command deletes the DNS server IP address.

By default, no DNS server IP address is configured.

Format

dns server *ip-address* [**track nqa** *admin-name test-name*]

undo dns server [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DNS server.	The value is in dotted decimal notation.
track nqa *admin-name test-name*	Specifies the NQA test instance to be associated with the DNS server. • *admin-name*: specifies the name of the administrator for the NQA test instance. • *test-name*: specifies the name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without any space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A maximum of six DNS servers can be specified on Router. During dynamic DNS resolution, query messages are sent to DNS servers based on the configuration sequence of DNS servers.

The system sends a query to the DNS server first configured. If no response is received in the specified period of time (which can be configured by running the command **8.4.14 dns forward retry-timeout**), it resends the query twice. If receiving no response for the specified times (which can be configured by running the command **8.4.13 dns forward retry-number**), the system sends the query to the DNS server second configured and so on.

Prerequisites

Before specifying the NQA test instance to be associated with the DNS server using **track nqa** *admin-name test-name*, perform the following operations and start the NQA test instance.

- Configuring and starting an NQA test instance of the DNS type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type dns** command to configure the test type to DNS.
  d. Run the **dns-server ipv4** *ip-address* command to configure the DNS server address.
  e. Run the **destination-address url** *urlstring* command to configure the destination host name.
  f. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  g. Run the **start** command to start the NQA test instance.

     An NQA test instance can be started immediately, at a specified time, or after a specified delay.

     - Run the **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance immediately.
     - Run the **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance at a specified time.
     - Run the **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance after a specified delay.

 Copyright © Huawei Technologies Co., Ltd.

- Configuring and starting an NQA test instance of the ICMP type
  a. Run the **system-view** command to enter the system view.
  b. Run the **nqa test-instance** *admin-name test-name* command to create an NQA test instance and enter the test instance view.
  c. Run the **test-type icmp** command to configure the test type to ICMP.
  d. Run the **destination-address ipv4** *ipv4-address* command to configure the destination IP address.
  e. Run the **frequency** *interval* command to set the automatic test interval for the NQA test instance.
  f. Run the **start** command to start the NQA test instance.

     An NQA test instance can be started immediately, at a specified time, or after a specified delay.

     - Run the **start now** [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance immediately.
     - Run the **start at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance at a specified time.
     - Run the **start delay** { **seconds** *second* | *hh*:*mm*:*ss* } [**end** { **at** [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss* | **delay** { **seconds** *second* | *hh*:*mm*:*ss* } | **lifetime** { **seconds** *second* | *hh*:*mm*:*ss* } }] command to start the test instance after a specified delay.

Example

Assign the IP address 10.2.0.70 to the DNS server.

```
<Huawei> system-view
[Huawei] dns server 10.2.0.70
```

Related Topics

8.4.9 display dns server

8.4.20 dns server vpn-instance

Function

The **dns server vpn-instance** command configures the device to send DNS query requests to the DNS server on a specified VPN network.

The **undo dns server vpn-instance** command disables the device from sending DNS query requests to the DNS server on a specified VPN network.

By default, the device can only send DNS query requests to the DNS server on a public network.

Format

dns server vpn-instance *vpn-instance-name*

undo dns server vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance name.	It must be the name of an existing VPN instance.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If an interface on the device and the DNS server have reachable routes to each other and the interface is on a VPN network, the device must use the DNS server on the VPN network for DNS query so that DNS packets can be exchanged properly.

NOTE

If you run this command multiple times, only the latest configuration takes effect.

The device can send DNS query requests to the DNS server on a public network or specified VPN network.

The device can respond to DNS query requests sent by DNS clients on multiple VPN networks.

Example

Configure the device to send DNS query requests to the DNS server on the VPN network **vpn1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] dns server vpn-instance vpn1
```

8.4.21 dns server source-ip

Function

The **dns server source-ip** command configures the source IP address for the device to send and receive DNS packets.

The **undo dns server source-ip** command deletes the source IP address for the device to send and receive DNS packets.

By default, no source IP address is configured for the device.

Format

dns server source-ip *ip-address*

undo dns server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for the device to send and receive DNS packets.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device sends and receives DNS packets, the administrator can specify a source IP address for the device to ensure the communication security. The route from the DNS server to the specified source IP address must be reachable. The DNS server uses the specified source IP address as the destination address and sends a DNS response packet to the local device.

When the device functions as a DNS proxy or relay, run the **dns server source-ip** *ip-address* command to configure the source IP address for communicating with the DNS server.

Precautions

To make the command take effect, pay attention to the following points:

- Ensure that the source IP address is the IP address of an interface or logical interface on the device, and there are reachable routes between the interface and the DNS server.
- Ensure that the source IP address and the IP address of the DNS server are on the same VPN or public network.

Example

Specify source IP address 172.16.1.1 for the local device.

```
<Huawei> system-view
[Huawei] dns server source-ip 172.16.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

8.4.22 dns-server-select-algorithm

Function

The **dns-server-select-algorithm** command configures the DNS server selection mode of the device.

The **undo dns-server-select-algorithm** command restores the default setting.

By default, the device selects a DNS server in **auto** mode.

Format

dns-server-select-algorithm { **fixed** | **auto** }

undo dns-server-select-algorithm

Parameters

Parameter	Description	Value
fixed	Selects a DNS server in **fixed** mode.	-
auto	Selects a DNS server in **auto** mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device can select a DNS server in either of the following modes:

- **auto**: The device uses the internal algorithm to calculate the priorities of all configured DNS servers (IP addresses of DNS servers can be configured by running the **8.4.19 dns server** command), and then sends a DNS query request to the DNS server with the highest priority. If no response is received within a specified period of time, the device retransmits the DNS query request. If the device still does not receive a response from the DNS server after sending query requests multiple times, the device sends the DNS query request to the next server in sequence until it receives a response or has sent to all of the configured DNS servers.
- **fixed**: The device sends a DNS query request to the first DNS server. If no response is received within a specified period of time, the device retransmits the DNS query request. If the device still does not receive a response from the DNS server after sending query requests multiple times, the device sends the

 Copyright © Huawei Technologies Co., Ltd.

DNS query request to the next server in sequence until it receives a response or has sent to all of the configured DNS servers.

NOTE

This function is supported when the device functions as a DNS client or DNS proxy/relay.

When the device functions as a DNS client:

- This function is supported only for DNS query requests sent by IPSec, voice, PKI, or DDNS services.
- The DNS server selection mode is not supported for DNS query requests sent by other services. The device sends the requests according to the order in which DNS servers are configured. If no response is received, the device retransmits the requests according to the order in which DNS servers are configured.

Example

Configure the device to select a DNS server in **fixed** mode.

```
<Huawei> system-view
[Huawei] dns-server-select-algorithm fixed
```

Related Topics

8.4.19 dns server

8.4.23 dns spoofing

Function

The **dns spoofing** command enables DNS spoofing and specifies an IP address in response messages.

The **undo dns spoofing** command disables DNS spoofing.

By default, DNS spoofing is disabled.

Format

dns spoofing *ip-address*

undo dns spoofing

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address in response messages.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the DNS server address or route to the DNS server is not configured on the DNS proxy or relay, you can enable DNS spoofing on the device to spoof a response message with the configured IP address. Currently, DNS spoofing takes effect for only Class-A query (IP address query based on domain names).

If you run the **dns spoofing** command multiple times, only the latest configuration takes effect.

Example

Enable DNS spoofing and specify the IP address in response messages as 10.1.1.1.

```
<Huawei> system-view
[Huawei] dns spoofing 10.1.1.1
```

Disable DNS spoofing.

```
<Huawei> system-view
[Huawei] undo dns spoofing
```

Related Topics

8.4.17 dns relay enable

8.4.15 dns proxy enable

8.4.24 interval (DDNS policy view)

Function

The **interval** command sets the interval for sending DDNS update requests after the DDNS update is enabled.

The **undo interval** command restores the default setting.

By default, the interval for sending DDNS update requests is 3600 seconds.

Format

interval *interval-time*

undo interval

Parameters

Parameter	Description	Value
interval-time	Specifies interval for sending DDNS update requests.	The value is an integer that ranges from 60 to 31536000, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the interval for sending DDNS update requests is set in the configured DDNS policy, the device is triggered to send DDNS update requests at the specified intervals. All the mappings between IP addresses and domain names defined in the DDNS policy are updated.

Precautions

- If you run the **interval** command multiple times, only the latest configuration takes effect.
- Regardless of whether the interval is reached, the device sends DDNS update requests immediately as long as the primary IP address of the corresponding interface changes or the link status of the interface changes from Down to Up.
- If the interval is changed, the device is triggered to send a DDNS update request immediately.
- When a device is connected to the DDNS server supporting www.oray.cn, this command does not take effect and the device initiates a DDNS update request at a fixed interval of 60 seconds.

Example

Set the interval for sending DDNS update requests to 3600 seconds.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] interval 3600
```

8.4.25 ip host

Function

The **ip host** command configures static DNS entries.

The **undo ip host** command deletes static DNS entries.

By default, no static DNS entries are configured.

Format

ip host *host-name ip-address*

undo ip host *host-name* [*ip-address*]

Parameters

Parameter	Description	Value
host-name	Specifies the host name.	The value is a string of 1 to 255 case-sensitive characters without spaces.
ip-address	Specifies the IP address mapping the host name.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A static domain name resolution table is manually set up using the **ip host** command, describing the mappings between host names and IP addresses. In addition, some common host names are added to the table. Then, static host name resolution can be performed according to the static domain name resolution table. When requiring the IP address corresponding to a host name, the client first searches the static host name resolution table for the specified host name and obtains the corresponding IP address. In this manner, the efficiency of host name resolution is improved.

Precautions

The **ip host** command configures a maximum of 50 static DNS entries. Each host name can be mapped to only one IP address. When multiple IP addresses are mapped to a host name, only the latest configuration takes effect.

Example

Configure the IP address 10.110.0.1 for the host test.

```
<Huawei> system-view
[Huawei] ip host test 10.110.0.1
```

Related Topics

8.4.10 display ip host

8.4.26 method (DDNS policy view)

Function

The **method** command sets the update mode for the device functioning as a DDNS client.

The **undo method** command restores the default update mode for the device functioning as a DDNS client.

By default, the update mode is **vendor-specific** for the device functioning as the DDNS client.

Format

method { **ddns** [**both**] | **http** | **vendor-specific** }

undo method

Parameters

Parameter	Description	Value
ddns [**both**]	Indicates that the update mode is ddns (defined by the RFC2136) for the device functioning as a DDNS client. If **both** is specified, both Class-A and PTR query records are updated. If **both** is not specified, only Class-A query records are updated ● Class-A query records: mapping between domain names and IP addresses provided by the DNS server for Class-A query. In Class-A query, an IP address is obtained based on a domain name. ● PTR query records: mapping between domain names and IP addresses provided by the DNS server for PTR query. In PTR query, a domain name is obtained using an IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
http	Indicates that the update mode is http for the device functioning as a DDNS client. After this parameter is specified, the DDNS client can communicate with a common DDNS server through HTTP.	-
vendor-specific	Indicates that the update mode is vendor-specific for the device functioning as a DDNS client. After this parameter is specified, the DDNS client can communicate with the DDNS servers provided at www.3322.org, www.dyndns.com, and www.oray.cn.	-

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

When the device functioning as a DDNS client needs to update the mapping between domain names and IP addresses on the DNS server, the following update modes are supported:

- DDNS update mode (defined by the RFC2136): The DDNS client dynamically updates the mapping between domain names and IP addresses on the DNS server. To configure this mode, specify the **ddns** parameter.
- Update mode implemented through the DDNS server: The DDNS client sends the mapping between domain names and IP addresses to the DDNS server with a specified URL. The DDNS server then informs the DNS server to dynamically update the mapping between domain names and IP addresses. To configure this mode, specify the **http** or **vendor-specific** parameter.
  - To use the Siemens DDNS server or DDNS server provided at www.3322.org, www.dyndns.com, or www.oray.cn, specify the **vendor-specific** parameter.
  - To use an HTTP-based common DDNS server, specify the **http** parameter.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Security risks exist if the update mode for the device functioning as a DDNS client is set to **http** or **vendor-specific**. It is recommended that you set the update mode to **ddns**.

Example

Set the update mode of the device functioning as the DDNS client to DDNS, and update Class-A and PTR query records.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] method ddns both
```

Restore the default update mode for the device functioning as the DDNS client.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] undo method
```

Related Topics

8.4.11 ddns policy

8.4.27 name-server (DDNS policy view)

Function

The **name-server** command configures a DNS server to receive update messages from a DDNS client when the device functions as the DDNS client and the update mode is DDNS.

The **undo name-server** command cancels the DNS server configured for receiving update messages from the DDNS client.

By default, no DNS server is configured to receive update messages from a DDNS client when the device functions as the DDNS client and the update mode is DDNS.

Format

name-server *name-server* [**vpn-instance** *vpn-instance-name*]

undo name-server

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name-server	Specifies the DNS server for receiving update messages from the DDNS client.	The value is a string of 1 to 128 case-sensitive characters without spaces. The value can be a domain name or an IP address.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 characters. The value must be the name of an existing VPN instance.

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DDNS client and the update mode is DDNS, you can run the **name-server** command to configure a DNS server to receive update messages from the DDNS client. After receiving the update request packets, the DNS server updates the mapping between the domain name and IP address of the DDNS client. When deploying a DNS server on a private network, you need to specify the name of the VPN instance to which the DNS server belongs.

Prerequisites

The update mode of the device functioning as a DDNS client has been set to DDNS using the **8.4.26 method (DDNS policy view)** command.

Example

Configure the DNS server with the domain name **ns.huawei.com** to receive update messages from a DDNS client when the device functions as the DDNS client and the update mode is DDNS.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] method ddns
[Huawei-ddns-policy-mypolicy] name-server ns.huawei.com
```

Related Topics

8.4.11 ddns policy

 Copyright © Huawei Technologies Co., Ltd.

8.4.28 reset ddns policy

Function

The **reset ddns policy** command configures the device to update mappings between IP addresses and domain names.

Format

reset ddns policy *policy-name* [**interface** *interface-type interface-num*]

Parameters

Parameter	Description	Value
policy *policy-name*	Specifies the name of a DDNS policy that is to be updated.	The value is a string of 1 to 32 case-sensitive characters without spaces.
interface-type interface-num	Specifies the type and number of the interface to which DDNS policies are bound.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After the **reset ddns policy** command is executed, all mappings between IP addresses and domain names defined in the DDNS policy are updated.

Example

Update the DDNS policy named **dyndns** on GE1/0/0.

```
<Huawei> reset ddns policy dyndns interface gigabitethernet 1/0/0
```

8.4.29 reset dns dynamic-host

Function

The **reset dns dynamic-host** command deletes dynamic DNS entries saved in the domain name cache.

Format

reset dns dynamic-host

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Clear dynamic DNS entries with caution because they cannot be restored after being cleared.

After confirming the action of clearing DNS entries, you can run the **reset** command to clear them.

Example

Clear dynamic DNS entries from the domain name cache.

```
<Huawei> reset dns dynamic-host
```

Related Topics

8.4.6 display dns dynamic-host

8.4.30 reset dns forward table

Function

The **reset dns forward table** command clears the DNS entries forwarded.

Format

reset dns forward table [**source-ip** *ip-address*]

Parameters

Parameter	Description	Value
source-ip *ip-address*	Clear the DNS entries of a specified source IP address.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

When the Router as a DNS proxy or relay is attacked, the DNS table will be full. The **reset dns forward table** command can delete all DNS entries.

Example

Clear DNS entries in the DNS table on the DNS proxy or DNS relay.

```
<Huawei> reset dns forward table
```

Related Topics

8.4.7 display dns forward table

8.4.31 reset dns statistics

Function

The **reset dns statistics** command clears statistics on DNS packets.

Format

reset dns statistics

Parameters

None

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **reset dns statistics** command clears statistics on DNS packets, including the DNS IPv4 and IPv6 addresses. The cleared statistics cannot be restored.

Example

Clear statistics on DNS packets.

```
<Huawei> reset dns statistics
```

8.4.32 ssl-policy (ddns-policy-view)

Function

The **ssl-policy** command binds an SSL policy to a DDNS policy.

The **undo ssl-policy** command deletes an SSL policy from a DDNS policy.

By default, no SSL policy is bound to a DDNS policy.

Format

ssl-policy *policy-name*

undo ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy bound to a DDNS policy.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain a space or question mark (?).

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as the DDNS client and communicates with a Siemens DDNS server, the device needs to encrypt packets using SSL. An SSL policy needs to be bound to the DDNS policy.

Prerequisites

An SSL policy has been created using the **ssl policy** *policy-name* [**type** { **client** | **server** }] command, and PKI domain to be used by the SSL policy has been configured using the **19.18.4 pki-realm** *realm-name* command.

A DDNS policy has been created using the **ddns policy** command and a URL has been configured for Siemens DDNS server using the **url** command.

Precautions

An SSL policy needs to be bound to the DDNS policy only when the device functions as the DDNS client and communicates with a Siemens DDNS server.

Example

Bind an SSL policy to a DDNS policy.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei] ssl policy siemens type client
[Huawei-ssl-policy-siemens] pki-realm abc
[Huawei-ssl-policy-siemens] quit
[Huawei] ddns policy huawei
[Huawei-ddns-policy-huawei] url https://192.168.36.67/nic/update?
group=med&user=huawei_test&password=12345&myip=192.168.19.2
[Huawei-ddns-policy-huawei] ssl-policy siemens
```

Related Topics

8.4.11 ddns policy

8.4.33 url (DDNS policy view)

8.4.33 url (DDNS policy view)

Function

The **url** command specifies the URL in DDNS update requests.

The **undo url** command deletes the URL in DDNS update requests.

By default, no URL is specified in DDNS update requests on the device.

Format

url *request-url* [**username** *username* **password** *password*]

undo url

Parameters

Parameter	Description	Value
request-url	Specifies the URL in DDNS update requests.	The value is a string case-sensitive characters without spaces and ranges from 20 to 256 characters. ● If **username** *username* **password** *password* is not specified, the URL contains the user name and password, and their configurations are displayed in explicit text. For example, when the device uses TCP to communicate with www.oray.cn, the URL format of the DDNS update request is oray://huawei1:huawei2@phddnsdev.oray.net (**huawei1** indicates the user name and **huawei2** indicates the password). ● If **username** *username* **password** *password* is specified, the URL only contains the fixed format <username>:<password>, not the user name and password. The user name and password are specified by **username** and **password**, and the password configuration is displayed in cipher text. For example, when the device uses TCP to communicate with www.oray.cn, the URL format of the

Parameter	Description	Value
		DDNS update request is oray://<username>:<password>@phddnsdev.oray.net (<username>:<password> is the fixed value).
username *username* **password** *password*	Specifies the user name and password for logging in to the DDNS server. **NOTE** To ensure password security, you are advised to run the **username** *username* **password** *password* command to configure a user name and password. The password information in the configuration file is displayed in cipher text.	• *username*: The value is a string of 1 to 32 case-sensitive characters without spaces. • *password*: The value is a string of 1 to 32 case-sensitive characters in explicit text or 48 to 68 case-sensitive characters in cipher text without spaces.

Views

DDNS policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DDNS policy is created, enter the URL and specify a DDNS server in the URL.

The processes for the device to request DDNS updates from different DDNS servers are different; therefore, the URL configurations of DDNS servers are different.

- If **username** *username* **password** *password* is not specified,
  - When the device uses HTTP to communicate with the DDNS server provided at www.3322.org, the URL in a DDNS update request is:

    http://username:password@members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>
  - When the device uses HTTP to communicate with the DDNS server provided at www.dyndns.com, the URL in a DDNS update request is:

http://username:password@update.dyndns.com/nic/update?hostname=<h>&myip=<a>

– When the device uses TCP to communicate with the DDNS server provided at www.oray.cn, the URL in a DDNS update request is:

  oray://username:password@phddnsdev.oray.net

– When the device uses HTTP to communicate with a common DDNS server, the URL in a DDNS update request is:

  http://username:password@merri.s.dnaip.fi/reg/h=<h>&a=<a>

NOTE

In the preceding URLs, *username* and *password* indicate the user name and password for logging in to the DDNS server. For example, in **http://huawei1:huawei2@merri.s.dnaip.fi/reg/h=<h>&a=<a>**, **huawei1** and **huawei2** indicate the user name and password for logging in to the DDNS server.

- When **username** *username* **password** *password* is specified,
  – When the device uses HTTP to communicate with the DDNS server provided at www.3322.org, the URL in a DDNS update request is:

    http://<username>:<password>@members.3322.org/dyndns/update?system=dyndns&hostname=<h>&myip=<a>

  – When the device uses HTTP to communicate with the DDNS server provided at www.dyndns.com, the URL in a DDNS update request is:

    http://<username>:<password>@update.dyndns.com/nic/update?hostname=<h>&myip=<a>

  – When the device uses TCP to communicate with the DDNS server provided at www.oray.cn, the URL in a DDNS update request is:

    oray://<username>:<password>@phddnsdev.oray.net

  – When the device uses HTTP to communicate with a common DDNS server, the URL in a DDNS update request is:

    http://<username>:<password>@merri.s.dnaip.fi/reg/h=<h>&a=<a>

NOTE

In the preceding URLs, <username> and <password> are fixed formats, which cannot be modified.

Where,

- The URL uses the default port number. The default port number of the DDNS server provided at www.oray.cn is 6060, the default HTTP port number is 80 and the default HTTPS port number is 443.
- The FQDN and IP address cannot be specified in the URL for the DDNS server provided at www.oray.cn. You can specify the FQDN when applying a DDNS policy on an interface. The IP address in the URL is the primary IP address of the interface to which a DDNS policy is applied.

NOTE

To prevent configuration errors, you are advised not to change <h> or <a> in the URL. The device automatically fills in <h> and <a> based on the FQDN specified when a DDNS policy is bound to the interface.

If you run the **url** command multiple times, only the latest configuration takes effect.

Precautions

In a URL, the user name and password are separated using :, the password and domain name are separated using @, and the domain name ends with /. Pay attention to the following points when using special characters in a URL.

Example

Specify the URL of the DDNS update request, in which the password is displayed in cipher text.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] url "http://<username>:<password>@members.3322.org/dyndns/
update?system=dyndns&hostname=<h>&ip=<a>" username steven password nevets
```

Delete the specified URL of the DDNS update request.

```
<Huawei> system-view
[Huawei] ddns policy mypolicy
[Huawei-ddns-policy-mypolicy] undo url
```

Related Topics

8.4.3 display ddns policy

8.4.34 dns resolve policy a

Function

The **dns resolve policy a** command enables the DNS resolution policy function for class-A query requests and displays the DNS resolution policy view.

The **undo dns resolve policy a** command disables the DNS resolution policy function for class-A query requests.

By default, the DNS resolution policy function for class-A query requests is disabled.

Format

dns resolve policy a

undo dns resolve policy a

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To control access traffic, the administrator requires that users can access only some websites on which they can browse only texts or pictures. For example, in Wi-Fi connection scenarios such as in metro or on bus, passengers can access only specified websites. If they attempt to access other websites, their access requests are rejected or redirected to the specified websites.

The administrator can run the **dns resolve policy a** command to enable the DNS resolution policy function for class-A query requests. Then only some specified domain names can be resolved to meet the wireless connection requirements.

Follow-up Procedure

Run the **8.4.35 rule (DNS resolution policy view)** command to configure a DNS resolution rule.

Example

Enable the DNS resolution policy function for class-A query requests and display the DNS resolution policy view.

```
<Huawei> system-view
[Huawei] dns resolve policy a
```

8.4.35 rule (DNS resolution policy view)

Function

The **rule** command configures a DNS resolution rule.

The **undo rule** command deletes the DNS resolution rule.

By default, no DNS resolution rule is configured.

Format

rule *rule-id* [**if-match name** *hostname*] { **deny** | **permit** | **spoofing** *ip-address* }

undo rule *rule-id*

Parameters

Parameter	Description	Value
rule-id	Specifies the DNS resolution rule ID. A smaller value indicates a higher rule priority.	The value is an integer that ranges from 0 to 127.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
if-match name *hostname*	Specifies the domain name matching the DNS resolution rule. If this parameter is not configured, the DNS resolution rule matches all domain names.	The value is a string of 1 to 255 case-insensitive characters without spaces. It supports the digits 0-9, letters, and the following symbols: - _ . *. The symbol * indicates the wildcard that can only be prefixed to the domain name once. For example, ***.example.com** indicates that all host names in example.com are matched.
deny	Rejects the domain name resolution request matching the DNS resolution rule.	-
permit	Allows the domain name resolution request matching the DNS resolution rule.	-
spoofing *ip-address*	Specified the IP address of the spoofing response to the domain name resolution request matching the DNS resolution rule. A spoofing response uses the configured IP address as the domain name resolution result to respond to the domain name resolution request. The IP address may be directed to the local homepage (providing resources such as website navigation, local videos, and applications).	The value is in dotted decimal notation.

Views

DNS resolution policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the DNS resolution policy function is enabled, you need to configure a resolution rule in the DNS resolution policy view to implement domain name resolution, resolution prohibition, and spoofing response for a specified domain name.

The administrator can run the **rule** command to configure a specified DNS resolution rule.

Prerequisites

The DNS resolution policy function for class-A query requests has been enabled and the DNS resolution policy view has been displayed using the **dns resolve policy a** command.

Precautions

- If the rule ID specified in *rule-id* already exists, the new rule overwrites the original rule no matter whether the new and original rules conflict with each other.
- If the specified *rule-id* does not exist, create a rule using the specified *rule-id* and determine the rule insertion position based on the rule size.

Example

Add a rule with *rule-id* as 0 to the DNS resolution policy, and configure address spoofing based on the DNS resolution request for www.huawei.com with the spoofing response address 192.168.1.1.

```
<Huawei> system-view
[Huawei] dns resolve policy a
[Huawei-dns-resolve-policy-a] rule 0 if-match name www.huawei.com spoofing 192.168.1.1
```

8.5 NAT Configuration Commands

NOTE

By default, the route forwarding function is enabled on 8FE1GE and 24GE cards. These cards do not send received IP packets to the CPU when the IP packets are forwarded on a LAN card. In this way, NAT services configured on VLANIF interfaces do not take effect.

8.5.1 display firewall-nat session aging-time

Function

The **display firewall-nat session aging-time** command displays the timeout interval of entries in the firewall session table or NAT session table.

Format

display firewall-nat session aging-time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the timeout interval of sessions on the firewall session table or NAT session table.

Example

Display the timeout time of all entries in the session table.

```
<Huawei> display firewall-nat session aging-time
---------------------------------------------
Protocol timeout:
  tcp protocol timeout         : 600    (s)
  tcp-proxy timeout            : 10     (s)
  http protocol timeout        : 120    (s)
  udp protocol timeout         : 120    (s)
  icmp protocol timeout        : 20     (s)
  dns protocol timeout         : 120    (s)
  ftp protocol timeout         : 120    (s)
  ftp-data protocol timeout    : 120    (s)
  rtsp protocol timeout        : 60     (s)
  rtsp-media protocol timeout  : 120    (s)
  sip protocol timeout         : 1800   (s)
  sip-media protocol timeout   : 120    (s)
User-define port timeout:
  tcp protocol port 10001      : 65535 (s)
  tcp protocol port 1          : 111    (s)
  tcp protocol port 4443       : 65535 (s)
  tcp protocol port 181        : 180    (s)
  udp protocol port 180        : 180    (s)
  udp protocol port 182        : 208    (s)
---------------------------------------------
```

Table 8-47 Description of the **display firewall-nat session aging-time** command output

Item	Description
Protocol timeout	Session timeout interval of each protocol.
tcp protocol timeout	Timeout interval of TCP connections. The default value is 600, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
tcp-proxy timeout	Timeout interval of the TCP proxy. The default value is 10, in seconds.
udp protocol timeout	Timeout interval of UDP connections. The default value is 120, in seconds.
icmp protocol timeout	Timeout interval of ICMP connections. The default value is 20, in seconds.
dns protocol timeout	Timeout interval of the DNS protocol. The default value is 120, in seconds.
http protocol timeout	Timeout interval of the HTTP connections. The default value is 120, in seconds.
ftp protocol timeout	Timeout interval of the FTP control connection. The default value is 120, in seconds.
ftp-data protocol timeout	Timeout interval of the FTP connections. The default value is 120, in seconds.
sip protocol timeout	Timeout interval of the SIP protocol. The default value is 1800, in seconds.
sip-media protocol timeout	Timeout interval of the SIP media protocol. The default value is 120, in seconds.
rtsp protocol timeout	Timeout interval of the RTSP protocol. The default value is 60, in seconds.
rtsp-media protocol timeout	Timeout interval of the RTSP media protocol. The default value is 120, in seconds.
User-define port timeout	Timeout interval of a connection with a user-defined port as the destination port.
tcp protocol port *port-number*	Timeout interval of a data connection with a user-defined TCP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.
udp protocol port *port-number*	Timeout interval of a data connection with a user-defined UDP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.

Related Topics

8.5.15 firewall-nat session aging-time

8.5.2 display nat address-group

Function

The **display nat address-group** command displays the configuration of a NAT address pool.

Format

display nat address-group [*group-index*] [**verbose**]

Parameters

Parameter	Description	Value
group-index	Indicates the index of a NAT address pool.	The value must be an existing NAT address pool index.
verbose	Displays details about the NAT address pool.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can check the configuration and application of the NAT address pool.

Example

Display all the NAT address pools.

```
<Huawei> display nat address-group
NAT Address-Group Information:
 --------------------------------------
 Index   Start-address      End-address
 --------------------------------------
 1            10.1.1.1        10.1.1.10
 2         10.10.10.10      10.10.10.15
 --------------------------------------
  Total : 2
```

Display the NAT address pool according to the index of the NAT address pool.

```
<Huawei> display nat address-group 1
 NAT Address-Group Information:
 --------------------------------------
 Index   Start-address      End-address
 --------------------------------------
```

```
1           10.1.1.1        10.1.1.10
--------------------------------------
 Total : 1
```

Display details about the NAT address pool.

```
<Huawei> display nat address-group 1 verbose
NAT Address-Group Information:
 -------------------------------------------------------------
 Index   Start-address      End-address  Ref-times  Ref-type
 -------------------------------------------------------------
 1           10.1.1.1        10.1.1.10          0      ----
 -------------------------------------------------------------
 Total : 1
```

Table 8-48 Description of the display nat address-group command output

Item	Description
NAT Address-Group Information	Information of the NAT address pool.
Index	Index of the NAT address pool.
Start-address	Start IP address of the NAT address pool.
End-address	End IP address of the NAT address pool
Ref-times	Number of times that a NAT address pool is referenced.
Ref-type	Mode in which the NAT address pool is referenced. ● pat: translates the IP address and port information of data packets. ● no-pat: only translates the IP addresses of data packets, not port information. ● ----: indicates that the NAT address pool is not referenced.
Total	Number of NAT address pools.

Related Topics

8.5.16 nat address-group

8.5.3 display nat alg

Function

The **display nat alg** command displays whether NAT application level gateway (ALG) is enabled for an application layer protocol.

Format

display nat alg

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status of NAT ALG.

```
<Huawei> display nat alg
NAT Application Level Gateway Information:
----------------------------------
 Application          Status
----------------------------------
 dns                  Disabled
 ftp                  Disabled
 rtsp                 Enabled
 sip                  Disabled
 pptp                 Disabled
----------------------------------
```

Table 8-49 Description of the display nat alg command output

Item	Description
NAT Application Level Gateway Information	Information of the NAT ALG.
Application	Application protocol type.
Status	Whether the NAT ALG function is enabled.

Related Topics

8.5.17 nat alg

8.5.4 display nat sip cac bandwidth information

Function

The **display nat sip cac bandwidth information** command displays the current total bandwidth and occupied bandwidth on the device.

Format

display nat sip cac bandwidth information [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays details about the current total bandwidth and occupied bandwidth.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display details about the current total bandwidth and occupied bandwidth on the device.

```
<Huawei> display nat sip cac bandwidth information verbose
-------------------------------------------------------------------------------
Total Bandwidth(Kbps)       Used Bandwidth(Kbps)
  3000                        1900
-------------------------------------------------------------------------------
Src-IP          Src-Port Dest-IP         Dest-Port Protocol Used Bandwidth(Kbps)
192.168.0.4     50       1.1.1.1         5060      udp        1900
-------------------------------------------------------------------------------
```

Table 8-50 Description of the display nat sip cac bandwidth information verbose command output

Item	Description
Total Bandwidth	Total bandwidth on the device, in Kbps. To configure the total bandwidth, run the **8.5.18 nat sip cac enable** command.
Used Bandwidth	Occupied bandwidth on the device, in Kbps.
Src-IP	Source IP address, that is, calling-party IP address.
Src-Port	Source port number, that is, calling-party port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dest-IP	Destination IP address, that is, called-party IP address.
Dest-Port	Destination port number, that is, called-party port number.
Protocol	Corresponding protocol of the SIP calling, and the protocol can only be UDP.

Related Topics

8.5.17 nat alg

8.5.18 nat sip cac enable

8.5.5 display nat dns-map

Function

The **display nat dns-map** command displays the configuration of DNS mapping.

Format

display nat dns-map [*domain-name*]

Parameters

Parameter	Description	Value
domain-name	Specifies the valid domain name that can be resolved by the DNS server.	The value is a string of 1 to 255 case-insensitive characters without spaces. The string cannot contain the following characters: / : < > @ \ | % ' ".

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the configuration of NAT DNS mapping.

```
<Huawei> display nat dns-map
 NAT DNS mapping information:
 Domain-name : www.huawei.com
 Global IP   : gigabitethernet0/0/1 (Real IP : 192.168.4.2)
 Global port : 2
 Protocol    : tcp

 Total : 1
```

Table 8-51 Description of the display nat dns-map command output

Item	Description
NAT DNS mapping information	Information of NAT DNS Mapping.
Domain-name	Domain name.
Global IP	IP address provided for external access.
Global port	Port number provided for external access.
Protocol	Type of the protocol carried over IP.
Total	Number of NAT DNS mapping information items.

Related Topics

8.5.19 nat dns-map

8.5.6 display nat filter-mode

Function

The **display nat filter-mode** command displays the current NAT filtering mode.

Format

display nat filter-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the current NAT filtering mode. The modes include:

- endpoint-independent: independent of the external address and port.
- endpoint-dependent: dependent on the external address and independent of the port.
- endpoint-and-port-dependent: dependent on the external address and port.

Example

Display the current NAT filtering mode.

```
<Huawei> display nat filter-mode
Nat filter mode is : endpoint-independent
```

Table 8-52 Description of the display nat dns-map command output

Item	Description
Nat filter mode is	The current NAT filtering mode.

Related Topics

8.5.20 nat filter-mode

8.5.7 display nat outbound

Function

The **display nat outbound** command displays information about outbound NAT.

Format

display nat outbound [**acl** *acl-number* | **address-group** *group-index* | **interface** *interface-type interface-number* [*.subnumber*]]

Parameters

Parameter	Description	Value
acl *acl-number*	Displays the number of a basic ACL or an advanced ACL.	The value must be an existing ACL number.
address-group *group-index*	Displays the index of a NAT address pool.	The value must be an existing address pool index.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number* [*.subnumber*]	Displays the type and number of an interface or a sub-interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all information about outbound NAT.

```
<Huawei> display nat outbound
 NAT Outbound Information:
 ----------------------------------------------------------------------------
 Interface                  Acl     Address-group/IP/Interface      Type
 ----------------------------------------------------------------------------
 GigabitEthernet0/0/2       2000                          1    no-pat
 ----------------------------------------------------------------------------
  Total : 1
```

Table 8-53 Description of the display nat outbound command output

Item	Description
Interface	Name of an interface.
Acl	Basic or advanced ACL that is in use.
Address-group/IP/Interface	The index of a NAT address pool or IP address or loopback interface.
Type	Type of NAT. (If no NAT address pool is specified, the IP address of the interface is used as the translated IP address. That is, Easy IP is used.)
Total	Number of outbound NAT information items.

Related Topics

8.5.24 nat outbound

8.5.8 display nat overlap-address

Function

The **display nat overlap-address** command displays information about the mapping between the overlapped address pool and the temporary address pool.

Format

display nat overlap-address { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }

Parameters

Parameter	Description	Value
map-index	Specifies the index of the mapping between the overlapped address pool and the temporary address pool.	The value must be an existing mapping index.
all	Displays the configuration of all the overlapped address pools.	-
inside-vpn-instance *inside-vpn-instance-name*	Displays the VPN instance of the private network.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the configuration of all the overlapped address pools.

```
<Huawei> display nat overlap-address all
Nat Overlap Address Pool To Temp Address Pool Map Information:
 -------------------------------------------------------------------------------
 Id  Overlap-Address  Temp-Address    Pool-Length        Inside-VPN-Instance-Name
 -------------------------------------------------------------------------------
 1   10.2.2.2         10.3.10.10      255                        cmml
```

```
-----------------------------------------------------------------------------
Total : 1
```

Table 8-54 Description of the display nat overlap-address command output

Item	Description
Id	Index of the mapping between the overlapped address pool and the temporary address pool.
Overlap-Address	Start IP address of the overlapped address pool.
Temp-Address	Start IP address of the temporary address pool.
Pool-Length	Length of the address pool.
Inside-VPN-Instance-Name	Name of the VPN instance of the private network.

Related Topics

8.5.26 nat overlap-address

8.5.9 display nat server

Function

The **display nat server** command displays the configuration of the NAT server.

Format

display nat server [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* [*.subnumber*] | **acl** *acl-number*]

Parameters

Parameter	Description	Value
global *global-address*	Indicates the public address of the NAT server.	The value is in dotted decimal notation.
inside *host-address*	Indicates the private address of the NAT server.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the VPN instance name.	The value is a string of 1 to 31 characters.
interface *interface-type interface-number* [*.subnumber*]	Indicates the type and number of an interface or a sub-interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl *acl-number*	Indicates the number of an ACL.	The value is an integer that ranges from 2000 to 3999.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check whether the NAT server is configured correctly.

Example

Display the configuration of all NAT servers.

```
<Huawei> display nat server
    Nat Server Information:
    Interface  : GigabitEthernet1/0/0
    Global IP/Port     : 1.1.1.1/1~2
    Inside IP/Port     : 10.10.10.2~10.10.10.3/1
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Description : ----

  Total :    1
```

Table 8-55 Description of the display nat server command output

Item	Description
Nat Server Information	Information of Nat Server.
Interface	Name of an interface.
Global IP/Port	Public IP address and port number.
Inside IP/Port	Private IP address and port number.
Protocol	Protocol number and protocol type.
VPN instance-name	Name of the VPN instance.
Acl number	Number of the ACL in the NAT server.
Vrrp id	VRRP ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Description	NAT description.
Total	Number of NAT servers.

Related Topics

8.5.27 nat server

8.5.10 display nat session

Function

The **display nat session** command displays the NAT mapping table.

Format

display nat session { **all** [**verbose**] | **number** }

display nat session protocol { *protocol-name* | *protocol-number* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display nat session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display nat session destination *destination-address* [*destination-port*] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all entries in the NAT mapping table.	-
verbose	Displays detailed information about the NAT mapping table.	-
number	Displays the number of entries in the NAT mapping table.	-
protocol { *protocol-name* | *protocol-number* }	Displays the NAT mapping table with a specified protocol type or port number.	• The value of *protocol-name* can be icmp, tcp, or udp. • The value of *protocol-number* is an integer that ranges from 1 to 255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source *source-address* [*source-port*]	Specifies the source IP address and port number before the NAT translation.	• *source-address*: The value is in dotted decimal notation. • *source-port*: The value is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Specifies the destination IP address and port number before the NAT translation.	• *destination-address*: The value is in dotted decimal notation. • *destination-port*: The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about the NAT mapping table. You can view information about all entries or display information by specifying keywords. The entries in a NAT mapping table are triggered by service packets. If the device does not receive any service packet, no entry is generated.

Example

Display details about all entries in the NAT mapping table.

```
<Huawei> display nat session all verbose
 NAT Session Table Information:

    Protocol          : TCP(6)
    SrcAddr  Port Vpn : 10.200.200.200 65532
    DestAddr Port Vpn : 10.100.100.100 1024
    Time To Live      : 60 s
    NAT-Info
      New SrcAddr     : 10.10.10.10
      New SrcPort     : 10240
      New DestAddr    : 10.30.30.30
      New DestPort    : 21

    Protocol          : UDP(6)
    SrcAddr  Port Vpn : 10.200.200.200 65532
    DestAddr Port Vpn : 10.100.100.100 1024
    Time To Live      : 60 s
    NAT-Info
      New SrcAddr     : 10.10.10.10
```

```
    New SrcPort     : 10240
    New DestAddr    : 10.30.30.3
    New DestPort    : 21

Total : 2
```

Table 8-56 Description of the display nat session all verbose command output

Item	Description
NAT Session Table Information	Information of NAT mapping entries.
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name before the translation.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name before the translation.
Time To Live	Time to live (TTL) of the mapping table entries.
NAT-Info	NAT information.
New SrcAddr	Source address after the translation.
New SrcPort	Source port number after the translation.
New DestAddr	Destination address after the translation.
New DestPort	Destination port number after the translation.
Total	Number of NAT mapping entries.

8.5.11 display nat static

Function

The **display nat static** command displays the configuration of static NAT.

Format

display nat static [**global** *global-address* | **inside** *host-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* [*.subnumber*] | **acl** *acl-number*]

Parameters

Parameter	Description	Value
global *global-address*	Indicates the public address for static NAT.	The value is in dotted decimal notation.

Parameter	Description	Value
inside *host-address*	Indicates the private address for static NAT.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance.	The value is a string of 1 to 31 characters.
interface *interface-type interface-number* [*.subnumber*]	Indicates the type and number of an interface or a sub-interface.	-
acl *acl-number*	Indicates the number of an ACL.	The value is an integer that ranges from 2000 to 3999.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After static NAT is configured, you can use the display nat static command to view the configuration of static NAT.

Example

Display the global configuration of static NAT.

```
<Huawei> display nat static
  Static Nat Information:
  Interface  : GigabitEthernet1/0/0
    Global IP/Port     : 1.1.1.1/1~2
    Inside IP/Port     : 10.2.2.2~10.2.2.3/2
    Protocol : 6(tcp)
    VPN instance-name  : ----
    Acl number         : ----
    Vrrp id            : ----
    Netmask  : 255.255.255.255
    Description : ----

  Total :    1
```

Table 8-57 Description of the display nat static command output

Item	Description
Static Nat Information	Information of Static Nat.
Interface	Name of an interface.

Item	Description
Global IP/Port	Public IP address and port number.
Inside IP/Port	Private IP address and port number.
Protocol	Protocol number and protocol type.
VPN instance-name	Name of the VPN instance.
Acl number	Number of the ACL in the static NAT.
Vrrp id	VRRP ID.
Netmask	Network mask.
Description	NAT description.
Total	Number of static NATs.

Related Topics

8.5.29 nat static (interface view)

8.5.12 display nat static interface enable

Function

The **display nat static interface enable** command displays the interface enabled with the static NAT function.

Format

display nat static interface enable

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the interface enabled with the static NAT function.

```
<Huawei> display nat static interface enable
 Static Nat  enable  Information :
-----------------------------------------------
 interface Vlanif300
-----------------------------------------------
  Total : 1
```

Table 8-58 Description of the display nat static interface enable command output

Item	Description
Static Nat enable Information	Interface enabled with the static NAT function.
Total	Number of interfaces enabled with the static NAT function.

Related Topics

8.5.31 nat static enable

8.5.13 display nat mapping-mode

Function

The **display nat mapping-mode** command displays the NAT mapping mode.

Format

display nat mapping-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After NAT mapping is configured, you can view the NAT mapping information. For example, you can view:

- Endpoint-independent mapping information about TCP packets.
- Endpoint-independent mapping information about UDP packets.
- Endpoint-independent mapping about TCP and UDP packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display NAT mapping information.

```
<Huawei> display nat mapping-mode
  NAT Mapping Mode Information:
-----------------------------------------------------------
nat mapping-mode endpoint-independent tcp
-----------------------------------------------------------
  Total : 1
```

Table 8-59 Description of display nat mapping-mode command output

Item	Description
NAT Mapping Mode Information	Information of the NAT mapping mode.
Total	Number of the NAT mapping mode.

Related Topics

8.5.32 nat mapping-mode

8.5.14 display nat mapping table

Function

The **display nat mapping table** command displays NAT mapping table information or the number of entries in the NAT table.

Format

display nat mapping table { **all** | **number** }

display nat mapping table inside-address *ip-address* **protocol** *protocol-name* **port** *port-number* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
all	Displays information about all entries in the NAT mapping table.	-
number	Displays the number of entries in the NAT mapping table.	-
inside-address *ip-address*	Indicates the internal IP address of the server.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol *protocol-name*	Indicates the protocol type.	The value can be tcp or udp.
port *port-number*	Indicates the protocol port number.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Indicates the VPN instance name.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The display nat mapping table command displays information about all entries in a NAT table or the number of entries in the NAT table. You can also enter keywords to view a specified entry.

Example

Display the number of entries in the NAT table.

```
<Huawei> display nat mapping table number
 The total number of NAT dynamic mapping tables is: 1
```

Display information about all entries in the NAT table.

```
<Huawei> display nat mapping table all
 NAT Dynamic Mapping Table Information:

   Protocol            : UDP(17)
   InsideAddr  Port Vpn : 192.168.1.121   555
   GlobalAddr  Port     : 1.1.1.1         10491

   Protocol            : UDP(17)
   InsideAddr  Port Vpn : 192.168.1.119   555
   GlobalAddr  Port     : 2.2.2.2         23099

  Total : 2
```

Table 8-60 Description of the display nat mapping table command output

Item	Description
The total number of NAT dynamic mapping tables is	Number of NAT mapping tables.

Item	Description
NAT Dynamic Mapping Table Information	Information of NAT mapping tables.
Protocol	Application protocol type.
InsideAddr Port Vpn	Private IP address, port number, and VPN instance name. **NOTE** If no VPN is configured, the VPN instance name is not displayed.
GlobalAddr Port	Public IP address and port number.
Total	Number of NAT mapping tables.

8.5.15 firewall-nat session aging-time

Function

The **firewall-nat session aging-time** command sets the timeout interval of each entry in the session table.

The **undo firewall-nat session aging-time** command restores the default timeout interval of each entry in the session table.

Format

firewall-nat session { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*

undo firewall-nat session { { **all** | **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time**

Parameters

Parameter	Description	Value
dns	Sets the timeout interval of the DNS protocol.	-
ftp	Sets the timeout interval of the FTP control connection.	-
ftp-data	Sets the timeout interval of the FTP connection.	-
http	Sets the timeout interval of the HTTP connection.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp	Sets the timeout interval of the ICMP connection.	-
tcp	Sets the timeout interval of the TCP connection.	-
tcp-proxy	Sets the timeout interval of the TCP proxy.	-
udp	Sets the timeout interval of the UDP connection.	-
sip	Sets the timeout interval of the SIP connection.	-
sip-media	Sets the timeout interval of the SIP media protocol.	-
rtsp	Sets the timeout interval of the RTSP protocol.	-
rtsp-media	Sets the timeout interval of the RTSP media protocol.	-
pptp	Sets the timeout interval of the PPTP control connection.	-
pptp-data	Sets the timeout interval of the PPTP connection.	-
all	Restores the default timeout interval of all the preceding connections.	-
user-define *port-number*	Specifies the user-defined TCP or UDP port number and configures the timeout interval for all data connections with this port as the destination port. **NOTE** This parameter only supports NAT and does not support firewall.	The value is an integer that ranges from 1 to 65535.
aging-time *time-value*	Specifies the timeout interval value.	The value is an integer that ranges from 1 to 65535, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **firewall-nat session aging-time** command sets the timeout interval for sessions of each protocol or port. If an entry in a session table is not used within the specified period, the entry expires. For example, the user with IP address 10.110.10.10 initiates a TCP connection through port 2000. If the TCP connection is not used within the timeout interval, the system deletes the TCP connection.

The default session timeout interval of a port is the same as that of the corresponding protocol. The following table lists the default session timeout interval of each protocol.

Protocol	Default Session Timeout Interval
tcp	600 seconds
tcp-proxy	10 seconds
udp	120 seconds
icmp	20 seconds
dns	120 seconds
http	120 seconds
ftp	120 seconds
ftp-data	120 seconds
sip	1800 seconds
sip-media	120 seconds
rtsp	60 seconds
rtsp-media	120 seconds
pptp	600 seconds
pptp-data	600 seconds

NOTE

When configuring the timeout interval for all sessions with a user-defined port as the destination port, you cannot set the port number to a default port number of the preceding protocols.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

For some services such as voice service, increase the TCP/UDP timeout interval to prevent service interruption.

You can set the session timeout interval for a maximum of 24 ports on the device.

Example

Set the timeout interval of the DNS connection to 60 seconds.

```
<Huawei> system-view
[Huawei] firewall-nat session dns aging-time 60
```

Related Topics

8.5.1 display firewall-nat session aging-time

8.5.16 nat address-group

Function

The **nat address-group** command configures a NAT address pool.

The **undo nat address-group** command deletes a NAT address pool.

By default, no NAT address pool is configured.

Format

nat address-group *group-index start-address end-address*

undo nat address-group *group-index*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-index	Specifies the index of a NAT address pool.	• The value on AR100, AR120, AR150, AR160, AR200 and AR1200 series is an integer that ranges from 0 to 7. • The value on AR2201-48FE, AR2202-48FE, AR2204E, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, and AR2204-51GE-P is an integer that ranges from 0 to 7. • The value on AR2204, AR2220E, AR2220, AR2240, and AR2240C is an integer that ranges from 0 to 255. • The value on AR3200 and AR3600 series is an integer that ranges from 0 to 255.
start-address	Specifies the start address of the address pool.	The value is in dotted decimal notation.
end-address	Specifies the end address of the address pool.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The address pool is a set of consecutive IP addresses. When a packet from the private network reaches the public network through address translation, the

source address of the packet will be translated to another address by the address pool.

Precautions

The start IP address of the address pool must be smaller than or equal to the end IP address of the address pool and up to 255 IP addresses can be configured in the address pool.

Example

Configure an address pool ranging from 10.110.10.10 to 10.110.10.15, with the address pool index being 1.

```
<Huawei> system-view
[Huawei] nat address-group 1 10.110.10.10 10.110.10.15
```

Related Topics

8.5.2 display nat address-group

8.5.17 nat alg

Function

The **nat alg** command enables the NAT ALG function for application protocols.

The **undo nat alg** command disables the NAT ALG function for application protocols.

By default, NAT ALG is disabled.

Format

nat alg { **all** | *protocol-name* } **enable**

undo nat alg { **all** | *protocol-name* } **enable**

Parameters

Parameter	Description	Value
all	Enables the NAT ALG function for DNS, FTP, SIP, PPTP and RTSP.	-
protocol-name	Enables the NAT ALG function for the specified protocol type.	The value can be sippptp and rtsp.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the NAT ALG function is enabled for an application protocol, packets of the application protocol can traverse the public network through NAT. Otherwise, the application protocol cannot work normally.

Example

Enable the NAT ALG function for FTP.

```
<Huawei> system-view
[Huawei] nat alg ftp enable
```

Disable the NAT ALG function for FTP.

```
<Huawei> system-view
[Huawei] undo nat alg ftp enable
```

Related Topics

8.5.13 display nat mapping-mode

8.5.18 nat sip cac enable

Function

The **nat sip cac enable** command enables the function of call admission control and configures the total bandwidth of the device to limit the SIP call bandwidth.

The **undo nat sip cac enable** command disables the function of call admission control and cancels the configuration of total bandwidth. The SIP call bandwidth is not limited.

The default bandwidth of a device is 0, and the call bandwidth is not limited.

Format

nat sip cac enable bandwidth { *bandwidth-value* | **percent** *value* **interface** *interface-type interface-number* [*.subnumber*] }

undo nat sip cac enable

Parameters

Parameter	Description	Value
bandwidth *bandwidth-value*	Specifies the total bandwidth of the device.	The value is an integer that ranges from 1 to 4294967295, in kbit/s.

Parameter	Description	Value
percent *value*	Specifies the total bandwidth on the device, which is a percentage of the bandwidth on SIP outgoing interface.	The value is an integer that ranges from 1 to 100.
interface *interface-type interface-number* [*.subnumber*]	Specifies the SIP outgoing interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* [*.subnumber*] specifies the interface number.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a SIP server is deployed on the public network and SIP phones in public and private networks are interconnected, the call quality is affected if the bandwidth on the NAT device is insufficient. You can enable call admission control (CAC) and set the total bandwidth on the NAT device to limit the bandwidth of SIP calls. If the bandwidth of a SIP exceeds the specified value, the SIP call is rejected.

Example

Set the total bandwidth of the device to 2000 kbit/s to limit the call bandwidth.

```
<Huawei> system-view
[Huawei] nat sip cac enable bandwidth 2000
```

Set the total bandwidth on the device to 10% of the bandwidth on GE1/0/0 to limit the call bandwidth.

```
<Huawei> system-view
[Huawei] nat sip cac enable bandwidth percent 10 interface gigabitethernet 1/0/0
```

Related Topics

8.5.4 display nat sip cac bandwidth information

8.5.19 nat dns-map

Function

The **nat dns-map** command configures a mapping entry from the domain name to the public IP address, port number, and protocol type.

The **undo nat dns-map** command deletes a mapping entry from the domain name to the public IP address, port number, and protocol type.

By default, no mapping entry is configured.

Format

nat dns-map *domain-name* { *global-address* | **interface** *interface-type interface-number* [*.subnumber*] } *global-port protocol-name*

undo nat dns-map *domain-name* { *global-address* | **interface** *interface-type interface-number* [*.subnumber*] } *global-port protocol-name*

Parameters

Parameter	Description	Value
domain-name	Specifies a valid domain name that can be resolved by the DNS server.	The value is a string of 1 to 255 case-insensitive characters without spaces. The domain name of each level contains a maximum of 63 characters. Domain names of different levels are separated by periods (.) and contain a maximum of 255 characters. The string cannot contain the following characters: / : < > @ \ | % ' ".
global-address	Specifies a valid IP address provided for external access.	The value is in dotted decimal notation.
interface *interface-type interface-number* [*.subnumber*]	Specifies the type and number of an interface or a sub-interface.	-
global-port	Specifies the port number of the service provided for external access.	The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol-name	Specifies the protocol carried over IP.	The value can be tcp and udp.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to configure the mapping from the domain name to the public IP address, port number, and protocol type for internal hosts. In this manner, internal hosts can differentiate and access corresponding internal servers according to domain names when no DNS server is deployed on the private network.

By default, DNS mapping is not configured. In this case, after the external DNS server resolves public IP addresses from domain name requests of internal hosts, the internal hosts can be mapped to only one internal server. In addition, internal hosts cannot differentiate and access corresponding internal servers according to domain names.

Follow-up Procedure

Run the **nat alg dns enable** command to enable the DNS NAT ALG function. The NAT ALG function allows hosts on a private network to access servers on the private network through the external DNS server.

Example

Configure a mapping entry from a domain name to public IP address, port number, and protocol type.

```
<Huawei> system-view
[Huawei] nat dns-map www.test.com 10.1.1.1 2012 tcp
```

Related Topics

8.5.5 display nat dns-map

8.5.20 nat filter-mode

Function

The **nat filter-mode** command sets the NAT filtering mode.

The default NAT filtering mode is **endpoint-and-port-dependent**.

Format

nat filter-mode { **endpoint-dependent** | **endpoint-independent** | **endpoint-and-port-dependent** }

Parameters

Parameter	Description	Value
endpoint-dependent	Indicates the NAT filtering mode dependent on the external address and independent of the port.	-
endpoint-independent	Indicates the NAT filtering mode independent of the external address and port.	-
endpoint-and-port-dependent	Indicates the NAT filtering mode dependent on the external address and port.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

NAT filtering allows applications using the STUN and TURN technologies to traverse the NAT server.

NAT is performed on the traffic from the external network to the internal network:

- If the NAT filtering mode is set to endpoint-independent, the system uses "destination IP address+destination port number+protocol number" as the key to search the mapping table. If a corresponding entry is found, the system generates a reverse mapping entry. The destination address and port in the entry are the IP address and port number on the internal network.
- If the NAT filtering mode is set to endpoint-dependent, the system uses "source IP address+destination IP address+destination port number+protocol

number" as the key to search the mapping table. If a corresponding entry is found, the system generates a reverse mapping entry. The behavior in the reverse mapping entry is the same as the behavior in the mapping table entry.

- If the NAT filtering mode is set to endpoint-and-port-dependent, the system uses "source IP address+source port number+destination IP address +destination port number+protocol number" as the key to search the mapping table. If a corresponding entry is found, the system generates a reverse mapping entry. The behavior in the reverse mapping entry is the same as the behavior in the mapping table entry.

You can change the NAT filtering mode only when no traffic is transmitted between the external network and internal network.

Example

Set the NAT filtering mode independent of the external address and port.

```
<Huawei> system-view
[Huawei] nat filter-mode endpoint-independent
```

Related Topics

8.5.6 display nat filter-mode

8.5.21 nat inside priority enable

Function

The **nat inside priority enable** command enables the NAT service to have a higher priority than routing service.

The **undo nat inside priority enable** command disables the NAT service priority function and restores the priority of routing service.

By default, the routing service has a higher priority.

Format

nat inside priority enable

undo nat inside priority enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

You can run this command to specify whether the NAT service or routing service has a higher priority. If the NAT service has a higher priority, NAT is performed for traffic entering the device before routing. If the routing service has a higher priority, traffic is routed before NAT. This function is applicable to multi-uplink scenarios. For example, in a dual-uplink scenario, when you run the **nat static** command in the interface view or **nat static** in the system view on the master device to configure a static mapping between a public IP address and a private IP address, a user network route (UNR) is generated. When you run the **ip route-static** command in the system view, a static route from the public IP address to the private IP address is configured. By running the preceding two commands, you expect that NAT can be performed on traffic entering the device and a backup route is available. A static route has a higher priority than that of the UNR. Therefore, the static route that is configured later overwrites the UNR, and NAT and route backup cannot be implemented on the device at the same time. To resolve this problem, run the **nat inside priority enable** command to enable the NAT service to take precedence over the routing service so that the device performs NAT on traffic before routing it.

Prerequisites

The static mapping from the private IP address to the public IP address has been configured. Two NAT methods are available to configure the static mapping from a private IP address to a public IP address:

- Run the **nat static (interface view)** command in the interface view to configure the static mapping between a private IP address and a public IP address.
- Run the **nat static (system view)** command in the system view to configure one-to-one NAT between private addresses and public addresses. Then run the **nat static enable** command in the interface view to enable the static NAT function.

Example

Enable the NAT service to have a higher priority than the routing service.

```
<Huawei> system-view
[Huawei] nat inside priority enable
```

8.5.22 nat log-format elog

Function

The **nat log-format elog** command sets the NAT log format to eLog. The logs are generated in the format specified by the eLog server.

The **undo nat log-format elog** command changes the current NAT log format from eLog to a common format.

By default, a common format is used as the NAT log format.

 Copyright © Huawei Technologies Co., Ltd.

Format

nat log-format elog

undo nat log-format elog

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In the scenario where connection between the device and eLog server is required, the device must send log packets in the specified format to the eLog server to establish the connection. You can run the **nat log-format elog** or **undo nat log-format elog** command to set the log format to eLog or a common format.

Example

Set the NAT session log format to eLog.

```
<Huawei> system-view
[Huawei] nat log-format elog
```

Set the NAT session log format to a common format.

```
<Huawei> system-view
[Huawei] undo nat log-format elog
```

Related Topics

19.8.55 firewall log session nat enable

8.5.23 nat miss forward deny

Function

The **nat miss forward deny** command enables a device to discard the packets that do not match the ACL rules bound to NAT.

The **undo nat miss forward deny** command disables a device from discarding the packets that do not match the ACL rules bound to NAT.

By default, the function of discarding the packets that do not match the ACL rules bound to NAT is disabled on a device.

Format

nat miss forward deny

 Copyright © Huawei Technologies Co., Ltd.

undo nat miss forward deny

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an ACL is associated with an NAT address pool, the device translates the source address of a data packet matching the ACL into an IP address in the NAT address pool. You can run the **nat miss forward deny** command to enable the function of discarding the packets that do not match the ACL rules bound to NAT.

After this command is run, packets are discarded if the number of session entries exceeds the upper limit.

Example

Enable the device to discard the packets that do not match the ACL rules bound to NAT.

```
<Huawei> system-view
[Huawei] nat miss forward deny
```

8.5.24 nat outbound

Function

The **nat outbound** command associates an ACL with a NAT address pool. In this manner, the addresses specified in the ACL can be translated using the NAT address pool.

The **undo nat outbound** command disables outbound NAT.

By default, outbound NAT is disabled.

Format

nat outbound *acl-number* **address-group** *group-index* [**no-pat**][**vrrp** *vrrpid*]

undo nat outbound *acl-number* **address-group** *group-index* [**no-pat**][**vrrp** *vrrpid*]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 3999.
address-group *group-index*	Indicates that the NAT address pool is used for address translation. If no NAT address pool is specified, the IP address of the interface is used as the translated IP address. That is, Easy IP is used.	• The value on AR100, AR120, AR150, AR160, AR200 and AR1200 series is an integer that ranges from 0 to 7. • The value on AR2201-48FE, AR2202-48FE, AR2204E, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, and AR2204-51GE-P is an integer that ranges from 0 to 7. • The value on AR2204, AR2220E, AR2220, AR2240, and AR2240C is an integer that ranges from 0 to 255. • The value on AR3200 and AR3600 series is an integer that ranges from 0 to 255.
no-pat	Indicates one-to-one NAT, that is, only the IP address in a datagram is translated and the port number is not translated.	-
vrrp *vrrpid*	Specifies the VRRP ID.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

After an ACL is associated with a NAT address pool, NAT translates the source IP address of a data packet matching the ACL to an IP address in the NAT address pool.

On the same interface, different IP addresses can be translated and associated. This interface usually connects to an ISP network and is the egress of the internal network.

NOTE

This command can only be used on Layer 3 interfaces, except the Loopback, Tunnel-Template, and NULL interfaces.

Precautions

On the Layer 2 interface card of the AR2220, AR2240, AR2240C, AR3200 series, 3600 series, NAT needs to be configured on the VLANIF interface. In this case, run the **set workmode lan-card l3centralize** command in the system view to enable centralized forwarding.

Example

Select the addresses from 1.1.1.1 to 1.1.1.3 to form NAT address pool 1, and configure the hosts in the network segment 10.110.10.0/24 to use the addresses in address pool 1 for many-to-one address translation (using TCP/UDP port information).

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] nat address-group 1 1.1.1.1 1.1.1.3
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat outbound 2001 address-group 1
```

Related Topics

8.5.7 display nat outbound

8.5.25 nat outbound (Easy-IP)

Function

The **nat outbound** command configures Easy IP.

The **undo nat outbound** command disables outbound NAT.

By default, Easy IP is disabled.

Format

nat outbound *acl-number* [**interface** *interface-type interface-number* [*.subnumber*]] [**vrrp** *vrrpid*]

undo nat outbound *acl-number* [**interface** *interface-type interface-number* [*.subnumber*]][**vrrp** *vrrpid*]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 3999.
interface *interface-type interface-number* [*.subnumber*]	Indicates that a specified interface address or a sub-interface is specified as the translated address.	-
vrrp *vrrpid*	Specifies the VRRP ID.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Easy IP indicates that the IP address of the interface is used as the translated IP address.

NOTE

This command can only be used on Layer 3 interfaces, except the Loopback, Tunnel-Template, and NULL interfaces.

Only one command can be configured on an interface.

Example

Set the IP address of the interface to the translated IP address.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat outbound 2001
```

Related Topics

8.5.7 display nat outbound

8.5.26 nat overlap-address

Function

The **nat overlap-address** command configures the mapping between an overlapped address pool and a temporary address pool.

The **undo nat overlap-address** command deletes the mapping between an overlapped address pool and a temporary address pool.

By default, the mapping between an overlapped address pool and a temporary address pool is not configured.

Format

nat overlap-address *map-index overlappool-startaddress temppool-startaddress* **pool-length** *length* [**inside-vpn-instance** *inside-vpn-instance-name*]

undo nat overlap-address { *map-index* | **all** | **inside-vpn-instance** *inside-vpn-instance-name* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
map-index	Specifies the index of the mapping between the overlapped address pool and the temporary address pool.	● The value on AR100, AR120, AR150, AR160, AR200 and AR1200 series is an integer that ranges from 0 to 7. ● The value on AR2201-48FE, AR2202-48FE and AR2204 is an integer that ranges from 0 to 7. ● The value on AR2220E and AR2220 is an integer that ranges from 0 to 15. ● The value on AR2204XE and AR2204XE-DC is an integer that ranges from 0 to 31. ● The value on the AR2240 and AR3200 varies according to the SRU model: – SRU40 and SRU60: 0-15. – SRU80, SRU100, SRU100E, SRU200, SRU200E and SRU400: 0-31. ● The value on AR3600 is an integer that ranges from 0 to 31.
overlappool-startaddress	Specifies the start address of the overlapped address pool. IP addresses of overlapped address pools must be different.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
temppool-startaddress	Specifies the start address of the temporary address pool. IP addresses of temporary address pools must be different.	The value is in dotted decimal notation.
pool-length *length*	Indicates the length of the address pool. The lengths of the overlapped address pool and the temporary address pool are the same and an address in the overlapped address pool maps an address in the temporary address pool.	The value is an integer that ranges from 1 to 255.
all	The configuration of all the overlapped address pools.	-
inside-vpn-instance *inside-vpn-instance-name*	Indicates the VPN instance of the private network.	The value is a string of 1 to 31 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When IP addresses of internal hosts and external hosts are overlapped, you need to configure the mapping between the overlapped address pool and the temporary address pool. After the mapping is configured, the overlapped address is translated into a unique temporary address. The packets can be forwarded correctly. In addition, you need to configure outbound NAT to implement twice NAT.

Example

Configure the mapping between an overlapped address pool and a temporary address pool with the index being 1. The length of the overlapped address pool is 255, the overlapped address pool belongs to the VPN **huawei**, and the start

address of the overlapped address pool is 10.10.10.1. The start address of the temporary address pool is 10.100.100.1.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] route-distinguisher 200:1
[Huawei-vpn-instance-huawei-af-ipv4]  quit
[Huawei-vpn-instance-huawei] quit
[Huawei] nat overlap-address 1 10.10.10.1 10.100.100.1 pool-length 255 inside-vpn-instance huawei
```

Related Topics

8.5.8 display nat overlap-address

8.5.27 nat server

Function

The **nat server** command defines a mapping table of internal servers so that external users can access internal servers through address and port translation.

The **undo nat server** command cancels the mapping table.

By default, no mapping table is configured.

Format

nat server protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]

nat server [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**acl** *acl-number*] [**description** *description*]

undo nat server protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*]

undo nat server [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
protocol	Indicates the protocol type.	-

Parameter	Description	Value
protocol-number	Specifies the protocol number.	The value is an integer that ranges from 1 to 255.
global	Configures external information about the NAT server.	-
icmp	Indicates that servers communicate with each other using ICMP.	-
tcp	Indicates that servers communicate with each other using TCP.	-
udp	Indicates that servers communicate with each other using UDP.	-
global-address	Specifies a valid IP address provided for external access.	The value is in dotted decimal notation.
inside	Configures internal information about the NAT server.	-
host-address	Specifies an IP address of the NAT server.	The value is in dotted decimal notation.
host-address2	Specifies the ending IP address of the private network.	The value is in dotted decimal notation.
global-port	Specifies the external service port number. You can use keywords to replace common port numbers. For example, the FTP port number is 21, so you can use the keyword **ftp**. If this parameter is not specified, the value of this parameter is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
global-port2	Specifies the external service ending port number. You can use keywords to replace common port numbers. For example, the FTP port number is 21, so you can use the keyword **ftp**. If this parameter is not specified, the value of this parameter is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.
host-port	Specifies the service port number provided by the NAT server. If this parameter is not specified, the value of this parameter is the same as the value of *global-port*.	The value is an integer that ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a private network-side VPN instance.	The value is a string of 1 to 31 characters.
vrrp *vrrpid*	Specifies the VRRP ID. After NAT address pools are configured on devices in a VRRP group, both devices may perform NAT for packets, resulting in conflicts. You can specify **vrrp** *vrrpid* to configure the master device to perform NAT, preventing conflicts.	The value is an integer that ranges from 1 to 255.
acl *acl-number*	Indicates the number of an ACL.	The value is an integer that ranges from 2000 to 3999.
description *description*	Indicates the NAT description.	The value is a string of 1 to 255 case-sensitive characters. It can contain spaces.
current-interface	Indicates a public address as the current interface address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number* [*.subnumber*]	Indicates a public address as the interface address.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure an internal server so that the external network can access the server in an active manner. When a host on the public network sends a connection request to the public address (global-address) of the internal NAT server, the NAT server translates the destination address of the request into a private address (inside-address). The request is then forwarded to the server on the private network.

NOTE

- This command can only be used on Layer 3 interfaces, except the Loopback, Tunnel-Template, and NULL interfaces.
- When configuring an internal NAT server, ensure that *global-address* and *host-address* are different from IP addresses of ports and IP addresses in the user address pool.
- You can use the IP address of **current-interface** or **loopback** as the internal server's IP address.
- The **undo nat server** command does not delete mapping entries immediately. You can run the **8.5.34 reset nat session** command to delete mapping entries.
- Compared with static NAT, NAT Server translates only the IP address, but not the port number, when the private network initiatively accesses the public network.
- When you configure one-to-one NAT Server that borrows an interface IP address (no interface number is specified and the IP address is mapped to a private network address), other services enabled on the interface may become unavailable. Confirm your action before performing the configuration. If you want to enable other applications on the interface, add an ACL rule after the configuration to filter out the number of the interface on which the applications are enabled.

Precautions

The specified *global-port* or *host-port* cannot be used by other applications. Otherwise, the configuration does not take effect.

When specifying *global-port2* to configure multiple public ports, you must also specify *host-address2* to configure multiple private addresses and ensure that the number of ports is the same as that of private addresses.

If you need to map the private address of an internal server into the IP address of the public network interface when configuring this command on the public

network interface, you must set the **current-interface** parameter to specify a global address as the current interface address.

If you specify **vrrp** *vrrpid* when configuring the **nat server** command on an interface, the interface must support the VRRP function.

The *vpn-instance-name* parameter in the command specifies a private network-side VPN instance and does not take effect on the *global-address* parameter. The **ip binding vpn-instance** *vpn-instance-name* command can be run in the interface view to bind a public network-side VPN instance to the interface.

Example

Add a NAT server and translate public address 1.1.1.1 of the TCP service to private address 192.168.0.1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat server protocol tcp global 1.1.1.1 inside 192.168.0.1
```

Configure NAT server on the public network interface Gigabitethernet 0/0/1 to map TCP port 8080 in the private IP address 192.168.20.2 of an internal server into port 8080 in the IP address of Gigabitethernet 0/0/1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] nat server protocol tcp global current-interface 8080 inside
192.168.20.2 8080
```

Add a NAT server, translate public address 1.1.1.1 of the TCP protocol to private address 192.168.0.1, and only allow users with public address 2.2.2.2 to access the intranet server using IP address 1.1.1.1.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 2.2.2.2 0
[Huawei-acl-basic-2001] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat server protocol tcp global 1.1.1.1 inside 192.168.0.1 acl 2001
```

Related Topics

8.5.9 display nat server
8.5.34 reset nat session

8.5.28 nat session limit

Function

The **nat session limit** command configures the maximum number of NAT mapping entries that can be used by a user.

The **undo nat session limit** command deletes the setting of the maximum number of NAT mapping entries that can be used by a user.

By default, the maximum number of NAT mapping entries that can be used by a user is not configured.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only V200R010C10 and later version support this function.

Format

nat session limit *limit-number* **per-ip** [**acl** *acl-number*]

undo nat session limit

Parameters

Parameter	Description	Value
limit-number	Specifies the maximum number of NAT mapping entries that can be used by a user.	The value is an integer ranging from 1 to 65535.
per-ip	Specifies the maximum number of NAT mapping entries that can be used by a user based on the user's source IP address.	-
acl *acl-number*	Specifies the number of an ACL.	The value is an integer ranging from 2000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Usage Scenario

Since terminals are vulnerable to network attacks on a complex network, the terminals under network attacks will occupy a large number of NAT mapping entries on the devices they connected to. Once the NAT mapping entries on the devices are exhausted, other terminals cannot access the Internet because no NAT mapping entry can be allocated to them. In this case, you can run the **nat session limit** command to set the maximum number of NAT mapping entries that can be used by users. When the number of NAT mapping entries created for a user exceeds the configured limit, the device does not generate new NAT mapping entries. As a result, denying the user's Internet access is restricted.

Precautions

- This command cannot be used together with other functions for creating flow tables, such as the firewall, IPS, and SAC. Otherwise, this command may not take effect.
- If an ACL is configured, ACL rule updates do not affect the maximum number of NAT mapping entries that can be used by a user.
- If an ACL is configured and the ACL rule defines **deny**, the number of NAT mapping entries that can be used by a user is not limited.
- The NAT session table created on the device before this command is run is not included in the statistics of NAT mapping entries.
- After an active/standby device switchover is performed, the devices clear the statistics of NAT mapping entries that have been collected before the switchover and re-collects the statistics.

Example

Set the maximum number of NAT mapping entries that can be created for a user's source IP address to 2000.

```
<Huawei> system-view
[Huawei] nat session limit 2000 per-ip
```

8.5.29 nat static (interface view)

Function

The **nat static** command configures the static mapping between a private IP address and a public IP address.

The **undo nat static** command deletes the static mapping between a private IP address and a public IP address.

By default, the static mapping between a private IP address and a public IP address is not configured.

Format

nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-port2*] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]

nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**global-to-inside** | **inside-to-global**] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port global-port2* [**vrrp** *vrrpid*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**acl** *acl-number*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port* [*global-*

port2] [**vrrp** *vrrpid*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**global-to-inside** | **inside-to-global**]

undo nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } [**vrrp** *vrrpid*] **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**global-to-inside** | **inside-to-global**]

undo nat static protocol { **tcp** | **udp** } **global** { *global-address* | **current-interface** | **interface** *interface-type interface-number* [*.subnumber*] } *global-port global-port2* [**vrrp** *vrrpid*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*]

Parameters

Parameter	Parameters	Value
protocol	Indicates the protocol.	-
protocol-number	Specifies a protocol number.	The value is an integer that ranges from 1 to 255.
icmp	Indicates address translation for ICMP packets.	-
tcp	Indicates address translation for TCP packets.	-
udp	Indicates address translation for UDP packets.	-
global	Configures public network information.	-
global-address	Specifies a public IP address.	The value is in dotted decimal notation.
global-port	Specifies the external service port number. If this parameter is not specified, the value of *global-port* is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Parameters	Value
global-port2	Specifies a public end port number. If this parameter is specified, a range of consecutive port numbers are translated. If this parameter is not specified, only the port number *global-port* is translated.	The value is an integer that ranges from 0 to 65535.
inside	Configures private network information.	-
host-address	Specifies a private IP address.	The value is in dotted decimal notation.
host-address2	Specifies a private end IP address. If this parameter is specified, a range of consecutive IP addresses are translated. If this parameter is not specified, only the private IP address *host-address* is translated.	The value is in dotted decimal notation.
host-port	Specifies a service port number provided by private network devices. If this parameter is not specified, the value of *host-port* is the same as the value of *global-port*.	The value is an integer that ranges from 0 to 65535.
host-port2	Specifies a private end port number.	The value is an integer that ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a private network-side VPN instance.	The value must be the name of an existing VPN instance.
vrrp *vrrpid*	Specifies a VRRP ID.	The value is an integer that ranges from 1 to 255.
netmask *mask*	Specifies the network mask for static NAT.	The value ranges from 255.255.255.0 to 255.255.255.255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Parameters	Value
acl *acl-number*	Specifies the number of an ACL. You can use an ACL to control NAT implementation, ensuring that NAT is performed only for data packets that meet rules in the ACL.	The value is an integer that ranges from 2000 to 3999.
global-to-inside	Indicates static NAT in the direction from the public network to the private network. If unidirectional static NAT is not configured, IP addresses are translated in both directions.	-
inside-to-global	Indicates static NAT in the direction from the private network to the public network. If unidirectional static NAT is not configured, IP addresses are translated in both directions.	-
description *description*	Specifies the NAT description.	The value is a string of 1 to 255 case-sensitive characters without question marks (?). It can contain spaces.
current-interface	Specifies a public IP address as the IP address of the current interface.	-
interface *interface-type interface-number* [*.subnumber*]	Specifies a public IP address as the IP address of an interface or sub-interface. ● *interface-type* specifies the interface type. ● *interface-number* [*.subnumber*] specifies the number of the interface or sub-interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If devices on a private network allow access from devices on a public network through a fixed IP address, for example, a private server provides services to public network devices, the public network devices can access the server through a fixed public IP address. You can configure static NAT to translate the private IP address of the private server into the specified public IP address.

If a private server provides services to multiple public network segments, the private IP address of the server needs to be translated into multiple public IP addresses to ensure security. Generally, bidirectional translation between private and public IP addresses is implemented in static NAT. When a private server accesses a public network, the private IP address of the server cannot be translated into multiple public IP addresses. You can configure unidirectional static NAT to solve this problem. When a public network device accesses the private server, multiple public IP addresses are translated into the private IP address of the server using static NAT. When the private server accesses the public network, IP addresses are translated using outbound NAT.

Static NAT also supports IP address translation between network segments, that is, private IP addresses within a specified range and public IP addresses within a specified range can be translated into each other.

Precautions

After the **undo nat static** command is run on the device, static mapping entries on the device will not be cleared immediately. To clear static mapping entries immediately, run the **8.5.34 reset nat session** command.

When the *global-port*, *global-port2*, *host-port*, and *host-port2* parameters are specified to configure mappings between public and private port numbers, the number of public port numbers must be the same as the number of private port numbers and the port numbers must be mapped in sequence. For example, when **nat static protocol tcp global 1.1.1.1 11 20 inside 10.10.10.1 21 30** is configured, the public IP address 1.1.1.1 maps the private IP address 10.10.10.1, and public port numbers 11 to 20 map private port numbers 21 to 30 in sequence.

When *host-address2* is specified, *global-port2* and *host-port* must also be specified. The number of private addresses must be the same as the number of public port numbers. That is, the same public address maps different private addresses, and different public port numbers map the same private port number. For example, when **nat static protocol tcp global 1.1.1.1 11 12 inside 10.10.10.1 10.10.10.2 30** is configured, 1.1.1.1 and public port 11 map 10.10.10.1 and private port 30, and 1.1.1.1 and public port 12 map 10.10.10.2 and private port 30.

 Copyright © Huawei Technologies Co., Ltd.

If you specify **vrrp** *vrrpid* when configuring the **nat static** command on an interface, the interface must support the VRRP function.

The *vpn-instance-name* parameter in the command specifies a private network-side VPN instance and does not take effect on the *global-address* parameter. The **ip binding vpn-instance** *vpn-instance-name* command can be run in the interface view to bind a public network-side VPN instance to the interface.

If you specify *acl-number* when configuring multiple **nat static** commands on an interface, the ACL number specified in the commands must be the same. Otherwise, the configuration fails.

Example

Translate the combination of the public IP address 1.1.1.1 and port 200 in TCP packets to the combination of the private IP address 10.10.10.1 and port 300.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat static protocol tcp global 1.1.1.1 200 inside 10.10.10.1 300
```

Replace the IP address of packets from the VPN **huawei** and on the network segment 10.2.2.2 (24-bit mask) with the IP address on the network segment 10.3.3.3 (24-bit mask).

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei]  quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat static global 10.3.3.3 inside 10.2.2.2 vpn-instance huawei netmask
255.255.255.0
```

Related Topics

8.5.11 display nat static

8.5.34 reset nat session

8.5.30 nat static (system view)

Function

The **nat static** command configures one-to-one NAT between private addresses and public addresses in the system view.

The **undo nat static** command deletes one-to-one NAT configured between private addresses and public addresses in the system view.

By default, no one-to-one NAT is configured.

Format

nat static protocol { **tcp** | **udp** } **global** *global-address global-port* [*global-port2*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-*

address [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **interface loopback** *interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global** *global-address global-port global-port2* **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port global-port2* [**vpn-instance** *vpn-instance-name*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global** *global-address global-port* [*global-port2*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static [**protocol** { *protocol-number* | **icmp** | **tcp** | **udp** }] **global** { *global-address* | **interface loopback** *interface-number* } **inside** *host-address* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global** *global-address global-port global-port2* **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

undo nat static protocol { **tcp** | **udp** } **global interface loopback** *interface-number global-port global-port2* [**vpn-instance** *vpn-instance-name*] **inside** *host-address host-port host-port2* [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

Parameters

Parameter	Description	Value
protocol	Indicates a protocol.	-
protocol-number	Specifies the protocol number.	The value is an integer that ranges from 1 to 255.
global	Configures external address and port number.	-
global-address	Specifies the public IP address for NAT.	The value is in dotted decimal notation.

Parameter	Description	Value
inside	Configures internal address and port number.	-
host-address	Specifies the private IP address for NAT.	The value is in dotted decimal notation.
host-address2	Specifies the ending IP address of the private network.	-
global-port	Specifies the external service port number. If this parameter is not specified, the value of this parameter is 0. That is, any type of service can be provided.	The value is an integer that ranges from 0 to 65535.
global-port2	Specifies the external service ending port number.	The value is an integer that ranges from 0 to 65535.
host-port	Specifies the service port number provided by the server. If this parameter is not specified, the value of this parameter is the same as the value of *global-port*.	The value is an integer that ranges from 0 to 65535.
host-port2	Specifies a private end port number.	The value is an integer that ranges from 0 to 65535.
icmp	Indicates that servers communicate with each other using ICMP.	-
tcp	Indicates that servers communicate with each other using TCP.	-
udp	Indicates that servers communicate with each other using UDP.	-
vpn-instance *vpn-instance-name*	Indicates the VPN instance name.	The value is a string of 1 to 31 characters.
netmask *mask*	Indicates the network mask for static NAT.	The value ranges from 255.255.255.0 to 255.255.255.255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
description *description*	Indicates the NAT description.	The value is a string of 1 to 255 characters. The character string is case sensitive. It can contain spaces but cannot contain the question mark (?).
interface loopback *interface-number*	Indicates a public address as the loopback interface address.	The value is an integer that ranges from 0 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Static NAT indicates that a private address is statically bound to a public address when NAT is performed. The public IP address in static NAT is only used for translation of the unique and fixed private IP address of a host.

Static PAT indicates that a combination of the private address of a host, TCP/UDP protocol number, and internal port number is statically bound to a combination of the public address, TCP/UDP protocol number, and external port number. The public IP address in static PAT can be used for translation of multiple private addresses.

Using static NAT or PAT, hosts on the private network and hosts on the public network can access each other.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If you run the **undo nat static** command, static mapping entries are not immediately deleted. To clear static mapping entries, run the **8.5.34 reset nat session** command.
- When the *global-port*, *global-port2*, *host-port*, and *host-port2* parameters are specified to configure mappings between public and private port numbers, the number of public port numbers must be the same as the number of private port numbers and the port numbers must be mapped in sequence. For example, when **nat static protocol tcp global 1.1.1.1 11 20 inside 10.10.10.1 21 30** is configured, the public IP address 1.1.1.1 maps the private IP address 10.10.10.1, and public port numbers 11 to 20 map private port numbers 21 to 30 in sequence.

  When *host-address2* is specified, *global-port2* and *host-port* must also be specified. The number of private addresses must be the same as the number of public port numbers. That is, the same public address maps different private addresses, and different public port numbers map the same private port number. For example, when **nat static protocol tcp global 1.1.1.1 11 12 inside 10.10.10.1 10.10.10.2 30** is configured, 1.1.1.1 and public port 11 map 10.10.10.1 and private port 30, and 1.1.1.1 and public port 12 map 10.10.10.2 and private port 30.
- **nat static protocol** { **tcp** | **udp** } **global interface loopback** *interface-number global-port* [*global-port2*] [**vpn-instance** *vpn-instance-name*] **inside** *host-address* [*host-address2*] [*host-port*] [**vpn-instance** *vpn-instance-name*] [**netmask** *mask*] [**description** *description*]

  In the command, the first *vpn-instance-name* parameter specifies the VPN instance bound to the loopback interface, and the second *vpn-instance-name* parameter specifies a private network-side VPN instance.
- If the **ip binding vpn-instance** *vpn-instance-name* command is run in the interface view to bind a public network-side VPN instance to the interface, the **nat static** command in the system view does not take effect. In this case, you need to run the **nat static** or **nat server** command in the interface view.

Example

Translate the combination of Loopback 4 interface address and port 43 in TCP packets to private address 192.168.2.55.

```
<Huawei> system-view
[Huawei] interface loopback 4
[Huawei-LoopBack4] ip address 192.168.8.8 24
[Huawei-LoopBack4] quit
[Huawei] nat static protocol tcp global interface loopback 4 43 inside 192.168.2.55 netmask
255.255.255.255
```

Related Topics

8.5.11 display nat static

8.5.34 reset nat session

8.5.31 nat static enable

Function

The **nat static enable** command enables static NAT on an interface.

The **undo nat static enable** command disables static NAT on an interface.

By default, static NAT on an interface is disabled.

Format

nat static enable

undo nat static enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Using the **nat static enable** command, you can enable static NAT on an interface.

NOTE

This command can only be used on Layer 3 interfaces, except loopback and NULL interfaces.

When enabling static NAT on a sub-interface, you must also enable the function on the main interface. Otherwise, the function does not take effect on the sub-interface.

Example

Enable static NAT on an interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] nat static enable
```

Related Topics

8.5.11 display nat static

8.5.32 nat mapping-mode

Function

The **nat mapping-mode** command sets the NAT mapping mode.

The **undo nat mapping-mode** command restores the NAT mapping mode.

The default NAT mapping mode is endpoint-and-port-dependent.

Format

nat mapping-mode endpoint-independent [*protocol-name* [**dest-port** *port-number*]]

undo nat mapping-mode endpoint-independent [*protocol-name* [**dest-port** *port-number*]]

Parameters

Parameter	Description	Value
endpoint-independent	Indicates the endpoint-independent mode.	-
protocol-name	Indicates the protocol type.	The value can be tcp and udp.
dest-port *port-number*	Indicates the destination port. NAT is performed on only the packets of which destination ports are this specified port.	The value is an integer that ranges from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The NAT function resolves the problem of IPv4 address shortage and improves network security. NAT implementation of different vendors may be different, so the applications using the STUN, TURN, and ICE technologies may fail to traverse the NAT devices of these vendors. These technologies are mainly used on the SIP proxy. NAT mapping enables these applications to traverse the NAT devices.

NAT mapping has the following modes:

- Endpoint-independent mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to any external IP address and port.
- Address and port-dependent mapping: The NAT reuses the port mapping for subsequent packets sent from the same internal IP address and port to the same external IP address and port while the mapping is still active.

Example

Enable the endpoint-and-port-independent mapping mode for TCP packets.

```
<Huawei> system-view
[Huawei] nat mapping-mode endpoint-independent tcp
```

Enable the endpoint-and-port-independent mapping mode for TCP and UDP packets.

```
<Huawei> system-view
[Huawei] nat mapping-mode endpoint-independent
```

Related Topics

8.5.13 display nat mapping-mode

8.5.33 port-mapping

Function

The **port-mapping** command configures the mappings between ports and application-layer protocols.

The **undo port-mapping** command deletes the mappings between ports and application-layer protocols.

Format

port-mapping { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*

undo port-mapping { **all** | { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number* }

Parameters

Parameter	Description	Value
all	Deletes the mappings from all ports.	-
dns	Specifies the mapping between the DNS protocol and a port.	-
ftp	Specifies the mapping between the FTP protocol and a port.	-
http	Specifies the mapping between the HTTP protocol and a port.	-
sip	Specifies the mapping between the SIP protocol and a port.	-
rtsp	Specifies the mapping between the RTSP protocol and a port.	-
pptp	Specifies the mapping between the PPTP protocol and a port.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port *port-number*	Specifies the port mapping to a protocol.	The value of *port-number* is an integer that ranges from 1 to 65535.
acl *acl-number*	Specifies the ACL that controls the packets to which port mapping is applied.	The value of *acl-number* is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Port mapping enables a server to provide various application-layer services for external systems through non-well-known ports. For example, the well-known port of the HTTP service is port 80. After port mapping is configured on the firewall, the firewall can use a non-well-known port to provide the HTTP service.

Port mapping reduces attacks to a certain service on the server.

Example

Map the HTTP service to port 10 and apply ACL 2000 to control the packets to which the mapping takes effect.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule  permit
[Huawei-acl-basic-2000] quit
[Huawei] port-mapping http port 10 acl 2000
```

Related Topics

19.8.20 display port-mapping

8.5.34 reset nat session

Function

The **reset nat session** command deletes entries from the NAT mapping table.

Format

reset nat session { **all** | **transit interface** *interface-type interface-number*[*.subnumber*] }

reset nat session protocol { *protocol-name* | *protocol-number* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]]

reset nat session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]]

reset nat session destination *destination-address* [*destination-port*]

NOTE

V200R010C10 and later versions support the **protocol**, **source**, and **destination** parameters.

Parameters

Parameter	Description	Value
all	Deletes all entries from the NAT mapping table.	-
transit	Deletes the entries of traffic passing a specified interface.	-
interface *interface-type interface-number*[*.subnumber*]	Indicates the type and number of an interface or a sub-interface.	-
protocol { *protocol-name* | *protocol-number* }	Deletes the NAT mapping table with a specified protocol type or port number.	• The value of *protocol-name* can be icmp, tcp, or udp. • The value of *protocol-number* is an integer that ranges from 1 to 255.
source *source-address* [*source-port*]	Specifies the source IP address and port number before the NAT translation.	• *source-address*: The value is in dotted decimal notation. • *source-port*: The value is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Specifies the destination IP address and port number before the NAT translation.	• *destination-address*: The value is in dotted decimal notation. • *destination-port*: The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the configurations of **nat alg**, **nat server**, **nat static**, and **nat outbound** are changed, the packets are not forwarded based on new configurations. You can run the **reset nat session** command to make the new configurations take effect. This command can be used to delete all entries or the entries for a specified protocol type or the entries of traffic passing a specified interface from the NAT mapping table.

Precautions

- After this command is used, entries are deleted from the NAT mapping table and the NAT configurations are modified immediately.
- After this command is executed, you must wait at least 10 seconds if you need to run the command again; otherwise, an error message is displayed.
- If all entries are deleted, communication among certain sessions may be affected for a short period.

Example

Delete all entries from the NAT mapping table.

```
<Huawei> system-view
[Huawei] reset nat session all
Warning:The current all NAT sessions will be deleted.
Are you sure to continue?[Y/N] y
```

Delete entries from the NAT mapping table on port GigabitEthernet0/0/1.

```
<Huawei> system-view
[Huawei] reset nat session transit interface gigabitethernet 0/0/1
Warning:The current all NAT sessions transiting GigabitEthernet0/0/1 will be deleted.
Are you sure to continue?[Y/N] y
```

Delete the NAT mapping entries of TCP.

```
<Huawei> system-view
[Huawei] reset nat session protocol tcp
Warning:The current NAT sessions (protocol: tcp) will be deleted.
Are you sure to continue?[Y/N] y
```

Related Topics

8.5.10 display nat session

 Copyright © Huawei Technologies Co., Ltd.

8.5.35 set nat-session self-healing enable

Function

The **set nat-session self-healing enable** command enables the self-healing function on the timer of a NAT module.

The **set nat-session self-healing disable** command disables the self-healing function on the timer of a NAT module.

By default, the self-healing function on the timer of a NAT module is disabled.

Format

set nat-session self-healing enable

set nat-session self-healing disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the running timer of a NAT module is faulty, the NAT service fails and the device cannot work properly. In this case, run the **set nat-session self-healing enable** command. After the self-healing function is enabled on the timer of a NAT module, the usage of the timer can be automatically detected. If the timer is faulty, you can reset the device to rectify the fault and ensure the proper running of the device.

Example

Enable the self-healing function on the timer of a NAT module.

```
<Huawei> system
[Huawei] set nat-session self-healing enable
```

8.5.36 tcp proxy

Function

The **tcp proxy** command enables the TCP proxy function.

The **undo tcp proxy** command disables the TCP proxy function.

By default, the TCP proxy function is disabled on the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

tcp proxy *ip-address port-number* [**acl** *acl-number*]

undo tcp proxy

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address bound to the TCP proxy.	The value is in dotted decimal notation. The IP address can only be a unicast IP address on the local device.
port-number	Specifies the listening port of the TCP proxy.	The value is an integer that ranges from 1024 to 65000. This port number cannot be occupied by other modules.
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999. It is recommended that ACL filtering be performed for the IP address of the TCP connection initiator.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the SIP ALG scenario, if a SIP data packet sent by the SIP client is too large to be sent to the SIP server at a time, the client divides the oversized SIP data packet into multiple small data packets and sends them to the SIP server. In this case, you need to enable the TCP proxy function on the device so that the device reassembles the received small data packets into the original SIP packet, performs NAT, and then forwards the packet to the SIP server.

The device listens to packets based on the specified IP address and port number after the TCP proxy function is enabled, and then sets up a TCP connection with

 Copyright © Huawei Technologies Co., Ltd.

host A that initiates a TCP connection. After successfully setting up the TCP connection, the device proactively sets up a TCP connection with host B which is the destination device of host A, ensuring that hosts A and B can communicate properly.

Precautions

After the TCP proxy function is disabled, the device deletes TCP connections set up with all hosts and the session table saved on the device. Run the **reset nat session all** command to delete all flow table information.

Example

Enable the TCP proxy function.

```
<Huawei> system-view
[Huawei] tcp proxy 10.1.1.1 3333
```

8.5.37 tcp proxy aging-time

Function

The **tcp proxy aging-time** command sets the aging time of a TCP connection set up by the TCP proxy.

The **undo tcp proxy aging-time** command restores the default aging time of a TCP connection set up by the TCP proxy.

By default, the aging time of a TCP connection set up by the TCP proxy is 120 seconds.

Format

tcp proxy aging-time *aging-time*

undo tcp proxy aging-time

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time of a TCP connection set up by the TCP proxy.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In the SIP ALG scenario, if a SIP data packet sent by the SIP client is too large to be sent to the SIP server at a time, the client divides the oversized SIP data packet into multiple small data packets and sends them to the SIP server. In this case, you need to enable the TCP proxy function on the device so that the device reassembles the received small data packets into the original SIP packet, performs NAT, and then forwards the packet to the SIP server.

If the TCP proxy function is enabled, the device exchanges TCP keepalive packets with a host after it sets up a TCP connection with the host. If the device does not receive TCP keepalive packets from the host within the time three times the aging time, it automatically deletes the TCP connection and corresponding session entry.

Example

Set the aging time of a TCP connection set up by the TCP proxy to 240 seconds.

```
<Huawei> system-view
[Huawei] tcp proxy aging-time 240
```

8.6 UDP Helper Configuration Commands

8.6.1 display udp-helper port

Function

The **display udp-helper port** command displays the configured UDP ports to which packets need to be relayed on the device.

Format

display udp-helper port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the configured UDP ports to which packets need to be relayed, run this command. If the UDP helper function is not enabled, this command does not display any information.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the UDP ports to which packets need to be relayed.

```
<Huawei> display udp-helper port
Udp-Port-Number       Description
-------------------------------------------------------------
      1             TCP Port Service Multiplexer
     37             Time
     49             TAC Access Control System
     53             Domain Name Server
     69             Trivial File Transfer Protocol
    137             NETBIOS Name Service
    138             NETBIOS Datagram Service
```

Table 8-61 Description of the display udp-helper port command output

Item	Description
Udp-Port-Number	UDP ports to which packets need to be relayed. UDP ports are classified into the following types: ● Well-known port: The well-known port numbers range from 0 to 1023. These ports are used by standard TCP/UDP protocols. ● Registered port: The registered port numbers range from 1024 to 49151. They are vendor-specific ports. ● Dynamic/Static port: The dynamic or static port numbers range from 49152 to 65535. These ports can be used as required and may conflict on a network. To configure the UDP ports, run the **8.6.5 udp-helper port** command.
Description	UDP port description. For details about port numbers, see RFC1700.

Related Topics

8.6.4 udp-helper enable

8.6.5 udp-helper port

8.6.2 display udp-helper server

Function

The **display udp-helper server** command displays statistics about packets relayed by UDP helper.

Format

display udp-helper server [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about UDP broadcast packets relayed on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays statistics about packets relayed by UDP helper. The statistics help you monitor the UDP helper function.

Example

Display statistics about packets relayed by UDP helper.

```
<Huawei> display udp-helper server
Server-interface          Server-Ip          packet-num
--------------------------------------------------------------------------
GigabitEthernet1/0/0      192.168.2.1            10
GigabitEthernet1/0/0.1    192.168.1.2            25
```

Table 8-62 Description of the display udp-helper server command output

Item	Description
Server-interface	Interface on which packets are relayed by UDP helper. To configure the interface, run the **8.6.6 udp-helper server** command in the interface view.

Item	Description
Server-Ip	Destination server address. To configure the destination server address, run the **8.6.6 udp-helper server** command in the interface view.
packet-num	Number of UDP packets sent to the destination server.

Related Topics

8.6.6 udp-helper server

8.6.3 reset udp-helper packet

Function

The **reset udp-helper packet** command clears statistics about packets relayed by UDP helper.

Format

reset udp-helper packet

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics about packets relayed by UDP helper. Before collecting packet statistics in a certain period, run this command to clear existing statistics first.

NOTICE

UDP helper statistics cannot be restored after being cleared. Exercise caution when you run the **reset udp-helper packet** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics about packets relayed by UDP helper.

```
<Huawei> reset udp-helper packet
Warning: This command will delete the packet statistics of udp-helper.Continue?[Y/N]y
```

Related Topics

8.6.4 udp-helper enable
8.6.5 udp-helper port
8.6.6 udp-helper server
8.6.2 display udp-helper server

8.6.4 udp-helper enable

Function

The **udp-helper enable** command enables the UDP Helper function.

The **undo udp-helper enable** command disables the UDP Helper function.

By default, the UDP Helper function is disabled.

Format

udp-helper enable

undo udp-helper enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts on an enterprise intranet may need to obtain the network configuration or resolve host names by sending UDP broadcast packets to the server. If the host and the server are located in different broadcast domains, broadcast packets cannot reach the server and the host cannot obtain the configuration from the server. The router provides the UDP Helper function to solve this problem. UDP Helper can relay the UDP broadcast packets with specified destination ports. It converts the broadcast packets into unicast packets and sends the unicast packets to the specified destination servers.

 Copyright © Huawei Technologies Co., Ltd.

The packets that can be forwarded by UDP Helper must meet the following requirements:

- The destination MAC address is the broadcast MAC address (ffff-ffff-ffff).
- The destination IP address is the broadcast IP address (255.255.255.255) or a subnet broadcast IP address (for example, 192.168.255.255).
- The Time-to-Live (TTL) is larger than 1.
- The protocol type is UDP.
- The destination port is a specified UDP port.

Precautions

UDP Helper does not relay DHCP packets. That is, the destination port number cannot be 67 or 68. To relay DHCP packets, run the **dhcp select relay** command.

After the UDP Helper function is enabled, the router relays broadcast packets destined for the following UDP ports by default.

Table 8-63 The relation of default UDP port number with UDP Protocol

Protocol	UDP Port Number
Time Service	37
Terminal Access Controller Access Control System (TACACS)	49
Domain Name System (DNS)	53
Trivial File Transfer Protocol (TFTP)	69
NetBIOS Name Service (NetBIOS-NS)	137
NetBIOS Datagram Service (NetBIOS-DS)	138

After UDP Helper is disabled, all specified UDP ports and default ports are canceled.

NOTE

After the UDP Helper function is enabled, the router automatically relays the UDP broadcast packets on six default ports. If you want to relay the packets on only one default port, run the **undo udp-helper port** { **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** } command to disable packet relay on other five ports.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable UDP Helper.

```
<Huawei> system-view
[Huawei] udp-helper enable
```

Related Topics

8.3.28 dhcp select relay

8.6.5 udp-helper port

8.6.6 udp-helper server

8.6.3 reset udp-helper packet

8.6.2 display udp-helper server

8.6.5 udp-helper port

Function

The **udp-helper port** command specifies the UDP ports to which UDP broadcast packets are relayed.

The **undo udp-helper port** command deletes the UDP ports to which packets are relayed.

By default, no UDP port is specified. After UDP helper is enabled, the router relays broadcast packets destined for ports 37, 49, 53, 69, 137, and 138 by default.

Format

udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

Parameters

Parameter	Description	Value
port-number	Specifies the UDP ports to which packets are relayed.	The value is an integer that ranges from 1 to 65535, excluding 67 and 68.
dns	Relays the UDP broadcast packets sent by DNS. The UDP port number is 53.	-
netbios-ds	Relays the UDP broadcast packets sent by NetBIOS-DS. The UDP port number is 138.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
netbios-ns	Relays the UDP broadcast packets sent by NetBIOS-NS. The UDP port number is 137.	-
tacacs	Relays the UDP broadcast packets sent by TACACS. The UDP port number is 49.	-
tftp	Relays the UDP broadcast packets sent by TFTP. The UDP port number is 69.	-
time	Relays the UDP broadcast packets sent by time service. The UDP port number is 37.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After UDP helper is enabled and the UDP ports are specified, the router relays the received UDP broadcast packets destined for the specified ports.

The **udp-helper port** command takes effect globally. That is, if the router is configured to relay packets destined for a UDP port, all the interfaces configured with the destination server address will relay such packets.

Precautions

UDP helper does not relay DHCP packets. That is, the destination port number cannot be 67 or 68. To relay DHCP messages, enable the DHCP relay function.

In addition to the 6 default ports that have UDP Helper enabled, another 10 destination ports can be specified.

Example

Configure the router to relay the broadcast packets destined for UDP port 100.

```
<Huawei> system-view
[Huawei] udp-helper enable
[Huawei] udp-helper port 100
```

Related Topics

8.6.4 udp-helper enable

8.6.6 udp-helper server

8.6.3 reset udp-helper packet

8.6.2 display udp-helper server

8.6.6 udp-helper server

Function

The **udp-helper server** command configures the destination server to which UDP packets are relayed.

The **undo udp-helper server** command deletes the destination server to which UDP packets are relayed.

By default, no destination server is configured for UDP Helper.

Format

udp-helper server *ip-address*

undo udp-helper server [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a destination server. The IP address can be a unicast address or a subnet broadcast address, but cannot be 255.255.255.255. Otherwise, the configuration fails.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If UDP Helper is enabled and the destination server is configured on an interface, when the interface receives the UDP broadcast packets destined for the specified port, it converts the broadcast packets into unicast packets with the destination address *ip-address* and sends them to the specified server.

Prerequisites

The UDP Helper function is enabled by the **8.6.4 udp-helper enable** command.

Precautions

- If multiple destination servers are configured on an interface, the router converts the broadcast packets into unicast packets and sends them to all these servers.
- When specifying the IP address of a destination server, ensure that the router has a reachable route to the network segment where the destination server is located. If no route is reachable, packets cannot be forwarded.
- When the **undo udp-helper server** command is used without parameter specified, all the configured destination servers on the interface are deleted.

Example

Configure destination server 10.1.1.2 on GE1/0/0.

```
<Huawei> system-view
[Huawei] udp-helper enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] udp-helper server 10.1.1.2
```

Related Topics

8.6.4 udp-helper enable

8.6.5 udp-helper port

8.6.3 reset udp-helper packet

8.6.2 display udp-helper server

8.7 IP Performance Configuration Commands

8.7.1 broadcast routing disable

Function

The **broadcast routing disable** command disables routing forwarding of broadcast packets.

The **undo broadcast routing disable** command enables routing forwarding of broadcast packets.

By default, routing forwarding of broadcast packets is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

broadcast routing disable

undo broadcast routing disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A router forwards broadcast packets according to its IP routing table by default. Broadcast packets carry the destination MAC address of FFFF-FFFF-FFFF and a unicast destination IP address. If there are multiple paths from the source device to the destination device, broadcast packets will be forwarded along multiple paths. As a result, multiple copies of packets will reach the destination device. To ensure that the destination device receives only one copy of packets, run the **broadcast routing disable** command. This command will enable routing forwarding of broadcast packets on the routers along only one path.

Example

Disable routing forwarding of broadcast packets.

```
<Huawei> system-view
[Huawei] broadcast routing disable
```

8.7.2 clear ip df

Function

The **clear ip df** command enables an interface to fragment outgoing IP packets.

The **undo clear ip df** command disables an interface from fragmenting outgoing IP packets.

By default, an interface does not fragment outgoing IP packets.

Format

clear ip df

undo clear ip df

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After forcible IP packet fragmentation is enabled on a device, the device sets the Don't Fragment (DF) field to 0 and fragments IP packets that meet the following conditions:

- The value of the DF field in the IP packet header is 1.
- The packet length is larger than the MTU value of the interface that sends the packets.

Example

Enable forcible fragmentation for outgoing packets on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] clear ip df
```

8.7.3 control-packet output car bypass

Function

The **control-packet output car bypass** command configures the control packets generated by the device not to support traffic policing function.

The **undo control-packet output car bypass** command configures the control packets generated by the device to support traffic policing function.

By default, control packets generated by the device do not support traffic policing function.

Format

control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output car bypass**

control-packet all output car bypass

undo control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output car bypass**

undo control-packet all output car bypass

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bgp	Indicates BGP packets.	-
icmp	Indicates ICMP packets.	-
igmp	Indicates IGMP packets.	-
ospf	Indicates OSPF packets.	-
pim	Indicates PIM packets.	-
rip	Indicates RIP packets.	-
snmp	Indicates SNMP packets.	-
ssh	Indicates SSH packets.	-
telnet	Indicates Telnet packets.	-
udp	Indicates UDP packets.	-
ip_address	Indicates IPv4 address.	The value is in dotted decimal notation.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
other-protocols	Indicates other control packets except BGP, ICMP, IGMP, OSPF, PIM, RIP, SNMP, SSH, Telnet, and UDP packets.	-
all	Indicates all control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function of the control packets generated by the device is enabled, you can run the **undo control-packet output car bypass** command to configures control packets generated by the device to support traffic policing function to apply QoS policies to different control packets.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The enhanced forwarding function of the control packets generated by the device has been enabled using the **8.7.29 ip soft-forward enhance enable** command.

Follow-up Procedures

After control packets generated by the device are configured to support traffic policing function, configure QoS policies to process different control packets. For details about traffic policing configuration, see Configuring Traffic Policing in *Huawei AR Series Access Routers Configuration Guide-QoS*.

Precautions

- Configuring control packets generated by the device to support traffic policing function may cause control packets to be discarded and affect user services.
- In versions earlier than V200R005C00, if the **8.7.29 ip soft-forward enhance enable** command has been executed to enable the enhanced forwarding function on the device, the device generates the configuration file of the **undo control-packet all output car bypass** command after the device is upgraded to V200R005C00.
- When **bgp**, **icmp**, **igmp**, **ospf**, **pim**, **rip**, **snmp**, **ssh**, **telnet**, **udp**, and **other-protocols** are specified in the **undo control-packet output car bypass** commands, the device generates a configuration file of the **undo control-packet all output car bypass** command. If the **control-packet output queue bypass** command is then executed to configure a specified type of control packets generated by the device not to support traffic policing function, the device does not generate the configuration file of the **undo control-packet all output car bypass** command but generates the configuration files of the control packets that are configured to support traffic policing function. For example, if BGP packets, ICMP packets, IGMP packets, OSPF packets, PIM packets, RIP packets, SNMP packets, SSH packets, and UDP packets generated by the device are configured not to support traffic policing function, the device generates the configuration files of the **undo control-packet telnet other-protocols output car bypass** commands.

Example

Configure BGP packets generated by the device to support traffic policing function.

```
<Huawei> system-view
[Huawei] undo control-packet bgp output car bypass
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.4 control-packet output filter bypass

Function

The **control-packet output filter bypass** command configures the device not to discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

 Copyright © Huawei Technologies Co., Ltd.

The **undo control-packet output filter bypass** command configures the device to discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

By default, the device does not discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

Format

control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output filter bypass**

control-packet all output filter bypass

undo control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output filter bypass**

undo control-packet all output filter bypass

Parameters

Parameter	Description	Value
bgp	Indicates BGP packets.	-
icmp	Indicates ICMP packets.	-
igmp	Indicates IGMP packets.	-
ospf	Indicates OSPF packets.	-
pim	Indicates PIM packets.	-
rip	Indicates RIP packets.	-
snmp	Indicates SNMP packets.	-
ssh	Indicates SSH packets.	-
telnet	Indicates Telnet packets.	-
udp	Indicates UDP packets.	-
ip_address	Indicates IPv4 address.	The value is in dotted decimal notation.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
other-protocols	Indicates other control packets except BGP, ICMP, IGMP, OSPF, PIM, RIP, SNMP, SSH, Telnet, and UDP packets.	-
all	Indicates all control packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for the control packets generated by the device, the device does not discard the control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action. After the **undo control-packet output filter bypass** command is executed, the device is configured to discard generated control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action and apply QoS policy to the control packets to meet different service requirements.

Prerequisites

The enhanced forwarding function of control packets generated by the device has been enabled using the **8.7.29 ip soft-forward enhance enable** command.

Follow-up Procedures

The packet filter action in the traffic policy or ACL-based simplified traffic policy has been set to deny.

Precautions

- Configuring the device to discard generated control packet when the traffic policy and ACL-based simplified traffic policy contain the deny action may affect user services.
- When **bgp**, **icmp**, **igmp**, **ospf**, **pim**, **rip**, **snmp**, **ssh**, **telnet**, **udp**, and **other-protocols** are specified in the **undo control-packet output filter bypass** commands, the device generates a configuration file of the **undo control-packet all output filter bypass** command. If the **control-packet output filter bypass** command is then executed to configure the device not to discard a specified type of control packets, the device does not generate the configuration file of the **undo control-packet all output filter bypass** command but generates the configuration files of the control packets that the device is configured to discard. For example, if the device is configured not to discard BGP packets, ICMP packets, IGMP packets, OSPF packets, PIM packets, RIP packets, SNMP packets, SSH packets, and UDP packets the device generates the configuration files of the **undo control-packet telnet other-protocols output filter bypass** commands.

Example

Configure the device to discard generated BGP packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] undo control-packet bgp output filter bypass
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.5 control-packet output queue bypass

Function

The **control-packet output queue bypass** command configures the control packets generated by the device not to support QoS queue functions.

The **undo control-packet output queue bypass** command configures the control packets generated by the device to support QoS queue functions.

By default, control packets generated by the device do not support QoS queue functions.

Format

control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output queue bypass**

control-packet all output queue bypass

undo control-packet { **bgp** | **icmp** | **igmp** | **ospf** | **pim** | **rip** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] | **other-protocols** } * **output queue bypass**

undo control-packet all output queue bypass

Parameters

Parameter	Description	Value
bgp	Indicates BGP packets.	-
icmp	Indicates ICMP packets.	-
igmp	Indicates IGMP packets.	-
ospf	Indicates OSPF packets.	-
pim	Indicates PIM packets.	-
rip	Indicates RIP packets.	-
snmp	Indicates SNMP packets.	-
ssh	Indicates SSH packets.	-
telnet	Indicates Telnet packets.	-
udp	Indicates UDP packets.	-
ip_address	Indicates IPv4 address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
other-protocols	Indicates other control packets except BGP, ICMP, IGMP, OSPF, PIM, RIP, SNMP, SSH, Telnet, and UDP packets.	-
all	Indicates all control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function of the control packets generated by the device is enabled, you can run the **undo control-packet output queue bypass** command to configures control packets generated by the device to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance) to apply QoS policies to different control packets.

Prerequisites

The enhanced forwarding function of the control packets generated by the device has been enabled using the **8.7.29 ip soft-forward enhance enable** command.

Follow-up Procedures

After control packets generated by the device are configured to support QoS queue functions, configure QoS policies to process different control packets.

Precautions

- Configuring control packets generated by the device to support QoS queue functions may cause control packets to be discarded and affect user services.
- In versions earlier than V200R005C00, if the **8.7.29 ip soft-forward enhance enable** command has been executed to enable the enhanced forwarding function on the device, the device generates the configuration file of the **undo control-packet all output queue bypass** command after the device is upgraded to V200R005C00.
- When **bgp**, **icmp**, **igmp**, **ospf**, **pim**, **rip**, **snmp**, **ssh**, **telnet**, **udp**, and **other-protocols** are specified in the **undo control-packet output queue bypass**

 Copyright © Huawei Technologies Co., Ltd.

commands, the device generates a configuration file of the **undo control-packet all output queue bypass** command. If the **control-packet output queue bypass** command is then executed to configure a specified type of control packets generated by the device not to support QoS queue functions, the device does not generate the configuration file of the **undo control-packet all output queue bypass** command but generates the configuration files of the control packets that are configured to support QoS queue functions. For example, if BGP packets, ICMP packets, IGMP packets, OSPF packets, PIM packets, RIP packets, SNMP packets, SSH packets, and UDP packets generated by the device are configured not to support QoS queue functions, the device generates the configuration files of the **undo control-packet telnet other-protocols output queue bypass** commands.

Example

Configure BGP packets generated by the device to support QoS queue functions.

```
<Huawei> system-view
[Huawei] undo control-packet bgp output queue bypass
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.6 display forward pie counter

Function

The **display forward pie counter** command displays statistics on packets of the Packet Input Export (PIE) queue.

NOTE

Only the AR169EGW-L, AR169EW, AR161EW, and AR161EW-M1 support this command.

Format

display forward pie counter

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device receives a large number of burst packets, the CPU usage of the device increases sharply. If the number of burst packets is beyond the processing

capacity of the CPU, excess packets are discarded, resulting in packet loss. You can run the **display forward pie counter** command to check whether packet loss occurs in the PIE queue and determine whether the CPU usage has reached the upper limit accordingly.

Example

Display PIE queue packet statistics.

```
<Huawei> display forward pie counter
PIE0: received packets :39                received bytes :2496
      dropped packets :0                  dropped bytes :0
PIE1: received packets :3823330           received bytes :5606902818
      dropped packets :0                  dropped bytes :0
PIE2: received packets :65                received bytes :4518
      dropped packets :0                  dropped bytes :0
PIE3: received packets :200               received bytes :19348
      dropped packets :0                  dropped bytes :0
PIE4: received packets :1308              received bytes :370543
      dropped packets :1                  dropped bytes :152
PIE5: received packets :0                 received bytes :0
      dropped packets :0                  dropped bytes :0
```

Table 8-64 Description of the **display forward pie counter** command output

Item	Description
PIE	PIE queue.
received packets	Number of packets received in the PIE queue.
received bytes	Number of bytes received in the PIE queue.
dropped packets	Number of packets discarded in the PIE queue.
dropped bytes	Number of bytes discarded in the PIE queue.

8.7.7 discard { ra | rr | srr | ts }

Function

The **discard { ra | rr | srr | ts }** command configures the device to discard the packets that contain the route alert option, route record option, source route option, or timestamp option on interfaces.

The **undo discard { ra | rr | srr | ts }** command configures the device to process the packets that contain the route alert option, route record option, source route option, or timestamp option on interfaces.

By default, the packets that contain the route option are not discarded.

Format

discard { ra | rr | srr | ts }

undo discard { ra | rr | srr | ts }

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

IP packets can carry route options including the route alert option (**ra**), route record option (**rr**), source route option (**srr**), and timestamp option (**ts**).

These route options are used to diagnose network paths and temporarily transmit special services. These options, however, may be used by attackers to spy on the network structure for initiating attacks. This degrades network security and device performance. To solve this problem, you can run the **discard { ra | rr | srr | ts }** command to configure the device to discard the IP packets that contain the route options.

NOTE

The **discard { ra | rr | srr | ts }** command only takes effect for the packets on inbound interfaces.

Example

Configure the device to discard the packets that contain the route alert option on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] discard ra
```

8.7.8 display icmp statistics

Function

The **display icmp statistics** command displays ICMP traffic statistics.

Format

display icmp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display ICMP traffic statistics.

```
<Huawei> display icmp statistics
  Input: bad formats          0          bad checksum            0
         echo                10         destination unreachable 0
         source quench        0          redirects               0
         echo reply          25          parameter problem       0
         timestamp request    0          information request      0
         mask requests        0          mask replies            0
         time exceeded        0          timestamp reply         0
         Mping request        0          Mping reply             0
  Output:echo                25          destination unreachable 0
         source quench        0          redirects               0
         echo reply          10          parameter problem       0
         timestamp request    0          information reply       0
         mask requests        0          mask replies            0
         time exceeded        0          timestamp reply         0
         Mping request        0          Mping reply             0
```

Table 8-65 Description of the display icmp statistics command output

Item	Description
Input	Received packets.
Output	Sent packets.
bad formats	Number of packets in incorrect format.
bad checksum	Number of packets with checksum errors.
echo	Number of echo request packets.
destination unreachable	Number of unreachable packets.
source quench	Number of source quench packets.
redirects	Number of redirection packets.
echo reply	Number of echo reply packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
parameter problem	Number of packets with incorrect parameters.
timestamp request	Number of timestamp request packets.
information request	Number of information request packets.
information reply	Number of information reply packets.
mask requests	Number of mask request packets.
mask replies	Number of mask reply packets.
time exceeded	Number of expired packets.
timestamp reply	Number of timestamp reply packets.
Mping request	Number of multicast ping request packets.
Mping reply	Number of multicast ping reply packets.

8.7.9 display ip socket

Function

The **display ip socket** command displays information about the created IPv4 socket.

Format

display ip [**ha**] **socket** [**monitor**] [**task-id** *task-id* **socket-id** *socket-id* | **socket-type** *socket-type*]

Parameters

Parameter	Description	Value
ha	Displays IPv4 socket information on the slave main control board.	-
monitor	Displays information about the socket monitor. Information about the socket monitor is displayed together with information about the socket. If no parameter is specified, this command displays information about all types of sockets.	-
task-id *task-id*	Displays socket information of the task with a specified ID.	The value must be an existing task ID.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
socket-id *socket-id*	Displays information about the socket with a specified ID.	The value must be an existing socket ID.
socket-type *socket-type*	Displays information about a socket of a specified type.	The value is an integer. **Table 8-66** shows the value range.

Table 8-66 Value range of **socket-type** *socket-type*

Value	Description
1	TCP socket
2	UDP socket
3	RAWIP socket
4	RAWLINK socket

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A socket monitor monitors and records each connection. A RawLink also monitors interfaces. The socket monitor records specific protocol events that occur during operations. In addition, it logs information in the disk space.

The socket monitor is similar to a black box of the system. It records specific events that happen during system operations. When the system fails, you can use information recorded by the socket monitor to locate faults.

You can also set the filtering rules, such as the task ID, socket ID, and socket type so that only the information matching the rules is displayed. This reduces information output and helps you locate faults accurately and efficiently.

Example

Display information about the IP socket.

```
<Huawei> display ip socket monitor
SOCK_STREAM:
Task = VTYD(30), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SENDVPNID(23553)
SO_SETKEEPALIVE SO_SETACL,
```

```
socket state = SS_PRIV SS_ASYNC
                        Socket Monitor:
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 cram time = 00H00M00S, lost msg = 0, msg type = 0x00000000;
Nothing else has been captured!
SOCK_DGRAM:
Task = DHCP(54), socketid = 2, Proto = 17,
LA = 0.0.0.0:67, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_BROADCAST SO_REUSEPORT SO_UDPCHECKSUM SO_SENDVPNID(14849),
socket state = SS_PRIV
                        Socket Monitor:
Statistics:
 input packets = 6,recv packets = 6,output packets = 0;
Rcvbuf status:
 cram time = 00H00M00S: full times = 0,dropped packets = 0;
Asyn Que status:
 read = 0, write = 0, connect = 0, close = 0,
 peer close = 0, accept = 0, keep alive down = 0,
 smb input = 0, smb output = 0, smooth over = 0,
 cram time = 00H00M00S, lost msg = 0, msg type = 0x00000000;
```

Table 8-67 Description of the display ip socket command output

Item	Description
SOCK_STREAM	Socket types: ● SOCK_STREAM ● SOCK_DGRAM ● SOCK_RAWLINK ● SOCK_RAWIP
Task = VTYD(30)	Type and ID of the task that invokes the socket. For example, the task named VTYD uses the socket, with the task ID being 30.
socketid = 1	Socket ID.
Proto = 6	Protocol number.
LA = 0.0.0.0:23, FA = 0.0.0.0:0,	● LA: Local address/port number. ● FA: Remote address/port number.
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,	● sndbuf: maximum socket send buffer size. The value is in bytes. ● rcvbuf: maximum socket receive buffer size. The value is in bytes. ● sb_cc: number of sent packets. The value is in bytes and is valid only when TCP caches data packets. ● rb_cc: number of received packets. The value is in bytes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_LINGER SO_REUSEPORT SO_SENDVPNID (23553) SO_SETKEEPALIVE SO_SETACL,	Set socket options: ● SO_DEBUG: indicates that debugging is enabled. ● SO_ACCEPTCONN: indicates that the socket is the server and is responsible for monitoring. ● SO_REUSEADDR: indicates that addresses are overlapped. After the option is set, multiple identical addresses can be bound to an interface. ● SO_KEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up. ● SO_DONTROUTE: indicates that a socket must choose the direct route to the destination when setting up a connection. ● SO_BROADCAST: indicates that an interface can send broadcast packets. ● SO_REUSEPORT: indicates that interfaces are overlapped. After the option is set, multiple identical interfaces can be bound to the local interface. This option is often set on servers. ● SO_UDPCHECKSUM: indicates that the socket calculates the checksum of UDP packets. ● SO_SENDVPNID: indicates an exclusive option for VPNs. ● SO_SETKEEPALIVE: indicates that the keepalive timer starts after a TCP connection is set up. ● SO_SETACL: indicates that an ACL can be configured on the interface. ● SO_USELOOPBACK: indicates that a socket can use a loopback interface to receive or send data. ● SO_LINGER: indicates the time for closing a TCP connection. If the time is not set to 0, a TCP connection is closed after the timer expires. If the time is set to 0, a TCP connection is closed immediately. ● SO_OOBINLINE: indicates out-band data. When receiving data, a socket processes the out-band data first.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• SO_SENDDATAIF: indicates that a socket uses the specified interface to receive or send data. • SO_SENDDATAIF_DONTSETTTL: indicates that a socket uses the specified interface to receive or send data but does not set the TTL value. • SO_SETSRCADDR: indicates that a socket sets the source address of outgoing packets. • SO_SENDBY_IF_NEXTHOP: indicates that a socket sets the outbound interface and next hop address of outgoing packets.
socket state = SS_PRIV SS_ASYNC	Socket status: • SS_NOFDREF: indicates that the socket ID is deleted. • SS_ISCONNECTED: indicates that a TCP connection is set up. • SS_ISCONNECTING: indicates that a TCP connection is being set up. • SS_ISDISCONNECTING: indicates that a TCP connection is being closed. • SS_CANTSENDMORE: indicates that a socket cannot send data. • SS_CANTRCVMORE: indicates that a socket cannot receive data. • SS_RCVMARK: indicates that a socket sets the receiving option in the received packet. • SS_NBIO: indicates that the type of a socket is non-blocking. • SS_ISCONFIRMING: indicates that the upper-layer application will complete processing a connection. • SS_BLOCKING: indicates that congestion occurs during packet receiving and sending. • SS_RECALL: indicates that the message notification method is set by an asynchronous socket. • SS_PRIV: indicates the option transferred from the Unix. The option is invalid in the current socket. • SS_ASYNC: indicates the status identifier of an asynchronous socket.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Asyn Que status	Current asynchronous queue status.
read=0	Number of messages read by the asynchronous queue is 0.
write=0	Number of messages written by the asynchronous queue is 0.
connect=0	Number of connection messages in the asynchronous queue is 0.
close=0	Number of messages about closed connections in the asynchronous queue is 0.
peer close=0	Number of messages about connections closed by the remote end in the asynchronous queue.is 0.
accept=0	Number of messages received by the asynchronous queue is 0.
keep alive down=0	Number of keepalivedown messages in the asynchronous queue is 0.
cram time=00H00M00S	Time for the asynchronous queue to become full is 00:00:00.
lost msg=0	Number of asynchronous messages discarded by the asynchronous queue is 0.
msg type	Current asynchronous message type.
smb input = 0	Number of times of notifying the application layer to read received packets on the backup board.
smb output = 0	Number of times of notifying the application layer to read sent packets on the backup board.
smooth over = 0	Number of times of notifying the application layer that the smoothing is over.

Related Topics

8.7.36 reset ip socket monitor

8.7.10 display ip socket register-port

Function

The **display ip socket register-port** command displays non-well-known port numbers that have been assigned to services on the device.

Format

display ip socket register-port

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

As defined in RFC standards, port numbers larger than 1024 are non-well-known port numbers and can be assigned to desired services, such as NQA and SSH services. However, a non-well-known port number can be assigned to only one service on the same device. If you assign a non-well-known port number to two or more services, this port number takes effect for only the latest configured service. As a result, the other services using this port number will fail.

Before you assign a non-well-known port number to a service, run the **display ip socket register-port** command to check non-well-known port numbers that have been assigned to other services, preventing service failures caused by conflicts of non-well-known port numbers.

Example

Display non-well-known port numbers that have been assigned to services on the device.

```
<Huawei> display ip socket register-port
Port      Task        Type
3232      mdt         UDP4
3503      MPLSFW      UDP4
3784      BFD         UDP4
4784      BFD         UDP4
31009     MPLSFW      UDP4
3232      mdt         UDP6
3503      MPLSFW      UDP6
3784      BFD         UDP6
4784      BFD         UDP6
31009     MPLSFW      UDP6
```

Table 8-68 Description of the **display ip socket register-port** command output

Item	Description
Port	Non-well-known port number that has been assigned to a service.
Task	Name of the task to which a non-well-known port number is assigned.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Port type, including TCP and UDP.

8.7.11 display ip statistics

Function

The **display ip statistics** command displays IP traffic statistics.

Format

display ip statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IP traffic statistics include statistics about received packets (including discarded packets that carry source-route options), sent packets, fragmented packets, and reassembled packets. If a large number of bad protocol and no route fields is displayed in the command output, the device receives a large volume of IP packets of unknown protocol types and IP packets for which no routes can be found. In this situation, the device may be attacked by the connected devices.

Example

Display IP traffic statistics.

```
<Huawei> display ip statistics
  Input:     sum                49617      local                40133
             bad protocol           0      bad format               0
             bad checksum           0      bad options              0
             discard srr            0      discard rr               0
             discard ra             0      discard ts               0
             TTL exceeded           0
  Output:    forwarding             0      local                44518
             dropped                0      no route                 0
  Fragment:  input                  0      output                   0
             dropped                0
             fragmented             0      couldn't fragment        0
  Reassembling:sum                  0      timeouts                 0
```

Table 8-69 Description of the display ip statistics command output

Item	Description
Input	Received packets.
sum	Total number of packets.
local	Number of packets sent to the upper-layer protocol.
bad protocol	Number of received IP packets of unknown protocol types. The protocol field in the IP header cannot be identified by the upper-layer protocol.
bad format	Number of packets in incorrect format.
bad checksum	Number of packets with checksum errors.
bad options	Number of packets with incorrect options.
discard srr	Number of discarded packets with source route options.
discard rr	Indicates the number of packets that are received and then discarded because of record-route options.
discard ra	Indicates the number of packets that are received and then discarded because of alert-route options.
discard ts	Indicates the number of packets that are received and then discarded because of time stamps options.
TTL exceeded	Number of packets discarded because the TTL expires.
Output	Sent packets.
forwarding	Number of forwarded packets.
local	Number of generated packets.
dropped	Number of discarded packets.
no route	Number of packets for which no correct route can be found, including the packets sent and forwarded by the local device.
Fragment	Number of packet fragments.
input	Number of received fragments.
output	Number of sent fragments.
dropped	Number of discarded fragments.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
fragmented	Number of successfully fragmented packets.
couldn't fragment	Number of packets that cannot be fragmented.
Reassembling:sum	Number of successfully reassembled fragments.
timeouts	Number of expired fragments.

Related Topics

5.1.9 display ip interface
8.7.38 reset ip statistics

8.7.12 display load-sharing

Function

The **display load-sharing** command displays the Unequal Cost Multiple Path (UCMP) configuration.

Format

display load-sharing [**vpn-instance** *vpn-instance*] **ip-address** *ip-address mask*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters.
ip-address *ip-address*	Specifies destination IP address of an equal-cost route in the routing table. The destination IP address can be a network segment.	The value is in dotted decimal notation.
mask	Specifies the mask length in the routing table.	The value is an integer that ranges from 0 to 32.

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Check the UCMP configuration.

```
<Huawei> display load-sharing vpn-instance 0 ip-address 3.3.3.3 32

------------------------Load Sharing Information------------------------
ECMP Index is 0
UCMP is Enabled
--------------------------------------------------------------------------
NextHop         BandWidth       State           Interface

40.1.1.2        1000            Active          GE1/0/0

30.1.1.2        2000            Active          Eth-Trunk1
```

Table 8-70 Description of the display load-sharing command output

Item	Description
ECMP Index	ECMP index, maintained by the system.
UCMP is Enabled	The UCMP function is enabled. To enable the UCMP function, run the **8.7.33 load-balance unequal-cost enable** command.
NextHop	IP address of the next hop in the route matching the destination IP address.
BandWidth	Bandwidth of the link involved in UCMP. To set the UCMP bandwidth, run the **8.7.34 load-balance bandwidth** command.
State	UCMP status: ● Active ● Inactive
Interface	Outbound interface in the route matching the destination IP address.

Related Topics

8.7.34 load-balance bandwidth

8.7.33 load-balance unequal-cost enable

 Copyright © Huawei Technologies Co., Ltd.

8.7.13 display network status

Function

Running the **display network status** command, you can check the network status of a device.

Format

display network status { **all** | **tcp** | **udp** | **port** *port-number* }

Parameters

Parameter	Description	Value
all	Displays all the network information.	-
tcp	Displays TCP.	-
udp	Displays UDP.	-
port *port-number*	Specifies the number of an interface.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display network status** command is used to check the network status, such as the running interfaces and services on the network. For example, when you find that an interface is being used by an unknown module during a security scan, run the command to check out the module.

Example

Display the IPv4 RawIP connection status.

```
<Huawei> display network status all
Proto Task/SockId Local Addr&Port          Foreign Addr&Port        State
TCP   VTYD/1      0.0.0.0:23               0.0.0.0:0                Listening
TCP   HTTP/2      0.0.0.0:80               0.0.0.0:0                Listening
TCP   HTTP/1      0.0.0.0:443              0.0.0.0:0                Listening
TCP   VTYD/59     192.168.50.166:23        10.135.19.141:60445      Established
TCP6  VTYD/2      ::->23                   ::->0                    Listening
UDP   AGNT/1      0.0.0.0:161              0.0.0.0:0
UDP   SLAG/1      0.0.0.0:1025             0.0.0.0:0
UDP   RDS /1      0.0.0.0:1812             0.0.0.0:0
UDP6  AGT6/1      ::->161                  ::->0
UDP6  RDS /2      ::->1812                 ::->0
```

Table 8-71 Description of the **display network status** command output

Item	Description
Proto Task/SockId	Protocol Task and Socket ID
Local Addr&Port	Local IP address and Port number
Foreign Addr&Port	Remote IP address and Port number
State	Connection status

8.7.14 display rawip statistics

Function

The **display rawip statistics** command displays RawIP traffic statistics.

Format

display rawip statistics [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed RawIP traffic statistics based on the ICMP, OSPF, RSVP, and Others protocols.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The statistics about RawIP packets include the number of sent RawIP packets and the number of received RawIP packets.

RSVP, OSPF, and ICMP packets are encapsulated into RawIP packets to be sent. During the ping operation, for example, you can run the **display rawip statistics** command to view the number of RawIP packets sent by the local device to check whether the abnormality on the network is caused by abnormal sending and receiving of RawIP packets.

If you want to diagnose problems and monitor information of specific applications, configure **verbose** in the **display rawip statistics** command to

display application-specific RawIP packet statistics. The applications can be ICMP, OSPF, RSVP, and others.

Precautions

The number of packets received by a router includes the number of forwarded packets, packets sent to the upper layer, and discarded packets.

RawIP traffic statistics are collected based on the well-known protocol number. The protocol number is identified by the protocol field in the IP packet header.

- The protocol number of ICMP statistics is 1.
- The protocol number of OSPF statistics is 89.
- The protocol number of RSVP statistics is 46.
- Statistics about packets with other protocol numbers are collected into the Others field.

Example

View the statistics about RawIP packets.

```
<Huawei> display rawip statistics
Received packets:
  dropped packets because the socket buffer is full   : 0
  dropped packets because no matching socket is found : 0

Sent packets:
  dropped packets : 0
```

Table 8-72 Description of the **display rawip statistics** command output

Item	Description
Received packets	Indicates the statistics about received packets.
dropped packets because the socket buffer is full	Indicates the number of RawIP packets that are discarded because the socket buffer is full.
dropped packets because no matching socket is found	Indicates the number of RawIP packets that are discarded because the socket of the receiver does not match with that of the sender.
Sent packets	Indicates the number of sent packets.
dropped packets	Indicates the number of discarded packets.

Display detailed RawIP traffic statistics.

```
<Huawei> display rawip statistics verbose
Received packets:
-------------------------------------------------------------------
Application    Overflow        No Matching
-------------------------------------------------------------------
ICMP           0               0
OSPF           0               0
RSVP           0               0
```

```
Others        0              1
-----------------------------------------------------------------

Sent packets:
-----------------------------------------------------------------
Application    Dropped Packets
-----------------------------------------------------------------
ICMP          0
OSPF          0
RSVP          0
Others        0
-----------------------------------------------------------------
```

Table 8-73 Description of the display rawip statistics verbose command output

Item	Description
Received packets	Statistics on received packets.
Application	Application type.
Overflow	Number of RawIP packets discarded because the Socket buffer is full.
No Matching	Number of RawIP packets discarded because the receiver's Socket is mismatching.
ICMP	ICMP packets.
OSPF	OSPF packets.
RSVP	RSVP packets.
Others	Other types of packets.
Sent packets	Statistics about sent packets.
Dropped Packets	Number of discarded packets.

Related Topics

8.7.39 reset rawip statistics

8.7.15 display tcp statistics

Function

The **display tcp statistics** command displays TCP traffic statistics.

Format

display tcp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays TCP traffic statistics including different types of received and sent packets. For example, duplicate received packets and packets with checksum errors. In addition, connection-related statistics are displayed, for example, times of accepted connections, the number of retransmitted packets, and the number of keepalive packets.

Most of the preceding statistics are expressed in number of packets, and some of them are expressed in number of bytes.

Example

Display TCP traffic statistics.

```
<Huawei> display tcp statistics
Received packets:
    Total: 0
    Total(64bit high-capacity counter): 0
    packets in sequence: 0 (0 bytes)
    window probe packets: 0, window update packets: 0
    checksum error: 0, offset error: 0, short error: 0

    duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets of data after window: 0 (0 bytes)
    packets received after close: 0

    ACK packets: 0 (0 bytes)
    duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
   Total: 0
    Total(64bit high-capacity counter): 0
    urgent packets: 0
    control packets: 0 (including 0 RST)
    window probe packets: 0, window update packets: 0

    data packets: 0 (0 bytes),    data packets retransmitted: 0 (0 bytes)
    ACK-only packets: 0 (0 delayed)

Other information:
   Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
   Keep alive timeout: 0, keep alive probe: 0,     Keep alive timeout, so connections disconnected : 0
   Initiated connections: 0,     accepted connections: 0, established connections: 0
   Closed connections: 0 (    dropped: 0, initiated dropped: 0)
   Packets dropped with MD5 authentication: 0
   Packets permitted with MD5 authentication: 0
   Send Packets permitted with Keychain authentication: 0
   Receive Packets permitted with Keychain authentication: 0
   Receive Packets Dropped with Keychain authentication: 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-74 Description of the display tcp statistics command output

Item	Description
Received packets	Statistics about received packets.
Total	Total number of packets.
Total (64bit high-capacity counter)	Total number of packets, using the 64-bit counter.
packets in sequence (bytes)	Number of bytes in the packets that arrive in order.
window probe packets	Number of window probe packets.
window update packets	Number of window update packets.
checksum error	Number of packets with checksum errors.
offset error	Number of packets with offset errors.
short error	Number of packets whose length is too short.
duplicate packets (bytes)	Number of bytes in the duplicate packets.
partially duplicate packets (bytes)	Number of bytes in partially duplicate packets.
out-of-order packets (bytes)	Number of bytes in the out-of-order packets.
packets of data after window (bytes)	Number of bytes in the packets whose size is greater than the window size.
packets received after close	Number of packets that arrive after a connection is closed.
ACK packets (bytes)	Number of acknowledged packets, in bytes.
duplicate ACK packets	Number of re-acknowledged packets.
too much ACK packets	Number of acknowledged packets with no data sent.
Sent packets	Number of sent packets.
urgent packets	Number of urgent packets.
control packets (RST)	Number of control packets (RST packets).
data packets	Number of data packets.
data packets retransmitted (0 bytes)	Number of bytes in the retransmitted packets.
ACK only packets (delayed)	Number of acknowledged packets that are delayed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Retransmitted timeout	Timeout interval of the retransmission timer.
connections dropped in retransmitted timeout	Number of connections discarded because the number of retransmission times exceeds the threshold.
Keep alive timeout	Timeout interval of the keepalive timer.
keep alive probe	Number of sent keepalive packets.
Keep alive timeout, so connections disconnected	Number of connections discarded because keepalive probe fails.
Initiated connections	Number of initiated connections.
accepted connections	Number of accepted connections.
established connections	Number of established connections.
Closed connections (dropped, initiated dropped)	Number of closed connections (number of discarded packets after a connection is set up or before a connection is set up).
Packets dropped with MD5 authentication	Number of packets that fail to pass MD5 authentication.
Packets permitted with MD5 authentication	Number of packets that pass MD5 authentication.
Send Packets permitted with Keychain authentication	Number of sent packets that carry keychain options.
Receive Packets permitted with Keychain authentication	Number of received packets that pass keychain authentication.
Receive Packets Dropped with Keychain authentication	Number of received packets that fail to pass keychain authentication.

Related Topics

8.7.16 display tcp status

8.7.16 display tcp status

Function

The **display tcp status** command displays current TCP connection status.

Format

display tcp status [[**task-id** *task-id*] [**socket-id** *socket-id*] | [**local-ip** *ip-address*] [**local-port** *local-port-number*] [**remote-ip** *ip-address*] [**remote-port** *remote-port-number*]]

Parameters

Parameter	Description	Value
task-id *task-id*	Displays the TCP connection status of the task with a specified ID.	The value must be an existing task ID.
socket-id *socket-id*	Displays the TCP connection status of the socket with a specified ID.	The value must be an existing socket ID.
local-ip *ip-address*	Displays the TCP connection status of a specified local IP address.	The value is in dotted decimal notation.
local-port *local-port-number*	Displays the TCP connection status of a specified local port ID.	The value must be an existing local port ID.
remote-ip *ip-address*	Displays the TCP connection status a specified remote IP address.	The value is in dotted decimal notation.
remote-port *remote-port-number*	Displays the TCP connection status of a specified remote port ID.	The value must be an existing remote port ID.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The transmission control protocol defined in RFC 793 ensures high reliability of transmission between hosts. TCP provides reliable and connection-oriented services in full duplex mode. Run the **display tcp status** command to monitor the TCP connection status. The following information is displayed.

- ID of the TCP task control block.
- ID of the IPv4 TCP task and socket.
- Local IPv4 address and port ID.

 Copyright © Huawei Technologies Co., Ltd.

- Remote IPv4 address and port ID.
- ID of the VPN instance to which the TCP connection belongs.
- IPv4 TCP connection status.

You can set filtering rules based on the Task ID, socket ID, IP address and port number of the local device, and IP address and port number of the remote device so that only the information matching the rules is displayed. This prevents unnecessary information from being displayed and helps you locate faults accurately and efficiently.

Precautions

The command output is null if there is no TCP connection.

Example

Display the TCP connection status on the local device.

```
<Huawei> display tcp status
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
0a5d560c 30 /1    0.0.0.0:23           0.0.0.0:0             14849 Listening
```

Display the status of the TCP connection originated from the local IP address 0.0.0.0 and port 23.

```
<Huawei> display tcp status local-ip 0.0.0.0 local-port 23
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
0a5d560c 30 /1    0.0.0.0:23           0.0.0.0:0             14849 Listening
```

Display the status of the TCP connection originated from the local IP address 0.0.0.0 and port 24.

```
<Huawei> display tcp status local-ip 0.0.0.0 local-port 24
TCPCB    Tid/Soid Local Add:port       Foreign Add:port      VPNID  State
```

Table 8-75 Description of the display tcp status command output

Field	Description
TCPCB	ID of the TCP task control block.
Tid/Soid	Task ID and socket ID.
Local Add: port	IP address and port number of the local device. If the value of Local Add is 0.0.0.0, TCP connections of all IP addresses are monitored. If the value of port is 0, the TCP connection of all ports is monitored.
Foreign Add: port	IP address and port number of the remote device. If the value of Foreign Add is 0.0.0.0, the TCP connection of all IP addresses is monitored. If the value of port is 0, TCP connections of all ports are monitored.

 Copyright © Huawei Technologies Co., Ltd.

Field	Description
VPNID	ID of the VPN instance to which the TCP connection belongs. ● -1: indicates all VPNs. ● 0: indicates the public VPN. ● Other values: indicates the private VPN. The VPNID is defined by users.
State	TCP connection status: ● Closed: indicates that the TCP connection is closed. ● Listening: indicates that the TCP connection is being monitored. ● Syn_Rcvd: indicates that a packet with the SYN flag is received. ● Established: indicates that the TCP connection has been set up. ● Close_Wait: indicates that a user sends a packet with the FIN flag to the server to close the TCP connection in Established state. The server then sends an ACK packet to the user after receiving the packet and enters the Close_Wait state. ● Fin_Wait1: indicates that a user sends a packet with the FIN flag to the server to close the TCP connection and enter this state. ● Fin_Wait2: indicates that a user receives an ACK packet that responds to the sent packet with the FIN flag. ● Time_Wait: indicates that TCP enters this state after the TCP connection is closed. When TCP has been in Time_Wait state two times the lifetime of the longest packets, records about the closed connection are deleted. ● Closing: indicates that the user and server close the TCP connection simultaneously.

8.7.17 display udp statistics

Function

The **display udp statistics** command displays UDP traffic statistics.

Format

display udp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays UDP traffic statistics including different types of received and sent packets. For example, packets with checksum errors. In addition, connection-related statistics are displayed, for example, the number of broadcast packets. The preceding statistics are expressed in number of packets.

Example

Display UDP traffic statistics.

```
<Huawei> display udp statistics
Received packets:
   Total: 0
   Total(64bit high-capacity counter): 0
   checksum error: 0
   shorter than header: 0
   data length larger than packet: 0
   unicast(no socket on port): 0
   broadcast/multicast(no socket on port): 0
   not delivered, input socket full: 0
   input packets missing pcb cache: 0

Sent packets:
   Total: 0
   Total(64bit high-capacity counter): 0
```

Table 8-76 Description of the display udp statistics command output

Item	Description
Received packet: Total: Total (64bit high-capacity counter):	Total number of received UDP packets. Total number of received UDP packets (using the 64-bit counter).
checksum error:	Number of packets with checksum errors.
shorter than header:	Number of packets whose length is shorter than the packet header.
data length larger than packet:	Number of packets whose data length is greater than the packet length.
unicast (no socket on port):	Number of unicast packets.

Item	Description
broadcast/multicast (no socket on port):	Number of broadcast and multicast packets.
not delivered, input socket full:	Number of packets that are not sent out because the socket buffer is full.
input packets missing pcb cache:	Number of sent packets that are not found in the PCB cache.
Sent packets: Total: Total (64bit high-capacity counter):	Total number of sent UDP packets. Total number of sent UDP packets (using the 64-bit counter).

Related Topics

8.7.41 reset udp statistics

8.7.18 icmp blackhole unreachable send

Function

The **icmp blackhole unreachable send** command enables the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

The **undo icmp blackhole unreachable send** command disables the terminal access from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

By default, the terminal access is disabled from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

Format

icmp blackhole unreachable send

undo icmp blackhole unreachable send

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If static IPv4 blackhole routes are configured on the terminal access and a user goes offline, only the IPv4 blackhole route corresponding to the user's address segment exists on the terminal access. When a tracert packet matches the IPv4 blackhole route, the terminal access discards the packet. As a result, an initiator cannot detect that the user has gone offline.

After you run the **icmp blackhole unreachable send** command, the terminal access sends a Destination Unreachable ICMP packet to an initiator, notifying the initiator that the user has gone offline if a user goes offline and a tracert packet matches the IPv4 blackhole route.

Pre-configuration Tasks

Static IPv4 blackhole routes have been configured on the terminal access.

Example

Enable the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv4 blackhole route.

```
<Huawei> system-view
[Huawei] icmp blackhole unreachable send
```

8.7.19 icmp host-unreachable send

Function

The **icmp host-unreachable send** command enables the device to send ICMP host unreachable packets.

The **undo icmp host-unreachable send** command disables the device from sending ICMP host unreachable packets.

By default, the device can send ICMP host unreachable packets.

Format

icmp host-unreachable send

undo icmp host-unreachable send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After you run the **undo icmp host-unreachable send** command, the device does not send ICMP host unreachable packets externally. This prevents the peer device from processing a large number of ICMP packets.

This command needs to be configured on the inbound interface of ICMP packets.

Example

Enable GE1/0/0 to send ICMP host unreachable packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] icmp host-unreachable send
```

Related Topics

8.7.8 display icmp statistics

8.7.20 icmp port-unreachable send

Function

The **icmp port-unreachable send** command enables the device to send ICMP port unreachable packets.

The **undo icmp port-unreachable send** command disables the device from sending ICMP port unreachable packets.

By default, the device does not send ICMP port unreachable packets.

Format

icmp port-unreachable send

undo icmp port-unreachable send

Parameters

None

Views

System view and Interface view

Default Level

2: Configuration level

Usage Guidelines

After the function of sending ICMP port unreachable packets is disabled, the device does not send ICMP port unreachable packets. This can reduce the number of ICMP packets on the network and reduce the workload on the peer device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the device to send ICMP port unreachable packets.

```
<Huawei> system-view
[Huawei] icmp port-unreachable send
```

8.7.21 icmp time-exceed

Function

The **icmp time-exceed** command specifies the format of ICMP Time Exceeded packets.

The **undo icmp time-exceed** command restores the format of ICMP Time Exceeded packets to the default setting.

By default, ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length.

Format

icmp time-exceed { **extension** { **compliant** | **non-compliant** } | **classic** }

undo icmp time-exceed

Parameters

Parameter	Description	Value
extension	Indicates that ICMP Time Exceeded packets carry extension headers.	-
compliant	Indicates that ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length.	-
non-compliant	Indicates that ICMP Time Exceeded packets carry extension headers in non-compliant mode and original datagrams are of fixed length.	-
classic	Indicates that ICMP Time Exceeded packets do not carry extension headers.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When using the **tracert** command to check the network connectivity, you can run the **icmp time-exceed** command to specify the format of ICMP Time Exceeded packets.

- When the **icmp time-exceed** command carry the parameter **extension compliant**, ICMP Time Exceeded packets carry extension headers in compliant mode and original datagrams are of variable length. ICMP Time Exceeded packets carry as many original datagrams as possible. Lengths of original datagrams carried in ICMP Time Exceeded packets are recorded in ICMP headers.
- When the **icmp time-exceed** command carry the parameter **extension non-compliant**, ICMP Time Exceeded packets carry extension headers in non-compliant mode and original datagrams are of fixed length. If the length of original datagrams is less than 128 bytes, the system automatically fills the length to 128 bytes.
- When the **icmp time-exceed** command carry the parameter **classic**, ICMP Time Exceeded packets do not carry extension headers.

Example

Configure ICMP Time Exceeded packets to carry extension headers in compliant mode.

```
<Huawei> system-view
[Huawei] icmp time-exceed extension compliant
```

Related Topics

21.15.3 tracert

8.7.22 icmp ttl-exceeded drop

Function

The **icmp ttl-exceeded drop** command enables the device to discard the ICMP packets whose TTL values are 1.

The **undo icmp ttl-exceeded drop** command disables the device from discarding the ICMP packets whose TTL values are 1.

By default, the device does not discard the ICMP packets whose TTL values are 1.

Format

icmp ttl-exceeded drop

undo icmp ttl-exceeded drop

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device receives a large number of IGMP packets, the function enables the device to discard some ICMP packets to reduce the workload on the device.

NOTE

After the function is enabled on the device, the **tracert** command does not take effect.

Example

Enable the device to discard the ICMP packets whose TTL values are 1.

```
<Huawei> system-view
[Huawei] icmp ttl-exceeded drop
```

8.7.23 icmp ttl-exceeded send

Function

The **icmp ttl-exceeded send** command enables an interface to send ICMP Time Exceeded messages.

The **undo icmp ttl-exceeded send** command disables an interface from sending ICMP Time Exceeded messages.

By default, an interface is enabled to send ICMP Time Exceeded messages.

Format

icmp ttl-exceeded send

undo icmp ttl-exceeded send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

By default, an interface replies with an ICMP Time Exceeded message after it receives a message with TTL 1. The interface adds its IP address as the source IP address in the ICMP Time Exceeded message, exposing the interface itself to attackers. In addition, after being attacked, the interface replies with numerous ICMP Time Exceeded messages, consuming CPU resources and degrading system performance. To resolve these problems, run the **undo icmp ttl-exceeded send** command to disable the interface from replying with ICMP Time Exceeded messages.

Example

Enable GE1/0/0 from sending ICMP Time Exceeded messages.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] icmp ttl-exceeded send
```

8.7.24 icmp unreachable drop

Function

The **icmp unreachable drop** command enables the function of discarding ICMP destination unreachable packets.

The **undo icmp unreachable drop** command disables the function of discarding the ICMP destination unreachable packets.

By default, the function of discarding ICMP destination unreachable packets is disabled.

Format

icmp unreachable drop

undo icmp unreachable drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the function is enabled on the device, the device discards some ICMP packets. This reduces the workload on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the function of discarding ICMP destination unreachable packets.

```
<Huawei> system-view
[Huawei] icmp unreachable drop
```

8.7.25 icmp with-options drop

Function

The **icmp with-options drop** command enables the device to discard ICMP packets that carry options.

The **undo icmp with-options drop** command disables the device from discarding ICMP packets that carry options.

By default, the device does not discard ICMP packets that carry options.

Format

icmp with-options drop

undo icmp with-options drop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device receives a large number of ICMP packets, the function enables the device to discard some ICMP packets to reduce the workload on the device.

Example

Enable the device to discard the ICMP packets that carry options.

```
<Huawei> system-view
[Huawei] icmp with-options drop
```

8.7.26 icmp receive

Function

The **icmp receive** command enables the device to receive ICMP messages.

 Copyright © Huawei Technologies Co., Ltd.

The **undo icmp receive** command disables the device from receiving ICMP messages.

By default, the device receives ICMP messages.

Format

icmp { **type** *icmp-type* **code** *icmp-code* | **name** *icmp-name* | **all** } **receive**

undo icmp { **type** *icmp-type* **code** *icmp-code* | **name** *icmp-name* | **all** } **receive**

Parameters

Parameter	Description	Value
type *icmp-type*	Specifies the type number of an ICMP message.	The value is an integer ranging from 0 to 255.
code *icmp-code*	Specifies the code of an ICMP message.	The value is an integer ranging from 0 to 255.
name *icmp-name*	Specifies the name of an ICMP message.	The value is a string of case-insensitive characters, with spaces not supported. The string length ranges from 1 to 32. The value can be any of the following: ● echo ● echo-reply ● fragmentneed-dfset ● host-redirect ● host-tos-redirect ● host-unreachable ● information-reply ● information-request ● net-redirect ● net-tos-redirect ● net-unreachable ● parameter-problem ● port-unreachable ● protocol-unreachable ● reassembly-timeout ● source-quench ● source-route-failed ● timestamp-reply ● timestamp-request ● ttl-exceeded

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Specifies all ICMP packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **undo icmp receive** command can be used to disable the device from receiving ICMP messages for the purpose of improving network performance or enhancing network security.

- On secure networks, the device can normally receive ICMP messages. In the case of heavy traffic on the network, if hosts or ports are frequently unreachable, the device will receive a large number of ICMP packets, which causes heavier traffic burdens over the network and degrades the performance of the device.
- On insecure networks, network attackers often make use of ICMP error messages to probe on the internal structure of the network.

Precautions

If the network status is normal and the device is required to receive ICMP messages, you can run the **icmp receive** command.

After the **undo icmp receive** command is run, the device no longer process ICMP messages of a certain type, causing the host to fail to ping the device.

Example

Disable the device from receiving ICMP messages with the type number being 3 and the code number being 1.

```
<Huawei> system-view
[Huawei] undo icmp type 3 code 1 receive
```

8.7.27 icmp-reply fast

Function

The **icmp-reply fast** command enables the fast ICMP reply function on the device.

The **undo icmp-reply fast** command disables the fast ICMP reply function on the device.

By default, the fast ICMP reply function is enabled on the device.

Format

icmp-reply fast

undo icmp-reply fast

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the fast ICMP reply function is enabled on the device, the switches fast respond to the ICMP echo request packets whose destination addresses are the addresses of the switches. This improves the device forwarding performance.

NOTE

After the fast ICMP reply function is enabled on the device, the local policy-based routing function does not take effect for ICMP packets. Therefore, if the local policy-based routing function is configured on the device, you are advised to disable the fast ICMP reply function.

Example

Enable the fast ICMP reply function on the device.

```
<Huawei> system-view
[Huawei] icmp-reply fast
```

8.7.28 ip forward-broadcast

Function

The **ip forward-broadcast** command enables an interface to forward directed broadcast packets.

The **undo ip forward-broadcast** command disables an interface from forwarding directed broadcast packets.

By default, an interface is disabled from forwarding directed broadcast packets.

Format

ip forward-broadcast [**acl** *acl-number*]

undo ip forward-broadcast

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 3999. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Directed broadcast packets are sent to a specified network. In the destination IP address of a directed broadcast packet, the network number is that of the specified network and the host number is all 1s.

To enable an interface to receive and forward directed broadcast packets destined for its direct network segment, run the **ip forward-broadcast** command. Then the following situations occur:

- The device is allowed to receive directed broadcast packets destined for the interface's direct network segment.
- When the device receives directed broadcast packets destined for this interface's direct network segment through other interfaces, the device forwards these packets through this interface.

Directed broadcast packets can be used by hackers to attack the network system, bringing security risks. However, the device interfaces may need to receive or forward directed broadcast packets in some scenarios. For example, to enable the Wake on LAN function so that directed broadcast packets can be sent to wake up computers on a remote network, enable the interface to receive and forward directed broadcast packets destined for its direct network segment.

The device can also be enabled to receive and forward a certain type of directed broadcast packets based on ACLs. For example, if the basic ACL is used, run the **acl (system view)** and **rule (basic ACL view)** commands to define the directed broadcast packets to be received and forwarded as **permit**, and then run the **ip forward-broadcast** command to bind this ACL.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

By default, the device identifies directed broadcast packets as malformed packets, and intercepts and discards them because the attack defense function of malformed packets is enabled on the device. In this case, the interface on the device cannot forward the directed broadcast packets.

To solve this problem, use either of the following methods:

- Run the **anti-attack abnormal disable** command to disable the attack defense function of malformed packets. However, after this command is configured, other malformed packets will not be intercepted and discarded, which brings certain security risks. Use this command with caution.
- Run the **anti-attack disable** command to disable all attack defense functions. However, after this command is configured, not only malformed packets but also fragmented, tcp-syn, udp-flood, and icmp-flood attack packets will not be intercepted and discarded, which brings certain security risks. Use this command with caution.

You can only configure this command in the VLANIF interface view, Ethernet interface view, GE interface view, XGE interface view, and virtual Ethernet interface view.

This command cannot be used in the VPN scenario, address borrowing scenario, and scenario where the host route and subnet broadcast route conflict because of network segment overlapping.

Example

Enable GE1/0/0 to forward broadcast packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip forward-broadcast
```

Related Topics

5.1.9 display ip interface

8.7.29 ip soft-forward enhance enable

Function

The **ip soft-forward enhance enable** command enables the enhanced forwarding function for control packets generated by the device.

The **undo ip soft-forward enhance enable** command disables the enhanced forwarding function for control packets generated by the device.

By default, the enhanced forwarding function is enabled for control packets generated by the device.

Format

ip soft-forward enhance enable

 Copyright © Huawei Technologies Co., Ltd.

undo ip soft-forward enhance enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure forwarding policies (such as QoS policies) for data packets to implement differentiated services. In some scenarios, you may need to manage control packets generated by the device to process different control packets. For example, carriers have limited the bandwidth of data packets through QoS policies and also want to limit the bandwidth of control packets. In this situation, QoS policies take effect only for data packets. You can configure the enhanced forwarding function to make QoS policies take effect for control packets. Currently, the enhanced forwarding function is valid only for the control packets generated by the device but not for the control packets forwarded by other devices.

You can run the **ip soft-forward enhance enable** command to enable the enhanced forwarding function for control packets generated by the device.

Follow-up Procedures

After enabling the enhanced forwarding function on the device, you can perform some configurations on the control packets generated by the device. For example, you can configure different QoS policies for different types of packets generated by the device.

Example

Disable the enhanced forwarding function for control packets generated by the device.

```
<Huawei> system-view
[Huawei] undo ip soft-forward enhance enable
```

8.7.30 ip verify source-address

Function

The **ip verify source-address** command enables an interface to check validity of source IP addresses of received packets.

The **undo ip verify source-address** command disables an interface from checking validity of source IP addresses of received packets.

By default, an interface does not check validity of source IP addresses of received packets.

Format

ip verify source-address

undo ip verify source-address

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The following IP addresses are illegal source addresses:

- Addresses with all 0s or 1s
- Multicast addresses (class D addresses)
- Class E addresses
- Loopback addresses that are not generated on local hosts (in 127.x.x.x format)
- Broadcast addresses of classes A, B, and C
- Subnet broadcast addresses that are on the same network segment as the address of the inbound interface

The interface only check validity of source IP addresses of the packets that are forwarded to the CPU and does not check validity of source IP addresses of the packets that will be directly forwarded according to the FIB table.

Example

Enable GE1/0/0 to check validity of source addresses of received packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip verify source-address
```

Related Topics

3.1.9 display this

8.7.31 ip option-virtual-reassembly

Function

The **ip option-virtual-reassembly** command enables virtual fragment reassembly of IP packets with options globally.

The **undo ip option-virtual-reassembly** command disables virtual fragment reassembly of IP packets with options globally.

By default, virtual fragment reassembly of IP packets with options is disabled globally.

Format

ip option-virtual-reassembly

undo ip option-virtual-reassembly

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Oversized IP packets are fragmented during transmission. The intermediate forwarding device forwards the fragmented packets, and the destination device reassembles the fragmented packets after receiving them. If some fragmented packets are discarded during transmission due to bandwidth limitation, the packets cannot be reassembled on the destination device. To solve this problem, you can enable virtual fragment reassembly of IP packets with options globally on the device functioning as the intermediate forwarding device of fragmented packets. The device then checks, sorts, and caches received fragmented packets, and processes the packets uniformly to ensure complete IP packet forwarding or scheduling.

Example

Enable virtual fragment reassembly of IP packets with options globally.

```
<Huawei> system-view
[Huawei] ip option-virtual-reassembly
```

 Copyright © Huawei Technologies Co., Ltd.

8.7.32 ip virtual-reassembly

Function

The **ip virtual-reassembly** command enables virtual fragment reassembly of IP packets.

The **undo ip virtual-reassembly** command disables virtual fragment reassembly of IP packets.

By default, virtual fragment reassembly of IP packets is disabled.

Format

ip virtual-reassembly

undo ip virtual-reassembly

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During network transmission, IP packets are fragmented if they have a long length. The forwarding device forwards the fragmented packets, and the destination device receives the fragmented packets and reassembles them. If some fragmented packets are discarded during transmission due to the bandwidth limitation, the packets cannot be reassembled on the destination device. To solve the problem, you can enable virtual fragment reassembly of IP packets on the device functioning as the intermediate of fragmented packets. After that, the device checks, sorts, and caches the fragmented packets received to ensure complete packet forwarding or scheduling.

Precautions

- If the NAT, firewall, smart application control (SAC), or in-depth security defense functions is configured on the device, virtual fragment reassembly is enabled by default and cannot be disabled. That is, the **undo ip virtual-reassembly** command does not take effect.
- If the upstream device first sends packets whose length is smaller than the interface MTU and then sends packets whose length is equal to the interface MTU after fragmenting packets, you need to run the **ip virtual-reassembly** command to enable the destination device to reassemble fragmented packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable virtual fragment reassembly of IP packets.

```
<Huawei> system-view
[Huawei] ip virtual-reassembly
```

8.7.33 load-balance unequal-cost enable

Function

Using the **load-balance unequal-cost enable** command, you can enable the Unequal-Cost Multiple Path (UCMP) function on an interface.

Using the **undo load-balance unequal-cost enable** command, you can disable the UCMP function on an interface.

By default, UCMP is disabled on an interface.

Format

load-balance unequal-cost enable

undo load-balance unequal-cost enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the device, there are multiple equal-cost routes over multiple equal-cost links to a destination. Among the equal-cost links, there are high-speed links and low-speed links. The device evenly load balances traffic over multiple equal-cost links to a single destination regardless of the bandwidth. Consequently, traffic congestion may occur on low-speed links and bandwidth of high-speed links cannot be used efficiently. To solve the preceding problems, configure UCMP so that the equal-cost links carry traffic by bandwidth.

Precautions

This command can only be used on Layer 3 interfaces.

Among all subinterfaces, only the Ethernet sub-interfaces (Dot1q and QinQ termination sub-interfaces) and Eth-trunk sub-interfaces (Dot1q termination sub-interfaces) support configuration of unequal cost multiple path.

 Copyright © Huawei Technologies Co., Ltd.

After enabling or disabling UCMP on an outbound interface of an equal-cost link, run the **shutdown** and **undo shutdown** commands on the outbound interface, or run the **restart** command restarts the interface, to make the configuration take effect.

The equal-cost links carry traffic by bandwidth only when UCMP is enabled on outbound interfaces of all the equal-cost links and FIB entry updating is triggered. If any outbound interface is not enabled with UCMP, the equal-cost links evenly load balance traffic though FIB entry updating is triggered.

On AR120, AR150, AR160, AR200 and AR1200, among the equal-cost links, the bandwidth of any link must be equal to or greater than 1/4 of the total bandwidth; otherwise, the link cannot participate in load balancing traffic by bandwidth.

On AR2200, AR3600 and AR3200, among the equal-cost links, the bandwidth of any link must be equal to or greater than 1/8 of the total bandwidth; otherwise, the link cannot participate in load balancing traffic by bandwidth.

You are advised to configure the bandwidth of each link participating in UCMP to an integral multiple of the minimum bandwidth. If the bandwidth of each link is not configured to an integral multiple of the minimum bandwidth, the system still uses an integral multiple of the minimum bandwidth to process. For example, if the bandwidths of four links participating in UCMP are configured to 2 Kbps, 3 Kbps, 4 Kbps, and 5 Kbps, the final bandwidths of the links are 2 Kbps, 2 Kbps, 4 Kbps, and 4 Kbps.

Before enabling UCMP on a logical interface, run the **load-balance bandwidth** command to manually configure the bandwidth for the logical interface.

Example

Enable UCMP on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] load-balance unequal-cost enable
Warning: The configuration succeeded. Please shutdown/undo shutdown the interfac
e to make changes take effect.
[Huawei-GigabitEthernet1/0/0] shutdown
[Huawei-GigabitEthernet1/0/0] undo shutdown
```

Enable UCMP on Eth-Trunk1.

```
<Huawei> system-view
[Huawei] interface eth-trunk 1
[Huawei-Eth-Trunk1] undo portswitch
[Huawei-Eth-Trunk1] load-balance bandwidth 300000
 Warning: The configuration succeeded. Please shutdown/undo shutdown the interfa
ce to make changes take effect.
[Huawei-Eth-Trunk1] load-balance unequal-cost enable
Warning: The configuration succeeded. Please shutdown/undo shutdown the interfac
e to make changes take effect.
[Huawei-Eth-Trunk1] shutdown
[Huawei-Eth-Trunk1] undo shutdown
```

Related Topics

8.7.34 load-balance bandwidth

8.7.34 load-balance bandwidth

Function

The **load-balance bandwidth** command sets the bandwidth of an interface manually.

The **undo load-balance bandwidth** command deletes the manually configured bandwidth of an interface.

For a logical interface, the interface bandwidth is not configured by default; for a physical interface, the actual interface bandwidth is used by default.

Format

load-balance bandwidth *bandwidth*

undo load-balance bandwidth

Parameters

Parameter	Description	Value
bandwidth	Specifies the manually configured bandwidth of an interface.	The value is an integer that ranges from 1 to 10000000, in Kbps.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the UCMP function, you need to manually set the bandwidth of an interface in the following scenarios:

- Users need to adjust the bandwidth of equal-cost links so that the equal-cost links load balance traffic based on the configured bandwidth.
- The outbound interface of the equal-cost route is a logical interface.

Precautions

This command can only be used on Layer 3 interfaces.

When the manually configured bandwidth of an interface changes or the physical bandwidth corresponding to a logical interface changes, run the **shutdown** and **undo shutdown** commands on the interface to make the new bandwidth take effect.

 Copyright © Huawei Technologies Co., Ltd.

When you manually configure the bandwidth for an interface, the bandwidth ratio of each equal-cost link will change. In UCMP mode, traffic is load balanced by bandwidth. If the bandwidth ratio changes, packets on a link will be lost when the allocated traffic exceeds the physical bandwidth of the link.

You are advised to configure the bandwidth of each link participating in UCMP to an integral multiple of the minimum bandwidth. If the bandwidth of each link is not configured to an integral multiple of the minimum bandwidth, the system still uses an integral multiple of the minimum bandwidth to process. For example, if the bandwidths of four links participating in UCMP are configured to 2 Kbps, 3 Kbps, 4 Kbps, and 5 Kbps, the final bandwidths of the links are 2 Kbps, 2 Kbps, 4 Kbps, and 4 Kbps.

Example

Set the bandwidth of GE1/0/0 to 500000 Kbps.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] load-balance bandwidth 500000
 Warning: The configuration succeeded. Please shutdown/undo shutdown the interfa
ce to make changes take effect.
[Huawei-GigabitEthernet1/0/0] shutdown
[Huawei-GigabitEthernet1/0/0] undo shutdown
```

Related Topics

8.7.33 load-balance unequal-cost enable

8.7.35 reset forward pie counter

Function

The **reset forward pie counter** command clears statistics on packets of the PIE queue.

NOTE

Only the AR169EGW-L, AR169EW, AR161EW, and AR161EW-M1 support this command.

Format

reset forward pie counter

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can run the **reset forward pie counter** command to clear statistics on packets of the PIE queue. The cleared statistics cannot be restored. Therefore, confirm your operation before running this command.

Example

Clear PIE queue packet statistics.

```
<Huawei> reset forward pie counter
```

8.7.36 reset ip socket monitor

Function

The **reset ip socket monitor** command clears information in a socket monitor.

Format

reset ip socket monitor [**task-id** *task-id* **socket-id** *socket-id*]

Parameters

Parameter	Description	Value
task-id *task-id*	Clears information about the task with a specified ID in the socket monitor.	The value must be an existing task ID.
socket-id *socket-id*	Clears information about the socket with a specified ID in the socket monitor.	The value must be an existing socket ID.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can specify the task ID and socket ID for deleting information about the socket monitor that meets the filtering condition.

Example

Clear information in a socket monitor.

```
<Huawei> reset ip socket monitor
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.7.9 display ip socket

8.7.37 reset ip socket pktsort

Function

The **reset ip socket pktsort** command resets statistics on the dual receive buffer of the socket.

Format

reset ip socket pktsort task-id *task-id* **socket-id** *socket-id*

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a task.	The value must be an existing task ID.
socket-id *socket-id*	Specifies the ID of a socket.	The value must be an existing socket ID.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics on the dual receive buffer of the socket and restarts the count. Therefore, confirm your action before running the command.

Example

Reset statistics on the dual receive buffer of the socket with the task ID of 2 and the socket ID of 6.

```
<Huawei> reset ip socket pktsort task-id 2 socket-id 6
```

8.7.38 reset ip statistics

Function

The **reset ip statistics** command clears IP traffic statistics on an interface.

Format

reset ip statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and ID of an interface. If no optional parameter is specified, all the IP statistics will be deleted.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect IP traffic statistics on an interface in a period of time, you must clear the existing traffic statistics and collect IP statistics after a period of time. Run the **display ip statistics** command to display information.

If no parameter is specified, the command clears IP traffic statistics on all boards.

Example

Clear IP statistics on all interfaces.

```
<Huawei> reset ip statistics
```

Related Topics

5.1.9 display ip interface

8.7.11 display ip statistics

8.7.39 reset rawip statistics

Function

The **reset rawip statistics** command clears RawIP packet statistics.

Format

reset rawip statistics

Parameters

None

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

The **reset rawip statistics** command clears RawIP packet statistics. Confirm your action before running this command.

Example

Clear RawIP packet statistics.

```
<Huawei> reset rawip statistics
```

Related Topics

8.7.14 display rawip statistics

8.7.40 reset tcp statistics

Function

The **reset tcp statistics** command deletes TCP traffic statistics.

Format

reset tcp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset tcp statistics** command deletes TCP traffic statistics. Confirm your action before running this command.

Example

Delete TCP traffic statistics.

```
<Huawei> reset tcp statistics
```

Related Topics

8.7.15 display tcp statistics

 Copyright © Huawei Technologies Co., Ltd.

8.7.41 reset udp statistics

Function

The **reset udp statistics** command deletes UDP traffic statistics.

Format

reset udp statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset udp statistics** command deletes UDP traffic statistics. Confirm your action before running this command.

Example

Delete UDP traffic statistics.

```
<Huawei> reset udp statistics
```

Related Topics

8.7.17 display udp statistics

8.7.42 set priority dscp

Function

The **set priority dscp** command sets the DSCP priority of control packets generated by the device.

The **undo set priority dscp** command restores the default DSCP priority of control packets generated by the device.

For the default DSCP priorities of control packets generated by the device, see **Table 8-77**.

Format

set priority protocol-type *protocol-type* **dscp** *dscp-value*

undo set priority protocol-type *protocol-type* **dscp**

set priority acl *acl-number* **dscp** *dscp-value*

undo set priority acl *acl-number*

Parameters

Parameter	Description	Value
protocol-type *protocol-type*	Sets the DSCP priority of control packets based on the protocol type.	The value can be bgp, ftp, icmp, snmp, ssh, **udp**, or telnet.
acl *acl-number*	Sets the DSCP priority of control packets based on the ACL.	The value is an integer that ranges from 3000 to 3999.
dscp *dscp-value*	Specifies the DSCP priority of control packets.	The value is as follows: ● The value is an integer that ranges from 0 to 63. ● The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

Table 8-77 Default DSCP priorities of control packets generated by the device

control Packet	Value
BGP	48
ICMP	0
SNMP	0
SSH	48
Telnet	48
FTP	48

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ip soft-forward enhance enable** command is executed to enable the enhanced forwarding function of control packets generated by the device, the same QoS policy will be applied to both the control packets and data packets. When the device maps packets based on DSCP priorities, it may send some control packets with low DSCP priorities generated on the device to low-priority queues, such as ICMP and Telnet packets. You can use the **set priority** command to set DSCP priorities of some control packets to prevent them from being sent to low-priority queues.

Precautions

If you run the **set priority** command with the same value of **protocol-type** multiple times, only the latest configuration takes effect.

If the device is configured to set the DSCP priority of control packets based on both the protocol type and ACL, the device sets the DSCP priority of control packets based on the protocol type.

If the device is configured to set the DSCP priority of protocol packets based on ACL rules, a maximum of 16 ACL rules can be configured.

To set DSCP priorities of multiple control packets, run the **set priority** command multiple times.

Example

Set the DSCP priority of Telnet packets to 56.

```
<Huawei> system-view
[Huawei] set priority protocol-type telnet dscp 56
```

Related Topics

8.7.29 ip soft-forward enhance enable

8.7.43 set priority dot1p

Function

The **set priority dot1p** command sets the 802.1p priority of control packets generated by the device.

The **undo set priority dot1p** command restores the default 802.1p priority of control packets generated by the device.

By default, the 802.1p priority of control packets generated by the device is 6.

 Copyright © Huawei Technologies Co., Ltd.

Format

set priority dot1p *priority-value*

undo set priority dot1p

Parameters

Parameter	Description	Value
priority-value	Specifies the 802.1p priority of control packets generated by the device.	The value is an integer that ranges from 0 to 7.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.1p priority is determined by the 3-bit priority field contained in a VLAN tag and is used to guarantee QoS in the differentiated services (DiffServ) model.

You can run the **set priority dot1p** command to change the 802.1p priority of control packets generated by the device.

Precautions

If you run the **set priority dot1p** command multiple times, only the latest configuration takes effect.

The **set priority dot1p** command will not take effect on a Layer 2 interface.

Example

Set the 802.1p priority of control packets generated by the device to 5.

```
<Huawei> system-view
[Huawei] set priority dot1p 5
```

8.7.44 set workmode lan-card l3centralize

Function

The **set workmode lan-card l3centralize** command disables the routing and forwarding function on 8FE1GE and 24GE cards.

The **undo set workmode lan-card l3centralize** command enables the routing and forwarding function on 8FE1GE and 24GE cards.

By default, the routing and forwarding function is enabled on 8FE1GE and 24GE cards.

Format

set workmode lan-card l3centralize

undo set workmode lan-card l3centralize

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring ACLs on 8FE1GE and 24GE cards is complex, and ACL-based traffic policy and URPF cannot be configured on 8FE1GE and 24GE cards. This restricts the use of ACLs. When the routing and forwarding function is disabled on 8FE1GE and 24GE cards, you can redirect the packets received on 8FE1GE and 24GE cards to the sub-core CPU for packet forwarding. In this situation, you can configure ACL-based traffic policies and URPF and simplify the ACL configuration.

Configuration Impact

- After the **set workmode lan-card l3centralize** command is used, an interface can only be manually added to a voice VLAN.
- After the **set workmode lan-card l3centralize** command is used, protocol packets with source or destination MAC addresses as blackhole MAC addresses will not be discarded.
- After the **set workmode lan-card l3centralize** command is used, the device CPU usage increases.

NOTE

Only AR1200, AR2200, AR3600 and AR3200 support this command.

Example

Disable the routing and forwarding function on 8FE1GE and 24GE cards.

```
<Huawei&gt; system-view
[Huawei] set workmode lan-card l3centralize
```

8.7.45 tcp adjust-mss

Function

The **tcp adjust-mss** command sets the maximum segment size (MSS) of TCP packets on an interface.

The **undo tcp adjust-mss** command deletes the configured MSS of TCP packets.

By default, the MSS of TCP packets is not set on the interface.

Format

tcp adjust-mss *value*

undo tcp adjust-mss

Parameters

Parameter	Description	Value
value	Specifies the MSS of TCP packets on an interface.	The value is an integer that ranges from 128 to 2048, in bytes.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MSS of TCP packets is an option defined in TCP. It refers to the maximum length of a TCP packet segment that can be received by the peer device. When establishing the TCP connection, the local and peer ends negotiate the MSS value to determine the maximum data length of TCP packets. If the length of a TCP packet sent by the peer device exceeds the negotiated MSS, the TCP packet is fragmented.

Precautions

- To ensure that TCP packets are not fragmented, pay attention to the relationship between the MSS and MTU during configuration. MTU is an option used to identify whether IP packets need to be fragmented. If the size of an IP packet sent by the peer device exceeds the MTU, the IP packet is fragmented. To ensure that the packet transmission is not affected, the MSS value plus the header lengths (such as the TCP header and IP header) does not exceed the MTU value. For example, the default MTU value of an

 Copyright © Huawei Technologies Co., Ltd.

Ethernet interface is 1500 bytes. To ensure that packets are not fragmented, the MSS value can be set to 1460 bytes. The formula is as follows: Default MTU value (1500 bytes) – Minimum length of the TCP header (20 bytes) – Minimum length of the IP header (20 bytes). The recommended MSS value is 1200 bytes.

- The **tcp adjust-mss** command does not only take effect for the router functioning as the client or server used for TCP connections. When another device functions as the client to perform MSS negotiation through the router, the negotiation result is modified based on the MSS configured on the router. In addition, the MSS value is changed to the value configured using the **tcp adjust-mss** command only when the MSS value received by the router is larger than the value configured using the **tcp adjust-mss** command executed on the router.
- If you run the **tcp adjust-mss** multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the MSS of TCP packets on GE1/0/0 to 1200 bytes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] tcp adjust-mss 1200
```

Related Topics

5.2.27 mtu (Ethernet interface view)

8.7.49 tcp timer syn-timeout

8.7.50 tcp window

8.7.46 tcp min-mss

Function

The **tcp min-mss** command sets the minimum value of maximum segment size (MSS) for a TCP connection.

The **undo tcp min-mss** command restores the default minimum value of the MSS for a TCP connection.

The default minimum MSS value for a TCP connection is 216 bytes.

Format

tcp min-mss *mss-value*

undo tcp min-mss

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mss-value	Specifies the minimum MSS value for a TCP connection.	The value ranges from 32 byte to 1500 bytes. By default, the value is 216 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. The TCP client on a network may send a request packet for establishing a TCP connection carrying a small MSS value. For example, the MSS value is 1. After the TCP server receives the request packet carrying the MSS value, the TCP connection is established. The TCP client then may send large numbers of requests to the server by an application, causing the TCP server to generate large numbers of reply packets. This may burden the TCP server or network, causing denial of service (DoS) attacks. To resolve this problem, run the **tcp min-mss** command to set the minimum MSS value for a TCP connection. This configuration prevents a server from receiving packets carrying a small MSS value.

Precautions

If the **tcp min-mss** command is run more than once in the same view, the latest configuration overrides the previous one.

Configure the parameters under the guidance of the technical personnel.

Example

Set the minimum MSS value for a TCP connection to 512 bytes.

```
<Huawei> system-view
[Huawei] tcp min-mss 512
```

Related Topics

8.7.50 tcp window

8.7.47 tcp timer fin-timeout

Function

The **tcp timer fin-timeout** command configures the value of the TCP FIN-Wait timer.

The **undo tcp timer fin-timeout** command restores the default value of the TCP FIN-Wait timer.

By default, the value of the TCP FIN-Wait timer is 675s.

Format

tcp timer fin-timeout *interval*

undo tcp timer fin-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP FIN-Wait timer.	The value is an integer that ranges from 76 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a TCP connection changes from FIN_WATI_1 to FIN_WAIT_2, the TCP FIN-Wait timer is started. If no response packet is received after the TCP FIN-Wait timer expires, the TCP connection is closed.

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the value of the TCP FIN-Wait timer to 400s.

```
<Huawei> system-view
[Huawei] tcp timer fin-timeout 400
```

Related Topics

8.7.49 tcp timer syn-timeout

 Copyright © Huawei Technologies Co., Ltd.

8.7.50 tcp window

8.7.48 tcp timer pathmtu-age

Function

The **tcp timer pathmtu-age** command sets the aging time for a TCP PMTU.

The **undo tcp timer pathmtu-age** command restores the aging time for a TCP PMTU to the default value.

By default, the aging time of the PMTU is 0 minutes, that is, the PMTU never ages.

Format

tcp timer pathmtu-age *age-time*

undo tcp timer pathmtu-age

Parameters

Parameter	Description	Value
age-time	Specifies the aging time for a TCP PMTU.	The value is an integer that ranges from 10 to 100, in minutes. The default value is 0 minutes, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When hosts on the same network communicate with each other, the MTU of the network is important for the hosts. When hosts communicate with each other across multiple networks, it is important to determine the minimum MTU on the network path because the MTUs of the link layers on different networks are different. The minimum MTU on the network path is called the path MTU (PMTU).

When hosts on the network communicate with each other, the interface MTU on the communication path may change. This may cause the following problems:

- If the interface MTU changes to a smaller value, the system refragments the data packets to be sent and learn a new PMTU. This affects data transmission efficiency and network performance.

 Copyright © Huawei Technologies Co., Ltd.

- If the interface MTU changes to a value greater than the PMTU, the interface MTU will be too big for transmitting the fragmented packets. This also affects data transmission efficiency and network performance.

To prevent the preceding problems, run the **tcp timer pathmtu-age** command to set the aging time for a PMTU. After the PMTU ages, the device sends data packets based on the MTU of the outbound interface to detect the PMTU change.

Configuration Impact

The **tcp timer pathmtu-age** command changes only the aging time of dynamic PMTUs. It is not applicable to static PMTUs because static PMTUs cannot age.

Precautions

You need to set a PMTU based on network stability. The default PMTU is recommended. That is, a PMTU does not age.

- If the aging time of a PMTU is set too longer, the PMTU may not be updated in time. This will affect network performance.
- If the aging time of a PMTU is set too short, data transmission efficiency on the network will be affected.

Example

Set the aging time of a TCP PMTU to 50 minutes.

```
<Huawei> system view
[Huawei] tcp timer pathmtu-age 50
```

8.7.49 tcp timer syn-timeout

Function

The **tcp timer syn-timeout** command configures the value of the TCP SYN-Wait timer.

The **undo tcp timer syn-timeout** command restores the default value of the TCP SYN-Wait timer.

By default, the value of the TCP SYN-Wait timer is 75s.

Format

tcp timer syn-timeout *interval*

undo tcp timer syn-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP SYN-Wait timer.	The value is an integer ranging from 2 to 600, in seconds. The default value is 75s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When an SYN packet is sent, the TCP SYN-Wait timer is started. If no response packet is received after the TCP SYN-Wait timer expires, the TCP connection is closed.

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the value of the TCP SYN-Wait timer to 100s.

```
<Huawei> system-view
[Huawei] tcp timer syn-timeout 100
```

Related Topics

8.7.47 tcp timer fin-timeout

8.7.50 tcp window

8.7.50 tcp window

Function

The **tcp window** command configures the size of the receive or send buffer of a connection-oriented socket.

The **undo tcp window** command restores the default size of the receive or send buffer of a connection-oriented socket.

By default, the size of the receive or send buffer of a connection-oriented socket is 8k bytes.

Format

tcp window *window-size*

undo tcp window

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
window-size	Specifies the size of the receive or send buffer of a connection-oriented socket.	The value is an integer that ranges from 1 to 32, in k bytes. The default value is 8k bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you run this command in the same view for multiple times, only the last configuration takes effect.

You are advised to configure this parameter under the supervision of technical support personnel.

Example

Set the size of the receive or send buffer of a connection-oriented socket to 3K bytes.

```
<Huawei> system-view
[Huawei] tcp window 3
```

Related Topics

8.7.47 tcp timer fin-timeout

8.7.49 tcp timer syn-timeout

8.8 Basic IPv6 Configuration Commands

8.8.1 control-packet-ipv6 output car bypass

Function

The **control-packet-ipv6 output car bypass** command configures the IPv6 control packets generated by the device not to support traffic policing function.

The **undo control-packet-ipv6 output car bypass** command configures the IPv6 control packets generated by the device to support traffic policing function.

By default, IPv6 control packets generated by the device do not support traffic policing function.

 Copyright © Huawei Technologies Co., Ltd.

Format

control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] } * **output car bypass**

control-packet-ipv6 all output car bypass

undo control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] } * **output car bypass**

undo control-packet-ipv6 all output car bypass

Parameters

Parameter	Description	Value
bgp4plus	Indicates BGP4+ control packets.	-
icmpv6	Indicates ICMPv6 control packets.	-
dns6	Indicates IPv6 DNS control packets.	-
snmp	Indicates IPv6 SNMP control packets.	-
ssh	Indicates IPv6 SSH control packets.	-
telnet	Indicates IPv6 TELNET control packets.	-
udp	Indicates IPv6 UDP control packets.	-
ip_address	Indicates IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
all	Indicates all IPv6 control packets.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for IPv6 control packets generated by the device, you can run the **undo control-packet-ipv6 output car bypass** command to configures IPv6 control packets generated by the device to support traffic policing function to apply QoS policies to different control packets.

Follow-up Procedures

After IPv6 control packets generated by the device are configured to support traffic policing function, configure QoS policies to process different control packets. For details about traffic policing configuration, see Configuring Traffic Policing in *Huawei AR Series Access Routers Configuration Guide-QoS*.

Precautions

- Before configuring IPv6 control packets generated by the device to support traffic policing function, enable the enhanced forwarding function for IPv6 control packets generated by the device (using the **8.8.57 ipv6 soft-forward enhance enable** command). After IPv6 control packets generated by the device are configured to support traffic policing function, control packets may be discarded, affecting user services.
- When **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **telnet** and **udp** are specified in the **undo control-packet-ipv6 car bypass** commands, the device generates a configuration file of the **undo control-packet-ipv6 all output car bypass** command. If the **control-packet-ipv6 output car bypass** command is then executed to configure a specified type of IPv6 control packets generated by the device not to support traffic policing function, the device does not generate the configuration file of the **undo control-packet-ipv6 all output car bypass** command but generates the configuration files of the control packets that are configured to support traffic policing function. For example, if BGP4+ packets, IPv6 DNS packets, ICMPv6 packets, IPv6 SNMP packets, IPv6 SSH packets and IPv6 UDP packets generated by the device are configured not to support traffic policing function, the device generates the configuration files of the **undo control-packet-ipv6 telnet output car bypass** commands.

Example

Configure BGP4+ packets generated by the device to support traffic policing function.

```
<Huawei> system-view
[Huawei] undo control-packet-ipv6 bgp4plus output car bypass
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

 Copyright © Huawei Technologies Co., Ltd.

8.8.2 control-packet-ipv6 output filter bypass

Function

The **control-packet-ipv6 output filter bypass** command configures the device not to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

The **undo control-packet-ipv6 output filter bypass** command configures the device to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

By default, the device does not discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

Format

control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] } * **output filter bypass**

control-packet-ipv6 all output filter bypass

undo control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] } * **output filter bypass**

undo control-packet-ipv6 all output filter bypass

Parameters

Parameter	Description	Value
bgp4plus	Indicates BGP4+ control packets.	-
dns6	Indicates IPv6 DNS control packets.	-
icmpv6	Indicates ICMPv6 control packets.	-
snmp	Indicates IPv6 SNMP control packets.	-
ssh	Indicates IPv6 SSH control packets.	-
telnet	Indicates IPv6 TELNET control packets.	-
udp	Indicates IPv6 UDP control packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip_address	Indicates IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
all	Indicates all IPv6 control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for IPv6 control packets generated by the device, the device does not discard the control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action. After the **undo control-packet-ipv6 output filter bypass** command is executed, the device is configured to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action and apply QoS policy to the control packets to meet different service requirements.

Follow-up Procedures

The packet filter action in the traffic policy or ACL-based simplified traffic policy has been set to deny.

Precautions

- Before configuring the device to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action, enable the enhanced forwarding function for IPv6 control packets generated by the device (using the **8.8.57 ipv6 soft-forward enhance enable command). After the device is configured to discard generated IPv6 control packets when the traffic policy and ACL-based simplified traffic policy contain the deny action, user services may be affected.**
- When **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **udp** and **telnet** are specified in the **undo control-packet-ipv6 output filter bypass** commands, the device

generates a configuration file of the **undo control-packet-ipv6 all output filter bypass** command. If the **control-packet-ipv6 output filter bypass** command is then executed to configure the device not to discard a specified type of control packets, the device does not generate the configuration file of the **undo control-packet-ipv6 all output filter bypass** command but generates the configuration files of the control packets that the device is configured to discard. For example, if the device is configured not to discard BGP4+ packets, IPv6 DNS packets, ICMPv6 packets, IPv6 SNMP packets and IPv6 SSH packets, the device generates the configuration files of the **undo control-packet-ipv6 telnet output filter bypass** commands.

Example

Configure the device to discard generated BGP4+ packets when the traffic policy and ACL-based simplified traffic policy contain the deny action.

```
<Huawei> system-view
[Huawei] undo control-packet-ipv6 bgp4plus output filter bypass
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.3 control-packet-ipv6 output queue bypass

Function

The **control-packet-ipv6 output queue bypass** command configures the IPv6 control packets generated by the device not to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance).

The **undo control-packet-ipv6 output queue bypass** command configures the IPv6 control packets generated by the device to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance).

By default, IPv6 control packets generated by the device do not support QoS queue functions.

Format

control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] } * **output queue bypass**

control-packet-ipv6 all output queue bypass

undo control-packet-ipv6 { **bgp4plus** | **icmpv6** | **dns6** | **snmp** | **ssh** | **telnet** | **udp** [*ip_address port*] } * **output queue bypass**

undo control-packet-ipv6 all output queue bypass

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bgp4plus	Indicates BGP4+ control packets.	-
icmpv6	Indicates ICMPv6 control packets.	-
dns6	Indicates IPv6 DNS control packets.	-
snmp	Indicates IPv6 SNMP control packets.	-
ssh	Indicates IPv6 SSH control packets.	-
telnet	Indicates IPv6 TELNET control packets.	-
udp	Indicates IPv6 UDP control packets.	-
ip_address	Indicates IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
port	Indicates the port.	The value is an integer that ranges from 0 to 65535.
all	Indicates all IPv6 control packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the enhanced forwarding function is enabled for IPv6 control packets generated by the device, you can run the **undo control-packet-ipv6 output queue bypass** command to configures IPv6 control packets generated by the

device to support QoS queue functions (such as traffic shaping, congestion management, and congestion avoidance) to apply QoS policies to different control packets.

Follow-up Procedures

After IPv6 control packets generated by the device are configured to support QoS queue functions, configure QoS policies to process different control packets.

Precautions

- Before configuring IPv6 control packets generated by the device to support QoS queue functions, enable the enhanced forwarding function for IPv6 control packets generated by the device (using the **8.8.57 ipv6 soft-forward enhance enable** command). After IPv6 control packets generated by the device are configured to support QoS queue functions, control packets may be discarded, affecting user services.
- When **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **udp**, and **telnet** are specified in the **undo control-packet-ipv6 output queue bypass** commands, the device generates a configuration file of the **undo control-packet-ipv6 all output queue bypass** command. If the **control-packet-ipv6 output queue bypass** command is then executed to configure a specified type of control packets generated by the device not to support QoS queue functions, the device does not generate the configuration file of the **undo control-packet-ipv6 all output queue bypass** command but generates the configuration files of the control packets that are configured to support QoS queue functions. For example, if BGP4+ packets, IPv6 DNS packets, ICMPv6 packets, IPv6 SNMP packets, and IPv6 SSH packets generated by the device are configured not to support QoS queue functions, the device generates the configuration files of the **undo control-packet-ipv6 telnet output queue bypass** commands.

Example

Configure BGP4+ packets generated by the device to support QoS queue functions.

```
<Huawei> system-view
[Huawei] undo control-packet-ipv6 bgp4plus output queue bypass
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.4 display default-parameter tcp6

Function

The **display default-parameter tcp6** command displays the default values of all configurable parameters on the TCP6 module.

Format

display default-parameter tcp6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the default values of all configurable parameters on the TCP6 module.

```
<Huawei> display default-parameter tcp6
---------------------------------
 SYN Timeout Value(sec) : 75
 FIN Timeout Value(sec) : 600
 Window Size(KBytes)    : 8
---------------------------------
```

Table 8-78 Description of the display default-parameter tcp6 command output

Item	Description
SYN Timeout Value(sec)	TCP SYN-WAIT timer value. To configure this parameter, run the **tcp ipv6 timer syn-timeout** command.
FIN Timeout Value(sec)	TCP FIN-WAIT timer value. To configure this parameter, run the **tcp ipv6 timer fin-timeout** command.
Window Size(KBytes)	TCP6 slide window size. To configure this parameter, run the **tcp ipv6 window** command.

Related Topics

8.8.73 tcp ipv6 timer syn-timeout

8.8.72 tcp ipv6 timer fin-timeout

8.8.74 tcp ipv6 window

 Copyright © Huawei Technologies Co., Ltd.

8.8.5 display icmpv6 statistics

Function

The **display icmpv6 statistics** command displays ICMPv6 traffic statistics.

Format

display icmpv6 statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays ICMPv6 traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, ICMPv6 traffic statistics on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display icmpv6 statistics** command to view ICMPv6 packet statistics, including statistics about received and sent ICMPv6 error packets and statistics about four types of ICMPv6 packets (RS, RA, NS, and NA packets) used in the neighbor discovery mechanism.

When you ping an IPv6 address from a device, run the **display icmpv6 statistics** command on the device to check whether the total number of sent and received packets is correct.

Precautions

The total number of packets received by the device includes the number of packets forwarded, number of packets delivered to upper-layer network devices, and number of packets discarded.

Example

Display ICMPv6 traffic statistics on the device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display icmpv6 statistics
ICMPv6 protocol:
  Sent packets:
    Total              : 0
    Unreached          : 0              Prohibited         : 0
    Hop count exceeded : 0              Parameter problem  : 0
    Too big            : 0              Echoed             : 0
    Echo replied       : 0              Router solicit     : 0
    Router advert      : 0              Neighbor solicit   : 2
    Neighbor advert    : 0              Redirected         : 0
    Rate limited       : 0
  Received packets:
    Total              : 0              Format error       : 0
    Checksum error     : 0              Too short          : 0
    Bad code           : 0              Bad length         : 0
    Unknown info type  : 0              Unknown error type : 0
    Unreached          : 0              Prohibited         : 0
    Hop count exceeded : 0              Parameter problem  : 0
    Too big            : 0              Echoed             : 0
    Echo replied       : 0              Router solicit     : 0
    Router advert      : 0              Neighbor solicit   : 0
    Neighbor advert    : 0              Redirected         : 0
    Rate limited       : 0
```

Table 8-79 Description of the display icmpv6 statistics command output

Item	Description
ICMPv6 protocol	ICMPv6 packet statistics.
Sent packets	Statistics about sent ICMPv6 packets.
Total	Total number of sent packets.
Unreached	Total number of sent ICMPv6 Destination Unreachable packets.
Prohibited	Total number of sent ICMPv6 Administratively Prohibited Unreachable packets.
Hop count exceeded	Total number of sent ICMPv6 packets whose hops exceed the limit.
Parameter problem	Total number of sent ICMPv6 Parameter Problem packets.
Too big	Total number of sent ICMPv6 Packet Too Big packets.
Echoed	Total number of sent ICMPv6 Echo Request packets.
Echo replied	Total number of sent ICMPv6 Echo Reply packets.
Router solicit	Total number of sent Router Solicitation (RS) packets.
Router advert	Total number of sent Router Advertisement (RA) packets.
Neighbor solicit	Total number of sent Neighbor Solicitation (NS) packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Neighbor advert	Total number of sent Neighbor Advertisement (NA) packets.
Redirected	Total number of sent ICMPv6 Redirect packets.
Rate limited	Total number of ICMPv6 packets that fail to be sent because of the rate limit.
Received packets	Statistics about received ICMPv6 packets.
Total	Total number of received packets.
Format error	Total number of received ICMPv6 packets with format errors.
Checksum error	Total number of received ICMPv6 packets with checksum errors.
Too short	Total number of received ICMPv6 packets that are too short.
Bad code	Total number of received ICMPv6 packets with code errors.
Bad length	Total number of received ICMPv6 packets with packet length errors.
Unknown info type	Total number of received ICMPv6 packets with an unknown information type.
Unknown error type	Total number of received ICMPv6 packets with an unknown error type.
Unreached	Total number of received ICMPv6 Destination Unreachable packets.
Prohibited	Total number of received ICMPv6 Administratively Prohibited Unreachable packets.
Hop count exceeded	Total number of received ICMPv6 packets whose hops exceed the limit.
Parameter problem	Total number of received ICMPv6 Parameter Problem packets.
Too big	Total number of received ICMPv6 packets that are oversized.
Echoed	Total number of received ICMPv6 Echo Request packets.
Echo replied	Total number of received ICMPv6 Echo Reply packets.
Router solicit	Total number of received RS packets.
Router advert	Total number of received RA packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Neighbor solicit	Total number of received NS packets.
Neighbor advert	Total number of received NA packets.
Redirected	Total number of received ICMPv6 Redirect packets.
Rate limited	Total number of ICMPv6 packets that fail to be received because of the rate limit.

Related Topics

8.8.13 display ipv6 statistics

8.8.6 display ipv6 address-policy

Function

The **display ipv6 address-policy** command displays address selection policy entries.

Format

display ipv6 address-policy [**vpn-instance** *vpn-instance-name*] { **all** | *ipv6-address prefix-length* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays address selection policy entries of a specified VPN instance.	The value must be an existing VPN instance.
all	Displays all address selection policy entries.	-
ipv6-address	Specifies an IPv6 address prefix.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When using this command, pay attention to the following points:

- If the **all** parameter is specified, all address selection policy entries including the default ones are displayed.
- If the *ipv6-address prefix-length* parameter is specified, address selection policy entries of the specific prefix are displayed.

Precautions

If no address selection policy entry is configured, this command displays only the default address selection policy entries. These entries are prefixed with ::1, ::, 2002::, FC00::, and ::FFFF:0.0.0.0.

Example

Display address selection policy entries of VPN instance R1_VPN6.

```
<Huawei> display ipv6 address-policy vpn-instance R1_VPN6 all
Policy Table :
            Total:5
-------------------------------------------------------------------------------
Prefix     : ::                                PrefixLength  : 0
Precedence : 40                                     Label        : 1
Default    : Yes

Prefix     : ::1                               PrefixLength  : 128
Precedence : 50                                     Label        : 0
Default    : Yes

Prefix     : ::FFFF:0.0.0.0                      PrefixLength  : 96
Precedence : 10                                     Label        : 4
Default    : Yes

Prefix     : 2002::                              PrefixLength  : 16
Precedence : 30                                     Label        : 2
Default    : Yes

Prefix     : FC00::                              PrefixLength  : 7
Precedence : 20                                     Label        : 3
Default    : Yes
-------------------------------------------------------------------------------
```

Table 8-80 Description of the display ipv6 address-policy command output

Item	Description
Policy Table	Address selection policy entries.
Total	Number of address selection policy entries.
Prefix	IPv6 address prefix.
PrefixLength	Length of the IPv6 address prefix.

Item	Description
Precedence	Priority of an IPv6 address when the address is the destination address.
Label	Priority of an IPv6 address when the address is the source address.
Default	Whether an address selection policy entry is the default policy entry: ● Yes: The policy entry is the default policy entry. ● No: The policy entry is not the default policy entry.

Related Topics

8.8.27 ipv6 address-policy

8.8.7 display ipv6 attack-source overlapping-fragment

Function

The **display ipv6 attack-source overlapping-fragment** displays source information about overlapping fragment attacks.

Format

display ipv6 attack-source overlapping-fragment

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When suffering from overlapping fragment attacks, you can use this command to view source information about attack packets. Source information includes the source and destination IP addresses of the packets, interface receiving the packets, source VLAN, source CE VLAN, and VPN to which the packets belongs. You can take proper actions on the attack source.

Example

Display source information about overlapping fragment attacks.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ipv6 attack-source overlapping-fragment
Attack-source overlapping fragment table:

-----------------------------------------------------------------------------
  Source IP          : FC00::1
  Destination IP     : FC00::2
  Interface name     : Eth0/0/0
  VPN name           :
  VLAN               : 0                          CEVLAN: 0
  Attacked time      : 2011-09-29 01:01:28
-----------------------------------------------------------------------------

Total: 1
```

Table 8-81 Description of the display ipv6 attack-source overlapping-fragment command output

Item	Description
Source IP	Source IPv6 address of an overlapping fragment attack packet.
Destination IP	Destination IPv6 address of the overlapping fragment attack packet.
Interface name	Interface that receives the overlapping fragment attack packet.
VPN name	Name of the VPN to which the overlapping fragment attack packet belongs.
VLAN	VLAN to which the overlapping fragment attack packet belongs.
CEVLAN	CE VLAN to which the overlapping fragment attack packet belongs.
Attacked time	Duration of the overlapping fragment attack.
Total	Number of pieces of source information about overlapping fragment attacks.

Related Topics

8.8.59 reset ipv6 attack-source overlapping-fragment

8.8.8 display ipv6 interface

Function

The **display ipv6 interface** command displays IPv6 information on an interface.

Format

display ipv6 interface [*interface-type interface-number* | **brief**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays IPv6 information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, IPv6 information on all interfaces configured with IPv6 addresses is displayed.	-
brief	Displays brief information about the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running this command, ensure that the interface is configured with an IPv6 address. If no IPv6 address is assigned to the interface, no interface information is displayed.

Example

Display IPv6 information on GE1/0/0.

```
<Huawei> display ipv6 interface gigabitethernet 1/0/0
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00
  Global unicast address(es):
    FC00::1, subnet is FC00::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF04:5D00
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  Hosts use stateless autoconfig for addresses
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-82 Description of the display ipv6 interface command output

Item	Description
link-local address	Link-local address configured on the interface. To configure a link-local address for an interface, run the **ipv6 address link-local** command.
Global unicast address(es)	Global unicast address configured on the interface. To configure a global unicast address for an interface, run the **ipv6 address** command.
Joined group address(es)	Addresses of all multicast groups that the interface joins.
MTU	MTU of the interface.
ND DAD is enabled	NS packets are sent when the system performs Duplicate Address Detection (DAD).
number of DAD attempts	Number of times duplicate address detection is performed.
ND reachable time	Neighbor reachable time.
ND retransmit interval	Retransmission interval.
Hosts use stateless autoconfig for addresses	Hosts obtain IPv6 addresses using stateless autoconfiguration.
ND stale time	Time period for the neighbor to keep the STALE state.

Related Topics

8.8.21 ipv6 address

8.8.9 display ipv6 interface tunnel

Function

The **display ipv6 interface tunnel** command displays IPv6 information on a tunnel interface.

Format

display ipv6 interface tunnel *interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Displays the tunnel interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display IPv6 information on Tunnel0/0/1.

```
<Huawei> display ipv6 interface tunnel 0/0/1
Tunnel0/0/1 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::201:102 [TENTATIVE]
  Global unicast address(es):
    ::2.1.1.2, subnet is ::/96 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF01:102
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Table 8-83 Description of the display ipv6 interface tunnel command output

Item	Description
Tunnel0/0/1 current state	Current status of the tunnel interface: ● UP: enabled ● DOWN: disabled When working properly, an IPv6 over IPv4 tunnel is in Up state.
IPv6 protocol current state	Current status of the link layer protocol: ● UP: enabled ● DOWN: disabled When working properly, an IPv6 over IPv4 tunnel is in Up state.
IPv6 is enabled	IPv6 is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link-local address	Link-local address. To configure a link-local address, run the **ipv6 address link-local** command.
Global unicast address(es)	IPv6 global unicast address. To configure an IPv6 global unicast address, run the **ipv6 address** command.
Joined group address(es)	Addresses of multicast groups that the interface joins.
MTU	MTU of the interface.
ND reachable time	Interval for ND unreachability detection.
ND retransmit interval	Interval for retransmitting ND packets.
Hosts use stateless autoconfig for addresses	Hosts obtain IPv6 addresses through stateless address autoconfiguration.

Related Topics

8.8.8 display ipv6 interface

8.8.10 display ipv6 neighbors

Function

The **display ipv6 neighbors** command displays information about neighbor entries.

Format

display ipv6 neighbors [*ipv6-address* | [**vid** *vid*] *interface-type interface-number* | **vpn-instance** *vpn-instance-name*]

display ipv6 neighbors *interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]

Parameters

Parameter	Description	Value
ipv6-address	Displays neighbor entries of a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
vid *vid*	Displays neighbor entries of a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays neighbor entries on a specified interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays neighbor entries of a specified VPN instance.	The value must be an existing VPN instance.
cevid *cevid*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ipv6 neighbors** command displays information about dynamic and static ND entries. The information helps you:

- Check whether the local routing device has learned MAC addresses from neighbors.
- Check the neighbor status of the local routing device, including neighbor unreachable, neighbor reachable, or unknown.

You can run one of the following commands as required:

- To view neighbor entries based on the neighbor IPv6 address, run the **display ipv6 neighbors** [*ipv6-address*] command.
- To view neighbor entries based on the neighbor interface number, run the **display ipv6 neighbors** *interface-type interface-number* command.

  To view neighbor entries on a VLANIF interface, run the **display ipv6 neighbors** [[**vid** *vlan-id*] *interface-type interface-number*] command or the **display ipv6 neighbors** [*interface-type interface-number* [**vid** *vid*]] command.
- To view neighbor entries on a QinQ or Dot1q termination sub-interface, run the **display ipv6 neighbors** [*interface-type interface-number* [**vid** *vid* [**cevid** *cevid*]]] command.

If no parameter is specified, the **display ipv6 neighbors** command displays all neighbor entries.

Example

Display neighbor entries on GE1/0/0.

```
<Huawei> display ipv6 neighbors gigabitethernet 1/0/0
--------------------------------------------------------------------------------
IPv6 Address : FC00::1
Link-layer   : 0000-1201-0102          State : REACH
Interface    : GE5/0/3                 Age   : 0
VLAN         : -                     CEVLAN: -
```

```
VPN name     :                        Is Router: FALSE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::82FB:6FF:FE35:45B6
Link-layer   : 80fb-0635-45b6                  State : STALE
Interface    : GE0/0/2                       Age   : 53
VLAN         : -                           CEVLAN: -
VPN name     :                               Is Router: TRUE
Secure FLAG  : UN-SECURE
--------------------------------------------------------------------------------
Total: 2        Dynamic: 2        Static: 0
```

Display neighbor entries of IPv6 address FC00::2.

```
<Huawei> display ipv6 neighbors fc00::2
--------------------------------------------------------------------------------
IPv6 Address : FC00::2
Link-layer   : 00e0-fc89-fe6e          State : STALE
Interface    : GE1/0/0                 Age   : 7
VLAN         : -                     CEVLAN: -
VPN name     :                         Is Router: FALSE
Secure FLAG  : UN-SECURE
--------------------------------------------------------------------------------
Total: 1        Dynamic: 1          Static: 0
```

Display neighbor entries of IPv6 VPN instance **vpnA**.

```
<Huawei> display ipv6 neighbors vpn-instance vpnA
--------------------------------------------------------------------------------
IPv6 Address : FE80::2E0:FCFF:FE8C:417D
Link-layer   : 00e0-fc8c-417d          State : STALE
Interface    : Eth4/2/0                Age   : #
VLAN         : -                     CEVLAN: -
VPN name     : vpnA                    Is Router: FALSE
Secure FLAG  : UN-SECURE

IPv6 Address : FE80::2E0:FCFF:FE95:DD66
Link-layer   : 00e0-fc95-dd66          State : STALE
Interface    : Eth4/2/0                Age   : #
VLAN         : -                     CEVLAN: -
VPN name     : vpnA                    Is Router: FALSE
--------------------------------------------------------------------------------
Total: 2        Dynamic: 2        Static: 0
```

Table 8-84 Description of the display ipv6 neighbors command output

Item	Description
IPv6 Address	IPv6 address of a neighbor.
Link-layer	Link layer address (MAC address) of a neighbor.

Item	Description
State	Status of a neighbor entry: ● INCMP: indicates that the neighbor is unreachable. When the address is being resolved, the link layer address of the neighbor is not detected. If resolution succeeds, the neighbor entry is in REACH state. ● REACH: indicates that the neighbor is reachable within a specified period. By default, the neighbor is reachable within 30s. If the period expires and the entry remains unused, the neighbor entry is in STALE state. ● STALE: indicates that whether the neighbor is reachable is unknown. The entry remains unused within a specified period. By default, the neighbor is reachable within 30s. A device does not detect neighbor reachability unless it needs to send packets to a neighbor. ● DELAY: indicates that whether the neighbor is reachable is unknown. A device has sent a packet to a neighbor. If the device does not receive any response from the neighbor within the specified period, the neighbor entry is in PROBE state. ● PROBE: indicates that whether the neighbor is reachable is unknown. A device has sent a packet to a neighbor to detect whether the neighbor is reachable. If the device receives a response from the neighbor within a specified period, the neighbor entry is in REACH state. Otherwise, the neighbor entry is in INCMP state.
Interface	Name of the interface to which the neighbor entry belongs.
Age	Aging time of the neighbor entry: ● The aging time of static entries is displayed as "-". ● The aging time of dynamic entries is the time elapsed since the neighbor becomes reachable, in minutes. If the neighbor is always unreachable, "#" is displayed (only for dynamic entries).
VLAN	ID of the VLAN to which the neighbor belongs.
VPN name	Name of a VPN instance to which the neighbor belongs.
CEVLAN	Inner VLAN ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Is Router	Whether an NA packet carries the R flag: ● If the NA packet carries the R flag, "TRUE" is displayed. In this case, the neighbor is a routing device. ● If the NA packet carries no R flag, "FALSE" is displayed. In this case, the neighbor may be a PC or a routing device that sends an NA packet carrying no R flag.
Secure FLAG	Whether the neighbor entry is secure: ● If the neighbor entry is static or the neighbor has the neighbor security function enabled, "SECURE" is displayed. ● If the neighbor entry is dynamic and the neighbor has no neighbor security function enabled, "UN-SECURE" is displayed.
Total	Total number of neighbor entries.
Dynamic	Number of dynamic neighbor entries.
Static	Number of static neighbor entries.

Related Topics

8.8.54 ipv6 neighbor

8.8.11 display ipv6 pathmtu

Function

The **display ipv6 pathmtu** command displays information about PMTU entries.

Format

display ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { *ipv6-address* | **all** | **dynamic** | **static** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays PMTU entries of a specified IPv6 VPN instance.	The value must be an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-address	Displays PMTU entries of a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
all	Displays all PMTU entries.	-
dynamic	Displays all dynamic PMTU entries.	-
static	Displays all static PMTU entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The path MTU (PMTU) discovery mechanism determines the maximum size of packets that can be transmitted on a path.

The **display ipv6 pathmtu** command displays information about dynamic and static PMTU entries. The device then fragments packets into a size smaller than the PMTU and forwards the fragmented packets.

Precautions

If no PMTU is set using the **8.8.55 ipv6 pathmtu** command, no static PMTU entry is displayed after the **display ipv6 pathmtu** command is run.

Example

Display all PMTU entries.

```
<Huawei> display ipv6 pathmtu all
IPv6 Destination Address              ZoneID  PathMTU  LifeTime(M)  Type
FC00::1                            0      1500     -            Static
--------------------------------------------------------------------------
Total: 1        Dynamic: 0      Static: 1
```

Display PMTU entries of VPN instance **vpn1**.

```
<Huawei> display ipv6 pathmtu vpn-instance vpn1 all
IPv6 Destination Address              ZoneID  PathMTU  LifeTime(M)  Type
FC00::1                             1      1600     -            Static
--------------------------------------------------------------------------
Total: 1        Dynamic: 0      Static: 1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 8-85 Description of the display ipv6 pathmtu command output

Item	Description
Total	Total number of PMTU entries.
Dynamic	Total number of dynamic PMTU entries.
Static	Total number of static PMTU entries.
IPv6 Destination Address	Destination IPv6 address.
ZoneID	Zone ID.
PathMTU	PMTU of an IPv6 address.
LifeTime(M)	Remaining lifetime of dynamic PMTU entries, in minutes. This field displays "-" for static entries.
Type	Type of the PMTU entry: ● Dynamic: dynamic entries ● Static: static entries

Related Topics

8.8.56 ipv6 pathmtu age

8.8.55 ipv6 pathmtu

8.8.12 display ipv6 socket

Function

The **display ipv6 socket** command displays information about IPv6 sockets.

If no parameter is specified, this command displays information about all types of sockets.

Format

display ipv6 [**ha**] **socket** [**socktype** *socket-type* | **task-id** *task-id* **socket-id** *socket-id*]

Parameters

Parameter	Description	Value
ha	Displays IPv6 socket information on the slave main control board.	-

Parameter	Description	Value
socktype *socket-type*	Specifies the type of a socket. The value can be: ● 1: indicates SOCK_STREAM, corresponding to the TCP-based socket. ● 2: indicates SOCK_DGRAM, corresponding to the UDP-based socket. ● 3: indicates SOCK_RAW, corresponding to the RawIP-based socket.	The value is an integer that ranges from 1 to 3.
socket-id *socket-id*	Specifies the socket ID.	The value is an integer that ranges from 1 to 131072.
task-id *task-id*	Specifies the task ID.	The value is an integer that ranges from 1 to 350.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To locate a fault, you can use this command to view detailed information about sockets of all types or a specified type.

Precautions

If there is no socket information, no information is displayed.

Example

Display information about a socket with a specified socket type, socket ID, and task ID.

```
<Huawei> display ipv6 socket
SOCK_STREAM:
Task = VTYD (14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
SOCK_DGRAM:
Task = VTYD (14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
```

```
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
```

Display information about the socket with socket type 1.

```
<Huawei> display ipv6 socket socktype 1
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC
```

Table 8-86 Description of the display ipv6 socket command output

Item	Description
SOCK_STREAM	One type of socket. Sockets are classified into the following types: ● SOCK_STREAM ● SOCK_DGRAM ● SOCK_RAW
Task = VTYD(14)	Type and ID of the task that invokes the socket. For example, **Task = VTYD(14)** shows that the task named VTYD uses the socket, with task ID 14.
socketid = 4	Socket ID.
Proto = 6	Protocol ID.
LA = ::->22, FA = ::->0	● LA: indicates the local address and local port number. ● FA: indicates the remote address and remote port number.
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,	● sndbuf: indicates the upper limit of the send buffer, in bytes. ● rcvbuf: indicates the upper limit of the receive buffer, in bytes. ● sb_cc: indicates the total number of sent bytes. ● rb_cc: indicates the total number of received bytes.
socket option	Socket option that has been set.
socket state	Socket status.

 Copyright © Huawei Technologies Co., Ltd.

8.8.13 display ipv6 statistics

Function

The **display ipv6 statistics** command displays IPv6 traffic statistics.

Format

display ipv6 statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays IPv6 traffic statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ipv6 statistics** command to view statistics on received and sent IPv6 packets.

During packet transmission, if the source node has fragmented packets, you can run this command to view the total number of IPv6 packets that are successfully fragmented and the total number of fragmented packets that have been sent, and then check whether the number of fragmented packets received by the destination node is correct.

Precautions

The total number of packets received by the device includes the number of forwarded packets, number of packets delivered by the routing device to the upper layer, and number of discarded packets.

Example

Display IPv6 traffic statistics on the device.

```
<Huawei> display ipv6 statistics
IPv6 Protocol:
  Sent packets:
```

```
  Total                : 2
  Local sent out       : 2          Forwarded            : 0
  Raw packets          : 0          Discarded            : 0
  Fragmented           : 0          Fragments            : 0
  Fragments failed     : 0          Multicast            : 2
Received packets:
  Total                : 0          Local host           : 0
  Hop count exceeded   : 0          Header error         : 0
  Too big              : 0          Routing failed       : 0
  Address error        : 0          Protocol error       : 0
  Truncated            : 0          Option error         : 0
  Fragments            : 0          Reassembled          : 0
  Reassembly timeout   : 0          Multicast            : 0
  Fragments overlap    : 0
  Extension header:
    Hop-by-hop options   : 0              Mobility header       : 0

    Destination options  : 0              Routing header        : 0

    Fragment header      : 0              Authentication header : 0

    Encapsulation header : 0              No header             : 0

    TLV length error     : 0              Header length error   : 0

    Unknown header type  : 0              Unknown TLV type      : 0
```

Table 8-87 Description of the display ipv6 statistics command output

Item	Description
Sent packets	Statistics about sent packets.
Total	Total number of sent packets.
Local sent out	Total number of packets sent by the local device.
Forwarded	Number of forwarded packets.
Raw packets	Total number of packets sent through the raw socket, such as ping or tracert packets.
Discarded	Total number of discarded packets.
Fragmented	Total number of IPv6 packets that are successfully fragmented.
Fragments	Total number of sent fragmented packets.
Fragments failed	Total number of IPv6 packets that fail to be fragmented.
Multicast	Total number of sent multicast packets.
Received packets	Statistics about received packets.
Total	Total number of received packets.

Item	Description
Local host	Total number of packets received by the local device.
Hop count exceeded	Total number of packets whose hops exceed the upper limit.
Header error	Total number of packets with incorrect packet header.
Too big	Total number of received packets that fail to be forwarded because of excessive size.
Routing failed	Total number of packets that fail to be routed.
Address error	Total number of packets with incorrect IP addresses.
Protocol error	Total number of packets with the incorrect protocol.
Truncated	Total number of packets discarded because the actual packet length is shorter than that specified in the packet length field.
Option error	Total number of packets that carry incorrect options.
Fragments	Total number of received fragmented packets.
Reassembled	Total number of packets that are successfully reassembled.
Reassembled timeout	Total number of packets that fail to be reassembled due to timeout.
Multicast	Total number of received multicast packets.
Fragments overlap	Total number of received fragmented packets that are overlapped.
Extension Header	Total count of the IPv6 extension headers
Hop-by-Hop Options	Total count of the hop-by-hop options headers
Mobility Header	Total count of the mobility headers
Destination Options	Total count of the destination options headers

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Routing Header	Total count of the routing options headers
Fragment Header	Total count of the fragment headers
Authentication Header	Total count of the authentication headers
Encapsulation Header	Total count of the encapsulation headers
No header	Total count of the packets without headers
TLV Length error	Total count of the extension headers in which the TLV length field is wrong
Header Length error	Total count of the extension headers in which the length field is wrong.
Unknown header type	Total count of the unknown extension header types
Unknown TLV type	Total count of the unknown TLV types

Related Topics

8.8.63 reset ipv6 statistics

8.8.14 display rawip ipv6 statistics

Function

The **display rawip ipv6 statistics** command displays Raw IPv6 packet statistics.

Format

display rawip ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rawip ipv6 statistics** command to view Raw IPv6 packet statistics, including:

- Statistics about received and sent Raw IPv6 packets
- Statistics about discarded Raw IPv6 packets

Example

Display Raw IPv6 packet statistics.

```
<Huawei> display rawip ipv6 statistics
 Received packets:
    total: 20
    packets sent for external pre processing: 0
    packets for which checksum has to be calculated: 0
    packets with invalid checksum : 0
    dropped packets due to socket buffer is full: 0
    dropped packets due to no matching socket: 20
    dropped multicast packets due to no matching socket: 0
 Sent packets:
    total (excluding ICMP6 packets): 0
```

Table 8-88 Description of the display rawip ipv6 statistics command output

Item	Description
total	Total number of received and sent packets.
packets sent for external pre processing	Number of received Raw IPv6 packets for external preprocessing.
packets for which checksum has to be calculated	Number of received Raw IPv6 packets for which checksum has been calculated.
packets with invalid checksum	Number of discarded Raw IPv6 packets with checksum errors.
dropped packets due to socket buffer is full	Number of Raw IPv6 packets that are discarded because the socket buffer is full.
dropped packets due to no matching socket	Number of discarded Raw IPv6 packets that do not match the receiving socket.
dropped multicast packets due to no matching socket	Number of discarded Raw IPv6 packets destined to a multicast address that do not match the receiving socket.

8.8.15 display tcp ipv6 authentication-statistics

Function

The **display tcp ipv6 authentication-statistics** command displays authentication statistics of a specified TCP6 connection.

Format

display tcp ipv6 authentication-statistics src-ip *src-ip* **src-port** *src-port* **dest-ip** *dest-ip* **dest-port** *dest-port*

Parameters

Parameter	Description	Value
src-ip *src-ip*	Specifies the source IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
src-port *src-port*	Specifies the source port.	The value is an integer that ranges from 0 to 65535.
dest-ip *dest-ip*	Specifies the destination IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
dest-port *dest-port*	Specifies the destination port.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display tcp ipv6 authentication-statistics** command to view authentication statistics of a specified TCP6 connection, including:

- Number of TCP6 packets with MD5 Option
- Number of TCP6 packets with Enhanced Authentication Option

Example

Display authentication statistics of a specified TCP6 connection.

```
<Huawei> display tcp ipv6 authentication-statistics src-ip fc00::1 src-port 3456 dest-ip fc00::5 dest-port
5678
MD5 Signature Option (MSO)is enabled |
 Enhanced Authentication Option (EAO)is enabled
Received packets:
    total: 0
    packets received with MSO: 0
    packets received with EAO: 0
    packets dropped due to MD5 authentication failure: 0
    packets dropped due to absence of MSO: 0
    packets dropped due to presence of MSO: 0
    packets dropped due to MAC authentication failure: 0
```

```
    packets dropped due to absence of active receive key: 0
    packets dropped due to invalid receive algorithm id: 0
    packets dropped due to absence of EAO: 0

Sent packets:
    total: 0
    packets sent with MSO: 0
    packets sent with EAO: 0
    packets not sent due to absence of active send key: 0
```

Table 8-89 Description of the display tcp ipv6 authentication-statistics command output

Item	Description
packets received with MSO	Total number of received TCP6 packets with MD5 Option.
packets received with EAO	Total number of received TCP6 packets with Enhanced Authentication Option.
packets dropped due to MD5 authentication failure	Total number of TCP6 packets discarded due to MD5 authentication failure.
packets dropped due to absence of MSO	Total number of TCP6 packets discarded due to absence of MD5 Option.
packets dropped due to presence of MSO	Total number of TCP6 packets discarded due to presence of MD5 Option.
packets dropped due to MAC authentication failure	Total number of TCP6 packets discarded due to MAC authentication failure.
packets dropped due to absence of active receive key	Total number of TCP6 packets discarded due to absence of active receive key.
packets dropped due to invalid receive algorithm id	Total number of TCP6 packets discarded due to invalid receive algorithm ID.
packets dropped due to absence of EAO	Total number of TCP6 packets discarded due to absence of Enhanced Authentication Option.
packets sent with MSO	Total number of sent TCP6 packets with MD5 Option.
packets sent with EAO	Total number of sent TCP6 packets with Enhanced Authentication Option.
packets not sent due to absence of active send key	Total number of TCP6 packets discarded due to absence of active send key.

Related Topics

8.8.65 reset tcp ipv6 authentication-statistics

8.8.16 display tcp ipv6 statistics

Function

The **display tcp ipv6 statistics** command displays IPv6 TCP traffic statistics.

Format

display tcp ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can check the network connection status according to the items in the command output:

- Established connections: You can view information about "Established connections" to check whether the number of connections exceeds the upper limit, and then determine whether to continue deploying services or adjust the load.
- Duplicate ACK packets: You can view information about "Duplicate ACK packets" to check whether the device is attacked by unknown ACK packets. If the device receives a large number of unknown ACK packets, the device may be attacked.
- Out-of-order packets: You can view information about "Out-of-order packets" to check network performance. If the network is in poor condition, a lot of out-of-order packets are generated.

Precautions

- The total number of received packets includes the number of forwarded packets, number of packets delivered to the upper layer, and number of discarded packets.
- Before running this command to view IPv6 TCP statistics within a specified period, run the **8.8.66 reset tcp ipv6 statistics** command to clear existing statistics.

Example

Display IPv6 TCP packet statistics.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display tcp ipv6 statistics
Received packets:
    total: 0
    total(64bit high-capacity counter): 0
    packets in sequence: 0 (0 bytes)
    window probe packets: 0
    window update packets: 0
    checksum error: 0
    offset error: 0
    short error: 0
    duplicate packets: 0 (0 bytes)
    partially duplicate packets: 0 (0 bytes)
    out-of-order packets: 0 (0 bytes)
    packets with data after window: 0 (0 bytes)
    packets after close: 0
    ACK packets: 0 (0 bytes)
    duplicate ACK packets: 0
    too much ACK packets: 0
    packets dropped due to MD5 authentication failure: 0
    packets dropped due to absence of MSO: 0
    packets dropped due to presence of MSO: 0
    packets received with MD5 Signature Option: 0
    packets dropped due to MAC authentication failure: 0
    packets dropped due to absence of active receive key: 0
    packets dropped due to invalid receive algorithm id: 0
    packets dropped due to absence of Enhanced Authentication Option: 0
    packets received with Enhanced Authentication Option: 0

Sent packets:
    total: 0
    urgent packets: 0
    total(64bit high-capacity counter): 0
    control packets: 0 (including 0 RST)
    window probe packets: 0
    window update packets: 0
    data packets: 0 (0 bytes)
    data packets retransmitted: 0 (0 bytes)
    ACK only packets: 0 (0 delayed)
    packets sent with MD5 Signature Option: 0
    packets sent with Enhanced Authentication Option: 0
    packets not sent due to absence of active send key: 0

Other Statistics:
    retransmitted timeout: 0
    connections dropped in retransmitted timeout: 0
    keepalive timeout: 0
    keepalive probe: 0
    keepalive timeout, so connections disconnected: 0
    initiated connections: 0
    accepted connections: 0
    established connections: 0
    closed connections: 0 (dropped: 0, initiated dropped: 0)
```

Table 8-90 Description of the display tcp ipv6 statistics command output

Item	Description
Received packets: total: 0	Total number of received packets.
total(64bit high-capacity counter)	Total number of received or sent packets counted by the 64-bit high-capacity counter.
packets in sequence	Number of packets received in sequence.

Item	Description
window probe packets	Number of received window probe packets.
window update packets	Number of received window update packets.
checksum error	Number of received packets with invalid checksum.
offset error	Number of received packets with incorrect TCP header length.
short error	Number of received packets with total length shorter than the set value in the packet header.
duplicate packets	Number of received duplicate packets.
partially duplicate packets	Number of received partially duplicate packets.
out-of-order packets	Number of received out-of-order packets.
packets with data after window	Number of received packets exceeding the receive window.
packets after close	Number of packets received after the connection is closed.
ACK packets	Number of received ACK packets.
duplicate ACK packets	Number of received duplicate ACK packets.
too much ACK packets	Number of received ACK packets with too large ACK values.
packets dropped due to MD5 authentication failure	Number of packets discarded due to MD5 authentication failure.
packets dropped due to absence of MSO	Number of packets discarded due to absence of MD5 Signature Option.
packets dropped due to presence of MSO	Number of packets discarded due to presence of MD5 Signature Option.
packets received with MD5 Signature Option	Number of received packets with MD5 Signature Option.
packets dropped due to MAC authentication failure	Number of packets discarded due to MAC authentication failure.
packets dropped due to absence of active receive key	Number of packets discarded due to absence of active receive key.
packets dropped due to invalid receive algorithm id	Number of packets discarded due to invalid receive algorithm ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
packets dropped due to absence of Enhanced Authentication Option	Number of packets discarded due to absence of Enhanced Authentication Option.
packets received with Enhanced Authentication Option	Number of received packets with Enhanced Authentication Option.
Sent packets: total: 0	Total number of sent packets.
urgent packets	Number of sent packets with the urgent pointer.
control packets	Number of sent control packets.
window probe packets	Number of sent window probe packets.
window update packets	Number of sent window update packets.
data packets	Number of sent data packets.
data packets retransmitted	Number of retransmitted data packets.
ACK only packets	Number of sent ACK only packets.
packets sent with MD5 Signature Option	Number of sent packets with MD5 Signature Option.
Other Statistics:	Other statistics.
retransmitted timeout	Number of retransmission timeout packets.
connections dropped in retransmitted timeout	Number of disconnected connections during the retransmission timeout.
keepalive timeout	Number of Keepalive timeouts.
keepalive probe	Number of Keepalive probes.
keepalive timeout, so connections disconnected	Number of connections disconnected due to Keepalive timeout.
initiated connections	Number of initiated connections.
accepted connections	Number of accepted connections.
established connections	Number of established connections.
closed connections	Number of closed connections.
dropped	Number of disconnected connections.
initiated dropped	Number of initiated and disconnected connections.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.8.66 reset tcp ipv6 statistics

8.8.17 display tcp ipv6 status

Function

The **display tcp ipv6 status** command displays the status of all IPv6 TCP connections.

Format

display tcp ipv6 status [**local-ip** *ipv6-address*] [**local-port** *local-port*] [**remote-ip** *ipv6-address*] [**remote-port** *remote-port*]

display tcp ipv6 status [**task-id** *task-id* [**sock-id** *sock-id*]]

Parameters

Parameter	Description	Value
local-ip *ipv6-address*	Displays the IPv6 TCP connection status of the specified IPv6 address. *ipv6-address* specifies the IPv6 address of the local device.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
local-port *local-port*	Displays the IPv6 TCP connection status of the specified port number. *local-port* specifies the port number of the local device.	The value is an integer that ranges from 0 to 65535.
remote-ip *ipv6-address*	Displays the IPv6 TCP connection status of the specified IPv6 address. *ipv6-address* specifies the IPv6 address of the remote device.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
remote-port *remote-port*	Displays the IPv6 TCP connection status of the specified port number. *remote-port* specifies the port number of the remote device.	The value is an integer that ranges from 0 to 65535.
task-id *task-id*	Displays the status of the IPv6 TCP connection with the specified task ID. *task-id* specifies the task ID.	The value is an integer that ranges from 1 to 200.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sock-id *sock-id*	Displays the status of the IPv6 TCP connection with the specified socket ID.	The value is an integer that ranges from 1 to 131072.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display tcp ipv6 status** command to view all valid IPv6 TCP control blocks, including the following information:

- IPv6 TCP socket ID
- APP CID
- Local IPv6 address and port number
- Remote IPv6 address and port number
- IPv6 TCP connection status
- VPN ID

To view the status of all valid IPv6 TCP connections, run the **display tcp ipv6 status** [**local-ip** *ipv6-address*] [**local-port** *local-port-number*] [**remote-ip** *ipv6-address*] [**remote-port** *remote-port-number*] command.

To view the status of the IPv6 TCP connection with a specified socket ID, run the **display tcp ipv6 status** [**task-id** *task-id* [**sock-id** *sock-id*]] command.

Precautions

If there is no TCP connection, no information is displayed.

Example

Display the status of IPv6 TCP connections.

```
<Huawei> display tcp ipv6 status
* - MD5 Authentication is enabled.
# - Keychain Authentication is enabled.
TCP6CB   TID/SoID  Local Address        Foreign Address      State        VPNID
19490ba4 9/2       ::->23               ::->0                Listening    23553
```

Table 8-91 Description of the **display tcp ipv6 status** command output

Item	Description
TCP6CB	Address of an IPv6 TCP control block, in hexadecimal notation.
TID/SoID	Task ID and socket ID.
Local Address	Local IPv6 address and port number.
Foreign Address	Remote IPv6 address and port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of an IPv6 TCP connection: ● Closed: indicates that the TCP connection is closed. ● Listening: indicates that the TCP connection is being listened on. ● Syn_Rcvd: indicates that a TCP packet with the SYN flag is received. ● Syn_Sent: indicates that a TCP packet with the SYN flag is sent. ● Established: indicates that the TCP connection has been set up. ● Close_Wait: indicates that a user host sends a packet with the FIN flag to the server, requesting the server to close the TCP connection in Established state. The server then sends an ACK packet to the user host after receiving the packet and enters the Close_Wait state. ● Fin_Wait1: indicates that a user host sends a packet with the FIN flag to the server, requesting the server to close the TCP connection and enters the Fin_Wait1 state. ● Fin_Wait2: indicates that a user host receives an ACK packet in a response to the sent packet with the FIN flag and enters the Fin_Wait2 state. ● Time_Wait: indicates that TCP enters this state after the TCP connection is closed. When TCP has been in Time_Wait state two times the longest packet lifetime, records about the closed connection are deleted. ● Closing: indicates that the two ends close the TCP connection simultaneously. ● LAST_ACK: indicates that the local end waits for acknowledging the TCP connection teardown request sent to the remote end.
VPNID	VPN interface ID.

 Copyright © Huawei Technologies Co., Ltd.

8.8.18 display this ipv6 interface

Function

The **display this ipv6 interface** command displays IPv6 information on the current interface.

Format

display this ipv6 interface

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After an IPv6 address is configured in the interface view, you can run the **display this ipv6 interface** command to check IPv6 information on the interface.

Example

Display IPv6 information on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] display this ipv6 interface
GigabitEthernet1/0/0 current state : UP
IPv6 protocol current state : UP
IPv6 is enabled, link-local address is FE80::2E0:4AFF:FE3D:9801
  Global unicast address(es):
    2001::1, subnet is 2001::/64
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF3D:9801
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  ND stale time is 1200 seconds
  Hosts use stateless autoconfig for addresses
```

Table 8-92 Description of the display this ipv6 interface command output

Item	Description
GigabitEthernet1/0/0 current state	Current physical status of GE1/0/0.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPv6 protocol current state	Current protocol status of the interface.
link-local address	Link-local address configured on the interface.
Global unicast address(es)	Global unicast address configured on the interface.
Joined group address(es)	Addresses of all multicast groups that the interface joins.
MTU	MTU of the interface.
number of DAD attempts	Number of times duplicate address detection is performed.
ND reachable time	Neighbor reachable time.
ND retransmit interval	Retransmission interval.
Hosts use stateless autoconfig for addresses	Hosts obtain addresses using stateless autoconfiguration.
ND stale time	Time period for the neighbor to keep the STALE state.

Related Topics

8.8.8 display ipv6 interface

8.8.19 display udp ipv6 statistics

Function

The **display udp ipv6 statistics** command displays IPv6 UDP packet statistics.

Format

display udp ipv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The User Datagram Protocol (UDP) is a simple protocol that exchanges packets on the Internet. You can run the **display udp ipv6 statistics** command to view statistics about sent and received IPv6 UDP packets.

Precautions

The total number of packets received by the device includes the number of forwarded packets, number of packets delivered by the device to the upper layer, and number of discarded packets.

Example

Display IPv6 UDP packet statistics.

```
<Huawei> display udp ipv6 statistics
Received packets:
    total: 0
    total(64bit high-capacity counter): 0
    checksum error: 0
    shorter than header: 0
    invalid message length: 0
    no socket on port: 0
    no multicast port: 0
    not delivered, input socket full: 0
    input packets missing pcb cache: 0
    packets sent for external pre processing: 0

Sent packets:
    total: 0
    total(64bit high-capacity counter): 0
```

Table 8-93 Description of the display udp ipv6 statistics command output

Item	Description
Received packets	Number of received packets.
total	Total number of received and sent packets.
checksum error	Total number of packets with invalid checksum.
shorter than header	Total number of IPv6 UDP packets with the length shorter than the packet header.
invalid message length	Total number of packets whose data length is longer than the packet length.
no socket on port	Number of packets without corresponding sockets on the interface.
no multicast port	Number of received packets carrying nonexistent multicast interfaces.
not delivered, input socket full	Number of unprocessed packets when the buffer is full.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
input packet missing pcb cache	Number of received packets failing to find the PCB cache.
packets sent for external pre processing	Number of received packets for external preprocessing.
Sent packets	Number of sent packets.

8.8.20 ipv6

Function

The **ipv6** command enables the device to forward IPv6 unicast packets, including sending and receiving local IPv6 packets.

The **undo ipv6** command disables the device from forwarding IPv6 unicast packets.

By default, a device is disabled from forwarding IPv6 unicast packets.

Format

ipv6

undo ipv6

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You must run the **ipv6** command in the system view before performing IPv6 configurations.

Example

Enable the device to forward IPv6 unicast packets.

```
<Huawei> system-view
[Huawei] ipv6
```

Disable the device from forwarding IPv6 unicast packets.

```
<Huawei> system-view
[Huawei] undo ipv6
Warning: This operation will interrupt all IPv6 services. Continue?[Y/N]:y
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.21 ipv6 address

Function

The **ipv6 address** command configures a global unicast address for an interface.

The **ipv6 address** *dhcpv6-prefix* command configures an IPv6 address bound to the DHCPv6 PD prefix for an interface.

The **undo ipv6 address** command deletes a global unicast address from an interface.

The **undo ipv6 address** *dhcpv6-prefix* command deletes the IPv6 address bound to the DHCPv6 PD prefix for an interface.

By default, no global unicast address is configured for an interface.

By default, no IPv6 address bound to the DHCPv6 PD prefix is configured for an interface.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* }

ipv6 address *dhcpv6-prefix* { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*|*prefix-length*]

undo ipv6 address *dhcpv6-prefix*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.
dhcpv6-prefix	Specifies the prefix assigned to a DHCPv6 PD client.	The value is a string of 1to 63 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A global unicast address is similar to an IPv4 public network address. Global unicast addresses are used on the links that can be summarized, and are provided for the Internet Service Providers (ISPs). These addresses allow route prefix summarization, limiting global routing entries. A global unicast address consists of a 48-bit route prefix managed by carriers, a 16-bit subnet ID managed by local nodes, and a 64-bit interface ID.

The device is required to function as a DHCPv6 PD client and obtain an IPv6 address prefix from the DHCPv6 PD server. You can run the **ipv6 address** *dhcpv6-prefix* { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* } command to configure an IPv6 address is bound to the DHCPv6 PD prefix. After you run this command, the device uses the prefix assigned to the DHCPv6 PD client and the IPv6 address to form an RA prefix for the interface only when the device functions as a DHCPv6 PD client and obtains a prefix. The prefix must be a 64-digit number. If not, the host cannot use this prefix for automatic assignment of IPv6 addresses.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The following conditions are prohibited for different interfaces on the same device:

- The IPv6 addresses are the same.
- The network prefixes of the IPv6 addresses are the same. For example, if the IPv6 address of interface A is 2001:db8::1/12 and its network prefix is 200:: and the IPv6 address of interface B is 2001:db8::1/127 and its network prefix is 2001:db8::, the configuration succeeds. If the IPv6 address of interface B is also 2002:db8::1/12 and its network prefix is also 200::, the configuration fails.
- A device functions as a DHCPv6 PD client and obtains an IPv6 address prefix from a DHCPv6 PD server. You can run the **ipv6 address** *dhcpv6-prefix*{ *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* }command to configure an IPv6 address bound to a DHCPv6 prefix on an interface. For example, if the ipv6 address dhcpv6-prefix1 ::1:0:0:0:1/64 and ipv6 address dhcpv6-prefix1 ::1:0:0:0:2/64 commands are configured on interfaces A and B respectively, the network prefixes of interfaces A and B are the same. As a result, the configuration is successful but takes effect only on one interface. If the preceding case occurs, check whether any address conflict exists.

A maximum of 10 global unicast addresses can be configured for an interface.

An IPv6 address with a 128-bit prefix can be configured only on a loopback interface.

 Copyright © Huawei Technologies Co., Ltd.

After the **ipv6 address** command is run to configure a global unicast address for an interface, the system generates a link-local address for the interface, if no link-local address is configured for the interface.

If no parameter (IPv6 address or prefix length) is specified in the **undo ipv6 address** command, all IPv6 addresses configured for the interface are deleted after the command is run.

Example

Configure global unicast address 2001::1/64 for GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address 2001::1 64
```

Configure an IPv6 address bound to the DHCPv6 PD prefix for GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address prefix1 ::1:0:0:0:1/64
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.22 ipv6 address anycast

Function

The **ipv6 address anycast** command configures an IPv6 anycast address.

The **undo ipv6 address** command deletes an IPv6 anycast address.

By default, no IPv6 anycast address is configured.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*|*prefix-length* } **anycast**

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*|*prefix-length*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An anycast address identifies a group of interfaces, which usually belong to different nodes. Packets sent to an anycast address are delivered to the nearest interface that is identified by the anycast address, depending on the routing protocols.

To implement communication between a 6to4 network and a local (native) IPv6 network using a 6to4 tunnel, configure an anycast address with prefix 2002:c058:6301:: for the tunnel interface of a 6to4 relay agent.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If no parameter is specified in the **undo ipv6 address** command, all IPv6 addresses except link-local addresses are deleted.

An anycast address cannot be used as the source address of a packet. Therefore, a global unicast address must be configured when a device needs to send packets.

An IPv6 address with a 128-bit prefix can be configured only on a loopback interface.

Example

Configure anycast address fc00:c058:6301::/48 for Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4 6to4
[Huawei-Tunnel0/0/1] ipv6 enable
[Huawei-Tunnel0/0/1] ipv6 address fc00:c058:6301:: 48 anycast
```

Related Topics

8.8.8 display ipv6 interface
8.8.28 ipv6 enable (interface view)

 Copyright © Huawei Technologies Co., Ltd.

8.8.23 ipv6 address auto global

Function

The **ipv6 address auto global** command enables a device to generate an IPv6 global address through stateless autoconfiguration.

The **undo ipv6 address auto global** command disables a device from generating an IPv6 global address through stateless autoconfiguration.

By default, the device is disabled from generating an IPv6 global address through stateless autoconfiguration.

Format

ipv6 address auto global [**local-identifier**] [**default**]

undo ipv6 address auto global

Parameters

Parameter	Description	Value
default	Indicates that the device learns the default route.	-
local-identifier	Indicates the interface identifier of a local link address based on which a global address is generated.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ipv6 address auto global** command is run, a device automatically generates an IPv6 global unicast address on the interface that receives a RA packet. The generated IPv6 address contains the address prefix in the received RA packet and interface identifier of the device. If the device does not receive RA packets, the device can only automatically configures a link-local address to interconnect with local nodes.

- If the **local-identifier** parameter is not specified, an interface identifier is generated in EUI-64 mode, and this identifier works together with the prefix in RA packets to composite a global address.
- If the **local-identifier** parameter is not specified, the interface identifier of the local link address is used to work together with the prefix in RA packets to composite a global address.

 Copyright © Huawei Technologies Co., Ltd.

A local link address can be generated either statically or dynamically. If the local link address is generated dynamically, this mode equals the EUI-64 mode, and the global address generated in this way is the same as that with the **local-identifier** parameter is specified. If the local link address is statically configured, the interface identifier of the global address is from the configuration of the local link address, which is different from the result with the **local-identifier** parameter not specified. You can choose the generation mode as required.

After the **ipv6 address auto global default** command is run, a device generates an IPv6 address based on the received RA packet and learns the source address in the RA packet. The device then uses the source IPv6 address as the next hop address of the default IPv6 route.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After the **ipv6 address auto global** command is run, if an interface receives a new RA packet, a new IPv6 address is generated for the interface based on the received RA packet, but the default routes learned by the interface are not deleted.

If an interface has been configured with an IPv6 address, the original IPv6 address is not deleted after the interface receives an RA packet and generates a new IPv6 address. If the interface receives no RA packet and the generated IPv6 address expires, the interface deletes the generated IPv6 address and uses the original IPv6 address.

A device learns a maximum of three default routes based on RA packets. New routes cannot override the existing three routes, and extra routes will be discarded. If multiple default routes have the same priority, packets are forwarded in load balancing mode.

Example

Enable a device to generate an IPv6 global address through stateless autoconfiguration on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto global local-identifier
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.24 ipv6 address auto link-local

Function

The **ipv6 address auto link-local** command configures an interface to automatically generate a link-local address.

The **undo ipv6 address auto link-local** command deletes the automatically generated link-local address.

By default, no link-local address is automatically generated on an interface.

Format

ipv6 address auto link-local

undo ipv6 address auto link-local

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface automatically obtains a link-local address, it can implement neighbor discovery and automatically configure a global unicast address or a unique local address.

Prerequisites

Before running this command, run the **ipv6 enable** command in the interface view to enable the IPv6 function.

Example

Configure GE1/0/0 to automatically generate a link-local address.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
```

8.8.25 ipv6 address eui-64

Function

The **ipv6 address eui-64** command configures a global unicast address in EUI-64 format for an interface.

The **undo ipv6 address eui-64** command deletes a global unicast address in EUI-64 format from an interface.

 Copyright © Huawei Technologies Co., Ltd.

By default, no global unicast address in EUI-64 format is configured for an interface.

Format

ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **eui-64**

undo ipv6 address { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } **eui-64**

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128. In EUI-64 format, the value must be smaller than 64.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IPv6, any IPv6 unicast address needs an interface identifier. The interface identifier is globally unique, similar to a 48-bit MAC address.

The interface identifier of an IPv6 host address uses the IEEE EUI-64 format. A 64-bit interface identifier is generated based on an existing MAC address; therefore, such an interface identifier is globally unique. These 64-bit interface identifiers are globally valid for addressing and uniquely identify each network interface. An interface automatically configures an IPv6 address based on the network prefix obtained from an RA packet and the interface identifier in EUI-64 format.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The following conditions are prohibited for different interfaces on the same device:

- The IPv6 addresses are the same.

 Copyright © Huawei Technologies Co., Ltd.

- The network prefixes of the IPv6 addresses are the same. For example, if the IPv6 address of interface A is 2001:db8::1/12 and its network prefix is 200:: and the IPv6 address of interface B is 2001:db8::1/127 and its network prefix is 2001:db8::, the configuration succeeds. If the IPv6 address of interface B is also 2002:db8::1/12 and its network prefix is also 200::, the configuration fails.

A maximum of 10 global unicast addresses can be configured for an interface.

The **ipv6 address eui-64** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces, loopback interfaces, and tunnel interfaces.

After the **ipv6 address eui-64** command is run to configure an IPv6 address in EUI-64 format for an interface, the system generates a link-local address for the interface, if no link-local address is configured for the interface.

The following IPv6 addresses in EUI-64 format cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- Anycast address

The **ipv6 address** command is used to specify a 128–bit IP address. Using the **ipv6 address eui-64** command, you can specify the high-order 64 bits of an IPv6 address. The low-order 64 bits of an IP address are automatically generated in the EUI-64 format. Even when the low-order 64 bits are manually specified, the automatically generated ones will override them.

Example

Configure IPv6 address 2001::1/64 in EUI-64 format for GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address 2001::1 64 eui-64
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.26 ipv6 address link-local

Function

The **ipv6 address link-local** command configures a link-local address for an interface.

The **undo ipv6 address link-local** command deletes a link-local address on an interface.

By default, no link-local address is configured for an interface.

Format

ipv6 address *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an interface.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X. When a link-local address is being configured, the prefix of the specified IPv6 address must match FE80::/10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Link-local addresses are used for the communication between nodes on the same local link in neighbor discovery or stateless autoconfiguration.

You can run the **ipv6 address link-local** command to manually configure a link-local address for an interface.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

Avoid changing link-local addresses.

You can configure multiple IPv6 addresses but only one link-local address for an interface.

The link-local address configured using the **ipv6 address link-local** command will override the link-local address automatically generated by the system.

The following IPv6 addresses cannot be configured for an interface:

- Loopback address (::1/128)
- Unspecified address (::/128)
- Multicast address
- Anycast address

 Copyright © Huawei Technologies Co., Ltd.

- IPv4-mapped IPv6 address (0:0:0:0:0:FFFF:IPv4-address)

Example

Configure link-local address fe80::1 for GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address fe80::1 link-local
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.27 ipv6 address-policy

Function

The **ipv6 address-policy** command configures address selection policies.

The **undo ipv6 address-policy** command deletes address selection policies.

By default, the system has only default address selection policy entries. These entries are prefixed with ::1, ::, 2002::, FC00::, and ::FFFF:0.0.0.0.

Format

ipv6 address-policy [**vpn-instance** *vpn-instance-name*] *ipv6-address prefix-length precedence label*

undo ipv6 address-policy [**vpn-instance** *vpn-instance-name*] *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance.
ipv6-address	Specifies an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
precedence	Specifies the priority of an IPv6 address when the address is used as a destination address.	The value is an integer that ranges from 0 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
label	Specifies the priority of an IPv6 address when the address is used as a source address.	The value is an integer that ranges from 0 to 4294967295.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When source and destination addresses need to be specified and planned, you can use this command to define a group of policies for selecting addresses. These address selection policies form a policy table. This table is similar to a routing table, allowing you to perform a longest match lookup on address selection policy. An address is selected based on the source and destination addresses.

- A source address is selected based on the *label* parameter. The address whose *label* value is the same as the *label* value of the destination address is preferred as the source address.
- A destination address is selected based on the *label* and *precedence* parameters. If *label* values of the candidate addresses are the same, the address with the largest *precedence* value is preferred as the destination address.

Precautions

The system supports a maximum of 50 address selection policy entries.

The default policy entries are those prefixed with ::1, ::, 2002::, FC00::, and ::FFFF:0.0.0.0.

Default policy entries cannot be created using a command.

Example

Set the priorities of IPv6 address FC00:1::/64 to 15 and 20 respectively when the address is used as a source address and a destination address.

```
<Huawei> system-view
[Huawei] ipv6 address-policy vpn-instance one fc00:1:: 64 15 20
```

Related Topics

8.8.6 display ipv6 address-policy

8.8.28 ipv6 enable (interface view)

Function

The **ipv6 enable** command enables the IPv6 function on an interface.

The **undo ipv6 enable** command disables the IPv6 function on an interface.

By default, the IPv6 function is disabled on an interface.

Format

ipv6 enable

undo ipv6 enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can perform IPv6 configurations on an interface only when the interface has the IPv6 function enabled.

Prerequisites

The **ipv6** command has been run in the system view.

Precautions

The IPv6 function is not supported on MEth interfaces.

After the IPv6 function is disabled on an interface, IPv6 configurations on the interface are deleted. In addition, IS-IS IPv6 and RIPng are disabled on the interface. That is, the **isis ipv6 enable** and **ripng enable** commands become ineffective.

When the **ipv6 enable** command is run in the interface view, IPv6 is enabled on the interface. You can then perform IPv6 configurations on the interface. To configure an interface to forward IPv6 data, you must run the **ipv6** command in the system view to enable IPv6 forwarding. To enable an interface to forward IPv6 packets, you must enable IPv6 packet forwarding in the system view and interface view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the IPv6 function on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
```

Related Topics

8.8.20 ipv6

8.8.29 ipv6 icmp blackhole unreachable send

Function

The **ipv6 icmp blackhole unreachable send** command enables the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

The **undo ipv6 icmp blackhole unreachable send** command disables the terminal access from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

By default, the terminal access is disabled from sending a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

Format

ipv6 icmp blackhole unreachable send

undo ipv6 icmp blackhole unreachable send

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If static IPv6 blackhole routes are configured on the terminal access and a user goes offline, only the IPv6 blackhole route corresponding to the user's address segment exists on the terminal access. When a tracert packet matches the IPv6 blackhole route, the terminal access discards the packet. As a result, an initiator cannot detect that the user has gone offline.

 Copyright © Huawei Technologies Co., Ltd.

After you run the **ipv6 icmp blackhole unreachable send** command, the terminal access sends a Destination Unreachable ICMP packet to an initiator, notifying the initiator that the user has gone offline if a user goes offline and a tracert packet matches the IPv6 blackhole route.

Pre-configuration Tasks

Static IPv6 blackhole routes have been configured on the terminal access.

Example

Enable the terminal access to send a Destination Unreachable ICMP packet to an initiator when a tracert packet matches an IPv6 blackhole route.

```
<Huawei> system-view
[Huawei] ipv6 icmp blackhole unreachable send
```

Related Topics

8.7.18 icmp blackhole unreachable send

8.8.30 ipv6 icmp-error

Function

The **ipv6 icmp-error** command sets the rate limit for sending ICMPv6 error packets.

The **undo ipv6 icmp-error** command restores the default rate limit for sending ICMPv6 error packets.

By default, the size of the token buckets is 10 and the limit rate is 100 milliseconds.

Format

ipv6 icmp-error { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

Parameters

Parameter	Description	Value
bucket *bucket-size*	Specifies the maximum number of tokens the bucket can hold.	The value is an integer that ranges from 1 to 200. The default value is 10, which is recommended.
ratelimit *interval*	Specifies the interval for placing tokens into the bucket.	The value is an integer that ranges from 0 to 2147483647, in milliseconds. The default value is 100, which is recommended.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a network is not attacked, a routing device can correctly send ICMPv6 error packets to notify other devices of exceptions in packet transmission. If an attacker frequently sends ICMPv6 packets to network devices, the network devices will be busy responding with ICMPv6 packets. This affects system throughput and CPU usage. To prevent the system from sending a great number of ICMPv6 packets, run the **ipv6 icmp-error** command to limit the rate at which ICMPv6 packets are sent.

In the token bucket algorithm, one token represents an ICMPv6 packet. The system places tokens into the virtual bucket at a certain interval until the number of tokens in the bucket reaches the upper limit. When an ICMPv6 error packet is sent, a token is taken out of the token bucket. When there is no token, excess ICMPv6 error packets are discarded. You can limit the rate at which ICMPv6 packets are sent by setting the bucket size and the interval for placing tokens into the bucket.

Precautions

If you run the **ipv6 icmp-error** command multiple times, only the latest configuration takes effect.

If the interval for placing tokens into the bucket is 0, there is no limit on the interval.

Example

Set the rate limit for sending ICMPv6 error packets to 100.

```
<Huawei> system-view
[Huawei] ipv6 icmp-error ratelimit 100
```

Set the bucket size of ICMPv6 to 50.

```
<Huawei> system-view
[Huawei] ipv6 icmp-error bucket 50
```

Set the rate limit for sending ICMPv6 error packets to 100 and the bucket size to 50.

```
<Huawei> system-view
[Huawei] ipv6 icmp-error bucket 50 ratelimit 100
```

8.8.31 ipv6 icmp port-unreachable send

Function

The **ipv6 icmp port-unreachable send** command enables an interface to send ICMPv6 Port Unreachable messages.

The **undo ipv6 icmp port-unreachable send** command disables the function.

By default, the enabling status of the function that the interface sends ICMPv6 Port Unreachable messages is the same as that of the function that the system sends ICMPv6 Port Unreachable messages.

Format

ipv6 icmp port-unreachable send

undo ipv6 icmp port-unreachable send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a router receives a TCP6/UDP6 packet but cannot find the corresponding socket entry, the router replies with an ICMPv6 Port Unreachable message. This ICMPv6 error message carries the IPv6 address of the router as its source IPv6 address, which exposes the IPv6 address of the router and brings security risks. If the router is attacked by flooding packets, the router keeps replying with ICMPv6 Port Unreachable messages, causing high CPU usage and affecting device performance. To address this problem, run the **undo ipv6 icmp port-unreachable send** command on the inbound interface of ICMPv6 packets to disable the transmission of ICMPv6 Port Unreachable message.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Example

Enable GE 1/0/0 to send ICMPv6 Port Unreachable messages.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 icmp port-unreachable send
```

8.8.32 ipv6 icmp hop-limit-exceeded send

Function

The **ipv6 icmp hop-limit-exceeded send** command enables an interface to send ICMPv6 Hop Limit Exceeded messages.

The **undo ipv6 icmp hop-limit-exceeded send** command disables the function.

By default, the enabling status of the function that the interface sends ICMPv6 Hop Limit Exceeded messages is the same as that of the function that the system sends ICMPv6 Hop Limit Exceeded messages.

Format

ipv6 icmp hop-limit-exceeded send

undo ipv6 icmp hop-limit-exceeded send

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If a router receives a packet with a hop limit of 1, it replies with an ICMPv6 Hop Limit Exceeded message. This ICMPv6 error message carries the IPv6 address of the router as its source IPv6 address, which exposes the IPv6 address of the router and brings security risks. If the router is attacked by flooding packets, the router keeps replying with ICMPv6 Hop Limit Exceeded messages, causing high CPU usage and affecting device performance. To address this problem, run the **undo ipv6 icmp hop-limit-exceeded send** command on the inbound interface of ICMPv6 packets to disable the transmission of ICMPv6 Hop Limit Exceeded messages.

Example

Disable GE 1/0/0 from sending ICMPv6 Hop Limit Exceeded messages.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo ipv6 icmp hop-limit-exceeded send
```

8.8.33 ipv6 icmp receive

Function

The **ipv6 icmp receive** command enables the system to receive ICMPv6 packets.

The **undo ipv6 icmp receive** command disables the system from receiving ICMPv6 packets.

By default, the system receives ICMPv6 packets.

Format

ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **receive**

undo ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **receive**

Parameters

Parameter	Description	Value
icmpv6-type	Specifies the type of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-code	Specifies the code of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-name	Specifies the name of ICMPv6 packets.	ICMPv6 packets are classified into the following types: ● echo: Echo packet ● echo-reply: Echo Reply packet ● err-header-field: Packet with an error header ● frag-time-exceeded: Fragmentation Timeout packet ● hop-limit-exceeded: Packet whose hop count exceeds the limit ● host-admin-prohib: Packet that is rejected by a host ● host-unreachable: ICMPv6 Host Unreachable packet ● neighbor-advertisement: Neighbor Advertisement packet ● neighbor-solicitation: Neighbor Solicitation packet ● network-unreachable: ICMPv6 Network Unreachable packet ● packet-too-big: Packet Too Big packet ● port-unreachable: ICMPv6 Port Unreachable packet ● redirect: Redirected packets ● router-advertisement: Router Advertisement packet ● router-solicitation: Router Solicitation packet ● unknown-ipv6-opt: Error packet with unknown options ● unknown-next-hdr: Error packet with unknown next header

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all ICMPv6 packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is in good performance, devices can receive a proper number of ICMPv6 packets. However, when network traffic load is heavy, host unreachable or port unreachable events frequently occur, the devices receive a large number of ICMPv6 packets, which burdens the network and degrades device performance. In addition, attackers may use ICMPv6 error packets to probe the internal network topology.

To improve network performance and security, run the **undo ipv6 icmp receive** command to disable the system from receiving ICMPv6 Echo Reply packets, Host Unreachable packets, and Port Unreachable packets.

Precautions

When the network is in good performance again, you can run the **ipv6 icmp receive** command to enable the system to receive ICMPv6 packets.

After the **undo ipv6 icmp receive** command is run, a main interface is disabled from processing ICMPv6 packets, and the system does not collect statistics about ICMP Echo Reply packets, Host Unreachable packets, and Port Unreachable packets. Only statistics about discarded packets are collected.

Example

Disable the system from receiving ICMPv6 Echo packets.

```
<Huawei> system-view
[Huawei] undo ipv6 icmp echo receive
```

8.8.34 ipv6 icmp send

Function

The **ipv6 icmp send** command enables the system to send ICMPv6 packets.

The **undo ipv6 icmp send** command disables the system from sending ICMPv6 packets.

By default, the system is enabled to send ICMPv6 packets.

Format

ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **send**

undo ipv6 icmp { *icmpv6-type icmpv6-code* | *icmpv6-name* | **all** } **send**

Parameters

Parameter	Description	Value
icmpv6-type	Specifies the type of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-code	Specifies the code of ICMPv6 packets.	The value is an integer that ranges from 0 to 255.
icmpv6-name	Specifies the name of ICMPv6 packets.	ICMPv6 packets are classified into the following types: ● echo: Echo packet ● echo-reply: Echo Reply packet ● err-header-field: Packet with an error header ● frag-time-exceeded: Fragmentation Timeout packet ● hop-limit-exceeded: Packet whose hop count exceeds the limit ● host-admin-prohib: Packet that is rejected by a host ● host-unreachable: ICMPv6 Host Unreachable packet ● neighbor-advertisement: Neighbor Advertisement packet ● neighbor-solicitation: Neighbor Solicitation packet ● network-unreachable: ICMPv6 Network Unreachable packet ● packet-too-big: Packet Too Big packet ● port-unreachable: ICMPv6 Port Unreachable packet ● redirect: ICMPv6 redirect message. ● router-advertisement: Router Advertisement packet ● router-solicitation: Router Solicitation packet ● unknown-ipv6-opt: Error packet with unknown options ● unknown-next-hdr: Error packet with unknown next header

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all ICMPv6 packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network is in good performance, routing devices can send or receive ICMPv6 packets. However, when network traffic load is heavy, host unreachable or port unreachable events frequently occur, the routing devices send a large number of ICMPv6 packets, which burdens the network and degrades the performance of the routing devices. In addition, attackers may use ICMPv6 error packets to probe the internal network topology.

To improve network performance and security, run the **undo ipv6 icmp send** command to disable the system from sending ICMPv6 packets.

Precautions

When the network is in good performance again, you can run the **ipv6 icmp send** command to enable the system to send ICMPv6 packets.

Example

Disable the system from sending all ICMPv6 packets packets.

```
<Huawei> system-view
[Huawei] undo ipv6 icmp all send
```

8.8.35 ipv6 icmp too-big-rate-limit

Function

The **ipv6 icmp too-big-rate-limit** command enables a device to limit oversized ICMPv6 error packets.

The **undo ipv6 icmp too-big-rate-limit** command disables a device from limiting oversized ICMPv6 error packets.

By default, a device limit oversized ICMPv6 error packets.

Format

ipv6 icmp too-big-rate-limit

undo ipv6 icmp too-big-rate-limit

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a host sends a large number of packets in a path with a small MTU, it may receive a large number of ICMPv6 error packets, affecting the processing of valid packets. This command limits the number of ICMPv6 error packets, ensuring host performance.

Example

Enable the device to limit oversized ICMPv6 error packets.

```
<Huawei> system-view
[Huawei] ipv6 icmp too-big-rate-limit
```

8.8.36 ipv6 mtu

Function

The **ipv6 mtu** command sets the MTU on the interface for sending IPv6 packets.

The **undo ipv6 mtu** command restores the default MTU of IPv6 packets on an interface.

By default, the MTU of IPv6 packets on an interface is 1500 bytes.

NOTE

- For the AR100 series, AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169EGW-L, AR169CVW, AR169CVW-4B4S, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, the default value on the tunnel interface of the IPv6 over IPv4 tunnel is 1480 bytes.

Format

ipv6 mtu *mtu*

undo ipv6 mtu

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mtu	Specifies the MTU value.	The value is an integer. The value of VE, VT, Dialer, GE, XGE, and Eth interfaces ranges from 1280 to 1610. The value of Eth, XGE sub-interfaces and GE sub-interfaces ranges from 1280 to 1606. The value of G.SHDSL and VDSL interfaces in the PTM mode ranges from 1280 to 1576. The value of PON, Async, Serial, POS, Cellular, Tunnel, VLANIF, Mp-group, and Eth-Trunk interfaces ranges from 1280 to 1500, in bytes. The default value is 1500.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After the MTU value is changed using this command, run the **shutdown** and **undo shutdown** or **5.1.14 restart (interface view)** commands to restart the interface to make the changed MTU take effect.

It is recommended that the MTU of IPv6 packets on an interface should not exceed the MTU of IPv4 packets on an interface. (You can run the **mtu** command to configure the MTU of IPv4 packets on an interface.)

NOTE

- When deploying PPPoE services through VT or the dialer interface, you are advised to configure the IPv6 MTU on an interface smaller than 1568.
- When deploying MPoE services through VT or the dialer interface, you are advised to configure the IPv6 MTU on an interface smaller than 1572.

Example

Set the MTU of IPv6 packets on GE1/0/0 to 1280 bytes.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 mtu 1280
```

8.8.37 ipv6 nd autoconfig managed-address-flag

Function

The **ipv6 nd autoconfig managed-address-flag** command sets the M flag of stateful autoconfiguration in an RA packet.

The **undo ipv6 nd autoconfig managed-address-flag** command deletes the M flag of stateful autoconfiguration in an RA packet.

By default, the "managed address configuration" flag (M flag) is not set in the RA message.

Format

ipv6 nd autoconfig managed-address-flag

undo ipv6 nd autoconfig managed-address-flag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the M flag is set, a host obtains an IPv6 address through stateful autoconfiguration.
- If the M flag is not set, a host uses stateless autoconfiguration to obtain an IPv6 address, that is, the host generates an IPv6 address based on the prefix information in the RA packet.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd autoconfig managed-address-flag** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

After the **ipv6 nd autoconfig managed-address-flag** command is run, a host can obtain configurations (excluding an IPv6 address) such as the router lifetime, neighbor reachable time, retransmission interval, and PMTU by means of stateful autoconfiguration even if the **ipv6 nd autoconfig other-flag** command is not run.

After the **display ipv6 interface** command is run, the command output shows that the attached hosts obtain IPv6 addresses through stateful autoconfiguration or stateless autoconfiguration.

The interface on the device cannot use stateful address autoconfiguration and stateless address autoconfiguration simultaneously to obtain IPv6 addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the M flag of stateful autoconfiguration on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd autoconfig managed-address-flag
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.38 ipv6 nd autoconfig other-flag

Function

The **ipv6 nd autoconfig other-flag** command sets the "other configuration" flag (O flag) of stateful autoconfiguration in an RA packet.

The **undo ipv6 nd autoconfig other-flag** command deletes the O flag of stateful autoconfiguration in an RA packet.

By default, the O flag is not set in the RA packet.

Format

ipv6 nd autoconfig other-flag

undo ipv6 nd autoconfig other-flag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the O flag is set, a host uses stateful autoconfiguration to obtain other configuration parameters (excluding an IPv6 address), including the router lifetime, neighbor reachable time, retransmission interval, and PMTU.
- If the O flag is not set, a host uses stateless autoconfiguration to obtain other configuration parameters, including the router lifetime, neighbor reachable time, retransmission interval, and PMTU. That is, the host obtains other configuration parameters through the RA packet advertised by routers.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd autoconfig other-flag** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

After the **ipv6 nd autoconfig managed-address-flag** command is run, a host can obtain other configurations (excluding IPv6 addresses) using stateful autoconfiguration even if the **ipv6 nd autoconfig other-flag** command is not run.

The interface on the device cannot use stateful autoconfiguration and stateless autoconfiguration simultaneously to obtain other configuration parameters excluding IPv6 addresses.

Example

Set the O flag of stateful autoconfiguration on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd autoconfig other-flag
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.39 ipv6 nd dad attempts

Function

The **ipv6 nd dad attempts** command sets the number of times NS packets are sent when the system performs Duplicate Address Detection (DAD).

The **undo ipv6 nd dad attempts** command restores the default value.

By default, the number of times NS packets are sent when the system performs DAD is 1.

Format

ipv6 nd dad attempts *value*

undo ipv6 nd dad attempts

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
value	Specifies the number of times NS packets are sent when the system performs DAD.	The value is an integer that ranges from 0 to 600. The default value is 1, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure an IPv6 address (a global unicast address or a link-local address) for an interface, check whether other interfaces connected to this interface have used the IPv6 address to be configured to prevent address conflicts.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd dad attempts** command applies to the following interfaces: Ethernet interfaces and sub-interfaces, GE interfaces and sub-interfaces, serial interfaces (only serial interfaces enabled with PPP or HDLC support the IPv6 function), VT interfaces, VE interfaces, Eth-Trunk interfaces and sub-interfaces, VLANIF interfaces, and tunnel interfaces.

If the number of times NS packets are sent when the system performs DAD is set 0, DAD is prohibited.

If the physical link connected to an interface fails, DAD cannot be performed on the interface.

Example

Set the number of times NS packets are sent when the system performs DAD to 20 on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd dad attempts 20
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.40 ipv6 nd hop-limit

Function

The **ipv6 nd hop-limit** command sets hop limit for IPv6 unicast packets initially sent by a device.

The **undo ipv6 nd hop-limit** command restores the hop limit for IPv6 unicast packets to the default value.

By default, the IPv6 unicast packets initially sent by a routing device can travel 64 hops.

Format

ipv6 nd hop-limit *limit*

undo ipv6 nd hop-limit

Parameters

Parameter	Description	Value
limit	Specifies the hop limit.	The value is an integer that ranges from 1 to 255. The default value is 64, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A hop limit on a device provides the following functions:

- Limiting the number of hops through which IPv6 unicast packets are allowed to travel.
- Functioning as a parameter in an RA packet to help a host automatically configure a hop limit (a limit on the number of hops through which IPv6 unicast packets initially sent by a host are allowed to travel).

Precautions

The hop limit for unicast packets is set using the **ipv6 nd hop-limit** command in the system view.

The hop limit for RA packets depends on the configuration of the **ipv6 nd hop-limit** command in the system view and the configuration of the **ipv6 nd ra hop-limit** command in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

- If the hop limit for RA packets is not set in the interface view or in the system view, the hop limit for RA packets is 64 by default.
- If the hop limit for RA packets is not set in the interface view, the value set using the **ipv6 nd hop-limit** command in the system view is used as the hop limit for RA packets.
- If the **ipv6 nd ra hop-limit** command is run in the interface view, the configuration in the interface view takes effect, no matter whether the hop limit is set in the system view.

The hop limit set for IPv6 unicast packets is the same as that set for RA packets. In the following cases, however, the hop limit for IPv6 unicast packets is 64, while the hop limit for RA packets is 0.

- No hop limit is set for IPv6 unicast packets. The default value takes effect.
- The **undo ipv6 nd hop-limit** command is run to restore the default hop limit set for IPv6 unicast packets.

After a host receives an RA packet with the hop limit of 0, it sets its hop limit to the default value 64, consistent with the default hop limit on the device.

Example

Set the hop limit for IPv6 unicast packets initially sent by a device to 100 in the system view.

```
<Huawei> system-view
[Huawei] ipv6 nd hop-limit 100
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.41 ipv6 nd learning strict

Function

The **ipv6 nd learning strict** command enables IPv6 neighbor discovery (ND) strict learning.

The **undo ipv6 nd learning strict** command disables IPv6 ND strict learning.

By default, IPv6 ND strict learning is disabled.

Format

In the system view:

ipv6 nd learning strict

undo ipv6 nd learning strict

In the interface view:

ipv6 nd learning strict { **force-disable** | **force-enable** | **trust** }

undo ipv6 nd learning strict

Parameters

Parameter	Description	Value
force-disable	Disables IPv6 ND strict learning forcibly.	-
force-enable	Enables IPv6 ND strict learning forcibly.	-
trust	Inherits the global setting of IPv6 ND strict learning.	-

Views

VLANIF interface view, Eth-trunk interface view, Eth-Trunk sub-interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device uses neighbor advertisement (NA) packets to establish neighbor entries, which does not comply with RFC. To comply with RFC 4861, run the **ipv6 nd learning strict** command to enable IPv6 ND strict learning. After you enable IPv6 ND strict learning on a device, the device uses NA packets only in response to neighbor solicitation (NS) packets to establish neighbor entries.

The **ipv6 nd learning strict** and **undo ipv6 nd learning strict** commands apply only to VLANIF interfaces, Eth-Trunk interfaces, and Eth-Trunk sub-interfaces.

Precautions

Before running this command in an Eth-Trunk view, run the **undo portswitch** command to switch the Eth-Trunk to a Layer 3 interface.

After you run the **ipv6 nd learning strict** command on a device, the device synchronizes fake entries. Synchronizing a large number of fake entries affects device performance. Therefore, you are advised to use the command only for protocol consistency tests.

Example

Enable IPv6 ND strict learning globally.

```
<Huawei> system-view
[Huawei] ipv6 nd learning strict
```

Enable IPv6 ND strict learning on VLANIF 100 forcibly.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ipv6 enable
[Huawei-Vlanif100] ipv6 nd learning strict force-enable
```

 Copyright © Huawei Technologies Co., Ltd.

8.8.42 ipv6 nd neighbor-limit

Function

The **ipv6 nd neighbor-limit** command configures the maximum number of dynamic neighbor entries that can be learned by an interface.

The **undo ipv6 nd neighbor-limit** command restores the default maximum number of dynamic neighbor entries that can be learned by an interface.

By default, an interface can learn a maximum of 1024 dynamic neighbor entries.

Format

ipv6 nd neighbor-limit *limit-number*

undo ipv6 nd neighbor-limit

Parameters

Parameter	Description	Value
limit-number	The maximum number of dynamic neighbor entries that can be learned by a specified interface.	The value is an integer in the range 2 to 4000.

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an interface learns too many neighbor entries, the processing load for the device will be increased and the performance of the device will be degraded. You can run the **ipv6 nd neighbor-limit** command to configure the maximum number of dynamic neighbor entries that can be learned by a specified interface.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command.

Example

Set the maximum number of dynamic neighbor entries that can be learned by the VLANIF100 interface to 10.

```
<Huawei> system-view
[Huawei] ipv6
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ipv6 enable
[Huawei-Vlanif100] ipv6 nd neighbor-limit 10
```

8.8.43 ipv6 nd ns multicast-enable

Function

The **ipv6 nd ns multicast-enable** command enables a QinQ or a dot1q termination sub-interface to send NS multicast packets.

The **undo ipv6 nd ns multicast-enable** command disables a QinQ or a dot1q termination sub-interface from sending NS multicast packets.

By default, a QinQ or a dot1q termination sub-interface is disabled from sending NS multicast packets.

Format

ipv6 nd ns multicast-enable

undo ipv6 nd ns multicast-enable

Parameters

None

Views

Ethernet sub-interface view, GE sub-interface view, Eth-Trunk sub-interface view, XGE sub-interfaces

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A QinQ or a dot1q termination sub-interface on a routing device can send NS multicast packets to actively learn ND entries or respond to NS packets to passively learn ND entries.

When a QinQ or a dot1q termination sub-interface needs to send multicast NS packets to learn ND entries but there is no corresponding ND entry, you need to run this command to enable a QinQ or a dot1q termination sub-interface to send NS multicast packets.

Precautions

- If this command is not run on the termination sub-interface, the system discards the NS multicast packets.
- If this command is run on the termination sub-interface, the system tags an NS multicast packet and forwards it through the termination sub-interface.

 Copyright © Huawei Technologies Co., Ltd.

Sending multicast NS packets consumes CPU resources. Therefore, when the CPU performance of the system is rather low, you are advised not to enable a termination sub-interface to send NS multicast packets to actively learn ND entries but to respond to NS packets to passively learn ND entries.

Example

Enable the QinQ termination sub-interface GE2/0/0.1 to send NS multicast packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 2/0/0.1
[Huawei-GigabitEthernet2/0/0.1] qinq termination pe-vid 100 ce-vid 10
[Huawei-GigabitEthernet2/0/0.1] ipv6 enable
[Huawei-GigabitEthernet2/0/0.1] ipv6 nd ns multicast-enable
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.44 ipv6 nd ns retrans-timer

Function

The **ipv6 nd ns retrans-timer** command sets the interval for sending NS packets.

The **undo ipv6 nd ns retrans-timer** command restores the interval for sending NS packets to the default value.

By default, the interval for sending NS packets is 1000 ms.

Format

ipv6 nd ns retrans-timer *interval*

undo ipv6 nd ns retrans-timer

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NS packets.	The value is an integer that ranges from 1000 to 4294967295, in milliseconds. The default value is 1000 milliseconds, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting the interval for sending NS packets provides the following functions:

- Controlling the interval at which a local routing device detects neighbor reachability.
- Controlling the interval at which a local routing device performs DAD.
- Functioning as a parameter in an RA packet to instruct hosts to specify this interval as their own interval for sending NS packets.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 nd ns retrans-timer** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces, and tunnel interfaces.

Frequently sending NS packets causes high CPU usage, which affects the system performance. Therefore, you are advised to set the interval for sending NS packets to a larger value. The default interval, 1000 milliseconds, is recommended.

If you run the **ipv6 nd ns retrans-timer** command multiple times, only the latest configuration takes effect.

The interval for sending NS packets is the same as that for sending RA packets. In the following cases, however, the interval for sending NS packets is the default value1000 ms, while the interval for sending RA packets is 0 ms.

- No interval for sending NS packets is set. The default value takes effect.
- The **undo ipv6 nd ns retrans-timer** command is run to restore the interval for sending NS packets to the default value.

After a host receives an RA packet of which the sending interval is 0 ms from a device, the host sets the interval for sending NS packet to 1000 ms, the same as that on the device.

Example

Set the interval for sending NS packets to 10000 milliseconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ns retrans-timer 10000
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.45 ipv6 nd nud reachable-time

Function

The **ipv6 nd nud reachable-time** command sets the IPv6 neighbor reachable time.

The **undo ipv6 nd nud reachable-time** command restores the IPv6 neighbor reachable time to the default value.

By default, the IPv6 neighbor reachable time is 1200000 ms.

Format

ipv6 nd nud reachable-time *value*

undo ipv6 nd nud reachable-time

Parameters

Parameter	Description	Value
value	Specifies the IPv6 neighbor reachable time.	The value is an integer that ranges from 1 to 3600000, in milliseconds. The default value is 1200000 ms, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting the IPv6 neighbor reachable time provides the following functions:

- Controlling the aging time of neighbor entries on a local routing device.
- Being a parameter in an RA packet to enable a host to configure the neighbor reachable time.

Each RA packet sent by a routing device carries the neighbor reachable time. This allows all nodes along the same link to use the same neighbor reachable time.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

A shorter neighbor reachable time enables a routing device to detect neighbor reachability more quickly. However, this consumes more network bandwidth and

 Copyright © Huawei Technologies Co., Ltd.

CPU resources. Therefore, a short neighbor reachable time is not recommended on an IPv6 network. The default value, 1200000 ms, is recommended.

If you run the **ipv6 nd nud reachable-time** command multiple times, only the latest configuration takes effect.

The **ipv6 nd nud reachable-time** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The neighbor reachable time set on a routing device is the same as that carried in an RA packet. In the following cases, however, the neighbor reachable time set on a routing device is the default value 1200000 ms while the neighbor reachable time carried in the RA packet is 0 millisecond:

- No neighbor reachable time is set on the routing device. The default value takes effect.
- The **undo ipv6 nd nud reachable-time** command is run to restore the neighbor reachable time to the default value.

After a host receives an RA packet in which the neighbor reachable time is 0 ms, the host sets the neighbor reachable time to 1200000 ms, the same as that on the device.

Example

Set the neighbor reachable time to 10000 ms on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd nud reachable-time 10000
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.46 ipv6 nd ra

Function

The **ipv6 nd ra** command sets the interval for sending Router Advertisement packets.

The **undo ipv6 nd ra** command restores the interval for sending RA packets to the default value.

By default, the maximum interval is 600s and the minimum interval is 200s.

Format

ipv6 nd ra { **max-interval** *maximum-interval* | **min-interval** *minimum-interval* }

undo ipv6 nd ra { **max-interval** | **min-interval** }

Parameters

Parameter	Description	Value
max-interval *maximum-interval*	Specifies the maximum interval for sending RA packets.	The value is an integer that ranges from 4 to 1800, in seconds. The default value is 600 seconds, which is recommended. The maximum interval cannot be less than the minimum interval.
min-interval *minimum-interval*	Specifies the minimum interval for sending RA packets.	The value is an integer that ranges from 3 to 1350, in seconds. The default value is 200 seconds, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A routing device periodically sends RA packets. An RA packet carries both the IPv6 address prefix and the flag of stateful address autoconfiguration.

You can run the **ipv6 nd ra** command to change the interval for sending RA packets.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

Running the **ipv6 nd ra** command changes the interval for sending RA packets during DAD. Therefore, you are advised to use the default interval, that is, the maximum value is 600s and the minimum value is 200s.

If the **ipv6 nd ra** command is run multiple times, the latest configuration takes effect.

The **ipv6 nd ra** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The interval for sending RA packets cannot be longer than the lifetime of the RA packets. The default lifetime of the RA packets is 1800s and, you can run the **ipv6 nd ra router-lifetime** command to change the value.

 Copyright © Huawei Technologies Co., Ltd.

The actual interval for sending RA packets is a random value between *min-interval* and *max-interval*.

Example

Set the maximum interval for sending RA packets to 1000s on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra max-interval 1000
```

Set the minimum interval for sending RA packets to 300s on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra min-interval 300
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.47 ipv6 nd ra halt

Function

The **ipv6 nd ra halt** command disables the system from sending RA packets.

The **undo ipv6 nd ra halt** command enables the system to send RA packets.

By default, the system is disabled from sending RA packets.

Format

ipv6 nd ra halt

undo ipv6 nd ra halt

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When a device is connected to a host, it periodically sends RA packets to the host. An RA packet carries the IPv6 address prefix and flag information of stateful autoconfiguration. You can run the **undo ipv6 nd ra halt** command to enable the device to send RA packets.
- When a device is connected to another device, that is, there is no host on the network, sending RA packets is not required. The default configuration is recommended.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After the **ipv6 nd ra halt** command is run, the device does not send RA packets. In such a case, the hosts on the network cannot periodically receive information about updated IPv6 prefixes.

The **ipv6 nd ra halt** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces, and tunnel interfaces.

By default, the device is disabled from sending RA packets. You can run the **display icmpv6 statistics** command to check whether a local device has sent RA packets.

Example

Disable GE1/0/0 from sending RA packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra halt
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.48 ipv6 nd ra hop-limit

Function

The **ipv6 nd ra hop-limit** command sets the hop limit for RA packets.

The **undo ipv6 nd ra hop-limit** command restores the hop limit for RA packets to the default value.

By default, the hop limit for RA packets is 64.

Format

ipv6 nd ra hop-limit *limit*

undo ipv6 nd ra hop-limit

Parameters

Parameter	Description	Value
limit	Specifies the hop limit for RA packets.	The value is an integer that ranges from 0 to 255. The default value is 64, which is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As a parameter in an RA packet, the hop limit enables a host to automatically configure a hop limit (a limit on the number of hops through which IPv6 unicast packets initially sent by a host are allowed to travel).

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After this command is run on the router, the device discards the RA packet whose hop limit is different from its configuration.

- If the **ipv6 nd ra hop-limit** command is run on an interface, the hop limit for RA packets is determined by the interface configuration.
- If the **ipv6 nd ra hop-limit** command is not run on an interface, the hop limit for RA packets is determined by the hop limit configured using the **ipv6 nd hop-limit** command.

Example

Set the hop limit for RA packets sent by GE1/0/0 to 126.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra hop-limit 126
```

8.8.49 ipv6 nd ra preference

Function

The **ipv6 nd ra preference** command sets the priority of the default router in an RA packet.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 nd ra preference** command restores the priority of the default router in an RA packet to the default value.

By default, the priority of the default router in an RA packet is medium.

Format

ipv6 nd ra preference { **high** | **medium** | **low** }

undo ipv6 nd ra preference

Parameters

Parameter	Description	Value
high	Sets the default router priority to high.	-
medium	Sets the default router priority to medium.	-
low	Sets the default router priority to low.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple routers exist on the link where a host resides, the host chooses the forwarding router based on the destination address of the packet. Each router sends an RA packet that contains the default router priority and route information to the host, which helps the host choose the proper router based on the destination address.

The host updates its routing table after receiving the RA packet. To forward packets to other devices, the host checks the routing table to choose the proper route.

When the default router list of the host includes multiple entries, run this command to configure the router with the highest priority on the local link as the default router (gateway) of the host.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

By default, the router does not send RA packets. You need to run the **undo ipv6 nd ra halt** command to enable the router to send RA packets to the host.

Precautions

If the interface is being unbound from the VPN instance that has IPv6 address family enabled, the system displays a message, indicating that this command cannot be run.

Example

Set the priority of the default router in an RA packet to high on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra preference high
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.47 ipv6 nd ra halt

8.8.51 ipv6 nd ra route-information

8.8.50 ipv6 nd ra prefix

Function

The **ipv6 nd ra prefix** command configures the prefix in an RA packet.

The **undo ipv6 nd ra prefix** command deletes the prefix in an RA packet.

By default, an RA packet carries only the address prefix configured using the **ipv6 address** command.

Format

ipv6 nd ra prefix { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig**] [**off-link**]

undo ipv6 nd ra prefix { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

ipv6 nd ra prefix default no-advertise

undo ipv6 nd ra prefix default no-advertise

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address carried in the RA packet.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128. You can calculate the IPv6 prefix carried in the RA packet based on the IPv6 address and prefix length.
valid-lifetime	Specifies the valid lifetime of the prefix.	The value is an integer that ranges from 0 to 4294967295, in seconds.
preferred-lifetime	Specifies the preferred lifetime of the prefix.	The value is an integer that ranges from 0 to 4294967295, in seconds. The preferred lifetime cannot be larger than the valid lifetime.
no-autoconfig	Deletes the A-Flag. If this parameter is configured, a configured prefix cannot be used in stateless address allocation.	-
off-link	Specifies the O-Flag. If **off-link** is specified, the prefix carried in the RA packet cannot be allocated to the local link. When the host sends a packet to the address specified by this prefix, the packet is forwarded through a default router.	-
default no-advertise	Specifies that RA packets do not carry the default prefix generated based on the interface IPv6 address.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a routing device to advertise only a specified prefix, run the **ipv6 nd ra prefix** command to configure the prefix.

If a prefix has been configured using the **ipv6 nd ra prefix** command, the device advertises both prefixes configured using the **ipv6 nd ra prefix** and **ipv6 address** commands.

By default, RA packets carry the default prefix generated based on the interface IPv6 address. If the default setting is not required, run the **ipv6 nd ra prefix default no-advertise** command.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

After a host receives the RA packet with the prefix configured using the **ipv6 nd ra prefix** command, the host updates the local prefix information.

The **ipv6 nd ra prefix** command applies to the following interfaces: GE interfaces and sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The prefix configured using the **ipv6 nd ra prefix** command cannot be fe80:: (prefix of a link-local address), ff00:: (prefix of a multicast address), :: (prefix of an unspecified address), or the prefix that has been used by another interface (including the interface address prefix and prefix carried in RA packets).

Example

Configure the prefix in the RA packet on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra prefix fc00:1::100 128 1000 400 no-autoconfig
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra prefix fc00:2::100 64 1000 400 off-link
```

Configure RA packets on GE1/0/0 not to carry the default prefix.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra prefix default no-advertise
```

Related Topics

8.8.47 ipv6 nd ra halt

8.8.51 ipv6 nd ra route-information

Function

The **ipv6 nd ra route-information** command configures route option information in an RA packet.

The **undo ipv6 nd ra route-information** command deletes route option information in an RA packet.

By default, no route option information is configured in an RA packet.

Format

ipv6 nd ra route-information *ipv6-address prefix-length* **lifetime** *route-lifetime* [**preference** { **high** | **medium** | **low** }]

undo ipv6 nd ra route-information *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the prefix of an IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
lifetime *route-lifetime*	Specifies the route lifetime.	The value is an integer that ranges from 0 to 4294967295, in seconds.
preference	Specifies the route priority.	-
high	Sets the route priority to high.	-
medium	Sets the route priority to medium.	-
low	Sets the route priority to low.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RA packet contains route options. The router sends the specified routes to the hosts on the local network segment by using these route options. The hosts can send packets by using these routes.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

By default, the router does not send RA packets. You need to run the **undo ipv6 nd ra halt** command to enable the router to send RA packets to the host.

Precautions

The host updates its routing table after receiving the RA packet that carries route option information. To forward packets to other devices, the host checks the routing table to choose the proper route.

A maximum of 17 route options are supported on each interface.

Route option information cannot be configured for a loopback address.

Example

Configure route information of RA packets on GE1/0/0: setting the lifetime of the route with the destination address of FC00:1::1/64 to 1550s, and the priority of this route to high.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ipv6 nd ra halt
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra route-information fc00:1::1 64 lifetime 1550 preference high
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.47 ipv6 nd ra halt

8.8.49 ipv6 nd ra preference

8.8.52 ipv6 nd ra router-lifetime

Function

The **ipv6 nd ra router-lifetime** command sets the lifetime of RA packets.

The **undo ipv6 nd ra router-lifetime** command restores the lifetime of RA packets to the default value.

By default, the lifetime for RA messages is three times of the maximum interval for advertising RA messages.

Format

ipv6 nd ra router-lifetime *ra-lifetime*

undo ipv6 nd ra router-lifetime

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ra-lifetime	Specifies the lifetime of RA packets.	The value is an integer and can be 0 or ranges from 4 to 9000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device adds the lifetime value to an RA packet before sending the RA packet to the host on the local network segment. The lifetime of RA packet indicates the time that a router functions as the default gateway for a host.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

If a host receives an RA packet with the lifetime field being 0, the host does not add the address of the router to its default router table.

The **ipv6 nd ra router-lifetime** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, Eth-Trunk interfaces and sub-interfaces, POS interfaces (only POS interfaces enabled with PPP or HDLC support the IPv6 function), and tunnel interfaces.

The lifetime of the RA packets cannot be smaller than the interval for sending RA packets. By default, the maximum interval for sending RA packets is 600s and the minimum interval is 200s. You can run the **ipv6 nd ra** command to set the interval. If the set lifetime value of the RA packets is smaller than the set interval for sending RA packets, the system displays an error. In such a case, you need to reset the lifetime value.

Example

Set the lifetime of the RA packets on GE1/0/0 to 1000s.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd ra router-lifetime 1000
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.53 ipv6 nd stale-timeout

Function

The **ipv6 nd stale-timeout** command sets the aging time of ND entries in STALE state.

The **undo ipv6 nd stale-timeout** command restores the aging time of ND entries in STALE state to the default value.

By default, the aging time of ND entries in STALE state is 1200s in the system view and is not set in the interface view.

Format

ipv6 nd stale-timeout *timeout-value*

undo ipv6 nd stale-timeout

Parameters

Parameter	Description	Value
timeout-value	Specifies the aging time of ND entries in STALE state.	The value is an integer that ranges from 60 to 172800, in seconds. The default value is 1200s, which is recommended.

Views

System view and Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The STALE state of an ND entry indicates that whether the neighbor is reachable is unknown. A device does not detect the neighbor reachability unless packets need to be sent to a neighbor.

The aging time of ND entries in STALE state is configurable. To quickly clear invalid ND entries, set the aging time to a smaller value using the **ipv6 nd stale-timeout** command. This speeds up entry aging.

Prerequisites

The device is enabled to forward IPv6 packets using the **ipv6** command in the system view.

IPv6 has been enabled on the interface using the **ipv6 enable** command in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After the **ipv6 nd stale-timeout** command is run, the status of ND entries can be updated after the aging time of ND entries in STALE state expires.

The system checks the validity of ND entries after the aging time of ND entries in STALE state expires. If the neighbor is reachable, the ND entry status changes to REACH; otherwise, the ND entry is deleted.

When the aging time is not set on interfaces, the aging time set in the system is used. When the aging time is set on interfaces, the setting on the interfaces takes effect with priority.

Example

Set the aging time of ND entries in STALE state to 3600s on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 nd stale-timeout 3600
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.54 ipv6 neighbor

Function

The **ipv6 neighbor** command configures static neighbor entries.

The **undo ipv6 neighbor** command deletes static neighbor entries.

By default, no static neighbor entry is configured.

Format

ipv6 neighbor *ipv6-address mac-address*

ipv6 neighbor *ipv6-address mac-address* **vid** *vlan-id interface-type interface-number*

ipv6 neighbor *ipv6-address mac-address* **vid** *vlan-id* [**cevid** *cevid*]

undo ipv6 neighbor *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a neighbor.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Parameter	Description	Value
mac-address	Specifies the MAC address of a static neighbor.	The value is a 48-digit number in H-H-H format.
vid *vlan-id*	Specifies the ID of the VLAN to which the VLANIF interface belongs.	The value is an integer that ranges from 1 to 4094.
cevid *cevid*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Specifies the interface type and number of a physical interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ipv6 neighbor** command applies to GE interfaces and sub-interfaces, XGE interfaces and XGE sub-interfaces, and Eth-Trunk interfaces and sub-interfaces. You can run the **ipv6 neighbor** command to configure the mapping between the IPv6 address and MAC address for a neighbor. A neighbor entry indicates the mapping between an IPv6 address and a MAC address.

To filter invalid packets, you can create static neighbor entries, binding the destination IPv6 addresses of these packets to nonexistent MAC addresses.

Run the following commands based on the interface type:

- To configure static neighbor entries for Layer 3 interfaces, run the **ipv6 neighbor** *ipv6-address mac-address* command.
- To configure static neighbor entries for VLANIF interfaces, run the **ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id interface-type nterface-number* command.
- To configure static neighbor entries for QinQ termination sub-interfaces or a dot1q termination sub-interfaces, run the **ipv6 neighbor** *ipv6-address mac-address* **vid** *vlan-id* [**cevid** *cevid*] command.

Prerequisites

The IPv6 function has been enabled on the interface using the **ipv6 enable** command in the interface view.

Precautions

A neighbor entry enters the REACHABLE state after being created, indicating that the interface connected to this neighbor is Up. If the interface connected to this neighbor becomes Down, the neighbor entry needs to be deleted.

The static neighbor entries overwrite the neighbor entries dynamically learnt by device. That is, static neighbor entries are of higher priorities than dynamically learnt neighbor entries.

If the IPv6 address or MAC address specified in the **ipv6 neighbor** command is incorrect, communication with this neighbor fails.

Example

Configure static neighbor entries on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 neighbor fc00::1 0019-7459-3301
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.8.10 display ipv6 neighbors

8.8.55 ipv6 pathmtu

Function

The **ipv6 pathmtu** command sets the PMTU for a specified destination IPv6 address.

The **undo ipv6 pathmtu** command deletes the PMTU for a specified destination IPv6 address.

Format

ipv6 pathmtu *ipv6-address* [**vpn-instance** *vpn-instance-name*] [*path-mtu*]

undo ipv6 pathmtu *ipv6-address* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for which a PMTU is to be set.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance for which a PMTU is to be set.	The value must be an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
path-mtu	Specifies the path MTU, that is, the maximum size of IPv6 packets allowed to be sent along the path.	The value is an integer that ranges from 1280 to 10000, in bytes. The default value is 1500, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PMTU is used to determine the proper size of packets to be transmitted along the path from a source to a destination. Usually, a device fragments and forwards packets based on the dynamically learnt PMTU. Packets that are sent using this PMTU do not need to be fragmented during transmission. This reduces pressure on routing devices and optimizes network resource utilization to obtain the maximum throughput.

In some special cases, however, to protect devices on the network and avoid large-size packet attacks, you can run the **ipv6 pathmtu** command to set a static PMTU for the specified destination IPv6 address to control the maximum size of packets that can be transmitted between the source and the destination.

Precautions

On the path along which packets are transmitted, a node discards the received packets if its MTU is smaller than the PMTU of the received packets. Therefore, in most cases, dynamic PMTU learning is recommend unless there are security vulnerabilities on the network. You can use the default PMTU value instead of running the **ipv6 pathmtu** command to set a static PMTU.

Example

Set the PMTU of a specified IPv6 destination address to 1300 bytes.

```
<Huawei> system-view
[Huawei] ipv6 pathmtu fc00::12 1300
```

Set the PMTU of the address fc00::1 of the IPv6 VPN instance to 1600 bytes.

```
<Huawei> system-view
[Huawei] ipv6 pathmtu fc00::1 vpn-instance vpn6 1600
```

Related Topics

8.8.56 ipv6 pathmtu age
8.8.11 display ipv6 pathmtu

8.8.56 ipv6 pathmtu age

Function

The **ipv6 pathmtu age** command sets the aging time of dynamic PMTU entries.

The **undo ipv6 pathmtu age** command restores the aging time of dynamic PMTU entries to the default value.

By default, the aging time of dynamic PMTU entries is 10 minutes.

Format

ipv6 pathmtu age *age-time*

undo ipv6 pathmtu age

Parameters

Parameter	Description	Value
age-time	Specifies the aging time of dynamic specified PMTU entries.	The value is an integer that ranges from 10 to 100, in minutes. The default value is 10 minutes, which is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The lifetime of a dynamic PMTU entry can be changed by setting an aging time for dynamic PMTU entries.

To slow down PMTU aging, run the **ipv6 pathmtu age** command to set the aging time of dynamic PMTU entries to a larger value.

Precautions

This command changes only the aging time of dynamic PMTUs but not static PMTUs because static PMTU entries never age.

The priority of a static PMTU is higher than that of a dynamic PMTU. If the static PMTU exists, the dynamic PMTU does not take effect.

The aging time for the PMTU is valid only for the dynamic PMTU entries generated after this configuration, instead of the PMTU entries generated before this configuration.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the aging time of dynamic PMTU entries to 40 minutes.

```
<Huawei> system-view
[Huawei] ipv6 pathmtu age 40
```

Related Topics

8.8.55 ipv6 pathmtu

8.8.11 display ipv6 pathmtu

8.8.57 ipv6 soft-forward enhance enable

Function

The **ipv6 soft-forward enhance enable** command enables the enhanced forwarding function for IPv6 control packets generated by the device.

The **undo ipv6 soft-forward enhance enable** command disables the enhanced forwarding function for IPv6 control packets generated by the device.

By default, the enhanced forwarding function is enabled for IPv6 control packets generated by the device.

Format

ipv6 soft-forward enhance enable

undo ipv6 soft-forward enhance enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure forwarding policies (such as QoS policies) for data packets to implement differentiated services. In some scenarios, you may need to manage control packets generated by the device to process different control packets. For example, carriers have limited the bandwidth of data packets through QoS policies and also want to limit the bandwidth of control packets. In this situation, QoS policies take effect only for data packets. You can configure the enhanced forwarding function to make QoS policies take effect for control packets. Currently, the enhanced forwarding function is valid only for the control packets

 Copyright © Huawei Technologies Co., Ltd.

generated by the device but not for the control packets forwarded by other devices.

You can run the **ipv6 soft-forward enhance enable** command to enable the enhanced forwarding function for IPv6 control packets generated by the device.

Follow-up Procedures

After enabling the enhanced forwarding function on the device, you can perform some configurations on the IPv6 control packets generated by the device. For example, you can configure different QoS policies for different types of IPv6 control packets generated by the device.

Example

Disable the enhanced forwarding function for IPv6 control packets generated by the device.

```
<Huawei> system-view
[Huawei] undo ipv6 soft-forward enhance enable
```

8.8.58 reset ipv6 address-policy

Function

The **reset ipv6 address-policy** command deletes policy entries for selecting addresses.

Format

reset ipv6 address-policy [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes policy entries for selecting the address of a specified VPN instance. *vpn-instance-name* specifies the name of a VPN instance.	The value must be an existing VPN instance.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset ipv6 address-policy** command deletes policy entries for selecting addresses. Therefore, confirm your action before running this command.

This command does not delete policy entries for selecting default addresses.

Example

Delete policy entries for selecting addresses.

```
<Huawei> reset ipv6 address-policy
```

8.8.59 reset ipv6 attack-source overlapping-fragment

Function

The **reset ipv6 attack-source overlapping-fragment** command clears statistics on overlapping fragment attack packets.

Format

reset ipv6 attack-source overlapping-fragment

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After overlapping fragment attack packets are processed manually, run the **reset ipv6 attack-source overlapping-fragment** command to clear statistics on overlapping fragment attack packets.

Example

Clear statistics on IPv6 overlapping fragment attack packets.

```
<Huawei> reset ipv6 attack-source overlapping-fragment
```

Related Topics

8.8.7 display ipv6 attack-source overlapping-fragment

8.8.60 reset ipv6 neighbors

Function

The **reset ipv6 neighbors** command clears neighbor entries.

Format

reset ipv6 neighbors { **all** | **dynamic** | **static** | **vid** *vlan-id* [*interface-type interface-number*] | *interface-type interface-number* [**dynamic** | **static**] }

Parameters

Parameter	Description	Value
all	Clears neighbor entries on all interfaces.	-
dynamic	The first **dynamic** indicates that dynamic neighbor entries on all interfaces are cleared. The second **dynamic** indicates that dynamic neighbor entries on the current interface are cleared.	-
static	The first **static** indicates that static neighbor entries on all interfaces are cleared. The second **static** indicates that static neighbor entries on the current interface are deleted.	-
vid *vlan-id*	Clears neighbor entries of a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Clears all neighbor entries on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of neighbor entries exceeds the upper limit, run the **reset ipv6 neighbors** command to clear excessive neighbor entries.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The **reset ipv6 neighbors** command clears specified neighbor entries, which affects IPv6 packet forwarding. Therefore, confirm your action before running this command.

Example

Clear all neighbor entries on all interfaces.

```
<Huawei> reset ipv6 neighbors all
Warning: This operation will delete all static and dynamic IPv6 ND entries and the configurations of all
static IPv6 ND. Continue?[Y
/N]:y
```

Clear all neighbor entries on GE1/0/0.

```
<Huawei> reset ipv6 neighbors gigabitethernet 1/0/0
```

Related Topics

8.8.10 display ipv6 neighbors

8.8.61 reset ipv6 pathmtu

Function

The **reset ipv6 pathmtu** command clears PMTU entries.

Format

reset ipv6 pathmtu [**vpn-instance** *vpn-instance-name*] { **all** | **dynamic** | **static** }

Parameters

Parameter	Description	Value
all	Clears all PMTU entries in the cache.	-
dynamic	Clears all dynamic PMTU entries in the cache.	-
static	Clears all static PMTU entries in the cache.	-
vpn-instance *vpn-instance-name*	Clears all PMTU entries of a specified IPv6 VPN instance.	The value must be an existing VPN instance.

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **reset ipv6 pathmtu** command clears all PMTU entries. Therefore, confirm your action before running this command.

Example

Clear all PMTU entries.

```
<Huawei> reset ipv6 pathmtu all
Warning: This operation will reset all static and dynamic IPv6 PMTU entries, and clear the configurations of all static IPv6 PMTU, c
ontinue?[Y/N]:y
```

Related Topics

8.8.55 ipv6 pathmtu

8.8.62 reset ipv6 socket pktsort

Function

The **reset ipv6 socket pktsort** command clears statistics on the dual receive buffer of an IPv6 socket.

Format

reset ipv6 socket pktsort task-id *task-id* **socket-id** *socket-id*

Parameters

Parameter	Description	Value
task-id *task-id*	Specifies the ID of a task.	The value is an integer that ranges from 1 to 350.
socket-id *socket-id*	Specifies the ID of a socket.	The value is an integer that ranges from 1 to 131072.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics on the dual receive buffer of an IPv6 socket and the count restarts. Therefore, confirm your action before running this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics on the dual receive buffer of the IPv6 socket with the task ID 2 and the socket ID 4.

```
<Huawei> reset ipv6 socket pktsort task-id 2 socket-id 4
```

8.8.63 reset ipv6 statistics

Function

The **reset ipv6 statistics** command clears IPv6 traffic statistics.

Format

reset ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To collect IPv6 traffic statistics within a specified period, clear the existing IPv6 traffic statistics before running the **display ipv6 statistics** command to display IPv6 traffic statistics.

Precautions

The **reset ipv6 statistics** command clears the specified IPv6 traffic statistics. Therefore, confirm your action before running this command.

Example

Clear IPv6 traffic statistics.

```
<Huawei> reset ipv6 statistics
```

Related Topics

8.8.13 display ipv6 statistics

8.8.64 reset rawip ipv6 statistics

Function

The **reset rawip ipv6 statistics** command clears all Raw IPv6 packet statistics.

Format

reset rawip ipv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You need to run this command to clear the existing statistics on Raw IPv6 packets before running the **display rawip ipv6 statistics** command to view statistics on Raw IPv6 packets in a specified period.

The **reset rawip ipv6 statistics** command clears statistics on Raw IPv6 packets. Therefore, confirm your action before running this command.

Example

Clear all Raw IPv6 packet statistics.

```
<Huawei> reset rawip ipv6 statistics
```

8.8.65 reset tcp ipv6 authentication-statistics

Function

The **reset tcp ipv6 authentication-statistics** command clears authentication statistics of a specified TCP6 connection.

Format

reset tcp ipv6 authentication-statistics src-ip *src-ip* **src-port** *src-port* **dest-ip** *dest-ip* **dest-port** *dest-port*

Parameters

Parameter	Description	Value
src-ip *src-ip*	Specifies the source IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
src-port *src-port*	Specifies the source port.	The value is an integer that ranges from 0 to 65535.
dest-ip *dest-ip*	Specifies the destination IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
dest-port *dest-port*	Specifies the destination port.	The value is an integer that ranges from 0 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset tcp ipv6 authentication-statistics** command clears authentication statistics of a TCP6 connection. Therefore, confirm your action before running this command.

Example

Clear authentication statistics of a TCP6 connection.

```
<Huawei> reset tcp ipv6 authentication-statistics src-ip fc00:1::1 src-port 3456 dest-ip fc00:3::5 dest-port 5678
```

Related Topics

8.8.15 display tcp ipv6 authentication-statistics

8.8.66 reset tcp ipv6 statistics

Function

The **reset tcp ipv6 statistics** command clears IPv6 TCP packet statistics.

Format

reset tcp ipv6 statistics

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to clear the existing statistics on IPv6 TCP packets before running the **display tcp ipv6 statistics** command to view the statistics on IPv6 TCP packets in a specified period.

Precautions

The **reset tcp ipv6 statistics** command clears statistics on IPv6 TCP packets. Therefore, confirm your action before running this command.

The **reset tcp ipv6 statistics** command clears IPv6 TCP packet statistics on all in-service interface boards.

Example

Clear IPv6 TCP packet statistics.

```
<Huawei> reset tcp ipv6 statistics
```

Related Topics

8.8.16 display tcp ipv6 statistics

8.8.67 reset udp ipv6 statistics

Function

The **reset udp ipv6 statistics** command clears IPv6 UDP packet statistics.

Format

reset udp ipv6 statistics

Parameters

None

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to run this command to clear the existing IPv6 UDP packet statistics before running the **display udp ipv6 statistics** command to view IPv6 UDP packet statistics in a specified period.

Precautions

The **reset udp ipv6 statistics** command clears IPv6 UDP packet statistics. Therefore, confirm your action before running this command.

The **reset udp ipv6 statistics** command clears IPv6 UDP packet statistics on all in-service interface boards.

Example

Clear IPv6 UDP packet statistics.

```
<Huawei> reset udp ipv6 statistics
```

8.8.68 set priority acl6 dscp

Function

The **set priority acl6 dscp** command configures the DSCP priority of IPv6 control packets generated by the device based on the ACL rule.

The **undo set priority acl6** command restores the default DSCP priority of IPv6 control packets generated by the device.

By default, the DSCP priority of IPv6 control packets generated by the device is not specified based on the ACL rule.

Format

set priority acl6 *acl6-number* **dscp** *dscp-value*

undo set priority acl6 *acl6-number*

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an ACL rule.	The value is an integer that ranges from 3000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dscp-value	Specifies the DSCP priority of IPv6 control packets.	The value is as follows: • The value is an integer that ranges from 0 to 63. • The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **8.8.57 ipv6 soft-forward enhance enable** command is executed to enable the enhanced forwarding function of IPv6 control packets generated by the device, the same QoS policy will be applied to both the control packets and data packets. When the device maps packets based on DSCP priorities, it may send some control packets with low DSCP priorities generated on the device to low-priority queues, such as ICMPv6 and IPv6 Telnet packets. You can run the **set priority acl6 dscp** command to configure the DSCP priority of IPv6 control packets generated by the device based on the ACL rule, to prevent these IPv6 control packets from entering low-priority queues.

Precautions

If you run the **set priority acl6 dscp** command with the same value of *acl6-number* multiple times, only the latest configuration takes effect.

You can run the **8.8.69 set priority protocol-type-ipv6 dscp** command to specify the DSCP priority of IPv6 control packets based on the protocol type. If you specify the DSCP priority of IPv6 control packets based on both the protocol type and ACL rule, the protocol type configuration takes effect preferentially.

If you specify the DSCP priority of IPv6 control packets based on the ACL rule, you can configure a maximum of 16 ACL rules.

Example

Set the DSCP priority of IPv6 control packets based on the ACL6 rule 3002 to 56.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] set priority acl6 3002 dscp 56
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.69 set priority protocol-type-ipv6 dscp

8.8.69 set priority protocol-type-ipv6 dscp

Function

The **set priority protocol-type-ipv6 dscp** command configures the DSCP priority of IPv6 control packets generated by the device based on the protocol type.

The **undo set priority protocol-type-ipv6 dscp** command restores the default DSCP priority of IPv6 control packets generated by the device.

By default, the DSCP priority of IPv6 control packets generated by the device is 0.

Format

set priority protocol-type-ipv6 *protocol-type* **dscp** *dscp-value*

undo set priority protocol-type-ipv6 *protocol-type* **dscp**

Parameters

Parameter	Description	Value
protocol-type	Specifies the DSCP priority based on the IPv6 protocol type.	Enumerated type. The value can be **bgp4plus**, **dns6**, **icmpv6**, **snmp**, **ssh**, **udp**, or **telnet**.
dscp-value	Specifies the DSCP priority of IPv6 control packets.	The value is as follows: • The value is an integer that ranges from 0 to 63. • The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **8.8.57 ipv6 soft-forward enhance enable** command is executed to enable the enhanced forwarding function of IPv6 control packets generated by the device, the same QoS policy will be applied to both the control packets and data packets. When the device maps packets based on DSCP priorities, it may send some control packets with low DSCP priorities generated on the device to low-priority queues, such as ICMPv6 and IPv6 Telnet packets. You can run the **set priority protocol-type-ipv6 dscp** command to configure the DSCP priority of IPv6 control packets generated by the device based on the protocol type, to prevent these IPv6 control packets from entering low-priority queues.

Precautions

If you run the **set priority protocol-type-ipv6 dscp** command with the same value of **protocol-type-ipv6** multiple times, only the latest configuration takes effect.

To configure DSCP priorities of multiple IPv6 control packets, run the **set priority protocol-type-ipv6 dscp** command multiple times.

You can run the **8.8.68 set priority acl6 dscp** command to specify the DSCP priority of IPv6 control packets based on the ACL rule. If you specify the DSCP priority of IPv6 control packets based on both the protocol type and ACL rule, the protocol type configuration takes effect preferentially.

Example

Set the DSCP priority of IPv6 Telnet packets to 56.

```
<Huawei> system-view
[Huawei] set priority protocol-type-ipv6 telnet dscp 56
```

Related Topics

8.8.57 ipv6 soft-forward enhance enable

8.8.68 set priority acl6 dscp

8.8.70 tcp ipv6 max-mss

Function

The **tcp ipv6 max-mss** command sets the maximum value of Maximum Segment Size (MSS) for a TCP6 connection.

The **undo tcp ipv6 max-mss** command deletes the maximum MSS value of a TCP6 connection.

By default, the maximum MSS value is not configured for TCP6 connections.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This function takes effect only for TCP6 packets transmitted over a TCP6 connection established with the local device.

Format

tcp ipv6 max-mss *mss-value*

undo tcp ipv6 max-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the maximum MSS value for a TCP6 connection.	The value is an integer ranging from 32 to 9600, in bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP6 connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. If the path MTU is unavailable on one end of a TCP6 connection, this end cannot adjust the TCP6 packet size based on the MTU. As a result, this end may send TCP6 packets that are longer than the MTUs on intermediate devices, which will discard these packets. To prevent this problem, run the **tcp ipv6 max-mss** command on either end of a TCP6 connection to set the maximum MSS value of TCP6 packets. Then the MSS value negotiated by both ends will not exceed this maximum MSS value, and accordingly TCP6 packets sent from both ends will not be longer than this maximum MSS value and can travel through the intermediate network.

Precautions

The maximum MSS value configured using the **tcp ipv6 max-mss** command must be greater than the minimum MSS value configured using the **tcp ipv6 min-mss** command.

Example

Set the maximum MSS value for a TCP6 connection to 1024 bytes.

```
<Huawei> system-view
[Huawei] tcp ipv6 max-mss 1024
```

Related Topics

8.8.71 tcp ipv6 min-mss

8.8.71 tcp ipv6 min-mss

Function

The **tcp ipv6 min-mss** command sets the minimum value of maximum segment size (MSS) for a TCP6 connection.

The **undo tcp ipv6 min-mss** command restores the default minimum value of the MSS for a TCP6 connection.

The default minimum MSS value for a TCP6 connection is 216 bytes.

NOTE

This function takes effect only for TCP6 packets transmitted over a TCP6 connection established with the local device.

Format

tcp ipv6 min-mss *mss-value*

undo tcp ipv6 min-mss

Parameters

Parameter	Description	Value
mss-value	Specifies the minimum MSS value for a TCP6 connection.	The value ranges from 32 byte to 1500 bytes. By default, the value is 216 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To establish a TCP6 connection, the MSS value is negotiated, which indicates the maximum length of packets that the local device can receive. The TCP6 client on a network may send a request packet for establishing a TCP6 connection carrying a small MSS value. For example, the MSS value is 1. After the TCP6 server receives the request packet carrying the MSS value, the TCP6 connection is established. The TCP6 client then may send large numbers of requests to the server by an application, causing the TCP6 server to generate large numbers of reply packets. This may burden the TCP6 server or network, causing denial of service (DoS)

 Copyright © Huawei Technologies Co., Ltd.

attacks. To resolve this problem, run the **tcp ipv6 min-mss** command to set the minimum MSS value for a TCP6 connection. This configuration prevents a server from receiving packets carrying a small MSS value.

Precautions

If the **tcp ipv6 min-mss** command is run more than once in the same view, the latest configuration overrides the previous one.

Configure the parameters under the guidance of the technical personnel.

Example

Set the minimum MSS value for a TCP6 connection to 512 bytes.

```
<Huawei> system-view
[Huawei] tcp ipv6 min-mss 512
```

Related Topics

8.8.74 tcp ipv6 window

8.8.72 tcp ipv6 timer fin-timeout

Function

The **tcp ipv6 timer fin-timeout** command sets the value of the TCP6 FIN-Wait timer.

The **undo tcp ipv6 timer fin-timeout** command restores the default value of the TCP6 FIN-Wait timer.

By default, the value of the TCP6 FIN-Wait timer is 675s.

Format

tcp ipv6 timer fin-timeout *interval*

undo tcp ipv6 timer fin-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP6 FIN-Wait timer.	The value is an integer that ranges from 76 to 3600, in seconds. The default value is 675s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a TCP6 connection changes from FIN_WAIT_1 to FIN_WAIT_2, the TCP FIN-Wait timer is started. If the local device does not receive a packet with the FIN flag after the TCP6 FIN-Wait timer expires, the TCP6 connection is closed.

Precautions

If you run the **tcp ipv6 timer fin-timeout** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the value of the TCP6 FIN-Wait timer to 800s.

```
<Huawei> system-view
[Huawei] tcp ipv6 timer fin-timeout 800
```

Related Topics

8.8.73 tcp ipv6 timer syn-timeout

8.8.74 tcp ipv6 window

8.8.73 tcp ipv6 timer syn-timeout

Function

The **tcp ipv6 timer syn-timeout** command sets the value of the TCP6 SYN-Wait timer.

The **undo tcp ipv6 timer syn-timeout** command restores the default value of the TCP6 SYN-Wait timer.

By default, the value of the TCP6 SYN-Wait timer is 75s.

Format

tcp ipv6 timer syn-timeout *interval*

undo tcp ipv6 timer syn-timeout

Parameters

Parameter	Description	Value
interval	Specifies the value of the TCP6 SYN-Wait timer.	The value is an integer that ranges from 2 to 600, in seconds. The default value is 75s.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an SYN packet is sent, the TCP6 SYN-Wait timer is started. If no response packet is received when the TCP6 SYN-Wait timer expires, the TCP6 connection is closed.

Precautions

If you run the **tcp ipv6 timer syn-timeout** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the value of the TCP6 SYN-Wait timer to 100s.

```
<Huawei> system-view
[Huawei] tcp ipv6 timer syn-timeout 100
```

Related Topics

8.8.72 tcp ipv6 timer fin-timeout

8.8.74 tcp ipv6 window

8.8.74 tcp ipv6 window

Function

The **tcp ipv6 window** command sets the size of the packet receive or send buffer of a connection-oriented socket.

The **undo tcp ipv6 window** command restores the default size of the packet receive or send buffer of a connection-oriented socket.

By default, the size of the packet receive or send buffer of a connection-oriented socket is 8K bytes.

Format

tcp ipv6 window *window-size*

undo tcp ipv6 window

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
window-size	Specifies the size of the packet receive or send buffer of a connection-oriented socket.	The value is an integer that ranges from 1 to 32, in K bytes. The default value is 8K bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command changes the default size of the packet receive or send buffer. The device uses the default size to establish a TCP6 session.

Precautions

If you run the **tcp ipv6 window** command multiple times, only the latest configuration takes effect.

You are advised to use this command under the supervision of technical support personnel.

Example

Set the size of the packet receive or send buffer of a connection-oriented socket to 4K bytes.

```
<Huawei> system-view
[Huawei] tcp ipv6 window 4
```

Related Topics

8.8.72 tcp ipv6 timer fin-timeout

8.8.73 tcp ipv6 timer syn-timeout

8.9 DHCPv6 Configuration Commands

8.9.1 address prefix

Function

The **address prefix** command configures the network prefix and lifetime in the IPv6 address pool view.

The **undo address prefix** command deletes the network prefix and lifetime that are configured in the IPv6 address pool view.

By default, no network prefix and lifetime are configured in the IPv6 address pool view.

Format

address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**eui-64**] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**eui-64**] [**life-time preferred-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]] **valid-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]]

address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**lock**]

undo address prefix [*prefix-name*] *ipv6-prefix/ipv6-prefix-length* [**lock**]

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of a network prefix.	The value is a string of 1 to 63 case-sensitive characters without spaces.
ipv6-prefix/ipv6-prefix-length	Specifies the network prefix and prefix length.	*ipv6-prefix*: The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 1 to 128.
eui-64	Generates the interface ID based on the user MAC address according to the EUI-64 specifications. This method can be used to allocate addresses only when the client DUID type is LL or LLT.	-
life-time	Specifies the network prefix lifetime.	-

Parameter	Description	Value
valid-lifetime	Specifies the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-
preferred-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the preferred lifetime of the IPv6 prefix. The time must be no less than 1 minute.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
valid-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the valid lifetime of the IPv6 prefix. The time must be no less than 1 minute and cannot be less than the preferred lifetime.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
lock	Locks the address prefix.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 server, run the **address prefix** command to configure the network prefix in an IPv6 address pool. If IPv6 addresses in an IPv6 address pool have been assigned to DHCPv6 clients, only the value of lifetime can be modified.

Precautions

If no DHCPv6 relay agent exists between the DHCPv6 server and client, the length of the network prefix configured to the DHCPv6 server address pool must be longer than or equal to the prefix length of IPv6 addresses of Layer 3 interfaces on the DHCPv6 server.

Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).

You can configure at most three network prefixes.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Example

Bind the network prefix fc00:1::/64 to the DHCPv6 server address pool pool1 and set the lifetime to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] address prefix fc00:1::/64 life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool

8.9.2 capwap-ac (IPv6 address pool view)

Function

The **capwap-ac** command configures the AC's IPv6 address in the IPv6 address pool view.

The **undo capwap-ac** command deletes the AC's IPv6 address configured in the IPv6 address pool view.

By default, the AC's IPv6 address is not configured in the IPv6 address pool view.

Format

capwap-ac *ipv6-address*

undo capwap-ac *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for an AC.	The total length is 128 bit, which is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters. The format is X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the AC+Fit AP scenario, the AC needs to establish connections with APs. The device functioning as a DHCPv6 server can specify the AC's IPv6 address for an AP. The AP then can connect to the specified AC. The device uses Option52 to carry the AC address.

If the AC and AP are located in the same network segment, the AP sends a broadcast packet to automatically discover the AC. In this case, the configuration of the **capwap-ac** command is optional. If the AC and AP are located in different network segments, you must configure the **capwap-ac** command.

Prerequisites

The IPv6 address pool is created using the **8.9.14 dhcpv6 pool** command.

Precautions

You can run the **capwap-ac** command multiple times to configure the IPv6 addresses of several ACs. The IPv6 addresses of at most eight ACs can be configured in an address pool, and the AC that is configured first takes precedence over the one configured later.

Example

Specify the AC's IPv6 address to fc00:1::1 in pool1 of the DHCPv6 server.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] capwap-ac fc00:1::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.3 conflict-address expire-time

Function

The **conflict-address expire-time** command sets the aging time for conflicted addresses in the IPv6 address pool.

The **undo conflict-address expire-time** command restores the default aging time of conflicted addresses in the IPv6 address pool.

By default, the aging time of conflicted addresses is 172800s (two days).

Format

conflict-address expire-time *expire-time*

undo conflict-address expire-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time for the conflicted addresses in the address pool.	The value is an integer that ranges from 60 to 4294967295, in seconds.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **conflict-address expire-time** command is used on DHCPv6 servers. If the IPv6 address in the address pool is marked as a conflicted address, it cannot be allocated. To use these conflicted addresses, the administrator needs to mark these addresses as assignable. After the aging time configured using the **conflict-address expire-time** command expires, the conflicted addresses automatically become assignable.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Example

Set the aging time of conflicted addresses in global address pool global1 to 36000s.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] conflict-address expire-time 36000
```

Related Topics

8.9.14 dhcpv6 pool

8.9.4 dhcpv6 client information-request

Function

The **dhcpv6 client information-request** command enables an interface to obtain configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

The **undo dhcpv6 client information-request** command disables an interface from obtaining configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

By default, the interface is disabled from obtaining configuration parameters (not including IPv6 addresses) using stateless DHCPv6 address autoconfiguration.

Format

dhcpv6 client information-request

undo dhcpv6 client information-request

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 client information-request** command is used on the DHCPv6 client. After you run the **dhcpv6 client information-request** on the WAN-side Layer 3 interface or sub-interface of the device that functions as a DHCPv6 client, IPv6 addresses are generated based on the Route Advertisement (RA) packets. The DHCPv6 server provides other configuration parameters such as IP addresses of the DNS, and SNTP servers except for IPv6 addresses and the interval for updating configuration parameters.

Prerequisites

1. IPv6 functions have been enabled globally using the **8.8.20 ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local** or **ipv6 address** *ipv6-address* **link-local** command in the interface view.

Precautions

The interval for updating configuration parameters is determined by the DHCPv6 server configuration. If the AR functions as a DHCPv6 server, you can run the **8.9.41 information-refresh** command to configure the interval for updating the configuration parameters obtained using stateless DHCPv6 address autoconfiguration. Limit the interval between 600 to 259200 seconds to prevent a long interval from causing the inconsistency in DNS information on the DHCPv6

 Copyright © Huawei Technologies Co., Ltd.

client and server and prevent a short interval from causing the client to frequently request the updated configuration parameters from the server. When the interval in the DHCPv6 server configuration is longer than 259200 seconds (3 days), the interval on the DHCPv6 client is 259200 seconds (3 days). When the interval in the DHCPv6 server configuration is shorter than 600 seconds, the interval on the DHCPv6 client is 600 seconds. When the interval in the DHCPv6 server configuration is between 600 and 259200 seconds, the interval on the DHCPv6 client is the same as the interval in the DHCPv6 server configuration.

Example

Configure the DHCPv6 client to obtain configuration parameters using stateless DHCPv6 address autoconfiguration on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
[Huawei-GigabitEthernet1/0/0] dhcpv6 client information-request
```

Related Topics

8.9.28 display dhcpv6 client statistics

8.9.50 reset dhcpv6 client statistics

8.9.26 display dhcpv6 client

8.9.5 dhcpv6 client pd

Function

The **dhcpv6 client pd** command configures the DHCPv6 PD client function.

The **undo dhcpv6 client pd** command disables the DHCPv6 PD client function.

By default, the DHCPv6 PD client function is disabled.

Format

dhcpv6 client [**dhcp** [**hint** *ipv6-address*]] **pd** *prefix-name* [**hint** *ipv6-prefix/ipv6-prefix-length*] [**rapid-commit**] [**unicast-option**]

dhcpv6 client dhcp [**hint** *ipv6-address*] **pd** *prefix-name* [**hint** *ipv6-prefix/ipv6-prefix-length*] [**rapid-commit**] [**unicast-option**] **union-mode**

undo dhcpv6 client [**dhcp**] **pd**

Parameters

Parameter	Description	Value
dhcp	Indicates that a client obtains both an IPv6 address and a prefix.	-

Parameter	Description	Value
hint *ipv6-address*	Specifies the required IPv6 address to be requested.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
prefix-name	Specifies the name of an IPv6 address prefix name.	The value is a string of 1 to 63 case-sensitive characters without spaces.
hint *ipv6-prefix/ipv6-prefix-length*	Specifies the required IPv6 address prefix and prefix length.	*ipv6-prefix*: The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 1 to 128.
rapid-commit	Indicates that the DHCPv6 PD client requests an IPv6 address prefix using the two-message exchange.	-
unicast-option	Indicates that the DHCPv6 PD client requests an IPv6 address prefix using the unicast mode.	-
union-mode	Indicates that the DHCPv6 PD client obtains both an IPv6 address and a prefix using a packet.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 client pd** command is used on the DHCPv6 PD client. After the **dhcpv6 client pd** is executed on the WAN-side Layer 3 interface or sub-interface of the device that functions as a DHCPv6 PD client, the device requests an IPv6 address prefix in the DHCPv6 mode. The requested prefix is bound to the configured prefix name. You can specify the **hint** *ipv6-prefix/ipv6-prefix-length* parameter to set the required IPv6 address prefix and prefix length.

Prerequisites

1. IPv6 functions have been enabled globally using the **8.8.20 ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local**, or **ipv6 address** *ipv6-address* **link-local** command in the interface view. Or the IPv6 global unicast IPv6 address has been configured using the **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* } command in the interface view.

Configuration Precautions

When configuring the DHCPv6 PD client function, you cannot set *prefix-name* to **a**, **au**, **aut**, or **auto**. These prefix names cannot be applied to interfaces.

Example

Configure the DHCPv6 PD client to obtain IPv6 address prefix using stateless DHCPv6 address autoconfiguration on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
[Huawei-GigabitEthernet1/0/0] dhcpv6 client pd huawei
```

8.9.6 dhcpv6 duid

Function

The **dhcpv6 duid** command configures a DUID for the DHCPv6 device.

By default, the device generates a DUID based on the link-layer (LL) address.

Format

dhcpv6 duid { **ll** | **llt** | *duid* }

Parameters

Parameter	Description	Value
ll	Configures the device to generate a DUID based on the link-layer address (MAC address).	-
llt	Configures the device to generate a DUID based on the link-layer address (MAC address) plus time.	-
duid	Specifies the DUID of the device.	The value is a hexadecimal string with an even number (in the range of 8 to 28) of characters. The value contains only combinations of digits 0 to 9, uppercase letters A to F, and lowercase letters a to f.

Views

System view

Default Level

3: Management level

Usage Guidelines

A DUID identifies a DHCPv6 device. Each DHCPv6 server or client has a unique DUID. Servers use DUIDs to identify clients and clients use DUIDs to identify servers. When this command is run, a new DUID is stored in the :/dhcp/dhcp-duid.txt file of the storage device. You can run the **display dhcpv6 duid** command to check the DUID of the device.

Example

Configure the device to generate a DUID based on the link-layer address.

```
<Huawei> system-view
[Huawei] dhcpv6 duid ll
Warning: The DHCP unique identifier should be globally-unique and stable. Are you sure to change it?
[Y/N]y
```

Related Topics

8.9.29 display dhcpv6 duid

8.9.7 dhcpv6 client renew

Function

The **dhcpv6 client renew** command updates the IPv6 address or prefix applied by a DHCPv6 client.

Format

dhcpv6 client renew

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **dhcpv6 client renew** command applies to only the DHCP client and updates the IPv6 address or prefix applied by the DHCPv6 client.

Example

Manually update the applied IPv6 address.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 address auto dhcp
[Huawei-GigabitEthernet1/0/0] dhcpv6 client renew
```

Manually update the applied IPv6 prefix.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] dhcpv6 client pd myprefix
[Huawei-GigabitEthernet1/0/0] dhcpv6 client renew
```

8.9.8 renew-time-percent rebind-time-percent

Function

The **renew-time-percent rebind-time-percent** command configures the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime of an IPv6 address pool.

The **undo renew-time-percent rebind-time-percent** command restores the default percentage of the lease renewal time and the default percentage of the rebinding time in the preferred lifetime of an IPv6 address pool.

 Copyright © Huawei Technologies Co., Ltd.

By default, the percentage of the lease renewal time in the preferred lifetime of an IPv6 address pool is 50%, and the percentage of the rebinding time is 80%.

Format

renew-time-percent *renew-time-percent* **rebind-time-percent** *rebind-time-percent*

undo renew-time-percent rebind-time-percent

Parameters

Parameter	Description	Value
renew-time-percent	Specifies the percentage of the lease renewal time in the preferred lifetime of an IPv6 address pool.	The value is an integer that ranges from 10 to 89. The default value is 50.
rebind-time-percent	Specifies the percentage of the rebinding time in the preferred lifetime of an IPv6 address pool. The value of *rebind-time-percent* must be greater than that of *renew-time-percent*, and the difference between the values must be greater than or equal to 10.	The value is an integer that ranges from 20 to 99. The default value is 80.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to change the lease renewal time and rebinding time in an IPv6 address pool.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When planning the lease renewal time and rebinding time, you can run the **address prefix** and **renew-time-percent rebind-time-percent** commands to configure the preferred lifetime and the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime respectively. If the lease renewal time and rebinding time are too short, the lease and renewal time (T1 and T2) of IPv6 addresses allocated to DHCPv6 clients by the DHCPv6 server are too short. As a result, DHCPv6 clients send lease renewal packets frequently. It is recommended that you set the lease renewal time and rebinding time based on the actual usage scenario.

Example

Configure the percentage of the lease renewal time and the percentage of the rebinding time in the preferred lifetime of the IPv6 address pool **test**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool test
[Huawei-dhcpv6-pool-test] renew-time-percent 55 rebind-time-percent 85
```

8.9.9 dhcpv6 interface-id format

Function

The **dhcpv6 interface-id format** command configures the Interface-ID format in DHCPv6 packets.

The **undo dhcpv6 interface-id format** command restores the default Interface-ID format in DHCPv6 packets.

By default, the Interface-ID format in DHCPv6 packets is **default**.

Format

dhcpv6 interface-id format { **default** | **user-defined** *text* }

undo dhcpv6 interface-id format

Parameters

Parameter	Description	Value
default	Specifies the default Interface-ID format. The default Interface-ID format is %04svlan.%04cvlan.%mac:%portname. The values of the S-VLAN and C-VLAN are integers containing four characters. If the length is fewer than four characters, the value is prefixed with 0s. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the device MAC address is 6afe-870b-0000, the Interface-ID generated during the system parsing process is 0011.0022.6afe870b0000:vlanif100.	-

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Interface-ID format. A user-defined format can be: ● Format defined by keywords: The Interface-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Interface-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 8-94**. ● Format defined by common character strings: The Interface-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Interface-ID can be directly defined as N8. ● Mixed format: The Interface-ID is defined by both the keywords and common character strings. For example, the Interface-ID can be defined as %sysname N8.	The value is a string of case-sensitive characters without spaces. The character string contains 1 to 251 characters, excluding the quotation marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID records user access information such as the inbound interfaces of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Interface-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 interface-id format** command to configure the format of the Interface-ID inserted into DHCPv6 packets.

 Copyright © Huawei Technologies Co., Ltd.

Table 8-94 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- The user-defined format content must be specified between the double quotation marks ("""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.

- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Configure a user-defined format as the format of the Interface-ID in DHCPv6 packets and the device MAC address as the encapsulated content.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 interface-id format user-defined "%mac"
```

8.9.10 dhcpv6 interface-id insert enable

Function

The **dhcpv6 interface-id insert enable** command enables the function of adding the Interface-ID option in DHCPv6 packets.

The **undo dhcpv6 interface-id insert enable** command disables the function of adding the Interface-ID option in DHCPv6 packets.

By default, the function of adding the Interface-ID option in DHCPv6 packets is enabled.

Format

dhcpv6 interface-id insert enable

undo dhcpv6 interface-id insert enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID option records user access information such as the inbound interface of the DHCPv6 Request packets sent from the clients to the device. The user access information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. When the device functions as a DHCPv6 relay agent or lightweight DHCPv6 relay agent (LDRA), and the device receives the Request packets sent from the DHCPv6 clients and forwards the packets to the DHCPv6 server, the device adds the Interface-ID option in the packets to identify location information of the DHCPv6 clients by default. If the DHCPv6 server interconnected to the device does not support the Interface-ID option, you can run the **undo dhcpv6 interface-id insert enable** command to configure the device not to add the Interface-ID option in DHCPv6 packets to flexibly control option information obtained by the DHCPv6 server.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Example

Enable the function of adding the Interface-ID option in DHCPv6 packets on the interface Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcpv6 interface-id insert enable
```

8.9.11 dhcpv6 packet-rate

Function

The **dhcpv6 packet-rate** command enables rate limit of DHCPv6 messages and sets the rate threshold for DHCPv6 messages.

The **undo dhcpv6 packet-rate** command disables rate limit of DHCPv6 messages and deletes the rate threshold for DHCPv6 messages.

By default, rate limit of DHCPv6 messages is disabled.

Format

dhcpv6 packet-rate *packet-rate*

undo dhcpv6 packet-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-rate	Specifies the rate threshold for DHCPv6 messages.	The value is an integer that ranges from 0 to 400, in pps. If the value is 0, rate limit of DHCPv6 messages is disabled.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent clients from sending a large number of messages to attack the device, the device limits the rate of DHCPv6 messages. After the DHCPv6 packet rate limit is enabled and the rate threshold is configured using the **dhcpv6 packet-rate** command, the DHCPv6 packets are discarded when the packet rate exceeds the rate threshold.

Prerequisites

DHCP functions have been enabled globally using the **dhcp enable** command.

Example

Enable rate limit of DHCPv6 messages and set the rate threshold for DHCPv6 messages to 200 pps.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 packet-rate 200
```

Related Topics

8.3.18 dhcp enable

8.9.12 dhcpv6 packet-rate drop-alarm enable

Function

The **dhcpv6 packet-rate drop-alarm enable** command enables the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit.

 Copyright © Huawei Technologies Co., Ltd.

The **undo dhcpv6 packet-rate drop-alarm enable** command disables the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit.

By default, the alarm function for discarding DHCPv6 messages is disabled when the rate of DHCPv6 messages exceeds the limit.

Format

dhcpv6 packet-rate drop-alarm enable

undo dhcpv6 packet-rate drop-alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of DHCPv6 messages discarded is enabled using the **dhcpv6 packet-rate drop-alarm enable** command, the device records alarm information when the number of DHCPv6 packets that are discarded exceeds the alarm threshold. The alarm threshold can be set using the **dhcpv6 packet-rate drop-alarm threshold** command.

Prerequisites

1. DHCP functions have been enabled globally using the **dhcp enable** command.
2. The DHCPv6 packet rate limit has been enabled using the **dhcpv6 packet-rate** command.

Example

Enable the alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds rate limit.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 packet-rate 200
[Huawei] dhcpv6 packet-rate drop-alarm enable
```

Related Topics

8.3.18 dhcp enable

 Copyright © Huawei Technologies Co., Ltd.

8.9.13 dhcpv6 packet-rate drop-alarm threshold

Function

The **dhcpv6 packet-rate drop-alarm threshold** command sets the alarm threshold for the number of DHCPv6 messages discarded when the rate of DHCPv6 messages exceeds the rate limit.

The **undo dhcpv6 packet-rate drop-alarm threshold** command restores the default alarm threshold of the number of DHCPv6 messages discarded.

By default, the alarm threshold is 100 packets when the alarm function of DHCPv6 messages discarded is enabled.

Format

dhcpv6 packet-rate drop-alarm threshold *threshold*

undo dhcpv6 packet-rate drop-alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of DHCPv6 messages discarded when the rate of DHCPv6 messages exceeds the rate limit.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function of DHCPv6 messages discarded is enabled using the **dhcpv6 packet-rate drop-alarm enable** command, the device records alarm information when the number of DHCPv6 packets that are discarded exceeds the alarm threshold.

Prerequisites

1. The DHCP function has been enabled globally using the **dhcp enable** command.

 Copyright © Huawei Technologies Co., Ltd.

2. The DHCPv6 packet rate limit has been enabled using the **dhcpv6 packet-rate** *packet-rate* command.
3. The alarm function for discarding DHCPv6 messages when the rate of DHCPv6 messages exceeds the limit has been enabled using the **dhcpv6 packet-rate drop-alarm enable** command.

Example

Configure the device to generate an alarm when the number of DHCPv6 messages discarded exceeds 150 packets.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 packet-rate 200
[Huawei] dhcpv6 packet-rate drop-alarm enable
[Huawei] dhcpv6 packet-rate drop-alarm threshold 150
```

Related Topics

8.3.18 dhcp enable

8.9.11 dhcpv6 packet-rate

8.9.12 dhcpv6 packet-rate drop-alarm enable

8.9.14 dhcpv6 pool

Function

The **dhcpv6 pool** command creates an IPv6/IPv6 PD address pool or displays the IPv6/IPv6 PD address pool view.

The **undo dhcpv6 pool** command deletes the created IPv6/IPv6 PD address pool.

By default, no IPv6/IPv6 PD address pool is created.

Format

dhcpv6 pool *pool-name*

undo dhcpv6 pool *pool-name*

Parameters

Parameter	Description	Value
pool-name	Specifies the name of an IPv6/IPv6 PD address pool.	The value is a string of 1 to 31 case-sensitive characters without spaces. The value contains digits, letters, underscores (_), and dots (.).

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **dhcpv6 pool** command is used on DHCPv6/DHCPv6 PD servers. When configuring the DHCPv6/DHCPv6 PD server, run the **dhcpv6 pool** command to create an IPv6/IPv6 PD address pool for the DHCPv6/DHCPv6 PD server to assign IPv6 addresses or prefixes to DHCPv6/DHCPv6 PD clients.

The total number of IPv6 and IPv6 PD address pools that can be configured varies according to the device models:

- AR100, AR120, AR150, AR160, AR200, AR1200, AR2201-48FE, AR2202-48FE or AR2204: 16
- AR2220E, AR2220, AR2240, AR3200 or AR3600: 32

Example

Create an IPv6 address pool **DHCPv6POOL**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool DHCPv6POOL
```

8.9.15 dhcpv6 relay destination

Function

The **dhcpv6 relay destination** command enables the DHCPv6 relay function on interfaces and configures the IPv6 address of the DHCPv6 server or next-hop relay agent.

The **undo dhcpv6 relay destination** command disables the DHCPv6 relay function on an interface.

By default, the DHCPv6 relay function is disabled on an interface.

Format

dhcpv6 relay { **destination** *ipv6-address* | **interface** *interface-type interface-number* }

undo dhcpv6 relay { **destination** *ipv6-address* | **interface** *interface-type interface-number* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6-address	Specifies the destination address of relay messages, which can be the IPv6 address of the DHCPv6 server or next hop relay agent.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of the outbound interface of relay messages.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a client applies to a DHCPv6 server on a different network segment for an IPv6 address, you need to deploy a relay agent between the client and the DHCPv6 server. In this manner, the relay agent transmits DHCPv6 messages exchanged between the client and the DHCPv6 server.

You can use the **dhcpv6 relay destination** command to enable the DHCPv6 relay function on an interface.

Prerequisites

The DHCP function has been enabled using the **8.3.18 dhcp enable** command in the system view.

Precautions

The device supports a maximum of eight DHCPv6 servers or next-hop relays.

Example

Enable the DHCPv6 relay function on GE0/0/1 and set the destination address of relay messages to fc00:1::1.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ipv6 enable
[Huawei-GigabitEthernet0/0/1] dhcpv6 relay destination fc00:1::1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.3.18 dhcp enable

8.9.33 display dhcpv6 relay

8.9.16 dhcpv6 relay server-select

Function

The **dhcpv6 relay server-select** command configures a DHCPv6 server group for a DHCPv6 relay agent.

The **undo dhcpv6 relay server-select** command deletes a DHCPv6 server group for a DHCPv6 relay agent.

By default, no DHCPv6 server group is configured.

Format

dhcpv6 relay server-select *group-name*

undo dhcpv6 relay server-select

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCPv6 server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6 relay server-select** command is used on DHCPv6 relay agents. When a DHCPv6 client sends DHCPv6 Request packets to a DHCPv6 server through a DHCPv6 relay agent, you can run the **dhcp relay server-select** command to specify a DHCPv6 server group for the DHCPv6 relay agent and configure the IPv6 address of the DHCPv6 server.

Prerequisites

1. A DHCPv6 server group has been created using the **8.9.25 dhcpv6 server group** command.

 Copyright © Huawei Technologies Co., Ltd.

2. The IPv6 function has been enabled using the **8.8.28 ipv6 enable (interface view)** command in the interface view.

Precautions

- Each DHCPv6 server group can be bound to multiple interfaces, but each interface can only be bound to one DHCPv6 server group.
- IP addresses of servers in a DHCPv6 server group cannot be on the same network segment with IP addresses of interfaces on the DHCPv6 relay agent.
- If you run the **dhcpv6 relay server-select** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Configure the DHCPv6 server group named group 1 for the DHCPv6 relay agent on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] dhcp enable
[Huawei] dhcpv6 server group group1
[Huawei-dhcpv6-server-group-group1] dhcpv6-server fc00:1::1
[Huawei-dhcpv6-server-group-group1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] dhcpv6 relay server-select group1
```

Related Topics

8.9.25 dhcpv6 server group

8.9.23 dhcpv6-server

8.9.33 display dhcpv6 relay

8.9.17 dhcpv6 relay source-interface

Function

The **dhcpv6 relay source-interface** command configures the IPv6 address of an interface as the source IPv6 address of packets.

The **undo dhcpv6 relay source-interface** command restores the default setting.

By default, the IPv6 address of an interface is not configured as the source IPv6 address of packets.

Format

dhcpv6 relay source-interface *interface-type interface-number*

undo dhcpv6 relay source-interface

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. • *interface-type*: specifies the interface type. Currently, only loopback interfaces are supported. • *interface-number*: specifies the interface number.	-

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When forwarding packets from a DHCPv6 client, a DHCPv6 relay agent uses the IPv6 address of the packet inbound interface as the source IPv6 address of the packets. Therefore, you need to configure an IPv6 address for each interface on the DHCPv6 relay agent. As a result, the configuration is complex and IPv6 addresses may be wasted. You can run the **dhcpv6 relay source-interface** *interface-type interface-number* command on the DHCPv6 relay agent to specify the IPv6 address of the loopback interface as the source IPv6 address of the DHCPv6 relayed packets, simplifying the configuration and saving IPv6 addresses.

Prerequisites

Before you run this command in the system view, the first four conditions must be met. Before you run this command in the interface view, all the following conditions must be met.

- The device has been enabled to forward IPv6 unicast packets using the **8.8.20 ipv6** command.
- A loopback interface has been created using the **5.20.10 interface loopback** *loopback-number* command.
- An IPv6 address has been configured for the loopback interface using the **8.8.21 ipv6 address** command.
- DHCP has been enabled globally using the **8.3.18 dhcp enable** command.
- In the interface view:

- The IPv6 function has been enabled on the interface using the **8.8.28 ipv6 enable (interface view)** command.
- The DHCPv6 relay function has been enabled on the interface using the **dhcpv6 relay** { **destination** *ipv6-address* | **interface** *interface-type interface-number* } or **dhcpv6 relay server-select** *group-name* command.

Precautions

If an IPv6 address is configured for the inbound interface that receives packets from DHCPv6 clients, the IPv6 address is used as the source IPv6 address of packets.

This command takes effect on all interfaces of the device if it is configured in the system view, and takes effect only on an interface if it is configured in the interface view. If this command is configured in both the interface view and system view, the configuration in the interface view takes effect.

Example

In the system view, configure the IPv6 address of a loopback interface as the source IPv6 address of packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface loopback 5
[Huawei-LoopBack5] ipv6 enable
[Huawei-LoopBack5] ipv6 address fc01:1::1/128
[Huawei-LoopBack5] quit
[Huawei] dhcp enable
[Huawei] dhcpv6 relay source-interface loopback 5
```

On VLANIF100, configure the IPv6 address of a loopback interface as the source IPv6 address of packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface loopback 5
[Huawei-LoopBack5] ipv6 enable
[Huawei-LoopBack5] ipv6 address fc01:1::1/128
[Huawei-LoopBack5] quit
[Huawei] dhcp enable
[Huawei] interface Vlanif 100
[Huawei-Vlanif100] ipv6 enable
[Huawei-Vlanif100] dhcpv6 relay destination fc00:1::1
[Huawei-Vlanif100] dhcpv6 relay source-interface loopback 5
```

Related Topics

8.8.20 ipv6

8.8.21 ipv6 address

8.3.18 dhcp enable

8.8.28 ipv6 enable (interface view)

8.9.15 dhcpv6 relay destination

8.9.18 dhcpv6 relay option79 insert enable

Function

The **dhcpv6 relay option79 insert enable** command inserts the Option79 field into DHCPv6 messages.

The **undo dhcpv6 relay option79 insert enable** command restores the default setting.

By default, the Option79 field is not inserted into DHCPv6 messages.

Format

dhcpv6 relay option79 insert enable

undo dhcpv6 relay option79 insert enable

Parameters

None

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

The MAC address is used to identify the DHCPv4 client on the IPv4 network and the DUID is used to identify the DHCPv6 client on the IPv6 network. In an IPv4 and IPv6 dual-stack service deployment scenario, the administrator wants to establish connections between clients' MAC addresses and IPv4 or IPv6 addresses obtained by the clients and perform unified management over dual-stack clients based on the MAC address. However, the MAC address of the DHCPv6 client cannot be identified using the DUID currently.

As defined in RFC, a DHCPv6 relay agent can fill the link address and link type of a client into the Option79 field. When a device functions as a DHCPv6 relay agent, you can run the **dhcpv6 relay option79 insert enable** command to insert the Option79 field into DHCPv6 messages for enabling the DHCPv6 server to obtain the clients' MAC addresses. When this command is run and the DHCPv6 relay agent receives a Request message from a client, it inserts the Option79 field into the Request message and forwards the message to the DHCPv6 server. The DHCPv6 server then obtains the MAC address of the client by parsing the Option79 field.

Prerequisites

- The DHCPv6 function has been enabled in the system view.
- The DHCPv6 relay function has been enabled in the interface view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- Only the first-hop DHCPv6 relay agent supports this function.
- This function takes effect for all interfaces if it is configured in the system view, and takes effect for a specified interface if it is configured in the view of the interface. If this command is configured in both the interface view and system view, the configuration in the interface view takes effect.

Example

Insert the Option79 option into DHCPv6 messages in the system view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] dhcpv6 relay option79 insert enable
```

Insert the Option79 field into DHCPv6 messages in the interface view.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] dhcpv6 relay destination fc00:1::1
[Huawei-GigabitEthernet1/0/0] dhcpv6 relay option79 insert enable
```

8.9.19 dhcpv6 remote-id format

Function

The **dhcpv6 remote-id format** command sets the format of the Remote-ID in DHCPv6 messages.

The **undo dhcpv6 remote-id format** command restores the default format of the Remote-ID in DHCPv6 messages.

By default, the default format of the Remote-ID in DHCPv6 messages is used.

Format

dhcpv6 remote-id format { **default** | **user-defined** *text* }

undo dhcpv6 remote-id format

Parameters

Parameter	Description	Value
default	Indicates to adopt the default format of the remote ID. The default format of the remote ID is %duid %portname:%04svlan.%04cvlan, where the values of the outer VLAN ID and inner VLAN ID are integers and composed of four characters. If the length is shorter than four characters, 0s are prefixed to the value. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the client DUID is 0003000180FB063545B3, the Remote-ID option generated during the system parsing process is 0003000180FB063545B3 vlanif100:0011.0022.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-defined *text*	Specifies a user-defined format as the Remote-ID format. A user-defined format can be: ● Format defined by keywords: The Remote-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Remote-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 8-95**. ● Format defined by common character strings: The Remote-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Remote-ID can be directly defined as N8. ● Mixed format: The Remote-ID is defined by both the keywords and common character strings. For	The value is a string of 3 to 247 case-sensitive characters with spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	example, the Remote-ID can be defined as %sysname N8.	

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The Remote-ID records user access information such as the DUID of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPfv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Remote-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 remote-id format** command to configure the format of the Remote-ID inserted into DHCPv6 packets.

Table 8-95 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.

 Copyright © Huawei Technologies Co., Ltd.

Keyword	Description
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Follow-up Procedure

When the device functions as a DHCPv6 relay, you must run the **8.9.20 dhcpv6 remote-id insert enable** command to enable the function of inserting the Remote-ID into DHCPv6 relay packets after running the **dhcpv6 remote-id format** command to configure the Remote-ID format in DHCPv6 packets.

NOTE

When the device functions as an LDRA, the Remote-ID is inserted into DHCPv6 relay packets by default and the function does not need to be enabled.

Precautions

- The user-defined format content must be specified between the double quotation marks ("")). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.

- An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Set the customized format for the remote ID carried in DHCPv6 messages and encapsulate the MAC address of the device into the remote ID.

```
<Huawei> system-view
[Huawei] dhcpv6 remote-id format user-defined "%mac"
```

Related Topics

8.9.20 dhcpv6 remote-id insert enable

8.9.20 dhcpv6 remote-id insert enable

Function

Using the **dhcpv6 remote-id insert enable** command, you can enable the function of appending the remote ID to DHCPv6 relay messages.

Using the **undo dhcpv6 remote-id insert enable** command, you can disable the function of appending the remote ID to DHCPv6 relay messages.

By default, the function of appending the remote ID to DHCPv6 relay messages is disabled.

Format

dhcpv6 remote-id insert enable

undo dhcpv6 remote-id insert enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The remote ID carries information about a client and identifies a client. The DHCPv6 server can make decisions about address allocation, parameter setting,

and prefix agent according to the remote ID. The remote ID is defined by the vendor. Usually, the remote ID carries the phone number of the caller in dialing, user name, IP address of the peer in a point-to-point connection, and access interface.

Prerequisite

1. The IPv6 function has been enabled using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
2. An IPv6 address has been assigned to the DHCPv6 server using the **8.9.15 dhcpv6 relay destination** command in the interface view or the a DHCPv6 server group has been specified for the DHCPv6 relay agent using the **8.9.16 dhcpv6 relay server-select** command.

Example

Enable the function of appending the remote ID to DHCPv6 relay messages on GE0/0/1.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] dhcpv6 remote-id insert enable
```

Related Topics

8.3.18 dhcp enable

8.9.19 dhcpv6 remote-id format

8.9.21 dhcpv6 server (system view)

Function

The **dhcpv6 server** command enables the DHCPv6 server or DHCPv6 PD server function in the system view.

The **undo dhcpv6 server** command disables the DHCPv6 server or DHCPv6 PD server function in the system view.

By default, the DHCPv6 server or DHCPv6 PD server function is disabled in the system view.

Format

dhcpv6 server { **allow-hint** | **preference** *preference-value* | **rapid-commit** | **unicast** } *

undo dhcpv6 server { **allow-hint** | **preference** | **rapid-commit** | **unicast** } *

Parameters

Parameter	Description	Value
allow-hint	Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests. If the **allow-hint** parameter is specified, the server preferentially allocates addresses, prefixes, and prefix lengths based on the client requests. If the address, prefix, and prefix length requested by a client are not within the address pool or have been allocated to another client, the server ignores the client request and allocates another available address, prefix, and prefix length to the client.	-
preference *preference-value*	Specifies the server priority in the Advertise packet sent by the device. The DHCPv6 client selects the server with the highest priority based on the server priority in the Advertise packet to assign IPv6 addresses or prefixes.	The value is an integer that ranges from 0 to 255. By default, the value is 0. A larger value indicates a higher server priority.
rapid-commit	Indicates that the device supports fast address or prefix assignment, that is, two-message exchange.	-
unicast	Specifies unicast communication between the client and server during the address lease renewal process.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 or DHCPv6 PD server, the DHCPv6 or DHCPv6 PD server function can be enabled in the system view or interface view. If the DHCPv6 or DHCPv6 PD server function is enabled in the interface view, the configuration information only takes effect on the interfaces and only one IPv6 address pool can be specified on an interface.

The DHCPv6 or DHCPv6 PD server and DHCPv6 clients are in different link scopes and a DHCPv6 relay exists. If the DHCPv6 or DHCPv6 PD server function is enabled in the interface view, configuration parameters such as IPv6 addresses or prefixes are assigned only to the clients in one network segment connected to the DHCPv6 relay, because only one IPv6 address pool can be specified on an interface. If configuration parameters such as IPv6 addresses or prefixes need to be assigned to the DHCPv6 clients in multiple network segments through the DHCPv6 relay, enable the DHCPv6 or DHCPv6 PD server function in the system view.

The configuration method of enabling the DHCPv6 or DHCPv6 PD server function in the interface view is affected by the physical interface status. If the interface status is Down, the DHCPv6 or DHCPv6 PD server cannot successfully assign network configuration parameters to clients through the DHCPv6 relay. When the DHCPv6 or DHCPv6 PD server function is enabled in the system view and there are multiple reachable routes between the DHCPv6 relay and DHCPv6 or DHCPv6 PD server, configuration parameters such as IPv6 addresses can be assigned to clients through the DHCPv6 relay as long as one route between the DHCPv6 relay and DHCPv6 or DHCPv6 PD server is reachable. This improves reliability of the configuration information obtained by the clients. In addition, no configuration is required on the interface, which reduces the administrator's maintenance workload.

When functioning as a DHCPv6 or DHCPv6 PD server, the device may be configured with multiple IPv6 address pools. After receiving the DHCPv6 request packets, the DHCPv6 or DHCPv6 PD server chooses the IPv6 address pool based on the following rules:

- When the device functions as the DHCPv6 server:
  - If a relay exists, the server chooses the address pool that belongs to the same link scope with the configured network prefix (using the **8.9.43 link-address** command or **8.9.1 address prefix**) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the device that functions as the DHCPv6 server only assigns configuration parameters to clients in DHCPv6 stateless mode. This indicates that the DHCPv6 server only assigns configuration

 Copyright © Huawei Technologies Co., Ltd.

parameters excluding IPv6 addresses and including DNS, NIS, and SNTP servers, and the IPv6 addresses for clients are automatically generated based on the RA packets. To enable the DHCPv6 server to assign network parameters in DHCPv6 stateful mode, enable the DHCPv6 server function in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.

- When the device functions as the DHCPv6 PD server:
  - If a relay exists, choose the address pool in the same link scope with the configured network prefix (using the **8.9.43 link-address** command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the DHCPv6 PD server function cannot be enabled in the system view and can be enabled in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.

Prerequisites

1. The DHCP function has been enabled globally using the **dhcp enable** command.
2. The IPv6 function has been enabled globally using the **ipv6** command.

Example

Enable the DHCPv6 server function in the system view, and configure the server priority to 255.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] dhcpv6 server preference 255
```

Related Topics

8.3.18 dhcp enable

8.8.20 ipv6

8.9.22 dhcpv6 server (interface view)

Function

The **dhcpv6 server** command enables the DHCPv6 server function on an interface.

The **undo dhcpv6 server** command disables the DHCPv6 server function on an interface.

By default, the DHCPv6 server function on an interface is disabled.

Format

dhcpv6 server *pool-name* [**allow-hint** | **preference** *preference-value* | **rapid-commit** | **unicast**] *

undo dhcpv6 server

Parameters

Parameter	Description	Value
pool-name	Specifies the name of the DHCPv6 address pool configured on an interface.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allow-hint	Specifies the DHCPv6 server to allocate addresses, prefixes, and prefix lengths based on the DHCPv6 client requests. If the **allow-hint** parameter is specified, the server preferentially allocates addresses, prefixes, and prefix lengths based on the client requests. If the address, prefix, and prefix length requested by a client are not within the address pool or have been allocated to another client, the server ignores the client request and allocates another available address, prefix, and prefix length to the client.	-
preference *preference-value*	Specifies the priority of the DHCPv6 server carried in the Advertise message sent by the DHCPv6 server. The DHCPv6 client chooses to obtain an IP address or prefix from the DHCPv6 server with the highest priority based on the server priority carried in the Advertise message.	The value is an integer that ranges from 0 to 255. The default value is 0. A larger value indicates a higher priority of the DHCPv6 server.
rapid-commit	Configures the DHCPv6 server to support fast address prefix allocation.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
unicast	Specifies the unicast communication between the DHCPv6 client and DHCPv6 server during IPv6 address lease.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcpv6 server** command is used on DHCP servers. If an IPv6 address pool is referenced by an interface, the interface assigns addresses or address prefixes in the address pool to clients after receiving the DHCPv6 Request messages.

Prerequisites

- DHCP functions have been enabled globally using the **dhcp enable** command.
- IPv6 functions have been enabled globally using the **ipv6** command.
- IPv6 functions have been enabled using the **ipv6 enable** command in the interface view.

Precautions

- The DHCPv6 client function, DHCPv6 relay function, and DHCPv6 server function cannot be enabled on the same interface simultaneously.
- Only one ipv6 address pool can be referenced by an interface.
- If the ipv6 address pool referenced by the interface does not exist, the DHCPv6 server function does not take effect.

Example

Associate DHCPv6 address pool Pool1 with GE 0/0/1 and set the priority of pool1 to 255.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] ipv6
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ipv6 enable
[Huawei-GigabitEthernet0/0/1] dhcpv6 server pool1 preference 255
```

 Copyright © Huawei Technologies Co., Ltd.

8.9.23 dhcpv6-server

Function

The **dhcpv6-server** command adds a DHCPv6 server or a next-hop relay agent to a DHCPv6 server group.

The **undo dhcpv6-server** command deletes a DHCPv6 server or a next-hop relay agent that is configured in a DHCPv6 server group.

By default, no DHCPv6 server or next-hop relay agent is configured in a DHCPv6 server group.

Format

dhcpv6-server *ipv6-address*

undo dhcpv6-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a DHCPv6 server or a next-hop relay agent.	The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X.

Views

DHCPv6 server group view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6-server** command is used on DHCPv6 relay agents. To ensure that the DHCPv6 relay agent can send DHCPv6 packets to multiple DHCPv6 servers, you can configure multiple DHCPv6 servers in a DHCPv6 server group. Multiple DHCPv6 servers can allocate IPv6 addresses and other network configuration information to DHCPv6 clients through the DHCPv6 relay agent.

A DHCPv6 client and a DHCPv6 server can have multiple DHCPv6 relay agents connected in between. A device functions as a DHCPv6 relay agent. If the device is connected to a DHCPv6 server, you need to specify the IPv6 address for the DHCPv6 server. If the device is connected to a next-hop relay agent, you need to specify the IPv6 address for the next-hop relay agent and specify the IPv6 address

 Copyright © Huawei Technologies Co., Ltd.

of the remote DHCPv6 server or the next-hop relay agent on the next-hop relay agent.

Prerequisites

A DHCPv6 server group has been created using the **8.9.25 dhcpv6 server group** command.

Precautions

If a DHCPv6 relay agent is connected to multiple DHCPv6 servers or next-hop relay agents, repeat this step. A maximum of 20 DHCPv6 servers or next-hop relay agents can be connected to the device.

Example

Add the DHCPv6 server at fc00:1::1 to the DHCPv6 server group named dhcp-srv1.

```
<Huawei> system-view
[Huawei] dhcpv6 server group dhcp-srv1
[Huawei-dhcpv6-server-group-dhcp-srv1] dhcpv6-server fc00:1::1
```

Related Topics

8.9.25 dhcpv6 server group

8.9.35 display dhcpv6 server group

8.9.16 dhcpv6 relay server-select

8.9.24 dhcpv6 server database

Function

The **dhcpv6 server database** command enables the device to save DHCPv6 data to storage devices.

The **undo dhcpv6 server database** command disables the device from saving DHCPv6 data to storage devices.

By default, the device is disabled from saving DHCPv6 data to storage devices.

Format

dhcpv6 server database *url* [**write-delay** *interval*]

undo dhcpv6 server database *url*

Parameters

Parameter	Description	Value
url	Specifies the path and name of the file that data is saved to.	The value is a string of 1 to 63 case-insensitive characters without spaces.

Parameter	Description	Value
write-delay *interval*	Specifies the interval at which DHCPv6 data is saved.	The value is an integer ranging from 300 to 86400, in seconds. The default value is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 or DHCPv6 PD server, run the **dhcpv6 server database** command to enable the device to save DHCPv6 data to storage devices. This avoids data loss caused by device faults. DHCPv6 data includes the last data recording time, address pool name, client DUID, IAID, address and prefix bound to the client DUID and IAID, conflicted address, and conflict detection time.

The device automatically saves current DHCPv6 data at the specified interval, and previous data files are overwritten. The interval can be set using the **write-delay** *interval* parameter.

Precautions

If the DHCPv6 client requests for lease renewal when the device (functioning as the DHCPv6 server) restarts, the device cannot receive the renewal request and the client fails to renew the lease.

Example

Configure the device to save DHCP data to the path flash:/dhcpv6.tbl and set the interval for saving data to 36000s.

```
<Huawei> system-view
[Huawei] dhcpv6 server database flash:/dhcpv6.tbl write-delay 36000
```

8.9.25 dhcpv6 server group

Function

The **dhcpv6 server group** command creates a DHCPv6 server group and enters the DHCPv6 server group view, or enters the view of a DHCPv6 server group that has been created.

The **undo dhcpv6 server group** command deletes a created DHCPv6 server group.

 Copyright © Huawei Technologies Co., Ltd.

By default, no DHCPv6 server group is created.

Format

dhcpv6 server group *group-name*

undo dhcpv6 server group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCPv6 server group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

The **dhcpv6 server group** command is used on DHCPv6 relay agents. Generally, a DHCPv6 relay agent serves multiple DHCPv6 servers. You can run the **dhcpv6 server group** command to create a DHCPv6 server group to manage all the DHCPv6 servers that share the DHCPv6 relay agent. The DHCPv6 server group allocates IPv6 addresses and other network configuration information to users connected to the DHCPv6 relay agent.

Follow-up Procedure

- After a DHCPv6 server group is configured, run the **dhcpv6-server** command to add DHCPv6 servers to the DHCPv6 server group.
- When configuring IP address for DHCPv6 servers, run the **dhcpv6 relay server-select** command on an interface to select the DHCPv6 server group of the DHCPv6 relay agent.

Precautions

A maximum of 32 DHCPv6 server groups can be configured on the device. A maximum of 20 DHCPv6 servers can be added to a DHCPv6 server group.

Example

Create a DHCPv6 server group named DHCPv6-srv1.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dhcpv6 server group DHCPv6-srv1
[Huawei-dhcpv6-server-group-DHCPv6-srv1]
```

Related Topics

8.9.23 dhcpv6-server

8.9.35 display dhcpv6 server group

8.9.16 dhcpv6 relay server-select

8.9.26 display dhcpv6 client

Function

The **display dhcpv6 client** command displays DHCPv6 client information.

Format

display dhcpv6 client [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the DHCPv6 client with the specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display dhcpv6 client** command on the DHCPv6 client to check the address that is applied.

Example

Display the DHCPv6 client information.

```
<Huawei> display dhcpv6 client
Vlanif10 is in stateful DHCPv6 client and DHCPv6-PD client
mode.
Stateful DHCPv6 client is in BOUND state.
Preferred server DUID   : 00030001000098764433
  Reachable via address : FE80::200:98FF:FE76:4433
```

```
IA NA IA ID 0x000001D1 T1 30 T2 48
  Obtained     : 2018-04-18 15:08:49
  Renews       : 2018-04-18 15:09:19
  Rebinds      : 2018-04-18 15:09:37
  Address      : FC00:3::2
    Lifetime valid 120 seconds, preferred 60 seconds
    Expires at 2018-04-18 15:10:49(99 seconds left)
DNS server     : FC00:4::1
SNTP server    : FC00:9::1
               : FC00:9::2

DHCPv6-PD client is in BOUND state.
Preferred server DUID   : 00030001000098765566
  Reachable via address : FE80::200:98FF:FE76:5566
IA PD IA ID 0x000001D1 T1 40 T2 64
  Prefix name  : test
  Obtained     : 2018-04-18 15:08:37
  Renews       : 2018-04-18 15:09:17
  Rebinds      : 2018-04-18 15:09:41
  Prefix       : 194:2::/48
    Lifetime valid 150 seconds, preferred 80 seconds
    Expires at 2018-04-18 15:11:07(117 seconds left)
DNS server     : FC00:4::1
```

Table 8-96 Description of the display dhcpv6 client command output

Item	Description
Vlanif10 is in stateful DHCPv6 client and DHCPv6-PD client mode.	The VLANIF10 interface is in stateful DHCPv6 client and DHCPv6-PD client mode.
Stateful DHCPv6 client is in BOUND state.	The DHCPv6 client is in BOUND state.
Preferred server DUID	DUID of a DHCPv6 server.
Reachable via address	Source IPv6 address from which a DHCPv6 client receives packets.
Prefix name	IPv6 Prefix name that the DHCPv6 client obtains.
Obtained	Time at which the DHCPv6 client obtains an IPv6 address.
Renews	Time (T1) at which the DHCPv6 client updates the lease extension time.
Rebinds	Time (T2) at which the DHCPv6 client rebinds the lease extension time.
Address	IPv6 address that the DHCPv6 client obtains.
Prefix	IPv6 Prefix that the DHCPv6 client obtains.
Lifetime valid 120 seconds, preferred 60 seconds	The valid lifetime is 120 seconds and preferred lifetime is 60 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Expires at 2018-04-18 15:10:49(99 seconds left)	The address used by the DHCPv6 client will expire at 2018-04-18 15:10:49, and there are 99 seconds left.
DNS server	IPv6 address of the DNS server that the DHCPv6 client obtains.
SNTP server	IPv6 address of the SNTP server that the DHCPv6 client obtains.

Related Topics

8.9.4 dhcpv6 client information-request

8.9.28 display dhcpv6 client statistics

8.9.50 reset dhcpv6 client statistics

8.9.27 display dhcpv6 client prefix

Function

The **display dhcpv6 client prefix** command displays the IPv6 address prefix obtained by the device.

Format

display dhcpv6 client prefix [**name** *prefix-name*]

Parameters

Parameter	Description	Value
name *prefix-name*	Specifies the IPv6 address prefix name.	The value must be an existing IPv6 address prefix name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display dhcpv6 client prefix** command to view IPv6 address prefixes on the device that functions as the DHCPv6 client.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about IPv6 prefix named **aaa** obtained by the device.

```
<Huawei> display dhcpv6 client prefix name aaa
Prefix name       : aaa
  Prefix          : FC00:3::/64
    Life time(sec): valid 172800 preferred 86400
```

Table 8-97 Description of the **display dhcpv6 client prefix** command output

Item	Description
Prefix name	IPv6 address prefix name.
Prefix	IPv6 address prefix.
Life time(sec)	• valid: Period during which an IPv6 address prefix is valid. • preferred: Period during which an IPv6 address prefix is valid since its lease is renewed.

Related Topics

8.9.5 dhcpv6 client pd

8.9.28 display dhcpv6 client statistics

Function

The **display dhcpv6 client statistics** command displays DHCPv6 message statistics on the DHCPv6 client.

Format

display dhcpv6 client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCPv6 message statistics on a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the device functions as a DHCPv6 client, run the **display dhcpv6 client statistics** command to view DHCPv6 message statistics on the DHCPv6 client.

Example

Display DHCPv6 message statistics on the DHCPv6 client.

```
<Huawei> display dhcpv6 client statistics
 Message statistics of interface GigabitEthernet0/0/2:
   Message                  Received
   Advertise                1
   Reply                    1
   Reconfigure              0
   Invalid                  0

   Message                  Sent
   Solicit                  1
   Request                  1
   Confirm                  0
   Renew                    0
   Rebind                   0
   Release                  0
   Decline                  0
   Information-request      0
```

Table 8-98 Description of the display dhcpv6 client statistics command output

Item	Description
Message	Message type.
Received	Number of received messages.
Advertise	Number of Advertise messages received by the DHCPv6 client.
Reply	Number of Reply messages received by the DHCPv6 client.
Reconfigure	Number of Reconfigure messages received by the DHCPv6 client.
Invalid	Number of unknown-type messages received by the DHCPv6 client.
Sent	Number of sent messages.
Solicit	Number of Solicit messages sent by the DHCPv6 client.
Request	Number of Request messages sent by the DHCPv6 client.
Confirm	Number of Confirm messages sent by the DHCPv6 client.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Renew	Number of Renew messages sent by the DHCPv6 client.
Rebind	Number of Rebind messages sent by the DHCPv6 client.
Release	Number of Release messages sent by the DHCPv6 client.
Decline	Number of Decline messages sent by the DHCPv6 client.
Information-request	Number of Information-request messages sent by the DHCPv6 client.

Related Topics

8.9.50 reset dhcpv6 client statistics

8.9.29 display dhcpv6 duid

Function

The **display dhcpv6 duid** command displays the DHCP unique identifier of a DHCPv6 device.

Format

display dhcpv6 duid

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A DUID identifies a DHCPv6 device. Each DHCPv6 server or client has a DUID. The **display dhcpv6 duid** command displays the DUID of a device.

Example

Display the DUID of a DHCPv6 device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display dhcpv6 duid
The device's DHCPv6 unique identifier: 0001000117C667C280FB063545B3
```

Related Topics

8.9.6 dhcpv6 duid

8.9.30 display dhcpv6 relay configuration

Function

The **display dhcpv6 relay configuration** command displays configuration information about a DHCPv6 relay agent.

Format

display dhcpv6 relay configuration [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays configuration information about the DHCPv6 relay agent with the specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command on a DHCPv6 relay agent to check configuration information about a DHCPv6 relay agent including the source interface information and whether the Option79 field is inserted into DHCP messages.

Example

Display configuration information about a DHCPv6 relay agent.

```
<Huawei> display dhcpv6 relay configuration
DHCPv6 relay running information: global
Source interface:       -
Option79 insert:        enable
DHCPv6 relay running information: Vlanif10
Source interface:       -
Option79 insert:        enable
```

Table 8-99 Description of the **display dhcpv6 relay configuration** command output

Item	Description
DHCPv6 relay running information	Configuration information about a DHCPv6 relay agent, including configuration information in the global view and interface view.
Source interface	Specifies the interface IPv6 address as the source IPv6 address for sending messages. To configure this item, run the **8.9.17 dhcpv6 relay source-interface** command.
Option79 insert	Whether to insert the Option79 field into DHCPv6 messages. The value can be: ● enable: The Option79 field is inserted into DHCPv6 messages. ● disable: The Option79 field is not inserted into DHCPv6 messages. To configure this item, run the **8.9.18 dhcpv6 relay option79 insert enable** command.

8.9.31 display dhcpv6 relay statistics

Function

Using the **display dhcpv6 relay statistics** command, you can view the statistics about DHCPv6 messages passing through the DHCPv6 relay agent.

Format

display dhcpv6 relay statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If no interface is specified, the statistics about all the DHCPv6 messages are displayed. If the interface is specified, the statistics about DHCPv6 messages on the specified interface are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device is enabled with the DHCPv6 relay function, the system takes the statistics about DHCPv6 messages passing through the DHCP relay agent. After this command is run, you can view the statistics about DHCPv6 messages passing through the DHCP relay agent.

Example

Display the statistics about DHCPv6 messages on VLANIF 10.

```
<Huawei> display dhcpv6 relay statistics interface vlanif 10
 Interface Vlanif10 :
 MessageType              Receive          Send             Error
 Solicit                  0                0                0
 Advertise                0                0                0
 Request                  0                0                0
 Confirm                  0                0                0
 Renew                    0                0                0
 Rebind                   0                0                0
 Reply                    0                0                0
 Release                  0                0                0
 Decline                  0                0                0
 Reconfigure              0                0                0
 Information-request      0                0                0
 Relay-forward            0                0                0
 Relay-reply              0                0                0
 UnknownType              0                0                0
```

Table 8-100 Description of the display dhcpv6 relay statistics command output

Item	Description
Interface	Interface enabled with related DHCPv6 functions.
MessageType	Type of DHCPv6 messages.
Receive	Number of received DHCPv6 messages.
Send	Number of sent DHCPv6 messages.
Error	Number of DHCPv6 messages that fail to be parsed.

Related Topics

8.9.15 dhcpv6 relay destination

8.9.32 display dhcpv6 pool

Function

The **display dhcpv6 pool** command displays the IPv6 address pool configurations.

Format

display dhcpv6 pool [*pool-name* [**allocated** { **address** | **prefix** } | **binding** [*duid*] | **conflict address** | *ipv6-address* | *ipv6-prefix/prefix-length*]]

Parameters

Parameter	Description	Value
pool *pool-name*	Specifies the IPv6 address pool name.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allocated { **address** | **prefix** }	Specifies IPv6 addresses or IPv6 address prefixes that have been assigned.	-
binding [*duid*]	Specifies addresses that are bound to DUIDs.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
conflict address	Specifies the conflicted IPv6 addresses in the IPv6 address pool.	-
ipv6-address	Specifies IPv6 addresses in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-prefix/prefix-length	Specifies IPv6 prefixes in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 1 to 128.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcpv6 pool** command is used on DHCPv6 servers. The **display dhcpv6 pool** command displays information about IPv6 address pool configurations and dynamic address allocation.

Example

Display information about the IPv6 address pool **pool1**.

```
<Huawei> display dhcpv6 pool pool1
DHCPv6 pool: pool1
  Address prefix: FC00:1::/64
    Lifetime valid 4294967295 seconds, preferred 4294967295 seconds
    0 in use, 0 conflicts
  Prefix delegation: FC00:3::/60 64
    Lifetime valid 172800 seconds, preferred 86400 seconds
    0 in use
  Information refresh time: 10000
  DNS server address: FC00:4::1
  SIP server address: FC00:3::1
  NIS server address: FC00:1::2
  NISP server address: FC00:1::2
  SNTP server address: FC00:1::1
  Domain name: huawei.com
  SIP server domain name: sip.com
  NIS server domain name: nis.com
  NISP server domain name: nisp.com
  Vendor-specific option:
    Enterprise ID: 2011
      Suboption 10 address FC00:1::5
```

```
conflict-address expire-time: 61
renew-time-percent : 55
rebind-time-percent : 85
Active normal clients: 0
Active pd clients: 0
```

Table 8-101 Description of the **display dhcpv6 pool** command output

Item	Description
DHCPv6 pool	Name of the IPv6 address pool.
Address prefix	Prefix bound to the IPv6 address pool. You can set the prefix using the **8.9.1 address prefix** command.
Prefix delegation	Agent prefix bound to the IPv6 address pool. You can set the agent prefix using the **8.9.49 prefix-delegation** command.
Information refresh time	Time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration. You can set the time using the **8.9.41 information-refresh** command.
DNS server address	DNS server address configured for the IPv6 address pool. You can configure the DNS server address using the **8.9.39 dns-server (IPv6 address pool view)** command.
SIP server address	SIP server address configured for the IPv6 address pool. You can configure the SIP server address using the **8.9.56 sip-server (IPv6 address pool view)** command.
NIS server address	NIS server address configured for the IPv6 address pool. You can configure the NIS server address using the **8.9.48 nis-server** command.
NISP server address	NISP server address configured for the IPv6 address pool. You can configure the NISP server address using the **8.9.47 nisp-server** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SNTP server address	SNTP server address configured for the IPv6 address pool. You can configure the SNTP server address using the **8.9.57 sntp-server** command.
Domain name	Domain name suffix allocated by the DHCPv6 server to the client. You can configure the domain name suffix using the **8.9.38 dns-domain-name** command.
SIP server domain name	SIP domain name suffix allocated by the DHCPv6 server to the client. You can configure the SIP domain name suffix using the **8.9.55 sip-domain-name** command.
NIS server domain name	NIS domain name suffix allocated by the DHCPv6 server to the client. You can configure the NIS domain name suffix using the **8.9.45 nis-domain-name** command.
NISP server domain name	NISP domain name suffix allocated by the DHCPv6 server to the client. You can configure the NISP domain name suffix using the **8.9.46 nisp-domain-name** command.
Vendor-specific option	Vendor-defined options. You can configure the vendor-defined options using the **8.9.61 vendor-specific** and **8.9.60 suboption** commands.
conflict-address expire-time	Aging time of conflicted addresses. You can set the aging time using the **8.9.3 conflict-address expire-time** command.
renew-time-percent	The percentage of the lease renewal time in the preferred lifetime. You can set the percentage of the lease renewal time in the preferred lifetime using the **8.9.8 renew-time-percent rebind-time-percent** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
rebind-time-percent	The percentage of the lease rebinding time in the preferred lifetime. You can set the percentage of the lease rebinding time in the preferred lifetime using the **8.9.8 renew-time-percent rebind-time-percent** command.
Active normal clients	Number of DHCP clients.
Active pd clients	Number of DHCPv6 PD clients.

8.9.33 display dhcpv6 relay

Function

The **display dhcpv6 relay** command displays the configuration of the interface enabled with the DHCPv6 relay function.

Format

display dhcpv6 relay [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the configuration of the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface is specified, the configuration of all the interfaces enabled with the DHCPv6 relay function is displayed.

Example

Display the configurations of all interfaces enabled with the DHCPv6 relay function.

```
<Huawei> display dhcpv6 relay
Interface              Mode          Destination
-----------------------------------------------------------------------
GigabitEthernet1/0/1     Relay         FC00:4::3
Vlanif10               Relay        FC00:1::1:1
Vlanif10               Relay        FC00:1::1:2
-------------------------------------------------------------------------------
 Print count : 2                    Total count : 2
```

Table 8-102 Description of the **display dhcpv6 relay** command output

Item	Description
Interface	Interface enabled with DHCPv6 relay functions.
Mode	DHCPv6 function mode.
Destination	Destination address of DHCPv6 relay messages. Address pointing to the DHCPv6 server, address of the next-hop DHCPv6 relay, or DHCPv6 server group. To configure the address, run the **8.9.15 dhcpv6 relay destination** or **8.9.16 dhcpv6 relay server-select** command.
Print count	The number of interfaces enabled with DHCPv6 relay functions that are displayed.
Total count	The total number of interfaces enabled with DHCPv6 relay functions.

8.9.34 display dhcpv6 server

Function

The **display dhcpv6 server** command displays information about the DHCPv6 server function.

Format

display dhcpv6 server [**database** | [**statistics**] [**interface** *interface-type interface-number*]]

Parameters

Parameter	Description	Value
database	Displays database configurations.	-
statistics	Displays message statistics on the DHCPv6 server.	-
interface *interface-type interface-number*	Displays information about the DHCP server with a specified interface type and number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcpv6 server** command is used on DHCPv6 servers. The **display dhcpv6 server** command displays information about the DHCPv6 server function.

Example

Display information about the DHCPv6 server function.

```
<Huawei> display dhcpv6 server
 Interface                       DHCPv6 pool
 Vlanif10                        pool1
```

Table 8-103 Description of the **display dhcpv6 server** command output

Item	Description
Interface	Interface enabled with the DHCPv6 server function.
DHCPv6 pool	Name of the IPv6 pool that is configured on the interface. You can configure the IPv6 pool name using the **dhcpv6 server** command.

Related Topics

8.9.14 dhcpv6 pool

8.9.35 display dhcpv6 server group

Function

The **display dhcpv6 server group** command displays the configuration of a DHCPv6 server group.

Format

display dhcpv6 server group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a specified DHCPv6 server group. If this parameter is not specified, the configuration of all DHCPv6 server groups is displayed.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use Scenario

The **display dhcpv6 server group** command is used on DHCPv6 relay agents. You can run the **display dhcpv6 server group** command to view the configuration of DHCPv6 server groups created on a DHCPv6 relay agent.

Prerequisites

DHCPv6 server groups have been configured on the DHCPv6 relay agent using the **dhcpv6 server group** command.

Example

View the configuration of the DHCPv6 server group named group1 on the DHCPv6 relay agent.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display dhcpv6 server group group1
 DHCPv6 Group-name   : group1
   (0)   server-ip   : FC00:1::1
```

View the configuration of all the DHCPv6 server groups on the DHCPv6 relay agent.

```
<Huawei> display dhcpv6 server group
dhcpv6 server group
--------------------------------------------------------------------------------
 DHCPv6 Group-name   : g1
   (0)   server-ip   : FC00:2::1
   (1)   server-ip   : FC00:2::2
   (2)   server-ip   : FC00:2::3
   (3)   server-ip   : FC00:2::4
   (4)   server-ip   : FC00:2::5
   (5)   server-ip   : FC00:4::1
 DHCPv6 Group-name   : g2
   (0)   server-ip   : FC00:3::111
   (1)   server-ip   : FC00:3::122
   (2)   server-ip   : FC00:3::123
   (3)   server-ip   : FC00:3::124
   (4)   server-ip   : FC00:3::125
   (5)   server-ip   : FC00:3::126
   (6)   server-ip   : FC00:3::127
 DHCPv6 Group-name   : g3
   (0)   server-ip   : FC00:3::1
   (1)   server-ip   : FC00:3::2
   (2)   server-ip   : FC00:3::3
   (3)   server-ip   : FC00:3::4
   (4)   server-ip   : FC00:3::5
   (5)   server-ip   : FC00:3::6
   (6)   server-ip   : FC00:3::7
--------------------------------------------------------------------------------
 Total count : 3
```

Table 8-104 Description of the display dhcpv6 server group command output

Item	Description
DHCPv6 Group-name	Name of a DHCPv6 server group. To set this parameter, run the **8.9.25 dhcpv6 server group** command.
server-ip	IPv6 address of a DHCPv6 server in a DHCPv6 server group. To set this parameter, run the **8.9.23 dhcpv6-server** command.

Related Topics

8.9.25 dhcpv6 server group

8.3.59 dhcp-server

8.9.36 display dhcpv6 statistics

Function

The **display dhcpv6 statistics** command displays DHCPv6 packet statistics.

Format

display dhcpv6 statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device may become faulty when running the DHCPv6 service. Some fault location methods are required for administrators or device maintenance personnel to locate faults quickly. The most convenient and effective method is to provide statistics about packets and packet loss reasons. Run the **display dhcpv6 statistics** command to view DHCPv6 packet statistics.

Example

View DHCPv6 packet statistics.

```
<Huawei> display dhcpv6 statistics
Input: total 10 packets, discarded 0 packets
  Solicit              :        10,  Advertise             :        0
  Request              :         0,  Confirm               :        0
  Renew                :         0,  Rebind                :        0
  Reply                :         0,  Release               :        0
  Decline              :         0,  Reconfigure           :        0
  Information-request  :         0,  Relay-forward         :        0
  Relay-reply          :         0,  Leasequery            :        0
  Leasequery-reply     :         0,

  Max-user limit       :       831,  Add bindtable failed  :      100
Output: total 0 packets, discarded 0 packets
```

Table 8-105 Description of the display dhcpv6 statistics command output

Item	Description
Input: total x packets, discarded y packets	Statistics about DHCPv6 packets received by the device. The number of received DHCPv6 packets is x and the number of discarded DHCPv6 packets is y.
Solicit	Number of SOLICIT packets received by the device.
Advertise	Number of ADVERTISE packets received by the device.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Request	Number of REQUEST packets received by the device.
Confirm	Number of CONFIRM packets received by the device.
Renew	Number of RENEW packets received by the device.
Rebind	Number of REBIND packets received by the device.
Reply	Number of REPLY packets received by the device.
Release	Number of RELEASE packets received by the device.
Decline	Number of DECLINE packets received by the device.
Reconfigure	Number of RECONFIGURE packets received by the device.
Information-request	Number of INFORMATION-REQUEST packets received by the device.
Relay-forward	Number of RELAY-FORW packets received by the device.
Relay-reply	Number of RELAY-REPL packets received by the device.
Leasequery	Number of LEASEQUERY packets received by the device.
Leasequery-reply	Number of LEASEQUERY-REPLY packets received by the device.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Max-user limit or Add bindtable failed	Information displayed if the DHCPv6 service is abnormal. The displayed information includes: ● Max-user limit: Total number of DHCP packets discarded because the maximum number of users is exceeded. ● Add bindtable failed: Total number of DHCP packets discarded because dynamic binding entries fail to be added. ● High cpu occupancy: Total number of DHCP packets discarded because the CPU usage is excessively high. ● Port blocked: Total number of DHCP packets discarded because the inbound interface is blocked. ● Rx buffers full: Total number of DHCP packets discarded because the remaining queue length is shorter than the reserved threshold. ● L2fdb lookup failed: Total number of DHCP packets discarded because entries fail to be queried. ● Bad vlan id: Total number of DHCP packets discarded because the VLAN ID is incorrect. ● Memory exhausted: Total number of DHCP packets discarded because the memory is exhausted. ● L3if protocol down: Total number of DHCP packets discarded because the Layer 3 protocol of the source interface goes Down. ● Rate limit: Total number of DHCP packets discarded because rates of the packets exceed the limit. ● Bad packet length: Total number of DHCP packets discarded because the packet length is incorrect. ● Bad ip header length: Total number of DHCP packets discarded because the IP header length is incorrect. ● Bad ip header checksum: Total number of DHCP packets discarded because the checksum of the IP header is incorrect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Bad udp checksum: Total number of DHCP packets discarded because the checksum of the UDP header is incorrect. • Hops exceeded: Total number of DHCP packets discarded because the number of next hops is incorrect. • Bad magic cookie: Total number of DHCP packets discarded because the magic-cookie field is incorrect. • Duplicate option: Total number of DHCP packets discarded because the option fields are duplicate. • Bad option length: Total number of DHCP packets discarded because the option field length is incorrect. • End option absent: Total number of DHCP packets discarded because of the incorrect end option. • Dest-port equals source: Total number of DHCP packets discarded because the source interface is also the outbound interface. • Bad chaddr: Total number of DHCP packets discarded because the MAC address of the client is incorrect. • Bad giaddr: Total number of DHCP packets discarded because the relay gateway is incorrect. • Bad request: Total number of DHCP packets discarded because the request packets are incorrect. • Bad reply: Total number of DHCP packets discarded because the response packets are incorrect. • Bad dest udp-port: Total number of DHCP packets discarded because the destination interface is incorrect. • Bad message type: Total number of DHCP packets discarded because of incorrect destination interfaces. • L2fdb lookup failed: Total number of incoming DHCP packets discarded because entries fail to be queried.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Client transfered: Total number of DHCP packets discarded due to interface flapping. • Bad original interface: Total number of DHCP packets discarded because dynamic binding entries are added. • Bad client-id: Total number of DHCP packets discarded because the client ID is incorrect. • Bad server-id: Total number of DHCP packets discarded because the server ID is incorrect. • Bad dest-ip: Total number of DHCP packets discarded because the destination IP address is incorrect. • Other error: Total number of DHCP packets discarded due to other reasons.
Output: total x packets, discarded y packets	Statistics about DHCPv6 packets sent by the device. The number of sent DHCPv6 packets is x and the number of discarded DHCPv6 packets is y.

8.9.37 display import all

Function

The **display import all** commands displays DNS and SNTP configurations that a DHCPv6 server automatically assigns to a DHCPv6 client.

Format

display import all

Parameters

None

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Run the **8.9.62 import all (IPv6 address pool view)** command on the DHCPv6 server to enable the DHCPv6 server to automatically assign configurations of DNS server and SNTP server to DHCPv6 clients. The **display import all** command displays configurations of DNS server and SNTP server that the DHCPv6 server automatically assigns to DHCPv6 clients.

Example

Display DNS and SNTP configurations that the DHCPv6 server automatically assigns to the DHCPv6 client.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] display import all
 -------------------------------------------------------------------------------
 Parameter      Update time          Value
 -------------------------------------------------------------------------------
 dns-server     -                    -
 sntp-server    -                    -
 -------------------------------------------------------------------------------
```

Table 8-106 Description of **display import all** command output

Item	Description
Parameter	Dynamically assigned information type: ● dns-server: DNS server information ● sntp-server: SNTP server information To set the dynamically assigned information type, run the **8.9.62 import all (IPv6 address pool view)** command.
Update time	Update time of dynamically assigned information.
Value	Contents of dynamically assigned information.

8.9.38 dns-domain-name

Function

The **dns-domain-name** command configures the DNS domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo dns-domain-name** command deletes the assigned domain name suffix.

By default, no DNS domain name suffix is configured for the DHCPv6 client.

 Copyright © Huawei Technologies Co., Ltd.

Format

dns-domain-name *dns-domain-name*

undo dns-domain-name *dns-domain-name*

Parameters

Parameter	Description	Value
dns-domain-name	Specifies the DNS domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dns-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies a domain name suffix when allocating IPv6 addresses for clients. You can use the **dns-domain-name** command on the DHCPv6 server to specify a domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffix to the clients.

Precautions

A maximum of four different DNS domain names can be configured for an IPv6 address pool.

Example

Configure the domain name suffix assigned to the DHCPv6 client as **huawei.com** for the address pool **pool1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] dns-domain-name huawei.com
```

Related Topics

8.9.14 dhcpv6 pool

8.9.39 dns-server (IPv6 address pool view)

Function

The **dns-server** command configures a DNS server address for the DHCPv6 address pool.

The **undo dns-server** command deletes the configured DNS server address.

By default, no DNS server address is configured for the IPv6 address pool.

Format

dns-server *ipv6-address*

undo dns-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	DNS server IPv6 address configured for the DHCPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dns-server** command is used on DHCPv6 servers. Before a host accesses the Internet, a DNS server needs to resolve the accessed domain name to an IP address. The DHCPv6 server needs to specify the IPv6 address of the DNS server for the global address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the DNS server when allocating IPv6 addresses to the clients.

Precautions

- To specify multiple DNS servers, run the **dns-server** command to configure multiple DNS server addresses.
- A maximum of two DNS server addresses can be configured for each IPv6 address pool. The first assigned DNS server address is used as a primary address. The priority of the first configured DNS server is higher than that of the other DNS server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify a DNS server with the IPv6 address fc00:1::1 for domain name resolution when IP addresses in the address pool **global1** are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] dns-server fc00:1::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.40 excluded-address

Function

The **excluded-address** command specifies the range of the IPv6 addresses that cannot be automatically assigned to clients from the IPv6 address pool.

The **undo excluded-address** command deletes the specified range of the IPv6 addresses that cannot be automatically assigned to clients from the address pool.

By default, all IPv6 addresses in the address pool can be automatically assigned to clients.

Format

excluded-address [*prefix-name*] *start-ipv6-address* [**to** *end-ipv6-address*]

undo excluded-address [*prefix-name*] *start-ipv6-address* [**to** *end-ipv6-address*]

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of a network prefix.	The value is a string of 1 to 63 case-sensitive characters without spaces.
start-ipv6-address	Specifies the start IPv6 address that cannot be automatically assigned.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
to *end-ipv6-address*	Specifies the end IPv6 address that cannot be automatically assigned.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X. *end-ipv6-address* and *start-ipv6-address* must be on the same network segment and *end-ipv6-address* must be greater than *start-ipv6-address*. If *end-ipv6-address* is not specified, only the *start-ipv6-address* cannot be automatically assigned.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **excluded-address** command is used on DHCPv6 servers. In an address pool, some IPv6 addresses need to be reserved for other services, and some IPv6 addresses are statically assigned to certain hosts (such as the DNS server and Web server) and cannot be automatically assigned to clients. You can run the **excluded-address** command to specify the range of the IPv6 addresses that cannot be automatically assigned to clients from the IPv6 address pool.

Prerequisites

1. An address pool has been created by using the **dhcpv6 pool** command.
2. Bind an IPv6 address prefix to an address pool by using the **address prefix**

Precautions

- The excluded IPv6 address or IPv6 address segment must be in the local address pool.
- The excluded IPv6 address or IPv6 address segment cannot be automatically assigned to clients from a local address pool.

 Copyright © Huawei Technologies Co., Ltd.

- If you run the **excluded-address** command multiple times, you can specify multiple IPv6 addresses or IPv6 address segments that cannot be automatically assigned to clients.

Example

Specify IPv6 addresses fc00:1::1 to fc00:1::10 not to be automatically allocated from the address pool **global1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] address prefix fc00:1::/64
[Huawei-dhcpv6-pool-global1] excluded-address fc00:1::1 to fc00:1::10
```

Related Topics

8.9.14 dhcpv6 pool

8.9.41 information-refresh

Function

The **information-refresh** command configures the time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration.

The **undo information-refresh** command restores the default time for updating IPv6 address pool configurations.

By default, the time for updating IPv6 address pool configurations is 86400s (24 hours).

Format

information-refresh *time*

undo information-refresh

Parameters

Parameter	Description	Value
time	Specifies the time for updating configuration parameters assigned to clients through stateless DHCPv6 address autoconfiguration.	The value is an integer that ranges from 600 to 4294967295, in seconds.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

The **information-refresh** command is used on DHCPv6 servers. When the DHCPv6 server assigns configuration parameters such as the DNS, NIS, and SNTP server addresses to the DHCPv6 clients through stateless autoconfiguration, you can use the **information-refresh** command to configure the time for updating these configuration parameters.

NOTE

If a Huawei device functions as a DHCPv6 client and the time configured using the **information-refresh** command on the DHCPv6 server is larger than three days (259200 seconds), the time for updating DHCPv6 client configuration information is three days. If the time configured using the **information-refresh** command on the DHCPv6 server is less than or equal to three days, the time for updating DHCPv6 client configuration information is the actually configured value.

Example

Set the time for updating configuration parameters assigned to clients to 10000s in the address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] information-refresh 10000
```

Related Topics

8.9.14 dhcpv6 pool

8.9.42 ipv6 address auto dhcp

Function

The **ipv6 address auto dhcp** command enables an interface to obtain IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

The **undo ipv6 address auto dhcp** command disables an interface from obtaining IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

By default, the interface is disabled from obtaining IPv6 addresses and other configuration parameters using stateful DHCPv6 address autoconfiguration.

Format

ipv6 address auto dhcp [**hint** *ipv6-address*] [**rapid-commit**] [**unicast-option**]

undo ipv6 address auto dhcp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hint *ipv6-address*	Specifies the IPv6 address applied by a DHCPv6 client.	The total length is 128 bit, which is divided into eight groups. The 16 bits of each group are represented by four hexadecimal characters. The format is X:X:X:X:X:X:X:X.
rapid-commit	Specifies that a DHCPv6 client applies for an IPv6 address using two-message exchange.	-
unicast-option	Specifies that a DHCPv6 client applies for an IPv6 address using a unicast option.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **ipv6 address auto dhcp** [**rapid-commit**] command on the WAN-side Layer 3 interface or sub-interface of the device that functions as a DHCPv6 client, the client uses stateful DHCPv6 address autoconfiguration to obtain IPv6 addresses and other configuration parameters, such as addresses of the DNS and SNTP servers, from the DHCPv6 server.

Prerequisites

1. IPv6 functions have been enabled globally using the **8.8.20 ipv6** command in the system view.
2. IPv6 functions have been enabled on interfaces using the **8.8.28 ipv6 enable (interface view)** command in the interface view.
3. The IPv6 link-local address has been configured using the **ipv6 address auto link-local** or **ipv6 address** *ipv6-address* **link-local** command in the interface view.
4. The interface has been configured to automatically learn the IPv6 default route using the **ipv6 address auto global default** command in the interface view.

Precautions

The DHCPv6 server assigns an IPv6 address and other configuration parameters to a DHCPv6 client using two-message exchange only when two-message exchange

 Copyright © Huawei Technologies Co., Ltd.

is configured on both the server and client. If two-message exchange is not configured on the server or client, the server assigns an IPv6 address and other configuration parameters to the client using four-message exchange. Two-message exchange applies to the scenarios with one DHCPv6 server, while four-message exchange applies to the scenarios with multiple DHCPv6 servers.

Example

Configure the interface GE1/0/0 to obtain IPv6 addresses and other configuration parameters from the DHCPv6 server using DHCPv6 stateful address autoconfiguration.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address auto link-local
[Huawei-GigabitEthernet1/0/0] ipv6 address auto dhcp
```

Related Topics

8.8.28 ipv6 enable (interface view)

8.9.43 link-address

Function

The **link-address** command configures the network prefix in the IPv6 address pool view.

The **undo link-address** command deletes the network prefix configured in the IPv6 address pool view.

By default, no network prefix is configured in the IPv6 address pool view.

Format

link-address *ipv6-prefix/ipv6-prefix-length*

undo link-address *ipv6-prefix/ipv6-prefix-length*

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the network prefix and prefix length.	*ipv6-prefix*: The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X. *ipv6-prefix-length*: The value is an integer that ranges from 16 to 128.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DHCPv6 client needs to apply for network configuration information (for example, the IP address of the DNS server) except for the IPv6 address from the DHCPv6 server. If the **8.9.1 address prefix** is not configured in the IPv6 address pool, you can run the **link-address** command to configure the network prefix in the IPv6 address pool view.

When functioning as a DHCPv6 or DHCPv6 PD server, the device may be configured with multiple IPv6 address pools. After receiving the DHCPv6 request packets, the DHCPv6 or DHCPv6 PD server chooses the IPv6 address pool based on the following rules:

- When the device functions as the DHCPv6 server:
  - If a relay exists, the server chooses the address pool that belongs to the same link scope with the configured network prefix (using the **link-address** or **8.9.1 address prefix**command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the device that functions as the DHCPv6 server only assigns configuration parameters to clients in DHCPv6 stateless mode. This indicates that the DHCPv6 server only assigns configuration parameters excluding IPv6 addresses and including DNS, NIS, and SNTP servers, and the IPv6 addresses for clients are automatically generated based on the RA packets. To enable the DHCPv6 server to assign network parameters in DHCPv6 stateful mode, enable the DHCPv6 server function in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.
- When the device functions as the DHCPv6 PD server:
  - If a relay exists, choose the address pool in the same link scope with the configured network prefix (using the **link-address** command) based on the first link-address field that is not 0. The link-address field identifies the link scope of the DHCPv6 clients.
  - If no relay exists, the DHCPv6 PD server function cannot be enabled in the system view and can be enabled in the interface view, using the **8.9.22 dhcpv6 server (interface view)** command.

Prerequisites

Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind the IPv6 address prefix fc00:1::/64 to the DHCPv6 server address pool named pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] link-address fc00:1::/64
```

8.9.44 lock (IPv6 address pool view)

Function

The **lock** command locks the IPv6 address pool.

The **undo lock** command unlocks the address pool.

By default, the IPv6 address pool is unlocked.

Format

lock

undo lock

Parameters

None

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **lock** command is used on DHCPv6 servers. When a DHCPv6 server needs to be migrated, you simply need to migrate address pools on the DHCPv6 server to another DHCPv6 server on the live network. To retain the addresses that have been assigned to clients from a global address pool, run the **lock** command to lock the global address pool. When new users get online, they apply for IPv6 addresses from a new address pool.

Precautions

After the **lock** command is executed, the IPv6 address pool is locked. The locked IPv6 address pool does not assign addresses or extend address lease but only release addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Lock the address pool **global1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] lock
```

Related Topics

8.9.14 dhcpv6 pool

8.9.45 nis-domain-name

Function

The **nis-domain-name** command configures the NIS domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo nis-domain-name** command deletes the NIS domain name suffix assigned to the DHCPv6 client.

By default, no NIS domain name suffix is configured for the DHCPv6 client.

Format

nis-domain-name *nis-domain-name*

undo nis-domain-name *nis-domain-name*

Parameters

Parameter	Description	Value
nis-domain-name	Specifies the NIS domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **nis-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an NIS domain name suffix when allocating IPv6 addresses for clients. You can use the **nis-domain-name** command on the DHCPv6 server to specify a NIS domain name suffix for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the NIS domain name suffix to the clients.

Precautions

A maximum of four different NIS domain names can be configured for an IPv6 address pool.

Example

Configure the NIS domain name assigned to the DHCPv6 client as **nis.com** for the address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] nis-domain-name nis.com
```

Related Topics

8.9.14 dhcpv6 pool

8.9.46 nisp-domain-name

Function

The **nisp-domain-name** command configures the NISP domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo nisp-domain-name** command deletes the assigned NISP domain name suffix.

By default, no NISP domain name suffix is configured for the DHCPv6 client.

Format

nisp-domain-name *nisp-domain-name*

undo nisp-domain-name *nisp-domain-name*

Parameters

Parameter	Description	Value
nisp-domain-name	Specifies the NISP domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

 Copyright © Huawei Technologies Co., Ltd.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nisp-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an NISP domain name suffix when allocating IPv6 addresses for clients. You can use the **nisp-domain-name** command on the DHCPv6 server to specify a NISP domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffix to the clients.

Precautions

A maximum of four different NISP domain name suffixes can be configured for an IPv6 address pool.

Example

Configure the NISP domain name assigned to the DHCPv6 client as **nisp.com** for the address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] nisp-domain-name nisp.com
```

Related Topics

8.9.14 dhcpv6 pool

8.9.47 nisp-server

Function

The **nisp-server** command configures the NISP server address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo nisp-server** command deletes the configured NISP server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no NISP server address is configured for the IPv6 address pool.

Format

nisp-server *ipv6-address*

undo nisp-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Indicates the NISP server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nisp-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the NISP server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the NISP server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two NISP server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple NISP servers are specified, you need to run the **nisp-server** repeatedly to configure multiple addresses.

Example

Specify fc00:1::2 as the IPv6 address of the NISP server when the IPv6 addresses in the address pool global1 are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] nisp-server fc00:1::2
```

Related Topics

8.9.14 dhcpv6 pool

8.9.48 nis-server

Function

The **nis-server** command configures the NIS server address assigned to the DHCPv6 client for the IPv6 address pool.

 Copyright © Huawei Technologies Co., Ltd.

The **undo nis-server** command deletes the configured NIS server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no NIS server address is configured for the IPv6 address pool.

Format

nis-server *ipv6-address*

undo nis-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Indicates the NIS server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nis-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the NIS server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the NIS server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two NIS server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple NIS servers are specified, you need to run the **nis-server** repeatedly to configure multiple addresses.

Example

Specify fc00:1::2 as the IPv6 address of the NIS server when IPv6 addresses in the address pool **global1** are assigned to clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] nis-server fc00:1::2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.9.14 dhcpv6 pool

8.9.49 prefix-delegation

Function

The **prefix-delegation** command configures an agent prefix in the address pool view.

The **undo prefix-delegation** command deletes the agent prefix in the address pool view.

By default, no IPv6 address agent prefix is configured in the address pool view.

Format

prefix-delegation *ipv6-prefix/ipv6-prefix-length assign-prefix-length* [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

prefix-delegation *ipv6-prefix/ipv6-prefix-length assign-prefix-length* [**life-time preferred-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]] **valid-lifetime days** *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]]

prefix-delegation *ipv6-prefix/ipv6-prefix-length* **lock**

undo prefix-delegation *ipv6-prefix/ipv6-prefix-length* [**lock**]

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the address prefix and the prefix length bound to an IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 1 to 128.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
assign-prefix-length	Specifies the default prefix length. **NOTE** If the DHCPv6 server has been configured to allocate prefix lengths based on the DHCPv6 client requests, and the client-requested prefix length is within the range from *ipv6-prefix-length* to *assign-prefix-length*, the server allocates the prefix length based on the client request. If the client-requested prefix length is not within the preceding range or the server is not configured to allocate prefix lengths based on the DHCPv6 client requests, the server allocates the default prefix length. You can run the **dhcpv6 server allow-hint** or **dhcpv6 server** *pool-name* **allow-hint** command to configure the server to allocate prefix lengths based on the DHCPv6 client requests.	The value is an integer that ranges from 1 to 128. The *assign-prefix-length* must be greater than or equal to *ipv6-prefix-length*. The difference between the *assign-prefix-length* and *ipv6-prefix-length* must be less than or equal to 16.
life-time	Specifies the lifetime of the address prefix bound to an IPv6 address pool.	-
valid-lifetime	Specifies the valid lifetime.	The value ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preferred-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the preferred lifetime of the IPv6 prefix. The time must be no less than 1 minute.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
valid-lifetime days *days* [**hours** *hours* [**minutes** *minutes* [**seconds** *seconds*]]]	Specifies the valid lifetime of the IPv6 prefix. The time must be no less than 1 minute and cannot be less than the preferred lifetime.	• *days*: indicates days. The value is an integer that ranges from 0 to 1999. • *hours*: indicates hours. The value is an integer that ranges from 0 to 23. • *minutes*: indicates minutes. The value is an integer that ranges from 0 to 59. • *seconds*: indicates seconds. The value is an integer that ranges from 0 to 59.
lock	Locks the address prefix.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a DHCPv6 PD server, run the **prefix-delegation** command to configure an agent prefix in the address pool view. The DHCPv6 PD

client divides the obtained prefix into prefixes of subnet segments and sends an RA message on the network segment that hosts directly connect to or exchange information with hosts using the DHCPv6 protocol. The RA message contains the prefixes of subnet segments. This enables hosts to automatically configure addresses.

Precautions

- Idle addresses or prefixes are assigned to DHCPv6 clients from the IPv6 address pool. Reserved addresses, conflicted addresses, and used addresses cannot be assigned to DHCPv6 clients. Reserved addresses include unspecified addresses, multicast addresses, loopback addresses, link-local addresses, NSAP addresses, and anycast addresses (defined in RFC 2526).
- The agent prefix cannot be overlapped.
- The agent prefix cannot be overlapped with the address prefix.
- The agent prefix cannot be overlapped with the prefix statically specified by a certain user.
- When the prefix pool is deleted, all prefix leases are deleted.
- Only one agent prefix can be configured for an address pool.

Example

Configure the agent prefix of the DHCPv6 server as fc00:1::/30 for the address pool pool1, set the prefix length to 42 and the lifetime to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] prefix-delegation fc00:1::/30 42 life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool

8.9.50 reset dhcpv6 client statistics

Function

The **reset dhcpv6 client statistics** command clears DHCPv6 message statistics on the DHCPv6 client.

Format

reset dhcpv6 client statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears DHCPv6 message statistics on a specified interface. If no interface is specified, all message statistics on the DHCPv6 client are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the DHCPv6 client. Collecting statistics about the DHCPv6 messages sent and received within a specified period helps you locate DHCPv6 faults. Before collecting new statistics, run the **reset dhcpv6 client statistics** [**interface** *interface-type interface-number*] command to clear the existing message statistics. After clearing existing statistics, run the **display dhcpv6 client statistics** [**interface** *interface-type interface-number*] command to view latest message statistics.

Example

Clear message statistics on the DHCPv6 client.

```
<Huawei> reset dhcpv6 client statistics
```

8.9.51 reset dhcpv6 pool

Function

The **reset dhcpv6 pool** command clears the IPv6 address pool configured on the device.

Format

reset dhcpv6 pool *pool-name* [**allocated** { **address** | **prefix** } | **binding** [*duid*] | **conflict address** | *ipv6-address* [**to** *ipv6-address*] | *ipv6-prefix/prefix-length*]

Parameters

Parameter	Description	Value
pool *pool-name*	Specifies the IPv6 address pool name.	The value is a string of 1 to 31 characters without spaces. The value contains digits, letters, underscores (_), and dots (.).
allocated { **address** | **prefix** }	Deletes IPv6 addresses or IPv6 address prefixes that have been assigned.	-
binding [*duid*]	Deletes addresses that are bound to DUIDs.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
conflict address	Resets the conflicted IPv6 addresses in the IPv6 address pool.	-
ipv6-address [**to** *ipv6-address*]	Resets IPv6 addresses in the IPv6 address pool. If only one IPv6 address is entered, only the entered IPv6 address is reset.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-prefix/prefix-length	Resets IPv6 prefixes in the IPv6 address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M. The IPv6 address prefix length ranges from 16 to 128

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset dhcpv6 pool** command resets the address pool status. If an IPv6 address conflict occurs because two clients use the same IPv6 address, you need to set the IPv6 address pool to idle.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If a user's IPv6 address is within the IPv6 address range specified when this command is run, the user cannot continue to use the IPv6 address after this command is run, and needs to send an IPv6 address application request again.

The address pool status cannot be restored after this command is run. Therefore, exercise caution when deciding to run this command.

Example

Set the status of all the conflicted IPv6 addresses in the IPv6 address pool mypool to idle.

```
<Huawei> reset dhcpv6 pool mypool conflict address
```

Related Topics

8.9.14 dhcpv6 pool

8.9.52 reset dhcpv6 relay statistics

Function

The **reset dhcpv6 relay statistics** command clears DHCPv6 message statistics on the DHCPv6 relay agent.

Format

reset dhcpv6 relay statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. If no interface is specified, all the DHCPv6 message statistics are cleared. If an interface is specified, DHCPv6 message statistics on the specified interface are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If a device is enabled with the DHCPv6 relay function, the system takes the statistics about DHCPv6 messages passing through the DHCP relay agent. You can use the **reset dhcpv6 relay statistics** command to clear current message statistics on the DHCPv6 relay agent.

Example

Clear the DHCPv6 message statistics on VLANIF 10.

```
<Huawei> reset dhcpv6 relay statistics interface vlanif 10
```

Related Topics

8.9.31 display dhcpv6 relay statistics

8.9.53 reset dhcpv6 server statistics

Function

The **reset dhcpv6 server statistics** command clears DHCPv6 message statistics on the DHCPv6 server.

Format

reset dhcpv6 server statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If a device is enabled with the DHCPv6 server function, the system takes the statistics about DHCPv6 messages passing through the DHCPv6 server. You can

 Copyright © Huawei Technologies Co., Ltd.

use the **reset dhcpv6 server statistics** command to clear current message statistics on the DHCPv6 server.

If no interface is specified, all the DHCPv6 message statistics are cleared. If an interface is specified, DHCPv6 message statistics on the specified interface are cleared.

Example

Clear DHCPv6 message statistics.

```
<Huawei> reset dhcpv6 server statistics
```

Related Topics

8.9.34 display dhcpv6 server

8.9.54 reset dhcpv6 statistics

Function

The **reset dhcpv6 statistics** command clears DHCPv6 packet statistics.

Format

reset dhcpv6 statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Collecting statistics about the DHCPv6 messages sent and received within a specified period helps you locate DHCPv6 faults. Before collecting new statistics, run the **reset dhcpv6 statistics** command to clear the existing message statistics. After clearing existing statistics, run the **display dhcpv6 statistics** command to view latest message statistics.

Example

Clear DHCPv6 packet statistics.

```
<Huawei> reset dhcpv6 statistics
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

8.9.36 display dhcpv6 statistics

8.9.55 sip-domain-name

Function

The **sip-domain-name** command configures the SIP domain name suffix assigned by the DHCPv6 server to a DHCPv6 client.

The **undo sip-domain-name** command deletes the assigned SIP domain name suffix.

By default, no SIP domain name suffix is configured for the DHCPv6 client.

Format

sip-domain-name *sip-domain-name*

undo sip-domain-name *sip-domain-name*

Parameters

Parameter	Description	Value
sip-domain-name	Specifies the SIP domain name suffix assigned to a DHCPv6 client.	The value is a string of 1 to 63 case-insensitive characters without spaces. The value contains letters, digits, underscores (_), and dots (.).

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sip-domain-name** command is used on DHCPv6 servers. The DHCPv6 server specifies an SIP domain name when allocating IPv6 addresses for clients. You can use the **sip-domain-name** command on the DHCPv6 server to specify a SIP domain name for each global address pool. When allocating IPv6 addresses to clients, the DHCPv6 server also sends the domain name suffixes to the clients.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

A maximum of four SIP domain name suffixes can be configured for an IPv6 address pool.

Example

Configure the SIP domain name assigned to the DHCPv6 client as **sip.com** for the address pool **pool1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] sip-domain-name sip.com
```

Related Topics

8.9.14 dhcpv6 pool

8.9.56 sip-server (IPv6 address pool view)

Function

The **sip-server** command configures the SIP server address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo sip-server** command deletes the configured SIP server address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no SIP server address is configured for the IPv6 address pool.

Format

sip-server *ipv6-address*

undo sip-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	SIP server IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sip-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the SIP server for the address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the SIP server when allocating IPv6 addresses to the clients.

Precautions

- A maximum of two SIP server addresses can be configured for each address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple SIP servers are specified, you need to run the **sip-server** repeatedly to configure multiple addresses.

Example

Specify fc00:3::1 as the IPv6 address of the SIP server when the assigned IPv6 address belongs to the address pool **global1**.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] sip-server fc00:3::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.57 sntp-server

Function

The **sntp-server** command configures the SNTP server IPv6 address assigned to the DHCPv6 client for the IPv6 address pool.

The **undo sntp-server** command deletes the configured SNTP server IPv6 address assigned to the DHCPv6 client from the IPv6 address pool.

By default, no SNTP server IPv6 address is configured for the IPv6 address pool.

Format

sntp-server *ipv6-address*

undo sntp-server *ipv6-address*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of an SNTP server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sntp-server** command is used on DHCPv6 servers. The DHCPv6 server needs to specify the IPv6 address of the SNTP server for the IPv6 address pool so that the DHCPv6 client can be connected to the Internet. The DHCPv6 server specifies the IPv6 address of the SNTP server when allocating IPv6 addresses to the clients. After the clients receive the IPv6 address of the SNTP server, the clients synchronize the system time with the specified SNTP server.

Precautions

- A maximum of two SNTP server addresses can be configured for each IPv6 address pool. The first assigned address functions as the primary address, and the other address functions as a secondary address.
- When multiple SNTP servers are specified, you need to run the **sntp-server** command repeatedly to configure multiple addresses.

Example

Specify fc00:1::1 as the IPv6 address of the SNTP server when IPv6 addresses in the address pool **global1** are assigned.

```
<Huawei> system-view
[Huawei] dhcpv6 pool global1
[Huawei-dhcpv6-pool-global1] sntp-server fc00:1::1
```

Related Topics

8.9.14 dhcpv6 pool

8.9.58 static-bind address

Function

The **static-bind address** command statically binds an IPv6 address to the client DUID in the DHCPv6 address pool view.

The **undo static-bind address** command deletes the statically bound entries between the IPv6 address and the client DUID in the DHCPv6 address pool view.

By default, no IPv6 address is bound to the client DUID in the address pool view.

Format

static-bind address [*prefix-name*] *ipv6-address* **duid** *client-duid* [**iaid** *iaid*] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

undo static-bind address [*prefix-name*] *ipv6-address*

Parameters

Parameter	Description	Value
prefix-name	Specifies the name of an IPv6 address prefix name.	The value is a string of 1 to 63 case-sensitive characters without spaces.
ipv6-address	Specifies the IPv6 address statically bound to an address pool.	The 128-bit IPv6 address is divided into eight groups. Each group contains four hexadecimal digits. The format is X:X:X:X:X:X:X:X.
duid *client-duid*	Configures the DUID of the DHCPv6 client that is statically bound to the IPv6 address.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
iaid *iaid*	Specifies IA identifier value.	The value is an integer that ranges from 1 to 4294967295.
life-time	Specifies the lifetime of the bound entries.	-
valid-lifetime	Specifies the valid lifetime of the bound entries.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime of the bound entries.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime of the bound entries to infinite.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind address** command is used on DHCPv6 servers. If some special clients need to be statically assigned with fixed IPv6 addresses, bind the DUIDs of these clients to the IPv6 addresses. When receiving a request from a special client for requesting an IPv6 address, a DHCPv6 server assigns the fixed IPv6 address bound to the client DUID to this client.

Prerequisites

1. An address pool has been created by using the **dhcpv6 pool** command.
2. Bind an IPv6 address prefix to an address pool by using the **address prefix**

Example

Bind the IPv6 address fc00:1::2 with the client with DUID abcdef in address pool pool1 and set the lifetime to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] address prefix fc00:1::/64
[Huawei-dhcpv6-pool-pool1] static-bind address fc00:1::2 duid abcdef life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool

8.9.1 address prefix

8.9.59 static-bind prefix

Function

The **static-bind prefix** command statically binds an IPv6 address prefix to the DHCPv6 PD client in the DHCPv6 address pool view.

The **undo static-bind prefix** command unbinds the IPv6 address prefixes from the DHCPv6 PD clients in the DHCPv6 address pool view.

By default, no IPv6 address prefix is bound to the DHCPv6 PD client in the address pool view.

Format

static-bind prefix *ipv6-prefix/ipv6-prefix-length* **duid** *client-duid* [**iaid** *iaid-value*] [**life-time** { *valid-lifetime* | **infinite** } { *preferred-lifetime* | **infinite** }]

undo static-bind prefix *ipv6-prefix/ipv6-prefix-length*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6-prefix/ipv6-prefix-length	Specifies the IPv6 address prefix that is statically bound to an address pool.	The value is a 32-digit hexadecimal number, in the format X:X::X:X/M.
duid *client-duid*	Specifies the DUID of the DHCPv6 PD client that is statically bound to the IPv6 address prefix.	The value is a string of 2 to 256 characters in hexadecimal notation. The length of the string is an even.
iaid *iaid-value*	Specifies the IAID of the DHCPv6 PD client that is statically bound to the IPv6 address prefix.	The value is an integer that ranges from 1 to 4294967295.
life-time	Specifies the lifetime of the bound entries.	-
valid-lifetime	Specifies the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 172800, that is two days.
preferred-lifetime	Specifies the preferred lifetime. The preferred lifetime cannot exceed the valid lifetime.	The value is an integer that ranges from 60 to 172799999, in seconds. The default value is 86400, that is one day.
infinite	Sets the lifetime to infinite. When the preferred lifetime is set to infinite, the valid lifetime must be set to infinite.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **static-bind prefix** command is used on DHCPv6 PD servers. If some special DHCPv6 PD clients need to be statically assigned with fixed IPv6 address prefixes, bind the DUIDs and IAIDs of these clients to the IPv6 address prefixes. When receiving a request for applying for an IP address prefix from a special DHCPv6 PD client, a DHCPv6 PD server assigns the fixed IPv6 address prefix bound to the DUIDs and IAIDs to this client.

Prerequisites

An address pool has been created by using the **dhcpv6 pool** command.

Precautions

- When assigning addresses for DHCPv6 PD clients, bind the address prefix to the DUID of the client. The IAID of the client cannot be specified.
- The statically bound prefix cannot be overlapped with the prefix that is configured using the **prefix-delegation** command.

Example

Bind the IPv6 address prefix fc00:1::/64 to the DHCPv6 PD client with DUID abcdef and IAID 12 in address pool pool1 and set the lifetime of the binding entries to infinite.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] static-bind prefix fc00:1::/64 duid abcdef iaid 12 life-time infinite infinite
```

Related Topics

8.9.14 dhcpv6 pool
8.9.49 prefix-delegation

8.9.60 suboption

Function

The **suboption** command configures vendor-defined DHCPv6 sub-options.

The **undo suboption** command deletes vendor-defined DHCPv6 sub-options.

By default, no vendor-defined DHCPv6 sub-option is configured.

Format

suboption *suboption-code* { **address** *ipv6-address* &<1-4> | **ascii** *ascii-string* | **hex** *hex-string* }

undo suboption *suboption-code*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
suboption-code	Specifies the code of the vendor-defined DHCPv6 sub-options.	The value is an integer that ranges from 1 to 65535.
address *ipv6-address*	Specifies the vendor-defined option code as the IPv6 address type.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
ascii *ascii-string*	Specifies the vendor-defined option code as an ASCII character string.	The value is a string of 1 to 255 characters. The value contains digits, letters, underscores (_), and dots (.).
hex *hex-string*	Specifies the vendor-defined option code as a hexadecimal string.	The value is a hexadecimal numeral string with an even number of characters (such as aa or aaaa). The even number ranges from 2 to 128.

Views

Vendor-defined mode view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **suboption** command is used on DHCPv6 servers. Run the **vendor-specific** command to enter the vendor-defined mode. In this mode, configure the vendor-defined DHCPv6 options. The DHCPv6 device can carry vendor-defined options such as the TFTP server name and address, and the configuration file of the device.

The **suboption** command configures vendor-defined DHCPv6 sub-options.

Precautions

A maximum of 16 vendor-defined sub-options can be configured in the vendor-defined mode view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set Huawei-defined sub-option 10 to fc00:1::5 in the IPv6 address pool pool1 view.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] vendor-specific 2011
[Huawei-dhcpv6-pool-pool1-vs-2011] suboption 10 address fc00:1::5
```

Related Topics

8.9.14 dhcpv6 pool

8.9.61 vendor-specific

8.9.61 vendor-specific

Function

The **vendor-specific** command configures vendor-defined options for the IPv6 address pool and enter the vendor-defined mode view.

The **undo vendor-specific** command deletes vendor-defined options configured for the IPv6 address pool.

By default, no vendor-defined option is configured.

Format

vendor-specific *vendor-id*

undo vendor-specific *vendor-id*

Parameters

Parameter	Description	Value
vendor-id	Indicates the ID of the vendor, which is assigned by the IANA. 2011 is the identifier for Huawei.	The value is an integer that ranges from 1 to 4294967295.

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **vendor-specific** command is used on DHCP servers. You can use the **vendor-specific** command to enter the vendor-defined mode. In this mode, you can configure the vendor-defined DHCPv6 options. The DHCPv6 device can carry vendor-defined options such as the TFTP server name and address, and the configuration file of the device.

Precautions

A maximum of eight vendor-defined modes are configured for one IPv6 address pool. 2011 is the identifier for Huawei.

Example

Configure Huawei-defined options for the IPv6 address pool pool1.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] vendor-specific 2011
[Huawei-dhcpv6-pool-pool1-vs-2011]
```

Related Topics

8.9.14 dhcpv6 pool

8.9.62 import all (IPv6 address pool view)

Function

The **import all** command enables the device to dynamically assign configurations of the DNS server and SNTP server to DHCPv6 clients.

The **undo import all** command disables the device from dynamically assigning configurations of the DNS server and SNTP server to DHCPv6 clients.

By default, the device does not dynamically assign configurations of the DNS server and SNTP server to DHCPv6 clients.

Format

import all interface *interface-type interface-number*

undo import all

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface to which a client connects. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-

Views

IPv6 address pool view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **import all** command is used on the DHCPv6 server. You can run this command to configure the DHCPv6 server to automatically assign configurations of the DNS server and SNTP server allocated by the carrier to DHCPv6 clients.

Prerequisites

An IPv6 address pool has been created using the **8.9.14 dhcpv6 pool** command.

Example

Configure the device to dynamically assign configurations of the DNS server and SNTP server to DHCPv6 clients.

```
<Huawei> system-view
[Huawei] dhcpv6 pool pool1
[Huawei-dhcpv6-pool-pool1] import all interface vlanif 100
```

8.10 IPv6 DNS Configuration Commands

8.10.1 dns proxy ipv6 enable

Function

The **dns proxy ipv6 enable** command enables IPv6 DNS proxy.

The **undo dns proxy ipv6 enable** command disables IPv6 DNS proxy.

By default, IPv6 DNS proxy is disabled.

Format

dns proxy ipv6 enable

undo dns proxy ipv6 enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

IPv6 DNS proxy is used to forward DNS requests and reply packets between the IPv6 DNS client and DNS server. The IPv6 DNS client sends a DNS request packet to the device on which IPv6 DNS proxy is enabled. The device sends the request packet to the DNS server and sends the reply packet to the IPv6 DNS client. The device functions as the IPv6 DNS proxy to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable IPv6 DNS proxy.

```
<Huawei> system-view
[Huawei] dns proxy ipv6 enable
```

8.10.2 dns relay ipv6 enable

Function

The **dns relay ipv6 enable** command enables IPv6 DNS relay.

The **undo dns relay ipv6 enable** command disables IPv6 DNS relay.

By default, IPv6 DNS relay is disabled.

Format

dns relay ipv6 enable

undo dns relay ipv6 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IPv6 DNS relay is used to forward DNS requests and reply packets between the IPv6 DNS client and DNS server. The IPv6 DNS client sends a DNS request packet to the device on which IPv6 DNS relay is enabled. The device sends the request packet to the DNS server and sends the reply packet to the IPv6 DNS client. The

 Copyright © Huawei Technologies Co., Ltd.

device functions as the IPv6 DNS relay to provide services of the DNS server. Users do not need to interact with the DNS server directly. This function simplifies route deployment and improves performance and security of the DNS server.

Example

Enable IPv6 DNS relay.

```
<Huawei> system-view
[Huawei] dns relay ipv6 enable
```

8.10.3 display dns ipv6 dynamic-host

Function

The **display dns ipv6 dynamic-host** command displays IPv6 dynamic DNS entries saved in the cache.

Format

display dns ipv6 dynamic-host [*domain-name* | **a6**]

Parameters

Parameter	Description	Value
domain-name	Displays IPv6 entries specified the domain name suffix.	The value must be an existing domain name suffix.
a6	Displays IPv6 entries specified A6 query type.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After dynamic domain name resolution is completed, you can run the **display dns ipv6 dynamic-host** command to check dynamic IPv6 DNS entries in the domain name cache.

Example

Display the IPv6 dynamic DNS entries saved in the cache.

```
<Huawei> display dns ipv6 dynamic-host
Host                                TTL      Type   Address
```

```
www.huawei.com                    3411      IPv6   FC00:1::1

Total  :  1
```

Table 8-107 Description of the **display dns ipv6 dynamic-host** command output

Item	Description
Host	Domain name.
TTL	Time left before dynamic DNS entries saved in the domain name cache will be aged out, in seconds.
Type	Dynamic DNS entry type.
Address	IPv6 address in a dynamic cache entry.

Related Topics

8.10.10 reset dns ipv6 dynamic-host

8.10.4 display dns ipv6 forward table

Function

The **display dns ipv6 forward table** command displays the DNS forwarding table.

Format

display dns ipv6 forward table [**source-ip** *ipv6-address*]

Parameters

Parameter	Description	Value
source-ip *ipv6-address*	Specifies the source IPv6 address in query messages.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X. Two or more consecutive zeros in the address can be replaced by "::".

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After IPv6 DNS proxy or IPv6 DNS relay is enabled, you can run the **display dns ipv6 forward table** command to view the DNS forwarding table of IPv6 addresses. When the IPv6 DNS proxy or IPv6 DNS relay is attacked, the DNS forwarding table will be full. As a result, new DNS entries cannot be queried. You can run the **reset dns ipv6 forward table** command to delete all DNS entries.

Example

Display the IPv6 DNS forwarding table.

```
<Huawei> display dns ipv6 forward table
Domain name            : www.ipv6.com
Source IPv6 address    : FC00:1::5
Source port            : 49154
Source packet id       : 5
Forward packet id      : 0
Query type             : 28
VPN-Instance           : vpna
```

Table 8-108 Description of the **display dns ipv6 forward table** command output

Item	Description
Domain name	Domain name.
Source IPv6 address	Source IPv6 address of a query message.
Source port	Source port of a query message.
Source packet id	ID of a query message.
Forward packet id	ID of the forwarded packet, which corresponds to the ID of the query message.
Query type	Query type ● 28: AAAA query ● 38: A6 query
VPN-Instance	Name of the VPN instance that the DNS client belongs to.

Related Topics

8.10.11 reset dns ipv6 forward table

8.10.5 display ipv6 host

Function

The **display ipv6 host** command displays the IPv6 static DNS table.

Format

display ipv6 host

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **ipv6 host** command to configure IPv6 static DNS entries, you can run this command to check whether mappings between host names and IPv6 addresses are correct.

Example

Display the IPv6 static DNS table.

```
<Huawei> display ipv6 host
Host                Age        Flags    IPv6Address (es)
www.huawei.com        0         static          FC00:1::8
www.sohu.com          0         static          FC00:1::9
```

Table 8-109 Description of the **display ipv6 host** command output

Item	Description
Host	Host name.
Age	Aging time. The value 0 indicates that the entry is not aged out.
Flags	DNS table identifiers. The value static indicates a static domain name.
IPv6Address (es)	IPv6 address mapping the domain name.

Related Topics

8.10.9 ipv6 host

 Copyright © Huawei Technologies Co., Ltd.

8.10.6 dns server ipv6

Function

The **dns server ipv6** command configures the IPv6 address for the DNS server that resolves dynamic domain names.

The **undo dns server ipv6** command deletes the configured IPv6 address for DNS server.

By default, no IPv6 address is configured for the DNS server that resolves dynamic domain names.

Format

dns server ipv6 *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 [*ipv6-address* [*interface-type interface-number*]]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address for a DNS server.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and number of an outbound interface that communicates with the DNS server.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IPv6 DNS client must work with the DNS server to implement dynamic domain name resolution. You can run the **dns server ipv6** command to specify the

 Copyright © Huawei Technologies Co., Ltd.

IPv6 address of the DNS server. The IPv6 DNS client sends requests to the specified DNS server for domain name resolution.

Precautions

- The IPv6 address of the DNS server must be a global unicast address or link-local address.
  - If a link-local address is configured as the IPv6 address of the DNS server, specify the outbound interface for communicating with the DNS server.
  - If a global unicast address is configured as the IPv6 address of the DNS server, do not specify the outbound interface for communicating with the DNS server.
- The device supports a maximum of six IPv6 addresses of the DNS server.

Example

Configure the IPv6 address of the DNS server to fc00:1::1.

```
<Huawei> system-view
[Huawei] dns server ipv6 fc00:1::1
```

8.10.7 dns server ipv6 source-ip

Function

The **dns server ipv6 source-ip** command configures the source IPv6 address for the local end functioning as the DNS client to communicate with the IPv6 DNS server.

The **undo dns server ipv6 source-ip** command deletes the source IPv6 address for the local end functioning as the DNS client to communicate with the IPv6 DNS server.

By default, no source IPv6 address is configured for the local end functioning as the DNS client to communicate with the IPv6 DNS server.

Format

dns server ipv6 source-ip *ipv6-address*

undo dns server ipv6 source-ip

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address of the local device.	The value has 128 bits. It is represented as eight groups of four hexadecimal digits with the groups being separated by colons, in the format of X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source IPv6 address of the local device is specified, the device uses the specified source IPv6 address to communicate with the IPv6 DNS server to ensure the security check. The DNS server returns the request for a domain name to the local device along the specified route. If no source IPv6 address is configured, the DNS client needs to select a source IPv6 address according to the destination address each time it sends an IPv6 DNS request.

Precautions

To make the command take effect, pay attention to the following points:

- If the DNS server has only one reachable route containing a specified destination IPv6 address to the device, you need to specify the source IPv6 address in the DNS query request sent from the device to the DNS server.
- Ensure that the source IPv6 address is the IPv6 address of an interface or logical interface on the device, and there are reachable routes between the interface and the DNS server.
- Ensure that the source IPv6 address and the IPv6 address of the DNS server are on the same VPN or public network.

Example

Configure the source IPv6 address of the local device to fc00:1::1.

```
<Huawei> system-view
[Huawei] dns server ipv6 source-ip fc00:1::1
```

8.10.8 dns spoofing ipv6

Function

The **dns spoofing ipv6** command enables IPv6 DNS spoofing and specifies an IPv6 address in response messages.

The **undo dns spoofing ipv6** command disables IPv6 DNS spoofing.

By default, IPv6 DNS spoofing is disabled.

Format

dns spoofing ipv6 *ipv6-address*

undo dns spoofing ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies an IPv6 address in response messages.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DNS server address or route to the DNS server is not configured on the DNS proxy or relay, you can enable DNS spoofing on the device to spoof a response message with the configured IPv6 address. Currently, IPv6 DNS spoofing takes effect for only AAAA query (IPv6 address query based on domain names) and A6 query.

Prerequisites

DNS relay or DNS proxy has been enabled using the **8.4.17 dns relay enable** or **8.4.15 dns proxy enable** command in the system view.

Precautions

If you run the **dns spoofing ipv6** command multiple times, only the latest configuration takes effect.

Example

Enable DNS spoofing and specify the IPv6 address in response messages as fc00:1::8.

```
<Huawei> system-view
[Huawei] dns spoofing ipv6 fc00:1::8
```

Related Topics

8.4.17 dns relay enable

8.4.15 dns proxy enable

 Copyright © Huawei Technologies Co., Ltd.

8.10.9 ipv6 host

Function

The **ipv6 host** command configures IPv6 static DNS entries.

The **undo ipv6 host** command deletes IPv6 static DNS entries.

By default, no IPv6 static DNS entry is configured.

Format

ipv6 host *host-name ipv6-address*

undo ipv6 host *host-name* [*ipv6-address*]

Parameters

Parameter	Description	Value
host-name	Specifies the host name.	The value is a string of 1 to 255 case-sensitive characters without any space. The value must contain at least one letter, and can consist of letters, digits, hyphens (-), dots (.), and underscores (_).
ipv6-address	Specifies the IPv6 address mapping the host name.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When device functions as a DNS proxy or DNS client and requests the IPv6 address mapping a domain name, the device searches for the specified domain

 Copyright © Huawei Technologies Co., Ltd.

name in the static DNS table to obtain the mapping IPv6 address. The **ipv6 host** command configures IPv6 static DNS entries.

Precautions

Each domain name supports a maximum of 8 IPv6 addresses.

Example

Configures IPv6 static DNS entries mapping the host named **www.huawei.com**.

```
<Huawei> system-view
[Huawei] ipv6 host www.huawei.com fc00:1::8
```

Related Topics

8.10.5 display ipv6 host

8.10.10 reset dns ipv6 dynamic-host

Function

The **reset dns ipv6 dynamic-host** command clears IPv6 dynamic DNS entries saved in the cache.

Format

reset dns ipv6 dynamic-host

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

IPv6 dynamic DNS entries cannot be restored after being deleted. Confirm the action before you run the command.

Example

Clear IPv6 dynamic DNS entries saved in the cache.

```
<Huawei> reset dns ipv6 dynamic-host
```

Related Topics

8.10.3 display dns ipv6 dynamic-host

 Copyright © Huawei Technologies Co., Ltd.

8.10.11 reset dns ipv6 forward table

Function

The **reset dns ipv6 forward table** command clears entries in the IPv6 DNS forward table.

Format

reset dns ipv6 forward table [**source-ip** *ipv6-address*]

Parameters

Parameter	Description	Value
source-ip *ipv6-address*	Specifies the source IPv6 address in query messages.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

When the DNS proxy or relay is attacked, the DNS table will be full. As a result, new DNS entries cannot be queried. You can run the **display dns ipv6 forward table** command to view the DNS table, and run the **reset dns ipv6 forward table** command to clear entries in the DNS table.

Example

Clear DNS entries in the DNS table on the IPv6 DNS proxy or DNS relay.

```
<Huawei> reset dns ipv6 forward table
```

Related Topics

8.10.4 display dns ipv6 forward table

8.11 IPv6 over IPv4 Tunnel Configuration Commands

 Copyright © Huawei Technologies Co., Ltd.

8.11.1 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE tunnel or IPSec tunnel, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, IPv4 over IPv6, IPSec, MPLS TE, manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, MPLS TE, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. Normally, two tunnel interfaces in a system cannot have the same encapsulation mode, source address, and destination address.

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

On the IPSec, IPv6 over IPv4, IPv4 over IPv6, or GRE tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface by the **source** command, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Set the destination address of the GRE tunnel Tunnel 0/0/1 to 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] destination 10.1.1.1
```

Set the destination address of the GRE tunnel Tunnel 0/0/0 to 10.1.1.1 that belongs to vpn1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre
[Huawei-Tunnel0/0/0] destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.3.10 interface tunnel
8.11.3 source
8.11.4 tunnel-protocol

8.11.2 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface.	The value is in the format slot ID/subcard ID/port sequence number and varies according to the device type.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data packet over tunnels (for example, VPN tunnels), ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- IPSec
- GRE
- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface.

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces

Example

Create a tunnel interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1]
```

8.11.3 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

8.11.4 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. ● **p2p**: indicates the P2P SVPN tunnel protocol. ● **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.

 Copyright © Huawei Technologies Co., Ltd.

- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

8.12 IPv4 over IPv6 Tunnel Configuration Commands

8.12.1 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the details of the tunnel interface.

```
<Huawei> display interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Tunnel0/0/2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1), destination 10.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-08-09 18:53:47
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    15 seconds input rate 0 bits/sec, 0 packets/sec
    15 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
```

 Copyright © Huawei Technologies Co., Ltd.

```
  0 input error
  0 packets output,  0 bytes
  0 output error
  Input bandwidth utilization  : 0%
  Output bandwidth utilization : 0%
```

Table 8-110 Description of the display interface tunnel command output

Item	Description
Tunnel0/0/2 current state	Physical layer status of the Tunnel0/0/2 interface: ● UP: The interface is in normal state. ● Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status of the Tunnel0/0/2 interface: ● UP: The link layer protocol of the tunnel interface works normally. ● DOWN: The link layer protocol of the tunnel interface is abnormal.
Description	Description of the tunnel interface.
Route Port,The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet protocol processing: disabled	IP protocol is disabled.
Encapsulation is TUNNEL	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1)	The source address of the tunnel is 10.10.10.1. That is, the IP address of the GigabitEthernet 0/0/1 interface sending packets at the source side is 10.10.10.1.
destination	Destination address of the tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● IPSec: indicates tunnel mode of IPSec to protect data stream. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● SVPN: encapsulates packets into SVPN packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive disabled	The keepalive function of GRE is not enabled.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
300 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
300 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
15 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface during the last query period.
15 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface during the last query period.
0 packets input, 0 bytes 0 input error	Total packets and bytes received on the interface and the total number of defective packets.
0 packets output, 0 bytes 0 output error	Total packets and bytes sent through the interface and the total number of defective packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input bandwidth utilization	Input bandwidth usage.
Output bandwidth utilization	Output bandwidth usage.

Related Topics

12.3.11 keepalive

8.12.2 tunnel ipv4-ipv6 encapsulation-limit

Function

The **tunnel ipv4-ipv6 encapsulation-limit** command configures the maximum number of times that IPv6 encapsulation can be performed after an IPv4 packet is encapsulated the first time.

The **undo tunnel ipv4-ipv6 encapsulation-limit** command restores the default value.

By default, a maximum of four times of IPv6 encapsulation can be performed on embedded tunnel nodes.

Format

tunnel ipv4-ipv6 encapsulation-limit *encapsulation-limit*

undo tunnel ipv4-ipv6 encapsulation-limit

Parameters

Parameter	Description	Value
encapsulation-limit	Specifies the maximum number of of times for performing IPv6 encapsulation on embedded tunnel nodes.	The value is an integer that ranges from 0 to 255.

Views

System view, tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The tunnel encapsulation limit is the value of the tunnel encapsulation limit option carried in the destination option extension header in the IPv6 tunnel header.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 encapsulation-limit** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

When Huawei devices communicate with non-Huawei devices, you must run the **undo tunnel ipv4-ipv6 encapsulation-limit** command to restores the default value.

Example

Set the maximum number of times of IPv6 encapsulation to be performed on the embedded tunnel nodes of the specified IPv4 over IPv6 tunnel to 3.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 encapsulation-limit 3
```

Set the maximum number of times of IPv6 encapsulation to be performed on the embedded tunnel nodes of all specified IPv4 over IPv6 tunnels to 3 on the local device.

```
<Huawei> system-view
[Huawei] tunnel ipv4-ipv6 encapsulation-limit 3
```

8.12.3 tunnel ipv4-ipv6 flow-label

Function

The **tunnel ipv4-ipv6 flow-label** command sets the flow label value.

The **undo tunnel ipv4-ipv6 flow-label** command restores the default flow label value.

The default flow label value is 0.

Format

tunnel ipv4-ipv6 flow-label *label-value*

undo tunnel ipv4-ipv6 flow-label

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
label-value	Specifies the flow label value.	The value is an integer that ranges from 0 to 1048575.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

The flow label value of the tunnel refers to the value specified in the flow label field in the IPv6 packet header on the inbound interface of the tunnel.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 flow-label** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the flow label value of a specified IPv4 over IPv6 tunnel to 10.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 flow-label 10
```

8.12.4 tunnel ipv4-ipv6 hop-limit

Function

The **tunnel ipv4-ipv6 hop-limit** command sets the hop limit.

The **undo tunnel ipv4-ipv6 hop-limit** command restores the hop limit to the default value.

By default, the hop limit is 64.

Format

tunnel ipv4-ipv6 hop-limit *hop-limit*

 Copyright © Huawei Technologies Co., Ltd.

undo tunnel ipv4-ipv6 hop-limit

Parameters

Parameter	Description	Value
hop-limit	Specifies the hop limit.	The value is an integer that ranges from 1 to 255.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

Setting the tunnel hop limit can terminate the packet transmission when routing loops occur on the IPv6 tunnel. To make IPv6 tunnel packets reach the egress of the tunnel, the tunnel hop limit cannot be set too small.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 hop-limit** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the hop limit of the specified tunnel interface to 100.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 hop-limit 100
```

8.12.5 tunnel ipv4-ipv6 traffic-class

Function

The **tunnel ipv4-ipv6 traffic-class** command sets the traffic level of the IPv4 over IPv6 tunnel.

The **undo tunnel ipv4-ipv6 traffic-class** command restores the traffic level to the default value.

By default, the traffic level of the IPv4 over IPv6 tunnel is 0.

 Copyright © Huawei Technologies Co., Ltd.

Format

tunnel ipv4-ipv6 traffic-class { **original** | *class-value* }

undo tunnel ipv4-ipv6 traffic-class

Parameters

Parameter	Description	Value
original	Indicates that the value of the Traffic Class field in the IPv6 field of the IPv6 tunnel header uses the value in Traffic Class field of the original packet. The parameter is unavailable now.	-
class-value	Specifies the traffic level of the IPv4 over IPv6 tunnel.	The value is an integer that ranges from 0 to 255.

Views

Tunnel interface view, system view

Default Level

2: Configuration level

Usage Guidelines

The traffic level of the IPv6 tunnel packets refers to the value of the traffic class field in the tunnel packet header of the ingress on the tunnel.

- If this command is configured in the tunnel interface view, it takes effect only on the current tunnel interface.
- If this command is configured in the system view, it takes effect only on the mobile IPv6 network.

Before running the **tunnel ipv4-ipv6 traffic-class** command in the tunnel interface view, run the **tunnel-protocol ipv4-ipv6** command in the same view to set the tunnel mode to the IPv4 over IPv6 manual tunnel.

The configuration in the system view and the configuration in the tunnel interface view are independent of each other.

Example

Set the traffic level of the IPv4 over IPv6 tunnel to 10.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv4-ipv6
[Huawei-Tunnel0/0/1] tunnel ipv4-ipv6 traffic-class 10
```

 Copyright © Huawei Technologies Co., Ltd.

9 IP Unicast Routing Commands

About This Chapter

9.1 Static Route Configuration Commands
9.2 RIP Configuration Commands
9.3 RIPng Configuration Commands
9.4 OSPF Configuration Commands
9.5 OSPFv3 Configuration Commands
9.6 IPv4 IS-IS Configuration Commands
9.7 IPv6 IS-IS Configuration Commands
9.8 BGP Configuration Commands
9.9 Routing Policy Configuration Commands
9.10 IP Routing Basic Configuration Commands
9.11 PBR Configuration Commands
9.12 Route Monitoring Group Configuration Commands

9.1 Static Route Configuration Commands

9.1.1 ip route recursive-lookup bgp-vpnv4-route

Function

The **ip route recursive-lookup bgp-vpnv4-route enable** command enables a static route to be iterated to a cross route on the remote VPN.

The **ip route recursive-lookup bgp-vpnv4-route disable** command disables a static route from being iterated to a cross route on the remote VPN.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ip route recursive-lookup bgp-vpnv4-route disable** command enables a static route to be iterated to a cross route on the remote VPN.

By default, a static route can be iterated to a cross route on the remote VPN.

Format

ip route recursive-lookup bgp-vpnv4-route { **enable** | **disable** }

undo ip route recursive-lookup bgp-vpnv4-route disable

Parameters

Parameter	Description	Value
enable	Enables a static route to be iterated to a cross route on the remote VPN.	-
disable	Disables a static route from being iterated to a cross route on the remote VPN.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A static route needs to be iterated if its next hop is not directly reachable. You can run the **ip route recursive-lookup bgp-vpnv4-route enable** command to enable the static route to be iterated to a cross route on the remote VPN. Then the static route can inherit the Label and Token information about the cross route. The device can forward data through the tunnel to which the static route is iterated.

Precautions

The **ip route recursive-lookup bgp-vpnv4-route enable** command and the **undo ip route recursive-lookup bgp-vpnv4-route disable** command have the same function and do not generate the configuration in the configuration file.

Example

Enable a static route to be iterated to a cross route on the remote VPN.

```
<Huawei> system-view
[Huawei] ip route recursive-lookup bgp-vpnv4-route enable
```

Disable a static route from being iterated to a cross route on the remote VPN.

```
<Huawei> system-view
[Huawei] ip route recursive-lookup bgp-vpnv4-route disable
```

Enable a static route to be iterated to a cross route on the remote VPN.

```
<Huawei> system-view
[Huawei] undo ip route recursive-lookup bgp-vpnv4-route disable
```

9.1.2 ip route recursive-lookup blackhole protocol static

Function

The **ip route recursive-lookup blackhole protocol static disable** command prevents static routes from being iterated to blackhole routes.

The **ip route recursive-lookup blackhole protocol static enable** command allows static routes to be iterated to blackhole routes.

The **undo ip route recursive-lookup blackhole protocol static disable** command allows static routes to be iterated to blackhole routes.

By default, static routes can be iterated to blackhole routes.

Format

ip route recursive-lookup blackhole protocol static { **disable** | **enable** }

undo ip route recursive-lookup blackhole protocol static disable

Parameters

Parameter	Description	Value
disable	Prevents static routes from being iterated to blackhole routes.	-
enable	Allows static routes to be iterated to blackhole routes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a link failure occurs on a network with IGP (OSPF for example), static, and blackhole routes, the static routes may be iterated to blackhole routes to remain active. The static routes will be preferentially selected over the OSPF routes because of a higher priority. Although active, the static routes are unreachable because they have been iterated to blackhole routes. As a result, services are interrupted. To address this problem, run the **ip route recursive-lookup blackhole protocol static disable** command to prevent the static routes from being iterated to the blackhole routes, so that the OSPF routes can be preferentially selected due to the inactivity of the static routes.

Precautions

The **ip route recursive-lookup blackhole protocol static enable** and **undo ip route recursive-lookup blackhole protocol static disable** commands have the same function, and either of them can be run.

Example

Prevent static routes from being iterated to blackhole routes.

```
<Huawei> system-view
[Huawei] ip route recursive-lookup blackhole protocol static disable
```

Allow static routes to be iterated to blackhole routes.

```
<Huawei> system-view
[Huawei] ip route recursive-lookup blackhole protocol static enable
```

Allow static routes to be iterated to blackhole routes.

```
<Huawei> system-view
[Huawei] undo ip route recursive-lookup blackhole protocol static disable
```

9.1.3 ip route-static

Function

The **ip route-static** command configures a unicast static route.

The **undo ip route-static** command deletes a unicast static route.

By default, the system does not configure IPv4 unicast static routes.

Format

ip route-static *ip-address* { *mask* | *mask-length* } { *nexthop-address* | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-instance-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** *cfg-name* | **efm-state** *interface-type interface-number* | **nqa** *admin-name test-name* } | **permanent**] [**description** *text*]

ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*]* **ldp-sync** [**description** *text*]

ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*]* [**track nqa** *admin-name test-name*] [**description** *text*]

ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [**preference** *preference* | **tag** *tag*]* **track route-monitor-group** *group-name* [**description** *text*]

ip route-static *ip-address* { *mask* | *mask-length* } **vpn-instance** *vpn-instance-name nexthop-address* [**preference** *preference* | **tag** *tag*]* [**permanent** | **track route-monitor-group** *group-name*] [**description** *text*]

ip route-static *ip-address* { *mask* | *mask-length* } *nexthop-address* [**preference** *preference* | **tag** *tag*]* [**permanent** | **track route-monitor-group** *group-name*] [**description** *text*]

undo ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*] *

undo ip route-static *ip-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*]* [**track** { **bfd-session** | **efm-state** } | **permanent**]

undo ip route-static *ip-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*]* **ldp-sync**

undo ip route-static [**track bfd-session**] **all**

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length. As 1s in a 32-bit mask must be consecutive, the mask in dotted decimal notation can be replaced by the mask length.	The value is an integer that ranges from 0 to 32.
nexthop-address	Specifies the next-hop address.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of the interface that forwards packets.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. If the VPN instance name is specified, a static route searches the routing table of the VPN instance for an outbound interface according to *nexthop-address*.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
preference *preference*	Specifies the preference of a static route. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255. The default value is 60.
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ldp-sync	Enables synchronization between LDP and static routes.	-
track bfd-session *cfg-name*	Binds a static BFD session to static routes to fast detect faults.	*cfg-name* is a string of 1 to 15 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
track efm-state *interface-type interface-number*	Detects the EFM OAM state of a specified interface.	-
track nqa *admin-name test-name*	Specifies the administrator name of an NQA test instance bound to a static route and the name of the test instance.	The values of *admin-name* and *test-name* are both a string of 1 to 32 case-sensitive characters without spaces.
permanent	Configures permanent advertisement of static routes.	-
description *text*	Configures the description of a static route.	The value is a string of 1 to 80 characters that can contain spaces.
all	Deletes all IPv4 unicast static routes.	-
dhcp	Associates the static route with DHCP so that the static route can obtain the next hop IP address dynamically.	-
track route-monitor-group *group-name*	Associates the static route with a specified route monitoring group.	The value is a string of 1 to 31 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a simple network, you only need to configure static routes to ensure that the network runs properly. When the router cannot use dynamic routing protocols or establish a route to the destination network, configure static routes.

A static route can be used for traffic forwarding only when a next hop IP address is available. If the next hop IP address manually specified for a static route changes, the device on which the static route is configured is unaware of the change. As a result, traffic fails to be forwarded along the static route. To address this problem, specify **dhcp** in the command to associate the static route with DHCP so that the static route can obtain the next hop IP address dynamically.

- If the next hop IP address obtained using DHCP changes, the static route updates it.
- If no next hop IP address can be obtained using DHCP, the static route is invalid.

After **track route-monitor-group** *group-name* is configured, the system determines whether to activate a static route based on the status of the specified route monitoring group. This allows the system to control route advertisement and ensure proper forwarding of remote traffic.

NOTE

After a static route is bound to a route monitoring group, the static route cannot be bound to a BFD session, Eth OAM, or NQA test instance.

Precautions

When configuring unicast static routes, note the following:

- Only public routes can be used for tunnel iteration.
- If no preference is configured for a static route, the static route uses the default preference 60.
- When both the destination IP address and the mask are set to 0.0.0.0, a default route is configured. If the router cannot find a route in the routing table to forward packets, the router uses the default route to forward packets.
- Setting different preferences can implement different routing management policies. For example, if multiple routes to the same destination are configured with the same preference, load balancing can be implemented. If multiple routes to the same destination are configured with different preferences, route backup can be implemented.
- You can configure the **description** *text* parameter to add the description of static routes so that the administrator can check and maintain static routes easily. You can run the **display this** command in the system view or run the **display current-configuration** command to view the descriptions of static routes.
- Ensure that the**description** *text* parameter is placed at the end of the command when it is configured. Otherwise, other parameters following **description** *text* may be incorrectly considered as the value of *text*.
- When configuring static routes, you can specify outbound interfaces or next-hop addresses based on the outbound interface type. For example, you can specify only outbound interfaces for static routes on P2P interfaces and specify only next hops for static routes on NBMA interfaces, and you must specify next hops for static routes on broadcast interfaces.

- In some cases, for example, the link layer protocol is PPP and the peer IP address is unknown, you can also specify outbound interfaces when configuring a router. In this manner, you do not need to modify the router configuration when the peer IP address changes.

If two static routes with the same destination IP address are configured, one of the routes is specified with a next hop IP address or outbound interface, and the other static route is configured with a next-hop VPN instance, without an outbound interface or next hop IP address, the latest configuration overwrites the previous one.

Static routes with the next hop associated with DHCP cannot work in load balancing mode with static routes with the same prefix that are not associated with DHCP.

Example

Set the next-hop address of the default route to 172.16.0.1.

```
<Huawei> system-view
[Huawei] ip route-static 0.0.0.0 0.0.0.0 172.16.0.1
```

Related Topics

9.10.8 display ip routing-table

9.1.4 ip route-static default-preference

Function

The **ip route-static default-preference** command sets the default preference for IPv4 static routes.

The **undo ip route-static default-preference** command restores the default preference value of IPv4 static routes.

By default, the default preference of IPv4 static routes is 60.

Format

ip route-static default-preference *preference*

undo ip route-static default-preference

Parameters

Parameter	Description	Value
preference	Specifies the default preference for IPv4 static routes. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can change the preference of a static route to change the status of the route. To change the default preference of a new IPv4 static route, run the **ip route-static default-preference** command.

Example

Set the default preference of IPv4 static routes to 70.

```
<Huawei> system-view
[Huawei] ip route-static default-preference 70
```

9.1.5 ip route-static selection-rule relay-depth

Function

The **ip route-static selection-rule relay-depth** command enables static routes to be selected based on the iteration depth.

The **undo ip route-static selection-rule relay-depth** command disables static routes from being selected based on the iteration depth.

By default, static routes are not selected based on the iteration depth.

Format

ip route-static selection-rule relay-depth

undo ip route-static selection-rule relay-depth

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent a loop when GGSN services are forwarded between boards, use the **ip route-static selection-rule relay-depth** command to enable static routes to be selected based on the iteration depth.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

In the system, some static routes have the same prefix and preference but different iteration depths. After the system enables static routes to be selected based on the iteration depth, the static route module selects the static route with the smallest iteration depth as the active route and delivers it to the FIB table. Other static routes then become inactive.

Example

Enable static routes to be selected based on the iteration depth.

```
<Huawei> system-view
[Huawei] ip route-static selection-rule relay-depth
```

9.1.6 ip route-static vpn-instance

Function

The **ip route-static vpn-instance** command configures static routes for a VPN instance.

The **undo ip route-static vpn-instance** command deletes static routes for a VPN instance.

By default, no static route is configured for a VPN instance.

Format

ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } { *nexthop-address* [**public**] | *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-destination-name nexthop-address* } [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** *cfg-name* | **efm-state** *interface-type interface-number* | **nqa** *admin-name test-name* } | **permanent**] [**description** *text*]

ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync** [**description** *text*]

ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*] * [**track nqa** *admin-name test-name*] [**description** *text*]

ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **track route-monitor-group** *group-name* [**description** *text*]

ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } [**vpn-instance** *vpn-destination-name*] *nexthop-address* [**preference** *preference* | **tag** *tag*]* **track route-monitor-group** *group-name* [**description** *text*]

undo ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } *interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*] *

undo ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } [*nexthop-address* | *interface-type interface-number* [*nexthop-address*]] [**preference** *preference* | **tag** *tag*] * [**track** { **bfd-session** | **efm-state** } | **permanent**]

undo ip route-static vpn-instance *vpn-source-name destination-address* { *mask* | *mask-length* } *interface-type interface-number* [*nexthop-address*] [**preference** *preference* | **tag** *tag*] * **ldp-sync**

undo ip route-static vpn-instance *vpn-source-name* **all**

Parameters

Parameter	Description	Value
vpn-instance *vpn-source-name*	Specifies the name of the source VPN instance. Each VPN instance has its own routing table. The configured static routes are added to the routing table of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
destination-address	Specifies the destination IP address of a static route.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address.	The value is an integer that ranges from 0 to 32.
interface-type interface-number	Specifies the type and number of the outbound interface of a static route.	-
nexthop-address	Specifies the next-hop address of a static route. If the outbound interface of a static route is a broadcast interface, the next-hop address must be specified for the static route.	The value is in dotted decimal notation.
preference *preference*	Specifies the preference of a static route.	The value is an integer that ranges from 1 to 255. If this parameter is not specified, the default preference of a static route is 60.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.
track bfd-session *cfg-name*	Binds a static BFD session to static routes to fast detect faults.	cfg-name is a string of 1 to 15 characters without spaces.
track efm-state *interface-type interface-number*	Detects the EFM OAM state of a specified interface.	-
track nqa *admin-name test-name*	Specifies the administrator name of an NQA test instance bound to a static route and the name of the test instance.	The values of *admin-name* and *test-name* are both a string of 1 to 32 case-sensitive characters without spaces.
ldp-sync	Enables synchronization between LDP and static routes.	-
permanent	Configures permanent advertisement of static routes.	-
description *text*	Specifies the description of a static route. You can specify **description** to add the description of static routes, facilitating static route query and maintenance.	The value is a string of 1 to 80 characters that can contain spaces.
vpn-instance *vpn-destination-name*	Specifies the name of the VPN instance to which the local device belongs.	The value is a string of 1 to 31 case-sensitive characters without spaces.
all	Deletes all static routes of a VPN instance.	-
dhcp	Associates the static route with DHCP so that the static route can obtain the next hop IP address dynamically.	-
track route-monitor-group *group-name*	Associates the static route with a specified route monitoring group.	The value is a string of 1 to 31 case-sensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to configure static routes for a VPN instance on a PE in the following scenarios:

- The PE connects to a CE.
- The specified VPN connects to the Internet.

A static route can be used for traffic forwarding only when a next hop IP address is available. If the next hop IP address manually specified for a static route changes, the device on which the static route is configured is unaware of the change. As a result, traffic fails to be forwarded along the static route. To address this problem, specify **dhcp** in the command to associate the static route with DHCP so that the static route can obtain the next hop IP address dynamically.

- If the next hop IP address obtained using DHCP changes, the static route updates it.
- If no next hop IP address can be obtained using DHCP, the static route is invalid.

After **track route-monitor-group** *group-name* is configured, the system determines whether to activate a static route based on the status of the specified route monitoring group. This allows the system to control route advertisement and ensure proper forwarding of remote traffic.

NOTE

After a static route is bound to a route monitoring group, the static route cannot be bound to a BFD session, Eth OAM, or NQA test instance.

Follow-up Procedure

After a static route is configured, import the static route to BGP running between PEs if the static route needs to be sent to the peer PE.

Precautions

During the configuration of a static route for a VPN instance, the next-hop address can belong to the VPN instance or a public network. When the next-hop address of the static route is a public network address, specify **public** following *nexthop-address*.

If the outbound interface of a static route is a broadcast interface, you must specify the next-hop address for the static route.

You can configure **description** *text* to add the description of static routes so that the administrator can query and maintain static routes easily. To view the description of static routes, run the **display this** command in the system view or run the **display current-configuration** command.

If two static routes with the same destination IP address are configured, one of the routes is specified with a next hop IP address or outbound interface, and the other static route is configured with a next-hop VPN instance, without an outbound interface or next hop IP address, the latest configuration overwrites the previous one.

Example

Configure a static route for VPN instance named **vpn1**, and set the destination address of the static route to 10.1.1.0/24 and next-hop address to 192.168.1.2 (IP address of VPN instance **vpn2**).

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] route-distinguisher 100:200
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] ip vpn-instance vpn2
[Huawei-vpn-instance-vpn2] route-distinguisher 300:400
[Huawei-vpn-instance-vpn2-af-ipv4] quit
[Huawei-vpn-instance-vpn2] quit
[Huawei] ip route-static vpn-instance vpn1 10.1.1.0 24 vpn-instance vpn2 192.168.1.2
```

9.1.7 ip route-static track bfd-session admindown invalid

Function

The **ip route-static track bfd-session admindown invalid** command prevents a static route from being selected if its bound BFD session is in AdminDown state.

The **undo ip route-static track bfd-session admindown invalid** command restores the default configuration.

By default, a static route can still be selected even if its bound BFD session is in AdminDown state.

Format

ip route-static track bfd-session session-name *bfd-name* **admindown invalid**

undo ip route-static track bfd-session session-name *bfd-name* **admindown invalid**

undo ip route-static track bfd-session admindown invalid

Parameters

Parameter	Description	Value
session-name *bfd-name*	Specifies a BFD session bound to a static route.	The value is a string of 1 to 15 case-insensitive characters without spaces. If the string is enclosed within double quotation marks ("), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a static route can still be selected even if its bound BFD session is in AdminDown state. However, the static route cannot be selected by some non-Huawei devices. As a result, communication with these non-Huawei devices may fail.

To address this problem, run the **ip route-static track bfd-session admindown invalid** command to avoid selecting the static route if its bound BFD session is in AdminDown state.

Prerequisites

The BFD session specified by *bfd-name* has been created.

Precautions

The **undo ip route-static track bfd-session admindown invalid** command enables all static routes to be selected even if their bound BFD sessions are in AdminDown state.

Example

Prevent a static route from being selected if its bound BFD session is in AdminDown state.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd bfda bind peer-ip 1.1.1.1
[Huawei-bfd-session-bfda] discriminator local 20
[Huawei-bfd-session-bfda] discriminator remote 10
[Huawei-bfd-session-bfda] commit
[Huawei-bfd-session-bfda] quit
[Huawei] ip route-static track bfd-session session-name bfda admindown invalid
```

9.1.8 ipv6 route-static

Function

The **ipv6 route-static** command configures IPv6 static routes.

The **undo ipv6 route-static** command deletes configured static routes.

By default, no IPv6 static route is configured.

Format

ipv6 route-static *dest-ipv6-address prefix-length* { *interface-type interface-number* [*nexthop-ipv6-address*] | *nexthop-ipv6-address* | **vpn-instance** *vpn-*

destination-name nexthop-ipv6-address } [**preference** *preference* | **tag** *tag*]* [**track nqa** *admin-name test-name* | **permanent** | **track bfd-session** *bfd-name*] [**description** *text*]

ipv6 route-static *dest-ipv6-address prefix-length interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*]* [**description** *text*]

undo ipv6 route-static *dest-ipv6-address prefix-length* [*interface-type interface-number* [*nexthop-ipv6-address*] | *nexthop-ipv6-address*] [**preference** *preference* | **tag** *tag*]* [**permanent** | **track bfd-session**]

undo ipv6 route-static *dest-ipv6-address prefix-length interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*]*

undo ipv6 route-static all

undo ipv6 route-static track bfd-session session-name *session-name*

Parameters

Parameter	Description	Value
dest-ipv6-address	Specifies the destination IPv6 address.	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.
prefix-length	Specifies the length of an IPv6 prefix, namely, the number of consecutive 1s in the mask.	The value is an integer that ranges from 0 to 128.
interface-type interface-number	Specifies the type and number of an outbound interface.	-
vpn-instance *vpn-destination-name*	Specifies the name of a VPN instance. If the VPN instance name is specified, the system searches the routing table of the VPN instance for the outbound interface of a static route according to the configured next-hop address.	The value is a string of 1 to 31 case-sensitive characters without spaces.
nexthop-ipv6-address	Specifies the next-hop IPv6 address	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.
dhcp	Associates the static route with DHCP so that the static route can obtain the next hop IPv6 address dynamically.	-
preference *preference*	Specifies the preference of an IPv6 static route.	The value is an integer that ranges from 1 to 255. The default value is 60.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.
track nqa *admin-name test-name*	Specifies the administrator name and test name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported.
permanent	Enables permanent advertisement for the IPv6 static route.	-
description *text*	Specifies the description of a static route.	The value is a string of 1 to 80 characters that can contain spaces.
all	Deletes all IPv6 static routes.	-
track bfd-session *bfd-name*	Specifies the BFD session bound to a static route.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported.
session-name *session-name*	Specifies the BFD session name bound to a static route.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a simple network, you only need to configure static routes to ensure that the network runs properly. When the router cannot use dynamic routing protocols or establish a route to the destination network, configure static routes on the router.

- You can configure **description** *text* to add the description of static routes so that the administrator can query and maintain static routes easily. To view the description of static routes, run the **display this** command in the system view or run the **display current-configuration** command.

- You can configure **track bfd-session** *bfd-name* to configure BFD for IPv6 static routes to bind BFD sessions to static routes. BFD sessions can detect the link status, which provides the detection mechanism for IPv6 static routes.

  NOTE

  The **undo** command with **track bfd-session** specified can only unbind the static route from the current BFD session and cannot delete the IPv6 static route.

- An IPv6 static route can be used for traffic forwarding only when a next hop IP address is available. If the next hop that is manually specified for an IPv6 static route changes, the device on which the static route is configured is unaware of the change. As a result, traffic fails to be forwarded along the static route. To address this problem, specify **dhcp** in the command to associate the static route with DHCP so that the static route can obtain a next hop IP address dynamically.
  - If the next hop IP address obtained using DHCP changes, the IPv6 static route updates it.
  - If no next hop IP address is obtained using DHCP, the IPv6 static route is invalid.

If service traffic needs to be forwarded along a specified path, you can detect the status of the path using a ping operation at a very low cost. If **permanent** is specified when configuring an IPv6 static route, the permanent advertisement function is configured for the IPv6 static route. The function detects link connectivity by pinging the destination address of the IPv6 static route.

Precautions

When configuring unicast static routes, note the following:

- If no preference is set for a static route, the static route uses the default preference 60.
- If the destination address and mask of a static route are all 0s, the static route is a default route.
- If **permanent** is specified in the command of the **undo** form, permanent advertisement is disabled for the IPv6 static route, but the static route is not deleted.

Example

Configure IPv6 static routes on the public network.

```
<Huawei> system-view
[Huawei] ipv6 route-static fc00:0:0:2001::1 128 fc00:0:0:2002::2
```

9.1.9 ipv6 route-static default-preference

Function

The **ipv6 route-static default-preference** command sets the default preference for IPv6 static routes.

The **undo ipv6 route-static default-preference** command restores the default preference of IPv6 static routes.

By default, the default preference of IPv6 static routes is 60.

Format

ipv6 route-static default-preference *preference*

undo ipv6 route-static default-preference

Parameters

Parameter	Description	Value
preference	Specifies the default preference of IPv6 static routes. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can change the preference of a static route to change the status of the route. To change the default preference of a new IPv6 static route, run the **ipv6 route-static default-preference** command.

Configuration Impact

After the **ipv6 route-static default-preference** command is used, the default preference of all the new IPv6 static routes is changed.

After a new default preference is specified, the new default preference is valid only for new IPv6 static routes but not for existing IPv6 static routes.

Example

Set the default preference of IPv6 static routes to 70.

```
<Huawei> system-view
[Huawei] ipv6 route-static default-preference 70
```

9.1.10 ipv6 route-static track bfd-session admindown invalid

Function

The **ipv6 route-static track bfd-session admindown invalid** command prevents an IPv6 static route from being selected if the BFD session associated with it is in the AdminDown state.

The **undo ipv6 route-static track bfd-session admindown invalid**command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, an IPv6 static route can still be selected by the AR even though the BFD session associated with it is in the AdminDown state.

Format

ipv6 route-static track bfd-session session-name *session-name* **admindown invalid**

undo ipv6 route-static track bfd-session session-name *session-name* **admindown invalid**

Parameters

Parameter	Description	Value
session-name *session-name*	Specifies a BFD session bound to an IPv6 static route.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an IPv6 static route can still be selected by the router even though the BFD session associated with it is in the AdminDown state, but not by non-Huawei devices. As a result, the router cannot interwork with non-Huawei devices.

To address this problem, run the **ipv6 route-static track bfd-session admindown invalid** command to configure the router not to select the IPv6 static route if the BFD session associated with it is in the AdminDown state.

Prerequisites

The BFD session specified by *bfd-name* has been created.

Precautions

The **undo ipv6 route-static track bfd-session admindown invalid** command enables all IPv6 static routes to be selected by the router even though the BFD sessions associated with them are in the AdminDown state. Running the command will delete configurations. Exercise caution when using this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Prevent the IPv6 static route from being selected if the BFD session associated with it is in the AdminDown state.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd bfda bind peer-ipv6 2001:db8:1::1
[Huawei-bfd-session-bfda] discriminator local 20
[Huawei-bfd-session-bfda] discriminator remote 10
[Huawei-bfd-session-bfda] commit
[Huawei-bfd-session-bfda] quit
[Huawei] ipv6 route-static track bfd-session session-name bfda admindown invaild
```

9.1.11 ipv6 route-static vpn-instance

Function

The **ipv6 route-static vpn-instance** command configures IPv6 static routes in a VPN instance.

The **undo ipv6 route-static vpn-instance** command withdraws IPv6 static routes in a VPN instance.

By default, the system does not configure IPv6 static routes for VPN instances.

Format

ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length* { [*interface-type interface-number* [*nexthop-ipv6-address*]] | *nexthop-ipv6-address* [**public**] | **vpn-instance** *vpn-destination-name nexthop-ipv6-address* } [**preference** *preference* | **tag** *tag*]* [**track nqa** *admin-name test-name* | **permanent** | **track bfd-session** *bfd-name*] [**description** *text*]

ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*]* [**description** *text*]

undo ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length* [*interface-type interface-number*] [*nexthop-ipv6-address*] [**preference** *preference* | **tag** *tag*]* [**permanent** | **track bfd-session**]

undo ipv6 route-static vpn-instance *vpn-instance-name dest-ipv6-address prefix-length interface-type interface-number* **dhcp** [**preference** *preference* | **tag** *tag*]*

undo ipv6 route-static vpn-instance *vpn-instance-name* **all**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. Each VPN instance has its own unicast routing table. The configured static routes are installed into the routing table of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
dest-ipv6-address	Specifies the destination IPv6 address.	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.
prefix-length	Specifies the length of an IPv6 prefix, namely, the number of consecutive 1s in the mask.	The value is an integer that ranges from 0 to 128.
interface-type	Specifies the type of an interface.	-
interface-number	Specifies the number of an interface.	-
nexthop-ipv6-address	Specifies the next-hop IPv6 address.	The value is a 32-bit hexadecimal number, in X:X:X:X:X:X:X:X format.
vpn-instance *vpn-destination-name*	Specifies the name of the destination VPN instance. If the name of the destination VPN instance is specified, a static route searches the destination VPN instance for an outbound interface based on the configured next hop address.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
public	Specifies the next-hop address as a public network address.	-
dhcp	Associates the static route with DHCP so that the static route can obtain the next hop IPv6 address dynamically.	-
preference *preference*	Specifies the preference of a static route.	The value is an integer that ranges from 1 to 255.
tag *tag*	Specifies the tag value of a static route. By configuring different tag values, you can classify static routes to implement different routing policies. For example, other routing protocols can import static routes with specified tag values through routing policies.	The value is an integer that ranges from 1 to 4294967295. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
track nqa *admin-name test-name*	Specifies the administrator name and test name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported.
permanent	Enables permanent advertisement for the IPv6 static route.	-
description *text*	Specifies the description of static routes.	The value is a string of 1 to 80 characters that can contain spaces.
all	Deletes all the IPv6 static routes configured for the specified VPN instance.	-
track bfd-session *bfd-name*	Specifies the BFD session bound to a static route. You can specify **track bfd-session** in the command to configure BFD to detect the link status and provide the detection mechanism for static routes.	A string of 1 to 15 case-insensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an IPv6 VPN network is simple, you can run the **ipv6 route-static vpn-instance** command to configure static routes for this VPN.

- To configure VPN users to access a public network, you can perform network address translation (NAT) or run the **ipv6 route-static vpn-instance** command with the keyword **public** to configure the VPN route with the next-hop address as the public network address.
- You can configure **description** *text* to add the description of static routes so that the administrator can query and maintain static routes easily. To view the description of static routes, run the **display this** command in the system view or run the **display current-configuration** command.
- An IPv6 static route can be used for traffic forwarding only when a next hop IP address is available. If the next hop that is manually specified for an IPv6 static route changes, the device on which the static route is configured is unaware of the change. As a result, traffic fails to be forwarded along the static route. To address this problem, specify **dhcp** in the command to

associate the static route with DHCP so that the static route can obtain a next hop IP address dynamically.

- If the next hop IP address obtained using DHCP changes, the IPv6 static route updates it.
- If no next hop IP address is obtained using DHCP, the IPv6 static route is invalid.

- If service traffic needs to be forwarded along a specified path, you can detect the status of the path using a ping operation at a very low cost. If **permanent** is specified when configuring an IPv6 static route, the permanent advertisement function is configured for the IPv6 static route. The function detects link connectivity by pinging the destination address of the IPv6 static route.

Precautions

If the destination address and the prefix length are set to all 0s, a default route is configured.

After a network fault occurs or the network topology changes, static routes cannot automatically change. Therefore, configure static routes with caution.

If **permanent** is specified in the command of the **undo** form, permanent advertisement is disabled for the IPv6 static route, but the static route is not deleted.

Example

Configure a default route with next-hop address FC00:0:0:2001::1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn1] ipv6-family
[Huawei-vpn1-af-ipv6] quit
[Huawei-vpn1] quit
[Huawei] ipv6 route-static vpn-instance vpn1 :: 0 fc00:0:0:2001::1
```

Related Topics

9.1.8 ipv6 route-static

9.1.12 routing-table download filter

Function

The **routing-table download filter** command configures the static route filtering function.

The **undo routing-table download filter** command cancels the static route filtering configuration.

By default, the static route filtering function is not configured.

Format

routing-table download filter acl *acl-number*

undo routing-table download filter acl *acl-number*

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If routes advertised through routing protocols by the device into a network must be different from the routes used by the device to forward packets, run the **routing-table download filter** command on the device to configure the static route filtering function. This configuration ensures that the device does not use the filtered static routes to forward packets, but it can still advertise static routes through routing protocols into the network.

Precautions

- You can specify an empty ACL (ACL number) in this command, and configure this ACL later.
- To ensure that the static route filtering function takes effect, run the **routing-table download filter** command and then configure static routes to be filtered.
- If the **undo ip soft-forward enhance enable** command has been configured, running the **routing-table download filter** command only ensures that the device does not use the filtered static routes to forward service packets. The device can still use static routes to forward the protocol packets sent by itself and advertise static routes through routing protocols into the network.

Example

Configure ACL 3100 to filter 24-bit mask routes with the destination network segment 10.215.10.0.

```
<Huawei> system-view
[Huawei] acl 3100
[Huawei-acl-adv-3100] rule 5 deny ip source 10.215.10.0 0.0.0.255
[Huawei-acl-adv-3100] quit
[Huawei] routing-table download filter acl 3100
[Huawei] ip route-static 10.215.10.0 255.255.255.0 NULL 0
```

Related Topics

19.7.4 acl (system view)

19.7.16 rule (advanced ACL view)
9.1.3 ip route-static

9.2 RIP Configuration Commands

NOTE

In practical application, in order to realize that business forwarding is not affected by motherboard failure, it is usually possible to configure BGP GR in the hardware environment of dual motherboard to make sense.

All the models support the GR Helper, and only AR3200 series support the GR Restarter.

9.2.1 bfd all-interfaces enable (RIP)

Function

The **bfd all-interfaces enable** command enables BFD on all the interfaces in a RIP process.

The **undo bfd all-interfaces enable** command disables BFD on all the interfaces in a RIP process.

By default, BFD is disabled in a RIP process.

Format

bfd all-interfaces enable

undo bfd all-interfaces enable

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

If BFD parameters are configured, but the **bfd all-interfaces enable** command is not configured, BFD sessions cannot be established.

NOTE

- The BFD priority on an interface is higher than the BFD priority on a RIP process.
- If the **rip bfd block** command is configured on an interface, the **bfd all-interfaces enable** command cannot be used to enable BFD on the interface.

Example

Enable BFD on all interfaces in a RIP process.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] rip
[Huawei-rip-1] bfd all-interfaces enable
```

Related Topics

9.2.33 rip bfd enable

9.2.2 bfd all-interfaces (RIP)

Function

The **bfd all-interfaces** command sets BFD session parameters.

The **undo bfd all-interfaces** command restores BFD session parameters to default values.

By default, the minimum intervals for receiving and sending BFD packets are 1000 ms and the detection time multiplier is 3.

Format

bfd all-interfaces { **min-rx-interval** *min-receive-value* | **min-tx-interval** *min-transmit-value* | **detect-multiplier** *detect-multiplier-value* } *

undo bfd all-interfaces { **min-rx-interval** [*min-receive-value*] | **min-tx-interval** [*min-transmit-value*] | **detect-multiplier** [*detect-multiplier-value*] } *

Parameters

Parameter	Description	Value
min-rx-interval *min-receive-value*	Specifies the minimum interval for receiving BFD packets from the peer.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-tx-interval *min-transmit-value*	Specifies the minimum interval for sending BFD packets to the peer.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
detect-multiplier *detect-multiplier-value*	Indicates the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Views

RIP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The priority of BFD configured on an interface is higher than that configured for a RIP process. If BFD is enabled on an interface, BFD sessions are established using the BFD parameters set on the interface.

Actual interval at which BFD packets are transmitted on the local device = Max { transmit-value on the local device, receive-value on the peer}.

Actual interval at which BFD packets are received on the local device = Max { transmit-value on the peer, receive-value on the local device}.

Local BFD detection time = Actual interval at which BFD packets are received on the local device x detect-multiplier-value on the peer.

Prerequisites

BFD has been enabled on all the interfaces using the **bfd all-interfaces enable** command in the RIP view.

Example

Configure BFD for a RIP process and set the minimum interval for sending BFD packets to 500 ms.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] rip
[Huawei-rip-1] bfd all-interfaces enable
[Huawei-rip-1] bfd all-interfaces min-tx-interval 500
```

Related Topics

9.2.31 rip bfd

9.2.1 bfd all-interfaces enable (RIP)

9.2.3 checkzero (RIP)

Function

The **checkzero** command enables the device to check the zero fields in RIP-1 packets.

The **undo checkzero** command disables the device from checking the zero fields in RIP-1 packets.

By default, the device checks the zero fields in RIP-1 packets.

Format

checkzero

 Copyright © Huawei Technologies Co., Ltd.

undo checkzero

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a RIP-1 packet, the values of some fields must be zero. These fields are zero fields. After zero field check is enabled, the device checks the zero fields in the RIP-1 packets and discards the packets in which the zero field values are not 0.

The **checkzero** command is valid only for RIP-1 packets.

Run the **undo checkzero** command to reduce CPU usage if there is no zero field to check (all neighbors are trusted).

Configuration Impact

By default, devices reject all RIP-1 packets in which the zero fields are not 0.

RIP-1 implementations vary with device manufacturers. If the third-party peer device allows zero fields in RIP-1 packets to carry non-zero values, run the **undo checkzero** command on the local device. The **undo checkzero** command causes potential security risks to network, so it is not recommended.

Example

Enable the device to check zero fields in RIP-1 packets.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] checkzero
```

9.2.4 default-cost (RIP)

Function

The **default-cost** command changes the default metric of imported routes.

The **undo default-cost** command restores the default metric of imported routes.

By default, the metric of imported routes is 0.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Specifies the default metric of imported routes.	The value is an integer that ranges from 0 to 15. The default value is 0.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

You can run one of the following commands to set the metric of imported routes. The following commands are listed in descending order of priorities.

- Run the **apply cost** command to set the metric of imported routes.
- Run the **import-route** (RIP) command to set the metric of imported routes.
- Run the **default-cost** (RIP) command to set the default metric of imported routes.

Example

Set the default metric for imported routes to 2.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-cost 2
```

Related Topics

9.2.22 import-route (RIP)

9.9.7 apply cost

9.2.5 default-route originate

Function

The **default-route originate** command configures RIP to originate a default route or advertise the default route in the routing table to neighbors.

The **undo default-route originate** command restores the default configuration.

By default, the device does not advertise the default route to neighbors.

 Copyright © Huawei Technologies Co., Ltd.

Format

default-route originate [**cost** *cost* | **tag** *tag* | { { **match default** | **route-policy** *route-policy-name* [**advertise-tag**] } [**avoid-learning**] }]*

undo default-route originate

Parameters

Parameter	Description	Value
cost *cost*	Specifies the metric of the default route.	The value is an integer that ranges from 0 to 15. The default value is 0.
tag *tag*	Specifies the tag value of the default route. Route tags classify routes as required. The same type of routes has the same tags. Routes are managed and controlled based on the tag by using the routing policy.	The value is an integer that ranges from 0 to 65535. The default value is 0.
match default	Indicates that the device advertises the default route imported from another routing protocol or RIP process in the routing table to neighbors.	-
avoid-learning	Disables RIP from importing default routes. If a default route in active state already exists in the routing table, the default route is set to inactive after this parameter is used.	-
route-policy *route-policy-name*	Specifies the name of the routing policy. RIP will originate the default route only if route permitted by the route policy is present as active in the routing table.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
advertise-tag	Specifies inherit the tag value applied through route-policy while advertising default route.	-

Views

RIP view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

In a routing table, the default route is a route to the network 0.0.0.0 (with the mask being 0.0.0.0). You can check whether the default route is configured by using the **display ip routing-table** command. When the destination address of a packet does not match any destination address in the routing table, the router uses a default route to forward this packet.

Example

Set the metric for the default route to 2.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-route originate cost 2
```

Set the metric for the default route in routing table to 2.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-route originate match default cost 2
```

Configure the device to originate the default route, which matches the route-policy named filter, and set the metric to 15.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-route originate route-policy filter cost 15
```

Prevent RIP from importing default routes from another routing protocol or RIP processes.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] default-route originate match default avoid-learning
```

Related Topics

9.10.8 display ip routing-table

9.2.6 description (RIP)

Function

The **description** command configures a description for a RIP process.

The **undo description** command deletes the description of a RIP process.

By default, there is no description for a RIP process.

Format

description *text*

undo description

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
text	Specifies a description for a RIP process.	It is a string of 1 to 80 case-sensitive characters. Spaces are supported.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring descriptions for RIP processes, you can easily identify RIP processes.

Configuration Impact

If the **description** command is run multiple times, only the latest configuration takes effect.

Example

Configure a description for RIP process 100.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] description this process configure the poison reverse process
```

9.2.7 display default-parameter rip

Function

The **display default-parameter rip** command displays the default RIP configuration.

Format

display default-parameter rip

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the default RIP configuration is modified, running the **display default-parameter rip** command still displays the default configuration during RIP initialization.

Example

Display the default RIP configuration.

```
<Huawei> display default-parameter rip

---------------------------------------------
 Protocol Level Default Configurations
---------------------------------------------
      RIP version   : 1
      Preference    : 100
      Checkzero     : Enabled
      Default-cost  : 0
      Auto Summary  : Enabled
      Host-route    : Enabled
      Maximum Balanced Paths : 8
      Update time   : 30 sec            Age time : 180 sec
      Garbage-collect time : 120 sec
      Default-route     : Disabled
      Verify-source     : Enabled
      Graceful restart  : Disabled
---------------------------------------------
 Interface Level Default Configurations
---------------------------------------------
  Metricin                : 0
  Metricout               : 1
  Input Packet Processing : Enabled
  Output Packet Processing: Enabled
  Poison Reverse          : Disabled
  Replay Protect          : Disabled
  Split Horizon
   For Broadcast and P2P Interfaces :  Enabled
   For NBMA Interfaces              :  Disabled
  Packet Transmit Interval          :  200 msecs
  Packet Transmit Number            :  50
  RIP Protocol Version              :  RIPv1 Compatible (Non-Standard)
```

Table 9-1 Description of the display default-parameter rip command output

Item	Description
Protocol Level Default Configurations	Default RIP protocol-level configuration.
RIP version	Default global RIP version.
Preference	Default RIP preference.
Checkzero	Whether zero fields in RIP-1 packets are checked by default.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default-cost	Default metric of routes imported from other routing protocols.
Auto Summary	Whether RIP summarization is enabled by default.
Host-route	Whether host routes are added to routing tables by default.
Maximum Balanced Paths	Default maximum number of equal-cost routes for load balancing.
Update time	Default interval for sending Update packets.
Age time	Default aging time of RIP routes.
Garbage-collect time	Default Garbage-collect time of RIP routes.
Default-route	Whether the default route is used if no entries in the routing table match packets.
Verify-source	Whether source address check is enabled by default.
Graceful restart	Whether RIP GR is enabled by default.
Interface Level Default Configurations	Default RIP configuration on the interface.
Metricin	Default metric added to routes when RIP packets are received.
Metricout	Default metric added to routes when RIP packets are sent.
Input Packet Processing	Whether an interface is allowed to receive RIP packets by default.
Output Packet Processing	Whether an interface is allowed to send RIP packets by default.
Poison Reverse	Whether poison reverse is enabled by default.
Replay Protect	Whether replay-protect is enabled by default.
Split Horizon	Whether split horizon is enabled for the following interfaces: ● Broadcast and P2P interfaces ● NBMA interfaces

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Packet Transmit Interval	Default interval for forwarding packets, in milliseconds.
Packet Transmit Number	Default number of forwarded packets.
RIP Protocol Version	Default RIP version on the interface.

9.2.8 display rip

Function

The **display rip** command displays the status and configuration of a RIP process.

Format

display rip [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Displays the status and configuration of a specified RIP process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays the status and configuration of a RIP process with the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status and configuration of a RIP process. The command output shows that two VPN instances are running. One is a public instance and another one is a VPN instance named **VPN-Instance-1**.

```
<Huawei> display rip
Public VPN-instance
    RIP process : 34
      RIP version   : 1
      Preference    : 100
      Checkzero     : Enabled
      Default-cost  : 1
      Summary       : Disabled
      Host-route    : Enabled
      Maximum number of balanced paths : 8
      Update time   : 30 sec    Age time  : 180 sec
      Suppress time : 0 sec   Garbage-collect time : 120 sec
      Graceful restart  : Disabled
      BFD               : Disabled
      Silent-interfaces : None
      Default-route     : Disabled
      Verify-source     : Enabled
      Networks          : 10.0.0.0
      Configured peers            : None
      Number of routes in database : 5
      Number of interfaces enabled : 3
      Triggered updates sent       : 0
      Number of route changes      : 0
      Number of replies to queries : 0
      Number of routes in ADV DB   : 14
Private VPN-instance name : VPN-Instance-1
    RIP process: 150
      Rip version   : 2
      Preference    : 120
      Checkzero     : Enabled
      Default-cost  : 4
      Summary       : Enabled
      Host-route    : Enabled
      Maximum number of balanced paths: 8
      Update time   : 30 sec    Age time  : 180 sec
      Suppress time : 0 sec   Garbage-collect time : 120 sec
      Graceful restart  : Disabled
      BFD               : Disabled
      Silent-interfaces : None
      Default-route : Disabled
      Verify-source : Enabled
      Networks      : 10.0.0.0
      Configured peers            : None
      Number of routes in database : 4
      Number of interfaces enabled : 3
      Triggered updates sent       : 0
      Number of route changes      : 25
      Number of replies to queries : 4
      Number of routes in ADV DB   : 14
  Total count for 2 process :
      Number of routes in database : 3
      Number of interfaces enabled : 2
      Number of routes sendable in a periodic update : 6
      Number of routes sent in last periodic update : 4
```

Table 9-2 Description of the display rip command output

Item	Description
RIP process	Running RIP process. To create a RIP process, run the **rip** command.
RIP version	Global RIP version. To set the RIP version, run the **version** command.

Item	Description
Preference	RIP preference. To set the RIP preference, run the **preference** command.
Checkzero	Whether zero fields in RIP-1 packets are checked. To check zero fields in RIP-1 packets, run the **checkzero** command.
Default-cost	Default metric for the routes imported from other routing protocols. To set the default metric, run the **default-cost** command.
Summary	Whether RIP summarization is enabled. To enable RIP summarization, run the **summary** command.
Host-route	Whether host routes are added to routing tables. To add host routes to routing tables, run the **host-route** command.
Maximum number of balanced paths	Maximum number of equal-cost routes for load balancing. To set the maximum number of equal-cost routes, run the **maximum load-balancing** command.
Update time	Interval for sending RIP Update packets. To set the interval for sending RIP Update packets, run the **timers rip** command.
Suppress time	Suppressing time of RIP routes.
Age time	Aging time of RIP routes. To set the RIP aging time, run the **timers rip** command.
Garbage-collect time	Garbage-collect time of RIP routes. To set the Garbage-collect time, run the **timers rip** command.
Graceful restart	Whether graceful restart is enabled for RIP routes.
BFD	Whether RIP is associated with BFD.
Silent-interfaces	Suppressed RIP interface, which only receive but does not send RIP packets. To specify the suppressed interface, run the **silent-interface** command.
Default-route	Whether RIP originates default routes. To configure RIP to originate default routes, run the **default-route originate** command.
Verify-source	Whether the source addresses of received RIP Update packets are checked. To check the source addresses of received RIP Update packets, run the **verify-source** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Networks	Network segment running RIP. To enable RIP for a network segment, run the **network** command.
Configured peers	RIP neighbors. To configure a RIP neighbor, run the **peer** command.
Number of routes in database	Number of routes in the RIP database.
Number of interfaces enabled	Number of interfaces running RIP.
Triggered updates sent	Number of RIP packets triggering update.
Number of route changes	Number of changed routes in the RIP database.
Number of replies to queries	Number of response packets to RIP requests.
Number of routes in ADV DB	Number of routes in each Update packet.
Number of routes sendable in a periodic update	Number of routes sent in each Update interval.
Number of routes sent in last periodic update	Number of routes sent in last Update interval.

Related Topics

9.2.29 rip
9.2.52 version (RIP)
9.2.26 preference (RIP)
9.2.3 checkzero (RIP)
9.2.4 default-cost (RIP)
9.2.48 summary (RIP)
9.2.21 host-route
9.2.23 maximum load-balancing (RIP)
9.2.50 timers rip
9.2.47 silent-interface (RIP)
9.2.5 default-route originate
9.2.51 verify-source (RIP)
9.2.24 network (RIP)
9.2.25 peer (RIP)

9.2.9 display rip bfd session

Function

The **display rip bfd session** command displays information about BFD sessions.

Format

display rip *process-id* **bfd session** { **interface** *interface-type interface-number* | *neighbor-id* | **all** }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
interface *interface-type interface-number*	Specifies the type and number of the interface on which the BFD session is configured.	-
neighbor-id	Specifies the RIP neighbor ID on which the BFD session is configured.	The value is in dotted decimal notation.
all	Displays information about BFD sessions established on all BFD-enabled interfaces in the RIP process.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display rip bfd session** command can be used to view the following information in a RIP process:

- BFD sessions of a specified process
- BFD sessions on a specified interface
- BFD sessions on a specified neighbor

Example

Display information about BFD sessions in all RIP processes with IDs of 1.

```
<Huawei> display rip 1 bfd session all
 LocalIp      :10.1.0.1         RemoteIp :10.1.0.2         BFDState  :Up
 TX           :1000             RX       :1000             Multiplier:3
 BFD Local Dis:8192             Interface:GigabitEthernet1/0/0
 Diagnostic Info: No diagnostic information
 LocalIp      :10.2.0.1         RemoteIp :10.2.0.2         BFDState  :Up
 TX           :1000             RX       :1000             Multiplier:3
 BFD Local Dis:8193             Interface:GigabitEthernet2/0/0
 Diagnostic Info: No diagnostic information
```

Table 9-3 Description of the display rip bfd session all command output

Item	Description
LocalIp	Local IP address
RemoteIp	Remote IP address
BFDState	A BFD session status can be either Up or Down.
TX	Minimum interval at which BFD packets are sent
RX	Minimum interval at which BFD packets are received
Multiplier	Remote detection multiplier
BFD Local Dis	Local discriminator dynamically assigned by BFD
Interface	Local interfaces on which BFD sessions are configured
Diagnostic Info	Diagnostic information

9.2.10 display rip database

Function

The **display rip database** command displays all the active routes in the RIP database. These routes are sent in RIP Update packets.

Format

display rip *process-id* **database** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about the routes in the RIP database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the RIP database.

```
<Huawei> display rip 100 database
-----------------------------------------------------
Advertisement State : [A] - Advertised
                      [I] - Not Advertised/Withdraw
-----------------------------------------------------
  10.0.0.0/8, cost 5, ClassfulSumm
    10.8.8.8/32, cost 5, [A], nexthop 10.1.1.2
  172.16.0.0/8, cost 7, ClassfulSumm
    172.16.9.9/32, cost 7, [A], Imported
```

Table 9-4 Description of the display rip database command output

Item	Description
Advertisement State	Route status. • [A]: Advertised • [I]: Not Advertised/Withdraw
ClassfulSumm	Classful route summarization.
cost	Link cost of a specified interface.
nexthop	Next-hop IP address.
Imported	Routes imported from other routing protocols.

Related Topics

9.2.29 rip
9.2.22 import-route (RIP)
9.2.48 summary (RIP)
9.2.24 network (RIP)

9.2.11 display rip graceful-restart

Function

The **display rip graceful-restart** command displays the GR status of RIP.

Format

display rip *process-id* **graceful-restart** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about GR status.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After receiving the GR abort notification from the helper or detecting a network topology change, the restarter stops the GR process.

Example

Display the GR status in RIP process 1.

```
<Huawei> display rip 1 graceful-restart
Restart mode     : Restarting
Restart status   : In Progress - Waiting for updates
Last complete reason : None
Update progress summary:
------------------------
Restart capable peers  : 0
 Completed: 0    Inprogress: 0
Restart incapable peers: 1
 Completed: 0    Inprogress: 1
Update period finishes in 293 seconds
```

Table 9-5 Description of the display rip graceful-restart command output

Item	Description
Restart mode	Role of a router: ● Restarting: indicates the restarter. ● Helper: indicates the helper. ● None: indicates a common router that does not participate in GR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Restart status	GR status: ● In Progress - Waiting for updates: indicates that the router is waiting for Update packets. ● In Progress - Calculating active routes: indicates that the router is calculating RIP routes. ● Aborted - Calculating active routes: indicates that the route exits from GR abnormally. ● GR completed: indicates that GR is complete.
Last complete reason	Reason that the router exits from GR for the last time: ● Unknown: indicates an unknown reason. ● Abort: indicates that the router exits from GR abnormally. ● Period Expired: indicates that GR period expires. ● Successful: indicates that the router exits from GR normally. ● None: indicates that the router does not perform GR.
Update progress summary	Title bar indicating the updated RIP progress summary
Restart capable peers	Number of neighbors that help the local router to perform GR
Completed	Number of neighbors that have sent all Update packets
Inprogress	Number of neighbors that have not sent all Update packets
Restart incapable peers	Number of neighbors that cannot help the local router to perform GR
Update period finishes in 293 seconds	Time to finish GR: 293 seconds

9.2.12 display rip interface

Function

The **display rip interface** command displays information about RIP interfaces.

Format

display rip *process-id* **interface** [*interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the type and the number of an interface.	-
verbose	Displays detailed information about a RIP interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display rip interface** command output displays the configuration and running status of RIP, which facilitate fault location and configuration verification.

Example

Display information about RIP on GE1/0/0.

```
<Huawei> display rip 1 interface gigabitethernet 1/0/0
 -------------------------------------------------------------------------------
 Interface                IP Address      State    Protocol            MTU
 -------------------------------------------------------------------------------
 GE0/0/1                   10.1.1.2        UP       RIPv1 Compatible    500
```

Table 9-6 Description of the display rip interface command output

Item	Description
Interface	RIP-enabled interfaces
IP Address	IP address of the interface
State	Status of the interface: ● UP ● DOWN
Protocol	Version of RIP running on the interface: ● RIPv1 Compatible ● RIPv2 Multicast ● RIPv2 Broadcast

Item	Description
MTU	MTU value of the link

Display detailed information about RIP on GE1/0/0.

```
<Huawei> display rip 1 interface gigabitethernet 1/0/0 verbose
 GigabitEthernet1/0/0 (10.1.1.1)
  State    :   UP            MTU : 500
  Metricin : 0
  Metricout : 1
  Input    : Enabled         Output : Enabled
  Protocol : RIPv1 Compatible (Non-Standard)
  Send version     : RIPv1 Packets
  Receive version  : RIPv1 Packets, RIPv2 Multicast and Broadcast Packets
  Poison-reverse                : Disabled
  Split-Horizon                 : Enabled
  Authentication type           : None
  Replay Protection   : Disabled
  BFD                 : Enabled (Static)
  Transmit-Interval   : 1000 ms
  Receive-Interval    : 1000 ms
  Detect-Multiplier   : 3
  Summary Address (es):  10.1.0.0/16
```

Table 9-7 Description of the display rip interface verbose command output

Item	Description
State	Status of the interface: ● UP ● DOWN
MTU	Maximum Transmission Unit
Metricin	Metric that is added to the route when the interface receives a RIP packet
Metricout	Metric that is added to the route when the interface sends a RIP packet
Input	Whether receiving packets is enabled
Output	Whether sending packets is enabled
Protocol	Protocol running on the interface: ● RIPv1 Compatible (Non-Standard) ● RIPv1 ● RIPv2 Multicast ● RIPv2 Broadcast

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Send version	Type of packets sent on the interface: ● RIPv1 packets ● RIPv2 Multicast Packets ● RIPv2 Broadcast Packets
Receive version	Type of packets received on the interface: ● RIPv1 packets ● RIPv2 Multicast and Broadcast Packets
Poison-reverse	Whether poison reverse is enabled on the interface
Split-Horizon	Whether split horizon is enabled on the interface
Authentication type	Authentication type configured on the interface
Replay Protection	Whether replay-protect is enabled on the interface
BFD	Whether BFD is enabled on the interface, including: ● Enabled (Dynamic): Indicates dynamic BFD is enabled on the interface. ● Blocked: Indicates BFD is blocked on the interface.
Transmit-Interval	Interval for sending BFD packets to the peer on the interface
Receive-Interval	Interval for receiving BFD packets from the peer on the interface
Detect-Multiplier	BFD detect multiplier value configured on the interface
Summary Address (es)	Summary address

Related Topics

9.2.29 rip

9.2.13 display rip neighbor

Function

The **display rip neighbor** command displays information about RIP neighbors.

Format

display rip *process-id* **neighbor** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about a RIP neighbor.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the neighbor in RIP process 1.

```
<Huawei> display rip 1 neighbor
-------------------------------------------------------------------
 IP Address      Interface                Type   Last-Heard-Time
-------------------------------------------------------------------
 10.1.1.1        GigabitEthernet1/0/0      RIP    0:0:7
 Number of RIP routes:1
```

Table 9-8 Description of the display rip neighbor command output

Item	Description
IP Address	IP address of the neighboring interface
Interface	Interface type
Type	Protocol used to establish adjacencies with neighbors
Last-Heard-Time	Time since the last time packets are received from neighbors
Number of RIP routes	Number of RIP routes

Display detailed information about the neighbor in RIP process 1.

```
<Huawei> display rip 1 neighbor verbose
-------------------------------------------------------------------
 IP Address      Interface               Type   Last-Heard-Time
-------------------------------------------------------------------
 10.1.1.1        GigabitEthernet1/0/0    RIP    0:0:17
```

```
Number of Active routes       : 1
Number of routes in garbage   : 0
Last Received Sequence Number : 0x0
```

Table 9-9 Description of the display rip neighbor verbose command output

Item	Description
Number of Active routes	Number of routes in the active state
Number of routes in garbage	Number of routes in the garbage state
Last Received Sequence Number	Sequence number of last received packet from neighbor

Related Topics

9.2.25 peer (RIP)

9.2.14 display rip neighbor last-nbr-down

Function

The **display rip neighbor last-nbr-down** command displays information about the last neighbor that goes Down in a RIP process.

Format

display rip *process-id* **neighbor last-nbr-down**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display rip neighbor last-nbr-down** command can be used to view information about the last 10 RIP neighbor that goes down and the reason why the neighbor goes down.

Example

View information about the last neighbor that goes Down in a RIP process.

```
<Huawei> display rip 1 neighbor last-nbr-down
 Neighbor IP Address              : 10.2.2.2
 Interface                        : GigabitEthernet1/0/0
 Reason for Neighbor down         : Interface Down
 Time at which neighbor went down : 2011-06-02 11:53:50
```

Table 9-10 Description of the display rip neighbor last-nbr-down command output

Item	Description
Neighbor IP Address	IP address of a neighbor
Interface	Interface connected to a neighbor
Reason for Neighbor down	Reason that a neighbor goes Down
Time at which neighbor went down	Time when a neighbor goes Down

9.2.15 display rip route

Function

The **display rip route** command displays all the RIP routes that are learned from other routers and view the values of different timers related to each route.

Format

display rip *process-id* **route**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a RIP process is enabled on all devices that need to run RIP and the **network** command is run to enable RIP on the related network segment, the **display rip route** command can be used to view RIP routing information.

Example

Display all the RIP routes and the values of different timers related to each route.

```
<Huawei> display rip 1 route
 Route Flags: R - RIP
              A - Aging, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer 192.168.5.1  on GigabitEthernet1/0/0
      Destination/Mask        Nexthop     Cost   Tag     Flags   Sec
       172.16.0.0/16         192.168.5.1    1     0       RA      15
     192.168.14.0/24         192.168.5.1    2     0       RA      15
```

Table 9-11 Description of the display rip route command output

Item	Description
Destination/Mask	Destination IP Address and its mask value
Nexthop	Next hop of the route
Cost	Metric value of the route
Tag	Tag that is used to differentiate internal RIP routes from external routes ● 0: indicates that a RIP route is internal route. ● 1: indicates that a RIP route is external route.
Flags	First character indicating that the route is a RIP or TRIP route Second character indicating the status of the route ● RA: indicates that a RIP route is active. ● RG: indicates that a RIP route is inactive and that the Garbage-Collect timer has been started.
Sec	Time during which a route remains in a specific state

9.2.16 display snmp-agent trap feature-name rip all

Function

The **display snmp-agent trap feature-name rip all** command displays all trap messages of the RIP module.

Format

display snmp-agent trap feature-name rip all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that manages network elements through network management software. The management agent on the network element automatically reports trap messages to the network management station. After that, the network administrator immediately takes measures to resolve network problems.

To check whether the trap functions of the RIP module are enabled, run the **display snmp-agent trap feature-name rip all** command.

Example

Display all trap messages of the RIP module.

```
<Huawei> display snmp-agent trap feature-name rip all
-----------------------------------------------------------------------------
Feature name: rip
Trap number : 2
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwRip2DBOverFlow                off                     on
hwRip2DBOverFlowResume          off                     on
```

Table 9-12 Description of the **display snmp-agent trap feature-name rip all** command output

Item	Description
Feature name	Name of the feature.
Trap number	Number of traps.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Name of the trap: • hwRip2DBOverFlow: is sent when the number of routes in the RIP database reaches the threshold. • hwRip2DBOverFlowResume: is sent when the number of routes in the RIP database falls below the threshold.
Default switch status	Default trap function status: • on: The trap function is enabled. • off: The trap function is disabled.
Current switch status	Current trap function status: • on: The trap function is enabled. • off: The trap function is disabled.

Related Topics

9.2.49 snmp-agent trap enable feature-name rip

9.2.17 display rip statistics interface

Function

The **display rip statistics interface** command displays statistics on a RIP interface, including the number of packets sent or received on the interface.

Format

display rip *process-id* **statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor** *neighbor-ip-address*] }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535.
all	Displays the statistics of all interfaces.	-
interface-type interface-number	Specifies the type and number of an interface.	-
verbose	Displays detail information about interface statistics.	-

Parameter	Description	Value
neighbor *neighbor-ip-address*	Specifies the IP address of a neighbor.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display statistics on GE1/0/0 in RIP process 1.

```
<Huawei> display rip 1 statistics interface gigabitethernet 1/0/0
GigabitEthernet1/0/0(10.0.0.11)
Statistical information          Last min     Last 5 min    Total
-----------------------------------------------------------------
Periodic updates sent            5            23            259
Triggered updates sent           5            30            408
Response packets sent            10           34            434
Response packets received        15           38            467
Response packets ignored         0            0             0
Request packets sent             1            3             8
Request packets received         4            20            40
Request packets ignored          0            0             0
Bad packets received             0            0             0
Routes received                  0            0             0
Routes sent                      0            0             0
Bad routes received              0            0             0
Packet authentication failed     0            0             0
Packet send failed               0            0             0
```

Table 9-13 Description of the display rip statistics interface command output

Item	Description
Statistical information	Packet type
Last min	Statistics within the last 1 minute
Last 5 min	Statistics within the last 5 minutes
Total	Total number of packets
Periodic updates sent	Number of periodic Update packets that are sent on the interface
Triggered updates sent	Number of triggered Update packets that are sent on the interface

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Response packets sent	Number of RIP Response packets that are sent on the interface
Response packets received	Number of RIP Response packets that are received on the interface
Response packets ignored	Number of RIP Response packets that are ignored on the interface
Request packets sent	Number of RIP Request packets that are sent on the interface
Request packets received	Number of RIP Request packets that are received on the interface
Request packets ignored	Number of RIP Request packets that are ignored on the interface
Bad packets received	Number of received packets that cannot be parsed correctly
Routes received	Number of received routes
Routes sent	Number of sent routes
Bad routes received	Number of received routes that cannot be parsed correctly
Packet authentication failed	Number of packets that fail to pass authentication
Packet send failed	Number of RIP packets that fail to be sent

9.2.18 filter-policy export (RIP)

Function

The **filter-policy export** command configures egress filtering policy for RIP routes.

The **undo filter-policy export** command deletes the filtering policy.

By default, no filtering policy is configured.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* }
export [*protocol* [*process-id*] | *interface-type interface-number*]

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name*]
export [*protocol* [*process-id*] | *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the basic ACL that is used to filter the destination addresses of routes.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the ACL filtering route destination addresses.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that is used to filter the destination addresses of routes.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol process-id	Specifies the name of the routing protocol that exports the routes and the protocol process ID. The imported route type can be **static**, **direct**, **rip**, **ospf**, **bgp**, **unr** and **isis**. The process ID must be specified when routes are imported from **isis**, **rip** or **ospf**.	The value is an integer that ranges from 1 to 65535.
interface-type interface-number	Specifies type and number of the interface based on which routes are filtered.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Only filtered routes can be added to routing tables and advertised in Update packets.

When you remove an interface-based filtering policy, you must specify *interface-type interface-number* in the **undo filter-policy export** command. The policy on only one interface can be deleted each time.

This command runs in the RIP view. If the filtering policy is based on interfaces or protocols, each interface or protocol can be configured with only one filtering

policy. If the interface or protocol is not specified, a global filtering rule is configured. Only one global filtering rule can be configured each time. If you run the command again when a global rule exists, the new policy overwrites the old one.

Example

Filter the imported static routes based on the IP prefix list named abc. Then, only the routes that match the filtering policy are added into the RIP routing table and then sent through RIP Update packets.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] filter-policy ip-prefix abc export static
```

Filter the routes imported from IS-IS process 1 based on ACL 2002. Only the routes that match the filtering policy are added into the RIP routing table and then sent through RIP Update packets.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] filter-policy 2002 export isis 1
```

Related Topics

9.2.22 import-route (RIP)

9.2.19 filter-policy import (RIP)

Function

The **filter-policy import** command filters the received RIP routes.

The **undo filter-policy import** command cancels route filtering.

By default, no filtering policy is configured.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import** [*interface-type interface-number*]

filter-policy gateway *ip-prefix-name* **import**

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*]] **import** [*interface-type interface-number*]

undo filter-policy [**gateway** *ip-prefix-name*] **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the basic ACL that is used to filter the destination addresses of routes.	The value is an integer ranging from 2000 to 2999.

Parameter	Description	Value
acl-name *acl-name*	Specifies the ACL filtering route destination addresses.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
interface-type interface-number	Indicates the type and the number of the interface based on which routes are filtered.	-
ip-prefix	Filters routes by using the IP prefix list.	-
ip-prefix-name	Specifies the address prefix list used to filter route destination addresses.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
gateway	Filters routes based on the gateway.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

The **filter-policy import** command filters received RIP routes, including:

- Filtering a specified route in the packet
- Not monitoring the Update packets from the device

To cancel route filtering, run the **undo filter-policy import** command. When you remove an interface-based filtering policy, you must specify *interface-type interface-number*. The policy on only one interface can be deleted each time.

This command runs in the RIP view. If the filtering policy is based on interfaces, each interface can be configured with only one filtering policy. If the interface is not specified, a global filtering policy is configured. Only one global filtering policy can be configured. If you run the command again when a global policy exists, the new policy overwrites the old one.

Example

Filter the RIP Update packets that are received from all the interfaces according to the IP prefix list named **abc**.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] filter-policy ip-prefix abc import
```

9.2.20 graceful-restart (RIP)

Function

The **graceful-restart** command enables RIP GR on the restarter.

The **undo graceful-restart** command disables RIP GR on the restarter.

By default, RIP GR is disabled.

Format

graceful-restart [**period** *period* | **wait-time** *time* | **planned-only** *time*] *

undo graceful-restart

Parameters

Parameter	Description	Value
period *period*	Specifies the period of GR.	It is an integer ranging from 30 to 3600, in seconds. The default value is 180 seconds.
wait-time *time*	Specifies the period of GR performed between the restarter and the neighbors that do not support GR. The value of **wait-time** *time* cannot be greater than the value of **period** *period*.	It is an integer ranging from 1 to 3600, in seconds. The default value is 45 seconds.
planned-only *time*	Specifies the period of GR performed between the restarter and the neighbors that support GR.	It is an integer ranging from 5 to 3600, in seconds. The default value is 60 seconds.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Planned GR indicates the master/slave switchover triggered through the command. Unplanned GR indicates the master/slave switchover triggered because of a fault.

When most routers on a network do not support RIP GR, it is recommended to set **wait-time** *time* to a larger value. This ensures that the restarter has enough time to learn correct routes.

If the restart router completes GR before the period specified by **period** *period* expires, the restart router automatically exits from GR. If the restart router does not complete GR after the period specified by **period** *period* expires, the restart router is forced to exit from GR.

If the period of GR performed between the restarter and the neighbors that do not support GR depends on **wait-time**, the restarter does not exit from GR regardless of whether GR is finished within **wait-time**. After **wait-time** expires, however, the restarter is forced to exit from GR.

Precautions

If the RIP-2 authentication mode and authentication parameters have been configured on an interface using the **rip authentication-mode** command, you also need to run the **rip replay-protect** command on the interface to enable the replay-protect function to ensure that packets can be received and sent normally during the GR period.

Example

Enable RIP GR and set the GR period to 200s.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] graceful-restart period 200
```

9.2.21 host-route

Function

The **host-route** command adds host routes with 32 bits into the routing table.

The **undo host-route** command disables host routes with 32 bits from being added into the routing table.

By default, host routes can be added into the routing table.

Format

host-route

undo host-route

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

This command is valid only in RIP-1.

Example

Add host routes into the routing table.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] host-route
```

Related Topics

9.2.15 display rip route

9.2.22 import-route (RIP)

Function

The **import-route** command configures RIP to import routes from other routing protocols.

The **undo import-route** command disables RIP from importing routes from other routing protocols.

By default, RIP does not import routes from other routing protocols.

Format

import-route bgp [**permit-ibgp**] [**cost** { *cost* | **transparent** } | **route-policy** *route-policy-name*] *

import-route { { **static** | **direct** | **unr** } | { { **rip** | **ospf** | **isis** } [*process-id*] } } [**cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route { { **static** | **direct** | **bgp** | **unr** } | { { **rip** | **ospf** | **isis** } [*process-id*] } }

Parameters

Parameter	Description	Value
bgp | **static** | **direct** | **rip** | **ospf** | **isis** | **unr**	Specifies the routing protocol from which RIP imports routes.	-
permit-ibgp	Imports routes from IBGP to RIP.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
process-id	Specifies a process ID. The process ID can be specified when you import routes from RIP, OSPF, or IS-IS to RIP.	The value is an integer that ranges from 1 to 65535.
cost *cost*	Specifies the metric for imported routes.	The value is an integer that ranges from 0 to 15.
cost transparent	This parameter is valid only when RIP imports routes from BGP. The metric of the imported routes is the MED of the BGP routes.	-
route-policy *route-policy-name*	Specifies the routing policy for importing routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

After you run the **import-route** command to set a routing policy, RIP can import only the specified routes and sets the route attributes.

To import routes from RIP, OSPF, or IS-IS, you can specify the process ID. If the process ID is specified, RIP imports routes only from the specified process. If no process ID is specified, RIP imports routes from all processes. When a static or direct route is imported, the process ID cannot be specified.

You can run one of the following commands to set the metric of the imported routes. The following commands are listed in the descending order of priorities.

- Run the **apply cost** command to set route metric.
- Run the **import-route** (RIP) command to set the metric for imported routes.
- Run the **default-cost (RIP)** command to set the default metric for routes.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- RIP defines a 16-bit tag, while other routing protocols define 32-bit tags. If the routes of other protocols are imported to RIP and the tag is used in the routing policy, the tag value cannot exceed 65535. If the tag value exceeds 65535, the routing policy becomes invalid or the matching result is incorrect.
- After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the RIP routing table. Therefore, use this command with caution.
- The **permit-ibgp** parameter cannot be set for the RIP VPN instance.
- Importing IBGP routes to RIP may cause routing loops.

Example

Import routes from IS-IS process 7 and set the route metric to 7.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] import-route isis 7 cost 7
```

Import IBGP routes, which are filtered by policy abc, to RIP process 1 and set the metric to 5.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] import-route bgp permit-ibgp cost 5 route-policy abc
```

Related Topics

9.9.7 apply cost
9.2.4 default-cost (RIP)
9.2.18 filter-policy export (RIP)

9.2.23 maximum load-balancing (RIP)

Function

The **maximum load-balancing** command configures the maximum number of equal-cost routes for load balancing.

The **undo maximum load-balancing** command restores the default setting.

By default, the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204 support a maximum of four equal-cost routes, and the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series support a maximum of eight equal-cost routes, AR2240 (using SRU200, SRU200E or SRU400), and AR3200 (using SRU200, SRU200E or SRU400) series support a maximum of sixteen equal-cost routes.

Format

maximum load-balancing *number*

undo maximum load-balancing

Parameters

Parameter	Description	Value
number	Specifies the number of equal-cost routes.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

If a network has multiple redundant links, the maximum number of equal-cost routes can be configured to implement load balancing. With load balancing, network resources are fully utilized, situations where some links are overloaded while others are idle can be avoided, and delay in packet transmissions is shortened.

Example

Set the maximum number of equal-cost routes to 4.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] maximum load-balancing 4
```

Related Topics

9.2.15 display rip route

9.2.24 network (RIP)

Function

The **network** command enables RIP for the interface on the specified network segment.

The **undo network** command disables RIP for the interface on the specified network segment.

By default, RIP is disabled for the interface on the specified network segment.

Format

network *network-address*

undo network *network-address*

Parameters

Parameter	Description	Value
network-address	Specifies the network address on which RIP is enabled. It must be the address of the natural network segment.	The value is in dotted decimal notation.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

An interface can be associated with only one RIP process.

If one sub-interface's network segment of an interface with multiple sub-interface IP addresses has been associated with an RIP process, the interface cannot be associated with any other RIP processes.

By running the **network 0.0.0.0** command, you can enable RIP on all interfaces. Dynamic allocation of IP addresses for PPPOE interface causes change of major network. To support dynamic IP address change and add interface to RIP, RIP should have default network configuration to allow to run RIP on any IP interface.

Example

Enable RIP routes for the interface on the specified network segment.

```
<Huawei> system-view
[Huawei] rip
[Huawei-rip-1] network 10.0.0.0
```

Related Topics

9.2.29 rip

9.2.25 peer (RIP)

Function

The **peer** command specifies the IP addresses of the RIP neighbors. After this command is configured, Update packets are sent to the peer in unicast instead of multicast or broadcast mode.

The **undo peer** command deletes the specified neighbor IP address.

By default, no RIP neighbor address is specified.

Format

peer *ip-address*

undo peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor.	The value is in dotted decimal notation.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Generally, it is not recommended to use the **peer** command because an interface may receive the same packets both in multicast (or broadcast) and unicast mode. It is recommended that you change the mode of the interface to the silent mode when configuring the **peer** command.

Example

Specify the IP address of the neighbor to 10.0.0.1.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] peer 10.0.0.1
```

Related Topics

9.2.13 display rip neighbor

 Copyright © Huawei Technologies Co., Ltd.

9.2.26 preference (RIP)

Function

The **preference** command sets the preference for RIP routes.

The **undo preference** command restores the default preference of RIP routes.

The default preference for RIP routes is 100.

Format

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Parameters

Parameter	Description	Value
preference	Specifies the preference for routes.	The value is an integer ranging from 1 to 255. By default, it is 100.
route-policy *route-policy-name*	Specifies the routing policy that sets preference for the routes meeting conditions.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

A small value indicates a high preference. To enable RIP routes to have a higher preference than the routes learned by other IGP protocols, you need to configure a smaller preference value for the RIP routes. The preference determines the algorithm through which the optimal route is obtained among the routes in the IP routing table.

Example

Set the preference of RIP routes to 120.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] preference 120
```

Set the preference of RIP routes that match the routing policy named **rt-policy1** to 120.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] preference 120 route-policy rt-policy1
```

9.2.27 reset rip configuration

Function

The **reset rip configuration** command resets system parameters for a specified RIP process. When a RIP process starts, all the parameters of the process retain the default values.

Format

reset rip *process-id* **configuration**

Parameters

Parameter	Description	Value
process-id	Specifies a RIP process ID.	The value is an integer that ranges from 1 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Restarting RIP processes may interrupt services. Exercise caution when you run this command.

After the command is executed, RIP neighbor relationships are set up again and learned routes are deleted.

Example

Reset the parameters of RIP process 100.

```
<Huawei> reset rip 100 configuration
```

 Copyright © Huawei Technologies Co., Ltd.

9.2.28 reset rip statistics

Function

The **reset rip statistics** command resets the counter that is maintained by a particular RIP process. This command allows you to repeatedly record statistics during debugging.

Format

reset rip *process-id* **statistics** [**interface** { **all** | *interface-type interface-number* [**neighbor** *neighbor-ip-address*] }]

Parameters

Parameter	Description	Value
process-id	Specifies a RIP process ID.	The value is an integer ranging from 1 to 65535.
all	Clears statistics of all RIP processes.	-
interface *interface-type interface-number*	Clears statistics on the interface with specified number and type.	-
neighbor *neighbor-ip-address*	Clears statistics on the RIP process between the local RIP interface and the specified neighbor.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Statistics cannot be restored after being cleared. Exercise caution when you run this command.

Example

Clear statistics in RIP process 100.

```
<Huawei> reset rip 100 statistics
```

9.2.29 rip

Function

The **rip** command starts the specified RIP in the system view.

The **undo rip** command stops the specified RIP process.

By default, no RIP process is started.

Format

rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer that ranges from 1 to 65535. The default value is 1.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If no VPN instance is specified, a RIP process is run globally or in the default VPN instance. Before configuring each global RIP parameter, you need to start RIP. This restriction is not applicable when you configure interface-related parameters.

Example

Start RIP process 1.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1]
```

Start RIP process 100 in the VPN instance named **abc**.

```
<Huawei> system-view
[Huawei] rip 100 vpn-instance abc
[Huawei-rip-100]
```

 Copyright © Huawei Technologies Co., Ltd.

9.2.30 rip authentication-mode

Function

The **rip authentication-mode** command sets the RIP-2 authentication mode and authentication parameters. Only one authentication password is used for each authentication. If multiple authentication passwords are configured, the latest one takes effect.

The **undo rip authentication-mode** command cancels authentication.

By default, no authentication is configured.

Format

rip authentication-mode simple { **plain** *plain-text* | [**cipher**] *password-key* }

rip authentication-mode keychain *keychain-name*

rip authentication-mode md5 usual { **plain** *plain-text* | [**cipher**] *password-key* }

rip authentication-mode md5 nonstandard { **keychain** *keychain-name* | { **plain** *plain-text* | [**cipher**] *password-key* } *key-id* }

rip authentication-mode hmac-sha256 { **plain** *plain-text* | [**cipher**] *password-key* } *key-id*

undo rip authentication-mode

Parameters

Parameter	Description	Value
simple	Specifies simple authentication. **NOTE** Simple authentication mode carries potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
md5	Specifies MD5 authentication. **NOTE** MD5 cipher text authentication carries potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
usual	Indicates that MD5 cipher text authentication packets use the universal format (private standard).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
nonstandard	Indicates that MD5 cipher text authentication packets use non-standard packet format (IETF standard).	-
plain	Indicates that only plain text can be entered and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
plain-text	Specifies the authentication password that is displayed in plain text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. When the authentication mode is **simple** or **md5 usual**, the password consists of 1 to 16 characters. When the authentication mode is **md5 nonstandard** or **hmac-sha256**, the password consists of 1 to 255 characters.
cipher	Indicates that either plain text or cipher text can be entered and cipher text is displayed when the configuration file is viewed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password-key	Specifies the authentication password that is displayed in cipher text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. ● When the authentication mode is **simple** or **md5 usual**, the password is in plain text (1 to 16 characters) or in cipher text (48, 24 or 32 characters). If the source version supports a ciphertext password which is a string of 24 or 32 characters, the target version also supports this type of password. ● When the authentication mode is **md5 nonstandard** or **hmac-sha256**, the password is in plain text (1 to 255 characters) or in cipher text (20 to 392 characters).
keychain *keychain-name*	Specifies keychain authentication.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
key-id	Specifies the key in MD5 authentication.	The value is an integer that ranges from 1 to 255.
hmac-sha256	Indicates Keyed-Hash Message Authentication Code (HMAC) for Secure Hash Algorithm 256 (SHA256).	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Keychain authentication improves UDP connection security. Keychain authentication must be configured on both ends of a link. Encryption algorithms and passwords configured on both ends must be the same; otherwise, the UDP connection cannot be set up and RIP messages cannot be transmitted.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set HMAC-SHA256 authentication on GE1/0/0, with the authentication password **admin@huawei** and key-id **255**.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip authentication-mode hmac-sha256 cipher admin@huawei 255
```

9.2.31 rip bfd

Function

The **rip bfd** command sets BFD session parameters on the specified interface.

The **undo rip bfd** command restores BFD session parameters set on the specified interface.

By default, the minimum intervals for receiving and sending BFD packets are 1000 ms and the detection time multiplier is 3.

Format

rip bfd { **min-rx-interval** *min-receive-value* | **min-tx-interval** *min-transmit-value* | **detect-multiplier** *detect-multiplier-value* } *

undo rip bfd { **min-rx-interval** [*min-receive-value*] | **min-tx-interval** [*min-transmit-value*] | **detect-multiplier** [*detect-multiplier-value*] } *

Parameters

Parameter	Description	Value
min-rx-interval *min-receive-value*	Specifies the minimum interval at which BFD packets are received from the remote device.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-tx-interval *min-transmit-value*	Specifies the minimum interval at which BFD packets are sent to the remote device.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
detect-multiplier *detect-multiplier-value*	Specifies the local detection multiplier.	The value is an integer ranging from 3 to 50. The default value is 3.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The *min-receive-value* value is obtained after the local **min-rx-interval** value and a neighbor's **min-tx-interval** value are negotiated. For detailed negotiation policies, see **9.2.2 bfd all-interfaces (RIP)**. If the router does not receive BFD packets from the neighbor at the interval of *min-receive-value* x *detect-multiplier-value*, the neighbor will go Down.

Prerequisites

Enable BFD globally and run the **rip bfd enable** command before establishing a BFD session.

Precautions

BFD session parameters configured in a RIP process take effect only after BFD is enabled on the interface.

The BFD priority configured on an interface is higher than the BFD priority configured in a RIP process. If BFD session parameters are configured on an interface, establish a BFD session based on the configured parameters.

Example

Enable BFD on GE1/0/0 and set the minimum sending interval to 600 ms and local detection multiplier to 4.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip bfd enable
[Huawei-GigabitEthernet1/0/0] rip bfd min-tx-interval 600 detect-multiplier 4
```

Related Topics

9.2.2 bfd all-interfaces (RIP)

9.2.33 rip bfd enable

9.2.32 rip bfd block

Function

The **rip bfd block** command blocks BFD on a specified interface.

The **undo rip bfd block** command disables the blocking function.

By default, the blocking function is disabled.

Format

rip bfd block

undo rip bfd block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can be used to block the specified interface from enabling BFD on some links where no BFD session is needed.

Precautions

The **rip bfd block** and **rip bfd enable** commands are mutually exclusive. If both of them are configured, only the later configured one takes effect.

Example

Block BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip bfd block
```

Related Topics

9.2.31 rip bfd

9.2.33 rip bfd enable

9.2.33 rip bfd enable

Function

The **rip bfd enable** command enables BFD on the specified interface to establish a BFD session with default parameters.

The **undo rip bfd enable** command disables BFD on the specified interface.

By default, BFD is disabled on a RIP interface.

Format

rip bfd enable

undo rip bfd enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If BFD is not enabled globally, you can set BFD parameters on the specified interface but you cannot establish a BFD session on this interface.

The **rip bfd block** and **rip bfd enable** commands are mutually exclusive. If both of them are configured, only the later configured one takes effect.

Example

Enable BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip bfd enable
```

Disable BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo rip bfd enable
```

Related Topics

9.2.2 bfd all-interfaces (RIP)

9.2.32 rip bfd block

9.2.34 rip bfd static

Function

The **rip bfd static** command enables static BFD on a specified RIP interface.

The **undo rip bfd static** command disables static BFD on a specified RIP interface.

By default, static BFD is disabled on a RIP interface.

Format

rip bfd static

undo rip bfd static

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network deployed with high-speed data services, if a fault occurs on a link, a large amount of data is lost because it takes too long time for RIP to detect the fault. Deploying BFD for RIP to accelerate fault detection is necessary.

The **rip bfd static** command is used to enable BFD for RIP on a specified link to rapidly detect the fault on the link.

In addition, because many devices do not support BFD on the live network, this command can be also used to implement BFD between a BFD-capable device and a BFD-incapable device.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

If **rip bfd static**, **rip bfd enable**, and **rip bfd block** are simultaneously configured, the latest configuration overrides the previous ones.

Example

Enable static BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip bfd static
```

Related Topics

9.2.32 rip bfd block

9.2.33 rip bfd enable

18.5.2 bfd

9.2.35 rip input

Function

The **rip input** command enables the specified interface to receive RIP packets.

The **undo rip input** command disables the specified interface from receiving RIP packets.

By default, interfaces can receive RIP packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

rip input

undo rip input

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The priority of **silent-interface** is higher than the priority of **rip input** or **rip output** configured in the interface view. By default, an interface does not work in the silent state.

Example

Enable the specified interface GE1/0/0 to receive RIP packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip input
```

Related Topics

9.2.39 rip output

9.2.47 silent-interface (RIP)

9.2.36 rip metricin

Function

The **rip metricin** command sets the metric that is added to the route when an interface receives a RIP packet.

The **undo rip metricin** command restores the additional metric to the default value.

By default, there is no metric added to the route when an interface receives a RIP packet.

Format

rip metricin { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } *value1* }

undo rip metricin

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
value	Specifies the metric that is added to the received route.	The value is an integer ranging from 0 to 15. By default, it is 0.
acl-number	Specifies the basic ACL number.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the ACL name.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
value1	Specifies the metric that is added to the route that passes the filtering of the ACL or IP prefix list.	The value is an integer ranging from 1 to 15.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When an interface receives a route, RIP adds the additional metric of the interface to the route, and then installs the route into the routing table. Therefore, increasing the metric of an interface also increases the metric of the RIP route received by the interface.

Adjust RIP route selection by increasing the metrics of received routes.

Example

Set the additional metric to 12 when GE1/0/0 receives RIP routes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricin 12
```

Set the additional metric to 12 using acl-name.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricin acl-name abcd 12
```

Set the additional metric to 12 using ip-prefix.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricin ip-prefix ip1 12
```

9.2.37 rip metricout

Function

The **rip metricout** command sets the metric that is added to the route when an interface sends a RIP packet.

The **undo rip metricout** command restores the additional metric to the default value.

By default, the metric that is added to the route when an interface sends a RIP packet is 1.

Format

rip metricout { *value* | { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } *value1* }

undo rip metricout

Parameters

Parameter	Description	Value
value	Specifies the metric that is added to the sent route.	The value is an integer ranging from 1 to 15. By default, it is 1.
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list. The name must be exclusive.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
value1	Specifies the metric that is added to the route that passes the filtering of the ACL or IP prefix list.	The value is an integer ranging from 2 to 15.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a RIP route is advertised, the additional metric is added to the route. Therefore, increasing the metric of an interface also increases the metric of the RIP route sent on the interface. However, the metric of the route in the routing table remains unchanged.

You can specify the metric to be added to the RIP route that passes the filtering of the ACL or IP prefix list by specifying *value1*. If a RIP route does not pass the filtering, its metric is increased by 1.

For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Set the metric that is added when the interface sends RIP routes to 12.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricout 12
```

Increase the metric of a RIP route that passes the filtering of ACL 2050 by 12.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricout 2050 12
```

Increase the metric of a RIP route that passes the filtering of the IP prefix list named **p1** by 12.

```
<Huawei> system-view
[Huawei] ip ip-prefix p1 permit 10.10.10.1 24
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip metricout ip-prefix p1 12
```

9.2.38 rip mib-binding

Function

The **rip mib-binding** command sets the binding between the Management Information Base (MIB) and RIP process ID, and specifies the ID of the RIP process that receives SNMP requests.

The **undo rip mib-binding** command cancels the binding.

By default, there is no binding between the Management Information Base and RIP process ID.

 Copyright © Huawei Technologies Co., Ltd.

Format

rip mib-binding *process-id*

undo rip mib-binding

Parameters

Parameter	Description	Value
process-id	Specifies the ID of a RIP process.	The value is an integer ranging from 1 to 65535. The default value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All SNMP requests are sent to the bound RIP process.

Prerequisites

A RIP process has been created using the **rip** command.

Example

Configure RIP process 100 to receive SNMP requests.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] quit
[Huawei] rip mib-binding 100
```

9.2.39 rip output

Function

The **rip output** command enables an interface to send RIP packets.

The **undo rip output** command disables an interface from sending RIP packets.

By default, an interface can send RIP packets.

Format

rip output

undo rip output

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The priority of **silent-interface** is higher than the priority of **rip input** or **rip output** that is configured in the interface view. By default, an interface does not work in the silent state.

Example

Enable the interface GE1/0/0 to send RIP packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip output
```

Related Topics

9.2.35 rip input

9.2.47 silent-interface (RIP)

9.2.40 rip pkt-transmit

Function

The **rip pkt-transmit** command sets the interval for sending Update packets and the number of packets sent each time on the specified interface.

The **undo rip pkt-transmit** command restores the default values on an interface.

By default, the interval for sending RIP Update packets is 200 ms and 50 packets are sent each time.

Format

rip pkt-transmit { **interval** *interval* | **number** *pkt-count* } *

undo rip pkt-transmit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for sending Update packets.	The value is an integer ranging from 50 to 500, in milliseconds. The default value is 200.
number *pkt-count*	Specifies the number of packets sent each time.	The value is an integer and ranges from 25 to 100. The default value is 50.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **rip pkt-transmit** command can be used on an interface to control the interval for sending Update packets and the number of sent packets. This improves RIP performance.

Example

Set the interval for sending packets on GE1/0/0 to 100 milliseconds and the number of the packets sent each time to 50.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip pkt-transmit interval 100 number 50
```

9.2.41 rip poison-reverse

Function

The **rip poison-reverse** command enables poison reverse.

The **undo rip poison-reverse** command disables poison reverse.

By default, poison reverse is disabled.

Format

rip poison-reverse

undo rip poison-reverse

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After poison reverse is enabled, RIP sets the cost of the routes learned from a specified interface to 16 (indicating unreachable), and then sends the routes to neighbors through the same interface.

When both split horizon and poison reverse are configured, only poison reverse takes effect.

Example

Enable poison reverse.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip poison-reverse
```

Related Topics

9.2.43 rip split-horizon

9.2.42 rip replay-protect

Function

The **rip replay-protect** command enables the replay-protect function.

The **undo rip replay-protect** command disables the replay-protect function.

By default, the replay-protect function is disabled.

Format

rip replay-protect [*window-range*]

undo rip replay-protect

Parameters

Parameter	Description	Value
window-range	Specifies the size of the connection-oriented transmission buffer.	It is an integer ranging from 50 to 50000. The default value is 50.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If the Identification field in the last RIP packet sent before a RIP interface goes Down is X, after the interface goes Up, the Identification field in the RIP packet sent by this interface becomes 0. If the remote end does not receive the RIP packet with the Identification field being 0, subsequent RIP packets will be discarded until the remote end receives the RIP packet with the Identification field being X+1. As a result, RIP routing information of both ends is inconsistent. To solve this problem, you need to configure the **rip replay-protect** command so that RIP can obtain the Identification field in the RIP packet sent before the RIP packet goes Down and increases the Identification field of the subsequently sent RIP packet by one.

Before configuring the **rip replay-protect** command, you need to configure the **rip authentication-mode** command in the RIP interface view to configure the authentication mode and authentication parameters of RIP-2.

NOTE

- For details of the Identification field in an IP packet, refer to *Configuration Guide - IP Services*.
- If you configure the **rip replay-protect** command in the same view for multiple times, only the last configuration takes effect.

Example

Enable the replay-protect function on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip replay-protect
```

Related Topics

9.2.30 rip authentication-mode

9.2.43 rip split-horizon

Function

The **rip split-horizon** command enables split horizon.

The **undo rip split-horizon** command disables split horizon.

By default, split horizon is enabled.

Format

rip split-horizon

undo rip split-horizon

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If a route is advertised through the interface from which the route is learned, the route is blocked by split horizon. Split horizon is used to avoid routing loops between neighboring devices.

Generally, it is not recommended that you disable split horizon.

If split horizon is enabled on the interface that is configured with secondary IP addresses, RIP Update packets may not be sent by each secondary address. An Update packet does not regard every network as the source unless split horizon is disabled.

If an interface is connected to a Non Broadcast Multiple Access (NBMA) network, split horizon on the interface is disabled by default.

If both poison reverse and split horizon are configured, simple split horizon (the route is suppressed by the interface through which the route is learned) is substituted by poison reverse. Here, simple split horizon means that the route is suppressed when it is advertised through the interface from which it is learned.

Example

Enable split horizon.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip split-horizon
```

Related Topics

9.2.41 rip poison-reverse

9.2.44 rip summary-address

Function

The **rip summary-address** command configures a RIP router to advertise a local summarized IP address.

The **undo rip summary-address** command disables a RIP router from advertising a local summarized IP address.

By default, a RIP router does not advertise local summarized IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

Format

rip summary-address *ip-address mask* [**avoid-feedback**]

undo rip summary-address *ip-address mask*

Parameters

Parameter	Description	Value
ip-address	Specifies the network IP address to be summarized.	The value is in dotted decimal notation.
mask	Specifies the network mask.	The value is in dotted decimal notation.
avoid-feedback	Specifies that learning the same summarized route from an interface is not allowed.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After the keyword **avoid-feedback** is specified, an interface no longer learns the summarized route with the same IP address as the advertised summarized IP address. This avoids routing loops.

Example

Configure the router to advertise a local summarized IP address.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip summary-address 10.0.0.0 255.0.0.0
```

Related Topics

9.2.48 summary (RIP)

9.2.45 rip valid-ttl-hops

Function

The **rip valid-ttl-hops** command enables the RIP GTSM functions and sets the TTL value to be detected.

The **undo rip valid-ttl-hops** command cancels the function.

By default, the RIP GTSM functions are disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

rip valid-ttl-hops *valid-ttl-hops-value* [**vpn-instance** *vpn-instance-name*]

undo rip valid-ttl-hops [*valid-ttl-hops-value*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
valid-ttl-hops-value	Specifies the number of TTL hops to be detected. The valid TTL range of the detected packets is [255 -*valid-ttl-hops-value* + 1, 255].	The value is an integer ranging from 1 to 255.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance. If this parameter is used, you need only to specify the TTL value to be detected by the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a network demanding higher security, you can enable GTSM to improve the security of the RIP network. GTSM defends against attacks by checking the TTL value. If an attacker simulates RIP unicast packets and keeps sending them to a router, an interface board on the router receives the packets and directly sends them to the main control board for RIP processing, without checking the validity of the packets. In this case, the router is busy processing these packets, causing high usage of the CPU. GTSM protects the routers and enhances the system security by checking whether the TTL value in the IP packet header is in a pre-defined range.

The **rip valid-ttl-hops** command is used to enable RIP GTSM.

Precautions

GTSM configurations must be symmetrical. That is, GTSM must be enabled on devices at both ends.

 Copyright © Huawei Technologies Co., Ltd.

If GTSM is enabled on a device, after the device receives a RIP packet, it checks whether the TTL value in the packet is in a pre-defined range. If the TTL value is beyond the pre-defined range, the device considers the packet as an attack packet and discards it.

Example

Enable the RIP GTSM functions, and configure the maximum number of TTL hops to 5 for the packets that a router is allowed to receive.

```
<Huawei> system-view
[Huawei] rip valid-ttl-hops 5
```

9.2.46 rip version

Function

The **rip version** command sets the RIP version of an interface.

The **undo rip version** command restores the default setting.

By default, an interface sends only RIP-1 packets, but it can receive both RIP-1 and RIP-2 packets.

Format

rip version { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

Parameters

Parameter	Description	Value
1	Indicates RIP-1 packets.	-
2	Indicates RIP-2 packets.	-
broadcast	Indicates that RIP-2 packets are sent in broadcast mode.	-
multicast	Indicates that RIP-2 packets are sent in multicast mode. **NOTE** By default, RIP-2 packets are sent in multicast mode.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The versions of the request packets and response packets vary with the configured RIP version.

- If the version of RIP is not set, a device sends RIP-1 packets in broadcast mode and receives the RIP-1 and RIP-2 packets that are sent in broadcast mode.
- If the RIP version is set to RIP-1, a device sends only RIP-1 packets in broadcast mode and receives the RIP-1 packets that are sent in broadcast mode.
- If the RIP version is set to RIP-2, a device sends only RIP-2 packets in multicast mode and receives RIP-2 packets that are sent in multicast or broadcast mode.
- If the RIP version is set to multicast RIP-2, a device sends RIP-2 packets in multicast mode and receives RIP-2 packets that are sent in multicast mode.
- If the RIP version is set to broadcast RIP-2, a device sends RIP-2 packets in broadcast mode and receives RIP-1 and RIP-2 packets.

Precautions

You can also set a RIP version in a RIP process, but the RIP version that is set on an interface has a higher priority.

Example

Send RIP-2 packets in broadcast mode.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] rip version 2 broadcast
```

9.2.47 silent-interface (RIP)

Function

The **silent-interface** command controls an interface only to receive packets to update its routing table and prevent it from sending RIP packets.

The **undo silent-interface** command enables an RIP interface to send Update packets.

The **silent-interface disable** command enables an RIP interface to send Update packets.

The **undo silent-interface disable** command controls an interface only to receive packets to update its routing table and prevent it from sending RIP packets.

By default, silent interface not enabled.

Format

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

silent-interface disable *interface-type interface-number*

undo silent-interface disable *interface-type interface-number*

Parameters

Parameter	Description	Value
all	Indicates that all interfaces are suppressed.	-
interface-type interface-number	Specifies the type and the number of the interface.	-
disable	Disables the suppression of the RIP interface so that the interface can send Update packets.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a router running RIP is connected to a network running other routing protocols, you can run the **silent-interface** command on the interface that connects the router to the network to prevent the interface from sending useless packets to the network.

The **silent-interface** command is used together with the **peer (RIP)** command to advertise routes to the specified equipment.

Configuration Impact

If an interface is suppressed, the direct routes of the network segment where the interface resides can still be advertised to other interfaces.

Precautions

When the **silent-interface** command is used to suppress the specified interface, the priority of the **silent-interface** command is higher than the priority of the **rip input** and **rip output** command that is configured in the interface view.

NOTE

After you configure all interfaces as silent interfaces, you can run the **silent-interface disable** *interface-type interface-number* command to activate a specified silent interface.

Example

Configure all the interfaces as silent interfaces.

```
Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] silent-interface all
```

Configure the RIP interface GE1/0/0 as a silent interface and enable it to send routes to the neighbor with the IP address of 10.1.1.1/24.

```
Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] silent-interface gigabitethernet 1/0/0
[Huawei-rip-100] peer 10.1.1.1
```

Configure all interfaces as silent interfaces, and then activate the interface GE1/0/0.

```
Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] silent-interface disable gigabitethernet 1/0/0
```

Related Topics

9.2.25 peer (RIP)

9.2.35 rip input

9.2.39 rip output

9.2.48 summary (RIP)

Function

The **summary** command enables RIP classful summarization. The summarized routes are advertised using natural masks.

The **undo summary** command disables classful summarization so that routing between subnets can be performed. The subnet information is then advertised. Route summarization reduces the routing table size.

By default, classful summarization is enabled for RIP-2.

Format

summary [**always**]

undo summary

Parameters

Parameter	Description	Value
always	Enables classful summarization no matter whether split horizon is configured.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

RIP-1 does not support classful summarization. When using RIP-2, you can use the **undo summary** command to disable classful summarization.

RIP-2 route summarization improves scalability and efficiency on large networks. IP address summarization means that there is no sub-routing entry in the routing table. That is, there is no routing entry composed of single IP address. In addition to reducing the routing table size, route summarization enables the router to handle more routes.

When classful summarization is enabled, the router summarizes subnet addresses to the natural network segment border while advertising routes to the natural network segment border. When split horizon or poison reverse is enabled, route summarization will be invalid if the **always** parameter is not specified. When summarized routes are sent outside the natural network segment, split horizon or poison reverse must be disabled.

NOTE

- By default, classful summarization is enabled for RIP-2. If split horizon or poison reverse has been configured, classful summarization is invalid. When summarized routes are sent to the network border, split horizon and poison reverse must be disabled.
- The **summary always** command can enable classful summarization no matter whether split horizon or poison reverse is enabled.
- The summarization preference on interfaces is higher than the summarization preference in RIP processes. That is, the preference of **rip summary-address** is higher than the preference of **summary**. When summarization is configured on both interface and RIP process, the summarized route is advertised only when a few specific routes are beyond the summarization range configured on the interface.

Example

Enable RIP-2 classful summarization.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] version 2
[Huawei-rip-1] summary
```

Enable RIP-2 classful summarization when split horizon is enabled.

```
<Huawei> system-view
[Huawei] rip 1
[Huawei-rip-1] summary always
```

Related Topics

9.2.41 rip poison-reverse

9.2.43 rip split-horizon

9.2.49 snmp-agent trap enable feature-name rip

Function

The **snmp-agent trap enable feature-name rip** command enables the trap function for the RIP module.

The **undo snmp-agent trap enable feature-name rip** command disables the trap function for the RIP module.

By default, rip trap functions are disabled.

Format

snmp-agent trap enable feature-name rip [**trap-name** { **hwrip2dboverflow** | **hwrip2dboverflowresume** }]

undo snmp-agent trap enable feature-name rip [**trap-name** { **hwrip2dboverflow** | **hwrip2dboverflowresume** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for a specified type of RIP events.	-
hwrip2dboverflow	Enables the trap function upon RIP database overflow.	By default, the trap function is disabled.
hwrip2dboverflowresume	Enables the trap function upon RIP database overflow recovery.	By default, the trap function is disabled.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Guidelines

The **snmp-agent trap enable feature-name rip** command enables the trap function to monitor the tunnel group status. To enable the trap function for one or more specific events on the RIP module, set the **trap-name** parameter in this command.

Follow-up Procedure

To view the traps related to the RIP module, run the **display snmp-agent trap feature-name rip all** command.

Example

Enable the trap function upon RIP database overflow.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name rip trap-name hwrip2dboverflow
```

Related Topics

9.2.16 display snmp-agent trap feature-name rip all

 Copyright © Huawei Technologies Co., Ltd.

9.2.50 timers rip

Function

The **timers rip** command sets the values of RIP timers.

The **undo timers rip** command restores the values of RIP timers to the default value.

By default, the interval for sending Update packets is 30s, the time for aging routes is 180s, the time for deleting a route from the routing table is 120s.

Format

timers rip *update age garbage-collect*

undo timers rip

Parameters

Parameter	Description	Value
update	Specifies the interval for sending Update packets.	The value is an integer ranging from 1 to 86400, in seconds.
age	Specifies the time for aging routes.	The value is an integer ranging from 1 to 86400, in seconds.
garbage-collect	Specifies the time for deleting a route from the routing table, that is, the standard garbage collection time.	The value is an integer ranging from 1 to 86400, in seconds.

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

By adjusting the RIP timers, you can improve routing protocol performance to meet network requirements. If the values of the preceding three timers are set improperly, route flapping occurs.

The relationship of the values of the three timers is: *update* < *age* and *update* < *garbage-collect*. For example, if the update time is longer than the aging time, routers cannot inform neighbors on time if RIP routes change during the update time.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Generally, the default values of the timers do not need to be changed, and thus the **timers rip** command must be used with caution.

Example

Set values for RIP timers.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] timers rip 35 170 240
```

9.2.51 verify-source (RIP)

Function

The **verify-source** command enables check on source IP addresses in RIP Update packets.

The **undo verify-source** command disables check on source IP addresses in RIP Update packets.

By default, the source IP addresses in RIP Update packets are checked.

Format

verify-source

undo verify-source

Parameters

None

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **verify-source** command is executed, RIP checks whether the IP addresses of interfaces that send and receive the Update packets are on the same network segment. If not, the device does not process the packets.

NOTE

It is not recommended that you disable source address check.

Example

Enable source address check in RIP 100.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] verify-source
```

9.2.52 version (RIP)

Function

The **version** command specifies a global RIP version.

The **undo version** command restores the default global RIP version.

By default, an interface sends only RIP-1 packets, and receives both RIP-1 and RIP-2 packets.

Format

version { **1** | **2** }

undo version

Parameters

Parameter	Description	Value
1	Set the global RIP version to RIP-1.	-
2	Set the global RIP version to RIP-2.	-

Views

RIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Send and receive RIP-2 packets.

```
<Huawei> system-view
[Huawei] rip 100
[Huawei-rip-100] version 2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.2.8 display rip

9.3 RIPng Configuration Commands

9.3.1 checkzero (RIPng)

Function

The **checkzero** command enables zero field check for RIPng packets.

The **undo checkzero** command disables zero field check for RIPng packets.

By default, zero field check is enabled for RIPng packets.

Format

checkzero

undo checkzero

Parameters

None

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

After zero field check is enabled, the router refuses to process the RIPng packets in which zero fields are not 0. If all RIPng packets are reliable and no zero field needs to be checked, run the **undo checkzero** command to reduce CPU usage.

Example

Disable zero field check for RIPng packets.

```
<Huawei> system-view
[Huawei] ripng 1
[Huawei-ripng-1] undo checkzero
```

Related Topics

9.3.18 ripng

 Copyright © Huawei Technologies Co., Ltd.

9.3.2 default-cost (RIPng)

Function

The **default-cost** command sets the default cost for imported routes.

The **undo default-cost** command restores the default value 0.

By default, the default cost of RIPng routes is 0.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Sets the default cost of imported routes.	The value is an integer that ranges from 0 to 15.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

You can run one of the following commands to set the cost of imported routes. The following commands are listed in descending order of priorities.

- Run the **apply cost** command to set the cost of routes.
- Run the **9.3.14 import-route (RIPng)** command to set the cost of imported routes.
- Run the **default-cost (RIPng)** command to set the default cost of imported routes.

Example

Set the default cost of imported routes to 2.

```
<Huawei> system-view
[Huawei] ripng 100
[Huawei-ripng-100] default-cost 2
```

Related Topics

9.9.7 apply cost

9.3.14 import-route (RIPng)

 Copyright © Huawei Technologies Co., Ltd.

9.3.18 ripng

9.3.3 description (RIPng)

Function

The **description** command configures a description for a RIPng process.

The **undo description** command deletes the configured description of a RIPng process.

By default, there is no description for a RIPng process.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Configures a description for a RIPng process.	The description is a string of 1 to 80 case-sensitive characters that can contain spaces.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring descriptions for RIPng processes helps identify and configure RIPng processes.

Precautions

If you run the **description** command multiple times, only the latest configuration takes effect.

Example

Configure a description for RIPng process 100.

```
<Huawei> system-view
[Huawei] ripng 100
[Huawei-ripng-100] description this process configure the poison reverse process
```

 Copyright © Huawei Technologies Co., Ltd.

9.3.4 display default-parameter ripng

Function

The **display default-parameter ripng** command displays the default RIPng configuration.

Format

display default-parameter ripng

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the default RIPng configuration is modified, you can use the **display default-parameter ripng** command to view the default RIPng configuration used when RIPng is initialized.

Example

Display the default RIPng configuration.

```
<Huawei> display default-parameter ripng
-------------------------------------------
 Protocol Level Default Configurations
-------------------------------------------
      Preference    : 100
      Checkzero     : Enabled
      Default-cost  : 0
      Maximum Balanced Paths : 8
      Update time   : 30 sec     Age time   : 180 sec
      Garbage-collect time           : 120 sec
-------------------------------------------
 Interface Level Default Configurations
-------------------------------------------
   Metricin                : 0
   Metricout               : 1
   Input Packet Processing : Enabled
   Output Packet Processing: Enabled
   Poison Reverse          : Disabled
   Split Horizon
    For Broadcast and P2P Interfaces     :  Enabled
    For NBMA Interfaces and LoopBack     :  Disabled
   Default Route                         :  Disabled
   Packet Transmit Interval              :  200 msecs
   Packet Transmit Number                :  30
```

Table 9-14 Description of the display default-parameter ripng command output

Item	Description
Protocol Level Default Configurations	Default RIPng process configuration.
Preference	RIPng route preference.
Checkzero	Whether zero field check is enabled for RIPng packets.
Default-cost	Default cost of routes imported by RIPng from other routing protocols.
Maximum Balanced Paths	Maximum number of equal-cost routes for load balancing.
Update time	Interval for sending Update packets.
Age time	Aging time of RIPng routes.
Garbage-collect time	Time from when a route is marked invalid until the route is removed from the routing table.
Interface Level Default Configurations	Default RIPng configuration on an interface.
Metricin	Metric that is added to a route when a RIPng packet is received.
Metricout	Metric that is added to a route when a RIPng packet is sent.
Poison Reverse	Whether poison reverse is enabled.
Split Horizon	Whether split horizon is enabled: ● For Broadcast and P2P Interfaces: broadcast and P2P interfaces ● For NBMA Interfaces and LoopBack: NBMA and loopback interfaces
Default Route	Default route. This route is used when no matching entry can be found for a packet in the routing table.
Packet Transmit Interval	Interval for forwarding packets, in milliseconds.
Packet Transmit Number	Number of forwarded packets.
Input Packet Processing	Whether this interface is enabled to receive RIPng packets
Output Packet Processing	Whether this interface is enabled to send RIPng packets

 Copyright © Huawei Technologies Co., Ltd.

9.3.5 display ripng

Function

The **display ripng** command displays the current operating status and configuration of a RIPng process.

Format

display ripng [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Displays the current operating status and configuration of the specified RIPng process. If this parameter is not specified, the configurations of all RIPng processes are displayed.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays the status and configuration of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about a RIPng process.

```
<Huawei> display ripng 100
Public vpn-instance
  RIPng process : 100
    Preference    : 100
    Checkzero     : Enabled
    Default-cost  : 0
    Maximum number of balanced paths : 8
    Update time   : 30 sec   Age time  : 180 sec
    Garbage-collect time           : 120 sec
    Number of periodic updates sent : 0
```

```
    Number of trigger updates sent  : 1
    Number of routes in database    : 1
    Number of interfaces enabled    : 1
    Total number of routes          : 3
    Total number of routes in ADV DB is : 0
```

Table 9-15 Description of the display ripng command output

Item	Description
Public vpn-instance	The Public VPN
RIPng process	RIPng process ID.
Preference	RIPng process preference.
Checkzero	Whether zero field check is enabled for RIPng packets.
Default-cost	Default cost of routes imported by RIPng from other routing protocols.
Maximum number of balanced paths	Maximum number of equal-cost routes for load balancing.
Update time	Interval for sending Update packets.
Age time	Aging time of RIPng routes.
Garbage-collect time	Time from when a route is marked invalid until the route is removed from the routing table.
Number of periodic updates sent	Number of RIPng Update packets sent periodically.
Number of trigger updates sent	Number of triggered RIPng Update packets.
Number of routes in database	Number of routes in the RIPng database.
Number of interfaces enabled	Number of RIPng interfaces.
Total number of routes	Total number of routes of an RIPng process.
Total number of routes in ADV DB is	Total number of advertised routes in the database.

Related Topics

9.3.18 ripng

9.3.6 display ripng database

Function

The **display ripng database** command displays all the active routes in the RIPng database.

Format

display ripng *process-id* **database** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Displays all the active routes of the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
verbose	Displays detailed information about the routes in the RIPng database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Displays routes in the RIPng database.

```
<Huawei> display ripng 100 database
1::/64,
      via FE80::82FB:6FF:FE35:45B6, GigabitEthernet2/0/0, cost 0, Imported
  2::/64,
      GigabitEthernet1/0/0, cost 0, RIPng-interface
  3::/64,
      via FE80::82FB:6FF:FE35:45B6, GigabitEthernet2/0/0, cost 16
  3::/64,
      GigabitEthernet2/0/0, cost 0, RIPng-interface
  4::/64,
      via FE80::82FB:6FF:FE35:45B6, GigabitEthernet2/0/0, cost 1
```

Table 9-16 Description of the display ripng database command output

Item	Description
1::/64	Destination IPv6 address of a route.

Item	Description
via	Next-hop link-local address.
cost	Cost of a route.
Imported	Route imported from other routing protocols.
RIPng-interface	Route generated by RIPng.

Related Topics

9.3.18 ripng

9.3.7 display ripng interface

Function

The **display ripng interface** command displays information about RIPng interfaces.

Format

display ripng *process-id* **interface** [*interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Displays interface information in the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
interface-type interface-number	Displays information on the interface with the specified type and number.	-
verbose	Displays detailed information about RIPng interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the configuration and operating status of RIPng. The information is helpful in fault location and configuration verification.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about GE1/0/0 of the specified RIPng process.

```
<Huawei> display ripng 1 interface gigabitethernet 1/0/0
 GigabitEthernet1/0/0
    FE80::A0A:200:1
    State : UP, Protocol : RIPNG, MTU : 1440
```

Table 9-17 Description of the display ripng interface command output

Item	Description
FE80::A0A:200:1	Link-local address of the interface.
State	Status of the interface: ● Up ● Down
Protocol	Routing protocol running on the interface.
MTU	Link MTU.

Display detailed information about GE1/0/0 of the specified RIPng process.

```
<Huawei> display ripng 1 interface gigabitethernet 1/0/0 verbose
 GE1/0/0
    FE80::A0A:200:1
    State : UP, Protocol : RIPNG, MTU : 1440
    Metricin       : 0
    Metricout      : 1
    Input          : Enabled     Output : Enabled
    Default Route  : Disabled
    Poison Reverse : Disabled
    Split Horizon  : Enabled
```

Table 9-18 Description of the display ripng interface verbose command output

Item	Description
FE80::A0A:200:1	Link-local address of the interface.
State	Status of the interface: ● UP ● DOWN
Protocol	Routing protocol running on the interface.
MTU	Link MTU.
Metricin	Metric added to a received route.
Metricout	Metric added to a sent route.
Input	Indicates whether this interface is enabled to receive RIPng packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output	Indicates whether this interface is enabled to send RIPng packets.
Default Route	Whether the interface is enabled to advertise default routes.
Poison Reverse	Whether poison reverse is enabled on the interface.
Split Horizon	Whether split horizon is enabled on the interface.

Related Topics

9.3.18 ripng

9.3.8 display ripng neighbor

Function

The **display ripng neighbor** command displays information about RIPng neighbors.

Format

display ripng *process-id* **neighbor** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Displays neighbor information in the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
verbose	Displays detailed information about RIPng neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Display neighbor information in RIPng process 1.

```
<Huawei> display ripng 1 neighbor
 Neighbor : FE80::A0A:201:1 GigabitEthernet1/0/0
    Protocol : RIPNG
```

Table 9-19 Description of the display ripng neighbor command output

Item	Description
Neighbor	Displays the IPv6 address and interface type of the neighbor interface.
Protocol	Routing protocol running.

Display detailed neighbor information in RIPng process 1.

```
<Huawei> display ripng 1 neighbor verbose
 Neighbor : FE80::A0A:201:1 GE1/0/0
    Protocol : RIPNG
    Number of Active routes      : 1
    Number of routes in garbage  : 0
```

Table 9-20 Description of the display ripng neighbor verbose command output

Item	Description
Number of Active routes	Number of active routes.
Number of routes in garbage	Number of garbage routes.

9.3.9 display ripng neighbor last-nbr-down

Function

The **display ripng neighbor last-nbr-down** command displays information about the last neighbor that goes Down in a RIPng process.

Format

display ripng *process-id* **neighbor last-nbr-down**

Parameters

Parameter	Description	Value
process-id	Displays information about the last neighbor that goes Down in the specified RIPng process.	The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ripng neighbor last-nbr-down** command can be used to view information about the last neighbor that goes Down in a RIPng process and the reason why the neighbor goes Down.

Example

Display information about the last neighbor that goes Down in a RIPng process.

```
<Huawei> display ripng 1 neighbor last-nbr-down
 Neighbor down index              : 1
 Neighbor Link local Address      : FE80::2E0:B7FF:FE5B:8242
 Interface                        : gigabitethernet 1/0/0
 Reason for Neighbor down         : Interface Down
 Time at which neighbor went down : 2011-06-02 12:03:40+03:00 DST
```

Table 9-21 Description of the display ripng neighbor last-nbr-down command output

Item	Description
Neighbor down index	Index of the neighbor that goes Down.
Neighbor Link local Address	IPv6 link-local address of the neighbor interface.
Interface	Interface connecting to the neighbor.
Reason for Neighbor down	Reason why the neighbor goes Down.
Time at which neighbor went down	Time the neighbor goes Down.

9.3.10 display ripng route

Function

The **display ripng route** command displays all the RIPng routes that the router learns from other routers.

Format

display ripng *process-id* **route**

Parameters

Parameter	Description	Value
process-id	Displays the RIPng routes of the specified RIPng process that the router learns from other routers.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ripng route** command is useful for debugging and testing protocols.

Example

Display all active and inactive RIPng routes and timers of each route.

```
<Huawei> display ripng 100 route
  Route Flags: R - RIPng
               A - Aging, G - Garbage-collect
 ------------------------------------------------------------------------------
 Peer FE80::200:5EFF:FE04:B602  on gigabitethernet1/0/0
 Dest 3FFE:C00:C18:1::/64,
    via FE80::200:5EFF:FE04:B602, cost  2, tag 0, RA, 34 Sec
 Dest 3FFE:C00:C18:2::/64,
    via FE80::200:5EFF:FE04:B602, cost  2, tag 0, RA, 34 Sec
 Peer FE80::200:5EFF:FE04:B602  on gigabitethernet1/0/0
 Dest 3FFE:C00:C18:1::/64,
    via FE80::200:5EFF:FE04:B601, cost  2, tag 0, RA, 13 Sec
 Dest 3FFE:C00:C18:3::/64,
    via FE80::200:5EFF:FE04:B601, cost  2, tag 0, RA, 13 Sec
 Peer FE80::200:5EFF:FE04:B602  on gigabitethernet1/0/0
 Dest 100::/32,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, RA, 6 Sec
 Dest 4000:1::/64,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, RA, 6 Sec
 Dest 4000:2::/64,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, RA, 6 Sec
 Dest 4000:3::/64,
    via FE80::200:5EFF:FE04:3302, cost  2, tag 0, RA, 6 Sec
```

 Copyright © Huawei Technologies Co., Ltd.

Table 9-22 Description of the display ripng route command output

Item	Description
Route Flags	Route tag. The first character indicates the type of the route, namely, a RIPng route; the second character indicates the status of the route: ● RA: The RIPng route is in aging state. ● RG: The RIPng route is in garbage collection state.
Peer	Neighbor connecting to the interface.
Dest	Destination IPv6 address.
via	Next-hop IPv6 address.
cost	Cost of a route.
tag	Route tag.
Sec	Time during which a route remains in the state indicated by the route tag.

Related Topics

9.3.18 ripng

9.3.11 display ripng statistics interface

Function

The **display ripng statistics interface** command displays statistics about packets received and sent by interfaces in a RIPng process.

Format

display ripng *process-id* **statistics interface** { **all** | *interface-type interface-number* [**verbose** | **neighbor** *neighbor-ipv6-address*] }

Parameters

Parameter	Description	Value
process-id	Displays statistics on the interface of the specified RIPng process.	The value is an integer that ranges from 1 to 65535.
all	Displays statistics on all interfaces.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Displays statistics on the specified interface.	-
verbose	Displays detailed statistics.	-
neighbor *neighbor-ipv6-address*	Displays statistics about the specified neighbor.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the configuration and operating status of RIPng. The information is helpful in fault location and configuration verification.

Example

Display statistics about GE1/0/0 of RIPng process 1.

```
<Huawei> display ripng 1 statistics interface gigabitethernet 1/0/0
GigabitEthernet1/0/0(FE80::2E0:B9FF:FE7F:1A01)
Statistical information          Last min     Last 5 min    Total
-----------------------------------------------------------------
Periodic updates sent            5            23            259
Triggered updates sent           5            30            408
Response packets sent            10           34            434
Response packets received        15           38            467
Response packets ignored         0            0             0
Request packets sent             1            3             8
Request packets received         4            20            40
Request packets ignored          0            0             0
Bad packets received             0            0             0
Routes received                  2            10            0
Routes sent                      1            4             4
Bad routes received              0            0             0
Packets send failed              0            0             0
```

Table 9-23 Description of the display ripng statistics interface command output

Item	Description
Statistical information	Packet type.
Last min	Statistics within the last minute.
Last 5 min	Statistics within the last 5 minutes.
Total	Total statistics.
Periodic updates sent	Number of periodically sent Update packets.

Item	Description
Triggered updates sent	Number of triggered sent Update packets.
Response packets sent	Number of sent RIPng Response packets.
Response packets received	Number of received RIPng Response packets.
Response packets ignored	Number of ignored RIPng Response packets.
Request packets sent	Number of sent RIPng Request packets.
Request packets received	Number of received RIPng Request packets.
Request packets ignored	Number of ignored RIPng Request packets.
Bad packets received	Number of received packets that cannot be parsed.
Bad routes received	Number of received routes that cannot be parsed.
Routes received	Number of received routes.
Routes sent	Number of sent routes.
Packets send failed	Number of RIPng packets that fail to be sent.

Related Topics

9.3.17 reset ripng statistics

9.3.12 filter-policy export (RIPng)

Function

The **filter-policy export** command specifies the filtering policy for sent routes.

The **undo filter-policy export** command cancels the configuration.

By default, no filtering policy is configured.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL, which is case sensitive.	The name is a string of 1 to 32 case-sensitive characters without spaces, which begins with a letter.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the name of a routing protocol from which routes are imported.	The value can be **bgp**, **direct**, **isis**, **unr**, **ripng**, **static**, or **ospfv3**.
process-id	Specifies the process ID of IS-IS, RIPng, or OSPFv3.	The value is an integer that ranges from 1 to 65535.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

In some cases, you need to precisely control the advertisement of RIPng routes to meet complicated network requirements. RIPng can use an IPv6 prefix list, route policy and ACL to filter imported routes, allowing only the routes matching the IPv6 prefix list, route policy and ACL to be advertised to RIPng neighbors.

Example

Use IPv6 prefix list **Filter2** to filter the RIPng Update packets that need to be advertised.

```
<Huawei> system-view
[Huawei] ripng 100
[Huawei-ripng-100] filter-policy ipv6-prefix Filter2 export
```

Related Topics

9.3.14 import-route (RIPng)

9.3.13 filter-policy import (RIPng)

Function

The **filter-policy import** command specifies the filtering policy for received routes. Only the routes that match the filtering policy can be received.

The **undo filter-policy import** command cancels the configuration.

By default, no filtering policy is configured.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL, which is case sensitive.	The name is a string of 1 to 32 case-sensitive characters without spaces, which begins with a letter.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIPng view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

In some cases, you need to precisely control the receiving of RIPng routes to meet complicated network requirements. RIPng can use an IPv6 prefix list, route policy and ACL to filter received RIPng routes, allowing only the routes matching the IPv6 prefix list, route policy and ACL to be added to RIPng routing tables.

Example

Use IPv6 prefix list **Filter1** to filter received RIPng Update packets.

```
<Huawei> system-view
[Huawei] ripng 1
[Huawei-ripng-1] filter-policy ipv6-prefix Filter1 import
```

9.3.14 import-route (RIPng)

Function

The **import-route** command imports routes.

The **undo import-route** command cancels importing routes.

By default, no route is imported.

Format

import-route { { **ripng** | **isis** | **ospfv3** } [*process-id*] | **bgp** [**permit-ibgp**] | **unr** | **direct** | **static** } [[**cost** *cost* | **inherit-cost**] | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

Parameters

Parameter	Description	Value
protocol	Specifies the routing protocol from which routes are imported.	The value can be **direct**, **static**, **ripng**, **isis**, **unr**, **bgp**, or **ospfv3**.
ripng	Imports RIPng routes.	-
isis	Imports IS-IS routes.	-
ospfv3	Imports OSPFv3 routes.	-
process-id	Specifies the process ID of imported routes. The process ID needs to be specified only when the *protocol* parameter is **ripng**, **ospfv3**, or **isis**.	The value is an integer that ranges from 1 to 65535.
bgp	Imports BGP routes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
permit-ibgp	Imports IBGP routes in a public network instance. **NOTE** • Import of IBGP routes in RIPng process can lead to routing loops. Administrators should take care of routing loops before configuring **permit-ibgp**.	-
unr	Imports UNR routes.	-
direct	Imports direct routes.	-
static	Imports static routes.	-
cost *cost*	Specifies the cost of imported routes. If no cost is specified, the default cost configured using the **default-cost** command is used.	The value is an integer that ranges from 0 to 15.
inherit-cost	Specifies to retain the original cost of the imported route.	-
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

You can configure a route-policy to allow RIPng to import only the routes that match the rout-policy and set attributes for imported routes.

You can run one of the following commands to set the cost of imported routes. The following commands are listed in descending order of priorities.

- Run the **apply cost** command to set the cost of routes.
- Run the **import-route** (RIPng view) command to set the cost of imported routes.
- Run the **default-cost (RIPng)** command to set the default cost of imported routes.

NOTE

After the **import-route direct** command is executed, routes to the network segment where the IPv6 address of the management interface belongs are also imported in the RIPng routing table. Therefore, use this command with caution.

Example

Import routes from IS-IS process 7 and set the cost of imported routes to 7.

```
Huawei system-view
[Huawei] ripng 1
[Huawei-ripng-1] import-route isis 7 cost 7
```

Import the IBGP routes matching route-policy **abc** to RIPng process 1 and set the cost of imported routes to 5.

```
Huawei> system-view
[Huawei] ripng 1
[Huawei-ripng-1] import-route bgp permit-ibgp cost 5 route-policy abc
```

9.3.15 maximum load-balancing (RIPng)

Function

The **maximum load-balancing** command configures the maximum number of equal-cost routes for load balancing.

The **undo maximum load-balancing** command restores the default setting.

By default, the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204 support a maximum of four equal-cost routes, and the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series support a maximum of eight equal-cost routes, AR2240 (using SRU200, SRU200E or SRU400), and AR3200 (using SRU200, SRU200E or SRU400) series support a maximum of sixteen equal-cost routes.

Format

maximum load-balancing *number*

undo maximum load-balancing

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes for load balancing.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

If there are multiple links on the network, you can set the maximum number of equal-cost routes for load balancing. This prevents some links from being heavily loaded and improves network resource efficiency.

Example

Set the maximum number of equal-cost routes to 4.

```
<Huawei> system-view
[Huawei] ripng 1
[Huawei-ripng-1] maximum load-balancing 4
```

Related Topics

9.3.10 display ripng route

9.3.16 preference (RIPng)

Function

The **preference** command specifies the preference for RIPng routes.

The **undo preference** command restores the default setting.

By default, the preference of RIPng routes is 100.

Format

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Parameters

Parameter	Description	Value
preference	Specifies the preference of RIPng routes.	The value is an integer that ranges from 1 to 255.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

A smaller value indicates a higher preference. To make RIPng routes take precedence over other IGP routes, set a smaller preference value for RIPng routes. The preference values also determine which routing protocol's routes are optimal routes in an IPv6 routing table.

Example

Set the preference of RIPng routes to 120.

```
<Huawei> system-view
[Huawei] ripng 100
[Huawei-ripng-100] preference 120
```

Set the preference of the RIPng routes matching route-policy **policy1** to 60.

```
<Huawei> system-view
[Huawei] ripng 100
[Huawei-ripng-100] preference route-policy policy1 60
```

9.3.17 reset ripng statistics

Function

The **reset ripng statistics** command clears statistics in a specified RIPng process.

Format

reset ripng *process-id* **statistics** [**interface** { **all** | *interface-type interface-number* [**neighbor** *neighbor-ipv6-address*] }]

Parameters

Parameter	Description	Value
process-id	Specifies a RIPng process ID.	The value is an integer that ranges from 1 to 65535.
interface all	Clears statistics on all interfaces.	-
interface *interface-type interface-number*	Clears statistics on the specified interface.	-
neighbor *neighbor-ipv6-address*	Clears statistics in the RIPng process with the specified neighbor.	The value is a 32-digit hexadecimal number, in the common format of X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use the **reset ripng statistics** command in the user view to clear statistics in a specified RIPng process and re-collect statistics for debugging.

NOTICE

Statistics about a RIPng process cannot be restored after being cleared. So, exercise caution when using this command.

Example

Clear statistics on all the interfaces in RIPng process 100.

```
<Huawei> reset ripng 100 statistics interface all
Warning:The RIPNG statistics will be reset. Continue? [Y/N] y
```

 Copyright © Huawei Technologies Co., Ltd.

9.3.18 ripng

Function

The **ripng** command creates a RIPng process.

The **undo ripng** command deletes a RIPng process.

By default, no RIPng process is created.

Format

ripng [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ripng *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies a RIPng process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring RIPng functions, run the **ripng** command to create a RIPng process.

When a RIPng process is deleted, the **ripng enable** command needs to be run again on interfaces.

Example

Create a specified RIPng process.

```
<Huawei> system-view
[Huawei] ripng 100
[Huawei-ripng-100]
```

Related Topics

9.3.21 ripng enable

9.3.19 ripng default-route

Function

The **ripng default-route** command generates a default route to the RIPng routing domain.

The **undo ripng default-route** command disables advertising RIPng default routes and forwarding IPv6 default routes.

By default, there is no default route in the RIPng routing domain.

Format

ripng default-route { **only** | **originate** } [**cost** *cost*]

undo ripng default-route

Parameters

Parameter	Description	Value
only	Advertises only IPv6 default routes (::/0) and suppresses the advertisement of other routes.	-
originate	Advertises IPv6 default routes (::/0) without affecting the advertisement of other routes.	-
cost *cost*	Specifies the cost of default routes.	The value is an integer that ranges from 0 to 15. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The generated default RIPng route is forcibly advertised in an Update packet through the specified interface, regardless of whether this route already exists in the IPv6 routing table.

This command can take effect only after IPv6 is enabled for the interface by the **ipv6 enable** command.

Example

Advertise only default routes in Update packets through an interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng default-route only
```

Advertise default routes together with other routes in Update packets through an interface.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng default-route originate
```

9.3.20 ripng input

Function

The **ripng input** command enables the specified interface to receive RIPng packets.

The **undo ripng input** command disables the specified interface from receiving RIPng packets.

By default, interfaces can receive RIPng packets.

Format

ripng input

undo ripng input

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a device running RIPng is connected to a network running other routing protocols, you can run the **undo ripng input** command on the interface that connects the device to the network to prevent the interface from receiving RIPng packets from the network.

Example

Disable GE1/0/0 interface to receive RIPng packets.

```
<Huawei> system-view
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo ripng input
```

Related Topics

9.3.24 ripng output

9.3.21 ripng enable

Function

The **ripng enable** command enables RIPng on an interface.

The **undo ripng** command disables RIPng on an interface.

By default, RIPng process is disabled.

Format

ripng *process-id* **enable**

undo ripng

Parameters

Parameter	Description	Value
process-id	Specifies a RIPng process ID.	The value is an integer that ranges from 1 to 65535.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

This command can take effect only after IPv6 is enabled for the RIPng process and interfaces. This command is not supported on ATM interfaces.

Example

Enable RIPng process 100 on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ripng 100
[Huawei-ripng-100] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address fc00:0:0:1::1/64
[Huawei-GigabitEthernet1/0/0] ripng 100 enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.3.18 ripng

9.3.22 ripng metricin

Function

The **ripng metricin** command sets the metric that is added to the RIPng route received by an interface.

The **undo ripng metricin** command restores the default metric added to a received RIPng route.

By default, an interface does not add the metric to a received RIPng route.

Format

ripng metricin *value*

undo ripng metricin

Parameters

Parameter	Description	Value
value	Specifies the value of the metric to be added to a received RIPng route.	The value is an integer that ranges from 0 to 15. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When an interface receives a valid RIPng route, the interface adds a metric to the route before adding the route to the routing table. The metric of this route is changed in the routing table. That is, increasing the metric of an interface also increases the metric of the RIPng route received by the interface.

Before running the **ripng metricin** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Set the metric that is added to a received RIPng route to 12.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng metricin 12
```

Related Topics

8.8.28 ipv6 enable (interface view)

9.3.23 ripng metricout

Function

The **ripng metricout** command sets the metric that is added to the RIPng route sent by an interface.

The **undo ripng metricout** command restores the default setting.

By default, the metric that is added to the RIPng route sent by an interface is 1.

Format

ripng metricout { *value* | { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } *value1* }

undo ripng metricout

Parameters

Parameter	Description	Value
value	Specifies the metric added to a sent route.	The value is an integer that ranges from 1 to 15. The default value is 1.
acl6-number	Specifies the number of a basic ACL6.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL.	The name is a string of 1 to 32 case-sensitive characters, which begins with a letter without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
value1	Specifies the metric added to the route matching the IPv6 prefix list.	The value is an integer that ranges from 2 to 15.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

An interface adds a metric to a route before advertising the route. Therefore, increasing the metric of an interface also increases the metric of the RIPng routes sent by the interface. The metric of the route in the routing table, however, remains unchanged.

Before running the **ripng metricout** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Set the metric that is added to a route sent on an interface to 12.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng metricout 12
```

Set the metric that is added to the RIPng route matching IPv6 prefix list **p1** to 12.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ip ipv6-prefix p1 permit fc00:0:0:1::1 128
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng metricout ipv6-prefix p1 12
```

Related Topics

8.8.28 ipv6 enable (interface view)

9.3.24 ripng output

Function

The **ripng output** command enables an interface to send RIPng packets.

The **undo ripng output** command disables an interface from sending RIPng packets.

By default, an interface can send RIPng packets.

Format

ripng output

undo ripng output

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When a device running RIPng is connected to a network running other routing protocols, you can run the **undo ripng output** command on the interface that connects the device to the network to prevent the interface from sending RIPng packets to the network.

Example

Disable GE1/0/0 interface to send RIPng packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo ripng output
```

Related Topics

9.3.20 ripng input

9.3.25 ripng pkt-transmit

Function

The **ripng pkt-transmit** command sets the interval for sending Update packets and the number of packets sent each time on a specified interface.

The **undo ripng pkt-transmit** command restores the default value.

By default, the interval for sending Update packets is 200 ms and the number of packets sent each time is 30 on the RIPng interface.

Format

ripng pkt-transmit { **interval** *interval* | **number** *pkt-count* } *

undo ripng pkt-transmit

Parameters

Parameter	Description	Value
interval *interval*	Specifies the interval for sending Update packets.	The value is an integer that ranges from 50 to 500, in milliseconds. The default value is 200.

Parameter	Description	Value
number *pkt-count*	Specifies the number of packets sent each time.	The value is an integer that ranges from 25 to 100. The default value is 30.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Running the **ripng pkt-transmit** command in the interface view as required can accurately control the interval for sending packets and the number of sent packets. RIPng performance is then improved.

Before running the **ripng pkt-transmit** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Set the interval for sending Update packets on GE1/0/0 to 100 ms and the number of packets sent each time to 50.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng pkt-transmit interval 100 number 50
```

Related Topics

8.8.28 ipv6 enable (interface view)

9.3.26 ripng poison-reverse

Function

The **ripng poison-reverse** command enables poison reverse for RIPng.

The **undo ripng poison-reverse** command disables poison reverse for RIPng.

By default, poison reverse is disabled for RIPng.

Format

ripng poison-reverse

undo ripng poison-reverse

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After poison reverse is configured, the route learned from an interface is also sent to the neighboring device through the same interface. The metric of this route is set to 16, indicating that the route is unreachable.

When split horizon and poison reverse are configured on the same interface, only poison reverse takes effect.

Before running the **ripng poison-reverse** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Enable poison reverse for RIPng Update packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng poison-reverse
```

Disable poison reverse for RIPng Update packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ripng poison-reverse
```

Related Topics

9.3.27 ripng split-horizon

8.8.28 ipv6 enable (interface view)

9.3.27 ripng split-horizon

Function

The **ripng split-horizon** command enables split horizon for RIPng.

The **undo ripng split-horizon** command disables split horizon for RIPng.

By default, split horizon is enabled except on the NBMA network.

 Copyright © Huawei Technologies Co., Ltd.

Format

ripng split-horizon

undo ripng split-horizon

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After split horizon is enabled, a route is blocked if the route is advertised through the interface that learns the route. The split horizon mechanism avoids routing loops between adjacent neighbors.

When poison reverse and split horizon are configured on the same interface, only poison reverse takes effect.

Before running the **ripng split-horizon** command on an interface, run the **ipv6 enable** command to enable IPv6 on the interface.

Example

Enable split horizon for RIPng Update packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ripng split-horizon
```

Disable split horizon for RIPng Update packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] undo ripng split-horizon
```

Related Topics

9.3.26 ripng poison-reverse

8.8.28 ipv6 enable (interface view)

 Copyright © Huawei Technologies Co., Ltd.

9.3.28 ripng summary-address

Function

The **ripng summary-address** command configures a RIPng device to advertise summarized IPv6 addresses on an interface.

The **undo ripng summary-address** command deletes this configuration.

By default, a RIPng router does not advertise summarized IPv6 addresses.

Format

ripng summary-address *ipv6-address prefix-length* [**avoid-feedback**]

undo ripng summary-address *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies a summarized IPv6 address.	The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.
avoid-feedback	Disables an interface from learning the same summarized route.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If the prefix and prefix length of a route match the defined IPv6 prefix, the defined IPv6 prefix is advertised instead of the route. As a result, multiple routes are replaced by a single route that has a lower metric.

After the keyword **avoid-feedback** is specified, an interface no longer learns the summarized route with the same IP address as the advertised summarized IP address. This avoids routing loops.

This command can take effect only after IPv6 is enabled for the RIPng process and interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure IPv6 address FC00:200::3EFF:FE11:6770 for GE1/0/0, set the prefix length to 64 bits, and summarize the configured IPv6 address as an IPv6 address with prefix FC00:200::/35 in RIPng process 100.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ripng 100
[Huawei-ripng-100] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address fc00:200::3EFF:FE11:6770/64
[Huawei-GigabitEthernet1/0/0] ripng 100 enable
[Huawei-GigabitEthernet1/0/0] ripng summary-address fc00:200:: 35
```

9.3.29 timers ripng

Function

The **timers ripng** command configures RIPng timers.

The **undo timers ripng** command restores the default values of timers.

By default, the interval for sending RIPng Update packets is 30s, the aging time of routes is 180s, and the time for deleting routes from an IPv6 routing table is 120s.

Format

timers ripng *update age garbage-collect*

undo timers ripng

Parameters

Parameter	Description	Value
update	Specifies the interval for sending Update packets. This parameter is the basic timing parameter of routing protocols.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 30 seconds.
age	Specifies the aging time of routes. The value of *age* must be at least three times the value of *update*. If no Update packet of a route is received within the aging time, the route becomes invalid (unreachable).	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 180 seconds.
garbage-collect	Specifies the time from when a route is found invalid until it is deleted from the routing table.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 120 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

RIPng view

Default Level

2: Configuration level

Usage Guidelines

The command can take effect only after global IPv6 is enabled.

If the values of the preceding four timers are set improperly, route flapping occurs. The relationship of the values of the three timers is: *update* < *age* and *update* < *garbage-collect*. For example, if the update time is longer than the aging time, routers cannot inform neighbors on time if RIP routes change during the update time.

Example

Set values for RIPng timers.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ripng 100
[Huawei-ripng-100] timers ripng 5 15 30
```

9.4 OSPF Configuration Commands

NOTE

In practical application, in order to realize that business forwarding is not affected by motherboard failure, it is usually possible to configure BGP GR in the hardware environment of dual motherboard to make sense.

All the models support the GR Helper, and only AR3200 series support the GR Restarter.

9.4.1 abr-summary (OSPF area)

Function

The **abr-summary** command configures route summarization on an Area Border Router (ABR).

The **undo abr-summary** command disables route summarization on an ABR.

By default, route summarization is not configured on ABRs.

Format

abr-summary *ip-address mask* [[**advertise** | **not-advertise**] | **cost** { *cost* | **inherit-minimum** }] *

abr-summary *ip-address mask* [[**advertise** [**generate-null0-route**] | **not-advertise** | **generate-null0-route** [**advertise**]] | **cost** { *cost* | **inherit-minimum** }] *

undo abr-summary *ip-address mask*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a summarized route.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address of the summarized route.	The value is in dotted decimal notation.
advertise | **not-advertise**	Determines whether to advertise the summarized route. By default, the summarized route is advertised.	-
cost *cost*	Specifies the cost of the summarized route. By default, the cost of the summarized route is the highest cost of specific routes.	The value is an integer that ranges from 0 to 16777214.
inherit-minimum	Indicates that the smallest cost of specific routes is used as the cost of the summarized route.	-
generate-null0-route	Generates a blackhole route to prevent routing loops.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale OSPF network, route search speed may decrease due to the large routing table size. Configure route summarization to reduce the routing table size and simplify management.

In route summarization, multiple routes with the same IP prefix are summarized into one. If a link connected to a device within a summarized IP address range alternates between Up and Down states, the link status change is not advertised to the devices outside the IP address range. This prevents route flapping and improves network stability.

The **abr-summary** command configures route summarization on an ABR. When the ABR sends routing information to other areas, it originates Type 3 LSAs for each network segment. If any contiguous segments exist in this area, run the **abr-summary** command to summarize these segments into one. The ABR then sends

just one summarized LSA, and no LSAs that belong to the summarized network segment specified by the command. Therefore, the routing table size is reduced, and router performance is improved.

Precautions

- This command applies only to ABRs for intra-area route summarization. The **asbr-summary** command configures AS Boundary Routers (ASBRs) to summarize the routes imported by OSPF.
- Route summarization cannot be configured on ABRs in different areas of the same process.

Example

In OSPF 100 area 1, summarize routes in two network segments, 10.42.10.0 and 10.42.110.0, into one route 10.42.0.0, and advertise the summarized route to other areas.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 1
[Huawei-ospf-100-area-0.0.0.1] network 10.42.10.0 0.0.0.255
[Huawei-ospf-100-area-0.0.0.1] network 10.42.110.0 0.0.0.255
[Huawei-ospf-100-area-0.0.0.1] abr-summary 10.42.0.0 255.255.0.0
```

Related Topics

9.4.2 area (OSPF)
9.4.69 ospf

9.4.2 area (OSPF)

Function

The **area** command creates an OSPF area and displays the OSPF area view.

The **undo area** command deletes a specified area.

By default, the system does not creates an OSPF area.

Format

area *area-id*

undo area *area-id*

Parameters

Parameter	Description	Value
area-id	Specifies the area ID. The area with the *area-id* being 0 is a backbone area.	The value can be a decimal integer or in dotted decimal notation. When the value is an integer, the value ranges from 0 to 4294967295.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of devices increases with the expansion of the network. This leads to a large LSDB on every OSPF-enabled device on a large-scale network. Consequently, route flapping frequently occurs and thus a large number of OSPF packets are transmitted on the network, which wastes bandwidth resources.

OSPF resolves this problem by partitioning an AS into different areas. An area is regarded as a logical group and each group is identified by an area ID.

Configuration Impact

After OSPF partitions the AS into different areas, functions, such as the timer, filter, and summarization, of multiple devices in the same area, can be planned and configured uniformly in the area. Therefore, the size of the LSDB is reduced and the network performance is improved.

Prerequisites

Run the **ospf** command before you run the **area** command to start the OSPF process and enter the OSPF view.

Precautions

- At the border of an area resides a router instead of a link.
- A network segment or a link belongs to only one area. The area to which each OSPF interface belongs must be specified.
- The backbone area is responsible for forwarding inter-area routing information. The routing information between the non-backbone areas must be forwarded through the backbone area.
- All non-backbone areas maintain the connectivity with the backbone area and the backbone areas in different OSPF areas maintain the connectivity with each other.

Example

Enter the view of an OSPF area.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 0
[Huawei-ospf-100-area-0.0.0.0]
```

Related Topics

9.4.65 network (OSPF Area)

9.4.3 asbr-summary

Function

The **asbr-summary** command configures AS Boundary Routers (ASBRs) to summarize the routes imported by OSPF.

The **undo asbr-summary** command disables ASBRs from summarizing the routes imported by OSPF.

By default, ASBRs do not summarize the routes imported by OSPF.

Format

asbr-summary *ip-address mask* [[**not-advertise** | **generate-null0-route**] | **tag** *tag* | **cost** *cost* | **distribute-delay** *interval*] *

asbr-summary type nssa-trans-type-reference [**cost nssa-trans-cost-reference**]

undo asbr-summary type

undo asbr-summary *ip-address mask*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a summarized route.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address of the summarized route.	The value is in dotted decimal notation.
not-advertise	Indicates that the summarized route is not advertised. If this parameter is not specified, the summarized route is advertised.	-
generate-null0-route	Generates a blackhole route to prevent routing loops.	-
tag *tag*	Specifies the tag of the summarized route.	The value is an integer that ranges from 0 to 4294967295. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cost *cost*	Specifies the cost of the summarized route. By default, for Type 1 external routes, the cost of the summarized route is the highest cost of specific routes; for Type 2 external routes, the cost of the summarized route equals the highest cost of specific routes plus 1.	The value is an integer that ranges from 0 to 16777214.
distribute-delay *interval*	Specifies the delay in advertising the summarized route.	The value is an integer that ranges from 1 to 65535, in seconds.
type nssa-trans-type-reference	Enables OSPF to refer to Type 5 LSAs that have been translated from Type 7 LSAs when it sets types for summary routes on ASBRs. By default, when OSPF sets types for summary routes on ASBRs, OSPF does not refer to Type 5 LSAs that have been translated from Type 7 LSAs.	-
cost nssa-trans-cost-reference	Enables OSPF to refer to Type 5 LSAs that have been translated from Type 7 LSAs when it sets costs for summary routes on ASBRs. By default, when OSPF sets types and costs for summary routes on ASBRs, OSPF does not refer to Type 5 LSAs that have been translated from Type 7 LSAs.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale OSPF network, route search speed may decrease due to the large routing table size. Configure route summarization to reduce the routing table size and simplify management.

In route summarization, multiple routes with the same IP prefix are summarized into one. If a link connected to a device within a summarized IP address range alternates between Up and Down states, the link status change is not advertised to the devices outside the IP address range. This prevents route flapping and improves network stability.

 Copyright © Huawei Technologies Co., Ltd.

Imported routes with the same prefix can be summarized into one and advertised as one route using the **asbr-summary** command. Route summarization reduces routing information and routing table size, improving device performance.

After route summarization is implemented:

- If the local device is an ASBR in a common area, the local device summarizes all imported Type 5 LSAs within the summary address range.
- If the local device is an ASBR in an NSSA, the local device summarizes all imported Type 7 LSAs within the summary address range.
- If the local device functions as both an ASBR and ABR in an NSSA, the local device summarizes all imported Type 5 and Type 7 LSAs within the summary address range, and summarizes the Type 5 LSAs that have been transformed from Type 7 LSAs.

Precautions

When a large number of routes are summarized, specify the **distribute-delay** parameter to set the delay in advertising the summarized routes. This ensures that the advertised summarized routes contain more valid routes and avoids network flapping and incorrect routing information.

Example

Configure route summarization for the imported routes.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 not-advertise tag 2 cost 100
```

Cancel route summarization for the imported routes.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] undo asbr-summary 10.2.0.0 255.255.0.0
```

Related Topics

9.4.15 display ospf asbr-summary

9.4.4 authentication-mode (OSPF area)

Function

The **authentication-mode** command sets the authentication mode and password for an OSPF area.

The **undo authentication-mode** command cancels the authentication mode configured for an OSPF area.

By default, no authentication mode is configured.

Format

authentication-mode simple [**plain** *plain-text* | [**cipher**] *cipher-text*]

authentication-mode { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]

authentication-mode keychain *keychain-name*

undo authentication-mode

Parameters

Parameter	Description	Value
simple	Sets simple authentication. In simple authentication, the password type is **cipher** by default. **NOTICE** Simple authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
plain	Sets a plain text password. Only a plain text password can be entered, and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is specified, the password is saved in the configuration file in plain text. This carries security risks. It is recommended to specify **cipher** to save the password in cipher text.	-
plain-text	Sets a plain text password.	The value is a string of case-sensitive characters that can be letters or digits without spaces. In **simple** authentication, the value is a string of 1 to 8 characters. In **md5**, **hmac-md5** or **hmac-sha256** authentication, the value is a string of 1 to 255 characters.
cipher	Sets a cipher text password. Either a plain or cipher text password can be entered, and cipher text is displayed when the configuration file is viewed.	When **cipher** is configured, the password can only be entered in cipher text. Then, the password is displayed in cipher text in configuration files. MD5 authentication, HMAC-SHA256 authentication or HMAC-MD5 authentication defaults to use the password in cipher text.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher-text	Specifies the ciphertext password.	The value is a string of case-sensitive characters that can be letters or digits without spaces. In **simple** authentication, the value is a string of 1 to 8 characters in plain text, or a string of 48, 24 or 32 characters in cipher text. In **md5**, **hmac-sha256** or **hmac-md5** authentication, the value is a string of 1 to 255 characters in plain text, or a string of 20 to 392 characters in cipher text.
md5	Indicates MD5 authentication using the cipher text password. **NOTICE** MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates HMAC MD5 authentication using the cipher text password. **NOTICE** HMAC-MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates HMAC-SHA256 authentication.	-
key-id	Specifies authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail. Currently, only the **HMAC-MD5** and **HMAC-SHA256** algorithms can be used in OSPF.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Precautions

The authentication modes and passwords of all the devices must be the same in any given area, but can differ between several areas.

The **ospf authentication-mode** command used in the interface view takes precedence over the **authentication-mode** command used in the OSPF area view.

Example

Configure HMAC-SHA256 authentication for OSPF area 0.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 0
[Huawei-ospf-100-area-0.0.0.0] authentication-mode hmac-sha256
```

Related Topics

9.4.70 ospf authentication-mode

9.4.5 bandwidth-reference (OSPF)

Function

The **bandwidth-reference** command sets the bandwidth reference value that is used to calculate interface costs.

The **undo bandwidth-reference** command restores the default bandwidth reference value.

The default bandwidth reference value is 100 Mbit/s.

Format

bandwidth-reference *value*

undo bandwidth-reference

Parameters

Parameter	Description	Value
value	Specifies the bandwidth reference value for link cost calculation.	The value is an integer ranging from 1 to 2147483648, in Mbit/s. The default value is 100 Mbit/s.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The calculation formula is as follows: Interface cost = Bandwidth reference value/Interface bandwidth. The integer of the calculated result is the interface cost. If the calculated result is smaller than 1, the interface cost value is 1. If the **bandwidth-reference** command is executed to configure a new bandwidth reference value, the interface cost will be changed. As a result, OSPF will re-select routes.

The calculation formula is as follows: cost = Reference bandwidth(M)/Negotiated rate of the physical interface.

The default bandwidth reference value is 100 Mbit/s. The interface cost value is 100000000 divided by the interface bandwidth value.

Precautions

After the **bandwidth-reference** command is configured in a process view, bandwidth reference values of all interfaces in the process are changed to the specified value.

Generally, OSPF automatically calculate the link cost for an interface based on the bandwidth of the interface. You can modify the interface cost using the **ospf cost** command.

The **bandwidth-reference** command can be run on Eth-Trunk interfaces as same with on physical interfaces. If the command is run on an Eth-Trunk interface, the bandwidth of the Eth-Trunk interface is equal to the total bandwidth of all its member interfaces.

Example

Set the bandwidth reference value of the link cost to 1000 Mbit/s.

```
<Huawei> system-view
[Huawei] ospf 100
```

```
[Huawei-ospf-100] bandwidth-reference 1000
```

9.4.6 bfd all-interfaces (OSPF)

Function

The **bfd all-interfaces enable** command enables BFD in an OSPF process.

The **bfd all-interfaces** { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } * command sets the parameter values of a BFD session.

The **undo bfd all-interfaces enable** command disables BFD in an OSPF process.

The **undo bfd all-interfaces** { **min-rx-interval** | **min-tx-interval** | **detect-multiplier** | **frr-binding** } * command restores the default parameter values of a BFD session.

By default, BFD is not enabled at OSPF process.

Format

bfd all-interfaces enable

undo bfd all-interfaces enable

bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value*} * (AR100&AR120&AR150&AR160&AR200 series)

undo bfd all-interfaces { **min-rx-interval** | **min-tx-interval** | **detect-multiplier**} * (AR100&AR120&AR150&AR160&AR200 series)

bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } * (AR1200&AR2200&AR3200 series)

undo bfd all-interfaces { **min-rx-interval** | **min-tx-interval** | **detect-multiplier** | **frr-binding** } * (AR1200&AR2200&AR3200 series)

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Indicates the minimum interval at which BFD packets are received from the remote end.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.

Parameter	Description	Value
min-tx-interval *transmit-interval*	Indicates the minimum interval at which BFD packets are sent to the remote end.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
detect-multiplier *multiplier-value*	Indicates the local detection multiplier. **NOTE** After BFD is enabled, OSPF establishes BFD sessions only with the neighbors in the Full state.	The value is an integer ranging from 3 to 50. By default, it is 3.
frr-binding	Associates the BFD session status and link status on an interface. That is, when the BFD status goes Down, the link status of the interface also goes Down. This enables traffic to be switched to the backup path. **NOTE** AR100&AR120&AR150&AR160&AR200 series does not support the parameter **frr-binding**.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD can fast detect faults in communication with neighbors, thus minimizing the impact of such faults on services.

OSPF IP FRR requires the lower layer to fast respond to the link change so that traffic can be rapidly switched to the backup link in the case of a link failure. In such a case, if **frr-binding** is configured, the association between the BFD session status and link status is enabled on an interface. If the BFD session on the interface becomes Down, the link status changes to Down accordingly, thus implementing fast fault sensing.

You can bind a BFD session to an interface or an OSPF process. If a BFD session is bound to an interface and an OSPF process, the BFD session bound to an interface takes precedence over that bound to an OSPF process.

Precautions

- *receive-interval* is negotiated between local **min-rx-interval** and remote **min-tx-interval**, and the smaller of local **min-rx-interval** and remote **min-tx-interval** is used as the remote **min-tx-interval**. If the local end does not

receive any BFD packets within the interval of *receive-interval* × *multiplier-value* (local detection multiplier), it declares that the remote end is unreachable.

- An OSPF device sets up BFD sessions with only the neighbors in Exstart state. Two ends can set up a BFD session only when the **bfd** command is run on both ends to configure BFD globally and the **bfd all-interfaces enable** command is run.
- The **bfd all-interfaces** command and the **ospf bfd block** command are mutually exclusive.

Example

Configure BFD in an OSPF process and set the minimum interval for sending BFD packets to 400 ms.

```
<Huawei> system-view
[Huawei] ospf
[Huawei-ospf-1] bfd all-interfaces enable
[Huawei-ospf-1] bfd all-interfaces min-tx-interval 400
```

Related Topics

9.4.71 ospf bfd

9.4.72 ospf bfd block

9.4.7 default (OSPF)

Function

The **default** command configures default parameters for OSPF to import external routes. The parameters include the cost, type (Type 1 or Type 2), tag, and number of imported routes.

The **undo default** command restores the default setting.

By default, the default cost of the external routes is 1; the upper limit of the imported external routes is 2147483647; the type of the imported external routes is Type 2; the default tag value is 1.

Format

default { **cost** { *cost-value* | **inherit-metric** } | **limit** *limit* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **limit** | **tag** | **type** } *

Parameters

Parameter	Description	Value
cost *cost-value*	Specifies the default cost of the external routes imported by OSPF.	The value is an integer ranging from 0 to 16777214. By default, it is 1.

Parameter	Description	Value
inherit-metric	Indicates that the cost of the imported route is the cost carried in the route. If no cost is specified, the default cost set through the **default** command is used.	-
limit *limit*	Specifies the default upper limit of the external routes to be imported within a given period.	The value is an integer ranging from 1 to 2147483647.
tag *tag*	Specifies the tag of the external routes.	The value is an integer ranging from 0 to 4294967295. By default, it is 1.
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. By default, it is 2. ● 1: Type 1 external route ● 2: Type 2 external route

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The imported external routes carry various parameters that can change the priorities and next hops of those routes in the OSPF routing table.

By setting default parameters for OSPF to import external routes, you can change the OSPF routing policies.

The route tag is used to identify protocol-related information. For example, it can be used to differentiate AS numbers when OSPF receives BGP routes. In addition, configuring **tag** applies the OSPF routing policies to tagged routes.

Follow-up Procedure

The priority of the **default (OSPF)** command is the lowest. Thus, ensure that no other commands are configured when configuring this command. Otherwise, this command cannot take effect.

Precautions

You can run the following commands to set the cost of the imported route. The following commands are listed in the descending order of cost priorities.

- Run the **apply cost** command to set the cost of a route.
- Run the **import-route (OSPF)** command to set the cost of an imported route.
- Run the **default (OSPF)** command to set the default cost of an imported route.

Example

Set the default values of the cost, type, and tag.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] default cost 10 tag 100 type 2
```

Related Topics

9.9.7 apply cost

9.4.54 import-route (OSPF)

9.4.8 default-cost (OSPF Aera)

Function

The **default-cost** command sets the cost of the Type3 default route that is transmitted to the Stub or NSSA by OSPF.

The **undo default-cost** command restores the default setting.

By default, the cost of the Type3 default route transmitted to the Stub or NSSA is 1.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Specifies the cost of the Type3 default route transmitted to the Stub or NSSA by OSPF.	The value is an integer ranging from 0 to 16777214.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring the cost of a default route can change the selected OSPF route, improving the flexibility of networking.

This command is applicable to the area border route (ABR) to the Stub or NSSA.

Prerequisites

A default route exists in the local routing table.

Example

Set Area 1 as a Stub area, and set the cost of the Type 3 default route transmitted to this Stub area to 20.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 1
[Huawei-ospf-100-area-0.0.0.1] stub
[Huawei-ospf-100-area-0.0.0.1] default-cost 20
```

Related Topics

9.4.112 stub (OSPF area)

9.4.9 default-route-advertise (OSPF)

Function

The **default-route-advertise** command advertises default routes in a common OSPF area.

The **undo default-route-advertise** command disables advertisement of default routes in a common OSPF area.

By default, OSPF devices in a common OSPF area do not advertise default routes.

Format

default-route-advertise [[**always** | **permit-calculate-other**] | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name* [**match-any**]] *

default-route-advertise summary cost *cost*

undo default-route-advertise

Parameters

Parameter	Description	Value
always	Generates and advertises an LSA that describes a default route, regardless of whether the local device has active default routes from processes other than the non-local OSPF process. ● If **always** is configured, the router configured with the **always** parameter does not calculate the default routes from other routers. ● If **always** is not configured, an LSA for advertising a default route is generated based on activated non-OSPF default routes in the routing table of the local device. If the routing table has no such a route, the LSA cannot be generated.	-
permit-calculate-other	Generates and advertises an ASE LSA that describes the default route only when the local device has active default routes learned from the non-local OSPF process. The device still calculates the default routes from other devices. **NOTE** If neither **always** nor **permit-calculate-other** is configured, ● If the local device has active default routes from processes other than the local OSPF process, the device no longer calculates the default routes from other devices. ● If the local device does not have active default routes from processes other than the local OSPF process, the device still calculates the default routes from other devices.	-
cost *cost*	Specifies the cost of the ASE LSA.	The value is an integer that ranges from 0 to 16777214. The default value is 1.
type *type*	Specifies the type of the external routes.	The value is 1 or 2. The default value is 2. ● 1: Type 1 external route ● 2: Type 2 external route

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a routing policy. The device advertises default routes according to the parameters of the configured routing policy when there are matched default OSPF routing entries generated by other processes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
summary	Advertises the Type 3 summary LSA of the specified default route. Before specifying this parameter, ensure that VPN is enabled. Otherwise, routes cannot be advertised.	-
match-any	Indicates that a device matches the routing entry in the routing table by using a routing policy and then advertises the default route according to the parameters set through the routing policy.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **import-route (OSPF)** command cannot be used to import a default route from another AS. Running the **default-route-advertise** command on an ASBR can advertise a non-OSPF default route in a common OSPF area.

If the ASBR has a default route, the **default-route-advertise** command enables the ASBR to advertise the default route 0.0.0.0 to the OSPF area.

If the ASBR has no default route, the **default-route-advertise always** command or the **default-route-advertise** command can be used:

- With **always** configured: The ASBR can advertise the default route 0.0.0.0 even if there is no default route. This allows the default route to retain in the routing table and prevents the ASBR from using a default route sent by another device.
- Without **always** configured: The ASBR generates an LSA that describes a default route only when the local routing table contains an active default route that is not an OSPF except BGP route.

 Copyright © Huawei Technologies Co., Ltd.

If the local routing table contains an active default BGP route, the default route can be injected to the OSPF routing table based on the following situations:

- Whether the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command is run together with the **vpn-instance-capability simple** command:
  - If the two commands are executed together, to inject an active default EBGP route into the OSPF routing table, run the **default-route-advertise** command. To inject an active default IBGP route to the OSPF routing table, run the **import-route bgp permit-ibgp** command before you run the **default-route-advertise** command.
  - If only the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command is run, to inject an active default EBGP or IBGP route into the OSPF routing table, run the **default-route-advertise** command.
- If the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command is not run, to inject an active default EBGP route into the OSPF routing table, run the **default-route-advertise** command. To inject an active default IBGP route to the OSPF routing table, run the **import-route bgp permit-ibgp** command before you run the **default-route-advertise** command.

NOTICE

Injecting an IBGP route into the OSPF routing table may cause a routing loop. Exercise caution when you perform this step.

If a routing policy is configured with **match-any**, and multiple routes match the policy, a default LSA will be generated based on the optimal route. The principles for select an optimal route are as follows:

1. A route configured with **type** takes precedence over that not configured with **type**, and a route configured with a smaller **type** value takes precedence over that configured with a larger **type** value.
2. A route configured with **cost** takes precedence over that not configured with **cost**, and a route configured with a smaller **cost** value takes precedence over that configured with a larger **cost** value.
3. A route configured with **tag** takes precedence over that not configured with **tag**, and a route configured with a smaller **tag** value takes precedence over that configured with a larger **tag** value.

Prerequisites

Before advertising a default route, OSPF compares the priorities of default routes in an OSPF area and then advertises a default route with the highest priority. If a static default route is configured on an OSPF device, check that the priority of the static default route is lower than that of the default route to be advertised by OSPF. This ensures that the default route advertised by OSPF will be added to the routing table of the OSPF device.

Configuration Impact

After the **default-route-advertise** command is configured on the ASBR, the ASBR will generate a Type 5 ASE LSA with a link state ID of 0.0.0.0 and mask of 0.0.0.0. In addition, it will advertise the ASE LSA in an entire OSPF area.

If a routing policy is configured, default routes are advertised based on the following principles:

- If a default route matches the routing policy, a default route is generated on an OSPF device based on the parameters configured in the routing policy. Parameters such as **cost**, **tag**, and **type** can be configured in the routing policy.
- If the default route does not match the routing policy, and **always** is configured, the default route is still advertised.
  - If **always** is not configured, the OSPF device will not advertise the default route.
  - If **always** is configured, OSPF devices will advertise the default route. In addition, only **always** configured in the **default-route-advertise** command takes effect on advertisement of default routes.

Precautions

In different OSPF areas, OSPF advertises default routes using different modes. This **default-route-advertise** command can be used to advertise default routes in a common OSPF area. In a stub area, totally stub area, or totally NSSA, default routes are advertised automatically. In an NSSA, the **nssa default-route-advertise** command is used to advertise default routes.

Example

Advertise the ASE LSA of the default route to the OSPF area, with no default route on the local device.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] default-route-advertise always
```

Related Topics

9.4.54 import-route (OSPF)
9.4.67 nssa (OSPF Area)

9.4.10 description (OSPF)

Function

The **description** command configures the description of an OSPF process.

The **undo description** command deletes the description.

By default, there is no description of an OSPF process.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an OSPF process.	The description is a string of 1 to 80 characters.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The description of an OSPF process helps identify special processes, facilitating network maintenance.

Configuration Impact

If the **description** command is run multiple times, the latest configuration overrides the previous one.

Example

Configure the description of the OSPF process.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] description this process contains 3 areas
```

9.4.11 description (OSPF Area)

Function

The **description** command configures the description of an OSPF area.

The **undo description** command deletes the description.

By default, there is no description of an OSPF area.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an OSPF area.	The description is a string of 1 to 80 characters.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

The description of an OSPF area helps identify special areas, facilitating network maintenance.

Example

Configure the description of OSPF area 1.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 1
[Huawei-ospf-100-area-0.0.0.1] description this is a stub area
```

Related Topics

9.4.10 description (OSPF)

9.4.12 display default-parameter ospf

Function

The **display default-parameter ospf** command displays the default OSPF configuration.

Format

display default-parameter ospf

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the default OSPF configuration.

```
<Huawei> display default-parameter ospf
 Process View:
 -------------------------------------------------------
   Default Metric                          : 1
   Default Tag                             : 1
   Default Type                            : 2
   SPF Intelligent-timer Max-interval(msec)     : 10000
   SPF Intelligent-timer Start-interval(msec)   : 500
   SPF Intelligent-timer Hold-interval(msec)    : 1000
   Lsa Maxage (sec)                        : 3600
   Lsa Refresh Time(sec)                   : 1800
   Lsa Maxagediff Interval (sec)           : 900
   Minimum Lsa Arrival Interval(sec)       : 1
   Minimum Lsa Originate Interval(sec)     : 5
   Sham Link Cost                          : 1
   VPN Domain ID                           : 0
   VPN Router Tag                          : 0
   Route Preference for Internal Routes    : 10
   Route Preference for External Routes    : 150
 -------------------------------------------------------

 Area View:
 -------------------------------------------------------
   Default Stub Cost                       : 1
 -------------------------------------------------------

 Interface View:
 -------------------------------------------------------
   P2P&Broadcast Hello Interval(sec)       : 10
   P2MP&NBMA Hello Interval(sec)           : 30
   P2P&Broadcast Dead Interval(sec)        : 40
   P2MP&NBMA Dead Interval(sec)            : 120
   Poll Interval(sec)                      : 120
   Router DR Priority                      : 1
   Retransmit Interval(sec)                : 5
   Transmit Delay(sec)                     : 1
 -------------------------------------------------------
```

Table 9-24 Description of the **display default-parameter ospf** command output

Item	Description
Process View	Indicates the process view.
Default Metric	Indicates the default metric of the imported external route.
Default Tag	Indicates the default tag value of the imported external route.

Item	Description
Default Type	Indicates the default type of the imported external route.
SPF Intelligent-timer Max-interval(msec)	Indicates the default maximum interval of SPF calculation.
SPF Intelligent-timer Start-interval(msec)	Indicates the default start interval of SPF calculation.
SPF Intelligent-timer Hold-interval(msec)	Indicates the default hold interval of SPF calculation.
Lsa Maxage(sec)	Indicates the default maximum age of the LSA.
Lsa Refresh Time(sec)	Indicates the default maximum interval for generating an LSA. If the LS age of the LSAs generated by the device reaches the LSA Refresh Time, a new instance needs to be generated for the LSAs.
Lsa Maxagediff Interval(sec)	Indicates the default value difference in the MaxAge fields of LSAs. If the value difference in the MaxAge fields of two LSAs is greater than MaxAgeDiff Interval, the two LSAs are considered to belong to different instances of the same LSA.
Minimum Lsa Arrival Interval(sec)	Indicates the default minimum interval for receiving the same LSA.
Minimum Lsa Originate Interval(sec)	Indicates the default minimum interval for sending the same LSA.
Sham Link Cost	Indicates the default cost of the sham link.
VPN Domain ID	Indicates the default domain ID of the VPN.
VPN Router Tag	Indicates the default router tag of the VPN.
Route Preference for Internal Routes	Indicates the default preference of the internal route.
Route Preference for External Routes	Indicates the default preference of the external route.
Area View	Indicates the area view.
Default Stub Cost	Indicates the default cost of a stub area.
Interface View	Indicates the interface view.
P2P&Broadcast Hello Interval(sec)	Indicates the default interval for sending Hello packets on a P2P or broadcast network.
P2MP&NBMA Hello Interval(sec)	Indicates the default interval for sending Hello packets on a P2MP or NBMA network.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
P2P&Broadcast Dead Interval(sec)	Indicates the default interval for declaring a neighbor to be Down after no Hello packets are received on a P2P or broadcast network.
P2MP&NBMA Dead Interval(sec)	Indicates the default interval for declaring a neighbor to be Down after no Hello packets are received on a P2MP or NBMA network.
Poll Interval(sec)	Indicates the default interval for the local device to send Hello packets to a neighbor in the Down state on the NBMA network. The value of Poll Interval is greater than the value of Hello Interval.
Router DR Priority	Indicates the default priority of the DR.
Retransmit Interval(sec)	Indicates the default interval for retransmitting packets.
Transmit Delay(sec)	Indicates the default estimated time for transmitting an LSU packet over this interface. LSAs in the LSU packet must have their age incremented by this amount before transmission.

9.4.13 display gtsm statistics

Function

The **display gtsm statistics** command displays GTSM statistics on all LPUs.

Format

display gtsm statistics all

Parameters

Parameter	Description	Value
all	Displays GTSM statistics on all LPUs.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display gtsm statistics** command to view GTSM statistics, including the total number of BGP, BGPv6, LDP, and OSPF packets, the number of packets that have passed, and the number of discarded packets, on all LPUs.

Example

View GTSM statistics on all LPUs.

```
<Huawei> display gtsm statistics all
GTSM Statistics Table
-----------------------------------------------------------------
SlotId  Protocol  Total Counters  Drop Counters  Pass Counters
-----------------------------------------------------------------
 0      BGP       0               0              0
 0      BGPv6     0               0              0
 0      OSPF      0               0              0
 0      LDP       0               0              0
 0      OSPFv3    0               0              0
 0      RIP       0               0              0
-----------------------------------------------------------------
```

Table 9-25 Description of the display gtsm statistics command output

Item	Description
SlotId	Slot ID
Protocol	Protocol type: ● Software-based forwarding: protocol differentiated, displaying BGP, BGPv6, OSPF, LDP, OSPFv3, or RIP ● Hardware-based forwarding: protocol undifferentiated, displaying "-----"
Total Counters	Total number of packets
Drop Counters	Total number of dropped packets
Pass Counters	Total number of packets that have passed

Related Topics

9.4.98 reset gtsm statistics

9.4.14 display ospf abr-asbr

Function

The **display ospf abr-asbr** command displays information about the ABRs and ASBRs of OSPF.

Format

display ospf [*process-id*] **abr-asbr** [*router-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
router-id	Specifies the router ID of an ABR or ASBR.	In dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Area Border Router (ABR) can belong to two or more areas, and one of the areas must be a backbone area. An ABR is used to connect the backbone area and non-backbone areas. It can be physically or logically connected to the backbone area.

AS Boundary Router (ASBR) exchanges routing information with other ASs. An ASBR may not reside at the boundary of an AS. It can be an internal device or an ABR. If an OSPF device imports external routes, the device is an ASBR.

This command can view information about the ABRs and ASBRs of OSPF.

Example

Display information about the ABRs and ASBRs of OSPF.

```
<Huawei> display ospf abr-asbr

         OSPF Process 1 with Router ID 100.10.10.10
                Routing Table to ABR and ASBR

 RtType      Destination      Area      Cost  Nexthop        Type
 Intra-area  10.10.10.11      0.0.0.0   1     10.2.0.3       ABR
```

Table 9-26 Description of the **display ospf abr-asbr** command output

Item	Description
RtType	Intra-area or inter-area router
Destination	Router ID of the ABR or ASBR
Area	Area ID
Cost	Cost of the route from the local device to the ABR or ASBR
NextHop	Next hop address through which packets are transmitted to the ABR or ASBR

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Area border router (ABR) or as boundary router (ASBR)

9.4.15 display ospf asbr-summary

Function

The **display ospf asbr-summary** command displays information about OSPF route summarization.

Format

display ospf [*process-id*] **asbr-summary** [*ip-address mask*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
ip-address	Specifies the matched IP address.	It is in dotted decimal notation.
mask	Specifies the mask of the IP address. If no IP address or mask is specified, summarization information of all the imported routes is displayed.	It is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an AS is divided into areas, configuring route aggregation can reduce routing information transmitted between areas, thus reducing the size of the routing table and improving route performance.

Run **asbr-summary** command displays information about OSPF route summarization.

Example

Display summarization information about all the imported OSPF routes.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ospf asbr-summary
         OSPF Process 1 with Router ID 192.168.1.2
                  Summary Addresses
 Total summary address count: 1
                  Summary Address
 net         : 10.0.0.0
 mask         : 255.0.0.0
 tag         : 10 (Configured)
 status       : Advertise
 Cost         : 0 (Not Configured)
 delay        : 30 (Configured)
 The Count of Route is : 2
 Destination     Net Mask        Proto      Process   Type     Metric
 10.1.0.0        255.255.0.0     Static     1         2        10
 10.2.0.0        255.255.0.0     Static     1         2        10
```

Table 9-27 Description of the **display ospf asbr-summary** command output

Item	Description
Total Summary address count	Number of routes that are being summarized through the **9.4.3 asbr-summary** command
net	Network address of the summarized route
mask	Network mask of the summarized route
tag	Tag of the summarized route
status	Advertisement status of the summarized route: ● Advertise: indicates that the summarized route is advertised. ● DoNotAdvertise: indicates that the summarized route is not advertised.
Cost	Cost of the summarized route
delay	Delay for advertising the summarized route
The Count of Route is	Number of routes that are being summarized
Destination	Destination address of the routes that are being summarized
Net Mask	Mask of the routes that are being summarized
Proto	Protocol of the routes that are being summarized
Process	Process ID
Type	Type of the imported AS external route, Type 1 or Type 2
Metric	Metric of the routes that are being summarized

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.4.3 asbr-summary

9.4.16 display ospf bfd session

Function

The **display ospf bfd session** command displays information about the BFD-enabled neighbor.

Format

display ospf [*process-id*] **bfd session** *interface-type interface-number* [*router-id*]

display ospf [*process-id*] **bfd session** { *router-id* | **all** }

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the type and number of the interface.	-
router-id	Specifies the router ID of the neighbor.	In dotted decimal notation.
all	Indicates all the OSPF-enabled interfaces in the OSPF process.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In BFD for OSPF, a BFD session is associated with OSPF. The BFD session fast detects a link fault and then notifies OSPF of the fault. This speeds up OSPF's response to the change of the network topology.

The **display ospf bfd session** command displays information about the BFD-enabled neighbor.

Example

Display information about the BFD-enabled neighbor.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ospf bfd session all

         OSPF Process 1 with Router ID 10.3.3.3
 Area 0.0.0.0 interface 100.1.1.1(GigabitEthernet1/0/0)'s BFD Sessions
NeighborId:10.2.2.2          AreaId:0.0.0.0          Interface:GigabitEthernet1/0/0
BFDState:up                  rx    :1000             tx       :1000
Multiplier:3                 BFD Local Dis:8198      LocalIpAdd:10.1.1.1
RemoteIpAdd:10.1.1.2         Diagnostic Info:No diagnostic information
```

Table 9-28 Description of the **display ospf bfd session all** command output

Item	Description
NeighborId	Router ID of the neighbor
AreaId	Area ID
Interface	Interface through which the local device establishes a BFD session with the neighbor
BFDState	BFD status: ● up ● down ● unknown
rx	Negotiated minimum interval for receiving BFD packets
tx	Negotiated minimum interval for sending BFD packets
Multiplier	Remote detection multiplier
BFD Local Dis	Local discriminator dynamically assigned by BFD
LocalIpAdd	Local IP address
RemoteIpAdd	Remote IP address

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Diagnostic Info	Diagnostic information: ● Init: indicates that the BFD session is in the Initiate state. ● Admin down: indicates that the **shutdown** command is run on the local BFD session. ● BFD global disable: indicates that BFD is not enabled globally. ● BFD session number exceed: indicates that the number of BFD sessions exceeds the limit. ● Detect down: indicates that the local link becomes Down. ● Receive admin down: indicates that the remote link becomes Down. ● BFD is in rearranging: indicates that the board of the BFD session changes, and the data of the BFD session is transferred to another board. ● No diagnostic information.

9.4.17 display ospf brief

Function

The **display ospf brief** command displays OSPF brief information.

Format

display ospf [*process-id*] **brief**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, brief information about all the OSPF processes is displayed.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In addition to OSPF brief information, running this command also displays the following information:

- Configure Router ID
- Configure VPN domain ID

When locating OSPF faults, you can run the **display ospf brief** command to obtain OSPF brief information. You can then analyze OSPF faults according to the brief information.

Example

Display OSPF brief information.

```
<Huawei> display ospf brief


         OSPF Process 1 with Router ID 10.137.217.210
                OSPF Protocol Information

 RouterID: 10.137.217.210   Border Router:  AREA
 Multi-VPN-Instance is not enabled
 Global DS-TE Mode: Non-Standard IETF Mode
 Graceful-restart capability: disabled
 Helper support capability  : not configured
 Applications Supported: MPLS Traffic-Engineering Spf-schedule-interval: max 10000ms, start 500ms, hold
1000ms
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Route Preference: 10
 ASE Route Preference: 150
 SPF Computation Count: 1
 RFC 1583 Compatible
 Retransmission limitation is disabled
 Area Count: 2   Nssa Area Count: 0
 ExChange/Loading Neighbors: 0
 Process total up interface count: 1
 Process valid up interface count: 0

 Area: 0.0.0.6          (MPLS TE not enabled)
 Authtype: None   Area flag: Normal
 SPF scheduled Count: 1
 ExChange/Loading Neighbors: 0
 Router ID conflict state: Normal
 Area interface up count: 1
 Interface: 10.10.1.2 (GigabitEthernet1/0/0)
 Cost: 1       State: DR        Type: Broadcast    MTU: 1500
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
```

Table 9-29 Description of the **display ospf brief** command output

Item	Description
RouterID	Indicates the current router ID

Item	Description
Border Router	Indicates the border router: ● AS: indicates an Autonomous System Border Router (ASBR). ● AREA: indicates an Area Border Router (ABR). ● NSSA: indicates the ABR of an NSSA.
Multi-VPN-Instance is not enabled	Indicates that the current process does not support multi-VPN-instance.
Applications Supported: MPLS Traffic-Engineering	Indicates that OSPF supports Traffic Engineering (TE).
Graceful-restart capability	Indicates whether graceful restart is enabled: ● disabled: indicates that graceful restart is disabled. ● planned only: indicates that planned-GR is supported. ● un-planned: indicates that unplanned-GR is supported. ● totally: indicates that totally GR is supported. ● planned and un-planned: indicates that planned-GR and unplanned-GR are supported
Helper support capability	Indicates whether the Helper mode is enabled: ● enabled: indicates that the Helper mode is enabled. ● not configured: indicates that the Helper mode is disabled.
Spf-schedule-interval	Indicates the interval for performing SPF calculation.
Route Preference	Indicates the preference of the default route
Default ASE parameters	Indicates the default parameters of the external LSA. ● Metric: Indicates the default metric of the external LSA. ● Tag: Indicates the default tag of the external LSA. ● Type: Indicates the default type of the external LSA.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ASE Route Preference	Indicates the preference of the ASE route
SPF Computation Count	Indicates the number of times that SPF calculation is performed.
RFC 1583 Compatible	Indicates whether RFC 1583 compatibility is enabled.
Retransmission limitation is disabled	Indicates that retransmission limit is disabled.
Area Count	Indicates the number of areas in the current process.
Nssa Area Count	Indicates the number of NSSAs in the current process.
ExChange/Loading Neighbors	Number of neighbors in the Exchange state and neighbors in the Loading state.
Process total up interface count	Indicates the number of interfaces that is up.
Process valid up interface count	Indicates the number of interfaces that is valid.
Area	Indicates information about each area in the current process, including ID of the current area in dotted decimal notation.
Authtype	Indicates the area authentication type, including none-authentication, simple authentication, MD5 authentication, HMAC-SHA256 authentication, and HMAC-MD5 authentication.
Area flag	Indicates the flag used to describe the area attributes, including Transit/Vlink/Stub/Nssa/Normal.
SPF scheduled Count	Indicates the number of times that the SPF calculation is performed.
Interface	Indicates interface information in the area.
Cost	Indicates the cost of an OSPF interface.
State	Indicates the interface status, including Down, Waiting, Loopback, P-2-P, DR, and BDR DROTHER. DR and BDR DROTHER exist in only broadcast and NBMA networks, and P-2-P exists in only P2P and P2MP Vlinks.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Indicates the interface type, including P2P, broadcast, NBMA, and P2MP.
MTU	Indicates the MTU value of the interface.
Timers	Indicates the interval of the timer.
Hello	Indicates the interval of the Hello timer.
Dead	Indicates the interval of the Dead timer.
Poll	Indicates the interval of the Poll timer.
Retransmit	Indicates the interval of the Retransmit timer.
Transmit Delay	(Optional) Indicates the delay for transmitting LSAs on the interface.
Global DS-TE Mode	Indicates the globally configured DS-TE mode: ● Non-standard IETF Mode: indicates that the IETF mode is not supported. ● Standard IETF Mode: indicates that the IETF mode is supported.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Router ID conflict state	Indicates the status of the automatic recovery function. The value can be one of the following: ● Normal: the automatic recovery function is properly detecting router ID conflict. ● Wait select: the automatic recovery function delays defining a new router ID if the device starts after an unexpected delay (two hours by default). ● Selecting: the automatic recovery function restarts the OSPF process with the router ID and waits for the restarted OSPF process to take effect. ● RtrId Changed: the automatic recovery function determines whether router ID conflict occurs after the new router ID takes effect and returns to the Normal state if no new router ID conflict is detected. ● Suspend: the automatic recovery function does not define a new router ID any longer if the maximum number of conflict times is reached (three times by default).

Related Topics

9.4.69 ospf

9.4.18 display ospf cumulative

Function

The **display ospf cumulative** command displays OSPF statistics.

Format

display ospf [*process-id*] **cumulative**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, statistics of all the OSPF processes are displayed.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can help you troubleshoot OSPF faults.

Example

Display OSPF statistics.

```
<Huawei> display ospf cumulative

         OSPF Process 1 with Router ID 10.1.1.1
                Cumulations

  IO Statistics
           Type        Input     Output
          Hello           26         62
   DB Description            3          2
   Link-State Req            1          1
Link-State Update            5          5
   Link-State Ack            3          3
  ASE: 2  Checksum Sum: 233779
  LSAs originated by this router

  Router: 1
  Network: 0
  Sum-Net: 0
  Sum-Asbr: 0
  External: 3
  NSSA: 0
  Opq-Link: 0
  Opq-Area: 0
  Opq-As: 0
  LSAs Originated: 4  LSAs Received: 14

  Routing Table:
    Intra Area: 2  Inter Area: 0  ASE: 2

  Up Interface Cumulate: 2

     Neighbor Cumulate:
  ========================================================

     Neighbor cumulative data. (Process 1)
  -------------------------------------------------------
  Down:       0 Init:        0 Attempt:    0 2-Way:    0
```

```
Exstart:    0 Exchange:    0 Loading:    0 Full:     1
Retransmit Count: 0

    Neighbor cumulative data. (Total)
-------------------------------------------------------
Down:       0 Init:        0 Attempt:    0 2-Way:    0
Exstart:    0 Exchange:    0 Loading:    0 Full:     1
Retransmit Count: 0
```

Table 9-30 Description of the **display ospf cumulative** command output

Item	Description
IO Statistics	Statistics of the transmitted packets and LSAs
Type	OSPF packet type
Input	Number of received packets
Output	Number of sent packets
Hello	OSPF Hello packet
DB Description	OSPF Database Description packet
Link-State Req	OSPF Link State Request packet
Link-State Update	OSPF Link State Update packet
Link-State Ack	OSPF Link State Acknowledgement packet
Checksum Sum	Checksum of the AS external LSA
ASE	Number of ASE routes (when there are no ASE routes, Disabled is displayed)
LSAs originated by this router	Detailed statistics of the transmitted LSAs
Router	Router LSA
Network	Network LSA
Sum-Net	Type 3 summary LSA
Sum-Asbr	Type 4 summary LSA
External	AS external LSA
NSSA	NSSA
Opq-Link	Number of Type 9 Opque LSAs
Opq-Area	Number of Type 10 Opque LSAs
Opq-As	Number of Type 11 Opque LSAs
LSAs Originated	Generated LSAs
LSAs Received	Received LSAs
Routing Table	Routing table

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Intra Area	Number of intra-area routes
Inter Area	Number of inter-area routes
Up Interface Cumulate	Statistics of up state interface
Neighbor Cumulate	Statistics of neighbors
Neighbor cumulative data.	Detailed statistics of neighbors: • Down • Init • Attempt • 2-Way • Exstart • Exchange • Loading • Full
Retransmit Count	Total number of nodes in the retransmission list

Related Topics

9.4.69 ospf

9.4.19 display ospf error

Function

The **display ospf error** command displays OSPF error information.

Format

display ospf [*process-id*] **error** [**lsa** | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, error information of all OSPF processes is displayed.	The value is an integer ranging from 1 to 65535.
lsa	Display the OSPF LSA errors.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating OSPF faults, you can run the **display ospf error** command to obtain OSPF error information. You can then analyze OSPF faults according to the OSPF error information information.

Example

Display OSPF error information.

```
<Huawei> display ospf error

         OSPF Process 1 with Router ID 10.1.1.1
                OSPF error statistics

General packet errors:
 0      : IP: received my own packet     0       : Bad packet
 0      : Bad version                    0       : Bad checksum
 0      : Bad area id                    0       : Drop on unnumbered interface
 0      : Bad virtual link               0       : Bad authentication type
 0      : Bad authentication key         0       : Packet too small
 0      : Packet size > ip length        0       : Transmit error
 0      : Interface down                 0       : Unknown neighbor
 0      : Bad net segment                0       : Extern option mismatch
 0      : Router id confusion            0       : Bad authentication sequence numb

HELLO packet errors:
 0      : Netmask mismatch               0       : Hello timer mismatch
 0      : Dead timer mismatch            0       : Virtual neighbor unknown
 0      : NBMA neighbor unknown          0       : Invalid Source Address

DD packet errors:
 0      : Neighbor state low             0       : Unknown LSA type
 0      : MTU option mismatch

LS ACK packet errors:
 0      : Neighbor state low             0       : Unknown LSA type

LS REQ packet errors:
 0      : Neighbor state low             0       : Empty request
 0      : Bad request

LS UPD packet errors:
 0      : Neighbor state low             0       : Newer self-generate LSA
 0      : LSA checksum bad               0       : Received less recent LSA
 0      : Unknown LSA type

Opaque errors:
```

```
 0      : 9-out of flooding scope        0       : 10-out of flooding scope
 0      : 11-out of flooding scope       0       : Unknown TLV type

Retransmission for packet over Limitation errors:
 0      : Number for DD Packet           0       : Number for Update Packet
 0      : Number for Request Packet

Receive Grace LSA errors:
 0      : Number of invalid LSAs         0       : Number of policy failed LSAs
 0      : Number of wrong period LSAs

Configuration errors:
 0      : Tunnel cost mistake
```

Table 9-31 Description of the display ospf error command output

Item	Description
General packet errors	Indicates general packet errors.
IP: received my own packet	Indicates that the packet sent by its own interface is received.
Bad packet	Indicates that the parsed packet is incorrect, including the checksum of the length field.
Bad version	Indicates that the OSPF version is incorrect, that is, it is not version 2.
Bad checksum	Indicates that the OSPF checksum is incorrect.
Bad area id	Indicates that the area ID in the received packet does not match the local area ID. (Vlink can receive packets from only Area 0 and its own area.)
Drop on unnumbered interface	Indicates that the unnumbered rather than P2P interface receives packets (the interface must be of the P2P type).
Bad virtual link	Indicates that the Vlink receives invalid packets.
Bad authentication type	Indicates that packet authentication is incorrect.
Bad authentication key	Indicates that authentication key is incorrect.
Packet size > ip length	Indicates that the length of the OSPF packet is greater than the permitted length of the IP packet.
Bad net segment	The source address of received packets is not on the same network segment as the IP address of the interface that receives packets.
Packet too small	Indicates that the length of the received packet does not equal the sum of the IP header length and the packet length.
Transmit error	Indicates that sending packets to the socket fails.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface down	Indicates the number of times that the OSPF interface goes Down.
Unknown neighbor	Indicates that OSPF packets are received from non-OSPF neighbors on NBMA networks, virtual links, and sham links.
Extern option mismatch	Indicates that the extension attributes of the Hello packets on the two ends are inconsistent. If the value of this field keeps increasing, the area types of the two devices that establish the neighbor relationship are inconsistent (the area type of one device is common area, and the area type of the other device is stub area or NSSA). In this case, configure the same area type for the two devices (in the OSPF area view, the **stub** command indicates the area type is stub and the **stub** command indicates the area type is nssa).
HELLO packet errors	Indicates Hello packet errors.
Netmask mismatch	Indicates that the address mask does not match the local address mask.
Hello timer mismatch	Indicates that the Hello intervals on the two ends are inconsistent.
Dead timer mismatch	Indicates that the Dead intervals on the two ends are inconsistent.
Router id confusion	Indicates that the router IDs on the two ends are the same.
Bad authentication sequence numb	Indicates the number of bad authentication sequence.
Virtual neighbor unknown	Indicates that the router ID of the packet is inconsistent with that of the neighbor that is configured by the virtual link.
NBMA neighbor unknown	Indicates that the status of the NBMA neighbor is not active.
Invalid Source Address	Indicates that the source address is invalid.
DD packet errors	Indicates DD packet errors.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Neighbor state low	Indicates the following situations: ● A DD packet is received but its neighbor status is lower than 2-way. ● An LSR packet is received but its neighbor status is lower than Exchange. ● An LSU packet is received but its neighbor status is lower than Exchange. ● An LSAck packet is received but its neighbor status is lower than Exchange.
Newer self-generate LSA	Indicates the number of new self-generated LSAs. This field is reserved for future use.
MTU option mismatch	Indicates that the MTU check of the OSPF interface is enabled and the MTU of the DD packet received by the interface is greater than the MTU of the interface.
Unknown LSA type	Indicates the unknown LSA type.
LSA checksum bad	Indicates that the LSA checksum is incorrect.
LS ACK packet errors	Indicates LSAck packet errors.
LS REQ packet errors	Indicates LSR packet errors.
Empty request	Indicates empty LSR packets.
Bad request	Indicates the BadRequest event in the protocol.
LS UPD packet errors	Indicates LSU packet errors.
Received less recent LSA	Indicates that the LSA older than the local LSA is received.
Opaque errors	Indicates opaque errors.
9-out of flooding scope	Indicates the number of Type 9 LSAs that exceed the flooding scope.
10-out of flooding scope	Indicates the number of Type 10 LSAs that exceed the flooding scope.
11-out of flooding scope	Indicates the number of Type 11 LSAs that exceed the flooding scope.
Unknown TLV type	Indicates the unknown TLV type.
Retransmission for packet over Limitation errors	Indicates the number of times that retransmitting packets expires.
Number for DD Packet	Indicates the number of times that retransmitting DD packets expires.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Number for Update Packet	Indicates the number of times that retransmitting LSU packets expires.
Number for Request Packet	Indicates the number of times that retransmitting LSR packets expires.
Receive Grace LSA errors	Indicates the number of received incorrect Grace LSAs.
Number of invalid LSAs	Indicates the number of invalid LSAs.
Number of policy failed LSAs	Indicates the number of policy failed LSAs.
Number of wrong period LSAs	Indicates the number of wrong period LSAs.
Configuration errors	Indicates configuration errors.
Tunnel cost mistake	Indicates the number of times that the cost of the OSPF tunnel interface is smaller than 1. This count increases by one each time the cost of the OSPF tunnel interface is smaller than one. If the cost is smaller than one, the cost is calculated as one.

Display OSPF error information about the specified interface.

```
<Huawei> display ospf error interface gigabitethernet 1/0/0

   OSPF Process 1 with Router ID 20.1.1.1
          OSPF error statistics

 Interface: GigabitEthernet1/0/0 (1.2.0.1)
 General packet errors:
  0     : Bad version                  0     : Bad checksum
  0     : Bad area id                  0     : Bad authentication type
  0     : Bad authentication key       0     : Unknown neighbor
  0     : Bad net segment              0     : Extern option mismatch
  0     : Router id confusion

 HELLO packet errors:
  0     : Netmask mismatch             0     : Hello timer mismatch
  0     : Dead timer mismatch          0     : Invalid Source Address

 DD packet errors:
  0     : MTU option mismatch

 LS REQ packet errors:
  0     : Bad request

 LS UPD packet errors:
  0     : LSA checksum bad

 Receive Grace LSA errors:
  0     : Number of invalid LSAs       0     : Number of policy failed LSAs
  0     : Number of wrong period LSAs
```

9.4.20 display ospf global-statistics

Function

The **display ospf global-statistics** command displays global OSPF statistics. If no OSPF process ID is specified, brief information about all the OSPF processes is displayed.

Format

display ospf global-statistics { **process** *process-id* | **vpn-instance** *vpn-instance-name* | **public-instance** | **timewheel** | **brief** }

Parameters

Parameter	Description	Value
process *process-id*	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
public-instance	Displays the statistics of all the public network instances.	-
timewheel	Displays the number of updated or aged LSAs in different periods.	-
brief	Displays brief information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display global OSPF statistics, including statistics of neighbors, processes, and instances.

```
<Huawei> display ospf global-statistics brief
  Neighbor cumulative data (OSPF total statistics):
```

```
-----------------------------------------------------------
Down:              0        Init:                 0      Attempt:     0    2-Way:     0
Exstart:           0        Exchange:             0      Loading:     0    Full:   2400
Instance Number:     1        Process Number:        2
HighSocketExpire:   27       HighSocketEmpty:  526275
Total Neighbor Number:                    0
Total Press:   LOW
```

Table 9-32 Description of the display ospf global-statistics brief command output

Item	Description
Neighbor cumulative data (OSPF total statistics)	Neighbor statistics
Instance Number	Number of instances, including public network instances and VPN instances
Process Number	Number of OSPF processes running on the device
HighSocketExpire	Number of unprocessed messages in high-priority queues
HighSocketEmpty	Number of processed messages in high-priority queues
Total Neighbor Number	Total number of OSPF neighbors
Total Press	Total pressure of the current service In most cases, the Total Press field is **LOW**. If the number of retransmission timers or the number of LSAs being flooded in the OSPF processes exceeds a certain value (default 300), or the number of OSPF neighbors exceeds 300, the Total Press field is **HIGH**. If the number of retransmission timers and the number of LSAs being flooded in the OSPF processes fall below a certain value (default 300), and the number of OSPF neighbors falls below 300, the Total Press field is **LOW**.

Display global statistics of OSPF process 1.

```
<Huawei> display ospf global-statistics process 1
  OSPF 1 statistics data:
  ----------------------------------------
  LSA NUM of Flood cache:          0
  Packet NUM of FloodUpdt Hash:          0
  Packet NUM of Flood Queue:          0
```

Table 9-33 Description of the **display ospf global-statistics process 1** command output

Item	Description
LSA NUM of Flood cache	Indicates the number of LSAs being flooded in the OSPF process.
Packet NUM of FloodUpdt Hash	Indicates the number of Update packets waiting to be flooded in the OSPF process, and the number does not reach the MTU.
Packet NUM of Flood Queue	Indicates the number of Update packets waiting to be flooded in the OSPF process, and the number reaches the MTU.

Display OSPF time wheel information.

```
<Huawei> display ospf global-statistics timewheel
 ================== TimeWheel Info Begin ==================
 TimeWheel current index is 2845, datanode count is 8
 Bucket Number: 3596, Expiry time: 1306(s), Datanode Count: 0
 High expiry time: 0, Low expiry time 527742(s)
 Bucket Number: 3597, Expiry time: 1307(s), Datanode Count: 0
 High expiry time: 0, Low expiry time 527743(s)
 Bucket Number: 3598, Expiry time: 1308(s), Datanode Count: 0
```

Table 9-34 Description of the **display ospf global-statistics timewheel** command output

Item	Description
TimeWheel current index	Indicates the current index of the time wheel.
Datanode Count	Indicates the total number of nodes in the time wheel.
Bucket Number	Indicates the total number of indexes of the time wheel.
Expiry time	Indicates the expiry time of the index.
High expiry time	Indicates the high expiry time corresponding to the index in the time wheel after the system starts.
Low expiry time	Indicates the low expiry time corresponding to the index in the time wheel after the system starts.

Related Topics

9.4.18 display ospf cumulative

9.4.21 display ospf graceful-restart

Function

The **display ospf graceful-restart** command displays the status of OSPF GR.

Format

display ospf [*process-id*] **graceful-restart** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about OSPF GR.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ospf graceful-restart** command to view details of the GR and the statistics.

Example

Display OSPF GR information.

```
<Huawei> display ospf graceful-restart

         OSPF Process 1 with Router ID 10.1.1.1
 Graceful-restart capability     : enabled
 Graceful-restart support        : planned and un-planned, totally
 Helper-policy support           : planned and un-planned, strict lsa check
 Current GR state                : normal
 Graceful-restart period         : 120 seconds

 Number of neighbors under helper:
  Normal neighbors    : 0
  Virtual neighbors   : 0
  Sham-link neighbors : 0
  Total neighbors     : 0

 Number of restarting neighbors : 0

 Last exit reason:
  On graceful restart : successful exit
  On Helper           : none
```

Display detailed information about OSPF GR.

```
<Huawei> display ospf graceful-restart verbose

         OSPF Process 1 with Router ID 10.1.1.1
 Graceful-restart capability      : enabled
 Graceful-restart support         : planned and un-planned, totally
 Helper-policy support            : planned and un-planned, strict lsa check
 Current GR state                 : normal
 Graceful-restart period          : 120 seconds

 Number of neighbors under helper:
  Normal neighbors    : 0
  Virtual neighbors   : 0
  Sham-link neighbors : 0
  Total neighbors     : 0
 Number of restarting neighbors : 0

 Last exit reason:
  On graceful restart : successful exit
  On Helper           : none

 All area count      : 1

                Area ID    : 0.0.0.0

 Authtype       : None     Area flag : Normal

 Normal interface count: 1

 Interface: 10.1.1.1 (GigabitEthernet1/0/0)
 GR state : normal                 State: P-2-P          Type: P2P
 Last Helper Exit reason: none
 Neighbor count of this interface : 1

 Neighbor          IP address        GR state    Last Helper Exit reason
 10.2.2.2          10.1.1.2          Normal      none
```

Table 9-35 Description of the **display ospf graceful-restart** command output

Item	Description
Graceful-restart capability	Whether IETF GR is enabled: ● enabled ● disabled
Graceful-restart support	IETF GR mode that is supported currently: ● planned: indicates that only planned-GR is supported. ● planned and un-planned: indicates that both planned GR and unplanned GR are supported. ● totally: indicates that totally GR is supported. ● partial: indicates that partial GR is supported.

Item	Description
Helper-policy support	Policy that supports the Helper: ● planned: indicates that the Helper supports only planned GR. ● planned and un-planned: indicates the Helper supports both planned GR and unplanned GR. ● strict lsa check: indicates that the Helper supports strict external LSA check. ● ignore external lsa check: indicates that the Helper does not check external LSAs. ● never: indicates that the device does not support the Helper mode.
Current GR state	Current GR status: ● Normal: indicates that GR is in the Normal state. ● Under GR: indicates that the device enters the Restarter mode. ● Under Helper: indicates that the device enters the Helper mode.
Graceful-restart period	GR period
Number of neighbors under helper	Number of neighbors in the Helper state: ● Normal neighbors: indicates the number of normal neighbors. ● Virtual neighbors: indicates the number of virtual neighbors. ● Sham-link neighbors: indicates the number of sham link neighbors. ● Total neighbors: indicates the total number of neighbors.
Number of restarting neighbors	Number of restarted devices displayed on the Helper
Last exit reason	Reason that a device exits from GR last time: ● On graceful restart: indicates the reason that the Restarter exits from GR. ● On Helper: indicates the reason that the Helper exits from GR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
On graceful restart	Reason that the Restarter exits from GR: ● 1-way hello received: indicates that 1-way Hello packets are received. ● back-link check failed: indicates that the back link check fails. ● DR election fail: indicates that DR election fails. ● grace period expired: indicates that the GR period expires. ● interface state change: indicates that the interface state machine changes. ● none: indicates that the device never performs GR since startup. ● successful exit: indicates that the Restarter successfully exits from GR. ● two Grace-LSAs received: indicates that two Grace LSAs are received.
On Helper	Reason that the Helper exits from GR: ● flooding change LSA: indicates that the changed LSAs are received. ● grace period expired: indicates that the GR period expires. ● graceful restart unconfigured at process level: indicates that the GR function of the OSPF process is disabled. ● interface state change: indicates that the interface state machine changes. ● policy check failed for received grace LSA: indicates the policy that mismatches the Helper. ● received 1-way hello packet: indicates that 1-way Hello packets are received. ● received flushed grace LSA: indicates that flushed Grace LSAs are received. ● received multiple grace LSA: indicates that multiple Grace LSAs are received. ● neighbor reset: indicates that GR is disabled when neighbors are in the Helper mode. ● none: indicates that the device never enters the Helper mode since startup. ● successful exit: indicates that the Helper successfully exits from GR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
All area count	Number of areas in the process
Area ID	Area ID
Authtype	Authentication type
Area flag	Area attributes: ● Normal ● NSSA ● Stub
Normal interface count	Number of interfaces in the area
Interface	IP address of the interface
GR state	GR status of the interface: ● Normal: indicates that the device is in the Normal state. ● Restarter: indicates that the device enters the Restarter mode. ● Helper: indicates that the device enters the Helper mode.
State	Interface status: ● P-2-P ● DR ● BDR ● DROther ● Waiting ● Down
Type	Interface type: ● P2P ● P2MP ● NBMA ● Broadcast

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last Helper Exit reason	Reason that the neighbor exits from the Helper mode the last time: ● none: indicates that the device never enters the Helper mode since startup. ● successful exit: indicates that the neighbor successfully exits from the Helper mode. ● grace period expired: indicates that the GR period expires. ● received flushed grace LSA: indicates that flushed Grace LSAs are received. ● flooding change LSA: indicates that the changed LSAs are received. ● received multiple grace LSA: indicates that multiple Grace LSAs are received. ● received 1-way hello packet: indicates that 1-way Hello packets are received. ● policy check failed for received grace LSA: indicates the policy that mismatches the Helper. ● neighbor reset: indicates that the network topology changes after the **reset** command is run on the neighbor of the Helper. ● interface state change: indicates that the interface state machine changes. ● graceful restart unconfigured at process level: indicates that the neighbor is not configured with the GR function.
Neighbor count of this interface	Total number of neighbors of this interface
Neighbor	Router ID of the neighbor
IP address	IP address of the neighboring interface
GR state	GR status of the neighbor: ● Normal: indicates that the neighbor is in the Normal state. ● Restarter: indicates that the neighbor enters the Restarter mode. ● Helper: indicates that the neighbor enters the Helper mode.

 Copyright © Huawei Technologies Co., Ltd.

9.4.22 display ospf interface

Function

The **display ospf interface** command displays information about OSPF interfaces.

Format

display ospf [*process-id*] **interface** [**all** | *interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
all	Displays information about all OSPF interfaces.	-
interface-type interface-number	Specifies the interface type and the interface number.	-
verbose	Display verbose configuration information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ospf interface** command output displays the configuration and operating status of OSPF, which facilitate fault location and configuration verification.

Example

Display OSPF interface information.

```
<Huawei> display ospf interface

         OSPF Process 1 with Router ID 192.168.1.1
                Interfaces

 Area: 0.0.0.0        (MPLS TE not enabled)
 IP Address      Type         State    Cost  Pri   DR              BDR
 192.168.1.2     Broadcast    DR        1     1    192.168.1.2     192.168.1.3

 Area: 0.0.0.1        (MPLS TE not enabled)
```

```
IP Address      Type         State    Cost  Pri   DR              BDR
172.16.0.1      Broadcast    DR        1     1    172.16.0.1      172.16.0.2
```

Display information about the specified OSPF interface.

```
<Huawei> display ospf interface gigabitethernet 1/0/0

         OSPF Process 1 with Router ID 1.1.1.1
                Interfaces

 Interface: 192.168.1.1 ( gigabitethernet 1/0/0 )
 Cost: 1       State: DR        Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 192.168.1.2
 Backup Designated Router: 192.168.1.3
 Timers: Hello 10 , Dead 40 , Poll  120 , Retransmit 5 , Transmit Delay 1
  IO Statistics
            Type        Input     Output
           Hello       161367      10436
 DB Description             18         18
 Link-State Req              5          6
 Link-State Update       203780        210
 Link-State Ack           90411        276
 ALLSPF GROUP
 ALLDR GROUP
 OpaqueId: 1    PrevState: BDR
 Effective cost: 1, enabled by OSPF Protocol.
 Suppress flapping peer: enable(flapping-count: 0, threshold: 20)
```

Table 9-36 Description of the **display ospf interface** command output

Item	Description
Area	ID of the area to which the interface belongs
IP address	IP address of the interface (regardless of whether TE is enabled on the interface)
Type	Interface type: P2P, PTMP, broadcast, or NBMA

Item	Description
State	Status of the interface, which is determined by the OSPF interface state machines ● Down: The status of the interface is Down. If an interface is Down, the interface is unavailable and cannot be used to transmit traffic. ● Loopback: The interface connecting to the network on the device is in the Loopback state. The loopback interface cannot be used to transmit data but can collect interface information by performing the ICMP ping operation or bit error detection. ● Waiting: The device is determining the DR and BDR on the network. The DR or BDR election mechanism should not be implemented until the waiting period ends. This prevents unnecessary changes in the DR and BDR roles. ● P-2-P: The interface is connected to the P2P network or a virtual link. ● DROther: The device itself is not elected as the DR or BDR. Instead, another device connecting to the broadcast network or NBMA network is elected as the DR. The device starts to set up adjacency with the DR and BDR (if existing). ● BDR: The device functions as the BDR on the network, and will turn into a DR when the current DR fails. The device sets up adjacency with other devices that access the network. ● DR: The device functions as the DR on the network. The device sets up adjacency with other devices that access the network.
Cost	Cost of the interface
Pri	Priority of the device interface during the DR and BDR election The greater the value, the higher the priority.
DR	DR of the network where the interface resides
BDR	BDR of the network where the interface resides
Interface	Interface IP address + interface number + IP address of the neighbor, which is used for P2P
MTU	MTU value of the interface

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Priority	Priority of the device interface during the DR and BDR election The greater the value, the higher the priority. The value is an integer ranging from 0 to 255.
Designated Router	DR of the network where the interface resides
Backup Designated Router	BDR of the network where the interface resides
Timer Hello	Interval for sending Hello packets
Dead	Dead time of devices
Poll	Interval for sending Poll packets
Retransmit	Interval for retransmitting LSAs
Transmit Delay	Interface transmission delay

 Copyright © Huawei Technologies Co., Ltd.

Item	Description

Suppress flapping peer	Status of OSPF neighbor relationship flapping suppression:
	• enable: OSPF neighbor relationship flapping suppression is enabled.
	  – flapping-count: number of valid flapping_events
	  If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count increases by 1. To change *detecting-interval*, run the **ospf suppress-flapping peer detecting-interval** *detecting-interval* command.
	  – threshold: flapping suppression threshold
	  When the flapping_count reaches or exceeds **threshold**, flapping suppression takes effect. To configure the threshold, run the **ospf suppress-flapping peer threshold** *threshold* command.
	• disable: OSPF neighbor relationship flapping suppression is disabled. In this case, the following information is displayed, without flapping-count or threshold:
	`Suppress flapping peer: disable`
	• hold-down: OSPF neighbor relationship flapping suppression works in Hold-down mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-down(start: 2016-01-02 09:58:41, remain-interval: 476 sec)`
	  – start: time when the flapping suppression started
	  – remain-interval: remaining time of the flapping suppression
	• hold-max-cost: OSPF neighbor relationship flapping suppression works in Hold-max-cost mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-max-cost(start: 2016-01-02 09:58:41, remain-interval: 476 sec)`

Related Topics

9.4.69 ospf

9.4.23 display ospf lsdb

Function

The **display ospf lsdb** command displays the OSPF Link-State Database (LSDB).

Format

display ospf [*process-id*] **lsdb** [**brief**]

display ospf [*process-id*] **lsdb** [{ **router** | **network** | **summary** | **asbr** | **ase** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as** } [*link-state-id*]] [**originate-router** [*advertising-router-id*] | **self-originate**] [**age** { **min-value** *min-age-value* | **max-value** *max-age-value* } *]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
brief	Displays brief information about the LSDB.	-
router	Displays information about the device LSA.	-
network	Displays information about the network LSA.	-
summary	Displays information about the network summary LSA.	-
asbr	Displays information about the ASBR summary LSA.	-
ase	Displays information about the AS external LSA.	-
nssa	Displays information about the status of external links in the NSSA.	-
opaque-link	Displays information about the opaque link LSA.	-
opaque-area	Displays information about the opaque area LSA.	-
opaque-as	Displays information about the opaque AS LSA.	-
originate-router	Displays the LSA of the advertising router.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
link-state-id	Specifies the ID of an LSA.	The value is an IP address in dotted decimal notation.
advertising-router-id	Specifies the Router ID of the device that advertises the LSA.	The value is an IP address in dotted decimal notation.
self-originate	Displays information about the self-originated LSA.	-
age	Displays the LSAs that meet the age filtering rule.	-
min-value *min-age-value*	Displays information about only LASs with the **age** value greater than or equal to the *min-age-value* value.	The value is an integer ranging from 0 to 3600.
max-value *max-age-value*	Displays information only about LASs with the **age** value less than or equal to the *max-age-value* value.	The value is an integer ranging from 0 to 3600.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By running the **display ospf lsdb** command displays information about the LSDB in various modes. That is, you can view any of the following:

- Brief information about the LSDB
- LSAs of a specified type
- LSAs of the originating device
- Locally originated LSAs

The command output can display information about the OSPF LSDB, which helps you troubleshoot OSPF faults.

Example

Display brief information about the OSPF LSDB.

```
<Huawei> display ospf lsdb
         OSPF Process 1 with Router ID 10.1.1.1
                Link State Database

                        Area: 0.0.0.0
 Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
 Router    10.2.2.2        10.2.2.2           98  36    8000000B       1
 Router    10.1.1.1        10.1.1.1           92  36    80000005       1
```

```
Network   10.1.1.2      10.2.2.2        98  32   80000004      0
Sum-Net   10.1.1.0      10.2.2.2       286  28   80000001      1
Sum-Net   10.1.1.0      10.1.1.1       282  28   80000001      1
Sum-Asbr  10.2.2.2      10.1.1.1        61  28   80000001      1
```

Table 9-37 Description of the display ospf lsdb command output

Item	Description
Area	Area whose LSDB information needs to be displayed
Type	LSA type: Router, Network, Sum-Net, Sum-Asbr, NSSA, External, Opq-Link, Opq-Area, and Opq-As
LinkState ID	Link State ID in the LSA header
AdvRouter	Device that advertises or generates LSAs
Age	Aging time of the LSA
Len	Size of the LSA
Sequence	Sequence number in the LSA header
Metric	Metric

Display brief information about the OSPF LSDB.

```
<Huawei> display ospf lsdb brief
        OSPF Process 123 with Router ID 192.168.200.183
                LS Database Statistics

 Area ID        Stub   Router   Network  S-Net   S-ASBR   Type-7   | Subtotal
 0.0.0.0         0      0        0        0       0        0        | 0
 Total           0      0        0        0       0        0        |
 ---------------------------------------------------------------------+---------
 Area ID        Opq-9  Opq-10                                        | Subtotal
 0.0.0.0         0      0                                            | 0
 Total           0      0                                            |
 ---------------------------------------------------------------------+---------
                ASE    Opq-11                                        | Subtotal
 Total           0      0                                            | 0
 ---------------------------------------------------------------------+---------
                                                                     | Total
                                                                     | 0
```

Table 9-38 Description of the display ospf lsdb brief command output

Item	Description
Area ID	Area ID whose LSDB information needs to be displayed
Stub	The stub area that displays the LSDB information
Router	Device that advertises or generates LSAs

Item	Description
Network	Network that advertises or generates LSAs
S-Net	System Network that advertises or generates LSAs
S-ASBR	S-ASBR that advertises or generates LSAs
Type-7	LSA type
Subtotal	Total number of stub areas

Display information about router LSAs in the LSDB.

```
<Huawei> display ospf lsdb router

         OSPF Process 1 with Router ID 10.137.217.208
                     Area: 0.0.0.1
               Link State Database


  Type      : Router
  Ls id     : 10.137.217.210
  Adv rtr   : 10.137.217.210
  Ls age    : 1564
  Len       : 36
  Options   :  ABR  E
  seq#      : 80000003
  chksum    : 0xeb06
  Link count: 1
   * Link ID: 192.168.4.1
     Data   : 192.168.4.2
     Link Type: TransNet
     Metric : 1

  Type      : Router
  Ls id     : 10.137.217.208
  Adv rtr   : 10.137.217.208
  Ls age    : 1556
  Len       : 36
  Options   :  E
  seq#      : 80000005
  chksum    : 0xf6fe
  Link count: 1
   * Link ID: 192.168.4.1
     Data   : 192.168.4.1
     Link Type: TransNet
     Metric : 1
     Priority : Medium
```

Table 9-39 Description of the display ospf lsdb router command output

Item	Description
Ls id	Link State ID in the LSA header
Adv rtr	The device that advertises or generates LSAs

Item	Description
Ls age	Aging time of the LSA
Options	Indicates the Options field as below: ● E: allows Flood AS-external-LSAs. ● MC: forwards IP multicast packets. ● N/P: processes Type-7 LSAs. ● DC: processes the required links.
seq#	Sequence number, which is used to check the order of LSAs
Chksum	LSA checksum
Link count	Number of links
* Link ID	Link ID of the router LSA, which is classified according to the link type ● If the type of link is Point-to-Point, Link ID indicates the router id of neighbor. ● If the type of link is TransNet, Link ID indicates IP address of DR. ● If the type of link is Stub, Link ID indicates IP address. ● If the type of link is Virtual Link, Link ID indicates the router id of neighbor.
Data	Link data of the router LSA ● If the type of link is Point-to-Point, TransNet, or Virtual Link, Data indicates IP address. ● If the type of link is Stub, Data indicates mask of IP address.
Link Type	Link type of the router LSA: P-2-P, TransNet, StubNet, or Virtual
Metric	Link metric of the router LSA
Priority	OSPF convergence priority

Display information about network LSAs in the LSDB.

```
<Huawei> display ospf 1 lsdb network 10.1.1.1

         OSPF Process 1 with Router ID 10.1.1.1
                     Area: 0.0.0.0
               Link State Database

 Type      : Network
 Ls id     : 10.1.1.1
```

```
Adv rtr   : 10.1.1.1
Ls age    : 167
Len       : 32
Options   :  E
seq#      : 80000002
chksum    : 0x3408
Net mask  : 255.255.255.0
Priority  : Low
Attached Router    10.2.2.2
Attached Router    10.1.1.1
```

Table 9-40 Description of the display ospf lsdb network command output

Item	Description
Net mask	Network mask of the network LSA
Attached Router	Device that is connected to the network

Display information about network summary LSAs in the LSDB.

```
<Huawei> display ospf 1 lsdb summary 10.20.1.0

        OSPF Process 1 with Router ID 10.1.1.1
                 Area: 0.0.0.0
               Link State Database

 Type      : Sum-Net
 Ls id     : 10.1.1.0
 Adv rtr   : 10.2.2.2
 Ls age    : 419
 Len       : 28
 Options   :  E
 seq#      : 80000001
 chksum    : 0x1d21
 Net mask  : 255.255.255.0
 Tos 0  metric: 1
 Priority  : Medium
```

Table 9-41 Description of the display ospf lsdb summary command output

Item	Description
Net mask	Network mask of the network summary LSA
Tos	Type of service of the network summary LSA
Metric	Metric or cost of the route from the advertising router to the network, which is carried in the network summary LSA

Display information about ASBR summary LSAs in the LSDB.

```
<Huawei> display ospf 1 lsdb asbr 10.2.2.2

        OSPF Process 1 with Router ID 10.1.1.1
                 Area: 0.0.0.2
               Link State Database
```

```
Type      : Sum-Asbr
Ls id     : 10.2.2.2
Adv rtr   : 10.1.1.1
Ls age    : 90
Len       : 28
Options   :  E
seq#      : 80000001
chksum    : 0xec62
Tos 0  metric: 1
```

Display information about AS external LSAs in the LSDB.

```
<Huawei> display ospf 100 lsdb ase 10.1.1.0

        OSPF Process 1 with Router ID 10.1.1.1
                Link State Database

Type      : External
Ls id     : 10.1.1.0
Adv rtr   : 10.2.2.2
Ls age    : 569
Len       : 36
Options   :  E
seq#      : 80000002
chksum    : 0x90d0
Net mask  : 255.255.255.0
TOS 0  Metric: 1
E type    : 2
Forwarding Address : 0.0.0.0
Tag       : 1
Priority  : Medium
```

Table 9-42 Description of the display ospf lsdb ase command output

Item	Description
Net mask	Network mask of the ASE or NSSA LSA
Tos	Type of service of the ASE or NSSA LSA
Metric	Metric or cost of the route from the advertising router to the network, which is carried in the ASE or NSSA LSA
E type	E type of the ASE or NSSA LSA
Forwarding Address	Forwarding address of the ASE or NSSA LSA
Tag	32-bit tag, which is carried in ASE or NSSA LSA to avoid routing loops

Display information about NSSA external LSAs in the LSDB.

```
<Huawei> display ospf 1 lsdb nssa 192.168.1.0

        OSPF Process 1 with Router ID 10.1.1.1
                Area: 0.0.0.1
                Link State Database

Type      : NSSA
Ls id     : 10.1.1.0
Adv rtr   : 10.2.2.2
```

```
 Ls age    : 521
 Len       : 36
 Options   : None
 seq#      : 80000005
 chksum    : 0x9ea7
 Net mask  : 255.255.255.0
 TOS 0  Metric: 1
 E type    : 2
 Forwarding Address : 10.1.1.2
 Tag       : 1
 Priority  : Medium
```

Display information about Opaque-link LSAs in the LSDB.

```
<Huawei> display ospf 1 lsdb opaque-link

         OSPF Process 1 with Router ID 10.1.1.1
                  Area: 0.0.0.0
                Link State Database
 Link State Database for interface 10.1.1.1 (Vlanif200) Type: Broadcast

 Type      : Opq-Link
 Ls id     : 10.0.0.0
 Adv rtr   : 10.2.2.2
 Ls age    : 12
 Len       : 44
 Options   :  E
 seq#      : 80000001
 chksum    : 0x9579
        Opaque type : 3, Opaque ID : 0
        Grace LSA TLV information:
        Grace Period        : 1800
        GR reason           : 1
        IP address          : 10.1.1.2
```

Table 9-43 Description of the display ospf lsdb opaque-link command output

Item	Description
Opaque Type	Opaque-link LSA
Opaque ID	Opaque ID of an Opaque-link LSA (Link state ID in the LSA header consists of Opaque type and Opaque ID.)
Grace LSA TLV information:	GR information
Grace Period	GR waiting period
GR reason	Cause of GR ● 0: unknown ● 1: software ● 2: upgrade ● 3: switchover
IP address	Address of the interface that performs GR on the router

Display information about Opaque-area LSAs in the LSDB.

```
<Huawei> display ospf 1 lsdb opaque-area
```

```
OSPF Process 1 with Router ID 10.1.1.1
Area: 0.0.0.0
                 Link State Database
  Type      : Opq-Area
  Ls id     : 10.0.0.1
  Adv rtr   : 10.1.1.1
  Ls age    : 639
  Len       : 200
  Options   :  E
  seq#      : 80000001
  chksum    : 0x2175
  Opaque Type: 1
  Opaque Id: 1
  Opaque lsa information:

    00 02 00 b0 00 01 00 01 02 00 00 00 00 02 00 04
    0a 01 01 01 00 03 00 04 0a 01 01 01 00 04 00 04
    00 00 00 00 00 05 00 04 00 00 00 01 80 02 00 04
    00 00 00 01 00 06 00 04 00 00 00 00 00 07 00 04
    00 00 00 00 80 00 00 04 00 00 00 00 00 09 00 04
    00 00 00 00 00 08 00 20 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 80 01 00 20 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
    00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 09
    00 00 00 00 00 00 00 00 00 00 00 00 00 0c 00 04
    00 01 00 01
```

Related Topics

9.4.69 ospf

9.4.24 display ospf migp-routing

Function

The **display ospf migp-routing** command displays OSPF Multicast IGP (MIGP) routing information.

Format

display ospf [*process-id*] **migp-routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
ip-address	Specifies the IP address.	In dotted decimal notation.
mask	Specifies the subnet mask.	In dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and the number of the interface.	-
nexthop *nexthop-address*	Displays the route with the specified next hop IP address.	In dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When multicast and MPLS TE tunnels are configured on the network, and the TE tunnels are configured with IGP Shortcut, the outbound interface that an IGP calculated for a route may be not a physical interface but a TE tunnel interface. Based on a unicast route to a multicast source address, a router can send a Join message through a TE tunnel interface. In this case, devices spanned by the TE tunnel cannot detect the Join message so that they do not create any multicast forwarding entry.

To solve this problem, you can run the **local-mt enable** command to configure local multicast topology (MT). MT allows multicast routing entries to be created correctly.

If local MT is enabled, and the outbound interface of the calculated route is a TE tunnel interface of IGP Shortcut type, the route management (RM) module creates a separate Multicast IGP (MIGP) routing table for the multicast protocol, calculates the physical outbound interface of the route, and adds the IP address of the physical outbound interface to the MIGP routing table.

Running the **display ospf migp-routing** command can view the physical outbound interface of the route with the outbound interface of the TE tunnel interface. The physical outbound interface is OSPF routing information in the MIGP routing table.

Precautions

- Local MT supports only OSPF processes of public network instances.
- Local MT does not support forwarding adjacency (FA).

Example

Display OSPF MIGP routing information.

```
<Huawei> display ospf migp-routing

         OSPF Process 1 with Router ID 10.2.2.2
```

```
                MIGP Routing Tables

Routing for Network
Destination        Cost  Type       NextHop        AdvRouter       Area
192.168.3.0/24      4     Stub       10.0.1.1       10.5.5.5        0.0.0.0
10.0.3.0/24         3     Transit    10.0.1.1       10.5.5.5        0.0.0.0

Total Nets: 4
Intra Area: 4  Inter Area: 0  ASE: 0  NSSA: 0
```

Table 9-44 Description of the display ospf migp-routing command output

Item	Description
Destination	Indicates the destination IP address.
Cost	Indicates the cost of the route to the destination address.
Type	Router types are as follows: ● Inter-area: Indicates routes between areas. ● Stub: indicates routes within an area, including routes advertised based on router LSAs, and direct routes to non-broadcast and non-NBMA networks. ● Transit: indicates routes within an area, including routes advertised based on network LSAs.
NextHop	Indicates the next hop address to the destination address.
AdvRouter	Indicates the advertising router.
Area	Indicates the area ID.
Total Nets	Indicates the total number of networks in an area, between areas, in ASE areas, and in NSSAs.
Intra Area	Indicates the total number of intra-area routes (that is, stub routes and transit routes).
Inter Area	Indicates the total number of inter-area routes.
ASE	Indicates the total number of routes in the ASE area.
NSSA	Indicates the total number of routes in the NSSA.

Display OSPF MIGP routing information with the specified next hop address.

```
<Huawei> display ospf migp-routing nexthop 10.0.1.1
```

```
        OSPF Process 1 with Router ID 10.2.2.2

Destination : 192.168.3.0/24
AdverRouter : 10.5.5.5              Area      : 0.0.0.0
Cost        : 4                     Type      : Stub
NextHop     : 10.0.1.1              Interface : Vlanif10
Priority    : Low

Destination : 10.4.4.4/32
AdverRouter : 10.4.4.4              Area      : 0.0.0.0
Cost        : 3                     Type      : Stub
NextHop     : 10.0.1.1              Interface : Vlanif20
Priority    : Medium
```

Table 9-45 Description of the display ospf migp-routing nexthop command output

Item	Description
Priority	Indicates OSPF convergence priorities: ● Critical: indicates that the convergence priority of OSPF routes is critical. ● High: indicates that the convergence priority of OSPF routes is high. ● Medium: indicates that the convergence priority of OSPF routes is medium. ● Low: indicates that the convergence priority of OSPF routes is low.

9.4.25 display ospf mesh-group

Function

The **display ospf mesh-group** command displays brief information about OSPF mesh groups.

Format

display ospf [*process-id*] **mesh-group** [**brief**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no process ID is specified, brief information about mesh groups in all OSPF processes is displayed.	The value is an integer ranging from 1 to 65535.
brief	Displays brief information about mesh groups in each OSPF area.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When concurrent links exist between a router and its neighbor, run the **mesh-group enable** command to enable the mesh group function and identify the mesh group using the router ID of the router. When receiving LSAs, the router will select a main link to flood LSAs. The link interface does not flood reversely. This avoid repeated flooding, reducing link load and saving resources.

Running the **display ospf mesh-group** command can view brief information about mesh groups in a specified process in an OSPF area.

Example

Display brief information about OSPF mesh groups.

```
<Huawei> display ospf mesh-group

        OSPF Process 1 with Router ID 1.1.1.1
               Mesh-Groups

 Area: 0.0.0.0
      Mesh-Group ID: 2.2.2.2
        Interface                    IP Address/Mask              Nbr State
        GigabitEthernet1/0/0               192.168.4.1/24               Full

      Count of Interface in this Mesh-Group: 1

      Count of Mesh-Group in this Area: 1
```

Table 9-46 Description of the **display ospf mesh-group** command output

Item	Description
Area	OSPF area
Mesh-Group ID	Key ID of a mesh group, namely, the router ID of a neighbor
Interface	Interface enabled with the mesh-group feature
IP Address/Mask	IP address and mask of the interface enabled with the mesh-group feature
Nbr State	Neighbor status on the interface enabled with the mesh-group feature
Count of Interface in this Mesh-Group	Number of interfaces in the mesh group

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Count of Mesh-Group in this Area	Number of mesh groups in the area

Related Topics

9.4.64 mesh-group enable

9.4.26 display ospf nexthop

Function

The **display ospf nexthop** command displays OSPF next hop information.

Format

display ospf [*process-id*] **nexthop**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can display information about all the OSPF next hops, which helps you troubleshoot OSPF faults.

Example

Display OSPF next hop information.

```
<Huawei> display ospf nexthop
             OSPF Process 100 with Router ID 10.0.0.1
                    Routing Nexthop information
Next hops:
Address         Type      Refcount  IntfAddr       Intf Name
-----------------------------------------------------------------------
10.0.0.1        Local     3         10.0.0.1       GigabitEthernet1/0/0
10.0.0.2        Local     5         10.0.0.1       GigabitEthernet1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 9-47 Description of the **display ospf nexthop** command output

Item	Description
Next hops	Detailed information about the next hop.
Address	Address of the next hop.
Type	Type of the route passing through the next hop. Local indicates that the route is destined for the local network segment.
Refcount	Number of OSPF routes that use the next hop.
IntfAddr	IP address of the interface.
Intf Name	Name of the interface.

Related Topics

9.4.69 ospf

9.4.27 display ospf peer

Function

The **display ospf peer** command displays information about neighbors in each OSPF area.

Format

display ospf [*process-id*] **peer** [[*interface-type interface-number*] [*neighbor-id*] | **brief** | **last-nbr-down**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the interface type and the interface number.	-
neighbor-id	Specifies the neighbor's Router ID.	It is in dotted decimal notation.
brief	Displays brief information about neighbors in each OSPF area.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
last-nbr-down	Displays brief information about the last neighbor that goes Down in the OSPF area.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can display information about OSPF neighbors, and help you troubleshoot OSPF faults, verify the configurations of OSPF neighbors, and check whether the neighbor performs Graceful Restart (GR).

Example

Display information about the OSPF neighbor.

```
<Huawei> display ospf peer

         OSPF Process 1 with Router ID 10.1.0.5
                Neighbors

 Area 0.0.0.0 interface 10.1.0.17(GigabitEthernet1/0/0)'s neighbors
 Router ID: 10.1.1.1          Address: 10.1.0.18          GR State: Normal
   State: Full  Mode:Nbr is Slave  Priority: 1
   DR: 10.1.0.18  BDR: 10.1.0.17   MTU: 0
   Dead timer due in 35  sec
   Retrans timer interval: 5
   Neighbor is up for 00:00:05
   Authentication Sequence: [ 0 ]
```

Table 9-48 Description of the display ospf peer command output

Item	Description
Area	Area to which the neighbor belongs
interface	Interface that connects to the neighbor
Router ID	Router ID of the neighbor
Address	Address of the neighboring interface

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GR State	GR status after OSPF GR is enabled: ● Normal: indicates that a router is in the Normal state and does not perform GR. ● Doing GR: indicates that a router is performing GR. ● Complete GR: indicates that a router finishes GR. ● Helper: indicates that the neighbor is the Helper when a router is performing GR.
State	Neighbor status: ● Down: It is the initial status of the neighbor, indicating that the neighbor does not receive any information. On an NBMA network, when the neighbor is in the Down state, Hello packets can still be transmitted at the poll interval, which is longer than the Hello interval. ● Attempt: It exists only on an NBMA network, indicating that two ends are attempting to establish the neighbor relationship. The interval for sending Hello packets is the Hello interval, which is shorter than the poll interval. ● Init: It indicates that the Hello packet has been received from the neighbor. ● 2-Way: It indicates that the Hello packet has been received from the neighbor, and the neighbor list of the Hello packet contains the local Router ID. That is, the two ends can interwork. ● ExStart: It is the first step of establishing adjacencies. In this step, the master and slave relationship and DD sequence number are negotiated. ● Exchange: It indicates that the LSDBs start to be synchronized. In this process, DD packets, LSR packets, and LSU packets are exchanged. ● Loading: It indicates that the LSDBs are being synchronized. In this process, LSR packets and LSU packets are exchanged. ● Full: It indicates that the LSDB of the neighbor is already synchronized, and the Full adjacency is established between both ends.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Master or slave in the process of exchanging DD packets: ● Nbr is Master: indicates that the neighbor is the master and actively sends DD packets. ● Nbr is Slave: indicates that the neighbor is the slave and cooperates with the master to send DD packets.
Priority	Priority of the neighboring device
DR	Designated router
BDR	Backup designated router
MTU	MTU value of the neighboring interface
Dead timer due in 35 sec	The dead timer due in 35 seconds
Retrans timer interval	Interval for retransmitting LSAs, in seconds
Neighbor is up for	Time before an OSPF neighbor relationship is established
Authentication Sequence	Authentication sequence number

Display brief information about OSPF neighbors.

```
<Huawei> display ospf 1 peer brief

         OSPF Process 1 with Router ID 1.1.1.1
                  Peer Statistic Information
 ----------------------------------------------------------------------
 Area Id          Interface                    Neighbor id      State
 0.0.0.0          GigabitEthernet1/0/0         3.3.3.3          Full
 ----------------------------------------------------------------------
 Total Peer(s):      1
```

Table 9-49 Description of the display ospf peer brief command output

Item	Description
Area Id	Area to which the neighbor belongs
Interface	Interface that connects to the neighbor
Neighbor id	Router ID of the neighbor
State	State of the neighbor

Display information about the OSPF neighbor that goes Down for the last time.

```
<Huawei> display ospf 1 peer last-nbr-down

         OSPF Process 1 with Router ID 10.1.1.1

                    Last Down OSPF Peer

        Neighbor Ip Address : 20.2.1.2
        Neighbor Area Id    : 0.0.0.0
        Neighbor Router Id  : 2.2.2.2
        Interface           : GigabitEthernet1/0/0
        Immediate Reason    : Neighbor Down Due to Kill Neighbor
        Primary Reason      : Logical Interface State Change
        Down Time           : 2012-09-14 17:17:7
```

Table 9-50 Description of the display ospf peer last-nbr-down command output

Item	Description
Neighbor Ip Address	Address of the neighboring interface
Neighbor Area Id	Area to which the neighbor belongs
Neighbor Router Id	Router ID of the neighbor
Interface	Interface that connects to the neighbor
Immediate Reason	Immediate reason that the neighbor goes Down: ● Neighbor Down Due to Inactivity: indicates that the inactivity timer times out. ● Neighbor Down Due to LL Down: indicates that the link is Down. For example, the interface goes Down from Up or the IP address of the link is deleted. ● Neighbor Down Due to Kill Neighbor: indicates that the kill neighbor event is generated on the neighbor state machine. ● Neighbor Down Due to 1-Wayhello: indicates that the neighbor goes Down because it receives a 1-way packet. ● Received: indicates that the AdjOK? event is generated on this interface. ● Neighbor Down Due to SequenceNum Mismatch: indicates that the SequenceNum Mismatch event is generated on the neighbor state machine. ● Neighbor Down Due to BadLSreq: indicates that the BadLSreq event is generated on the neighbor state machine.

Item	Description
Primary Reason	Primary reason that the neighbor goes Down: • Hello Not Seen: indicates that no Hello packet is received. • Interface Parameter Mismatch: indicates that the parameters set on both ends of the link do not match. • Logical Interface State Change: indicates that the status of the logical interface changes. • Physical Interface State Change: indicates that the status of the physical interface changes. • OSPF Process Reset: indicates that the OSPF process restarts. • Area reset: indicates that the area restarts because the area type changes. • Area Option Mis-match: indicates that the area options of the interfaces on both ends of the link do not match. • Vlink Peer Not Reachable: indicates that the neighbor on the virtual link is not reachable. • Sham-Link Unreachable: indicates that the neighbor on the sham link is not reachable. • Undo Network Command: indicates that the **network** command is deleted. • Undo NBMA Peer: indicates that the neighbor configuration on the NBMA interface is deleted. • Passive Interface Down: indicates that the neighbor relationship goes Down because the **silent-interface** command is configured on the local interface. • Opaque Capability Enabled: indicates that Opaque capability is enabled. • Opaque Capability Disabled: indicates that Opaque capability is disabled. • Virtual Interface State Change: indicates that the status of a virtual link interface changes. • BFD Session Down: indicates that the BFD session goes Down. • Down Retransmission Limit Exceed: indicates that the number of retransmission times reaches the limit. • 1-Wayhello Received: indicates that the device receives 1-way hello packets. • Router State Change from DR or BDR to DROTHER: indicates that the interface state machine changes to DROTHER from DR or BDR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Neighbor State Change from DR or BDR to DROTHER: indicates that the neighbor state machine changes to DROTHER from DR or BDR. • NSSA Area Configure Change: indicates that the configuration of the NSSA area changes. • Stub Area Configure Change: indicates that the configuration of the Stub area changes. • Received Invalid DD Packet: indicates that invalid DD packets are received. • Not Received DD during RouterDeadInterval: indicates that no DD packet is received during the time when the Dead timer starts. • M,I,MS bit or SequenceNum Incorrect: indicates that the M, I, and MS bits do not comply with specifications in the protocol. • Unable Opaque Capability,Find 9,10,11 Type Lsa: indicates that Type9, Type10, and Type11 LSAs are received and Opaque capability is disabled. • Not NSSA,Find 7 Type Lsa in Summary List: indicates that this area is not an NSSA area and Type7 LSAs are found in the summary table. • LSrequest Packet,Unknown Reason: indicates that LSR packets are received with the reason unknown. • NSSA or STUB Area,Find 5 ,11 Type Lsa: indicates that this area is an NSSA or Stub area and Type5 and Type11 LSAs are found. • LSrequest Packet,Request Lsa is Not in the Lsdb: indicates that the neighbor sends an LSR to this process or area to request an LSA and this LSA does not exist in the LSDB of this process. • LSrequest Packet, exist same lsa in the Lsdb: indicates that this process receives an LSA that is same as that in the LSDB and the LSA is found in the request list of the neighbor. • LSrequest Packet, exist newer lsa in the Lsdb: indicates that this process receives a new LSA that exists in the local LSDB and the LSA is found in the request list of the neighbor. • Neighbor state was not full when LSDB overflow: indicates that the LSDB overflows and the neighbor state machine is not Full. • Filter LSA configuration change: indicates that the configuration of LSA filter changes. • ACL changed for Filter LSA: indicates that the ACL configuration of LSA filter changes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Reset Ospf Peer: indicates that the OSPF neighbor is restarted.
Down Time	Time when the neighbor goes Down

Related Topics

9.4.95 peer (OSPF)

9.4.28 display ospf request-queue

Function

The **display ospf request-queue** command displays the OSPF request list.

Format

display ospf [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies the interface type and number.	-
neighbor-id	Specifies the neighbor's Router ID.	It is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can help you troubleshoot OSPF faults.

Example

Display the OSPF request list.

```
<Huawei> display ospf request-queue
```

```
OSPF Process 1 with Router ID 10.1.1.1
OSPF Request List
 The Router's Neighbor is Router ID 10.4.4.4        Address 172.16.4.2
 Interface 172.16.4.1        Area 0.0.0.2
 Request list:
     Type       LinkState ID      AdvRouter         Sequence   Age
     Router     10.1.1.1          10.1.1.1          8000001b   677
```

Table 9-51 Description of the display ospf request-queue command output

Item	Description
The Router's Neighbor is Router ID	Router ID of the neighbor
Address	IP address of the neighboring interface
Interface	IP address of the interface
Area	Area to which the local device belongs
Request list	Request list
Type	LSA type: Router LSA, network LSA, network summary LSA, ASBR summary LSA, AS external LSA, NSSA LSA, and opaque LSA
LinkState ID	Link state ID in the LSA header
AdvRouter	Advertising router in the LSA header
Sequence	Sequence number in the LSA header
Age	Aging time in the LSA header

9.4.29 display ospf retrans-queue

Function

The **display ospf retrans-queue** command displays the OSPF retransmission list.

Format

display ospf [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*] [**low-level-of-retrans-times-range** *min-time*] [**high-level-of-retrans-times-range** *max-time*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number.	-
neighbor-id	Specifies the neighbor's Router ID.	It is in dotted decimal notation.
low-level-of-retrans-times-range *min-time*	Min value of LSA retrans timers range.	The value is an integer ranging from 0 to 65535.
high-level-of-retrans-times-range *max-time*	Max value of LSA retrans timers range.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can help you troubleshoot OSPF faults.

Example

Display the OSPF retransmission list.

```
<Huawei> display ospf retrans-queue

        OSPF Process 1 with Router ID 10.1.1.1
                OSPF Retransmit List

 The Router's Neighbor is Router ID 10.2.2.2  Address 192.168.0.2
 Interface 192.168.0.1       Area 0.0.0.0
 Retransmit list:
     Type       LinkState ID      AdvRouter          Sequence   Age
     Router      10.1.1.1          10.1.1.1          80000002   533
```

Table 9-52 Description of the display ospf retrans-queue command output

Item	Description
The Router's Neighbor	Basic information about the neighboring router
Router ID	Router ID of the neighbor
Address	IP address of the neighboring interface
Interface	IP address of the interface
Area	Area ID
Retransmit list	Retransmission list

Item	Description
Type	LSA type Router LSA, network LSA, network summary LSA, ASBR summary LSA, AS external LSA, NSSA LSA, and opaque LSA
LinkState ID	Link state ID in the LSA header
AdvRouter	Advertising router in the LSA header
Sequence	Sequence number in the LSA header
Age	Aging time in the LSA header

9.4.30 display ospf routing

Function

The **display ospf routing** command displays the OSPF routing table.

Format

display ospf [*process-id*] **routing router-id** [*router-id*]

display ospf [*process-id*] **routing** [*ip-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
router-id *router-id*	Specifies the router ID of a destination router.	The value is in dotted decimal notation.
ip-address	Specifies the IP address.	The value is in dotted decimal notation.
mask	Specifies the subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
interface *interface-type interface-number*	Specifies the type and number of the interface.	-
nexthop *nexthop-address*	Displays the route with the specified next hop IP address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By using this command with different parameters, you can view the routes of a specified interface or next hop.

The command output can help you troubleshoot OSPF faults.

Example

Display the OSPF routing table.

```
<Huawei> display ospf routing
        OSPF Process 1 with Router ID 10.2.2.9
                Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter       Area
 10.12.12.0/24       1    Transit    10.12.12.10     10.2.2.9        0.0.0.1
 10.13.13.0/24       1    Stub       10.13.13.1      10.2.2.9        0.0.0.0
 10.11.11.0/24       2    Transit    10.12.12.11     10.0.0.1        0.0.0.1

 Routing for ASEs
 Destination        Cost      Type       Tag      NextHop         AdvRouter
 10.0.0.0/8          1         Type2      1        10.12.12.11     10.0.0.1

 Total Nets: 4
 Intra Area: 3  Inter Area: 0  ASE: 1  NSSA: 0
```

Table 9-53 Description of the display ospf routing command output

Item	Description
Destination	Destination network
Cost	Cost of the route to the destination address
Type	Type of the destination network: ● Inter-area: indicates inter-area routes. ● Intra-area: indicates intra-area routes. – Stub: indicates the routes advertised by router LSAs, which correspond to the direct routes of non-broadcast and non-NBMA networks. – Transit: indicates the routes advertised by network LSAs.
NextHop	Next hop address to the destination address
AdvRouter	Device that advertises LSAs
Area	Area ID

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tag	Tag of the external route
Total Nets	Total number of networks in an area, between areas, in ASE areas, and in NSSAs.
Intra Area	Total number of intra-area networks (that is, stub networks and transit networks)
Inter Area	Total number of inter-area networks
ASE	Total number of networks in the ASE area
NSSA	Total number of networks in the NSSA

Related Topics

9.4.69 ospf

9.4.31 display ospf sham-link

Function

The **display ospf sham-link** command displays the sham links of the OSPF area.

If no OSPF process ID or area ID is specified, all sham links are displayed.

Format

display ospf [*process-id*] **sham-link** [**area** *area-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the ID of an OSPF area.	The value is an integer ranging from 0 to 4294967295 or in the IPv4 address format.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display all OSPF sham links.

```
<Huawei> display ospf sham-link
         OSPF Process 100 with Router ID 10.1.1.2
 Sham Link:
 Area       NeighborId     Source-IP     Destination-IP   State   Cost
 0.0.0.1    10.1.1.2       10.3.3.3      10.5.5.5         P-2-P   10
```

Display the OSPF sham link of Area 1.

```
<Huawei> display ospf sham-link area 1
         OSPF Process 100 with Router ID 10.1.1.2
  Sham-Link: 10.3.3.3 --> 10.5.5.5
  Neighbor ID: 10.1.1.2,    State: Full
  Area: 0.0.0.1
  Cost: 10  State: P-2-P, Type: Sham
  Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 9-54 Description of the **display ospf sham-link** command output

Item	Description
Area	OSPF area that the sham link belongs to
NeighborId	Neighbor ID of the router
Source-IP	Source IP address of the sham link
Destination-IP	Destination IP address of the sham link
State	Interface status of the sham link (P-2-P indicates the point-to-point link.)
Cost	Cost of the sham link
Type	Connection type
Timers	Information about the following items: the interval for sending Hello messages, Dead time, restransmission interval, and transmission delay on the interface

9.4.32 display ospf spf-statistics

Function

The **display ospf spf-statistics** command displays route calculation statistics in OSPF processes.

Format

display ospf [*process-id*] **spf-statistics** [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, brief information about route calculation statistics in all processes is displayed.	The value is an integer ranging from 1 to 65535.
verbose	Displays detailed information about route calculation statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ospf spf-statistics** command displays route calculation statistics in OSPF processes, including the time when route calculation occurs, cause of route calculation, and number of changed routes.

When identifying the cause of OSPF route flapping, you can run this command to obtain OSPF route calculation statistics, and then identify the cause according to the command output.

Example

Display brief information about route calculation statistics in OSPF process 1.

```
<Huawei> display ospf 1 spf-statistics

          OSPF Process 1 with Router ID 10.2.2.2
Routing table change statistics:
Date        Time        Intra     Inter    External    Reason
2008-08-14  10:17:16    17        17       17          LSA
2008-08-14  09:16:47    77        62       127         Other
2008-08-14  08:16:37    0         0        0           LSA
2008-08-14  07:04:40    24        230      108         LSA
2008-08-14  06:03:15    204       230      18          Other
2008-08-14  05:02:55    34        236      128         LSA
2008-08-14  04:01:49    54        130      158         LSA
2008-08-14  03:01:48    44        220      138         LSA
2008-08-14  02:01:43    22        233      158         LSA
2008-08-14  01:00:53    977       897      907         LSA
```

Table 9-55 Description of the **display ospf spf-statistics** command output

Item	Description
Date	Date when route calculation occurs
Time	Time when route calculation occurs
Intra	Number of intra-area routes in the routing table, which are changed because of route calculation
Inter	Number of inter-area routes in the routing table, which are changed because of route calculation
External	Number of external routes in the routing table, which are changed because of route calculation
Reason	Cause of route calculation: ● LSA: indicates that route calculation is caused by LSAs. ● Other: indicates that route calculation is caused by other causes. For example, the configuration changes; or the interface goes Down.

Display detailed information about route calculation statistics in OSPF process 1.

```
<Huawei> display ospf 1 spf-statistics verbose

        OSPF Process 1 with Router ID 10.10.10.2
Routing table change statistics:
Index: 1
        Time     : 2008-11-29,17:36:59
        Intra    : 0 Added,0 Deleted, 0 Modified
        Inter    : 0 Added,0 Deleted, 0 Modified
        External : 10 Added,0 Deleted, 0 Modified
        The reason of calculation is:LSA
        NO.    Type        LS ID          Adv Router
        1      External    10.1.5.0       10.10.10.1
        2      External    10.1.3.0       10.10.10.1
        3      External    10.1.9.0       10.10.10.1
        4      External    10.1.4.0       10.10.10.1
        5      External    10.1.2.0       10.10.10.1
        6      External    10.1.8.0       10.10.10.1
        7      External    10.1.7.0       10.10.10.1
        8      External    10.1.6.0       10.10.10.1
        9      External    10.1.10.0      10.10.10.1
        10     External    10.1.1.0       10.10.10.1
```

Table 9-56 Description of the **display ospf spf-statistics verbose** command output

Item	Description
Time	Date and time when route calculation occurs
Intra	Number of intra-area routes in the routing table, which are added, modified and deleted because of route calculation.

Item	Description
Inter	Number of inter-area routes in the routing table, which are added, modified and deleted because of route calculation.
External	Number of external routes in the routing table, which are added, modified and deleted because of route calculation.
The reason of calculation is	Cause of route calculation: ● LSA: indicates that route calculation is caused by LSAs. ● Other: indicates that route calculation is caused by other causes. For example, the configuration changes; or the interface goes Down.
NO.	Sequence number of the LSA that causes route calculation, which ranges from 1 to 10
Type	Type of the LSA that causes route calculation, including Router, Network, Sum-Net, External, and NSSA
LS ID	Link state ID of the LSA that causes route calculation
Adv Router	Router ID of the router that generates the LSA that causes route calculation

9.4.33 display ospf statistics updated-lsa

Function

The **display ospf statistics updated-lsa** command displays the frequent updates of the LSAs that the LSDB receives.

Format

display ospf [*process-id*] **statistics updated-lsa** [**originate-router** *advertising-router-id* | **history**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If no OSPF process ID is specified, this command displays brief information about the route calculation statistics in all processes.	The value is an integer ranging from 1 to 65535.
originate-router	Specifies the link status of the advertising router.	-
advertising-router-id	Specifies the ID of the advertising router.	In dotted decimal notation
history	Specifies the update history of LSAs that the LSDB receives.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display ospf statistics updated-lsa** command is used to display the frequent updates of LSAs, facilitating the location of the cause for a routing flapping.

- If the **history** parameter is not configured, the **display ospf statistics updated-lsa** command only displays the updates of LSAs within the latest hour.
- If the **history** parameter is configured, the **display ospf statistics updated-lsa** command displays the update history of LSAs within the last 24 hours.

Precautions

- If you run the **reset ospf process** command to restart the OSPF process, the real-time and historical statistics on the process will be cleared.
- The **display ospf statistics updated-lsa** command is used only to display the frequent updates of LSAs. The updated LSAs are compared with the LSAs in the local LSDB, and those with the **age** greater than 900 will not be displayed except those with the **age** of 3600.

Example

Display the LSA updates within the last one hour.

```
<Huawei> display ospf statistics updated-lsa
```

```
        OSPF Process 1 with Router ID 10.1.1.1
            Statistics of Received LSAs

Begin time: 11:37:32/2011/04/25

AdvRouter          Total       Updated at
10.1.1.1           18          11:37:40/2011/04/25
10.2.2.2           5           11:37:40/2011/04/25
10.3.3.3           5           11:37:41/2011/04/25
10.4.4.4           5           11:37:41/2011/04/25
10.5.5.5           2           11:37:40/2011/04/25
10.6.6.6           3           11:37:40/2011/04/25
10.7.7.7           5           11:37:40/2011/04/25
10.8.8.8           6           11:37:41/2011/04/25
```

Table 9-57 Description of the **display ospf statistics updated-lsa** command output

Item	Description
Begin time	Start time of collecting statistics
AdvRouter	Advertising router
Total	Total update times of LSAs
Updated at	Latest update time

Display the LSA updates of the specified advertising router.

```
<Huawei> display ospf statistics updated-lsa originate-router 10.1.1.1

        OSPF Process 1 with Router ID 10.2.2.2
            Statistics of Received LSAs

Begin time: 2011-04-25 11:37:32

AdvRouter      : 10.1.1.1
Total          : 6                 Updated at      : 2011-04-25 11:37:41
Router(1)      : 3                   Network(2)      : 2
Summary-Net(3) : 0                     Summary-Asbr(4) : 0
External(5)    : 1                 nssa(7)         : 0
Opaque-link(9) : 0                   Opaque-area(10) : 0
Opaque-AS(11)  : 0
```

Table 9-58 Description of the **display ospf statistics updated-lsa originate-router** command output

Item	Description
Router(1)	Update times of Router LSAs
Network(2)	Update times of Network LSAs
Summary-Net(3)	Update times of Network Summary LSAs
Summary-Asbr(4)	Update times of ASBR Summary LSAs
External(5)	Update times of AS External LSAs

Item	Description
nssa(7)	Update times of Type7 LSAs
Opaque-link(9)	Update times of Type9 LSAs
Opaque-area(10)	Update times of Type10 LSAs
Opaque-AS(11)	Update times of Type11 LSAs

Display the update history of LSAs.

```
<Huawei> display ospf statistics updated-lsa history

        OSPF Process 1 with Router ID 10.1.1.1
        History Information for Received LSAs

 Record  1:
 Begin time: 2011-04-25 11:39:32
 End time  : 2011-04-25 11:41:32

 no Record

 Record  2:
 Begin time: 2011-04-25 11:37:32
 End time  : 2011-04-25 11:39:32

 AdvRouter      : 10.1.1.1          Total           : 18
 Router(1)      : 0                 Network(2)      : 0
 Summary-Net(3) : 0                 Summary-Asbr(4) : 18
 External(5)    : 0                 nssa(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0

 AdvRouter      : 10.2.2.2          Total           : 5
 Router(1)      : 3                 Network(2)      : 2
 Summary-Net(3) : 0                 Summary-Asbr(4) : 0
 External(5)    : 0                 nssa(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0

 AdvRouter      : 10.3.3.3          Total           : 5
 Router(1)      : 3                 Network(2)      : 2
 Summary-Net(3) : 0                 Summary-Asbr(4) : 0
 External(5)    : 0                 nssa(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0

 AdvRouter      : 10.4.4.4          Total           : 5
 Router(1)      : 2                 Network(2)      : 2
 Summary-Net(3) : 0                 Summary-Asbr(4) : 0
 External(5)    : 1                 nssa(7)         : 0
 Opaque-link(9) : 0                 Opaque-area(10) : 0
 Opaque-AS(11)  : 0
```

Table 9-59 Description of the **display ospf statistics updated-lsa history** command output

Item	Description
Record	Record number

Item	Description
End time	End time of collecting statistics

9.4.34 display ospf vlink

Function

The **display ospf vlink** command displays OSPF virtual links.

Format

display ospf [*process-id*] **vlink**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output can help you troubleshoot OSPF faults.

Example

Display OSPF virtual links.

```
<Huawei> display ospf vlink
         OSPF Process 1 with Router ID 10.1.1.1
                 Virtual Links
 Virtual-link Neighbor-id  -> 10.2.2.2, Neighbor-State: Full
 Interface: 10.1.1.1 (GigabitEthernet1/0/0)
 Cost: 1  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
 GR State: Normal
```

Table 9-60 Description of the **display ospf vlink** command output

Item	Description
Virtual-link Neighbor-id	ID of the neighboring router that is connected through the virtual link
Neighbor-State	Neighbor status, such as Down, Init, 2-Way, ExStart, Exchange, Loading, and Full
Interface	Information about interfaces in the area, that is, IP address and name of the primary interface (If the interface is a serial interface, **Unknown** is displayed.)
Cost	Cost
State	Interface status
Type	Interface type
Transit Area	Transit area ID if the current interface is a virtual link
Timers	Information about the following items: the interval for sending Hello messages, Dead time, retransmission interval, and transmission delay on the interface
GR State	GR status: • Normal: indicates that a router is in the Normal state and does not perform GR. • Doing GR: indicates that a router is performing GR. • Complete GR: indicates that a router finishes GR. • Helper: indicates that the neighbor is the Helper when a router is performing GR.

Related Topics

9.4.115 vlink-peer (OSPF area)

9.4.35 display snmp-agent trap feature-name ospf all

Function

The **display snmp-agent trap feature-name ospf all** command displays all trap messages of the OSPF module.

Format

display snmp-agent trap feature-name ospf all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display all trap messages of the OSPF module.

```
<Huawei> display snmp-agent trap feature-name ospf all
-----------------------------------------------------------------------------
Feature name: OSPF

Trap number : 24
-----------------------------------------------------------------------------
Trap name                          Default switch status   Current switch status
ospfIfStateChange                        off                     off
ospfVirtIfStateChange                    off                     off
ospfNbrStateChange                       off                     off
ospfVirtNbrStateChange                   off                     off
ospfIfAuthFailure                        off                     off
ospfVirtIfAuthFailure                    off                     off
ospfIfRxBadPacket                        off                     off
ospfVirtIfRxBadPacket                    off                     off
ospfLsdbOverflow                         off                     off
ospfLsdbApproachingOverflow              off                     off
ospfRestartStatusChange                  off                     off
ospfNbrRestartHelperStatusChange         off                     off
ospfVirtNbrRestartHelperStatusChange     off                     off
ospfNssaTranslatorStatusChange           off                     off
ospfIfConfigError                        off                     off
ospfVirtIfConfigError                    off                     off
ospfTxRetransmit                         off                     off
ospfVirtIfTxRetransmit                   off                     off
ospfOriginateLsa                         off                     off
ospfMaxAgeLsa                            off                     off
hwOspfv2IntraAreaRouteridConflict        on                      on
hwOspfv2IntraAreaDRIpAddressConflict     on                      on
hwOspfv2IntraAreaRouterIdConflictRecovered  on                   on
hwOspfv2PeerFlappingSuppressStatusChange    off                  off
```

Table 9-61 Description of the **display snmp-agent trap feature-name ospf all** command output

Item	Description
Feature name	Name of the feature
Trap number	Number of traps

Item	Description
Trap name	Name of the trap: • **ospfIfStateChange**: It is sent when the interface status changes. • **ospfVirtIfStateChange**: It is sent when the status of the interface on the virtual link changes. • **ospfNbrStateChange**: It is sent when the neighbor status changes. • **ospfVirtNbrStateChange**: It is sent when the status of the neighbor on the virtual link changes. • **ospfIfAuthFailure**: It is sent when interface authentication fails. • **ospfVirtIfAuthFailure**: It is sent when the authentication of the interface on the virtual link fails. • **ospfIfRxBadPacket**: It is sent when a bad packet is received on the interface. • **ospfVirtIfRxBadPacket**: It is sent when a bad packet is received on the interface on the virtual link. • **ospfLsdbOverflow**: It is sent when the LSDB overflows. • **ospfLsdbApproachingOverflow**: It is sent when the LSDB is about to overflow. • **ospfRestartStatusChange**: It is sent when the GR Restarter status changes. • **ospfNbrRestartHelperStatusChange**: It is sent when the GR Helper status changes. • **ospfVirtNbrRestartHelperStatusChange**: It is sent when the GR Helper status of the neighbor on the virtual link changes. • **ospfNssaTranslatorStatusChange**: It is sent when the status of the NSSA device that translates Type 7 LSAs into Type 5 LSAs changes. • **ospfIfConfigError**: It is sent when the interface configuration is incorrect. • **ospfVirtIfConfigError**: It is sent when the configuration of the interface on the virtual link is incorrect. • **ospfTxRetransmit**: It is sent when packets are retransmitted.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• **ospfVirtIfTxRetransmit**: It is sent when packets are retransmitted on the interface on the virtual link. • **ospfOriginateLsa**: It is sent when local LSAs are generated. • **ospfMaxAgeLsa**: It is sent when Max Age LSAs are generated. • **hwOspfv2IntraAreaDRIpAddressConflict**: It is sent when IP addresses of DRs in an OSPF area conflict. • **hwOspfv2IntraAreaRouteridConflict**: It is sent when router ID conflict was detected in an OSPF area. • **hwOspfv2IntraAreaRouterIdConflictRecovered**: It is sent when the router ID conflict was resolved in an OSPF area. • **hwOspfv2PeerFlappingSuppressStatusChange**: It is sent when OSPF neighbor flapping suppression status changed.
Default switch status	Status of the default trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.
Current switch status	Status of the current trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

9.4.110 snmp-agent trap enable feature-name ospf

9.4.36 dn-bit-set

Function

The **dn-bit-set disable** command disables OSPF from setting the DN bit in LSAs.

The **undo dn-bit-set disable** command enables OSPF to set the DN bit in LSAs.

By default, OSPF is enabled to set the DN bit in LSAs.

 Copyright © Huawei Technologies Co., Ltd.

Format

dn-bit-set disable { **summary** | **ase** | **nssa** }

undo dn-bit-set disable { **summary** | **ase** | **nssa** }

Parameters

Parameter	Description	Value
summary	Specifies that the DN bit is not set in summary LSAs.	-
ase	Specifies that the DN bit is not set in ASE LSAs.	-
nssa	Specifies that the DN bit is not set in NSSA LSAs.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dn-bit-set disable** command can be used in the following scenarios:

- In the VPN option A scenario, the local PE imports BGP routes to generate LASs and advertise the generated LASs to the peer PE. Setting of the DN bit is restricted. The peer PE may fail to calculate a route. In this situation, the **dn-bit-set disable** command can be used to set the DN bit on or remove the setting of the DN bit from the local PE.
- When a PE is connected to an MCE, the MCE needs to calculate routes advertised by the PE. By default, the MCE does not check the DN bit. In this situation, the **dn-bit-set disable** command can be used to set the DN bit on or remove the setting of the DN bit from the local PE.

NOTE

To prevent routing loops, the OSPF multi-instance process uses a bit as a flag. The bit is called DN bit.

Configuration Impact

When the **dn-bit-set disable** command is used to disable OSPF from setting the DN bit in LSAs, routing loops may occur. If the parameter **ase** or **nssa** is specified, the DN bit in ASE LSAs or NSSA LSAs is not set. You can use the **route-tag** command to set the same tag value to prevent routing loops. Therefore, it is recommended that the **dn-bit-set disable** command be used in only the scenarios specified in **Usage Scenario**.

If the **dn-bit-set disable ase** command is configured, the DN bit is not set in type 5 LSAs that are converted from type 7 LSAs even if the DN bit is set in type 7 LSAs.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The **dn-bit-set disable** command can be configured for only private OSPF processes. The configuration of this command takes effect only on the PEs.

The **dn-bit-check disable** command can be used to control whether OSPF running on the peer PE checks the DN bit when calculating routes.

Example

Disable OSPF from setting the DN bit in ASE LSAs.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] route-distinguisher 100:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] ospf 100 vpn-instance huawei
[Huawei-ospf-100] dn-bit-set disable ase
```

Related Topics

9.4.105 route-tag

9.4.37 dn-bit-check

9.4.37 dn-bit-check

Function

The **dn-bit-check disable** command disables OSPF from checking the DN bit in LSAs.

The **undo dn-bit-check disable** command enables OSPF to check the DN bit in LSAs.

By default, OSPF is enabled to check the DN bit in LSAs.

Format

dn-bit-check disable { **summary** [**router-id** *router-id*] | **ase** | **nssa** }

undo dn-bit-check disable { **summary** [**router-id** *router-id*] | **ase** | **nssa** }

Parameters

Parameter	Description	Value
summary	Specifies that the DN bit in summary LSAs is not checked.	-
router-id *router-id*	Specifies the ID of a device on which the DN bit in summary LSAs is checked.	-
ase	Specifies that the DN bit in ASE LSAs is not checked.	-
nssa	Specifies that the DN bit in NSSA LSAs is not checked.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the VPN option A scenario, the local PE imports BGP routes to generate LSAs and advertise the generated LSAs to the peer PE. Setting of the DN bit is restricted. The peer PE may fail to calculate a route. In this situation, you need to use the **dn-bit-check disable** command to disable OSPF from checking the DN bit in LSAs.

NOTE

To prevent routing loops, the OSPF multi-instance process uses a bit as a flag. The bit is called DN bit.

Configuration Impact

When the **dn-bit-check disable** command is run, routing loops may occur. If the parameter **ase** or **nssa** is specified, the DN bit in ASE LSAs or NSSA LSAs is not checked. You can use the **route-tag** command to set the same tag value to prevent routing loops. Therefore, run the **dn-bit-check disable** command only in the scenario specified in **Usage Scenario**.

Precautions

When a PE is connected to an MCE, the MCE does not check the DN bit by default.

The **dn-bit-check disable** command can be configured only for private OSPF processes. The configuration of this command takes effect only on the PEs.

In this scenario, you can run the **dn-bit-set disable** command to set the DN bit on or remove the setting of the DN bit from the local PE.

Example

Disable OSPF from checking the DN bit in Summary LSAs.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] route-distinguisher 100:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] ospf 100 vpn-instance huawei
[Huawei-ospf-100] dn-bit-check disable summary router-id 10.1.1.1
```

Related Topics

9.4.105 route-tag
9.4.36 dn-bit-set

9.4.38 domain-id (OSPF)

Function

The **domain-id** command sets the ID for an OSPF domain.

The **undo domain-id** command restores the default setting.

By default, the domain ID is null.

Format

domain-id { **null** | *domain-id* [**type** *type* **value** *value* | **secondary**] * }

undo domain-id [*domain-id* [**type** *type* **value** *value*]]

Parameters

Parameter	Description	Value
domain-id	Specifies the ID of an OSPF domain.	The domain ID can be an integer or in dotted decimal notation. ● If it is an integer, the value ranges from 0 to 4294967295, and it is converted to dotted decimal notation when the ID is displayed. ● If it is in dotted decimal notation, it is displayed as entered.
null	Indicates that the OSPF domain ID is null.	-
type *type*	Specifies the type of the OSPF domain ID.	It can be 0005, 0105, 0205, or 8005. By default, it is 0005.
value *value*	Specifies the value of the type of the OSPF domain ID.	The value is a hexadecimal number that ranges from 0x0 to 0xffff, and the default value is 0x0.
secondary	Indicates the ID of a secondary domain.	The maximum number of **domain-id secondary** in each OSPF process is 1000.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Domain IDs are used to identify domains.

If the local OSPF area and an OSPF area of a remote VPN attempt to exchange Type 3 LSAs, the two areas must be in the same OSPF domain. You can run the **domain-id** command to configure the same domain ID for the two OSPF areas.

The routes that are imported from a PE router are advertised using External-LSAs. The routes destined for different nodes in the same OSPF domain are advertised based on Type 3 LSAs. This requires that the nodes in the same OSPF domain be configured with the same domain ID.

If the **undo domain-id** command without any parameter is executed, the primary domain ID will be deleted.

NOTE

OSPF direct routes to the PE do not carry the domain ID, while BGP direct routes to the PE carry the domain ID.

Configuration Impact

Before sending routes to a remote CE router, a PE router sends Type 3 LSAs or Type 5 LSAs to the CE based on domain ID. If local domain IDs are the same as or compatible with remote domain IDs in BGP routes, the PE advertises Type 3 routes. If local domain IDs are different from or incompatible with remote domain IDs in BGP routes, the PE advertises Type 5 routes.

Precautions

- Each OSPF domain has one or multiple domain IDs. One of them is a primary ID and the others are secondary IDs.
- If an OSPF instance does not have a specific domain ID, its ID is considered as null.
- If the value of the domain ID is 0, **secondary** cannot be configured.
- The maximum number of **domain-id secondary** items configured in an OSPF process is 1000.
- The **domain-id** command is forbidden in public network.

Example

Set the OSPF domain ID.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] domain-id 234
```

9.4.39 eca-route-type compatible

Function

The **eca-route-type compatible** command sets the route type of the extended community attribute of OSPF VPN to 0x8000.

The **undo eca-route-type compatible** command restores the route type of the extended community attribute of OSPF VPN to 0x0306.

By default, the route type of the extended community attribute of OSPF VPN is 0x0306.

Format

eca-route-type compatible

undo eca-route-type compatible

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **eca-route-type compatible** command is used in OSPF VPN scenarios.

- For the router supporting RFC 4577, you can set the route type of the extended community attribute of OSPF VPN to 0x0306 and configure the router to identify both 0x0306 and 0x8000 route types.
- For the router that does not support RFC 4577, you can set the route type of the extended community attribute of OSPF VPN to 0x8000 and configure the router to identify only the 0x8000 route type.

By running the **eca-route-type compatible** command enables different routers to communicate with each other and avoid the failure in parsing the route type because the route type of the extended community attribute of OSPF VPN is unrecognized.

Precautions

The **eca-route-type compatible** command is forbidden in public network.

Example

Set the route type of the extended community attribute of OSPF VPN to 0x8000.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] route-distinguisher 100:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] ospf 1 vpn-instance huawei
[Huawei-ospf-1] eca-route-type compatible
```

 Copyright © Huawei Technologies Co., Ltd.

9.4.40 enable log

Function

The **enable log** command enables log.

The **undo enable log** command disables log.

By default, log is disabled.

Format

enable log [**config** | **error** | **state** | **snmp-trap**]

undo enable log [**config** | **error** | **state** | **snmp-trap**]

Parameters

Parameter	Description	Value
config	Enables the configuration log.	-
state	Enables the state log.	-
error	Enables the error log.	-
snmp-trap	Enables the SNMP trap log.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Running the **enable log** command can enable the logging function. You can view running status of devices based on logs, facilitating device maintenance.

If the **undo enable log** command is executed, the logging function will be disabled. Then, running status of devices will be not displayed. This is inconvenient for network maintenance.

Precautions

Configuring different parameters in the **enable log** command can display different log information. If no parameter is not specified, the command output displays all log information.

Example

Enable the OSPF log.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] enable log
```

9.4.41 filter export (OSPF Area)

Function

The **filter export** command filters the outgoing Type3 LSAs of the local area.

The **undo filter export** command restores the default setting.

By default, the outgoing Type3 LSAs of the local area cannot be filtered.

Format

filter { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export**

undo filter [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **export**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used to filter out invalid LSAs sent to neighbors to reduce the size of the LSDB and speed up network convergence.

Configuration Impact

After filtering conditions are set for the outgoing summary LSAs to be advertised using the **filter export** command, only the outgoing Type3 LSAs that pass the filtering can be advertised.

Precautions

- The command can be configured only on an ABR.
- For a named ACL configured using the **acl name** command, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.
- Run the **filter import** command to set filtering conditions for the incoming Type3 LSAs to be advertised.

Example

Configure OSPF to filter outgoing Type 3 LSAs.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] area 1
[Huawei-ospf-1-area-0.0.0.1] filter 2000 export
```

Related Topics

9.4.42 filter import (OSPF Area)

19.7.4 acl (system view)

9.4.42 filter import (OSPF Area)

Function

The **filter import** command filters the incoming Type3 LSAs of the local area.

The **undo filter import** command restores the default setting.

By default, the incoming Type3 LSAs cannot be filtered.

Format

filter { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After filtering conditions are set for the incoming summary LSAs to be advertised using the **filter import** command, only the incoming Type3 LSAs that pass the filtering can be received.

Configuration Impact

The command can be used to filter out invalid LSAs sent to neighbors to reduce the size of the LSDB and speed up network convergence.

Precautions

- The command can be configured only on an ABR.
- For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.
- Run the **filter export** command to set filtering conditions for the outgoing Type3 LSAs to be advertised.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure an ABR to filter incoming Type 3 LSAs of the area where the ABR resides.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 1
[Huawei-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
```

Related Topics

19.7.4 acl (system view)

9.4.41 filter export (OSPF Area)

9.4.43 filter-lsa-out peer

Function

The **filter-lsa-out peer** command configures a router to filter the LSAs that are sent by the specified neighbors on a P2MP network.

The **undo filter-lsa-out peer** command cancels the configuration.

By default, the LSAs that are sent by the specified neighbor on a P2MP network are not filtered.

Format

filter-lsa-out peer *ip-address* { **all** | { **summary** [**acl** { *acl-number* | *acl-name* }] | **ase** [**acl** { *acl-number* | *acl-name* }] | **nssa** [**acl** { *acl-number* | *acl-name* }] } * }

undo filter-lsa-out peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a P2MP neighbor. This parameter is configured by the neighbor using the **ip address** command.	The value is in dotted decimal notation.
all	Filters all the outgoing LSAs except Grace LSAs.	-
summary	Filters the outgoing network summary LSAs (Type 3).	-
acl *acl-number*	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ase	Filters the outgoing AS external LSAs (Type 5).	-
nssa	Filters the outgoing NSSA LSAs (Type 7).	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a P2MP network, when multiple P2MP links exist between two devices, you can configure the local device to filter the outgoing LSAs on the specified link. This can reduce unnecessary LSA retransmission attempts and save bandwidth resources.

For a named ACL, when the **rule** command is used to configure filtering rules, only the source address range that is specified by the **source** parameter and the period of time that is specified by the **time-range** parameter take effect.

Prerequisites

OSPF does not regard a network as a P2MP network by default regardless of any link layer protocol. A P2MP network is forcibly changed from the network of another type. The network type has been changed to the P2MP by using the **ospf network-type p2mp** command.

Configuration Impact

This command is valid for all the interfaces of the OSPF process.

Follow-up Procedure

Configure a device to filter the outgoing LSAs on the specified OSPF interface by using the **ospf filter-lsa-out** command.

Example

On a P2MP network, configure a router to filter all the LSAs (except Grace LSAs) sent to neighbor 10.1.1.1.

```
<Huawei> system-view
```

```
[Huawei] ospf 1
[Huawei-ospf-1] filter-lsa-out peer 10.1.1.1 all
```

Related Topics

9.4.76 ospf filter-lsa-out

9.4.44 filter-policy export (OSPF)

Function

The **filter-policy export** command filters the imported routes when these routes are advertised based on a filtering policy.

The **undo filter-policy export** command restores the default setting.

By default, the imported routes to be advertised cannot be filtered.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol process-id	Filters imported routes of a specified protocol. The value can be **direct**, **rip**, **isis**, **bgp**, **ospf**, **unr**, or **static**. When the routing protocol is RIP, IS-IS, or OSPF, you can specify a process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After OSPF imports external routes using the **import-route** command, you can use the **filter-policy export** command to filter the imported routes to be advertised. Only the external routes that pass the filtering can be converted into AS-external LSAs and advertised.

The *protocol* or *process-id* parameter can be specified to determine a specified protocol or process. If the *protocol* or *process-id* parameter is not specified, OSPF filters all imported routes.

Precautions

- This command can be configured only on the ASBR because AS-external-LSAs are generated by an ASBR.
- For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.

Example

Filter the routes that are imported from RIP and advertised by OSPF based on a filtering policy.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] import-route rip
[Huawei-ospf-100] filter-policy 2000 export
```

Related Topics

9.4.54 import-route (OSPF)

19.7.4 acl (system view)

9.4.45 filter-policy import (OSPF)

Function

The **filter-policy import** command configures a filtering policy to filter routes received by OSPF.

The **undo filter-policy import** command restores the default setting.

By default, OSPF does not filter routes.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* [**secondary**] } **import**

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* [**secondary**]] **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the basic ACL number.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a Named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of the address prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the route policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
secondary	Specifies the secondary route.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **filter-policy import** command is used to set a filtering policy for received routes. Only the routes that pass the filtering can be added to the routing table. The routes that fails to pass the filtering cannot be added to the routing table but can be advertised.

The OSPF routing information is recorded in the LSDB. Instead of filtering the received or sent LSAs, the device filters routes calculated by OSPF using the **filter-policy import** command.

Precautions

For a named ACL configured using the **acl** command, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.

Example

Configure OSPF to filter the received routes.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] filter-policy 2000 import
```

9.4.46 flooding-control

Function

The **flooding-control** command restricts the flooding of update LSAs.

The **undo flooding-control** command cancels the restriction on the flooding of update LSAs.

By default, this function is enabled when the number of neighbors exceeds 256.

Format

flooding-control [**number** *transmit-number* | **timer-interval** *transmit-interval*] *

undo flooding-control [**number** | **timer-interval**] *

Parameters

Parameter	Description	Value
number *transmit-number*	Sets the number of update LSAs to be flooded each time.	The value is an integer ranging from 1 to 1000. By default, the value is 50.
timer-interval *transmit-interval*	Sets the interval for flooding update LSAs.	The value is an integer that ranges from 30 to 100000, in milliseconds. By default, the value is 30.

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple neighbors are configured or a large number of update LSAs are flooded, a router may receive a large number of update LSAs in a short period. If the router is busy processing these Update packets and discards the Hello packets that maintain neighbor relationships, neighbor relationships may be interrupted. During the reestablishment of neighbor relationships, more packets need to be exchanged, which deteriorates the processing of packets.

To avoid the preceding problem, you can run the **flooding-control** command to restrict the flooding of update LSAs to keep stable neighbor relationships.

Configuration Impact

After the **flooding-control** command is run, the flooding of update LSAs is immediately restricted.

Precautions

By default, a router spends 50 ms in flooding update LSAs each time. If not all the update LSAs are flooded within 50 ms, the router floods the remaining LSAs after the time specified by *transmit-interval*.

Example

Set the number of update LSAs to be flooded each time to 100.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] flooding-control number 100
```

9.4.47 frr (OSPF)

Function

The **frr** command creates an OSPF FRR view and displays the OSPF FRR view.

The **undo frr** command enables the system to exit from an OSPF FRR view and deletes the OSPF FRR view.

By default, no OSPF FRR view is created.

NOTE

AR100&AR120&AR150&AR160&AR200 series does not support this command.

Format

frr

undo frr

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **frr** command is used to enter the OSPF FRR view. OSPF FRR functions need to be configured in the OSPF FRR view.

OSPF IP FRR allows devices to fast switch traffic from faulty links to backup links without interrupting traffic. This function protects traffic and greatly improves the reliability of OSPF networks. OSPF IP FRR must be configured in the OSPF FRR view. The **frr** command run in the OSPF view creates and displays the OSPF FRR view.

Prerequisites

The OSPF function has been enabled using the **ospf** command.

Configuration Impact

The **frr** command is only used to enter the OSPF FRR view but not to enable FRR. To enable FRR, you need to run this command and other commands in the OSPF FRR view.

Follow-up Procedure

You can run the **loop-free-alternate** command to implement basic FRR functions. In this manner, the device can create the loop-free backup link.

Example

Enter the OSPF FRR view.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] frr
[Huawei-ospf-1-frr]
```

Related Topics

9.4.57 loop-free-alternate (OSPF FRR)

 Copyright © Huawei Technologies Co., Ltd.

9.4.48 frr-policy route (OSPF FRR)

Function

The **frr-policy route** command configures a filtering policy for the OSPF IP FRR backup routes. The filtering policy determines what kind of OSPF backup route can be added to the routing table.

The **undo frr-policy route** command cancels the filtering function.

By default, the filtering function is disabled.

NOTE

AR100&AR120&AR150&AR160&AR200 series does not support this command.

Format

frr-policy route route-policy *route-policy-name*

undo frr-policy route

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the policy used to filter OSPF backup routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF IP FRR allows devices to fast switch traffic on fault links to backup links without interrupting traffic. This protects traffic and greatly improves the reliability of OSPF networks.

After the filtering policy is configured using the **frr-policy route** command, only the OSPF backup route that satisfies filtering rules can be delivered to the forwarding table.

To protect the traffic over a specific OSPF route, you can configure a filtering policy *route-policy-name* that the OSPF route matches to ensure that the backup

route can be added to the forwarding table. When this route fails, OSPF can fast switch the traffic to a backup route.

Prerequisites

Before using the **frr-policy route** command, the OSPF IP FRR view has been entered by using the **frr** command, and the function of OSPF IP FRR has been enabled by using the **loop-free-alternate** command.

Precautions

The **frr-policy route** command is cyclic in nature, and only the latest configuration takes effect.

Example

Configure OSPF to add the OSPF backup routes that match the named ACL **abc** to the IP routing table.

```
<Huawei> system-view
[Huawei] ospf
[Huawei-ospf-1] frr
[Huawei-ospf-1-frr] loop-free-alternate
[Huawei-ospf-1-frr] frr-policy route route-policy abc
```

Related Topics

9.4.47 frr (OSPF)

9.4.57 loop-free-alternate (OSPF FRR)

9.4.49 frr-priority static low

Function

The **frr-priority static low** command enables dynamic backup links to take preference over static backup links so that the LFA algorithm is used to calculate the nexthop and outbound interface.

The **undo frr-priority static** command disables this function.

By default, this function is disabled, static backup links take preference over dynamic backup links during route selection.

NOTE

AR100&AR120&AR150&AR160&AR200 series do not support OSPF IP FRR.

Format

frr-priority static low

undo frr-priority static

Parameters

None

Views

OSPF FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The nexthop and outbound interface of an OSPF loop-free backup link can be obtained using either of the following methods:

- For a static backup link, after IP FRR is enabled using the **ip frr** command in the system view or **ip frr** command in VPN instance view, configure a nexthop and an outbound interface for the static backup link.
- For a dynamic backup link, after OSPF IP FRR is enabled using the **loop-free-alternate** command, enable the device to use the LFA algorithm to calculate the nexthop and outbound interface for the dynamic backup link.

By default, static backup links take preference over dynamic backup links during route selection. However, static backup links are less flexible than dynamic backup links. If a link failure occurs, static backup links cannot update automatically, but dynamic backup links can. Therefore, to ensure automatic link updates, run the **frr-priority static low** command to enable dynamic backup links to take preference over static backup links so that the LFA algorithm is used to calculate the nexthop and outbound interface.

Prerequisites

The OSPF IP FRR view has been displayed using the **frr** command.

Example

Enable the device to use the LFA algorithm to calculate the backup nexthop and outbound interface.

```
<Huawei> system-view
[Huawei] ospf
[Huawei-ospf-1] frr
[Huawei-ospf-1-frr] frr-priority static low
```

Related Topics

9.4.47 frr (OSPF)

9.4.50 graceful-restart (OSPF)

Function

The **graceful-restart** command enables the GR function.

The **undo graceful-restart** command disables GR function.

By default, OSPF GR is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

graceful-restart [**period** *period* | **planned-only** | **partial**] *

undo graceful-restart [**period** | **planned-only** | **partial**] *

Parameters

Parameter	Description	Value
period *period*	Specifies the duration of GR.	It is an integer ranging from 1s to 1800s. The default value is 120s.
planned-only	Indicates that the router supports only the planned GR. By default, the router supports both the planned GR and unplanned GR.	-
partial	Indicates that the router partially supports the GR. By default, the router totally supports the GR.	-

NOTE

Planned GR: indicates that a device manually restarts or performs a master/slave MPU switchover by using the command. Before the device restarts or performs a master/slave MPU switchover, Restarter will send a grace LSA.

Unplanned GR: indicates that a device restarts or performs a master/slave MPU switchover because of faults. A device directly performs a master/slave MPU switchover without sending a grace LSA, and then enters GR after the slave MPU goes Up. It is different from the planned GR.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **graceful-restart** command enables OSPF GR to avoid the route flapping due to the traffic interruption or master/slave MPU switchover. After the **graceful-restart** command is run to enable GR for a router, the Helper function is also enabled.

Prerequisites

Opaque LSAs provide a generic mechanism for OSPF extension:

- OSPF supports GR using Type 9 LSAs.

 Copyright © Huawei Technologies Co., Ltd.

- OSPF supports TE using Type 10 LSAs.

Before configuring OSPF GR, you must enable opaque LSA capability running the **opaque-capability enable** command.

Configuration Impact

After an OSPF process is restarted using GR, the Restarter router and the Helper router reestablish the neighbor relationship, exchange routing information, synchronize the LSDB, and update the routing table and forwarding table. This implements OSPF fast convergence, prevents traffic interruption, and stabilizes the network topology.

Precautions

If there are special requirements on the GR Helper, run the **graceful-restart helper-role** command to configure the requirements.

Example

Enable OSPF GR and the GR period is set to 200s.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] opaque-capability enable
[Huawei-ospf-1] graceful-restart period 200
```

Related Topics

9.4.68 opaque-capability enable

9.4.51 graceful-restart helper-role (OSPF)

9.4.51 graceful-restart helper-role (OSPF)

Function

The **graceful-restart helper-role** command configures a device as a GR helper.

The **undo graceful-restart helper-role** command cancels the configuration.

By default, the device does not function as a GR helper.

Format

graceful-restart [**period** *period* | **partial** | **planned-only**] * **helper-role** { { [**ip-prefix** *ip-prefix-name* | **acl-number** *acl-number* | **acl-name** *acl-name*] | **ignore-external-lsa** | **planned-only** } * | **never** }

undo graceful-restart [**period** | **partial** | **planned-only**] * **helper-role** [[{ **ip-prefix** | **acl-number** | **acl-name** } | **ignore-external-lsa** | **planned-only**] * | **never**]

Parameters

Parameter	Description	Value
period *period*	Specifies the duration of GR.	The value is an integer that ranges from 1 to 1800, in seconds. The default value is 120.
planned-only	Configures the device to support only planned GR. By default, the device supports both the planned GR and unplanned GR.	-
partial	Configures the device to support partial GR. By default, the device supports totally GR.	-
ip-prefix *ip-prefix-name*	Specifies the name of the address prefix list. The name is a string.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
acl-number *acl-number*	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a Named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ignore-external-lsa	Indicates that the device does not check Type 5 and Type 7 LSAs.	-
planned-only	Indicates that the device supports only planned GR.	By default, the device supports both planned GR and unplanned GR.
never	Indicates that the device does not support the Helper mode.	-

Views

OSPF view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After an OSPF process is restarted through GR, only the restarter and the helper reestablish the neighbor relationship, then stabilizes the network topology.

Prerequisites

Before configuring GR of the device, you need to enable Opaque LSA by running the **opaque-capability enable** command.

Example

Configure a device as an OSPF GR helper and configure the helper to support only Planned-GR.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] graceful-restart helper-role planned-only
```

Related Topics

9.4.68 opaque-capability enable

9.4.52 gtsm default-action

Function

The **gtsm default-action** command sets the default action that is performed on the packets that do not match the GTSM policies.

The **undo gtsm default-action drop** command cancels the setting that the packets that do not match the GTSM policy cannot pass the filtering.

By default, the packets that do not match the GTSM policies can pass the filtering.

Format

gtsm default-action { **drop** | **pass** }

undo gtsm default-action drop

Parameters

Parameter	Description	Value
drop	Indicates that the packets that do not match the GTSM policies cannot pass the filtering. The packets are dropped.	-
pass	Indicates that the packets that do not match the GTSM policies can pass the filtering.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a network demanding high security, you can configure Generalized TTL Security Mechanism (GTSM) to improve the security of the OSPF network. GTSM defends against attacks by checking the Time-to-Live (TTL) value. If an attacker simulates real OSPF packets and keeps sending them to a router, an interface board on the router receives the packets and directly sends them to the main control board for OSPF processing, without checking the validity of the packets. In this case, the router is busy in processing these packets, causing high usage of the CPU. GTSM function protects the router by checking whether the TTL value in the IP packet header is in a pre-defined range to improve the system security.

GTSM only checks the TTL values of the packets that match the GTSM policy. The packets that do not match the GTSM policy can pass the filtering using the **undo gtsm default-action drop**command or using the **gtsm default-action** command to set the **pass** parameter, or be dropped after the **gtsm default-action** command is run to set the **drop** parameter.

Configuration Impact

If the default action to be taken on GTSM packets is drop, the connection cannot be established by the router. Therefore, GTSM ensures better security but reduces the ease of use.

Precautions

You can enable the log function by using the **gtsm log drop-packet** command to record the information about dropped packets for further fault location.

If you configure the default action by using the **gtsm default-action** command but not configure GTSM policy (the **drop** or **pass** parameter), GTSM does not take effect.

Example

Set the default action performed on the packets that do not match the GTSM policies as "drop".

```
<Huawei> system-view
[Huawei] gtsm default-action drop
```

Set the default action performed on the packets that do not match the GTSM policy as pass the filtering.

```
<Huawei> system-view
[Huawei] undo gtsm default-action drop
```

Related Topics

9.4.53 gtsm log drop-packet
9.4.94 ospf valid-ttl-hops

9.4.53 gtsm log drop-packet

Function

The **gtsm log drop-packet** command enables the log function on the slot. The information that GTSM drops packets is recorded in the log.

The **undo gtsm log drop-packet** command disables the log function on the slot.

By default, the information that GTSM drops packets is not recorded in the log.

Format

gtsm log drop-packet all

undo gtsm log drop-packet all

Parameters

Parameter	Description	Value
all	Indicates all the slots.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

NOTE

On the AR, the **gtsm log drop-packet** command can enable the log function only on the MPU, but not on LPUs.

Usage Scenario

For a network demanding higher security, you can configure Generalized TTL Security Mechanism (GTSM) to improve the security of the OSPF network. GTSM defends against attacks by checking the Time-to-Live (TTL) value. If an attacker simulates real OSPF packets and keeps sending them to a device, an interface board on the device receives the packets and directly sends them to the main control board for OSPF processing, without checking the validity of the packets. In this case, the device is busy in processing these packets, causing high usage of the CPU. GTSM function protects the device by checking whether the TTL value in the IP packet header is in a pre-defined range to improve the system security.

GTSM only checks the TTL values of the packets that match the GTSM policy. The packets that do not match the GTSM policy can be allowed or dropped by using the **gtsm default-action** command.

 Copyright © Huawei Technologies Co., Ltd.

You can also enable the log function by using the **gtsm log drop-packet** command to record the information about dropped packets for further fault location.

Prerequisites

Run the **gtsm default-action drop** command to drop packets before the log function is enabled.

Example

Enable the GTSM log function on all the slots.

```
<Huawei> system-view
[Huawei] gtsm default-action drop
[Huawei] gtsm log drop-packet all
```

Related Topics

9.4.52 gtsm default-action

9.4.54 import-route (OSPF)

Function

The **import-route** command imports routes learned by other protocols.

The **undo import-route** command cancels the configuration.

By default, routes learned by other protocols are not imported.

Format

import-route { **limit** *limit-number* | { **bgp** [**permit-ibgp**] | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf** [*process-id-ospf*] } [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * }

undo import-route { **limit** | **bgp** | **direct** | **unr** | **rip** [*process-id-rip*] | **static** | **isis** [*process-id-isis*] | **ospf** [*process-id-ospf*] }

Parameters

Parameter	Description	Value
bgp	Specifies the BGP protocol whose routes are imported. For an OSPF process that is not bound to a VPN instance or is bound to a VPN instance but the vpn-instance-capability simple command is run, the parameter imports only EBGP routes.	-

Parameter	Description	Value
permit-ibgp	IBGP routes that are permitted to be imported. The import of IBGP routes may cause route loops. Therefore, this command must not be configured unless it is necessary. **NOTICE** For an OSPF process that is not bound to a VPN instance or is bound to a VPN instance but the vpn-instance-capability simple command is run, importing IBGP routes may cause routing loops. Therefore, exercise caution when using this parameter.	-
direct	Specifies the direct protocol whose routes are imported.	-
unr	Specifies the imported source routing protocol as **unr**. User Network Route (UNR) is allocated if dynamic routing protocols cannot be used when users are getting online.	-
rip	Specifies the imported source routing protocol as **rip**.	-
process-id-rip	Specifies the process ID of the imported RIP routing protocol.	The value is an integer ranging from 1 to 65535. The default value is 1.
static	Specifies the imported source routing protocol as **static**. **NOTE** The parameter can only active static routes are imported.	-
isis	Specifies the imported source routing protocol as **isis**.	-
process-id-isis	Specifies the process ID of the imported IS-IS routing protocol.	The value is an integer ranging from 1 to 65535. The default value is 1.
ospf	Specifies the imported source routing protocol as **ospf**.	-
process-id-ospf	Specifies the process ID of the imported OSPF routing protocol.	The value is an integer ranging from 1 to 65535. The default value is 1.
limit *limit-number*	The maximum number of external routes that can be imported into an OSPF process.	The value is an integer that ranges from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cost *cost*	Indicates the route cost.	The value is an integer ranging from 0 to 16777214. By default, it is 1.
route-policy *route-policy-name*	Imports only the route that meets the requirements of the specified route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the tag of the external LSA.	The value is an integer ranging from 0 to 4294967295. By default, it is 1.
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. By default, it is 2. ● 1: Type 1 external route ● 2: Type 2 external route

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Importing the routes discovered by other routing protocols can enrich OSPF routing information.

When OSPF imports external routes, you can set default values for some additional parameters using the **import-route** command, such as metric, route tag, and route type. A route tag is used to identify protocol-related information. For example, it can be used to differentiate AS numbers carried in BGP routes imported by OSPF.

By default, the cost of the external routes imported by OSPF is 1; the type of the imported external routes is Type 2; the default tag value of the imported routes is 1.

OSPF routes are classified into the following types in the descending order of priorities:

 Copyright © Huawei Technologies Co., Ltd.

- Intra-area routes: refer to the routes in an area within an autonomous system.
- Inter-area routes: refer to the routes between different areas of the same AS. Intra-area routes and area external routes are internal routes of an AS.
- Type 1 external routes: When the cost of external routes equals that of AS internal routes, and can be compared with the cost of OSPF routes, these external routes have a high reliability and can be configured as Type 1 external routes.
- Type 2 external routes: When the cost of the routes from an ASBR to the destination outside an AS is much greater than the cost of the internal routes to the ASBR, these external routes has a low reliability and can be configured as Type 2 external routes.

On a non-PE device, only EBGP routes are imported after the **import-route bgp** command is configured. IBGP routes are also imported after the **import-route bgp permit-ibgp** command is configured. If IBGP routes are imported, routing loops may occur. In this case, run the **preference (OSPF)** and **preference (BGP)** commands to prevent loops by specifying preferences of OSPF and BGP routes. If IBGP routes need to be imported, configure the **import-route bgp permit-ibgp** command, and run the **preference (OSPF)** and **preference (BGP)** commands to set the preference of OSPF ASE routes lower than that of IBGP routes (preference value of OSPF ASE routes larger than that of IBGP routes).

On a PE, configuring the **import-route bgp** command imports both EBGP routes and IBGP routes, no matter whether the **import-route bgp permit-ibgp** command is configured or not. If the **import-route bgp permit-ibgp** command and the **default-route-advertise (OSPF)** command are both configured, the active IBGP default routes can be imported into OSPF.

Prerequisites

You must create a route-policy by running the **route-policy** command before running the **import-route** command to import certain external routes by the route-policy.

Procedure

The costs of a Type 1 external route and a Type 2 external route are as follows:

- The cost of a Type 1 external route equals the cost for the OSPF device to reach an ASBR plus the cost of the route from the ASBR to the destination.
- The cost of a Type 2 external route equals the cost of the route from an ASBR to the destination.

Configuration Impact

After a route-policy is configured, the OSPF process imports only routes of a network segment that satisfy certain conditions. This prevents devices from receiving routes not required.

Precautions

You can use the **default (OSPF)** command to configure default parameters for OSPF to import external routes, including the cost, type (Type 1 or Type 2), tag, and number of routes.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The **import-route (OSPF)** command cannot import the default route of an external protocol. To enable a device to advertise the default route of an external protocol it learns when updating the OSPF routing table to other devices within the area, run the **default-route-advertise (OSPF)** command.

After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the OSPF routing table. Therefore, use this command with caution.

Example

Import Type 2 RIP routes, with the process 40, the tag being 33 and cost being 50.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

Related Topics

9.4.7 default (OSPF)

9.9.53 route-policy

9.4.55 local-mt filter-policy (OSPF)

Function

The **local-mt filter-policy** command configures the filtering policy of OSPF Local Multicast-Topology (MT).

The **undo local-mt filter-policy** command deletes the filtering policy of OSPF local MT.

By default, the filtering policy of OSPF local MT is not configured.

Format

local-mt filter-policy { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* }

undo local-mt filter-policy

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of the basic access control list (ACL).	The value is an integer ranging from 2000 to 2999.
acl *acl-name*	Specifies the name of a Named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of the route policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast and an MPLS TE tunnel are configured on a network and the TE tunnel is configured with IGP Shortcut, the outbound interface of the route calculated by an IGP is not an actual physical interface but a TE tunnel interface. The device uses a unicast route to the multicast source address to send multicast Join messages from the TE tunnel interface. The device through which the TE tunnel passes, however, cannot sense the multicast Join messages. As a result, multicast forwarding entries will not be created.

To avoid the preceding problem, you can create a proper multicast routing table to guide the forwarding of multicast packets by configuring local MT. After OSPF local MT is enabled, if the outbound interface of the calculated route is a TE tunnel interface of the IGP Shortcut type, the route management (RM) module creates a separate MIGP routing table for the multicast protocol, calculates the actual physical outbound interface for the route, and adds the physical interface to the MIGP routing table for multicast forwarding.

To control the number of entries in the MIGP routing table and speed up the MIGP routing table search, you can configure filtering conditions by using the **local-mt filter-policy** command to allow only the matching routes to the multicast source address to be added to the MIGP routing table.

Prerequisites

OSPF local MT has been enabled using the **local-mt enable** command.

Precautions

You are recommended to configure the routing policy before enabling local MT. This can prevent the excessive routes to the not-multicast source address from

 Copyright © Huawei Technologies Co., Ltd.

being added to the MIGP routing table and keeps the number of routes in the MIGP routing table within the upper limit.

When the **rule(basic ACL6 view)** or **rule (basic ACL view)** command is used to configure filtering rules for a named ACL configured using the **acl** command, only the source address range that is specified by the **source** parameter and the period of time that is specified by the **time-range** parameter take effect.

Example

Configure the filtering policy of OSPF local MT.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] local-mt enable
[Huawei-ospf-1] local-mt filter-policy acl 2000
```

Related Topics

9.4.56 local-mt enable (OSPF)

19.7.4 acl (system view)

9.4.56 local-mt enable (OSPF)

Function

The **local-mt enable** command enables OSPF Local Multicast-Topology (MT).

The **undo local-mt enable** command disables OSPF local MT.

By default, OSPF local MT is disabled.

Format

local-mt enable

undo local-mt enable

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multicast and an MPLS TE tunnel are configured on a network and the TE tunnel is configured with IGP Shortcut, the outbound interface of the route

calculated by an IGP is not an actual physical interface but a TE tunnel interface. The device uses a unicast route to the multicast source address to send multicast Join messages from the TE tunnel interface. The device spanned by the TE tunnel, however, cannot sense the multicast Join messages. As a result, multicast forwarding entries will not be created on these devices.

To avoid the preceding problem, you can run the **local-mt enable** command to enable OSPF local Multicast-Topology (MT). MT allows the multicast routing entries to be correct created to guide the forwarding of multicast traffic.

After OSPF local MT is enabled, if the outbound interface of the calculated route is a TE tunnel interface of the IGP Shortcut type, the route management (RM) module creates a separate MIGP routing table for the multicast protocol, calculates the actual physical outbound interface for the route, and adds the physical interface to the MIGP routing table for multicast forwarding.

Prerequisites

IGP Shortcut feature has been enabled using the **enable traffic-adjustment** command.

Precautions

- To control the number of entries in the MIGP routing table and speed up the MIGP routing table search, you can run the **local-mt filter-policy** command to configure a policy for filtering multicast source address. Then only the multicast source address that matches the policy to be added to the MIGP routing table. Configure the routing policy before enabling local MT. This can prevent excessive routes to non-multicast source address from being added to the MIGP routing table and keeps the number of routes in the MIGP routing table within the upper limit.
- Local MT is applicable only to the OSPF process of a public network instance.
- OSPF local MT does not support forwarding adjacency (FA).

Example

Enable local MT on OSPF process 1.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] local-mt enable
```

Related Topics

9.4.55 local-mt filter-policy (OSPF)

11.2.49 enable traffic-adjustment

9.4.57 loop-free-alternate (OSPF FRR)

Function

The **loop-free-alternate** command enables OSPF IP FRR enable the device to use the LFA algorithm to calculate the nexthop and outbound interface for the dynamic backup link.

The **undo loop-free-alternate** command disables OSPF IP FRR.

By default, OSPF IP FRR is disabled.

NOTE

AR100&AR120&AR150&AR160&AR200 series does not support this command.

Format

loop-free-alternate

undo loop-free-alternate

Parameters

None

Views

OSPF FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Loop Free Alternate (LFA) is a method of implementing FRR. Through LFA, a device can generate a loop-free backup link and FRR can be implemented.

OSPF IP FRR takes effect only after the **loop-free-alternate** command is run.

Prerequisites

before configuring the command, you can create an OSPF IP FRR view and enter the OSPF IP FRR view by running the **frr** command.

Precautions

If you do not want the link that transmits important service traffic to function as the backup link of other links, you need to configure the **ospf frr block** command on the interface connecting to the link before configuring the OSPF IP FRR function. In this manner, the link will not be designated as the backup link during FRR calculation.

Example

Enable OSPF IP FRR through LFA.

```
<Huawei> system-view
[Huawei] ospf
[Huawei-ospf-1] frr
[Huawei-ospf-1-frr] loop-free-alternate
```

Related Topics

9.4.47 frr (OSPF)

9.4.77 ospf frr block

9.4.58 lsa-arrival-interval

Function

The **lsa-arrival-interval** command sets the interval for receiving LSAs.

The **undo lsa-arrival-interval** command restores the default interval for receiving LSAs.

By default, an intelligent timer is enabled. The interval for receiving LSAs is expressed in milliseconds. The maximum interval for updating LSAs is 1000 milliseconds (ms), the initial interval is 500 ms, and the Holdtime interval is 500 ms.

Format

lsa-arrival-interval { *interval* | **intelligent-timer** *max-interval start-interval hold-interval* }

lsa-arrival-interval suppress-flapping *suppress-interval* [**threshold** *threshold*]

undo lsa-arrival-interval

undo lsa-arrival-interval suppress-flapping *suppress-interval* [**threshold** *threshold*]

Parameters

Parameter	Description	Value
interval	Specifies the interval for receiving LSAs.	The value is an integer ranging from 0 to 10000, in ms.
intelligent-timer	Enables an intelligent timer to receive LSAs.	-
max-interval	Specifies the maximum interval for receiving LSAs.	The value is an integer ranging from 1 to 120000, in ms. The default value is 1000.
start-interval	Specifies the initial interval for receiving LSAs.	The value is an integer ranging from 0 to 60000, in ms. The default value is 500.
hold-interval	Specifies the Holdtime interval for receiving LSAs.	The value is an integer ranging from 1 to 60000, in ms. The default value is 500.
suppress-flapping *suppress-interval*	Specifies an OSPF LSA suppression period.	The value is an integer ranging from 0 to 600, in seconds. The default value is 10 seconds.
threshold *threshold*	Specifies the suppression threshold of OSPF LSAs.	The value is an integer ranging from 3 to 100. The default value is 30.

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In OSPF, the interval for receiving LSAs is 1s. This prevents network connections or frequent route flapping from consuming excessive network bandwidth or device resources.

On a stable network where routes need to be fast converged, you can change the interval for receiving LSAs to 0s. In this manner, the change of the topology or route can be immediately sensed, which speeds up route convergence.

To configure the maximum LSA suppression period, run the **lsa-arrival-interval suppress-flapping** command. If frequent LSA flapping occurs, the larger value between **lsa-arrival-interval suppress-flapping** and **lsa-arrival-interval** is used to suppress LSA flapping.

If there is no special network requirement, default values are recommended.

Procedure

After an intelligent timer is enabled, the interval for receiving LSAs is as follows:

1. The initial interval for receiving LSAs is specified by *start-interval*.
2. The interval for receiving LSAs for the nth (n≥2) time is equal to *hold-interval* x $2^{(n-2)}$.
3. When the interval specified by *hold-interval* x $2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPF receives LSAs at the maximum interval for three consecutive times. Then, Step 1 is repeated, that is, OSPF receives LSAs at the initial interval specified by *start-interval*.
4. When the interval specified by *hold-interval*×$2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPF performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

Precautions

It is recommended that you set the receiving interval specified by **lsa-arrival-interval** to a value smaller than or equal to the Holdtime interval specified by**lsa-originate-interval**.

Example

Set the interval for receiving LSAs to 0 milliseconds.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] lsa-arrival-interval 0
```

Set the maximum LSA suppression period to 200s.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] lsa-arrival-interval suppress-flapping 200
```

Related Topics

9.4.59 lsa-originate-interval

9.4.59 lsa-originate-interval

Function

The **lsa-originate-interval** command sets the interval for updating LSAs.

The **undo lsa-originate-interval** command restores the default interval for updating LSAs.

By default, the intelligent timer is enabled; the maximum interval for updating LSAs is 5000 ms, the initial interval is 500 ms, and the Holdtime interval is 1000 ms.

Format

lsa-originate-interval { **0** | { **intelligent-timer** *max-interval start-interval hold-interval* | **other-type** *interval* } * }

lsa-originate-interval other-type *interval* [**intelligent-timer** *max-interval start-interval hold-interval*]

undo lsa-originate-interval

Parameters

Parameter	Description	Value
0	Sets the interval for updating LSAs to 0 ms, that is, deletes the initial interval (5000 ms) for updating LSAs.	-
intelligent-timer	Enables an intelligent timer to update OSPF router LSAs and network LSAs.	-
max-interval	Specifies the maximum interval for updating OSPF LSAs.	The value is an integer ranging from 1 to 120000, in ms. The default value is 5000.
start-interval	Specifies the initial interval for updating OSPF LSAs.	The value is an integer that ranges from 0 to 60000, in ms. The default value is 500.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hold-interval	Specifies the Holdtime interval for updating OSPF LSAs.	The value is an integer ranging from 1 to 60000, in ms. The default value is 1000.
other-type	Sets the interval for updating the LSAs other than the OSPF router LSAs and network LSAs.	-
interval	Specifies the interval for updating LSAs.	The value is an integer ranging from 0 to 10, in seconds. The default value is 5.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF sets the interval for updating LSAs to 5s. This prevents network connections or frequent route flapping from consuming excessive network bandwidth or device resources.

On a stable network where routes need to be fast converged, you can change the interval for updating LSAs to 0s. In this manner, the change of the topology or route can be immediately advertised on the network through LSAs, which speeds up route convergence.

If there is no special network requirement, default values are recommended.

To configure the maximum LSA suppression period, run the **lsa-originate-interval suppress-flapping** command. If frequent LSA flapping occurs, the larger value between **lsa-originate-interval suppress-flapping** and **lsa-originate-interval** is used to suppress LSA flapping.

Execution Process

After an intelligent timer is enabled, the interval for updating LSAs is as follows:

1. The initial interval for updating LSAs is specified by *start-interval*.
2. The interval for updating LSAs for the nth (n≥2) time is equal to *hold-interval* x $2^{(n-2)}$.
3. When the interval specified by *hold-interval*×$2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPF performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

It is recommended that you set the receiving interval specified by **lsa-originate-interval** to a value longer than or equal to the Holdtime interval specified by **lsa-arrival-interval**.

Example

Set the interval for updating LSAs to 0 milliseconds.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] lsa-originate-interval 0
```

Set the maximum LSA suppression period to 200s.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] lsa-originate-interval suppress-flapping 200
```

Related Topics

9.4.58 lsa-arrival-interval

9.4.60 lsdb-overflow-limit

Function

The **lsdb-overflow-limit** command sets the maximum number of external LSAs in OSPF LSDB.

The **undo lsdb-overflow-limit** command removes the maximum number of external LSAs.

By default, the maximum number of external LSAs is not set.

Format

lsdb-overflow-limit *number*

undo lsdb-overflow-limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of external LSAs in LSDB.	The value is an integer ranging from 1 to 1000000.

Views

OSPF view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the number of external LSAs (Type 5 and Type 7 LSAs) imported by OSPF exceeds the limit, the excessive external LSAs cannot be processed properly and are discarded.

To avoid the preceding problem, you can set the maximum number of external LSAs in the LSDB to adjust and optimize OSPF networks.

Prerequisites

Running the **display ospf lsdb brief** command, you can see **OSPF is in LSDB overflow status** in the command output. Then, run the **lsdb-overflow-limit** command to set the maximum number of external LSAs imported by OSPF.

Precautions

The configuration of this command must be consistent in the entire AS.

Example

Set the maximum number 400000 of external LSA in LSDB.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] lsdb-overflow-limit 400000
```

Related Topics

9.4.23 display ospf lsdb

9.4.61 maxage-lsa route-calculate-delay (OSPF)

Function

The **maxage-lsa route-calculate-delay** command configures the route calculation delay function to suppress frequent OSPF LSA flapping.

The **undo maxage-lsa route-calculate-delay** command disables the function.

By default, the route calculation delay to suppress frequent OSPF LSA flapping is 10s.

Format

maxage-lsa route-calculate-delay *delay-interval*

undo maxage-lsa route-calculate-delay

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delay-interval	Specifies a route calculation delay.	The value is an integer ranging from 0 to 65535, in seconds. The default value is 10 seconds.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Frequent OSPF LSA flapping on the remote device may lead to route flapping on the local device, affecting services. To address this problem, run the **maxage-lsa route-calculate-delay** command to configure the local device to delay route calculation in the case of frequent OSPF LSA flapping, which suppresses route flapping locally.

Example

Set the route calculation delay to suppress frequent OSPF LSA flapping to 200s.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] maxage-lsa route-calculate-delay 200
```

9.4.62 maximum load-balancing (OSPF)

Function

The **maximum load-balancing** command sets the maximum number of equal-cost routes for carrying out load balancing.

The **undo maximum load-balancing** command restores the default setting.

By default, the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204 support a maximum of four equal-cost routes, and the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series support a maximum of eight equal-cost routes, AR2240 (using SRU200, SRU200E or SRU400), and AR3200 (using SRU200, SRU200E or SRU400) series support a maximum of sixteen equal-cost routes.

Format

maximum load-balancing *number*

 Copyright © Huawei Technologies Co., Ltd.

undo maximum load-balancing

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a routing protocol discovers multiple routes with the same cost to a single destination, they can carry out load balancing. The **maximum load-balancing** command sets the maximum number of equal-cost routes that can carry out load balancing. This optimizes the routing policy and ensures traffic forwarding on a complex network.

Configuration Impact

Packets will be load-balanced by multiple equal-cost routes to a single destination.

Follow-up Procedure

If more existing equal-cost OSPF routes than the value set using the **maximum load-balancing** command are available, if equal-cost routes need to be specified for load balancing, the **nexthop** *ip-address* **weight** *value* command allows routes with a specified weight to carry out load balancing.

Precautions

To disable load balancing, set the value of *number* to 1.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum number of the equal-cost routes.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] maximum load-balancing 2
```

Restore the default maximum number of equal-cost routes for carrying out load balancing.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] undo maximum load-balancing
```

Related Topics

9.4.66 nexthop (OSPF)

9.4.63 maximum-routes

Function

The **maximum-routes** command sets the maximum number of routes of different types that OSPF supports.

The **undo maximum-routes** command restores the default maximum number of routes of different types that OSPF supports.

By default, OSPF supports a maximum number of 5000000 external routes, 1000000 inter-area routes, and 100000 intra-area routes.

Format

maximum-routes { **external** | **inter** | **intra** } *number*

undo maximum-routes { **external** | **inter** | **intra** }

Parameters

Parameter	Description	Value
external	Indicates the maximum number of AS external routes that OSPF supports.	-
inter	Indicates the maximum number of inter-area routes that OSPF supports.	-
intra	Indicates the maximum number of intra-area routes that OSPF supports.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
number	Specifies the maximum number of routes of different types.	The value is an integer. ● When configuring the **external** parameter, the value of *number* is an integer ranging from 100 to 5000000. The default value is 5000000. ● When configuring the **inter** parameter, the value of *number* is an integer ranging from 100 to 1000000. By default, the value is 1000000. ● When configuring the **intra** parameter, the value of *number* is an integer ranging from 100 to 100000. By default, the value is 100000.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the real world situation of a network such as the convergence speed, the **maximum-routes** command configures the maximum number of routes of different types to make full use of network resources and improve network performance.

Precautions

The maximum number of routes supported by OSPF cannot exceed the maximum number of all routes supported by the router.

The **maximum-routes** command configuration limits the maximum number of routes that can be locally calculated. Therefore, the command configuration affects the maximum number of routes that can be sent, but does not affect the maximum number of LSAs that can be received.

Example

Set the maximum number of routes that OSPF supports.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] maximum-routes intra 500
```

9.4.64 mesh-group enable

Function

The **mesh-group enable** command enables the mesh-group function.

The **undo mesh-group enable** command disables the mesh-group function.

By default, the mesh-group function is disabled.

Format

mesh-group enable

undo mesh-group enable

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When concurrent links exist between the device and its neighbor, the **mesh-group enable** command enables the mesh-group function. The router ID of a neighboring device uniquely identifies a mesh group. After LSAs are received, the device selects a primary link to flood the received LSAs, without performing reverse flooding. This prevents repeated flooding, reduce the load on the links, and save system resources.

device interfaces that meet the following conditions can form a mesh group:

- The interfaces belong to the same area and OSPF process.
- The neighbor status is Exchange or Full.
- Each interface is connected only to one neighbor.

Precautions

After the device is enabled with the mesh-group function, if the router IDs of the directly connected neighbor are the same, the LSDBs of the entire network cannot be synchronized and routes cannot be calculated correctly. In this case, you need to reconfigure the router ID of the neighbor, and then restart the neighbor to validate the configured router ID.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the mesh-group function on the router.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] mesh-group enable
```

Related Topics

9.4.25 display ospf mesh-group

9.4.65 network (OSPF Area)

Function

The **network** command specifies the interface that runs OSPF and the area to which the interface belongs.

The **undo network** command deletes the interface that runs OSPF.

By default, an interface does not belong to any area.

Format

network *network-address wildcard-mask* [**description** *text*]

undo network *network-address wildcard-mask*

Parameters

Parameter	Description	Value
network-address	Specifies the address of the network segment where the interface resides.	The value is in dotted decimal notation.
wildcard-mask	Specifies the wildcard mask of an IP address, which is similar to the reversed form of the mask of the IP address. For example, 0.0.0.255 indicates that the mask length is 24 bits.	The value is in dotted decimal notation.
description *text*	Specifies the description of the specified OSPF network segment.	The value is a string of 1 to 80 case-sensitive characters with spaces allowed.

Views

OSPF area view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After creating an OSPF process, you can run the **network** command to configure the network segments in an area and specify *network-address* and *wildcard-mask* to configure one or multiple interfaces in an area. To run OSPF on an interface, ensure that the primary IP address of this interface is in the network segment range specified in the **network** (OSPF) command. If the secondary IP address of the main interface is in the network segment range specified in this command, the main interface cannot run OSPF.

OSPF can run on an interface only when the following two conditions are met:

- The mask length of the interface's IP address is not less than that specified in the **network** command. OSPF uses a reverse mask. For example, 0.0.0.255 indicates that the mask length is 24 bits.

  NOTE

  When the *wildcard-mask* parameter in the **network** command is set to all 0s, OSPF can run on the interface if the IP address of the interface is the IP address specified in the **network** *network-address* command.

- The primary address of the interface is within the network segment range specified in the **network** command.

Precautions

- OSPF neighbor relationships cannot be established using the secondary IP addresses of interfaces.
- After the **network** 0.0.0.0 255.255.255.255 command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the OSPF routing table. Therefore, use this command with caution.
- For the same **network** *address wildcard-mask*, the last description configured by **description** takes effect.
- On a loopback interface, by default, OSPF advertises its IP address in the form of a 32-bit host route, independent of the mask length of the IP address on the interface.
- To advertise the network segment route of a loopback interface, you need to run the **ospf network-type** command to set the network type to broadcast or NBMA.
- When an OSPF sham link is configured, the local address cannot be advertised through the OSPF process of a private network.
- Two areas that overlap cannot be configured between different processes in the same instance, or between different areas in the same process.
- The **ospf enable** command configuration takes precedence over the **network** command configuration.

Example

Configure the primary IP address of the interface that runs OSPF to be in the network segment of 192.168.1.0/24, set the ID of the OSPF area where the interface resides to 2, and configure the description for the network segment.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 2
[Huawei-ospf-100-area-0.0.0.2] network 192.168.1.0 0.0.0.255 description this network is connected to
Beijing
```

Related Topics

9.4.69 ospf

9.4.81 ospf network-type

9.4.75 ospf enable

9.4.66 nexthop (OSPF)

Function

The **nexthop** command sets the preference for the equal-cost routes. After OSPF calculates the equal-cost routes, the next hop is chosen from these equal-cost routes based on the value of weight. The smaller the value is, the higher the preference is.

The **undo nexthop** command cancels the preference of these equal-cost routes.

By default, the value of weight is 255. Equal-cost routes have no preference, and they forward packets at the same time. Load balancing is performed among them.

Format

nexthop *ip-address* **weight** *value*

undo nexthop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Indicates the IP address of next hop.	The value is in dotted decimal notation.
weight *value*	Indicates the weight of the next hop. The smaller the value is, the higher the preference of the route is.	It is an integer that ranges from 1 to 254.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

If the number of equal-cost routes in a network is greater than the value set by using the **maximum load-balancing** command, if equal-cost routes need to be

specified for load balancing, the **nexthop** command to used to increase the priorities of these routes.

Example

Set the preference of equal-cost routes in OSPF.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] nexthop 10.0.0.3 weight 1
```

Related Topics

9.4.62 maximum load-balancing (OSPF)

9.4.67 nssa (OSPF Area)

Function

The **nssa** command configures an NSSA.

The **undo nssa** command cancels the configuration of an NSSA.

By default, no OSPF area is configured as an NSSA.

Format

nssa [{ **default-route-advertise** [**backbone-peer-ignore**] | **suppress-default-route** } | **flush-waiting-timer** *interval-value* | **no-import-route** | **no-summary** | **set-n-bit** | **suppress-forwarding-address** | **translator-always** | **translator-interval** *interval-value* | **zero-address-forwarding** | **translator-strict**] *

undo nssa [**flush-waiting-timer** *interval-value*]

Parameters

Parameter	Description	Value
default-route-advertise	Generates default Type7 LSAs on the ASBR and then advertises them to the NSSA. **NOTE** The ABR generates a default NSSA LSA (Type7 LSA) automatically and advertises it in the NSSA. Type 7 LSAs carrying the default route will be generated only when the default route 0.0.0.0/0 exists in the routing table on the ASBR.	-
backbone-peer-ignore	Prevents the ABR from checking the neighbor status when the ABR generates default Type 7 LSAs and advertises them to the NSSA. Specifically, the ABR generates default Type 7 LSAs and advertises them to the NSSA as long as an interface that is Up exist in the backbone area.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
suppress-default-route	Generates default Type-7 LSAs on the ASBR or ABR and then not advertises them to the NSSA.	-
flush-waiting-timer *interval-value*	Indicates the interval for an ASBR to send aged Type 5 LSAs. The parameter takes effect only when it is set.	The value is an integer that ranges from 1 to 40, in seconds.
no-import-route	Indicates that no external route is imported to an NSSA.	-
no-summary	Indicates that an ABR is prohibited from sending summary LSAs to the NSSA.	-
set-n-bit	Sets the N-bit in DD packets.	-
suppress-forwarding-address	Sets the FA of the Type 5 LSAs translated from Type 7 LSAs by the NSSA ABR to 0.0.0.0.	-
translator-always	Specifies an ABR in an NSSA as an all-the-time translator. Multiple ABRs in an NSSA can be configured as translators.	-
translator-interval *interval-value*	Specifies the timeout period of a translator.	The value is an integer ranging from 1 to 120, in seconds. The default value is 40.
zero-address-forwarding	Sets the FA of the generated NSSA LSAs to 0.0.0.0 when external routes are imported by the ABR in an NSSA.	-
translator-strict	Configures the translator to perform strict check on the P-bit flag. The translator determines whether to translate Type 7 LSAs into Type 5 LSAs based on the P-bit flag.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NSSA is configured in the scenario where AS external routes are to be imported but not forwarded to save system resources. AS external routes can be imported to an NSSA and transmitted to the entire NSSA.

All routers in the NSSA must be configured with NSSA attributes using the **nssa** command.

The **nssa** command is applicable to the following scenarios:

- The **default-route-advertise** parameter is configured to advertise Type 7 LSAs carrying the default route on the ASBR to the NSSA.

  Regardless of whether the default route 0.0.0.0/0 exists in the routing table on the ABR, Type 7 LSAs carrying the default route will be generated. However, Type 7 LSAs carrying the default route will be generated only when the default route 0.0.0.0/0 exists in the routing table on the ASBR.
- When the area to which the ASBR belongs is configured as an NSSA, invalid Type 5 LSAs from other routers in the area where LSAs are flooded will be reserved. These LSAs will be deleted only when the aging time reaches 40s. The router performance is affected because the forwarding of a large number of LSAs consumes the memory resources. To resolve such a problem, you can set the parameter **flush-waiting-timer** to the maximum value 40s for Type 5 LSAs so that the invalid Type 5 LSAs from other routers can be deleted in time.

  NOTE

  - When the LS age field value (aging time) in the header of an LSA reaches 40s, the LSA is deleted.
  - If an ASBR also functions as an ABR, **flush-waiting-timer** does not take effect. This prevents Type 5 LSAs in the non-NSSAs from being deleted.
- If an ASBR also functions as an ABR, the **no-import-route** parameter is configured to prevent external routes imported using the **import-route** command from being advertised to the NSSA.
- The **no-summary** parameter is configured on an ABR to reduce the number of LSAs that are transmitted to the NSSA. This implementation prevents the ABR from transmitting Type 3 LSAs to the NSSA.

  NOTE

  After the **nssa default-route-advertise backbone-peer-ignore no-summary** command is run, the ABR generates default Type 7 and Type 3 LSAs as long as an interface that is Up exist in the backbone area. The default Type 3 LSAs preferentially take effect.
- After the **set-n-bit** parameter is configured, the N-bit is set in the database description (DD) packets during the synchronization between the router and neighboring routers.
- If multiple ABRs are deployed in the NSSA, the system automatically selects an ABR (generally the router with the largest router ID) as a translator to convert Type 7 LSAs into Type 5 LSAs. You can configure the **translator-always** parameter on an ABR to specify the ABR as an all-the-time translator. To specify two ABRs for load balancing, configure the **translator-always** parameter on the chosen ABRs to specify the ABRs as all-the-time translators. You can use this command to pre-configure a fixed translator to prevent LSA flooding caused by translator role changes.

 Copyright © Huawei Technologies Co., Ltd.

- The **translator-interval** parameter is used to ensure uninterrupted services when translator roles change. The value of *interval-value* must be greater than the flooding period.

Configuration Impact

Configuring or deleting NSSA attributes may trigger routing update in the area. A second configuration of NSSA attributes can be implemented or canceled only after a routing update is complete.

Precautions

It is recommended that a loopback address be configured for an router in the NSSA so that the loopback address can be automatically selected as the FA. If other routers have routes of the same cost to the router in the NSSA, load balancing is performed.

When the last ordinary area (other than a stub area or NSSA) under an OSPF process is deleted, useless Type 5 LSAs originated by the local router in the area where are flooded will be deleted immediately. The local router still reserves useless Type 5 LSAs from other routers. These useless Type 5 LSAs will be deleted only when the aging time reaches 40s.

Example

Configure area 1 as an NSSA.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] area 1
[Huawei-ospf-1-area-0.0.0.1] nssa
```

Related Topics

9.4.8 default-cost (OSPF Aera)

9.4.68 opaque-capability enable

Function

The **opaque-capability enable** command enables the Opaque-LSA capability so that an OSPF process can generate Opaque LSAs, and receive Opaque LSAs from neighbors.

The **undo opaque-capability** command disables the Opaque-LSA capability.

By default, the Opaque-LSA capability is disabled.

Format

opaque-capability enable

undo opaque-capability

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Enabling or disabling the Opaque-LSA capability function can delete and reestablish all sessions and instances.

Example

Enable OSPF Opaque.

```
<Huawei> system-view
[Huawei] ospf
[Huawei-ospf-1] opaque-capability enable
```

Related Topics

9.4.69 ospf

9.4.69 ospf

Function

The **ospf** command creates and run an OSPF process.

The **undo ospf** command terminates an OSPF process.

By default, OSPF is disabled, that is, no OSPF process runs.

Format

ospf [*process-id* | **router-id** *router-id* | **vpn-instance** *vpn-instance-name*] *

undo ospf *process-id* [**flush-waiting-timer** *time*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535. By default, it is 1.
router-id *router-id*	Specifies a router ID.	It is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
flush-waiting-timer *time*	Indicates the interval for generating aged LSAs. The parameter takes effect only when it is set.	The value is an integer that ranges from 1 to 40, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set OSPF parameters only after creating an OSPF process.

OSPF supports multi-process. More than one OSPF process can run on the same device, and is independent of each other. Route interaction between different OSPF processes is similar to route interaction between different routing protocols.

The ID of an OSPF device can be configured manually. If no ID is specified through a command for an OSPF device, the system automatically selects an IP address of the interface as the router ID. The IP addresses of loopback interfaces are sequenced in descending order, and then the IP addresses of non-loopback interfaces are also sequenced in descending order. Among these IP addresses, the second largest one is selected as the router ID. If a router ID conflict occurs on a device, the conflicting IP address will be removed from the preceding sequence.

In any of the following situations, the router ID is re-selected:

- The **ospf** command is used to re-configure an OSPF router ID, and then the OSPF process is restarted.
- The system router ID is re-configured, and then the OSPF process is restarted.
- The IP address of the original system router ID is deleted, and then the OSPF process is restarted.

Configuration Impact

After an OSPF process is disabled by using **undo ospf** command, the receive end still maintains the LSAs generated by this OSPF process. These invalid LSAs occupy the system memory and are deleted only when the LS age field (aging time) reaches 3600 seconds. When the **undo ospf** *process-id* **flush-waiting-timer** *time* command is used to stop an OSPF process, the router regenerates an LSA in the

set time and sets the LS age field to 3600 seconds. After other routers receive the LSA with the LS age field as 3600 seconds, they delete the LSA immediately. If the host does not send all the LSAs in the set time, other routers still reserve invalid LSAs.

NOTE

When the LS age field (aging time) in the LSA header reaches 3600 seconds, this LSA is deleted.

Precautions

An interface on a device belongs to only one OSPF process.

If a VPN instance is specified, the OSPF process specified in this command belongs to this VPN instance. If no VPN instance is specified, the OSPF process specified in this command belongs to the global VPN instance. *vpn-instance-name* cannot be changed after being specified.

NOTE

The router ID of each OSPF process must be unique on the entire network; otherwise, the OSPF neighbor relationship cannot be set up and routing information is incorrect. Configuring a unique router ID for each OSPF process on each OSPF device is recommended.

Example

Run an OSPF process.

```
<Huawei> system-view
[Huawei] ospf 100 router-id 10.10.10.1 vpn-instance huawei
```

9.4.70 ospf authentication-mode

Function

The **ospf authentication-mode** command sets the authentication mode and password used between neighboring nodes.

The **ospf authentication-mode null** command configures the null authentication mode on an interface.

The **undo ospf authentication-mode** command deletes the authentication mode on an interface.

By default, an interface does not authenticate OSPF packets.

Format

ospf authentication-mode { **simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | **null** }

ospf authentication-mode { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }]

ospf authentication-mode keychain *keychain-name*

undo ospf authentication-mode

Parameters

Parameter	Description	Value
simple	Indicates simple authentication. In simple authentication, the password type is **cipher** by default. **NOTICE** Simple authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
plain	Indicates plain authentication. Only plain text can be entered, and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This carries security risks. It is recommended that you select **cipher** to save the password in cipher text.	When **cipher** is configured, enter only the password in plain text. Then, the password is displayed in plain text in configuration files. Simple authentication uses the password in plain text by default.
plain-text	Specifies a plain text password.	*plain-text* is a string of 1 to 8 characters without spaces when **simple** is configured, and is a string of 1 to 255 characters without spaces when **md5**, **hmac-md5** or **hmac-sha256** is configured.
cipher	Indicates cipher authentication. Either plain text or cipher text can be entered, and cipher text is displayed when the configuration file is viewed.	When **cipher** is configured, enter only the password in cipher text. Then, the password is displayed in cipher text in configuration files. MD5 authentication, HMAC-SHA256 authentication or HMAC-MD5 authentication uses the password in cipher text by default.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher-text	Specifies a cipher text password.	The value is a string of characters without spaces. In simple authentication, a plain text password is a string of 1 to 8 characters and a cipher text password is a string of 48, 24 or 32 characters. In MD5 authentication, HMAC-SHA256 authentication or HMAC-MD5 authentication, a plain text password is a string of 1 to 255 characters and a cipher text password is a string of 20 to 392 characters.
md5	Indicates MD5 authentication. **NOTICE** MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates HMAC-MD5 authentication. **NOTICE** HMAC-MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates HMAC-SHA256 authentication.	-
key-id	Specifies the authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
null	Indicates null authentication.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to the defects and non-strict implementation of the TCP/IP protocol suite and increasing attacks on TCP/IP networks, the impact generated by attacks on the network may become more serious. Attacks on network devices may lead to a network crash. To improve OSPF network security, configure authentication.

Configuration Impact

Interface authentication is used to set the authentication mode and password used between neighboring devices. It takes precedence over area authentication.

Precautions

Null authentication is an authentication method. It does not indicate that no authentication is configured.

The authentication mode and password configured for interfaces on the same network segment must be the same.

OSPF does not support the configuration on the null interface.

An authentication password does not contain spaces.

Example

Configure OSPF HMAC-SHA256 authentication on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf authentication-mode hmac-sha256
```

Related Topics

9.4.4 authentication-mode (OSPF area)

9.4.71 ospf bfd

Function

The **ospf bfd** command enables the BFD on the specified interface enabled with OSPF, or sets the parameter values of a BFD session.

The **undo ospf bfd** command deletes the BFD on the specified interface, or restores the default parameter values of a BFD session.

By default, BFD is not enabled or configured at OSPF interface view.

Format

ospf bfd enable

undo ospf bfd enable

ospf bfd { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* } * (AR100&AR120&AR150&AR160&AR200 series)

ospf bfd { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } * (AR1200&AR2200 &AR3200 series)

undo ospf bfd { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] } * (AR100&AR120&AR150&AR160&AR200 series)

undo ospf bfd { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] | **frr-binding** } * (AR1200&AR2200&AR3200 series)

Parameters

Parameter	Description	Value
enable	Enables BFD.	-
min-rx-interval *receive-interval*	Indicates the minimum interval at which BFD packets are received from the remote end.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-tx-interval *transmit-interval*	Indicates the minimum interval at which BFD packets are sent to the remote end.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
detect-multiplier *multiplier-value*	Specifies the local detection multiplier. **NOTE** After BFD is enabled, OSPF establishes BFD sessions only with neighbors in the Full state.	The value is an integer ranging from 3 to 50. By default, it is 3.
frr-binding	Binds the BFD session status and the link status of an interface. That is, when the BFD status goes Down, the link status of the interface also goes Down. This enables traffic to be switched to the backup path. **NOTE** The AR100&AR120&AR150&AR160&AR200 series does not support **frr-binding** parameter.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The link failure or the topology change causes devices to re-calculate routes. Therefore, the convergence of routing protocols must be sped up to improve the network performance.

Link faults are unavoidable. Therefore, a feasible solution is required to detect faults faster and notify the faults to routing protocols immediately. If BFD is associated with routing protocols, once a link fault occurs, BFD can speed up the convergence of routing protocols.

OSPF IP FRR requires the low layer to fast respond to the link change. Traffic, therefore, can be rapidly switched to the backup link when a link fails. After the **frr-binding** parameter is configured, the BFD status is bound to the link status of an interface. Specifically, when the BFD status goes Down, the link status of the interface also goes Down. This ensures that faults are detected quickly.

Prerequisites

The configured parameters of the BFD session are valid on an interface only when BFD is enabled on the interface.

Procedure

The *receive-interval* is obtained through the negotiation between the local end and peer end by comparing the values of the local **min-rx-interval** and the peer **min-tx-interval**. If the local end fails to receive a BFD packet from the peer end within an interval of *receive-interval* × *multiplier-value*, it considers that the neighbor is Down.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

If global BFD is not enabled, you can enable BFD on an interface but cannot set up BFD sessions. Similarly, if only parameters of a BFD session are set but the **ospf bfd enable** command is not used, the BFD session cannot be set up.

BFD configured on an interface take precedence over BFD configured in a process. If BFD is enabled on an interface, the BFD parameters on the interface are used to establish BFD sessions.

Precautions

- After BFD is enabled, OSPF establishes BFD sessions only with neighbors.
- The **ospf bfd enable** command and the **ospf bfd block** command are mutually exclusive.
- After BFD is disabled from an interface through the **undo ospf bfd enable** command, the parameters for setting up BFD sessions remain on this interface but do not take effect.

Example

Enable BFD on GE1/0/0 and specify the minimum interval for receiving BFD packets to 400 ms and the local detection multiplier to 4.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf bfd enable
[Huawei-GigabitEthernet1/0/0] ospf bfd min-rx-interval 400 detect-multiplier 4
```

Related Topics

9.4.6 bfd all-interfaces (OSPF)

9.4.72 ospf bfd block

9.4.47 frr (OSPF)

9.4.57 loop-free-alternate (OSPF FRR)

9.4.72 ospf bfd block

Function

The **ospf bfd block** command prevents an interface from dynamically setting up a BFD session.

The **undo ospf bfd block** command cancels the configuration.

By default, the device does not prevent an interface from dynamically setting up a BFD session.

Format

ospf bfd block

undo ospf bfd block

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **bfd all-interfaces enable** command is used for an OSPF process, BFD sessions are created on all the OSPF interfaces whose neighbor status is Full. You can run the **ospf bfd block** command on interfaces where BFD is not required to prevent the interfaces from dynamically setting up BFD sessions.

Prerequisites

BFD is enabled on interfaces.

Precautions

The **ospf bfd enable** command and the **ospf bfd block** command are mutually exclusive.

Example

Prevent GE1/0/0 from dynamically setting up a BFD session.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf bfd block
```

Related Topics

9.4.71 ospf bfd

9.4.6 bfd all-interfaces (OSPF)

9.4.73 ospf cost

Function

The **ospf cost** command sets the cost of an OSPF on an interface.

The **undo ospf cost** command restores the default cost for OSPF.

By default, the cost of an interface running OSPF is calculated using the following formula: **Interface cost = Bandwidth reference value/Interface bandwidth** where, the bandwidth reference value can be changed using the **bandwidth-reference** command. The default cost of lookback interface is 0.

Format

ospf cost *cost*

undo ospf cost

Parameters

Parameter	Description	Value
cost	Specifies the cost of an OSPF-enabled interface.	The value is an integer ranging from 1 to 65535.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF can automatically calculate the link cost for an interface based on the interface bandwidth. You can also set the link cost for the interface through **ospf cost** commands.

Load balancing can be performed among several routes with the same protocol, cost, and destination address. According to the actual networking condition, you can determine whether to perform load balancing by changing the cost of the interface.

Configuration Impact

If no cost is set for an OSPF interface through the **ospf cost** command, OSPF automatically calculates its cost based on the interface bandwidth. The calculation formula is as follows: Cost of the interface = Bandwidth reference value/Interface bandwidth. The integer of the calculated result is the cost of the interface. If the calculated result is smaller than 1, the cost is 1. Changing the bandwidth reference value can change the cost of an interface.

By default, the bandwidth reference value is 100 Mbit/s divided by the interface bandwidth. With the formula 100000000/Bandwidth, the default costs of the Ethernet (100 Mbit/s) interface is 1.

With the formula 100000000/Bandwidth, the default costs of various types of interfaces are as follows:

- 56 kbit/s Serial port: 1785
- 64 kbit/s Serial port: 1562
- E1 (2.048 Mbit/s): 48
- Ethernet (100 Mbit/s): 1

 Copyright © Huawei Technologies Co., Ltd.

NOTE

No default cost is configured for trunk interfaces, because a trunk interface has multiple member interfaces that are in constant change.

Precautions

The **ospf cost** command cannot run on null interfaces.

Example

Set the cost of GE1/0/0 that runs OSPF to 65.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf cost 65
```

Related Topics

9.4.5 bandwidth-reference (OSPF)

9.4.74 ospf dr-priority

Function

The **ospf dr-priority** command sets the priority of the interface that participates in the DR election.

The **undo ospf dr-priority** command restores the default setting.

By default, the priority is 1.

Format

ospf dr-priority *priority*

undo ospf dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the interface that participates in the DR or BDR election. The greater the value, the higher the priority.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DR priority of an interface determines whether it is qualified to be a DR. The interface with the highest DR priority is elected as the DR. If the DR priority of an interface on a device is 0, the device cannot be elected as a DR or a BDR. On a broadcast or NBMA network, you can set the DR priority of an interface to determine whether it is qualified to be a DR or a BDR.

Configuration Impact

When the DR and BDR are elected on a network segment, they send DD packets to all neighboring nodes and set up adjacencies with all neighboring nodes.

Precautions

NOTICE

Restarting or shutting down an interface will interrupt the OSPF adjacency between devices. Therefore, perform the operation with caution.

If the DR priority of a device is re-configured, the DR or BDR on the network will not be re-elected. You can re-elect a DR or a BDR by using either of the following methods. This, however, will interrupt the OSPF adjacency between devices. Therefore, use the following methods with caution.

- Restart the OSPF processes on all devices.
- Run the **shutdown** and then **undo shutdown** commands on the interfaces where OSPF adjacencies are set up.

In OSPF, the DR priority cannot be configured for null interfaces.

Example

Set the priority of GE1/0/0 that participates in the DR election to 8.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf dr-priority 8
```

9.4.75 ospf enable

Function

The **ospf enable** command enables OSPF on an interface.

The **undo ospf enable** command disables OSPF on an interface.

By default, the interface does not run the OSPF.

Format

ospf enable [*process-id*] **area** *area-id*

undo ospf enable [*process-id*] **area** *area-id*

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535. The default value is 1.
area *area-id*	Specifies an area ID.	The value can be a decimal integer or an IP address. When the value is an integer, the value ranges from 0 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ospf enable** command configuration takes precedence over the **network** command configuration.

After the **undo ospf enable** command is run to disable OSPF on an interface, the **network** configuration takes effect on the interface automatically.

Configuration Impact

The interface will alternate between up and down when the **ospf enable** command and the **network** command are run on the interface repeatedly.

Precautions

An interface can be configured with only one OSPF process.

The configured interface and the OSPF process must be in the same VPN.

- The **ospf enable** command can be configured on an interface before an OSPF process is created. The interface specified by the **ospf enable** command and the created OSPF process must be in the same VPN.
- If a process is created before the **ospf enable** command is run on an interface, the process of the interface and existing process must belong to the same VPN. Otherwise, the **ospf enable** command cannot be run.
- If no OSPF process is created, interfaces belonging to different VPN instances cannot be added to the same OSPF process.

Example

Enable GE1/0/0 in the specified OSPF area.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf enable 1 area 0
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.4.65 network (OSPF Area)

9.4.76 ospf filter-lsa-out

Function

The **ospf filter-lsa-out** command configures the specified interface enabled with OSPF to filter outgoing LSAs.

The **undo ospf filter-lsa-out** command configures a router not to filter outgoing LSAs.

By default, outgoing LSAs are not filtered.

Format

ospf filter-lsa-out { **all** | { **summary** [**acl** { *acl-number* | *acl-name* }] | **ase** [**acl** { *acl-number* | *acl-name* }] | **nssa** [**acl** { *acl-number* | *acl-name* }] } * }

undo ospf filter-lsa-out

Parameters

Parameter	Description	Value
all	Filters all outgoing LSAs except grace LSAs.	-
summary	Filters outgoing network summary LSAs (Type 3).	-
ase	Filters outgoing AS external LSAs (Type 5).	-
nssa	Filters outgoing NSSA LSAs (Type 7).	-
acl *acl-number*	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl *acl-name*	Specifies the name of a Named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When multiple links exist between two routers, based on the filtering policy, the **ospf filter-lsa-out** command configures the local router to filter the outgoing LSAs before sending them along specified links. This can reduce the unnecessary retransmission of LSAs and save bandwidth resources.

Configuration Impact

Filtering the outgoing LSAs on the specified OSPF interface can prevent useless LSAs from being sent to neighbors. This can reduce the size of the LSDB of neighbors and speed up the network convergence.

NOTE

After the command is configured on an interface, the OSPF neighbor relationship of the interface will automatically re-establish.

The command takes effect only on the interfaces on which it is run and must be run on both local and remote interfaces. The LSAs that have been sent are aged in 3600s.

Precautions

When the **rule** command is used to configure the filtering rules for a named ACL configured using the **acl** command, only the source address range that is specified by the **source** parameter and the period of time that is specified by the **time-range** parameter take effect.

Grace LSAs are used to inform the neighbor of the Graceful Restart (GR) time, cause, and interface instance ID when GR starts and ends. The command is not used to filter the grace LSAs.

Example

Configure GE1/0/0 to filter all outgoing LSAs except grace LSAs.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf filter-lsa-out all
```

9.4.77 ospf frr block

Function

The **ospf frr block**, you can block FRR on a specified OSPF interface.

The **undo ospf frr block** command restores the default configuration.

By default, FRR is not blocked on an interface.

NOTE

AR100&AR120&AR150&AR160&AR200 series does not support this command.

Format

ospf frr block

undo ospf frr block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF IP FRR can be disabled using the **ospf frr block** command on an interface of a specific device that is running important services and resides on an FRR backup link. This setting prevents the device connected to this interface from being a part of a backup link and being burdened after FRR switches traffic to the backup link.

Precautions

Before configuring OSPF IP FRR, you need to run the **ospf frr block** command to block FRR on a specified interface. In this manner, the link where the interface resides is not calculated as a backup link during FRR calculation.

Example

Block OSPF IP FRR on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf frr block
```

Related Topics

9.4.47 frr (OSPF)

9.4.57 loop-free-alternate (OSPF FRR)

9.4.78 ospf maxage-lsa auto-protect disable

Function

The **ospf maxage-lsa auto-protect disable** command disables master/slave board switching triggered by abnormal OSPF LSA aging.

The **undo ospf maxage-lsa auto-protect disable** command enables master/slave board switching triggered by abnormal OSPF LSA aging.

By default, master/slave board switching triggered by abnormal OSPF LSA aging is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

ospf maxage-lsa auto-protect disable

undo ospf maxage-lsa auto-protect disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the local device's aging timer expires, the local device incorrectly clears all Router LSAs from the peer device, which causes route flapping and service interruptions. To resolve this issue, master/slave board switching triggered by abnormal OSPF LSA aging is automatically enabled. Master/Slave board switching is triggered to restore network connections and service traffic when the following condition is met:

(Number of incorrectly cleared Router LSAs/Total number of Router LSAs) x 100% ≥ 80% (Router LSAs are those sent by the peer device to the local device)

By default, master/slave board switching triggered by abnormal OSPF LSA aging is enabled. To disable master/slave board switching triggered by abnormal OSPF LSA aging, run the **ospf maxage-lsa auto-protect disable** command.

Example

Disable master/slave board switching triggered by abnormal OSPF LSA aging.

```
<Huawei> system-view
[Huawei] ospf maxage-lsa auto-protect disable
```

9.4.79 ospf mib-binding

Function

The **ospf mib-binding** command binds an OSPF process to SNMP and make OSPF respond to SNMP requests.

The **undo ospf mib-binding** command disables the binding.

By default, OSPF processes are not bound to SNMP.

Format

ospf mib-binding *process-id*

undo ospf mib-binding

Parameters

Parameter	Description	Value
process-id	Specifies the OSPF process ID.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The OSPF MIB is a virtual database of the device status maintained by the managed devices.

When multiple OSPF processes are started, you can specify which OSPF process is processed by the OSPF MIB. That is, you can bind the OSPF MIB to a specified OSPF process.

Prerequisites

An OSPF process has been created using the **ospf** command in the system view.

Example

Bind OSPF process 100 to SNMP.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] quit
[Huawei] ospf mib-binding 100
```

Disable the binding.

```
<Huawei> system-view
[Huawei] undo ospf mib-binding
```

Related Topics

9.4.17 display ospf brief

9.4.80 ospf mtu-enable

Function

The **ospf mtu-enable** command enables an interface to add its actual MTU in DD packets to be sent and check whether the MTU in a received DD packet is greater than the local MTU.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ospf mtu-enable** command restores the default settings.

By default, an interface adds the MTU 0 (not the actual MTU) in DD packets to be sent and does not check the MTUs in received DD packets.

Format

ospf mtu-enable

undo ospf mtu-enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve compatibility with a non-Huawei device, an OSPF-enabled Huawei device adds the MTU 0 in DD packets to be sent and does not check the MTUs in received DD packets, allowing an OSPF neighbor relationship to be set up even if the two ends have different MTU settings.

However, under the default configuration, the non-Huawei device may discard an OSPF packet received from the Huawei device if the packet's actual MTU is greater than the MTU of the non-Huawei device. If the discarded packet is an LSU, an OSPF neighbor relationship can still be set up, but the route carried in the LSU fails to be learned, causing service interruptions.

To resolve this issue, run the **ospf mtu-enable** command to configure an interface to add the actual MTU in DD packets to be sent and check whether the MTU in a received DD packet is greater than the local MTU. If the interface MTU settings of the local and remote ends are different, an OSPF neighbor relationship cannot enter the Full state. In this manner, MTU inconsistency can then be identified in time.

Precautions

OSPF does not support configuration on the Null interface.

After the command is configured, the system automatically restarts the OSPF process.

Example

Set GigabitEthernet1/0/0 to fill in the MTU field when sending DD packets.

```
<Huawei> system-view
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf mtu-enable
```

9.4.81 ospf network-type

Function

The **ospf network-type** command sets the network type of the OSPF interface.

The **undo ospf network-type** command restores the default network type of the OSPF interface.

By default, the network type of an interface is determined by the physical interface. The network type of Ethernet interface is **broadcast**, that of the serial interface (encapsulated with PPP or HDLC) is **p2p**, and that of ATM interface and Frame-relay interface is **nbma**.

Format

ospf network-type { **broadcast** | **nbma** | **p2mp** | **p2p** [**peer-ip-ignore**] }

undo ospf network-type

Parameters

Parameter	Description	Value
broadcast	Indicates that the network type of the interface is changed to broadcast.	-
nbma	Indicates that the network type of the interface is changed to NBMA.	-
p2mp	Indicates that the network type of the interface is changed to point-to-multipoint.	-
p2p	Indicates that the network type of the interface is changed to point-to-point.	-
peer-ip-ignore	Disables network segment check when IP address unnumbering is not configured for a P2P interface changed from a broadcast interface and the interface tries to establish an OSPF neighbor relationship. By default, if **peer-ip-ignore** is not specified in the command, OSPF checks the network segment of the two ends during which an OSPF neighbor relationship is to be established. Specifically, OSPF performs an AND operation on the local subnet mask and the local IP address and on the local subnet mask and the remote IP address. An OSPF neighbor relationship can be established only when the results on the two ends are the same.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When link layer protocols remain unchanged, you can change network types and configure OSPF features to flexibly build networks.

- In the broadcast network, if there is a device that does not support multicast address, you can change the network type of the interface to NBMA.
- If the network type of the interface is NBMA, when the interface type is changed to broadcast, the neighboring device is not needed.

The condition for changing a NBMA network to broadcast network is that there should be a direct virtual circuit between any two devices. The network should be a full mesh network. If a network does not meet the preceding conditions, you must change the type of network to point-to-multipoint. In this manner, two indirect devices can communicate with the help of one or two direct and reachable devices. Instead of configuring the neighboring device, you can change the network type of the interface to point-to-multipoint.

If there are only two devices that run OSPF in the same network segment, the network type of an interface can be changed to p2p.

Precautions

- OSPF does not support the configuration on the Null interface.
- When the network type of an interface is NBMA, or the network type of an interface is changed to NBMA manually, you must run the **peer** command to configure the neighbor.
- If the network type of an OSPF interface is NBMA, OSPF does not advertise the interface's information to RSVP-TE, and TE tunnels passing through this interface fail to go Up.
- Generally, the network types of two OSPF interfaces on the both ends of the link must be identical. Otherwise, the two interfaces cannot set up the neighbor relationship.
- When the network type of one OSPF interface is broadcast and the network type of the other OSPF interface is P2P or P2MP, the two interfaces can still set up the neighbor relationship, but cannot learn the OSPF routing information each other.

Example

Set network type of GE1/0/0 to NBMA.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf network-type nbma
```

Related Topics

9.4.95 peer (OSPF)

9.4.74 ospf dr-priority

9.4.82 ospf p2mp-mask-ignore

Function

The **ospf p2mp-mask-ignore** command configures the device not to check the network mask on a Point-to-Multipoint (P2MP) network.

The **undo ospf p2mp-mask-ignore** command configures the device to check the network mask on a P2MP network.

By default, no device on a P2MP network checks the network mask.

Format

ospf p2mp-mask-ignore

undo ospf p2mp-mask-ignore

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

OSPF checks the network masks carried in Hello packets. If the network mask carried in a received Hello packet is not the same as the network mask of the local device, the Hello packet is discarded.

On a P2MP network, when the mask lengths of devices are different, you can use the **ospf p2mp-mask-ignore** command not to check the network mask in Hello packets. In this manner, the OSPF neighbor relationship can be established.

Prerequisites

Because P2MP is not a link layer protocol, each P2MP network is forcibly changed from a network of another type. A common P2MP network is changed from a non-fully connected Non-Broadcast Multi-Access (NBMA) network through the **ospf network-type p2mp** command.

Example

Configure the device not to check the network mask on a P2MP network.

```
<Huawei> system-view
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf network-type p2mp
[Huawei-GigabitEthernet1/0/0] ospf p2mp-mask-ignore
```

Related Topics

9.4.81 ospf network-type

9.4.83 ospf router-id auto-recover disable

Function

Using the **ospf router-id auto-recover disable** command, you can disable automatic recovery that will take effect after router ID conflict is detected.

Using the **undo ospf router-id auto-recover disable** command, you can enable automatic recovery that will take effect after router ID conflict is detected.

By default, automatic recovery takes effect after router ID conflict occurs.

Format

ospf router-id auto-recover disable

undo ospf router-id auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If router ID conflict occurs in an OSPF area, the system can define a new router ID, preventing route flapping and reducing route calculation operations. Other protocols will not go Down when the CPU usage is controlled.

NOTE

- If the automatic recovery function is enabled and a router ID conflict occurs between indirectly connected routers in one OSPF area, the system replaces the conflicted router ID with a newly calculated one. The automatic recovery function takes effect on both configured and automatically generated router IDs.
- The system can replace a router ID in a maximum of three attempts in case the router ID conflict persists.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable automatic recovery that will take effect after router ID conflict is detected.

```
<Huawei> system-view
[Huawei] ospf router-id auto-recover disable
```

9.4.84 ospf smart-discover

Function

The **ospf smart-discover** command enables smart-discover on an interface.

The **undo ospf smart-discover** command disables smart-discover on an interface.

By default, smart-discover is disabled on interfaces.

Format

ospf smart-discover

undo ospf smart-discover

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, devices periodically send Hello packets through OSPF interfaces. By sending Hello packets, devices set up and maintain neighbor relationships, and elect the DR and BDR on the multi-access network (broadcast or NBMA network). When setting up neighbor relationships or electing the DR and BDR on the multi-access network, interfaces can send Hello packets only when the Hello timer expires. This slows down the establishment of neighbor relationships and election of the DR and BDR.

After smart-discover is configured, when the status of the neighbor relationship changes or the DR and BDR on the multi-access network changes, the device can send Hello packets to its neighbor immediately without waiting for the expiration of the Hello timer.

Procedure

On broadcast and NBMA networks, neighbor relationships can be rapidly set up and a DR and a BDR can be rapidly elected.

 Copyright © Huawei Technologies Co., Ltd.

- When the neighbor status becomes 2-way for the first time or returns to Init from the 2-way or higher state, the smart-discover-enabled interface sends Hello packets to a neighbor without waiting for the expiration of the Hello timer when detecting that the neighbor status changes.
- When the status of the interface functioning as the DR or BDR on the multi-access network changes, the smart-discover-enabled interface actively sends Hello packets on the network segment and then participates in the DR or BDR election.

The principle of setting up adjacencies rapidly on P2P or P2MP networks is the same as that on broadcast and NBMA networks.

Configuration Impact

The interval for sending Hello packets on an interface is determined by the interval for sending Hello packets set on the interface.

Precautions

The default interval for sending Hello packets varies with the network type.

Example

Enable smart-discover on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf smart-discover
```

9.4.85 ospf suppress-flapping peer

Function

The **ospf suppress-flapping peer** command configures detection parameters for OSPF neighbor relationship flapping suppression.

The **undo ospf suppress-flapping peer** command restores the default detection parameters.

By default, the detection interval of OSPF neighbor relationship flapping suppression is 60s, the suppression threshold is 10, and the interval for exiting from suppression is 120s.

Format

ospf suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } *

undo ospf suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } *

Parameters

Parameter	Description	Value
detecting-interval *detecting-interval*	Specifies the detection interval of OSPF neighbor relationship flapping suppression. Each OSPF interface on which OSPF neighbor relationship flapping suppression is enabled starts a flapping counter. If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping-count increases by 1.	The value is an integer ranging from 1 to 300, in seconds. The default value is 60s.
threshold *threshold*	Specifies the threshold of OSPF neighbor relationship flapping suppression. When the flapping-count reaches or exceeds *threshold*, flapping suppression takes effect.	The value is an integer ranging from 1 to 1000. The default value is 10.
resume-interval *resume-interval*	Specifies the interval for exiting from OSPF neighbor relationship flapping suppression. If the interval between two successive neighbor status changes from Full to a non-Full state is longer than *resume-interval*, the flapping-count is reset. **NOTE** The value of *resume-interval* must be greater than that of *detecting-interval*.	The value is an integer ranging from 2 to 1000, in seconds. The default value is 120s.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure detection parameters for OSPF neighbor relationship flapping suppression on an interface, run the **ospf suppress-flapping peer** command. However, keeping the default configurations is recommended.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you configure detection parameters for it. By default, the function is

enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the detection parameters.

Example

Set the detection interval of OSPF neighbor relationship flapping suppression to 5s, the suppression threshold to 40, and the interval for exiting from suppression to 20s on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf suppress-flapping peer detecting-interval 5 threshold 40 resume-interval 20
```

Related Topics

9.4.114 suppress-flapping peer disable (OSPF)

9.4.86 ospf suppress-flapping peer disable

Function

The **ospf suppress-flapping peer disable** command disables OSPF neighbor relationship flapping suppression from an interface.

The **undo ospf suppress-flapping peer disable** command enables OSPF neighbor relationship flapping suppression on an interface.

By default, OSPF neighbor relationship flapping suppression is enabled on all interfaces.

Format

ospf suppress-flapping peer disable

undo ospf suppress-flapping peer disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, OSPF neighbor relationship flapping suppression is enabled on all interfaces in the same OSPF process. To disable the function from one of the interfaces, run the **ospf suppress-flapping peer disable** command.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When an interface enters the flapping suppression state, all neighbor relationships on the interface enter the state accordingly.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you enable the function on an interface using the **undo ospf suppress-flapping peer disable** command. By default, the function is enabled globally. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it first.

Example

Disable OSPF neighbor relationship flapping suppression from GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf suppress-flapping peer disable
```

Related Topics

9.4.114 suppress-flapping peer disable (OSPF)

9.4.87 ospf suppress-flapping peer hold-down

Function

The **ospf suppress-flapping peer hold-down** command configures the Hold-down mode and sets duration for this mode.

The **undo ospf suppress-flapping peer hold-down** command cancels the Hold-down mode.

By default, the Hold-down mode is disabled, and the Hold-max-cost mode is enabled.

Format

ospf suppress-flapping peer hold-down *interval*

undo ospf suppress-flapping peer hold-down [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the duration of the Hold-down mode.	The value is an integer ranging from 1 to 600, in seconds. The default value is 60.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **ospf suppress-flapping peer hold-down** *interval* command.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you configure the Hold-down mode and set duration for this mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the Hold-down mode and set duration for this mode.

Example

Configure the Hold-down mode and set its duration to 200s on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf suppress-flapping peer hold-down 200
```

Related Topics

9.4.114 suppress-flapping peer disable (OSPF)

9.4.88 ospf suppress-flapping peer hold-max-cost disable

9.4.88 ospf suppress-flapping peer hold-max-cost disable

Function

The **ospf suppress-flapping peer hold-max-cost disable** command disables the Hold-max-cost mode.

The **undo ospf suppress-flapping peer hold-max-cost disable** command enables the Hold-max-cost mode.

By default, the Hold-max-cost mode is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

ospf suppress-flapping peer hold-max-cost disable

undo ospf suppress-flapping peer hold-max-cost disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **ospf suppress-flapping peer hold-down** *interval* command.

Prerequisites

OSPF neighbor relationship flapping suppression must have been enabled globally before you configure duration for the Hold-max-cost mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure duration for the Hold-max-cost mode.

Precautions

The Hold-max-cost mode takes effect only unidirectionally. If a remote device does not support OSPF neighbor relationship flapping suppression, bidirectional traffic between the local and remote devices may travel along different paths.

Example

Disable the Hold-max-cost mode on GE1/0/0.

```
<Huawei> system-view
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf suppress-flapping peer hold-max-cost disable
```

Related Topics

9.4.114 suppress-flapping peer disable (OSPF)

9.4.87 ospf suppress-flapping peer hold-down

9.4.89 ospf timer dead

Function

The **ospf timer dead** command sets the dead interval of the OSPF neighbor.

The **undo ospf timer dead** command restores the default dead interval of the neighbor.

By default, for the interface of P2P and Broadcast, the dead interval for the OSPF neighbors is 40 seconds; for that of NBMA and P2MP, it is 120 seconds.

Format

ospf timer dead *interval*

undo ospf timer dead

Parameters

Parameter	Description	Value
interval	Specifies dead interval of the OSPF neighbors.	The value is an integer ranging from 1 to 235926000, in seconds. **NOTE** Setting the dead interval of an OSPF neighbor to be longer than 20s is recommended.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The dead interval of OSPF neighbors refers to that within this interval, if no Hello packet is received from the neighbor, the neighbor is considered as invalid. The dead interval on an OSPF-running interface must be greater than the transmission interval of Hello messages. In addition, the dead intervals of devices on the same network segment must be the same.

 Copyright © Huawei Technologies Co., Ltd.

By default, the dead interval of OSPF neighbors is four times the transmission interval of Hello messages.

Precautions

OSPF does not support the configuration on a null interface.

If the dead interval of an OSPF neighbor is shorter than 20s, the session may be closed. Therefore, if **dead** *interval* is shorter than 20s, the actual dead interval of an OSPF neighbor is not shorter than 20s.

To speed up OSPF convergence in the case of a link failure, configuring Configuring BFD for OSPF is recommended.

Example

Set the dead interval on GE1/0/0 to 60 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf timer dead 60
```

Related Topics

9.4.90 ospf timer hello

9.4.90 ospf timer hello

Function

The **ospf timer hello** command sets the interval for sending Hello packets on an interface.

The **undo ospf timer hello** command restores the default value of the interval.

By default, for the interface of P2P and Broadcast type, the interval for sending Hello packets is 10 seconds; for the interface of NBMA and P2MP type, it is 30 seconds.

Format

ospf timer hello *interval* [**conservative**]

undo ospf timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending the Hello packet on an interface.	The value is an integer ranging from 1 to 65535, in seconds. Setting **hello** *interval* to be longer than or equal to 5s is recommended.

Parameter	Description	Value
conservative	Indicates the conservative mode of the dead timer. If the conservative mode is configured, the value configured for the dead timer using the **ospf timer dead** command takes effect even when the value is less than 20s.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello packets are are periodically sent on OSPF interfaces to establish and maintain neighbor relationships. A Hello packet contains information about timers, DRs, BDRs, and known neighbors.

The smaller the **hello** *interval* is, the faster the changing speed of the network topology is. The cost of routes, however, becomes greater. Ensure that the parameters of this interface and the adjacent routers are consistent.

Precautions

OSPF does not support the configuration on a null interface.

If **hello** *interval* is set but a dead interval is not set using the **ospf timer dead** command, the dead interval of an OSPF neighbor is four times the value of **hello** *interval*. If the dead interval of an OSPF neighbor is shorter than 20s, the session may be closed. Therefore, if **hello** *interval* is shorter than 5s, the actual dead interval of an OSPF neighbor is not shorter than 20s.

To speed up OSPF convergence in the case of a link failure, configuring Configuring BFD for OSPF is recommended.

Example

Set the interval for sending Hello packets on GE1/0/0 to 20 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf timer hello 20
```

Related Topics

9.4.89 ospf timer dead

9.4.91 ospf timer poll

Function

The **ospf timer poll** command sets the poll interval for sending Hello packets on NBMA network.

The **undo ospf timer poll** command restores the default poll interval.

By default, it is 120 seconds.

Format

ospf timer poll *interval*

undo ospf timer poll

Parameters

Parameter	Description	Value
interval	Specifies the poll interval for sending Hello packets.	The value is an integer ranging from 1 to 3600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the NBMA network, if a neighbor is invalid, the device periodically sends the Hello packets to the neighbor according to the poll interval set in the **ospf timer poll** command. The poll interval should be at least 4 times that of the **Hello** interval.

Precautions

OSPF does not support the configuration on a null interface.

Example

Set the poll interval for sending Hello packets on GE1/0/0 to 130 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf timer poll 130
```

9.4.92 ospf timer retransmit

Function

The **ospf timer retransmit** command sets the interval for retransmitting LSA on an interface.

The **undo ospf timer retransmit** command restores the default interval for retransmitting LSA on the interface.

By default, the interval time is 5 seconds.

Format

ospf timer retransmit *interval*

undo ospf timer retransmit

Parameters

Parameter	Description	Value
interval	Specifies interval for retransmitting LSA on an interface.	The value is an integer ranging from 1 to 3600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device transmits an LSA to its neighbor, it has to wait for the ACK packet from the neighbor. If no ACK packet is received from the neighbor in the LSA retransmission interval, this LSA is retransmitted.

You should not set too short LSA retransmission intervals between adjacent routers. Otherwise, it leads to unnecessary retransmission.

Precautions

OSPF does not support the configuration on a Null interface.

Example

Specify the interval for retransmitting LSAs between GE1/0/0 and the adjacent device to 8 seconds.

```
<Huawei> system-view
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf timer retransmit 8
```

9.4.93 ospf trans-delay

Function

The **ospf trans-delay** command adds an extension period for LSAs that are transmitted on an interface.

The **undo ospf trans-delay** command restores the default delay on the interface.

By default, the delay is 1 second.

Format

ospf trans-delay *interval*

undo ospf trans-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay for transmitting LSA on an interface.	The value is an integer ranging from 1 to 500, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LSA ages in LSDB (increase by 1 each second), but LSA does not age during transmission in the network. It is therefore necessary to use this command to set a certain delay before the LSA is transmitted. This configuration is important for a low-speed network.

Precautions

OSPF does not support the configuration on the Null interface.

Example

Specify the delay for transmitting LSA on GE1/0/0 to 3 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf trans-delay 3
```

9.4.94 ospf valid-ttl-hops

Function

The **ospf valid-ttl-hops** command enables OSPF GTSM and set the TTL value to be checked.

The **undo ospf valid-ttl-hops** command disables OSPF GTSM.

By default, OSPF GTSM is disabled.

Format

ospf valid-ttl-hops *hops* [**nonstandard-multicast**] [**vpn-instance** *vpn-instance-name*]

undo ospf valid-ttl-hops [*hops* [**nonstandard-multicast**]] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
hops	Specifies the TTL value to be checked.	The value is an integer that ranges from 1 to 255. The default value is 255.
nonstandard-multicast	Specifies the GTSM configuration is also valid for multicast packets. When the **nonstandard-multicast** parameter is configured: ● The TTL values of the multicast packets which will be sent are set as 255. ● The received multicast packets will be checked for the TTL value 1 or in the range of [255-*hops*+1, 255].	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. If this parameter is specified, it indicates that only the TTL value of the packets in the specified VPN instance needs to be checked.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a network demanding higher security, you can enable GTSM to improve the security of the OSPF network. GTSM defends against attacks by checking the TTL value. If an attacker simulates OSPF unicast packets and keeps sending them to a router, the router receives the packets and directly sends them to the main control board for OSPF processing, without checking the validity of the packets. In this case, the router is busy processing these packets, causing high usage of the CPU. GTSM protects the routers and enhances the system security by checking whether the TTL value in the IP packet header is in a pre-defined range.

The **ospf valid-ttl-hops** command is used to enable OSPF GTSM. The **vpn-instance** parameter must be specified in the command if you need to check the TTL value of packets that match the GTSM policy.

For example, if running the **ospf valid-ttl-hops** command enables OSPF GTSM on both the public network and the private network. If running the **ospf valid-ttl-hops 5 vpn-instance** *vpn1* command, in addition to enabling OSPF GTSM on both the public network and the private network, you can detect the TTL value of OSPF packets in the VPN instance named *vpn1*, configure the default TTL value for packets unmatched with the GTSM policy for the OSPF packets from other instances of the private network and the public nework.

Precautions

- If a VPN instance is specified in the **ospf valid-ttl-hops** command and the interface is bound to the VPN instance, all the unicast packets sent to this interface are dropped when the set number of TTL hops is smaller than the actual number of hops on the network.
- If a virtual link or sham link is configured, the actual TTL value and the configured TTL value must be the same. That means that the number of virtual links or sham links that pass through the router is calculated. Otherwise, packets sent from neighbors of a virtual link or a sham link will be dropped.
- GTSM only checks the TTL values of the packets that match the GTSM policy. If the packets do not match the GTSM policy, you can set the **pass** parameter or **drop** parameter in the **gtsm default-action** command to pass or drop these packets.
- If only a private or public network policy is configured, run the **gtsm default-action** command to set the default behavior for processing the packets unmatched with the GTSM policy to **pass** to prevent the OSPF packets of other instances from being discarded.

Example

Enable OSPF GTSM, and set the maximum number of TTL hops to 5 for the packets that can be received from the public network.

```
<Huawei> system-view
```

```
[Huawei] ospf valid-ttl-hops 5
```

Related Topics

9.4.52 gtsm default-action

9.4.53 gtsm log drop-packet

9.4.95 peer (OSPF)

Function

The **peer** command sets the IP addresses and the DR priority for the adjacent router on an NBMA network.

The **undo peer** command cancels the IP address of the adjacent router on an NBMA network.

By default, the IP addresses and the DR priority for the adjacent router on an NBMA network is not set.

Format

peer *ip-address* [**dr-priority** *priority*]

undo peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address for the adjacent devices.	The value is in dotted decimal notation.
dr-priority *priority*	Sets the priority for the adjacent devices to select a DR.	The value of the priority is an integer that ranges from 0 to 255. By default, it is 1.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

In an NBMA network (such as an X.25 or FR network), the entire network can be fully meshed based on the mapping configuration. That means that there is a virtual link between any two devices. In this case, the network running OSPF can be considered as a broadcast network where a DR or a BDR can be selected. You need, however, manually specify the IP address and the DR priority for the adjacent devices using the **peer** command, because it is impossible to find the adjacent devices dynamically by broadcasting the Hello packet.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the IP address of the adjacent router to 10.1.1.1 in an NBMA network.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] peer 10.1.1.1
```

Related Topics

9.4.27 display ospf peer

9.4.22 display ospf interface

9.4.96 preference (OSPF)

Function

The **preference** command sets the preference of an OSPF route.

The **undo preference** command restores the default preference of the OSPF route.

By default, the preference of the OSPF route is 10. When ASE is specified, the default value is 150.

Format

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Parameters

Parameter	Description	Value
ase	Indicates the preference of the AS external route.	-
preference	Specifies the preference of the OSPF route. The smaller the preference value, the higher the preference.	The value of the preference is an integer ranging from 1 to 255.
route-policy *route-policy-name*	Specifies the name of the route policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Multiple dynamic routing protocols can be run on a router at the same time. In this case, there is a problem of route sharing and selecting among routing protocols. The system sets a default preference for each routing protocol. If different protocols have routes to the same destination, the protocol with the higher preference is selected to forward IP packets. Using this command, you can set the preference of an OSPF route.

You can create a route-policy to set the preference of a specific route by setting the **route-policy** parameter in the **preference** command:

- If the **apply preference** clause is configured for the route-policy, route preference is determined as follows:
  - Route matching the route-policy: Its preference is determined by the **apply** clause.
  - Route that does not match the route-policy: Its preference is determined by the **preference** command.

  In the following example, the preference of the route matching the route-policy **abc** is set to 50 and the preference of the route that does not match the route-policy is set to 30.

```
#
route-policy abc permit node 1
 if-match cost 20
 apply preference 50
#
ospf 1
 preference 30 route-policy abc
```

- If the **apply preference** clause is not included in the route-policy, the preference of routes is set by the **preference** command.

  In the above example, if the **apply preference 50** clause is not included in the policy **abc**, the preference of all routes is set to 30.

Configuration Impact

When there are routes discovered by multiple routing protocols on the same router, you can make the router prefer OSPF routes by setting the OSPF route preference.

Example

Set the preference of routes in OSPF process 100 to 150.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] preference 150
```

Set the preference of external routes in OSPF process 200 to 130.

```
<Huawei> system-view
[Huawei] ospf 200
[Huawei-ospf-200] preference ase 130
```

Related Topics

9.9.53 route-policy

9.4.97 prefix-priority (OSPF)

Function

The **prefix-priority** command sets the convergence priority of OSPF routes.

The **undo prefix-priority** command restores the default convergence priority of OSPF routes.

By default, the convergence priority of public 32-bit host routes is **medium**, and the convergence of other OSPF routes is **low**.

Format

prefix-priority { **critical** | **high** | **medium** } **ip-prefix** *ip-prefix-name*

undo prefix-priority { **critical** | **high** | **medium** }

Parameters

Parameter	Description	Value
critical	Sets the convergence priority of OSPF routes to critical.	-
high	Sets the convergence priority of OSPF routes to high.	-
medium	Sets the convergence priority of OSPF routes to medium.	-
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **prefix-priority** command sets the convergence priority of OSPF routes according to the specified IP prefix list name, and takes effect on the public network only.

After the **prefix-priority** command is used in the OSPF view, OSPF route calculation, link-state advertisement (LSA) flooding, and LSDB synchronization can be implemented according to the configured priority, which accelerates route convergence.

Prerequisites

An IP prefix list has been created using the **ip ip-prefix** command in the system view.

Configuration Impact

When an LSA meets multiple priorities, the highest priority takes effect.

With the **prefix-priority** command, OSPF can calculate and flood LSAs, and synchronize LSDBs according to priorities. This speeds up route convergence. OSPF calculates LSAs in the sequence of intra-area routes, inter-area routes, and AS external routes. This command makes OSPF calculate the three types of routes separately according to the specified route calculation priorities. Convergence priorities are **critical**, **high**, **medium**, and **low**. To speed up the processing of LSAs with the higher priority, during LSA flooding, the LSAs need to be placed into the corresponding **critical**, **high**, **medium**, and **low** queues according to priorities.

Precautions

By default, the convergence priorities of public OSPF host routes, direct routes, static routes, and other protocol (such as BGP and RIP) routes are **medium**, **high**, **medium**, and **low** respectively. In the public network, OSPF 32-bit host routes are uniformly identified as **medium**.

Example

Set the convergence priority of OSPF routes of 10.0.0.0/8 to **critical**.

```
<Huawei> system-view
[Huawei] ip ip-prefix critical-prefix index 10 permit 10.0.0.0 8
[Huawei] ospf 1
[Huawei-ospf-1] prefix-priority critical ip-prefix critical-prefix
```

Related Topics

9.9.47 ip ip-prefix

9.4.98 reset gtsm statistics

Function

The **reset gtsm statistics** command clears the GTSM statistics.

Format

reset gtsm statistics all

Parameters

Parameter	Description	Value
all	Clears the GTSM statistics on LPUs in all slots.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting the GTSM statistic within a certain period, you need to clear the existing statistics.

NOTE

On the router, the **reset gtsm statistics** command can clear the GTSM statistics only on the MPU, but not on LPUs.

Example

Clear the GTSM statistics on all boards.

```
<Huawei> reset gtsm statistics all
```

Related Topics

9.4.13 display gtsm statistics

9.4.99 reset ospf counters

Function

The **reset ospf counters** command resets the OSPF counter.

Format

reset ospf [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

Parameters

Parameter	Description	Value
process-id	Indicates the OSPF process ID. If the parameter is not specified, all OSPF processes are restarted.	The value is an integer ranging from 1 to 65535.

Parameter	Description	Value
neighbor	The statistics of neighbors for the interface.	-
interface-type interface-number	Specifies the type and the number of the interface.	-
router-id	The Router ID of the neighbor.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

When the router restarts an OSPF process, the neighboring router always reserves invalid LSAs. This occupies the memory of the system. These LSAs are deleted only when they expire, that is, when the LS age field in the LSA reaches 3600 seconds. After the **reset ospf** is used to restart an OSPF process and only when the router ID is changed, the router generates an LSA in the set time and sets the LS age field to 3600 seconds. After receiving the LSA, other routers delete the LSA immediately from their LSDBs. If a device does not send all the LSAs within the set time, other neighboring routers still store some invalid LSAs.

Clearing OSPF statistics does not affect the normal operation of OSPF services.

NOTICE

Once deleted, statistics cannot be restored. Therefore, use caution when deleting statistics.

Example

Reset the OSPF counters.

```
<Huawei> reset ospf counters
```

9.4.100 reset ospf counters maxage-lsa

Function

The **reset ospf counters maxage-lsa** command deletes the statistics about router LSAs that have reached the maximum aging time.

Format

reset ospf [*process-id*] **counters maxage-lsa**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

After the statistics about router LSAs that have reached the maximum aging time are deleted, OSPF services are not affected.

NOTICE

Statistics cannot be restored after being deleted, but the statistics about router LSAs that have reached the maximum aging time will not be deleted. Therefore, exercise caution when running the command.

Example

Delete the statistics about router LSAs that have reached the maximum aging time.

```
<Huawei> reset ospf counters maxage-lsa
```

9.4.101 reset ospf process

Function

The **reset ospf process** command restarts the OSPF process.

Format

reset ospf [*process-id*] **process** [**flush-waiting-timer** *time* | **graceful-restart**]

Parameters

Parameter	Description	Value
process-id	Indicates the OSPF process ID. If the parameter is not specified, all OSPF processes are restarted.	The value is an integer ranging from 1 to 65535.
flush-waiting-timer *time*	Specified the time when the LSA is generated. The parameter takes effect only when it is set.	The value is an integer that ranges from 1 to 40, in seconds.
graceful-restart	Indicates that graceful restart is enabled.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset ospf process** command can be used to clear OSPF information to reset the board.

NOTICE

If OSPF connections are reset, OSPF neighbor relationships will be interrupted and the original information cannot be restored. Exercise caution before running the **reset ospf process** command.

Configuration Impact

After the **reset ospf process** command is used to restart OSPF, the following situations may occur:

- If the router ID is changed, a new router ID will take affect after the command is run.
- Re-elect DR and BDR.
- OSPF configuration will not be lost after OSPF restarts.

Precautions

Configuring the **flush-waiting-timer** parameter when OSPF starts, you can clear invalid LSAs within the set time before LSAs time out.

Whether all invalid LSAs on other routers can be deleted is related to the set time.

When the router restarts an OSPF process, the neighboring router always reserves invalid LSAs. This occupies the memory of the system. These LSAs are deleted only

 Copyright © Huawei Technologies Co., Ltd.

when they expire, that is, when the LS age field in the LSA reaches 3600 seconds. After the **reset ospf** is used to restart an OSPF process and only when the router ID is changed, the router generates an LSA in the set time and sets the LS age field to 3600 seconds. After receiving the LSA, other routers delete the LSA immediately from their LSDBs. If a device does not send all the LSAs within the set time, other neighboring routers still store some invalid LSAs.

Example

Restart all OSPF processes.

```
<Huawei> reset ospf process
Warning: The OSPF process will be reset. Continue? [Y/N]: y
```

9.4.102 reset ospf redistribution

Function

The **reset ospf redistribution** command resets OSPF route redistribution.

Format

reset ospf [*process-id*] **redistribution**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process. If this parameter is not specified, all OSPF processes are restarted.	The value is an integer that ranges from 1 to 65535.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset ospf redistribution** command resets OSPF route redistribution to generate Type 5 or Type 7 LSA.

Example

Reset OSPF route redistribution in OSPF process 1.

```
<Huawei> reset ospf 1 redistribution
```

9.4.103 reset ospf suppress-flapping peer

Function

The **reset ospf suppress-flapping peer** command forces an interface to exit from OSPF neighbor relationship flapping suppression.

Format

reset ospf *process-id* **suppress-flapping peer** [*interface-type interface-number*] [**notify-peer**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPF process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies an interface type and number.	-
notify-peer	Instructs neighbors to exit from OSPF neighbor relationship flapping suppression too.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Interfaces exit from flapping suppression in the following scenarios:

- The suppression timer expires.
- The corresponding OSPF process is reset.
- The **reset ospf suppress-flapping peer** command is run.
- OSPF neighbor relationship flapping suppression is disabled globally using the **suppress-flapping peer disable** command in the OSPF view.

If **notify-peer** is specified when the **reset ospf suppress-flapping peer** command is run on a device, the device sends Hello packets in which **HelloInterval** and **RouterDeadInterval** are 0s to its neighbors to instruct the neighbors to exit from OSPF neighbor relationship flapping suppression too. If the neighbors fail to receive such Hello packets, the function of **notify-peer** does not take effect. To force the neighbors to exit from OSPF neighbor relationship flapping suppression, run the **reset ospf suppress-flapping peer** command on them.

 Copyright © Huawei Technologies Co., Ltd.

Example

Force interfaces to exit from OSPF neighbor relationship flapping suppression.

```
<Huawei> reset ospf 1 suppress-flapping peer
```

Related Topics

9.4.114 suppress-flapping peer disable (OSPF)

9.4.104 retransmission-limit

Function

The **retransmission-limit** command enables retransmission limit and set the maximum number of retransmissions.

The **undo retransmission-limit** command disables retransmission limit.

By default, retransmission limit is disabled.

Format

retransmission-limit [*max-number*]

undo retransmission-limit

Parameters

Parameter	Description	Value
max-number	Indicates the maximum number of retransmissions.	The value is an integer that ranges from 2 to 255. The default value is 30.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **retransmission-limit** command can be used to enable Retransmission Limitation for OSPF (RL-for OSPF) to prevent dead loops caused by repeated transmissions when neighbors cannot receive packets.

Configuration Impact

The OSPF retransmission limit can be used in the following packets:

 Copyright © Huawei Technologies Co., Ltd.

- DD packet
- LSU packet
- LSR packet

If the three types of packets cannot receive the response packets, enable the retransmission attribute, limit the count of retransmission, and disconnect the neighbor when the retransmission exceeds the specified count.

Example

Enable OSPf retransmission limit and set the maximum number of retransmissions to 40.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] retransmission-limit 40
```

Related Topics

9.4.29 display ospf retrans-queue

9.4.18 display ospf cumulative

9.4.19 display ospf error

9.4.105 route-tag

Function

The **route-tag** command sets the tag value for imported VPN routes.

The **undo route-tag** command restores the default setting.

By default, the tag value of a VPN route is calculated based on the AS number of BGP. If no BGP is configured, the default tag value is 0.

Format

route-tag { *tag* | **disable** }

undo route-tag

Parameters

Parameter	Description	Value
tag	Specifies the tag value of the imported VPN routes.	The value is an integer ranging from 0 to 4294967295.
disable	Forbids the using of the tag to detect the loop.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **route-tag** command can only be used in VPN scenarios to prevent loops on As-external-LSAs when a CE is dual-homed to two PEs.

In a networking where a CE is dual-homed to two PEs, PE1 generates As-external-LSAs based on the imported BGP routes and sends the LSAs to the CE, then to PE2. Because OSPF routes have higher priorities over BGP routes, the former will replace the latter on PE2, causing loops. After the **route-tag** command is run, if the tag value of the PE and an LSA are the same, the PE will neglect the LSA and a loop is prevented.

By default, the first two bytes of the tag value are fixed as 0xD000, whereas the last two bytes are the AS number of the local BGP. If a BGP AS number is greater than 65535, the default tag 0 is used. You can use the command to change the tag in this case.

Configuration Impact

The route tags of a VPN can be configured only and takes effect on the PEs where BGP routes and received and OSPF LSAs are generated.

Precautions

- Configuring the same VPN route tag on the PEs within the same area is recommended.
- Different OSPF processes can be configured with the same VPN route tag.

The tags set by the **route-tag** command or other commands are different only in preference.

1. The preference of the tag configured using the **import-route** command is the highest.
2. The preference of the tag configured using the **route-tag** command is medium.
3. The preference of the tag configured using the **default tag** command is the lowest.

Example

Set the route tag for OSPF process 100 to 100 in a VPN instance named **huawei**.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] route-distinguisher 100:1
[Huawei-vpn-instance-huawei-af-ipv4] quit
[Huawei-vpn-instance-huawei] quit
[Huawei] ospf 100 vpn-instance huawei
[Huawei-ospf-100] route-tag 100
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.4.54 import-route (OSPF)

9.4.7 default (OSPF)

9.4.106 rfc1583 compatible

Function

The **rfc1583 compatible** command converts rules defined in RFC 2328 into rules defined in RFC 1583.

The **undo rfc1583 compatible** command converts rules defined in RFC 1583 into rules defined in RFC 2328.

By default, OSPF supports the routing rule of RFC 1583.

Format

rfc1583 compatible

undo rfc1583 compatible

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

RFC 2328 and RFC 1583 define different OSPF route selection rules. When enabling OSPF, configure the same route selection rules on all devices in the same OSPF area. For example, an OSPF device supports route selection rules defined in RFC 1583 by default. If the other routers in the same OSPF area support route selection rules defined in RFC 2328, you need to run the **undo rfc1583 compatible**

Example

Converts rules defined in RFC 1583 into rules defined in RFC 2328.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] undo rfc1583 compatible
```

 Copyright © Huawei Technologies Co., Ltd.

9.4.107 sham-hello enable (OSPF)

Function

The **sham-hello enable** command enables the sham-hello function of OSPF.

The **undo sham-hello** command disables the sham-hello feature.

By default, the sham-hello feature is disabled.

Format

sham-hello enable

undo sham-hello

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the device maintains neighbors through not only the Hello packet but also all OSPF protocol packets, so as to sensitively sense the existence of OSPF neighbors and stabilize neighboring relations.

Example

Enable the sham-hello feature.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] sham-hello enable
```

9.4.108 sham-link (OSPF Area)

Function

The **sham-link** command configures a sham link or sets the parameter values of a sham link.

The **undo sham-link** command deletes a sham link or restores the default parameter values of a sham link.

By default, no sham link is configured for OSPF.

 Copyright © Huawei Technologies Co., Ltd.

Format

sham-link *source-ip-address destination-ip-address* [[**simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | { **md5** | **hmac-md5 hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] | **authentication-null** | **keychain** *keychain-name*] | **smart-discover** | **cost** *cost* | **dead** *dead-interval* | **hello** *hello-interval* | **retransmit** *retransmit-interval* | **trans-delay** *trans-delay-interval*] *

undo sham-link *source-ip-address destination-ip-address* [[**simple** | **md5** | **hmac-md5 hmac-sha256** | **authentication-null** | **keychain**] | **smart-discover** | **cost** | **dead** | **hello** | **retransmit** | **trans-delay**] *

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source IP address.	The value is in dotted decimal notation.
destination-ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
smart-discover	Indicates that Hello packets are sent automatically and immediately.	-
simple	Indicates simple authentication. In simple authentication, the password type is **cipher** by default. **NOTICE** Simple authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
plain	Indicates plain authentication. Only plain text can be entered, and only plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This carries security risks. It is recommended that you select **cipher** to save the password in cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
plain-text	Specifies a plain text password.	• In **simple** authentication, the value is a string of 1 to 8 characters without spaces. • In **md5**, **hmac-sha256** or **hmac-md5** authentication, the value is a string of 1 to 255 characters.
cipher	Indicates cipher authentication. Either plain text or cipher text can be entered, and cipher text is displayed when the configuration file is viewed.	-
cipher-text	Specifies a cipher text password.	• In **simple** authentication, the value is a string of 1 to 8 plain text characters and 32, 24 or 4832 cipher text characters. • In **md5**, **hmac-sha256** or **hmac-md5** authentication, the value is a string of 1 to 255 plain text characters and 20 to 392 cipher text characters.
md5	Indicates MD5 authentication. **NOTICE** MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates **hmac-md5** authentication. **NOTICE** HMAC-MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates **HMAC-SHA256** authentication.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-id	Specifies the authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.
authentication-null	Indicates that no authentication is used.	-
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail. Currently, only the **hmac-md5** and **hmac-sha256** algorithms can be used for OSPF.	-
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
cost *cost*	Specifies the cost of the sham link.	The value of the cost is an integer that ranges from 1 to 65535. The default value is 1.
dead *dead-interval*	Specifies the dead interval. This value must be equal to *dead-interval* of the router that sets up a virtual link with the local router, and must be at least four times that of *hello-interval*.	The value of the interval is an integer that ranges from 1 to 23592600, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hello *hello-interval*	Specifies the interval for transmitting Hello packets on an interface. This value must be equal to *hello-interval* of the router that sets up a virtual link with the local router.	The value is an integer that ranges from 1 to 65535, in seconds.
retransmit *retransmit-interval*	Specifies the interval for retransmitting the LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds.
trans-delay *trans-delay-interval*	Specifies the delay in transmitting LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sham-link** command can only be used in VPN scenarios.

This command can create a sham link to allow VPN traffic to be preferentially forwarded through routes within the backbone area. This prevents traffic from the same VPN in the same OSPF area from being forwarded through intra-area OSPF routes.

Before enabling neighbors of a sham link to set up adjacencies quickly, configure the **smart-discover** parameter to actively send Hello packets immediately.

Configuration Impact

After a sham link is configured between two PEs, the sham link is considered as an intra-area OSPF route. This configuration enables a route passing through an MPLS VPN backbone network to become an intra-area OSPF route, preventing VPN traffic from being transmitted through this route. A 32-bit loopback interface address is specified as the source and destination addresses of the sham link. The loopback interface must be bound to a VPN instance and advertised using BGP.

NOTE

The AR100&AR120&AR150&AR160&AR200 do not support MPLS.

Precautions

The route to the endpoint address of a sham link cannot be advertised to the remote PE using an OSPF process in a private network. Otherwise, two routes to

the endpoint address of the sham link exist on the remote PE. One route is learned from the OSPF process and the other is learned using MP-BGP. OSPF routes have higher priorities over BGP routes, so the remote PE select an incorrect OSPF route. As a result, the sham link cannot be created.

Example

Create a sham link with the source address 10.1.1.1 and destination address 10.2.2.2 in a VPN instance named **huawei**.

```
<Huawei> system-view
[Huawei] ospf 1 vpn-instance huawei
[Huawei-ospf-1] area 1
[Huawei-ospf-1-area-0.0.0.1] sham-link 10.1.1.1 10.2.2.2
```

Related Topics

9.4.31 display ospf sham-link

9.4.109 silent-interface (OSPF)

Function

The **silent-interface** command disables an interface from receiving and sending OSPF packets.

The **undo silent-interface** command restores the default setting.

By default, the interface is permitted to receive or send OSPF packet.

Format

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type* [*interface-number*] }

Parameters

Parameter	Description	Value
all	Indicates all interfaces in a specified process.	-
interface-type interface-number	Specifies the interface type and the interface number.	-

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that OSPF routing information cannot be obtained by the devices of a certain network and the local device does not receive routing update information advertised by other devices, you can run the **silent-interface** command to disable an interface from receiving and sending OSPF packets.

Disabling interfaces from receiving or sending OSPF packets is a solution to routing loops.

Configuration Impact

After an OSPF interface is set to be in the silent state, the interface can still advertise its direct routes. Hello packets on the interface, however, will be blocked and no neighbor relationship can be established on the interface. This can enhance the networking adaptability of OSPF and reduce the consumption of system resources.

Example

Disable VLANIF200 from sending or receiving OSPF packets.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] silent-interface vlanif 200
```

9.4.110 snmp-agent trap enable feature-name ospf

Function

The **snmp-agent trap enable feature-name ospf** command enables the trap function for the OSPF module.

The **undo snmp-agent trap enable feature-name ospf** command disables the trap function for the OSPF module.

By default, the trap function is disabled for the OSPF module.

Format

snmp-agent trap enable feature-name ospf trap-name { **ospfifauthfailure** | **ospfifconfigerror** | **ospfifrxbadpacket** | **ospfifstatechange** | **ospflsdbapproachingoverflow** | **ospflsdboverflow** | **ospfmaxagelsa** | **ospfnbrrestarthelperstatuschange** | **ospfnbrstatechange** | **ospfnssatranslatorstatuschange** | **ospforiginatelsa** | **ospfrestartstatuschange** | **ospftxretransmit** | **ospfvirtifauthfailure** | **ospfvirtifconfigerror** | **ospfvirtifrxbadpacket** | **ospfvirtifstatechange** | **ospfvirtiftxretransmit** | **ospfvirtnbrrestarthelperstatuschange** | **ospfvirtnbrstatechange** | **hwospfv2intraareadripaddressconflict** | **hwospfv2intraarearouteridconflict** | **hwospfv2intraarearouteridconflictrecovered** | **hwospfv2peerflappingsuppressstatuschange** }

undo snmp-agent trap enable feature-name ospf trap-name { **ospfifauthfailure** | **ospfifconfigerror** | **ospfifrxbadpacket** | **ospfifstatechange** | **ospflsdbapproachingoverflow** | **ospflsdboverflow** | **ospfmaxagelsa** | **ospfnbrrestarthelperstatuschange** | **ospfnbrstatechange**| **ospfnssatranslatorstatuschange** | **ospforiginatelsa** | **ospfrestartstatuschange** | **ospftxretransmit** | **ospfvirtifauthfailure** | **ospfvirtifconfigerror** |

ospfvirtifrxbadpacket | **ospfvirtifstatechange** | **ospfvirtiftxretransmit** | **ospfvirtnbrrestarthelperstatuschange** | **ospfvirtnbrstatechange** | **hwospfv2intraareadripaddressconflict** | **hwospfv2intraarearouteridconflict** | **hwospfv2intraarearouteridconflictrecovered** | **hwospfv2peerflappingsuppressstatuschange** }

Parameters

Parameter	Description	Value
trap-name	Enables the traps of OSPF events of specified types.	-
hwospfv2intraareadripaddressconflict	Enables the traps of the ip addresses conflict of DRs in an intra area.	By default, this trap is disabled.
hwospfv2intraarearouteridconflict	Enables the traps of the router IDs conflict in an intra area.	By default, this trap is disabled.
ospfifauthfailure	Enables the traps of the failure of the interface authentication.	By default, this trap is disabled.
ospfifconfigerror	Enables the traps of errors of the interface configuration.	By default, this trap is disabled.
ospfifrxbadpacket	Enables the traps of received bad packets.	By default, this trap is disabled.
ospfifstatechange	Enables the traps of changes of the interface state.	By default, this trap is disabled.
ospflsdbapproachingoverflow	Enables the traps of LSDB is approaching Overflow.	By default, this trap is disabled.
ospflsdboverflow	Enables the traps of LSDB overflow.	By default, this trap is disabled.
ospfmaxagelsa	Enables the traps of Max Age of LSA.	By default, this trap is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ospfnbrrestarthelperstatuschange	Enables the traps of changes of the neighbor state.	By default, this trap is disabled.
ospfnbrstatechange	Enables the traps of changes of the state of the helper during GR.	By default, this trap is disabled.
ospfnssatranslatorstatuschange	Enables the traps of the status change of the NSSA router converting Type7 LSAs to Type5 LSAs.	By default, this trap is disabled.
ospforiginatelsa	Enables the traps of LSAs that are locally generated.	By default, this trap is disabled.
ospfrestartstatuschange	Enables the traps of changes of the state of the restarter during GR.	By default, this trap is disabled.
ospftxretransmit	Enables the traps of the receiving and sending of packets on the interface.	By default, this trap is disabled.
ospfvirtifauthfailure	Enables the traps of failure of the virtual interface authentication.	By default, this trap is disabled.
ospfvirtifconfigerror	Enables the traps of error of the virtual interface configuration.	By default, this trap is disabled.
ospfvirtifrxbadpacket	Enables the traps of the bad packet that is received on the virtual interface.	By default, this trap is disabled.
ospfvirtifstatechange	Enables the traps of changes of the virtual interface state.	By default, this trap is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ospfvirtiftxretransmit	Enables the traps of sending and receiving of packets on the virtual interface.	By default, this trap is disabled.
ospfvirtnbrrestarthelperstatuschange	Enables the traps of changes of the GR helper state of neighboring nodes on the virtual link.	By default, this trap is disabled.
ospfvirtnbrstatechange	Enables the traps of changes of the state for the neighbor of the virtual-link.	By default, this trap is disabled.
hwospfv2intraarearouteridconflictrecovered	The OSPF router ID conflict is resolved.	By default, this trap is enabled.
hwOspfv2PeerFlappingSuppressStatusChange	The status of OSPF neighbor relationship flapping suppression changed.	By default, this trap is disabled.

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the traps of one or more events, you can specify **trap-name**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The non-excessive traps of OSPF module includes:
  - ospfIfStateChange
  - ospfVirtIfStateChange
  - ospfNbrStateChange
  - ospfVirtNbrStateChange
  - ospfIfAuthFailure
  - ospfVirtIfAuthFailure
  - ospfIfRxBadPacket
  - ospfVirtIfRxBadPacket
  - ospfLsdbOverflow
  - ospfLsdbApproachingOverflow
  - ospfRestartStatusChange
  - ospfNbrRestartHelperStatusChange
  - ospfVirtNbrRestartHelperStatusChange
  - ospfNssaTranslatorStatusChange
  - hwOspfv2IntraAreaRouteridConflict
  - hwospfv2intraareadripaddressconflict
- The excessive traps of OSPF module includes:
  - ospfIfConfigError
  - ospfVirtIfConfigError
  - ospfTxRetransmit
  - ospfVirtIfTxRetransmit
  - ospfOriginateLsa
  - ospfMaxAgeLsa

Example

Enable the trap of the status change of OSPF neighbors on the virtual link.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name ospf trap-name ospfvirtnbrstatechange
```

Related Topics

9.4.35 display snmp-agent trap feature-name ospf all

9.4.111 spf-schedule-interval

Function

The **spf-schedule-interval** command sets the interval for OSPF to calculate routes.

The **undo spf-schedule-interval** command restores the default setting.

By default, the intelligent timer is enabled. The interval for the SPF calculation is expressed in milliseconds. The maximum interval for the SPF calculation is 10000 ms, the initial interval is 500 ms, and the Holdtime interval is 1000 ms.

Format

spf-schedule-interval { *interval1* | **intelligent-timer** *max-interval start-interval hold-interval* | **millisecond** *interval2* }

undo spf-schedule-interval

Parameters

Parameter	Description	Value
interval1	Specifies the interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 10, in seconds.
intelligent-timer	Sets the interval for the SPF calculation of OSPF through an intelligent timer.	-
max-interval	Specifies the maximum interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 120000, in milliseconds. The default value is 10000.
start-interval	Specifies the initial interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 60000, in milliseconds. The default value is 500.
hold-interval	Specifies the Holdtime interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 60000, in milliseconds. The default value is 1000.
millisecond *interval2*	Specifies the interval for OSPF to perform the SPF calculation.	The value is an integer ranging from 1 to 10000, in milliseconds.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the LSDB, the device that runs OSPF calculates the SPT with itself as the root based on the SPF arithmetic, and determines the next hop to the destination network according to the SPT. When the OSPF LSDB changes, the shortest path needs to be recalculated. Frequent network changes and continual calculation of the shortest path consume many system resources and affect the efficiency of the devices. You can configure an intelligent timer and set a proper interval for the SPF calculation to prevent excessive device memory and bandwidth resources from being consumed.

 Copyright © Huawei Technologies Co., Ltd.

In a networking environment, in which the convergence time of routes is required to be shorter, you can set millisecond as the unit of interval to increase the frequency of calculating routes. Route convergence therefore speeds up. In other networking environments, the default value is recommended.

Configuration Impact

After this command is configured, the interval for the SPF calculation is as follows:

1. The initial interval for the SPF calculation is specified by the parameter *start-interval*.
2. The interval for the SPF calculation for the nth (n≥2) time is equal to *hold-interval*×$2^{(n-2)}$.
3. When the interval specified by *hold-interval*×$2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPF performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

Example

Set the interval for OSPF to calculate routes to 6 seconds.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] spf-schedule-interval 6
```

9.4.112 stub (OSPF area)

Function

The **stub** command sets an area to the stub area.

The **undo stub** command cancels the settings.

By default, no area is set to the stub area.

Format

stub [**no-summary** | **default-route-advertise backbone-peer-ignore**] *

undo stub

Parameters

Parameter	Description	Value
no-summary	Forbids the ABR to send Summary LSAs to the stub area.	-
default-route-advertise	Enables the ABR to generate default Type 3 LSAs and advertise them to the stub area.	-

Parameter	Description	Value
backbone-peer-ignore	Prevents the ABR from checking the neighbor status when the ABR generates default Type 3 LSAs and advertises them to the stub area. Specifically, the ABR generates default Type 3 LSAs and advertises them to the stub area as long as an interface that is Up exist in the backbone area.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

There are two configuration commands for stub area: **stub** and **default-cost (OSPF Area)** If you want to configure one area as the stub area, you must configure all devices in the area by the **stub** command.

The **default-cost (OSPF Area)** command takes effect only when it is configured on an ABR. The command is used to specify the cost of the default summary route transmitted by the ABR to the stub area.

On an ABR, you can configure the **no-summary** of the **stub** command to prevent Type 3 LSA from entering the stub area that the ABR connects to.

The backbone area cannot be configured as a stub area.

Example

Set the OSPF area 1 as the stub area.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 1
[Huawei-ospf-100-area-0.0.0.1] stub
```

Related Topics

9.4.8 default-cost (OSPF Aera)

9.4.113 stub-router (OSPF)

Function

The **stub-router** command configures the stub router.

The **undo stub-router** command restores the default configuration.

By default, no device is configured as a stub router.

Format

stub-router [**on-startup** [*interval*]]

undo stub-router

Parameters

Parameter	Description	Value
on-startup [*interval*]	Specifies the interval during which a device acts as a stub router when the device is restarted or faulty. ● If **on-startup** is not specified, the device is always a stub router, even if the cost of all routes advertised by the device is 65535. ● If **on-startup** is specified, the device works as a stub router only when it restarts or is faulty. The hold time of the stub router state is determined by *interval* parameter. If the *interval* parameter is not configured, the default interval (500 seconds) is used.	The value is an integer that ranges from 5 to 65535, in seconds. By default, the value is 500 seconds.

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **stub router** command is configured on a device, the device informs other devices not to use this stub router to forward data by increasing the metric (65535) of the links in the LSA that is generated by the device. The metric is not infinite. Thus, the routes to this stub router still exist. The metric of the LSA links that is generated by the stub router is very high.

Precautions

- If you run the **stub-router** command on a device without specifying **on-startup**, the router always functions as a stub device, and the cost of the routes from this device stays at 65535.
- If you run the **stub-router on-startup** command on a device, the device becomes a stub router after it restarts or a master/slave main control board switchover is performed and stays as a stub device for a period specified by *interval*. If *interval* is not specified, the default value (500s) takes effect.

Example

Configure the device as a stub router.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ospf 1
[Huawei-ospf-1] stub-router
```

9.4.114 suppress-flapping peer disable (OSPF)

Function

The **suppress-flapping peer disable** command disables OSPF neighbor relationship flapping suppression globally.

The **undo suppress-flapping peer disable** command enables OSPF neighbor relationship flapping suppression globally.

By default, OSPF neighbor relationship flapping suppression is enabled globally.

Format

suppress-flapping peer disable

undo suppress-flapping peer disable

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

If an interface carrying OSPF services alternates between Up and Down, OSPF neighbor relationship flapping occurs on the interface. During the flapping, OSPF frequently sends Hello packets to reestablish the neighbor relationship, synchronizes LSDBs, and recalculates routes. In this process, a large number of packets are exchanged, adversely affecting neighbor relationship stability, OSPF services, and other OSPF-dependent services, such as LDP and BGP. OSPF neighbor relationship flapping suppression can address this problem by delaying OSPF neighbor relationship reestablishment or preventing service traffic from passing through flapping links.

By default, OSPF neighbor relationship flapping suppression is enabled globally. To disable this function globally, run the **suppress-flapping peer disable** command.

Example

Disable neighbor relationship flapping suppression globally.

```
<Huawei> system-view
[Huawei] ospf
[Huawei-ospf-1] suppress-flapping peer disable
```

Related Topics

9.4.86 ospf suppress-flapping peer disable

9.4.115 vlink-peer (OSPF area)

Function

The **vlink-peer** command creates and configures a virtual link.

The **undo vlink-peer** command deletes the virtual link or restores the default setting.

By default, no virtual link is configured for OSPF.

Format

vlink-peer *router-id* [**dead** *dead-interval* | **hello** *hello-interval* | **retransmit** *retransmit-interval* | **smart-discover** | **trans-delay** *trans-delay-interval* | [**simple** [**plain** *plain-text* | [**cipher**] *cipher-text*] | { **md5** | **hmac-md5** | **hmac-sha256** } [*key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }] | **authentication-null** | **keychain** *keychain-name*]] *

undo vlink-peer *router-id* [**dead** | **hello** | **retransmit** | **smart-discover** | **trans-delay** | [**simple** | **md5** | **hmac-md5** | **hmac-sha256** | **authentication-null** | **keychain**]] *

Parameters

Parameter	Description	Value
router-id	Specifies the router ID of virtual link neighbor.	-
dead *dead-interval*	Specifies the dead interval. This value must be equal to *dead-interval* of the Router that sets up a virtual link with the interface and must be at least 4 times that of *hello-interval*.	The value is an integer that ranges from 1 to 235926000, in seconds. The default value is 40 seconds.
hello *hello-interval*	Specifies the interval for transmitting Hello packets on an interface. This value must be equal to *hello-interval* value of the Router that sets up a virtual link with the interface. The default value is 10 seconds.	The value ranges from 1 to 65535 seconds. The default value is 10 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
retransmit *retransmit-interval*	Specifies the interval for retransmitting the LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds. The default value is 5 seconds.
smart-discover	Automatically sends Hello packets	-
trans-delay *trans-delay-interval*	Specifies the delay in transmitting LSA packets on an interface.	The value is an integer that ranges from 1 to 3600, in seconds. The default value is 1 second.
simple	Indicates simple authentication. In simple authentication, the password type is **cipher** by default. **NOTICE** Simple authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
plain	Indicates plain authentication. Only plain text can be entered, and plain text is displayed when the configuration file is viewed. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This carries security risks. It is recommended to select **cipher** to save the password in cipher text.	-
plain-text	Specifies a plain text password.	• In **simple** mode, the value is a string of 1 to 8 characters without spaces. • In **md5**, **hmac-sha256** or **hmac-md5** mode, the value is a string of 1~255 characters without spaces.
cipher	Indicates cipher authentication. Either plain text or cipher text can be entered, and cipher text is displayed when the configuration file is viewed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher-text	Specifies a cipher text password.	• In **simple** mode, the value is a string of 1 to 8 characters (plaintext password) or 32, 24 or 48 characters (ciphertext password) without spaces. • In **md5**, **hmac-sha256** or **hmac-md5** mode, the value is a string of 1 to 255 (plain text password) and 20 to392 characters (cipher text password) without spaces.
md5	Indicates MD5 authentication. In MD5 authentication, the password type is **cipher** by default. **NOTICE** MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-md5	Indicates HMAC-MD5 authentication. In HMAC-MD5 authentication, the password type is **cipher** by default. **NOTICE** HMAC-MD5 authentication carries potential risks. HMAC-SHA256 authentication is recommended.	-
hmac-sha256	Indicates HMAC-SHA256 authentication. In HMAC-SHA256 authentication, the password type is **cipher** by default.	-
key-id	Specifies the authentication key ID of the interface's cipher authentication. The key ID must be consistent with that of the peer.	The value is an integer that ranges from 1 to 255.
authentication-null	Indicates that no authentication is used.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
keychain	Indicates keychain authentication. **NOTE** Before configuring this parameter, run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, OSPF authentication will fail. Currently, only the **hmac-md5** and **hmac-sha256** algorithms can be used for OSPF.	-
keychain-name	Specifies the keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

After OSPF areas are defined, OSPF route updates between non-backbone areas are transmitted through a backbone area. Therefore, OSPF requires that all non-backbone areas be directly connected to the backbone area and devices within the backbone area stay connected. However, these requirements may not be met due to various limitations. OSPF virtual links can be configured to solve the problem.

Follow-up Procedure

After virtual links are established, devices provided by different vendors may use different default MTUs. To ensure consistent MTUs on the devices, run the **undo ospf mtu-enable** command to set the default MTU in DD packets sent by interfaces to 0.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Configuring the MTU in DD packets will cause the neighbor relationship to be re-established.

Precautions

When configuring parameters, pay attention to the following:

- A smaller **hello** value indicates faster detection of network topology changes and higher network resource usage.
- A too small **retransmit** value leads to unnecessary retransmission of LSAs. You are advised to set a large **retransmit** value on a low-speed network.
- The authentication mode of a virtual link must be the same as that in the backbone area.

Example

Configure a virtual link with the peer device's router ID 10.1.1.1.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] area 2
[Huawei-ospf-100-area-0.0.0.2] vlink-peer 10.1.1.1
```

Related Topics

9.4.34 display ospf vlink

9.4.80 ospf mtu-enable

9.4.4 authentication-mode (OSPF area)

9.4.116 vpn-instance-capability simple (OSPF)

Function

The **vpn-instance-capability simple** command directly calculates the route instead of conducting the routing loop detection.

The **undo vpn-instance-capability** command detects the DN bit to avoid the routing loops.

By default, the routing-loop check is enabled.

Format

vpn-instance-capability simple

undo vpn-instance-capability

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If OSPF VPN multi-instance is deployed on a Multi-VPN-Instance CE (MCE), routes cannot be calculated based on Type3, Type5, or Type7 LSAs with the DN bit. Therefore, OSPF detects routing loops when calculating routes. In this case, the **vpn-instance-capability simple** command is used to disable OSPF routing loop detection and enable OSPF to calculate routes based on received LSAs without checking the DN bit and route-tag in the LSAs. The route-tag is restored to the default value 1.

Prerequisites

OSPF VPN multi-instance has been deployed on an MCE using the **ospf** *process-id* **vpn-instance** *vpn-instance-name* command.

Configuration Impact

- If there is no ABR and the **vpn-instance-capability simple** command is run on an MCE, the MEC cannot become an ABR.
- After the **vpn-instance-capability simple** command is run in an OSPF process, the OSPF process will not import IBGP routes.
- After the **vpn-instance-capability simple** command is run, OSPF routes that have been imported by BGP do not carry any OSPF domain ID, route tag, or router ID.
- By default, when BGP imports an OSPF route, it uses the cost of the OSPF route plus 1 as the MED value. The MED in BGP is similar to the cost in an IGP in terms of functions. After the **vpn-instance-capability simple** command is run, BGP uses the cost of an OSPF route as the MED when it imports the OSPF route. Therefore, MED values change after the command is run, which may affect the route selection result.

Precautions

NOTE

The **undo vpn-instance-capability** command cannot be used to enable OSPF routing loop detection in a scenario without MCEs.

Example

Disable the OSPF routing-loop check.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] vpn-target 3:3 export-extcommunity
[Huawei-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-vpn-instance-vrf1-af-ipv4] quit
[Huawei-vpn-instance-vrf1] quit
[Huawei] ospf 100 vpn-instance vrf1
[Huawei-ospf-100] vpn-instance-capability simple
```

9.5 OSPFv3 Configuration Commands

9.5.1 abr-summary (OSPFv3 Area)

Function

The **abr-summary** command configures IPv6 route summarization on an ABR.

The **undo abr-summary** command cancels IPv6 route summarization on an ABR.

By default, IPv6 route summarization is not configured on an ABR.

Format

abr-summary *ipv6-address prefix-length* [**cost** *cost* | **not-advertise**] *

undo abr-summary *ipv6-address prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the address range of IPv6 routes to be summarized.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length.	The value is an integer ranging from 1 to 128.
cost *cost*	Specifies the cost of a summarized route. By default, the cost of a summarized route is the maximum cost among those of routes that are summarized.	The value is an integer ranging from 1 to 16777214.
not-advertise	Indicates that the summarized IPv6 routes that match a specified IPv6 address prefix or prefix length are not advertised.	-

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

This command is applicable only to the ABR for route aggregation of the current area. The ABR transmits only one summarized route to other areas.

An area can be configured with multiple summarized network segments. Thus OSPFv3 can summarize multiple network segments.

Example

Summarize two routes FC00:0:0:1::/64 and FC00:0:0:2::/64 of OSPFv3 area 1 into route FC00:0:0::/48 with the cost being 400, and advertise it to other areas.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] area 1
[Huawei-ospfv3-1-area-0.0.0.1] abr-summary fc00:0:0:: 48 cost 400
```

Related Topics

9.5.2 area (OSPFv3)

9.5.49 ospfv3

9.5.2 area (OSPFv3)

Function

The **area** command displays the OSPFv3 area view.

Format

area *area-id*

Parameters

Parameter	Description	Value
area-id	Specifies the OSPFv3 area ID. It can be an integer in the decimal format or in the IPv4 address format.	If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of devices increases with the expansion of the network. This leads to a large LSDB on every OSPFv3-enabled device on a large-scale network. Consequently, route flapping frequently occurs and thus a large number of OSPF packets are transmitted on the network, which wastes bandwidth resources.

OSPFv3 addresses the preceding problem by logically partitioning an AS into different areas.

Prerequisites

Before creating an OSPFv3 area and enter the OSPFv3 area view, you need to enter the OSPFv3 process view.

Precautions

After an AS is partitioned into different areas, not all areas are equal. The area with the ID being 0 is a backbone area. The backbone area is responsible for forwarding inter-area routes. In addition, the routing information between non-backbone areas must be forwarded through the backbone area.

The first time the **area** command is run, an OSPFv3 area is created and the OSPFv3 area view is displayed; running the **area** command later enters the OSPFv3 area view only.

Example

Enter the OSPFv3 area 0 view.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] area 0
[Huawei-ospfv3-1-area-0.0.0.0]
```

Related Topics

9.5.49 ospfv3

9.5.3 asbr-summary (OSPFv3)

Function

The **asbr-summary** command configures IPv6 route summarization on an ASBR.

The **undo asbr-summary** command cancels IPv6 route summarization on an ASBR.

By default, IPv6 route summarization is not configured on an ASBR.

Format

asbr-summary *ipv6-address summary-prefix-length* [**cost** *summary-cost* | **tag** *summary-tag* | **distribute-delay** *dist-delay-interval* | **not-advertise**] *

undo asbr-summary *ipv6-address summary-prefix-length*

Parameters

Parameter	Description	Value
ipv6-address	Specifies the address range of IPv6 routes to be summarized.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
summary-prefix-length	Specifies the prefix length.	The value is an integer ranging from 1 to 128.
cost *summary-cost*	Specifies the cost of a summarized route. By default, the cost of a summarized route is the maximum cost among those of routes that are summarized.	The value is an integer ranging from 1 to 16777214. By default: ● For Type 1 external routes, the cost of the summarized route is the highest among the cost of the routes being summarized. ● For Type 2 external routes, the cost of the summarized route equals the highest among the cost of the routes being summarized plus 1.
tag *summary-tag*	Specifies the tag used to control route advertisement.	The value is an integer ranging from 0 to 4294967295. The default value is 1.
distribute-delay *dist-delay-interval*	Specifies the delay for advertising summarized routes.	The value is an integer ranging from 1 to 65535, in seconds. This parameter has no default value.
not-advertise	Indicates that the summarized IPv6 routes that match a specified IPv6 prefix/prefix length are not advertised.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

An ASBR connects two or more ASs, and generates AS-External-LSAs.

The **asbr-summary** command is used on an ASBR to summarize the imported routes that have the same prefix and advertise only the summarized route. This command can be used only on ASBRs.

 Copyright © Huawei Technologies Co., Ltd.

An ASBR can be configured with multiple summarized routes. Therefore, OSPFv3 can aggregate routes of multiple network segments.

Example

Configure route summarization.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] asbr-summary aa:: 64 cost 20 tag 100
```

9.5.4 authentication-mode (OSPFv3)

Function

The **authentication-mode** command configures an authentication mode and a password for an OSPFv3 process or area.

The **undo authentication-mode** command deletes the authentication mode and password configured for an OSPFv3 process or area.

By default, no authentication mode or password are configured for any OSPFv3 process or area.

Format

authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* }

authentication-mode keychain *keychain-name*

undo authentication-mode hmac-sha256 key-id *key-id*

undo authentication-mode keychain

Parameters

Parameter	Description	Value
hmac-sha256	Configures HMAC-SHA256 authentication.	-
key-id *key-id*	Specifies the key ID for authentication, which must be the same as the one configured at the other end.	The value is an integer ranging from 1 to 65535.
plain	Configures the plaintext password type. Only a plaintext password can be entered, and the password is displayed in plaintext in the configuration file. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-

Parameter	Description	Value
plain-text	Specifies a plaintext password.	The value is a string of 1 to 255 characters, spaces not supported.
cipher	Configures the ciphertext password type. You can enter either a plaintext or ciphertext password, but the password is displayed in ciphertext in the configuration file.	-
cipher-text	Specifies a ciphertext password.	The value can be a string of 1 to 255 characters for plaintext passwords and 20 to 392 characters for ciphertext passwords, spaces not supported.
keychain	Configures keychain authentication. **NOTE** Before configuring this parameter, you must run the **keychain** command to create a keychain. Then, run the **key-id**, **key-string**, and **algorithm** commands to configure a key ID, a password, and an authentication algorithm for this keychain. Otherwise, the OSPF authentication will fail. OSPFv3 supports only hmac-sha256 in the algorithm command.	-
keychain-name	Specifies a keychain name.	The value is a string of 1 to 47 case-insensitive characters.

Views

OSPFv3 view or OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to inherent defects and flawed implementation of the TCP/IP protocol suite, there are an increasing number of attacks, which poses greater threats on TCP/IP networks than ever before. The attacks on network devices may lead to network failures. To configure an authentication mode and a password for an OSPFv3 process or area to improve OSPFv3 network security, run the **authentication-mode** command.

Precautions

If you use area authentication, the authentication and password configurations on the interfaces of all the routers in the area must be the same.

OSPFv3 area authentication has a lower priority than OSPFv3 interface authentication.

To configure OSPFv3 interface authentication, run the **ospfv3 authentication-mode** command.

Example

Configure HMAC-SHA256 authentication for OSPFv3 process 100.

```
<Huawei> system-view
[Huawei] ospfv3 100
[Huawei-ospfv3-100] authentication-mode hmac-sha256 key-id 10 cipher huawei
```

Configure HMAC-SHA256 authentication for OSPFv3 area 0.

```
<Huawei> system-view
[Huawei] ospfv3 100
[Huawei-ospfv3-100] area 0
[Huawei-ospfv3-100-area-0.0.0.0] authentication-mode hmac-sha256 key-id 10 cipher huawei
```

Related Topics

9.5.51 ospfv3 authentication-mode

9.5.5 bandwidth-reference (OSPFv3)

Function

The **bandwidth-reference** command sets the bandwidth reference value used to calculate the link cost.

The **undo bandwidth-reference** command restores the default setting.

By default, the bandwidth reference value of the link cost is 100 Mbit/s. That is, the link cost is 100000000/bandwidth.

Format

bandwidth-reference *value*

undo bandwidth-reference

Parameters

Parameter	Description	Value
value	Specifies the bandwidth reference value used to calculate the link cost.	It is an integer ranging from 1 to 2147483648, in Mbit/s. The default value is 100 Mbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

If the link cost is not set, OSPFv3 calculates the link cost according to the link bandwidth (Cost = Reference Value/Bandwidth). Using the **ospfv3 cost** command sets the cost of an interface that runs OSPFv3. The priority of the cost set through the **ospfv3 cost** command is higher than that of the cost set through the **bandwidth-reference** command.

The **bandwidth-reference** command has the same function on Eth-Trunk interfaces and physical interfaces. If the command is executed on an Eth-Trunk interface, the bandwidth of the Eth-Trunk interface is the total bandwidth of all its member interfaces.

Example

Set the bandwidth reference value of the link cost to 1000.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] bandwidth-reference 1000
```

Related Topics

9.5.54 ospfv3 cost

9.5.6 bfd all-interfaces (OSPFv3)

Function

The **bfd all-interfaces** command enables BFD for OSPFv3 or configures bidirectional forwarding detection (BFD) specific parameters for OSPFv3.

The **undo bfd all-interfaces** command disables BFD for OSPFv3 or unconfigures BFD specific parameters for OSPFv3.

By default, BFD is not enabled or configured at OSPFv3 process level.

Format

bfd all-interfaces { **enable** | { **min-transmit-interval** *min-transmit-value* | **min-receive-interval** *min-receive-value* | **detect-multiplier** *detect-multiplier-value* }* }

undo bfd all-interfaces { **enable** | { **min-transmit-interval** [*min-transmit-value*] | **min-receive-interval** [*min-receive-value*] | **detect-multiplier** [*detect-multiplier-value*] }* }

Parameters

Parameter	Description	Value
enable	Indicates enable BFD for OSPFv3.	-
min-transmit-interval *min-transmit-value*	Indicates minimum transmit interval for BFD support in OSPFv3 on a given OSPFv3 process.	The value is an integer that ranges from 10~2000, in milliseconds. By default, it is 10 milliseconds.
min-receive-interval *min-receive-value*	Indicates minimum receive interval for BFD support in OSPFv3 on a given OSPFv3 process.	The value is an integer that ranges from 10~2000, in milliseconds. By default, it is 10 milliseconds.
detect-multiplier *detect-multiplier-value*	Indicates detect multiplier value for BFD support in OSPFv3 on a given OSPFv3 process.	The value is an integer that ranges from 3 to 50. By default, it is 3.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- You can run this command to enable BFD and configure BFD session parameters. Faults between adjacent devices, therefore, are quickly detected, OSPFv3 is instructed to recalculate routes, and OSPFv3 convergence speeds up. When the OSPFv3 neighbor relationship goes Down, the BFD session between OSPFv3 neighbors is dynamically deleted.
- When you configure OSPFv3 IP FRR, the status of the BFD session is bound to OSPFv3 IP FRR after the **frr-binding** command parameters are configured. So the lower layer fast responds to the link change, traffic is rapidly switched to the backup link, and faults are detected within a short time.

After OSPFv3 establishes a BFD session, the default parameter value is used. BFD session parameters can also be modified as required.

- Actual interval at which BFD packets are transmitted on the local devices = Max { configured interval *min-transmit-value* at which BFD packets are transmitted, configured interval *min-receive-value* at which BFD packets are received on the peer device }
- Actual interval at which BFD packets are received on the local devices = Max { configured interval *min-transmit-value* at which BFD packets are transmitted on the peer device, configured interval *min-receive-value* at which BFD packets are received on the local device }

 Copyright © Huawei Technologies Co., Ltd.

- Actual time for detecting BFD packets = Actual interval at which BFD packets are received on the local device x Configured detection multiplier *detect-multiplier-value*

For example:

- On the local device, the configured interval at which BFD packets are transmitted is 200 ms; the interval at which BFD packets are received is set to 300 ms; the detection multiplier is 4.
- On the peer device, the configured interval at which BFD packets are transmitted is 100 ms; the interval at which BFD packets are received is 600 ms; the detection multiplier is 5.

Then:

- On the local device, the actual interval at which BFD packets are transmitted is 600 ms calculated by using the formula max {200 ms, 600 ms}; the interval at which BFD packets are received is 300 ms calculated by using the formula max {100 ms, 300 ms}; the detection period is 1500 ms calculated by multiplying 300 ms by 5.
- On the peer device, the actual interval at which BFD packets are transmitted is 300 ms calculated by using the formula max {100 ms, 300 ms}, the actual interval at which BFD packets are received is 600 ms calculated by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms calculated by multiplying 600 ms by 4.

Prerequisites

Before configuring BFD for OSPFv3, BFD must have been enabled globally using the **bfd** command.

After BFD in the OSPFv3 process is enabled using the **bfd all-interfaces enable** command, OSPFv3 establish BFD sessions only with neighbors whose status is Full.

Follow-up Procedure

- Configure a BFD session on a specified interface.

  If you need to configure BFD on specified interfaces, or global BFD for OSPFv3 is configured but some interface need to be quicker to find link faults, you can configure BFD on specified interfaces using the **ospfv3 bfd** command.
- An interface is prevented from dynamically creating a BFD session.

  If you do not want to enable BFD on specified interfaces, you can disable the interfaces from dynamically creating BFD sessions using the **ospfv3 bfd block** command.

Precautions

The **bfd all-interfaces** command and the **ospfv3 bfd block** command are mutually exclusive.

Example

Enabling BFD on OSPFv3 process.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] bfd all-interfaces enable
```

```
[Huawei-ospfv3-1] bfd all-interfaces min-transmit-interval 100 min-receive-interval 100 detect-multiplier 5
```

9.5.7 default (OSPFv3)

Function

The **default** command sets the default parameters of the external routes that are imported by OSPFv3, The default parameters include cost, tag and type (Type 1 or Type 2).

The **undo default** command restores the default value of the parameters of the external routes that are imported by OSPFv3.

By default, the default cost of the external routes is 1; the default tag value is 1; the type of the imported external routes is Type 2.

Format

default { **cost** *cost* | **tag** *tag* | **type** *type* } *

undo default { **cost** [*cost*] | **tag** [*tag*] | **type** [*type*] } *

Parameters

Parameter	Description	Value
cost *cost*	Specifies the default cost of the external route that is imported by OSPFv3.	The value is an integer ranging from 1 to 16777214. By default, it is 1.
tag *tag*	Specifies the tag value of the imported routes.	The value is an integer that ranges from 0 to 4294967295. By default, the value is 1.
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. By default, it is 2. ● 1: Type 1 external route ● 2: Type 2 external route

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Since OSPFv3 can import external routing information and advertise it to the entire AS, it is necessary to specify the default cost of the external route that is imported by the protocol.

If multiple OSPFv3 processes are enabled, the command is valid only for this process.

Example

Specify the default cost of the external routes that are imported by OSPFv3 as 10.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] default cost 10
```

9.5.8 default-cost (OSPFv3 Area)

Function

The **default-cost** command specifies the cost of the default route that is sent to the stub area by OSPFv3.

The **undo default-cost** command restores the cost to the default value.

By default, the cost of the Type 3 default route transmitted to the stub area is 1.

Format

default-cost *cost*

undo default-cost

Parameters

Parameter	Description	Value
cost	Specifies the cost of the default route that is sent to the stub area by OSPFv3.	The value ranges from 0 to 16777214. By default, it is 1.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

This command is applicable only to the ABR that is connected to the stub area.

Before setting the cost of the default route that is transmitted to the stub area by OSPFv3, you need to configure the local area as a stub area by using the **stub** command. You can use the **default-cost** command to specify the cost of the default route that is transmitted to the stub area by the ABR.

If multiple OSPFv3s are enabled, the command takes effect only on this process.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the area 1 as the stub area and the cost of the default route that is sent to the stub area to 60.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] area 1
[Huawei-ospfv3-1-area-0.0.0.1] stub
[Huawei-ospfv3-1-area-0.0.0.1] default-cost 60
```

Related Topics

9.5.81 stub (OSPFv3 Area)

9.5.9 default-route-advertise (OSPFv3)

Function

The **default-route-advertise** command advertises default routes into an OSPFv3 routing domain.

The **undo default-route-advertise** command cancels advertising default routes.

Format

default-route-advertise [**always** | **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name* [**match-any**]] *

undo default-route-advertise [**always** | **cost** [*cost*] | **type** [*type*] | **tag** [*tag*] | **route-policy** [*route-policy-name*] [**match-any**]] *

Parameters

Parameter	Description	Value
always	Generates and advertises an LSA that describes a default route, regardless of whether the local device has active non-local OSPFv3 default routes. The router that has **always** configured does not calculate default routes of other routers. If **always** is not specified, an LSA is generated only when there are active non-local OSPFv3 default routes in the routing table of the local device.	-
cost *cost*	Specifies the cost of an advertised default route.	The value is an integer that ranges from 1 to 16777214. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
type *type*	Specifies the type of an external route.	The value is 1 or 2. The default value is 2. ● 1: Type 1 external route ● 2: Type 2 external route
tag *tag*	Specifies the tag value of an advertised default route.	The value is an integer that ranges from 0 to 4294967295. The default value is 1.
route-policy *route-policy-name*	Specifies the name of a route-policy. The device advertises default routes according to the parameters configured in the route-policy when there are matched non-local OSPFv3 default routes in the routing table.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
match-any	Indicates that through a route-policy, the device advertises default routes according to the parameters configured in the route-policy when there are matched routes in the routing table.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Before a device advertises a default route into an OSPFv3 routing domain, it compares the preferences of default routes. For example, if an OSPFv3 router within the domain also has a static default route configured, ensure that the preference of the static default route is lower than that of the default route advertised by OSPFv3 so that the default route can be added into the current routing table.

Default routes cannot be imported using the **import-route** command. To advertise default routes, run the **default-route-advertise** command. The metric of a generated default route is determined by the **cost** and **type** parameters in the **default-route-advertise** command, and the default **tag** value is 1. If the local routing table does not contain non-local OSPFv3 default routes, specify the **always** parameter to generate an ASE LSA of a default route.

A route-policy is only used to filter existing active non-local OSPFv3 default routes of the local device, and match routes according to the following rules:

- If a default route matches the policy, the local device generates a default route according to the parameters configured in the route-policy, such as cost, tag, and type.
- If a default route does not match the policy and **always** is not specified, the local device does not generate any default route.
- If a default route does not match the policy and **always** is specified, the router generates a default route. The parameters of the generated default route are determined by the **default-route-advertise** [**always** | **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * command.

NOTE

The preferences of parameters of the default route configured in a route-policy are higher than those of parameters configured in the **default-route-advertise** [**always** | **cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] * command.

Example

Advertise the ASE LSA that describes a default route into an OSPFv3 routing domain. The local device does not have a default route.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] default-route-advertise always
```

Related Topics

9.5.40 import-route (OSPFv3)

9.5.10 description (OSPFv3 Area)

Function

The **description** command configures a description for an OSPFv3 area.

The **undo description** command deletes the configured description of an OSPFv3 area.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies a description for an OSPFv3 area.	The value is a string of 1 to 80 case-sensitive space-tolerant characters.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

By configuring a description for an OSPFv3 area, you can identify different OSPFv3 areas easily.

Example

Describe the OSPFv3 area 0.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] area 0
[Huawei-ospfv3-1-area-0.0.0.0] description main area
```

9.5.11 description (OSPFv3)

Function

The **description** command configures a description for an OSPFv3 process.

The **undo description** command deletes the configured description of an OSPFv3 process.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies a description for an OSPFv3 process.	The value is a string of 1 to 80 case-sensitive space-tolerant characters.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

By configuring a description for an OSPFv3 process, you can identify different OSPFv3 processes easily.

 Copyright © Huawei Technologies Co., Ltd.

Example

Describe the OSPFv3 process 1.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] description main process
```

9.5.12 display default-parameter ospfv3

Function

The **display default-parameter ospfv3** command displays the default OSPFv3 configuration.

Format

display default-parameter ospfv3

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays only the default configurations, regardless of whether the configurations about OSPFv3 parameters are changed.

Example

Display the default OSPFv3 configuration.

```
<Huawei> display default-parameter ospfv3

 OSPFv3 Default Values:

 Process View:
 -----------------------------------------------------
 Maximum ECMP Count                        : 32
 SPF Delay Time(sec)                       : 5
 SPF Hold Time(sec)                        : 10
 SPF Max Time(millisec)                    : 10000
 SPF Start Time(millisec)                  : 500
 SPF ExpHold Time(millisec)                : 2000
 LSA Reorig Time(sec)                      : 5
 LSA Max Time(millisec)                    : 5000
 LSA Start Time(millisec)                  : 500
 LSA ExpHold Time(millisec)                : 5000
 LSA Arrival Time(millisec)                : 1000
 Wait Interval for stub-router on-startup   : 500
 Grace Period(sec)                         : 120
```

```
Retransmit-Interval for Grace LSAs(sec)    : 5
Ack wait-time for Grace LSAs(sec)          : 15
Helper Max Grace Period Support(sec)       : 1800
Bandwidth-Reference(Mbps)                  : 100
Sham Link Cost                             : 1
VPN Domain ID                              : 0
VPN Router Tag                             : 0
Default Metric                             : 1
Default Tag                                : 1
Default Type                               : 2
Route Preference for Internal Routes       : 10
Route Preference for External Routes       : 150
Suppress flapping peer                     : Enable

-----------------------------------------------------

Area View:
-----------------------------------------------------

Default Stub Cost                          : 1
NSSA Translator Stability Index(sec)       : 40
-----------------------------------------------------

Interface View:
-----------------------------------------------------
Hello Interval(sec)                        : 10
NBMA Hello Interval(sec)                   : 30
Dead Interval(sec)                         : 40
NBMA Dead Interval(sec)                    : 120
Poll Interval(sec)                         : 120
Retransmit Interval(sec)                   : 5
Transmit Delay(sec)                        : 1
Router DR Priority                         : 1
Suppress flapping peer                     : Enable
Suppress flapping detect interval          : 3
Suppress flapping detect threshold         : 30
Suppress flapping Resume interval          : 10
Suppress flapping mechanism                : Hold-max-cost
Hold-max-cost interval                     : 60
```

Table 9-62 Description of the **display default-parameter ospfv3** command output

Item	Description
OSPFv3 Default Values	Default values of OSPFv3
Process View	Process view
Area View	Area view
Interface View	Interface view
Maximum ECMP Count	Maximum number of equal-cost routes
SPF Delay Time(sec)	Default delay for SPF calculation
SPF Hold Time(sec)	Hold time interval between two consecutive SPF calculations
SPF Max Time(millisec)	Maximum delay time between two consecutive SPF calculations
SPF Start Time(millisec)	Initial SPF schedule delay

Item	Description
SPF ExpHold Time(millisec)	Maximum hold time between two consecutive SPF calculations
LSA Reorig Time(sec)	The minimum time between distinct originations of any particular LSA.
LSA Max Time(millisec)	The maximum age that an LSA can attain.
LSA Start Time(millisec)	The default value of LSA origination.
LSA ExpHold Time(millisec)	The intelligent timer for lsa reorigination time.
LSA Arrival Time(millisec)	The minimum time that must elapse between reception of new LSA instances during flooding.
Wait Interval for stub-router on-startup	Default period during which a router remains to be a stub router during master/slave switchover
Grace Period(sec)	GR period
Retransmit-Interval for Grace LSAs(sec)	Default interval for retransmitting Grace LSAs, in seconds
Ack wait-time for Grace LSAs(sec)	Default time during which a router waits to reply the received Grace LSA with an LSAck message If the router does not receive any Grace LSA within the default waiting time, the router does not send the LSAck message.
Helper Max Grace Period Support(sec)	Default GR period of the Helper device
Bandwidth-Reference(Mbps)	Default bandwidth reference value used to calculate the link cost, in Mbit/s
Sham Link Cost	Default cost of a sham link
VPN Domain ID	Default domain ID of the VPN
VPN Router Tag	Default router tag of the VPN
Default Metric	Default metric of the imported external route
Default Tag	Default tag of the imported external route
Default Type	Default type of the imported external route

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Route Preference for Internal Routes	Default preference of the internal route
Route Preference for External Routes	Default preference of the external route
Default Stub Cost	Default cost of a stub area
NSSA Translator Stability Index(sec)	Default dead time of a translator
Hello Interval(sec)	Default interval for sending Hello packets on a P2P or a broadcast network
NBMA Hello Interval(sec)	Default interval for sending Hello packets on an NBMA network
Dead Interval(sec)	Default interval for declaring a neighbor to be Down after no Hello packets are received on a P2P or broadcast network
NBMA Dead Interval(sec)	Default interval for declaring a neighbor to be Down after no Hello packets are received on an NBMA network
Poll Interval(sec)	Default poll interval for sending Hello packets on an NBMA network
Retransmit Interval(sec)	Default interval for retransmitting packets
Transmit Delay(sec)	Default estimated time for transmitting an LSU over this interface Before packet transmission, the estimated time needs to be added to the time limit of each LSA. The estimated time should be added to the transmission delay of the inbound interface.
Router DR Priority	Default priority of the DR
Suppress flapping peer	Whether OSPFv3 neighbor relationship flapping suppression is enabled
Suppress flapping detect interval	Default detection interval of OSPFv3 neighbor relationship flapping suppression
Suppress flapping detect threshold	Default threshold of OSPFv3 neighbor relationship flapping suppression
Suppress flapping Resume interval	Default interval for exiting from OSPFv3 neighbor relationship flapping suppression

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Suppress flapping mechanism	Default mode of OSPFv3 neighbor relationship flapping suppression
Hold-max-cost interval	Default duration of the Hold-max-cost mode

9.5.13 display ospfv3

Function

The **display ospfv3** command displays the brief information of OSPFv3.

Format

display ospfv3 [*process-id*]

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID. If process-id is not specified, the brief information of all OSPFv3 processes is displayed in the ascending order of the process ID.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the brief information of OSPFv3.

```
<Huawei> display ospfv3

 Routing Process "OSPFv3 (1)" with ID 0.0.0.0
 Route Tag: 0
 Multi-VPN-Instance is not enabled
 SPF Intelligent Timer[millisecs] Max: 10000, Start: 1000, Hold: 2000
 LSA Intelligent Timer[millisecs] Max: 10000, Start: 1000, Hold: 2000
 LSA Arrival interval 1000 millisecs
 Default ASE parameters: Metric: 1 Tag: 1 Type: 2
 Number of AS-External LSA 0. AS-External LSA's Checksum Sum 0x0000
```

 Copyright © Huawei Technologies Co., Ltd.

```
Number of AS-Scoped Unknown LSA 0. AS-Scoped Unknown LSA's Checksum Sum 0x0000
Number of FULL neighbors 0
Number of Exchange and Loading neighbors 0
Number of LSA originated 0
Number of LSA received 0
SPF Count          : 0
Non Refresh LSA    : 0
Non Full Nbr Count : 0
Number of areas in this router is 1
```

Table 9-63 Description of the **display ospfv3** command output

Item	Description
Route Tag	The tag value for the imported VPN route.
Multi-VPN-Instance is not enabled	That the current process does not support Multi-VPN instance.
SPF Intelligent Timer[millisecs]	Indicates the intelligent timers: ● Max: maximum delay time between two consecutive SPF calculations ● Start: initial SPF schedule delay ● Hold: minimum hold time between two consecutive SPF calculations
LSA Intelligent Timer[millisecs]	Indicates LSA by the intelligent timers: ● Max: maximum delay time between two consecutive re-origination of same instance of LSA ● Start: initial delay for LSA origination ● Hold: minimum hold time between two consecutive re-origination of same instance of LSA
LSA Arrival interval	Indicates minimum interval for receiving the same LSA.
Default ASE parameters	Indicates default parameters for AS external LSA, including: ● Metric: cost of the route ● Tag: tag value ● Type: type of LSA (1 or 2)
Number of AS-External LSA	Number of LSA originated for routes outside an AS.
AS-External LSA's Checksum Sum	Indicates checksum of LSA originated for routes outside an AS.
Number of AS-Scoped Unknown LSA	Number of unknown LSA with the flooding range of an entire AS.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AS-Scoped Unknown LSA's Checksum Sum	Indicates checksum of unknown LSA with the flooding range of an entire AS.
Number of FULL neighbors	Number of Full neighbors.
Number of Exchange and Loading neighbors	Number of neighbors in the Exchange state and neighbors in the Loading state.
Number of LSA originated	Number of generated LSAs.
Number of LSA received	Number of received LSAs.
SPF Count	Number of the events triggered by the SPF calculation.
Non Refresh LSA	Number of LSAs that are not updated in the retransmission list during GR.
Non Full Nbr Count	Number of neighbors in the Exchange state and neighbors in the Loading state during GR.
Number of areas in this router is	Number of areas on a router.

Related Topics

9.5.49 ospfv3

9.5.14 display ospfv3 abr-summary-list

Function

The **display ospfv3 abr-summary-list** command displays the aggregation of the route that is imported by OSPFv3.

If the IP address and mask are not specified, the aggregation of all routes that are imported by OSPFv3 is displayed.

Format

display ospfv3 [*process-id*] **abr-summary-list** [*ipv6-address prefix-length*]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
ipv6-address	Specifies the matched IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
prefix-length	Specifies the length of the route prefix.	The value is an integer ranging from 1 to 128.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the aggregation of the all the routes that are imported by OSPFv3.

```
<Huawei> display ospfv3 abr-summary-list
OSPFv3 Process (1)
Area ID  :  0.0.0.1
Prefix          Prefix-Len  Matched       Status
FC00:0:0:2001::  16          2[Active]     Advertise
FC00:0:0:3001::  16          0[NotActive]  Advertise
FC00:0:0:4001::  16          0[NotActive]  Advertise
```

Table 9-64 Description of the **display ospfv3 abr-summary-list** command output

Item	Description
OSPFv3 Process (1)	OSPFv3 process ID
Area ID	Area ID
Prefix	IPv6 prefix
Prefix-Len	Length of the prefix
Matched	Status of the aggregated routes
Status	Advertisement status of the aggregated routes: ● Advertise: Advertise after the aggregation. ● NotAdvertise: Do not advertise after the aggregation.

Related Topics

9.5.1 abr-summary (OSPFv3 Area)

9.5.15 display ospfv3 area

Function

The **display ospfv3 area** command displays OSPFv3 area information.

Format

display ospfv3 [*process-id*] **area** [*area-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID for an OSPFv3 process.	The value is an integer ranging from 1 to 65535.
area-id	Specifies the area ID for the area to be displayed.	If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display OSPFv3 area information.

```
<Huawei> display ospfv3 area

OSPFv3 Process (1)

 Area 0.0.0.0(BACKBONE)  InActive
     Number of interfaces in this area is 1
     SPF algorithm executed 0 times
     Number of LSA 0. Checksum Sum 0x0000
     Number of Unknown LSA 0
     Area Bdr Router count: 0
     Area ASBdr Router count: 0
     Next SPF Trigger Time 500 millisecs
     Router ID conflict state: Normal
 Area 0.0.0.1 Active
     Number of interfaces in this area is 1
     SPF algorithm executed 3 times
     Number of LSA 4. Checksum Sum 0x23AC8
     Number of Unknown LSA 0
     Area Bdr Router count: 0
```

```
Area ASBdr Router count: 1
Next SPF Trigger Time 500 millisecs
Router ID conflict state: Normal
```

Table 9-65 Description of the display ospfv3 area command output

Item	Description
Number of interfaces in this area	Indicates the number of active interfaces.
SPF algorithm executed	Indicates the number of SPF calculations.
Number of LSA	Indicates the number of LSAs in this area.
Check Sum	Indicates the area checksum.
Number of Unknown LSA	Indicates the number of unknown LSAs in the area.
Area Bdr Router count	Indicates the number of ABRs in the area.
Area ASBdr Router count	Indicates the number of ASBRs in the area.
Next SPF Trigger Time	Indicates the time for triggering the next SPF calculation, in milliseconds.
Router ID conflict state	Indicates the Router ID conflict state.

9.5.16 display ospfv3 asbr-summary

Function

The **display ospfv3 asbr-summary** command displays OSPFv3 route summarization.

Format

display ospfv3 [*process-id*] **asbr-summary** [*ipv6-address prefix-length*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 65535.
ipv6-address	Specifies a matching IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of a route prefix.	The value is an integer ranging from 1 to 128.

Parameter	Description	Value
verbose	Displays detailed information about OSPFv3 route summarization.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If neither *ipv6-address* nor *prefix-length* is specified, this command displays all detailed information about OSPFv3 route summarization.

Example

Display OSPFv3 route summarization.

```
<Huawei> display ospfv3 asbr-summary verbose

 OSPFv3 Process (1)
 Total summary address count :1

         Summary Address

 Prefix        : 10::
 Prefix length : 32
 Tag           : 0 (Not Configured)
 Status        : Advertised
 Cost          : 10 (Configured)
 Delay         : (Not Configured)
 Type          : 2 (Larger than any link state path)
 The Count of Route is: 3

Destination      Mask       Protocol     Proc      Type     Metric
   10::0         64         Static       0          2        1
   10::2         128        Static       0          2        1
   10::3         128        Static       0          2        1
```

Table 9-66 Description of the display ospfv3 asbr-summary command output

Item	Description
Total Summary address count	Number of summarized routes configured by using the **asbr-summary** command
Summary Address	Detailed information about summarized routes
Prefix	Prefix of a summarized route
Prefix length	Prefix length of a summarized route
Tag	Tag of a summarized route

Item	Description
Status	Whether a summarized route is advertised: • Advertised: indicates that a summarized route is advertised. • NotAdvertised: indicates that a summarized route is not advertised.
Cost	Cost of a summarized route
Delay	Delay time to start aggregating routes
Type	Type of AS-External routes • Type: 1 • Type: 2
The Count of Route is	Number of summarized routes
Destination	Destination address of a summarized route
Mask	Mask of a summarized route
Protocol	Protocol carried by a summarized route
Proc	Process ID carried by a summarized route
Metric	Metric of a summarized route

Related Topics

9.5.3 asbr-summary (OSPFv3)

9.5.17 display ospfv3 black-box neighbor-down

Function

The **display ospfv3 black-box neighbor-down** command displays detailed information about OSPFv3 neighbors in the Down state.

Format

display ospfv3 black-box neighbor-down [*number*]

Parameters

Parameter	Description	Value
number	Specifies the number of OSPFv3 neighbors in the Down state to be displayed.	The value is an integer ranging from 1 to 10.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *number* is not specified, the **display ospfv3 black-box neighbor-down** command displays detailed information about the latest 10 OSPFv3 neighbors in the Down state.

Example

Display the latest 2 OSPFv3 neighbors in the Down state.

```
<Huawei> display ospfv3 black-box neighbor-down 2
 Neighbor Router-id                    : 10.11.11.99
 Interface                           : GigabitEthernet1/0/0
 Process ID                           : 99
 Instance ID                          : 1
 Reason for Neighbor down             : Interface down
 Time at which neighbor went down     : 2010-12-28 12:45:20+08:00
 Neighbor Router-id                    : 10.11.11.99
 Interface                           : GigabitEthernet1/0/0
 Process ID                           : 99
 Instance ID                          : 1
 Reason for Neighbor down             : One-way received
 Time at which neighbor went down     : 2010-12-28 12:45:20+08:00
```

Table 9-67 Description of the **display ospfv3 black-box neighbor-down** command output

Item	Description
Neighbor Router-id	Router ID of a neighbor whose neighbor relationship becomes Down
Interface	Interface of a device involved in a neighbor relationship
Process ID	ID of the OSPFv3 process to which the neighbor relationship belongs
Instance ID	ID of the OSPFv3 instance to which the neighbor relationship belongs

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason for Neighbor down	Reason why a neighbor relationship becomes Down: ● Interface down ● Dead timer Expired ● Sequence number mismatch ● One-way received ● Forced down ● Bad LS Request ● DR or BDR has changed
Time at which neighbor went down	Date and time at which the neighbor went Down.

9.5.18 display ospfv3 bfd session

Function

The **display ospfv3 bfd session** command displays bidirectional forwarding detection (BFD) session information of all OSPFv3 processes.

Format

display ospfv3 [*process-id*] **bfd session** [*interface-type interface-number*] [*neighbor-id*] [**verbose** | **all**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID for an OSPFv3 process. If the process number is not specified, the information about all OSPFv3 processes is displayed in an ascending order.	The value is an integer ranges from 1 to 65535.
interface-type interface-number	Specifies the type and number of the interface.	-
neighbor-id	Specifies router ID of the neighbor.	-
verbose	Displays detailed information of the neighbor.	-
all	Displays all the BFD sessions configured in OSPFv3.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The **display ospfv3 bfd session** command display bidirectional forwarding detection (BFD) session information of all OSPFv3 processes.

Example

Display BFD session information of all OSPFv3 processes.

```
<Huawei> display ospfv3 bfd session
* - STALE
OSPFv3 Process (1)
Neighbor-Id      Interface        BFD-Status
2.2.2.2          GE1/0/0          Up
OSPFv3 Process (2)
Neighbor-Id      Interface        BFD-Status
1.1.1.1          GE1/0/0          Up
2.2.2.2          GE1/0/0          Up
OSPFv3 Process (5)
Neighbor-Id      Interface        BFD-Status
1.1.1.1          GE1/0/0          Up
```

Table 9-68 Description of the **display ospfv3 bfd session** command output

Item	Description
* - STALE	Indicates stale BFD session.
OSPFv3 Process	Indicates ID of the OSPFv3 process.
Neighbor-Id	Indicates neighbor ID.
Interface	Indicates interface to which this session is associated.
BFD-Status	Indicates BFD session status: ● Up ● Down

Display the BFD session information for process 1 in details.

```
<Huawei> display ospfv3 1 bfd session verbose
* - STALE
OSPFv3 Process (1)
 Neighbor-Id: 3.3.3.3
 BFD Status: Up
 Interface: GE1/0/0
 IPv6-Local-Address: FE80::2E0:B1FF:FE49:8142
 IPv6-Remote-Address: FE80:23:22::
 BFD Module preferred timer values
    Transmit-Interval(ms): 1000
    Receive-Interval(ms): 1000
    Detect-Multiplier: 3
OSPFv3 Module preferred timer values
    Transmit-Interval(ms): 1000
```

```
    Receive-Interval(ms): 1000
    Detect-Multiplier: 3
Configured timer values
    Transmit-Interval(ms): 1000
    Receive-Interval(ms): 1000
    Detect-Multiplier: 3
```

Table 9-69 Description of the **display ospfv3 bfd session** command output

Item	Description
IPv6-Local-Address	Indicates Local IPv6 address to which this session is associated.
IPv6-Remote-Address	Indicates Remote IPv6 address to which this session is associated.
BFD Module preferred timer values	Indicates the actual BFD parameter values which are negotiated by BFD Module for the established session.
Transmit-Interval(ms)	Indicates the minimum interval for sending BFD packets.
Receive-Interval(ms)	Indicates the minimum interval between received BFD packets.
Detect-Multiplier	Indicates detection multiplier.
OSPFv3 Module preferred timer values	Indicates the preferred BFD parameter values across the processes sharing the session.
Configured timer values	Indicates the configured BFD parameter values for the neighbor.

Display all the BFD sessions in OSPFv3.

```
<Huawei> display ospfv3 bfd session all
* - STALE

BFD Session (1)
 BFD Status: Up
 Interface: GE1/0/0
 IPv6-Local-Address:  FE80::2E0:7FFF:FE0E:8142
 IPv6-Remote-Address: FE80::2E0:8BFF:FE68:8142
 Process-Id  Neighbor-Id
    1        10.13.1.1
BFD Session (2)
 BFD Status: Up
 Interface: GE1/0/0
 IPv6-Local-Address:  FE80::2E0:7FFF:FE0E:8442
 IPv6-Remote-Address: FE80::2E0:8BFF:FE68:8442
 Process-Id  Neighbor-Id
    5        10.13.1.1
```

Table 9-70 Description of the **display ospfv3 bfd session all** command output

Item	Description
BFD Session	Indicates BFD session number configured in OSPFv3.
Process-Id	Indicates process-id of the configured OSPFv3 process.
Neighbor-Id	Indicates OSPFv3 neighbor ID.

9.5.19 display ospfv3 error

Function

The **display ospfv3 error** command displays OSPFv3 errors.

Format

display ospfv3 [*process-id*] **error** [**lsa**]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID. If no OSPFv3 process number is specified, errors of all OSPFv3 processes are displayed.	The value ranges from 1 to 65535.
lsa	Display OSPFv3 LSA errors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

While analyzing OSPFv3 faults, you can obtain information of errors using the command. You can then diagnose OSPFv3 faults according to the information.

Example

Display OSPFv3 errors.

```
<Huawei> display ospfv3 error

        OSPFv3 Process 1 with Router ID 10.0.0.0
```

```
                OSPFv3 Error Statistics

General Packet Errors :
 0    : Bad packet                  0    : Bad version
 0    : Bad area ID                 0    : Bad virtual link
 0    : Packet too small            0    : Transmit error
 0    : Bad Instance ID             0    : Interface down
 0    : Unknown neighbor            0    : Authentication failure
 0    : AuthSeqNum mismatch         0    : AuthKeyId mismatch
 0    : IPv6: received my own packet  0    : Bad Checksum

Hello Packet Errors :
 0    : Hello timer mismatch        0    : Dead timer mismatch
 0    : Extern option mismatch      0    : Router ID confusion
 0    : Virtual neighbor unknown

DD Packet Errors :
 0    : Neighbor state low          0    : Extern option mismatch
 0    : Unknown LSA Type            0    : MTU option mismatch
 0    : Router ID confusion

LS ACK packet Errors :
 0    : Neighbor state low          0    : Bad ACK
 0    : Duplicate ACK               0    : Unknown LSA type

LS REQ packet Errors :
 0    : Neighbor state low          0    : Bad request
 0    : Empty Request

LS UPD packet Errors :
 0    : Neighbor state low          0    : LSA checksum bad
 0    : Received less recent LSA    0    : Unknown LSA type
 0    : Newer self-generate LSA
 0    : Received LSA within LSA Arrival interval

Receive Grace LSA errors :
 0    : Number of invalid LSAs
 0    : Number of policy failed LSAs
 0    : Number of wrong period LSAs

License Errors :
 0    : Max external routes reached   0    : Max NBRs reached
```

Table 9-71 Description of the **display ospfv3 error** command output

Item	Description
General Packet Errors	General packet errors.
Bad packet	The analyzed packet errors, including the verification of the length field.
Bad version	OSPFv3 version errors, that is, it is not version 3.
Bad area ID	Area ID in the received packet does not match. That is, when the area IDs in the received packets are different from the local area ID, except area 0, other area IDs are considered incorrect.
Bad virtual link	V-link receives illegal packets.

Item	Description
Packet too small	Length of the received packet is less than the sum of length of IP header and the length field of the packet.
Transmit error	Transmitting packets to socket fails.
Bad Instance ID	The Instance ID errors
Interface down	Times that the OSPFv3 interface goes Down.
Unknown neighbor	For NBMA, sham-link, and V-link networks, the device receives OSPFv3 packets from neighbors that are not enabled with OSPFv3.
Authentication failure	Times that the authentication failed.
AuthSeqNum mismatch	Number of packets with the mismatched receive sequence number.
AuthKeyId mismatch	Number of packets of which the key ID does not match the configured value.
IPv6: received my own packet	Number of IPv6 packets received from self.
Bad Checksum	The Checksum errors.
Hello Packet Errors	Hello packet errors.
Hello timer mismatch	The Hello interval is not consistent.
Dead timer mismatch	The Dead interval is not consistent.
Extern option mismatch	The extension attributes of the Hello packet are not consistent.
Router ID confusion	Router id is configured to the same.
Virtual neighbor unknown	Router id of the packet is inconsistent with that of the neighbor that is configured by the V-link.
DD Packet Errors	DD packet errors.
Neighbor state low	Cases of error: ● DD packet is received but its neighbor status is lower than 2-way. ● LSR packet is received but its neighbor status is lower than Exchange. ● LSU packet is received but its neighbor status is lower than Exchange. ● ACK packet is received but its neighbor status is lower than Exchange.
Extern option mismatch	Option of the DD packets is not matched.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Unknown LSA Type	The router receives unknown LSA type from neighbors that are not enabled with OSPFv3.
MTU option mismatch	MTU check of the interface on which OSPFv3 is enabled. The MTU value of the DD packet that is received on the interface is greater than that of this interface.
LS ACK packet Errors	LS ACK packet errors.
Bad ACK	Count of receiving incorrect ACK packets.
Duplicate ACK	Count of receiving repeat ACK packets.
LS REQ packet Errors	Title bar: LS REQ packet errors.
Bad request	BadRequest event in the protocol.
Empty Request	Number of Empty Request.
LS UPD packet Errors	LS UPD packet error.
LSA checksum bad	LSA checksum not proper
Received less recent LSA	Receiving older LSA than the local copy.
Newer self-generate LSA	LSA recently generated by self.
Received LSA within LSA Arrival interval	Received LSA within arrival interval.
Receive Grace LSA errors	Title bar: Grace LSA error.
Number of invalid LSAs	Number of LSAs that are invalid.
Number of policy failed LSAs	Number of LSAs with policy failure.
Number of wrong period LSAs	Number of LSAs with wrong period.
License Errors	License errors.
Max external routes reached	Number of external routes reached the maximum value.
Max NBRs reached	Number of neighbors reached the maximum value.

9.5.20 display ospfv3 graceful-restart-information

Function

The **display ospfv3 graceful-restart-information** command displays the status of OSPFv3 GR.

Format

display ospfv3 [*process-id*] **graceful-restart-information**

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process number. If the process number is not specified, the brief information about all OSPFv3 processes is displayed in an ascending order.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status of OSPFv3 GR.

```
<Huawei> display ospfv3 graceful-restart-information

          OSPFv3 Router with ID (10.0.0.0) (Process 1)

 Graceful-restart capability      : enabled
 Graceful-restart support         : planned and unplanned, strict lsa check
 Grace-Period Configured          : 120 Sec
 Last Restart-exit Reason         : none

 Helper capability                : enabled
 Helper support                   : planned and unplanned, strict lsa check
 Max Grace-Period Configured      : 1800 Sec
 Last Helper-exit Reason          : none
```

Table 9-72 Description of the **display ospfv3 graceful-restart-information** command output

Item	Description
Graceful-restart capability	Indicates whether GR is enabled. ● enabled ● disabled

Item	Description
Graceful-restart support	Indicates the GR configuration feature. ● planned: indicates that only the planned GR is supported. ● unplanned: indicates that only the un-planned GR is supported. ● strict lsa check: indicates that the Helper supports strict external LSA check.
Grace-Period Configured	Indicates the GR period.
Last Restart-exit Reason	Indicates the reason for the Restart device exiting from GR last time: ● none: indicates that no GR is performed. ● successful: indicates that the device is successfully restarted through GR, and then exits from GR. ● topology change: indicates that the network topology changes. ● grace lsa not recv: indicates that no Grace-LSAs are received. ● grace period exp: indicates that the GR period expires. ● process reset: indicates that a parameter of the OSPFv3 process is reset during GR. ● hold timer expire: indicates that the hold timer expires. ● interface address deleted: indicates that the interface address is deleted. ● interface down: indicates that the interface goes Down. ● DR/BDR change on network: indicates that the DR or BDR on the network changes. ● Received route uninstall notification: indicates that the message indicating that OSPFv3 routes are not installed to the RM is received.
Helper capability	Indicates whether Helper is enabled. ● enabled ● disabled

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Helper support	Indicates the Helper Graceful-restart configuration feature. ● planned: indicates that only the planned GR is supported. ● unplanned: indicates that only the un-planned GR is supported. ● strict lsa check: indicates that the Helper supports strict external LSA check.
Max Grace-Period Configured	Indicates the GR period.
Last Helper-exit Reason	Indicates the reason for the Helper device exiting from GR last time. ● none: indicates that the router never enters the Helper mode since it starts. ● successful: indicates that the Helper successfully exits from GR. ● topology change: indicates that the network topology changes. ● interface id change: indicates that the interface ID changes. ● grace period exp: indicates that GR period expires. ● hold timer expire: indicates that the hold timer expires. ● interface address deleted: indicates that the interface address is deleted.

9.5.21 display ospfv3 interface

Function

The **display ospfv3 interface** command displays the OSPFv3 interface.

Format

display ospfv3 [*process-id*] **interface** [**area** *area-id*] [*interface-type interface-number*]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID. The value of the area ID can be a decimal integer or in the IPv4 address format.	If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.
interface-type interface-number	Specifies the type and the number of the interface. If the interface is not specified, information of all OSPFv3 interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the OSPFv3 GigabitEthernet1/0/0.

```
<Huawei> display ospfv3 interface gigabitethernet 1/0/0

 GigabitEthernet1/0/0 is up, line protocol is up
   Interface ID 0x102
   Interface MTU 1500
   IPv6 Prefixes
     FE80::2E0:FFF:FE4E:F101 (Link-Local Address)
OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
   Router ID 10.1.1.1, Network Type BROADCAST, Cost: 1
   Transmit Delay is 1 sec, State Waiting, Priority 1
   Designated Router (ID) 10.1.1.1
   Interface Address FE80::2E0:9AFF:FE60:8142
   Backup Designated Router (ID) 10.3.3.3
   Interface Address FE80::2E0:68FF:FE05:8142
   Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
     Hello due in 00:00:02
   Neighbor Count is 0, Adjacent neighbor count is 1
   Interface Event: 2, Lsa Count: 2, Lsa Checksum: 0x9b74
   Interface Physical BandwidthHigh 0, BandwidthLow 100000000
   Suppress flapping peer: enable(flapping-count: 0, threshold: 3)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 9-73 Description of the **display ospfv3 interface** command output

Item	Description
Interface ID	Interface ID
Interface MTU	The MTU value
IPv6 Prefixes	IPv6 prefixes
Link-Local Address	The address of local link
OSPFv3 Process	OSPFv3 process ID
Area	Area that the interface belongs to
Instance ID	ID of the instance that the interface belongs to
Router ID	Router ID
Network Type	Network type of the interface that can be displayed as Point-to-Point and Broadcast
Cost	Cost of the interface
Transmit Delay	Transmission delay
State	State of the interface
Priority	Priority of the interface
Designated Router (ID)	Indicates designated router on the link
Backup Designated Router (ID)	Indicates backup designated router on the link
Timer interval configured	Configured interval ● Hello: Interval for sending Hello packets ● Dead: Interval of the Dead timer ● Wait: Interval of the Wait timer ● Retransmit: Retransmission interval
Hello due in	Indicates time remaining to send Hello packet
Neighbor Count	Number of neighbors
Adjacent neighbor count	Number of adjacency
Interface Event	Indicates number of events on this interface
Lsa Count	Total number of LSA in the interface scope database

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Lsa Checksum	Indicates checksum of all the LSAs in the database
Interface Physical BandwidthHigh	Maximum physical bandwidth on the interface
BandwidthLow	Minimum physical bandwidth on the interface

 Copyright © Huawei Technologies Co., Ltd.

Item	Description

Suppress flapping peer	Status of OSPFv3 neighbor relationship flapping suppression:
	● enable: OSPFv3 neighbor relationship flapping suppression is enabled.
	– flapping-count: number of valid flapping_events
	If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count increases by 1. To change *detecting-interval*, run the **ospfv3 suppress-flapping peer detecting-interval** *detecting-interval* command.
	– threshold: flapping suppression threshold
	When the flapping_count reaches or exceeds **threshold**, flapping suppression takes effect. To configure the threshold, run the **ospfv3 suppress-flapping peer threshold** *threshold* command.
	● disable: OSPFv3 neighbor relationship flapping suppression is disabled. In this case, the following information is displayed, without flapping-count or threshold:
	`Suppress flapping peer: disable`
	● hold-down: OSPFv3 neighbor relationship flapping suppression works in Hold-down mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-down(start: 2016-01-29 12:09:36-08:00, remain-interval: 500s)`
	– start: time when the flapping suppression started
	– remain-interval: remaining time of the flapping suppression
	● hold-max-cost: OSPFv3 neighbor relationship flapping suppression works in Hold-max-cost mode. In this case, an example of the displayed information is as follows:
	`Suppress flapping peer: hold-max-cost(start: 2016-01-29 12:09:36-08:00, remain-interval: 476s)`

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.5.49 ospfv3

9.5.22 display ospfv3 lsdb

Function

The **display ospfv3 lsdb** command displays the LSDB of OSPFv3.

Format

display ospfv3 [*process-id*] **lsdb** [**area** *area-id*] [**originate-router** *advertising-router-id* | **self-originate**] [{ **router** | **network** | **inter-router** [**asbr-router** *asbr-router-id*] | { **inter-prefix** | **nssa** } [*ipv6-address prefix-length*] | **link** | **intra-prefix** | **grace** } [*link-state-id*]]

display ospfv3 [*process-id*] **lsdb** [**originate-router** *advertising-router-id* | **self-originate**] **external** [*ipv6-address prefix-length*] [*link-state-id*]

display ospfv3 [*process-id*] **lsdb statistics**

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID. The value of the area ID can be a decimal integer or in the IPv4 address format.	If the value is a decimal integer, it ranges from 0 to 4294967295. If the value is an IPv4 address, it specifies the matched IP address in dotted decimal notation.
external	Displays the AS-external LSA in the LSDB. If the **area** parameter is selected, the **external** parameter cannot be selected.	-
grace	Displays the Grace-LSA in the LSDB.	-
inter-prefix	Displays the Inter-area-prefix LSA in the LSDB.	-
nssa	Displays the NSSA in the LSDB.	-
inter-router	Displays the Inter-area-router LSA in the LSDB.	-
intra-prefix	Displays the Intra-area-prefix LSA in the LSDB.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
link	Displays the Link-local LSA in the LSDB.	-
network	Displays the Network-LSA in the LSDB.	-
router	Displays the Router-LSA in the LSDB.	-
link-state-id	Indicates the link state ID.	It is in dotted decimal notation.
originate-router *advertising-router-id*	Specifies the Router ID of the router that advertises LSA packet.	It is in dotted decimal notation.
asbr-router *asbr-router-id*	Specifies the router ID of the ASBR.	It is in dotted decimal notation.
self-originate	Displays LSAs in the LSDB that are advertised by the local router.	-
ipv6-address prefix-length	Specifies the IPv6 destination address and the length of the prefix.	*ipv6-address* is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X. *prefix-length* is an integer ranging from 0 to 128.
statistics	Indicates the statistics of the LSDB.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the OSPFv3 LSDB.

```
<Huawei> display ospfv3 lsdb

* indicates STALE LSA

        OSPFv3 Router with ID (10.5.5.5) (Process 1)
            Link-LSA (Interface Vlanif1002)
```

```
Link State ID   Origin Router    Age   Seq#       CkSum  Prefix
0.0.0.71        10.2.2.2         0995  0x8000000c 0xa44c      1
0.0.0.69        10.5.5.5         0621  0x8000000f 0x20ff      1

            Router-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum    Link
0.0.0.0         10.2.2.2         0565  0x8000008b 0xa54f      1
0.0.0.0         10.5.5.5         0616  0x80000014 0x243c      1

            Network-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.71        10.2.2.2         0565  0x8000000a 0x585c

            Inter-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         10.2.2.2         0320  0x8000000c 0x6a0f
0.0.0.2         10.2.2.2         1637  0x8000000b 0xe1a3
0.0.0.1         10.5.5.5         0616  0x8000000d 0x81f7

            Intra-Area-Prefix-LSA (Area 0.0.0.0)

Link State ID   Origin Router    Age   Seq#       CkSum  Prefix  Reference
0.0.0.1         10.2.2.2         0564  0x8000000e 0x79a6      1  Network-LSA

            Router-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum    Link
0.0.0.0         10.5.5.5         0621  0x8000000b 0x8c84      0

            Inter-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         10.5.5.5         0621  0x8000000a 0x8f08
0.0.0.2         10.5.5.5         0612  0x8000000a 0x105d
0.0.0.3         10.5.5.5         0612  0x8000000a 0x85f2

            Intra-Area-Prefix-LSA (Area 0.0.0.1)

Link State ID   Origin Router    Age   Seq#       CkSum  Prefix  Reference
0.0.0.1         10.5.5.5         0621  0x8000000b 0xab89      1  Router-LSA

            Router-LSA (Area 0.0.0.3)

Link State ID   Origin Router    Age   Seq#       CkSum    Link
0.0.0.0         10.5.5.5         0621  0x8000000b 0x8092      0

            Inter-Area-Prefix-LSA (Area 0.0.0.3)

Link State ID   Origin Router    Age   Seq#       CkSum
0.0.0.1         10.5.5.5         0617  0x8000000b 0x85f5
0.0.0.2         10.5.5.5         0621  0x8000000a 0x8511
0.0.0.3         10.5.5.5         0612  0x8000000a 0x0666
0.0.0.4         10.5.5.5         0612  0x8000000a 0x7bfb

            NSSA-external-LSA (Area 0.0.0.3)

Link State ID   Origin Router    Age   Seq#       CkSum  Type
0.0.0.1         10.5.5.5         0626  0x8000000a 0xe72a E2
```

Table 9-74 Description of the **display ospfv3 lsdb** command output

Item	Description
Link-LSA	Description of the Link-LSA

Item	Description
Router-LSA	Description of the Router-LSA
Network-LSA	Description of the Network-LSA
Inter-Area-Prefix-LSA	Description of the Inter-Area-Prefix-LSA
NSSA-external-LSA	Description of the NSSA-external-LSA
Intra-Area-Prefix-LSA	Description of the Intra-Area-Prefix-LSA
AS-External-LSA	Description of the AS-external-LSA
Link State ID	Link state ID in LSA header
Origin Router	router that generates LSA
Age	Aging time of LSA
Seq#	Sequence number of LSA (from LSA header)
CkSum	Checksum of LSA
Link	Number of links in router LSA
Prefix	Number of prefixes in Link LSA
Reference	Router-LSA/Network-LSA reference information

Display the Link-local LSA in LSDB.

```
<Huawei> display ospfv3 lsdb link

          OSPFv3 Router with ID (10.2.2.2) (Process 1)

              Link-LSA (Interface GigabitEthernet1/0/0)
 LS age: 11
 LS Type: Link-LSA
 Link State ID: 0.0.2.6
 Originating Router: 10.2.2.2
 LS Seq Number: 0x80000002
 Retransmit Count: 0
 Checksum: 0xEFFA
 Length: 56
 Priority: 1
 Options: 0x000013 (-|R|-|-|E|V6)
 Link-Local Address: FE80::1441:0:E213:1
 Number of Prefixes: 1

   Prefix: 2000:1::/64
    Prefix Options: 0 (-|-|-|-|-)
```

Table 9-75 Description of the **display ospfv3 lsdb link** command output

Item	Description
LS age	Aging time of LSA

Item	Description
LS Type	Type of LSA: ● Router-LSA ● Network-LSA ● Inter-Area-Prefix-LSA ● Inter-Area-Router-LSA ● AS-external-LSA ● Link-LSA ● Intra-Area-Prefix-LSA ● NSSA-LSA
Link State ID	Link state ID in LSA header
Originating Router	Router that generates LSA
LS Seq Number	Sequence number of LSA (from LSA header)
Checksum	Checksum of LSA
Length	Length of the LSA
Priority	Priority of the interface that corresponds to the link.
Options	Value of options of the link
Link-Local Address	Link local address
Number of Prefixes	Number of IPv6 prefixes in the LSA
Prefix	IPv6 prefix
Prefix Options	Value of options of the prefix

Related Topics

9.5.49 ospfv3

9.5.23 display ospfv3 next-hop

Function

The **display ospfv3 next-hop** command displays the next-hop routing table of OSPFv3.

Format

display ospfv3 [*process-id*] **next-hop**

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the next-hop routing table of OSPFv3 process 1.

```
<Huawei> display ospfv3 1 next-hop
OSPFv3 Process (1)
Neighbor-Id     Next-Hop                        Interface   RefCount
3.3.3.9         FE80::2E0:FCFF:FE01:814F          GE1/0/0     1
```

Table 9-76 Description of the **display ospfv3 next-hop** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Neighbor-Id	Neighbor ID
Next-Hop	Next hop address
Interface	Egress
RefCount	Number of routes applying the next hop

9.5.24 display ospfv3 path

Function

The **display ospfv3 path** command displays the paths to a destination address.

Format

display ospfv3 [*process-id*] **path**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the process ID is not specified, paths in all processes are displayed.

Example

Display all OSPFv3 paths.

```
<Huawei> display ospfv3 path
OSPFv3 Process (1)
Type        AreaId/LSACost   PathCost
Intra       0.0.0.1          2
Inter       0.0.0.1          2
External    0.0.0.10         1
```

Table 9-77 Description of the **display ospfv3 path** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Type	Path type: ● Intra: indicates the intra-area routes. ● Inter: indicates the inter-area routes. ● External: indicates the AS-external routes.
AreaId/LSACost	● Area ID in case of an intra-area or inter-area path. ● LSA cost in case the path type is External. ● Cost in case of a path to a destination outside an AS
PathCost	Cost of the path

 Copyright © Huawei Technologies Co., Ltd.

9.5.25 display ospfv3 peer

Function

The **display ospfv3 peer** command displays the qualified OSPFv3 neighbor.

Format

display ospfv3 [*process-id*] [**area** *area-id*] **peer** [*interface-type interface-number* | *neighbor-id*] [**verbose**]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the neighbor of the specific area.	The area-id can be a decimal integer or in IPv4 address format. The integer ranges from 0 to 4294967295.
interface-type interface-number	Indicates the type and the number of the interface.	-
neighbor-id	Specifies router-ID of the neighbor.	It is in dotted decimal notation.
verbose	Displays detailed information of the neighbor of each area.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display neighbor information about OSPFv3 process 1 on GigabitEthernet1/0/0.

```
<Huawei> display ospfv3 1 peer gigabitethernet 1/0/0
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.0)
Neighbor ID     Pri  State          Dead Time Interface          Instance ID
1.1.1.1           1  Full/ -        00:00:30  GE1/0/0              0
```

Display the detailed neighbor information of OSPFv3 process 100 on GigabitEthernet1/0/0.

```
<Huawei> display ospfv3 100 peer gigabitethernet 1/0/0 verbose
OSPFv3 Process (100)
 Neighbor 10.1.1.1 is Full, interface address FE80::3D43:0:8C14:1
    In the area 0.0.0.1 via interface GigabitEthernet1/0/0
    DR Priority is 1 DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)
    Dead timer due in 00:00:29
    Neighbour is up for 18:40:40
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
    Neighbour Event: 6
    Neighbour If Id: 0x1017
```

Table 9-78 Description of the **display ospfv3 peer** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
OSPFv3 Area	ID of the OSPFv3 area
Neighbor ID	Neighbor ID
Pri	Priority of the neighbor router
State	State of the neighbor, including Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, and Full
Dead Time	Dead time of the neighbor
Interface	Interface that connects with the neighbor
Instance ID	ID of the instance that the neighbor belongs to
Neighbor	Neighbor ID
interface address	Link address of the neighbor interface
In the area 0.0.0.1 via interface GigabitEthernet1/0/0	GigabitEthernet 1/0/0 of the neighbor is in Area 1
DR Priority	Priority of DR
DR	Designated Router
BDR	Border Area Router
Options	Options of the neighbor
Dead timer due in 00:00:29	Time before the neighbor dies
Database Summary Packets List	Number of packets in the database summary list of the neighbor

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Link State Request List	Number of LSAs in the request list of the neighbor
Link State Retransmission List	Number of LSAs in the retransmission list of the neighbor
Neighbour Event	Number of times NFSM (Neighbor Finite State Machine) state changed
Neighbour If Id	Interface ID of the neighbor

9.5.26 display ospfv3 request-list

Function

The **display ospfv3 request-list** command displays the statistics of the request list of OSPFv3.

Format

display ospfv3 [*process-id*] **request-list** [[**area** *area-id* | **interface** *interface-type interface-number* | **peer** *router-id*] * | **statistics**]

Parameters

Parameter	Description	Value
process-id	Specifies the process ID of OSPFv3.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID.	The integer ranges from 0 to 4294967295. The value of the area ID can be a decimal integer or in the IPv4 address format.
interface *interface-type interface-number*	Specifies the type and number of the interface.	-
peer *router-id*	Indicates the Router ID of a neighbor.	It is in dotted decimal notation.
statistics	Displays the statistics of the request list of OSPFv3.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The display of the command is used to diagnose faults.

Example

Display the statistics of the request list in OSPFv3.

```
<Huawei> display ospfv3 request-list
  OSPFv3 Process (1)
  Interface  GE1/0/0        Area-ID   0.0.0.1
  Nbr-ID   10.254.255.255
  LS-Type              LS-ID          AdvRouter       SeqNum       Age
  Link-LSA             0.0.2.2        10.254.255.255  0x80000001   151
  Router-LSA           0.0.0.0        10.254.255.255  0x80000005   46
  Intra-Area-Prefix-LSA 0.0.0.1       10.254.255.255  0x80000001   45
  AS-External-LSA      0.0.0.1        10.254.255.255  0x80000001   113
  AS-External-LSA      0.0.0.2        10.254.255.255  0x80000001   113
```

Table 9-79 Description of the **display ospfv3 request-list** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Interface	Interface that connects with the neighbor
Area-ID	ID of the area that the interface belongs to
Nbr-ID	Router ID of the neighbor
LS-Type	LSA type: ● Link-LSA: is generated by the router for each link and is advertised in the local link. ● Router-LSA: is generated by each router and advertised in the area whether the router resides. It describes the link state and cost of the router. ● Intra-Area-Prefix-LSA: – An LSA generated on a router describes the IPv6 address prefix associated with the router LSA. – An LSA generated on a DR describes the IPv6 address prefix associated with the network LSA. ● AS-External-LSA: is generated by the ASBR and is advertised to the entire AS (except the stub area). It describes the routes that reach other ASs.
LS-ID	Link State ID (from LSA header)
AdvRouter	Advertising router (from LSA header)
SeqNum	Sequence number (from LSA header)

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Age	Aging time (from LSA header)

9.5.27 display ospfv3 retrans-list

Function

The **display ospfv3 retrans-list** command displays the statistics of the retransmission list in OSPFv3.

Format

display ospfv3 [*process-id*] **retrans-list** [[**area** *area-id* | **interface** *interface-type interface-number* | **peer** *router-id*] * | **statistics**]

Parameters

Parameter	Description	Value
process-id	Specifies the process ID of OSPFv3.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID.	The integer ranges from 0 to 4294967295. The value of the area ID can be a decimal integer or in the IPv4 address format.
interface *interface-type interface-number*	Specifies the type and number of the interface.	-
peer *router-id*	Indicates the Router ID of a neighbor.	It is in dotted decimal notation.
statistics	Displays the statistics of the retransmission list in OSPFv3.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The display of the command is used to diagnose faults.

Example

Display the statistics of the retransmission list in OSPFv3.

```
<Huawei> display ospfv3 retrans-list
    OSPFv3 Process (1)
    Interface  GE1/0/0        Area-ID   0.0.0.1
    Nbr-ID   10.22.2.255
    LS-Type              LS-ID          AdvRouter       SeqNum       Age
    Network-LSA          0.0.2.2        10.254.255.255  0x80000002   1
    Intra-Area-Prefix-LSA 0.0.0.2       10.254.255.255  0x80000002   1
```

Table 9-80 Description of the **display ospfv3 retrans-list** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
Interface	Interface that connects with the neighbor
Area-ID	ID of the area that the interface belongs to
Nbr-ID	Router ID of the neighbor
LS-Type	LSA type: ● Network-LSA: is generated by the DR of a broadcast network or an NBMA network and is advertised in the area where the DR resides. It describes the link state of the network segment. ● Intra-Area-Prefix-LSA: – An LSA generated on a router describes the IPv6 address prefix associated with the router LSA. – An LSA generated on a DR describes the IPv6 address prefix associated with the network LSA.
LS-ID	Link State ID (from the LSA header)
AdvRouter	Advertising router (from LSA header)
SeqNum	Sequence number (from LSA header)
Age	Aging time (from LSA header)

9.5.28 display ospfv3 routing

Function

The **display ospfv3 routing** command displays the OSPFv3 routing table.

Format

display ospfv3 [*process-id*] **routing** [*ipv6-address prefix-length* | **abr-routes** | **asbr-routes** | **intra-routes** | **inter-routes** | **ase-routes** | **nssa-routes** | [**statistics**] [**uninstalled**]]

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
ipv6-address	Indicates the IPv6 address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of the prefix.	The value is an integer ranging from 0 to 128.
abr-routes	Displays the routing table of ABR in OSPFv3.	-
asbr-routes	Displays routing table of ASBR in OSPFv3.	-
intra-routes	Displays the statistics of OSPFv3 routes in an area.	-
inter-routes	Displays the statistics of OSPFv3 routes between areas.	-
ase-routes	Displays the statistics of OSPFv3 routes outside an AS.	-
nssa-routes	Displays the statistics of OSPFv3 routes in an NSSA.	-
statistics	Displays the statistics of all routing tables.	-
uninstalled	Displays the routes are not installed into the RM.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

By using this command with different parameters, you can view the routes of a specified interface or next hop.

The command output can help you troubleshoot OSPFv3 faults.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the OSPFv3 routing table.

```
<Huawei> display ospfv3 routing

Codes : E2 - Type 2 External, E1 - Type 1 External, IA - Inter-Area,
        N - NSSA, U - Uninstalled, D - Denied by Import Policy
OSPFv3 Process (1)
     Destination                                    Metric
       Next-hop
     U  100::/64                                     1
       via FE80::2E0:48FF:FE66:2701, GigabitEthernet2/0/0
     2000:1::/64                                     3124
       via FE80::1441:0:E213:1, GigabitEthernet1/0/0
```

Table 9-81 Description of the **display ospfv3 routing** command output

Item	Description
Codes	The following information provides the full spelling and explanation: ● E2: Type 2 external route ● E1: Type 1 external route ● IA: Inter-area route ● N: NSSA route ● U: OSPFv3 routers that not advertise to IPv6 router table ● D: OSPFv3 routes denied by import route policy
OSPFv3 Process	OSPFv3 process
Destination	Destination address
Metric	Metric to the destination
Next-hop	Next hop to the destination
U	display OSPFv3 routes that not advertise to IPv6 routing table

Related Topics

9.5.49 ospfv3

9.5.29 display ospfv3 topology

Function

The **display ospfv3 topology** command displays the OSPFv3 area topology.

Format

display ospfv3 [*process-id*] **topology** [**area** *area-id*]

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the area ID.	The value of the area ID can be a decimal integer or in the IPv4 address format. The integer ranges from 0 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the topology of OSPFv3 area 1.

```
<Huawei> display ospfv3 topology area 1
OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)      Bits     Metric    Next-Hop        Interface
Rtr   1.1.1.1                    --
```

Table 9-82 Description of the **display ospfv3 topology** command output

Item	Description
OSPFv3 Process	ID of the OSPFv3 process
OSPFv3 Area	ID of the OSPFv3 area
Type	SPF type: ● Rtr: Router ● Net: Network
ID (If-Index)	Router ID (If-Index) is the interface ID of the DR in the network type.
Bits	B bit and E bit indicates router type ● B bit: ABR ● E bit: ASBR
Metric	Metric of path to the node

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Next-Hop	Next hop of the path to the node
Interface	Egress of the path to the node

Related Topics

9.5.49 ospfv3

9.5.30 display ospfv3 vlink

Function

The **display ospfv3 vlink** command displays the OSPFv3 virtual links.

Format

display ospfv3 [*process-id*] **vlink**

Parameters

Parameter	Description	Value
process-id	Identifies the OSPFv3 process ID.	The value ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ospfv3 vlink** command is used to display OSPFv3 virtual links.

Example

Display OSPFv3 virtual links.

```
<Huawei> display ospfv3 vlink
OSPFv3 Process (100)

Virtual Link VLINK1 to router 10.2.2.2 is up
 Transit area 0.0.0.1 via interface GigabitEthernet1/0/0, instance ID 0
 Local address FC00:0:0:2000::1
 Remote address FC00:0:0:1001::2
 Interface ID 0x80000001
 VirtualInterface Event: 1
 VirtualInterface LsaCount: 0
 VirtualInterface Lsa Checksum: 0x0
 Transmit Delay is 1 sec, State Point-To-Point, Cost 1562
```

```
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Adjacency state Init
```

Table 9-83 Description of the **display ospfv3 vlink** command output

Item	Description
Transit area	If the current interface is the V-link interface, the transfer area ID is displayed
via interface	Interface of the V-link
instance ID	Instance ID
Local address	Local address
Remote address	Remote address
Interface ID	Interface ID
VirtualInterface Event	Number of interface events of the V-link
VirtualInterface LsaCount	Number of LSAs sent from all V-link interfaces
VirtualInterface Lsa Checksum	Checksum of the LSA sent from the V-link interface
Transmit Delay	Transmission delay of the interface
State	Interface state: ● Down ● Point-to-Point
Cost	Cost
Timer intervals	Timers: ● Hello: Hello interval ● Dead: Interval of Dead timer ● Wait: Interval of Wait timer. It is pointless to use a virtual link. ● Retransmit: Retransmission interval
Adjacency state	State of the V-link: ● Down ● Init ● Exch ● Start ● Exchange ● Loading ● Full

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.5.85 vlink-peer (OSPFv3)

9.5.31 display ospfv3 statistics maxage-lsa

Function

The **display ospfv3 statistics maxage-lsa** command displays information about MaxAge Router LSAs.

Format

display ospfv3 [*process-id*] **statistics maxage-lsa**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process. If no process ID is specified, information about MaxAge Router LSAs in all OSPFv3 processes is displayed.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To query information about MaxAge Router LSAs, run the **display ospfv3 statistics maxage-lsa** command. The command output helps troubleshooting route flapping.

Example

Display information about MaxAge Router LSAs.

```
<Huawei> display ospfv3 statistics maxage-lsa

         OSPFv3 Process 1 with Router ID 10.10.10.2
                Statistics of Router-LSAs
         ---------------------------------------------------

                      Area: 0.0.0.1
Origin Router              MaxAge count     Last MaxAge time
10.10.10.2                        1  2015-07-25 15:06:49
```

Table 9-84 Description of the **display ospfv3 statistics maxage-lsa** command output

Item	Description
Origin Router	Device that advertised the MaxAge Router LSA
MaxAge count	Number of times an LSA reached the maximum aging time
Last MaxAge time	Time when an LSA last reached the maximum aging time

9.5.32 display snmp-agent trap feature-name ospfv3 all

Function

The **display snmp-agent trap feature-name ospfv3 all** command displays all trap messages of the OSPFv3 module.

Format

display snmp-agent trap feature-name ospfv3 all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all trap messages of the OSPFv3 module.

```
<Huawei> display snmp-agent trap feature-name ospfv3 all
-----------------------------------------------------------------
Feature name: ospfv3
Trap number : 12
-----------------------------------------------------------------
Trap name                    Default switch status   Current switch status
virtifstatechange             off                     off
nbrstatechange                 off                     off
virtnbrstatechange             off                     off
ifconfigerror                 off                     off
```

```
virtifconfigerror                    off                    off
ifrxbadpacket                        off                    off
virtifrxbadpacket                    off                    off
ifstatechange                        off                    off
restartstatuschange                  off                    off
nbrrestarthelperstatuschange         off                    off
virtnbrrestarthelperstatuschange
                                     off                    off
nssatranslatorstatuschange           off                    off
lastauthenticationkeyexpiry          off                    off
authenticationsequencenumberwrap     off                    off
intraarearouteridconflictrecovered
                                     off                    on
peerflappingsuppressstatuschange
                                     off                    on
```

Table 9-85 Description of the **display snmp-agent trap feature-name ospfv3 all** command output

Item	Description
Feature name	Name of feature
Trap number	Number of traps of OSPFv3 module.

Item	Description
Trap name	Name of traps of OSPFv3 module, including: ● virtifstatechange: enables the traps for virtual interface state changes. ● nbrstatechange: enables the traps for neighbor state changes. ● virtnbrstatechange: enables the traps for neighbor state changes on the virtual-link. ● ifconfigerror: enables the traps for interface configuration errors. ● virtifconfigerror: enables the traps for virtual interface configuration errors. ● ifrxbadpacket: enables the traps for bad packets received on the interface. ● virtifrxbadpacket: enables the traps for bad packets received on the virtual interface. ● ifstatechange: enables the traps for the interface state changes. ● restartstatuschange: enables the traps for restarter state changes during GR. ● nbrrestarthelperstatuschange: enables the traps for helper state changes during GR. ● virtnbrrestarthelperstatuschange: enables the traps for helper state changes during GR on the virtual link. ● nssatranslatorstatuschange: enables the traps for the NSSA translator state changes. ● lastauthenticationkeyexpiry: enables the trap for last authentication key in keychain expiry. ● authenticationsequencenumberwrap: enables the trap for cryptographic sequence number wrapping. ● intraarearouteridconflictrecovered : enables the trap for router ID conflict resolving. ● peerflappingsuppressstatuschange : enables the trap for neighbor flapping suppression status changes.
Default switch status	Status of the default trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Status of the current trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

9.5.78 snmp-agent trap enable feature-name ospfv3

9.5.33 domain-id (OSPFv3)

Function

The **domain-id** command sets an OSPFv3 domain ID.

The **undo domain-id** command restores the default setting.

By default, the domain ID is null.

Format

domain-id { **null** | *domain-id* [**type** *type* **value** *value* | **secondary**] * }

undo domain-id { *domain-id* [**type** *type* **value** *value*] }

Parameters

Parameter	Description	Value
null	Specifies the OSPFv3 domain ID to null.	-
domain-id	Specifies the OSPFv3 domain ID.	It can be expressed by an integer or in dotted decimal notation. If the domain ID is expressed by an integer, its value ranges from 0 to 4294967295; it is converted to the dotted decimal notation and carried 1 with 256 when being displayed. If the domain ID is in dotted decimal notation format, it is displayed as originally entered.
type *type*	Specifies the type of the OSPFv3 domain ID.	The value is an integer that can be 0005, 0105, 0205, or 8005. The default value is 0005.
value *value*	Specifies the value of the OSPFv3 domain ID type.	The value is a hexadecimal number that ranges from 0 to FFFF. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
secondary	Indicates the ID of a secondary domain.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Generally, the routes that are imported from a PE are advertised as External-LSAs. The routes that belong to different nodes of the same OSPFv3 domain are advertised as Type 3 LSAs (intra-domain routes). This requires that different nodes in the same OSPFv3 domain have the same domain ID.

Two values, 0 and null, of the domain ID indicate different meanings.

The maximum number of secondary domain IDs on each OSPFv3 process is 10. The maximum number of secondary domain IDs may vary with products.

The parameter **secondary** can be configured only when the primary domain ID is configured. When the **undo domain-id** command is run, if no parameter is specified, the primary domain ID is deleted.

Example

Set the VPN domain ID in OSPFv3 VPN extension.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] ipv6-family
[Huawei-vpn-instance-huawei] route-distinguisher 100:1
[Huawei-vpn-instance-huawei] quit
[Huawei] ospfv3 1 vpn-instance huawei
[Huawei-ospfv3-1] domain-id 234
```

9.5.34 filter export (OSPFv3)

Function

The **filter export** command filters the outgoing Type3 LSAs of the local area.

The **undo filter export** command restores the default setting.

By default, the outgoing Type3 LSAs of the local area cannot be filtered.

Format

filter { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export**

undo filter [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **export**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used to filter out invalid LSAs sent to neighbors to reduce the size of the LSDB and speed up network convergence.

Configuration Impact

After filtering conditions are set for the outgoing Type3 LSAs to be advertised using the **filter export** command, only the outgoing Type3 LSAs that pass the filtering can be received and advertised.

Precautions

- The command can be configured only on an ABR.
- For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **filter import (OSPFv3)** command to set filtering conditions for the incoming Type3 LSAs to be advertised.

Example

Configure OSPFv3 to filter the outgoing Type3 LSAs.

```
<Huawei> system-view
[Huawei] ospfv3 100
[Huawei-ospfv3-100] area 1
[Huawei-ospfv3-100-area-0.0.0.1] filter 2000 export
```

9.5.35 filter import (OSPFv3)

Function

The **filter import** command filters the incoming Type3 LSAs of the local area.

The **undo filter import** command restores the default setting.

By default, the incoming Type3 LSAs cannot be filtered.

Format

filter { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used to filter out invalid LSAs sent to neighbors to reduce the size of the LSDB and speed up network convergence.

Configuration Impact

After filtering conditions are set for the incoming Type3 LSAs to be advertised using the **filter import** command, only the incoming Type3 LSAs that pass the filtering can be received and advertised.

Precautions

- The command can be configured only on an ABR.
- For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule takes effective only when the source address range is specified by the **source** parameter and the time period is specified by the **time-range** parameter.
- Run the **filter export (OSPFv3)** command to set filtering conditions for the outgoing Type3 LSAs to be advertised.

Example

Filter incoming Type3 LSAs within the local area.

```
<Huawei> system-view
[Huawei] ospfv3 100
[Huawei-ospfv3-100] area 1
[Huawei-ospfv3-100-area-0.0.0.1] filter ipv6-prefix my-prefix-list import
```

9.5.36 filter-policy export (OSPFv3)

Function

The **filter-policy export** command sets the OSPFv3 rules to filter the imported routes.

The **undo filter-policy export** command restores the default setting.

By default, the imported routes are not filtered.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl6-number	Specifies the ACL6 number.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a IPv6 Named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ipv6-prefix *ipv6-prefix-name*	Specifies the name of the prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the protocol from which the route is imported. If the routes of other protocols are imported, you can use the parameter to filter the imported routes. If the parameter is the default one, all imported routes are filtered.	It can be **bgp**, **direct**, **isis**, **unr**, **ospfv3**, **ripng,** or **static**.
process-id	Needs to be specified for **ripng**, **isis,** or **ospfv3**.	The value is an integer ranging from 1 to 65535.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

The **filter-policy export** command is only valid for the routes that are imported by using the **import-route** command.

Example

Filter the imported routes based on the rule defined by ACL6 2002.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] filter-policy 2002 export
```

Related Topics

9.5.40 import-route (OSPFv3)

9.5.37 filter-policy import (OSPFv3)

Function

The **filter-policy import** command sets the OSPFv3 rules to filter the received routes.

The **undo filter-policy import** command restores the default setting.

By default, the received routes are not filtered.

Format

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the ACL6 number.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a IPv6 Named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ipv6-prefix *ipv6-prefix-name*	Specifies the name of the IPv6 address prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **filter-policy import** command only filters the routes calculated by OSPFv3. Routes that do not pass the filtering are neither added to the OSPFv3 routing table nor advertised.

For a IPv6 Named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Filter the received routes based on the IPv6 address prefix list named **abc**.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] filter-policy ipv6-prefix abc import
```

9.5.38 graceful-restart (OSPFv3)

Function

The **graceful-restart** command enables GR of the OSPFv3 process.

The **undo graceful-restart** command disables GR of the OSPFv3 process.

By default, OSPFv3 GR is not enabled.

Format

graceful-restart [**period** *period* | **ack-time** *time* | **retransmit-interval** *interval* | **lsa-checking-ignore** | **planned-only**] *

undo graceful-restart [**period** [*period*] | **ack-time** [*time*] | **retransmit-interval** [*interval*] | **lsa-checking-ignore** | **planned-only**] *

Parameters

Parameter	Description	Value
period *period*	Specifies the GR period.	The value is an integer ranging from 1 to 1800, expressed in seconds. By default, the value is 120 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ack-time *time*	Specifies the period during which a router waits for the Grace-LSA Ack message from its neighbor.	The value is an integer ranging from 1 to 30, expressed in seconds. By default, the value is 15 seconds.
retransmit-interval *interval*	Specifies the interval for retransmitting Grace-LSAs.	The value is an integer ranging from 1 to 5, expressed in seconds. By default, the value is 5 seconds.
lsa-checking-ignore	Indicates that strict check is not performed on LSAs. By default, routers perform strict check on received LSAs.	-
planned-only	Indicates that routers support Planned-GR only. By default, routers support Planned-GR and Unplanned-GR.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

ack-time is an optional parameter. After the parameter is specified, the restarter can discover more neighbors in *ack-time* period.

Example

Enable GR of the OSPFv3 process.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] graceful-restart
```

9.5.39 helper-role (OSPFv3)

Function

The **helper-role** command configures a router to support the GR Helper mode.

The **undo helper-role** command cancels GR Helper mode.

By default, the router is not enabled to support GR Helper mode.

 Copyright © Huawei Technologies Co., Ltd.

Format

helper-role [{ **ip-prefix** *ip-prefix-name* | **acl-number** *acl-number* | **acl-name** *acl-name* } | **max-grace-period** *period* | **planned-only** | **lsa-checking-ignore**] *

undo helper-role [[**ip-prefix** [*ip-prefix-name*] | **acl-number** [*acl-number*] | **acl-name** [*acl-name*]] | **max-grace-period** *period* | **planned-only** | **lsa-checking-ignore**] *

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
acl-number *acl-number*	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a IPv6 Named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
max-grace-period *period*	Specifies the permitted maximum restart period.	The value is an integer ranging from 1 to 1800, expressed in seconds. By default, the value is 1800 seconds.
planned-only	Indicates that routers support Planned-GR only. By default, routers support Planned-GR and Unplanned-GR.	-
lsa-checking-ignore	Indicates that strict check is not performed on LSAs. By default, routers perform strict check on received LSAs.	-

Views

OSPFv3 view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Routers cannot use the helper mode during the GR process.

For a Named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Configure a router to support the helper mode.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] helper-role acl-number 2001 max-grace-period 250 planned-only lsa-checking-ignore
```

Related Topics

9.5.20 display ospfv3 graceful-restart-information

9.5.40 import-route (OSPFv3)

Function

The **import-route** command imports an external route. Before the routes are imported, the OSPFv3 process of the route must be active.

The **undo import-route** command stops importing external routes.

By default, no route of other protocols is imported.

Format

import-route { **bgp** [**permit-ibgp**] | **unr** | **direct** | **ripng** *help-process-id* | **static** | **isis** *help-process-id* | **ospfv3** *help-process-id* } [{ **cost** *cost* | **inherit-cost** } | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*] *

undo import-route { **bgp** | **unr** | **direct** | **ripng** *help-process-id* | **static** | **isis** *help-process-id* | **ospfv3** *help-process-id* }

Parameters

Parameter	Description	Value
bgp	Specifies the protocol from which routes are imported, as **bgp**.	-
permit-ibgp	IBGP routes that are permitted to be imported. The import of IBGP routes may cause route loops. Therefore, this command must not be configured unless it is necessary.	-

Parameter	Description	Value
unr	Specifies the imported source routing protocol as **unr**. User Network Route (UNR) is allocated if dynamic routing protocols cannot be used when users are getting online.	-
direct	Specifies the imported source routing protocol as **direct**.	-
ripng	Specifies the protocol from which routes are imported, as **ripng**.	-
static	Specifies the imported source routing protocol as **static**.	-
isis	Specifies the protocol from which routes are imported, as **isis**.	-
ospfv3	Specifies the protocol from which routes are imported, as **ospfv3**.	-
help-process-id	Specifies the process ID of the imported source protocol. When the imported protocol is **ripng**, **isis** or **ospfv3**, you should specify the parameter.	The value is an integer ranging from 1 to 65535.
cost *cost*	Indicates the cost of the imported route.	The value is an integer ranging from 1 to 16777214. By default, it is 1.
inherit-cost	Indicates the original cost of the imported routes.	-
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. By default, it is 2. ● 1: Type 1 external route ● 2: Type 2 external route
tag *tag*	Specifies the tag value of the imported routes.	The value is an integer that ranges from 0 to 4294967295. By default, the value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the routing policy. Only the routes that match the *route-policy-name* are imported.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

On a non-PE device, only EBGP routes are imported after the **import-route bgp** command is configured. IBGP routes are also imported after the **import-route bgp permit-ibgp** command is configured. If IBGP routes are imported, routing loops may occur. In this case, run the **preference (OSPFv3)** and **preference (BGP)** commands to prevent loops by specifying preferences of OSPFv3 and BGP routes. If IBGP routes need to be imported, configure the **import-route bgp permit-ibgp** command, and run the **preference (OSPFv3)** and **preference (BGP)** commands to set the preference of OSPFv3 ASE routes lower than that of IBGP routes (preference value of OSPFv3 ASE routes larger than that of IBGP routes).

On a PE, configuring the **import-route bgp** command imports both EBGP routes and IBGP routes, no matter whether the **import-route bgp permit-ibgp** command is configured or not. If the **import-route bgp permit-ibgp** command and the **default-route-advertise (OSPFv3)** command are both configured, the active IBGP default routes can be imported into OSPFv3.

NOTE

After the **import-route direct** command is executed, routes to the network segment where the IPv6 address of the management interface belongs are also imported in the OSPFv3 routing table. Therefore, use this command with caution.

Example

Import the RIPng route of type 2. The cost of the route is 50.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] import-route ripng 1 type 2 cost 50
```

OSPFv3 process 100 imports the routes discovered by OSPFv3 process 160.

```
<Huawei> system-view
[Huawei] ospfv3 100
[Huawei-ospfv3-100] import-route ospfv3 160
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.5.36 filter-policy export (OSPFv3)

9.5.41 ipsec sa (OSPFv3)

Function

The **ipsec sa** command configures an SA in an OSPFv3 area or OSPFv3 process.

The **undo ipsec sa** command deletes the SA configured in an OSPFv3 area or OSPFv3 process.

By default, no SA is configured in an OSPFv3 area or OSPFv3 process.

Format

ipsec sa *sa-name*

undo ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of an SA.	The value is a string of 1 to 15 case-insensitive characters without spaces.

Views

OSPFv3 view or OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SA defines a set of security algorithms and keys to ensure IP security. Incoming and outgoing OSPFv3 packets are authenticated and encrypted based on the rules defined by the SA.

The **ipsec sa** *sa-name* command run in the OSPFv3 process view is used to authenticate packets of the OSPFv3 process. An SA applied in an OSPFv3 process is used to authenticate the packets of this process. After an OSPFv3 process is associated with an OSPFv3 area, the SA applied in the OSPFv3 process is also applied to the OSPFv3 area.

The **ipsec sa** *sa-name* command run in the OSPFv3 area view is used to authenticate packets of the OSPFv3 area.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The SA applied in an OSPFv3 area takes precedence over that applied in an OSPFv3 process.
- If the SA applied in the OSPFv3 area is deleted, the SA applied in the OSPFv3 process is used to authenticate packets.

Prerequisites

Before configuring the **ipsec sa** command, ensure that an **IPSec proposal** and IPSec SA have been configured on the device.

Example

Configure an SA named **sa1** in an OSPFv3 process.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] ipsec sa sa1
```

9.5.42 lsa-arrival-interval (OSPFv3)

Function

The **lsa-arrival-interval** command sets the interval for receiving OSPFv3 LSA.

The **undo lsa-arrival-interval** command restores the default setting.

By default, the interval for receiving OSPFv3 LSAs is 1000 milliseconds.

Format

lsa-arrival-interval *arrival-interval*

undo lsa-arrival-interval

Parameters

Parameter	Description	Value
arrival-interval	Specifies the interval for receiving OSPFv3 LSAs.	The value is an integer ranging from 1 to 10000, in milliseconds. The default value is 1000.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

To prevents too many device resources from being consumed due to network connections or frequent route flapping, the **lsa-arrival-interval** command can be

used to set the interval for receiving OSPFv3 LSAs. A device updates an LSA only when the receiving interval expires.

On a stable network where routes need to be rapidly converged, the **lsa-arrival-interval** command can be used to set the millisecond-level interval for receiving LSAs and update LSAs in time so that topology changes or route changes can be immediately sensed. In this manner, the LSDB synchronization can speed up.

Example

Set the interval for receiving OSPFv3 LSAs to 10000 ms.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] lsa-arrival-interval 10000
```

9.5.43 lsa-forwarding-address(OSPFv3)

Function

The **lsa-forwarding-address** command enables the OSPFv3 forwarding address (FA) function.

The **undo lsa-forwarding-address** command disables the OSPFv3 FA function.

By default, the OSPFv3 FA function is disabled.

Format

lsa-forwarding-address { **standard** | **zero-translate** }

undo lsa-forwarding-address

Parameters

Parameter	Description	Value
standard	Indicates that the function is compatible with RFC 3101.	-
zero-translate	Allows the Type 7 LSAs with the P-bit set and the FA being 0 to be translated to Type 5 LSAs.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

The FA in an OSPFv3 Type 5 or Type 7 LSA is used to notify the devices in the local routing domain of the shortcut next hop to the AS external network described in the LSA. This prevents internal devices from routing packets to themselves as the

next hop before forwarding the packets to the devices in the external routing domain on the same broadcast network.

To enable the OSPFv3 FA function, run the **lsa-forwarding-address** { **standard** | **zero-translate** } command.

Example

Enable the OSPFv3 FA function that is compatible with RFC 3101.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] lsa-forwarding-address standard
```

9.5.44 lsa-originate-interval (OSPFv3)

Function

The **lsa-originate-interval** command sets the interval for updating OSPFv3 LSAs.

The **undo lsa-originate-interval** command restores the default setting.

By default, the interval for updating OSPFv3 LSAs is the default value of the SPF intelligent timer.

Format

lsa-originate-interval intelligent-timer *lsa-originate-max-interval lsa-originate-start-interval hold-interval*

undo lsa-originate-interval

lsa-originate-interval suppress-flapping *suppress-interval* [**threshold** *count*]

undo lsa-originate-interval suppress-flapping

Parameters

Parameter	Description	Value
intelligent-timer	Sets the interval for updating OSPFv3 Type 1 Router-LSAs, Type 2 Network-LSAs, and Type 8 Link-LSAs by using an intelligent timer.	-
lsa-originate-max-interval	Specifies the maximum interval for updating OSPFv3 LSAs.	The value ranges from 1 to 10000, in milliseconds. The default value is 5000.
lsa-originate-start-interval	Specifies the initial interval for updating OSPFv3 LSAs.	The value ranges from 0 to 1000, in milliseconds. The default value is 500.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hold-interval	Specifies the hold interval for updating OSPFv3 LSAs.	The value ranges from 1 to 5000, in milliseconds. The default value is 1000.
suppress-flapping *suppress-interval*	Specifies the maximum OSPFv3 LSA suppression period.	The value is an integer ranging from 0 to 600, in seconds. The default value is 10 seconds. If the value is set to 0, OSPFv3 LSAs are not suppressed.
threshold *count*	Specifies an OSPFv3 LSA suppression threshold.	The value is an integer ranging from 3 to 100. The default value is 30.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

On a stable network where routes need to be fast converged, the parameter **intelligent-timer** needs to be specified to set the interval for updating LSAs (in milliseconds) so that topology changes or route changes can be immediately advertised to the network by using LSAs. In this manner, route convergence can speed up. This prevents too many network bandwidths and device resources from being consumed due to network connections or frequent route flapping.

Example

Set the maximum interval for updating OSPFv3 LSAs to 10000 ms, the initial interval to 700 ms, and the hold interval to 4000 ms.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] lsa-originate-interval intelligent-timer 10000 700 4000
```

9.5.45 maximum load-balancing (OSPFv3)

Function

The **maximum load-balancing** command sets the maximum number of equal-cost routes for carrying out load balancing.

The **undo maximum load-balancing** command restores the default setting.

By default, the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204 support a maximum of four equal-cost routes, and the AR2220, AR2220E, AR2204XE,

AR2204XE-DC, AR2240 (using SRU40, SRU60, SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series support a maximum of eight equal-cost routes, AR2240 (using SRU200, SRU200E or SRU400), and AR3200 (using SRU200, SRU200E or SRU400) series support a maximum of sixteen equal-cost routes.

Format

maximum load-balancing *number*

undo maximum load-balancing

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

If a routing protocol discovers multiple routes with the same cost to a single destination, they can carry out load balancing. The **maximum load-balancing** command sets the maximum number of equal-cost routes that can carry out load balancing. This optimizes the routing policy and ensures traffic forwarding on a complex network.

Effect

Packets will be load-balanced by multiple equal-cost routes to a single destination.

Follow-up Procedure

If more existing equal-cost OSPFv3 routes than the value set using the **maximum load-balancing** command are available, the system randomly selects equal-cost routes equal to the value set using this command to carry out load balancing. The **nexthop** command allows routes with a specified weight to carry out load balancing.

Precautions

To disable load balancing, set the value of *number* to 1.

Example

Set the maximum number of equal-cost routes that OSPFv3 can support to 3.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] maximum load-balancing 3
```

Restore the default maximum number of equal-cost routes for carrying out load balancing.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] undo maximum load-balancing
```

Related Topics

9.5.47 nexthop (OSPFv3)

9.5.46 maxage-lsa route-calculate-delay (OSPFv3)

Function

The **maxage-lsa route-calculate-delay** command configures a route calculation delay that is triggered when the device receives a MaxAge Router LSA.

The **undo maxage-lsa route-calculate-delay** command restores the default configuration.

By default, the delay is 20s.

Format

maxage-lsa route-calculate-delay *delay-interval*

undo maxage-lsa route-calculate-delay

Parameters

Parameter	Description	Value
delay-interval	Specifies a route calculation delay that is triggered when the device receives a MaxAge Router LSA.	The value is an integer ranging from 0 to 65535, in seconds. If the value is set to 0, route calculation is not delayed when the device receives a MaxAge Router LSA.

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Frequent OSPFv3 LSA flapping may lead to route flapping, adversely affecting services. To address this problem, run the **maxage-lsa route-calculate-delay** command to configure the device to delay route calculation when it receives a MaxAge Router LSA, which suppresses the frequent OSPFv3 LSA flapping that may occur.

Example

Configure the device to delay route calculation for 200s when the device receives a MaxAge Router LSA.

```
<Huawei> system-view
[Huawei] ospfv3 100
[Huawei-ospfv3-100] maxage-lsa route-calculate-delay 200
```

9.5.47 nexthop (OSPFv3)

Function

The **nexthop** command sets the preference for equal-cost routes.

The **undo nexthop** command cancels the preference of equal-cost routes.

By default, the preference is not set for equal-cost routes. That is, equal-cost routes forward packets at the same time for load balancing.

Format

nexthop *router-id interface-type interface-number* **weight** *value*

undo nexthop *router-id interface-type interface-number*

Parameters

Parameter	Description	Value
router-id	Specifies the router ID of a neighbor.	It is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of an interface.	-
weight *value*	Specifies the weight of the next hop. The smaller the weight is, the higher the route preference is.	It is an integer ranging from 1 to 254.

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

After OSPFv3 calculates equal-cost routes, you can run the **nexthop** command to select the route with the highest preference from the equal-cost routes as the next hop. OSPFv3 selects a next hop from these equal-cost routes according to the weight. The smaller the weight is, the higher the route preference is.

Example

Set the preference for equal-cost routes in OSPFv3.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] nexthop 10.2.2.2 gigabitethernet 1/0/0 weight 240
```

9.5.48 nssa (OSPFv3 Area)

Function

The **nssa** command configures an OSPFv3 area as an NSSA.

The **undo nssa** command cancels the configuration.

Format

nssa [**default-route-advertise** [**cost** *cost* | **type** *type* | **tag** *tag*] * | **no-import-route** | **no-summary** | **translator-always** | **translator-interval** *translator-interval* | **set-n-bit** | **suppress-forwarding-address**] *

undo nssa

Parameters

Parameter	Description	Value
default-route-advertise	Generates default Type7 LSAs on the ASBR and then advertises them to the NSSA. **NOTE** The ABR generates a default NSSA LSA (Type7 LSA) automatically and advertises it in the NSSA.	-
cost *cost*	Specifies the default cost of Type 7 LSAs.	It is an integer ranging from 1 to 16777214. The default value is 1.

Parameter	Description	Value
type *type*	Specifies the type of the external routes.	The value is an integer ranging from 1 to 2. By default, it is 2. • 1: Type 1 external route • 2: Type 2 external route
tag *tag*	Specifies the tag value of the OSPFv3 route imported to an NSSA.	It is an integer ranging from 0 to 4294967295. The default value is 0.
no-import-route	Indicates that no external routes are imported to NSSAs.	-
no-summary	Disables ABRs from sending summary LSAs to NSSAs.	-
translator-always	Specifies the ABR in an NSSA as the translator. Multiple ABRs in an NSSA can be configured as translators.	-
translator-interval *translator-interval*	Specifies the timeout period of a translator.	It is an integer ranging from 1 to 120, in seconds. The default value is 40 seconds.
set-n-bit	Indicates that the N-bit is set in DD packets.	-
suppress-forwarding-address	Enables the device to suppress the forwarding address of a Type 5 LSA translated from a Type 7 LSA.	-

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

If an area is configured to the nssa area, all routers of the area must be configured with the NSSA attribute.

The area may be updated after NSSA attributes are configured or deleted. Thus, the NSSA attributes can be re-configured or deleted only after the last update of NSSA attributes is complete.

The keyword **default-route-advertise** is used to generate default Type 7 LSAs. Regardless of whether there is route ::/0 in the routing table on an ABR, a Type 7

LSA default route is generated. A Type 7 LSA default route can be generated only when there is route ::/0 in the routing table on an ASBR.

When an ASBR is also an ABR, you can specify **no-import-route** to disable OSPFv3 from advertising the external routes imported through the **import-route** command to NSSAs. To reduce the number of LSAs to be transmitted to NSSAs, you can specify **no-summary** on an ABR to disable the ABR from transmitting summary LSAs (Type 3 LSAs) to NSSAs.

NOTE

- When the LS age field (aging time) in the LSA header reaches 3600 seconds, this LSA is deleted.
- After the keyword **set-n-bit** is set, a router re-establishes neighbor relationships with routers directly connected to it in the NSSA.

Example

Configure Area 1 as an NSSA, and set the timeout period of the translator to 20s.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] area 1
[Huawei-ospfv3-1-area-0.0.0.1] nssa translator-interval 20
```

Related Topics

9.5.9 default-route-advertise (OSPFv3)

9.5.40 import-route (OSPFv3)

9.5.49 ospfv3

Function

The **ospfv3** command enables an OSPFv3 process and bind it to a default or specified VPN instance.

The **undo ospfv3** command disables the OSPFv3 process.

By default, the system does not support OSPFv3.

Format

ospfv3 [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo ospfv3 *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535. By default, it is 1.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Only when you configure the Route ID in the OSPFv3 view, the OSPFv3 process can run normally. Otherwise, the OSPFv3 process can be viewed but cannot generate LSAs.

If a VPN instance is specified, the OSPFv3 process belongs to the VPN instance. If no VPN instance is specified, the OSPFv3 process is a global instance.

NOTE

Before configuring OSPFv3-related parameters, you must enable OSPFv3.

Example

Enable the OSPFv3 protocol.

```
<Huawei> system-view
[Huawei] ospfv3
```

9.5.50 ospfv3 area

Function

The **ospfv3 area** command enables the OSPFv3 process on an interface and specifies the area the process belongs to.

The **undo ospfv3 area** command disables the OSPFv3 process on the interface.

By default, the OSPFv3 protocol is not enabled on the interface.

Format

ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value is an integer ranging from 1 to 65535.
area *area-id*	Specifies the OSPFv3 area ID.	The value of the area ID can be a decimal integer or in the IPv4 address format. The integer ranges from 0 to 4294967295.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ipv6 enable** command to enable IPv6 in the interface view.

Example

Enable OSPFv3 in GigabitEthernet1/0/0, and enable OSPFv3 in area 1.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ospfv3
[Huawei-ospfv3-1] router-id 10.1.1.1
[Huawei-ospfv3-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ospfv3 1 area 1
```

Related Topics

8.8.28 ipv6 enable (interface view)

9.5.51 ospfv3 authentication-mode

Function

The **ospfv3 authentication-mode** command configures an authentication mode and a password for an OSPFv3 interface.

The **undo ospfv3 authentication-mode** command deletes the authentication mode and password configured for an OSPFv3 interface.

By default, no authentication mode or password are configured for any OSPFv3 interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

ospfv3 authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* } [**instance** *instance-id*]

ospfv3 authentication-mode keychain *keychain-name* [**instance** *instance-id*]

undo ospfv3 authentication-mode hmac-sha256 key-id *key-id* [**plain** *plain-text* | **cipher** *cipher-text*] [**instance** *instance-id*]

undo ospfv3 authentication-mode keychain [*keychain-name*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
hmac-sha256	Configures the HMAC-SHA256 authentication mode.	N/A
key-id *key-id*	Specifies the key ID for authentication, which must be the same as the one configured at the other end.	The value is an integer ranging from 1 to 255.
plain	Configures the plaintext password type. Only a plaintext password can be entered, and the password is displayed in plaintext in the configuration file. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	N/A
plain-text	Specifies a plaintext password.	The value is a string of 1 to 255 characters, spaces not supported.
cipher	Configures the ciphertext password type. You can enter either a plaintext or ciphertext password, but the password is displayed in ciphertext in the configuration file.	N/A
cipher-text	Specifies a ciphertext password.	The value can be a string of 1 to 255 characters for plaintext passwords and 20 to 392 characters for ciphertext passwords, spaces not supported.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
keychain	Configures keychain authentication. **NOTE** Before you configure keychain authentication, run the **keychain** command to configure a keychain, the **key-id** command to configure a key ID, the **key-string** command to configure a password, and the **algorithm** command to configure an algorithm. If these commands are not run, OSPFv3 authentication fails. OSPFv3 supports only hmac-sha256 in the **algorithm** command.	N/A
keychain-name	Specifies a keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
instance *instance-id*	Specifies the ID of a VLAN to which the specified interface belongs.	The value ranges from 0 to 255, with default value 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to inherent defects and flawed implementation of the TCP/IP protocol suite, there are an increasing number of attacks, which poses greater threats on TCP/IP networks than ever before. The attacks on network devices may lead to network failures. To configure an authentication mode and a password for an OSPFv3 interface to improve OSPFv3 network security, run the **ospfv3 authentication-mode** command.

Precautions

OSPFv3 interface authentication takes precedence over OSPFv3 area authentication.

To configure OSPFv3 area authentication, run the **authentication-mode** command.

Example

Configure OSPFv3 HMAC-SHA256 authentication on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ospfv3
[Huawei-ospfv3-1] router-id 10.1.1.1
[Huawei-ospfv3-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ospfv3 1 area 0
[Huawei-GigabitEthernet1/0/0] ospfv3 authentication-mode hmac-sha256 key-id 10 cipher huawei
```

Related Topics

9.5.51 ospfv3 authentication-mode

9.5.52 ospfv3 bfd

Function

The **ospfv3 bfd** command enables the bidirectional forwarding detection (BFD) on the specified interface enabled with OSPFv3, or sets the parameter values of a BFD session.

The **undo ospfv3 bfd** command deletes the BFD on the specified interface, or restores the default parameter values of a BFD session.

By default, BFD is not enabled at OSPFv3 interface level.

Format

ospfv3 bfd enable [**instance** *instance-id*]

ospfv3 bfd { **min-transmit-interval** *min-transmit-value* | **min-receive-interval** *min-receive-value* | **detect-multiplier** *detect-multiplier-value* }* [**instance** *instance-id*]

undo ospfv3 bfd enable [**instance** *instance-id*]

undo ospfv3 bfd { **min-transmit-interval** [*min-transmit-value*] | **min-receive-interval** [*min-receive-value*] | **detect-multiplier** [*detect-multiplier-value*] }* [**instance** *instance-id*]

Parameters

Parameter	Description	Value
enable	Indicates enable BFD for OSPFv3 in the specified interface.	-
min-transmit-interval *min-transmit-value*	Indicates minimum transmit interval for BFD support in OSPFv3 on a given interface.	The value is an integer that ranges from 10 to 2000 milliseconds. By default, the value is 10 milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
min-receive-interval *min-receive-value*	Indicates minimum receive interval for BFD support in OSPFv3 on a given interface.	The value is an integer that ranges from 10 to 2000 milliseconds. By default, the value is 10 milliseconds.
detect-multiplier *detect-multiplier-value*	Indicates detect multiplier value for BFD support in OSPFv3 on a given interface.	The value is an integer that ranges from 3 to 50.
instance *instance-id*	Indicates the interface instance id.	The value is an integer ranges from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A link fault or a topology change causes devices to recalculate routes. Therefore, the convergence of routing protocols must be as fast as possible to improve network performance.

Link faults are inevitable. Therefore, quickly detecting faults and notifying routing protocols of the faults is a feasible solution to immediately rectify link faults. If BFD is associated with routing protocols, BFD can speed up the convergence of routing protocols when a link fault occurs.

OSPFv3 IP FRR requires the low layer to fast respond to the link change. Traffic, therefore, can be rapidly switched to the backup link when a link fails. After the **frr-binding** parameter is configured, the BFD status is bound to the link status of an interface. Specifically, when the BFD status goes Down, the link status of the interface also goes Down. This ensures that faults are detected quickly.

After OSPFv3 establishes a BFD session, the default parameter value is used. BFD session parameters can also be modified as required.

- Actual interval at which BFD packets are transmitted on the local devices = Max { configured interval *min-transmit-value* at which BFD packets are transmitted, configured interval *min-receive-value* at which BFD packets are received on the peer device }
- Actual interval at which BFD packets are received on the local devices = Max { configured interval *min-transmit-value* at which BFD packets are transmitted on the peer device, configured interval *min-receive-value* at which BFD packets are received on the local device }

 Copyright © Huawei Technologies Co., Ltd.

- Actual time for detecting BFD packets = Actual interval at which BFD packets are received on the local device x Configured detection multiplier *detect-multiplier-value*

For example:

- On the local device, the configured interval at which BFD packets are transmitted is 200 ms; the interval at which BFD packets are received is set to 300 ms; the detection multiplier is 4.
- On the peer device, the configured interval at which BFD packets are transmitted is 100 ms; the interval at which BFD packets are received is 600 ms; the detection multiplier is 5.

Then:

- On the local device, the actual interval at which BFD packets are transmitted is 600 ms calculated by using the formula max {200 ms, 600 ms}; the interval at which BFD packets are received is 300 ms calculated by using the formula max {100 ms, 300 ms}; the detection period is 1500 ms calculated by multiplying 300 ms by 5.
- On the peer device, the actual interval at which BFD packets are transmitted is 300 ms calculated by using the formula max {100 ms, 300 ms}, the actual interval at which BFD packets are received is 600 ms calculated by using the formula max {200 ms, 600 ms}, and the detection period is 2400 ms calculated by multiplying 600 ms by 4.

Prerequisites

The set BFD session parameters take effect only when BFD is enabled on the interface.

Configuration Impact

If the global BFD is not configured, BFD on the interface can be configured but the BFD session cannot be set up. Similarly, if the parameters of a BFD session are set but the **ospfv3 bfd enable** command is not configured, the BFD session cannot be set up.

The priority of BFD configured on an interface is higher than what is configured in the process. If the BFD is enabled on the interface, the BFD session is set up by using the parameters of the BFD configured on the interface.

Precautions

- After BFD is configured, OSPFv3 establishes BFD sessions only with neighbors.
- The **ospfv3 bfd enable** command and the **ospfv3 bfd block** command are mutually exclusive.
- After BFD is disabled on the interface using the **undo ospfv3 bfd enable** command, the configurations of the parameters of the BFD session on the interface still exist.

Example

Enabling BFD on OSPFv3 on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
```

```
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ospfv3 1 area 1 instance 1
[Huawei-GigabitEthernet1/0/0] ospfv3 bfd enable instance 1
```

Configure BFD parameters on OSPFv3 on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 bfd min-transmit-interval 100 min-receive-interval 100 detect-multiplier 3 instance 1
```

Related Topics

9.5.53 ospfv3 bfd block

9.5.53 ospfv3 bfd block

Function

The **ospfv3 bfd block** command blocks the bidirectional forwarding detection (BFD) dynamically created by an interface.

The **undo ospfv3 bfd block** command cancels the feature.

By default, BFD is not blocked.

Format

ospfv3 bfd block [**instance** *instance-id*]

undo ospfv3 bfd block [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Indicates the interface instance id.	The value is an integer ranges from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the **bfd all-interfaces enable** command is run in the OSPFv3 process, all neighbors that enable OSPFv3 and the neighbor relationship is in Full state create BFD sessions. To prevent specific interfaces from being enabled with BFD, you can disable their interfaces from dynamically creating BFD sessions.

Prerequisites

- BFD has been enabled on these interfaces.
- The **ipv6 enable** command has been enabled in the interface view.

Precautions

The **ospfv3 bfd enable** command and the **ospfv3 bfd block** command are mutually exclusive.

Example

Block the BFD dynamically created by GigabitEthernet1/0/0 when configured the BFD for OSPF3 of all interfaces in the OSPF3 process.

```
<Huawei> system-view
[Huawei] interface GigabitEthernet1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 bfd block instance 1
```

Related Topics

9.5.52 ospfv3 bfd

9.5.54 ospfv3 cost

Function

The **ospfv3 cost** command sets the cost of the interface in different instances.

The **undo ospfv3 cost** command restores the default cost of the interface in different instances.

By default, the cost of an interface running OSPF is calculated using the following formula: **Interface cost = Bandwidth reference value/Interface bandwidth** where, the bandwidth reference value can be changed using the **bandwidth-reference** command.

Format

ospfv3 cost *cost* [**instance** *instance-id*]

undo ospfv3 cost [*cost*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
cost	Specifies the cost for running OSPFv3.	The value is an integer ranging from 1 to 65535.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the cost for public instance to run OSPFv3 on GigabitEthernet1/0/0 to 33.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 1 area 1
[Huawei-GigabitEthernet1/0/0] ospfv3 cost 33
```

9.5.55 ospfv3 dr-priority

Function

The **ospfv3 dr-priority** command sets the priority of an interface that takes part in the DR or BDR election.

The **undo ospfv3 dr-priority** command restores the default value.

By default, the priority of an interface that takes part in the DR or BDR election is 1.

Format

ospfv3 dr-priority *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [*priority*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
priority	Specifies the priority of the interface that candidates for DR or BDR.	The value is an integer ranging from 0 to 255. The default value is 1.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The priority of the interface determines the qualification of the interface when electing DR or BDR. The interface with the higher priority is preferred. The router whose priority is 0 cannot be elected as a DR or a BDR.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the priority of public instance for electing DR or BDR to 8 on GigabitEthernet1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 1 area 1
[Huawei-GigabitEthernet1/0/0] ospfv3 dr-priority 8
```

9.5.56 ospfv3 ipsec sa

Function

The **ospfv3 ipsec sa** command configures an SA on an interface.

The **undo ospfv3 ipsec sa** command deletes the SA configured on an interface.

By default, no SA is configured on an interface.

Format

ospfv3 ipsec sa *sa-name*

undo ospfv3 ipsec sa

Parameters

Parameter	Description	Value
sa-name	Specifies the name of an SA.	It is a string of 1 to 15 case-insensitive characters, spaces not supported. The characters can be letters or numbers, hyphens (-) not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an SA is configured on an interface, OSPFv3 uses the SA to authenticate packets sent and received by the interface.

If no SA is configured on the interface, OSPFv3 uses the SA configured in the process or the area where the interface resides to authenticate packets sent and received by the interface.

NOTE

- The SA configured in the interface view takes precedence over that configured in the OSPFv3 area view or OSPFv3 process view.
- The **ospfv3 ipsec sa** command can be used on all the OSPFv3 instances of an interface.

Prerequisites

- Before configuring the **ospfv3 ipsec sa** command, ensure that an **IPSec proposal** and IPSec SA have been configured on the device.
- Before configuring this command, ensure that **OSPFv3 has been enabled on an interface** of the device.

Example

Configure an existing SA named **sa3** on the interface GigabitEthernet1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 ipsec sa sa3
```

9.5.57 ospfv3 mib-binding

Function

The **ospfv3 mib-binding** command binds an OSPFv3 process to SNMP and makes OSPFv3 respond to SNMP requests.

The **undo ospfv3 mib-binding** command disables the binding.

By default, there is no binding between the OSPFv3 process and SNMP.

Format

ospfv3 mib-binding *process-id*

undo ospfv3 mib-binding

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process ID.	The value ranges from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When multiple OSPFv3 processes are enabled, you can bind OSPFv3 MIB to a process so that this process can be processed.

Before running this command, run the **ospfv3** command in the system view to create an OSPFv3 process.

NOTE

Only after the **ospfv3 mib-binding** *process-id* command is run on a device, can the trap associated with the specified *process-id* be triggered on the device.

Example

Bind OSPFv3 process to SNMP.

```
<Huawei> system-view
[Huawei] ospfv3
[Huawei-ospfv3-1] quit
[Huawei] ospfv3 mib-binding 100
```

Disable the binding.

```
<Huawei> system-view
[Huawei] undo ospfv3 mib-binding
```

9.5.58 ospfv3 mtu-ignore

Function

The **ospfv3 mtu-ignore** command disables the MTU check on DD packets.

The **undo ospfv3 mtu-ignore** command restores the default value.

By default, the MTU check on DD packets is enabled.

Format

ospfv3 mtu-ignore [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Disable OSPFv3 from checking the MTU of the DD packets.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ospfv3
[Huawei-ospfv3-1] router-id 10.1.1.1
[Huawei-ospfv3-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ospfv3 1 area 1
[Huawei-GigabitEthernet1/0/0] ospfv3 mtu-ignore
```

9.5.59 ospfv3 network-type

Function

The **ospfv3 network-type** command sets the network type of the OSPFv3 interface.

The **undo ospfv3 network-type** command restores the default network type of the OSPFv3 interface.

By default, the network type of an interface is determined by the physical interface. The network type of Ethernet interface is **broadcast**, that of the serial interface (encapsulated with PPP or HDLC) is **p2p**, and that of ATM interface and Frame-relay interface is **nbma**.

Format

ospfv3 network-type { **broadcast** | **nbma** | **p2mp** [**non-broadcast**] | **p2p** } [**instance** *instance-id*]

undo ospfv3 network-type [**broadcast** | **nbma** | **p2mp** [**non-broadcast**] | **p2p**] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
broadcast	Indicates that the network type of the interface is changed to broadcast.	-
nbma	Indicates that the network type of the interface is changed to NBMA.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
p2mp	Indicates that the network type of the interface is changed to point-to-multipoint.	-
non-broadcast	Indicates that the network type of the interface is changed to non-broadcast point-to-multipoint.	-
p2p	Indicates that the network type of the interface is changed to point-to-point.	-
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before configuring this command, you need to run the **ospfv3 area** command in the interface view to enable the OSPFv3 process.

Example

Set network type of GigabitEthernet1/0/0 to NBMA.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 network-type nbma
```

9.5.60 ospfv3 peer router-id

Function

The **ospfv3 peer router-id** command sets the DR priority and IPv6 addresses for adjacent routers on an NBMA network.

The **undo ospfv3 peer router-id** command removes the setting.

By default, the IPv6 addresses for the adjacent routers on an NBMA network is not set.

Format

ospfv3 peer router-id *router-id ipv6-address* [**dr-eligible** | **cost** *cost* | **poll** *interval* | **instance** *instance-id*] *

undo ospfv3 peer router-id *router-id* [*ipv6-address*] [**dr-eligible** | **cost** [*cost*] | **poll** [*interval*] | **instance** *instance-id*] *

Parameters

Parameter	Description	Value
router-id	Specifies the Router ID of the adjacent node.	The value is in dotted decimal notation.
ipv6-address	Specifies the Link-local address of the adjacent node.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
dr-eligible	Specifies the neighbor can take part in the DR election.	-
cost *cost*	Specifies the cost of the interface on the neighbor router of the NBMA network.	The value is an integer ranging from 1 to 65535.
poll *interval*	Specifies the interval for sending the polling Hello packet on the neighbor router of the NBMA network.	The value is an integer ranging from 1 to 65535.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

On GigabitEthernet1/0/0, specify the peer end to take part in DR selection.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 peer router-id 1.1.1.1 FE80::1 dr-eligible
```

Related Topics

9.5.25 display ospfv3 peer

9.5.61 ospfv3 router-id auto-recover disable

Function

The **ospfv3 router-id auto-recover disable** command disables router ID automatic recovery after a router detects a router ID conflict.

The **undo ospfv3 router-id auto-recover disable** command enables router ID automatic recovery after a router detects a router ID conflict.

By default, router ID automatic recovery takes effect after a router detects a router ID conflict.

Format

ospfv3 router-id auto-recover disable

undo ospfv3 router-id auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a router ID conflict occurs in an OSPFv3 area, the system selects a new router ID, which prevents route flapping and reduces route calculation operations. Other protocols will not go Down when the CPU usage is controlled.

NOTE

- If the automatic recovery function is enabled and a router ID conflict occurs between indirectly connected routers in one OSPFv3 area, the system replaces the conflicted router ID with a newly calculated one. The automatic recovery function takes effect on both configured and automatically generated router IDs.
- The system can replace a router ID in a maximum of three attempts in case the router ID conflict persists.

Example

Disable router ID automatic recovery after a router detects a router ID conflict.

```
<Huawei> system-view
[Huawei] ospfv3 router-id auto-recover disable
```

9.5.62 ospfv3 suppress-flapping peer

Function

The **ospfv3 suppress-flapping peer** command configures detection parameters for OSPFv3 neighbor relationship flapping suppression.

The **undo ospfv3 suppress-flapping peer** command restores the default detection parameters.

By default, the detection interval of OSPFv3 neighbor relationship flapping suppression is 60s, the suppression threshold is 10, and the interval for exiting from suppression is 120s.

Format

ospfv3 suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } * [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } * [**instance** *instance-id*]

Parameters

Parameter	Description	Value
detecting-interval *detecting-interval*	Specifies the detection interval of OSPFv3 neighbor relationship flapping suppression. Each OSPFv3 interface on which OSPFv3 neighbor relationship flapping suppression is enabled starts a flapping counter. If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping_count increases by 1.	The value is an integer ranging from 1 to 300, in seconds. The default value is 60s.
threshold *threshold*	Specifies the threshold of OSPFv3 neighbor relationship flapping suppression. When the flapping_count reaches or exceeds *threshold*, flapping suppression takes effect.	The value is an integer ranging from 1 to 1000. The default value is 10.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
resume-interval *resume-interval*	Specifies the interval for exiting from OSPFv3 neighbor relationship flapping suppression. If the interval between two successive neighbor status changes from Full to a non-Full state is longer than *resume-interval*, the flapping_count is reset. **NOTE** The value of *resume-interval* must be greater than that of *detecting-interval*.	The value is an integer ranging from 2 to 1000, in seconds. The default value is 120s.
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure detection parameters for OSPFv3 neighbor relationship flapping suppression on an interface, run the **ospfv3 suppress-flapping peer** command. However, keeping the default configurations is recommended.

Prerequisites

OSPFv3 neighbor relationship flapping suppression must have been enabled globally before you configure detection parameters for it. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the detection parameters.

Example

Set the detection interval of OSPFv3 neighbor relationship flapping suppression to 5s, the suppression threshold to 40, and the interval for exiting from suppression to 20s on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 suppress-flapping peer detecting-interval 5 threshold 40 resume-interval 20
```

Related Topics

9.5.84 suppress-flapping peer disable (OSPFv3)

9.5.63 ospfv3 suppress-flapping peer disable

Function

The **ospfv3 suppress-flapping peer disable** command disables OSPFv3 neighbor relationship flapping suppression from an interface.

The **undo ospfv3 suppress-flapping peer disable** command enables OSPFv3 neighbor relationship flapping suppression on an interface.

By default, OSPFv3 neighbor relationship flapping suppression is enabled on all interfaces.

Format

ospfv3 suppress-flapping peer disable [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer disable [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, OSPFv3 neighbor relationship flapping suppression is enabled on all interfaces in the same OSPFv3 process. To disable the function from one of the interfaces, run the **ospfv3 suppress-flapping peer disable** command.

NOTE

When an interface enters the flapping suppression state, all neighbor relationships on the interface enter the state accordingly.

Prerequisites

OSPFv3 neighbor relationship flapping suppression must have been enabled globally before you enable the function on an interface using the **undo ospfv3 suppress-flapping peer disable** command. By default, the function is enabled globally. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it first.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable OSPFv3 neighbor relationship flapping suppression from GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 suppress-flapping peer disable
```

Related Topics

9.5.84 suppress-flapping peer disable (OSPFv3)

9.5.64 ospfv3 suppress-flapping peer hold-down

Function

The **ospfv3 suppress-flapping peer hold-down** command configures the Hold-down mode and sets duration for this mode.

The **undo ospfv3 suppress-flapping peer hold-down** command cancels the Hold-down mode.

By default, the Hold-down mode is disabled, and the Hold-max-cost mode is enabled.

Format

ospfv3 suppress-flapping peer hold-down *interval* [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer hold-down *interval* [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Specifies the duration of the Hold-down mode.	The value is an integer ranging from 1 to 600, in seconds.
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **ospfv3 suppress-flapping peer hold-down** *interval* command.

Prerequisites

OSPFv3 neighbor relationship flapping suppression must have been enabled globally before you configure the Hold-down mode and set duration for this mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the Hold-down mode and set duration for this mode.

Example

Configure the Hold-down mode and set its duration to 200s on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 suppress-flapping peer hold-down 200
```

Related Topics

9.5.84 suppress-flapping peer disable (OSPFv3)

9.5.65 ospfv3 suppress-flapping peer hold-max-cost disable

9.5.65 ospfv3 suppress-flapping peer hold-max-cost disable

Function

The **ospfv3 suppress-flapping peer hold-max-cost disable** command disables the Hold-max-cost mode.

The **undo ospfv3 suppress-flapping peer hold-max-cost disable** command enables the Hold-max-cost mode.

By default, the Hold-max-cost mode is enabled.

Format

ospfv3 suppress-flapping peer hold-max-cost disable [**instance** *instance-id*]

undo ospfv3 suppress-flapping peer hold-max-cost disable [**instance** *instance-id*]

Parameters

Parameter	Description	Value
instance *instance-id*	Specifies the ID of the instance to which an interface belongs.	The value is an integer ranging from 0 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use 65535 as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **ospfv3 suppress-flapping peer hold-down** *interval* command.

NOTE

The Hold-max-cost mode can prevent a device from being isolated from the network. If a device on a key path is isolated from the network due to OSPFv3 neighbor relationship flapping, the network is separated into two isolated parts. To prevent this problem, use the Hold-max-cost mode on the key path.

Precautions

The Hold-max-cost mode takes effect only unidirectionally. If a remote device does not support OSPFv3 neighbor relationship flapping suppression, bidirectional traffic between the local and remote devices may travel along different paths.

Example

Disable the Hold-max-cost mode on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 suppress-flapping peer hold-max-cost disable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.5.84 suppress-flapping peer disable (OSPFv3)
9.5.64 ospfv3 suppress-flapping peer hold-down

9.5.66 ospfv3 timer dead

Function

The **ospfv3 timer dead** command sets the dead interval of the OSPFv3 neighbor of the instance on the interface.

The **undo ospfv3 timer dead** command restores the default value.

By default, the dead interval of OSPFv3 neighbor is 40 seconds for the interface of P2P or Broadcast type. The dead interval of OSPFv3 neighbor is 120 seconds for the interface of P2MP or NBMA type.

Format

ospfv3 timer dead *interval* [**instance** *instance-id*]

undo ospfv3 timer dead [*interval*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Indicates the dead interval of OSPFv3.	The value is an integer ranging from 1 to 65535, in seconds.
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Dead interval of OSPFv3 neighbor refers to that the neighbor is invalid if the neighbor does not receive the Hello packets from its neighbor in the interval. The dead interval of routers in the same network segment must be consistent.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the dead interval of the neighbor to 80 seconds for GigabitEthernet1/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 timer dead 80
```

Related Topics

9.5.67 ospfv3 timer hello

9.5.67 ospfv3 timer hello

Function

The **ospfv3 timer hello** command specifies the interval for sending Hello packets on the interface instance.

The **undo ospfv3 timer hello** command restores the default interval.

By default, for the interface of the P2P and broadcast type, the interval for sending Hello packets is 10 seconds. For the interface of the P2MP and NBMA type, the interval for sending Hello packets is 30 seconds.

Format

ospfv3 timer hello *interval* [**conservative**] [**instance** *instance-id*]

undo ospfv3 timer hello [*interval* [**conservative**]] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Indicates the interval for an interface to send the Hello packets.	The value is an integer ranging from 1 to 65535, in seconds.
conservative	Indicates the conservative mode of the dead timer. If the conservative mode is configured, the value configured for the dead timer using the **ospfv3 timer dead** command takes effect even when the value is less than 10s.	-
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the interval for sending Hello packets on GigabitEthernet1/0/0 to 20 seconds.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 timer hello 20
```

Related Topics

9.5.66 ospfv3 timer dead

9.5.68 ospfv3 timer poll

Function

The **ospfv3 timer poll** command sets the polling interval for sending Hello packets on NBMA network.

The **undo ospfv3 timer poll** command restores the default polling interval.

By default, the polling interval for sending Hello packets on NBMA network is 120 seconds.

Format

ospfv3 timer poll *interval* [**instance** *instance-id*]

undo ospfv3 timer poll [*interval*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Specifies the polling interval of Hello packets.	The value is an integer ranging from 1 to 65535, in seconds.
instance *instance-id*	Specifies the instance ID of the interface.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

On the NBMA network, if a neighbor is invalid, you can configure routers to send Hello packet based on the polling interval that is set by the **ospfv3 timer poll** command. The polling interval should be at least 4 times that of the Hello interval.

OSPFv3 does not support the configuration on a null interface.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the polling interval for sending Hello packets on the GigabitEthernet1/0/0 to 130 seconds.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 timer poll 130
```

9.5.69 ospfv3 timer retransmit

Function

The **ospfv3 timer retransmit** command specifies the interval for retransmitting the LSA on the interface instance.

The **undo ospfv3 timer retransmit** command restores the default value.

By default, the interval for retransmitting LSAs is 5 seconds.

Format

ospfv3 timer retransmit *interval* [**instance** *instance-id*]

undo ospfv3 timer retransmit [*interval*] [**instance** *instance-id*]

Parameters

Parameter	Description	Value
interval	Indicates the interval for retransmitting LSAs.	The value is an integer ranging from 1 to 3600, in seconds.
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After sending an LSA to its neighbor, a router needs to wait for the Ack packet from the neighbor. If the router does not receive the Ack packet in the retransmission interval, the router retransmits the LSA.

The interval for retransmitting LSA between the neighboring routers should not be set too short. Otherwise, it leads to unnecessary retransmission.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the interval for retransmitting the LSA between GigabitEthernet1/0/0 and its neighboring router to 12 seconds.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] ospfv3
[Huawei-ospfv3-1] router-id 10.1.1.1
[Huawei-ospfv3-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ospfv3 1 area 1
[Huawei-GigabitEthernet1/0/0] ospfv3 timer retransmit 12
```

9.5.70 ospfv3 trans-delay

Function

The **ospfv3 trans-delay** command sets the delay for transmitting LSA on an interface instance.

The **undo ospfv3 trans-delay** command restores the default value.

By default, the delay for transmitting LSA is 1 second.

Format

ospfv3 trans-delay *interval* [**instance** *instance-id*]

undo ospfv3 trans-delay [*interval*] [**instance** *instance-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Indicates the delay for transmitting LSA on an interface.	The value is an integer ranging from 1 to 800, in seconds. By default, it is 1 second.
instance *instance-id*	Specifies the interface instance ID.	The value is an integer ranging from 0 to 255. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The LSA in the LSDB of the local router ages with time. The aging of the LSA increases by 1 per second, but the aging of the LSA does not change in the transmission process. Therefore, it is necessary to add the delay to the aging time of the LSA before the LSA is sent.

Before running this command on an interface, run the **ospfv3 area** command on the interface to enable OSPFv3.

Example

Set the delay for transmitting LSA on GigabitEthernet1/0/0 to 3 seconds.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospfv3 trans-delay 3
```

9.5.71 ospfv3 valid-ttl-hops

Function

The **ospfv3 valid-ttl-hops** command enables OSPFv3 GTSM and sets a TTL value.

The **undo ospfv3 valid-ttl-hops** command disables OSPFv3 GTSM.

By default, OSPFv3 GTSM is disabled.

Format

ospfv3 valid-ttl-hops *valid-ttl-hops-value* [**vpn-instance** *vpn-instance-name*]

undo ospfv3 valid-ttl-hops [*valid-ttl-hops-value*] [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
valid-ttl-hops-value	Specifies a TTL.	The value is an integer ranging from 1 to 255.
vpn-instance *vpn-instance-name*	Indicates the name of a VPN instance. If this parameter is specified, only the TTL values of the packets in the specified VPN instance are checked.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an OSPFv3 network requires high security, you can configure OSPFv3 GTSM and an authentication mode to improve network security. During network attacks, attackers may simulate OSPFv3 packets and continuously send them to a device. If the packets are destined for the device, it directly sends them to the control plane for processing without validating them. As a result, the increased processing workload on the control plane results in high CPU usage. GTSM protects devices against potential attacks and improves system security by checking whether the TTL value in each IP packet header is within a pre-defined range.

To enable OSPFv3 GTSM, run the **ospfv3 valid-ttl-hops**. To check the TTL values of packets that match a GTSM policy in a specified VPN instance, specify **vpn-instance** in the command.

The **ospfv3 valid-ttl-hops** command enables OSPFv3 GTSM on both the public network and VPNs. For example, if you run the **ospfv3 valid-ttl-hops 5 vpn-instance** *vpn1* command, OSPFv3 GTSM takes effect on both the public network and VPN 1, the TTL values of the OSPFv3 packets in the VPN 1 are checked, and the default action is performed on the packets that fail to match the GTSM policy.

Follow-up Procedure

GTSM checks the TTL values of only the packets that match a GTSM policy. For packets that do not match the GTSM policy, you can specify **pass** in the **gtsm default-action** command to allow these packets to pass the filtering or specify **drop** in the command to discard them.

Precautions

- If a VPN instance is specified in the **ospfv3 valid-ttl-hops** command and an interface is bound to the VPN instance, the interface discards all received

 Copyright © Huawei Technologies Co., Ltd.

unicast packets if the set TTL value is less than the actual hop count on the network.

- If a virtual link or sham link is deployed, configure a TTL value based on the actual hop count on the network (the number of routers through which the virtual link or sham link passes) to prevent the local router from discarding packets from neighbors over the virtual link or sham link.
- Therefore, if you want to apply the configured TTL value to packets only in a VPN or the public network, specify **pass** in the **gtsm default-action** command to prevent the OSPFv3 packets in other instances from being discarded incorrectly.

Example

Enable OSPFv3 GTSM and set the maximum number of TTL hops to 5 for the packets that can be received from the public network.

```
<Huawei> system-view
[Huawei] ospfv3 valid-ttl-hops 5
```

Related Topics

9.4.52 gtsm default-action

9.4.53 gtsm log drop-packet

9.5.72 preference (OSPFv3)

Function

The **preference** command sets the preference for an OSPFv3 route.

The **undo preference** command restores the default setting.

By default, the preference of the OSPFv3 route is 10. When ASE is specified, the default value is 150.

Format

preference [**ase**] { *preference* | **route-policy** *route-policy-name* } *

undo preference [**ase**]

Parameters

Parameter	Description	Value
ase	Sets the preference for an AS external route or an NSSA route.	-
preference	Specifies the preference for OSPFv3 routes.	It is an integer ranging from 1 to 255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a routing policy and sets the preference for specified routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

The smaller the preference value, the higher the preference.

Multiple dynamic routing protocols may be run on a router at the same time. Consequently, there is a problem of sharing and selecting routing information among routing protocols. Therefore, the system sets a default reference for each routing protocol. If different routing protocols find multiple routes to the same destination, the route discovered by the routing protocol with a higher preference is selected to forward IP packets.

Example

Set the preference for OSPFv3 routes.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] preference 5
```

9.5.73 reset ospfv3

Function

The **reset ospfv3** command restarts the OSPFv3 process.

The **reset ospfv3 counters** command resets OSPFv3 statistics.

Format

reset ospfv3 { *process-id* | **all** } [**graceful-restart** [**extend-period** *period*]]

reset ospfv3 { *process-id* | **all** } **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPFv3 process number.	The value is an integer that ranges from 1 to 65535.
all	Restarts all OSPFv3 processes.	-
graceful-restart	Restarts the OSPFv3 process in GR mode.	-
extend-period *period*	Prolongs the current GR period.	The value is an integer that ranges from 1 to 1800, expressed in seconds.
neighbor	Resets neighbor statistics.	-
interface-type interface-number	Specifies the type and number of the interface.	-
router-id	Specifies the router ID of a neighbor.	It is in dotted decimal notation.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You can choose general restart or graceful restart through the parameters.

By setting **extend-period**, you can prolong the current GR period. The prolonged GR period becomes invalid after the process restarts. This parameter takes effect for one time. That is, after the router performs GR next time, the value of the period returns to the one set by using **graceful-restart** [**extend-period** *period*].

NOTICE

If OSPFv3 connections are reset, OSPFv3 neighbor relationships will be interrupted and the original information cannot be restored. Exercise caution before running the **reset ospfv3** command.

Example

Reset OSPFv3 statistics.

```
<Huawei> reset ospfv3 1 counters
```

9.5.74 router-id (OSPFv3)

Function

The **router-id** command sets the Router ID for the router that runs OSPFv3.

The **undo router-id** command deletes the Router ID that is set for OSPFv3 router.

By default, there is no Router ID for the router that runs OSPFv3.

Format

router-id *router-id*

undo router-id

Parameters

Parameter	Description	Value
router-id	Indicates the Router ID.	It is in dotted decimal notation.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

The Router ID of an OSPFv3 process is unique in an AS. If no Router ID is set, the OSPFv3 process does not run.

When you set a Router ID, ensure that the Router IDs of any two processes are different in an AS.

NOTE

Multiple OSPFv3 processes can run on a router by setting the different process ID. In this case, you need to specify different Router IDs for different processes.

Example

Set the Router ID of the OSPFv3 process 1 to 10.1.1.3.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] router-id 10.1.1.3
```

Related Topics

9.5.49 ospfv3

 Copyright © Huawei Technologies Co., Ltd.

9.5.75 reset ospfv3 suppress-flapping peer

Function

The **reset ospfv3 suppress-flapping peer** command forces an interface to exit from OSPFv3 neighbor relationship flapping suppression.

Format

reset ospfv3 *process-id* **suppress-flapping peer** [*interface-type interface-number*] [**notify-peer**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies an interface type and number.	-
notify-peer	Instructs neighbors to exit from OSPFv3 neighbor relationship flapping suppression too.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After the fault that causes OSPFv3 neighbor relationship flapping is rectified, to enable an OSPFv3 interface to exit from flapping suppression in advance, you can run the **reset ospfv3 suppress-flapping peer** command.

Interfaces exit from flapping suppression in the following scenarios:

- The suppression timer expires.
- The corresponding OSPFv3 process is reset.
- An OSPFv3 neighbor is reset using the **reset ospfv3** command.
- The **reset ospfv3 suppress-flapping peer** command is run.
- OSPFv3 neighbor relationship flapping suppression is disabled globally using the **suppress-flapping peer disable (OSPFv3)** command in the OSPFv3 view.

If **notify-peer** is specified when the **reset ospfv3 suppress-flapping peer** command is run on a device, the device sends Hello packets in which **HelloInterval** and **RouterDeadInterval** are 0s to its neighbors to instruct the

 Copyright © Huawei Technologies Co., Ltd.

neighbors to exit from OSPFv3 neighbor relationship flapping suppression too. If the neighbors fail to receive such Hello packets, the function of **notify-peer** does not take effect. To force the neighbors to exit from OSPFv3 neighbor relationship flapping suppression, run the **reset ospfv3 suppress-flapping peer** command on them.

Example

Force interfaces to exit from OSPFv3 neighbor relationship flapping suppression.

```
<Huawei> reset ospfv3 1 suppress-flapping peer
```

Related Topics

9.5.84 suppress-flapping peer disable (OSPFv3)

9.5.76 sham-hello enable (OSPFv3)

Function

The **sham-hello enable** command enables OSPFv3 to regard the LSU packets and the LSAck packets the same as the Hello packets.

The **undo sham-hello** command disables the operation.

By default, the sham-hello feature is disabled.

Format

sham-hello enable

undo sham-hello

Parameters

none

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

The **sham-hello enable** command, OSPFv3 can regard the LSU packets and the LSAck packets the same as the Hello packets. After receiving this kind of packets, OSPFv3 refreshes the timeout timer of the neighbors to maintain the integrity of their relationship.

Example

Enable sham-hello.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] sham-hello enable
```

9.5.77 silent-interface (OSPFv3)

Function

The **silent-interface** command suppresses the specified interface from sending and receiving OSPFv3 packets.

The **undo silent-interface** command restores the default setting.

By default, the interface is permitted to send or receive OSPFv3 packets.

Format

silent-interface { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Indicates all interfaces.	-
interface-type interface-number	Indicates the interface type and interface number.	-

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Different processes can suppress the same interface from sending and receiving OSPFv3 packets, but the **silent-interface** command takes effect only on the OSPFv3 interface of the process.

Example

Suppress GigabitEthernet1/0/0 from sending and receiving OSPFv3 packets.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] silent-interface GigabitEthernet 1/0/0
```

9.5.78 snmp-agent trap enable feature-name ospfv3

Function

The **snmp-agent trap enable feature-name ospfv3** command enables the trap function for the OSPFv3 module.

The **undo snmp-agent trap enable feature-name ospfv3** command disables the trap function for the OSPFv3 module.

By default, all traps function of the OSPFv3 module are disabled.

Format

snmp-agent trap enable feature-name ospfv3 [**trap-name** { **ifconfigerror** | **ifrxbadpacket** | **ifstatechange** | **nbrrestarthelperstatuschange** | **nbrstatechange** | **nssatranslatorstatuschange** | **restartstatuschange** | **virtifconfigerror** | **virtifrxbadpacket** | **virtifstatechange** | **virtnbrrestarthelperstatuschange** | **virtnbrstatechange** | **authenticationsequencenumberwrap** | **lastauthenticationkeyexpiry** }]

undo snmp-agent trap enable feature-name ospfv3 [**trap-name** { **ifconfigerror** | **ifrxbadpacket** | **ifstatechange** | **nbrrestarthelperstatuschange** | **nbrstatechange** | **nssatranslatorstatuschange** | **restartstatuschange** | **virtifconfigerror** | **virtifrxbadpacket** | **virtifstatechange** | **virtnbrrestarthelperstatuschange** | **virtnbrstatechange** | **authenticationsequencenumberwrap** | **lastauthenticationkeyexpiry** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of OSPFv3 events of specified types.	-
ifconfigerror	Enables the traps of errors of the interface configuration.	-
ifrxbadpacket	Enables the traps of received bad packets.	-
ifstatechange	Enables the traps of changes of the interface state.	-
nbrrestarthelperstatuschange	Enables the traps of changes of the state of the helper during GR.	-
nbrstatechange	Enables the traps of changes of the neighbor state.	-
nssatranslatorstatuschange	Enables the traps of changes of the NSSA translator state.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
restartstatuschange	Enables the traps of changes of the state of the restarter during GR.	-
virtifconfigerror	Enables the traps of error of the virtual interface configuration.	-
virtifrxbadpacket	Enables the traps of the bad packet that is received on the virtual interface.	-
virtifstatechange	Enables the traps of changes of the virtual interface state.	-
virtnbrrestarthelperstatuschange	Enables the traps of changes of the GR helper state of neighboring nodes on the virtual link.	-
virtnbrstatechange	Enables the traps of changes of the state for the neighbor of the virtual-link.	-
authenticationsequencenumberwrap	Enables the trap for cryptographic sequence number wrapping.	-
lastauthenticationkeyexpiry	Enables the trap for last authentication key in keychain expiry.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the traps of one or more events, you can specify **trap-name**.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The non-excessive traps of OSPFv3 module includes:
  - VirtIfStateChange
  - NbrStateChange
  - VirtNbrStateChange
  - IfConfigError
  - VirtIfConfigError
  - IfRxBadPacket
  - VirtIfRxBadPacket
  - IfStateChange
  - RestartStatusChange
  - NbrRestartHelperStatusChange
  - NSSATransLlatorStatusChange
  - VirtNbrRestartHelperStatusChange
  - authenticationsequencenumberwrap
  - lastauthenticationkeyexpiry
- OSPFv3 module has no excessive trap.

Example

Enable the router to send the trap of errors of the OSPFv3 interface configuration.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name ospfv3 trap-name ifconfigerror
```

Related Topics

9.5.32 display snmp-agent trap feature-name ospfv3 all

9.5.79 spf timers

Function

The **spf timers** command sets the interval for calculating OSPFv3 routes by a common SPF timer.

The **undo spf timers** command restores the default setting.

By default, the interval for calculating OSPFv3 routes by a common SPF timer is not set.

Format

spf timers *delay-interval hold-interval*

undo spf timers

Parameters

Parameter	Description	Value
delay-interval	Specifies the delay for OSPFv3 from receiving network changes to performing SPF calculation.	The value is an integer ranging from 0 to 65535 seconds. By default, it is 5 seconds.
hold-interval	Specifies the hold interval between two consecutive SPF calculations.	The value is an integer ranging from 0 to 65535 seconds. By default, it is 10 seconds.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

According to the local LSDB, the router that runs OSPFv3 can calculate an SPT with itself as the root and determines the next hop to the destination network according to the SPT. Adjusting SPF calculation interval can avoid the exhaustion of bandwidth and router sources caused by frequent change of the network.

NOTE

A common SPF timer and an intelligent SPF timer are mutually exclusive.

Example

Set both the OSPFv3 route calculation interval and the hold interval to 6 seconds.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] spf timers 6 6
```

9.5.80 spf-schedule-interval (OSPFv3)

Function

The **spf-schedule-interval** command sets the interval for OSPFv3 to calculate routes by an intelligent SPF timer.

The **undo spf-schedule-interval** command restores the default setting.

By default, the intelligent timer is enabled. The interval for the SPF calculation is expressed in milliseconds. The maximum interval for the SPF calculation is 10000 ms, the initial interval is 500 ms, and the Holdtime interval is 2000 ms.

 Copyright © Huawei Technologies Co., Ltd.

Format

spf-schedule-interval { *delay-interval hold-interval* | **intelligent-timer** *max-interval start-interval hold-interval-1* }

undo spf-schedule-interval

Parameters

Parameter	Description	Value
delay-interval	Specifies the delay from the time when OSPFv3 receives a route change to the time when the SPF calculation is performed.	The value is an integer ranging from 0 to 65535, in seconds. The default value is 5.
hold-interval	Specifies the hold interval between two consecutive SPF calculations.	The value is an integer ranging from 0 to 65535, in seconds. The default value is 10.
intelligent-timer	Specifies the SPF calculation interval set through an intelligent timer.	-
max-interval	Specifies the maximum interval for performing the SPF calculation.	The value is an integer ranging from 1 to 20000, in milliseconds. The default value is 10000.
start-interval	Specifies the initial interval for performing the OSPFv3 SPF calculation.	The value is an integer ranging from 1 to 1000, in milliseconds. The default value is 500.
hold-interval-1	Specifies the hold interval for performing the OSPFv3 SPF calculation.	The value is an integer ranging from 1 to 5000, in milliseconds. The default value is 2000.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

Based on the local LSDB, a device that runs OSPFv3 uses the SPF algorithm to calculate the shortest path tree with itself as the root, and determines the next hop to the destination network based on the shortest path tree. Adjusting the interval at which the SPF calculation is performed can prevent too many bandwidth resources and device resources from being consumed due to frequent network changes.

NOTE

A common SPF timer and an intelligent SPF timer are mutually exclusive.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

After this command is configured, the interval for the SPF calculation is as follows:

1. The initial interval for the SPF calculation is specified by the parameter *start-interval*.
2. The interval for the SPF calculation for the nth (n≥2) time is equal to *hold-interval*×$2^{(n-2)}$.
3. When the interval specified by *hold-interval*×$2^{(n-2)}$ reaches the maximum interval specified by *max-interval*, OSPFv3 performs SPF calculation at the maximum interval until *max-interval* expires without flapping or the OSPF process is restarted.

Example

Set the interval at which OSPFv3 route calculation is performed to 5s and the hold interval at which OSPFv3 route calculation is performed to 6s.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] spf-schedule-interval 5 6
```

Set the maximum interval for performing the SPF calculation to 10000 ms, the initial interval to 700 ms, and the hold interval to 4000 ms.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] spf-schedule-interval intelligent-timer 10000 700 4000
```

9.5.81 stub (OSPFv3 Area)

Function

The **stub** command sets an OSPFv3 area to the stub area.

The **undo stub** command cancels the settings.

By default, no area is set to the stub area.

Format

stub [**no-summary**]

undo stub

Parameters

Parameter	Description	Value
no-summary	Indicates that the parameter is used only for the ABR of the stub area. After the parameter is configured, ABR advertises only one summary-LSA of the default route, and does not generate any other summary-LSA. This area is also called a totally stub area.	-

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

If an area is configured to the stub area, all routers of the area must be configured with the stub attribute.

The backbone area cannot be configured as a stub area.

Example

Set the OSPFv3 area 1 to the stub area.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] area 1
[Huawei-ospfv3-1-area-0.0.0.1] stub
```

Related Topics

9.5.8 default-cost (OSPFv3 Area)

9.5.82 stub-router (OSPFv3)

Function

The **stub-router** command configures a device as stub router.

The **undo stub-router** command restores the default configuration.

By default, no stub router exists.

Format

stub-router [**on-startup** [*interval*]]

undo stub-router

Parameters

Parameter	Description	Value
on-startup [*interval*]	Specifies the interval during which a device acts as a stub router when the device is restarted or faulty. ● If **on-startup** is not specified, the device is always a stub router, even if the cost of all routes advertised by the device is 65535. ● If **on-startup** is specified, the device works as a stub router only when it restarts or is faulty. The hold time of the stub router state is determined by *interval* parameter. If the *interval* parameter is not configured, the default interval (500 seconds) is used.	The value is an integer ranging from 5 to 65535, in seconds. By default, it is 500 seconds.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

After the **stub-router** command is configured on a router, the stub router informs other OSPFv3 devices not to use this stub router for data forwarding by increasing the metrics of the links in the Router-LSA generated by the router. Since the metric is not infinite, the devices to this stub router still exist. The metrics of all links in the device Router-LSAs generated by the stub router are set to 65535.

Example

Configure the device as a stub router.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] stub-router
```

9.5.83 reset ospfv3 statistics maxage-lsa

Function

The **reset ospfv3 statistics maxage-lsa** command deletes the statistics about router LSAs that have reached the maximum aging time.

Format

reset ospfv3 [*process-id*] **statistics maxage-lsa**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an OSPFv3 process.	The value is an integer ranging from 1 to 65535.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

After the statistics about router LSAs that have reached the maximum aging time are deleted, OSPFv3 services are not affected.

NOTICE

Statistics cannot be restored after being deleted. Therefore, exercise caution when running the command.

Example

Delete the statistics about router LSAs that have reached the maximum aging time.

```
<Huawei> reset ospfv3 statistics maxage-lsa
```

9.5.84 suppress-flapping peer disable (OSPFv3)

Function

The **suppress-flapping peer disable** command disables OSPFv3 neighbor relationship flapping suppression globally.

The **undo suppress-flapping peer disable** command enables OSPFv3 neighbor relationship flapping suppression globally.

By default, OSPFv3 neighbor relationship flapping suppression is enabled globally.

Format

suppress-flapping peer disable

undo suppress-flapping peer disable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

OSPFv3 view

Default Level

2: Configuration level

Usage Guidelines

If an interface carrying OSPFv3 services alternates between Up and Down, OSPFv3 neighbor relationship flapping occurs on the interface. During the flapping, OSPFv3 frequently sends Hello packets to reestablish the neighbor relationship, synchronizes LSDBs, and recalculates routes. In this process, a large number of packets are exchanged, adversely affecting neighbor relationship stability, OSPFv3 services, and other OSPFv3-dependent services, such as LDP and BGP. OSPFv3 neighbor relationship flapping suppression can address this problem by delaying OSPFv3 neighbor relationship reestablishment or preventing service traffic from passing through flapping links.

By default, OSPFv3 neighbor relationship flapping suppression is enabled globally. To disable this function globally, run the **suppress-flapping peer disable** command.

Example

Disable OSPFv3 neighbor relationship flapping suppression globally.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] suppress-flapping peer disable
```

Related Topics

9.5.63 ospfv3 suppress-flapping peer disable

9.5.85 vlink-peer (OSPFv3)

Function

The **vlink-peer** command creates and configures a virtual link.

The **undo vlink-peer** command deletes the existing virtual link.

By default, OSPFv3 virtual links are not configured.

Format

vlink-peer *router-id* [**hello** *hello-interval* | **retransmit** *retransmit-interval* | **trans-delay** *trans-delay-interval* | **dead** *dead-interval* | **ipsec sa** *sa-name* | **authentication-mode** { **hmac-sha256 key-id** *key-id* { **plain** *plain-text* | [**cipher**] *cipher-text* } | **keychain** *keychain-name* } | **instance** *instance-id*] *

undo vlink-peer *router-id* [**hello** [*hello-interval*] | **retransmit** [*retransmit-interval*] | **trans-delay** [*trans-delay-interval*] | **dead** [*dead-interval*] | **ipsec sa** [*sa-name*] | **authentication-mode** { **hmac-sha256 key-id** *key-id* | **keychain** }] *

Parameters

Parameter	Description	Value
router-id	Specifies the router ID of a virtual link neighbor, in the IPv4 address format.	The value is in dotted decimal notation.
hello *hello-interval*	Specifies the interval at which an interface sends Hello packets. This value must be equal to the *hello-interval* of the router that sets up a virtual link with the local router.	The value is an integer ranging from 1 to 65535, in seconds. By default, it is 10 seconds.
retransmit *retransmit-interval*	Specifies the interval at which an interface retransmits LSAs.	The value is an integer ranging from 1 to 3600, in seconds. By default, it is 5 seconds.
trans-delay *trans-delay-interval*	Specifies the delay in which an interface sends LSAs.	The value is an integer ranging from 1 to 800 seconds. By default, it is 1 second.
dead *dead-interval*	Specifies the dead interval. This value must be equal to the *dead-interval* of the router that sets up a virtual link with the local router and at least four times the value of *hello-interval*.	The value is an integer ranging from 1 to 65535, in seconds. By default, it is 40 seconds.
ipsec sa *sa-name*	Specifies the name of an SA configured for an OSPFv3 virtual link.	It is a string of 1 to 15 case-insensitive characters, spaces not supported. The characters can be letters or numbers, hyphens (-) not supported. When double quotation marks are used around the string, spaces are allowed in the string.
authentication-mode	Indicates the authentication mode over the virtual link.	-
hmac-sha256	Sets the HMAC-SHA256 authentication mode.	-
key-id *key-id*	Specifies the key ID for authentication, which must be the same as the one configured at the other end.	The value is an integer ranging from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
plain	Configures the simple password type. Only a simple password can be entered, and the password is displayed in simple text in the configuration file. **NOTICE** When configuring an authentication password, select the ciphertext mode because the password is saved in configuration files in simple text if you select simple text mode, which has a high risk. To ensure device security, change the password periodically.	-
plain-text	Specifies a simple password.	The value is a string of 1 to 255 characters.
cipher	Configures the ciphertext password type. You can enter either a password in simple text mode or ciphertext mode, but the password is displayed in ciphertext in the configuration file.	-
cipher-text	Specifies a ciphertext password.	The value can be a string of 1 to 255 characters for simple passwords and 20 to 392 characters for ciphertext passwords.
keychain	Configures keychain authentication. **NOTE** Before you configure keychain authentication, run the **keychain** command to configure a keychain, the **key-id** command to configure a key ID, the **key-string** command to configure a password, and the **algorithm** command to configure an algorithm. If these commands are not run, OSPFv3 authentication fails. OSPFv3 supports only **hmac-sha256** in the **algorithm** command.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
keychain-name	Specifies a keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
instance *instance-id*	Specifies the instance ID of the virtual link.	The value is an integer ranging from 0 to 255. By default, it is 0.

Views

OSPFv3 area view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **vlink-peer** command to set up a logical connection in a discontinuous backbone area or a non-backbone area which is not connected to the backbone area directly. The virtual link can be regarded as a common interface on which OSPFv3 is enabled, because the principles of **hello**, **retransmit,** and **trans-delay** that are configured on the virtual link are similar.

The SA configured using the **ipsec sa (OSPFv3)** command can be applied to all virtual links in an OSPFv3 process or area. The SA configured using the **vlink-peer ipsec sa** command is applied to a specified virtual link. The SA configured using the **ipsec sa (OSPFv3)** command in area 0 can be applied to a specified virtual link.

To improve OSPFv3 network security, configure the **authentication-mode** parameter.

Prerequisites

Before configuring the **vlink-peer** command, ensure that an **IPSec proposal** and an **IPSec SA** have been configured on the device.

Precautions

- The **ipsec sa** and **authentication-mode** parameters cannot be configured on the same interface or in the same OSPFv3 area.
- A virtual link must be configured at both ends of the link, or it will not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an OSPFv3 virtual link to 10.110.0.3.

```
<Huawei> system-view
[Huawei] ospfv3 1
[Huawei-ospfv3-1] area 10.0.0.0
[Huawei-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```

Related Topics

9.5.30 display ospfv3 vlink

9.5.41 ipsec sa (OSPFv3)

9.6 IPv4 IS-IS Configuration Commands

NOTE

In practical application, in order to realize that business forwarding is not affected by motherboard failure, it is usually possible to configure BGP GR in the hardware environment of dual motherboard to make sense.

All the models support the GR Helper, and only AR3200 series support the GR Restarter.

9.6.1 adjacency-strict-check enable

Function

The **adjacency-strict-check enable** command enables IS-IS adjacency strict-check.

The **undo adjacency-strict-check enable** command disables IS-IS adjacency strict-check.

The **adjacency-strict-check disable** command disables IS-IS adjacency strict-check.

By default, IS-IS adjacency strict-check is disabled when IS-IS establishes neighbor relationships.

Format

adjacency-strict-check enable

undo adjacency-strict-check [**enable**]

adjacency-strict-check disable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the establishment of IS-IS neighbor relationships, if both IPv4 and IPv6 are configured at both ends, both IPv4 and IPv6 neighbors are established. By default, IPv4 and IPv6 share the standard topology. When the faulty link is restored, IPv4 goes Up faster than IPv6. After the IS-IS router receives a message indicating that IPv4 goes Up, it considers that both IPv4 and IPv6 neighbors are established. If IPv6 packets are being transmitted at that time, some of these IPv6 packets are discarded.

To resolve this problem, run the **adjacency-strict-check enable** command to enable IS-IS adjacency strict-check to ensure that an IS-IS neighbor is established only when both IPv4 and IPv6 go Up.

Prerequisites

You have created an IS-IS process and entered the IS-IS view using the **isis** command.

Configuration Impact

After you run the **adjacency-strict-check enable** command on a broadcast network, the basic topology becomes Down if the IP protocol enabled on the local router is different from that on its neighbors.

After you run the **adjacency-strict-check enable** command on a P2P network, neighbor relationships cannot be established if the IP protocol enabled on the local router is different from that on its neighbors and only the basic topology is available for the local router.

Example

Enable adjacency strict-check on IS-IS process 1.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] adjacency-strict-check enable
```

Related Topics

9.6.56 isis

9.6.2 area-authentication-mode

Function

The **area-authentication-mode** command configures an IS-IS area to authenticate received Level-1 packets (LSPs and SNPs) using the specified authentication mode and password or adds authentication information to Level-1 packets to be sent.

 Copyright © Huawei Technologies Co., Ltd.

The **undo area-authentication-mode** command restores the default configuration.

By default, the system neither encapsulates generated Level-1 packets with authentication information nor authenticates received Level-1 packets.

Format

area-authentication-mode { { **simple** { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } | **md5** { [**cipher**] *plain-cipher-text* | **plain** *plain-text* } } [**ip** | **osi**] | { **keychain** *keychain-name* } } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

area-authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

undo area-authentication-mode

Parameters

Parameter	Description	Value
simple	Transmits the password in plain text. **NOTICE** Simple authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
plain *plain-text*	Specifies the authentication password in plain text. You can enter only the password in plain text. When you view the configuration file, the password is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *plain-cipher-text*	Specifies the authentication password in cipher text. You can enter the password in plain or cipher text. When you view the configuration file, the password is displayed in cipher text. By default, the password is in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters in plain text or a string of 32 or 48 characters in cipher text. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters in plain text or a string of 20 to 392 characters in cipher text.
md5	Transmits the password that is encrypted using MD5. **NOTICE** MD5 authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
ip	Indicates the IP authentication password. This parameter cannot be configured when keychain authentication is used.	-
osi	Indicates the OSI authentication password. This parameter cannot be configured when keychain authentication is used. When neither **osi** nor **ip** is specified, the default parameter **osi** is used.	-
keychain *keychain-name*	Indicates the keychain that changes with time and is encrypted using MD5. This parameter takes effect only when *keychain-name* is set using the **19.20.4 keychain** command.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
snp-packet	Authenticates SNPs.	-

Parameter	Description	Value
authentication-avoid	Encapsulates generated LSPs but not SNPs with authentication information and authenticates received LSPs but not SNPs.	-
send-only	Encapsulates generated LSPs and SNPs with authentication information, and authenticates received LSPs but not SNPs.	-
all-send-only	Encapsulates generated LSPs and SNPs with authentication information, but does not authenticate received LSPs and SNPs.	-
hmac-sha256	Encapsulates generated packets with the HMAC-SHA256 authentication and a password encrypted by the HMAC-SHA256 algorithm and authenticates received packets.	-
key-id *key-id*	Indicates key ID of the HMAC-SHA256 algorithm.	It is an integer ranging from 0 to 65535.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IS-IS packets to be sent are not encapsulated with authentication information, and the received packets are not authenticated. If a user sends malicious packets to attack a network, information on the entire network may be stolen. Therefore, you can configure IS-IS authentication to improve the network security.

The area authentication password is encapsulated into Level-1 IS-IS packets. Only the packets that pass the area authentication can be accepted. Therefore, you can configure IS-IS area authentication to authenticate the Level-1 area.

Precautions

The **area-authentication-mode** command is valid only on Level-1 or Level-1-2 routers.

By using this command enables IS-IS to discard all the Level-1 LSPs and SNPs whose area authentication passwords are not consistent with the one set by this

command. At the same time, IS-IS inserts the configured area authentication password into all the Level-1 routing packets (LSPs and SNPs) sent from the local node. The establishment of the Level-1 neighbor relationship is not affected, regardless of whether the packets pass the area authentication.

The authentication takes effect only on the peer configured with authentication. The peer with no authentication configured can still receive the LSP and SNP packet with the password.

Example

Set the area authentication mode to HMAC-SHA256, key id to 23, and password to **admin@huawei**.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] area-authentication-mode hmac-sha256 key-id 23 cipher admin@huawei
```

Related Topics

9.6.42 domain-authentication-mode

9.6.57 isis authentication-mode

19.20.4 keychain

9.6.3 attached-bit advertise

Function

The **attached-bit advertise** command configures a rule for setting the ATT bit in Link state Protocol Data Units (LSPs).

The **undo attached-bit advertise** command restores the default setting rule.

By default, the Level-1-2 device sets the ATT bit in LSPs using the default rule.

Format

attached-bit advertise { **always** | **never** }

undo attached-bit advertise

Parameters

Parameter	Description	Value
always	Indicates that the ATT bit is set to 1.	-
never	Indicates that the ATT bit is set to 0.	-

Views

IS-IS view or IS-IS topology view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ATT bit is a field in link state packets. An ATT bit identifies whether Level-1 area is attached to other areas. A Level-1-2 device sets the ATT bit to 1 to notify the devices in Level-1 area of its attachment to a Level-2 backbone area. After a Level-1 device receives the LSPs carrying the ATT bit 1 from the Level-1-2 device, the Level-1 device generates a route with the same destination address as the default route of the Level-1-2 device. Traffic can be forwarded along this route.

The preceding rule is the default rule for setting the ATT bit in the Intermediate System to Intermediate System (IS-IS) protocol. You can run the **attached-bit advertise** command to configure a rule for setting the ATT bit as required.

- If you want the ATT bit in LSPs to be set to 1, run the **attached-bit advertise always** command.
- If you want to disable the Level-1 device connected to the Level-1-2 device from advertising default routes when the ATT bit is set to 1, run either of the following commands:
  - Run the **attached-bit advertise never** command on the Level-1-2 device to disable the device from sending LSPs with the ATT bit 1.
  - Run the **attached-bit avoid-learning** command on the Level-1 device that is connected to the Level-1-2 device.

  Running the **attached-bit advertise never** command applies to all Level-1 devices that receive LSPs with the ATT bit 0. Therefore, it is more convenient.

Precautions

The ATT bit is defined in both Level-1 and Level-2 LSPs, but it can be set to 1 only in Level-1 LSPs. Additionally, only the Level-1-2 device can set the ATT bit. Therefore, running the **attached-bit avoid-learning** command takes effect only on the Level-1-2 device.

Example

Enable the Level-1-2 device to set the ATT bit to 1 in the LSPs sent in IS-IS process 1.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] attached-bit advertise always
```

Related Topics

9.6.4 attached-bit avoid-learning

9.6.4 attached-bit avoid-learning

Function

The **attached-bit avoid-learning** command disables a device from advertising default routes to a routing table when the ATT bit is set to 1.

The **undo attached-bit avoid-learning** command restores the device to generates default routes when the ATT bit is set to 1.

By default, a device advertises default routes when the ATT bit is set to 1.

Format

attached-bit avoid-learning

undo attached-bit avoid-learning

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

An ATT bit is a field in link state packets. An ATT bit identifies whether Level-1 area is attached to other areas. A Level-1-2 device sets the ATT bit to 1 to notify the devices in Level-1 area of its attachment to a Level-2 backbone area. After a Level-1 device receives the LSPs carrying the ATT bit 1 from the Level-1-2 device, the Level-1 device generates a route with the same destination address as the default route of the Level-1-2 device. Traffic can be forwarded along this route.

To prevent the Level-1 device from advertising the default route when the ATT bit is set to 1, run the **attached-bit avoid-learning** command.

To prevent the Level-1 device from advertising default routes to the routing table, run either of the following commands:

- Run the **attached-bit advertise never** command on the Level-1-2 device to disable the device from sending LSPs with the ATT bit 1.
- Run the **attached-bit avoid-learning** command on the Level-1 device that is connected to the Level-1-2 device.

The difference between the preceding commands lies in that the **attached-bit avoid-learning** command applies to a specified device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable IS-IS-enabled device from advertising default routes to a routing table when the ATT bit is set to 1.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] attached-bit avoid-learning
```

Related Topics

9.6.3 attached-bit advertise

9.6.5 auto-cost enable

Function

The **auto-cost enable** command enables IS-IS to automatically calculate the interface cost based on the interface bandwidth.

The **undo auto-cost enable** command disables IS-IS from automatically calculating the interface cost based on the interface bandwidth.

By default, IS-IS is disabled from automatically calculating the interface cost based on the interface bandwidth.

Format

auto-cost enable [**compatible**]

undo auto-cost enable

Parameters

Parameter	Description	Value
compatible	Specifies the IS-IS to calculate the cost of an interface based on the bandwidth of the interface automatically in compatible.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is run, if the cost of an IS-IS interface is not set in the interface view and no cost is set in the IS-IS view, the system automatically calculates a cost for the interface.

 Copyright © Huawei Technologies Co., Ltd.

If the cost style of the system is wide or wide-compatible:

When **auto-cost enable** command is configured, Interface cost = (Bandwidth-reference/Link-bandwidth) x 10.

When **auto-cost enable compatible** command is configured, Interface cost = (Bandwidth-reference/Link-bandwidth).

The cost style is set by the **cost-style** command. The Bandwidth-reference is set by the **bandwidth-reference** command. The Link-bandwidth is the interface bandwidth.

If the cost style of the system is narrow, narrow-compatible or compatible, the cost of each interface is based on the following table.

Table 9-86 Relationship between the IS-IS interface cost and the bandwidth

Cost	Range of the Interface Bandwidth
60	Interface bandwidth =< 10 Mbit/s
50	10 Mbit/s < Interface bandwidth ≤ 100 Mbit/s
40	100 Mbit/s < Interface bandwidth ≤ 155 Mbit/s
30	155 Mbit/s < Interface bandwidth ≤ 622 Mbit/s
20	622 Mbit/s < Interface bandwidth ≤ 2.5 Gbit/s
10	2.5 Gbit/s < Interface bandwidth

Precautions

The priority of the cost value of the global configured by the **circuit-cost** command is higher than the auto cost value.

The **auto-cost enable** command cannot change the cost of the loopback interface.

Example

Enable IS-IS to automatically calculate the interface cost.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] auto-cost enable
```

Related Topics

9.6.6 bandwidth-reference (IS-IS)

9.6.9 circuit-cost

9.6.64 isis cost

 Copyright © Huawei Technologies Co., Ltd.

9.6.11 cost-style

9.6.6 bandwidth-reference (IS-IS)

Function

The **bandwidth-reference** command sets the bandwidth reference value that is used in automatic IS-IS interface cost calculation.

The **undo bandwidth-reference** command restores the default bandwidth reference value that is used in automatic IS-IS interface cost calculation.

By default, the bandwidth reference value is 100 Mbit/s.

Format

bandwidth-reference *value*

undo bandwidth-reference

Parameters

Parameter	Description	Value
value	Specifies the bandwidth reference value used in automatic IS-IS interface cost calculation.	The value is an integer that ranges from 1 to 2147483648, in Mbit/s.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the set link cost of IS-IS routes reflect the actual link cost, configure a proper link cost for all interfaces or enable automatic interface cost calculation. To enable automatic interface cost calculation, set a proper bandwidth reference value.

You can run the **bandwidth-reference** command to set a proper bandwidth reference value. After automatic interface cost calculation is enabled, and the cost type is wide or wide-compatible, the system calculates the cost of each interface with the following formula: Interface cost = (Bandwidth-reference/Interface bandwidth) x 10. If the interface cost calculated through this formula is greater than 16777214, 16777214 is used as the interface cost for route calculation. That is, the interface cost will never be greater than 16777214.

 Copyright © Huawei Technologies Co., Ltd.

After the **9.6.5 auto-cost enable** command enables automatic IS-IS interface cost calculation, the system automatically calculates the interface cost based on the bandwidth reference value set using the **bandwidth-reference** command.

NOTE

The cost style is set by the **cost-style** command.

Precautions

Rules for automatically calculating the IS-IS interface cost vary according to the cost style of the IS-IS interface:

- The bandwidth reference value set using the **bandwidth-reference** command takes effect only when the cost style is wide or wide-compatible. In this case, the interface cost is calculated using the following formula:

  Interface cost = (Bandwidth-reference/Interface bandwidth) x 10.
- If the cost style of the system is narrow, narrow-compatible or compatible, the cost of each interface is based on the **Table 9-87**.

Table 9-87 Relationship between the IS-IS interface cost and the bandwidth

Cost	Range of the Interface Bandwidth
60	Interface bandwidth ≤ 10 Mbit/s
50	10 Mbit/s < Interface bandwidth ≤ 100 Mbit/s
40	100 Mbit/s < Interface bandwidth ≤ 155 Mbit/s
30	155 Mbit/s < Interface bandwidth ≤ 622 Mbit/s
20	622 Mbit/s < Interface bandwidth ≤ 2.5 Gbit/s
10	2.5 Gbit/s < Interface bandwidth

Example

Set the reference value of the system bandwidth to 1000 Mbit/s.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] bandwidth-reference 1000
```

Related Topics

9.6.5 auto-cost enable

9.6.11 cost-style

9.6.7 bfd all-interfaces (IS-IS)

Function

The **bfd all-interfaces** command sets values for BFD session parameters used in BFD for IS-IS.

The **undo bfd all-interfaces** command restores the default values of BFD session parameters used in BFD for IS-IS.

By default, the minimum intervals for receiving and sending BFD packets are 1000 ms and the detection time multiplier is 3.

Format

bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* } *
(AR100&AR120&AR150&AR160&AR200 series)

undo bfd all-interfaces { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] } *
(AR100&AR120&AR150&AR160&AR200 series)

bfd all-interfaces { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } *
(AR1200&AR2200&AR3200 series)

undo bfd all-interfaces { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] | **frr-binding** } *
(AR1200&AR2200&AR3200 series)

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Specifies the minimum interval for receiving BFD packets from the peer end. The interval for receiving BFD packets between determines the BFD session detection time. On an unstable link, a smaller receive interval may result in BFD session flapping. To prevent BFD session flapping, increase the receive interval.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-tx-interval *transmit-interval*	Specifies the minimum interval for transmitting BFD packets to the peer end. The interval for transmitting BFD packets determines the BFD session detection time. On a stable link, you can increase the transmit interval to prevent frequent link status detection.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
detect-multiplier *multiplier-value*	Specifies the local detection multiplier. On a stable link, you can increase the BFD detection multiplier to prevent frequent link status detection.	The value is an integer that ranges from 3 to 50. The default value is 3.
frr-binding	Binds the BFD session status to IS-IS Auto FRR. When BFD detects a link fault on an interface, the BFD session goes Down, triggering FRR on the interface. Then traffic is switched from the faulty link to the backup link to ensure traffic forwarding. **NOTE** The AR100&AR120&AR150&AR160&AR200 series do not support this parameter.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the establishment of a BFD session, you can adjust the interval for transmitting BFD packets, interval for receiving BFD packets, and local detection multiplier according to network and performance requirements.

Precautions

The value of *receive-interval* is obtained by negotiating the local **min-rx-interval** value and the remote **min-tx-interval** value. If a router does not receive any BFD packet from its peer in the *receive-interval* × *multiplier-value* period, the router advertises that its peer is Down.

If only parameters of a BFD session are set but the **bfd all-interfaces enable** command is not used, the BFD session cannot be set up.

NOTE

The BFD priority of the interface is higher than the BFD priority of the process. If BFD of the interface is enabled, the BFD session is set up based on the BFD parameters on the interface.

Example

Enable BFD in an IS-IS process and set the minimum interval for transmitting BFD packets to 600 ms.

```
<Huawei> system-view
```

```
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] isis
[Huawei-isis-1] bfd all-interfaces enable
[Huawei-isis-1] bfd all-interfaces min-tx-interval 600
```

Enable BFD in an IS-IS process and bind the BFD session status to IS-IS Auto FRR.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] bfd all-interfaces enable
[Huawei-isis-1] bfd all-interfaces frr-binding
```

Related Topics

9.6.8 bfd all-interfaces enable

9.6.58 isis bfd

9.6.8 bfd all-interfaces enable

Function

The **bfd all-interfaces enable** command enables BFD in an IS-IS process.

The **undo bfd all-interfaces enable** command disables BFD in an IS-IS process.

By default, BFD is disabled in an IS-IS process.

Format

bfd all-interfaces enable

undo bfd all-interfaces enable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If global BFD is not enabled, you can configure IS-IS BFD but cannot set up the BFD session. Before establishing BFD sessions, you need to enable BFD on the two ends.

Precautions

When BFD is enabled in the process using the **bfd all-interfaces enable** command, the interface does not set up a BFD session in the following cases:

- The **isis bfd block** command is used on the interface. The command suppresses the BFD capability of the interface. To set up a session on the interface, run the **undo isis bfd block** command.
- When the **isis bfd static** command is used on the interface, the interface does not set up the BFD session. To set up a session on the interface, run the **undo isis bfd static** command.

NOTE

The BFD priority of the interface is higher than the BFD priority of the process. If BFD of the interface is enabled, a BFD session is set up based on the BFD parameters on the interface.

Example

Enable BFD in an IS-IS process.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] isis
[Huawei-isis-1] bfd all-interfaces enable
```

Related Topics

9.6.7 bfd all-interfaces (IS-IS)

9.6.59 isis bfd block

9.6.61 isis bfd static

9.6.58 isis bfd

9.6.9 circuit-cost

Function

The **circuit-cost** command sets the link cost for all IS-IS interfaces during SPF calculation.

The **undo circuit-cost** command deletes the configured link cost of all IS-IS interfaces.

By default, no link cost is set for IS-IS interfaces.

Format

circuit-cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo circuit-cost [*cost* | **maximum**] [**level-1** | **level-2**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cost	Specifies the interface cost used in SPF calculation.	If the IS-IS cost style is wide or wide-compatible, the cost of imported routes ranges from 1 to 16777214; otherwise, the cost ranges from 1 to 63.
maximum	Sets the link cost of IS-IS interfaces to 16777215. **NOTE** You can configure this parameter only when the IS-IS cost style is wide or wide-compatible. After the interface cost is set to 16777215, the neighbor TLV generated on the link can only be used to transmit TE information but cannot be used for route calculation.	-
level-1	Specifies the link cost for all Level-1 interfaces. If no level is specified, the link cost is set for Level-1-2 interfaces.	-
level-2	Specifies the link cost for all Level-2 interfaces. If no level is specified, the link cost is set for Level-1-2 interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large network, there are often multiple valid routes to the same destination. IS-IS can use the SPF algorithm to calculate the optimal route to forward traffic. This may cause the following problems:

- All traffic is forwarded along the optimal path, resulting in load unbalance.
- If the optimal path is intermittently disconnected, traffic is still forwarded along the optimal path, resulting in traffic loss.

To solve the preceding problems, run the **circuit-cost** command to change the cost of all IS-IS interfaces so that traffic can be forwarded along different physical links.

Precautions

The **isis cost** command takes precedence over the **circuit-cost** command. The **circuit-cost** command cannot change the cost of loopback interfaces.

Changing the link cost of interfaces will cause routes of the entire network to be recalculated and change the forwarding path of traffic.

Example

Set the default cost of all Level-1-2 interfaces to 30.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] circuit-cost 30
```

Set the link cost of all IS-IS interfaces to 16777215.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] circuit-cost maximum
```

Related Topics

9.6.64 isis cost

9.6.11 cost-style

9.6.10 circuit default-tag

Function

The **circuit default-tag** command sets the administrative tag value for all interfaces in an IS-IS process.

The **undo circuit default-tag** command restores the default administrative tag value for all interfaces in an IS-IS process.

By default, the administrative tag value of all IS-IS interfaces is 0.

Format

circuit default-tag *tag* [**level-1** | **level-2**]

undo circuit default-tag [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag value for all interfaces in an IS-IS process.	The value is an integer that ranges from 1 to 4294967295.
level-1	Specifies the administrative tag value for all Level-1 interfaces in an IS-IS process. If no interface level is specified, the administrative tag values of Level-1 and Level-2 interfaces are set.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
level-2	Specifies the administrative tag value for all Level-2 interfaces in an IS-IS process. If no interface level is specified, the administrative tag values of Level-1 and Level-2 interfaces are set.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrative tag carries management information about IP address prefixes to control the import of routes of different levels and areas. You can use the administrative tag to control the advertisement of IP address prefixes in an IS-IS routing domain to simplify route management.

The **circuit default-tag** command allows you to set the administrative tag value for all routes in an IS-IS process. You can filter routes based on the configured administrative tag value.

The administrative tag for an interface is advertised along with routing information.

- When the cost style of IS-IS is narrow or narrow-compatible, the administrative tag value is neither advertised nor takes effect in the LSP.
- When the cost style of IS-IS is wide, wide-compatible, or compatible, the administrative tag value is advertised in the LSP.

Precautions

The value of the administrative tag configured through the**circuit default-tag** command is the global administrative tag. The priority of the interface administrative tag configured by the **isis tag-value** command is higher than the priority of the global administrative tag.

Example

Set the administrative tag value of Level-1 interfaces to 30.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] circuit default-tag 30 level-1
```

 Copyright © Huawei Technologies Co., Ltd.

9.6.11 cost-style

Function

The **cost-style** command sets the cost style of routes received and sent by an IS-IS device.

The **undo cost-style** command restores the default cost style of routes received and sent by an IS-IS device.

By default, the cost style of routes received and sent by an IS-IS device is narrow.

Format

cost-style { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }

undo cost-style

Parameters

Parameter	Description	Value
narrow	Configures an IS-IS device to receive and send only routes with cost style narrow. When the cost style is narrow, the cost of routes ranges from 1 to 63.	-
wide	Configures an IS-IS device to receive and send only routes with cost style wide. When the cost style is wide, the cost of routes ranges from 1 to 16777215.	-
wide-compatible	Configures an IS-IS device to receive routes with cost style narrow or wide and sent only routes with cost style wide.	-
compatible	Configures an IS-IS device to receive and send routes with cost style narrow or wide.	-
narrow-compatible	Configures an IS-IS device to receive routes with cost style narrow or wide and sent only routes with cost style narrow.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
relax-spf-limit	Configures an IS-IS device to receive routes with cost higher than 1023. If this parameter is specified, there is no restriction on the link costs of interfaces or route costs. The cost of a received route is the actual cost. If this parameter is not specified, the following situations occur: ● If the cost of a route is smaller than or equal to 1023, and the link cost of each interface through which the route passes is smaller than or equal to 63: The cost of the route is the sum of link costs of all interfaces through which the route passes. ● If the cost of a route is smaller than or equal to 1023, and the link costs of certain interfaces through which the route passes are larger than 63: An IS-IS device can learn only the routes imported by the interfaces and direct routes of the network segment where the interfaces reside. The costs of these routes are the actual cost. ● If the cost of a route is larger than 1023: The device can receive only the routes of the network segment where the interface with link cost smaller than 1023 resides. If the cost of a route is larger than 1023, the cost is calculated as 1023.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the cost style of IS-IS routes is narrow, indicating that only routes with the cost ranging from 1 to 63 can be received and sent. LSPs carrying tag information to be filtered by a routing policy cannot be flooded when the cost style is narrow. The **cost-style** command can be used to change the cost style of IS-IS routes so that they can be transmitted successfully.

NOTE

The AR100&AR120&AR150&AR160&AR200 do not support MPLS.

To implement extended IS-IS functions, setting the cost style of IS-IS routes to **wide** is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When the cost style of a route is changed from wide to narrow, transmission of the route may be interrupted.

If you want to change the cost style of IS-IS routes, running the command while configuring basic IS-IS functions is recommended. If the cost style of IS-IS routes is changed during network operation, the IS-IS process is restarted and neighbors are disconnected.

Example

Configure an IS-IS device to send only the packets with cost style narrow and to receive the packets with cost style narrow or wide.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] cost-style narrow-compatible
```

Related Topics

9.6.9 circuit-cost

9.6.10 circuit default-tag

9.6.12 default-route-advertise (IS-IS)

Function

The **default-route-advertise** command configures IS-IS devices to generate default routes.

The **undo default-route-advertise** command disables IS-IS devices from generating default routes.

By default, IS-IS devices do not generate default routes.

Format

default-route-advertise [**always** | **match default** | **route-policy** *route-policy-name*] [**cost** *cost* | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] * [**avoid-learning**]

undo default-route-advertise

Parameters

Parameter	Description	Value
always	Configures an IS-IS device to unconditionally advertise default routes with itself as the next hop.	-

Parameter	Description	Value
match default	Advertises a default route through an LSP if the default route is generated by other routing protocols or other IS-IS processes in the routing table. If this default route is deleted from the routing table, it is not advertised through an LSP.	-
route-policy *route-policy-name*	Specifies the name of a route-policy. A Level-1-2 device advertises default routes to the IS-IS routing domain only when there are external routes matching the route-policy in the routing table of the device. This prevents routing blackhole when link faults make some important external routes unavailable but default routes are still advertised. This route-policy does not affect external route import in IS-IS.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
cost *cost*	Specifies the cost of default routes.	The value is an integer. The value range varies according to the cost style. When the cost style is narrow, narrow-compatible, or compatible, the value ranges from 0 to 63. When the cost style is wide or wide-compatible, the value ranges from 0 to 4261412864.
tag *tag*	Specifies the tag value of advertised default routes. Advertised LSPs carry the tag value only when the IS-IS cost style is wide, wide-compatible, or compatible.	The value is an integer that ranges from 1 to 4294967295.
level-1	Sets the level of default routes to Level-1. If no level is specified, Level-2 default routes are generated by default.	-
level-2	Sets the level of default routes to Level-2. If no level is specified, Level-2 default routes are generated by default.	-
level-1-2	Sets the level of default routes to Level-1-2. If no level is specified, Level-2 default routes are generated by default.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
avoid-learning	Prevents an IS-IS process from learning default routes or adding them to the routing table. If existing default routes in the routing table are active, set the default route that needs to be added to the routing table to inactive.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IS-IS and other routing protocols are running on a network, use either of the following methods to allow the traffic within the IS-IS domain to be transmitted to other routing domains:

- Configure a boundary router in the IS-IS domain to advertise default routes to the IS-IS domain.
- Configure a boundary router in the IS-IS domain to import routes from the other routing domains to the IS-IS domain.

The first method is simpler, because the routers in the IS-IS domain do not need to learn routes imported form the other routing protocols.

Precautions

You can specify **always** to allow default routes to be advertised unconditionally; in this case, the device still calculates default routes from other devices.

NOTE

If **always** is configured on multiple devices within the same area, a routing loop may occur.

After this command is run on an IS-IS router, all traffic in an IS-IS domain will be forwarded by this IS-IS router to a destination outside the domain. Compared with configuring a static default route on each router in an IS-IS domain, running this command simplifies configurations, because this command only needs to be run on a boundary router in the IS-IS domain. In addition, you can specify different parameters to allow default routes to be advertised in different ways.

If this command is run on a Level-1 router, the router advertises default routes only to the Level-1 area.

Example

Configure the current IS-IS device to advertise the IPv4 default routes that match route-policy **filter** and set the cost of these default routes to 15.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] default-route-advertise route-policy filter cost 15
```

9.6.13 description (IS-IS)

Function

The **description** command configures a description for an IS-IS process.

The **undo description** command deletes the description of an IS-IS process.

By default, no description is configured for an IS-IS process.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Configures a description for an IS-IS process.	The value is a string of 1 to 80 case-sensitive characters. Spaces are supported.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring descriptions for IS-IS processes helps identify and maintain IS-IS processes.

IS-IS process description that is configured through the **description** command is not advertised in an LSP.

IS-IS process description that is configured through the **is-name** command is advertised in an LSP.

Precautions

If you run the **description** command multiple times, only the latest configuration takes effect.

Example

Configure description for IS-IS process 1.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] description this process configure the area-authentication-mode
```

9.6.14 display default-parameter isis

Function

The **display default-parameter isis** command displays the default IS-IS configuration.

Format

display default-parameter isis

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the default IS-IS configuration.

```
<Huawei> display default-parameter isis

Default Configurations For Process
-----------------------------------------------------------------------------
  Cost-Style                          : Narrow
  Circuit-Cost <IPv4>                 : L1 10 L2 10
  Circuit-Cost <IPv6>                 : L1 10 L2 10
  IS-Level                            : L12
  LSP-Originate-Length                : 1497
  LSP-Receive-Length                  : 1497
  LSP-Max-Age <s>                     : 1200
  LSP-Generation-IntelliTimer <s,ms,ms> : L1 Max 2 Init 0 Incr 0
                                        L2 Max 2 Init 0 Incr 0
  LSP-Refresh-Interval <s>            : 900
  Preference                          : IPv4 15 IPv6 15
  SPF-IntelliTimer <s,ms,ms>          : Max 5 Init 50 Incr 200

                Default Configurations For Interfaces
                -------------------------------------
  Circuit-Level                       : L12
  CSNP-Interval <s>                   : L1 10 L2 10
  Cost <IPv4>                         : L1 10 L2 10
  Cost <IPv6>                         : L1 10 L2 10
  DIS-Priority                        : L1 64 L2 64
```

```
Hello-Interval <s>              : L1 10 L2 10
Holding-Multiplier               : L1 3 L2 3
LSP-Retransmit <s>                : 5
LSP-Throttle <ms>                 : 50 count 10
PPP-Negotiation                  : 3-Way
```

Table 9-88 Description of the display default-parameter isis command output

Item	Description
Default Configurations For Process	Default configuration of an IS-IS process.
Cost-Style	IS-IS cost style: ● narrow ● wide ● wide-compatible ● compatible ● narrow-compatible To set the IS-IS cost style, run the **9.6.11 cost-style** command.
Circuit-Cost <IPv4>	Cost of all IS-IS IPv4 interfaces. To set the cost of IS-IS IPv4 interfaces, run the **9.6.9 circuit-cost** command.
Circuit-Cost <IPv6>	Cost of all IS-IS IPv6 interfaces. To set the cost of IS-IS IPv6 interfaces, run the **9.7.3 ipv6 circuit-cost** command.
IS-Level	Level of an IS-IS device: ● L1: Level-1 device ● L2: Level-2 device ● L12: Level-1-2 device To set the level of an IS-IS device, run the **9.6.91 is-level** command.
LSP-Originate-Length	Maximum length of an LSP generated by IS-IS. To set the maximum length of an LSP generated by IS-IS, run the **9.6.99 lsp-length** command.
LSP-Receive-Length	Maximum length of an LSP received by IS-IS. To set the maximum length of an LSP received by IS-IS, run the **9.6.99 lsp-length** command.
LSP-Max-Age <s>	Maximum lifetime of an LSP generated by an IS-IS process, in seconds. To set the maximum lifetime of an LSP generated by an IS-IS process, run the **9.6.124 timer lsp-max-age** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
LSP-Generation-IntelliTimer <s,ms,ms>	Delay in generating LSPs: • L1: delay for a Level-1 router to generate LSPs • L2: delay for a Level-2 router to generate LSPs • Max: maximum delay in generating LSPs, in seconds • Init: initial delay in generating LSPs, in milliseconds • Incr: incremental delay in generating LSPs, in milliseconds To set the delay in generating LSPs, run the **9.6.123 timer lsp-generation** command.
LSP-Refresh-Interval <s>	Interval for refreshing LSPs, in seconds. To set the interval for refreshing LSPs, run the **9.6.125 timer lsp-refresh** command.
Preference	Protocol preference of IS-IS routes. To set the protocol preference of IS-IS routes, run the **9.6.104 preference (IS-IS)** command.
SPF-IntelliTimer <s,ms,ms>	Delay in SPF calculation: • Max: maximum delay in SPF calculation, in seconds • Init: initial delay in SPF calculation, in milliseconds • Incr: incremental delay in SPF calculation, in milliseconds To set the delay in SPF calculation, run the **9.6.127 timer spf** command.
Default Configurations For Interfaces	Default configuration of IS-IS interfaces.
Circuit-Level	IS-IS interface level. To set the IS-IS interface level, run the **9.6.62 isis circuit-level** command.
CSNP-Interval <s>	Interval for sending CSNPs, in seconds. To set the interval for sending CSNPs, run the **9.6.86 isis timer csnp** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Cost <IPv4>	Cost of IS-IS interfaces in an IPv4 topology. To set the cost of IS-IS interfaces in an IPv4 topology, run the **9.6.64 isis cost** command.
Cost <IPv6>	Cost of IS-IS interfaces in an IPv6 topology. To set the cost of IS-IS interfaces in an IPv6 topology, run the **9.7.17 isis ipv6 cost** command.
DIS-Priority	Priority for DIS election. To set the priority for DIS election, run the **9.6.67 isis dis-priority** command.
Hello-Interval <s>	Interval for sending Hello packets, in seconds. To set the interval for sending Hello packets, run the **9.6.87 isis timer hello** command.
Holding-Multiplier	Number of consecutive Hello packets that are not received before the neighbor is declared Down. To set this value, run the **9.6.88 isis timer holding-multiplier** command.
LSP-Retransmit <s>	Interval for retransmitting LSPs on a P2P link, in seconds. To set the retransmit interval, run the **9.6.89 isis timer lsp-retransmit** command.
LSP-Throttle <ms>	Interval for sending LSPs or CSNPs, in seconds, and number of LSPs or CSNPs that are sent each time. To set the two values, run the **9.6.90 isis timer lsp-throttle** command.
PPP-Negotiation	PPP negotiation type during the establishment of IS-IS adjacencies: • 2-way • 3-way • only To set the PPP negotiation type during the establishment of IS-IS adjacencies, run the **9.6.74 isis ppp-negotiation** command.

Related Topics

9.6.11 cost-style

9.6.9 circuit-cost

9.7.3 ipv6 circuit-cost
9.6.91 is-level
9.6.99 lsp-length
9.6.124 timer lsp-max-age
9.6.123 timer lsp-generation
9.6.125 timer lsp-refresh
9.6.104 preference (IS-IS)
9.6.127 timer spf
9.6.62 isis circuit-level
9.6.86 isis timer csnp
9.6.64 isis cost
9.7.17 isis ipv6 cost
9.6.67 isis dis-priority
9.6.87 isis timer hello
9.6.88 isis timer holding-multiplier
9.6.89 isis timer lsp-retransmit
9.6.90 isis timer lsp-throttle
9.6.74 isis ppp-negotiation

9.6.15 display isis cost interface

Function

The **display isis cost interface** command displays costs of an interface and how they are generated.

Format

display isis cost interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display isis cost interface** command to check costs of an IS-IS interface, including the link cost and route prefix cost that the interface uses in each topology, and how the costs are generated.

Example

Display costs of GE 1/0/0 and how they are generated.

```
<Huawei> display isis cost interface gigabitethernet 1/0/0
Interface: GE 1/0/0
                        Level-2 interface cost
 Topology base(0):
  Link effective cost: 10(A)                    enabled by circuit cost
  IP prefix effective cost:
   10.10.7.0/24                cost: 10         enabled by circuit cost
   10.10.8.0/24                cost: 10         enabled by circuit cost
   10.10.9.0/24                cost: 10         enabled by circuit cost
 Topology red(7):
  Link effective cost: 87(A)                    enabled by circuit cost
  IP prefix effective cost:
   10.10.7.0/24                cost: 87         enabled by circuit cost
   10.10.8.0/24                cost: 87         enabled by circuit cost
   10.10.9.0/24                cost: 87         enabled by circuit cost
 Topology ipv6(2):
  Link effective cost: 10(A)                    enabled by circuit cost
  IPv6 prefix effective cost:
   63::/64                   cost: 10          enabled by circuit cost
   101:10:7::/64               cost: 10         enabled by circuit cost
   101:10:8::/64               cost: 10         enabled by circuit cost
   101:10:9::/64               cost: 10         enabled by circuit cost

                 Flags: R-Relative cost  A-Absolute cost
```

Table 9-89 Description of the **display isis cost interface** command output

Item	Description
Interface	Type and ID of an interface on which IS-IS is enabled
Link effective cost	Link cost
IP prefix effective cost	Cost of an IPv4 route
enabled by circuit cost	Default cost or cost configured in the **isis cost** command
enabled by auto cost	Cost configured in the **auto-cost enable** command
enabled by global cost	Cost configured in the **circuit cost** command
enabled by igp ldp	The interface cost is configured by LDP
enabled by rui cost	Cost that inherits the cost of the RUI route
enabled by silent cost	Cost configured in the **isis silent** command in the interface view

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
enabled by tunnel cost	Cost generated after the TE Tunnel is configured
IPv6 prefix effective cost	Cost of an IPv6 route
Flags	Cost flag ● R-Relative cost: relative cost ● A-Absolute cost: absolute cost

9.6.16 display isis bfd interface

Function

The **display isis bfd interface** command displays information about BFD-enabled IS-IS interfaces.

Format

display isis [*process-id*] **bfd interface**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about BFD-enabled interfaces.

```
<Huawei> display isis 1 bfd interface

                 BFD information of interface for ISIS(1)
                ----------------------------------------
 Interface                  BFD.State      Min-Tx       Min-Rx        Mul
 Vlanif101                    enable        1000         1000          3
 Total interfaces: 1                     Total bfd enabled interfaces: 1
```

Table 9-90 Description of the display isis bfd interface command output

Item	Description
Interface	BFD-enabled IS-IS interface. To enable BFD on an IS-IS interface, run the **9.6.8 bfd all-interfaces enable** or **9.6.60 isis bfd enable** command.
BFD.State	BFD status on the IS-IS interface: ● enable: BFD is enabled on the interface. ● disable: BFD is disabled on the interface. To enable BFD on an IS-IS interface, run the **9.6.8 bfd all-interfaces enable** or **9.6.60 isis bfd enable** command.
Min-Tx	Minimum interval for transmitting BFD packets. To set the minimum interval, run the **9.6.7 bfd all-interfaces (IS-IS)** or **9.6.58 isis bfd** command.
Min-Rx	Minimum interval for receiving BFD packets. To set the minimum interval, run the **9.6.7 bfd all-interfaces (IS-IS)** or **9.6.58 isis bfd** command.
Mul	Local detection multiplier. To set the local detection multiplier, run the **9.6.7 bfd all-interfaces (IS-IS)** or **9.6.58 isis bfd** command.

Related Topics

9.6.8 bfd all-interfaces enable

9.6.60 isis bfd enable

9.6.7 bfd all-interfaces (IS-IS)

9.6.58 isis bfd

9.6.17 display isis bfd session

Function

The **display isis bfd session** command displays information about dynamic BFD sessions.

Format

display isis [*process-id* | **vpn-instance** *vpn-instance-name*] **bfd session** { **all** | **peer** *ip-address* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Specifies all IS-IS interfaces in the IS-IS process.	-
peer *ip-address*	Specifies the IP address of a neighbor.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Specifies the interface on which BFD session statistics need to be collected.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the BFD session with a specified neighbor.

```
<Huawei> display isis bfd session all
                    BFD session information for ISIS(1)
                    -----------------------------------
Peer System ID : 0000.0000.0002          Interface : GE1/0/0
TX : 1000          BFD State : up        Peer IP Address : 10.1.1.2
RX : 1000          LocDis : 8194         Local IP Address: 10.1.1.1
Multiplier : 3     RemDis : 8197          Type : L1
Diag : No diagnostic information
Total BFD session(s) : 1
```

Table 9-91 Description of the display isis bfd session all command output

Item	Description
Peer System ID	System ID of the neighbor.

Item	Description
Interface	Local IS-IS interface connected to the neighbor.
TX	Negotiated minimum interval for transmitting BFD packets.
BFD State	BFD session status: Up or Down.
Peer IP Address	IP address of the remote IS-IS interface.
RX	Negotiated minimum interval for receiving BFD packets.
LocDis	Local discriminator dynamically assigned by BFD.
Local IP Address	IP address of the local IS-IS interface.
Multiplier	Remote detection multiplier.
RemDis	Remote identifier dynamically assigned by BFD.
Type	Level of the neighbor: ● L1: Level-1 device ● L2: Level-2 device ● L1L2: Level-1-2 device
Diag	Diagnostic information. "No diagnostic information" indicates that BFD runs properly and no diagnostic information is displayed.
Total BFD session (s)	Total number of BFD sessions.

9.6.18 display isis brief

Function

The **display isis brief** command displays brief information about IS-IS.

Format

display isis brief [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis [*process-id*] **brief**

Parameters

Parameter	Description	Value
process-id	Display brief information about a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Display brief information about the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display brief information about the IS-IS processes of all public network instances.

```
<Huawei> display isis brief

                    ISIS Protocol Information for ISIS(1)
                    -------------------------------------
SystemId: 1010.1020.1030      System Level: L12
Area-Authentication-mode: NULL
Domain-Authentication-mode: NULL
Ipv6 is not enabled
ISIS is in starting status
ISIS is in protocol hot standby state: Real-Time Backup
Flush Protect Mode: False

Interface: (GE1/0/0)
Cost: L1 10        L2 10                Ipv6 Cost: L1 10   L2 10
State: IPV4 Up                         IPV6 Down
Type: BROADCAST                            MTU: 1497
Priority: L1 64   L2 64
Timers:     Csnp: L1 10    L2 10    ,Retransmit: L12 5   , Hello: L1 10 L2 10  ,

Hello Multiplier: L1 3    L2 3     , LSP-Throttle Timer: L12 1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 9-92 Description of the display isis brief command output

Item	Description
ISIS Protocol Information for ISIS(1)	Information about IS-IS process 1. To create an IS-IS process, run the **9.6.56 isis** command.
SystemId	System ID of the current IS-IS device. To set the system ID, run the **9.6.101 network-entity** command.
System Level	Level of an IS-IS device: ● L1: Level-1 device ● L2: Level-2 device ● L12: Level-1-2 device To set the level of an IS-IS device, run the **9.6.91 is-level** command.
Area-Authentication-mode	IS-IS area authentication mode. To set the IS-IS area authentication mode and password, run the **9.6.2 area-authentication-mode** command.
Domain-Authentication-mode	IS-IS routing domain authentication mode. To set the IS-IS domain authentication mode and password, run the **9.6.42 domain-authentication-mode** command.
Ipv6 is not enabled	IPv6 is not enabled in the IS-IS process.
ISIS is in starting status	IS-IS is running.
ISIS is in protocol hot standby state: Real-Time Backup	IS-IS hot standby is real-time backup.
Flush Protect Mode	Indicates whether the process works in purge LSP protection mode.
Interface	Interface on which IS-IS is enabled. To enable IS-IS on an interface, run the **9.6.68 isis enable** command.
Cost	Cost of IS-IS IPv4 interfaces. To set the cost of IS-IS IPv4 interfaces, run the **9.6.9 circuit-cost** or **9.6.64 isis cost** command.
Ipv6 Cost	Cost of IS-IS IPv6 interfaces. To set the cost of IS-IS IPv6 interfaces, run the **9.7.3 ipv6 circuit-cost** or **9.7.17 isis ipv6 cost** command.
State	Status of the IS-IS interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Network type of the IS-IS interface: P2P or broadcast. To set the network type of an IS-IS interface, run the **9.6.63 isis circuit-type** command.
MTU	MTU of the IS-IS interface.
Priority	Priority of the IS-IS interface. **NOTE** When the current interface is a virtual link interface, the priority field is not displayed.
Timers	IS-IS timer.
Csnp	Interval for sending CSNPs. To set the interval for sending CSNPs, run the **9.6.86 isis timer csnp** command.
Retransmit	Interval for retransmitting LSPs on a P2P link. To set the retransmit interval, run the **9.6.89 isis timer lsp-retransmit** command.
Hello	Interval for sending Hello packets. To set the interval for sending Hello packets, run the **9.6.87 isis timer hello** command.
Hello Multiplier	Number of consecutive Hello packets that are not received before the neighbor is declared Down. To set this value, run the **9.6.88 isis timer holding-multiplier** command.
LSP-Throttle Timer	Interval for sending LSPs or CSNPs and number of LSPs or CSNPs that are sent each time. To set the two values, run the **9.6.90 isis timer lsp-throttle** command.

Related Topics

9.6.56 isis
9.6.101 network-entity
9.6.91 is-level
9.6.2 area-authentication-mode
9.6.42 domain-authentication-mode
9.6.68 isis enable
9.6.9 circuit-cost
9.7.3 ipv6 circuit-cost
9.6.64 isis cost
9.7.17 isis ipv6 cost

 Copyright © Huawei Technologies Co., Ltd.

9.6.63 isis circuit-type
9.6.86 isis timer csnp
9.6.87 isis timer hello
9.6.88 isis timer holding-multiplier
9.6.89 isis timer lsp-retransmit
9.6.90 isis timer lsp-throttle

9.6.19 display isis debug-switches

Function

The **display isis debug-switches** command displays the current IS-IS debugging status.

Format

display isis debug-switches [*process-id*]

display isis [*process-id*] **debug-switches**

Parameters

Parameter	Description	Value
process-id	Displays the current status of IS-IS debugging of specified IS-IS process ID. If *process-id* is not specified, display the current status of IS-IS debugging of all IS-IS process.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no IS-IS process is enabled or IS-IS debugging is not enabled, the **display isis debug-switches** command output is empty.

Example

Display the IS-IS debugging status.

```
<Huawei> debugging isis spf-event
<Huawei> display isis debug-switches 1
ISIS-1 SPF events related debugging switch is on
```

9.6.20 display isis error

Function

The **display isis error** command displays statistics about error LSPs and Hello packets that are received by IS-IS interfaces or processes.

Format

display isis error [{ *process-id* | **vpn-instance** *vpn-instance-name* } [**interface**]]

display isis error interface *interface-type interface-number*

Parameters

Parameter	Description	Value
process-id	Displays statistics about error packets received by a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays statistics about error packets received by the IS-IS process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface	Displays statistics about error packets received on all interfaces in a specified IS-IS process or VPN instance.	-
interface-type interface-number	Displays statistics about error packets received by a specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display statistics about error LSPs received on all interfaces in IS-IS process 1.

```
<Huawei> display isis error 1

                    Statistics of error packets for ISIS(1)
                    ---------------------------------------
LSP packet errors:
Longer LSP              : 0          Smaller LSP             : 0
Mismatched Level        : 0          Invalid Sysid           : 0
Zero Sequence Number    : 0          Illegal IS Type         : 0
Zero Checksum           : 0          Incorrect Checksum      : 0
Bad Authentication      : 0          Bad Auth Count          : 0
More Protocol TLV       : 0          Bad Nbr TLV             : 0
Bad Extended IS TLV     : 0          Bad IF Addr TLV         : 0
Bad Reach TLV           : 0          Bad Inter Domain TLV    : 0
Mismatched Area Id(L1)  : 0          Bad TLV Length          : 0
Bad Alias TLV           : 0          Bad Area TLV            : 0
Bad SRLG TLV            : 0          Unknown Adjacency       : 0
Bad Protocol ID         : 0          Bad Version             : 0
Zero Lifetime           : 0          Bad Ext Reach TLV       : 0
Bad TE Router ID TLV    : 0          Bad TE Sub TLV          : 0

Hello packet errors:
Bad Packet Length       : 0          Reserved CircType       : 0
Repeated System ID      : 0          Bad Circuit Type        : 0
Longer packet           : 0          More Area Addr          : 0
Longer Area Addr        : 0          Bad Area Addr TLV       : 0
More IF Addr            : 0          Bad Formatted IF TLV    : 0
More Nbr SNPA(LAN)      : 0          Invalid Sysid           : 0
Bad TLV Length          : 0          Zero HoldingTime        : 0
Unusable IP Addr        : 0          Repeated IPv4 Addr      : 0
Mismatched Area Addr(L1): 0          Mismatched Proto        : 0
SNPA Conflicted(LAN)    : 0          Mismatched Level        : 0
Mismatched Max Area Addr: 0          Bad Authentication      : 0
More Auth TLV           : 0          3-Way Option Error(P2P) : 0
No Area Addr TLV        : 0          Bad Protocol ID         : 0
Bad Version             : 0          Invalid IPv6 Addr       : 0
More IPv6 IF Addr       : 0          Duplicate IPv6 Addr     : 0
---------------------------------------------------------------------
```

Table 9-93 Description of the display isis error command output

Item	Description
LSP packet errors	LSP errors.
Longer LSP	The LSP length is greater than the value set using the **lsp-length receive** command.
Smaller LSP	The LSP header length is smaller than the fixed length.
Mismatched Level	The level of received LSPs mismatches the local IS-IS level.
Invalid Sysid	The system ID in an LSP is invalid.
Zero Sequence Number	The sequence number of an LSP is 0.
Illegal IS Type	The IS type is invalid.
Zero Checksum	The checksum of an LSP is 0.
Incorrect Checksum	The checksum of an LSP is incorrect.
Bad Authentication	The authentication field of an LSP is incorrect.

Item	Description
Bad Auth Count	The number of authentication fields carried in an LSP is incorrect, that is, it is greater than 1.
More Protocol TLV	The number of protocol TLVs in an LSP is greater than 1.
Bad Nbr TLV	The neighbor TLV is incorrect.
Bad Extended IS TLV	The extended IS TLV is incorrect.
Bad IF Addr TLV	The interface address TLV is incorrect.
Bad Reach TLV	The reachability TLV is incorrect.
Bad Inter Domain TLV	The inter-domain TLV is incorrect. The correct TLV is 0x83.
Mismatched Area Id(L1)	Mismatched Level-1 area ID.
Bad TLV Length	The TLV length is incorrect.
Bad Alias TLV	The Alias TLV is incorrect.
Bad Area TLV	The area TLV is incorrect.
Bad SRLG TLV	The SRLG TLV is incorrect.
Unknown Adjacency	LSPs are received from unknown adjacency.
Bad Protocol ID	The protocol ID is incorrect.
Bad Version	The version is incorrect.
Zero Lifetime	The remaining lifetime of an LSP is 0.
Bad Ext Reach TLV	The Ext Reach TLV is incorrect.
Bad TE Router ID TLV	The TE Router ID TLV is incorrect.
Bad TE Sub TLV	The TE sub-TLV is incorrect.
Hello packet errors	Hello packet errors.
Bad Packet Length	The Hello packet length is incorrect.
Reserved CircType	The reserved link type is incorrect.
Repeated System ID	The system ID is repeated.
Bad Circuit Type	The link type is incorrect.
Longer packet	The Hello packet length is greater than the larger value between the interface MTU and the value set using the **lsp-length originate** command.
More Area Addr	Area addresses are superfluous.
Longer Area Addr	The area address is too long.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Bad Area Addr TLV	The area address TLV is incorrect.
More IF Addr	Interface addresses are superfluous.
Bad Formatted IF TLV	The format of the interface TLV is incorrect.
More Nbr SNPA(LAN)	Sub-network Points of Attachment (SNPAs) of a neighbor on a broadcast network are superfluous.
Invalid Sysid	The system ID length field is not 0 or 6.
Bad TLV Length	The TLV length is incorrect.
Zero HoldingTime	The neighbor holdtime is 0.
Unusable IP Addr	The IP address is on a different network segment than the peer end.
Repeated IPv4 Addr	The IPv4 address is repeated.
Mismatched Area Addr(L1)	Mismatched Level-1 area address.
Mismatched Proto	Mismatched protocol.
SNPA Conflicted(LAN)	Conflicting SNPA on a broadcast network.
Mismatched Level	The level of received Hello packets mismatches the local IS-IS level.
Mismatched Max Area Addr	The maximum area address is incorrect.
Bad Authentication	The authentication field of a Hello packet is incorrect.
More Auth TLV	Authentication TLVs are superfluous.
3-Way Option Error(P2P)	3-way information is incorrect.
No Area Addr TLV	The received Hello packet has no area address TLV.
Bad Protocol ID	The protocol ID is incorrect.
Bad Version	The version is incorrect.
Invalid IPv6 Addr	An IPv6 address is invalid.
More IPv6 IF Addr	A Hello packet carries more than 11 IPv6 addresses.
Duplicate IPv6 Addr	The IPv6 address is repeated.

 Copyright © Huawei Technologies Co., Ltd.

9.6.21 display isis graceful-restart status

Function

The **display isis graceful-restart status** command displays the IS-IS GR status.

Format

display isis *process-id* **graceful-restart status** [**level-1** | **level-2**]

display isis graceful-restart status [**level-1** | **level-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
level-1	Displays the Level-1 IS-IS GR status.	-
level-2	Displays the Level-2 IS-IS GR status.	-
process-id	Displays the IS-IS GR status of a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays the IS-IS GR status of the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the IS-IS GR status.

```
<Huawei> display isis graceful-restart status

                    Restart information for ISIS(1)
                    -------------------------------
```

```
IS-IS(1) Level-1 Restart Status
Restart Interval: 300
SA Bit Not Supported
  Total Number of Interfaces = 1
  Restart Status: RESTART COMPLETE
```

Table 9-94 Description of the display isis graceful-restart status command output

Item	Description
Restart Interval	Expected restart time of the device. This parameter is configured using the **graceful-restart interval** command.
SA Bit Supported	Whether the device supports SA.
Total Number of Interfaces = 1	Number of interfaces on which IS-IS is enabled. IS-IS is enabled using the **isis enable** command on an interface.
Restart Status:	Restart status of the current device. RESTART COMPLETE indicates that the restart is complete.

Related Topics

9.6.48 graceful-restart (IS-IS)

9.6.22 display isis interface

Function

The **display isis interface** command displays information about IS-IS interfaces.

Format

display isis interface [[**verbose** | **traffic-eng**] * | **te-tunnel**] [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **interface** [**te-tunnel** | [**traffic-eng** | **verbose**] *]

display isis interface *interface-type interface-number* [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about IS-IS interfaces.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
traffic-eng	Displays Traffic Engineering information of IS-IS.	-
te-tunnel	Displays information on the MPLS TE tunnel of IS-IS.	-
vpn-instance *vpn-instance-name*	Display IS-IS interface information in the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IS-IS interface information, including the interface name, IP address, link status of the interface. If **verbose** is specified, the command output also includes the configuration of IS-IS parameters for the interface, such as the CSNP broadcast interval, Hello packet broadcast interval, and number of IS-IS Hello packets that fail to be received before IS-IS declares the neighbor Down.

Example

Display information about IS-IS interfaces.

```
<Huawei> display isis interface

                    Interface information for ISIS(1)
                    ---------------------------------
 Interface       Id      IPV4.State          IPV6.State      MTU  Type  DIS
 GE1/0/0         001        Up                  Down         1497 L1/L2 No/No
```

Display detailed information about IS-IS interfaces.

```
<Huawei> display isis interface verbose

                    Interface information for ISIS(1)
                    ---------------------------------
 Interface                 Id      IPV4.State          IPV6.State      MTU  Type  DIS
 GE1/0/0                   001        Up                  Down         1497 L1/L2 No/No
   Circuit MT State                     : Standard
   Description                         : HUAWEI,AR Series, GE1/0/0 Interface
   SNPA Address                         : 00e0-fc01-0004
   IP Address                          : 10.1.1.1
```

```
 IPV6 Link Local Address              :
 IPV6 Global Address(es)              :
 Csnp Timer Value                    :  L1    10  L2    10
 Hello Timer Value                   :  L1    10  L2    10
 DIS Hello Timer Value                :  L1     3  L2     3
 Hello Multiplier Value              :  L1     3  L2     3
 LSP-Throttle Timer                  :  L12   50
 Cost                            :  L1    10  L2    10
 Ipv6 Cost                        :  L1    10  L2    10
 Priority                        :  L1    64  L2    64
 Retransmit Timer Value              :  L12    5
 Bandwidth-Value                     :  Low 100000000  High         0
 Static Bfd                       :  NO
 Dynamic Bfd                         :  NO
 Fast-Sense Rpr                      :  NO
```

Display detailed information about IS-IS P2P interfaces.

```
<Huawei> display isis interface verbose

                    Interface information for ISIS(1)
                    ---------------------------------
Interface       Id      IPV4.State            MTU  Type  DIS
S1/0/0          001     Mtu:Up/Lnk:Dn/IP:Dn   1500 L1/L2 --
 Circuit Parameters          :p2p
 Description                 : HUAWEI, AR Series, Serial1/0/0 Interface
 SNPA Address                : 0000-0000-0000
 IP Address                  : 10.1.2.1
 IPV6 Link Local Address     :
 IPV6 Global Address(es)     :
 Csnp Timer Value            :  L12   10
 Hello Timer Value           :        10
 DIS Hello Timer Value       :
 Hello Multiplier Value      :         3
 Cost                        :  L1    10  L2    10
 Ipv6 Cost                   :  L1    10  L2    10
 Retransmit Timer Value      :  L12    5
 LSP-Throttle Timer          :  L12   50
 Bandwidth-Value             :  Low      64000  High         0
 Static Bfd                  :  NO
 Dynamic Bfd                 :  NO
 Fast-Sense Rpr              :  NO
 Extended-Circuit-Id Value   :  0000000001
```

Table 9-95 Description of the display isis interface command output

Item	Description
Interface	IS-IS interface type and number.
Id	Link ID.
IPV4.State	IPv4 link status.
IPV6.State	IPv6 link status.
MTU	Interface MTU. An IS-IS neighbor relationship can be established only when two interfaces on both ends of a link have the same MTU. **NOTE** To enable the IS-IS interface, the MTU value needs to be more than 1500 bytes.

Item	Description
Type	Interface type: ● L1: Level-1 interface ● L2: Level-2 interface ● L1/L2: Level-1-2 interface
DIS	Whether the interface is a Designated Intermediate System (DIS): ● No/No: the interface is not DIS neither in Level-1 nor in Level-2 area. ● Yes/Yes: the interface is DIS in Level-1 and Level-2 area. ● Yes/No: the interface is DIS in Level-1 area. ● No/Yes: the interface is DIS in Level-2 area. ● --: the interface is of the P2P type, and it cannot function as the DIS.
Circuit MT State	Topology status on the interface: ● Standard: – IPv4 is enabled on the interface, but IPv6 is not. – IPv6 is enabled on the interface, but IPv4 is not. In addition, the topology type is standard. – Both IPv4 and IPv6 are enabled on the interface. In addition, the topology type is standard. ● IPv6: IPv6 is enabled on the interface, but IPv4 is not. In addition, the topology type is IPv6. ● Standard IPv6: – IPv6 is enabled on the interface, but IPv4 is not. In addition, the topology type is compatible. – Both IPv4 and IPv6 are enabled on the interface. In addition, the topology type is compatible or IPv6. To configure the IPv6 topology type, run the **ipv6 enable** command in the IS-IS view.
Description	Description of the interface.
SNPA Address	MAC address.
IP Address	IPv4 address of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPV6 Link Local Address	IPv6 link-local address.
IPV6 Global Address(es)	IPv6 global address.
Csnp Timer Value	Interval for sending CSNPs. To set the interval for sending CSNPs, run the **9.6.86 isis timer csnp** command.
Hello Timer Value	Interval for sending Hello packets. To set the interval for sending Hello packets, run the **9.6.87 isis timer hello** command.
DIS Hello Timer Value	Interval at which the DIS sends Hello packets. This field value is displayed only when the local device is the DIS. It is the same as the Hello Timer Value.
Hello Multiplier Value	Number of consecutive Hello packets that are not received before the neighbor is declared Down. To set this value, run the **9.6.88 isis timer holding-multiplier** command.
LSP-Throttle Timer	Interval for sending LSPs or CSNPs and number of LSPs or CSNPs that are sent each time. To set the two values, run the **9.6.90 isis timer lsp-throttle** command.
Cost	Cost of an IPv4 interface. This field value affects route selection.
Ipv6 Cost	Cost of an IPv6 interface. This field value affects route selection in IPv6 topologies.
Priority	Priority for DIS election. To set the priority for DIS election, run the **9.6.67 isis dis-priority** command.
Retransmit Timer Value	Interval for retransmitting LSPs on a P2P link. To set the retransmit interval, run the **9.6.89 isis timer lsp-retransmit** command.
Bandwidth-Value	Physical bandwidth of an interface. The value can be calculated using the following formula: **Bandwidth-Value** = 4294967296 x **high** + **low**. For example, if the value of **high** is 1 and the value of **low** is 705032704, Bandwidth-Value = 1 x 4294967296 + 705032704 = 5000000000. • low: low bandwidth with the maximum value of 4294967295 • high: high bandwidth with the maximum value of 4294967295

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Static Bfd	Status BFD status: ● NO: Static BFD is not enabled. ● YES: Static BFD is enabled. To enable BFD on an interface, run the **9.6.61 isis bfd static** command.
Dynamic Bfd	Dynamic BFD status: ● NO: Dynamic BFD is not enabled. ● YES: Dynamic BFD is enabled. To enable dynamic BFD on an interface, run the **9.6.8 bfd all-interfaces enable** or **9.6.60 isis bfd enable** command.
Fast-Sense Rpr	Whether the fast sense RPR function is enabled.
Extended-Circuit-Id Value	Link ID of an interface.

Related Topics

9.6.86 isis timer csnp
9.6.67 isis dis-priority
9.6.87 isis timer hello
9.6.88 isis timer holding-multiplier
9.6.89 isis timer lsp-retransmit
9.6.90 isis timer lsp-throttle
9.6.61 isis bfd static
9.6.8 bfd all-interfaces enable
9.6.60 isis bfd enable

9.6.23 display isis last-peer-change

Function

The **display isis last-peer-change** command displays changes in IS-IS neighbor relationships.

Format

display isis *process-id* **last-peer-change**

display isis last-peer-change [*process-id* | **vpn-instance** *vpn-instance-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display isis last-peer-change** command to view a maximum of 100 latest records in each IS-IS process.

Example

Display changes in IS-IS neighbor relationships.

```
<Huawei> display isis last-peer-change
                    Peer change information for ISIS(1)
                    -----------------------------------

Time      : 2011-03-28 09:30:34
System Id : 0000.0000.0002
Type      : L1 LAN
Interface : GE1/0/0
State     : IPv4 -> IPv4/IPv6
Details   : Protocol change
```

Table 9-96 Description of the display isis last-peer-change command output

Item	Description
Time	Time a neighbor relationship changes.
System Id	System ID of a neighbor.
Type	Neighbor type: ● L1 LAN ● L2 LAN ● P2P
Interface	Interface connected to the neighbor.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Changes in the IS-IS neighbor relationship status: ● Init -> Up ● Up -> Down ● Up -> Init ● Down -> Up ● IPv4/IPv6 -> IPv4 ● IPv4/IPv6 -> IPv6 ● IPv4 -> IPv4/IPv6 ● IPv6 -> IPv4/IPv6 ● IPv4 -> IPv6 ● IPv6 -> IPv4 ● L12 -> L2 ● L2 -> L12
Details	Causes for IS-IS neighbor relationship changes: ● Circuit down ● BFD down ● Hold timer expired ● New adjacency created ● Clear neighbor ● Multiple P2P adjacency ● Adjacency usage mismatch ● Internal error ● Memory low ● P2P circuit ID conflict ● Area mismatch ● Three way down ● Three way init ● Three way up ● Protocol change ● Mt usage mismatch ● Peer state change ● Peer level change

 Copyright © Huawei Technologies Co., Ltd.

9.6.24 display isis lsdb

Function

The **display isis lsdb** command displays information about IS-IS LSDBs.

Format

display isis *process-id* **lsdb** [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] *

display isis lsdb [{ **level-1** | **level-2** } | **verbose** | { **local** | *lsp-id* | **is-name** *symbolic-name* }] * [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
level-1	Displays Level-1 LSDBs. If no level is specified, Level-1 and Level-2 LSDBs are displayed.	-
level-2	Displays Level-2 LSDBs. If no level is specified, Level-1 and Level-2 LSDBs are displayed.	-
verbose	Displays detailed information about IS-IS LSDBs.	-
local	Displays information about the local LSDB.	-
lsp-id	Specifies an LSP ID.	The value is in dotted decimal notation. The value ranges from 16 to 20 in ####.####.####.##-## format, such as 0050.0500.5004.00-00.
is-name *symbolic-name*	Specifies the dynamic host name in is-name or is-name.##-## format. ##-## indicates the pseudonode ID-LSP fragment ID.	If the value is in is-name format, the value is a string of 1 to 64 characters. If the value is in is-name.##-##, the value is a string of 1 to 70 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the LSDB of the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display IS-IS LSDB information.

```
<Huawei> display isis lsdb
                    Database information for ISIS(1)
                    --------------------------------
                      Level-2 Link State Database
LSPID               Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x0000017a   0xa21c        846           84      0/0/0
2222.2222.2222.00-00* 0x000001ce   0xbdcc        845          111      0/0/0
3333.3333.3333.00-00  0x00000013   0x8847        1004          84      0/0/0
3333.3333.3333.01-00  0x0000000b   0x95bc        1004          55      0/0/0
Total LSP(s): 4
   *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
         ATT-Attached, P-Partition, OL-Overload
```

Table 9-97 Description of the display isis lsdb command output

Item	Description
LSPID	LSP ID.
Seq Num	LSP sequence number.
Checksum	LSP checksum.
Holdtime	LSP holdtime.
Length	LSP length.
ATT/P/OL	• ATT: Attach bit • P: partition bit • OL: overload bit
Total LSP(s)	Number of LSPs.

Item	Description
*/+	• *(In TLV): Leaking route. • *(By LSPID): Locally generated LSP. • +: Locally generated extended LSP.

Display detailed information about IS-IS LSDB.

```
<Huawei> display isis lsdb verbose

                    Database information for ISIS(1)
                    --------------------------------

                     Level-1 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0001.00-00  0x00000010   0xc776        0 (724)       36      0/0/0
 SOURCE       0000.0000.0001.00
 NLPID        IPV4
 AREA ADDR    10
 INTF ADDR    10.22.21.1
 NBR  ID      0000.0000.0002.02  COST: 10
 IP-Internal  10.22.21.0       255.255.255.0    COST: 10

0000.0000.0003.00-00* 0x00000026   0x6fb4        1145          350     0/0/0
 SOURCE       0000.0000.0003.00
 HOST NAME    RouterA
 NLPID        IPV4
 NLPID        IPV6
 AREA ADDR    10
 INTF ADDR    10.1.1.2
 INTF ADDR    10.1.2.2
 INTF ADDR V6 FC00:1::1
 Topology     Standard
 NBR  ID      0000.0000.0001.00  COST: 10
+NBR  ID      0000.0000.0001.00  COST: 10
 IP-Internal  10.1.1.0       255.255.255.0    COST: 10
 IP-Internal  10.1.2.0       255.255.255.0    COST: 10
+IP-Extended  10.1.1.0       255.255.255.0    COST: 10
+IP-Extended  10.1.2.0       255.255.255.0    COST: 10
 IPV6         FC00:1::/64                     COST: 10
Total LSP(s): 2
   *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
         ATT-Attached, P-Partition, OL-Overload


                     Level-2 Link State Database

LSPID                 Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
0000.0000.0003.00-00* 0x0000001c   0x9b0d        1131          233     0/0/0
 SOURCE       RouterA.00 ORG ID: RouterA.00 ORG ID: 0000.0000.0003.00
 HOST NAME    RouterA
 NLPID        IPV4
 NLPID        IPV6
 AREA ADDR    10
 INTF ADDR    10.1.1.2
 INTF ADDR    10.1.2.2
 INTF ADDR V6 FC00:1::1
 Topology     Standard
 NBR  ID      0000.0000.0004.00  COST: 10
+NBR  ID      0000.0000.0004.00  COST: 10
+MT NBR ID    0000.0000.0004.00  COST: 10
 IP-Internal  10.1.1.0       255.255.255.0    COST: 10
```

```
 IP-Internal  10.1.2.0       255.255.255.0    COST: 10
+IP-Extended  10.1.1.0       255.255.255.0    COST: 10
+IP-Extended  10.1.2.0       255.255.255.0    COST: 10
 IPV6         FC00:1::/64                     COST: 10

0000.0000.0003.00-01* 0x00000005   0x5ec1        1129          70      0/0/0
 SOURCE        RouterA.00
Auth: *****     Len: --     Type: MD5
 IP-External  10.1.3.0       255.255.255.0    COST: 0
+IP-Extended  10.1.3.0       255.255.255.0    COST: 0
Total LSP(s): 2
   *(In TLV)-Leaking Route, *(By LSPID)-Self LSP, +-Self LSP(Extended),
         ATT-Attached, P-Partition, OL-Overload
```

Table 9-98 Description of the display isis lsdb verbose command output

Item	Description
SOURCE	System ID of the source node.
ORG ID	Source system ID of the virtual system.
HOST NAME	Dynamic host name.
Auth	Authentication password.
Len	Authentication password length.
Type	Authentication type: ● Plain Text: indicates that the password is sent in plain text. ● MD5: indicates that the password is encrypted using the MD5 algorithm. ● CRYPTO_AUTH: The password is encrypted with the HMAC-SHA256 encryption algorithm.
NLPID	Supported network protocol. ● IPV4: supported the IPv4 network protocol. ● IPV6: supported the IPv6 network protocol.
AREA ADDR	Area address.
INTF ADDR	Interface address.
INTF ADDR V6	Interface IPv6 address.
Topology	Topology type.
NBR ID	System ID of a neighbor.
+NBR ID	System ID of a neighbor, which can carry TE information.
+MT NBR ID	Neighbor ID in the MT topology.
COST	Route cost.
IP-Internal	Internal IPv4 routing information.

Item	Description
IP-External	External IPv4 routing information.
+IP-Extended	Extended IP routing information, which can carry TE information.
IPV6	Internal IPv6 routing information.

9.6.25 display isis migp-routing

Function

The **display isis migp-routing** command displays IS-IS Multicast IGP (MIGP) routing information.

Format

display isis [*process-id*] **migp-routing** [*ip-address* [*mask* | *mask-length*] | { **level-1** | **level-2** } | **verbose**] *

Parameters

Parameter	Description	Value
process-id	Specifies the IS-IS process ID.	The value is an integer ranging from 1 to 65535.
ip-address	Displays the route with the specified destination address.	It is in dotted decimal notation.
mask	Specifies the mask of the ip address.	It is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
level-1	Displays IS-IS Level-1 routes.	-
level-2	Displays IS-IS Level-2 routes.	-
verbose	Displays the administrative tag of the route.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display isis migp-routing** command to view the physical interface of the route with the outgoing interface as a TE tunnel interface.

Example

Display IS-IS MIGP routing information.

```
<Huawei> display isis migp-routing

                    MIGP Route information for ISIS(1)
                    ----------------------------------

                     ISIS(1) Level-2 Forwarding Table
                     --------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
-------------------------------------------------------------------------------
 192.168.3.0/24       40         NULL    Vlanif10        10.0.1.1        A/-
 10.5.5.5/32          30         NULL    Vlanif10        10.0.1.1        A/-
 10.4.4.4/32          20         NULL    Vlanif10        10.0.1.1        A/-
 10.0.2.0/24          20         NULL    Vlanif10        10.0.1.1        A/-
 10.0.3.0/24          30         NULL    Vlanif10        10.0.1.1        A/-
          Flags: A-Added to MIGP, U-Up/Down Bit Set
```

Table 9-99 Description of the **display isis migp-routing** command output

Item	Description
IPV4 Destination	Indicates the IPv4 destination address and the mask.
IntCost	Indicates the internal cost.
ExtCost	Indicates the external cost.
ExitInterface	Indicates the outgoing interface of the IS-IS route.
NextHop	Indicates the next hop of the IS-IS route.
Flags ● A-Added to MIGP ● U-Up/Down Bit Set	Indicates routing information flags: ● A-Added to MIGP: indicates that a route is added to the MIGP table. ● U-Up/Down Bit Set-Up/Down Bit Set: indicates the Up/Down bit.

```
<Huawei> display isis migp-routing verbose

                    MIGP Route information for ISIS(1)
                    ----------------------------------

                     ISIS(1) Level-2 Forwarding Table
                     --------------------------------

 IPV4 Dest  : 192.168.3.0/24     Int. Cost : 40            Ext. Cost : NULL
 Admin Tag  : -                  Src Count : 1             Flag      : A/-
```

```
Priority   : Low
NextHop    :                Interface :              ExitIndex :
  10.0.1.1                     Vlanif10                0x00000009

IPV4 Dest  : 10.5.5.5/32       Int. Cost : 30           Ext. Cost : NULL
Admin Tag  : -               Src Count : 1            Flag      : A/-

Priority   : Low
NextHop    :                Interface :              ExitIndex :
  10.0.1.1                     Vlanif10                0x00000009

IPV4 Dest  : 10.4.4.4/32       Int. Cost : 20           Ext. Cost : NULL
Admin Tag  : -               Src Count : 1            Flag      : A/-

Priority   : Low
NextHop    :                Interface :              ExitIndex :
  10.0.1.1                     Vlanif10                0x00000009

IPV4 Dest  : 10.0.2.0/24       Int. Cost : 20           Ext. Cost : NULL
Admin Tag  : -               Src Count : 1            Flag      : A/-

Priority   : Low
NextHop    :                Interface :              ExitIndex :
  10.0.1.1                     Vlanif10                0x00000009

IPV4 Dest  : 10.0.3.0/24       Int. Cost : 30           Ext. Cost : NULL
Admin Tag  : -               Src Count : 1            Flag      : A/-

Priority   : Low
NextHop    :                Interface :              ExitIndex :
  10.0.1.1                     Vlanif10                0x00000009

        Flags: A-Added to MIGP, U-Up/Down Bit Set
```

Table 9-100 Description of the **display isis migp-routing verbose** command output

Item	Description
IPV4 Dest	Indicates the IPv4 destination address and the mask.
Int.Cost	Indicates the internal cost.
Ext.Cost	Indicates the external cost.
Admin Tag	Indicates the administrative tag of the IS-IS route.
Src Count	Indicates the number of source addresses to the same destination.
Flags ● A-Added to MIGP ● U-Up/Down Bit Set	Indicates the routing information flags. ● A-Added to MIGP: indicates that a route is added to the MIGP table. ● U-Up/Down Bit Set: indicates the Up/Down bit.

Item	Description
Priority	Convergence priorities of IS-IS routes ● Critical ● High ● Medium ● Low
NextHop	Indicates the next hop of the route.
Interface	Indicates the outgoing interface of the IS-IS route.
ExitIndex	Indicates the index value of the outgoing interface.

9.6.26 display isis mesh-group

Function

The **display isis mesh-group** command displays the configuration of the IS-IS mesh-group.

Format

display isis mesh-group [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **mesh-group**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Add GE1/0/0 GE2/0/0 that run IS-IS to mesh-group 100.

```
<Router> system view
[Router] interface gigabitethernet 1/0/0
[Router-GigabitEthernet1/0/0] isis mesh-group 100
[Router-GigabitEthernet1/0/0] quit
[Router] interface gigabitethernet 2/0/0
[Router-GigabitEthernet2/0/0] isis mesh-group 100
```

Display information about the configured IS-IS mesh-group.

```
<Router> display isis mesh-group
            Mesh Group information for ISIS(1)
-----------------------------------------------------------------
Interface          Status
GE1/0/0             100
GE2/0/0             100
```

Table 9-101 Description of the display isis mesh group command output

Item	Description
Interface	Type and number of the interface in the mesh group.
Status	Mesh-group number.

Related Topics

9.6.71 isis mesh-group

9.6.27 display isis name-table

Function

The **display isis name-table** command displays the mapping between the local or remote IS-IS device and the system ID.

Format

display isis name-table [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **name-table**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Configure a name for the local IS-IS system.

```
[Router] isis
[Router-isis-1] is-name RUTA
```

Configure a static name mapping for the remote IS-IS system (0000.0000.0041).

```
[Router-isis-1] is-name map 0000.0000.0041 RUTB
```

Display the IS-IS system name table.

```
<Router> display isis name-table
          Name table information for ISIS(1)
System ID          Hostname      Type
-----------------------------------------------------------
6789.0000.0001       RUTA        DYNAMIC
0000.0000.0041       RUTB        STATIC
```

Table 9-102 Description of the display isis name-table command output

Item	Description
System ID	System ID of the current IS-IS device. To set the system ID, run the **9.6.101 network-entity** command.
Hostname	Host name of the device. To set a host name for the local or remote device, run the **9.6.92 is-name** or **9.6.93 is-name map** command.

Item	Description
Type	Type of the mapping between the host name and system ID: static or dynamic.

Related Topics

9.6.92 is-name

9.6.93 is-name map

9.6.101 network-entity

9.6.28 display isis peer

Function

The **display isis peer** command displays IS-IS neighbor information.

Format

display isis *process-id* **peer** [**verbose**]

display isis peer [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis peer interface *interface-type interface-number* [**verbose**]

Parameters

Parameter	Description	Value
verbose	Displays detailed IS-IS neighbor information, including the area address, period during which the neighbor remains Up, and IP address of its directly connected interface.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an IS-IS area, if you need to check whether two devices can communicate properly, run the **display isis peer** command to view information about the neighbor, including the neighbor status, period during which the neighbor remains Up, and neighbor type.

Example

Display information about IS-IS neighbors.

```
<Huawei> display isis peer
                    Peer information for ISIS(1)

 System Id     Interface         Circuit Id       State HoldTime Type     PRI
-------------------------------------------------------------------------------
0000.0000.0001   GE1/0/0         0000.0000.0001.01   Up    24s   L1(L1L2)  64
0000.0000.0001   GE1/0/0         0000.0000.0001.01   Up    24s   L2(L1L2)  64

Total Peer(s): 2
```

Table 9-103 Description of the display isis peer command output

Item	Description
System Id	System ID of the neighbor.
Interface	Type and number of the interface.
Circuit Id	Circuit ID.
State	Neighbor status: ● Up: indicates that the neighbor is Up and the two ends can communicate. ● Init: indicates that the local end can receive packets from the remote end but the remote end cannot receive packets from the local end. This status is displayed when authentication is configured on the remote end. ● Down: indicates that the neighbor is Down. This is the initial status, indicating that no message is received from the neighbor. In most cases, this status is not displayed.
HoldTime	Neighbor holdtime.

Item	Description
Type	Neighbor type: ● L1: indicates that the neighbor type is Level-1 and interfaces on both ends are Level-1 interfaces. ● L2: indicates that the neighbor type is Level-2 and interfaces on both ends are Level-2 interfaces. ● L1(L1L2): indicates that the neighbor type is Level-1 and interfaces on both ends are Level-1-2 interfaces. ● L2(L1L2): indicates that the neighbor type is Level-2 and interfaces on both ends are Level-1-2 interfaces.
PRI	Priority of the neighbor in DIS election.

Display detailed information about IS-IS neighbor.

```
<Huawei> display isis peer verbose
                    Peer information for ISIS(1)

  System Id     Interface          Circuit Id         State  HoldTime   Type     PRI
-------------------------------------------------------------------------------
0000.0000.0001  GE1/0/0           0000.0000.0001.01      Up     26s     L1(L1L2)   64
  MT IDs supported     : 0(UP)
  Local MT IDs         : 0
  Area Address(es)     : 10
  Peer IP Address(es)  : 10.10.10.1
  Peer IPv6 Address(es): FE80::82FB:6FF:FE35:45B6
  Uptime               : 00:00:19
  Adj Protocol         : IPV4  IPV6
  Restart Capable      : YES
  Suppressed Adj       : NO
  Peer System Id       : 0000.0000.0001

0000.0000.0001  GE1/0/0           0000.0000.0001.01      Up     27s     L2(L1L2)   64
  MT IDs supported     : 0(UP)
  Local MT IDs         : 0
  Area Address(es)     : 10
  Peer IP Address(es)  : 10.10.10.1
  Peer IPv6 Address(es): FE80::82FB:6FF:FE35:45B6
  Uptime               : 00:00:19
  Adj Protocol         : IPV4  IPV6
  Restart Capable      : YES
  Suppressed Adj       : NO
  Peer System Id       : 0000.0000.0001


Total Peer(s): 2
```

Table 9-104 Description of the display isis peer verbose command output

Item	Description
MT IDs supported	IDs of topology instances supported by the remote interface.
Local MT IDs	IDs of topology instances supported by the local interface.
Area Address(es)	Area addresses of the neighbor.
Peer IP Address(es)	IP address of the remote interface.
Peer IPv6 Address(es)	IPv6 address of the remote interface.
Uptime	Period during which the neighbor remains Up.
Adj Protocol	Protocol used for establishing the adjacency.
Restart Capable	Whether GR is supported: ● YES: indicates that GR is supported. ● NO: indicates that GR is not supported.
Suppressed Adj	Whether neighbor suppression is supported: ● YES: indicates that neighbor suppression is supported. ● NO: indicates that neighbor suppression is not supported.
Peer System Id	The System ID of IS-IS peer
Total Peer(s)	Number of neighbors.

9.6.29 display isis purge packet

Function

The **display isis purge packet** command displays statistics about received IS-IS purge LSPs carrying the POI TLV.

Format

display isis *process-id* **purge packet** [*packet-number*]

display isis purge packet *process-id* [*packet-number*]

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer ranging from 1 to 65535.
packet-number	Specifies the number of purge LSPs whose statistics are to be displayed.	The value is an integer ranging from 1 to 20.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check statistics about received IS-IS purge LSPs carrying the POI TLV, run the **display isis purge packet** command. You can specify *packet-number* in the command to check statistics about a specified number of purge LSPs, and the maximum value of *packet-number* is 20. If its value is set to 20:

- The first two displayed purge LSPs are sent by the local source system, with fragment number 0, one of which is Level-1, and the other is Level-2.
- The first 10 displayed purge LSPs are generated locally, and the next 10 purge LSPs are from neighbors. The purge LSPs are displayed in reverse order of the time when they were received. If the LSP ID is followed by an asterisk (*), the purge LSP is generated locally.

Example

Display statistics about received IS-IS purge LSPs carrying the POI TLV.

```
<Huawei> display isis purge packet 1 10

                Purge LSP packet for ISIS(1)
-------------------------------------------------------------
Packet information(Index 1):
-----------------------------------------------------
Received LSPID      :  0000.0000.0027.00-00*
Source Interface    :  Vlanif100
Time                :  2015-1-22 13:55:06
Level               :  Level-2
PDU Type            :  20(Level-2 LSP)
PDU Length          :  55
Sequence Number     :  0x00000015
Checksum            :  0xc891
POI NAME            :  0000.0000.0004
POI NAME(Neighbor)  :  0000.0000.0005
HOST NAME           :  RT4-Pro1
Auth Type           :  **
0010: 83 1b 01 06 12 01 00 03 00 43 00 00 00 00 00 00
0020: 00 27 00 00 00 01 6a 6c bd ed 01 0d 07 01 00 00
0030: 00 00 00 01 89 0a 52 54 31 2d 50 72 6f 2d 30 31
0040: ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **
```

```
0050: ** ** **
-----------------------------------------------------
   **-Authentication TLV, *(By LSPID)-Self LSP
```

Table 9-105 Description of the **display isis purge packet** command output

Item	Description
Received LSPID	ID of a received purge LSP
Source Interface	Source interface of a received purge LSP
Time	Time when a purge LSP was received
Level	Level of a received purge LSP
PDU Type	Type of received purge LSP
PDU Length	Length of a received purge LSP
Sequence Number	Sequence number (LSN) of a received purge LSP
Checksum	Checksum of a received purge LSP
POI NAME	POI TLV carried in a received purge LSP
POI NAME(Neighbor)	Neighbor system ID in the POI TLV carried in a received purge LSP
HOST NAME	Dynamic hostname carried in a received purge LSP
Auth Type	Authentication information carried in a received purge LSP

9.6.30 display isis route

Function

The **display isis route** command displays IS-IS routing information.

Format

display isis route [*process-id* | **vpn-instance** *vpn-instance-name*] [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]] *

display isis route [*process-id* | **vpn-instance** *vpn-instance-name*] **ipv6** [**verbose** | [**level-1** | **level-2**] | *ipv6-address* [*prefix-length*]] *

display isis *process-id* **route** [**ipv4**] [**verbose** | [**level-1** | **level-2**] | *ip-address* [*mask* | *mask-length*]] *

display isis *process-id* **route ipv6** [**verbose** | [**level-1** | **level-2**] | *ipv6-address* [*prefix-length*]] *

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4	Displays IPv4 routes. If this parameter is not specified, both IPv4 and IPv6 IS-IS routes are displayed.	-
verbose	Displays detailed routing information.	-
level-1	Displays Level-1 IS-IS routes.	-
level-2	Displays Level-2 IS-IS routes.	-
ip-address	Displays the routes with the specified IPv4 destination address.	The value is in dotted decimal notation.
mask	Specifies the mask of an IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of an IP address.	The value is an integer that ranges from 0 or 32.
ipv6	Displays IPv6 routes. If this parameter is not specified, both IPv4 and IPv6 IS-IS routes are displayed.	-
ipv6-address	Displays the routes with the specified IPv6 destination address.	The value is a 32-digit hexadecimal number, in X:X:X:X:X:X:X:X format.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 0 to 128.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display all IS-IS routes.

```
<Huawei> display isis route

                    Route information for ISIS(1)
                    -----------------------------

                   ISIS(1) Level-1 Forwarding Table
                   --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
10.2.1.0/24          10         NULL    GE0/0/2         Direct          D/-/L/-
172.18.0.0/16        20         NULL    GE0/0/2         10.2.1.1        A/-/L/-

 IPV6 Dest.      ExitInterface   NextHop                     Cost       Flags
--------------------------------------------------------------------------------
 FC00:200::/64   GE0/0/2         Direct                      10         D/L/-

    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                         U-Up/Down Bit Set


                   ISIS(1) Level-2 Forwarding Table
                   --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
10.2.1.0/24          10         NULL    GE0/0/2         Direct          D/-/L/-
172.18.0.0/16        20         NULL

 IPV6 Dest.      ExitInterface   NextHop                     Cost       Flags
--------------------------------------------------------------------------------
 100:200::/64    GE0/0/2         Direct                      10         D/L/-

    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                         U-Up/Down Bit Set
```

Table 9-106 Description of the display isis route command output

Item	Description
IPV4 Destination	IPv4 destination address and mask.
IPV6 Dest.	IPv6 destination address and mask.
IntCost	IPv4 internal cost or IS-IS route cost. To change the IS-IS IPv4 route cost, run the **9.6.9 circuit-cost** or **9.6.64 isis cost** command to set the link cost of an IS-IS IPv4 interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ExtCost	IPv4 external cost or cost of routes imported from other routing protocols. To set the cost of imported routes, run the **9.6.53 import-route (IS-IS)** command. **NOTE** The costs of external routes imported using the **import-route cost-type external** command are displayed in this field to differentiate the costs of IS-IS routes.
Cost	IPv6 route cost. To change the IS-IS IPv6 route cost, run the **9.7.3 ipv6 circuit-cost** or **9.7.17 isis ipv6 cost** command to set the link cost of an IS-IS IPv6 interface.
ExitInterface	Outbound interface of a route.
NextHop	Next hop address of a route. This field displays Direct if the destination network segment is the direct network segment.
Flags	Route flag: ● D-Direct: indicates a direct route. ● A-Added to URT: indicates that a route is added to the unicast routing table. ● L-Advertised in LSPs: indicates that a route is advertised through an LSP. ● S-IGP Shortcut: indicates that the interface on which IGP-Shortcut is enabled exists on the path to the destination. ● U-Up/Down Bit Set: indicates the Up/Down bit.

Display IS-IS IPv4 routes.

```
<Huawei> display isis route ipv4

                    Route information for ISIS(1)
                    -----------------------------

                   ISIS(1) Level-1 Forwarding Table
                   --------------------------------

IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
10.1.1.0/24          10         NULL    Loop1           Direct          D/-/L/-
10.2.2.0/24          10         NULL    Loop2           Direct          D/-/L/-
    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                         U-Up/Down Bit Set


                   ISIS(1) Level-2 Forwarding Table
                   --------------------------------
```

```
IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
10.1.1.0/24          10         NULL    Loop1           Direct          D/-/L/-
10.2.2.0/24          10         NULL    Loop2           Direct          D/-/L/-
    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                         U-Up/Down Bit Set
```

Display IS-IS IPv6 routes.

```
<Huawei> display isis route ipv6

                     Route information for ISIS(1)
                     -----------------------------

                    ISIS(1) Level-1 Forwarding Table
                    --------------------------------

 IPV6 Dest.          ExitInterface   NextHop                    Cost       Flags
--------------------------------------------------------------------------------
 FC00:0:0:200::/64    GE0/0/2         Direct                     10         D/L/-

    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                         U-Up/Down Bit Set


                    ISIS(1) Level-2 Forwarding Table
                    --------------------------------

 IPV6 Dest.          ExitInterface   NextHop                    Cost       Flags
--------------------------------------------------------------------------------
 FC00:0:0:200::/64    GE0/0/2         Direct                     10         D/L/-


    Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                         U-Up/Down Bit Set
```

Display detailed IS-IS routing information.

```
<Huawei> display isis route verbose

                     Route information for ISIS(1)
                     -----------------------------

                    ISIS(1) Level-1 Forwarding Table
                    --------------------------------

 IPV4 Dest  : 10.0.0.0/24        Int. Cost : 10           Ext. Cost : NULL
 Admin Tag  : -                  Src Count : 2            Flags     : D/-/L/-
 Priority   : -
 NextHop    :                    Interface :              ExitIndex :
   Direct                           GE1/0/0                  0x00000000

 IPV4 Dest  : 10.2.0.0/24        Int. Cost : 10           Ext. Cost : NULL
 Admin Tag  : -                  Src Count : 2            Flags     : D/-/L/-
 Priority   : -
 NextHop    :                    Interface :              ExitIndex :
   Direct                           GE2/0/0                  0x00000000

 IPV4 Dest  : 10.3.0.0/24        Int. Cost : 20           Ext. Cost : NULL
 Admin Tag  : -                  Src Count : 2            Flags     : A/-/L/-
 Priority   : Low
 NextHop    :                    Interface :              ExitIndex :
   10.2.0.2                         GE2/0/0                  0x00000003
   10.0.0.2                         GE1/0/0                  0x00000005

 IPV4 Dest  : 10.1.1.1/32        Int. Cost : 10           Ext. Cost : NULL
 Admin Tag  : -                  Src Count : 1            Flags     : A/-/L/-
 Priority   : Medium
```

```
NextHop    :                Interface :            ExitIndex :
  10.0.0.2                     GE1/0/0                0x00000005
(B)10.2.0.2                     GE2/0/0                0x00000003

   Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                        U-Up/Down Bit Set


                  ISIS(1) Level-2 Forwarding Table
                  --------------------------------

IPV4 Dest  : 10.0.0.0/24       Int. Cost : 10          Ext. Cost : NULL
Admin Tag  : -                 Src Count : 3           Flags     : D/-/L/-
Priority   : -
NextHop    :                Interface :            ExitIndex :
  Direct                       GE1/0/0                0x00000000

IPV4 Dest  : 10.2.0.0/24       Int. Cost : 10          Ext. Cost : NULL
Admin Tag  : -                 Src Count : 3           Flags     : D/-/L/-
Priority   : -
NextHop    :                Interface :            ExitIndex :
  Direct                       GE2/0/0                0x00000000

IPV4 Dest  : 10.3.0.0/24       Int. Cost : 20          Ext. Cost : NULL
Admin Tag  : -                 Src Count : 2           Flags     : -/-/-/-
Priority   : Low

IPV4 Dest  : 10.1.1.1/32       Int. Cost : 10          Ext. Cost : NULL
Admin Tag  : -                 Src Count : 2           Flags     : -/-/-/-
Priority   : Medium

   Flags: D-Direct, A-Added to URT, L-Advertised in LSPs, S-IGP Shortcut,
                        U-Up/Down Bit Set
```

Table 9-107 Description of the display isis route verbose command output

Item	Description
IPV4 Dest	IPv4 destination address and mask.
Int.Cost	IPv4 internal cost, the cost of an IS-IS route.
Ext.Cost	IPv4 external cost, the cost of other protocol route imported by IS-IS. **NOTE** The costs of non-IS-IS routes imported by the **import-route cost-type external** command are displayed in this field so that the costs of non-IS-IS routes are kept independently from the costs of IS-IS routes.
Admin Tag	Administrative tag.
Src Count	Number of source addresses to the same destination.

Item	Description
Priority	Convergence priority of IS-IS routes: • Critical • High • Medium • Low To set the convergence priority of IS-IS routes, run the **9.6.106 prefix-priority (IS-IS)** command.
NextHop	Next hop of the route (B) indicates the backup route label.
Interface	Outbound interface of a route.
ExitIndex	Index of the outbound interface.
Flags	Flags of routing information.

Related Topics

9.6.9 circuit-cost
9.6.64 isis cost
9.6.53 import-route (IS-IS)
9.7.3 ipv6 circuit-cost
9.7.17 isis ipv6 cost
9.6.106 prefix-priority (IS-IS)

9.6.31 display isis spf-log

Function

The **display isis spf-log** command displays IS-IS SPF logs.

Format

display isis spf-log [*process-id* | **vpn-instance** *vpn-instance-name*] [[**level-1** | **level-2**] | **ipv6** | **verbose**]*

display isis *process-id* **spf-log** [[**level-1** | **level-2**] | **ipv6** | **verbose**]*

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6	Displays SPF logs in IPv6 topologies.	-
level-1	Displays Level-1 SPF logs.	-
level-2	Displays Level-2 SPF logs.	-
verbose	Displays detailed information about SPF logs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IS-IS SPF logs, including the start time, duration, number of nodes, and triggered events of SPF calculation.

Example

Display IS-IS SPF logs.

```
<Huawei> display isis spf-log

                    SPF Log information for ISIS(10)
                    --------------------------------

                       ISIS(10) Level-1 SPF Log
                       ------------------------

 StartTime  Duration  Nodes  Count  Last Trigger LSP      Trigger Event
--------------------------------------------------------------------------------
 2013-09-05 10:14:48
          0         1      1      NULL                ISPF_CIRC_DR_CHANGE
 2013-09-05 10:13:23
          1         1      2      NULL                FULL_SPF

                       ISIS(10) Level-2 SPF Log
                       ------------------------

 StartTime  Duration  Nodes  Count  Last Trigger LSP      Trigger Event
--------------------------------------------------------------------------------
 2013-09-05 10:14:48
          1         1      1      NULL                ISPF_CIRC_DR_CHANGE
 2013-09-05 10:13:23
          1         1      2      NULL                FULL_SPF
```

Table 9-108 Description of the display isis spf-log command output

Item	Description
StartTime	Start time of SPF calculation.
Duration	Duration of SPF calculation.
Nodes	Number of nodes in SPF calculation.
Count	Number of times SPF calculated is triggered.
Last Trigger LSP	LSP that triggers the last SPF calculation: ● NULL indicates that the LSP is local. ● LSP ID (specific ID) indicates that the LSP is not local.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trigger Event	Event that triggers the last SPF calculation: ● NEWAREA indicates that a new NET is configured. ● TUNNEL_ADJ indicates that a tunnel neighbor relationship is established. ● ADJDOWN indicates that a tunnel neighbor goes Down. ● NEWLSP indicates that the router receives an LSP of a new process. ● LSPCHANGE indicates that the received LSP is different from local LSPs. ● RST_T2_CANCEL indicates that the GR T2 Timer is disabled. ● RST_T3_EXPIRE indicates that the GR T3 Timer expires. ● RESTART_COMPLETE indicates that the GR is over. ● CIRC_VLINK_CHANGE indicates that the status of the VLink interface changes. ● PRC_IPV4_PREFIX_ADD indicates that an IPv4 route is added. ● PRC_IPV4_PREFIX_DEL indicates that an IPv4 route is deleted. ● PRC_IPV4_PREFIX_MODIFY indicates that an IPv4 route is modified. ● PRC_IPV4_PREFIX_MIGP_ADD indicates that an MIGP IPv4 route is added. ● PRC_IPV4_PREFIX_MIGP_DEL indicates that an MIGP IPv4 route is deleted. ● PRC_IPV4_PREFIX_MIGP_MODIFY indicates that an MIGP IPv4 route is modified. ● PRC_IPV6_PREFIX_ADD indicates that an IPv6 route is added. ● PRC_IPV6_PREFIX_DEL indicates that an IPv6 route is deleted. ● PRC_IPV6_PREFIX_MODIFY indicates that an IPv6 route is modified. ● ISPF_ADJ_STATE_CHANGE indicates that the IS-IS neighbor status changes. ● ISPF_ADJ_USAGE_CHANGE indicates that the IS-IS neighbor level changes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• ISPF_ADJ_PROT_USAGE_CHANGE indicates that the protocol used by the IS-IS neighbor changes. • ISPF_ADJ_NEXTHOP_CHANGE indicates that the next hop of the IS-IS neighbor changes. • ISPF_CIRC_METRIC_CHANGE indicates that the cost on the interface changes. • ISPF_CIRC_DR_CHANGE indicates that the DIS changes. • ISPF_NODE_DEL indicates that the nodes in the SPT change. • ISPF_NODE_OLOAD_CHANGE indicates that the overload bit of the system changes. • ISPF_LINK_ADD indicates that a new link is added to the SPT. • ISPF_LINK_DEL indicates that a link is deleted from the SPT. • ISPF_LINK_METRIC_CHANGE indicates that the cost of a link changes. • FULL_SPF indicates that a full SPF calculation is triggered. • AREA_CFG_CHANGE indicates that the area of the process changes. • AREA_LEARNT_CHANGE indicates that the area of the IS-IS neighbor changes. • ISPF_TUNNEL_TYPE_CHANGE indicates that the tunnel type changes. • PRC_LEAVE_MAN_OVERLOAD indicates that the system exits the **set-overload** state that is set manually. • PRC_IPV4_SELFLSP_CHANGE indicates that the IPv4 route in the local LSP changes. • PRC_IPV6_SELFLSP_CHANGE indicates that the IPv6 route in the local LSP changes. • PRC_ALIAS_TLV_CHANGE indicates that the **ALIAS TLV** in the LSP changes. • LFA_LINK_ADD indicates that a link is added to the routes for FRR. • LFA_LINK_DEL indicates that a link is deleted from the routes for FRR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• LFA_LINK_CHANGE indicates that the links of the routes for FRR change. • LFA_NODE_ADD indicates that a node is added along the links of the routes for FRR. • LFA_NODE_DEL indicates that a node is deleted from the links of the routes for FRR. • LFA_NODE_CHANGE indicates that the nodes along the links of the routes for FRR change. • KEY_RESRORE indicates that the local device receives an indirect next hop key.

9.6.32 display isis spf-tree

Function

The **display isis spf-tree** command displays the topology of the SPF tree that is generated by IS-IS.

Format

display isis spf-tree [**systemid** *systemid* | **dname** *dname*] [[**level-1** | **level-2**] | **ipv6** | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **spf-tree** [**systemid** *systemid* | **dname** *dname*] [[**level-1** | **level-2**] | **ipv6** | **verbose**] *

display isis *process-id* **spf-tree statistics** [[**level-1** | **level-2**] | **ipv6**] *

display isis spf-tree statistics [[**level-1** | **level-2**] | **ipv6**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
systemid *systemid*	Displays the SPF tree of the router with a specified system ID or pseudonode ID.	The value is in XXXX.XXXX.XXXX[.XX] format.

Parameter	Description	Value
dname *dname*	Displays the SPF tree of the router with a specified dynamic name.	The value is a string of 1 to 64 characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
level-1	Displays Level-1 SPF tree.	-
level-2	Displays Level-2 SPF tree.	-
ipv6	Displays SPF tree in IPv6 topologies.	-
verbose	Displays detailed information about SPF tree.	-
process-id	Display SPF tree in a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays SPF tree of the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
statistics	Displays SPF tree statistics, including information about links and nodes on the SPF tree.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify **statistics** to view the current status of the SPF tree. The generated SPF tree can be used to calculate routes only when the SPF calculation status is Completed, that is, incremental SPF (ISPF) calculation is complete.

Example

Display information about the SPF tree.

```
<Huawei> display isis spf-tree
                    Shortest Path Tree for ISIS(1)
                    ------------------------------

      Flags:   T-System is on SPF TREE  R-System is directly reachable
               O-System is Overload     D-System or Link is to be deleted
               C-Neighbor is child      P-Neighbor is parent
```

```
                G-Cost gets greater      L-Cost gets lower
                H-Nexthop is changed     U-Protocol usage is changed
                V-Link is involved       N-Link is a new path
                S-Link is IGP Shortcut   *-Relative cost
                    ISIS(1) Level-1 Shortest Path Tree
                    ----------------------------------

 SpfNode          NodeFlags  NeighbourNode     LinkCost   LinkFlags
-----------------------------------------------------------------------
-----------------------------------------------------------------------
 0000.0000.0001.00 T/-/-/-   >0000.0000.0002.01       10   P/-/-/-/-/-/-
>0000.0000.0002.00 T/-/-/-    0000.0000.0003.01       10   C/-/-/-/-/-/-
                        >0000.0000.0002.01       10   C/-/-/-/-/-/-
                         0000.0000.0004.00      -10*  C/-/-/-/S/-/-
>0000.0000.0002.01 T/R/-/-    0000.0000.0001.00        0   C/-/-/-/-/-/-
                        >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0003.00 T/-/-/-    0000.0000.0004.02       10   C/-/-/-/-/-/-
                         0000.0000.0003.01       10   P/-/-/-/-/-/-
 0000.0000.0003.01 T/R/-/-    0000.0000.0003.00        0   C/-/-/-/-/-/-
                        >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0004.00 T/-/-/-    0000.0000.0004.02       10   P/-/-/-/-/-/-
                         0000.0000.0004.01       10   C/-/-/-/-/-/-
 0000.0000.0004.01 T/-/-/-    0000.0000.0004.00        0   P/-/-/-/-/-/-
                         0000.0000.0005.00        0   C/-/-/-/-/-/-
 0000.0000.0004.02 T/-/-/-    0000.0000.0004.00        0   C/-/-/-/-/-/-
                         0000.0000.0003.00        0   P/-/-/-/-/-/-
 0000.0000.0005.00 T/-/-/-    0000.0000.0004.01       10   P/-/-/-/-/-/-
                    ISIS(1) Level-2 Shortest Path Tree
                    ----------------------------------

 SpfNode          NodeFlags  NeighbourNode     LinkCost   LinkFlags
-----------------------------------------------------------------------
-----------------------------------------------------------------------
 0000.0000.0001.00 T/-/-/-   >0000.0000.0002.01       10   P/-/-/-/-/-/-
>0000.0000.0002.00 T/-/-/-    0000.0000.0003.01       10   C/-/-/-/-/-/-
                        >0000.0000.0002.01       10   C/-/-/-/-/-/-
                         0000.0000.0004.00      -10*  C/-/-/-/S/-/-
>0000.0000.0002.01 T/R/-/-    0000.0000.0001.00        0   C/-/-/-/-/-/-
                        >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0003.00 T/-/-/-    0000.0000.0004.02       10   C/-/-/-/-/-/-
                         0000.0000.0003.01       10   P/-/-/-/-/-/-
 0000.0000.0003.01 T/R/-/-    0000.0000.0003.00        0   C/-/-/-/-/-/-
                        >0000.0000.0002.00        0   P/-/-/-/-/-/-
 0000.0000.0004.00 T/-/-/-    0000.0000.0004.02       10   P/-/-/-/-/-/-
                         0000.0000.0004.01       10   C/-/-/-/-/-/-
 0000.0000.0004.01 T/-/-/-    0000.0000.0004.00        0   P/-/-/-/-/-/-
                         0000.0000.0005.00        0   C/-/-/-/-/-/-
 0000.0000.0004.02 T/-/-/-    0000.0000.0004.00        0   C/-/-/-/-/-/-
                         0000.0000.0003.00        0   P/-/-/-/-/-/-
 0000.0000.0005.00 T/-/-/-    0000.0000.0004.01       10   P/-/-/-/-/-/-
```

Table 9-109 Description of the display isis spf-tree command output

Item	Description
SpfNode	Node ID in the network topology.
NodeFlags	Node flag: ● T: The node is on the SPF tree. ● R: The node is directly reachable. ● O: The node is overloaded. ● D: The node is to be deleted.
NeighbourNode	ID of the neighboring node.

Item	Description
LinkCost	Link cost.
LinkFlags	Link flag: ● C: Neighbor is child ● P: Neighbor is parent ● G: Cost gets greater ● L: Cost gets lower ● H: Nexthop is changed ● U: Protocol usage is changed ● V: Link is involved ● N: Link is a new path ● S: Link is IGP Shortcut ● *: Relative cost
>	Mark of the local node.

Display detailed information about SPF tree.

```
<Huawei> display isis spf-tree verbose

                    Shortest Path Tree for ISIS(1)
                    ------------------------------

                   ISIS(1) Level-1 Shortest Path Tree
                   ----------------------------------
>0000.0000.0001.00
  Distance           : 0
  Distance-URT       : 0
  Flags              : SPT
  IPv4 Nexthops-URT   : 0
  IPv6 Nexthops       : 0
  Neighbors: 1 (Children:1 Parents:0 Others:0)
          (1)   0000.0000.0003.02
                Cost  : 10
                Flags : Child

 0000.0000.0003.00
  Distance           : 10
  Distance-URT       : 10
  Flags              : SPT
  IPv4 Nexthops-URT   : 1
          (1) 10.2.1.1         IF:GE0/0/2  NBR:0000.0000.0003.00
  IPv6 Nexthops       : 1
          (1) FE80::82FB:6FF:FE35:45B6  IF:GE0/0/2  NBR:0000.0000.0003.00
  Neighbors: 1 (Children:0 Parents:1 Others:0)
          (1)   0000.0000.0003.02
                Cost  : 10
                Flags : Parent

 0000.0000.0003.02
  Distance           : 10
  Distance-URT       : 10
  Flags              : SPT/Direct/Isolate/V6_Islt
  IPv4 Nexthops-URT   : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
```

```
          (1)   0000.0000.0003.00
                Cost  : 0
                      C:0 I:GigabitEthernet0/0/2
                Flags : Adj/Child

          (2)  >0000.0000.0001.00
                Cost  : 0
                Flags : Parent


                 ISIS(1) Level-2 Shortest Path Tree
                 ----------------------------------
>0000.0000.0001.00
  Distance           : 0
  Distance-URT       : 0
  Flags              : SPT
  IPv4 Nexthops-URT   : 0
  IPv6 Nexthops       : 0
  Neighbors: 1 (Children:1 Parents:0 Others:0)
          (1)   0000.0000.0003.02
                Cost  : 10
                Flags : Child

 0000.0000.0003.00
  Distance           : 10
  Distance-URT       : 10
  Flags              : SPT
  IPv4 Nexthops-URT   : 1
          (1) 10.2.1.1         IF:GE0/0/2  NBR:0000.0000.0003.00
  IPv6 Nexthops       : 1
          (1) FE80::82FB:6FF:FE35:45B6  IF:GE0/0/2  NBR:0000.0000.0003.00
  Neighbors: 1 (Children:0 Parents:1 Others:0)
          (1)   0000.0000.0003.02
                Cost  : 10
                Flags : Parent

 0000.0000.0003.02
  Distance           : 10
  Distance-URT       : 10
  Flags              : SPT/Direct/Isolate/V6_Islt
  IPv4 Nexthops-URT   : 0
  IPv6 Nexthops       : 0
  Neighbors: 2 (Children:1 Parents:1 Others:0)
          (1)   0000.0000.0003.00
                Cost  : 0
                      C:0 I:GigabitEthernet0/0/2
                Flags : Adj/Child

          (2)  >0000.0000.0001.00
                Cost  : 0
                Flags : Parent
```

Table 9-110 Description of the display isis spf-tree verbose command output

Item	Description
Distance	Cost of the shortest path from the root node to the destination node, excluding the TE tunnel link.
Distance-URT	Cost of the shortest path from the root node to the destination node, including the TE tunnel link.

Item	Description
Flags	Flag: ● SPT: The node is in the tree. ● Direct: The node is a direct node. ● Shortcut: The node is on a shortcut link. ● Oload: The node is in Overload state. ● Isolate: The node is not in the tree. ● Del: The node will be deleted. ● Remote: The node is on a tunnel.
IPv4 Nexthops-URT	IPv4 next hop of the node in the unicast routing table.
IPv6 Nexthops	IPv6 next hop of the node in the unicast routing table.
Neighbors	Information about all the neighbors of this node.
Cost	Cost of the link from the root node to this node.
Flags	Relationship with the neighbor: ● Parent: The neighbor is a parent node. ● Child: The neighbor is a child node.
IF	Name of the outbound interface.
NBR	System ID of the next hop.

Display the current status statistics of the SPF tree.

```
<Huawei> display isis spf-tree statistics

                Statistics information of SPT for ISIS(1)
                -----------------------------------------

                        Level-1 Statistics
                        ------------------
Nodes information:
        Total:                          3
        Count of nodes in SPT:              3
        Count of isolate nodes in SPT:      1
        Count of IPv6 isolate nodes in SPT:  1
        Max Distance of nodes in SPT:       10
Links information:
        Total:                          4
        Count of links from Parent to Son:   2
        Count of links from Son to Parent:   2
        Count of links that just changed:    0
Status of SPF:                              Completed


                        Level-2 Statistics
                        ------------------
Nodes information:
        Total:                          3
        Count of nodes in SPT:              3
        Count of isolate nodes in SPT:      1
        Count of IPv6 isolate nodes in SPT:  1
        Max Distance of nodes in SPT:       10
```

```
Links information:
        Total:                          4
        Count of links from Parent to Son:   2
        Count of links from Son to Parent:   2
        Count of links that just changed:    0
Status of SPF:                          Completed
```

Table 9-111 Description of the display isis spf-tree statistics command output

Item	Description
Total (Nodes information)	Total number of nodes.
Count of nodes in SPT	Number of nodes in the SPT tree.
Count of isolate nodes in SPT	Number of isolated nodes in the network topology.
Count of IPv6 isolate nodes in SPT	Number of isolated IPv6 nodes in the network topology.
Max Distance of nodes in SPT	Maximum distance from the root node to the leaf node.
Total (Links information)	Total number of links.
Count of links from Parent to Son	Number of links from the parent node to the child node.
Count of links from Son to Parent	Number of links from the child node to the parent node.
Count of links that just changed	Number of links that just changed.
Status of SPF	Status of SPF calculation: ● Completed: indicates that SPF calculation is complete. ● Scheduled: indicates that SPF calculation is triggered but does not start. ● Running: indicates that SPF calculation is being performed.

9.6.33 display isis statistics

Function

The **display isis statistics** command displays IS-IS process statistics.

Format

display isis statistics packet [**interface** *interface-type interface-number*]

display isis statistics [**updated-lsp** [**history**]] [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **statistics** [[[**updated-lsp** [**history**]] [**level-1** | **level-2** | **level-1-2**]] | **packet**]

display isis *process-id* **statistics packet** [**lsp**]

display isis statistics packet lsp [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
packet	Displays IS-IS packet statistics.	-
interface *interface-type interface-number*	Displays IS-IS packet statistics on a specified interface.	-
updated-lsp	Displays real-time data of received LSPs. By default, statistics about the LSPs received within the last 1 hour are displayed.	-
history	Displays historical data of received LSPs. By default, statistics about the LSPs received within the last 24 hours are displayed.	-
level-1	Displays IS-IS Level-1 statistics.	-
level-2	Displays IS-IS Level-2 statistics.	-
level-1-2	Displays IS-IS Level-1-2 statistics.	-
process-id	Displays statistics in a specified IS-IS process.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Displays statistics about the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
lsp	Displays statistics about IS-IS LSPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display isis statistics** command to view IS-IS process statistics, including the number of routes learned from other IS-IS devices, number of routes imported from other routing protocols, number of locally generated LSPs, and convergence priorities of IS-IS routes.

Example

Display IS-IS process statistics.

```
<Huawei> display isis statistics
                    Statistics information for ISIS(1)
                    ----------------------------------
                          Level-1 Statistics
                          ------------------
Forwarding routes information:
        Total IPV4 Learnt Routes: 0
                     Critical: 0
                     High    : 0
                     Medium  : 0
                     Low     : 0
        Total IPv4 Forwarding Routes: 1
Total IPv6 Learnt Routes: 0
                    Critical: 0
                    High    : 0
                    Medium  : 0
                    Low     : 0
        Total IPv6 Forwarding Routes: 1
Imported routes information:
        IPv4 Imported Routes:
                     Static: 0       Direct: 0
                     ISIS:   0       BGP:    0
                     RIP:    0       OSPF:   0
        IPv6 Imported Routes:
                     Static: 0       Direct: 0
                     ISIS:   0       BGP:    0
                     RIPng:  0       OSPFv3: 0
Number of advertised imported routes:
       IPv4 Imported Routes:   0
       IPv6 Imported Routes:   0
Lsp information:
                LSP Source ID:          No. of used LSPs
                0000.0000.0022                  002
                          Level-2 Statistics
                          ------------------
Forwarding routes information:
        Total IPV4 Learnt Routes: 0
                     Critical: 0
                     High    : 0
                     Medium  : 0
                     Low     : 0
        Total IPv4 Forwarding Routes: 1
Total IPv6 Learnt Routes: 0
                    Critical: 0
                    High    : 0
                    Medium  : 0
                    Low     : 0
        Total IPv6 Forwarding Routes: 1
Imported routes information:
        IPv4 Imported Routes:
                     Static: 0       Direct: 0
```

```
                    ISIS:   0       BGP:    0
                    RIP:    0       OSPF:   0
        IPv6 Imported Routes:
                    Static: 0       Direct: 0
                    ISIS:   0       BGP:    0
                    RIPng:  0       OSPFv3: 0
Number of advertised imported routes:
        IPv4 Imported Routes:   0
        IPv6 Imported Routes:   0
Lsp information:
                LSP Source ID:          No. of used LSPs
                0000.0000.0002                  001
```

Table 9-112 Description of the display isis statistics command output

Item	Description
Total IPV4 Learnt Routes ● Critical ● High ● Medium ● Low	Number of IPv4 routes learned by IS-IS: ● Critical: indicates the number of IPv4 routes with convergence priority critical. ● High: indicates the number of IPv4 routes with convergence priority high. ● Medium: indicates the number of IPv4 routes with convergence priority medium. ● Low: indicates the number of IPv4 routes with convergence priority low.
Total IPv4 Forwarding Routes	Number of IPv4 routes counted based on the destination address. If there are multiple routes to the same destination, these routes are counted as one route.
Total IPv6 Learnt Routes ● Critical ● High ● Medium ● Low	Number of IPv6 routes learned by IS-IS: ● Critical: indicates the number of IPv6 routes with convergence priority critical. ● High: indicates the number of IPv6 routes with convergence priority high. ● Medium: indicates the number of IPv6 routes with convergence priority medium. ● Low: indicates the number of IPv6 routes with convergence priority low.
Total IPv6 Forwarding Routes	Number of IPv6 routes counted based on the destination address. If there are multiple routes to the same destination, these routes are counted as one route.
IPv4 Imported Routes	Imported IPv4 routes.
Static	Number of imported static routes.
Direct	Number of imported direct routes.
ISIS	Number of imported IS-IS routes.
BGP	Number of imported BGP routes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RIP	Number of imported RIP routes.
OSPF	Number of imported OSPF routes.
IPv6 Imported Routes	Imported IPv6 routes.
RIPng	Number of imported RIPng routes.
OSPFv3	Number of imported OSPFv3 routes.
LSP Source ID	System ID of the router that generates the LSP.
No. of used LSPs	Number of used LSPs.
Number of advertised imported routes	Number of imported external routes that are advertised.

Display IS-IS packet statistics.

```
<Huawei> display isis statistics packet

                    PDUs information for ISIS(1)
                    ----------------------------
        Sent packets:
        PDU type                Total(packets)
        L1 IIH                  2516
        L1 LSP                    84
        L1 CSNP                    8
        L1 PSNP                   44
        L2 IIH                  5028
        L2 LSP                    80
        L2 CSNP                    8
        L2 PSNP                   46

        Received packets:
        PDU type                Total(packets)
        L1 IIH                 12943
        L1 LSP                   216
        L1 CSNP                 3911
        L1 PSNP                   40
        L2 IIH                 14907
        L2 LSP                   206
        L2 CSNP                 3900
        L2 PSNP                   41
```

Table 9-113 Description of the display isis statistics packet command output

Item	Description
PDU type	Packet type.
Total(packets)	Total number of packets.
L1 IIH	Level-1 Hello packets.
L1 LSP	Level-1 LSPs.
L1 CSNP	Level-1 CSNPs.

Item	Description
L1 PSNP	Level-1 PSNPs.
L2 IIH	Level-2 Hello packets.
L2 LSP	Level-2 LSPs.
L2 CSNP	Level-2 CSNPs.
L2 PSNP	Level-2 PSNPs.

9.6.34 display isis statistics purge-lsp

Function

The **display isis statistics purge-lsp** command displays statistics about purge LSPs on the network.

Format

display isis [*process-id*] **statistics purge-lsp** [**level-1** | **level-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process. If *process-id* is not specified in the command, statistics about purge LSPs of all IS-IS processes are displayed.	The value is an integer ranging from 1 to 65535.
level-1	Displays statistics about IS-IS Level-1 purge LSPs.	-
level-2	Displays statistics about IS-IS Level-2 purge LSPs.	-
vpn-instance *vpn-instance-name*	Displays statistics about purge LSPs of specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

When monitoring the device status or locating a fault, you can run the **display isis statistics purge-lsp** command to check statistics about purge LSPs. The statistics help traffic statistics collection and troubleshooting.

Example

Display statistics about purge LSPs.

```
<Huawei> display isis statistics purge-lsp
 Statistics of Purge packets Received for ISIS(1)
             ---------------------------------------

                     Level-1 Statistics
LSP ID                   Purge count   Last Purge time
0000.0000.0001.00-00               0    --

                     Level-2 Statistics
LSP ID                   Purge count   Last Purge time
0000.0000.0001.00-00               0    --
```

Table 9-114 Description of the **display isis statistics purge-lsp** command output

Item	Description
LSP ID	LSP ID
Purge count	Number of times purge LSPs are received. 0 indicates that no purge LSPs are received.
Last Purge time	Time when the system last received a purge LSP. If the system does not receive any purge LSP, **--** is displayed.

9.6.35 display isis traffic-eng advertisements

Function

The **display isis traffic-eng advertisements** command displays latest advertised traffic engineering (TE) information.

Format

display isis traffic-eng advertisements [{ **level-1** | **level-2** | **level-1-2** } | { *lsp-id* | **local** }] * [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng advertisements** [{ **level-1** | **level-2** | **level-1-2** } | { *lsp-id* | **local** }] *

Parameters

Parameter	Description	Value
level-1	Displays TE information in a Level-1 LSDB.	-
level-2	Displays TE information in a Level-2 LSDB.	-
level-1-2	Displays TE information in a Level-1 or Level-2 LSDB based on the local node type. That is, if the local node is a Level-1 or Level-2 node, TE information in a Level-1 or Level-2 LSDB is displayed. If the local node is a Level-1-2 node, TE information in Level-1 and Level-2 LSDBs is displayed.	-
lsp-id	Displays TE information in the specified LSP.	The value is in dotted decimal notation. The value ranges from 16 to 20 in ####.####.####.##-## format, such as 0050.0500.5004.00-00.
local	Displays locally advertised TE information.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display advertised TE information.

```
<Huawei> display isis traffic-eng advertisements
                        TE information for ISIS(1)
                        --------------------------
Level-1 Link State Database
---------------------------
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.0001.00-00* 0x00000001   0x3f57        534           0/0/0
 NLPID      : IPV4
 AREA ADDR  : 00.0005
Level-2 Link State Database
---------------------------
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.0001.00-00* 0x0000001c   0xf1ec        687           0/0/0
 NLPID      : IPV4
 AREA ADDR  : 00.0005
 Router ID  : 10.1.1.9
+NBR        : 0000.0000.0002.02  COST: 10
   Affinity: 0x00000000
   Interface IP Address:  10.1.1.1
   Physical BW  :      12500 Bytes/sec
   Reservable BW:       6250 Bytes/sec
   Unreserved BW:
   BW Unresrv[0] :       6250 Bytes/sec BW Unresrv[1] :       6250 Bytes/sec
   BW Unresrv[2] :       6250 Bytes/sec BW Unresrv[3] :       6250 Bytes/sec
   BW Unresrv[4] :       6250 Bytes/sec BW Unresrv[5] :       6250 Bytes/sec
   BW Unresrv[6] :       6250 Bytes/sec BW Unresrv[7] :       6250 Bytes/sec
   TE Cost      :         10
   Sub Unreserved BW for Class Type 1:
   BW Unresrv[0] :          0 Bytes/sec BW Unresrv[1] :          0 Bytes/sec
   BW Unresrv[2] :          0 Bytes/sec BW Unresrv[3] :          0 Bytes/sec
   BW Unresrv[4] :          0 Bytes/sec BW Unresrv[5] :          0 Bytes/sec
   BW Unresrv[6] :          0 Bytes/sec BW Unresrv[7] :          0 Bytes/sec
   Bandwidth Constraint Model: Russian Doll
   Bandwidth Constraints:
   BC[0] :       6250 Bytes/sec BC[1] :          0 Bytes/sec
   Local Overbooking Multiplier:
   LOM[0] :        100 %         LOM[1] :        100 %
+NBR        : 0000.0000.0004.00  COST: 10
   Affinity: 0x00000000
   Interface IP Address:  10.3.1.1
   Peer IP Address     :  10.3.1.2
   Physical BW  :      12500 Bytes/sec
   Reservable BW:       6250 Bytes/sec
   Unreserved BW:
   BW Unresrv[0] :       6250 Bytes/sec BW Unresrv[1] :       6250 Bytes/sec
   BW Unresrv[2] :       6250 Bytes/sec BW Unresrv[3] :       6250 Bytes/sec
   BW Unresrv[4] :       6250 Bytes/sec BW Unresrv[5] :       6250 Bytes/sec
   BW Unresrv[6] :       6250 Bytes/sec BW Unresrv[7] :       6250 Bytes/sec
   TE Cost      :         10
   Sub Unreserved BW for Class Type 1:
   BW Unresrv[0] :          0 Bytes/sec BW Unresrv[1] :          0 Bytes/sec
   BW Unresrv[2] :          0 Bytes/sec BW Unresrv[3] :          0 Bytes/sec
   BW Unresrv[4] :          0 Bytes/sec BW Unresrv[5] :          0 Bytes/sec
   BW Unresrv[6] :          0 Bytes/sec BW Unresrv[7] :          0 Bytes/sec
   Bandwidth Constraint Model: Russian Doll
   Bandwidth Constraints:
   BC[0] :       6250 Bytes/sec BC[1] :          0 Bytes/sec
   Local Overbooking Multiplier:
   LOM[0] :        100 %         LOM[1] :        100 %
+SRLG NBR ID: 0000.0000.0004.00
   Interface IP Address: 10.3.1.1
   Neighbor IP Address : 10.3.1.2
   Shared Risk Link Group: 10,20
```

Table 9-115 Description of the display isis traffic-eng advertisements command output

Item	Description
LSPID	LSP ID.
LSP Seq Num	LSP sequence number.
LSP Checksum	LSP checksum.
LSP Holdtime	LSP holdtime.
ATT/P/OL	Attach bit (ATT), partition bit (P), or overload bit (OL).
NLPID	Network protocol.
AREA ADDR	Area address.
Router ID	Router ID of the router.
+NBR	System ID of the neighbor with the cost style wide, wide-compatible, or compatible.
COST	Cost.
Affinity:	Affinity attribute of a link.
Interface IP Address	IP address of an interface.
Peer IP Address	Peer IP address of an interface.
Physical BW :	Physical bandwidth of a link.
Reservable BW:	Reservable bandwidth of a link.
Unreserved BW	Unreserved bandwidth.
Sub Unreserved BW for Class Type 1	Unreserved bandwidth for CT1.
BW Unresrv [x]	Unreserved bandwidth for the link with priority x.
TE Cost	TE cost of a link.
Bandwidth Constraint Model	Bandwidth constraint model used by a link.
Bandwidth Constraints	Bandwidth constraint.
BC[x]	Bandwidth constraint of BCx.
Local Overbooking Multiplier	Local overbooking multiplier.
LOM[x]	Local overbooking multiplier of BCx.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
+SRLG NBR ID	System ID of a neighbor in a shared risk link group (SRLG).
Neighbor IP Address	IP address of the neighbor.
Shared Risk Link Group	Shared risk link group. **NOTE** When SRLG is enabled on an interface, TE information contains SRLG information.

Related Topics

11.2.151 traffic-eng

9.6.36 display isis traffic-eng link

Function

The **display isis traffic-eng link** command displays IS-IS TE link information.

Format

display isis traffic-eng link [{ **level-1** | **level-2** | **level-1-2** } | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng link** [{ **level-1** | **level-2** | **level-1-2** } | **verbose**] *

Parameters

Parameter	Description	Value
level-1	Displays TE link information on a Level-1 router.	-
level-2	Displays TE link information on a Level-2 router.	-
level-1-2	Displays TE link information on a Level-1-2router.	-
verbose	Displays detailed TE link information.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the IS level is not specified, Level-1-2 TE link information is displayed.

Example

Display IS-IS TE link information.

```
<Huawei> display isis traffic-eng link
                    TE information for ISIS(1)
                    --------------------------
Level-2 Link Information
------------------------
 0000.0000.0001.00--> 0000.0000.0001.01    Type: MULACC  LinkID: 10.1.1.1
 0000.0000.0002.00--> 0000.0000.0003.00    Type: P2P     LinkID: 10.3.3.9
 0000.0000.0002.00--> 0000.0000.0001.01    Type: MULACC  LinkID: 10.1.1.1
 0000.0000.0003.00--> 0000.0000.0002.00    Type: P2P     LinkID: 10.2.2.9
 0000.0000.0003.00--> 0000.0000.0004.01    Type: MULACC  LinkID: 10.1.1.2
 0000.0000.0004.00--> 0000.0000.0004.01    Type: MULACC  LinkID: 10.1.1.2
 Total Number of TE Links in Level-2 Area: 6, Num Active: 6
```

Table 9-116 Description of the display isis traffic-eng link command output

Item	Description
Type	Link type, including MULACC and P2P.
LinkID	TE link ID.
Total Number of TE Links in Level-2 Area	Total number of TE links in a Level-2 area.
Num Active	Number of active TE links.

Display detailed IS-IS TE link information.

```
<Huawei> display isis traffic-eng link verbose
                    TE information for ISIS(1)
```

```
                    --------------------------

Level-2 Link Information
------------------------
 Link Status In CSPF : INACTIVE
 0000.0000.0001.00-->0000.0000.0002.00        Type: P2P     LinkID: 10.2.2.2
         Process ID       :  1          Router ID        :  10.2.2.1
         Area ID          :  2          Admin Group      :  0
         Te Cost          :  10         Igp Cost         :  10
         Max Bandwidth    :  0          Max Res Bandwidth:  0
         Shared Risk Link Group: 20
         BC Model         :  RDM
         DS-TE Mode       :  Non-standard IETF DS-TE Mode

 Link Status In CSPF : INACTIVE
 0000.0000.0002.00-->0000.0000.0001.00        Type: P2P     LinkID: 10.2.2.1
         Process ID       :  1          Router ID        :  10.2.2.2
         Area ID          :  2          Admin Group      :  0
         Te Cost          :  10         Igp Cost         :  10
         Max Bandwidth    :  0          Max Res Bandwidth:  0
         BC Model         :  RDM
         DS-TE Mode       :  Non-standard IETF DS-TE Mode

 Total Number of TE Links in Level-2 Area: 2, Num Active: 0
```

Table 9-117 Description of the display isis traffic-eng link verbose command output

Item	Description
Link Status In CSPF	Link status in CSPF calculation.
Process ID	IS-IS process ID.
Router ID	Router ID.
Area ID	Area ID.
Admin Group	Administrative group.
Te Cost	TE cost.
Igp Cost	IGP cost.
Max Bandwidth	Maximum bandwidth.
Max Res Bandwidth	Maximum reservable bandwidth.
Shared Risk Link Group	Shared risk link group.
BC Model	Bandwidth constraint model.
DS-TE Mode	DS-TE mode, including standard and non-standard DS-TE modes.

Related Topics

11.2.151 traffic-eng

9.6.37 display isis traffic-eng network

Function

The **display isis traffic-eng network** command displays IS-IS TE network information.

Format

display isis traffic-eng network [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng network** [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Displays TE network information on a Level-1 router.	-
level-2	Displays TE network information on a Level-2 router.	-
level-1-2	Displays TE network information on a Level-1-2 router.	-
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command does not take effect on P2P networks.

If the IS level is not specified, Level-1-2 TE network information is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display IS-IS TE network information.

```
<Huawei> display isis traffic-eng network
                    TE information for ISIS(1)
                    --------------------------
Level-2 Network Information
---------------------------
   DIS Router ID   : 10.1.1.9     DIS''s Ip Address          : 10.1.1.1
   Status In CSPF : ACTIVE      Attached Router Count     : 2
   List of Attached Routers
 RouterId : 10.1.1.9   Nbr : 0000.0000.0001.00  Link State : 1
 RouterId : 10.2.2.9   Nbr : 0000.0000.0002.00  Link State : 1
   DIS Router ID   : 10.4.4.9     DIS''s Ip Address          : 10.1.1.2
   Status In CSPF : ACTIVE      Attached Router Count     : 2
   List of Attached Routers
 RouterId : 10.4.4.9   Nbr : 0000.0000.0004.00  Link State : 1
 RouterId : 10.3.3.9   Nbr : 0000.0000.0003.00  Link State : 1
 Total Number of TE Networks in Level-2 Area: 2, Num Active: 2
```

Table 9-118 Description of the display isis traffic-eng network command output

Item	Description
DIS Router ID	Router ID of the DIS.
DIS's Ip Address	IP address of the DIS.
Status In CSPF	Whether CSPF is enabled on the router.
Attached Router Count	Number of connected routers, including the local router.
List of Attached Routers	List of connected routers.
RouterId	Router ID of the local router.
Nbr	IP address of the neighbor.
Link State	Link status.
Total Number of TE Networks in Level-2 Area	Total number of networks on which TE is enabled in a Level-2 area.

Related Topics

11.2.151 traffic-eng

9.6.38 display isis traffic-eng statistics

Function

The **display isis traffic-eng statistics** command displays IS-IS TE statistics.

Format

display isis traffic-eng statistics [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng statistics**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID. If no process ID is specified, TE statistics about all IS-IS processes are displayed.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IS-IS TE statistics on the router, including the IS level, cost style, IS-IS TE level, and IS-IS router ID.

Example

Display IS-IS TE statistics.

```
<Huawei> display isis traffic-eng statistics
                        TE information for ISIS(1)
                        --------------------------
TE Statistics Information
-------------------------
 IS-IS System Type                        : Level-1-2
 IS-IS Cost Style Status                  : Wide
 IS-IS Level-1 Traffic Engineering Status   : Disabled
 IS-IS Level-2 Traffic Engineering Status   : Enabled
 IS-IS Router ID                          : 10.1.1.9
```

Table 9-119 Description of the display isis traffic-eng statistics command output

Item	Description
IS-IS System Type	IS level.
IS-IS Cost Style Status	Cost style of the router.
IS-IS Level-1 Traffic Engineering Status	TE status of a Level-1 router.

Item	Description
IS-IS Level-2 Traffic Engineering Status	TE status of a Level-2 router.
IS-IS Router ID	Router ID of an IS-IS router.

Related Topics

11.2.151 traffic-eng

9.6.39 display isis traffic-eng sub-tlvs

Function

The **display isis traffic-eng sub-tlvs** command displays the types of sub-TLVs carrying DS-TE parameters.

Format

display isis traffic-eng sub-tlvs [*process-id* | **vpn-instance** *vpn-instance-name*]

display isis *process-id* **traffic-eng sub-tlvs**

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the types of sub-TLVs carrying DS-TE parameters.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display isis traffic-eng sub-tlvs
IS-IS(1) SubTlv Information
---------------------------------
 Unreserved sub-pool bandwidth sub-tlv value : 251
 Bandwidth constraint sub-tlv value          : 252
 LO multiplier sub-tlv value                 : 253
```

Table 9-120 Description of the display isis traffic-eng sub-tlvs command output

Item	Description
IS-IS(1) SubTlv Information	Sub-TLV information about IS-IS process 1.
Unreserved sub-pool bandwidth sub-tlv value	Sub-TLV of the unreserved sub-pool bandwidth.
Bandwidth constraint sub-tlv value	Sub-TLV of the bandwidth constraint.
LO multiplier sub-tlv value	Sub-TLV of the local overbooking multiplier.

Related Topics

11.2.151 traffic-eng

9.6.40 display snmp-agent trap feature-name isis all

Function

The **display snmp-agent trap feature-name isis all** command displays the status of the trap function on the IS-IS module.

Format

display snmp-agent trap feature-name isis all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the trap function has been enabled, the status is displayed as **on**. Otherwise, the status is displayed as **off**.

To change the status of the trap function, run the **snmp-agent trap enable feature-name isis** command to enable the trap function or run the **undo snmp-agent trap enable feature-name isis** command to disable the trap function.

Example

Display all trap messages of the IS-IS module.

```
<Huawei> display snmp-agent trap feature-name isis all
-----------------------------------------------------------------------------
Feature name: ISIS
Trap number : 17
-----------------------------------------------------------------------------
Trap name                        Default switch status      Current switch status
isisDatabaseOverload             off                        off
isisManualAddressDrops           off                        off
isisCorruptedLSPDetected         off                        off
isisAttemptToExceedMaxSequence   off                        off
isisIDLenMismatch                off                        off
isisMaxAreaAddressesMismatch     off                        off
isisOwnLSPPurge                  off                        off
isisSequenceNumberSkip           off                        off
isisAuthenticationTypeFailure    off                        off
isisAuthenticationFailure        off                        off
isisVersionSkew                  off                        off
isisAreaMismatch                 off                        off
isisRejectedAdjacency            off                        off
isisLSPTooLargeToPropagate       off                        off
isisOrigLSPBuffSizeMismatch      off                        off
isisProtocolsSupportedMismatch   off                        off
isisAdjacencyChange              off                        off
```

Table 9-121 Description of the display snmp-agent trap feature-name isis all command output

Item	Description
Feature name	Name of the module that trap messages belong to.
Trap number	Number of trap messages.

Item	Description
Trap name	Name of the trap message of the IS-IS module: ● isisAdjacencyChange: indicates neighbor changes. ● isisAreaMismatch: indicates that the area address of the received Level-1 Hello packet does not match the local area address. ● isisAttemptToExceedMaxSequence: indicates that the LSP sequence number is close to the maximum value. ● isisAuthenticationFailure: indicates that the authentication code in the received packet does not match the local authentication code. ● isisAuthenticationTypeFailure: indicates that the authentication type in the received packet does not match the local authentication type. ● isisCorruptedLSPDetected: indicates the LSP checksum error. ● isisDatabaseOverload: indicates that the LSDB overload bit changes. ● isisIDLenMismatch: indicates that the system ID length in the received packet does not match the local system ID length. ● isisLSPTooLargeToPropagate: indicates that the length of the forwarded LSP is greater than the interface MTU. ● isisManualAddressDrops: indicates that some area IDs will be dropped if the number of Level-2 area IDs exceeds 3 on the Level-1-2 router after the router advertises LSPs with Level-1 area IDs to a Level-2 area. ● isisMaxAreaAddressesMismatch: indicates that the maximum area address in the received packet does not match the local area address. ● isisOrigLSPBuffSizeMismatch: indicates that the received LSP size does not match the local buffer size. ● isisOwnLSPPurge: indicates that an IS detects that its LSPs are purged on the network. ● isisProtocolsSupportedMismatch: indicates that the protocol in the received packet is not supported by the local device. ● isisRejectedAdjacency: indicates that the PDU is received from the neighbor but the neighbor relationship cannot be established. ● isisSequenceNumberSkip: indicates that the local router receives the LSP sent by itself with the sequence number greater than that of the LSP in the local LSDB. ● isisVersionSkew: indicates that the version of the Hello packet received by IS-IS is incorrect.
Default switch status	Default status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Current status of the trap function: • on: The trap function is enabled. • off: The trap function is disabled.

Related Topics

9.6.114 snmp-agent trap enable feature-name isis

9.6.41 display snmp-agent trap feature-name isis-std all

Function

The **display snmp-agent trap feature-name isis-std all** command displays the status of the trap function in the IS-IS standard MIB.

Format

display snmp-agent trap feature-name isis-std all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the trap function has been enabled, the status is displayed as **on**. Otherwise, the status is displayed as **off**.

To change the status of the trap function, run the **snmp-agent trap enable feature-name isis-std** command to enable the trap function or run the **undo snmp-agent trap enable feature-name isis-std** command to disable the trap function.

Example

Display all trap messages of the IS-IS module.

```
<Huawei> display snmp-agent trap feature-name isis-std all
-----------------------------------------------------------------------------
Feature name: ISIS-STD
Trap number : 18
-----------------------------------------------------------------------------
```

```
Trap name                      Default switch status      Current switch status
isisDatabaseOverload             off                        on
isisManualAddressDrops           off                        on
isisCorruptedLSPDetected         off                        on
isisAttemptToExceedMaxSequence   off                        on
isisIDLenMismatch                off                        on
isisMaxAreaAddressesMismatch     off                        on
isisOwnLSPPurge                  off                        on
isisSequenceNumberSkip           off                        on
isisAuthenticationTypeFailure    off                        on
isisAuthenticationFailure        off                        on
isisVersionSkew                  off                        on
isisAreaMismatch                 off                        on
isisRejectedAdjacency            off                        on
isisLSPTooLargeToPropagate       off                        on
isisOrigLSPBuffSizeMismatch      off                        on
isisProtocolsSupportedMismatch   off                        on
isisAdjacencyChange              off                        on
isisLSPErrorDetected             off                        on
```

Table 9-122 Description of the display snmp-agent trap feature-name isis-std all command output

Item	Description
Feature name	Name of the module that trap messages belong to.
Trap number	Number of trap messages.

Item	Description
Trap name	Name of the trap message of the IS-IS module: ● isisAdjacencyChange: indicates neighbor changes. ● isisAreaMismatch: indicates that the area address of the received Level-1 Hello packet does not match the local area address. ● isisAttemptToExceedMaxSequence: indicates that the LSP sequence number is close to the maximum value. ● isisAuthenticationFailure: indicates that the authentication code in the received packet does not match the local authentication code. ● isisAuthenticationTypeFailure: indicates that the authentication type in the received packet does not match the local authentication type. ● isisCorruptedLSPDetected: indicates the LSP checksum error. ● isisDatabaseOverload: indicates that the LSDB overload bit changes. ● isisIDLenMismatch: indicates that the system ID length in the received packet does not match the local system ID length. ● isisLSPErrorDetected: indicates that an LSP with a parse error is received. ● isisLSPTooLargeToPropagate: indicates that the length of the forwarded LSP is greater than the interface MTU. ● isisManualAddressDrops: indicates that some area IDs will be dropped if the number of Level-2 area IDs exceeds 3 on the Level-1-2 router after the router advertises LSPs with Level-1 area IDs to a Level-2 area. ● isisMaxAreaAddressesMismatch: indicates that the maximum area address in the received packet does not match the local area address. ● isisOrigLSPBuffSizeMismatch: indicates that the received LSP size does not match the local buffer size. ● isisOwnLSPPurge: indicates that an IS detects that its LSPs are purged on the network. ● isisProtocolsSupportedMismatch: indicates that the protocol in the received packet is not supported by the local device. ● isisRejectedAdjacency: indicates that the PDU is received from the neighbor but the neighbor relationship cannot be established. ● isisSequenceNumberSkip: indicates that the local router receives the LSP sent by itself with the sequence number greater than that of the LSP in the local LSDB. ● isisVersionSkew: indicates that the version of the Hello packet received by IS-IS is incorrect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default switch status	Default status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.
Current switch status	Current status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

9.6.115 snmp-agent trap enable feature-name isis-std

9.6.42 domain-authentication-mode

Function

The **domain-authentication-mode** command configures an IS-IS routing domain to authenticate received Level-2 packets using the specified authentication mode and password and adds authentication information to Level-2 packets to be sent.

The **undo domain-authentication-mode** command cancels authenticating Level-2 packets and deletes the added authentication information from Level-2 packets.

By default, the system neither encapsulates generated Level-2 packets with authentication information nor authenticates received Level-2 packets.

Format

domain-authentication-mode { **simple** { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } | **md5** { [**cipher**] *plain-cipher-text* | **plain** *plain-text* } } [**ip** | **osi**] [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

domain-authentication-mode keychain *keychain-name* [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

domain-authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**snp-packet** { **authentication-avoid** | **send-only** } | **all-send-only**]

undo domain-authentication-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
simple	Transmits the password in plain text. **NOTICE** Simple authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
plain *plain-text*	Specifies the authentication password in plain text. You can enter only the password in plain text. When you view the configuration file, the password is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters.
cipher *plain-cipher-text*	Specifies the authentication password in cipher text. You can enter the password in plain or cipher text. When you view the configuration file, the password is displayed in cipher text. By default, the password is in cipher text.	The value is a string of case-sensitive characters without spaces. The value contains digits and letters. When the authentication mode is **simple**, the value is a string of 1 to 16 characters in plain text or a string of 32 or 48 characters in cipher text. When the authentication mode is **md5** or **hmac-sha256**, the value is a string of 1 to 255 characters in plain text or a string of 20 to 392 characters in cipher text.
md5	Transmits the password that is encrypted using MD5. **NOTICE** MD5 authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
keychain *keychain-name*	Indicates that the password is a keychain that changes with time. This parameter takes effect only when *keychain-name* is set using the **19.20.4 keychain** command. If keychain authentication is used, the encryption algorithm must be configured to HMAC-MD5 or HMAC-SHA-256 algorithm.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
ip	Indicates the IP authentication password. When neither **ip** nor **osi** is specified, the default parameter **osi** is used.	-
osi	Indicates the OSI authentication password. When neither **ip** nor **osi** is specified, the default parameter **osi** is used.	-
snp-packet	Authenticates SNPs.	-
authentication-avoid	Encapsulates generated LSPs but not SNPs with authentication information and authenticates received LSPs but not SNPs.	-
send-only	Encapsulates generated LSPs and SNPs with authentication information, and authenticates received LSPs but not SNPs.	-
all-send-only	Encapsulates generated LSPs and SNPs with authentication information, but does not authenticate received LSPs and SNPs.	-
hmac-sha256	Encapsulates generated packets with the HMAC-SHA256 authentication and a password encrypted by the HMAC-SHA256 algorithm and authenticates received packets.	-
key-id *key-id*	Indicates key ID of the HMAC-SHA256 algorithm.	It is an integer ranging from 0 to 65535.

Views

IS-IS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IS-IS packets to be sent are not encapsulated with authentication information, and the received packets are not authenticated. If a user sends malicious packets to attack a network, information on the entire network may be stolen. Therefore, you can configure IS-IS authentication to improve the network security.

The domain authentication password is encapsulated into Level-2 IS-IS packets. Only the packets that pass the domain authentication can be accepted. Therefore, you can configure IS-IS domain authentication to authenticate Level-2 area.

Precautions

This command is valid in all the topologies in the specified IS-IS process and is only valid for Level-2 or Level-1-2 routers.

By using this command, you can discard all the Level-2 packets whose domain authentication password does not contain the one set through this command. At the same time, IS-IS adds the configured domain authentication password in all the Level-2 packets carrying routing information sent from the local node.

The authentication takes effect on the interface with the password. The port without the password can still receive the LSP and SNP with password.

Example

Set the domain authentication mode to HMAC-SHA256, authentication password to **admin@huawei**, and key id to **33** to authenticate Level-2 packets.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] domain-authentication-mode hmac-sha256 key-id 33 cipher admin@huawei
```

Related Topics

9.6.2 area-authentication-mode

9.6.57 isis authentication-mode

9.6.43 filter-policy export (IS-IS)

Function

The **filter-policy export** command configures a filtering policy to allow IS-IS to filter the imported routes to be advertised.

The **undo filter-policy export** command cancels the filtering function.

By default, IS-IS does not filter the imported routes to be advertised.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix-list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the imported routes that need to be filtered when the routes are advertised. If this parameter is not specified, all the imported routes to be advertised are filtered.	The value can be **direct**, **static**, **rip**, **bgp**, **unr**, **ospf**, or another **isis** process.
process-id	Specifies the process ID if *protocol* is **rip**, **ospf**, or another **isis** process.	The value is an integer that ranges from 1 to 65535.

Views

IS-IS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When IS-IS and other routing protocols are running on the network, and a boundary router in the IS-IS routing domain has imported routes of other routing protocols, the boundary router will advertise all the imported routes to its IS-IS neighbors by default. To advertise some of the imported routes to neighbors, use the **filter-policy export** command.

Precautions

Running the **filter-policy export** command does not affect the routes on the local device, but only advertises specific imported routes to IS-IS neighbors.

For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Configure IS-IS to filter the imported routes using ACL 2000 before advertising the routes to other routers.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] filter-policy 2000 export
```

Related Topics

9.6.53 import-route (IS-IS)

9.7.7 ipv6 filter-policy export

9.6.44 filter-policy import (IS-IS)

Function

The **filter-policy import** command configures a filtering policy to allow IS-IS to filter the received routes to be added to the IP routing table.

The **undo filter-policy import** command cancels the filtering function.

By default, IS-IS does not filter the received routes to be added to the IP routing table.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name*] **import**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS routing entries need to be added to an IP routing table to guide IP packet forwarding. If an IS-IS routing table has routes destined for a specific network segment, but these routes are not expected to be added to an IP routing table, run the **filter-policy import** command with specified parameters to allow only the needed IS-IS routes to be added to the IP routing table.

Precautions

Running the **filter-policy import** command on a router does not affect LSP flooding and LSDB synchronization on the router, but affects the local IP routing table.

For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure IS-IS to filter the received routes using ACL 2000 and add the routes matching the filtering conditions to the IP routing table.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] filter-policy 2000 import
```

Related Topics

9.6.43 filter-policy export (IS-IS)

9.7.8 ipv6 filter-policy import

9.6.45 flash-flood

Function

The **flash-flood** command enables LSP fast flooding to speed up IS-IS network convergence.

The **undo flash-flood** command disables LSP fast flooding.

By default, LSP fast flooding is disabled.

Format

flash-flood [*lsp-count* | **max-timer-interval** *interval* | [**level-1** | **level-2**]] *

undo flash-flood [*lsp-count* | **max-timer-interval** *interval* | [**level-1** | **level-2**]] *

Parameters

Parameter	Description	Value
lsp-count	Specifies the maximum number of LSPs to be flooded at a time on an interface.	The value is an integer that ranges from 1 to 15. The default value is 5.
max-timer-interval *interval*	Specifies the maximum interval for LSP flooding.	The value is an integer that ranges from 10 to 50000, in milliseconds. The default value is 10 ms.
level-1	Enables LSP fast flooding in Level-1. If no level is specified, by default, LSP fast flooding is enabled in both Level-1 and Level-2.	-
level-2	Enables LSP fast flooding in Level-2. If no level is specified, by default, LSP fast flooding is enabled in both Level-1 and Level-2.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In most cases, when an IS-IS router receives new LSPs from other routers, it updates the LSPs in its LSDB and periodically floods the updated LSPs according to a timer.

LSP fast flooding speeds up LSDB synchronization because it allows a device to flood fewer LSPs than the specified number before route calculation when the device receives one or more new LSPs. This mechanism also speeds up network convergence.

Precautions

You can specify the number of LSPs to be flooded each time. The number is valid for all IS-IS interfaces. If the number of LSPs to be flooded is greater than the specified value, the *lsp-count* number of the LSPs are sent. If the timer is configured and does not time out before route calculation, LSPs are flooded immediately; otherwise, LSPs are flooded when the timer times out.

Example

Enable LSP fast flooding, configure each interface to send a maximum of six LSPs at a time, and set the maximum interval for sending LSPs to 100 ms.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] flash-flood 6 max-timer-interval 100
```

9.6.46 frr (IS-IS)

Function

The **frr** command enables the IS-IS Fast Reroute (FRR) function and displays the IS-IS FRR view.

The **undo frr** command disables the IS-IS FRR function.

By default, the IS-IS FRR function is disabled.

Format

frr

undo frr

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

With the development of networks, the Voice over IP (VoIP) and on-line video services require high-quality real-time transmission. Nevertheless, if an IS-IS fault occurs, multiple processes, including fault detection, LSP update, LSP flooding, route calculation, and FIB entry delivery, must be performed to switch traffic to a new link. As a result, the traffic interruption time is much greater than 50 ms, which cannot meet the requirement for real-time services.

IS-IS Auto FRR can fast switch traffic to a backup link, ensuring that the traffic interruption time is within 50 ms. This protects traffic and improves IS-IS network reliability.

Precautions

After running this command, run the **loop-free-alternate** command to calculate a loop-free backup route.

Example

Enter the IS-IS FRR view.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] frr
[Huawei-isis-1-frr] loop-free-alternate
```

Related Topics

9.6.97 loop-free-alternate

9.6.69 isis lfa-backup

9.6.47 frr-policy route

Function

The **frr-policy route** command configures a filtering policy to allow IS-IS to filter the IS-IS backup routes to be added in the IP routing table.

The **undo frr-policy route** command cancels the filtering function.

By default, IS-IS does not filter the IS-IS backup routes to be added in the IP routing table.

 Copyright © Huawei Technologies Co., Ltd.

Format

frr-policy route route-policy *route-policy-name*

undo frr-policy route

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy to filter IS-IS backup routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The filtering policy can be configured as required. In this case, the IS-IS backup route that satisfies specified rules can be added to the IP routing table and delivered to the forwarding table. When a fault occurs on the route, the system can fast switch the forwarded traffic to the IS-IS backup route to protect traffic.

You can use IP prefix lists or ACLs to filter IS-IS backup routes.

Precautions

If you run the **frr-policy route** command multiple times, only the latest configuration takes effect.

Example

Configure IS-IS to filter IS-IS backup routes using named ACL **abc** and add the routes matching the ACL to the IP routing table.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] frr
[Huawei-isis-1-frr] frr-policy route route-policy abc
```

Related Topics

9.6.46 frr (IS-IS)

9.6.48 graceful-restart (IS-IS)

Function

The **graceful-restart** command enables the graceful restart (GR) function for an IS-IS process.

The **undo graceful-restart** command disables the GR function for an IS-IS process.

By default, the GR function is disabled for an IS-IS process.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an IS-IS process on a device is restarted, neighbors delete neighbor relationships with the device and delete LSPs from the device. As a result, routes of neighbors are calculated incorrectly and packets are lost. Consequently, the network is temporarily interrupted.

After the **graceful-restart** command is run, the GR function is enabled. The device notifies its restart status to neighbors and permits neighbors to maintain neighbor relationships so that traffic forwarding is not interrupted.

Configuration Impact

If IS-IS GR is enabled on a router, the holdtimes of this router's neighbors are automatically changed to 60s if they are smaller than 60s, and the holdtimes of this router's neighbors are kept unchanged if they are equal to or greater than 60s. If a router is faulty in non-GR scenarios, its neighbors need to take 60 seconds to detect the fault. A large number of packets may be discarded within the 60 seconds.

To resolve this problem, run the **graceful-restart no-impact-holdtime** command to configure the holdtimes of the neighbors to remain unchanged after IS-IS GR is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the GR function for IS-IS process 1.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] graceful-restart
```

Related Topics

9.6.50 graceful-restart interval

9.6.51 graceful-restart suppress-sa

9.6.49 graceful-restart no-impact-holdtime

Function

The **graceful-restart no-impact-holdtime** command configures the holdtime of an IS-IS neighbor to remain unchanged after IS-IS GR is enabled.

The **undo graceful-restart no-impact-holdtime** command cancels the configuration.

By default, after IS-IS GR is enabled, the holdtime of an IS-IS neighbor is automatically changed to 60s if it is smaller than 60s, and the holdtime of an IS-IS neighbor is kept unchanged if it is equal to or greater than 60s.

Format

graceful-restart no-impact-holdtime

undo graceful-restart no-impact-holdtime

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If IS-IS GR is enabled on a router, the holdtimes of this router's neighbors are automatically changed to 60s if they are smaller than 60s, and the holdtimes of this router's neighbors are kept unchanged if they are equal to or greater than 60s. If a router is faulty in non-GR scenarios, its neighbors need to take 60 seconds to detect the fault. A large number of packets may be discarded within the 60 seconds.

 Copyright © Huawei Technologies Co., Ltd.

To resolve this problem, run the **graceful-restart no-impact-holdtime** command to configure the holdtimes of the neighbors to remain unchanged after IS-IS GR is enabled. After you run this command, the router can still fast detect neighbor status, implementing rapid network convergence.

Prerequisites

You have run the **graceful-restart (IS-IS)** command in the IS-IS view.

Example

Configure the holdtime of an IS-IS neighbor to remain unchanged after IS-IS GR is enabled.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] graceful-restart
[Huawei-isis-1] graceful-restart no-impact-holdtime
```

Related Topics

9.6.48 graceful-restart (IS-IS)

9.6.50 graceful-restart interval

Function

The **graceful-restart interval** command sets the GR T3 timer.

The **undo graceful-restart interval** command restores the default T3 timer.

By default, the GR T3 timer is 300 seconds.

Format

graceful-restart interval *interval-value*

undo graceful-restart interval

Parameters

Parameter	Description	Value
interval-value	Specifies the GR T3 timer.	The value is an integer that ranges from 30 to 1800, in seconds. Setting a value greater than that of the GR T2 timer specified using the **graceful-restart t2-interval** command is recommended. If the value is smaller than that of the GR T2 timer, the GR may fail.

Views

IS-IS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS GR can be classified into restarting GR and starting GR based on the restart type. The restarting GR is triggered by a master/slave main control board switchover or an IS-IS process restart, while the starting GR is triggered by a restart of the IS-IS-enabled router.

During a restarting GR, the restarter restarts the protocol and starts the T1, T2, and T3 timers at the same time. The value of the T1 timer indicates the longest time during which the GR restarter waits for the LSP from the GR helper. The value of the T2 timer indicates the longest time during which the system waits for the LSDB synchronization. The value of the T3 timer indicates the longest time that a GR lasts. A router disables the T3 timer after the LSDB synchronization ends in all areas. If LSDBs are not synchronized yet when the T3 timer expires, the GR fails.

You can run the **graceful-restart interval** command to adjust the value of the T3 timer so that the LSDB synchronization can end before the T3 timer expires, which prevents the GR failure.

Prerequisites

The GR of the IS-IS process has been enabled using the **graceful-restart** command.

Configuration Impact

If the **graceful-restart interval** command is run on an IS-IS-enabled router, *interval-value* is used as the holdtime of its neighbor.

Precautions

The **graceful-restart interval** command is applicable only to restarting GRs.

Example

Set the GR interval for IS-IS process 1 to 120 seconds (2 minutes).

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] graceful-restart
[Huawei-isis-1] graceful-restart interval 120
```

Related Topics

9.6.48 graceful-restart (IS-IS)

9.6.51 graceful-restart suppress-sa

Function

The **graceful-restart suppress-sa** command suppresses the suppress-advertisement (SA) bit of the restart TLV.

The **undo graceful-restart suppress-sa** command restores the default setting.

By default, the SA bit of the restart TLV is not suppressed.

Format

graceful-restart suppress-sa

undo graceful-restart suppress-sa

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The router that starts for the first time (not including GR) does not maintain the forwarding status. If the router does not start for the first time, the LSPs generated when the router run last time may exist in the LSP database of other routers in the network.

The sequence number of the LSP fragment is reinitialized when the router starts, so the LSPs stored in the LSP database of other routers seem to be newer than the LSPs generated after the router starts. This leads to the black hole in the network, and the black hole lasts until the router regenerates its LSPs and advertises the LSPs with the highest sequence number.

If the neighbor suppresses the advertisement of the adjacency relationship to this router during the router starting until the router advertises the updated LSPs, the preceding case can be avoided.

Prerequisites

GR has been enabled for the IS-IS process using the **graceful-restart** command.

Example

Suppress the SA bit in the restart TLV of IS-IS process 1.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] graceful-restart
[Huawei-isis-1] graceful-restart suppress-sa
```

Related Topics

9.6.48 graceful-restart (IS-IS)

9.6.52 graceful-restart t2-interval

Function

The **graceful-restart t2-interval** command configures a value for the T2 timer during an IS-IS GR.

The **undo graceful-restart t2-interval** command restores the default value of the T2 timer.

By default, the GR T2 timer is 60 seconds.

Format

graceful-restart t2-interval *interval-value*

undo graceful-restart t2-interval

Parameters

Parameter	Description	Value
interval-value	Specifies the value of the T2 timer during the IS-IS GR.	The value is an integer that ranges from 30 to 1800, in seconds. Setting a value smaller than that of the GR T3 timer specified using the **graceful-restart interval** command is recommended.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS GR can be classified into restarting GR and starting GR based on the restart type. The restarting GR is triggered by a master/slave main control board switchover or an IS-IS process restart, while the starting GR is triggered by a restart of the IS-IS-enabled router.

 Copyright © Huawei Technologies Co., Ltd.

A GR restarter starts the T1 and T2 timers during all GRs. The value of the T1 timer indicates the longest time during which the GR restarter waits for the LSP from the GR helper. The value of the T2 timer indicates the longest time during which the system waits for the LSDB synchronization. The T2 timer is disabled after the LSDB synchronization among Level-1 or Level-2 routers ends. If LSDBs are not synchronized yet when the T2 timer expires, the GR fails.

You can run the **graceful-restart t2-interval** command to adjust the value of the T2 timer so that the LSDB synchronization can end before the T2 timer expires, which prevents the GR failure.

Prerequisites

The GR of the IS-IS process has been enabled using the **graceful-restart** command.

Precautions

If the value of the T2 timer is too small, a GR may fail. Keeping the default value is recommended. If you want to adjust it, configure a value to meet the conditions on the live network.

Example

Set the GR T2 timer of IS-IS process 1 to 120 seconds (2 minutes).

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] graceful-restart
[Huawei-isis-1] graceful-restart t2-interval 120
```

Related Topics

9.6.50 graceful-restart interval

9.6.53 import-route (IS-IS)

Function

The **import-route** command configures IS-IS to import routes from other routing protocols.

The **undo import-route** command restores the default setting.

By default, IS-IS does not import routes from other routing protocols.

Format

import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **static** | **direct** | **unr** | **bgp** [**permit-ibgp**] } [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **direct** | **unr** | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

import-route limit *limit-number* [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

undo import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **static** | **direct** | **unr** | **bgp** [**permit-ibgp**] } [**cost-type** { **external** | **internal** } | **cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo import-route { { **rip** | **isis** | **ospf** } [*process-id*] | **direct** | **unr** | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo import-route limit [*limit-number*] [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

Parameters

Parameter	Description	Value
rip	Indicates that the routing protocol from which routes are imported is RIP.	-
isis	Indicates that the routing protocol from which routes are imported is IS-IS.	-
ospf	Indicates that the routing protocol from which routes are imported is OSPF.	-
process-id	Specifies a process ID. When *protocol* is **rip**, **ospf**, or **isis**, a process ID needs to be specified. The default process ID is 1.	The value is an integer that ranges from 1 to 65535.
static	Indicates that the imported routes are active static routes.	-
direct	Indicates that the imported routes are direct routes.	-
unr	Specifies the imported source routing protocol as **unr**. User Network Route (UNR) is allocated if dynamic routing protocols cannot be used when users are getting online.	-
bgp	Indicates that the routing protocol from which routes are imported is BGP. **NOTE** IS-IS can only import EBGP routes but not IBGP routes.	-
permit-ibgp	Specifies the imported source route as an IBGP route. If you do not configure this parameter, only the EBGP routes are imported.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cost-type { **external** | **internal** }	Specifies the cost type of imported routes. The default cost type is **external**. The configuration of this parameter affects the cost value of imported routes: ● If the cost type of an imported route is set to **external** the new route cost value equals the imported route cost value (the default cost value is 0) plus 64. ● If the cost type of an imported route is set to **internal**, the new route cost value equals the imported route cost value (the default cost value is 0). **NOTE** If the cost style of the router is wide, compatible, or wide-compatible, the cost types of imported routes are not differentiated between **external** and **internal**.	-
cost *cost*	Specifies the cost value of imported routes.	If the cost style of the router is wide or wide-compatible, the cost value of imported routes ranges from 0 to 4261412864. Otherwise, the value ranges from 0 to 63. The default value is 0.
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
level-1	Indicates that routes are imported into Level-1 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-

Parameter	Description	Value
level-2	Indicates that routes are imported into Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
level-1-2	Indicates that routes are imported into Level-1 and Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
inherit-cost	Indicates that the original cost value of imported external routes is retained. When IS-IS is configured to retain the original cost value of imported routes, the cost style and cost value cannot be set for the imported routes.	-
limit *limit-number*	Specifies the maximum number of external routes allowed to be imported to the IS-IS area.	The value is an integer ranging from 1 to 10000000.
threshold-alarm	Specifies the alarm threshold for imported routes.	-
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 80.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 70.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IS-IS and other routing protocols are deployed on a network, you can enable the traffic within an IS-IS routing domain to reach a destination outside the IS-IS routing domain using either of the following methods:

- Configure boundary devices in the IS-IS routing domain to advertise default routes to the IS-IS routing domain.
- Configure boundary devices in the IS-IS routing domain to import routes from other routing domains into the IS-IS routing domain.

 Copyright © Huawei Technologies Co., Ltd.

If there are multiple boundary devices in the IS-IS routing domain, optimal routes destined for another routing domain need to be selected. This requires all devices in the IS-IS routing domain learn all or some external routes. Configure boundary devices in the IS-IS routing domain to import routes from other routing domains into the IS-IS routing domain. Alternatively, run the **route-policy** *route-policy-name* command to import some external routes from other routing domains.

Precautions

When the routes of the other protocols are imported, you can set the cost value and cost style for the imported route. You can also configure IS-IS to retain the original cost value of the imported external route. During route advertisement and route calculation, the original cost values of these routes are used. In this case, the cost style and cost value of the imported routes cannot be set, and static routes cannot be imported.

After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the ISIS routing table. Therefore, use this command with caution.

Example

Configure IS-IS to import static routes and set the cost value of the routes to 15.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] import-route static cost 15
```

Configure IS-IS to import OSPF routes and retain the original cost value of the routes.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] import-route ospf inherit-cost
```

Related Topics

9.6.43 filter-policy export (IS-IS)
9.7.9 ipv6 import-route

9.6.54 import-route isis level-1 into level-2

Function

The **import-route isis level-1 into level-2** command configures route leaking from Level-1 areas to Level-2 areas.

The **undo import-route isis level-1 into level-2** command prohibits route leaking from Level-1 areas to Level-2 areas.

By default, all Level-1 routing information, excluding information about default routes, is leaked to Level-2 areas.

Format

import-route isis level-1 into level-2 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

undo import-route isis level-1 into level-2 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy.	-
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list. Only the routes that match the IP prefix can be leaked to Level-2 areas.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the administrative tag value of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Specifies the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can be shared with the Level-2 area with this parameter, and all Level-1 area direct routing information will be shared with the Level-2 area without this parameter.	-

Views

IS-IS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS is designed for a hierarchical network. This means that routes of Level-1 areas are leaked to Level-2 areas, whereas routes of Level-2 areas are not leaked to Level-1 areas.

The import-route isis level-1 into level-2 command can be run only on Level-1-2 routers to allow some or no Level-1 routes to be leaked to Level-2 areas. For example, there are two Level-1-2 routers in a Level-1 area. You can run the import-route isis level-1 into level-2 command on one Level-1-2 router to allow some Level-1 routes to be leaked to the Level-2 area, and run the import-route isis level-1 into level-2 command on the other Level-1-2 router to allow the remaining Level-1 routes to be leaked to the Level-2 area. Then, traffic that is sent from the Level-2 area and destined for different network segments in Level-1 area will be forwarded to different Level-1-2 routers. This allows route selection to be controlled.

Precautions

For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Control route leaking from Level-1 areas to Level-2 areas on Level-1-2 routers using filtering policy 2000.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] import-route isis level-1 into level-2 filter-policy 2000
```

Related Topics

9.6.55 import-route isis level-2 into level-1

9.6.55 import-route isis level-2 into level-1

Function

The **import-route isis level-2 into level-1** command configures route leaking from Level-2 areas to Level-1 areas.

The **undo import-route isis level-2 into level-1** command prohibits route leaking from Level-2 areas to Level-1 areas.

By default, Level-2 routing information is not leaked to Level-1 areas.

 Copyright © Huawei Technologies Co., Ltd.

Format

import-route isis level-2 into level-1 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

undo import-route isis level-2 into level-1 [**filter-policy** { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy.	-
acl-number	Specifies the number of a basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list. Only the routes that match the specified IP prefix can be imported.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the administrative tag value of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Indicates the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can leak to the Level-2 area with this parameter, and all Level-1 area direct routing information is available to the Level-2 area without this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
direct allow-up-down-bit	Indicates that the Up or Down bit is used during the leak of directs routes. If **direct allow-up-down-bit** is specified, the direct routes that have already leaked to the Level-1 area have the lowest priority and cannot leak back.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple Level-1-2 routers in a Level-1 area are connected to a Level-2 area, Level-1 routers are unable to know the network topology of the Level-2 area, but forward traffic to the nearest Level-1-2 router (based on the route with the smallest cost). For Level-2 routers, however, this route may not be the optimal one. Therefore, you need to allow some Level-2 routes to be leaked to the Level-1 area to help Level-1 routers select the optimal route for forwarding traffic to the Level 2 area.

To solve the preceding problem, IS-IS provides the route leaking function to enable Level-1 devices to choose the best path for traffic forwarding.

The **import-route isis level-2 into level-1** command can be run only on Level-1-2 routers to allow all or some Level-2 routes to be leaked to the Level-1 area.

Precautions

For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Configure IS-IS to perform route leaking from a Level-2 area to a Level-1 area using filtering policy 2000.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] import-route isis level-2 into level-1 filter-policy 2000
```

Related Topics

9.6.54 import-route isis level-1 into level-2
9.7.11 ipv6 import-route isis level-2 into level-1

9.6.56 isis

Function

The **isis** command starts an IS-IS process and a specified VPN instance, and displays the IS-IS view.

The **undo isis** command deletes a specified IS-IS process.

By default, no IS-IS instance exists on the network.

Format

isis [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo isis *process-id*

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure other functions and features of the interface, you need to enable IS-IS first. You can enter the IS-IS view after the command is used.

In addition, to ensure that different services are forwarded properly on the network, you can run the **isis** command to start multiple IS-IS processes on one device to isolate these services.

Precautions

One IS-IS process can be bound to only one VPN instance. Multiple IS-IS interfaces can be bound to one VPN instance.

If a VPN instance is deleted, the IS-IS process bound to the VPN instance is deleted.

When creating an IS-IS process, you need to bind it to a VPN instance. If the IS-IS process is not bound to any VPN instance when it is created, it cannot be bound to any VPN instance later through configuration.

Example

Bind IS-IS process 2 to VPN instance **vpn1**.

```
<Huawei> system-view
[Huawei] isis 2 vpn-instance vpn1
```

Related Topics

9.6.68 isis enable

9.6.101 network-entity

9.6.57 isis authentication-mode

Function

The **isis authentication-mode** command configures an IS-IS interface to authenticate Hello packets using the specified mode and password.

The **undo isis authentication-mode** command cancels the authentication and deletes the authentication information in Hello packets.

By default, no authentication information is added to Hello packets and no authentication is performed on received Hello packets.

Format

isis authentication-mode { **simple** | **md5** } { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]

isis authentication-mode keychain *keychain-name* [**level-1** | **level-2**] [**send-only**]

isis authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | [**cipher**] *plain-cipher-text* } [**level-1** | **level-2**] [**send-only**]

undo isis authentication-mode [**level-1** | **level-2**]

undo isis authentication-mode keychain *keychain-name* [**level-1** | **level-2**] [**send-only**]

undo isis authentication-mode { **simple** { **plain** *plain-text* | **cipher** *plain-cipher-text* } | **md5** { **cipher** *plain-cipher-text* | **plain** *plain-text* } } [**level-1** | **level-2**] [**ip** | **osi**] [**send-only**]

undo isis authentication-mode hmac-sha256 key-id *key-id* { **plain** *plain-text* | **cipher** *plain-cipher-text* } [**level-1** | **level-2**] [**send-only**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
simple	Indicates that the password is transmitted in plain text. **NOTICE** Simple authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-
plain *plain-text*	Indicates that the password is in plain text. Only a plain-text password can be entered. The password in the configuration file is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. In **simple** authentication mode, the value is a string of 1 to 16 characters. In **md5** or **hmac-sha256** authentication mode, the value is a string of 1 to 255 characters.
cipher *plain-cipher-text*	Indicates that the password is in cipher text. A plain-text or cipher-text password can be entered. The password in the configuration file is displayed in cipher text. By default, the password is in cipher text.	The value is a string of case-sensitive characters. It contains letters and digits without spaces. In **simple** authentication mode, the value is a string of 1 to 16 characters in plain text or a string of 32 or 48 characters in cipher text. In **md5** or **hmac-sha256** authentication mode, the value is a string of 1 to 255 characters in plain text or a string of 20 to 392 characters in cipher text.
md5	Indicates that the password to be transmitted is encrypted using MD5. **NOTICE** MD5 authentication has potential risks. HMAC-SHA256 cipher text authentication is recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
level-1	Indicates Level-1 authentication. When the link type of an IS-IS interface is Level-1-2, if **level-1** and **level-2** are not specified, both Level-1 and Level-2 Hello packets are configured with the authentication mode and password.	-
level-2	Indicates Level-2 authentication. When the link type of an IS-IS interface is Level-1-2, if **level-1** and **level-2** are not specified, both Level-1 and Level-2 Hello packets are configured with the authentication mode and password. **NOTE** Parameters **level-1** and **level-2** are only visible on WAN-side Ethernet interfaces and LAN-side VLANIF interfaces. IS-IS must have been enabled on the interfaces first.	-
ip	Indicates the IP authentication password. This parameter cannot be configured in keychain authentication mode. If parameters **ip** and **osi** are not specified, the parameter **osi** is used by default.	-
osi	Indicates the OSI authentication password. This parameter cannot be configured in **keychain** authentication mode. If parameters **ip** and **osi** are not specified, the parameter **osi** is used by default.	-
send-only	Encapsulates sent Hello packets with authentication information but does not authenticate received Hello packets.	-
keychain *keychain-name*	Indicates that the password is a keychain that changes with time. This parameter takes effect only when *keychain-name* is set using the **19.20.4 keychain** command.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
hmac-sha256	Encapsulates generated packets with the HMAC-SHA256 authentication and a password encrypted by the HMAC-SHA256 algorithm and authenticates received packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-id *key-id*	Indicates key ID of the HMAC-SHA256 algorithm.	It is an integer ranging from 0 to 65535.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve network security, authenticate received packets or encapsulate sent packets with authentication information. Only the packets that pass the authentication can be transmitted on the network.

You can use the **isis authentication-mode** command to discard the Hello packets whose authentication passwords are different from the authentication password configured using this command. At the same time, IS-IS adds the configured interface authentication password into all the Hello packets sent from the local node.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If a broadcast interface is emulated as a P2P interface using the **isis circuit-type** command and then restored to the broadcast interface using the **undo isis circuit-type** command, the authentication configuration of the IS-IS area is restored to the default setting.

Example

Set HMAC-SHA256 authentication password **admin@huawei** key id **33** on GE1/0/0

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis authentication-mode hmac-sha256 key-id  33 cipher admin@huawei
```

Related Topics

9.6.2 area-authentication-mode

9.6.42 domain-authentication-mode

19.20.4 keychain

 Copyright © Huawei Technologies Co., Ltd.

9.6.58 isis bfd

Function

The **isis bfd** command sets values of BFD session parameters on a specified IS-IS interface.

The **undo isis bfd** command restores the default values of BFD session parameters on a specified IS-IS interface.

By default, BFD session parameters use default values.

Format

isis bfd { **min-rx-interval** *receive-interval* | **min-tx-interval** *transmit-interval* | **detect-multiplier** *multiplier-value* | **frr-binding** } *

undo isis bfd { **min-rx-interval** [*receive-interval*] | **min-tx-interval** [*transmit-interval*] | **detect-multiplier** [*multiplier-value*] | **frr-binding** } *

Parameters

Parameter	Description	Value
min-rx-interval *receive-interval*	Specifies the minimum interval for receiving BFD packets from the peer end.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-tx-interval *transmit-interval*	Specifies the minimum interval for transmitting BFD packets to the peer end.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
detect-multiplier *multiplier-value*	Specifies the local detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.
frr-binding	Binds the BFD session status to IS-IS Auto FRR. When BFD detects the link fault on an interface, the BFD session goes Down, triggering FRR on the interface. After that, the traffic is switched from the faulty link to the backup link, which protects the traffic. **NOTE** The AR150&AR160&AR200 series do not support this parameter.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD can quickly detect faults on links. Configure proper parameters based on the actual network situation to improve the IS-IS convergence speed when network faults occur. You can use the **isis bfd** command to change BFD session parameters such as the minimum interval for sending BFD packets, minimum interval for receiving BFD packets, and local detection multiplier.

In an IS-IS process, after IS-IS establishes a BFD session, the value of *receive-interval* is obtained after the negotiation of the local **min-rx-interval** value and the remote **min-tx-interval** value. If no BFD packet is received from the peer end within the specified period (*receive-interval* x *multiplier-value*), the neighbor is considered Down.

Negotiation principle: Actual interval for the local device to receive BFD packets = MAX {local **min-rx-interval** value, remote **min-tx-interval** value}

Prerequisites

BFD has been enabled globally. In the interface view, IS-IS has been enabled and BFD has been enabled on the interface using the **isis bfd enable** command.

Precautions

The BFD priority of the interface is higher than that of the process. If BFD of the interface is enabled, the BFD session is set up based on the BFD parameters on the interface.

Example

Enable BFD on GE1/0/0 and set the minimum receive interval to 600 ms and local detection multiplier to 4.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis bfd enable
[Huawei-GigabitEthernet1/0/0] isis bfd min-rx-interval 600 detect-multiplier 4
```

Enable BFD on IS-IS interface and bind the status of the BFD session to IS-IS Auto FRR.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis bfd enable
[Huawei-GigabitEthernet1/0/0] isis bfd frr-binding
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.6.60 isis bfd enable
9.6.59 isis bfd block
9.6.61 isis bfd static

9.6.59 isis bfd block

Function

The **isis bfd block** command prevents an IS-IS interface from dynamically establishing a BFD session.

The **undo isis bfd block** command restores the default setting.

By default, an interface can dynamically establish a BFD session.

Format

isis bfd block

undo isis bfd block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD can provide millisecond-level fault detection, help IS-IS rapidly detect the faults that occur on neighboring devices or links, and instruct IS-IS to recalculate routes for correct packet forwarding. If the network contains unstable links that do not require high reliability and BFD has been enabled, a link cannot transmit data normally when it flaps. You can use the **isis bfd block** command to prevent specified interfaces from dynamically establishing BFD sessions.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If the **isis bfd block**, **isis bfd enable**, and **isis bfd static** commands are executed, only the last command takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Prevent GE1/0/0 from dynamically establishing a BFD session.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis bfd block
```

Related Topics

9.6.60 isis bfd enable
9.6.61 isis bfd static

9.6.60 isis bfd enable

Function

The **isis bfd enable** command enables BFD on a specified IS-IS interface.

The **undo isis bfd enable** command disables BFD on a specified IS-IS interface.

By default, BFD is not enabled on an IS-IS interface.

Format

isis bfd enable

undo isis bfd enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD can provide millisecond-level fault detection, help IS-IS to detect the faults that occur on neighboring devices or links more rapidly, and instruct IS-IS to recalculate routes for correct packet forwarding. The **isis bfd enable** command can be used to enable BFD on a specified IS-IS interface and establish BFD sessions by using default parameters.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If global BFD is not enabled, you can configure BFD parameters on an interface but cannot establish a BFD session.

The BFD priority of the interface is higher than the BFD priority of the process. If BFD of the interface is enabled, the BFD session is set up based on the BFD parameters on the interface.

If the **isis bfd block**, **isis bfd enable**, and **isis bfd static** commands are run, only the last command takes effect.

Example

Enable BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis bfd enable
```

Related Topics

18.5.2 bfd

9.6.58 isis bfd

9.6.59 isis bfd block

9.6.61 isis bfd static

9.6.61 isis bfd static

Function

The **isis bfd static** command enables static BFD on a specified IS-IS interface.

The **undo isis bfd static** command disables static BFD on a specified IS-IS interface.

By default, static BFD is disabled on an IS-IS interface.

Format

isis bfd static

undo isis bfd static

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In static BFD, BFD session parameters are set manually and BFD session establishment requests are delivered manually. Then static BFD can quickly detect faults on links. You can run the **isis bfd static** command to enable static BFD on a specified interface to establish static BFD sessions on specified links.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If the **isis bfd block**, **isis bfd enable**, and **isis bfd static** commands are run, only the last command takes effect.

Example

Enable static BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis bfd static
```

Related Topics

9.6.59 isis bfd block

9.6.60 isis bfd enable

9.6.62 isis circuit-level

Function

The **isis circuit-level** command sets the link type of an interface on a Level-1-2 router.

The **undo isis circuit-level** command restores the default link type of an interface on a Level-1-2 router.

By default, the link type of an interface on a Level-1-2 router is Level-1-2, and both Level-1 and Level-2 neighbor relationships can be established on the interface.

Format

isis circuit-level [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
level-1	Specifies the Level-1 link type. That is, only Level-1 neighbor relationship can be established on the interface.	-
level-1-2	Specifies the Level-2 link type. That is, both Level-1 and Level-2 neighbor relationships can be established on the interface.	-
level-2	Specifies the Level-2 link type. That is, only Level-2 neighbor relationship can be established on the interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an adjacency is established between a Level-1-2 router and a remote device, the Level-1-2 router sends and receives both Level-1 and Level-2 Hello packets, wasting bandwidth and memory resources. To solve this problem, run the **isis circuit-level** command to set a specified link type for an interface.

Prerequisites

IS-IS has been enabled using the **isis enable** command in the interface view.

Precautions

Network flapping may occur if the link type of an IS-IS interface is changed during network operation. Therefore, setting a link type for an IS-IS interface on the router when configuring IS-IS is recommended.

The configuration of the **isis circuit-level** command takes effect only when the IS-IS system type is Level-1-2. Otherwise, the level configured using the **is-level** command is used as the link type.

Example

If GE1/0/0 is connected to a non-backbone router in the same area, set this interface to Level-1, and prohibit the interface from sending and receiving Level-2 Hello packets.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis circuit-level level-1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.6.68 isis enable
9.6.91 is-level

9.6.63 isis circuit-type

Function

The **isis circuit-type** command simulates the network type of an IS-IS broadcast interface to a P2P interface.

The **undo isis circuit-type** command restores the default network type of an IS-IS interface.

By default, the network type of an interface is determined by the physical type of the interface.

Format

isis circuit-type p2p [**strict-snpa-check**]

undo isis circuit-type

Parameters

Parameter	Description	Value
p2p	Sets the network type of an IS-IS interface to P2P.	-
strict-snpa-check	Enables IS-IS to check the SNPA address of each received LSP or SNP.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The network type of IS-IS interfaces at the ends of the link must be identical. Otherwise, the two interfaces cannot set up the neighbor relationship. In most cases, the network types of interfaces on a broadcast network and a P2P network are Ethernet and P2P respectively.

The **isis circuit-type** command sets the network type of an interface to simulate a P2P interface so that the network type of IS-IS interfaces at the ends of the link is identical and the neighbor relationship can be established between them.

When an IS-IS neighbor relationship is established between a P2P interface and a simulated P2P interface and the simulated P2P interface has direct neighbors, the

 Copyright © Huawei Technologies Co., Ltd.

P2P interface may receive unneeded packets from these direct neighbors. To prevent the P2P interface from accepting these unneeded packets, specify **strict-snpa-check** in the **isis circuit-type** command to enable IS-IS to check the SNPA address of each received LSP or SNP. After the command is run, the P2P interface accepts only the packets whose SNPA addresses are included in the local neighbor address list, which improves network security.

Precautions

For an interface enabled with IS-IS using the **isis enable** command, when the network type of an interface changes, the corresponding configurations change. Details are as follows:

- After a broadcast interface is simulated as a P2P interface using the **isis circuit-type** command, the interval for sending Hello packets, the number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down, interval for resending LSP packets on a P2P link, and various IS-IS authentication modes are restored to the default settings; other configurations such as the DIS priority, DIS name, and interval for sending CSNP packets on a broadcast network become invalid.
- After the **undo isis circuit-type** command is run to restore the network type of an IS-IS interface, the interval for sending Hello packets, the number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down, interval for resending LSP packets on a P2P link, various IS-IS authentication modes, DIS priority, and interval for sending CSNP packets on a broadcast network are restored to the default settings.

Example

Set the network type of GE1/0/0 to P2P.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis circuit-type p2p
```

Related Topics

9.6.68 isis enable

9.6.64 isis cost

Function

The **isis cost** command sets the link cost value of an IS-IS interface.

The **undo isis cost** command restores the default link cost value of an IS-IS interface.

By default, the link cost value of an IS-IS interface is 10.

Format

isis cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo isis cost [*cost* | **maximum**] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
cost	Specifies the link cost value of an interface.	The value is an integer that varies according to the cost style. ● When the cost style is **narrow**, **narrow-compatible**, or **compatible**, the value ranges from 1 to 63. ● When the cost style is **wide** or **wide-compatible**, the value ranges from 1 to 16777214. The default value is 10.
maximum	Sets the link cost of IS-IS interfaces to 16777215. **NOTE** You can configure this parameter only when the IS-IS cost style is wide or wide-compatible. After the interface cost is set to 16777215, the neighbor TLV generated on the link can only be used to transmit TE information but cannot be used for route calculation.	-
level-1	Specifies the link cost value of a Level-1 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-
level-2	Specifies the link cost value of a Level-2 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On large networks, there may be multiple valid routes to the same destination. IS-IS uses the SPF algorithm to calculate an optimal route and transmits traffic over it, which brings the following problems:

- All traffic is transmitted over the optimal route, causing load imbalance.
- If the optimal route is faulty, traffic will get lost.

To solve the preceding problems, run the **isis cost** command to set a link cost for interfaces so that traffic can be transmitted over different physical links.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Configuration Impact

If the link cost of an interface is changed, routes will be re-calculated on the whole network, causing the changes in traffic forwarding paths.

Precautions

On the TE tunnel interface that is enabled with IGP shortcut, the link cost is the value specified through the **mpls te igp metric** command. If the command is not configured, the IS-IS cost is adopted as the link cost of the TE tunnel interface.

The priority of the **circuit-cost** command is lower than that of the **isis cost** command.

Example

Set the Level-2 link cost of GE1/0/0 to 5.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis cost 5 level-2
```

Related Topics

9.6.11 cost-style

9.6.68 isis enable

11.2.109 mpls te igp metric

9.6.9 circuit-cost

9.6.65 isis delay-peer

Function

The **isis delay-peer** command configures a delay for an interface so that the interface delays establishing neighbor relationships after the neighbor relationship with the last neighbor goes Down due to packet timeout.

The **undo isis delay-peer** command deletes the configured delay and restores the default configurations.

By default, if the neighbor relationship goes Down due to packet timeout, the interface re-establishes the neighbor relationship after it receives a new Hello packet.

Format

isis delay-peer track last-peer-expired [**delay-time** *delay-interval*]

undo isis delay-peer [**track last-peer-expired** [**delay-time** *delay-interval*]]

Parameters

Parameter	Description	Value
track	Tracks the mode of the neighbor relationship establishment delay.	-
last-peer-expired	Indicates that neighbor relationship establishment is delayed after the neighbor relationship with the last neighbor goes Down due to packet timeout.	-
delay-time *delay-interval*	Specifies the neighbor relationship establishment delay.	The value is an integer ranging from 1 to 3600, in seconds. The default value is 60 seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On IS-IS networks, devices at both ends of a link establish a neighbor relationship by exchanging Hello packets. After the neighbor relationship is established, both devices need to send Hello packets at a specified interval to maintain the neighbor relationship. If an IS-IS device does not receive any Hello packets from the neighbor at the other end within the specified period (Holddown time), the local device considers the neighbor Down and re-establishes the neighbor relationship after it receives a new Hello packet. If links are unstable or some Hello packets are lost or incorrect due to network transmission delay or poor transmission, neighbor relationships may alternate between Up and Down frequently, which causes a route flapping.

To address this issue, run the **isis delay-peer** command to configure a neighbor relationship establishment delay after the neighbor relationship goes Down.

 Copyright © Huawei Technologies Co., Ltd.

Pre-configuration Tasks

IS-IS has been enabled using the **isis enable** command in the interface view.

Precautions

If a new *delay-interval* is configured and it is less than the remaining time of the ongoing delay, the new *delay-interval* takes effect immediately; if the new *delay-interval* is greater than the remaining time of the ongoing delay, the ongoing delay continues until the new *delay-interval* takes effect at the next delay.

Example

Set the delay to 100s on GE1/0/0 so that the neighbor relationship establishment is delayed after the neighbor relationship with the last neighbor goes Down due to packet timeout.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis delay-peer track last-peer-expired delay-time 100
```

Related Topics

9.6.68 isis enable

9.6.66 isis dis-name

Function

The **isis dis-name** command configures a host name for the DIS.

The **undo isis dis-name** command deletes the host name configured for the DIS.

By default, no host name is configured for the DIS.

Format

isis dis-name *symbolic-name*

undo isis dis-name

Parameters

Parameter	Description	Value
symbolic-name	Specifies a host name for the DIS.	The value is a string of 1 to 64 characters without spaces. It is case sensitive. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You can configure the name for the DIS on an interface only after you run the **isis enable** command to enable IS-IS on the interface. The DIS name is advertised in a pseudo-node LSP. In this manner, the configured DIS name is associated with the system ID of the DIS.

NOTE

This command takes effect only on the DIS in the broadcast network.

If the **isis circuit-type** command is run to emulate the interface as a P2P interface, the **isis dis-name** command becomes invalid on the interface; after the **undo isis circuit-type** command is run to restore the broadcast interface, the **isis dis-name** command becomes valid on the interface.

Example

Configure a host name for the DIS on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis dis-name LOCALAREA
```

Related Topics

9.6.68 isis enable

9.6.63 isis circuit-type

9.6.67 isis dis-priority

Function

The **isis dis-priority** command sets the priority of the IS-IS interface that is a candidate for the DIS at a specified level.

The **undo isis dis-priority** command restores the default priority.

By default, the DIS priority of broadcast IS-IS interfaces at Level-1 and Level-2 is 64.

Format

isis dis-priority *priority* [**level-1** | **level-2**]

undo isis dis-priority [*priority*] [**level-1** | **level-2**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
priority	Specifies the priority for DIS election.	The value is an integer that ranges from 0 to 127. The default value is 64. A larger value indicates a higher DIS priority.
level-1	Indicates the DIS priority of interfaces at Level 1. If the level is not specified, the same priority is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the DIS priority of interfaces at Level 2. If the level is not specified, the same priority is set for Level-1 and Level-2 interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The configuration is useful only for the broadcast network.

The DIS priority is advertised through Hello packets. The router with the highest priority is elected as the DIS. In the case of the same priority, the router with the largest MAC address is elected as the DIS.

NOTE

IS-IS has been enabled on the interface using the **isis enable** command.

If the **9.6.63 isis circuit-type** command is run to emulate the interface as a P2P interface, the **isis dis-priority** command becomes invalid on the interface; after the **undo isis circuit-type** command is run to restore the broadcast interface, the **isis dis-priority** command becomes valid on the interface.

Example

Set the Level-2 priority for electing the DIS to 127 on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis dis-priority 127 level-2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.6.63 isis circuit-type

9.6.68 isis enable

Function

The **isis enable** command enables IS-IS on an interface and specifies the ID of the IS-IS process to be associated with the interface.

The **undo isis enable** command disables IS-IS on an interface and cancels the ID of the IS-IS process associated with the interface.

By default, IS-IS is disabled on an interface.

Format

isis enable [*process-id*]

undo isis enable

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an IS-IS process is configured in the system view, to make the IS-IS protocol function normally, enable IS-IS on an interface to associate the interface with the IS-IS process.

Prerequisites

An IS-IS process has been enabled using the **isis** command in the system view.

Precautions

An interface can be associated with only one IS-IS process.

Example

Create IS-IS process 1 and activate the process on GE1/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] network-entity 10.0001.1010.1020.1030.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
```

Related Topics

9.6.56 isis

9.6.69 isis lfa-backup

Function

The **isis lfa-backup** command enables an IS-IS interface to participate in loop-free alternate (LFA) calculation so that the interface can be a candidate for a backup interface.

The **undo isis lfa-backup** command disables an IS-IS interface from participating in LFA calculation.

By default, an IS-IS interface can participate in LFA calculation.

Format

isis lfa-backup [**level-1** | **level-2** | **level-1-2**]

undo isis lfa-backup [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Indicates that an interface can be a backup interface in Level-1 areas.	-
level-2	Indicates that an interface can be a backup interface in Level-2 areas.	-
level-1-2	Indicates that an interface can be a backup interface in both Level-1 and Level-2 areas.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

To facilitate traffic management and avoid the uncertainty in the traffic forwarding path in the case the primary link fails, run the **undo isis lfa-backup**

command on some interfaces to disable them from participating in LFA calculation.

IS-IS has been enabled on the interface using the **isis enable** command.

Example

Disable GE1/0/0 from becoming a backup interface for Auto FRR.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] undo isis lfa-backup
```

Related Topics

9.6.46 frr (IS-IS)

9.6.97 loop-free-alternate

9.6.70 isis lsp seq-overflow auto-recover disable

Function

The **isis lsp seq-overflow auto-recover disable** command prevents an IS-IS system from changing its system ID when it receives a locally generated LSP with the maximum sequence number (0xFFFFFFFF).

The **undo isis lsp seq-overflow auto-recover disable** command restores the default configuration.

By default, an IS-IS system changes its system ID when it receives a locally generated LSP with the maximum sequence number.

Format

isis lsp seq-overflow auto-recover disable

undo isis lsp seq-overflow auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On an IS-IS network, if a device receives a locally generated LSP with the sequence number greater than that of the corresponding LSP stored locally, the device adds 1 to the sequence number of the received LSP and floods it. An attacker may send an IS-IS LSP with the maximum sequence number (0xFFFFFFFF) and the system ID of a target device. Upon receipt of the LSP, the target device considers it a locally generated LSP because it carries the local system ID and adds 1 to the sequence number because the sequence number is greater than that of the corresponding LSP stored locally. Consequently, the sequence number exceeds the maximum number, causing the target device to enter the hibernation state. The state can last 18 hours and 1 minute, affecting network operation. To prevent this problem, an IS-IS system changes its system ID when it receives a locally generated LSP with the sequence number of 0xFFFFFFFF. However, if the IS-IS system has changed its system ID for three times within 24 hours when it receives one more such an LSP, it directly enters the hibernation state.

The preceding function also applies to CSNPs and PSNPs.

By default, an IS-IS system changes its system ID when it receives a locally generated LSP with the maximum sequence number. To disable this function, run the **isis lsp seq-overflow auto-recover disable** command.

Example

Prevent an IS-IS system from changing its system ID when it receives a locally generated LSP with the maximum sequence number (0xFFFFFFFF).

```
<Huawei> system-view
[Huawei] isis lsp seq-overflow auto-recover disable
```

9.6.71 isis mesh-group

Function

The **isis mesh-group** command adds an IS-IS interface to a specified mesh group.

The **undo isis mesh-group** command deletes an IS-IS interface from a specified mesh group.

By default, an IS-IS interface does not belong to any mesh group and floods LSPs normally.

Format

isis mesh-group { *mesh-group-number* | **mesh-blocked** }

undo isis mesh-group

Parameters

Parameter	Description	Value
mesh-group-number	Specifies the mesh group number.	The value is an integer that ranges from 1 to 4294967295.
mesh-blocked	Blocks an interface to prevent it from flooding received LSPs to other interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving LSPs, the interface, not in the mesh group, floods the LSPs to other interfaces following the normal procedure. For the NBMA network that is with higher connectivity and several P2P links, this process causes repeated LSP flooding and wastes bandwidth.

After receiving LSPs, the interface that joins a mesh group only floods the LSPs to the interfaces that are not in the local mesh group.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

When adding interfaces to mesh groups or blocking interfaces, keep certain interfaces from being configured with the isis mesh-group command. This can prevent link faults from affecting the normal spreading of LSPs.

Example

Add GE1/0/0 to mesh group 3.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis mesh-group 3
```

 Copyright © Huawei Technologies Co., Ltd.

9.6.72 isis padding-hello

Function

The **isis padding-hello** command configures an IS-IS interface to send Hello packets with the padding field.

The **undo isis padding-hello** command restores the default setting.

By default, an IS-IS interface is not configured to send Hello packets with the padding field.

Format

isis padding-hello

undo isis padding-hello

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **isis padding-hello** and **isis small-hello** commands are mutually exclusive and cannot be configured on the same interface simultaneously.

If an interface that is not configured with the two commands, it sends Hello packets based on the following rules:

- For a P2P interface
  - Before the P2P neighbor relationship is established, the P2P interface sends Hello packets with the padding field.
  - After the P2P neighbor relationship is established, the P2P interface sends Hello packets without the padding field.

  NOTE

  For a P2P interface, the length of padding field is equal to the length of LSP packets originated by local IS.
- For a broadcast interface

  It sends Hello packets with the padding field.

  NOTE

  For a broadcast interface, the length of padding field is equal to the length of MTU.

 Copyright © Huawei Technologies Co., Ltd.

IS-IS has been enabled on the interface using the **isis enable** command.

Example

Configure GE1/0/0 to send Hello packets with the padding field.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis padding-hello
```

Related Topics

9.6.78 isis small-hello

9.6.73 isis peer-ip-ignore

Function

The **isis peer-ip-ignore** command configures IS-IS not to check the IP address of Hello packets received by an interface.

The **undo isis peer-ip-ignore** command restores the default setting.

By default, IS-IS checks the IP address of received Hello packets.

Format

isis peer-ip-ignore

undo isis peer-ip-ignore

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IS-IS checks the IP address carried in the Hello packet. The neighbor relationship can be set up only when the local interface address and the interface address carried in the received packets belong to the same network segment. When the two interface IP addresses are not in the same network segment, if the **isis peer-ip-ignore** command is used, the check on the peer IP address is ignored, and the two IS-IS interfaces can set up normal neighbor relationship. Routes of

this two network segments exist in the routing table, but cannot ping through each other.

Precautions

This command is valid for P2P interfaces, NBMA interfaces and the interface with the network type configured to P2P by using the **isis circuit-type p2p** command. The command takes effect only when the command is used on the two ends of the link.

NOTE

- For the broadcast interface, you can run the **isis peer-ip-ignore** command only after you run the **isis circuit-type p2p** command. The isis circuit-type p2p command is valid only for the broadcast interface.
- For the P2P and NBMA interfaces, you can run the isis **isis peer-ip-ignore** command without running the isis circuit-type p2p command.

Example

Configure GE1/0/0 not to check the IP address of the Hello packets sent by the peer.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis circuit-type p2p
[Huawei-GigabitEthernet1/0/0] isis peer-ip-ignore
```

Related Topics

9.6.63 isis circuit-type

9.6.74 isis ppp-negotiation

Function

The **isis ppp-negotiation** command specifies the PPP negotiation mode for establishing neighbor relationships.

The **undo isis ppp-negotiation** command restores the default negotiation mode.

By default, the 3-way handshake mode is used.

Format

isis ppp-negotiation { **2-way** | **3-way** [**only**] }

undo isis ppp-negotiation

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
2-way	Establishes the neighbor relationship using the 2-way handshake negotiation mode.	-
3-way	Establishes the neighbor relationship using the 3-way handshake negotiation mode.	-
only	Establishes the neighbor relationship using the 3-way handshake negotiation mode that is not backward compatible.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The 3-way handshake negotiation mode is backward compatible. If the neighbor only supports 2-way handshake, use the 2-way handshake negotiation mode to establish a neighbor relationship.

The command is applicable only for P2P interfaces. It can be used on the broadcast interfaces only after the circuit type is set to P2P.

Example

Establish the neighbor relationship on GE1/0/0 using the 2-way handshake negotiation mode.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis circuit-type p2p
[Huawei-GigabitEthernet1/0/0] isis ppp-negotiation 2-way
```

Related Topics

9.6.63 isis circuit-type

9.6.75 isis ppp-osicp-check

Function

The **isis ppp-osicp-check** command enables OSICP negotiation check on a PPP interface. The negotiation status can affect IS-IS interface status.

The **undo isis ppp-osicp-check** command restores the default setting.

 Copyright © Huawei Technologies Co., Ltd.

By default, IS-IS does not check OSICP status of PPP.

Format

isis ppp-osicp-check

undo isis ppp-osicp-check

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is configured, OSI network negotiation status of PPP can affect IS-IS interface status. When PPP senses that the OSI network fails, the link status of the IS-IS interface turns Down and the route to the network segment where the interface resides is not advertised through LSP.

Precautions

This command applies to only PPP interfaces. For other point-to-point interfaces, this command is invalid.

Example

Configure Serial1/0/0 to check OSICP status of PPP.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] isis enable 1
[Huawei-Serial1/0/0] isis ppp-osicp-check
```

9.6.76 isis purge-lsp auto-protect disable

Function

The **isis purge-lsp auto-protect disable** command disables IS-IS purge LSPs from triggering master/slave main control board switchovers.

The **undo isis purge-lsp auto-protect disable** command restores the default configuration.

By default, IS-IS purge LSPs trigger master/slave main control board switchovers.

Format

isis purge-lsp auto-protect disable

undo isis purge-lsp auto-protect disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When an IS-IS process on a device proactively sends a purge LSP, the device deletes the corresponding LSP and floods it to the network. In most cases, before the device sends a purge LSP, the end that generated the corresponding LSP sends an updated LSP. If the clock on the device runs fast, the device frequently floods purge LSPs to devices on the entire network, causing network flapping. If the device generates more than five purge LSPs for 80% or more non-pseudonode LSPs with a non-zero fragment number in the local LSDB within 6500s, a master/slave main control board switchover is performed if the device has two main control boards, or the device is restarted if it has only one main control board. The switchover or restart prevents network flapping.

By default, IS-IS purge LSPs trigger master/slave main control board switchovers. To disable IS-IS purge LSPs from triggering master/slave main control board switchovers, run the **isis purge-lsp auto-protect disable** command.

Example

Disable IS-IS purge LSPs from triggering master/slave main control board switchovers.

```
<Huawei> system-view
[Huawei] isis purge-lsp auto-protect disable
```

9.6.77 isis silent

Function

The **isis silent** command configures an IS-IS interface as a silent interface. That is, the interface is suppressed from sending and receiving IS-IS packets, but routes of the network segment on which the interface resides can be advertised.

The **undo isis silent** command restores the default setting.

By default, no IS-IS interface is configured as a silent interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

isis silent [**advertise-zero-cost**]

undo isis silent

Parameters

Parameter	Description	Value
advertise-zero-cost	Specifies the route cost as 0. The default cost of IS-IS routes is 10.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an IS-IS network is connected to other ASs, it is required to enable IS-IS on the interfaces that connect the IS-IS network to other ASs so that the router on the IS-IS network can learn the routes to other ASs. This interface, however, unnecessarily advertises IS-IS Hello packets on its network segment. In this case, you can run the **isis silent** command to suppress the IS-IS interface.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Example

Configure GE1/0/0 as a silent interface.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis silent
```

Related Topics

9.6.68 isis enable

 Copyright © Huawei Technologies Co., Ltd.

9.6.78 isis small-hello

Function

The **isis small-hello** command configures an IS-IS interface to send Hello packets without the padding field.

The **undo isis small-hello** command restores the default setting.

By default, an IS-IS interface is not configured to send Hello packets without the padding field.

Format

isis small-hello

undo isis small-hello

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The command can simplify the operations of sending and receiving Hello packets.

The **isis small-hello** and **isis padding-hello** commands are mutually exclusive and cannot be configured on the same interface simultaneously.

If an interface is not configured with the two commands, it sends Hello packets based on the following rules:

- P2P interface
  - Before the P2P neighbor relationship is established, the P2P interface sends Hello packets with the padding field.
  - After the P2P neighbor relationship is established, the P2P interface sends Hello packets without the padding field.

  NOTE

  For a P2P interface, the length of padding field is equal to the length of LSP packets originated by local IS.
- Broadcast interface

  The interface sends Hello packets with the padding field.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

For a broadcast interface, the length of padding field is equal to the length of MTU.

Before running this command on an interface, run the **isis enable** command on the interface to enable IS-IS.

Example

Configure GE1/0/0 to send Hello packets without the padding field.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis small-hello
```

Related Topics

9.6.72 isis padding-hello

9.6.79 isis suppress-flapping peer

Function

The **isis suppress-flapping peer** command configures detection parameters for IS-IS neighbor relationship flapping suppression.

The **undo isis suppress-flapping peer** command restores the default detection parameters.

By default, the detection interval of IS-IS neighbor relationship flapping suppression is 60s, the suppression threshold is 10, and the interval for exiting from suppression is 120s.

Format

isis suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } *

undo isis suppress-flapping peer { **detecting-interval** *detecting-interval* | **threshold** *threshold* | **resume-interval** *resume-interval* } *

Parameters

Parameter	Description	Value
detecting-interval *detecting-interval*	Specifies the detection interval of IS-IS neighbor relationship flapping suppression. Each IS-IS interface on which IS-IS neighbor relationship flapping suppression is enabled starts a flapping counter. If the interval between two successive neighbor status changes from Full to a non-Full state is shorter than *detecting-interval*, a valid flapping_event is recorded, and the flapping-count increases by 1.	The value is an integer ranging from 1 to 300, in seconds. The default value is 60s.
threshold *threshold*	Specifies the threshold of IS-IS neighbor relationship flapping suppression. When the flapping-count reaches or exceeds *threshold*, flapping suppression takes effect.	The value is an integer ranging from 1 to 1000. The default value is 10.
resume-interval *resume-interval*	• Specifies the interval for exiting from IS-IS neighbor relationship flapping suppression. If the interval between two successive neighbor status changes from Full to a non-Full state is longer than *resume-interval*, the flapping-count is reset. • If IS-IS neighbor relationship flapping suppression works in hold-max-cost mode, *resume-interval* indicates the duration of this mode. **NOTE** The value of *resume-interval* must be greater than that of *detecting-interval*.	The value is an integer ranging from 2 to 1000, in seconds. The default value is 120s.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure detection parameters for IS-IS neighbor relationship flapping suppression on an interface, run the **isis suppress-flapping peer** command. However, keeping the default configurations is recommended.

Prerequisites

IS-IS neighbor relationship flapping suppression must have been enabled globally before you configure detection parameters for it. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the detection parameters.

Example

Set the detection interval of IS-IS neighbor relationship flapping suppression to 5s, the suppression threshold to 40, and the interval for exiting from suppression to 20s on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] isis suppress-flapping peer detecting-interval 5 threshold 40 resume-interval 20
```

Related Topics

9.6.121 suppress-flapping peer disable (IS-IS)

9.6.80 isis suppress-flapping peer disable

Function

The **isis suppress-flapping peer disable** command disables IS-IS neighbor relationship flapping suppression from an interface.

The **undo isis suppress-flapping peer disable** command enables IS-IS neighbor relationship flapping suppression on an interface.

By default, IS-IS neighbor relationship flapping suppression is enabled on all interfaces.

Format

isis suppress-flapping peer disable

undo isis suppress-flapping peer disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IS-IS neighbor relationship flapping suppression is enabled on all interfaces in the same IS-IS process. To disable the function from one of the interfaces, run the **isis suppress-flapping peer disable** command.

NOTE

When an interface enters the flapping suppression state, all neighbor relationships on the interface enter the state accordingly.

Prerequisites

IS-IS neighbor relationship flapping suppression must have been enabled globally before you enable the function on an interface using the **undo isis suppress-flapping peer disable** command. By default, the function is enabled globally. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it first.

Example

Disable IS-IS neighbor relationship flapping suppression from GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] isis suppress-flapping peer disable
```

Related Topics

9.6.121 suppress-flapping peer disable (IS-IS)

9.6.81 isis suppress-flapping peer hold-down

Function

The **isis suppress-flapping peer hold-down** command configures the Hold-down mode and sets duration for this mode.

The **undo isis suppress-flapping peer hold-down** command cancels the Hold-down mode.

By default, the Hold-down mode is disabled, and the Hold-max-cost mode is enabled.

Format

isis suppress-flapping peer hold-down *interval*

undo isis suppress-flapping peer hold-down [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the duration of the Hold-down mode.	The value is an integer ranging from 1 to 600, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes LSDB synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use the maximum value (16777214 for the wide mode and 63 for the narrow mode) as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **isis suppress-flapping peer hold-down** *interval* command.

Prerequisites

IS-IS neighbor relationship flapping suppression must have been enabled globally before you configure the Hold-down mode and set duration for this mode. By default, the function is enabled. If it is disabled, run the **undo suppress-flapping peer disable** command to enable it before you configure the Hold-down mode and set duration for this mode.

Example

Configure the Hold-down mode and set its duration to 200s on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] isis suppress-flapping peer hold-down 200
```

Related Topics

9.6.121 suppress-flapping peer disable (IS-IS)

9.6.82 isis suppress-flapping peer hold-max-cost disable

 Copyright © Huawei Technologies Co., Ltd.

9.6.82 isis suppress-flapping peer hold-max-cost disable

Function

The **isis suppress-flapping peer hold-max-cost disable** command disables the Hold-max-cost mode.

The **undo isis suppress-flapping peer hold-max-cost disable** command enables the Hold-max-cost mode.

By default, the Hold-max-cost mode is enabled.

Format

isis suppress-flapping peer hold-max-cost disable

undo isis suppress-flapping peer hold-max-cost disable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flapping suppression works in either Hold-down or Hold-max-cost mode.

- Hold-down mode: In the case of frequent flooding and topology changes during neighbor relationship establishment, interfaces prevent neighbor relationship reestablishment during Hold-down suppression, which minimizes synchronization attempts and packet exchanges.
- Hold-max-cost mode: If the traffic forwarding path changes frequently, interfaces use the maximum value (16777214 for the wide mode and 63 for the narrow mode) as the cost of the flapping link during Hold-max-cost suppression, which prevents traffic from passing through the flapping link. If a device on a key path is isolated from the network due to IS-IS neighbor relationship flapping, the network is separated into two isolated parts. To prevent this problem, use the Hold-max-cost mode on the key path.

If the neighbor relationship does not go Down within successive **resume-interval**s, or the interval between two successive neighbor Down events is greater than or equal to **resume-interval**, the suppression in Hold-max-cost mode exits.

Flapping suppression can also work first in Hold-down mode and then in Hold-max-cost mode.

 Copyright © Huawei Technologies Co., Ltd.

By default, the Hold-max-cost mode takes effect. To configure the Hold-down mode and set duration for this mode, run the **isis suppress-flapping peer hold-down** *interval* command.

Precautions

The Hold-max-cost mode takes effect only unidirectionally. If a remote device does not support IS-IS neighbor relationship flapping suppression, bidirectional traffic between the local and remote devices may travel along different paths.

Example

Disable the Hold-max-cost mode on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] isis suppress-flapping peer hold-max-cost disable
```

Related Topics

9.6.121 suppress-flapping peer disable (IS-IS)

9.6.81 isis suppress-flapping peer hold-down

9.6.83 isis suppress-reachability

Function

The **isis suppress-reachability** command suppresses the advertisement of direct routes on an IS-IS interface in a specified topology.

The **undo isis suppress-reachability** command restores the default setting.

By default, direct routes on an IS-IS interface are advertised.

Format

isis suppress-reachability [**level-1** | **level-1-2** | **level-2**]

undo isis suppress-reachability

Parameters

Parameter	Description	Value
level-1	Indicates that the advertisement of IPv4 addresses is suppressed on Level-1 interfaces. If the level is not specified, the advertisement of IPv6 addresses on Level-1 and Level-2 interfaces is suppressed.	-
level-1-2	Indicates that the advertisement of IPv4 addresses is suppressed on Level-1 and Level-2 interfaces.	-
level-2	Indicates that the advertisement of IPv4 addresses is suppressed on Level-2 interfaces. If the level is not specified, the advertisement of IPv4 addresses is suppressed on Level-1 and Level-2 interfaces.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Before running this command on an interface, run the **isis enable** command on the interface to enable IS-IS.

Example

Suppress the advertisement of IPv4 addresses on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis suppress-reachability
```

9.6.84 isis system-id auto-recover disable

Function

The **isis system-id auto-recover disable** command disables the system from automatically resolving IS-IS system ID conflicts.

The **undo isis system-id auto-recover disable** command enables the system to automatically resolve IS-IS system ID conflicts.

By default, if the system detects an IS-IS system ID conflict, it automatically changes the local system ID to resolve the conflict.

Format

isis system-id auto-recover disable

undo isis system-id auto-recover disable

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A system ID uniquely identifies an IS-IS device. If the same system ID is configured for more than one device on the network, a routing loop may occur. By default, if the system detects an IS-IS system ID conflict, it automatically changes the local system ID to resolve the conflict.

To disable the system from automatically resolving IS-IS system ID conflicts, run the **isis system-id auto-recover disable** command. After the command is run, IS-IS system ID conflicts need to be manually resolved.

NOTE

The first two bytes of the system ID automatically changed by the system are Fs, and the last four bytes are randomly generated. For example, FFFF:1234:5678 is such a system ID.

Precautions

If an IS-IS system ID conflict occurs between two directly connected devices, a neighbor relationship fails to be established only between the two devices, without affecting the entire network. As a result, the conflict is not automatically resolved in this case.

On broadcast networks, the system ID generated automatically is not recorded in the configuration file. If the device is restarted, the system restores this system ID to the originally configured one and then generates another one, which may be different from the one last generated automatically. If the conflict persists after the system automatically generates three system IDs, the system no longer resolves this conflict.

Example

Disable the system to automatically resolve IS-IS system ID conflicts.

```
<Huawei> system-view
[Huawei] isis system-id auto-recover disable
```

9.6.85 isis tag-value

Function

The **isis tag-value** command sets the administrative tag value of an IS-IS interface.

The **undo isis tag-value** command deletes the administrative tag value on an IS-IS interface.

By default, an IS-IS interface has no administrative tag value.

Format

isis tag-value *tag* [**level-1** | **level-2**]

undo isis tag-value [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag of an IS-IS interface.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates the administrative tag value of a Level-1 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the administrative tag value of a Level-2 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrative tag carries administrative information about IP address prefixes. The tag can be used to import routes of different levels and different areas. Administrative tags can advertise IP address prefixes in an IS-IS routing domain to control routes and simplify management.

Using the **isis tag-value** command, you can set the administrative tag value for all routes of a specified IS-IS process. The tag can be used as a filtering condition of a route-policy to filter routes.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

The advertised LSPs contain the administrative tag value only when the IS-IS cost style is wide, wide-compatible, or compatible.

The administrative tag value set using the **isis tag-value** command has a higher priority than the administrative tag value set using the **9.6.10 circuit default-tag** command.

Example

Set the administrative tag value of GE1/0/0 to 77.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis tag-value 77
```

Related Topics

9.6.10 circuit default-tag

9.6.11 cost-style

9.6.86 isis timer csnp

Function

The **isis timer csnp** command sets the interval for sending CSNPs on a broadcast network.

The **undo isis timer csnp** command restores the default setting.

By default, the interval for sending CSNPs on a broadcast network is 10 seconds.

Format

isis timer csnp *csnp-interval* [**level-1** | **level-2**]

undo isis timer csnp [*csnp-interval*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
csnp-interval	Specifies the interval for sending CSNPs on a broadcast network.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 10 seconds.
level-1	Indicates the interval for sending Level-1 CSNPs. If no level is specified, the interval for the IS-IS process of the current level to send CSNP packets is set by default.	-
level-2	Indicates the interval for sending Level-2 CSNPs. If no level is specified, the interval for the IS-IS process of the current level to send CSNP packets is set by default.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a broadcast network, a DIS sends CSNPs periodically to enable all devices to synchronize LSDBs with one another. If a device finds that the local LSDB does not have a specific LSP or an existing LSP is not the latest one after the device has received a CSNP, the device will send a PSNP to request the corresponding LSP. Only a DIS sends CSNPs periodically. Therefore, the **isis timer csnp** command will take effect only on a broadcast interface of the DIS. This command can be used to set an interval for sending CSNPs in an area at a specified level. A router may be elected as a DIS in both Level-1 and Level-2 areas. Therefore, you can set different intervals at which the DIS sends CSNPs in Level-1 and Level-2 areas.

Prerequisites

Before running this command on an interface, run the **isis enable** command on the interface to enable IS-IS.

Precautions

The IS-IS route convergence speed depends on the LSDB synchronization speed. Therefore, reducing the interval for sending CSNPs can speed up LSDB synchronization and IS-IS route convergence. If the interval is set too small, however, the DIS will send CSNPs frequently. This causes high CPU, memory, and network bandwidth usage and affects services.

NOTE

If the **isis circuit-type** command is run to emulate the interface as a P2P interface, the **isis timer csnp** command becomes invalid on the interface; after the **undo isis circuit-type** command is run to restore the broadcast interface, the interval for sending CSNPs is restored to the default setting.

Example

Set the interval for sending Level-2 CSNPs to 15 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis timer csnp 15 level-2
```

Related Topics

9.6.91 is-level

9.6.63 isis circuit-type

9.6.87 isis timer hello

Function

The **isis timer hello** command sets the interval for sending Hello packets on an IS-IS interface.

The **undo isis timer hello** command restores the default setting.

By default, the interval for sending Hello packets 10 seconds on an interface.

Format

isis timer hello *hello-interval* [**level-1** | **level-2**] [**conservative**]

undo isis timer hello [*hello-interval*] [**level-1** | **level-2**] [**conservative**]

Parameters

Parameter	Description	Value
hello-interval	Specifies the interval for sending Hello packets.	The value is an integer that ranges from 3 to 255, in seconds. The default value is 10 seconds.
level-1	Indicates the interval for sending Level-1 Hello packets. If the level is not specified, the interval for sending Level-1 and Level-2 Hello packets is set by default.	-
level-2	Indicates the interval for sending Level-2 Hello packets. If the level is not specified, the interval for sending Level-1 and Level-2 Hello packets is set by default. **NOTE** Parameters **level-1** and **level-2** are configured only on a broadcast interface that is enabled with IS-IS. Level-1 and Level-2 Hello packets are sent separately and their intervals must be set respectively. There is only one Hello packet on a point-to-point link. Therefore, level-1 and level-2 parameters are not used.	-
conservative	Indicates the conservative mode of the dead timer. If the conservative mode is configured, the value configured for the dead timer takes effect even when the value is less than 10s.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS maintains neighbor relationships between neighbors by sending and receiving Hello packets. If the local device does not receive Hello packets from its neighbor within a specified period, the device considers the neighbor Down.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

The shorter the interval, the more system resources used to send Hello packets. The interval should therefore be set according to the actual conditions.

If a broadcast interface is emulated as a P2P interface through the **isis circuit-type** command or then restored to the broadcast interface through the **undo isis circuit-type** command, the interval for sending IS-IS Hello packets is restored to the default value.

Example

Set the interval for sending Level-2 Hello packets to 20 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis timer hello 20 level-2
```

Related Topics

9.6.63 isis circuit-type

9.6.88 isis timer holding-multiplier

9.6.88 isis timer holding-multiplier

Function

The **isis timer holding-multiplier** command sets the multiplier of the interval for sending Hello packets to change the holdtime of IS-IS neighbor relationship.

The **undo isis timer holding-multiplier** command restores the default setting.

By default, the multiplier of the interval for sending Hello packets is 3, that is, the neighbor holdtime is three times the interval for sending Hello packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

isis timer holding-multiplier *number* [**level-1** | **level-2**]

undo isis timer holding-multiplier [*number*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
number	Indicates that the neighbor holdtime is a multiplier of the interval for sending Hello packets.	The value is an integer that ranges from 3 to 1000. The default value is 3.
level-1	Indicates the holdtime of Level-1 neighbors. If the level is not specified, the holdtime is set for both Level-1 and Level-2 neighbors.	-
level-2	Indicates the holdtime of Level-2 neighbors. If the level is not specified, the holdtime is set for both Level-1 and Level-2 neighbors. **NOTE** Parameters **level-1** and **level-2** are configured only on a broadcast interface that is enabled with IS-IS. Level-1 and Level-2 Hello packets are sent separately and their intervals must be set respectively. There is only one Hello packet on a point-to-point link. Therefore, level-1 and level-2 parameters are not used.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Devices at both ends of a link establish a neighbor relationship by sending Hello packets to each other. After the neighbor relationship is established, both devices need to send Hello packets at a specified interval to maintain the neighbor relationship. If a device does not receive any Hello packet from its neighbor within a specified period of time, the device considers the neighbor to be Down. The specified time period is known as the neighbor holdtime.

For example, run the **isis timer hello** command on a local device to set the interval for sending Hello packets to 20s. Then, run the **isis timer holding-multiplier** 4 command. The holdtime is 80s (four times the interval for sending

 Copyright © Huawei Technologies Co., Ltd.

Hello packets). If the interval for sending Hello packets is changed using the **isis timer hello** 20 command, the holdtime will be changed accordingly.

Prerequisites

IS-IS has been enabled on the interface using the **isis enable** command.

Precautions

If the *number* value is set too large, the local device needs to wait a long time before detecting that the remote device has gone Down. This slows down IS-IS route convergence. If the value of *number* is set too small, the neighbor relationship will alternate between **Up** and **Down** when some Hello packets are lost due to transmission delays and errors on the network. This causes route flapping on the IS-IS network. Therefore, exercise caution when setting the value of *number*. Set the same interval for sending Hello packets and the same neighbor holdtime for all devices on the IS-IS network is recommended. This is to ensure that all devices detect link failures at the same time and guarantee timely IS-IS route convergence.

If a broadcast interface is emulated as a P2P interface through the **isis circuit-type** command or then restored to the broadcast interface through the **undo isis circuit-type** command, the number of Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down is restored to the default value.

Example

Set the number of Level-2 Hello packets that IS-IS does not receive from a neighbor before the neighbor is declared Down to 6 on GE1/0/0.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis timer holding-multiplier 6 level-2
```

Related Topics

9.6.87 isis timer hello

9.6.63 isis circuit-type

9.6.89 isis timer lsp-retransmit

Function

The **isis timer lsp-retransmit** command sets the interval for retransmitting LSPs over a P2P link.

The **undo isis timer lsp-retransmit** command restores the default value.

By default, the interval for retransmitting LSPs over a P2P link is 5 seconds.

Format

isis timer lsp-retransmit *retransmit-interval*

undo isis timer lsp-retransmit

Parameters

Parameter	Description	Value
retransmit-interval	Specifies the interval for retransmitting LSPs.	The value is an integer that ranges from 1 to 300.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a point-to-point network, devices at both ends of a link synchronize LSDBs with each other by flooding LSPs. The device at one end of the link sends an LSP. If the device at the other end receives this LSP, it replies with a PSNP. If the device that has sent an LSP does not receive a PSNP from the other end in a period of time, the device will retransmit the LSP.

The **isis timer lsp-retransmit** command is used to set an interval for retransmitting LSPs. Only the devices on a point-to-point network send PSNPs. Therefore, the **isis timer lsp-retransmit** command will take effect only when it is run on point-to-point interfaces.

Precautions

After the **isis timer lsp-retransmit** command is run on a device, the device will wait *retransmit-interval* after having sent an LSP. If the device receives a PSNP from the other end, the device will not retransmit the LSP. Otherwise, the device will retransmit the LSP.

If the value of *retransmit-interval* is set too small, an LSP will be retransmitted even though it is not necessary, causing high CPU, memory, and network bandwidth usage.

NOTE

If a broadcast interface is emulated as a P2P interface through the **isis circuit-type** command or restored a P2P interface to the broadcast interface through the **undo isis circuit-type** command, the interval for retransmitting LSP packets on a P2P link is restored to the default value.

Example

Set the interval for retransmitting LSPs on Serial1/0/0 to 10 seconds.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
```

```
[Huawei-isis-1] quit
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] isis enable 1
[Huawei-Serial1/0/0] isis timer lsp-retransmit 10
```

Related Topics

9.6.90 isis timer lsp-throttle

9.6.63 isis circuit-type

9.6.90 isis timer lsp-throttle

Function

The **isis timer lsp-throttle** command sets the minimum interval for sending LSPs on an IS-IS interface and the maximum number of LSPs sent within the interval.

The **undo isis timer lsp-throttle** command restores the default setting.

By default, the minimum interval for sending LSPs on an IS-IS interface is 50 milliseconds and the maximum number of LSPs sent within the interval is 10.

Format

isis timer lsp-throttle *throttle-interval* [**count** *count*]

undo isis timer lsp-throttle

Parameters

Parameter	Description	Value
throttle-interval	Specifies the minimum interval for sending LSPs.	The value is an integer that ranges from 1 to 10000, in milliseconds.
count *count*	Specifies the maximum number of LSPs that are sent within the interval specified by *throttle-interval*.	The value is an integer that ranges from 1 to 1000.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The value specified by *throttle-interval* is the interval between two consecutive LSPs and is also the interval for sending multiple fragments of a CSNP.

 Copyright © Huawei Technologies Co., Ltd.

Before running this command on an interface, run the **isis enable** command on the interface to enable IS-IS.

Example

Set the interval for retransmitting LSPs on GE1/0/0 to 500 ms.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 01.0000.0000.0001.00
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis timer lsp-throttle 500
```

Related Topics

9.6.89 isis timer lsp-retransmit

9.6.91 is-level

Function

The **is-level** command sets the level of an IS-IS router.

The **undo is-level** command restores the default setting.

By default, the level of an IS-IS router is Level-1-2.

Format

is-level { **level-1** | **level-1-2** | **level-2** }

undo is-level

Parameters

Parameter	Description	Value
level-1	Indicates that the level of the router is Level-1. The router calculates only intra-area routes and maintains the Level-1 LSDB.	-
level-1-2	Indicates that the level of the router is Level-1-2. The router calculates Level-1 and Level-2 routes and maintains Level-1 and Level-2 LSDBs.	-
level-2	Indicates that the level of the router is Level-2. The router calculates only Level-2 routes, and maintains the Level-2 LSDB.	-

Views

IS-IS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To support a network with a large number of routes, IS-IS uses a two-level structure in an IS-IS routing domain. IS-IS routers are classified into the following levels:

- Level-1 router: A Level-1 router manages intra-area routing. It establishes neighbor relationships with only Level-1 and Level-1-2 routers in the same area. Level-1 routers can be connected to other areas through Level-1-2 routers only.
- Level-2 router: A Level-2 router manages intra-area routing. It establishes neighbor relationships with Level-2 routers in the same area and Level-1-2 routers in other areas only. All Level-2 routers form the backbone network of the routing domain. They are responsible for communications between areas. The Level-2 routers in the routing domain must be reachable, and no router of other levels is deployed between every two Level-2 routers.
- Level-1-2 router: A Level-1-2 router can establish Level-1 neighbor relationships with Level-1 routers and Level-1-2 routers in the same area. It can also establish Level-2 neighbor relationships with Level-2 routers and Level-1-2 routers in other areas.

In most cases, Level-1 routers are located within an area, Level-2 routers are located between areas, and Level-1-2 routers are located between Level-1 routers and Level-2 routers.

The level of an IS-IS router and of an interface determine the level of a neighbor relationship. By default, neighbor relationships between two Level-1-2 routers are Level-1 and Level-2. To establish a Level-1 or Level-2 neighbor relationship, run the **isis circuit-level** command to modify the level of interfaces.

If only one area exists, setting the level of routers to Level-1 or Level-2 is recommended to prevent devices from maintaining two LSDBs that are the same. On an IP network, setting the level of all routers to Level-2 for future extension is recommended.

Precautions

If the levels of IS-IS routers are changed during network operation, the IS-IS process will be restarted and IS-IS neighbor relationships will be disconnected. Setting the levels of routers when configuring IS-IS is recommended.

If the Level-1 and Level-2 is not specified, the router works at Level-1-2. That is, the router calculates Level-1 and Level-2 routes and maintains Level-1 and Level-2 LSDBs simultaneously.

Example

Set the level of the current router to Level-1.

```
<Huawei> system-view
[Huawei] isis 1
```

```
[Huawei-isis-1] is-level level-1
```

Related Topics

9.6.62 isis circuit-level

9.6.92 is-name

Function

The **is-name** command enables the capability of identifying the host name in an LSP and configures the dynamic host name for the IS-IS system of the local router. The dynamic hostname is advertised in an LSP packet.

The **undo is-name** command deletes the dynamic host name configured for the IS-IS system of the local router.

By default, the IS-IS system of the local router has no dynamic host name.

Format

is-name *symbolic-name*

undo is-name [*symbolic-name*]

Parameters

Parameter	Description	Value
symbolic-name	Specifies a dynamic host name.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

In most cases, to check information about IS-IS neighbors and LSDBs on an IS-IS router, you need to use a system ID of a 12-digit hexadecimal number, for example, aaaa.eeee.1234. This representation, however, is complicated and not easy to use. The dynamic host name mapping mechanism is introduced to facilitate maintenance and management of IS-IS networks. The **is-name** command is used to configure a simple host name for a local router and enables the router to advertise it in an LSP.

After the configuration is completed, you can run the **display isis name-table** command to check the configured hostname.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure host name **RUTA** for the local IS-IS system.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] is-name RUTA
```

Related Topics

9.6.27 display isis name-table

9.6.93 is-name map

Function

The **is-name map** command enables the local router to identify the host name in LSPs, and sets a static host name for a remote IS-IS system on the local router.

The **undo is-name map** command disables the local router from identifying the host name in LSPs, and deletes the static host name for a remote IS-IS system set by the local router.

By default, the local device does not have the static host name of a remote IS-IS system.

Format

is-name map *system-id symbolic-name*

undo is-name map *system-id* [*symbolic-name*]

Parameters

Parameter	Description	Value
system-id	Specifies the ID of the remote mapped IS-IS system or pseudonode ID.	The format is XXXX.XXXX.XXXX[.XX].
symbolic-name	Specifies the static host name of the remote mapped IS-IS system.	The value is a string of 1 to 64 characters without spaces. It is case sensitive. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When checking information about IS-IS neighbors and LSDBs on the router that runs IS-IS, each router in the IS-IS routing domain is represented by a system ID with a 12-bit hexadecimal number, for example, aaaa.eeee.1234. This representation is complicated and not easy to use. To manage and maintain IS-IS networks conveniently, IS-IS uses the dynamic host name exchange mechanism. The **is-name map** command can configure a host name for the remote router and does not advertise the host name through an LSP.

After running the **is-name map** command to map the remote router to the host name, you can find that the system ID of the remote router is replaced by the host name configured using the **display isis name-table** command.

Precautions

This configuration is static configuration and takes effect only on the local device. Therefore, the configured host name *symbolic-name* is not advertised through an LSP. If dynamic host name mapping is configured on an IS-IS device, dynamic host name mapping takes precedence over static host name mapping.

Example

Configure static host name mapping for the IS-IS system on the remote router as 0000.0000.0041.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] is-name map 0000.0000.0041 RUTB
```

Related Topics

9.6.27 display isis name-table

9.6.94 log-peer-change

Function

The **log-peer-change** command enables the output of IS-IS adjacency changes.

The **undo log-peer-change** command disables the output of IS-IS adjacency changes.

By default, the output of IS-IS adjacency changes is disabled.

Format

log-peer-change [**topology**]

undo log-peer-change

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
topology	Enables the output of the IS-IS adjacency changes in an IPv6 topology.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, IS-IS adjacency changes pose a threat to network stability, causing frequent route convergence which consumes a lot of memory resources and possible traffic loss. Therefore, diagnose the fault immediately when the IS-IS adjacency changes.

To locate the fault, run the **log-peer-change** command to enable the output of IS-IS adjacency changes and record the changes in the log.

Precautions

IS-IS adjacency changes are recorded only when the **terminal monitor** and **log-peer-change** commands are run.

Example

Enable the output of IS-IS adjacency changes on the current router.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] log-peer-change
```

Related Topics

4.3.41 terminal monitor

9.6.95 local-mt enable (IS-IS)

Function

The **local-mt enable** command enables IS-IS local MT.

The **undo local-mt enable** command disables IS-IS local MT.

By default, IS-IS local MT is not enabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

local-mt enable

undo local-mt enable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

This command can be configured only if IS-IS TE is enabled and the IS-IS cost type is wide, wide-compatible, or compatible.

Example

Enable IS-IS local MT.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] cost-style compatible
[Huawei-isis-1] traffic-eng
[Huawei-isis-1] local-mt enable
```

Related Topics

9.6.11 cost-style

9.6.96 local-mt filter-policy (IS-IS)

11.2.151 traffic-eng

9.6.96 local-mt filter-policy (IS-IS)

Function

The **local-mt filter-policy** command configures the policy of IS-IS local Multi Topology (MT).

The **undo local-mt filter-policy** command cancels the policy of IS-IS local MT.

By default, the policy of local MT is not configured.

Format

local-mt filter-policy { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* }

undo local-mt filter-policy

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of the basic ACL.	The value is an integer ranging from 2000 to 2999.
acl *acl-name*	Specifies the name of a Named ACL. It is case-sensitive.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

After the policy of local MT is configured, only the routes to the multicast source addresses are added to the Multicast IGP (MIGP) routing table. This saves CPU and memory resources.

For a Named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Configure the policy of IS-IS local MT.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] local-mt filter-policy acl 2000
```

Related Topics

9.6.95 local-mt enable (IS-IS)

 Copyright © Huawei Technologies Co., Ltd.

9.6.97 loop-free-alternate

Function

The **loop-free-alternate** command enables IS-IS Auto FRR to calculate loop-free backup routes using the loop-free alternate (LFA) algorithm.

The **undo loop-free-alternate** command disables IS-IS Auto FRR from calculating loop-free backup routes using the LFA algorithm.

By default, IS-IS Auto FRR is disabled from calculating loop-free backup routes using the LFA algorithm.

NOTE

AR100&AR120&AR150&AR160&AR200 series do not support IS-IS Auto FRR.

Format

loop-free-alternate [**level-1** | **level-2** | **level-1-2**]

undo loop-free-alternate [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Enables Level-1 IS-IS Auto FRR to generate loop-free backup routes. If the IS level is not specified, Level-1 and Level-2 IS-IS Auto FRR is enabled to generate backup routes.	-
level-2	Enables Level-2 IS-IS Auto FRR to generate loop-free backup routes. If the IS level is not specified, Level-1 and Level-2 IS-IS Auto FRR is enabled to generate backup routes.	-
level-1-2	Enables Level-1 and Level-2 IS-IS Auto FRR to generate loop-free backup routes.	-

Views

IS-IS FRR view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS Auto FRR pre-computes a backup link by using the Loop-Free Alternate (LFA) algorithm, and then adds the backup link and the primary link to the forwarding table. In the case of an IS-IS network failure, IS-IS Auto FRR can fast switch traffic to the backup link before routes on the control plane converge.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

To make IS-IS Auto FRR to take effect, enter the IS-IS FRR view and then run the **loop-free-alternate** command.

IS-IS can generate loop-free backup routes only when the IS-IS Auto FRR traffic protection inequality is met. For details of IS-IS Auto FRR, see the *Huawei AR Series Access Routers Feature Description - IP Routing*.

Example

Enable Level-2 IS-IS Auto FRR to generate loop-free backup routes.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] frr
[Huawei-isis-1-frr] loop-free-alternate level-2
```

Related Topics

9.6.46 frr (IS-IS)

9.6.69 isis lfa-backup

9.6.98 lsp-fragments-extend

Function

The **lsp-fragments–extend** command enables LSP fragment extension on the IS-IS router.

The **undo lsp-fragments-extend** command disables LSP fragment extension on the IS-IS router.

By default, LSP fragment extension is disabled on the IS-IS router.

Format

lsp-fragments-extend [[**level-1** | **level-2** | **level-1-2**] | [**mode-1** | **mode-2**]] *

undo lsp-fragments-extend [**mode-1** | **mode-2**] [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Enables LSP fragment extension on a Level-1 router.	-
level-2	Enables LSP fragment extension on a Level-2 router.	-
level-1-2	Enables LSP fragment extension on a Level-1-2 router.	-
mode-1	Indicates that the router supporting LSP fragment extension is compatible with the router with an earlier version that does not support LSP fragment extension.	-
mode-2	Requires that all the routers support LSP fragment extension. **NOTE** By default, **mode-1** and **level-1-2** are used.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

To enable the IS-IS router to generate extended LSP fragments, run the **9.6.128 virtual-system** command to configure at least one virtual system ID.

After the **lsp-fragments–extend** command is run, run the **9.6.107 reset isis all** command to restart the IS-IS process to make LSP fragment extension take effect.

Example

Enable Level-2 LSP fragment extension in mode 1.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] lsp-fragments-extend mode-1 level-2
```

Related Topics

9.6.128 virtual-system

9.6.107 reset isis all

9.6.99 lsp-length

Function

The **lsp-length** command sets the length of the LSP that is generated and received by the current IS-IS router.

The **undo lsp-length** command restores the default setting.

By default, the IS-IS router generates and receives 1497-byte LSPs.

Format

lsp-length { **originate** | **receive** } *max-size*

undo lsp-length { **originate** | **receive** }

Parameters

Parameter	Description	Value
originate	Indicates the maximum length of generated LSPs.	-
receive	Indicates the maximum length of received LSPs.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
max-size	Specifies the maximum length of LSPs. The *max-size* of a generated LSP must be smaller than or equal to the *max-size* of a received LSP.	The value is an integer that ranges from 512 to 16384, in bytes. The default value is 1497. **NOTE** Because the maximum MTU supported by interfaces is 9600 bytes and the LSP header length is 3 bytes, the allowed maximum LSP length is 9597 (9600 – 3) bytes to ensure that two devices on both ends communicate properly.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By controlling the length of LSPs generated and received by IS-IS routers, you can adjust the LSDB synchronization speed and change the network convergence speed.

Precautions

The *max-size* set using the **lsp-length** command must meet the following requirements:

- The MTU of an Ethernet interface must be greater than or equal to the sum of the value of *max-size* and 3.
- The MTU of a P2P interface must be greater than or equal to the value of *max-size*.

Example

Set the maximum length of an LSP generated by the IS-IS router to 1024 bytes.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] lsp-length originate 1024
```

9.6.100 maximum load-balancing (IS-IS)

Function

The **maximum load-balancing** command sets the maximum number of equal-cost routes for load balancing. You need to set the maximum value according to memory capacity.

The **undo maximum load-balancing** command restores the default maximum number of equal-cost routes for load balancing.

By default, the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204 support a maximum of four equal-cost routes, and the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series support a maximum of eight equal-cost routes, AR2240 (using SRU200, SRU200E or SRU400), and AR3200 (using SRU200, SRU200E or SRU400) series support a maximum of sixteen equal-cost routes.

Format

maximum load-balancing *number*

undo maximum load-balancing [*number*]

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost routes for load balancing.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple routes are available on an IS-IS network, multiple equal-cost routes may exist. Use the load balancing method to allocate traffic evenly to each link. This method improves link efficiency on the network and reduces the congestion possibility caused by overloaded links.

Specify the *number* parameter to limit the number of equal-cost routes for load balancing.

Precautions

To cancel load balancing, set the *number* parameter to 1 or run the **nexthop** command to set the preferences of equal-cost routes.

Example

Set the maximum number of equal-cost routes for load balancing to 2.

```
<Huawei> system-view
[Huawei] isis 100
[Huawei-isis-100] maximum load-balancing 2
```

Restore the default value.

```
<Huawei> system-view
[Huawei] isis 100
[Huawei-isis-100] undo maximum load-balancing
```

9.6.101 network-entity

Function

The **network-entity** command configures a network entity title (NET) for an IS-IS process.

The **undo network-entity** command deletes the NET of an IS-IS process.

By default, no NET is configured for an IS-IS process.

Format

network-entity *net*

undo network-entity *net*

Parameters

Parameter	Description	Value
net	Specifies a NET.	The format is X…X.XXXX.XXXX.XXXX.00, in which X…X indicates an area address, the 12 Xs in the middle indicate the system ID of the router, and the last 00 indicates the selector (SEL).

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NET is the special form of the network service access point (NSAP). After the IS-IS view is displayed, IS-IS can start only when a NET is configured for an IS-IS process.

A NET consists of the following parts:

- Area ID: is 1 to 13 bytes in length.
- System ID: is 6 bytes in length.
- SEL: is 1 byte in length and fixed as 00.

Generally, you only need to configure one NET for an IS-IS process. When an area needs to be redefined, for example, the area needs to be merged with other areas or divided into sub-areas, configure multiple NETs to ensure route correctness.

Precautions

An area address uniquely identifies an area in a routing domain. All the routers in the same Level-1 area must have the same area address. The routers in a Level-2 area can have different area addresses.

The system ID must be unique in the whole domain.

A maximum of three area addresses can be configured for an IS-IS process. Therefore, a maximum of three NETs can be configured for an IS-IS process. When configuring multiple NETs, ensure that their system IDs are the same.

Example

Set the NET to 10.0001.1010.1020.1030.00, in which the system ID is 1010.1020.1030 and the area ID is 10.0001.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] network-entity 10.0001.1010.1020.1030.00
```

Related Topics

9.6.56 isis

9.6.102 nexthop (IS-IS)

Function

The **nexthop** command sets the preference of equal-cost routes.

The **undo nexthop** command cancels the preference of equal-cost routes.

By default, no preference is set for equal-cost routes.

Format

nexthop *ip-address* **weight** *value*

undo nexthop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies a next-hop IP address.	The value is in dotted decimal notation.
weight *value*	Specifies the next-hop weight.	The value is an integer that ranges from 1 to 254.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When there are multiple redundant links on an IS-IS network, there may be multiple equal-cost routes to the same destination network segment.

You can use this command to set the next-hop preference to determine the next hop when the interface cost remains unchanged. A smaller preference value indicates a higher preference.

Precautions

After this command is used, an IS-IS device does not load balance traffic when forwarding the traffic. Instead, the device forwards the traffic to the next hop with the highest preference.

Example

Set the preference of IS-IS equal-cost routes.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] nexthop 10.0.0.3 weight 1
```

Related Topics

9.6.100 maximum load-balancing (IS-IS)

9.6.103 optional-checksum enable

Function

The **optional-checksum enable** command enables IS-IS to configure Hello packets and SNP packets to carry optional checksum TLVs and to check received IS-IS packets and SNP packets.

 Copyright © Huawei Technologies Co., Ltd.

The **undo optional-checksum enable** command restores IS-IS packets to default settings.

By default, Hello packets and SNPs do not carry checksum TLVs and the receiver does not check received packets.

Format

optional-checksum enable

undo optional-checksum enable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of malicious packets and to ensure packets are correctly received on an IS-IS network, you can configure the **optional-checksum enable** command to enable IS-IS routers to send SNP packets and Hello packets carrying optional checksum TLVs. After the peer device receives the packets, it checks whether the carried optional checksum TLVs are correct. If the TLVs are not correct, the peer device rejects the packets.

Prerequisites

You have run the **isis** command to create an IS-IS process and entered the IS-IS view.

Precautions

If MD5 authentication or Keychain authentication with valid MD5 authentication is configured on an IS-IS interface or area, IS-IS routers send Hello packets and SNP packets carrying no checksum TLVs and verify the checksum of the received packets.

Example

Configure IS-IS to add optional checksum TLVs to Hello packets and SNPs.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] optional-checksum enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.6.56 isis

9.6.104 preference (IS-IS)

Function

The **preference** command sets the IS-IS preference.

The **undo preference** command restores the default IS-IS preference.

The default IS-IS preference is 15.

Format

preference { *preference* | **route-policy** *route-policy-name* } *

undo preference

Parameters

Parameter	Description	Value
preference	Specifies the IS-IS preference. A smaller value indicates a higher preference.	The value is an integer that ranges from 1 to 255.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device may run multiple dynamic routing protocols and there may be multiple routes of different routing protocols to the same destination. Therefore, routing protocols may share and select routing information. To solve this problem, the system sets a preference for each routing protocol. If different protocols discover routes to the same destination, the system selects the route with a higher protocol preference to forward traffic.

The **preference** command can set the preference of IS-IS routes to affect routing information sharing and selection:

 Copyright © Huawei Technologies Co., Ltd.

- The **preference** *preference* command can set the preference for all IS-IS routes.
- The **preference** *preference* **route-policy** *route-policy-name* command can set different preferences for matched and unmatched routes.
- The **preference route-policy** *route-policy-name preference* command can set the preference for matched routes without affecting the preference of other IS-IS routes.

Precautions

You can use route-policies to set the preference for specified routes. If the **apply preference** clause is configured in the **route-policy** command, the route preference is as follows:

- The preference of matched routes is set using the **apply** clause.
- The preference of unmatched routes is set using the **preference** command.

As shown in the following example, the preference of the routes that pass route-policy **abc** is set to 50 and the preference of the routes that do not pass the route-policy is set to 30.

```
#
route-policy abc permit node 1
 if-match cost 20
 apply preference 50
#
isis 1
 preference 30 route-policy abc
```

If the **apply preference 50** clause is not configured in route-policy **abc**, the preference of all routes is set to 30.

Example

Set the IPv4 IS-IS preference to 25.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] preference 25
```

Related Topics

9.9.19 apply preference

9.6.105 purge-originator-identification enable

Function

The **purge-originator-identification enable** command configures IS-IS to add purge-originator-identification (POI) TLV to Purge packets. If a dynamic hostname has been configured for the local device, the hostname TLV is also added to the Purge packets.

The **undo purge-originator-identification enable** command deletes POI TLV and hostname TLV from Purge packets.

By default, Purge packets do not carry POI TLV or hostname TLV.

Format

purge-originator-identification enable [**always**]

undo purge-originator-identification enable [**always**]

Parameters

Parameter	Description	Value
always	Enables IS-IS to always add the POI TLV and dynamic hostname TLV to Purge LSPs to be sent.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When **Remaining Lifetime** of an LSP is 0, the LSP is invalid, and this invalid packet is a Purge packet. In most cases, a Purge packet does not carry any information about the router that generated the Purge packet. Without such information, troubleshooting is difficult if a network problem occurs.

To address this issue, you can run the **purge-originator-identification enable** command to configure IS-IS to add POI TLV to Purge packets. If a dynamic hostname has been configured for the local device, the hostname TLV is also added to the Purge packets, which facilitates troubleshooting.

- If the **purge-originator-identification enable** command is run and the any authentication is configured, generated Purge LSPs do not carry the POI TLV or hostname TLV.
- If the **purge-originator-identification enable** command is run and no authentication is configured, generated Purge LSPs will carry the POI TLV or hostname TLV.
- If the **purge-originator-identification enable always** command is run, generated Purge LSPs carry the POI TLV and hostname TLV, regardless of whether authentication is configured.

Example

Configure IS-IS to add POI TLV to Purge packets.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] purge-originator-identification enable
```

Related Topics

9.6.56 isis

9.6.106 prefix-priority (IS-IS)

Function

The **prefix-priority** command sets the convergence priority of IS-IS routes.

The **undo prefix-priority** command restores the default convergence priority of IS-IS routes.

By default, the convergence priority of IS-IS host routes and default routes is medium, and the convergence priority of other IS-IS routes is low.

Format

prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** } { **ip-prefix** *prefix-name* | **tag** *tag-value* }

undo prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** }

Parameters

Parameter	Description	Value
level-1	Specifies the convergence priority of Level-1 IS-IS routes.	-
level-2	Specifies the convergence priority of Level-2 IS-IS routes.	-
critical	Sets the convergence priority of IS-IS routes to critical.	-
high	Sets the convergence priority of IS-IS routes to high.	-
medium	Sets the convergence priority of IS-IS routes to medium.	-
ip-prefix *prefix-name*	Sets the convergence priority of the IS-IS routes matching the specified IP prefix.	The value is a string of 1 to 169 case-sensitive characters without spaces.
tag *tag-value*	Sets the convergence priority of the IS-IS routes with the specified tag value. To use the tag value to filter the IPv4 routes for which convergence priorities need to be set, ensure that the IS-IS cost style of sent packets is not narrow and the routes carry the tag value.	The value is an integer that ranges from 1 to 4294967295.

Views

IS-IS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a routing table has a large number of routing entries on an IS-IS device, the device needs to spend much time performing SPF calculation. To enable some key routes to be calculated first, run the **prefix-priority** command to set the convergence priority for these routes.

The convergence priorities of IS-IS routes are classified as critical, high, medium, and low in descending order.

The rules for applying convergence priorities to IS-IS routes are as follows:

- Existing IS-IS routes are converged based on the priorities set using the **prefix-priority** command.
- New IS-IS routes are converged based on the priorities set using the **prefix-priority** command.
- If an IS-IS route conforms to the matching rules of multiple convergence priorities, the highest convergence priority is used.
- If the route level is not specified, the **prefix-priority** command configuration takes effect for both Level-1 and Level-2 IS-IS routes.

Precautions

The **prefix-priority** command applies only to the public network.

After the **prefix-priority** command is run to set the convergence priority for IS-IS routes (including IS-IS host routes and default routes), the convergence priority of all the IS-IS routes that meet the matching rules is changed according to the command configuration, and the convergence priority of the IS-IS routes that do not meet the matching rules is changed to low.

Example

Set the convergence priority of Level-1 routes with tag value 3 to critical.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] prefix-priority level-1 critical tag 3
```

Set the convergence priority of the routes matching IP prefix **p1** to medium.

```
<Huawei> system-view
[Huawei] ip ip-prefix p1 permit 192.168.0.1 24
[Huawei] isis 1
[Huawei-isis-1] prefix-priority medium ip-prefix p1
```

Related Topics

9.6.56 isis
9.9.47 ip ip-prefix

 Copyright © Huawei Technologies Co., Ltd.

9.6.107 reset isis all

Function

The **reset isis all** command restarts IS-IS processes.

Format

reset isis all [[*process-id* | **vpn-instance** *vpn-instance-name*] | **graceful-restart**] *

reset isis *process-id* **all** [**graceful-restart**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an IS-IS process to be restarted.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance. *vpn-instance-name* specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
graceful-restart	Restarts an IS-IS process in GR mode.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset isis all** command is used when LSPs need to be updated immediately. For example, after the **9.6.2 area-authentication-mode** and **9.6.42 domain-authentication-mode** commands are used, you can run the **reset isis all** command to clear old LSPs.

Precautions

NOTICE

Restarting IS-IS processes may interrupt services. Therefore, confirm the action before running the **reset isis all** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Restart IS-IS processes.

```
<Huawei> reset isis all
Warning: The ISIS process(es) will be reset. Continue?[Y/N]y
```

Related Topics

9.6.2 area-authentication-mode

9.6.42 domain-authentication-mode

9.6.108 reset isis peer

Function

The **reset isis peer** command resets a specified IS-IS neighbor relationship.

Format

reset isis peer *system-id* [*process-id* | **vpn-instance** *vpn-instance-name*]

reset isis *process-id* **peer** *system-id*

Parameters

Parameter	Description	Value
system-id	Specifies the system ID of an IS-IS neighbor.	The value is 6 bytes in length and in XXXX.XXXX.XXXX format.
process-id	Specifies the IS-IS process ID for which the neighbor relationship needs to be reset.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the IS-IS multi-instance process in a specified VPN instance. This parameter is optional for a default VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset isis peer** command is used when a device needs to re-establish the neighbor relationship with a specified neighbor.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Exercise caution when using the **reset isis peer** command. This command will re-establish neighbor relationships with a specified neighbor, which may result in route flapping.

Example

Reset the IS-IS neighbor with system ID 0000.0c11.1111.

```
<Huawei> reset isis peer 0000.0c11.1111
```

9.6.109 reset isis statistics packet

Function

The **reset isis statistics packet** command clears IS-IS packet statistics.

Format

reset isis statistics packet lsp { *process-id* | **vpn-instance** *vpn-instance-name* }

reset isis [*process-id*] **statistics packet lsp**

Parameters

Parameter	Description	Value
process-id	Specifies the ID of the IS-IS process whose IS-IS packet statistics are to be cleared.	The value is an integer ranging from 1 to 65535.
lsp	Deletes statistics about LSPs.	-
vpn-instance *vpn-instance-name*	Deletes LSP packet statistics of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When troubleshooting IS-IS network faults, you can run the **reset isis statistics packet** command to clear the existing statistics before checking new information about incorrect LSPs and Hello packets.

Example

Clear packet statistics of IS-IS process 1.

```
<Huawei> reset isis 1 statistics packet lsp
```

9.6.110 reset isis statistics purge-lsp

Function

The **reset isis statistics purge-lsp** command deletes statistics about purge LSPs of a specified IS-IS process.

Format

reset isis statistics purge-lsp [**level-1** | **level-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an IS-IS process.	The value is an integer ranging from 1 to 65535.
vpn-instance *vpn-instance-name*	Deletes statistics about IS-IS purge LSPs of specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

To locate a problem on an IS-IS network, you can run the **reset isis statistics purge-lsp** command to delete existing statistics about purge LSPs and then check the latest statistics.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete statistics about purge LSPs of IS-IS process 1.

```
<Huawei> reset isis 1 statistics purge-lsp
```

9.6.111 reset isis suppress-flapping peer

Function

The **reset isis suppress-flapping peer** command forces an interface to exit from IS-IS neighbor relationship flapping suppression.

Format

reset isis *process-id* **suppress-flapping peer** [**interface** *interface-type interface-number*] [**notify-peer**]

Parameters

Parameter	Description	Value
process-id	Specifies the ID of an IS-IS process.	The value is an integer ranging from 1 to 65535.
interface-type interface-number	Specifies an interface type and number.	-
notify-peer	Instructs neighbors to exit from IS-IS neighbor relationship flapping suppression too.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Interfaces exit from flapping suppression in the following scenarios:

- The suppression timer expires.
- The corresponding IS-IS process is reset.
- An IS-IS neighbor is reset using the **reset isis peer** command.
- IS-IS neighbor relationship flapping suppression is disabled globally using the **suppress-flapping peer disable (IS-IS)** command in the IS-IS view.
- The **reset isis suppress-flapping peer** command is run.

 Copyright © Huawei Technologies Co., Ltd.

- Suppression is aborted forcibly using the **reset isis suppress-flapping peer** [*interface-type interface-number*] **notify-peer** command on the remote device.

Example

Force interfaces to exit from IS-IS neighbor relationship flapping suppression.

```
<Huawei> reset isis 1 suppress-flapping peer
```

Related Topics

9.6.108 reset isis peer

9.6.121 suppress-flapping peer disable (IS-IS)

9.6.112 set isis bfd delete delay-time

Function

The **set isis bfd delete delay-time** command configures the delay after which BFD reports an Up event during association between IS-IS Auto FRR and BFD.

The **undo set isis bfd delete delay-time** command restores the default delay after which BFD reports an Up event during association between IS-IS Auto FRR and BFD.

By default, during association between IS-IS Auto FRR and BFD, the delay after which BFD reports an Up event is 5s.

NOTE

AR100&AR120&AR150&AR160&AR200 series routers do not support this command.

Format

set isis bfd delete delay-time *delay-time*

undo set isis bfd delete delay-time

Parameters

Parameter	Description	Value
delay-time	Specifies the delay after which BFD reports an Up event during association between IS-IS Auto FRR and BFD.	The value is an integer that ranges from 5 to 50, in seconds. By default, the value is 5s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In association between IS-IS Auto FRR and BFD, the default duration for the process of BFD session deletion, BFD session setup, and Up event report is 5s during an active/standby link switchover. If a large number of IS-IS routes are configured in the scenario, some routes cannot be re-established within 5s. However, the system has received the Up event reported by BFD and determines that the link switchover is complete. Services are forwarded based on the switched link. As a result, some routes are not established and some packets fail to be forwarded.

To solve this problem, run the **set isis bfd delete delay-time** *delay-time* command to increase the delay after which BFD reports an Up event during an active/standby link switchover.

Example

Set the delay after which BFD reports an Up event to 10s.

```
<Huawei> system-view
[Huawei] set isis bfd delete delay-time 10
```

9.6.113 set-overload

Function

The **set-overload** command sets the overload bit for non-pseudonode LSPs.

The **undo set-overload** command removes the overload bit of non-pseudonode LSPs.

By default, no overload bit is set for non-pseudonode LSPs.

Format

set-overload [**on-startup** [*timeout1* | **start-from-nbr** *system-id* [*timeout1* [*timeout2*]] | **wait-for-bgp** [*timeout1*]] [**send-sa-bit** [*timeout3*]]] [**allow** { **interlevel** | **external** }*]

undo set-overload

Parameters

Parameter	Description	Value
on-startup	Indicates that the overload bit remains set within the specified period when the router restarts or is faulty.	-
timeout1	Specifies the duration of the overload bit after the system starts.	The value is an integer that ranges from 5 to 86400, in seconds. The default value is 600 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
start-from-nbr *system-id*	Specifies the duration of the system overload bit according to the status of a specified neighbor.	The value is in XXXX.XXXX.XXXX format.
timeout1 [*timeout2*]	Specifies the period during which the overload bit remains set, which is related to the neighbor status.	• If the specified neighbor does not go Up before *timeout2* expires, the duration of the system overload bit is *timeout2*. *timeout2* ranges from 5 to 86400, in seconds. The default value is 1200 seconds (20 minutes). • If the specified neighbor goes Up before *timeout2* expires, the duration of the system overload bit is *timeout1*. *timeout1* ranges from 5 to 86400, in seconds. The default value is 600 seconds (10 minutes).
wait-for-bgp	Specifies the period during which the overload bit of the system remains set according to the BGP convergence status.	-
send-sa-bit	Specifies the overload bit remains in Hello packets after the device is started.	-
timeout3	Specifies the period during which the overload bit remains in Hello packets after the device is started.	The value is an integer ranging from 5 to 120, in seconds. The default value is 30 seconds.
allow	Allows advertising IP prefixes. By default, the system is prohibited from advertising IP prefixes when the system enters the overload state.	-
interlevel	Allows advertising the IP prefixes learned from IS-IS of different levels when **allow** is specified.	-
external	Allows advertising the IP prefixes learned from other protocols when **allow** is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Although LSPs with the overload bit are flooded on the network, the LSPs are ignored in the calculation of the routes that pass through the router in overload state. That is, after the overload bit is set on the router, other routers ignore the router when performing SPF calculation. Direct routes of the router are not ignored during SPF calculation.

To prevent the local router from being used by other routers to perform SPF calculation, run the **set-overload** command on the local router without specifying the **on-startup** keyword. Then the system immediately sets the overload bit in the LSP to be sent. To remove the overload bit, run the **undo set-overload** command.

When the local router restarts or is faulty, to prevent the local router from being used by other routers to perform SPF calculation, run the **set-overload** command on the local router and specify the **on-startup** keyword.

When the router is experiencing memory shortage, the system automatically sets the overload bit in the sent LSPs regardless of whether the **set-overload** command is run.

You can set the overload bit to solve the problem of network traffic loss caused by the difference between the BGP convergence speed and IGP convergence speed.

Precautions

If a TE LSP uses the local device as a transit node before the **set-overload** command is run, the TE LSP is not torn down and re-established and still uses the local device as a transit node after the **set-overload** command is run; if the local device is restarted after the command is run and fast convergence is not configured on the ingress of the RSVP-LSP, TE LSP forwarding fails, and services are affected. Therefore, the **mpls te path-selection overload** command needs to be run on the ingress of the RSVP-LSP before the device is restarted.

Example

Set the overload bit for IS-IS process 1.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] set-overload
Warning: The IS-IS process overload state will be set. Continue?[Y/N]
```

Configure IS-IS process 1 to enter the overload state during the startup, and configure the local router to remain the overload state for 300 seconds after it establishes the neighbor relationship with neighbor 0000.0000.0002 within 1000 seconds during which the system starts.

```
<Huawei> system-view
[Huawei] isis
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-isis-1] set-overload on-startup start-from-nbr 0000.0000.0002 300 1000
```

Configure IS-IS process 1 to enter the overload state during the startup, allow IS-IS to advertise the IP prefixes learned from IS-IS of different levels, and prohibit IS-IS from advertising the IP prefixes learned from other protocols.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] set-overload on-startup allow interlevel
```

9.6.114 snmp-agent trap enable feature-name isis

Function

The **snmp-agent trap enable feature-name isis** command enables the trap function for the IS-IS module.

The **undo snmp-agent trap enable feature-name isis** command disables the trap function for the IS-IS module.

By default, the trap function is disabled for the IS-IS module.

Format

snmp-agent trap enable feature-name isis [**trap-name** { **isisadjacencychange** | **isisareamismatch** | **isisattempttoexceedmaxsequence** | **isisauthenticationfailure** | **isisauthenticationtypefailure** | **isiscorruptedlspdetected** | **isisdatabaseoverload** | **isisidlenmismatch** | **isislsptoolargetopropagate** |**isismanualaddressdrops** | **isismaxareaaddressesmismatch** | **isisoriglspbuffsizemismatch** | **isisownlsppurge** | **isisprotocolssupportedmismatch** | **isisrejectedadjacency** | **isissequencenumberskip** | **isisversionskew** }]

undo snmp-agent trap enable feature-name isis [**trap-name** { **isisadjacencychange** | **isisareamismatch** | **isisattempttoexceedmaxsequence** | **isisauthenticationfailure** | **isisauthenticationtypefailure** | **isiscorruptedlspdetected** | **isisdatabaseoverload** | **isisidlenmismatch** | **isislsptoolargetopropagate** |**isismanualaddressdrops** | **isismaxareaaddressesmismatch** | **isisoriglspbuffsizemismatch** | **isisownlsppurge** | **isisprotocolssupportedmismatch** | **isisrejectedadjacency** | **isissequencenumberskip** | **isisversionskew** }]

Parameters

Parameter	Description	Value
trap-name	Specifies the trap name.	-
isisadjacencychange	Enables the trap function for neighbor changes.	-
isisareamismatch	Enables the trap function when the area address of the received Level-1 Hello packet does not match the local area address.	-

Parameter	Description	Value
isisattempttoexceedmaxsequence	Enables the trap function when the LSP sequence number reaches the maximum value.	-
isisauthenticationfailure	Enables the trap function when the authentication password in the received LSP is not the same as the local authentication password.	-
isisauthenticationtypefailure	Enables the trap function when the authentication type in the received LSP is not the same as the local authentication type.	-
isiscorruptedlspdetected	Enables the trap function when the LSP checksum authentication fails.	-
isisdatabaseoverload	Enables the trap function when the LSDB overload status changes.	-
isisidlenmismatch	Enables the trap function when the system ID length in the received LSP is not the same as the local system ID length.	-
isislsptoolargetopropagate	Enables the trap function when the PDU length exceeds the interface MTU.	-
isismanualaddressdrops	Enables the trap function when the number of Level-2 area addresses exceeds the maximum value and some Level-2 area addresses may be lost after IS-IS leaks Level-1 area addresses to the Level-2 area.	-
isismaxareaaddressesmismatch	Enables the trap function when the maximum area address in the received LSP does not match the local one.	-
isisoriglspbuffsizemismatch	Enables the trap function when the buffer size in the received LSP does not match the local one.	-
isisownlsppurge	Enables the trap function when an IS detects that its LSPs are purged on the network.	-
isisprotocolssupportedmismatch	Enables the trap function when the protocol type in the received LSP does not match the local protocol type.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
isisrejectedadjacency	Enables the trap function when the neighbor relationship cannot be established after IS-IS receives the Hello packet.	-
isissequencenumberskip	Enables the trap function when the local router receives the LSP sent by itself with the sequence number greater than that of the LSP in the local LSDB.	-
isisversionskew	Enables the trap function when the version in the Hello packet is incorrect.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for all non-excessive trap messages of the IS-IS module, specify **non-excessive all**.

To enable the trap function for one or more specific events of the IS-IS module, specify **trap-name**.

You can run the **display snmp-agent trap feature-name isis all** command to view all the trap messages of the IS-IS module.

Currently defined non-excessive trap messages of the IS-IS module include **isisattempttoexceedmaxsequence**, **isisdatabaseoverload**, **isismanualaddressdrops**, **isisownlsppurge**, and **isissequencenumberskip**.

NOTE

If the IS-IS trap function is enabled before a version upgrade, you need to run the **snmp-agent trap enable feature-name isis** command to re-enable the trap function after the version upgrade. Otherwise, the previous configuration is lost.

Example

Enable the trap function for IS-IS neighbor changes.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name isis trap-name isisadjacencychange
```

Related Topics

9.6.40 display snmp-agent trap feature-name isis all

9.6.115 snmp-agent trap enable feature-name isis-std

Function

The **snmp-agent trap enable feature-name isis-std** command enables the trap function for the IS-IS standard MIB.

The **undo snmp-agent trap enable feature-name isis-std** command disables the trap function of the IS-IS standard MIB.

By default, the trap function is disabled for the IS-IS standard MIB.

Format

snmp-agent trap enable feature-name isis-std [**trap-name** { **isisadjacencychange** | **isisareamismatch** | **isisattempttoexceedmaxsequence** | **isisauthenticationfailure** | **isisauthenticationtypefailure** | **isiscorruptedlspdetected** | **isisdatabaseoverload** | **isisidlenmismatch** | **isislsperrordetected** | **isislsptoolargetopropagate** |**isismanualaddressdrops** | **isismaxareaaddressesmismatch** | **isisoriglspbuffsizemismatch** | **isisownlsppurge** | **isisprotocolssupportedmismatch** | **isisrejectedadjacency** | **isissequencenumberskip** | **isisversionskew** }]

undo snmp-agent trap enable feature-name isis-std [**trap-name** { **isisadjacencychange** | **isisareamismatch** | **isisattempttoexceedmaxsequence** | **isisauthenticationfailure** | **isisauthenticationtypefailure** | **isiscorruptedlspdetected** | **isisdatabaseoverload** | **isisidlenmismatch** | **isislsperrordetected** | **isislsptoolargetopropagate** |**isismanualaddressdrops** | **isismaxareaaddressesmismatch** | **isisoriglspbuffsizemismatch** | **isisownlsppurge** | **isisprotocolssupportedmismatch** | **isisrejectedadjacency** | **isissequencenumberskip** | **isisversionskew** }]

Parameters

Parameter	Description	Value
isisadjacencychange	Enables the trap function for neighbor changes.	-
isisareamismatch	Enables the trap function when the area address of the received Level-1 Hello packet does not match the local area address.	-
isisattempttoexceedmaxsequence	Enables the trap function when the LSP sequence number reaches the maximum value.	-
isisauthenticationfailure	Enables the trap function when the authentication password in the received LSP is not the same as the local authentication password.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
isisauthenticationtypefailure	Enables the trap function when the authentication type in the received LSP is not the same as the local authentication type.	-
isiscorruptedlspdetected	Enables the trap function when the LSP checksum authentication fails.	-
isisdatabaseoverload	Enables the trap function when the LSDB overload status changes.	-
isisidlenmismatch	Enables the trap function when the system ID length in the received LSP is not the same as the local system ID length.	-
isislsperrordetected	Enables the trap function when the LSP fails to be parsed.	-
isislsptoolargetopropagate	Enables the trap function when the PDU length exceeds the interface MTU.	-
isismanualaddressdrops	Enables the trap function when the number of Level-2 area addresses exceeds the maximum value and some Level-2 area addresses may be lost after IS-IS leaks Level-1 area addresses to the Level-2 area.	-
isismaxareaaddressesmismatch	Enables the trap function when the maximum area address in the received LSP does not match the local one.	-
isisoriglspbuffsizemismatch	Enables the trap function when the buffer size in the received LSP does not match the local one.	-
isisownlsppurge	Enables the trap function when an IS detects that its LSPs are purged on the network.	-
isisprotocolssupportedmismatch	Enables the trap function when the protocol type in the received LSP does not match the local protocol type.	-
isisrejectedadjacency	Enables the trap function when the neighbor relationship cannot be established after IS-IS receives the Hello packet.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
isissequencenumberskip	Enables the trap function when the local router receives the LSP sent by itself with the sequence number greater than that of the LSP in the local LSDB.	-
isisversionskew	Enables the trap function when the version in the Hello packet is incorrect.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent trap feature-name isis-std all** command to view all the trap messages of the IS-IS standard MIB.

Example

Enable the trap function for IS-IS neighbor changes.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name isis-std trap-name isisadjacencychange
```

Related Topics

9.6.41 display snmp-agent trap feature-name isis-std all

9.6.116 spf-priority

Function

The **spf-priority** command sets the priority of SPF calculation.

The **undo spf-priority** command restores the default priority of SPF calculation.

By default, the priority of SPF calculation in a base topology is 64.

Format

spf-priority *priority-value*

undo spf-priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of SPF calculation. A larger value indicates a higher priority.	The value is an integer that ranges from 1 to 127.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

If a higher priority is set for a topology, routes of the topology instance are converged first, ensuring that important services are running properly.

Example

Set the priority of SPF calculation in an IPv4 base topology to 30.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] spf-priority 30
```

9.6.117 spf-slice-size

Function

The **spf-slice-size** command sets the maximum duration for IS-IS route calculation.

The **undo spf-slice-size** command restores the default setting.

By default, IS-IS route calculation lasts for a maximum of 2 ms at a time.

Format

spf-slice-size *duration-time*

undo spf-slice-size

Parameters

Parameter	Description	Value
duration-time	Specifies the maximum duration for IS-IS route calculation.	The value is an integer that ranges from 1 to 5000, in milliseconds. The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

When a routing table contains a large number of routes, run the **spf-slice-size** command to specify the maximum duration of SPF calculation to prevent route calculation from using system resources for a long period.

Example

Set the maximum duration of IS-IS route calculation to 50 ms.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] spf-slice-size 50
```

9.6.118 summary (IS-IS)

Function

The **summary** command configures IS-IS to generate summarized routes.

The **undo summary** command disables IS-IS from generating summarized routes.

By default, IS-IS does not generate summarized routes.

Format

summary *ip-address mask* [**avoid-feedback** | **generate_null0_route** | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] *

undo summary *ip-address mask* [**level-1** | **level-1-2** | **level-2**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a summarized route.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address of a summarized route.	The value is in dotted decimal notation.
avoid-feedback	Prevents summarized routes from being learned through SPF calculation.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
generate_null0_route	Generates null0 routes to prevent routing loops.	-
tag *tag*	Assigns administrative tags to advertised routes.	The value is an integer that ranges from 1 to 4294967295.
level-1	Summarizes only the routes imported into Level-1 areas. If no level is specified, Level-2 is used by default.	-
level-1-2	Summarizes the routes imported into Level-1 areas and the backbone network. If no level is specified, Level-2 is used by default.	-
level-2	Summarizes only the routes imported into the backbone network. If no level is specified, Level-2 is used by default.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Route summarization on a large-scale IS-IS network efficiently reduces routing entries. This minimizes system resource consumption and maintains system performance.

If a link frequently alternates between Up and Down, the links not involved in the route summarization will not be affected. Therefore, route summarization prevents route flapping on the network and improves network stability.

Precautions

Configuring route summarization does not affect the routing table of the local device because each specific route is still displayed in the routing table. Route summarization reduces the flooding of LSPs. Routing tables of other devices that receive the LSP from the local device contain only one summarized routes but not specific routes. Specific routes are still displayed in the routing table of the device directly connected to the summarized network segment.

Both IS-IS routes and routes imported from other protocols can be summarized. The lowest cost among that of the routes that are summarized is used as the cost of the summarized route.

 Copyright © Huawei Technologies Co., Ltd.

Example

Generate a summarized route with destination subnet 10.0.0.0/8.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] summary 10.0.0.0 255.0.0.0
```

9.6.119 suppress-flapping lsp-flood

Function

The **suppress-flapping lsp-flood** command configures a period for the system to delay LSP flooding during route flapping.

The **suppress-flapping lsp-flood disable** command restores the default configuration.

The **undo suppress-flapping lsp-flood** command restores the default configuration.

By default, if route flapping occurs, the device delays LSP flooding for 10s.

Format

suppress-flapping lsp-flood timer *delay-interval* [**threshold** *threshold-value*]

suppress-flapping lsp-flood disable

undo suppress-flapping lsp-flood

undo suppress-flapping lsp-flood timer *delay-interval* [**threshold** *threshold-value*]

undo suppress-flapping lsp-flood disable

Parameters

Parameter	Description	Value
delay-interval	Specifies a period for the system to delay LSP flooding during route flapping.	The value is an integer ranging from 1 to 600, in seconds.
threshold *threshold-value*	Specifies a route flapping threshold. If a route flaps for the specified number of times, LSP flooding is delayed.	The value is an integer ranging from 3 to 100, in times.

Views

IS-IS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On an IS-IS network, if the device receives an LSP with a routing information change, the device floods LSPs to advertise the change. If routing information changes frequently and LSPs are flooded immediately, a lot of system resources will be consumed. To prevent this problem, run the **suppress-flapping lsp-flood** command to configure a period for the device to delay LSP flooding during route flapping.

Configuration Impact

If the device delays LSP flooding too long, other devices on the network cannot detect the route information change in time, slowing down route convergence.

Example

Configure the device to delay flooding LSPs for 5s after a route flaps 10 times.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] suppress-flapping lsp-flood timer 5 threshold 10
```

9.6.120 suppress-flapping lsp-generation

Function

The **suppress-flapping lsp-generation** command configures a period for the system to delay generation of the same LSP during route flapping.

The **suppress-flapping lsp-generation disable** command restores the default configuration.

The **undo suppress-flapping lsp-generation** command restores the default configuration.

By default, the system delays generation of the same LSP for 10s during route flapping.

Format

suppress-flapping lsp-generation timer *delay-interval* [**threshold** *threshold-value*]

suppress-flapping lsp-generation disable

undo suppress-flapping lsp-generation

undo suppress-flapping lsp-generation timer *delay-interval* [**threshold** *threshold-value*]

undo suppress-flapping lsp-generation disable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delay-interval	Specifies a period for the system to delay generation of the same LSP during route flapping.	The value is an integer ranging from 1 to 600, in seconds.
threshold *threshold-value*	Specifies a route flapping threshold. If a route flaps for the specified number of times, LSP generation is delayed.	The value is an integer ranging from 3 to 100, in times.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, when the local routing information changes, the device sends LSPs to advertise the change. If the local routing information changes frequently and new LSPs are generated immediately, a lot of system resources will be consumed. To prevent this problem, run the **suppress-flapping lsp-generation** command to configure a period for the device to delay generation of the same LSP during route flapping.

Prerequisites

An IS-IS process has been created and the IS-IS view has been displayed using the **isis** command.

Configuration Impact

If the device delays generation of the same LSP too long, the local routing information cannot be advertised to neighbors in time, slowing down route convergence.

Example

Configure the device to delay generation of the same LSP for 5s after a route flaps 10 times.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] suppress-flapping lsp-generation timer 5 threshold 10
```

 Copyright © Huawei Technologies Co., Ltd.

9.6.121 suppress-flapping peer disable (IS-IS)

Function

The **suppress-flapping peer disable** command disables IS-IS neighbor relationship flapping suppression globally.

The **undo suppress-flapping peer disable** command enables IS-IS neighbor relationship flapping suppression globally.

By default, IS-IS neighbor relationship flapping suppression is enabled globally.

Format

suppress-flapping peer disable

undo suppress-flapping peer disable

Parameters

None

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

If an interface carrying IS-IS services alternates between Up and Down, IS-IS neighbor relationship flapping occurs on the interface. During the flapping, IS-IS reestablishes the neighbor relationship and recalculates routes. In this process, a large number of packets are exchanged, adversely affecting neighbor relationship stability, IS-IS services, and other IS-IS-dependent services, such as LDP and BGP. IS-IS neighbor relationship flapping suppression can address this problem by delaying IS-IS neighbor relationship reestablishment or preventing service traffic from passing through flapping links.

By default, IS-IS neighbor relationship flapping suppression is enabled globally. To disable this function globally, run the **suppress-flapping peer disable** command.

Example

Disable neighbor relationship flapping suppression globally.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] suppress-flapping peer disable
```

Related Topics

9.6.80 isis suppress-flapping peer disable

 Copyright © Huawei Technologies Co., Ltd.

9.6.122 suppress-flapping route-calculate

Function

The **suppress-flapping route-calculate** command configures a period for the device to delay route calculation when the device receives an LSP during route flapping.

The **suppress-flapping route-calculate disable** command restores the default configuration.

The **undo suppress-flapping route-calculate** command restores the default configuration.

By default, if the device receives an LSP during route flapping, it delays route calculation for 10s.

Format

suppress-flapping route-calculate timer *delay-interval* [**threshold** *threshold-value*]

suppress-flapping route-calculate disable

undo suppress-flapping route-calculate

undo suppress-flapping route-calculate timer *delay-interval* [**threshold** *threshold-value*]

undo suppress-flapping route-calculate disable

Parameters

Parameter	Description	Value
delay-interval	Specifies a period for the device to delay route calculation when the device receives an LSP during route flapping.	The value is an integer ranging from 1 to 600, in seconds.
threshold *threshold-value*	Specifies a route flapping threshold. If a route flaps for the specified number of times, route calculation is delayed.	The value is an integer ranging from 3 to 100, in times. By default, it is 30.

Views

IS-IS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On an IS-IS network, if the device receives an LSP with a routing information change, the device needs to calculate routes based on the LSP. If routing information changes frequently and routes are calculated immediately, a lot of system resources will be consumed. To prevent this problem, run the **suppress-flapping route-calculate** command to configure a period for the device to delay route calculation when the router receives an LSP during route flapping.

Prerequisites

An IS-IS process has been created and the IS-IS view has been displayed using the **isis** command.

Example

Configure the device to delay route calculation for 5s after a route flaps 10 times.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] suppress-flapping route-calculate timer 5 threshold 10
```

9.6.123 timer lsp-generation

Function

The **timer lsp-generation** command configures an intelligent timer for generating LSPs.

The **undo timer lsp-generation** command cancels the intelligent timer for generating LSPs.

By default, no intelligent timer is configured to generate LSPs.

Format

timer lsp-generation *max-interval* [*init-interval* [*incr-interval*]] [**level-1** | **level-2**]

undo timer lsp-generation [*max-interval* [*init-interval* [*incr-interval*]]] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
max-interval	Specifies the maximum delay in generating LSPs with the same LSP ID.	The value is an integer that ranges from 1 to 120, in seconds. The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
init-interval	Specifies the initial delay in generating LSPs.	The value is an integer that ranges from 1 to 60000, in milliseconds. By default, this delay is not used.
incr-interval	Specifies the incremental delay in generating two LSPs with the same LSP ID.	The value is an integer that ranges from 1 to 60000, in milliseconds. By default, this delay is not used.
level-1	Specifies the delay in generating Level-1 LSPs. If no level is specified, the delay in generating Level-1 and Level-2 LSPs is set.	-
level-2	Specifies the delay in generating Level-2 LSPs. If no level is specified, the delay in generating Level-1 and Level-2 LSPs is set.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, if the local routing information changes, a device needs to generate a new LSP to notify this change. If the local routing information changes frequently, a large number of new LSPs are generated, which occupies a lot of system resources and decreases system performance.

To speed up network convergence and prevent system from being affected, run the **timer lsp-generation** command to configure an intelligent timer for generating LSPs. This timer can adjust the delay in generating LSPs based on the routing information change frequency. This command can implement different functions when different parameters are specified:

- When only *max-interval* is specified, the intelligent timer functions as an ordinary one-time triggering timer.
- When both *init-interval* and *incr-interval* are specified, the delay in generating an LSP for the first time is determined by *init-interval*, and the delay in generating an LSP with the same LSP ID for the second time is determined by *incr-interval*. Subsequently, each time routes change, the delay in generating an LSP doubles the last delay until the delay reaches the value specified by *max-interval*. After the delay remains at the value specified by *max-interval* for three times or the IS-IS process is restarted, the delay decreases to the value specified by *init-interval*.

 Copyright © Huawei Technologies Co., Ltd.

- When *init-interval* is specified but *incr-interval* is not, the delay in generating an LSP for the first time is determined by *init-interval*, and the delay in generating subsequent LSPs is determined by *max-interval*. After the delay remains at the value specified by *max-interval* for three times or the IS-IS process is restarted, the delay decreases to the value specified by *init-interval*.
- The initial delay for generating an LSP is *init-interval*; the delay for generating the LSP with the same LSP ID is *incr-interval*. From the third time on, the delay for generating the LSP doubles each time until the delay reaches *max-interval*. After *max-interval* expires without flapping or the IS-IS process is restarted, the delay decreases to *init-interval*.
- The initial delay for generating an LSP is *init-interval*; the delay for generating the LSP with the same LSP ID is *incr-interval*. From the third time on, the delay for generating the LSP doubles each time until the delay reaches *max-interval*. After *max-interval* expires without flapping or the IS-IS process is restarted, the delay decreases to *init-interval*.

Precautions

If the delay in generating an LSP is too long, a device cannot advertise routing information changes to neighbors in time. This slows down network convergence.

Example

Set the delay in generating LSPs to 5s.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] timer lsp-generation 5
```

Set the maximum delay in generating LSPs to 20s, initial delay to 50 ms, and incremental delay to 2000 ms.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] timer lsp-generation 20 50 2000
```

9.6.124 timer lsp-max-age

Function

The **timer lsp-max-age** command sets the maximum lifetime for the LSPs generated by an IS-IS process.

The **undo timer lsp-max-age** command restores the default setting.

By default, the maximum lifetime of LSPs is 1200 seconds.

Format

timer lsp-max-age *age-time*

undo timer lsp-max-age

Parameters

Parameter	Description	Value
age-time	Specifies the maximum lifetime for LSPs.	The value is an integer that ranges from 2 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the router generates the system LSP, the system fills in the LSP with its maximum lifetime. After other routers receive this LSP, the lifetime of the LSP is reduced accordingly. If the router does not receive an updated LSP, the lifetime of the LSP is reduced to 0, and the router retains the LSP for another 60 seconds. If the router still does not received any updated LSP within 60 seconds, the router deletes the LSP.

You can run the **timer lsp-max-age** command to adjust the maximum lifetime of LSPs to ensure the validity of existing LSPs before new LSPs are received.

Precautions

The maximum lifetime of LSPs must be longer than the interval for updating LSPs to ensure that LSPs can be updated before being deleted.

Example

Set the maximum lifetime of the LSPs generated by the current IS-IS process to 25 minutes (1500 seconds).

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] timer lsp-max-age 1500
```

Related Topics

9.6.125 timer lsp-refresh

9.6.125 timer lsp-refresh

Function

The **timer lsp-refresh** command sets the interval for updating LSPs.

The **undo timer lsp-refresh** command restores the default setting.

By default, the interval for updating LSPs is 900 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

timer lsp-refresh *refresh-time*

undo timer lsp-refresh

Parameters

Parameter	Description	Value
refresh-time	Specifies the interval for updating LSPs.	The value is an integer that ranges from 1 to 65534, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, LSDB synchronization is implemented through LSP flooding. During LSP flooding, a device sends an LSP to its neighbors and then the neighbors send the received LSP to their respective neighbors except the device that first sends the LSP. In this manner, the LSP is flooded among the devices of the same level. LSP flooding allows each device of the same level to have the same LSP information and synchronize its LSDB with each other.

LSPs need to be periodically flooded. When the system generates the system LSP, the system fills in the LSP with its maximum lifetime. After other devices receive this LSP, the lifetime of the LSP is reduced accordingly. If the device does not receive an updated LSP, the lifetime of the LSP is reduced to 0, and the device retains the LSP for another 60 seconds. If the device still does not received any updated LSP within 60 seconds, the device deletes the LSP.

You can run the **timer lsp-refresh** command to set the interval for updating LSPs to control network convergence speed.

Precautions

If the interval for updating LSPs is small, LSPs may be updated frequently, which occupies a lot of bandwidth. If the interval is long, routing information changes cannot be notified in a timely manner.

Example

Set the interval for updating LSPs to 1200 seconds.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] timer lsp-refresh 1200
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.6.124 timer lsp-max-age

9.6.126 timer purge-zero-lsp route-calculate-delay

Function

The **timer purge-zero-lsp route-calculate-delay** command configures a period for the device to delay route calculation when the device receives a purge LSP.

The **undo timer purge-zero-lsp route-calculate-delay** command restores the default configuration.

By default, if the device receives a purge LSP, it delays route calculation for 10s.

Format

timer purge-zero-lsp route-calculate-delay *delay-interval*

undo timer purge-zero-lsp route-calculate-delay [*delay-interval*]

Parameters

Parameter	Description	Value
delay-interval	Specifies a period for the device to delay route calculation when the device receives a purge LSP.	The value is an integer ranging from 0 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IS-IS network, if a local LSP changes, the device sends a purge LSP to advertise the change. If purge LSPs are received or sent frequently and routes are recalculated immediately, a lot of system resources will be consumed. To prevent this problem, run the **timer purge-zero-lsp route-calculate-delay** command to configure a period for the device to delay route calculation when the device receives a purge LSP.

Prerequisites

An IS-IS process has been created and the IS-IS view has been displayed using the **isis** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the device to delay route calculation for 5s when the device receives a purge LSP.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] timer purge-zero-lsp route-calculate-delay 5
```

9.6.127 timer spf

Function

The **timer spf** command sets the delay in SPF calculation.

The **undo timer spf** command restores the default setting.

By default, the maximum delay in SPF calculation is 5 seconds.

Format

timer spf *max-interval* [*init-interval* [*incr-interval*]]

undo timer spf

Parameters

Parameter	Description	Value
max-interval	Specifies the maximum delay in SPF calculation.	The value is an integer that ranges from 1 to 120, in seconds. The default value is 5s.
init-interval	Specifies the initial delay in SPF calculation. If the *init-interval* parameter is not specified, the intelligent timer functions as an ordinary one-time triggering timer.	The value is an integer that ranges from 1 to 60000, in milliseconds. The default value is 50 milliseconds.
incr-interval	Specifies the incremental delay in two SPF calculations. If the *incr-interval* parameter is not specified, the delay in SPF calculation for the first time is determined by *init-interval*. From the second time on, the delay in SPF calculation is determined by *max-interval*.	The value is an integer that ranges from 1 to 60000, in milliseconds. The default value is 200 milliseconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IS-IS, route calculation is required when an LSDB changes. Frequent route calculations, however, consume lots of system resources and decrease system performance. Delaying SPF calculation can improve route calculation efficiency. However, a long delay in SPF calculation slows down route convergence.

To speed up route convergence without affecting the efficiency of routers, configure an intelligent timer for SPF calculation. This timer automatically adjusts the delay in SPF calculation based on the LSDB change frequency.

When SPF calculation is performed for the first time, the interval is *init-interval*. Each time a route changes, the interval is added by *incr-interval* until the interval reaches *max-interval*. After *max-interval* expires without flapping or the IS-IS process is restarted, the delay decreases to *init-interval*.

Example

Set the delay in SPF calculation to 5s.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] timer spf 5
```

Set the maximum delay in SPF calculation to 15s, initial delay to 10 ms, and incremental delay to 5000 ms.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] timer spf 15 10 5000
```

9.6.128 virtual-system

Function

The **virtual-system** command sets the virtual system ID for an IS-IS process. If no virtual system ID is set, no extended LSP can be generated. A maximum of 50 virtual system IDs can be configured for an IS-IS process.

The **undo virtual-system** command deletes the virtual system ID of an IS-IS process.

By default, no virtual system ID is configured for an IS-IS process.

Format

virtual-system *virtual-system-id*

undo virtual-system *virtual-system-id*

Parameters

Parameter	Description	Value
virtual-system-id	Specifies a virtual system ID for an IS-IS process.	The value is 6 bytes in length and in XXXX.XXXX.XXXX format.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Like a common system ID, a virtual system ID must be unique in a routing domain.

The **virtual-system** command is used together with the **lsp-fragments-extend** command. The configured virtual system ID takes effect only when LSP fragment extension is enabled and the IS-IS process is restarted using the **reset isis all** command.

If LSP fragment extension is not enabled and the IS-IS process is not restarted, you can configure the virtual system ID but the configured virtual system ID does not take effect.

Before running this command, run the **network-entity** command in the IS-IS view to configure a network entity title for the IS-IS process.

Example

Set the virtual system ID of IS-IS process 1 to 2222.2222.2222.

```
<Huawei> system-view
[Huawei] isis
[Huawei-isis-1] network-entity 10.0000.0000.0001.00
[Huawei-isis-1] virtual-system 2222.2222.2222
```

Related Topics

9.6.107 reset isis all

9.7 IPv6 IS-IS Configuration Commands

9.7.1 ipv6 auto-cost enable

Function

The **ipv6 auto-cost enable** command enables IS-IS to automatically calculate the interface cost on an IPv6 network according to the interface bandwidth.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 auto-cost enable** command disables IS-IS from automatically calculating the interface cost on an IPv6 network according to the interface bandwidth.

By default, the automatic interface cost calculation function is disabled on an IPv6 network.

Format

ipv6 auto-cost enable [**compatible**]

undo ipv6 auto-cost enable

Parameters

Parameter	Description	Value
compatible	Specifies the IS-IS to calculate the cost of an interface on an IPv6 network based on the bandwidth of the interface automatically in compatible.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function is enabled, for a certain IS-IS interface, if the cost of the interface is not configured in the interface view, and the global cost is not configured in the IS-IS view, the system calculates the cost for the interface automatically.

If the cost style of the system is wide or wide-compatible:

When **auto-cost enable** command is configured, Interface cost = (Bandwidth-reference/Link-bandwidth) x 10.

When **auto-cost enable compatible** command is configured, Interface cost = (Bandwidth-reference/Link-bandwidth).

The cost style is set by the **cost-style** command. The Bandwidth-reference is set by the **ipv6 bandwidth-reference** command. The Link-bandwidth is the interface bandwidth.

If the cost-style of the system is narrow, narrow-compatible, or compatible, the cost of each interface is determined according to the following table.

Table 9-123 Relationship of the IS-IS interface cost and the bandwidth

Cost	Range of Interface Bandwidth
60	Interface bandwidth ≤ 10 Mbit/s
50	10 Mbit/s < Interface bandwidth ≤ 100 Mbit/s
40	100 Mbit/s < Interface bandwidth ≤ 155 Mbit/s
30	155 Mbit/s < Interface bandwidth ≤ 622 Mbit/s
20	622 Mbit/s < Interface bandwidth ≤ 2.5 Gbit/s
10	2.5 Gbit/s < Interface bandwidth

Precautions

The priority of the cost value of the global IPv6 configured by the **ipv6 circuit-cost** command is higher than the auto cost value.

This command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

The **ipv6 auto-cost enable** command cannot change the cost of the loopback interface.

Example

Enable IS-IS to automatically calculate the interface cost on an IPv6 network according to the interface bandwidth.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 auto-cost enable
```

Related Topics

9.7.2 ipv6 bandwidth-reference

9.7.3 ipv6 circuit-cost

9.7.6 ipv6 enable(IS-IS)

9.7.2 ipv6 bandwidth-reference

Function

The **ipv6 bandwidth-reference** command sets the bandwidth reference value used in automatic interface cost calculation on an IPv6 network.

The **undo ipv6 bandwidth-reference** command restores the default setting.

By default, the bandwidth reference value is 100 Mbit/s.

Format

ipv6 bandwidth-reference *bandwidth-reference-value*

undo ipv6 bandwidth-reference

Parameters

Parameter	Description	Value
bandwidth-reference-value	Specifies the bandwidth reference value used in automatic interface cost calculation.	The value is an integer that ranges from 1 to 2147483648, in Mbit/s.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the link cost of IS-IS routes reflect the actual link cost, configure a proper link cost for all interfaces or enable the automatic interface cost calculation function. To enable automatic interface cost calculation, set a proper bandwidth reference value.

You can run the **ipv6 bandwidth-reference** command to set a proper reference bandwidth value. After the automatic interface cost calculation function is enabled, the system automatically calculates the interface cost according to the bandwidth reference value set using the command.

Precautions

The **ipv6 bandwidth-reference** command takes effect only after IPv6 is enabled for the IS-IS process using the **ipv6 enable** command.

Example

Set the IPv6 reference bandwidth value used in automatic interface cost calculation to 200 Mbit/s.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 bandwidth-reference 200
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.7.1 ipv6 auto-cost enable

9.7.6 ipv6 enable(IS-IS)

9.7.3 ipv6 circuit-cost

Function

The **ipv6 circuit-cost** command sets the cost value of all IPv6 interfaces in IS-IS SPF calculation, that is, the global IPv6 cost value.

The **undo ipv6 circuit-cost** command deletes the configured global IPv6 cost value.

By default, the global IPv6 cost value is not set.

Format

ipv6 circuit-cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo ipv6 circuit-cost [*cost* | **maximum**] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
cost	Specifies the cost value of IPv6 interfaces in IS-IS SPF calculation.	IF the IS-IS cost style is **wide** or **wide-compatible**, the cost value of imported routes ranges from 1 to 16777214. Otherwise, the value ranges from 1 to 63.
maximum	Sets the link cost value of an interface to 16777215. **NOTE** This parameter can be configured only when the IS-IS cost style is **wide** or **wide-compatible**. When the link cost value of an interface is set to 16777215, the neighbor TLV generated on the link cannot be used for route calculation and can only be used to transmit TE information.	-
level-1	Indicates the cost value of a Level-1 interface. If the interface level is not specified, the cost value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the cost value of a Level-2 interface. If the interface level is not specified, the cost value is set for Level-1 and Level-2 interfaces.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, multiple valid routes to the same destination are available on large IPv6 networks. IS-IS calculates the optimal routes using SPF calculation and chooses the optimal routes for traffic forwarding. This process often causes the following two problems:

- All the traffic is forwarded through the optimal route, which may cause unbalanced load.
- If the optimal route on a network is disconnected intermittently, traffic is still forwarded through the optimal route, which causes traffic loss.

To solve the preceding problems, run the **ipv6 circuit-cost** command to change the cost value of all interfaces at a time and traffic can be forwarded through different physical links.

Precautions

The priority of the IPv6 cost value on the interface is higher than the priority of the global IPv6 cost value.

The **ipv6 circuit-cost** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set the global IPv6 cost value in SPF calculation to 20.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 circuit-cost 20
```

Related Topics

9.7.6 ipv6 enable(IS-IS)

9.7.4 ipv6 circuit default-tag

Function

The **ipv6 circuit default-tag** command sets the administrative tag value of all interfaces in IS-IS processes on an IPv6 network.

The **undo ipv6 circuit default-tag** command restores the default tag value.

By default, the administrative tag value of all interfaces in IS-IS processes on an IPv6 network is 0.

 Copyright © Huawei Technologies Co., Ltd.

Format

ipv6 circuit default-tag *tag* [**level-1** | **level-2**]

undo ipv6 circuit default-tag [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag value of an interface in an IS-IS process on an IPv6 network.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates the administrative tag value of all Level-1 interfaces in IS-IS processes on an IPv6 network. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the administrative tag value of all Level-2 interfaces in IS-IS processes on an IPv6 network. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using the **ipv6 circuit default-tag** command, you can set the administrative tag value for all routes of a specified IS-IS process and use the tag to filter routes.

The administrative tag value is advertised together with the routing information.

- When the cost style of IS-IS is narrow or narrow-compatible, the administrative tag value is not advertised in the LSP and does not takes effect.
- When the cost style of IS-IS is wide, wide-compatible, or compatible, the administrative tag value is advertised in the LSP.

Precautions

The **ipv6 circuit default-tag** command takes effect only after IPv6 is enabled for the IS-IS process using the **ipv6 enable** command.

Example

Set the administrative tag value for a Level-1 IPv6 interface to 30.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 circuit default-tag 30 level-1
```

Related Topics

9.7.6 ipv6 enable(IS-IS)

9.7.5 ipv6 default-route-advertise

Function

The **ipv6 default-route-advertise** command configures the router to advertise default IPv6 routes.

The **undo ipv6 default-route-advertise** disables the router from advertising default IPv6 routes.

By default, the router does not advertise default IPv6 routes.

Format

ipv6 default-route-advertise [**always** | **match default** | **route-policy** *route-policy-name*] [**cost** *cost* | **tag** *tag* | [**level-1** | **level-2** | **level-1-2**]] * [**avoid-learning**]

undo ipv6 default-route-advertise

Parameters

Parameter	Description	Value
always	Indicates that the router always advertises default IPv6 routes.	-
match default	Indicates that if the routing table contains a default IPv6 route generated by other routing protocols but not IS-IS, the default route is advertised through an LSP.	-
route-policy *route-policy-name*	Specifies the name of a route-policy. A Level-1-2 device advertises default routes to the IS-IS routing domain only when there are external routes matching the route-policy in the routing table of the device. This prevents routing blackhole when link faults make some important external routes unavailable but default routes are still advertised. This route-policy does not affect external route import in IS-IS.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cost *cost*	Specifies the cost value of an advertised default route.	The value is an integer that ranges from 0 to 4261412864.
tag *tag*	Specifies the tag value of an advertised default route.	The value is an integer that ranges from 1 to 4294967295.
level-1	Sets the level of advertised default IPv6 routes to Level-1. If the level is not specified, Level-2 default routes are generated by default.	-
level-2	Sets the level of advertised default IPv6 routes to Level-2. If the level is not specified, Level-2 default routes are generated by default.	-
level-1-2	Sets the level of advertised default IPv6 routes to Level-1-2. If the level is not specified, Level-2 default routes are generated by default.	-
avoid-learning	Prevents an IS-IS process from learning default routes and adding them to the routing table. If there has been an active default IPv6 route in the routing table, the default IPv6 route becomes inactive after this parameter is specified.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, if other routing protocols are configured on an IS-IS network, to forward traffic in the IS-IS routing domain outside the domain, use the following two methods:

- Configure IS-IS on a Level-1-2 device to advertise default routes into the IS-IS routing domain.
- Configure IS-IS on a Level-1-2 device to import routes of other routing domains into the IS-IS routing domain.

Advertising default routes is easy to configure and does not require an IS-IS process to learn external routes. You can run the **ipv6 default-route-advertise**

command to configure IS-IS devices to advertise default routes into the IS-IS routing domain.

Precautions

Using the route-policy, you can force IS-IS to generate default routes only when there are matched routes in the routing table.

- If the **apply isis level-1** command is used in the route-policy view, IS-ISv6 can generate default routes in Level-1 LSPs. If the **apply isis level-1** command is used in the route-policy view, IS-IS can generate default routes in Level-1 LSPs.
- If the **apply isis level-2** command is used in the route-policy view, IS-ISv6 can generate default routes in Level-2 LSPs.
- If the **apply isis level-1-2** command is used in the route-policy view, IS-ISv6 can generate default routes in Level-1 and Level-2 LSPs.

The **ipv6 default-route-advertise** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Precautions

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, an ABR advertises the default IPv6 route to the IS-IS domain as long as the local routing table contains external routes.

Example

Configure the current router to generate default IPv6 routes in Level-1-2 LSPs.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 default-route-advertise level-1-2
```

Related Topics

9.7.6 ipv6 enable(IS-IS)

9.7.6 ipv6 enable(IS-IS)

Function

The **ipv6 enable** command enables the IPv6 capability of an IS-IS process.

The **undo ipv6 enable** command disables the IPv6 capability of an IS-IS process.

By default, the IPv6 capability of an IS-IS process is disabled.

Format

ipv6 enable [**topology** { **compatible** [**enable-mt-spf**] | **ipv6** | **standard** }]

undo ipv6 enable

Parameters

Parameter	Description	Value
topology	Specifies the network topology type.	-
compatible	Sets the topology type to compatible. That is, the standard topology and the IPv6 topology are compatible. After IS-IS IPv6 adjacency relationship is established, IS-IS advertises IPv6 topology links and standard topology links. SPF, however, runs only in a standard topology. The compatible mode is helpful in a transition from the standard topology to the IPv6 topology.	-
enable-mt-spf	Indicates that SPF runs in the IPv6 topology in compatible mode.	-
ipv6	Sets the topology type to IPv6. That is, the IPv6 capability of an IS-IS process can be enabled in an IPv6 topology. Links on the network can be configured as IPv4 or IPv6 links. SPF calculation is performed separately in IPv4 and IPv6 topologies.	-
standard	Sets the topology type to standard. That is, the IPv6 capability of an IS-IS process can be enabled in the integrated topology. Network administrators must ensure that all links on the network support the same topology mode. If the IPv6 capability of an IS-IS process is enabled, **standard** is used by default.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

To enable the IPv6 capability of an IS-IS process, perform the following operations:

1. Run the **ipv6** command in the system view to enable IPv6 globally.
2. Run the **isis** command to enable an IS-IS process.
3. Run the **network-entity** command to set a NET for IS-IS.
4. Run the **ipv6 enable** command in the IS-IS view to enable the IPv6 capability of an IS-IS process.
5. On each interface that needs to run an IS-IS process, run the **ipv6 enable** command to enable the IPv6 capability and configure an IPv6 address.
6. Run the **isis ipv6 enable** command to enable IS-IS for IPv6 on each interface.

Example

Enable the IPv6 capability in the IPv6 topology in IS-IS process 1.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] network-entity 10.0001.1010.1020.1030.00
[Huawei-isis-1] ipv6 enable topology ipv6
```

Related Topics

9.6.56 isis

9.6.101 network-entity

8.8.28 ipv6 enable (interface view)

9.7.18 isis ipv6 enable

9.7.7 ipv6 filter-policy export

Function

The **ipv6 filter-policy export** command configures a filtering policy to allow IS-IS to filter the imported IPv6 routes to be advertised.

The **undo ipv6 filter-policy export** command cancels the filtering function.

By default, IS-IS does not filter imported IPv6 routes to be advertised.

Format

ipv6 filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*] | **unr**]

undo ipv6 filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **export** [*protocol* [*process-id*] | **unr**]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value of *acl6-name* is a string of 1 to 32 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the imported routes that need to be filtered when the routes are advertised. Currently, the *protocol* can be **direct**, **static**, **ripng**, **bgp**, **unr**, **ospfv3**, or another **isis** process. If the *protocol* parameter is not specified, all imported routes are filtered.	-
process-id	Specifies the process ID if *protocol* is **ripng**, **ospfv3**, or another **isis** process.	The value is an integer that ranges from 1 to 65535.
unr	Indicates the imported UNR routes that need to be filtered when the routes are advertised.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

The **ipv6 filter-policy export** command together with the **ipv6 import-route** command can be used to filter only the imported routes that are advertised to other routers. If *protocol* is not specified, the routes that are imported from all other protocols are filtered. If *protocol* is specified, the routes that are imported from the specific protocol are filtered.

The **ipv6 filter-policy export** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Configure IS-IS to filter the imported IPv6 routes before advertising the routes to other routers.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
```

```
[Huawei-isis-1] ipv6 filter-policy route-policy test export
```

Related Topics

9.7.8 ipv6 filter-policy import

9.7.6 ipv6 enable(IS-IS)

9.7.8 ipv6 filter-policy import

Function

The **ipv6 filter-policy import** command configures a filtering policy to allow IS-IS to filter the received routes to be added to the IPv6 routing table.

The **undo ipv6 filter-policy import** command cancels the filtering function.

By default, IS-IS does not filter the received routes to be added to the IPv6 routing table.

Format

ipv6 filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo ipv6 filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name*] **import**

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value of *acl6-name* is a string of 1 to 32 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy to filter routes based on tag and other protocol parameters.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IS-IS routing entries need to be added to an IPv6 routing table to guide IPv6 packet forwarding. If an IS-IS routing table has routes destined for a specified network segment, but these routes do not need to be sent to the IPv6 routing table, run the **ipv6 filter-policy import** command and specify an IPv6 prefix list or a route-policy to allow only the required IS-IS routes to be added to the IPv6 routing table.

Precautions

The **ipv6 filter-policy import** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

For a IPv6 named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all IPv6 routes received by IS-IS are delivered to the IPv6 routing table.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all IPv6 routes received by IS-IS are delivered to the IPv6 routing table.

Example

Filter received IPv6 routes using a route-policy.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 filter-policy route-policy test import
```

Related Topics

9.7.7 ipv6 filter-policy export

9.7.6 ipv6 enable(IS-IS)

9.7.9 ipv6 import-route

Function

The **ipv6 import-route** command configures IS-IS to import IPv6 routes from other routing protocols.

The **undo ipv6 import-route** command disables IS-IS form importing IPv6 routes from other routing protocols.

By default, IS-IS does not import IPv6 routes from other routing protocols.

Format

ipv6 import-route { **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

ipv6 import-route { **static** | **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } [**cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

ipv6 import-route limit *limit-number* [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

undo ipv6 import-route { **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } **inherit-cost** [**tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo ipv6 import-route { **static** | **direct** | **unr** | { **ospfv3** | **ripng** | **isis** } [*process-id*] | **bgp** [**permit-ibgp**] } [**cost** *cost* | **tag** *tag* | **route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo ipv6 import-route limit [*limit-number*] [**threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*] { **level-1** | **level-2** | **level-1-2** }

Parameters

Parameter	Description	Value
direct	Indicates that the imported routes are direct routes.	-
static	Indicates that the imported routes are activated static routes.	-
unr	Indicates that the routing protocol from which routes are imported is UNR. The user network route (UNR) is used to allocate routes to user traffic when users cannot use dynamic routing protocols during logins.	-
ospfv3	Indicates that the routing protocol from which routes are imported is OSPFv3.	-
ripng	Indicates that the routing protocol from which routes are imported is RIPng.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
isis	Indicates that the routing protocol from which routes are imported is IS-IS.	-
process-id	When the protocol is **ospfv3**, **ripng**, or **isis**, a process ID needs to be specified.	The value is an integer that ranges from 1 to 65535.
bgp	Indicates that the routing protocol from which routes are imported is BGP.	-
permit-ibgp	Indicates that the imported routes are IBGP routes. If this parameter is not set, only EBGP routes can be imported.	-
inherit-cost	Indicates that the original cost value of imported external routes is retained.	-
cost *cost*	Specifies the cost value of imported routes.	The value is an integer that ranges from 0 to 4261412864. The default value is 0.
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
level-1	Indicates that routes are imported into Level-1 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
level-2	Indicates that routes are imported into Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-
level-1-2	Indicates that routes are imported into Level-1 and Level-2 routing tables. If no level is specified, routes are imported to Level-2 routing tables by default.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
limit *limit-number*	Specifies the maximum number of external IPv6 routes allowed to be imported to the IS-IS area.	The value is an integer ranging from 1 to 10000000.
threshold-alarm	Specifies the alarm threshold for imported routes.	-
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 80.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for imported routes.	The value is an integer ranging from 1 to 100. The default value is 70.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If other routing protocols are configured on an IS-IS network, to forward traffic in the IS-IS routing domain outside the domain, use either of the following methods:

- Configure IS-IS on a Level-1-2 device to advertise default routes into the IS-IS routing domain.
- Configure IS-IS on a Level-1-2 device to import routes of other routing domains into the IS-IS routing domain.

If there are multiple Level-1-2 devices in the IS-IS routing domain, optimal routes destined for another routing domain need to be selected. This requires all devices in the IS-IS routing domain learn all or some external routes.

Configure IS-IS on a Level-1-2 device to import routes of other routing domains into the IS-IS routing domain. Alternatively, run the **route-policy** *route-policy-name* command to import some external routes from other routing domains.

Prerequisites

IS-IS has been enabled using the **isis** command and the IS-IS view has been displayed. IPv6 has been enabled for the IS-IS process using the **ipv6 enable** command.

Precautions

When routes of other routing protocols are imported, you can set the cost value and cost style of the imported routes. You can also configure IS-IS to retain the original cost value of the imported external routes. During route advertisement and route calculation, the original cost values of these routes are used. In this

case, the cost style and cost value of the imported routes cannot be set, and static routes cannot be imported.

After the **ipv6 import-route direct** command is executed, routes to the network segment where the IPv6 address of the management interface belongs are also imported in the IS-IS routing table. Therefore, use this command with caution.

Example

Configure IS-IS to import static IPv6 routes and set the cost value of the routes to 15.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 import-route static cost 15
```

Configure IS-IS to import OSPFv3 routes and retain the original cost value of the routes.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 import-route ospfv3 1 inherit-cost
```

Related Topics

9.6.53 import-route (IS-IS)

9.6.56 isis

9.7.6 ipv6 enable(IS-IS)

9.7.10 ipv6 import-route isis level-1 into level-2

Function

The **ipv6 import-route isis level-1 into level-2** command configures IPv6 route leaking from Level-1 areas to Level-2 areas.

The **undo ipv6 import-route isis level-1 into level-2** command prohibits IPv6 route leaking from Level-1 areas to Level-2 areas.

By default, all Level-1 routing information, excluding information about default routes, is leaked to Level-2 areas.

Format

ipv6 import-route isis level-1 into level-2 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

undo ipv6 import-route isis level-1 into level-2 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct allow-filter-policy**] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy for IPv6 routes.	-
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL.	The value of *acl6-name* is a string of 1 to 32 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list. Only the routes that match the IPv6 prefix can be imported to Level-2 areas.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Specifies the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can be shared with the Level-2 area with this parameter, and all Level-1 area direct routing information will be shared with the Level-2 area without this parameter.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

The **ipv6 import-route isis level-1 into level-2** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

For a IPv6 named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Precautions

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all IPv6 routes in the Level-1 area leak to the Level-2 area.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all IPv6 routes in the Level-1 area leak to the Level-2 area.

Example

Control IPv6 route leaking from Level-1 areas to Level-2 areas on Level-1-2 routers using IPv6 prefix list **list**.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 import-route isis level-1 into level-2 filter-policy ipv6-prefix list
```

Related Topics

9.7.11 ipv6 import-route isis level-2 into level-1

9.7.6 ipv6 enable(IS-IS)

9.7.11 ipv6 import-route isis level-2 into level-1

Function

The **ipv6 import-route isis level-2 into level-1** command configures IPv6 route leaking from Level-2 areas to Level-1 areas.

The **undo ipv6 import-route isis level-2 into level-1** command prohibits IPv6 route leaking from Level-2 areas to Level-1 areas.

By default, Level-2 routing information is not leaked to Level-1 areas.

Format

ipv6 import-route isis level-2 into level-1 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

undo ipv6 import-route isis level-2 into level-1 [**filter-policy** { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag* | **direct** { **allow-filter-policy** | **allow-up-down-bit** } *] *

Parameters

Parameter	Description	Value
filter-policy	Specifies a filtering policy for IPv6 routes.	-
acl6-number	Specifies the number of a basic ACL6.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 named ACL. The value is a string of case-sensitive characters.	The value of *acl6-name* is a string of 1 to 32 case-sensitive characters without spaces.
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
tag *tag*	Specifies the administrative tag of imported routes.	The value is an integer that ranges from 1 to 4294967295.
direct allow-filter-policy	Specifies the filtering policy to filter the direct routes. Only the IS-IS Level-1 area direct routing information that matches the filtering policy can be shared with the Level-2 area with this parameter, and all Level-1 area direct routing information will be shared with the Level-2 area without this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
direct allow-up-down-bit	Indicates that the Up or Down bit is used during the leak of directs routes. If **direct allow-up-down-bit** is specified, the direct routes that have already leaked to the Level-1 area have the lowest priority and cannot leak back.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

The **ipv6 import-route isis level-2 into level-1** command must be configured on Level-1-2 routers at the area border.

The **ipv6 import-route isis level-2 into level-1** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

For a IPv6 named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Precautions

Creating an ACL6 or IPv6 prefix list before it is referenced is recommended. If a nonexistent ACL6 or IPv6 prefix list is referenced using the command, all IPv6 routes in the Level-2 area leak to the Level-1 area.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all IPv6 routes in the Level-2 area leak to the Level-1 area.

Example

Configure the router to perform route leaking from a Level-2 area to a Level-1 area using filtering policy 2002.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 import-route isis level-2 into level-1 filter-policy 2002
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.7.10 ipv6 import-route isis level-1 into level-2

9.7.6 ipv6 enable(IS-IS)

9.7.12 ipv6 maximum load-balancing

Function

The **ipv6 maximum load-balancing** command sets the maximum number of IS-IS IPv6 equal-cost routes for load balancing.

The **undo ipv6 maximum load-balancing** command restores the default number of equal-cost routes for load balancing.

By default, the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204 support a maximum of four equal-cost routes, and the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series support a maximum of eight equal-cost routes, AR2240 (using SRU200, SRU200E or SRU400), and AR3200 (using SRU200, SRU200E or SRU400) series support a maximum of sixteen equal-cost routes.

Format

ipv6 maximum load-balancing *number*

undo ipv6 maximum load-balancing [*number*]

Parameters

Parameter	Description	Value
number	Specifies the number of IPv6 equal-cost routes for load balancing.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.

Views

IS-IS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **ipv6 maximum load-balancing** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set the maximum number of IS-IS IPv6 equal-cost routes for load balancing to 2.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 100
[Huawei-isis-100] ipv6 enable
[Huawei-isis-100] ipv6 maximum load-balancing 2
```

Related Topics

9.7.6 ipv6 enable(IS-IS)

9.7.13 ipv6 preference

Function

The **ipv6 preference** command configures the preference of IPv6 routes generated by the IS-IS protocol.

The **undo ipv6 preference** command restores the default reference of IPv6 routes generated by the IS-IS protocol.

By default, the preference of IPv6 routes generated by the IS-IS protocol is 15.

Format

ipv6 preference { **route-policy** *route-policy-name* | *preference* } *

undo ipv6 preference

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preference	Specifies the preference of IPv6 routes generated by the IS-IS. A smaller value indicates a higher priority.	The value is an integer that ranges from 1 to 255.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

The routing policy can be used to set the preference for the filtered routes. If the preference is set, only the routes that pass the route-policy can apply the preference specified by this command; otherwise, routes apply the default value of the preference.

Multiple dynamic routing protocols can be run on a router at the same time. To properly select routes, the system sets a default preference for each routing protocol. If different protocols find routes to the same destination, the route of the protocol with a higher priority is preferred.

The **ipv6 preference** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Precautions

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, the configured priority applies to all IS-IS IPv6 routes.

Example

Set the IS-IS protocol preference to 20.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 preference 20
```

Related Topics

9.7.6 ipv6 enable(IS-IS)

9.7.14 ipv6 prefix-priority (IS-IS)

Function

The **ipv6 prefix-priority** command configures the convergence priority of IS-IS IPv6 routes.

The **undo ipv6 prefix-priority** command restores the default convergence priority of IS-IS IPv6 routes.

By default, the convergence priority of IS-IS IPv6 host routes and default routes is medium, and the convergence priority of other IS-IS IPv6 routes is low.

Format

ipv6 prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** } { **ipv6-prefix** *prefix-name* | **tag** *tag-value* }

undo ipv6 prefix-priority [**level-1** | **level-2**] { **critical** | **high** | **medium** }

Parameters

Parameter	Description	Value
level-1	Specifies the convergence priority of Level-1 IS-IS IPv6 routes.	-
level-2	Specifies the convergence priority of Level-2 IS-IS IPv6 routes.	-
critical	Sets the convergence priority of IS-IS IPv6 routes to critical.	-
high	Sets the convergence priority of IS-IS IPv6 routes to high.	-
medium	Sets the convergence priority of IS-IS IPv6 routes to medium.	-
ipv6-prefix *prefix-name*	Specifies the prefix name of IPv6 addresses for filtering routes to set the convergence priority for IS-IS IPv6 routes that match the specified IPv6 address prefix.	The value of *prefix-name* is a string of 1 to169 case-sensitive characters without spaces.
tag *tag-value*	Specifies the tag value used for filtering routes to set the convergence priority for IS-IS IPv6 routes that carry the specified tag value. To specify the tag value to filter the IPv6 routes that need to be set with the convergence priority, ensure that IS-IS IPv6 routes carry the tag value.	The value is an integer that ranges from 1 to 4294967295.

Views

IS-IS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command takes effect only in IPv6 base topologies but not in VPNs.

The convergence priorities of IS-IS IPv6 routes are classified as critical, high, medium, and low in descending order.

After the **ipv6 prefix-priority** command is run to set the convergence priority for IS-IS IPv6 routes, the following situations occur:

- The convergence priority of existing IS-IS IPv6 routes is re-set according to the configuration of the **ipv6 prefix-priority** command.
- The convergence priority of new IS-IS IPv6 routes is set according to the filtering result of the **ipv6 prefix-priority** command.
- If an IS-IS IPv6 route meets the matching rules specified in multiple commands that are used to configure convergence priorities, this IS-IS IPv6 route is of top convergence priority among the set convergence priorities.
- no level is specified, the convergence priority is set for both Level-1 routes and Level-2 routes according to the configuration of the **ipv6 prefix-priority** command.

NOTE

The **ipv6 prefix-priority** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

After the **ipv6 prefix-priority** command is run to set the convergence priority for IS-IS IPv6 routes (including IS-IS IPv6 host routes and default routes), the convergence priority of all the IS-IS IPv6 routes that meet the matching rules is changed according to the configuration of the **ipv6 prefix-priority** command, and the convergence priority of the IS-IS IPv6 routes that do not meet the matching rules is changed to low.

Example

In an IPv6 base topology, set the convergence priority of IS-IS Level-1 routes with tag value 3 to critical.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 prefix-priority level-1 critical tag 3
```

Related Topics

9.6.56 isis

9.9.47 ip ip-prefix

9.7.6 ipv6 enable(IS-IS)

 Copyright © Huawei Technologies Co., Ltd.

9.7.15 ipv6 spf-priority

Function

The **ipv6 spf-priority** command configures a priority for SPF calculation in an IPv6 base topology.

The **undo ipv6 spf-priority** command restores the default priority for SPF calculation in an IPv6 base topology.

By default, the priority of SPF calculation in an IPv6 base topology is 64.

Format

ipv6 spf-priority *priority-value*

undo ipv6 spf-priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority for SPF calculation in an IPv6 base topology. A larger value indicates a higher priority.	The value is an integer that ranges from 1 to 127.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

A higher priority of SPF calculation in an IPv6 base topology means that the routes in the IPv6 base topology are converged preferentially, which ensures the proper operation of important services.

The **ipv6 spf-priority** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set the priority of SPF calculation in an IPv6 base topology to 30.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 spf-priority 30
```

Related Topics

9.6.116 spf-priority

 Copyright © Huawei Technologies Co., Ltd.

9.7.6 ipv6 enable(IS-IS)

9.7.16 ipv6 summary

Function

The **ipv6 summary** command configures IS-IS to generate IPv6 summarized routes.

The **undo ipv6 summary** command disables IS-IS from generating IPv6 summarized routes.

By default, IS-IS does not generate IPv6 summarized routes.

Format

ipv6 summary *ipv6-address prefix-length* [**avoid-feedback** | **generate_null0_route** | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] *

undo ipv6 summary *ipv6-address prefix-length* [**level-1** | **level-1-2** | **level-2**]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the address range of IPv6 routes to be summarized.	-
prefix-length	Specifies the prefix length of an IPv6 route.	The value is an integer that ranges from 0 to 128.
avoid-feedback	Avoids learning summarized routes through SPF calculation.	-
generate_null0_route	Generates NULL0 routes to avoid routing loop.	-
tag *tag*	Specifies the administrative tag value.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates that only routes in Level-1 areas are summarized. If the level is not specified, **level-2** is used by default.	-
level-1-2	Indicates that routes in Level-1 and Level-2 areas are summarized. If the level is not specified, **level-2** is used by default.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
level-2	Indicates that only routes in Level-2 areas are summarized. If the level is not specified, **level-2** is used by default.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

The routes with the same prefix can be aggregated into one route. This can reduce the scale of the routing table, the size of the LSPs generated by the local router, and the scale of the LSDB. The aggregated routes can be the routes discovered by IS-IS or the imported IPv6 routes. After the aggregation, the smallest cost among those of the routes that are aggregated is used as the cost of the aggregated IPv6 route.

The **ipv6 summary** command can take effect only after IPv6 is enabled for the IS-IS process by the **ipv6 enable** command.

Example

Set a summarized route fc00::/32.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] ipv6 summary fc00:: 32
```

Related Topics

9.7.6 ipv6 enable(IS-IS)

9.7.17 isis ipv6 cost

Function

The **isis ipv6 cost** command sets the link cost value of an IS-IS interface in an IPv6 topology.

The **undo isis ipv6 cost** command restores the default link cost value of an IS-IS interface in an IPv6 topology.

By default, the link cost value of an IS-IS interface in an IPv6 topology is 10.

 Copyright © Huawei Technologies Co., Ltd.

Format

isis ipv6 cost { *cost* | **maximum** } [**level-1** | **level-2**]

undo isis ipv6 cost [*cost* | **maximum**] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
cost	Specifies the IPv6 link cost value of an interface.	The value is an integer that varies according to the cost style. ● When the cost style is **narrow**, **narrow-compatible** or **compatible**, the value ranges from 1 to 63. ● When the cost style is **wide** or **wide-compatible**, the value ranges from 1 to 16777214. The default value is 10. To set the cost style, use the **cost-style** command.
maximum	Sets the link cost value of an interface to 16777215. **NOTE** This parameter can be configured only when the IS-IS cost style is **wide** or **wide-compatible**. When the link cost value of an interface is set to 16777215, the neighbor TLV generated on the link cannot be used for route calculation and can only be used to transmit TE information.	-
level-1	Specifies the link cost value of a Level-1 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-
level-2	Specifies the link cost value of a Level-2 interface. If the interface level is not specified, link cost values of Level-1 and Level-2 interfaces are set.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale IPv6 networks, there may be multiple valid routes to the same destination. IS-IS uses the SPF algorithm to calculate an optimal route and transmits traffic over it, which brings the following problems:

- All traffic is transmitted over the optimal route, causing load imbalance.
- If the optimal route is faulty, traffic will get lost.

To solve the preceding problems, run the **isis ipv6 cost** command to set IPv6 link costs for interfaces so that traffic can be transmitted over different physical links.

Prerequisites

IS-IS has been enabled on a specified interface using the **isis ipv6 enable** [*process-id*] command in the interface view.

Configuration Impact

If the link cost of an interface is changed, routes will be re-calculated on the whole network, causing the changes in traffic forwarding paths.

The priority of the **ipv6 circuit-cost** command is lower than that of the **isis ipv6 cost** command.

If the IPv6 topology type is **compatible** or **standard**, the IPv6 and IPv4 link costs are the same on an interface even though the IPv6 link cost set using the **isis ipv6 cost** command is different from the IPv4 link cost. The IPv6 link cost set using the **isis ipv6 cost** command takes effect only when the IPv6 topology type is **compatible enable-mt-spf** or **ipv6**.

NOTE

The IPv6 topology type can be set for an IS-IS process using the **ipv6 enable (IS-IS)** command.

Example

Set the IPv6 link cost of GE1/0/0 to 50.

```
Huawei system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] isis ipv6 enable
[Huawei-GigabitEthernet1/0/0] isis ipv6 cost 50
```

Related Topics

9.6.11 cost-style

9.7.18 isis ipv6 enable

9.7.3 ipv6 circuit-cost
9.7.6 ipv6 enable(IS-IS)

9.7.18 isis ipv6 enable

Function

The **isis ipv6 enable** command enables the IS-IS IPv6 capability for an interface and specifies the ID of the IS-IS process to be associated with the interface.

The **undo isis ipv6 enable** command disables the IS-IS IPv6 capability of an interface and disassociates an IS-IS process from the interface.

By default, the IS-IS IPv6 capability is disabled on an interface.

Format

isis ipv6 enable [*process-id*]

undo isis ipv6 enable

Parameters

Parameter	Description	Value
process-id	Specifies an IS-IS process ID.	The value is an integer that ranges from 1 to 65535. The default value is 1.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After completing the configuration of an IS-IS process in the system view, enable IS-IS IPv6 on the interface that runs IS-IS and associate the interface with the IS-IS process using the **isis ipv6 enable** command.

Prerequisites

The following steps have been performed:

1. Enable IPv6 globally using the **ipv6** command in the system view.
2. Enable an IS-IS process using the **isis** command and configure a network entity title (NET) for the device running IS-IS using the **network-entity** command.
3. Enable IPv6 for the IS-IS process using the **ipv6 enable (IS-IS)** command in the IS-IS view.

 Copyright © Huawei Technologies Co., Ltd.

4. Enable IPv6 and configure an IPv6 address using the **ipv6 enable** command on each interface that runs the IS-IS process.

Precautions

An interface can be associated with only one IS-IS process.

NOTE

To perform IPv6-related IS-IS configurations, you must enable IPv6 first.

Example

Create IS-IS process 1, enable the IPv6 capability, and activate the IPv6 capability on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis 1
[Huawei-isis-1] network-entity 10.0001.1010.1020.1030.00
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address 2002::1/64
[Huawei-GigabitEthernet1/0/0] isis ipv6 enable 1
```

Related Topics

9.6.56 isis

9.6.101 network-entity

9.7.6 ipv6 enable(IS-IS)

8.8.28 ipv6 enable (interface view)

9.7.19 isis ipv6 suppress-reachability

Function

The **isis ipv6 suppress-reachability** command suppresses the advertisement of direct routes on an IPv6 interface in a specified topology.

The **undo isis ipv6 suppress-reachability** command restores the default configuration of an IPv6 interface.

By default, the advertisement of IPv6 addresses on an interface is not suppressed.

Format

isis ipv6 suppress-reachability [**level-1** | **level-1-2** | **level-2**]

undo isis ipv6 suppress-reachability

Parameters

Parameter	Description	Value
level-1	Suppresses the advertisement of IPv6 addresses is suppressed on Level-1 interfaces. If the level is not specified, Level-1-2 is used by default.	-
level-1-2	Indicates that the advertisement of IPv6 addresses is suppressed on Level-1 and Level-2 interfaces. If the level is not specified, Level-1-2 is used by default.	-
level-2	Indicates that the advertisement of IPv6 addresses is suppressed on Level-2 interfaces. If the level is not specified, Level-1-2 is used by default.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

You must enable the IPv6 capability for an IS-IS process before running this command. For details, see the **isis ipv6 enable** command.

Example

Suppress the advertisement of IPv6 addresses on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
[Huawei-isis-1] quit
[Huawei] interfacegigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] isis ipv6 enable
[Huawei-GigabitEthernet1/0/0] isis ipv6 suppress-reachability
```

9.7.20 isis ipv6 tag-value

Function

The **isis ipv6 tag-value** command configures the IPv6 administrative tag value on an IS-IS interface.

The **undo ipv6 isis tag-value** command deletes the IPv6 administrative tag value on an IS-IS interface.

By default, an IS-IS interface has no IPv6 administrative tag value.

 Copyright © Huawei Technologies Co., Ltd.

Format

isis ipv6 tag-value *tag* [**level-1** | **level-2**]

undo isis ipv6 tag-value [*tag*] [**level-1** | **level-2**]

Parameters

Parameter	Description	Value
tag	Specifies the administrative tag value.	The value is an integer that ranges from 1 to 4294967295.
level-1	Indicates the administrative tag value of a Level-1 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-
level-2	Indicates the administrative tag value of a Level-2 interface. If the interface level is not specified, the administrative tag value is set for Level-1 and Level-2 interfaces.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using the **isis ipv6 tag-value** command, you can set the administrative tag value for all routes of a specified IS-IS process. The tag can be used as a filtering condition of a route-policy to filter routes.

Precautions

You must enable the IPv6 capability for an IS-IS process before running this command.

If the IS-IS cost style is wide, wide-compatible, or compatible, the administrative tag for an interface is advertised using an LSP.

Example

Set the IPv6 administrative tag value of GE1/0/0 to 77.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] isis
[Huawei-isis-1] ipv6 enable
```

```
[Huawei-isis-1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] isis ipv6 enable
[Huawei-GigabitEthernet1/0/0] isis ipv6 tag-value 77
```

Related Topics

9.7.6 ipv6 enable(IS-IS)

8.8.28 ipv6 enable (interface view)

9.7.18 isis ipv6 enable

9.8 BGP Configuration Commands

NOTE

In practical application, in order to realize that business forwarding is not affected by motherboard failure, it is usually possible to configure BGP GR in the hardware environment of dual motherboard to make sense.

All the models support the GR Helper, and only AR3200 series support the GR Restarter.

9.8.1 active-route-advertise

Function

The **active-route-advertise** command enables BGP to advertise only the preferred routes in the IP routing table.

The **undo active-route-advertise** command restores the default setting.

By default, BGP advertises all preferred routes in the BGP routing table to neighbors.

Format

active-route-advertise

undo active-route-advertise

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, BGP advertises all preferred routes in the BGP routing table to neighbors. After the **active-route-advertise** is configured, only the routes preferred by BGP and also active at the routing management layer are advertised to neighbors.

Precautions

The **active-route-advertise** command and the **routing-table rib-only** command are mutually exclusive.

Example

Enable BGP to advertise only the preferred routes in the IP routing table to neighbors.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] active-route-advertise
```

9.8.2 aggregate (BGP)

Function

The **aggregate** command creates an aggregated route in the BGP routing table.

The **undo aggregate** command deletes an aggregated route in the BGP routing table.

By default, no aggregated route is created in the BGP routing table.

Format

aggregate *ipv4-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*]*

aggregate *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*]*

undo aggregate *ipv4-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*]*

undo aggregate *ipv6-address prefix-length* [**as-set** | **attribute-policy** *route-policy-name1* | **detail-suppressed** | **origin-policy** *route-policy-name2* | **suppress-policy** *route-policy-name3*]*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an aggregated route.	The address is in dotted decimal notation.
mask	Specifies the network mask of an aggregated route.	The mask is in dotted decimal notation.
mask-length	Specifies the network mask length of an aggregated route.	It is an integer ranging from 0 to 32.
ipv6-address	Specifies the IPv6 address of an aggregated route.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of the prefix of an aggregated IPv6 route.	It is an integer ranging from 0 to 128.
as-set	Generates a route with the AS-SET.	-
attribute-policy *route-policy-name1*	Specifies the name of an attribute policy for aggregated routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
detail-suppressed	Advertises only the aggregated route.	-
origin-policy *route-policy-name2*	Specifies the name of a policy that allows route aggregation.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
suppress-policy *route-policy-name3*	Specifies the name of a policy for suppressing the advertisement of specified routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP route aggregation is classified into manual aggregation and automatic aggregation. The **aggregate** command can be used to configure manual aggregation. This command can aggregate routes in the local BGP routing table. Manually-aggregated routes take precedence over automatically-aggregated routes.

If the specific member routes of an aggregated route have different Origin attributes, the Origin attribute of the aggregated route uses the value in the order of incomplete, egp, and igp. The aggregated route will carry the community attribute of every specific route.

The parameter **as-set** is used to create an aggregated route whose AS_Path attribute contains AS_Path information of specific routes. Exercise caution when using this parameter if many AS_Path attributes need to be aggregated because frequent changes in routes may cause route flapping.

The parameter **detail-suppressed** is used to suppress the advertisement of specific routes. After **detail-suppressed** is configured, only aggregated routes are advertised. Aggregated routes carry the atomic-aggregate attribute, not the community attributes of specific routes.

The parameter **suppress-policy** is used to suppress the advertisement of specified routes. The **if-match** clause of **route-policy** can be used to filter the routes to be suppressed. This means that only the routes matching the policy will be suppressed, and the other routes will still be advertised. The **peer route-policy** command can also be used to filter out the routes not to be advertised to peers.

After the parameter **origin-policy** is used, only the routes matching **route-policy** are aggregated.

The parameter **attribute-policy** is used to set attributes for a aggregated route. If the AS_Path attribute is set in the policy using the **apply as-path** command and **as-set** is set in the **aggregate** command, the AS_Path attribute in the policy does not take effect. The **peer route-policy** command can also be used to set attributes for an aggregated route.

Precautions

If the **undo aggregate** command is run, the system will match routes base on the configured parameter **attribute-policy**, **origin-policy**, **suppress-policy**, **as-set**, or **detail-suppressed**. If the parameter is not configured, the system will fail to execute the **undo aggregate** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an aggregated route. The path that is used to advertise this route is an AS-SET consisting of all aggregated paths.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] aggregate 172.16.0.0 255.255.0.0 as-set
```

Related Topics

9.8.135 peer route-policy

9.8.173 summary automatic

9.8.3 apply-label explicit-null

Function

The **apply-label explicit-null** command enables IPv6 Provider Edge (6PE) routes to share the explicit null label.

The **undo apply-label explicit-null** command disables 6PE routes from sharing the explicit null label.

By default, the function is disabled.

Format

apply-label explicit-null

undo apply-label explicit-null

Parameters

None

Views

BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To save label resources on a 6PE device and avoid the problem that IPv6 routes cannot be advertised due to the shortage of labels, you can run the **apply-label explicit-null** command on the 6PE device.

Configuration Impact

After the **apply-label explicit-null** command is run on a 6PE device, all the routes sent by the 6PE device to its peer share the explicit null label.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If you run the **apply-label explicit-null** or **undo apply-label explicit-null** command after a 6PE peer relationship is established, temporary packet loss occurs.

Example

Enable 6PE routes to share the explicit null label in the BGP-IPv6 unicast address family view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv6-family unicast
[Huawei-bgp-af-ipv6] apply-label explicit-null
```

9.8.4 as-notation plain

Function

The **as-notation plain** command configures a BGP 4-byte AS number to be displayed as an integer.

The **undo as-notation plain** command configures a BGP 4-byte AS number to be displayed in dotted notation.

By default, a BGP 4-byte AS number is displayed in dotted notation (that is, in the format of x.y).

Format

as-notation plain

undo as-notation plain

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, display commands such as the **display bgp peer** command display 4-byte AS numbers in dotted notation.

To display a 4-byte AS number as an integer, run the **as-notation plain** command. After the **as-notation plain** command is run, display commands display all 4-byte AS numbers as integers. These 4-byte AS numbers include:

- Independent 4-byte AS number
- 4-byte AS number in an extended community attribute
- 4-byte AS number in a route distinguisher (RD)
- 4-byte AS number in a VPN target (also called a route target)
- 4-byte AS number in the Site-of-Origin attribute

Assume that a 4-byte AS number in dotted notation is *x.y*. Following is the conversion relationship between an integral 4-byte AS number and a 4-byte AS number in dotted notation:

Integral 4-byte AS number = *x* x 65536 + *y*

For example, if a 4-byte AS number in dotted notation is 2.3, the corresponding integral 4-byte AS number is 131075 (2 x 65536 + 3).

Precautions

After the **as-notation plain** command is run, the formats of 4-byte AS numbers in configuration information generated by the system do not change.

- If integral 4-byte AS numbers are configured, 4-byte AS numbers in configuration information generated by the system are also displayed as integers.
- If 4-byte AS numbers in dotted notation are configured, 4-byte AS numbers in configuration information generated by the system are also displayed in dotted notation.

Changing the format of 4-byte AS numbers will affect matching results of AS_Path regular expressions and extended community attribute filters. Therefore, if the system is using an AS_Path regular expression or an extended community attribute filter as an import or export policy, you must reconfigure an AS_Path regular expression using the **ip as-path-filter** command or an extended community attribute filter using the **ip extcommunity-filter** command after changing the format of 4-byte AS numbers. This reconfiguration ensures that routes match the import or export policy.

- If integral 4-byte AS numbers are configured, you must change 4-byte AS numbers in AS_Path regular expressions and extended community attribute filters to integral 4-byte AS numbers.
- If 4-byte AS numbers in dotted notation are configured, you must change 4-byte AS numbers in AS_Path regular expressions and extended community attribute filters to 4-byte AS numbers in dotted notation.

Example

Configure a BGP 4-byte AS number to be displayed as an integer.

```
<Huawei> system-view
[Huawei] as-notation plain
Warning: If the configuration takes effect, the regular expression of the filter for 4-byte AS path should be
changed to the asplain format, otherwise match will fail. Continue? [Y/N]y
```

Configure a BGP 4-byte AS number to be displayed in dotted notation.

```
<Huawei> system-view
[Huawei] undo as-notation plain
Warning: If the configuration takes effect, the regular expression of the filter for 4-byte AS path should be
changed to the asdot format, otherwise match will fail. Continue? [Y/N]y
```

9.8.5 as-path-limit

Function

The **as-path-limit** command sets the maximum number of AS numbers in the AS_Path attribute.

The **undo as-path-limit** command restores the default setting.

By default, no limit is configured on the maximum number of AS numbers in the AS_Path attribute, but the maximum number of AS numbers carried in the AS_Path attribute is limited by the BGP message length.

Format

as-path-limit [*as-path-limit-num*]

undo as-path-limit

Parameters

Parameter	Description	Value
as-path-limit-num	Specifies the maximum number of AS numbers in the AS-Path attribute.	The value is an integer ranging from 1 to 2000. **NOTE** • The maximum value of *as-path-limit-num* for the 2-byte and 4-byte AS number is the same. • If *as-path-limit-num* is not specified, the maximum number of AS numbers in the AS_Path attribute is 255.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to restrict the maximum number of AS numbers in the AS_Path attribute only when the AS_Path attribute is reconstructed or the aggregated routes are generated.

Precautions

After the **as-path-limit** command is configured, a router checks whether the number of AS numbers in the AS-Path attribute of the incoming route exceeds the maximum value. If the number of AS numbers exceeds the maximum value, the

local router will discard the route. Therefore, if the maximum number of AS numbers in the AS-Path attribute is set too small, routes will be lost.

Example

Set the maximum number of AS numbers in the AS-Path attribute to 200.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] as-path-limit 200
```

9.8.6 bestroute as-path-ignore

Function

The **bestroute as-path-ignore** command configures BGP to ignore the AS_Path attribute when it selects the optimal route.

The **undo bestroute as-path-ignore** command restores the default configuration.

By default, BGP uses the AS_Path attribute as one of route selection rules.

Format

bestroute as-path-ignore

undo bestroute as-path-ignore

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **bestroute as-path-ignore** command is used, BGP does not compare the AS path lengths of routes. By default, the route with the shortest AS path is preferred.

Precautions

After the **bestroute as-path-ignore** command is run, the AS_Path attribute is not used as one of the BGP route selection rules.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure BGP to ignore the AS_Path attribute when selecting the optimal route.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] bestroute as-path-ignore
```

9.8.7 bestroute igp-metric-ignore

Function

The **bestroute igp-metric-ignore** command configures BGP to ignore the metric value of the next-hop IGP route when selecting the optimal route.

The **undo bestroute igp-metric-ignore** command restores the default setting.

By default, BGP selects a route with the smallest metric value of the next-hop IGP route as the optimal route.

Format

bestroute igp-metric-ignore

undo bestroute igp-metric-ignore

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv6 address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a BGP network, the BGP device always receives multiple routes with the same prefix but to different paths from neighbors. BGP must select the optimal route to the prefix to guide packet forwarding. By default, BGP compares the next-hop IGP route metric values of these routes and selects the route with the smallest metric value as the optimal route.

 Copyright © Huawei Technologies Co., Ltd.

To customize route selection policies, you can run the **bestroute igp-metric-ignore** command to configure BGP to ignore the metric value of the next-hop IGP route when selecting the optimal route.

Example

Configure BGP to ignore the IGP metric when selecting the optimal route.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] bestroute igp-metric-ignore
```

9.8.8 bestroute med-confederation (BGP)

Function

The **bestroute med-confederation** command enables BGP to compare the Multi Exit Discriminator (MED) values of routes in a confederation when BGP selects the optimal route.

The **undo bestroute med-confederation** command restores the default settings.

By default, BGP compares the MED values of the routes that are from the same AS only.

Format

bestroute med-confederation

undo bestroute med-confederation

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

By default, BGP compares only MED values of routes from the same AS, not including sub-ASs in a confederation. To enable BGP to compare MED values of routes in a confederation when selecting the optimal route, run the **bestroute med-confederation** command.

After the **bestroute med-confederation** command is configured, BGP compares MED values only when AS_Path does not contain the external AS (AS that is not in the confederation) number. Otherwise, BGP does not compare MED values.

 Copyright © Huawei Technologies Co., Ltd.

For example, ASs 65000, 65001, 65002, and 65004 belong the same confederation. Routes to the same destination are listed as follows:

- path1: AS_Path=65000 65004, med=2
- path2: AS_Path=65001 65004, med=3
- path3: AS_Path=65002 65004, med=4
- path4: AS_Path=65003 65004, med=1

After the **bestroute med-confederation** command is run, the AS_Path attributes of paths 1, 2, and 3 does not contain the numbers of ASs that belong to other confederations. Therefore, when selecting routes based on MED values, BGP compares the MED values of paths 1, 2, and 3 only. This is because the AS_Path attribute of path 4 contains the number of an AS that does not belong to this confederation.

Example

Configure BGP to compare the MED values of routes only in the confederation when selecting the optimal route.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] bestroute med-confederation
```

9.8.9 bestroute med-none-as-maximum

Function

The **bestroute med-none-as-maximum** command configures BGP to assign the maximum Multi Exit Discriminator (MED), 4294967295, to a route without an MED in route selection.

The **undo bestroute med-none-as-maximum** command restores the default configuration.

By default, BGP assigns 0 to a route without an MED in route selection.

Format

bestroute med-none-as-maximum

undo bestroute med-none-as-maximum

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **bestroute med-none-as-maximum** command takes effect in BGP route selection and is used only when no MED is in the route attributes. When the MED is lost, the MED uses the maximum value 4294967295 if the **bestroute med-none-as-maximum** command is used. Otherwise, the MED uses the default value 0, which may cause a failure to select the optimal route.

Example

Configure BGP to assign the maximum MED of 4294967295 to a route without an MED in route selection.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] bestroute med-none-as-maximum
```

9.8.10 bestroute nexthop-resolved

Function

The **bestroute nexthop-resolved** command configures the condition of the route selection for next hop iteration.

The **undo bestroute nexthop-resolved** command restores the default configuration.

By default, labeled BGP IPv4 routes participate in route selection only when their next hops are iterated to IP addresses.

NOTE

AR100&AR120&AR150&AR160&AR200 series does not support this command.

Format

bestroute nexthop-resolved { **ip** | **tunnel** }

undo bestroute nexthop-resolved

Parameters

Parameter	Description	Value
ip	Allows labeled routes that are iterated to IP addresses to participate in route selection.	-
tunnel	Allows labeled routes that are iterated to MPLS tunnels to participate in route selection.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, labeled BGP IPv4 unicast routes that are iterated to IP address participate in route selection. In non-RR networking, or RR networking where the BGP next hop is changed, BGP needs to check whether there is an LSP destined for the next hop. If such an LSP is not found, BGP needs to establish an LSP. If the default setting is adopted, a labeled BGP IPv4 unicast route may be selected prior to LSP establishment. As a result, services are incorrectly switched before LSP establishment, packet loss may occur, which affects service stability. The **bestroute nexthop-resolved tunnel** command can be run to allow route selection only after the labeled BGP IPv4 route is iterated to an LSP.

By default, the BGP VPNv4 routes can participate in route selection if the next hop iterates to an IP address. If the current device is an ASBR, it is required that the next hop of the preferred route can iterate to the LSP tunnel; if the ASBR is configured with load balancing, it is also required that next hop of the routes which are not preferred can iterate to the LSP tunnel so that these routes can participate in load balancing. Now the BGP VPNv4 routes can be set to participate in route selection when next hop iterates to the LSP tunnel.

Precautions

The **bestroute nexthop-resolved ip** and **bestroute nexthop-resolved tunnel** commands are mutually exclusive.

Example

In the BGP IPv4 unicast view, configure labeled BGP IPv4 unicast routes that are iterated to LSP tunnels to participate in route selection.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] bestroute nexthop-resolved tunnel
```

In the BGP VPNv4 view, configure BGP VPNv4 routes that are iterated to LSP tunnels to participate in route selection.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] bestroute nexthop-resolved tunnel
```

 Copyright © Huawei Technologies Co., Ltd.

9.8.11 bestroute routerid-prior-clusterlist

Function

The **bestroute routerid-prior-clusterlist** command enables Router ID to take precedence over Cluster_List during BGP route selection.

The **undo bestroute routerid-prior-clusterlist** command restores the default configurations.

By default, Cluster_List takes precedence over Router ID during BGP route selection.

Format

bestroute routerid-prior-clusterlist

undo bestroute routerid-prior-clusterlist

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view, BGP-IPv4 multicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

On a BGP network, after a router receives multiple routes with the same prefix but different paths from different peers, the router needs to select an optimal route from these routes to forward packets. By default, Cluster_List takes precedence over Router ID during BGP route selection. To enable Router ID to take precedence over Cluster_List during BGP route selection, run the **bestroute routerid-prior-clusterlist** command.

Example

Enable Router ID to take precedence over Cluster-List during BGP route selection.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] bestroute routerid-prior-clusterlist
```

 Copyright © Huawei Technologies Co., Ltd.

9.8.12 bgp

Function

The **bgp** command enables BGP and displays the BGP view.

The **undo bgp** command disables BGP.

By default, BGP is disabled.

Format

bgp { *as-number-plain* | *as-number-dot* }

undo bgp [*as-number-plain* | *as-number-dot*]

Parameters

Parameter	Description	Value
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP is an inter-AS dynamic routing protocol. BGP running within an AS is called Internal BGP (IBGP), and BGP running between ASs is called External BGP (EBGP).

Whether to apply BGP to routing information transmission between ASs depends on the following conditions:

- If at least one of the following conditions is met, BGP can be used:
  - Data packets are allowed to be transmitted from one AS to another AS.
  - Multiple connections to external ISPs and Internet exist in ASs.
  - Data flows entering or leaving ASs must be controlled.
- If one of the following conditions is met, BGP does not need to be used:
  - Users are connected to only one ISP network.

 Copyright © Huawei Technologies Co., Ltd.

- The ISP does not need to provide Internet access services for users.
- ASs adopt default routes between each other.

Precautions

After the **bgp** command is run, BGP is enabled.

Each device runs in only one AS; therefore, each device can be specified with only one local AS number.

NOTICE

Exercise caution when using the **undo bgp** command because it will delete all BGP configurations on a device.

Example

Enable BGP and enter the BGP view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp]
```

9.8.13 bgp dynamic-session-limit

Function

The **bgp dynamic-session-limit** command configures a maximum number for dynamic BGP peer sessions.

The **undo bgp dynamic-session-limit** command restores the default configuration.

By default, a maximum of the total specification dynamic BGP peer sessions can be established.

Format

bgp dynamic-session-limit *limit-value*

undo bgp dynamic-session-limit [*limit-value*]

Parameters

Parameter	Description	Value
limit-value	Specifies the maximum number of dynamic BGP peer sessions allowed.	The value is an integer ranging from 1 to the maximum value defined in the PAF file.

Views

BGP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the dynamic BGP peer function is enabled using the **peer listen-net** command, BGP listens to BGP connection requests from the network segment specified in the command and establish BGP peer relationships dynamically. If a large number of dynamic BGP peer sessions are established on the network segment, excessive system resources will be consumed. To prevent this problem, run the **bgp dynamic-session-limit** command to configure a maximum number for dynamic BGP peer sessions as required.

Precautions

This command does not apply to static BGP peer sessions.

Example

Set the maximum number of dynamic BGP peer sessions to 128.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] bgp dynamic-session-limit 128
```

9.8.14 check-first-as

Function

The **check-first-as** command enables the function to check the first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer.

The **undo check-first-as** command disables the function.

By default, the function is enabled.

Format

check-first-as

undo check-first-as

Parameters

None

Views

BGP view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

By default, BGP checks the first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer. If only the first AS number indicates the AS where the EBGP peer locates, the Update message is accepted. Otherwise, the Update message is denied, and the EBGP connection goes Down.

Precautions

The **check-first-as** command is not listed in the configuration file.

After the **undo check-first-as** command is configured, loops have a greater chance to occur. Therefore, use the command with caution.

Follow-up Procedure

After the configuration is complete, run the **refresh bgp** command if you want to check the received routes again.

Example

Check the first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] check-first-as
```

Related Topics

9.8.149 refresh bgp

9.8.15 compare-different-as-med

Function

The **compare-different-as-med** command enables BGP to compare the MEDs in the routes of peers in different ASs.

The **undo compare-different-as-med** command restores the default configuration.

By default, BGP does not compare the MEDs in the routes of peers in different ASs.

Format

compare-different-as-med

undo compare-different-as-med

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command is used to control the MEDs to change the policy of BGP route selection. If the **compare-different-as-med** command is run, BGP will compare the MEDs of the routes from different ASs. If there are multiple reachable paths to the same destination, BGP prefers the route with the smallest MED.

Precautions

Do not use this command unless different ASs use the same IGP and route selection mode.

Example

Enable BGP to compare the MEDs in the routes of peers in different ASs.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] compare-different-as-med
```

9.8.16 confederation id

Function

The **confederation id** command configures a BGP confederation and specifies a confederation ID for the BGP confederation.

The **undo confederation id** command removes the BGP specified confederation.

By default, no BGP confederation is configured.

Format

confederation id { *as-number-plain* | *as-number-dot* }

undo confederation id

Parameters

Parameter	Description	Value
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.

Parameter	Description	Value
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large AS may contain a huge number of fully meshed IBGP peer relationships. In this situation, configure a confederation.

Divide the AS into multiple small sub-ASs and group them into a confederation. Then establish EBGP connections between sub-ASs and establish fully meshed IBGP connections within the same sub-AS. Some key attributes of routes, such as the next hop, MED, and local preference are not discarded when these routes pass through sub-ASs. This can reduce the number of fully meshed IBGP peer relationships in an AS and keep the integrity of the original AS.

Precautions

The confederation ID is equal to the AS number. An external AS must specify the confederation ID when specifying the AS number of the peer. All the sub-ASs in the same confederation must be configured with the same confederation ID that must be different from the number of any sub-AS.

Example

Configure a confederation ID. An AS is divided into sub-AS 65001, 65002, 65003, and 65004, and their confederation ID is 9. Peer 10.2.3.4 is a member of the AS confederation. Peer 10.4.5.6 is a member outside the AS confederation. For the external members, confederation 9 is a complete AS.

```
<Huawei> system-view
[Huawei] bgp 65001
[Huawei-bgp] confederation id 9
[Huawei-bgp] confederation peer-as 65002 65003 65004
[Huawei-bgp] peer 10.2.3.4 as-number 65002
[Huawei-bgp] peer 10.4.5.6 as-number 65005
```

Related Topics

9.8.18 confederation peer-as

9.8.17 confederation nonstandard

Function

The **confederation nonstandard** command configures standard devices in a confederation to communicate with nonstandard devices.

The **undo confederation nonstandard** command configures standard devices in a confederation to communicate only with standard devices.

By default, only standard devices in a confederation can communicate.

Format

confederation nonstandard

undo confederation nonstandard

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make nonstandard devices interwork, configure this command on all routers in a confederation.

Precautions

After the confederation ID is configured, running the **confederation nonstandard** command will disconnect the sessions between a router and its IBGP peers as well as its confederation EBGP peers. Then, new connections are re-established.

Example

Enable the router to communicate with nonstandard routers. The AS 100 contains two sub-ASs, 64000 and 65000.

```
<Huawei> system-view
[Huawei] bgp 64000
[Huawei-bgp] confederation id 100
[Huawei-bgp] confederation peer-as 65000
[Huawei-bgp] confederation nonstandard
```

Related Topics

9.8.16 confederation id

 Copyright © Huawei Technologies Co., Ltd.

9.8.18 confederation peer-as

9.8.18 confederation peer-as

Function

The **confederation peer-as** command configures the number of each sub-AS of the same confederation.

The **undo confederation peer-as** command removes the specified sub-AS from the confederation.

By default, no sub-AS number of the confederation is configured.

Format

confederation peer-as { *as-number-plain* | *as-number-dot* } &<1-32>

undo confederation peer-as { *as-number-plain* | *as-number-dot* } &<1-32>

Parameters

Parameter	Description	Value
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large AS may contain a huge number of fully meshed IBGP peer relationships. In this situation, configure a confederation.

Prerequisites

The **confederation id** command specifies the confederation ID of each sub-AS. If the confederation ID is not configured, this configuration is invalid.

Precautions

The sub-ASs configured in this command belong to the same confederation, and each sub-AS uses fully meshed network.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a sub-AS for the confederation.

```
<Huawei> system-view
[Huawei] bgp 1090
[Huawei-bgp] confederation id 100
[Huawei-bgp] confederation peer-as 1091 1092 1093
```

Related Topics

9.8.16 confederation id

9.8.19 confederation route unicast-to-label disable

Function

The **confederation route unicast-to-label disable** command prevents non-RRs from advertising the IPv6 non-labeled routes learned from peers in the local confederation as labeled routes carrying a label of all Fs to the BGP peers in another confederation.

The **undo confederation route unicast-to-label disable** command restores the default configuration.

By default, non-RRs can advertise the IPv6 non-labeled routes learned from peers in the local confederation as labeled routes carrying a label of all Fs to the BGP peers in another confederation.

Format

confederation route unicast-to-label disable

undo confederation route unicast-to-label disable

Parameters

None

Views

BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

If two PEs that are not RRs reside in two confederations, the PEs can advertise labeled routes carrying a label of all Fs to each other by default. However, non-Huawei devices may consider the label of all Fs invalid, and if these non-Huawei devices receive such labeled routes, BGP peer relationships may be disconnected. To prevent this problem, run the **confederation route unicast-to-label disable** command to prevent the PEs from advertising labeled routes carrying a label of all Fs.

 Copyright © Huawei Technologies Co., Ltd.

Example

Prevent non-RRs from advertising the IPv6 non-labeled routes learned from peers in the local confederation as labeled routes carrying a label of all Fs to the BGP peers in another confederation.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] confederation id 100
[Huawei-bgp] confederation peer-as 38 39
[Huawei-bgp] peer 191.1.1.1 as-number 38
[Huawei-bgp] peer 191::1 as-number 39
[Huawei-bgp] ipv6-family unicast
[Huawei-bgp-af-ipv6] peer 191.1.1.1 enable
[Huawei-bgp-af-ipv6] peer 191.1.1.1 label-route-capability
[Huawei-bgp-af-ipv6] peer 191::1 enable
[Huawei-bgp-af-ipv6] confederation route unicast-to-label disable
```

Related Topics

9.8.122 peer label-route-capability (BGP)

9.8.20 dampening

Function

The **dampening** command enables BGP route flap suppression and modifies BGP route flap suppression parameters.

The **undo dampening** command restores the default configuration.

By default, BGP route flap suppression is disabled.

Format

dampening [**ibgp**] [*half-life-reach reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening [**ibgp**]

Parameters

Parameter	Description	Value
half-life-reach	Specifies the half life of a reachable route.	The value is an integer ranging from 1 to 45, in minutes. The default value is 15.
reuse	Specifies the threshold for the route to be unsuppressed. If the penalty of the route falls below the threshold, the route is reused.	The value is an integer ranging from 1 to 20000. The default value is 750.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
suppress	Specifies the threshold for the route to be suppressed. If the penalty value of the route exceeds the threshold, the route is not used.	The value is an integer ranging from 1 to 20000, which must be greater than the value of *reuse*. The default value is 2000.
ceiling	Specifies the penalty ceiling.	The value is an integer ranging from 1001 to 20000. The configured value must be greater than that of *suppress*. The default value is 16000.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ibgp	Specify the route type as IBGP route. When this parameter is not specified, the route type is EBGP. **NOTE** The **ibgp** parameter takes effect only in the BGP-VPNv4 address pool view.	-

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP route flap dampening measures the stability of a route by using a penalty value. The greater the penalty value, the less stable the route. Each time route flapping occurs, that is, when the router receives a Withdraw packet or an Update packet for a route, BGP adds a certain penalty value (1000) for the route.

When the penalty value of the route exceeds the suppression threshold, the route is suppressed. The router does not add the route to the IP routing table or advertise any Update packet to other BGP peers. If the route is marked with the d flag, the last packet received by the router is an Update packet; if the route is marked with the h flag, the last packet received by the router is a Withdraw

packet. After the penalty value reaches a certain limit, it does not increase any more. The limit is called the penalty ceiling.

After the route is suppressed for a certain period, the penalty value is reduced by half. If the penalty value of a route marked with the d flag decreases to the reuse threshold, the d flag is removed, and the route becomes available and is selected preferentially. After that, the route can be added to the IP routing table and used to send Update packets to other BGP peers. If the penalty value of a route marked with the h flag decreases to 0, the route is deleted from the BGP routing table.

You can run the **display bgp routing-table label** command to check the d flag and h flag indicating the routes that have been dampened and were dampened respectively.

Precautions

If the **dampening** command is run multiple times, the latest configuration overrides the previous one.

After the **dampening** command is run, the system suppresses unstable routes. This means that the system does not add unstable routes to the BGP routing table or advertise them to other BGP peers.

Note the following items when configuring BGP route flap dampening:

- The value of *suppress* must be greater than that of *reuse* and smaller than that of *ceiling*.
- If MaxSuppressTime obtained by using the formula of MaxSuppressTime = *half-life-reach* x 60 x (ln(*ceiling*/*reuse*)/ln(2)) is smaller than 1, suppression cannot be performed. You need to ensure that the value of MaxSuppressTime is equal to or greater than 1. This means that the value of *ceiling*/*reuse* must be great enough.

NOTE

The **dampening** command is valid only for EBGP routes.

The **dampening ibgp** command is valid only for BGP VPNv4 routes.

Example

Enable EBGP route dampening and modify EBGP route damping parameters.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] dampening 10 1000 2000 5000
```

Enable IBGP route flap dampening and modify various IBGP route flap damping parameters.

```
<Huawei> system-view
<Huawei> bgp 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] dampening ibgp 10 1000 2000 5000
```

 Copyright © Huawei Technologies Co., Ltd.

9.8.21 default ipv4-unicast

Function

The **default ipv4-unicast** command enables the IPv4 unicast address family for BGP peers by default.

The **undo default ipv4-unicast** command disables the IPv4 unicast address family for BGP peers by default.

By default, the IPv4 unicast address family is enabled for BGP peers.

Format

default ipv4-unicast

undo default ipv4-unicast

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the IPv4 unicast address family needs to be enabled by default for created BGP peers, the **default ipv4-unicast** command can be used to configure the default address family of BGP to the IPv4 unicast address family.

If the IPv4 unicast address family does not need to be enabled by default for created BGP peers, the **undo default ipv4-unicast** command can be used to disable the IPv4 unicast address family for all peers.

Precautions

After the **undo default ipv4-unicast** command is run, the **peer enable** command needs to be run if the created BGP peer needs to be enabled with the IPv4 unicast address family.

Example

Enable the IPv4 unicast address family for all peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] default ipv4-unicast
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.8.114 peer enable (BGP)

9.8.87 ipv4-family

9.8.22 default local-preference

Function

The **default local-preference** command sets the default local preference for BGP routes.

The **undo default local-preference** command restores the default configuration.

By default, the local preference for BGP routes is 100.

Format

default local-preference *local-preference*

undo default local-preference

Parameters

Parameter	Description	Value
local-preference	Specifies the local preference for BGP routes. The greater the value, the higher the preference.	The value is an integer ranging from 0 to 4294967295.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Local_Pref attribute is used to determine an optimal route for traffic before traffic leaves an AS. When the router that runs BGP has multiple routes to the same destination, the router selects the route with the highest local preference as the optimal route.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If the router is already configured with a default local preference for BGP routes, the configuration of a new default local preference will override the previous configuration and the new default local preference will overwrite the previous one.

The local preference is exchanged only between IBGP peers and is not advertised to other ASs.

Example

Set the default local preference for BGP routes to 200.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] default local-preference 200
```

9.8.23 default med

Function

The **default med** command sets the default multi-exit-discriminator (MED) for BGP routes.

The **undo default med** command restores the default configuration.

By default, the MED is 0.

Format

default med *med*

undo default med

Parameters

Parameter	Description	Value
med	Specifies the Multi-Exit-Discriminator (MED) for BGP routes.	The value is an integer ranging from 0 to 4294967295.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **default med** command is valid only for the routes imported by using the **import-route (BGP)** command and the routes summarized by BGP on the local device.

The **default med** command sets the default MED and controls route selection for the traffic entering an AS. If the other attributes of routes to the same destination are the same, BGP will select the route with the smallest MED as the optimal route.

Precautions

If a default MED is configured on a device, configuring a new default MED will override the previous configuration and the new default MED will overwrite the previous one.

The MED is transmitted between two neighboring ASs only. Devices in an AS do not advertise the received MED to peers in other ASs.

Example

Set the default MED of a BGP route to 10.

```
<Huawei> system-view
[Huawei] bgp 1
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] default med 10
```

9.8.24 default-route imported

Function

The **default-route imported** command enables import the default routes in the local IP routing table to the BGP routing table.

The **undo default-route imported** command disables the import of the default routes in the local IP routing table to the BGP routing table.

By default, BGP does not add the default route to the BGP routing table.

Format

default-route imported

undo default-route imported

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This configuration reduces the number of routes on the network and minimizes the routing table size. If the **default-route imported** command is run and a default route exists in the local IP routing table, the system imports the default route to the BGP routing table. After default routes are imported, the packets can be transmitted over the default route when no matched routing entry is found in the routing table, preventing packet loss.

Precautions

To import default routes, you need to run both the **default-route imported** command and the **import-route (BGP)** command. If only the **import-route (BGP)** command is used, default routes cannot be imported. In addition, the **default-route imported** command is used to import only the default routes that exist in the local routing table.

When a device needs to advertise default routes to a peer (group) and no default route exists in the local routing table, the **peer default-route-advertise** command needs to be used.

Example

Import default routes to the BGP routing table.

```
<Huawei> system-view
[Huawei] bgp 1
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] default-route imported
[Huawei-bgp-af-ipv4] import-route ospf 1
```

Related Topics

9.8.86 import-route (BGP)
9.8.110 peer default-route-advertise

9.8.25 deterministic-med (BGP)

Function

The **deterministic-med** command enables the BGP deterministic-MED function so that routes with the same leftmost AS number are first compared during route selection.

The **undo deterministic-med** command disables the BGP deterministic-MED function so that routes are compared against each other according to the sequence in which they are received.

By default, the BGP deterministic-MED function is disabled.

Format

deterministic-med

undo deterministic-med

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

After the BGP deterministic-MED function is enabled, when an optimal route is to be selected from routes that are received from different ASs and carry the same prefix, routes are first grouped based on the leftmost AS number in the AS_Path attribute. Routes with the same leftmost AS number are grouped together, and after comparison, an optimal route is selected for the group. The group optimal route is then compared with optimal routes from other groups to determine the final optimal route. This mode of route selection ensures that the sequence in which routes are received is irrelevant to the route selection result.

If the BGP deterministic-MED function is disabled, routes are compared against each other according to the sequence in which they are received. In this manner, the sequence in which routes are received is relevant to the result of route selection.

For example: Assume that the following BGP routes are available on the router.

- Route A1: AS(PATH) 12, med 100, igp metric 13, internal, rid 4.4.4.4
- Route A2: AS(PATH) 12, med 150, igp metric 11, internal, rid 5.5.5.5
- Route B: AS(PATH) 3, med 0, igp metric 12, internal, rid 6.6.6.6

If Route A1, Route A2, and Route B are received in turn, Route A1 and Route A2 are first compared. The leftmost AS number of Route A1 is the same as the leftmost AS number of Route A2, and therefore Route A1 is selected because its MED is smaller. After that, Route A1 and Route B are compared. Because the leftmost AS numbers of the two routes are different, the optimal route cannot be selected by comparing the MEDs of the two routes unless the **compare-different-**

as-med command is configured. As a result, Route B is selected because its IGP metric is smaller.

If Route A2, Route B, and Route A1 are received in turn, Route A2 and Route B are first compared. Because leftmost AS number of Route A2 is different from the leftmost AS number of Route B, the optimal route cannot be selected by comparing the MEDs of the two routes unless the **compare-different-as-med** command is configured. As a result, Route A2 is selected because its IGP metric is smaller. After that, Route A2 and Route A1 are compared. The leftmost AS number of Route A1 is the same as the leftmost AS number of Route A2, and therefore Route A1 is selected because its MED is smaller.

Judging from the preceding route selection procedure, when the BGP deterministic-MED function is disabled, the sequence in which routes are received is relevant to the result of route selection. After the BGP deterministic-MED function is enabled, the sequence in which routes are received is no longer relevant to the result of route selection. Route A1 and Route A2 have the same leftmost AS number, Route A1 and Route A2 are compared first regardless of the sequence in which routes are received.

Example

Enable the deterministic-MED function in the BGP view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] deterministic-med
```

Related Topics

9.8.15 compare-different-as-med

9.8.26 display bgp bfd session

Function

The **display bgp bfd session** command displays information about BFD sessions between BGP peers.

Format

display bgp bfd session { [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** *ipv4-address* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpnv4 vpn-instance *vpn-instance-name*	Displays information about the BFD session between BGP peers with the specified IPv4 VPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer *ipv4-address*	Displays information about the BFD session of the BGP peer with the specified IPv4 address.	The value is in dotted decimal notation.
all	Displays all BFD sessions between BGP peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The BFD session set up by BGP helps BGP quickly discover faults between BGP peers and inform BGP to recalculate routes for packet forwarding.

Run the **display bgp bfd session** command to display information about the BFD session set up by BGP in the following situations:

- Check whether the BFD session is successfully set up or view detailed information about the BFD session that is successfully configured.
- Check whether the BFD session set up by BGP is successfully deleted after running the **undo peer bfd enable** command.
- Verify the configuration after running the **undo peer bfd block** command to prevent a peer from inheriting the BFD function of the peer group.
- Verify the configuration after running the **peer bfd** command to set BFD parameters.

The information about the BFD session of a specified BGP peer can be displayed by specifying different parameters.

- Run the **display bgp bfd session vpnv4 vpn-instance** *vpn-instance-name* **peer** *ipv4-address* command to display information about the BFD session of a specified BGP peer in a specified VRF.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **display bgp bfd session peer** *ipv4-address* command to display information about the BFD session of a specified BGP peer on the public network.
- Run the **display bgp bfd session all** command to display information about the BFD sessions of all BGP peers.

Prerequisites

The BFD session has been set up using the **peer bfd enable** command. If the BFD session has not been set up by BGP, no information is displayed after running the **display bgp bfd session** command.

Example

Display all BFD sessions between BGP peers.

```
<Huawei> display bgp bfd session all
 Local_Address      Peer_Address       LD/RD       Interface
 10.1.1.2           10.1.1.1           8192/8193   Unknown
 Tx-interval(ms)    Rx-interval(ms)    Multiplier  Session-State
 1000               1000               3           Up
 Wtr-interval(m)
 0
```

Table 9-124 Description of the display bgp bfd session command output

Item	Description
Local_Address	Local address
Peer_Address	Peer address
LD/RD	Local/remote discriminator
Interface	Interface on which the BFD session is set up **NOTE** Information about the interface on which the BFD session is set up only when the directly connected interface is used to set up the EBGP neighbor relationship. In other cases, information about the interface is displayed as Unknown.
Tx-interval (ms)	Interval for sending BFD packets, in milliseconds
Rx-interval (ms)	Interval for receiving BFD packets, in milliseconds
Multiplier	Local detection multiple

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Session-State	BFD status • Admin down: The BFD session is closed on the local end. • BFD global disable: BFD is disabled globally. • BFD session number exceed: The number of BFD sessions exceeds the maximum limit. • Detect down: BFD detects a link status fault and interrupts the connection. • Init: The BFD session is in the initialized state. • Neighbor down: The peer end detects that the BFD session goes Down and informs the local end of the change, and the local end then sets the neighbor status to Down. • Receive admin down: The BFD session is closed on the peer end (for example, the BFD session is disabled on the peer end). • Up: The BFD session is set up.
Wtr-interval(m)	Interval for flap dampening, in minutes

Related Topics

9.8.105 peer bfd enable
9.8.103 peer bfd

9.8.27 display bgp error

Function

The **display bgp error** command displays BGP errors.

Format

display bgp error

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a BGP fault occurs, run the **display bgp error** command to display BGP error information. BGP error information includes peer error information, route error information, and resource threshold-crossing error information.

Precautions

If no BGP fault occurs, no information is displayed after running the **display bgp error** command.

Example

Display BGP errors.

```
<Huawei> display bgp error
 Error Type    : Peer Error
 Date/Time     : 2010/03/22 11:40:39
 Peer Address  : 10.1.1.2
 VRF Name      : Public
 Error Info    : Router-ID conflict

 Error Type    : Peer Error
 Date/Time     : 2010/03/22 11:40:39
 Peer Address  : 10.1.1.2
 VRF Name      : Public
 Error Info    : Incorrect remote AS

 Error Type    : Route Error
 AddressFamily : IPv4-UNC
 InstanceID    : 0
 Discard count : 20

 Error Type    : Resource exceed limit
 Date/Time     : 2010/03/22 11:40:39
 Limit info    : Route number limit

 Error Type    : Resource exceed limit
 Date/Time     : 2010/03/22 11:40:39
 Limit info    : Label number limit
```

Table 9-125 Description of the display bgp error command output

Item	Description
Error Type	Error type: ● Peer Error: indicates neighbor errors. ● Route Error: indicates route errors. ● Resource exceed limit: indicates that resources exceed the limit.
Date/Time	Date and Time when an error occurs
Peer Address	Address of a peer
VRF Name	VPN Instance name

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Error Info	Error information: ● Router-ID conflict: indicates that router IDs conflict. ● Incorrect remote AS: indicates an incorrect remote AS number.
AddressFamily	Address family
Discard count	Number of discarded routes
Limit info	Information indicating that resources exceed the limit: ● Memory shortage: indicates that memory exceeds the limit. ● Route number limit: indicates that the number of routes exceeds the limit. ● Label number limit: indicates that the number of labels exceeds the limit.

9.8.28 display bgp error discard

Function

The **display bgp error discard** command displays the information about the discarded error BGP packets.

Format

display bgp error discard [**peer** { *ipv4-address* | *ipv6-address* }]

Parameters

Parameter	Description	Value
peer	Displays errors on a specified peer.	-
ipv4-address	Displays errors on a peer with the specified IPv4 address.	It is in dotted decimal notation.
ipv6-address	Displays errors on a peer with the specified IPv6 address.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When a BGP fault occurs, the **display bgp error discard** command can be run to check the information about discarded error packets. The errors include cluster ID conflicts and the threshold overflow of AS-Path attributes.

By specifying the **peer** parameter, you can check the information about the error packets discarded by a specified BGP peer.

Precautions

The **display bgp error discard** command can be used to check only the error routing. To check the error routing among BGP peers, run the **display bgp error** command.

Example

Display information about discarded BGP error packets.

```
<Huawei> display bgp error discard
BGP Discard Info Counts:
Routes received with cluster ID loop          : 0
Routes received with as path count over limit  : 0
Routes advertised with as path count over limit: 0

 No discard record.
```

Table 9-126 Description of the display bgp error discard command output

Item	Description
BGP Discard Info Counts	Number of discarded BGP routes
Routes received with cluster ID loop	Number of discarded BGP routes with a duplicate cluster ID
Routes received with as path count over limit	Number of received BGP routes discarded due to the number of AS-Paths exceeding the upper threshold
Routes advertised with as path count over limit	Number of sent BGP routes discarded due to the number of AS-Paths exceeding the upper threshold
No discard record	No record about packet discarding

 Copyright © Huawei Technologies Co., Ltd.

9.8.29 display bgp group

Function

The **display bgp group** command displays information about BGP peer groups.

Format

display bgp group [*group-name*]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **group** [*group-name*]

display bgp ipv6 group [*group-name*]

display bgp evpn group [*group-name*]

display bgp mdt all group [*group-name*]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **group** [*group-name*]

display bgp multicast group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpnv4	Displays information about BGP VPNv4 peer groups. **NOTE** The AR100&AR120&AR150&AR160&AR200 series does not support this parameter.	-
all	Displays information about all BGP VPNv4 peer groups. **NOTE** The AR100&AR120&AR150&AR160&AR200 series does not support this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about BGP peer groups in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6	Displays information about IPv6 peer groups.	-
evpn	Displays information about EVPN peer groups.	-
mdt	Displays information about BGP peer groups of MDT.	-
vpnv6	Displays information about BGP VPNv6 peer groups.	-
multicast	Displays information about MBGP peer groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Configuring BGP peer groups simplifies BGP network configuration and improves the route advertisement efficiency.

The **display bgp group** command displays information about the peer group, including peers in the peer group and configuration information about the peer group. The **display bgp group** command is used in the following scenarios:

- Verify the configuration after running the **group** command to configure the peer group.
- Verify the configuration after running the **peer group** command to add a peer to the peer group.
- Verify the configuration after running the **undo peer group** command to delete a peer from the peer group.
- Verify the configuration after modifying the configuration of the peer group.

Precautions

BGP has multiple address families, each of which is configured independently. Information about peer groups in address families can be displayed by specifying different parameters.

If no parameter is specified, the **display bgp group** command displays default information about peer groups in the IPv4 unicast address family.

Example

Display information about a peer group named **my-peer**.

```
<Huawei> display bgp group my-peer

 BGP peer-group: my-peer
 Remote AS: 200
 listen-net: 10.2.2.0 24
 Authentication type configured: None
 Group's BFD has been enabled
 Type : internal
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum route advertisement interval is 15 seconds
 listen-only has been configured
 PeerSession Members:
   10.2.2.2

 Maximum allowed route limit: 8000
 Threshold: 75%, Parameter:  always connect-retry(default)
 listen-net: 10.2.2.0 24
 Peer Preferred Value: 0
 No routing policy is configured
 Peer Members:
  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv
  *10.2.2.2         4   200        0        0     0 00:00:47      Active       0
```

Table 9-127 Description of the display bgp group command output

Item	Description
BGP peer-group	Indicates the name of a BGP peer group.
Remote AS	Indicates the number of the AS where a peer group resides.
listen-net	Network segment from which BGP listens to BGP connection requests.
Authentication type configured	Indicates the configured BGP authentication type: ● MD5 ● None: indicates that no BGP authentication is configured.
Group's BFD has been enabled	Indicates that BFD has been enabled for a peer group.

Item	Description
Type	Indicates the type of a peer group: ● internal: indicates that the peer group is an IBGP peer group. ● external: indicates that the peer group is an EBGP peer group.
Configured hold timer value	Indicates the value of the Hold timer.
Keepalive timer value	Indicates the value of the Keepalive timer.
Minimum route advertisement interval	Indicates the minimum interval between route advertisements.
listen-only has been configured	Indicates that the peer or peer group only detects connection requests, and does not initiate any connection.
PeerSession Members	Indicates peers that set up sessions.
Maximum allowed route limit	Indicates the maximum number of allowed BGP routes.
Threshold	Indicates the threshold for the quantity of received BGP routes (in percentage) out of the maximum number of routes that can be received.
Parameter	If **peer route-limit** command is configured, this parameter will be displayed: ● always connect-retry(default): By default, BGP Always connect-retry when the maximum is exceeded and the BGP session is terminated. ● alert-only: Allows the router to generate log message without terminating BGP session when the maximum is exceeded. ● idle-forever: Don't auto-connect-retry until **reset bgp** when the maximum is exceeded and then terminating BGP session. ● idle-timeout: Auto-connect-retry after timeout when the maximum is exceeded and then terminating BGP session.
Peer Preferred Value	Indicates the preferred value of a peer.
Peer Members	Indicates that the following information is about peers.
Peer	Indicates the IP address of a peer.
V	Indicates the BGP version.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AS	Indicates the number of the AS where a member of a peer group resides.
MsgRcvd	Indicates the number of received messages.
MsgSent	Indicates the number of sent messages.
OutQ	Indicates the number of messages to be sent to peers.
Up/Down	Indicates the period of time during which a BGP session keeps the current state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Indicates the BGP state mechanism: ● Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. ● Idle(Admin): indicates that the peer relationship is shut down initiatively and no attempt is made to establish the neighbor relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. ● Idle(Ovlmt): indicates that the peer relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP peer relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP peer relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP peer relationship will not be reestablished. ● Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for the other Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
PrefRcv	Indicates the number of route prefixes received by the local peer from the remote peer.

Related Topics

9.8.117 peer group

9.8.30 display bgp ipv6 bfd session

Function

The **display bgp ipv6 bfd session** command displays information about the BFD session set up by BGP.

Format

display bgp ipv6 bfd session { [**vpnv6 vpn-instance** *vpn-instance-name*] **peer** *ipv6-address* | **all** }

Parameters

Parameter	Description	Value
vpnv6	Displays the BFD session of VPNv6.	-
vpn-instance *vpn-instance-name*	Specifies the name of the VPNv6 instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported.
peer *ipv6-address*	Specifies the IPv6 address of the peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
all	Displays all BFD sessions set up by BGP4+.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The BFD session set up by BGP4+ helps BGP4+ quickly discover faults between BGP4+ peers and inform BGP4+ to recalculate routes for packet forwarding.

Run the **display bgp ipv6 bfd session** command to display information about the BFD session set up by BGP4+ in the following situations:

- Check whether the BFD session is successfully set up or view detailed information about the BFD session that is successfully configured.
- Check whether the BFD session set up by BGP4+ is successfully deleted after running the **undo peer bfd enable** command.
- Verify the configuration after running the **undo peer bfd block** command to prevent a peer from inheriting the BFD function of the peer group.
- Verify the configuration after running the **peer bfd** command to set BFD parameters.

The information about the BFD session of a specified peer can be displayed by specifying different parameters.

- Run the **display bgp ipv6 bfd session vpnv6 vpn-instance** *vpn-instance-name* **peer** *ipv6-address* command to display information about the BFD session of a specified peer in a VPNv6 instance.
- Run the **display bgp ipv6 bfd session peer** *ipv6-address* command to display information about the BFD session of a specified peer on the public network.
- Run the **display bgp ipv6 bfd session all** command to display information about the BFD sessions of all BGP4+ peers.

Prerequisites

The BFD session has been set up using the **peer bfd enable** command. If the BFD session has not been set up by BGP4+, no information is displayed after running the **display bgp ipv6 bfd session** command.

Example

Display all BFD sessions set up by BGP.

```
<Huawei> display bgp ipv6 bfd session all
  Local_Address   : 2001:db8:11::11  Peer_Address    : 2001:db8:22::22
  Tx-interval(ms) : 1000             Rx-interval(ms) : 1000
  Multiplier      : 3                Interface       : Unknown
  LD/RD           : 1111/4444        Session-State   : Init
  Wtr-interval(m) : 0

VPN-Instance vrf1:
  Local_Address  : 2001:db8:1::2     Peer_Address   : 2001:db8:1::1
```

```
Tx-interval(ms): 0              Rx-interval(ms): 0
Multiplier     : 0            Interface      : Unknown
LD/RD          : 8195/0         Session-State  : Init
Wtr-interval(m): 0
```

Table 9-128 Description of the **display bgp ipv6 bfd session** command output

Item	Description
Local_Address	Local address
Peer_Address	Peer address
Tx-interval (ms)	Interval for sending BFD packets, in milliseconds
Rx-interval (ms)	Interval for receiving BFD packets, in milliseconds
Multiplier	Local detection multiple
Interface	Interface on which the BFD session is set up **NOTE** Information about the interface on which the BFD session is set up only when the directly connected interface is used to set up the EBGP neighbor relationship. In other cases, information about the interface is displayed as Unknown.
LD/RD	Local/remote discriminator
Session-State	BFD status • Admin down: The BFD session is closed on the local end. • BFD global disable: BFD is disabled globally. • BFD session number exceed: The number of BFD sessions exceeds the maximum limit. • Detect down: BFD detects a link status fault and interrupts the connection. • Init: The BFD session is in the initialized state. • Neighbor down: The peer end detects that the BFD session goes Down and informs the local end of the change, and the local end then sets the neighbor status to Down. • Receive admin down: The BFD session is closed on the peer end (for example, the BFD session is disabled on the peer end). • Up: The BFD session is set up.
Wtr-interval(m)	Interval for flap dampening, in minutes
VPN-Instance vrf1	VPN instance name VRF1

Related Topics

9.8.105 peer bfd enable

9.8.103 peer bfd

9.8.31 display bgp ipv6 routing-table

Function

The **display bgp ipv6 routing-table** command displays BGP IPv6 routes.

Format

display bgp ipv6 routing-table [**verbose**]

display bgp ipv6 routing-table *ipv6-address* [*prefix-length*]

display bgp ipv6 routing-table as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

display bgp ipv6 routing-table community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**]* [**whole-match**]

display bgp ipv6 routing-table community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp ipv6 routing-table different-origin-as

display bgp ipv6 routing-table regular-expression *as-regular-expression*

display bgp ipv6 routing-table peer { *ipv6-address* | ipv4-address } { **accepted-routes** | **advertised-routes** [*dest-ipv6-address* [*prefix-length*]] | **received-routes** [**active**] }

display bgp ipv6 routing-table peer *ipv6-address* **received-routes** *dest-ipv6-address* [*prefix-length* [**original-attributes**]]

display bgp ipv6 routing-table time-range *start-time end-time*

Parameters

Parameter	Description	Value
verbose	Displays detailed information about routes.	-
ipv6-address	Specifies the IPv6 address of the peer.	It is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of the prefix.	The value is an integer that ranges from 0 to 128.
as-path-filter	Displays the routes that match the specified filter.	-

Parameter	Description	Value
as-path-filter-number	Specifies the number of the matching AS-Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
community	Displays the routing information of the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	It is an integer ranging from 0 to 4294967295.
aa:nn	Specifies the community attribute number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
whole-match	Indicates the exact matching.	-
community-filter	Displays the routes that match the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	The name is a string of 1 to 51 characters. The string cannot be all numbers.
basic-community-filter-number	Specifies the number of basic community filter.	It is an integer ranging from 1 to 99.
advanced-community-filter-number	Specifies the number of advanced community filter.	It is an integer ranging from 100 to 199.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
different-origin-as	Displays routes that have the same destination address but different source ASs.	-
peer	Displays the routing information for the specified BGP peer.	-
advertised-routes	Displays the routes advertised to the specified peer.	-
dest-ipv6-address	Specifies the destination IPv6 address.	It is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
received-routes	Displays the routes received from the specified peer.	-
active	Displays the active routes received from the specified peer.	-
original-attributes	Displays the original attributes of a public route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
regular-expression *as-regular-expression*	Specifies the matched AS regular expression.	The value is a string of 1 to 80 characters.
accepted-routes	Displays the routes that are received from the peer and filtered through a routing policy.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-range *start-time end-time*	Displays IPv6 BGP routes that flap within the specified time period. For example, the value 0d0h5m0s of *start-time* indicates five minutes before the current time. The value 0d0h10m0s of *end-time* indicates 10 minutes before the current time. All IPv6 BGP routes with the Keepalive time in the range of 5 to 10 minutes are displayed.	The value ranges of *start-time* and *end-time* both are 0d0h0m0s-10000d23h59m59s.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

You can run the **display bgp ipv6 routing-table time-range** *start-time end-time* command to view BGP4+ routes that flap within the specified time period. For example, if service traffic is abnormal or CPU usage of the device remains high within a certain time period, you can run this command to check whether route flapping occurs within the specified time period. The faulty route can be viewed in the command output, facilitating fault location.

Example

Display BGP+ routes.

```
<Huawei> display bgp ipv6 routing-table

 BGP Local router ID is 10.1.1.1
 Status codes: * - valid, > - best, d - damped, x - best external,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 1
 *>  Network  : FC00:0:0:2000::                    PrefixLen : 64
     NextHop  : FC00:0:0:2000::1                   LocPrf    :
     MED      : 0                              PrefVal   : 0
     Label    :
     Path/Ogn : i
```

Displays BGP IPv6 routes that flap within the specified time period.

```
<Huawei> display bgp ipv6 routing-table time-range 0d5h0m0s 1d5h0m0s
BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>i Network  : FC00:0:0:100::100                PrefixLen : 128
     NextHop  : FC00:0:0:12::1                  Duration  : 05h46m16s
     Peer     : FC00:0:0:12::1
     Path/Ogn : ?
 * i
     NextHop  : FC00:0:0:112::1                 Duration  : 05h46m16s
     Peer     : FC00:0:0:112::1
     Path/Ogn : ?
 *>i Network  : FC00:0:0:111::111                PrefixLen : 128
     NextHop  : FC00:0:0:12::1                  Duration  : 05h46m16s
     Peer     : FC00:0:0:12::1
     Path/Ogn : ?
 * i
     NextHop  : FC00:0:0:112::1                 Duration  : 05h46m16s
     Peer     : FC00:0:0:112::1
     Path/Ogn : ?
```

Table 9-129 Description of the display bgp ipv6 routing-table command output

Item	Description
BGP Local router ID	Router ID of the local BGP device.
Network	Indicates the network address in the BGP routing table.
PrefixLen	Indicates the prefix length.
NextHop	Indicates the next-hop address of the packet.
LocPrf	Indicates the local preference.
MED	Indicates the MED of the route.
PrefVal	Indicates the preferred value.
Label	Indicates the label value.
Duration	Route duration
Peer	Peer IP address
Path/Ogn	Indicates the AS_Path number and the Origin attribute.

Display detailed information about the specified invalid BGP4+ routes.

```
<Huawei> display bgp ipv6 routing-table 1::1
 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Paths:   1 available, 0 best, 0 select
 BGP routing table entry information of 1::1/128:
 From: 10::2 (10.1.1.2)
 Route Duration: 00h17m46s
 Relay IP Nexthop: ::
 Relay IP Out-Interface:
```

```
 Original nexthop: 20::2
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP
unreachable
 Not advertised to any peer yet
```

Table 9-130 Description of the **display bgp ipv6 routing-table** command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Paths	Information about paths of BGP routes
BGP routing table entry information of 1::1/128:	The following information is about 1::1/128 routing entries.
From	IP address of the router that sends the route. 10.1.1.2 is the source interface IP address of the peer with which the BGP connection is established, and 10::2 is the router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	IP iterated next hop.
Relay IP Out-Interface	IP iterated outbound interface.
Original nexthop	Original next hop.
AS-path 200	AS_Path attribute.
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
pre 255	The priority of the BGP route is 255.
invalid for IP unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to be iterated to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to be iterated to a tunnel.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

9.8.32 display bgp ipv6 routing-table statistics

Function

The **display bgp ipv6 routing-table statistics** command displays statistics about BGP IPv6 routes.

Format

display bgp ipv6 routing-table statistics

display bgp ipv6 routing-table statistics as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

display bgp ipv6 routing-table statistics community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp ipv6 routing-table statistics community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp ipv6 routing-table peer { *ipv6-address* | *ipv4-address* } { **advertised-routes** | **received-routes** [**active**] } **statistics**

display bgp ipv6 routing-table statistics regular-expression *as-regular-expression*

display bgp ipv6 routing-table statistics different-origin-as

Parameters

Parameter	Description	Value
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
community	Displays the routing information of the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	It is an integer ranging from 0 to 4294967295.
aa:nn	Specifies the community attribute number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with the No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays the routing information that matches the specified BGP community filter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
community-filter-name	Specifies the name of the community filter.	The name is a string of 1 to 51 characters. The string cannot be all numbers.
basic-community-filter-number	Specifies the number of basic community filter.	It is an integer ranging from 1 to 99.
advanced-community-filter-number	Specifies the number of advanced community filter.	It is an integer ranging from 100 to 199.
peer	Displays the routing information for the specified BGP peer.	-
ipv6-address	Specifies the IPv6 address of the peer.	It is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv4-address	Specifies the IPv4 address of the peer.	The value is in dotted decimal notation.
advertised-routes	Displays the routes advertised to the specified peer.	-
received-routes	Displays the routes received from the specified peer.	-
active	Displays the active routes received from the specified peer.	-
regular-expression *as-regular-expression*	Specifies the matched AS regular expression.	The value is a string of 1 to 80 characters.
different-origin-as	Displays routes that have the same destination address but different source ASs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display statistics of BGP4+ routes.

```
<Huawei> display bgp ipv6 routing-table statistics

 Total Number of Routes: 4
```

Table 9-131 Description of the **display bgp ipv6 routing-table statistics** command output

Item	Description
Total Number of Routes	Total number of routes in the routing table.

9.8.33 display bgp mdt routing-table

Function

The **display bgp mdt routing-table** command displays BGP Multicast Distribution Tree (MDT) routes.

Format

display bgp mdt { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

display bgp mdt route-distinguisher *route-distinguisher* **routing-table** [*network* [*mask* | *mask-length*]]

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table regular-expression** *as-regular-expression*

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community** [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp mdt all routing-table peer *ipv4-address* { **advertised-routes** [**statistics** | *ipv4-address*] | **received-routes** [**active**] [**statistics**] }

display bgp mdt all routing-table peer *ipv4-address* **received-routes** *network*

Parameters

Parameter	Description	Value
all	Displays all the BGP routes of MDT.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays BGP routing information of the specified Route Distinguisher (RD).	-
vpn-instance *vpn-instance-name*	Displays the BGP routing information of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
network	Specifies the IPv4 network address.	-
mask | *mask-length*	Specifies mask in dotted decimal notation or mask-length.	-
longer-prefixes	Matches according to the mask longer than the specified length.	-
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS_Path filter.	-
as-path-filter-name	Specifies the name of the matching AS_Path filter.	It is case-sensitive.
cidr	Displays the information about the Classless Inter-Domain Routing (CIDR).	-
different-origin-as	Displays routes that have the same destination address but different source ASs.	-
regular-expression *as-regular-expression*	Specifies the matched AS regular expression.	The value is a string of 1 to 80 characters.
community-filter	Displays the routes that match the specified BGP community filter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
community-filter-name	Specifies the name of the community filter.	-
basic-community-filter-number	Specifies the number of basic community filter.	-
advanced-community-filter-number	Specifies the number of advanced community filter.	-
community	Displays the routing information of the specified BGP community attribute in the routing table.	-
aa:nn	Specifies the community attribute number. You can set a maximum of 29 community numbers.	-
community-number	Specifies the community number.	-
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
whole-match	Indicates the exact matching.	-
peer *ipv4-address*	Displays the routing information for the specified BGP peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

When BGP MDT routing table is displayed, if the length of the destination address mask of an IPv4 route is the same as that of its natural mask, the mask length is not displayed.

Example

Display all the BGP MDT routing information.

```
<Huawei> display bgp mdt all routing-table

 BGP Local router ID is 192.168.7.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 3
 Route Distinguisher: 100:1

     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                    0      ?

 Route Distinguisher: 200:1

     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>i  1.1.1.1/32         192.168.100.10  0          100        0      33 55?
 *>i  2.2.2.2/32         192.168.100.10  0          100        0      33 55?

 Total number of routes of IPv4-MDT-family for vpn-instance vrf1: 3
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

 *>   1.1.1.1/32         0.0.0.0         0                    0      ?
 * i                    192.168.100.10  0          100        0      33 55?
 *>i  2.2.2.2/32         192.168.100.10  0          100        0      33 55?
```

Display all the BGP MDT routing information of the VPN instance named vpna.

```
<Huawei> display bgp mdt vpn-instance vpna routing-table

Total Number of Routes: 2

 BGP Local router ID is 2.2.2.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network          NextHop        MED      LocPrf    PrefVal Path/Ogn

 *>i  10.1.1.0/24      1.1.1.9         0        100        0      ?
 *>i  10.2.1.0/24      3.3.3.9         0        100        0      ?
```

Display the BGP MDT routing information of the specified RD.

```
<Huawei> display bgp mdt route-distinguisher 100:1 routing-table

 BGP Local router ID is 192.168.7.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 100:1

 Total Number of Routes: 1
```

```
     Network          NextHop       MED       LocPrf    PrefVal Path/Ogn

*>   1.1.1.1/32       0.0.0.0       0                   0      ?

Total number of routes of IPv4-MDT-family for vpn-instance vrf1: 3
     Network          NextHop       MED       LocPrf    PrefVal Path/Ogn

*>   1.1.1.1/32       0.0.0.0       0                   0      ?
* i                 192.168.100.10  0         100       0      33 55?
*>i  2.2.2.2/32       192.168.100.10  0         100       0      33 55?
```

Display all BGP MDT routes of community 1000:100.

```
<Huawei> display bgp mdt all routing-table community 1000:100

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total number of routes from all PE: 1

Route Distinguisher: 100:1

     Network          NextHop       MED       LocPrf    PrefVal Community

*>i  10.1.1.0/24      1.1.1.1       0         100       0      <1000:100>

Total number of routes of IPv4-MDT-family for vpn-instance vpna: 1
     Network          NextHop       MED       LocPrf    PrefVal Community

*>i  10.1.1.0/24      1.1.1.1       0         100       0      <1000:100>
```

Table 9-132 Description of the **display bgp mdt routing-table** command output

Item	Description
Network	Network address in the BGP routing table
Next Hop	Next Hop address through which the packet has to be sent
MED	Multi-Exit discriminator
LocPrf	Local priority
PrefVal	Value preferred by the protocol
Path/Ogn	AS_Path number and the attributes of Origin
Community	Community attributes

Display all BGP MDT routes of community 1000:100 with the internet community attribute.

```
<Huawei> display bgp mdt all routing-table community 1000:100 internet

BGP Local router ID is 2.2.2.2
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Total number of routes from all PE: 1
```

```
Route Distinguisher: 100:1


     Network           NextHop        MED        LocPrf    PrefVal Community

*>i  10.1.1.0/24       1.1.1.1         0          100        0      <1000:100>

Total number of routes of IPv4-MDT-family for vpn-instance vpna: 4
     Network           NextHop        MED        LocPrf    PrefVal Community

*>i  10.1.1.0/24       1.1.1.1         0          100        0      <1000:100>
*>   10.2.1.0/24       0.0.0.0         0                     0
*                    10.2.1.1        0                     0
*>   10.2.1.2/32       0.0.0.0
```

Table 9-133 Description of the **display bgp mdt all routing-table peer received-routes** command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Route Distinguisher	Route distinguisher.
BGP routing table entry information of 2.2.2.2/32	The following information is about 2.2.2.2/32 routing entries.
From	IP address of the router that sends the route. 2.2.2.2 is the IP address of the source interface of the peer with which the BGP connection is established, and 2.2.2.9 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	IP iterated next hop.
Relay IP Out-Interface	IP iterated outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
localpref	Local priority.
pref-val	Value preferred by the protocol.
valid	The BGP route is a valid route.
internal	The BGP route is an internal route.
best	The BGP route is an optimal route.
select	The BGP route is a preferred route.
pre 255	The priority of the BGP route is 255.
IGP cost	Cost of the relied next hop route of BGP route.
MDT group address	Group address of MDT.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

Display detailed information about the specified invalid BGP MDT routes.

```
<Huawei> display bgp mdt all routing-table 1.1.1.11
BGP local router ID : 192.168.1.108
Local AS number : 100

Total routes of Route Distinguisher(1:2): 1
BGP routing table entry information of 1.1.1.11/32:
From: 1.1.1.1 (192.168.1.104)
Route Duration: 00h00m05s
Relay IP Nexthop: 48.1.1.4
Relay IP Out-Interface: Ethernet0/0/1
```

```
Original nexthop: 1.1.1.1
Qos information : 0x0
Ext-Community:RT <111 : 1>
AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for route-policy
not pass

MDT group address: 232.1.1.2
Not advertised to any peer yet


Total number of routes of IPv4-MDT-family for vpn-instance 2: 1
BGP routing table entry information of 1.1.1.11/32:
From: 1.1.1.1 (192.168.1.104)
Route Duration: 00h00m05s
Original nexthop: 1.1.1.1
Qos information : 0x0
Ext-Community:RT <111 : 1>
AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for route-policy
not pass
MDT group address: 232.1.1.2
Not advertised to any peer yet
```

Table 9-134 Description of the **display bgp mdt routing-table** command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Total routes of Route Distinguisher(1:2)	The total number of routes with the RD of 1:2.
BGP routing table entry information of 1.1.1.11/32	The following information is about 1.1.1.11/32 routing entries.
From	IP address of the router that sends the route. 192.168.1.104 is the IP address of the source interface of the peer with which the BGP connection is established, and 1.1.1.1 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	IP iterated next hop.
Relay IP Out-Interface	IP iterated outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
pre 255	The priority of the BGP route is 255.
invalid for route-policy not pass	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to be iterated to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to be iterated to a tunnel.
MDT group address	Group address of MDT.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

9.8.34 display bgp mdt brief

Function

The **display bgp mdt brief** command displays brief information about VPN instances in BGP-MDT address family.

Format

display bgp mdt { **all** | **vpn-instance** *vpn-instance-name* } **brief**

Parameters

Parameter	Description	Value
all	Displays information about Multicast Distribution Tree (MDT) instances and all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the **display bgp mdt brief** command is used to display information about MDT, VPN instances are listed in the lexicographic order of the VPN instance name.

Example

Display brief information about MDT instances and all VPN instances.

```
<Huawei> display bgp mdt all brief

MDT:
  Rd Num             Peer Num           Route Num
  0                  1                  0

VPN-Instance(IPv4-MDT-family):
  VPN-Instance Name   Peer Num           Route Num
  vrf0                0                  0
  vrf1                0                  0
  vrf11               0                  0
  vrf12               0                  0
  vrf13               0                  0
  vrf14               0                  0
  vrf2                0                  20
  vrf3                0                  20
  vrf4                0                  24
  vrf5                0                  24
  vrf6                0                  0
  vrf7                0                  0
  vrf8                0                  20
```

Table 9-135 Description of the **display bgp mdt all brief** command output

Item	Description
Rd Num	Number of Route Distinguishers (RDs)
Peer Num	Number of peers
Route Num	Number of routes
VPN-Instance Name	Name of a VPN instance

9.8.35 display bgp mdt routing-table statistics

Function

The **display bgp mdt routing-table statistics** command displays the statistics of the BGP Multicast Distribution Tree (MDT) routes.

Format

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics**

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics regular-expression** *as-regular-expression*

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp mdt { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community** [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

Parameters

Parameter	Description	Value
all	Displays all the BGP routes of MDT.	-
route-distinguisher *route-distinguisher*	Displays BGP routing information of the specified Route Distinguisher (RD).	-
vpn-instance *vpn-instance-name*	Displays the BGP routing information of the specified VPN instance.	-
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matched AS_Path filter.	-
as-path-filter-name	Specifies the name of the matching AS_Path filter.	It is case-sensitive.
cidr	Displays the information about the Classless Inter-Domain Routing (CIDR).	-
different-origin-as	Displays the routes that have the same destination address but different source AS number.	-
regular-expression *as-regular-expression*	Indicates the matched AS regular expression.	The value is a string of 1 to 80 characters.
community-filter	Displays the routing information that matches the specified BGP community filter.	-
community-filter-name	Specifies the name of the community filter.	-
basic-community-filter-number	Specifies the number of basic community filter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
whole-match	Indicates exact matching.	-
advanced-community-filter-number	Specifies the number of advanced community filter.	-
community	Displays the routing information of the specified BGP community attribute in the routing table.	-
aa:nn	Specifies the community number.	-
community-number	Specifies the community number.	-
internet	Displays the BGP routes with Internet community attribute.	-
no-advertise	Displays the BGP routes with the No-Advertise community attribute.	-
no-export	Displays the BGP routes with the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes with the No-Export-Subconfed community attribute.	-
peer *ipv4-address*	Displays the routing information for the specified BGP peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the statistics of the BGP MDT routing table.

```
<Huawei> display bgp mdt all routing-table statistics

 Total number of routes from all PE: 20
```

```
Total number of routes of IPv4-MDT-family for vpn-instance vpn1: 12
```

Table 9-136 Description of the **display bgp mdt routing-table statistics** command output

Item	Description
Total number of routes from all PE	The number of the routes received from PEs in the BGP MDT routing table
Total number of routes of IPv4-MDT-family for vpn-instance	The number of the routes of the specified VPN instance in the BGP MDT routing table

9.8.36 display bgp multicast group

Function

The **display bgp multicast group** command displays the information about an MBGP peer group.

Format

display bgp multicast group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the peer group is specified, the detailed information on the specified peer group is displayed.

If the peer group is not specified, the information on all MBGP peer groups is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the information about peer group **my-peer**.

```
<Huawei> display bgp multicast group my-peer
BGP peer-group: my-peer
 Remote AS: 1
 Authentication type configured: None
 Type : external
 Configured hold timer value: 180
 Keepalive timer value: 60
 Connect-retry timer value: 32
 Minimum route advertisement interval is 30 seconds
 PeerSession Members:
   172.16.14.1
 Peer Preferred Value: 0
 No routing policy is configured
 Peer Members:
  Peer          V  AS  MsgRcvd  MsgSent  OutQ   Up/Down     State   PrefRcv
  172.16.14.1   4   1      43       29     0    00:03:03   Established   21
```

Table 9-137 Description of the display bgp multicast group command output

Item	Description
BGP peer-group: my-peer	Peer group: name of the group
Remote AS	The number of the AS where the peer resides
Authentication type configured	Indicates the configured BGP authentication type: ● MD5 ● Keychain (kk), in which kk indicates the name of the configured keychain authentication ● None, which indicates no BGP authentication is configured
Type	Indicates the types of peers: ● internal: The type of the peer group is IBGP ● external: The type of the peer group is EBGP
Configured hold timer value	Value of the holdtime timer
Keepalive timer value	Value of the Keepalive timer
Connect-retry timer value	Value of the Connect-retry timer
Minimum route advertisement interval	Shortest interval for advertising routes
PeerSession Members	Indicates peers that set up session connections
Peer Preferred Value	Preferred value of peers

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Peer	IP address of the peer
V	MBGP version
As	The number of the AS where the peer reside
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent to the peer
Up/Down	Time during which the MBGP session is in the current state
State	Indicates the MBGP state mechanism: ● Idle: indicates that MBGP denies the connection request. This is the initiate status of MBGP. ● Active: indicates that MBGP tries to set up TCP connection. This is the intermediate status of MBGP. ● Established: In the status, MBGP peers can exchange Update, Notification and Keepalive packets. ● Connect: indicates that MBGP performs other actions after the TCP connection is set up. ● OpenSent: indicates that MBGP waits for an Open message from the peer. ● OpenConfirm: indicates that MBGP wait for a Notification message or a Keepalive message.
PrefRcv	The number of prefixes received by the local peer from the remote peer

9.8.37 display bgp multicast network

Function

The **display bgp multicast network** command displays the routes to be advertised by MBGP through the **network** command.

Format

display bgp multicast network

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command is used to display all the configurations of the **network (BGP)** command in the IPv4 multicast address family view. Routes can be imported and then advertised by MBGP only when the route prefix satisfies the following conditions:

- It is specified in the **network** command
- It already exists in the IP routing table.
- It is active.

Example

Display the routing information of a network segment advertised by MBGP.

```
<Huawei> display bgp multicast network
 BGP Local Router ID is 10.2.2.9
 Local AS Number is 100(Multicast)
 Network          Mask            Route-policy

 10.1.1.1         255.255.255.0
 10.2.2.2         255.255.255.0
```

Table 9-138 Description of the display bgp multicast network command output

Item	Description
BGP Local Router ID	ID of the local MBGP router
Local AS Number	Number of the local AS
Network	Network address locally advertised
Mask	Mask of the network address
Route-policy	Used Routing policy

Related Topics

9.8.93 network (BGP)

 Copyright © Huawei Technologies Co., Ltd.

9.8.38 display bgp multicast paths

Function

The **display bgp multicast paths** command displays the information about path attributes of MBGP.

Format

display bgp multicast paths [*as-regular-expression*]

Parameters

Parameter	Description	Value
as-regular-expression	Displays the regular expression of the matched AS.	The value is a string of 1 to 80

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the information about MBGP paths.

```
<Huawei> display bgp multicast paths 1

Total Number of Routes: 17


  Address         Refcount   MED        Path/Origin
  0x54169A4         17         0          1?
```

Table 9-139 Description of the display bgp multicast paths command output

Item	Description
Total Number of Routes	Total Number of Routes
Address	Address of the path attribute node in the local database in the hexadecimal format
Refcount	Number of times that the route are referenced
MED	Multi-Exit discriminator

Item	Description
Path	AS_Path list of the route
Origin	Origin of the route

9.8.39 display bgp multicast peer

Function

The **display bgp multicast peer** command displays the information about a specified MBGP peer. If *peer-address* is not specified, the information about all MBGP peers is displayed.

Format

display bgp multicast peer [[*peer-address*] **verbose**]

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MBGP peer.	The address is in dotted decimal notation.
verbose	Specifies the detailed information about an MBGP peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the information about all MBGP peers.

```
<Huawei> display bgp multicast peer
 BGP local router ID : 10.13.13.9
 Local AS number : 1
 Total number of peers : 1                 Peers in established state : 1
  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv
  10.2.1.2        4     2       36       37     0 00:15:35 Established      24
```

Table 9-140 Description of the display bgp multicast peer command output

Item	Description
BGP local router ID	ID of the local MBGP Router
Local AS number	Local AS number
Total number of peers	Total number of peers
Peers in established state	Number of peers in established state
Peer	IP address of peers
V	MBGP version of peers
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Messages to be sent to the specified peers
Up/Down	Period during which the MBGP session is in the current state
State	Status of the peers
PrefRcv	Indicates the number of prefixes received by the local peer from the remote peer

Related Topics

9.8.114 peer enable (BGP)

9.8.40 display bgp multicast routing-table

Function

The **display bgp multicast routing-table** command displays the MBGP routing information of a specified network in the MBGP routing table.

Format

display bgp multicast routing-table [*ip-address* [*mask-length* [**longer-prefixes**] | *mask* [**longer-prefixes**]]]

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address.	The address is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the mask length of the IPv4 address.	The value is an integer ranges from 0 to 32.
mask	Specifies the mask of the IPv4 address.	The value is in dotted decimal notation.
longer-prefixes	Matches routes whose masks are shorter than the specified mask length.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *ip-address* is not specified, this command will display all the information in the MBGP routing table.

Example

Display MBGP routing information.

```
<Huawei> display bgp multicast routing-table
 BGP local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 14
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>   10.1.2.0/24        10.2.1.2                       0      2?
 *>   10.1.13.0/24       0.0.0.0        0               0      ?
 *>   10.1.13.2/32       0.0.0.0        0               0      ?
 *>   10.2.1.0/24        0.0.0.0        0               0      ?
 *>   10.2.1.0/24        10.2.1.2       0               0      2?
 *>   10.2.1.1/32        0.0.0.0        0               0      ?
 *>   10.2.13.0/24       0.0.0.0        0               0      ?
 *>   10.2.13.1/32       0.0.0.0        0               0      ?
 *>   10.2.13.2/32       0.0.0.0        0               0      ?
```

Table 9-141 Description of the display bgp multicast routing-table command output

Item	Description
BGP local router ID	BGP local router ID.
Status codes	Status of a routing entry.
Total Number of Routes	Total number of routes in the routing table.

Item	Description
Network	Indicates the network address in the MBGP routing table.
NextHop	Indicates the next-hop address for the packet.
MED	Indicates the MED of the route.
LocPrf	Indicates the local preference.
PrefVal	Indicates the preferred value.
Path/Ogn	Indicates the AS_Path number and the Origin attribute.

Display detailed information about the specified invalid MBGP routes.

```
<Huawei> display bgp multicast routing-table 1.1.1.1
 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Paths:   2 available, 0 best, 0 select
 BGP routing table entry information of 1.1.1.1/32:
 From: 2.2.2.2 (10.1.1.2)
 Route Duration: 00h01m15s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 20.1.1.2
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP
unreachable
 Not advertised to any peer yet

 BGP routing table entry information of 1.1.1.1/32:
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h01m15s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 20.1.1.2
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP
unreachable
 Not advertised to any peer yet
```

Table 9-142 Description of the **display bgp multicast routing-table** command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Paths	Information about paths of BGP routes
BGP routing table entry information of 1.1.1.1/32	The following information is about 1.1.1.1/32 routing entries.

Item	Description
From	IP address of the router that sends the route. 10.1.1.2 is the IP address of the source interface of the peer with which the BGP connection is established, and 2.2.2.2 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	IP iterated next hop.
Relay IP Out-Interface	IP iterated outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information.
AS-path 200	AS_Path attribute.
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
pre 255	The BGP route preference is 255.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
invalid for IP unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to be iterated to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to be iterated to a tunnel.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

9.8.41 display bgp multicast routing-table as-path-filter

Function

The **display bgp multicast routing-table as-path-filter** command displays the routing information that matches the filtering list.

Format

display bgp multicast routing-table as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

Parameters

Parameter	Description	Value
as-path-filter-number	Specifies the number of the matched AS Path filtering list.	The value is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matched AS Path filtering list.	The value is a string of 1 to 51 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display routing information that match the AS-path filtering list 1.

```
<Huawei> display bgp multicast routing-table as-path-filter 1
BGP local router ID is 10.14.14.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 15
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>i  10.1.13.0/24       10.2.1.1       0          100       0       1?
 *>i  10.2.1.0/24        10.2.1.1       0          100       0       1?
 *>i  10.2.13.0/24       10.2.1.1       0          100       0       1?
 *>i  10.2.13.1/32       10.2.1.1       0          100       0       1?
```

Table 9-143 Description of the display bgp multicast routing-table as-path-filter command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packet
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Path/Ogn	AS_Path and the Origin attribute

9.8.42 display bgp multicast routing-table cidr

Function

The **display bgp multicast routing-table cidr** command displays the routing information of classless inter-domain routing (CIDR).

Format

display bgp multicast routing-table cidr

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the information about CIDR.

```
<Huawei> display bgp multicast routing-table cidr
 BGP Local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 9
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>   10.1.2.0/24        10.2.1.2                       0      2?
 *>   10.2.1.0/24        10.2.1.2        0              0      2?
 *>   10.7.1.0/24        10.2.1.2                       0      2?
 *>   10.7.1.1/32        10.2.1.2                       0      2?
 *>   10.7.1.2/32        10.2.1.2        0              0      2?
 *>   10.11.12.0/24      10.2.1.2        0              0      2?
 *>   10.11.12.1/32      10.2.1.2        0              0      2?
```

Table 9-144 Description of the display bgp multicast routing-table cidr command output

Item	Description
BGP Local router ID	BGP local router ID
Status codes	Status of a routing entry.
Total Number of Routes	Total number of routes in the routing table.
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packet
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Path/Ogn	Displays the AS path and the Origin attribute

 Copyright © Huawei Technologies Co., Ltd.

9.8.43 display bgp multicast routing-table community

Function

The **display bgp multicast routing-table community** command displays the routing information of a specified MBGP community.

Format

display bgp multicast routing-table community [*aa:nn* | *community-number*] & <1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

Parameters

Parameter	Description	Value
aa:nn	Specifies the MBGP community number. You can specify a maximum of 29 MBGP communities.	Both aa and nn are integers ranging from 0 to 65535.
community-number	Specifies the MBGP community number. You can specify a maximum of 29 MBGP communities.	It is an integer ranging from 0 to 4294967295.
internet	Displays the MBGP routes with the Internet community attribute. The Internet community attribute indicates the matching routes sent to all remote peers.	-
no-advertise	Displays MBGP routes with the no-advertise community attribute. The no-advertise community attribute indicates that the matching routes are not sent to any peer.	-
no-export	Indicates MBGP routes with the no-export community attribute. The no-expert community attribute indicates that the matching routes are not advertised to other ASs but to other sub-ASs in the confederation.	-
no-export-subconfed	Displays MBGP routes with the no-export-subconfed community attribute. The no-export-subconfed community attribute indicates that the matching routes are not advertised outside the local AS.	-
whole-match	Indicates the precise matching.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display MBGP routing information of Community 100:100.

```
<Huawei> display bgp multicast routing-table community 100:100
 BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 1
      Network          NextHop       MED     LocPrf    PrefVal    Community
 *>   10.1.1.0/24      10.2.1.1      0                 0          <100:100>
```

Display MBGP routing information with the internet community attribute or that of Community 100:100.

```
<Huawei> display bgp multicast routing-table community 100:100 internet

 BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 5
      Network          NextHop       MED       LocPrf    PrefVal   Community

 *>   10.1.1.1/32      10.1.1.2      0                   0         <100:100>,internet
 *>   10.3.3.3/32      10.2.1.1      0                   0         <100:100>,internet
 *>   10.1.1.0/24      10.2.1.1      0                   0         <100:100>,internet
 *>   10.2.13.0/24     10.2.1.1      0                   0         <100:100>,internet
```

Table 9-145 Description of the display bgp multicast routing-table community command output

Item	Description
BGP local router ID	BGP local router ID
Status codes	Status of a routing entry.
Total Number of Routes	Total number of routes in the routing table.
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packets
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Community	Community attribute

 Copyright © Huawei Technologies Co., Ltd.

9.8.44 display bgp multicast routing-table community-filter

Function

The **display bgp multicast routing-table community-filter** command displays the multicast routing information that matches a specified MBGP community list.

Format

display bgp multicast routing-table community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

Parameters

Parameter	Description	Value
basic-community-filter-number	Specifies the number of basic community filter.	The value is an integer that ranges from 1 to 99.
advanced-community-filter-number	Specifies the number of advanced community filter.	The value is an integer that ranges from 100 to 199.
community-filter-name	Specifies the name of the community filter.	The value is a string of 1 to 51 case-sensitive characters without spaces.
whole-match	Indicates the exact matching.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the routing information the matches a specified MBGP community list.

```
<Huawei> display bgp multicast routing-table community-filter 1
BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal    Community
 *>   10.10.10.0/24      10.2.1.1       0                    0          <100:100>
```

Table 9-146 Description of the display bgp multicast routing-table community-filter command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
NextHop	Next hop address of the packet
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value
Community	community attribute

9.8.45 display bgp multicast routing-table dampened

Function

The **display bgp multicast routing-table dampened** command displays the dampened MBGP routes.

Format

display bgp multicast routing-table [**statistics**] **dampened**

Parameters

Parameter	Description	Value
statistics	Displays the statistics of dampened routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the dampened routes of MBGP.

```
<Huawei> display bgp multicast routing-table dampened
 BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 1
     Network            From            Reuse      Path/Ogn
 d   10.1.0.0/16        10.2.1.1        00:45:05   1?
```

Table 9-147 Description of the display bgp multicast routing-table dampened command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
From	IP address of MBGP peer from which the route is received
Reuse	Reuse value
Path/Ogn	AS-Path number and the attributes of Origin

Related Topics

9.8.20 dampening

9.8.46 display bgp multicast routing-table dampening parameter

Function

The **display bgp multicast routing-table dampening parameter** command displays the information about the MBGP dampening parameters.

Format

display bgp multicast routing-table dampening parameter

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the MBGP dampening parameters.

```
<Huawei> display bgp multicast routing-table dampening parameter
 Maximum Suppress Time(in second) : 3973
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in second)         : 900
 Suppress-Limit                   : 2000
```

Table 9-148 Description of the display bgp multicast routing-table dampening parameter command output

Item	Description
Maximum Suppress Time (in second)	Maximum suppression time (in second)
Ceiling Value	Ceiling value of the penalty
Reuse Value	Threshold for routes leaving the suppression state
HalfLife Time (in second)	Half life time of the reachable route
Suppress-Limit	Threshold for routes entering the suppression state

Related Topics

9.8.20 dampening

9.8.47 display bgp multicast routing-table different-origin-as

Function

The **display bgp multicast routing-table different-origin-as** command displays the routes with the same destination but different source AS numbers.

Format

display bgp multicast routing-table different-origin-as

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Displays the routes with the same destination but different source AS numbers.

```
<Huawei> display bgp multicast routing-table different-origin-as
BGP local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 8
      Network            NextHop        MED     LocPrf    PrefVal Path/Ogn
 *>   10.2.1.0/24        10.2.1.2        0                 0        2?
 *>                      0.0.0.0         0                 0        ?
 *>   10.2.0.0/16        10.2.1.2                          0        2?
 *>                      0.0.0.0         0                 0        ?
 *>   192.168.14.0       10.2.1.2                          0        2?
 *>                      0.0.0.0         0                 0        ?
 *>   192.168.14.1/32    10.2.1.2                          0        2?
 *>                      0.0.0.0         0                 0        ?
```

Table 9-149 Description of the display bgp multicast routing-table different-origin-as command output

Item	Description
BGP local router ID	BGP local router ID
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packet
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Path/Ogn	Displays the AS path and the Origin attribute

9.8.48 display bgp multicast routing-table flap-info

Function

The **display bgp multicast routing-table flap-info** command displays the information about MBGP route flapping.

Format

display bgp multicast routing-table flap-info [*ip-address* [*mask* [**longer-match**] | *mask-length* [**longer-match**]] | **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }]

display bgp multicast routing-table flap-info regular-expression *as-regular-expression*

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 network address.	The address is in dotted decimal notation.
mask	Specifies the mask of an IPv4 network address.	The address is in dotted decimal notation.
mask-length	Specifies the mask length of the IPv4 network address.	The value is an integer that ranges from 0 to 32.
longer-match	Indicates the longest prefix matching rules.	-
regular-expression *as-regular-expression*	Displays the statistics of route flapping that matches the AS_Path regular expression. *as-path-filter-number* specifies the AS path regular expression.	The value is a string of 1 to 80 characters.
as-path-filter *as-path-filter-number*	Displays the statistics of the route flapping for the specified AS path list. *as-path-filter-number* indicates the matched AS path list number.	The value is an integer that ranges from 1 to 256.
as-path-filter *as-path-filter-name*	Displays the statistics of the route flapping for the specified AS path list. *as-path-filter-number* indicates the matched AS path list name.	The value is a string of 1 to 51 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the information about the route flapping of MBGP.

```
<Huawei> display bgp multicast routing-table flap-info
BGP Local router ID is 10.12.12.9
 Status codes: * - valid, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
      Network          From          Flaps  Duration     Reuse  Path/Ogn
 *>   10.1.1.0/24      10.2.1.1      1      00:00:29           1?
```

Table 9-150 Description of the display bgp multicast routing-table flap-info command output

Item	Description
BGP Local router ID	BGP local router ID
Network	Network address in the MBGP routing table
From	IP address of MBGP peer from which the route is received
Flaps	Count of route flapping
Duration	Duration of the route flapping
Reuse	Reuse value
Path/Ogn	AS-Path number and the attributes of Origin

9.8.49 display bgp multicast routing-table peer

Function

The **display bgp multicast routing-table peer** command displays the routes received from or sent to a specified MBGP peer.

Format

display bgp multicast routing-table peer *peer-address* { **advertised-routes** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]] | **received-routes** [**active**] | **accepted-routes** }

display bgp multicast routing-table peer *peer-address* **received-routes** *network* [{ *mask* | *mask-length* } [**longer-prefixes** | **original-attributes**]]

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MBGP peer.	The address is in dotted decimal notation.

Parameter	Description	Value
advertised-routes	Indicates the routes sent to a specified peer.	-
Indicates the routes are not advertised.	-	
network	Specifies the IPv4 network address.	The address is in dotted decimal notation.
mask	Specifies the address mask.	The address is in dotted decimal notation.
mask-length	mask-length.	The value is an integer ranging from 0 to 32.
longer-prefixes	Use the longest match rule to select routes.	-
received-routes	Indicates the routes received from a specified peer.	-
active	Displays the active routes received from the specified peer.	-
original-attributes	Displays the original attributes of a public route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the routes sent to multicast peer 10.10.1.11.

```
<Huawei> display bgp multicast routing-table peer 10.10.1.11 advertised-routes
 BGP local router ID is 10.12.12.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
```

```
Total Number of Routes: 9
     Network          NextHop        MED        LocPrf    PrefVal Path/Ogn
 *>i  10.1.2.0/24      10.7.1.2       0          100       0      ?
 *>   10.2.1.0/24      0.0.0.0        0                    0      ?
 *>   10.7.1.0/24      0.0.0.0        0                    0      ?
 *>i  10.7.1.0/24      10.7.1.2       0          100       0      ?
 *>i  10.7.1.1/32      10.7.1.2       0          100       0      ?
 *>   10.7.1.2/32      0.0.0.0        0                    0      ?
 *>   10.10.1.0/24      0.0.0.0        0                    0      ?
```

Table 9-151 Description of the display bgp multicast routing-table peer command output

Item	Description
BGP local router ID	BGP local router ID
Total Number of Routes	Total Number of Routes
Network	Network address in the MBGP routing table
NextHop	Next hop address for forwarding packet
MED	Multi-Exit discriminator
LocPrf	Local preference
PrefVal	Preferred value of protocols
Path/Ogn	Displays the AS path and the Origin attribute

9.8.50 display bgp multicast routing-table regular-expression

Function

The **display bgp multicast routing-table regular-expression** command displays the routes that match the specified AS_Path regular expression.

Format

display bgp multicast routing-table regular-expression *as-regular-expression*

Parameters

Parameter	Description	Value
as-regular-expression	Specifies the AS_Path regular expression.	The value is a string of 1 to 80 case-sensitive characters, spaces not supported.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the routes that match the AS_Path regular expression 2.

```
<Huawei> display bgp multicast routing-table regular-expression 2
BGP local router ID is 10.13.13.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Total Number of Routes: 13
      Network            NextHop        MED      LocPrf    PrefVal Path/Ogn
 *>   10.1.2.0/24        10.2.1.2                           0       2?
 *>   10.2.1.0/24        10.2.1.2        0                  0       2?
 *>   10.7.1.0/24        10.2.1.2                           0       2?
 *>   10.7.1.1/32        10.2.1.2                           0       2?
 *>   10.7.1.2/32        10.2.1.2        0                  0       2?
 *>   10.11.12.0/24      10.2.1.2        0                  0       2?
 *>   10.11.12.1/32      10.2.1.2        0                  0       2?
```

Table 9-152 Description of the display bgp multicast routing-table regular-expression command output

Item	Description
BGP local router ID	BGP local router ID
Network	Indicates the network address in the MBGP routing table.
NextHop	Indicates the next-hop address for the packet.
MED	Indicates the MED of the route.
LocPrf	Indicates the local preference.
PrefVal	Indicates the preferred value.
Path/Ogn	Indicates the AS_Path number and the Origin attribute.

9.8.51 display bgp multicast routing-table statistics

Function

The **display bgp multicast routing-table statistics** command displays the statistics of the MBGP routes.

Format

display bgp multicast routing-table statistics

display bgp multicast routing-table peer [*ipv4-address*] { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
peer *ipv4-address*	Displays the number of routes with a specified peer address.	The value is in dotted decimal notation.
advertised-routes	Displays the number of routes advertised to a specified peer.	-
received-routes	Displays the number of routes received from a specified peer.	-
active	Displays the number of active routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display statistics about routes in the MBGP routing table.

```
<Huawei> display bgp multicast routing-table statistics
Total Number of Routes: 50
```

Table 9-153 Description of the display bgp multicast routing-table statistics command output

Item	Description
Total Number of Routes	Indicates the total number of routes in the MBGP routing table.

9.8.52 display bgp multicast update-peer-group

Function

The **display bgp multicast update-peer-group** command displays information about MBGP update-groups.

Format

display bgp multicast update-peer-group [**index** *update-group-index*]

Parameters

Parameter	Description	Value
index *update-group-index*	Specifies the index of an update-group.	The value is an integer ranging from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the index of an update-group is specified, the command will display detailed information about the specified update-group.

Example

Display information about MBGP update-groups.

```
<Huawei> display bgp multicast update-peer-group
 The Multicast instance's update peer group number : 1
 Keep buffer update peer group number : 0
 BGP Version : 4

 Group ID : 0
 Group Type : external
 Addr Family : IPv4-MLC
 AdvMinTimeVal : 30
 Total Peers : 1
 Leader Peer : 192.168.1.2
 Peers List : 192.168.1.2
```

Table 9-154 Description of the display bgp multicast update-peer-group command output

Item	Description
The Multicast instance's update peer group number	Indicates the number of update-groups in the instance.

Item	Description
Keep buffer update peer group number	Number of packets in update-groups saved in the batch buffer.
BGP Version	Indicates the BGP version.
Group ID	Indicates the ID of the update-group.
Group Type	Indicates the type of the update-group, which can be one of the following: ● external: indicates an EBGP update-group. ● internal: indicates an IBGP update-group. ● external-confed: indicates an EBGP update-group in the confederation. ● internal-confed: indicates an IBGP update-group in the confederation. ● unknown: indicates an update-group of an unknown type.
Addr Family	Indicates the address family.
AdvMinTimeVal	Indicates the minimum interval for sending Update packets with the same route prefix.
Total Peers	Indicates the total number of peers in an update-group.
Leader Peer	Indicates the representative of an update-group.
Peers List	Indicates a list of peers.

9.8.53 display bgp network

Function

The **display bgp network** command displays the routes imported into the BGP routing table by using the **network** command.

Format

display bgp network

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **network**

display bgp ipv6 network

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **network**

display bgp multicast network

Parameters

Parameter	Description	Value
vpnv4	Displays the VPNv4 routes that are advertised by using the **network** command.	-
all	Displays all the VPNv4 routes that are advertised by using the **network** command.	-
vpn-instance *vpn-instance-name*	Displays the routes of a specified VPN instance that are advertised by using the **network** command.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6	Displays the IPv6 routes advertised by BGP.	-
vpnv6	Displays the VPNv6 routing information advertised by BGP through the **network** command.	-
multicast	Displays the routing information advertised by Multicast BGP (MBGP) through the **network**command.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

BGP cannot discover routes by itself. Run the **network (BGP)** command and the **import-route (BGP)** command to import routes from other protocols, such as IGP routes or static routes, to the BGP routing table.

The **display bgp network** command displays the routing information advertised by BGP through the **network (BGP)** command.

Precautions

BGP has multiple address families and the routing information about each address family is isolated from each other. The routing information about address families

 Copyright © Huawei Technologies Co., Ltd.

advertised by BGP through the **network (BGP)** command can be displayed by specifying different parameters.

If no parameter is specified, the **display bgp network** command displays the routing information about the IPv4 unicast address family advertised by BGP through the **network (BGP)** command.

Example

Display information about routes that are imported using the **network** command.

```
<Huawei> display bgp network
  BGP Local Router ID is 10.1.1.9
  Local AS Number is 10(Public)
  Network          Mask            Route-policy
  10.2.0.0         255.255.0.0
  10.0.0.0         255.0.0.0       Policy1
  10.4.4.0         255.255.255.0
```

Table 9-155 Description of the display bgp network command output

Item	Description
Local AS Number is	Indicates the local AS number.
Network	Indicates the locally-advertised network address.
Mask	Indicates the mask of the network address.
Route-policy	Indicates the used routing policy.

Display information about BGP VPNv4 routes that are imported using the **network** command.

```
<Huawei> display bgp vpnv4 all network
  BGP Local Router ID is 10.2.2.9
  Local AS Number is 100
 VPN-Instance vrf1, Router ID 10.2.2.9:
  Network          Mask            Route-policy
  10.4.4.4         255.255.255.255
 VPN-Instance vrf2, Router ID 10.2.2.9:
  Network          Mask            Route-policy
  10.5.5.5         255.255.255.255
```

Table 9-156 Description of the display bgp vpnv4 all network command output

Item	Description
VPN-Instance	Name of the VPN instance
Router ID	Router ID of the local BGP router.

Display IPv6 routes advertised by BGP.

```
<Huawei> display bgp ipv6 network
```

```
BGP Local Router ID is 10.5.5.5
Local AS Number is 100(PublicV6)
Network         Prefix          Route-policy
FC00:0:0:100::  64
FC00:0:0:200::  64
```

Table 9-157 Description of the display bgp ipv6 network command output

Item	Description
BGP Local Router ID	Indicates the ID of the local BGP device. The ID is in the same format as an IPv4 address.
Local AS Number	Indicates the local AS number.
Prefix	Indicates the network address mask advertised by the local BGP device.

9.8.54 display bgp paths

Function

The **display bgp paths** command displays the AS_Path information of BGP routes.

Format

display bgp paths [*as-regular-expression*]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*]

display bgp ipv6 paths [*as-regular-expression*]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*]

display bgp multicast paths [*as-regular-expression*]

display bgp mdt { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*]

Parameters

Parameter	Description	Value
as-regular-expression	Specifies the regular expression used to match the AS_Path information.	The name is a string of 1 to 80 characters.
vpnv4	Displays the AS_Path information of the routes of a VPNv4 instance.	-

Parameter	Description	Value
vpnv6	Displays the path attributes of BGP Virtual Private Network version 6 (VPNv6).	-
all	Displays the AS_Path information of all VPNv4 routes.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6	Displays the path attributes of IPv6-BGP routes in the local BGP database.	-
multicast	Displays the path attributes of Multicast BGP (MBGP).	-
mdt	Displays the path attributes of Multicast Distribution Tree (MDT).	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bgp paths** command displays the path attributes of BGP stored in the system.

BGP usually has a large number of path attributes. The **display bgp paths** command displays a lot of BGP path information for viewing. After configuring *as-regular-expression*, the **display bgp paths** command displays only the path attributes of BGP that match *as-regular-expression*. For details on a regular expression, see "Filtering Command Outputs" in the *Huawei AR Series Access Routers - Configuration Guide - Basic Configuration*.

Precautions

BGP has a number of address families and the path attributes of BGP in each address family is stored independently. By default, the **display bgp paths** command displays only the path attributes of BGP in the IPv4 unicast address family. The path attributes of BGP in other address families can be displayed by specifying address family parameters.

Example

Display the AS_Path information.

```
<Huawei> display bgp paths

 Total number of routes of IPv4-family for vpn-instance _public_: 6
 Total Number of Paths: 1

 Address          Refcount        MED  Path/Origin
 1282430404              6          0  N?
```

Table 9-158 Description of the display bgp paths command output

Item	Description
Address	Indicates the address of the route in the local database, in hexadecimal notation.
Refcount	Indicates the number of times that the route is referenced.
MED	Indicates the MED of the route.
Path	Indicates the list of ASs through which the packet has to pass through.
Origin	Indicates the origin of the route.

Display information about BGP4+ paths.

```
<Huawei> display bgp ipv6 paths

Total Number of Routes: 6
Total Number of Paths: 4

   Address       Refcount  MED        Path/Origin
   0x41036F0      1        0           i
   0x4103758      1        0           i
   0x41037C0      1        0           i
   0x41038F8      3        0           200i
```

Display information about BGP4+ paths of VPN instance named vpn1.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 paths

 Total number of routes of IPv6-family for vpn-instance vpn1: 2
 Total Number of Paths: 3

   Address       Refcount  MED        Path/Origin
   0xF9E4120      1                   100?
   0xF9E42EC      1        0          65410?
   0xF9E40C4      1        0           ?
```

Display the BGP4+ paths, including AS_Path 65420, of VPN instance named vpn1.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 paths 65420*

 Total number of routes of IPv6-family for vpn-instance vpn1: 1
```

```
  Address      Refcount  MED        Path/Origin
  0xF9E42EC     1         0          65420?
```

Display the information about MBGP paths.

```
<Huawei> display bgp multicast paths 1

Total Number of Routes: 17
Total Number of Paths: 1

  Address        Refcount   MED       Path/Origin
  0x54169A4       17         0         1?
```

9.8.55 display bgp peer

Function

The **display bgp peer** command displays information about BGP peers.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **peer** [{ *group-name* | *ipv4-address* } **log-info** | [*ipv4-address*] **verbose**]

display bgp vpnv6 vpn-instance *vpn-instance-name* **peer** [{ *group-name* | *ipv6-address* } **log-info** | [*ipv6-address*] **verbose**]

display bgp vpnv6 all peer [[*ipv4-address*] **verbose**]

display bgp vpnv4 all peer [[*ipv4-address*] **verbose**]

display bgp ipv6 peer [**verbose**]

display bgp ipv6 peer *ipv6-address* { **log-info** | **verbose** }

display bgp ipv6 peer *ipv4-address* **verbose**

display bgp evpn peer [[*ipv4-address*] **verbose**]

display bgp mdt all peer [[*ipv4-address*] **verbose**]

display bgp multicast peer [[*ipv4-address*] **verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer to be displayed. To display IPv6 Provider Edge (6PE) peers, run the **display bgp ipv6 peer** *ipv4-address* **verbose** command.	It is in dotted decimal notation.
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
log-info	Indicates to display log information of the specified peer.	-
verbose	Indicates to display detailed peer information.	-
vpnv4	Indicates to display information about peers in a VPNv4 instance.	-
all	Indicates to display information about peers in all VPNv4 instances.	-
ipv6	Displays IPv6 peers.	-
ipv6-address	Specifies the IPv6 address of a peer to be displayed.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
evpn	Displays information about EVPN peer groups.	-
vpnv6	Displays information about BGP Virtual Private Network version 6 (VPNv6) peers.	-
mdt	Displays information about peers in the BGP-Multicast Distribution Tree (MDT) view.	-
multicast	Displays Multicast BGP (MBGP) peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bgp peer** command displays information about a BGP peer. You can implement the following operations based on the command output:

- To check the status of BGP connections
- To check information about a BGP peer
- To check whether a BGP peer is successfully configured using the **peer as-number** command
- To check whether a BGP peer is successfully deleted using the **undo peer as-number** command

Precautions

BGP has multiple address families. By default, the **display bgp peer** command displays information about BGP peers in IPv4 unicast address family only. If you want to view information about BGP peers in another address family, you need to specify its address family parameter.

To view detailed information about a BGP peer, such as information about BGP timers, the number of sent and received routes, capacities supported, the number of sent and received BGP messages, and enabled functions, specify **verbose** in the command.

If **log-info** is specified in the command, log information about a BGP peer is displayed, including information about BGP peer flapping.

Example

Display peer information.

```
<Huawei> display bgp peer
 Status codes: * - Dynamic
 BGP Local router ID : 10.2.3.4
 local AS number : 10
 Total number of peers : 2
 Peers in established state : 1

 Total number of dynamic peers : 1
  Peer        V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  10.1.1.1    4   100        0        0     0 00:00:07        Idle       0
  10.2.5.6    4   200       32       35     0 00:17:49 Established       0
```

Table 9-159 Description of the display bgp peer command output

Item	Description
Status codes: * - Dynamic	Status code. If the value starts with an asterisk (*), the peer is a dynamic peer. Currently, the value can only be *** - Dynamic**.
BGP Local router ID	Indicates the ID of the BGP local router.

Item	Description
local AS number	Indicates the local AS number.
Total number of peers	Indicates the number of the peer.
Peers in established state	Indicates the number of the peer in established state.
Total number of dynamic peers	Total number of dynamic BGP peers.
Peer	Indicates the IP address of the peer.
V	Indicates the BGP version used on the peer.
AS	Indicates the AS number.
MsgRcvd	Indicates the number of received messages.
MsgSent	Indicates the number of sent messages.
OutQ	Indicates the message to be sent to the specified peer.
Up/Down	Indicates the period of time during which a BGP session keeps the current state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of the peer: ● Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. ● No neg: The capabilities of the BGP peer's address family have not been negotiated. ● Idle(Admin): indicates that the peer relationship is shut down initiatively and no attempt is made to establish the neighbor relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. ● Idle(Ovlmt): indicates that the peer relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP peer relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP peer relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP peer relationship will not be reestablished. ● Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for the other Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established. ● Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
PrefRcv	Indicates the number of route prefixes sent from the peer.

Display detailed information about the peer 10.2.2.9.

```
<Huawei> display bgp peer 10.2.2.9 verbose

    BGP Peer is 10.2.2.9,  remote AS 100
    Type: IBGP link
    Dynamic peer
    Belong to peer-group: gp1
    Belong to listen-net: 10.2.2.0 24
    BGP version 4, Remote router ID 10.1.1.1
    Update-group ID: 1
    BGP current state: Established, Up for 00h57m53s
    BGP current event: RecvKeepalive
    BGP last state: Established
    BGP Peer Up count: 1
    Received total routes: 0
    Received active routes total: 0
    Received mac routes: 0
    Advertised total routes: 2
    Port: Local - 42796        Remote - 179
    Configured: Connect-retry Time: 32 sec
    Configured: Min Hold Time: 0 sec
    Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
    Received  : Active Hold Time: 180 sec
    Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
    Peer optional capabilities:
    Peer supports bgp multi-protocol extension
    Peer supports bgp route refresh capability
```

```
        Peer supports bgp 4-byte-as capability
        Address family IPv4 Unicast: advertised and received
Received:
                Total messages              60
                Update messages              1
                Open messages                1
                KeepAlive messages           58
                Notification messages        0
                Refresh messages             0
Sent:
                Total messages              61
                Update messages              2
                Open messages                1
                KeepAlive messages           58
                Notification messages        0
                Refresh messages             0
Authentication type configured: None
Last keepalive received: 2012/03/06 19:17:37
Last keepalive sent    : 2012/03/06 19:17:37
Last update    received: 2012/03/06 19:17:43
Last update    sent    : 2012/03/06 19:17:37

Minimum route advertisement interval is 15 seconds
Optional capabilities:
Route refresh capability has been enabled
4-byte-as capability has been enabled
Listen-only has been configured
Peer's BFD has been enabled
Peer Preferred Value: 0
Routing policy configured:
No routing policy is configured
```

Table 9-160 Description of the display bgp peer verbose command output

Item	Description
Type	Indicates the BGP link type, which can be IBGP or EBGP.
Dynamic peer	The peer is a dynamic BGP peer.
Belong to peer-group	Peer group to which the peer belongs.
Belong to listen-net	Network segment to which the dynamic peer belongs.
BGP version	Indicates the BGP version.
remote router ID	Indicates the router ID of the peer.
Update-group ID	Indicates the ID of the update-group to which the peer belongs.

Item	Description
BGP current state	Current state of BGP: ● Idle: indicates that BGP denies any request of entering. This is the initiatory status of BGP. Upon receiving a Start event, BGP initiates a TCP connection to the remote BGP peer, starts the ConnectRetry Timer with the initial value, detects a TCP connection initiated by the remote BGP peer, and changes its state to Connect. ● No neg: The capabilities of the BGP peer's address family have not been negotiated. ● Idle(Admin): indicates that the peer relationship is shut down initiatively and no attempt is made to establish the neighbor relationship. If the **peer ignore** command is configured or the peer is set to the Down state through the MIB, the neighbor is in the Idle (Admin) state. ● Idle(Ovlmt): indicates that the peer relationship is interrupted because the number of routes exceeds the upper threshold. After a BGP peer relationship is interrupted due to the running of the **peer route-limit** command, the status of the BGP peer relationship is displayed as Idle(Ovlmt). If the **reset bgp** command is not run, the BGP peer relationship will not be reestablished. ● Connect: indicates that BGP waits for the TCP connection to be set up before it determines whether to perform other operations. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the TCP connection fails, BGP restarts the ConnectRetry Timer

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	with the initial value, continues to detect a TCP connection initiated by the remote peer, and changes its state to Active. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value, initiates a TCP connection to the remote BGP peer, and stays in the Connect state. ● Active: indicates that BGP tries to set up a TCP connection. This is the intermediate status of BGP. – If the TCP connection succeeds, BGP stops the ConnectRetry Timer, sends an Open message to the remote peer, and changes its state to OpenSent. – If the ConnectRetry Timer has expired before a TCP connection is established, BGP restarts the timer with the initial value and changes its state to Connect. – If BGP initiates a TCP connection with an unknown IP address, the TCP connection fails. When this occurs, BGP restarts the ConnectRetry Timer with the initial value and stays in the Active state. ● OpenSent: indicates that BGP has sent one Open message to its peer and waits for the other Open message from the peer. – If there are no errors in the Open message received, BGP changes its state to OpenConfirm. – If there are errors in the Open message received, BGP sends a Notification message to the remote peer and changes its state to Idle. – If the TCP connection fails, BGP restarts the ConnectRetry Timer with the initial value, continues

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	to detect a TCP connection initiated by the remote peer, and changes its state to Active. ● OpenConfirm: indicates that BGP waits for a Notification message or a Keepalive message. – If BGP receives a Notification message, or the TCP connection fails, BGP changes its state to Idle. – If BGP receives a Keepalive message, BGP changes its state to Established. ● Established: indicates that BGP peers can exchange Update, Notification and Keepalive packets. – If BGP receives an Update or a Keepalive message, its state stays in Established. – If BGP receives a Notification message, BGP changes its state to Idle.
BGP current event	Indicates the current BGP event.
BGP last state	Indicates the last BGP status, which may be Idle, Connect, Active, OpenSent, OpenConfirm, or Established.
BGP Peer Up count	Indicates the flapping count of a BGP peer in a specified period of time.
Received total routes	Indicates the number of received route prefixes
Received active routes total	Indicates the number of received active route prefixes.
Advertised total routes	Indicates the number of sent route prefixes.
Port	Indicates the port number. ● Local: indicates the local port number, which is always 179. BGP uses TCP at the transport layer. ● Remote: indicates the port number used on the peer.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Configured	Indicates locally configured timers. ● Connect-retry Time: indicates the ConnectRetry interval for a BGP peer or peer group, in seconds. When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires. ● Min Hold Time: indicates the minimum Holdtime configured on the local device, in seconds. ● Active Hold Time: indicates the hold time. If BGP does not receive any Keepalive message from the peer in the hold time, BGP considers that the peer is Down and then instructs other peers to remove the routes that are sent from the peer. ● Keep Alive Time: indicates the interval for sending Keepalive messages to the peer. BGP peers send Keepalive messages to each other periodically to maintain their relationships.
Received : Active Hold Time	Indicates the hold time on the peer.
Received mac routes	Number of MAC routes received.
Negotiated : Active Hold Time	Indicates the hold time agreed between the BGP peers after capability negotiation.
Address family IPv4 Unicast	Indicates the IPv4 unicast address family.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Received	Indicates the number of packets received from a peer. ● Total: indicates the total number of messages received from a peer. ● Update messages: indicates the number of Update messages received from a peer. ● Open messages: indicates the number of Open messages received from a peer. ● KeepAlive messages: indicates the number of Keepalive messages received from a peer. ● Notification messages: indicates the number of Notification messages received from a peer. ● Refresh messages: indicates the number of route-refresh messages received from a peer.
Sent	Indicates the number of messages sent to a peer. ● Total: indicates the total number of messages sent to a peer. ● Update messages: indicates the number of Update messages sent to a peer. ● Open messages: indicates the number of Open messages sent to a peer. ● KeepAlive messages: indicates the number of Keepalive messages sent to a peer. ● Notification messages: indicates the number of Notification messages sent to a peer. ● Refresh messages: indicates the number of route-refresh messages sent to a peer.
Authentication type configured	Authentication type configured

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last keepalive received	Indicates the time when the Keepalive packet is received last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
Last keepalive sent	Indicates the time when the Keepalive packet is sent last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last update received	Indicates the time when the Update packet is received last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
Last update sent	Indicates the time when the Update packet is sent last time. It can be in the following formats: ● YYYY/MM/DD HH:MM:SS ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST ● YYYY/MM/DD HH:MM:SS UTC ±HH:MM ● YYYY/MM/DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is set through the **clock timezone** command; DST indicates that the daylight saving time is set through the **clock daylight-saving-time** command.
Minimum route advertisement interval is 15 seconds	Indicates the minimum interval between route advertisements. ● The minimum interval for advertising EBGP routes is 30 seconds. ● The minimum interval for advertising IBGP routes is 15 seconds.
Optional capabilities	(Optional) Indicates the peer-supported capabilities.
Route refresh capability has been enabled	Indicates that route refreshing has been enabled.
4-byte-as capability has been enabled	4-byte-As is enabled

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Listen-only has been configured	Indicates that only connection requests are snooped and no connections will be initiated proactively.
Peer optional capabilities	Capability supported by peers (optional). ● Peer supports bgp multi-protocol extension: Indicates the BGP peer supports BGP multi-protocol extension. ● Peer supports bgp route refresh capability: Indicates the BGP peer supports BGP route refresh. ● Peer supports bgp 4-byte-as capability: Indicates the BGP peer supports BGP 4-byte AS numbers.
Peer Preferred Value	Indicates the preferred value of the peer.
Routing policy configured	Indicates the configured routing policy.
Peer's BFD has been enabled	Indicates that BFP has been enabled on the peer.

Display log information on BGP peer 10.1.1.2.

```
<Huawei> display bgp peer 10.1.1.2 log-info
Peer : 10.1.1.2
 Date/Time     : 2011/13/06 11:53:21
 State         : Up
 Date/Time     : 2011/13/06 11:53:09
 State         : Down
 Error Code    : 6(CEASE)
 Error Subcode : 4(Administrative Reset)
 Notification  : Receive Notification
 Date/Time     : 2011/13/06 10:34:05
 State         : Up
```

Table 9-161 Description of the display bgp peer 1.1.1.2 log-info command output

Item	Description
Error Code	Error code.
Error Subcode	Error subcode.
Notification	Notification packet sent or received by a peer.

Display information about the BGP peer of the VPN instance vrf1.

```
<Huawei> display bgp vpnv4 vpn-instance vrf1 peer

 Status codes: * - Dynamic
 BGP local router ID : 10.1.1.9
 Local AS number : 100
 VPN-Instance vrf1, router ID 10.1.1.1:
 Total number of peers : 1                 Peers in established state : 1

 Total number of dynamic peers : 1
  Peer        V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

 *10.1.1.1    4 65410      207      192     0 02:59:49 Established       1
```

Display detailed information about the BGP peer of the VPN instance vpna.

```
<Huawei> display bgp vpnv4 vpn-instance vpna peer verbose

         BGP Peer is 10.1.1.1,  remote AS 200
         Type: EBGP link
         Dynamic peer
         Belong to peer-group: gp2
         Belong to listen-net: 10.1.2.0 24
         BGP version 4, remote router ID 10.1.1.1

         Update-group ID: 1
         BGP current state: Established, Up for   03h01m22s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         BGP Peer Up count: 1
                 Received total routes: 0
                 Received active routes total: 0
                 Received mac routes: 0
                 Advertised total routes: 3
         Port:  Local - 3722     Remote - 179
         Configured: Connect-retry Time: 32 sec
         Configured: Min Hold Time: 0 sec
         Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec
         Peer optional capabilities:
         Peer supports bgp multi-protocol extension
         Peer supports bgp route refresh capability
         Peer supports bgp 4-byte-as capability
         Address family IPv4 Unicast: advertised and received

 Received: Total 76 messages
                 Update messages              0
                 Open messages                5
                 KeepAlive messages          71
                 Notification messages        0
                 Refresh messages             0

 Sent: Total 91 messages
                 Update messages              0
                 Open messages               10
                 KeepAlive messages          77
                 Notification messages        4
                 Refresh messages             0
 Authentication type configured: None
 Last keepalive received: 2012/03/06 19:17:37
 Last keepalive sent    : 2012/03/06 19:17:37
 Last update    received: 2012/03/06 19:17:43
 Last update    sent    : 2012/03/06 19:17:37
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Minimum route advertisement interval is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 Peer Preferred Value: 0
```

```
Routing policy configured:
No routing policy is configured
```

Display information about IPv6 peers.

```
<Huawei> display bgp ipv6 peer

 BGP Local router ID : 10.0.0.1
 local AS number : 100
  Total number of peers : 1                 Peers in established state : 1

  Peer            V    AS  MsgRcvd  MsgSent  OutQ  Up/Down       State PrefRcv

  2001:db8:1::1   4   200       17       19     0 00:09:59 Established       3
```

Display information about IPv6 peers.

```
<Huawei> display bgp ipv6 peer fc00:0:0:2001::1 verbose
        BGP Peer is 2001:db8:1::1,  remote AS 1
        Type: EBGP link
        BGP version 4, remote router ID 10.1.1.1

        Update-group ID: 1
        BGP current state: Established, Up for 00h00m59s
        BGP current event: RecvKeepalive
        BGP last state: OpenConfirm
        BGP Peer Up count: 2
        Received total routes: 0
        Received active routes total: 0
        Received mac routes: 0
        Advertised total routes: 0
        Port:  Local - 179      Remote - 49153
        Configured: Connect-retry Time: 32 sec
        Configured: Min Hold Time: 0 sec
        Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
        Received  : Active Hold Time: 180 sec
        Negotiated: Active Hold Time: 180 sec   Keepalive Time:60 sec
        Peer optional capabilities:
        Peer supports bgp multi-protocol extension
        Peer supports bgp route refresh capability
        Peer supports bgp 4-byte-as capability
        Address family IPv6 Unicast: advertised and received

 Received: Total 76 messages
                Update messages              0
                Open messages                5
                KeepAlive messages          71
                Notification messages        0
                Refresh messages             0

 Sent: Total 91 messages
                Update messages              0
                Open messages               10
                KeepAlive messages          77
                Notification messages        4
                Refresh messages             0
 Authentication type configured: None
 Last keepalive received: 2012/03/06 19:17:37
 Last keepalive sent    : 2012/03/06 19:17:37
 Last update    received: 2012/03/06 19:17:43
 Last update    sent    : 2012/03/06 19:17:37
 Minimum route advertisement interval is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 4-byte-as capability has been enabled
 listen-only has been configured
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured
```

Related Topics

9.8.101 peer as-number

9.8.56 display bgp peer orf ip-prefix

Function

The **display bgp peer orf ip-prefix** command displays the prefix-based Outbound Routes Filter (ORF) received by a device from a specified peer.

Format

display bgp peer *ipv4-address* **orf ip-prefix**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a device successfully negotiates the ORF capability with its peer, this command can be used to display information about the prefix-based ORF received from the peer.

Example

Display the prefix-based ORF received by a device from a peer at 10.1.1.2.

```
<Huawei> display bgp peer 10.1.1.2 orf ip-prefix
Total number of ip-prefix received: 1
 Index  Action  Prefix          MaskLen  MinLen  MaxLen
 10     Permit  10.4.4.0        24       32      32
```

Table 9-162 Description of the display bgp peer orf ip-prefix command output

Item	Description
Index	Indicates the index of an IP prefix list.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Action	Indicates the action associated with an IP prefix list, which can be one of the following: ● deny ● permit
Prefix	Indicates an IP prefix.
MaskLen	Indicates the mask length of an IP prefix.
MinLen	Indicates the minimum mask length of an IP prefix.
MaxLen	Indicates the maximum mask length of an IP prefix.

9.8.57 display bgp resource

Function

The **display bgp resource** command displays statistics about BGP specification information.

Format

display bgp resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check statistics about BGP specification information, run the **display bgp resource** command. This command displays only the total number of supported BGP peer sessions, including the numbers of various configured sessions.

Example

Display statistics about BGP specification information.

```
<Huawei> display bgp resource

 BGP Peer session support total number : 500
```

```
Capacity Statistics     Used Number

BGP Peer Session          3
IBGP Peer Session         3
EBGP Peer Session         0
```

Table 9-163 Description of the **display bgp resource** command output

Item	Description
BGP Peer session support total number	Maximum number of BGP peer sessions that are supported.
Capacity Statistics	BGP peer session type.
Used Number	Number of currently configured peer sessions.
BGP Peer Session	Total number of currently configured BGP peer sessions.
IBGP Peer Session	Number of IBGP peer sessions, including confederation IBGP and common IBGP peer sessions.
EBGP Peer Session	Number of EBGP peer sessions, including confederation EBGP and common EBGP peer sessions.

9.8.58 display bgp routing-table

Function

The **display bgp routing-table** command displays information about BGP routes. Information about specified routes can be displayed by specifying different parameters.

Format

display bgp routing-table [**verbose** | *ipv4-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

display bgp routing-table [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp routing-table regular-expression *as-regular-expression*

display bgp routing-table community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp routing-table community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp routing-table peer *ipv4-address* { **advertised-routes** [*ipv4-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]] | **received-routes** [**active**] }

display bgp routing-table peer *ipv4-address* **received-routes** *ipv4-address* [{ *mask* | *mask-length* } [**longer-prefixes** | **original-attributes**]]

display bgp routing-table peer *ipv4-address* **accepted-routes**

display bgp routing-table time-range *start-time end-time*

Parameters

Parameter	Description	Value
verbose	Displays detailed information about BGP routes.	-
ipv4-address	Specifies an IPv4 network address.	The value is in dotted decimal notation.
mask | *mask-length*	Specifies a mask in dotted decimal notation or the mask length.	-
longer-prefixes	Matches any route whose prefix mask is longer than the specified length.	-
as-path-filter	Displays the routes that match a specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
cidr	Displays Classless InterDomain Routing (CIDR) information.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
different-origin-as	Displays routes that have the same destination address but different source AS numbers.	-
community-filter	Displays the routes that match a specified BGP community filter.	-
community-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 characters. The string cannot be all numbers.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	-
aa:*nn*	Specifies the community number.	-
internet	Displays the matching routes that can be sent to any peer.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-
no-export	Displays the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
peer *ipv4-address*	Displays routes of a specified peer.	-
advertised-routes	Displays the routes advertised to a specified peer.	-
received-routes	Displays the routes received from a specified peer.	-
active	Displays the active routes received from a specified peer.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
original-attributes	Displays the original attributes of a public route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
accepted-routes	Displays the routes that are received from the peer and filtered through a routing policy.	-
time-range *start-time end-time*	Displays BGP routes that flap within the specified time period. For example, the value 0d0h5m0s of *start-time* indicates five minutes before the current time. The value 0d0h10m0s of *end-time* indicates 10 minutes before the current time. All BGP routes with the Keepalive time in the range of 5 to 10 minutes are displayed.	The value ranges of *start-time* and *end-time* both are 0d0h0m0s-10000d23h59m59s.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about specified routes can be displayed by specifying different parameters.

The **display bgp routing-table** command is used to display active and inactive BGP routes on the public network.

Example

Display all BGP routing information.

```
<Huawei> display bgp routing-table
```

```
BGP Local router ID is 10.1.1.2
Status codes: * - valid, > - best, d - damped, h - history,
              i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 4
     Network          NextHop        MED        LocPrf    PrefVal Path/Ogn
*    10.1.1.0/24      10.1.1.1       0                    0       100?
*    10.1.1.2/32      10.1.1.1       0                    0       100?
*>   10.1.1.0/24      10.1.1.1       0                    0       100?
*>   10.1.1.0/24      10.1.1.1       0                    0       100?
```

Display routes with the community attribute.

```
<Huawei> display bgp routing-table community

BGP Local router ID is 10.1.1.2
Status codes: * - valid, > - best, d - damped, h - history,
              i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete
Total Number of Routes: 4
     Network          NextHop        MED        LocPrf    PrefVal Community
*    10.1.1.0/24      10.1.1.1       0                    0       no-export
*    10.1.1.2/32      10.1.1.1       0                    0       no-export
*>   10.1.1.0/24      10.1.1.1       0                    0       no-export
*>   10.1.1.0/24      10.1.1.1       0                    0       no-export
```

Table 9-164 Description of the display bgp routing-table command output

Item	Description
BGP Local Router ID	Router ID of the local BGP device.
Network	Indicates the network address in the BGP routing table.
NextHop	Indicates the next-hop address for the packet.
MED	Indicates the MED of the route.
LocPrf	Indicates the local preference.
PrefVal	Indicates the preferred value.
Path/Ogn	Indicates the AS_Path number and the origin attribute.
Community	Indicates the community attribute information.

Display the detailed information of the specified routes.

```
<Huawei> display bgp routing-table 10.1.1.1
 BGP local router ID : 10.2.3.107
 Local AS number : 100
 Paths:   1 available, 1 best, 1 select
 BGP routing table entry information of 10.1.1.1/32:
 Imported route.
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 0d00h01m33s
 Direct Out-interface: Ethernet3/0/1
 Original nexthop: 10.1.1.2
```

```
Qos information : 0x0
AS-path 200, origin incomplete, MED 0, pref-val 0, valid, external, best, select, pre 255
Advertised to such 1 peers:
   10.1.1.2
```

Table 9-165 Description of the display bgp routing-table command output

Item	Description
Local AS Number	Local AS number.
Paths	Indicates the route selection result.
BGP routing table entry information of	Routing entry information.
Imported route	Routes imported to BGP using the **import-route** command.
From	IP address of an advertising device.
Route Duration	Route duration.
Direct Out-interface	Indicates the directly-connected interface.
Original nexthop	Original next hop.
Qos information	QoS information.
AS-path	AS_Path attribute. **Nil** indicates that the attribute value is null.
origin	Origin attribute of a BGP route: ● IGP: indicates that the origin attribute of a route added to the BGP routing table by using the **network** command is IGP. ● EGP: indicates that the origin attribute of a route obtained by using EGP is EGP. ● Incomplete: indicates that the origin attribute of a route whose source is unknown is Incomplete. For example, the origin attribute of the routes imported by using the **import-route** command is Incomplete.
valid	Valid route.
external	External route.
best	Optimal route.
select	Preferred route.
Pre	BGP route preference.

Display detailed information about the specified invalid BGP routes.

```
<Huawei> display bgp routing-table 1.1.1.1
 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Paths:   2 available, 0 best, 0 select
 BGP routing table entry information of 1.1.1.1/32:
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h01m31s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 20.1.1.2
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP
unreachable
 Not advertised to any peer yet
 BGP routing table entry information of 1.1.1.1/32:
 From: 2.2.2.2 (10.1.1.2)
 Route Duration: 00h00m51s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface:
 Original nexthop: 20.1.1.2
 Qos information : 0x0
 AS-path 200, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for IP
unreachable
 Not advertised to any peer yet
```

Table 9-166 Description of the **display bgp routing-table** command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Paths	Information about paths of BGP routes.
BGP routing table entry information of 1.1.1.1/32	The following information is about 1.1.1.1/32 routing entries.
From	IP address of the router that sends the route. 10.1.1.1 is the IP address of the source interface of the peer with which the BGP connection is established, and 2.2.2.2 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	IP iterated next hop.
Relay IP Out-Interface	IP iterated outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information.
AS-path 200	AS_Path attribute.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
internal	The BGP route is an internal route.
pre 255	The BGP route preference is 255.
invalid for IP unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to be iterated to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to be iterated to a tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

9.8.59 display bgp routing-table dampened

Function

The **display bgp routing-table dampened** command displays BGP dampened routes.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table dampened**

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table** [**statistics**] **dampened**

display bgp ipv6 routing-table [**statistics**] **dampened**

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table** [**statistics**] **dampened**

Parameters

Parameter	Description	Value
vpnv4	Displays the BGP routes of a VPNv4 instance.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
statistics	Displays the statistics of dampened routes.	-
ipv6	Displays all dampened IPv6 routes.	-
vpnv6	Displays the BGP routes of a VPNv6 instance.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the Route Distinguisher dampened BGP routes.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the length of the destination address mask of an IPv4 route is the same as that of its natural mask, the mask length is not displayed after the command is run.

Example

Display BGP dampened routes.

```
<Huawei> display bgp routing-table dampened


 BGP Local router ID is 10.1.41.102
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 8
     Network            From            Reuse      Path/Origin
  d  10.6.244.0/23      10.10.41.247      01:06:25  65534 4837 174 11096 6356i
  d  10.17.79.0/24      10.10.41.247      01:06:25  65534 837 3356 23504 29777i
  d  10.17.110.0/24     10.10.41.247      01:06:25  65534 837 3356 23504 29777i
  d  10.57.144.0/20     10.10.41.247      01:06:25  65534 4837 10026 9924 18429,18429i
  d  10.76.216.0/24     10.10.41.247      01:06:25  65534 4837 701 26959i
  d  10.78.142.0/24     10.10.41.247      01:06:25  65534 4837 701 26959i
  d  10.115.136.0/23    10.10.41.247      01:06:25  65534 4837 701 26956i
  d  10.243.170.0/24    10.10.41.247      01:06:25  65534 4837 701 26959i
```

Table 9-167 Description of the display bgp routing-table dampened command output

Item	Description
Network	Indicates the network address in the BGP routing table.
From	Indicates the IP address of the peer that receives the routes.
Reuse	Indicates the reuse value (in seconds).
Path/Origin	Indicates the AS_Path number and the Origin attribute.

Display IPv6 dampened routes in the BGP routing table.

```
<Huawei> display bgp ipv6 routing-table dampened



 BGP Local router ID is 10.0.0.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale,
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 4
  d  Network : FC00:0:0:1:1::                PrefixLen : 48
     From    : FC00:0:0:1::2:2               Reuse     : 01:06:26
     Path/Ogn: 65001?

  d  Network : FC00:0:0:1:2::                PrefixLen : 48
     From    : FC00:0:0:1::2:2               Reuse     : 01:06:26
     Path/Ogn: 65001?

  d  Network : FC00:0:0:1:3::                PrefixLen : 48
     From    : FC00:0:0:1::2:2               Reuse     : 01:06:26
     Path/Ogn: 65001?
```

```
 d  Network : FC00:0:0:1:4::                    PrefixLen : 48
    From    : FC00:0:0:1::2:2                   Reuse     : 01:06:26
    Path/Ogn: 65001?
```

Table 9-168 Description of the **display bgp ipv6 routing-table dampened** command output

Item	Description
PrefixLen	Prefix length

Related Topics

9.8.20 dampening

9.8.60 display bgp routing-table dampening parameter

Function

The **display bgp routing-table dampening parameter** command displays configured BGP route dampening parameters.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table dampening parameter**

display bgp vpnv4 all routing-table dampening parameter

display bgp ipv6 routing-table dampening parameter

display bgp vpnv6 vpn6-instance *vpn6-instance-name* **routing-table dampening parameter**

Parameters

Parameter	Description	Value
vpnv4	Displays the BGP route dampening parameters of a VPNv4 instance.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6	Displays configured BGP4+ route dampening parameters.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpnv6	Displays the BGP route dampening parameters of a VPNv6 instance.	-
all	Displays all BGP VPNv4 route dampening parameters	-
vpn6-instance *vpn6-instance-name*	Specifies the name of a VPNv6 instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display BGP route dampening parameters.

```
<Huawei> display bgp routing-table dampening parameter
 Maximum Suppress Time(in second) : 3973
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in  second)        : 900
 Suppress-Limit                   : 2000
```

Table 9-169 Description of the display bgp routing-table dampening parameter command output

Item	Description
Maximum Suppress Time (in second)	Indicates the maximum time taken for route suppression, in seconds.
Ceiling Value	Indicates the penalty ceiling.
Reuse Value	Indicates the threshold for a route to be unsuppressed.
HalfLife Time(in second)	Indicates the half life of a reachable route, in seconds.

Item	Description
Suppress-Limit	Indicates the threshold for a route to be suppressed.

Display BGP4+ route dampening parameters.

```
<Huawei> display bgp ipv6 routing-table dampening parameter
 Maximum Suppress Time(in second) : 3069
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in  second)        : 900
 Suppress-Limit                   : 2000
```

Related Topics

9.8.20 dampening

9.8.61 display bgp routing-table flap-info

Function

The **display bgp routing-table flap-info** command displays statistics about BGP route flapping.

Format

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table flap-info** [**regular-expression** *as-regular-expression*]

display bgp routing-table flap-info [**regular-expression** *as-regular-expression* | **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [{ *mask* | *mask-length* } [**longer-match**]]]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table flap-info** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **regular-expression** *as-regular-expression* | *network-address* [{ *mask* | *mask-length* } [**longer-match**]]]

display bgp [**vpnv4 vpn-instance** *vpn-instance-name*] **routing-table flap-info** { **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [{ *mask* | *mask-length* } [**longer-match**]] }

display bgp ipv6 routing-table flap-info [**regular-expression** *as-regular-expression*]

display bgp ipv6 routing-table flap-info { **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [*prefix-length* [**longer-match**]] }

display bgp vpnv6 vpn6-instance *vpn6-instance-name* **routing-table flap-info** [**regular-expression** *as-regular-expression*]

display bgp vpnv6 vpn6-instance *vpn6-instance-name* **routing-table flap-info** { **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [*prefix-length* [**longer-match**]] }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpnv4	Displays statistics about route flapping of a VPNv4 instance.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpn6-instance *vpn6-instance-name*	Specifies the name of a VPNv6 instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
regular-expression *as-regular-expression*	Displays statistics about the flapping routes that match the AS_Path regular expression.	The value is a string of 1 to 80 characters.
as-path-filter *as-path-filter-number*	Specifies the number of an AS_Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter *as-path-filter-name*	Specifies the name of an AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without any spaces. When double quotation marks are used around the string, spaces are allowed in the string.
network-address	Specifies the network address related to dampened routes.	-
mask	Specifies the network mask.	It is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer ranging from 0 to 32.
longer-match	Matches a route with a longer prefix.	-
prefix-length	Specifies the prefix length.	It is an integer ranging from 0 to 128.
vpnv6	Displays statistics about route flapping of a VPNv6 instance.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the Route Distinguisher dampened BGP routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display statistics about BGP route flapping.

```
<Huawei> display bgp routing-table flap-info


 BGP Local router ID is 10.20.200.201
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed,
               Origin codes: i - IGP, e - EGP, ? - incomplete

Total Number of Routes: 7
     Network          From            Flaps   Duration      Reuse   Path/Ogn

 d  10.1.1.0         10.20.200.200   5       00:00:36  00:40:47  600i
 *>  10.1.1.0         10.20.200.202   1       00:04:07            100?
 d  10.1.2.0         10.20.200.200   5       00:00:36  00:40:47  600i
 *>  10.1.2.0         10.20.200.202   1       00:04:07            100?
 d  10.1.3.0         10.20.200.200   5       00:00:36  00:40:47  600i
 d  10.1.4.0         10.20.200.200   5       00:00:36  00:40:47  600i
 d  10.1.5.0         10.20.200.200   5       00:00:36  00:40:47  600i
```

Table 9-170 Description of the display bgp routing-table flap command output

Item	Description
Network	Indicates the network address in the BGP routing table.
From	Indicates the IP address of the peer that receives the routes.
Flaps	Indicates the total number of times of route flapping.
Duration	Indicates the total time length of flapping.
Reuse	Indicates the reuse value.

Item	Description
Path/Ogn	Indicates the AS_Path number and the Origin attribute.

Display statistics about BGP4+ route flapping.

```
<Huawei> display bgp ipv6 routing-table flap-info


 BGP Local router ID is 10.53.53.53
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 3
  d  Network : FC00:0:0:1::                    PrefixLen : 96
     From    : FC00:0:0:1::1                   Flaps     : 8
     Duration: 00:02:11                        Reuse     : 00:49:21
     Path/Ogn: 100?

  d  Network : FC00:0:0:2::2                    PrefixLen : 128
     From    : FC00:0:0:1::1                   Flaps     : 5
     Duration: 00:00:18                        Reuse     : 00:41:06
     Path/Ogn: 100?

  d  Network : FC00:0:0:2::3                    PrefixLen : 128
     From    : FC00:0:0:1::1                   Flaps     : 5
     Duration: 00:00:18                        Reuse     : 00:41:06
     Path/Ogn: 100?
```

9.8.62 display bgp routing-table label

Function

The **display bgp routing-table label** command displays labeled routes in the BGP routing table.

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support this command.

Format

display bgp routing-table label [**statistics** | **include-mask**]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [**statistics**] **label**

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table label** [**include-mask**]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** [**statistics**] **label**

display bgp vpnv6 all routing-table [**statistics**]

display bgp ipv6 routing-table [**statistics**] **label**

Parameters

Parameter	Description	Value
include-mask	Displays labeled routes carrying masks.	-
statistics	Indicates statistics about labeled routes.	-
vpnv4	Displays VPNv4 labeled routes.	-
vpnv6	Displays VPNv6 labeled routes.	-
all	Displays the labeled routes of all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display BGP labeled routes of all VPN instances.

```
<Huawei> display bgp vpnv4 all routing-table label
 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 3
 Route Distinguisher: 100:1

        Network            NextHop           In/Out Label
 *>i    10.22.22.22        10.3.3.9          NULL/1036

 Route Distinguisher: 100:4

        Network            NextHop           In/Out Label
 *>     10.1.2.0           10.1.2.1          1037/NULL
```

```
*>     10.11.11.11       127.0.0.1         1038/NULL

VPN-Instance vpn1, router ID 1.1.1.9:
Total Number of Routes: 1

      Network           NextHop           In/Out Label
*>i    10.22.22.22       10.3.3.9          NULL/1036

VPN-Instance vpn2, router ID 10.1.1.9:
Total Number of Routes: 0
```

Table 9-171 Description of the display bgp vpnv4 all routing-table label command output

Item	Description
Network	Network address in the BGP routing table.
NextHop	IP address of the reachable next hop.
In/Out Label	Incoming label and outgoing label.

Display BGP4+ labeled routing information.

```
<Huawei> display bgp ipv6 routing-table label
Total Number of Routes: 3

 Network     Prefix     NextHop           Label
 2001:db8::4 128     ::FFFF:20.0.0.2      1024
 2001:db8::5 128     ::FFFF:20.0.0.2      1025
 2001:db8::6 128     ::FFFF:20.0.0.2      1026
```

Table 9-172 Description of the **display bgp routing-table label** command output

Item	Description
Prefix	Indicates an IP prefix

Display the BGP labeled routes of all IPv6 VPN instances.

```
<Huawei> display bgp vpnv6 all routing-table label
 BGP Local router ID is 1.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 2
 Route Distinguisher: 100:1
    Network              Prefix     NextHop           In/Out Label
 *>  2001:db8:1::         64     2001::1               1039/NULL

 Route Distinguisher: 100:2
    Network              Prefix     NextHop           In/Out Label
 *>i 2001:db8:2::         64     ::FFFF:3.3.3.9        NULL/1037

 VPN-Instance vpn1, Router ID 10.4.4.4 :
 Total Number of Routes: 1
    Network              Prefix     NextHop           In/Out Label
 *>i 2001:db8:2::         64     ::FFFF:3.3.3.9        NULL/1037
```

Display the BGP4+ labeled routes of the VPN instance named vpna.

```
<Huawei> display bgp vpnv6 vpn-instance vpna routing-table label
 BGP Local router ID is 1.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 VPN-Instance vpna, Router ID 10.4.4.4 :
 Total Number of Routes: 1
     Network            Prefix     NextHop           In/Out Label
 *>i 2001:db8:2::        64     ::FFFF:3.3.3.9        NULL/1037
```

Display IPv4 labeled routes carrying masks.

```
<Huawei> display bgp routing-table label include-mask
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 10

       Network          NextHop          In/Out Label
 *>i   10.1.92.0/24     1.1.1.1          NULL/1035
 *>i   10.1.93.0/24     1.1.1.1          NULL/1034
 *>i   10.1.94.0/24     1.1.1.1          NULL/1033
```

9.8.63 display bgp routing-table peer no-advertise

Function

The **display bgp routing-table peer no-advertise** command displays the routes that a device is prevented from advertising to a specified peer in different address families.

Format

display bgp routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table peer** *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp multicast routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp ipv6 routing-table peer *ipv6-address* **no-advertise** *ipv6–network* [*prefix-length*]

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp ipv6 routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp vpnv6 all routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

display bgp mdt all routing-table peer *ipv4-address* **no-advertise** *network* [*mask* | *mask-length*]

Parameters

Parameter	Description	Value
peer *ipv4-address*	Displays the routes that a device is prevented from advertising to the specified IPv4 peer.	The value is in dotted decimal notation.
network	Displays the routes with the specified destination IPv4 address that are prevented from being advertised.	The value is in dotted decimal notation.
mask	Specifies the subnet mask of the specified IPv4 address.	The value is in dotted decimal notation.
mask-length	Specifies the subnet mask length of the specified IPv4 address.	The value is an integer ranging from 0 to 32.
vpnv4	Displays the routes that a device is prevented from advertising to a specified peer in the VPNv4 address family.	-
all	Displays the routes that a device is prevented from advertising to a specified peer in all VPN instances of the current address family.	-
vpn-instance *vpn-instance-name*	Displays the routes that a device is prevented from advertising to a specified peer in the specified VPN instance of the current address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
multicast	Displays the routes that a device is prevented from advertising to a specified peer in the IPv4 multicast address family.	-
ipv6	Displays the routes that a device is prevented from advertising to a specified peer in the IPv6 unicast address family.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
peer *ipv6-address*	Displays the routes that a device is prevented from advertising to the specified IPv6 peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv6–network	Displays the routes with the specified destination IPv6 address that are prevented from being advertised.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer ranging from 0 to 128.
vpnv6	Displays the routes that a device is prevented from advertising to a specified peer in the VPNv6 address family.	-
mdt	Displays the routes that a device is prevented from advertising to a specified peer in the multicast distribution tree (MDT) address family.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the routes that a device is prevented from advertising to a specified peer in different address families, run the **display bgp routing-table peer no-advertise** command. The command output also includes the reasons why the routes are not advertised.

You can specify an address family to check the routes that a device is prevented from advertising to a specified peer in the address family. If you do not specify any address family, the command output shows the routes that a device is prevented from advertising to a specified peer in the IPv4 unicast address family.

Example

Display the route 3.3.3.4/32 that a device is prevented from advertising to peer with IP address 1.1.1.1 in the IPv4 unicast address family.

```
<Huawei> display bgp routing-table peer 1.1.1.1 no-advertise 3.3.3.4 32
 BGP routing table entry information of 3.3.3.4/32:
 From: 1.1.1.1 (10.1.1.1)
 Route Duration: 22h36m17s
 Relay IP Nexthop: 10.1.1.1
 Relay IP Out-Interface: GigabitEthernet1/0/0
 Original nexthop: 1.1.1.1
 Qos information : 0x0
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, active, pre 255,
IGP cost 1
 No advertise without config reflect-client
```

Table 9-173 Description of the **display bgp routing-table peer no-advertise** command output

Item	Description
From	Peer from which the route was received.
Route Duration	Duration of the route.
Relay IP Nexthop	Next-hop IP address to which the route is iterated.
Relay IP Out-Interface	Outbound interface to which the route is iterated.
Original nexthop	Original next-hop IP address of the route.
Qos information	QoS information carried in the route.
AS-path	AS_Path attribute. **Nil** indicates that the attribute value is null.
Origin	Origin attribute: ● IGP: indicates that the route is added to the BGP routing table using the **network (BGP)** command. ● EGP: indicates that the route is learned through the EGP protocol. ● Incomplete: indicates that the origin of the route cannot be identified. For example, if a route is imported using the **import-route (BGP)** command, its origin is **Incomplete**.
MED	MED of the route.
localpref	Local_Pref of the BGP route.
pref-val	PrefVal of the route.
valid	Valid route.
internal	Internal route.
best	Optimal route.
select	Selected route.

Item	Description
active	Active route.
pre 255	Priority of the route (255 in this example).
IGP cost 1	IGP cost of the route (1 in this example).
No advertise without config reflect-client	Reason why the route is not advertised: ● No advertise with no-adv flag: The route carries the No-Advertise flag. ● No advertise with peer default-route-advertise in vt family: The local device is configured to advertise only default routes to the peer in the VT address family. ● No advertise with no-adv flag in community attr: The route carries the No-Advertise community attribute. ● No advertise with no-export flag in community attr: The route carries the No-Export community attribute. ● No advertise with no-export-subconfed flag in community attr: The route carries the No_Export_Subconfed community attribute. ● No advertise by detail route with config aggregate: Specific routes for summarization are not advertised. ● No advertise with config active-route-advertise: Only the active routes in the IP routing table are advertised. ● No advertise with config peer upe and no export policy: The specified peer is a UPE, and the route fails to match the export policy. ● No advertise without config reflect-client: No RR is configured. ● No advertise with config reflect-client but without config reflect between-clients: Route reflection among RR clients is disabled. ● No advertise for other reason: Other reasons prevent the route from being advertised.

 Copyright © Huawei Technologies Co., Ltd.

9.8.64 display bgp routing-table peer statistics

Function

The **display bgp routing-table peer statistics** command displays statistics about received and advertised BGP routes.

Format

display bgp { **vpnv4** | **vpnv6** } { **all** | **vpn-instance** *vpn-instance-name* } **routing-table peer statistics**

display bgp [**multicast** | **ipv6** | **mdt**] **routing-table peer statistics**

display bgp evpn routing-table peer statistics

Parameters

Parameter	Description	Value
multicast	Displays statistics about routes in the IP multicast routing table.	-
ipv6	Displays statistics about routes in the BGP IPv6 unicast address family.	-
mdt	Displays statistics about routes in the BGP MDT address family.	-
vpnv4	Displays statistics about routes in the BGP-VPNv4 address family.	-
vpnv6	Displays statistics about routes in the BGP-VPNv6 address family.	-
all	Displays statistics about all types of routes.	-
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
evpn	Displays information about EVPN peer groups.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

To check statistics of received and advertised BGP routes, run the **display bgp routing-table peer statistics** command. You can specify parameters as needed. If no parameter is specified in the command, statistics about BGP IPv4 unicast routes are displayed.

Example

Display statistics about received and advertised BGP IPv4 unicast routes.

```
<Huawei> display bgp routing-table peer statistics

 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Total number of peers : 3              Number of Peers in established state : 3

  Peer            Received routes          Advertised routes

  10.2.2.2          1                        1
  10.2.2.3          1                        1
  10.3.3.3          2                        0
```

Table 9-174 Description of the **display bgp routing-table peer statistics** command output

Item	Description
BGP local router ID	Local router ID
Local AS number	AS number
Total number of peers	Total number of peers
Number of Peers in established state	Number of peers in the established state
Peer	IP address of a peer
Received routes	Total number of routes received from the peer
Advertised routes	Total number of routes advertised to the peer

9.8.65 display bgp routing-table statistics

Function

The **display bgp routing-table statistics** command displays statistics about BGP routes.

Format

display bgp routing-table statistics

display bgp routing-table statistics as-path-filter { *as-path-filter-number* | *as-path-filter-name* }

display bgp routing-table statistics cidr

display bgp routing-table statistics community [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp routing-table statistics community-filter { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp routing-table statistics dampened

display bgp routing-table statistics different-origin-as

display bgp routing-table statistics regular-expression *as-regular-expression*

display bgp routing-table peer *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
as-path-filter *as-path-filter-number*	Displays the routes that match the specified the number of the matching AS-Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter *as-path-filter-name*	Displays the routes that match the specified the name of the matching AS-Path filter.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
cidr	Displays CIDR information.	-
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	It is an integer ranging from 0 to 4294967295.
aa:nn	Specifies the community attribute number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the matching routes that can be sent to any peer.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-export	Displays the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays the routes that match a specified BGP community filter.	-
basic-community-filter-number	Specifies the number of a basic community filter.	It is an integer ranging from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	It is an integer ranging from 100 to 199.
community-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 characters. The string cannot be all numbers.
dampened	Displays the statistics of BGP dampened roues.	-
different-origin-as	Displays routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
peer *ipv4-address*	Displays the routing information for the specified BGP peer.	It is in dotted decimal notation.
advertised-routes	Displays the routes advertised to the specified peer.	-
received-routes	Displays the routes received from the specified peer.	-
active	Specifies the number of active routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display bgp routing-table statistics** command is used to display statistics about BGP routes on the public network.

The **display bgp routing-table statistics as-path-filter** command is used to display statistics about the BGP routes that match the specified AS_Path filter on the public network.

The **display bgp routing-table statistics cidr** command is used to display statistics about the BGP CIDR information of the public network.

The **display bgp routing-table statistics community** command is used to display statistics about the BGP routes carrying the specified community attribute on the public network.

The **display bgp routing-table statistics community-filter** command is used to display statistics about the BGP routes that match the specified community filter on the public network.

The **display bgp routing-table statistics dampened** command is used to display statistics about BGP dampened routes on the public network.

The **display bgp routing-table statistics different-origin-as** command is used to display statistics about the BGP routes with the same destination address but different source AS numbers on the public network.

The **display bgp routing-table statistics regular-expression** command is used to display statistics about the BGP routes whose AS_Path information matches the AS_Path regular expression on the public network.

Example

Display route statistics.

```
<Huawei> display bgp routing-table statistics
 Total Number of Routes: 4
```

Table 9-175 Description of the display bgp routing-table statistics command output

Item	Description
Total Number of Routes	Total number of routes in the routing table

9.8.66 display bgp update-peer-group

Function

The **display bgp update-group** command displays information about update-groups. By setting **index** in the command displays detailed information about a specified update-group. If no address family is specified, information about the update-group of the IPv4 unicast address family is displayed by default.

Format

display bgp update-peer-group [**index** *update-group-index*]

display bgp ipv6 update-peer-group [**index** *update-group-index*]

display bgp [**vpnv4** { **vpn-instance** *vpn-instance-name* | **all** }] **update-peer-group** [**index** *update-group-index*]

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **update-peer-group** [**index** *update-group-index*]

display bgp mdt all update-peer-group [**index** *update-group-index*]

Parameters

Parameter	Description	Value
index *update-group-index*	Specifies the index of an update-group.	The value is an integer ranging from 0 to 65535.
ipv6	Displays information about the BGP update-groups of IPv6 routes.	-
vpnv4	Displays information about the BGP update-groups of a VPNv4 instance. **NOTE** The AR100&AR120&AR150&AR160&AR200 series does not support this parameter.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** The AR100&AR120&AR150&AR160&AR200 series does not support this parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpnv6	Displays information about BGP Virtual Private Network version 6 (VPNv6) update-groups.	-
all	Displays information about all the update-groups in a VPNv4 address family. **NOTE** The AR100&AR120&AR150&AR160&AR200 series does not support this parameter.	-
mdt	Displays information about Multicast Distribution Tree (MDT) BGP update-groups.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display bgp update-peer-group** command is used to display information about all the update-groups in the IPv4 unicast address family on the public network.

The **display bgp update-peer-group index** command is used to display information about the update-group matching a specified index in the IPv4 unicast address family on the public network.

The **display bgp vpnv4 all update-peer-group** command is used to display information about all the update-groups in the VPNv4 unicast address family.

The **display bgp vpnv4 all update-peer-group index** command is used to display information about the update-group matching a specified index in the VPNv4 unicast address family on the public network.

The **display bgp vpnv4 vpn-instance update-peer-group** command is used to display information about the update-groups in the IPv4 unicast address family in a specified VRF.

The **display bgp vpnv4 vpn-instance update-peer-group index** command is used to display information about the update-group matching a specified index in the IPv4 unicast address family in a specified VRF.

Example

Display information about the update-groups in a certain address family.

```
<Huawei> display bgp update-peer-group
 The Public instance's update peer group number : 1
 Keep buffer update peer group number : 0
 BGP Version : 4
 Group ID : 0
 Group Type : external
 Addr Family : IPv4-UNC
 AdvMinTimeVal : 30
 Total Peers : 1
 Leader Peer : 192.168.1.2
 Peers List : 192.168.1.2
```

Table 9-176 Description of the display bgp update-peer-group command output

Item	Description
The Public instance's update peer group number	Number of update-groups in the instance

Item	Description
Keep buffer update peer group number	Number of packets in update-groups saved in the batch buffer
BGP Version	Indicates the BGP version.
Group ID	Indicates the ID of the update-group.
Group Type	Indicates the type of the update-group, which can be one of the following: ● external: indicates that this is an EBGP peer group. ● internal: indicates that this is an IBGP peer group. ● unknown: indicates that the type is unknown.
Addr Family	Indicates the address family.
AdvMinTimeVal	Indicates the minimum interval for sending Update packets with the same route prefix.
Total Peers	Indicates the total number of peers in an update-group.
Leader Peer	Indicates the representative of an update-group.
Peers List	Indicates a list of peers.

Display information about the update-group with a specified index.

```
<Huawei> display bgp update-peer-group index 0
 Group ID : 0
 BGP Version : 4
 Group Type : external
 Addr Family : IPv4-UNC
 AdvMinTimeVal : 30
 Total Peers : 1
  Leader Peer : 192.168.1.2

 Total format packet number : 3
 Total send packet number : 3
 Total replicate packet number : 0
 The replication percentages(%) : 0

 Peers List : 192.168.1.2
```

Table 9-177 Description of the display bgp update-peer-group index command output

Item	Description
Total format packet number	Indicates the total number of formatted packets.
Total send packet number	Indicates the total number of sent packets.

Item	Description
Total replicate packet number	Indicates the total number of replicate packets, which equals the total number of sent packets minus the total number of formatted packets.
The replication percentages(%)	Indicates the replication percentage, which is obtained with the formula: (Total number of sent packet - Total number of formatted packets) x 100/Total number of formatted packets.

9.8.67 display bgp vpnv4 brief

Function

The **display bgp vpnv4 brief** command displays brief information about VPNv4 and VPN instances (IPv4 address family).

Format

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **brief**

Parameters

Parameter	Description	Value
all	Displays information about all VPNv4 and VPN instances (IPv4 address family).	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **display bgp vpnv4 brief** command is used to display information about VPNv4 and VPN instances (IPv4 address family), the VPN instances are displayed and arranged alphabetically by name.

Example

Display brief information about VPNv4 instances and all VPN instances (IPv4 address family).

```
<Huawei> display bgp vpnv4 all brief

VPNV4 :
  Rd Num             Peer Num           Route Num
  0                  1                  0

VPN-Instance(IPv4-family):
  VPN-Instance Name   Peer Num           Route Num
  vrf0                0                  0
  vrf1                0                  0
  vrf11               0                  0
  vrf12               0                  0
  vrf13               0                  0
  vrf14               0                  0
  vrf2                0                  20
  vrf3                0                  20
  vrf4                0                  24
  vrf5                0                  24
  vrf6                0                  0
  vrf7                0                  0
  vrf8                0                  20
```

Table 9-178 Description of the display bgp vpnv4 brief command output

Item	Description
Rd Num	Indicates the number of RDs.
Peer Num	Indicates the number of peers.
Route Num	Indicates the number of routes.
VPN-Instance Name	Indicates the name of a VPN instance.

9.8.68 display bgp vpnv4 routing-table

Function

The **display bgp vpnv4 routing-table** command displays BGP routes of VPNv4 address family and the private networks.

Format

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table regular-expression** *as-regular-expression*

display bgp vpnv4 route-distinguisher *route-distinguisher* **routing-table** *ipv4-address* [*mask* | *mask-length*]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table** *ipv4-address* [*mask* [**longer-prefixes**] | *mask-length* [**longer-prefixes**]]

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table peer** *ipv4-address* { **advertised-routes** [*network* [{ *mask* | *mask-length* } [**longer-prefixes**]]] | **received-routes** [**active**] }

display bgp vpnv4 all routing-table peer *ipv4-address* **received-routes** *network* [{ *mask* | *mask-length* } [**longer-prefixes**]]

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table peer** *ipv4-address* **received-routes** *network* [{ *mask* | *mask-length* } [**longer-prefixes** | **original-attributes**]]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table peer** *ipv4-address* **accepted-routes**

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table time-range** *start-time end-time*

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table** [**verbose** | **statistics** | *ipv4-address* [*mask* | *mask-length*]]

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table** [**verbose** | **statistics** | *ipv4-address* [{ *mask* | *mask-length* }[**longer-prefixes**]]]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about BGP public network routes.	-
all	Displays all BGP VPNv4 routes.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays the BGP routes with the specified RD.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the BGP routes of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	The value is an integer ranging from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
cidr	Displays CIDR information.	-
different-origin-as	Displays the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
ipv4-address	Specifies the destination address.	-
mask	Specifies a mask in dotted decimal notation.	The value is in dotted decimal notation.
mask-length	Specifies the the mask length.	The value is an integer that ranges from 0 to 32.
peer *ipv4-address*	Displays routes of a specified peer.	-
advertised-routes	Displays the routes advertised to a specified peer.	-
network	Specifies the IPv4 network address.	It is in dotted decimal notation.
longer-prefixes	Matches any route whose prefix mask is longer than the specified length.	-
received-routes	Displays the routes received from a specified peer.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
active	Displays the active routes received from a specified peer.	-
original-attributes	Displays the original attributes of a BGP route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
community-filter	Displays the routes that match a specified BGP community filter.	-
community-filter-name	Specifies the name of a community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer that ranges from 1 to 99.
whole-match	Indicates exact matching.	-
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer that ranges from 100 to 199.
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the number of a community.	-
aa:*nn*	Specifies the community number. A maximum of 29 community numbers can be set.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays the matching routes that can be sent to any peer.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-
no-export	Displays the BGP routes carrying the No-Export community attribute.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
accepted-routes	Displays the routes that are received from a neighbor and accepted by a routing policy.	-
time-range *start-time end-time*	Displays information about BGP VPNv4 routes that have undergone status flapping during the specified period. For example, when *start-time* is set to 0d0h5m0s and *end-time* is set to 0d0h10m0s, information about all BGP VPNv4 routes whose lifetime ranges from 5 to 10 minutes is displayed.	In the values of *start-time* and *end-time*, d ranges from 0 to 10000, h ranges from 0 to 23, m ranges from 0 to 59, and s ranges from 0 to 59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

When BGP routing table is displayed, if the length of the destination address mask of an IPv4 route is the same as that of its natural mask, the mask length is not displayed.

You can run the **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **routing-table time-range** *start-time end-time* command to view BGP VPNv4 routes that flap within the specified time period. For example, if service traffic is abnormal or CPU usage of the device remains high within a certain time period, you can run this command to check whether route flapping occurs within the specified time period. The faulty route can be viewed in the command output, facilitating fault location.

Example

Display all the BGP routing information of the VPN instance named vpn1.

```
<Huawei> display bgp vpnv4 vpn-instance vpn1 routing-table

 BGP Local router ID is 10.1.1.9
```

```
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


VPN-Instance vpn1, Router ID 10.1.1.9:

Total Number of Routes: 4
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.2.0/24        0.0.0.0        0                    0      ?
*>   10.1.2.1/32        0.0.0.0        0                    0      ?
*>   10.11.11.11/32     0.0.0.0        0                    0      ?
*>i  10.22.22.22/32     10.3.3.9       0          100       0      ?
```

Display all the BGP VPNv4 routing information.

```
<Huawei> display bgp vpnv4 all routing-table


BGP Local router ID is 10.1.1.9
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete



Total number of routes from all PE: 4
Route Distinguisher: 100:1


     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>i  10.22.22.22/32     10.3.3.9       0          100       0      ?

Route Distinguisher: 100:4


     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.2.0/24        0.0.0.0        0                    0      ?
*>   10.1.2.1/32        0.0.0.0        0                    0      ?
*>   10.11.11.11/32     0.0.0.0        0                    0      ?

VPN-Instance vpn1, Router ID 10.1.1.9:

Total Number of Routes: 4
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.2.0/24        0.0.0.0        0                    0      ?
*>   10.1.2.1/32        0.0.0.0        0                    0      ?
*>   10.11.11.11/32     0.0.0.0        0                    0      ?
*>i  10.22.22.22/32     10.3.3.9       0          100       0      ?
```

Display the VPNv4 routing information of the specified RD.

```
<Huawei> display bgp vpnv4 route-distinguisher 100:1 routing-table

BGP Local router ID is 10.1.1.9
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete

Route Distinguisher: 100:1


Total Number of Routes: 3
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.1.0/24        0.0.0.0        0                    0      ?
*                       10.1.1.1       0                    0      65410?
```

```
*>   10.1.1.2/32        0.0.0.0         0                    0      ?

VPN-Instance vpna, Router ID 10.1.1.9:

Total Number of Routes: 7
     Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

*>   10.1.1.0/24        0.0.0.0         0                    0      ?
                     10.1.1.1        0                    0      65410?
*>   10.1.1.2/32        0.0.0.0         0                    0      ?
*>   10.2.1.0/24        10.2.1.2        0                    0      ?
* i                   10.3.3.9        0          100        0      ?
*>   10.2.1.2/32        127.0.0.1       0                    0      ?
*>i  10.4.1.0/24        3.3.3.9         0          100        0      ?
```

Display all BGP VPNv4 routes of community 1000:100.

```
<Huawei> display bgp vpnv4 all routing-table community 1000:100

BGP Local router ID is 10.1.1.9
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


Total number of routes from all PE: 1

Route Distinguisher: 100:1


     Network            NextHop        MED        LocPrf    PrefVal Community

*>i  10.22.22.22/32     10.3.3.9        0          100        0      <1000:100>

VPN-Instance vpn1, Router ID 10.1.1.9:

Total Number of Routes: 1
     Network            NextHop        MED        LocPrf    PrefVal Community

*>i  10.22.22.22/32     10.3.3.9        0          100        0      <1000:100>

VPN-Instance vpn2, Router ID 10.1.1.9:

Total Number of Routes: 0
```

Displays BGP VPNv4 routes that flap within the specified time period.

```
<Huawei> display bgp vpnv4 all routing-table time-range 0d5h0m0s 1d5h0m0s

BGP Local router ID is 192.168.1.250
Status codes: * - valid, > - best, d - damped,
              h - history,  i - internal, s - suppressed, S - Stale
              Origin : i - IGP, e - EGP, ? - incomplete


Route Distinguisher: 2:2

     Network            NextHop         Peer            Duration        Path/Ogn

*>i  0.0.0.0            10.2.2.2        10.2.2.2        05h30m11s       i
*>   10.2.3.4/32        0.0.0.0         0.0.0.0         05h30m42s       ?

VPN-Instance 1, Router ID 192.168.1.250:
     Network            NextHop         Peer            Duration        Path/Ogn

*>   10.2.3.4/32        0.0.0.0         0.0.0.0         05h30m42s       ?

VPN-Instance 2, Router ID 192.168.1.250:
     Network            NextHop         Peer            Duration        Path/Ogn
```

```
*>i  0.0.0.0          10.2.2.2       10.2.2.2       05h30m11s       i
*>   10.2.3.4/32       0.0.0.0        0.0.0.0        05h30m42s       ?
```

Table 9-179 Description of the display bgp vpnv4 routing-table command output

Item	Description
BGP Local router ID	ID of the local BGP device.
Network	Network address in the BGP routing table.
NextHop	Next Hop address through which the packet has to be sent
MED	MED of the route.
LocPrf	Local preference.
PrefVal	Preferred value.
Peer	Peer IP address
Duration	Route duration
Path/Ogn	AS_Path number and the origin attribute.
Community	Community attribute information.

Display information about a specified VPNv4 route.

```
<Huawei> display bgp vpnv4 all routing-table 192.168.2.0


 BGP local router ID : 10.2.2.9
 Local AS number : 100

 Total routes of Route Distinguisher(100:10): 2
 BGP routing table entry information of 192.168.2.0/24:
 Imported route.
 Label information (Received/Applied): NULL/1025
 From: 0.0.0.0 (0.0.0.0)
 Route Duration: 00h50m09s
 Direct Out-interface: GigabitEthernet0/0/2
 Original nexthop: 192.168.2.1
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select,
pre 255
 Advertised to such 1 peers:
    10.3.3.3
 BGP routing table entry information of 192.168.2.0/24:
 From: 192.168.2.2 (1.1.1.1)
 Route Duration: 00h48m50s
 Direct Out-interface: GigabitEthernet0/0/2
 Original nexthop: 192.168.2.2
 Qos information : 0x0
 Ext-Community:RT <1 : 1>
 AS-path 10, origin incomplete, MED 0, pref-val 0, valid, external, pre 255, not
 preferred for route type
 Not advertised to any peer yet
```

```
 VPN-Instance vpna, Router ID 10.2.2.9:

 Total Number of Routes: 2
 BGP routing table entry information of 192.168.2.0/24:
 Imported route.
 From: 0.0.0.0 (0.0.0.0)
 Route Duration: 00h50m09s
 Direct Out-interface: GigabitEthernet0/0/2
 Original nexthop: 192.168.2.1
 Qos information : 0x0
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select,
pre 0
 Advertised to such 1 peers:
    192.168.2.2
 BGP routing table entry information of 192.168.2.0/24:
 From: 192.168.2.2 (1.1.1.1)
 Route Duration: 00h48m51s
 Direct Out-interface: GigabitEthernet0/0/2
 Original nexthop: 192.168.2.2
 Qos information : 0x0
 AS-path 10, origin incomplete, MED 0, pref-val 0, external, pre 255
 Not advertised to any peer yet
```

Table 9-180 Description of the display bgp vpnv4 routing-table command output

Item	Description
Local AS Number	Local AS number.
Total routes of Route Distinguisher	Total number of VPNv4 routes with a specified RD.
BGP routing table entry information of x.x.x.x/x	The following information is about a specified BGP routing entry.
Imported route	Routes imported to BGP using the **import-route** command.
Label information (Received/Applied)	Information about labels, including received and sent labels.
From	IP address of the route originator.
Route Duration	Route duration.
Direct Out-interface	Direct outbound interface.
Original nexthop	Original next hop.
Qos information	QoS information.
Ext-Community	Extended community attribute of BGP.
AS-path	AS_Path attribute.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Origin	Origin attribute of the BGP route. The value can be IGP (for example, the routes imported into the BGP routing table by using the **network (BGP)** command), EGP (the routes obtained by EGP), or Incomplete (the routes whose origin cannot be identified, for example, the routes imported into the BGP routing table by using the **import-route (BGP)** command).
pref-val	Preferred value.
valid	Valid BGP route.
external	The BGP route is learned from the EBGP peer.
best	The BGP route is the optimal route.
select	The BGP route is a preferred route.
Pre 255	The preference of the BGP route is 255.
Advertised to such 1 peers	The BGP route has been advertised to one peer.
Not advertised to any peer yet	The BGP route has not been advertised to any peer.
VPN-Instance vpna, Router ID 10.2.2.9	The VPN instance is vpna, the Route ID is 10.2.2.9
Total Number of Routes	Number of routes in VPN instance vpna.

Display detailed information about the specified invalid BGP VPNv4 routes.

```
<Huawei> display bgp vpnv4 all routing-table 4.4.4.4
 BGP local router ID : 10.1.1.1
 Local AS number : 100

 Total routes of Route Distinguisher(10:10): 1
 BGP routing table entry information of 4.4.4.4/32:
 Label information (Received/Applied): 1025/NULL
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h12m26s
 Relay IP Nexthop: 0.0.0.0
 Relay IP Out-Interface: GigabitEthernet0/0/0
 Relay Tunnel Out-Interface:
 Relay token: 0x0
 Original nexthop: 10.1.1.2
 Qos information : 0x0
 Ext-Community:RT <10 : 10>, RT <20 : 20>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, valid, internal, best, select, pre 255
 Not advertised to any peer yet

 VPN-Instance vrf1, Router ID 10.1.1.1:

 Total Number of Routes: 1
 BGP routing table entry information of 4.4.4.4/32:
```

```
 Label information (Received/Applied): 1025/NULL
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h12m26s
 Relay Tunnel Out-Interface:
 Relay token: 0x0
 Original nexthop: 10.1.1.2
 Qos information : 0x0
 Ext-Community:RT <10 : 10>, RT <20 : 20>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for tunnel
unreachable
 Not advertised to any peer yet
```

Table 9-181 Description of the **display bgp vpnv4 routing-table** command output

Item	Description
BGP local router ID	ID of the local BGP device. The format is the same as the IPv4 address.
Local AS number	Local AS number.
Total routes of Route Distinguisher(10:10)	Total number of BGP VPNv4 routes of the specified RD.
BGP routing table entry information of 4.4.4.4/32	The following information is about 4.4.4.4/32 routing entries.
Label information (Received/Applied)	Label information (received or sent).
From	IP address of the device that sends the route. 10.1.1.2 is the IP address of the source interface of the peer with which the BGP connection is established, and 10.1.1.2 is the Router ID of the peer.
Route Duration	Duration of routes.
Relay IP Nexthop	IP iterated next hop.
Relay IP Out-Interface	IP iterated outbound interface.
Relay Tunnel Out-Interface	Tunnel iterated outbound interface.
Relay token	Iterated token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.
Original nexthop	Original next hop.
Qos information	QoS information.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.

Item	Description
origin incomplete	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
localpref	Local priority.
pref-val	Value preferred by the protocol.
valid	The BGP route is a valid route.
internal	The BGP route is an internal route.
best	The BGP route is an optimal route.
select	The BGP route is a preferred route.
pre 255	The priority of the BGP route is 255.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
invalid for tunnel unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to be iterated to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to be iterated to a tunnel.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.
VPN-Instance vrf1, Router ID 10.1.1.1	The local VPN instance is vrf1, and its router ID is 10.1.1.1.
Total Number of Routes	Total number of BGP VPNv4 routes that match 4.4.4.4/32 in VPN instance vrf1.

9.8.69 display bgp vpnv4 routing-table statistics

Function

The **display bgp vpnv4 routing-table statistics** command displays statistics about BGP VPNv4 routes.

Format

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **cidr** | **different-origin-as**]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics regular-expression** *as-regular-expression*

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv4 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table statistics dampened**

display bgp vpnv4 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table peer** *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
all	Displays all the statistics of the BGP routes for VPNv4.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays statistics about the BGP routes with a specified RD.	The RD formats are divided into the following types: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about the BGP routes of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	The value is an integer ranging from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
cidr	Displays CIDR statistics.	-
different-origin-as	Displays statistics about the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
community	Displays statistics about the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	The value is an integer ranging from 0 to 4294967295.
aa:*nn*	Specifies a community attribute value.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays statistics about the matching routes that can be sent to any peer.	-
no-advertise	Displays statistics about the BGP routes carrying the No-Advertise community attribute.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-export	Displays statistics about the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays statistics about the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays statistics about the routes that match a specified BGP community filter.	-
basic-community-filter-number	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.
community-filter-name	Specifies the name of a community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits.
dampened	Displays the statistics of BGP dampened routes.	-
active	Displays statistics about the routes that have the same destination address but different source AS numbers.	-
peer *ipv4-address*	Displays statistics about routes of a specified peer.	It is in dotted decimal notation.
advertised-routes	Displays statistics about the routes advertised to a specified peer.	-
received-routes	Displays statistics about the routes received from a specified peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display statistics about VPNv4 routes.

```
<Huawei> display bgp vpnv4 all routing-table statistics

 Total number of routes from all PE: 2

 VPN-Instance vpn1, Router ID 10.1.1.9:

 Total Number of Routes: 2
```

Display statistics about the VPNv4 routes with the specified RD.

```
<Huawei> display bgp vpnv4 route-distinguisher 100:1 routing-table statistics

 Route Distinguisher: 100:1


 Total Number of Routes: 2

 VPN-Instance vpn1, Router ID 10.1.1.9:

 Total Number of Routes: 2
```

Table 9-182 Description of the display bgp vpnv4 routing-table statistics command output

Item	Description
Total number of routes from all PE	Total number of VPNv4 routes
VPN-Instance vpn1	Indicating the name of VPN instance is vpn1.
Router ID 10.1.1.9	Indicating the router ID is 10.1.1.9.
Total Number of Routes	Total number of routes of the VPN instance.
Route Distinguisher	RD of the VPN instance IPv4 address family.

9.8.70 display bgp vpnv6 brief

Function

The **display bgp vpnv6 brief** command displays brief information about VPNv6 and VPN instances (IPv6 address family).

Format

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **brief**

Parameters

Parameter	Description	Value
all	Displays information about all VPNv6 and VPN instances (IPv6 address family).	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPNv6 instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **display bgp vpnv6 brief** command is used to display information about VPNv6 and VPN instances (IPv6 address family), the VPN instances are displayed and arranged alphabetically by name.

Example

Display brief information about VPNv6 and VPN instances (IPv6 address family).

```
<Huawei> display bgp vpnv6 all brief

VPN-Instance(IPv6-family):
 VPN-Instance Name   Peer Num          Route Num
   vrf0                1                2
   vrf1                0                0
   vrf11               0                0
   vrf12               0                0
   vrf13               0                0
   vrf14               0                0
   vrf2                0                20
   vrf3                0                20
   vrf4                0                24
   vrf5                0                24
   vrf6                0                0
```

Table 9-183 Description of the display bgp vpnv6 all brief command output

Item	Description
Peer Num	Number of peers.
Route Num	Number of routes.

Item	Description
VPN-Instance Name	Name of a VPN instance.

9.8.71 display bgp vpnv6 routing-table

Function

The **display bgp vpnv6 routing-table** command displays BGP VPNv6 routes.

Format

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* | **route-distinguisher** *route-distinguisher* } **routing-table** [**verbose** | *ipv6-address* [*prefix-length*]]

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table as-path-filter** { *as-path-filter-number* | *as-path-filter-name* }

display bgp vpnv6 all routing-table

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv6 route-distinguisher *route-distinguisher* **routing-table community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table different-origin-as**

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table different-origin-as**

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table regular-expression** *as-regular-expression*

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* } **routing-table regular-expression** *as-regular-expression*

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* { **advertised-routes** [*dest-ipv6-address* [*prefix-length*]] | **received-routes** [**active**] }

display bgp vpnv6 all routing-table peer *ipv6-address* { **advertised-routes** [*dest-ipv6-address* [*prefix-length*]] | **received-routes** [**active**] }

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* **received-routes** *dest-ipv6-address* [*prefix-length* [**original-attributes**]]

display bgp vpnv6 all routing-table peer *ipv6-address* **received-routes** *dest-ipv6-address* [*prefix-length*]

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* **accepted-routes**

display bgp vpnv6 { **all** | **vpn-instance** *vpn-instance-name* } **routing-table time-range** *start-time end-time*

Parameters

Parameter	Description	Value
all	Displays statistics about all BGP VPNv6 routes.	-
vpn-instance *vpn-instance-name*	Displays the BGP routes of a specified an IPv6 address family-enabled VPN instance on the local end.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about BGP VPNv6 routes. **NOTE** Only the V009C00SPC301 version supports this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Indicates the route distinguisher (RD).	The RD formats are divided into the following types: ● 2-byte AS number:32-bit user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of x.y, where x and y are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● 32-bit IP address:16-bit user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer to be displayed.	It is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	-
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	The value is an integer ranging from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
community	Displays the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	-
aa:nn	Specifies the community number. A maximum of 29 community numbers can be set.	-
internet	Displays the BGP routes carrying the Internet community attribute.	-
no-advertise	Displays the BGP routes carrying the No-Advertise community attribute.	-
no-export	Displays the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays the routes that match a specified BGP community filter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
community-filter-name	Specifies the name of a community filter.	-
basic-community-filter-number	Specifies the number of a basic community filter.	-
advanced-community-filter-number	Specifies the number of an advanced community filter.	-
different-origin-as	Displays the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
peer *ipv6-address*	Displays the BGP routes of a specified peer.	-
advertised-routes	Displays the routes advertised to a specified peer.	-
dest-ipv6–address	Specifies the destination IPv6 address.	-
received-routes	Displays the routes received from a specified peer.	-
active	Displays the active routes received from a specified peer.	-
original-attributes	Displays the original attributes of a BGP route from a specified BGP peer before the route is filtered by the local import policy. To display such attributes, the **peer keep-all-routes** command must have been run.	-
accepted-routes	Displays the routes that are received from a neighbor and accepted by a routing policy.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-range *start-time end-time*	Displays information about BGP VPNv6 routes that have undergone status flapping during the specified period. For example, when *start-time* is set to 0d0h5m0s and *end-time* is set to 0d0h10m0s, information about all BGP VPNv6 routes whose lifetime ranges from 5 to 10 minutes is displayed.	In the values of *start-time* and *end-time*, d ranges from 0 to 10000, h ranges from 0 to 23, m ranges from 0 to 59, and s ranges from 0 to 59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about specified routes can be displayed by specifying different parameters.

To view information about BGP VPNv6 route flapping during a specified period, you can run the **display bgp vpnv6 vpn-instance** *vpn-instance-name* **routing-table time-range** *start-time end-time* command. When service traffic is abnormal during a period of time, you can run this command to check whether route flapping occurs. When the CPU usage is high during a period of time, you can run this command to check whether a large number routes have undergone status flapping. This command allows you to find the flapping routes, which facilitates fault location.

Example

Display all BGP VPNv6 routes.

```
<Huawei> display bgp vpnv6 all routing-table


 BGP Local router ID is 10.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total number of routes from all PE: 3
 Route Distinguisher: 100:1


 *>i Network  : FC00:0:0:2001::                    PrefixLen : 64
     NextHop  : FC00:0:0:2001::1                   LocPrf    :
     MED      : 0                              PrefVal   : 0
     Label    : NULL
```

```
    Path/Ogn :  ?
*>  Network  : FC00:0:0:2001::2                    PrefixLen : 128
    NextHop  : ::                                 LocPrf    :
    MED      : 0                                  PrefVal   : 0
    Label    : NULL
    Path/Ogn :  ?
*>  Network  : FE80::                               PrefixLen : 10
    NextHop  : ::                                 LocPrf    :
    MED      : 0                                  PrefVal   : 0
    Label    : NULL
    Path/Ogn :  ?

 VPN-Instance whm1 :

 Total Number of Routes: 3
*>  Network  : FC00:0:0:2001::                     PrefixLen : 64
    NextHop  : ::                                 LocPrf    :
    MED      : 0                                  PrefVal   : 0
    Label    : NULL
    Path/Ogn :  ?
*>  Network  : FC00:0:0:2001::2                    PrefixLen : 128
    NextHop  : ::                                 LocPrf    :
    MED      : 0                                  PrefVal   : 0
    Label    : NULL
    Path/Ogn :  ?
*>  Network  : FE80::                               PrefixLen : 10
    NextHop  : ::                                 LocPrf    :
    MED      : 0                                  PrefVal   : 0
    Label    : NULL
    Path/Ogn :  ?
```

Display information about BGP VPNv6 route flapping of a specified VPN instance during the specified period.

```
<Huawei> display bgp vpnv6 vpn-instance 1 routing-table time-range 0d5h0m0s 1d5h0m0s
BGP Local router ID is 10.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 300:1

*>  Network  : FC00:0:0:1991::                     PrefixLen : 64
    NextHop  : ::                                 Duration  : 16h32m17s
    Peer     : ::
    Path/Ogn : ?
*>  Network  : FC00:0:0:2004::                     PrefixLen : 64
    NextHop  : ::                                 Duration  : 16h34m02s
    Peer     : ::
    Path/Ogn : ?

 Route Distinguisher: 10011:1

*>i Network  : FC00:0:0:1998::                     PrefixLen : 32
    NextHop  : FC00:0:0:1::9                      Duration  : 16h38m16s
    Peer     : 10.1.1.9
    Path/Ogn : 65410  ?
*>i Network  : FC00:0:0:1998::                     PrefixLen : 64
    NextHop  : FC00:0:0:1::9                      Duration  : 16h37m01s
    Peer     : 10.1.1.9
    Path/Ogn : ?
*>i Network  : FC00:0:0:2001::                     PrefixLen : 64
    NextHop  : FC00:0:0:1::9                      Duration  : 16h47m31s
    Peer     : 10.1.1.9
    Path/Ogn : ?
*>i Network  : FC00:0:0:3001::                     PrefixLen : 64
    NextHop  : FC00:0:0:1::9                      Duration  : 16h45m40s
    Peer     : 10.1.1.9
    Path/Ogn : 65410  ?
```

```
VPN-Instance vpna :
*>  Network  : FC00:0:0:1991::                PrefixLen : 64
    NextHop  : ::                           Duration  : 16h32m17s
    Peer     : ::
    Path/Ogn : ?
*>i Network  : FC00:0:0:1998::                PrefixLen : 32
    NextHop  : FC00:0:0:1::9                  Duration  : 16h38m16s
    Peer     : 10.1.1.9
    Path/Ogn : 65410  ?
*>i Network  : FC00:0:0:1998::                PrefixLen : 64
    NextHop  : FC00:0:0:1::9                  Duration  : 16h37m01s
    Peer     : 10.1.1.9
    Path/Ogn : ?
*>i Network  : FC00:0:0:2001::                PrefixLen : 64
    NextHop  : FC00:0:0:1::9                  Duration  : 16h47m31s
    Peer     : 10.1.1.9
    Path/Ogn : ?
*>  Network  : FC00:0:0:2004::                PrefixLen : 64
    NextHop  : ::                           Duration  : 16h34m02s
    Peer     : ::
    Path/Ogn : ?
*>i Network  : FC00:0:0:3001::                PrefixLen : 64
    NextHop  : FC00:0:0:1::9                  Duration  : 16h45m40s
    Peer     : 10.1.1.9
    Path/Ogn : 65410  ?
```

Table 9-184 Description of the display bgp vpnv6 all routing-table command output

Item	Description
BGP Local router ID	ID of the local BGP router. The ID is in the same format as an IPv4 address.
Total number of routes from all PE	Total number of BGP VPNv6 routes received by the router from its peer PEs.
Network	Destination network or host address of the route.
PrefixLen	Prefix length of the destination network or host address of the route.
NextHop	IPv6 address of the next hop.
LocPrf	Local preference of the BGP route. The default value is 100.
MED	MED of the route. The default value is 0.
PrefVal	Preferred value of the route.
Label	Label carried by the data packet destined for the destination network or host address of the route.
Duration	Route duration.
Peer	IP addresses of the peer.
Path/Ogn	AS_Path number and Origin attribute of the route.

Display the routes of an IPv6 address family-enabled VPN instance named vpn1 on the local device.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 2
 *>i Network  : FC00:0:0:1::                    PrefixLen : 64
     NextHop  : FC00:0:0:3::1                    LocPrf    :
     MED      : 0                            PrefVal   : 0
     Label    :
     Path/Ogn : 65410  ?
 *>i Network  : FC00:0:0:1::                    PrefixLen : 64
     NextHop  : FC00:0:0:2::1                    LocPrf    : 100
     MED      : 0                            PrefVal   : 0
     Label    : 1037/NULL
     Path/Ogn : ?
```

Display BGP4+ routes with the specified destination address of the VPN instance.

```
<Huawei> display bgp vpnv6 vpn-instance vrf1 routing-table fc00:0:0:1::

 BGP local router ID : 10.1.1.1
 Local AS number : 100
 Paths:   2 available, 1 best, 1 select
 BGP routing table entry information of FC00:0:0:1::/64:
 Imported route.
 From: :: (0.0.0.0)
 Route Duration: 1d03h46m24s
 Direct Out-interface: Vlanif100
 Original nexthop: ::
 AS-path Nil, origin incomplete, MED 0, pref-val 0, valid, local, best, select,
pre 0
 Advertised to such 1 peers:
    FC00:0:0:2::2
 BGP routing table entry information of 2001::/64:
 From: FC00:0:0:1::1 (10.10.10.10)
 Route Duration: 02h39m43s
 Direct Out-interface: Vlanif100
 Original nexthop: FC00:0:0:1::1
 AS-path 65410, origin incomplete, MED 0, pref-val 0, external, pre 255
 Not advertised to any peer yet
```

Display all BGP VPNv6 routes whose AS_Path attribute contains 65420.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table as-path-filter 1

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 VPN-Instance vpn1 :

 Total Number of Routes: 1
     Network  : FC00:0:0:1::2001::                PrefixLen : 64
     NextHop  : FC00:0:0:1::2001::1                LocPrf    :
     MED      : 0                            PrefVal   : 0
```

```
    Label    :
    Path/Ogn : 65420  ?
```

Display BGP4+ routes of the VPN instance named **vpn1** and matching the BGP community filter 1.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table community-filter 1 whole-match

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 VPN-Instance vpn1 :

 Total Number of Routes: 2
    Network  : FC00:0:0:2001::                    PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    :
    MED      : 0                              PrefVal   : 0
    Label    :
 *>i Network  : FC00:0:0:2002::                    PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    : 100
    MED      : 0                              PrefVal   : 0
    Label    : 1037/NULL
```

Display all BGP4+ routes of the VPN instance named **vpn1** and matching the AS regular expression.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table regular-expression ^65420


 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 VPN-Instance vpn1, Router ID 10.4.4.4, Router ID 10.4.4.4 :
    Network  : FC00:0:0:2001::                    PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    :
    MED      : 0                              PrefVal   : 0
    Label    :
    Path/Ogn : 65420  ?
```

Display all BGP4+ routes of the VPN instance named **vpn1** that are received from the peer at FC00:0:0:2001::1.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table peer fc00:0:0:2001::1 received-routes

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
    Network  : FC00:0:0:2001::                    PrefixLen : 64
    NextHop  : FC00:0:0:2001::1                    LocPrf    :
    MED      : 0                              PrefVal   : 0
    Label    :
    Path/Ogn : 65410  ?
```

Display BGP4+ routes sent to the peer at FC00:0:0:2001::1.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table peer fc00:0:0:2001::1 advertised-routes

 BGP Local router ID is 10.1.1.9
 Status codes: * - valid, > - best, d - damped,
```

```
            h - history,  i - internal, s - suppressed, S - Stale
            Origin : i - IGP, e - EGP, ? - incomplete


 Total Number of Routes: 1
 *>i Network  : FC00:0:0:2002::                    PrefixLen : 64
     NextHop  : FC00:0:0:2001::1                   LocPrf    : 100
     MED      : 0                              PrefVal   : 0
     Label    : 1037/NULL
     Path/Ogn : ?
```

Display detailed information about the specified invalid BGP VPNv6 routes.

```
<Huawei> display bgp vpnv6 vpn-instance vrf1 routing-table 5::5
 BGP local router ID : 10.1.1.1
 Local AS number : 100

 VPN-Instance vrf1, Router ID 10.1.1.1:
 Paths:   1 available, 0 best, 0 select
 BGP routing table entry information of 5::5/128:
 Label information (Received/Applied): 1027/NULL
 From: 10.1.1.2 (10.1.1.2)
 Route Duration: 00h01m22s
 Relay Tunnel Out-Interface:
 Relay token: 0x0
 Original nexthop: ::FFFF:10.1.1.2
 Ext-Community:RT <100 : 100>
 AS-path Nil, origin incomplete, MED 0, localpref 100, pref-val 0, internal, pre 255, invalid for tunnel
unreachable
 Not advertised to any peer yet
```

Table 9-185 Description of the **display bgp vpnv6 routing-table** command output

Item	Description
BGP Local Router ID	Router ID of the local BGP device. The format is the same as the IPv4 address.
Local AS Number	Local AS number.
VPN-Instance vrf1, Router ID 10.1.1.1	The local VPN instance is vrf1, and its router ID is 10.1.1.1.
Paths	Information about paths of BGP routes
BGP routing table entry information of 5::5/128	The following information is about 5::5/128 routing entries.
Label information (Received/Applied)	Label information (received or sent).
From	IP address of the router that sends the route. 10.1.1.2 is the source interface IP address of the peer with which the BGP connection is established, and 10.1.1.2 is the router ID of the peer.
Route Duration	Duration of routes.
Relay Tunnel Out-Interface	Tunnel iterated outbound interface.

Item	Description
Relay token	Iterated token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.
Original nexthop	Original next hop.
Ext-Community	Extended community attribute.
AS-path Nil	AS_Path attribute, with Nil indicating that the attribute value is null.
Origin	Well-known mandatory property. This property defines the origin of a path and records how a route turns to a BGP route. The property has the following three values: ● IGP: The priority of this value is the highest. The origin property of the routes that are added to the BGP routing table by using the **network (BGP)** command is IGP. ● EGP: The priority of this value is second to that of IGP. The origin property of the routes imported from EGP is EGP. ● Incomplete: The priority of this value is the lowest. The value indicates the origin of a route is unknown. The origin property of the routes that are added to the BGP routing table by using the **import-route (BGP)** command is Incomplete.
MED	Multi-Exit discriminator of route.
Localpref	Local priority.
pref-val	Preferred value of the protocol.
internal	The BGP route is an internal route.
Pre 255	The priority of the BGP route is 255.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
invalid for tunnel unreachable	Reason why a route is invalid: ● invalid for route-policy not pass: The route does not match the route-policy. ● invalid for supernet route: The route is a supernet route. ● invalid for IP unreachable: The route fails to be iterated to another route. ● invalid for supernet route not advertise: No supernet routes are advertised. ● invalid for supernet label route not advertise: No supernet labeled routes are advertised. ● invalid for next-hop unreachable: The next-hop IP address is unreachable. ● invalid for tunnel unreachable: The route fails to be iterated to a tunnel.
Not advertised to any peer yet	The BGP route has not been advertised to any peer yet.

9.8.72 display bgp vpnv6 routing-table statistics

Function

The **display bgp vpnv6 routing-table statistics** command displays statistics about BGP VPNv6 routes.

Format

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | **different-origin-as**]

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics regular-expression** *as-regular-expression*

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community** [*community-number* | *aa:nn*] &<1-29> [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

display bgp vpnv6 { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* } **routing-table statistics community-filter** { { *community-filter-name* | *basic-community-filter-number* } [**whole-match**] | *advanced-community-filter-number* }

display bgp vpnv6 all routing-table peer *ipv4-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

display bgp vpnv6 vpn-instance *vpn-instance-name* **routing-table peer** *ipv6-address* { **advertised-routes** | **received-routes** [**active**] } **statistics**

Parameters

Parameter	Description	Value
all	Displays statistics about all BGP VPNv6 routes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Indicates the route distinguisher (RD).	The RD formats are divided into the following types: ● 2-byte AS number:32-bit user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● 32-bit IP address:16-bit user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about the BGP routes of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
as-path-filter	Displays the routes that match the specified filter.	-
as-path-filter-number	Specifies the number of the matching AS-Path filter.	The value is an integer ranging from 1 to 256.
as-path-filter-name	Specifies the name of the matching AS-Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
different-origin-as	Displays statistics about the routes that have the same destination address but different source AS numbers.	-
regular-expression *as-regular-expression*	Specifies the regular expression used to match the AS_Path information.	The value is a string of 1 to 80 characters.
community	Displays statistics about the routes carrying the specified BGP community attribute in the routing table.	-
community-number	Specifies the community number.	It is an integer ranging from 0 to 4294967295.
aa:nn	Specifies the community number.	Both *aa* and *nn* are integers ranging from 0 to 65535.
internet	Displays statistics about the BGP routes carrying the Internet community attribute.	-
no-advertise	Displays statistics about the BGP routes carrying the No-Advertise community attribute.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-export	Displays statistics about the BGP routes carrying the No-Export community attribute.	-
no-export-subconfed	Displays statistics about the BGP routes carrying the No-Export-Subconfed community attribute.	-
whole-match	Indicates exact matching.	-
community-filter	Displays statistics about the routes that match a specified BGP community filter.	-
community-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.
basic-community-filter-number	Specifies the number of a basic community filter.	It is an integer ranging from 1 to 99.
advanced-community-filter-number	Specifies the number of an advanced community filter.	It is an integer ranging from 100 to 199.
peer *ipv6-address*	Displays statistics about the BGP routes of a specified peer.	-
advertised-routes	Displays statistics about the routes advertised to a specified peer.	-
received-routes	Displays statistics about the routes received from a specified peer.	-
active	Displays the active routes received from a specified peer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display statistics about BGP VPNv6 routes on the local device.

```
<Huawei> display bgp vpnv6 all routing-table statistics

 Total number of routes from all PE: 2

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 2
```

Display statistics of BGP VPNv6 routes with RD 100:1 on local router.

```
<Huawei> display bgp vpnv6 route-distinguisher 100:1 routing-table statistics

 Route Distinguisher: 100:1


 Total Number of Routes: 1

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 2
```

Display statistics about the routes of an IPv6 address family-enabled VPN instance named vpn1 on the local device.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table statistics

 Total Number of Routes: 5
```

Display the number of BGP VPNv6 routes received from peer 1.1.1.1.

```
<Huawei> display bgp vpnv6 all routing-table peer 1.1.1.1 received-routes statistics
  Received routes total: 1
```

Display statistics of VPN-IPv6 routes with the internet community attribute of the specified RD on the local router.

```
<Huawei> display bgp vpnv6 route-distinguisher 100:1 routing-table statistics community internet

 Total number of routes from all PE: 1

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 2
```

Display statistics of all BGP VPNv6 routes of the specified community list on the local router.

```
<Huawei> display bgp vpnv6 all routing-table statistics community-filter 1

 Total number of routes from all PE: 1

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 2
```

Display statistics of all BGP VPNv6 routes that match the specified AS_Path regular expression.

```
<Huawei> display bgp vpnv6 all routing-table statistics regular-expression 65420*

 Total number of routes from all PE: 1

 VPN-Instance vpn1, Router ID 10.4.4.4 :

 Total Number of Routes: 1
```

Display statistics of BGP routes sent by the local device to peer 2000::1 of the IPv6 VPN instance named vpn1.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table peer 2000::1 received-routes statistics
  Received routes total: 2
```

Display statistics about the IPv6 routes sent by the local device to peer 2000::1 in a VPN instance named vpn1.

```
<Huawei> display bgp vpnv6 vpn-instance vpn1 routing-table peer 2000::1 advertised-routes statistics
  Advertised routes total: 2

  Default originated : 0
```

9.8.73 display default-parameter bgp

Function

The **display default-parameter bgp** command displays default configurations in BGP initialization.

Format

display default-parameter bgp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display default configurations in BGP initialization.

```
<Huawei> display default-parameter bgp
BGP version                 : 4
EBGP preference             : 255
IBGP preference             : 255
Local preference            : 255
BGP connect-retry           : 32s
BGP holdtime                : 180s
BGP keepAlive               : 60s
EBGP route-update-interval  : 30s
IBGP route-update-interval  : 15s
Default local-preference    : 100
Default MED                 : 0
IPv4-family unicast         : enable
EBGP-interface-sensitive    : enable
```

```
Reflect between-clients     : enable
Check-first-as              : enable
Synchronization             : disable
Nexthop-resolved rules    :
    IPv4-family           : unicast(ip)
                          label-route(ip)
                          mdt(ip)
                          multicast(ip)
                          vpn-instance(tunnel)
                          vpnv4(ip)
    IPv6-family           : unicast(ip)
                          vpn-instance(tunnel)
                          vpnv6(ip)
                          6PE(tunnel)
 Routing-table limit max-alarm upper limit : 100
 Routing-table limit max-alarm lower limit : 95
 Routing-table limit threshold-alarm upper limit : 80
 Routing-table limit threshold-alarm lower limit : 70
```

Table 9-186 Description of the **display default-parameter bgp** command output

Item	Description
BGP version	BGP version number.
EBGP preference	EBGP route preference.
IBGP preference	IBGP route preference.
Local preference	Local route preference.
BGP connect-retry	BGP ConnectRetry interval.
BGP holdtime	BGP holdtime interval.
BGP keepAlive	BGP keepalive interval.
EBGP route-update-interval	Minimum interval for sending EBGP Update messages.
IBGP route-update-interval	Minimum interval for sending IBGP Update messages.
Default local-preference	Local preference of a BGP route.
Default MED	MED of a BGP route.
IPv4-family unicast	BGP-IPv4 unicast address family view.
EBGP-interface-sensitive	The BGP session between the directly connected peer and an interface is deleted immediately when the interface becomes Down.
Reflect between-clients	Route reflection between clients.
Check-first-as	The first AS number in the AS_Path list that is carried in the Update message sent by the EBGP peer is checked.
Synchronization	Synchronization between IBGP and IGP.
Nexthop-resolved rules	Default iteration mode of preferred routes.

Item	Description
Routing-table limit max-alarm upper limit	Upper alarm threshold for the number of BGP routes.
Routing-table limit max-alarm lower limit	Lower alarm threshold for the number of BGP routes.
Routing-table limit threshold-alarm upper limit	Default upper alarm threshold for the number of BGP routes.
Routing-table limit threshold-alarm lower limit	Default lower alarm threshold for the number of BGP routes.

9.8.74 display mbgp routing-table

Function

The **display mbgp routing-table** command displays MBGP routes.

Format

display mbgp routing-table [*ipv4-address* [*mask* | *mask-length*]] [**verbose**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the destination IP address in dotted decimal notation.	-
mask | *mask-length*	Specifies mask in dotted decimal notation or mask-length.	-
verbose	Displays detailed information about active and inactive routes. If the parameter **verbose** is not specified, detailed information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

Example

Display information about all MBGP routes.

```
<Huawei> display mbgp routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: MBGP
         Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost  Flags  NextHop  Interface

 10.5.5.1/32     MBGP   255     0     R   10.1.1.1  Vlanif10
```

Table 9-187 Description of the display mbgp routing-table command output

Item	Description
Route Flags	Indicates the route flag: ● R: indicates an iterated route. ● D: indicates that the route is downloaded to the FIB table.
Routing Tables: MBGP	Indicates an MBGP routing table.
Destinations	Indicates the total number of destination networks or hosts.
Routes	Indicates the total number of routes.
Destination/Mask	Indicates the address and mask length of the destination network or host.
Proto	Indicates the protocol through which routes are learned.
Pre	Indicates the preference.
Cost	Indicates the route cost.
Flags	Indicates the route flag, that is, Route Flags in the header of the routing table.
NextHop	Indicates the next hop.
Interface	Indicates the outbound interface through which the next hop is reachable.

Display the detailed information of the specified routes.

```
<Huawei> display mbgp routing-table 5.5.5.1 verbose
Routing Table : MBGP
Summary Count : 1

 Destination: 10.5.5.1/32
    Protocol: MBGP              Process ID: 0
  Preference: 255                    Cost: 0
     NextHop: 10.1.1.1          Neighbour: 0.0.0.0
       State: Active Adv GotQ          Age: 00h43m25s
```

```
        Tag: 0                Priority: 0
      Label: NULL               QoSInfo: 0x0
RelayNextHop: 0.0.0.0          Interface: Vlanif 10
    TunnelID: 0x0              Flags: R
```

Table 9-188 Description of the display mbgp routing-table verbose command output

Item	Description
Destination	Indicates the address and mask length of the destination network or host.
Protocol	Indicates the routing protocol.
Process ID	Indicates the process ID of the routing protocol.
Preference	Indicates the preference of the route.
Cost	Indicates the route cost.
NextHop	Indicates the next hop.
Neighbour	Indicates the neighbor.
State	Indicates the status of routes: ● Active: indicates active routes. ● Invalid: indicates invalid routes. ● Inactive: indicates inactive routes. ● NoAdv: indicates the routes that cannot be advertised. ● Adv: indicates the routes that can be advertised. ● Del: indicates the routes to be deleted. ● GotQ: indicates the route that finds the next hop and outbound interface or the route that finds the tunnel. ● WaitQ: indicates the route that does not find the next hop or outbound interface or the route that does not find the tunnel. ● Stale: indicates the routes with the stale flag. The routes are used in GR.
Age	Indicates the lifetime of the route.
Tag	Indicates the administrative tag for routes.
Priority	Indicates the priority.
Label	Indicates the allocated MPLS label.
QoSInfo	Indicates QoS information.
RelayNextHop	Indicates the relay next hop.
Interface	Indicates the outbound interface through which the next hop is reachable.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tunnel ID	Indicates the tunnel ID.
Flags	Indicates the route flag, that is, Route Flags in the header of the routing table.

9.8.75 display mbgp routing-table statistics

Function

The **display mbgp routing-table statistics** command displays the statistics of the MBGP routes.

Format

display mbgp routing-table statistics

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include:

- Total number of routes that are added or deleted by the protocol
- Number of active routes or inactive routes that are labeled for deletion but are not actually deleted

Example

Display statistics of the MBGP routing table.

```
<Huawei> display mbgp routing-table statistics
Proto     total      active      added       deleted      freed
          routes     routes      routes      routes       routes
MBGP      6          4           10          0            0
```

Table 9-189 Description of the display mbgp routing-table statistics command output

Item	Description
Proto	Routing protocol
total routes	Total number of routes in the routing table
active routes	Number of active routes in the routing table
added routes	Number of active and inactive routes added in the routing table
deleted routes	Number of routes to be deleted from the routing table
freed routes	Number of routes that are permanently deleted from the routing table

9.8.76 display snmp-agent trap feature-name bgp all

Function

The **display snmp-agent trap feature-name bgp all** command displays all the traps related to the BGP module.

Format

display snmp-agent trap feature-name bgp all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display snmp-agent trap feature-name bgp all** command is used to display the status of all the traps related to the BGP module.

To change the status of the traps related to the BGP module, run the **snmp-agent trap enable feature-name bgp** command.

Example

Display all the traps related to the BGP module.

```
<Huawei>display snmp-agent trap feature-name bgp all
-------------------------------------------------------------------------------
Feature name: bgp
Trap number : 13
-------------------------------------------------------------------------------
Trap name                        Default switch status   Current switch status
ESTABLISHED                      off                     on
BACKWARD                         off                     on
ROUTETHRESHOLDEXCEED             off                     on
ROUTETHRESHOLDCLEAR              off                     on
GRSTATUSCHANGE                   off                     on
HWESTABLISHED                    off                     on
HWBACKWARD                       off                     on
HWBGPROUTEMAXEXCEED              off                     off
HWBGPROUTEMAXCLEAR               off                     off
HWBGPROUTETHRESHOLDEXCEED        off                     off
HWBGPROUTETHRESHOLDCLEAR         off                     off
HWBGPDYNAMICPEERSESSIONEXCEED    off                     off
HWBGPDYNAMICPEERSESSIONEXCEEDCLEAR
                                 off                     off
```

Table 9-190 Description of the display snmp-agent trap feature-name bgp all command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Name of a trap message of the BGP module: ● ESTABLISHED: indicates that the BGP neighbor has entered the Established state. ● BACKWARD: indicates the disconnection of BGP neighbors. ● ROUTETHRESHOLDEXCEED: indicates that the number of routes of BGP neighbors exceeds the alarm threshold. ● ROUTETHRESHOLDCLEAR: indicates that the number of routes of BGP neighbors falls below the alarm threshold. ● GRSTATUSCHANGE: indicates that the GR status of BGP neighbors changes. ● HWESTABLISHED: indicates that the BGP neighbor has entered the Established state. ● HWBACKWARD: indicates the disconnection of BGP neighbors. ● HWBGPROUTEMAXEXCEED: indicates that the number of BGP routes exceeds the alarm threshold. ● HWBGPROUTEMAXCLEAR: indicates that the number of BGP routes falls below the alarm threshold. ● HWBGPROUTETHRESHOLDEXCEED: indicates that the number of BGP routes exceeds the alarm threshold. ● HWBGPROUTETHRESHOLDCLEAR: indicates that the number of BGP routes falls below the alarm threshold. ● HWBGPDYNAMICPEERSESSIONEXCEED: indicates the alarm generated when the number of dynamic BGP peer sessions exceeds the maximum number. ● HWBGPDYNAMICPEERSESSIONEXCEEDCLEAR: indicates the alarm generated when the number of dynamic BGP peer sessions falls below the maximum number.
Default switch status	Default status of the trap function: ● on: The trap function is enabled by default. ● off: The trap function is disabled by default.
Current switch status	Current status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.8.172 snmp-agent trap enable feature-name bgp

9.8.77 ebgp-interface-sensitive

Function

The **ebgp-interface-sensitive** command immediately resets a BGP session on an interface that is directly connected to an external peer when the interface goes Down.

The **undo ebgp-interface-sensitive** command disables the function.

By default, this function is enabled.

Format

ebgp-interface-sensitive

undo ebgp-interface-sensitive

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the **ebgp-interface-sensitive** command is not configured, the system does not immediately select the sub-optimal route for packet transmission when an interface goes Down. Instead, the system waits for a period of time (defaulting to 180 seconds) before checking whether another interface can be used to send packets to the same destination address. This will interrupt services for a period of time. If the **ebgp-interface-sensitive** command is run, BGP can quickly detect EBGP link faults and use another interface to establish a BGP peer relationship with the remote peer.

When the interface used for a BGP connection alternates between Up and Down states, running the **undo ebgp-interface-sensitive** command can prevent the repeated reestablishment and deletion of the BGP session in the event of route flapping. This reduces the use of network bandwidth.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If the interface used for a BGP connection alternates between Up and Down states, it would be better not to run the **ebgp-interface-sensitive** command to prevent route flapping.

Example

Enable the function that automatically resets a BGP session.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ebgp-interface-sensitive
```

9.8.78 ext-community-change enable

Function

The **ext-community-change enable** command enables a device to change extended community attributes based on a Route-Policy.

The **undo ext-community-change enable** command disables a device from changing extended community attributes based on a Route-Policy.

By default, extended community attributes cannot be changed based on a Route-Policy.

Format

ext-community-change enable

undo ext-community-change enable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, BGP prevents a device from changing extended community attributes from a peer or peer group based on an import policy or changing extended community attributes to be advertised to a peer or peer group based on an export policy. To enable a device to change extended community attributes from a peer

 Copyright © Huawei Technologies Co., Ltd.

or peer group based on an import policy and change extended community attributes to be advertised to a peer or peer group based on an export policy before advertising them, run the **ext-community-change enable** command.

Precautions

- The **ext-community-change enable** and **peer route-policy import** commands must both be run so that the device can change extended community attributes from a peer or peer group based on an import policy.
- The **ext-community-change enable** command must be run with either of the following commands so that the extended community attributes changed based on an export policy can be advertised to a peer or peer group.
  - **peer advertise-ext-community**
  - **peer route-policy export**

Example

Enable the device to change extended community attributes of the BGP routes received from peer 10.1.1.1 based on a Route-Policy named **policy1**.

```
<Huawei> system-view
[Huawei] route-policy policy1 permit node 10
[Huawei-route-policy] if-match as-path-filter 2
[Huawei-route-policy] apply extcommunity rt 10.1.1.1:1 additive
[Huawei-route-policy] quit
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] ext-community-change enable
[Huawei-bgp-af-ipv4] peer 10.1.1.1 route-policy policy1 import
```

Related Topics

9.8.99 peer advertise-ext-community

9.8.79 filter-policy export (BGP)

Function

The **filter-policy export** command configures a device to filter the routes to be advertised. BGP advertises only the routes that pass filtering.

The **undo filter-policy export** command restores the default configuration.

By default, the routes to be advertised are not filtered.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name*] **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

undo filter-policy [*acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name*] **export** [*protocol* [*process-id*]]

undo filter-policy [*acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name*] **export** [*protocol* [*process-id*]]

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IPv4 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Specifies the name of a routing protocol.	The BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view support **direct**, **isis**, **ospf**, **rip**, **static**, and **unr**. The BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view support **direct**, **isis**, **ospfv3**, **ripng**, **static**, and **unr**.
process-id	Specifies the number of a process that needs to perform matching. If *protocol* is **direct**, **static**, or **unr**, no process ID is required.	The value is an integer ranging from 1 to 65535.
acl6-number	Specifies the number of a basic ACL6.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
acl6-name *acl6-name*	Specifies the name of a named ACL6.	The value is a string of 1 to 32 case-sensitive characters without spaces. The name should start with a letter (case sensitive) and can contain numbers, hyphens (-), or underlines (_).
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- *protocol* [*process-id*] is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.
- **acl-name** *acl-name*, *acl-number*, and **ip-prefix** *ip-prefix-name* are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- **acl6-name** *acl6-name*, *acl6-number*, and **ipv6-prefix** *ipv6-prefix-name* are valid only in the BGP-IPv6 unicast address family view, BGP-VPNv6 address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPN instance IPv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

The **filter-policy export** command affects the routes advertised by BGP. After the command is run, BGP filters the routes that are imported by using the **import-route (BGP)** command. Only the routes that pass the filtering can be added to the local BGP routing table and advertised by BGP.

If *protocol* is specified, only the routes imported from the specified protocol will be filtered. If *protocol* is not specified, the routes imported from all protocols will be filtered.

When the **rule** command is run to configure rules for a named ACL, only the source address range specified by **source** and the time period specified by **time-range** are valid as the rules.

Example

Use ACL 2000 to filter all the routes to be advertised by BGP.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] filter-policy 2000 export
```

Related Topics

9.8.86 import-route (BGP)

19.7.18 rule (basic ACL view)

19.7.19 rule (basic ACL6 view)

9.8.80 filter-policy import (BGP)

Function

The **filter-policy import** command configures a device to filter received routes.

The **undo filter-policy import** command restores the default configuration.

By default, received routes are not filtered.

Format

filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**

filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

undo filter-policy { *acl-number* | **acl-name** *acl-name* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy { *acl6-number* | **acl6-name** *acl6-name* | **ipv6-prefix** *ipv6-prefix-name* } **import**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IPv4 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
acl6-number	Specifies the number of a basic ACL6.	-
acl6-name *acl6-name*	Specifies the name of a named ACL6.	The value is a string of 1 to 32 case-sensitive characters without spaces. The name should start with a letter (case sensitive) and can contain numbers, hyphens (-), or underlines (_).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-prefix *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- **acl-name** *acl-name*, *acl-number*, and **ip-prefix** *ip-prefix-name* are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- **acl6-name** *acl6-name*, *acl6-number*, and **ipv6-prefix** *ipv6-prefix-name* are valid only in the BGP-IPv6 unicast address family view, BGP-VPNv6 address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

The **filter-policy import** command is used to filter the routes received by BGP to determine whether to add them to the BGP routing table.

When the **rule** command is run to configure rules for a named ACL, only the source address range specified by **source** and the time period specified by **time-range** are valid as the rules.

Example

Use ACL 2000 to filter the routes received by BGP.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] filter-policy 2000 import
```

Related Topics

19.7.19 rule (basic ACL6 view)

9.8.81 graceful-restart (BGP)

Function

The **graceful-restart** command enables GR for the BGP speaker.

The **undo graceful-restart** command restores the default configuration.

By default, GR is disabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP restart causes reestablishment of peer relationships and traffic interruption. After the **graceful-restart** command is run to enable GR, traffic interruption can be prevented in the event of BGP restart.

After running the **graceful-restart** command, run the **graceful-restart timer wait-for-rib** command to set the time for waiting for the End-Of-RIB flag.

Precautions

Enabling or disabling GR may delete and reestablish all BGP sessions and instances.

If the **graceful-restart timer wait-for-rib** command has been configured, using the **undo graceful-restart** command will delete the **graceful-restart timer wait-for-rib** command configuration.

Example

Enable GR for the speaker in BGP process 100.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] graceful-restart
```

 Copyright © Huawei Technologies Co., Ltd.

9.8.82 graceful-restart peer-reset

Function

The **graceful-restart peer-reset** command enables a device to reset a BGP connection in GR mode.

The **undo graceful-restart peer-reset** command restores the default configuration.

By default, a device is not enabled to reset a BGP connection in GR mode.

Format

graceful-restart peer-reset

undo graceful-restart peer-reset

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, BGP does not support dynamic capability negotiation. Therefore, each time a new BGP capability is enabled on a BGP speaker, the BGP speaker tears down existing sessions with its peer and renegotiates BGP capabilities. To prevent the service interruptions, run the **graceful-restart peer-reset** command to enable the BGP speaker to reset a BGP session in GR mode.

With the GR reset function configured, when you enable a new BGP capability on the BGP speaker, the BGP speaker enters the GR state, resets the BGP session, and renegotiates BGP capabilities with the peer. In the whole process, the BGP speaker re-establishes the existing sessions but does not delete the routing entries for the existing sessions, so that the existing services are not interrupted.

Prerequisites

GR has been enabled by running the **graceful-restart** command. If this prerequisite is not met, the system does not allow you to configure the **graceful-restart peer-reset** command.

Precautions

After you run the **undo graceful-restart** command to disable GR, the **graceful-restart peer-reset** command configuration will be deleted automatically.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the router to reset a BGP connection in GR mode.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] graceful-restart
[Huawei-bgp] graceful-restart peer-reset
```

9.8.83 graceful-restart timer restart

Function

The **graceful-restart timer restart** command sets the maximum period from the time when the peer finds that the local peer restarts to the time when the BGP session is reestablished.

The **undo graceful-restart timer restart** command deletes the setting.

By default, the maximum period from the time when the peer finds that the local peer restarts to the time when the BGP session is reestablished is 150 seconds.

Format

graceful-restart timer restart *time*

undo graceful-restart timer restart

Parameters

Parameter	Description	Value
time	Specifies the maximum period from the time when the peer finds that the local peer restarts to the time when the BGP session is reestablished.	The value ranges from 3 to 4095, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Modifying the maximum period for reestablishing the BGP session leads to the reestablishment of the BGP peer relationship.

NOTE

The **graceful-restart timer restart** command can be run only after the **graceful-restart** command is run.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum period for reestablishing the BGP session to 250 seconds.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] graceful-restart
[Huawei-bgp] graceful-restart timer restart 250
```

Related Topics

9.8.81 graceful-restart (BGP)

9.8.84 graceful-restart timer wait-for-rib

Function

The **graceful-restart timer wait-for-rib** command sets the length of time that the BGP restarter waits for the End-Of-RIB flag.

The **undo graceful-restart timer wait-for-rib** command deletes the configured length of time that the BGP restarter waits for the End-Of-RIB flag.

By default, the time that the BGP restarter waits for the End-Of-RIB flag is 600 seconds.

Format

graceful-restart timer wait-for-rib *time*

undo graceful-restart timer wait-for-rib

Parameters

Parameter	Description	Value
time	Specifies the length of time that the BGP restarter waits for the End-Of-RIB flag.	The value is an integer ranging from 3 to 3000, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a BGP session is established or reestablished, the BGP restarter needs to receive the End-Of-RIB flag within the period of time specified by the command. If no End-Of-RIB flag is received before that period expires, the BGP restarter exits

 Copyright © Huawei Technologies Co., Ltd.

from the GR process and chooses the optimal route from the current reachable routes.

Prerequisites

Graceful restart has been enabled before this command is used.

Precautions

The latest configuration overrides the previous one.

If there are lots of routes, setting *time* to a great value is recommended.

Example

Set the time that the BGP restarter waits for the End-Of-RIB flag to 100 seconds.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] graceful-restart timer wait-for-rib 100
```

Related Topics

9.8.81 graceful-restart (BGP)

9.8.85 group

Function

The **group** command creates a peer group.

The **undo group** command deletes a peer group.

By default, no peer group is created.

Format

group *group-name* [**external** | **internal**]

undo group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Creates an EBGP peer group.	-
internal	Creates an IBGP peer group.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A peer group is a group of peers with the same configurations. After a peer is added to a peer group, it inherits the configurations of this peer group. Peers in a peer group inherit the configurations of the peer group. When the configurations of the peer group are changed, the configurations of these peers are changed accordingly.

On a large-scale BGP network, there are a large number of peers and many of them have the same configurations. To configure these peers, you have to repeatedly use some commands. In such a case, configuring peer groups can simplify configurations. If the configurations for several peers are the same, these peers can be added to a created and configured peer group. The peers in the peer group then inherit the configurations of the peer group.

Precautions

If the **group** command is run multiple times, the latest configuration does not override the previous one.

If the type (IBGP or EBGP) of peer group is not specified, an IBGP peer group is created by default.

If an attribute configuration of a BGP peer in a peer group differs from that of the peer group, you can disable the attribute configuration of the peer by using an **undo** command; then the peer inherits the attribute configuration of the peer group.

NOTICE

Deleting a peer group closes the connections on the peers that have no AS numbers in the peer group. Before deleting a peer group, you are recommended to delete these peers or configure AS numbers for these peers.

Example

Create a IBGP peer group named in.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] group in internal
```

Create a EBGP peer group named ex, and set its AS number to 500.1.

```
<Huawei> system-view
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] bgp 100
[Huawei-bgp] group ex external
[Huawei-bgp] peer ex as-number 500.1
```

9.8.86 import-route (BGP)

Function

The **import-route** command configures BGP to import routes of other routing protocols and types.

The **undo import-route** command restores the default setting.

By default, BGP does not import routes.

Format

import-route *protocol* [*process-id*] [**med** *med* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

Parameters

Parameter	Description	Value
protocol	Specifies the routing protocol type and route type.	The BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view support **direct**, **isis**, **ospf**, **rip**, **static**, and **unr**. The BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view support **direct**, **isis**, **ospfv3**, **ripng**, **static**, and **unr**.
process-id	Specifies a process ID if BGP is configured to import routes. If *protocol* is **direct**, **static**, or **unr**, no process ID is required.	The value is an integer ranging from 1 to 65535.
med *med*	Specifies the MED.	The value is an integer that ranges from 0 to 4294967295.
route-policy *route-policy-name*	Indicates that routes are filtered and route attributes are modified by using the Route-Policy specified by the parameter when these routes are imported from other protocols.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP can import routes by using the **import-route** command or **network** command:

- In import mode, IGP routes, including RIP, OSPF, and IS-IS routes, are imported into BGP routing tables based on protocol type. To ensure the validity of imported IGP routes, BGP can also import static routes and direct routes in import mode.
- In network mode, BGP imports the routes in the IP routing table one by one to BGP routing tables. The network mode is more accurate than the import mode.

Precautions

If the **default-route imported** command has not been used, BGP cannot import default routes when you run the **import-route** command to import routes from other protocols.

After the **import-route direct** command is executed, routes to the network segment where the IP address of the management interface belongs are also imported in the BGP routing table. Therefore, use this command with caution.

Example

Import routes from RIP process 1.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] import-route rip 1
```

9.8.87 ipv4-family

Function

The **ipv4-family** command enables the IPv4 address family of BGP, and then displays the address family view.

The **undo ipv4-family** command deletes the configurations in the IPv4 address family.

By default, the BGP-IPv4 unicast address family view is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Format

ipv4-family unicast

ipv4-family mdt

ipv4-family multicast

ipv4-family vpnv4 [**unicast**]

ipv4-family vpn-instance *vpn-instance-name*

undo ipv4-family { **multicast** | **mdt** | **unicast** | **vpnv4** [**unicast**] | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
unicast	Displays the unicast address family view.	-
multicast	Displays the multicast address family view.	-
vpnv4	Displays the BGP-VPNv4 address family view. **NOTE** AR100&AR120&AR150&AR160&AR200 series does not support this parameter.	-
vpn-instance *vpn-instance-name*	Associates a specified VPN instance with the IPv4 address family. Displays the BGP-VPN instance IPv4 address family view.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
mdt	Displays the BGP-MDT address family view.	-

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing BGP configurations in an IPv4 address family, you need to run the **ipv4-family** command in the BGP view to enable the IPv4 address family, and

 Copyright © Huawei Technologies Co., Ltd.

then enter the address family view. By default, BGP uses the IPv4 unicast address family.

Precautions

To disable the IPv4 unicast address family from being the default BGP route, run the **undo default ipv4-unicast** command.

Example

Enter the BGP-IPv4 unicast address family view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4]
```

Enter the BGP-VPNv4 address family view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4]
```

9.8.88 ipv6-family

Function

The **ipv6-family** command enters the IPv6 address family view of BGP.

The **undo ipv6-family** command quits the IPv6 address family view and deletes the configurations in the view.

Format

ipv6-family [**unicast** | **vpnv6** | **vpn-instance** *vpn-instance-name*]

undo ipv6-family [**unicast** | **vpnv6** | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
unicast	Displays the unicast address family view.	-
vpnv6	Displays the BGP-VPNv6 address family view.	-
vpn-instance *vpn-instance-name*	Associates a specified VPN instance with the IPv6 address family. You can enter the BGP-VPN instance IPv6 address family view by using the parameter.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If no parameter is specified, the IPv6 address family view is displayed by default. The **undo ipv6-family** command without any parameter is used to delete configurations in the BGP-IPv6 unicast address family view.

Precautions

The **undo ipv6-family** command without any parameters deletes all IPv6 unicast address family configurations.

Example

Enter the BGP-IPv6 unicast address family view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv6-family
[Huawei-bgp-af-ipv6]
```

Enter the BGP-VPNv6 address family view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv6-family vpn-instance vrf1
[Huawei-bgp6-vrf1]
```

9.8.89 keep-all-routes

Function

The **keep-all-routes** command saves the routes carried in the BGP Update messages that are advertised by all BGP peers or peer groups after BGP connections are established.

The **undo keep-all-routes** command disables this function.

By default, the device saves only accepted routes (routes that match the import policy).

Format

keep-all-routes

undo keep-all-routes

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After changing a BGP import policy, you must reset BGP connections for the new import policy to take effect, interrupting these BGP connections temporarily. If a device's peer does not support route-refresh, you can run the **keep-all-routes** command on the device to save all routing updates received from the peer so that the device can refresh its routing table without resetting the connection with the peer.

Precautions

If the router does not support route-refresh, you need to run the **keep-all-routes** command on both ends. If the **keep-all-routes** command is run on the device for the first time, the sessions between the device and its peers are reestablished.

If the router supports route-refresh, running this command does not result in reestablishment of the sessions between the router and its peers. After the **refresh bgp** command is run, however, the route-refresh capability does not take effect on the router.

Example

Configure a device to save all BGP routing updates received from its peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] keep-all-routes
```

Related Topics

9.8.149 refresh bgp

9.8.90 load-balancing as-path-ignore

Function

The **load-balancing as-path-ignore** command configures a router not to compare the AS_Path attributes of routes that are to be used for load balancing.

The **undo load-balancing as-path-ignore** command configures a router to compare the AS_Path attributes of routes that are to be used for load balancing.

 Copyright © Huawei Technologies Co., Ltd.

By default, a router compares the AS-Path attributes of routes that are to be used for load balancing.

Format

load-balancing as-path-ignore

undo load-balancing as-path-ignore

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **load-balancing as-path-ignore** command is run, a router does not compare the AS-Path attributes of the routes (including the AS_Path length and content) that are to be used for load balancing. This command applies to the scenarios where EBGP and IBGP routes carry out load balancing. Exercise caution when using the command because the execution of this command will change the conditions of load balancing.

Precautions

The **load-balancing as-path-ignore** command and the **bestroute as-path-ignore** command are mutually exclusive. This means that if the **bestroute as-path-ignore** command is configured, the **load-balancing as-path-ignore** command cannot be configured.

Example

Configure a router not to compare the AS-Path attributes of the routes that are to be used for load balancing.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] load-balancing as-path-ignore
```

 Copyright © Huawei Technologies Co., Ltd.

9.8.91 maximum load-balancing (BGP)

Function

The **maximum load-balancing** command configures the maximum number of equal-cost routes for load balancing.

The **undo maximum load-balancing** command restores the default value.

By default, the maximum number of equal-cost routes is 1, and load balancing is not implemented.

Format

maximum load-balancing [**ebgp** | **ibgp**] *number* [**ecmp-nexthop-changed**]

undo maximum load-balancing [**ebgp** | **ibgp**]

Parameters

Parameter	Description	Value
ebgp	Indicates that only EBGP routes implement load balancing.	-
ibgp	Indicates that only IBGP routes implement load balancing.	-
number	Specifies the maximum number of equal-cost routes in the BGP routing table.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ecmp-nexthop-changed	Configures a BGP device to change the next-hop addresses of only the routes that participate in load balancing to its address. **NOTE** This parameter is invalid in the BGP-IPv4 multicast address family view.	-

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **maximum load-balancing** command is run, multiple BGP equal-cost routes will implement load balancing, improving network resource efficiency.

After BGP load balancing is configured, the routes that meet the following conditions will become equal-cost routes and implement load balancing:

- Original next-hop addresses are different.
- PrefVal values are the same.
- Local_Pref attributes are the same.
- All BGP routes are summarized or non-summarized routes.
- Origin attributes (IGP, EGP, or incomplete) are the same.
- MED values are the same.
- All BGP routes are EBGP or IBGP routes.
- IGP metric values within an AS are the same.
- AS_Path attributes are the same.

After the **maximum load-balancing ebgp** *number* command is run, only EBGP routes implement load balancing. After the **maximum load-balancing ibgp** *number* command is run, only IBGP routes implement load balancing. If neither **ebgp** nor **ibgp** is configured, both EBGP and IBGP routes participate in load balancing, and the number of EBGP routes for load balancing is the same as the number of IBGP routes for load balancing.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

By default, after the **maximum load-balancing ebgp** *number* or **maximum load-balancing ibgp** *number* command is run on a BGP device, the BGP device does not change the next-hop of a route to itself before advertising the route to a peer, regardless of whether the route participates in load balancing.

Precautions

If the **maximum load-balancing** *number*, **maximum load-balancing ebgp** *number*, or **maximum load-balancing ibgp** *number* command is run multiple times, only the latest configuration takes effect.

The **maximum load-balancing** *number* command cannot be configured together with the **maximum load-balancing ebgp** *number* or **maximum load-balancing ibgp** *number* command.

Example

Set two equal-cost routes to a specified destination.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] maximum load-balancing 2
```

9.8.92 maximum load-balancing eibgp

Function

The **maximum load-balancing eibgp** command configures the maximum number of EBGP and IBGP routes for load balancing.

The **undo maximum load-balancing eibgp** command deletes the configured maximum number of EBGP and IBGP routes for load balancing.

By default, the maximum number of EBGP and IBGP routes for load balancing is not configured.

Format

maximum load-balancing eibgp *number* [**ecmp-nexthop-changed**]

undo maximum load-balancing eibgp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the maximum number of equal-cost EBGP and IBGP routes.	The value is an integer that ranges from 1 to 4 on the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204, from 1 to 8 on the AR2220, AR2220E, AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80, SRU100E), AR2240C, AR3600 (using SRUX5), and AR3200 (using SRU40, SRU60, SRU80, SRU100E) series, and from 1 to 16 on the AR2240 (using SRU200, SRU200E, or SRU400), AR3600 (using SRUX5), and AR3200 (using SRU200, SRU200E, or SRU400) series.
ecmp-nexthop-changed	Configures a BGP device to change the next-hop addresses of only the routes that participate in load balancing to its address.	-

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **maximum load-balancing eibgp** command is run in the BGP-VPN instance view, load balancing is implemented among equal-cost BGP VPN routes, including EBGP and IBGP routes.

After BGP load balancing is configured, BGP routes that meet the following conditions and have the same AS_Path attribute will become equal-cost routes and implement load balancing:

- PrefVal values are the same.
- Local_Pref attributes are the same.

- All BGP routes are summarized or non-summarized routes.
- Accumulated Interior Gateway Protocol (AIGP) metric values are the same.
- Lengths of AS_Path attributes are the same.
- Origin types (IGP, EGP, or Incomplete) are the same.
- Multi_Exit Discriminator (MED) values are the same.
- Protocol priorities are the same.

  By default, EBGP and IBGP routes have the same protocol priority (255). If the protocol priorities of EBGP and IBGP routes are changed to be different, for example, using a route-policy, load balancing cannot be implemented among EBGP and IBGP routes.

Load balancing cannot be implemented among the following routes:

- Blackhole routes and non-blackhole routes
- Labeled routes and non-labeled routes
- Local routes and non-local routes

Example

Set the maximum number of EBGP and IBGP routes for load balancing to 3.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpna
[Huawei-vpn-instance-vpna] route-distinguisher 100:1
[Huawei-vpn-instance-vpna-af-ipv4] quit
[Huawei-vpn-instance-vpna] quit
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpn-instance vpna
[Huawei-bgp-vpna] maximum load-balancing eibgp 3
```

9.8.93 network (BGP)

Function

The **network** command configures BGP to statically add routes in the IP routing table to the BGP routing table and advertise these routes to peers.

The **undo network** command deletes the routes statically added to the BGP routing table.

By default, BGP does not statically add routes in the IP routing table to the BGP routing table.

Format

network { *ipv4-address* [*mask* | *mask-length*] | *ipv6-address prefix-length* } [**route-policy** *route-policy-name*]

undo network { *ipv4-address* [*mask* | *mask-length*] | *ipv6-address prefix-length* }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the route to be imported by BGP.	It is in dotted decimal notation.
mask	Specifies the IP address mask. If no mask is specified, the IP address is considered as a classful address.	It is in dotted decimal notation.
mask-length	Specifies the mask length of the IP address. If no mask length is specified, the IP address is considered as a classful address.	It is an integer ranging from 0 to 32.
ipv6-address	Specifies the IPv6 address of the route to be imported by BGP.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of the IPv6 network address advertised by BGP.	It is an integer ranging from 0 to 128.
route-policy *route-policy-name*	Specifies the name of the route-policy that is used for route import.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP itself cannot discover routes. Instead, it imports routes discovered by other protocols such as an IGP or static routes into the BGP routing table. These

imported routes then are transmitted within an AS or between ASs. Before adding routes to the BGP routing table, BGP filters these routes by the routing protocol. If routes in the local IP routing table need to be statically added to the BGP routing table and then advertised, you can use the **network** command.

The Origin attribute of the routes imported into the BGP routing table by using the **network** command is IGP.

If a route with a specific prefix or mask is added to the BGP routing table by using the **network** command, this route is the optimal route selected from all types of protocol routes. Unlike the **network** command, the **import-route (BGP)** command is used to add all routes of a particular protocol such as RIP, OSPF, IS-IS, static route, or direct route to the BGP routing table.

Precautions

The **network** command is used to import exactly-matching routes. This means that only the routes in the local IP routing table that exactly match the specified destination address and prefix length can be added to the BGP routing table. If *mask* is not specified, routes are exactly matched against the natural network mask.

When using the **undo network** command to delete the existing configuration, specify a correct mask.

Example

Configure BGP to import the local route 10.0.0.0/16.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] network 10.0.0.0 255.255.0.0
```

9.8.94 nexthop recursive-lookup (BGP)

Function

The **nexthop recursive-lookup** command configures next hop iteration based on the routing policy.

The **undo nexthop recursive-lookup** command restores the default setting.

By default, BGP does not perform next hop iteration based on the routing policy.

Format

nexthop recursive-lookup route-policy *route-policy-name*

undo nexthop recursive-lookup route-policy

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Indicates the name of a routing policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP needs to iterate indirect next hops. If an indirect next hop is not iterated based on a routing policy, the BGP route may be iterated to an incorrect forwarding path, causing traffic loss. Therefore, next hops should be iterated according to certain conditions to control the iterated routes.

The **nexthop recursive-lookup route-policy** *route-policy-name* command can be run to control the iterated next hop based on a routing policy. If an iterated route is filtered out by the routing policy, the route is considered unreachable. In this manner, the BGP route will not be iterated to an incorrect forwarding path.

Prerequisites

The next hop to which a BGP route is iterated has been determined and a routing policy has been configured.

NOTICE

Before configuring a routing policy, ensure that all desirably iterated routes cannot be filtered out by the routing policy. If some desirably iterated routes are filtered out by the routing policy, the BGP route may be considered unreachable by mistake and traffic cannot be forwarded over the route.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The command does not apply to the routes received from directly connected EBGP peers or LinkLocal peers.

Example

Configure next hop iteration based on the routing policy **rp_nexthop**.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] nexthop recursive-lookup route-policy rp_nexthop
```

9.8.95 nexthop recursive-lookup delay

Function

The **nexthop recursive-lookup delay** command configures the delay in responding to changes of the next hop.

The **undo nexthop recursive-lookup delay** command restores the default setting.

By default, the delay in responding to changes of the next hop is not configured.

Format

nexthop recursive-lookup delay [*delay-time*]

undo nexthop recursive-lookup delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay in responding to changes of the next hop.	The value is an integer that ranges from 1 to 100, in seconds. The default value is 5 seconds.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-IPv4 multicast address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the route path on the upstream of a PE connected to an RR changes, if the PE detects that the iterated next hop becomes unreachable before the RR instructs the PE to switch the route, the PE withdraws the original optimal route advertised to its connected CE. After the RR re-advertises the switched route to the PE, the PE re-advertises an optimal route to the CE after route selection. During the route switchover, a huge volume of traffic will be dropped. If the **nexthop recursive-lookup delay** command is run on the PE to delay responding to the next hop unreachable event and to respond to this event only after the RR advertises the switched route, the volume of lost traffic will be reduced during route switchover.

Example

Set the delay in responding to changes of the next hop to 10s.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] nexthop recursive-lookup delay 10
```

9.8.96 nexthop recursive-lookup non-critical-event delay

Function

The **nexthop recursive-lookup non-critical-event delay** command enables a device to respond to non-urgent BGP next-hop iteration changes after a specified delay time.

The **undo nexthop recursive-lookup non-critical-event delay** command enables a device to immediately respond to non-urgent BGP next-hop iteration changes.

By default, a device immediately responds to non-urgent BGP next-hop iteration changes.

Format

nexthop recursive-lookup non-critical-event delay [*delay-time*]

undo nexthop recursive-lookup non-critical-event delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay time.	The value is an integer that ranges from 1 to 100, in seconds. The default value is 5.

Views

BGP view, BGP-IPv4 unicast address family view, or BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If repeated iteration causes the BGP next hop to frequently change on a device, the device frequently selects and advertises routes. To prevent unwanted re-routing and route advertisement, run the **nexthop recursive-lookup delay** command to enable the device to respond to BGP next-hop iteration changes after a specified delay time. The iteration results are as follows:

- Urgent iteration result change: The iterated next hop is changed, and BGP route reachability is also changed. For example, if a fault occurs on a network, a device finds no next-hop route or tunnel to which a BGP route is iterated. As a result, traffic is interrupted.
- Non-urgent iteration result change: The iterated next hop is changed, and BGP route reachability is not affected. For example, after the interface or type of a tunnel to which the next hop of a BGP route is iterated is changed, traffic keeps traveling over the BGP route.

To delay a response to the non-urgent iteration change, run the **nexthop recursive-lookup non-critical-event delay** command, not the **nexthop recursive-lookup delay** command.

Configuration Impact

After the **nexthop recursive-lookup delay** command is run, the device delays responses to all next-hop iteration changes. After the **nexthop recursive-lookup non-critical-event delay** command is run, the device delays responses only to non-urgent BGP next-hop iteration changes. If both commands are run, the **nexthop recursive-lookup non-critical-event delay** command takes precedence over the **nexthop recursive-lookup non-critical-event delay** command. **Table 9-191** provides examples of the two commands.

Table 9-191 Functions and their descriptions

Example	Description
[Huawei-bgp] **nexthop recursive-lookup delay**	The device responds to all BGP next-hop iteration changes after a 5-second delay.
[Huawei-bgp] **nexthop recursive-lookup non-critical-event delay**	The device immediately responds to urgent BGP next-hop iteration changes and responds to non-urgent BGP next-hop iteration changes after a 5-second delay.
[Huawei-bgp] **nexthop recursive-lookup delay 3**	The device responds to all BGP next-hop iteration changes after a 3-second delay.
[Huawei-bgp] **nexthop recursive-lookup non-critical-event delay 6**	The device immediately responds to urgent BGP next-hop iteration changes and responds to non-urgent BGP next-hop iteration changes after a 6-second delay.
[Huawei-bgp] **nexthop recursive-lookup delay** [Huawei-bgp] **nexthop recursive-lookup non-critical-event delay**	The device responds to all BGP next-hop iteration changes after a 5-second delay.

 Copyright © Huawei Technologies Co., Ltd.

Example	Description
[Huawei-bgp] **nexthop recursive-lookup delay 3** [Huawei-bgp] **nexthop recursive-lookup non-critical-event delay**	The device responds to urgent BGP next-hop iteration changes after a 3-second delay and responds to non-urgent BGP next-hop iteration changes after a 5-second delay.
[Huawei-bgp] **nexthop recursive-lookup delay 3** [Huawei-bgp] **nexthop recursive-lookup non-critical-event delay 6**	The device responds to urgent BGP next-hop iteration changes after a 3-second delay and responds to non-urgent BGP next-hop iteration changes after a 6-second delay.
[Huawei-bgp] **nexthop recursive-lookup delay** [Huawei-bgp] **nexthop recursive-lookup non-critical-event delay 6**	The device responds to urgent BGP next-hop iteration changes after a 5-second delay and responds to non-urgent BGP next-hop iteration changes after a 6-second delay.

Precautions

The delay time specified in the **nexthop recursive-lookup non-critical-event delay** command must be greater than or equal to that specified in the **nexthop recursive-lookup delay** command if both commands are run.

Example

Enable the device to respond to non-urgent BGP next-hop iteration changes after a **10**-second delay.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] nexthop recursive-lookup non-critical-event delay 10
```

Related Topics

9.8.95 nexthop recursive-lookup delay

9.8.97 out-delay

Function

The **out-delay** command configures a delay for sending Update packets to all BGP peers.

The **undo out-delay** command deletes the configured delay value.

The default delay value is 0, indicating that the intermediate device on the primary path sends Update packets without a delay.

Format

out-delay *delay-value*

undo out-delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay for sending Update packets.	The value is an integer ranging from 0 to 3600, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario with both primary and backup routes, traffic may be lost after it switches back to the primary path. Use a VPN FRR scenario as an example. PE3 and CE connect both to PE1 and PE2. The primary path is PE3 -> PE1 -> CE, and the backup path is PE3 -> PE2 -> CE. CE uses BGP to communicate with PE1 and PE2. FRR is configured on PE3. If PE1 restarts or the link between PE3 and PE1 fails, traffic switches from the primary path to the backup path. After the primary path recovers, traffic switches back to the primary path. If PE3 completes refreshing forwarding entries before PE1 does, PE1 may temporarily fail to forward traffic from PE3, and packet loss may occur. The severity of packet loss is proportional to the number of routes stored on PE1.

To solve this problem, run the **out-delay** command on PE1 to configure a delay for sending Update packets. An appropriate delay ensures that traffic switches back to the primary path after PE1 completes refreshing forwarding entries.

To configure a delay for sending Update packets to all BGP peers, run the **out-delay** command. To configure a delay for sending Update packets to a specified BGP peer or peer group, run the **peer out-delay** command.

Precautions

If you run the **out-delay** command more than once, the latest configuration overrides the previous one.

If the **out-delay** and **peer route-update-interval** commands are both configured, only the **out-delay** command takes effect.

If a network has high route convergence requirements, do no use the **out-delay** command.

Example

Set the delay for sending Update packets to all BGP peers to 300s in the BGP view.

```
<Huawei> system-view
[Huawei] bgp 100
```

```
[Huawei-bgp] out-delay 300
```

Related Topics

9.8.128 peer out-delay

9.8.98 peer advertise-community

Function

The **peer advertise-community** command configures a device to advertise a community attribute to its peer or peer group.

The **undo peer advertise-community** command restores the default setting.

By default, a device advertises no community attribute to its peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IP address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BPG-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer advertise-community** command is used to configure a device to advertise a community attribute to its peer or peer group. If a device advertises a community attribute to its peer group, all the members of the peer group will inherit the configuration. This simplifies the application of routing policies and facilitates route maintenance and management.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Before publishing the BGP group properties through the **peer advertise-community** Command, a specific community attribute has been defined by in a routing policy.

Example

Configure a device to advertise a community attribute to its peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 advertise-community
```

9.8.99 peer advertise-ext-community

Function

The **peer advertise-ext-community** command enables a device to advertise an extended community attribute to its peer or peer group.

The **undo peer advertise-ext-community** command restores the default setting.

By default, a device does not advertise extended community attribute to its peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-ext-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-ext-community**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IP address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer advertise-ext-community** command is used to enable a device to advertise an extended community attribute to a specified peer or peer group. If a device advertises an extended community attribute to a specified peer group, all the members of the peer group will inherit the configuration. This simplifies the application of routing policies and facilitates route maintenance and management.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A specific extended community attribute has been defined in a routing policy.

Example

Configure a device to advertise an extended community attribute to its peer.

```
<Huawei> system-view
[Huawei] bgp 100
```

```
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 advertise-ext-community
```

9.8.100 peer allow-as-loop

Function

The **peer allow-as-loop** command sets the number of local AS number repetitions.

The **undo peer allow-as-loop** command restores the default setting.

By default, the local AS number cannot be repeated.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop** [*number*] [**global-as** [**vpn-as**]]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop** [*number*] [**global-as** [**vpn-as**]]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
number	Specifies the number of local AS number repetitions.	The value is an integer ranging from 1 to 10. The default value is 1.
global-as	Indicates a global AS number.	-
vpn-as	Indicates a VPN instance AS number.	-

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- *ipv4-address* is valid only in the BGP view, BPG-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.
- The **global-as** and **vpn-as** parameters apply only to BGP VPN instance IPv4 and BGP VPN instance IPv6 address family views.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP uses AS numbers to detect routing loops. The AS numbers in the AS_Path of each received route are matched against the local AS number configured using the **bgp** command, the fake AS number configured using the **peer fake-as** command, and the VPN instance AS number configured using the **as-number** command. The largest number of times any of the configured AS numbers is repeated is considered as the maximum number. In the Hub and Spoke networking, if EBGP runs between a Hub-PE and a Hub-CE on a Hub site, the route sent from the Hub-PE to the Hub-CE carries the AS number of the Hub-PE. If the Hub-CE sends a routing update to the Hub-PE, the Hub-PE will deny it because the routing update contains the AS number of the Hub-PE.

To ensure proper route transmission in the Hub and Spoke networking, configure all the BGP peers on the path, along which the Hub-CE advertises private network routes to the Spoke-CE, to accept the routes in which the AS number repeats once.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer allow-as-loop** command is run for a peer or peer group multiple times, the latest configuration overrides the previous one.

Example

Set the number of local AS number repetitions to 2.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 allow-as-loop 2
```

9.8.101 peer as-number

Function

The **peer as-number** command creates a peer or configures an AS number for a specified peer group.

The **undo peer as-number** command deletes a specified peer or the AS number of a specified peer group.

By default, no BGP peer is configured, and no AS number is specified for a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-number** { *as-number-plain* | *as-number-dot* }

peer *group-name* **as-number** { *as-number-plain* | *as-number-dot* } [**optional-as** { *optional-as-number-plain* | *optional-as-number-dot* } & <1-5>]

undo peer { *group-name* **as-number** | *ipv4-address* | *ipv6-address* }

undo peer *group-name* **as-number** { *as-number-plain* | *as-number-dot* } [**optional-as** { *optional-as-number-plain* | *optional-as-number-dot* } & <1-5>]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer. The IPv4 address can be the IP address of an interface that is directly connected to the peer or the IP address of a loopback interface of the reachable peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Parameter	Description	Value
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
optional-as-number-plain	Specifies an integral optional AS number.	The value is an integer ranging from 1 to 4294967295.
optional-as-number-dot	Specifies an optional AS number in dotted notation.	The value is in the format of *x.y*, where *x* and *y* are integers ranging from 1 to 65535 and from 0 to 65535, respectively.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.
- **optional-as** is valid only in the BGP view and BGP-VPN instance IPv4 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer** *ipv4-address* **as-number** { *as-number-plain* | *as-number-dot* } command is used to create a BGP peer.

The **peer** *group-name* **as-number** { *as-number-plain* | *as-number-dot* } command is used to configure an AS number for a specified peer group.

Dynamic peers on the same network segment must be added to the same peer group. If the dynamic peers reside in different ASs, run the **peer** *group-name* **as-number** { *as-number-plain* | *as-number-dot* } **optional-as** { *optional-as-number-plain* | *optional-as-number-dot* } & <1-5> command to configure an optional AS number for the peer group.

Precautions

If a peer does not join any peer group or the peer group to which a peer belongs is not configured with an AS number, deleting the AS number of the peer will reset the peer relationship.

If a peer in a peer group is not configured with an AS number, deleting the AS number of the peer group will interrupt the connection on the peer.

The AS number for external session group cannot be the same as the local AS number.

Example

Set the AS number to 100 for IPv4 peer 10.1.1.1.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.1 as-number 100
```

Set the AS number to 100 for a peer group named test.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] group test
[Huawei-bgp] peer test as-number 100
```

9.8.102 peer as-path-filter

Function

The **peer as-path-filter** command configures a BGP route filtering policy based on an AS_Path list for a peer or peer group.

The **undo peer as-path-filter** command cancels the existing configuration.

By default, no route filtering policy based on an AS_Path list is configured for a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
as-path-filter-number	Specifies the number of an AS_Path filter.	The value is an integer ranging from 1 to 256.
as-path-filter-name	Specifies the name of an AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters. It cannot be all numbers. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a route filtering policy to received routes.	-
export	Applies a route filtering policy to routes to be advertised.	-

NOTE

- *ipv4-address* is valid only in the BGP view, BPG-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer as-path-filter** command is used to apply a route filtering policy based on an AS_Path list to BGP routes, the routers that do not match the policy are filtered out.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

The **ip as-path-filter** command has been run to define an AS-Path filter.

Precautions

Only one AS_Path filter can be used to filter the routes received from the same peer. Similarly, only one AS_Path filter can be used to filter routes to be advertised to the same peer.

Creating an AS_Path filter before it is referenced is recommended. By default, the command in an IPv4 address family cannot reference a non-existent AS_Path filter, but the command in an IPv6 address family can reference a non-existent AS_Path filter.

Example

Configure an AS_Path filter for a peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 as-path-filter 3 export
```

9.8.103 peer bfd

Function

The **peer bfd** command sets BFD detection parameters for a peer or peer group.

The **undo peer bfd** command restores default BFD detection parameter values.

By default, the interval for sending BFD packets is 1000 ms, the interval for receiving BFD packets is 1000 ms, and the local detection multiplier is 3.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* | **wtr** *wtr-value* }*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **bfd** { **min-tx-interval** | **min-rx-interval** | **detect-multiplier**| **wtr** }*

undo peer { *group-name* | *ipv4-address* } **bfd** { **min-tx-interval** *min-tx-interval* | **min-rx-interval** *min-rx-interval* | **detect-multiplier** *multiplier* | **wtr** *wtr-value* }*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
min-tx-interval *min-tx-interval*	Specifies the interval at which BFD packets are sent.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-rx-interval *min-rx-interval*	Specifies the interval at which BFD packets are received.	The value is an integer ranging from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
detect-multiplier *multiplier*	Specifies the local detection time multiplier.	The value is an integer ranging from 3 to 50.
wtr *wtr-value*	Specifies the interval for waiting for the BFD session to restore.	The value is an integer that ranges from 1 to 60, in minutes. By default, the value is 0 minute, indicating no waiting.

Views

BGP view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD provides millisecond-level fault detection. It helps BGP to detect faults in neighboring devices or links more quickly, and instructs BGP to recalculate routes for correct packet forwarding. The **peer bfd** command can be used to set the values of BFD session parameters on a specified interface.

The BFD configuration of a peer takes precedence over that of the peer group to which the peer belongs. If BFD is not configured on a peer and the peer group to which the peer belongs is enabled with BFD, the peer will inherit the BFD configurations of the peer group.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A BFD session can be established only when the corresponding BGP session is in the Established state.

Precautions

If the **peer bfd** command is run multiple times, the latest configuration overwrites the previous one. The BFD session uses the latest parameters as the detection parameters.

Assume that BFD is configured on a peer group. If the **peer bfd block** command is not run on members of the peer group, the members will establish BFD sessions.

If BFD parameters are set on a peer, a BFD session will be established by using the BFD parameters on the peer.

If the peer's interface is a tunnel interface, the **peer bfd** command cannot be used to configure BFD for BGP. For example, BFD for EBGP cannot be configured in DSVPN scenarios.

Example

Configure BFD and set detection parameters on peer 10.2.2.9.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.2.2.9 as-number 200
[Huawei-bgp] peer 10.2.2.9 bfd min-tx-interval 100 min-rx-interval 100 detect-multiplier 5
```

Related Topics

9.8.105 peer bfd enable

9.8.26 display bgp bfd session

9.8.55 display bgp peer

9.8.29 display bgp group

9.8.104 peer bfd block

Function

The **peer bfd block** command prevents a peer from inheriting the BFD function of its peer group.

The **undo peer bfd block** command restores the default configuration.

By default, a peer inherits the BFD function from its peer group.

Format

peer *ipv4-address* **bfd block**

peer *ipv6-address* **bfd block**

undo peer *ipv6-address* **bfd block**

undo peer *ipv4-address* **bfd block**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

BGP view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BFD provides millisecond-level fault detection. It helps BGP to detect faults in neighboring devices or links more quickly, and instructs BGP to recalculate routes for correct packet forwarding. If a peer group is configured with BFD, all members of the peer group will establish BFD sessions. The **peer bfd block** command can be used to prevent a peer from inheriting the BFD function from its peer group.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A BFD session has been established.

Precautions

After the **peer bfd block** command is run on a peer, the corresponding BFD session on the peer is deleted. As a result, fast link fault detection cannot be implemented.

The **peer bfd block** command and the **peer bfd enable** command are mutually exclusive. After the **peer bfd block** command is run, related BFD sessions are automatically deleted.

Example

Prevent peer 10.2.2.9 from inheriting the BFD function of its peer group.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.2.2.9 as-number 200
[Huawei-bgp] peer 10.2.2.9 bfd block
```

Related Topics

9.8.105 peer bfd enable

9.8.55 display bgp peer
9.8.29 display bgp group

9.8.105 peer bfd enable

Function

The **peer bfd enable** command enables BFD for peers or a peer group.

The **undo peer bfd enable** command disables BFD for peers or a peer group.

By default, BFD is disabled for peers or a peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **bfd enable** [**single-hop-prefer**]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **bfd enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
single-hop-prefer	Indicates that single-hop BFD sessions are preferentially established. **single-hop-prefer** takes effect only on IBGP peers. By default, **single-hop-prefer** is not specified, multi-hop sessions are established between direct IBGP peers (Huawei devices). To interconnect a Huawei device and a non-Huawei device that defaults the sessions between IBGP peers to single-hop, configure **single-hop-prefer** in the command.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP uses BFD to quickly detect faults in links between BGP4 peers. This accelerates network convergence. The **peer bfd enable** command is used to configure a device to establish a BFD session with its peer or peer group by using default detection parameter values.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A BFD session can be established only when the corresponding BGP peer relationship is in the Established state.

Precautions

The BFD configuration of a peer takes precedence over that of the peer group to which the peer belongs. If BFD is not configured on a peer and the peer group to which the peer belongs is enabled with BFD, the peer inherits the BFD configurations from the peer group.

Before enabling BFD on a BGP peer, enable BFD in the system view. If no BFD detection parameter is specified, a BFD session is established by using default parameter values.

NOTE

The **peer bfd block** command and the **peer bfd enable** command are mutually exclusive.

Example

Configure BFD for peer 10.2.2.9.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.2.2.9 as-number 200
[Huawei-bgp] peer 10.2.2.9 bfd enable
```

Related Topics

9.8.55 display bgp peer

9.8.29 display bgp group

9.8.26 display bgp bfd session

9.8.103 peer bfd

9.8.104 peer bfd block

 Copyright © Huawei Technologies Co., Ltd.

9.8.106 peer capability-advertise

Function

The **peer capability-advertise** command enables a BGP device to advertise optional BGP capabilities to its peer.

The **undo peer capability-advertise** command restores the default setting.

By default, a BGP device advertises route-refresh and 4-byte AS number to its peer.

Format

peer { *group-name* | *ipv4-address* } **capability-advertise** { **4-byte-as** | **route-refresh** | **conventional** }

peer *ipv6-address* **capability-advertise** { **4-byte-as** | **route-refresh** }

undo peer { *group-name* | *ipv4-address* } **capability-advertise** { **4-byte-as** | **route-refresh** | **conventional** }

undo peer *ipv6-address* **capability-advertise** { **4-byte-as** | **route-refresh** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
4-byte-as	Indicates the 4-byte AS number capability.	-
route-refresh	Indicates the route-refresh capability.	-
conventional	Indicates the regular router capability.	-

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer capability-advertise route-refresh** command is used to configure a device to advertise the route-refresh capability to its peer.

The **peer capability-advertise conventional** command is used to configure a device to advertise the regular router capability to its peer. If **conventional** is specified in the command, the router does not have all extension functions such as route-refresh capability, GR capability, and multi-address family negotiation. This allows the router to be compatible with routers of earlier versions.

The **peer capability-advertise 4-byte-as** command is used to configure a device to advertise the 4-byte AS number capability to its peer. If AS number resources are used up, this command can be used to configure devices to use 4-byte AS numbers.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

The corresponding BGP session must be in the Established state.

Precautions

If you enable or disable the route-refresh, general router, or 4-byte AS number function, the BGP peer relationship will be re-established, which can lead to a temporary network interruption. Therefore, exercise caution when running the related commands.

Example

Configure a BGP device to advertise the route-refresh capability to its peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.89.2.33 as-number 100
[Huawei-bgp] peer 10.89.2.33 capability-advertise route-refresh
```

9.8.107 peer capability-advertise orf

Function

The **peer capability-advertise orf** command configures a BGP device to advertise the prefix-based outbound route filtering (ORF) capability to its peer or peer group.

The **undo peer capability-advertise orf** command restores the default setting.

By default, a BGP device does not advertise the prefix-based ORF capability to its peer or peer group.

Format

peer { *group-name* | *ipv4-address* } **capability-advertise orf** [**non-standard-compatible**] **ip-prefix** { **both** | **receive** | **send** } [**standard-match**]

undo peer { *group-name* | *ipv4-address* } **capability-advertise orf** [**non-standard-compatible**] **ip-prefix** { **both** | **receive** | **send** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
non-standard-compatible	Indicates that ORF supported by Huawei devices is compatible with other devices.	-
both	Indicates that a peer or peer group is allowed to send and receive ORF packets.	-
receive	Indicates that a peer or peer group is allowed only to receive ORF packets.	-
send	Indicates that a peer or peer group is allowed only to send ORF packets.	-
standard-match	Filters routes according to the prefix matching rules defined in an RFC.	-

Views

BGP view or BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ORF enables a BGP device to send to its BGP peer a set of routing policies that can be used by its peer to filter out unwanted routes during route advertisement.

Prerequisites

BGP peer relationships have been established using the **peer as-number** command.

Precautions

Because the ORF capability code supported by other devices may differ from that defined in the associated RFC, set the **non-standard-compatible** parameter to implement interworking between a Huawei device and a non-Huawei device. If the Huawei device adopts the ORF capability defined in the associated RFC but the non-Huawei device adopts its own ORF capability, ORF negotiation fails.

Example

Configure a BGP device to advertise the prefix-based ORF capability to its peer or peer group.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 192.168.1.1 as-number 200
[Huawei-bgp] peer 192.168.1.1 capability-advertise orf ip-prefix both
```

9.8.108 peer connect-interface

Function

The **peer connect-interface** command specifies a source interface from which BGP packets are sent, and a source address used for initiating a connection.

The **undo peer connect-interface** command restores the default setting.

By default, the outbound interface of a BGP packet serves as the source interface of a BGP packet.

Format

peer { *group-name* | *ipv4-address* } **connect-interface** *interface-type interface-number* [*ipv4-source-address*]

peer { *group-name* | *ipv6-address* } **connect-interface** *interface-type interface-number* [*ipv6-source-address*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **connect-interface**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of an interface.	-
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv4-source-address	Specifies an IPv4 source address used for establishing a connection.	It is in dotted decimal notation.
ipv6-source-address	Specifies an IPv6 source address used for establishing a connection.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command is used in the following scenarios:

- To establish a BGP peer connection between two indirectly connected physical interfaces, the **peer connect-interface** command must be run on both sides.

  To establish a BGP peer connection between a local loopback interface and a remote interface, the loopback interface must be specified as the source

interface in the command. To establish a BGP peer connection between a local physical interface and a remote interface, the physical interface must be specified as the source interface in the command.

- If multiple IP addresses are configured for the physical interface that needs a BGP peer connection established with a remote interface, the **peer connect-interface** command must be run, with *ipv4-source-address* or *ipv6-source-address* set to the source IP address.
- If two devices need multiple BGP peer connections established through different interfaces, the **peer connect-interface** command must be run for each BGP peer connection, with the source interface specified.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

Running the **peer connect-interface** command causes the teardown and re-establishment of peer relationships.

NOTE

Because the BGP peer relationships in various address families on the same device share one TCP connection, **connect-interface** configured in the BGP view can be inherited in the IPv4 unicast address family.

To enable a device to send BGP packets even if its physical interface fails, you can configure the device to use a loopback interface as the source interface of the BGP packets. When configuring a device to use a loopback interface as the source interface of BGP packets, note the following points:

- The loopback interface of the device's BGP peer must be reachable.
- In the case of an EBGP connection, the **peer ebgp-max-hop** command needs to be run to enable the two devices to establish an indirect peer relationship.

NOTE

When loopback interfaces are used to establish a BGP connection, you are recommended to run the **peer connect-interface** command at both ends of the connection to ensure that the connection is correctly established. If this command is run on only one end, the BGP connection may fail to be established.

If the specified interface borrows the IP address of another interface and then the IP address of the specified interface is changed, BGP still uses the borrowed IP address to keep the connection if no connection reestablishment is triggered, and data receiving and sending is not affected; if connection reestablishment is triggered, BGP uses the new IP address to reestablish the connection.

Example

Specify a source interface for sending BGP packets and a source address for initiating a connection.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.16.2.3 as-number 100
[Huawei-bgp] peer 10.16.2.3 connect-interface gigabitethernet 1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.8.113 peer ebgp-max-hop

9.8.109 peer connected-check-ignore

Function

The **peer connected-check-ignore** command configures a device not to check the hop count when establishing a one-hop EBGP peer relationship using a loopback interface address.

The **undo peer connected-check-ignore** command cancels the configuration.

By default, a device checks the hop count when establishing a one-hop EBGP peer relationship using a loopback interface address.

Format

peer{ *group-name* | *ipv4-address* | *ipv6-address* } **connected-check-ignore**

undo peer{ *group-name* | *ipv4-address* | *ipv6-address* } **connected-check-ignore**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

BGP view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

NOTE

AR150&160&200 series does not support BGP-VPNv4 address family view.

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To allow one-hop EBGP peer relationships to be established using loopback interface addresses, run the **peer connected-check-ignore** command or the **peer ebgp-max-hop** command (in which *hop-count* is greater than or equal to 2).

Example

Configure the device not to check the hop count when establishing a one-hop EBGP peer relationship using a loopback interface address.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.2 as-number 200
[Huawei-bgp] peer 1.1.1.2 connected-check-ignore
```

9.8.110 peer default-route-advertise

Function

The **peer default-route-advertise** command configures a BGP device to advertise a default route to its peer or peer group.

The **undo peer default-route-advertise** command restores the default setting.

By default, a BGP device does not advertise default routes to its peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*] [**conditional-route-match-all** { *ipv4-address1* { *mask1* | *mask-length1* } } &<1-4> | **conditional-route-match-any** { *ipv4-address2* { *mask2* | *mask-length2* } } &<1-4>]

peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*] [**conditional-route-match-all** { *ipv6-address1 prefix-length1* } &<1-4> | **conditional-route-match-any** { *ipv6-address2 prefix-length2* } &<1-4>]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
conditional-route-match-all	Configures the BGP device to send default routes to a peer or peer group when the routing table contains all conditional routes. **NOTE** **conditional-route-match-all** is only valid in the BGP view, BGP-IPv4 unicast address family view, and BGP-VPN instance IPv4 address family view.	-
ipv4-address1	Specifies the IPv4 address of conditional routes.	The value is in dotted decimal notation.
ipv6-address1	Specifies the IPv6 address of conditional routes.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length1	Specifies the IPv6 prefix range using the mask length.	The value is an integer that ranges from 0 to 128. If ::0 less-equal 128 is used, all IPv6 addresses will be matched.
prefix-length2	Specifies the IPv6 prefix range using the mask length.	The value is an integer that ranges from 0 to 128. If ::0 less-equal 128 is used, all IPv6 addresses will be matched.
mask1	Specifies the mask of conditional routes.	The value is in dotted decimal notation.
mask-length1	Specifies the mask length of conditional routes.	The value is an integer that ranges from 0 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
conditional-route-match-any	Configures the BGP device to send default routes to a peer or peer group when the routing table contains any conditional route. **NOTE** **conditional-route-match-any** is only valid in the BGP view, BGP-IPv4 unicast address family view, and BGP-VPN instance IPv4 address family view.	-
ipv4-address2	Specifies the IPv4 address of conditional routes.	The value is in dotted decimal notation.
ipv6-address2	Specifies the IPv6 address of conditional routes.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
mask2	Specifies the mask of conditional routes.	The value is in dotted decimal notation.
mask-length2	Specifies the mask length of conditional routes.	The value is an integer that ranges from 0 to 32.

NOTE

- *ipv4-address* is only valid in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is only valid in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Default routes are commonly used on a network that meets the following conditions:

- Each device has multiple EBGP peers and receives all routes on the network from each EBGP peer.
- There are multiple route reflectors (RRs), and each RR receives all routes on the network.

If load balancing is not implemented on the network, a BGP peer receives at most one copy of active routes on the network. If load balancing is implemented on the network, the number of active routes received by a BGP peer will be increased by multiple times, causing the number of routes on the network to sharply increase. To greatly reduce the number of routes on such a network, configure a BGP device to advertise only default routes to its BGP peer and use default routes for traffic load balancing.

Prerequisites

BGP peer relationships have been established using the **peer as-number** command.

Precautions

After this command is run, a BGP device sends a default route with the next hop as itself to its peer or peer group regardless of whether default routes exist in the routing table.

Example

Configure a BGP device to advertise a default route to its peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 default-route-advertise
```

Related Topics

9.8.24 default-route imported

9.8.111 peer description (BGP)

Function

The **peer description** command configures a description for a peer or peer group.

The **undo peer description** command deletes the description of a peer or peer group.

By default, no description is configured for a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **description** *description-text*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **description**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
description-text	Specifies a description, which can be letters and digits.	The value is a string of 1 to 80 characters, with spaces supported.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer description** can be used to configure a description for a peer or peer group, which facilitates management of peers or peer groups. The description records information about the peer or peer group, such as the VPN instance to which the peer or peer group belongs, and devices that establish peer relationships with the peer or peer group.

Precautions

The description configured by using the **peer description** command for a peer is displayed from the first non-space character, and a maximum of 80 characters can be displayed.

Follow-up Procedure

You can run **display bgp peer** *ipv4-address* **verbose** command can be used to view the description of a peer.

Example

Configure a description for a peer group named group1.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] group group1
[Huawei-bgp] peer group1 description ISP1
```

9.8.112 peer discard-ext-community (BGP)

Function

The **peer discard-ext-community** command configures a BGP device to discard the extended community attributes carried by routes received from a specified peer.

The **undo peer discard-ext-community** command restores the default setting.

By default, BGP does not discard the extended community attributes carried by routes received from a specified peer.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **discard-ext-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **discard-ext-community**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Peer relationships have been established using the **peer as-number** command.

After the **peer discard-ext-community** command is run on a peer, the peer discards the extended community attributes carried by routes.

Example

Configure a BGP device to discard the extended community attribute carried by a route.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 discard-ext-community
```

9.8.113 peer ebgp-max-hop

Function

The **peer ebgp-max-hop** command configures a BGP device to establish an EBGP peer relationship with a peer on an indirectly-connected network and set the maximum number of hops between the two devices.

The **undo peer ebgp-max-hop** command restores the default setting.

By default, an EBGP connection can be set up only on a directly-connected physical link.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **ebgp-max-hop**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hop-count	Specifies the maximum number of hops.	The value is an integer ranging from 1 to 255. The default value is 255. If the maximum number of hops is 1, a device cannot establish an EBGP connection with a peer on an indirectly-connected network.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A directly-connected physical link must be available between EBGP peers. Otherwise, the **peer ebgp-max-hop** command must be used to allow EBGP peers to establish a TCP connection over multiple hops.

If loopback interfaces are used to establish an EBGP peer relationship, the **peer ebgp-max-hop** command (*hop-count* ≥ 2) must be run; otherwise, the peer relationship cannot be established.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer ebgp-max-hop** command is used on one end of an EBGP connection, it must also be used on the other end.

The configurations of GTSM and EBGP-MAX-HOP affect the TTL values of sent BGP packets, and the configurations of the two functions are mutually exclusive.

Example

Allow indirectly connected EBGP peer with the IP address of 10.1.1.2 to establish a connection with the local device.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
```

```
[Huawei-bgp] peer 10.1.1.2 ebgp-max-hop
```

9.8.114 peer enable (BGP)

Function

The **peer enable** command enables a BGP device to exchange routes with a specified peer or peer group in the address family view.

The **undo peer enable** command disables a BGP device from exchanging routes with a specified peer or peer group.

By default, only the peer in the BGP IPv4 unicast address family view is automatically enabled.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **enable**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, and BGP-EVPN address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-EVPN address family view, BGP-IPv6 unicast address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, only peers in the BGP IPv4 unicast address family are automatically enabled. After the **peer as-number** command is used in the BGP view, the system automatically runs the **peer enable** command to enable a peer. In other address family view, however, a peer must be enabled manually.

After the **undo default ipv4-unicast** command is run, the **peer enable** command needs to be run in the BGP view or the BGP-IPv4 unicast address family view to enable the IPv4 unicast address family for the created BGP peer.

Precautions

Enabling or disabling a BGP peer in an address family, for example, running the **peer enable** command or the **undo peer enable** command in a VPNv4 address family, causes teardown and re-establishment of the BGP connection of the peer in other address families.

Configuring the ipv4-address parameter in the BGP-IPv6 unicast address family view is a tested function.

Example

Disable a BGP device from exchanging IPv4 routes with a specified peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] undo peer 10.1.1.2 enable
```

Enable a BGP device to exchange BGP-VPNv4 routes with a specified peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] peer 10.1.1.2 enable
```

Related Topics

9.8.101 peer as-number

9.8.115 peer fake-as

Function

The **peer fake-as** command configures the local device to use the fake AS number to set up a BGP peer relationship with the specified peer.

The **undo peer fake-as** command restores the default setting.

By default, a peer uses the actual local AS number.

 Copyright © Huawei Technologies Co., Ltd.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **fake-as** { *as-number-plain* | *as-number-dot* } [**prepend-global-as**]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **fake-as**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.
prepend-global-as	Indicates that the actual AS number is added to packets to be sent.	-

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer fake-as** command is often used for network deployment changing of carriers' networks. For example, if carrier A purchases the network of carrier B and the networks of the two carriers belong to different ASs, the ASs of the two carriers need to be combined and the AS number of carrier B needs to be changed to the AS number of carrier A. BGP peers (in another AS) of devices on carrier B's network may not be willing to have their BGP configurations changed or changed immediately during network combination. As a result, the connections with these BGP peers will be interrupted.

To ensure that the ASs are combined properly, you can run the **peer fake-as** command on the ASBR on carrier's B network to set the AS number of carrier B to the fake AS number of carrier A. This setting enables the BGP peers of devices in carrier B's network to use the fake AS number to set up connections.

Prerequisites

Peers have been created by using the **peer as-number** command.

Precautions

If the **peer fake-as** command is run several times for a peer or a peer group, the latest configuration will overwrite the previous one.

The **peer fake-as** command is valid only for EBGP peers.

After the 4-byte AS number capability is disabled on a peer, configuring a 4-byte fake AS number for the peer may cause a failure to establish a BGP session.

Example

Set a 2-byte fake AS number for a peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 fake-as 99
```

Set a 4-byte fake AS number for a peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 fake-as 100.200
```

Related Topics

9.8.101 peer as-number

9.8.116 peer filter-policy

Function

The **peer filter-policy** command configures a filtering policy to advertise or receive routes from peers or peer group.

The **undo peer filter-policy** command deletes the filtering policy used to advertise or receive routes from peers or peer group.

By default, no filtering policy is configured to advertise or receive routes from peers or peer group.

 Copyright © Huawei Technologies Co., Ltd.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** { *acl-number* | **acl-name** *acl-name* | *acl6-number* | **acl6-name** *acl6-name* } { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** { *acl-number* | **acl-name** *acl-name* | *acl6-number* | **acl6-name** *acl6-name* } { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The name should start with a letter (case sensitive) and can contain numbers, hyphens (-), or underlines (_).
import	Filters received routes.	-
export	Filters routes to be advertised.	-

NOTE

- *ipv4-address*, **acl-name** *acl-name*, and *acl-number* are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address*, **acl6-name** *acl6-name*, and *acl6-number* are valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer filter-policy** command is used to configure an ACL-based policy for filtering routes received from peers or routes to be advertised to peers.

A proper basic ACL needs to be selected based on the address family of a peer or peer group.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

A basic ACL needs to be configured.

Precautions

If the **peer filter-policy** command is run multiple times, the latest configuration overwrites the previous one. For example, if the **peer 10.1.1.2 filter-policy 2600 import** command is run and then the **peer 10.1.1.2 filter-policy 2400 import** command is run, the configuration of the **peer 10.1.1.2 filter-policy 2400 import** command overwrites that of the **peer 10.1.1.2 filter-policy 2600 import** command.

When the **rule** command is run to configure rules for a named ACL, only the source address range specified by **source** and the time period specified by **time-range** take effect.

Example

Set the IPv4 filtering policy for peers.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit
[Huawei-acl-basic-2000] quit
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 filter-policy 2000 import
```

Set the IPv6 filtering policy for peers.

```
<Huawei> system-view
```

```
[Huawei] acl ipv6 2001
[Huawei-acl6-basic-2001] rule permit
[Huawei-acl6-basic-2001] quit
[Huawei] bgp 100
[Huawei-bgp] peer fc00:0:0:2::3 as-number 200
[Huawei-bgp] ipv6-family unicast
[Huawei-bgp-af-ipv6] peer fc00:0:0:2::3 filter-policy 2000 import
```

Related Topics

19.7.18 rule (basic ACL view)

19.7.19 rule (basic ACL6 view)

9.8.117 peer group

Function

The **peer group** command adds a peer to a peer group.

The **undo peer group** command removes a peer from a peer group and deletes all configurations of the peer.

By default, no peer group is created.

Format

peer { *ipv4-address* | *ipv6-address* } **group** *group-name*

undo peer { *ipv4-address* | *ipv6-address* } **group** *group-name*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-EVPN address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv4 address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale BGP network, there are a large number of peers and many of them have the same routing policies. To configure these peers, you have to repeatedly use some commands. In such a case, configuring peer groups can simplify configurations. If you intend to perform the same configuration on several peers, create and configure a peer group. Then, add the peers to the peer group. The peers will inherit the configurations of the peer group.

Precautions

Peers with different AS numbers can be added to the same peer group. If a peer has an AS number, the peer keeps its own AS number after being added to a peer group. If a peer has no AS number but the peer group to which the peer will be added has an AS number, the peer inherits the AS number of the peer group after being added to the peer group.

The members of a peer group can be configured with different route receiving and advertising policies.

The **undo peer group** command has the same function with the **undo peer** command and the **undo peer enable** command.

Example

Create an IBGP peer group named test, and then add a peer to it.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] group test internal
[Huawei-bgp] peer 10.1.1.1 group test
```

Related Topics

9.8.101 peer as-number

9.8.114 peer enable (BGP)

 Copyright © Huawei Technologies Co., Ltd.

9.8.118 peer ignore

Function

The **peer ignore** command prevents a BGP device from establishing a session with a peer or peer group.

The **undo peer ignore** command permits a BGP device from establishing a session with a peer or peer group.

By default, the device is permitted to set up the session with the BGP peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **ignore**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **ignore**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

When a BGP device needs to transitorily close the session with a peer and reconfiguring the peer requires too much workload, the **peer ignore** command can be used to avoid the reconfiguration of the peer. For example, if the peer relationship frequently alternates between Up and Down because of the upgrade of a peer or the adjustment of the link, the BGP peer relationship needs to be interrupted temporarily. In this case, the **peer ignore** command can be used on the stabler end to prevent frequent flapping of the route or peer relationship.

The **peer ignore** command is used to tear down sessions between a BGP device and its peer or peer group and delete all related routing information. In the case of a peer group, a large number of sessions are suddenly torn down.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

After the **peer ignore** command is run on a device, the session between the device and its peer is closed and all the related routing information is cleared.

After a BGP session is successfully established, running the **peer ignore** command interrupts the BGP session. The interrupted BGP session cannot be established again, and the status of the corresponding BGP peer relationship is displayed as Idle.

Running the **peer ignore** command together with the **peer enable** command equals running of the **reset bgp** command. Both methods can be used to configure a device to re-establish a session.

Example

Prohibit a device from establishing any session with peer 10.1.1.2.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 ignore
```

Related Topics

9.8.114 peer enable (BGP)

9.8.154 reset bgp

9.8.119 peer ip-prefix

Function

The **peer ip-prefix** command configures a route filtering policy based on an IP address prefix list for a peer or peer group.

The **undo peer ip-prefix** command cancels the route filtering policy based on an IP address prefix list of a peer or peer group.

By default, no route filtering policy based on an IP address prefix list is configured for a peer or peer group.

 Copyright © Huawei Technologies Co., Ltd.

Format

peer { *group-name* | *ipv4-address* } **ip-prefix** *ip-prefix-name* { **import** | **export** }

peer { *group-name* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* } **ip-prefix** [*ip-prefix-name*] { **import** | **export** }

undo peer { *group-name* | *ipv6-address* } **ipv6-prefix** [*ipv6-prefix-name*] { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ip-prefix *ip-prefix-name*	Indicates the filtering policy that is based on the IPv4 prefix list of the peer or peer group.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a filtering policy to the routes received from a peer or peer group.	-
export	Applies a filtering policy to the routes to be advertised to a peer or peer group.	-
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv6-prefix *ipv6-prefix-name*	Indicates the filtering policy that is based on the IPv6 prefix list of the peer or peer group.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- *ipv4-address* and *ip-prefix-name* are valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* and *ipv6-prefix-name* are valid only in the BGP-IPv6 unicast address family view, BGP-VPNv6 address family view, and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-IPv6 unicast address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer ip-prefix** command can be used to configure a route filtering policy that is based on an IP prefix list to filter routes received or routes to be advertised, implementing route control.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

If the **peer ip-prefix** command specifies an IP prefix list that does not exist for a peer or peer group, use the **ip ip-prefix** or **ip ipv6-prefix** command to create an IP prefix list.

Precautions

If an IP prefix list is specified for a peer group, all the members of the peer group inherit the configuration.

After an IP prefix list is specified for a peer or peer group, the peer or peers in the peer group filter the routes to be advertised to or received from other peers based on the IP prefix list. Only the routes that pass the filtering of the IP prefix list can be advertised or received.

Example

Configure a route filtering policy based on an IP prefix list.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-bgp-af-ipv4] peer 10.1.1.2 ip-prefix list1 import
```

Related Topics

9.9.47 ip ip-prefix
9.9.48 ip ipv6-prefix
9.8.79 filter-policy export (BGP)
9.8.80 filter-policy import (BGP)
9.8.116 peer filter-policy
9.8.135 peer route-policy

9.8.120 peer keychain (BGP)

Function

The **peer keychain** command configures the Keychain authentication for establishing the TCP connection between BGP peers.

The **undo peer keychain** command restores the default setting.

By default, the Keychain authentication is not configured for BGP peers.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **keychain** *keychain-name*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **keychain**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
keychain-name	Specifies the name of the Keychain authentication.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

ipv6-address is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

If the peer address is an IPv6 address and keychain authentication is configured, the authentication algorithm supports only HMAC-MD5, HMAC-SHA1-12, or HMAC-SHA-256.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configuring Keychain authentication improves the security of the TCP connection. You must configure Keychain authentication specified for TCP-based applications on both BGP peers. Note that encryption algorithms and passwords configured for the Keychain authentication on both peers must be the same; otherwise, the TCP connection cannot be set up between BGP peers and BGP messages cannot be transmitted.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Before configuring the BGP Keychain authentication, a Keychain in accordance with the configured *keychain-name* must be configured first. For keychain configuration details, see the "Keychain Configuration" chapter in *Huawei AR Series Configuration Guide - Security*.

Precautions

The **peer keychain** command and the **peer password** command are mutually exclusive. SHA256 and HMAC-SHA256 encryption algorithm are recommended in keychain authentication.

Example

Configure the Keychain authentication named Huawei for BGP peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 keychain Huawei
```

9.8.121 peer keep-all-routes

Function

The **peer keep-all-routes** command saves all the BGP routing updates from the specified peer or the peer group after the BGP connection is set up, even though those routes do not pass the configured ingress policy.

The **undo peer keep-all-routes** command restores the default setting.

By default, only the BGP routing updates received from the peers and passing the configured ingress policy are saved.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After changing a BGP import policy, you can reset BGP connections for the new import policy to take effect immediately, interrupting these BGP connections temporarily. If a device's peer does not support route-refresh, the **peer keep-all-routes** command can be used on the device to remain all routing updates received from the peer so that the device can refresh its routing table without closing the connection with the peer.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If the router does not support the route-refresh capability, the peer keep-all-routes command needs to be run on the router and its peer. If the **peer keep-all-routes** command is run on a device for the first time, the sessions between the device and its peers will be re-established.

If the router supports the route-refresh capability, running this command does not result in re-establishment of the sessions between the router and its peers. After the **refresh bgp** command is run on the router, however, the router does not refresh its routing table.

After the **keep-all-routes** command is run, the **undo peer keep-all-routes** command becomes ineffective. To have the **undo peer keep-all-routes** command become effective, run the **undo keep-all-routes** command and then the **peer keep-all-routes** command.

NOTE

If the router supports the route-refresh capability, the **peer keep-all-routes** command does not need to be run on it.

Example

Configure a device to store all BGP routing updates received from its IPv4 peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 keep-all-routes
```

Related Topics

9.8.106 peer capability-advertise

9.8.149 refresh bgp

9.8.122 peer label-route-capability (BGP)

Function

The **peer label-route-capability** command enables a BGP device to send labeled routes to a specified peer or peer group.

The **undo peer label-route-capability** command disables this function.

By default, this function is disabled.

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support this command.

Format

peer { *group-name* | *ipv4-address* } **label-route-capability** [**check-tunnel-reachable**]

undo peer { *group-name* | *ipv4-address* } **label-route-capability**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
check-tunnel-reachable	Checks tunnel reachability when imported routes are sent as labeled routes. **NOTE** **check-tunnel-reachable** is valid only in the BGP view, BGP-IPv4 unicast address family view	-

Views

BGP view, BGP-IPv4 unicast address family view, and BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the capability of sending labeled routes is enabled or disabled, BGP connection is automatically closed and the capability of the neighbor is re-negotiated.

Configuring the **check-tunnel-reachable** parameter can only be used to check tunnels on IPv4 public networks.

- If the **check-tunnel-reachable** parameter is configured, BGP advertises IPv4 unicast routes to peers when routed tunnels are unreachable or advertises labeled routes to peers when routed tunnels are reachable. In VPN scenario, this eliminates the risk of establishing an MP-EBGP peer relationship between PEs over a faulty LSP because this will cause data forwarding failures.
- If the **check-tunnel-reachable** parameter is not configured, BGP advertises labeled routes to peers whether the tunnels for imported routes are reachable or not.

NOTE

To disable tunnel reachability checking, run the **peer** { *group-name* | *ipv4-address* } **label-route-capability** command, not the **undo peer label-route-capability** command.

Before you run the **peer label-route-capability (BGP)** command, the **peer as-number** command should be used to create a peer or peer group.

Precautions

Configuring the ipv4-address parameter in the BGP-IPv6 unicast address family view is a tested function.

Example

Enable BGP to send the labeled routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 label-route-capability
```

Enable BGP to send labeled routes, and enable tunnel reachability checking.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 label-route-capability check-tunnel-reachable
```

9.8.123 peer listen-net

Function

The **peer listen-net** command configures BGP to listen to BGP connection requests from a specified network segment and establish BGP peer relationships dynamically.

The **undo peer listen-net** command restores the default configuration.

By default, BGP does not listen to BGP connection requests from any network segment.

Format

peer *group-name* **listen-net** *network* { *mask* | *mask-length* }

undo peer *group-name* **listen-net** *network* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The value is a string of 1 to 47 case-sensitive characters, spaces not supported.
network	Specifies the address of the network segment from which BGP listens to BGP connection requests.	The value is in dotted decimal notation.
mask	Specifies the mask of the network segment from which BGP listens to BGP connection requests.	The value is in dotted decimal notation.

Parameter	Description	Value
mask-length	Specifies the mask length of the network segment from which BGP listens to BGP connection requests.	The value is an integer ranging from 0 to 32.

Views

BGP or BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple BGP peers reside on the same network segment, and the number of the peers may change, you can run the **peer listen-net** command to configure BGP to listen to BGP connection requests from the network segment, establish BGP peer relationships dynamically, and add the peers to a peer group. This spares the local device from adding or deleting BGP peer configurations in response to each change in the peer number, which reduces the maintenance workload.

Prerequisites

A peer group has been configured using the **group** *group-name* command.

Precautions

If you run the command multiple times, BGP listens to BGP connection requests from multiple network segments.

Example

Configure BGP to listen to BGP connection requests from network segment 20.1.1.0/24 and establish BGP peer relationships dynamically.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] group test internal
[Huawei-bgp] peer test listen-net 20.1.1.0 24
```

9.8.124 peer listen-only

Function

The **peer listen-only** command configures a peer or peer group to only detect connection requests and not to initiatively send connection requests.

The **undo peer listen-only** command restores the default setting.

By default, a peer or peer group detects and sends connection requests.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **listen-only**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **listen-only**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer listen-only** command is used to configure a peer or peer group to only detect connection requests and not to initiatively send connection requests.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer listen-only** command is run multiple times, the latest configuration overwrites the previous one.

After the **peer listen-only** command is executed, the local end does not initiate any connection request to a specified peer.

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

The **peer listen-only** command can be run at only one end of a peer relationship. If this command is run at both ends of a peer relationship, the ends fail to establish a connection.

Example

Configure peer 10.1.1.1 to only detect connection requests from the remote peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.1 as-number 200
[Huawei-bgp] peer 10.1.1.1 listen-only
Warning: Changing the parameter in this command resets the peer session. Continue? [Y/N]:Y
```

Related Topics

9.8.55 display bgp peer

9.8.29 display bgp group

9.8.125 peer log-change

Function

The **peer log-change** command enables a BGP device to log the session status and events of a specified peer or a peer group.

The **undo peer log-change** command disables a BGP device to log the session status and events of a specified peer or a peer group.

By default, a BGP device is enabled to log the session status and events of a specified peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **log-change**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **log-change**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

The **peer log-change** command can be used to enable a device to log the session status and events of a specified peer or peer group, facilitating service management.

Peer relationships have been established using the **peer as-number** command.

Example

Configure a BGP device to log the session status and events of peer 10.1.1.2.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 log-change
```

Related Topics

9.8.55 display bgp peer

9.8.126 peer next-hop-invariable

Function

The **peer next-hop-invariable** command configures PEs in different ASs not to change next hops of routes when the PEs advertise them to their EBGP peers, and configure the PEs to use the next hops of imported IGP routes when the PEs advertise them to their IBGP peers.

The **undo peer next-hop-invariable** command restores the default setting.

By default, when advertising routes to its EBGP peers and imported IGP routes to IBGP peers, a BGP speaker changes the next hop to its interface address.

 Copyright © Huawei Technologies Co., Ltd.

Format

peer { *ipv4-address* | *group-name* } **next-hop-invariable**

undo peer { *ipv4-address* | *group-name* } **next-hop-invariable**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPNv4 address family view, BGP-EVPN address family view

NOTE

The AR150&AR160&AR200 series do not support BGP-VPNv4 address family view.

AR100&AR120&AR150&AR160&AR200 series does not support BGP-EVPN address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer next-hop-invariable** command is used on a device, the device does not change the next hop of an imported IGP route when advertising it to its IBGP peers, and does not change the next hop of a route when advertising it to its EBGP peers.

In the inter-AS VPN option C networking where an RR is used, the **peer next-hop-invariable** command needs to be run to configure the RR not to change the next-hop address of a route when advertising the route to an EBGP peer. This ensures that the remote PE iterates a route to the BGP LSP destined for the local PE during traffic transmission.

Prerequisites

The **peer as-number** command has been used to create a peer or peer group.

Configuration Impact

After the **peer next-hop-invariable** command is used on a device, the device does not change the next hop of an imported IGP route when advertising it to its IBGP

peers, and does not change the next hop of a route when advertising it to its EBGP peers.

Precautions

When the **peer next-hop-invariable** command is configured on EBGP peers, the command configuration takes effect only for VPNv4 and VPNv6 routes.

If a device needs to advertise routes to its IBGP peer or peer group, the **peer next-hop-invariable** and **peer next-hop-local** commands are mutually exclusive on the device.

Example

Configure a BGP device not to change the next hop of a route when the BGP device advertises it to its EBGP peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 next-hop-invariable
```

Use the next hop of an IGP route when advertising the IGP route to IBGP peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 next-hop-invariable
```

9.8.127 peer next-hop-local

Function

The **peer next-hop-local** command configures a BGP device to set its IP address as the next hop of routes when the BGP device advertises routes to an IBGP peer or peer group.

The **undo peer next-hop-local** command restores the default setting.

By default, a BGP device sets its IP address as the next hop address of routes when advertising them to its EBGP peer; the BGP device does not change the next hop address of routes when advertising them to its IBGP peer.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **next-hop-local**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **next-hop-local**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BPG-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view, and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer next-hop-local** command is usually run on an ASBR. By default, when an ASBR forwards a route learned from an EBGP peer to its IBGP peers, the ASBR does not change the next hop of the route. The next hop address of a route advertised by an EBGP peer is the address of the EBGP peer. After being forwarded to the IBGP peers, the route cannot become an active route because of the unreachable next hop. The **peer next-hop-local** command needs to be run to configure the ASBR to change the next hop of the route to its IP address when the ASBR advertises the route to an IBGP peer. Therefore, after being forwarded to the IBGP peer, the route can become an active route because the next hop is reachable.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The **peer next-hop-local** command is valid only for the label routes on a BGP route reflector.

Precautions

If the **peer next-hop-local** command is run several times, the latest configuration overrides the previous one.

After the **peer next-hop-local** command is configured on a device, the device sets its IP address as the next hop of routes when the BGP device advertises the routes to its IBGP peer or peer group.

The **peer next-hop-local** command is applicable to IBGP peers.

When the BGP device advertises routes to an IBGP peer or peer group, the **peer next-hop-local** command and the **peer next-hop-invariable** command are mutually exclusive.

Example

Configure a BGP device to set its IP address as the next hop of routes when advertising the routes to peer 10.1.1.2.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 next-hop-local
```

9.8.128 peer out-delay

Function

The **peer out-delay** command configures a delay for sending Update packets.

The **undo peer out-delay** command deletes the delay for sending Update packets.

The default delay is 0, indicating that Update packets are sent without a delay.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **out-delay** *delay-value*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **out-delay**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The value is a 32-bit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
delay-value	Specifies the delay for sending Update packets.	The value is an integer ranging from 0 to 3600, in seconds.

NOTE

- The *ipv4-address* parameter applies to the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, BGP-VPN instance IPv4 address family view.
- The *ipv6-address* parameter applies to the BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv4 address family view, BGP-IPv4 multicast address family view, BGP-EVPN address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario in which primary and backup routes exist, packets may get lost after traffic switches back to the primary path from the backup path. Use a VPN FRR scenario as an example. PE3 and CE connect both to PE1 and PE2. The primary path is PE3 -> PE1 -> CE, and the backup path is PE3 -> PE2 -> CE. CE uses BGP to communicate with PE1 and PE2. FRR is configured on PE3. If PE1 restarts or the link between PE3 and PE1 is disconnected, traffic switches from the primary path to the backup path. After the primary path recovers, traffic switches back to the primary path. If PE3 completes refreshing forwarding entries before PE1 does so, PE1 may temporarily fail to forward traffic received from PE3, and packet loss may occur. The severity of packet loss is proportional to the number of routes stored on PE1.

To solve this problem, run the **peer out-delay** command on PE1 to configure a delay for sending Update packets. An appropriate delay ensures that traffic switches back to the primary path after PE1 completes refreshing forwarding entries.

Precautions

If you run the **peer out-delay** command repeatedly, the latest configuration overrides the previous configurations.

 Copyright © Huawei Technologies Co., Ltd.

If the **peer out-delay** and **peer route-update-interval** commands are both configured, only the **peer out-delay** command takes effect.

If a network has high route convergence requirements, do no use the **peer out-delay** command.

Example

In the BGP view, configure the delay for sending Update packets to 10.1.1.1 as 300s.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.1 out-delay 300
```

9.8.129 peer password

Function

The **peer password** command enables a BGP device to implement MD5 authentication for BGP messages exchanged during the establishment of a TCP connection with a peer.

The **undo peer password** command restores the default setting.

By default, a BGP device does not perform MD5 authentication for BGP messages exchanged during the establishment of a TCP connection with a peer.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **password** { **cipher** *cipher-password* | **simple** *simple-password* }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **password**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-password*	Specifies a cipher text password.	In the case of a plain text password, the value is a string of 1 to 255 case-sensitive characters, without spaces. In the case of a cipher text password, the value is a string of 20 to 392 case-sensitive characters, without spaces.
simple *simple-password*	Specifies a simple password. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of 1 to 255 case-sensitive characters, without spaces.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP uses TCP as the transport layer protocol. To enhance BGP security, MD5 authentication can be implemented for BGP packets exchanged during the establishment of a TCP connection. MD5 authentication sets the MD5 authentication password for the TCP connection, and the authentication is performed by TCP.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

After the **peer password** command is run, if the MD5 authentication fails, no TCP connection is established.

MD5 authentication and keychain authentication are mutually exclusive on a peer. Simple and MD5 authentication has potential risks. Keychain authentication is recommended.

After the **peer password** command is run on a device to enable MD5 authentication, the device will re-establish the peer relationship with its peer.

Example

Configure authentication for the TCP connection between a device and peer 10.1.1.2.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 password cipher huawei
```

9.8.130 peer path-mtu auto-discovery

Function

The **peer path-mtu auto-discovery** command enables path MTU discovery.

The **undo peer path-mtu auto-discovery** command disables path MTU discovery.

By default, path MTU discovery is disabled.

Format

peer { *group-name* | *ipv4-address* } **path-mtu auto-discovery**

undo peer { *group-name* | *ipv4-address* } **path-mtu auto-discovery**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Views

BGP view or BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When hosts on the same network communicate, the MTU of the network is important to both communication ends. When hosts need to communicate across multiple networks, the smallest MTU on the communication path is most important to both ends. This is because different networks along the communication path have different link-layer MTUs. The minimum MTU on the communication path is called the path MTU.

For example, if BGP packets are encapsulated in TCP packets and the default Maximum Segment Size (MSS) of a TCP packet is 536 bytes, the length of Update packets transmitted between BGP peers is 536 bytes. As a result, a large amount of BGP update information is distributed to different packets, and the number of ACK packets corresponding to the update information increases. Transmission this mode is inefficient. To improve the efficiency of transmitting BGP packets, the path MTU discovery mechanism can be used by both communication ends.

The path MTU has the following characteristics:

- Uncertainty: During communication, the path MTU of hosts depends on the selected path and thus may change.
- Inconsistency: The path MTUs in the inbound and outbound directions may be inconsistent because the path from the sender to the receiver may be different from the path from the receiver to the sender.

Precautions

After the **peer path-mtu-discovery** command is run, peers learn the number of bytes of the maximum data packet on a transmission path to prevent packet fragmentation.

By default, path MTU discovery is disabled on a peer because enabling path MTU discovery by default requires the additional cost. If the MTU is known during network planning, path MTU discovery does not need to be enabled.

Example

Configure path MTU discovery for peer 1.1.1.2.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.2 path-mtu auto-discovery
```

9.8.131 peer preferred-value

Function

The **peer preferred-value** command sets a preferred value for the routes that a BGP device learns from its peer.

The **undo peer preferred-value** command restores the default preferred value for the routes that a BGP device learns from its peer.

By default, the preferred value of a route learned from a BGP peer is 0.

 Copyright © Huawei Technologies Co., Ltd.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **preferred-value** *value*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **preferred-value**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
value	Specifies the preferred value of the routes that a BGP device learns from its peer.	The value is an integer ranging from 0 to 65535.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer preferred-value** command is run, all the routes learned from the specified peer have the preferred value. If there are multiple routes to the same address prefix, the route with the highest preferred value is preferred.

Prerequisites

A BGP peer has been configured. If the **peer preferred-value** command is used but no BGP peer exists, a message is displayed, indicating that the peer does not exist.

Precautions

If a preferred value is set for the routes that a BGP device learns from a peer group, all members of the peer group inherit the configuration.

Example

Set a preferred value to 50 for the routes that a BGP device learns from a specified peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 preferred-value 50
```

9.8.132 peer public-as-only

Function

The **peer public-as-only** command configures the AS-Path attribute in a BGP Update packet not to carry the private AS number. Only the public AS number is contained in the update packets.

The **undo peer public-as-only** command restores the default setting.

By default, the AS-Path attribute in a BGP Update packet is allowed to carry private AS numbers.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **public-as-only** [**force**]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **public-as-only**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In general, the number of the AS ranges from 1 to 4294967295. The public AS number ranges from 1 to 64511, and 65536 (1.0 in the format of x.y) to 4294967295 (65535.65535 in the format of x.y), and the private AS number ranges from 64512 to 65534. 65535 is used as the reserved AS number in certain circumstances.

Public AS numbers can be used on the Internet. Private AS numbers cannot be advertised to the Internet, and they are used only within ASs. If private AS numbers are advertised to the Internet, a routing loop may occur. After this command is configured, if the AS path attribute contains only private AS numbers, BGP deletes the private AS numbers and then advertises these update routes.

BGP does not delete private AS numbers in either of the following scenarios if the **peer public-as-only** command is run, without any parameter following **public-as-only** specified:

- The AS_Path attribute of a route carries the AS number of the remote peer. In this case, deleting private AS numbers may lead to a routing loop.
- The AS_Path attribute carries both public and private AS numbers, which indicates that the route has passed through the public network. In this case, deleting private AS numbers may lead to a traffic forwarding error.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Example

Configure a device to remove all private AS numbers from the AS_Path attribute when sending a BGP Update packet to its peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 public-as-only
```

9.8.133 peer reflect-client

Function

The **peer reflect-client** command configures the local device as the route reflector and the peer or peer group as the client of the route reflector.

The **undo peer reflect-client** command restores the default setting.

By default, the route reflector and its client are not configured.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Full-meshed connections need to be established between IBGP peers to ensure the connectivity between the IBGP peers. If there are n routers in an AS, n (n-1)/2 IBGP connections need to be established. A large number of IBGP peer uses a lot of network and CPU resources. An RR can be used to solve the problem.

In an AS, one router functions as an RR and other routers function as clients. The clients establish IBGP connections with the RR. The RR and its clients form a cluster. The RR reflects routes among the clients, and therefore the clients do not need to establish any IBGP connection. Assume that an AS has n devices. If one of the device functions as a RR, and other devices function as clients, the number of IBGP connections to be established is n-1. This means that network and CPU resources are greatly reduced.

An RR is easy to configure, because it needs to be configured only on the device that functions as a reflector and clients do not need to know that they are clients.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

The device where the **peer reflect-client** command is run serves as the RR and a specified peer or peer group serves as the client of the RR.

The **peer reflect-client** command can be only used between IBGP peers or IBGP peer groups.

reflect-client configured in an address family is valid in this family address and cannot be inherited by other address families. Configuring **reflect-client** in a specified address family is recommended.

Example

Configure a peer as a client of an RR.

```
<Huawei> system-view
[Huawei] bgp 100
```

```
[Huawei-bgp] peer 10.1.1.2 as-number 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 reflect-client
```

Related Topics

9.8.146 reflect between-clients

9.8.148 reflector cluster-id

9.8.134 peer route-limit

Function

The **peer route-limit** command sets the maximum number of routes that can be received from a peer.

The **undo peer route-limit** command restores the default setting.

By default, there is no limit on the number of routes that can be received from a peer.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit** *limit* [*percentage*] [**alert-only** | **idle-forever** | **idle-timeout** *minutes*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
limit	Specifies the maximum number of routes that can be received from a peer.	The value is an integer. The value range varies according to devices: ● AR150 series: 1 to 1000. ● AR100&AR120&AR160 series: 1 to 20000. ● AR200 series: 1 to 5000. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE, AR2204E, AR2204-51GE-R, AR2204E-D and AR2204: 1 to 30000. ● AR2220, AR2220E: 1 to 80000. ● AR2204XE and AR2204XE-DC: 1 to 500000. ● AR2240 and AR3200 series: – SRU40: 1 to 300000. – SRU60: 1 to 400000. – SRU80 or SRU100E or SRU100: 1 to 500000. – SRU200, SRU200E or SRU400: 1 to 1000000. ● AR2240C: 1 to 300000. ● AR3600 (using SRUX5) series: 1 to 1000000.
percentage	Specifies the percentage of received routes when the router starts to generate alarms.	The value is an integer ranging from 1 to 100. The default value is 75.
alert-only	Indicates that if the number of received routes exceeds the limit, an alarm will be generated and no additional routes will be accepted.	-
idle-forever	Indicates that after the number of routes exceeds the limit, no connection is established automatically until the **reset bgp** command is run.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
idle-timeout *minutes*	Specifies the value of the timeout timer. The connection, which is closed because the number of routes exceeds the threshold, is automatically re-established in the period specified by the timeout timer. Before the timer expires, the **reset bgp** command can be used to re-establish a connection.	The value is an integer ranging from 1 to 1200, in minutes.

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **peer route-limit** command is used to set the maximum number of routes that a BGP router is allowed to receive from its peer. This provides a mechanism for controlling the routes received from peers in addition to distribution lists, filtering lists, and route mappings.

If a peer relationship between two devices is in the Established state, the following situations occur:

- If the number of routes received by the router exceeds the upper limit and the **peer route-limit** command is used for the first time, the router and its peer re-establish the peer relationship, regardless of whether **alert-only** is set.

- If the upper limit set on the router is increased to be greater than the number of received routes, the router sends Refresh packets to receive routes again. If the router does not support the route-refresh capability, the router needs to re-establish the connection with its peer.
- If the upper limit set on the router is reduced but is still greater than the number of received routes, only configuration parameters need to be modified.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

If the **peer route-limit** command is run for a peer group, the peers of the peer group inherit the configuration.

If the peer relationship is in the Idle state because the number of received routes exceeds the upper limit and **idle-forever** or **idle-timeout** is set, the **reset bgp** command can be used to re-establish the peer relationship.

Assume that none of **alert-only**, **idle-forever**, and **idle-timeout** is configured. If the number of routes exceeds the upper limit, an alarm is generated and recorded in the log. Then, the peer relationship is disconnected. The devices try to re-establish the peer relationship after 30 seconds.

Example

Set the maximum number of routes that can be received from a peer to 5000.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 route-limit 5000
```

Related Topics

9.8.154 reset bgp

9.8.135 peer route-policy

Function

The **peer route-policy** command specifies a route-policy for filtering routes received from a peer or peer group or routes to be advertised to a peer or peer group.

The **undo peer route-policy** command restores the default setting.

By default, no route-policy is configured for filtering routes received from a peer or peer group or routes to be advertised to a peer or peer group.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
route-policy-name	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a route-policy to routes to be imported from a peer or peer group.	-
export	Applies a route-policy to routes to be advertised to a peer or peer group.	-

NOTE

- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPNv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-IPv6 unicast address family view

NOTE

The AR150&160&200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a route-policy is created, the **peer route-policy** command is used to apply a Route-Policy to a peer or a peer group so that the routes advertised to or received from the peer or peer group can be controlled. To be specific, only the necessary routes are received from or advertised to the peer or peer group. In this manner, route management is implemented, the scale of the routing table is reduced, and fewer network resources are consumed.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

If the command specifies a route-policy that does not exist, use the **route-policy** command to create the route-policy.

Precautions

If the **peer route-policy** command is run for a peer group, all the members of the peer group inherit the configuration.

Example

Apply a route-policy named test-policy to the routes received from a peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer 10.1.1.2 route-policy test-policy import
```

Related Topics

9.9.53 route-policy

9.8.79 filter-policy export (BGP)

9.8.80 filter-policy import (BGP)

9.8.116 peer filter-policy

9.8.119 peer ip-prefix

9.8.136 peer route-update-interval

Function

The **peer route-update-interval** command sets the interval at which a device sends routing updates carrying the same prefix to a peer or peer group.

The **undo peer route-update-interval** command restores the default setting.

By default, the interval at which routing updates are sent to IBGP peers is 15s, and the interval at which routing updates are sent to EBGP peers is 30s.

 Copyright © Huawei Technologies Co., Ltd.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-update-interval** *interval*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-update-interval**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
interval	Specifies the minimum interval at which routing updates are sent.	The value is an integer ranging from 0 to 600, in seconds.

NOTE

- *group-name* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, and BGP-VPN instance IPv6 address family view.
- *ipv4-address* is valid only in the BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-IPv6 unicast address family view, and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP-IPv6 unicast address family view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When routes change, the router sends routing updates to notify its peers. If a route changes frequently, the **peer route-update-interval** command can be used to adjust the interval at which Update packets are sent for changes of this route. This frees the router from sending Update packets for every route change.

Prerequisites

If the **peer route-update-interval** command is used but no peer exists, a message is displayed, indicating that the peer does not exist.

Precautions

If a route is removed or added, the router sends an Update (Withdraw) packet to its peers immediately, without waiting the interval set using the **peer route-update-interval** command to expire.

Example

Set the interval at which routing updates are sent to a peer to 10s.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 route-update-interval 10
```

9.8.137 peer timer

Function

The **peer timer** command sets the Keepalive timer and Hold timer for a peer or peer group.

The **undo peer timer** command restores the default values of the Keepalive timer and Hold timer.

By default, the value of a Keepalive timer is 60s and the value of a Hold timer is 180s.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive hold** [**min-holdtime**]

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
keepalive-time	Specifies the Keepalive period.	The value is an integer ranging from 0 to 21845, in seconds.
hold-time	Indicates the holdtime.	The value is an integer that can be 0, or ranges from 3 to 65535, in seconds. **NOTE** Setting the hold interval of a BGP peer or peer group to be longer than 20s is recommended. If the hold interval of a BGP peer or peer group is shorter than 20s, the session may be closed.
min-holdtime *min-holdtime*	Specifies the minimum Holdtime configured on the local device. **NOTE** The value of *min-holdtime* configured cannot exceed the value of *hold-time*.	The value is an integer ranging from 20 to 65535, in seconds.

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After establishing a BGP connection, two peers send Keepalive messages periodically to each other to detect the status of the BGP connection. If a device receives no Keepalive message or any other types of packets from its peer within the holdtime, the device considers the BGP connection closed, and it closes the BGP connection.

When the peers set up a connection, the values of *keepalive-time* and *hold-time* are determined by negotiations between the peers. Each of the two peers sends the other an Open packet containing *hold-time*. The smaller of the *hold-time*

values contained in the Open packets from both peers is used. The smaller of the locally configured *keepalive-time* value and one third of the negotiated *hold-time* value is used as the actual *keepalive-time* value.

The **peer timer** command is used to set the Keepalive period and holdtime.

- If short Keepalive period and holdtime are set, BGP can detect a link fault quickly and implement link switching. The number of Keepalive messages on the network, however, is increased. This increases device loads and consumption of network bandwidth resources.
- If long Keepalive period and holdtime are set, the number of Keepalive messages on the network is reduced. This reduces device loads. If, however, the Keepalive period is too long, BGP is unable to detect link status changes in a timely manner, causing many packets to be lost.

If the local device establishes BGP peer relationships with many devices, it needs to process huge BGP messages. If *hold-time* negotiated among BGP peers is small, the timer may expire before the local device processes the Keepalive messages sent from other BGP peers. The peer relationships are then interrupted, and routes flap. To solve the preceding problem, you can configure an appropriate value for **min-holdtime** *min-holdtime* based on the CPU processing capability of the local device.

If the value of *min-holdtime* is changed, but the values of *keepalive-time* and *hold-time* negotiated between two BGP peers remain unchanged, the established peer relationship is not affected. Only when the local device attempts to re-establish a relationship with a remote device, the value of *min-holdtime* configured on the local device takes effect. The local device compares *min-holdtime* with *hold-time* sent from the remote device. If the value of *min-holdtime* exceeds that of *hold-time*, *hold-time* negotiation fails, and the peer relationship fails to be established.

NOTE

If *min-holdtime* is configured on the local device, and the value of *hold-time* sent from the remote device is 0, *hold-time* negotiation between the two devices succeeds. The negotiated value of *hold-time* is 0, and the peer relationship is established. The value 0 of *hold-time* indicates that the peer relationship never expires.

Prerequisites

Peer relationships have been established using the **peer as-number** command.

Precautions

NOTICE

If the value of a timer changes, the BGP peer relationship between devices will be disconnected. This is because the devices need to re-negotiate the values of *keepalive-time* and *hold-time*. Therefore, exercise caution before changing the value of a timer.

The Keepalive period must be at least three times of the holdtime.

When setting the values of *keepalive-time* and *hold-time*, note the following points:

- The values of *keepalive-time* and *hold-time* cannot both be set to 0. This renders the BGP timers invalid. BGP is unable to detect link faults using the timers.
- The *hold-time* value cannot be significantly greater than the *keepalive-time* value. A setting of **timer keepalive 1 hold 65535**, for example, would be improper. If the holdtime is too long, link faults cannot be detected in a timely manner.

The Keepalive period and Holdtime can be configured globally, or on a particular peer or peer group. The Keepalive period and Holdtime configured on a specific peer or peer group takes precedence over the global Keepalive period and Holdtime. Using this command can still change the Keepalive period and Holdtime configured on a peer or peer group, although they were globally configured through the **timer** command.

After the **keep-all-routes** command is run, the **undo peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* command becomes ineffective. To have the **undo peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* command become effective, run the **undo keep-all-routes** command and then the **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer keepalive** *keepalive-time* command.

Example

Set the Keepalive timer and Hold timer for peer 10.1.1.2.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 timer keepalive 10 hold 30
Warning: Changing the parameter in this command resets the peer session. Continue?[Y/N]: y
```

Related Topics

9.8.175 timer (BGP)

9.8.138 peer timer connect-retry

Function

The **peer timer connect-retry** command sets a ConnectRetry interval for a peer or peer group.

The **undo peer timer connect-retry** command restores the default setting.

By default, the ConnectRetry interval is 32s.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies an IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies an IPv6 address of a peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
connect-retry-time	Specifies a ConnectRetry interval.	The value ranges from 1 to 65535, in seconds.

NOTE

- *ipv4-address* can be set only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view.

Views

BGP view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires. The ConnectRetry interval can be adjusted as needed.

- The ConnectRetry interval can be reduced in order to lessen the time BGP waits to retry establishing a TCP connection after the first attempt fails.
- To suppress route flapping caused by constant peer flapping, the ConnectRetry interval can be increased to accelerate route convergence.

Prerequisites

The **peer as-number** command has been used to create a peer or peer group.

Precautions

A ConnectRetry interval can be configured globally, or on a particular peer or peer group. A ConnectRetry interval configured on a specific peer or peer group takes precedence over a global ConnectRetry interval.

 Copyright © Huawei Technologies Co., Ltd.

- If both the **peer** { *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command and the **peer** *group-name* **timer connect-retry** *connect-retry-time* command are run on a device, the configuration of the **peer** { *ipv4-address* | *ipv6-address* }**timer connect-retry** *connect-retry-time* command takes effect, but the configuration of the **peer** *group-name* **timer connect-retry** *connect-retry-time* command does not.
- If both the **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command and the **timer connect-retry** *connect-retry-time* command are run on a device, the configuration of the **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **timer connect-retry** *connect-retry-time* command takes effect, but the configuration of the **timer connect-retry** *connect-retry-time* command does not.

After the **keep-all-routes** command is run, the **undo peer timer connect-retry** command becomes ineffective. To have the **undo peer timer connect-retry** command become effective, run the **undo keep-all-routes** command and then the **peer timer connect-retry** command.

Example

Set the ConnectRetry interval to 60s for peer 10.1.1.2.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 timer connect-retry 60
```

Related Topics

9.8.176 timer connect-retry

9.8.139 peer tracking

Function

The **peer tracking** command enables BGP peer tracking. That is, you can configure BGP to fast detect the unreachable state of a peer and re-establish the connection between the local device and the peer.

The **undo peer tracking** command disables BGP peer tracking.

By default, BGP peer tracking is disabled.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **tracking** [**delay** *delay-time*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **tracking**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The address is a 32-digit hexadecimal number in the X:X:X:X:X:X:X:X format.
delay *delay-time*	Indicates the interval between when BGP detects the peer unreachable and when BGP tears down the corresponding connection.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.

NOTE

- *ipv4-address* can be set only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* can be set only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a network where BFD is unsuitable to be deployed, you can configure BGP peer tracking on the local device to implement fast network convergence by rapidly detecting the unreachable state of the peer.

A proper value of *delay-time* can ensure network stability when a peer is detected unreachable.

- If *delay-time* is set to 0, BGP immediately tears down the connection between the local device and its peer after the peer is detected unreachable.
- If IGP route flapping occurs and *delay-time* for an IBGP peer is set to 0, the peer relationship between the local device and the peer alternates between

Up and Down. Therefore, *delay-time* for an IBGP peer should be set to a value greater than the actual IGP route convergence time.

- When BGP neighbors successfully perform the GR negotiation, the active/standby switchover occurs on the BGP neighbors, to prevent the failure of GR, *delay-time* should be set to a value greater than GR convergence time. If *delay-time* is set to be smaller than the GR convergence time, the connection between the local device and the BGP peer will be torn down, which leads to the failure of GR.

Prerequisites

The **peer as-number** command has been used to create a peer or peer group.

Precautions

IGP is configured with GR, and the BGP neighbor relationship is established based on IGP routes. In such a situation, when a node fails on the network and the master/slave switchover occurs on the node, IGP does not delete the routes from the node, and BGP neighbors cannot sense the fault on the node. Therefore, the BGP peer tracking function does not take effect.

Example

Configure BGP peer tracking.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 tracking delay 20
```

9.8.140 peer tnl-policy

Function

The **peer tnl-policy** command applies the tunnel policy to the specified IPv4 peer.

The **undo peer tnl-policy** command removes the tunnel policy applied to the peer.

By default, no tunnel policy is applied to the peer.

Format

peer *ipv4-address* **tnl-policy** *tnl-policy-name*

undo peer *ipv4-address* **tnl-policy**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of the peer.	The value is in dotted decimal notation.
tnl-policy-name	Specifies the name of the tunnel policy.	The name is a string of 1 to 39 characters. It is case-sensitive.

 Copyright © Huawei Technologies Co., Ltd.

Views

BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

When you configure the 6PE to support the tunnel, you need to configure the tunnel policy and apply the tunnel policy by using the command.

Before you configure the **peer tnl-policy** command, the **peer as-number** command should be used to create a peer or peer group.

Example

Apply the tunnel policy to the specified peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 100
[Huawei-bgp] ipv6-family unicast
[Huawei-bgp-af-ipv6] peer 10.1.1.2 enable
[Huawei-bgp-af-ipv6] peer 10.1.1.2 tnl-policy policy-a
```

9.8.141 peer valid-ttl-hops

Function

The **peer valid-ttl-hops** command applies the GTSM functions on the peer or peer group.

The **undo peer valid-ttl-hops** command cancels the application of the GTSM functions on the peer or peer group.

By default, GTSM functions on the peer or peer group is not configured.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **valid-ttl-hops** [*hops*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **valid-ttl-hops**

Parameters

Parameter	Description	Value
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a peer.	It is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
hops	Specifies the number of TTL hops to be checked.	It is an integer ranging from 1 to 255. The default value is 255. If the value is configured as *hops*, the valid TTL range of the detected packet is [255 - *hops* + 1, 255].

NOTE

- *ipv4-address* is valid only in the BGP view and BGP-VPN instance IPv4 address family view.
- *ipv6-address* is valid only in the BGP view and BGP-VPN instance IPv6 address family view.

Views

BGP view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device against the attacks of forged BGP packets, you can configure GTSM to check whether the TTL value in the IP packet header is within the specified range.

Prerequisites

Before configuring GTSM for a peer group, run the **peer group** command to add peers to the peer group.

Precautions

When the **undo peer valid-ttl-hops** command is run and no parameter is specified, all the GTSM configurations on a peer or a peer group are deleted.

The configuration in the BGP view is also valid for the VPNv6 extension of MP-BGP. This is because they use the same TCP connection.

The GTSM configurations are symmetrical, that is, GTSM must be enabled on both ends of the BGP connection at the same time.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- GSTM and EBGP-MAX-HOP are mutually exclusive because both of them affect the TTL of the sent BGP packet. Therefore, the two functions cannot be enabled on a peer or peer group simultaneously.
- If GTSM is enabled on two directly connected EBGP peers, the fast sensing function is invalid on the interfaces directly connecting the two EBGP peers. This is because BGP considers the EBGP peers indirectly connected when GTSM is enabled on the EBGP peers.

Example

Configure the GTSM function for the peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.2 as-number 200
[Huawei-bgp] peer 10.1.1.2 valid-ttl-hops 1
```

Configure the GTSM function for the peer group.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] group gtsm-group external
[Huawei-bgp] peer gtsm-group valid-ttl-hops 1
```

Related Topics

9.8.113 peer ebgp-max-hop

9.8.142 preference (BGP)

Function

The **preference** command sets protocol preferences for EBGP routes, IBGP routes, and local BGP routes.

The **undo preference** command restores the default setting.

By default, the protocol preferences of EBGP routes, IBGP routes, and local BGP routes are all 255.

Format

preference { *external internal local* | **route-policy** *route-policy-name* }

preference *external internal local* **route-policy** *route-policy-name*

undo preference

Parameters

Parameter	Description	Value
external	Specifies the protocol preference of an EBGP route. An EBGP route is the optimal route learned from a peer outside the local AS.	The value is an integer ranging from 1 to 255. The smaller the value is, the higher the preference is.

Parameter	Description	Value
internal	Specifies the protocol preference of an IBGP route. An IBGP route is a route learned from a peer inside the AS.	The value is an integer ranging from 1 to 255. The smaller the value is, the higher the preference is.
local	Specifies the protocol preference of a local BGP route. A local BGP route is a route obtained by using the **summary automatic** command (automatic summarization) or the **aggregate (BGP)** command (manual aggregation).	The value is an integer ranging from 1 to 255. The smaller the value is, the higher the preference is.
route-policy *route-policy-name*	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Running the **preference** command to set protocol preferences for BGP routes affects route selection among BGP routes and routes of other routing protocols.

After a route-policy is configured on a device, the device sets preferences only for the routes received from peers, which meet the matching rules. The routes that do not meet the rules use the default preference.

The smaller the preference value, the higher the preference.

Different protocol preferences can be configured for BGP routes in different address family views.

If both *external internal local* and **route-policy** *route-policy-name* are specified in the command, the priority of the routes that match the route-policy is set based on the route-policy, and the priorities of other routes are set based on the *external internal local* configuration.

Prerequisites

Create the route-policy first if the **preference** command uses the **route-policy** to set preferences.

Perform the following steps when the route-policy is used to set preferences:

- Use the **route-policy** command to create the route-policy, and enter the route-policy view.
- Configure the **if-match** clause to set the matching rules for routes. The relationship between the **if-match** clauses in a node of a route-policy is "AND". A route must match all the rules before the action defined by the **apply** clause is taken. If no **if-match** clause is specified, all routes will match the node in the route-policy.
- Use the **apply preference** command to set preferences for routes that pass the filtering.

Example

Set the preference to 2 for an EBGP route, 2 for an IBGP route, and 20 for a local BGP route.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] preference 2 2 20
```

Related Topics

9.8.173 summary automatic

9.8.2 aggregate (BGP)

9.9.53 route-policy

9.9.19 apply preference

9.8.135 peer route-policy

9.8.143 qos-local-id behavior

Function

The **qos-local-id behavior** command binds the QoS local ID carried in a local route to a specified traffic behavior.

The **undo qos-local-id behavior** command unbinds the QoS local ID carried in a local route from a specified traffic behavior.

By default, the QoS local ID carried in a local route is not bound to any traffic behavior.

Format

qos-local-id *qos-local-id* **behavior** *behavior*

undo qos-local-id *qos-local-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
qos-local-id	Specifies a QoS local ID.	The value is an integer that ranges from 1 to 4095.
behavior *behavior*	Specifies a traffic behavior name, which must be the name of an existing traffic behavior. This parameter is configured using the **traffic behavior** command and can be a system-defined or user-defined traffic behavior.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

QPPB local policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To apply a QoS traffic behavior to traffic of a specific route, run the **qos-local-id behavior** command to bind the QoS local ID carried in this route to the specified traffic behavior.

Prerequisites

- The **apply qos-local-id** *qos-local-id* command has been executed in the route-policy view to configure a QoS local ID for the route requiring QoS control.
- The **traffic behavior** *behavior-name* command has been executed in the system view to create a traffic behavior.

Precautions

Every QoS local ID can be bound to only one traffic behavior.

The traffic behavior bound to a QoS local ID cannot be configured based on the interface rate percentage, such as interface CAR, queue scheduling, or traffic shaping.

Example

Bind the QoS policy 1 carried in a local route to the traffic behavior **destination**.

```
<Huawei> system-view
[Huawei] route-policy test permit node 10
[Huawei-route-policy] apply qos-local-id 1
[Huawei-route-policy] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] traffic behavior destination
[Huawei-destination] quit
[Huawei] qppb local-policy 1
[Huawei-local-policy-1] qos-local-id 1 behavior destination
```

Related Topics

9.9.21 apply qos-local-id

20.1.44 traffic behavior

9.8.144 qppb local-policy

9.8.144 qppb local-policy

Function

The **qppb local-policy** command creates a QPPB policy.

The **undo qppb local-policy** command deletes a QPPB policy.

By default, no QPPB policy is created.

Format

qppb local-policy *policy-name*

undo qppb local-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies a QPPB policy.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A QPPB local policy needs to be defined during QPPB deployment. After binding the QoS policy ID (qos local-id) carried in a local route to a specified traffic behavior, you need to enable the QPPB local policy on an interface.

Configuration Impact

After the **qppb local-policy** command is executed, a QPPB local policy is created in the system. To make the QPPB function take effect, apply the QPPB local policy to an interface.

Example

Create QPPB policy 1.

```
<Huawei> system-view
[Huawei] qppb local-policy 1
```

9.8.145 qppb-policy enable

Function

The **qppb-policy enable** command enables a QPPB policy on an interface.

The **undo qppb-policy enable** command disables a QPPB policy on an interface.

By default, no QPPB policy is enabled on an interface.

Format

qppb-policy *policy-name* **enable**

undo qppb-policy *policy-name* **enable**

Parameters

Parameter	Description	Value
policy-name	Specifies a QPPB policy name.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A QPPB local policy needs to be defined during QPPB deployment. After binding the QoS policy ID (qos local-id) carried in a local route to a specified traffic behavior, you need to enable the QPPB local policy on an interface.

Prerequisites

The **qppb local-policy** *policy-name* command has been executed in the system view to create the QPPB local policy.

Example

Enable a QPPB policy on GigabitEthernet0/0/0.

```
<Huawei> system-view
[Huawei] qppb local-policy 1
[Huawei-local-policy-1] quit
[Huawei] interface GigabitEthernet 0/0/0
[Huawei-GigabitEthernet0/0/0] qppb-policy 1 enable
```

Related Topics

9.8.144 qppb local-policy

9.8.146 reflect between-clients

Function

The **reflect between-clients** command enables route reflection among clients.

The **undo reflect between-clients** command disables route reflection among clients.

By default, route reflection among clients is enabled.

Format

reflect between-clients

undo reflect between-clients

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On some networks, if the clients of an RR establish full-mesh connections with each other, they can directly exchange routing information. Route reflection

among clients is unnecessary. The **undo reflect between-clients** command can be used to prohibit the clients from reflecting routes to each other to reduce costs.

Prerequisites

An RR has been configured.

Precautions

The **reflect between-clients** command is run only on RRs.

Example

Disable route reflection among fully-meshed clients.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] group rr-client internal
[Huawei-bgp] peer 10.1.2.1 group rr-client
[Huawei-bgp] peer 10.1.3.1 group rr-client
[Huawei-bgp] peer 10.1.4.1 group rr-client
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] peer rr-client reflect-client
[Huawei-bgp-af-ipv4] undo reflect between-clients
```

Related Topics

9.8.148 reflector cluster-id

9.8.133 peer reflect-client

9.8.147 reflect change-path-attribute

Function

The **reflect change-path-attribute** command enables an route-reflector (RR) to modify the route attributes of BGP routes using the export policy.

The **undo reflect change-path-attribute** command disables an RR from modifying the route attributes of BGP routes using the export policy.

By default, an RR is disabled from modifying route attributes of BGP routes using the export policy.

Format

reflect change-path-attribute

undo reflect change-path-attribute

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Using an RR to modify route attributes may cause route loops. You cannot enable an RR to modify the route attributes using the export policy. So an RR is disabled from modifying route attributes using the export policy by default.

To re-plan the network traffic, run the **reflect change-path-attribute** command to enable the RR to modify the route attributes using the export policy. After the command is run, the following configurations take effect.

- Run the **apply as-path** command to modify the AS-Path attributes of BGP routes.
- Run the **apply comm-filter delete** command to delete all community attributes from BGP routes.
- Run the **apply community** command to modify the community attributes of BGP routes.
- Run the **apply cost** command to modify the cost of BGP routes, that is to modify its MED.
- Run the **apply ip-address next-hop** command to modify the next hop of BGP routes.
- Run the **apply ipv6 next-hop** command to modify the next hop of BGP4+ routes.
- Run the **apply local-preference** command to modify the local preference of BGP routes.
- Run the **apply origin** command to modify the Origin attributes of BGP routes.
- Run the **apply extcommunity** command to modify the extended community attributes of BGP routes.

After the **undo reflect change-path-attribute** command is used, the previous configurations on the RR do not take effect.

Precautions

Export policies on the RR do not take effect before the **reflect change-path-attribute** command is run. After the **reflect change-path-attribute** command is run, these configurations may take effect and affect BGP route selection. Exercise caution when using this command.

For example, peer relationships are established between Router A(10.1.1.1) and Router B(10.1.1.2), and Router A functions as an RR. If two configurations are on RouterA:

1. [Huawei] **bgp 65001**
   [Huawei-bgp] **peer 10.1.1.2 next-hop-local**

2.
```
[Huawei] route-policy aa permit node 10
[Huawei-route-policy] apply ip-address next-hop 10.3.3.3
[Huawei-route-policy] quit
[Huawei] bgp 65001
[Huawei-bgp] peer 10.1.1.2 route-policy aa export
```

Then:

- Before the **reflect change-path-attribute** command is run, the former configuration takes effect but the latter does not. After A receives routes information from its IBGP peers, it reflects the information to Router B, and changes the next hop to 10.1.1.1.
- After the **reflect change-path-attribute** command is run, the latter configuration takes effect but the former does not. After A receives routes information from its IBGP peers, it reflects the information to Router B, and changes the next hop to 10.3.3.3.

NOTE

After you enable the **reflect change-path-attribute** command on the RR, the **peer route-policy export** command takes precedence over the **peer next-hop-invariable** and **peer next-hop-local**.

Example

Enable the RR to modify the route attributes of the BGP routes by using the export policy.

```
<Huawei> system-view
[Huawei] bgp 65001
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] reflect change-path-attribute
```

9.8.148 reflector cluster-id

Function

The **reflector cluster-id** command sets a cluster ID for an RR.

The **undo reflector cluster-id** command restores the default setting.

By default, each RR uses its router ID as the cluster ID.

Format

reflector cluster-id *cluster-id*

undo reflector cluster-id

Parameters

Parameter	Description	Value
cluster-id	Specifies the cluster ID of an RR.	The value can be an integer ranging from 1 to 4294967295 or in the format of an IPv4 address.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view

NOTE

The AR100&AR120&AR150&AR160&AR200 series does not support BGP-VPNv4 address family view, BGP-VPNv6 address family view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Sometimes, more than one RR needs to be configured in a cluster to improve network reliability and prevent single-point failures. If a cluster has more than one RR, the **reflector cluster-id** command needs to be used to set the same cluster ID for the RRs. This helps to identify the cluster and avoid routing loops.

Configuring an RR allows IBGP peers to advertise routes learned in the local AS to each other. The Cluster_List attribute is introduced to avoid loops within an AS. The Cluster_List is composed of a series of Cluster_IDs. It records all the RRs through which a route passes.

Precautions

If the **reflector cluster-id** command is run several times, the latest configuration overrides the previous one.

The **reflector cluster-id** command is run only on RRs.

To enable clients to receive routes reflected by RRs, ensure that the cluster ID of the RRs is different from the router ID of any client. If the cluster ID of the RRs is the same as the router ID of a client, the client will discard received routes.

Example

Configure the cluster ID to 50 for the router, which is an RR in a cluster.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] reflector cluster-id 50
```

Related Topics

9.8.146 reflect between-clients

9.8.133 peer reflect-client

9.8.149 refresh bgp

Function

The **refresh bgp** command softly resets a BGP connection.

Format

refresh bgp [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

refresh bgp ipv6 { **all** | **group** *group-name* | *ipv4-address* | *ipv6-address* | **external** | **internal** } { **export** | **import** }

refresh bgp vpnv6 { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

refresh bgp vpn-instance *vpn-instance-name* **ipv6-family** { **all** | *ipv6-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Softly resets the connection of a specified VPN instance enabled with an IPv4 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpnv4	Softly resets the BGP connections in a VPNv4 address family. **NOTE** The AR100&AR120&AR150&AR160&AR200 series does not support this parameter.	-
all	Softly resets all the BGP IPv4 connections.	-
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
group *group-name*	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
external	Softly resets EBGP connections.	-
internal	Softly resets IBGP connections.	-
export	Triggers outbound soft resetting.	-
import	Triggers inbound soft resetting.	-
ipv6	Softly resets BGP4+ connections.	-
ipv6-address	Specifies the IPv6 address of a BGP4+ peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vpnv6	Softly resets the BGP connections in a VPNv6 address family.	-
vpn-instance *vpn-instance-name* **ipv6-family**	Reset the connection of a specified VPN instance enabled with an IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device's peer supports route-refresh, the **refresh bgp** command can be used on the device to softly reset the BGP connection with the peer. BGP soft resetting can be used to refresh the BGP routing table and apply new routing policies, without closing any BGP connection.

Prerequisites

Configuring BGP soft resetting requires that the peers support the route-refresh capability.

Precautions

Assume that a device supports route-refresh and is configured with the **peer keep-all-routes** command. After the **refresh bgp** command is run on the device, the device does not refresh its routing table.

Example

Perform inbound soft resetting for all BGP connections to make new configurations take effect.

```
<Huawei> refresh bgp all import
```

Related Topics

9.8.121 peer keep-all-routes

9.8.150 refresh bgp mdt

Function

The **refresh bgp mdt** command softly resets the BGP connections related to Multicast Distribution Tree (MDT), manually.

The softly resetting of BGP connection related to MDT can refresh the BGP routing table and apply a new policy without cutting off the BGP connection.

Format

refresh bgp mdt { *ipv4-address* | **all** | **group** *group-name* | **internal** | **external** } { **import** | **export** }

Parameters

Parameter	Description	Value
all	Softly resets all the BGP connections related to MDT.	-
ipv4-address	Specifies the IPv4 address of the BGP peer.	It is in dotted decimal notation.
group *group-name*	Specifies the name of the BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Softly resets EBGP connections.	-
internal	Softly resets IBGP connections.	-
export	Triggers softly reset at the outgoing interface.	-
import	Triggers softly reset at the incoming interface.	-

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a device's peer supports route-refresh, the **refresh bgp mdt** command can be used on the device to softly reset the BGP connection related to MDT with the peer. BGP soft resetting can be used to refresh the BGP routing table and apply new routing policies, without closing any BGP connection.

If a delay is configured to apply a route-policy:

- If an import policy is configured to filter the routes learned from a peer or peer group using the **peer route-policy import** command, BGP applies the import policy immediately when the **refresh bgp mdt all** command is run.
- If an export policy is configured to filter the routes to be sent to a peer or peer group using the **peer route-policy export** command, BGP does not apply the export policy until the configured delay expires although the **refresh bgp mdt all** command is run.

Prerequisites

The route-refresh capability has been enabled on all BGP devices on the network.

Precautions

Assume that a device supports route-refresh and is configured with the **peer keep-all-routes** command. After the **refresh bgp mdt** command is run on the device, the device does not refresh its routing table.

Example

Softly reset all the BGP connections related to MDT at the incoming interface to validate the new configuration.

```
<Huawei> refresh bgp mdt all import
```

Related Topics

9.8.121 peer keep-all-routes

9.8.151 refresh bgp multicast

Function

The **refresh bgp multicast** command softly resets an MBGP connection. MBGP soft resetting can be used to refresh the MBGP routing table and apply new routing policies, without closing any MBGP connection.

Format

refresh bgp multicast { *peer-address* | **all** | **group** *group-name* } { **import** | **export** }

Parameters

Parameter	Description	Value
peer-address	Softly resets the MBGP connections with a specified peer.	The peer address is in dotted decimal notation.
all	Softly resets all MBGP connections.	-
group-name	Specifies the name of an MBGP peer group. If the parameter is set, the MBGP connections between a device and the members of the specified MBGP peer group are softly reset.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Triggers inbound soft resetting.	-
export	Triggers outbound soft resetting.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

MBGP soft resetting requires that all MBGP devices on a network support the route-refresh capability. The **reset bgp** command can be used on a device that does not support the route-refresh capability to reset the connections between the device and its peer and enable the device to refresh its routing table.

Example

Perform inbound soft resetting for all the MBGP connections to make new configurations take effect.

```
<Huawei> refresh bgp multicast all import
```

9.8.152 refresh bgp multicast external

Function

The **refresh bgp multicast external** command softly resets the connections between multicast EBGP peers.

Format

refresh bgp multicast external { **import** | **export** }

Parameters

Parameter	Description	Value
import	Triggers inbound soft resetting.	-
export	Triggers outbound soft resetting.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Trigger inbound soft resetting for all multicast EBGP connections.

```
<Huawei> refresh bgp multicast external import
```

Related Topics

9.8.121 peer keep-all-routes

9.8.153 refresh bgp multicast internal

Function

The **refresh bgp multicast internal** command softly resets the connections between multicast IBGP peers.

Format

refresh bgp multicast internal { **import** | **export** }

Parameters

Parameter	Description	Value
import	Triggers inbound soft resetting.	-
export	Triggers outbound soft resetting.	-

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Trigger inbound soft resetting for all multicast IBGP connections.

```
<Huawei> refresh bgp multicast internal import
```

9.8.154 reset bgp

Function

The **reset bgp** command resets specified BGP connections.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family** | **vpnv4**] { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **group** *group-name* | **external** | **internal** } [**graceful**]

reset bgp ipv4 all [**graceful**]

reset bgp ipv6 { **all** | *as-number-plain* | *as-number-dot* | **group** *group-name* | *ipv6-address* | *ipv4-address* | **external** | **internal** } [**graceful**]

reset bgp vpnv6 { **all** | *as-number-plain* | *as-number-dot* | *ipv4-address* | **group** *group-name* | **external** | **internal** } [**graceful**]

reset bgp vpn-instance *vpn-instance-name* **ipv6-family** { **all** | *as-number-plain* | *as-number-dot* | *ipv6-address* | **group** *group-name* | **external** } [**graceful**]

reset bgp evpn { **all** | *as-number-plain* | *as-number-dot* | **group** *group-name* | *ipv4-address* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Reset the connection of a specified VPN instance enabled with an IPv4 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
vpnv4	Reset BGP connections associated with VPNv4. **NOTE** The AR150&AR160&AR200 series does not support this parameter.	-
all	Reset all BGP connections.	-
as-number-plain	Integral AS number.	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Reset the BGP connection with a specified peer.	It is in dotted decimal notation.
group *group-name*	Reset the BGP connection with a specified peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Reset all EBGP connections.	-
internal	Reset all IBGP connections.	-
ipv4	Reset BGP IPv4 connections.	-
ipv6	Reset BGP IPv6 connections.	-
ipv6-address	Reset the TCP connection with a specified BGP4+ peer (all the routes learned by using the connection are deleted).	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vpnv6	Reset BGP connections associated with VPNv6.	-
vpn-instance *vpn-instance-name* **ipv6-family**	Reset the connection of a specified VPN instance enabled with an IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
graceful	Specifies to reset BGP connections in GR mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
evpn	Resets BGP connections associated with the EVPN address family.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **reset bgp** command is used to make new BGP configurations take effect.

If a BGP routing policy is configured on the device that does not support Route-Refresh, the **reset bgp** command can be used to make the new routing policy to take effect.

To reset a BGP connection in GR mode, run the **reset bgp** command with the **graceful** parameter specified and run the **graceful-restart peer-reset** command. If the **graceful** parameter is not specified in the **reset bgp** command or if the **graceful-restart peer-reset** command is not run, the GR reset mode does not take effect, so that routing entries will be deleted for existing sessions, interrupting services. The services will be restored after the BGP peer relationship is reestablished.

The **reset bgp ipv4 all** command resets all public-network BGP IPv4 connections.

Precautions

After the **reset bgp** command is run on a device, the TCP connection established by the BGP device and the corresponding peer relationship is re-established. Exercise caution when running this command.

Example

Reset all BGP connections.

```
<Huawei> reset bgp all
```

Reset BGP connections with the peer 2345:ABCD::9.

```
<Huawei> reset bgp ipv6 2345:ABCD::9
```

Reset BGP sessions with BGP peers within a specified 4-byte AS number.

```
<Huawei> reset bgp vpnv4 200.300
```

Reset all BGP VPNv6 connections.

```
<Huawei> reset bgp vpnv6 all
```

 Copyright © Huawei Technologies Co., Ltd.

9.8.155 reset bgp dampening

Function

The **reset bgp dampening** command clears BGP route dampening information and release the suppressed routes.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] **dampening** [*ipv4-address* [*mask* | *mask-length*]]

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } **dampening** [*ipv6-address prefix-length*]

reset bgp vpnv4 dampening [*ipv4-address* [*mask* | *mask-length*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears the route dampening information of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-family	Indicates an IPv4 unicast address family.	-
ipv4-address	Specifies an IPv4 network address.	It is in dotted decimal notation.
mask	Specifies the network mask in dotted decimal notation. If neither of the mask and mask length is specified, the address is considered as a classful address.	It is in dotted decimal notation.
mask-length	Specifies the network mask length. If neither of the mask and mask length is specified, the address is considered as a classful address.	The value is an integer that ranges from 0 to 32.
ipv6	Clears IPv6 route dampening information and releases the suppressed routes.	-
ipv6-family	Indicates an IPv6 unicast address family.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-address	Specifies the IPv6 network address.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the length of an IPv6 prefix in decimal notation. It specifies the number of bits in the network address.	The value is an integer that ranges from 0 to 128.
vpnv4	Clears the route dampening information of the BGP VPNv4 routes and releases the suppressed routes.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Route dampening is enabled to solve the problem of route instability. In most situations, BGP is applied to complex networks where routes change frequently. Route dampening is then used to suppress instable routes.

The **reset bgp dampening** command is used to clear the dampening information about specified routes on the public network and release specified suppressed routes. If no IP address is specified in the command, the dampening information about all the routes on the public network is cleared and all suppressed routes are released.

Prerequisites

You can use **display bgp routing-table dampened** command to view the information about suppressed routes.

Precautions

After the **reset bgp dampening** command is run, the suppressed routes are released. If the status of some routes still changes frequently, route flapping may occur. Routing flapping consumes a large number of bandwidth and CPU resources.

When *ipv6-address prefix-length* is not specified, after you run the **reset bgp ipv6 dampening** command, IPv6 route dampening information in the whole BGP routing table is cleared.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear the dampening information about routes to network segment 10.1.0.0 and release suppressed routes.

```
<Huawei> reset bgp dampening 10.1.0.0 255.255.0.0
```

Clear the dampening information about the IPv6 routes to network segment FC00:0:0:1:: and release suppressed routes.

```
<Huawei> reset bgp ipv6 dampening fc00:0:0:1:: 64
```

Clear the dampening information about the routes of IPv6 VPN instance named vpn1.

```
<Huawei> reset bgp vpn-instance vpn1 ipv6-family dampening
```

Related Topics

9.8.20 dampening

9.8.59 display bgp routing-table dampened

9.8.156 reset bgp flap-info

Function

The **reset bgp flap-info** command clears route flapping statistics.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] **flap-info** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [*mask* | *mask-length*] | **regexp** *as-path-regexp*]

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } **flap-info** [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-ipv6-address prefix-length* | **regexp** *as-path-regexp*]

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] *ipv4-address* **flap-info**

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } *ipv6-address* **flap-info**

reset bgp vpnv4 flap-info [**as-path-filter** { *as-path-filter-number* | *as-path-filter-name* } | *network-address* [*mask* | *mask-length*] | **regexp** *as-path-regexp*]

reset bgp vpnv4 *ipv4-address* **flap-info**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Clears the route flapping information of a specified VPN instance enabled with an IPv4 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
as-path-filter *as-path-filter-number*	Clears route flapping statistics based on a specified AS_Path filter.	It is an integer that ranges from 1 to 256.
as-path-filter *as-path-filter-name*	Clears route flapping statistics based on a specified AS_Path filter.	The value of *as-path-filter-name* is a string of 1 to 51 case-sensitive characters. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
network-address	Specifies the IPv4 prefix address that is used to filter the BGP IPv4 routes.	It is in dotted decimal notation.
mask	Specifies the network mask that is used to filter the BGP IPv4 routes. If the mask or mask length is not specified, the address is processed as a classful address.	It is in dotted decimal notation.
mask-length	Specifies the network mask length that is used to filter the BGP IPv4 routes. If the mask or mask length is not specified, the address is processed as a classful address.	The value is an integer that ranges from 0 to 32.
regexp *as-path-regexp*	Clears statistics about the flapping routes that match the AS_Path regular expression.	-
ipv6	Clears the route flapping statistics on all IPv6 peers.	-
vpn-instance *vpn-instance-name* **ipv6-family**	Clears the route flapping information of a specified VPN instance enabled with an IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
network-ipv6-address	Specifies the IPv6 prefix address that is used to filter the BGP IPv6 routes.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the network mask length that is used to filter the BGP IPv6 routes.	The value is an integer that ranges from 0 to 128.
ipv4-address	Specifies the network address of an IPv4 peer.	It is in dotted decimal notation.
ipv6-address	Specifies the network address of an IPv6 peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
vpnv4	Resets route flapping statistics of BGP VPNv4 routes.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The process of adding a route to and then deleting the route from a routing table is called route flapping.

When route flapping occurs, the routing protocol sends Update packets to neighbors. The neighbors that receive the Update packets needs to recalculate routes and modify its routing table. Therefore, frequent route flapping consumes great bandwidth and CPU resources and even seriously affects network operations.

The **reset bgp flap-info** command is used to clear the flapping information about routes. This allows the router to re-collect statistics about flapping routes and helps to monitor route changes and locate network problems.

Prerequisites

You can use **display bgp routing-table flap-info** command to view the information about BGP route flapping.

If there are a large number of flapping routes, define an AS_Path filter or an AS_Path regular expression to be referenced in the **reset bgp flap-info** command. The flapping statistics of the routes matching the AS_Path filter or the AS_Path regular expression are then cleared.

Precautions

After the **reset bgp flap-info** command is run, the flapping statistics of routes are reset and cannot be displayed.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

After the flapping statistics of routes are cleared, run the **display bgp routing-table flap-info** command again to display the flapping statistics about BGP routes in order to locate problems.

Example

Clear the flapping statistics about the routes that match AS_Path filter 10.

```
<Huawei> reset bgp flap-info as-path-filter 10
```

Clear the flapping statistics about the BGP4+ routes of the VPN instance named vpn1.

```
<Huawei> reset bgp vpn-instance vpn1 ipv6-family flap-info
```

Related Topics

9.8.20 dampening

9.8.157 reset bgp flapping-count

Function

The **reset bgp flapping-count** command resets the flapping count of a specified BGP peer.

Format

reset bgp [**vpn-instance** *vpn-instance-name* **ipv4-family**] *ipv4-address* **flapping-count**

reset bgp { **ipv6** | **vpn-instance** *vpn-instance-name* **ipv6-family** } *ipv6-address* **flapping-count**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv4-family**	Specifies the name of VPN instance enabled with an IPv4 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6	Clears the flapping count of a specified BGP IPv6 peer.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name* **ipv6-family**	Specifies the name of VPN instance enabled with an IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The prefix is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

BGP peer flapping affects the stability of a BGP network and BGP route convergence.

The **reset bgp flapping-count** command can be used to clear the flapping account of a BGP peer. This allows the router to re-collect the flapping statistics of a peer to locate BGP network problems.

Precautions

After the **reset bgp flapping-count** command is run, the flapping statistics of BGP peers are reset and cannot be displayed.

Follow-up Procedure

After the reset bgp flapping-count command is used to clear the statistics count of a specified BGP peer, run the **display bgp peer** command to display the flapping count of BGP peers and locate BGP network problems.

Example

Clear the flapping count of a specified BGP peer.

```
<Huawei> reset bgp 10.116.10.2 flapping-count
```

9.8.158 reset bgp mdt

Function

The **reset bgp mdt** command resets the specified BGP connection related to MDT.

Format

reset bgp mdt { **all** | *ipv4-address* | **group** *group-name* | *as-number-plain* | *as-number-dot* } [**graceful**]

reset bgp mdt { **internal** | **external** } [**graceful**]

Parameters

Parameter	Description	Value
all	Resets all the BGP connections related to MDT.	-
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
ipv4-address	Resets the connections with a specified BGP peer.	It is in dotted decimal notation.
group *group-name*	Resets the BGP connections related to MDT with the specified peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Resets all EBGP connections related to MDT.	-
internal	Resets all IBGP connections related to MDT.	-
graceful	Specifies to reset BGP connections related to MDT in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **reset bgp mdt** command is used to make new BGP configurations take effect.

If a BGP routing policy is configured on the router that does not support Route-Refresh, the **reset bgp mdt** command can be used to make the new routing policy to take effect.

To reset a BGP connection in GR mode, run the **reset bgp mdt** command with the **graceful** parameter specified and run the **graceful-restart peer-reset** command. If the **graceful** parameter is not specified in the **reset bgp mdt** command or if the **graceful-restart peer-reset** command is not run, the GR reset mode does not take effect, so that routing entries will be deleted for existing sessions, interrupting services. The services will be restored after the BGP peer relationship is reestablished.

NOTICE

After you run this command, the TCP connection is reset, and the neighbor relationship between two peers is reestablished. So, confirm the action before you use the command.

Example

Reset all BGP connections related to MDT.

```
<Huawei> reset bgp mdt all
```

9.8.159 reset bgp multicast

Function

The **reset bgp multicast** command resets the connections between a device and specified MBGP peers.

Format

reset bgp multicast { **all** | *peer-address* | **group** *group-name* | *as-number-plain* | *as-number-dot* | **external** | **internal** } [**graceful**]

Parameters

Parameter	Description	Value
all	Resets all MBGP connections.	-
peer-address	Resets the MBGP connection with a specified peer.	The peer address is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group *group-name*	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.
external	Reset all EBGP connections.	-
internal	Reset all IBGP connections.	-
graceful	Specifies to reset MBGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

NOTE

After the **reset bgp multicast** is run on a device, the TCP connection established by the device and the corresponding peer relationship is reset and then re-established. Exercise caution when running this command.

Example

Reset the MBGP connections of all address families.

```
<Huawei> reset bgp multicast all
```

9.8.160 reset bgp multicast dampening

Function

The **reset bgp multicast dampening** command clears dampening information about routes in the MBGP routing table.

Format

reset bgp multicast dampening [*ip-address* [*mask* | *mask-length*]]

Parameters

Parameter	Description	Value
ip-address	Specifies a network address.	The value is in dotted decimal notation.
mask	Specifies the mask of a network address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a network address.	The value is an integer that ranges from 0 to 32.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

If a network address is specified in the **reset bgp multicast dampening** command, running this command clears the dampening information about a specific route and releases the suppressed route.

Example

Clear the dampening information about routes to network segment 10.1.0.0 and release suppressed routes.

```
<Huawei> reset bgp multicast dampening 10.1.0.0 255.255.0.0
```

9.8.161 reset bgp multicast external

Function

The **reset bgp multicast external** command resets all multicast EBGP connections.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset bgp multicast external [**graceful**]

Parameters

Parameter	Description	Value
graceful	Specifies to reset MBGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Reset all multicast EBGP connections.

```
<Huawei> reset bgp multicast external
```

9.8.162 reset bgp multicast flap-info

Function

The **reset bgp multicast flap-info** command clears route flapping statistics.

Format

reset bgp multicast flap-info [*ip-address* [*mask* | *mask-length*] | **as-path-filter** { *as-path-list-number* | *as-path-list-name* } | **regexp** *regexp*]

reset bgp multicast *ip-address* **flap-info**

Parameters

Parameter	Description	Value
ip-address	Specifies a network address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a network address.	The value is an integer that ranges from 0 to 32.
mask	Specifies the mask of a network address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
as-path-filter *as-path-list-number*	Clears route flapping statistics based on a specified AS_Path filter.	The value is an integer ranging from 1 to 256.
as-path-filter *as-path-list-name*	Deletes route flapping statistics matching a specified AS_Path filter.	The value is a string of 1 to 51 case-sensitive characters without spaces.
regexp *regexp*	Clears flapping statistics about the routes that match the AS_Path regular expression.	-The value is a string of 1 to 80.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Clear the flapping statistics about the routes that match AS_Path filter 10.

```
<Huawei> reset bgp multicast flap-info as-path-filter 10
```

9.8.163 reset bgp multicast internal

Function

The **reset bgp multicast internal** command resets the multicast IBGP connections in an AS.

Format

reset bgp multicast internal [**graceful**]

Parameters

Parameter	Description	Value
graceful	Specifies to reset MBGP connections in GR mode.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Reset all multicast IBGP connections.

```
<Huawei> reset bgp multicast internal
```

9.8.164 router-id (BGP)

Function

The **router-id** command configures a Router ID for the router.

The **undo router-id** command deletes the Router ID configured for the router.

By default, no BGP Router ID is configured, and the Router ID configured for the route management module through the **router id** command is used.

Format

router-id { *ipv4-address* | **vpn-instance auto-select** }

undo router-id [**vpn-instance auto-select**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies a Router ID.	It is in dotted decimal notation.
vpn-instance auto-select	Configures automatic Router ID selection for all BGP-VPN instance IPv4 address families. If a Router ID is manually specified for a BGP-VPN instance IPv4 address family, the manually specified Router ID takes precedence over the automatically selected Router ID.	-

Views

BGP view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **router-id** command is used to configure a Router ID for the router. Each Router ID uniquely identifies one BGP router in an AS.

By configuring automatic Router ID selection for BGP-VPN instance IPv4 address family, you can differentiate the configured Router ID of BGP-VPN instance IPv4 address family from the BGP Router ID. For more information about the Router ID of a BGP-VPN instance IPv4 address family, see the **router-id (BGP-VPN Instance IPv4 Address Family View)** command.

Prerequisites

The **bgp** command is run to enable BGP.

Precautions

Changing or deleting a configured Router ID in the BGP view resets a BGP session. If a BGP session has been established in a BGP-VPN instance IPv4 address family, deleting the configured Router ID resets the BGP session. Exercise caution when changing or deleting a Router ID.

By default, the router that is not configured with any interface uses the Router ID of 0.0.0.0 assigned by routing management.

Example

Configure a Router ID for the router.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] router-id 10.1.1.1
```

Configure automatic Router ID selection for all BGP-VPN instance IPv4 address families.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] router-id vpn-instance auto-select
```

9.8.165 router-id (BGP-VPN Instance IPv4 Address Family View)

Function

The **router-id** command configures router ID for BGP VPN instance IPv4 address family.

The **undo router-id** command deletes the router ID configured for BGP VPN instance IPv4 address family.

By default, no router ID is configured for BGP VPN instance IPv4 address family, and the BGP router ID is used as the router ID.

Format

router-id { *ipv4-address* | **auto-select** }

undo router-id

Parameters

Parameter	Description	Value
ipv4-address	Specifies the router ID of a BGP VPN instance IPv4 address family. The router ID is expressed in the IPv4 address format.	It is in dotted decimal notation.
auto-select	Configures automatic route ID selection for the current BGP VPN instance IPv4 address family.	-

Views

BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring router ID for BGP VPN instance IPv4 address family, you can differentiate the configured router ID of BGP VPN instance IPv4 address family from the BGP router ID.

For example, if two VPN instances named **vrf1** and **vrf2** are configured on a PE, and a BGP session needs to be established between the interfaces bound to the two VPN instances, you need to configure different router IDs for the two VPN instance IPv4 address families. If no router ID is configured for the two VPN instance IPv4 address families, no BGP session can be established because the two VPN instance IPv4 address families have the same router ID, which is consistent with the BGP router ID.

Rules for automatically selecting a router ID for a BGP VPN instance IPv4 address family are as follows:

- If loopback interfaces configured with IP addresses are bound to the VPN instance, the largest IP address among the IP addresses of the loopback interfaces is selected as the router ID.
- If no loopback interfaces configured with IP addresses are bound to the VPN instance, the largest IP address among the IP addresses of other interfaces bound to the VPN instance is selected as the router ID, regardless of whether the interface is Up or Down.

Precautions

If a BGP session has been established in a BGP VPN instance IPv4 address family, changing or deleting the configured router ID resets the BGP session. So, confirm the action before you use the **router-id** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a router ID for a BGP VPN instance IPv4 address family.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] quit
[Huawei-vpn-instance-vrf1] quit
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpn-instance vrf1
[Huawei-bgp-vrf1] router-id 192.168.100.1
```

9.8.166 route-select delay

Function

The **route-select delay** command configures a delay for selecting routes.

The **undo route-select delay** command deletes the delay for selecting routes.

The default delay is 0, indicating that routes are selected without a delay.

Format

route-select delay *delay-value*

undo route-select delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay for selecting routes.	The value is an integer ranging from 0 to 3600, in seconds.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv6 address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario in which primary and backup routes exist, packets may get lost after traffic switches back to the primary path from the backup path.

Precautions

If you run the **route-select delay** command repeatedly, the latest configuration overrides the previous configurations. If a route selection delay timer has started

when you configure a new route select delay, the new route selection delay takes effect since the next route selection.

Example

Configure the delay for selecting routes as 300s.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] route-select delay 300
```

9.8.167 routing-table limit threshold-alarm

Function

The **routing-table limit threshold-alarm** command configures alarm and alarm clear thresholds for the number of BGP routes.

The **undo routing-table limit threshold-alarm** command restores the default settings.

By default, the alarm threshold is 80%, and the alarm clear threshold is 70%.

Format

routing-table limit threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo routing-table limit threshold-alarm [**upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*]

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies an alarm threshold for the number of BGP routes.	The value is an integer that ranges from 1 to 100, in percentage. The default value is 80.
lower-limit *lower-limit-value*	Specifies an alarm clear threshold for the number of BGP routes.	The value is an integer that ranges from 1 to 100, in percentage. The default value of is 70. *lower-limit-value* must be smaller than *upper-limit-value*; otherwise, alarms are generated and cleared repeatedly if route flapping occurs.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The number of BGP routes that can be added to a routing table is limited. If the value exceeds the limit, new routes cannot be added to the routing table, causing service interruptions. To address this problem, run the **routing-table limit threshold-alarm** command to configure alarm and alarm clear thresholds for the number of BGP routes. Alarms are then generated and cleared as expected. The alarms act as a prompt for checking whether an exception occurs and to take preventive measures.

- When the ratio of BGP routes to the maximum value exceeds *upper-limit-value*, an alarm is generated. New routes can still be accepted until the number of BGP routes reaches the maximum value.
- When the ratio falls below *lower-limit-value*, the alarm is cleared.

Configuration Impact

If the **routing-table limit threshold-alarm** command is run multiple times, the latest configuration takes effect.

Precautions

In addition to the **routing-table limit threshold-alarm** command, the **snmp-agent trap enable feature-name bgp trap-name** { **hwBgpRouteThresholdExceed** | **hwBgpRouteThresholdClear** } command must be run to enable the alarm and alarm clear functions; otherwise, alarms cannot be generated and cleared as expected.

Example

Configure alarm and alarm clear thresholds for the number of BGP routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] routing-table limit threshold-alarm upper-limit 70 lower-limit 60
```

9.8.168 routing-table rib-only

Function

The **routing-table rib-only** command prevents BGP routes from being added into the IP routing table.

The **undo routing-table rib-only** command restores the default setting.

By default, the preferred BGP routes are added to the IP routing table.

Format

routing-table rib-only [**route-policy** *route-policy-name*]

undo routing-table rib-only

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a Route-Policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, if the BGP routing table has large numbers of VPN routes, these routes will consume large numbers of memory resources after being delivered to the IP VPN routing table. If these routes are not used in traffic forwarding, you can run the **routing-table rib-only** command to prevent these routes from being added to the IP VPN routing table. If some of these routes are not used in traffic forwarding, you can run the **routing-table rib-only route-policy** command to prevent this part of routes from being added to the IP VPN routing table.

If a route reflector (RR) is used and preferred BGP routes do not need to be used during the forwarding, the **routing-table rib-only** command can be used to make BGP routes unable to be added to the IP routing table or the forwarding layer. This improves forwarding efficiency and the system capacity.

When **route-policy** *route-policy-name* is specified in the command, the routes matching the policy are not added to the IP routing table, and the routes not matching the policy are added the IP routing table with the route attributes unchanged.

Configuration Impact

After the **routing-table rib-only** command is run, the routes preferred by BGP are not added to the IP routing table.

Precautions

The **routing-table rib-only** command and the **active-route-advertise** command are mutually exclusive.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the routing policy named **ribonly** to prevent certain BGP routes from being added into the IP routing table.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] routing-table rib-only route-policy ribonly
```

9.8.169 shutdown (BGP)

Function

The **shutdown** command terminates all sessions between a device and its BGP peers.

The **undo shutdown** command restores the default setting.

By default, the function of closing all sessions between a device and its BGP peers is disabled.

Format

shutdown

undo shutdown

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

NOTICE

Running the **shutdown** command closes all sessions between a device and its peers. Exercise caution when using this command.

During system upgrade or maintenance, the sessions between a device and its BGP peers need to be closed to minimize the impact of BGP route flapping on the network. If a large number of BGP peers exist, the **shutdown** command can be run in the BGP view to close all sessions with BGP peers. This frees you from running the **peer ignore** command repeatedly to close the sessions one by one.

 Copyright © Huawei Technologies Co., Ltd.

Example

Close all sessions between a device and its BGP peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] shutdown
```

9.8.170 slow-peer detection disable

Function

The **slow-peer detection disable** command disables slow peer detection.

The **undo slow-peer detection disable** command restores the default configuration.

By default, slow peer detection is enabled.

Format

slow-peer detection disable

undo slow-peer detection disable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An update peer-group may consist of multiple BGP peers. If a network problem (for example, congestion) occurs and slows down the speed at which the local device advertises routes to a BGP peer in the update peer-group, the speed at which the local device advertises routes to other BGP peers in the update peer-group is affected. To address this problem, slow peer detection is enabled by default.

When slow peer detection is enabled, the local device identifies the BGP peer to which routes are sent the slowest based on the time taken to send 100 packets to each BGP peer. If this time is greater than the period threshold for slow peer detection plus the average time taken to send 100 packets to BGP peers (excluding the longest and shortest times), the local device considers the peer a

 Copyright © Huawei Technologies Co., Ltd.

slow peer and removes it from the update peer-group. Slow peer detection prevents this slow peer from affecting route advertisement to other peers in the update peer-group.

To disable slow peer detection, run this command.

Example

Disable slow peer detection.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] slow-peer detection disable
```

9.8.171 slow-peer detection threshold

Function

The **slow-peer detection threshold** command sets a period threshold for slow peer detection.

The **undo slow-peer detection** command restores the default configuration.

By default, the period threshold for slow peer detection is 300s.

Format

slow-peer detection threshold *threshold-value*

undo slow-peer detection [**threshold** *threshold-value*]

Parameters

Parameter	Description	Value
threshold-value	Specifies a period threshold for slow peer detection. If the time taken to send 100 packets to a BGP peer is greater than the configured period plus the average time taken to send 100 packets to BGP peers (excluding the longest and shortest times), the local device considers the peer a slow peer.	The value is an integer ranging from 120 to 3600, in seconds.

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv6 unicast address family view, BGP-VPNv4 address family view, BGP-VPNv6 address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When slow peer detection is enabled, the local device identifies the BGP peer to which routes are sent the slowest based on the time taken to send 100 packets to each BGP peer. If this time is greater than the period threshold for slow peer detection plus the average time taken to send 100 packets to BGP peers (excluding the longest and shortest times), the local device considers the peer a slow peer and removes it from the update peer-group. Slow peer detection prevents this slow peer from affecting route advertisement to other peers in the update peer-group.

By default, slow peer detection is enabled and the period threshold for slow peer detection is 300s. To adjust the period threshold for slow peer detection, run this command.

Configuration Impact

If the command is run more than once, the latest configuration overrides the previous one.

Precautions

After a slow peer is removed from the update peer-group, the peer relationship between the local device and the slow peer is reestablished.

Example

Set the period threshold for slow peer detection to 200s.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] slow-peer detection threshold 200
```

9.8.172 snmp-agent trap enable feature-name bgp

Function

The **snmp-agent trap enable feature-name bgp** command enables the trap function for the BGP module.

The **undo snmp-agent trap enable feature-name bgp** command disables the trap function for the BGP module.

By default, the trap function is disabled for the BGP module.

Format

snmp-agent trap enable feature-name bgp [**trap-name** { **backward** | **established** | **grstatuschange** | **hwbackward** | **hwestablished** | **routethresholdclear** | **routethresholdexceed** | **hwbgproutethresholdclear** | **hwbgproutethresholdexceed** | **hwbgproutemaxclear** | **hwbgproutemaxexceed** | **hwbgpdynamicpeersessionexceed** | **hwbgpdynamicpeersessionexceedclear** }]

undo snmp-agent trap enable feature-name bgp [**trap-name** { **backward** | **established** | **grstatuschange** | **hwbackward** | **hwestablished** |

routethresholdclear | **routethresholdexceed** | **hwbgproutethresholdclear** | **hwbgproutethresholdexceed** | **hwbgproutemaxclear** | **hwbgproutemaxexceed** | **hwbgpdynamicpeersessionexceed** | **hwbgpdynamicpeersessionexceedclear** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for a specified type of BGP events.	-
backward	Enables the trap function upon the disconnection of BGP neighbors.	-
established	Enables the trap function when BGP neighbors are in Established state.	-
grstatuschange	Enables the trap upon the BGP GR status change.	-
hwbackward	Enables the trap function upon the disconnection of BGP neighbors.	-
hwestablished	Enables the trap function when BGP neighbors are in Established state.	-
routethresholdclear	Enables the trap function when the number of BGP routes falls below the trap threshold.	-
routethresholdexceed	Enables the trap function when the number of BGP routes exceeds the trap threshold.	-
hwbgproutethresholdclear	Enables the trap function when the number of BGP routes falls below the threshold.	-
hwbgproutethresholdexceed	Enables the trap function when the number of BGP routes exceeds the threshold.	-
hwbgproutemaxclear	Enables the trap function when the number of BGP routes falls below the lower threshold of the maximum value.	-
hwbgproutemaxexceed	Enables the trap function when the number of BGP routes exceeds the upper threshold of the maximum value.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwbgpdynamicpeersessionexceed	Enables the alarm that is generated when the number of dynamic BGP peer sessions exceeds the maximum number.	-
hwbgpdynamicpeersessionexceedclear	Enables the alarm that is generated when the number of dynamic BGP peer sessions falls below the maximum number.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The BGP module is not configured with the function of excessive traps. To enable the trap function for one or more events, specify the **trap-name** parameter.

Example

Enable the trap function upon the disconnection of BGP neighbors.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name bgp trap-name backward
```

9.8.173 summary automatic

Function

The **summary automatic** command enables automatic aggregation for the locally-imported routes.

The **undo summary automatic** command disables automatic aggregation for the locally-imported routes.

By default, automatic aggregation is disabled for the locally-imported routes.

Format

summary automatic

undo summary automatic

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **summary automatic** command is used in the BGP-IPv4 unicast address family view to configure a BGP device to automatically aggregate locally-imported routes on the public network.

The **summary automatic** command is used in the BGP-VPN instance IPv4 address family view to configure a BGP device to automatically aggregate locally-imported routes on a private network.

The **summary automatic** command is used to aggregate the routes imported by BGP. These routes can be direct routes, static routes, RIP routes, OSPF routes, or IS-IS routes. After this command is run on a BGP device, the BGP device aggregates routes based on the natural network segment (for example, 10.1.1.0/24 and 10.2.1.0/24 are aggregated to 10.0.0.0/8, a Class A address), and sends only the aggregated route to its peers. This reduces the number of routes.

Precautions

BGP route aggregation is classified into manual aggregation and automatic aggregation. The command is used to implement automatic aggregation. Manual aggregation takes precedence over automatic aggregation.

The **summary automatic** command is invalid for the routes imported by using the **network** command.

Example

Enable automatic aggregation for imported routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] summary automatic
```

Related Topics

9.8.2 aggregate (BGP)

9.8.174 supernet unicast advertise

Function

The **supernet unicast advertise enable** command configures a BGP device to advertise BGP supernet unicast routes to its peers.

 Copyright © Huawei Technologies Co., Ltd.

The **undo supernet unicast advertise enable** or **supernet unicast advertise disable** command restores the default configuration.

By default, BGP supernet unicast routes are considered invalid and cannot be advertised to BGP peers or delivered to the IP routing table.

Format

supernet unicast advertise enable

supernet unicast advertise disable

undo supernet unicast advertise enable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-VPN instance IPv4 address family view, BGP-IPv6 unicast address family view, or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BGP supernet route has the same destination address and next hop address or has a more detailed destination address than the next hop address. Any route that meets one of the following conditions is a BGP supernet route.

- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are the same, and the destination address mask is greater than or equal to the next hop address mask.
- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are different. However, if you perform bitwise AND operations on the next hop address mask with the destination address and next hop address, respectively, the calculated network addresses are the same.

For example, the route destined for 10.6.6.6 in the following command output is a BGP supernet route.

```
<Huawei> display bgp routing-table
 BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn
  *>i  10.6.6.6/32        10.6.6.6       0          100       0       ?
```

BGP supernet routes include BGP supernet labeled routes and BGP supernet unicast routes. To allow a Huawei device to advertise BGP supernet unicast routes that it receives from a connected non-Huawei device to its BGP peers, run the **supernet unicast advertise enable** command on the Huawei device.

Example

Configure a BGP device to advertise BGP supernet unicast routes to its peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] supernet unicast advertise enable
```

9.8.175 timer (BGP)

Function

The **timer** command sets the values for the Keepalive timer and Hold timer.

The **undo timer** command restores the default values of the Keepalive timer and Hold timer.

By default, the value of a Keepalive timer is 60s and the value of a Hold timer is 180s.

Format

timer keepalive *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo timer keepalive *keepalive-time* **hold** *hold-time* [**min-holdtime** *min-holdtime*]

undo timer keepalive hold [**min-holdtime**]

Parameters

Parameter	Description	Value
keepalive *keepalive-time*	Specifies the Keepalive period.	The value is an integer ranging from 0 to 21845, in seconds.
hold *hold-time*	Specifies the holdtime.	The value is an integer that can be 0, or ranges from 3 to 65535, in seconds.
min-holdtime *min-holdtime*	Specifies the minimum Holdtime configured on the local device. **NOTE** The value of *min-holdtime* configured cannot exceed the value of *hold-time*.	The value is an integer ranging from 20 to 65535, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a connection is established between peers, the values of *keepalive-time* and *hold-time* are negotiated by the peers.

- The smaller of the *hold-time* values carried by Open messages of both peers is taken as the *hold-time* value.
- The smaller of one third of the *hold-time* value and the locally configured *keepalive-time* value is taken as the *keepalive-time* value.

If the local device establishes BGP peer relationships with many devices, it needs to process huge BGP messages. If *hold-time* negotiated among BGP peers is small, the timer may expire before the local device processes the Keepalive messages sent from other BGP peers. The peer relationships are then interrupted, and routes flap. To solve the preceding problem, you can configure an appropriate value for **min-holdtime** *min-holdtime* based on the CPU processing capability of the local device.

If the value of *min-holdtime* is changed, but the values of *keepalive-time* and *hold-time* negotiated between two BGP peers remain unchanged, the established peer relationship is not affected. Only when the local device attempts to re-establish a relationship with a remote device, the value of *min-holdtime* configured on the local device takes effect. The local device compares *min-holdtime* with *hold-time* sent from the remote device. If the value of *min-holdtime* exceeds that of *hold-time*, *hold-time* negotiation fails, and the peer relationship fails to be established.

NOTE

If *min-holdtime* is configured on the local device, and the value of *hold-time* sent from the remote device is 0, *hold-time* negotiation between the two devices succeeds. The negotiated value of *hold-time* is 0, and the peer relationship is established. The value 0 of *hold-time* indicates that the peer relationship never expires.

Precautions

The timers configured for a specific peer or peer group by using the **peer timer** command override the timers configured for all BGP peers by using the **timer** command.

If the value of a timer changes, the BGP peer relationship between devices is disconnected. This is because the devices need to re-negotiate the values of *keepalive-time* and *hold-time*. Therefore, exercise caution before changing the value of a timer.

Setting the Hold timer value to at least three times the Keepalive timer value is recommended. When setting the values of *keepalive-time* and *hold-time*, note the following points:

 Copyright © Huawei Technologies Co., Ltd.

- The values of *keepalive-time* and *hold-time* cannot both be set to 0. This renders the BGP timers become invalid. This means that BGP is unable to detect link faults using the timers.
- The *hold-time* value cannot be significantly greater than the *keepalive-time* value. A setting of **timer keepalive 1 hold 65535**, for example, would be improper. If the holdtime is too long, link faults cannot be detected in a timely manner.

Example

On a BGP device, set the value of the Keepalive timer to 30s and the value of the Hold timer to 90s.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] timer keepalive 30 hold 90
```

Related Topics

9.8.137 peer timer

9.8.176 timer connect-retry

Function

The **timer connect-retry** command sets a global ConnectRetry interval.

The **undo timer connect-retry** command restores the default setting.

By default, the ConnectRetry interval is 32s.

Format

timer connect-retry *connect-retry-time*

undo timer connect-retry

Parameters

Parameter	Description	Value
connect-retry-time	Specifies a ConnectRetry interval.	The value is an integer ranges from 1 to 65535, in seconds.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Applicable Environment

When BGP initiates a TCP connection, the ConnectRetry timer is stopped if the TCP connection is established successfully. If the first attempt to establish a TCP connection fails, BGP tries again to establish the TCP connection after the ConnectRetry timer expires. The ConnectRetry interval can be adjusted as needed.

- The ConnectRetry interval can be reduced in order to lessen the time BGP waits to retry establishing a TCP connection after the first attempt fails.
- To suppress route flapping caused by constant peer flapping, the ConnectRetry interval can be increased to accelerate route convergence.

Note

A ConnectRetry interval can be configured globally, or on a particular peer or peer group. A ConnectRetry interval configured on a specific peer or peer group takes precedence over a global ConnectRetry interval.

If both the **peer** { *group-name* | *ipv4-address* } **timer connect-retry** *connect-retry-time* command and the **timer connect-retry** *connect-retry-time* command are run on a device, the configuration of the **peer** { *group-name* | *ipv4-address* } **timer connect-retry** *connect-retry-time* command takes effect, but the configuration of the **timer connect-retry** *connect-retry-time* command does not.

Example

Set a global BGP ConnectRetry interval to 60s.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] timer connect-retry 60
```

Related Topics

9.8.138 peer timer connect-retry

9.8.177 undo synchronization (BGP)

Function

The **undo synchronization** command disables synchronization between BGP and an IGP.

By default, synchronization between BGP and an IGP is disabled.

Format

undo synchronization

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view, BGP-IPv4 multicast address family view, BGP-IPv6 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

None

Precautions

The device does not support synchronization between BGP and IGP.

Example

Disable synchronization between BGP and an IGP.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] undo synchronization
```

9.9 Routing Policy Configuration Commands

9.9.1 apply as-path

Function

The **apply as-path** command sets the action for changing the AS_Path attribute of BGP routes in a routing policy.

The **undo apply as-path** command restores the default setting.

By default, the action for changing the AS_Path attribute of BGP routes is not set in a routing policy.

Format

apply as-path { { *as-number-plain* | *as-number-dot* } &<1-10> { **additive** } | **none overwrite** }

undo apply as-path

Parameters

Parameter	Description	Value
as-number-plain	Specifies a integral AS number to be added to the AS_Path list or to replace the existing AS_Path list. A maximum of 10 AS numbers can be specified in one command.	The value is an integer ranging from 1 to 4294967295.

Parameter	Description	Value
as-number-dot	Specifies an AS number in dotted notation to be added to the AS_Path list or to replace the existing AS_Path list. A maximum of 10 AS numbers can be specified in one command.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
additive	Adds the specified AS number to the original AS_Path attribute.	-
overwrite	Replaces the original AS_Path with the specified AS number.	-
none	Clears the original AS_Path list.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the AS_Path attribute of BGP routes BGP for selecting the optimal route, you can apply a routing policy containing the **apply as-path** command.

AS_Path is a private attribute of BGP and records all ASs that a route passes through from the local end to the destination address. Using the AS_Path attribute controls route selection and prevents routing loops. If multiple routes are destined for the same destination address, BGP compares the AS_Path lists of these routes and considers the route with the shortest AS_Path list as the optimal route.

After this command is configured, the AS_Path list for matched BGP routes will change. Assume that the original AS-Path is (30, 40, 50) and the BGP route matching condition is met. In this case:

- If the **apply as-path 60 70 80 additive** command is run, the AS-Path list is changed to (60, 70, 80, 30, 40, 50). This configuration change is generally used to make the BGP route not preferentially selected.
- If the **apply as-path 60 70 80 overwrite** command is run, the AS-Path list is changed to (60, 70, 80). There are many application scenarios for changing the AS-Path list, and the major application scenarios are as follows:
  - Hide the real path information of routes. For example, after the AS-Path list is changed to (60, 70, 80), the AS-Path information of the route (30, 40, 50) is lost.
  - Implement load balancing. For example, a router receives two routes with the same destination IP address 10.1.0.0/16. The AS_Path list of one route is (60, 70, 80) and that of the other route is (30, 40, 50). In this case, you

 Copyright © Huawei Technologies Co., Ltd.

can change the AS_Path list (30, 40, 50) to (60, 70, 80), and load balancing then may be implemented on the two routes.

  - Shorten the AS-Path list to prevent the route from being discarded. If the **as-path-limit** command is configured, whether the number of AS numbers in the AS-Path list of the incoming route exceeds the maximum value needs to be checked. If the number exceeds the maximum value, the route is discarded. Therefore, before receiving a route with a long AS-Path list, replace the AS-Path list with a shorter AS-Path list. For example, if the original AS-Path list is (60, 70, 80, 65001, 65002, 65003), run the **apply as-path 60 70 80 overwrite** command to change the AS-Path list to (60, 70, 80). In this manner, the length of the AS-Path is shortened, preventing the route from being discarded.
  - Shorten the AS-Path list to make the route preferentially selected and traffic directed to the local AS.

- If the **apply as-path none overwrite** command is run, the AS-Path list is changed to be vacant. In BGP route selection, if the AS-Path list is vacant, the length of the AS-Path list is considered as 0. Therefore, clearing the AS-Path list can not only hide the real path information, but also make the route preferentially selected and traffic directed to the local AS because the AS-Path list is shortened.

Prerequisites

The **apply as-path** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

Running the apply as-path command changes the path through which network traffic passes. Use this command only when you are familiar with the network topology and impact of the command on services.

Example

Change the AS number in the original AS_Path attribute to 200, 10.10.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply as-path 200 10.10 additive
```

9.9.2 apply backup-interface

Function

The **apply backup-interface** command sets the action for configuring a backup outbound interface in a routing policy.

The **undo apply backup-interface** command restores the default setting.

By default, the action for configuring the backup outbound interface is not set in a routing policy.

Format

apply backup-interface *interface-type interface-number*

undo apply backup-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the backup outbound interface.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply backup-interface** command is used in IP FRR scenarios to configure a backup outbound interface for a route. After IP FRR is enabled, data traffic can be quickly switched to the backup outbound interface if the primary link fails.

Prerequisites

The **route-policy** command must be used before the **apply backup-interface** command.

if-match clauses can be used to configure matching rules such as IP prefix lists, and ACLs before a backup outbound interface is configured.

Follow-up Procedure

Reference a configured route-policy in the **ip frr (system view)** command or the **ip frr (VPN instance view)** command to configure IP FRR on a public network or VPN.

The **apply backup-interface** command is usually used together with the **apply backup-nexthop** command.

NOTE

For P2P links, a backup next hop is not necessary. For non-P2P links, a backup next hop is necessary.

Example

Configure the backup outbound interface and the backup next hop in the route-policy named **ip_frr_rp**.

```
<Huawei> system-view
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] route-policy ip_frr_rp permit node 10
[Huawei-route-policy] apply backup-interface gigabitethernet1/0/0
[Huawei-route-policy] apply backup-nexthop 192.168.20.2
```

Delete the configured backup outbound interface from the route-policy named **ip_frr_rp**.

```
<Huawei> system-view
[Huawei] route-policy ip_frr_rp permit node 10
[Huawei-route-policy] undo apply backup-interface
```

Related Topics

9.9.3 apply backup-nexthop

9.10.30 ip frr (system view)

9.9.53 route-policy

9.9.3 apply backup-nexthop

Function

The **apply backup-nexthop** command sets the action for configuring a backup next hop in a routing policy.

The **undo apply backup-nexthop** command deletes the configured backup next hop.

By default, the action for configuring a backup next hop is not set in a routing policy.

Format

apply backup-nexthop { *ipv4-address* | **auto** }

undo apply backup-nexthop

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IP address of a backup next hop.	It is in dotted decimal notation.
auto	Automatically searches for the backup next hop.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply backup-nexthop** command is used to configure a backup next hop for a route in IP FRR and VPN FRR scenarios. After IP FRR is enabled, data traffic can be quickly switched to the backup next hop if the primary link fails.

Prerequisites

The **route-policy** command has been run before the **apply backup-nexthop** command.

if-match clauses can be used to set matching rules such as interfaces, IP prefix lists, and ACLs before a backup next hop is configured.

Follow-up Procedure

The configured route-policy can be used in the **ip frr (system view)** command or the **ip frr (VPN instance view)** command that is run to configure IP FRR for a public or private network. It can also be used in the **vpn frr** command that is run to enable VPN FRR.

In a VPN FRR scenario, you only need to run the **apply backup-nexthop** command to configure a backup next hop.

In an IP FRR scenario, you need to run both the **apply backup-nexthop** and **apply backup-interface** commands.

NOTE

On a P2P link, a backup next hop may not be set. On a non-P2P link, the **apply backup-nexthop** command must be run to configure a backup next hop.

Example

Configure the backup interface and the backup next hop 192.168.20.2 in the route-policy named **ip_frr_rp**.

```
<Huawei> system-view
[Huawei] route-policy ip_frr_rp permit node 10
[Huawei-route-policy] apply backup-interface gigabitethernet1/0/0
[Huawei-route-policy] apply backup-nexthop 192.168.20.2
```

Delete the configured backup next hop from the route-policy named **ip_frr_rp**.

```
<Huawei> system-view
[Huawei] route-policy ip_frr_rp permit node 10
[Huawei-route-policy] undo apply backup-nexthop
```

Related Topics

9.9.2 apply backup-interface
9.10.30 ip frr (system view)
9.9.53 route-policy

9.9.4 apply behavior

Function

The **apply behavior** command configures a QoS traffic behavior for routes.

The **undo apply behavior** command restores the default setting.

By default, no QoS traffic behavior is configured.

Format

apply behavior *behavior-name*

undo apply behavior

Parameters

Parameter	Description	Value
behavior-name	Specifies the name of a QoS traffic behavior.	The value is a string of 1 to 31 case-sensitive characters without spaces, and must start with a letter.

Views

Route-policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large and complex network is deployed, traffic flows of different types, such as voice, video, and data, need to be managed separately, with different bandwidth and delays assigned to these traffic flows. In this case, class-based QoS needs to be configured and complex traffic classification needs to be performed. The **apply behavior** command is used to associate filtered route with a specific traffic behavior.

Prerequisites

Before running the **apply behavior** *behavior-name* command, you need to create a traffic behavior.

Meanwhile, certain matching conditions need to be configured to classify routes, such as the AS-Path lost, community attribute list, address prefix list, and route cost.

Precautions

The **apply behavior** command is mutually exclusive with the **apply ip-precedence** command and the **apply qos-local-id** command, and only one of these

commands can be configured on a node of a routing policy. For example, if the **apply behavior** command is configured in the view created by the **route-policy test permit node 10** command, configuring the **apply qos-local-id** command replaces **apply behavior** command.

Example

Configure the behavior named **example** in the system view, and then apply this QoS traffic behavior in the route-policy view.

```
<Huawei> system-view
[Huawei] traffic behavior example
[Huawei-behavior-example] quit
[Huawei] route-policy test permit node 10
[Huawei-route-policy] apply behavior example
```

Related Topics

9.9.21 apply qos-local-id

9.9.13 apply ip-precedence

9.9.5 apply comm-filter delete

Function

The **apply comm-filter delete** command sets the action for deleting community attributes of a specified community filter in a routing policy.

The **undo apply comm-filter** command restores the default setting.

By default, the action for deleting community attributes of a specified community filter is not set in a routing policy.

Format

apply comm-filter { *basic-comm-filter-number* | *adv-comm-filter-number* | *comm-filter-name* } **delete**

undo apply comm-filter

Parameters

Parameter	Description	Value
basic-comm-filter-number	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
adv-comm-filter-number	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
comm-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all digits. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To delete the community attributes, you can run the **ip community-filter** command several times to configure community attributes one by one, and apply the routing policy containing the **apply comm-filter delete** command to delete these community attributes.

The community attribute is a private attribute of BGP. The **apply comm-filter delete** command takes effect only for BGP routes.

Prerequisites

The **apply comm-filter delete** command can be used only after the **route-policy** command is used.

Precautions

After routes meet the filtering conditions, the specified community attributes of these routes are deleted.

1. When the delete operation is configured on a specified community attribute list, only one community attribute can be configured for the specified community attribute list. To delete multiple community attributes, you need to configure multiple community attribute lists. For example, if community attribute list 1 is used to delete 100:100 200:200 from the community attribute 100:100 200:200 carried in a route, you need to perform the following configurations on community attribute list 1:

```
[Huawei] ip community-filter 1 permit 100:100
[Huawei] ip community-filter 1 permit 200:200
[Huawei] display ip community-filter
Community filter Number: 1
permit 100:100
permit 200:200
[Huawei] route-policy RP1 permit node 10
[Huawei-route-policy] apply comm-filter 1 delete
```

   If multiple community attributes are configured in the same community filter, the **apply comm-filter delete** command cannot delete these community

attributes. To delete the community attributes, you can run the **ip community-filter** command several times to configure community attributes one by one, and apply the routing policy containing the **apply comm-filter delete** command to delete these community attributes. For example, the following command cannot delete the community attribute 100:100 200:200 of the route:

```
[Huawei] ip community-filter 1 permit 100:100 200:200
[Huawei] display ip community-filter
Community filter Number: 1
permit 100:100 200:200
[Huawei] route-policy RP1 permit node 10
[Huawei-route-policy] apply comm-filter 1 delete
```

2. When the **apply community** and **apply comm-filter delete** commands are run on the same node in a routing policy, the system performs the delete operation before the set operation regardless of the sequence in which the two commands are run.

```
[Huawei] display route-policy
Route-policy : 123a
  permit : 10
Match clauses:
Apply clauses: a
apply community 999:9 additive
apply comm-filter 1 delete
```

The following command output shows that community attribute 111:1 of the corresponding BGP route is deleted and community attribute 999:9 is added.

```
[Huawei] display ip community-filter
Community filter Number: 1
permit 111:1
permit 999:9
```

Example

Delete the specified BGP route community attributes 1:200, 2:200, and 3:200 from the community filter.

```
<Huawei> system-view
[Huawei] ip community-filter 1 permit 1:200
[Huawei] ip community-filter 1 permit 2:200
[Huawei] ip community-filter 1 permit 3:200
[Huawei] route-policy test permit node 10
[Huawei-route-policy] apply comm-filter 1 delete
```

Related Topics

9.9.6 apply community

9.9.45 ip community-filter

9.9.6 apply community

Function

The **apply community** command sets the action for changing the community attribute of BGP routes in a routing policy.

The **undo apply community** command restores the default setting.

By default, the action for changing the community attribute of BGP routes is not set in a routing policy.

Format

apply community none

apply community { *community-number* | *aa:nn* | **internet** | **no-advertise** | **no-export** | **no-export-subconfed** } &<1-32> [**additive**]

undo apply community

Parameters

Parameter	Description	Value
none	Indicates that all the community attributes of routes are deleted.	-
community-number | *aa:nn*	Specifies the community number. A maximum of 32 community numbers can be configured in the **apply community** command. ● If you do not configure any one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 32 *community-number* and *aa:nn* together. ● If you configure one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 31 *community-number* and *aa:nn* together. ● If you configure two of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 30*community-number* and *aa:nn* together. ● If you configure three of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 29 *community-number* and *aa:nn* together. ● If you configure all of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 28 *community-number* and *aa:nn* together.	The value of *community-number* is an integer ranging from 0 to 4294967295. The value of *aa* or *nn* ranges from 0 to 65535.
internet	Indicates that matching routes are sent to any peer. By default, all routes belong to the Internet community.	-
no-advertise	Indicates that matching routes are not sent to any peer. That is, after a router receives a route with this attribute, it does not advertise the route to other BGP peers.	-
no-export	Indicates that matching routes are sent to other sub-ASs but not to other ASs. That is, after a router receives a route with this attribute, it does not advertise the route outside the local AS.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-export-subconfed	Indicates that matching routes are neither sent to other sub-ASs nor to other ASs. That is, after a router receives a route with this attribute, it does not advertise the route to other sub-ASs.	-
additive	Indicates that community attributes are added to matching routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify the BGP routes, you can apply a routing policy containing the **apply community** command to configure the community attribute of matched BGP routes.

The community attribute is a private attribute of BGP. It simplifies the application of routing policies and facilitates route maintenance and management. A community is a set of destination addresses with the same characteristics. These addresses have no physical boundary and are independent of their ASs. They share one or multiple community attributes, which can be changed or set by running the **apply community** command.

Prerequisites

The **apply community** command can be used only after the **route-policy** command is used.

Precautions

If the **apply community** command is configured in a routing policy, the community attributes of the BGP routes that match the routing policy are changed according to the configurations in the routing policy.

Assume that the original community name of a BGP route is 30. If this BGP route matches a certain routing policy, the AS number is replaced or added on the basis of the routing policy. For example:

- If the **apply community 100** command is run, the community name is changed to 100.
- If the **apply community 100 150** command is run, the community name is changed to 100 or 150. That is, the BGP route belongs to two communities.
- If the **apply community 100 150 additive** command is run, the community name is changed to 30, 100 or 150. That is, the BGP route belongs to three communities.

 Copyright © Huawei Technologies Co., Ltd.

- If the **apply community none** command is run, the community attribute of the BGP route is deleted.

Example

Configure a routing policy named **setcommunity**, match the route with the AS_Path filter being 8, and change its community attribute to **no-export**.

```
<Huawei> system-view
[Huawei] route-policy setcommunity permit node 16
[Huawei-route-policy] if-match as-path-filter 8
[Huawei-route-policy] apply community no-export
```

Related Topics

9.9.5 apply comm-filter delete

9.9.45 ip community-filter

9.9.7 apply cost

Function

The **apply cost** command sets the action for changing the cost of routes in a routing policy.

The **undo apply cost** command restores the default setting.

By default, the action for changing the cost of routes is not set in a routing policy.

Format

apply cost [**+** | **-**] *cost*

undo apply cost

Parameters

Parameter	Description	Value
+	Increases the route cost.	If the MED of BGP routes or cost of non-BGP routes is greater than the maximum value (4294967295) after the adjustment, 4294967295 takes effect.
-	Reduces the route cost.	If the MED of BGP routes or cost of non-BGP routes is less than the minimum value (0) after the adjustment, 0 takes effect.
cost	Specifies the route cost. To control route selection, you can adjust the route cost to prevent routing loops.	The value is an integer ranging from 0 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the cost of routes for selecting the optimal route, you can apply a routing policy containing the **apply cost** command.

Prerequisites

The **apply cost** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects route selection.

The costs of imported routes are independent of the routing policy after the **undo apply cost** command is used to cancel the configuration of route costs.

Example

Define an **apply** clause to set the route cost to 120.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply cost 120
```

9.9.8 apply cost-type

Function

The **apply cost-type** command sets the action for changing the cost type of routes in a routing policy.

The **undo apply cost-type** command restores the default setting.

By default, the action for changing the cost type of routes is not set in a routing policy.

Format

apply cost-type { **external** | **internal** | **type-1** | **type-2** }

undo apply cost-type

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
external	Sets the cost type of IS-IS external routes.	-
internal	Sets the cost type of IS-IS internal routes or sets the MED value of BGP routes as the IGP cost of the next hop.	-
type-1	Sets Type 1 external routes of OSPF.	-
type-2	Sets Type 2 external routes of OSPF.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the cost type of routes for selecting the optimal route, you can apply a routing policy containing the **apply cost-type** command.

Prerequisites

The **apply cost-type** command can be used only after the **route-policy** command is used.

Precautions

The priority of the **apply cost-type** clause is higher than that of the **apply cost** clause, which affects route selection when a routing policy takes effect.

Precautions

Different operations are performed when the **apply cost-type internal** command is applied to IS-IS routes and BGP routes:

- When the **apply cost-type internal** command is applied to IS-IS routes:

  Routes are configured as IS-IS internal routes.
- When the **apply cost-type internal** command is applied to BGP routes:

  When a router advertises a route learned from an IBGP peer to an EBGP peer, if the **apply cost-type internal** command is run, the router sets the MED value of the route to be advertised to the EBGP peer as the IGP cost of the next hop of the route.

Example

Set the cost type to OSPF external Type-1.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
```

```
[Huawei-route-policy] apply cost-type type-1
```

9.9.9 apply dampening

Function

The **apply dampening** command sets the action for changing the dampening parameters of EBGP routes in a routing policy.

The **undo apply dampening** command restores the default setting.

By default, the action for changing the dampening parameters of EBGP routes is not set in a routing policy.

Format

apply dampening *half-life-reach reuse suppress ceiling*

undo apply dampening

Parameters

Parameter	Description	Value
half-life-reach	Specifies the half-life of a reachable route.	The value is an integer ranging from 1 to 45, in minutes.
reuse	Specifies the threshold for routes to be released from the dampening state. When the penalty value falls below the threshold, routes are reused.	The value is an integer ranging from 1 to 20000.
suppress	Specifies the threshold for routes to enter the dampening state. When the penalty value exceeds the threshold, routes are suppressed.	The value is an integer ranging from 1 to 20000. The configured value of *suppress* must be greater than the value of *reuse*.
ceiling	Specifies the upper limit of the penalty value of routes.	The value is an integer ranging from 1001 to 20000. The configured value of *ceiling* must be greater than the value of *suppress*.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply dampening** command, which is mostly used in BGP, is used to prevent frequent route dampening from affecting routers on the network.

You can configure different route dampening parameters for different nodes in the same routing policy. When route flapping occurs, BGP can use different route dampening parameters to suppress the routes that match the routing policy.

Procedure

If the **apply dampening** command is run multiple times, the latest configuration overwrites the previous one.

Configuration Impact

If the **apply dampening** command is run, each time route flapping occurs, BGP adds a certain penalty value to this route.

Precautions

The parameters in this command do not have default values and must be set. The values of *reuse*, *suppress*, and *ceiling* are listed in ascending order: *reuse* < *suppress* <*ceiling*. According to the formula, MaxSuppressTime = *half-life-reach* x 60 x (ln (*ceiling*/*reuse*)/ln (2)), routes are unsuppressed if the value of MaxSuppressTime is less than 1. Therefore, the value of the *ceiling*/*reuse* must be great enough so that the value of MaxSuppressTime can be equal to or greater than 1.

Example

Set dampening parameters for EBGP routes.

```
<Huawei> system-view
[Huawei] route-policy aa permit node 10
[Huawei-route-policy] apply dampening 20 2000 10000 16000
```

9.9.10 apply extcommunity

Function

The **apply extcommunity** command sets the action for changing the extended community attribute of BGP routes in a routing policy.

The **undo apply extcommunity** command restores the default setting.

By default, the action for changing the extended community attribute of BGP routes is not set in a routing policy.

Format

apply extcommunity { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address:nn* } } &<1-16> [**additive**]

undo apply extcommunity

Parameters

Parameter	Description	Value
rt	Indicates the route-target extended community. A maximum of 16 route targets can be configured.	-
as-number	Specifies the AS number.	The value is an integer ranging from 0 to 65535.
4as-number	Specifies a 4-byte AS number.	A 4-byte AS number is divided into the following types: ● It is an integer ranging from 65536 to 4294967295. ● It is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535, respectively
ipv4-address	Specifies the IPv4 address.	It is in dotted decimal notation.
nn	Specifies an integer.	● When the value of *as-number* is a 2-byte AS number, the value of *nn* ranges from 0 to 4294967295. ● When the value of *4as-number* is a 4-byte AS number, the value of *nn* ranges from 0 to 65535. ● For *ipv4-address*, the value of *nn* ranges from 0 to 65535.
additive	Indicates that existing community attributes can be added to routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When controlling inter-AS VPN route receiving and advertising, apply the routing policy that contains the **apply extcommunity** command to change the RT

extended community attribute of matched routes. Currently, only the RT extended community attribute is supported. This command cannot specify an extended community attribute for public routes.

Prerequisites

The **apply extcommunity** command can be used only after the **route-policy** command is used.

Precautions

When the routing policy that contains the action is used in the BGP view, BGP IPv4 unicast address view, or BGP IPv6 unicast address view, the action does not take effect.

When a routing policy takes effect, it affects inter-AS VPN route receiving and advertising.

If the keyword **additive** is not set in the **apply extcommunity** command, the original extended community attribute is replaced.

Example

Add 100:2, 10.1.1.1:22, 100.100:100 to the VPN route-target extended community attribute of BGP.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply extcommunity rt 100:2 rt 10.1.1.1:22 rt 100.100:100 additive
```

9.9.11 apply ip-address next-hop (Route-Policy view)

Function

The **apply ip-address next-hop** command sets the action for changing the next hop address of BGP routes in a routing policy.

The **undo apply ip-address next-hop** command restores the default setting.

By default, the action for changing the next hop address of BGP routes is not set in a routing policy.

Format

apply ip-address next-hop { *ipv4-address* | **peer-address** }

undo apply ip-address next-hop { *ipv4-address* | **peer-address** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the next hop address.	It is in dotted decimal notation.

Parameter	Description	Value
peer-address	Sets the next hop address to the local address when the **apply** clause is used by an export policy. Sets the next hop address to the peer address when the **apply** clause is used by an import policy.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the next hop address of BGP routes for selecting the optimal route, you can apply a routing policy containing the **apply ip-address next-hop** command.

The next hop address of a BGP route is set using the policy in the following situations:

- IBGP: Configure the import or export policy for the IBGP peer. If the next hop address configured in the routing policy is unreachable, the IBGP peer adds the corresponding route to the BGP routing table. However, this route is invalid.
- EBGP: Configure the import policy for the EBGP peer. If an export policy is configured, the route destined for the EBGP peer is discarded because the next hop address is unreachable.

Prerequisites

The **apply ip-address next-hop** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

When a routing policy is specified in the **import-route** and **network** commands, the **apply ip-address next-hop** clause in the routing policy does not take effect.

Example

Define an **apply** clause to set the next hop address as 192.168.1.8.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply ip-address next-hop 192.168.1.8
```

9.9.12 apply ipv6 next-hop

Function

The **apply ipv6 next-hop** command sets the action for changing an IPv6 next hop address of a BGP route in a route-policy.

The **undo apply ipv6 next-hop** command restores the default setting.

By default, the action for changing the IPv6 next hop addresses of BGP routes are not configured in a route-policy.

Format

apply ipv6 next-hop { **peer-address** | *ipv6-address* }

undo apply ipv6 next-hop { **peer-address** | *ipv6-address* }

Parameters

Parameter	Description	Value
ipv6-address	Specifies the IPv6 next hop address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
peer-address	Specifies the peer address as the next hop.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply ipv6 next-hop** command configures an IPv6 next hop address for a BGP route.

In BGP, the next hop address of a route can be set through the route-policy in the following situations:

- IBGP

  For an IBGP peer, the configured inbound and outbound policies can take effect. If the next hop address configured in the policy is unreachable, the IBGP peer still adds the route to the BGP routing table, but the route is not valid.
- EBGP

 Copyright © Huawei Technologies Co., Ltd.

For an EBGP peer, when the policy is used to modify the next hop address of a route, the inbound policy is configured. If the outbound policy is configured, the route is discarded because its next hop is unreachable.

Prerequisites

The **apply ipv6 next-hop** command can be used only after the **route-policy** command is used.

After a BGP route matches a route-policy, you can change the IPv6 next hop address of the BGP route.

When a route-policy is being applied in the **import-route** and **network** commands, the **apply ipv6 next-hop** clause in the route-policy does not take effect.

Example

Set FC00:0:0:6::1 as the next hop address.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply ipv6 next-hop fc00:0:0:6::1
```

9.9.13 apply ip-precedence

Function

The **apply ip-precedence** command sets the QoS parameter *ip-precedence* for routes.

The **undo apply ip-precedence** command restores the configuration.

By default, no IP preference is set.

Format

apply ip-precedence *ip-precedence*

undo apply ip-precedence

Parameters

Parameter	Description	Value
ip-precedence	IP precedence	The value can be a preference value or a keyword: • The value is an integer ranging from 0 to 7. • The preference keyword can be Routine, Priority, Immediate, Flash, Flash-override, Critical, Internet, or Network. **Table 9-192** shows the relationship between preference values and keywords.

Table 9-192 Relationship between preference values and keywords

Value	Keyword
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash-override
5	Critical
6	Internet
7	Network

Views

Route-policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving routes, a BGP route receiver matches the attributes of the BGP routes based on the import route-policy, sets the IP precedence, delivers the BGP routes together with the associated QoS parameters, and applies QoS traffic policies to the classified data. In this case, the BGP route receiver can apply QoS policies to the data sent to the destination network segment based on the IP precedence. This applies QoS policies in BGP.

Prerequisites

The **apply ip-precedence** command can be used only after the **route-policy** command is used.

Configuration Impact

If a route matches a route-policy, you can change the value of the Precedence field in the IP header. The Precedence field is the first three bits of the Type of Service (ToS) field in the IP header.

Precautions

If an integer is used to specify *ip-precedence*, the preference is saved as an integer in the configuration file. If a keyword is used to specify *ip-precedence*, the preference is saved as a keyword in the configuration file.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the IP precedence in the route-policy named **test**.

```
<Huawei> system-view
[Huawei] route-policy test permit node 10
[Huawei-route-policy] apply ip-precedence internet
```

9.9.14 apply isis

Function

The **apply isis** command sets the action for changing the level of routes imported to IS-IS in a routing policy.

The **undo apply isis** command restores the default setting.

By default, the action for changing the level of routes imported to IS-IS is not set in a routing policy.

Format

apply isis { **level-1** | **level-1-2** | **level-2** }

undo apply isis

Parameters

Parameter	Description	Value
level-1	Indicates IS-IS Level-1 routes.	-
level-1-2	Indicates IS-IS Level-1 and Level-2 routes.	-
level-2	Indicates IS-IS Level-2 routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of external routes can be imported to IS-IS, which causes extra burdens on IS-IS-enabled devices. To solve this problem, run the **apply isis** command to set the level of the routes to be imported to IS-IS.

Prerequisites

The **apply isis** command can be used only after the **route-policy** command is used.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When a routing policy takes effect, it affects route receiving and advertising in IS-IS.

Example

Set the level of the routes imported to IS-IS.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply isis level-1
```

9.9.15 apply local-preference

Function

The **apply local-preference** command sets the action for changing the local preference of BGP routes in a routing policy.

The **undo apply local-preference** command restores the default setting.

By default, the action for changing the local preference of BGP routes is not set in a routing policy.

Format

apply local-preference *preference*

undo apply local-preference

Parameters

Parameter	Description	Value
preference	Specifies the local preference of BGP routes.	The value is an integer ranging from 0 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Local-Pref attribute is a private attribute of BGP. The **apply local-preference** command sets only the local preference for BGP routes. The Local_Pref attribute is used to determine the optimal route when traffic leaves an AS. When a BGP router obtains multiple routes to the same destination address but with different

 Copyright © Huawei Technologies Co., Ltd.

next hops through IBGP peers, the route with the largest Local_Pref value is selected.

Prerequisites

The **apply local-preference** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

The Local_Pref attribute applies to the routing within an AS rather than be advertised to the outside of the AS. In this case, the **apply local-preference** command does not take effect when EBGP neighbor relationships are set up.

Example

Set the local preference of BGP routes to 130.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply local-preference 130
```

9.9.16 apply mpls-label

Function

The **apply mpls-label** command sets the action for allocating MPLS labels to public routes in a routing policy.

The **undo apply mpls-label** command restores the default setting.

By default, the action for allocating MPLS labels to public routes is not set in a routing policy.

Format

apply mpls-label

undo apply mpls-label

Parameters

None

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario where inter-AS VPN Option C or Carrier Support Carrier (CSC) is deployed, you can use the **apply mpls-label** command to allocate labels to public routes.

Prerequisites

The **apply mpls-label** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it allocates MPLS labels to public routes.

Example

Assign MPLS labels to the routes that match the routing policy.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply mpls-label
```

Related Topics

9.9.40 if-match mpls-label

9.9.17 apply origin

Function

The **apply origin** command sets the action for changing the Origin attribute of BGP routes in a routing policy.

The **undo apply origin** command restores the default setting.

By default, the action for changing the Origin attribute of BGP routes is not set in a routing policy.

Format

apply origin { **egp** { *as-number-plain* | *as-number-dot* } | **igp** | **incomplete** }

undo apply origin

Parameters

Parameter	Description	Value
egp *as-number-plain*	Sets the origin of BGP routes as EGP. The parameter *as-number-plain* specifies the Integral AS number of an external route. An AS number uniquely identifies an AS. *as-number-plain* is required when you need to change the origin of BGP routes as EGP. EGP has the secondary highest priority. The Origin attribute of the routes obtained through EGP is EGP.	The value is an integer ranging from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
egp *as-number-dot*	Sets the origin of BGP routes as EGP. The parameter *as-number-dot* specifies the AS number in dotted notation of an external route. An AS number uniquely identifies an AS. *as-number-dot* is required when you need to change the origin of BGP routes as EGP. EGP has the secondary highest priority. The Origin attribute of the routes obtained through EGP is EGP.	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.
igp	Sets the origin of BGP routes as IGP. IGP has the highest priority. The Origin attribute of the routes obtained through an IGP of the AS that originates the routes, such as the routes imported to the BGP routing table through the **network** command, is IGP.	-
incomplete	Sets the origin code of BGP routes as unknown. Incomplete has the lowest priority. The Origin attribute of the routes learned through other methods, such as the routes imported by BGP through the **import-route** command, is Incomplete.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the Origin attribute of routes for selecting the optimal route, you can apply a routing policy containing the **apply origin** command. The Origin attribute is a private attribute of BGP and defines the origin of a route.

Prerequisites

The **apply origin** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

Example

Set the origin of BGP routes to IGP.

```
<Huawei> system-view
```

```
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply origin igp
```

9.9.18 apply ospf

Function

The **apply ospf** command sets the action performed for configuring an OSPF area to which the route is imported in a routing policy.

The **undo apply ospf** command restores the default setting.

By default, the action performed for configuring an OSPF area to which the route is imported is not set in a routing policy.

Format

apply ospf { **backbone** | **stub-area** }

undo apply ospf

Parameters

Parameter	Description	Value
backbone	Imports routes to the OSPF backbone area.	-
stub-area	Imports routes to an OSPF NSSA.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **apply ospf** command can be used to specify the OSPF backbone area or NSSA area to which routes are imported. This can prevent OSPF from importing too many external routes, which brings heavy burden on OSPF devices.

Prerequisites

The **apply ospf** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, routes are imported to the specified OSPF area.

 Copyright © Huawei Technologies Co., Ltd.

Example

Import routes to the OSPF backbone area.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply ospf backbone
```

9.9.19 apply preference

Function

The **apply preference** command sets the action for changing the preference of routes in a routing policy.

The **undo apply preference** command restores the default setting.

By default, the action for changing the preference of routes is not set in a routing policy.

Format

apply preference *preference*

undo apply preference

Parameters

Parameter	Description	Value
preference	Specifies the route precedence. Route sharing and route selection are difficult because multiple routing protocols can run on the device at the same time; therefore, a default preference needs to be specified for each routing protocol. When different protocols discover multiple routes to the same destination, the route discovered by the protocol with a higher preference is selected to forward IP packets. The smaller the preference value, the higher the preference.	The value is an integer ranging from 1 to 255.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the preference of routes for selecting the optimal route, you can apply a routing policy containing the **apply preference** command.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The **apply preference** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects route selection.

Example

Set the preference for routes.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply preference 90
```

9.9.20 apply preferred-value

Function

The **apply preferred-value** command sets the action for changing the preferred value of BGP routes in a routing policy.

The **undo apply preferred-value** command restores the default setting.

By default, the action for changing the preferred value of BGP routes is not set in a routing policy.

Format

apply preferred-value *preferred-value*

undo apply preferred-value

Parameters

Parameter	Description	Value
preferred-value	Specifies the preferred value of BGP routes. In route selection, the BGP route with the largest preferred value is preferred.	The value is an integer ranging from 0 to 65535.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the preferred value of BGP routes for selecting the optimal route, you can apply a routing policy containing the **apply preferred-value** command.

Prerequisites

The **apply preferred-value** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effect, it affects BGP route selection.

The preferred value of a route indicates the weight of the route in BGP routing. The preferred value is not a standard RFC-defined attribute and is valid only on local devices. The preferred value is inapplicable to export policies of BGP.

Example

Set the preferred value for BGP routes.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply preferred-value 66
```

9.9.21 apply qos-local-id

Function

The **apply qos-local-id** command sets the QoS local ID.

The **undo apply qos-local-id** command cancels the configuration.

By default, no QoS local ID is set.

Format

apply qos-local-id *qos-local-id*

undo apply qos-local-id

Parameters

Parameter	Description	Value
qos-local-id	Specifies the QoS local ID.	The value is an integer ranging from 1 to 4095.

Views

Route-policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The QoS local ID is a local identifier of QoS. In actual applications, you can set the QoS local ID in the route-policy, and add the command that matches the QoS local ID in the QoS policy. The QoS local ID set in the route-policy is delivered to the FIB table. During packet forwarding, the system obtains the QoS local ID from the FIB table and applies the related QoS policy according to the QoS local ID.

Configuration Impact

The **apply qos-local-id** command is mutually exclusive with the **apply behavior** and **apply ip-precedence** commands, and only one of these commands can be configured on a node of a routing policy. For example, if the **apply qos-local-id** command is configured in the view created by the **route-policy test permit node 10** command, configuring the **apply ip-precedence** command replaces **apply qos-local-id** command.

Example

Set the QoS local ID in the route-policy named **test**.

```
<Huawei> system-view
[Huawei] route-policy test permit node 10
[Huawei-route-policy] apply qos-local-id 10
```

Related Topics

9.9.13 apply ip-precedence

9.9.4 apply behavior

9.9.22 apply tag

Function

The **apply tag** command sets the action for changing the tag of routes in a routing policy.

The **undo apply tag** command restores the default setting.

By default, the action for changing the tag of routes is not set in a routing policy.

Format

apply tag *tag*

undo apply tag

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tag	Specifies the tag of routes. Routes can be tagged as required. You can set the same tag for the same type of route. Routes can be flexibly controlled and managed through tags in the routing policy.	The value is an integer ranging from 0 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify the routes, you can apply a routing policy containing the **apply tag** command to add the same tag to the matched routes.

Prerequisites

The **apply tag** command can be used only after the **route-policy** command is used.

Precautions

When a routing policy takes effects, routes will be matched by routing policies related to the tag.

BGP routes do not support tags. The **apply tag** command sets the tag for only IGP routes.

Example

Set the tag of routes to 100.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] apply tag 100
```

9.9.23 description (Route-Policy view)

Function

The **description** command configures the description of a route-policy.

The **undo description** command deletes the description of a route-policy.

By default, no description is configured for the route-policy.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a route-policy.	The description is a string of 1 to 80 case-sensitive characters that can contain spaces.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command can be used to configure a description for a created route-policy. If many route-policies have been configured, configuring descriptions for the policies will facilitate policy management.

Prerequisites

A route-policy has been created by using **route-policy** command.

Example

Configure the description of the route-policy named **temp**.

```
<Huawei> system-view
[Huawei] route-policy temp permit node 10
[Huawei-route-policy] description This policy-name is temp
```

Related Topics

9.9.53 route-policy

9.9.24 display ip as-path-filter

Function

display ip as-path-filter command displays the configuration of the AS_Path filter.

Format

display ip as-path-filter [*as-path-filter-number* | *as-path-filter-name*]

Parameters

Parameter	Description	Value
as-path-filter-number	Displays the configuration of an AS_Path filter with a specified number.	It is an integer that ranges from 1 to 256.
as-path-filter-name	Displays the configuration of an AS_Path filter with a specified name.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The AS-Path attribute is a BGP-specific attribute. An AS-Path filter is used to filter BGP routes.

You can run the **display ip as-path-filter** command to:

- View detailed information about a configured AS path filter.
- Check whether an AS-Path filter is deleted successfully after running the **undo ip as-path-filter** command.

Precautions

The **display ip as-path-filter** command:

- Displays the configuration information about a specified AS-Path filter, if the number or name of the AS-Path filter is specified.
- Displays the configuration information about all AS-Path filters, if neither the number nor name of the AS-Path filter is specified.
- Does not display any information, if the AS-Path filter does not exist in the system or the AS-Path filter that is queried does not exist.

Example

Display the configured AS_Path filter.

```
<Huawei> display ip as-path-filter
As path filter number: 1
        permit    1.1 100,200
As path filter name: abc
        deny      2.2 200,400
```

Table 9-193 Description of the display ip as-path-filter command output

Item	Description
As path filter number	AS-Path filter number.
As path filter name	AS-Path filter name.
permit	Matching mode is permit.
1.1 100,200	Content of the regular expression.
deny	Matching mode is deny.

Related Topics

9.9.44 ip as-path-filter

9.9.25 display ip community-filter

Function

The **display ip community-filter** command displays the configuration of the community filter.

Format

display ip community-filter [*basic-comm-filter-num* | *adv-comm-filter-num* | *comm-filter-name*]

Parameters

Parameter	Description	Value
basic-comm-filter-num	Displays the configuration of a basic community filter with a specified number.	The value is an integer ranging from 1 to 99.
adv-comm-filter-num	Displays the configuration of an advanced community filter with a specified number.	The value is an integer ranging from 100 to 199.
comm-filter-name	Displays the configuration of a community filter with a specified name.	The name is a string of 1 to 51 characters. The string cannot be all numerals.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The community attribute is a BGP-specific attribute. A community filter is used to filter BGP routes.

You can run the **display ip community-filter** command to:

- View detailed information about a configured community filter.
- Check whether a community filter is successfully deleted after running the **undo ip community-filter** command.

Precautions

The **display ip community-filter** command:

- Displays the configuration information about a specified community filter, if the number or name of the community filter is specified.
- Displays the configuration information about all community filters, if neither the number nor name of the community filter is specified.
- Does not display any information, if the community filter does not exist in the system or the community filter that is queried does not exist.

Example

Display all community filters.

```
<Huawei> display ip community-filter
Community filter Number: 10
        deny  no-export
Community filter Number: 110
        permit 110:110
Named Community basic filter: aa (ListID = 200)
        permit  1 internet
Named Community advanced filter: bb (ListID = 700)
        permit ^20
```

Table 9-194 Description of the display ip community-filter command output

Item	Description
Community filter Number	Indicates the number of a community filter.
permit	Indicates that the matching mode is permit.
deny	Indicates that the matching mode is deny.
Named Community basic filter	Indicates the name of a basic community filter.
Named Community advanced filter	Indicates the name of an advanced community filter.

Related Topics

9.9.45 ip community-filter

9.9.26 display ip extcommunity-filter

Function

display ip extcommunity-filter command displays the configuration of the extended community filter.

Format

display ip extcommunity-filter [*basic-extcomm-filter-num* | *advanced-extcomm-filter-num* | *extcomm-filter-name*]

Parameters

Parameter	Description	Value
basic-extcomm-filter-num	Specifies the basic extended community filter number.	It is an integer that ranges from 1 to 199.
advanced-extcomm-filter-num	Specifies the advanced extended community filter number.	It is an integer that ranges from 200 to 399.
extcomm-filter-name	Displays the configuration of an extended community filter with a specified name.	The name is a string of 1 to 51 characters without any space. It is case-sensitive.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The extended community attribute is a BGP-specific attribute. An extended community filter is used to filter VPN routes.

You can run the **display ip extcommunity-filter** command to:

- View detailed information about a configured extended community filter.
- Check whether an extended community filter is successfully deleted after running the **undo ip excommunity-filter** command.

Precautions

The **display ip extcommunity-filter** command:

- Displays the configuration information about a specified extended community filter, if the number or name of the extended community filter is specified.
- Displays the configuration information about all extended community filters, if neither the number nor name of the extended community filter is specified.

 Copyright © Huawei Technologies Co., Ltd.

- Does not display any information, if the extended community filter does not exist in the system or the extended community filter that is queried does not exist.

Example

Display information about the extended community filter.

```
<Huawei> display ip extcommunity-filter
Extended Community filter Number 10
        permit rt : 100:10
Extended Community filter Number 280
        permit rt 100:65
Extended Community filter basic filter: bas-abc
        permit rt : 200:10
Extended Community filter advanced filter: adv-abc
        deny 1.1.1.1:10
```

Table 9-195 Description of the display ip extcommunity-filter command output

Item	Description
Extended Community filter Number	Indicates the number of an extended community filter.
Extended Community filter basic filter	Basic extended community filter name.
Extended Community filter advanced filter	Advanced extended community filter name.
permit	Indicates that the matching mode is permit.
deny	Indicates that the matching mode is deny.
rt	Indicates the extended community attribute of the specified RT.

Related Topics

9.9.46 ip extcommunity-filter

9.9.27 display ip ip-prefix

Function

The **display ip ip-prefix** command displays the configuration of IPv4 prefix lists.

Format

display ip ip-prefix [*ip-prefix-name*]

Parameters

Parameter	Description	Value
ip-prefix-name	Displays the configuration of an IP prefix list with a specified name.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An IPv4 prefix list is used to filter IPv4 addresses. To achieve the following purposes, run the **display ip ip-prefix** command:

- View detailed configuration of a configured IPv4 prefix list.
- Check whether an IPv4 prefix list is deleted after running the **undo ip ip-prefix** command.
- View the number of routes that do or do not match the route-policy in an IPv4 prefix list.

Precautions

The **display ip ip-prefix** command:

- Displays the configuration of a specified IPv4 prefix list if the name of the IPv4 prefix list is specified.
- Displays the configuration of all IPv4 prefix lists if no IPv4 prefix list name is specified.
- Does not display information if no IPv4 prefix list exists in the system or the queried IPv4 prefix list does not exist.

Before collecting the number of routes that do or do not match the route-policy in an IPv4 prefix list within a certain period, run the **reset ip ip-prefix** command to clear existing statistics.

NOTE

If **The specified filter list does not exist** is displayed in the command output, the specified IPv4 prefix list failed to be configured. To re-configure it, run the **ip ip-prefix** command in the system view.

Example

Display the configuration of the IP prefix list named **p1**.

```
<Huawei> display ip ip-prefix p1
Prefix-list pl
Permitted 0
  Description prefixok
Denied 0
        index: 10      permit  192.168.0.0/16          ge  17  le  18
```

Table 9-196 Description of the display ip ip-prefix command output

Item	Description
Prefix-list	Name of an IPv4 prefix list.
Permitted	Number of routes that match a route-policy.
Description	Description of an IPv4 prefix list. This field is displayed only after a description is configured using the **ip ip-prefix** *ip-prefix-name* **description** *text* command.
Denied	Number of routes that do not match the route-policy.
index	Index of the entry in the IPv4 prefix list.
permit	Contents of the entry in the IPv4 prefix list.
ge 17	The mask is greater than or equal to 17.
le 18	The mask is less than or equal to 18.

Related Topics

9.9.47 ip ip-prefix

9.9.28 display ip ipv6-prefix

Function

display ip ipv6-prefix displays the configuration of IPv6 prefix lists.

Format

display ip ipv6-prefix [*ipv6-prefix-name*]

Parameters

Parameter	Description	Value
ipv6-prefix-name	Displays the configuration of an IP prefix list with a specified name. If *ipv6-prefix-name* is not specified, the configuration of all the configured IPv6 prefix lists is displayed.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An IPv6 prefix list is used to filter IPv6 addresses. To achieve the following purposes, run the **display ip ipv6-prefix** command:

- View detailed configuration of a configured IPv6 prefix list.
- Check whether an IPv6 prefix list is deleted after running the **undo ip ipv6-prefix** command.
- View the number of routes that do or do not match the route-policy in an IPv6 prefix list.

Precautions

The **display ip ipv6-prefix** command:

- Displays the configuration of a specified IPv6 prefix list if the name of the IPv6 prefix list is specified.
- Displays the configuration of all IPv6 prefix lists if no IPv6 prefix list name is specified.
- Does not display information if no IPv6 prefix list exists in the system or the queried IPv6 prefix list does not exist.

Before collecting the number of routes that do or do not match the route-policy in an IPv6 prefix list within a certain period, run the **reset ip ipv6-prefix** command to clear existing statistics.

Example

Display the configuration of all the IPv6 prefix lists.

```
<Huawei> display ip ipv6-prefix
  Prefix-list6 abc
  Description prefixok
  Permitted 0
  Denied 0
  index:   10          permit  ::/0
  index:   20          permit  ::/1          ge  1   le  128
```

Table 9-197 Description of the display ip ipv6-prefix command output

Item	Description
Prefix-list6	Name of an IPv6 prefix list.
Description	Description of an IPv6 prefix list. This field is displayed only after a description is configured using the **ip ipv6-prefix** *ipv6-prefix-name* **description** *text* command.

Item	Description
Permitted	Number of routes that match a route-policy.
Denied	Number of routes that do not match a route-policy.
index	Index of the entry in the IPv6 prefix list.
permit	Contents of the entry in the IPv6 prefix list.
ge	Greater than or equal to.
le	Less than or equal to.

Related Topics

9.9.48 ip ipv6-prefix

9.9.29 display ip rd-filter

Function

The **display ip rd-filter** command displays the configuration of the route distinguisher (RD) filter.

Format

display ip rd-filter [*rd-filter-number*]

Parameters

Parameter	Description	Value
rd-filter-number	Displays the configuration of a RD filter with a specified number.	The value is an integer ranging from 1 to 255.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The RD attribute is carried in VPN routes. An RD filter is used to filter VPN routes.

You can run the **display ip rd-filter** command to:

- View detailed information about a configured RD filter.

 Copyright © Huawei Technologies Co., Ltd.

- Check whether an RD filter is successfully deleted after running the **undo ip rd-filter** command.

Precautions

The **display ip rd-filter** command:

- Displays the configuration information about a specified RD filter, if the number of RD filter is specified.
- Displays the configuration information about all RD filters, if the number of the RD filter is not specified.
- Does not display any information, if the RD filter does not exist in the system or the RD filter that is queried does not exist.

Example

Display the configured RD filter.

```
<Huawei> display ip rd-filter
Route Distinguisher Filter 1
        permit 10.1.1.1:1 10.2.2.2:* 100:1 200:*
Route Distinguisher Filter 2
        deny 1:1 2:2
        permit 1:* 2:*
```

Table 9-198 Description of the display ip rd-filter command output

Item	Description
Route Distinguisher Filter	Number of the RD filter
permit	Matching mode: permit
deny	Matching mode: deny

Related Topics

9.9.49 ip rd-filter

9.9.30 display route-policy

Function

The **display route-policy** command displays the configuration of the Route-Policy.

Format

display route-policy [*route-policy-name*]

Parameters

Parameter	Description	Value
route-policy-name	Displays the configuration of a routing policy with a specified name.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the routing policy named **policy1**.

```
<Huawei> display route-policy policy1
Route-policy : policy1
  permit : 10 (matched counts: 2)
    Match clauses :
        if-match acl 2000
    Apply clauses :
        apply cost 100
        apply tag 100
```

Table 9-199 Description of the display route-policy command output

Item	Description
Route-policy	Name of the routing policy
permit	Matching mode and node index of the routing policy
matched counts: 2	Number of nodes that routes are matched in a routing policy
Match clauses	Matching condition list
Apply clauses	Apply clause list

Related Topics

9.9.53 route-policy

9.9.31 if-match acl (Route-Policy view)

Function

The **if-match acl** command sets a matching rule that is based on the Access Control List (ACL).

The **undo if-match acl** command deletes the matching rule based on the specified ACL.

By default, no matching rule based on the ACL is configured.

Format

if-match acl { *acl-number* | *acl-name* }

undo if-match acl { *acl-number* | *acl-name* }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match acl** command to set a matching rule based on the ACL to match IPv4 prefixes.

Prerequisites

The **if-match acl** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes using the ACL. Routes that match the ACL will be checked by other **if-match** clauses of this node. Routes that do not match the ACL will be checked by the next node.

 Copyright © Huawei Technologies Co., Ltd.

An ACL name is a character string that starts with a letter. For example, **2a** is an invalid ACL name.

The **if-match acl** command and the **if-match ip-prefix** command are mutually exclusive. If you run the **if-match ip-prefix** command after running the **if-match acl** command, the configuration of the **if-match ip-prefix** command overrides the configuration of the **if-match acl** command.

For a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the source address range that is specified by the **source** parameter and with the time period that is specified by the **time-range** parameter.

Example

Set a matching rule that is based on ACL 2000.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match acl 2000
```

Related Topics

19.7.18 rule (basic ACL view)

19.7.19 rule (basic ACL6 view)

9.9.32 if-match as-path-filter

Function

The **if-match as-path-filter** command creates a matching rule based on the AS_Path filter.

The **undo if-match as-path-filter** command deletes a matching rule based on the specified AS_Path filter.

By default, no matching rule based on the AS_Path filter is configured.

Format

if-match as-path-filter { *as-path-filter-number* &<1-16> | *as-path-filter-name* }

undo if-match as-path-filter [*as-path-filter-number* &<1-16> | *as-path-filter-name*]

Parameters

Parameter	Description	Value
as-path-filter-number	Specifies the number of an AS_Path filter. A maximum of 16 AS_Path filters can be specified.	The value is an integer ranging from 1 to 256.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
as-path-filter-name	Specifies the name of the AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The value cannot contain only numerals. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AS_Path attribute is the private attribute of BGP. The **if-match as-path-filter** command is applicable to only BGP routes. The **ip as-path-filter** command must be used to define an AS_Path filter so that the matching rule based on this AS_Path filter can take effect. For example:

- If the **if-match as-path-filter 1** command is used but AS_Path filter 1 is not configured, all routes are permitted, that is, all routes match the matching rule.
- If the **if-match as-path-filter 1** command after the **ip as-path-filter 1 permit *20** command is used, the BGP routes with the AS_Path attribute being 20 are permitted.

Multiple **if-match as-path-filter** clauses can be specified. The relationship between **if-match as-path-filter** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

Before running the **if-match as-path-filter** command, run the **ip as-path-filter** command to configure an AS_Path filter.

Precautions

The routing policy matches routes using the AS-Path filter. Routes that match the AS-Path filter will be checked by other **if-match** clauses of this node. Routes that do not match the AS-Path filter will be checked by the next node.

A maximum of 16 AS_Path filters can be specified. The relationship between these AS_Path filters is OR. Specifically, if a route matches one of these AS_Path filters, it matches the matching rules of the command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure AS_Path filter 2 to permit AS200 and AS300. Create a routing policy named **test**, and define AS_Path filter 2 in an **if-match** clause for node 10 of the routing policy.

```
<Huawei> system-view
[Huawei] ip as-path-filter 2 permit _200_300
[Huawei] route-policy test permit node 10
[Huawei-route-policy] if-match as-path-filter 2
```

Related Topics

9.9.44 ip as-path-filter

9.9.33 if-match community-filter

Function

The **if-match community-filter** command creates a matching rule based on the community filter.

The **undo if-match community-filter** command deletes the matching rule based on the specified community filter.

By default, no matching rule based on the community filter is configured.

Format

if-match community-filter { *basic-comm-filter-num* [**whole-match**] | *adv-comm-filter-num* } &<1-16>

if-match community-filter *comm-filter-name* [**whole-match**]

undo if-match community-filter [*basic-comm-filter-num* | *adv-comm-filter-num*] &<1-16>

undo if-match community-filter *comm-filter-name*

Parameters

Parameter	Description	Value
basic-comm-filter-num	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
adv-comm-filter-num	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.
comm-filter-name	Specifies the name of a community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
whole-match	Indicates complete matching. That is, all the communities in the command must be matched. Complete matching is valid only for the basic community filter.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The community attribute is a private attribute of BGP. The **if-match community-filter** command is applicable to only BGP routes. The **ip community-filter** command must be used to define a community filter so that the matching rule based on this community filter can take effect. For example:

- If the **if-match community-filter 1** command is used but community filter 1 is not configured, all routes are permitted, that is, all routes can match the matching rule.
- If the **if-match community-filter 1** command is used after the **ip community-filter 1 permit 1:1** command is used, the BGP routes with the community attribute being 1:1 are permitted.

Multiple **if-match community-filter** clauses can be specified. The relationship between **if-match community-filter** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

Before using the **if-match community-filter** command, you must use the **ip community-filter** command to configure a community filter.

The **if-match community-filter** command can be used only after a route-policy is configured by using the **route-policy** command.

Precautions

The routing policy matches routes using the community filter. Routes that match the community filter will be checked by other **if-match** clauses of this node. Routes that do not match the community filter will be checked by the next node.

A maximum of 16 community filters can be configured in the **if-match community-filter** command.

The parameter **whole-match** is valid only for its front community filter number. If multiple community filters are specified in the **if-match community-filter**

command and packets are required to completely match each filter, you need to specify the parameter **whole-match** behind each community filter and it is valid to only the basic community filter.

The name of a community filter cannot be all numerals.

Example

Set a matching rule that is based on the community filter 1.

```
<Huawei> system-view
[Huawei] ip community-filter 1 permit 100:200
[Huawei] route-policy test permit node 10
[Huawei-route-policy] if-match community-filter 1
```

Set the complete matching rule for community attribute filters 1 and 2.

```
<Huawei> system-view
[Huawei] route-policy test permit node 11
[Huawei-route-policy] if-match community-filter 1 whole-match 2 whole-match
```

Set a matching rule that is based on the community filter named **aa**.

```
<Huawei> system-view
[Huawei] route-policy test permit node 12
[Huawei-route-policy] if-match community-filter aa
```

Related Topics

9.9.45 ip community-filter

9.9.34 if-match cost

Function

The **if-match cost** command creates a matching rule based on the route cost.

The **undo if-match cost** command deletes the matching rule based on the specified route cost.

By default, no matching rule based on the route cost is configured.

Format

if-match cost *cost*

undo if-match cost

if-match cost { **greater-equal** *greater-equal-value* [**less-equal** *less-equal-value*] | **less-equal** *less-equal-value* }

Parameters

Parameter	Description	Value
cost	Specifies the route cost. Route costs can be changed to prevent routing loops.	The value is an integer ranging from 0 to 4294967295.

Parameter	Description	Value
greater-equal *greater-equal-value*	Specifies the minimum value of route cost.	The value is an integer ranging from 0 to 4294967294.
less-equal *less-equal-value*	Specifies the maximum value of route cost. *less-equal-value* is demanded to be greater than *greater-equal-value*.	The value is an integer ranging from 1 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **if-match cost** command to configure a node to filter routes based on the route costs. After such a matching rule is configured, you can apply the **apply** clauses to change the attributes of the routes that match the matching rule.

Prerequisites

The **if-match cost** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on the route cost. Routes that match the route cost will be checked by other **if-match** clauses of this node. Routes that do not match the route cost will be checked by the next node.

Example

Match the route with the cost 8.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match cost 8
```

9.9.35 if-match extcommunity-filter

Function

The **if-match extcommunity-filter** command sets a matching rule that is based on the extended community filter.

The **undo if-match extcommunity-filter** command deletes the matching rule based on the specified extended community filter.

 Copyright © Huawei Technologies Co., Ltd.

By default, no matching rule based on the extended community filter is configured.

Format

if-match extcommunity-filter { { *basic-extcomm-filter-num* | *adv-extcomm-filter-num* } &<1-16> | *extcomm-filter-name* }

undo if-match extcommunity-filter [[*basic-extcomm-filter-num* | *adv-extcomm-filter-num*] &<1-16> | *extcomm-filter-name*]

Parameters

Parameter	Description	Value
basic-extcomm-filter-num	Specifies the number of a basic extended community filter.	It is an integer ranging from 1 to 199.
adv-extcomm-filter-num	Specifies the number of an advanced extended community filter.	It is an integer ranging from 200 to 399.
extcomm-filter-name	Specifies the name of an extended community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The extended community attributes help flexibly control the routing policy. You can use the **if-match extcommunity-filter** command to configure a node to filter routes based on the extended community filter.

The **if-match extcommunity-filter** command is applicable to only BGP routes and must work in conjunction with the **ip extcommunity-filter** command. For example:

- If the **if-match extcommunity-filter 1** command is used but the extended community filter 1 is not configured, all routes are permitted, that is, all routes can match the matching rule.
- If the **if-match extcommunity-filter 1** command is used after the **ip extcommunity-filter 1 permit rt 1:1** command is used, the BGP routes with the extended community attribute being 1:1 are permitted.

 Copyright © Huawei Technologies Co., Ltd.

Multiple **if-match extcommunity-filter** clauses can be specified. The relationship between **if-match extcommunity-filter** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

Before using the **if-match extcommunity-filter** command, you must use the **ip extcommunity-filter** command to configure an extended community filter.

Precautions

The routing policy matches routes using the extended community filter. Routes that match the extended community filter will be checked by other **if-match** clauses of this node. Routes that do not match the extended community filter will be checked by the next node.

A maximum of 16 extended community filters can be configured in the **if-match extcommunity-filter** command. The relationship between these AS_Path filters is OR. Specifically, if a route matches one of these AS_Path filters, it matches the matching rules of the command.

Example

Define a rule to match the routes of the specified extended community filter.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match extcommunity-filter 100
```

Related Topics

9.9.46 ip extcommunity-filter

9.9.36 if-match interface

Function

The **if-match interface** command creates a matching rule based on the outbound interface.

The **undo if-match interface** command deletes the matching rule based on the specified outbound interface.

By default, no matching rule based on the outbound interface is configured.

Format

if-match interface { *interface-type interface-number* } &<1-16>

undo if-match interface [*interface-type interface-number*] &<1-16>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the outbound interface. A maximum of 16 outbound interfaces can be specified in the **if-match interface** command.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **if-match interface** command is used to filter routes based on the outbound interfaces.

A maximum of 16 outbound interfaces can be configured in this command.

If a node contains multiple **if-match interface** clauses, the relationship between the **if-match interface** clauses is OR. If a node contains both **if-match interface** clauses and other **if-match** clauses with different matching rules, the relationship between the **if-match interface** clauses and other **if-match** clauses is AND. For example, if a node contains **if-match interface 10ge1/0/1**, **if-match interface 10ge1/0/2**, and **if-match acl 2000** clauses, **if-match interface 10ge1/0/1** and **if-match interface 10ge1/0/2** are ORed, whereas **if-match interface 10ge1/0/1** and **if-match acl 2000** are ANDed.

Prerequisites

The **if-match interface** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on outbound interface information. Routes that match the outbound interface information will be checked by other **if-match** clauses of this node. Routes that do not match the outbound interface information will be checked by the next node.

Example

Define a rule to match the routes with the outbound interface GE1/0/0.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match interface gigabitethernet 1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

9.9.37 if-match ip

Function

The **if-match ip** command creates a matching rule based on IP information.

The **undo if-match ip** command deletes the matching rule based on specified IP information.

By default, no matching rule based on IP information is configured.

Format

if-match ip { **next-hop** | **route-source** | **group-address** } { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* }

undo if-match ip { **next-hop** | **route-source** | **group-address** } [**acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name*]

Parameters

Parameter	Description	Value
next-hop	Specifies the next hop address.	-
route-source	Specifies the source address of routes.	-
group-address	Indicates the IP address of the multicast group.	The value is in dotted decimal notation.
acl	Indicates route filtering using the ACL.	-
acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl-name	Specifies the name of a basic ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list that is used to filter routes.	The value is a string of case-sensitive characters without space and ranges from 1 to 169.

Views

Route-Policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

An ACL or IP prefix must be configured before running the **if-match ip** command so that the matching rule can take effect. For example:

- If the **if-match ip next-hop ip-prefix aa** command is used but the IP prefix **aa** is not configured, all routes are permitted, that is, all routes match the matching rule. This rule also applies to ACL.
- If the **if-match ip next-hop ip-prefix aa** and **ip ip-prefix aa permit 10.1.1.1 32** commands are used, the routes with the next hop being 10.1.1.1 is permitted. This rule also applies to ACL.

Prerequisites

The **if-match ip** command can be used only after the **route-policy** command is used.

Before running the **if-match ip** command, configure an **ACL** or an **IP prefix**.

Precautions

The routing policy matches routes based on the next hop address or source address. Routes that match the next hop address or source address will be checked by other **if-match** clauses of this node. Routes that do not match the next hop address or source address will be checked by the next node.

If the next hop address or source address of a route is 0.0.0.0, the system considers the mask length of the route as 0 to match the filtering rules by default.

If the next hop address or source address of a route to be filtered is not 0.0.0.0, by default, the system considers the mask length as 32 and matches the route.

When you run the **rule** command to configure a filtering rule in a named ACL, only the **source** and **time-range** parameters are valid for the filtering rule.

Example

Set an IP prefix list named **p1** to filter routes.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match ip next-hop ip-prefix p1
```

Set a rule that source addresses of routes match ACL 2000 to filter routes.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match ip route-source acl 2000
```

Related Topics

9.9.47 ip ip-prefix
19.7.18 rule (basic ACL view)
19.7.19 rule (basic ACL6 view)

9.9.38 if-match ip-prefix

Function

The **if-match ip-prefix** command creates a matching rule based on the IP prefix list.

The **undo if-match ip-prefix** command deletes the matching rule based on the specified IP prefix list.

By default, no matching rule based on the IP prefix list is configured in the routing policy.

Format

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix *ip-prefix-name*

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IP address prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The routing policy matches routes using the IP prefix list. Routes are either permitted or denied.

The **ip ip-prefix** command must be used so that the matching rule can take effect. For example:

- If the **if-match ip-prefix aa** command is used but the IP prefix **aa** is not configured, all routes are permitted, that is, all routes match the matching rule.
- If the **if-match ip-prefix aa** and **ip ip-prefix aa permit 10.1.1.1 32** commands are used, the routes with the IP prefix being 10.1.1.1 and mask being 32 are permitted.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **if-match ip-prefix** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on IP prefix information. Routes that match the IP prefix information will be checked by other **if-match** clauses of this node. Routes that do not match the IP prefix information will be checked by the next node.

The **if-match acl** and **if-match ip-prefix** commands cannot be used together in the same node of a routing policy, because the latest configuration will override the previous one.

Example

Set an IP prefix list named **p1** to filter routes.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match ip-prefix p1
```

Related Topics

9.9.47 ip ip-prefix

9.9.31 if-match acl (Route-Policy view)

9.9.39 if-match ipv6

Function

The **if-match ipv6** command sets a matching rule that is based on IPv6 information.

The **undo if-match ipv6** command deletes the matching rule based on specified IPv6 information.

By default, no matching rule based on IPv6 information is set.

Format

if-match ipv6 { **address** | **next-hop** | **route-source** } **prefix-list** *ipv6-prefix-name*

undo if-match ipv6 { **address** | **next-hop** | **route-source** } **prefix-list** *ipv6-prefix-name*

Parameters

Parameter	Description	Value
address	Matches the destination address of IPv6 routes.	-
next-hop	Matches the next hop of IPv6 routes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-source	Matches the source address of the advertised IPv6 routes.	-
prefix-list	Specifies the IP prefix list.	-
ipv6-prefix-name	Specifies the name of the IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip ipv6-prefix** command must be used to configure an IPv6 prefix so that the matching rule (based on the destination addresses, next hop addresses, or source addresses of IPv6 routes) configured through the **ip ipv6-prefix** command can take effect. Otherwise, all routes are permitted.

Prerequisites

The **if-match ipv6** command can be used only after the **route-policy** command is used.

Before using the **if-match ipv6** command, you must use the **ip ipv6-prefix** command to configure an IPv6 prefix.

Configuration Impact

When you filter routes based on the destination addresses, next hop addresses, or source addresses of IPv6 routes, the routes that match the matching rule are permitted and the route that do not match the matching rule are denied.

If the next hop address or source address of a route to be filtered is 0::0, by default, the system matches the route considering that its mask length is 0.

If the next hop address or source address of a route to be filtered is not 0::0, by default, the system matches the route and considers its mask length as 128.

Creating an IPv6 prefix list before it is referenced is recommended. If a nonexistent IPv6 prefix list is referenced using the command, all routes match the IPv6 prefix list.

 Copyright © Huawei Technologies Co., Ltd.

Example

Define an if-match clause to match the related IPv6 routing information.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match ipv6 address prefix-list p1
[Huawei-route-policy] if-match ipv6 next-hop prefix-list p1
[Huawei-route-policy] if-match ipv6 route-source prefix-list p1
```

Related Topics

9.9.53 route-policy

9.9.48 ip ipv6-prefix

9.9.40 if-match mpls-label

Function

The **if-match mpls-label** command creates a matching rule based on the MPLS label.

The **undo if-match mpls-label** command deletes the matching rule based on the specified MPLS label.

By default, no matching rule based on the MPLS label is configured.

Format

if-match mpls-label

undo if-match mpls-label

Parameters

None

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario where inter-AS VPN Option C or Carrier Support Carrier (CSC) is deployed, you can use the **if-match mpls-label** command to allocate labels to public routes.

Prerequisites

The **if-match mpls-label** command can be used only after the **route-policy** command is used.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The routing policy matches routes based on the MPLS label. Routes that match the MPLS label will be checked by other **if-match** clauses of this node. Routes that do not match the MPLS label will be checked by the next node.

Example

Assign MPLS labels to the routes that match the routing policy.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match mpls-label
```

Related Topics

9.9.16 apply mpls-label

9.9.41 if-match rd-filter

Function

The **if-match rd-filter** command creates a matching rule based on the RD filter.

The **undo if-match rd-filter** command deletes the matching rule based on the specified RD filter.

By default, no matching rule based on the RD filter is configured.

Format

if-match rd-filter *rd-filter-number*

undo if-match rd-filter

Parameters

Parameter	Description	Value
rd-filter-number	Specifies the number of an RD filter.	The value is an integer ranging from 1 to 255.

Views

Route-Policy view or tunnel-selector view.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **if-match rd-filter** command and the **ip rd-filter** command work together to filter routes based on RD attributes. For example:

- If **if-match rd-filter 1** is configured, but **rd-filter 1** is not configured, then all current routes will be permitted.
- If **if-match rd-filter 1** is configured, and **ip rd-filter 1 permit 1:1** has been configured, then routes with RD 1:1 will be permitted.

Prerequisites

The **if-match rd-filter** command must be run after the **route-policy** command is run.

Precautions

The routing policy matches routes using the RD filter. Routes that match the RD filter will be checked by other **if-match** clauses of this node. Routes that do not match the RD filter will be checked by the next node.

Example

Define a matching rule to match an RD filter.

```
<Huawei> system-view
[Huawei] route-policy abc permit node 10
[Huawei-route-policy] if-match rd-filter 1
```

Related Topics

9.9.49 ip rd-filter

9.9.29 display ip rd-filter

9.9.42 if-match route-type

Function

The **if-match route-type** command sets a matching rule that is based on the route type.

The **undo if-match route-type** command deletes the matching rule based on the specified route type.

By default, no matching rule based on the route type is configured.

Format

if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** }

undo if-match route-type { **external-type1** | **external-type1or2** | **external-type2** | **internal** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type1or2** | **nssa-external-type2** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
external-type1	Indicates OSPF external Type 1 routes.	-
external-type1or2	Indicates OSPF external routes.	-
external-type2	Indicates OSPF external Type 2 routes.	-
internal	Indicates internal routes, including OSPF inter-area routes and intra-area routes.	-
is-is-level-1	Indicates IS-IS Level-1 routes.	-
is-is-level-2	Indicates IS-IS Level-2 routes.	-
nssa-external-type1	Indicates NSSA external Type 1 routes.	-
nssa-external-type1or2	Indicates NSSA external routes.	-
nssa-external-type2	Indicates NSSA external Type 2 routes.	-

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match route-type** command to filter OSPF or IS-IS routes based on the route type.

Multiple **if-match route-type** clauses can be specified. The relationship between **if-match route-type** clauses is "OR". The relationship between **if-match** clauses is "AND".

Prerequisites

The **if-match route-type** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on the route type. Routes that match the route type will be checked by other **if-match** clauses of this node. Routes that do not match the route type will be checked by the next node.

For the same node in a routing policy, if two **if-match route-type** clauses are the same, the latter **if-match route-type** will not override the previous **if-match route-type**. After the latter clause is configured, both clauses take effect simultaneously. The relationship between **if-match route-type** clauses is "OR". That is, the actions defined by **apply** clauses can be performed on a route as long as the route meets one of the matching rules. For example, if both the **if-match**

route-type is-is-level-1 and **if-match route-type external-type1or2** commands are configured on the same node of a route policy, both IS-IS Level-1 routes and OSPF external routes can match the route policy.

NOTE

external-type1or2 refers to **external-type1** or **external-type2**. For the same node in a route policy, configuring both the **if-match route-type external-type1** and **if-match route-type external-type2** is equivalent to configuring the **if-match route-type external-type1or2** command. The two operations generate the same configuration file.

Similarly, **nssa-external-type1or2** refers to **nssa-external-type1** or **nssa-external-type2**. For the same node in a route policy, configuring both the **if-match route-type nssa-external-type1** and **if-match route-type nssa-external-type2** commands is equivalent to configuring the **if-match route-type nssa-external-type1or2** command. The two operations generate the same configuration file.

Example

Define a rule to match the routes of the specified type.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match route-type nssa-external-type1
```

9.9.43 if-match tag

Function

The **if-match tag** command sets a matching rule that is based on the route tag.

The **undo if-match tag** command deletes the matching rule based on the specified route tag.

By default, no matching rule based on the route tag is configured.

Format

if-match tag *tag*

undo if-match tag

Parameters

Parameter	Description	Value
tag	Indicates the tag value. Route tags classify routes as required. The same type of routes has the same tags. Routes are managed and controlled based on the tag by using the routing policy.	The value is an integer ranging from 0 to 4294967295.

Views

Route-Policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match tag** command to filter routes based on the tags.

Prerequisites

The **if-match tag** command can be used only after the **route-policy** command is used.

Precautions

The routing policy matches routes based on the route tag. Routes that match the route tag will be checked by other **if-match** clauses of this node. Routes that do not match the route tag will be checked by the next node.

Example

Define a rule to match the OSPF routes with the tag value 8.

```
<Huawei> system-view
[Huawei] route-policy policy permit node 10
[Huawei-route-policy] if-match tag 8
```

9.9.44 ip as-path-filter

Function

The **ip as-path-filter** command creates an AS_Path filter.

The **undo ip as-path-filter** command deletes a specified AS_Path filter.

By default, no AS_Path filter is configured.

Format

ip as-path-filter { *as-path-filter-number* | *as-path-filter-name* } { **deny** | **permit** } *regular-expression*

undo ip as-path-filter { *as-path-filter-number* | *as-path-filter-name* } [{ **deny** | **permit** } *regular-expression*]

Parameters

Parameter	Description	Value
as-path-filter-number	Specifies the number of an AS_Path filter.	The value is an integer ranging from 1 to 256.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
as-path-filter-name	Specifies the name of an AS_Path filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The string cannot be all numerals. When double quotation marks are used around the string, spaces are allowed in the string.
deny	Sets the matching mode of the AS_Path filter to deny.	-
permit	Sets the matching mode of the AS_Path filter to permit.	-
regular-expression	Specifies the AS_Path regular expression. For details about a regular expression, see **Filtering Command Outputs** in the *Huawei AR Seriesrouter - Configuration Guide - Basic Configuration*.	The value is a string of 1 to 255 characters, with spaces supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AS_Path filter uses the regular expression to define matching rules. After an AS_Path filter is set, the RM module immediately instructs each protocol to apply the filter by default.

The AS_Path attribute is a private attribute of BGP, and is used to filter BGP routes.

- The filter can be directly applied by using a command such as **peer as-path-filter**.
- The filter can be used as a matching condition of a routing policy by using a command such as **if-match as-path-filter zz**.

Configuration Impact

Multiple rules, permit or deny, can be specified in an AS_Path filter. The relationship between theses rules is "OR". This means that if a route meets one of the matching rules, the route matches the AS_Path filter.

By default, AS_Path filters work in **deny** mode. If all matching rules in a filter are configured to work in **deny** mode, all routes are denied by the filter; to prevent

 Copyright © Huawei Technologies Co., Ltd.

this problem, configure one matching rule in **permit** mode after one or multiple matching rules in **deny** mode so that the routes except for those denied by preceding matching rules are permitted by the filter.

Follow-up Procedure

To view detailed configurations of the AS_Path filter, run the **display ip as-path-filter** command.

Example

Create the AS_Path filter with the sequence number being 1, and permit routes that begin with 10 in the AS_Path to pass.

```
<Huawei> system-view
[Huawei] ip as-path-filter 1 permit ^10_
```

Create the AS_Path filter 2, and permit routes that contain 20 in the AS_Path to pass through.

```
<Huawei> system-view
[Huawei] ip as-path-filter 2 permit _20_
```

Create the AS_Path filter 3, and prohibit routes that contain 30 or 40 in the AS_Path from passing through.

```
<Huawei> system-view
[Huawei] ip as-path-filter 3 deny _30_
[Huawei] ip as-path-filter 3 deny _40_
[Huawei] ip as-path-filter 3 permit .*
```

Related Topics

9.9.24 display ip as-path-filter

9.9.45 ip community-filter

Function

The **ip community-filter** command creates a community filter.

The **undo ip community-filter** command deletes a community filter.

By default, no community filter is configured.

Format

ip community-filter { **basic** *comm-filter-name* | *basic-comm-filter-num* } { **permit** | **deny** } [*community-number* | *aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**] &<1-20>

ip community-filter { **advanced** *comm-filter-name* | *adv-comm-filter-num* } { **permit** | **deny** } *regular-expression*

undo ip community-filter { **basic** *comm-filter-name* | *basic-comm-filter-num* } [**permit** | **deny**] [*community-number* | *aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**] &<1-20>

undo ip community-filter { **advanced** *comm-filter-name* | *adv-comm-filter-num* } [[**permit** | **deny**] *regular-expression*]

Parameters

Parameter	Description	Value
basic *comm-filter-name*	Specifies the name of a basic community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
basic-comm-filter-num	Specifies the number of a basic community filter.	The value is an integer ranging from 1 to 99.
deny	Sets the matching mode of the community filter to deny.	-
permit	Sets the matching mode of the community filter to permit.	-
community-number	Specifies the community number.	The value is an integer ranging from 0 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
aa:nn	Specifies the community number. You can configure a maximum of 20 community numbers once. ● If you do not configure any one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 20 *community-number* and *aa:nn* together. ● If you configure one of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 19 *community-number* and *aa:nn* together. ● If you configure two of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 18 *community-number* and *aa:nn* together. ● If you configure three of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 17 *community-number* and *aa:nn* together. ● If you configure all of **internet**, **no-export-subconfed**, **no-advertise**, and **no-export**, you can specify 16 *community-number* and *aa:nn* together.	*aa* and *nn* are integers ranging from 0 to 65535.
internet	Indicates that the matching routes can be sent to any peer.	-
no-export-subconfed	Indicates that routes are not advertised outside an AS. If an AS confederation is used, routes are not advertised to any other sub-ASs in the AS confederation.	-
no-advertise	Indicates that routes are not advertised to other peers.	-
no-export	Indicates that routes are not advertised outside an AS. If an AS confederation is used, routes are not advertised outside the AS confederation, but to other sub-ASs.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
advanced *comm-filter-name*	Specifies the name of an advanced community filter.	The value is a string of 1 to 51 case-sensitive characters. The string cannot be all digits. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
adv-comm-filter-num	Specifies the number of an advanced community filter.	The value is an integer ranging from 100 to 199.
regular-expression	Specifies the regular expression used to match the community information. For details about the regular expression, see "CLI Overview" in the *Huawei AR Seriesrouter Configuration Guide - Basic Configuration*.	The value is a string of 1 to 255 case-sensitive characters, with spaces supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The community attribute is a private attribute of BGP, and can be used only to filter BGP routes. The community attribute can be used as a matching rule of a routing policy by using the **ip community-filter** and **if-match community-filter** commands together.

Precautions

Only the community number or known community attribute can be specified for a basic community filter. The regular expression can be used as a matching rule in an advanced community filter.

- The **ip community-filter basic** *comm-filter-name* command or the **ip community-filter** *basic-comm-filter-num* command can be used to configure a basic community filter. **basic** *comm-filter-name* specifies the name of a basic community filter, and the name cannot be all digits. A maximum of 20 community numbers can be configured in one command. *basic-comm-filter-num* specifies only the basic community filter with the number ranging from 1 to 99. A maximum of 20 community numbers can be configured in one command.
- The **ip community-filter advanced** *comm-filter-name* command or the **ip community-filter** *adv-comm-filter-num* command can be used to configure

an advanced community filter. **advanced** *comm-filter-name* specifies the name of an advanced community filter, and the name cannot be all digits. *adv-comm-filter-num* specifies only the advanced community filter with the number ranging from 100 to 199.

The relationship between the rules of the community filter is "AND". This is different from the RD filter. This is because each route has only one RD but can have multiple communities.

For example, the community filters in the following formats have different matching results:

Format 1:

```
ip community-filter 1 permit 100:1 200:1 300:1
```

Format 2:

```
ip community-filter 1 permit 100:1
ip community-filter 1 permit 200:1 300:1
```

In the preceding configuration of the community filter, the community defined in each rule must be a sub-set of route communities so that the rule can be matched.

The **apply comm-filter delete** command run in the Route-Policy view deletes the specified community attribute from routes. An **ip community-filter** command can be used to specify community attributes but one such command specifies only one community attribute each time. To delete more than one community attribute, run the **ip community-filter** command multiple times. If multiple community attributes are specified in one filter, none of them can be deleted. For information about examples, see **apply comm-filter delete**.

A community filter must have been configured using the **ip community-filter** command before the filter is referenced by another command using *comm-filter-num* or *comm-filter-name*.

A community filter cannot be deleted using the **undo ip community-filter** command when it is being referenced using *comm-filter-num* or *comm-filter-name*. To delete the community filter, cancel the reference configuration first.

By default, Community filters work in **deny** mode. If all matching rules in a filter are configured to work in **deny** mode, all routes are denied by the filter; to prevent this problem, configure one matching rule in **permit** mode after one or multiple matching rules in **deny** mode so that the routes except for those denied by preceding matching rules are permitted by the filter.

Follow-up Procedure

Run the **display ip community-filter** command to view detailed configuration for the community filter.

Example

Configure a basic community filter of which the sequence number is 1.

```
<Huawei> system-view
[Huawei] ip community-filter 1 deny internet
```

Configure an advanced community filter of which the sequence number is 100.

```
<Huawei> system-view
```

```
[Huawei] ip community-filter 100 permit ^10
```

Related Topics

9.9.25 display ip community-filter

9.9.46 ip extcommunity-filter

Function

The **ip extcommunity-filter** command creates an extended community filter.

The **undo ip extcommunity-filter** command deletes an extended community filter.

By default, no extended community filter is configured.

Format

ip extcommunity-filter { *basic-extcomm-filter-num* | **basic** *basic-extcomm-filter-name* } { **deny** | **permit** } { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address:nn* } } &<1-16>

ip extcommunity-filter { *advanced-extcomm-filter-num* | **advanced** *advanced-extcomm-filter-name* } { **deny** | **permit** } *regular-expression*

undo ip extcommunity-filter { *basic-extcomm-filter-num* | **basic** *basic-extcomm-filter-name* } [{ **deny** | **permit** } { **rt** { *as-number:nn* | *4as-number:nn* | *ipv4-address:nn* } } &<1-16>]

undo ip extcommunity-filter { *advanced-extcomm-filter-num* | **advanced** *advanced-extcomm-filter-name* } [*regular-expression*]

Parameters

Parameter	Description	Value
deny	Sets the matching mode of the extended community filter to deny.	-
permit	Sets the matching mode of the extended community filter to permit.	-
rt	Sets the extended community filter type to RT.	-
as-number	Specifies the AS number.	The value is an integer ranging from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
4as-number	Specifies a 4-byte AS number.	A 4-byte AS number is divided into the following types: ● It is an integer ranging from 65536 to 4294967295. ● It is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively
ipv4-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
nn	Specifies an integer.	● When the value of *as-number* is a 2-byte AS number, the value of *nn* ranges from 0 to 4294967295. ● When the value of *4as-number* is a 4-byte AS number, the value of *nn* ranges from 0 to 65535. ● For *ipv4-address*, the value of *nn* ranges from 0 to 65535.
basic-extcomm-filter-num	Specifies the number of a basic extended community filter.	The value is an integer ranging from 1 to 199.
basic *basic-extcomm-filter-name*	Specifies the name of a basic extended community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The value cannot contain only numerals. When double quotation marks are used around the string, spaces are allowed in the string.
advanced-extcomm-filter-num	Specifies the number of an advanced extended community filter.	The value is an integer ranging from 200 to 399.
advanced *advanced-extcomm-filter-name*	Specifies the name of an advanced extended community filter.	The name is a string of 1 to 51 case-sensitive characters without spaces. The value cannot contain only numerals. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
regular-expression	Specifies the regular expression used to match the extended community information. For details about a regular expression, see "CLI Overview" in the *Huawei AR Seriesrouter - Configuration Guide - Basic Configuration*.	It is a string of 1 to 255 space-tolerant characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The extended community attribute is a private attribute of BGP, and can be used only to filter BGP routes. The extended community attribute can be used as a matching rule of a routing policy by using the **ip extcommunity-filter** and **if-match extcommunity-filter** commands together. Currently, only the RT extended community attribute is supported.

The relationship between **ip extcommunity-filter** commands with the same extended community filter number specified is "AND".

Run the **display ip extcommunity-filter** command to view detailed configuration for the extended community filter.

Precautions

By default, extended community filters work in **deny** mode. If all matching rules in a filter are configured to work in **deny** mode, all routes are denied by the filter; to prevent this problem, configure one matching rule in **permit** mode after one or multiple matching rules in **deny** mode so that the routes except for those denied by preceding matching rules are permitted by the filter.

Example

Configure an RT extended community filter of which the sequence number is 1.

```
<Huawei> system-view
[Huawei] ip extcommunity-filter 1 deny rt 200:200
```

Related Topics

9.9.26 display ip extcommunity-filter

9.9.47 ip ip-prefix

Function

The **ip ip-prefix** command creates an IPv4 prefix list or an entry in an IPv4 prefix list.

The **undo ip ip-prefix** command deletes an IPv4 prefix list or an entry from an IPv4 prefix list.

By default, no IPv4 prefix list is created.

Format

ip ip-prefix *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ipv4-address mask-length* [**match-network**] [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number*]

ip ip-prefix *ip-prefix-name* **description** *text*

undo ip ip-prefix *ip-prefix-name* **description** [*text*]

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IPv4 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
index *index-number*	Specifies the sequence number of an entry in the IPv4 prefix list.	The value is an integer that ranges from 1 to 4294967295. By default, the sequence number increases by 10 according to the configuration order, and the first sequence number is 10. **NOTE** A maximum of 65535 entries can be configured in an IP prefix list.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
permit	Specifies the matching mode of the IP prefix list as permit. In permit mode, if the IP address to be filtered is within the defined prefix range, the IP address matches the routing policy and does not continue to match the next entry. Otherwise, the IP address continues to match the next entry.	-
deny	Specifies the matching mode of the IP prefix list as deny. In deny mode, if the IP address to be filtered is within the defined prefix range, the IP address fails to match the routing policy and cannot match the next entry. Otherwise, the IP address continues to match the next entry.	-
ipv4-address	Specifies an IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 0 to 32.
match-network	Matches the network address. **match-network** is used to filter routes to a specified IP address and can be configured only when *ipv4-address* is 0.0.0.0. For example, the **ip ip-prefix prefix1 permit 0.0.0.0 8** command filters all routes with mask length 8, while the **ip ip-prefix prefix1 permit 0.0.0.0 8 match-network** command filters all routes to the IP address range from 0.0.0.1 to 0.255.255.255.	-
greater-equal *greater-equal-value*	Specifies the lower threshold of the mask length. If **greater-equal** *greater-equal-value* and **less-equal** *less-equal-value* are not specified, the value of *mask-length* is the mask length.	*greater-equal-value* must meet the following requirement: *mask-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. If **greater-equal** is configured, the mask ranges from *greater-equal-value* to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
less-equal *less-equal-value*	Specifies the upper threshold of the mask length. If **greater-equal** *greater-equal-value* and **less-equal** *less-equal-value* are not specified, the value of *mask-length* is the mask length.	*less-equal-value* must meet the following requirement: *mask-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 32. If **less-equal** is configured, the mask ranges from *mask-length* to *less-equal-value*.
description *text*	Specifies the description of the IP prefix list.	The value is a string of 1 to 80 case-sensitive characters without spaces. If the string is enclosed within double quotation marks ("), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **ip ip-prefix** command is used to configure an IPv4 prefix list. An IP prefix can be used as a filter by various protocols or used together with a routing policy.

- The **ip ip-prefix** command can be used together with the following commands to filter routing information to be advertised globally based on an IP prefix list:
  - **filter-policy export** (RIP)
  - **filter-policy export** (OSPF)
  - **filter-policy export** (IS-IS)
  - **filter-policy export** (BGP)
- The **ip ip-prefix** command can be used together with the following commands to filter routing information to be accepted globally based on an IP prefix list:
  - **filter-policy import** (RIP)
  - **filter-policy import** (OSPF)
  - **filter-policy import** (IS-IS)
  - **filter-policy import** (BGP)
- The **ip ip-prefix** command can be used together with the following commands to configure a route filtering policy based on an IP prefix list for a specific peer:

 Copyright © Huawei Technologies Co., Ltd.

  - **peer ip-prefix** (BGP)
- The **import-route isis level-1 into level-2 filter-policy ip-prefix** *ip-prefix-name* [**tag** *tag*] command configures route leak from an IS-IS Level-1 area to a Level-2 area based on an IP prefix list.
- The **import-route isis level-2 into level-1 filter-policy ip-prefix** *ip-prefix-name* [**tag** *tag*] command configures route leak from an IS-IS Level-2 area to a Level-1 area based on an IP prefix list.
- The **ip ip-prefix** command and the **if-match ip-prefix** command can be used together to test received or sent routes based on an IP prefix list.

An IP prefix list can contain multiple entries with each entry specifying an IP prefix range. The relationship between the entries is "OR". That is, if a route matches one entry, the route matches the IP prefix list; if a route does not match any entry, the route fails to match the IP prefix list.

An IP prefix range is determined by *mask-length* and [*greater-equal-value*, *less-equal-value*]. If *mask-length* and [*greater-equal-value*, *less-equal-value*] are specified, an IP address must match the specified prefix range.

When the value of *ipv4-address* is 0.0.0.0, a wildcard address, all routes within the mask length range are permitted or denied no matter what value the mask length is specified as.

For example, the five routes to 10.1.1.0/24, 10.1.1.1/32, 10.1.1.0/26, 10.2.2.0/24, and 10.1.0.0/16 are filtered based on different IP prefix lists, and the results are different.

- Single-Node Matching
  - Case 1:

    ```
    ip ip-prefix aa index 10 permit 10.1.1.0 24
    ```

    Matching result: The route 10.1.1.0/24 is permitted, and the other routes are denied.

    Note: This is a single-node accurate matching case, which indicates that only the route whose destination IP address and mask are the same as those specified by the IP prefix meets the matching conditions. In this case, permit is configured as the matching mode. Therefore, the route 10.1.1.0/24 is permitted, and the other routes are denied because they do not meet the matching conditions.
  - Case 2:

    ```
    ip ip-prefix aa index 10 deny 10.1.1.0 24
    ```

    Matching result: All routes are denied.

    Note: This is also a single-node accurate matching case, which indicates that only the route whose destination IP address and mask are the same as those specified by the IP prefix meets the matching conditions. In this case, deny is configured as the matching mode. Therefore, all routes are denied, regardless of whether they meet the matching conditions.
- Multi-Node Matching
  - Case 1:

    ```
    ip ip-prefix aa index 10 deny 10.1.1.0 24
    ip ip-prefix aa index 20 permit 10.1.1.1 32
    ```

    Matching result: The route 10.1.1.0/24 is denied; the route 10.1.1.1/32 is permitted; the other routes are denied.

Note: This is a multi-node accurate matching case.

- When the route 10.1.1.0/24 is matching node 10 (node with the index 10), it meets the matching conditions but is denied because the matching mode is **deny**.
- When the route 10.1.1.1/32 is matching node 10, it does not meet the matching conditions and continues to match node 20 (node with the index 20). Because this route matches the matching conditions of node 20, and the matching mode of node 20 is **permit**, this route is permitted.
- Other routes do not meet the matching conditions of nodes 10 and 20, and these routes are denied by default.

– Case 2:

```
ip ip-prefix aa index 10 permit 10.1.1.0 24 less-equal 32
```

Configuration result: *greater-equal-value* is 24, and *less-equal-value* is 32.

Matching result: The routes 10.1.1.0/24, 10.1.1.1/32, and 10.1.1.0/26 are permitted, and the other routes are denied.

When configuring **greater-equal** and **less-equal**, ensure that their values meet the requirement: *mask-length* ≤ *greater-equal-value* ≤ *less-equal-value*. Otherwise, the configuration fails.

– Case 3:

```
ip ip-prefix aa index 10 permit 10.1.1.0 24 greater-equal 26
```

Configuration result: *greater-equal-value* is 26, and *less-equal-value* is 32.

Matching result: The routes 10.1.1.1/32 and 10.1.1.0/26 are permitted, and the other routes are denied.

– Case 4:

```
ip ip-prefix aa index 10 permit 10.1.1.0 24 greater-equal 26 less-equal 32
```

Configuration result: *greater-equal-value* is 26, and *less-equal-value* is 32.

Matching result: The routes 10.1.1.1/32 and 10.1.1.0/26 are permitted, and the other routes are denied.

- Wildcard-Address Matching

  – Case 1:

```
ip ip-prefix aa index 10 permit 0.0.0.0 8 less-equal 32
```

Configuration result: *greater-equal-value* is 8, and *less-equal-value* is 32. Because the address 0.0.0.0 is a wildcard address, routes with the mask length ranging from 8 to 32 bits meet the matching conditions.

Matching result: Routes with the mask length ranging from 8 to 32 bits are all permitted.

– Case 2:

```
ip ip-prefix aa index 10 deny 0.0.0.0 24 less-equal 32
ip ip-prefix aa index 20 permit 0.0.0.0 0 less-equal 32
```

Configuration result: For node 10, *greater-equal-value* is 24, and *less-equal-value* is 32. Because the address 0.0.0.0 is a wildcard address, routes with the mask length ranging from 24 to 32 bits are all denied. For node 20, *greater-equal-value* is 0, and *less-equal-value* is 32. Because the address 0.0.0.0 is a wildcard address, all routes except the routes with the mask length ranging from 24 to 32 bits are permitted.

 Copyright © Huawei Technologies Co., Ltd.

Matching result: The route 10.1.0.0/16 is permitted, and the other routes are denied.

– Case 3:

```
ip ip-prefix aa index 10 deny 10.2.2.0 24
ip ip-prefix aa index 20 permit 0.0.0.0 0 less-equal 32
```

Configuration result: For node 10, the route 10.2.2.0/24, which meets the matching conditions, is denied. For node 20, the other routes are all permitted.

Matching result: All routes except the route 10.2.2.0/24 are permitted.

Example

Configure the IP prefix list named **p1** to permit only the routes with the mask length ranging from 17 to 18 on the network segment 10.0.0.0/8.

```
<Huawei> system-view
[Huawei] ip ip-prefix p1 permit 10.0.0.0 8 greater-equal 17 less-equal 18
```

Configure the IP prefix list named **p3** to deny the routes to the IP address ranging from 0.0.0.1 to 0.255.255.255.

```
<Huawei> system-view
[Huawei] ip ip-prefix p3 index 10 deny 0.0.0.0 8 match-network
[Huawei] ip ip-prefix p3 index 20 permit 0.0.0.0 0 less-equal 32
```

Related Topics

9.9.37 if-match ip

9.9.38 if-match ip-prefix

9.9.27 display ip ip-prefix

9.9.48 ip ipv6-prefix

Function

The **ip ipv6-prefix** command configures an IPv6 prefix list or an entry in an IPv6 prefix list.

The **undo ip ipv6-prefix** command deletes an IPv6 prefix list or an entry from an IPv6 prefix list.

By default, no IPv6 prefix list is created.

Format

ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address prefix-length* [**match-network**] [**greater-equal** *greater-equal-value*] [**less-equal** *less-equal-value*]

undo ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*]

ip ipv6-prefix *ipv6-prefix-name* **description** *text*

undo ip ipv6-prefix *ipv6-prefix-name* **description** [*text*]

Parameters

Parameter	Description	Value
ipv6-prefix-name	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
index *index-number*	Specifies the sequence number of an entry in the IPv6 prefix list.	The value is an integer that ranges from 1 to 4294967295. By default, the sequence number increases by 10 according to the configuration order, and the first sequence number is 10. **NOTE** A maximum of 65535 entries can be configured in an IPv6 prefix list.
permit	Specifies the matching mode of the IPv6 prefix list as permit. In permit mode, if the IPv6 address to be filtered is within the defined prefix range, the IPv6 address matches the routing policy and does not continue to match the next entry. Otherwise, the IPv6 address continues to match the next entry.	-
deny	Specifies the matching mode of the IPv6 prefix list as deny. In deny mode, if the IPv6 address to be filtered is within the defined prefix range, the IPv6 address fails to match the routing policy and cannot match the next entry. Otherwise, the IPv6 address continues to match the next entry.	-
ipv6-address	Specifies the IPv6 prefix range in the form of an IPv6 address. If :: is specified, the address 0::0 is matched.	-
prefix-length	Specifies the IPv6 prefix range using the mask length.	The value is an integer that ranges from 0 to 128. If ::0 less-equal 128 is used, all IPv6 addresses are matched.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match-network	Matches the network address. **match-network** is used to filter routes to a specified IPv6 address and can be configured only when *ipv6-address* is 0.0.0.0. For example, the **ip ipv6-prefix prefix1 permit :: 96** command filters all IPv6 routes with mask length 96, while the **ip ipv6-prefix prefix1 permit :: 96 match-network** command filters all routes to the IPv6 address range from ::1 to ::FFFF:FFFF.	-
greater-equal *greater-equal-value*	Specifies the lower threshold of the mask length.	*greater-equal-value* must meet the following requirement: *prefix-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128.
less-equal *less-equal-value*	Specifies the upper threshold of the mask length.	*less-equal-value* must meet the following requirement: *prefix-length* ≤ *greater-equal-value* ≤ *less-equal-value* ≤ 128.
description *text*	Specifies the description of the IPv6 prefix list.	The value is a string of 1 to 80 case-sensitive characters without spaces. If the string is enclosed within double quotation marks ("), the string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An IPv6 prefix list is used to filter IPv6 addresses. An IPv6 prefix list may contain multiple entries with each entry specifying an IPv6 prefix range. The relationship between the entries is "OR". That is, if a route matches one entry, the route matches the IPv6 prefix list; if a route does not match any entry, the route fails to match the IPv6 prefix list.

After an IPv6 prefix list is configured, by default, the RM module immediately instructs each protocol application to use the list to filter IPv6 addresses. To delay using an IPv6 prefix list to filter IPv6 addresses, run the **route-policy-change notify-delay** command to set the delay.

NOTE

On the AR, all unmatched routes are filtered by default. If all entries are in **deny** mode, all routes are filtered. It is recommended to define a **permit :: 0 less-equal 128** entry after multiple entries in **deny** mode to permit all the other IPv6 routes.

Example

Permit the routes with the mask length ranging from 32 to 64 bits.

```
<Huawei> system-view
[Huawei] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
```

Deny the routes with the IP prefix FC00:0:0:D00::/32 and with the prefix longer than 32 bits, and permit the other IPv6 routes.

```
<Huawei> system-view
[Huawei] ip ipv6-prefix abc deny fc00:0:0:d00:: 32 less-equal 128
[Huawei] ip ipv6-prefix abc permit :: 0 less-equal 128
```

Configure the IPv6 prefix list named **p3** to deny the routes to the IPv6 address ranging from ::1 to ::FFFF:FFFF.

```
<Huawei> system-view
[Huawei] ip ipv6-prefix p3 index 10 deny :: 96 match-network
[Huawei] ip ipv6-prefix p3 index 20 permit :: 0 less-equal 128
```

Related Topics

9.9.54 route-policy-change notify-delay

9.9.49 ip rd-filter

Function

The **ip rd-filter** command creates an RD filter.

The **undo ip rd-filter** command deletes an RD filter.

By default, no RD filter is configured.

Format

ip rd-filter *rd-filter-number* { **deny** | **permit** } *route-distinguisher* &<1-10>

undo ip rd-filter *rd-filter-number* [{ **deny** | **permit** } *route-distinguisher* &<1-10>]

Parameters

Parameter	Description	Value
rd-filter-number	Specifies the number of an RD filter.	The value is an integer ranging from 1 to 255.
permit	Permits a route to match the rules if its RD matches the rules.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
deny	Denied a route if its RD matches the rules.	-
route-distinguisher	Specifies the RD to aa:nn or ipv4-address:nn. You can set a maximum of 10 RDs. The AR support RDs in the following formats: • ipv4-address:nn, such as 10.1.1.1:200 • aa:nn, such as 100:1 • aa.aa:nn, such as 100.100:1 • ipv4-address:* in the wildcard format, such as 10.1.1.1:*, indicating that the RD begins with 10.1.1.1 • aa:* in the wildcard format, such as 100:*, indicating that the RD begins with 100 • aa.aa:* in the wildcard format, such as 100.100:*, indicating that the RD begins with 100.100	• The IPv4 address is in dotted decimal notation. • The *nn* in ipv4-address:nn is an integer ranging from 0 to 65535. • In aa:nn, the *aa* is an integer ranging from 0 to 65535, and *nn* is an integer ranging from 0 to 4294967295. • The *aa* and *nn* in aa:*, aa.aa:*, and aa.aa:nn are both integers ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **ip rd-filter** command is used together with the **if-match rd-filter** command. First use the **ip rd-filter** command to configure an RD filter, and use the **if-match rd-filter** command to configure a matching rule based on the RD filter in a routing policy. The routing policy is used to filter routes that are received and advertised.

The RD filter has the following rules:

- If the RD filter is not configured but is used to filter routes, the matching result is **permit**.

  For example, the RD filter 100 is not configured but is used by the routing policy:

  ```
  route-policy test permit node 10
  if-match rd-filter 100
  ```

When the routing policy is used to filter routes, the routes match this **if-match** clause, and the routes match the node 10 in the routing policy named **test**.

- If the RD filter is configured but the RD of routes does not match any RD defined in the RD filter, the default matching result is **deny**.

  For example, the RD of routes is 100:1, and the configuration of the RD filter is as follows:

  ```
  ip rd-filter 100 permit 10.1.1.1:100
  ```

  When the RD filter is used to filter routes, the matching result is **deny**.

- The relationship between the rules of the RD filter is "OR". This is different from the community filter. This is because each route has only one RD but can have multiple communities.

  For example, the RD filters in the following formats have the same matching results:

  Format 1:

  ```
  ip rd-filter 100 permit 100:1 200:1 10.2.2.2:1 10.3.3.3:1
  ```

  Format 2:

  ```
  ip rd-filter 100 permit 100:1 200:1
  ip rd-filter 100 permit 10.2.2.2:1
  ip rd-filter 100 permit 10.3.3.3:1
  ```

  The community filters in the following formats have different matching results:

  Format 1:

  ```
  ip community-filter 1 permit 100:1 200:1 300:1
  ```

  Format 2:

  ```
  ip community-filter 1 permit 100:1
  ip community-filter 1 permit 200:1 300:1
  ```

  In the preceding configuration of the community filter, the community defined in each rule must be a sub-set of route communities so that the rule can be matched.

- Routes are filtered according to the configuration order of multiple rules. For example:

  ```
  ip rd-filter 100 deny 200:1 10.5.5.5:1
  ip rd-filter 100 permit 200:* 10.5.5.5:*
  ```

  In this situation, the route with the RD 200:1 or 5.5.5.5:1 is denied. If the configuration order of multiple rules is reversed as follows:

  ```
  ip rd-filter 100 permit 200:* 10.5.5.5:*
  ip rd-filter 100 deny 200:1 10.5.5.5:1
  ```

  In this situation, the route with the RD 200:1 or 10.5.5.5:1 is permitted.

- Each RD filter can be configured with a maximum of 255 rules.

Example

Configure an RD filter.

```
<Huawei> system-view
[Huawei] ip rd-filter 1 permit 100:1
```

Related Topics

9.9.41 if-match rd-filter

9.9.29 display ip rd-filter

9.9.50 reset ip ip-prefix

Function

The **reset ip ip-prefix** command resets the statistics of the specified IPv4 prefix list.

Format

reset ip ip-prefix [*ip-prefix-name*]

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IPv4 prefix list. If *ip-prefix-name* is not specified, you can reset the statistics of all the IPv4 prefix lists.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IPv4 prefix list can be used to filter IPv4 addresses. When filtering IPv4 addresses, the system records the numbers of prefixes that are permitted and denied by the IPv4 prefix list. You can run the **display ip ip-prefix** command to view the numbers.

To view the number of IPv4 prefixes that are permitted and denied by the IPv4 prefix list, run the **reset ip ip-prefix** command to clear statistics about permitted and denied routes in the IPv4 prefix list, and then run the **display ip ip-prefix** command to display the number of IPv4 prefixes since the previous operation.

Configuration Impact

The **reset ip ip-prefix** command clears statistics about the IPv4 prefix list. After that, the previous statistics cannot be shown.

Precautions

The **reset ip ip-prefix** command:

 Copyright © Huawei Technologies Co., Ltd.

- Clears statistics in a specified IPv4 prefix list, if the name of the IPv4 prefix list is specified using *ip-prefix-name*.
- Clears statistics in all IPv4 prefix lists, if the name of the IPv4 prefix list is not specified using *ip-prefix-name*.

Example

Reset the statistics of the specified IPv4 prefix list.

```
<Huawei> reset ip ip-prefix abc
```

9.9.51 reset ip ipv6-prefix

Function

The **reset ip ipv6-prefix** command resets the timer of a specified IPv6 prefix list.

Format

reset ip ipv6-prefix [*ipv6-prefix-name*]

Parameters

Parameter	Description	Value
ipv6-prefix-name	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IPv6 prefix list can be used to filter IPv6 addresses. When filtering IPv6 addresses, the system records the numbers of prefixes that are permitted and denied by the IPv6 prefix list. You can run the **display ip ipv6-prefix** command to view the numbers.

To view the number of IPv6 prefixes that are permitted and denied by the IPv6 prefix list, run the **reset ip ipv6-prefix** command to clear statistics about permitted and denied routes in the IPv6 prefix list, and then run the **display ip ipv6-prefix** command to display the number of IPv6 prefixes since the previous operation.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

The **reset ip ipv6-prefix** command clears statistics about the IPv6 prefix list. After that, the previous statistics cannot be shown.

Precautions

The **reset ip ipv6-prefix** command:

- Clears statistics in a specified IPv6 prefix list, if the name of the IPv6 prefix list is specified using *ipv6-prefix-name*.
- Clears statistics in all IPv6 prefix lists, if the name of the IPv6 prefix list is not specified using *ipv6-prefix-name*.

Example

Resets the timer of the IPv6 prefix list named **abc**.

```
<Huawei> reset ip ipv6-prefix abc
```

9.9.52 reset route-policy counters

Function

The **reset route-policy** command resets route-policy counters.

Format

reset route-policy *route-policy-name* **counters**

Parameters

Parameter	Description	Value
route-policy-name	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The route-policy is used to filter routes and set the attributes of a route that matches a route-policy. When a route-policy filters routes, the system records the

number of routes that match the route-policy nodes. You can run the **display route-policy** to view the numbers.

The **reset route-policy counters** command clears the number of routes which match or do not match the route-policy. You can run both the **reset route-policy counters** command and the **display route-policy** command to instruct whether to record the number of routes matching a specified route-policy.

Configuration Impact

The **reset route-policy counters** command clears the number of routes which match or do not match the route-policy. After that, the number cannot be restored.

Example

Reset the counters of a route-policy named **policy1**.

```
<Huawei> reset route-policy policy1 counters
```

Related Topics

9.9.30 display route-policy

9.9.53 route-policy

Function

The **route-policy** command creates a routing policy and displays the Route-Policy view.

The **undo route-policy** command deletes a specified routing policy.

By default, no routing policy is configured.

Format

route-policy *route-policy-name* { **permit** | **deny** } **node** *node*

undo route-policy *route-policy-name* [**node** *node*]

Parameters

Parameter	Description	Value
route-policy-name	Specifies the name of a routing policy. If the routing policy does no exist, create a routing policy and enter its Route-Policy view. If the routing policy exists, enter its Route-Policy view.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
permit	Specifies the matching mode of the routing policy as permit. In permit mode, a route matches all the **if-match** clauses, the route matches the routing policy and the actions defined by the **apply** clause are performed on the route. Otherwise, the route continues to match the next entry.	-
deny	Specifies the matching mode of the routing policy as deny. In deny mode, if a route matches all the **if-match** clauses, the route fails to match the routing policy and cannot match the next node.	-
node *node*	Specifies the index of the node in the routing policy. When the routing policy is used to filter routes, the node with the smaller value of *node* is matched first.	The value is an integer ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A routing policy is used to filter routes and set route attributes for the routes that match the routing policy. A routing policy consists of multiple nodes. One node can be configured with multiple **if-match** and **apply** clauses.

The **if-match** clauses define matching rules for this node, and the **apply** clauses define behaviors for the routes that match the rules.

The relationship among **if-match** clauses of the same node that are based on different route attributes is AND. A route matches a node only when the route matches all the filtering rules specified in the **if-match** clauses of the node. The **apply** clauses specify actions. The relationship among **if-match** clauses of the same node that are based on the same route attribute is OR. The system matches routes against the **if-match** clauses in order. If a route matches an **if-match** clause, the system no longer matches the route against the rest **if-match** clauses. For example, the **if-match community-filter 1** and **if-match as-path-filter 1** configurations in node 10 are based on different route attributes. Therefore, the relationship among **if-match** clauses of this node is AND. The **if-match community-filter 1** and **if-match community-filter 2** configurations in node 20 are both based on the community attribute. Therefore, the relationship among **if-match** clauses of this node is OR. If no **if-match** clause is specified, all the routes can pass the node.

 Copyright © Huawei Technologies Co., Ltd.

You can run the **display route-policy** command to view the number of routes that match and do not match the routing policy.

Procedure

After a routing policy is created, the system prompts "Info: New Sequence of this List !" and displays the Route-Policy view. The system displays no prompt when a routing policy is deleted.

Precautions

After a route-policy is configured, by default, the RM immediately notifies each protocol to apply the route-policy to filter routes. To delay applying a route-policy, you need to run the **route-policy-change notify-delay** command to set the delay for applying the route-policy.

You can run the **display route-policy** command to view the number of routes that match and do not match the route-policy.

An *route-policy-name* must have been configured using the **route-policy** command before the *route-policy-name* is referenced by another command.

An *route-policy-name* cannot be deleted using the **undo route-policy** command when it is being referenced using *route-policy-name*. To delete the *route-policy-name*, cancel the reference configuration first.

If an **if-match** clause of a route-policy defines an **ip-prefix**-based filtering rule, the filtering rule applies to IPv4 prefixes, not to IPv6 prefixes, and IPv6 prefixes match the filtering rule by default. If IPv6 prefixes also need to be filtered, add an **ipv6-prefix**-based **if-match** clause. Similarly, if an **if-match** clause of a route-policy defines an **ipv6-prefix**-based filtering rule, the filtering rule applies to IPv6 prefixes, not to IPv4 prefixes, and IPv4 prefixes match the filtering rule by default. If IPv4 prefixes also need to be filtered, add an **ip-prefix**-based **if-match** clause.

The configuration of a peer takes precedence over that of the peer group to which the peer belongs. That is, when a routing policy is used to control BGP route advertisement or receiving, the priority of this configuration on a BGP peer is higher than that of the configuration on the peer group.

Example

Configure the routing policy named **policy1** whose node number is 10 and the matching mode is **permit**.

```
<Huawei> system-view
[Huawei] route-policy policy1 permit node 10
[Huawei-route-policy]
```

Related Topics

9.9.30 display route-policy

9.9.54 route-policy-change notify-delay

Function

The **route-policy-change notify-delay** command sets the delay before the RM to notify each protocol of applying a new policy after the original route-policy changes.

The **undo route-policy-change notify-delay** command restores the default setting.

By default, this command is not configured, and the delay time is 0s.

Format

route-policy-change notify-delay *delay-time*

undo route-policy-change notify-delay

Parameters

Parameter	Description	Value
delay-time	Specifies the delay for applying a new policy after the original route-policy changes.	The value is an integer ranging from 1 to 180, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The AR process the changes of a route-policy according to the following rules.

After the configuration of a route-policy changes, by default, the RM immediately notifies the protocol of performing related operations. To delay processing the changes of the route-policy, you can run the **route-policy-change notify-delay** command to set the delay for change processing. The new policy is applied after the timer expires:

- If the configuration of the route-policy changes again within the delay, the RM resets the timer.
- If the new policy is configured for BGP, the **refresh bgp all** command can be used within the delay set by the **route-policy-change notify-delay** command to trigger BGP to immediately use the new policy.

The following commands are related to the timer:

- **route-policy**

 Copyright © Huawei Technologies Co., Ltd.

- **ip ip-prefix**
- **ip ipv6-prefix**
- **ip as-path-filter**
- **ip community-filter**
- **ip extcommunity-filter**
- **ip rd-filter**
- **acl**

Example

Set the delay before the RM to notify each protocol of applying a new policy after the original route-policy changes.

```
<Huawei> system-view
[Huawei] route-policy-change notify-delay 20
```

Related Topics

9.9.53 route-policy
9.9.47 ip ip-prefix
9.9.48 ip ipv6-prefix
9.9.44 ip as-path-filter
9.9.45 ip community-filter
9.9.46 ip extcommunity-filter
9.9.49 ip rd-filter
19.7.4 acl (system view)

9.10 IP Routing Basic Configuration Commands

9.10.1 display fib

Function

The **display fib** command displays information about the FIB table.

Format

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] [**verbose**]

Parameters

Parameter	Description	Value
slot-id	Displays information about the FIB table with a specified slot ID.	The value is an integer and the value range depends on the device configuration.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about the FIB table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display fib** command displays information about the FIB table. Each row represents a route.

NOTE

If there are lots of routes, using wildcard (|, **begin**, **exclude**, **include**, *regular-expression*) to display information or details lasts a long time. You can press Ctrl+C to terminate information display.

Example

Display brief information about the FIB table.

```
<Huawei> display fib
Route Flags: G - Gateway Route, H - Host Route,    U - Up Route
             S - Static Route,  D - Dynamic Route, B - Black Hole Route
             L - Vlink Route
------------------------------------------------------------------------------
 FIB Table:
 Total number of Routes : 4
Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
127.0.0.1/32       127.0.0.1       HU   t[49]         InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[49]         InLoop0         0x0
127.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
255.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
```

Display information starting with the line that contains 127.0.0.0.

```
<Huawei> display fib | begin 127.0.0.0

Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
127.0.0.0/8        127.0.0.1       U    t[49]         InLoop0         0x0
127.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
255.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
```

Display information about all the lines that contain HU.

```
<Huawei> display fib | include HU

Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
127.0.0.1/32       127.0.0.1       HU   t[49]         InLoop0         0x0
127.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
255.255.255.255/32 127.0.0.1       HU   t[49]         InLoop0         0x0
```

Display information about all the lines that do not contain HU.

```
<Huawei> display fib | exclude HU

Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
127.0.0.0/8        127.0.0.1       U    t[49]         InLoop0         0x0
```

Display detailed information about the FIB table.

```
<Huawei> display fib verbose
Route Flags: G - Gateway Route, H - Host Route,    U - Up Route
             S - Static Route,  D - Dynamic Route, B - Black Hole Route
             L - Vlink Route
------------------------------------------------------------------------------
 FIB Table:
 Total number of Routes : 23

 Destination: 10.0.0.255          Mask     : 255.255.255.255
 Nexthop    : 127.0.0.1           OutIf    : InLoopBack0
 LocalAddr  : 127.0.0.1           LocalMask: 0.0.0.0
 Flags      : HU                  Age      : 445874sec
 ATIndex    : 0                   Slot     : 0
 LspFwdFlag : 0                   LspToken : 0x0
 InLabel    : NULL                OriginAs : 0
 BGPNextHop : 0.0.0.0             PeerAs   : 0
 QosInfo    : 0x0                 OriginQos: 0x0
 NexthopBak : 0.0.0.0             OutIfBak : [No Intf]
 LspTokenBak: 0x0                 InLabelBak : NULL
 LspToken_ForInLabelBak     : 0x0
 EntryRefCount : 0
 VlanId : 0x0
 BgpKey : 0
 BgpKeyBak : 0
 LspType         : 0              Label_ForLspTokenBak   : 0
 MplsMtu         : 0              Gateway_ForLspTokenBak : 0
 NextToken       : 0x0            IfIndex_ForLspTokenBak : 0
 Label_NextToken : 0              Label : 0
 LspBfdState     : 0

 Destination: 10.0.0.1            Mask     : 255.255.255.255
 Nexthop    : 127.0.0.1           OutIf    : InLoopBack0
 LocalAddr  : 127.0.0.1           LocalMask: 0.0.0.0
 Flags      : HU                  Age      : 445874sec
 ATIndex    : 0                   Slot     : 0
 LspFwdFlag : 0                   LspToken : 0x0
 InLabel    : NULL                OriginAs : 0
 BGPNextHop : 0.0.0.0             PeerAs   : 0
 QosInfo    : 0x0                 OriginQos: 0x0
 NexthopBak : 0.0.0.0             OutIfBak : [No Intf]
 LspTokenBak: 0x0                 InLabelBak : NULL
 LspToken_ForInLabelBak     : 0x0
 EntryRefCount : 0
 VlanId : 0x0
 BgpKey : 0
 BgpKeyBak : 0
 LspType         : 0              Label_ForLspTokenBak   : 0
 MplsMtu         : 0              Gateway_ForLspTokenBak : 0
 NextToken       : 0x0            IfIndex_ForLspTokenBak : 0
 Label_NextToken : 0              Label : 0
 LspBfdState     : 0

 Destination: 10.0.0.255          Mask     : 255.255.255.255
 Nexthop    : 127.0.0.1           OutIf    : InLoopBack0
```

```
LocalAddr  : 127.0.0.1          LocalMask: 0.0.0.0
Flags      : HU                 Age      : 445874sec
ATIndex    : 0                  Slot     : 0
LspFwdFlag : 0                  LspToken : 0x0
InLabel    : NULL               OriginAs : 0
BGPNextHop : 0.0.0.0            PeerAs   : 0
QosInfo    : 0x0                OriginQos: 0x0
NexthopBak : 0.0.0.0            OutIfBak : [No Intf]
LspTokenBak: 0x0                InLabelBak : NULL
LspToken_ForInLabelBak     : 0x0
EntryRefCount : 0
VlanId : 0x0
BgpKey : 0
BgpKeyBak : 0
LspType         : 0             Label_ForLspTokenBak   : 0
MplsMtu         : 0             Gateway_ForLspTokenBak : 0
NextToken       : 0x0           IfIndex_ForLspTokenBak : 0
Label_NextToken : 0             Label : 0
LspBfdState     : 0

Destination: 10.0.0.1           Mask     : 255.255.255.255
Nexthop    : 127.0.0.1          OutIf    : InLoopBack0
LocalAddr  : 127.0.0.1          LocalMask: 0.0.0.0
Flags      : HU                 Age      : 445874sec
ATIndex    : 0                  Slot     : 0
LspFwdFlag : 0                  LspToken : 0x0
InLabel    : NULL               OriginAs : 0
BGPNextHop : 0.0.0.0            PeerAs   : 0
QosInfo    : 0x0                OriginQos: 0x0
NexthopBak : 0.0.0.0            OutIfBak : [No Intf]
LspTokenBak: 0x0                InLabelBak : NULL
LspToken_ForInLabelBak     : 0x0
EntryRefCount : 0
VlanId : 0x0
BgpKey : 0
BgpKeyBak : 0
LspType         : 0             Label_ForLspTokenBak   : 0
MplsMtu         : 0             Gateway_ForLspTokenBak : 0
NextToken       : 0x0           IfIndex_ForLspTokenBak : 0
Label_NextToken : 0             Label : 0
LspBfdState     : 0
```

Table 9-200 Description of the **display fib** command output

Item	Description
FIB Table	FIB table.
Total number of Routes	Total number of routes.
Destination/Mask	Destination address or mask length.
Nexthop	Next hop of a route.

Item	Description
Flag	Flag of a route, which is the combination of G, H, U, S, D, and B. ● G: indicates that the next hop is a gateway. ● H: indicates that the route is a host route. ● U: indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B: indicates a blackhole route of which the next hop is a null interface. ● L: indicates a Vlink route.
TimeStamp	How long an entry has been in the FIB table, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. If the value is not 0, packets matching the entry are forwarded by the tunnel. If the value is 0, packets matching the entry are not forwarded by the tunnel.

Table 9-201 Description of the **display fib verbose** command output

Item	Description
Destination	Destination address.
Mask	Mask length.
Nexthop	Next hop of a route.
OutIf	Outbound interface.
LocalAddr	Local IP address.
LocalMask	Mask of the local IP address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Flags	Flag of a route, which is the combination of G, H, U, S, D, and B. ● G: indicates that the next hop is a gateway. ● H: indicates that the route is a host route. ● U: indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B: indicates a blackhole route of which the next hop is a null interface. ● L: indicates a Vlink route.
Age	How long a route has been in the FIB table, in seconds.
ATIndex	Index of the virtual link between the local end and the gateway.
Slot	Slot ID of the outbound interface.
LspFwdFlag	LSP forwarding flag.
LspToken	LSP forwarding ID.
InLabel	Inner label of a VPN LSP.
OriginAs	Original AS number.
BGPNextHop	BGP next-hop address.
PeerAs	Peer AS number.
QosInfo	QoS information.
OriginQos	Original QoS information.
NexthopBak	Backup next hop.
OutIfBak	Backup outbound interface.
LspTokenBak	ID of the backup LSP.
InLabelBak	Backup inner label of a VPN LSP.
LspToken_ForInLabelBak	Backup LSP ID in the backup inner label of a VPN LSP.
EntryRefCount	Number of times an entry has been referenced.
VlanId	VLAN ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
BgpKey	Index allocated by BGP.
BgpKeyBak	Backup index allocated by BGP.
LspType	LSP type.
Label_ForLspTokenBak	Backup label of the LSP.
MplsMtu	MTU of MPLS packets.
Gateway_ForLspTokenBak	Next hop of the backup LSP.
NextToken	Token of the tunnel.
IfIndex_ForLspTokenBak	Backup outbound interface of the LSP.
Label_NextToken	Label of the tunnel.
Label	Label of the current LSP.
LspBfdState	Status of the BFD session that detects an LSP.

9.10.2 display fib acl

Function

The **display fib acl** command displays information about FIB entries that match a specified ACL rule.

Format

display fib [**vpn-instance** *vpn-instance-name*] **acl** *acl-number* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
acl-number	Displays information about the FIB table with a specified ACL rule.	The value is an integer that ranges from 2000 to 2999.
verbose	Displays detailed information about the FIB table.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display FIB entries that match an ACL rule.

```
<Huawei> display fib acl 2010
Route Entry matched by access-list 2010
 Summary Counts: 1
Destination/Mask Nexthop  Flag TimeStamp Interface     TunnelID
127.0.0.0/8      127.0.0.1 U    t[0]      InLoop0       0x0
```

Table 9-202 Description of the display fib acl command output

Item	Description
Route Entry matched by access-list	FIB entries that match an ACL rule.
Summary Counts	Total number of the FIB entries.
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.
Flag	Current flag, which is the combination of G, H, U, S, D, B and T. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface. ● T: indicates ingress TOKEN_SETBYLSPM nodes.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

9.10.3 display fib interface

Function

The **display fib interface** command displays information about FIB entries with a specified outbound interface.

Format

display fib [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface-type interface-number	Specifies the type and number of the outbound interface to a specified destination address.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display FIB entries with a specified outbound interface.

```
<Huawei> display fib interface vlanif10
Destination/Mask   Nexthop     Flag TimeStamp   Interface        TunnelID
10.1.1.0/24        10.1.1.2     U    t[115]      Vlanif10           0x0
100.1.1.1/32       100.1.1.1    HU   t[115]      Vlanif10           0x0
```

Table 9-203 Description of the display fib interface command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.
Flag	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

 Copyright © Huawei Technologies Co., Ltd.

9.10.4 display fib ip-prefix

Function

The **display fib ip-prefix** command displays information about the FIB table.

Format

display fib [**vpn-instance** *vpn-instance-name*] **ip-prefix** *prefix-name* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the FIB table of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
prefix-name	Specifies the name of an IP prefix list.	The value is a string of 1 to 169 characters.
verbose	Displays detailed information about the FIB table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays FIB entries that match a specified IP prefix list.

If 0 FIB entries match, the command output displays that zero FIB entries match.

If the name of an IP prefix list is not found, all FIB entries are displayed.

Example

Display FIB entries matching the IP prefix list **abc0**.

```
<Huawei> display fib ip-prefix abc0
Route Entry matched by prefix-list abc0
 Summary Counts: 4
Destination/Mask  Nexthop  Flag  TimeStamp  Interface   TunnelID
127.0.0.0/8       127.0.0.1 U     t[0]       InLoop0       0x0
127.0.0.1/32      127.0.0.1 U     t[0]       InLoop0       0x0
172.16.0.0/8      10.1.1.1  SU    t[0]       Vlanif10      0x0
172.16.0.0/15     10.1.1.1  SU    t[0]       Vlanif10      0x0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 9-204 Description of the display fib ip-prefix command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.
Flag	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

9.10.5 display fib longer

Function

The **display fib longer** command displays FIB entries that match a specified parameter.

The **display fib** [*slot-id*] *destination-address* command displays FIB entries that match a specified destination IP address. If the specified destination IP address matches an FIB entry in the natural mask range, all the subnets are displayed. Otherwise, FIB entries are displayed based on the longest matching principle.

The **display fib** [*slot-id*] *destination-address destination-mask* command displays FIB entries that accurately match the destination address and mask.

The **display fib** [*slot-id*] *destination-address* **longer** command displays all FIB entries that match destination IP addresses in the natural mask range.

 Copyright © Huawei Technologies Co., Ltd.

The **display fib** [*slot-id*] *destination-address* destination-mask **longer** command displays all FIB entries that match destination IP addresses in a specified mask range.

The **display fib** [*slot-id*] *destination-address1 destination-mask1 destination-address2 destination-mask2* command displays FIB entries that match destination IP addresses in the range of *destination-address1 destination-mask1* to *destination-address2 destination-mask2*.

If *slot-id* is specified, FIB entries on the specified LPU are displayed.

Format

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] *destination-address1* [*destination-mask1*] [**longer**] [**verbose**]

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] *destination-address1 destination-mask1 destination-address2 destination-mask2* [**verbose**]

Parameters

Parameter	Description	Value
slot-id	Displays information about the FIB table with a specified slot ID.	The value is an integer and the value range depends on the device configuration.
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
destination-address1	Indicates destination IP address 1.	The value is in dotted decimal notation.
destination-mask1	Indicates subnet mask 1.	The value is in dotted decimal notation or an integer that ranges from 0 to 32.
destination-address2	Indicates destination IP address 2.	The value is in dotted decimal notation.
destination-mask2	Indicates subnet mask 2.	The value is in dotted decimal notation or an integer that ranges from 0 to 32.
longer	Displays FIB entries matching a specified network segment or mask.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Displays detailed information about the FIB table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display FIB entries that match destination address 172.16.0.0 in the natural mask range or based on the longest match principle.

```
<Huawei> display fib 172.16.0.0
  Route Entry Count: 1
Destination/Mask  Nexthop  Flag  TimeStamp  Interface  TunnelID
172.16.0.0/16     10.1.1.1 U     t[0]       Vlanif10   0x0
```

Display the FIB entries with the destination addresses in the range of 72.16.0.0/16 to 172.16.0.6/16.

```
<Huawei> display fib 172.16.0.0 255.255.0.0 172.16.0.6 255.255.0.0
  Route Entry Count: 1
Destination/Mask  Nexthop  Flag  TimeStamp  Interface  TunnelID
172.16.0.1/8      10.1.1.1 U     t[0]       Vlanif10   0x0
```

Table 9-205 Description of the display fib longer command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Flag	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

9.10.6 display fib next-hop

Function

The **display fib next-hop** command displays FIB entries that match a specified next-hop IP address.

Format

display fib [**vpn-instance** *vpn-instance-name*] **next-hop** *ip-address*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about the FIB table of a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip-address	Specifies the next-hop IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display FIB entries that match a specified next-hop IP address.

```
<Huawei> display fib next-hop 10.1.1.1
Destination/Mask   Nexthop         Flag TimeStamp     Interface      TunnelID
10.1.1.1/32        10.1.1.1        HU   t[115]        Vlanif10       0x0
```

Table 9-206 Description of the display fib next-hop command output

Item	Description
Destination/Mask	Destination address or mask length.
Nexthop	Next hop.
Flag	Current flag, which is the combination of G, H, U, S, D, and B. ● G (gateway route): indicates that the next hop is a gateway. ● H (host route): indicates that the route is a host route. ● U (available route): indicates that the route status is Up. ● S: indicates a static route. ● D: indicates a dynamic route. ● B (blackhole route): indicates that the next hop is a null interface.
TimeStamp	Timestamp, which indicates the lifetime of an entry, in seconds.
Interface	Outbound interface to the destination address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TunnelID	Index of a forwarding entry. It is used in packet forwarding between the upstream and downstream boards. If the value is not 0, packets matching the entry are forwarded through the MPLS tunnel. If the value is 0, packets matching the entry are not forwarded through the MPLS tunnel.

9.10.7 display fib statistics

Function

The **display fib statistics** command displays the total number of IPv4 FIB entries.

Format

display fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] **statistics**

display fib statistics all

Parameters

Parameter	Description	Value
slot-id	Displays status information about a specified IPv4 FIB module.	The value is an integer and the value range depends on the device configuration.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Displays all FIB entries statistics.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display the total number of FIB entries on the LPU in slot 0.

```
<Huawei> display fib 0 statistics
Route Entry Count : 30
Route Prefix Count : 30
```

Display statistics about all FIB entries on the SRU.

```
<Huawei> display fib statistics all
IPv4 FIB Total Route Prefix Count : 24; Entry Count : 24

IPv4 FIB Public Route Prefix Count : 22; Entry Count : 22
```

Display the total number of FIB entries of the IPv4 VPN instance **vpna**.

```
<Huawei> display fib vpn-instance vpna statistics
Route Entry Count : 1
Route Prefix Count : 1
```

Table 9-207 Description of the **display fib statistics** command output

Item	Description
Route Entry Count	Total number of FIB entries.
Route Prefix Count	Total number of route prefix entries.
IPv4 FIB Total Route Prefix Count: Entry Count:	Numbers of route prefix entries and FIB entries.
IPv4 FIB Public Route Prefix Count: Entry Count:	Numbers of IP route prefix entries and FIB entries on a public network.

9.10.8 display ip routing-table

Function

The **display ip routing-table** command displays information about an IPv4 routing table.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name*] [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address* [*mask* | *mask-length*] [**longer-match**] [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address* { *mask* | *mask-length* } **nexthop** *nexthop-address* [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] *ip-address1* { *mask1* | *mask-length1* } *ip-address2* { *mask2* | *mask-length2* } [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] **acl** { *acl-number* | *acl-name* } [**verbose**]

display ip routing-table [**vpn-instance** *vpn-instance-name*] **ip-prefix** *ip-prefix-name* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of an VPN instance of an enabled IPv4 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about active routes and inactive routes. If this keyword is not specified, only brief information about active routes is displayed.	-
ip-address	Displays the routes with the specified destination address.	The value is in dotted decimal notation.
nexthop *nexthop-address*	Displays the routes with the specified next-hop address.	The value is in dotted decimal notation.
longer-match	Displays the routes with the specified destination address and mask.	-
mask	Specifies the mask of the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address.	The value is an integer that ranges from 0 to 32.
ip-address1	Specifies the start IP address in an IP address range. *ip-address1* and *ip-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is in dotted decimal notation.
ip-address2	Specifies the end IP address in an IP address range. *ip-address1* and *ip-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is in dotted decimal notation.
mask1	Specifies the subnet mask of the start IP address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mask-length1	Specifies the mask length of the start IP address.	The value is an integer that ranges from 0 to 32.
mask2	Specifies the subnet mask of the end IP address.	The value is in dotted decimal notation.
mask-length2	Specifies the mask length of the end IP address.	The value is an integer that ranges from 0 to 32.
acl *acl-number*	Displays the routes that match the ACL with the specified ACL number. If the specified ACL does not exist, information about all active routes is displayed.	The value is an integer that ranges from 2000 to 2999.
acl *acl-name*	Displays the routes that match the ACL with the specified ACL name. If the specified ACL does not exist, information about all active routes is displayed.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Displays the routes that match the specified IP prefix list. If the specified IP prefix list does not exist, information about all active routes is displayed.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the **verbose** keyword is not specified in the **display ip routing-table** command, each line in the command output indicates a route, including the destination address, mask length, protocol, preference, cost, flag, next hop, and outbound interface of the route.

NOTE

An iterated route is counted as one route regardless of how many outbound interfaces and next hops the route finds.

Matching rules vary with parameters in the command:

- If the **display ip routing-table** *ip-address* command is used, the routes that longest match the destination address are displayed.

- If the **display ip routing-table** *ip-address mask* command is used, the routes that accurately match the destination address and mask are displayed.
- If the **display ip routing-table** *ip-address* **longer-match** command is used, all the routes that match the IP address specified by the destination address and the natural mask are displayed.
- If the **display ip routing-table** *ip-address mask* **longer-match** command is used, all the routes that match the IP address specified by the destination address and the input mask are displayed.
- If the **display ip routing-table** *ip-address1 mask1 ip-address2 mask2* command is used, the routes whose destination address ranges from *ip-address1 mask1* to *ip-address2 mask2* are displayed.

Example

Display brief information about the current IPv4 routing table. The command output shows that there are two static routes with the same destination address 10.1.1.1/32 but different next hops.

```
<Huawei> display ip routing-table
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 9

  Destination/Mask  Proto  Pre  Cost  Flags   NextHop    Interface

       10.1.1.1/32   Static  60      0      D    0.0.0.0     NULL0
                     Static  60      0      D    192.168.0.2  GigabitEthernet1/0/0
     192.168.0.0/24   Direct   0      0      D    192.168.0.1  GigabitEthernet1/0/0
     192.168.0.1/32   Direct   0      0      D    127.0.0.1  GigabitEthernet1/0/0
   192.168.0.255/32   Direct   0      0      D    127.0.0.1  GigabitEthernet1/0/0
     127.0.0.0/8      Direct   0      0      D    127.0.0.1  InLoopBack0
     127.0.0.1/32     Direct   0      0      D    127.0.0.1  InLoopBack0
127.255.255.255/32    Direct   0      0      D    127.0.0.1  InLoopBack0
255.255.255.255/32    Direct   0      0      D    127.0.0.1  InLoopBack0
```

Table 9-208 Description of the display ip routing-table command output

Item	Description
Route Flags	Flag of a route: ● R: indicates that the route is an iterated route. ● D: indicates that the route is delivered to the FIB table.
Routing Table: Public	The routing table is a public routing table. If the routing table is a private routing table, a private network name is displayed, for example, Routing Tables: ABC.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.

Item	Description
Destination/Mask	Address and mask length of the destination network or host.
Proto	Routing protocol that learns a route.
Pre	Preference of a route.
Cost	Cost of a route.
Flags	Route flags in the heading of the routing table.
NextHop	Next-hop address of a route.
Interface	Outbound interface through which the next hop of a route is reachable.

Display the summary of the routing table of the IPv4 VPN instance named **vpn1**.

```
<Huawei> display ip routing-table vpn-instance vpn1
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table: vpn1
         Destinations : 5        Routes : 5

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

       10.1.1.0/24  Direct 0    0           D  10.1.1.1         Vlanif10
       10.1.1.1/32  Direct 0    0           D  127.0.0.1        Vlanif10
     10.1.1.255/32  Direct 0    0           D  127.0.0.1        Vlanif10
       10.5.5.0/24  Static 60   0          RD  10.1.1.2         Vlanif10
255.255.255.255/32  Direct 0    0           D  127.0.0.1        InLoopBack0
```

Table 9-209 Description of the display ip routing-table vpn-instance command output

Item	Description
Route Flags	Route flag: ● R: indicates an iterated route. ● D: indicates that the route is downloaded to the FIB table.
Routing Table: vpn1	VPN routing table named vpn1.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Routing protocol.

Item	Description
Pre	Preference.
Cost	Route cost.
Flags	Route flag, that is, Route Flags in the heading of the routing table.
NextHop	Next hop.
Interface	Outbound interface through which the next hop is reachable.

Display brief information about the current routing table. Route 2.2.2.2/32 is a static route with next hop 1.1.1.1. This route is an iterated route and has two outbound interfaces because 1.1.1.1 has two outbound interfaces.

```
<Huawei> display ip routing-table
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 9        Routes : 11

  Destination/Mask  Proto   Pre  Cost Flags NextHop    Interface

       1.1.1.1/32   Static  60   0       D    0.0.0.0     NULL0
                    Static  60   0       D    100.0.0.2   GigabitEthernet1/0/0
       2.2.2.2/32   Static  60   0      RD    1.1.1.1     NULL0
                    Static  60   0      RD    1.1.1.1     GigabitEthernet1/0/0
     100.0.0.0/24   Direct   0   0       D    100.0.0.1   GigabitEthernet1/0/0
     100.0.0.1/32   Direct   0   0       D    127.0.0.1   GigabitEthernet1/0/0
   100.0.0.255/32   Direct   0   0       D    127.0.0.1   GigabitEthernet1/0/0
     127.0.0.0/8    Direct   0   0       D    127.0.0.1   InLoopBack0
     127.0.0.1/32   Direct   0   0       D    127.0.0.1   InLoopBack0
127.255.255.255/32  Direct   0   0       D    127.0.0.1   InLoopBack0
255.255.255.255/32  Direct   0   0       D    127.0.0.1   InLoopBack0
```

Display detailed information about the IPv4 routing table.

```
<Huawei> display ip routing-table verbose
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 8        Routes : 8


Destination: 10.0.0.36/32
     Protocol: Direct            Process ID: 0
   Preference: 0                      Cost: 0
      NextHop: 127.0.0.1          Neighbour: 0.0.0.0
        State: Active Adv               Age: 01h03m56s
          Tag: 0                  Priority: high
        Label: NULL                 QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0            Interface: InLoopBack0
     TunnelID: 0x0                    Flags:  D

Destination: 10.10.36.0/24
     Protocol: Direct            Process ID: 0
   Preference: 0                      Cost: 0
      NextHop: 10.10.36.2         Neighbour: 0.0.0.0
```

```
      State: Active Adv            Age: 00h26m36s
        Tag: 0                Priority: high
      Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0        Interface: GigabitEthernet1/0/0
    TunnelID: 0x0             Flags:  D

Destination: 10.10.36.2/32
    Protocol: Direct          Process ID: 0
  Preference: 0               Cost: 0
     NextHop: 127.0.0.1       Neighbour: 0.0.0.0
      State: Active Adv            Age: 00h26m46s
        Tag: 0                Priority: high
      Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0        Interface: GigabitEthernet1/0/0
    TunnelID: 0x0             Flags:  D

Destination: 10.10.36.255/32
    Protocol: Direct          Process ID: 0
  Preference: 0               Cost: 0
     NextHop: 127.0.0.1       Neighbour: 0.0.0.0
      State: Active Adv            Age: 00h26m46s
        Tag: 0                Priority: high
      Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0        Interface: GigabitEthernet1/0/0
    TunnelID: 0x0             Flags:  D

Destination: 127.0.0.0/8
    Protocol: Direct          Process ID: 0
  Preference: 0               Cost: 0
     NextHop: 127.0.0.1       Neighbour: 0.0.0.0
      State: Active NoAdv          Age: 3d01h20m39s
        Tag: 0                Priority: high
      Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0        Interface: InLoopBack0
    TunnelID: 0x0             Flags:  D

Destination: 127.0.0.1/32
    Protocol: Direct          Process ID: 0
  Preference: 0               Cost: 0
     NextHop: 127.0.0.1       Neighbour: 0.0.0.0
      State: Active NoAdv          Age: 3d01h20m39s
        Tag: 0                Priority: high
      Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0        Interface: InLoopBack0
    TunnelID: 0x0             Flags:  D

Destination: 127.255.255.255/32
    Protocol: Direct          Process ID: 0
  Preference: 0               Cost: 0
     NextHop: 127.0.0.1       Neighbour: 0.0.0.0
      State: Active NoAdv          Age: 3d01h20m46s
        Tag: 0                Priority: high
      Label: NULL             QoSInfo: 0x0
  IndirectID: 0x0
 RelayNextHop: 0.0.0.0        Interface: InLoopBack0
    TunnelID: 0x0             Flags:  D

Destination: 255.255.255.255/32
    Protocol: Direct          Process ID: 0
  Preference: 0               Cost: 0
     NextHop: 127.0.0.1       Neighbour: 0.0.0.0
      State: Active NoAdv          Age: 3d01h20m54s
        Tag: 0                Priority: high
      Label: NULL             QoSInfo: 0x0
```

```
  IndirectID: 0x0
RelayNextHop: 0.0.0.0          Interface: InLoopBack0
   TunnelID: 0x0               Flags:  D
```

Table 9-210 Description of the display ip routing-table verbose command output

Item	Description
Route Flags	Flag of a route: ● R: indicates that the route is an iterated route. ● D: indicates that the route is delivered to the FIB table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of active routes and inactive routes.
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol of a route.
Process ID	Routing protocol process ID of a route.
Preference	Preference of a route.
Cost	Cost of a route.
NextHop	Next-hop address of a route.
Neighbour	Neighbor address of a route.
State	Status of a route: ● Active: active route ● Invalid: invalid route ● Inactive: inactive route ● NoAdv: route that cannot be advertised ● Adv: route that can be advertised ● Del: route to be deleted ● Relied: route iterated to an outbound interface and a next hop or route iterated to a tunnel ● Stale: route that is marked Stale and used in GR
Age	Lifetime of a route.
Tag	Routing management tag. The value is an integer that ranges from 0 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Priority	Convergence priority of route: ● low ● medium ● high ● critical
Label	VPN label.
QoSInfo	QoS information. The value 0x0 indicates that QoS information is empty.
IndirectID	ID of indirect next hop.
RelayNextHop	Iterated next-hop address.
Interface	Outbound interface.
TunnelID	Tunnel ID.
Flags	Route flags in the heading of the routing table.

9.10.9 display ip routing-table limit

Function

The **display ip routing-table limit** command displays the maximum number of routes and prefixes.

Format

display ip routing-table limit [**all-vpn-instance** | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all IPv4 VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a IPv4 VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays limits on the number of IPv4 routes and prefixes.

- The **display ip routing-table limit** command displays limits on the number of IPv4 public routes and prefixes.
- The **display ip routing-table limit all-vpn-instance** command displays the limit on the number of routes and prefixes of all IPv4 VPN instances.
- The **display ip routing-table limit vpn-instance** *vpn-instance-name* command displays the limit on the number of routes and prefixes of a specified IPv4 VPN instance.

Example

Display the limits on the number of IPv4 public routes and prefixes.

```
<Huawei> display ip routing-table limit
Public Instance:
Limit-Object Limit-Type     Upper-Limit  Warning    Current    Log-Interval
Route        Default        -            -          32         5
Prefix       Default        -            -          31         5
```

Display limits on the numbers of routes and prefixes of all IPv4 VPN instances.

```
<Huawei> display ip routing-table limit all-vpn-instance
Limit-Object     Limit-Type    Upper-Limit     Warning     Current    Log-Interval
-------------------------------------------------------------------------------
VPN Instance Name: vpn1
Route            Simply-Alert   5000           -           4223       5
Prefix           Alert-Percent  1000           800         760        5
-------------------------------------------------------------------------------
VPN Instance Name: vpn2
Route            Alert-Percent  2000           1000        823        5
Prefix           Default        -              -           760        5
```

Display limits on the numbers of routes and prefixes of the IPv4 VPN instance named **vpn1**.

```
<Huawei> display ip routing-table limit vpn-instance vpn1
VPN Instance Name: vpn1
Limit-Object     Limit-Type     Upper-Limit    Warning    Current    Log-Interval
Route            Simply-Alert   5000           -          4223       5
Prefix           Alert-Percent  1000           800        760        5
```

Table 9-211 Description of the display ip routing-table limit command output

Item	Description
Limit-Object	Object whose total number is limited: ● Prefix ● Route

Item	Description
Limit-Type	Limit type for the routes and prefixes in the routing table: ● Simply-Alert: indicates that only alarms are generated when the number of routes or prefixes exceeds the upper limit. ● Alert-Percent: indicates the percentage of the alarm threshold of routes. ● Default: indicates that the number of routes or prefixes is not limited by default.
Upper-Limit	Upper limit of routes or prefixes in the current routing table.
Warning	Alarm threshold of routes or prefixes in the current routing table.
Current	Number of routes or prefixes in the current routing table.
Log-Interval	Frequency of displaying logs when the number of routes or prefixes in the current routing table exceeds the upper limit, in seconds. The default value is 5s. The value is set by using the **limit-log-interval** command.

9.10.10 display ip routing-table protocol

Function

The **display ip routing-table protocol** command displays routing information about a specified routing protocol.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of an VPN instance of an enabled IPv4 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Displays routing information about the specified routing protocol: ● **direct**: displays direct routes. ● **static**: displays static routes. ● **bgp**: displays BGP routes. ● **isis**: displays IS-IS routes. ● **ospf**: displays OSPF routes. ● **rip**: displays RIP routes. ● **unr**: displays user network routes.	-
inactive	Displays brief information about inactive routes only.	-
verbose	Displays detailed information about active routes and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If neither **verbose** nor **inactive** is specified, brief information about all the routes of each routing protocol is displayed.

Example

Display brief information about all direct routes.

```
<Huawei> display ip routing-table protocol direct
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Public routing table : Direct
         Destinations : 7        Routes : 7

Direct routing table status : <Active>
```

```
        Destinations : 7        Routes : 7

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

   10.137.216.0/23  Direct  0    0           D   10.137.217.210  GigabitEthernet1/0/0
 10.137.217.210/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
 10.137.217.255/32  Direct  0    0           D   127.0.0.1       GigabitEthernet1/0/0
      127.0.0.0/8   Direct  0    0           D   127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct  0    0           D   127.0.0.1       InLoopBack0
127.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0
255.255.255.255/32  Direct  0    0           D   127.0.0.1       InLoopBack0

Direct routing table status : <Inactive>
        Destinations : 0        Routes : 0
```

Table 9-212 Description of the display ip routing-table protocol command output

Item	Description
Route Flags	Flag of a route: ● R: indicates that the route is an iterated route. ● D: indicates that the route is delivered to the FIB table.
Public routing table	Contents of a public routing table.
Direct routing table status	Status of direct routes: ● **Inactive**: inactive routes in the routing table ● **Active**: active routes in the routing table
Destinations	Total number of destination addresses.
Routes	Total number of routes in the routing table.
Destination/Mask	Destination address or mask length.
Proto	Routing protocol of a route.
Pre	Routing protocol preference of a route.
Cost	Cost of a route.
Flags	Route flags in the heading of the routing table.
Nexthop	Next-hop address of a route.
Interface	Outbound interface of a route.

Display detailed information about all OSPF routes.

```
<Huawei> display ip routing-table protocol ospf verbose
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
        Destinations : 3        Routes : 3
```

```
Destination: 1.1.1.1/32
     Protocol: OSPF            Process ID: 1
   Preference: 10                   Cost: 1
      NextHop: 10.11.1.1        Neighbour: 0.0.0.0
        State: Active Adv            Age: 21h23m44s
          Tag: 0                Priority: medium
        Label: NULL               QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0          Interface: GigabitEthernet1/0/0
     TunnelID: 0x0                  Flags:  D

Destination: 30.1.1.1/32
     Protocol: OSPF            Process ID: 1
   Preference: 10                   Cost: 1
      NextHop: 10.11.1.1        Neighbour: 0.0.0.0
        State: Active Adv            Age: 21h23m44s
          Tag: 0                Priority: medium
        Label: NULL               QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0          Interface: GigabitEthernet1/0/0
     TunnelID: 0x0                  Flags:  D

Destination: 40.1.1.1/32
     Protocol: OSPF            Process ID: 1
   Preference: 10                   Cost: 1
      NextHop: 10.11.1.1        Neighbour: 0.0.0.0
        State: Active Adv            Age: 21h23m44s
          Tag: 0                Priority: medium
        Label: NULL               QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0          Interface: GigabitEthernet1/0/0
     TunnelID: 0x0                  Flags:  D
```

Table 9-213 Description of the display ip routing-table protocol verbose command output

Item	Description
Routing Tables: Public	The routing table is a public routing table.
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol of a route.
Process ID	Routing protocol process ID of a route.
Preference	Routing protocol preference of a route.
Cost	Cost of a route.
NextHop	Next-hop address of a route.
Neighbour	Neighbor address of a route.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of a route: ● Active: active route ● Invalid: invalid route ● Inactive: inactive route ● NoAdv: route that cannot be advertised ● Adv: route that can be advertised ● Del: route to be deleted ● Relied: route iterated to an outbound interface and a next hop or route iterated to a tunnel ● Stale: route that is marked Stale and used in GR
Age	Lifetime of a route.
Tag	Routing management tag. The value is an integer that ranges from 0 to 4294967295.
Priority	Convergence priority of route: ● low ● medium ● high ● critical
Label	Label allocated by MPLS.
QoSInfo	QoS information. The value 0x0 indicates that QoS information is empty.
IndirectID	ID of indirect next hop.
RelayNextHop	Iterated next-hop address.
Interface	Outbound interface.
TunnelID	Tunnel ID.
Flags	Route flags in the heading of the routing table.

Display all the direct routes of the VPN instance named **vpn1**.

```
<Huawei> display ip routing-table vpn-instance vpn1 protocol direct
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
vpn4 routing table : Direct
         Destinations : 4          Routes : 4

Direct routing table status : <Active>
         Destinations : 4          Routes : 4
```

```
Destination/Mask    Proto  Pre  Cost     Flags NextHop         Interface

        1.1.1.0/24  Direct 0    0           D  1.1.1.1         Vlanif30
        1.1.1.1/32  Direct 0    0           D  127.0.0.1       Vlanif30
      1.1.1.255/32  Direct 0    0           D  127.0.0.1       Vlanif30
255.255.255.255/32  Direct 0    0           D  127.0.0.1       InLoopBack0
Direct routing table status : <Inactive>
         Destinations : 0          Routes : 0
```

Table 9-214 Description of the display ip routing-table vpn-instance protocol command output

Item	Description
Active	Active routes.
Inactive	Inactive routes.

9.10.11 display ip routing-table statistics

Function

The **display ip routing-table statistics** command displays statistics about routes in an IPv4 routing table.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

display ip routing-table[**all-vpn-instance**] **statistics**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about routes in the routing table of a specified VPN instance. If neither **vpn-instance** *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-vpn-instance	Displays statistics about routes in the routing tables of all VPN instances. If neither **vpn-instance** *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include:

- Total number of routes that are added or deleted through routing protocols
- Number of active or inactive routes that are labeled for deletion but are not deleted

Example

Display statistics about routes in an IPv4 routing table.

```
<Huawei> display ip routing-table statistics
Summary Prefixes: 9
Proto   total   active  added     deleted    freed
        routes  routes  routes    routes     routes
DIRECT  6       6       42        36         36
STATIC  3       3       21        18         18
RIP     0       0       0         0          0
OSPF    0       0       0         0          0
IS-IS   0       0       0         0          0
BGP     0       0       0         0          0
UNR     0       0       0         0          0
Total   9       9       63        54         54
```

Table 9-215 Description of the display ip routing-table statistics command output

Item	Description
Summary Prefixes	Total number of prefixes in the current routing table.
Proto	Routing protocol type
total routes	Total number of routes that a routing protocol learns in the routing table, including active and inactive routes.
active routes	Number of active routes that a routing protocol learns in the routing table.
added routes	Number of active and inactive routes that are added to the routing table through a routing protocol.
deleted routes	Number of routes to be deleted from the routing table.
freed routes	Number of routes that are permanently deleted from the routing table.

 Copyright © Huawei Technologies Co., Ltd.

Display statistics about routes in routing tables of all VPN instances.

```
<Huawei> display ip routing-table all-vpn-instance statistics
Summary prefixes: 9
Proto   total   active  added     deleted    freed
        routes  routes  routes    routes     routes
DIRECT  6       6       42        36         36
STATIC  3       3       21        18         18
RIP     0       0       0         0          0
OSPF    0       0       0         0          0
IS-IS   0       0       0         0          0
BGP     0       0       0         0          0
UNR     0       0       0         0          0
Total   9       9       63        54         54
```

9.10.12 display ip routing-table time-range

Function

The **display ip routing-table time-range** command displays information about routes generated in a specified time range in an IP routing table.

Format

display ip routing-table [**vpn-instance** *vpn-instance-name*] **time-range** *min-age max-age* [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about routes generated in a specified time range in the IP routing table of the specified VPN instance. If you do not specify this parameter, the **display ip routing-table time-range** command displays information about routes generated in a specified time range in the public IP routing table.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
min-age	Specifies the end time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. ● d indicates days. The value is an integer that ranges from 0 to 10000. ● h indicates hours. The value is an integer that ranges from 0 to 23. ● m indicates minutes. The value is an integer that ranges from 0 to 59. ● s indicates seconds. The value is an integer that ranges from 0 to 59. For example, you can enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.
max-age	Specifies the start time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. ● d indicates days. The value is an integer that ranges from 0 to 10000. ● h indicates hours. The value is an integer that ranges from 0 to 23. ● m indicates minutes. The value is an integer that ranges from 0 to 59. ● s indicates seconds. The value is an integer that ranges from 0 to 59. For example, you can enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.
verbose	Displays detailed information about active and inactive routes. If you do not specify this parameter, the **display ip routing-table time-range** command displays only brief information about active routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If route flapping occurs on a network, you can run the **display ip routing-table time-range** command and specify a small time range for the command. You can then find the flapping route rapidly and accelerate fault location.

Precautions

max-age must be larger than *min-age*. Otherwise, the **display ip routing-table time-range** command does not display any information.

If *max-age* is larger than *min-age* but no route was generated within this time range, the **display ip routing-table time-range** command displays only the table heading.

Example

Display information about public network routes generated in the last 20 minutes.

```
<Huawei> display ip routing-table time-range 0 20m
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 2        Routes : 2

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

       10.3.3.3/32  Direct  0    0           D   127.0.0.1       LoopBack1
       10.4.4.0/24  Static  60   0           D   0.0.0.0         NULL0
```

Table 9-216 Description of the display ip routing-table time-range command output

Item	Description
Route Flags	Route flags: ● R: The route is an iterated route. ● D: The route is sent to the FIB table.
Routing Tables: Public	The routing table is a public routing table.
Destinations	Number of destination networks and hosts.
Routes	Number of routes.
Destination/Mask	Address and mask length of the destination network and host.
Proto	Protocol used to learn routes.

Item	Description
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the heading of the routing table.
NextHop	Next hop.
Interface	Outbound interface in a route with a reachable next hop.

Display detailed information about public network routes generated in the last 20 minutes.

```
<Huawei> display ip routing-table time-range 0 20m verbose
Route Flags:
R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 3        Routes : 3


Destination: 10.3.3.3/32
     Protocol: Direct           Process ID: 0
   Preference: 0                      Cost: 0
      NextHop: 127.0.0.1         Neighbour: 0.0.0.0
        State: Active Adv              Age: 00h14m06s
          Tag: 0                 Priority: high
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: LoopBack1
     TunnelID: 0x0                   Flags:  D

Destination: 10.4.4.0/24
     Protocol: Static           Process ID: 0
   Preference: 60                     Cost: 0
      NextHop: 0.0.0.0           Neighbour: 0.0.0.0
        State: Active Adv              Age: 00h01m38s
          Tag: 0                 Priority: medium
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x0
 RelayNextHop: 0.0.0.0           Interface: NULL0
     TunnelID: 0x0                   Flags:  D

Destination: 10.4.4.4/32
     Protocol: Static           Process ID: 0
   Preference: 60                     Cost: 0
      NextHop: 10.4.4.0          Neighbour: 0.0.0.0
        State: Invalid Adv Relied      Age: 00h01m38s
          Tag: 0                 Priority: medium
        Label: NULL                QoSInfo: 0x0
   IndirectID: 0x80000002
 RelayNextHop: 0.0.0.0           Interface: NULL0
     TunnelID: 0x0                   Flags: R
```

 Copyright © Huawei Technologies Co., Ltd.

Table 9-217 Description of the display ip routing-table time-range verbose command output

Item	Description
Process ID	Process ID of the routing protocol.
Preference	Route preference.
Cost	Route cost.
NextHop	Next hop.
Neighbour	IP address of a neighbor. 0.0.0.0 indicates that the route is generated by a local device.
State	Route status: ● Active: an active route ● Invalid: an invalid route ● Inactive: an inactive route ● NoAdv: a route that cannot be advertised ● Adv: a route that can be advertised ● Del: a route to be deleted ● Relied: a route that is iterated to the next hop and outbound interface or a tunnel ● Stale: a route with the Stale flag and used in GR
Age	Time after the route is generated.
Tag	Administrative tag of the route. The value is an integer that ranges from 0 to 4294967295.
Priority	Convergence priority of the route: ● low: The convergence priority of a route is low. ● medium: The convergence priority of a route is medium. ● high: The convergence priority of a route is high. ● critical: The convergence priority of a route is critical.
Label	Label allocated by MPLS.
QoSInfo	QoS information. 0x0 indicates QoS information is empty.
IndirectID	ID of the indirect next hop.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RelayNextHop	Iterated next hop.
Interface	Iterated outbound interface.
Tunnel ID	Tunnel ID: ● The value 0x0 indicates that the route does not use a tunnel or the tunnel fails to be set up. ● If the value is not 0x0, the route is iterated to a tunnel.
Flags	Route flags in the heading of the routing table.

9.10.13 display ipv6 fib

Function

The **display ipv6 fib** command displays FIB entries on the device.

Format

display ipv6 fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] [*ipv6-address* [*prefix-length*]] [**verbose**]

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID of an LPU.	-
ipv6-address	Specifies the prefix of an IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Displays FIB entries of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer that ranges from 1 to 128.
verbose	Displays detailed information about FIB entries.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all FIB entries on the device.

```
<Huawei> display ipv6 fib
 IPv6 FIB Table:
 Total number of Routes : 4

Destination:  ::1                          PrefixLength : 128
Nexthop    :  ::1                          Flag         : HU
Interface  :  InLoopBack0                  Tunnel ID    : 0x0
TimeStamp  :  Date- 16:12:2010, Time- 15:1:54

Destination:  FE80::                       PrefixLength : 10
Nexthop    :  ::                           Flag         : BU
Interface  :  NULL0                        Tunnel ID    : 0
TimeStamp  :  Date- 16:12:2010, Time- 15:1:54

Destination:  2001::2                      PrefixLength : 128
NextHop    :  ::1                          Flag         : HU
Interface  :  InLoopBack0                  Tunnel ID    : 0x0
TimeStamp  :  Date- 16:12:2010, Time- 15:1:54

Destination:  2001::                       PrefixLength : 64
NextHop    :  2001::2                      Flag         : U
Interface  :  NULL0                        Tunnel ID    : 0
TimeStamp  :  Date- 16:12:2010, Time- 15:1:54
```

Table 9-218 Description of the display ipv6 fib command output

Item	Description
Destination	Destination IPv6 address of a route.
PrefixLength	Prefix length of the destination IPv6 address.
NextHop	Next hop that forwards packets to the destination address.
Flag	Description of route characteristics using S/U/G/H/B/D: ● S: static ● U: Up ● G: gateway ● H: host ● B. blackhole ● D: dynamic

Item	Description
Interface	Outbound interface through which packets are forwarded.
Tunnel ID	ID of the tunnel. If packets are forwarded to the next hop using MPLS forwarding, the tunnel ID of the packets cannot be 0. If packets are forwarded using IP forwarding, the tunnel ID of the packets is 0.
TimeStamp	Time taken to generate a route in the FIB table.

Display detailed information about FIB entries.

```
<Huawei> display ipv6 fib verbose
IPv6 FIB Table:
 Total number of Routes : 1

Destination:  ::1                          PrefixLength : 128
Nexthop    :  ::1                          Flag         : HU
Interface  :  InLoopBack0                      Tunnel ID    : 0x0
TimeStamp  :  Date- 13:5:2010, Time- 9:42:54       ATIndex      : 0x0
Slot       :  0                            InLabel      : NULL
IP6Token   :  0x0                            VlanId       : 0
RefCount   :  0                              BgpKey       : 0
NexthopBak :  ::                             IP6TokenBak  : 0x0
IfIndexBak :  [No Intf]                        Tunnel ID Bak: 0x0
BgpKeyBak  :  0                              InLabelBak   : NULL
TokenForLabelBak  :  0x0                       UnrType      : 0
NexthopForLabelBak:  ::
IfIndexForLabelBak:  [No Intf]                 OriginAs     : 0
BgpNexthop :  ::                             PeerAs       : 0
```

Table 9-219 Description of the display ipv6 fib verbose command output

Item	Description
Destination	Destination IPv6 address of a route.
PrefixLength	Prefix length of the destination IPv6 address.
Nexthop	Next-hop router that forwards packets to the destination address.
Flag	Description of route characteristics using S/U/G/H/B/D: ● S: static ● U: Up ● G: gateway ● H: host ● B. blackhole ● D: dynamic
Interface	Outbound interface through which packets are forwarded.

Item	Description
Tunnel ID	ID of the tunnel. If packets are forwarded to the next hop using MPLS forwarding, the tunnel ID of the packets cannot be 0. If packets are forwarded using IP forwarding, the tunnel ID of the packets is 0.
TimeStamp	Time taken to generate a route in the FIB table.
ATIndex	AT index.
Slot	Slot ID of the LPU where the outbound interface is located.
InLabel	Private network label.
IP6Token	Index of the ND entry allocated by the system for an adaptation module when the route is destined for a gateway. The value of this field is 0 when the route is not destined for a gateway.
VlanId	VLAN ID.
RefCount	Number of times a route is referenced.
BgpKey	Key value of a BGP route.
NexthopBak	Backup next hop.
IP6TokenBak	Backup ND token.
IfIndexBak	Backup outbound interface.
Tunnel ID Bak	Backup tunnel ID.
BgpKeyBak	Backup key value of the BGP route.
InLabelBak	Inner private network label.
TokenForLabelBak	Backup of the private network token.
UnrType	Route of the UNR type.
NexthopForLabelBak	Backup next hop for the private network token and route.
IfIndexForLabel-Bak	Backup outbound interface for the private network token and route.
OriginAs	Original AS number.
BgpNexthop	BGP next-hop address.
PeerAs	Peer AS number.

 Copyright © Huawei Technologies Co., Ltd.

9.10.14 display ipv6 fib statistics

Function

The **display ipv6 fib statistics** command displays IPv6 FIB statistics. The statistics include the LPU capacity and number of forwarding entries in each forwarding instance.

Format

display ipv6 fib [*slot-id*] **statistics** [**all**]

display ipv6 fib [*slot-id*] [**vpn-instance** *vpn-instance-name*] [**verbose**] **statistics**

Parameters

Parameter	Description	Value
slot-id	Displays statistics about IPv6 FIB entries on an LPU in a specified slot.	If this parameter is not specified, statistics about all IPv6 FIB entries on the MPU are displayed.
all	Displays all information.	-
vpn-instance *vpn-instance-name*	Displays FIB entries of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
verbose	Displays detailed information about FIB entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display ipv6 fib statistics** command:

- If the slot ID is specified, you can view the IPv6 FIB route prefix capacity on a specified LPU and the number of forwarding entries in each forwarding instance.
- If the slot ID is not specified, statistics about all IPv6 FIB entries on the MPU are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics about IPv6 FIB entries on the LPU in slot 2.

```
<Huawei> display ipv6 fib 2 statistics all
IPv6 FIB Total Route Prefix Count: 1 ; Entry Count : 1

IPv6 FIB Public Route Prefix Count :1 ; Entry Count : 1
```

Table 9-220 Description of the display ipv6 fib statistics all command output

Item	Description
IPv6 FIB Total Route Prefix Count : Entry Count :	Total number of IPv6 route prefix entries and total number of IPv6 forwarding entries.
IPv6 FIB Public Route Prefix Count : Entry Count :	Total number of IPv6 route prefix entries and total number of IPv6 public forwarding entries.

9.10.15 display ipv6 routing-table

Function

The **display ipv6 routing-table** command displays information about an IPv6 routing table.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address* [*prefix-length*] [**longer-match**] [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] *ipv6-address1* [*prefix-length1*] *ipv6-address2 prefix-length2* [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **acl** { *acl6-number* | *acl6-name* } [**verbose** | **brief**]

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **ipv6-prefix** *ipv6-prefix-name* [**verbose** | **brief**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance of an enabled IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
verbose	Displays detailed information about all the routes in the current routing table, including active and inactive routes.	-
brief	Displays brief information about active routes in the current routing table.	-
ipv6-address	Displays the routes with the specified IPv6 destination address.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 destination address.	The value is an integer that ranges from 0 to 128.
longer-match	Displays the routes with the specified destination address and mask.	-
ipv6-address1	Specifies the start IPv6 address in an IP address range. *ipv6-address1* and *ipv6-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
ipv6-address2	Specifies the end IPv6 address in an IP address range. *ipv6-address1* and *ipv6-address2* determine an IP address range. Only the routes in the IP address range are displayed.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length1	Specifies the mask length of the start IPv6 address.	The value is an integer that ranges from 0 to 128.
prefix-length2	Specifies the mask length of the end IPv6 address.	The value is an integer that ranges from 0 to 128.
acl *acl6-number*	Displays the routes that match the ACL6 with the specified ACL number. If the specified ACL6 does not exist, information about all active routes is displayed.	The value is an integer that ranges from 2000 to 2999.
acl *acl6-name*	Displays the routes that match the ACL6 with the specified ACL name. If the specified ACL6 does not exist, information about all active routes is displayed.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-prefix *ipv6-prefix-name*	Displays the routes that match the specified IPv6 prefix list. If the specified IPv6 prefix list does not exist, information about all active routes is displayed.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the **verbose** keyword is not specified, the command output includes the destination address, prefix length, protocol type, preference, cost, next hop, outbound interface, tunnel ID, flag, and status of a route.

NOTE

An iterated route is counted as one route regardless of how many outbound interfaces and next hops the route finds.

Example

Display brief information about the current IPv6 routing table.

```
<Huawei> display ipv6 routing-table
Routing Table : Public
         Destinations : 4        Routes : 4

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:112::               PrefixLength : 64
 NextHop      : FC00:0:0:112::2              Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    :GigabitEthernet1/0/0          Flags        : D

 Destination  : FC00:0:0:112::2              PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    :GigabitEthernet1/0/0          Flags        : D

 Destination  : FE80::                       PrefixLength : 10
 NextHop      : ::                           Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : D
```

 Copyright © Huawei Technologies Co., Ltd.

Table 9-221 Description of the display ipv6 routing-table command output

Item	Description
Routing Tables : Public	The routing table is a public routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination	IP address of the destination network or host of a route.
PrefixLength	Prefix length of a route.
NextHop	Next-hop IPv6 address of a route.
Preference	Preference of a route.
Cost	Cost of a route.
Protocol	Routing protocol of a route.
RelayNextHop	Iterated next-hop address.
TunnelID	Tunnel ID. The value 0x0 indicates that no tunnel is used or the tunnel fails to be established.
Interface	Outbound interface through which the next hop of a route can be reached.
Flags	Flag of a route: ● R: The route is an iterated route. ● D: The route is delivered to the FIB table.

Display detailed information about the IPv6 routing table.

```
<Huawei> display ipv6 routing-table verbose
Routing Table : Public
         Destinations : 2        Routes : 2

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Direct
 State        : Active NoAdv                 Cost         : 0
 Entry ID     : 1                            EntryFlags   : 0x80010050
 Reference Cnt: 1                            Tag          : 0
 Priority     : high                         Age          : 84410sec
 IndirectID   : 0x0
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : FC00:0:0:2::2                Preference   : 60
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Static
 State        : Active Adv Relied            Cost         : 0
```

```
Entry ID     : 2                    EntryFlags   : 0x80020140
Reference Cnt: 1                       Tag          : 0
Priority     : high                 Age          : 79036sec
IndirectID   : 0x80000001
RelayNextHop : ::                      TunnelID     : 0x0
Interface    : NULL0                   Flags        : RD
```

Table 9-222 Description of the display ipv6 routing-table verbose command output

Item	Description
Neighbour	IPv6 address of a neighbor interface.
ProcessID	Routing protocol process ID of a route.
Label	Label carried in a route.
State	Status of a route: ● Active: active route ● Invalid: invalid route ● Inactive: inactive route ● NoAdv: route that cannot be advertised ● Adv: route that can be advertised ● Del: route to be deleted ● Relied: route iterated to an outbound interface and a next hop or route iterated to a tunnel ● Stale: route that is marked Stale and used in GR
Entry ID	ID of a routing entry in the routing table.
EntryFlags	Flag of a routing entry.
Reference Cnt	Number of times a route is referenced.
Tag	Routing management tag. The value is an integer that ranges from 0 to 4294967295.
Priority	Convergence priority of a route: ● low ● medium ● high ● critical
IndirectID	ID of indirect next hop.
Age	Time a route is generated.

Display brief information about the routes with the specified IPv6 destination address.

```
<Huawei> display ipv6 routing-table 111::1 64
Routing Table :Public
Summary Count : 1

 Destination  : FC00:0:0:111::          PrefixLength : 64
 NextHop      : FC00:0:0:111::2         Preference   : 0
 Cost         : 0                       Protocol     : Direct
 RelayNextHop : ::                      TunnelID     : 0x0
 Interface    : GigabitEthernet1/0/0    Flags        : D
```

Display the routes within the specified IPv6 address range.

```
<Huawei> display ipv6 routing-table 111::1 64 111::2 128
Routing Table :
Summary Count : 2

 Destination  : FC00:0:0:111::          PrefixLength : 64
 NextHop      : FC00:0:0:111::2         Preference   : 0
 Cost         : 0                       Protocol     : Direct
 RelayNextHop : ::                      TunnelID     : 0x0
 Interface    : GigabitEthernet1/0/0    Flags        : D

 Destination  : FC00:0:0:111::2         PrefixLength : 128
 NextHop      : ::1                     Preference   : 0
 Cost         : 0                       Protocol     : Direct
 RelayNextHop : ::                      TunnelID     : 0x0
 Interface    : GigabitEthernet1/0/0    Flags        : D
```

Display brief information about the active routes that match IPv6 prefix list **abc2**.

```
<Huawei> display ipv6 routing-table ipv6-prefix abc2
Routes Matched by Prefix-list : abc2
Summary Count: 3

 Destination  : ::1                     PrefixLength : 128
 NextHop      : ::1                     Preference   : 0
 Cost         : 0                       Protocol     : Direct
 RelayNextHop : ::                      TunnelID     : 0x0
 Interface    : InLoopBack0             Flags        : D

 Destination  : FC00:0:0:112::          PrefixLength : 64
 NextHop      : FC00:0:0:112::1         Preference   : 0
 Cost         : 0                       Protocol     : Direct
 RelayNextHop : ::                      TunnelID     : 0x0
 Interface    : Ethernet3/0/0           Flags        : D

 Destination  : FC00:0:0:112::1         PrefixLength : 128
 NextHop      : ::1                     Preference   : 0
 Cost         : 0                       Protocol     : Direct
 RelayNextHop : ::                      TunnelID     : 0x0
 Interface    : GigabitEthernet1/0/0    Flags        : D
```

9.10.16 display ipv6 routing-table limit

Function

The **display ipv6 routing-table limit** command displays limits on the numbers of routes and prefixes.

Format

display ipv6 routing-table limit [**all-vpn-instance** | **vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all IPv6 VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command displays limits on the number of IPv6 routes and prefixes.

- The **display ipv6 routing-table limit** command displays limits on the number of IPv6 public routes and prefixes.
- The **display ipv6 routing-table limit all-vpn-instance** command displays the limit on the number of routes and prefixes of all IPv6 VPN instances.
- The **display ipv6 routing-table limit vpn-instance** *vpn-instance-name* command displays the limit on the number of routes and prefixes of a specified IPv6 VPN instance.

Example

Display limits on the numbers of routes and prefixes of all IPv6 VPN instances.

```
<Huawei> display ipv6 routing-table limit all-vpn-instance

Limit-Object     Limit-Type    Upper-Limit     Warning     Current    Log-Interval
--------------------------------------------------------------------------------
IPv6 VPN Instance Name: VPN1
Route            Simply-Alert   5000           -           4223       5
Prefix           Alert-Percent  1000           800         760        5
--------------------------------------------------------------------------------
IPv6 VPN Instance Name: VPN2
Route            Alert-Percent  2000           1000        823        5
Prefix           Default        -              -           760        5
```

Display limits on the numbers of routes and prefixes of the IPv6 VPN instance named **vpn1**.

```
<Huawei> display ipv6 routing-table limit vpn-instance vpn1
IPv6 VPN Instance Name: vpn1
Limit-Object     Limit-Type     Upper-Limit    Warning    Current    Log-Interval
Route            Simply-Alert    5000          -          4223       5
Prefix           Alert-Percent   1000          800        760        5
```

 Copyright © Huawei Technologies Co., Ltd.

Display the limits on the number of IPv6 public routes and prefixes.

```
<Huawei> display ipv6 routing-table limit
Public Instance:
Limit-Object Limit-Type     Upper-Limit  Warning    Current    Log-Interval
Route        Default        -            -          1          5
Prefix       Default        -            -          1          5
```

Table 9-223 Description of the **display ipv6 routing-table limit** command output

Item	Description
Limit-Object	Indicates the object whose total number is limited: ● Prefix ● Route
Limit-Type	Indicates the limit mode for the routes and prefixes in the current routing table: ● Simply-Alert: indicates that only alarms are generated after the number of routes or prefixes exceeds the upper limit. ● Alert-Percent: indicates the percentage of the alarm threshold of routes. ● Default: indicates that the number of routes or prefixes is not limited by default.
Upper-Limit	Indicates the upper limit of routes or prefixes in the current routing table.
Warning	Indicates the alarm threshold of routes or prefixes in the current routing table.
Current	Indicates the number of routes or prefixes in the current routing table.
Log-Interval	Indicates the frequency of displaying logs when the number of routes or prefixes in the current routing table exceeds the upper limit, in seconds.

Related Topics

12.9.51 routing-table limit

9.10.17 display ipv6 routing-table protocol

Function

The **display ipv6 routing-table protocol** command displays routing information about a specified IPv6 routing protocol.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **protocol** *protocol* [**inactive** | **verbose** | **brief**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance of an enabled IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
protocol	Displays routing information about the specified routing protocol: ● **direct**: displays direct IPv6 routes. ● **static**: displays static IPv6 routes. ● **bgp**: displays BGP4+ routes. ● **ripng**: displays RIPng routes. ● **isis**: displays IS-IS IPv6 routes. ● **ospfv3**: displays OSPFv3 routes. ● **unr**: displays user network routes.	-
inactive	Displays information about inactive routes. If this parameter is not specified, information about all active and inactive routes is displayed.	-
verbose	Displays detailed information about active and inactive routes. If this keyword is not specified, only brief information about active routes is displayed.	-
brief	Displays brief information about active and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display brief information about all IPv6 direct routes.

```
<Huawei> display ipv6 routing-table protocol direct
Public Routing Table : Direct
Summary Count : 2

Direct Routing Table's Status : < Active >
Summary Count : 2

 Destination  : ::1                    PrefixLength : 128
 NextHop      : ::1                    Preference   : 0
 Cost         : 0                      Protocol     : Direct
 RelayNextHop : ::                     TunnelID     : 0x0
 Interface    : InLoopBack0            Flags        : D

 Destination  : FE80::                 PrefixLength : 10
 NextHop      : ::                     Preference   : 0
 Cost         : 0                      Protocol     : Direct
 RelayNextHop : ::                     TunnelID     : 0x0
 Interface    : NULL0                  Flags        : D

Direct Routing Table's Status : < Inactive >
Summary Count : 0
```

Table 9-224 Description of the display ipv6 routing-table protocol command output

Item	Description
Public Routing Table	Contents of a public routing table: ● Direct: direct IPv6 route ● Static: static IPv6 route ● bgp: BGP4+ route ● ripng: RIPng route ● isis: IS-IS IPv6 route ● ospfv3: OSPFv3 route ● unr: user network route
Summary Count	Number of prefixes of routes.
Direct Routing Table's Status	Status of direct routes: ● active: information about active routes ● inactive: information about inactive routes
Destination	IP address of the destination network or host of a route.
PrefixLength	Prefix length of a route.
NextHop	Next-hop address of a route.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Preference	Routing protocol preference of a route.
Cost	Cost of a route.
Protocol	Routing protocol that learns a route.
RelayNextHop	Iterated next-hop address.
TunnelID	Tunnel ID. The value 0x0 indicates that no tunnel is used or the tunnel fails to be established.
Interface	Outbound interface through which the next hop of a route can be reached.
Flags	Flag of a route: ● R: The route is an iterated route. ● D: The route is delivered to the FIB table.

9.10.18 display ipv6 routing-table statistics

Function

The **display ipv6 routing-table statistics** command displays statistics about routes in an IPv6 routing table.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name* | **all-vpn-instance**] **statistics**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about routes in the routing table of a specified VPN instance. If neither *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all-vpn-instance	Displays statistics about routes in the routing tables of all VPN instances. If neither *vpn-instance-name* nor **all-vpn-instance** is specified, statistics about routes in a public routing table are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include the total number of routes, number of added routes, and number of deleted routes.

Example

Display statistics about routes in an IPv6 routing table.

```
<Huawei> display ipv6 routing-table statistics
Summary Prefixes: 1
Protocol    route       active      added       deleted     freed
DIRECT      1           1           1           0           0
STATIC      0           0           0           0           0
RIPng       0           0           0           0           0
OSPFv3      0           0           0           0           0
IS-IS       0           0           0           0           0
BGP         0           0           0           0           0
UNR         0           0           0           0           0
Total       1           1           1           0           0
```

Table 9-225 Description of the display ipv6 routing-table statistics command output

Item	Description
Summary Prefixes	Total number of prefixes in the current routing table.

Item	Description
Protocol	Routing protocol type: ● **direct**: direct IPv6 route ● **static**: static IPv6 route ● **bgp**: BGP4+ route ● **ripng**: RIPng route ● **isis**: IS-IS IPv6 route ● **ospfv3**: OSPFv3 route ● **unr**: user network route
route	Total number of routes that a routing protocol learns in the routing table, including active and inactive routes.
active	Number of active routes of a routing protocol in the routing table.
added	Number of active and inactive routes that are added to the routing table through a routing protocol.
deleted	Number of routes that are deleted from the routing table.
freed	Number of routes that are permanently deleted from the routing table.

9.10.19 display ipv6 routing-table time-range

Function

The **display ipv6 routing-table time-range** command displays information about routes generated in a specified time range in an IPv6 routing table.

Format

display ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **time-range** *min-age max-age* [**verbose** | **brief**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about routes generated in a specified time range in the IPv6 routing table of the specified VPN instance. If this parameter is not specified, the **display ipv6 routing-table time-range** command displays information about routes generated in a specified time range in the public IPv6 routing table.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
min-age	Specifies the end time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. ● d indicates days. The value is an integer that ranges from 0 to 10000. ● h indicates hours. The value is an integer that ranges from 0 to 23. ● m indicates minutes. The value is an integer that ranges from 0 to 59. ● s indicates seconds. The value is an integer that ranges from 0 to 59. For example, enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
max-age	Specifies the start time of the period when routes are generated.	The value is in xxdxxhxxmxxs format. ● d indicates days. The value is an integer that ranges from 0 to 10000. ● h indicates hours. The value is an integer that ranges from 0 to 23. ● m indicates minutes. The value is an integer that ranges from 0 to 59. ● s indicates seconds. The value is an integer that ranges from 0 to 59. For example, enter 5d4h30m20s to specify 5 days, 4 hours, 30 minutes, and 20 seconds. **NOTE** If the value of d is 10000, the values of h, m, and s can only be 0.
verbose	Displays detailed information about active and inactive routes. If this parameter is not specified, the **display ipv6 routing-table time-range** command displays only brief information about active routes.	-
brief	Displays brief information about active and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If route flapping occurs on a network, to find the flapping route rapidly and accelerate fault location, run the **display ipv6 routing-table time-range** command and specify a small time range.

Precautions

max-age must be larger than *min-age*. Otherwise, the **display ipv6 routing-table time-range** command does not display any information.

If *max-age* is larger than *min-age* but no route is generated within this time range, the **display ipv6 routing-table time-range** command displays only the table heading.

Example

Display information about public network IPv6 routes generated in the last 2 hours, 20 minutes, and 10 seconds.

```
<Router> display ipv6 routing-table time-range 0 2h20m10s
Routing Table : Public
         Destinations : 4        Routes : 4

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : LoopBack2                    Flags        : D

 Destination  : FC00:0:0:1::2                PrefixLength : 128
 NextHop      : ::                           Preference   : 60
 Cost         : 0                            Protocol     : Static
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : D

 Destination  : FE80::                       PrefixLength : 10
 NextHop      : ::                           Preference   : 0
 Cost         : 0                            Protocol     : Direct
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : D
```

Table 9-226 Description of the display ipv6 routing-table time-range command output

Item	Description
Routing Tables: Public	The routing table is a public routing table.
Destinations	Number of destination networks or hosts.
Routes	Number of routes.
Destination	IP addresses of the destination network or host.
PrefixLength	Prefix length of a route.
NextHop	Next-hop IPv6 address.
Preference	Route preference.
Cost	Route cost.
Protocol	Name of the routing protocol.
RelayNextHop	Iterated next hop.

Item	Description
TunnelID	Tunnel ID: ● The value 0x0 indicates that the route does not use a tunnel or the tunnel fails to be set up. ● If the value is not 0x0, the route is iterated to a tunnel.
Interface	Outbound interface through which the next hop of a route can be reached.
Flags	Route flag: ● R: The route is an iterated route. ● D: The route is delivered to the FIB table.

Display detailed information about public network routes generated in the last 20 minutes.

```
<Router> display ipv6 routing-table time-range 0 20m verbose
Routing Table : Public
         Destinations : 4        Routes : 5

 Destination  : ::1                          PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Direct
 State        : Active NoAdv                 Cost         : 0
 Entry ID     : 262551588                    EntryFlags   : 0x80010050
 Reference Cnt: 2                            Tag          : 0
 Priority     : high                         Age          : 7694sec
 IndirectID   : 0x0
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : InLoopBack0                  Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : ::1                          Preference   : 0
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Direct
 State        : Active Adv                   Cost         : 0
 Entry ID     : 262552100                    EntryFlags   : 0x80010040
 Reference Cnt: 2                            Tag          : 0
 Priority     : high                         Age          : 101sec
 IndirectID   : 0x0
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : LoopBack2                    Flags        : D

 Destination  : FC00:0:0:1::1                PrefixLength : 128
 NextHop      : FC00:0:0:1::2                Preference   : 60
 Neighbour    : ::                           ProcessID    : 0
 Label        : NULL                         Protocol     : Static
 State        : Inactive Adv Relied          Cost         : 0
 Entry ID     : 262551716                    EntryFlags   : 0x20140
 Reference Cnt: 2                            Tag          : 0
 Priority     : medium                       Age          : 7668sec
 IndirectID   : 0x80000001
 RelayNextHop : ::                           TunnelID     : 0x0
 Interface    : NULL0                        Flags        : R

 Destination  : FC00:0:0:1::2                PrefixLength : 128
 NextHop      : ::                           Preference   : 60
```

```
Neighbour    : ::                    ProcessID    : 0
Label        : NULL                  Protocol     : Static
State        : Active Adv            Cost         : 0
Entry ID     : 262551844             EntryFlags   : 0x80000040
Reference Cnt: 2                     Tag          : 0
Priority     : medium                Age          : 7670sec
IndirectID   : 0x0
RelayNextHop : ::                    TunnelID     : 0x0
Interface    : NULL0                 Flags        : D

Destination  : FE80::                PrefixLength : 10
NextHop      : ::                    Preference   : 0
Neighbour    : ::                    ProcessID    : 0
Label        : NULL                  Protocol     : Direct
State        : Active NoAdv          Cost         : 0
Entry ID     : 262551972             EntryFlags   : 0x80010010
Reference Cnt: 2                     Tag          : 0
Priority     : high                  Age          : 104sec
IndirectID   : 0x0
RelayNextHop : ::                    TunnelID     : 0x0
Interface    : NULL0                 Flags        : D
```

Table 9-227 Description of the display ipv6 routing-table time-range verbose command output

Item	Description
Neighbour	IP address of a neighboring interface. :: indicates that the route is generated by a local device.
ProcessID	Process ID of the routing protocol.
Label	Label carried in a route.
State	Status of the route: ● Active: an active route ● Invalid: an invalid route ● Inactive: an inactive route ● NoAdv: a route that cannot be advertised ● Adv: a route that can be advertised ● Del: a route to be deleted ● Relied: a route that is iterated to the next hop and outbound interface or a tunnel ● Stale: a route with the Stale flag and used in GR
Entry ID	ID of a route in the routing table.
EntryFlags	Flag of a route.
Reference Cnt	Number of times the route is referenced.

Item	Description
Tag	Administrative tag of the route. The value is an integer that ranges from 0 to 4294967295.
Priority	Convergence priority of the route: ● low ● medium ● high ● critical
IndirectID	ID of the indirect next hop.
Age	Time when the route is generated.

9.10.20 display rm bfd-session

Function

The **display rm bfd-session** command displays the BFD session configuration in routing management (RM).

Format

display rm bfd-session [**vpn-instance** *vpn-instance-name*] [**destination** *destination-address*] [**source** *source-address*] [**interface** *interface-type interface-number*] [**protocol** { **bgp** | **isis-l1** | **isis-l2** | **isis-l1l2** | **ospf** | **rip** | **pim** }]

display rm bfd-session all

Parameters

Parameter	Description	Value
all	Displays all the BFD session configurations in RM, including the BFD session configurations of the public and private networks. If **all** is not specified, only the BFD session configuration on the public network is displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the configurations of BFD sessions of the specified VPN instance in RM.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
destination *destination-address*	Displays the configurations of BFD sessions with the specified destination address in RM.	The value is in dotted decimal notation.
source *source-address*	Displays the configurations of BFD sessions with the specified source address in RM.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Displays the configurations of BFD sessions with the specified outbound interface type and number in RM.	-
protocol	Displays the configurations of BFD sessions of the specified routing protocol in RM: ● **bgp**: BGP ● **isis-l1**: IS-IS Level-1 ● **isis-l2**: IS-IS Level-2 ● **isis-l1l2**: IS-IS Level-1-2 ● **ospf**: OSPF ● **rip**: RIP ● **pim**: PIM	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view the configuration of BFD sessions dynamically created by routing protocols. The command output includes the global BFD status, number of BFD sessions, and BFD session configuration, such as VPN instance, destination address, source address, interface, and status.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the BFD configuration in RM.

```
<Huawei> display rm bfd-session
BFD Global Status: ON
BFD Session Total Number: 1

BFD Session: 1
  Interface: GigabitEthernet 1/0/0
  Destination     Source          Session-State Create-State
  10.8.1.2        10.8.1.1        Up           Established
  Route-Protocol  Rx-Interval(ms) Tx-Interval(ms) Multiplier
  ISIS_Level2     1000            1000           5
```

Table 9-228 Description of the display rm bfd-session command output

Item	Description
BFD Global Status	Global BFD status: • ON: BFD is enabled globally. • OFF: BFD is disabled globally. To set the global BFD status, run the **18.5.2 bfd** command.
BFD Session Total Number	Total number of BFD sessions.
BFD Session	Number of the BFD session.
Interface	Local physical interface bound to the BFD session.
Destination	Peer IP address bound to the BFD session.
Source	Source IP address bound to the BFD session.
Session-State	Status of the BFD session: • AdminDown: indicates that the BFD session is in AdminDown state when the **18.5.34 shutdown (BFD session view)** command is run. • Down: indicates that the BFD session in Down state. • Init: indicates that the BFD session is in Init state. • Up: indicates that the BFD session is in Up state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Create-State	BFD session setup status in RM: ● Creating: indicates that the routing protocol notifies RM of the session, but RM does not instruct BFD to set up a session. ● Established: indicates that RM notifies BFD to set up a BFD session. You can view the Session-State field to check whether a BFD session is set up.
Route-Protocol	Routing protocol enabled with BFD: ● BGP ● IS-IS Level-1 ● IS-IS Level-2 ● IS-IS Level-1-2 ● OSPF ● RIP ● PIM
Rx-Interval(ms)	Configured receiving interval, in milliseconds.
Tx-Interval(ms)	Configured sending interval, in milliseconds.
Multiplier	Configured local detection multiplier.

Related Topics

18.5.2 bfd
9.2.2 bfd all-interfaces (RIP)
9.6.7 bfd all-interfaces (IS-IS)
9.4.6 bfd all-interfaces (OSPF)
9.2.31 rip bfd
9.6.58 isis bfd
9.4.71 ospf bfd
9.8.103 peer bfd
10.3.47 pim bfd
18.5.34 shutdown (BFD session view)

 Copyright © Huawei Technologies Co., Ltd.

9.10.21 display rm interface

Function

The **display rm interface** command displays routing management (RM) information on an interface.

Format

display rm interface [*interface-type interface-number*]

display rm interface [**vpn-instance** *vpn-instance-name*] [**ip-address** *ip-address*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RM information on the specified interface.	-
vpn-instance *vpn-instance-name*	Displays RM information on the interface of the specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ip-address *ip-address*	Displays RM information on the interface with the specified destination address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IPv4 RM information on an interface, including information about physical and logical interfaces of the interface. This information helps locate routing problems.

Example

Display RM information on GE1/0/0.

```
<Huawei> display rm interface gigabitethernet 1/0/0
Name: GigabitEthernet1/0/0
Physical IF Info:
```

```
 IfnetIndex: 0x4
 State: UP BCA MULT OSI
 Hardware Address: 0819-A6D0-269C
 Slot: 0(Logic Slot: 1)
 IntType: 36, PriLog: 5, MTU: 1500, Reference Count 2
 Bandwidth: 0, 1000000000
 Baudrate: 0, 1000000000
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 17973sec
Logical IF Info:
 IfnetIndex: 0x4, PhyIndex: 4 Logical Index : 5,
 Dest: 30.1.1.2, Mask: 255.255.255.0
 State: UP PRM BCA MULT , Reference Count 1
 Age: 17977sec
```

Display RM information on interfaces.

```
<Huawei> display rm interface

Name: InLoopBack0
Physical IF Info:
 IfnetIndex: 0x1
 State: UP LOOP MULT
 Slot: 0(Logic Slot: 0)
 IntType: 26, PriLog: 1, MTU: 1500, Reference Count 4
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 470sec
Logical IF Info:
 IfnetIndex: 0x1, PhyIndex: 1 Logical Index : 1,
 Dest: 127.0.0.1, Mask: 255.0.0.0
 State: UP LOOP PRM MULT , Reference Count 3
 Age: 470sec

Name: NULL0
Physical IF Info:
 IfnetIndex: 0x2
 State: UP NBMA MULT
 Slot: 0(Logic Slot: 0)
 IntType: 27, PriLog: 2, MTU: 1500, Reference Count 1
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 470sec
Logical IF Info:
 IfnetIndex: 0x2, PhyIndex: 2 Logical Index : 2,
 Dest: 0.0.0.0, Mask: 255.255.255.255
 State: UP PRM NBMA MULT , Reference Count 0
 Age: 472sec

Name: Serial0/0/0
Physical IF Info:
 IfnetIndex: 0x4
 State: DOWN P2P MULT
 Slot: 0(Logic Slot: 0)
 IntType: 3, PriLog: 0, MTU: 1500, Reference Count 1
 Bandwidth: 0, 64000
 Baudrate: 0, 64000
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
```

```
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 472sec

Name: LoopBack1
Physical IF Info:
 IfnetIndex: 0xC
 State: UP LOOP P2P MULT
 Slot: 0(Logic Slot: 0)
 IntType: 26, PriLog: 3, MTU: 1500, Reference Count 1
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 39sec
Logical IF Info:
 IfnetIndex: 0xC, PhyIndex: 7 Logical Index : 3,
 Dest: 1.1.1.9, Mask: 255.255.255.255
 State: UP LOOP PRM P2P MULT , Reference Count 0
 Age: 32sec

Name: Tunnel0/0/1
Physical IF Info:
 IfnetIndex: 0xD
 State: DOWN P2P MULT
 Slot: 0(Logic Slot: 0)
 IntType: 32, PriLog: 0, MTU: 1500, Reference Count 1
 Bandwidth: 0, 64000
 Baudrate: 0, 64000
 Delay: 0, Reliability: 0, Load: 0
 LDP-ISIS sync capability: disabled
 LDP-OSPF sync capability: disabled
 InstanceID: 0, Instance Name: Public
 Age: 20sec
```

Table 9-229 Description of the display rm interface command output

Item	Description
Name	Name of the interface.
Physical IF Info	Physical interface information.
IfnetIndex	Network segment index of the interface.
State	Current interface status.
Hardware Address	MAC address of the interface.
Slot	Slot ID of the interface.
IntType	Type of the interface.
PriLog	Index of the primary logical interface.
MTU	Maximum transmission unit (MTU) of the interface.
Reference Count	Number of times the interface is referenced.
Bandwidth	Bandwidth of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Baudrate	Baud rate of the interface.
Delay	Link delay.
Reliability	Link reliability.
Load	Link load.
LDP-ISIS sync capability	Whether synchronization between LDP and IS-IS is enabled: ● enabled: indicates that synchronization is enabled. ● disabled: indicates that synchronization is disabled.
LDP-OSPF sync capability	Whether synchronization between LDP and OSPF is enabled: ● enabled: indicates that synchronization is enabled. ● disabled: indicates that synchronization is disabled.
InstanceID	Instance ID.
Instance Name	Instance name.
Logical IF Info	Logical interface information.
PhyIndex	Physical interface index.
Logical Index	Logical interface index.
Dest	Destination address.
Mask	Mask of the destination address.
Age	Lifetime of the displayed information.

9.10.22 display rm ipv6 interface

Function

The **display rm ipv6 interface** command displays IPv6 routing management (RM) information on an interface.

Format

display rm ipv6 interface [*interface-type interface-number*]

display rm ipv6 interface [**vpn-instance** *vpn-instance-name*] [**ipv6-address** *ipv6-address*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays IPv6 RM information on the specified interface.	-
vpn-instance *vpn-instance-name*	Displays IPv6 RM information in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv6-address *ipv6-address*	Displays IPv6 RM information with the specified destination IPv6 address.	The value is a 32-digit hexadecimal number, in the X:X:X:X:X:X:X:X format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view IPv6 RM information on an interface, including information about physical and logical interfaces of the interface. This information helps locate routing problems.

Example

Display IPv6 RM information on all interfaces.

```
<Huawei> display rm ipv6 interface

Name: InLoopBack0
Physical IF Info:
 IfnetIndex: 0x1
 State: UP LOOP MULT
 Slot: 0(Logic Slot: 0)
 IntType: 26, PriLog: 1, MTU: 1500, Ref: 1
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0
 Age: 1635sec

Logical IF Info:
 IfnetIndex: 0x1, PhyIndex: 1, LogiIndex: 1
 Dest: ::1, Mask: 128
 State: UP LOOP PRM MULT , Ref 1
 Age: 1635sec

Name: NULL0
Physical IF Info:
```

```
 IfnetIndex: 0x2
 State: UP NBMA MULT
 Slot: 0(Logic Slot: 0)
 IntType: 27, PriLog: 2, MTU: 1500, Ref: 0
 Bandwidth: 0, 0
 Baudrate: 0, 0
 Delay: 0, Reliability: 0, Load: 0
 Age: 1635sec

Logical IF Info:
 IfnetIndex: 0x2, PhyIndex: 2, LogiIndex: 2
 Dest: ::, Mask: 128
 State: UP PRM NBMA MULT , Ref: 0
 Age: 1635sec
```

Table 9-230 Description of the display rm ipv6 interface command output

Item	Description
Name	Name of an interface.
Physical IF Info	Physical interface information.
IfnetIndex	Network segment index of the interface.
State	Interface status.
IntType	Interface type.
Slot	Slot ID.
PriLog	Index of the primary logical interface.
MTU	Maximum transmission unit (MTU) of the interface.
Ref	Number of times the interface is referenced.
Bandwidth	Bandwidth of the interface.
Baudrate	Baud rate of the interface.
Delay	Link delay.
Reliability	Link reliability.
Load	Link load.
Age	Lifetime of the displayed information.
Logical IF Info	Logical interface information.
PhyIndex	Physical index.
LogiIndex	Logical index.
Dest	Destination IPv6 address.
Mask	Prefix length of the destination IPv6 address.

 Copyright © Huawei Technologies Co., Ltd.

9.10.23 display rm ipv6 bfd-session

Function

The **display rm ipv6 bfd-session** command displays the configurations of BFD sessions in Route Management (RM). The configurations include the global status of BFD, number of BFD sessions, and VPN instance, destination address, source address, interface, and session status of each BFD session.

Format

display rm ipv6 bfd-session [**all** | [[**vpn-instance** *vpn-instance-name*] [**destination** *destination-address*] [**source** *source-address*] [**interface** *interface-type interface-number*] [**protocol** { **bgp** | **ospfv3** }]]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPNv6 instance.	The value is the name of an existing VPNv6 instance.
destination *destination-address*	Specifies the remote destination address.	-
source *source-address*	Specifies the local source address.	-
interface *interface-type interface-number*	Specifies the type and number of an outbound interface.	-
protocol { **bgp** | **ospfv3** }	Indicates a routing protocol. ● bgp: indicates the Border Gateway Protocol (BGP). ● ospfv3: indicates the Open Shortest Path First (OSPF) version 3 protocol.	-
all	Displays all the configurations of BFD sessions in RM, including the BFD sessions of the public network and VPN. If **all** is not specified, only the configurations of BFD sessions in the public network are displayed.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

You can use the command to view the BFD sessions that are dynamically created by the routing protocol. To modify the parameters of a BFD session, refer to the **display rm ipv6 bfd-session**.

Example

Display the configurations of BFD sessions in RM.

```
<Huawei> display rm ipv6 bfd-session vpn-instance a destination 2001:db8:1::1 source 2001:db8:1::2
interface GigabitEthernet2/0/0

BFD Global Status: ON
RM IPv6 BFD Session Total Number: 1
Destination: 2001:db8:1::1
Source     : 2001:db8:1::2
  Session-State      Local-Discr      Interface            VPN-Name
  Up                 8192             GigabitEthernet2/0/0  a
  Route-Protocol     Rx-Interval(ms)  Tx-Interval(ms)       Multiplier
  BGP                1000             1000                  7
```

Table 9-231 Description of the **display rm ipv6 bfd-session** command output

Item	Description
BFD Global Status	Global status of BFD: ● On: indicates that BFD is enabled globally. ● Off: indicates that BFD is disabled globally.
RM IPv6 BFD Session Total Number	Total number of BFD sessions
Destination	Destination IP address bound to the BFD session
Source	Source IP address bound to the BFD session
Session-State	Current status of a BFD session: ● AdmDown: If the **shutdown (BFD session view)** command is used, the BFD session enters the AdmDown state. ● Down: the BFD session is in the Down state. ● Init: the BFD session is in the Init state. ● Up: the BFD session is in the Up state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Local-Discr	Local discriminator of the BFD session ● If the value is 0, it indicates that the RM is notified of the need to set up of a BFD session, but the RM has not instructed BFD to set up the session. ● If the value is not 0, it indicates that RM has instructed BFD to set up a BFD session. If you need to learn the establishment of the BFD session, you can view the Session-State.
Interface	Local physical interface bound to the BFD session
VPN-Name	VPN Name
Route-Protocol	Routing protocol enabled with BFD: ● BGP ● OSPFv3
Rx-Interval (ms)	Configured receiving interval in milliseconds
Tx-Interval (ms)	Configured sending interval in milliseconds
Multiplier	Configured local detection multiplier

9.10.24 display router id

Function

The **display router id** command displays the configured router ID.

Format

display router id [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays the configured router ID of the specified VPN instance. If this parameter is not specified, the configured router ID of the public network is displayed.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the configured router ID.

```
<Huawei> display router id
RouterID:10.1.1.1
```

Display the configured router ID of VPN instance **vpna**.

```
<Huawei> display router id vpn-instance vpna
RouterID:10.1.1.1
```

Related Topics

9.10.49 router id

12.9.35 ip vpn-instance

9.10.25 display route resource

Function

The **display route resource** command displays the total number of IPv4 and IPv6 route prefixes in the IP routing table on the device.

Format

display route resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display route resource** command displays the total number of IPv4 and IPv6 route prefixes in the IP routing table on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the total number of IPv4 and IPv6 route prefixes in the IP routing table on the device.

```
<Huawei> display route resource
 Total number of IPv4 Prefixes: 16
 Total number of IPv6 Prefixes: 13
```

Table 9-232 Description of the **display route resource** command output

Item	Description
Total number of IPv4 Prefixes	Current number of IPv4 route prefixes.
Total number of IPv6 Prefixes	Current number of IPv6 route prefixes.

9.10.26 fib download all

Function

Using the **fib download all** command, you can configure the device to deliver all the routing entries to the FIB of a LAN-side subcard.

Using the **undo fib download all** command, you can restore the default configuration.

To reduce routing entries, the device delivers only local routing entries of a LAN-side subcard to the FIB by default.

Format

fib download all slot *slot-id*

undo fib download all [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a running LAN-side subcard. The value varies according to device hardware.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce routing entries in the routing table, the device delivers only local routing entries of a LAN-side subcard to the FIB but does not deliver routes with WAN-side outbound interfaces. Sometimes, there are two routing entries with the same destination IP address but different mask lengths, and the entry with the longer mask length is on the WAN-side subcard. Packets reaching the LAN-side subcard match the routing entry with the shorter mask, which does not comply with the longest match principle. As a result, the packets are forwarded using an incorrect route. To solve this problem, run the **fib download all** command to configure the device to deliver routing entries with WAN-side outbound interfaces to the FIB of the LAN-side subcard.

Precautions

After the **fib download all** command is executed, only newly generated routes are updated in the routing table of the LAN-side subcard. That is, the **fib download all** command takes effect for only newly generated routes.

If the **fib download all** command is executed, resources on a LAN-side subcard are occupied and system performance deteriorates. Exercise caution when you run the command.

NOTE

Only AR2200, AR3600, and AR3200 support this command.

Example

configure to deliver all the routing entries to the FIB of a LAN-side subcard, on slot 2

```
<Huawei> system-view
[Huawei] fib download all slot 2
```

9.10.27 fib regularly-refresh

Function

The **fib regularly-refresh** command specifies an interval at which FIB entries are refreshed and the number of FIB entries refreshed per circle.

The **undo fib regularly-refresh** command restores the default configuration.

The default interval and number are 1 second and 100, respectively.

Format

fib regularly-refresh { **interval** *interval* [**entry-number** *entry-number*] | **entry-number** *entry-number* }

undo fib regularly-refresh { **interval** *interval* [**entry-number** *entry-number*] | **entry-number** *entry-number* }

Parameters

Parameter	Description	Value
interval *interval*	Specifies an interval at which FIB entries are refreshed.	The value is an integer ranging from 1 to 300.
entry-number *entry-number*	Specifies the number of FIB entries refreshed per circle.	The value is an integer ranging from 20 to 2000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Regular FIB entry refreshing occupies system resources, including CPU and memory resources. A longer interval and smaller number result in less impact on other services. You can flexibly configure the interval and number based on system resources. By default, CPU usage during regular FIB entry refreshing is not 10% greater than the original CPU usage.

Prerequisites

Regular FIB entry refreshing has been enabled using the **undo fib regularly-refresh disable** command in the system view.

Example

Set an interval at which FIB entries are refreshed to 5 seconds and the number of FIB entries refreshed per circle to 200.

```
<Huawei> system-view
[Huawei] fib regularly-refresh interval 5 entry-number 200
```

9.10.28 fib regularly-refresh disable

Function

The **fib regularly-refresh disable** command disables an FIB from being refreshed every 24 hours.

The **undo fib regularly-refresh disable** command enables an FIB to be refreshed every 24 hours.

By default, an FIB is not refreshed every 24 hours.

Format

fib regularly-refresh disable

undo fib regularly-refresh disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To avoid high CPU usage and CPU performance deterioration caused by FIB refreshment, you can use the **fib regularly-refresh disable** command to disable an FIB from being refreshed every 24 hours temporarily.

Precautions

NOTICE

Disabling FIB refreshment may result in that some hardware errors cannot be corrected timely. Exercise caution when using this command.

Example

Disable the FIB from being refreshed every 24 hours.

```
<Huawei> system-view
[Huawei] fib regularly-refresh disable
Warning: This operation will disable the function of the FIB regularly refresh,
Confirm?[Y/N]:y
Info: The function of the FIB regularly refresh is disabled.
```

9.10.29 fib regularly-refresh start-time

Function

Using the **fib regularly-refresh start-time** command, you can set the time at which an FIB is refreshed.

Using the **undo fib regularly-refresh start-time** command, you can restore the default value of the time at which an FIB is refreshed.

By default, an FIB is refreshed at 1 every 24 hours.

 Copyright © Huawei Technologies Co., Ltd.

Format

fib regularly-refresh start-time *start-time*

undo fib regularly-refresh start-time

Parameters

Parameter	Description	Value
start-time	Time at which an FIB is refreshed	The value ranges from 0 to 23, in hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Usually, a device refreshes an FIB at 1 o'clock every 24 hours. When the FIB is refreshed, a large amount of routing information is delivered, causing high usage of CPU. If refreshment is performed at the traffic peak period, the CPU performance may deteriorate. You can use the **fib regularly-refresh start-time** command to choose any time between 0 to 23 to refresh FIB entries, so as to prevent FIB entries from being refreshed during the traffic peak period.

Prerequisites

Ensure that the FIB every-24-hour refreshment function is enabled.

Precautions

If the system time changes, the FIB every-24-hour refreshment function fails to change the interval at which an FIB entry is refreshed accordingly. To correct the interval, run the fib regularly-refresh start-time command.

Example

Set the FIB to be refreshed every 4 o'clock.

```
<Huawei> system-view
[Huawei] fib regularly-refresh start-time 4
Warning: This operation will reset the start time of the FIB regularly refresh,Confirm?[Y/N]:y
Info: System will start the FIB regularly refresh at 4 o'clock.
```

9.10.30 ip frr (system view)

Function

The **ip frr** command enables IP FRR for public routes.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ip frr** command disables IP FRR for public routes.

By default, IP FRR is disabled for public routes.

Format

ip frr route-policy *route-policy-name*

undo ip frr [**all**]

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Enables IP FRR for public routes matching the specified route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Disables IP FRR for all public and private routes. If this parameter is not specified, IP FRR is disabled for all public routes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

However, under traditional forwarding modes, when multiple routes to the same destination exist, router selects the optimal route, which is delivered to FIB table to direct data forwarding. When the optimal link is faulty, router waits for the completion of route convergence, then selects another optimal route, and then deliver the route to the FIB table. Then the service is recovered. This process leads to a long-time service interruption and cannot meet service requirements.

Using the **ip frr** command, you can enable IP FRR of the public network. IP FRR can specify a backup next hop and a backup interface and set backup forwarding information for IPv4 routes. When the active link is faulty, the system can switch the traffic immediately to the backup link. This process is irrelevant to route convergence and therefore services are interrupted for short time.

Pre-configuration Tasks

 Copyright © Huawei Technologies Co., Ltd.

The **ip frr** command should be used with the **apply backup-interface** command and the **apply backup-nexthop** command. It is recommended to use the **route-policy** command to create Route-Policy at first, in which the **apply backup-interface** command and the **apply backup-nexthop** command are used to set a backup outbound interface and a backup next hop for IPv4 route of the public network.

Precautions

Only one policy can be used at one time. New configuration will replace the previous one if another policy is configured. Configuration in the system view and that in the VPN instance IPv4 address family view will not interfere each other.

Using the **undo ip frr all** command, IP FRR of all the public network and the private networks is disabled. Use it with caution.

Example

Specify a backup outbound interface and a backup next hop in route-policy **ip_frr_rp** and enable IP FRR for public routes in the system view.

```
<Huawei> system-view
[Huawei] route-policy ip_frr_rp permit node 10
[Huawei-route-policy] apply backup-interface gigabitethernet 1/0/0
[Huawei-route-policy] apply backup-nexthop 192.168.20.2
[Huawei-route-policy] quit
[Huawei] ip frr route-policy ip_frr_rp
```

9.10.31 ip load-balance hash

Function

The **ip load-balance hash** command configures the UCMP and ECMP load balancing algorithms.

The **undo ip load-balance hash** command restores the default load balancing mode.

By default, IP packets are load balanced based on the source IP address and destination IP address. TCP packets or UDP packets are load balanced based on the source IP address, destination IP address, source port number, and destination port number.

Format

ip load-balance hash { **src-ip** | **dst-ip** | **src-dst-ip** }

undo ip load-balance hash

Parameters

Parameter	Description	Value
src-ip	Indicates that the load balancing is based on the source IP address.	-

Parameter	Description	Value
dst-ip	Indicates that the load balancing is based on the destination IP address.	-
src-dst-ip	Indicates that the load balancing is based on the source IP address and destination IP address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The router supports the multi-route mode. You can configure multiple routes to the same destination and with the same priority. If a routing protocol discovers multiple routes to the same destination and they have the same cost, the router performs load balancing among the routes.

In network applications, the router often uses load balancing to improve link utilization and increase network bandwidth. By default, IP packets are forwarded based on the source IP address and destination IP address. IP packets with the same source IP address and destination IP address are forwarded through the same route. IP packets with different source IP addresses and destination IP addresses are forwarded through different equal-cost routes. In practical applications, packets need to be forwarded using different methods to properly use link resources. Flexible load balancing algorithms can meet requirements in different scenarios.

- If the **src-ip** parameter is configured, the load balancing is based on the source IP address. In a scenario that has multiple equal-cost uplink routes, traffic from different users is load balanced among different equal-cost routes.
- If the **dst-ip** parameter is configured, the load balancing is based on the destination IP address. In a scenario that has multiple equal-cost uplink routes, traffic from different users to the same destination IP address is forwarded through the same link.

NOTE

The **ip load-balance hash** and **ip load-balance packet** commands cannot take effect simultaneously.

Example

Configure the load balancing based on the source IP address.

```
<Huawei> system-view
[Huawei] ip load-balance hash src-ip
```

9.10.32 ip load-balance packet

Function

The **ip load-balance packet** command configures per-packet load balancing for traffic distribution.

The **undo ip load-balance packet** command restores the default load balancing mode.

By default, traffic is distributed in per-flow load balancing mode.

Format

ip load-balance packet

undo ip load-balance packet

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Routers support the multi-routed mode. That is, you can configure multiple routes with the same destination and preference. When multiple routes have the same destination and cost and are discovered by the same routing protocol, routers load balance traffic among these routes.

By default, traffic is forwarded in per-flow load balancing mode. That is, each flow is forwarded over only one link. You can run the **ip load-balance packet** command to configure the per-packet load balancing mode for traffic forwarding. That is, each flow can be distributed to all links for forwarding, reducing the possibility of link congestion and improving link efficiency.

Precautions

- The **ip load-balance packet** and **ip load-balance hash** commands cannot take effect simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

- When packets need to be fragmented and the delay difference between two links is large, packet mis-sequencing may occur during packet reassembly if traffic is distributed in per-packet load balancing mode.

Example

Configure the per-packet load balancing mode.

```
<Huawei> system-view
[Huawei] ip load-balance packet
```

9.10.33 ip prefix-limit

Function

The **ip prefix-limit** command configures a limit on the number of IPv4 public route prefixes.

The **undo ip prefix-limit** command restores the default configuration.

By default, the maximum number of IPv4 public route prefixes is not limited.

Format

ip prefix-limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo ip prefix-limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IPv4 public route prefixes.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.
alert-percent	Specifies the percentage of the maximum number of IPv4 public route prefixes. If you specify *alert-percent* in the command, when the number of IPv4 public route prefixes exceeds the value calculated by (*number* x *alert-percent*) / 100, an alarm is generated. Additional IPv4 public route prefixes can still be added to the routing table until the number of IPv4 public route prefixes reaches *number*. Subsequent route prefixes are discarded.	The value is an integer ranging from 1 to 100.

Parameter	Description	Value
route-unchanged	Indicates that the routing table remains unchanged. If you decrease *alert-percent* after the number of IPv4 public route prefixes exceeds *number*, whether the routing table remains unchanged is determined by **route-unchanged**. ● If you specify **route-unchanged** in the command, the routing table remains unchanged. ● If you do not specify **route-unchanged** in the command, the system deletes the routes from the routing table and re-adds routes. By default, the system deletes the routes from the routing table and re-adds routes.	-
simply-alert	Indicates the following function: If you specify *simply-alert* in the command, new IPv4 public route prefixes can still be added to the routing table and only an alarm is generated after the number of IPv4 public route prefixes exceeds *number*. However, when the total number of private and public route prefixes reaches the limit on the number of unicast route prefixes specified in the PAF file, subsequent IPv4 public route prefixes are discarded.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the router imports a large number of routes, system performance may be affected when processing services because the routes consume a lot of system resources. To improve system security and reliability, you can run the **ip prefix-limit** command to configure a limit on the number of IPv4 public route prefixes. When the number of IPv4 public route prefixes exceeds the limit, an alarm is generated, prompting you to check whether unneeded IPv4 public route prefixes exist.

Configuration Impact

After the **ip prefix-limit** command is run, the router may discard unneeded IPv4 public route prefixes.

Precautions

If you run the **ip prefix-limit** command for several times, the last configuration overrides previous configurations.

After the number of IPv4 public route prefixes exceeds the limit, note the following rules:

- If you run the **ip prefix-limit** command to increase *number* or the **undo ip prefix-limit** command to delete the limit, the router relearns IPv4 public route prefixes.
- Direct and static routes can still be added to the IP routing table.

Example

Configure **simply-alert** so that only an alarm is generated when the router imports more than 10000 IPv4 public route prefixes.

```
<Huawei> system-view
[Huawei] ip prefix-limit 10000 simply-alert
```

9.10.34 ip prefix-limit log-interval

Function

The **ip prefix-limit log-interval** command configures an interval at which logs are generated after the number of IPv4 public route prefixes exceeds the limit.

The **undo ip prefix-limit log-interval** command restores the default configuration.

By default, the system generates logs at an interval of 5s after the number of IPv4 public route prefixes exceeds the limit.

Format

ip prefix-limit log-interval *interval*

undo ip prefix-limit log-interval

Parameters

Parameter	Description	Value
interval	Specifies an interval at which logs are generated after the number of IPv4 public route prefixes exceeds the limit.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system generates logs at an interval of 5s after the number of IPv4 public route prefixes exceeds the limit. You can run the **ip prefix-limit log-interval** command to set a larger value for the interval to decrease the frequency at which these logs are generated.

The maximum number of IPv4 public route prefixes supported by the routing table can be adjusted using the **ip prefix-limit** command.

Precautions

If a log is generated to record the event that the number of IPv4 public route prefixes reaches the limit, no more routes can be added to the routing table, and subsequent routes are discarded.

Example

Set the interval at which logs are generated after the number of IPv4 public route prefixes exceeds the limit to 30s.

```
<Huawei> system-view
[Huawei] ip prefix-limit log-interval 30
```

Related Topics

9.10.33 ip prefix-limit

9.10.35 ip route prefix-priority-scheduler

Function

The **ip route prefix-priority-scheduler** command sets the priority-based scheduling weight of IPv4 routes.

The **undo ip route prefix-priority-scheduler** command restores the default priority-based scheduling weight of IPv4 routes.

By default, the priority-based scheduling weight of IPv4 routes is 8:4:2:1.

Format

ip route prefix-priority-scheduler *critical-weight high-weight medium-weight low-weight*

undo ip route prefix-priority-scheduler

Parameters

Parameter	Description	Value
critical-weight	Sets the scheduling weight of a critical queue.	The value is an integer that ranges from 1 to 10.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high-weight	Sets the scheduling weight of a high queue.	The value is an integer that ranges from 1 to 10.
medium-weight	Sets the scheduling weight of a medium queue.	The value is an integer that ranges from 1 to 10.
low-weight	Sets the scheduling weight of a low queue.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The integration of network services urgently requires differentiated services. Routes for key services, such as Voice over IP (VoIP), video conferences, and multicast services, need to be converged rapidly, while routes for common services can be converged relatively slowly. In this case, the system needs to converge routes based on their convergence priorities to improve network reliability.

Different routes can be set with different convergence priorities, which can be critical, high, medium, and low listed in descending order. Critical is the highest convergence priority; low is the lowest convergence priority. The system converges routes based on the convergence priorities and convergence rules, that is, schedules the convergence of routes of different convergence priorities in proportion, to guide service forwarding.

When the system is processing a large number of high-priority routes, low-priority routes may fail to be processed for a long time. In this case, to prevent system performance from being affected, run the **ip route prefix-priority-scheduler** command to adjust the priority-based scheduling weight of IPv4 routes.

Follow-up Procedure

In most cases, convergence priorities of routes are determined by route types. On an OSPF network, you can run the **prefix-priority (OSPF)** command to adjust the convergence priority of OSPF routes. On an IS-IS network, you can run the **prefix-priority (IS-IS)** command to adjust the convergence priority of IS-IS routes.

Example

Set the priority-based scheduling weight of IPv4 routes to 10:2:1:1.

```
<Huawei> system-view
[Huawei] ip route prefix-priority-scheduler 10 2 1 1
```

 Copyright © Huawei Technologies Co., Ltd.

9.10.36 ip route recursive-lookup default-route

Function

The **ip route recursive-lookup default-route** command enables routes of a specified routing protocol to be iterated to the default route.

The **undo ip route recursive-lookup default-route** command disables routes of a specified routing protocol from being iterated to the default route.

By default, routes of a specified routing protocol cannot be iterated to the default route.

Format

ip route recursive-lookup default-route protocol { **static** | **unr** | **bgp** | **msr** }

undo ip route recursive-lookup default-route protocol { **static** | **unr** | **bgp** | **msr** }

Parameters

Parameter	Description	Value
static	Static route	-
unr	User Network Route	-
bgp	Border Gateway Protocol	-
msr	Multicast Static Route	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic cannot be transmitted along static, UNR, or BGP routes with an unreachable next hop. In this situation, iteration is required. Run the **ip route recursive-lookup default-route** command to iterate routes of these protocols to the default route.

Precautions

After iteration, the actual forwarding route may change.

Example

Enable static routes to be iterated to the default route.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip route recursive-lookup default-route protocol static
```

9.10.37 ipv6 fib-loadbalance-type hash-based

Function

The **ipv6 fib-loadbalance-type hash-based** command configures packets sent from a specified source to a specified destination to be forwarded using the same route.

The **undo ipv6 fib-loadbalance-type hash-based** command restores the default configuration.

By default, flow-based load balancing is used.

Format

ipv6 fib-loadbalance-type hash-based

undo ipv6 fib-loadbalance-type hash-based

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

NOTE

This command takes effect only when the FIB cache fails.

Example

Configure packets sent from a specified source to a specified destination to be forwarded using the same route.

```
<Huawei> system-view
[Huawei] ipv6 fib-loadbalance-type hash-based
```

9.10.38 ipv6 fib regularly-refresh entry-number

Function

The **ipv6 fib regularly-refresh entry-number** command configures the number of entries refreshed each time for the IPv6 FIB.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ipv6 fib regularly-refresh entry-number** command restores the default number of entries refreshed each time for the IPv6 FIB.

By default, the number of entries refreshed each time for the IPv6 FIB is 100.

Format

ipv6 fib regularly-refresh entry-number *entry-number*

undo ipv6 fib regularly-refresh entry-number [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Specifies the number of IPv6 FIB entries refreshed each time.	The value is an integer ranging from 20 to 2000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPv6 FIB 24-hour refresh occupies system resources, including CPU and memory resources. The less the number of entries refreshed is configured, the minor negative impacts it has on other services. Users can configure the number of entries refreshed flexibly based on system resources.

To reduce the system resource usage, run the **ipv6 fib regularly-refresh entry-number** command and the **ipv6 fib regularly-refresh interval** command to adjust the interval at which IPv6 FIB entries are refreshed and the number of IPv6 FIB entries refreshed each time.

Prerequisites

IPv6 FIB 24-hour refresh has been enabled. By default, this function has been enabled. If not, run the **undo ipv6 fib regularly-refresh disable** command in the system view to enable it.

Precautions

If the number of entries refreshed is too small, the lower layer hardware entries cannot be refreshed periodically, and this affects IPv6 route forwarding.

Example

Configure the number of entries refreshed each time for the IPv6 FIB to 200.

```
<Huawei> system-view
[Huawei] undo ipv6 fib regularly-refresh disable
```

 Copyright © Huawei Technologies Co., Ltd.

```
Warning: This operation will enable the function of the FIB regularly refresh,Confirm?[Y/N]:y
Info: The function of the FIB regularly refresh is enabled.
[Huawei] ipv6 fib regularly-refresh entry-number 200
```

Related Topics

9.10.39 ipv6 fib regularly-refresh disable

9.10.40 ipv6 fib regularly-refresh interval

9.10.41 ipv6 fib regularly-refresh start-time

9.10.39 ipv6 fib regularly-refresh disable

Function

The **ipv6 fib regularly-refresh disable** command disables IPv6 FIB 24-hour refresh.

The **undo ipv6 fib regularly-refresh disable** command enables IPv6 FIB 24-hour refresh.

By default, IPv6 FIB 24-hour refresh is enabled.

Format

ipv6 fib regularly-refresh disable

undo ipv6 fib regularly-refresh disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During peak hours, refreshing the IPv6 FIB can cause over-high CPU usage and affect service reliability. To resolve this problem, run the **ipv6 fib regularly-refresh disable** command to disable IPv6 FIB 24-hour refresh. After the CPU usage restores to a normal state, run the **undo ipv6 fib regularly-refresh disable** command to restore IPv6 FIB 24-hour refresh.

Precautions

Disabling IPv6 FIB 24-hour refresh may prevent the rectification of certain hardware forwarding entry faults. Exercise caution when running the **ipv6 fib regularly-refresh disable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable IPv6 FIB 24-hour refresh.

```
<Huawei> system-view
[Huawei] ipv6 fib regularly-refresh disable
Warning: This operation will disable the function of the FIB regularly refresh,Confirm?[Y/N]:y
Info: The function of the FIB regularly refresh is disabled.
```

Related Topics

9.10.40 ipv6 fib regularly-refresh interval

9.10.38 ipv6 fib regularly-refresh entry-number

9.10.41 ipv6 fib regularly-refresh start-time

9.10.40 ipv6 fib regularly-refresh interval

Function

The **ipv6 fib regularly-refresh interval** command configures a refresh interval each time for the IPv6 FIB.

The **undo ipv6 fib regularly-refresh interval** command restores the default refresh interval each time for the IPv6 FIB.

By default, the refresh interval each time for the IPv6 FIB is 1s.

Format

ipv6 fib regularly-refresh interval *interval*

undo ipv6 fib regularly-refresh interval [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies an interval at which IPv6 FIB entries are refreshed.	The value is an integer ranging from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPv6 FIB 24-hour refresh occupies system resources, including CPU and memory resources. The longer a refresh interval is configured, the minor negative impacts

 Copyright © Huawei Technologies Co., Ltd.

it has on other services. You can configure a refresh interval flexibly based on system resources.

To reduce the system resource usage, run the **ipv6 fib regularly-refresh entry-number** command and the **ipv6 fib regularly-refresh interval** command to adjust the interval at which IPv6 FIB entries are refreshed and the number of IPv6 FIB entries refreshed each time.

Prerequisites

IPv6 FIB 24-hour refresh has been enabled. By default, this function has been enabled. If not, run the **undo ipv6 fib regularly-refresh disable** command in the system view to enable it.

Precautions

If the configured refresh interval is too long, the lower layer hardware entries cannot be refreshed periodically, and this affects IPv6 route forwarding.

Example

Configure the refresh interval each time to 5s.

```
<Huawei> system-view
[Huawei] undo ipv6 fib regularly-refresh disable
Warning: This operation will enable the function of the FIB regularly refresh,Confirm?[Y/N]:y
Info: The function of the FIB regularly refresh is enabled.
[Huawei] ipv6 fib regularly-refresh interval 5
```

Related Topics

9.10.39 ipv6 fib regularly-refresh disable

9.10.38 ipv6 fib regularly-refresh entry-number

9.10.41 ipv6 fib regularly-refresh start-time

9.10.41 ipv6 fib regularly-refresh start-time

Function

The **ipv6 fib regularly-refresh start-time** command configures a start time for IPv6 FIB 24-hour refresh.

The **undo ipv6 fib regularly-refresh start-time** command restores the default start time for IPv6 FIB 24-hour refresh.

By default, the start time for IPv6 FIB 24-hour refresh is 00:00 a.m.

Format

ipv6 fib regularly-refresh start-time *start-time*

undo ipv6 fib regularly-refresh start-time [*start-time*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start-time	Specifies a start time for IPv6 FIB 24-hour refresh.	The value is an integer ranging from 0 to 23.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the refresh, the IPv6 FIB table delivers enormous route messages, which causes high CPU usage in a short period. If the periodic refresh also starts during peak hours, it may affect service reliability. To refresh the IPv6 FIB entries in off-peak hours, run the **ipv6 fib regularly-refresh start-time** command to configure a start time for IPv6 FIB 24-hour refresh flexibly.

Prerequisites

IPv6 FIB 24-hour refresh has been enabled. By default, this function has been enabled. If not, run the **undo ipv6 fib regularly-refresh disable** command in the system view to enable it.

Precautions

If the system time changes, the 24-hour refresh timer will not adjust the latest timeout interval automatically. You need to configure a new start time to adjust the timeout interval for the refresh timer.

Example

Configure the start time for IPv6 FIB 24-hour refresh to 4:00.

```
<Huawei> system-view
[Huawei] undo ipv6 fib regularly-refresh disable
Warning: This operation will enable the function of the FIB regularly refresh,Confirm?[Y/N]:y
Info: The function of the FIB regularly refresh is enabled.
[Huawei] ipv6 fib regularly-refresh start-time 4
Warning: This operation will reset the start time of the FIB regularly refresh,Confirm?[Y/N]:y
Info: System will start the FIB regularly refresh at 4 o'clock.
```

Related Topics

9.10.39 ipv6 fib regularly-refresh disable
9.10.40 ipv6 fib regularly-refresh interval
9.10.38 ipv6 fib regularly-refresh entry-number

9.10.42 ipv6 prefix-limit

Function

The **ipv6 prefix-limit** command configures a limit on the number of IPv6 public route prefixes.

The **undo ipv6 prefix-limit** command restores the default configuration.

By default, the maximum number of IPv6 public route prefixes is not limited.

Format

ipv6 prefix-limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo ipv6 prefix-limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IPv6 public route prefixes.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.
alert-percent	Specifies the percentage of the maximum number of IPv6 public route prefixes. If you specify *alert-percent* in the command, when the number of IPv6 public route prefixes exceeds the value calculated by (*number* x *alert-percent*) / 100, an alarm is generated. Additional IPv6 public route prefixes can still be added to the routing table until the number of IPv6 public route prefixes reaches *number*. Subsequent route prefixes are discarded.	The value is an integer ranging from 1 to 100.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-unchanged	Indicates that the routing table remains unchanged. If you decrease *alert-percent* after the number of IPv6 public route prefixes exceeds *number*, whether the routing table remains unchanged is determined by **route-unchanged**. ● If you specify **route-unchanged** in the command, the routing table remains unchanged. ● If you do not specify **route-unchanged** in the command, the system deletes the routes from the routing table and re-adds routes. By default, the system deletes the routes from the routing table and re-adds routes.	-
simply-alert	Indicates the following function: If you specify *simply-alert* in the command, new IPv6 public route prefixes can still be added to the routing table and only an alarm is generated after the number of IPv6 public route prefixes exceeds *number*. However, when the total number of private and public route prefixes reaches the limit on the number of unicast route prefixes specified in the PAF file, subsequent IPv6 public route prefixes are discarded.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the router imports a large number of routes, system performance may be affected when processing services because the routes consume a lot of system resources. To improve system security and reliability, you can run the **ipv6 prefix-limit** command to configure a limit on the number of IPv6 public route prefixes. When the number of IPv6 public route prefixes exceeds the limit, an alarm is generated, prompting you to check whether unneeded IPv6 public route prefixes exist.

Configuration Impact

After the **ipv6 prefix-limit** command is run, the router may discard unneeded IPv6 public route prefixes.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If you run the **ipv6 prefix-limit** command for several times, the last configuration overrides previous configurations.

After the number of IPv6 public route prefixes exceeds the limit, note the following rules:

- If you run the **ipv6 prefix-limit** command to increase *number* or the **undo ipv6 prefix-limit** command to delete the limit, the router relearns IPv6 public route prefixes.
- Direct and static routes can still be added to the IPv6 routing table.

Example

Configure **simply-alert** so that only an alarm is generated when the router imports more than 10000 IPv6 public route prefixes.

```
<Huawei> system-view
[Huawei] ipv6 prefix-limit 10000 simply-alert
```

9.10.43 ipv6 prefix-limit log-interval

Function

The **ipv6 prefix-limit log-interval** command configures an interval at which logs are generated after the number of IPv6 public route prefixes exceeds the limit.

The **undo ipv6 prefix-limit log-interval** command restores the default configuration.

By default, the system generates logs at an interval of 5s after the number of IPv6 public route prefixes exceeds the limit.

Format

ipv6 prefix-limit log-interval *interval*

undo ipv6 prefix-limit log-interval

Parameters

Parameter	Description	Value
interval	Specifies an interval at which logs are generated after the number of IPv6 public route prefixes exceeds the limit.	The value is an integer ranging from 1 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system generates logs at an interval of 5s after the number of IPv6 public route prefixes exceeds the limit. You can run the **ip prefix-limit log-interval** command to set a larger value for the interval to decrease the frequency at which these logs are generated.

The maximum number of IPv6 public route prefixes supported by the routing table can be adjusted using the **ipv6 prefix-limit** command.

Precautions

If a log is generated to record the event that the number of IPv6 public route prefixes reaches the limit, no more routes can be added to the routing table, and subsequent routes are discarded.

Example

Set the interval at which logs are generated after the number of IPv6 public route prefixes exceeds the limit to 30s.

```
<Huawei> system-view
[Huawei] ipv6 prefix-limit log-interval 30
```

Related Topics

9.10.42 ipv6 prefix-limit

9.10.44 ipv6 route prefix-priority-scheduler

Function

The **ipv6 route prefix-priority-scheduler** command sets the priority-based scheduling weight of IPv6 routes.

The **undo ipv6 route prefix-priority-scheduler** command restores the default priority-based scheduling weight of IPv6 routes.

By default, the priority-based scheduling weight of IPv6 routes is 8:4:2:1.

Format

ipv6 route prefix-priority-scheduler *critical-weight high-weight medium-weight low-weight*

undo ipv6 route prefix-priority-scheduler

Parameters

Parameter	Description	Value
critical-weight	Sets the scheduling weight of a critical queue.	The value is an integer that ranges from 1 to 10.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high-weight	Sets the scheduling weight of a high queue.	The value is an integer that ranges from 1 to 10.
medium-weight	Sets the scheduling weight of a medium queue.	The value is an integer that ranges from 1 to 10.
low-weight	Sets the scheduling weight of a low queue.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The integration of network services urgently requires differentiated services. IPv6 routes for key services, such as Voice over IP (VoIP), video conferences, and multicast services, need to be converged rapidly, while routes for common services can be converged relatively slowly. In this case, the system needs to converge IPv6 routes based on their convergence priorities to improve network reliability.

Different IPv6 routes can be set with different convergence priorities, which can be critical, high, medium, and low listed in descending order. Critical is the highest convergence priority; low is the lowest convergence priority. The system converges IPv6 routes based on the convergence priorities and convergence rules, that is, schedules the convergence of IPv6 routes of different convergence priorities in proportion, to guide service forwarding.

When the system is processing a large number of high-priority IPv6 routes, low-priority IPv6 routes may fail to be processed for a long time. In this case, to prevent system performance from being affected, run the **ipv6 route prefix-priority-scheduler** command to adjust the priority-based scheduling weight of IPv6 routes.

Follow-up Procedure

In most cases, convergence priorities of IPv6 routes are determined by route types. On an ISISv6 network, run the **ipv6 prefix-priority (IS-IS)** command to adjust the convergence of ISISv6 routes.

Example

Set the priority-based scheduling weight of IPv6 routes to 10:2:1:1 (critical:high:medium:low).

```
<Huawei> system-view
[Huawei] ipv6 route prefix-priority-scheduler 10 2 1 1
```

Related Topics

9.7.14 ipv6 prefix-priority (IS-IS)

9.10.45 refresh fib

Function

The **refresh fib** command delivers IPv4 FIB policies and forwarding entries.

Format

refresh fib slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of an LPU that needs to update IPv4 FIB policies.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the IPv4 FIB policy changes, you must run the **refresh fib** command to update the LPU to make the configuration take effect.

After the **refresh fib** command is executed, you can view the FIB table to check whether the update succeeds.

Precautions

If the FIB module is in overload state and the LPU works in overload suspension mode, the IPv4 and IPv6 modules need to be updated.

Example

Refresh IPv4 FIB module on the LPU in slot 2.

```
<Huawei> system-view
[Huawei] refresh fib slot 2
```

 Copyright © Huawei Technologies Co., Ltd.

9.10.46 refresh ipv6 fib

Function

The **refresh ipv6 fib** command delivers IPv6 FIB policies and forwarding entries.

Format

refresh ipv6 fib slot *slot-id*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of an LPU that needs to update IPv6 FIB policies.	The value is determined based on the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the IPv6 FIB policy changes, you must run the **refresh ipv6 fib** command to update the LPU to make the configuration take effect.

After the **refresh ipv6 fib** command is executed, you can view the FIB table to check whether the update succeeds.

NOTE

If the FIB module is in overload state and the LPU works in overload suspension mode, the IPv4 and IPv6 modules need to be updated.

Example

Update the IPv6 FIB module on the LPU in slot 2.

```
<Huawei> system-view
[Huawei] refresh ipv6 fib slot 2
```

9.10.47 reset ip routing-table statistics protocol

Function

The **reset ip routing-table statistics protocol** command clears route statistics in an IPv4 routing table.

Format

reset ip routing-table statistics protocol [**vpn-instance** *vpn-instance-name*] { **all** | *protocol* }

reset ip routing-table all-vpn-instance statistics protocol { **all** | *protocol* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears route statistics in an IPv4 routing table of the specified VPN instance. If this parameter is not specified, route statistics in an IPv4 routing table of the public network are cleared.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Clear route statistics of all routing protocols in an IPv4 routing table.	-
protocol	Clears route statistics of the specified routing protocol in an IPv4 routing table. This parameter can be one of the following: **direct**, **bgp**, **isis**, **ospf**, **rip**, **static**, and **unr**.	-
all-vpn-instance	Clears the statistics in the IPv4 routing tables of all VPN instances.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to clear route statistics in an IPv4 routing table, including statistics about the routes added, deleted, and released by each routing protocol. Subsequently, the system can re-collect route statistics of each routing protocol again to monitor route changes and locate network faults.

Precautions

IPv4 route statistics cannot be restored after being cleared. Exercise caution when you use this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear route statistics of all routing protocols in an IPv4 routing table.

```
<Huawei> reset ip routing-table statistics protocol all
```

9.10.48 reset ipv6 routing-table statistics protocol

Function

The **reset ipv6 routing-table statistics protocol** command clears route statistics in an IPv6 routing table.

Format

reset ipv6 routing-table [**vpn-instance** *vpn-instance-name*] **statistics protocol** { **all** | *protocol* }

reset ipv6 routing-table all-vpn-instance statistics protocol { **all** | *protocol* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Clear route statistics of all routing protocols in an IPv6 routing table.	-
protocol	Clears route statistics of the specified routing protocol in an IPv6 routing table. This parameter can be one of the following: **bgp**, **direct**, **isis**, **ospfv3**, **unr**, **ripng**, and **static**.	-
all-vpn-instance	Clears the statistics in the IPv6 routing tables of all VPN instances.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to clear route statistics of each routing protocol in an IPv6 routing table. Subsequently, the router can re-collect route statistics of each routing protocol to monitor route changes and locate network faults.

Precautions

IPv6 route statistics cannot be restored after being cleared. Exercise caution when you use this command.

Example

Clear route statistics of all routing protocols in an IPv6 routing table.

```
<Huawei> reset ipv6 routing-table statistics protocol all
```

9.10.49 router id

Function

The **router id** command sets the router ID in RM.

The **undo router id** command deletes the configured router ID.

By default, the router ID in RM is 0.0.0.0 when no IPv4 interface address is configured.

Format

router id *router-id*

undo router id

Parameters

Parameter	Description	Value
router-id	Sets a router ID in the IPv4 address format.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Some dynamic routing protocols require that a router ID uniquely identify a device. If no router ID is specified when these protocols are started on a device, the router ID in RM is used by default.

The rules for selecting a router ID are as follows:

1. If you set a router ID using the **router id** command, the configured router ID is used.
2. If no router ID is set, the router ID is selected according to the following rules:
   - If loopback interfaces configured with IP addresses exist, the largest IP address among the IP addresses of the loopback interfaces is selected as the router ID.
   - If there is no loopback interface configured with an IP address, the highest IP address among the IP addresses of other interfaces is selected as the router ID, regardless of whether the interface is Up or Down.

   NOTE

   The router ID is reselected only when the interface address that is selected as the router ID is deleted or changed. The router ID is not reselected in any of the following situations:

   - The interface is Down.
   - A loopback interface is configured when the IP address of a non-loopback interface is selected as the router ID.
   - A larger interface address is configured later.

   You can run the **display router id** command to view the router ID.
3. Each VPN instance selects the router ID from the IP addresses of the interfaces in the VPN instance based on rules 1 and 2.
4. When active and standby MPUs are installed, the system backs up the router ID set through the **router id** command and selects the router ID from IP addresses of interfaces. After the active/standby switchover is performed, the system checks the validity of the router ID selected from interface addresses. If the router ID is invalid, the system reselects a router ID.

After the router ID is changed, manually run the **reset** command for each routing protocol to make the new router ID take effect.

Precautions

The IP address of the interface whose configuration is restored the first is used as the router ID after the restart.

NOTE

To enhance network reliability, configure the address of a loopback interface as the router ID.

Example

Set the router ID in RM to 10.10.10.1.

```
<Huawei> system-view
[Huawei] router id 10.10.10.1
```

Related Topics

9.10.24 display router id

9.11 PBR Configuration Commands

9.11.1 apply access-vpn

Function

The **apply access-vpn** command configures VPN instances for forwarding packets in the local PBR.

The **undo apply access-vpn** command deletes the configured VPN instances for forwarding packets in the local PBR.

By default, no VPN instance is configured for forwarding packets in the local PBR.

Format

apply access-vpn vpn-instance *vpn-instance-name* &<1-6>

undo apply access-vpn vpn-instance [{ *vpn-instance-name* } &<1-6>]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value is a string of 1 to 31 case-sensitive characters without spaces. A maximum of six instances can be specified in a command.

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When packets enter a VPN, run the **apply access-vpn vpn-instance** *vpn-instance-name* &<1-6> command to configure a VPN instance for forwarding the packets.

Prerequisites

VPN instances have been created.

Example

Set VPN instances **vpn1** and **vpn2** for forwarding packets.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply access-vpn vpn-instance vpn1 vpn2
```

Related Topics

9.11.44 policy-based-route

9.11.2 apply default output-interface

Function

The **apply default output-interface** command configures the default outbound interface in the local PBR.

The **undo apply default output-interface** command deletes the default outbound interface in the local PBR.

By default, no default outbound interface is configured in the local PBR.

Format

apply default output-interface *interface-type interface-number*

undo apply default output-interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the default outbound interface. Two outbound interfaces can be configured to implement load balancing. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. **NOTE** The outbound interface cannot be a broadcast interface, for example, an Ethernet interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

Packets obtaining no routing information from the routing table are forwarded on the default outbound interface. Two outbound interfaces can be configured to implement load balancing.

Example

Set the default outbound interface to Dialer 1.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply default output-interface dialer 1
```

Related Topics

9.11.44 policy-based-route

9.11.3 apply ip-address backup-nexthop

Function

The **apply ip-address backup-nexthop** command configures a backup next hop for packet forwarding in local PBR.

The **undo apply ip-address backup-nexthop** command deletes the backup next hop for packet forwarding in local PBR.

By default, no backup next hop is configured for packet forwarding in local PBR.

Format

apply ip-address backup-nexthop *ip-address*

undo apply ip-address backup-nexthop

Parameters

Parameter	Description	Value
ip-address	Specifies a backup next-hop IP address in PBR.	The value is in dotted decimal notation.

Views

Policy-based-route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In local PBR, a next hop and backup next hop are specified for packet forwarding. If the configured next hop is unavailable, the device forwards packets according to the configured backup next hop. If the configured backup next hop is also unavailable, the device searches the routing table for a route according to the destination address of packets to forward the packets.

Prerequisites

The next hop for packet forwarding in local PBR has been specified using the **9.11.5 apply ip-address next-hop (policy-based route view)** command. If only the backup next hop is configured in local PBR, the backup next hop does not take effect.

Precautions

The backup next-hop IP address for packet forwarding cannot be a local IP address.

Example

Set the backup next-hop IP address for packet forwarding in local PBR to 1.1.2.1.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply ip-address next-hop 1.1.1.1
[Huawei-policy-based-route-policy1-10] apply ip-address backup-nexthop 1.1.2.1
```

Related Topics

9.11.44 policy-based-route

9.11.5 apply ip-address next-hop (policy-based route view)

9.11.4 apply ip-address default next-hop

Function

The **apply ip-address default next-hop** command configures the default next hop in the local PBR.

The **undo apply ip-address default next-hop** command deletes the default next hop in the local PBR.

By default, no default next hop is configured in the local PBR.

Format

apply ip-address default next-hop *ip-address1* [*ip-address2*]

undo apply ip-address default next-hop [*ip-address1*] [*ip-address2*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address1	Specifies the IP address of the default next hop.	-
ip-address2	Specifies the IP address of the default next hop. Two IP addresses of the next hop can be configured to implement load balancing.	-

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

This command applies to the packets matching no route in the routing table. The IP address of the default next hop cannot be a local IP address.

Example

Set the IP address of the default next hop to 1.1.1.1 in the local PBR.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply ip-address default next-hop 1.1.1.1
```

Related Topics

9.11.44 policy-based-route

9.11.5 apply ip-address next-hop (policy-based route view)

Function

The **apply ip-address next-hop** command configures the next hop to which packets are forwarded in the local PBR.

The **undo apply ip-address next-hop** command deletes the next hop to which packets are forwarded in the local PBR.

By default, no next hop to which packets are forwarded is configured in the local PBR.

 Copyright © Huawei Technologies Co., Ltd.

Format

apply ip-address next-hop *ip-address1* [*ip-address2*]

undo apply ip-address next-hop [*ip-address1*] [*ip-address2*]

Parameters

Parameter	Description	Value
ip-address1	Specifies the IP address of the next hop.	-
ip-address2	Specifies the IP address of the next hop. Two IP addresses of the next hop can be configured to implement load balancing.	-

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

The IP address of the next hop specified in the **apply ip-address next-hop** command cannot be a local IP address.

If you configure a next hop while two next hops have been configured, the new next hop configuration overwrites the first next hop configuration, not the second next hop configuration.

Example

Set the IP address of the next hop to which packets are forwarded to 1.1.1.1 in the local PBR.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply ip-address next-hop 1.1.1.1
```

Related Topics

9.11.44 policy-based-route

 Copyright © Huawei Technologies Co., Ltd.

9.11.6 apply ip-address next-hop track ip-route

Function

The **apply ip-address next-hop track ip-route** command configures association between next hop and route in local PBR.

The **undo apply ip-address next-hop** command cancels association between next hop and routes in local PBR.

By default, association between next hop and route is not configured in local PBR.

Format

apply ip-address next-hop { *ip-address1* **track ip-route** *ip-address2* { *mask* | *mask-length* } } &<1-2>

undo apply ip-address next-hop [*ip-address1*] &<1-2>

Parameters

Parameter	Description	Value
ip-address1	Specifies the next-hop IP address in PBR.	The value is in dotted decimal notation.
ip-address2 { *mask* | *mask-length* }	Specifies the IP address of the route associated with the next hop in PBR. • *ip-address2* specifies the IP address. • *mask* specifies the mask of the IP address. • *mask-length* specifies the mask length of the IP address.	• The value of *ip-address2* is in dotted decimal notation. • The value of *mask* is in dotted decimal notation. • *mask-length* is an integer that ranges from 0 to 32.

Views

Policy-based-route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In local PBR, a next hop is specified for packet forwarding. However, specifying a next-hop IP address can only detect whether the direct link is available. When a

 Copyright © Huawei Technologies Co., Ltd.

fault occurs on the remote link, packets cannot reach the destination if the packets are forwarded based on local PBR. You can configure association between next hop and route. Then the device detects whether the configured IP address of the route associated with the next hop in PBR is reachable.

- If the IP address is reachable, the configured next hop takes effect, and the device forwards packets according to the configured next hop.
- If the IP address is unreachable, the configured next hop does not take effect, and the device checks whether a backup next-hop IP address has been configured.

Precautions

The next-hop IP address specified for packet forwarding cannot be a local IP address.

You can use the **apply ip-address next-hop** *ip-address1* **track ip-route** *ip-address2* { *mask* | *mask-length* } or **9.11.5 apply ip-address next-hop (policy-based route view)** command to specify a maximum of two next hops for packet forwarding in local PBR. If two next hops have been configured and then another next hop is configured, this next hop replaces the first configured next hop but not the second configured next hop.

Example

Set the next-hop IP address for packet forwarding in local PBR to 1.1.1.1, IP address of the route associated with the next hop to 1.1.2.1, and mask length of the IP address of the route to 24.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply ip-address next-hop 1.1.1.1 track ip-route 1.1.2.1 24
```

Related Topics

9.11.44 policy-based-route

9.11.5 apply ip-address next-hop (policy-based route view)

9.11.7 apply ip-precedence (policy-based route view)

Function

The **apply ip-precedence** command configures the priority of IP packets in the local PBR.

The **undo apply ip-precedence** command deletes the priority of IP packets in the local PBR

By default, the priority of IP packets is not configured in the local PBR.

Format

apply ip-precedence { *precedence* | **routine** | **priority** | **immediate** | **flash** | **flash-override** | **critical** | **internet** | **network** }

undo apply ip-precedence

Parameters

Parameter	Description	Value
precedence	Specifies the priority of IP packets.	The value is an integer ranging from 0 to 7. You can replace the *precedence* value with a keyword. **Table 9-233** shows the mappings between the *precedence* value and the keyword.
routine	Specifies the preference of IP packets as 0.	-
priority	Specifies the preference of IP packets as 1.	-
immediate	Specifies the preference of IP packets as 2.	-
flash	Specifies the preference of IP packets as 3.	-
flash-override	Specifies the preference of IP packets as 4.	-
critical	Specifies the preference of IP packets as 5.	-
internet	Specifies the preference of IP packets as 6.	-
network	Specifies the preference of IP packets as 7.	-

Table 9-233 Mappings between the *precedence* value and the keyword

Value	Keyword
0	Routine
1	Priority
2	Immediate
3	Flash
4	Flash-override
5	Critical
6	Internet
7	Network

 Copyright © Huawei Technologies Co., Ltd.

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

You can run the **apply ip-precedence** *precedence* command to change the priority of IP packets matching a PBR node in permit mode.

Example

Set the IP packet priority to 5 (Critical).

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply ip-precedence critical
```

Related Topics

9.11.44 policy-based-route

9.11.8 apply output-interface

Function

The **apply output-interface** command configures the outbound interface in the local PBR.

The **undo apply output-interface** command deletes the outbound interface in the local PBR.

By default, no outbound interface is configured in the local PBR.

Format

apply output-interface *interface-type interface-number*

undo apply output-interface *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the outbound interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** The outbound interface cannot be a broadcast interface, for example, an Ethernet interface.	-

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to set the outbound interface for matched IP packets. Two outbound interfaces can be configured to implement load balancing.

Precautions

If you configure an outbound interface while two outbound interfaces have been configured, the new outbound interface configuration overwrites the first outbound interface configuration, not the second outbound interface configuration.

Example

Configure Dialer 1 as the outbound interface of matched IP packets.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] apply output-interface dialer 1
```

Related Topics

9.11.44 policy-based-route

9.11.9 backup-interface

Function

The **backup-interface** command configures the next-hop IPv4 address of the outbound interface of the best-effort link in smart policy routing (SPR).

The **undo backup-interface** command deletes the best-effort link configuration in SPR.

By default, no next-hop IPv4 address of the outbound interface of the best-effort link is configured in SPR.

Format

backup-interface *interface-type interface-number* [*next-hop-address*]

undo backup-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and interface number of a best-effort link. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** The interface of a best-effort link must be a Layer 3 interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
next-hop-address	Specifies the next-hop IPv4 address of the outbound interface of a best-effort link. **NOTE** When the best-effort link is a PPP link, you can specify only the outbound interface but not the next hop IP address for the best-effort link. If the best-effort link is a non-PPP link, for example, an Ethernet link, you must specify both the outbound interface and next hop IP address for the best-effort link. Otherwise, packets cannot be forwarded.	-

Views

Smart policy routing view

Default Level

2: Configuration level

Usage Guidelines

After a best-effort link is configured, SPR allows service flows to be transmitted over the best-effort link when links in the active and standby link groups are unavailable, ensuring high-reliability transmission.

Example

Configure GE1/0/0 as the outbound interface of the best-effort link, and set the next hop IP address to 10.1.1.1.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] backup-interface gigabitethernet 1/0/0 10.1.1.1
```

Related Topics

9.11.63 smart-policy-route

9.11.10 backup-ipv6-interface

Function

The **backup-ipv6-interface** command configures the next-hop IPv6 address of the outbound interface of the best-effort link in SPR.

The **undo backup-ipv6-interface** command deletes the best-effort link configuration in SPR.

By default, no next-hop IPv6 address of the outbound interface of the best-effort link is configured in SPR.

Format

backup-ipv6-interface *interface-type interface-number* [*next-hop-address*]

undo backup-ipv6-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and interface number of a best-effort link. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** The interface of a best-effort link must be a Layer 3 interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
next-hop-address	Specifies the next-hop IPv6 address of the outbound interface of a best-effort link. **NOTE** When the best-effort link is a PPP link, you can specify only the outbound interface but not the next hop IP address for the best-effort link. If the best-effort link is a non-PPP link, for example, an Ethernet link, you must specify both the outbound interface and next hop IP address for the best-effort link. Otherwise, packets cannot be forwarded.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

Smart policy routing view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a best-effort link is configured in SPR, SPR uses the best-effort link to transmit service data when all the links in the active and standby link groups cannot meet service requirements.

Precautions

The next-hop IPv6 address configured using the **backup-ipv6-interface** command and next-hop IPv4 address configured using the **backup-interface** can belong to the same outbound interface.

If you run the **backup-ipv6-interface** command multiple times, only the latest configuration takes effect.

Example

Configure GE1/0/0 as the outbound interface of the best-effort link, and set the next hop IPv6 address to FC00:0:0:2001::1.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] backup-ipv6-interface gigabitethernet 1/0/0 FC00:0:0:2001::1
```

Related Topics

9.11.63 smart-policy-route

9.11.9 backup-interface

9.11.11 cmi-method

Function

The **cmi-method** command configures the CMI calculation formula for SPR.

The **undo cmi-method** restores the default CMI calculation formula for SPR.

By default, the CMI calculation formula is 9000 − [D (delay) + J (jitter) + L (packet loss rate)].

Format

cmi-method *cmi-method*

undo cmi-method

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cmi-method	Specifies the CMI calculation formula. ● The CMI calculation formula is 9000 – *cmi-method*. The *cmi-method* parameter is configurable, and its default value is D + J + L. ● In the CMI calculation formula, if there is coefficient before D, J, or L, the product of D, J, or L and the coefficient must be respectively smaller than or equal to 5000, 3000, and 1000. For example, when *cmi-method* is set to 10*D + 10*J + 10*L, the delay is 1000 ms, jitter is 100 ms, and packet loss rate is 10‰, the CMI is calculated as follows: CMI = 9000 − (5000 + 1000 + 100) = 2900 This is because 10 x D is 10000, which exceeds the maximum value of 5000 and can only be calculated as 5000.	The value is a string of 1 to 20 case-insensitive characters. The value contains only digits, plus sign (+), asterisk (*), slash (/), and letters (only D, d, J, j, L, or l). Only the plus operator (+) can be used among parameters D, J, and L. These parameters can be multiplied or divided by a positive integer. For example: ● 10*D ● D*10+J/10 ● D*100+J*10+L/10 **NOTE** D or d indicates the delay, J or j indicates the jitter, and L or l indicates the packet loss rate.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to customize the CMI calculation formula based on the service requirements. SPR determines link quality based on the CMI value and selects an optimal link to forward service data flows.

Precautions

The CMI threshold changes after you run the **cmi-method** command. The minimum CMI threshold is the value calculated in the CMI calculation formula using the thresholds of the delay, jitter, and packet loss rate. The maximum value is 9000.

Example

Set the CMI calculation formula of service profile **spr1** to 9000 − (D + J).

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] cmi-method d+j
```

Related Topics

9.11.58 set cmi threshold

9.11.12 description (service profile view)

Function

The **description** command configures the description for a service profile in the SPR.

The **undo description** command deletes the description of a service profile in the SPR.

By default, no description is configured for a service profile in the SPR.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description for a service profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

This command configures the description of a service profile, helping differentiate service profiles.

Example

Set the description of service profile **spr1** to **testspr**.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] description testspr
```

Related Topics

9.11.56 service-map

9.11.13 display ip policy-based-route

Function

The **display ip policy-based-route** command displays the policy of local PBR applied to the local device.

Format

display ip policy-based-route

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the policy of local PBR applied on the local device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ip policy-based-route
 Policy Name          Interface
 aaa                  local
```

Table 9-234 Description of the display ip policy-based-route command output

Item	Description
Policy Name	Name of a local PBR. To set this parameter, run the **9.11.27 ip local policy-based-route** command.
Interface	local: indicates the local PBR, that is, apply PBR to the packets sent from the local host rather than the packet forwarded by the local host.

Related Topics

9.11.27 ip local policy-based-route

9.11.14 display ip policy-based-route setup

Function

The **display ip policy-based-route setup** command displays the configurations of local PBR.

Format

display ip policy-based-route setup local [**verbose**]

display ip policy-based-route setup interface *interface-type interface-number* [**verbose**]

Parameters

Parameter	Description	Value
local	Displays the configurations of the local PBR on the local device.	-
interface *interface-type interface-number*	Displays the type and the number of the interface enabled with PBR.	-
verbose	Displays the details about the local PBR.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip policy-based-route setup** command to display the configurations of PBR.

Example

Display the configurations of PBR on the local device.

```
<Huawei> display ip policy-based-route setup local
 policy-based-route policy1 permit node 10
 if-match acl 3000
 if-match packet-length  1000  2000
 apply ip-precedence critical (5)
 apply access-vpn vpn-instance vpn1 vpn2 vpn3 vpn4 vpn5 VPN5
 apply output-interface GigabitEthernet0/0/1
 apply ip-address next-hop 4.4.4.4 1.1.1.1
 apply default output-interface GigabitEthernet0/0/0
 apply ip-address default next-hop 2.2.2.2 3.3.3.3
 policy-based-route policy1 permit node 20
 if-match packet-length  3000  65535
 policy-based-route policy1 permit node 30
 if-match packet-length  2001  2999
```

Table 9-235 Description of the display ip policy-based-route setup command output

Item	Description
policy-based-route	Name, mode, and number of a PBR node. To set these parameters, run the **9.11.44 policy-based-route** command.
if-match acl	Matching rules based on IP addresses. To set this parameter, run the **9.11.23 if-match acl (policy-based route view)** command.
if-match packet-length	Matching rules based on IP packet length. To set this parameter, run the **9.11.24 if-match packet-length** command.
apply ip-precedence	Priority of IP packets. To set this parameter, run the **9.11.7 apply ip-precedence (policy-based route view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
apply access-vpn vpn-instance	VPN instances for forwarding packets. To set this parameter, run the **9.11.1 apply access-vpn** command.
apply output-interface	Outbound interface for sending packets. To set this parameter, run the **9.11.8 apply output-interface** command.
apply ip-address next-hop	Next hop of forwarded packets. To set this parameter, run the **9.11.5 apply ip-address next-hop (policy-based route view)** command.
apply default output-interface	Default outbound interface for sending packets. To set this parameter, run the **9.11.2 apply default output-interface** command.
apply ip-address default next-hop	Default next hop of forwarded packets. To set this parameter, run the **9.11.4 apply ip-address default next-hop** command.

Related Topics

9.11.27 ip local policy-based-route

9.11.15 display ip policy-based-route statistics local

Function

The **display ip policy-based-route statistics local** command displays packet statistics of the local PBR.

Format

display ip policy-based-route statistics local

display ip policy-based-route statistics interface *interface-num interface-type*

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run this command to view statistics about matched packet forwarding in each PBR node of the local PBR enabled on the device.

Example

Display packet statistics of the local PBR.

```
<Huawei> display ip policy-based-route statistics local
 Local policy based routing information:
 policy-based-route: pbr1
   permit node 1
     apply output-interface Ethernet1/0/0
       Denied: 0,
       Forwarded: 0
   permit node 2
     apply output-interface Ethernet1/0/1
       Denied: 0,
       Forwarded: 0
 Total denied: 0, forwarded: 0
```

Table 9-236 Description of the display ip policy-based-route statistics local command output

Item	Description
policy-based-route	Name of a local PBR. To set this parameter, run the **9.11.44 policy-based-route** command.
permit node	Number of a PBR node. A smaller number indicates a higher priority of the corresponding PBR node. To set this parameter, run the **9.11.44 policy-based-route** command.
apply output-interface	Outbound interface.
Total denied	Number of unforwarded packets.
forwarded	Number of forwarded packets.

Related Topics

9.11.27 ip local policy-based-route

9.11.16 display ip policy-based-route statistics

Function

The **display ip policy-based-route statistics** command displays the statistics of PBR.

 Copyright © Huawei Technologies Co., Ltd.

Format

display ip policy-based-route statistics interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface	Collects statistics of PBR enabled on the specified interface.	-
interface-type	Specifies the type of the interface enabled with PBR.	-
interface-number	Specifies the number of the interface enabled with PBR.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the statistics of PBR enabled on the specified interface.

```
<Huawei> display ip policy-based-route statistics interface gigabitethernet 1/0/0
Interface GigabitEthernet1/0/0 policy routing information:
 policy-based-route: test
   permit node 10
     apply output-interface GigabitEthernet1/0/0
       Denied: 0,
       Forwarded: 0
   permit node 20
     apply output-interface GigabitEthernet1/0/0
       Denied: 0,
       Forwarded: 0
 Total denied: 0, forwarded: 0
```

Table 9-237 Description of the **display ip policy-based-route statistics** command output

Item	Description
policy-based-route	Displays the name of PBR.
permit node	Displays the permitted node number. The smaller the node number is, the earlier the corresponding policy is applied.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
apply output-interface	Displays the outbound interface.
Total denied	Displays the number of the packets unavailable to be forwarded.
forwarded	Displays the number of the forwarded packets.

9.11.17 display policy-based-route

Function

The **display policy-based-route** command displays configurations of created local PBRs.

Format

display policy-based-route [*policy-name* [**verbose**]]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a local PBR.	The value is a string of 1 to 19 case-sensitive characters without spaces.
verbose	Displays detailed information about the specified PBR.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view configurations of created local PBRs.

When using this command, note the following points:

- If no parameter is specified in this command, configurations of all created local PBRs are displayed. Before enabling a local PBR, run this command to view configurations of all created local PBRs.
- If a local PBR is specified in this command, configurations of the local PBR are displayed. After configuring a local PBR, run this command to view configurations of the local PBR.

Example

Display configurations of all created local PBRs.

```
<Huawei> display policy-based-route
 policy-based-route : policy1
  Node  10  permit :
    if-match acl 3000
    if-match packet-length  1000  2000
    apply ip-precedence critical (5)
    apply access-vpn vpn-instance vpn1 vpn2 vpn3 vpn4 vpn5 VPN5
    apply output-interface GigabitEthernet0/0/1
    apply ip-address next-hop 4.4.4.4 1.1.1.1
    apply ip-address default next-hop 2.2.2.2 3.3.3.3
  Node  20  permit :
    if-match packet-length  3000  65535
  Node  30  deny :
    if-match packet-length  2001  2999
```

Table 9-238 Description of the display policy-based-route command output

Item	Description
policy-based-route	Name of a local PBR. To set this parameter, run the **9.11.44 policy-based-route** command.
Node	Number of a PBR node. A smaller number indicates a higher priority of the corresponding PBR node. To set this parameter, run the **9.11.44 policy-based-route** command.
permit,deny	Mode of a PBR node. • permit: indicates PBR is enabled for matched packets. • deny: indicates PBR is disabled for matched packets. To set this parameter, run the **9.11.44 policy-based-route** command.
if-match acl	Matching rules based on IP addresses. To set this parameter, run the **9.11.23 if-match acl (policy-based route view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
if-match packet-length	Matching rules based on IP packet length. To set this parameter, run the **9.11.24 if-match packet-length** command.
apply ip-precedence	Priority of IP packets. To set this parameter, run the **9.11.7 apply ip-precedence (policy-based route view)** command.
apply access-vpn vpn-instance	VPN instances for forwarding packets. To set this parameter, run the **9.11.1 apply access-vpn** command.
apply output-interface	Outbound interface for sending packets. To set this parameter, run the **9.11.8 apply output-interface** command.
apply ip-address next-hop	Next hop of forwarded packets. To set this parameter, run the **9.11.5 apply ip-address next-hop (policy-based route view)** command.
apply ip-address default next-hop	Default next hop of forwarded packets. To set this parameter, run the **9.11.4 apply ip-address default next-hop** command.

Related Topics

9.11.44 policy-based-route

9.11.18 display smart-policy-route

Function

The **display smart-policy-route** command displays SPR routing configurations.

Format

display smart-policy-route [**link-path** [*path-name*]]

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring SPR, run the **display smart-policy-route** command to view SPR routing configurations. You can run the **display smart-policy-route link-path** command to view the link-path configuration on the device.

Before applying SPR to new services, you can run this command to check whether the current SPR configurations meet new service requirements.

Example

Display SPR routing configurations.

```
<Huawei> display smart-policy-route
-------------------------------------------------------------------------------
Period          :  10
WTRPeriod       :  0( seconds )
FlappingValue   :  20
BackupName      :  GigabitEthernet0/0/2
Backup-NhpIp    :  19.0.0.2

BackupIpv6Name  :  GigabitEthernet0/0/0
Backup-NhpIpv6  :  fc01::15B:E0EA:3524:E791
-------------------------------------------------------------------------------
```

Table 9-239 Description of the **display smart-policy-route** command output

Item	Description
Period	SPR switchover period. To set this parameter, run the **9.11.43 period** command.
WTRPeriod	Waiting time before traffic is switched from the backup link to the primary link. To set the time, run the **9.11.66 wtr period** command.
FlappingValue	Flapping suppression period. To set this parameter, run the **9.11.54 route flapping suppression** command.
BackupName	Name of the IPv4 outbound interface of the best-effort link. To set this parameter, run the **9.11.9 backup-interface** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Backup-NhpIp	Next-hop IPv4 address of the outbound interface of the best-effort link. To set this parameter, run the **9.11.9 backup-interface** command.
BackupIpv6Name	Name of the IPv6 outbound interface of the best-effort link. To set the next-hop IPv6 address, run the **9.11.10 backup-ipv6-interface** command.
Backup-NhpIpv6	Next-hop IPv6 address of the outbound interface of the best-effort link. To set the next-hop IPv6 address, run the **9.11.10 backup-ipv6-interface** command.

Display the link-path configuration on the device.

```
<Huawei> display smart-policy-route link-path
SPR link-path
-------------------------------------------------------------------------------
link-path                    link-name                    Peer
-------------------------------------------------------------------------------
aaa                        GigabitEthernet0/0/3         3.3.3.3
bbb                        GigabitEthernet0/0/4         4.4.4.4
Route_to_PC                    Tunnel0/0/0               10.1.1.1
-------------------------------------------------------------------------------
```

Table 9-240 Description of the **display smart-policy-route link-path** command output

Item	Description
link-path	Name of the link-path detection link.
link-name	Local interface of the link-path detection link.
Peer	Peer address of the link-path detection link.

Related Topics

9.11.63 smart-policy-route
9.11.19 display smart-policy-route link-state
9.11.21 display smart-policy-route service-map
9.11.9 backup-interface

9.11.19 display smart-policy-route link-state

Function

The **display smart-policy-route link-state** command displays the detection link status of SPR.

Format

display smart-policy-route link-state [*interface-type interface-number* | **link-path** *path-name*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface for a detection link. When no interface is specified for a detection link, this command displays the status of all detection links. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
link-path *path-name*	Specifies a detection link as a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays detection link quality parameters, including the delay, jitter, interface that can be automatically shut down when the detection link is not selected in SPR, delay in automatically shutting down the interface, and packet

loss rate. When no interface is specified for a detection link, this command displays the status of all detection links.

Example

Display the status of all detection links.

```
<Huawei> display smart-policy-route link-state
-------------------------------------------------------------------------------
link-name                          Delay    Jitter   Loss
-------------------------------------------------------------------------------
GigabitEthernet0/0/1                   2         2       0
GigabitEthernet0/0/0                   2         2       0
-------------------------------------------------------------------------------
```

Display the status of GE0/0/1 of the detection link.

```
<Huawei> display smart-policy-route link-state gigabitethernet 0/0/1
-------------------------------------------------------------------------------
Delay            : 2
Loss             : 0
Jitter           : 2
Congestion       : 2
StandbyFlag      : ENABLE
StandbyShutDown  : UP
-------------------------------------------------------------------------------
Service Name:1                                  CMI:20
Service Name:2                                  CMI:4
Service Name:3                                  CMI:4
-------------------------------------------------------------------------------
```

Table 9-241 Description of the **display smart-policy-route link-state** command output

Item	Description
link-name	Interface name of a detection link.
Delay	Delay of the detection link.
Loss	Packet loss rate of the detection link.
Jitter	Jitter of the detection link.
StandbyFlag	Whether the function that automatically shuts down an interface when the detection link is not selected in SPR is enabled: ● ENABLE: The function is enabled. ● DISABLED: The function is disabled. To configure the function, run the **9.11.64 standby-interface (smart-policy-route view)** command.

Item	Description
StandbyShutDown	Status of the interface that is automatically shut down when the detection link is not selected in SPR: ● UP: The interface is automatically activated. ● DOWN: The interface is automatically shut down.
Congestion	Congestion value.
Service Name	Name of the service. To set this parameter, run the **9.11.56 service-map** command. **NOTE** Different services can be configured with different CMI calculation formulas.
CMI	Composite measure indicator.

Related Topics

9.11.18 display smart-policy-route

9.11.21 display smart-policy-route service-map

9.11.20 display smart-policy-route nqa-server link-state

Function

The **display smart-policy-route nqa-server link-state** command displays the NQA server link status.

NOTE

Only the AR2204XE, AR2204XE-DC, and the AR2240 and AR3260 that have the SRU80, SRU100E, SRU200, SRU200E, SRUX5 or SRU400 support this command.

Format

display smart-policy-route nqa-server link-state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display smart-policy-route nqa-server link-state** command displays the NQA server link status.

Example

Display the NQA server link status.

```
<Huawei> display smart-policy-route nqa-server link-state
-----------------------------------------------------------------------------
link-name                        Delay      Jitter     Loss
-----------------------------------------------------------------------------
GigabitEthernet1/0/0               12          7         0
GigabitEthernet2/0/0               12          7         0
-----------------------------------------------------------------------------
```

Table 9-242 Description of the display smart-policy-route nqa-server link-state command output

Item	Description
link-name	Interface name of the NQA server link.
Delay	Delay on the NQA server link.
Loss	Packet loss ratio on the NQA server link.
Jitter	Jitter on the NQA server link.

Related Topics

9.11.41 nqa-server

9.11.19 display smart-policy-route link-state

9.11.21 display smart-policy-route service-map

Function

The **display smart-policy-route service-map** command displays the configuration of a service profile in SPR.

Format

display smart-policy-route service-map [*name*]

Parameters

Parameter	Description	Value
name	Displays the configuration of a specified service profile. If no service profile is specified, configurations of all service profiles are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When using this command, note the following points:

- If no parameter is specified in this command, configurations of all service profiles are displayed.
- If a service profile is specified in this command, configurations of the service profile are displayed, including service flows bound to the service profile, thresholds for link quality parameters, active link group, and standby link group.

Example

Display configurations of all service profiles.

```
<Huawei> display smart-policy-route service-map
SPR service-map
-------------------------------------------------------------------------------
service Name                  CurLink Name
-------------------------------------------------------------------------------
map1                          GigabitEthernet0/0/0
-------------------------------------------------------------------------------
```

Display the configuration of service profile **map1**.

```
<Huawei> display smart-policy-route service-map map1
-------------------------------------------------------------------------------
Match acl          : 3001
DelayThreshold     : 5000
LossThreshold      : 1000
JitterThreshold    : 1000
CmiThreshold       : 0
WTRRemainTime(s)   : 0
GroupName          : 3
BackupGroupName    : 4
Description        :
Cmi-Method         : d*10+l*5+j*10
```

```
CurLinkName       : Tunnel0/0/0
-----------------------------------------------------------------------------
```

Table 9-243 Description of the display smart-policy-route service-map command output

Item	Description
service Name	Names of all service profiles. To set this parameter, run the **9.11.56 service-map** command.
CurLink Name	Currently used link.
Match acl	ACL for matching service flows. To set this parameter, run the **9.11.35 match acl** command.
DelayThreshold	Delay threshold. To set this parameter, run the **9.11.59 set delay threshold** command.
LossThreshold	Packet loss rate threshold. To set this parameter, run the **9.11.62 set loss threshold** command.
JitterThreshold	Jitter threshold. To set this parameter, run the **9.11.60 set jitter threshold** command.
CmiThreshold	CMI threshold. To set this parameter, run the **9.11.58 set cmi threshold** command.
WTRRemainTime(s)	Remaining time until traffic is switched from the backup link to the primary link. To set the parameter, run the **9.11.66 wtr period** command.
GroupName	Name of the active link group. To set this parameter, run the **9.11.61 set link-group** command.
BackupGroupName	Name of the standby link group. To set this parameter, run the **9.11.61 set link-group** command.
Description	Service profile description. To set this parameter, run the **9.11.12 description (service profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Cmi-Method	CMI calculation formula. To set this parameter, run the **9.11.11 cmi-method** command.
CurLinkName	Currently used link.

Related Topics

9.11.56 service-map
9.11.18 display smart-policy-route
9.11.19 display smart-policy-route link-state

9.11.22 display smart-policy-route redirect-link link-state

Function

The **display smart-policy-route redirect-link link-state** command displays the SPR redirect link status.

Format

display smart-policy-route redirect-link link-state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A redirect link can be configured to send traffic from a specified next hop. To view the redirect link status, including the delay, jitter, and packet loss rate, run the **display smart-policy-route redirect-link link-state** command.

Prerequisites

An SPR redirect link has been configured to redirect packets to the specified link using the **redirect-link** { *interface-type interface-number* | *interface-name* | **link-path** *path-name* } *next-hop-address* command.

Example

Display the SPR redirect link status.

```
<Huawei> display smart-policy-route redirect-link link-state
--------------------------------------------------------------------------------
nqa-redirect link          NhpAddress        Delay    Jitter   Loss
--------------------------------------------------------------------------------
GigabitEthernet0/0/4       192.168.3.1        2        2        0
--------------------------------------------------------------------------------
```

Table 9-244 Description of the **display smart-policy-route redirect-link link-state** command output

Item	Description
nqa-redirect link	Interface name for the redirect link.
NhpAddress	Next-hop address.
Delay	Redirect link delay.
Jitter	Redirect link jitter.
Loss	Redirect link packet loss rate.

Related Topics

9.11.52 redirect-link

9.11.23 if-match acl (policy-based route view)

Function

The **if-match acl** command configures a matching rule of IP addresses in the local PBR.

The **undo if-match acl** command deletes the matching rule of IP addresses in the local PBR.

By default, no matching rule of IP addresses is configured in the local PBR.

Format

if-match acl *acl-number*

undo if-match acl

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the ACL number.	The value is an integer ranging from 2000 to 3999. The number of a basic ACL ranges from 2000 to 2999, and the number of an advanced ACL ranges from 3000 to 3999.

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to define a matching rule of IP addresses in the local PBR.

Precautions

If you run this command multiple times for the same PBR node, only the latest configuration takes effect.

Example

Apply PBR to packets matching ACL 2000.

```
<Huawei> system-view
[Huawei] policy-based-route policy1 permit node 10
[Huawei-policy-based-route-policy1-10] if-match acl 2000
```

Related Topics

9.11.44 policy-based-route

9.11.24 if-match packet-length

Function

The **if-match packet-length** command configures a matching rule of IP packet length in the local PBR.

The **undo if-match packet-length** command deletes the matching rule of IP packet length in the local PBR.

 Copyright © Huawei Technologies Co., Ltd.

By default, no matching rule of IP packet length is configured in the local PBR.

Format

if-match packet-length *min-length max-length*

undo if-match packet-length

Parameters

Parameter	Description	Value
min-length	Specifies the minimum length of IP packets.	The value is an integer ranging from 0 to 65535, in bytes.
max-length	Specifies the maximum length of IP packets.	The value is an integer ranging from 1 to 65535, in bytes. The value of *min-length* must be smaller than the value of *max-length*.

Views

Policy-based route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When defining a matching rule of IP packet length, run the **if-match packet-length** *min-length max-length* command to specify the IP packet length range.

Precautions

If you run this command in the same PBR node multiple times, only the latest configuration takes effect.

Example

Apply PBR to packets that have 100 to 200 bytes.

```
<Huawei> system-view
[Huawei] policy-based-route map1 permit node 10
[Huawei-policy-based-route-map1-10] if-match packet-length 100 200
```

Related Topics

9.11.44 policy-based-route

9.11.25 ip policy-based-route

Function

The **ip policy-based-route** command enables PBR on an MPLS TE interface.

The **undo ip policy-based-route** command disables PBR on the MPLS TE interface.

By default, disable PBR on the interface.

Format

ip policy-based-route *policy-name*

undo ip policy-based-route *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the policy name.	It is a string of 1 to 19 characters.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable PBR named AAA on GE 1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip policy-based-route AAA
```

9.11.26 ip policy-based-route refresh-time

Function

The **ip policy-based-route refresh-time** command sets the interval at which policy-based local PBR updates LSPs.

The **undo ip policy-based-route refresh-time** command restores the default interval at which local PBR updates LSPs.

By default, the interval at which local PBR updates LSPs is 5000 ms.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip policy-based-route refresh-time [*refreshtime-value*]

undo ip policy-based-route refresh-time

Parameters

Parameter	Description	Value
refreshtime-value	Specifies the value of the refresh timer.	The value is an integer that ranges from 1000 to 65535, in milliseconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To speed up packet forwarding, PBR must save forwarding information for LSPs. The forwarding information changes according to the network status change. When the network status changes, the forwarding information for LSPs also needs to be updated. In this situation, you can use the **ip policy-based-route refresh-time** *refreshtime-value* command to set the interval at which PBR updates LSPs.

Example

Set the interval at which PBR updates LSPs to 4000 ms.

```
<Huawei> system view
[Huawei] ip policy-based-route refresh-time 4000
```

9.11.27 ip local policy-based-route

Function

The **ip local policy-based-route** command enables the local PBR.

The **undo ip local policy-based-route** command disables the local PBR.

By default, the local PBR is disabled.

Format

ip local policy-based-route *policy-name*

undo ip local policy-based-route [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a local PBR.	The value is a string of 1 to 19 case-sensitive characters without spaces.

Views

System view, Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **ip local policy-based-route** command to enable the local PBR that applies only to locally generated packets.

Precautions

If you run the **ip local policy-based-route** command multiple times, only the latest configuration takes effect.

Example

Enable local PBR named **AAA**.

```
<Huawei> system-view
[Huawei] ip local policy-based-route AAA
```

Related Topics

9.11.44 policy-based-route

9.11.28 ip local route-based-source enable

Function

The **ip local route-based-source enable** command enables a router to select an outbound interface to forward a locally generated packet based on the packet's source IP address when there are multiple upstream equal-cost routes.

The **undo ip local route-based-source enable** command disables a router from selecting an outbound interface to forward a locally generated packet based on the packet's source IP address when there are multiple upstream equal-cost routes.

 Copyright © Huawei Technologies Co., Ltd.

By default, a router selects an outbound interface to forward a locally generated packet based on the packet's source IP address when there are multiple upstream equal-cost routes.

NOTE

This command is supported only in V200R010C10 and later versions.

Format

ip local route-based-source enable

undo ip local route-based-source enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ip local route-based-source enable** command to enable a router to select an outbound interface to forward a locally generated packet based on the packet's source IP address when there are multiple upstream equal-cost routes.

Example

Enable a router to select an outbound interface to forward a locally generated packet based on the packet's source IP address when there are multiple upstream equal-cost routes.

```
<Huawei> system-view
[Huawei] ip local route-based-source enable
```

9.11.29 ip route re-search acl

Function

The **ip route re-search acl** command enables the SPR function for IPv4 protocol packets generated on a device.

The **undo ip route re-search acl** command disables the SPR function for IPv4 protocol packets generated on a device.

By default, the SPR function is disabled for IPv4 protocol packets generated on a device.

 Copyright © Huawei Technologies Co., Ltd.

The following protocols support this command: DNS, HTTP, HWTACACS, ICMP, RADIUS, SNMP, SSH, Telnet, BGP, GRE (GRE-KeepAlive), UDP (UDP-Helper), NQA, NHRP, CAPWAP, and SSL VPN.

Format

ip route re-search acl *acl-number*

undo ip route re-search acl

Parameters

Counter	Description	Value
acl-number	Specifies the number of an ACL. It is configured using the **acl** [**number**] *acl-number* [**match-order** { **auto** | **config** }] command.	The value is an integer that ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the SPR function cannot be enabled for IPv4 protocol packets generated on a device. For example, when POTS phones are directly connected through FXS interfaces on the device, the device converts voice signals on the phones into voice packets. These voice packets do not support the SPR function. When the quality of the voice transmission link changes, the service data link must be dynamically switched to ensure voice quality. In this case, run the **ip route re-search acl** command to enable the SPR function for IPv4 protocol packets generated on the device.

Before applying the SPR function to IPv4 protocol packets generated on the device, you must run the **rule (advanced ACL view)** command to create an ACL and then run the **match acl** command to bind SPR to the ACL.

Precautions

The ACL number of protocol packets enabled with SPR must be the same as the ACL number specified in **match acl** *acl-number*.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the SPR function for HTTP packets generated on a device.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 1 permit 80
[Huawei-acl-adv-3000] quit
[Huawei] ip route re-search acl 3000
```

Related Topics

19.7.4 acl (system view)

9.11.35 match acl

19.7.16 rule (advanced ACL view)

9.11.30 ipv6 route re-search acl

Function

The **ipv6 route re-search acl** command enables the SPR function for IPv6 protocol packets generated on the device.

The **undo ipv6 route re-search acl** command disables the SPR function for IPv6 protocol packets generated on the device.

By default, the SPR function is disabled for IPv6 protocol packets generated on a device.

The following commands support this command: DNSv6, SSH, TELNET, SNMP, ICMPv6, and BGP4+.

Format

ipv6 route re-search acl *acl6-number*

undo ipv6 route re-search acl

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL.	The value is an integer that ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

By default, the SPR function cannot be enabled for IPv6 protocol packets generated on a device. For example, when POTS phones are directly connected through FXS interfaces on the device, the device converts voice signals on the phones into voice packets. These voice packets do not support the SPR function. When the quality of the voice transmission link changes, the service data link must be dynamically switched to ensure voice quality. In this case, run the **ip route re-search acl** command to enable the SPR function for IPv6 protocol packets generated on the device.

Before applying the SPR function to IPv6 protocol packets generated on the device, you must run the **rule (advanced ACL6 view)** command to create an IPv6 ACL and then run the **match acl ipv6** command to bind SPR to the IPv6 ACL.

Precautions

- Before running the **ipv6 route re-search acl** command, you can run the **display acl ipv6** command to check whether the ACL used to match service traffic exists. If not, run the **acl ipv6** command to create an IPv6 ACL that needs to be bound to the service profile of SPR.
- The IPv6 ACL number used in the **ipv6 route re-search acl** command must be the same as that configured in the **match acl ipv6** *acl6-number* command.
- If you run the **ipv6 route re-search acl** command multiple times, only the latest configuration takes effect.

Example

Enable the SPR function for HTTP packets generated on a device.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule 1 permit 80
[Huawei-acl6-adv-3000] quit
[Huawei] ipv6 route re-search acl 3000
```

Related Topics

19.7.17 rule (advanced ACL6 view)

9.11.36 match acl ipv6

19.7.8 display acl ipv6

19.7.2 acl ipv6 (system view)

9.11.31 link-group

Function

The **link-group** command creates a link group of SPR and displays the link group view.

The **undo link-group** command deletes a link group.

By default, no link group is created for SPR.

Format

link-group *name*

undo link-group *name*

Parameters

Parameter	Description	Value
name	Specifies name of a link group.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Smart policy routing view

Default Level

2: Configuration level

Usage Guidelines

In practice, services have different requirements for links. To improve link efficiency, add detection links to link groups.

Example

Create a link group named **group1** and enter the link group view.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] link-group group1
[Huawei-smart-policy-route-link-group-group1]
```

Related Topics

9.11.32 link-member

9.11.61 set link-group

9.11.32 link-member

Function

The **link-member** command adds a detection link to a link group of SPR.

The **undo link-member** command deletes a detection link from a link group of SPR.

By default, detection links are not added to the link group.

Format

link-member { *interface-type interface-number* | **link-path** *path-name* } &<1-8>

undo link-member { *interface-type interface-number* | **link-path** *path-name* } &<1-8>

undo link-member all

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and interface number of a detection link. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
link-path *path-name*	Specifies a detection link as a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
all	Indicates all the interfaces of a detection link.	-

Views

Link group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command adds a detection link to a link group. Then an SPR service profile can be bound to the link group to associate services with the detection link.

Prerequisites

A detection link has been configured using the **prober** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Add GE1/0/0 of the detection link to link group **group1**.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] link-group group1
[Huawei-smart-policy-route-link-group-group1] link-member gigabitethernet 1/0/0
```

Add the link-path link **Link_1** to the link group **group1**.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] link-group group1
[Huawei-smart-policy-route-link-group-group1] link-member link-path Link_1
```

Related Topics

9.11.45 prober
9.11.31 link-group

9.11.33 link-path

Function

The **link-path** command creates a link-path link in SPR.

The **undo link-group** command deletes a link-path link in SPR.

By default, no link-path link is created in SPR.

Format

link-path *path-name* { *interface-name* | *interface-type interface-number* } **peer** *ip-address*

undo link-path *path-name*

undo link-path all

Parameters

Parameter	Description	Value
path-name	Specifies the name for a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
interface-name	Specifies the local interface name for a link-path link.	The value range depends on the interface type and slot ID. **NOTE** Only the tunnel interface type is supported.

Parameter	Description	Value
interface-type interface-number	Specifies the local interface type and number for a link-path link.	The value range depends on the interface type and slot ID.
peer *ip-address*	Specifies the peer IP address of a link-path link.	The value is in dotted decimal notation.

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

When there are point-to-multipoint (P2MP) links (used to transmit DSVPN services for example) on the network, a link needs to be selected based on the local interface and peer IP address to transmit data. The **link-path** command can create a link-path link based on the local interface and peer IP address to implement SPR.

Example

Create the link-path link **Link_1** and set the local interface name and peer IP address to Tunnel0/0/0 and 10.1.1.1.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] link-path Link_1 tunnel0/0/0 peer 10.1.1.1
```

Related Topics

9.11.18 display smart-policy-route

9.11.32 link-member

9.11.34 match

Function

The **match** command binds an SPR service profile to an IPv4 ACL or SA application protocol.

The **undo match** command unbinds an SPR service profile from an IPv4 ACL or SA application protocol.

By default, an SPR service profile is not bound to an IPv4 ACL or SA application protocol.

 Copyright © Huawei Technologies Co., Ltd.

Format

match [**acl** { *acl-number* | *acl-name* }] **application** *application-name*

undo match [**acl** { *acl-number* | *acl-name* }] [**application** *application-name*]

match acl *acl-name*

undo match acl *acl-name*

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies an ACL number.	The value is an integer that ranges from 2000 to 3999. A basic ACL number ranges from 2000 to 2999, and an advanced ACL number ranges from 3000 to 3999.
acl *acl-name*	Specifies an ACL name.	The value is a string of 1 to 32 case-sensitive characters without spaces.
application *application-name*	Specifies the name of an SA application protocol.	The value is a string of characters without spaces. The value depends on application protocols in the signature database. You can run the **display sa application-list** command to view the value.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ACLs or application protocols can define different service flows. The **match** command can bind an SPR service profile to an ACL or application protocol to implement SPR based on the ACL or application protocol.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A service profile has been created in SPR using the **service-map** command.

Deep security defense has been enabled and the SA signature file has been loaded using the **engine enable** command.

Precautions

- Before running the **match** command, ensure that *acl-number* or *acl-name* specifies an existing ACL number or name. You can run the **display acl** command to check whether the ACL used to match service traffic already exists. If not, run the **acl** or **acl name** command to create an ACL that needs to be bound to the SPR service profile.
- When you run the **undo match** command, the ACL number, ACL name, and application protocol name specified by *acl-number*, *acl-name*, and *application-name* must have been bound to the SPR service profile.
- If you run the **match** command multiple times, all the configurations take effect.

Example

Bind the service profile **spr1** to an ACL 3000 and SA application protocol **163disk**.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] match acl 3000 application 163disk
```

Related Topics

9.11.56 service-map

19.7.7 display acl

19.7.4 acl (system view)

9.11.35 match acl

Function

The **match acl** command binds an IPv4 ACL to a service profile of SPR.

The **undo match acl** command unbinds an IPv4 ACL from a service profile of SPR.

By default, no IPv4 ACL is bound to a service profile of SPR.

Format

match acl *acl-number* &<1-10>

undo match acl *acl-number* &<1-10>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the ACL number.	The value is an integer ranging from 2000 to 3999. The number of a basic ACL ranges from 2000 to 2999, and the number of an advanced ACL ranges from 3000 to 3999.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ACLs can define different service flows. You can run the **match acl** command to bind an IPv4 ACL to a service profile of SPR for route selection.

Prerequisites

The service profile has been configured using the **service-map** command.

Precautions

- Before running the **match acl** command, ensure that the IPv4 ACL has been created. You can run the **display acl** command to check whether the IPv4 ACL used to match service traffic exists. If not, run the **acl** command to create an IPv4 ACL that needs to be bound to the service profile of SPR.
- Before you run the **undo match acl** command, the IPv4 ACL specified by *acl-number* must have been bound to the service profile of SPR.
- If you run the **match acl** command multiple times, all the configurations take effect.

Example

Bind service profile **spr1** to an ACL.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] match acl 2000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.11.56 service-map
19.7.7 display acl
19.7.4 acl (system view)

9.11.36 match acl ipv6

Function

The **match acl ipv6** command binds an IPv6 ACL to a service profile of SPR.

The **undo match acl ipv6** command unbinds an IPv6 ACL from a service profile of SPR.

By default, no IPv6 ACL is bound to a service profile of SPR.

Format

match acl ipv6 *acl6-number* &<1-10>

undo match acl ipv6 *acl6-number* &<1-10>

Parameters

Parameter	Description	Value
acl6-number	Specifies the IPv6 ACL number. **NOTE** You can create a maximum of 10 IPv6 ACLs.	The value is an integer ranging from 2000 to 3999. The number of a basic ACL ranges from 2000 to 2999, and the number of an advanced ACL ranges from 3000 to 3999.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ACLs can define different service flows. You can run the **match acl ipv6** command to bind an IPv6 ACL to a service profile of SPR for route selection.

Prerequisites

The service profile has been configured using the **service-map** command.

Precautions

- Before running the **match acl ipv6** command, ensure that the IPv6 ACL has been created. You can run the **display acl ipv6** command to check whether the IPv6 ACL used to match service traffic exists. If not, run the **acl ipv6** command to create an IPv6 ACL that needs to be bound to the service profile of SPR.
- Before you run the **undo match acl ipv6** command, the IPv6 ACL specified by *acl6-number* must have been bound to the service profile of SPR.
- IPv4 and IPv6 ACLs cannot be bound to the same SPR service profile.
- If you run the **match acl ipv6** command multiple times, all the configurations take effect.

Example

Bind service profile **spr1** to an IPv6 ACL.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] match acl ipv6 2000
```

Related Topics

9.11.56 service-map

19.7.8 display acl ipv6

19.7.2 acl ipv6 (system view)

9.11.37 nqa-client

Function

The **nqa-client** command specifies an NQA client port number.

The **undo nqa-client** command deletes an NQA client port number.

By default, an NQA client port number is not configured.

Format

nqa-client { *interface-type interface-number* | **link-path** *path-name* } **port** *port-num*

undo nqa-client { *interface-type interface-number* | **link-path** *path-name* }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
link-path *path-name*	Specifies a detection link as a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
port *port-num*	Specifies an NQA client port number.	The value is an integer that ranges from 1025 to 49151.

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The test result of an NQA test instance is saved on the NQA client, so the NQA client can select the optimal route based on the test result. To select an optimal route on the NQA server, create an NQA server link where the test result of an NQA test instance can be sent from the NQA client to the NQA server, and run the **nqa-client** command to configure an NQA client port number.

Prerequisites

A detection link has been configured using the **9.11.45 prober** command.

Precautions

The NQA client port number must be the same as the NQA server port number.

Example

Configure NQA client port 10000.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] nqa-client gigabitethernet 1/0/0 port 10000
```

Related Topics

9.11.45 prober

9.11.38 nqa-relay

Function

The **nqa-relay** command enables the device to send the NQA detection result of a detection link to all the members of an NQA-relay-group.

The **undo nqa-relay** command disables the device from sending the NQA detection result of a specified link to all the members of an NQA-relay-group.

By default, a device does not send the NQA detection result of a specified link to all the members of an NQA-relay-group.

Format

nqa-relay { *interface-type interface-number* | *interface-name* | **link-path** *path-name* } **nqa-relay-group** *group-name*

undo nqa-relay { *interface-type interface-number* | *interface-name* | **link-path** *path-name* | **all** }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number of a detection link: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	The value range depends on the interface type and slot ID.
interface-name	Specifies the interface number of a detection link.	The value range depends on the interface type and slot ID. **NOTE** Only the tunnel interface type is supported.
link-path *path-name*	Specifies a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
nqa-relay-group *group-name*	Specifies an NQA-relay-group.	The value is a string of 1 to 31 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

In a dual-gateway scenario, the gateway with the **nqa-relay** command configured can send the NQA detection result of a specified probe link to the remote gateway. The remote gateway can compare the received and local NQA detection results to implement SPR.

Example

Send the NQA detection result of **Link_1** to all the members of the NQA-relay-group **group1**.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] nqa-relay link-path Link_1 nqa-relay-group group1
```

Related Topics

9.11.39 nqa-relay-group

9.11.40 nqa-relay-member

9.11.39 nqa-relay-group

Function

The **nqa-relay-group** command creates an NQA-relay-group and displays its view.

The **undo nqa-relay-group** command deletes an NQA-relay-group in SPR.

By default, no NQA-relay-group is created in SPR.

Format

nqa-relay-group *group-name*

undo nqa-relay-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of an NQA-relay-group.	The value is a string of 1 to 31 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

Creating an NQA-relay-group can enable a device to send the NQA detection result of a specified probe link to multiple remote devices, improving SPR efficiency.

Example

Create the NQA-relay-group **group1** and enter its view.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] nqa-relay-group group1
[Huawei-smart-policy-route-nqa-relay-group-group1]
```

Related Topics

9.11.32 link-member

9.11.61 set link-group

9.11.40 nqa-relay-member

Function

The **nqa-relay-member** command adds the interface that sends the NQA detection result into an NQA-relay-group.

The **undo nqa-relay-member** command deletes the interface that sends the NQA detection result from an NQA-relay-group.

By default, the interface that sends the NQA detection result is added into an NQA-relay-group.

Format

nqa-relay-member { *interface-type interface-number* | *interface-name* } **destination** *dest-ip-address* **port** *port-num*

undo nqa-relay-member { *interface-type interface-number* | *interface-name* }

undo nqa-relay-member all

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number of a detection link: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	The value range depends on the interface type and slot ID.
interface-name	Specifies the interface number of a detection link.	The value range depends on the interface type and slot ID. **NOTE** Only the tunnel interface type is supported.
destination *dest-ip-address*	Specifies the destination IP address to which the NQA detection result is sent.	The value is in dotted decimal notation.
port *port-num*	Specifies the destination port number to which the NQA detection result is sent.	The value is an integer that ranges from 1025 to 49151.
all	Indicates interfaces of all detection links.	-

Views

NQA-relay-group view

Default Level

2: Configuration level

Usage Guidelines

You can run the **nqa-relay-member** command to add the interface that sends the NQA detection result into an NQA-relay-group. Using this NQA-relay-group, the device can send the NQA detection result of a specified probe link to multiple remote devices.

Example

Add Tunnel0/0/0 of a detection link into an NQA-relay group.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] nqa-relay-group group1
[Huawei-smart-policy-route-nqa-relay-group-group1] nqa-relay-member tunnel0/0/0 destination
10.1.1.1 port 1026
```

Related Topics

9.11.39 nqa-relay-group

9.11.38 nqa-relay

9.11.41 nqa-server

Function

The **nqa-server** command configures an NQA server link.

The **undo nqa-server** command deletes an NQA server link.

By default, no NQA server link is configured.

Format

nqa-server { *interface-type interface-number* | **link-path** *path-name* }

undo nqa-server { *interface-type interface-number* | **link-path** *path-name* | **all-interface** }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
link-path *path-name*	Specifies the name for a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
all-interface	Indicates all interfaces.	-

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The test result of an NQA test instance is saved on the NQA client, so the NQA client can select the optimal route based on the test result. To select an optimal route on the NQA server, create an NQA server link where the test result of an NQA test instance can be sent from the NQA client to the NQA server.

Follow-up Procedure

Run the **link-member** *interface-type interface-number* command to add the NQA server interface into a link group.

Example

Create an NQA server link.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] nqa-server gigabitethernet 1/0/0
```

Related Topics

9.11.42 nqa-server port

9.11.42 nqa-server port

Function

The **nqa-server port** command specifies an NQA server port number.

The **undo nqa-server port** command deletes an NQA server port number.

By default, an NQA server port number is not configured.

Format

nqa-server port *port-num*

undo nqa-server port

Parameters

Parameter	Description	Value
port-num	Specifies an NQA server port number.	The value is an integer that ranges from 1025 to 49151.

Views

Smart policy routing view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The test result of an NQA test instance is saved on the NQA client, so the NQA client can select the optimal route based on the test result. To select an optimal route on the NQA server, create an NQA server link where the test result of an NQA test instance can be sent from the NQA client to the NQA server, and run the **nqa-server port** command to configure an NQA server port number.

NOTE

The NQA server port number must be different from the port number of the NQA test instance.

Example

Configure NQA server port 10000.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] nqa-server port 10000
```

9.11.43 period

Function

The **period** command sets the SPR switchover period.

The **undo period** command restores the default SPR switchover period.

The default SPR switchover period is 60 seconds.

Format

period *period-value*

undo period

Parameters

Parameter	Description	Value
period-value	Specifies the SPR switchover period.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 60 seconds.

Views

Smart policy routing view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

SPR periodically obtains NQA test results to determine whether a link needs to be switched. If the optimal link calculated based on obtained NQA test results is not the currently used link, SPR starts the switchover timer. If the optimal link calculated based on obtained NQA test results is the currently used link before the switchover timer expires, SPR resets the timer and starts the timer the next time the two links become different. If the two links are always different before the switchover timer expires, SPR triggers a link switchover.

Set the SPR switchover period based on service characteristics. You can set a short switchover period for delay-sensitive services such as voice services.

Example

Set the SPR switchover period to 3600 seconds.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] period 3600
```

Related Topics

9.11.54 route flapping suppression

9.11.44 policy-based-route

Function

The **policy-based-route** command creates or modifies a policy and a PBR node of the local PBR and displays the local PBR view.

The **undo policy-based-route** command deletes a policy or a PBR node of the local PBR.

By default, no policy or PBR node is created for the local PBR.

Format

policy-based-route *policy-name* { **permit** | **deny** } **node** *node-id*

undo policy-based-route *policy-name* [**permit** | **deny** | **node** *node-id*]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a local PBR.	The value is a string of 1 to 19 case-sensitive characters without spaces.
permit	Indicates a PBR mode in which PBR is enabled for matched packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
deny	Indicates a PBR mode in which PBR is disabled for matched packets.	-
node *node-id*	Specifies the sequence number of a PBR node. A smaller number indicates a higher priority of the corresponding PBR node.	The value is an integer ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring local PBR, run the **policy-based-route** command to enter the local PBR view.

Example

Create a PBR named **pbr1** and PBR node 1, and specify PBR node 1 in **permit** mode.

```
<Huawei> system-view
[Huawei] policy-based-route pbr1 permit node 1
[Huawei-policy-based-route-pbr1-1]
```

Related Topics

9.11.17 display policy-based-route

9.11.45 prober

Function

The **prober** command configures an SPR detection link.

The **undo prober** command deletes an SPR detection link.

By default, no SPR detection link is configured.

Format

prober { *interface-type interface-number* | **link-path** *path-name* } **nqa** *admin-name test-name*

undo prober { *interface-type interface-number* | **link-path** *path-name* } **nqa** *admin-name test-name*

undo prober all

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and interface number of a detection link. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** The interface of a detection link must be a Layer 3 interface.	-
link-path *path-name*	Specifies a detection link as a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
all	Indicates all the interfaces of a detection link.	-
nqa	Indicates the NQA test instance.	-
admin-name	Specifies the administrator of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces.
test-name	Specifies the name of the NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SPR uses detection links to implement intelligent route selection. You can specify an NQA test instance to probe a link. One or more detection links are added to a link group that is then associated with a service profile.

To enable an NQA test instance to probe a link, specify the NQA test instance and interface in the **prober** command.

Prerequisites

The specified NQA test instance has been configured.

Precautions

The local end and remote end of the detection link is the NQA client and NQA server respectively.

Example

Configure the link-path link **Link_1** to be probed by an NQA test instance **jitter** with the administrator **admin**.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] prober link-path Link_1 nqa admin jitter
```

Related Topics

9.11.63 smart-policy-route

9.11.31 link-group

9.11.32 link-member

9.11.46 redirect backup-nexthop

Function

The **redirect backup-nexthop** command configures an action of redirecting packets to the backup next-hop IP address in a traffic behavior.

The **undo redirect backup-nexthop** command deletes an action of redirecting packets to the backup next-hop IP address in a traffic behavior.

By default, an action of redirecting packets to the backup next-hop IP address is not configured.

Format

redirect backup-nexthop *ip-address* [**vpn-instance** *vpn-instance-name*]

undo redirect backup-nexthop

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the backup next-hop IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **redirect backup-nexthop** command configures an action of redirecting packets to the backup next-hop IP address in a traffic behavior. When redirection to a next-hop IP address does not take effect, packets are forwarded according to the backup next-hop IP address. If redirection to the backup next-hop IP address does not take effect, packets are forwarded according to the routing table or discarded. Redirection to the backup next-hop IP address ensures user network robustness.

Prerequisites

The **redirect ip-nexthop** command has been executed to configure an action of redirecting packets to a next-hop IP address in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to a next-hop IP address.

Example

In the traffic behavior **b1**, configure redirection to the next-hop IP address 10.0.0.1 and backup next-hop IP address 20.0.0.1.

```
<Huawei> system-view
[Huawei] traffic behavior b1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-behavior-b1] redirect ip-nexthop 10.0.0.1
[Huawei-behavior-b1] redirect backup-nexthop 20.0.0.1
```

Related Topics

20.1.44 traffic behavior

9.11.50 redirect ip-nexthop

9.11.47 redirect backup-interface

Function

The **redirect backup-interface** command configures an action of redirecting packets to the backup interface in a traffic behavior.

The **undo redirect backup-interface** command deletes the redirection configuration.

By default, an action of redirecting packets to the backup interface is not configured in a traffic behavior.

Format

redirect backup-interface *interface-type interface-number*

undo redirect backup-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the backup interface to which packets are redirected. • *interface-type* specifies the interface type. • *interface-type* specifies the interface number.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **redirect backup-interface** command to define the action of redirecting packets to the backup interface in a traffic behavior, if the redirected-to interface does not take effect, packets are forwarded through the backup interface.

Prerequisites

The **redirect interface** command has been run to configure an action of redirecting packets to an interface in a traffic behavior.

Precautions

- A traffic policy containing redirection can be applied only to the inbound direction of an interface.
- Currently, packets can be redirected only to GRE tunnel interfaces and cellular interfaces on the device.

Example

In the traffic behavior **b1**, redirect packets to **Dialer1** preferentially and to the backup interface **Tunnel 0/0/0** when **Dialer1** is unavailable.

```
<Huawei> system-view
[Huawei] interface Tunnel 0/0/0
[Huawei-Tunnel0/0/0] quit
[Huawei] interface Dialer 1
[Huawei-Dialer1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] redirect interface Dialer 1
[Huawei-behavior-b1] redirect backup-interface Tunnel 0/0/0
```

Related Topics

9.11.49 redirect interface

20.1.44 traffic behavior

9.11.48 redirect enhance enable

Function

The **redirect enhance enable** command enables redirection enhancement for a redirect-link.

The **undo redirect enhance enable** command disables redirection enhancement for a redirect-link.

By default, redirection enhancement is not enabled for a redirect-link.

Format

redirect enhance enable

undo redirect enhance enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

In current SPR scenarios, three types of link exist: prober, nqa-server, and redirect-link. The prober and nqa-server links can guide packet forwarding only when there are equal-cost routes on the device. If there are non-equal-cost routes on the device, even if the two types of link are selected as the optimal links, traffic is still forwarded based on the routing table and eventually forwarded over the link with a higher route priority if the selected optimal link has a lower route priority.

In this situation, if you still want to use SPR, run the **redirect enhance enable** command to ensure that traffic is still forwarded over the optimal link selected in SPR when this link does not have a higher route priority.

Example

Enable redirection enhancement for a redirect-link.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] redirect enhance enable
```

Related Topics

9.11.63 smart-policy-route

9.11.49 redirect interface

Function

The **redirect interface** command configures an action of redirecting packets to an interface in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, an action of redirecting packets to an interface is not configured in a traffic behavior.

Format

redirect interface *interface-type interface-number* [**track** { **nqa** *admin-name test-name* | **ip-route** *ip-address* { *mask* | *mask-length* } [**weak**] | **ipv6-route** *ipv6-address mask-length* }] [**discard**]

undo redirect

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface to which packets are redirected. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
track	Enables the track function.	-
nqa *admin-name test-name*	Specifies the NQA test instance associated with redirection. ● *admin-name* specifies the administrator of an NQA test instance. The value is a string of 1 to 32 case-sensitive characters without spaces. ● *test-name* specifies the name of an NQA test instance. The value is a string of 1 to 32 case-sensitive characters without spaces. **NOTE** Only an NQA test instance of ICMP can be associated with redirection.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip-route *ip-address* { *mask* | *mask-length* }	Specifies the IP route associated with redirection. ● *ip-address* specifies the destination IP address. The value is in dotted decimal notation. ● *mask* specifies the subnet mask. The value is in dotted decimal notation. ● *mask-length* specifies the length of the subnet mask. The value is an integer that ranges from 0 to 32.	-
weak	Indicates a weak policy. If this parameter is specified, the outbound interface of the route associated with redirection can be different from the configured redirect outbound interface.	-
ipv6-route *ipv6-address mask-length*	Specifies the IPv6 route associated with redirection. ● *ipv6-address* specifies the destination IPv6 address. The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. ● *mask-length* specifies the length of the subnet mask. The value is an integer that ranges from 1 to 128.	-
discard	Indicates that the device is configured to discard packets when redirection becomes invalid.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **redirect interface** command configures an action of redirecting packets to an interface in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to an interface.

Precautions

A traffic policy containing redirection can be applied to only the inbound direction of an interface.

Currently, the device only supports redirection to Virtual-Template, 3G/LTE and dialer interfaces. In MPoEoA scenarios, the device does not support redirection to a dialer interface.

Example

Redirect packets to **Dialer2** in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] interface Dialer 2
[Huawei-Dialer2] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] redirect interface Dialer 2
```

Related Topics

20.1.44 traffic behavior

9.11.50 redirect ip-nexthop

Function

The **redirect ip-nexthop** command configures an action of redirecting packets to a next-hop IP address in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, an action of redirecting packets to a next-hop IP address is not configured in a traffic behavior.

 Copyright © Huawei Technologies Co., Ltd.

Format

redirect ip-nexthop *ip-address* [**vpn-instance** *vpn-instance-name*] [**track** { **nqa** *admin-name test-name* | **ip-route** *ip-address* { *mask* | *mask-length* } | **interface** *interface-type interface-number* }] [**post-nat**] [**discard**] [**sfc-nsh spi** *spi-index* **si** *si-index*]

undo redirect

Parameters

Parameter	Description	Value
ip-address	Specifies a next-hop IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
track	Specifies a policy to redirect the next hop.	-
nqa *admin-name test-name*	Specifies the NQA test instance associated with redirection. ● *admin-name* specifies the administrator of an NQA test instance. ● *test-name* specifies the name of an NQA test instance. **NOTE** Only an NQA test instance of ICMP can be associated with redirection.	● *admin-name*, the value is a string of 1 to 32 case-sensitive characters without spaces. ● *test-name*, the value is a string of 1 to 32 case-sensitive characters without spaces.
ip-route *ip-address* { *mask* | *mask-length* }	Specifies the IP route associated with redirection. ● *ip-address* specifies the destination IP address. ● *mask* specifies the subnet mask. ● *mask-length* specifies the length of the subnet mask.	● *ip-address*, the value is in dotted decimal notation. ● *mask*, the value is in dotted decimal notation. ● *mask-length*, the value is an integer that ranges from 0 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the type and number of an interface associated: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
post-nat	Indicates that packets are redirected after packets are translated using NAT.	-
discard	Indicates that the device is configured to discard packets when redirection becomes invalid.	-
sfc-nsh	Specifies the message encapsulated NSH header information after the redirect.	-
spi *spi-index*	Specifies the Service Path Identifier (SPI) index added to packets during redirection.	The value is an integer that ranges from 1 to 16777215.
si *si-index*	Specifies the Service Index (SI) added to packets during redirection.	The value is an integer that ranges from 1 to 255.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure redirection in a traffic behavior to implement PBR.

 Copyright © Huawei Technologies Co., Ltd.

After **track interface** *interface-type interface-number* is configured, the system determines whether redirection takes effect based on the physical status of the interface associated with the track detection function:

- the system determines whether redirection takes effect based on the physical status of the interface associated with the track detection function.
- If the physical status of the interface is Down, the system considers that redirection does not take effect. If the redirection configuration is not backed up and the packets are forwarded along the original path.

NOTE

If a sub-interface is associated with the track detection function, the system determines whether redirection takes effect based on the physical status of the main interface for this sub-interface.

After the **track nqa** *admin-name test-name* or **track ip-route** *ip-address* { *mask* | *mask-length* } command is executed, the system determines whether to activate redirection based on the result of the link detected by the NQA test instance or routing module:

- If the NQA test instance or routing module detects a reachable destination IP address, redirection takes effect.
- When the NQA test instance or routing module detects a reachable destination IP address, redirection is invalid. The device forwards packets based on the original forwarding path if **discard** is not specified. If **discard** is specified, the device discards packets.

post-nat is valid for packets transmitted from the public network to the private network and redirected to the SAE board. After **post-nat** is specified:

- If NAT is configured for these packets, packets are redirected after NAT is performed.
- If NAT is not configured for these packets, **post-nat** does not take effect.

The **sfc-nsh spi** *spi-index* **si** *si-index* parameter is used only in the CloudVPN scenario to encapsulate Network service header (NSH) information in redirected packets to identify a service chain.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to a next-hop IP address.

Precautions

This action is valid for only IPv4 packets.

A traffic policy containing the redirection action can only be used on an interface in the inbound direction.

If the device has no ARP entry matching the specified next-hop IP address, ARP learning is triggered. If no ARP entry is learned, redirection is invalid. The device forwards packets based on the original forwarding path if **discard** is specified; otherwise, the device discards packets.

Example

Redirect packets to the next hop 10.0.0.1 in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] redirect ip-nexthop 10.0.0.1
```

Related Topics

20.1.44 traffic behavior

9.11.51 redirect ipv6-nexthop

Function

The **redirect ipv6-nexthop** command configures an action of redirecting packets to a next hop IPv6 address in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, an action of redirecting packets to a next hop IPv6 address is not configured in a traffic behavior.

Format

redirect ipv6-nexthop *ipv6-address* [**track** { **nqa** *admin-name test-name* | **ipv6-route** *ipv6-address mask-length* }] [**discard**]

undo redirect

Parameters

Parameter	Description	Value
ipv6-address	Specifies a next hop IPv6 address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
track	Enables the track function.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
nqa *admin-name test-name*	Specifies the NQA test instance associated with redirection. ● *admin-name* specifies the administrator of an NQA test instance. The value is a string of 1 to 32 case-sensitive characters without spaces. ● *test-name* specifies the name of an NQA test instance. The value is a string of 1 to 32 case-sensitive characters without spaces. **NOTE** Only an NQA test instance of ICMP can be associated with redirection.	-
ipv6-route *ipv6-address mask-length*	Specifies the IPv6 route associated with redirection. ● *ipv6-address* specifies the destination IPv6 address. The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. ● *mask-length* specifies the length of the subnet mask. The value is an integer that ranges from 1 to 128.	-
discard	Indicates that the device is configured to discard packets when redirection becomes invalid.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure redirection in a traffic behavior to implement PBR.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing redirection to a next hop IPv6 address.

Precautions

This action is valid for only IPv6 packets.

A traffic policy containing redirection can be applied to only the inbound direction of an interface.

If the device does not match the neighbor entry corresponding to the next-hop IPv6 address, the device sends NS packets to check whether the neighbor is reachable. If the neighbor is unreachable, packets are forwarded based on the original path and redirection is invalid. The device forwards packets based on the original forwarding path if **discard** is not specified. If **discard** is specified, the device discards packets.

If you run the **redirect ipv6-nexthop** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a next hop IPv6 address in the traffic behavior **b1**: FC00:0:0:2001::1.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] redirect ipv6-nexthop fc00:0:0:2001::1
```

Related Topics

20.1.44 traffic behavior

9.11.52 redirect-link

Function

The **redirect-link** command redirects packets to a specified link in SPR.

The **undo redirect-link** command cancels the redirection configuration in SPR.

By default, packets are not redirected to a specified link in SPR.

 Copyright © Huawei Technologies Co., Ltd.

Format

redirect-link { *interface-type interface-number* | *interface-name* | **link-path** *path-name* } *next-hop-address*

undo redirect-link { *interface-type interface-number* | *interface-name* | **link-path** *path-name* | **all** }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number of a detection link: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	The value range depends on the interface type and slot ID.
interface-name	Specifies the interface number of a detection link.	The value range depends on the interface type and slot ID. **NOTE** Only the tunnel interface type is supported.
link-path *path-name*	Specifies a link-path link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
next-hop-address	Specifies the next-hop IP address for redirection.	The value is in dotted decimal notation.
all	Deletes all redirection configurations.	-

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

In a dual-gateway scenario, after the **redirect-link** command is configured on the local gateway, this gateway compares the NQA detection result of a specified detection link received from the remote gateway with that of the local detection

link. If the received NQA detection result is better, packets are redirected to the link with the better NQA detection result.

Example

Redirect packets to the specified link with the next hop 10.1.1.1.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] redirect-link tunnel0/0/0 10.1.1.1
```

Related Topics

20.1.44 traffic behavior

9.11.53 redirect vpn-instance

Function

The **redirect vpn-instance** command configures an action of redirecting packets to a VPN instance in a traffic behavior.

The **undo redirect** command deletes the redirection configuration.

By default, the action of redirecting packets to a VPN instance is not configured in a traffic behavior.

Format

redirect vpn-instance *vpn-instance-name*

undo redirect

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance to which packets need to be redirected.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the character string is quoted by double quotation marks, the character string can contain spaces.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

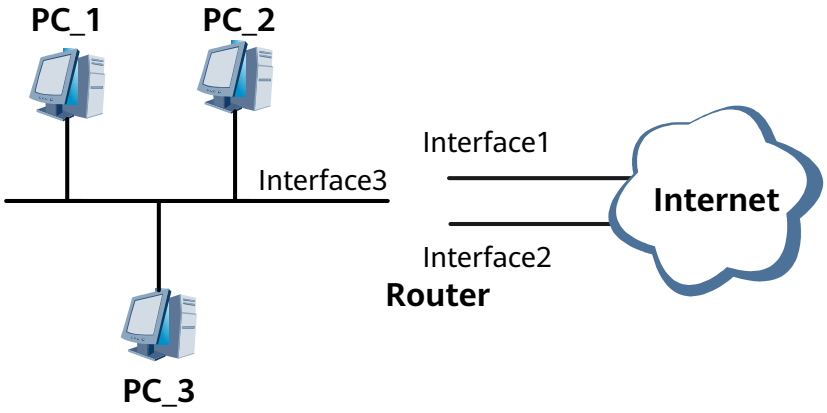
Usage Scenario

When there are multiple egresses to the external network and some packets need to be forwarded through a specified egress, you can configure redirection.

After the **redirect vpn-instance** command is used, the device redirects packets matching traffic classification rules to a specified VPN instance.

As shown in **Figure 9-1**, Interface1 and Interface2 are bound to different VPN instances, and the action of redirecting packets to a VPN instance is configured on Interface3.

Figure 9-1 Networking of redirection



Packet forwarding rules are as follows:

1. The device searches for the routing table according to the redirected VPN instance. If no routing entry is found, packets are discarded.
2. If packets are not redirected to a specified VPN instance, packets are forwarded according to the path before redirection.

Prerequisites

A traffic behavior has been created using the **traffic behavior** command in the system view.

Precautions

- This command is valid for only incoming packets on an interface.
- The command is delivered only to the SRU but not the interface card.
- When Layer 3 traffic does not pass through the SRU and there is no reachable route, the packets match the default route and is sent to the multi-core forwarding engine. In this case, the redirection takes effect.

Example

Configure the device to redirect packets to the VPN instance **vpna** in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] redirect vpn-instance vpna
```

Related Topics

20.1.44 traffic behavior

9.11.54 route flapping suppression

Function

The **route flapping suppression** command sets the flapping suppression period of SPR.

The **undo route flapping suppression** command deletes the flapping suppression period of SPR.

By default, the flapping suppression period is not set for SPR.

Format

route flapping suppression *period-value*

undo route flapping suppression

Parameters

Parameter	Description	Value
period-value	Specifies the flapping suppression period.	The value is an integer, in seconds. The maximum value is 131070, and the minimum value is two times the SPR switchover period, the minimum value is 2.

Views

Smart policy route view

Default Level

2: Configuration level

Usage Guidelines

If SPR performs link switchover frequently because of link flappings, service forwarding efficiency deteriorates. To prevent frequent link switchovers, run the **route flapping suppression** command to set a flapping suppression period. SPR does not perform link switchovers within the flapping suppression period.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The flapping suppression function is disabled by default, and the flapping suppression period is configurable. After traffic is switched to a new link, SPR starts the flapping suppression timer. Within a flapping suppression period, SPR does not perform a link switchover even if it does not obtain link NQA test results indicating that the link meets service requirements within a switchover period. After the flapping suppression timer expires, if SPR still does not obtain NQA test results indicating that the link meets service requirements within a switchover period, SPR performs a link switchover. If SPR obtains NQA test results indicating that the link meets service requirements within a switchover period, SPR retains traffic on the link.
- You are advertised to set the flapping suppression period to a multiple of the switchover period. The minimum flapping suppression period is two times the SPR switchover period that is set using the **9.11.43 period** command.

Example

Set the flapping suppression period to 360 seconds.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] route flapping suppression 360
```

Related Topics

9.11.43 period

9.11.55 route-policy nonexistent-config-check

Function

The **route-policy nonexistent-config-check** command controls whether the system allows a nonexistent route-policy to be specified in a command.

The **undo route-policy nonexistent-config-check disable** command forbids a nonexistent route-policy to be specified in a command.

By default, the system does not allow a nonexistent route-policy to be specified in a command.

Format

route-policy nonexistent-config-check { **disable** | **enable** }

undo route-policy nonexistent-config-check disable

Parameters

Parameter	Description	Value
disable	Indicates that the system allows a nonexistent route-policy to be specified in a command.	-
enable	Indicates that the system does not allow a nonexistent route-policy to be specified in a command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, if you specify a nonexistent route-policy in a command, the command does not take effect. To enable the system to allow a nonexistent route-policy to be specified in a command, run the **route-policy nonexistent-config-check disable** command.

Example

Enable the system to allow a nonexistent route-policy to be specified in a command.

```
<Huawei> system-view
[Huawei] route-policy nonexistent-config-check disable
```

9.11.56 service-map

Function

The **service-map** command creates a service profile of SPR and displays the service profile view.

The **undo service-map** command deletes a service profile of SPR.

By default, no service profile is configured for SPR.

Format

service-map *name*

undo service-map *name*

Parameters

Parameter	Description	Value
name	Specifies the name of a service profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Smart policy routing view

Default Level

2: Configuration level

Usage Guidelines

The service traffic that needs to be forwarded based on smart policies must be associated with service profiles. The link group, service delay threshold, service packet loss threshold, and service CMI threshold must be configured for the service profiles. SPR matches service traffic with the service profile to select routes for the service traffic.

Example

Create service profile **spr1** and enter the service profile view.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1]
```

Related Topics

9.11.21 display smart-policy-route service-map

9.11.12 description (service profile view)

9.11.63 smart-policy-route

9.11.57 service-map default-policy

Function

The **service-map default-policy** command creates the SPR default service profile and displays its view.

By default, service profile is configured in SPR.

Format

service-map default-policy

Parameters

None

Views

Smart-policy-route view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The service traffic requiring SPR must be associated with an SPR service profile, and the link group, service delay threshold, service packet loss threshold, and service CMI threshold must be configured in the service profile. SPR matches the service traffic against the service profile to select routes for the service traffic.

Precautions

- The **match** command cannot be configured in the SPR default service profile, and all the service traffic transmitted over the links configured in this profile will be forwarded based on SPR.
- All the service traffic transmitted over the links configured in the SPR default service profile cannot be forwarded based on any ACL or SA protocol and will only be forwarded based on SPR.
- The SPR default service profile will be automatically generated on the device that has **9.11.63 smart-policy-route** configured.
- The created SPR default service profile cannot be deleted.

Example

Create the SPR default service profile and enter its view.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map default-policy
[Huawei-smart-policy-route-service-map-default-policy]
```

Related Topics

9.11.21 display smart-policy-route service-map

9.11.12 description (service profile view)

9.11.63 smart-policy-route

9.11.58 set cmi threshold

Function

The **set cmi threshold** command sets the composite measure indicator (CMI) threshold for SPR.

The **undo set cmi threshold** command restores the default CMI threshold of SPR.

The default CMI threshold is 0.

Format

set cmi threshold *threshold-value*

undo set cmi threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
threshold-value	Specifies a CMI threshold.	The value is an integer, and the value range varies according to the CMI calculation formula, and thresholds of the delay, jitter, and packet loss rate. The minimum CMI threshold is the value calculated in the CMI calculation formula using the thresholds of the delay, jitter, and packet loss rate. The maximum value is 9000. For example, when the delay threshold is 1000 ms, jitter threshold is 1000 ms, packet loss rate threshold is 100‰, and CMI calculation formula is 9000 – (D + J + L), the CMI threshold ranges from 6900 to 9000. **NOTE** The CMI threshold ranges from 0 to 9000 when the default CMI calculation formula and the default thresholds of the delay, jitter, and packet loss rate are used.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the CMI calculation formula, run the **cmi-method** command. The default CMI calculation formula is 9000 – [D (delay) + J (jitter) + L (loss)]. Many services have requirements for link delay, jitter, and packet loss rate. Therefore, users need to configure the correct CMI calculation formula according to service requirements and run the **set cmi threshold** command to set the CMI threshold.

 Copyright © Huawei Technologies Co., Ltd.

When the calculated CMI value is smaller than the configured CMI threshold, SPR determines that the link CMI does not meet service requirements.

Precautions

The CMI threshold range varies according to values set using the **cmi-method**, **set delay threshold**, **set jitter threshold**, and **set loss threshold** commands. The minimum CMI threshold is the value calculated in the CMI calculation formula using the thresholds of the delay, jitter, and packet loss rate. The maximum value is 9000.

Example

Set the CMI threshold for service profile **spr1** to 7000.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] set cmi threshold 7000
```

Related Topics

9.11.11 cmi-method

9.11.59 set delay threshold

9.11.60 set jitter threshold

9.11.62 set loss threshold

9.11.59 set delay threshold

Function

The **set delay threshold** command sets the service delay threshold of SPR.

The **undo set delay threshold** command restores the service delay threshold of SPR.

The default service delay threshold is 5000 ms.

Format

set delay threshold *threshold-value*

undo set delay threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies a service delay threshold.	The value is an integer ranging from 0 to 5000, in milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The service delay threshold is the maximum service delay allowed by services on a link. If services require a short delay, this threshold needs to be set. When the link delay is longer than the threshold, the link quality is unsatisfied.

Precautions

The CMI threshold changes after you run the **set delay threshold** command. The minimum CMI threshold is the value calculated in the CMI calculation formula using the thresholds of the delay, jitter, and packet loss rate. The maximum value is 9000.

Example

Set the service delay threshold for service profile **spr1** to 1000 ms.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] set delay threshold 1000
```

Related Topics

9.11.58 set cmi threshold

9.11.60 set jitter threshold

9.11.62 set loss threshold

9.11.60 set jitter threshold

Function

The **set jitter threshold** command sets the service jitter threshold of SPR.

The **undo set jitter threshold** command restores the default service jitter threshold of SPR.

The default service jitter threshold of SPR is 3000 ms.

Format

set jitter threshold *threshold-value*

undo set jitter threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies a service jitter threshold.	The value is an integer ranging from 0 to 3000, in milliseconds.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The service jitter threshold is the maximum service jitter allowed by services on a link. If services require a low jitter, this threshold needs to be set. When the link jitter is higher than the threshold, the link quality is unsatisfied.

Precautions

The CMI threshold changes after you run the **set jitter threshold** command. The minimum CMI threshold is the value calculated in the CMI calculation formula using the thresholds of the delay, jitter, and packet loss rate. The maximum value is 9000.

Example

Set the service jitter threshold for service profile **spr1** to 1000 ms.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] set jitter threshold 1000
```

Related Topics

9.11.58 set cmi threshold

9.11.59 set delay threshold

9.11.62 set loss threshold

9.11.61 set link-group

Function

The **set link-group** command associates a service profile with a link group in SPR.

The **undo set link-group** command unbinds a link group from a service profile in SPR.

 Copyright © Huawei Technologies Co., Ltd.

By default, a service profile is not associated with any link group in SPR.

Format

set link-group *name* [**backup**]

undo set link-group *name* [**backup**]

Parameters

Parameter	Description	Value
name	Specifies the name of the active link group associated with a service profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.
backup	Specifies the name of the standby link group associated with a service profile. **NOTE** If this parameter is not specified, the link group associated with the service profile is an active link group.	-

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a link group is associated with a service profile, SPR selects the optimal link from the group for services according to the NQA test results.

SPR prefers the links in the active link group. If the links in the active link group do not meet service requirements, SPR selects links from the standby link group.

Prerequisites

A link group has been configured using the **link-group** command.

Precautions

When you run this command to specify the active or standby link group multiple times, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Associate service profile **spr1** with active link group **group1** and standby link group **group2**.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] set link-group group1
[Huawei-smart-policy-route-service-map-spr1] set link-group group2 backup
```

Related Topics

9.11.31 link-group

9.11.62 set loss threshold

Function

The **set loss threshold** command sets the packet loss rate threshold of SPR.

The **undo set loss threshold** command restores the default packet loss rate threshold of SPR.

The default packet loss rate threshold of SPR is 1000‰.

Format

set loss threshold *threshold-value*

undo set loss threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies a packet loss rate threshold.	The value is an integer ranging from 0 to 1000, in permillage.

Views

Service profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The packet loss rate threshold is the maximum packet loss rate allowed by services on a link. If services require a low packet loss rate, this threshold needs to

be set. When the packet loss rate of a link is higher than this threshold, the link quality is unsatisfied.

Precautions

The CMI threshold changes after you run the **set loss threshold** command. The minimum CMI threshold is the value calculated in the CMI calculation formula using the thresholds of the delay, jitter, and packet loss rate. The maximum value is 9000.

Example

Set the packet loss ratio for the service profile **spr1** to 100‰.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] service-map spr1
[Huawei-smart-policy-route-service-map-spr1] set loss threshold 100
```

Related Topics

9.11.58 set cmi threshold

9.11.59 set delay threshold

9.11.60 set jitter threshold

9.11.63 smart-policy-route

Function

The **smart-policy-route** command creates SPR and displays the SPR view.

The **undo smart-policy-route** command deletes SPR.

By default, the SPR is not configured.

Format

smart-policy-route

undo smart-policy-route

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring SPR, run the **smart-policy-route** command to enter the SPR view.

NOTE

If an SPR exists, the **smart-policy-route** command displays the smart-policy-route view.

Example

Create SPR and enter the SPR view.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route]
```

Related Topics

9.11.18 display smart-policy-route

9.11.56 service-map

9.11.64 standby-interface (smart-policy-route view)

Function

The **standby-interface** command configures an interface that can be automatically shut down when the backup link is not selected in SPR.

The **undo standby-interface** command restores the default configuration.

By default, no interface is automatically shut down when the backup link is not selected in SPR.

Format

standby-interface { *interface-type interface-number* } [**track nqa** *admin-name test-name* **re-probe** { *interface-type interface-number* | **link-path** *path-name* }]

undo standby-interface { *interface-type interface-number* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface that can be automatically shut down when the backup link is not selected in SPR. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If you select the **track nqa** *admin-name test-name* **re-probe** *interface-type interface-number* parameter, **standby-interface** *interface-type interface-number* specifies a backup link interface, and **re-probe** *interface-type interface-number* specifies a master link interface.	Currently, only a cellular or GigabitEthernet interface can function as an SPR backup link interface.
track nqa *admin-name test-name*	Specifies the administrator and name of an NQA test instance. ● *admin-name*: specifies the name of the administrator for an NQA test instance. ● *test-name*: specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-insensitive characters without spaces.
re-probe *interface-type interface-number*	Specifies the interface type and number of the master link. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
re-probe link-path *path-name*	Specifies a link-path link as the master link.	The value is a string of 1 to 31 case-sensitive characters without spaces.
all	All the interfaces that can be automatically shut down when the backup link is not selected in SPR.	-

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **standby-interface** command to shut down the backup link that is not selected in SPR to save traffic and reduce the costs.

In SPR, an NQA test instance is automatically performed on the master link at a long interval, failing to meet complex scenario requirements. If you select the **track nqa** *admin-name test-name* **re-probe** *interface-type interface-number* parameter, the device adds an associated NQA test instance for the specified master link interface according to the **re-probe** *interface-type interface-number* parameter. The added NQA test instance can work with the NQA test instance on the master link to provide more frequent link detection, removing the need to change the interval for performing the NQA test instance on the master link. Subsequently, link information can be obtained in a more timely manner.

Prerequisites

An SPR detection link has been configured using the **9.11.45 prober** command when only the **standby-interface** *interface-type interface-number* command is executed.

Precautions

When the CMIs of all the links in SPR are smaller than the threshold, the SPR detection link activates the shutdown interface to set up a connection again for SPR route selection.

If you need to select the **track nqa** *admin-name test-name* **re-probe** *interface-type interface-number* parameter, pay attention to the following points:

- The configured interval for performing an NQA test instance on the backup link must be shorter than that on the master link. To set the interval for

performing NQA test instances on the master and backup links, run the **frequency** command.

- The NQA test instance must be an ICMP test.
- The backup link must use a different interface than the master link. That is, the backup link interface configured by **standby-interface** *interface-type interface-number* cannot be the same as the master link interface configured by **re-probe** *interface-type interface-number*.

Example

Configure Gigabitethernet0/0/0 to be automatically shut down when the backup link is not selected in SPR. Gigabitethernet0/0/0 is the detection link interface, NQA test instance is **nqa1**, and the administrator is **admin**.

```
<Huawei> system-view
[Huawei] nqa test-instance admin nqa1
[Huawei-nqa-admin-nqa1] start now
[Huawei-nqa-admin-nqa1] quit
[Huawei] smart-policy-route
[Huawei-smart-policy-route] prober gigabitethernet 0/0/0 nqa admin nqa1
[Huawei-smart-policy-route] standby-interface gigabitethernet 0/0/0
```

Configure the backup link interface Gigabitethernet0/0/0 to be automatically shut down when the backup link is not selected in SPR. Gigabitethernet0/0/1 is the master link interface, NQA test instance is **nqa2**, and the administrator is **admin**.

```
<Huawei> system-view
[Huawei] nqa test-instance admin nqa2
[Huawei-nqa-admin-nqa2] test-type icmp
[Huawei-nqa-admin-nqa2] destination-address ipv4 10.1.1.1
[Huawei-nqa-admin-nqa2] frequency 10
[Huawei-nqa-admin-nqa2] source-interface gigabitethernet 0/0/1
[Huawei-nqa-admin-nqa2] start now
[Huawei-nqa-admin-nqa2] quit
[Huawei] smart-policy-route
[Huawei-smart-policy-route] standby-interface gigabitethernet 0/0/0 track nqa admin nqa2 re-probe
gigabitethernet 0/0/1
```

Related Topics

9.11.45 prober

21.7.31 frequency

9.11.63 smart-policy-route

9.11.65 standby-limit-time (smart-policy-route view)

9.11.19 display smart-policy-route link-state

9.11.65 standby-limit-time (smart-policy-route view)

Function

The **standby-limit-time** command sets the delay in automatically shutting down an interface when the backup link is not selected in SPR.

The **undo standby-limit-time** command restores the default delay.

By default, the delay in automatically shutting down an interface when the backup link is not selected in SPR is 3600 seconds.

Format

standby-limit-time *standby-limit-time*

undo standby-limit-time

Parameters

Parameter	Description	Value
standby-limit-time	Specifies the delay in automatically shutting down an interface when the backup link is not selected in SPR.	The value is an integer that ranges from 60 to 28800, in seconds.

Views

Smart-policy-route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **9.11.64 standby-interface (smart-policy-route view)** command configures an interface that can be automatically shut down when the backup link is not selected in SPR, the interface is shut down if the backup link is not selected as the primary link within the configured delay.

Precautions

When the CMIs of all the links in SPR are smaller than the threshold, the SPR detection link activates the shutdown interface to set up a connection again for SPR route selection. The connection needs to be set up again after a certain period. Therefore, a large delay in automatically shutting down the interface ensures service stability, while a small delay saves traffic.

Example

Set the delay in automatically shutting down an interface when the backup link is not selected in SPR to 7000s.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] standby-limit-time 7000
```

Related Topics

9.11.64 standby-interface (smart-policy-route view)

9.11.19 display smart-policy-route link-state

 Copyright © Huawei Technologies Co., Ltd.

9.11.66 wtr period

Function

The **wtr period** command sets the waiting time before the SPR switches from the backup link to the primary link.

The **undo wtr period** command deletes the configured waiting time.

By default, SPR switches from the backup link to the primary link immediately after it detects that the primary link recovers.

Format

wtr period { *seconds* | **days** *days* | **hours** *hours* | **minutes** *minutes* }

undo wtr period

Parameters

Parameter	Description	Value
seconds	Specifies the waiting time before traffic is switched from the backup link to the primary link, in seconds.	The value is an integer that ranges from 1 to 259200.
days *days*	Specifies the waiting time before traffic is switched from the backup link to the primary link, in days.	The value is an integer that ranges from 1 to 3.
hours *hours*	Specifies the waiting time before traffic is switched from the backup link to the primary link, in hours.	The value is an integer that ranges from 1 to 72.
minutes *minutes*	Specifies the waiting time before traffic is switched from the backup link to the primary link, in minutes.	The value is an integer that ranges from 1 to 4320.

Views

Smart policy routing view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the primary link fails, SPR switches from the primary link to the backup link. When the primary link recovers, SPR switches back from the backup link to the primary link immediately. If some important services are being transmitted on the backup link, some traffic is lost in the switchover process. To ensure transmission reliability for important services on the backup link, configure the waiting time before traffic is switched from the backup link to the primary link.

After the waiting time is configured, the device starts calculating the waiting time when SPR switches to the backup link, the flapping suppression time ends, and the primary link recovers. If the device detects that the primary link is working properly within the configured waiting time, the device switches traffic from the backup link to the primary link after the waiting time ends. If the device detects that the primary link does not meet traffic forwarding requirements within the waiting time, the device starts calculating the waiting time again next time it detects that the primary link recovers.

Example

Set the waiting time before SPR switches from the backup link to the primary link to 24 hours.

```
<Huawei> system-view
[Huawei] smart-policy-route
[Huawei-smart-policy-route] wtr period hours 24
```

9.12 Route Monitoring Group Configuration Commands

9.12.1 ip route-monitor-group

Function

The **ip route-monitor-group** command creates a route monitoring group and displays the route monitoring group view or directly displays the route monitoring group view if the route monitoring group has been created.

The **undo ip route-monitor-group** command deletes a route monitoring group.

By default, no route monitoring groups are created.

Format

ip route-monitor-group *group-name*

undo ip route-monitor-group *group-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a route monitoring group.	The value is a string of 1 to 31 case-sensitive characters, with spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All monitored network-side routes of the same type can be added to a group called a route monitoring group. Each route monitoring group is identified by a unique name. To create a route monitoring group, run the **ip route-monitor-group** command.

A route monitoring group monitors the status of its member routes. If the **operator and** command is run, the status of a route monitoring group is up only when all routes in the group are up. If one or more routes in the group go down, the status of the route monitoring group is down. If the **operator and** command is not run, the status of a route monitoring group is up as long as one route in the group is up. If all routes in the group go down, the status of the route monitoring group is down.

Follow-up Procedure

Run the **track ip route** command to add routes to the route monitoring group. After routes are added to the route monitoring group, run the **monitor enable** command in the route monitoring group view to enable the route monitoring group.

In a dual-device hot backup scenario, you can also associate specified service modules with a route monitoring group to protect specified services.

Example

Create a route monitoring group named **uplink**.

```
<Huawei> system-view
[Huawei] ip route-monitor-group uplink
```

9.12.2 monitor enable (route monitoring group view)

Function

The **monitor enable** command enables a route monitoring group.

The **undo monitor enable** command disables a route monitoring group.

By default, the route monitoring group is disabled.

Format

monitor enable

undo monitor enable

Parameters

None

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of routes are being added to or deleted from a route monitoring group, the status of the route monitoring group may change frequently, which in turn leads to service flapping of the service modules associated with the route monitoring group. To prevent such service flapping, run the **undo monitor enable** command to disable the route monitoring group so that it is dissociated from all service modules. After the routes are added or deleted, run the **monitor enable** command to re-associate the route monitoring group with all service modules.

Configuration Impact

After the **monitor enable** command is run, the route monitoring group takes effect immediately. If you add routes or delete routes from the route monitoring group, the down-weight sum of the route monitoring group may change frequently, which in turn leads to service flapping of the service modules associated with the route monitoring group.

Example

Enable route monitoring group named **uplink**.

```
<Huawei> system-view
[Huawei] ip route-monitor-group uplink
[Huawei-route-monitor-group-uplink] monitor enable
```

9.12.3 operator and

Function

The **operator and** command sets the status of routes in a route monitoring group to be of the AND relation so that the status of the route monitoring group is up only when all routes in the group are up.

The **undo operator and** command restores the default configuration.

By default, the status of routes in a route monitoring group is of the OR relation. That is, the status of the route monitoring group is up as long as one route in the group is up.

Format

operator and

undo operator and

Parameters

None

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

To set the status of routes in a route monitoring group to be of the AND relation, run the **operator and** command. After this command is run, the status of the route monitoring group is up only when all routes in the monitoring group are up. The status of the monitoring group is down as long as one route in the group is down.

By default, the status of routes in a route monitoring group is of the OR relation. That is, the status of the route monitoring group is up as long as one route in the group is up. The status of the monitoring group is down only when all routes in the group are down.

Example

Set the status of routes in a route monitoring group to be of the AND relation.

```
<Huawei> system-view
[Huawei] ip route-monitor-group uplink
[Huawei-route-monitor-group-uplink] operator and
```

9.12.4 track ip route

Function

The **track ip route** command adds a route to a route monitoring group.

The **undo track ip route** command deletes a route from a route monitoring group.

By default, no routes are added to a route monitoring group.

Format

track ip route [**vpn-instance** *vpn-instance-name*] *dest-address* { *mask* | *mask-length* }

undo track ip route [**vpn-instance** *vpn-instance-name*] *dest-address* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which a route belongs. If **vpn-instance** *vpn-instance-name* is specified, a VPN route in the VPN instance is added to the route monitoring group; if **vpn-instance** *vpn-instance-name* is not specified, a public network route is added to the route monitoring group.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
dest-address	Specifies the destination IP address of a route.	The value is in dotted decimal notation.
mask	Specifies the mask of a route IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a route IP address.	The value is an integer ranging from 0 to 32.

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A route monitoring group monitors the status of its member routes, each of which has a down-weight. The down-weight sum of the route monitoring group changes with the number of routes that are Down and indicates the link quality. If a route in the route monitoring group goes Down, its down-weight is added to the down-weight sum of the route monitoring group. If a route in the route monitoring group goes Up again, its down-weight is subtracted from the down-weight sum of the route monitoring group. To add a route to a route monitoring group, run the **track ip route** command.

A route monitoring group monitors the status of its member routes. If the **operator and** command is run, the status of a route monitoring group is up only when all routes in the group are up. If one or more routes in the group go down, the status of the route monitoring group is down. If the **operator and** command is not run, the status of a route monitoring group is up as long as one route in the group is up. If all routes in the group go down, the status of the route monitoring group is down. To add a route to a route monitoring group, run the **track ip route** command.

Prerequisites

A route monitoring group has been created using the **ip route-monitor-group** command.

Precautions

A maximum of 16 routes can be added to a route monitoring group, and one route can be added to multiple route monitoring groups.

Example

Add routes 10.1.1.0/24 and 10.1.2.0/24 to route monitoring group named **uplink**, respectively.

```
<Huawei> system-view
[Huawei] ip route-monitor-group uplink
[Huawei-route-monitor-group-uplink] track ip route 10.1.1.0 24
[Huawei-route-monitor-group-uplink] track ip route 10.1.2.0 24
```

9.12.5 trigger-down-delay (route monitoring group view)

Function

The **trigger-down-delay** command configures a delay after which the RM module instructs the associated service modules to perform link switchovers.

The **undo trigger-down-delay** command restores the default configuration.

By default, the delay is 0s.

Format

trigger-down-delay *delay-value*

undo trigger-down-delay *delay-value*

Parameters

Parameter	Description	Value
delay-value	Specifies a delay after which the RM module instructs the associated service modules to perform link switchovers.	The value is an integer ranging from 0 to 1000, in seconds.

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

In dual-device hot backup scenarios, service modules can be associated with a route monitoring group to trigger link switchovers.

In dual-device hot backup scenarios, service modules can be associated with a route monitoring group to trigger link switchovers. If the **operator and** command is run, the status of a route monitoring group is up only when all routes in the group are up. If one or more routes in the group go down, the status of the route monitoring group is down. If the **operator and** command is not run, the status of a route monitoring group is up as long as one route in the group is up. If all routes in the group go down, the status of the route monitoring group is down.

- When the status of a route monitoring group goes down, the RM module instructs the associated service modules to perform link switchovers.
- When the status of a route monitoring group goes up again, the RM module instructs the associated service modules to perform link switchbacks.

During a link switchover, the RM module re-delivers routes to the forwarding table and establishes forwarding entries for the routes, which takes some time. Packet loss may occur if the RM module instructs the associated service modules to perform link switchovers immediately. To resolve this problem, run the **trigger-down-delay** command to configure a delay after which the RM module instructs the associated service modules to perform link switchovers.

Example

Set the delay to 10s after which the RM module instructs the associated service modules to perform link switchovers.

```
<Huawei> system-view
[Huawei] ip route-monitor-group uplink
[Huawei-route-monitor-group-uplink] trigger-down-delay 10
```

9.12.6 trigger-up-delay (route monitoring group view)

Function

The **trigger-up-delay** command configures a delay after which the RM module instructs the service module to perform a link switchback.

The **undo trigger-up-delay** command restores the default configuration.

By default, the delay is 5s.

Format

trigger-up-delay *delay-value*

undo trigger-up-delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay after which the RM module instructs the service module to perform a link switchback.	The value is an integer ranging from 0 to 1000, in seconds.

Views

Route monitoring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On dual-device hot backup scenarios, service modules can be associated with a route monitoring group to trigger link switchovers.

In dual-device hot backup scenarios, service modules can be associated with a route monitoring group to trigger link switchovers. If the **operator and** command is run, the status of a route monitoring group is up only when all routes in the group are up. If one or more routes in the group go down, the status of the route monitoring group is down. If the **operator and** command is not run, the status of a route monitoring group is up as long as one route in the group is up. If all routes in the group go down, the status of the route monitoring group is down.

- When a route in the route monitoring group goes down, the RM module instructs the associated service modules to perform link switchovers.
- When a route in the monitoring group goes up again, the RM module instructs the associated service modules to perform link switchbacks.

If a route in a route monitoring group goes Up, the RM module delivers this route to the forwarding table and establishes a forwarding entry for it, which takes some time. Packet loss may occur if the RM module instructs the service module to perform a link switchback immediately when the down-weight sum of the

 Copyright © Huawei Technologies Co., Ltd.

route monitoring group falls below the switchover threshold of the service module. To address this issue, run the **trigger-up-delay** command to configure a delay after which the RM module instructs the service module to perform a link switchback.

Precautions

If the value of *delay-value* is set to 0, the RM module instructs the associated service modules to perform link switchbacks immediately when the status of the route monitoring group changes to up.

Example

Set the delay to 10s after which the RM module instructs the service module to perform a link switchback.

```
<Huawei> system-view
[Huawei] ip route-monitor-group uplink
[Huawei-route-monitor-group-uplink] trigger-up-delay 10
```

9.12.7 display ip route-monitor-group

Function

The **display ip route-monitor-group** command displays information about all route monitoring groups or a specific one.

Format

display ip route-monitor-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays information about a specified route monitoring group. If *group-name* is specified, detailed information about the specified route monitoring group is displayed; if *group-name* is not specified, a summary of all route monitoring groups is displayed.	The value is a string of 1 to 31 case-sensitive characters, with spaces not supported.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a route monitoring group is configured, you can run the **display ip route-monitor-group** command to check information about the route monitoring group, such as its status, and information about the routes in the route monitoring group.

Example

Display information about all route monitoring groups.

```
<Huawei> display ip route-monitor-group
  Route monitor group number : 2
  Route monitor group          State
  uplink                       Enabled
```

Table 9-245 Description of the **display ip route-monitor-group** command output

Item	Description
Route monitor group number	Number of route monitor groups
Route monitor group	Name of the route monitoring group
State	Status of the route monitoring group: ● Enabled ● Disabled

Display information about the route monitoring group **uplink**.

```
<Huawei> display ip route-monitor-group uplink
route monitor group uplink
 State        : Enabled
-------------------------------------------------------
 route monitor group tracking route number : 1
-------------------------------------------------------
 VPN name     : Public
 Destination  : 2.2.2.2
 Mask         : 255.255.255.255
 State        : Inactive
```

Table 9-246 Description of the **display ip route-monitor-group** command output

Item	Description
route monitor group tracking route number	Number of routes in the route monitoring group
VPN name	VPN instance to which the route belongs
Destination	Destination IP address of the route
Mask	Mask of the route IP address

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Route status: ● Active ● Inactive

9.12.8 display ip route-monitor-group track-route

Function

The **display ip route-monitor-group track-route** command displays information about all route monitoring groups to which a route has been added.

Format

display ip route-monitor-group track-route [**vpn-instance** *vpn-instance-name*] *dest-address* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which a route belongs. If **vpn-instance** *vpn-instance-name* is specified, information about all route monitoring groups to which a VPN route in the VPN instance has been added is displayed; if **vpn-instance** *vpn-instance-name* is not specified, information about all route monitoring groups to which a public network route has been added is displayed.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
dest-address	Specifies the destination IP address of a route.	The value is in dotted decimal notation.
mask	Specifies the mask of a route IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a route IP address.	The value is an integer ranging from 0 to 32.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After a route monitoring group is configured using the **ip route-monitor-group** command, you can run the **track ip route** command to add all monitored network-side routes of the same type to the route monitoring group. One route can be added to multiple route monitoring groups. You can run the **display ip route-monitor-group track-route** command to check the following information:

- Information about all route monitoring groups to which a route has been added
- Whether a route has been added to a route monitoring group
- Whether a route has been deleted from a route monitoring group

Example

Display information about all route monitoring groups to which the route to 192.168.1.0/24 has been added.

```
<Huawei> display ip route-monitor-group track-route 192.168.1.0 24
  Route monitor group          State
  uplink                     Enabled
  downlink                     Enabled
```

Table 9-247 Description of the **display ip route-monitor-group track-route** command output

Item	Description
Route monitor group	Name of the route monitoring group
State	Status of the route monitoring group: ● Enabled ● Disabled

 Copyright © Huawei Technologies Co., Ltd.

10 IP Multicast Commands

About This Chapter

10.1 IGMP Configuration Commands
10.2 MLD Configuration Commands
10.3 PIM (IPv4) Configuration Commands
10.4 PIM (IPv6) Configuration Commands
10.5 MSDP Configuration Commands
10.6 Multicast VPN (IPv4) Configuration Commands in Rosen Mode
10.7 Multicast Route Management (IPv4) Commands
10.8 Multicast Route Management (IPv6) Commands
10.9 IGMP Snooping Configuration Commands
10.10 MLD Snooping Configuration Commands
10.11 Multicast Network Management Commands

10.1 IGMP Configuration Commands

10.1.1 display default-parameter igmp

Function

The **display default-parameter igmp** command displays default IGMP configurations.

Format

display default-parameter igmp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays default IGMP parameter settings even if IGMP parameters have been modified. Therefore, you can use this command to check which parameters have been modified.

Example

Display default IGMP configurations.

```
<Huawei> display default-parameter igmp
  IGMP View Default Configurations:
  ---------------------------------
  Lastmember-queryinterval: 1 s
  Max-response-time: 10 s
  Require-router-alert: disabled
  Robust-count: 2
  Send-router-alert: enabled
  Ssm-mapping: disabled
  Timer other-querier-present: 125 s
  Timer query: 60 s

  Interface View Default Configurations:
  --------------------------------------
  Group-policy: disabled
  Lastmember-queryinterval: 1 s
  Lastmember-query time: 2 s
  Max-response-time: 10 s
  Other-querier-present-timer-expiry: off
  Prompt-leave: disabled
  Require-router-alert: disabled
  Robust-count: 2
  Send-router-alert: enabled
  Ssm-mapping: disabled
  Startup-query-timer-expiry: off
  Static-group: disabled
  Timer other-querier-present: 125 s
  Timer query: 60 s
  Version: 2
  Ip-source-policy: disabled
```

Table 10-1 Description of the display default-parameter igmp command output

Item	Description
IGMP View Default Configurations	Default configurations in the IGMP view. The default configurations take effect globally.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Lastmember-queryinterval	Interval for sending IGMP Group-Specific Query messages. This parameter is configured using the **lastmember-queryinterval (IGMP view)** command in the IGMP view or the **igmp lastmember-queryinterval** command in the interface view.
Max-response-time	Maximum response time for IGMP Query messages. This parameter is configured using the **max-response-time (IGMP view)** command in the IGMP view or the **igmp max-response-time** command in the interface view.
Require-router-alert	Whether the device checks for the Router-Alert option in the received IGMP message. This parameter is configured using the **require-router-alert (IGMP view)** command in the IGMP view or the **igmp require-router-alert** command in the interface view.
Robust-count	Robustness variable of an IGMP querier. This parameter is configured using the **robust-count (IGMP view)** command in the IGMP view or the **igmp robust-count** command in the interface view.
Send-router-alert	Whether the IGMP messages sent from the device carry the Router-Alert option. This parameter is configured using the **send-router-alert (IGMP view)** command in the IGMP view or the **igmp send-router-alert** command.
Ssm-mapping	Whether SSM mapping is enabled. SSM mapping is enabled using the **igmp ssm-mapping enable** command.
Timer other-querier-present	Length of the other querier present timer. This parameter is configured using the **timer other-querier-present (IGMP view)** command in the IGMP view or the **igmp timer other-querier-present** command in the interface view.
Timer query	Interval for sending IGMP General Query messages. This parameter is configured using the **timer query (IGMP view)** command in the IGMP view or the **igmp timer query** command in the interface view.
Interface View Default Configurations	Default configurations in the interface view. The configurations take effect only for IGMP-enabled interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Group-policy	Whether a multicast group filtering policy is configured. A multicast group filtering policy is configured using the **igmp group-policy** command.
Lastmember-query time	Last member query time, calculated using the following formula: Last member query time = Last member query interval x Robustness variable The last member query time is not defined in IGMPv1.
Other-querier-present-timer-expiry	Status of the other querier present timer. The value **off** indicates that the interface considers itself as a querier and that no other queriers exist.
Prompt-leave	Whether the fast leave function is configured. The fast leave function is configured using the **igmp prompt-leave** command.
Startup-query-timer-expiry	Startup query interval of the querier. The interface sends Query messages at this interval when it starts to function as a querier. The value is expressed in seconds and is 1/4 of the query interval (Timer query). The value **off** indicates that the interface has not started to send Query messages as a querier. The startup query timer is enabled only when the interface starts as a querier.
Static-group	Whether static multicast groups are configured. A static multicast group is configured using the **igmp static-group** command.
Version	IGMP version number. IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3, which is configured using the **igmp version** command.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses. This function is configured using the **igmp ip-source-policy** command.

Related Topics

10.1.17 igmp group-policy
10.1.18 igmp ip-source-policy
10.1.19 igmp lastmember-queryinterval

10.1.21 igmp max-response-time
10.1.23 igmp prompt-leave
10.1.28 igmp require-router-alert
10.1.29 igmp robust-count
10.1.30 igmp send-router-alert
10.1.31 igmp ssm-mapping enable
10.1.32 igmp static-group
10.1.33 igmp timer other-querier-present
10.1.34 igmp timer query
10.1.36 igmp version
10.1.37 lastmember-queryinterval (IGMP)
10.1.39 max-response-time (IGMP)
10.1.43 require-router-alert (IGMP)
10.1.48 robust-count (IGMP)
10.1.49 send-router-alert (IGMP)
10.1.51 timer other-querier-present (IGMP)
10.1.52 timer query (IGMP)

10.1.2 display igmp control-message counters

Function

The **display igmp control-message counters** command displays statistics about IGMP control messages.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IGMP message statistics in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays IGMP message statistics in all instances.	-

Parameter	Description	Value
interface *interface-type interface-number*	Displays IGMP message statistics on a specified interface. If this parameter is not specified, the command displays IGMP message statistics on all interfaces.	-
message-type	Indicates the IGMP message type. If this parameter is not specified, the command displays statistics about all types of IGMP messages.	-
query	Displays statistics about Query messages received by the interface. Query messages are sent from a querier.	-
report	Displays statistics about Report messages received by the interface. Report messages are sent by hosts to join a multicast group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the number of IGMP control messages sent and received on the device.

Example

Display statistics about the IGMP messages sent and received by GE1/0/0.

```
<Huawei> display igmp control-message counters interface gigabitethernet 1/0/0
Interface message counter information of VPN-Instance: public net
 GigabitEthernet1/0/0(192.168.2.1):
 Message Type              Sent       Valid      Invalid     Ignore
 ----------------------------------------------------------------
 General Query             280        0          0           0
 Group Query               0          0          0           0
 Source Group Query        0          0          0           0
 ----------------------------------------------------------------
 IGMPV1V2
 Report ASM                0          279        0           0
 Report SSM                0          0          0           0
 ----------------------------------------------------------------
 LEAVE ASM                 0          0          0           0
 LEAVE SSM                 0          0          0           0
 ----------------------------------------------------------------
 IGMPV3
 ISIN Report               0          0          0           0
 ISEX Report               0          0          0           0
```

```
TOIN Report              0          0          0          0
TOEX Report              0          0          0          0
ALLOW Report             0          0          0          0
BLOCK Report             0          0          0          0
Source Records Total     0          0          0          0
-----------------------------------------------------------------
Others                   -          -          0          0
-----------------------------------------------------------------
```

Table 10-2 Description of the display igmp control-message counters interface gigabitethernet 1/0/0 command output

Item	Description
Interface message counter information of VPN-Instance: public net	VPN instance to which the interface belongs.
GigabitEthernet1/0/0(192.168.2.1)	Type, number, and IP address of the interface.
Message Type	Type of IGMP messages.
Sent	Number of IGMP messages sent from the interface.
Valid	Number of valid IGMP messages received by the interface.
Invalid	Number of wrong IGMP messages received by the interface.
Ignore	Number of received IGMP messages ignored by the interface.
General Query	Number of IGMP General Query messages.
Group Query	Number of IGMP Group-Specific Query messages.
Source Group Query	Number of IGMP Group-and-Source-Specific Query messages.
Report ASM	Number of IGMPv1 and IGMPv2 Report messages with multicast group addresses in the ASM group address range.
Report SSM	Number of IGMPv1 and IGMPv2 Report messages with multicast group addresses in the SSM group address range.
LEAVE ASM	Number of IGMP Leave messages with multicast group addresses in the ASM group address range.
LEAVE SSM	Number of IGMP Leave messages with multicast group addresses in the SSM group address range.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ISIN Report	Number of IGMPv3 IS_IN Report messages.
ISEX Report	Number of IGMPv3 IS_EX Report messages.
TOIN Report	Number of IGMPv3 TO_IN Report messages.
TOEX Report	Number of IGMPv3 TO_EX Report messages.
ALLOW Report	Number of IGMPv3 ALLOW Report messages.
BLOCK Report	Number of IGMPv3 BLOCK Report messages.
Source Records Total	Number of multicast sources carried in IGMPv3 messages.
Others	Number of invalid and ignored IGMP messages of unknown types.

Related Topics

10.1.44 reset igmp control-message counters

10.1.3 display igmp explicit-tracking

Function

The **display igmp explicit-tracking** command displays explicit (S, G) entries of IGMPv3 hosts, that is, (S, G) entries that IGMPv3 hosts have joined in Include mode.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **explicit-tracking** [**interface** *interface-type interface-number* [**host-address** *host-address* | **group** *group-address* **source** *source-address*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all-instance	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode in all instances.	-
interface *interface-type interface-number*	Displays information about IGMPv3 hosts that join a specified multicast source in INCLUDE mode on a specified interface.	-
host-address *host-address*	Specifies the address of an IGMP host.	The address is in dotted decimal notation.
group *group-address*	Specifies the address of a multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
source *source-address*	Specifies the address of a multicast source.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the IGMPv3 hosts that join the specific source/group in INCLUDE mode.

```
<Huawei> display igmp explicit-tracking
Explicit-tracking information of VPN-Instance: public net
 Total 1 host, 2 entries

 GigabitEthernet1/0/0(192.168.0.12)
  0001.Host: 192.168.0.28
        Uptime: 00:02:47
        Expires: 00:01:33
        (S, G) List:
          Group: 232.1.1.1
              Source: 10.12.12.12
                Uptime: 00:02:47
                Time since last refresh: 00:02:47
              Source: 10.13.13.13
                Uptime: 00:02:47
                Time since last refresh: 00:02:47
```

Table 10-3 Description of the display igmp explicit-tracking command output

Item	Description
Explicit-tracking information of VPN-Instance	VPN instance to which IGMP host information belongs.
Total 1 host, 2 entries	There is one IGMP host and two (S, G) entries.
GigabitEthernet1/0/0(192.168.0.12)	Type, number, and IP address of an interface.
Host	IGMP host address.
Uptime	Running time since an IGMP host joins a multicast group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Amount of time left before an IGMP host times out. After the IGMP host expires, it is deleted from the IGMP member host list. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
(S, G) List	List of multicast sources and groups an IGMP host has joined.
Group	Multicast group address.
Source	Multicast source address.
Time since last refresh	Amount of time since an IGMP host last joins a group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.1.45 reset igmp explicit-tracking

10.1.4 display igmp group

Function

The **display igmp group** command displays information about IGMP groups that hosts have dynamically joined by sending IGMP Report messages.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP groups in a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays information about IGMP groups in all instances.	-
group-address	Displays information about the IGMP group with a specified group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about the IGMP group on the specified interface.	-
verbose	Displays detailed information about IGMP groups. If the parameter is not specified, the command displays only the summary of IGMP groups.	-
entry-number	Displays statistics about IGMP multicast groups that hosts dynamically join.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check information about multicast groups that have established memberships.

Example

Display information about dynamic IGMP groups.

```
<Huawei> display igmp group
Interface group report information of VPN-Instance: public net
 GigabitEthernet1/0/0(10.1.6.2):
  Total 1 IGMP Group reported
   Group Address   Last Reporter   Uptime      Expires
   225.1.1.2       10.1.6.10       00:02:04    00:01:17
```

Display detailed information about IGMP groups.

```
<Huawei> display igmp group verbose
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 GigabitEthernet1/0/0(10.1.6.2):
  Total entry on this interface: 1
  Limited entry on this interface: -
  Total 1 IGMP Group reported
   Group: 225.1.1.2
     Uptime: 00:03:59
     Expires: off
     Last reporter: 10.1.6.10
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: off
     Group mode: include
     Version1-host-present-timer-expiry: off
     Version2-host-present-timer-expiry: off
     Source list:
       Source: 192.168.232.1
          Uptime: 00:51:07
          Expires: 00:02:05
          Last-member-query-counter: 0
          Last-member-query-timer-expiry: off
```

Display statistics about IGMP multicast groups that hosts dynamically join in the public network instance.

```
<Huawei> display igmp group entry-number
Interface group report information of VPN-Instance: public net
  Total 4 IGMP Groups reported
 Vlanif200(10.36.1.10):
  Total 2 IGMP Groups reported
 Vlanif100(10.0.0.4):
  Total 2 IGMP Groups reported
```

Table 10-4 Description of the display igmp group verbose command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP groups on an interface belong.

Item	Description
Limited entry of this VPN-Instance	Maximum number of IGMP entries that can be created for this instance.
GigabitEthernet1/0/0(10.1.6.2)	Interface type and interface number (IP address).
Total entry on this interface	Total number of IGMP entries on the current interface.
Limited entry on this interface	Maximum number of IGMP entries that the current interface can create.
Total 1 IGMP Group reported	Number of IGMP groups that the current interface has dynamically joined.
Group	Address of a multicast group.
Uptime	Amount of time since a multicast group is created. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Time left before a group will be deleted from the IGMP group table. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days. "off" indicates that the group will never be aged out.
Last reporter	Last host that sends a Report message.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last-member-query-counter	Number of times the querier will send Group-Specific Query messages after receiving a Leave message. The counter value decreases by 1 every time the querier sends a Group-Specific Query message. This parameter is configured using the **igmp robust-count** command. The value 0 indicates that the querier does not send Group-Specific Query messages after receiving a Leave message.
Last-member-query-timer-expiry	Length of the last member query timer. The timer starts only when a Leave message is received from a group member. The timer value is configured using the **igmp lastmember-queryinterval** command. The value **off** indicates that the last member query timer has not started.
Group mode	Multicast group record type. It is displayed only when the interface is running IGMPv3.
Version1-host-present-timer-expiry	Timeout interval of IGMPv1 hosts. IGMPv1 does not define the Leave message; therefore, memberships of IGMPv1 hosts are aged using a timer. The device starts the timer when receiving a Report message from an IGMPv1 host. The timer value is calculated using the following formula: IGMPv1 timeout interval = General group query interval x Robustness variable + Maximum response time for Query messages The general group query interval is configured using the **igmp timer query** command. The robustness variable is configured using the **igmp robust-count** command. The maximum response time for Query messages is configured using the **igmp max-response-time** command. The value **off** indicates that the device has not received any Report messages from IGMPv1 hosts.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Version2-host-present-timer-expiry	Timeout interval of IGMPv2 hosts. It is displayed only when the interface is running IGMPv3. The value **off** indicates that the device has not received any Report messages from IGMPv2 hosts.
Source list	List of multicast sources. It is displayed only when the interface is running IGMPv3 and has IGMPv3 receiver hosts attached.
Source	IP address of a multicast source.

Related Topics

10.1.19 igmp lastmember-queryinterval
10.1.21 igmp max-response-time
10.1.29 igmp robust-count
10.1.34 igmp timer query
10.1.46 reset igmp group

10.1.5 display igmp group ssm-mapping

Function

The **display igmp group ssm-mapping** command displays information about multicast group memberships established with SSM mapping.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group ssm-mapping** [**interface** *interface-type interface-number*] **entry-number**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays group memberships established with SSM mapping in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays group memberships established with SSM mapping in all instances.	-
group-address	Displays information about the specified multicast group memberships established with SSM mapping. If this parameter is not specified, the command displays information about all multicast group memberships established with SSM mapping.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about multicast group memberships established with SSM mapping on the specified interface. If this parameter is not specified, the command displays information about multicast group memberships established with SSM mapping on all interfaces.	-
verbose	Displays detailed information about group membership established with SSM mapping. If the parameter is not specified, the command displays only the summary of group membership established with SSM mapping.	-
entry-number	Displays statistics about IGMP multicast groups that hosts dynamically join.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display igmp group ssm-mapping** command to view information about multicast group memberships that are established with SSM mapping. SSM mapping entries are configured using the **ssm-mapping** command.

Example

Display summary of all multicast group memberships established with SSM mapping.

```
<Huawei> display igmp group ssm-mapping

IGMP SSM mapping interface group report information of VPN-Instance: public net

 Limited entry of this VPN-Instance: -
 GigabitEthernet1/0/0(192.167.101.1):
  Total 1 IGMP SSM-Mapping Group reported
   Group Address   Last Reporter   Uptime      Expires
   232.0.0.1       192.167.101.2   00:00:02    00:02:08
```

Display detailed information about all multicast group memberships established with SSM mapping.

```
<Huawei> display igmp group ssm-mapping verbose
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 GigabitEthernet1/0/0(192.167.101.1):
  Total entry on this interface: 1
  Limited entries on this interface: -
  Total 1 IGMP SSM-Mapping Group reported
   Group: 232.0.0.1
     Uptime: 00:00:15
     Expires: 00:01:55
     Last reporter: 192.167.101.2
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: off
     Version2-host-present-timer-expiry: 00:01:55
```

Display detailed information about IGMP multicast groups configured with SSM mapping that hosts dynamically join in the public network instance.

```
<Huawei> display igmp group ssm-mapping entry-number
Interface group report information of VPN-Instance: public net
  Total 4 IGMP SSM-Mapping Groups reported
 Vlanif200(10.36.1.10):
  Total 2 IGMP SSM-Mapping Groups reported
 Vlanif100(10.0.0.4):
  Total 2 IGMP SSM-Mapping Groups reported
```

Table 10-5 Description of the display igmp group ssm-mapping verbose command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP SSM mapping information belongs.
Limited entry of this VPN-Instance	Maximum number of entries that can be generated in the VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GigabitEthernet1/0/0(192.167.101.1)	Interface type and interface number (IP address).
Total entry on this interface	Total number of entries generated on the interface.
Limited entries on this interface	Maximum number of entries that can be generated on the interface.
Total 1 IGMP SSM-Mapping Group reported	Number of IGMP Report messages with SSM group address received on the interface.
Group	Group address.
Uptime	Amount of time since the last Report message is received.
Expires	Timeout period of a group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Last reporter	Last host that sends a Report message.
Last-member-query-counter	Number of times Group-Specific Query messages are sent.
Last-member-query-timer-expiry	Length of the last member query timer.
Group mode	Filter mode of a group, which can be include or exclude.
Version1-host-present-timer-expiry	Timeout period of IGMPv1 hosts. The value **off** indicates that the device has not received any Report messages from IGMPv1 hosts.
Version2-host-present-timer-expiry	Timeout period of IGMPv2 hosts. The value **off** indicates that the device has not received any Report messages from IGMPv2 hosts.

Related Topics

10.1.50 ssm-mapping (IGMP)

10.1.6 display igmp group static

Function

The **display igmp group static** command displays information about static IGMP entries.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static** [**up** | **down**] [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] **static interface-number**

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*]* **static** [**verbose**]

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group static interface** *interface-type interface-number* **entry-number**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about static IGMP entries in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays information about static IGMP entries in all instances.	-
group-address	Displays information about static IGMP entries of a specified group. If this parameter is not specified, the command displays static IGMP entries of all groups.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
up | **down**	Displays information about interfaces in Up or Down state. If this parameter is not specified, the command displays all interfaces in IGMP entries.	-
verbose	Displays detailed interface list in a static IGMP group. If the parameter is not specified, the command displays only summary of static IGMP entries.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-number	Displays the number of interfaces in a static IGMP group.	-
interface *interface-type interface-number*	Displays information about the static IGMP groups on a specified interface. *interface-type interface-number* specifies the type and number of an interface.	-
entry-number	Displays the number of static IGMP groups on an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about static IGMP entries configured using the **igmp static-group** command.

Example

Display information about all static IGMP entries.

```
<Huawei> display igmp group static
Static join group information of VPN-Instance: public net
 Total 2 entries, Total 2 active entries
  Group Address   Source Address  Interface          State     Expires
  225.1.1.1       10.1.1.1        GE0/0/1            UP        never
  225.1.1.2       10.1.1.1        GE0/0/2            UP        never
```

Table 10-6 Description of the display igmp group static command output

Item	Description
Static join group information of VPN-Instance	VPN instance to which static IGMP groups belong.
Total 2 entries, Total 2 active entries	Number of static IGMP entries and active IGMP entries on the interface.
Group Address	Multicast group address.
Source Address	Multicast source address.
Interface	Interface type and number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of an interface, which can be: ● UP: The interface is operating normally. ● DOWN: An error occurs on the physical link of the interface.
Expires	Scheduled time when a group will be deleted from the IGMP group table. **never** indicates that the group never ages.

Display detailed information about static IGMP entries.

```
<Huawei> display igmp group static verbose
Static join group information of VPN-Instance: public net
 Total 2 entries
  00001.(*, 225.1.1.1)
     Total List of 1 joined interface
     1.GigabitEthernet0/0/1
        State:            UP
        Reference Count:   1
        Multicast Boundary:NO
        Outgoing Interface:YES
  00002.(*, 225.1.1.2)
     Total List of 1 joined interface
     1.GigabitEthernet0/0/2
        State:            UP
        Reference Count:   1
        Multicast Boundary:NO
        Outgoing Interface:YES
```

Table 10-7 Description of the display igmp group static verbose command output

Item	Description
Static join group information of VPN-Instance	VPN instance to which static IGMP groups belong.
Total 2 entries	Number of static IGMP entries on the interface.
00001.(*, 225.1.1.1)	(*, G) entry ID.
Total List of 1 joined interface	Downstream interface list of the (*, G) entry.
1.GigabitEthernet0/0/1	Interface type and interface number.
State	Status of an interface, which can be: ● UP: The interface is operating normally. ● DOWN: An error occurs on the physical link of the interface.
Reference Count	Number of the IGMP entry on the current interface is referenced.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Multicast Boundary	Whether the multicast forwarding boundary is configured.
Outgoing Interface	Whether downstream interfaces exist.

Display lists of Up interfaces in static IGMP entries.

```
<Huawei> display igmp group static up
Static join group information of VPN-Instance: public net
 Total 4 entries
  00001.(*,225.1.1.1)
      Total List of 2 joined interfaces
      Total Matched 2 interfaces
      1.GigabitEthernet0/0/1
      2.GigabitEthernet0/0/2
  00002.(*,225.1.1.2)
      Total List of 2 joined interfaces
      Total Matched 2 interfaces
      1.GigabitEthernet0/0/1
      2.GigabitEthernet0/0/2
```

Table 10-8 Description of the display igmp group static up command output

Item	Description
Total List of 2 joined interfaces	Number of interfaces in a static group.
Total Matched 2 interfaces	List of Up interfaces in a static group.

Display information about IGMP groups statically configured on GE1/0/0.

```
<Huawei> display igmp group interface gigabitethernet 1/0/0 static
Static join group information of VPN-Instance: public net
 Total 2 entries
 Specified interface state:UP
 Total 2 entries matched
   Group Address   Source Address  Expires
   226.0.0.1       10.0.5.120      never
   226.0.0.2       0.0.0.0         never
```

Table 10-9 Description of the display igmp group interface gigabitethernet 1/0/0 static command output

Item	Description
Static join group information of VPN-Instance	VPN instance to which static IGMP groups belong.
Total 2 entries	Number of static IGMP entries on the interface.
Specified interface state	Status of the specified interface.

Item	Description
Total 2 entries matched	Number of IGMP groups that meet the query conditions.
Group Address	Multicast group address.
Source Address	Multicast source address.
Expires	Scheduled time when a group will be deleted from the IGMP group table. **never** indicates that the group never ages.

Related Topics

10.1.32 igmp static-group

10.1.7 display igmp interface

Function

The **display igmp interface** command displays information about IGMP interfaces.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP interfaces in a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays information about IGMP interfaces in all instances.	-
interface-type interface-number	Displays information about a specified IGMP interface. If this parameter is not specified, the command displays information about all IGMP interfaces.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
up	Displays information about the IGMP interfaces with the IP protocol in Up state and the IGMP protocol in Active state.	-
down	Displays information about the IGMP interfaces with the IP protocol in Down state and the IGMP protocol in Inactive state.	-
verbose	Displays detailed information about IGMP interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the IGMP configuration and running information on an interface, run the **display igmp interface** command. This command displays IGMP information only when IGMP is enabled on interfaces of the device.

Example

Display the IGMP configuration and running information on GE1/0/0.

```
<Huawei> display igmp interface gigabitethernet 1/0/0
Interface information of VPN-Instance: public net
 GigabitEthernet1/0/0(192.168.1.2):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
   Value of other querier timeout for IGMP: 0 s
   Value of maximum query response time for IGMP: 10 s
   Querier for IGMP: 192.168.1.2 (this router)
  Total 1 IGMP Group reported
```

Display IGMP parameters on all interfaces.

```
<Huawei> display igmp interface verbose
Interface information of VPN-Instance: public net
 GigabitEthernet1/0/0(192.168.1.2):
   IGMP is enabled
   Current IGMP version is 2
   IGMP state: up
   IGMP group policy: none
   IGMP limit: -
   Value of query interval for IGMP (negotiated): -
   Value of query interval for IGMP (configured): 60 s
```

```
 Value of other querier timeout for IGMP: 0 s
 Value of maximum query response time for IGMP: 10 s
 Value of last member query time: 2 s
 Value of last member query interval: 1 s
 Value of startup query interval: 15 s
 Value of startup query count: 2
 General query timer expiry (hours:minutes:seconds): 00:00:44
 Querier for IGMP: 192.168.1.2 (this router)
 IGMP activity: 1 joins, 0 leaves
 Robustness (negotiated): -
 Robustness (configured): 2
 Require-router-alert: disabled
 Send-router-alert: enabled
 Ip-source-policy: disabled
 Query Ip-source-policy: disabled
 Prompt-leave: disabled
 SSM-Mapping: enabled
 Startup-query-timer-expiry: off
 Other-querier-present-timer-expiry: off
 TTL-check: disabled
Total 1 IGMP Group reported
```

Table 10-10 Description of the display igmp interface verbose command output

Item	Description
Interface information of VPN-Instance	VPN instance to which IGMP interface information belongs.
GigabitEthernet1/0/0(192.168.1.2)	Interface type and interface number (IP address).
IGMP is enabled	IGMP has been enabled on an interface. IGMP can be enabled on an interface using the **igmp enable** command.
Current IGMP version is 2	IGMP version running on an interface. IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. This parameter is configured using the **igmp version** command.
IGMP state	Status of an IGMP interface, which can be up or down.
IGMP group policy	Number of the ACL used in an IGMP group policy, which is used to control the number of groups that an interface can join. The ACL is specified by using the **igmp group-policy** command. The value **none** indicates that no ACL is applied to the interface.
IGMP limit	Maximum number of IGMP group memberships that the current interface can maintain. This parameter is configured using the **igmp limit** command.
Value of query interval for IGMP (negotiated)	Interval negotiated by non-queriers for sending Query messages. The negotiated value is only supported by IGMPv3.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Value of query interval for IGMP (configured)	Configured interval for sending IGMP Query messages. This parameter is configured using the **igmp timer query** command.
Value of other querier timeout for IGMP	Length of the other querier present timer. This parameter is configured using the **igmp timer other-querier-present** command. The value is 0 on the interface that functions as the querier.
Value of maximum query response time for IGMP	Maximum response time carried by an IGMP Query message. This parameter is configured using the **igmp max-response-time** command.
Value of last member query time	Last member query time, calculated using the following formula: Last member query time = Last member query interval x Robustness variable The last member query time is not defined in IGMPv1.
Value of last member query interval	Interval for sending Group-Specific Query messages. The value is configured using the **igmp lastmember-queryinterval** command. This interval is not defined in IGMPv1.
Value of startup query interval	Startup query interval of the querier. The interface sends Query messages at this interval when it starts to function as a querier. The is 1/4 of the query interval configured using the **igmp timer query** command. The startup query interval is not defined in IGMPv1.
Value of startup query count	Number of query messages the querier interface sends at startup. The value is configured using the **igmp robust-count** command. The startup query count is not defined in IGMPv1.
General query timer expiry (hours:minutes:seconds)	Timeout interval of a general query timer.
Querier for IGMP	IGMP querier. In IGMPv1, the querier is selected based on the multicast routing protocol. In IGMPv2, the multicast router with the smallest IP address functions as the querier on the shared network segment.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IGMP activity: 1 joins, 0 leaves	Active group memberships on an interface. ● joins: indicates the number of IGMP groups that the interface has joined. When the interface joins a new group, the value increases by 1. When the interface leaves a group, the value remains unchanged. ● leaves: indicates the number of groups that the interface has left. When the interface leaves a group, the value increases by 1.
Robustness (negotiated)	Robustness variable negotiated by non-queriers. The negotiated value is only supported by IGMPv3.
Robustness (configured)	Robustness variable configured on an interface. This parameter is configured using the **igmp robust-count** command.
Require-router-alert	Whether the local device discards IGMP packets that do not contain the Router-Alert option in IP packet headers. This function is configured using the **igmp require-router-alert** command.
Send-router-alert	Whether the local device sends IGMP packets with the Router-Alert option. This function is configured using the **igmp send-router-alert** command.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses. This function is configured using the **igmp ip-source-policy** command.
Query Ip-source-policy	Whether to filter IGMP Query messages based on source addresses. This function is configured using the **igmp query ip-source-policy** command.
Prompt-leave	Whether fast leave is enabled. The fast leave function is configured using the **igmp prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. SSM mapping is enabled using the **igmp ssm-mapping enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Startup-query-timer-expiry	Interval at which the interface sends Query messages when it starts to function as a querier. The value is 1/4 of Timer query. The value **off** indicates that the interface has not started to send Query messages. The startup query timer is enabled only when the interface starts as a querier.
Other-querier-present-timer-expiry	Status of the other querier present timer. The value **off** indicates that the interface considers itself as a querier and that no other queriers exist.
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: ● enabled ● disabled
Total 1 IGMP Group reported	Indicates the number of IGMP groups that the interface dynamically joins.

Related Topics

10.1.15 igmp enable
10.1.17 igmp group-policy
10.1.18 igmp ip-source-policy
10.1.19 igmp lastmember-queryinterval
10.1.21 igmp max-response-time
10.1.23 igmp prompt-leave
10.1.27 igmp query ip-source-policy
10.1.28 igmp require-router-alert
10.1.29 igmp robust-count
10.1.30 igmp send-router-alert
10.1.31 igmp ssm-mapping enable
10.1.34 igmp timer query
10.1.36 igmp version

10.1.8 display igmp invalid-packet

Function

The **display igmp invalid-packet** command displays statistics and details about invalid IGMP packets received by a device.

 Copyright © Huawei Technologies Co., Ltd.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**interface** *interface-type interface-number* | **message-type** { **leave** | **query** | **report** }] *

display igmp invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid IGMP messages received in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays statistics about invalid IGMP messages received in all VPN instances.	-
interface *interface-type interface-number*	Displays statistics about invalid IGMP messages received on a specified interface. If this parameter is not specified, the command displays statistics about IGMP messages received on all interfaces.	-
message-type	Displays statistics about invalid IGMP messages of a specific type.	-
leave	Displays statistics about invalid Leave messages.	-
query	Displays statistics about invalid Query messages.	-
report	Displays statistics about invalid Report messages.	-
packet-number	Displays details about a specified number of invalid, recently received IGMP messages.	The value is an integer that ranges from 1 to 100. By default, details about all invalid, currently stored IGMP messages are displayed.
verbose	Displays details about invalid IGMP messages.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display igmp invalid-packet** command to view statistics and details about invalid IGMP messages for fault location and rectification.

If IGMP entries fail to be generated on a multicast network, you can run the **display igmp invalid-packet** command to check whether devices have received invalid IGMP messages. If the command output contains statistics about invalid IGMP messages, run the **display igmp invalid-packet** [*packet-number*] **verbose** command to view details about invalid IGMP messages to locate faults.

You can run the following commands to view information about specific invalid IGMP messages:

- Run the **display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** command to view statistics about invalid IGMP messages received in a specified VPN instance or in all VPN instances.
- Run the **display igmp invalid-packet interface** *interface-type interface-number* command to view statistics about invalid IGMP messages received by a specified interface.
- Run the **display igmp invalid-packet** *packet-number* **verbose** command to view details about invalid, recently received IGMP messages. Currently, details about a maximum of 100 invalid IGMP messages can be displayed.

Example

Display statistics about invalid IGMP messages received by the device.

```
<Huawei> display igmp invalid-packet

          Statistics of invalid packets for public net:
-----------------------------------------------------------------
IGMP Query invalid packet:
Unwanted Source List    : 1000        Zero Max Resp Code      : 0
Fault Length            : 1000        Invalid Multicast Group : 0
Bad Checksum            : 0

IGMP Report invalid packet:
Fault Length            : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Bad Checksum            : 0
Illegal Report Type     : 0

IGMP Leave invalid packet:
Invalid Multicast Group : 0           Bad Checksum            : 0
-----------------------------------------------------------------
```

Table 10-11 Description of the display igmp invalid-packet command output

Item	Description
Statistics of invalid packets for public net	Statistics of invalid IGMP messages in public network.
IGMP Query invalid packet	Number of invalid IGMP Query messages.

Item	Description
Unwanted Source List	Number of messages with unwanted source lists.
Zero Max Resp Code	Number of messages whose Max Resp Code field is 0.
Fault Length	Number of messages with invalid lengths.
Invalid Multicast Group	Number of messages with invalid group addresses.
Bad Checksum	Number of messages with checksum errors.
IGMP Report invalid packet	Number of invalid IGMP Report messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Illegal Report Type	Number of IGMP Report messages of invalid types.
IGMP Leave invalid packet	Number of invalid IGMP Leave messages.

Display details of one invalid recently received IGMP message.

```
<Huawei> display igmp invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 6):
-----------------------------------------------------
Interface           :  GigabitEthernet1/0/0
Time                :  2010-06-09 11:03:51 UTC-08:00
Message Length      :  24
Invalid Type        :  Invalid Multicast Group
0000: 16 3c 00 00 01 34 04 04
-----------------------------------------------------
```

Table 10-12 Description of the display igmp invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details about the invalid IGMP message.
Packet information (Index 6)	Sequence number of the invalid IGMP message, which is numbered in the opposite order in which the message is received.
Interface	Interface receiving invalid IGMP messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Time	Time when the invalid IGMP message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid IGMP message.
Invalid Type	Type of the invalid IGMP message.
0000: 16 3c 00 00 01 34 04 04	Contents of the invalid IGMP message.

Related Topics

10.7.23 multicast invalid-packet

10.1.9 display igmp proxy group

Function

The **display igmp proxy group** command displays information about IGMP proxy groups.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address*] [**interface** *interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP proxy groups in a specific VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all-instance	Displays information about IGMP proxy groups in all VPN instances.	-
group-address	Specifies a multicast group address. If you specify *group-address* in this command, the command displays information about a specified multicast group.	The value ranges from 224.0.0.0 to 239.255.255.255, in dotted decimal notation.
interface *interface-type interface-number*	Displays information about IGMP proxy groups in the specified instances.	-
verbose	Displays detailed information about IGMP proxy groups. If you specify **verbose** in this command, the command displays status parameters of IGMP groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the status of an IGMP proxy group or find out the cause of a fault in an IGMP proxy group, run the **display igmp proxy group** command to view information about the IGMP proxy group.

Example

Display information about IGMP proxy groups in a public network instance.

```
<Huawei> display igmp proxy group
Interface group report information of VPN-Instance: public net
    GigabitEthernet1/0/0(10.1.6.2):
     Total 2 IGMP proxy Groups
      Group Address   Filter mode
      225.1.1.1       exclude
      225.1.1.2       include
```

Table 10-13 Description of the display igmp proxy group command output

Item	Description
Interface group report information of VPN-Instance	VPN instance to which IGMP group information on an interface belongs.
GigabitEthernet1/0/0(10.1.6.2)	Interface number (IP address).
Total 2 IGMP proxy Groups	Total two IGMP proxy groups on an interface.
Group Address	Multicast group address.
Filter mode	Filter mode of a group, which can be exclude or include.

Display details of IGMP proxy groups in a public network instance.

```
<Huawei> display igmp proxy group verbose
Interface group report information of VPN-Instance: public net
    GigabitEthernet1/0/0(10.1.6.2):
     Total 2 IGMP proxy Groups
     Group: 225.1.1.1
       Filter mode: exclude
       Query Response Expiry: 00:00:02
       Source list (total 1 source)
         Source: 2.1.1.1
     Group: 225.1.1.2
       Filter mode: include
       Query Response Expiry: off
       Source list (total 1 source)
         Source: 2.1.1.2
```

Table 10-14 Description of the display igmp proxy group verbose command output

Item	Description
Query Response Expiry	Amount of time before the query response time expires.
Source list (total 1 source)	Source list (number of sources in the source list).
Source	Multicast source address.
Group	Multicast group address.

Related Topics

10.1.24 igmp proxy

10.1.25 igmp proxy backup

 Copyright © Huawei Technologies Co., Ltd.

10.1.10 display igmp proxy interface

Function

The **display igmp proxy interface** command displays information about IGMP proxy interfaces.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about IGMP proxy interfaces in a specific VPN instance. If neither **vpn-instance** nor **all-instance** is specified, the command displays only IGMP proxy interfaces in the public network instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays information about IGMP proxy interfaces in all VPN instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the status of an IGMP proxy interface or find out the cause of a fault in an IGMP proxy interface, run the **display igmp proxy interface** command to view information about the IGMP proxy interface.

Example

Display information about IGMP proxy interfaces in a public network instance.

```
<Huawei> display igmp proxy interface
Interface information of VPN-Instance: public net
 GigabitEthernet1/0/0(192.168.1.2):
   IGMP proxy is enabled
   Current IGMP proxy version (negotiated) is 3
   Current IGMP proxy version (configured) is 2
```

```
IGMP proxy state: up
Value of query interval for IGMP (negotiated): 60 s
Value of query interval for IGMP (configured): 60 s
Value of querier present timeout for IGMPv1: off
Value of querier present timeout for IGMPv2: off
Value of querier present timeout for IGMPv3: 124 s
General query response expiry: off
Querier for IGMP: 192.168.1.1
Robustness (negotiated): 2
Robustness (configured): 2
Require-router-alert: disabled
Send-router-alert: enabled
Ip-source-policy: disabled
Query Ip-source-policy: disabled
TTL-check: disabled
```

Table 10-15 Description of the display igmp proxy interface command output

Item	Description
Interface information of VPN-Instance	VPN instance to which IGMP proxy interface information belongs.
GigabitEthernet1/0/0(192.168.1.2)	Interface number (IP address).
IGMP proxy is enabled	IGMP proxy is enabled on the interface.
Current IGMP proxy version (negotiated) is 3	Negotiated IGMP version on the IGMP proxy interface is IGMPv3.
Current IGMP proxy version (configured) is 2	IGMPv2 is configured on the IGMP proxy interface.
IGMP proxy state	Status of the IGMP proxy interface, which can be Up or Down.
Value of query interval for IGMP (negotiated)	Query interval negotiated between the query interval configured on the IGMP proxy interface and the query interval carried in a Query message, in seconds. Only IGMPv3 Query messages carry this field. This field takes effect only in IGMPv3.
Value of query interval for IGMP (configured)	Interval at which the IGMP proxy interface sends IGMP Query messages, in seconds.
Value of querier present timeout for IGMPv1	Timeout period of an IGMPv1 querier.
Value of querier present timeout for IGMPv2	Timeout period of an IGMPv2 querier.
Value of querier present timeout for IGMPv3	Timeout period of an IGMPv3 querier.
General query response expiry	Timeout period of a general group query timer.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Querier for IGMP	Address of an IGMP querier. In IGMPv1, a querier is selected based on a multicast routing protocol; in IGMPv2 and IGMPv3, the router with the lowest IP address acts as the querier on the shared network segment. If no querier exists, this field is displayed as "-".
Robustness (negotiated)	Robustness variable negotiated between the robustness variable configured on an IGMP proxy interface and the robustness variable carried in a Query message. This field takes effect only in IGMPv3.
Robustness (configured)	Robustness variable configured on the IGMP proxy interface.
Require-router-alert	Whether the device accepts only IGMP messages carrying the Router-Alert option.
Send-router-alert	Whether the device sends IGMP messages carrying the Router-Alert option.
Ip-source-policy	Whether to filter IGMP Report/Leave messages based on host addresses.
Query Ip-source-policy	Whether to filter IGMP Query messages based on source addresses.
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: ● enabled ● disabled

10.1.11 display igmp proxy routing-table

Function

The **display igmp proxy routing-table** command displays information about an IGMP proxy routing table.

Format

display igmp proxy [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **none** } | **incoming-interface** *interface-type interface-number* | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays information about an IGMP proxy routing table in a specific VPN instance. If you specify neither **vpn-instance** nor **all-instance** in this command, the command displays only the IGMP proxy routing table in the public network instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays information about IGMP proxy routing tables in all VPN instances.	-
group-address	Displays information about the routing entry of a specified group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask	Indicates the mask of a multicast group address or a source address.	-
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of a multicast group address.	The value is in dotted decimal notation.
source-address	Displays the routing entry for a multicast source.	The value is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of a multicast source address.	The value is in dotted decimal notation.
outgoing-interface	Displays the routing entries with a specific interface as the outbound interface.	-
include	Displays the routing entries of which the downstream interface list has a specific interface.	-
exclude	Displays the routing entries of which the downstream interface list does not have a specific interface.	-
match	Displays the routing entries of which the downstream interface list has only a specific interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
none	Displays the routing entries with an empty downstream interface list.	-
incoming-interface	Displays the routing entries with a specified inbound interface.	-
flags *flag-value*	Indicates an IGMP proxy routing entry with a specific type. *flag-value* specifies the flag of a routing entry. If you specify **flags** *flag-value* in this command, the command displays IGMP proxy routing entries with the flag.	*flag-value* can be act, del, join, none, niif, sgjoin, wcjoin, upchg, or wc. For information about each value, see the flag-value field description in the **display pim routing-table** command output.
fsm	Displays detailed information about a finite state machine (FSM).	-
outgoing-interface-number	Displays the number of downstream interfaces in an IGMP proxy routing entry.	-
number	Specifies the number of downstream interfaces in an entry to be queried.	The value is an integer that ranges from 0 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you need to know information about an IGMP proxy routing table, run the **display igmp proxy routing-table** command. You can specify different parameters in this command to view specific routing information. This command helps you find specific routes and locate faults.

Example

Display details of an FSM in an IGMP proxy routing table in a public network instance.

```
<Huawei> display igmp proxy routing-table fsm
Routing table of VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, 225.1.1.1)
     Flag: WC, UpTime: 6d:10h
     Upstream interface: GigabitEthernet1/0/2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/1
             Protocol: igmp, UpTime: 17:27:13
             IGMP querier: 11.1.1.1(this router)
             IGMP state: EXCLUDE

     FSM information for non-downstream interfaces: None

 (33.3.3.100, 225.1.1.1)
     Flag: JOIN ACT, UpTime: 6d:17h
     Upstream interface: GigabitEthernet1/0/2
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/1
             Protocol: igmp, UpTime: 17:27:13
             IGMP querier: 11.1.1.1(this router)
             IGMP state: NI

     FSM information for non-downstream interfaces: None
```

Table 10-16 Description of the display igmp proxy routing-table fsm command output

Item	Description
Routing table of VPN-Instance	VPN instance to which IGMP proxy routing information belongs.
Total 1 (*, G) entry; 1 (S, G) entry	Total number of (*, G) and (S, G) entries in the IGMP proxy routing table.
(*, 225.1.1.1)	(*, G) or (S, G) entry in the IGMP proxy routing table.
Flag	Flag of a (*, G) or an (S, G) entry in the IGMP proxy routing table.
UpTime	Amount of time since a (*, G) or an (S, G) entry is created.
Upstream interface	Upstream interface of a (*, G) or an (S, G) entry.
Downstream interface(s) information	Information about downstream interfaces.
Total number of downstreams	Total number of downstream interfaces.
GigabitEthernet1/0/1	Name of a downstream interface.
Protocol	Protocol of a downstream interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
UpTime	Amount of time a downstream interface has been in Up state, expressed in hh:mm:ss format.
IGMP querier	Address of an IGMP querier
IGMP state	IGMP status on a downstream interface: ● NI: indicates that an (S, G) entry inherits the downstream interfaces of a (*, G) entry. ● BLOCK: indicates that the interface does not forward traffic based on an (S, G) entry. ● INCLUDE: indicates that the interface needs to join the specified group and source. ● EXCLUDE: indicates that the interface does not join the specified group and source.
FSM information for non-downstream interfaces	Interfaces that do not forward multicast data packets matching (*, G) or (S, G) entries.

10.1.12 display igmp routing-table

Function

The **display igmp routing-table** command displays the IGMP routing table.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }]] * [**static**] [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays IGMP routing information in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays IGMP routing information in all instances.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group-address	Displays IGMP routing information of a specified multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the mask of a multicast group address or a multicast source address.	-
group-mask	Specifies the mask of a multicast group address.	It is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	It is an integer that ranges from 4 to 32.
source-address	Displays IGMP routing information of a specified multicast source.	It is in dotted decimal notation.
source-mask	Specifies the mask of a multicast source address.	It is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	It is an integer that ranges from 0 to 32.
static	Displays static IGMP routing entries.	-
outgoing-interface-number	Displays the number of the outbound interfaces in IGMP routing entries.	-
number	Specifies the number of outbound interfaces. If this parameter is specified, the command displays the specified number of outbound interfaces.	The value is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display igmp routing-table** command provides IGMP routing information. You can specify different parameters to view specific IGMP routing information for problem location.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This command provides output information only when PIM is not enabled on the IGMP-capable interface.

Example

Display the IGMP routing table.

```
<Huawei> display igmp routing-table
Routing table of VPN-Instance: public net
 Total 2 entries

 00001. (10.10.10.10, 232.1.1.3)
      List of 1 downstream interface in include mode
       GigabitEthernet1/0/0 (10.20.20.1),
                Protocol: SSM-MAP

 00002. (*, 225.1.1.1)
      List of 1 downstream interface
       GigabitEthernet1/0/0 (10.20.20.1),
                Protocol: IGMP
```

Table 10-17 Description of the display igmp routing-table command output

Item	Description
Routing table of VPN-Instance: public net	VPN instance to which the IGMP routing table belongs.
Total 2 entries	Total number of IGMP routing entries.
00001. (10.10.10.10, 232.1.1.3)	Entry 00001. (S, G) indicates that data is transmitted from S to G. (*, G) indicates that data is transmitted from any source to G.
List of 1 downstream interface in include mode	Downstream interface list in include mode.
GigabitEthernet1/0/0 (10.20.20.1)	Interface type and interface number (IP address).
Protocol	Protocol type, including: ● SSM-MAP: Entries are generated using SSM mapping. ● IGMP: Entries are generated using IGMP. ● STATIC: Entries are generated by configuring static IGMP groups.

 Copyright © Huawei Technologies Co., Ltd.

10.1.13 display igmp ssm-mapping

Function

The **display igmp ssm-mapping** command displays configuration of IGMP SSM mapping.

Format

display igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **ssm-mapping** { **group** [*group-address*] | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays SSM mapping entries in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays SSM mapping entries in all instances.	-
group [*group-address*]	Displays the SSM mapping entries of a specified group. If *group-address* is not specified, the command displays SSM mapping entries of all groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
interface [*interface-type interface-number*]	Displays whether SSM mapping is enabled on a specified interface. If *interface-type interface-number* is not specified, the command displays all the interfaces that are in Up state and have SSM mapping enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays mapping between multicast groups and multicast sources configured using the **ssm-mapping** command. You can also use this command to

check the SSM mapping configuration on an interface. To enable SSM mapping on an interface, run the **igmp ssm-mapping enable** command in the interface view.

Example

Display SSM mapping entries of all the multicast sources and multicast groups.

```
<Huawei> display igmp ssm-mapping group
IGMP SSM-Mapping conversion table of VPN-Instance: public net
 Total 2 entries    2 entries matched

 00001. (10.1.0.2, 225.1.1.0/24)

 00002. (10.1.0.2, 239.255.255.0/24)

 Total 2 entries matched
```

Table 10-18 Description of the display igmp ssm-mapping group command output

Item	Description
IGMP SSM-Mapping conversion table of VPN-Instance	VPN instance to which the IGMP SSM mapping table belongs.
Total 2 entries 2 entries matched	Total number of SSM mapping entries and total number of entries matching the query conditions.
00001. (10.1.0.2, 225.1.1.0/24) 00002. (10.1.0.2, 239.255.255.0/24)	Number of an (S, G) entry.
Total 2 entries matched	Number of SSM mapping entries matching the query conditions.

Display whether IGMP SSM mapping is enabled on GE1/0/0.

```
<Huawei> display igmp ssm-mapping interface gigabitethernet 1/0/0
IGMP SSM-Mapping is enabled
```

Table 10-19 Description of the display igmp ssm-mapping interface gigabitethernet 1/0/0 command output

Item	Description
IGMP SSM-Mapping is enabled	SSM mapping is enabled on the interface.

Related Topics

10.1.31 igmp ssm-mapping enable
10.1.50 ssm-mapping (IGMP)

 Copyright © Huawei Technologies Co., Ltd.

10.1.14 igmp

Function

The **igmp** command displays the IGMP view.

The **undo igmp** command deletes all configurations in the IGMP view.

Format

igmp [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Global IGMP parameters must be configured in the IGMP view.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Enter the IGMP view of the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp]
```

Enter the IGMP view of VPN instance mvpn.

```
<Huawei> system-view
[Huawei] ip vpn-instance mvpn
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-vpn-instance-mvpn] ipv4-family
[Huawei-vpn-instance-mvpn-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-mvpn-af-ipv4] quit
[Huawei-vpn-instance-mvpn] multicast routing-enable
[Huawei-vpn-instance-mvpn] quit
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn]
```

Related Topics

10.7.28 multicast routing-enable

10.1.15 igmp enable

Function

The **igmp enable** command enables IGMP on an interface.

The **undo igmp enable** command disables IGMP on an interface.

By default, IGMP is disabled on an interface.

Format

igmp enable

undo igmp enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a shared network segment, user hosts and Layer 3 multicast devices directly connected to the user network segment must run IGMP. A multicast device can process IGMP messages sent from user hosts only after IGMP is enabled on the interfaces connected to user network segments.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- If PIM and IGMP need to be enabled on the same interface, enable PIM, and then IGMP.

 Copyright © Huawei Technologies Co., Ltd.

- If IGMP parameters are configured on an interface, the parameter settings take effect only after IGMP is enabled.

Example

Enable IGMP on GE1/0/0 connected to a user network segment.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp enable
```

Related Topics

10.7.28 multicast routing-enable

10.1.7 display igmp interface

10.1.16 igmp global limit

Function

The **igmp global limit** command sets the maximum number of IGMP entries that can be created on the router.

The **undo igmp global limit** command deletes the configured maximum number of IGMP entries.

By default, the maximum number of IGMP entries that can be created on the router varies according to device models:

- AR150&200 series: 128
- AR100&AR120&AR160&AR1200 series: 3000
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-Dand AR2204: 256
- AR2220, and AR2220E: 20480
- AR2204XE and AR2204XE-DC: 34816
- AR2240C: 33792
- AR2240 series and AR3200 series:
  - Configured with SRU40: 33792
  - Configured with SRU60: 33792
  - Configured with SRU80: 34816
  - Configured with SRU100: 34816
  - Configured with SRU100E: 34816
  - Configured with SRU200: 34816
  - Configured with SRU200E: 34816
  - Configured with SRU400: 34816
- AR3600 series (SRUX5): 34816

Format

igmp global limit *number*

undo igmp global limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created on the router.	The value is an integer that ranges from: ● 1 to 128 for the AR150&200 series ● 1 to 3000 for the AR100&AR120&AR160&AR1200 series ● 1 to 256 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D and AR2204 ● 1 to 20480 for the AR2220, and AR2220E ● 1 to 34816 for the AR2204XE and AR2204XE-DC ● AR2240C: 1 to 33792 ● AR2240 series and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 33792 – Configured with SRU60: 1 to 33792 – Configured with SRU80: 1 to 34816 – Configured with SRU100: 1 to 34816 – Configured with SRU100E: 1 to 34816 – Configured with SRU200: 1 to 34816 – Configured with SRU200E: 1 to 34816 – Configured with SRU400: 1 to 34816 ● 1 to 34816 for the AR3600 series (SRUX5)

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To enable the router to create new IGMP entries, useless entries or increase the limit. Alternatively, you can configure static IGMP entries.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.

 Copyright © Huawei Technologies Co., Ltd.

- Each (*, G) entry established with SSM mapping is counted as one entry.

Example

Set the maximum number of IGMP entries that can be created on the router to 126.

```
<Huawei> system-view
[Huawei] igmp global limit 126
```

Related Topics

10.1.38 limit (IGMP)

10.1.20 igmp limit

10.1.17 igmp group-policy

Function

The **igmp group-policy** command configures an IGMP group policy on an interface to limit the range of multicast groups that the hosts can join.

The **undo igmp group-policy** command deletes the IGMP group policy.

By default, no IGMP group policy is configured on an interface, and the hosts can join any multicast groups.

Format

igmp group-policy { *acl-number* | **acl-name** *acl-name* } [**1** | **2** | **3**]

undo igmp group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL or an advanced ACL. The ACL defines a multicast group range.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
1	Sets the range of multicast groups that IGMPv1 hosts can join.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
2	Sets the range of multicast groups that IGMPv2 hosts can join.	-
3	Sets the range of multicast groups that IGMPv3 hosts can join.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To control the multicast groups that hosts on the network attached to an interface can join, specify an ACL in the **igmp group-policy** command as a filter to specify the range of multicast groups served by the interface. This configuration improves security of the IGMP application. You can also use this command to prevent the router from receiving Join messages for specified groups.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- Before running the **igmp group-policy** command, run the **acl** command to configure the ACL that you want to apply to the group policy to limit the range of multicast groups that hosts connected to the interface can join.
  - In the basic ACL view, set **source** in the **rule** command to the range of multicast groups that an interface can join.
  - In the advanced ACL view, set **source** in the **rule** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.
- After the **igmp group-policy** command is executed on an interface:
  - The interface filters the received Report messages based on the ACL and maintains memberships only for the multicast groups permitted by the ACL.
  - The interface discards the Report messages that are denied by the ACL. If the entries of the multicast groups denied by the ACL exist on the router, the router deletes these entries when the aging time of the entries expires.
  - If the IGMP version is not specified, the specified ACL applies to IGMPv1, IGMPv2, and IGMPv3 hosts.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create ACL 2005, and configure a rule that allows hosts to receive data of multicast group 225.1.1.1. Configure an IGMP group policy on GE1/0/0 and reference ACL 2005 to allow hosts connected to the interface to join only multicast group 225.1.1.1.

```
<Huawei> system-view
[Huawei] acl number 2005
[Huawei-acl-basic-2005] rule permit source 225.1.1.1 0
[Huawei-acl-basic-2005] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp group-policy 2005
```

Create an ACL named **myacl**, and configure a rule that allows hosts to receive data of multicast groups in the range of 225.1.0.0/16. Configure an IGMP group policy on GE1/0/0 and reference the ACL to allow hosts connected to the interface to join only the specified multicast groups.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp group-policy acl-name myacl
```

Related Topics

10.1.4 display igmp group

10.1.7 display igmp interface

10.7.28 multicast routing-enable

10.1.18 igmp ip-source-policy

Function

The **igmp ip-source-policy** command enables filtering of IGMP Report/Leave messages based on source addresses.

The **undo igmp ip-source-policy** command disables filtering of IGMP Report/Leave messages based on source addresses.

By default, the router does not filter IGMP Report/Leave messages based on source addresses.

Format

igmp ip-source-policy [*basic-acl-number* | **acl-name** *acl-name*]

undo igmp ip-source-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP runs on member hosts and their directly connected multicast devices. A multicast device processes all received Report/Leave messages. To improve security, you can configure the multicast device to filter Report/Leave messages received on an interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

IGMP Report/Leave messages are encapsulated in IP packets. The **igmp ip-source-policy** command configures the router to check the source address in the IP header of each received Report/Leave message. The router filters Report/Leave messages based on the following rules (if ACL rules are not configured):

- If the source IP address of a Report/Leave message is 0.0.0.0 or on the same network segment as the IP address of the inbound interface, the router processes the Report/Leave message.
- If the source IP address of a Report/Leave message is on a different network segment than the IP address of the inbound interface, the router discards the Report/Leave message.

If you have specified an ACL rule, the interface filters out the IGMP Report/Leave messages whose source addresses do not match the ACL rule.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable filtering of IGMP Report/Leave messages based on source addresses on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ip-source-policy
```

Configure GE1/0/0 to accept the IGMP Report/Leave messages with the source address 10.10.1.1.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.10.1.1 0
[Huawei-acl-basic-2001] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ip-source-policy 2001
```

Related Topics

10.1.7 display igmp interface
10.7.28 multicast routing-enable

10.1.19 igmp lastmember-queryinterval

Function

The **igmp lastmember-queryinterval** command configures interval at which an IGMP querier interface sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages after receiving IGMP Leave messages from hosts.

The **undo igmp lastmember-queryinterval** command restores the default value.

By default, the interval at which an IGMP querier interface sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages is 1s.

Format

igmp lastmember-queryinterval *interval*

undo igmp lastmember-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a querier receives a Leave message for a group, the querier periodically sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to check for other members in the group. The **igmp lastmember-queryinterval** command sets the interval at which the querier sends Last Member Query messages. The querier stops forwarding multicast data to the group if it receives no Report message from the group within the period specified by *interval* x *robust-value*. Here, *robust-value* is the robustness variable configured using the **igmp robust-count** or **robust-count** command.

If the querier receives Report messages from the group within the specified period, the querier continues maintaining memberships of the group. Otherwise, the querier considers that the last member has left the group and no longer maintains memberships of the group.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 and IGMPv3.
- The **igmp lastmember-queryinterval** command has the same function as the **lastmember-queryinterval** command used in the IGMP view. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is incomplete.

Example

Set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp lastmember-queryinterval 3
```

Related Topics

10.1.7 display igmp interface

10.1.29 igmp robust-count

10.1.37 lastmember-queryinterval (IGMP)

10.7.28 multicast routing-enable

10.1.48 robust-count (IGMP)

 Copyright © Huawei Technologies Co., Ltd.

10.1.20 igmp limit

Function

The **igmp limit** command sets the maximum number of IGMP group memberships allowed on an interface.

The **undo igmp limit** command restores the maximum number of IGMP group memberships allowed on an interface to the default value.

By default, the maximum number of IGMP entries that can be created on an interface varies according to device models:

- AR150&AR200 series: 64
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128
- AR100&AR120&AR160&AR1200 series, AR2220E, AR2240C and AR2220: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100E: 2000
  - Configured with SRU200: 3000
  - Configured with SRU200E: 3000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 3000

Format

igmp limit *number* [**except** { *acl-number* | **acl-name** *acl-name* }]

undo igmp limit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries allowed on an interface.	The value is an integer that ranges from: ● 1 to 64 for the AR150&AR200 series ● 1 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 ● 1 to 1000 for the AR100&AR120&AR160&AR1200 series, AR2220E, AR2240C, AR2220 ● 1 to 2000 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 1000 – Configured with SRU60: 1 to 1000 – Configured with SRU80: 1 to 2000 – Configured with SRU100E: 1 to 2000 – Configured with SRU200: 1 to 3000 – Configured with SRU200E: 1 to 3000 – Configured with SRU400: 1 to 4000 ● 1 to 3000 for the AR3600 series (SRUX5)
except	Specifies the range of multicast groups whose IGMP entries are not limited by the IGMP limit.	-
acl-number	Specifies a basic ACL or an advanced ACL.	The value is an integer. The basic ACL number ranges from 2000 to 2999. A basic ACL filters group addresses only. The advanced ACL number ranges from 3000 to 3999. An advanced ACL filters (S, G) entries as well as group addresses.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To allow the router to create more IGMP entries, delete useless entries or increase the limit. Alternatively, you can configure static IGMP entries.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Precautions

If **except** is not specified in the command, the configured IGMP limit restricts the maximum number of all dynamic IGMP (*, G) or (S, G) entries. Before setting **except**, configure the associated ACL. The interface then uses the ACL to filter the received IGMP Report messages. The number of entries corresponding to the multicast groups that match the ACL is not limited.

The **igmp limit** command must be used with ACL configuration commands. When configuring ACL rules, note that:

- In the basic ACL view, specify the **source** parameter in the **rule** command to set the range of multicast groups whose IGMP entries are not limited.
- In the advanced ACL view, specify the **source** parameter in the **rule** command to set the range of sources that send multicast data to the multicast groups. Specify the **destination** parameter to set the range of multicast groups whose IGMP entries are not limited.

Example

Set the maximum number of IGMP entries that can be created on the GE1/0/0 to 60.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp limit 60
```

Create a named ACL **myacl**, and configure a rule that allows hosts to receive messages sent from multicast source 10.1.1.1 to multicast group 232.0.0.0/16. Set the maximum number of IGMP entries that can be created on the GE1/0/0 to 60,

 Copyright © Huawei Technologies Co., Ltd.

and exclude multicast group 232.0.0.0/16 whose IGMP entries do not need to be limited.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.1.1.1 0 destination 232.0.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp limit 60 except acl-name myacl
```

Related Topics

10.1.16 igmp global limit

10.1.38 limit (IGMP)

10.1.21 igmp max-response-time

Function

The **igmp max-response-time** command sets the maximum response time for IGMP General Query messages on an interface.

The **undo igmp max-response-time** command restores the default maximum response time for General IGMP Query messages.

By default, the maximum response time for IGMP General Query messages is 10s on an interface.

Format

igmp max-response-time *interval*

undo igmp max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large

number of Report messages sent from many hosts at the same time. The network may be congested when this situation occurs.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- This command is valid only for IGMPv2 and IGMPv3.
- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The **igmp max-response-time** command has the same function as the **max-response-time** command used in the IGMP view, except for the function range. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the maximum response time for IGMP General Query messages to 8 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp max-response-time 8
```

Related Topics

10.1.7 display igmp interface

10.1.39 max-response-time (IGMP)

10.7.28 multicast routing-enable

10.1.22 igmp on-demand

Function

The **igmp on-demand** command enables the IGMP on-demand function. This function enables a querier to maintain group memberships according to

requirements of group members, without sending Query messages. After IGMP on-demand is enabled on an interface, dynamic IGMP entries on the interface will never age out.

The **undo igmp on-demand** command restores the default configuration.

By default, a querier does not maintain group memberships according to requirements of group members, and dynamic entries are aged out when the aging time expires.

Format

igmp on-demand

undo igmp on-demand

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a standard IGMP working process, a querier sends General Query messages periodically and collects multicast membership information based on received Report and Leave messages. Multicast members respond to every Query message they receive. After IGMP on-demand is configured on the querier, the querier does not send Query messages, reducing IGMP packets exchanged between the querier and member hosts.

The IGMP on-demand function enables a querier to maintain multicast memberships based on requirements of members. The querier does not send Query messages to collect member information, reducing the number of IGMP messages exchanged between the querier and hosts.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- IGMP on-demand applies only to IGMPv2 and IGMPv3.
- If dynamic IGMP entries have been generated on the querier, run the **reset igmp group** command to clear these dynamic IGMP entries before running the **igmp on-demand** command.

 Copyright © Huawei Technologies Co., Ltd.

- After the **igmp on-demand** command is executed on an interface (IGMP querier):
  - The interface does not send IGMP Query messages
  - IGMP group entries are generated after the interface receives IGMP Report messages. The entries will never age out.
  - When the interface receives an IGMP Leave message, it deletes the corresponding IGMP entry.

Example

Enable the IGMP on-demand function on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp on-demand
```

Related Topics

10.7.28 multicast routing-enable

10.1.23 igmp prompt-leave

Function

The **igmp prompt-leave** command enables the fast leave function on an interface. This function enables an IGMP querier to delete IGMP entries immediately after receiving Leave messages from group members, without sending Group-Specific Query messages.

The **undo igmp prompt-leave** command disables fast leave on an interface.

By default, an IGMP querier sends a Group-Specific Query message after receiving a Leave message for a specific multicast group.

Format

igmp prompt-leave [**group-policy** { *acl-number* | **acl-name** *acl-name* }]

undo igmp prompt-leave

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-policy	Specifies an IGMP group policy. If this parameter is specified, the fast leave function takes effect only for multicast groups specified in the policy. When specifying this parameter, ensure that the referenced ACL has been configured. The device filters Leave messages on the interface based on the ACL. ● If a host leaves a multicast group in the range permitted by the ACL, the device immediately deletes the multicast group entry without sending a Group-Specific Query message. ● If a host leaves a multicast group out of the range permitted by the ACL, the device sends a Group-Specific Query message. If this parameter is not specified, the fast leave function takes effect for all multicast groups.	-
acl-number	Specifies the number of a basic ACL or an advanced ACL. This ACL defines a range of multicast groups.	The number of a basic ACL is an integer that ranges from 2000 to 2999. The number of an advanced ACL ranges from 3000 to 3999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In some scenarios, a querier interface connects to only one receiver host. If the host frequently switches between multiple multicast groups, you can configure the fast leave function on the interface so that the interface can quickly respond to Leave messages sent from the host. After the fast leave function is configured, the querier does not send a Group-Specific Query message after receiving a Leave message. Instead, the querier directly notifies the upstream multicast device that the host has left the multicast group. The fast leave function reduces delay in response to Leave messages and saves network bandwidth.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- IGMP fast leave applies only to IGMPv2 and IGMPv3.
- When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.
- When configuring an ACL to specify the range of multicast groups, pay attention to the following points:
  - When you run the **rule** command in the view of a basic ACL, set **source** to the address range of multicast groups that hosts can fast leave.
  - When you run the **rule** command in the view of an advanced ACL, set **source** to the multicast source address and **destination** to the range of multicast groups that hosts can fast leave.

Example

Create ACL 2005 and configure a rule that allows hosts to fast leave multicast groups in the range of 225.1.0.0/16. Configure fast leave on GE1/0/0 so that the entry of group 225.1.0.0/16 will be delete immediately after the interface receives an IGMP Leave message for the group GE1/0/0.

```
<Huawei> system-view
[Huawei] acl number 2005
[Huawei-acl-basic-2005] rule permit source 225.1.0.0 0.0.255.255
[Huawei-acl-basic-2005] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp prompt-leave group-policy 2005
```

Create an ACL named **myacl** and configure a rule that allows hosts to fast leave multicast groups in the range of 225.1.0.0/16. Configure fast leave on GE1/0/0 so that the entry of group 225.1.0.0/16 will be delete immediately after the interface receives an IGMP Leave message for the group GE1/0/0.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp prompt-leave group-policy acl-name myacl
```

Related Topics

10.1.7 display igmp interface

10.7.28 multicast routing-enable

10.1.24 igmp proxy

Function

The **igmp proxy** command enables IGMP proxy on an interface.

The **undo igmp proxy** command disables IGMP proxy on an interface.

By default, IGMP proxy is disabled on an interface.

Format

igmp proxy [**track nqa** *admin-name test-name*]

undo igmp proxy

Parameters

Parameter	Description	Value
track nqa *admin-name test-name*	Specifies the administrator name and test name of an NQA test instance.	The value of either *admin-name* or *test-name* is a string of 1 to 32 case-insensitive characters, spaces not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a simple tree topology, multicast routers directly connected to user network segments do not need to run any complicated multicast routing protocol (such as PIM). However, the upstream access devices have to manage many users because the multicast routers transparently transmit all IGMP messages from hosts. To reduce loads on the upstream device, configure IGMP proxy on the multicast

 Copyright © Huawei Technologies Co., Ltd.

routers. The multicast routers then collect and summarize Report/Leave messages received from downstream hosts before sending them to the upstream device. The multicast routers also maintain group memberships and forward multicast packets based on the group memberships. The upstream device considers the multicast routers as hosts.

IGMP proxy lacks a fault detection mechanism to trigger link switchover quickly. Therefore, multicast services may be interrupted for a long time when a link failure occurs. You can solve this problem by associating IGMP proxy with a network quality analysis (NQA) test instance. If you specify **track nqa** *admin-name test-name* in the command, IGMP proxy will be associated with the specified NQA test instance for end-to-end link status monitoring. When the NQA test instance detects a link failure on the primary IGMP proxy interface, the device configured with the IGMP proxy backup function can switch multicast traffic to the backup link to minimize the communication interruption time.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Precautions

A public network or VPN instance supports only one IGMP proxy interface

IGMP proxy conflicts with the following features:

- PIM: If the **pim sm** or **pim dm** command has been configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command is configured first, the **pim sm** or **pim dm** command cannot be used on the interface.
- IGMP: If the **igmp enable** command has been configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command is configured first, the **igmp enable** command cannot be used on the interface.
- Static group: After a static group is configured on an interface, the **igmp proxy** command cannot be used on the interface. If the **igmp proxy** command has been configured, no static group can be configured on the interface.

Example

Enable IGMP proxy on GE 1/0/0 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp proxy
```

Enable IGMP proxy on GE1/0/0, and associate GE1/0/0 with an NQA test instance named user test.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] destination-address ipv4 1.1.1.1
[Huawei-nqa-user-test] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp proxy track nqa user test
```

Related Topics

10.1.9 display igmp proxy group
10.1.10 display igmp proxy interface
10.1.11 display igmp proxy routing-table

10.1.25 igmp proxy backup

Function

The **igmp proxy backup** command configures a backup IGMP proxy interface.

The **undo igmp proxy backup** command cancels the configuration.

By default, IGMP proxy backup is disabled on an interface.

Format

igmp proxy backup

undo igmp proxy backup

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, the IGMP proxy function becomes unavailable if the upstream interface with IGMP proxy configured fails. To enhance reliability of the IGMP service, configure a backup IGMP proxy interface after configuring IGMP proxy on the upstream interface. If the upstream interface fails, the backup interface takes over the IGMP proxy service to resume multicast services.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Precautions

An instance allows only one IGMP proxy interface and one backup IGMP proxy interface. Only one backup IGMP proxy interface can be configured on a device.

IGMP proxy conflicts with the following features:

 Copyright © Huawei Technologies Co., Ltd.

- PIM: If the **pim sm** or **pim dm** command has been configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command is configured first, the **pim sm** or **pim dm** command cannot be used on the interface.
- IGMP: If the **igmp enable** command has been configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command is configured first, the **igmp enable** command cannot be used on the interface.
- Static group: After a static group is configured on an interface, the **igmp proxy backup** command cannot be used on the interface. If the **igmp proxy backup** command has been configured, no static group can be configured on the interface.

Example

Configure GE1/0/0 as a backup IGMP proxy interface in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp proxy backup
```

Related Topics

10.1.9 display igmp proxy group

10.1.10 display igmp proxy interface

10.1.11 display igmp proxy routing-table

10.1.26 igmp proxy interface reroute

Function

The **igmp proxy interface reroute** command deletes switchback delay configurations of IGMP proxy interfaces, so that the interfaces enter the switchback state immediately after the switchback trigger conditions are met.

Format

igmp proxy [**vpn-instance** *vpn-instance* | **all-instance**] **interface** [*interface-type interface-number*] **reroute**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance*	Specifies a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks ('').

Parameter	Description	Value
all-instance	Indicates all VPN instances.	-
interface *interface-type interface-number*	Specifies an IGMP proxy interface.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To delete switchback delay configurations of IGMP proxy interfaces, run the **igmp proxy interface reroute** command, after which the IGMP proxy interfaces enter the switchback state immediately after the switchback trigger conditions are met.

If neither **vpn-instance** *vpn-instance* nor **all-instance** is specified, the command deletes switchback delay configurations of IGMP proxy interfaces in the public network instance only.

Example

Delete switchback delay configurations of IGMP proxy interfaces in the public network instance.

```
<Huawei> igmp proxy interface reroute
Warning: This operation will lead to reroute IGMP proxy in the instance to which the interface belongs.
Continue? [Y/N]:Y
```

10.1.27 igmp query ip-source-policy

Function

The **igmp query ip-source-policy** command configures IGMP Query message filtering based on source addresses.

The **undo igmp query ip-source-policy** command restores the default configuration.

By default, no source address-based IGMP Query message filtering is configured.

Format

igmp query ip-source-policy { *basic-acl-number* | **acl-name** *acl-name* }

undo igmp query ip-source-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of an ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends forged IGMP Query messages with an IP addresses smaller than the querier IP address, the querier will be replaced by the attacker. As a result, the real querier cannot response to Report messages from group members and bandwidth is wasted. Source address-based IGMP Query message filtering can protect the querier from such attacks. After this function is configured on a device, the device accepts only the IGMP Query messages with source addresses permitted by the specified ACL. This function controls querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- IGMP Query messages are encapsulated into IP messages. This command is used to filter IGMP Query messages based on the source addresses in IP headers.
- This command configures a policy to filter IGMP Query messages based on source addresses. The ACL referenced in the policy defines the source addresses allowed. The device accepts only the IGMP Query messages with source addresses in the allowed range.

Example

Configure GE1/0/0 to accept only the IGMP Query messages with the source address 10.10.1.1.

```
<Huawei> system-view
[Huawei] multicast routing-enable
```

```
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.10.1.1 0
[Huawei-acl-basic-2001] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp query ip-source-policy 2001
```

10.1.28 igmp require-router-alert

Function

The **igmp require-router-alert** command configures an interface to discard IGMP messages without the Router-Alert Option.

The **undo igmp require-router-alert** command disables an interface from checking for the Router-Alert Option in IGMP messages.

By default, the device does not check for the Router-Alert Option in IGMP messages and processes all the IGMP messages received on an interface.

Format

igmp require-router-alert

undo igmp require-router-alert

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a packet to the corresponding protocol module for processing only when the destination address of the packet is a local interface address. Destination addresses of IGMP packets are multicast addresses but not interface addresses of multicast devices. Therefore, multicast devices do not send IGMP packets to the IGMP module, and the IGMP module cannot maintain group memberships.

The Router-Alert option in the IP header of an IGMP message solves this problem. If an IGMP message contains the Router-Alert option, the device sends the message to the routing protocol module.

You can configure the device to accept only IGMP messages with the Router-Alert option to improve IGMP security.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command has the same function as the **require-router-alert** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Configure GE1/0/0 to discard IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp require-router-alert
```

Related Topics

10.1.7 display igmp interface

10.1.30 igmp send-router-alert

10.7.28 multicast routing-enable

10.1.43 require-router-alert (IGMP)

10.1.29 igmp robust-count

Function

The **igmp robust-count** command sets an IGMP querier robustness variable on an interface.

The **undo igmp robust-count** command restores the default IGMP querier robustness variable on an interface.

By default, the IGMP querier robustness variable is 2.

Format

igmp robust-count *robust-value*

undo igmp robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the IGMP querier robustness variable.	The value is an integer that ranges from 2 to 5.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IGMP querier robustness variable specifies the retransmission count of IGMP packets to minimize impact of packet loss on the network.

On a shared network segment, a querier maintains IGMP-attached group memberships. The robustness variable affects the timeout interval of group memberships. The timeout interval of group memberships is calculated using the formula:

Timeout interval of group memberships = Interval for sending IGMP General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages certain times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the query interval configured using the **igmp timer query** or **timer query** command.
- Number of times the querier sends IGMPv2 Group-Specific Query messages or IGMPv3 Source-and-Group-Specific Query messages when the querier receives a Leave message

  When receiving an IGMP Leave message of a multicast group, the querier sends Group-Specific Query messages certain times specified by the robustness variable to check whether the group has members. When the querier receives a Report message indicating that source-group mapping changes, the querier sends Source-and-Group-Specific Query messages certain times specified by the robustness variable. The interval for sending Group-Specific Query messages and Source-and-Group-Specific Query messages can set using the **igmp lastmember-queryinterval** or **lastmember-queryinterval** command.

A larger robustness variable makes an IGMP querier more robust, but increases the timeout interval of group memberships.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **igmp robust-count** command has the same function as the **robust-count** command, except for the function range. The configuration in the IGMP view is

globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the querier robustness variable on GE1/0/0 to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp robust-count 3
```

Related Topics

10.1.7 display igmp interface

10.1.19 igmp lastmember-queryinterval

10.1.34 igmp timer query

10.1.37 lastmember-queryinterval (IGMP)

10.7.28 multicast routing-enable

10.1.48 robust-count (IGMP)

10.1.52 timer query (IGMP)

10.1.30 igmp send-router-alert

Function

The **igmp send-router-alert** command configures an interface to send IGMP messages containing the Router-Alert option in IP headers.

The **undo igmp send-router-alert** command disables an interface from sending IGMP messages containing the Router-Alert option in IP headers.

By default, the IP headers of IGMP messages sent by an interface contain the Router-Alert option.

Format

igmp send-router-alert

undo igmp send-router-alert

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

By default, the router sends IGMP messages that contain the Router-Alert option in IP headers. If the router needs to communicate with a device that does not support the Router-Alert option, run the **undo igmp send-router-alert** command to configure the router to send IGMP messages without the Router-Alert option. The **igmp send-router-alert** command is usually used together with the **igmp require-router-alert** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **igmp send-router-alert** command has the same function as the **send-router-alert** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Configure GE1/0/0 to send IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo igmp send-router-alert
```

Related Topics

10.1.7 display igmp interface

10.1.28 igmp require-router-alert

10.7.28 multicast routing-enable

10.1.49 send-router-alert (IGMP)

10.1.31 igmp ssm-mapping enable

Function

The **igmp ssm-mapping enable** command enables SSM mapping on an interface.

The **undo igmp ssm-mapping enable** command disables SSM mapping on an interface.

By default, SSM mapping is disabled on an interface.

Format

igmp ssm-mapping enable

undo igmp ssm-mapping enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM model allows only IGMPv3 hosts to specify the multicast sources which they want to receive data from. However, some hosts can only run IGMPv1 or IGMPv2. To enable these hosts to use the SSM service, configure IGMP SSM mapping on the router. IGMP SSM mapping is implemented based on static SSM mapping entries on the router. The router converts (*, G) information in IGMPv1 and IGMPv2 Report messages to (S, G) information according to static SSM mapping entries to provide the SSM service for IGMPv1 and IGMPv2 hosts.

The **igmp ssm-mapping enable** command enables SSM mapping on an interface. The mappings between multicast source addresses and group addresses take effect only when SSM mapping is enabled on an interface. SSM mappings are configured using the **ssm-mapping** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Enable SSM mapping on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ssm-mapping enable
```

Related Topics

10.1.7 display igmp interface

10.1.50 ssm-mapping (IGMP)

10.7.28 multicast routing-enable

10.1.32 igmp static-group

Function

The **igmp static-group** command configures a static multicast group on an interface.

 Copyright © Huawei Technologies Co., Ltd.

The **undo igmp static-group** command deletes a static multicast group from an interface.

By default, no static multicast group is configured on an interface.

Format

igmp static-group *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number*] [**source** *source-address*] }

igmp static-group *group-address* [**source** *source-address*] **mping-echo**

undo igmp static-group *group-address* [**source** *source-address*] **mping-echo**

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address. In batch configuration mode, this parameter specifies the start address of the multicast group range.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
inc-step-mask	Sets the step mask of group addresses in batch configuration mode.	-
group-mask	Specifies the step mask of a group address in batch configuration mode, that is, the gap between two consecutive group addresses.	The value is a wildcard mask format that ranges from 0.0.0.1 to 15.255.255.255, in dotted decimal notation.
group-mask-length	Specifies the step mask length in batch configuration mode.	The value is an integer that ranges from 4 to 32. If *group-mask-length* is used to configure the step mask and the **display current-configuration** command is used to display related configurations, the step mask of group addresses is displayed in *group-mask* format.
number *group-number*	Specifies the number of group addresses in batch configuration mode.	The value is an integer that ranges from 2 to 512.
source *source-address*	Specifies a multicast source address.	The address is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all multicast groups that an interface statically joins.	-
mping-echo	Configures the device to respond to multicast ping packets received on the interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure static multicast groups on user-side interfaces of the router in some scenarios, for example:

- There are long-term group members on a shared network segment, and the router needs to forward multicast data to these group members quickly and steadily.
- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the router considers that the multicast group always has members on the network segment of the interface. Therefore, the router always forwards multicast data of the multicast group.

The **igmp static-group** command is used on an interface connected to user hosts. The command can configure a single group or source-group binding on an interface at a time or configure multiple groups or source-group bindings in a batch.

If **mping-echo** is specified in the **igmp static-group** command, the interface cannot only send and receive multicast data packets but also respond to received multicast ping packets. This keyword enables the device to implement the multicast ping function without the need of a user host that can parse and respond to multicast ping packets. This makes fault location more flexible and convenient.

To add an interface to multiple multicast groups in batches, run the **igmp static-group** *group-address* **inc-step-mask** { *group-mask* | *group-mask-length* } **number** *group-number* command. To convert a *group-mask-length* value to a *group-mask* value, use the following formula: *group-mask* = 1<<(32 – *group-mask-length*). The << symbol represents the left-shift operator, using which the binary format of an

integer is shifted left for a specified number of digits. Extra binary digits out of the left boundary are discarded, and 0s are added at the right boundary. For example, 1<<0 represents 0.0.0.1, 1<<1 represents 0.0.0.2, and 1<<3 represents 0.0.0.4.If *group-mask-length* is set to configure the incremental mask of group addresses, when you use the **display current-configuration** command to view related configurations, the format of the displayed incremental mask of group address is converted to *group-mask*.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Follow-up Procedure

If a user host no longer needs to receive multicast data of a static group, delete the static group configuration.

Precautions

- The IGMP entries of static groups configured on an interface never time out. The router considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment of the interface.
- If you perform a second batch configuration by changing only *group-number* in the command and retaining the values of *group-address* and *group-mask* | *group-mask-length* configured in the first batch configuration, the second batch configuration overrides the first one.
- You can configure overlapping multicast group addresses in different batch configurations. When you configure multiple static multicast groups in a batch on an interface, do not delete any static group configuration before the system completes the batch static group configuration.

Example

Configure static multicast group 224.1.1.1 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 224.1.1.1
```

Configure the router to forward multicast packets from multicast source 192.168.11.1 to multicast group 232.1.1.1 through GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 232.1.1.1 source 192.168.11.1
```

Configure 10 static multicast groups on GE1/0/0 in a batch. Set the start multicast group address to 225.1.1.1 and the step mask length to 32.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 225.1.1.1 inc-step-mask 32 number 10
```

Configure 10 source-group bindings on GE1/0/0 in a batch. Set the start multicast group address to 232.1.1.1, the source address to 192.168.11.1, and the step mask length to 32.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 232.1.1.1 inc-step-mask 32 number 10 source
192.168.11.1
```

Configure static group 224.1.1.1 on GE1/0/0 connected to a user host network segment and enable the interface to respond to received multicast ping packets.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp static-group 224.1.1.1 mping-echo
```

Related Topics

10.1.4 display igmp group

10.7.28 multicast routing-enable

10.1.33 igmp timer other-querier-present

Function

The **igmp timer other-querier-present** command sets the other querier present timer on an interface.

The **undo igmp timer other-querier-present** command restores the default value of the other querier present timer on an interface.

The formula used to calculate the other querier present timer value is:

Other querier present timer = Robustness variable x Interval for sending IGMP General Query messages + 1/2 x Maximum response time for IGMP query messages

If the default values of the robustness variable, the interval for sending IGMP General Query messages, and the maximum response time for IGMP query messages are used, the other querier present timer value is 125s.

Format

igmp timer other-querier-present *interval*

undo igmp timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the IGMP querier to send Query messages to hosts on the network segment. If the querier fails to send Query messages, group memberships cannot be created or maintained. Non-queriers running IGMPv2 or IGMPv3 start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- The **igmp timer other-querier-present** command applies only to IGMPv2 and IGMPv3.
- The **igmp timer other-querier-present** command has the same function as the **timer other-querier-present**command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

NOTICE

If the other querier present timer value is shorter than the interval for sending IGMP General Query messages, the querier election is triggered frequently.

Example

On GE1/0/0, set the other querier present timer to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp timer other-querier-present 200
```

Related Topics

10.1.7 display igmp interface

10.1.34 igmp timer query

10.7.28 multicast routing-enable

10.1.51 timer other-querier-present (IGMP)

 Copyright © Huawei Technologies Co., Ltd.

10.1.34 igmp timer query

Function

The **igmp timer query** command sets the interval at which an interface sends IGMP General Query messages.

The **undo igmp timer query** command restores the default interval at which an interface sends IGMP General Query messages.

By default, an interface sends IGMP General Query messages at an interval of 60s.

Format

igmp timer query *interval*

undo igmp timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an interface sends IGMP General Query messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP querier sends IGMP General Query messages at an interval to check whether a local network segment has group members. This interval is the general query interval. You can set the general query interval based on situations on your network. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages certain times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is 1/4 of the general query interval. The robustness variable can be set using the **igmp robust-count** command or the **robust-count** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval. However, more bandwidth and resources are consumed in this case.
- The function of the **igmp timer query** command is the same as that of the **timer query** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

Set the interval at which GE1/0/0 sends General Query messages to 50 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp timer query 50
```

Related Topics

10.1.7 display igmp interface

10.1.29 igmp robust-count

10.1.33 igmp timer other-querier-present

10.7.28 multicast routing-enable

10.1.48 robust-count (IGMP)

10.1.52 timer query (IGMP)

10.1.35 igmp ttl-check

Function

The **igmp ttl-check** command enables the device to check the TTL values in received IGMP Report, Leave, and Query messages on a specific interface.

The **undo igmp ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received IGMP Report, Leave, and Query messages on an interface.

Format

igmp ttl-check

undo igmp ttl-check

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device against IGMP message attacks, run the **igmp ttl-check** command to enable the device to check the TTL values in received IGMP Report, Leave, and Query messages on a specific interface and discard such a message if its TTL value is not 1.

The **igmp ttl-check** command provides the same function as the **ttl-check** command run in the IGMP view, except that the **ttl-check** command configuration takes effect for all interfaces in the instance.

Configuration Impact

If both the **igmp ttl-check** and **ttl-check** commands are run, the **igmp ttl-check** configuration in the interface view takes precedence over the **ttl-check** configuration in the IGMP view.

Example

Enable the device to check the TTL values in received IGMP Report, Leave, and Query messages on a specific interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp ttl-check
```

10.1.36 igmp version

Function

The **igmp version** command specifies an IGMP version on an interface.

The **undo igmp version** command restores the default IGMP version on an interface.

By default, an interface runs IGMPv2.

Format

igmp version *version*

undo igmp version

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
version	Specifies the IGMP version running on the interface.	The value is integer that ranges from 1 to 3.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The router can identify IGMP messages of a version earlier than its own IGMP version but cannot identify IGMP messages of a later version. To ensure normal IGMP operation, ensure that the router runs the same IGMP version as member hosts or a later IGMP version.

If multiple routers exist on a shared network segment, configure the same IGMP version on all router interfaces connected to hosts. Otherwise, errors may occur in IGMP operation because interfaces running different IGMP versions send packets with different formats.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Configure IGMPv1 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] igmp version 1
```

Related Topics

10.1.7 display igmp interface

10.7.28 multicast routing-enable

10.1.37 lastmember-queryinterval (IGMP)

Function

The **lastmember-queryinterval** command configures interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages after receiving IGMP Leave messages from hosts.

 Copyright © Huawei Technologies Co., Ltd.

The **undo lastmember-queryinterval** command restores the default value.

By default, the interval at which an IGMP querier sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages is 1 second.

Format

lastmember-queryinterval *interval*

undo lastmember-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the querier receives a Leave message that a host sends to leave a multicast group, the querier periodically sends IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to check for other members in the multicast group. The **lastmember-queryinterval** command sets the interval at which the querier sends Last Member Query messages. The querier stops forwarding multicast data to the group if it receives no Report message from the group within the period specified by *interval* x *robust-value*. Here, *robust-value* is the robustness variable configured using the **igmp robust-count** or **robust-count** command.

If the querier does not receive any Report message within the specified period, it considers that the last member has left the group and no longer maintains the membership of this group.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- The **igmp lastmember-queryinterval** command is valid only when the IGMP querier runs IGMPv2 or IGMPv3.

 Copyright © Huawei Technologies Co., Ltd.

- This command has the same function as the **igmp lastmember-queryinterval** command, except for the function range. The configuration in the IGMP view is globally valid in the instance, whereas the configuration in the interface view is valid only for the current interface. The system prefers the configuration in the interface view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

Example

In the IGMP view, set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] lastmember-queryinterval 3
```

In VPN instance mvpn, set the interval for sending IGMP Group-Specific Query messages or IGMP Group-and-Source-Specific Query messages to 3 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] lastmember-queryinterval 3
```

Related Topics

10.1.7 display igmp interface

10.1.19 igmp lastmember-queryinterval

10.1.29 igmp robust-count

10.7.28 multicast routing-enable

10.1.48 robust-count (IGMP)

10.1.38 limit (IGMP)

Function

The **limit** command sets the maximum number of IGMP entries that can be created for an instance.

The **undo limit** command restores the maximum number of IGMP entries that can be created for an instance to the default value.

By default, the maximum number of IGMP entries that can be created for an instance varies according to device models:

- AR150&200 series: 128
- AR100&AR120&AR160&AR1200 series: 3000
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-Dand AR2204: 256
- AR2220, and AR2220E: 20480
- AR2204XE and AR2204XE-DC: 34816
- AR2240C: 33792
- AR2240 series and AR3200 series:

 Copyright © Huawei Technologies Co., Ltd.

  - Configured with SRU40: 33792
  - Configured with SRU60: 33792
  - Configured with SRU80: 34816
  - Configured with SRU100: 34816
  - Configured with SRU100E: 34816
  - Configured with SRU200: 34816
  - Configured with SRU200E: 34816
  - Configured with SRU400: 34816
- AR3600 series (SRUX5): 34816

Format

limit *number*

undo limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of IGMP entries that can be created for an instance.	The value is an integer that ranges from: ● 1 to 128 for the AR150&200 series ● 1 to 3000 for the AR100&AR120&AR160&AR1200 series ● 1 to 256 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D and AR2204 ● 1 to 20480 for the AR2220, and AR2220E ● 1 to 34816 for the AR2204XE and AR2204XE-DC ● AR2240C: 1 to 33792 ● AR2240 series and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 33792 – Configured with SRU60: 1 to 33792 – Configured with SRU80: 1 to 34816 – Configured with SRU100: 1 to 34816 – Configured with SRU100E: 1 to 34816 – Configured with SRU200: 1 to 34816 – Configured with SRU200E: 1 to 34816 – Configured with SRU400: 1 to 34816 ● 1 to 34816 for the AR3600 series (SRUX5)

 Copyright © Huawei Technologies Co., Ltd.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the maximum number of IGMP entries for an instance.

When the number of IGMP entries reaches the limit, the system does not create any IGMP entries. To enable the router to create more IGMP entries, delete useless entries or increase the limit. Alternatively, create static IGMP entries.

The number of IGMP entries is counted as follows:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry established with SSM mapping is counted as one entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Example

Set the maximum number of IGMP entries that can be created in the public network instance to 126.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] limit 126
```

Set the maximum number of IGMP entries that can be created in VPN instance mvpn to 126.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] limit 126
```

Related Topics

10.1.20 igmp limit
10.1.16 igmp global limit
10.7.28 multicast routing-enable

 Copyright © Huawei Technologies Co., Ltd.

10.1.39 max-response-time (IGMP)

Function

The **max-response-time** command sets a global maximum response time for IGMP General Query messages.

The **undo max-response-time** command restores the global maximum response time for IGMP General Query messages to the default value.

By default, the global maximum response time for IGMP General Query messages is 10 seconds.

Format

max-response-time *interval*

undo max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send IGMP Report messages immediately after they receive IGMP General Query messages, the querier on a shared network segment may receive a large number of Report messages sent from many hosts at the same time. The network may be congested when this situation occurs.

To avoid such situations, IGMPv2 and IGMPv3 messages specify the maximum response time for IGMP General Query messages. When a host running IGMPv2 or IGMPv3 receives an IGMP General Query message, it starts a timer for the group it wants to join. The timer length is a random value between 0 and the maximum response time. When the timer times out, the host sends a Report message.

The maximum response time specifies the deadline for the host to send a Report message. An appropriate maximum response time allows hosts to respond to Query messages quickly and prevents hosts from sending Report messages at the same time.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- This command applies only to IGMPv2 and IGMPv3.
- A smaller response time allows the router to learn multicast memberships more quickly but occupies more bandwidth and system resources.
- This command has the same function as the **igmp max-response-time** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the maximum response time for IGMP General Query messages to 8 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] max-response-time 8
```

In VPN instance mvpn, set the maximum response time for IGMP General Query messages to 8 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] max-response-time 8
```

Related Topics

10.1.7 display igmp interface

10.1.21 igmp max-response-time

10.7.28 multicast routing-enable

10.1.40 proxy source-lifetime

Function

The **proxy source-lifetime** command sets the timeout period for an (S, G) entry that an IGMP proxy-capable router generates.

The **undo proxy source-lifetime** command restores the default configuration.

By default, the timeout period of an (S, G) entry that an IGMP proxy-capable router generates is 210 seconds.

Format

proxy source-lifetime *interval*

undo proxy source-lifetime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of an (S, G) entry.	The value is an integer that ranges from 60 to 65535, in seconds. The default value is recommended for general use.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP proxy-capable router starts timer for each (S, G) entry and records the time when a multicast source S sends multicast packets. The **proxy source-lifetime** command sets the timeout period for (S, G) entries on an IGMP proxy-capable router. An IGMP proxy interface starts a timer when receiving the first multicast packet from a multicast source and resets the timer every time it receives a multicast packet from the multicast source. If the interface does not receive any multicast packet from the multicast source within the timeout period, it considers the (S, G) entry invalid.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Example

In the public network instance, Set the timeout period for (S, G) entries to 200s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] proxy source-lifetime 200
```

In VPN instance mvpn, set the timeout period for (S, G) entries to 200s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] proxy source-lifetime 200
```

10.1.41 proxy source-policy

Function

The **proxy source-policy** command configures an IGMP proxy-capable router to filter received multicast data packets based on source addresses or source and group addresses.

The **undo proxy source-policy** command restores the default configuration.

By default, an IGMP proxy-capable router does not filter received multicast data packets.

Format

proxy source-policy { *acl-number* | **acl-name** *acl-name* }

undo proxy source-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of a basic ACL or an advanced ACL. The ACL defines a multicast group range.	The number of a basic ACL is an integer in the range 2000 to 2999. The number of an advanced ACL is an integer in the range 3000 to 3999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an IGMP proxy-capable router needs to restrict multicast data packets sent from some multicast sources, run the **proxy source-policy** command configure the device to filter multicast data packets based on source addresses or source and group addresses. This command can also be used to filter the multicast data encapsulated in Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Precautions

The **proxy source-policy** command takes effect on a device only when IGMP proxy is enabled on the device.

 Copyright © Huawei Technologies Co., Ltd.

To reference a numbered ACL to a proxy source policy, run the **proxy source-policy** and **acl** commands together.

- In the basic ACL view, specify the **source** parameter in the **rule** command to set a multicast group range.
- In the advanced ACL view, specify **source** in the **rule** command to set a source address range and specify **destination** to set a group address range.

Named ACLs are classified into basic and advanced ACLs. The configuration rules of a named ACL are the same as that of a numbered ACL.

Example

In the public network instance, configure an IGMP proxy-capable router to accept the multicast data packets from multicast source 10.10.1.2 and to discard the multicast data packets from the multicast source 10.10.1.1.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.10.1.2 0
[Huawei-acl-basic-2001] rule deny source 10.10.1.1 0
[Huawei-acl-basic-2001] quit
[Huawei] igmp
[Huawei-igmp] proxy source-policy 2001
```

In the public network instance, configure an IGMP proxy-capable router to accept the multicast data packets sent from multicast source 10.10.1.2 to multicast group 232.1.0.0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.10.1.2 0 destination 232.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] igmp
[Huawei-igmp] proxy source-policy acl-name myacl
```

In VPN instance mvpn, configure an IGMP proxy-capable router to accept the multicast data packets from multicast source 10.10.1.2 and discard the multicast data packets from multicast source 10.10.1.1.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.10.1.2 0
[Huawei-acl-basic-2001] rule deny source 10.10.1.1 0
[Huawei-acl-basic-2001] quit
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] proxy source-policy 2001
```

Related Topics

10.1.24 igmp proxy

10.1.42 proxy ssm-policy

Function

The **proxy ssm-policy** command configures an SSM group address range for IGMP proxy.

The **undo proxy ssm-policy** command restores the default configuration.

The default SSM group address range for IGMP proxy is 232.0.0.0/8.

Format

proxy ssm-policy { *basic-acl-number* | **acl-name** *acl-name* }

undo proxy ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL. This ACL defines a range of multicast groups.	The sequence number is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default SSM group address range is 232.0.0.0 to 232.255.255.255. Generally, an IGMP proxy device provides the SSM service for hosts only when it receives Report messages with group address in this range. Sometimes, the SSM group address range must be narrowed to ensure security of a multicast network, and sometimes, the SSM group address range needs to be expanded because the default SSM group addresses are insufficient. In these cases, configure an SSM group address range on IGMP proxy devices. Ensure that all the multicast devices on the network are configured with the same SSM group address range.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance view.

Precautions

The SSM model can be used in the following situations:

- Multicast group addresses are in an SSM address range, IGMPv3 is running on the user network segment, and multicast source addresses are specified in Report messages.

 Copyright © Huawei Technologies Co., Ltd.

- Multicast group addresses are in an SSM address range, IGMPv1 or IGMPv2 is running on the user network segment, and SSM mapping is configured.

The **proxy ssm-policy** command works with the **acl** command. If a basic ACL is configured, you can specify **source** in the **rule** command to configure an SSM address range.

Example

In the public network instance, set the SSM group address range for IGMP proxy to 232.1.0.0/16.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Huawei-acl-basic-2000] quit
[Huawei] igmp
[Huawei-igmp] proxy ssm-policy 2000
```

In VPN instance mvpn, set the SSM group address range for IGMP proxy to 232.1.0.0/16.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Huawei-acl-basic-2000] quit
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] proxy ssm-policy 2000
```

10.1.43 require-router-alert (IGMP)

Function

The **require-router-alert** command configures the router to discard IGMP messages without the Router-Alert option.

The **undo require-router-alert** command disables the router from checking for the Router-Alert option in IGMP messages.

By default, the router does not check whether the received IGMP messages contain the Router-Alert option in IP headers, and it accepts all the received IGMP messages.

Format

require-router-alert

undo require-router-alert

Parameters

None

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a packet to the corresponding protocol module for processing only when the destination address of the packet is a local interface address. Destination addresses of IGMP packets are multicast addresses but not interface addresses of multicast devices. Therefore, multicast devices do not send IGMP packets to the IGMP module, and the IGMP module cannot maintain group memberships.

The Router-Alert option in IP packet headers solves this problem. This option indicates that a packet needs to be sent to the protocol module.

You can configure the router to accept only IGMP messages with the Router-Alert option. This configuration improves security of the IGMP service.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command has the same function as the **igmp require-router-alert** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, configure the router to discard IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] require-router-alert
```

In VPN instance mvpn, configure the router to discard IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] require-router-alert
```

Related Topics

10.1.7 display igmp interface

10.1.28 igmp require-router-alert

10.7.28 multicast routing-enable

 Copyright © Huawei Technologies Co., Ltd.

10.1.44 reset igmp control-message counters

Function

The **reset igmp control-message counters** command clears statistics about IGMP messages.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears IGMP message statistics in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Clears IGMP message statistics in all instances.	-
interface *interface-type interface-number*	Clears IGMP message statistics on a specified interface. If this parameter is not specified, the command clears IGMP statistics on all interfaces.	-
message-type	Clears statistics about IGMP messages of a specified type. If this parameter is not specified, the command clears statistics about all IGMP messages.	-
query	Clears statistics about Query messages received by an interface.	-
report	Clears statistics about Report messages received by an interface.	-

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

IGMP still operates normally after IGMP message statistics are deleted.

Example

Clear statistics about IGMP messages on all interfaces.

```
<Huawei> reset igmp control-message counters
```

Clear statistics about IGMP messages on GE1/0/0.

```
<Huawei> reset igmp control-message counters interface gigabitethernet 1/0/0
```

Related Topics

10.1.2 display igmp control-message counters

10.1.45 reset igmp explicit-tracking

Function

The **reset igmp explicit-tracking** command deletes information about the hosts with dynamic group memberships established through IGMP on an interface.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **explicit-tracking** { **all** | **interface** *interface-type interface-number* [**host** *host-address* [**group** *group-address* [**source** *source-address*]]] }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes information about the hosts with IGMP-attached group memberships on interfaces in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Deletes information about the hosts with IGMP-attached group memberships on interfaces in all instances.	-
all	Deletes information about all the hosts.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Deletes information about the hosts with IGMP-attached group memberships on a specified interface. If this parameter is not specified, the command deletes information about the hosts with IGMP-attached group memberships on all interfaces.	-
host *host-address*	Specifies the IP address of a host.	The address is in dotted decimal notation.
group *group-address*	Specifies the address of a multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
source *source-address*	Specifies the address of a multicast source.	The address is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete information about the hosts with dynamic group memberships established through IGMP on interfaces.

Example

Delete information about IGMP host 192.168.0.12 in group 232.1.1.1 on GE1/0/0.

```
<Huawei> reset igmp explicit-tracking interface gigabitethernet 1/0/0 host 192.168.0.12 group 232.1.1.1
```

Related Topics

10.1.3 display igmp explicit-tracking

10.1.46 reset igmp group

Function

The **reset igmp group** command deletes dynamic IGMP entries on interfaces.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes dynamic IGMP entries in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Deletes dynamic IGMP entries in all instances.	-
all	The first **all** deletes dynamic IGMP entries on all interfaces. The second **all** deletes all dynamic IGMP entries on a specified interface.	-
interface *interface-type interface-number*	Deletes dynamic IGMP entries on a specified interface.	-
group-address	Deletes dynamic IGMP entries of a specified group.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask	Sets the mask of a multicast source address or group address.	-
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.
source-mask	Specifies the mask of a multicast source address.	The mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command does not delete static group memberships configured on interfaces.

After IGMP entries on an interface are deleted, the interface can join the involved groups again.

NOTICE

After IGMP group memberships are cleared, group members may fail to receive multicast data. Therefore, confirm your operation before clearing IGMP group information.

Example

Delete dynamic IGMP entries on all interfaces.

```
<Huawei> reset igmp group all
```

Delete all dynamic IGMP entries on GE1/0/0.

```
<Huawei> reset igmp group interface gigabitethernet 1/0/0 all
```

Delete the IGMP entries of group 225.0.0.1 on GE1/0/0.

```
<Huawei> reset igmp group interface gigabitethernet 1/0/0 225.0.0.1
```

Delete IGMP entries of groups 225.1.1.0 to 225.1.1.255 on GE1/0/0.

```
<Huawei> reset igmp group interface gigabitethernet 1/0/0 225.1.1.0 mask 255.255.255.0
```

Related Topics

10.1.4 display igmp group

10.1.47 reset igmp group ssm-mapping

Function

The **reset igmp group ssm-mapping** command deletes group memberships established with SSM mapping.

Format

reset igmp [**vpn-instance** *vpn-instance-name* | **all-instance**] **group ssm-mapping** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *group-mask* | *group-mask-length* }] } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Deletes group memberships established with SSM mapping in a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Deletes group memberships established with SSM mapping in all instances.	-
all	First **all**: deletes group memberships established with SSM mapping on all interfaces. Second **all**: deletes all group membership established with SSM mapping on the specified interface.	-
interface *interface-type interface-number*	Deletes group memberships established with SSM mapping on a specified interface.	-
group-address	Deletes the group membership established with SSM mapping for a specified group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Sets the mask of a multicast group address.	-
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can use this command to delete group memberships established with SSM mapping.

NOTICE

After IGMP group memberships are cleared, group members may fail to receive multicast data. Therefore, confirm your operation before clearing IGMP group information.

Example

Delete group memberships established with SSM mapping on all the interfaces.

```
<Huawei> reset igmp group ssm-mapping all
```

Related Topics

10.1.13 display igmp ssm-mapping

10.1.48 robust-count (IGMP)

Function

The **robust-count** command sets a global robustness variable for an IGMP querier.

The **undo robust-count** command restores the default robustness variable.

By default, the robustness variable of an IGMP querier is 2.

Format

robust-count *robust-value*

undo robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an IGMP querier.	The value is an integer that ranges from 2 to 5.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The IGMP querier robustness variable specifies the retransmission count of IGMP packets to minimize impact of packet loss on the network.

On a shared network, a querier maintains IGMP-attached group memberships on an interface. The robustness variable determines the timeout interval of group memberships. The timeout interval of group memberships is calculated using the following formula:

Timeout interval of group memberships = Interval for sending IGMP General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the queries sends General Query messages at startup

  When the querier starts, it sends General Query messages certain times specified by the robustness variable to query members of multicast groups. The interval for sending General Query messages during this process is 1/4 of the interval configured using the **igmp timer query** or **timer query** command.
- In IGMPv2 and IGMPv3, the robustness variable determines the number of times the querier sends Group-Specific Query or Source-and-Group-Specific Query messages.

  When receiving an IGMP Leave message of a multicast group, the querier sends Group-Specific Query messages certain times specified by the robustness variable to check whether the group has members. When the querier receives a Report message indicating that source-group mapping changes, the querier sends Source-and-Group-Specific Query messages certain times specified by the robustness variable. The interval for sending Group-Specific Query messages and Source-and-Group-Specific Query messages can be set using the **igmp lastmember-queryinterval** or **lastmember-queryinterval** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- A larger robustness variable makes an IGMP querier more robust, but increases the timeout interval of group memberships.
- This command has the same function as the **igmp robust-count** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view is valid only for the current interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, set the robustness variable of an IGMP querier to 3.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] robust-count 3
```

In VPN instance mvpn, set the robustness variable of an IGMP querier to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] robust-count 3
```

Related Topics

10.1.7 display igmp interface

10.1.29 igmp robust-count

10.7.28 multicast routing-enable

10.1.49 send-router-alert (IGMP)

Function

The **send-router-alert** command configures the router to send IGMP messages with the Router-Alert option in IP headers.

The **undo send-router-alert** command configures the router to send IGMP messages without the Router-Alert option.

By default, IGMP messages sent by the router contain the Router-Alert option.

Format

send-router-alert

undo send-router-alert

Parameters

None

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP messages sent by the router contain the Router-Alert option in their IP headers. If the router needs to communicate with a device that does not support the Router-Alert option, run the **undo send-router-alert** command to configure the router to send IGMP messages without the Router-Alert option. The

send-router-alert command is usually used together with the **require-router-alert** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command has the same function as the **igmp send-router-alert** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the IGMP view, configure the router to send IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] undo send-router-alert
```

In VPN instance mvpn, configure the router to send IGMP messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] undo send-router-alert
```

Related Topics

10.1.7 display igmp interface

10.1.30 igmp send-router-alert

10.7.28 multicast routing-enable

10.1.43 require-router-alert (IGMP)

10.1.50 ssm-mapping (IGMP)

Function

The **ssm-mapping** command configures an SSM mapping rule to map a multicast source to a group address.

The **undo ssm-mapping** command deletes an SSM mapping rule.

By default, no SSM mapping rule is configured.

Format

ssm-mapping *group-address* { *group-mask* | *group-mask-length* } *source-address*

 Copyright © Huawei Technologies Co., Ltd.

undo ssm-mapping { *group-address* { *group-mask* | *group-mask-length* } [*source-address*] | **static all** }

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
group-mask	Specifies the mask of a multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.
static all	Deletes all the configured static SSM mapping entries.	-

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts that support only IGMPv1 and IGMPv2 cannot join SSM groups. To enable multicast devices to provide the SSM service for these hosts, configure SSM mapping on the multicast devices. An SSM mapping entry maps a multicast source to a multicast group. After SSM mapping entries are configured on a multicast device, the device can convert (*, G) information in Report messages of IGMPv1 and IGMPv2 to (S, G) information.

The default range of SSM group addresses is 232.0.0.0 to 232.255.255.255. You can use the **ssm-policy** command to change the address range. All multicast groups out of this range are ASM groups.

The configured SSM mapping entries take effect only after the **igmp ssm-mapping enable** command is run on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- You can run this command several times to configure multiple static SSM mapping entries.
- To delete an SSM mapping entry, run the **undo ssm-mapping** *group-address* { *group-mask* | *group-mask-length* } *source-address* command. The **undo ssm-mapping static all** command deletes all the SSM mapping entries. Do not use this command unless necessary.

Example

In the public network instance, configure an SSM mapping entry to map multicast source address 10.8.8.8 to group address 225.5.5.5/32.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] ssm-mapping 225.5.5.5 32 10.8.8.8
```

In VPN instance mvpn, configure an SSM mapping entry to map multicast source address 10.8.8.8 to group address 225.5.5.5/32.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] ssm-mapping 225.5.5.5 32 10.8.8.8
```

Related Topics

10.1.13 display igmp ssm-mapping

10.1.31 igmp ssm-mapping enable

10.7.28 multicast routing-enable

10.3.79 ssm-policy (IPv4)

10.1.51 timer other-querier-present (IGMP)

Function

The **timer other-querier-present** command sets the other querier present timer.

The **undo timer other-querier-present** command restores the default value of the other querier present timer.

The formula used to calculate the other querier present timer value is:

Other querier present timer = Robustness variable x Interval for sending IGMP General Query messages + 1/2 x Maximum response time for IGMP query messages

If the robustness variable, the interval for sending IGMP General Query messages, and the maximum response time for IGMP Query messages all use default values, the other querier present timer value is 125 seconds.

Format

timer other-querier-present *interval*

undo timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer value.	The value is an integer that ranges from 60 to 300, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the IGMP querier to send Query messages to hosts on the network segment. If the querier fails to send Query messages, group memberships cannot be created or maintained. Non-queriers running IGMPv2 or IGMPv3 start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- This command applies only to IGMPv2 and IGMPv3.
- This command has the same function as the **igmp timer other-querier-present** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when the configuration in the interface view is not done.

NOTICE

If the other querier present timer value is shorter than the interval for sending IGMP General Query messages, the querier election is triggered frequently.

Example

In the IGMP view, set the other querier present timer to 200 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] timer other-querier-present 200
```

In VPN instance mvpn, set the other querier present timer to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] timer other-querier-present 200
```

Related Topics

10.1.7 display igmp interface

10.1.33 igmp timer other-querier-present

10.7.28 multicast routing-enable

10.1.52 timer query (IGMP)

Function

The **timer query** command sets a global interval for sending IGMP General Query messages.

The **undo timer query** command restores the default interval for sending IGMP General Query messages.

By default, the interval for sending IGMP General Query messages is 60 seconds.

Format

timer query *interval*

undo timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending IGMP General Query messages	The value is an integer that ranges from 1 to 18000, in seconds.

Views

IGMP view of the public network instance, IGMP view of a VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IGMP querier sends IGMP General Query messages at an interval to check whether a local network segment has group members. This interval is the general query interval. You can set the general query interval based on situations on your network. The general query interval affects the following processes:

- When the querier starts, it sends General Query messages certain times specified by the robustness variable to query members of multicast groups. The message sending interval during this process is 1/4 of the interval for sending General Query messages. The robustness variable is configured using the **igmp robust-count** or **robust-count** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

- The querier is more sensitive when it sends General Query messages at a shorter interval. However, more bandwidth and router resources are consumed in this case.
- This command has the same function as the **igmp timer query** command used in the interface view. The configuration in the IGMP view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the IGMP view. The configuration in the IGMP view is used only when no configuration is performed in the interface view.

Example

In the public network instance, set the global interval for sending IGMP General Query messages to 125 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp
[Huawei-igmp] timer query 125
```

In VPN instance mvpn, set the global interval for sending IGMP General Query messages to 125 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] igmp vpn-instance mvpn
[Huawei-igmp-mvpn] timer query 125
```

Related Topics

10.1.7 display igmp interface
10.1.34 igmp timer query
10.7.28 multicast routing-enable

10.1.53 ttl-check (IPv4)

Function

The **ttl-check** command enables the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces.

The **undo ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received IGMP Report, Leave, and Query messages.

Format

ttl-check

undo ttl-check

Parameters

None

Views

IGMP view of the public network instance or IGMP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

To protect a device against IGMP message attacks, run the **ttl-check** command to enable the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces and discard such a message if its TTL value is not 1.

Example

Enable the device to check the TTL values in received IGMP Report, Leave, and Query messages on all interfaces.

```
<Huawei> system-view
[Huawei] igmp
[Huawei-igmp] ttl-check
```

10.2 MLD Configuration Commands

NOTE

AR120 series do not support this function.

10.2.1 display default-parameter mld

Function

The **display default-parameter mld** command displays default MLD configurations.

Format

display default-parameter mld

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check default MLD parameter settings even after MLD parameters are modified. This command helps you determine which MLD parameters have been modified.

Example

Display default MLD configurations.

```
<Huawei> display default-parameter mld
  MLD View Default Configurations:
  --------------------------------
  Lastmember-queryinterval: 1 s
  Lastmember-query time: 2 s
  Max-response-time: 10 s
  Require-router-alert: disabled
  Robust-count: 2
  Send-router-alert: enabled
  Ssm-mapping: disabled
  Timer query: 125 s

  Interface View Default Configurations:
  --------------------------------------
  Group-policy: disabled
  Last listener query time: 2 s
  Lastlistener-query-interval: 1 s
  Max-response-time: 10 s
  Other-querier-present-timer-expiry: off
  Prompt-leave: disabled
  Require-router-alert: disabled
  Robust-count: 2
  Send-router-alert: enabled
  Ssm-mapping: disabled
  Startup-query-timer-expiry: off
  Static-group:  disabled
```

 Copyright © Huawei Technologies Co., Ltd.

```
Timer query: 125 s
Version: 2
```

Table 10-20 Description of the display default-parameter mld command output

Item	Description
MLD View Default Configurations	Default configurations in the MLD view.
Lastmember-queryinterval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. To set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages, run the **lastlistener-queryinterval (MLD view)** command in the MLD view or the **mld lastlistener-queryinterval** command in the interface view.
Lastmember-query time	Last listener query time, equaling Lastmember-query-interval x Robust-count.
Max-response-time	Maximum response time for MLD Query messages. To set the maximum response time for MLD Query messages, run the **max-response-time (MLD view)** command in the MLD view or the **mld max-response-time** command in the interface view.
Require-router-alert	Whether the device checks the Router-Alert option in the received MLD message. To set whether the device checks the Router-Alert option in the received MLD message, run the **require-router-alert (MLD view)** command in the MLD view or the **mld require-router-alert** command in the interface view.
Robust-count	Robustness variable of the MLD querier. To set the robustness variable of an MLD querier, run the **robust-count (MLD view)** command in the MLD view or the **mld robust-count** command in the interface view.
Send-router-alert	Whether the MLD messages sent from the device carry the Router-Alert option. To set whether the MLD messages sent from the device carry the Router-Alert option, run the **send-router-alert (MLD view)** command in the MLD view or the **mld send-router-alert** command in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ssm-mapping	Whether SSM mapping is enabled. To enable SSM mapping, run the **mld ssm-mapping enable** command in the interface view.
Timer query	Interval for sending MLD General Query messages. To set the interval for sending MLD General Query messages, run the **timer query (MLD view)** command in the MLD view or the **mld timer query** command in the interface view.
Interface View Default Configurations	Default configurations in the interface view.
Group-policy	Whether a multicast group filtering policy is configured. To configure a multicast group filtering policy, run the **mld group-policy** command.
Last listener query time	Last listener query time, equaling Lastlistener-query-interval x Robust-count.
Lastlistener-query-interval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Other-querier-present-timer-expiry	Status of the other querier present timer. ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
Prompt-leave	Whether the fast leave function is configured. To configure the fast leave function, run the **mld prompt-leave** command.
Startup-query-timer-expiry	Status of the query timer on the interface that functions as the querier. ● off: The interface has sent Query messages. ● on: The interface has not finished sending Query messages.
Static-group	Whether static multicast groups are configured. To configure a static multicast group on an interface, run the **mld static-group** command.
Version	MLD version number. MLD has two versions: MLDv1 and MLDv2. To set the MLD version, run the **mld version** command.

 Copyright © Huawei Technologies Co., Ltd.

10.2.2 display mld control-message counters

Function

The **display mld control-message counters** command displays statistics about MLD control messages.

Format

display mld control-message counters [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about MLD messages on a specified interface. If this parameter is not specified, the command displays statistics about MLD messages on all interfaces.	-
message-type	Displays statistics about MLD messages of a specified type. If this parameter is not specified, the command displays statistics about all types of MLD messages.	-
query	Displays statistics about Query messages received by the interface. Query messages are sent from a querier.	-
report	Displays statistics about Report messages received by the interface. Report messages are sent by hosts to join a multicast group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check the number of MLD control messages sent and received on an interface.

Example

Display statistics about the MLD messages sent and received by GE1/0/0.

```
<Huawei> display mld control-message counters interface gigabitethernet 1/0/0
Interface message counter information
 GigabitEthernet1/0/0(FE80::219:74FF:FE59:3302):
 Message Type              Sent       Valid      Invalid    Ignore
 ---------------------------------------------------------------
 General Query             45         0          0          0
```

```
Group Query              0          0          0          0
Source Group Query         0          0          0          0
-----------------------------------------------------------------
MLDV1
Report ASM               0          35679      0          0
Report SSM               0          0          0          0
-----------------------------------------------------------------
DONE  ASM                 0          0          0          0
DONE  SSM                 0          0          0          0
-----------------------------------------------------------------
MLDV2
ISIN Report              0          0          0          0
ISEX Report              0          0          0          0
TOIN Report               0          0          0          0
TOEX Report               0          0          0          0
ALLOW Report               0          0          0          0
BLOCK Report              0          0          0          0
Source Records Total       0          0          0          0
-----------------------------------------------------------------
Others                   -          -          0          0
-----------------------------------------------------------------
```

Table 10-21 Description of the display mld control-message counters interface gigabitethernet 1/0/0 command output

Item	Description
Interface message counter information	Statistics about MLD messages on an interface.
GigabitEthernet1/0/0(FE80::219:74FF:FE59:3302)	Interface type and interface number (IPv6 link-local address).
Message Type	Type of the MLD messages.
Sent	Number of MLD messages sent from the interface.
Valid	Number of valid MLD messages received by the interface.
Invalid	Number of invalid MLD messages received by the interface.
Ignore	Number of received MLD messages ignored by the interface.
General Query	Number of MLD General Query messages.
Group Query	Number of MLD Multicast Address Specific Query messages.
Source Group Query	Number of MLD Multicast Address and Source Specific Query messages.
Report ASM	Number of MLDv1 Multicast Listener Report messages with multicast group addresses in the ASM group address range.

Item	Description
Report SSM	Number of MLDv1 Multicast Listener Report messages with multicast group addresses in the SSM group address range.
DONE ASM	Number of MLDv1 Multicast Listener Done messages with multicast group addresses in the ASM group address range.
DONE SSM	Number of MLDv1 Multicast Listener Done messages with multicast group addresses in the SSM group address range.
ISIN Report	Number of MLDv2 Multicast Listener ISIN Report messages.
ISEX Report	Number of MLDv2 Multicast Listener ISEX Report messages.
TOIN Report	Number of MLDv2 Multicast Listener TOIN Report messages.
TOEX Report	Number of MLDv2 Multicast Listener TOEX Report messages.
ALLOW Report	Number of MLDv2 Multicast Listener ALLOW Report messages.
BLOCK Report	Number of MLDv2 Multicast Listener BLOCK Report messages.
Source Records Total	Number of multicast sources carried in MLDv2 messages.
Others	Total number of ignored MLD messages and invalid MLD messages whose types cannot be identified.

Related Topics

10.2.36 reset mld control-message counters

10.2.3 display mld explicit-tracking

Function

The **display mld explicit-tracking** command displays information about the MLDv2 hosts that join the specific source and group in INCLUDE mode.

Format

display mld explicit-tracking [**interface** *interface-type interface-number* [**host-address** *ipv6-host-address* | **group** *ipv6-group-address* **source** *ipv6-source-address*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about MLDv2 hosts that join a specified multicast source in INCLUDE mode on a specified interface. If this parameter is not specified, the command displays information about MLDv2 hosts that join a specified multicast source in INCLUDE mode on all interfaces.	-
host-address *ipv6-host-address*	Specifies the link-local address of a host.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
group *ipv6-group-address*	Specifies the IPv6 address of a multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the MLDv2 hosts that join the specific source and group in INCLUDE mode.

```
<Huawei> display mld explicit-tracking
Explicit-tracking information
```

```
Total 2 hosts, 4 entries

GigabitEthernet1/0/0(FE80::2:4)
 0001.Host: FE80::224
      Uptime: 00:02:47
      Expires: 00:01:33
      (S, G) List:
        Group: FF44::1
            Source: FC00:0:0:1::1
              Uptime: 00:02:47
              Time since last refresh: 00:02:47
            Source: FC00:0:0:2222::3
              Uptime: 00:02:47
              Time since last refresh: 00:02:47
 0002.Host: FE80::225
      Uptime: 00:01:59
      Expires: 00:02:21
      (S, G) List:
        Group: FF44::1
            Source: FC00:0:0:1::1
              Uptime: 00:01:59
              Time since last refresh: 00:01:59
            Source: FC00:0:0:1::3
              Uptime: 00:01:59
              Time since last refresh: 00:01:59
```

Table 10-22 Description of the display mld explicit-tracking command output

Item	Description
Explicit-tracking information	Host information.
Total 2 hosts, 4 entries	Two hosts and four (S, G) entries in total.
GigabitEthernet1/0/0(FE80::2:4)	Interface type and interface number (IPv6 link-local address).
Host	IPv6 host address.
Uptime	Running time after a host joins a multicast group. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Expires	Predicted timeout period of a host. After the host times out, the host is deleted from the MLD member list. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
(S, G) List	List of (S, G) entries.
Group	IPv6 multicast group address.
Source	IPv6 unicast address of a multicast source.
Time since last refresh	Time since the host joins a multicast group last time. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.

Related Topics

10.2.37 reset mld explicit-tracking

10.2.4 display mld group

Function

The **display mld group** command displays information about MLD groups that hosts have dynamically joined by sending Report messages.

Format

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* [**verbose**]

display mld group [**interface** *interface-type interface-number*] **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
interface *interface-type interface-number*	Specifies the type and number of an interface. If this parameter is not specified, the command displays MLD group membership information on all interfaces.	-
verbose	Displays detailed information about a multicast group. If this parameter is not specified, the command displays only the summary of the MLD group.	-
entry-number	Displays statistics about MLD multicast groups that hosts dynamically join.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check information about multicast groups that have established memberships.

Example

Display detailed information about all multicast groups that the interface dynamically joins.

```
<Huawei> display mld group verbose
Total entry on this router: 1
Interface group report information of VPN-Instance: public net
```

```
Limited entry of this VPN-Instance: -
GigabitEthernet1/0/0(FE80::2E0:49FF:FE29:1103):
 Total entry on this interface: 1
 Limited entry on this interface: -
 Total 1 MLD Group reported
  Group: FF05::2
    Uptime: 00:01:07
    Expires: 00:03:45
    Last reporter: FE80::215:E9FF:FEAC:7666
    Last-listener-query-counter: 0
    Last-listener-query-timer-expiry: off
    Group mode: exclude
    Version1-host-present-timer-expiry: 00:03:45
```

Display statistics about MLD multicast groups that hosts dynamically join in the public network instance.

```
<Huawei> display mld group entry-number
Interface group report information of VPN-Instance: public net
  Total 100 MLD Groups reported
 Vlanif100(FE80:2300::4):
  Total 100 MLD Groups reported
```

Table 10-23 Description of the display mld group verbose command output

Item	Description
Total entry on this router	Total number of dynamic MLD multicast groups on the router.
Interface group report information of VPN-Instance	VPN instance to which the group carried in the Multicast Listener Report message received on the interface belongs.
Limited entry of this VPN-Instance	Maximum number of MLD entries that can be created for this instance.
GigabitEthernet1/0/0(FE80::2E0:49FF:FE29:1103)	Interface type and interface number (IPv6 link-local address).
Total entry on this interface	Total number of dynamic MLD multicast groups on the interface.
Limited entry on this interface	Maximum number of MLD entries that the current interface can create.
Total 1 MLD Group reported	One MLD Report message is received on the interface.
Group	IPv6 address of an IPv6 multicast group.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Uptime	Time since a multicast group is discovered. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Timeout period of a multicast group.
Last reporter	Link-local address of the last host that sends a Multicast Listener Report message.
Last-listener-query-counter	Number of times for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Last-listener-query-timer-expiry	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Group mode	Filter mode of multicast groups, that is, exclude or include.
Version1-host-present-timer-expiry	Timeout period of an MLDv1 host.

Related Topics

10.2.38 reset mld group

10.2.5 display mld group ssm-mapping

Function

The **display mld group ssm-mapping** command displays information about multicast group entries established with MLD SSM mapping.

Format

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* **ssm-mapping** [**verbose**]

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address. If this parameter is not specified, the command displays information about all multicast group entries established with SSM mapping.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
interface *interface-type interface-number*	Displays information about the multicast group entries established with SSM mapping on a specified interface. If this parameter is not specified, the command displays information about multicast group entries established with SSM mapping on all interfaces.	-
verbose	Displays detailed information about multicast group entries established with SSM mapping. If this parameter is not specified, the command displays only the summary of multicast groups mapped by SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display mld group ssm-mapping** command to view information about multicast group entries that are established with SSM mapping. SSM

mapping entries can be configured using the **ssm-mapping (MLD view)** command.

Example

Display detailed information about all multicast group entries established with SSM mapping.

```
<Huawei> display mld group ssm-mapping verbose
Total entry on this router: 1
Interface group report information of VPN-Instance: public net
 Limited entry of this VPN-Instance: -
 GigabitEthernet1/0/0(FE80::DD:84):
  Total entry on this interface: 1
  Limited entry on this interface: -
  Total 1 MLD SSM-Mapping Group reported
   Group: FF36::1
     Uptime: 00:00:13
     Expires: 00:04:07
     Last reporter: FE80::10
     Last-listener-query-counter: 0
     Last-listener-query-timer-expiry: off
     Group mode: exclude
     Version1-host-present-timer-expiry: 00:04:07
```

Display detailed information about the multicast groups configured with SSM mapping that hosts dynamically join in the public network instance.

```
<Huawei> display mld group ssm-mapping entry-number
Interface group report information of VPN-Instance: public net
  Total 100 MLD SSM-Mapping Groups reported
 Vlanif100(FE80:2300::4):
  Total 100 MLD SSM-Mapping Groups reported
```

Table 10-24 Description of the display mld group ssm-mapping verbose command output

Item	Description
Total entry on this router	Number of multicast group entries established with SSM mapping on the router.
Interface group report information of VPN-Instance	VPN instance to which the multicast group on the interface belongs.
Limited entry of this VPN-Instance	Maximum number of multicast group entries that can be generated in the VPN instance.
GigabitEthernet1/0/0(FE80::DD:84)	Interface type and interface number (IPv6 link-local address).
Total entry on this interface	Number of multicast group entries established with SSM mapping on the interface.
Limited entry on this interface	Maximum number of multicast group entries that can be generated on the interface.
Total 1 MLD SSM-Mapping Group reported	Total number of SSM mapping groups is 1.
Group	Multicast group address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Uptime	Time since a multicast group is discovered. The time format is as follows: ● If the time is shorter than or equal to 24 hours, the format is hours:minutes:seconds. ● If the time is longer than 24 hours but shorter than or equal to one week, the format is days:hours. ● If the time is longer than one week, the format is weeks:days.
Expires	Scheduled time after which a group is deleted from the MLD group list.
Last reporter	Link-local address of the last host that sends a Multicast Listener Report message.
Last-listener-query-counter	Number of times for sending Last Listener Query messagesMulticast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Last-listener-query-timer-expiry	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.
Group mode	Filter mode of the multicast group, that is, include or exclude.
Version1-host-present-timer-expiry	Timeout period of an MLDv1 host.

Related Topics

10.2.42 ssm-mapping (MLD view)
10.2.39 reset mld group ssm-mapping

10.2.6 display mld group static

Function

The **display mld group static** command displays information about static MLD multicast groups on interfaces.

Format

display mld group [*ipv6-group-address*] **static** [**up** | **down**] [**verbose**]

display mld group [*ipv6-group-address*] **static interface-number**

display mld group [*ipv6-group-address* | **interface** *interface-type interface-number*]* **static** [**verbose**]

display mld group static interface *interface-type interface-number* **entry-number**

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address. If this parameter is not specified, the command displays information about all multicast groups with memberships.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
up | **down**	Displays information about an Up or Down interface. If this parameter is not specified, the command displays information about all interfaces.	-
verbose	Displays detailed information about the interfaces that statically join MLD multicast groups or source-specific multicast groups. If this parameter is not specified, the command displays only the summary of the MLD group.	-
interface-number	Displays the number of the interfaces that statically join MLD multicast groups.	-
interface *interface-type interface-number*	Displays information about the MLD multicast groups that the specified interface statically joins.	-
entry-number	Displays the number of the MLD multicast groups that the interface statically joins.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mld group static** command to view information about the multicast groups and the interfaces that statically join MLD multicast groups or source-specific multicast groups. To configure a static multicast group on an interface, run the **mld static-group** command.

Example

Display information about statically joined MLD groups.

```
<Huawei> display mld group static
Static join group information
 Total 2 entries, Total 2 active entries
  (*, FF25::1)
  Interface:GE1/0/0
  State:UP
  Expires:Never

  (*, FF25:100::1)
  Interface:GE1/0/0
  State:UP
  Expires:Never
```

Table 10-25 Description of the display mld group static command output

Item	Description
Static join group information	Information about the MLD multicast groups that a router statically joins.
Total 2 entries, Total 2 active entries	Total number of static multicast groups and active entries set on the router.
(*, FF25::1)	(*, G) entry.
Interface:GE1/0/0	Interface where the multicast group exists.
State	Status of an entry.
Expires	Timeout period of a multicast group.

Display detailed information about all static MLD multicast groups on an interface.

```
<Huawei> display mld group static verbose
Static join group information
 Total 1 entry
```

```
 00001.(*, FF25::1)
    Total List of 2 joined interfaces
    1.GigabitEthernet0/0/1
       State:            UP
       Reference Count:   1
       Multicast Boundary:YES
       Outgoing Interface:YES
    2.GigabitEthernet0/0/2
       State:            UP
       Reference Count:   1
       Multicast Boundary:YES
       Outgoing Interface:YES
```

Table 10-26 Description of the display mld group static verbose command output

Item	Description
Static join group information	Information about the multicast groups that an interface statically joins.
Total 1 entry	Number of static MLD group memberships on the device.
00001.(*, FF25::1)	(*, G) entry.
Total List of 2 joined interfaces	List of the interfaces that statically join multicast groups.
1.GigabitEthernet0/0/1	Type and number of the interface.
State	Status of an interface, including: ● UP: The interface is working properly. ● DOWN: An error occurs on the physical link of the interface.
Reference Count	Number of times when a multicast group on the current interface is referenced.
Multicast Boundary	Whether the multicast forwarding boundary is configured.
Outgoing Interface	Whether the downstream interfaces exist.

Display information about all the interfaces that statically join multicast groups and are in Up state.

```
<Huawei> display mld group static up
Static join group information
 Total 4 entries
  00001.(*,FF25::1)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
     1.GigabitEthernet0/0/1
     2.GigabitEthernet0/0/2
  00002.(FC00:0:0:1::1,FF25::1)
     Total List of 2 joined interfaces
     Total Matched 2 interfaces
```

```
  1.GigabitEthernet0/0/1
  2.GigabitEthernet0/0/2
```

Table 10-27 Description of the display mld group static up command output

Item	Description
Total List of 2 joined interfaces	Number of the interfaces that statically join multicast groups.
Total Matched 2 interfaces	List of the interfaces that statically join multicast groups and are in Up state.

Display the number of interfaces that statically join all multicast groups.

```
<Huawei> display mld group static interface-number
Static join group information
 Total 2 entries
  (*, FF25::1)
  Interface-Number:24

  (*, FF25::2)
  Interface-Number:24
```

Table 10-28 Description of the display mld group static interface-number command output

Item	Description
Interface-Number	Number of the interfaces that statically join multicast groups.

Related Topics

10.2.30 mld static-group

10.2.7 display mld interface

Function

The **display mld interface** command displays MLD information on an interface.

Format

display mld interface [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays MLD information on a specified interface. If this parameter is not specified, the command displays MLD information on all interfaces.	-
up	Indicates that the status of the IPv6 protocol on the MLD interface is Up, that is, MLD is in Active state.	-
down	Indicates that the status of the IPv6 protocol on the MLD interface is Down, that is, MLD is in Inactive state.	-
verbose	Displays detailed information about MLD interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the MLD configuration and running status on an interface, run the **display mld interface** command. This command displays MLD information only when MLD-enabled interfaces exist on the device.

Example

Display the MLD configuration and running status on GE1/0/0.

```
<Huawei> display mld interface gigabitethernet 1/0/0 verbose
Interface information
 GigabitEthernet1/0/0(FE80::2E0:B4FF:FE35:FF01):
   MLD is enabled
   Current MLD version is 2
   MLD state: up
   MLD group policy: none
   MLD limit: -
   Value of query interval for MLD (negotiated): 125 s
   Value of query interval for MLD (configured): 125 s
   Value of other querier timeout for MLD: 0 s
   Value of maximum query response time for MLD: 10 s
   Value of last listener query time: 2 s
   Value of last listener query interval: 1 s
   Value of startup query interval: 31 s
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:28
   Querier for MLD: FE80::2E0:B4FF:FE35:FF01 (this router)
   MLD activity: 2 joins, 0 dones
   Robustness (negotiated): 2
   Robustness (configured): 2
   Require-router-alert: disabled
   Send-router-alert: enabled
   Ip-source-policy: disabled
   Query Ip-source-policy: disabled
   Prompt-leave: disabled
```

 Copyright © Huawei Technologies Co., Ltd.

```
 SSM-Mapping: enabled
 Startup-query-timer-expiry: off
 Other-querier-present-timer-expiry: off
 TTL-check: disabled
Total 2 MLD Groups reported
```

Table 10-29 Description of the display mld interface verbose command output

Item	Description
GigabitEthernet1/0/0(FE80::2E0:B4FF:FE35:FF01)	Interface type and interface number (IPv6 link-local address).
MLD is enabled	MLD is enabled. To enable MLD, run the **mld enable** command.
Current MLD version is 2	MLD version is set to 2 on the interface. To set the MLD version, run the **mld version** command.
MLD state	Status of the MLD interface, that is, up or down.
MLD group policy	ACL6 number of the MLD group policy. To set ACL6 number of the MLD group policy, run the **mld group-policy** command.
MLD limit	Maximum number of MLD group members that the current interface can maintain. To set the maximum number of MLD group members that the current interface can maintain, run the **mld limit** command.
Value of query interval for MLD (negotiated)	Actual interval for sending MLD Query messages after negotiation, in seconds.
Value of query interval for MLD (configured)	Configured interval for sending MLD Query messages, in seconds. To set the interval for sending MLD Query messages, run the **mld timer query** command.
Value of other querier timeout for MLD	Timeout period of other MLD queriers, in seconds. To set the timeout period of an MLD querier, run the **mld timer other-querier-present** command.
Value of maximum query response time for MLD	Maximum response time for MLD Query messages, in seconds. To set the maximum response time for MLD Query messages, run the **mld max-response-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Value of last listener query time	Last listener query time, in seconds. The last listener query time is calculated by multiplying the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages by the robustness variable.
Value of last listener query interval	Interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages messages (Last listener query), in seconds. To set the interval for sending Last listener query, run the **mld lastlistener-queryinterval** command.
Value of startup query interval	Interval for sending Query messages when a querier starts, in seconds. The interval is one-fourth the query interval configured using the **mld timer query** command.
Value of startup query count	Number of times the querier sends Query messages when a querier starts. To set the number of times for sending Query messages when the querier starts, run the **mld robust-count** command.
General query timer expiry (hours:minutes:seconds)	Timeout period of the general query timer.
Querier for MLD	Link-local address of the MLD querier.
MLD activity	Statistics about MLD activities (join or leave).
Robustness (negotiated)	Robustness variable after negotiation by the non-querier device.
Robustness (configured)	Robustness variable set on the interface. To set the robustness variable on an interface, run the **mld robust-count** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Require-router-alert	Whether the MLD packet without the Router-Alert option is discarded. To configure whether the MLD packet without the Router-Alert option is discarded, run the **mld require-router-alert** command.
Send-router-alert	Whether the sent MLD packet carries the Router-Alert option. To configure whether the sent MLD packet carries the Router-Alert option, run the **mld send-router-alert** command.
Ip-source-policy	Whether to filter Multicast Listener Report/Done messages based on host addresses. To configure whether to filter Multicast Listener Report/Done messages based on host addresses, run the **mld ip-source-policy** command.
Query Ip-source-policy	Whether to filter MLD Query messages based on host addresses. To configure whether to filter MLD Query messages based on host addresses, run the **mld query ip-source-policy** command.
Prompt-leave	Whether fast leave is enabled. To enable fast leave, run the **mld prompt-leave** command.
SSM-Mapping	Whether SSM mapping is enabled. To enable SSM mapping, run the **mld ssm-mapping enable** command.
Startup-query-timer-expiry	Status of the timer for the interface functioning as the querier after startup to send Query messages. • off: The interface sends Query messages immediately after startup. • on: The interface delays sending Query messages after startup.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Other-querier-present-timer-expiry	Status of the timer identifying whether another querier is present. ● off: The interface considers itself a querier and no other queriers exist. ● on: The interface no longer considers itself a querier and another querier exists.
TTL-check	Whether the function to check the TTL values in received IGMP Report, Leave, and Query messages is enabled: ● enabled ● disabled
Total 2 MLD Groups reported	Two Multicast Listener Report messages are received on the interface.

Related Topics

10.2.16 mld enable
10.2.34 mld version
10.2.18 mld group-policy
10.2.21 mld limit
10.2.32 mld timer query
10.2.31 mld timer other-querier-present
10.2.22 mld max-response-time
10.2.20 mld lastlistener-queryinterval
10.2.27 mld robust-count
10.2.26 mld require-router-alert
10.2.28 mld send-router-alert
10.2.19 mld ip-source-policy
10.2.24 mld prompt-leave
10.2.29 mld ssm-mapping enable

10.2.8 display mld invalid-packet

Function

The **display mld invalid-packet** command displays statistics and details about invalid MLD packets received by a device.

 Copyright © Huawei Technologies Co., Ltd.

Format

display mld invalid-packet [**interface** *interface-type interface-number* | **message-type** { **done** | **query** | **report** }]*

display mld invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about invalid MLD messages received by a specified interface. If this parameter is not specified, the command displays statistics about invalid MLD messages on all interfaces.	-
message-type	Displays statistics about invalid MLD messages of a specified type.	-
done	Displays statistics about invalid Multicast Listener Done messages.	-
query	Displays statistics about invalid Query messages.	-
report	Displays statistics about invalid Multicast Listener Report messages.	-
packet-number	Displays details of a specified number of invalid MLD messages recently received.	The value is an integer that ranges from 1 to 100.
verbose	Displays details of invalid MLD messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mld invalid-packet** command to view statistics and details of invalid MLD messages for fault location and rectification.

If MLD entries fail to be generated on a multicast network, you can run the **display mld invalid-packet** command first to check whether devices have received invalid MLD messages. If the command output contains statistics about invalid MLD messages, you need to run the **display mld invalid-packet** [*packet-number*] **verbose** command to view details of invalid MLD messages to locate the fault.

 Copyright © Huawei Technologies Co., Ltd.

You can run the following related commands to view information about specific invalid MLD messages:

- Run the **display mld invalid-packet** command to view statistics about invalid MLD messages received by a device.
- Run the **display mld invalid-packet interface** *interface-type interface-number* command to view statistics about invalid MLD messages received by a specified interface.
- Run the **display mld invalid-packet** *packet-number* **verbose** command to view details of invalid MLD messages recently received. Currently, details of a maximum of 100 invalid MLD messages can be displayed.

Example

Display statistics about invalid MLD messages received by the device.

```
<Huawei> display mld invalid-packet
        Statistics of invalid packets for public net:
-----------------------------------------------------------------
MLD Query invalid packet:
Unwanted Source List    : 1000        Zero Max Resp Code      : 0
Fault Length            : 1000        Invalid Multicast Group : 0
Bad Checksum            : 0

MLD Report invalid packet:
Fault Length            : 0           Invalid Multicast Group : 0
Invalid Multicast Source: 0           Bad Checksum            : 0
Illegal Report Type     : 0

MLD Done invalid packet:
Invalid Multicast Group : 0           Bad Checksum            : 0
-----------------------------------------------------------------
```

Table 10-30 Description of the display mld invalid-packet command output

Item	Description
Statistics of invalid packets for public net	Invalid packets received in the public net.
MLD Query invalid packet	Invalid MLD Query messages.
Unwanted Source List	Messages with unwanted source lists.
Zero Max Resp Code	Messages with the Max Resp Code fields being 0.
Fault Length	Messages with invalid lengths.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Bad Checksum	Messages with checksum errors.
MLD Report invalid packet	Invalid MLD Report messages.
Invalid Multicast Source	Messages with invalid multicast source addresses.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Illegal Report Type	Messages with the illegal Report message type.
MLD Done invalid packet	Invalid Multicast Listener Done messages.

Display details of one invalid MLD message recently received by the device.

```
<Huawei> display mld invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Interface           :  GigabitEthernet1/0/0
Time                :  2012-06-09 11:03:51 UTC-08:00
Message Length      :  24
Invalid Type        :  Invalid Multicast Group
0000: 84 00 4c d7 00 00 00 00 11 17 00 00 00 00 00 00
0010: 00 00 00 00 00 01 00 01
-----------------------------------------------------
```

Table 10-31 Description of the display mld invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details of the invalid MLD message.
Packet information (Index 1)	Sequence number of the invalid MLD message (numbered in the opposite order that the message is received).
Interface	Interface receiving the invalid MLD message.
Time	Time when the invalid MLD message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured using the **clock timezone** command; DST indicates that the daylight saving time is configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid MLD message.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Invalid Type	Type of the invalid MLD message: • Unwanted Source List • Zero Max Resp Code • Fault Length • Invalid Multicast Group • Bad Checksum • Invalid Multicast Source • Illegal Report Type
0000: 84 00 4c d7 00 00 00 00 11 17 00 00 00 00 00 00 0010: 00 00 00 00 00 01 00 01	Contents of the invalid MLD message.

Related Topics

10.8.12 multicast ipv6 invalid-packet

10.2.9 display mld routing-table

Function

The **display mld routing-table** command displays information about the MLD routing table.

Format

display mld routing-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*]] * [**static**] [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
ipv6-source-mask-length	Specifies the mask length of the IPv6 address of a multicast source.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
static	Displays the MLD routing table of the static multicast group.	-
outgoing-interface-number	Displays the number of the outgoing interfaces in MLD routing entries.	-
number	Specifies the number of outgoing interfaces. After this parameter is specified, the command displays information about the specified number of outgoing interfaces.	The value is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view MLD routing entries, run the **display mld routing-table** command. You can specify parameters to view specified routing information, which facilitates fault location.

NOTE

This command provides output information only when PIM (IPv6) is not enabled on the MLD-capable interface.

Example

Display the MLD routing entry of the specified multicast group.

```
<Huawei> display mld routing-table
Routing table
```

```
Total 2 entries

00001. (FC00:0:0:1::3, FF44::)
     List of 1 downstream interface in include mode
      GigabitEthernet1/0/0 (FE80::EE:53),
               Protocol: STATIC

00002. (*, FF55::)
     List of 1 downstream interface
      GigabitEthernet1/0/0 (FE80::EE:53),
               Protocol: MLD
```

Table 10-32 Description of the display mld routing-table command output

Item	Description
Routing table	MLD routing table.
Total 2 entries	Total number of MLD routing entries.
00001. (FC00:0:0:1::3, FF44::)	Entry 00001. (S, G) indicates that data is transmitted from S to G. (*, G) indicates that data is transmitted from any source to G.
List of 1 downstream interface in include mode	List of the downstream interfaces that join the multicast group in INCLUDE mode.
GigabitEthernet1/0/0(FE80::EE:53)	Interface type and interface number (IPv6 link-local address).
Protocol	Protocol type. ● SSM-MAP: Entries are generated using MLD SSM mapping. ● MLD: Entries are generated using MLD. ● STATIC: Entries are generated by the MLD static multicast group.
List of 1 downstream interface	Downstream interface list.

10.2.10 display mld ssm-mapping

Function

The **display mld ssm-mapping** command displays the configuration of MLD SSM mapping.

Format

display mld ssm-mapping { **group** [*ipv6-group-address*] | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
group *ipv6-group-address*	Specifies the source IPv6 address of a specified multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
interface *interface-type interface-number*	Displays whether a specified interface is enabled with SSM mapping. If this parameter is not specified, the command displays information about all Up interfaces enabled with SSM mapping.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view multicast sources mapped to a multicast group. SSM mapping entries can be configured using the **ssm-mapping (MLD view)** command. The **display mld ssm-mapping** command also allows you to view the SSM mapping status on an interface, which can be configured using the **mld ssm-mapping enable** command.

Example

Display information about the interface configured with SSM mapping.

```
<Huawei> display mld ssm-mapping interface
Interface information of VPN-Instance: public net
GigabitEthernet1/0/0(FE80::1)
```

Table 10-33 Description of the display mld ssm-mapping interface command output

Item	Description
Interface information of VPN-Instance: public net	VPN instance to which the interface enabled with SSM mapping belongs. Currently, only the public network instance is supported.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GigabitEthernet1/0/0(FE80::1)	Interface type and interface number (IPv6 address).

Display information about SSM mapping of all multicast sources and groups.

```
<Huawei> display mld ssm-mapping group
MLD SSM-Mapping conversion table
 Group: FF3E::/64
  Number of Source(s): 3
    FC00:0:0:1::1
    FC00:0:0:1::2
    FC00:0:0:1::3
```

Table 10-34 Description of the display mld ssm-mapping group command output

Item	Description
MLD SSM-Mapping conversion table	MLD SSM mapping switching table.
Group	Address of a multicast group.
Number of Source(s)	Number of multicast sources configured with SSM mapping.
FC00:0:0:1::1::1	Multicast source address.

Check whether MLD SSM mapping is enabled on GE1/0/0.

```
<Huawei> display mld ssm-mapping interface GigabitEthernet 1/0/0
MLD SSM-Mapping is enabled
```

Table 10-35 Description of the display mld ssm-mapping interface GigabitEthernet 1/0/0 command output

Item	Description
MLD SSM-Mapping is enabled	SSM mapping is enabled on the interface.

Related Topics

10.2.29 mld ssm-mapping enable

10.2.42 ssm-mapping (MLD view)

10.2.11 display mld ssm-mapping interface

Function

The **display mld ssm-mapping interface** command displays information about interfaces enabled with SSM mapping.

Format

display mld ssm-mapping interface [*interface-type interface-number* [**group** *ipv6-group-address*]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies an interface.	-
group *ipv6-group-address*	Displays the source address list associated with a specified group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display mld ssm-mapping interface** command to view information about an interface enabled with SSM mapping.

Example

Display information about the interface configured with SSM mapping.

```
<Huawei> display mld ssm-mapping interface
Interface information of VPN-Instance: public net
 GigabitEthernet1/0/0(FE80::1)
```

Table 10-36 Description of the display mld ssm-mapping interface command output

Item	Description
Interface information of VPN-Instance: public net	VPN instance to which the interface enabled with SSM mapping belongs. Currently, only the public network instance is supported.
GigabitEthernet1/0/0(FE80::1)	Interface type and interface number (IPv6 link-local address).

 Copyright © Huawei Technologies Co., Ltd.

10.2.12 lastlistener-queryinterval (MLD view)

Function

The **lastlistener-queryinterval** command globally sets the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after the MLD querier receives an MLD Done message from a host.

The **undo lastlistener-queryinterval** command restores the default value.

By default, the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is 1 second.

Format

lastlistener-queryinterval *interval*

undo lastlistener-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after the MLD querier receives a Multicast Listener Done message.	The value is an integer that ranges from 1 to 5, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MLD querier receives a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages continuously to check for other members in the multicast group. The **lastlistener-queryinterval** command sets the interval at which the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If the querier receives no Multicast Listener Report message for a specified period, the querier stops forwarding data to the multicast group. The period is calculated by multiplying *interval* by *robust-value*. To set *robust-value*, run the **mld robust-count** or **robust-count (MLD view)** command.

 Copyright © Huawei Technologies Co., Ltd.

If the querier receives a Multicast Listener Report message from a host within the maximum response time, the querier maintains the membership of the multicast group. If the querier receives no Multicast Listener Report message within the maximum response time, the querier considers that the last member has left the group and does not maintain the membership of the multicast group.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld lastlistener-queryinterval** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages to 3 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] lastlistener-queryinterval 3
```

Related Topics

10.2.20 mld lastlistener-queryinterval

10.2.27 mld robust-count

10.2.40 robust-count (MLD view)

10.2.13 limit (MLD view)

Function

The **limit** command sets the maximum number of MLD entries that can be created globally.

The **undo limit** command restores the maximum number of MLD entries that can be created globally to the default value.

By default, the maximum number of MLD entries that can be created on the entire router varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201, AR2202, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256

 Copyright © Huawei Technologies Co., Ltd.

  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 4000
  - Configured with SRU200E: 4000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 4000

Format

limit *number*

undo limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that can be created globally.	The value is an integer that ranges from: ● 1 to 64 for the AR100&AR120&AR150&AR160&AR200 series. ● 1 to 128 for the AR1200 series, AR2201, AR2202, and AR2204. ● 1 to 256 for the AR2220, AR2240C, and AR2220E. ● 1 to 512 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 256 – Configured with SRU60: 1 to 256 – Configured with SRU80: 1 to 512 – Configured with SRU100: 1 to 512 – Configured with SRU100E: 1 to 512 – Configured with SRU200: 1 to 4000 – Configured with SRU200E: 1 to 4000 – Configured with SRU400: 1 to 4000 ● 1 to 4000 for the AR3600 series (SRUX5)

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the maximum number of MLD entries globally.

When the number of MLD entries reaches the limit, the system does not create any more. To enable the router to allow new join requests, you can either delete useless entries or modify the limit. Alternatively, you can enable static addition on a multicast group or source group.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **mld global limit** *number* command in the system view to set the maximum number of global MLD group memberships. If both the **limit** and **mld global limit** *number* commands are run, the smaller value takes effect.

Example

Set the maximum number of MLD entries to 60 globally.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] limit 60
```

Related Topics

10.2.21 mld limit

10.2.17 mld global limit

10.2.14 max-response-time (MLD view)

Function

The **max-response-time** command sets a global maximum response time for MLD General Query messages.

The **undo max-response-time** command restores the default global maximum response time for MLD General Query messages.

By default, the global maximum response time for MLD General Query messages is 10 seconds.

Format

max-response-time *interval*

 Copyright © Huawei Technologies Co., Ltd.

undo max-response-time

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for MLD General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send Multicast Listener Report messages immediately after receiving MLD General Query messages, the querier on the local network segment may receive a large number of Multicast Listener Report messages from the hosts at the same time. The network is congested.

To avoid such situations, MLD messages specify the maximum response time for MLD General Query messages. When a host receives an MLD Query message, the host starts a timer for the multicast group that it joins. The value of the timer ranges from 0 to the maximum response time. When the timer times out, the host sends a Multicast Listener Report message to the querier.

The maximum response time specifies the deadline for the host to send a Multicast Listener Report message. A proper maximum response time allows hosts to respond to MLD Query messages and prevents hosts from sending Report messages at the same time.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The function of this command is the same as that of the **mld max-response-time** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the MLD view, set the maximum response time for MLD General Query messages to 8 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] max-response-time 8
```

Related Topics

10.2.22 mld max-response-time

10.2.15 mld

Function

The **mld** command displays the MLD view.

The **undo mld** command clears all configurations in the MLD view.

Format

mld

undo mld

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Global MLD parameters must be configured in the MLD view.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Enter the MLD view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] mld
[Huawei-mld]
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.2.16 mld enable

Function

The **mld enable** command enables MLD on an interface.

The **undo mld enable** command disables MLD on an interface.

By default, MLD is disabled on an interface.

Format

mld enable

undo mld enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a shared IPv6 network segment, hosts and multicast devices must run MLD. A multicast device can process MLD messages sent from hosts only after MLD is enabled on the interfaces connected to user network segments.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- If MLD parameters are configured on an interface, the parameter settings take effect only after MLD is enabled.
- If PIM (IPv6) and MLD need to be enabled on the same interface, enable PIM (IPv6) and MLD in sequence.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable MLD on GE1/0/0 connected to a user network segment.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld enable
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.2.17 mld global limit

Function

The **mld global limit** command sets the maximum number of MLD entries that can be created on the entire router.

The **undo mld global limit** command deletes the configured maximum number of MLD entries.

By default, the maximum number of MLD entries that can be created on the entire router varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201, AR2202, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256
  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 4000
  - Configured with SRU200E: 4000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 4000

Format

mld global limit *number*

undo mld global limit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that can be created on the entire router.	The value is a decimal integer that ranges from: ● 1 to 64 for the AR100&AR120&AR150&AR160&AR200 series. ● 1 to 128 for the AR1200 series, AR2201, AR2202, and AR2204. ● 1 to 256 for the AR2220, AR2240C, and AR2220E. ● 1 to 512 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 256 – Configured with SRU60: 1 to 256 – Configured with SRU80: 1 to 512 – Configured with SRU100: 1 to 512 – Configured with SRU100E: 1 to 512 – Configured with SRU200: 1 to 4000 – Configured with SRU200E: 1 to 4000 – Configured with SRU400: 1 to 4000 ● 1 to 4000 for the AR3600 series (SRUX5)

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of MLD entries reaches the limit, the system does not create any more. To enable the router to allow new join requests, you can either delete useless entries or modify the limit. Alternatively, you can enable static addition on a multicast group or source group.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **limit (MLD view)** command in the MLD view to set the maximum number of global MLD group entries. If both the **igmp global limit** and **limit (MLD view)** commands are run, the smaller value takes effect.

Example

Set the maximum number of MLD entries that can be created on the router to 60.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld global limit 60
```

Related Topics

10.2.13 limit (MLD view)

10.2.21 mld limit

10.2.18 mld group-policy

Function

The **mld group-policy** command configures an MLD group policy on an interface to limit the range of multicast groups that the hosts can join.

The **undo mld group-policy** command deletes the MLD group policy.

By default, no MLD group policy is configured on an interface, and the hosts can join any multicast groups.

Format

mld group-policy { *acl6-number* | **acl6-name** *acl6-name* } [**1** | **2**]

undo mld group-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of a basic or advanced IPv6 ACL6. This ACL6 defines the range of multicast groups.	The number of a basic ACL6 is an integer that ranges from 2000 to 2999. The number of an advanced ACL6 is an integer that ranges from 3000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
1	Limits the range of multicast groups that MLDv1 hosts can join.	-
2	Limits the range of multicast groups that MLDv2 hosts can join.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To control the multicast groups that hosts on the network attached to an interface can join, specify an ACL6 in the **mld group-policy** command as a filter to specify the range of multicast groups served by the interface. This configuration improves security of the MLD application. You can also run this command to prevent router from receiving Multicast Listener Report messages for specified groups.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

An ACL6 defining the range of multicast groups has been created.

The **mld group-policy** command is used with the **acl ipv6** command. To use a numbered ACL6 in the MLD group policy:

- In the basic ACL6 view, set **source** in the **rule (basic ACL6 view)** command to the range of multicast groups that an interface can join.
- In the advanced ACL6 view, set **source** in the **rule (advanced ACL6 view)** command to the source address that is allowed to send multicast data to the specified multicast groups, and set **destination** to the range of multicast groups that an interface can join.

After the **mld group-policy** command is executed on an interface:

- The interface filters the received Report messages based on the ACL6 and maintains memberships only for the multicast groups permitted by the ACL6.

 Copyright © Huawei Technologies Co., Ltd.

- The interface discards the Report messages that are denied by the ACL6. If the entries of the multicast groups denied by the ACL6 exist on the router, the router deletes these entries when the aging time of the entries expires.

Example

Create ACL6 2005, and configure a rule that allows hosts to receive data of multicast group FF13::101. Configure an MLD group policy on GE1/0/0 and reference ACL6 2005 to allow hosts connected to the interface to join only multicast group FF13::101.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2005
[Huawei-acl6-basic-2005] rule permit source ff13::101 128
[Huawei-acl6-basic-2005] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld group-policy 2005
```

Create an ACL6 named **myacl6**, and configure a rule that allows hosts to receive data of multicast groups in the range of FF13::101. Configure an MLD group policy on GE1/0/0 and reference the ACL6 to allow hosts connected to the interface to join only the specified multicast groups.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff13::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld group-policy acl6-name myacl6
```

10.2.19 mld ip-source-policy

Function

The **mld ip-source-policy** command enables filtering of Multicast Listener Report/Done messages based on source addresses.

The **undo mld ip-source-policy** command disables filtering of MLD messages based on source addresses.

By default, a multicast device does not filter MLD messages based on source addresses.

Format

mld ip-source-policy { *basic-acl6-number* | **acl6-name** *acl6-name* }

undo mld ip-source-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic ACL6, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD runs on receiver hosts and their directly connected multicast devices. A multicast device processes all received Multicast Listener Report/Done messages. To improve security, you can configure the multicast device to filter Multicast Listener Report/Done messages received on an interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Configure GE1/0/0 to receive the Multicast Listener Report/Done messages with the source address FC00::1.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2001
[Huawei-acl6-basic-2001] rule permit source fc00::1 128
[Huawei-acl6-basic-2001] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld ip-source-policy 2001
```

Related Topics

10.2.7 display mld interface

10.8.16 multicast ipv6 routing-enable

10.2.20 mld lastlistener-queryinterval

Function

The **mld lastlistener-queryinterval** command sets the interval at which the MLD querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages after receiving Multicast Listener Done messages from a host.

 Copyright © Huawei Technologies Co., Ltd.

The **undo mld lastlistener-queryinterval** command restores the default value.

By default, the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is 1 second.

Format

mld lastlistener-queryinterval *interval*

undo mld lastlistener-queryinterval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.	The value is an integer that ranges from 1 to 5, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the MLD querier receives a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages continuously to check for other members in the multicast group. The **mld lastlistener-queryinterval** command sets the interval at which the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If the querier receives no Multicast Listener Report message for a specified period, the querier stops forwarding data to the multicast group. The period is calculated by multiplying *interval* by *robust-value*. To set *robust-value*, run the **mld robust-count** or **robust-count (MLD view)** command.

If the querier receives a Multicast Listener Report message from a host within the maximum response time, the querier maintains the membership of the multicast group. If the querier receives no Multicast Listener Report message within the maximum response time, the querier considers that the last member has left the group and does not maintain the membership of the multicast group.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The function of the **mld lastlistener-queryinterval** command is the same as that of the **lastlistener-queryinterval** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query message to 3 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld lastlistener-queryinterval 3
```

Related Topics

10.2.12 lastlistener-queryinterval (MLD view)

10.2.27 mld robust-count

10.2.40 robust-count (MLD view)

10.2.21 mld limit

Function

The **mld limit** command sets the maximum number of MLD group memberships that the current interface can maintain.

The **undo mld limit** command restores the maximum number of MLD group memberships that the current interface can maintain to the default value.

By default, the maximum number of MLD entries that can be created on the current interface varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201, AR2202, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256
  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 1024
  - Configured with SRU200E: 1024
  - Configured with SRU400: 2048
- AR3600 series (SRUX5): 1024

 Copyright © Huawei Technologies Co., Ltd.

Format

mld limit *number* [**except** { *acl6-number* | **acl6-name** *acl6-name* }]

undo mld limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of MLD entries that the current interface can create.	The value is an integer that ranges from: ● 1 to 64 for the AR100&AR120&AR150&AR160&AR200 series. ● 1 to 128 for the AR1200 series, AR2201, AR2202, and AR2204. ● 1 to 256 for the AR2220, AR2240C, and AR2220E. ● 1 to 512 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 256 – Configured with SRU60: 1 to 256 – Configured with SRU80: 1 to 512 – Configured with SRU100E: 1 to 512 – Configured with SRU200: 1 to 1024 – Configured with SRU200E: 1 to 1024 – Configured with SRU400: 1 to 2048 ● 1 to 1024 for the AR3600 series (SRUX5)
except	Specifies the range of multicast groups that are not limited by the set maximum number.	-
acl6-number	Specifies the basic or advanced ACL6.	The value is an integer. The number of the basic ACL6 ranges from 2000 to 2999. The basic ACL6 filters group addresses only, without distinguishing (*, G) entries and (S, G) entries. The number of the advanced ACL6 ranges from 3000 to 3999. The advanced ACL6 filters (S, G) entries of the interface only.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of MLD entries reaches the limit, the system does not create any MLD entries. To make the router allow more new join requests, delete some useless entries or modify the limit. Alternatively, you can enable static addition on a multicast group or source group.

The number of MLD entries can be counted in the following methods:

- Each (*, G) entry is counted as one entry.
- Each (S, G) entry is counted as one entry.
- Each (*, G) entry for SSM mapping is counted as one entry.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If **except** is not set in the command, the maximum number of MLD entries corresponding to all the groups or source/groups is limited.

Before setting **except**, configure the associated ACL6. The interface then filters the received MLD Join messages according to the ACL6. The maximum number of entries corresponding to the multicast groups that match the ACL6 is not limited.

The **mld limit** command must be used with ACL6 configuration commands. When configuring ACL6 rules, note that:

- In the basic ACL6 view, specify the **source** parameter in the **rule (basic ACL6 view)** command for setting the range of multicast groups whose MLD entries do not need to be limited.
- In the advanced ACL6 view, specify the **source** parameter in the **rule (advanced ACL6 view)** command for setting the range of sources that are

allowed to send multicast data to the multicast groups. Specify the **destination** parameter in the **rule (advanced ACL6 view)** command for setting the range of multicast groups whose MLD entries do not need to be limited.

Example

Set the maximum number of MLD entries that can be created on the GE1/0/0 to 60.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld limit 60
```

Create the advanced ACL6 with the number being 3100; set the maximum number of MLD entries that can be created on GE1/0/0 to 60; allow the hosts to receive messages from the specific-source multicast group (FC00:0:0:2001::1, FF3E::1). That is, the specific-source multicast group (FC00:0:0:2001::1, FF3E::1) is not limited by the maximum number of MLD entries.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] acl ipv6 3100
[Huawei-acl6-adv-3100] rule permit ipv6 source fc00:0:0:2001::1 64 destination ff3e::1 64
[Huawei-acl6-adv-3100] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld limit 60 except 3100
```

Related Topics

10.2.17 mld global limit
10.2.13 limit (MLD view)

10.2.22 mld max-response-time

Function

The **mld max-response-time** command sets the maximum response time for MLD General Query messages on an interface.

The **undo mld max-response-time** command restores the default maximum response time for General MLD Query messages.

By default, the maximum response time for MLD General Query messages is 10s on an interface.

Format

mld max-response-time *interval*

undo mld max-response-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the maximum response time for MLD General Query messages.	The value is an integer that ranges from 1 to 25, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If hosts send Multicast Listener Report messages immediately after receiving MLD General Query messages, the querier on the local network segment may receive a large number of Multicast Listener Report messages from the hosts at the same time. The network is congested.

To avoid such situations, MLD messages specify the maximum response time for MLD General Query messages. When a host receives an MLD Query message, the host starts a timer for the multicast group that it joins. The value of the timer ranges from 0 to the maximum response time. When the timer times out, the host sends a Multicast Listener Report message to the querier.

The maximum response time specifies the deadline for the host to send a Multicast Listener Report message. A proper maximum response time allows hosts to respond to MLD Query messages and prevents hosts from sending Report messages at the same time.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- A shorter response time allows a multicast device to obtain multicast group member information more quickly, but consumes more bandwidth and system resources.
- The function of the **mld max-response-time** command is the same as that of the **max-response-time (MLD view)** command used in the MLD view. The configuration in the MLD view takes effect for all interfaces, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum response time for MLD General Query messages to 8 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld max-response-time 8
```

Related Topics

10.2.14 max-response-time (MLD view)

10.2.23 mld on-demand

Function

The **mld on-demand** command enables the MLD on-demand function. This function enables a querier to maintain group memberships according to requirements of group members, without sending Query messages. After MLD on-demand is enabled on an interface, dynamic MLD entries on the interface will never age out.

The **undo mld on-demand** command restores the default configuration.

By default, a querier does not maintain group memberships according to requirements of group members, and dynamic entries are aged out when the aging time expires.

Format

mld on-demand

undo mld on-demand

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a standard MLD working process, a querier sends General Query messages periodically and collects group membership information based on received Multicast Listener Report and Done messages. Group members respond to every Query message they receive. After MLD on-demand is configured on the querier,

 Copyright © Huawei Technologies Co., Ltd.

the querier does not send Query messages, reducing MLD packets exchanged between the querier and receiver hosts.

The MLD on-demand function enables a querier to maintain group memberships based on Report messages sent from hosts. The querier does not send Query messages to collect membership information, reducing traffic transmitted between the querier and receiver hosts.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

IPv6 function has been enabled using the **ipv6 enable (interface view)** command in the interface view.

Precautions

- If dynamic MLD entries have been generated on the querier, run the **reset mld group** command to clear these dynamic MLD entries before running the **mld on-demand** command.
- After the **mld on-demand** command is executed on an interface:
  - The interface no longer sends MLD Query messages.
  - MLD group entries are generated after the interface receives Multicast Listener Report messages. The entries will never age out.
  - When the interface receives a Multicast Listener Done message, it deletes the corresponding MLD group entry.

Example

Enable the MLD on-demand function on GE1/0/0.

```
<Huawei> system-view
[Huawei] ipv6
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] mld on-demand
```

10.2.24 mld prompt-leave

Function

The **mld prompt-leave** command enables the fast leave function on an interface. This function enables an MLD querier to delete MLD entries immediately after receiving Multicast Listener Done messages from group members, without sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages.

The **undo mld prompt-leave** command disables fast leave on an interface.

By default, an MLD querier sends a Multicast Address Specific Query message or Multicast Address and Source Specific Query message after receiving a Multicast Listener Done message for a specific multicast group.

 Copyright © Huawei Technologies Co., Ltd.

Format

mld prompt-leave [**group-policy** { *acl6-number* | **acl6-name** *acl6-name* }]

undo mld prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies an MLD multicast group policy. If this parameter is specified, the fast leave function takes effect only for multicast groups specified in the policy. When specifying this parameter, ensure that the referenced ACL6 has been configured. The interface filters Multicast Listener Done messages on the interface based on the ACL6. ● If a host leaves a multicast group in the range permitted by the ACL6, the device immediately deletes the multicast group entry without sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. ● If a host leaves a multicast group out of the range permitted by the ACL6, the device sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages. If this parameter is not specified, the fast leave function takes effect for all multicast groups.	-
acl6-number	Specifies the number of a basic ACL6 or an advanced ACL6. This ACL6 defines the range of multicast groups.	The number of a basic ACL6 is an integer that ranges from 2000 to 2999. The number of an advanced ACL6 is an integer that ranges from 3000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some scenarios, an interface on the MLD querier connects to only one receiver host. If the host frequently switches between multiple multicast groups, you can configure fast leave on the interface of the querier so that the interface can quickly respond to Multicast Listener Done messages sent from the host. After fast leave is configured, the querier does not send a Multicast Address Specific Query message or Multicast Address and Source Specific Query message after receiving a Multicast Listener Done message. Instead, the querier directly notifies the upstream multicast device that the host has left the multicast group. The fast leave function reduces delay in response to Multicast Listener Done messages and saves network bandwidth.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- When an interface has more than one receiver connected, enabling fast leave interrupts multicast traffic of the other receivers in the multicast group. You are advised to enable this function on interfaces with only one receiver.
- When configuring an ACL6 to specify the range of multicast groups, pay attention to the following points:
  - When you run the **rule** command in the view of a basic ACL6, set **source** to the address range of multicast groups that hosts can fast leave.
  - When you run the **rule** command in the view of an advanced ACL6, set **source** to the multicast source address and **destination** to the range of multicast groups that hosts can fast leave.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure fast leave on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld prompt-leave
```

Create an ACL6 named **myacl6**. Configure fast leave on GE1/0/0 and apply the **myacl6** to allow the interface to immediately leave multicast group FF13::101 defined in the **myacl6**.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff13::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld prompt-leave group-policy acl6-name myacl6
```

10.2.25 mld query ip-source-policy

Function

The **mld query ip-source-policy** command configures MLD Query message filtering based on source addresses.

The **undo mld query ip-source-policy** command restores the default configuration.

By default, no source address-based MLD Query message filtering is configured.

Format

mld query ip-source-policy { *basic-acl6-number* | **acl6-name** *acl6-name* }

undo mld query ip-source-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic ACL6, which defines the range of source addresses.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends forged MLD Query messages with an IPv6 address smaller than the querier IPv6 address, the querier is replaced by the attacker. As a result, the real querier cannot response to Multicast Listener Report messages from group members and bandwidth is wasted. Source address-based MLD Query message filtering can protect the querier from such attacks. After this function is configured on a device, the device accepts only the MLD Query messages with source addresses permitted by the specified ACL6. This function controls querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- MLD Query messages are encapsulated into IPv6 messages. This command is used to filter the source addresses in IPv6 headers.
- After you configure source address-based MLD Query message filtering on an interface, the interface filters out the MLD Query messages whose source addresses do not match a specified ACL6 rule.

Example

Configure GE1/0/0 to receive the MLD Query messages with the source address FC00::1.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2001
[Huawei-acl6-basic-2001] rule permit source fc00::1 128
[Huawei-acl6-basic-2001] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld query ip-source-policy 2001
```

10.2.26 mld require-router-alert

Function

The **mld require-router-alert** command configures an interface to discard MLD messages without the Router-Alert option.

The **undo mld require-router-alert** command disables an interface from checking for the Router-Alert option in MLD messages.

By default, all received MLD messages are processed, including the MLD messages without the Router-Alert option.

 Copyright © Huawei Technologies Co., Ltd.

Format

mld require-router-alert

undo mld require-router-alert

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a message to the routing protocol module for processing only when the destination address of the message is a local interface address. Destination addresses of MLD messages are multicast addresses but not addresses of interfaces on multicast devices. Therefore, multicast devices do not send MLD messages to the MLD module for processing, and the MLD module cannot maintain group memberships.

The Router-Alert option in the IPv6 header of an MLD message solves this problem. If an MLD message contains the Router-Alert option, the device sends the message to the MLD module.

You can configure the device to accept only MLD messages with the Router-Alert option to improve MLD security.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld require-router-alert** command is the same as that of the **require-router-alert (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The system prefers the configuration in the interface view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Configure GE1/0/0 to discard MLD messages without the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld require-router-alert
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.2.28 mld send-router-alert
10.2.35 require-router-alert (MLD view)

10.2.27 mld robust-count

Function

The **mld robust-count** command sets a robustness variable of an MLD querier on an interface.

The **undo mld robust-count** command restores the default robustness variable of an MLD querier.

By default, the robustness variable of an MLD querier is 2.

Format

mld robust-count *robust-value*

undo mld robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an MLD querier.	The value is an integer that ranges from 2 to 5.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD querier robustness variable specifies the retransmission count of MLD packets to minimize impact of packet loss on the network.

On a shared network segment, a querier maintains MLD group memberships. The robustness variable affects the timeout period of group memberships. The timeout period of the group membership is calculated using the formula:

Timeout period of the group memberships = Interval for sending MLD General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

 Copyright © Huawei Technologies Co., Ltd.

When a querier starts, it sends General Query messages certain times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The interval for sending General Query messages is configured using the **mld timer query** or **timer query (MLD view)** command.

- Number of times the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages

  When receiving a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages certain times specified by the robustness variable to check whether the group has members. When the querier receives a Multicast Listener Report message indicating that source-group mapping changes, the querier sends Multicast Address and Source Specific Query messages certain times specified by the robustness variable. The interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is set using the **mld lastlistener-queryinterval** or **lastlistener-queryinterval (MLD view)** command.

A larger robustness variable makes an MLD querier more robust but increases the timeout period of group memberships.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld robust-count** command is the same as that of the **robust-count (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the robustness variable of the querier on GE1/0/0 to 3.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld robust-count 3
```

Related Topics

10.2.12 lastlistener-queryinterval (MLD view)

10.2.20 mld lastlistener-queryinterval

10.2.32 mld timer query

10.2.40 robust-count (MLD view)

10.2.44 timer query (MLD view)

 Copyright © Huawei Technologies Co., Ltd.

10.2.28 mld send-router-alert

Function

The **mld send-router-alert** command configures an interface to send MLD messages containing the Router-Alert option in IPv6 headers.

The **undo mld send-router-alert** command disables an interface from sending MLD messages containing the Router-Alert option in IPv6 headers.

By default, the IPv6 headers of MLD messages sent by an interface contain the Router-Alert option.

Format

mld send-router-alert

undo mld send-router-alert

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the router sends MLD messages that contain the Router-Alert option in IPv6 headers. If the router needs to communicate with a device that does not support the Router-Alert option, run the **undo mld send-router-alert** command to configure the router to send MLD messages without the Router-Alert option. The **mld send-router-alert** command is usually used together with the **mld require-router-alert** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld send-router-alert** command is the same as that of the **send-router-alert (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE1/0/0 to send MLD messages with the Router-Alert option.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld send-router-alert
```

Related Topics

10.2.26 mld require-router-alert

10.2.41 send-router-alert (MLD view)

10.2.29 mld ssm-mapping enable

Function

The **mld ssm-mapping enable** command enables MLD SSM mapping on an interface.

The **undo mld ssm-mapping enable** command disables MLD SSM mapping on an interface.

By default, MLD SSM mapping is disabled on an interface.

Format

mld ssm-mapping enable

undo mld ssm-mapping enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM model allows MLDv2 hosts to specify the multicast sources from which they want to receive data. However, some hosts can only run MLDv1. To allow these hosts to use SSM, configure MLD SSM mapping on the router. MLD SSM mapping is implemented based on static SSM mapping entries on the router. The router converts (*, G) information in MLDv1 Multicast Listener Report messages to (S, G) information according to static SSM mapping entries to provide the SSM service for MLDv1 hosts.

 Copyright © Huawei Technologies Co., Ltd.

The **mld ssm-mapping enable** command enables MLD SSM mapping on an interface. The mappings between SSM sources and multicast group addresses take effect only when MLD SSM mapping is enabled on an interface. SSM mapping entries are configured using the **ssm-mapping (MLD view)** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Enable MLD SSM mapping on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld ssm-mapping enable
```

Related Topics

10.2.5 display mld group ssm-mapping

10.2.42 ssm-mapping (MLD view)

10.2.30 mld static-group

Function

The **mld static-group** command configures a static multicast group on an interface.

The **undo mld static-group** command deletes a static multicast group from an interface.

By default, no static multicast group is configured on an interface.

Format

mld static-group *ipv6-group-address* [**inc-step-mask** *ipv6-group-mask-length* **number** *group-number*] [**source** *ipv6-source-address*]

undo mld static-group { **all** | *ipv6-group-address* [**inc-step-mask** *ipv6-group-mask-length* **number** *group-number*] [**source** *ipv6-source-address*] }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies the IPv6 address of the multicast group that an interface statically joins. In batch configuration mode, this parameter specifies the initial address of the multicast group addresses.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
inc-step-mask *ipv6-group-mask-length*	Specifies the incremental length of the step mask in batch configuration mode.	The value is an integer that ranges from 8 to 128.
number *group-number*	Specifies the number of group addresses in batch configuration mode.	The value is an integer that ranges from 2 to 512.
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
all	Specifies all the multicast groups that the interface statically joins.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure static multicast groups on user-side interfaces of the router in some scenarios, for example:

- There are long-term group members on a shared network segment, and the router needs to forward multicast data to these group members quickly and steadily.

 Copyright © Huawei Technologies Co., Ltd.

- A network segment has no group member or hosts on the network segment cannot send Report messages, but multicast data needs to be sent to this network segment.

After a static multicast group is configured on an interface, the router considers that the multicast group always has members on the network segment of the interface. Therefore, the router always forwards multicast data of the multicast group.

The **mld static-group** command is used on an interface connected to user hosts. The command can configure a single group or source-group binding on an interface at a time or configure multiple groups or source-group bindings in a batch.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- After you run the **mld static-group** command on an interface connected to user hosts, the entries matching the MLD groups that the interface statically joins never time out. The router considers that this interface is always connected to group members, and keeps forwarding multicast packets of the specified multicast groups to the network segment where the interface resides.
- You can configure overlapping multicast group addresses in different batch configurations. When you configure multiple static multicast groups in a batch on an interface, do not delete any static group configuration before the system completes the batch static group configuration.
- If a user host no longer needs to receive multicast data of a static group, delete the static group configuration.

Example

Configure static multicast group FF13::101 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff13::101
```

Configure the router to forward multicast packets from multicast source FC00::101 to multicast group FF14::202 through GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff14::202 source fc00::101
```

Add GE1/0/0 statically to two multicast groups in a batch. Set the start multicast group address to FF25::1 and the step mask length to 24.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff25::1 inc-step-mask 24 number 2
```

 Copyright © Huawei Technologies Co., Ltd.

Add GE1/0/0 statically to two multicast source/groups in a batch. Set the start multicast group address to FF33::1, the source address to FC00::101, and the step mask length to 24.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld static-group ff33::1 inc-step-mask 24 number 2 source fc00::101
```

10.2.31 mld timer other-querier-present

Function

The **mld timer other-querier-present** command sets the other querier present timer on an interface.

The **undo mld timer other-querier-present** command restores the default value of the other querier present timer on an interface.

By default, the Keepalive period of the other queriers is calculated as follows:

Other querier present timer = Robustness variable x Interval for sending MLD General Query messages + 1/2 x Maximum response time

If the default values of the robustness variable, interval for sending MLD General Query messages, and maximum response time are used, the other querier present timer value is 255 seconds.

Format

mld timer other-querier-present *interval*

undo mld timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the MLD querier to send Query messages to hosts on the network segment. To create and maintain normal group

memberships, non-queriers running MLD start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of the **mld timer other-querier-present** command is the same as that of the **timer other-querier-present (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer is shorter than the interval for sending General Query messages, the querier election is triggered frequently.

Example

On GE1/0/0, set the other querier present timer to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld timer other-querier-present 200
```

Related Topics

10.2.7 display mld interface

10.2.43 timer other-querier-present (MLD view)

10.2.32 mld timer query

10.2.32 mld timer query

Function

The **mld timer query** command sets the interval at which an interface sends MLD General Query messages.

The **undo mld timer query** command restores the default interval at which an interface sends MLD General Query messages.

By default, an interface sends MLD General Query messages at an interval of 125s.

 Copyright © Huawei Technologies Co., Ltd.

Format

mld timer query *interval*

undo mld timer query

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an interface sends MLD General Query messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MLD querier sends MLD General Query messages at an interval to check whether a local network segment has multicast group members. This interval is the general query interval. You can set the general query interval based on the network situation. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages certain times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is one-fourth of the interval for sending General Query messages. The robustness variable can be set using the **mld robust-count** or **robust-count (MLD view)** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The querier is more sensitive when it sends General Query messages at a smaller interval. However, more bandwidth and router resources are consumed in this case.
- The function of the **MLD timer query** command is the same as that of the **timer query (MLD view)** command used in the MLD view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The system prefers the

 Copyright © Huawei Technologies Co., Ltd.

configuration in the interface view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the interval at which GE1/0/0 sends General Query messages to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld timer query 200
```

Related Topics

10.2.27 mld robust-count

10.2.40 robust-count (MLD view)

10.2.44 timer query (MLD view)

10.2.33 mld ttl-check

Function

The **mld ttl-check** command enables the device to check the TTL values in received MLD Report, Done, and Query messages on a specific interface.

The **undo mld ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received MLD Report, Done, and Query messages on an interface.

Format

mld ttl-check

undo mld ttl-check

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device against MLD message attacks, run the **mld ttl-check** command to enable the device to check the TTL values in received MLD Report,

 Copyright © Huawei Technologies Co., Ltd.

Done, and Query messages on a specific interface and discard such a message if its TTL value is not 1.

The **mld ttl-check** command provides the same function as the **ttl-check** command run in the MLD view, except that the **ttl-check** command configuration takes effect for all interfaces.

Configuration Impact

If both the **mld ttl-check** and **ttl-check** commands are run, the **mld ttl-check** configuration in the interface view takes precedence over the **ttl-check** configuration in the MLD view.

Example

Enable the device to check the TTL values in received MLD Report, Done, and Query messages on a specific interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld ttl-check
```

10.2.34 mld version

Function

The **mld version** command specifies an MLD version on an interface.

The **undo mld version** command restores the default MLD version on an interface.

By default, an interface runs MLDv2.

Format

mld version *version*

undo mld version

Parameters

Parameter	Description	Value
version	Specifies the MLD version running on the interface.	The value is integer that ranges from 1 to 2.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast router can identify MLD messages of a version earlier than its own MLD version but cannot identify MLD messages of a later version. To ensure normal MLD operation, ensure that the router runs the same MLD version as receiver hosts or a later MLD version.

If many routers exist on a shared network segment, configure the same MLD version on all router interfaces connected to hosts. If multicast devices run MLD of different versions, errors may occur in MLD operation because interfaces running different MLD versions send messages in different formats.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Configure MLDv2 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mld version 2
```

10.2.35 require-router-alert (MLD view)

Function

The **require-router-alert** command configures the router to discard MLD messages without the Router-Alert option.

The **undo require-router-alert** command disables the router from checking the Router-Alert option in MLD messages.

By default, the router does not check whether the received MLD messages contain Router-Alert options in IPv6 headers, and it accepts all the received MLD messages.

Format

require-router-alert

undo require-router-alert

Parameters

None

Views

MLD view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, a network device sends a message to the routing protocol module for processing only when the destination address of the message is a local interface address. Destination addresses of MLD messages are multicast addresses but not addresses of interfaces on multicast devices. Therefore, multicast devices do not send MLD messages to the MLD module for processing, and the MLD module cannot maintain group memberships.

The Router-Alert option in the IPv6 header of an MLD message solves this problem. If an MLD message contains the Router-Alert option, the device sends the message to the MLD module.

You can configure the device to accept only MLD messages with the Router-Alert option to improve MLD security.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld require-router-alert** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, configure the router to discard the MLD messages that do not contain Router-Alert options in IPv6 headers.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] require-router-alert
```

Related Topics

10.2.26 mld require-router-alert

10.2.36 reset mld control-message counters

Function

The **reset mld control-message counters** command deletes statistics of MLD messages.

Format

reset mld control-message counters [**interface** *interface-type interface-number*] [**message-type** { **query** | **report** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears MLD packet statistics on a specified interface. If this parameter is not specified, MLD packets on all interfaces are deleted.	-
message-type	Clears statistics about MLD messages of a specified type. If this parameter is not specified, the command clears statistics about MLD messages of all types.	-
query	Clears the number of received Query messages.	-
report	Clears the number of received Multicast Listener Report messages.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

After statistics about MLD messages are deleted, MLD still operates properly.

Example

Delete statistics about MLD messages from all interfaces.

```
<Huawei> reset mld control-message counters
```

Delete statistics about MLD messages from GE1/0/0.

```
<Huawei> reset mld control-message counters interface gigabitethernet 1/0/0
```

Related Topics

10.2.2 display mld control-message counters

10.2.37 reset mld explicit-tracking

Function

The **reset mld explicit-tracking** command deletes hosts that dynamically join a multicast group using MLD from an interface.

Format

reset mld explicit-tracking { **all** | **interface** *interface-type interface-number* [**host** *ipv6-host-address* [**group** *ipv6-group-address* [**source** *ipv6-source-address*]]] }

Parameters

Parameter	Description	Value
all	Indicates information about all MLD hosts.	-
interface *interface-type interface-number*	Specifies the type and number of an interface. If this parameter is not specified, the command deletes hosts that dynamically join the host group using MLD from all interfaces.	-
host *ipv6-host-address*	Specifies the link-local address of a host.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF80:: to FF80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
group *ipv6-group-address*	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
source *ipv6-source-address*	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.

Views

User view

Default Level

3: Management level

Usage Guidelines

You can use this command to delete hosts that dynamically join a multicast group using MLD from an interface. A host can rejoin the multicast group after being deleted from this group.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete the host FE80::101 that joins multicast group FF23::101 through MLD on GE1/0/0.

```
<Huawei> reset mld explicit-tracking interface gigabitethernet 1/0/0 host fe80::101 group ff23::101
```

Delete the host FE80::101 that joins the (FC00:0:0:1::12, FF23::101) forwarding entry from GE1/0/0.

```
<Huawei> reset mld explicit-tracking interface gigabitethernet 1/0/0 host fe80::101 group ff23::101
source fc00:0:0:1::12
```

Related Topics

10.2.3 display mld explicit-tracking

10.2.38 reset mld group

Function

The **reset mld group** command deletes dynamic MLD entries on interfaces.

Format

reset mld group all

reset mld group interface *interface-type interface-number* { **all** | *ipv6-group-address* [*ipv6-group-mask-length*] [*ipv6-source-address* [*ipv6-source-mask-length*]] }

Parameters

Parameter	Description	Value
all	The first **all** deletes dynamic MLD entries on all interfaces. The second **all** deletes all MLD entries on a specified interface.	-
interface *interface-type interface-number*	Deletes dynamic MLD entries on a specified interface.	-
ipv6-group-address	Deletes dynamic MLD entries of a specified multicast group.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-group-mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 8 to 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
ipv6-source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 128.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command deletes all the dynamic MLD group memberships on an interface, including common group memberships and group memberships established with SSM mapping. This command cannot delete statically configured MLD group memberships.

A host can rejoin the multicast group after being deleted from this group.

NOTICE

After dynamic MLD entries on an interface are deleted, the interface cannot receive multicast data. Exercise caution before running this command.

Example

Delete dynamic MLD entries within the range of FF03::101:0 to FF03::101:FFFF on GE1/0/0.

```
<Huawei> reset mld group interface gigabitethernet 1/0/0 ff03::101:0 112
```

Related Topics

10.2.4 display mld group

10.2.39 reset mld group ssm-mapping

 Copyright © Huawei Technologies Co., Ltd.

10.2.39 reset mld group ssm-mapping

Function

The **reset mld group ssm-mapping** command deletes multicast group entries established with MLD SSM mapping.

Format

reset mld group ssm-mapping all

reset mld group ssm-mapping interface *interface-type interface-number* { **all** | *ipv6-group-address* [*ipv6-group-mask-length*] }

Parameters

Parameter	Description	Value
all	The first **all** deletes multicast group entries established with MLD SSM mapping on all interfaces. The second **all** deletes all multicast group entries established with MLD SSM mapping on a specified interface.	-
interface *interface-type interface-number*	Deletes the multicast group entries established with MLD SSM mapping on a specified interface.	-
ipv6-group-address	Specifies an IPv6 multicast group address.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 8 to 128.

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command is valid on the multicast groups that the interface dynamically joins only, and only the MLDv1 multicast group entries within the range of SSM group addresses are deleted.

SSM mapping can be re-configured after being deleted.

NOTICE

After the multicast group entries established with MLD SSM mapping on an interface are deleted, the interface cannot receive multicast data. Exercise caution before running this command.

Example

Delete multicast group entries established with MLD SSM mapping within the range of FF13::101:0 to FF13::101:FFFF on GE1/0/0.

```
<Huawei> reset mld group ssm-mapping interface gigabitethernet 1/0/0 ff13::101:0 112
```

Related Topics

10.2.5 display mld group ssm-mapping

10.2.40 robust-count (MLD view)

Function

The **robust-count** command sets a global robustness variable for an MLD querier.

The **undo robust-count** command restores the default robustness variable.

By default, the robustness variable of an MLD querier is 2.

Format

robust-count *robust-value*

undo robust-count

Parameters

Parameter	Description	Value
robust-value	Specifies the robustness variable of an MLD querier.	The value is an integer that ranges from 2 to 5.

 Copyright © Huawei Technologies Co., Ltd.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD querier robustness variable specifies the retransmission count of MLD packets to minimize impact of packet loss on the network.

On a shared network segment, a querier maintains MLD group memberships. The robustness variable affects the timeout period of group memberships. The timeout period of the group membership is calculated using the formula:

Timeout period of the group memberships = Interval for sending MLD General Query messages x Robustness variable + Maximum response time

The robustness variable determines the following values:

- Number of times the querier sends General Query messages when the querier starts

  When a querier starts, it sends General Query messages certain times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The interval for sending General Query messages is configured using the **mld timer query** or **timer query (MLD view)** command.

- Number of times the querier sends Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages

  When receiving a Multicast Listener Done message of a multicast group, the querier sends Multicast Address Specific Query messages certain times specified by the robustness variable to check whether the group has members. When the querier receives a Multicast Listener Report message indicating that source-group mapping changes, the querier sends Multicast Address and Source Specific Query messages certain times specified by the robustness variable. The interval for sending Multicast Address Specific Query messages or Multicast Address and Source Specific Query messages is set using the **mld lastlistener-queryinterval** or **lastlistener-queryinterval (MLD view)** command.

A larger robustness variable makes an MLD querier more robust but increases the timeout period of group memberships.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld robust-count** command used in the interface view. The configuration in the MLD view is globally

 Copyright © Huawei Technologies Co., Ltd.

valid, whereas the configuration in the interface view takes effect only for the current interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

Set the robustness variable of an MLD querier to 3 in the MLD view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] robust-count 3
```

Related Topics

10.2.12 lastlistener-queryinterval (MLD view)

10.2.20 mld lastlistener-queryinterval

10.2.27 mld robust-count

10.2.32 mld timer query

10.2.44 timer query (MLD view)

10.2.41 send-router-alert (MLD view)

Function

The **send-router-alert** command configures the router to send MLD messages containing the Router-Alert option in IPv6 headers.

The **undo send-router-alert** command disables the router from sending MLD messages containing the Router-Alert option in IPv6 headers.

By default, MLD messages sent by the router contain the Router-Alert option.

Format

send-router-alert

undo send-router-alert

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, MLD messages sent by the router contain the Router-Alert option in their IPv6 headers. If the router needs to communicate with a device that does not support the Router-Alert option, run the **undo send-router-alert** command to configure the router to send MLD messages without the Router-Alert option. The **send-router-alert** command is usually used together with the **require-router-alert (MLD view)** command.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld send-router-alert** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, configure the router to send MLD packets with the Router-Alert option in IPv6 headers.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] send-router-alert
```

Related Topics

10.2.28 mld send-router-alert

10.2.35 require-router-alert (MLD view)

10.2.42 ssm-mapping (MLD view)

Function

The **ssm-mapping** command configures an SSM mapping entry to map a multicast source to a group address.

The **undo ssm-mapping** command deletes an SSM mapping entry.

By default, no SSM mapping entry is configured.

Format

ssm-mapping *ipv6-group-address ipv6-group-mask-length ipv6-source-address*

undo ssm-mapping { **all** | *ipv6-group-address ipv6-group-mask-length* [*ipv6-source-address*] }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies the IPv6 address of a multicast group configured with SSM mapping.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The value ranges from FF00:: to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer, which can be 16, 32, 64, or 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The value is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
all	Deletes all the configured static SSM mapping entries.	-

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hosts that support only MLDv1 cannot join SSM groups. To enable multicast devices to provide the SSM service for these hosts, configure SSM mapping on the multicast devices. An SSM mapping entry maps a multicast source to a multicast group. After SSM mapping entries are configured on a multicast device, the device can convert (*, G) information in Report messages of MLDv1 to (S, G) information.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- You can repeatedly run the **ssm-mapping** command to configure multiple static SSM mapping entries.
- To delete an SSM mapping entry, run the **undo ssm-mapping** *ipv6-group-address ipv6-group-mask-length* [*ipv6-source-address*] command. The **undo ssm-mapping all** command deletes all the SSM mapping entries. Exercise caution before running this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure an SSM mapping entry mapping the source address FC00::1 to group address FF35::1/128.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] ssm-mapping ff35::1 128 fc00::1
```

10.2.43 timer other-querier-present (MLD view)

Function

The **timer other-querier-present** command sets a global other querier present timer.

The **undo timer other-querier-present** command restores the default value of the other querier present timer.

By default, the Keepalive period of the other queriers is calculated as follows:

Other querier present timer = Robustness variable x Interval for sending MLD General Query messages + 1/2 x Maximum response time

If the default values of the robustness variable, interval for sending MLD General Query messages, and maximum response time are used, the other querier present timer value is 255 seconds.

Format

timer other-querier-present *interval*

undo timer other-querier-present

Parameters

Parameter	Description	Value
interval	Specifies the other querier present timer.	The value is an integer that ranges from 60 to 300, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user network segment connects to multiple Layer 3 multicast devices, only one Layer 3 multicast device is elected as the MLD querier to send Query

 Copyright © Huawei Technologies Co., Ltd.

messages to hosts on the network segment. To create and maintain normal group memberships, non-queriers running MLD start the other querier present timer after they fail in the querier election. If the non-queriers do not receive Query messages from the querier before the timer times out, they consider the querier failed and start a new querier election.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The function of this command is the same as that of the **mld timer other-querier-present** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

NOTICE

If the other querier present timer is shorter than the interval for sending General Query messages, the querier election is triggered frequently.

Example

Set the other querier present timer to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] timer other-querier-present 200
```

Related Topics

10.2.31 mld timer other-querier-present

10.2.44 timer query (MLD view)

Function

The **timer query** command sets a global interval for sending MLD General Query messages.

The **undo timer query** command restores the default interval for sending MLD General Query messages.

By default, the interval for sending MLD General Query messages is 125 seconds.

Format

timer query *interval*

undo timer query

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Interval for sending MLD General Query messages	The value is an integer that ranges from 1 to 18000, in seconds.

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MLD querier sends MLD General Query messages at an interval to check whether a local network segment has multicast group members. This interval is the general query interval. You can set the general query interval based on the network situation. The general query interval affects the following processes:

- When a querier starts, it sends General Query messages certain times specified by the robustness variable to query the multicast groups that have members on the shared network segment. The message sending interval during this process is one-fourth of the interval for sending General Query messages. The robustness variable can be set using the **mld robust-count** or **robust-count (MLD view)** command.
- After the startup process is complete, the querier sends General Query messages at intervals to maintain the group memberships on the interface.

Prerequisites

Layer 3 IPv6 multicast has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

- The querier is more sensitive when it sends General Query messages at a smaller interval. However, more bandwidth and router resources are consumed in this case.
- The function of this command is the same as that of the **mld timer query** command used in the interface view. The configuration in the MLD view is globally valid, whereas the configuration in the interface view takes effect only for the specified interface. The configuration in the interface view takes precedence over the configuration in the MLD view. The configuration in the MLD view is used only when no configuration is performed in the interface view.

Example

In the MLD view, set the interval for sending MLD General Query messages to 200 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] mld
[Huawei-mld] timer query 200
```

Related Topics

10.2.32 mld timer query

10.2.27 mld robust-count

10.2.40 robust-count (MLD view)

10.2.45 ttl-check (IPv6)

Function

The **ttl-check** command enables the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces.

The **undo ttl-check** command restores the default configuration.

By default, the device does not check the TTL values in received MLD Report, Done, and Query messages.

Format

ttl-check

undo ttl-check

Parameters

None

Views

MLD view

Default Level

2: Configuration level

Usage Guidelines

To protect a device against MLD message attacks, run the **ttl-check** command to enable the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces and discard such a message if its TTL value is not 1.

Example

Enable the device to check the TTL values in received MLD Report, Done, and Query messages on all interfaces.

```
<Huawei> system-view
[Huawei] mld
[Huawei-mld] ttl-check
```

 Copyright © Huawei Technologies Co., Ltd.

10.3 PIM (IPv4) Configuration Commands

NOTE

AR120 series do not support this function.

10.3.1 anycast-rp (IPv4)

Function

The **anycast-rp** command configures an Anycast RP and displays the Anycast-RP view or directly displays the existing Anycast-RP view.

The **undo anycast-rp** command deletes the configurations of an Anycast RP.

By default, no Anycast RP is configured.

Format

anycast-rp *rp-address*

undo anycast-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Indicates the Anycast RP address.	The value is in dotted decimal notation. This address must be a valid unicast IP address and cannot be an address on the network segment 127.0.0.0/8.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a traditional PIM-SM domain, all multicast groups map to one RP. When the network is overloaded or traffic concentrates on an RP, the RP may be overburdened. If the RP fails, routes are converged slowly or multicast packets are forwarded over non-optimal paths.

Configuring the Anycast RP in the PIM-SM domain can address this problem. IP routing will automatically select the topologically closest RP for each source and receiver. This releases burdens on RPs, implements RP backup, and optimizes the forwarding paths.

 Copyright © Huawei Technologies Co., Ltd.

Currently, the Anycast RP can be implemented in a PIM domain by using the following schemes:

- MSDP Anycast RP, which is applicable to IPv4 networks
- PIM Anycast RP, which is applicable to IPv4 networks

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If PIM Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message. In such a manner, Anycast RP peers can learn source/group information from each other.

Precautions

- In IPv4 network deployment, you can choose either of the two schemes. Mixed use of the two schemes is not recommended.
- The Anycast RP address must be the same as that of the elected RP on the current network.
- In a single instance, you can configure a maximum of four Anycast RP addresses on each device.
- Either static or dynamic RPs can be used on the network. Configuring RPs on loopback interfaces is recommended. You need to configure the same RP address on the devices to be deployed with the Anycast RP. If the dynamic RP is used on the network, before configuring an Anycast RP address, run the **display pim rp-info** command to check the address of the RP on the current network.

Example

Set the Anycast RP address to 10.10.10.10 in the public network instance and enter the Anycast-RP view.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] anycast-rp 10.10.10.10
[Huawei-pim-anycast-rp-10.10.10.10]
```

Related Topics

10.3.43 local-address (IPv4)
10.3.45 peer (IPv4)
10.3.30 display pim rp-info

10.3.2 auto-rp listening enable

Function

The **auto-rp listening enable** command enables the auto-RP listening function. A device receives auto-RP announcement and discovery messages and learns RP information from the messages.

The **undo auto-rp listening enable** command restores the default configuration.

By default, auto-RP listening is disabled.

Format

auto-rp listening enable

undo auto-rp listening enable

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The auto-RP listening function enables the device to receive auto-RP announcement and discovery messages and learn RP information from the messages. After receiving an Auto-RP Advertisement or Discovery message, the device obtains the source address of the message, and then performs reverse path forwarding (RPF) check based on the source address. If the RPF check fails, the device discards the packet. If the RPF check succeeds, the device forwards the packet to other PIM neighbors.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

In the public network instance, enable auto-RP listening on a router.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] auto-rp listening enable
```

 Copyright © Huawei Technologies Co., Ltd.

10.3.3 bsm semantic fragmentation (IPv4)

Function

The **bsm semantic fragmentation** command enables BSR message fragmentation.

The **undo bsm semantic fragmentation** command disables BSR message fragmentation.

By default, BSR message fragmentation is not enabled.

Format

bsm semantic fragmentation

undo bsm semantic fragmentation

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BSR message carries information about all C-RPs on the network. Therefore, if there is a large number of C-RPs on the network, the length of a BSR message exceeds the MTU of the outgoing interface. As a result, the BSR message cannot be processed and RP election fails. Consequently, multicast services cannot be transmitted normally. In this case, you can enable BSR message fragmentation to ensure that the devices on the network can learn consistent RP information and MDTs can be successfully established.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

You can also configure IP fragmentation to solve the preceding problem. The difference between IP fragmentation and BSR message fragmentation is as follows:

- If IP fragmentation is enabled, the protocol layer transmits the entire BSR message up to the IP layer regardless of the length of the BSR message. The BSR message is then fragmented at the IP layer. During the transmission of

 Copyright © Huawei Technologies Co., Ltd.

BSR message fragments to the destination, if one fragment is lost, the destination cannot parse the entire BSR message. As a result, the destination cannot learn RP information and MDTs cannot be established, which causes a multicast data forwarding failure.

- If BSR message fragmentation is enabled, the protocol layer directly fragments a long BSR message. During the transmission of BSR message fragments to the destination, if one fragment is lost, only the information carried in this fragment is lost. As a result, only MDTs corresponding to the information carried in the lost fragments cannot be established. Since the other BSR message fragments can still reach the destination, the corresponding MDTs can be correctly established.

BSR message fragmentation is recommended because it can solve the problem faced by IP fragmentation that all fragments become unavailable due to loss of fragment information.

Precautions

Enable BSR message fragmentation on all devices on the network. If BSR message fragmentation is not enabled on some devices, RP information on these devices is inconsistent with that on other devices and MDTs cannot be established on these devices.

Example

Enable BSR message fragmentation in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] bsm semantic fragmentation
```

10.3.4 bsr-policy (IPv4)

Function

The **bsr-policy** command specifies the range of valid bootstrap router (BSR) addresses. Then the router drops the BSR messages sent from the addresses out of this range to defend against BSR spoofing.

The **undo bsr-policy** command restores the default configuration.

By default, the range of BSR addresses is not limited, and all BSR packets are considered valid.

Format

bsr-policy { *basic-acl-number* | **acl-name** *acl-name* }

undo bsr-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the basic ACL number. The ACL defines the filtering policy for the range of source addresses of BSR packets. This parameter corresponds to *basic-acl-number* in the **acl** command.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-SM network that applies the BSR mechanism, you can configure any router as a C-BSR to elect the BSR. Once being elected as the BSR, the router is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, use the following measures:

- Certain hosts try changing the RP mapping to spoof the router by forging BSR packets.

  Solution: The attack often occurs on edge routers because the BSR packet is a multicast packet and the TTL value of the BSR packet is 1. The BSR is inside the network, and hosts are outside the network. The routers can perform neighbor check and RPF check on the received BSR packets to prevent the attack.
- Certain attackers control the router on the network, or the router accesses the network. The attackers configure the router as a C-BSR, and help the router win the BSR election. The attackers obtain the right of advertising RP information in the network.

  Solution: After the router is configured as a C-BSR, the router spreads BSR packets in the network. The BSR packets are multicast packets. The TTL value of BSR packets is 1. The BSR packets are forwarded hop by hop. As long as the neighboring router cannot receive the packets, the packets are not spread in the entire network. The solution is to use the **bsr-policy** command on every router in the network to limit the valid BSR range. For example, only routers 10.1.1.1/32 and 10.1.1.2/32 are elected as BSRs; therefore, the routers do not receive or forward other BSR packets. This type of attack is prevented.

 Copyright © Huawei Technologies Co., Ltd.

The two countermeasures mentioned above can partially protect BSRs in the network. If attackers control a valid BSR, it also brings problems to the network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

After the **bsr-policy** command is run, the router accepts only BSR messages matching the configured policy.

Precautions

The **bsr-policy** command and the **acl** command are used together. In the ACL view, you can set the source address range for BSR packets by specifying the **source** parameter in the **rule** command.

When you use the **rule** command to configure a filtering rule for the Named ACL, the rule is effective only within the source address range specified by the **source** parameter and within the time period specified by the **time-range** parameter.

Example

In the public network instance, configure address 10.1.1.0/24 as the valid BSR address range.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.1.1.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] pim
[Huawei-pim] bsr-policy 2001
```

In the public network instance, use a Named ACL to configure address 10.1.1.0/24 as the valid BSR address range.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.1.1.0 0.0.0.255
[Huawei-acl-adv-myacl] quit
[Huawei] pim
[Huawei-pim] bsr-policy acl-name myacl
```

10.3.5 c-bsr (IPv4)

Function

The **c-bsr** command configures a C-BSR.

The **undo c-bsr** command restores the default configuration.

By default, the C-BSR is not configured.

Format

c-bsr *interface-type interface-number* [*hash-length* [*priority*]]

undo c-bsr

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface. C-BSR is configured on this interface. PIM-SM must be enabled on this interface to make the configuration effective. **NOTE** To avoid frequent protocol changes caused by interface flapping, using loopback interfaces is recommended.	-
hash-length	Specifies the hash mask length of the C-BSR. The mask is used in a hash function to calculate the RP.	The value is an integer that ranges from 0 to 32. By default, the value is 30.
priority	Specifies a priority of the C-BSR. The greater the value, the higher the priority of the C-BSR.	The value is an integer ranging from 0 to 255. By default, the value is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more C-BSRs need to be configured in a PIM-SM domain. A BSR is elected from C-BSRs. The BSR is responsible for collecting C-RP information and summarizing C-RP information into an RP-set. The RP-set is then encapsulated in a BootStrap message and advertised to all the devices in the PIM domain.

The process of BSR election is as follows:

1. Each C-BSR considers itself as the BSR of the local PIM-SM domain and uses IP address of this interface as the address of the BSR to send Bootstrap messages.
2. When a C-BSR receives a Bootstrap message from other devices, it compares the BSR in the received Bootstrap message with the current BSR. The BSR with the highest priority is preferred. If BSRs have the same priority, the BSR with a larger IP address is preferred. If the BSR carried in the received Bootstrap message is better than the current BSR, the C-BSR replaces its BSR address with the address of the BSR carried in the received Bootstrap message.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Before configuring an interface as a C-BSR, enable PIM-SM on the interface.

Example

In the public network instance, configure a C-BSR on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim sm
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] pim
[Huawei-pim] c-bsr gigabitethernet 1/0/0
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.62 pim sm

10.3.6 c-bsr admin-scope

Function

The **c-bsr admin-scope** command configures a BSR administrative scope in a PIM-SM domain.

The **undo c-bsr admin-scope** command restores the default configuration.

By default, no BSR administrative scope is configured.

Format

c-bsr admin-scope

undo c-bsr admin-scope

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BSR and the BSR serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative domains and a global domain. This can reduce the workload of a single BSR and designate a private-network group address for users in a specific domain.

Each BSR administrative domain maintains one BSR that serves multicast groups on network segment 239.0.0.0/8. Multicast packets for groups on this network segment cannot pass through the border of the BSR administrative domain. Multicast groups that do not belong to any BSR administrative domain belong to a global domain. The global domain maintains a BSR, serving all the remained multicast groups, namely, multicast groups beyond the range 239.0.0.0/8.

A BSR administrative domain is similar to a VPN in unicast and multicast address segment 239.0.0.0/8 equals unicast address segment 10.0.0.0/8. Other multicast group addresses can be used on the public network and address conflicts need be avoided. If a PIM-SM domain is divided into different BSR administrative domains, each BSR administrative domain equals a VPN, serving the multicast groups on the network segment 239.0.0.0/8. You can use the same multicast group address in different BSR administration domains. If you configure the BSR in a BSR administration domain to serve multicast groups beyond 239.0.0.0/8, a message indicating a configuration error will be displayed.

The **c-bsr admin-scope** command configures a BSR administrative scope on the router.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **c-bsr admin-scope** command needs to be run on all the devices in a PIM-SM domain.

Example

In the public network instance, configure a BSR administrative scope in a PIM-SM domain.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-bsr admin-scope
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.7 c-bsr global

Function

The **c-bsr global** command configures the router as a C-BSR in the global domain.

The **undo c-bsr global** command restores the default configuration.

By default, no C-BSR is configured in the global domain.

Format

c-bsr global [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

Parameters

Parameter	Description	Value
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in the global domain.	The value is an integer that ranging from 0 to 32. By default, the value is 30.
priority *priority*	Specifies the priority of the C-BSR in the global domain. The greater the value, the higher the priority of the C-BSR.	The value is an integer ranging from 0 to 255. By default, it is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PIM-SM network is divided into multiple BSR administrative domains and a global domain. The global domain maintains a BSR that serves the remaining multicast groups.

The **c-bsr global** command configures the router as a C-BSR in the global domain. The BSR in the global domain is generated through election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **c-bsr global** command takes effect only in a BSR administrative domain. This means that the **c-bsr global** command can enable a device in a BSR administrative domain to accept multicast data of group out of the BSR administrative domain.

The **c-bsr global** command needs to be used together with the **c-bsr admin-scope** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the public network instance, configure the router as a C-BSR in the global domain, and then set the priority of the C-BSR to 1.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-bsr global priority 1
```

Related Topics

10.3.6 c-bsr admin-scope

10.3.8 c-bsr group

10.3.12 c-bsr priority (IPv4)

10.3.8 c-bsr group

Function

The **c-bsr group** command specifies the range of multicast groups that an administrative domain can serve on a C-BSR.

The **undo c-bsr group** command restores the default configuration.

By default, range of multicast groups that an administrative domain can serve is not configured.

Format

c-bsr group *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr group *group-address*

Parameters

Parameter	Description	Value
group-address	Specifies a multicast group address.	The address is in dotted decimal notation. The value ranges from 239.0.0.0 to 239.255.255.255.
mask	Specifies the mask of a multicast group address.	The address is in dotted decimal notation.
mask-length	Indicates the mask length of a multicast address.	The value is an integer ranging from 8 to 32.
hash-length *hash-length*	Specifies the hash mask length for the C-BSR in a BSR administrative domain.	The value is an integer ranging from 0 to 32. By default, it is 30.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
priority *priority*	Specifies the priority of the C-BSR in the BSR administrative domain. A larger value indicates a higher priority.	The value is an integer ranging from 0 to 255. By default, it is 0.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PIM-SM domain is divided into different BSR administrative domains, configure a multicast group address for each BSR administrative domain on the C-BSR. The group addresses must be in the range of 239.0.0.0/8. The group address ranges served by different BSR administrative domains can overlap. The address of a multicast group that a BSR administrative domain serves is used as a private group address.

By running this command on the C-BSR of each administrative domain, you can specify the group address of the administrative domain served by each C-BSR and priority of each C-BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

In the public network instance, configure a C-BSR in the BSR administrative domain to serve groups 239.0.0.0/8, and set the priority of the C-BSR to 10.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

Related Topics

10.3.6 c-bsr admin-scope

10.3.7 c-bsr global

10.3.12 c-bsr priority (IPv4)

 Copyright © Huawei Technologies Co., Ltd.

10.3.9 c-bsr hash-length (IPv4)

Function

The **c-bsr hash-length** command configures the global hash mask length of a C-BSR.

The **undo c-bsr hash-length** command restores the default configuration.

By default, the global hash mask length of a C-BSR is 30.

Format

c-bsr hash-length *hash-length*

undo c-bsr hash-length

Parameters

Parameter	Description	Value
hash-length	Specifies the global hash mask length of a C-BSR.	The value is an integer that ranges from 0 to 32.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During dynamic RP election, if C-RPs have the same interface address mask and priority for a specified multicast group, a hash function needs to be executed to select the RP for the multicast group. The router performs hash calculation for the group address of G, C-RP address, and hash mask length of the C-RPs with the same priority and compares the hash values. The C-RP with the greatest hash value acts as the RP for G.

The hash mask length is used to adjust the hash calculation result.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

You can run the **c-bsr** *interface-type interface-number hash-length* command in the PIM view to configure the C-BSR interface and specify the hash mask length. The **c-bsr hash-length** *hash-length* command specifies the global hash mask

 Copyright © Huawei Technologies Co., Ltd.

length. If both **c-bsr** *interface-type interface-number hash-length* and **c-bsr hash-length** *hash-length* are used, the **c-bsr** *interface-type interface-number hash-length* command takes effect.

Example

In the public network instance, set the global hash mask length of a C-BSR to 16.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-bsr hash-length 16
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.7 c-bsr global

10.3.8 c-bsr group

10.3.10 c-bsr holdtime (IPv4)

Function

The **c-bsr holdtime** command configures the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR.

The **undo c-bsr holdtime** command restores the default configuration.

By default, the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR is 130s.

Format

c-bsr holdtime *interval*

undo c-bsr holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which C-BSR waits for the Bootstrap message to be sent by BSR.	The value is an integer that ranges from 1 to 214748364, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, the C-BSR periodically sends Bootstrap messages carrying the IP address of the C-BSR and the RP-set information. The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the elected BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command.

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer. The C-BSRs that fail in the election also refresh the timeout period of the BSR according to the hold time. After the BSR times out, the C-BSRs receive new BSR messages.
- If the timer times out, the elected BSR is considered faulty. The C-BSRs that fail the previous election elect a new BSR. Services are not interrupted.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime. If the configured values are different, the BSR may become unstable. This may result in multicast faults. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If BS_interval or holdtime is configured, use the following formula to calculate the other one:

  holdtime = 2 x BS_interval + 10

  The following determines which value is used:

  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither BS_interval nor holdtime is configured, the default values are used. The default BS_interval is 60 seconds and the default holdtime is 130s.

Example

In the public network instance, set the timeout interval during which the C-BSR waits for the Bootstrap message to be sent by BSR to 150 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-bsr holdtime 150
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.5 c-bsr (IPv4)

10.3.11 c-bsr interval (IPv4)

10.3.11 c-bsr interval (IPv4)

Function

The **c-bsr interval** command configures the interval for the BSR to continuously send Bootstrap messages.

The **undo c-bsr interval** command restores the default configuration.

By default, the interval for the BSR to continuously send Bootstrap messages is 60s.

Format

c-bsr interval *interval*

undo c-bsr interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for the BSR to continuously send the Bootstrap messages.	The value is an integer that ranges from 1 to 107374177, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, the C-BSR periodically sends Bootstrap messages carrying the IP address of the C-BSR and the RP-set information to the network.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command. The following applies to the timer:

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer.

 Copyright © Huawei Technologies Co., Ltd.

- If the timer times out, the BSR is considered to be faulty. The C-BSRs that fail in the election triggers a new BSR election. Services are not interrupted.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime. If the configured values are different, the BSR may become unstable. This may result in a multicast fault. Note the following points:

- If BS_interval and holdtime are configured at the same time, ensure that BS_interval is less than holdtime.
- If only one of the BS_interval and holdtime is configured, use the following formula to calculate the other parameter: holdtime = 2 x BS_interval + 10. The following determines which value is used:
  - If holdtime is configured and the calculated BS_interval is less than the minimum value of BS_interval, the minimum value is used.
  - If BS_interval is configured and the calculated holdtime is more than the maximum value of holdtime, the maximum value is used.
- If neither the BS_interval nor the holdtime is configured, default values are used. The default value of BS_interval is 60s, and the default value of holdtime is 130s.

Example

In the public network instance, set the interval for the C-BSR to continuously send Bootstrap messages to 30 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-bsr interval 30
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.10 c-bsr holdtime (IPv4)

10.3.12 c-bsr priority (IPv4)

Function

The **c-bsr priority** command configures the global priority for a C-BSR.

The **undo c-bsr priority** command restores the default configuration.

By default, the global priority of the C-BSR is 0.

Format

c-bsr priority *priority*

undo c-bsr priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of the C-BSR. The greater the value, the higher the priority of the C-BSR.	The value is an integer that ranges from 0 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple C-BSRs take part in the BSR election in the PIM-SM domain, the following situations occur:

- The router with the highest priority wins in the BSR election.
- In the case of the same priority, the router with the largest IP address wins in the BSR election.

To enable a C-BSR to function as the BSR, you can run the **c-bsr priority** command to increase the priority value of the C-BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

You can run the **c-bsr** *interface-type interface-number priority* command in the PIM view to configure the C-BSR interface and specify the C-BSR priority. The **c-bsr priority** *priority* command specifies the global C-BSR priority. If both **c-bsr** *interface-type interface-number priority* and **c-bsr priority** *priority* are used, the **c-bsr** *interface-type interface-number priority* command takes effect.

Example

In the public network instance, configure the global priority of the C-BSR to 5.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-bsr priority 5
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.8 c-bsr group
10.3.7 c-bsr global

10.3.13 c-rp (IPv4)

Function

The **c-rp** command configures the router to advertise itself as a C-RP to the BSR.

The **undo c-rp** command restores the default configuration.

By default, no C-RP is configured.

Format

c-rp *interface-type interface-number* [**group-policy** { *basic-acl-number* | **acl-name** *acl-name* } | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and the number of an interface. The IP address of the specified interface is advertised as a C-RP address. **NOTE** To avoid frequent protocol changes caused by interface flapping, using loopback interfaces is recommended.	-
group-policy *basic-acl-number*	Specifies the range of the multicast groups served by a C-RP. The range is restricted to the multicast group range permitted by the specified ACL. The *basic-acl-number* parameter specifies the number of the basic ACL to identify the service range of the advertised RP.	The value is an integer ranging from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
priority *priority*	Specifies the priority of a C-RP. The greater the value, the lower the priority.	The value is an integer ranging from 0 to 255. The default value is 0.
holdtime *hold-interval*	Specifies the timeout period during which the BSR waits to receive an Advertisement message from a C-RP.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 150.
advertisement-interval *adv-interval*	Specifies the interval for a C-RP to send Advertisement messages.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 60.

Views

PIM view of the public network instance or PIM view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RP is the core of a PIM-SM or Bidir-PIM domain, and therefore a C-RP must be able to communicate with the other devices in the PIM-SM or Bidir-PIM domain. You are advised to configure a C-RP on the core router and reserve enough bandwidth between the router and each of the other devices in the PIM-SM or Bidir-PIM domain.

An RP is elected from multiple C-RPs following these rules:

1. The C-RP with the longest mask length of the served group address range matching the multicast group that users have joined wins.
2. The C-RP with highest priority wins.
3. If multiple C-RPs have the same priority, the C-RP with the largest hash value wins.
4. If all the preceding factors are the same, the C-RP with the largest address wins.

Prerequisites

- IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.
- PIM-SM has been enabled on the interface that acts as the C-RP.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

An interface is specified in the command; therefore, the settings of **group-policy** { *basic-acl-number* | **acl-name** *acl-name* }, **priority** *priority*, **holdtime** *hold-interval* and **advertisement-interval** *adv-interval* configured using this command override the global parameter settings that the interface obtains from the PIM view. If you run this command multiple times and specify the same interface, only the latest configuration takes effect.

NOTE

If IP address unnumbered is configured, it is not recommended to configure C-RP on the interfaces that use the same addresses. If the interfaces have different priorities, the BSR considers that the C-RP configuration has been repeatedly modified.

Precautions

- *basic-acl-number* specifies a group range. All permitted group ranges will be advertised as the ranges of groups that the RP serves. If no group range is specified, the C-RP serves all multicast groups.
- To enable a C-RP to serve multiple PIM-SM domains, configure multiple **rule**s in the ACL to specify multicast group ranges for the domains.

Example

In the public network instance, use basic ACL 2069 to specify Loopback 0 as the C-RP for PIM-SM domains 225.1.0.0/16 and 226.2.0.0/16, and set the C-RP priority to 10.

```
<Huawei> system-view
[Huawei] acl number 2069
[Huawei-acl-basic-2069] rule permit source 225.1.0.0 0.0.255.255
[Huawei-acl-basic-2069] rule permit source 226.2.0.0 0.0.255.255
[Huawei-acl-basic-2069] quit
[Huawei] multicast routing-enable
[Huawei] interface loopback 0
[Huawei-LoopBack0] pim sm
[Huawei-LoopBack0] quit
[Huawei] pim
[Huawei-pim] c-rp loopback 0 group-policy 2069 priority 10
```

In the public network instance, use named ACL **myacl** to specify Loopback 0 as the C-RP of PIM-SM multicast domains 225.1.0.0/16 and 226.2.0.0/16, and set the C-RP priority to 10.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] rule permit ip destination 226.2.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] interface loopback 0
[Huawei-LoopBack0] pim sm
[Huawei-LoopBack0] quit
[Huawei] pim
[Huawei-pim] c-rp loopback 0 group-policy acl-name myacl priority 10
```

Related Topics

10.3.5 c-bsr (IPv4)

10.3.14 c-rp advertisement-interval (IPv4)

Function

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages.

The **undo c-rp advertisement-interval** command restores the default interval.

By default, a C-RP sends Advertisement messages at an interval of 60 seconds.

Format

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a C-RP sends Advertisement messages.	The value ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All C-RPs in a PIM-SM domain periodically send Advertisement messages to the same BSR. The BSR can collect the integrated RP-Set.

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages to the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

You can also set the advertisement interval when you run the **c-rp** *interface-type interface-number* **advertisement-interval** *adv-interval* command in the PIM view to configure the C-RP interface. The **c-rp advertisement-interval** *interval* command specifies the global advertisement interval. If both the commands are configured, the interval configured by the **c-rp** *interface-type interface-number* **advertisement-interval** *adv-interval* command takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the public network instance, set the interval at which a C-RP sends Advertisement messages to 30s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-rp advertisement-interval 30
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.15 c-rp holdtime (IPv4)

Function

The **c-rp holdtime** command configures the holdtime for a received Advertisement message on a BSR.

The **undo c-rp holdtime** command restores the default holdtime.

By default, the holdtime for a received Advertisement message is 150 seconds.

Format

c-rp holdtime *interval*

undo c-rp holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period for a BSR to wait the Advertisement message from a C-RP.	The value ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When *interval* is set on a C-RP, the C-RP encapsulates *interval* in an Advertisement message and sends it to the BSR. The BSR obtains this *interval* from the message and starts the timer. If the BSR receives no Advertisement message from the C-RP within the timeout period, the BSR regards the C-RP invalid or unreachable.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

You can also set the holdtime for a received Advertisement message when you run the **c-rp** *interface-type interface-number* **holdtime** *hold-interval* in the PIM view to configure a C-PR interface. The **c-rp holdtime** *hold-interval* configures the global hold time for Advertisement messages. If both the two commands are configured, the holdtime configured by the **c-rp** *interface-type interface-number* **holdtime** *hold-interval* command takes effect.

Example

In the public network instance, set the holdtime for a received Advertisement message to 100s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-rp holdtime 100
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.16 c-rp priority (IPv4)

Function

The **c-rp priority** command configures the global priority of a C-RP.

The **undo c-rp priority** command restores the default configuration.

By default, the global priority of a C-RP is 0.

Format

c-rp priority *priority*

undo c-rp priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of a C-RP. The greater the value, the lower the priority.	The value is an integer that ranges from 0 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following rules are used to elect an RP from multiple C-RPs:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- In case of the same priority, hash functions are operated. The C-RP with the greatest calculated value wins.
- If all the preceding factors are the same, the C-RP with the largest address wins.

To enable a C-RP to function as an RP, you can run the **c-rp priority** command to increase the priority of the C-RP.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

You can run the **c-rp** *interface-type interface-number* **priority** *priority* command in the PIM view to configure the C-RP interface and specify the C-RP priority. The **c-rp priority** *priority* command specifies the global C-RP priority. If both **c-rp** *interface-type interface-number* **priority** *priority* and **c-rp priority** *priority* are used, the **c-rp** *interface-type interface-number* **priority** *priority* command takes effect.

Example

In the public network instance, set the global priority of a C-RP to 5.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] c-rp priority 5
```

Related Topics

10.3.13 c-rp (IPv4)

10.3.17 crp-policy (IPv4)

Function

The **crp-policy** limits the range of valid C-RP addresses and the range of the multicast addresses served by a C-RP. The BSR drops the C-RP messages with addresses out of the specified range to protect valid C-RPs.

The **undo crp-policy** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, the BSR does not limit the range of valid C-RP addresses and the range of the multicast groups served by a C-RP. The BSR considers all the received C-RP messages valid.

Format

crp-policy { *advanced-acl-number* | **acl-name** *acl-name* }

undo crp-policy

Parameters

Parameter	Description	Value
advanced-acl-number	Specifies the number of an advanced ACL. The ACL defines the range of the C-RP addresses and the range of the group addresses served by a C-RP.	The value is an integer that ranges from 3000 to 3999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM SM network that uses the BSR mechanism, any router can be configured as a C-RP to serve the multicast groups in a specified range. Each C-RP sends its information to the BSR in unicast mode. The BSR summarizes all received C-RP information as the RP-set, and floods it through BSR messages on the entire network. The local router then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RP from being spoofed, configure **crp-policy** on BSR routers to limit the range of valid C-RP addresses and the range of multicast group addresses served by a C-RP. Configure the same filtering rule on each C-BSR because any C-BSR can become the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

If an ACL rule is specified but no C-RP address range is set, all C-RP messages are denied.

Precautions

The **crp-policy** command and the **acl** command are used together. In the ACL view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule** command. You can set the address range of multicast groups that are served by specifying the **destination** parameter in the **rule** command.

Example

Configure a C-RP policy on the C-BSR, which allows only the C-RP with the address 10.1.1.1/32 and allows the C-RP to serve only the multicast groups 225.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl number 3100
[Huawei-acl-adv-3100] rule permit ip source 10.1.1.1 0 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-3100] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] crp-policy 3100
```

Use a named ACL to configure a C-RP policy on the C-BSR : only 10.1.1.1/32 can function as the C-RP, and the C-RP is allowed to service only the multicast groups in the range of 225.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.1.1.1 0 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] crp-policy acl-name myacl
```

10.3.18 display default-parameter pim-dm

Function

The **display default-parameter pim-dm** command displays default configurations about PIM-DM.

Format

display default-parameter pim-dm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-dm** command displays default configurations about PIM-DM. Even if PIM-DM parameters are modified, the **display default-parameter pim-dm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configurations about PIM-DM.

```
<Huawei> display default-parameter pim-dm
 PIM View Default Configurations:
 ---------------------------------
 Hello-option dr-priority: 1
 Hello-option holdtime: 105 s
 Hello-option lan-delay: 500 ms
 Hello-option neighbor-tracking: disabled
 Hello-option override-interval: 2500 ms
 Holdtime assert: 180 s
 Holdtime join-prune: 210 s
 Source-lifetime: 210 s
 State-refresh-interval: 60 s
 State-refresh-rate-limit: 30 s
 State-refresh-ttl: 255
 Hello periodic interval: 30 s
 Join-prune periodic interval: 60 s

 Interface View Default Configurations:
 --------------------------------------
 Pim bfd: disabled
 Pim hello-option dr-priority: 1
 Pim hello-option holdtime: 105 s
 Pim hello-option lan-delay: 500 ms
 Pim hello-option neighbor-tracking: disabled
 Pim hello-option override-interval: 2500 ms
 Pim holdtime assert: 180 s
 Pim holdtime join-prune: 210 s
 Pim require-genid: disabled
 Pim silent: disabled
 Pim state-refresh-capable: enabled
 Pim timer dr-switch-delay: disabled
 Pim timer graft-retry: 3 s
 Pim hello periodic interval: 30 s
 Pim join-prune periodic interval: 60 s
 Pim triggered-hello-delay: 5 s
 Pim version: 2
 Pim neighbor-policy: disabled
```

Table 10-37 Description of the **display default-parameter pim-dm** command output

Item	Description
PIM View Default Configurations	Indicates default configurations in the PIM view.
Hello-option dr-priority	Indicates the priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hello-option holdtime	Indicates the time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Indicates the delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Indicates whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Indicates the interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Indicates the time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Indicates the time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Source-lifetime	Indicates the timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv4)** command.
State-refresh-interval	Indicates the interval for sending State-Refresh messages. This parameter is configured by the **state-refresh-interval (IPv4)** command.
State-refresh-rate-limit	Indicates the minimum interval from when the last State-Refresh message is received to when the next State-Refresh message is received. This parameter is configured by the **state-refresh-rate-limit (IPv4)** command.
State-refresh-ttl	Indicates the TTL value of the State-Refresh message. This parameter is configured by the **state-refresh-ttl (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hello periodic interval	Indicates the interval for sending Hello messages. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Indicates the interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv4)** command.
Interface View Default Configurations	Indicates the default configurations in the interface view.
Pim bfd	Indicates the PIM BFD on an interface. This parameter is configured by the**pim bfd enable** command.
Pim hello-option dr-priority	Indicates the priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Indicates the time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Indicates the delay in transmitting Prune messages at the shared network segment where the interface resides. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Indicates whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Indicates the interval for the interface to send Prune Override messages. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Indicates the time period for the interface to hold the Assert state. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Indicates the time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim holdtime join-prune** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim require-genid	Indicates whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Indicates whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim state-refresh-capable	Indicates whether State-Refresh is enabled on the interface. This parameter is configured by the **pim state-refresh-capable** command.
Pim timer dr-switch-delay	Indicates whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim timer graft-retry	Indicates the interval for the interface to retransmit Graft messages. This parameter is configured by the **pim timer graft-retry** command.
Pim hello periodic interval	Indicates the interval for the interface to send Hello messages. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Indicates the interval for the interface to send Join/Prune messages. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Indicates the maximum delay for the interface to send Hello messages. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Indicates the version of PIM enabled on the interface.
Pim neighbor-policy	Indicates whether the neighbor-policy is set on the interface. This parameter is configured by the **pim neighbor-policy** command.

 Copyright © Huawei Technologies Co., Ltd.

10.3.19 display default-parameter pim-sm

Function

The **display default-parameter pim-sm** command displays default configurations about PIM-SM.

Format

display default-parameter pim-sm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-sm** command displays default configurations about PIM-SM. Even if PIM-SM parameters are modified, the **display default-parameter pim-sm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configurations about PIM-SM.

```
<Huawei> display default-parameter pim-sm
  PIM View Default Configurations:
  --------------------------------
  Auto-rp listening enable: disabled
  Bsr-policy: disabled
  C-bsr admin-scope: disabled
  C-bsr global: disabled
  C-bsr group: none
  C-bsr hash-length: 30
  C-bsr holdtime: 130 s
  C-bsr interval: 60 s
  C-bsr priority: 0
  C-rp advertisement-interval: 60 s
  C-rp holdtime: 150 s
  C-rp priority: 0
  Crp-policy: disabled
  Bsm semantic fragmentation: disabled
  Hello-option dr-priority: 1
  Hello-option holdtime: 105 s
  Hello-option lan-delay: 500 ms
  Hello-option neighbor-tracking: disabled
  Hello-option override-interval: 2500 ms
  Holdtime assert: 180 s
```

 Copyright © Huawei Technologies Co., Ltd.

```
Holdtime join-prune: 210 s
Probe-interval: 5 s
Register-header-checksum: disabled
Register-policy: disabled
Register-suppression-timeout: 60 s
Source-lifetime: 210 s
Source-policy: disabled
Spt-switch-threshold: disabled
Ssm-policy: disabled
Static-rp:  disabled
Hello periodic interval: 30 s
Join-prune periodic interval: 60 s
Timer spt-switch: 15 s

Interface View Default Configurations:
--------------------------------------
Pim bfd: disabled
Pim bsr-boundary: disabled
Pim hello-option dr-priority: 1
Pim hello-option holdtime: 105 s
Pim hello-option lan-delay: 500 ms
Pim hello-option neighbor-tracking: disabled
Pim hello-option override-interval: 2500 ms
Pim holdtime assert: 180 s
Pim holdtime join-prune: 210 s
Pim require-genid: disabled
Pim silent: disabled
Pim timer dr-switch-delay: disabled
Pim hello periodic interval: 30 s
Pim join-prune periodic interval: 60 s
Pim triggered-hello-delay: 5 s
Pim version: 2
Pim join-policy: disabled
Pim neighbor-policy: disabled
```

Table 10-38 Description of the **display default-parameter pim-sm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.
Auto-rp listening enable	Whether auto-RP listening is enabled. This parameter is configured by the **auto-rp listening enable** command.
Bsr-policy	Whether the valid address range of the BSR is set. This parameter is configured by the **bsr-policy (IPv4)** command.
C-bsr admin-scope	Whether the BSR administrative domain is configured. This parameter is configured by the **c-bsr admin-scope** command.
C-bsr global	Whether the C-BSR in the global domain is configured. This parameter is configured by the **c-bsr global** command.
C-bsr group	Whether the C-BSR in the BSR administrative domain is configured. This parameter is configured by the **c-bsr group** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
C-bsr hash-length	Global hash mask length of the C-BSR. This parameter is configured by the **c-bsr hash-length (IPv4)** command.
C-bsr holdtime	Waiting time for the BSR to receive the Bootstrap message. This parameter is configured by the **c-bsr holdtime (IPv4)** command.
C-bsr interval	Interval for the BSR to send Bootstrap messages. This parameter is configured by the **c-bsr interval (IPv4)** command.
C-bsr priority	Global priority of the C-BSR. This parameter is configured by the **c-bsr priority (IPv4)** command.
C-rp advertisement-interval	Interval for the C-RP to send Advertisement messages. This parameter is configured by the **c-rp advertisement-interval (IPv4)** command.
C-rp holdtime	Waiting time for the BSR to receive the Advertisement message. This parameter is configured by the **c-rp holdtime (IPv4)** command.
C-rp priority	Global priority of the C-RP. This parameter is configured by the **c-rp priority (IPv4)** command.
Crp-policy	Whether the valid address range of the C-RP and the range of multicast groups that the C-RP serves are set. This parameter is configured by the **crp-policy (IPv4)** command.
Bsm semantic fragmentation	Whether the BSR fragmentation is enabled. This parameter is configured by the **bsm semantic fragmentation (IPv4)** command.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state, in seconds. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment, in milliseconds. This parameter is configured by the **hello-option lan-delay (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Interval for sending Prune Override messages, in milliseconds. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state, in seconds. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state, in seconds. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP, in seconds. This parameter is configured by the **probe-interval (IPv4)** command.
Register-header-checksum	Whether calculating the checksum based on information in Register message header is required. This parameter is configured by the **register-header-checksum** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv4)** command.
Register-suppression-timeout	Time period for holding the register-suppression state, in seconds. This parameter is configured by the **register-suppression-timeout (IPv4)** command.
Source-lifetime	Timeout period of an (S, G) entry, in seconds. This parameter is configured by the **source-lifetime (IPv4)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv4)** command.
Spt-switch-threshold	Whether the threshold of the multicast packet rate that triggers the switch from the RPT to the SPT is configured. This parameter is configured by the **spt-switch-threshold (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv4)** command.
Static-rp	Whether the static RP is configured. This parameter is configured by the **static-rp (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages, in seconds. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages, in seconds. This parameter is configured by the **timer join-prune (IPv4)** command.
Timer spt-switch	Whether the interval for checking whether the multicast packet rate exceeds the threshold before the switchover from RPT to SPT is configured, in seconds. This parameter is configured by the **timer spt-switch (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.
Pim bsr-boundary	Whether the PIM boundary is configured on the interface. This parameter is configured by the **pim bsr-boundary** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state, in seconds. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface, in milliseconds. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim hello-option neighbor-tracking** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim hello-option override-interval	Interval for the interface to send Prune Override messages, in milliseconds. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state, in seconds. This parameter is configured by the **pim holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state, in seconds. This parameter is configured by the **pim holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages, in seconds. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages, in seconds. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages, in seconds. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

 Copyright © Huawei Technologies Co., Ltd.

10.3.20 display default-parameter pim-ssm

Function

The **display default-parameter pim-ssm** command displays default configurations of PIM-SM for SSM.

Format

display default-parameter pim-ssm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-ssm** command displays default configuration of PIM-SM for SSM. Even if the configuration of PIM-SM for SSM is modified, the **display default-parameter pim-ssm** command still displays default parameter settings. Therefore, you can use this command to check which parameters on the device have been modified.

Example

Display default configuration of PIM-SM for SSM.

```
<Huawei> display default-parameter pim-ssm
  PIM View Default Configurations:
  --------------------------------
  Hello-option dr-priority: 1
  Hello-option holdtime: 105 s
  Hello-option lan-delay: 500 ms
  Hello-option neighbor-tracking: disabled
  Hello-option override-interval: 2500 ms
  Holdtime assert: 180 s
  Holdtime join-prune: 210 s
  Probe-interval: 5 s
  Register-header-checksum: disabled
  Register-policy: disabled
  Register-suppression-timeout: 60 s
  Source-lifetime: 210 s
  Source-policy: disabled
  Ssm-policy: disabled
  Hello periodic interval: 30 s
  Join-prune periodic interval: 60 s

  Interface View Default Configurations:
  --------------------------------------
  Pim bfd: disabled
```

 Copyright © Huawei Technologies Co., Ltd.

```
Pim hello-option dr-priority: 1
Pim hello-option holdtime: 105 s
Pim hello-option lan-delay: 500 ms
Pim hello-option neighbor-tracking: disabled
Pim hello-option override-interval: 2500 ms
Pim holdtime assert: 180 s
Pim holdtime join-prune: 210 s
Pim require-genid: disabled
Pim silent: disabled
Pim timer dr-switch-delay: disabled
Pim hello periodic interval: 30 s
Pim join-prune periodic interval: 60 s
Pim triggered-hello-delay: 5 s
Pim version: 2
Pim join-policy: disabled
Pim neighbor-policy: disabled
```

Table 10-39 Description of the **display default-parameter pim-ssm** command output

Item	Description
PIM View Default Configurations	Default configurations in the PIM view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv4)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state, in seconds. This parameter is configured by the **hello-option holdtime (IPv4)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment, in milliseconds. This parameter is configured by the **hello-option lan-delay (IPv4)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv4)** command.
Hello-option override-interval	Interval for sending Prune Override messages, in milliseconds. This parameter is configured by the **hello-option override-interval (IPv4)** command.
Holdtime assert	Time period for holding the Assert state, in seconds. This parameter is configured by the **holdtime assert (IPv4)** command.
Holdtime join-prune	Time period for holding the Join or Prune state, in seconds. This parameter is configured by the **holdtime join-prune (IPv4)** command.
Source-lifetime	Timeout period of an (S, G) entry, in seconds. This parameter is configured by the **source-lifetime (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv4)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv4)** command.
Hello periodic interval	Interval for sending Hello messages, in seconds. This parameter is configured by the **timer hello (IPv4)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages, in seconds. This parameter is configured by the **timer join-prune (IPv4)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bfd	Whether PIM BFD is enabled on the interface. This parameter is configured by the **pim bfd enable** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state, in seconds. This parameter is configured by the **pim hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface, in milliseconds. This parameter is configured by the **pim hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages, in milliseconds. This parameter is configured by the **pim hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state, in seconds. This parameter is configured by the **pim holdtime assert** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state, in seconds. This parameter is configured by the **pim holdtime join-prune** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP, in seconds. This parameter is configured by the **probe-interval (IPv4)** command.
Register-header-checksum	Whether calculating the checksum based on information in Register message header is required. This parameter is configured by the **register-header-checksum** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv4)** command.
Register-suppression-timeout	Time period for holding the register-suppression state, in seconds. This parameter is configured by the **register-suppression-timeout (IPv4)** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages, in seconds. This parameter is configured by the **pim timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages, in seconds. This parameter is configured by the **pim timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages, in seconds. This parameter is configured by the **pim triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim neighbor-policy** command.

10.3.21 display pim bfd session

Function

The **display pim bfd session** command displays the information about PIM BFD sessions.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bfd session statistics**

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bfd session** [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. The *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-
statistics	Displays PIM BFD statistics.	-
interface *interface-type interface-number*	Specifies an interface to be displayed. *interface-type interface-number* specifies the type and number of the interface.	-
neighbor *neighbor-address*	Specifies the IP address of a PIM neighbor to be displayed.	The address is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim bfd session** command output helps you locate communication faults between neighbors.

Example

Display PIM BFD sessions on GE 0/0/1 in the public network instance.

```
<Huawei> display pim bfd session interface gigabitethernet 0/0/1
 VPN-Instance: public net

 GigabitEthernet0/0/1 (12.1.1.2): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 12.1.1.1        1000      1000      3        8192/8192   Up
```

Display PIM BFD sessions on GE 0/0/1 in the public network instance when the router is not enabled with global BFD.

```
<Huawei> display pim bfd session interface gigabitethernet 0/0/1
 VPN-Instance: public net

 GigabitEthernet0/0/1 (12.1.1.2): Total 1 BFD session Created

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 12.1.1.1        --        --        --       0/0      BFD global disable
```

Display the statistics of a PIM BFD session.

```
<Huawei> display pim bfd session statistics
 VPN-Instance: public net
  Total 1 PIM BFD session in this instance.

   Total 1 PIM BFD session up.
   Total 0 PIM BFD session down.
```

Display information about PIM BFD sessions of the public network instance neighbor 10.1.2.3.

```
<Huawei> display pim bfd session neighbor 10.1.2.3
 VPN-Instance: public net

 GigabitEthernet0/0/1 (12.1.1.2)

 Neighbor        ActTx(ms) ActRx(ms) ActMulti Local/Remote State
 12.1.1.1        1000      1000      3        8192/8192   Up
```

Table 10-40 Description of the **display pim bfd session** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which PIM BFD session information belongs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GigabitEthernet0/0/1 (12.1.1.2)	Indicates the PIM interface name (the IP address).
Neighbor	Indicates the IP address of a PIM neighbor.
ActTx (ms)	Indicates the actual minimum transmission interval, in milliseconds.
ActRx (ms)	Indicates the actual minimum receiving interval, in milliseconds.
ActMulti	Indicates the actual local detection multiple.
Local/Remote	Indicates the local and remote discriminators.
State	Indicates the status of the PIM BFD session. ● Up: indicates that the BFD session is set up successfully and detection packets are periodically exchanged. ● Init: indicates that the local end can communicate with the remote end and wants the session status to be Up. ● BFD global disable: indicates that BFD is globally disabled. ● Detect down: indicates that no BFD packets are not received when the detection time expires. ● Neighbour down: indicates that the packets with the State field being Down are received from neighbors.
Total 1 PIM BFD session in this instance	Indicates the total number of PIM BFD sessions in a public network instance or a VPN instance.
Total 1 PIM BFD session up	Indicates the number of PIM BFD sessions in the Up state in a public network instance or a VPN instance.
Total 0 PIM BFD session down	Indicates the number of PIM BFD sessions in the Down state in a public network instance or a VPN instance, that is, all PIM BFD sessions except the PIM BFD sessions in the Up state.

10.3.22 display pim bsr-info

Function

The **display pim bsr-info** command displays the BSRs in a PIM-SM domain.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **bsr-info**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command applies to the PIM-SM domain where the RP is dynamically elected among BSRs. You can run this command on any router in the domain to view the BSR information.

- If the current router is configured with the C-BSR, the command output includes information about the elected BSR and locally configured C-BSR.
- If the current router is not configured with the C-BSR, the command output includes information about the elected BSR only.

Precautions

When the **display pim bsr-info** command is used, only information about the public network instance is displayed if the **vpn-instance** or **all-instance** is not specified.

This command has output only after C-BSRs have been configured in a PIM-SM domain.

Example

Display information about the BSR in the PIM-SM domain of the current public network instance. If the router is not configured with C-BSR, only information about the elected BSR is displayed.

```
<Huawei> display pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 10.1.2.2
     Priority: 0
     Hash mask length: 30
     State: Accept Preferred
     Scope: Not scoped
```

```
    Uptime: 00:01:46
    Expires: 00:02:02
    C-RP Count: 1
```

Display information about BSR in the current PIM-SM of the current public network instance.

If the router is configured with C-BSR, information about the elected BSR and C-BSR is displayed.

```
<Huawei> display pim bsr-info
 VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: 10.1.2.2
    Priority: 0
    Hash mask length: 30
    State: Elected
    Scope: Not scoped
    Uptime: 00:10:42
    Next BSR message scheduled at: 00:00:31
    C-RP Count: 1
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: 10.1.2.2
    Priority: 0
    Hash mask length: 30
    State: Elected
    Scope: Not scoped
    Wait to be BSR: 0
```

Table 10-41 Description of the **display pim bsr-info** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which BSR information belongs.
Elected AdminScoped BSR Count	Indicates the number of elected AdminScoped BSRs.
Elected BSR Address	Indicates the address of the elected BSR. **NOTE** If stably running devices in the same BSR domain display different values in the **Elected BSR Address** field, the elected BSR is incorrect. Contact technical support personnel to troubleshoot faults.
Priority	Indicates the priority of the BSR. By default, the value is 0.
Hash mask length	Indicates the mask length in the RP hash calculation.
State	Indicates the status of the BSR.
Scope	Indicates the range of multicast addresses in the administrative scope when the BSR is an AdminScoped BSR. Not scoped indicates that the BSR is not an AdminScoped BSR.

Item	Description
Uptime	Indicates the period during which the BSR exists.
Expires	Indicates the remaining time of the BSR.
C-RP Count	Indicates the number of RPs learned through the BSR.
Next BSR message scheduled at	Indicates the period after which the next BSR message is sent. BSR messages are sent only when the timer maintained by the elected BSR times out.
Candidate AdminScoped BSR Count	Indicates the number of AdminScoped C-BSRs.
Candidate BSR Address	Indicates the address of the C-BSR.
Wait to be BSR	Indicates whether the current C-BSR is valid. The values are as follows: ● 0: indicates that the current C-BSR is valid. The current C-BSR takes part in the BSR election. ● 1: indicates that the current C-BSR is invalid. The current C-BSR does not take part in the BSR election. When the number of C-BSRs configured on the router exceeds the threshold, the value is 1.

Related Topics

10.3.5 c-bsr (IPv4)
10.3.13 c-rp (IPv4)

10.3.23 display pim claimed-route

Function

The **display pim claimed-route** command displays the unicast routing information used by PIM.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **claimed-route** [*source-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-
source-address	Specifies the multicast source address.	The address is in decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display pim claimed-route** command is used to view unicast routes used by PIM, such as RPF neighbors, interfaces, route types, and route selection policies.

Configuration Impact

Differences between the **display pim claimed-route** and **display multicast rpf-info** commands are as follows:

- The **display multicast rpf-info** command is used to check information about RPF neighbors, RPF interfaces, or whether there is a route to a specified source address.
- The **display pim claimed-route** command is used to check information about unicast routes used by multicast routing and entries of these routes.

Example

Display the unicast routing information used by PIM.

```
<Huawei> display pim claimed-route
 VPN-Instance: public net
 multicast load-splitting rule: source-group
 RPF information about: 10.1.0.0 in PIM-SM routing table
     RPF interface: GigabitEthernet2/0/0, RPF neighbor: 10.1.2.2
     Referenced route/mask: 10.1.0.0/24
     Referenced route type: igp
     RPF-route selecting rule: preference-preferred
     The (S, G) or (*, G) list dependent on this route entry
     (10.1.0.1, 225.0.0.1)
```

Table 10-42 Description of the **display pim claimed-route** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which the unicast routing information corresponds.
multicast load-splitting rule	Indicates the way in which multi-cast loads are split. The following policies apply: • group: multicast group-based load splitting • source: multicast source-based load splitting • source-group: multicast source and group-based load splitting This parameter is configured by the **multicast load-splitting** command.
RPF information about: 10.1.0.0 in PIM-SM routing table	Indicates the RPF routing information with the source address of 10.1.0.0 in the PIM-SM routing table
RPF interface	Indicates the RPF interface.
RPF neighbor	Indicates the RPF neighbor.
Referenced route/mask	Indicates the referenced route/mask.
Referenced route type	Indicates the type of route.
RPF-route selecting rule	Indicates the preferred rule for selecting the RPF-route.
The (S,G) or (*,G) list dependent on this route entry	Indicates the list of multicast entries based on RPF routes.

Related Topics

10.7.13 display multicast rpf-info

10.3.24 display pim control-message counters

Function

The **display pim control-message counters** command displays the number of sent, received, and invalid PIM control messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters message-type** { **probe** | **register** | **register-stop** | **crp** }

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-
message-type	Indicates a PIM control message type.	-
probe	Indicates the Probe message.	-
register	Indicates the Register message.	-
register-stop	Indicates the Register-stop message.	-
crp	Indicates the C-RP message.	-
assert	Indicates the Assert message.	-
graft	Indicates the Graft message.	-
graft-ack	Indicates the Graft-ack message.	-
hello	Indicates the Hello message.	-
join-prune	Indicates the Join/Prune message.	-
state-refresh	Indicates the State-Refresh message.	-
bsr	Indicates the BSR message.	-
interface *interface-type interface-number*	Indicates the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When multicast data messages cannot be forwarded on a PIM network, run the **display pim control-message counters** command to view statistics on protocol messages. The command output helps you locate faults.

When you run the **display pim control-message counters** command:

- If you specify **interface** *interface-type interface-number*, you can view the number of various PIM control messages that were sent and received on the interface only.
- If you specify **message-type**, you can view the number of PIM control messages of this type sent and received on all interfaces of the router.

Example

Display the statistics about sent, received, and invalid PIM control messages in the public network instance.

```
<Huawei> display pim control-message counters
 VPN-Instance: public net
 Register* - Register Anycast-RP, Probe* - Probe Anycast-RP
 ----------------------------------------------------------------------------
 PIM global control-message counters:
 Message Type     Received         Sent             Invalid          Filtered
 Register         51               0                0                0
 Register-Stop    0                48               0                0
 Probe            44               0                0                0
 C-RP             0                0                0                0
 Register*        0                0                0                0
 Probe*           0                0                0                0

 PIM control-message counters for interface: GigabitEthernet1/0/1
 Message Type     Received         Sent             Invalid          Filtered
 Assert           0                6                0                0
 Graft            0                0                0                0
 Graft-Ack        0                0                0                0
 Hello            34496            34495            0                0
 Join-prune       26171            90               0                0
 State-Refresh    0                0                0                0
 BSR              0                0                0                0

 PIM control-message counters for interface: GigabitEthernet1/0/2
 Message Type     Received         Sent             Invalid          Filtered
 Assert           0                0                0                0
 Graft            0                0                0                0
 Graft-Ack        0                0                0                0
 Hello            34491            34495            0                0
 Join-prune       0                41               0                0
 State-Refresh    0                0                0                0
 BSR              0                0                0                0
```

Display statistics about sent, received, invalid PIM control messages on GE1/0/0 in the public network instance.

```
<Huawei> display pim control-message counters interface GigabitEthernet 1/0/0
 VPN-Instance: public net
 PIM control-message counters for interface: GigabitEthernet1/0/0
 Message Type     Received         Sent             Invalid      Filtered
 Assert           0                0                0            0
 Graft            0                0                0            0
 Graft-Ack        0                0                0            0
 Hello            328              331              0            0
 Join-prune       2                0                0            0
```

```
State-Refresh    0            0            0          0
BSR           9778            0            0          0
```

Table 10-43 Description of the **display pim control-message counters** command output

Item	Description
VPN-Instance	VPN instance to which the statistics of PIM messages belong.
PIM global control-message counters	Number of PIM control messages in the public network.
PIM control-message counters for interface	Name of the interface where statistics about PIM control messages are collected.
Message Type	Type of the control messages.
Received	Number of control messages received by the interface.
Sent	Number of control messages sent by the interface.
Invalid	Number of invalid control messages.
Filtered	Number of control messages filtered out by the interface.
Register	Statistics about Register messages.
Register-Stop	Statistics about Register-Stop messages.
Probe	Statistics about Probe messages.
C-RP	Statistics about CRP messages.
Register*	Statistics about Register messages for anycast RP.
Probe*	Statistics about Probe messages for anycast RP.
Assert	Statistics about Assert messages.
Graft	Statistics about Graft messages.
Graft-Ack	Statistics about Graft-Ack messages.
Hello	Statistics about Hello messages.
Join-prune	Statistics about Join/Prune messages.
State-Refresh	Statistics about State-Refresh messages.
BSR	Statistics about Bootstrap messages.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.74 reset pim control-message counters

10.3.25 display pim grafts

Function

The **display pim grafts** command displays the information about unacknowledged PIM-DM Graft messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **grafts**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Specifies all the instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In PIM-DM, after sending the Graft message, the router needs to wait to receive the Graft-Ack message from the upstream device. You can run the **display pim grafts** command to view the information about the PIM-DM Graft messages sent but unacknowledged.

Example

Display the unacknowledged PIM-DM graft messages in the public network instance.

```
<Huawei> display pim grafts
VPN-Instance: public net
Source          Group          Expire   RetransmitIn
10.0.5.200       226.3.3.3      00:02:52 00:00:02
```

Table 10-44 Description of the **display pim grafts** command output

Item	Description
VPN-Instance	Indicates the VPN instance to which the Graft messages belong.
Source	Indicates the multicast source address.
Group	Indicates the multicast group address.
Expire	Indicates the timeout period of an (S, G) entry.
RetransmitIn	Indicates the waiting period before the next Graft message is received.

10.3.26 display pim interface

Function

The **display pim interface** command displays PIM information on an interface.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Specifies all the instances.	-
interface-type interface-number	Specifies the type and number of an interface.	-
up	Displays PIM information on interfaces in Up state.	-
down	Displays PIM information on interfaces in Down state.	-
verbose	Displays detailed information about a PIM interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An interface with PIM enabled is called a PIM interface. The **display pim interface** command is used to display information about PIM interfaces, including the PIM state, number of PIM neighbors, interval at which Hello messages are sent, DR priority, and DR address.

When the **display pim interface** command is used, the following situations occur:

- If *interface-type interface-number* is specified, the information about various PIM state parameters on the interface is displayed.
- If *interface-type interface-number* is not specified, the information about the state parameters of all the PIM interfaces is displayed.
- If **up** is set in the command, the information about the parameters of the PIM interfaces in the Up state is displayed.
- If **down** is set in the command, the information about the parameters of the PIM interfaces in the Down state is displayed.

Example

Display information about all the PIM interfaces in the public network instance.

```
<Huawei> display pim interface
 VPN-Instance: public net
 Interface       State   NbrCnt   HelloInt   DR-Pri     DR-Address
 GE1/0/0          up      1        30         1          10.1.1.2
 GE2/0/0          up      0        30         1          10.1.2.2    (local)
 Loopback0         up      0        30         1          10.1.3.2    (local)
```

Table 10-45 Description of the **display pim interface** command output

Item	Description
VPN-Instance	VPN instance to which the PIM interface belongs.
Interface	Name of the PIM interface.
State	Status of the PIM interface, Up or Down.
NbrCnt	Number of PIM neighbors on the interface.
HelloInt	Interval for sending Hello messages, in seconds.
DR-Pri	DR priority.
DR-Address	DR address.

 Copyright © Huawei Technologies Co., Ltd.

Display detailed information about PIM on GE1/0/0 of the public network instance.

```
<Huawei> display pim interface gigabitethernet 1/0/0 verbose
 VPN-Instance: public net
 Interface: GigabitEthernet1/0/0, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0XF5712241
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: enabled
     PIM BFD min-tx-interval: 1000 ms
     PIM BFD min-rx-interval: 1000 ms
     PIM BFD detect-multiplier: 3
     PIM dr-switch-delay timer : 20 s
     Number of routers on link not using DR priority: 0
     Number of routers on link not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 2
     ACL of PIM neighbor policy: myacl
     ACL of PIM ASM join policy: 2000
     ACL of PIM SSM join policy: -
     ACL of PIM join policy: -
```

Table 10-46 Description of the **display pim interface verbose** command output

Item	Description
VPN-Instance	VPN instance to which the PIM interface belongs.
Interface	Name and IP address of the PIM interface.
PIM version	PIM version enabled on the interface.
PIM mode	PIM mode used on the interface.
PIM state	Status of the PIM interface, Up or Down.
PIM DR	DR address on the interface.
PIM DR Priority (configured)	DR priority configured on the interface.
PIM neighbor count	Number of PIM neighbors on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PIM hello interval	Interval for sending PIM Hello messages, in seconds.
PIM LAN delay (negotiated)	Negotiated delay for transmitting packets on the interface, in milliseconds.
PIM LAN delay (configured)	Configured delay for transmitting packets on the interface, in milliseconds.
PIM hello override interval (negotiated)	Negotiated override interval on the interface, in milliseconds.
PIM hello override interval (configured)	Configured override interval on the interface, in milliseconds.
PIM Silent	Whether the PIM Silent function is enabled on the interface.
PIM neighbor tracking (negotiated)	Whether the PIM neighbor tracking function is enabled on the interface after negotiation.
PIM neighbor tracking (configured)	Whether the PIM neighbor tracking function is configured on the interface.
PIM generation ID	Generation ID option on the interface.
PIM require-GenID	Whether the function that rejects the Hello messages without the Generation ID option is enabled.
PIM hello hold interval	Interval during which the receiver of the Hello message to keep its neighbor reachable, in seconds.
PIM assert hold interval	Interval for sending Assert messages, in seconds.
PIM triggered hello delay	Maximum random delay for triggering Hello messages, in seconds.
PIM J/P interval	Interval at which the interface sends Join/Prune messages, in seconds.
PIM J/P hold interval	Period for holding the Join/Prune status on the interface, in seconds.
PIM BSR domain border	Whether the BSR domain boundary is configured on the interface.
PIM BFD	Whether PIM BFD is enabled.
PIM BFD min-tx-interval	Minimum interval for sending BFD packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PIM BFD min-rx-interval	Minimum interval for receiving BFD packets.
PIM BFD detect-multiplier	PIM BFD detection multiplier.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of routers that do not use DR priority in all the network segments connected to the interface.
Number of routers on link not using LAN delay	Number of routers that do not use LAN delay in all the network segments connected to the interface.
Number of routers on link not using neighbor tracking	Indicates the number of router that are not enabled with the neighbor tracing function in the network segment where the interface resides.
ACL of PIM neighbor policy	Neighbor filtering policy configured on the interface.
ACL of PIM ASM join policy	ASM Join information filtering policy configured on the interface.
ACL of PIM SSM join policy	SSM Join information filtering policy configured on the interface.
ACL of PIM join policy	Join information filtering policy configured on the interface.

10.3.27 display pim invalid-packet

Function

The **display pim invalid-packet** command displays statistics about invalid PIM messages received by a device and details of these messages.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** }] *

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet message-type** { **crp** | **register** | **register-stop** }

display pim invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid PIM messages received in a specified VPN instance. The *vpn-instance-name* parameter specifies the VPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays statistics about invalid PIM messages received in all VPN instances.	-
interface *interface-type interface-number*	Specifies the type and number of an interface on the router.	-
message-type	Displays statistics about invalid PIM messages of a specific type.	-
assert	Displays statistics about invalid Assert messages.	-
bsr	Displays statistics about invalid BSR messages.	-
hello	Displays statistics about invalid Hello messages.	-
join-prune	Displays statistics about invalid Join/Prune messages.	-
graft	Displays statistics about invalid Graft messages.	-
graft-ack	Displays statistics about invalid Graft-Ack messages.	-
state-refresh	Displays statistics about invalid State-Refresh messages.	-
crp	Displays statistics about invalid C-RP messages.	-
register	Displays statistics about invalid Register messages.	-
register-stop	Displays statistics about invalid Register-Stop messages.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
packet-number	Displays details about a specified number of invalid PIM messages recently received.	The value is an integer that ranges from 1 to 100. By default, details of all the invalid PIM messages currently stored are displayed.
verbose	Displays details of invalid PIM messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device fails to create PIM entries, you can run the **display pim invalid-packet** command first to check whether the device has received invalid PIM messages. If the command output displays counters of invalid PIM messages, run the **display pim invalid-packet** [*packet-number*] **verbose** command to view details of invalid PIM messages for fault location.

You can run the following commands to view information about specific invalid PIM messages:

- Run the **display pim invalid-packet interface** *interface-type interface-number* command to view statistics about invalid PIM messages received by a specified interface.
- Run the **display pim invalid-packet** *packet-number* **verbose** command to view details of invalid PIM messages recently received. Currently, details of a maximum of 100 invalid PIM messages can be displayed.

Example

Display statistics about invalid PIM messages received in the public network instance.

```
<Huawei> display pim invalid-packet

            Statistics of invalid packets for public net:
-----------------------------------------------------------------------
PIM General invalid packet:
Invalid PIM Version     : 0          Invalid PIM Type        : 0
Fault Length            : 0          Bad Checksum            : 0

PIM Register invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0

AnycastRP Register invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
```

```
Invalid Dest Addr       : 0

PIM Register-Stop invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0          IP Source not RP        : 0

PIM CRP invalid packet:
Invalid Dest Addr       : 0          Invalid CRP Addr        : 0
Fault Length            : 0          CRP Adv Fault Length    : 0
Invalid Multicast Group : 0

PIM Assert invalid packet:
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0
Invalid Multicast Source: 0          Invalid Multicast Group : 0

PIM BSR invalid packet:
Bad Payload             : 0          Fault Length            : 0
Bad Scope Mask          : 0          Invalid Multicast Group : 0
Not CBSR But BSR        : 0          Invalid BSR Addr        : 0
Fault Hash Length       : 0          Invalid IP Source Addr  : 0

PIM Hello invalid packet:
Invalid Addr List       : 0          Fault Length            : 0
Bad Holdtime Length     : 0          Bad LanPruneDelay Length: 0
Bad DrPriority Length   : 0          Bad GenID Length        : 0
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0

PIM Join/Prune invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Invalid Dest Addr       : 0          Fault Length            : 0

PIM Graft invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Fault Length            : 0

PIM Graft-Ack invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Fault Length            : 0

PIM State Refresh invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Originator Addr : 0          Fault Length            : 0
------------------------------------------------------------------
```

Table 10-47 Description of the **display pim invalid-packet** command output

Item	Description
Statistics of invalid packets for public net	VPN instance in which statistics about invalid PIM messages need to be displayed.
PIM General invalid packet	General invalid PIM messages.
Invalid PIM Version	Messages with invalid PIM versions.
Invalid PIM Type	Messages with invalid PIM message types.
Fault Length	Messages of invalid lengths.
Bad Checksum	Messages with invalid checksum.
PIM Register invalid packet	Invalid PIM Register messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Invalid Multicast Source	Messages with invalid multicast source addresses.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Invalid Dest Addr	Messages with invalid destination addresses.
AnycastRP Register invalid packet	Statistics about invalid Register messages in the anycast-RP scenario.
PIM Register-Stop invalid packet	Invalid PIM Register-Stop messages.
IP Source not RP	Messages whose source addresses are not the RP address.
PIM CRP invalid packet	Invalid PIM C-RP messages.
Invalid CRP Addr	Messages with invalid C-RP addresses.
CRP Adv Fault Length	Messages whose CRP Adv fields are of invalid lengths.
PIM Assert invalid packet	Invalid PIM Assert messages.
Invalid IP Source Addr	Indicates messages with invalid source addresses.
PIM BSR invalid packet	Invalid PIM BSR messages.
Bad Payload	Messages with invalid payloads.
Bad Scope Mask	Messages with invalid scope masks.
Not CBSR But BSR	BSR messages received on interfaces that do not act as a C-BSR.
Invalid BSR Addr	Messages with invalid BSR addresses.
Fault Hash Length	Messages with hash mask fields of invalid lengths.
PIM Hello invalid packet	Indicates invalid PIM Hello messages.
Invalid Addr List	Indicates messages with invalid address lists.
Bad Holdtime Length	Messages with Holdtime fields of invalid lengths.
Bad LanPruneDelay Length	Messages with LanPruneDelay fields of invalid lengths.
Bad DrPriority Length	Messages with DrPriority fields of invalid lengths.
Bad GenID Length	Messages with GenerationID fields of invalid lengths.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PIM Join/Prune invalid packet	Invalid PIM Join/Prune messages.
Invalid Up Neighbor	Messages with invalid upstream neighbors.
PIM Graft invalid packet	Invalid PIM Graft messages.
PIM Graft-Ack invalid packet	Invalid PIM Graft-Ack messages.
PIM State Refresh invalid packet	Invalid PIM State-Refresh messages.
Invalid Originator Addr	Messages with invalid Originator address.

Display details of one invalid PIM message recently received in the public network instance.

```
<Huawei> display pim invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Interface           :  GigabitEthernet1/0/0
Time                :  2010-6-1 20:04:35 UTC-08:00
Message Length      :  26
Invalid Type        :  Invalid Multicast Source
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00
0010: 00 00 80 00 00 64 00 00 00 00
-----------------------------------------------------
```

Table 10-48 Description of the **display pim invalid-packet 1 verbose** command output

Item	Description
Detailed information of invalid packets	Details of an invalid PIM message.
Packet information (Index 1)	Sequence number of the invalid PIM message (numbered in the opposite order the message is received. For example, the index of the last received message is 1, the index of the penultimate message is 2, and so on).
Interface	Interface that received the invalid PIM message.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Time	Time when the invalid SPT switch message was received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST The format UTC±HH:MM indicates that a time zone has been configured using the **clock timezone** command; DST indicates that the daylight saving time has been configured using **clock daylight-saving-time** command.
Message Length	Length of the invalid PIM message.
Invalid Type	Type of the invalid PIM message.
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00 0010: 00 00 80 00 00 64 00 00 00 00	Contents of the invalid PIM message.

Related Topics

10.7.23 multicast invalid-packet

10.3.28 display pim neighbor

Function

The **display pim neighbor** command displays information about PIM neighbors.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **neighbor** [*neighbor-address* | **interface** *interface-type interface-number* | **verbose**] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Specifies all the instances.	-
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
neighbor-address	Specifies the IP address of a PIM neighbor.	The address is in dotted decimal notation.
verbose	Displays detailed information about PIM neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim neighbor** command displays information about PIM neighbors, including the number of neighbors, DR priority, and BFD session status. You can adjust PIM neighbor relationships based on the command output.

When you run the **display pim neighbor** command:

- If you specify **interface** *interface-type interface-number*, the command displays information about PIM neighbors connected to the specified interface.
- If you do not specify **interface** *interface-type interface-number*, the command displays information about all PIM neighbors attached to the router.

Example

Display information about all PIM neighbors in the public network instance.

```
<Huawei> display pim neighbor
 VPN-Instance: public net
 Total Number of Neighbors = 2

 Neighbor        Interface     Uptime       Expires      Dr-Priority  BFD-Session
```

```
10.1.1.2        GE1/0/0      02:50:49    00:01:31    1          Y
10.1.2.2        GE2/0/0      02:49:39    00:01:42    1          Y
```

Table 10-49 Description of the **display pim neighbor** command output

Item	Description
VPN-Instance	VPN instance to which PIM neighbors belong.
Total Number of Neighbors	Total number of PIM neighbors on an interface.
Neighbor	IP Address of a PIM neighbor.
Interface	Interface connected to a PIM neighbor.
Uptime	Time elapsed since a PIM neighbor relationship is set up.
Expires	Amount of time left before a PIM relationship times out.
Dr-Priority	DR priority of a PIM neighbor.
BFD-Session	Whether the BFD session has been set up with a neighbor.

Display detailed information about the PIM neighbor with IP address 10.1.1.2 in the public network instance.

```
<Huawei> display pim neighbor 192.168.11.1 verbose
 VPN-Instance: public net
 Neighbor: 192.168.11.1
     Interface: Vlanif11
     Uptime: 04:56:41
     Expiry time: 00:01:44
     DR Priority: 1
     Generation ID: 0XD287B917
     Holdtime: 105 s
     LAN delay: 500 ms
     Override interval: 2500 ms
     Neighbor tracking: Disabled
     PIM BFD-Session: Y
     PIM BFD-Session min-tx-interval: 1000 ms
     PIM BFD-Session min-rx-interval: 1000 ms
     PIM BFD-Session detect-multiplier: 3
```

Table 10-50 Description of the **display pim neighbor verbose** command output

Item	Description
Expiry time	Amount of time left before a PIM relationship times out.
Generation ID	PIM neighbor status random value.
Holdtime	Keepalive period of the PIM neighbor.

Item	Description
LAN delay	Delay in transmitting Prune messages.
Override interval	Override interval for a prune action.
Neighbor tracking	Whether the neighbor tracking function is enabled.
PIM BFD-Session	Whether the BFD session is set up.
PIM BFD-Session min-tx-interval	Minimum interval at which PIM BFD packets are sent.
PIM BFD-Session min-rx-interval	Minimum interval at which PIM BFD packets are received.
PIM BFD-Session detect-multipler	PIM BFD detection multiplier.

10.3.29 display pim routing-table

Function

The **display pim routing-table** command displays the PIM routing table.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table brief** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **incoming-interface** { *interface-type interface-number* | **mcast-extranet** | **register** }] *

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask-length* | *group-mask* }] | *source-address* [**mask** { *source-mask-length* | *source-mask* }] | **extranet** { **source-vpn-instance** { *vpn-instance-name* | **all** | **public** } | **receive-vpn-instance** { *vpn-instance-name* | **all** } } | **incoming-interface** { *interface-type interface-number* | **register** | **mcast-extranet** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | **vpn-instance** *vpn-instance-name* | **mode** { **dm** | **sm** | **ssm** } | **flags** *flag-value* | **fsm**] * [**outgoing-interface-number** [*number*]] [**rpf-vector** [*vector-address*]]

NOTE

If you specify the **register** keyword before **mode**, the value of **mode** can only be **sm**.

After the PIM mode is set to **dm** or **ssm**, the **register** keyword cannot be specified in the command.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays PIM routing entries in a specified VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays PIM routing entries in all the instances.	-
group-address	Displays the PIM routing entry of a specified group.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast source address or group address.	-
group-mask	Specifies the group address mask.	The address is in dotted decimal notation.
group-mask-length	Specifies the length of the group address mask.	The value is an integer that ranges from 4 to 32.
source-address	Displays the PIM routing entry of a specified multicast source.	The source address is in dotted decimal notation.
source-mask	Specifies the multicast source IP address mask.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the length of the source address mask.	The value is an integer that ranges from 0 to 32.
extranet	Displays multicast extranet routing entries.	-
source-vpn-instance *vpn-instance-name*	Indicates the source VPN instance. *vpn-instance-name* specifies the name of the source VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Indicates all instances.	-
public	Indicates the public network instance.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
receive-vpn-instance *vpn-instance-name*	Indicates the receiver VPN instance. *vpn-instance-name* specifies the name of the receiver VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface	Displays the PIM routing entries with a specified interface as the upstream interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface.	-
mcast-extranet	Indicates that the upstream interface is an extranet interface.	-
outgoing-interface	Displays the PIM routing entries with a specified interface as the downstream interface.	-
include	Displays the PIM routing entries with the downstream interface list containing a specified interface.	-
exclude	Displays the PIM routing entries with the downstream interface list not containing a specified interface.	-
match	Displays the PIM routing entries with the downstream interface list containing only the specified interface.	-
none	Displays the PIM routing entries with an empty downstream interface list.	-
mode	Specifies the PIM operation mode.	-
dm	Displays PIM-DM routing entries.	-
sm	Displays PIM-SM routing entries.	-
ssm	Displays PIM-SSM routing entries.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
flags *flag-value*	Displays PIM-SSM routing entries with the specified flag. The *flag-value* parameter is the type flag of entries.	-
fsm	Displays the details of FSM states.	-
outgoing-interface-number	Displays the number of downstream interfaces of PIM routing entries.	-
number	Specifies the number of the downstream interfaces to be displayed.	The value is an integer that ranges from 0 to 2048.
rpf-vector *vector-address*	Displays detailed information about Reverse Path Forwarding (RPF) vectors. *vector-address* specifies the vector address.	The address mask is in dotted decimal notation.
brief	Displays only the upstream interface names and the number of downstream interfaces in PIM routing entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to:

- Check whether PIM has been configured successfully on the network.
- Check the inbound interfaces, outbound interfaces, flags, and other information in the routing entries to identify failure points when forwarding errors occur on the PIM network.

The PIM routing table includes both (*, G) and (S, G) entries. (*, G) entries are used to set up a rendezvous point tree (RPT), and (S, G) entries are used to set up a shortest path tree (SPT).

Table 10-51 lists the values of the **flags** *flag-value* parameter.

Table 10-51 Values of the flag-value parameter

Item	Description
2msdp	The RP received a Register message recently and learned the (S, G) entry. The RP will notify MSDP of the (S, G) entry in the next SA message.
act	Multicast routing entries that have matched received data.
del	Multicast routing entries to be deleted.
exprune	Multicast routing entries pruned from the RPT, with no receiver interested in the data from the source.
ext	Multicast routing entries that contain downstream interfaces provided by other multicast routing protocols.
loc	Multicast routing entries the router directly connected to the network segment of the multicast source.
msdp	Multicast routing entries learned from recently received MSDP SA messages.
niif	Multicast routing entries with unknown upstream interfaces.
nonbr	Multicast routing entries in which the upstream neighbor address (link-local address) towards the RP or the source is not found.
none	Multicast routing entries without any flag.
rpt	Multicast routing entries that are on the RPT but do not use the RPT data.
sg_rcvr	The router has receivers of the source specified in the (S, G) entry, and PIM is the owner of the downstream interfaces.
sgjoin	The router has receivers of the source specified in the (S, G) entry, but PIM is not the owner of the downstream interfaces.
spt	Multicast routing entries on the shortest path tree (SPT).
swt	Multicast routing entries during the SPT switchover.
upchg	A route change has occurred. The current entry is using the original upstream interface to forward data and waiting for data received from a new interface.
wc	(*, G) entry.

Example

Display the PIM routing table of the public network instance.

```
<Huawei> display pim routing-table
 VPN-Instance: public net
 Total 0 (*, G) entry; 1 (S, G) entry

 (172.16.0.12, 227.0.0.1)
```

```
RP: 10.2.2.2
Protocol: pim-sm, Flag: SPT LOC ACT
UpTime: 02:54:43
Upstream interface: GigabitEthernet1/0/0
    Upstream neighbor: NULL
    RPF prime neighbor: NULL
Downstream interface(s) information:
Total number of downstreams: 1
    1: GigabitEthernet2/0/0
        Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 10-52 Description of the **display pim routing-table** command output

Item	Description
VPN-Instance	VPN instance to which PIM routing information belongs.
Total 0 (*, G) entry; 1 (S, G) entry	Total number of (S, G) and (*, G) entries in the PIM routing table.
(172.16.0.12, 227.0.0.1)	(S, G) entry in the PIM routing table.
RP	RP address.
Protocol	PIM protocol type, which can be PIM-DM, PIM-SM or PIM-SSM.
Flag	Flag of PIM (S, G) or (*, G) entry.
UpTime	Amount of time an interface has been Up.
Upstream interface	Upstream interface in an (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of an (S, G) or (*, G) entry.
RPF prime neighbor	RPF neighbor of an (S, G) or (*, G) entry. ● For a (*, G) entry, when the local device is an RP, the RPF neighbor in the (*, G) entry is null. ● For an (S, G) entry, when the local device is directly connected to the source, the RPF neighbor in the (S, G) entry is null.
Downstream interface(s) information	Information about the downstream interface, including the following: ● Total number of downstream interfaces ● Name of each downstream interface ● PIM protocol type configured for the downstream interface ● Keepalive period and timeout period of the downstream interface
Total number of downstreams	Number of downstream interfaces.
Expires	Timeout period of an interface.

 Copyright © Huawei Technologies Co., Ltd.

Display the number of the downstream interfaces of PIM routing entries in the public network instance.

```
<Huawei> display pim routing-table outgoing-interface-number
 VPN-Instance: public net
 Total 2 (*, G) entries; 0 (S, G) entry

 (*, 226.1.1.1)
     RP: 10.2.2.2 (local)
     Protocol: pim-sm, Flag: WC EXT
     UpTime: 21:37:28
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 50

 (*, 226.1.2.1)
     RP: 10.2.2.2 (local)
     Protocol: pim-sm, Flag: WC EXT
     UpTime: 21:37:28
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 50
```

Table 10-53 Description of the **display pim routing-table outgoing-interface-number** command output

Item	Description
Total 2 (*, G) entries; 0 (S, G) entry	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
Total number of downstreams	Total number of the downstream interfaces of the (*, G) entries or (S, G) entries.

Display brief information about the PIM routing entries in the public network instance.

```
<Huawei> display pim routing-table brief
  VPN-Instance: public net
 Total 0 (*, G) entry; 6 (S, G) entries

  00001.(10.0.4.100, 225.0.0.1)
       Upstream interface:GigabitEthernet1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00002.(10.0.4.100, 225.0.0.2)
       Upstream interface:GigabitEthernet1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00003.(10.0.4.100, 225.0.0.3)
       Upstream interface:GigabitEthernet1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00004.(10.0.4.100, 225.0.0.4)
       Upstream interface:GigabitEthernet1/0/0
       Number of downstream:1
       Number of receive vrf:0
  00005.(10.0.4.100, 225.0.0.5)
       Upstream interface:GigabitEthernet1/0/0
       Number of downstream:1
       Number of receive vrf:0
```

 Copyright © Huawei Technologies Co., Ltd.

```
00006.(10.0.4.100, 225.0.0.6)
    Upstream interface:GigabitEthernet1/0/0
    Number of downstream:1
    Number of receive vrf:0
```

Table 10-54 Description of the **display pim routing-table brief** command output

Item	Description
Total 0 (*, G) entry; 6 (S, G) entries	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
Upstream interface	Upstream interface in an (S, G) or (*, G) entry.
Number of downstream	Number of downstream interfaces.
Number of receive vrf	Number of receiving VRFs.

Related Topics

10.7.11 display multicast routing-table

10.3.30 display pim rp-info

Function

The **display pim rp-info** command displays information about the RP for a multicast group.

Format

display pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **rp-info** [*group-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Specifies all the instances.	-
group-address	Displays the information about the RP for a specified multicast group.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view information about the RP for a multicast group.

Configuration Impact

The command output includes information about the RP discovered through the BSR mechanism, static RP, and auto-RP.

If *group-address* is not specified, the command displays RP information for all the multicast groups.

Example

Display RP information for all the multicast groups.

```
<Huawei> display pim rp-info
VPN-Instance: public net
PIM-SM BSR RP Number:1
Group/MaskLen: 224.0.0.0/4
    RP: 10.2.2.2 (local)
    Priority: 0
    Uptime: 03:01:36
    Expires: 00:02:29
PIM SM static RP Number:1
    Static RP: 10.1.1.1
```

Table 10-55 Description of the display pim rp-info command output

Item	Description
VPN-Instance	VPN instance to which RP information belongs.
PIM-SM BSR RP Number	Number of PIM-SM BSR RPs.
Group/MaskLen	Multicast group address and mask length.
RP	RP address.
Priority	Priority of the RP.
Uptime	Time elapsed since presence of the RP.
Expires	Amount of time left before the RP times out.
PIM SM static RP Number	Number of static RPs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Static RP	IP address of a static RP.

10.3.31 graceful-restart (IPv4)

Function

The **graceful-restart** command enables PIM GR.

The **undo graceful-restart** command disables PIM GR.

By default, PIM GR is not enabled.

NOTE

Only the AR3200 series routers support PIM GR.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-SM network, after an active/standby switchover is performed on the router equipped with two MPUs, the new active MPU deletes original PIM forwarding entries. Because the active MPU on the router cannot create new PIM forwarding entries in a short time, multicast data transmission is interrupted.

PIM GR enables the router to back up join and prune information in PIM routing entries to the new MPU when an active/standby switchover is performed on the router. This ensures normal multicast data forwarding during restoration of the multicast distribution tree.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

At least one router interface is enabled with PIM-SM so that the **graceful-restart** command takes effect.

Example

Enable PIM GR in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] graceful-restart
```

Related Topics

10.3.32 graceful-restart period (IPv4)

10.3.32 graceful-restart period (IPv4)

Function

The **graceful-restart period** command configures the minimum PIM GR period.

The **undo graceful-restart period** command restores the default minimum PIM GR period.

By default, the minimum PIM GR period is 120 seconds.

NOTE

Only the AR3200 series routers support PIM GR.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	It is an integer that ranges from 90 to 3600 in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **graceful-restart period** command ensures the minimal time for maintaining forwarding entries.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If you run the **graceful-restart period** command multiple times, only the latest configuration takes effect.

Precautions

PIM GR is on the basis of unicast GR; therefore, the minimum PIM GR period should be longer than the corresponding unicast GR period.

The PIM GR period also depends on the complexity of the network topology and increases as the expansion of unicast route capacity and multicast route capacity.

Example

Set the minimum PIM GR period in the public network instance to 150 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] graceful-restart
[Huawei-pim] graceful-restart period 150
```

Related Topics

10.3.31 graceful-restart (IPv4)

10.3.33 hello-option dr-priority (IPv4)

Function

The **hello-option dr-priority** command configures the priority of the router that candidates for the Designated Router (DR).

The **undo hello-option dr-priority** command restores the default priority.

By default, the priority of the router that candidates for the DR is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
priority	Specifies the priority of the router that candidates for the DR. The greater the value, the higher the priority.	The value is an integer ranging from 0 to 4294967295.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM, routers on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IP address. To elect the DR, the routers send the Hello message that contains the priority to each other. The router with the highest priority functions as the DR. If the routers have the same priority, the router with the largest IP address functions as the DR.

If there is at least one router that does not support Hello packets that contain the priority in the network, the DR election is based on the IP address of each router. The router with the largest IP address functions as the DR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **hello-option dr-priority** command has the same function as the **pim hello-option dr-priority** command in the interface view. By default, if the **pim hello-option dr-priority** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the public network instance, configure the DR priority of a router to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option dr-priority 3
```

Related Topics

10.3.51 pim hello-option dr-priority

10.3.34 hello-option holdtime (IPv4)

Function

The **hello-option holdtime** command sets the timeout period for a router to wait to receive Hello messages from its PIM neighbor.

The **undo hello-option holdtime** command restores the default configuration.

By default, the timeout period for a router to wait to receive Hello messages from its PIM neighbor is 105 seconds.

Format

hello-option holdtime *interval*

undo hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which a router waits to receive a Hello message from its PIM neighbor.	The value is an integer ranging from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device considers the neighbor invalid or unreachable.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The timeout period must be greater than the interval for sending Hello messages. You can run the **timer hello** command to set the interval for sending Hello messages.

 Copyright © Huawei Technologies Co., Ltd.

The **hello-option holdtime** command has the same function as the **pim hello-option holdtime** command in the interface view. By default, if the **pim hello-option holdtime** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the public network instance, set the timeout interval to 120 seconds. The timeout interval is the period during which a router waits to receive the Hello message from its PIM neighbor.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option holdtime 120
```

Related Topics

10.3.52 pim hello-option holdtime

10.3.35 hello-option lan-delay (IPv4)

Function

The **hello-option lan-delay** command sets the delay in transmitting Prune message on the shared network segment.

The **undo hello-option lan-delay** command restores the default delay.

By default, the delay in transmitting Prune message on the shared network segment is 500 milliseconds.

Format

hello-option lan-delay *interval*

undo hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting Prune message on the shared network segment.	The value is an integer that ranges from 1 to 32767, in milliseconds (ms).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all routers on the same link are different, the maximum value of these values is used.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current router receives a Prune message from the downstream interface and performs the prune action. If the router receives a Join message from the downstream interface in PPT, the router cancels the prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the delay in transmitting Prune message is too short, the upstream router will stop forwarding multicast packets before the downstream router determines whether to override the Prune action or not. Exercise caution when you run the **hello-option lan-delay** command.

The **hello-option lan-delay** command has the same function as the **pim hello-option lan-delay** command in the interface view. By default, if the **pim hello-option lan-delay** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting Prune message on the shared network segment to 200 ms in public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option lan-delay 200
```

Related Topics

10.3.37 hello-option override-interval (IPv4)

10.3.55 pim hello-option override-interval

10.3.53 pim hello-option lan-delay

 Copyright © Huawei Technologies Co., Ltd.

10.3.36 hello-option neighbor-tracking (IPv4)

Function

The **hello-option neighbor-tracking** command enables the neighbor tracking function.

The **undo hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. The upstream neighbor cannot update neighbor relationships with downstream devices because of Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This command is valid for only PIM-SM.

Neighbor tracking can be implemented only when this function is enabled on all devices on the shared network segment.

The **hello-option neighbor-tracking** command has the same function as the **pim hello-option neighbor-tracking** command in the interface view. By default, if neighbor tracking is not used on an interface, the neighbor tracking configuration in the PIM view takes effect.

Example

In the public network instance, enable the downstream neighbor tracking function.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option neighbor-tracking
```

Related Topics

10.3.54 pim hello-option neighbor-tracking

10.3.37 hello-option override-interval (IPv4)

Function

The **hello-option override-interval** command sets the interval for overriding the prune action in a Hello message.

The **undo hello-option override-interval** command restores the default interval.

By default, the interval for overriding the prune action in a Hello message is 2500 ms.

Format

hello-option override-interval *interval*

undo hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for overriding the prune action in a Hello message.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

PIM view of public network instance or PIM view of VPN instance

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

When the values of **override-interval** on all routers in the same network segment are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the router does not perform the prune action until the PPT times out. If the router receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

The **hello-option override-interval** command has the same function as the **pim hello-option override-interval** command in the interface view. By default, if the **pim hello-option override-interval** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

In the public network instance, set the interval for denying the prune action in a Hello message to 2000 ms.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] hello-option override-interval 2000
```

Related Topics

10.3.35 hello-option lan-delay (IPv4)

10.3.53 pim hello-option lan-delay

10.3.55 pim hello-option override-interval

10.3.38 holdtime assert (IPv4)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local router.

The **undo holdtime assert** command restores the default timeout.

By default, the timeout period for all PIM interfaces to keep the Assert state on the local router is 180 seconds.

Format

holdtime assert *interval*

undo holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the time during which the PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retains the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The **holdtime assert** command has the same function as the **pim holdtime assert** command in the interface view. By default, if the timeout period is not used on an interface, the timeout period configured in the PIM view is used.

Example

In the public network instance, set the interval during which a router keeps the Assert state to 100s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] holdtime assert 100
```

Related Topics

10.3.39 holdtime join-prune (IPv4)

10.3.57 pim holdtime join-prune

10.3.56 pim holdtime assert

10.3.39 holdtime join-prune (IPv4)

Function

The **holdtime join-prune** command sets the holdtime value in Join/Prune messages sent by all PIM interfaces. routers that receive Join/Prune messages set the time during which the downstream interface keeps the Join or Prune state according to holdtime.

The **undo holdtime join-prune** command restores the default value.

By default, the holdtime value in Join/Prune messages sent by all PIM interfaces is 210 seconds.

Format

holdtime join-prune *interval*

undo holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime carried in Join/Prune messages sent by the local router.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the router starts the holdtime timer. After the timeout interval, if the router does not receive subsequent Join/Prune messages from the downstream device, the downstream interface of a multicast group is suppressed from forwarding Join/Prune messages with information about multicast group joining. If Join/Prune messages carry information about multicast group prune, the downstream interface of the multicast group is restored.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

The holdtime of Join/Prune messages must be larger than the interval for sending Join/Prune messages and is generally 3.5 times the interval for sending Join/Prune messages.

The **holdtime join-prune** command has the same function as the **pim holdtime join-prune** command in the interface view. By default, if the holdtime value is not used on an interface, the holdtime value configured in the PIM view is used.

Example

In the public network instance, set the time during which the downstream interface of a router keeps the Join or Prune state to 280 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] holdtime join-prune 280
```

Related Topics

10.3.57 pim holdtime join-prune

10.3.40 join-prune max-packet-length (IPv4)

Function

The **join-prune max-packet-length** command sets the maximum size of each PIM-SM Join/Prune message to be sent.

The **undo join-prune max-packet-length** command restores the default maximum size of each PIM-SM Join/Prune message to be sent.

By default, the maximum length of Join/Prune message sent by PIM-SM is 8100 bytes.

 Copyright © Huawei Technologies Co., Ltd.

Format

join-prune max-packet-length *packet-length*

undo join-prune max-packet-length

Parameters

Parameter	Description	Value
packet-length	Specifies the maximum size of each PIM-SM Join/Prune message to be sent.	The value is an integer ranging from 100 to 8100, in bytes.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has low performance and takes a long time to process a single Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be set to a small value to limit the number of (S, G) entries in each message, relieving the burden on the peer device.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the maximum size specified in the **join-prune max-packet-length** command is greater than the interface MTU, the maximum size of each message to be sent is equal to the interface MTU.

Example

Set the maximum size of each Join/Prune message to be sent to 2100 bytes.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] join-prune max-packet-length 2100
```

 Copyright © Huawei Technologies Co., Ltd.

10.3.41 join-prune periodic-messages queue-size (IPv4)

Function

The **join-prune periodic-messages queue-size** command sets the maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.

The **undo join-prune periodic-messages queue-size** command restores the default maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.

By default, a PIM-SM Join/Prune message that is sent every second contains 1020 entries.

Format

join-prune periodic-messages queue-size *queue-size*

undo join-prune periodic-messages queue-size

Parameters

Parameter	Description	Value
queue-size	Specifies the maximum number of (S, G) entries carried in a PIM-SM Join/Prune message that is sent every second.	The value is an integer ranging from 16 to 4096.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has a low throughput, change the length of a queue for periodically sending messages to a small value to control the number of (S, G) entries. This setting allows the local device to send Join/Prune messages with a small number of (S, G) entries multiple times, preventing packet loss or route flapping.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

 Copyright © Huawei Technologies Co., Ltd.

Example

Allow each PIM-SM Join/Prune message that is sent every second to carry a maximum of 2000 (S, G) entries.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] join-prune periodic-messages queue-size 2000
```

10.3.42 join-prune triggered-message-cache disable (IPv4)

Function

The **join-prune triggered-message-cache disable** command disables the Join/Prune message package function.

The **undo join-prune triggered-message-cache disable** command enables the Join/Prune message package function.

By default, the Join/Prune message package function is enabled.

Format

join-prune triggered-message-cache disable

undo join-prune triggered-message-cache disable

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system performs more efficiently to send a cacheage of PIM Join/Prune messages than to send a large number of individual PIM Join/Prune messages. A device sends PIM Join/Prune messages in cacheages. To disable the cacheage function, run the **join-prune triggered-message-cache disable** command.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the Join/Prune message cacheage function.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] join-prune triggered-message-cache disable
```

10.3.43 local-address (IPv4)

Function

The **local-address** command sets a local address for an Anycast RP.

The **undo local-address** command deletes the local address set for an Anycast RP.

By default, no local address is set for an Anycast RP.

Format

local-address *local-address*

undo local-address

Parameters

Parameter	Description	Value
local-address	Specifies the local address of Anycast RP.	The value is in dotted decimal notation. This address must be a valid unicast IP address and cannot be an address on the network segment 127.0.0.0/8.

Views

Anycast RP view of public network instance or Anycast RP view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IP address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the

destination addresses of the Register message. In such a manner, Anycast RP peers can learn source/group information from each other. This command is used to set a local address for an Anycast RP.

Prerequisites

The local address specified for Anycast RP must be an existing interface IP address.

Precautions

The local address must be different from the Anycast RP address.

NOTE

Setting a Loopback interface address as the local address of the Anycast RP is recommended.

Example

In the public network instance, set the Anycast RP address to 10.10.10.10 and local address of Anycast RP to 10.1.1.1.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] anycast-rp 10.10.10.10
[Huawei-pim-anycast-rp-10.10.10.10] local-address 10.1.1.1
```

Related Topics

10.3.1 anycast-rp (IPv4)

10.3.45 peer (IPv4)

10.3.44 neighbor-check (IPv4)

Function

The **neighbor-check** command enables the PIM neighbor check function.

The **undo neighbor-check** command restores the default setting.

By default, the PIM neighbor check function is not enabled.

Format

neighbor-check { **receive** | **send** }

undo neighbor-check { **receive** | **send** }

Parameters

Parameter	Description	Value
receive	Checks whether the Join/Prune and Assert messages are received from a PIM neighbor. If not, these messages are discarded.	-

Parameter	Description	Value
send	Checks whether the Join/Prune and Assert messages are sent to a PIM neighbor. If not, these messages are not sent.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices send Join/Prune messages to the upstream PIM neighbor to perform join and prune actions and PIM neighbor often exchange Assert messages. To save system resources and protect security of Join/Prune messages and Assert messages, run the **neighbor-check** command to enable the PIM neighbor check function.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

You can specify both **receive** and **send** to enable the PIM neighbor check function for the received and sent Join/Prune and Assert messages.

Precautions

This command is valid only for PIM-SM.

Example

In the public network instance, enable the PIM neighbor check function for the received Join/Prune and Assert messages.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] neighbor-check receive
```

10.3.45 peer (IPv4)

Function

The **peer** command configures Anycast RP peers.

The **undo peer** command removes the configurations of Anycast RPs.

By default, no Anycast RP peer is configured.

Format

peer *peer-address* [**fwd-msdp-sa** [*acl-number* | **acl-name** *acl-name*]]

undo peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an Anycast RP peer.	The value is in dotted decimal notation.
fwd-msdp-sa	Enables a local RP to extract source/group information from the received MSDP SA message, encapsulates the information into a Register message, and sends the Register message to Anycast RP peers.	-
acl-number	Specifies the range of multicast groups to which an MSDP SA message can be forwarded. *acl-number* specifies an ACL number.	The value is an integer ranging from 2000 to 3999.
acl-name *acl-name*	Specifies the range of multicast groups to which an MSDP SA message can be forwarded. *acl-name* specifies an ACL name. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Anycast RP view of public network instance or Anycast RP view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IP address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the destination addresses of the Register message. In such a manner, Anycast RP peers

can learn source/group information from each other. This command is used to configure an address for an Anycast RP peer. This address is used as the destination address of the Register message to be sent by the local RP.

To enable an RP to obtain information about the multicast source in another PIM-SM domain, you can adopt either of the following schemes:

- Set up MSDP peer relationships between every Anycast RP member in a PIM-SM domain and the RP in another PIM-SM domain.
- Set up MSDP peer relationships between some Anycast RP members with the RP in another PIM-SM domain. After the members who have set up MSDP peer relationships receive SA messages, they extract source/group information from SA messages, encapsulate the information into Register messages, and forward the Register messages to the members who do not set up MSDP peer relationships with the RP.

Precautions

You can specify a maximum of 16 Anycast RP peers for each Anycast RP.

In a PIM-SM domain, all the devices deployed with Anycast RP must be fully connected logically. Anycast RP peer relationships need to be configured between every two devices deployed with the Anycast RP.

Example

In the public network instance, set the Anycast RP address to 10.3.3.3 and the peer address to 10.2.2.2, and enable the local RP to forward MSDP SA messages to its peers.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] anycast-rp 10.3.3.3
[Huawei-pim-anycast-rp-10.3.3.3] peer 10.2.2.2 fwd-msdp-sa
```

Related Topics

10.3.43 local-address (IPv4)

10.3.1 anycast-rp (IPv4)

10.3.46 pim

Function

The **pim** command displays the PIM view.

The **undo pim** command clears the configuration in the PIM view.

Format

pim [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing PIM configurations, run the **pim** command to enter the PIM view.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

NOTICE

In using the **undo pim** command, enter Y or N to confirm the action. This command clears global IPv4 PIM configurations in the current instance. Use this command with caution.

Example

Enter the PIM view of the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim]
```

Enter the PIM view of VPN instance **mytest**.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-mytest-af-ipv4] multicast routing-enable
[Huawei-vpn-instance-mytest-af-ipv4] quit
[Huawei-vpn-instance-mytest] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] pim vpn-instance mytest
[Huawei-pim-mytest]
```

Related Topics

10.3.50 pim dm

10.3.62 pim sm

10.3.47 pim bfd

Function

The **pim bfd** command adjusts the PIM BFD parameters on an interface.

The **undo pim bfd** command restores the default values of PIM BFD parameters.

By default, the minimum interval for transmitting BFD packets and minimum interval for receiving BFD packets are 1000 ms, and the BFD detection multiplier is 3.

Format

pim bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *

undo pim bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo pim bfd { **min-tx-interval** *tx-value* | **min-rx-interval** *rx-value* | **detect-multiplier** *multiplier-value* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-value*	Specifies the minimum interval for transmitting BFD packets.	The value is an integer that ranges from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
min-rx-interval *rx-value*	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 10 to 2000, in milliseconds. The default value is 1000 milliseconds.
detect-multiplier *multiplier-value*	Specifies the BFD detection multiplier.	The value is an integer that ranges from 3 to 50. The default value is 3.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After PIM BFD is enabled, sometimes you need to run the **pim bfd** command to adjust PIM BFD parameters to adapt to the link. You can use this command to set the minimum interval for sending BFD packets, minimum interval for receiving PIM BFD packets, and local detection multiplier.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid only for PIM-SM.

Before setting PIM BFD parameters, run the **pim bfd enable** command to enable PIM BFD. Otherwise, the configured parameters do not take effect.

The minimum values of *tx-value* and *rx-value* vary with products. You are recommended to set the two values to be equal to or greater than 100. Otherwise, the BFD session flapping may occur.

Example

Adjust the minimum interval for transmitting BFD packets on GE 0/0/1.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] pim sm
[Huawei-GigabitEthernet0/0/1] pim bfd enable
[Huawei-GigabitEthernet0/0/1] pim bfd min-tx-interval 100
```

Related Topics

10.3.26 display pim interface

10.3.21 display pim bfd session

10.3.48 pim bfd enable

10.3.48 pim bfd enable

Function

The **pim bfd enable** command enables PIM BFD on an interface.

The **undo pim bfd enable** command disables PIM BFD on an interface.

By default, PIM BFD is not enabled on an interface.

Format

pim bfd enable

undo pim bfd enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command enables PIM BFD on an interface to quickly detect link failures on the interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

PIM BFD depends on the BFD protocol. If the **bfd** command is not run to enable global BFD, the session status is **BFD global disable** though PIM BFD sessions can be set up.

This command is applicable to NBMA interfaces and broadcast interfaces rather than P2P interfaces.

Example

Enable PIM BFD on GE1/0/0.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim sm
[Huawei-GigabitEthernet1/0/0] pim bfd enable
```

Related Topics

10.3.21 display pim bfd session

10.3.49 pim bsr-boundary

Function

The **pim bsr-boundary** command configures the BSR boundary of a PIM-SM domain on an interface.

The **undo pim bsr-boundary** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, the BSR boundary of a PIM-SM domain is not set.

Format

pim bsr-boundary

undo pim bsr-boundary

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the management core of the PIM-SM network, the BSR is responsible for sending collected RP-set information to PIM neighbors through Bootstrap messages.

You can divide a large PIM-SM network into multiple PIM-SM domains by configuring the bsr boundary on an interface. Each BSR then serves the local PIM-SM domain.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

The Bootstrap messages cannot traverse the BSR boundary but other multicast packets can.

Example

Configure the BSR boundary of a PIM-SM domain on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim bsr-boundary
```

Related Topics

10.3.5 c-bsr (IPv4)

10.7.17 multicast boundary

 Copyright © Huawei Technologies Co., Ltd.

10.3.50 pim dm

Function

The **pim dm** command enables PIM-DM on an interface.

The **undo pim dm** command restores the default configuration.

By default, PIM-DM is disabled on an interface.

Format

pim dm

undo pim dm

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-DM network, after PIM-DM is enabled on an interface, the router can set up the PIM neighbor relationship with the neighboring device. The router then can process protocol packets received from PIM neighbors.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

PIM-DM and PIM-SM cannot be enabled simultaneously on interfaces bound to the same VPN instance or public network instance.

If PIM-DM and IGMP need to be enabled on the same interface, enable PIM-DM, and then enable IGMP.

Example

Enable PIM-DM on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim dm
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.62 pim sm

10.3.51 pim hello-option dr-priority

Function

The **pim hello-option dr-priority** command sets the priority for the PIM interface that is elected as DR.

The **undo pim hello-option dr-priority** command restores the default value of the priority.

By default, the priority for the PIM interface that is elected as DR is 1.

Format

pim hello-option dr-priority *priority*

undo pim hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the priority of the PIM interface that is elected as DR. The greater the value, the higher the priority.	The value is an integer ranging from 0 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM, routers on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IP address. To elect the DR, the routers send the Hello message that contains the priority to each other. The router with the highest priority functions as the DR. If the routers have the same priority, the router with the largest IP address functions as the DR.

If there is at least one router that does not support Hello packets that contain the priority in the network, the DR election is based on the IP address of each router. The router with the largest IP address functions as the DR.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **pim hello-option dr-priority** command has the same function as the **hello-option dr-priority (IPv4)** command in the PIM view. By default, if the **pim hello-option dr-priority** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the priority of GE1/0/0 that is elected as DR to 3.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option dr-priority 3
```

Related Topics

10.3.33 hello-option dr-priority (IPv4)

10.3.52 pim hello-option holdtime

Function

The **pim hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

The **undo pim hello-option holdtime** command restores the default value of the timeout.

By default, the timeout period during which the PIM interface waits to receive the Hello message from its neighbor is 105 seconds.

Format

pim hello-option holdtime *interval*

undo pim hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the PIM interface waits to receive Hello messages from its neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device considers the neighbor invalid or unreachable.

The **pim hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The timeout period must be greater than the interval for sending Hello messages. You can run the **pim timer hello** command to set the interval for sending Hello messages.

The **pim hello-option holdtime** command has the same function as the **hello-option holdtime (IPv4)** command in the PIM view. By default, if the **pim hello-option holdtime** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period during which GE1/0/0 waits to receive Hello messages from its neighbor to 120 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option holdtime 120
```

Related Topics

10.3.66 pim timer hello

10.3.34 hello-option holdtime (IPv4)

10.3.53 pim hello-option lan-delay

Function

The **pim hello-option lan-delay** command sets the delay in transmitting messages in a shared network in the interface view.

The **undo pim hello-option lan-delay** command restores the default value of the delay.

 Copyright © Huawei Technologies Co., Ltd.

By default, the delay in transmitting messages in the shared network is 500 ms.

Format

pim hello-option lan-delay *interval*

undo pim hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting messages in the shared network.	The value is an integer that ranges from 1 to 32767, in milliseconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all routers on the same link are different, the maximum value of these values is used.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current router receives a Prune message from the downstream interface and performs the prune action. If the router receives a Join message from the downstream interface in PPT, the router cancels the prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

If the prune delay is set too short, the upstream router stops forwarding multicast packets before the downstream router overrides Prune messages of neighbors. Exercise caution when you run this command.

 Copyright © Huawei Technologies Co., Ltd.

The function of this command in the interface view is the same as that of the **hello-option lan-delay (IPv4)** command in the PIM view, except for the view. By default, if the configuration on the interface is not performed, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting messages to 200 ms in GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option lan-delay 200
```

Related Topics

10.3.51 pim hello-option dr-priority

10.3.37 hello-option override-interval (IPv4)

10.3.35 hello-option lan-delay (IPv4)

10.3.54 pim hello-option neighbor-tracking

Function

The **pim hello-option neighbor-tracking** command enables the neighbor tracking function in the interface view.

The **undo pim hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

pim hello-option neighbor-tracking

undo pim hello-option neighbor-tracking

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device

status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. The upstream neighbor cannot update neighbor relationships with downstream devices because of Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

Neighbor tracking can be implemented only when on all devices on the shared network segment have this function enabled.

The **pim hello-option neighbor-tracking** command has the same function as the **hello-option neighbor-tracking (IPv4)** command in the PIM view. By default, if the **pim hello-option neighbor-tracking** command is not used, the configuration in the PIM view takes effect; otherwise, the configuration in the interface view takes effect.

Example

Enable the neighbor tracking function in GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option neighbor-tracking
```

Related Topics

10.3.36 hello-option neighbor-tracking (IPv4)

10.3.55 pim hello-option override-interval

Function

The **pim hello-option override-interval** command sets the interval carried in Hello messages for overriding the prune action on the interface.

The **undo pim hello-option override-interval** command, restores the default configuration.

By default, the interval carried in Hello messages for overriding the prune action on the interface is 2500 milliseconds.

Format

pim hello-option override-interval *interval*

undo pim hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval of overriding the prune action.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

When the values of **override-interval** on all routers on the same link are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the router does not perform the prune action until the PPT times out. If the router receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If you run the **pim hello-option override-interval** command multiple times, only the latest configuration takes effect.

Precautions

This command is valid for PIM-SM and PIM-DM.

The **pim hello-option override-interval** command has the same function as the **hello-option override-interval (IPv4)** command in the PIM view. By default, if

the **pim hello-option override-interval** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval for overriding the prune action in Hello messages to 2000 ms in GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim hello-option override-interval 2000
```

Related Topics

10.3.53 pim hello-option lan-delay

10.3.35 hello-option lan-delay (IPv4)

10.3.37 hello-option override-interval (IPv4)

10.3.56 pim holdtime assert

Function

The **pim holdtime assert** command sets the timeout period during which a PIM interface keeps the Assert state.

The **undo pim holdtime assert** command restores the default value of the timeout.

By default, the timeout period during which a PIM interface keeps the Assert state is 180 seconds.

Format

pim holdtime assert *interval*

undo pim holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which a PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM routers need to initiate the assert mechanism. The router that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retains the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The **pim holdtime assert** command has the same function as the **holdtime assert (IPv4)** command in the PIM view. By default, if the **pim holdtime assert** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period for the interface GE1/0/0 to keep the Assert state to 100s.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim holdtime assert 100
```

Related Topics

10.3.39 holdtime join-prune (IPv4)

10.3.57 pim holdtime join-prune

10.3.38 holdtime assert (IPv4)

10.3.57 pim holdtime join-prune

Function

The **pim holdtime join-prune** command sets the holdtime in a Join/Prune message sent by the PIM interface.

The **undo pim holdtime join-prune** command restores the default value of the holdtime.

By default, the holdtime in a Join/Prune message sent by the PIM interface is 210 seconds.

Format

pim holdtime join-prune *interval*

 Copyright © Huawei Technologies Co., Ltd.

undo pim holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime in a Join/Prune message sent by the PIM interface.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the router starts the holdtime timer. If the router does not receive subsequent Join/Prune messages from the downstream device within the holdtime interval, the router suppresses forwarding of Join/Prune messages carrying group join information on the downstream interface in the group. If Join/Prune messages carry group prune information, the downstream interface is restored.

The **pim holdtime join-prune** command sets the holdtime interval for Join/Prune messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for PIM-SM and PIM-DM.

The holdtime of Join/Prune messages must be larger than the interval for sending Join/Prune messages and is generally 3.5 times the interval for sending Join/Prune messages.

The **pim holdtime join-prune** command has the same function as the **holdtime join-prune (IPv4)** command in the PIM view. By default, if the **pim holdtime join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the holdtime in a Join/Prune message sent by the interface GE1/0/0 to 280 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
```

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim holdtime join-prune 280
```

Related Topics

10.3.38 holdtime assert (IPv4)

10.3.56 pim holdtime assert

10.3.39 holdtime join-prune (IPv4)

10.3.58 pim join-policy

Function

The **pim join-policy** command enables the system to filter join information in Join/Prune messages.

The **undo pim join-policy** command restores the default setting.

By default, join information in Join/Prune message is not filtered.

Format

pim join-policy { **asm** { *basic-acl-number* | **acl-name** *acl-name* } | **ssm** { *advanced-acl-number* | **acl-name** *acl-name* } | *advanced-acl-number* | **acl-name** *acl-name* }

undo pim join-policy [**asm** | **ssm**]

Parameters

Parameter	Description	Value
asm	Filters join information, with the group address in the ASM group address range.	-
basic-acl-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ssm	Filters join messages, with the group addresses within the SSM group address range and specified source address.	-
advanced-acl-number	Specifies the advanced ACL number.	The value is an integer that ranges from 3000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from joining multicast groups on the PIM-SM network, run the **pim join-policy** command to enable the system to filter join information in Join/Prune messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

The **pim join-policy** command and the **acl** command are used together.

- If **asm** is specified, in the basic ACL view, you can set the multicast group address range of join information by specifying the **source** parameter in the **rule** command.
- If **ssm** is specified, in the advanced ACL view, you can set the source address range and multicast group address range of join information by respectively specifying the **source** parameter and **destination** parameter in the **rule** command.

The rule configurations for a named ACL and an advanced ACL are the same. The **time-range** parameter takes effect in the **rule** command only for the named ACL.

Example

Configure GE1/0/0 to accept the join information with the group address in the range of 225.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[Huawei-acl-basic-2001] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim join-policy asm 2001
```

10.3.59 pim neighbor-policy

Function

The **pim neighbor-policy** command configures a policy for filtering PIM neighbors on an interface.

The **undo pim neighbor-policy** command restores the default setting.

By default, PIM neighbors on the interface are not filtered.

Format

pim neighbor-policy { *basic-acl-number* | **acl-name** *acl-name* }

undo pim neighbor-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the ACL name. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized neighbors from being involved in the PIM protocol, run the **pim neighbor-policy** command to configure a policy for filtering PIM neighbors and set the address range of PIM neighbors. The router sets up neighbor relationships with the addresses matching the filtering rules and deletes the neighbors that do not match the filtering rules.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

The **pim neighbor-policy** command and the **acl** command are used together. In the ACL view, set the address range of PIM neighbors by specifying **source** in the **rule** command.

For the named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, the filtering rule takes effect for only the multicast group address range specified by **source** and the time range specified by **time-range**.

Precautions

This command is valid for both PIM-DM and PIM-SM.

If a PIM device has established a neighbor relationship with the router but its IP address is not in the configured range of valid neighbor addresses, the router will

 Copyright © Huawei Technologies Co., Ltd.

no longer receive Hello messages from this PIM neighbor. When the holdtime of Hello messages expires, the neighbor relationship between the PIM device and the router is terminated.

Example

Allow GE1/0/0 to set up a PIM neighbor relationship with a PIM device at 10.4.4.4.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.4.4.4 0.0.0.0
[Huawei-acl-basic-2001] quit
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim neighbor-policy 2001
```

10.3.60 pim require-genid

Function

The **pim require-genid** command configures a PIM interface to reject the Hello messages without the generation ID.

The **undo pim require-genid** command restores the default configuration.

By default, a PIM interface receives the Hello messages without the generation ID.

Format

pim require-genid

undo pim require-genid

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface on the device is enabled with PIM, the device generates a random number as the generation ID of the Hello message. If the status of the device is updated, the device generates a new Generation ID. When the device finds that the Hello message received from a PIM neighbor contains a different Generation ID, the device considers that the status of the PIM neighbor changes.

To ensure that connected PIM neighbors work properly, run the **pim require-genid** command to configure a PIM interface to reject the Hello messages without the generation ID.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

Configure GE1/0/0 to reject the Hello messages without the generation ID.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim require-genid
```

10.3.61 pim silent

Function

The **pim silent** command enables the PIM silent function on an interface.

The **undo pim silent** command cancels the PIM silent function on an interface.

By default, the PIM silent function is disabled on an interface.

Format

pim silent

undo pim silent

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the router against pseudo PIM Hello messages sent from malicious hosts, configure the **pim silent** command on the interface directly connected to the host network segment to set the interface to PIM silent mode. Then the

interface cannot receive or forward any PIM packet, and all PIM neighbors and PIM state machines on this interface are deleted. This interface becomes the DR, but the IGMP function on the interface is not affected.

The PIM silent function applies only to the interface directly connected to a host network segment, and only one PIM router can be connected to this network segment.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

NOTICE

After you run this command on an interface, the interface no longer receives or sends any PIM packets and other PIM functions on the interface become invalid. Confirm your action before using this command.

If a host network segment is connected to multiple routers and PIM silent is enabled on multiple interfaces, all these interfaces become static DRs. This causes multicast forwarding failures.

Example

Configure the PIM silent function on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim silent
```

10.3.62 pim sm

Function

The **pim sm** command enables PIM-SM on an interface.

The **undo pim sm** command restores the default configuration.

By default, PIM-SM is disabled on an interface.

Format

pim sm

undo pim sm

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIM-SM is enabled on interfaces, routers can set up PIM neighbor relationships with each other and process protocol packets received from PIM neighbors.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

PIM-DM and PIM-SM cannot be enabled simultaneously on interfaces bound to the same VPN instance or public network instance.

If PIM-SM and IGMP need to be enabled on the same interface, enable PIM-SM, and then enable IGMP.

Example

Enable PIM-SM on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim sm
```

Related Topics

10.3.50 pim dm

10.3.63 pim state-refresh-capable

Function

The **pim state-refresh-capable** command enables PIM-DM state refresh on an interface.

The **undo pim state-refresh-capable** command disables PIM-DM state refresh.

By default, PIM-DM state refresh is enabled.

Format

pim state-refresh-capable

undo pim state-refresh-capable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM state refresh is implemented by periodically sending State-Refresh messages in the network. After receiving a State-Refresh message, the router in the pruned state resets the prune-status timer. As a result, the downstream interface cannot forward packets before the prune-status timer times out.

After PIM-DM state refresh is disabled, the interface starts to forward multicast data when the prune timer times out. The downstream routers that do not want to receive the data can send Prune messages. The process is performed periodically, which wastes a lot of network resources. Enabling PIM-DM state refresh can optimize the network traffic.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Disable PIM-DM state refresh on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo pim state-refresh-capable
```

Related Topics

10.3.80 state-refresh-interval (IPv4)

10.3.81 state-refresh-rate-limit (IPv4)

10.3.82 state-refresh-ttl (IPv4)

10.3.64 pim timer dr-switch-delay

Function

The **pim timer dr-switch-delay** command enables PIM DR switching delay and configures the delay on an interface. When the interface changed from a DR to a non-DR, the interface continues to forward data before the delay expires.

The **undo pim timer dr-switch-delay** command disables PIM DR switching delay on the interface.

 Copyright © Huawei Technologies Co., Ltd.

By default, when the interface changes from a DR to a non-DR, the interface stops forwarding data immediately.

Format

pim timer dr-switch-delay *interval*

undo pim timer dr-switch-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DR on a shared network segment becomes the non-DR, original multicast forwarding entries will be deleted immediately, causing multicast data interruption in a short time. To solve the problem, set the DR switching delay. Original multicast forwarding entries still take effect until the delay is reached.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

Example

Enable PIM DR switching delay on GE1/0/0 and set the delay to 20 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer dr-switch-delay 20
```

10.3.65 pim timer graft-retry

Function

The **pim timer graft-retry** command sets the interval for retransmitting Graft messages on an interface.

 Copyright © Huawei Technologies Co., Ltd.

The **undo pim timer graft-retry** command restores the default value of the interval.

By default, the interval for retransmitting Graft messages on an interface is 3 seconds.

Format

pim timer graft-retry *interval*

undo pim timer graft-retry

Parameters

Parameter	Description	Value
interval	Specifies the interval of retransmitting Graft messages.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM mode, when a member joins a pruned group, the router sends a Graft message and waits to receive an ACK message from the upstream router. If the downstream router does not receive the ACK message in the period configured through the command, the router resends the Graft message until the router receives the ACK message from the upstream router.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Set the interval for retransmitting Graft messages to 80s on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer graft-retry 80
```

 Copyright © Huawei Technologies Co., Ltd.

10.3.66 pim timer hello

Function

The **pim timer hello** command sets the interval for sending Hello messages on an interface.

The **undo pim timer hello** command restores the default value of the interval.

By default, the interval for sending Hello messages on an interface is 30 seconds.

Format

pim timer hello *interval*

undo pim timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim timer hello** command to set the interval for sending Hello messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The interval for sending Hello messages must be shorter than the timeout period of PIM neighbors. You can run the **hello-option holdtime (IPv4)** command to set the timeout period of PIM neighbors.

The configuration is the same as the **timer hello (IPv4)** command in the PIM view, except for the view. The system prefers the configuration in the interface view. The value configured in the PIM view is used if no value is configured on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval for sending Hello messages to 40 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer hello 40
```

Related Topics

10.3.84 timer hello (IPv4)

10.3.67 pim timer join-prune

Function

The **pim timer join-prune** command sets the interval for periodically sending Join/Prune messages to the upstream device.

The **undo pim timer join-prune** command restores the default interval.

By default, the interval for periodically sending Join/Prune messages to the upstream device is 60 seconds.

Format

pim timer join-prune *interval*

undo pim timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Join/Prune messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends join information to the upstream device, requesting the upstream device to forward multicast data. The device sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune

 Copyright © Huawei Technologies Co., Ltd.

messages. The device periodically sends Join/Prune messages to the upstream device to update the forwarding status.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid only for PIM-SM.

The interval configured through this command must be shorter than the interval configured through the **pim holdtime join-prune** command. The interval at which Join or Prune messages are sent must be shorter than the holdtime carried in Join/Prune messages.

The configuration is the same as that of the **timer join-prune (IPv4)** command in the PIM view. The system prefers the configuration in the interface view. The value configured in the PIM view is used if no value is configured on the interface.

Example

Set the interval for sending Join or Prune messages to 80 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim timer join-prune 80
```

Related Topics

10.3.85 timer join-prune (IPv4)

10.3.68 pim triggered-hello-delay

Function

The **pim triggered-hello-delay** command sets the maximum delay for triggering Hello messages.

The **undo pim triggered-hello-delay** command restores the default maximum delay.

By default, the maximum delay for triggering Hello messages is 5 seconds.

Format

pim triggered-hello-delay *interval*

undo pim triggered-hello-delay

Parameters

Parameter	Description	Value
interval	Specifies the maximum delay for triggering Hello messages.	The value is an integer that ranges from 1 to 5, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To avoid the conflict caused by multiple PIM devices sending Hello message at the same time, the PIM device automatically selects a random number smaller than the configured value as the delay. When detecting Hello messages in the network, the PIM device sends Hello message after the delay.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Set the maximum delay for triggering the Hello message to 3 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim triggered-hello-delay 3
```

10.3.69 probe-interval (IPv4)

Function

The **probe-interval** command sets the interval for a router to send Probe messages (null Register message) to the RP.

The **undo probe-interval** command restores the default value of the interval.

By default, the interval for a router to send Probe messages to the RP is 5 seconds.

Format

probe-interval *interval*

undo probe-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Probe messages to RP.	The value is an integer that ranges from 1 to 1799, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving a Register-Stop message sent by the RP, the DR at the source side stops sending Register messages and enters the register suppression state.

During the register suppression, the DR at the source side sends Probe messages to notify the RP that the multicast source is still in the Active state. After the register suppression times out, the DR at the source side starts to send Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

The interval set using the **probe-interval** command must be less than half the interval set using the **register-suppression-timeout (IPv4)** command.

Example

In the public network instance, set the interval for sending Probe messages to RP to 6 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] probe-interval 6
```

Related Topics

10.3.73 register-suppression-timeout (IPv4)

10.3.70 register-header-checksum

Function

The **register-header-checksum** command configures devices to calculate the checksum based on the header of a Register message only.

The **undo register-header-checksum** command restores the default configuration.

By default, the checksum is calculated according to all the contents of a Register message.

 Copyright © Huawei Technologies Co., Ltd.

Format

register-header-checksum

undo register-header-checksum

Parameters

None

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the source's DR calculates the checksum based on all fields in a Register message. After the **register-header-checksum** command is executed, the source's DR calculates the checksum based on the Register message header. This shortens checksum calculation and improves encapsulation of multicast data in Register messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

Example

Calculate the checksum based only on the header of a Register message in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-header-checksum
```

Related Topics

10.3.71 register-policy (IPv4)
10.3.73 register-suppression-timeout (IPv4)

 Copyright © Huawei Technologies Co., Ltd.

10.3.71 register-policy (IPv4)

Function

The **register-policy** command sets the rules used by an RP to filter Register messages.

The **undo register-policy** command restores the default setting.

By default, the rules for filtering Register messages are not configured.

Format

register-policy { *advanced-acl-number* | **acl-name** *acl-name* }

undo register-policy

Parameters

Parameter	Description	Value
advanced-acl-number	Specifies the number of the advanced ACL that defines the rules for filtering packets based on source addresses or group addresses.	The value is an integer that ranges from 3000 to 3999.
acl-name *acl-name*	Specifies the name of a Named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of invalid Register messages, you can configure devices to receive or deny Register messages according to the packet filtering rules.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

When the **register-policy** command is used on the RP, only Register messages matching the rule of the ACL are received by the RP. If an undefined ACL is specified, the RP denies all Register messages.

This command is valid for only PIM-SM.

The **register-policy** command takes effect for only subsequently received Register messages. The multicast entries that have been registered successfully are not deleted and can still be used for multicast data forwarding.

Example

Configure the RP to receive Register packets sent by the source on network segment 10.10.0.0/16 to group 225.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl number 3000
[Huawei-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-3000] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-policy 3000
```

Configure a Named ACL: the RP receives Register packets sent by the source on network segment 10.10.0.0/16 to group 225.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-policy acl-name myacl
```

Related Topics

10.3.73 register-suppression-timeout (IPv4)

10.3.72 register-source

Function

The **register-source** command specifies the source address used by the source's DR to send Register messages.

The **undo register-source** command restores the default setting.

By default, the source address used by the source's DR to send Register messages is not specified.

Format

register-source *interface-type interface-number*

undo register-source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source's DR.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the source IP address for sending Register messages is no longer the only IP address in the network for the RP router or the source IP address is filtered out, errors occur in the registration process and extra traffic occupies bandwidth on the network. In this case, use the **register-source** command to specify an appropriate interface as the source IP address for sending Register messages. Using the loopback address of the source's DR as the source IP address is recommended.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

The command is effective only when the specified interface is in Up state.

Example

In the public network instance, specify the IP address of loopback 0 as the source IP address for source's DR to send Register messages.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-source loopback 0
```

10.3.73 register-suppression-timeout (IPv4)

Function

The **register-suppression-timeout** command sets the timeout period during which a router keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a router keeps the register suppression state for 60 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

register-suppression-timeout *interval*

undo register-suppression-timeout

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the router keeps the register suppression state.	The value is an integer that ranges from 11 to 3600, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Register-Stop message from the RP, the router immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the router keeps the register suppression state. When the timeout period expires, the router (source DR) starts to send Register messages to the RP.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If the timeout period is too short, the RP receives burst multicast data more frequently. If the timeout period is too long, the delay for a new receiver to join a group is long when an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv4)** command to configure the router to send null Register messages before the suppression timer times out. This configuration reduces burst Register messages and shortens the timeout period to reduce the delay for a new receiver to join a group.

Precautions

This command is valid only for PIM-SM.

The interval set by the **register-suppression-timeout** command must be larger than two times the interval set by the **probe-interval (IPv4)** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the public network instance, set the timeout period during which the router keeps the register suppression state to 70 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] register-suppression-timeout 70
```

Related Topics

10.3.69 probe-interval (IPv4)

10.3.71 register-policy (IPv4)

10.3.74 reset pim control-message counters

Function

The **reset pim control-message counters** command resets the statistics about PIM Control messages.

Format

reset pim [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Specifies all the instances.	-
interface *interface-type interface-number*	Specifies the name and the number of an interface. It is used to reset the statistics about PIM control messages on a specified interface.	-

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If a PIM-enabled interface on the device has been forwarding multicast packets in a long period of time, the device stores statistics on a large number of Cotrol messages. You can run this command to reset statistics on Control messages.

Example

Reset the statistics about PIM control messages on all interfaces in the public network instance.

```
<Huawei> reset pim control-message counters
```

Reset the statistics about PIM control messages on the GE1/0/0 in the public network instance.

```
<Huawei> reset pim control-message counters interface gigabitethernet 1/0/0
```

Related Topics

10.3.24 display pim control-message counters

10.3.75 reset pim routing-table

Function

The **reset pim routing-table** command resets PIM status of a specified downstream interface in a specified PIM routing entry.

Format

reset pim [**vpn-instance** *vpn-instance-name*] **routing-table group** *group-address* **mask** { *group-mask-length* | *group-mask* } **source** *source-address* **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
group *group-address*	Specifies the multicast group address of a PIM routing entry.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
mask *group-mask-length*	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mask *group-mask*	Specifies the mask of a multicast group address.	It is in dotted decimal notation.
source *source-address*	Specifies the source address of a PIM routing entry.	The value is in dotted decimal notation. If a (*, G) entry is specified, the source address is 0.0.0.0.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset pim routing-table** command resets PIM status of a specified downstream interface in a specified PIM routing entry.

Configuration Impact

This command can reset the PIM status of the specified interface in a specified PIM routing entry. It cannot reset the IGMP state and static group memberships on a specified interface.

Precautions

This command is valid only for PIM-SM.

NOTICE

Resetting PIM status of downstream interfaces can trigger transmission of Join/Prune messages, which causes multicast service interruption.

Example

In the public network instance, reset PIM status of downstream interface GE1/0/0 of (10.1.1.1, 225.0.0.1).

```
<Huawei> reset pim routing-table group 225.0.0.1 mask 255.255.255.0 source 10.1.1.1 interface gigabitethernet 1/0/0
```

10.3.76 source-lifetime (IPv4)

Function

The **source-lifetime** command specifies the timeout period of an (S, G) or (*, G) entry on the router.

The **undo source-lifetime** command restores the default value of the timeout period.

By default, the timeout period is 210 seconds.

Format

source-lifetime *interval*

undo source-lifetime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of an (S, G) or (*, G) entry on the router.	The value is an integer that ranges from 60 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router starts a timer for each (S, G) or (*, G) entry. The **source-lifetime** command sets the timer value. After receiving a multicast packet from S, the interface resets the timer. If the timer times out, the (S, G) or (*, G) entry is considered invalid.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for both PIM-DM and PIM-SM.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the public network instance, set the timeout period of an (S, G) or (*, G) entry of the router to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] source-lifetime 200
```

10.3.77 source-policy (IPv4)

Function

The **source-policy** command configures the router to filter received multicast data packets based on source addresses or source/group addresses.

The **undo source-policy** command deletes the configuration.

By default, a router does not filter received multicast data packets based on source addresses or source/group addresses.

Format

source-policy { *acl-number* | **acl-name** *acl-name* }

undo source-policy

Parameters

Parameter	Description	Value
acl-number	Specifies number of the basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized source information from being advertised on the PIM network, run the **source-policy** command to configure the router to filter received multicast data packets based on source addresses or source/group addresses.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If **source-policy** and the basic ACL are applied, all multicast data packets received should match the source address. Packets that do not pass the filtering are discarded.

If **source-policy** and the advanced ACL are used, the source addresses and group addresses of all received multicast data packets should be matched. Packets that do not pass the filtering are discarded.

The configurations of the Named ACL and advanced ACL are the same, and can implement filtering of both source addresses and multicast group addresses. The Named ACL can also be configured with the **time-range** parameter.

Precautions

This command is valid for both PIM-DM and PIM-SM.

Example

In the public network instance, configure the router to receive multicast data packets with the source address of 10.10.1.2 and to discard those with the source address of 10.10.1.1.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 10.10.1.2 0
[Huawei-acl-basic-2001] rule deny source 10.10.1.1 0
[Huawei-acl-basic-2001] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] source-policy 2001
```

In the public network instance, configure a Named ACL where multicast data packets with the source address of 10.10.1.2 are received, and those with the source address of 10.10.1.1 are dropped.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.10.1.2 0
[Huawei-acl-adv-myacl] rule deny ip source 10.10.1.1 0
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] source-policy acl-name myacl
```

10.3.78 spt-switch-threshold (IPv4)

Function

The **spt-switch-threshold** command sets the rate threshold of the multicast packets when the DR at the member side joins the SPT.

The **undo spt-switch-threshold** command restores the default value.

By default, the system performs SPT switchover on receiving the first multicast data packet through the RPT.

 Copyright © Huawei Technologies Co., Ltd.

Format

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** { *basic-acl-number* | **acl-name** *acl-name* } [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy** { *basic-acl-number* | **acl-name** *acl-name* }]

Parameters

Parameter	Description	Value
traffic-rate	Specifies the threshold rate for the switchover from the RPT to the SPT. **NOTE** Setting this parameter may affect operation of multicast services. You are advised to use the default triggering condition. That is, an SPT switchover is triggered immediately after the first multicast data packet is received from the RPT. The default triggering condition can reduce the number of multicast packets forwarded on the RPT.	The value is an integer that ranges from 1 to 4194304, in kbit/s.
infinity	Indicates that the SPT switchover is never triggered.	-
basic-acl-number	Specifies an entry of the group-policy list. It works with the multicast group that matches **group-policy** *basic-acl-number* to enable the threshold. *basic-acl-number* specifies the number of the basic ACL that defines the range of multicast groups.	If the parameter is not set, the threshold is applied to all multicast groups. The value ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a Named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
order *order-value*	Adjusts the order of the ACLs in the group-policy list.	If a group matches multiple ACLs, the threshold is selected in the order specified by *order-value*. *order-value* specifies the updated number. It is an integer. The value is any value other than original one in the current group-policy list. If the parameter is not set, the order of the ACLs in the group-policy list does not change.

 Copyright © Huawei Technologies Co., Ltd.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source's DR encapsulates multicast packets in a Register message, and then transmits the unicast Register message to the RP. Then, the RP decapsulates the Register message and forwards the multicast packets to the receivers along the RPT. By default, when the RP or receiver's DR receives a first multicast packet, it initiates an SPT switchover to the source.

After the **spt-switch-threshold** command is executed on the receiver's DR, the receiver's DR periodically checks the forwarding rate of multicast packets. When the forwarding rate exceeds the threshold, the receiver's DR sends a Join messages to the source, triggering the SPT switchover.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid to all devices that may function as the DR at the member side, but is invalid to RPs.

This command is valid for only PIM-SM.

If this command is used several times for the same group, the command that is first matched according to the order takes effect.

Example

In the public network instance, set the traffic rate threshold to 4 kbit/s. If the transmission rate of packets from the source to the multicast group exceeds the threshold, the router triggers an SPT switchover so that packets are forwarded along the SPT towards the source.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] spt-switch-threshold 4
```

In the public network instance, create a group-policy that uses ACL 2010, specify the **infinity** keyword in the command to ensure that an SPT switchover will never be triggered, and set the order of ACL 2010 in the group-policy to 1.

```
<Huawei> system-view
[Huawei] acl number 2010
[Huawei-acl-basic-2010] rule permit source 225.1.1.1 0
[Huawei-acl-basic-2010] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] spt-switch-threshold infinity group-policy 2010 order 1
```

 Copyright © Huawei Technologies Co., Ltd.

In the public network instance, create a group-policy that uses ACL 2010, set the traffic rate threshold to 100 kbit/s, and order ACL 2010 in the group-policy to 1.

```
<Huawei> system-view
[Huawei] acl number 2010
[Huawei-acl-basic-2010] rule permit source 225.1.1.1 0
[Huawei-acl-basic-2010] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] spt-switch-threshold 100 group-policy 2010 order 1
```

In the public network instance, create a group-policy that uses ACL **myacl**, set the traffic rate threshold to 100 kbit/s, and order ACL **myacl** in the group-policy to 1.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] spt-switch-threshold 100 group-policy acl-name myacl order 1
```

10.3.79 ssm-policy (IPv4)

Function

The **ssm-policy** command sets the range of SSM group addresses.

The **undo ssm-policy** command restores the default configuration.

By default, the range of SSM group addresses is 232.0.0.0/8.

Format

ssm-policy { *basic-acl-number* | **acl-name** *acl-name* }

undo ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL that defines the range of SSM group addresses.	The value is an integer that ranges from 2000 to 2999.
acl-name *acl-name*	Specifies the name of a Named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the address of an SSM group ranges from 232.0.0.0 to 232.255.255.255. You can run the **ssm-policy** command to specify the range of PIM SSM group addresses. All the PIM-SM interfaces consider that PIM SSM is enabled on all the multicast groups in the specified address range. The specified SSM group address range can beyond 232.0.0.0/8.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

Example

In the public network instance, set the range of PIM SSM multicast addresses to 232.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Huawei-acl-basic-2000] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] ssm-policy 2000
```

In the public network instance, configure a Named ACL: the PIM SSM multicast address range is 232.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 232.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] ssm-policy acl-name myacl
```

Related Topics

10.1.50 ssm-mapping (IGMP)

10.3.80 state-refresh-interval (IPv4)

Function

The **state-refresh-interval** command sets the interval for sending PIM State-Refresh messages.

The **undo state-refresh-interval** command restores the default value of the interval.

By default, the interval for sending PIM State-Refresh messages is 60 seconds.

Format

state-refresh-interval *interval*

 Copyright © Huawei Technologies Co., Ltd.

undo state-refresh-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending PIM State-Refresh messages.	The value is an integer that ranges from 1 to 255, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-DM network, the device periodically sends State-Refresh messages to update the timeout interval of the prune timer on the downstream device. By doing this, the interface that has no multicast requirements retains in prune state. You can use the **state-refresh-interval** command to set the interval at which State-Refresh messages are sent.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

To prevent a pruned interface from forwarding packets when the Prune status times out, the interval for sending State-Refresh messages is shorter than the period for keeping the Prune status.

You can run the **holdtime join-prune (IPv4)** command to set the period during which the device keeps the Prune status.

This command is valid for only PIM-DM.

This command takes effect only on the routers directly connected to a source.

Example

Set the interval for sending PIM State-Refresh messages to 70s in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] state-refresh-interval 70
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.3.39 holdtime join-prune (IPv4)

10.3.81 state-refresh-rate-limit (IPv4)

Function

The **state-refresh-rate-limit** command sets the minimum period to wait before receiving the next PIM State-Refresh message.

The **undo state-refresh-rate-limit** command restores the default value.

By default, the minimum period to wait to receive the next PIM State-Refresh message is 30 seconds.

Format

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

Parameters

Parameter	Description	Value
interval	Specifies the minimum period for waiting to receive the next PIM State-Refresh message.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router can receive multiple PIM State-Refresh messages in a short period. Some of the messages are the same. To avoid duplicate messages, you can run the **state-refresh-rate-limit** command to set the period to wait to receive the next State-Refresh message.

- Before the State-Refresh timer times out, the router discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the router can receive the next State-Refresh message.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

Example

Set the minimum period to wait to receive the next PIM State-Refresh message to 45s in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] state-refresh-rate-limit 45
```

10.3.82 state-refresh-ttl (IPv4)

Function

The **state-refresh-ttl** command sets the TTL value for sending PIM State-Refresh messages.

The **undo state-refresh-ttl** command restores the default value of the TTL.

By default, the TTL value for sending PIM State-Refresh messages is 255.

Format

state-refresh-ttl *ttl-value*

undo state-refresh-ttl

Parameters

Parameter	Description	Value
ttl-value	Specifies the TTL value of the PIM State-Refresh message sent by an interface.	The value is an integer that ranges from 1 to 255.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a State-Refresh message, the router decreases the value of the TTL in the message by 1, and then sends the message to the downstream router until

the value of the TTL becomes 0. If the scale of the network is small, the message is delivered in a loop. You can use the **state-refresh-ttl** command to set the value of the TTL according to the scale of the network.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-DM.

This command takes effect only on the routers directly connected to a source.

Example

Set the TTL value for sending PIM State-Refresh messages to 45 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] state-refresh-ttl 45
```

10.3.83 static-rp (IPv4)

Function

The **static-rp** command configures a static RP.

The **undo static-rp** command restores the default configuration.

By default, no static RP is configured.

Format

static-rp *rp-address* [*basic-acl-number* | **acl-name** *acl-name*] [**preferred**]

undo static-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Specifies address of a static RP.	The address is in dotted decimal notation. It must be a valid unicast IP address and cannot be configured as an address of network segment 127.0.0.0/8.
basic-acl-number	Specifies the basic ACL that is used to control the range of multicast groups served by a static RP.	The value is an integer that ranges from 2000 to 2999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl-name *acl-name*	Specifies the name of a named ACL. **NOTE** **acl-name** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
preferred	Indicates that the static RP is preferred.	-

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only one RP exists on a network, you can manually specify the static RP address and do not need to configure dynamic RP. This saves the bandwidth used to exchange information between the C-RPs and the BSR.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

If the static RP address is the address of an Up interface on the local device, the local device works as the static RP. PIM does not need to be enabled on the interface where the static RP address is located.

If no ACL is specified, the static RP serves all the multicast groups of 224.0.0.0/4. If an ACL is specified but no rule is configured in the ACL, the static RP serves all the groups of 224.0.0.0/4. If ACL rules are configured, the static RP serves only the multicast groups permitted by the ACL.

If the **static-rp** command does not contain **preferred**, devices apply the BSR mechanism to elect a dynamic RP. If dynamic RP is not configured or the dynamic RP is invalid, the static RP becomes valid. If the **static-rp** command contains **preferred**, the static RP is preferred over the dynamic RP.

If you run this command multiple times, multiple static RPs are configured. If multiple static RPs serve the same group, the RP with the largest IP address is selected to serve the group. If you specify the same RP address when running the **static-rp** command multiple times, the latest RP takes effect.

The **static-rp** and **acl** commands are used together.

- For the numbered ACL, in the ACL view, you can set the address range of multicast groups that are served by the static RP by specifying the **source** parameter in the **rule** command.

 Copyright © Huawei Technologies Co., Ltd.

- For the Named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the multicast group address range specified by the **destination** parameter and the time period specified by the **time-range** parameter.
- For the numbered ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **source** parameter in the **rule** command. The filtering rule is effective only with the **source** parameter and the time period specified by the **time-range** parameter.
- For the Named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **destination** parameter in the **rule** command. The filtering rule is effective only with the **destination** parameter and the time period specified by the **time-range** parameter.

Precautions

NOTE

Up to 50 static RPs can be configured by using this command, but an ACL cannot be applied to multiple static RPs. If no ACL is referenced, only one static RP can be configured.

To ensure normal operating of a static RP, run the **static-rp** command to configure the same RP information on all devices in the PIM-SM domain.

This command is valid only for PIM-SM.

Example

In the public network instance, configure the router with address 10.110.0.6 as a static RP serving the groups permitted by ACL 2001, and configure the static RP to be preferred.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 225.1.0.0 0.0.255.255
[Huawei-acl-basic-2001] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] static-rp 10.110.0.6 2001 preferred
```

In the public network instance, configure the router with address 10.110.0.6 as a static RP serving the groups permitted by ACL **myacl**, and configure the static RP to be preferred.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] static-rp 10.110.0.6 acl-name myacl preferred
```

Related Topics

10.3.30 display pim rp-info

10.3.84 timer hello (IPv4)

Function

The **timer hello** command sets the interval at which the PIM router sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM router sends Hello messages is 30 seconds.

Format

timer hello *interval*

undo timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer ranging from 1 to 18000, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM routers periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim timer hello** command to set the interval for sending Hello messages.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Configuration Impact

This command is valid for both PIM-DM and PIM-SM.

The interval at which the PIM router sends Hello messages should be less than the timeout period of the PIM neighbor. You can run the **hello-option holdtime (IPv4)** command to set the timeout period of PIM neighbors.

The **timer hello** command has the same function as the **pim timer hello** command in the interface view. By default, if the **pim timer hello** command is not

 Copyright © Huawei Technologies Co., Ltd.

used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which PIM Hello messages are sent to 40s in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] timer hello 40
```

Related Topics

10.3.66 pim timer hello

10.3.34 hello-option holdtime (IPv4)

10.3.85 timer join-prune (IPv4)

Function

The **timer join-prune** command configures the interval at which Join/Prune messages are sent to an upstream router.

The **undo timer join-prune** command restores the default interval.

By default, the interval at which Join/Prune messages are sent to an upstream router is 60 seconds.

Format

timer join-prune *interval*

undo timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Join/Prune messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The router sends join information to the upstream device, requesting the upstream device to forward multicast data. The router sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The PIM router periodically sends Join/Prune messages to the upstream router to update the forwarding status.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid only for PIM-SM.

The interval configured using the **timer join-prune** command must be shorter than the interval configured using the **holdtime join-prune (IPv4)** command.

The **timer join-prune** command has the same function as the **pim timer join-prune** command in the interface view. By default, if the **pim timer join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which Join/Prune messages are sent to 80s in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] timer join-prune 80
```

Related Topics

10.3.67 pim timer join-prune

10.3.86 timer spt-switch (IPv4)

Function

The **timer spt-switch** command sets the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT.

The **undo timer spt-switch** command restores the default value of the interval.

By default, the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT is 15 seconds.

Format

timer spt-switch *interval*

undo timer spt-switch

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from RPT to SPT.	The value is an integer that ranges from 15 to 65535, in seconds.

Views

PIM view of public network instance or PIM view of VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **timer spt-switch** command to set the interval for checking whether the rate for transmitting multicast data exceeds the threshold.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is valid for only PIM-SM.

Before running this command, you must set the threshold for SPT switchover by using the **spt-switch-threshold (IPv4)** command; otherwise, the **timer spt-switch** command takes no effect.

Example

In the public network instance, set the interval for checking the rate for transmitting the multicast data before the switchover from RPT to SPT to 30 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] spt-switch-threshold 100
[Huawei-pim] timer spt-switch 30
```

Related Topics

10.3.78 spt-switch-threshold (IPv4)

 Copyright © Huawei Technologies Co., Ltd.

10.4 PIM (IPv6) Configuration Commands

NOTE

AR120 series do not support this function.

10.4.1 anycast-rp (IPv6)

Function

The **anycast-rp** command configures an Anycast RP and displays the Anycast-RP view or directly displays the existing Anycast-RP view.

The **undo anycast-rp** command deletes the configurations of an Anycast RP.

By default, no Anycast RP is configured.

Format

anycast-rp *rp-address*

undo anycast-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Indicates the Anycast RP address.	The value must be a legal IPv6 global unicast IP address in hexadecimal notation.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a traditional PIM-SM (IPv6) domain, all multicast groups map to one RP. When the network is overloaded or traffic concentrates on an RP, the RP may be overburdened. If the RP fails, routes are converged slowly or multicast packets are forwarded over non-optimal paths.

Configuring the Anycast RP in the PIM-SM (IPv6) domain can address this problem. IPv6 routing will automatically select the topologically closest RP for each source and receiver. This releases burdens on RPs, implements RP backup, and optimizes the forwarding paths.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If PIM (IPv6) Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message. In such a manner, Anycast RP peers can learn source/group information from each other.

Precautions

- The Anycast RP address must be the same as that of the elected RP on the current network.
- Either static or dynamic RPs can be used on the network. Configuring RPs on loopback interfaces is recommended. You need to configure the same RP address on the devices to be deployed with the Anycast RP. If the dynamic RP is used on the network, before configuring an Anycast RP address, run the **display pim ipv6 rp-info** command to check the address of the RP on the current network.

Example

Set the Anycast RP address to FC00:0:0:2001::1 in the PIM-IPv6 view and enter the Anycast-RP view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] anycast-rp fc00:0:0:2001::1
[Huawei-pim6-anycast-rp-fc00:0:0:2001::1]
```

Related Topics

10.4.42 local-address (IPv6)

10.4.44 peer (IPv6)

10.4.28 display pim ipv6 rp-info

10.4.2 bsm semantic fragmentation (IPv6)

Function

The **bsm semantic fragmentation** command enables BSR message fragmentation.

The **undo bsm semantic fragmentation** command disables BSR message fragmentation.

By default, BSR message fragmentation is not enabled.

Format

bsm semantic fragmentation

 Copyright © Huawei Technologies Co., Ltd.

undo bsm semantic fragmentation

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BSR message carries information about all C-RPs on the network. Therefore, if there is a large number of C-RPs on the network, the length of a BSR message exceeds the MTU of the outgoing interface. As a result, the BSR message cannot be processed and RP election fails. Consequently, multicast services cannot be transmitted normally. In this case, you can enable BSR message fragmentation to ensure that the devices on the network can learn consistent RP information and MDTs can be successfully established.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

You can also configure IP fragmentation to solve the preceding problem. The difference between IP fragmentation and BSR message fragmentation is as follows:

- If IP fragmentation is enabled, the protocol layer transmits the entire BSR message up to the IP layer regardless of the length of the BSR message. The BSR message is then fragmented at the IP layer. If one fragment is lost during transmission, the destination cannot parse the entire BSR message. As a result, the destination cannot learn RP information and MDTs cannot be established, which causes a multicast data forwarding failure.
- If BSR message fragmentation is enabled, the protocol layer directly fragments a long BSR message. If one fragment is lost during transmission, only the information carried in this fragment is lost. As a result, only MDTs corresponding to the information carried in the lost fragments cannot be established. Since the other BSR message fragments can still reach the destination, the corresponding MDTs can be correctly established.

BSR message fragmentation is recommended because it can solve the problem faced by IP fragmentation that all fragments become unavailable due to loss of fragment information.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Enable BSR message fragmentation on all devices on the network. If BSR message fragmentation is not enabled on some devices, RP information on these devices is inconsistent with that on other devices and MDTs cannot be established on these devices.

Example

Enable BSR message fragmentation in the PIM-IPv6 view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] bsm semantic fragmentation
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.3 bsr-policy (IPv6)

Function

The **bsr-policy** command specifies the range of valid bootstrap router (BSR) addresses so that the device discards BSR messages sent from addresses out of this range. This prevents BSR spoofing.

The **undo bsr-policy** command restores the default configuration.

By default, the range of BSR addresses is not limited, and all BSR packets are considered valid.

Format

bsr-policy { *basic-acl6-number* | **acl6-name** *acl6-name* }

undo bsr-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the basic ACL number. The ACL defines the filtering policy for the range of source addresses of BSR packets.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM-SM network that applies the BSR mechanism, you can configure any router as a C-BSR to elect the BSR. Once being elected as the BSR, the router is responsible for advertising RP information in the network. To prevent the valid BSR from being maliciously replaced, use the following measures:

- Certain hosts try changing the RP mapping to spoof the router by forging BSR packets.

  Solution: The attack often occurs on edge routers because the BSR packet is a multicast packet and the TTL value of the BSR packet is 1. The BSR is inside the network, and hosts are outside the network. The routers can perform neighbor check and RPF check on the received BSR packets to prevent the attack.
- Certain attackers control the router on the network, or unauthorized users connect to the router. The attackers configure the router as a C-BSR, and help the router win the BSR election. The attackers obtain the right of advertising RP information in the network.

  Solution: After the router is configured as a C-BSR, the router spreads BSR packets in the network. The BSR packets are multicast packets. The TTL value of BSR packets is 1. The BSR packets are forwarded hop by hop. As long as the neighboring router cannot receive the packets, the packets are not spread in the entire network. The solution is to use the **bsr-policy** command on every router in the network to limit the valid BSR range. For example, only routers FC00:0:0:2001::1/62 and FC00:0:0:2001::2/64 are elected as BSRs; therefore, the routers do not receive or forward other BSR packets. This type of attack is prevented.

The two countermeasures mentioned above can partially protect BSRs in the network. If attackers control a valid BSR, it also brings problems to the network.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

After the **bsr-policy** command is run, the router accepts only BSR messages matching the configured policy.

Precautions

The **bsr-policy** command and the **acl ipv6 (system view)** command are used together. In the ACL view, you can set the source address range for BSR packets by specifying the **source** parameter in the **rule (basic ACL6 view)** command.

When you use the **rule (basic ACL6 view)** command to configure a filtering rule for the Named ACL, the rule is effective only within the source address range specified by the **source** parameter and within the time period specified by the **time-range** parameter.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the PIM-IPv6 view, configure address FC00:0:0:2001::/64 as the valid BSR address range.

```
<Huawei> system-view
[Huawei] acl ipv6 2001
[Huawei-acl6-basic-2001] rule permit source fc00:0:0:2001:: 64
[Huawei-acl6-basic-2001] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] bsr-policy 2001
```

In the PIM-IPv6 view, use a Named ACL to configure address FC00:0:0:2001::/64 as the valid BSR address range.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:2001:: 64
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] bsr-policy acl6-name myacl6
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.4 c-bsr (IPv6)

Function

The **c-bsr** command configures a C-BSR.

The **undo c-bsr** command restores the default configuration.

By default, the C-BSR is not configured.

Format

c-bsr *ipv6-address* [*hash-length* [*priority*]]

undo c-bsr

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of a C-BSR. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the global IPv6 unicast address of the C-BSR.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
hash-length	Specifies the hash mask length of the C-BSR. The mask is used in a hash function to calculate the RP.	The value is an integer that ranges from 0 to 128. By default, the value is 126.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
priority	Specifies a priority of the C-BSR. A larger value indicates a higher priority.	The value is an integer ranging from 0 to 255. By default, the value is 0.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more C-BSRs need to be configured in a PIM-SM domain. A BSR is elected from C-BSRs. The BSR is responsible for collecting C-RP information and summarizing C-RP information into an RP-set. The RP-set is then encapsulated in a BootStrap message and advertised to all the devices in the PIM domain.

The process of BSR election is as follows:

- Each C-BSR considers itself as the BSR of the local PIM-SM domain and uses IPv6 address of this interface as the address of the BSR to send Bootstrap messages.
- When a C-BSR receives a Bootstrap message from other devices, it compares the BSR in the received Bootstrap message with the current BSR. The BSR with the highest priority is preferred. If BSRs have the same priority, the BSR with a larger IPv6 address is preferred. If the BSR carried in the received Bootstrap message is better than the current BSR, the C-BSR replaces its BSR address with the address of the BSR carried in the received Bootstrap message.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If PIM-SM (IPv6) is disabled on an interface, the interface can be configured as a C-BSR but the configuration does not take effect.

Example

In the PIM-IPv6 view, set the IPv6 address of the C-BSR to FC00:0:0:3001::1.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr fc00:0:0:3001::1
```

Related Topics

10.4.59 pim ipv6 sm

10.4.12 c-rp (IPv6)

10.4.5 c-bsr admin-scope (IPv6)

Function

The **c-bsr admin-scope** command configures a BSR administrative scope in a PIM-SM domain.

The **undo c-bsr admin-scope** command restores the default configuration.

By default, no BSR administrative scope is configured.

Format

c-bsr admin-scope

undo c-bsr admin-scope

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, each PIM-SM domain has only one BSR and the BSR serves all the devices in the entire PIM-SM domain. To achieve more effective management, you can divide a PIM-SM domain into multiple BSR administrative scopes and a global domain. This can reduce the workload of a single BSR and designate a private-network group address for users in a specific domain.

Each BSR administrative scope maintains a BSR that serves the multicast groups in a specified range. The multicast packets for the groups in a BSR administrative domain cannot travel across the boundary of the domain. The global domain serves all multicast groups that do not belong to any BSR administrative domains. The global domain maintains a BSR that serves multicast groups that do not belong to any BSR administrative domains.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The **c-bsr admin-scope** command needs to be run on all the devices in a PIM-SM domain.

Example

Configure a BSR administrative scope in a PIM-SM domain.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr admin-scope
```

Related Topics

10.4.6 c-bsr global (IPv6)
10.4.11 c-bsr scope

10.4.6 c-bsr global (IPv6)

Function

The **c-bsr global** command configures the router as a C-BSR in the global domain.

The **undo c-bsr global** command restores the default configuration.

By default, no C-BSR is configured in the global domain.

Format

c-bsr global [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

Parameters

Parameter	Description	Value
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in the global domain.	The value is an integer that ranging from 0 to 128. By default, the value is 126.
priority *priority*	Specifies the priority of the C-BSR in the global domain.	The value is an integer that ranges from 0 to 255. By default, it is 0. The greater the value, the higher the priority of the C-BSR.

Views

PIM-IPv6 view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A PIM-SM network is divided into multiple BSR administrative domains and a global domain. The global domain maintains a BSR that serves the remaining multicast groups.

The **c-bsr global** command configures the router as a C-BSR in the global domain. The BSR in the global domain is generated through election.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **c-bsr global** command takes effect only in a BSR administrative domain. This means that the **c-bsr global** command can be used to enable a device in a BSR administrative domain to accept multicast data for groups beyond the address range of the administrative domain.

Example

In the PIM-IPv6 view, configure the router as a C-BSR in the global domain, and then set the priority of the C-BSR to 1.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr global priority 1
```

Related Topics

10.4.5 c-bsr admin-scope (IPv6)

10.4.11 c-bsr scope

10.4.7 c-bsr hash-length (IPv6)

Function

The **c-bsr hash-length** command configures the global hash mask length of a C-BSR.

The **undo c-bsr hash-length** command restores the default configuration.

By default, the global hash mask length of a C-BSR is 126.

Format

c-bsr hash-length *hash-length*

undo c-bsr hash-length

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hash-length	Specifies the global hash mask length of a C-BSR.	The value is an integer that ranges from 0 to 128.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During dynamic RP election, if C-RPs have the same interface address mask and priority for a specified multicast group, a hash function needs to be executed to select the RP for the multicast group. The router performs hash calculation for the group address of G, C-RP address, and hash mask length of the C-RPs with the same priority and compares the hash values. The C-RP with the greatest hash value acts as the RP for G.

The hash mask length is used to adjust the hash calculation result.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-bsr** *ipv6-address hash-length* command in the PIM-IPv6 view configure the hash mask length while configuring a C-BSR address. The **c-bsr hash-length** *hash-length* command specifies the global hash mask length. If both the two commands are configured, the hash mask length configured by the **c-bsr** *ipv6-address hash-length* command takes effect.

Example

In the PIM-IPv6 view, set the global hash mask length of a C-BSR to 16.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr hash-length 16
```

Related Topics

10.4.4 c-bsr (IPv6)

 Copyright © Huawei Technologies Co., Ltd.

10.4.8 c-bsr holdtime (IPv6)

Function

The **c-bsr holdtime** command configures the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR.

The **undo c-bsr holdtime** command restores the default configuration.

By default, the timeout period during which the C-BSR waits to receive Bootstrap messages sent by the BSR is 130s.

Format

c-bsr holdtime *interval*

undo c-bsr holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which C-BSR waits for the Bootstrap message to be sent by BSR.	The value is an integer that ranges from 1 to 214748364, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, the C-BSR periodically sends Bootstrap messages carrying the IPv6 address of the C-BSR and the RP-set information. The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the elected BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command.

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer. The C-BSRs that fail in the election also refresh the timeout period of the BSR according to the hold time.
- If the timer times out, the elected BSR is considered faulty. The C-BSRs that fail the previous election elect a new BSR. Services are not interrupted.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In actual application, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime, and BS_interval must be smaller than holdtime. If C-BSRs use different BS_interval or holdtime values or if BS_interval must is larger than the holdtime, the BSR changes frequently, causing multicast forwarding errors.

Example

In the PIM-IPv6 view, set the timeout interval during which the C-BSR waits for the Bootstrap message to be sent by BSR to 150 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr holdtime 150
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.9 c-bsr interval (IPv6)

10.4.9 c-bsr interval (IPv6)

Function

The **c-bsr interval** command configures the interval at which the BSR continuously sends Bootstrap messages.

The **undo c-bsr interval** command restores the default interval.

By default, the BSR sends Bootstrap messages at a 60-second interval.

Format

c-bsr interval *interval*

undo c-bsr interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a BSR continuously sends Bootstrap messages.	The value is an integer that ranges from 1 to 107374177, in seconds.

Views

PIM-IPv6 view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a C-BSR is elected as the BSR, the C-BSR periodically sends Bootstrap messages carrying the IPv6 address of the C-BSR and the RP-set information to the network.

The interval for sending Bootstrap messages is BS_interval, which can be configured using the **c-bsr interval** command.

Other C-BSRs that fail in the election are suppressed from sending Bootstrap messages and start the timer to monitor the BSR. The timeout period of a timer is holdtime, which can be configured using the **c-bsr holdtime** command. The following applies to the timer:

- If the C-BSR receives the Bootstrap messages sent by the BSR, the C-BSR refreshes the timer.
- If the timer times out, the BSR is considered to be faulty. The C-BSRs that fail in the election triggers a new BSR election. Services are not interrupted.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

In actual applications, all C-BSRs in the same PIM domain must use the same BS_interval and holdtime, and BS_interval must be smaller than the holdtime. If C-BSRs use different BS_interval or holdtime values or BS_interval must is larger than the holdtime, the BSR changes frequently, causing multicast forwarding errors.

Example

In the PIM-IPv6 view, set the interval for the C-BSR to continuously send Bootstrap messages to 30 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr interval 30
```

Related Topics

10.4.4 c-bsr (IPv6)
10.4.8 c-bsr holdtime (IPv6)

10.4.10 c-bsr priority (IPv6)

Function

The **c-bsr priority** command configures the global C-BSR priority.

The **undo c-bsr priority** command restores the default configuration.

By default, the global C-BSR priority is 0.

Format

c-bsr priority *priority*

undo c-bsr priority

Parameters

Parameter	Description	Value
priority	Specifies the global priority of the C-BSR.	The value is an integer that ranges from 0 to 255. A larger value indicates a higher priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple C-BSRs participate in the BSR election in the PIM-SM domain, the following situations occur:

- The router with the highest priority wins in the BSR election.
- In the case of the same priority, the router with the largest IPv6 address wins in the BSR election.

To enable a C-BSR to function as the BSR, you can run the **c-bsr priority** command to increase the priority value of the C-BSR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-bsr** *ipv6-address hash-length priority* command in the PIM-IPv6 view to set the C-BSR priority while configuring a C-BSR. The **c-bsr priority**

 Copyright © Huawei Technologies Co., Ltd.

priority command sets the global priority. When both the two commands are configured, the priority configured by the **c-bsr** *ipv6-address hash-length priority* command takes effect.

Example

In the PIM-IPv6 view, set the global C-BSR priority to 5.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr priority 5
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.11 c-bsr scope

Function

The **c-bsr scope** command specifies the scope ID of the BSR administrative domain served by a C-BSR.

The **undo c-bsr scope** command restores the default configuration.

By default, no scope ID is specified for a C-BSR. That is, the C-BSR does not belong to any BSR administrative domain.

Format

c-bsr scope *scope-id* [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr scope *scope-id*

Parameters

Parameter	Description	Value
scope-id	Specifies the scope ID of the administrative domain served by a C-BSR.	The value is an integer that ranges from 3 to 15.
hash-length *hash-length*	Specifies the hash mask length of a C-BSR in a BSR administrative domain.	The value is an integer that ranges from 0 to 128. The default value is 126.
priority *priority*	Specifies the priority of a C-BSR in a BSR administrative domain.	The value is an integer that ranges from 0 to 255. The default value is 0. The greater the value, the higher the priority.

Views

PIM-IPv6 view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each BSR administrative domain is assigned a scope ID. To configure a C-BSR to serve a BSR administrative domain, use the **c-bsr scope** command to specify the scope ID of the BSR administrative domain. Packets forwarded by the C-BSR cannot travel across the boundary of the BSR administrative domain.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

In the PIM-IPv6 view, configure the router as a C-BSR in the BSR administrative domain to serve groups of Scope 5, and set the priority of the C-BSR to 10.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-bsr scope 5 priority 10
```

Related Topics

10.4.5 c-bsr admin-scope (IPv6)

10.4.6 c-bsr global (IPv6)

10.4.12 c-rp (IPv6)

Function

The **c-rp** command configures the router to advertise itself as a C-RP to the BSR.

The **undo c-rp** command restores the default configuration.

By default, no C-RP is configured.

Format

c-rp *ipv6-address* [**advertisement-interval** *adv-interval* | [**group-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* } | **scope** *scope-id*] | **holdtime** *hold-interval* | **priority** *priority*] *

undo c-rp *ipv6-address* [**scope** *scope-id*]

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of a C-RP. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the global IPv6 unicast address of the C-RP.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
advertisement-interval *adv-interval*	Specifies the interval at which the C-RP sends Advertisement messages.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the value is 60 seconds.
group-policy *basic-acl6-number*	Specifies the range of multicast groups that the C-RP serves. The range is limited through the ACL6. *basic-acl6-number* specifies the number of the basic ACL6 used to limit the range of multicast groups that the C-RP serves.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named ACL6. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
scope *scope-id*	Specifies the scope ID of the BSR administrative domain that a C-RP serves.	The value is an integer that ranges from 3 to 15.
holdtime *hold-interval*	Specifies the holdtime period during which the C-RP sends Advertisement messages. *hold-interval* specifies the time remaining before the C-RP sends Advertisement messages.	The value is an integer that ranges from 1 to 65535, in seconds. By default, the value is 150 seconds.
priority *priority*	Specifies the priority of a C-RP. The value of *priority* indicates the priority of a C-RP.	The value is an integer that ranges from 0 to 255. By default, the value is 192. The greater the value is, the lower the priority is.

Views

PIM-IPv6 view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An RP is the core of a PIM-SM (IPv6) domain, and therefore a C-RP must be able to communicate with the other devices in the PIM-SM (IPv6) domain. It is recommended that you configure a C-RP on the device that aggregates multicast traffic and reserve enough bandwidth between this device and each of the other devices in the PIM-SM (IPv6) domain.

The rules used to elect an RP from multiple C-RPs are as follows:

1. The C-RP with the longest mask length of the served group address range matching the multicast group that users have joined wins.
2. The C-RP with highest priority wins.
3. In case of the same priority, hash functions are operated. The C-RP with the greatest calculated value wins.
4. If all the preceding factors are the same, the C-RP with the largest IPv6 address wins.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **group-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* }, **priority** *priority*, **holdtime** *hold-interval* and **advertisement-interval** *adv-interval* set by using the command take precedence over the values of the global parameters configured in the PIM-IPv6 view because this command specifies an interface address. If this command is run several times on the same interface, only the latest configuration is valid.

Precautions

- If PIM-SM (IPv6) is disabled on an interface, the interface can be configured as a C-RP but the configuration does not take effect.
- **group-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* } specifies a group range. All permitted group ranges will be advertised as the ranges of groups that the RP serves. If no group range is specified for a C-RP or a C-RP is configured to serve all addresses, the C-RP serves all multicast groups.

Example

In the PIM-IPv6 view, configure an interface with the IPv6 address FC00:0:0:2001::1 as a C-RP of the PIM-SM (IPv6) domain.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-rp fc00:0:0:2001::1
```

 Copyright © Huawei Technologies Co., Ltd.

In the PIM-IPv6 view, use a named ACL6 **myacl6** to configure an interface with the IPv6 address FC00:0:0:2001::1 as a C-RP of the PIM-SM (IPv6) multicast domain ff02:0:1391::/96. Set the priority to of the C-RP to 10.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff02:0:1391:: 96
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-rp fc00:0:0:2001::1 group-policy acl6-name myacl6 priority 10
```

Related Topics

10.4.59 pim ipv6 sm

10.4.4 c-bsr (IPv6)

10.4.13 c-rp advertisement-interval (IPv6)

Function

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages.

The **undo c-rp advertisement-interval** command restores the default interval.

By default, a C-RP sends Advertisement messages at an interval of 60 seconds.

Format

c-rp advertisement-interval *interval*

undo c-rp advertisement-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a C-RP sends Advertisement messages.	The value ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All C-RPs in a PIM-SM domain periodically send Advertisement messages to the same BSR. The BSR can collect the integrated RP-Set.

 Copyright © Huawei Technologies Co., Ltd.

The **c-rp advertisement-interval** command sets the interval at which a C-RP sends Advertisement messages to the BSR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **advertisement-interval** *interval* command in the PIM-IPv6 view to configure the advertisement interval while configuring a C-RP. The **c-rp advertisement-interval** *interval* command specifies the global interval. If both the commands are configured, the interval configured by the **c-rp** *ipv6-address* **advertisement-interval** *interval* command takes effect.

Example

In the PIM-IPv6 view, set the interval at which a C-RP sends Advertisement messages to 30s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-rp advertisement-interval 30
```

Related Topics

10.4.12 c-rp (IPv6)

10.4.14 c-rp holdtime (IPv6)

10.4.14 c-rp holdtime (IPv6)

Function

The **c-rp holdtime** command configures the holdtime for a received Advertisement message on a BSR.

The **undo c-rp holdtime** command restores the default holdtime.

By default, the holdtime for a received Advertisement message is 150 seconds.

Format

c-rp holdtime *hold-interval*

undo c-rp holdtime

Parameters

Parameter	Description	Value
hold-interval	Specifies the timeout period for a BSR to wait the Advertisement message from a C-RP.	The value ranges from 1 to 65535, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When *hold-interval* is set on a C-RP, the C-RP encapsulates *hold-interval* in an Advertisement message and sends it to the BSR. The BSR obtains this *hold-interval* from the message and starts the timer. If the BSR receives no Advertisement message from the C-RP within the timeout period, the BSR regards the C-RP invalid or unreachable.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **holdtime** *hold-interval* command in the PIM-IPv6 view to configure the advertisement message holdtime while configuring a C-RP. The **c-rp holdtime** *hold-interval* configures the global holdtime for Advertisement messages. If both the two commands are configured, the holdtime configured by the **c-rp** *ipv6-address* **holdtime** *hold-interval* command takes effect.

Example

In the PIM-IPv6 view, set the holdtime for a received Advertisement message to 100s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-rp holdtime 100
```

Related Topics

10.4.12 c-rp (IPv6)
10.4.13 c-rp advertisement-interval (IPv6)

10.4.15 c-rp priority (IPv6)

Function

The **c-rp priority** command configures the global C-RP priority.

The **undo c-rp priority** command restores the default configuration.

By default, the global C-RP priority is 192.

 Copyright © Huawei Technologies Co., Ltd.

Format

c-rp priority *priority*

undo c-rp priority

Parameters

Parameter	Description	Value
priority	Specifies the global C-RP priority.	The value is an integer that ranges from 0 to 255. A larger value indicates a lower priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following rules are used to elect an RP from multiple C-RPs:

- The C-RP with the interface address that has the longest mask wins.
- The C-RP with highest priority wins.
- In case of the same priority, hash functions are operated. The C-RP with the greatest calculated value wins.
- If all the preceding factors are the same, the C-RP with the largest IPv6 address wins.

To enable a C-RP to function as an RP, you can run the **c-rp priority** command to increase the priority of the C-RP.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can also run the **c-rp** *ipv6-address* **priority** *priority* command in the PIM-IPv6 view to configure the C-RP priority while configuring a C-RP. The **c-rp priority** *priority* command specifies the global C-RP priority. If both the two commands are configured, the priority configured by the **c-rp** *ipv6-address* **priority** *priority* command takes effect.

Example

In the PIM-IPv6 view, set the global C-RP priority to 5.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] c-rp priority 5
```

Related Topics

10.4.12 c-rp (IPv6)

10.4.16 crp-policy (IPv6)

Function

The **crp-policy** command limits the range of valid C-RP addresses and the range of the multicast addresses served by a C-RP. The BSR drops the C-RP messages with addresses out of the specified range to protect valid C-RPs.

The **undo crp-policy** command restores the default configuration.

By default, the BSR does not limit the range of valid C-RP addresses and the range of the multicast groups served by a C-RP. The BSR considers all the received C-RP messages valid.

Format

crp-policy { *advanced-acl6-number* | **acl6-name** *acl6-name* }

undo crp-policy

Parameters

Parameter	Description	Value
advanced-acl6-number	Specifies the number of an advanced ACL. The ACL defines the range of the C-RP addresses and the range of the group addresses served by a C-RP.	The value is an integer that ranges from 3000 to 3999.
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a PIM SM network that uses the BSR mechanism, any router can be configured as a C-RP to serve the multicast groups in a specified range. Each C-RP sends its information to the BSR in unicast mode. The BSR summarizes all received C-RP information as the RP-set, and floods it through BSR messages on the entire network. The local router then works out the RP serving a specific multicast group address range according to the RP-set.

To protect valid C-RP from being spoofed, configure **crp-policy** on BSR routers to limit the range of valid C-RP addresses and the range of multicast group addresses served by a C-RP. Configure the same filtering rule on each C-BSR because any C-BSR can become the BSR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **crp-policy** command and the **acl ipv6 (system view)** command are used together. In the ACL6 view, you can set the valid source address range for the C-RP by specifying the **source** parameter in the **rule (advanced ACL6 view)** command. You can set the address range of multicast groups that are served by specifying the **destination** parameter in the **rule (advanced ACL6 view)** command.

If an ACL rule is specified but no C-RP address range is set, all C-RP messages are denied.

Example

Configure a C-RP policy on the C-BSR, which allows only the C-RP with the address FC00:0:0:2001::1/128 and allows the C-RP to serve only the multicast groups FF13::101/128.

```
<Huawei> system-view
[Huawei] acl ipv6 number 3100
[Huawei-acl6-adv-3100] rule permit ipv6 source fc00:0:0:2001::1 128 destination ff13::101 128
[Huawei-acl6-adv-3100] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] crp-policy 3100
```

Use a named ACL to configure a C-RP policy on the C-BSR: only FC00:0:0:2001::1/128 can function as the C-RP, and the C-RP is allowed to service only the multicast groups in the range of FF13::101/128.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:2001::1 128 destination ff13::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] crp-policy acl6-name myacl6
```

Related Topics

10.4.12 c-rp (IPv6)

10.4.17 display default-parameter pim-dm6

Function

The **display default-parameter pim-dm6** command displays default PIM-DM (IPv6) configurations.

Format

display default-parameter pim-dm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-dm6** command displays default PIM-DM (IPv6) configurations. Even if PIM-DM (IPv6) parameters are modified, the **display default-parameter pim-dm6** command still displays default parameter settings. Therefore, you can use this command to check which parameters have been modified.

Example

Display default configurations about PIM-DM (IPv6).

```
<Huawei> display default-parameter pim-dm6
  PIM6 View Default Configurations:
  ---------------------------------
  Hello-option dr-priority: 1
  Hello-option holdtime: 105 s
  Hello-option lan-delay: 500 ms
  Hello-option neighbor-tracking: disabled
  Hello-option override-interval: 2500 ms
  Holdtime assert: 180 s
  Holdtime join-prune: 210 s
  Source-lifetime: 210 s
  State-refresh-interval: 60 s
  State-refresh-rate-limit: 30 s
  State-refresh-ttl: 255
  Hello periodic interval: 30 s
  Join-prune periodic interval: 60 s

  Interface View Default Configurations:
  --------------------------------------
  Pim bfd: disabled
  Pim hello-option dr-priority: 1
  Pim hello-option holdtime: 105 s
  Pim hello-option lan-delay: 500 ms
```

 Copyright © Huawei Technologies Co., Ltd.

```
Pim hello-option neighbor-tracking: disabled
Pim hello-option override-interval: 2500 ms
Pim holdtime assert: 180 s
Pim holdtime join-prune: 210 s
Pim require-genid: disabled
Pim silent: disabled
Pim state-refresh-capable: enabled
Pim timer dr-switch-delay: disabled
Pim timer graft-retry: 3 s
Pim hello periodic interval: 30 s
Pim join-prune periodic interval: 60 s
Pim triggered-hello-delay: 5 s
Pim version: 2
Pim ipsec sa: disabled
Pim neighbor-policy: disabled
```

Table 10-56 Description of the display default-parameter pim-dm6 command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State-refresh-interval	Interval for sending State-Refresh messages. This parameter is configured by the **state-refresh-interval (IPv6)** command.
State-refresh-rate-limit	Minimum interval from when the last State-Refresh message is received to when the next State-Refresh message is received. This parameter is configured by the **state-refresh-rate-limit (IPv6)** command.
State-refresh-ttl	TTL value of the State-Refresh message. This parameter is configured by the **state-refresh-ttl (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at the shared network segment where the interface resides. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim ipv6 require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim ipv6 silent** command.
Pim state-refresh-capable	Whether State-Refresh is enabled on the interface. This parameter is configured by the **pim ipv6 state-refresh-capable** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim ipv6 timer dr-switch-delay** command.
Pim timer graft-retry	Interval for the interface to retransmit Graft messages. This parameter is configured by the **pim ipv6 timer graft-retry** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim neighbor-policy	Whether the neighbor-policy is set on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

 Copyright © Huawei Technologies Co., Ltd.

10.4.18 display default-parameter pim-sm6

Function

The **display default-parameter pim-sm6** command displays default PIM-SM (IPv6) configurations.

Format

display default-parameter pim-sm6

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-sm6** command displays default configurations about PIM-SM (IPv6) for both ASM and SSM. Even if PIM-SM (IPv6) parameters are modified, the **display default-parameter pim-sm6** command still displays default parameter settings. This command helps you determine which parameters have been modified.

Example

Display default PIM-SM (IPv6) configurations.

```
<Huawei> display default-parameter pim-sm6
 PIM6 View Default Configurations:
  --------------------------------
  Bsr-policy: disabled
  C-bsr admin-scope: disabled
  C-bsr global: disabled
  C-bsr group: none
  C-bsr hash-length: 126
  C-bsr holdtime: 130 s
  C-bsr interval: 60 s
  C-bsr priority: 0
  C-rp advertisement-interval: 60 s
  C-rp holdtime: 150 s
  C-rp priority: 192
  Crp-policy: disabled
  Bsm semantic fragmentation: disabled
  Embedded-rp: enabled
  Hello-option dr-priority: 1
  Hello-option holdtime: 105 s
  Hello-option lan-delay: 500 ms
  Hello-option neighbor-tracking: disabled
  Hello-option override-interval: 2500 ms
  Holdtime assert: 180 s
```

 Copyright © Huawei Technologies Co., Ltd.

```
Holdtime join-prune: 210 s
Probe-interval: 5 s
Register-policy: disabled
Register-suppression-timeout: 60 s
Source-lifetime: 210 s
Source-policy: disabled
Spt-switch-threshold: disabled
Ssm-policy: disabled
Static-rp:  disabled
Hello periodic interval: 30 s
Join-prune periodic interval: 60 s
Timer spt-switch: 15 s

Interface View Default Configurations:
--------------------------------------
Pim bfd: disabled
Pim bsr-boundary: disabled
Pim hello-option dr-priority: 1
Pim hello-option holdtime: 105 s
Pim hello-option lan-delay: 500 ms
Pim hello-option neighbor-tracking: disabled
Pim hello-option override-interval: 2500 ms
Pim holdtime assert: 180 s
Pim holdtime join-prune: 210 s
Pim require-genid: disabled
Pim silent: disabled
Pim timer dr-switch-delay: disabled
Pim hello periodic interval: 30 s
Pim join-prune periodic interval: 60 s
Pim triggered-hello-delay: 5 s
Pim version: 2
Pim ipsec sa: disabled
Pim join-policy: disabled
Pim neighbor-policy: disabled
```

Table 10-57 Description of the display default-parameter pim-sm6 command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Bsr-policy	Whether the valid address range of the BSR is set. This parameter is configured by the **bsr-policy (IPv6)** command.
C-bsr admin-scope	Whether the BSR administrative domain is configured. This parameter is configured by the **c-bsr admin-scope (IPv6)** command.
C-bsr global	Whether the C-BSR in the global domain is configured. This parameter is configured by the **c-bsr global (IPv6)** command.
C-bsr group	Whether the C-BSR in the BSR administrative domain is configured. This parameter is configured by the **c-bsr scope** command.
C-bsr hash-length	Global hash mask length of the C-BSR. This parameter is configured by the **c-bsr hash-length (IPv6)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
C-bsr holdtime	Waiting time for the BSR to receive the Bootstrap message. This parameter is configured by the **c-bsr holdtime (IPv6)** command.
C-bsr interval	Interval for the BSR to send Bootstrap messages. This parameter is configured by the **c-bsr interval (IPv6)** command.
C-bsr priority	Global priority of the C-BSR. This parameter is configured by the **c-bsr priority (IPv6)** command.
C-rp advertisement-interval	Interval for the C-RP to send Advertisement messages. This parameter is configured by the **c-rp advertisement-interval (IPv6)** command.
C-rp holdtime	Waiting time for the BSR to receive the Advertisement message. This parameter is configured by the **c-rp holdtime (IPv6)** command.
C-rp priority	Global priority of the C-RP. This parameter is configured by the **c-rp priority (IPv6)** command.
Crp-policy	Whether the valid address range of the C-RP and the range of multicast groups that the C-RP serves are set. This parameter is configured by the **crp-policy (IPv6)** command.
Bsm semantic fragmentation	Whether the BSR fragmentation is enabled. This parameter is configured by the **bsm semantic fragmentation (IPv6)** command.
Embedded-rp	Whether the embedded RP is enabled. This parameter is configured by the **embedded-rp** command.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Probe-interval	Interval for sending Probe messages (empty Register messages) to the RP. This parameter is configured by the **probe-interval (IPv6)** command.
Register-policy	Whether the rule for filtering Register messages is configured. This parameter is configured by the **register-policy (IPv6)** command.
Register-suppression-timeout	Time period for holding the register-suppression state. This parameter is configured by the **register-suppression-timeout (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv6)** command.
Spt-switch-threshold	Whether the threshold of the multicast packet rate that triggers the switch from the RPT to the SPT is configured. This parameter is configured by the **spt-switch-threshold (IPv6)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv6)** command.
Static-rp	Whether the static RP is configured. This parameter is configured by the **static-rp (IPv6)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.
Timer spt-switch	Whether the interval for checking whether the multicast packet rate exceeds the threshold before the switchover from RPT to SPT is configured. This parameter is configured by the **timer spt-switch (IPv6)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim bsr-boundary	Whether the PIM boundary is configured on the interface. This parameter is configured by the **pim ipv6 bsr-boundary** command.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim ipv6 require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim ipv6 silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim ipv6 timer dr-switch-delay** command.
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim ipv6 join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

10.4.19 display default-parameter pim-ssm6

Function

The **display default-parameter pim-ssm6** command displays default configurations of PIM-SM (IPv6) for SSM.

Format

display default-parameter pim-ssm6

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display default-parameter pim-ssm6** command displays default configuration of PIM-SM (IPv6) for SSM. Even if the configuration of PIM-SM (IPv6) for SSM is modified, the **display default-parameter pim-ssm6** command still displays default parameter settings. This command helps you determine which parameters have been modified.

Example

Display default configuration of PIM-SM (IPv6) for SSM.

```
<Huawei> display default-parameter pim-ssm6
  PIM6 View Default Configurations:
  ---------------------------------
  Hello-option dr-priority: 1
  Hello-option holdtime: 105 s
  Hello-option lan-delay: 500 ms
  Hello-option neighbor-tracking: disabled
  Hello-option override-interval: 2500 ms
  Holdtime assert: 180 s
  Holdtime join-prune: 210 s
  Probe-interval: 5 s
  Register-policy: disabled
  Register-suppression-timeout: 60 s
  Source-lifetime: 210 s
  Source-policy: disabled
  Ssm-policy: disabled
  Hello periodic interval: 30 s
  Join-prune periodic interval: 60 s

  Interface View Default Configurations:
  --------------------------------------
  Pim bfd: disabled
  Pim hello-option dr-priority: 1
  Pim hello-option holdtime: 105 s
  Pim hello-option lan-delay: 500 ms
  Pim hello-option neighbor-tracking: disabled
  Pim hello-option override-interval: 2500 ms
  Pim holdtime assert: 180 s
  Pim holdtime join-prune: 210 s
  Pim require-genid: disabled
  Pim silent: disabled
  Pim timer dr-switch-delay: disabled
  Pim hello periodic interval: 30 s
  Pim join-prune periodic interval: 60 s
  Pim triggered-hello-delay: 5 s
  Pim version: 2
  Pim ipsec sa: disabled
  Pim join-policy: disabled
  Pim neighbor-policy: disabled
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-58 Description of the display default-parameter pim-ssm6 command output

Item	Description
PIM6 View Default Configurations	Default configurations in the PIM-IPv6 view.
Hello-option dr-priority	Priority for DR election. This parameter is configured by the **hello-option dr-priority (IPv6)** command.
Hello-option holdtime	Time period for the neighbor to hold the reachable state. This parameter is configured by the **hello-option holdtime (IPv6)** command.
Hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment. This parameter is configured by the **hello-option lan-delay (IPv6)** command.
Hello-option neighbor-tracking	Whether neighbor tracking is enabled. This parameter is configured by the **hello-option neighbor-tracking (IPv6)** command.
Hello-option override-interval	Interval for sending Prune Override messages. This parameter is configured by the **hello-option override-interval (IPv6)** command.
Holdtime assert	Time period for holding the Assert state. This parameter is configured by the **holdtime assert (IPv6)** command.
Holdtime join-prune	Time period for holding the Join or Prune state. This parameter is configured by the **holdtime join-prune (IPv6)** command.
Source-lifetime	Timeout period of an (S, G) entry. This parameter is configured by the **source-lifetime (IPv6)** command.
Source-policy	Whether the rule for filtering multicast sources is configured. This parameter is configured by the **source-policy (IPv6)** command.
Ssm-policy	Whether the SSM group address range is set. This parameter is configured by the **ssm-policy (IPv6)** command.
Hello periodic interval	Interval for sending Hello messages. This parameter is configured by the **timer hello (IPv6)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Join-prune periodic interval	Interval for sending Join/Prune messages. This parameter is configured by the **timer join-prune (IPv6)** command.
Interface View Default Configurations	Default configurations in the interface view.
Pim hello-option dr-priority	Priority for DR election on the interface. This parameter is configured by the **pim ipv6 hello-option dr-priority** command.
Pim hello-option holdtime	Time period for the neighbor on the interface to hold the reachable state. This parameter is configured by the **pim ipv6 hello-option holdtime** command.
Pim hello-option lan-delay	Delay in transmitting Prune messages at a shared network segment on the interface. This parameter is configured by the **pim ipv6 hello-option lan-delay** command.
Pim hello-option neighbor-tracking	Whether neighbor tracking is enabled on the interface. This parameter is configured by the **pim ipv6 hello-option neighbor-tracking** command.
Pim hello-option override-interval	Interval for the interface to send Prune Override messages. This parameter is configured by the **pim ipv6 hello-option override-interval** command.
Pim holdtime assert	Time period for the interface to hold the Assert state. This parameter is configured by the **pim ipv6 holdtime assert** command.
Pim holdtime join-prune	Time period for the interface to hold the Join or Prune state. This parameter is configured by the **pim ipv6 holdtime join-prune** command.
Pim require-genid	Whether the received Hello message is required to carry the Generation ID. This parameter is configured by the **pim ipv6 require-genid** command.
Pim silent	Whether PIM Silent is enabled on the interface. This parameter is configured by the **pim ipv6 silent** command.
Pim timer dr-switch-delay	Whether the DR switch delay is set on the interface. This parameter is configured by the **pim ipv6 timer dr-switch-delay** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pim hello periodic interval	Interval for the interface to send Hello messages. This parameter is configured by the **pim ipv6 timer hello** command.
Pim join-prune periodic interval	Interval for the interface to send Join/Prune messages. This parameter is configured by the **pim ipv6 timer join-prune** command.
Pim triggered-hello-delay	Maximum delay for the interface to send Hello messages. This parameter is configured by the **pim ipv6 triggered-hello-delay** command.
Pim version	Version of PIM enabled on the interface.
Pim join-policy	Whether the join-policy is configured on the interface. This parameter is configured by the **pim ipv6 join-policy** command.
Pim neighbor-policy	Whether the neighbor-policy is configured on the interface. This parameter is configured by the **pim ipv6 neighbor-policy** command.

10.4.20 display pim ipv6 bsr-info

Function

The **display pim ipv6 bsr-info** command displays the BSRs in a PIM-SM (IPv6) domain.

Format

display pim ipv6 bsr-info

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check BSR configuration on a PIM-SM (IPv6) network.

Example

Display information about BSR in the current PIM-SM (IPv6) domain. If the router is configured with C-BSR, information about the elected BSR and C-BSR is displayed.

```
<Huawei> display pim ipv6 bsr-info
VPN-Instance: public net
 Elected AdminScoped BSR Count: 0
 Elected BSR Address: FC00:0:0:2004::2
     Priority: 0
     Hash mask length: 128
     State: Elected
     Scope: 5
     Uptime: 00:00:07
     Next BSR message scheduled at: 00:00:53
     C-RP Count: 0
 Candidate AdminScoped BSR Count: 0
 Candidate BSR Address: FC00:0:0:2004::2
     Priority: 0
     Hash mask length: 128
     State: Elected
     Scope: 5
     Wait to be BSR: 0
```

Table 10-59 Description of the display pim ipv6 bsr-info command output

Item	Description
Elected AdminScoped BSR Count	number of elected AdminScoped BSRs.
Elected BSR Address	IPv6 address of the elected BSR.
Priority	Priority of the BSR.
Hash mask length	Mask length in the RP hash calculation.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of the BSR. ● Accept Preferred: No C-BSR is configured on the device and another device functions as a BSR and does not time out. ● Accept Any: No C-BSR is configured on the device and the current BSR times out (applicable to the situation that a BSR administrative domain is set) ● Candidate: A C-BSR is configured on a device and another device functions as a BSR. ● Pending: The device changes from the non-BSR state to the BSR state or a C-BSR is configured on the device and the current BSR times out. ● Elected: The device is elected as the BSR.
Scope	Scope ID of the BSR administrative domain served by a BSR. Not scoped indicates that the BSR is not an AdminScoped BSR.
Uptime	Period during which the BSR exists.
Next BSR message scheduled at	Period after which the next BSR message is sent. BSR messages are sent only when the timer maintained by the elected BSR times out.
C-RP Count	Number of RPs learned through the BSR.
Candidate AdminScoped BSR Count	Number of AdminScoped C-BSRs.
Candidate BSR Address	IPv6 Address of the C-BSR.
Wait to be BSR	Whether the current C-BSR is valid. The values are as follows: ● 0: The current C-BSR is valid. The current C-BSR takes part in the BSR election. ● 1: The current C-BSR is invalid. The current C-BSR does not take part in the BSR election. When the number of C-BSRs configured on the router exceeds the threshold, the value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.4.4 c-bsr (IPv6)
10.4.12 c-rp (IPv6)

10.4.21 display pim ipv6 claimed-route

Function

The **display pim ipv6 claimed-route** command displays the unicast routing information used by PIM (IPv6).

Format

display pim ipv6 claimed-route [*ipv6-source-address*]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is in hexadecimal format.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim ipv6 claimed-route** command displays the unicast routes used by PIM (IPv6), such as the RPF neighbors, detailed information about interfaces, route types, and route selection policy.

Example

Display the unicast route of multicast source FC00:0:0:2001::2.

```
<Huawei> display pim ipv6 claimed-route fc00:0:0:2001::2
VPN-Instance: public net
Multicast load-splitting rule: source-group
RPF information about: FC00:0:0:2001::2 in PIM-SM routing table
    RPF interface: GigabitEthernet1/0/0, RPF neighbor: FE80::A01:100:1
    Referenced route/mask: FC00:0:0:2001::/64
    Referenced route type: igp
    The (S, G) or (*, G) list dependent on this route entry
    (FC00:0:0:2001::2, FF03::1)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-60 Description of the display pim ipv6 claimed-route command output

Item	Description
Multicast load-splitting rule	Mode in which multi-cast loads are split. The following policies apply: ● group: multicast group-based load splitting ● source: multicast source-based load splitting ● source-group: multicast source and group-based load splitting ● stable-preferred: stable-preferred load splitting ● balance-preferred: balance-preferred load splitting
RPF information about: FC00:0:0:2001::2 in PIM-SM routing table	RPF routing information with the source address of FC00:0:0:2001::2 in the PIM-SM (IPv6) routing table
RPF interface	RPF interface in a routing entry.
RPF neighbor	RPF neighbor in a routing entry.
Referenced route/mask	Route/mask used by PIM.
Referenced route type	Type of a route.
The (S, G) or (*, G) list dependent on this route entry	List of multicast entries based on RPF routes.

10.4.22 display pim ipv6 control-message counters

Function

The **display pim ipv6 control-message counters** command displays the number of sent and received PIM (IPv6) control messages.

Format

display pim ipv6 control-message counters message-type { **probe** | **register** | **register-stop** | **crp** }

display pim ipv6 control-message counters [**message-type** { **assert** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** | **bsr** } | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
message-type	Indicates the types of PIM control message.	-
probe	Indicates the Probe message.	-
register	Indicates the Register message.	-
register-stop	Indicates the Register-stop message.	-
crp	Indicates the C-RP message.	-
assert	Indicates the Assert message.	-
graft	Indicates the Graft message.	-
graft-ack	Indicates the Graft-ack message.	-
hello	Indicates the Hello message.	-
join-prune	Indicates the Join/Prune message.	-
state-refresh	Indicates the State-refresh message.	-
bsr	Indicates the BSR message.	-
interface *interface-type interface-number*	Indicates the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When multicast forwarding fails on a PIM (IPv6) network, run the **display pim control-message counters** command to view statistics about protocol packets. The command output helps you locate faults.

Example

Display the number of PIM (IPv6) control messages that were sent and received on the device.

```
<Huawei> display pim ipv6 control-message counters
VPN-Instance: public net
 Register* - Register Anycast-RP, Probe* - Probe Anycast-RP
 ----------------------------------------------------------------------------
 PIM global control-message counters:
 Message Type     Received        Sent          Invalid        Filtered
 Register         0               0             0              0
 Register-Stop    0               0             0              0
 Probe            0               0             0              0
 C-RP             0               0             0              0
 Register*        0               0             0              0
 Probe*           0               0             0              0
```

```
PIM control-message counters for interface: GigabitEthernet1/0/1
Message Type     Received         Sent            Invalid         Filtered
Assert           0                0               0               0
Graft            0                0               0               0
Graft-Ack        0                0               0               0
Hello            0                35              0               0
Join-prune       0                0               0               0
State-Refresh    0                0               0               0
BSR              0                0               0               0
```

Table 10-61 Description of the display pim ipv6 control-message counters command output

Item	Description
VPN-Instance	VPN instance to which the statistics of PIM messages belong.
PIM global control-message counters	Number of PIM control messages in the public network.
PIM control-message counters for interface	Name of the interface for collecting statistics on PIM control messages
Message Type	Type of the control message.
Received	Number of control messages received by the current interface.
Sent	Number of control messages sent by the current interface.
Invalid	Number of invalid control packets.
Filtered	Number of control messages filtered out by the current interface.
Register	Number of Register messages.
Register-Stop	Number of Register-Stop messages.
Probe	Number of Probe messages.
C-RP	Number of Advertisement messages.
Assert	Number of Assert messages.
Graft	Number of Graft messages.
Graft-Ack	Number of Graft-Ack messages.
Hello	Number of Hello messages.
Join-prune	Number of Join/Prune messages.
State-Refresh	Number of State-Refresh messages.
BSR	Number of Bootstrap messages.
Register*	Number of Register messages for anycast RP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Probe*	Number of Probe messages for anycast RP.

Related Topics

10.4.70 reset pim ipv6 control-message counters

10.4.23 display pim ipv6 grafts

Function

The **display pim ipv6 grafts** command displays the information about unacknowledged PIM-DM (IPv6) Graft messages.

Format

display pim ipv6 grafts

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In PIM-DM (IPv6), after sending the Graft message, the router needs to wait to receive the Graft-Ack message from the upstream device.

You can run the **display pim ipv6 grafts** command to view the information about the PIM-DM (IPv6) Graft messages sent but unacknowledged.

Example

Display the unacknowledged PIM-DM (IPv6) graft messages.

```
<Huawei> display pim ipv6 grafts
Source                  Group                   Expire    RetransmitIn
fc00:0:0:2001::2          ff03::101               00:02:52  00:00:02
```

Table 10-62 Description of the display pim ipv6 grafts command output

Item	Description
Source	Multicast source address.

Item	Description
Group	Multicast group address.
Expire	Timeout period of an (S, G) entry.
RetransmitIn	Amount of time before the next Graft message is transmitted.

10.4.24 display pim ipv6 interface

Function

The **display pim ipv6 interface** command displays information about PIM (IPv6) on an interface.

Format

display pim ipv6 interface [*interface-type interface-number* | **up** | **down**] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Indicates the type and number of an interface.	-
up	Indicates that the IPv6 status is Up on the PIM interface.	-
down	Indicates that the IPv6 status is Down on the PIM interface.	-
verbose	Indicates detailed information about a PIM (IPv6) interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

An interface enabled with PIM (IPv6) is called a PIM (IPv6) interface. The **display pim ipv6 interface** command is used to display information about PIM (IPv6) interfaces, including status of the PIM (IPv6) interface, the number of PIM (IPv6) neighbors, interval at which Hello messages are sent, DR priority, and DR address.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display PIM (IPv6) information on GE1/0/0.

```
<Huawei> display pim ipv6 interface gigabitethernet 1/0/0
 VPN-Instance: public net
 Interface      State   NbrCnt   HelloInt   DR-Pri     DR-Address
 GE1/0/0         up      0        30         1          FE80::2E0:3FFF:FE27:AE01(local)
```

Table 10-63 Description of the display pim ipv6 interface command output

Item	Description
Interface	Name of the PIM (IPv6) interface.
State	Status of the PIM (IPv6) interface, up or down.
NbrCnt	Number of PIM (IPv6) neighbors on the interface.
HelloInt	Interval for sending Hello messages, in seconds.
DR-Pri	DR priority.
DR-Address	DR address.

Display detailed information about PIM (IPv6) on GE1/0/0.

```
<Huawei> display pim ipv6 interface gigabitethernet 1/0/0 verbose
 VPN-Instance: public net
 Interface: GigabitEthernet1/0/0, FE80::2E0:3FFF:FE27:AE01
     PIM version: 2
     PIM mode: Sparse
     PIM state: up
     PIM DR: FE80::2E0:3FFF:FE27:AE01 (local)
     PIM DR Priority (configured): 1
     PIM neighbor count: 0
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM hello override interval (negotiated): 2500 ms
     PIM hello override interval (configured): 2500 ms
     PIM Silent: disabled
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0x18FF94EC
     PIM require-GenID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     PIM BFD: disabled
     PIM dr-switch-delay timer : not configured
     Number of routers on link not using DR priority: 0
     Number of routers on link not using LAN delay: 0
     Number of routers on link not using neighbor tracking: 1
     ACL of PIM neighbor policy: myacl6
     ACL of PIM ASM join policy: 2000
     ACL of PIM SSM join policy: -
     ACL of PIM join policy: -
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-64 Description of the display pim ipv6 interface verbose command output

Item	Description
PIM version	Version number of PIM (IPv6) enabled on the interface.
PIM mode	PIM mode.
PIM state	Status of the PIM (IPv6) interface, up or down.
PIM DR	DR address on the interface.
PIM DR Priority (configured)	Configured DR priority on the interface.
PIM neighbor count	Number of PIM (IPv6) neighbors on the interface.
PIM hello interval	Interval for sending Hello messages.
PIM LAN delay (negotiated)	Negotiated delay for transmitting packets on the interface.
PIM LAN delay (configured)	Configured delay for transmitting packets on the interface.
PIM hello override interval (negotiated)	Negotiated override interval on the interface.
PIM hello override interval (configured)	Configured override interval on the interface.
PIM Silent	Whether the PIM Silent (IPv6) function is enabled on the interface.
PIM neighbor tracking (negotiated)	Whether the PIM (IPv6) neighbor tracking function is enabled on the interface after negotiation.
PIM neighbor tracking (configured)	Whether the PIM (IPv6) neighbor tracking function is configured on the interface.
PIM generation ID	Generation ID option on the interface.
PIM require-GenID	Whether the function of rejecting the Hello messages without the Generation ID option is enabled.
PIM hello hold interval	Interval for the receiver of the Hello message to keep its neighbor reachable.
PIM assert hold interval	Interval for sending Assert messages.
PIM triggered hello delay	Maximum random delay for triggering Hello messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PIM J/P interval	Interval for the interface to send Join/Prune messages.
PIM J/P hold interval	Period for holding the Join/Prune status on the interface.
PIM BSR domain border	Whether the BSR domain border is configured on the interface.
PIM dr-switch-delay timer	DR switching delay.
Number of routers on link not using DR priority	Number of routers that do not use DR priority in all the network segments connected to the interface.
Number of routers on link not using LAN delay	Number of routers that do not use LAN delay in all the network segments connected to the interface.
Number of routers on link not using neighbor tracking	Number of routers that are not enabled with the neighbor tracing function in the network segment where the interface resides.
ACL of PIM neighbor policy	Neighbor filtering policy configured on the interface.
ACL of PIM ASM join policy	ASM Join information filtering policy configured on the interface.
ACL of PIM SSM join policy	SSM Join information filtering policy configured on the interface.
ACL of PIM join policy	Join information filtering policy configured on the interface.

Related Topics

10.4.26 display pim ipv6 neighbor

10.4.25 display pim ipv6 invalid-packet

Function

The **display pim ipv6 invalid-packet** command displays statistics about invalid PIM (IPv6) messages received by a device and details of these messages.

Format

display pim ipv6 invalid-packet [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **hello** | **join-prune** | **graft** | **graft-ack** | **state-refresh** }] *

display pim ipv6 invalid-packet message-type { **crp** | **register** | **register-stop** }

display pim ipv6 invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about invalid PIM (IPv6) messages received by a specified interface. *interface-type interface-number* specifies the interface type and interface number.	-
message-type	Displays statistics about invalid PIM (IPv6) messages of a specific type.	-
assert	Displays statistics about invalid Assert messages.	-
bsr	Displays statistics about invalid BSR messages.	-
hello	Displays statistics about invalid Hello messages.	-
join-prune	Displays statistics about invalid Join/Prune messages.	-
graft	Displays statistics about invalid Graft messages.	-
graft-ack	Displays statistics about invalid Graft-Ack messages.	-
state-refresh	Displays statistics about invalid State-Refresh messages.	-
crp	Displays statistics about invalid C-RP messages.	-
register	Displays statistics about invalid Register messages.	-
register-stop	Displays statistics about invalid Register-Stop messages.	-
packet-number	Displays details of a specified number of invalid PIM (IPv6) messages recently received.	The value is an integer that ranges from 1 to 100. By default, details of all the invalid PIM (IPv6) messages currently stored are displayed.
verbose	Displays details of invalid PIM (IPv6) messages.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs on an PIM (IPv6) network, use the **display pim ipv6 invalid-packet** command to check statistics and details about invalid PIM (IPv6) packets. The command output can help you locate the fault.

If PIM (IPv6) entries fail to be generated on a multicast network, you can run the **display pim ipv6 invalid-packet** command first to check whether devices have received invalid PIM (IPv6) messages. If the command output contains statistics about invalid PIM (IPv6) messages, run the **display pim ipv6 invalid-packet** [*packet-number*] **verbose** command to view details of invalid PIM (IPv6) messages to locate the fault.

Example

Display statistics about invalid PIM (IPv6) messages received by a device.

```
<Huawei> display pim ipv6 invalid-packet

            Statistics of invalid packets for public net:
-----------------------------------------------------------------------
PIM General invalid packet:
Invalid PIM Version     : 0          Invalid PIM Type        : 0
Fault Length            : 0          Bad Checksum            : 0

PIM Register invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0

AnycastRP Register invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0

PIM Register-Stop invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Dest Addr       : 0          IP Source not RP        : 0

PIM CRP invalid packet:
Invalid Dest Addr       : 0          Invalid CRP Addr        : 0
Fault Length            : 0          CRP Adv Fault Length    : 0
Invalid Multicast Group : 0

PIM Assert invalid packet:
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0
Invalid Multicast Source: 0          Invalid Multicast Group : 0

PIM BSR invalid packet:
Bad Payload             : 0          Fault Length            : 0
Bad Scope Mask          : 0          Invalid Multicast Group : 0
Not CBSR But BSR        : 0          Invalid BSR Addr        : 0
Fault Hash Length       : 0          Invalid IP Source Addr  : 0

PIM Hello invalid packet:
Invalid Addr List       : 0          Fault Length            : 0
Bad Holdtime Length     : 0          Bad LanPruneDelay Length: 0
```

```
Bad DrPriority Length   : 0          Bad GenID Length        : 0
Invalid Dest Addr       : 0          Invalid IP Source Addr  : 0

PIM Join/Prune invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Invalid Dest Addr       : 0          Fault Length            : 0

PIM Graft invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Fault Length            : 0

PIM Graft-Ack invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Up Neighbor     : 0          Invalid IP Source Addr  : 0
Fault Length            : 0

PIM State Refresh invalid packet:
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Originator Addr : 0          Fault Length            : 0
-----------------------------------------------------------------
```

Table 10-65 Description of the display pim ipv6 invalid-packet command output

Item	Description
PIM General invalid packet	Number of general invalid PIM (IPv6) messages.
Invalid PIM Version	Number of messages with invalid PIM (IPv6) version.
Invalid PIM Type	Number of messages with invalid PIM (IPv6) message type.
Fault Length	Number of messages with invalid lengths.
Bad Checksum	Number of messages with invalid checksum.
PIM Register invalid packet	Number of PIM Register messages.
Invalid Multicast Source	Number of messages with invalid multicast source addresses.
Invalid Multicast Group	Number of messages with invalid multicast group addresses.
Invalid Dest Addr	Number of messages with invalid destination addresses.
AnycastRP Register invalid packet	Statistics about invalid Register packets in the anycast-RP scenario.
PIM Register-Stop invalid packet	Number of invalid Register-Stop messages.
IP Source not RP	Number of messages whose source addresses are not the RP address.
PIM CRP invalid packet	Number of invalid C-RP messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Invalid CRP Addr	Number of messages with invalid C-RP addresses.
CRP Adv Fault Length	Number of messages with CRP Adv fields of invalid lengths.
PIM Assert invalid packet	Number of invalid Assert messages.
Invalid IP Source Addr	Number of messages with invalid source addresses.
PIM BSR invalid packet	Number of invalid BSR messages.
Bad Payload	Number of messages with invalid payloads.
Bad Scope Mask	Number of messages with invalid scope masks.
Not CBSR But BSR	Number of messages received from non-C-BSRs.
Invalid BSR Addr	Number of messages with invalid BSR addresses.
Fault Hash Length	Number of messages whose hash mask fields of invalid lengths.
PIM Hello invalid packet	Number of invalid Hello messages.
Invalid Addr List	Number of messages with invalid address lists.
Bad Holdtime Length	Number of messages whose Holdtime fields are of invalid lengths.
Bad LanPruneDelay Length	Number of messages whose LanPruneDelay fields are of invalid lengths.
Bad DrPriority Length	Number of messages with DrPriority fields of invalid lengths.
Bad GenID Length	Number of messages with GenerationID fields of invalid lengths.
PIM Join/Prune invalid packet	Number of invalid Join/Prune messages.
Invalid Up Neighbor	Number of messages with invalid upstream neighbors.
PIM Graft invalid packet	Number of invalid Graft messages.
PIM Graft-Ack invalid packet	Number of invalid Graft-Ack messages.
PIM State Refresh invalid packet	Number of invalid State-Refresh messages.
Invalid Originator Addr	Number of messages with invalid Originator address.

 Copyright © Huawei Technologies Co., Ltd.

Display details of one invalid PIM (IPv6) message recently received lately.

```
<Huawei> display pim ipv6 invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Interface          :  GigabitEthernet1/0/0
Time               :  2012-06-01 20:04:35 UTC-08:00
Message Length     :  26
Invalid Type       :  Invalid Multicast Source
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00
0010: 00 00 80 00 00 64 00 00 00 00
-----------------------------------------------------
```

Table 10-66 Description of the display pim ipv6 invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details about invalid PIM (IPv6) messages.
Packet information (Index 1)	Sequence number of an invalid PIM (IPv6) message (numbered in the opposite order).
Interface	Number of interfaces that receive the invalid PIM (IPv6) message.
Time	Time when the invalid SPT switch message was received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST The format UTC±HH:MM indicates that a time zone was configured with the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid PIM (IPv6) message.
Invalid Type	Type of the invalid PIM (IPv6) message.
0000: 25 00 96 77 01 00 00 20 e1 01 01 01 01 00 e0 00 0010: 00 00 80 00 00 64 00 00 00 00	Contents of the invalid PIM (IPv6) message.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.8.12 multicast ipv6 invalid-packet

10.4.26 display pim ipv6 neighbor

Function

The **display pim ipv6 neighbor** command displays information about PIM (IPv6) neighbors.

Format

display pim ipv6 neighbor [*ipv6-link-local-address* | **interface** *interface-type interface-number* | **verbose**] *

Parameters

Parameter	Description	Value
ipv6-link-local-address	Specifies the IPv6 link-local address of a neighbor.	The value ranges from FE80:: to FE80:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, in hexadecimal notation.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
verbose	Indicates the details of PIM neighbors.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pim ipv6 neighbor** command displays PIM (IPv6) neighbor information, including the number of PIM (IPv6) neighbors and DR priorities of neighbors. You can adjust PIM (IPv6) neighbor relationships according to the command output.

Example

Display detailed information about PIM (IPv6) neighbors on GE1/0/0.

```
<Huawei> display pim ipv6 neighbor interface gigabitethernet 1/0/0 verbose
 VPN-Instance: public net
```

```
 Total Number of Neighbors on this interface  = 1

Neighbor: FE80::FFE0:FFFF:FE4A:8E04
    Interface: GigabitEthernet1/0/0
    Uptime: 00:01:18
    Expiry time: 00:01:31
    DR Priority: 1
    Generation ID: 0x7751638D
    Holdtime: 105 s
    LAN delay: 500 ms
    Override interval: 2500 ms
    Neighbor tracking: disabled
    PIM BFD-session: N
    Neighbor Secondary Address(es):
    FC00:0:0:2004::2
```

Table 10-67 Description of the display pim ipv6 neighbor command output

Item	Description
Total Number of Neighbors on this interface	Total number of PIM (IPv6) neighbors on an interface.
Neighbor	Address of a PIM (IPv6) neighbor.
Interface	Interface where the PIM (IPv6) neighbor resides.
Uptime	How long has the PIM (IPv6) neighbor been in Up state.
Expiry time	How soon the PIM (IPv6) neighbor will time out.
DR Priority	DR priority of the PIM (IPv6) neighbor.
Generation ID	Indicates the randomly generated 32-bit value of PIM (IPv6) neighbor.
Holdtime	Keepalive period of the PIM (IPv6) neighbor.
LAN delay	Delay in transmitting Prune messages.
Override interval	Interval for overriding the Prune action.
Neighbor tracking	Whether the neighbor tracking neighbor function is enabled.
PIM BFD-session	Whether a BFD session is set up.
Neighbor Secondary Address (es)	IPv6 address of the neighbor.

Related Topics

10.4.24 display pim ipv6 interface

10.4.27 display pim ipv6 routing-table

Function

The **display pim ipv6 routing-table** command displays the PIM (IPv6) multicast routing table.

Format

display pim ipv6 routing-table [*ipv6-source-address* [**mask** *mask-length*] | *ipv6-group-address* [**mask** *mask-length*] | **flags** *flag-value* | **fsm** | **incoming-interface** { *interface-type interface-number* | **register** } | **mode** { **dm** | **sm** | **ssm** } | **outgoing-interface** { **exclude** | **include** | **match** } { *interface-type interface-number* | **none** | **register** }] * [**outgoing-interface-number** [*number*]]

display pim ipv6 routing-table brief [*ipv6-source-address* [**mask** *mask-length*] | *ipv6-group-address* [**mask** *mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** }] *

NOTE

If you specify the **register** keyword before **mode**, the value of **mode** can only be **sm**.

After the PIM mode is set to **dm** or **ssm**, the **register** keyword cannot be specified in the command.

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-group-address	Specifies the IPv6 address of a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
mask *mask-length*	Specifies the mask length of a multicast source or group.	The value is an integer. The mask length of a multicast source ranges from 0 to 128. The mask length of a multicast group ranges from 8 to 128.
flags *flag-value*	Displays of routing entries of a specified type. *flag-value* specifies the flag of a routing entry.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
fsm	Displays detailed information about the finite state machine (FSM).	-
incoming-interface	Displays the routing entry with the specified upstream interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Displays the register interface.	-
dm	Displays PIM-DM (IPv6) routing entries.	-
sm	Displays PIM-SM (IPv6) routing entries.	-
ssm	Displays PIM-SSM (IPv6) routing entries.	-
outgoing-interface { **exclude** | **include** | **match** }	Displays the routing entries with or without a specified outbound interface. ● exclude: displays the entries that do not contain the specified interface. ● include: displays the entries that contain the specified interface. ● match: displays the entries match the specified interface.	-
none	Displays the routing entry without the downstream interface.	-
outgoing-interface-number	Displays the number of the outbound interfaces of routing entries.	-
number	Specifies the number of the outbound interfaces to be queried.	The value is an integer that ranges from 0 to 2048.
brief	Displays only the name of upstream interface and the number of downstream interfaces of routing entries.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to:

- Check whether PIM (IPv6) has been configured successfully on the network.
- Check the inbound interfaces, outbound interfaces, flags, and other information in the routing entries to identify failure points when forwarding errors occur on the PIM (IPv6) network.

The PIM (IPv6) routing table includes both (*, G) and (S, G) entries. (*, G) entries are used to set up a rendezvous point tree (RPT), and (S, G) entries are used to set up a shortest path tree (SPT).

Table 10-68 lists the values of the **flags** *flag-value* parameter.

Table 10-68 Values of the *flag-value* parameter

Item	Description
act	Indicates that the multicast routing entry at which actual data arrives exists.
del	Indicates the multicast routing entry to be deleted.
exprune	Indicates that the entry on the RPT is pruned and no receiver on the RPT requests the information sent by the source.
ext	Indicates routing entries that contain downstream interfaces provided by other multicast routing protocols.
loc	Indicates routing entries on the router directly connected to the network segment where the source resides.
niif	Indicates routing entries with unknown upstream interfaces.
nonbr	Indicates that the routing entry of the upstream neighbor address (link-local address) towards the RP or the source is not found.
none	Indicates routing entries without any flag.
rpt	Indicates the routing entries that are on the RPT but do not use the RPT data.
sg_rcvr	Indicates that the (S, G) receiver of S exists on the local router and PIM (IPv6) is the owner of the downstream interface.
sgjoin	Indicates that the (S, G) receiver of S exists on the local router and PIM (IPv6) is not the owner of the downstream interface.
spt	Indicates routing entries on the shortest path tree (SPT).
swt	Indicates routing entries during the SPT switchover.
upchg	Indicates a route change has occurred. The current entry uses the original upstream interface to forward data and waits for data received from a new interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
wc	Indicates a (*, G) entry.

Example

Display the PIM (IPv6) multicast routing table.

```
<Huawei> display pim ipv6 routing-table
 VPN-Instance: public net
 Total 1 (*, G) entry; 1 (S, G) entry

 (*, FFE3::1)
     RP: FC00:0:0:1::1
     Protocol: pim-sm, Flag: WC
     UpTime: 00:57:31
     Upstream interface: NULL
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: static, UpTime: 00:57:31, Expires: never

 (FC00:0:0:2001::2, FFE3::1)
     Protocol: pim-sm, Flag: SWT ACT
     UpTime: 00:04:24
     Upstream interface: GigabitEthernet2/0/0
         Upstream neighbor: FE80::A01:100:1
         RPF prime neighbor: FE80::A01:100:1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: GigabitEthernet1/0/0
             Protocol: pim-sm, UpTime: 00:04:24, Expires:  -
```

Table 10-69 Description of the display pim ipv6 routing-table command output

Item	Description
Total 1 (*, G) entry; 1 (S, G) entry	Total number of the (S, G) entries and (*, G) entries in the PIM routing table.
(*, FFE3::1)	(*, G) entry in the PIM routing table.
RP	RP address.
Protocol	Type of PIM (IPv6) protocols, PIM-DM (IPv6), PIM-SM (IPv6), or PIM-SSM (IPv6).
Flag	Flag of a (S, G) entry or (*, G) entry in the PIM (IPv6) routing table.
UpTime	Lifetime of an interface.
Upstream interface	Upstream interface of a (S, G) entry or (*, G) entry.
Upstream neighbor	Upstream neighbor of a (S, G) entry or (*, G) entry.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RPF prime neighbor	RPF neighbor of a (S, G) entry or (*, G) entry. ● For a (*, G) entry, when the local device is an RP, the RPF neighbor is Null. ● For a (S, G) entry, when the local device is directly connected to the multicast source, the RPF neighbor is Null.
Downstream interface(s) information	Information about downstream interfaces, including: ● Number of downstream interfaces ● Names of downstream interfaces ● Type of the PIM (IPv6) protocol configured on the downstream interfaces ● Existing period and timeout period of downstream interfaces
Total number of downstreams	Number of downstream interfaces.
GigabitEthernet1/0/0	Interface name.
Expires	Timeout period of an entry.

Display the brief information about PIM (IPv6) routing entries.

```
<Huawei> display pim ipv6 routing-table brief FF25::1
 VPN-Instance: public net
 Total 3 (*, G) entries; 3 (S, G) entries

 Total matched 1 (*, G) entry; 1 (S, G) entry

 00001.(FC00:0:0:2008::55, FF25::1)
     Upstream interface: GE1/0/0
     Number of downstreams: 2
 00002.(*, FF25::1)
     Upstream interface: GE1/0/0
     Number of downstreams: 2
```

Table 10-70 Description of the display pim ipv6 routing-table brief command output

Item	Description
Total 3 (*, G) entries; 3 (S, G) entries	Total number of the (S, G) entries and (*, G) entries in the PIM (IPv6) routing table.
Total matched 1 (*, G) entry; 1 (S, G) entry	Total number of the (S, G) entries and (*, G) entries that meet the query conditions in the PIM routing table.
00001. (FC00:0:0:2008::55, FF25::1)	(S, G) entry.

Item	Description
Number of downstreams	Number of downstream interfaces in (S, G) entries or (*, G) entries.

Display the number of the outbound interfaces of PIM (IPv6)routing entries.

```
<Huawei> display pim ipv6 routing-table outgoing-interface-number
 VPN-Instance: public net
 Total 2 (*, G) entries; 0 (S, G) entry

 (*, FF25::1)
     RP: FC00:0:0:2008::5:3:2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:00:04
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2

 (*, FF25::2)
     RP: FC00:0:0:2008::5:3:2 (local)
     Protocol: pim-sm, Flag: WC
     UpTime: 00:00:05
     Upstream interface: Register
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 2
```

Related Topics

10.8.4 display multicast ipv6 routing-table

10.4.28 display pim ipv6 rp-info

Function

The **display pim ipv6 rp-info** command displays information about the RP corresponding to a multicast group.

Format

display pim ipv6 rp-info [*ipv6-group-address*]

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display pim ipv6 rp-info** command displays information about the RP to which a multicast group corresponds. This command can help determine whether multicast forwarding errors are caused by faults of an RP.

Precautions

The RP information contains the information about the RP discovered through the BSR mechanism and static RP.

If the group address is not specified in this command, the corresponding RP information of all the multicast groups is displayed.

Example

Display the RP of multicast group FF1E::1.

```
<Huawei> display pim ipv6 rp-info ff1e::1
 VPN-Instance: public net
 BSR RP Address is: FE1E::1
     Priority: 192
     Uptime: 00:00:52
     Expires: 00:01:38
 RP mapping for this group is: FC00:0:0:2001::1 (local host)
```

Table 10-71 Description of the display pim ipv6 rp-info command output

Item	Description
BSR RP Address is	IP address of a dynamical RP
Priority	RP priority
Uptime	Period during which the RP exists
Expires	Time before an RP times out
RP mapping for this group is	Address of the RP to which multicast group corresponds

Related Topics

10.4.12 c-rp (IPv6)

10.4.29 embedded-rp

Function

The **embedded-rp** command enables the embedded RP function.

The **undo embedded-rp** command disables the embedded RP function.

By default, the embedded RP function is enabled.

Format

embedded-rp [*basic-acl6-number* | **acl6-name** *acl6-name*]

undo embedded-rp [*basic-acl6-number* | **acl6-name** *acl6-name*]

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of the basic ACL.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of an IPv6 Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The embedded RP function is enabled by default after PIM-SM (IPv6) is enabled. This function enables the router to obtain the RP address from the IPv6 multicast address of a received multicast packet, so that the router does not need to know the RP information beforehand.

By default, the router can parse group addresses in the range of FF7x::/12. The value of x can 0 or any integer in the range of 3 to F. When the router receives a multicast packet with an IPv6 group address in this range, the router can obtain the RP address from the IPv6 group address. This RP will replace the static RP or dynamically elected RP. If you do not want the router to use RP information obtained from IPv6 multicast addresses of multicast packets, run the **undo embedded-rp** command to disable the embedded RP function.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If an IPv6 ACL is specified in the command, the final group address range for embedded RP is the intersection of the group address range specified by the IPv6 ACL and the default group address range. All the devices in the PIM (IPv6) domain must be configured with the same group address range.

Example

Enable the embedded RP function on multicast group ff73::.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2000
[Huawei-acl6-basic-2000] rule permit source ff73:: 12
[Huawei-acl6-basic-2000] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] embedded-rp 2000
```

Configure a named ACL6 to enable the embedded RP on the multicast group ff73::.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff73:: 12
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] embedded-rp acl6-name myacl6
```

Related Topics

10.4.59 pim ipv6 sm

10.4.30 graceful-restart (IPv6)

Function

The **graceful-restart** command enables PIM GR.

The **undo graceful-restart** command disables PIM GR.

By default, PIM GR is not enabled.

NOTE

Only the AR3200 series routers support PIM GR (IPv6).

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-SM (IPv6) network, after an active/standby switchover is performed on the router equipped with two MPUs, the new active MPU deletes original PIM (IPv6) forwarding entries. Because the active MPU on the router cannot create new PIM (IPv6) forwarding entries in a short time, multicast data transmission is interrupted.

PIM GR enables the router to back up join and prune information in PIM (IPv6) routing entries to the new MPU when an active/standby switchover is performed on the router. This ensures normal multicast data forwarding during restoration of the multicast distribution tree.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

At least one router interface is enabled with PIM-SM (IPv6) so that the **graceful-restart** command takes effect.

Example

Enable PIM GR in the PIM-IPv6 view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] graceful-restart
```

Related Topics

10.4.59 pim ipv6 sm

10.4.31 graceful-restart period (IPv6)

10.4.31 graceful-restart period (IPv6)

Function

The **graceful-restart period** command configures the minimum PIM GR period.

The **undo graceful-restart period** command restores the default minimum PIM GR period.

By default, the minimum PIM GR period is 120 seconds.

NOTE

Only the AR3200 series routers support PIM GR (IPv6).

 Copyright © Huawei Technologies Co., Ltd.

Format

graceful-restart period *period*

undo graceful-restart period

Parameters

Parameter	Description	Value
period	Specifies the minimum PIM GR period.	It is an integer that ranges from 90 to 3600 in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **graceful-restart period** command ensures the minimal time for maintaining forwarding entries.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM GR is on the basis of unicast GR; therefore, the minimum PIM GR period should be longer than the corresponding unicast GR period.

The PIM GR period also depends on the complexity of the network topology and increases as the expansion of unicast route capacity and multicast route capacity.

Example

Set the minimum PIM GR period in the PIM-IPv6 view to 150 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] graceful-restart
[Huawei-pim6] graceful-restart period 150
```

Related Topics

10.4.59 pim ipv6 sm

10.4.30 graceful-restart (IPv6)

 Copyright © Huawei Technologies Co., Ltd.

10.4.32 hello-option dr-priority (IPv6)

Function

The **hello-option dr-priority** command configures the DR (Designated Router) priority for the router.

The **undo hello-option dr-priority** command restores the default DR priority.

By default, the DR priority for the router is 1.

Format

hello-option dr-priority *priority*

undo hello-option dr-priority

Parameters

Parameter	Description	Value
priority	Specifies the DR priority of the router.	The value is an integer that ranges from 0 to 4294967295. The greater the value, the higher the priority.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-SM (IPv6), routers on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IPv6 address. To elect the DR, the routers send the Hello message that contains the priority to each other. The router with the highest priority functions as the DR. If the routers have the same priority, the router with the largest IPv6 address functions as the DR.

If there is at least one router that does not support Hello packets that contain the priority in the network, the DR election is based on the IPv6 address of each router. The router with the largest IPv6 address functions as the DR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The **hello-option dr-priority** command has the same function as the **pim ipv6 hello-option dr-priority** command in the interface view. By default, if the **pim ipv6 hello-option dr-priority** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, configure the DR priority of a router to 3.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] hello-option dr-priority 3
```

Related Topics

10.4.48 pim ipv6 hello-option dr-priority

10.4.33 hello-option holdtime (IPv6)

Function

The **hello-option holdtime** command sets the timeout period for a router to wait to receive Hello messages from its PIM neighbor.

The **undo hello-option holdtime** command restores the default configuration.

By default, the timeout period for a router to wait to receive Hello messages from its PIM neighbor is 105 seconds.

Format

hello-option holdtime *interval*

undo hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout time during which a router waits to receive a Hello message from its PIM neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On the PIM (IPv6) network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device considers the neighbor invalid or unreachable.

The **hello-option holdtime (IPv6)** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The timeout period must be greater than the interval for sending Hello messages. You can run the **timer hello (IPv6)** command to set the interval for sending Hello messages.

The **hello-option holdtime** command has the same function as the **pim ipv6 hello-option holdtime** command in the interface view. By default, if the **pim ipv6 hello-option holdtime** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, set the timeout interval to 120 seconds. The timeout interval is the period during which a router waits to receive the Hello message from its PIM neighbor.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] hello-option holdtime 120
```

Related Topics

10.4.49 pim ipv6 hello-option holdtime

10.4.34 hello-option lan-delay (IPv6)

Function

The **hello-option lan-delay** command sets the delay in transmitting Prune message on the shared network segment.

The **undo hello-option lan-delay** command restores the default delay.

By default, the delay in transmitting Prune message on the shared network segment is 500 milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

hello-option lan-delay *interval*

undo hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting Prune message on the shared network segment.	The value is an integer that ranges from 1 to 32767, in milliseconds (ms).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by devices carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all devices on the same link are different, the maximum value of these values is used.

When a device sends a Prune message to the upstream device in the same network segment, if other device still requests the multicast data, it needs to send a Join message to the upstream device in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current device receives a Prune message from the downstream interface and performs the prune action. If the device receives a Join message from the downstream interface in PPT, the device cancels the prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If the delay in transmitting Prune message is too short, the upstream device will stop forwarding multicast packets before the downstream device determines whether to override the Prune action or not. Exercise caution when you run the **hello-option lan-delay** command.

The **hello-option lan-delay** command has the same function as the **pim ipv6 hello-option lan-delay** command in the interface view. By default, if the **pim ipv6 hello-option lan-delay** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the delay in transmitting Prune message on the shared network segment to 200 ms in the PIM-IPv6 view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] hello-option lan-delay 200
```

Related Topics

10.4.36 hello-option override-interval (IPv6)

10.4.50 pim ipv6 hello-option lan-delay

10.4.35 hello-option neighbor-tracking (IPv6)

Function

The **hello-option neighbor-tracking** command enables the neighbor tracking function.

The **undo hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

hello-option neighbor-tracking

undo hello-option neighbor-tracking

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment send Join messages to the same upstream PIM neighbor, only one device

 Copyright © Huawei Technologies Co., Ltd.

is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. The upstream neighbor cannot update neighbor relationships with downstream devices because of Generation ID change.

When the device with neighbor tracking enabled detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Neighbor tracking can be implemented only when this function is enabled on all devices on the shared network segment.

The **hello-option neighbor-tracking** command has the same function as the **pim ipv6 hello-option neighnor-tracking** command in the interface view. By default, if neighbor tracking is not used on an interface, the neighbor tracking configuration in the PIM-IPv6 view takes effect.

Example

In the PIM-IPv6 view, enable the downstream neighbor tracking function.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] hello-option neighbor-tracking
```

Related Topics

10.4.51 pim ipv6 hello-option neighbor-tracking

10.4.36 hello-option override-interval (IPv6)

Function

The **hello-option override-interval** command sets the interval for overriding the prune action in a Hello message.

The **undo hello-option override-interval** command restores the default interval.

By default, the interval for overriding the prune action in a Hello message is 2500 ms.

Format

hello-option override-interval *interval*

undo hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for overriding the prune action in a Hello message.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by routers carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a router sends a Prune message to the upstream router in the same network segment, if other router still requests the multicast data, it needs to send a Join message to the upstream router in the override-interval period.

When the values of **override-interval** on all routers on the same link are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the router does not perform the prune action until the PPT times out. If the router receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **hello-option override-interval** command has the same function as the **pim ipv6 hello-option override-interval** command in the interface view. By default, if the **pim ipv6 hello-option override-interval** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

In the PIM-IPv6 view, set the interval for denying the prune action in a Hello message to 2000 ms.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] hello-option override-interval 2000
```

Related Topics

10.4.34 hello-option lan-delay (IPv6)

10.4.52 pim ipv6 hello-option override-interval

10.4.37 holdtime assert (IPv6)

Function

The **holdtime assert** command sets the timeout period for all PIM interfaces to keep the Assert state on the local router.

The **undo holdtime assert** command restores the default timeout.

By default, the timeout period for all PIM interfaces to keep the Assert state on the local router is 180 seconds.

Format

holdtime assert *interval*

undo holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the time during which the PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM devices need to initiate the assert mechanism. The device that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retain the Assert

state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **holdtime assert** command has the same function as the **pim ipv6 holdtime assert** command in the interface view. By default, if the timeout period is not used on an interface, the timeout period configured in the PIM-IPv6 view is used.

Example

In the PIM-IPv6 view, set the interval during which a router keeps the Assert state to 100s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] holdtime assert 100
```

Related Topics

10.4.53 pim ipv6 holdtime assert

10.4.38 holdtime join-prune (IPv6)

Function

The **holdtime join-prune** command sets the holdtime value in Join/Prune messages sent by all PIM interfaces. Devices that receive Join/Prune messages set the time during which the downstream interface keeps the Join or Prune state according to holdtime.

The **undo holdtime join-prune** command restores the default value.

By default, the holdtime value in Join/Prune messages sent by all PIM interfaces is 210 seconds.

Format

holdtime join-prune *interval*

undo holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime carried in Join/Prune messages sent by the local device.	The value is an integer that ranges from 1 to 65535, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the device starts the holdtime timer. After the timeout interval, if the device does not receive subsequent Join/Prune messages from the downstream device, the downstream interface of a multicast group is suppressed from forwarding Join/Prune messages with information about multicast group joining. If Join/Prune messages carry information about multicast group prune, the downstream interface of the multicast group is restored.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **holdtime join-prune** command has the same function as the **pim ipv6 holdtime join-prune** command in the interface view. By default, if the holdtime value is not used on an interface, the holdtime value configured in the PIM-IPv6 view is used.

Example

In the PIM-IPv6 view, set the time during which the downstream interface of a router keeps the Join or Prune state to 280 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] holdtime join-prune 280
```

Related Topics

10.4.54 pim ipv6 holdtime join-prune

10.4.39 join-prune max-packet-length (IPv6)

Function

The **join-prune max-packet-length** command sets the maximum size of each Join/Prune message to be sent.

The **undo join-prune max-packet-length** command restores the default maximum size of each Join/Prune message to be sent.

 Copyright © Huawei Technologies Co., Ltd.

By default, the maximum length of Join/Prune message sent by is 8100 bytes.

Format

join-prune max-packet-length *packet-length*

undo join-prune max-packet-length

Parameters

Parameter	Description	Value
packet-length	Specifies the maximum size of each PIM-SM Join/Prune message to be sent.	The value is an integer that ranges from 100 to 64000, in bytes.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has low performance and takes a long time to process a single Join/Prune message carrying a lot of (S, G) entries, the maximum size of each Join/Prune message can be set to a small value to limit the number of (S, G) entries in each message, relieving the burden on the peer device.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

If the maximum size specified in the **join-prune max-packet-length** command is greater than the interface MTU, the maximum size of each message to be sent is equal to the interface MTU.

Example

Set the maximum size of each Join/Prune message to be sent to 2100 bytes.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] join-prune max-packet-length 2100
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.4.40 join-prune periodic-messages queue-size (IPv6)
10.4.41 join-prune triggered-message-cache disable (IPv6)

10.4.40 join-prune periodic-messages queue-size (IPv6)

Function

The **join-prune periodic-messages queue-size** command sets the maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.

The **undo join-prune periodic-messages queue-size** command restores the default maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.

By default, a Join/Prune message that is sent every second contains 1020 entries.

Format

join-prune periodic-messages queue-size *queue-size*

undo join-prune periodic-messages queue-size

Parameters

Parameter	Description	Value
queue-size	Specifies the maximum number of (S, G) entries carried in a Join/Prune message that is sent every second.	The value is an integer that ranges from 16 to 4096.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the peer device has a low throughput, change the length of a queue for periodically sending messages to a small value to control the number of (S, G) entries. This setting allows the local device to send Join/Prune messages with a small number of (S, G) entries multiple times, preventing packet loss or route flapping.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

Example

Allow each Join/Prune message that is sent every second to carry a maximum of 2000 (S, G) entries.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] join-prune periodic-messages queue-size 2000
```

Related Topics

10.4.39 join-prune max-packet-length (IPv6)
10.4.41 join-prune triggered-message-cache disable (IPv6)

10.4.41 join-prune triggered-message-cache disable (IPv6)

Function

The **join-prune triggered-message-cache disable** command disables the Join/Prune message package function.

The **undo join-prune triggered-message-cache disable** command enables the Join/Prune message package function.

By default, the Join/Prune message package function is enabled.

Format

join-prune triggered-message-cache disable

undo join-prune triggered-message-cache disable

Parameters

None

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The system performs more efficiently to send a package of Join/Prune messages than to send a large number of individual Join/Prune messages. A device sends

 Copyright © Huawei Technologies Co., Ltd.

Join/Prune messages in packages. To disable the package function, run the **join-prune triggered-message-cache disable** command.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

Example

Disable the Join/Prune message package function.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] join-prune triggered-message-cache disable
```

Related Topics

10.4.39 join-prune max-packet-length (IPv6)

10.4.40 join-prune periodic-messages queue-size (IPv6)

10.4.42 local-address (IPv6)

Function

The **local-address** command sets a local address for an Anycast RP.

The **undo local-address** command deletes the local address set for an Anycast RP.

By default, no local address is set for an Anycast RP.

Format

local-address *local-address*

undo local-address

Parameters

Parameter	Description	Value
local-address	Specifies the local address of Anycast RP.	The value must be a legal IPv6 unicast IP address in hexadecimal notation.

Views

Anycast-RP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM (IPv6) Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IPv6 address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the destination addresses of the Register message. In such a manner, Anycast RP peers can learn source/group information from each other. This command is used to set a local address for an Anycast RP.

Prerequisites

The local address specified for Anycast RP must be an existing interface IPv6 address.

Precautions

The local address must be different from the Anycast RP address.

NOTE

Setting a Loopback interface address as the local address of the Anycast RP is recommended.

Example

In the Anycast RP view, set the Anycast RP address to FC00:0:0:2001::1 and local address of Anycast RP to FC00:0:0:1::1.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] anycast-rp fc00:0:0:2001::1
[Huawei-pim6-anycast-rp-2001::1] local-address fc00:0:0:1::1
```

Related Topics

10.4.1 anycast-rp (IPv6)

10.4.44 peer (IPv6)

10.4.43 neighbor-check (IPv6)

Function

The **neighbor-check** command enables the PIM neighbor check function.

The **undo neighbor-check** command restores the default setting.

 Copyright © Huawei Technologies Co., Ltd.

By default, the PIM neighbor check function is not enabled.

Format

neighbor-check { **receive** | **send** }

undo neighbor-check { **receive** | **send** }

Parameters

Parameter	Description	Value
receive	Checks whether the Join/Prune and Assert messages are received from a PIM neighbor. If not, these messages are discarded.	-
send	Checks whether the Join/Prune and Assert messages are sent to a PIM neighbor. If not, these messages are not sent.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices send Join/Prune messages to the upstream PIM neighbor to perform join and prune actions and PIM neighbors often exchange Assert messages. To save system resources and protect security of Join/Prune messages and Assert messages, run the **neighbor-check** command to enable the PIM neighbor check function.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

You can specify both **receive** and **send** to enable the PIM neighbor check function for the received and sent Join/Prune and Assert messages.

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

Example

In the PIM-IPv6 view, enable the PIM neighbor check function for the received Join/Prune and Assert messages.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] pim-ipv6
[Huawei-pim6] neighbor-check receive
```

10.4.44 peer (IPv6)

Function

The **peer** command configures Anycast RP peers.

The **undo peer** command removes the configurations of Anycast RPs.

By default, no Anycast RP peer is configured.

Format

peer *peer-address*

undo peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an Anycast RP peer.	The value is in hexadecimal notation.

Views

Anycast-RP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If PIM (IPv6) Anycast RP is configured, after an RP receives a Register message, it checks the source address of the Register message. If the Register message is sent by the source's DR, the RP forwards the Register message to Anycast RP peers. If the Register message is sent by an Anycast RP peer, it does not forward the Register message.

When forwarding a PIM Register message to other Anycast RP peers, the local RP needs to use its own IPv6 address (called the local address) as the source address of the Register message and use the addresses of Anycast RP peers as the destination addresses of the Register message. In such a manner, Anycast RP peers can learn source/group information from each other. This command is used to configure an address for an Anycast RP peer. This address is used as the destination address of the Register message to be sent by the local RP.

Precautions

You can specify a maximum of 16 Anycast RP peers for each Anycast RP.

 Copyright © Huawei Technologies Co., Ltd.

In a PIM-SM (IPv6) domain, all the devices deployed with Anycast RP must be fully connected logically. Anycast RP peer relationships need to be configured between every two devices deployed with the Anycast RP.

Example

In the Anycast RP view, set the Anycast RP address to FC00:0:0:3::3 and the peer address to FC00:0:0:2::2.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] anycast-rp fc00:0:0:3::3
[Huawei-pim6-anycast-rp-fc00:0:0:3::3] peer fc00:0:0:2::2
```

Related Topics

10.4.42 local-address (IPv6)

10.4.1 anycast-rp (IPv6)

10.4.45 pim-ipv6

Function

The **pim-ipv6** command displays the PIM-IPv6 view.

The **undo pim-ipv6** command clears the configuration in the PIM-IPv6 view.

Format

pim-ipv6

undo pim-ipv6

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before performing PIM (IPv6) configurations, run the **pim-ipv6** command to enter the PIM-IPv6 view.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

In using the **undo pim-ipv6** command, enter Y or N to confirm the action. This command clears global PIM (IPv6) configurations in the current instance. Use this command with caution.

Example

Enter the PIM-IPv6 view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6]
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.4.46 pim ipv6 bsr-boundary

Function

The **pim ipv6 bsr-boundary** command configures the BSR boundary of a PIM-SM (IPv6) domain on an interface.

The **undo pim ipv6 bsr-boundary** command restores the default configuration.

By default, the BSR boundary of a PIM-SM (IPv6) domain is not set.

Format

pim ipv6 bsr-boundary

undo pim ipv6 bsr-boundary

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

As the management core of the PIM-SM (IPv6) network, the BSR is responsible for sending collected RP-set information to PIM neighbors through Bootstrap messages.

You can divide a large PIM-SM (IPv6) network into multiple PIM-SM (IPv6) domains by configuring the bsr boundary on an interface. Each BSR then serves the local PIM-SM (IPv6) domain.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The Bootstrap messages cannot traverse the BSR boundary but other multicast packets can.

Example

Configure the BSR boundary of a PIM-SM (IPv6) domain on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 bsr-boundary
```

Related Topics

10.4.4 c-bsr (IPv6)

10.4.47 pim ipv6 dm

Function

The **pim ipv6 dm** command enables PIM-DM (IPv6) on an interface.

The **undo pim ipv6 dm** command restores the default configuration.

By default, PIM-DM (IPv6) is disabled on an interface.

Format

pim ipv6 dm

undo pim ipv6 dm

Parameters

None

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM-DM (IPv6) is a multicast routing protocol in dense mode and applies to small-scale network with densely-distributed group members.

After PIM-DM (IPv6) is enabled on an interface, the router can set up the PIM neighbor relationship with the neighboring device. The router then can process protocol packets received from PIM neighbors.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM-DM (IPv6) and PIM-SM (IPv6) cannot be enabled simultaneously on the device.

If PIM-DM (IPv6) and MLD need to be enabled on the same interface, enable PIM-DM (IPv6), and then enable MLD.

Example

Enable PIM-DM (IPv6) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 dm
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.4.59 pim ipv6 sm

10.4.48 pim ipv6 hello-option dr-priority

Function

The **pim ipv6 hello-option dr-priority** command sets the priority for the PIM interface that is elected as DR.

The **undo pim ipv6 hello-option dr-priority** command restores the default value of the priority.

By default, the priority for the PIM interface that is elected as DR is 1.

Format

pim ipv6 hello-option dr-priority *priority*

undo pim ipv6 hello-option dr-priority

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
priority	Specifies the priority of the PIM interface that is elected as DR.	The value is an integer that ranges from 0 to 4294967295. The greater the value, the higher the priority.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM (IPv6), devices on the shared network segment candidates for the DR. The DR is responsible for the registering of the local multicast source and the joining of the receivers.

The DR election is based on the priority and the IPv6 address. To elect the DR, the devices send the Hello message that contains the priority to each other. The device with the highest priority functions as the DR. If the devices have the same priority, the device with the largest IPv6 address functions as the DR.

If there is at least one device that does not support Hello packets that contain the priority in the network, the DR election is based on the IPv6 address of each device. The device with the largest IPv6 address functions as the DR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 hello-option dr-priority** command has the same function as the **hello-option dr-priority (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option dr-priority** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the priority of GE1/0/0 that is elected as DR to 3.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option dr-priority 3
```

Related Topics

10.4.32 hello-option dr-priority (IPv6)

10.4.49 pim ipv6 hello-option holdtime

Function

The **pim ipv6 hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

The **undo pim ipv6 hello-option holdtime** command restores the default value of the timeout.

By default, the timeout period during which the PIM interface waits to receive the Hello message from its neighbor is 105 seconds.

Format

pim ipv6 hello-option holdtime *interval*

undo pim ipv6 hello-option holdtime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the PIM interface waits to receive Hello messages from its neighbor.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM (IPv6) network, after the device receives a Hello message from its PIM neighbor, the device starts the timer. The timer value is the value of Holdtime in the Hello message. If the device does not receive any Hello message from its PIM neighbor after the timeout, the device considers the neighbor invalid or unreachable.

The **pim ipv6 hello-option holdtime** command sets the timeout period during which the PIM interface waits to receive the Hello message from its neighbor.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The timeout period must be greater than the interval for sending Hello messages. You can run the **pim ipv6 time hello** command to set the interval for sending Hello messages.

The **pim ipv6 hello-option holdtime** command has the same function as the **hello option holdtime (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option holdtime** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period during which GE1/0/0 waits to receive Hello messages from its neighbor to 120 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option holdtime 120
```

Related Topics

10.4.33 hello-option holdtime (IPv6)

10.4.50 pim ipv6 hello-option lan-delay

Function

The **pim ipv6 hello-option lan-delay** command sets the delay in transmitting messages in a shared network in the interface view.

The **undo pim ipv6 hello-option lan-delay** command restores the default value of the delay.

By default, the delay in transmitting messages in the shared network is 500 ms.

Format

pim ipv6 hello-option lan-delay *interval*

undo pim ipv6 hello-option lan-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay in transmitting messages in the shared network.	The value is an integer that ranges from 1 to 32767, in milliseconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hello messages sent by devices carry **lan-delay** and **override-interval**. The **lan-delay** parameter indicates the delay in transmitting messages in the LAN. When the values of **lan-delay** on all devices on the same link are different, the maximum value of these values is used.

When a device sends a Prune message to the upstream device in the same network segment, if other device still requests the multicast data, it needs to send a Join message to the upstream device in the override-interval period.

The value of the Prune-Pending Timer (PPT) is obtained by the value of **lan-delay** plus the value of **override-interval**. PPT refers to the delay during which the current device receives a Prune message from the downstream interface and performs the prune action. If the device receives a Join message from the downstream interface in PPT, the device cancels the prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

If the prune delay is set too short, the upstream device stops forwarding multicast packets before the downstream device overrides Prune messages of neighbors. Exercise caution when you run this command.

The function of this command in the interface view is the same as that of the **hello-option lan-delay (IPv6)** command in the PIM-IPv6 view. By default, if the configuration on the interface is not performed, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the delay in transmitting messages to 200 ms on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option lan-delay 200
```

Related Topics

10.4.52 pim ipv6 hello-option override-interval

10.4.34 hello-option lan-delay (IPv6)

 Copyright © Huawei Technologies Co., Ltd.

10.4.51 pim ipv6 hello-option neighbor-tracking

Function

The **pim ipv6 hello-option neighbor-tracking** command enables the neighbor tracking function in the interface view.

The **undo pim ipv6 hello-option neighbor-tracking** command restores the default configuration.

By default, the neighbor tracking function is not enabled.

Format

pim ipv6 hello-option neighbor-tracking

undo pim ipv6 hello-option neighbor-tracking

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When sending a Hello message, the device generates a Generation ID and encapsulates it into the message. The Generation ID changes only when the device status changes. After receiving the Hello message, the neighboring device detects Generation ID change and immediately sends a Join message to the device to update the neighbor relationship. If multiple devices on the shared network segment send Join messages to the same upstream PIM neighbor, only one device is allowed to send the Join message. After other devices detect the Join message, they do not send Join messages to the upstream neighbor. The upstream neighbor cannot update neighbor relationships with downstream devices because of Generation ID change.

After the neighbor tracking function is enabled, when the device detects Join messages from other devices, the device still sends the Join messages to the same upstream PIM neighbor.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This command is valid for only PIM-SM (IPv6).

The neighbor tracking function can be implemented on a shared network segment only when this function is enabled on all devices on the network segment.

The **pim ipv6 hello-option neighbor-tracking** command has the same function as the **hello-option neighbor-tracking (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option neighbor-tracking** command is not used, the configuration in the PIM-IPv6 view takes effect; otherwise, the configuration in the interface view takes effect.

Example

Enable the neighbor tracking function on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option neighbor-tracking
```

Related Topics

10.4.35 hello-option neighbor-tracking (IPv6)

10.4.52 pim ipv6 hello-option override-interval

Function

The **pim ipv6 hello-option override-interval** command sets the interval carried in Hello messages for overriding the prune action on the interface.

The **undo pim ipv6 hello-option override-interval** command, restores the default configuration.

By default, the interval carried in Hello messages for overriding the prune action on the interface is 2500 milliseconds.

Format

pim ipv6 hello-option override-interval *interval*

undo pim ipv6 hello-option override-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval of overriding the prune action.	The value is an integer that ranges from 1 to 65535, in milliseconds.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Hello messages sent by devices carry **lan-delay** and **override-interval**. The **override-interval** parameter refers to the period during which a downstream router overrides the prune action.

When a device sends a Prune message to the upstream device in the same network segment, if other device still requests the multicast data, it needs to send a Join message to the upstream device in the override-interval period.

When the values of **override-interval** on all devices on the same link are different, the maximum value of these values is used.

The value of PPT is obtained by the value of **lan-delay** plus the value of **override-interval**. When receiving a Prune message from a downstream interface, the device does not perform the prune action until the PPT times out. If the device receives a Join message from the downstream interface in PPT, the interface cancels the Prune action.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 hello-option override-interval** command has the same function as the **hello-option override-interval (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 hello-option override-interval** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval for overriding the prune action in Hello messages to 2000 ms on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 hello-option override-interval 2000
```

Related Topics

10.4.50 pim ipv6 hello-option lan-delay

10.4.36 hello-option override-interval (IPv6)

10.4.53 pim ipv6 holdtime assert

Function

The **pim ipv6 holdtime assert** command sets the timeout period during which a PIM interface keeps the Assert state.

The **undo pim ipv6 holdtime assert** command restores the default value of the timeout.

 Copyright © Huawei Technologies Co., Ltd.

By default, the timeout period during which a PIM interface keeps the Assert state is 180 seconds.

Format

pim ipv6 holdtime assert *interval*

undo pim ipv6 holdtime assert

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which a PIM interface keeps the Assert state.	The value is an integer that ranges from 7 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the shared network segment connected to multiple PIM devices, if the same multicast packets reach these PIM devices and pass the RPF check, multiple copies of the same multicast packets are forwarded to this network segment. In this situation, these PIM routers need to initiate the assert mechanism. The router that wins assert election is responsible for multicast forwarding on the shared network segment. Other devices suppress multicast data forwarding and retains the Assert state for a period of time. After the timer for a PIM interface in the Assert state expires, the device that fails to be elected triggers a new round of election.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for PIM-SM (IPv6) and PIM-DM (IPv6).

The **pim ipv6 holdtime assert** command has the same function as the **holdtime assert (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 holdtime assert** command is not used, the value configured in the PIM-IPv6 view is used; otherwise, the value configured in the interface view is used.

Example

Set the timeout period for GE1/0/0 to keep the Assert state to 100s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 holdtime assert 100
```

Related Topics

10.4.37 holdtime assert (IPv6)

10.4.54 pim ipv6 holdtime join-prune

Function

The **pim ipv6 holdtime join-prune** command sets the holdtime in a Join/Prune message sent by the PIM interface.

The **undo pim ipv6 holdtime join-prune** command restores the default value of the holdtime.

By default, the holdtime in a Join/Prune message sent by the PIM interface is 210 seconds.

Format

pim ipv6 holdtime join-prune *interval*

undo pim ipv6 holdtime join-prune

Parameters

Parameter	Description	Value
interval	Specifies the value of holdtime in a Join/Prune message sent by the PIM interface.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Join/Prune message from the downstream device, the router starts the holdtime timer. After the timeout interval, if the router does not receive subsequent Join/Prune messages from the downstream device, the downstream interface of a multicast group is suppressed from forwarding Join/Prune messages with information about multicast group joining. If Join/Prune messages carry information about multicast group prune, the downstream interface of the multicast group is restored.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

The **pim ipv6 holdtime join-prune** command has the same function as the **holdtime join-prune (IPv6)** command in the PIM-IPv6 view. By default, if the **pim ipv6 holdtime join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the holdtime in a Join/Prune message sent by GE1/0/0 to 280 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 holdtime join-prune 280
```

Related Topics

10.4.38 holdtime join-prune (IPv6)

10.4.55 pim ipv6 join-policy

Function

The **pim ipv6 join-policy** command enables the system to filter join information in Join/Prune messages.

The **undo pim ipv6 join-policy** command restores the default setting.

By default, join information in Join/Prune message is not filtered.

Format

pim ipv6 join-policy { **asm** { *basic-acl6-number* | **acl6-name** *acl6-name* } | **ssm** { *advanced-acl6-number* | **acl6-name** *acl6-name* } | *advanced-acl6-number* | **acl6-name** *acl6-name* }

undo pim ipv6 join-policy [**asm** | **ssm**]

Parameters

Parameter	Description	Value
asm	Filters join information, with the group address in the ASM group address range.	-
basic-acl6-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ssm	Filters join messages, with the group addresses within the SSM group address range and specified source address.	-
advanced-acl6-number	Specifies the advanced ACL number.	The value is an integer that ranges from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from joining multicast groups on the PIM-SM (IPv6) network, run the **pim ipv6 join-policy** command to enable the system to filter join information in Join/Prune messages.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **pim ipv6 join-policy** command and the **acl ipv6 (system view)** command are used together.

- If **asm** is specified, in the basic ACL6 view, you can set the multicast group address range of join information by specifying the **source** parameter in the **rule (basic ACL6 view)** command.
- If **ssm** is specified, in the advanced ACL6 view, you can set the source address range and multicast group address range of join information by respectively specifying the **source** parameter and **destination** parameter in the **rule (advanced ACL6 view)** command.

The rule configurations for a named ACL and an advanced ACL are the same. The **time-range** parameter takes effect in the **rule** command only for the named ACL.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE1/0/0 to accept the join information with the group address FF25::1.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2001
[Huawei-acl6-basic-2001] rule permit source ff25::1 128
[Huawei-acl6-basic-2001] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 join-policy asm 2001
```

Use a named ACL6 to configure GE1/0/0 to accept the Join messages with the source address FC00:0:0:2001::4 and group address FF35::1.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl
[Huawei-acl6-adv-myacl] rule permit ipv6 source fc00:0:0:2001::4 128 destination ff35::1 128
[Huawei-acl6-adv-myacl] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 join-policy ssm acl6-name myacl
```

10.4.56 pim ipv6 neighbor-policy

Function

The **pim ipv6 neighbor-policy** command configures a policy for filtering PIM neighbors on an interface.

The **undo pim ipv6 neighbor-policy** command restores the default setting.

By default, PIM neighbors on the interface are not filtered.

Format

pim ipv6 neighbor-policy { *basic-acl6-number* | **acl6-name** *acl6-name* }

undo pim ipv6 neighbor-policy

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the basic ACL number.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the ACL name. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized neighbors from being involved in the PIM protocol, run the **pim ipv6 neighbor-policy** command to configure a policy for filtering PIM neighbors and set the address range of PIM neighbors. The device sets up neighbor relationships with the addresses matching the filtering rules and deletes the neighbors that do not match the filtering rules.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

The **pim ipv6 neighbor-policy** command and the **acl ipv6** command are used together. In the ACL view, set the address range of PIM neighbors by specifying **source** in the **rule** command.

For the named ACL, in the ACL view, when the **rule** command is used to configure a filtering rule, the filtering rule takes effect for only the multicast group address range specified by **source** and the time range specified by **time-range**.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

If the IPv6 address of a PIM neighbor that has established a neighbor relationship with the device is not in the configured range of valid neighbor IPv6 addresses, the device will no longer receive Hello messages from this PIM neighbor. When the holdtime of Hello messages expires, the neighbor relationship between the PIM device and the device is terminated.

Example

Configure GE1/0/0 to set up the PIM neighbor relationship with the router of the address FC00:0:0:2000::1.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2001
[Huawei-acl6-basic-2001] rule permit source fc00:0:0:2000::1 128
[Huawei-acl6-basic-2001] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 neighbor-policy 2001
```

10.4.57 pim ipv6 require-genid

Function

The **pim ipv6 require-genid** command configures a PIM interface to reject the Hello messages without the generation ID.

The **undo pim ipv6 require-genid** command restores the default configuration.

By default, a PIM interface is allowed to receive the Hello messages without the generation ID.

Format

pim ipv6 require-genid

undo pim ipv6 require-genid

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an interface on the device is enabled with PIM, the device generates a random number as the generation ID of the Hello message. If the status of the device is updated, the device generates a new Generation ID. When the device finds that the Hello message received from a PIM neighbor contains a different Generation ID, the device considers that the status of the PIM neighbor changes.

To ensure that connected PIM neighbors work properly, run the **pim ipv6 require-genid** command to configure a PIM interface to reject the Hello messages without the generation ID.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

Configure GE1/0/0 to reject the Hello messages without the generation ID.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 require-genid
```

 Copyright © Huawei Technologies Co., Ltd.

10.4.58 pim ipv6 silent

Function

The **pim ipv6 silent** command enables the PIM silent (IPv6) function on an interface.

The **undo pim ipv6 silent** command cancels the PIM silent (IPv6) function on an interface.

By default, the PIM silent (IPv6) function is disabled on an interface.

Format

pim ipv6 silent

undo pim ipv6 silent

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect the router against pseudo PIM Hello (IPv6) messages sent from malicious hosts, configure the **pim ipv6 silent** command on the interface directly connected to the host network segment to set the interface to PIM silent (IPv6) mode. Then the interface cannot receive or forward any PIM (IPv6) packet, and all PIM (IPv6) neighbors and PIM (IPv6) state machines on this interface are deleted. This interface becomes the DR, but the MLD function on the interface is not affected.

The PIM silent (IPv6) function applies only to the interface directly connected to a host network segment, and only one PIM router can be connected to this network segment.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

After you run this command on an interface, the interface no longer receives or sends any PIM (IPv6) packets and other PIM (IPv6) functions on the interface become invalid. Confirm your action before using this command.

If a host network segment is connected to multiple routers and PIM silent (IPv6) is enabled on multiple interfaces, all these interfaces become static DRs. This causes multicast forwarding failures.

Example

Configure the PIM silent (IPv6) function on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 silent
```

10.4.59 pim ipv6 sm

Function

The **pim ipv6 sm** command enables PIM-SM (IPv6) on an interface.

The **undo pim ipv6 sm** command disables PIM-SM (IPv6).

By default, PIM-SM (IPv6) is disabled on an interface.

Format

pim ipv6 sm

undo pim ipv6 sm

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After PIM-SM (IPv6) is enabled on interfaces, devices can set up PIM neighbor relationships with each other and process protocol packets received from PIM neighbors.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

PIM-DM (IPv6) and PIM-SM (IPv6) cannot be enabled simultaneously on the device.

If PIM-SM (IPv6) and MLD need to be enabled on the same interface, enable PIM-SM (IPv6), and then enable MLD.

Example

Enable PIM-SM (IPv6) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 sm
```

Related Topics

10.8.16 multicast ipv6 routing-enable

10.4.47 pim ipv6 dm

10.4.60 pim ipv6 state-refresh-capable

Function

The **pim ipv6 state-refresh-capable** command enables PIM-DM (IPv6) State-Refresh on an interface.

The **undo pim ipv6 state-refresh-capable** command disables PIM-DM (IPv6) State-Refresh.

By default, PIM-DM (IPv6) State-Refresh is enabled.

Format

pim ipv6 state-refresh-capable

undo pim ipv6 state-refresh-capable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

PIM-DM (IPv6) State-Refresh is implemented by periodically sending State-Refresh messages in the network. After receiving a State-Refresh message, the router in the pruned state resets the prune-status timer. As a result, the downstream interface cannot forward packets before the prune-status timer times out.

After PIM-DM (IPv6) state-refresh is disabled, the interface starts to forward multicast data when the prune timer times out. The downstream routers that do not want to receive the data can send Prune messages. The process is performed periodically, which wastes a lot of network resources. Enabling PIM-DM (IPv6) State-Refresh can optimize the network traffic.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Disable PIM-DM (IPv6) State-Refresh on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] undo pim ipv6 state-refresh-capable
```

10.4.61 pim ipv6 timer dr-switch-delay

Function

The **pim ipv6 timer dr-switch-delay** command enables PIM DR switching delay and configures the delay on an interface. When the interface changed from a DR to a non-DR, the interface continues to forward data before the delay expires.

The **undo pim ipv6 timer dr-switch-delay** command disables PIM DR switching delay on the interface.

By default, when the interface changes from a DR to a non-DR, the interface stops forwarding data immediately.

Format

pim ipv6 timer dr-switch-delay *interval*

undo pim ipv6 timer dr-switch-delay

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the delay.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the DR on a shared network segment becomes the non-DR, original multicast forwarding entries will be deleted immediately, causing multicast data interruption in a short time. To solve the problem, set the DR switching delay. Original multicast forwarding entries still take effect until the delay is reached.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Example

Enable PIM DR switching delay on GE1/0/0 and set the delay to 20 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer dr-switch-delay 20
```

10.4.62 pim ipv6 timer graft-retry

Function

The **pim ipv6 timer graft-retry** command sets the interval for retransmitting Graft messages on an interface.

The **undo pim ipv6 timer graft-retry** command restores the default value of the interval.

By default, the interval for retransmitting Graft messages on an interface is 3 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

pim ipv6 timer graft-retry *interval*

undo pim ipv6 timer graft-retry

Parameters

Parameter	Description	Value
interval	Specifies the interval of retransmitting Graft messages.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In PIM-DM (IPv6) mode, when a member joins a pruned group, the router sends a Graft message and waits to receive an ACK message from the upstream router. If the downstream router does not receive the ACK message in the period configured through the command, the router resends the Graft message until the router receives the ACK message from the upstream router.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Set the interval for retransmitting Graft messages to 80s on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer graft-retry 80
```

10.4.63 pim ipv6 timer hello

Function

The **pim ipv6 timer hello** command sets the interval for sending Hello messages on an interface.

 Copyright © Huawei Technologies Co., Ltd.

The **undo pim ipv6 timer hello** command restores the default value of the interval.

By default, the interval for sending Hello messages on an interface is 30 seconds.

Format

pim ipv6 timer hello *interval*

undo pim ipv6 timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello messages.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim ipv6 timer hello** command to set the interval for sending Hello messages.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval for sending Hello messages must be shorter than the timeout period of PIM neighbors. You can run the **pim ipv6 hello-option holdtime** command to set the timeout period of PIM neighbors.

The configuration is the same as the **timer hello (IPv6)** command in the PIM-IPv6 view, except for the view. The system prefers the configuration in the interface view. The value configured in the PIM-IPv6 view is used if no value is configured on the interface.

Example

Set the interval for sending Hello messages to 40 seconds on GE1/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer hello 40
```

Related Topics

10.4.80 timer hello (IPv6)

10.4.49 pim ipv6 hello-option holdtime

10.4.64 pim ipv6 timer join-prune

Function

The **pim ipv6 timer join-prune** command sets the interval for periodically sending Join/Prune messages to the upstream device.

The **undo pim ipv6 timer join-prune** command restores the default interval.

By default, the interval for periodically sending Join/Prune messages to the upstream device is 60 seconds.

Format

pim ipv6 timer join-prune *interval*

undo pim ipv6 timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Join/Prune messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends join information to the upstream device, requesting the upstream device to forward multicast data. The device sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The device periodically sends Join/Prune messages to the upstream device to update the forwarding status.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval configured through this command must be shorter than the interval configured through the **pim ipv6 holdtime join-prune** command. The interval at which Join or Prune messages are sent must be shorter than the holdtime carried in Join/Prune messages.

The configuration is the same as that of the **timer join-prune (IPv6)** command in the PIM-IPv6 view. The system prefers the configuration in the interface view. The value configured in the PIM-IPv6 view is used if no value is configured on the interface.

Example

Set the interval for sending Join or Prune messages to 80 seconds on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 timer join-prune 80
```

Related Topics

10.4.81 timer join-prune (IPv6)

10.4.54 pim ipv6 holdtime join-prune

10.4.65 pim ipv6 triggered-hello-delay

Function

The **pim ipv6 triggered-hello-delay** command sets the maximum delay for triggering Hello messages.

The **undo pim ipv6 triggered-hello-delay** command restores the default maximum delay.

By default, the maximum delay for triggering Hello messages is 5 seconds.

Format

pim ipv6 triggered-hello-delay *interval*

undo pim ipv6 triggered-hello-delay

Parameters

Parameter	Description	Value
interval	Specifies the maximum delay for triggering Hello messages.	The value is an integer that ranges from 1 to 5, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To avoid the conflict caused by multiple PIM devices sending Hello message at the same time, the PIM device automatically selects a random number smaller than the configured value as the delay. When detecting Hello messages in the network, the PIM device sends Hello message after the delay.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Set the maximum delay for triggering the Hello message to 3 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] pim ipv6 triggered-hello-delay 3
```

10.4.66 probe-interval (IPv6)

Function

The **probe-interval** command sets the interval for a router to send Probe messages (null Register message) to the RP.

The **undo probe-interval** command restores the default value of the interval.

By default, the interval for a router to send Probe messages to the RP is 5 seconds.

Format

probe-interval *interval*

undo probe-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Probe messages to RP.	The value is an integer that ranges from 1 to 1799, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When receiving a Register-Stop message sent by the RP, the DR at the source side stops sending Register messages and enters the register suppression state.

During the register suppression, the DR at the source side sends Probe messages to notify the RP that the multicast source is still in the Active state. After the register suppression times out, the DR at the source side starts to send Register messages.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

The interval set using the **probe-interval** command must be less than half the interval set using the **register-suppression-timeout (IPv6)** command.

Example

In the PIM-IPv6 view, set the interval for sending Probe messages to RP to 6 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] probe-interval 6
```

Related Topics

10.4.69 register-suppression-timeout (IPv6)

10.4.67 register-policy (IPv6)

Function

The **register-policy** command sets the rules used by an RP to filter Register messages.

The **undo register-policy** command restores the default setting.

By default, the rules for filtering Register messages are not configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

register-policy { *advanced-acl6-number* | **acl6-name** *acl6-name* }

undo register-policy

Parameters

Parameter	Description	Value
advanced-acl6-number	Specifies the number of the advanced ACL that defines the rules for filtering packets based on source addresses or group addresses.	The value is an integer that ranges from 3000 to 3999.
acl6-name *acl6-name*	Specifies the name of a Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent the attack of invalid Register messages, you can configure devices to receive or deny Register messages according to the packet filtering rules.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

NOTICE

When the **register-policy** command is used on the RP, only Register messages matching the rule of the ACL are received by the RP. If an undefined ACL is specified, the RP denies all Register messages.

This command is valid for only PIM-SM (IPv6).

The **register-policy** command takes effect for only subsequently received Register messages. The multicast entries that have been registered successfully are not deleted and can still be used for multicast data forwarding.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the RP to receive Register packets sent by the multicast source on the network segment FC00:0:0:2001::2/64 to the multicast group FF02:13::/64.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule permit ipv6 source fc00:0:0:2001::2 64 destination ff02:13:: 64
[Huawei-acl6-adv-3000] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] register-policy 3000
```

Configure an IPv6 Named ACL, the RP receives Register packets sent by the multicast source on the network segment FC00:0:0:2001::2/64 to the multicast group FF02:13::/64.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:2001::2 64 destination ff02:13:: 64
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] register-policy acl6-name myacl6
```

10.4.68 register-source (IPv6)

Function

The **register-source** command specifies the source IPv6 address used by the source's DR to send Register messages.

The **undo register-source** command restores the default setting.

By default, the source IPv6 address used by the source's DR to send Register messages is not specified.

Format

register-source *ipv6-address*

undo register-source

Parameters

Parameter	Description	Value
ipv6-address	Specifies the global IPv6 unicast address of the registered source.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

PIM-IPv6 view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the source IPv6 address for sending Register messages is no longer the only IPv6 address in the network for the RP device or the source IPv6 address is filtered out, errors occur in the registration process and extra traffic occupies bandwidth on the network. In this case, use the **register-source** command to specify an appropriate interface as the source IPv6 address for sending Register messages. Using the loopback address of the source's DR as the source IPv6 address is recommended.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Specify the source IPv6 address used by the source's DR to send Register message as FC00:0:0:1101::1.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] register-source fc00:0:0:1101::1
```

10.4.69 register-suppression-timeout (IPv6)

Function

The **register-suppression-timeout** command sets the timeout period during which a router keeps the register suppression state.

The **undo register-suppression-timeout** command restores the default timeout period.

By default, a router keeps the register suppression state for 60 seconds.

Format

register-suppression-timeout *interval*

undo register-suppression-timeout

Parameters

Parameter	Description	Value
interval	Specifies the timeout period during which the router keeps the register suppression state.	The value is an integer that ranges from 11 to 3600, in seconds.

Views

PIM-IPv6 view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a Register-Stop message from the RP, the router immediately stops sending Register messages and enters the register suppression state.

The **register-suppression-timeout** command determines how long the router keeps the register suppression state. When the timeout period expires, the router (source DR) starts to send Register messages to the RP.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid only for PIM-SM (IPv6).

If the timeout period is too short, the RP receives burst multicast data more frequently. If the timeout period is too long, the delay for a new receiver to join a group is long when an (S, G) entry on the RP times out.

You can use the **probe-interval (IPv6)** command to configure the router to send null Register messages before the suppression timer times out. This configuration reduces burst Register messages and shortens the timeout period to reduce the delay for a new receiver to join a group.

Example

In the PIM-IPv6 view, set the timeout period during which the router keeps the register suppression state to 70 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] register-suppression-timeout 70
```

Related Topics

10.4.66 probe-interval (IPv6)

10.4.70 reset pim ipv6 control-message counters

Function

The **reset pim ipv6 control-message counters** command resets the statistics about PIM (IPv6) Control messages.

Format

reset pim ipv6 control-message counters [**interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the name and the number of an interface. It is used to reset the statistics about PIM (IPv6) control messages on a specified interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If an interface with PIM (IPv6) enabled on the device has been forwarding multicast packets in a long period of time, the device stores statistics on a large number of control messages. You can run this command to reset statistics on Control messages.

Example

Reset the statistics about PIM (IPv6) control messages on all interfaces.

```
<Huawei> reset pim ipv6 control-message counters
```

Related Topics

10.4.22 display pim ipv6 control-message counters

10.4.71 reset pim ipv6 routing-table

Function

The **reset pim ipv6 routing-table** command clears PIM status of the specified downstream interface of a specified PIM (IPv6) entry.

Format

reset pim ipv6 routing-table group *ipv6-group-address* **mask** *ipv6-group-mask-length* **source** *ipv6-source-address* **interface** *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group *ipv6-group-address*	Specifies the group address of an IPv6 PIM entry.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
mask *ipv6-group-mask-length*	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 0 to 128.
source *ipv6-source-address*	Specifies the source address of an IPv6 PIM entry.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset pim ipv6 routing-table** command clears PIM status of the specified downstream interface of a specified PIM entry.

Configuration Impact

Using this command can clear the PIM status of the specified interface in a specified PIM entry. The command cannot be used to clear the MLD and static group join status on a specified interface.

Precautions

This command is valid for only PIM-SM (IPv6).

NOTICE

Clearing PIM status of the downstream interfaces can trigger the sending of corresponding Join/Prune messages, which cause multicast service interruption.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear PIM status of the downstream interface GE1/0/0 of the (S, G) entry (FC00:0:0:2001::4,FF25::1).

```
<Huawei> reset pim ipv6 routing-table group ff25::1 mask 128 source fc00:0:0:2001::4 interface gigabitethernet 1/0/0
```

10.4.72 source-lifetime (IPv6)

Function

The **source-lifetime** command specifies the timeout period of an (S, G) entry on the router.

The **undo source-lifetime** command restores the default value of the timeout period.

By default, the timeout period is 210 seconds.

Format

source-lifetime *interval*

undo source-lifetime

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of an (S, G) entry on the router.	The value is an integer that ranges from 60 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router creates a timer for each (S, G) entry. The **source-lifetime** command is used to set the value of the timer. After receiving a multicast packet from S, the interface resets the timer. If the timer times out, the (S, G) entry is considered invalid.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

Set the timeout period of an (S, G) entry of the router to 200 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] source-lifetime 200
```

10.4.73 source-policy (IPv6)

Function

The **source-policy** command configures the router to filter received multicast data packets based on source addresses or source/group addresses.

The **undo source-policy** command deletes the configuration.

By default, a router does not filter received multicast data packets based on source addresses or source/group addresses.

Format

source-policy { *acl6-number* | **acl6-name** *acl6-name* }

undo source-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies number of the basic or advanced ACL.	The value is an integer that ranges from 2000 to 3999.
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized source information from being advertised on the PIM network, run the **source-policy** command to configure the router to filter received multicast data packets based on source addresses or source/group addresses.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If **source-policy** and the basic ACL are applied, all multicast data packets received should match the source address. Packets that do not pass the filtering are discarded.

If **source-policy** and the advanced ACL are used, the source addresses and group addresses of all received multicast data packets should be matched. Packets that do not pass the filtering are discarded.

The configurations of the Named ACL and advanced ACL are the same, and can implement filtering of both source addresses and multicast group addresses. The Named ACL can also be configured with the **time-range** parameter.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

Example

In the public network instance, configure the router to receive multicast data packets with the source address of fc00:0:0:3121::1 and to discard those with the source address of FC00:0:0:3121::2.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2001
[Huawei-acl6-basic-2001] rule permit source fc00:0:0:3121::1 128
[Huawei-acl6-basic-2001] rule deny source fc00:0:0:3121::2 128
[Huawei-acl6-basic-2001] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] source-policy 2001
```

In the public network instance, configure a Named ACL where multicast data packets with the source address of FC00:0:0:3121::1 are received, and those with the source address of 3121::2 are dropped.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source fc00:0:0:3121::1 128
[Huawei-acl6-adv-myacl6] rule deny ipv6 source fc00:0:0:3121::2 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] source-policy acl6-name myacl6
```

10.4.74 spt-switch-threshold (IPv6)

Function

The **spt-switch-threshold** command sets the rate threshold of the multicast packets when the DR at the member side joins the SPT.

The **undo spt-switch-threshold** command restores the default value.

By default, the system performs SPT switchover on receiving the first multicast data packet through the RPT.

Format

spt-switch-threshold { *traffic-rate* | **infinity** } [**group-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* } [**order** *order-value*]]

undo spt-switch-threshold [*traffic-rate* | **infinity**] [**group-policy** { *basic-acl6-number* | **acl6-name** *acl6-name* }]

Parameters

Parameter	Description	Value
traffic-rate	Specifies the threshold rate for the switchover from the RPT to the SPT. **NOTE** Setting this parameter may affect operation of multicast services. You are advised to use the default triggering condition. That is, an SPT switchover is triggered immediately after the first multicast data packet is received from the RPT. The default triggering condition can reduce the number of multicast packets forwarded on the RPT.	The value is an integer that ranges from 1 to 4194304, in kbit/s.
infinity	Indicates that the SPT switchover is never enabled.	-
basic-acl6-number	Specifies an entry of the group-policy list. It works with the multicast group that matches *basic-acl6-number* to enable the threshold. *basic-acl6-number* specifies the number of the basic ACL that defines the range of multicast groups.	If the parameter is not set, the threshold is applied to all multicast groups. The value ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive) and can contain numbers, hyphens (-), or underlines (_).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
order *order-value*	Adjusts the order of the ACLs in the group-policy list. If a group matches multiple ACLs, the threshold is selected in the order specified by *order-value*. *order-value* specifies the updated number.	The value is an integer. The value is any value other than original one in the current group-policy list. If the parameter is not set, the order of the ACLs in the group-policy list does not change.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source's DR encapsulates multicast packets in a Register message, and then transmits the unicast Register message to the RP. Then, the RP decapsulates the Register message and forwards the multicast packets to the receivers along the RPT. By default, when the RP or receiver's DR receives a first multicast packet, it initiates an SPT switchover to the source.

After the **spt-switch-threshold** command is executed on the receiver's DR, the receiver's DR periodically checks the forwarding rate of multicast packets. When the forwarding rate exceeds the threshold, the receiver's DR sends a Join messages to the source, triggering the SPT switchover.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If this command is used several times for the same group, the command that is first matched according to the order takes effect.

This command is valid to all devices that may function as the DR at the member side, but is invalid to RPs.

Precautions

This command is valid for only PIM-SM (IPv6).

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the threshold to 4 kbit/s. If the transmission rate of packets from the source to the multicast group is higher than the threshold, the router switches packets to the SPT towards the source.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] spt-switch-threshold 4
```

Add a group-policy: the ACL number, rate threshold, and order of the group-policy are 2010, 100 kbit/s, and 1 respectively.

```
<Huawei> system-view
[Huawei] acl ipv6 2010
[Huawei-acl6-basic-2010] rule permit source ff02:: 96
[Huawei-acl6-basic-2010] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] spt-switch-threshold 100 group-policy 2010 order 1
```

Add a group-policy: the ACL name, rate threshold, and order of the group-policy are myacl6, 100 kbit/s, and 1 respectively.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff03::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] spt-switch-threshold 100 group-policy acl6-name myacl6 order 1
```

Related Topics

10.4.82 timer spt-switch (IPv6)

10.4.75 ssm-policy (IPv6)

Function

The **ssm-policy** command sets the range of SSM group addresses.

The **undo ssm-policy** command restores the default configuration.

By default, the range of IPv6 SSM group addresses is FF3x::/32, where x cannot be 1 or 2.

Format

ssm-policy { *basic-acl6-number* | **acl6-name** *acl6-name* }

undo ssm-policy

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of the basic ACL that defines the range of SSM group addresses.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the SSM group address range is FF3x::/32, where x cannot be 1 or 2. You can run the **ssm-policy** command to specify the range of PIM SSM group addresses. All the PIM-SM (IPv6) interfaces consider that PIM SSM is enabled on all the multicast groups in the specified address range. The specified SSM group address range can exceed the default group address range.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Example

Set the range of PIM SSM multicast addresses to FF31:0:8192::/96.

```
<Huawei> system-view
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule permit source ff31:0:8192:: 96
[Huawei-acl6-basic-2000] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] ssm-policy 2000
```

Use a named ACL to set the PIM SSM group address range to FF31:0:8192::/96.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff31:0:8192:: 96
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] pim-ipv6
[Huawei-pim6] ssm-policy acl6-name myacl6
```

Related Topics

10.2.42 ssm-mapping (MLD view)

10.4.76 state-refresh-interval (IPv6)

Function

The **state-refresh-interval** command sets the interval for sending PIM State-Refresh messages.

The **undo state-refresh-interval** command restores the default value of the interval.

By default, the interval for sending PIM State-Refresh messages is 60 seconds.

Format

state-refresh-interval *interval*

undo state-refresh-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending PIM State-Refresh messages.	The value is an integer that ranges from 1 to 255, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the PIM-DM (IPv6) network, the device periodically sends State-Refresh messages to update the timeout interval of the prune timer on the downstream device. By doing this, the interface that has no multicast requirements retains in prune state.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This command is valid for only PIM-DM (IPv6).

To prevent a pruned interface from forwarding packets when the Prune status times out, the interval for sending State-Refresh messages is shorter than the period for keeping the Prune status.

You can run the **holdtime join-prune (IPv6)** command to set the period during which the device keeps the Prune status.

This command takes effect only when it is run on the routers directly connected to the source.

Example

Set the interval for sending PIM State-Refresh messages to 70s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] state-refresh-interval 70
```

Related Topics

10.4.60 pim ipv6 state-refresh-capable

10.4.77 state-refresh-rate-limit (IPv6)

10.4.78 state-refresh-ttl (IPv6)

10.4.77 state-refresh-rate-limit (IPv6)

Function

The **state-refresh-rate-limit** command sets the minimum period to wait before receiving the next PIM State-Refresh message.

The **undo state-refresh-rate-limit** command restores the default value.

By default, the minimum period to wait to receive the next PIM State-Refresh message is 30 seconds.

Format

state-refresh-rate-limit *interval*

undo state-refresh-rate-limit

Parameters

Parameter	Description	Value
interval	Specifies the minimum period for waiting to receive the next PIM State-Refresh message.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

PIM-IPv6 view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router can receive multiple PIM State-Refresh messages in a short period. Some of the messages are the same. To avoid duplicate messages, you can run the **state-refresh-rate-limit** command to set the period to wait to receive the next State-Refresh message.

- Before the State-Refresh timer times out, the router discards the received duplicate State-Refresh messages.
- After the State-Refresh timer times out, the router can receive the next State-Refresh message.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

Example

Set the minimum period to wait to receive the next PIM State-Refresh message to 45s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] state-refresh-rate-limit 45
```

Related Topics

10.4.60 pim ipv6 state-refresh-capable
10.4.76 state-refresh-interval (IPv6)
10.4.78 state-refresh-ttl (IPv6)

10.4.78 state-refresh-ttl (IPv6)

Function

The **state-refresh-ttl** command sets the TTL value for sending PIM State-Refresh messages.

The **undo state-refresh-ttl** command restores the default value of the TTL.

By default, the TTL value for sending PIM State-Refresh messages is 255.

Format

state-refresh-ttl *ttl-value*

 Copyright © Huawei Technologies Co., Ltd.

undo state-refresh-ttl

Parameters

Parameter	Description	Value
ttl-value	Specifies the minimum TTL value of the PIM state refresh message sent by an interface.	The value is an integer that ranges from 1 to 255.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a State-Refresh message, the router decreases the value of the TTL in the message by 1, and then sends the message to the downstream router until the value of the TTL becomes 0. If the scale of the network is small, the message is delivered in a loop.

You can use the **state-refresh-ttl** command to set the value of the TTL according to the scale of the network.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-DM (IPv6).

This command takes effect only when it is run on the routers directly connected to the source.

Example

Set the TTL value for sending PIM State-Refresh messages to 45.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] state-refresh-ttl 45
```

Related Topics

10.4.60 pim ipv6 state-refresh-capable

10.4.76 state-refresh-interval (IPv6)

10.4.77 state-refresh-rate-limit (IPv6)

 Copyright © Huawei Technologies Co., Ltd.

10.4.79 static-rp (IPv6)

Function

The **static-rp** command configures a static RP.

The **undo static-rp** command restores the default configuration.

By default, no static RP is configured.

Format

static-rp *rp-address* [*basic-acl6-number* | **acl6-name** *acl6-name*] [**preferred**]

undo static-rp *rp-address*

Parameters

Parameter	Description	Value
rp-address	Specifies address of a static RP.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
basic-acl6-number	Specifies the basic ACL that is used to control the range of multicast groups served by a static RP.	The value is an integer that ranges from 2000 to 2999.
acl6-name *acl6-name*	Specifies the name of a Named ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
preferred	Indicates that the static RP is preferred.	-

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only one RP exists in the network, you can manually configure a static RP rather than a dynamic RP. This can reduce bandwidth used to exchange information between the C-RP and the BSR.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

If the address of the static RP is the address of an interface in the Up state on the local host, the local host acts as the static RP. PIM (IPv6) does not need to be enabled on the interface of the static RP.

If no ACL number is specified in the command, the static RP serves all the multicast groups. If an ACL is specified but the ACL does not contain any rules, the static RP serves all the multicast groups. If the specified ACL has rules configured, the static RP serves only the multicast groups permitted by the ACL.

If the command used to configure the static RP does not contain **preferred**, devices apply BSR mechanism to elect a dynamic RP. If the dynamic RP is not configured in the network or the dynamic RP is invalid, the static RP becomes valid. If the command used to configure static RP contains **preferred**, the static RP is preferred.

If this command is used many times, multiple static RPs are configured. In the case that multiple static RPs serve a group, the RP with the largest IPv6 address is selected to serve the group. If *rp-address* of the RPs is identical, the latest RP replaces the previous one.

The **static-rp** command and the **acl ipv6** command are used together.

- For the IPv6 numbered ACL, in the ACL6 view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **source** parameter in the **rule** command. The filtering rule is effective only with the **source** parameter and the time period specified by the **time-range** parameter.
- For the IPv6 Named ACL, in the ACL6 view, when the **rule** command is used to configure a filtering rule, you can set the address range of multicast groups that are served by the static RP by specifying the **destination** parameter in the **rule** command. The filtering rule is effective only with the **destination** parameter and the time period specified by the **time-range** parameter.

Precautions

NOTE

Up to 50 static RPs can be configured by using this command repeatedly, but the same ACL cannot correspond to multiple static RPs. If the ACL is not referenced, only one static RP can be configured.

To make the static RP work normally, run the **static-rp** command on all devices in the PIM-SM (IPv6) domain.

Example

Configure the router with the address of FC00:0:0:1111::1111 as the static RP in the PIM-SM (IPv6) domain.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] static-rp fc00:0:0:1111::1111
```

Configure a Named ACL: the router with the address of FC00:0:0:1111::1111 functions as the static RP in the PIM-SM (IPv6) domain and serves groups defined by the ACL **myacl6**; preferential use of the static RP is enabled.

```
<Huawei> system-view
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 destination ff03::101 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] static-rp fc00:0:0:1111::1111 acl6-name myacl6 preferred
```

Related Topics

10.4.28 display pim ipv6 rp-info

10.4.80 timer hello (IPv6)

Function

The **timer hello** command sets the interval at which the PIM router sends Hello messages.

The **undo timer hello** command restores the default interval.

By default, the interval at which the PIM router sends Hello messages is 30 seconds.

Format

timer hello *interval*

undo timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer that ranges from 1 to 18000, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PIM devices periodically send Hello messages to maintain PIM neighbor relationships. You can run the **pim ipv6 timer hello** command to set the interval for sending Hello messages.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Configuration Impact

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval at which the PIM device sends Hello messages should be less than the timeout period of the PIM neighbor. You can run the **hello-option holdtime (IPv6)** command to set the timeout period of PIM neighbors.

The **timer hello** command has the same function as the **pim ipv6 timer hello** command in the interface view. By default, if the **pim ipv6 timer hello** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which PIM Hello messages are sent to 40s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] timer hello 40
```

Related Topics

10.4.63 pim ipv6 timer hello

10.4.33 hello-option holdtime (IPv6)

10.4.81 timer join-prune (IPv6)

Function

The **timer join-prune** command configures the interval at which Join/Prune messages are sent to an upstream device.

The **undo timer join-prune** command restores the default interval.

By default, the interval at which Join/Prune messages are sent to an upstream device is 60 seconds.

Format

timer join-prune *interval*

undo timer join-prune

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Join/Prune messages.	The value is an integer that ranges from 1 to 18000, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The router sends join information to the upstream device, requesting the upstream device to forward multicast data. The router sends prune information to the upstream device, requesting the upstream device to stop forwarding multicast data. Join information and prune information are encapsulated in Join/Prune messages. The PIM router periodically sends Join/Prune messages to the upstream router to update the forwarding status.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for both PIM-DM (IPv6) and PIM-SM (IPv6).

The interval configured using the **timer join-prune** command must be shorter than the interval configured using the **holdtime join-prune (IPv6)** command.

The **timer join-prune** command has the same function as the **pim ipv6 timer join-prune** command in the interface view. By default, if the **pim ipv6 timer join-prune** command is not used, the value configured in the PIM view is used; otherwise, the value configured in the interface view is used.

Example

Set the interval at which Join/Prune messages are sent to 80s.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] timer join-prune 80
```

Related Topics

10.4.64 pim ipv6 timer join-prune

10.4.82 timer spt-switch (IPv6)

Function

The **timer spt-switch** command sets the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT.

The **undo timer spt-switch** command restores the default value of the interval.

 Copyright © Huawei Technologies Co., Ltd.

By default, the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from the RPT to the SPT is 15 seconds.

Format

timer spt-switch *interval*

undo timer spt-switch

Parameters

Parameter	Description	Value
interval	Specifies the interval for checking whether the rate for transmitting multicast data exceeds the threshold before the switchover from RPT to SPT.	The value is an integer that ranges from 15 to 65535, in seconds.

Views

PIM-IPv6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **timer spt-switch** command to set the interval for checking whether the rate for transmitting multicast data exceeds the threshold.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is valid for only PIM-SM (IPv6).

Before running this command, you must set the threshold for SPT switchover by using the **spt-switch-threshold (IPv6)** command; otherwise, the **timer spt-switch** command takes no effect.

Example

Set the interval for checking the rate for transmitting the multicast data before the switchover from RPT to SPT to 30 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] pim-ipv6
[Huawei-pim6] timer spt-switch 30
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.4.74 spt-switch-threshold (IPv6)

10.5 MSDP Configuration Commands

NOTE

AR120 series do not support this function.

10.5.1 cache-sa-enable

Function

The **cache-sa-enable** command enables the SA cache function on a router. After receiving an SA message, the router caches (S, G) information carried in the SA message.

The **cache-sa-disable** command disables the SA cache function.

The **undo cache-sa-enable** command disables the SA cache function.

By default, the SA cache function is enabled on a router.

Format

cache-sa-enable

cache-sa-disable

undo cache-sa-enable

Parameters

None

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router enabled with the SA cache function locally saves (S, G) information carried in the received SA messages. When the router receives requests for receiving multicast data, it directly obtains (S, G) information from the SA cache.

A router no long saves (S, G) information carried in the received SA messages locally after the **undo cache-sa-enable** or the **cache-sa-disable** command is run to disable the SA cache function. When the router receives requests for receiving

 Copyright © Huawei Technologies Co., Ltd.

multicast data, it must wait for the SA messages sent by the MSDP peer in the next sending period. This may result in a delay in receiving multicast data.

Prerequisites

MSDP has been enabled using the **msdp** command.

Configuration Impact

When an RP receives a new (*, G) Join message,

- If the SA cache function is enabled, the RP searches the SA cache for the (S, G) information.
  - If the SA cache contains related (S, G) information, the RP directly joins the SPT with the root being S.
  - If the SA cache does not contain related (S, G) information, the RP does not process the received Join message.
- If the SA cache function is disabled, the RP processes the message according to whether the sending of SA Request messages is enabled.
  - If the sending of SA Request messages is enabled, the RP sends an SA Request message to the specified MSDP peer and waits for the response.
  - If the sending of SA Request messages is disabled, the RP must wait for the SA message sent by the MSDP peer in the next sending period.

Precautions

The **cache-sa-disable** and **undo cache-sa-enable** commands' configurations are both **undo cache-sa-enable** in the configuration file.

Example

Disable the SA cache function on the router in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] undo cache-sa-enable
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.20 peer request-sa-enable

10.5.2 display default-parameter msdp

Function

The **display default-parameter msdp** command displays default configurations about MSDP.

Format

display default-parameter msdp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command still displays the default configurations even after the MSDP parameters are changed. You can use this command to check the consistency of default configurations about MSDP parameters on MSDP peers.

Example

Display default configurations about MSDP.

```
<Huawei> display default-parameter msdp
  MSDP View Default Configurations:
  ---------------------------------
  Cache-sa-enable: enabled
  Msdp description:
  Encap-data-enable: disabled
  Request-sa-enable: disabled
  Sa-request-policy: disabled
  Sa-policy: disabled
  Connect-retry-period: 30 s
  Minimum TTL: 0
```

Table 10-72 Description of the display default-parameter msdp command output

Item	Description
MSDP View Default Configurations	Default configurations in the MSDP view.
Cache-sa-enable	Whether SA cache is enabled. By default, SA cache is enabled. This parameter is configured using the **cache-sa-enable** command.
Msdp description	Whether MSDP peer description is configured. By default, no description is configured for an MSDP peer. This parameter is configured using the **peer description (MSDP)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Encap-data-enable	Whether encapsulating multicast data packets into the SA message is enabled. By default, an SA message does not encapsulate any multicast packet. This parameter is configured using the **encap-data-enable** command.
Request-sa-enable	Whether sending an SA Request message immediately when a Join message is received. By default, when receiving a Join message, the router waits for the SA message in the next period instead of sending an SA Request message to its MSDP peer. This parameter is configured using the **peer request-sa-enable** command.
Sa-request-policy	Whether the filtering rule for responding to the SA Request message is configured. By default, the router is not configured with any filtering rule for responding to the SA Request message and responds to all SA Request messages from all MSDP peers. This parameter is configured using the **peer sa-request-policy** command.
Sa-policy	Whether the filtering rule for receiving or forwarding the SA message is configured. By default, the router does not filter the received or forwarded SA messages. This parameter is configured using the **peer sa-policy** command.
Connect-retry-period	Interval for retrying to set up a TCP connection between MSDP peers. By default, the interval for retrying to set up an MSDP peer relationship is 30 seconds. This parameter is configured using the **timer retry** command.
Minimum TTL	TTL value of SA messages that are encapsulated with multicast data. By default, the TTL value of SA messages that are encapsulated with multicast data is 0. This parameter is configured using the **peer minimum-ttl** command.

Related Topics

10.5.1 cache-sa-enable

10.5.10 encap-data-enable
10.5.14 peer connect-interface (MSDP)
10.5.15 peer description (MSDP)
10.5.18 peer minimum-ttl
10.5.20 peer request-sa-enable
10.5.23 peer sa-request-policy
10.5.22 peer sa-policy
10.5.30 timer retry

10.5.3 display msdp brief

Function

The **display msdp brief** command displays summary information about the status of MSDP peers.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **brief** [**state** { **connect** | **down** | **listen** | **shutdown** | **up** }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
state	Displays summary information about the MSDP peers in specified status.	-
connect	Indicates the MSDP peers in Connect state.	-
down	Indicates the MSDP peers in Down state.	-
listen	Indicates the MSDP peers in Listen state.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
shutdown	Indicates the MSDP peers in Shutdown state.	-
up	Indicates the MSDP peers in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MSDP peers establish a TCP connection, the **display msdp brief** command can be used to display the brief information about the remote MSDP peer, such as the address, AS number, the number of (S, G) entries, and the status of the TCP connection.

Precautions

This command displays summary information about the status of MSDP peers only when the MSDP peer has been configured.

Example

Display summary information about MSDP peers in the public network instance.

```
<Huawei> display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
 Configured   Up          Listen       Connect      Shutdown     Down
 2            2           0            0            0            0

 Peer's Address     State     Up/Down time    AS     SA Count   Reset Count
 192.168.3.2        Up        01:07:08        ?      8          0
 192.168.5.1        Up        00:16:39        ?      13         0
```

Table 10-73 Description of the display msdp brief command output

Item	Description
MSDP Peer Brief Information of VPN-Instance	VPN instance to which summary information about MSDP peers corresponds.
Configured	Total number of configured MSDP peers.
Up	Number of MSDP peers in Up state.
Listen	Number of MSDP peers in Listen state.
Connect	Number of MSDP peers in Connect state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Shutdown	Number of MSDP peers in Shutdown state.
Down	Number of MSDP peers in Down state.
Peer's Address	Address of the peer. This parameter is configured using the **peer connect-interface (MSDP)** command.
State	Status of the MSDP session. • Up: The connection is set up and is in Up state. • Listen: The local device acts as the server and is in Listen state. The connection is not set up. • Connect: The local device acts as the client and is in Connect state. The connection is not set up. • Shutdown: The MSDP peer is in Shutdown state. • Down: The connection fails.
Up/Down time	Time when the session becomes Up or Down. The time format is as follows: • Time that is shorter than or equal to 24 hours: hour: minute: second. • Time that is longer than 24 hours but shorter than or equal one week: day: hour. • Time that is longer than one week: week: day.
AS	The AS number of the MSDP peer. A question mark (?) indicates that the AS number cannot be obtained.
SA Count	Number of (S, G) entries in the SA cache.
Reset Count	Resetting times, including the resetting because the Notification message is received or Holdtimer times out.

Related Topics

10.5.6 display msdp peer-status
10.5.27 reset msdp statistics

10.5.4 display msdp control-message counters

Function

The **display msdp control-message counters** command displays statistics about MSDP messages.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**peer** *peer-address* | **message-type** { **source-active** | **sa-request** | **sa-response** | **keepalive** | **notification** | **traceroute-request** | **traceroute-reply** | **data-packets** | **unknown-type** }] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all instances, including the public network instance and all VPN instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
peer *peer-address*	Specifies IP address of MSDP peer. If **peer** *peer-address* is specified, only statistics about the MSDP messages received, sent, and discarded on a specified MSDP peer are displayed.	The value is in dotted decimal notation.
message-type	Specifies MSDP message types. If **message-type** is specified, only statistics about the MSDP messages received, sent, and discarded of a specified type are displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-active	Displays the statistics about Source-Active messages on the interface.	-
sa-request	Displays the statistics about Source-Active Request messages on the interface.	-
sa-response	Displays the statistics about Source-Active Response messages on the interface.	-
keepalive	Displays the statistics about KeepAlive messages on the interface.	-
notification	Displays the statistics about Notification messages on the interface.	-
traceroute-request	Displays the statistics about Traceroute Request messages on the interface.	-
traceroute-reply	Displays the statistics about Traceroute Reply messages on the interface.	-
data-packets	Displays the statistics about data packets on the interface.	-
unknown-type	Displays the statistics about unknown type messages on the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command helps you learn MSDP running status by displaying statistics about received, sent, and discarded MSDP messages.

Precautions

This command displays statistics about MSDP messages only when the MSDP peer has been configured.

Example

Display statistics about the MSDP messages that are received, sent, and discarded by the peer 192.168.3.3 in the public network instance.

```
<Huawei> display msdp control-message counters peer 192.168.3.3
 VPN-Instance: public net
```

```
MSDP message counters for peer: 192.168.3.3
                        Received        Sent            Invalid
Source-Active           0               0               0
Source-Active Request   0               0               0
Source-Active Response  0               0               0
KeepAlive               48              49              0
Notification            0               1               0
Traceroute Request      0               -               -
Traceroute Reply        0               -               -
Data Packets            0               0               0
Unknown Type            1               -               1
```

Table 10-74 Description of the display msdp control-message counters peer 192.168.3.3 command output

Item	Description
VPN-Instance	VPN instance in which MSDP message statistics are collected.
MSDP message counters for peer	IP addresses of MSDP peers.
Received	Number of received messages.
Sent	Number of sent messages.
Invalid	Number of invalid messages.
Source-Active	Source-Active message.
Source-Active Request	Source-Active Request message.
Source-Active Response	Source-Active Response message.
KeepAlive	Keepalive message.
Notification	Notification message.
Traceroute Request	Traceroute Request message.
Traceroute Reply	Traceroute Reply message.
Data Packets	Data packets.
Unknown Type	Unknown type message.

Related Topics

10.5.6 display msdp peer-status
10.5.24 reset msdp control-message counters

10.5.5 display msdp invalid-packet

Function

The **display msdp invalid-packet** command displays statistics about invalid MSDP messages received by a device and details of these messages.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **invalid-packet** [**peer** *peer-address* | **message-type** { **keepalive** | **notification** | **sa-request** | **sa-response** | **source-active** }] *

display msdp invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays statistics about invalid MSDP messages received in all VPN instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
peer *peer-address*	Displays statistics about invalid MSDP messages received from a specified peer. *peer-address* specifies an MSDP peer address.	The address is in dotted decimal notation.
message-type	Displays statistics about invalid MSDP messages of a specific type.	-
keepalive	Displays statistics about invalid Keepalive messages.	-
notification	Displays statistics about invalid Notification messages.	-
sa-request	Displays statistics about invalid Source-Active Request messages.	-
sa-response	Displays statistics about invalid Source-Active Response messages.	-
source-active	Displays statistics about invalid Source-Active messages.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
packet-number	Displays details about a specified number of invalid MSDP messages recently received. If this parameter is not specified, details about all invalid MSDP messages.	The value is an integer that ranges from 1 to 100.
verbose	Displays details about invalid MSDP messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display msdp invalid-packet** command to view statistics and details of invalid MSDP messages for fault location and rectification.

If MSDP peer relationships fail to be set up on a multicast network, you can run the **display msdp invalid-packet** command first to check whether devices have received invalid MSDP messages. If the command output contains statistics about invalid MSDP messages, run the **display msdp invalid-packet** [*packet-number*] **verbose** command to view details of invalid MSDP messages to locate the fault.

Example

Display statistics about invalid MSDP messages received by a device in the public network instance.

```
<Huawei> display msdp invalid-packet peer 192.168.1.1

            Statistics of invalid packets for public net:
-----------------------------------------------------------------
MSDP SA invalid packet:
Fault Length            : 0          Bad Length-x            : 0
Bad Sprefix             : 0          Invalid Multicast Group : 0
Invalid Multicast Source: 0          Bad Encap Data          : 0
Illegal RP Addr         : 0          RP Loop                 : 0

MSDP SA Response invalid packet:
Fault Length            : 0          Bad Length-x            : 0
Bad Sprefix             : 0          Invalid Multicast Group : 0
Invalid Multicast Source: 0          Illegal RP Addr         : 0
RP Loop                 : 0

MSDP SA Request invalid packet:
Fault Length            : 0          Invalid Multicast Group : 0

MSDP Keep Alive invalid packet:
Fault Length            : 0

MSDP Notification invalid packet:
Fault Length            : 0
-----------------------------------------------------------------
```

Table 10-75 Description of the display msdp invalid-packet peer 192.168.1.1 command output

Item	Description
Statistics of invalid packets for public net	Statistics about invalid MSDP messages in the public network instance.
MSDP SA invalid packet	Invalid SA messages.
Fault Length	Messages with invalid lengths.
Bad Length-x	Messages with invalid Length-x fields.
Bad Sprefix	Messages with invalid Sprefix fields.
Invalid Multicast Group	Messages with invalid multicast group addresses.
Invalid Multicast Source	Messages with invalid multicast source addresses.
Bad Encap Data	Messages with invalid data encapsulated.
Illegal RP Addr	Messages with illegal RP addresses.
RP Loop	Messages whose RP addresses are local addresses.
MSDP SA Response invalid packet	Invalid SA Response messages.
MSDP SA Request invalid packet	Invalid SA Request messages.
MSDP Keep Alive invalid packet	Invalid Keepalive messages.
MSDP Notification invalid packet	Invalid Notification messages.

Display details of a specific invalid MSDP message recently received in the public network instance.

```
<Huawei> display msdp invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Peer                 :  10.2.2.2
Time                 :  2010-6-9 11:25:46 UTC-08:00
Message Length       :  22
Invalid Type         :  Invalid Addr List
0000: 00 01 00 02 00 69 00 13 00 04 00 00 00 64 00 02
0010: 00 04 81 f4 09 c4
-----------------------------------------------------
```

Table 10-76 Description of the display msdp invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details about invalid MSDP messages.
Packet information (Index 1)	Sequence number of the invalid MSDP message (numbered in the opposite order that the message is received, for example, the index of the last received message is 1, the index of the last but one message is 2, and so on).
Peer	IP address of the peer that sends the invalid MSDP message.
Time	Time when the invalid MSDP message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid MSDP message.
Invalid Type	Type of the invalid MSDP message.
0000: 00 01 00 02 00 69 00 13 00 04 00 00 00 64 00 02 0010: 00 04 81 f4 09 c4	Contents of the invalid MSDP message.

Related Topics

10.7.23 multicast invalid-packet

10.5.6 display msdp peer-status

Function

The **display msdp peer-status** command displays the detailed information about MSDP peers.

 Copyright © Huawei Technologies Co., Ltd.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer-status** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
peer-address	Specifies the address of a remote MSDP peer. If this parameter is not specified, information about all the MSDP peers in the instance is displayed.	The address is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MSPD peers establish a TCP connection, the **display msdp peer-status** command can be used to display the detailed information about a specified MSDP peer, such as the interface status, interface configuration, policy for filtering messages, and number of messages.

Precautions

This command displays the detailed information about a specified MSDP peer only when the MSDP peer has been configured.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the detailed information about the MSDP peer 10.110.11.11 in the public network instance.

```
<Huawei> display msdp peer-status 10.110.11.11
MSDP Peer Information of VPN-Instance: public net
  MSDP Peer 10.110.11.11, AS 100
  Description:
  Information about connection status:
    State: Up
    Up/down time: 14:41:08
    Resets: 0
    Connection interface: LoopBack0 (10.110.11.22)
    Number of sent/received messages: 867/947
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 14:42:40
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
  Peer authentication: unconfigured
  Peer authentication type: none
```

Table 10-77 Description of the display msdp peer-status command output

Item	Description
MSDP Peer Information of VPN-Instance	VPN instance to which MSDP peer information belongs.
MSDP Peer	Address of the peer. This parameter is configured using the **peer connect-interface (MSDP)** command.
AS	AS number of the MSDP peer. A question mark (?) indicates that the AS number cannot be obtained.
Description	Description of the verbose information.
Information about connection status	Information of connection status.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of the MSDP session. ● Up: The connection is set up and is in the Up state. ● Listen: The local device acts as the server. The connection is not set up. ● Connect: The local device acts as the client. The connection is not set up. ● Shutdown: The MSDP peer is in Shutdown state. ● Down: The connection fails.
Up/down time	Time when the session becomes Up or Down. The time format is as follows: ● Time that is shorter than or equal to 24 hours: hour: minute: second. ● Time that is longer than 24 hours but shorter than or equal to one week: day: hour. ● Time that is longer than one week: week: day.
Resets	Resetting times.
Connection interface	Address of a connect-interface that is used to set up the TCP connection with the peer address. This parameter is configured using the **peer connect-interface (MSDP)** command.
Number of sent/ received messages	Number of MSDP messages received or sent through the connection.
Number of discarded output messages	Number of discarded messages.
Elapsed time since last connection or counters clear	Time that elapsed since the MSDP peer resetting count and control packet statistics were reset.
Information about (Source, Group)-based SA filtering policy	● Import policy: is used to receive the filtering list of the SA messages of a specified MSDP peer. You can configure the policy using the **peer sa-policy import** command. ● Export policy: is used to forward the filtering list of the SA messages of a specified MSDP peer. You can configure the policy using the **peer sa-policy export** command. By default, the SA messages received and forwarded are not filtered. The MSDP peer receives and forwards all the SA messages. The item is expressed by none.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Information about SA-Requests	• Policy to accept SA-Request messages: restricts the SA request messages received from an MSDP peer by the router. By default, the router receives all the SA Request messages sent by the MSDP peer. The item is expressed by none. You can set the policy using the **peer sa-request-policy** command. • Sending SA-Requests status: enables or disables the router to send SA request messages to a specified MSDP peer when the router receives a Join message. By default, when receiving a Join message, the router does not send the SA Request message to its MSDP peers, but waits for the next SA message. You can configure the router to send SA Request messages using the **peer request-sa-enable** command.
Minimum TTL to forward SA with encapsulated data	If the SA message received is encapsulated with the multicast data packet, the router forwards the SA message to other peers only when the TTL of the packet is not smaller than the minimum TTL. You can configure the function using the **peer minimum-ttl** command.
SAs learned from this peer	SA messages that pass through the MSDP peer and the number of SA entries in the cache.
SA-cache maximum for the peer	Maximum number of (S, G) entries in the cache when the router receives the SA message from an MSDP peer. You can configure the maximum number of (S, G) entries in the cache using the **peer sa-cache-maximum** command.
Input queue size	Length of the data in the input cache.
Output queue size	Length of the data in the output cache.
Counters for MSDP message	Number of MSDP messages. • Count of RPF check failure: indicates the number of SA messages discarded because of the RPF check failure. • Incoming/outgoing SA messages: indicates the number of sent or received SA messages. • Incoming/outgoing SA requests: indicates the number of sent or received SA-Request messages. • Incoming/outgoing SA responses: indicates the number of sent or received SA-Response messages. • Incoming/outgoing data packets: indicates the number of sent or received SA messages that are encapsulated with multicast data packets.
Peer authentication	Whether MSDP authentication is configured.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Peer authentication type	MSDP authentication modes, including: • none: indicates authentication is not configured. • MD5: indicates MD5 authentication. This parameter is configured using the **peer password (MSDP)** command. • Keychain: indicates Keychain authentication. This parameter is configured using the **peer keychain (MSDP)** command.

Related Topics

10.5.3 display msdp brief
10.5.14 peer connect-interface (MSDP)
10.5.16 peer keychain (MSDP)
10.5.18 peer minimum-ttl
10.5.19 peer password (MSDP)
10.5.20 peer request-sa-enable
10.5.23 peer sa-request-policy
10.5.21 peer sa-cache-maximum
10.5.22 peer sa-policy
10.5.25 reset msdp peer

10.5.7 display msdp rpf-peer

Function

The **display msdp rpf-peer** command displays information about all RPF peers of a specific source RP address, including RPF peer selection rules and RPF route types.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **rpf-peer original-rp** *original-rp-address*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Displays information about all the RPF peers of a specific source's RP address in all instances. If **vpn-instance** or **all-instance** is not specified, only the public network instance is displayed.	-
original-rp *original-rp-address*	Displays information about all the RPF peers of a specific source's RP address. *original-rp-address* specifies the source's RP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To prevent SA messages from being forwarded circularly between MSDP peers, MSDP performs RPF check on received SA messages to control the incoming SA messages. SA messages that do not comply with RPF rules are discarded.

The **display msdp rpf-peer** command is used to check whether the forwarding path of SA messages works properly. Based on the RPF peer information in the command output, you can check every hop in the forwarding path. If the forwarding path is works improperly, this command helps you locate the faulty node.

Precautions

A device does not perform the RPF peer check on the SA messages received from an MSDP peer in the following situations:

- The address of the MSDP peer is the RP address of the source.

 Copyright © Huawei Technologies Co., Ltd.

- The MSDP peer is a static RPF peer of the device.
- The MSDP peer is a unique MSDP peer of the device.
- The MSDP peer has joined a full-mesh group. It is a member of a mesh group.

Before configuring this command, ensure that MSDP peers are configured. Only the MSDP peers with Up TCP connection can become RPF peers.

Example

Display information about RPF peers of the source RP 192.168.4.5 in the public network instance.

```
<Huawei> display msdp rpf-peer original-rp 192.168.4.5
MSDP RPF peer information of VPN-Instance: public net
 MSDP RPF peer information for Original RP: 192.168.4.5
 01. RPF peer: 10.6.6.6
  RPF selection rule: Peer is IGP next hop of best route
  RPF used topology: default
  RPF route type: multicast(static)
```

Table 10-78 Description of the display msdp rpf-peer original-rp command output

Item	Description
MSDP RPF peer information of VPN-Instance: public net	VPN instance to which MSDP peer information belongs.
MSDP RPF peer information for Original RP	Information about the MSDP RPF peer of a specific source's RP address.
01. RPF peer	RPF peer address.
RPF selection rule	RPF peer selection rule: ● Peer is IGP next hop of best route: RPF peer is a next hop of an IGP route. ● Peer is IGP advertiser of best route: RPF peer is a forwarder of an IGP route. ● Peer is in the AS-path to original RP: RPF peer is on an AS-path to the RP address of the source. ● Peer is BGP/MBGP next hop of best route: RPF peer is a next hop of a/an BGP/MBGP route. ● Peer is BGP/MBGP advertiser of best route: RPF peer is a forwarder of a/an BGP/MBGP route.
RPF used topology	RPF used topology: ● default: default topology. ● multicast: multicast topology. ● topology name (user-defined): unicast topology.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RPF route type	RPF route type: ● mbgp: MBGP route. ● unicast(bgp): BGP route ● multicast(static): static multicast route. ● unicast: IGP route (unicast route).

10.5.8 display msdp sa-cache

Function

The **display msdp sa-cache** command displays (S, G) entries in the SA cache.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address* | *source-address* | [*as-number-plain* | *as-number-dot*]] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
group-address	Specifies the group address of an (S, G) entry. It is used to display the corresponding (S, G) of the group in SA Cache.	The value is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
source-address	Specifies the source address of an (S, G) entry. It is used to display the corresponding the (S, G) of the source.	The value is in dotted decimal notation.
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the SA cache function is enabled, the **display msdp sa-cache** command can be used to display the information about (S, G) entries learned from other MSDP peers in the SA cache. The information includes the source address, group address, address of the source's RP, routing protocol, AS number, and timeout period of entries.

Precautions

This command displays (S, G) entries in the SA cache only when SA cache has been enabled. By default, SA cache is enabled.

Example

Display (S, G) entries in the SA cache in the public network instance.

```
<Huawei> display msdp sa-cache
MSDP Source-Active Cache Information of VPN-Instance: public net
 MSDP Total Source-Active Cache - 2 entries
 MSDP matched 2 entries

(10.0.5.120, 225.0.0.1)
 Origin RP: 3.3.3.3
 Pro: ?, AS: ?
 Uptime: 00:01:01, Expires: 00:05:59

(10.0.5.120, 225.0.0.2)
 Origin RP: 3.3.3.3
 Pro: ?, AS: ?
 Uptime: 00:00:01, Expires: 00:05:59
```

Table 10-79 Description of the display msdp sa-cache command output

Item	Description
MSDP Source-Active Cache Information of VPN-Instance	MSDP SA cache in the public network instance.

Item	Description
MSDP Total Source-Active Cache - 2 entries	Two entries are cached by MSDP SA.
MSDP matched 2 entries	Two entries are matched by MSDP, such as the filtering policy and specified source/group address.
(10.0.5.120, 225.0.0.1)	(source address, group address) entry.
Origin RP	Source RP address that advertises the (S, G) entry.
Pro	Type of the protocol from which the AS number of the source RP is obtained. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.
AS	AS number of the source RP. A question mark (?) indicates the protocol type if the AS number of the source RP cannot be obtained.
Uptime	Time when the (S, G) entry is created in the cache.
Expires	Time when the (S, G) entry in the cache times out.

Related Topics

10.5.1 cache-sa-enable
10.5.26 reset msdp sa-cache

10.5.9 display msdp sa-count

Function

The **display msdp sa-count** command displays statistics about the (S, G) entries in the SA cache.

Format

display msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-count** [*as-number-plain* | *as-number-dot*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only statistics about the public network instance is displayed.	-
as-number-plain	Specifies the number of the AS, in integer format.	The value is an integer that ranges from 1 to 4294967295.
as-number-dot	Specifies the number of the AS, in dotted notation.	The value is in the x.y format. Here, "x" and "y" are integers that range from 1 to 65535 and 0 to 65535 respectively.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the SA cache function is enabled, the **display msdp sa-count** command can be used to display the statistics about the (S, G) entries in the SA cache, including the addresses of the peers that send SA messages and the (S, G) entry statistics collected according to the AS numbers of sources' RPs.

Precautions

This command displays the number of (S, G) entries in the SA cache only when the MSDP peer has been enabled with SA cache. By default, the SA cache function is enabled.

Example

Display the number of (S, G) entries in the SA cache in the public network instance.

```
<Huawei> display msdp sa-count
MSDP Source-Active Count Information of VPN-Instance: public net
  Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5

  Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                   3

  Total 5 Source-Active entries matched
```

Table 10-80 Description of the display msdp sa-count command output

Item	Description
MSDP Source-Active Count Information of VPN-Instance	VPN instance to which the SA cache information belongs.
Number of cached Source-Active entries, counted by Peer	Number of the (S, G) entries that are cached according to peers.
Peer's Address	Address of the peer that sends the SA message.
Number of SA	Number of the (S, G) entries received from the peer.
Number of source and group, counted by AS	Number of the (S, G) entries that is counted according to the AS to which the source RP belongs.
AS	AS number.
Number of source	Number of sources in the AS.
Number of group	Number of groups in the AS.
Total 5 Source-Active entries matched	Number of (S, G) entries matching specified conditions in the cache.

Related Topics

10.5.1 cache-sa-enable
10.5.21 peer sa-cache-maximum

10.5.10 encap-data-enable

Function

The **encap-data-enable** command enables the device to encapsulate a multicast data packet into an SA message.

The **undo encap-data-enable** command disables the device from encapsulating a multicast data packet into an SA message.

By default, no multicast data packet is encapsulated into an SA message.

Format

encap-data-enable

undo encap-data-enable

Parameters

None

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The source RP encapsulates information about all active sources into multiple SA messages to advertise it. Each SA message contains multiple (S, G) entries.

After the **encap-data-enable** command is used on the RP at the source side, the RP encapsulates the multicast data carried in the Register message into an SA message, and then sends the SA message to the MSDP peer. Only one multicast data packet can be encapsulated into an SA message.

After the **encap-data-enable** command is used on the MSDP peer, the router can transmit the SA messages carrying a multicast data packet between PIM-SM domains.

Prerequisites

MSDP has been enabled using the **msdp** command.

Example

Encapsulate a multicast data packet into an SA message

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] encap-data-enable
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

 Copyright © Huawei Technologies Co., Ltd.

10.5.11 import-source

Function

The **import-source** command prevents the information about active sources in a domain from being advertised when an SA message is created.

The **undo import-source** command restores the default configuration.

By default, the information about all active sources is advertised in a domain through SA messages.

Format

import-source [**acl** { *acl-number* | *acl-name* }]

undo import-source

Parameters

Parameter	Description	Value
acl	Indicates the ACL that controls which source is to be advertised to a domain through an SA message and to which groups the SA message is to be advertised. If this parameter is not specified, multicast sources are not advertised.	-
acl-number	Specifies the number of the basic ACL or advanced ACL. ● Basic ACL: filters source addresses. ● Advanced ACL: filters source addresses and multicast group addresses.	The value is an integer that ranges from 2000 to 3999.
acl-name	Specifies the name of a named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the **import-source** command is used, MSDP filters advertised (S, G) forwarding entries based on source addresses when creating SA messages. Therefore, when creating SA messages, MSDP can control the transmission of information about multicast sources.

You can also run the **peer sa-policy** command to filter the SA messages to be forwarded.

Prerequisites

MSDP has been enabled using the **msdp** command.

Precautions

The **import-source** and **acl** commands are used together.

- In the basic ACL view, set the source address range of advertised multicast packets using SA messages by specifying the **source** parameter in the **rule** command.
- In the advanced ACL view, set the source address range of advertised multicast packets using SA messages by specifying the **source** parameter in the **rule** command, and set the address range of advertised multicast groups using SA messages by specifying the **destination** parameter in the **rule** command.

Example

Configure an MSDP peer to advertise the information about a specified active source when creating SA messages in the public network instance. The multicast source is on 10.10.0.0/16 network segment, and the multicast group address is 225.1.0.0/16.

```
<Huawei> system-view
[Huawei] acl number 3101
[Huawei-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-3101] quit
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] import-source acl 3101
```

Configure an MSDP peer to advertise the information about a specified active source when creating SA messages. The multicast source is on 10.10.0.0/16 network segment, and the multicast group address is 225.1.0.0/16 in the public network instance using a named ACL.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.10.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] import-source acl myacl
```

Related Topics

10.5.12 msdp
10.7.28 multicast routing-enable

10.5.22 peer sa-policy

10.5.12 msdp

Function

The **msdp** command enables MSDP and displays the MSDP view in the public network instance or the VPN instance.

The **undo msdp** command clears all configurations in the MSDP view, releases the resources occupied by MSDP, and restores the initial state.

By default, MSDP is disabled.

Format

msdp [**vpn-instance** *vpn-instance-name*]

undo msdp [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MSDP in the public network instance or the VPN instance, you can run the **msdp** command to enable MSDP and display the MSDP view. All the configurations related to MSDP peers must be done in the MSDP view.

Prerequisites

The multicast routing function has been enabled using the **multicast routing-enable** command in the public network instance view or VPN instance view.

Configuration Impact

Running the **undo msdp** command interrupts MSDP services. Therefore, use this command with caution.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable MSDP in the public network instance and enter the MSDP view of the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp]
```

Enable MSDP in the VPN instance **mytest** and enter the MSDP view of the VPN instance.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] route-distinguisher 100:1
[Huawei-vpn-instance-mytest-af-ipv4] multicast routing-enable
[Huawei-vpn-instance-mytest-af-ipv4] quit
[Huawei-vpn-instance-mytest] quit
[Huawei] msdp vpn-instance mytest
[Huawei-msdp-mytest]
```

Related Topics

10.7.28 multicast routing-enable

10.5.13 originating-rp

Function

The **originating-rp** command configures an RP to replace the source RP address in the SA message with an IP address of a specified interface when the RP constructs an SA message. This interface is also called a logical RP.

The **undo originating-rp** command restores the default configuration.

By default, the source RP address in an SA message is the address of the RP that actually sends the SA message.

Format

originating-rp *interface-type interface-number*

undo originating-rp

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface that functions as a logical RP.	The routes on multicast tunnel interfaces (MTIs) are not advertised to private networks, so do not use the addresses of MTIs as the logical RP addresses.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You must run this command when configuring anycast RP in a PIM-SM domain.

An MSDP peer performs the RPF check on a received SA message and then discards the message if the address of the local RP and the remote RP are the same. In anycast RP, however, you need to configure RPs on two or more devices in a PIM-SM domain, assign the same IP address to these RPs, and set up MSDP peer relationships between these devices. You must configure an address that is different from the actual RP address for the logical RP so that the SA message can pass the RPF check.

Prerequisites

MSDP has been enabled using the **msdp** command.

Precautions

The interface functioning as a logical RP cannot be an actual RP interface. Commonly, the interfaces setting up an MSDP peer relationship can be specified as logical RP addresses.

Example

Configure GE1/0/0 as the logical RP for the SA message in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] originating-rp gigabitethernet 1/0/0
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

Function

The **peer connect-interface** command configures an MSDP peer.

The **undo peer** command removes the configured MSDP peer.

By default, no MSDP peer is configured.

Format

peer *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a remote MSDP peer.	The address is in dotted decimal notation.
interface-type interface-number	Specifies the type and the number of the interface. The local router uses the primary address of the interface as the source IP address to set up the TCP connection with the remote MSDP peer.	The routes on multicast tunnel interfaces (MTIs) are not advertised to private networks, so do not use the addresses of MTIs as the logical RP addresses.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP peers are identified by addresses. You can run the **peer connect-interface** command on two devices to specify the peer addresses for each other and specify interfaces for establishing the TCP connection. In this way, an MSDP peer connection is established.

Prerequisites

MSDP has been enabled using the **msdp** command.

Configuration Impact

You can run the **peer** *peer-address* **connect-interface** *interface-type interface-number* command repeatedly to configure multiple MSDP peers for the local router.

- You can specify the same *interface-type interface-number* for different *peer-address*. That is, you can specify the same local interface for different remote peers.
- You can specify different *interface-type interface-number* for different *peer-address*. That is, you can specify different local interfaces for different remote peers.

Precautions

Run the **peer connect-interface** command before running other peer commands. Otherwise, the system prompts that the peer does not exist.

When configuring a static RPF peer, you need to first run the **peer connect-interface** command to set the remote end as an MSDP peer and then the **static-rpf-peer** command to set the MSDP peer as a static RPF peer.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure IP address 10.10.7.6 for the remote MSDP peer and specify GE1/0/0 as the local interface in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.29 static-rpf-peer

10.5.15 peer description (MSDP)

Function

The **peer description** command adds the description text for an MSDP peer.

The **undo peer description** command restores the default configuration.

By default, an MSDP peer does not have the description text.

Format

peer *peer-address* **description** *text*

undo peer *peer-address* **description**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
text	Specifies the description text.	The description text is a string of 1 to 80 case-sensitive characters.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

If multiple MSDP peers are configured on the network, the MSDP peers cannot be easily distinguished only based on IP addresses. The administrator can distinguish the MSDP peers by setting the description texts for them.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Add an description **ClientA** for the MSDP peer with the IP address being 10.10.7.6 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 description ClientA
```

Related Topics

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.16 peer keychain (MSDP)

Function

The **peer keychain** command configures keychain authentication for establishing a TCP connection between MSDP peers and transmitting MSDP message.

The **undo peer keychain** command removes keychain authentication between MSDP peers.

By default, MSDP keychain authentication is not configured.

Format

peer *peer-address* **keychain** *keychain-name*

undo peer *peer-address* **keychain**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
keychain-name	Specifies the name of the keychain. This parameter is set using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP supports MD5 authentication and keychain authentication that improves security on TCP connections between MSDP peers. Keychain authentication supports multiple algorithms. Compared to MD5 authentication, keychain authentication applies to networks require high security.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

A keychain in accordance with the configured *keychain-name* has been enabled using the **keychain** command; otherwise, the TCP connection cannot be set up.

Precautions

You must configure keychain authentication on both MSDP peers. Note that encryption algorithms and passwords configured for keychain authentication on both peers must be the same; otherwise, the TCP connection cannot be set up between MSDP peers and MSDP messages cannot be transmitted.

MSDP MD5 authentication and MSDP keychain authentication are mutually exclusive.

Example

Configure MSDP keychain authentication between the local router and the peer 10.1.1.2 and configure a keychain named **huawei** in the public network instance.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] algorithm sha-256
[Huawei-keychain-huawei-keyid-1] key-string cipher Huawei@1234
[Huawei-keychain-huawei-keyid-1] quit
[Huawei-keychain-huawei] quit
[Huawei] multicast routing-enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] msdp
[Huawei-msdp] peer 10.1.1.2 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.1.1.2 keychain huawei
```

Related Topics

19.20.4 keychain
10.5.12 msdp
10.7.28 multicast routing-enable
10.5.19 peer password (MSDP)

10.5.17 peer mesh-group

Function

The **peer mesh-group** command adds an MSDP peer to a mesh group.

The **undo peer mesh-group** command restores the default configuration.

By default, an MSDP peer does not belong to any mesh group.

Format

peer *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer that is to be a member of a mesh group.	The address is in dotted decimal notation.
name	Specifies the name of a mesh group.	The name is a string of 1 to 32 case-sensitive characters.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If multiple MSDP peers exist on a network, SA messages may be flooded between peers. Especially when many MSDP peers are configured in the same PIM-SM domain, RPF rules cannot filter out useless SA messages effectively. The MSDP peer needs to perform the RPF check on each received SA messages, which brings a heavy load to the system.

 Copyright © Huawei Technologies Co., Ltd.

Configuring multiple MSDP peers to join the same mesh group can reduce the number of SA messages transmitted between these MSDP peers and release the load of the system.

Prerequisites

The device has established MSDP peer relationships with current mesh group members using the **peer connect-interface** command.

Configuration Impact

One MSDP peer can join only one mesh group. If an MSDP peer is configured to join different mesh groups for several times, the latest configuration takes effect.

When a member of the mesh group receives an SA message, it checks the source of the SA message:

- If the SA message is sent by a certain MSDP peer outside the mesh group, the member performs the RPF check on the SA message. If the SA message passes the check, the member forwards it to other members of the mesh group.
- If the SA message is sent by a member of the mesh group, the member directly accepts the message without performing the RPF check. In addition, it does not forward the message to other members in the mesh group.

Precautions

The MSDP peer relationships must be established between the peers in a mesh group.

Commonly, the MSDP peers in the same AS join the same mesh group and EBGP routes need be configured between inter-AS MSDP peers.

Example

Add the MSDP peer with the address of 10.10.7.6 to the mesh group **Group1** in the public network instance

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 mesh-group Group1
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.18 peer minimum-ttl

Function

The **peer minimum-ttl** command sets a TTL threshold for the multicast data packet that can be encapsulated in an SA message and forwarded to a specified MSDP peer.

The **undo peer minimum-ttl** command restores the default value.

By default, the TTL threshold is 0.

Format

peer *peer-address* **minimum-ttl** *ttl*

undo peer *peer-address* **minimum-ttl**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
ttl	Specifies the TTL threshold.	The value is an integer that ranges from 0 to 255.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP peers transmit SA messages to each other over an established TCP connection. The **peer minimum-ttl** command is used to limit the forwarding of SA messages with multicast data packets encapsulated.

After the TTL threshold is set for a specified peer, the router checks the TTL of a multicast data packet before encapsulating the multicast data packet in an SA message. Only the multicast data packet with the TTL being greater than the threshold is encapsulated in an SA message and sent to the peer of the router.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Set the TTL threshold to 10. Only the multicast data packet with the TTL value being greater than 10 is encapsulated in the SA message and forwarded to MSDP peer 10.10.10.1 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.10.1 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.10.1 minimum-ttl 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.5.6 display msdp peer-status
10.5.12 msdp
10.7.28 multicast routing-enable
10.5.14 peer connect-interface (MSDP)

10.5.19 peer password (MSDP)

Function

The **peer password** command configures MD5 authentication for establishing a TCP connection between MSDP peers.

The **undo peer password** command removes the MD5 authentication between MSDP peers.

By default, the MSDP MD5 authentication is not configured.

Format

peer *peer-address* **password** { **cipher** *cipher-password* | **simple** *simple-password* }

undo peer *peer-address* **password**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.
cipher *cipher-password*	Specifies the password in the cipher text.	The value is a string of case sensitive characters without any space. A cipher password may contain 1 to 255 plain characters or 20 to 392 encrypted characters. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
simple *simple-password*	Specifies the password in the plain text. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings high security risks. It is recommended that you select **cipher** to save the password in cipher text. To improve the device security, change the password periodically.	The value is a string of 1 to 255 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MSDP supports MD5 authentication and keychain authentication that improves security on TCP connections between MSDP peers.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

MD5 is not a secure authentication algorithm. For security purposes, you are advised to use the more secure Keychain algorithm for MSDP authentication.

MSDP peers must be configured with the same authentication password; otherwise, the TCP connections cannot be set up between MSDP peers and MSDP messages cannot be transmitted. The authentication password on peers can be in different formats, for example, the password on one end can be in the cipher text while the password on the peer can be in the plain text.

MSDP MD5 authentication and MSDP keychain authentication are mutually exclusive.

Example

Configure MSDP MD5 authentication between the local router and the peer 10.1.1.1 and set the authentication password to **Huawei@1234** in the cipher text.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
```

```
[Huawei-msdp] peer 10.1.1.1 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.1.1.1 password cipher Huawei@1234
```

Related Topics

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.16 peer keychain (MSDP)

10.5.20 peer request-sa-enable

Function

The **peer request-sa-enable** command enables the function of immediately sending the SA Request message to a specified MSDP peer.

The **undo peer request-sa-enable** command restores the default configuration.

By default, when receiving a new Join message for a group, the router does not send an SA Request messages to MSDP peer but waits to receive the next SA message.

Format

peer *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a new user joins multicast group G in a PIM-SM domain, a (*, G) entry is created on the RP. If no corresponding (S, G) information exists on the RP and SA cache is not enabled on the RP, multicast routes cannot be generated for this user. The RP then must wait for the next SA message from the remote MSDP peer to obtain valid (S, G) information.

 Copyright © Huawei Technologies Co., Ltd.

Generally, the interval for an MSDP peer to send SA messages is set to a large value to reduce traffic load in the PIM-SM domain. This, however, will cause a delay in joining the source's SPT. To minimize the delay, enable the function of immediately sending SA Request messages on the local RP and enable the SA cache function on the remote MSDP peer. Then after a new Join message is received but the local entries and SA cache do not contain corresponding (S, G) information, the local RP immediately sends an SA Request message to the remote MSDP peer instead of waiting to receive the next SA message.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Precautions

Before configuring the **peer request-sa-enable** command on the local router, disable SA cache on the local router and enable SA cache on the peer of the specified *peer-address*. Therefore, when the local router has new receiving requests, it can actively send SA Request messages to the peer and receive responses from the peer.

Example

Configure the router to send SA Request messages to the MSDP peer 10.10.7.6 when receiving a new Join message in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 request-sa-enable
```

Related Topics

10.5.1 cache-sa-enable

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.21 peer sa-cache-maximum

Function

The **peer sa-cache-maximum** command sets the maximum number of (S, G) entries that are learned from MSDP peers and cached in the SA cache.

The **undo peer sa-cache-maximum** command restores the maximum number of (S, G) entries that are learned from MSDP peers and cached in the SA cache to the default value.

By default, the maximum number of (S, G) entries in the SA cache is 1638.

 Copyright © Huawei Technologies Co., Ltd.

Format

peer *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

Parameters

Parameter	Description	Value
peer-address	Specifies the IP address of an MSDP peer.	The address is in dotted decimal notation.
sa-limit	Specifies the maximum number of (S, G) entries that are allowed to cache.	The number is an integer that ranges from 1 to 4294967295.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

It is recommended that you perform this configuration on all MSDP peers on a network vulnerable to DoS attacks.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Configuration Impact

The total number of (S, G) entries that can be stored in SA-Cache is limited by the specification of the SA-Cache. At present, for an entire router, the maximum number of (S, G) entries in SA-Cache is 1638.

For the (S, G) entries of a single peer, the following situations occur:

- If the number of (S, G) entries is not set or exceeds 1638, the maximum number of (S, G) entries in the SA cache can be set to 1638.
- If the number of (S, G) entries is smaller than 1638, the maximum number of (S, G) entries in the SA cache is the configured value. The redundant (S, G) entries are not cached or advertised to PIM-SM but can be forwarded through SA messages.

Example

Set the maximum number of (S, G) entries that are learned from MSDP peer 10.10.7.6 in the public network instance and cached in the SA cache to 100.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] cache-sa-enable
[Huawei-msdp] peer 10.10.7.6 sa-cache-maximum 100
```

Related Topics

10.5.1 cache-sa-enable

10.5.9 display msdp sa-count

10.5.6 display msdp peer-status

10.5.3 display msdp brief

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.22 peer sa-policy

Function

The **peer sa-policy** command sets a filtering policy for SA messages received or forwarded.

The **undo peer sa-policy** command restores the default configuration.

By default, the SA messages received and forwarded are not filtered. That is, all (S, G) entries are received and forwarded to MSDP peers.

Format

peer *peer-address* **sa-policy** { **import** | **export** } [**acl** { *advanced-acl-number* | *acl-name* }]

undo peer *peer-address* **sa-policy** { **import** | **export** }

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a remote MSDP peer.	The address is in dotted decimal notation.
import	Receives the SA messages from a specified MSDP peer. After the **import** parameter is used, when an SA message reaches the local router from the specified peer, the local router filters the message using the import policy to determine whether to process the SA message.	-

Parameter	Description	Value
export	Forwards the SA messages to a specified MSDP peer. After the **export** parameter is used, a router filters an SA message using the export policy to determine whether to forward the SA message.	-
acl	Indicates the ACL that defines the import or export policy. ● In the import policy, if this parameter is not configured, the router does not receive SA messages from any MSDP peer; if this parameter is configured, the router receives SA messages that carry the (S, G) entry only from a specified MSDP peer. ● In the export policy, if this parameter is not configured, the router does not forward SA messages from any MSDP peer; if this parameter is configured, the router forwards SA messages that carry the (S, G) entry only to a specified MSDP peer.	-
advanced-acl-number	Specifies the number of the advanced ACL.	The number is an integer that ranges from 3000 to 3999.
acl-name	Specifies the name of a named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **peer sa-policy** command is used, MSDP can filter (S, G) forwarding entries carried in the SA message received from or forwarded to specified MSDP

peers according to multicast sources. The transmission of multicast source information is controlled when SA messages are received and forwarded.

Besides controlling the transmission of SA messages, you can run the **import-source** command on the peer nearest to the source to control the creation of SA messages.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Example

Configure the router to forward only the SA messages that pass the ACL3100 filtering to peer 10.10.7.6 in the public network instance.

```
<Huawei> system-view
[Huawei] acl number 3100
[Huawei-acl-adv-3100] rule permit ip source 10.15.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-3100] quit
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 sa-policy export acl 3100
```

Configure a named ACL so that the router forwards SA messages only to peer 10.10.7.6 in the public network instance.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 10.15.0.0 0.0.255.255 destination 225.1.0.0 0.0.255.255
[Huawei-acl-adv-myacl] quit
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.10.7.6 sa-policy export acl myacl
```

Related Topics

10.5.6 display msdp peer-status

10.5.11 import-source

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.23 peer sa-request-policy

Function

The **peer sa-request-policy** command configures the filtering policy to respond to the SA Request messages sent by a specified MSDP peer. Once the SA Request message passes the filtering, the router responds to the SA message immediately.

The **undo peer sa-request-policy** command restores the default configuration.

By default, the router responds to all SA request messages sent by all MSDP peers.

Format

peer *peer-address* **sa-request-policy** [**acl** { *basic-acl-number* | *acl-name* }]

undo peer *peer-address* **sa-request-policy**

Parameters

Parameter	Description	Value
peer-address	Specifies the address of MSDP peer that sends the SA Request message.	The address is in dotted decimal notation.
acl	Indicates an ACL. If the ACL is not specified, all SA Requests messages of the MSDP peer are ignored. If the ACL is specified, only the SA Request messages of the group that meets the requirements of the ACL are processed.	-
basic-acl-number	Indicates the number of the basic ACL.	The number is an integer that ranges from 2000 to 2999.
acl-name	Specifies the name of a named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a local MSDP peer receives SA Request messages, the MSDP peer responds to all SA Request messages by default. To configure the router to respond only to certain SA Request messages, configure the **peer sa-request-policy** command.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The **peer sa-request-policy** and **acl** commands are used together.

- In the basic ACL view, you can set the multicast group address range of SA messages that are forwarded by the MSDP peer by specifying the **source** parameter in the **rule** command.
- In the advanced ACL view of a named ACL, when the **rule** command is used to configure a filtering rule, the filtering rule is effective only with the multicast group address range specified by the **destination** parameter and with the time period specified by the **time-range** parameter.

Example

Configure the ACL for filtering SA request messages sent by the MSDP peer 10.58.6.5: only SA request messages bound for the group whose address is 225.1.1.0/24 are received in the public network instance.

```
<Huawei> system-view
[Huawei] acl number 2001
[Huawei-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.58.6.5 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.58.6.5 sa-request-policy acl 2001
```

Configure a named ACL for filtering SA request messages sent by the MSDP peer 10.58.6.5: only SA Request messages bound for the group whose address is 225.1.1.0/24 are received in the public network instance.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip destination 225.1.1.0 0.0.0.255
[Huawei-acl-adv-myacl] quit
[Huawei] msdp
[Huawei-msdp] peer 10.58.6.5 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] peer 10.58.6.5 sa-request-policy acl myacl
```

Related Topics

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.24 reset msdp control-message counters

Function

The **reset msdp control-message counters** command clears statistics about MSDP messages.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**peer** *peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all instances, including the public network instance and all VPN instances. If **vpn-instance** or **all-instance** is not specified, only information about the public network instance is cleared.	-
peer *peer-address*	Specifies IP address of MSDP peer. If **peer** *peer-address* is specified, only statistics about the MSDP messages exchanged with a specified MSDP peer are cleared.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command clears statistics about the received, sent, and discarded MSDP messages.

Example

Clear statistics about the MSDP messages received, sent, and discarded on the peer 10.3.3.3 in the public network instance.

```
<Huawei> reset msdp control-message counters peer 10.3.3.3
```

Related Topics

10.5.4 display msdp control-message counters

10.5.6 display msdp peer-status

10.5.25 reset msdp peer

Function

The **reset msdp peer** command resets the TCP connection with a specified MSDP peer, and clears statistics about the specified MSDP peer.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, the TCP connections set up between MSDP peers in the public network instance are reset and statistics about MSDP peers in the public network instance are cleared.	-
peer-address	Specifies the address of an MSDP peer. If the *peer-address* is not specified, all peers are reset.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-configure the TCP connection between MSDP peers or clear statistics about the specified MSDP peer, run the **reset msdp peer** command.

 Copyright © Huawei Technologies Co., Ltd.

Use the **reset msdp statistics** command to clear the statistics about an MSDP peer without resetting the MSDP peer.

Configuration Impact

NOTICE

After this command is run, the TCP connection with the specified MSDP peer is torn down and a new TCP is set up again. During this process, MSDP services are interrupted, which may affect multicast services, for example, multicast data transmission fails. Therefore, use this command with caution.

Example

Reset the TCP connection with MSDP peer 10.10.7.6 and clear the statistics about MSDP peer 10.10.7.6 in the public network instance.

```
<Huawei> reset msdp peer 10.10.7.6
```

Related Topics

10.5.6 display msdp peer-status

10.5.27 reset msdp statistics

10.5.26 reset msdp sa-cache

Function

The **reset msdp sa-cache** command clears (S, G) entries in the SA cache.

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only the entries in the SA cache of the public network instance are cleared.	-
group-address	Specifies the group address carried in (S, G) information. If this parameter is not specified, all (S, G) information in the SA cache is cleared.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear (S, G) information from an SA cache, run the **reset msdp sa-cache** command.

Configuration Impact

NOTICE

(S, G) information in the SA cache cannot be restored after you clear it. Therefore, confirm the action before you use this command.

Example

Clear the (S, G) entries with the group address of 225.5.4.3 in the SA cache in the public network instance.

```
<Huawei> reset msdp sa-cache 225.5.4.3
```

Related Topics

10.5.1 cache-sa-enable
10.5.8 display msdp sa-cache

10.5.27 reset msdp statistics

Function

The **reset msdp statistics** command clears statistics about one or more MSDP peers without resetting the MSDP peer (s).

Format

reset msdp [**vpn-instance** *vpn-instance-name* | **all-instance**] **statistics** [*peer-address*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances. If **vpn-instance** or **all-instance** is not specified, only information about the public network instance is cleared.	-
peer-address	Specifies the address of an MSDP peer. If the *peer-address* is not specified, the statistics about all MSDP peers are cleared.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **reset msdp statistics** command is used, the statistics about the MSDP peer are cleared automatically. However, the TCP connections among peers are not closed, and MSDP services are not affected.

To clear the statistics about an MSDP peer and to rebuild the TCP connections among MSDP peers at the same time, use the **reset msdp peer** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear the statistics of MSDP peer 10.10.7.6 in the public network instance.

```
<Huawei> reset msdp statistics 10.10.7.6
```

Related Topics

10.5.3 display msdp brief
10.5.25 reset msdp peer

10.5.28 shutdown (MSDP)

Function

The **shutdown** command terminates a specified MSDP peer.

The **undo shutdown** command restores the default configuration.

By default, the MSDP peers are not closed after the peer relationship is established.

Format

shutdown *peer-address*

undo shutdown *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of an MSDP peer.	The address is in dotted decimal notation.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **shutdown** command can be used to close the TCP connection between two MSDP peers while keeping the MSDP peer relationship.

Prerequisites

MSDP peers have been configured using the **peer connect-interface (MSDP)** command.

Configuration Impact

After the **shutdown** command is run on MSDP peers, the MSDP peers do not transmit SA messages or attempt to establish a connection. When the **display msdp brief** command or the **display msdp peer-status** command is used to check the status of MSDP peers, **State** in the command output is displayed as **Shutdown**.

Precautions

You only need to run the **undo shutdown** command to restore the configuration. You do not need to run the **peer connect-interface (MSDP)** command to reconfigure the MSDP peer.

Example

Close MSDP peer 10.10.7.6 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 10.10.7.6 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] shutdown 10.10.7.6
```

Related Topics

10.5.3 display msdp brief

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.29 static-rpf-peer

Function

The **static-rpf-peer** command configures an MSDP peer as a static RPF peer. The SA messages sent by the static RPF peer are free from the RPF check.

The **undo static-rpf-peer** command restores the default configuration.

By default, no MSDP peer is configured as a static RPF peer.

Format

static-rpf-peer *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

Parameters

Parameter	Description	Value
peer-address	Specifies the address of a static RPF peer.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rp-policy *ip-prefix-name*	Specifies the filtering policy based on RP addresses. The filtering policy is used to filter SA messages based on RP addresses. **ip ip-prefix** specifies the name of the filtering policy.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent SA messages from being circularly forwarded between MSDP peers, MSDP performs the RPF check on the received SA message. MSDP strictly controls the incoming SA messages. The SA message that does not comply with the RPF rules are discarded.

To protect the SA messages transmitted between MSDP peers from being discarded because of RPF rules and reduce redundant traffic, you can specify MSDP peers as static RPF peers. The SA messages received from a static RPF peer do not need to be checked according to RPF rules.

Prerequisites

The MSDP peer relationship has been established between the router and a specified RPF peer using the **peer connect-interface (MSDP)** command.

Configuration Impact

You can specify multiple remote static RPF peers for the router using the **static-rpf-peer** *peer-address* command repeatedly.

Precautions

When you specify multiple static RPF peers for the router, pay attention to the following points:

- All the peers are configured with **rp-policy**

  When SA messages sent by a static RPF peer in the active state reaches the local router, the local router filters the SA messages according to specified **rp-policy** on the peers, and receives only the SA messages passing the filtering.
- None of the peers is configured with **rp-policy**

  The local router receives all the SA messages from the static RPF peers in the active state.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure 192.168.3.2 as a static RPF peer, with the source RP address range of 192.168.0.0/16 in the public network instance.

```
<Huawei> system-view
[Huawei] ip ip-prefix list-df permit 192.168.0.0 16 greater-equal 16 less-equal 32
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] peer 192.168.3.2 connect-interface gigabitethernet 1/0/0
[Huawei-msdp] static-rpf-peer 192.168.3.2 rp-policy list-df
```

Related Topics

10.5.6 display msdp peer-status

9.9.47 ip ip-prefix

10.5.12 msdp

10.7.28 multicast routing-enable

10.5.14 peer connect-interface (MSDP)

10.5.30 timer retry

Function

The **timer retry** command sets the interval for retrying to set up an MSDP peer relationship.

The **undo timer retry** command restores the default value.

By default, the interval for retrying to set up an MSDP peer relationship is 30 seconds.

Format

timer retry *interval*

undo timer retry

Parameters

Parameter	Description	Value
interval	Specifies the interval for retrying to set up an MSDP peer relationship.	The value is an integer that ranges from 1 to 60, in seconds.

Views

MSDP view of the public network instance or MSDP view of the VPN instance

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The TCP connection needs to be set up between the MSDP peers. MSDP requires the peer with the larger IP address to listen at the port 639, and the peer with the smaller IP address to start a connection. If the connection fails, the peer restarts the connection after a period of time. Such a period of time is called "interval retrying to set up an MSDP peer relationship".

You need to establish a TCP connection between MSDP peers when an MSDP peer is created, the closed MSDP peer connection is restarted, or the faulty MSDP peer tries to restore the work. You can run the **timer retry** command to adjust the interval for retrying to set up an MSDP peer relationship.

Prerequisites

MSDP has been enabled using the **msdp** command.

Example

Set the interval for retrying to set up an MSDP peer relationship to 60 seconds in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] msdp
[Huawei-msdp] timer retry 60
```

Related Topics

10.5.6 display msdp peer-status

10.5.12 msdp

10.7.28 multicast routing-enable

10.6 Multicast VPN (IPv4) Configuration Commands in Rosen Mode

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact technical support personnel.

10.6.1 auto-discovery

Function

The **auto-discovery** command configures the auto-discovery (A-D) mode for the multicast VPN, ensuring the transmission of multicast VPN services on the public network tunnel which is based on the Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) multicast distribution tree (MDT), and associates an inbound multicast route-policy with the IPv4 address family of the current VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

The **undo auto-discovery** command deletes the configurations of the A-D mode for the multicast VPN and removes the association between the inbound multicast route-policy and the IPv4 address family of the current VPN instance.

By default, the A-D mode for the multicast VPN is not configured and the IPv4 address family of the current VPN instance is not associated with an inbound multicast route-policy.

Format

auto-discovery { **mdt** | **mvpn** } [**import route-policy** *route-policy-name*]

undo auto-discovery

Parameters

Parameter	Description	Value
mdt	Specifies that the multicast VPN adopts the MDT-Subsequent Address Family Identifier (SAFI) A-D mode.	-
mvpn	Specifies that the multicast VPN adopts the MCAST-VPN SAFI A-D mode.	-
route-policy *route-policy-name*	Specifies the inbound multicast route-policy to associate with the IPv4 address family of the VPN instance.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Currently, the mechanism of implementing the multicast VPN is that all Provider Edges (PEs) on the network know information about the Rendezvous Point (RP); in this manner, the PIM-SM MDT is established on the public network to transmit multicast VPN services. This mechanism, however, does not support the Share-Group address within the SSM address range. This is because PEs in the same VPN do not know the peer information of each other, therefore knowing nothing about the multicast source information. As a result, these PEs cannot directly send Join messages to the multicast source and establish the PIM-SSM MDT.

 Copyright © Huawei Technologies Co., Ltd.

To solve this problem, in an autonomous system (AS), you can configure the BGP A-D mode to enable the automatic discovery of the PE information about PEs in the same VPN. In this manner, multicast VPN services can be transmitted on the public network tunnel which is based on the PIM-SSM MDT.

At present, the multicast VPN supports two A-D modes:

- MDT-SAFI A-D mode: defines a new address family in the MDT-SAFI message advertised through BGP. After the multicast VPN is configured on a PE, the multicast VPN configurations, including the Route Distinguisher (RD) and the Share-Group address, can be advertised to all BGP peers. After a remote PE (a BGP peer) receives the MDT-SAFI message advertised through BGP, the remote PE compares the RD carried in the message with its RD. If the RDs are the same, it indicates the remote PE is in the same VPN with the local PE. The remote PE then uses the MDT-SAFI message to establish the PIM-SSM MDT for transmitting multicast VPN services.
- MCAST-VPN SAFI A-D mode: defines a new address family in the MCAST-VPN-SAFI message advertised through BGP. Similar to the MDT-SAFI A-D mode, the MCAST-VPN SAFI A-D mode uses the MCAST-VPN-SAFI message advertised between BGP peers to transmit multicast VPN configurations, including the RD and Share-Group address. The difference is that the MCAST-VPN SAFI A-D mode has a broader definition, supports additional extensions, and carries more multicast VPN attributes and information for establishing the public network tunnel. Therefore, the MCAST-VPN SAFI A-D mode is applied to the next-generation multicast VPN.

Prerequisites

The **multicast routing-enable** command has been run in the public network instance view or the VPN instance view.

Precautions

When configuring the A-D mode for the multicast VPN, you need to configure an A-D address family in the BGP view so that the corresponding BGP A-D mode can be used to implement the multicast VPN function. If the configured A-D mode is inconsistent with the A-D address family enabled in the BGP view, you cannot implement the A-D mode.

NOTE

This command is applied to the single-AS scenario, with no RP configured on the public network.

In the same VPN enabled with the IPv4 address family, only one A-D mode can be adopted. Different VPNs enabled with the IPv4 address family on the same PE can adopt different A-D modes. In this case, you need to enable two kinds of A-D address families in the BGP view, and then the specific A-D mode is adopted by each VPN to forward multicast data.

The PEs enabled with the BGP A-D function must support the same PIM protocol and use the Share-Group address within the SSM address range.

Running this command does not affect the original multicast VPN service flow. When the Share-Group address is in the Any-Source Multicast (ASM) address range, or the PIM-DM protocol is adopted on the public network, multicast VPN traffic can still be transmitted along the multicast tunnel in PIM-SM mode or in PIM-DM mode on the public network.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the MDT-SAFI A-D mode for vpn1 enabled with the IPv4 address family, implementing the transmission of multicast VPN services along the public network tunnel (PIM-SSM MDT) in vpn1.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family mdt
[Huawei-bgp-af-mdt] peer 3.3.3.3 enable
[Huawei-bgp-af-mdt] quit
[Huawei-bgp] quit
[Huawei] ip vpn-instatnce vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn1-af-ipv4] vpn-target 100:1 both
[Huawei-vpn-instance-vpn1-af-ipv4] multicast routing-enable
[Huawei-vpn-instance-vpn1-af-ipv4] multicast-domain share-group 232.2.2.0 binding mtunnel 0
[Huawei-vpn-instance-vpn1-af-ipv4] auto-discovery mdt
```

Related Topics

10.6.5 display multicast-domain vpn-instance share-group

9.8.87 ipv4-family

10.6.2 display default-parameter mvpn

Function

The **display default-parameter mvpn** command displays default configurations about the multicast VPN (MVPN).

Format

display default-parameter mvpn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using this command displays only default configurations, regardless of whether the configurations about MVPN parameters are changed.

Example

Display default configurations about the MVPN.

```
<Huawei> display default-parameter mvpn
  MVPN Instance View Default Configurations:
  ------------------------------------------
  Multicast-domain switch-delay: 5 s
  Multicast-domain switch threshold: 0 kbps-preferred
  Multicast-domain holddown-time: 60 s
  Multicast-domain log switch-group-reuse: disabled
  Multicast-domain share-group: disabled
  Multicast-domain switch-group-pool: disabled
  Multicast-domain auto-discovery: disabled
  Multicast-domain switch-without-register: disabled
  Multicast extranet select-rpf rule: disabled
```

Table 10-81 Description of the **display default-parameter mvpn** command output

Item	Description
MVPN Instance View Default Configurations	Indicates the default configurations in the MVPN instance view.
Multicast-domain switch-delay	Indicates the delay in switching from the share-multicast distribution tree (MDT) to the switch-MDT.
Multicast-domain switch threshold	Indicates the threshold of the multicast packet rate that can trigger the switch to the switch-MDT.
Multicast-domain holddown-time	Indicates the delay in switching from the switch-MDT to the share-MDT.
Multicast-domain log switch-group-reuse	Indicates whether recording logs about switch-group address reuse is configured.
Multicast-domain share-group	Indicates whether the share-group address is configured and whether the Multicast Tunnel Interface (MTI) is bound to a VPN instance.
Multicast-domain switch-group-pool	Indicates whether the range of the switch-MDT switch-group-pool and the switch condition are configured.
Multicast-domain auto-discovery	Indicates whether the auto-discovery (A-D) mode is configured for the VPN.
Multicast-domain switch-without-register	Indicates whether the source Provider Edge (PE) sends the null Register message to the Rendezvous Point (RP) to establish the shortest path tree (SPT) on the public network before the Switch-Group address is used to encapsulate VPN data.
Multicast extranet select-rpf rule	Indicates whether the multicast routing policy configured for a VPN is configured.

 Copyright © Huawei Technologies Co., Ltd.

10.6.3 display multicast-domain control-message counters

Function

The **display multicast-domain control-message counters** command displays statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances.

Format

display multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **control-message counters**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about sent and received MDT switch messages in a specified VPN instance. *vpn-instance-name* specifies the VPN instance name.	-
all-instance	Displays statistics about sent and received MDT switch messages in all VPN instances.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast-domain control-message counters** command to view statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances and check whether packets are normally sent and received on the current device.

You can set the **vpn-instance** *vpn-instance-name* parameter so as to view statistics about sent and received MDT switch messages in a specified VPN instance.

Example

Displays statistics about sent and received MDT switch messages in VPN instance **red**.

```
<Huawei> display multicast-domain vpn-instance red control-message counters
VPN-Inastance red:
 Message Type     Received         Sent            Invalid
 Switch           5000             0               5000
```

Table 10-82 Description of the display multicast-domain vpn-instance red control-message counters command output

Item	Description
VPN-Instance red	VPN instance in which statistics about sent and received MDT switch messages need to be displayed
Message Type	Message type. The value can only be: Switch: MDT switch message
Received	Number of received messages
Sent	Number of sent messages
Invalid	Number of received invalid messages

10.6.4 display multicast-domain invalid-packet

Function

The **display multicast-domain invalid-packet** command displays statistics about invalid MDT switch messages received by a device and details of these messages.

Format

display multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **invalid-packet**

display multicast-domain invalid-packet [*packet-number*] **verbose**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Displays statistics about invalid MDT switch messages received in a specified VPN instance. *vpn-instance-name* specifies the VPN instance name.	The value is a string of case-sensitive characters.
all-instance	Displays statistics about invalid MDT switch messages received in all VPN instances.	-
packet-number	Displays details of a specified number of invalid MDT switch messages recently received.	The value is an integer ranging from 1 to 100. By default, details of all the invalid MDT switch messages currently stored are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Displays details of invalid MDT switch messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast-domain invalid-packet** command to view statistics and details of invalid MDT switch messages for fault location and rectification.

If a shortest path tree (SPT) fails to be set up in a VPN instance on a multicast network, you can run the **display multicast-domain invalid-packet** command first to check whether devices have received invalid MDT switch messages. If the command output contains statistics about invalid MDT switch messages, you need to run the **display multicast-domain invalid-packet** [*packet-number*] **verbose** command to view details of invalid MDT switch messages to locate the fault.

You can run the following related commands to view information about specific invalid MDT switch messages:

- Run the **display multicast-domain vpn-instance** *vpn-instance-name* **invalid-packet** command to view statistics about invalid MDT switch messages received in a specified VPN instance.
- Run the **display multicast-domain invalid-packet** *packet-number* **verbose** command to view details of invalid MDT switch messages recently received. Currently, details of a maximum of 10 invalid MDT switch messages can be displayed.

Example

Displays statistics about invalid MDT switch messages received in vpn1.

```
<Huawei> display multicast-domain vpn-instance vpn1 invalid-packet

            Statistics of invalid packets for vpn1:
-------------------------------------------------------------------
MDT Switch invalid packet:
Fault Length            : 0          Invalid Message Type    : 0
Invalid Multicast Source: 0          Invalid Multicast Group : 0
Invalid Switch Group    : 0
-------------------------------------------------------------------
```

Table 10-83 Description of the display multicast-domain vpn-instance vpn1 invalid-packet command output

Item	Description
Statistics of invalid packets for vpn1	VPN instance in which statistics about MDT switch messages need to be displayed
MDT Switch invalid packet	Invalid MDT switch messages
Fault Length	Messages with invalid lengths
Invalid Message Type	Messages with invalid message types
Invalid Multicast Source	Messages with invalid multicast source addresses
Invalid Multicast Group	Messages with invalid multicast group addresses
Invalid Switch Group	Messages with invalid switch group addresses

Display details of one invalid MDT switch message recently received in the public network instance.

```
<Huawei> display multicast-domain invalid-packet 1 verbose
      Detailed information of invalid packets
-----------------------------------------------------
Packet information (Index 1):
-----------------------------------------------------
Interface           :  10.10.10.10
Time                :  2010-6-1 10:50:08 UTC-08:00
Message Length      :  16
Invalid Type        :  Invalid Switch Group
0000: 01 00 10 00 64 64 64 64 e8 00 00 00 0a 00 00 00
-----------------------------------------------------
```

Table 10-84 Description of the display multicast-domain invalid-packet 1 verbose command output

Item	Description
Detailed information of invalid packets	Details of the invalid MDT switch message
Packet information (Index 1)	Sequence number of the invalid MDT switch message (numbered in the opposite order that the message is received, for example, the index of the last received message is 1, the index of the last but one message is 2, and so on)
Interface	Interface receiving the invalid MDT switch message

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Time	Time when the invalid MDT switch message is received, in any of the following formats: ● YYYY-MM-DD HH:MM:SS ● YYYY-MM-DD HH:MM:SS UTC±HH:MM DST ● YYYY-MM-DD HH:MM:SS UTC±HH:MM ● YYYY-MM-DD HH:MM:SS DST UTC±HH:MM indicates that a time zone is configured through the **clock timezone** command; DST indicates that the daylight saving time is configured through **clock daylight-saving-time** command.
Message Length	Length of the invalid MDT switch message
Invalid Type	Type of the invalid MDT switch message
0000: 01 00 10 00 64 64 64 64 e8 00 00 00 0a 00 00 00	Contents of the invalid MDT switch message

Related Topics

10.7.23 multicast invalid-packet

10.6.5 display multicast-domain vpn-instance share-group

Function

The **display multicast-domain vpn-instance share-group** command, displays information about the share-group address configured for a specified VPN instance in a multicast domain (MD).

Format

display multicast-domain vpn-instance *vpn-instance-name* **share-group** [**local** | **remote**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The name is a case-sensitive character string.
local	Indicates the locally configured share-group address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remote	Indicates the share-group address learned through BGP Update packets.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an autonomous system (AS), BGP Auto-Discovery (BGP A-D) ensures the automatic discovery of peers in a multicast VPN. In this manner, a Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) multicast distribution tree (MDT) can be directly established on the public network to transmit multicast VPN services. The **display multicast-domain vpn-instance share-group** command displays information about the Share-Group of the remote peer, peer IP address, and tunnel type, which facilitates you to determine whether the multicast tunnel is correctly established to forward multicast services.

When **display multicast-domain vpn-instance share-group** command is used, the following situations occur:

- If **local** is specified, only the information of the share-group configured locally is displayed.
- If **remote** is specified, the share-group information learned through the BGP Update packets is displayed.
- If both **local** and **remote** are not specified, information of all share-groups is displayed.

The share-group information learned through BGP Update packets is displayed in an ascending order of share-groups. If the share-groups are the same, the information is displayed in an ascending order of peer addresses.

Example

Display the share-group information of a specified VPN instance in an MD.

```
<Huawei> display multicast-domain vpn-instance BLUE share-group
MD local share-group information for VPN-Instance: BLUE
  Share-group: 232.2.2.0
  MTunnel address: 3.3.3.3
MD remote share-group information for VPN-Instance: BLUE
  Share-group     Peer-address    Tunnel-type
  232.2.2.0       1.1.1.1         PIM SSM
```

Table 10-85 Description of the **display multicast-domain vpn-instance share-group** command output

Item	Description
MD local share-group information for VPN-Instance	VPN instance to which local share-group information in the multicast domain belongs
Share-group	Configured share-group address on the local device
MTunnel address	Configured IP address of the MTI bound to the share-group on the local device
MD remote share-group information for VPN-Instance	VPN instance to which remote share-group information in the multicast domain belongs
Share-group	Share-group address of the remote provider edge (PE)
Peer-address	IP address of the remote PE
Tunnel-type	Tunnel type, including: ● PIM SM: indicates that the Share-Group address of the remote PE is in the any-source multicast (ASM) address range. ● PIM SSM: indicates that the Share-Group address of the remote PE is in the source-specific multicast (SSM) address range. **NOTE** The Tunnel-type field is displayed only if the remote PE is configured with the MCAST-SAFI A-D mode.

Related Topics

10.6.12 multicast-domain share-group

10.6.6 display multicast-domain vpn-instance switch-group receive

Function

The **display multicast-domain vpn-instance switch-group receive** command displays the Switch-Group information received by a specified VPN instance.

Format

display multicast-domain vpn-instance *vpn-instance-name* **switch-group receive brief**

display multicast-domain vpn-instance *vpn-instance-name* **switch-group receive** [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [**mask** { *source-mask-length* | *source-mask* }] | *vpn-group-address* [**mask** { *group-mask-length* | *group-mask* }]] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The name is a string of 1 to 31 characters.
active	Displays the received Switch-Group that joins the Switch-multicast distribution tree (MDT).	-
brief	Displays brief information about the received Switch-Group.	-
group *group-address*	Displays the Switch-Group related to a multicast group specified by *group-address* of the public network. *group-address* specifies the address of the multicast group.	The address is in dotted decimal notation and ranges from 224.0.0.0 to 239.255.255.255.
sender *source-address*	Displays the Switch-Group information related to the specified multicast source *source-address* of the public network. The *source-address* indicates the multicast.	The address is in dotted decimal notation.
vpn-source-address	Displays the Switch-Group information related to a VPN multicast source specified by *vpn-source-address*.	The address is in dotted decimal notation.
mask	Indicates the mask of the VPN multicast group or source address.	-
source-mask-length	Specifies the mask length of the VPN multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of VPN multicast source address.	The mask is in dotted decimal notation.
vpn-group-address	Displays the Switch-Group information related to a VPN multicast group specified by *vpn-group-address*.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
group-mask-length	Specifies the mask length of the VPN multicast group address.	The value is an integer that ranges from 4 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group-mask	Specifies the mask of VPN multicast group address.	The mask is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Use the **display multicast-domain vpn-instance switch-group receive** command is run to display the Switch-Group information received by the local router:

- Each VPN instance corresponds to a multicast domain (MD). *vpn-instance-name* specifies a VPN instance. Use the command to display the information about the Switch-Group of a specified MD.
- If **brief** is specified, the brief information of all Switch-Groups is displayed in an ascending order of the Switch-Group address.
- If **active** is specified, only the information of the Switch-Group that joins the Switch-Group is displayed in an ascending order of the VPN (S, G).
- If **group** is specified, only the Switch-Group information related to the multicast group of the public network is displayed.
- If the **sender** is specified, only the Switch-Group information related to the multicast source of the public network is displayed.
- If *vpn-source-address* is specified, only information about the Switch-Group related to a specified VPN multicast source is displayed.
- If *vpn-group-address* is specified, only information about the Switch-Group related to a specified VPN multicast group is displayed.

Example

Display Switch-Group information received by a specified VPN instance in an MD.

```
<Huawei> display multicast-domain vpn-instance VPN1 switch-group receive
MD switch-group information received by VPN-Instance: VPN1
Switch group:  226.1.1.0 ref count: 8, active count: 8
  Sender:  172.100.1.1 active count: 8
    (192.6.1.5, 239.1.1.1)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.1.158)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.2.12)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.2.197)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.5, 239.1.3.62)
    Up time: 01:20:20  expire time: 00:03:10  active
    (192.6.1.2, 225.1.1.109)
    Up time: 01:20:20  expire time: 00:03:10  active
```

```
  (192.6.1.2, 225.1.4.80)
  Up time: 01:20:20  expire time: 00:03:10  active
  (192.6.1.2, 225.1.4.173)
  Up time: 01:20:20  expire time: 00:03:10  active
<Huawei> display multicast-domain vpn-instance VPN1 switch-group receive brief
MD switch-group information received by VPN-Instance: VPN1
switch group:  226.1.1.0 ref count: 8, active count: 0
switch group:  226.1.1.1 ref count: 4, active count: 0
switch group:  226.1.1.2 ref count: 8, active count: 0
switch group:  226.1.1.3 ref count: 4, active count: 0
switch group:  226.1.1.4 ref count: 8, active count: 0
```

Table 10-86 Description of the **display multicast-domain vpn-instance switch-group receive** command output

Item	Description
MD switch-group information received by VPN-Instance	VPN instance to which MD Switch-group information belongs.
switch group	Address of the received Switch-group
ref count	Number of VPN multicast groups referenced by the Switch-group
active count	Number of active VPN multicast groups (where receivers exist) referenced by the Switch-group
sender	BGP peer IP address of the PE that sends Switch-group information
expire time	Timeout period of switching messages in which the VPN multicast (S, G) entry are referenced by the Switch-group

Related Topics

10.6.7 display multicast-domain vpn-instance switch-group send

10.6.7 display multicast-domain vpn-instance switch-group send

Function

The **display multicast-domain vpn-instance switch-group send** command displays the Switch-Group information sent by the specified VPN instance in a multicast domain (MD).

Format

display multicast-domain vpn-instance *vpn-instance-name* **switch-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [**mask** { *source-mask-length* | *source-mask* }] | *vpn-group-address* [**mask** { *group-mask-length* | *group-mask* }]] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The name is a string of 1 to 31 characters.
group *group-address*	Displays the Switch-Group information related to a multicast group G. The *group-address* indicates multicast group address.	The address is in dotted decimal notation format. The address ranges from 224.0.0.0 to 239.255.255.255.
reuse *interval*	Displays Switch-Group information that is reused by an MD in the specified period. The *interval* indicates the specified period.	The value of the interval is an integer that ranges from 1 to 2147483647 seconds.
vpn-source-address	Displays the Switch-Group information related to the specified VPN multicast source.	The address is in dotted decimal notation format.
mask	Indicates the mask of VPN multicast group or source address.	-
source-mask-length	Specifies the mask length of a VPN multicast source address.	The value is an integer that ranges from 0 to 32.
source-mask	Specifies the mask of a VPN multicast source address.	The address is in dotted decimal notation.
vpn-group-address	Displays the Switch-Group information related to the specified VPN multicast group G.	The address is in dotted decimal notation and ranges from 224.0.0.0 to 239.255.255.255.
group-mask-length	Specifies the mask length of a VPN multicast group address.	The value is an integer that ranges from 4 to 32.
group-mask	Specifies the mask of a VPN multicast group address.	The address mask is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Use the **display multicast-domain vpn-instance switch-group send** command to display the Switch-Group information sent by the local Huawei:

- Each VPN instance corresponds to an MD. *vpn-instance-name* specifies the VPN instance. The command is only used to display the Switch-Group information related to the specified MD.
- The Switch-Group information is displayed in an ascending order of VPN (S, G) entry.
- If **reuse** *interval* is specified, the group information that is reused in a specified interval is displayed in an ascending order of Switch-Group address.

Example

Display the Switch-Group information sent by a specified VPN instance in an MD.

```
<Huawei> display multicast-domain vpn-instance VPN1 switch-group send
MD switch-group information sent by VPN-Instance: VPN1
  226.1.1.0 reference_count: 3
    (192.168.1.5, 239.1.1.1)              switch time: 00:00:21
    (192.168.1.5, 239.1.1.158)             switch time: 00:00:21
    (192.168.1.5, 239.1.2.50)             switch time: 00:00:05
  226.1.1.1 reference_count: 3
    (192.168.1.2, 225.1.1.1)              switch time: 00:00:21
    (192.168.1.2, 225.1.2.50)             switch time: 00:00:05
    (192.168.1.5, 239.1.1.159)             switch time: 00:00:21
<Huawei> display multicast-domain vpn-instance VPN1 switch-group send reuse 30
MD switch-group information sent by VPN-Instance: VPN1
  226.1.1.0 reuse_count: 1
  226.1.1.1 reuse_count: 1
  226.1.1.2 reuse_count: 1
```

Table 10-87 Description of the **display multicast-domain vpn-instance switch-group send** command output

Item	Description
MD switch-group information sent by VPN-Instance	VPN instance to which MD Switch-group information belongs.
226.1.1.0 reference_count: 3	Number of VPN multicast groups referenced by the Switch-group sent
switch time	Switching time of the VPN multicast (S, G) entry referenced by the Switch-group
226.1.1.0 reuse_count: 1	Number of times of reusing the Switch-group sent in the specified period

Related Topics

10.6.6 display multicast-domain vpn-instance switch-group receive

10.6.8 mtu (MTI view)

Function

The **mtu** command sets the MTU for an MTI.

The **undo mtu** command restores the default MTU of an MTI.

By default, the MTU of an MTI is 1472 bytes.

Format

mtu *mti-mtu*

undo mtu

Parameters

Parameter	Description	Value
mti-mtu	Specifies the MTU value of an MTI.	The value is an integer that ranges from 128 to 1500, in bytes.

Views

MTI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the length of a VPN multicast packet is equal or close to the MTU of the outbound interface of the public network instance, the length of the GRE-encapsulated public network multicast data packet is larger than the MTU of the outbound interface of the public network instance. In this case, the local PE must fragment the encapsulated packet and sends it through the outbound interface of the public network instance. Upon receiving the packet, the remote PE reassembles the packet.

To enable an MTI to fragment a VPN multicast packet before performing GRE encapsulation, run the **mtu** command to set a smaller MTU for the MTI. This method reduces unnecessary fragmentation on the public network and packet reassembly, improving packet transmission efficiency.

Configuration Impact

If the MTU is set too small and the size of packets is large, packets are broken into a great number of fragments, and may be discarded by QoS queues.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the MTU of MTunnel 10 to 1400.

```
<Huawei> system-view
[Huawei] interface mtunnel 10
[Huawei-MTunnel10] mtu 1400
```

10.6.9 multicast extranet select-rpf

Function

The **multicast extranet select-rpf** command configures a multicast routing policy, setting the upstream of the Reverse Path Forwarding (RPF) route selected by the PIM entry corresponding to a multicast group address to another VPN instance or the public network instance.

The **undo multicast extranet select-rpf** command deletes the multicast routing policy configured for a VPN.

By default, no multicast routing policy is configured for a VPN.

Format

multicast extranet select-rpf { **vpn-instance** *vpn-instance-name* | **public** } **group** *group-address* { *group-mask* | *group-mask-length* }

undo multicast extranet select-rpf { **all** | { **vpn-instance** *vpn-instance-name* | **public** } **group** *group-address* { *group-mask* | *group-mask-length* } }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a source VPN instance. *vpn-instance-name* specifies the name of the source VPN instance.	The value is a string of 1 to 31 case-sensitive characters.
public	Indicates that the source VPN instance is a public network instance.	-
group *group-address*	Specifies the range of the addresses of multicast groups running the multicast VPN extranet service.	The value ranges from 224.0.0.0 to 239.255.255.255, in dotted decimal notation.
group-mask	Indicates the mask of a group address.	The value ranges from 240.0.0.0 to 255.255.255.255, in dotted decimal notation.
group-mask-length	Indicates the length of the mask of a group address.	The value is an integer ranging from 4 to 32.
all	Indicates all multicast routing policies.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In regular multicast VPN applications, multicast traffic can be transmitted only among different VPN sites in the same VPN, and VPN sites that belong to different VPNs cannot access each other.

In actual situations, enterprises in different VPNs need to communicate with each other, or service providers need to provide multicast services for users who reside in other VPNs. Multicast services need to be transmitted between different VPNs so that the multicast data from a VPN user needs to be provided for other VPN users.

Multicast VPN extranet is therefore introduced. Through this feature, receivers in a VPN can receive multicast data sent by the multicast sources in other VPNs or in the public network.

In multicast VPN extranet, the multicast source and the multicast receiver can belong to different VPN instances or the multicast source belongs to the public network instance whereas the multicast receiver belongs to a VPN instance. The public network and the VPN can be only PIM-SM/Source-Specific Multicast (SSM) networks.

Prerequisites

The **multicast routing-enable** command has been run in the public network instance view or the VPN instance view.

Precautions

The **multicast extranet select-rpf** command applies to MVPN extranet in remote cross scenarios. When using this command, note the following precautions:

- The VPN instance specified in the **vpn-instance** parameter cannot be the VPN instance in which view the command is run.
- If a public network instance is specified on the upstream device, a public network instance must be specified using the **public** parameter on the local device.
- If a VPN instance is specified on the upstream device, a VPN instance must be specified using the **vpn-instance** parameter on the local device. By default, an MVPN selects its tunnel interface as the upstream interface. Therefore, the remote-cross source VPN instance specified for VPN groups in a specified group address range must the same as the source VPN instance of the route to the multicast source.
- The rendezvous point (RP) set for source VPN and receiver VPN must be a static RP and the static RP must reside at the source VPN side to serve the multicast groups adopting the multicast VPN extranet service. RPs that server

 Copyright © Huawei Technologies Co., Ltd.

other multicast groups in this VPN can be either dynamic or static. The anycast RP function will not be affected.

- The address range of the multicast groups adopting the multicast VPN extranet service cannot overlap the multicast group address range used by the local VPN; the address range of the multicast groups adopting the multicast VPN extranet service set in the newly configured multicast routing policy cannot overlap the address range that has been configured for the multicast groups adopting the multicast VPN extranet service.
- The SSM group address range must be set consistently for both the source VPN and the receiver VPN for providing the multicast VPN extranet service.

Example

Configure a multicast routing policy for VPN RED, specifying VPN BLUE as the upstream of the RPF route selected by group 225.1.1.0/24.

```
<Huawei> system-view
[Huawei] ip vpn-instance RED
[Huawei-vpn-instance-RED] ipv4-family
[Huawei-vpn-instance-RED-af-ipv4] multicast routing-enable
[Huawei-vpn-instance-RED-af-ipv4] multicast extranet select-rpf vpn-instance BLUE group 225.1.1.0 24
```

Related Topics

10.3.29 display pim routing-table
10.7.11 display multicast routing-table
10.7.13 display multicast rpf-info

10.6.10 multicast-domain holddown-time

Function

The **multicast-domain holddown-time** command sets the delay for the switching from the switch-multicast distribution tree (MDT) to the share-MDT.

The **undo multicast-domain holddown-time** command restores the default value of the interval.

By default, the delay for the switching from the switch-MDT to the share-MDT is 60 seconds.

Format

multicast-domain holddown-time *interval*

undo multicast-domain holddown-time

Parameters

Parameter	Description	Value
interval	Specifies the delay for the switching from the switch-MDT to the share-MDT.	The value of the delay ranges from 0 to 512, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During the switch-MDT configuration, the forwarding rate of VPN multicast data may fluctuate around the switchover threshold due to network instability. To prevent multicast data traffic from being frequently switched between the switch-MDT and share-MDT, the system does not perform the switchover immediately after it finds that the forwarding rate is smaller than the switching threshold. Instead, the system starts the holddown timer. The system will perform the switchover after the holddown timer expires.

Prerequisites

The **multicast-domain share-group** command has been run in the corresponding VPN.

Precautions

In actual switchover, from the time when flow changes to the time when device senses the change, there is a delay about 1 to 30 seconds. That is, the delay from the time when the forwarding rate of the data changes and the time when system starts Holddown timer is about 1 to 30 seconds. The delay is not added to the value of the holddown-time. The total delay from the time when the forwarding rate of the data changes to the time when the system completes, the switchover is longer than the Holddown period by 1 to 30 seconds.

When *interval* is set to 0, the system finds that the forwarding rate is below the threshold and switches from the switch-MDT to the share-MDT.

Example

Set the delay for the switching from the switch-MDT to the share-MDT to 80 seconds.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain holddown-time 80
```

10.6.11 multicast-domain log switch-group-reuse

Function

The **multicast-domain log switch-group-reuse** command enables the output of log information about reusing Switch-Group.

The **undo multicast-domain log** command restores the default configuration.

By default, the output of log information about reusing Switch-Group is disabled.

Format

multicast-domain log switch-group-reuse

undo multicast-domain log

Parameters

None

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

If Share-Group is not configured in a VPN, you are not recommended to run this command.

Example

Enable the output of log information about reusing Switch-Group in VPN **mytest**.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain log switch-group-reuse
```

10.6.12 multicast-domain share-group

Function

The **multicast-domain share-group binding mtunnel** command specifies the Share-multicast distribution tree (MDT) group and binds the Multicast Tunnel Interface (MTI) to a VPN instance.

The **undo multicast-domain share-group** command restores the default configuration.

By default, the group address of Share-MDT is not specified.

Format

multicast-domain share-group *group-address* **binding mtunnel** *number*

undo multicast-domain share-group

Parameters

Parameter	Description	Value
group-address	Specifies the multicast group address.	The address is in the dotted decimal notation. The address ranges from 224.0.1.0 to 239.255.255.255.
mtunnel *number*	Specifies the MTI number.	The number is an integer that ranges from 0 to 1023.

Views

VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

On the same Provider Edge (PE), different VPN instances are configured with the different group addresses. The value of *group-address* must be different from the Switch-Group address of all the instances on this PE. *number* cannot be the same as that of the MTI.

You cannot perform the same configuration repeatedly in the same VPN instance view. Instead, you can configure the new address and the MTI only after the previous configuration is deleted.

The IP address and Maximum Transmission Unit (MTU) can be configured on the MTI. The MTU is an integer that ranges from 46 to 1500 bytes.

Run the **undo multicast-domain share-group** command to delete all configurations related to the MTI.

Enable multicast routing in the VPN before running the command.

Example

Specify the Share-Group of VPN instance **mytest** as 224.1.1.1 and bind MTI0.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain share-group 224.1.1.1 binding mtunnel 0
```

Related Topics

10.7.28 multicast routing-enable

 Copyright © Huawei Technologies Co., Ltd.

10.6.13 multicast-domain source-interface

Function

The **multicast-domain source-interface** command allows a Multicast Tunnel Interface (MTI) to use an IP address of a default interface.

The **undo multicast-domain source-interface** command restores the default setting.

By default, an MTI does not use an IP address of a default interface.

Format

multicast-domain source-interface *interface-type interface-number*

undo multicast-domain source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. **NOTE** To avoid frequent protocol changes caused by interface flapping, use the loopback interface address as the MTI address.	-

Views

System view or VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

The **multicast-domain source-interface** command can take effect only after multicast routing is enabled.

If the **multicast-domain source-interface** command is run in the system view, the setting takes effect globally. The command run in the VPN IPv4 address family view takes precedence over that run in the system view. If the command is run in the system view, but not in the VPN IPv4 address family view, the setting in the system view takes effect.

A manually configured IP address on an MTI takes precedence over a default interface address specified using the **multicast-domain source-interface** command. If an IP address is manually configured on an MTI, the default interface address specified using this command does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the MTI to use the IP address of the default interface named **loopback 1**.

```
<Huawei> system-view
[Huawei] multicast-domain source-interface loopback 1
```

10.6.14 multicast-domain switch-delay

Function

The **multicast-domain switch-delay** command specifies delay for the switching from Share-multicast distribution tree (MDT) to Switch-MDT.

The **undo multicast-domain switch-delay** command restores the default value of the delay.

By default, the delay for the switching from Share-MDT to Switch-MDT is 5 seconds.

Format

multicast-domain switch-delay *switch-delay*

undo multicast-domain switch-delay

Parameters

Parameter	Description	Value
switch-delay	Specifies the delay for the switching from Share-MDT to Switch-MDT.	The value of the delay is an integer that ranges from 3 to 60, in seconds.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a downstream Provider Edge (PE) joins the Switch-Group, it takes certain time to set up the Switch-MDT in the public network. Therefore, the switching delay needs to be configured. The upstream PE sends a switching message. After the delay expires, the system uses the Switch-Group to encapsulate data. That is, data is switched from Share-MDT to Switch-MDT. Before the switch-delay timer times out, the system continues to detect the data forwarding rate. If the rate is always higher than the switchover threshold, the data packets are switched to the Switch-MDT. Otherwise, the packets are still forwarded by using the Share-MDT.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The **multicast-domain share-group** command has been run in the corresponding VPN.

Configuration Impact

If the **multicast-domain switch-delay** command is run several times in the same VPN instance view, the latest configuration will overwrite the previous ones.

Precautions

In actual switchover, from the time when flow changes to the time when device senses the change, there is a delay about 1 to 30 seconds. That is, the delay from the time when the forwarding rate of the data changes and the time when system starts the switch-delay timer is about 1 to 30 seconds. The delay is not added to the value of the switch-delay. The total delay from the time when the forwarding rate of the data changes to the time when the system completes the switchover time is longer than the switch-delay period by 1 to 30 seconds.

Example

Specify the delay for the switching to Switch-MDT to 20 seconds in VPN instance **mytest**.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain switch-delay 20
```

10.6.15 multicast-domain switch-group-pool

Function

The **multicast-domain switch-group-pool** command specifies the range of the Switch-multicast distribution tree (MDT) switch-group-pool and the switching condition.

The **undo multicast-domain switch-group-pool** command restores the default configuration.

By default, switch-group-pool is not specified, and the switching to the Switch-MDT is not performed.

Format

multicast-domain switch-group-pool *switch-group-pool* { *network-mask* | *network-mask-length* } [**threshold** *threshold-value* | **acl** { *advanced-acl-number* | *acl-name* }] *

undo multicast-domain switch-group-pool

Parameters

Parameter	Description	Value
switch-group-pool	Specifies the start address of Switch-Group-pool.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
network-mask	Specifies the mask of Switch-Group-pool address.	The mask is in dotted decimal notation and ranges from 255.255.255.0 to 255.255.255.255.
network-mask-length	Specifies the mask length of Switch-Group-pool address.	The value is an integer that ranges from 24 to 32; that is, the range of the group address in Switch-MDT switch-group-pool is from 0 to 255.
threshold *threshold-value*	Specifies the switching threshold.	The value is an integer that ranges from 0 to 4194304, in kbit/s. By default, it is 0.
acl *advanced-acl-number*	Specifies the (S, G) entry which the Switch-Group-pool takes effect on. *advanced-acl-number* indicates the advanced ACL number.	If the ACL is not specified, the Switch-Group-pool takes effect on all (S, G) entries. The number is an integer that ranges from 3000 to 3999.
acl-name	Specifies the name of a Named ACL. **NOTE** *acl-name* can only be the name of a named advanced ACL.	It is case-sensitive.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Between the Provider Edge (PE) connected to the VPN receivers and the PE connected to the VPN multicast source, a special switch-MDT is set up for the high-speed VPN multicast data packets flowing into the public network. The multicast data flow can therefore be switched from the share-MDT to the switch-MDT. Therefore, on-demand multicast can be realized. This prevents data from be flooded in the public network when the share-MDT is used to transmit VPN multicast data packets.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A share-group has been configured in the corresponding VPN.

Configuration Impact

In some cases, the forwarding rate of VPN multicast data fluctuates around the switchover threshold. If the rate remains higher than the switchover threshold, data packets are switched to the switch-MDT. Otherwise, the packets are still forwarded by using the share-MDT.

This command is cyclical in nature. That is, the latest command overwrites the previous one, and takes effect.

Precautions

The Named ACL includes the basic ACL and the advanced ACL, whose configurations are same with the numbered ACL.

From the time when data forwarding rate changes to the time when the system starts the switch-delay timer, there is a delay of 1 to 30 seconds because of necessary traffic calculation and protocol processing. In actual switchover, the delay is longer than the switch-delay period by 1 to 30 seconds.

Example

Set the Switch-group-pool of VPN instance named **mytest** to be from 225.2.2.1 to 225.2.2.15.

```
<Huawei> system-view
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain switch-group-pool 225.2.2.1 28
```

Use a Named ACL to set the Switch-group-pool to be from 225.2.2.1 to 225.2.2.15.

```
<Huawei> system-view
[Huawei] acl name myacl
[Huawei-acl-adv-myacl] rule permit ip source 1.1.1.1 0 destination 225.1.0.0 0.0.255.255
[Huawei] ip vpn-instance mytest
[Huawei-vpn-instance-mytest] ipv4-family
[Huawei-vpn-instance-mytest-af-ipv4] multicast-domain switch-group-pool 225.2.2.1 28 acl myacl
```

Related Topics

10.6.6 display multicast-domain vpn-instance switch-group receive
10.6.7 display multicast-domain vpn-instance switch-group send

10.6.16 multicast-domain switch-without-register

Function

The **multicast-domain switch-without-register** command disables the source Provider Edge (PE) from sending null Register messages to the Rendezvous Point (RP) to establish the shortest path tree (SPT) on the public network before the Switch-Group address is used to encapsulate VPN data.

The **undo multicast-domain switch-without-register** command restores the default setting.

By default, before the Switch-Group address is used to encapsulate VPN data, the source PE sends null Register messages to the RP and establishes the SPT on the public network.

Format

multicast-domain switch-without-register

undo multicast-domain switch-without-register

Parameters

None.

Views

VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In previous implementation, if the Switch-Group address is in the Any-Source Multicast (ASM) address range, when the SPT switchover occurs on the multicast tunnel of the public network, the source PE sends the switchover message to all receiver PEs. After receiving the switchover message, these receiver PEs send the (*, G) Join messages to the RP of the public network to establish the rendezvous point tree (RPT). When the Switch-Group address is used in the VPN to encapsulate multicast data, the public network side of the source PE receives the data forwarded from the VPN based on the Switch-Group address. Afterwards, the forwarding entries are created on the source PE, and the source PE encapsulates the data to the Register messages which are sent to the RP of the public network. Then, the RP decapsulates the Register messages, and sends the data to the receiver PEs. Then, the receiver PEs trigger the SPT switchover towards the source PE. In this manner, the SPT is established on the public network.

When the entries with the SPT switchover are in a large number, the speed of sending Register messages is limited. As a result, sending the first Register message to the RP takes a long time for certain entries, and establishing the SPT on the public network is delayed. In addition, in the process of establishing the SPT on the public network, multicast services are interrupted and certain VPN data may also be discarded, leading to the service interruption on the user end.

To solve the preceding problem, before configuring the VPN to use the Switch-Group address to encapsulate the VPN data, you can configure the source PE to send the null Register message to the RP to establish the SPT on the public network.

Configuration Impact

After the VPN data traffic exceeds the upper limit, the source PE uses the Switch-Group address to encapsulate data and sends the switchover message to the

 Copyright © Huawei Technologies Co., Ltd.

receiver PEs. If the Switch-Group address is allocated for the first time, when sending the switchover message, the source PE sends the Register message that is encapsulated with the VPN Hello message to the RP, and the RP forwards the Register message to the receiver PEs. Based on the received messages, the receiver PEs and the RP directly send the (S,G) Join messages to the source PE and establish the SPT on the public network in advance. In this manner, when the public network tunnel is switched from the RPT to the SPT, the number of discarded multicast messages is reduced and the impact on multicast services is minimized.

Example

When the Switch-Group address is not used to encapsulate VPN data for vpn1, configure the source PE to send the null Register message to the RP to establish the SPT on the public network.

```
<Huawei> system-view
[Huawei] ip vpn-instatnce vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] multicast-domain switch-without-register
```

Related Topics

10.6.5 display multicast-domain vpn-instance share-group
10.6.15 multicast-domain switch-group-pool

10.6.17 reset multicast-domain control-message counters

Function

The **reset multicast-domain control-message counters** command clears statistics about sent and received MDT switch messages in a specified VPN instance or all VPN instances.

Format

reset multicast-domain { **vpn-instance** *vpn-instance-name* | **all-instance** } **control-message counters**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Clears statistics about sent and received MDT switch messages in a specified VPN instance. *vpn-instance-name* specifies the VPN instance name.	The value is a string of case-sensitive characters.
all-instance	Clears statistics about sent and received MDT switch messages in all VPN instances.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a fault occurs on a multicast VPN network, you need to check whether MDT switch messages are normally sent and received. If the current device already records a large number of statistics about MDT switch messages, you can run the **reset multicast-domain control-message counters** command to clear statistics about sent and received messages in a specified VPN instance or all VPN instances and then run the **display multicast-domain control-message counters** command to check whether the count of MDT switch messages increases, which helps fault location.

Precautions

Running the **reset multicast-domain control-message counters** command will clear all statistics about MDT switch messages. Therefore, exercise caution before using this command.

Example

Clear statistics about sent and received MDT switch messages in VPN instance **red**.

```
<Huawei> reset multicast-domain vpn-instance red control-message counters
```

10.6.18 multicast extranet traffic-forward type

Function

The **multicast extranet traffic-forward type** command enables the traffic forwarding function for VLANIF interfaces on a multicast VPN extranet.

The **undo multicast extranet traffic-forward type** command restores the default configuration.

By default, the traffic forwarding function is disabled for VLANIF interfaces on a multicast VPN extranet.

Format

multicast extranet traffic-forward type vlanif

undo multicast extranet traffic-forward type vlanif

Parameters

Parameter	Description	Value
vlanif	Enables the traffic forwarding function for VLANIF interfaces on a multicast VPN extranet.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, VLANIF interfaces do not forward traffic on a multicast VPN extranet, causing traffic interruptions. To resolve this issue, run the **multicast extranet traffic-forward type** command to enable the traffic forwarding function for VLANIF interfaces. After this command is run, forwarding information on the VLANIF interfaces will be delivered from the VPN routing and forwarding (VRF) table for receivers to the VRF table for multicast sources. Then, the VLANIF interfaces will be capable of forwarding traffic to receivers.

Precautions

The **multicast extranet traffic-forward type** command configuration is ineffective for existing multicast entries. To resolve this issue, run the **reset multicast forwarding-table** command to delete the existing multicast entries. After the multicast entries are regenerated, the **multicast extranet traffic-forward type** command will become effective for them.

Example

Enable the traffic forwarding function for VLANIF interfaces on a multicast VPN extranet.

```
<Huawei> system-view
[Huawei] multicast extranet traffic-forward type vlanif
```

10.6.19 rpf-vector compatible standard

Function

The **rpf-vector compatible standard** command configures a device to use the standard format defined in a relevant RFC to encapsulate Hello or Join/Prune messages carrying vector attributes.

The **undo rpf-vector compatible standard** command enables a device to use a private format to encapsulate Hello or Join/Prune messages carrying vector attributes.

 Copyright © Huawei Technologies Co., Ltd.

By default, a private format is used to encapsulate Hello or Join/Prune messages carrying vector attributes.

Format

rpf-vector compatible standard

undo rpf-vector compatible standard

Parameters

None

Views

Public network instance PIM view or VPN instance PIM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The vector attribute needs to be added to Join/Prune messages as the join attribute on PEs in an inter-AS MVPN Option B scenario. The **rpf-vector compatible standard** command can be used to configure the Provider Edges (PEs) to use the standard format to encapsulate Hello or Join/Prune messages carrying vector attributes. This command configuration facilitates device communication.

Prerequisites

The **multicast routing-enable** command has been run in the public network instance view or the VPN instance view.

Example

Configure a device on the public network to use the standard format to encapsulate Hello and Join/Prune messages carrying vector attributes.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] rpf-vector compatible standard
```

10.6.20 rpf-vector

Function

The **rpf-vector** command enables a device to add the vector attribute to a Join/Prune message as the join attribute.

The **undo rpf-vector** command disables a device from adding the vector attribute to a Join/Prune message as the join attribute.

 Copyright © Huawei Technologies Co., Ltd.

By default, a device is disabled from adding the vector attribute to a Join/Prune message as the join attribute.

Format

rpf-vector rd

undo rpf-vector rd

Parameters

Parameter	Description	Value
rd	Specifies the RD attribute in a vector.	-

Views

Public network instance PIM view or VPN instance PIM view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **rpf-vector rd** command needs to be run on Provider Edges (PEs) in an inter-AS MVPN Option B scenario to enable the PEs to add vector attributes with Route Distinguishers (RDs) to Join/Prune messages as join attributes. Then MDTs can be set up and inter-AS MVPN can be implemented.

Prerequisites

The **multicast routing-enable** command has been run in the public network instance view or the VPN instance view.

Example

Enable a device on the public network to add the vector attribute to a Join/Prune message as the join attribute.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim
[Huawei-pim] rpf-vector rd
```

Enable a device in VPN RED to add the vector attribute to a Join/Prune message as the join attribute.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] pim vpn-instance RED
[Huawei-pim-RED] rpf-vector rd
```

 Copyright © Huawei Technologies Co., Ltd.

10.7 Multicast Route Management (IPv4) Commands

10.7.1 display default-parameter mrm

Function

The **display default-parameter mrm** command displays the default configurations for multicast routing management (MRM).

Format

display default-parameter mrm

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays only the default configurations, regardless of whether MRM parameters are changed. Therefore, you can use this command to check which parameters have been modified.

Example

Display default configurations for MRM.

```
<Huawei> display default-parameter mrm
  System View Default Configurations:
  -----------------------------------
  Load splitting rule: disabled
  Load-splitting-timer: 1800 s
  Route selection rule: preference-preferred
  Multi-topology: disabled

  Interface View Default Configurations:
  --------------------------------------
  Minimum TTL: 1
  Reject inbound data: disabled
  Reject outbound data: disabled
  Multicast load-splitting weight: 1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-88 Description of the display default-parameter mrm command output

Item	Description
System View Default Configurations	Default configurations in the system view.
Load splitting rule	Whether multicast load splitting is configured. By default, multicast load splitting is not configured. To configure multicast load splitting, run the **multicast load-splitting** command.
Load-splitting-timer	Default value of the multicast load splitting balancing timer. By default, the value is 1800s. You can run the **multicast load-splitting-timer** command to set the value of the multicast load splitting balancing timer.
Route selection rule	RPF route selection rule. By default, RPF route selection is based on the preference of the routing protocol.
Multi-topology	The Multicast-Topology function.
Interface View Default Configurations	Default configurations in the interface view.
Minimum TTL	Minimum TTL value for multicast packet forwarding.
Reject inbound data	Whether the interface is disabled from receiving multicast packets.
Reject outbound data	Whether the interface is disabled from forwarding multicast packets.
Multicast load-splitting weight	Multicast load splitting weight of the interface. By default, the multicast load splitting weight of an interface is 1. You can run the **multicast load-splitting weight** command to set the value of the multicast load splitting weight.

Related Topics

10.7.24 multicast load-splitting
10.7.26 multicast load-splitting-timer
10.7.25 multicast load-splitting weight

10.7.2 display migp routing-table

Function

The **display migp routing-table** command displays brief information about the MIGP routing table.

Format

display migp routing-table [*ip-address* [*mask-length* | *mask*]] [**verbose**]

Parameters

Parameter	Description	Value
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Indicates a mask.	The mask is in dotted decimal notation.
mask-length	Specifies the length of the mask.	The value is a decimal integer ranging from 0 to 32.
verbose	Displays detailed information about active routes and inactive routes. If the parameter is not specified, only brief information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display brief information about the MIGP routing table.

```
<Huawei> display migp routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: MIGP
         Destinations : 4        Routes : 4

Destination/Mask    Proto  Pre  Cost      Flags NextHop         Interface

10.4.4.4/32         OSPF   10   3           10.0.1.1        GigabitEthernet1/0/0
```

```
10.5.5.5/32        OSPF   10   4            10.0.1.1        GigabitEthernet1/0/0
10.0.3.0/24        OSPF   10   3            10.0.1.1        GigabitEthernet1/0/0
192.168.3.0/24      OSPF   10   4            10.0.1.1        GigabitEthernet1/0/0
```

Table 10-89 Description of the display migp routing-table command output

Item	Description
Route Flags	Route flag that identifies the attribute of a route. ● R: indicates that the route is an iterated route. ● D: indicates that the route is delivered to the FIB table.
Routing Tables: MIGP	MIGP routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Routing protocol that learns a route.
Pre	Route preference.
Cost	Route cost.
Flags	Route flags in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

Display detailed information about the MIGP routing table.

```
<Huawei> display migp routing-table verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : MIGP
         Destinations : 5        Routes : 5


Destination: 10.4.4.4/32
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 20
      NextHop: 10.0.1.1         Interface: GigabitEthernet1/0/0
        State: Active Adv            Age: 00h34m26s

Destination: 10.5.5.5/32
     Protocol: ISIS            Process ID: 1
   Preference: 15                    Cost: 30
      NextHop: 10.0.1.1         Interface: GigabitEthernet1/0/0
        State: Active Adv            Age: 00h34m26s
```

```
Destination: 10.0.2.0/24
    Protocol: ISIS          Process ID: 1
  Preference: 15                  Cost: 20
     NextHop: 10.0.1.1       Interface: GigabitEthernet1/0/0
       State: Active Adv           Age: 00h34m26s

Destination: 10.0.3.0/24
    Protocol: ISIS          Process ID: 1
  Preference: 15                  Cost: 30
     NextHop: 10.0.1.1       Interface: GigabitEthernet1/0/0
       State: Active Adv           Age: 00h34m27s

Destination: 192.168.3.0/24
    Protocol: ISIS          Process ID: 1
  Preference: 15                  Cost: 40
     NextHop: 10.0.1.1       Interface: GigabitEthernet1/0/0
       State: Active Adv           Age: 00h34m28s
```

Table 10-90 Description of the display migp routing-table verbose command output

Item	Description
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol that learns a route.
Process ID	Process ID of the routing protocol.
Preference	Preference of a route.
Cost	Indicates the route cost.
NextHop	Next hop of a route.
Interface	Outbound interface of a route.
State:	Status of routes, which can be: ● Active: indicates routes in the Active state. ● Invalid: indicates invalid routes. ● Inactive: indicates routes in the Inactive state. ● NoAdv: indicates routes that cannot be advertised. ● Adv: indicates routes that can be advertised. ● Del: indicates routes to be deleted. ● GotQ: indicates routes that are relayed successfully. ● WaitQ: indicates routes that are not relayed successfully yet. ● Stale: indicates routes with the Stale flag. The routes are used in GR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Age	Time that elapsed since a route is generated.

10.7.3 display migp routing-table statistics

Function

The **display migp routing-table statistics** command displays the statistics about the MIGP routing table.

Format

display migp routing-table statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Integrated route statistics contain the total number of routes added or deleted through protocols and the total number of active or inactive routes with deletion flags but are not deleted.

Example

Display the statistics about routes in the MIGP routing table.

```
<Huawei> display migp routing-table statistics
Proto     total      active      added        deleted      freed
         routes     routes      routes       routes       routes
OSPF       0          0           0            0            0
IS-IS      5          5           45           40           40
Total      5          5           45           40           40
```

Table 10-91 Description of the display migp routing-table statistics command output

Item	Description
Proto	Routing protocol.

Item	Description
total routes	Total number of routes in the current routing table.
active routes	Number of active routes in the routing table.
added routes	Number of routes (active and inactive) added to the routing table.
deleted routes	Number of routes deleted from the routing table.
freed routes	Number of released routes that are deleted permanently from the routing table.

10.7.4 display mrt routing-table

Function

The **display mrt routing-table** command displays MRT routes.

Format

display mrt routing-table [**vpn-instance** *vpn-instance-name*] [*ip-address* [*mask* | *mask-length*]] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Specifies mask.	The mask is in dotted decimal notation.
mask-length	Specifies mask length.	It is an integer ranging from 0 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Displays detailed information about active and inactive routes. If the parameter **verbose** is not specified, detailed information about active routes is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view specific routing information.

Example

Display information about all MRT routes.

```
<Huawei> display mrt routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: MRT
         Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost  Flags  NextHop  Interface

  10.5.5.1/32     MSR    255     0     R   10.1.1.1  GigabitEthernet1/0/0
```

Table 10-92 Description of the display mrt routing-table command output

Item	Description
Route Flags	Route flag that identifies the attribute of a route. ● R: indicates an iterated route. ● D: indicates that the route is downloaded to the FIB table.
Routing Tables: MRT	IMRT routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Protocol that learns a route.
Pre	Route preference.

Item	Description
Cost	Route cost.
Flags	Route flag in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

Display the detailed information of the specified routes.

```
<Huawei> display mrt routing-table 10.12.12.12 verbose
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Table : MRT
Summary Count : 1

Destination: 10.12.12.12/32
     Protocol: MSR            Process ID: 0
   Preference: 1                    Cost: 0
      NextHop: 10.11.11.12      Neighbour: 0.0.0.0
        State: Active Adv Relied      Age: 00h04m49s
          Tag: 0                 Priority: low
        Label: NULL                 QoSInfo: 0x0
   IndirectID: 0x80000002
 RelayNextHop: 0.0.0.0            Interface: GigabitEthernet1/0/0
     TunnelID: 0x0                Flags: R
```

Table 10-93 Description of the display mrt routing-table verbose command output

Item	Description
Routing Table: MRT	MRT routing table.
Summary Count	Number of the destination network and host.
Destination	Address and mask length of the destination network or host.
Protocol	Routing protocol that learns a route.
Process ID	Process ID of the routing protocol.
Preference	Route preference.
Cost	Route cost.
NextHop	Next hop of a route.
Neighbour	Address of the neighbor.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	Status of routes: ● Active: indicates active routes. ● Invalid: indicates invalid routes. ● Inactive: indicates inactive routes. ● NoAdv: indicates the routes that cannot be advertised. ● Adv: indicates the routes that can be advertised. ● Del: indicates the routes to be deleted. ● Relied: indicates the route that finds the next hop and outbound interface or the route that finds the tunnel during packet forwarding. ● WaitQ: indicates the route that does not find the next hop or outbound interface or the route that does not find the tunnel. ● Stale.: indicates the routes with the stale flag. The routes are used in GR.
Age	Time that elapsed since a route is generated.
Tag	Administrative tag for routes.
Priority	Priority of a route.
Label	MPLS label allocated to a route.
QoSInfo	QoS information.
IndirectID	ID of the indirect next hop.
RelayNextHop	Relay next hop.
Interface	Outbound interface through which the next hop is reachable.
TunnelID	Tunnel ID.
Flags	Route flag in the header of the routing table.

10.7.5 display mrt routing-table statistics

Function

The **display mrt routing-table statistics** command displays statistics about the MRT routes.

Format

display mrt routing-table [**vpn-instance** *vpn-instance-name*] **statistics**

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Route statistics include:

- Total number of routes that are added or deleted by the protocol
- Number of active or inactive routes that are tagged for deletion but not deleted

Example

Display statistics about routes in the MRT routing table.

```
<Huawei> display mrt routing-table statistics
Proto     total      active     added       deleted     freed
          routes     routes     routes      routes      routes
MSTATIC   1          0          1           0           0
```

Table 10-94 Description of the display mrt routing-table statistics command output

Item	Description
Proto	Routing protocol.
total routes	Total number of routes in the routing table.
active routes	Number of active routes in the routing table.
added routes	Number of active and inactive routes added in the routing table.
deleted routes	Number of routes to be deleted from the routing table.
freed routes	Number of routes that are permanently deleted from the routing table.

 Copyright © Huawei Technologies Co., Ltd.

10.7.6 display mrt routing-table vpn-instance

Function

The **display mrt routing-table vpn-instance** command displays the MRT routing table of a VPN instance.

Format

display mrt routing-table vpn-instance *vpn-instance-name* [*ip-address* [*mask* | *mask-length*] [**longer-match**]] [**verbose**]

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ip-address	Specifies a destination IP address.	The address is in dotted decimal notation.
mask	Specifies mask.	The mask is in dotted decimal notation.
mask-length	Specifies mask length.	The value is a decimal integer that ranges from 0 to 32.
longer-match	Displays only routes that match the specified network or mask.	-
verbose	Displays detailed information about active and inactive routes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can specify different parameters to view the specific routing information.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the MRT routing table of the IPv4 VPN instance named vpn1.

```
<Huawei> display mrt routing-table vpn-instance vpn1
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: MSR
         Destinations : 1        Routes : 1

Destination/Mask  Proto  Pre  Cost  Flags  NextHop  Interface

  10.5.5.1/32     MSR    255    0     R    10.1.1.1    GigabitEthernet1/0/0
```

Table 10-95 Description of the display mrt routing-table vpn-instance command output

Item	Description
Route Flags	Route flag that identifies the attribute of a route. ● R: indicates an iterated route. ● D: indicates that the route is downloaded to the FIB table.
Routing Tables: MSR	MRT routing table.
Destinations	Total number of destination networks or hosts.
Routes	Total number of routes.
Destination/Mask	Address and mask length of the destination network or host.
Proto	Protocol through which routes are learned.
Pre	Route preference.
Cost	Route cost.
Flags	Route flag in the header of the routing table.
NextHop	Next hop of a route.
Interface	Outbound interface to a reachable next hop.

10.7.7 display mtrace statistics

Function

The **display mtrace statistics** command displays statistics about multicast trace (Mtrace) packets.

Format

display mtrace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To collect statistics about Mtrace traffic generated in a certain period, clear the original statistics.

Example

Display statistics about the current Mtrace traffic.

```
<Huawei> display mtrace statistics
Mtrace statistics:
 Type        Send       Receive       Invalid
 Query        10          5             0
 Request      20          4             0
 Response      3          7             1
```

Table 10-96 Description of the display mtrace statistics command output

Item	Description
Type	Indicates the types of Mtrace packets. The types are as follows: ● Query: IGMP-Tracert-Query packets. ● Request: IGMP-Tracert-Request packets. ● Response: IGMP-Tracert-Response packets.
Send	Indicates the number of sent packets.
Receive	Indicates the number of received packets.
Invalid	Indicates the number of invalid packets.

Related Topics

10.7.30 reset mtrace statistics

10.7.8 display multicast boundary

Function

The **display multicast boundary** command displays the multicast boundary configured on an interface.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Specifies all the instances.	-
group-address	Specifies a multicast group address.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of the multicast group address.	The mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast group address.	The value is a decimal integer that ranges from 4 to 32.
interface *interface-type interface-number*	Specifies the type and the number of an interface. The parameter is used to specify an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to check the boundary of a PIM-SM network. When some hosts cannot receive multicast data, you can use this command to check whether the problem is caused by multicast boundary configuration.

Example

Display the boundaries configured on all the interfaces in the public network instance.

```
<Huawei> display multicast boundary
Multicast boundary information of VPN-Instance: public net
```

```
Total 1 Multicast IPv4 boundary
 Interface          Boundary
 GigabitEthernet1/0/0          225.1.1.0/24
```

Table 10-97 Description of the display multicast boundary command output

Item	Description
Multicast boundary information of VPN-Instance	VPN instance to which multicast boundary information belongs.
Total 1 Multicast IPv4 boundary	Total number of multicast boundaries configured on a router.
Interface	Interface configured with a multicast boundary.
Boundary	Information about the multicast boundary address.

Related Topics

10.7.17 multicast boundary

10.7.9 display multicast boundary policy

Function

The **display multicast boundary policy** command displays information about multicast boundary policies.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **boundary policy** [*group-address source-address* | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all instances.	-
group-address	Specifies a multicast group address.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-address	Specifies a multicast source address.	The value is in dotted decimal notation. If the multicast source address is 0.0.0.0 in an entry, the entry is a (*, G) entry.
interface *interface-type interface-number*	Specifies the type and number of an interface on the router.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. The **display multicast boundary policy** command can be used to view information about multicast boundary policies.

Precautions

When using the **display multicast boundary policy** command, note the following points:

- If neither **vpn-instance** nor **all-instance** is specified, information about multicast boundary policies configured in the public network instance is displayed.
- If *group-address source-address* are specified, information about the multicast boundary policy that filters packets based on source and group addresses on each interface.
- If **interface** *interface-type interface-number* are specified, information about the multicast boundary on a specific interface is displayed.

Before running this command to check multicast boundary configuration, enable PIM in the interface view.

Example

Display information about multicast boundary policies in the public network instance.

```
<Huawei> display multicast boundary policy
Direction Flags: I - in, O - out, A - filter-autorp
-----------------------------------------------------------------
```

```
Multicast boundary policy information of VPN-Instance: public net
Total 1 multicast IPv4 boundary policies
 Interface            Boundary policy     Direction          Result
 Eth0/0/1              2000                I O                --
```

Display information about the multicast boundary policy for (10.0.0.1, 225.0.0.0) in the public network instance.

```
<Huawei> display multicast boundary policy 225.0.0.0 10.0.0.1
Direction Flags: I - in, O - out, A - filter-autorp
-----------------------------------------------------------------
Multicast boundary policy information of VPN-Instance: public net
Total 1 multicast IPv4 boundary policies
 Interface            Boundary policy     Direction          Result
 Eth0/0/1              2000                I O                Block
```

Table 10-98 Description of the **display multicast boundary policy** command output

Item	Description
Direction Flags	Flag indicating the direction in which a multicast boundary policy takes effect: ● 1: indicates the inbound direction. ● O: indicates the outbound direction. ● A: filters Auto-RP packets.
Multicast boundary policy information of VPN-Instance	VPN instance to which multicast boundary information belongs
Total 2 multicast IPv4 boundary policies	Total number of multicast boundary policies configured on the router
Interface	Interface on which a multicast boundary is configured
Boundary policy	ACL applied to a multicast boundary policy on a specific interface
Direction	Flag indicating the direction in which a multicast boundary policy takes effect: ● 1: inbound direction ● O: indicates the outbound direction. ● A: filters Auto-RP packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Result	Whether a multicast boundary is configured in a specific direction for a specific multicast source and group on a specific interface: ● Block: indicates that a multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. ● Unblock: indicates that no multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. ● --: indicates that the multicast source and group addresses are not identified.

Related Topics

10.7.18 multicast boundary policy

10.7.19 multicast boundary policy in

10.7.20 multicast boundary policy out

10.7.10 display multicast forwarding-table

Function

The **display multicast forwarding-table** command displays the multicast forwarding table.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** } | { **statistics** | **verbose** }] *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-
group-address	Specifies a multicast group address.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast address or source address.	-
group-mask	Specifies the mask of the multicast group address.	The mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of the multicast group address.	The value is a decimal integer that ranges from 4 to 32.
source-address	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
source-mask	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is a decimal integer that ranges from 0 to 32.
incoming-interface	Indicates the inbound interface of a multicast forwarding entry.	-
interface-type interface-number	Specifies the type and the number of an interface.	-
register	Indicates the register interface of a multicast forwarding entry.	-
outgoing-interface	Indicates the outbound interface of a multicast forwarding entry.	-
include	Displays the (S, G) entry list that contains the specified downstream interface.	-
exclude	Displays the (S, G) entry list that does not contain the specified downstream interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match	Displays the (S, G) entry list that matches the specified interface and the (S, G) entries have only one specified interface.	-
none	Indicates that the downstream interface list is null.	-
verbose	Displays detailed information about forwarding entries.	-
statistics	Displays the statistics about the multicast forwarding table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During multicast routing and forwarding, routing information generated by multicast routing protocols is saved in a multicast routing table. The router selects the optimal multicast routes from the routing table according to multicast routing and forwarding policies, and then delivers the selected multicast routes to the multicast forwarding table to guide multicast data forwarding.

You can use the **display multicast forwarding-table** command to check whether multicast forwarding entries have been generated and whether multicast data can be forwarded normally.

Example

Display the multicast forwarding table of the public network instance.

```
<Huawei> display multicast forwarding-table
Multicast Forwarding Table of VPN-Instance: public net
Total 1 entry, 1 matched

00001. (10.10.10.2, 225.0.0.1)
    MID: 0, Flags: ACT
    Uptime: 00:08:32, Timeout in: 00:03:26
    Incoming interface: GigabitEthernet1/0/0
    List of 1 outgoing interfaces:
      1:  GigabitEthernet2/0/0
          Activetime: 00:23:15
    Matched 1775842131 packets(113653895502 bytes), Wrong If 0 packets
    Forwarded 1769618431 packets(1071392 bytes)
```

Table 10-99 Description of the display multicast forwarding-table command output

Item	Description
Multicast Forwarding Table of VPN-Instance: public net	VPN instance to which the multicast forwarding table corresponds.
Total 1 entry, 1 matched	Total number of forwarding entries and number of eligible forwarding entries
00001	Sequence number of the (S, G) entry
(10.10.10.2, 225.0.0.1)	(S, G) entry in the multicast forwarding table
MID	Uniquely identifies the multicast forwarding entry in the MFIB table. MID is used to rapidly search the multicast forwarding table.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Flags	Indicates the status flag of the (S, G) entry. ● ACT: indicates that an active event is triggered. ● DUM: indicates a dummy entry. ● MISS: indicates that the nocache time needs to be reported. ● DROP: indicates packet dropping. ● LTH: indicates that the traffic volume is below the threshold. ● DEL: indicates a deleted entry. ● RST: indicates that registration of the known timer is started. ● 2IODEL: indicates that an entry is deleted from the MFIB table, and the update needs to be synchronized to the IO board. ● 2PDEL: indicates that an entry is deleted from the device, and the update needs to be synchronized to the IO board. ● 2SYNC: indicates that the entry is contained in the MFIB table but it does not exist on the device. ● 2ADD: indicates that the entry existing on the device has not been added to the MFIB table. ● CLR: indicates that the MFIB table is resetting. ● L2FWD: indicates that the device forwards Layer 2 traffic in multicast mode. ● NORPF: indicates that the device does not perform RPF check. ● 2ACK: indicates that the VPN instance is waiting for the ACK message from the slave main control board. ● 2RSED: indicates that the entry is waiting for retransmission. ● IOACK: indicates that the VPN instance has received the ACK message from the LPU. ● SACK: indicates that the VPN instance has received the ACK message forwarded by software. ● BKCLR: indicates that the MFIB table on the slave main control board is resetting. ● EXTR: indicates an extranet entry. ● 2DEL: indicates that the entry deleted from the device has not been removed from the MFIB table. ● PDEL: indicates that the entry does not exist on the device. ● A denotes addition; D denotes deletion; I denotes upstream update; R denotes RP update; P denotes PMBR; F denotes flag.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• S denotes SPT; E denotes encapsulation group update; US denotes status update; CS denotes status clearing.
Uptime	Period duration of the (S, G) entry
Timeout in	Remaining time of the (S, G) entry
Incoming interface	Upstream interface of the (S, G) entry
List of 1 outgoing interfaces	Downstream interface list. The contents of the downstream interface list are as follows: • Name and number of the outbound interface • The existing time of outbound interface • Multicast traffic that takes this interface as the outbound interface, in bytes • Number of packets with an incorrect incoming interface • Forwarded multicast traffic, in bytes

Related Topics

10.7.21 multicast forwarding-table downstream-limit
10.7.22 multicast forwarding-table route-limit
10.7.11 display multicast routing-table
10.7.31 reset multicast forwarding-table

10.7.11 display multicast routing-table

Function

The **display multicast routing-table** command displays information about a multicast routing table.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **extranet** { **source-vpn-instance** { *vpn-instance-name* | **all** | **public** } | **receive-vpn-instance** { *vpn-instance-name* | **all** } } | **incoming-interface** { *interface-type interface-number* | **register** | **mcast-extranet** } | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** | **none** | **vpn-instance** *vpn-instance-name*}] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Specifies all the instances.	-
group-address	Indicates the multicast group address.	The address is in dotted decimal notation. The value ranges from 224.0.1.0 to 239.255.255.255.
mask { *group-mask* | *group-mask-length* }	Indicates the mask of the multicast group address.	• *group-mask*: The address is in dotted decimal notation. The value ranges from 240.0.0.0 to 255.255.255.255. • *group-mask-length*: The value is an integer that ranges from 4 to 32
source-address	Indicates the multicast source address.	The address is in dotted decimal notation.
mask { *source-mask* | *source-mask-length* }	Indicates the mask of the specified source address.	• *source-mask*: The address is in dotted decimal notation. The value ranges from 0.0.0.0 to 255.255.255.255. • *source-mask-length*: The value is an integer that ranges from 0 to 32
extranet	Indicates multicast extranet routing entries.	-
source-vpn-instance *vpn-instance-name*	Indicates the source VPN instance. *vpn-instance-name* specifies the name of the source VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Indicates all instances.	-
public	Indicates the public network instance.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
receive-vpn-instance *vpn-instance-name*	Indicates the receiver VPN instance. *vpn-instance-name* specifies the name of the receiver VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface	Indicates the upstream interface of a multicast routing entry.	-
interface-type interface-number	Indicates the type and the number of an interface.	-
register	Indicates the register interface of a multicast routing entry.	-
mcast-extranet	Indicates that the upstream interface is an extranet interface.	-
outgoing-interface	Indicates the downstream interface of a multicast routing entry.	-
include	Indicates the (S, G) entries whose downstream interface list contains specified downstream interfaces.	-
exclude	Indicates the (S, G) entries whose downstream interface list does not contain specified downstream interfaces.	-
match	Indicates (S, G) entries whose the downstream interface list contains only one interface that is the same as a specified downstream interface.	-
none	Indicates that the downstream interface list is null.	-
outgoing-interface-number	Indicates the number of downstream interfaces of multicast routing entries.	-
number	Specifies the number of downstream interfaces.	The value is an integer that ranges from 0 to 2048.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display multicast routing-table** command is used to display the information of a multicast routing table.

Example

Display the corresponding routing entry of a multicast group in the multicast routing table of the public network instance.

```
<Huawei> display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry
 00001. (192.168.0.2, 227.0.0.1)
      Uptime: 00:00:28
      Upstream Interface: GigabitEthernet1/0/0
      List of 2 downstream interfaces
         1:  GigabitEthernet2/0/0
         2:  GigabitEthernet3/0/0
```

Table 10-100 Description of the display multicast routing-table command output

Item	Description
Multicast routing table of VPN-Instance	VPN instance to which the multicast routing information corresponds.
Total 1 entry	Number of eligible routing entries.
00001	Sequence number of the (S, G) entry.
(192.168.0.2, 227.0.0.1)	(S, G) entry in the multicast routing table.
Uptime	Time that elapsed since the (S, G) entry was generated.
Upstream Interface	Upstream interface of the (S, G) entry.
List of 2 downstream interfaces	Downstream interface list.

Display the number of downstream interfaces of the multicast routing entries in the public network instance.

```
<Huawei> display multicast routing-table outgoing-interface-number
Multicast routing table of VPN-Instance: public net
 Total 2 entries

 00001. (10.1.1.22, 232.1.1.1)
      Uptime: 00:00:07
      Upstream Interface: GigabitEthernet1/0/0
      List of 20 downstream interfaces
```

```
00002. (10.1.1.22, 232.1.2.1)
    Uptime: 00:00:07
    Upstream Interface: GigabitEthernet2/0/0
    List of 20 downstream interfaces
```

Table 10-101 Description of the display multicast routing-table outgoing-interface-number command output

Item	Description
List of 20 downstream interfaces	Number of downstream interfaces in multicast routing entries.

Related Topics

10.7.10 display multicast forwarding-table

10.7.32 reset multicast routing-table

10.7.12 display multicast routing-table static

Function

The **display multicast routing-table static** command displays the multicast static routes.

Format

display multicast routing-table [**vpn-instance** *vpn-instance-name*] **static** [**config**] [*source-address* { *mask* | *mask-length* }]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
config	Displays the configuration of the multicast static routes.	-
source-address	Specifies a multicast source address.	The address is in dotted decimal notation.
mask	Specifies the mask of the multicast source address.	The mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether multicast RPF static routes are configured successfully, run the **display multicast routing-table static** command.

Example

Display all multicast static routes in the public network instance.

```
<Huawei> display multicast routing-table static
Multicast Routing Table
Routes : 1

 Mroute 10.1.0.0/24
         Interface = GigabitEthernet1/0/0        RPF Neighbor = 10.1.2.2
         Matched routing protocol = ospf, process-id = 100, Route-policy = none
         Preference = 1, Order = 1
 Running Configuration = ip rpf-route-static 10.1.0.0 24 ospf 100 10.1.2.2 order 1
```

Table 10-102 Description of the display multicast routing-table static command output

Item	Description
Multicast Routing Table	Multicast routing table.
Routes	Number of routes.
Mroute	Source address and mask length of a multicast route.
Interface	Outbound interface of the reachable multicast source.
RPF Neighbor	Neighbor IP address through which the source address is reachable.
Matched routing protocol	Matching unicast route type, which can be: ● IS-IS ● RIP ● OSPF ● BGP ● Unicast static route
process-id	Process ID of a routing protocol.
Route-policy	Routing policy. The source address of a route must match the routing policy.
Preference	Preference of a route.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Order	Order of a route.
Running Configuration	Command line for configuring a static route.

Related Topics

10.7.14 ip rpf-route-static

10.7.13 display multicast rpf-info

Function

The **display multicast rpf-info** command displays the Reverse Path Forwarding (RPF) routes of a specified IPv4 multicast source or source/group.

Format

display multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **rpf-info** *source-address* [*group-address*] [**rpt** | **spt**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-
source-address	Specifies the address of a multicast source, used to display the information of RPF routing corresponding to the source.	The address is in dotted decimal notation.
group-address	Specifies the multicast group address, used to display the information of RPF routing corresponding to the source/group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
rpt	Displays the RPF routing information corresponding to a specified source or source/group on the shared RP-tree.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
spt	Displays the RPF routing information corresponding to a specified source or source/group on the shortest path tree.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The RPF route with the *source-address* as the destination address is an optimal route selected from unicast routes, multicast static routes, MBGP routes, and MIGP routes. You can use the **display multicast rpf-info** command to check the RPF route to the specified source or source-group.

Example

Display all RPF routes to the source address 192.168.0.1 in the public network instance.

```
<Huawei> display multicast rpf-info 192.168.0.1
 VPN-Instance: public net
 RPF information about source: 192.168.0.1
     RPF interface: GigabitEthernet1/0/0, RPF neighbor: 10.1.5.2
     Referenced route/mask: 192.168.0.0/24
     Referenced route type: unicast
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 10-103 Description of the display multicast rpf-info command output

Item	Description
VPN-Instance	VPN instance to which displayed information belongs.
RPF information about source	Multicast source to which the multicast RPF path belongs.
RPF interface	RPF interface.
RPF neighbor	RPF neighbor.
Referenced route/mask	Referenced route and its mask.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Referenced route type	Referenced route types: ● unicast: unicast routes ● MBGP: MBGP routes ● mstatic: multicast static routes ● MIGP: MIGP routes
Route selection rule	RPF route selection rules: ● preference-preferred: selecting routes based on the preference of the routing protocols ● longest-match: selecting routes based on the longest matching rule
Load splitting rule	Load splitting rules: ● disable: load splitting disabled. ● balance-preferred: load balancing preferred. ● stable-preferred: stable-preferred load splitting. ● source: load splitting based on source addresses. ● group: load splitting based on group addresses. ● source-group: load splitting based source and group addresses.

Related Topics

10.7.11 display multicast routing-table
10.7.10 display multicast forwarding-table
10.7.14 ip rpf-route-static

10.7.14 ip rpf-route-static

Function

The **ip rpf-route-static** command configures a multicast static route.

The **undo ip rpf-route-static** command deletes a multicast static route.

By default, no multicast static route is configured.

Format

ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**]

[**route-policy** *route-policy-name*] { *rpf-nbr* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] { *source-address* { *mask* | *mask-length* } [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **static**] [**route-policy** *route-policy-name*] | **all** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* specifies the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
source-address	Specifies the address of a multicast source.	The address is in dotted decimal notation.
mask	Indicates the address mask of the multicast source.	The address mask is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast source address.	The value is a decimal integer that ranges from 0 to 32.
isis *process-id*	Specifies that matched routes must be generated by the IS-IS protocol. *process-id* indicates the IS-IS process ID.	The value is a decimal integer that ranges from 1 to 65535.
ospf *process-id*	Specifies that matched routes must be generated by the OSPF protocol. *process-id* indicates the OSPF process ID.	The value is a decimal integer that ranges from 1 to 65535.
rip *process-id*	Specifies that matched routes must be generated by the RIP protocol. *process-id* indicates the RIP process ID.	The value is a decimal integer that ranges from 1 to 65535.
bgp	Specifies that matched routes must be generated by the BGP protocol.	-
static	Specifies that matched routes must be static routes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
route-policy *route-policy-name*	Indicates the matching rule of multicast static routes. *route-policy-name* specifies the name of a route matching rule.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
rpf-nbr	Specifies the IP address of the RPF neighbor.	-
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
order *order-number*	Indicates the configuration order of routes in the same network segment.	The value is a decimal integer that ranges from 1 to 100.
preference *preference*	Indicates the preference of routes. The greater the value is, the lower the preference is.	The value is a decimal integer that ranges from 1 to 255. By default, it is 1.
all	Indicates all multicast static routes in the multicast static routing table.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast static route specifies an RPF interface or RPF neighbor for multicast packets from a specified multicast source. You can configure a multicast static route to:

- Change an RPF route.

  If you want an interface to receive multicast data packets from a specified multicast source but the interface is not the RPF interface for the multicast source, configure a multicast static route to specify this interface as the RPF interface for the multicast source. When the router receives multicast data packets from the multicast source, it performs RPF check using the configured RPF route. Packets sent from the source to the router through other interfaces fail the RPF check.
- Connect RPF routes.

If the unicast route on a network segment is incomplete, multicast packets cannot be forwarded due to lack of an RPF route. For example, when two adjacent devices run different routing protocols but the routing protocols do not import routes from each other, packets cannot be forwarded between the two devices. In this case, you can configure RPF static routes on the devices. The devices can perform RPF check using the specified RPF interfaces so that multicast packets can be forwarded successfully.

Precautions

- If you specify a protocol type in the **ip rpf-route-static** command, the router compares the configured multicast static route with the unicast routes of the specified protocol. If protocol types of the optimal unicast route and the multicast static route are different, the router selects the optimal unicast route as the RPF route.
- A multicast static route is identified by three elements: *source-address* { *mask* | *mask-length* }, protocol type, and *route-policy-name*. Two multicast static routes are considered different as long as one element has different values in the two routes. A maximum of eight multicast static routes can be configured on a network segment.
- If the next-hop interface of a multicast static route is a P2P interface, you can specify the next-hop interface in the command. If the next-hop interface is a P2MP interface, you must specify the next-hop address.
- A multicast static route may not take effect after you configure it using the **ip rpf-route-static**, because the specified interface is Down. After configuring a multicast static route, you are advised to run the **display multicast routing-table static** command to check whether the route is configured successfully and takes effect.

Example

Configure a multicast static route.

```
<Huawei> system-view
[Huawei] ip rpf-route-static 10.0.0.0 255.0.0.0 rip 1 route-policy map1 10.10.0.1
```

Related Topics

10.7.12 display multicast routing-table static
10.7.13 display multicast rpf-info

10.7.15 mtrace

Function

The **mtrace** command detects the multicast path or RPF path from a multicast source to the querier or to a destination host. The querier indicates the router on which the **mtrace** command is executed.

Format

mtrace [**-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **source** *source-address*

mtrace -g *group* [**-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **source** *source-address*

mtrace { **-gw** *last-hop-router* | **-d** } **-r** *receiver* [**-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **source** *source-address*

mtrace { **-gw** *last-hop-router* | **-b** | **-d** } **-r** *receiver* **-g** *group* [**-a** *source-ip-address* | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | [**-mr** | **-ur** *resp-dest*] | **-q** *nqueries* | **-tr** *ttl* | **-ts** *ttl* | **-v** | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * **source** *source-address*

mtrace -r *receiver* [**-g** *group*] [[**-mr** | **-ur** *resp-dest*] | **-l** [*stat-times*] [**-st** *stat-int*] | **-m** *max-ttl* | **-q** *nqueries* | **-ts** *ttl* | **-tr** *ttl* | **-v** | **-w** *timeout* | **-vpn-instance** *vpn-instance-name*] * **source** *source-address*

Parameters

Parameter	Description	Value
-l	Performs Mtrace tracking for multiple times, collects traffic statistics and rate, uses detailed display mode, and ignores the configuration of **-v**.	If **-l** is not specified, Mtrace tracking is performed once.
stat-times	Indicates the number of times for Mtrace tracking.	The value is an integer that ranges from 2 to 65535. If **-l** is specified while *stat-times* is not specified, Mtrace tracking stops after it is performed 65535 times.
-st *stat-int*	Sets the interval at which the rate is calculated during cyclic query.	The value is an integer that ranges from 10 to 60, in seconds. The default value is 10. To configure **-st**, configure **-l** first. In addition, the cyclic count must be greater than or equal to 2.
-m *max-ttl*	Specifies the maximum number of hops to be traced.	The value is an integer that ranges from 1 to 255. The default value is 255.
-mr	Indicates that the response address is specified as the traced multicast group address.	The **-mr** is applicable only when the querier resides in a multicast distribution tree.
-q *nqueries*	Sets the number of retry times of mtrace.	The value is an integer that ranges from 1 to 65535. The default value is 3.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-tr *ttl*	Specifies the TTL value of the IGMP Tracert Response messages sent in multicast mode.	The value is an integer that ranges from 1 to 255. The default value is 30.
-ts *ttl*	Sets the maximum number of hops to be traced in hop-by-hop mode.	The value is an integer that ranges from 1 to 255. The default value is 30. When Mtrace in max-hop mode fails, Mtrace automatically enters the hop-by-hop mode. The number of hops increases by one each time a new hop is traced.
-ur *resp-dest*	Specifies the response address as a unicast address. The value of *resp-dest* must be a local interface address. **NOTE** If neither **-mr** nor **-ur** *resp-dest* is specified, multicast address 224.0.1.32 is used as the response address.	-
-v	Sets the detailed mode and exports time and statistics.	-
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
-w *timeout*	Specifies the timeout period to wait for an IGMP Tracert Response message.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 3.
-g *group*	Specifies the multicast group address to be traced.	The address cannot be a reserved group address.
-gw *last-hop-router*	Specifies the last-hop router address, which ensures that unicast packets can be transmitted between the querier and the last-hop router. After this parameter is specified, the initiating mode of Mtrace is specified as last-hop.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-d	Indicates that unicast packets can be transmitted between the querier and the destination host. After this parameter is specified, the initiating mode of Mtrace is specified as destination.	-
-r *receiver*	Specifies the destination host address.	The value is in dotted decimal notation.
-a *source-ip-address*	Specifies the source address of an IGMP Tracert Query message. The value of *source-ip-address* must be a local interface address. **NOTE** When you need to detect the multicast path or the RPF path from the multicast source to the querier, **-a** is not supported.	The value is in dotted decimal notation.
-b	Indicates that the querier is directly connected to the destination host, but whether the querier is the last-hop router is unknown. After this parameter is specified, the initiating mode of Mtrace is specified as all-router. **NOTE** After a VPN or RPF is specified, the initiating mode of Mtrace cannot be specified as all-router.	-
source *source-address*	Specifies the multicast source address.	The value is in dotted decimal notation.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

During multicast troubleshooting and routine maintenance, you can run the **mtrace** command to collect traffic information for locating faulty nodes, which helps reduce configuration errors, perform cyclic tracert, and collect statistics on multicast flow rates.

 Copyright © Huawei Technologies Co., Ltd.

The **mtrace** command format varies according to the types of paths.

- **mtrace source** *source-address*: detects the RPF path from the multicast source to the querier.
- **mtrace -g** *group* **source** *source-address*: detects the multicast path from the multicast source to the querier.

  The corresponding (S, G) entry must exist on the querier.
- **mtrace** [**-gw** *last-hop-router* | **-d**] **-r** *receiver* **source** *source-address*: detects the RPF path from the multicast source to the destination host.
  - The querier is directly connected to the destination host, or the querier can ping the last-hop router or detonation host in unicast mode.
  - When multiple routers are connected to the specified host, RPF paths from different routers can be different. You can specify the last-hop router using **-gw** *last-hop-router* to uniquely define an RPF path.
- **mtrace** [**-b** | **-gw** *last-hop-router* | **-d**] **-r** *receiver* **-g** *group* **source** *source-address*: detects the multicast path from the multicast source to the destination host.

  The corresponding (S, G) entry must exist on the querier. In addition, one of the following conditions must be met:
  - The querier is directly connected to the destination host.
  - The querier can ping the last-hop router or the destination host in unicast mode.
  - The querier resides in the multicast path from the multicast source to the destination host. For example, the querier is the first hop router.

When running the **mtrace** [**-b** | **-gw** *last-hop-router* | **-d**] **-r** *receiver* **-g** *group* **source** *source-address* command to detect the multicast path from a multicast source to a destination host, specify **-gw** *last-hop-router*, **-b** or **-d**, which helps implement tracking quickly and accurately.

- **-b**: indicates that the querier is directly connected to the destination host.
- **-gw** *last-hop-router*: specifies the last-hop router address. Unicast packets can be transmitted between the querier and the last-hop router.
- **-d**: indicates that unicast packets can be transmitted between the querier and the destination host.
- If none of the preceding three parameters are specified, Mtrace fails unless the querier resides in the multicast path from the multicast source to the destination host.

Precautions

According to the draft-fenner-traceroute-ipm-01, the Router Alert option needs to be carried in the IGMP Tracert Query messages that are sent to the destination address in unicast mode and in the IGMP Tracert Response messages that are replied in multicast mode. At present, however, manufacturers have no unified opinion on this issue. In Huawei AR, the Router Alert option is carried in a packet. If Huawei devices need to communicate with devices that do not support the Router Alert option, use **-gw** to specify the last hop address and **-ur** to specify the unicast response address in the command line.

The parameter **vpn-instance** is used on the PE to initiate a multicast VPN probe.

Example

- Detect the RPF path from a multicast source to the querier.

Detect the RPF path from the multicast source 10.1.0.1 to the querier 10.1.5.1.

```
<Huawei> mtrace source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace reverse path to source (10.1.0.1) according to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.5.1
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute finished.
```

- Detect the multicast path from a multicast source to the querier.

Detect the multicast path from the multicast source 10.1.0.1 to the querier 10.1.5.1. The group address is 225.0.0.1, the cyclic count is 2, and the interval at which the rate is calculated is 10s.

```
<Huawei> mtrace -g 225.0.0.1 -l 2 -st 10 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.5.1), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table
 In calculating-rate mode, current statistic times is: 1

 -1 10.1.5.1
   Incoming Interface Address: 10.1.5.1 Input packets rate: 0
   Outgoing Interface Address: 0.0.0.0 Output packets rate: 0xffffffff
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -2 10.1.2.1
   Incoming Interface Address: 10.1.2.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.5.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -3 10.1.0.1
   Incoming Interface Address: 10.1.0.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.2.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
 *********************************************************
  In calculating-rate mode, reach the demanded number of statistic,and multicast
  traceroute finished.
```

- Detect the RPF path from the multicast source to the destination host.

Detect the RPF path from the multicast source 10.1.0.1 to the destination host 10.1.6.4. The last hop address is 10.1.6.3, unicast packets can be transmitted, and the time and statistics are displayed in detail.

```
<Huawei> mtrace -gw 10.1.6.3 -r 10.1.6.4 -v source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace reverse path to source (10.1.0.1) according to RPF rules

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.6.4
 -1   10.1.5.1        1      PIM
   Incoming Interface Address: 10.1.5.1
   Outgoing Interface Address: 10.1.6.3
   Previous-Hop Router Address: 10.1.5.2
   Input packet count on incoming interface: 0
   Output packet count on outgoing interface: 0
   Total number of packets for this source-group pair: 0xffffffff
   Forwarding TTL: 1
   Forwarding Code: NO_ERROR
 -2   10.1.2.1        1      PIM
   Incoming Interface Address: 10.1.2.1
   Outgoing Interface Address: 10.1.5.2
```

```
  Previous-Hop Router Address: 10.1.2.2
  Input packet count on incoming interface: 0
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 0xffffffff
  Forwarding TTL: 1
  Forwarding Code: NO_ERROR
 -3   10.1.0.1        1      PIM
  Incoming Interface Address: 10.1.0.1
  Outgoing Interface Address: 10.1.2.2
  Previous-Hop Router Address: 0.0.0.0
  Input packet count on incoming interface: 0
  Output packet count on outgoing interface: 0
  Total number of packets for this source-group pair: 0xffffffff
  Forwarding TTL: 1
  Forwarding Code: NO_ERROR
 In maximum-hop mode, received the response message, and multicast traceroute finished.
```

- Detect the multicast path from the multicast source to the destination host.

Detect the multicast path from the multicast source 10.1.0.1 to the destination 225.0.0.1. The destination host address is 10.1.6.4, the querier is directly connected to the destination host, the response address is the default value 224.0.1.32, and the TTL value of a Response packet is 5.

```
<Huawei> mtrace -b -r 10.1.6.4 -g 225.0.0.1 -tr 5 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table

 Num  Reverse-Path    FwdTTL Protocol
  0   10.1.6.4
 -1   10.1.5.1        1      PIM
 -2   10.1.2.1        1      PIM
 -3   10.1.0.1        1      PIM
  In maximum-hop mode, received the response message, and multicast traceroute finished.
```

Detect the multicast path from the multicast source 10.1.0.1 to the destination 225.0.0.1. The destination host address is 10.1.6.4, the last hop address is 10.1.6.3, unicast packets are reachable, the number of cyclic times is 2, and the interval at which the rate is calculated is 12s.

```
<Huawei> mtrace -gw 10.1.6.3 -r 10.1.6.4 -g 225.0.0.1 -l 2 -st 12 source 10.1.0.1
 Press Ctrl+C to break multicast traceroute facility
 From the receiver(10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table
 In calculating-rate mode, current statistic times is: 1

 -1 10.1.5.1
   Incoming Interface Address: 10.1.5.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.6.3 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -2 10.1.2.1
   Incoming Interface Address: 10.1.2.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.5.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0

 -3 10.1.0.1
   Incoming Interface Address: 10.1.0.1 Input packets rate: 0
   Outgoing Interface Address: 10.1.2.2 Output packets rate: 0
   Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0
*********************************************************
 In calculating-rate mode, reach the demanded number of statistic, and multicast
traceroute finished.
```

Table 10-104 Description of the **mtrace** command output

Item	Description
Press Ctrl+C to break multicast traceroute facility	The ongoing Mtrace test is terminated after you press **Ctrl+C**.
From the receiver (10.1.6.4), trace reverse path to source (10.1.0.1) according to RPF rules	The RPF path from destination host 10.1.6.4 to multicast source 10.1.0.1 is detected.
From the receiver (10.1.6.4), trace (10.1.0.1, 225.0.0.1)'s reverse path according to multicast routing-table	The transmission path of multicast data (10.1.0.1, 225.0.0.1) from the destination host 10.1.6.4 to the source is tested.
Num	Number of traced hops.
Reverse-Path	Reverse path of multicast traffic.
FwdTTL	Minimum TTL value for multicast packet forwarding.
Protocol	Multicast routing protocol used on the router.
-1 10.1.5.1 1 PIM	The address of the last hop is 10.1.5.1, the minimum TTL value for multicast forwarding is 1, and the multicast routing protocol used on the router is PIM.
In calculating-rate mode, current statistic times is: 1	The rate is calculated for the first time in the calculating rate mode.
-1 10.1.5.1	Last hop with the address as 10.1.5.1 in calculating rate mode.
Incoming Interface Address: 10.1.5.1 Input packets rate: 0	Multicast inbound interface address and the inbound packet rate on the inbound interface in calculating rate mode.
Outgoing Interface Address: 0.0.0.0 Output packets rate: 0xffffffff	Multicast outbound interface address and the outbound packet rate on the outbound interface in calculating rate mode.
Forwarding Cache (10.1.0.1, 225.0.0.1) Forwarding packets rate: 0	Rate for a router to forward multicast packets of the (S, G) entry in calculating rate mode.
In maximum-hop mode, received the response message, and multicast traceroute finished.	IGMP Tracert Response messages are received in maximum hop tracking mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
In calculating-rate mode, reach the demanded number of statistic, and multicast traceroute finished.	Mtrace is complete in calculating rate mode when the required number of calculating times is reached.

10.7.16 mtrace query-policy

Function

The **mtrace query-policy** command enables a device to filter IGMP-Tracert-Query packets in unicast mode based on the source address of these packets.

The **undo mtrace query-policy** command cancels the filtering of IGMP-Tracert-Query packets.

By default, the router does not filter IGMP-Tracert-Query packets.

Format

mtrace query-policy [*basic-acl-number*]

undo mtrace query-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of the basic ACL. This ACL defines the address range of a trusted querier. According to this ACL, the last hop router rejects the IGMP-Tracert-Query packets sent by an invalid querier.	The value is an integer ranging from 2000 to 2999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The source address of IGMP-Tracert-Query packets in unicast mode is the local interface address. Before you create an ACL rule, create an ACL.

Run this command on the router that is connected to the host.

- This command takes effect only on the last hop router, which is not the querier.

 Copyright © Huawei Technologies Co., Ltd.

- This command filers only the IGMP-Tracert-Query packets encapsulated in unicast IP packets.
- This command is not applicable to the tracking initiated from the querier.

When you run the **mtrace query-policy** command on the last hop router, note the following points:

- If *basic-acl-number* is not specified, the last hop router does not reject IGMP-Tracert-Query packets in unicast mode.
- If *basic-acl-number* is specified but the ACL is not defined on the router, the last hop router rejects any IGMP-Tracert-Query packet in unicast mode.
- If *basic-acl-number* is specified and this ACL is defined on the router, only the IGMP-Tracert-Query packets allowed by the ACL can be received.

Example

Apply the querier filtering rules to the last hop router.

```
<Huawei> system-view
[Huawei] mtrace query-policy 2000
```

10.7.17 multicast boundary

Function

The **multicast boundary** command configures a multicast boundary for a single administrative range.

The **undo multicast boundary** command deletes the configured multicast boundary.

By default, no multicast boundary is configured on an interface.

Format

multicast boundary *group-address* { *mask* | *mask-length* }

undo multicast boundary { *group-address* { *mask* | *mask-length* } | **all** }

Parameters

Parameter	Description	Value
group-address	Specifies the address of a multicast group, used to specify a multicast group and configure the forwarding range of the multicast packets for the group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the mask of a specified group address.	The mask is in dotted decimal notation.
mask-length	Indicates the mask length of a specified group address.	The value is an integer that ranges from 4 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Deletes all the multicast boundaries configured on an interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Data of some multicast groups needs to be forwarded within a specified range. For example, each BSR administrative domain serves a specific group address range, and data packets sent from multicast sources to these groups need to be forwarded within the matching administrative domain. After a multicast boundary is configured for specified multicast groups on an interface, multicast packets sent to these groups cannot be forwarded through the interface. This restricts multicast forwarding within a range.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

To configure the boundary for different multicast groups, you can repeat the command on the same interface.

A and B are the forwarding boundary sets of the multicast group range to be configured, and B is a subset of A. If A is first configured on an interface, B cannot be configured. If you configure A on the interface that has been configured with B, B is replaced by A.

Example

Configure GE1/0/0 as the boundary of group 239.2.0.0/16.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary 239.2.0.0 16
```

Related Topics

10.7.8 display multicast boundary

10.7.18 multicast boundary policy

Function

The **multicast boundary policy** command configures an inbound and outbound multicast boundary policy on a specific interface.

The **undo multicast boundary policy** command cancels the configuration.

By default, no inbound and outbound multicast boundary policy is configured on an interface.

Format

multicast boundary policy *basic-acl-number* [**filter-autorp**]

undo multicast boundary policy *basic-acl-number* [**filter-autorp**]

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
filter-autorp	Filters Auto-RP messages received on the interface. If this parameter is not specified, whether Auto-RP messages received on the interface are filtered depends on the ACL specified in the command.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound and outbound multicast boundary policy

 Copyright © Huawei Technologies Co., Ltd.

has the functions of both an inbound multicast boundary policy and an outbound multicast boundary policy and filters auto-RP packets by multicast group address.

Configuration Impact

If you run the **multicast boundary policy** command several times, the latest configuration overrides the previous configurations.

Precautions

The **multicast boundary policy** command works with the **acl** command. The parameter **source** in the **rule** command in the ACL view can be used to specify a group address range for an inbound and outbound multicast boundary policy.

A multicast boundary policy and IGMP proxy are mutually exclusive on an interface.

NOTE

If the AR connects to a third-party device and needs to receive Auto-RP messages from the third-party device, you must configure a rule to allow packets with destination addresses 224.0.1.39 and 224.0.1.40 to pass in the ACL specified in the multicast boundary policy.

Example

Configure an inbound and outbound multicast boundary policy for multicast group 225.0.0.0 on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 225.0.0.0 0
[Huawei-acl-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary policy 2000
```

Related Topics

10.7.9 display multicast boundary policy

10.7.19 multicast boundary policy in

Function

The **multicast boundary policy in** command configures an inbound multicast boundary policy on a specific interface.

The **undo multicast boundary policy in** command cancels the configuration.

By default, no inbound multicast boundary policy is configured on an interface.

Format

multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **in**

undo multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **in**

Parameters

Parameter	Description	Value
acl-name *acl-name*	Specifies the name of a named ACL. Only named advanced ACLs are supported.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl-number	Specifies the number of an advanced ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound multicast boundary policy effectively controls sourcegroup-specific data packets that can enter the local domain. An inbound multicast boundary filters multicast data packets received by an interface and PIM JoinPrune and IGMP Report messages to be sent by the interface to control multicast data direction and reception on the protocol control and forwarding planes.

Configuration Impact

If you run the **multicast boundary policy in** command several times, the latest configuration overrides the previous configurations.

Precautions

The **multicast boundary policy in** command works with the **acl** command.

- The parameter **source** in the **rule** command in the view of a numbered basic ACL can be used to specify a group address range for an inbound multicast boundary policy.
- The parameter **source** in the **rule** command in the view of a numbered advanced ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

- A named ACL uses the same rules as a numbered advanced ACL. The parameter **source** in the **rule** command in the ACL view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

A multicast boundary policy and IGMP proxy are mutually exclusive on an interface.

NOTE

If the AR connects to a third-party device and needs to receive Auto-RP messages from the third-party device, you must configure a rule to allow packets with destination addresses 224.0.1.39 and 224.0.1.40 to pass in the ACL specified in the multicast boundary policy.

Example

Use a numbered basic ACL to configure an inbound multicast boundary policy for multicast group 225.0.0.0 on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 225.0.0.0 0
[Huawei-acl-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary policy 2000 in
```

Related Topics

10.7.9 display multicast boundary policy

10.7.20 multicast boundary policy out

Function

The **multicast boundary policy out** command configures an outbound multicast boundary policy on a specific interface.

The **undo multicast boundary policy out** command cancels the configuration.

By default, no outbound multicast boundary policy is configured on an interface.

Format

multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **out**

undo multicast boundary policy { **acl-name** *acl-name* | *basic-acl-number* | *advanced-acl-number* } **out**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-name *acl-name*	Specifies the name of a named ACL. Only named advanced ACLs are supported.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl-number	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl-number	Specifies the number of an advanced ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to defined multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. Outbound multicast boundary policy effectively controls data packets that can be sent out of the local domain. An interface on which an outbound multicast boundary policy is configured filters received PIM JoinPrune messages, and IGMP Report messages and controls the generation of downstream interface lists of entries.

Configuration Impact

If you run the **multicast boundary policy out** command several times, the latest configuration overrides the previous configurations.

Precautions

The **multicast boundary policy out** command works together with the **acl** command.

- The **source** parameter in the **rule** command in the view of a numbered basic ACL can be used to specify a group address range for an outbound multicast boundary policy.
- The parameter **source** in the **rule** command in the view of a numbered advanced ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

- A named ACL uses the same rules as a numbered advanced ACL. The parameter **source** in the **rule** command in the ACL view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.

A multicast boundary policy and IGMP proxy are mutually exclusive on an interface.

Example

Configure an outbound multicast boundary policy for multicast group 225.0.0.0 on GigabitEthernet 1/0/0.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule permit source 225.0.0.0 0
[Huawei-acl-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast boundary policy 2000 out
```

Related Topics

10.7.9 display multicast boundary policy

10.7.21 multicast forwarding-table downstream-limit

Function

The **multicast forwarding-table downstream-limit** command sets the maximum number of downstream nodes of an entry in the multicast forwarding table.

The **undo multicast forwarding-table downstream-limit** command restores the default setting.

By default, the maximum number of downstream nodes of an entry is 128.

Format

multicast forwarding-table downstream-limit *limit*

undo multicast forwarding-table downstream-limit

Parameters

Parameter	Description	Value
limit	Indicates the maximum number of downstream nodes of an entry in the forwarding table.	The value is an integer that ranges from: 0 to 128.

Views

System view, VPN instance view, VPN IPv4 address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the router receives a multicast packet, it copies the packet for each downstream node in the matching multicast forwarding entry. If the router has a large number of multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the loads of the router, limit the maximum number of downstream nodes in each multicast forwarding entry.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

If the configured number is smaller than the current number, the excessive downstream nodes are not deleted immediately, and must be deleted by the multicast routing protocol. In addition, no new downstream node can be added to the entry in the forwarding table.

Example

Set the maximum number of downstream nodes of an entry in the forwarding table to 32 in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast forwarding-table downstream-limit 32
```

Related Topics

10.7.10 display multicast forwarding-table

10.7.22 multicast forwarding-table route-limit

Function

The **multicast forwarding-table route-limit** command sets the limit on the number of entries in the multicast forwarding table.

The **undo multicast forwarding-table route-limit** command restores the default value of the limit.

By default, the limit on the number of entries in the multicast forwarding table varies according to device models:

- AR150&AR200 series: 64
- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128

 Copyright © Huawei Technologies Co., Ltd.

- AR100&AR120&AR160&AR1200 series, AR2220, AR2220L, AR2220E, AR2240C: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100E: 2000
  - Configured with SRU200: 3000
  - Configured with SRU200E: 3000
  - Configured with SRU400: 4000
- AR3600 series (SRUX5): 3000

Format

multicast forwarding-table route-limit *limit*

undo multicast forwarding-table route-limit

Parameters

Parameter	Description	Value
limit	Specifies the limit on the number of entries in the multicast forwarding table.	The value is an integer that ranges from ● 0 to 64 for the AR150&AR200 series ● 0 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 ● 0 to 1000 for the AR100&AR120&AR160&AR1200 series, AR2220E, AR2240C, AR2220 ● 0 to 2000 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series: – Configured with SRU40: 0 to 1000 – Configured with SRU60: 0 to 1000 – Configured with SRU80: 0 to 2000 – Configured with SRU100: 0 to 2000 – Configured with SRU100E: 0 to 2000 – Configured with SRU200: 0 to 3000 – Configured with SRU200E: 0 to 3000 – Configured with SRU400: 0 to 4000 ● 1 to 3000 for the AR3600 series (SRUX5)

 Copyright © Huawei Technologies Co., Ltd.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Excessive multicast forwarding entries will exhaust the memory of the router. To prevent this problem, use the **multicast forwarding-table route-limit** command to limit the number of entries in the multicast forwarding table.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

NOTICE

If the limit on the number of entries in the multicast forwarding table is set after multicast services are deployed on a router, ensure that the limit on the number of entries in the multicast forwarding table is equal to or greater than the number of current forwarding entries. Otherwise, faults may occur.

You are recommended to limit the number of entries in the multicast forwarding table according to the actual network environment before the router operates multicast services.

If the newly-configured limit on the number of entries are less than the number of existing entries, the excessive entries are not deleted immediately. The configured limit on the number of entries takes effect in the following cases:

- Entries are added to the multicast forwarding table after the existing entries age out.
- The **reset multicast forwarding-table all** command is run.

Example

Set the limit on the number of the entries in the forwarding table of the public network instance to 60.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast forwarding-table route-limit 60
```

Related Topics

10.7.10 display multicast forwarding-table

10.7.31 reset multicast forwarding-table

 Copyright © Huawei Technologies Co., Ltd.

10.7.23 multicast invalid-packet

Function

The **multicast invalid-packet** command sets the maximum number of invalid multicast protocol packets that can be stored on the router.

The **undo multicast invalid-packet** command deletes the set maximum number of invalid multicast protocol packets that can be stored on the router.

By default, the router can save a maximum of 10 invalid packets for each specific multicast protocol.

Format

multicast invalid-packet { **igmp** | **msdp** | **pim** } **max-count** *max-number*

undo multicast invalid-packet { **igmp** | **msdp** | **pim** }

Parameters

Parameter	Description	Value
igmp	Sets the maximum number of invalid IGMP messages.	-
msdp	Sets the maximum number of invalid MSDP messages.	-
pim	Sets the maximum number of invalid PIM messages.	-
max-count *max-number*	Sets the maximum number of invalid multicast protocol packets that can be stored on a device.	The value is an integer ranging from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If multicast entries fail to be generated or peer relationships fail to be set up, you can enable the router to store invalid multicast protocol packets and view statistics and details of the invalid multicast protocol packets. Based on the command output, you can locate and rectify faults.

Example

Set the maximum number of invalid IGMP messages that can be stored on the router to 20.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast invalid-packet igmp max-count 20
```

Related Topics

10.1.8 display igmp invalid-packet

10.5.5 display msdp invalid-packet

10.3.27 display pim invalid-packet

10.7.24 multicast load-splitting

Function

The **multicast load-splitting** command enables load splitting among multicast routes.

The **undo multicast load-splitting** command restores the default configuration.

By default, load splitting among multicast routes is disabled.

Format

multicast load-splitting { **balance-preferred** | **stable-preferred** | **group** | **source** | **source-group** }

undo multicast load-splitting

Parameters

Parameter	Description	Value
balance-preferred	Indicates balance-preferred load splitting. This policy is applicable to the scenario where hosts frequently join or leave groups, which requires automatic load adjustment.	-
stable-preferred	Indicates stable-preferred load splitting. This policy is applicable to stable multicast networking.	-
group	Indicates group address-based load splitting. This policy is applicable to the scenario of one source to multiple groups.	-
source	Indicates source address-based load splitting. This policy is applicable to the scenario of multiple sources to one group.	-
source-group	Indicates source and group addresses-based load splitting. This policy is applicable to the scenario of multiple sources to multiple groups.	-

Views

System view, VPN instance view, VPN IPv4 address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if there are multiple equal-cost routes to a multicast source, the router applies the following route selection rules during RPF check:

- If the equal-cost routes are in the same routing table, for example, unicast routing table, multicast static routing table, or MBGP routing table, the router selects the route with the largest next-hop address as the RPF route.
- If the equal-cost routes are in different routing tables, the router selects the route with the highest preference. If the routes have the same preference, the router selects the route with the longest mask length. If the routes have the same preference and mask length, the router uses certain algorithm to select a route as the RPF route.

No matter which rule is used, the router selects only one route as the RPF route. To enable multicast data to be forwarded through multiple paths, run the **multicast load-splitting** command to configure multicast load splitting. After multicast load splitting is configured, the router uses the specified load splitting policy to distribute multicast data among multiple paths. This function improves quality of multicast forwarding.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Follow-up Procedure

Because the forwarding capabilities of equal-cost routes are different from the actual load distribution situation on the equal-cost routes, even load splitting cannot meet network requirements in some scenarios. Then, you can run the **multicast load-splitting weight** command to configure the multicast load splitting weight on the interface to realize unbalanced load splitting.

Precautions

The five load splitting policies are mutually exclusive. It is recommended that you use a fixed load splitting policy based on the actual situation on your network. The **balance-preferred** or **stable-preferred** policy is preferred.

If PIM-DM is enabled on the router, the **balance-preferred** or **stable-preferred** policy cannot be used.

Example

Configure group address-based load splitting in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast load-splitting group
```

Related Topics

10.7.26 multicast load-splitting-timer
10.7.25 multicast load-splitting weight

10.7.25 multicast load-splitting weight

Function

The **multicast load-splitting weight** command sets the multicast load splitting weight for an interface.

The **undo multicast load-splitting weight** command restores the default setting.

By default, the multicast load splitting weight of an interface is 1.

Format

multicast load-splitting weight *weight-value*

undo multicast load-splitting weight

Parameters

Parameter	Description	Value
weight-value	Specifies the multicast load splitting weight of an interface.	The value is an integer that ranges from 0 to 32.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stable-preferred or balance-preferred multicast splitting policy is configured, you can run this command to set load splitting weights for interfaces to realize unbalanced load splitting. An interface with a larger weight value has more multicast routing entries with it as the upstream interface.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Precautions

This command is applicable only when the multicast load splitting policy is set to stable-preferred or balance-preferred.

 Copyright © Huawei Technologies Co., Ltd.

When the multicast load splitting weight on an interface is 0, the routes with this interface as the upstream interface do not take part in load splitting.

Example

Set the multicast load splitting weight on GE1/0/0 to 10.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] interface gigabitethernet  1/0/0
[Huawei-GigabitEthernet1/0/0] multicast load-splitting weight 10
```

Related Topics

10.7.24 multicast load-splitting

10.7.26 multicast load-splitting-timer

Function

The **multicast load-splitting-timer** command sets a load splitting timer.

The **undo multicast load-splitting-timer** command restores the default setting.

By default, the value of a load splitting timer is 1800 seconds.

Format

multicast load-splitting-timer *interval*

undo multicast load-splitting-timer

Parameters

Parameter	Description	Value
interval	Specifies the value of the load splitting timer.	The value is an integer ranging from 10 to 1800, in seconds.

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In stable-preferred load splitting or balance-preferred load splitting mode, entries may not be well-balanced among paths because of the addition or deletion of entries, change of load splitting weights of the paths, or change of equal-cost routes. In such a case, the device will balance entries after a certain waiting time to reduce the impact of frequent changes on the system.

 Copyright © Huawei Technologies Co., Ltd.

Currently, setting a load splitting timer to change the waiting time before balancing entries is supported.

- If the network is relatively stable, such as when entries are not deleted or added frequently or equal-cost routes are not changed frequently, set the load splitting timer value to a smaller value so that entries can be balanced rapidly. The recommended value is 300 to 600 seconds.
- If the network is not stable, such as when entries are deleted or added frequently or equal-cost routes are changed frequently, set the load splitting timer value to a greater value to reduce the impact of frequent entry changes on the system and network stability. The recommended value is 1200 to 1800 seconds.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Set a load splitting timer to 100 seconds.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast load-splitting-timer 100
```

Related Topics

10.7.24 multicast load-splitting

10.7.27 multicast longest-match

Function

The **multicast longest-match** command configures the router to select the RPF route based on the longest matching rule.

The **undo multicast longest-match** command restores the default configuration.

By default, the router selects the route with the highest preference as the RPF route.

Format

multicast longest-match

undo multicast longest-match

Parameters

None

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the router selects the RPF route based on route preference. This command changes the route selection policy used by the router during RPF check. After you run this command, the router selects the RPF route with the longest mask. If multiple routes have the same mask length, the router selects the route with the highest preference.

Prerequisites

IP multicast routing has been enabled using the **multicast routing-enable** command in the public network instance or VPN instance.

Example

Select routes according to the longest match in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
[Huawei] multicast longest-match
```

10.7.28 multicast routing-enable

Function

The **multicast routing-enable** command enables the multicast routing function.

The **undo multicast routing-enable** command restores the default configuration.

By default, the multicast routing function is disabled.

Format

multicast routing-enable

undo multicast routing-enable

Parameters

None

Views

System view, VPN instance view, VPN IPv4 address family view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Before configuring Layer 3 multicast, you must enable the multicast routing function globally. Layer 3 multicast protocols (such as PIM and IGMP) and other Layer 3 multicast functions can be configured only after multicast routing is enabled.

Precautions

NOTICE

The **undo multicast routing-enable** command deletes all multicast configurations of the public network instance or a VPN instance. If multicast services are running in the instance, the multicast services are interrupted when this command is executed. To restore multicast services on the instance, you must re-configure the corresponding commands.

Example

Enable multicast routing in the public network instance.

```
<Huawei> system-view
[Huawei] multicast routing-enable
```

Related Topics

10.1.15 igmp enable

10.3.50 pim dm

10.3.62 pim sm

10.5.12 msdp

10.7.29 ping multicast

Function

The **ping multicast** command enables a device to detect the reserved members in the network segment, simulates the common group traffic, triggers the establishment of a distribution tree, and checks whether the network can normally bear multicast services.

Format

ping multicast [**-c** *count* | **-h** *ttl-value* | **-i** *interface-type interface-number* | **-m** *time* | **-p** *pattern* | **-q** | **-s** *packetsize* | **-t** *timeout* | **-tos** *tos-value* | **-v**] * *host*

Parameters

Parameter	Description	Value
-c *count*	Specifies the number of times for sending ICMP Echo Request messages.	The value is an integer that ranges from 1 to 65535. The default value is 5.
-h *ttl-value*	Sets the TTL value of an ICMP Echo Request message.	The value is an integer that ranges from 1 to 255. The default value is 255.
-i *interface-type interface-number*	Sets the outgoing interface that sends ICMP Echo Request messages. ● When the Mping destination group address is a reserved multicast group address, **-i** must be specified. ● When the Mping destination group address is a common multicast group address, **-i** cannot be specified.	-
-m *time*	Specifies the time to wait before sending the next ICMP Echo Request message. Each time the source sends an ICMP Echo Request message using the **ping multicast** command, the source waits a period of time (2000 ms by default) before sending the next ICMP Echo Request message. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-p *pattern*	Specifies the padding byte of ICMP Echo Request messages. After the padding byte of the ICMP Echo Request message is set, the destination host can identify a certain ICMP Echo Reply message.	The value ranges from 0 to FFFFFFFF, in the hexadecimal format. By default, the padding starts from 0x01, and continues in ascending order.
-q	Indicates that only statistics are displayed. When **-q** is specified in the **ping multicast** command, only the number of sent and received packets, packet loss rate, and the minimum, average, and maximum RTTs are displayed.	By default, all information is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-s *packetsize*	Sets the length of an ICMP Echo Request message, excluding the IP or ICMP header.	The value is an integer that ranges from 20 to 8100, in bytes. The default value is 56.
-t *timeout*	Specifies the timeout period to wait for an ICMP Echo Reply message after an ICMP Echo Request message is sent. After the **ping multicast** command is run, the source sends an ICMP Echo Request message to a destination and waits for an ICMP Echo Reply message. If the destination, after receiving the ICMP Echo Request message, returns an ICMP Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMP Echo Reply message within the specified period, the source displays information indicating that the message times out. Normally, the source receives an ICMP Echo Reply message within 1 to 10 seconds after sending an ICMP Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-tos *tos-value*	Specifies the ToS value of the sent ICMP Echo Request messages.	The value is an integer that ranges from 0 to 255. The default value is 196.
-v	Displays all received ICMP Echo Reply messages. ● If **-v** is not specified, the system displays the received ICMP Echo Reply messages of the user. ● If **-v** is specified, the system displays all received ICMP Echo Reply messages.	By default, only ICMP Echo Reply messages of the user are displayed.
host	Specifies the destination address of an ICMP Echo Request message, also called the Mping destination group address.	It includes reserved group addresses and common group addresses.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping multicast** command is used to check a multicast network in the following scenarios:

Scenario 1: When configuring the destination group address *host* as a reserved group address, you can run the **ping multicast** command to check which reserved multicast members reside on the network segment of the outbound interface. In this scenario, the TTL of an ICMP Echo Request message cannot be set.

The reserved multicast group identifies a group of network devices (reserved multicast members) that match certain conditions. When the reserved multicast members receive ICMP Echo Request messages with the destination addresses as the reserved group addresses, they return ICMP Echo Reply messages. Common reserved group addresses are as follows:

- 224.0.0.1: indicates all systems in the subnet.
- 224.0.0.2: indicates all routers in the subnet.
- 224.0.0.5: indicates OSPF IGP routers.
- 224.0.0.13: indicates PIM routers.

NOTE

In this scenario, **-i** must be specified in the **ping multicast** command.

Scenario 2: When setting the destination group address *host* as a common group address, you can run the **ping multicast** command to implement the following functions:

- Simulates the multicast traffic and triggers a series of protocol processes. By viewing the multicast routing information on the router, check whether the protocol running status is normal and whether the multicast distribution tree is correctly established.
- Check multicast members in the network and calculate the TTL value and the RTT from the Mping initiator to multicast members. This function requires that the host support Mping and is implemented by calculating the number of ICMP Echo Reply messages sent by the destination host. Mping is performed continuously at a certain interval to calculate the network delay and route jitter.

NOTE

In this scenario, **-i** cannot be specified in the **ping multicast** command.

You can specify different parameters in **ping multicast** command for different scenarios:

- On an unstable network, you can run the **ping multicast -c** *count* **-t** *timeout host* command to check the quality of the multicast network. By analyzing

the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.

- You can run the **ping multicast -s** *packetsize host* to set the size of a multicast probe packet. In this way, you can check the quality of the multicast network by simulating real service datagrams. The path MTU is then obtained through multiple probes.

Prerequisites

Before running the **ping multicast** command, ensure that the ICMP module is working properly.

Configuration Impact

If an intermediate device is disabled from responding to ICMP messages, detection on this node fails.

Precautions

If a fault occurs in the Mping process, you can press **Ctrl+C** to terminate the Mping operation.

Example

Perform Mping, specify the reserved multicast group address as 224.0.0.5 and the outbound interface as GE1/0/0, and detect the OSPF IGP router in the network segment.

```
<Huawei> ping multicast -i gigabitethernet 1/0/0 224.0.0.5
MULTICAST PING 224.0.0.5 : 56 data bytes, press Ctrl+C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 TTL =255 time=30ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 TTL =255 time=20ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 TTL =255 time=10ms
Destination multicast address 224.0.0.5
--- Multicast ping statistics ---
5 Request packet(s) transmitted
5 Reply packet(s) received
0.00% packet loss
Round-trip min/avg/max = 10/16/40 ms
```

Specify the padding field of **-p**.

```
<Huawei> ping multicast -i gigabitethernet 1/0/0 -p 12345678 224.0.0.5
MULTICAST PING 224.0.0.5 : 56 data bytes, press Ctrl+C to break
The padding string: 12345678
Reply from 10.1.1.5 : bytes=56 Sequence=1 TTL =255 time=30ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 TTL =255 time=10ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 TTL =255 time=20ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 TTL =255 time=10ms
Destination multicast address 224.0.0.5
--- Multicast ping statistics ---
5 Request packet(s) transmitted
5 Reply packet(s) received
0.00% packet loss
Round-trip min/avg/max = 10/16/40 ms
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-105 Description of the ping multicast command output

Item	Description
MULTICAST PING 224.0.0.5	The destination group address of Mping is 224.0.0.5.
56 data bytes	The length of the sent ICMP Echo Request message is 56 bytes.
press Ctrl+C to break	The ongoing Mtrace test is terminated after you press **Ctrl+C**.
The padding string: 12345678	The padding string is 12345678. If **-p** is not specified, the padding character string is not displayed.
Reply from 10.1.1.5: bytes=56 Sequence=1 TTL=255 time=30ms	The ICMP Echo Reply message sent from 10.1.1.5 is received. The message carries the following information: ● bytes=56: indicates the length of the ICMP Echo Reply message. ● Sequence=1: indicates the sequence number of the ICMP Echo Reply message. ● TTL=255: indicates the TTL value of the ICMP Echo Reply message. ● time=30ms: indicates the RTT, in milliseconds. If no ICMP Echo Reply message is received after the timeout period, "Request time out" is displayed.
Destination multicast address 224.0.0.5	The destination group address is 224.0.0.5.
--- Multicast ping statistics --- 5 Request packet(s) transmitted 5 Reply packet(s) received 0.00% packet loss Round-trip min/avg/max = 10/16/40 ms	Statistics collected after the Ping test on the destination host. The statistics are as follows: ● Number of sent ICMP Echo Request messages: 5 ● Number of received ICMP Echo Reply messages: 5 ● Percentage of non-Reply messages against total sent messages: 0.00% ● The minimum RTT is 10 ms, the average RTT is 16 ms, and the maximum RTT is 40 ms.

10.7.30 reset mtrace statistics

Function

The **reset mtrace statistics** command clears statistics about Mtrace packets.

Format

reset mtrace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

To collect statistics about Mtrace traffic generated in a certain period, reset the original statistics.

Example

Clear statistics about the current Mtrace traffic.

```
<Huawei> reset mtrace statistics
```

Related Topics

10.7.7 display mtrace statistics

10.7.31 reset multicast forwarding-table

Function

The **reset multicast forwarding-table** command clears the entries of the multicast forwarding table.

Format

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table all**

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* indicates the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-
all	Indicates all forwarding entries of multicast forwarding tables.	-
group-address	Specifies the address of a multicast group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Specifies the mask of a multicast group address or source address.	-
group-mask	Specifies the address mask of a multicast group.	The address mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the address of a multicast source.	The address is in dotted decimal notation.
source-mask	Specifies the address mask of a multicast source.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.
incoming-interface	Indicates the upstream interface of the forwarding entry.	-
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
register	Indicates the register interface in PIM-SM.	-

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the multicast forwarding table, multicast data will be interrupted for a period. Confirm the action before you use the command.

Example

Delete the multicast forwarding entries of the group 225.5.4.3 from the forwarding table in the public network instance.

```
<Huawei> reset multicast forwarding-table 225.5.4.3
```

Related Topics

10.7.10 display multicast forwarding-table

10.7.32 reset multicast routing-table

Function

The **reset multicast routing-table** command clears the entries in the multicast routing table. The corresponding forwarding entries in the forwarding table are deleted at the same time.

Format

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table all**

reset multicast [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** { *group-address* [**mask** { *group-mask* | *group-mask-length* }] | *source-address* [**mask** { *source-mask* | *source-mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies a VPN instance. *vpn-instance-name* indicates the name of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all-instance	Indicates all the instances.	-
all	Indicates all entries in the multicast routing table.	-
group-address	Specifies the address of the specified group.	The address is in dotted decimal notation and ranges from 224.0.1.0 to 239.255.255.255.
mask	Indicates the address mask of a multicast group or source.	-
group-mask	Specifies the address mask of a multicast group.	The address mask is in dotted decimal notation.
group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the address of a specified source.	The address is in dotted decimal notation.
source-mask	Specifies the address mask of a multicast source, in dotted decimal notation.	The address mask is in dotted decimal notation.
source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 32.
incoming-interface	Specifies the incoming interface of a multicast entry.	-
interface-type interface-number	Specifies the type and the number of an interface, used to specify an interface.	-
register	Indicates the register interface of PIM-SM.	-

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

NOTICE

After you run this command to delete information from the multicast routing table, the matching entries in the multicast forwarding table are also deleted. As a result, multicast forwarding will be interrupted for a period. Confirm the action before you use the command.

Example

Delete the entries of the group 225.5.4.3 from the multicast routing table of the public network instance.

```
<Huawei> reset multicast routing-table 225.5.4.3
```

Related Topics

10.7.11 display multicast routing-table
10.7.10 display multicast forwarding-table

10.8 Multicast Route Management (IPv6) Commands

10.8.1 display multicast ipv6 boundary

Function

The **display multicast ipv6 boundary** command displays the multicast boundary configured on an interface.

Format

display multicast ipv6 boundary [*ipv6-group-address ipv6-group-mask-length* | **scope** *scope-id*] [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address to display the corresponding multicast routing table.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of the IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
scope *scope-id*	Specifies a scope ID.	The value is an integer that ranges from 3 to 15.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to check the boundary of a PIM-SM (IPv6) network. When some hosts cannot receive multicast data, you can use this command to check whether the problem is caused by multicast boundary configuration.

Example

Display the boundaries configured on all the interfaces.

```
<Huawei> display multicast ipv6 boundary
IPv6 multicast boundary information
Total 1 Multicast IPv6 boundary
 Interface          Boundary
 GE1/0/0             FF02::/64
```

Table 10-106 Description of the display multicast ipv6 boundary command output

Item	Description
IPv6 multicast boundary information	IPv6 multicast boundary.
Total 1 Multicast IPv6 boundary	Total number of IPv6 multicast boundaries.
Interface	Name of the interface configured with multicast boundary.
Boundary	Multicast group with the interface as the boundary.

Related Topics

10.8.6 multicast ipv6 boundary

10.8.2 display multicast ipv6 boundary policy

Function

The **display multicast ipv6 boundary policy** command displays information about IPv6 multicast boundary policies.

Format

display multicast ipv6 boundary policy [*ipv6-group-address ipv6-source-address* | **interface** *interface-type interface-number*] *

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies an IPv6 multicast group address.	The value ranges from FF00::0 to FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF, in hexadecimal notation.
ipv6-source-address	Specifies an IPv6 multicast source address.	The value is in dotted decimal notation. If the multicast source address is 0::0 in an entry, the entry is a (*, G) entry.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast forwarding boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. The **display ipv6 multicast boundary policy** command can be used to view information about multicast boundary policies.

Precautions

When using the **display multicast ipv6 boundary policy** command, note the following points:

 Copyright © Huawei Technologies Co., Ltd.

- If *ipv6-group-address ipv6-source-address* is specified, information about the IPv6 multicast boundary policy that filters packets based on source and group addresses on each interface is displayed.
- If **interface** *interface-type interface-number* is specified, information about the IPv6 multicast boundary on a specific interface is displayed.

Example

Display information about IPv6 multicast boundaries on the router.

```
<Huawei> display multicast ipv6 boundary policy
Direction Flags: I - in, O - out
-----------------------------------------------------------------------
IPv6 multicast boundary policy information
Total 1 multicast IPv6 boundary policy
 Interface            Boundary policy     Direction           Result
 GE1/0/0                  2000                I O                --
```

Display information about an IPv6 multicast boundary policy for (2000::2000, ff1e::1) and packet filtering results on the router.

```
<Huawei> display multicast ipv6 boundary policy ff1e::1 2000::2000
Direction Flags: I - in, O - out
IPv6 multicast boundary policy information
Total 1 multicast IPv6 boundary policy
 Interface            Boundary policy     Direction           Result
 GE1/0/0                  2000                I O              Block
```

Table 10-107 Description of the **display multicast ipv6 boundary policy** command output

Item	Description
Direction Flags	Flag indicating the direction in which a multicast boundary policy takes effect: ● I: inbound direction ● O: outbound direction
IPv6 multicast boundary policy information	Information about an IPv6 multicast boundary policy
Total 1 multicast IPv6 boundary policy	Total number of multicast boundary policies configured on the router
Interface	Interface on which a multicast boundary is configured
Boundary policy	IPv6 multicast boundary policy on an interface
Direction	Flag indicating the direction in which a multicast boundary policy takes effect: ● I: inbound direction ● O: outbound direction

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Result	Whether a multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface: ● Block: indicates that a multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. ● Unblock: indicates that no multicast forwarding boundary is configured in a specific direction for a specific multicast source and group on a specific interface. ● --: indicates that the source and multicast addresses are not identified.

Related Topics

10.8.7 multicast ipv6 boundary policy

10.8.8 multicast ipv6 boundary policy in

10.8.9 multicast ipv6 boundary policy out

10.8.3 display multicast ipv6 forwarding-table

Function

The **display multicast ipv6 forwarding-table** command displays the IPv6 multicast forwarding table.

Format

display multicast ipv6 forwarding-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** | **none** } } | { **statistics** | **verbose** }] *

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-source-mask-length	Specifies the mask length of the multicast source address.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 8 to 128.
incoming-interface	Indicates the incoming interface of an IPv6 multicast forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of PIM-SM.	-
outgoing-interface	Indicates the outgoing interface of an IPv6 multicast forwarding entry.	-
exclude	Indicates that the downstream interface list does not contain the route forwarding entries of a specified interface.	-
include	Indicates that the downstream interface list contains the route forwarding entries of a specified interface.	-
match	Indicates that the downstream interface list matches the route forwarding entries of a specified interface.	The downstream interface list contains only one eligible interface. After **match** is configured, the route forwarding entries of a null downstream interface list are displayed if the outgoing interface is not specified.
none	Displays the (S, G) entry without a downstream interface.	-
statistics	Displays the statistics of the multicast forwarding table.	-
verbose	Displays detailed information about forwarding entries.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During IPv6 multicast routing and forwarding, routing information generated by IPv6 multicast routing protocols is saved in an IPv6 multicast routing table. The router selects the optimal multicast routes from the routing table according to multicast routing and forwarding policies, and then delivers the selected multicast routes to the IPv6 multicast forwarding table to guide multicast data forwarding.

You can use the **display multicast ipv6 forwarding-table** command to check whether IPv6 multicast forwarding entries have been generated and whether multicast data can be forwarded normally.

Example

Display the IPv6 multicast forwarding table.

```
<Huawei> display multicast ipv6 forwarding-table
IPv6 Multicast Forwarding Table
Total 2 entries, 2 matched

00001. (FC00:AA::123, FF33::)
    MID: 0, Flags: ACT
    Uptime: 00:01:03, Timeout in: 00:02:27
    Incoming interface: GigabitEthernet1/0/0
    List of 1 outgoing interfaces:
      1: LoopBack0
        Activetime: 00:23:15
    Matched 0 packets(0 bytes), Wrong If 0 packets
    Forwarded 0 packets(0 bytes)

00002. (FC00:AA::123, FF34::)
    MID: 1, Flags: ACT
    Uptime: 00:00:03, Timeout in: 00:03:27
    Incoming interface: GigabitEthernet2/0/0
    List of 1 outgoing interfaces:
      1: LoopBack0
        Activetime: 00:23:15
    Matched 0 packets(0 bytes), Wrong If 0 packets
    Forwarded 0 packets(0 bytes)
```

Table 10-108 Description of the **display multicast ipv6 forwarding-table** command output

Item	Description
IPv6 Multicast Forwarding Table	IPv6 multicast forwarding table.
Total 2 entries, 2 matched	Total forwarding entries and total eligible forwarding entries.
00001	Number of the (S, G) entry.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
(FC00:AA::123, FF33::)	(S, G) entry in the multicast routing table.
MID	Unique multicast forwarding entry in the MFIB table. MID is used to rapidly search the multicast forwarding table.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Flags	Status flag of the (S, G) entry. ● ACT: indicates that an active event is triggered. ● DUM: indicates a dummy entry. ● MISS: indicates that the nocache time needs to be reported. ● DROP: indicates packet dropping. ● LTH: indicates that the traffic volume is below the threshold. ● DEL: indicates a deleted entry. ● RST: indicates that registration of the known timer is started. ● 2IODEL: indicates that an entry is deleted from the MFIB table, and the update needs to be synchronized to the IO board. ● 2PDEL: indicates that an entry is deleted from the device, and the update needs to be synchronized to the IO board. ● 2SYNC: indicates that the entry is contained in the MFIB table but it does not exist on the device. ● 2ADD: indicates that the entry existing on the device has not been added to the MFIB table. ● CLR: indicates that the MFIB table is resetting. ● L2FWD: indicates that the device forwards Layer 2 traffic in multicast mode. ● NORPF: indicates that the device does not perform RPF check. ● 2ACK: indicates that the VPN instance is waiting for the ACK message from the slave main control board. ● 2RSED: indicates that the entry is waiting for retransmission. ● IOACK: indicates that the VPN instance has received the ACK message from the LPU. ● SACK: indicates that the VPN instance has received the ACK message forwarded by software.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• BKCLR: indicates that the MFIB table on the slave main control board is resetting. • EXTR: indicates an extranet entry. • 2DEL: indicates that the entry deleted from the device has not been removed from the MFIB table. • PDEL: indicates that the entry does not exist on the device. • A denotes addition; D denotes deletion; I denotes upstream update; R denotes RP update; P denotes PMBR; F denotes flag. • S denotes SPT; E denotes encapsulation group update; US denotes status update; CS denotes status clearing.
Uptime	Period during which the (S, G) entry exists.
Timeout in	Remaining time of the (S, G) entry.
Incoming interface	Incoming interface of the (S, G) entry.
List of 1 outgoing interfaces: 1: LoopBack0	Outgoing interface list, including the outgoing interface number and name.
Activetime	Existing time of the outgoing interface of the (S, G) entry.
Matched 0 packets(0 bytes)	Number of multicast packets and bytes that match the (S, G) entry.
Wrong If 0 packets	Number of packets with an incorrect incoming interface.
Forwarded 0 packets(0 bytes)	Number of packets and bytes forwarded by the (S, G) entry.

Related Topics

10.8.10 multicast ipv6 forwarding-table downstream-limit
10.8.11 multicast ipv6 forwarding-table route-limit
10.8.4 display multicast ipv6 routing-table

10.8.4 display multicast ipv6 routing-table

Function

The **display multicast ipv6 routing-table** command displays information about an IPv6 multicast routing table.

Format

display multicast ipv6 routing-table [*ipv6-source-address* [*ipv6-source-mask-length*] | *ipv6-group-address* [*ipv6-group-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** | **none** }] * [**outgoing-interface-number** [*number*]]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
incoming-interface	Indicates the incoming interface of a multicast forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicates the register interface of IPv6 PIM-SM.	-
outgoing-interface	Indicates the outgoing interface of a multicast forwarding entry.	-
include	Displays the (S, G) entries whose downstream interface list contains specified outgoing interfaces.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
exclude	Displays the (S, G) entries whose downstream interface list does not contain specified outgoing interfaces.	-
match	Displays (S, G) entries whose the downstream interface list contains only one interface that is the same as a specified outgoing interface.	If no interface is specified, the (S, G) entry with the null downstream interface list is displayed.
none	Displays the routing entry without a downstream interface.	-
outgoing-interface-number	Displays the number of the outgoing interfaces of multicast routing entries.	-
number	Specifies the number of outgoing interfaces.	The value is an integer that ranges from 0 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display multicast ipv6 routing-table** command to view the IPv6 multicast routing table, including the multicast source address, multicast group address, upstream interface, and downstream interface list.

Example

Display the corresponding routing entry of a multicast group in the IPv6 multicast routing table.

```
<Huawei> display multicast ipv6 routing-table
IPv6 multicast routing table
 Total 1 entry

 00001. (FC00::2, FFE3::1)
      Uptime: 00:00:14
      Upstream Interface: GigabitEthernet1/0/0
      List of 1 downstream interface
          1:  GigabitEthernet2/0/0
```

Table 10-109 Description of the display multicast ipv6 routing-table command output

Item	Description
IPv6 multicast routing table	IPv6 multicast routing table.
Total 1 entry	Number of routing entries that meet the query condition.
00001	Sequence number of the (S, G) entry.
(FC00::2, FFE3::1)	(S, G) entry in the IPv6 multicast routing table.
Uptime	Period during which the (S, G) entry exists.
Upstream Interface	Upstream interface of the (S, G) entry.
List of 1 downstream interface	Downstream interface list.

Display the number of downstream interfaces of the IPv6 multicast routing entries.

```
<Huawei> display multicast ipv6 routing-table outgoing-interface-number
IPv6 multicast routing table
 Total 2 entries

 00001. (FC00::55, FF33::1)
      Uptime: 00:00:05
      Upstream Interface: GigabitEthernet1/0/0
      List of 2 downstream interfaces

 00002. (FC00::55, FF33::2)
      Uptime: 00:00:05
      Upstream Interface: GigabitEthernet2/0/0
      List of 2 downstream interfaces
```

Table 10-110 Description of the display multicast ipv6 routing-table outgoing-interface-number command output

Item	Description
List of 2 downstream interfaces	Number of the outgoing interfaces of IPv6 multicast routing entries.

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.18 reset multicast ipv6 routing-table

10.8.5 display multicast ipv6 rpf-info

Function

The **display multicast ipv6 rpf-info** command displays the Reverse Path Forwarding (RPF) routes of a specified IPv6 multicast source or source/group.

Format

display multicast ipv6 rpf-info *ipv6-source-address* [*ipv6-group-address*] [**rpt** | **spt**]

Parameters

Parameter	Description	Value
ipv6-source-address	Specifies the IPv6 address of a multicast source, used to display the information of RPF routing corresponding to the source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-group-address	Specifies the IPv6 address of a multicast group, used to display the information of RPF routing corresponding to the group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
rpt	Displays the RPF routing information corresponding to a specified source or group on the RPT.	-
spt	Displays the RPF routing information corresponding to a specified source or group on the SPT.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The RPF route with the *ipv6-source-address* as the destination address is an optimal route selected from IPv6 unicast routes. You can use the **display multicast ipv6 rpf-info** command to check the RPF route to the specified source or source-group.

Example

Display all RPF routes to the source address FC00::101.

```
<Huawei> display multicast ipv6 rpf-info fc00::101
 VPN-Instance: public net
 RPF information about source: FC00::101
     RPF interface: GigabitEthernet1/0/0, RPF neighbor: FE80::208:ACFF:FE10:48
     Referenced route/mask: FC00::/64
     Referenced route type: unicast
     Load splitting rule: disable
```

Table 10-111 Description of the display multicast ipv6 rpf-info command output

Item	Description
RPF information about source	Indicates the multicast source to which RPF information belongs.
RPF interface	Indicates the RPF interface.
RPF neighbor	Indicates the RPF neighbor.
Referenced route/mask	Indicates the referenced route and its mask.
Referenced route type	Indicates the referenced route type.
Load splitting rule	Load splitting rules: • disable: load splitting disabled. • balance-preferred: load balancing preferred. • stable-preferred: stable-preferred load splitting. • source: source address-based load splitting. • group: group address-based load splitting. • source-group: source and group addresses-based load splitting.

Related Topics

10.8.4 display multicast ipv6 routing-table
10.8.3 display multicast ipv6 forwarding-table

10.8.6 multicast ipv6 boundary

Function

The **multicast ipv6 boundary** command configures a multicast boundary on an interface.

The **undo multicast ipv6 boundary** command deletes the configured multicast boundary.

By default, no multicast boundary is configured on an interface.

Format

multicast ipv6 boundary { *ipv6-group-address ipv6-group-mask-length* | **scope** *scope-id* }

undo multicast ipv6 boundary { *ipv6-group-address ipv6-group-mask-length* | **all** | **scope** }

Parameters

Parameter	Description	Value
ipv6-group-address	Specifies a multicast group address.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
scope *scope-id*	Specifies a scope ID.	The value is an integer that ranges from 3 to 15.
all	Deletes all the multicast boundaries configured on an interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Data of some multicast groups needs to be forwarded within a specified range. For example, each BSR administrative domain serves a specific group address range, and data packets sent from multicast sources to these groups need to be forwarded within the matching administrative domain. After a multicast boundary is configured for specified multicast groups on an interface, multicast packets sent to these groups cannot be forwarded through the interface. This restricts multicast forwarding within a range.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

To configure the boundary for different multicast groups, you can repeat the command on the same interface.

A and B are the forwarding boundary sets of the multicast group range to be configured, and B is a subset of A. If A is first configured on an interface, B cannot be configured. If you configure A on the interface that has been configured with B, B is replaced by A.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure GE1/0/0 as the boundary of group FF02::101/16.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary FF02::101 16
```

Related Topics

10.8.1 display multicast ipv6 boundary

10.8.7 multicast ipv6 boundary policy

Function

The **multicast ipv6 boundary policy** command configures an IPv6 inbound and outbound multicast boundary policy on a specific interface.

The **undo multicast ipv6 boundary policy** command cancels the configuration.

By default, no IPv6 inbound and outbound multicast boundary policy is configured on an interface.

Format

multicast ipv6 boundary policy *basic-acl6-number*

undo multicast ipv6 boundary policy *basic-acl6-number*

Parameters

Parameter	Description	Value
basic-acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound and outbound multicast boundary policy

 Copyright © Huawei Technologies Co., Ltd.

has the functions of both an inbound multicast boundary policy and an outbound multicast boundary policy.

Precautions

The **multicast ipv6 boundary policy** command works with the **acl ipv6** command. The **source** parameter in the **rule** command can be run in the ACL6 view to specific a group address range for an inbound and outbound multicast boundary policy.

Example

Configure an inbound and outbound multicast boundary policy for multicast group FF1E::1/128 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule deny source FF1E::1 128
[Huawei-acl6-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy 2000
```

Related Topics

10.8.2 display multicast ipv6 boundary policy

10.8.8 multicast ipv6 boundary policy in

Function

The **multicast ipv6 boundary policy in** command configures an IPv6 inbound multicast boundary policy on a specific interface.

The **undo multicast ipv6 boundary policy in** command cancels the configuration.

By default, no IPv6 inbound multicast boundary policy is configured on an interface.

Format

multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **in**

undo multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **in**

Parameters

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl6-number	Specifies the number of an advanced IPv6 ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. An inbound multicast boundary policy effectively controls source/group-specific data packets that can enter the local domain. An inbound multicast boundary filters the multicast data packets that an interface can receive and the PIM Join/Prune and MLD Report messages that an interface can send. By filtering these messages, an inbound multicast boundary policy controls the direction in which multicast data is forwarded and received on the protocol control and forwarding planes.

Precautions

- If you run the **multicast ipv6 boundary policy in** command several times, the latest configuration overrides the previous configurations.
- The **multicast ipv6 boundary policy in** command works with the **acl ipv6** command.
  - The parameter **source** in the **rule** command can be run in the view of a numbered basic IPv6 ACL to specify a group address range for an inbound multicast boundary policy.
  - The parameter **source** in the **rule** command in the view of a numbered advanced IPv6 ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

– A named IPv6 ACL uses the same rules as a numbered advanced IPv6 ACL. The parameter **source** in the **rule** command in the ACL6 view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an inbound multicast boundary policy.

Example

Configure an inbound multicast boundary policy for multicast group FF1E::1/128 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule permit source FF1E::1 128
[Huawei-acl6-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy 2000 in
```

Use a named IPv6 ACL to configure an inbound multicast boundary policy for the entry (2001::5, FF0E::1) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source 2001::5 128 destination FF0E::1 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy acl6-name myacl6 in
```

Related Topics

10.8.2 display multicast ipv6 boundary policy

10.8.9 multicast ipv6 boundary policy out

Function

The **multicast ipv6 boundary policy out** command configures an IPv6 outbound multicast boundary policy on a specific interface.

The **undo multicast ipv6 boundary policy out** command cancels the configuration.

By default, no IPv6 outbound multicast boundary policy is configured on an interface.

Format

multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **out**

undo multicast ipv6 boundary policy { **acl6-name** *acl6-name* | *basic-acl6-number* | *advanced-acl6-number* } **out**

Parameters

Parameter	Description	Value
acl6-name *acl6-name*	Specifies the name of a named IPv6 ACL. **NOTE** **acl6-name** *acl6-name* can only be the name of a named advanced ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
basic-acl6-number	Specifies the number of a basic IPv6 ACL.	The value is an integer ranging from 2000 to 2999.
advanced-acl6-number	Specifies the number of an advanced IPv6 ACL.	The value is an integer ranging from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Deploying a multicast forwarding boundary enhances multicast data security and prevents network congestion caused by forwarding multicast traffic within a large range. Multicast boundary policies can be used to define multicast boundaries. Multicast boundary policies are classified into inbound multicast boundary policies, outbound multicast boundary policies, and inbound and outbound multicast boundary policies. Outbound multicast boundary policy effectively controls source/group-specific data packets that can be sent out of the local domain. An interface on which an outbound multicast boundary policy is configured filters the PIM Join/Prune and MLD Report messages that an interface can receive. By filtering these messages, an outbound multicast boundary policy controls the downstream interfaces in the downstream interface list of a multicast forwarding entry.

Configuration Impact

Precautions

- If you run the **multicast ipv6 boundary policy out** command several times, the latest configuration overrides the previous configurations.
- The **multicast ipv6 boundary policy out** command works with the **acl ipv6** command.
  - The parameter **source** in the **rule** command can be run in the view of a numbered basic IPv6 ACL to specify a group address range for an outbound multicast boundary policy.

 Copyright © Huawei Technologies Co., Ltd.

- The parameter **source** in the **rule** command in the view of a numbered advanced IPv6 ACL can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.
- A named IPv6 ACL uses the same rules as a numbered advanced IPv6 ACL. The parameter **source** in the **rule** command in the ACL6 view can be used to specify a source address range and the parameter **destination** in this command can be used to specify a group address range for an outbound multicast boundary policy.

Example

Use a numbered basic IPv6 ACL to configure an outbound multicast boundary policy for multicast group FF1E::1/128 on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule permit source FF1E::1 128
[Huawei-acl6-basic-2000] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy 2000 out
```

Use a named IPv6 ACL to configure an outbound multicast boundary policy for the entry (2001::5, FF0E::1) on GE1/0/0.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] ipv6
[Huawei] acl ipv6 name myacl6
[Huawei-acl6-adv-myacl6] rule permit ipv6 source 2001::5 128 destination FF0E::1 128
[Huawei-acl6-adv-myacl6] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 boundary policy acl6-name myacl6 out
```

Related Topics

10.8.2 display multicast ipv6 boundary policy

10.8.10 multicast ipv6 forwarding-table downstream-limit

Function

The **multicast ipv6 forwarding-table downstream-limit** command sets the maximum number of downstream nodes of an entry in the IPv6 multicast forwarding table.

The **undo multicast ipv6 forwarding-table downstream-limit** command restores the default setting.

By default, the maximum number of downstream nodes of an entry is 128.

Format

multicast ipv6 forwarding-table downstream-limit *limit*

undo multicast ipv6 forwarding-table downstream-limit

Parameters

Parameter	Description	Value
limit	Indicates the maximum number of downstream nodes of an entry in the forwarding table.	The value is an integer that ranges from: 0 to 128.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the router receives a multicast packet, it copies the packet for each downstream node in the matching IPv6 multicast forwarding entry. If the router has a large number of IPv6 multicast forwarding entries or each entry has many downstream nodes, many system resources are consumed. To reduce the loads of the router, limit the maximum number of downstream nodes in each IPv6 multicast forwarding entry.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

If the configured number is smaller than the current number, the excessive downstream nodes are not deleted immediately, and must be deleted by the IPv6 multicast routing protocol. In addition, no new downstream node can be added to the entry in the forwarding table.

Example

In the system view, set the maximum number of downstream nodes of an entry in the IPv6 multicast forwarding table to 32.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] multicast ipv6 forwarding-table downstream-limit 32
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.11 multicast ipv6 forwarding-table route-limit

Function

The **multicast ipv6 forwarding-table route-limit** command sets the limits on the number of entries in the IPv6 multicast forwarding table.

The **undo multicast ipv6 forwarding-table route-limit** command restores the default value of the limit.

By default, the limit on the number of entries in the IPv6 multicast forwarding table varies according to device models:

- AR100&AR120&AR150&AR160&AR200 series: 64
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 256
- AR2204XE and AR2204XE-DC: 512
- AR2240 and AR3200 series:
  - Configured with SRU40: 256
  - Configured with SRU60: 256
  - Configured with SRU80: 512
  - Configured with SRU100: 512
  - Configured with SRU100E: 512
  - Configured with SRU200: 1024
  - Configured with SRU200E: 1024
  - Configured with SRU400: 2048
- AR3600 series (SRUX5): 1024

Format

multicast ipv6 forwarding-table route-limit *limit*

undo multicast ipv6 forwarding-table route-limit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
limit	Specifies the limit on the number of entries in the IPv6 multicast forwarding table.	The value is an integer that ranges from ● 0 to 64 for the AR100&AR120&AR150&AR160&AR200 series ● 0 to 128 for the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 ● 0 to 256 for the AR2220, AR2240C, and AR2220E ● 0 to 512 for the AR2204XE and AR2204XE-DC ● AR2240 and AR3200 series: – Configured with SRU40: 0 to 256 – Configured with SRU60: 0 to 256 – Configured with SRU80: 0 to 512 – Configured with SRU100: 0 to 512 – Configured with SRU100E: 0 to 512 – Configured with SRU200: 0 to 1024 – Configured with SRU200E: 0 to 1024 – Configured with SRU400: 0 to 2048 ● 1 to 1024 for the AR3600 series (SRUX5)

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Excessive IPv6 multicast forwarding entries will exhaust the memory of the router. To prevent this problem, use the **multicast ipv6 forwarding-table route-limit** command to limit the number of entries in the IPv6 multicast forwarding table.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

If the limit on the number of entries in the IPv6 multicast forwarding table is set after multicast services are deployed on a router, ensure that the limit on the number of entries in the IPv6 multicast forwarding table is equal to or greater than the number of current forwarding entries. Otherwise, faults may occur.

You are recommended to limit the number of entries in the IPv6 multicast forwarding table according to the actual network environment before the router operates multicast services.

If the newly-configured limit on the number of entries are less than the number of existing entries, the excessive entries are not deleted immediately. The configured maximum number of entries takes effect in the following cases:

- Entries are added to the IPv6 multicast forwarding table after the existing entries age out.
- The **reset multicast ipv6 forwarding-table all** command is run.

Example

Set the limit on the number of the entries in the IPv6 forwarding table to 60.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] multicast ipv6 forwarding-table route-limit 60
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.17 reset multicast ipv6 forwarding-table

10.8.12 multicast ipv6 invalid-packet

Function

The **multicast ipv6 invalid-packet** command sets the maximum number of invalid IPv6 multicast protocol packets that can be stored on the router.

The **undo multicast ipv6 invalid-packet** command deletes the set maximum number of invalid IPv6 multicast protocol packets that can be stored on the router.

By default, the router can save a maximum of 10 invalid packets for each specific IPv6 multicast protocol.

Format

multicast ipv6 invalid-packet { **mld** | **pim** } **max-count** *max-number*

undo multicast ipv6 invalid-packet { **mld** | **pim** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mld	Sets the maximum number of invalid MLD messages.	-
pim	Sets the maximum number of invalid PIM (IPv6) messages.	-
max-count *max-number*	Sets the maximum number of invalid IPv6 multicast protocol packets that can be stored on a device.	The value is an integer that ranges from 1 to 100.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If IPv6 multicast entries fail to be generated or peer relationships fail to be set up, you can enable the router to store invalid IPv6 multicast protocol packets and view statistics and details of the invalid IPv6 multicast protocol packets. Based on the command output, you can locate and rectify faults.

Example

Set the maximum number of invalid MLD messages that can be stored on the router to 20.

```
<Huawei> system-view
[Huawei] multicast ipv6 invalid-packet mld max-count 20
```

Related Topics

10.2.8 display mld invalid-packet

10.4.25 display pim ipv6 invalid-packet

10.8.13 multicast ipv6 load-splitting

Function

The **multicast ipv6 load-splitting** command enables load splitting among IPv6 multicast routes.

The **undo multicast ipv6 load-splitting** command restores the default configuration.

By default, load splitting among IPv6 multicast routes is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

multicast ipv6 load-splitting { **balance-preferred** | **stable-preferred** | **group** | **source** | **source-group** }

undo multicast ipv6 load-splitting

Parameters

Parameter	Description	Value
balance-preferred	Indicates balance-preferred load splitting. This policy is applicable to the scenario where hosts frequently join or leave groups, which requires automatic load adjustment.	-
group	Indicates group address-based load splitting. This policy is applicable to the scenario of one source to multiple groups.	-
source	Indicates source address-based load splitting. This policy is applicable to the scenario of multiple sources to one group.	-
source-group	Indicates source and group addresses-based load splitting. This policy is applicable to the scenario of multiple sources to multiple groups.	-
stable-preferred	Indicates stable-preferred load splitting. This policy is applicable to stable multicast networking.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if there are multiple equal-cost routes to a multicast source, the device selects the route with the largest next-hop address as the RPF route. To enable multicast data to be forwarded through multiple paths, run this command to configure multicast load splitting. After multicast load splitting is configured, the device uses the specified load splitting policy to distribute multicast data among multiple paths. This function improves quality of multicast forwarding.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Because the forwarding capabilities of equal-cost routes are different from the actual load distribution situation on the equal-cost routes, even load splitting cannot meet network requirements in some scenarios. Then, you can run the **multicast ipv6 load-splitting weight** command to configure the IPv6 multicast load splitting weight on the interface to realize unbalanced load splitting.

Precautions

The five load splitting policies are mutually exclusive. It is recommended that you use a fixed load splitting policy based on the actual situation on your network. The **balance-preferred** or **stable-preferred** policy is preferred.

If PIM-DM (IPv6) is enabled on the router, the **balance-preferred** or **stable-preferred** policy cannot be used.

Example

Configure stable-preferred load splitting in the system view.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] multicast ipv6 load-splitting stable-preferred
```

Related Topics

10.8.14 multicast ipv6 load-splitting weight

10.8.15 multicast ipv6 load-splitting-timer

10.8.14 multicast ipv6 load-splitting weight

Function

The **multicast ipv6 load-splitting weight** command sets the IPv6 multicast load splitting weight for an interface.

The **undo multicast ipv6 load-splitting weight** command restores the default setting.

By default, the IPv6 multicast load splitting weight of an interface is 1.

Format

multicast ipv6 load-splitting weight *weight-value*

undo multicast ipv6 load-splitting weight

Parameters

Parameter	Description	Value
weight-value	Specifies the IPv6 multicast load splitting weight of an interface.	The value is an integer that ranges from 0 to 32.

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a stable-preferred or balance-preferred multicast splitting policy is configured, you can run this command to set load splitting weights for interfaces to realize unbalanced load splitting. An interface with a larger weight value has more IPv6 multicast routing entries with it as the upstream interface.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Precautions

This command is applicable only when the IPv6 multicast load splitting policy is set to stable-preferred or balance-preferred.

When the IPv6 multicast load splitting weight on an interface is 0, the routes with this interface as the upstream interface do not take part in load splitting.

Example

Set the IPv6 multicast load splitting weight on GE1/0/0 to 10.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] multicast ipv6 load-splitting weight 10
```

Related Topics

10.8.13 multicast ipv6 load-splitting

10.8.15 multicast ipv6 load-splitting-timer

Function

The **multicast ipv6 load-splitting-timer** command sets a load splitting timer.

The **undo multicast ipv6 load-splitting-timer** command restores the default setting.

By default, the value of a load splitting timer is 1800 seconds.

Format

multicast ipv6 load-splitting-timer *interval*

undo multicast ipv6 load-splitting-timer

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the value of the load splitting timer.	The value is an integer that ranges from 10 to 1800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In stable-preferred load splitting or balance-preferred load splitting mode, entries may not be well-balanced among paths because of the addition or deletion of entries, change of load splitting weights of the paths, or change of equal-cost routes. In such a case, the device will balance entries after a certain waiting time to reduce the impact of frequent changes on the system.

Currently, setting a load splitting timer to change the waiting time before balancing entries is supported.

- If the network is relatively stable, such as when entries are not deleted or added frequently or equal-cost routes are not changed frequently, set the load splitting timer value to a smaller value so that entries can be balanced rapidly. The recommended value is 300 to 600 seconds.
- If the network is not stable, such as when entries are deleted or added frequently or equal-cost routes are changed frequently, set the load splitting timer value to a larger value to reduce the impact of frequent entry changes on the system and network stability. The recommended value is 1200 to 1800 seconds.

Prerequisites

IPv6 multicast routing has been enabled using the **multicast ipv6 routing-enable** command in the system view.

Example

Set a load splitting timer to 100 seconds.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
[Huawei] multicast ipv6 load-splitting-timer 100
```

Related Topics

10.8.13 multicast ipv6 load-splitting

 Copyright © Huawei Technologies Co., Ltd.

10.8.16 multicast ipv6 routing-enable

Function

The **multicast ipv6 routing-enable** command enables the IPv6 multicast routing function.

The **undo multicast ipv6 routing-enable** command restores the default configuration.

By default, the IPv6 multicast routing function is disabled.

Format

multicast ipv6 routing-enable

undo multicast ipv6 routing-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before configuring Layer 3 IPv6 multicast, you must enable the IPv6 multicast routing function globally. Layer 3 IPv6 multicast protocols (such as PIM (IPv6) and MLD) and other Layer 3 IPv6 multicast functions can be configured only after IPv6 multicast routing is enabled.

Precautions

NOTICE

The **undo multicast ipv6 routing-enable** command deletes all IPv6 multicast configurations of the device. If IPv6 multicast services are running on the device, the IPv6 multicast services are interrupted when this command is executed. To restore IPv6 multicast services on the instance, you must re-configure the corresponding commands.

Example

Enable IPv6 multicast routing globally.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast ipv6 routing-enable
```

Related Topics

10.2.16 mld enable

10.4.47 pim ipv6 dm

10.4.59 pim ipv6 sm

10.8.17 reset multicast ipv6 forwarding-table

Function

The **reset multicast ipv6 forwarding-table** command clears the entries of the IPv6 multicast forwarding table.

Format

reset multicast ipv6 forwarding-table all

reset multicast ipv6 forwarding-table { *ipv6-group-address* [*ipv6-group-mask-length*] | *ipv6-source-address* [*ipv6-source-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
all	Resets all the multicast forwarding caches (MFCs) in the multicast forwarding table.	-
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of a multicast group address.	The value is an integer that ranges from 8 to 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
incoming-interface	Indicates the incoming interface of a forwarding entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
register	Indicates the register interface of IPv6 PIM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the IPv6 multicast forwarding table, multicast data will be interrupted for a period. Confirm the action before you use the command.

Example

Delete all the IPv6 multicast forwarding entries.

```
<Huawei> reset multicast ipv6 forwarding-table all
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.18 reset multicast ipv6 routing-table

Function

The **reset multicast ipv6 routing-table** command clears the entries in the IPv6 multicast routing table. The corresponding forwarding entries in the forwarding table are deleted at the same time.

Format

reset multicast ipv6 routing-table all

reset multicast ipv6 routing-table { *ipv6-group-address* [*ipv6-group-mask-length*] | *ipv6-source-address* [*ipv6-source-mask-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } *

Parameters

Parameter	Description	Value
all	Resets all routing entries in the multicast core routing table.	-
ipv6-group-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.
ipv6-group-mask-length	Specifies the mask length of an IPv6 multicast group address.	The value is an integer that ranges from 8 to 128.
ipv6-source-address	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
ipv6-source-mask-length	Specifies the mask length of a multicast source address.	The value is an integer that ranges from 0 to 128.
incoming-interface	Indicates the incoming interface of a routing entry.	-
interface-type interface-number	Specifies the type and number of an interface.	-
register	Indicate the register interface of IPv6 PIM.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run this command to delete information from the IPv6 multicast routing table, the matching entries in the IPv6 multicast forwarding table are also deleted. As a result, multicast forwarding will be interrupted for a period. Confirm the action before you use the command.

Example

Delete the entries of the group FF02::101 from the IPv6 multicast routing table.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> reset multicast ipv6 routing-table FF02::101
```

Related Topics

10.8.3 display multicast ipv6 forwarding-table

10.8.4 display multicast ipv6 routing-table

10.9 IGMP Snooping Configuration Commands

NOTE

Only AR129CV, AR129CVW, AR129CGVW-L and AR2200&AR3200&AR3600 series support IGMP Snooping.

Only the 8FE1GE, 24GE and 24ES2GP cards support IGMP Snooping.

10.9.1 display igmp-snooping

Function

The **display igmp-snooping** command displays the IGMP snooping running parameters.

Format

display igmp-snooping [**vlan** [*vlan-id*]]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the IGMP snooping running parameters in a specified VLAN. If this parameter is not specified, the system displays the IGMP running parameters in all VLANs with IGMP snooping configured.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view the IGMP snooping running parameters.

To view the IGMP snooping configuration, run the **display igmp-snooping configuration** command.

Precautions

This command can display the IGMP snooping running parameters in a VLAN only when the VLAN is in Up state (at least one interface in the VLAN is in Up state) and has IGMP snooping enabled. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Display the IGMP snooping running parameters.

```
<Huawei> display igmp-snooping
 IGMP Snooping Information for VLAN 3
  IGMP Snooping is Enable
  IGMP Version is Set to default 2
  IGMP Query Interval is Set to default 60
  IGMP Max Response Interval is Set to default 10
  IGMP Robustness is Set to default 2
  IGMP Last Member Query Interval is Set to default 1
  IGMP Router Port Aging Interval is Set to 180s or holdtime in hello
  IGMP Filter Group-Policy is Set to default : Permit All
  IGMP Prompt Leave Disable
  IGMP Router Alert is Not Required
  IGMP Send Router Alert Enable
  IGMP Proxy Disable
  IGMP Report Suppress Disable
  IGMP Suppress Time is set to default 10 seconds
  IGMP Querier Disable
  IGMP Router Port Learning Enable
  IGMP SSM-Mapping Disable
```

Table 10-112 Description of the display igmp-snooping command output

Item	Description
IGMP Snooping Information for VLAN 3	The following information displayed is the IGMP snooping running parameters in VLAN 3.
IGMP Snooping is Enable	IGMP snooping is enabled in the VLAN. By default, IGMP snooping is disabled in a VLAN. IGMP snooping can be enabled in a VLAN using the **igmp-snooping enable (VLAN view)** command.
IGMP Version is Set to default 2	Version of IGMP messages that can be processed in the VLAN. In this example, the default version 2 is displayed, indicating that both IGMPv1 and IGMPv2 messages can be processed. This parameter is configured using the **igmp-snooping version** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IGMP Query Interval is Set to default 60	Interval at which IGMP General Query messages are sent. In this example, the default value (60 seconds) is displayed. This parameter is configured using the **igmp-snoopig query-interval** command.
IGMP Max Response Interval is Set to default 10	Maximum response time for IGMP General Query messages. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **igmp-snoopig max-response-time** command.
IGMP Robustness is Set to default 2	IGMP robustness variable, In this example, the default value 2 is displayed. This parameter is configured using the **igmp-snooping robust-count** command.
IGMP Last Member Query Interval is Set to default 1	Interval at which IGMP Group-Specific Query messages are sent. In this example, the default value (1 second) is displayed. This parameter is configured using the **igmp-snoopig lastmember-queryinterval** command.
IGMP Router Port Aging Interval is Set to 180s or holdtime in hello	Aging time of a router port. In this example, the default value (180 seconds or the holdtime value contained in PIM Hello messages) is displayed. This parameter is configured using the **igmp-snooping router-aging-time** command.
IGMP Filter Group-Policy is Set to default : Permit All	Multicast group policy. In this example, the default configuration is displayed. That is, no policy is configured. A multicast group policy is configured using the **igmp-snooping group-policy** command.
IGMP Prompt Leave Disable	The prompt leave function is disabled for interfaces in the VLAN (default configuration). The prompt leave function can be enabled using the **igmp-snooping prompt-leave** command.
IGMP Router Alert is Not Required	The router does not require that the IGMP messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The router can be configured to discard IGMP messages without the Router-Alert option using the **igmp-snooping require-router-alert** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IGMP Send Router Alert Enable	The router sends the IGMP messages with the Router-Alert option to the VLAN (default configuration). The router can be configured to send IGMP messages with the Router-Alert option using the **igmp-snooping send-router-alert** command.
IGMP Router Port Learning Enable	Router port learning is enabled (default configuration). Router port learning can be enabled using the **igmp-snooping router-learning** command.
IGMP Proxy Disable	IGMP snooping proxy is disabled (default configuration).
IGMP Report Suppress Disable	IGMP message suppression is disabled (default configuration). IGMP message suppression can be enabled using the **igmp-snooping report-suppress** command.
IGMP Suppress Time is set to default 10 seconds	IGMP message suppression time. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **igmp-snooping suppress-time** command.
IGMP Querier Disable	IGMP snooping querier is disabled (default configuration). IGMP snooping querier can be enabled using the **igmp-snooping querier enable** command.
IGMP SSM-Mapping Disable	IGMP snooping SSM mapping is disabled (default configuration). IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.

Related Topics

10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)
10.9.13 igmp-snooping lastmember-queryinterval
10.9.15 igmp-snooping max-response-time
10.9.16 igmp-snooping prompt-leave
10.9.17 igmp-snooping querier enable
10.9.18 igmp-snooping query-interval
10.9.19 igmp-snooping report-suppress
10.9.20 igmp-snooping require-router-alert

 Copyright © Huawei Technologies Co., Ltd.

10.9.21 igmp-snooping robust-count
10.9.22 igmp-snooping router-aging-time
10.9.23 igmp-snooping router-learning (VLAN view)
10.9.26 igmp-snooping send-router-alert
10.9.28 igmp-snooping ssm-mapping enable
10.9.31 igmp-snooping suppress-time
10.9.32 igmp-snooping version

10.9.2 display igmp-snooping configuration

Function

The **display igmp-snooping configuration** command displays the IGMP snooping configuration.

Format

display igmp-snooping [**vlan** [*vlan-id*]] **configuration**

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays the IGMP snooping configuration in a specified VLAN. If this parameter is not specified, the system displays the IGMP snooping configuration in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays only the IGMP snooping configuration so that you can check whether the IGMP snooping configuration made in the system is proper.

To check all IGMP snooping running parameters, run the **display igmp-snooping** command.

Prerequisites

The IGMP snooping configuration in a VLAN can be displayed as long as IGMP snooping parameters have been configured in the VLAN, no matter whether the VLAN contains interfaces in Up state.

Global IGMP snooping must be enabled using the **igmp-snooping enable (system view)** command before any IGMP snooping configuration is performed.

Example

Display the IGMP snooping configuration in all VLANs.

```
<Huawei> display igmp-snooping configuration
 IGMP Snooping Configuration for VLAN 7
    igmp-snooping enable
    igmp-snooping version 3
    igmp-snooping ssm-mapping enable
    igmp-snooping ssm-policy 2000
    igmp-snooping ssm-mapping 232.1.1.0 255.255.255.0 10.1.2.1
```

Table 10-113 Description of the display igmp-snooping configuration command output

Item	Description
IGMP Snooping Configuration for VLAN 7	The following information displayed is the IGMP snooping configuration in VLAN 7.
igmp-snooping enable	IGMP snooping is enabled in the VLAN. By default, IGMP snooping is disabled in a VLAN. IGMP snooping can be enabled in a VLAN using the **igmp-snooping enable (VLAN view)** command.
igmp-snooping version 3	Messages of IGMPv1, IGMPv2, and IGMPv3 can be processed in the VLAN. By default, IGMPv1 and IGMPv2 messages can be processed in a VLAN. This parameter is configured using the **igmp-snooping version** command.
igmp-snooping ssm-mapping enable	IGMP snooping SSM mapping is enabled in the VLAN. By default, IGMP snooping SSM mapping is disabled in a VLAN. IGMP snooping SSM mapping can be enabled using the **igmp-snooping ssm-mapping enable** command.
igmp-snooping ssm-policy 2000	The SSM mapping policy that references ACL 2000 is configured in the VLAN. By default, no SSM group policy is applied to a VLAN. An SSM group policy is configured using the **igmp-snooping ssm-policy** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
igmp-snooping ssm-mapping 232.1.1.0 255.255.255.0 10.1.2.1	In the SSM mapping policy, multicast group addresses 232.1.1.0 through 232.1.1.255 are mapped to multicast source 10.1.2.1. By default, group-source mapping is configured in a VLAN. A group-source mapping is configured using the **igmp-snooping ssm-mapping** command.

Related Topics

10.9.1 display igmp-snooping
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)
10.9.13 igmp-snooping lastmember-queryinterval
10.9.15 igmp-snooping max-response-time
10.9.16 igmp-snooping prompt-leave
10.9.17 igmp-snooping querier enable
10.9.18 igmp-snooping query-interval
10.9.19 igmp-snooping report-suppress
10.9.20 igmp-snooping require-router-alert
10.9.21 igmp-snooping robust-count
10.9.22 igmp-snooping router-aging-time
10.9.23 igmp-snooping router-learning (VLAN view)
10.9.26 igmp-snooping send-router-alert
10.9.27 igmp-snooping ssm-mapping
10.9.28 igmp-snooping ssm-mapping enable
10.9.29 igmp-snooping ssm-policy
10.9.31 igmp-snooping suppress-time
10.9.32 igmp-snooping version

10.9.3 display igmp-snooping port-info

Function

The **display igmp-snooping port-info** command displays information about multicast group member ports.

Format

display igmp-snooping port-info [**vlan** *vlan-id* [**group-address** *group-address*]] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays information about multicast group member ports in a specified VLAN. If this parameter is not specified, the system displays multicast group member ports in all VLANs.	The value is an integer ranging from 1 to 4094.
group-address *group-address*	Displays information about member ports of a specified multicast group. If this parameter is not specified, the system displays member ports of all multicast groups.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.
verbose	Displays detailed information about multicast group member ports. If this parameter is not specified, the system displays the summary of multicast group member ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When the router with IGMP snooping enabled receives IGMP messages exchanged between hosts and a Layer 3 device, the router maintains a Layer 2 multicast forwarding table based on information in the messages. The **display igmp-snooping port-info** command shows member ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink ports of the router have multicast users connected, and control multicast services conveniently.

Precautions

This command can display information about multicast group member ports in a VLAN only when IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command, and at least one interface in the VLAN is in Up state.

Example

Display information about multicast group member ports in VLAN 7.

```
<Huawei> display igmp-snooping port-info vlan 7
----------------------------------------------------------------------
                (Source, Group)    Port                    Flag
----------------------------------------------------------------------
VLAN 7, 5 Entry(s)
                 (*,226.1.1.1)    Eth2/0/0                 -D-
                                    1 port(s)
            (10.1.1.1,226.1.1.2)   Eth2/0/0                 --M
                                    1 port(s)
            (10.1.1.1,226.1.1.3)   Eth2/0/0                 --M
                                    1 port(s)
                (*, 227.1.1.2)    Eth2/0/0                 S--
                                    1 port(s)
                (*, 227.1.1.3)    Eth2/0/0                 S--
                                    1 port(s)
----------------------------------------------------------------------
```

Table 10-114 Description of the display igmp-snooping port-info command output

Item	Description
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. Multicast data is sent from multicast source S to group G. If S is displayed as *, multicast data may be sent from any multicast source. If S is displayed as an IP address, multicast data is sent from this IP address.
Port	Member port.
Flag	Type of a member port, which can be: ● S: static member port, which is configured using the **l2-multicast static-group** command ● D: dynamic member port learned through IGMP snooping ● M: member port established through SSM mapping
VLAN 7, 5 Entry(s)	VLAN ID and the number of entries in the VLAN.

Display detailed information about all multicast group member ports.

```
<Huawei> display igmp-snooping port-info verbose

The port information of Group 239.255.255.250 on VLAN 22:
   Time of this group has been up : 00:01:22

 The port information of (10.1.1.2, 239.255.255.250):
   Time of this source has been up : 00:01:22
```

```
    Port Table on this source(10.1.1.2):
      No.1
        Port name : Eth2/0/0
        Time of this port has been up as a host-port : 00:01:22
        Remain time of port expire as dynamic host-port : 00:02:58
        Version2-host-present-timer-expiry: 00:04:14
        Host-port flags : Dynamic

The port information of Group 227.1.1.1 on VLAN 200:
    Time of this group has been up : 1d:05h

  The port information of (0.0.0.0, 227.1.1.1):
    Time of this source has been up : 1d:05h
    Port Table on this source(0.0.0.0):
      No.1
        Port name : Eth2/0/0
        Time of this port has been up as a host-port : 1d:05h
        Remain time of port expire as dynamic host-port : NA
        Host-port flags : Static
```

Table 10-115 Description of the display igmp-snooping port-info verbose command output

Item	Description
The port information of Group 239.255.255.250 on VLAN 22	Information about member ports of multicast group 239.255.255.250 in VLAN 22.
Time of this group has been up	Time that elapsed since the multicast group was set up.
The port information of (10.1.1.2, 239.255.255.250)	Information about member ports of a specified (S, G).
Time of this source has been up	Time that elapsed since the multicast source was set up.
Port Table on this source	List of member ports of the specified multicast source.
No.1	First member port.
Port name	Type and number of the first member port.
Time of this port has been up as a host-port	Time that elapsed since the first member port was bound to a source or (S, G).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remain time of port expire as dynamic host-port	Aging time of the first member port. This field displays "NA" for a static member port. The aging time of a dynamic member port is calculated using the following formula: Aging time = Robustness variable x General query interval + Maximum response time for General Query messages. The robustness variable is configured using the **igmp-snooping robust-count** command. The general query interval is configured using the **igmp-snooping query-interval** command. The maximum response time for General Query messages is configured using the **igmp-snooping max-response-time** command.
Version2-host-present-timer-expiry	Agile time of the IGMPv2 host.
Host-port flags	Type of a member port, which can be: • Static: static member • Dynamic: dynamic member port learned through IGMP snooping • Mapping: member port established through SSM mapping

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.15 igmp-snooping max-response-time
10.9.18 igmp-snooping query-interval
10.9.21 igmp-snooping robust-count
10.9.33 l2-multicast static-group

10.9.4 display igmp-snooping querier

Function

The **display igmp-snooping querier** command displays whether the IGMP snooping querier function is enabled in a VLAN.

Format

display igmp-snooping querier vlan [*vlan-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays whether the IGMP snooping querier function is enabled in a specified VLAN. If *vlan-id* is not specified, the system displays status of the IGMP snooping querier function in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can configure an IGMP snooping querier on the router to send IGMP Query messages instead of the upstream Layer 3 device in the following situations:

- The Layer 3 device cannot send IGMP messages for some reasons, for example, IGMP is not enabled on the Layer 3 device.
- The Layer 3 device uses static multicast forwarding entries and does not need to learn multicast forwarding entries.

You can use the **display igmp-snooping querier** command to check in which VLANs the IGMP snooping querier function is enabled.

Precautions

The querier function is disabled in a VLAN by default after IGMP snooping is enabled in the VLAN. To enable the querier function, run the **igmp-snooping querier enable** command.

Example

Display the status of the IGMP snooping querier function in all VLANs.

```
<Huawei> display igmp-snooping querier vlan
 VLAN            Querier-state
-----------------------------------------------
 10              Enable
 20              Disable
 30              Disable
-----------------------------------------------
 total entry 3
```

Table 10-116 Description of the display igmp-snooping querier vlan command output

Item	Description
VLAN	VLAN ID.
Querier-state	Querier status in a VLAN. • Disable: The IGMP snooping querier function is disabled in the VLAN. • Enable: The IGMP snooping querier function is enabled in the VLAN.
total entry 3	Number of VLANs in which the querier status is displayed.

Related Topics

10.9.17 igmp-snooping querier enable

10.9.5 display igmp-snooping router-port

Function

The **display igmp-snooping router-port** command displays information about the router ports in a specified VLAN, including static and dynamic router ports.

Format

display igmp-snooping router-port vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays information about the router ports in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port connects the router to an upstream Layer 3 multicast device. The router port can be statically configured or dynamically generated after the interface receives an IGMP Query message or a PIM Hello message.

You can run the **display igmp-snooping router-port** command to view the type, name, lifetime, and aging time of a router port.

Precautions

This command can display information about router ports in a VLAN only when IGMP snooping has been enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command, and at least one interface in the VLAN is in Up state.

Example

Display information about router ports in VLAN 2.

```
<Huawei> display igmp-snooping router-port vlan 2
Port Name                UpTime      Expires     Flags
-----------------------------------------------------------------
VLAN 2, 2 router-port(s)
Eth2/0/0                 03:28:16    00:01:20    DYNAMIC
Eth1/0/2                 2d:10h      --          STATIC
```

Table 10-117 Description of the display igmp-snooping router-port command output

Item	Description
Port Name	Type and number of a router port.
UpTime	Time that elapsed since the interface became a router port.
Expires	Aging time of the router port. ● The aging time is displayed for a dynamic router port. This parameter is configured using the **igmp-snooping router-aging-time** command. ● For a static router port, "--" is displayed, indicating that the static router does not age.
Flags	Type of the router port, which can be: ● STATIC: static router port configured using the **igmp-snooping static-router-port** command. ● DYNAMIC: dynamic router port

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.22 igmp-snooping router-aging-time

10.9.30 igmp-snooping static-router-port

 Copyright © Huawei Technologies Co., Ltd.

10.9.6 display igmp-snooping statistics

Function

The **display igmp-snooping statistics** command displays IGMP snooping statistics.

Format

display igmp-snooping statistics vlan [*vlan-id*]

Parameters

Parameter	Description	Value
vlan [*vlan-id*]	Displays IGMP snooping statistics in a specified VLAN. ● If *vlan-id* is not specified, the system displays IGMP snooping statistics in all VLANs. ● If *vlan-id* is specified, the system displays statistics about IGMP messages in the specified VLAN, but does not display the counts of IGMP snooping events that occur in the VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration, you can use the **display igmp-snooping statistics** command to view IGMP snooping statistics, including the number of IGMP messages sent, number of IGMP messages received, and number of PIM Hello messages received in each VLAN, and number of Layer 2 events that have occurred in all VLANs. Layer 2 events include changes in interface status,

 Copyright © Huawei Technologies Co., Ltd.

changes in VLAN status, changes in VLAN member interfaces (interfaces join or leave VLANs), and MSTP events. When a multicast fault occurs, the IGMP snooping statistics help you identify the cause of the fault.

Precautions

This command displays IGMP snooping statistics only when IGMP snooping has been enabled globally using the **igmp-snooping enable (VLAN view)** command.

Example

Display IGMP snooping statistics in all VLANs.

```
<Huawei> display igmp-snooping statistics vlan
 IGMP Snooping Events Counter
    Recv VLAN Up Event Times      1027
    Recv VLAN Down Event Times    5
    Recv VLAN Del Event Times     0
    Recv Port Up Event Times      12
    Recv Port Down Event Times    12
    Recv Port Del Event Times     0
    Recv Port Inc Event Times     3069
    Recv Port Exc Event Times     1023
    Recv MSTP Block Event Times   7
    Recv MSTP Forward Event Times 7
    Recv LINK Change Event Times  0
 IGMP Snooping Packets Counter
   Statistics for VLAN 10
    Recv V1 Report  16
    Recv V2 Report  8768
    Recv V3 Report  0
    Recv V1 Query   0
    Recv V2 Query   2243
    Recv V3 Query   0
    Recv Leave      215
    Recv Pim Hello  0
    Send Query(S=0) 0
    Send Query(S!=0)529
    Proxy Send General Query              0
    Proxy Send Group-Specific Query       0
    Proxy Send Group-Source-Specific Query 0
```

Display IGMP snooping statistics in VLAN 10.

```
<Huawei> display igmp-snooping statistics vlan 10
 IGMP Snooping Packets Counter
   Statistics for VLAN 10
    Recv V1 Report  16
    Recv V2 Report  8768
    Recv V3 Report  0
    Recv V1 Query   0
    Recv V2 Query   2243
    Recv V3 Query   0
    Recv Leave      215
    Recv Pim Hello  0
    Send Query(S=0) 0
    Send Query(S!=0)529
    Proxy Send General Query              0
    Proxy Send Group-Specific Query       0
    Proxy Send Group-Source-Specific Query 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 10-118 Description of the display igmp-snooping statistics command output

Item	Description
IGMP Snooping Events Counter	Statistics on IGMP snooping events, including changes in interface status, changes in VLAN status, interfaces joining or leaving VLANs, and MSTP events.
Recv VLAN Up Event Times	Number of VLAN Up events.
Recv VLAN Down Event Times	Number of VLAN Down events.
Recv VLAN Del Event Times	Number of VLAN deletion events.
Recv Port Up Event Times	Number of interface Up events.
Recv Port Down Event Times	Number of interface Down events.
Recv Port Del Event Times	Number of interface deletion events.
Recv Port Inc Event Times	Number of times interfaces join VLANs.
Recv Port Exc Event Times	Number of times interfaces leave VLANs.
Recv MSTP Block Event Times	Number of MSTP interface blocking events.
Recv MSTP Forward Event Times	Number of MSTP forwarding events.
Recv LINK Change Event Times	Number of link status change events.
IGMP Snooping Packets Counter	Statistics on IGMP and PIM packets.
Statistics for VLAN 10	Packet statistics in VLAN 10.
Recv V1 Report	Number of IGMPv1 Report messages received.
Recv V2 Report	Number of IGMPv2 Report messages received.
Recv V3 Report	Number of IGMPv3 Report messages received.
Recv V1 Query	Number of IGMPv1 Query messages received.
Recv V2 Query	Number of IGMPv2 Query messages received.
Recv V3 Query	Number of IGMPv3 Query messages received.
Recv Leave	Number of IGMP Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.
Send Query(S=0)	Number of IGMP Query messages sent with the source address 0.0.0.0.
Send Query(S!=0)	Number of IGMP Query messages sent with source addresses other than 0.0.0.0.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Proxy Send General Query	Number of General Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Specific Query	Number of Group-Specific Query messages sent by the IGMP snooping proxy.
Proxy Send Group-Source-Specific Query	Number of Group-Source-Specific Query messages sent by the IGMP snooping proxy.

Related Topics

10.9.9 igmp-snooping enable (VLAN view)

10.9.36 reset igmp-snooping statistics

10.9.7 display l2-multicast forwarding-table

Function

The **display l2-multicast forwarding-table** command displays the Layer 2 multicast forwarding table.

Format

display l2-multicast forwarding-table vlan *vlan-id* [[**source-address** *source-address*] **group-address** { *group-address* | **router-group** }]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays Layer 2 multicast forwarding entries in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
source-address *source-address*	Displays the forwarding entries of a specified multicast source.	The value is in dotted decimal notation.
group-address *group-address*	Displays multicast forwarding entries of a specified multicast group.	The value ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.
router-group	Displays multicast forwarding entries of all router ports.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing IGMP snooping configuration, you can use the **display l2-multicast forwarding-table** command to view the Layer 2 multicast forwarding table. This command displays statically configured and dynamic learned multicast forwarding entries.

Each entry contains the multicast source, multicast group, list of outbound interfaces, and VLAN ID of multicast data packets. When the IGMP snooping version is set to v3 in a VLAN or when the IGMP snooping version is set to v2 or v1 but SSM mapping is configured, the **display l2-multicast forwarding-table** command displays (S, G) entries.

Precautions

This command displays multicast forwarding entries in a VLAN only when at least one interface in the VLAN is in Up state.

Example

Display multicast forwarding entries in VLAN 10.

```
<Huawei> display l2-multicast forwarding-table vlan 10
VLAN ID : 10, Forwarding Mode : IP
--------------------------------------------------------------------------------
                 (Source, Group)     Interface            Out-Vlan
--------------------------------------------------------------------------------
                     Router-port     Ethernet2/0/0            10
                 (*, 225.1.1.6)     Ethernet2/0/0            10
                                    Ethernet1/0/2            10
             (*, 235.80.68.83)      Ethernet2/0/0            10
                                    Ethernet1/0/2            10
--------------------------------------------------------------------------------
Total Group(s): 2
```

Table 10-119 Description of the display l2-multicast forwarding-table command output

Item	Description
VLAN ID	VLAN ID of the forwarding entries.
Forwarding Mode	Multicast forwarding mode in the VLAN.
(Source, Group)	(S, G) entry, specifying the multicast source and multicast group. The Router-port field indicates a router port.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface	Outbound interface.
Out-Vlan	VLAN ID of packets.
Total Group(s)	Total number of multicast forwarding entries.

Related Topics

10.9.33 l2-multicast static-group

10.9.8 igmp-snooping enable (system view)

Function

The **igmp-snooping enable** command enables IGMP snooping globally.

The **undo igmp-snooping enable** command disables IGMP snooping globally.

By default, IGMP snooping is disabled globally and in a VLAN.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping runs on a Layer 2 device between a Layer 3 multicast device and hosts. By listening on the multicast protocol packets exchanged between the Layer 3 device and hosts, IGMP snooping maintains a multicast forwarding table to control Layer 2 multicast forwarding.

Before configuring IGMP snooping parameters, run the **igmp-snooping enable** command in the system view to enable IGMP snooping globally. Other IGMP snooping configuration commands can be used only after IGMP snooping is enabled globally.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **igmpsnooping enable vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command multiple times, all the configurations take effect.

Precautions

When you run the **undo igmp-snooping enable** command in the system view, the system displays a message, asking you whether to disable IGMP snooping globally. When you disable IGMP snooping globally, all the IGMP snooping configuration is deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping globally again, the router uses the default IGMP snooping configuration.

Example

Enable IGMP snooping globally.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.9 igmp-snooping enable (VLAN view)

10.9.9 igmp-snooping enable (VLAN view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a VLAN.

The **undo igmp-snooping enable** command disables IGMP snooping in a VLAN.

By default, IGMP snooping is disabled in a VLAN.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, IGMP snooping is disabled in a VLAN after IGMP snooping is enabled in the system view. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable** command in the VLAN view.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

After IGMP snooping is enabled in a VLAN, this function takes effect only on interfaces in this VLAN.

Example

Enable IGMP snooping in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.10 igmp-snooping group-limit

Function

The **igmp-snooping group-limit** command sets the maximum number of multicast entries that an interface can learn.

The **undo igmp-snooping group-limit** command cancels the limit on the number of multicast entries that an interface can learn.

By default, the maximum number of multicast entries that an interface can learn varies according to device models:

- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D and AR2204: 128
- AR2220E andAR2220: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240C: 1000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100: 2000
  - Configured with SRU100E: 2000

 Copyright © Huawei Technologies Co., Ltd.

  - Configured with SRU200: 2000
  - Configured with SRU200E: 2000
  - Configured with SRU400: 2000
- AR3600 series (SRUX5): 2000

Format

igmp-snooping group-limit *group-limit* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping group-limit vlan { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-limit	Specifies the maximum number of multicast groups that an interface can learn.	The value is an integer ranging from ● 1 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-Dand AR2204 ● 1 to 1000 for the AR2220, and AR2220E ● AR2204XE and AR2204XE-DC: 1 to 2000 ● AR2240C: 1 to 1000 ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 1000 – Configured with SRU60: 1 to 1000 – Configured with SRU80: 1 to 2000 – Configured with SRU100E: 1 to 2000 – Configured with SRU200: 1 to 2000 – Configured with SRU200E: 1 to 2000 – Configured with SRU400: 1 to 2000 ● 1 to 2000 for the AR3600 series (SRUX5)
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a VLAN. *vlan-id1* and *vlan-id2* identify a range of VLAN IDs.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Cancels the limit on the number of multicast groups that interfaces in all VLANs can learn.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **igmp-snooping group-limit** command to limit the number of multicast programs that a user can request. This configuration limits the multicast data traffic volume on the interface.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

During the configuration, if the number of multicast entries on the interface already exceeds the configured threshold, the number of multicast entries on the interface does not change and the interface cannot learn new multicast entries.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Configure Eth2/0/0 to learn a maximum of 10 IGMP snooping entries in VLAN 10, and IGMP snooping is enabled globally and in VLAN 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping group-limit 10 vlan 10
```

Configure Eth2/0/0 to learn a maximum of 50 IGMP snooping entries in VLANs 20 to 30, and IGMP snooping is enabled globally and in these VLANs.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping group-limit 50 vlan 20 to 30
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)

10.9.11 igmp-snooping group-policy (interface view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy on an interface.

The **undo igmp-snooping group-policy** command deletes a multicast group policy from an interface.

By default, no multicast group policy is available on an interface, and hosts connected to the interface can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*] **vlan** *vlan-id1* [**to** *vlan-id2*]

undo igmp-snooping group-policy vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL that limits the multicast groups that hosts in a VLAN can join.	The value is an integer ranging from 2000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer ranging from 1 to 3. • 1: IGMPv1 • 2: IGMPv2 • 3: IGMPv3
vlan *vlan-id1* [**to** *vlan-id2*]	Applies the multicast group policy to the specified VLANs on the interface.	*vlan-id1* and *vlan-id2* are integers that range 1 from 4094.
all	Deletes multicast groups policies in all VLANs from the interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a device with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message to the device, requesting to join the multicast group. The device checks whether the multicast group matches the ACL in the multicast group policy applied to the user VLAN on the interface:

- If so, the Layer 2 device allows the hosts in the VLANs to join the group and forwards the Report messages.
- If not, the Layer 2 device prevents the hosts from joining the group and drops the Report messages.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when both the following conditions are met:

- IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)** command.
- The ACL referenced in the policy exists and has filtering rules configured.

This command must reference an ACL. Before using this command, create an ACL and configure rules for the ACL. The ACL referenced in a group policy permits all multicast groups by default. Therefore, to allow interfaces in a VLAN to receive only multicast data sent to specific groups, use a **rule deny source any** rule with **permit** rules in the ACL. For details about ACL configuration commands, see **19.7 ACL Configuration Commands**.

A multicast group policy can also be configured in the VLAN view to control the multicast groups that users in the VLAN can join. A multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent users in VLAN 2 from joining multicast group 225.1.1.123.

```
<Huawei> system-view
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule deny source 225.1.1.123 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-acl-basic-2000] quit
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping group-policy 2000 vlan 2
```

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)
10.9.12 igmp-snooping group-policy (VLAN view)

10.9.12 igmp-snooping group-policy (VLAN view)

Function

The **igmp-snooping group-policy** command configures a multicast group policy in a VLAN.

The **undo igmp-snooping group-policy** command deletes the multicast group policy from a VLAN.

By default, no multicast group policy is available in a VLAN, and hosts in the VLAN can join any multicast group.

Format

igmp-snooping group-policy *acl-number* [**version** *version-number*]

undo igmp-snooping group-policy

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL used to restrict the range of groups users can join. A basic or advanced ACL can be used in a multicast group policy.	The value is an integer that ranges from 2000 to 3999.
version *version-number*	Applies the multicast group policy only to the IGMP messages of the specified version. If this parameter is not specified, the multicast group policy applies to all IGMP messages.	The value is an integer that ranges from 1 to 3. • 1: IGMPv1 • 2: IGMPv2 • 3: IGMPv3

 Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A multicast group policy controls the multicast programs that users can order on a router with IGMP snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. After the router receives the message, it checks whether the multicast group matches the multicast group policy applied to the VLAN. If so, the router drops the Report message and prohibits the user from joining the multicast group. If not, the router forwards the message, allowing the user to join the multicast group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when both the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- The ACL referenced in the policy exists and has filtering rules configured.

This command must reference an ACL. Before using this command, create an ACL and configure rules for the ACL. The ACL referenced in a group policy permits all multicast groups by default. Therefore, to allow interfaces in a VLAN to receive only multicast data sent to specific groups, use a **rule deny source any** rule with **permit** rules in the ACL. For details about ACL configuration commands, see **19.7 ACL Configuration Commands**.

A multicast group policy can also be configured in the interface view to control the multicast groups that users in one or more VLANs on the interface can join. A multicast group policy configured in the VLAN view controls the multicast groups that users in the VLAN can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 2 from joining group 225.1.1.123.

```
<Huawei> system-view
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule deny source 225.1.1.123 0
[Huawei-acl-basic-2000] quit
[Huawei] igmp-snooping enable
[Huawei] vlan 2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] igmp-snooping group-policy 2000
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.13 igmp-snooping lastmember-queryinterval

Function

The **igmp-snooping lastmember-queryinterval** command sets the last member query interval in a VLAN, that is, the interval at which Group-Specific Query messages are sent in the VLAN.

The **undo igmp-snooping lastmember-queryinterval** command restores the default last member query interval in a VLAN.

By default, Group-Specific Query messages are sent in a VLAN at intervals of 1 second.

Format

igmp-snooping lastmember-queryinterval *lastmember-queryinterval*

undo igmp-snooping lastmember-queryinterval

Parameters

Parameter	Description	Value
lastmember-queryinterval	Specifies the interval at which IGMP Group-Specific Query messages are sent.	The value is an integer that ranges from 1 to 5, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the last member query interval, you can:

 Copyright © Huawei Technologies Co., Ltd.

- Configure the router to send IGMP Group-Specific Query messages at intervals when the querier function is enabled.
- Change the aging time of multicast group member ports.

  When the router receives an IGMP Leave message from a host, the router starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last member query interval x Last member query count. The **igmp-snooping lastmember-queryinterval** command sets the last member query interval. The last member query count is set by the **igmp-snooping robust-count** command.

  If the router (querier) receives Report messages from other hosts within the aging time, it continues to maintain memberships of the multicast group. If the router does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The router sets the maximum response time field in the Group-Specific Query message to the configured last member query interval. Therefore, the maximum response time for Group-Specific Query messages is the same as the interval at which Group-Specific Query messages are sent.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- The IGMP message version is set to v2 or v3 messages in the VLAN. (Hosts running IGMPv1 do not send Leave messages when they leave a multicast group.)

Example

Set the last member query interval in VLAN 3 to 4 seconds.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping lastmember-queryinterval 4
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.17 igmp-snooping querier enable

10.9.21 igmp-snooping robust-count

 Copyright © Huawei Technologies Co., Ltd.

10.9.14 igmp-snooping learning

Function

The **igmp-snooping learning** command enables learning of multicast group memberships on an interface.

The **undo igmp-snooping learning** command disables learning of multicast group memberships on an interface.

By default, learning of multicast group memberships is enabled on an interface.

Format

igmp-snooping learning vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

undo igmp-snooping learning vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables learning of multicast group memberships in specified VLANs. The interface must have been added to the specified VLAN. *vlan-id1* [**to** *vlan-id2*] specifies the range of VLAN IDs. ● *vlan-id1*: specifies the first VLAN ID. ● **to** *vlan-id2*: specifies the last VLAN ID. If **to** *vlan-id2* is not specified, learning of multicast group memberships is enabled only in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters identify a range of VLANs.
all	Enables learning of multicast group memberships in all VLANs that an interface has joined.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A group member port is a user-side interface that connects to multicast group members. Group memberships can be learned dynamically or configured statically. After IGMP snooping is enabled in a VLAN, all interfaces in the VLAN are enabled to learn forwarding entries from multicast packets. An interface is identified as a dynamic group member port when it receives an IGMP Report message.

If users connected to an interface need to receive data of a fixed multicast group, the interface can be statically bound to the multicast group. In this case, run the **undo igmp-snooping learning** command on the interface to disable learning of group memberships. This reduces the system resources used for protocol packet exchange.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- The interface belongs to the specified VLANs.

Example

Disable learning of group memberships in VLAN 3 and VLAN 4 on Eth2/0/0.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] quit
[Huawei] vlan 4
[Huawei-vlan4] igmp-snooping enable
[Huawei-vlan4] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 3 to 4
[Huawei-Ethernet2/0/0] undo igmp-snooping learning vlan 3 to 4
```

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)

 Copyright © Huawei Technologies Co., Ltd.

10.9.15 igmp-snooping max-response-time

Function

The **igmp-snooping max-response-time** command sets the maximum response time for IGMP General Query messages in a VLAN.

The **undo igmp-snooping max-response-time** command restores the default maximum response time for IGMP General Query messages in a VLAN.

By default, the maximum response time for IGMP General messages in a VLAN is 10 seconds.

Format

igmp-snooping max-response-time *max-response-time*

undo igmp-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for IGMP General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve multicast forwarding performance. By setting the maximum response time for IGMP General Query messages, you can:

- Control the deadline for a host to send an IGMP Report message. When hosts are required to respond to IGMP General Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of IGMP messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the router receives a Report message, it starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query

 Copyright © Huawei Technologies Co., Ltd.

messages. The **igmp-snooping max-response-time** command sets the maximum response time. The General query count is set by the **igmp-snooping robust-count** command, and the general query interval is set by the **igmp-snooping query-interval** command.

The router sets the maximum response time field in General Query messages to the value set by the **igmp-snooping max-response-time** command.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

The maximum response time for General Query messages must be shorter than the interval at which General Query messages are sent. Otherwise, the router may delete multicast memberships that should not be deleted.

Example

Set the maximum response time for IGMP Query messages in VLAN 3 to 20 seconds.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping max-response-time 20
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.13 igmp-snooping lastmember-queryinterval

10.9.18 igmp-snooping query-interval

10.9.21 igmp-snooping robust-count

 Copyright © Huawei Technologies Co., Ltd.

10.9.16 igmp-snooping prompt-leave

Function

The **igmp-snooping prompt-leave** command enables the fast leave function in a VLAN so that member ports in the VLAN can fast leave multicast groups.

The **undo igmp-snooping prompt-leave** command disables the fast leave function in a VLAN.

By default, the fast leave function is disabled in a VLAN.

Format

igmp-snooping prompt-leave [**group-policy** *acl-number*]

undo igmp-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy	Specifies a multicast group policy that allows member ports to fast leave some multicast groups. Before using this parameter, create an ACL and configure filter rules in the ACL.	-
acl-number	Specifies the number of an ACL that defines a range of multicast groups. A basic or advanced ACL can be used.	The value is an integer that ranges from 2000 to 3999.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the router to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives an IGMP Leave message for the group. This function saves bandwidth and system

 Copyright © Huawei Technologies Co., Ltd.

resources because the router does not need to wait until the aging timer of the interface expires.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when all the following conditions are met:

- IGMP snooping is enabled in the VLAN using the **igmp-snooping enable (VLAN view)** command.
- IGMPv2 or IGMPv3 messages can be processed in the VLAN.
- An ACL has been created and has filtering rules configured if a multicast group policy is specified in the command. The default ACL rule of the router permits all multicast groups. Therefore, after configuring a rule that permits a specified multicast group, run the **rule deny source any** command to deny all the other multicast groups. For details about ACL configuration commands, see **19.7 ACL Configuration Commands** in "Security Commands."

Example

Allow member ports in VLAN 2 to fast leave all groups.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] igmp-snooping prompt-leave
```

Allow member ports in VLAN 3 to fast leave group 225.1.1.123.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule permit source 225.1.1.123 0
[Huawei-acl-basic-2000] rule deny source any
[Huawei-acl-basic-2000] quit
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping prompt-leave group-policy 2000
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

 Copyright © Huawei Technologies Co., Ltd.

10.9.17 igmp-snooping querier enable

Function

The **igmp-snooping querier enable** command enables the IGMP snooping querier function in a VLAN.

The **undo igmp-snooping querier enable** command disables the IGMP snooping querier function in a VLAN.

By default, the IGMP snooping querier function is disabled in a VLAN.

Format

igmp-snooping querier enable

undo igmp-snooping querier enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an IGMP-capable network, a Layer 3 multicast device functions as a querier to send IGMP Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run IGMP or it uses only static multicast forwarding entries, it cannot function as a querier. You can enable IGMP snooping querier on the downstream Layer 2 device. Then the Layer 2 device can act as a querier to send IGMP Query messages.

On a Layer 2 network without Layer 3 devices, multicast sources are connected to Layer 2 devices. IGMP snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations as required on your network:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.
- Run the **igmp-snooping robust-count** command to set the number of times Query messages are sent.

Configuration Impact

The IGMP snooping querier does not participate in IGMP querier election. However, the IGMP snooping querier on an IGMP-capable multicast network may affect the election result, because the Query messages sent by the IGMP snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the IGMP snooping querier function is not recommended on an IGMP-capable multicast network.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- The IGMP snooping querier function cannot be enabled in a VLAN if the corresponding Layer 3 VLANIF interface has Layer 3 multicast functions (such as IGMP and PIM) enabled.

Example

Enable the querier function in VLAN 3.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping querier enable
Warning: Please confirm that no other querier is configured on the network, otherwise this command may
cause querier re-election, continue? [Y/N]:y
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.4 display igmp-snooping querier
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.13 igmp-snooping lastmember-queryinterval
10.9.21 igmp-snooping robust-count
10.9.18 igmp-snooping query-interval

10.9.18 igmp-snooping query-interval

Function

The **igmp-snooping query-interval** command sets the general query interval in a VLAN, that is, the interval at which IGMP General Query messages are sent in the VLAN.

The **undo igmp-snooping query-interval** command restores the default general query interval in a VLAN.

 Copyright © Huawei Technologies Co., Ltd.

By default, the general query interval is 60 seconds.

Format

igmp-snooping query-interval *query-interval*

undo igmp-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which IGMP General Query messages are sent.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the general query interval, you can:

- Configure the router to send IGMP General Query messages at intervals to maintain memberships of interfaces. When a shorter interval is configured, the router is more sensitive to multicast membership changes, but more bandwidth and system resources are consumed.
- Change the aging time of multicast member ports.

  When receiving an IGMP Report message from a host, the router starts the aging timer for the multicast member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping query-interval** command sets the general query interval. The general query count is set by the **igmp-snooping robust-count** command, and the maximum response time for General Query messages is set by the **igmp-snooping max-response-time** command.

NOTE

The default *interval* value in this command is 60 seconds, which is different than the default value 125 seconds defined by RFC documents. A Huawei querier and a non-Huawei querier must send IGMP general query messages at the same interval.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the router may delete multicast memberships that should not be deleted.

Example

Set the general query interval in VLAN 3 to 100 seconds.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping query-interval 100
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.15 igmp-snooping max-response-time
10.9.17 igmp-snooping querier enable
10.9.21 igmp-snooping robust-count

10.9.19 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command enables suppression of IGMP Report and Leave messages in a VLAN.

The **undo igmp-snooping report-suppress** command disables suppression of IGMP Report and Leave messages in a VLAN.

By default, IGMP Report and Leave message suppression is disabled in a VLAN.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages on the same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.
- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Leave messages from the member hosts.

After Report message suppression is enabled on a Layer 2 device, the device forwards only one IGMP Membership Report message to the upstream device in the following scenarios:

- When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream can create or maintain the matching forwarding entry based on the Report message.
- When the last member of a multicast group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry.

This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Configuration Impact

- The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.
- IGMP message suppression cannot be configured in a VLAN if the corresponding VLANIF interface has Layer 3 multicast function (such as IGMP and PIM) enabled.
- The device can suppress duplicate Report messages even when IGMP message suppression is disabled. The default suppression time is 10 seconds. To change

 Copyright © Huawei Technologies Co., Ltd.

the suppression time, run the **igmp-snooping suppress-time** *suppress-time* command. If the *suppress-time* is set to 0, all the membership packets are forwarded immediately.

Example

Enable suppression of Report and Leave messages in VLAN 2.

```
<Huawei> system view
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] igmp-snooping report-suppress
```

Related Topics

10.9.1 display igmp-snooping
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.17 igmp-snooping querier enable
10.9.31 igmp-snooping suppress-time

10.9.20 igmp-snooping require-router-alert

Function

The **igmp-snooping require-router-alert** command configures the router to drop the IGMP messages without the Router-Alert option in the IP header received from a VLAN.

The **undo igmp-snooping require-router-alert** command restores the default configuration.

By default, the router does not check the Router-Alert option of IGMP messages and processes all the received IGMP messages, regardless of whether they carry the Router-Alert option in the IP header.

Format

igmp-snooping require-router-alert

undo igmp-snooping require-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the router does not check whether IGMP messages contain the Router-Alert option and sends all the IGMP messages to the upper-layer routing protocol. Discarding IGMP messages without the Router-Alert option improves device performance, reduces cost, and enhances security of the upper-layer routing protocol. After the **igmp-snooping require-router-alert** command is executed, the router checks each IGMP message for the Router-Alert option and discards those IGMP messages without this option.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Configure the router to forward only the IGMP messages with the Router-Alert option in the IP header received from VLAN 3.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping require-router-alert
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.21 igmp-snooping robust-count

Function

The **igmp-snooping robust-count** command sets the IGMP robustness variable in a VLAN, which specifies how many times IGMP Query messages are sent.

The **undo igmp-snooping robust-count** command restores the default IGMP robustness variable in a VLAN.

By default, the robustness variable in a VLAN is 2.

 Copyright © Huawei Technologies Co., Ltd.

Format

igmp-snooping robust-count *robust-count*

undo igmp-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the IGMP robustness variable in a VLAN.	The value is an integer that ranges from 2 to 5.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting IGMP snooping parameters helps improve multicast forwarding performance. By setting the IGMP robustness variable, you can:

- Specify the number of times the querier sends a Group-Specific Query message, which prevents packet loss on the network.

  When receiving an IGMP Leave message for a multicast group, the router sends a Group-Specific Query message certain times (specified by the IGMP robustness variable) to check whether this group has any other members. If the quality of transmission links is low, increase the IGMP robustness variable.
- Change the aging time of multicast group member ports.

  When receiving an IGMP Report message from a host, the router starts the aging timer for the member port. The aging time is calculated using the following formula: Aging time = IGMP robustness variable x General query interval + Maximum response time for General Query messages. The **igmp-snooping robust-count** command sets the general query count.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **igmp-snooping query-interval** command to set the interval at which General Query messages are sent.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **igmp-snooping lastmember-queryinterval** command to set the interval at which Group-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

Example

Set the IGMP robustness variable to 5 in VLAN 3.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping robust-count 5
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.13 igmp-snooping lastmember-queryinterval

10.9.15 igmp-snooping max-response-time

10.9.18 igmp-snooping query-interval

10.9.22 igmp-snooping router-aging-time

Function

The **igmp-snooping router-aging-time** command sets the aging time of dynamic router ports in a VLAN.

The **undo igmp-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VLAN.

By default, the aging time of dynamic router ports in a VLAN is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

igmp-snooping router-aging-time *router-aging-time*

undo igmp-snooping router-aging-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
router-aging-time	Specifies the aging time of dynamic router ports in a VLAN.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on the network, it takes a longer time to transmit Query messages from the IGMP querier to the router. If a router port on the router ages in this period, the router does not send Report or Leave messages to router ports. As a result, multicast data forwarding may be interrupted. Therefore, set a long aging time for the router port on an unstable network.

When a dynamic router port on the router receives an IGMP Query message or a PIM Hello message, the router resets the aging time of the router port.

- If the router port receives an IGMP Query message, the router sets the remaining aging time of the interface to the configured value.
- If the router port receives a PIM Hello message and the holdtime value in the Hello message is larger than the remaining aging time of the router port, the router sets the aging time of the interface to the holdtime value. If the holdtime value is smaller than the remaining aging time of the router port, the router does not change the aging time of the router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in VLAN 3 to 300 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping router-aging-time 300
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.23 igmp-snooping router-learning (VLAN view)

Function

The **igmp-snooping router-learning** command enables router port learning in a VLAN.

The **undo igmp-snooping router-learning** command disables router port learning in a VLAN.

By default, router port learning is enabled in a VLAN.

Format

igmp-snooping router-learning

undo igmp-snooping router-learning

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router port is located on a Layer 2 device and connects to an upstream Layer 3 device (a multicast router or Layer 3 switch). A router running IGMP snooping considers an interface as a dynamic router port when the interface receives an IGMP General Query message with any source IP address except 0.0.0.0 or a PIM Hello message. If the router does not need to receive Query messages or PIM Hello messages from a VLAN, disable router port learning in the VLAN. A router port provides the following functions:

 Copyright © Huawei Technologies Co., Ltd.

- Receives multicast data from the upstream device.
- Forwards IGMP Report/Leave messages. IGMP Report/Leave messages received in a VLAN are forwarded only to router ports in the VLAN.

By default, router port learning is enabled on an interface. To prevent interfaces in a VLAN from becoming a router port, disable router port learning in the VLAN.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

The router does not listen on IGMP Query messages in a VLAN after router port learning is disabled in the VLAN. To ensure normal multicast forwarding in the VLAN, run the **igmp-snooping static-router-port** command to configure a static router port.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Disable router port learning in VLAN 3.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] undo igmp-snooping router-learning
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.30 igmp-snooping static-router-port

10.9.24 igmp-snooping send-query enable

Function

The **igmp-snooping send-query enable** command enables the router to send IGMP General Query messages to non-router ports when receiving topology change events.

The **undo igmp-snooping send-query enable** command disables the router from sending IGMP General Query messages to non-router ports.

By default, the router does not send IGMP General Query messages to non-router ports when receiving topology change events.

 Copyright © Huawei Technologies Co., Ltd.

Format

igmp-snooping send-query enable

undo igmp-snooping send-query enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network topology changes, the router receives a topology change event. By default, the router does not send IGMP General Query messages in this case. A network topology change triggers recalculation of the Multiple Spanning Tree Protocol (MSTP), but multicast data packets cannot be switched to the new path immediately. To enable multicast data flows to be switched to the new forwarding path immediately after a network topology change, configure the router to send IGMP General Query messages upon topology changes.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

This command is used on a ring network. When the ring network topology changes, the router sends IGMP General Query messages with source IP address 192.168.0.1. When this address has been occupied by another device on the network, run the **igmp-snooping send-query source-address** command to set the source IP address to 0.0.0.0.

Precautions

Use this command only when MSTP is enabled on the network.

Example

Configure the router to send IGMP General Query messages upon topology changes.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] igmp-snooping send-query enable
```

Related Topics

10.9.6 display igmp-snooping statistics
10.9.8 igmp-snooping enable (system view)
10.9.25 igmp-snooping send-query source-address

10.9.25 igmp-snooping send-query source-address

Function

The **igmp-snooping send-query source-address** command sets the source IP address of IGMP General Query messages.

The **undo igmp-snooping send-query source-address** command restores the default source IP address of IGMP General Query messages.

By default, the source IP address of IGMP General Query messages is 192.168.0.1.

Format

igmp-snooping send-query source-address *ip-address*

undo igmp-snooping send-query source-address

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address of IGMP General Query messages.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 device sends two types of IGMP General Query messages:

- IGMP General Query messages sent by the querier when the querier function is enabled using the **igmp-snooping querier enable** command.
- IGMP General Query messages that the Layer 2 device sends after receiving Layer 2 topology change events (configured using the **igmp-snooping send-query enable** command).

By default, IGMP General Query messages sent from a Layer 2 device use the source IP address 192.168.0.1. When this IP address is used by another device on

the network, run the **igmp-snooping send-query source-address** command to change the source IP address of IGMP General Query messages.

When multiple Layer 2 devices exist on a shared network, you can set source IP addresses of IGMP Query messages to identify the devices. For example, when multiple devices with different performance need to participate in querier election, you must configure a different source IP address of IGMP Query messages for each device.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Example

Set the source IP address of IGMP Query messages sent by the router to 192.168.0.2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] igmp-snooping send-query source-address 192.168.0.2
```

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.17 igmp-snooping querier enable

10.9.24 igmp-snooping send-query enable

10.9.26 igmp-snooping send-router-alert

Function

The **igmp-snooping send-router-alert** command configures the router to send IGMP messages with the Router-Alert option in the IP header to a VLAN.

The **undo igmp-snooping send-router-alert** command configures the router to send IGMP messages without the Router-Alert option in the IP header to a VLAN.

By default, the router sends IGMP messages with the Router-Alert option in the IP header.

Format

igmp-snooping send-router-alert

undo igmp-snooping send-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the router sends IGMP messages with the Router-Alert option. If some devices in the same VLAN as the router can process only the IGMP messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the router to send IGMP messages without the Router-Alert option.

The router adds the Router-Alert option only to locally originated IGMP messages and does not add this option to IGMP messages received from other devices.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

Example

Configure the router to send IGMP messages that do not contain the Router-Alert option in the IP header to VLAN 3.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] undo igmp-snooping send-router-alert
```

Related Topics

10.9.1 display igmp-snooping

10.9.2 display igmp-snooping configuration

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.27 igmp-snooping ssm-mapping

Function

The **igmp-snooping ssm-mapping** command configures the mapping between a multicast group and a multicast source in a VLAN.

The **undo igmp-snooping ssm-mapping** command deletes the mapping between a multicast group and a multicast source in a VLAN.

By default, no mappings between multicast groups and multicast sources exist in a VLAN.

Format

igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

undo igmp-snooping ssm-mapping *group-address* { *group-mask* | *mask-length* } *source-address*

Parameters

Parameter	Description	Value
group-address	Specifies the IP address of a multicast group.	The value is in dotted decimal notation, and the value range is specified by the **igmp-snooping ssm-policy** command.
group-mask	Specifies the mask of the multicast group address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the multicast group address.	The value is an integer that ranges from 4 to 32.
source-address	Specifies the IP address of the multicast source mapped to a multicast group.	The value is in dotted decimal notation.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSM mapping mechanism converts IGMPv1 and IGMPv2 Report messages into messages with (S, G) information. This mechanism enables hosts that do not support IGMPv3 to work with SSM. To use this mechanism, enable SSM mapping and configure mappings between a multicast group G and multicast sources such

 Copyright © Huawei Technologies Co., Ltd.

as S1, S2 on the Layer 2 device connected to user hosts. When the Layer 2 device receives IGMPv1 and IGMPv2 Report messages for a multicast group, it checks the group address of the messages. If the group address is in the SSM group range, the Layer 2 device converts the messages into one or more IGMPv3 IS_IN (S1, S2...) messages with the group address G.

Prerequisites

- IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

Before configuring the mapping between a multicast group and a multicast source:

- IGMP snooping has been enabled in the specified VLAN using the **igmp-snooping enable (VLAN view)** command.
- The IGMP message version is set to IGMPv3 using the **igmp-snooping version** command in the VLAN.
- SSM mapping has been enabled using the **igmp-snooping ssm-mapping enable** command.
- An SSM group policy has been configured using the **igmp-snooping ssm-policy** command in the VLAN to add the multicast group address to the SSM group range. This prerequisite is required when the multicast group address is an any-source multicast (ASM) address.

Example

Map multicast groups 238.1.1.1 through 238.1.1.255 to multicast source 10.1.1.1 in VLAN 10.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 10
[Huawei-vlan10] igmp-snooping enable
[Huawei-vlan10] igmp-snooping version 3
[Huawei-vlan10] igmp-snooping ssm-mapping enable
[Huawei-vlan10] igmp-snooping ssm-mapping 238.1.1.0 24 10.1.1.1
```

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.28 igmp-snooping ssm-mapping enable
10.9.29 igmp-snooping ssm-policy
10.9.32 igmp-snooping version

10.9.28 igmp-snooping ssm-mapping enable

Function

The **igmp-snooping ssm-mapping enable** command enables Source-Specific Multicast (SSM) mapping in a VLAN.

The **undo igmp-snooping ssm-mapping enable** command disables SSM mapping in a VLAN.

By default, SSM mapping is disabled in a VLAN.

Format

igmp-snooping ssm-mapping enable

undo igmp-snooping ssm-mapping enable

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an SSM network, hosts running IGMPv1 or IGMPv2 cannot select multicast sources when they join a multicast group. To provide SSM services for these hosts, enable SSM mapping on the Layer 2 devices connected to the hosts.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Run the **igmp-snooping ssm-mapping** command to configure group-source mappings.

Precautions

- If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.
- SSM mapping is applicable only to the VLANs where IGMP snooping can process IGMPv3 messages. To set the IGMP message version to v3, use the **igmp-snooping version** command in the VLAN.
- If the multicast group address is an Any-Source Multicast (ASM) address, configure an SSM group policy to add the multicast group address to the SSM group range using the **igmp-snooping ssm-policy** command in the VLAN view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable SSM mapping in VLAN 10.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 10
[Huawei-vlan10] igmp-snooping enable
[Huawei-vlan10] igmp-snooping version 3
[Huawei-vlan10] igmp-snooping ssm-mapping enable
```

Related Topics

10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)
10.9.27 igmp-snooping ssm-mapping
10.9.29 igmp-snooping ssm-policy
10.9.32 igmp-snooping version

10.9.29 igmp-snooping ssm-policy

Function

The **igmp-snooping ssm-policy** command configures an SSM group policy in a VLAN to specify the range of SSM groups.

The **undo igmp-snooping ssm-policy** command deletes the SSM group policy from a VLAN.

By default, no SSM group policy is available in a VLAN.

Format

igmp-snooping ssm-policy *basic-acl-number*

undo igmp-snooping ssm-policy

Parameters

Parameter	Description	Value
basic-acl-number	Specifies the number of a basic ACL that defines the range of SSM groups.	The value is an integer that ranges from 2000 to 2999.

Views

VLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

SSM allows multicast group addresses in the range of 232.0.0.0 to 232.255.255.255. If hosts join multicast groups out of this range or they are allowed to join only some of multicast groups in the range, configure an SSM group range for the hosts.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Enable SSM mapping and configure SSM mapping in the VLAN. The multicast group in the SSM mapping must be in the SSM group range.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

This command must reference an ACL. Before using this command, create an ACL and configure rules for the ACL. By default, the ACL applied to an SSM group policy denies all multicast groups. Therefore, to exclude specific group addresses from the SSM group address range, use a **rule permit source any** rule with **deny** rules in the ACL. For details about ACL configuration commands, see **19.7 ACL Configuration Commands**.

Example

Specify multicast group 225.1.1.123 as an SSM group in VLAN 3.

```
<Huawei> system-view
[Huawei] acl number 2000
[Huawei-acl-basic-2000] rule permit source 225.1.1.123 0
[Huawei-acl-basic-2000] quit
[Huawei] igmp-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] igmp-snooping enable
[Huawei-vlan3] igmp-snooping ssm-policy 2000
```

Related Topics

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.27 igmp-snooping ssm-mapping

10.9.28 igmp-snooping ssm-mapping enable

10.9.30 igmp-snooping static-router-port

Function

The **igmp-snooping static-router-port** command configures an interface as a static router port in specified VLANs.

 Copyright © Huawei Technologies Co., Ltd.

The **undo igmp-snooping static-router-port** command cancels the router port configuration in specified VLANs.

By default, an interface is not a static router port.

Format

igmp-snooping static-router-port vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo igmp-snooping static-router-port vlan { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>	Specifies VLAN IDs. This parameter specifies in which VLANs the current interface functions as a router port. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface functions as a router port only in the VLAN specified by *vlan-id1*.	The value is an integer that ranges from 1 to 4094. The value of vlan-id2 must be greater than the value of vlan-id1. The vlan-id1 and vlan-id2 parameters identify a range of VLANs.
all	Cancels the static router port configuration in all VLANs on the interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to forward IGMP Report/Leave messages for a long time, configure the interface as a static router port.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

This command takes effect only when the interface is added to the specified VLANs.

Example

Configure Eth2/0/0 as a static router port in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] igmp-snooping static-router-port vlan 2
```

Related Topics

10.9.5 display igmp-snooping router-port
10.9.8 igmp-snooping enable (system view)

10.9.31 igmp-snooping suppress-time

Function

The **igmp-snooping suppress-time** command sets the IGMP message suppression time in a VLAN.

The **undo igmp-snooping suppress-time** command restores the default IGMP message suppression time in a VLAN.

By default, the IGMP message suppression time is 10 seconds.

Format

igmp-snooping suppress-time *suppress-time*

undo igmp-snooping suppress-time

Parameters

Parameter	Description	Value
suppress-time	Specifies the IGMP message suppression time in a VLAN.	The value is an integer that ranges from 0 to 300, in seconds. The value 0 indicates that IGMP messages are not suppressed.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To reduce the IGMP messages sent from a Layer 2 device to the upstream Layer 3 device and protects the Layer 3 device from attacks, enable the Layer 2 device to suppress IGMP Report and IGMP Leave messages sent by hosts in a VLAN. After this function is enabled, the Layer 2 device processes IGMP Report and IGMP Leave messages as follows:

- After receiving an IGMP Report/Leave message and forwarding the message, the Layer 2 device does not forward the same type of messages to the router port within the suppression time.
- If the Layer 2 device receives an IGMP General Query message or Group-Specific message, it does not suppress the first IGMP Report message that responds to the General Query message. In addition, the Layer 2 device resets the suppression timer when receiving the first IGMP Report message.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Follow-up Procedure

Run the **igmp-snooping max-response-time** command to set the maximum response time for General Query messages. It is recommended that the suppression time be the same as the maximum response time for IGMP Query messages in a VLAN.

Precautions

The configuration takes effect only after you run the **igmp-snooping enable (VLAN view)** command to enable IGMP snooping in the VLAN.

The configured suppression time is invalid for IGMPv3 messages.

Example

Set the IGMP message suppression time in VLAN 2 to 15 seconds.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] igmp-snooping suppress-time 15
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)

 Copyright © Huawei Technologies Co., Ltd.

10.9.15 igmp-snooping max-response-time

10.9.32 igmp-snooping version

Function

The **igmp-snooping version** command configures the version of IGMP messages that IGMP snooping can process in a VLAN.

The **undo igmp-snooping version** command restores the default IGMP message version.

By default, IGMP snooping can process IGMPv1 and IGMPv2 messages in a VLAN.

Format

igmp-snooping version *version*

undo igmp-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of IGMP messages that can be processed in a VLAN.	The value is an integer ranging from 1 to 3. • 1: indicates that IGMP snooping processes only IGMPv1 messages. • 2: indicates that IGMP snooping processes IGMPv1 and IGMPv2 messages. • 3: indicates that IGMP snooping processes IGMPv1, IGMPv2, and IGMPv3 messages.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The IGMP protocol maintains group memberships between Layer 3 multicast devices and hosts. IGMP has three versions: v1, v2, and v3. This command specifies the version of IGMP messages that IGMP snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If IGMP is not enabled on the Layer 3 multicast device, configure the IGMP message version on the Layer 2 device to be later than or equal to the version running on downstream hosts.

When hosts in a VLAN run different IGMP versions, run the **igmp-snooping version** command to enable the Layer 2 device to process IGMP messages sent from all the hosts.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

If IGMP snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until IGMP snooping is enabled in the VLAN. To enable IGMP snooping in a VLAN, run the **igmp-snooping enable (VLAN view)** command.

When the IGMP message version is changed from IGMPv3 to IGMPv2, the system deletes all the dynamic IGMP snooping entries when the aging time is reached and processes static IGMP snooping entries as follows:

- Does not delete static entries that have only multicast groups but not multicast sources.
- Deletes the static entries that have both multicast groups and multicast sources. When the IGMP message version is restored to IGMPv3, the system restores these entries.

Example

Set the version of the IGMP messages that can be processed by IGMP snooping to IGMPv1 in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] igmp-snooping enable
[Huawei-vlan2] igmp-snooping version 1
```

Related Topics

10.9.1 display igmp-snooping
10.9.2 display igmp-snooping configuration
10.9.8 igmp-snooping enable (system view)
10.9.9 igmp-snooping enable (VLAN view)

10.9.33 l2-multicast static-group

Function

The **l2-multicast static-group** command configures static group memberships on an interface.

The **undo l2-multicast static-group** command deletes static group memberships from an interface.

By default, no static group membership is configured on an interface.

Format

Configure a single static multicast group:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address* **vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Configure a series of static multicast groups:

l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address** *group-ip-address1* **to** *group-ip-address2* **vlan** *vlan-id*

undo l2-multicast static-group [**source-address** *source-ip-address*] **group-address all vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
source-address *source-ip-address*	Specifies the IP address of a multicast source.	The value of *source-ip-address* can be any Class A, Class B, or Class C address, in dotted decimal notation.
group-address *group-ip-address*	Specifies the IP address of a multicast group.	The value of *group-ip-address* ranges from 224.0.1.0 to 239.255.255.255 in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Specifies the VLANs that the interface belongs to. *vlan-id1* [**to** *vlan-id2*] specifies a range of VLAN IDs. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. If **to** *vlan-id2* is not specified, the interface is bound only to the multicast group in the VLAN specified by *vlan-id1*.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.
all	Deletes all group memberships from the interface. ● In **group-address all**, **all** indicates that the interface is removed from all multicast groups. ● In **vlan** { **all** | {*vlan-id1* [**to** *vlan-id2*] } &<1-10> }, **all** indicates that the interface is removed from multicast groups in all VLANs.	-
group-ip-address1 **to** *group-ip-address2*	Configures multiple static group memberships on the interface. *group-ip-address1* and *group-ip-address2* identify a range of multicast group addresses.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation. The values of *group-ip-address1* and *group-ip-address2* must be in the same network segment (with a 24-bit mask).
vlan *vlan-id*	Specifies the VLANs that the interface belongs to.	The values of *vlan-id* are integers that range from 1 to 4094.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocol protocols, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can receive multicast data of the multicast group for a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

IGMP snooping has been enabled globally using the **igmp-snooping enable (system view)** command.

Precautions

The configuration takes effect only when both the following conditions are met:

- IGMP snooping is enabled in the specified VLANs using the **igmp-snooping enable (VLAN view)**.
- The specified VLANs have been created and the interface has been added to these VLANs.
- The reserved group address cannot be used as the static multicast group address.

Example

Configure a static multicast group 224.1.1.1 on Eth2/0/0 in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/0] l2-multicast static-group group-address 224.1.1.1 vlan 2
```

Configure static multicast groups 224.1.1.1 to 224.1.1.3 on Eth2/0/0 in VLAN 2.

```
<Huawei> system-view
[Huawei] igmp-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/0] l2-multicast static-group group-address 224.1.1.1 to 224.1.1.3 vlan 2
```

Delete static multicast group 224.1.1.1 from Eth2/0/0 in all VLANs.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo l2-multicast static-group group-address 224.1.1.1 vlan all
```

Related Topics

10.9.3 display igmp-snooping port-info

10.9.7 display l2-multicast forwarding-table

10.9.8 igmp-snooping enable (system view)

10.9.9 igmp-snooping enable (VLAN view)

10.9.32 igmp-snooping version

10.9.34 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the router to drop unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

By default, the router broadcasts unknown multicast flows in a VLAN.

NOTE

AR129CV, AR129CVW, AR129CGVW-L, AR2204-24GE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, AR2204XE-DC, AR2220L, AR2220E and AR2240C do not support this command.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are multicast data flows that match no entry in the multicast forwarding table. By default, the router broadcasts unknown multicast

flows in the corresponding VLAN. You can use the **multicast drop-unknown** command to configure the router to drop unknown multicast flows, which reduces instant bandwidth usage compared with the broadcast mode.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown multicast packets are dropped, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

Example

Drop unknown multicast flows in VLAN 10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] multicast drop-unknown
```

10.9.35 reset igmp-snooping group

Function

The **reset igmp-snooping group** command deletes dynamic group memberships learned by IGMP snooping.

Format

reset igmp-snooping group { **all** | **vlan** { **all** | *vlan-id* } }

Parameters

Parameter	Description	Value
all	Deletes all dynamic group memberships learned by IGMP snooping.	-
vlan { **all** | *vlan-id* }	Deletes the dynamic group memberships of a specified VLAN. If **all** is specified, the system deletes IGMP dynamic group memberships of all VLANs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When multicast groups on a network change, the router generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the router to generate new multicast forwarding entries immediately, use the **reset igmp-snooping group** command to delete existing group memberships.

Precautions

NOTICE

Deleting group memberships in a VLAN temporarily interrupts multicast forwarding in the VLAN. The router generates new forwarding entries only when receiving IGMP Report messages from hosts in the VLAN. The hosts can then receive multicast data.

This command cannot delete static group memberships.

This command is valid only for VLANs with IGMP snooping enabled and is invalid for a VLAN if IGMP is enabled on the corresponding VLANIF interface.

Example

Delete all dynamic group memberships learned by IGMP snooping.

```
<Huawei> reset igmp-snooping group all
```

Delete dynamic group memberships in VLAN 3.

```
<Huawei> reset igmp-snooping group vlan 3
```

Related Topics

10.9.3 display igmp-snooping port-info

10.9.36 reset igmp-snooping statistics

Function

The **reset igmp-snooping statistics** command clears IGMP snooping statistics.

Format

reset igmp-snooping statistics { **all** | **vlan** { **all** | *vlan-id* } }

Parameters

Parameter	Description	Value
all	Clears all the IGMP snooping statistics.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan { **all** | *vlan-id* }	Clears IGMP snooping statistics of a specified VLAN. If **all** is specified, the system clears IGMP snooping statistics of all VLANs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To analyze the IGMP snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display igmp-snooping statistics** command to view the IGMP snooping statistics.

Precautions

NOTICE

The cleared IGMP snooping statistics cannot be restored.

Example

Clear IGMP snooping statistics of VLAN 2.

```
<Huawei> reset igmp-snooping statistics vlan 2
```

Related Topics

10.9.6 display igmp-snooping statistics

10.10 MLD Snooping Configuration Commands

NOTE

Only AR2200&AR3200&AR3600 series support MLD Snooping.

Only the 8FE1GE, 24GE and 24ES2GP cards support MLD Snooping.

10.10.1 display mld-snooping

Function

The **display mld-snooping** command displays the MLD snooping running parameters in a VLAN.

Format

display mld-snooping [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the MLD snooping running parameters in a specified VLAN. If this parameter is not specified, the system displays the MLD running parameters in all VLANs with MLD snooping configured.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use this command to view the MLD snooping running parameters. If you run this command after configuring MLD snooping parameters, the command displays the configured parameter values.

To view the MLD snooping configuration, run the **display mld-snooping configuration** command.

Precautions

This command can display the MLD snooping configuration in a VLAN only when the VLAN is in Up state (at least one interface in the VLAN is in Up state) and has MLD snooping enabled.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the MLD snooping running parameters in VLAN 3.

```
<Huawei> display mld-snooping vlan 3
MLD Snooping Vlan Information for VLAN 3
  MLD Snooping is Enabled
  MLD Version is Set to default 1
  MLD Query Interval is Set to default 60
  MLD Max Response Interval is Set to default 10
  MLD Robustness is Set to default 2
  MLD Last Member Query Interval is Set to default 1
  MLD Router Port Aging Interval is Set to 180s or holdtime in hello
  MLD Filter Group-Policy is Set to default : Permit All
  MLD Prompt Leave Disable
  MLD Router Alert is Not Required
  MLD Send Router Alert Enable
  MLD Snooping Querier Disable
```

Table 10-120 Description of the display mld-snooping vlan 3 command output

Item	Description
MLD Snooping Vlan Information for VLAN 3	The following information displayed is the MLD snooping running parameters in VLAN 3.
MLD Snooping is Enabled	MLD snooping is enabled in the VLAN. By default, MLD snooping is disabled in a VLAN. MLD snooping can be enabled using the **mld-snooping enable** command.
MLD Version is Set to default 1	Version of MLD messages that can be processed in the VLAN. In this example, the default version 1 is displayed. This parameter is configured using the **mld-snooping version** command.
MLD Query Interval is Set to default 60	Interval at which MLD General Query messages are sent. In this example, the default value (60 seconds) is displayed. This parameter is configured using the **mld-snooping query-interval** command.
MLD Max Response Interval is Set to default 10	Maximum response time for MLD General Query messages. In this example, the default value (10 seconds) is displayed. This parameter is configured using the **mld-snooping max-response-time** command.
MLD Robustness is Set to default 2	MLD robustness variable. In this example, the default value 2 is displayed. This parameter is configured using the **mld-snooping robust-count** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MLD Last Member Query Interval is Set to default 1	Interval at which MLD Group-Specific Query messages are sent. In this example, the default value (1 second) is displayed. This parameter is configured using the **mld-snooping last-listener-query-interval** command.
MLD Router Port Aging Interval is Set to 180s or holdtime in hello	Aging time of a router port. In this example, the default value (180 seconds or the holdtime value contained in PIM Hello messages) is displayed. This parameter is configured using the **mld-snooping router-aging-time** command.
MLD Filter Group-Policy is Set to default : Permit All	Multicast group policy. In this example, the default configuration is displayed. That is, no policy is configured. A multicast group policy is configured using the **mld-snooping group-policy (VLAN view)** command.
MLD Prompt Leave Disable	The prompt leave function is disabled for interfaces in the VLAN (default configuration). The prompt leave function can be enabled using the **mld-snooping prompt-leave** command.
MLD Router Alert is Not Required	The router does not require that MLD messages received from the VLAN contain the Router-Alert option in the IP header (default configuration). The router can be configured to discard MLD messages without the Router-Alert option using the **mld-snooping require-router-alert** command.
MLD Send Router Alert Enable	The router sends MLD messages with the Router-Alert option to the VLAN (default configuration). The router can be configured to send MLD messages with the Router-Alert option using the **mld-snooping send-router-alert** command.
MLD Snooping Querier Disable	MLD snooping querier is disabled (default configuration). MLD snooping querier can be enabled using the **mld-snooping querier enable** command.

Related Topics

10.10.6 mld-snooping enable
10.10.8 mld-snooping group-policy (VLAN view)
10.10.9 mld-snooping last-listener-query-interval
10.10.10 mld-snooping max-response-time

10.10.11 mld-snooping prompt-leave
10.10.12 mld-snooping querier enable
10.10.14 mld-snooping require-router-alert
10.10.15 mld-snooping robust-count
10.10.16 mld-snooping router-aging-time
10.10.19 mld-snooping send-router-alert
10.10.24 mld-snooping version

10.10.2 display mld-snooping configuration

Function

The **display mld-snooping configuration** command displays the MLD snooping configuration.

Format

display mld-snooping [**vlan** *vlan-id*] **configuration**

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the MLD snooping configuration in a specified VLAN. If this parameter is not specified, the system displays the MLD snooping configuration in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays only the MLD snooping configuration so that you can check whether the MLD snooping configuration made in the system is proper.

To check all MLD snooping running parameters, run the **display mld-snooping** command.

Precautions

Before running the **display mld-snooping configuration** command, run the **mld-snooping enable** commands to enable IGMP snooping globally and in the VLAN. Otherwise, no information is displayed.

Example

Display the MLD snooping configuration in all VLANs.

```
<Huawei> display mld-snooping configuration
 MLD Snooping Configuration for VLAN 20
    mld-snooping enable
    mld-snooping version 2
 MLD Snooping Configuration for VLAN 90
    mld-snooping enable
```

Table 10-121 Description of the display mld-snooping configuration command output

Item	Description
MLD Snooping Configuration for VLAN	The following information displayed is the MLD snooping configuration in a specific VLAN.
mld-snooping enable	MLD snooping is enabled in the VLAN. By default, MLD snooping is disabled in a VLAN. MLD snooping can be enabled using the **mld-snooping enable** command.
mld-snooping version 2	MLDv1 and MLDv2 messages can be processed in the VLAN. By default, only MLDv1 messages can be processed in a VLAN. This parameter is configured using the **mld-snooping version** command.

Related Topics

10.10.6 mld-snooping enable
10.10.8 mld-snooping group-policy (VLAN view)
10.10.9 mld-snooping last-listener-query-interval
10.10.10 mld-snooping max-response-time
10.10.11 mld-snooping prompt-leave
10.10.14 mld-snooping require-router-alert
10.10.15 mld-snooping robust-count
10.10.16 mld-snooping router-aging-time
10.10.19 mld-snooping send-router-alert
10.10.24 mld-snooping version

10.10.3 display mld-snooping port-info

Function

The **display mld-snooping port-info** command displays information about multicast group ports.

Format

display mld-snooping port-info [**vlan** *vlan-id* [**group** *ipv6-group-address* [**source-address** *ipv6-source-address*]]] [**verbose**]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays multicast group ports in a specified VLAN. If this parameter is not specified, the system displays multicast group ports in all VLANs.	The value is an integer that ranges from 1 to 4094.
group *ipv6-group-address*	Displays member ports of a specified multicast group. If this parameter is not specified, the system displays ports of all multicast groups.	The value is an IPv6 multicast address, which is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format. The first two digits are FF.
source-address *ipv6-source-address*	Displays member ports of a specified multicast source.	The value is an IPv6 multicast address, which is a 32-digit hexadecimal number in X:X:X:X:X:X:X:X format.
verbose	Displays detailed information about multicast group ports. If this parameter is not specified, the system displays the summary of multicast group ports.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

MLD snooping creates and maintains a Layer 2 multicast forwarding table by listening on MLD messages exchanged between hosts and a Layer 3 device. The **display mld-snooping port-info** command shows ports in the Layer 2 multicast forwarding table. According to the command output, you can know which downlink interfaces have multicast users connected, and control multicast services conveniently.

Precautions

This command can display port information only when MLD snooping is enabled globally and in a VLAN using the **mld-snooping enable** command and the VLAN is in Up state.

Example

Display information about multicast group ports.

```
<Huawei> display mld-snooping port-info
 ----------------------------------------------------------------------
                  (Source, Group)  Port                      Flag
 ----------------------------------------------------------------------
VLAN 10, 1 Entry(s)
(            *, ff13:0:0:0:0:0:0:2)Eth2/0/0                   S--
                                     1 port(s)
 ----------------------------------------------------------------------
```

Table 10-122 Description of the display mld-snooping port-info command output

Item	Description
(Source, Group)	An (S, G) entry, specifying the multicast source and multicast group.
Port	Multicast group port.

Related Topics

10.10.6 mld-snooping enable

10.10.20 mld-snooping static-group

10.10.4 display mld-snooping router-port

Function

The **display mld-snooping router-port** command displays information about router ports, including static and dynamic router ports.

Format

display mld-snooping router-port [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the router interfaces in a specified VLAN. If this parameter is not specified, the system displays router ports in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A router port is a router port connected to an upstream Layer 3 multicast device. Router ports can be statically configured or dynamically created after receiving an MLD Query message or a PIM Hello message. A router port receives multicast data packets from the upstream multicast device and forwards the packets to group member ports.

The **display mld-snooping router-port** command displays information about router ports, including the type, name, age, and aging time of each router port.

Precautions

This command can display router port information only when MLD snooping is enabled globally and in a VLAN using the **mld-snooping enable** command and the VLAN is in Up state.

Example

Display information about router ports.

```
<Huawei> display mld-snooping router-port
 Total Number of Router Port on VLAN 2 is 1
   Port Name          UpTime        Expires        Flags
   Eth2/0/0           00:00:06      --             STATIC
```

Table 10-123 Description of the display mld-snooping router-port command output

Item	Description
Total Number of Router Port on VlAN 2 is 1	Number of router ports in VLAN 2.
Port Name	Type and number of a router port.
UpTime	Age of a router port, that is, time that elapsed since the interface became a router port.
Expires	Aging time of the router port. ● The aging time is displayed for a dynamic router port. ● For a static router interface, "--" is displayed, indicating that the interface does not age.
Flags	Type of the router port, which can be: ● **STATIC**: static router port, which is configured using the **mld-snooping static-router-port** command ● **DYNAMIC**: dynamic router port

Related Topics

10.10.6 mld-snooping enable

10.10.21 mld-snooping static-router-port

10.10.5 display mld-snooping statistics

Function

The **display mld-snooping statistics** command displays MLD snooping statistics.

Format

display mld-snooping statistics [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MLD snooping statistics in a specified VLAN. If this parameter is not specified, the system displays MLD snooping statistics in all VLANs.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing MLD snooping configuration, you can use the **display mld-snooping statistics** command to view MLD snooping statistics, including the number of MLD messages sent, number of MLD messages received, and number of PIM Hello messages received in each VLAN, and number of Layer 2 events that have occurred in all VLANs. Layer 2 events include changes in interface status, changes in VLAN status, changes in VLAN member interfaces (interfaces join or leave VLANs), and MSTP events. When a multicast fault occurs, the MLD snooping statistics help you identify the cause of the fault.

Precautions

This command displays information only when global MLD snooping is enabled using the **mld-snooping enable** command.

Example

Display MLD snooping statistics in all VLANs.

```
<Huawei> display mld-snooping statistics
MLD Snooping Events Counter
    Recv VLAN Up Event Times      1027
    Recv VLAN Down Event Times    5
    Recv VLAN Del Event Times     0
    Recv Port Up Event Times      12
    Recv Port Down Event Times    12
    Recv Port Del Event Times     0
    Recv Port Inc Event Times     3069
    Recv Port Exc Event Times     1023
    Recv MSTP Block Event Times   7
    Recv MSTP Forward Event Times 7
    Recv LINK Change Event Times  0
 MLD Snooping Packets Counter
```

```
  Statistics for VLAN 10
    Recv V1 Report 16
    Recv V2 Report 8768
    Recv V1 Query  0
    Recv V2 Query  2243
    Recv Done     215
    Recv Pim Hello 0
    Send Query(S=0) 0
    Send Query(S!=0)0
```

Display MLD snooping in VLAN 20.

```
<Huawei> display mld-snooping statistics vlan 20
 MLD Snooping Packets Counter
   Statistics for VLAN 20
     Recv V1 Report  0
     Recv V2 Report  0
     Recv V1 Query   0
     Recv V2 Query   0
     Recv Done       0
     Recv Pim Hello  0
     Send Query(S=0) 0
     Send Query(S!=0)0
```

Table 10-124 Description of the display mld-snooping statistics command output

Item	Description
MLD Snooping Events Counter	Statistics about MLD snooping events.
Recv VLAN Up Event Times	Number of VLAN Up events.
Recv VLAN Down Event Times	Number of VLAN Down events.
Recv VLAN Del Event Times	Number of VLAN deletion events.
Recv Port Up Event Times	Number of interface Up events.
Recv Port Down Event Times	Number of interface Down events.
Recv Port Del Event Times	Number of interface deletion events.
Recv Port Inc Event Times	Number of times interfaces join VLANs.
Recv Port Exc Event Times	Number of times interfaces leave VLANs.
Recv MSTP Block Event Times	Number of MSTP blocking events.
Recv MSTP Forward Event Times	Number of MSTP forwarding events.
Recv LINK Change Event Times	Number of link change events.
MLD Snooping Packets Counter	Statistics about MLD snooping packets.
Statistics for VLAN 10	Packet statistics in VLAN 10.
Recv V1 Report	Number of MLDv1 Report messages received.
Recv V2 Report	Number of MLDv2 Report messages received.
Recv V1 Query	Number of MLDv1 Query messages received.

Item	Description
Recv V2 Query	Number of MLDv2 Query messages received.
Recv Done	Number of MLD Leave messages received.
Recv Pim Hello	Number of PIM Hello messages received.
Send Query(S=0)	Number of MLD Query messages sent with the source address of ::.
Send Query(S!=0)	Number of MLD Query messages with sent source addresses other than ::.

Related Topics

10.10.6 mld-snooping enable

10.10.27 reset mld-snooping statistics

10.10.6 mld-snooping enable

Function

The **mld-snooping enable** command enables MLD snooping globally or in a VLAN.

The **undo mld-snooping enable** command disables MLD snooping globally or in a VLAN.

By default, MLD snooping is disabled.

Format

System view

mld-snooping enable [**vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo mld-snooping enable [**vlan** { **all** | { *vlan-id1* [**to** *vlan-id2*] } &<1-10> }]

VLAN view

mld-snooping enable

undo mld-snooping enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Disables MLD snooping on the specified VLANs. *vlan-id1* and *vlan-id2* identify a range of VLANs. If VLAN IDs are specified, MLD snooping is enabled in the specified VLANs. If no VLAN ID is specified, MLD snooping is enabled globally.	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094. *vlan-id2* must be larger than *vlan-id1*.
all	Disables MLD snooping on all VLANs.	-

Views

System view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MLD snooping runs on a Layer 2 device between a Layer 3 multicast device and hosts, and listens on multicast protocol packets exchanged between the Layer 3 device and hosts to maintain a Layer 2 multicast forwarding table. The Layer 2 device manages and controls Layer 2 multicast forwarding based on this forwarding table.

Before configuring MLD snooping, enable global MLD snooping using the **mld-snooping enable** command in the system view. Other MLD snooping configuration commands can be used only after global MLD snooping is enabled.

You can enable MLD snooping in multiple VLANs by using the **mld-snooping enable** command in the system view.

Precautions

After you run the **undo mld-snooping enable** command to disable global MLD snooping, all MLD snooping configurations on the router are deleted. After you run the **mld-snooping enable** command to enable global MLD snooping again, the router uses the default MLD snooping configuration.

Example

Enable global MLD snooping.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mld-snooping enable
```

Enable MLD snooping in multiple VLANs in the system view.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] mld-snooping enable vlan 2 to 10
```

Enable MLD snooping in VLAN 10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] mld-snooping enable
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.7 mld-snooping group-policy (interface view)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy on an interface.

The **undo mld-snooping group-policy** command deletes an IPv6 multicast group policy from an interface.

By default, no IPv6 multicast group policy is available on an interface, and hosts connected to the interface can join any IPv6 multicast group.

Format

mld-snooping group-policy *acl6-number* **vlan** *vlan-id* [*mld-version*]

undo mld-snooping group-policy vlan *vlan-id* [*mld-version*]

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 to 3999.
vlan *vlan-id*	Applies the IPv6 multicast group policy to a specified VLAN on an interface.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mld-version	Specifies an MLD version. The multicast group policy is applied only to the MLD messages of this version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. ● 1: MLDv1 ● 2: MLDv2

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPv6 multicast group policy controls the multicast programs that users can order on a Layer 2 device with MLD snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. When the Layer 2 device receives the message, it checks whether the multicast group matches the multicast group policy applied to the interface. If so, the Layer 2 device drops the Report message and prohibits the user from joining the multicast group. If not, the Layer 2 device forwards the message, allowing the user to join the multicast group.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configured multicast group policy takes effect only when all the following conditions are met:

- The interface has been added to the specified VLAN.
- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The ACL specified in the command has been created and had filtering rules configured.

When configuring the ACL for a multicast group policy in a VLAN, set the action in the ACL rule to deny. That is, the policy only prohibits hosts in the VLAN from joining all or specified multicast groups. For details about ACL configuration commands, see **19.7 ACL Configuration Commands** in "Security Commands."

An IPv6 multicast group policy can also be configured in the VLAN view (using the **mld-snooping group-policy (VLAN view)** command) to control the multicast groups that users in the VLAN can join. An IPv6 multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 10 on Eth2/0/0 from joining IPv6 multicast group ff1c::3/32.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2000
[Huawei-acl6-basic-2000] rule deny source ff1c::3/32
[Huawei-acl6-basic-2000] quit
[Huawei] mld-snooping enable
[Huawei] vlan 10
[Huawei-vlan10] mld-snooping enable
[Huawei-vlan10] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 10
[Huawei-Ethernet2/0/0] mld-snooping group-policy 2000 vlan 10
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.8 mld-snooping group-policy (VLAN view)

10.10.8 mld-snooping group-policy (VLAN view)

Function

The **mld-snooping group-policy** command configures an IPv6 multicast group policy in a VLAN.

The **undo mld-snooping group-policy** command deletes an IPv6 multicast group policy from a VLAN.

By default, no IPv6 multicast group policy is available in a VLAN, and hosts in the VLAN can join any IPv6 multicast group.

Format

mld-snooping group-policy *acl6-number* [*mld-version*]

undo mld-snooping group-policy

Parameters

Parameter	Description	Value
acl6-number	Specifies the number of an IPv6 ACL that defines a range of multicast groups. A basic or advanced ACL can be used in an IPv6 multicast group policy.	The value is an integer that ranges from 2000 to 3999.
mld-version	Applies the multicast group policy only to the MLD messages of the specified version. If this parameter is not specified, the multicast group policy applies to all MLD messages.	The value is 1 or 2. • 1: MLDv1 • 2: MLDv2

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPv6 multicast group policy controls the multicast programs that users can order on a Layer 2 device with MLD snooping enabled. When a user orders a multicast program, the user host sends a Report message, requesting to join the multicast group. When the Layer 2 device receives the message, it checks whether the multicast group matches the multicast group policy applied to the VLAN. If so, the Layer 2 device drops the Report message and prohibits the user from joining the multicast group. If not, the Layer 2 device forwards the message, allowing the user to join the multicast group.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configured multicast group policy takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.

 Copyright © Huawei Technologies Co., Ltd.

- The ACL specified in the command has been created and had filtering rules configured.

When configuring the ACL for a multicast group policy in a VLAN, set the action in the ACL rule to deny. That is, the policy only prohibits hosts in the VLAN from joining all or specified multicast groups. For details about ACL configuration commands, see **19.7 ACL Configuration Commands** in "Security Commands."

An IPv6 multicast group policy can also be configured in the interface view using the **mld-snooping group-policy (interface view)** command to control the multicast groups that users in one or more VLANs on the interface can join. An IPv6 multicast group policy configured in the interface view controls the multicast groups that users in one or more VLANs on the interface can join. If you configure multicast group policies for the same VLAN in the interface view and VLAN view, the system first uses the policy configured in the interface view and then the policy configured in the VLAN view to determine the groups that user hosts can join.

Example

Prevent hosts in VLAN 4 from joining IPv6 multicast group ff1e::1/32.

```
<Huawei> system-view
[Huawei] acl ipv6 number 2001
[Huawei-acl6-basic-2001] rule deny source ff1e::1/32
[Huawei-acl6-basic-2001] quit
[Huawei] mld-snooping enable
[Huawei] vlan 4
[Huawei-vlan4] mld-snooping enable
[Huawei-vlan4] mld-snooping group-policy 2001
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.7 mld-snooping group-policy (interface view)

10.10.9 mld-snooping last-listener-query-interval

Function

The **mld-snooping last-listener-query-interval** command sets the last listener query interval, that is, the interval at which Multicast-Address-Specific Query messages are sent in MLD snooping.

The **undo mld-snooping last-listener-query-interval** command restores the default interval.

By default, the last listener query interval is 1 second.

Format

mld-snooping last-listener-query-interval *query-interval*

undo mld-snooping last-listener-query-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
query-interval	Specifies interval at which Multicast-Address-Specific Query messages are sent.	The value ranges from 1 to 5, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By configuring the last listener query interval, you can:

- Adjust the interval at which the querier sends Multicast-Address-Specific Query messages.

  When MLD snooping querier is enabled, you can use the **mld-snooping last-listener-query-interval** command to set the interval at which the querier sends Multicast-Address-Specific Query messages.
- Change the aging time of member ports.

  When a Layer 2 device receives an MLD Done message from a host, it starts an aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = Last listener query interval x Last listener query count. This command sets the last listener query interval in the formula. The last listener query count is set by the **mld-snooping robust-count** command.

  If the querier receives Report messages from other hosts within the aging time, it continues to maintain the memberships of the multicast group. If the querier does not receive any Report messages within the aging time, it stops maintaining memberships of the multicast group.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The querier sets the maximum response time field in the Multicast-Address-Specific Query messages to the configured last listener query interval. Therefore, the maximum response time for Multicast-Address-Specific Query messages is the same as the interval at which Multicast-Address-Specific Query messages are sent.

The configuration takes effect only when both the following conditions are met:

 Copyright © Huawei Technologies Co., Ltd.

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- The local device is enabled to send Query messages using the **mld-snooping querier enable** command.

Example

Set the last listener query interval to 2 seconds in VLAN 4.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 4
[Huawei-vlan4] mld-snooping enable
[Huawei-vlan4] mld-snooping last-listener-query-interval 2
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.12 mld-snooping querier enable

10.10.15 mld-snooping robust-count

10.10.10 mld-snooping max-response-time

Function

The **mld-snooping max-response-time** command sets the maximum response time for MLD General Query messages in a VLAN.

The **undo mld-snooping max-response-time** command restores the maximum response time for MLD General Query messages in a VLAN to the default value.

By default, the maximum response time for MLD Listener Query messages is 10 seconds.

Format

mld-snooping max-response-time *max-response-time*

undo mld-snooping max-response-time

Parameters

Parameter	Description	Value
max-response-time	Specifies the maximum response time for General Query messages.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 10.

 Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting MLD snooping parameters helps improve multicast forwarding performance on the router. By setting the maximum response time for MLD General messages, you can:

- Control the deadline for a host to send a Report message. When hosts are required to respond to Query messages quickly, set a short maximum response time. To avoid congestion caused by a large number of Report messages sent by hosts, set a long maximum response time.
- Adjust the aging time of member ports. When the router receives a Report message from a host, it starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. This command sets the maximum response time in the formula. The number of times General Query messages are sent is set by the **mld-snooping robust-count** command, and the general query interval is set by the **mld-snooping query-interval** command.

The router sets the maximum response time field in General Query messages to the value configured by the **mld-snooping max-response-time** command.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations to improve multicast performance:

- Run the **mld-snooping query-interval** command to set the interval at which General Query messages are sent.
- Run the **mld-snooping last-listener-query-interval** command to set the interval at which Multicast-Address-Specific Query messages are sent.

Precautions

To make the configured maximum response time effective in a VLAN, run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the router may delete multicast memberships that should not be deleted.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum response time for General Query messages in VLAN 3 to 20 seconds.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping max-response-time 20
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.9 mld-snooping last-listener-query-interval

10.10.13 mld-snooping query-interval

10.10.15 mld-snooping robust-count

10.10.11 mld-snooping prompt-leave

Function

The **mld-snooping prompt-leave** command enables the fast leave function in a VLAN so that member ports in the VLAN can fast leave multicast groups.

The **undo mld-snooping prompt-leave** command disables the fast leave function in a VLAN.

By default, the fast leave function is disabled in a VLAN.

Format

mld-snooping prompt-leave [**group-policy** *acl6-number*]

undo mld-snooping prompt-leave

Parameters

Parameter	Description	Value
group-policy *acl6-number*	Allows member ports to fast leave the multicast groups matching an ACL6. *acl6-number* specifies the number of an ACL6. A basic or advanced ACL6 can be used.	The value is an integer that ranges from 2000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The fast leave function enables the router to delete the multicast forwarding entry of a multicast group from an interface immediately after the interface receives a Done message for the group. This function saves bandwidth and system resources because the router does not need to wait until the aging timer of the interface expires.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

When an interface has more than one receiver connected, enabling the fast leave function interrupts multicast traffic of the other receivers in the multicast group. It is recommended that you enable this function only on interfaces with one receiver.

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the VLAN using the **mld-snooping enable** command.
- An ACL has been created and has filtering rules configured if a multicast group policy is specified in the command. The default ACL rule permits all multicast groups. Therefore, after configuring a rule that permits a specified multicast group, run the **rule deny source any** command to deny all the other multicast groups. For details about ACL configuration commands, see **19.7 ACL Configuration Commands** in "Security Commands."

Example

Allow member ports in VLAN 2 to fast leave all multicast groups.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] mld-snooping enable
[Huawei-vlan2] mld-snooping prompt-leave
```

Allow member ports in VLAN 3 to fast leave multicast group 0xff13::0001:0002.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] acl ipv6 number 2000
[Huawei-acl6-basic-2000] rule permit source ff13::0001:0002 128
[Huawei-acl6-basic-2000] rule deny source any
[Huawei-acl6-basic-2000] quit
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping prompt-leave group-policy 2000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.12 mld-snooping querier enable

Function

The **mld-snooping querier enable** command enables the MLD snooping querier in a VLAN.

The **undo mld-snooping querier enable** command disables the MLD snooping querier in a VLAN.

By default, the MLD snooping querier is disabled in a VLAN.

Format

mld-snooping querier enable

undo mld-snooping querier enable

Parameters

None.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MLD-capable network, a Layer 3 multicast device functions as the querier to send MLD Query messages and maintain group memberships on the local network segment. If the Layer 3 multicast device does not run MLD or it uses only static multicast forwarding entries, it cannot function as a querier. You can enable MLD snooping querier on the downstream Layer 2 device. Then the Layer 2 device can act as a querier to send MLD Query messages.

On a Layer 2 network without Layer 3 devices, multicast sources are connected to Layer 2 devices. MLD snooping querier needs to be enabled on the Layer 2 devices so that they can maintain multicast group memberships.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Perform the following operations as required on your network:

- Set the interval at which the MLD snooping querier sends General Query messages using the **mld-snooping query-interval** command.
- Set the interval at which the MLD snooping querier sends Multicast-Address-Specific Query messages using the **mld-snooping last-listener-query-interval** command.
- Set the query count using the **mld-snooping robust-count** command.

Configuration Impact

The MLD snooping querier does not participate in MLD querier election. However, the MLD snooping querier on an MLD-capable multicast network may affect the election result, because the Query messages sent by the MLD snooping querier may have a smaller source IP address than the Query messages sent by other devices. Therefore, the MLD snooping querier function is not recommended on an MLD-enabled multicast network.

Precautions

- The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Enable the MLD snooping querier in VLAN 3.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping querier enable
```

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable
10.10.9 mld-snooping last-listener-query-interval
10.10.13 mld-snooping query-interval
10.10.15 mld-snooping robust-count

10.10.13 mld-snooping query-interval

Function

The **mld-snooping query-interval** command sets the general query interval in a VLAN, that is, the interval at which MLD General Query messages are sent in the VLAN.

The **undo mld-snooping query-interval** command restores the default general query interval in a VLAN.

By default, MLD General Query messages are sent at an interval of 60 seconds.

Format

mld-snooping query-interval *query-interval*

undo mld-snooping query-interval

Parameters

Parameter	Description	Value
query-interval	Specifies the interval at which General Query messages are sent.	The value is an integer that ranges from 10 to 65535, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the MLD general query interval, you can:

- Specify the interval at which the querier sends MLD General Query messages.

  When the querier function is enabled in a VLAN, you can use this command to set the general query interval. Then the querier sends General Query messages at the configured interval to maintain group memberships. The querier is more sensitive when it sends General Query messages at a smaller interval. However, more bandwidth and resources are consumed in this case.
- Change the aging time of member ports.

  When receiving an MLD Report message from a host, the router starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = General query count x General query interval + Maximum response time for General Query messages. The **mld-snooping query-interval** command sets the general query interval. The general query count is set by the **mld-snooping robust-count** command, and the maximum response time for General Query messages is set by the **mld-snooping max-response-time** command.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

 Copyright © Huawei Technologies Co., Ltd.

Use this command only when the router can send MLD Query message. The router can send MLD Query messages only MLD snooping querier is enabled using the **mld-snooping querier enable** command.

The interval at which General Query messages are sent must be longer than the maximum response time for General Query messages. Otherwise, the router may delete multicast memberships that should not be deleted.

Example

Set the general MLD query interval in VLAN 3 to 100 seconds.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping query-interval 100
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.10 mld-snooping max-response-time

10.10.12 mld-snooping querier enable

10.10.15 mld-snooping robust-count

10.10.14 mld-snooping require-router-alert

Function

The **mld-snooping require-router-alert** command configures the router to check the received MLD messages for the Router-Alert option and discard the MLD messages without the Router-Alert option.

The **undo mld-snooping require-router-alert** command restores the default configuration.

By default, the router processes the received MLD messages regardless of whether the messages contain the Router-Alert option.

Format

mld-snooping require-router-alert

undo mld-snooping require-router-alert

Parameters

None

Views

VLAN view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the router does not check whether MLD messages contain the Router-Alert option and sends all the MLD messages to the upper-layer routing protocol. Discarding MLD messages without the Router-Alert option improves device performance, reduces cost, and enhances security of the upper-layer routing protocol. After the **mld-snooping require-router-alert** command is executed, the router checks each MLD message for the Router-Alert option and discards those MLD messages without this option.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

If MLD snooping is disabled in the specified VLAN, the configuration succeeds but does not take effect until MLD snooping is enabled in the VLAN. To enable MLD snooping in a VLAN, run the **mld-snooping enable** command in the VLAN view.

Example

Configure the router to accept only MLD messages with the Router-Alert option in VLAN 3.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping require-router-alert
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.15 mld-snooping robust-count

Function

The **mld-snooping robust-count** command sets the MLD robustness variable in a VLAN.

The **undo mld-snooping robust-count** command restores the default MLD robustness variable in a VLAN.

 Copyright © Huawei Technologies Co., Ltd.

By default, the MLD robustness variable in a VLAN is 2.

Format

mld-snooping robust-count *robust-count*

undo mld-snooping robust-count

Parameters

Parameter	Description	Value
robust-count	Specifies the MLD robustness variable.	The value is an integer that ranges from 2 to 5.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Setting MLD snooping parameters helps improve multicast forwarding performance. By setting the MLD robustness variable, you can:

- Set the last listener query count for the querier to prevent packet loss.

  When receiving an MLD Done message of a multicast group, the querier sends Multicast-Address-Specific Query messages certain times specified by the robustness variable to check whether the multicast has members. If the quality of transmission links is low, increase the MLD robustness variable.
- Change the aging time of member ports.

  When receiving an MLD Report message from a host, the router starts the aging timer for the corresponding member port. The aging time is calculated using the following formula: Aging time = MLD robustness variable x General query interval + Maximum response time for General Query messages. The **mld-snooping robust-count** command sets the MLD robustness variable.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

Perform the following operations to optimize multicast service performance:

- Run the **mld-snooping query-interval** command to set the interval at which General Query messages are sent.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **mld-snooping max-response-time** command to set the maximum response time for General Query messages.
- Run the **mld-snooping last-listener-query-interval** command to set the interval at which Multicast-Address-Specific Query messages are sent.

Precautions

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Set the robustness variable to 5 in VLAN 3.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping robust-count 5
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.9 mld-snooping last-listener-query-interval

10.10.10 mld-snooping max-response-time

10.10.13 mld-snooping query-interval

10.10.16 mld-snooping router-aging-time

Function

The **mld-snooping router-aging-time** command sets the aging time of dynamic router ports in a VLAN.

The **undo mld-snooping router-aging-time** command restores the default aging time of dynamic router ports in a VLAN.

By default, the aging time of dynamic router ports in a VLAN is 180 seconds or equal to the holdtime value contained in PIM Hello messages.

Format

mld-snooping router-aging-time *router-aging-time*

undo mld-snooping router-aging-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
router-aging-time	Indicates the aging time of a router port.	The value is an integer that ranges from 1 to 1000, in seconds.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a short-term congestion occurs on a network, it takes a longer time to transmit Query messages from the MLD querier to a Layer 2 device. If a router port on the Layer 2 device ages out within this period, the Layer 2 device does not send Report or Done messages to the router port. As a result, multicast data forwarding may be interrupted. To solve this problem, set a longer aging time for router ports on an unstable network.

When a dynamic router port receives an MLD Query message or PIM Hello message, the Layer 2 device sets the aging time of the router port as follows:

- If the router port receives an MLD Query message, the Layer 2 device sets the aging time of the router port to the configured value.
- If the router port receives a PIM Hello packet and the Holdtime value in the Hello packet is larger than the remaining aging time of the router port, the Layer 2 device sets the aging time of the router port to the Holdtime value contained in the PIM Hello packet. If the Holdtime value in the Hello packet is smaller than the remaining aging time of the router port, the Layer 2 device does not reset the aging time of the router port.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

If the aging time of a router port is too short, the router port ages frequently, degrading system performance.

Example

Set the aging time of router ports in VLAN 3 to 300 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] mld-snooping router-aging-time 300
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.17 mld-snooping send-query enable

Function

The **mld-snooping send-query enable** command enables the router to send MLD General Query messages to non-router ports when receiving Layer 2 topology change events.

The **undo mld-snooping send-query enable** command disables the router from sending MLD General Query messages when receiving Layer 2 topology change events.

By default, the router does not send MLD General Query messages when receiving Layer 2 topology change events.

Format

mld-snooping send-query enable

undo mld-snooping send-query enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the network topology changes, the router receives a topology change event. By default, the router does not send MLD General Query messages in this case. The network topology change triggers recalculation of the Multiple Spanning Tree Protocol (MSTP). If the router cannot respond to the topology change immediately, multicast data traffic cannot be switched to the new path in a timely manner. The **mld-snooping send-query enable** command enables the router to

send MLD General Query messages to update group memberships when the network topology changes. This ensures that multicast data traffic can be switched to the new transmission path.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Follow-up Procedure

This command is used on a ring network. When the ring network topology changes, the router sends MLD General Query messages with source IPv6 address FE80::0. When this address has been occupied by another device on the network, run the **mld-snooping send-query source-address** command to set the source IPv6 address to FE80::.

Precautions

Use this command only when MSTP is enabled on the network.

Example

Enable the router to send MLD General Query messages to non-router ports when receiving Layer 2 topology change events.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] mld-snooping send-query enable
```

Related Topics

10.10.6 mld-snooping enable

10.10.18 mld-snooping send-query source-address

10.10.18 mld-snooping send-query source-address

Function

The **mld-snooping send-query source-address** command sets the source IPv6 address of MLD General Query.

The **undo mld-snooping send-query source-address** command restores source IPv6 address of MLD General Query messages.

By default, the source IPv6 address of MLD General Query messages is FE80::.

Format

mld-snooping send-query source-address *ipv6-address*

undo mld-snooping send-query source-address

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address of MLD General Query messages.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X, the network prefix must be FE80::/64.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 device sends two types of MLD General Query messages:

- MLD General Query messages sent by the querier when the querier function is enabled using the **mld-snooping querier enable** command.
- MLD General Query messages that the Layer 2 device sends after receiving Layer 2 topology change events (configured using the **mld-snooping send-query enable** command).

By default, MLD General Query messages sent from a Layer 2 device use the source IPv6 address FE80::. When this IPv6 address is used by another device on the network, run the **mld-snooping send-query source-address** command to change the source IPv6 address of MLD General Query messages.

When multiple Layer 2 devices exist on a shared network, you can set source IPv6 addresses of MLD Query messages to identify the devices. For example, when multiple devices with different performance need to participate in querier election, you must configure a different source IPv6 address of MLD Query messages for each device.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Example

Set the source IPv6 address of MLD General Query messages to FE80::1.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] mld-snooping send-query source-address fe80::1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.10.6 mld-snooping enable

10.10.12 mld-snooping querier enable

10.10.17 mld-snooping send-query enable

10.10.19 mld-snooping send-router-alert

Function

The **mld-snooping send-router-alert** command configures the router to send MLD messages with the Router-Alert option in the IP header to a VLAN.

The **undo mld-snooping send-router-alert** command configures the router to send MLD messages without the Router-Alert option to a VLAN.

By default, the MLD messages sent by the router contain the Router-Alert option.

Format

mld-snooping send-router-alert

undo mld-snooping send-router-alert

Parameters

None

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Router-Alert option identifies the protocol messages that need to be processed by upper-layer routing protocols.

By default, the router sends MLD messages with the Router-Alert option. If some devices in the same VLAN as the router can process only the MLD messages without the Router-Alert option, use the **undo igmp-snooping send-router-alert** command to configure the router to send MLD messages without the Router-Alert option.

The router adds the Router-Alert option only to locally originated MLD messages and does not add this option to MLD messages received from other devices.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Configure the router to send MLD messages that do not contain the Router-Alert option in the IP header to VLAN 3.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 3
[Huawei-vlan3] mld-snooping enable
[Huawei-vlan3] undo mld-snooping send-router-alert
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.20 mld-snooping static-group

Function

The **mld-snooping static-group** command configures static IPv6 group memberships on an interface.

The **undo mld-snooping static-group** command deletes the static IPv6 group memberships on an interface.

By default, no static IPv6 group membership is configured on an interface.

Format

mld-snooping static-group *group-ipv6-address* [**source** *source-ipv6-address*] **vlan** *vlan-id*

undo mld-snooping static-group { *group-ipv6-address* [**source** *source-ipv6-address*] **vlan** *vlan-id* | **all** }

Parameters

Parameter	Description	Value
group-ipv6-address	Specifies the IPv6 address of a multicast group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X. An IPv6 multicast address starts with FF.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source *source-ipv6-address*	Specifies the IPv6 address of a multicast source.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Deletes all static group memberships from an interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In addition to dynamic multicast forwarding entries generated by Layer 2 multicast protocols, you can configure static Layer 2 multicast forwarding entries by binding interfaces to multicast groups. After an interface is statically bound to a multicast group, users connected to this interface can receive multicast data of the multicast group for a long time. The interface then becomes a static member interface.

Configuring static member interfaces has the following advantages:

- Protects the system against attacks from protocol packets.
- Reduces the network delay by directly forwarding multicast packets based on static forwarding entries.
- Prevents unregistered users from receiving multicast flows, improving information security and protecting service providers' interests.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only when both the following conditions are met:

- MLD snooping is enabled in the specified VLAN using the **mld-snooping enable** command.

- The specified VLAN has been created and the interface has been added to the VLAN.

Example

Statically bind Eth2/0/0 in VLAN 2 to multicast group ff1a::1.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port link-type trunk
[Huawei-Ethernet2/0/0] port trunk allow-pass vlan 2
[Huawei-Ethernet2/0/0] mld-snooping static-group ff1a::1 vlan 2
```

Related Topics

10.10.1 display mld-snooping
10.10.2 display mld-snooping configuration
10.10.6 mld-snooping enable
10.10.24 mld-snooping version

10.10.21 mld-snooping static-router-port

Function

The **mld-snooping static-router-port** command configures a static router port in a VLAN.

The **undo mld-snooping static-router-port** command deletes a static router port in a VLAN.

By default, no static router port is configured in a VLAN.

Format

mld-snooping static-router-port vlan *vlan-id*

undo mld-snooping static-router-port { **all** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID. This parameter specifies in which VLAN the current interface functions as a router port.	The value is an integer that ranges from 1 to 4094.
all	Disables the interface from functioning as a router port in all VLANs.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface needs to receive or forward multicast data packets in a long time, configure the interface as a static router port.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

This command takes effect only when the interface is added to the specified VLAN.

Example

Configure Eth2/0/0 as a router port in VLAN 2.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mld-snooping static-router-port vlan 2
```

Related Topics

10.10.4 display mld-snooping router-port

10.10.6 mld-snooping enable

10.10.22 mld-snooping suppression-time

Function

The **mld-snooping suppression-time** command sets the MLD message suppression time.

The **undo mld-snooping suppression-time** command restores the default MLD message suppression time.

By default, the MLD message suppression time is 10 seconds.

Format

mld-snooping suppression-time *suppression-time*

undo mld-snooping suppression-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
suppression-time	Specifies the MLD message suppression time.	The value is an integer ranging from 0 to 300, in seconds. The value 0 indicates that MLD messages are not suppressed.

Views

system view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect an upstream Layer 3 device from attacks and reduce the loads on the Layer 3 device, a Layer 2 device can suppress duplicate MLD Report messages. The default MLD message suppression time is 10 seconds. You can change the MLD message suppression time using the **mld-snooping suppression-time** command.

After you set the MLD message suppression time on a Layer 2 multicast device, the device acts as follows:

- After the Layer 2 device receives an MLD Report message, it does not forward identical MLD Report messages to the router port within the suppression time.
- If the Layer 2 device receives an MLD General Query message or Multicast-Address-Specific Query message within the suppression time, it does not suppress the first MLD Report message sent in response to the Query message. In addition, the Layer 2 device resets the suppression timer when receiving the first MLD Report message.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

You can run this command for MLDv1 Done and MLDv2 packets, but the command does not take effect.

Example

Set the MLD message suppression time to 15 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] mld-snooping suppression-time 15
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.23 mld-snooping table limit

Function

The **mld-snooping table limit** command sets the maximum number of MLD snooping entries that can be learned on an interface.

The **undo mld-snooping table limit** command cancels the limit on the number of MLD snooping entries that can be learned on an interface.

By default, the maximum number of multicast entries that an interface can learn varies according to device models:

- AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 128
- AR2220, AR2240C, and AR2220E: 1000
- AR2204XE and AR2204XE-DC: 2000
- AR2240 and AR3200 series:
  - Configured with SRU40: 1000
  - Configured with SRU60: 1000
  - Configured with SRU80: 2000
  - Configured with SRU100E: 2000
  - Configured with SRU200: 2000
  - Configured with SRU200E: 2000
  - Configured with SRU400: 2000
- AR3600 series (SRUX5): 2000

Format

mld-snooping table limit *limit* **vlan** *vlan-id*

undo mld-snooping table limit vlan *vlan-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
limit	Specifies the maximum number of MLD snooping entries that can be learned on an interface.	The value is an integer ranging from ● 1 to 128 for the AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204 ● 1 to 1000 for the AR2220, AR2240C, and AR2220E ● AR2204XE and AR2204XE-DC: 1 to 2000 ● AR2240 and AR3200 series (depending on the SRU model used on the router): – Configured with SRU40: 1 to 1000 – Configured with SRU60: 1 to 1000 – Configured with SRU80: 1 to 2000 – Configured with SRU100: 1 to 2000 – Configured with SRU100E: 1 to 2000 – Configured with SRU200: 1 to 2000 – Configured with SRU200E: 1 to 2000 – Configured with SRU400: 1 to 2000 ● 1 to 2000 for the AR3600 series (SRUX5)
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer ranging from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The maximum number of MLD snooping entries on an interface limits the number of programs that users on the interface can order. You can set this limit to control the multicast data traffic on an interface.

Prerequisites

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Configuration Impact

During the configuration, if the number of multicast entries on the interface already exceeds the configured threshold, the number of multicast entries on the interface does not change and the interface cannot learn new multicast entries.

Precautions

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Set the maximum number of MLD snooping entries that can be learned on Eth2/0/0 in VLAN 5 to 100. (Eth2/0/0 has been added to VLAN 5, and MLD snooping has been enabled globally and in VLAN 5.)

```
<Huawei> system view
[Huawei] mld-snooping enable
[Huawei] vlan 5
[Huawei-vlan5] mld-snooping enable
[Huawei-vlan5] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mld-snooping table limit 100 vlan 5
```

Related Topics

10.10.6 mld-snooping enable

10.10.24 mld-snooping version

Function

The **mld-snooping version** command sets the version of MLD messages that MLD snooping can process in a VLAN.

The **undo mld-snooping version** command restores the default MLD message version.

By default, MLD snooping can process only MLDv1 messages.

Format

mld-snooping version *version*

undo mld-snooping version

Parameters

Parameter	Description	Value
version	Specifies the version of MLD messages that MLD snooping can process.	The value is 1 or 2. ● 1: Only MLDv1 messages can be processed. ● 2: Both MLDv1 and MLDv2 messages can be processed.

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MLD protocol maintains group memberships between Layer 3 multicast devices and hosts. MLD has two versions: v1 and v2. This command specifies the version of MLD messages that MLD snooping can process. Generally, configure the same version on the Layer 2 device as that on the upstream Layer 3 multicast device. If MLD is not enabled on the Layer 3 multicast device, configure the MLD message version on the Layer 2 device to be later than or equal to the MLD version running on downstream hosts.

When hosts in a VLAN run different MLD versions, run the **mld-snooping version** command to enable the Layer 2 device to process MLD messages sent from all the hosts.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

MLD snooping has been enabled globally using the **mld-snooping enable** command.

Precautions

The configuration takes effect only after you run the **mld-snooping enable** command to enable MLD snooping in the VLAN.

Example

Set the MLD message version to 2 in VLAN 2.

```
<Huawei> system-view
[Huawei] mld-snooping enable
[Huawei] vlan 2
[Huawei-vlan2] mld-snooping enable
[Huawei-vlan2] mld-snooping version 2
```

Related Topics

10.10.1 display mld-snooping

10.10.2 display mld-snooping configuration

10.10.6 mld-snooping enable

10.10.25 multicast drop-unknown

Function

The **multicast drop-unknown** command configures the router to drop unknown multicast flows in a VLAN.

The **undo multicast drop-unknown** command restores the default measure taken for unknown multicast flows.

By default, the router broadcasts unknown multicast flows in a VLAN.

NOTE

AR2204-24GE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, AR2204XE-DC, AR2220L, AR2220E and AR2240C do not support this command.

Format

multicast drop-unknown

undo multicast drop-unknown

Parameters

None

Views

VLAN view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unknown multicast flows are multicast data flows that match no entry in the multicast forwarding table. By default, the router broadcasts unknown multicast flows in the corresponding VLAN. You can use the **multicast drop-unknown** command to configure the router to drop unknown multicast flows, which reduces instant bandwidth usage compared with the broadcast mode.

Configuration Impact

After the **multicast drop-unknown** command is executed, all unknown multicast packets are dropped, including the protocol packets that are transparently transmitted within the VLAN and use the reserved multicast address.

Example

Drop unknown multicast flows in VLAN 10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] multicast drop-unknown
```

10.10.26 reset mld-snooping group

Function

The **reset mld-snooping group** command deletes dynamic group memberships learned by MLD snooping.

Format

reset mld-snooping group { **all** | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Deletes dynamic group memberships learned by MLD snooping.	-
vlan *vlan-id*	Deletes dynamic group memberships in a specified VLAN.	The value of *vlan-id* is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When multicast groups change on a network, the router generates new Layer 2 multicast forwarding entries until the aging time of member ports expire. To enable the router to generate new multicast forwarding entries immediately, use the **reset mld-snooping group** command to delete old memberships.

Precautions

NOTICE

Deleting group memberships in a VLAN temporarily interrupts multicast forwarding in the VLAN. The router generates new forwarding entries only when receiving MLD Report messages from hosts in the VLAN. The hosts can then receive multicast data.

This command cannot delete static group memberships.

This command is valid only for VLANs with MLD snooping enabled and is invalid for a VLAN if MLD is enabled on the corresponding VLANIF interface.

Example

Delete dynamic group memberships in VLAN 2.

```
<Huawei> reset mld-snooping group vlan 2
```

Related Topics

10.10.3 display mld-snooping port-info

10.10.27 reset mld-snooping statistics

Function

The **reset mld-snooping statistics** command clears MLD snooping statistics.

Format

reset mld-snooping statistics [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears the MLD snooping statistics in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To analyze the MLD snooping statistics collected in a certain period, run this command to clear the previous statistics. After a while, run the **display mld-snooping statistics** command to view the MLD snooping statistics.

Precautions

NOTICE

The cleared MLD snooping statistics cannot be restored.

Example

Clear MLD snooping statistics in VLAN 2.

```
<Huawei> reset mld-snooping statistics vlan 2
```

Related Topics

10.10.5 display mld-snooping statistics

10.11 Multicast Network Management Commands

10.11.1 display pim mib-control-message

Function

The **display pim mib-control-message counters** command displays the number of neighbor loss events, the number of times for DR election, the number of

invalid Join/Prune messages, the number of invalid Register messages, the number of RP-mapping changes, and the number of received and sent Assert messages.

The **display pim mib-control-message join-prune** command displays the source address, group address, and RP address carried in the invalid Join/Prune message that is received at the last time.

The **display pim mib-control-message assert** command displays the source address and group address carried in the last received or sent Assert message.

The **display pim mib-control-message register** command displays the source address, group address, and RP address carried in the invalid Register message that is received at the last time.

Format

display pim mib-control-message { **counters** | **join-prune** | **assert** | **register** }

Parameters

Parameter	Description	Value
counters	Indicates related PIM counters.	-
join-prune	Indicates the number of invalid Join/Prune messages that are received at the last time.	-
assert	Indicates the number of Assert messages that are received or sent at the last time.	-
register	Indicates the number of invalid Register messages that are received at the last time.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the number of neighbor loss events, the number of times for DR election, the number of invalid Join/Prune messages, the number of invalid Register messages, the number of RP-mapping changes, the number of received and sent Assert messages.

```
<Huawei> display pim mib-control-message counters
pim mib-control-message counters
Neighbor-loss(times)        : 0
DR-Election(times)          : 0
```

```
Invalid-join-prune(times)   : 0
RP-Mapping(times)           : 0
Invalid-register(times)     : 0
Assert-received(times)      : 0
Assert-send(times)          : 0
```

Display the invalid Join/Prune message that is received at the last time.

```
<Huawei> display pim mib-control-message join-prune
The last invalid join-prune message received information:
Group address  : 225.1.1.1
Source address : 0.0.0.0
RP address     : 10.0.5.5
```

Display the Assert message that is sent or received at the last time. If the interface that receives or sends the Assert message is pulled out when this command is used, the prompt that "The last assert message was received or sent on lost interface" is displayed.

```
<Huawei> display pim mib-control-message assert
The last assert message received or sent on GigabitEthernet1/0/0
Group address   : 226.3.3.3
Source address  : 10.0.5.55
```

Display the invalid Register message that is received at the last time.

```
<Huawei> display pim mib-control-message register
The last invalid register message received information:
Group address  : 225.1.1.1
Source address : 10.0.5.100
RP address     : 10.0.3.1
```

Table 10-125 Description of the **display pim mib-control-message** command output

Item	Description
pim mib-control-message counters	the number of times for DR election, the number of invalid Join/Prune messages, the number of invalid Register messages, the number of RP-mapping changes, and the number of received and sent Assert messages.
The last invalid join-prune message received information	Display the invalid Join/Prune message that is received at the last time
The last assert message received or sent on GigabitEthernet1/0/0	Display the Assert message that is sent or received at the last time
The last invalid register message received information	Display the invalid Register message that is received at the last time
Neighbor-loss(times)	The number of neighbor loss events
DR-Election (times)	The number of times for DR election
Invalid-join-prune(times)	The number of invalid Join/Prune messages
RP-Mapping(times)	The number of RP-mapping changes

Item	Description
Invalid-register(times)	The number of invalid Register messages
Assert-received(times)	The number of received Assert messages
Assert-send(times)	The number of sent Assert messages
Group address	Multicast group address
Source address	Multicast source address
RP address	RP address

10.11.2 display pim mib-notification interval

Function

The **display pim mib-notification interval** command displays the interval for sending PIM notification messages.

Format

display pim mib-notification interval

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the interval for sending PIM notification messages is set or modified by using the **pim mib-notification interval** command, you can run the **display pim mib-notification interval** command to view the configured interval.

Example

Display the interval for sending PIM notification messages.

```
<Huawei> display pim mib-notification interval
Neighbor-loss notification interval      : 0 s
Invalid-join-prune notification interval : 50 s
RP-mapping-change notification interval  : 100 s
Interface-election notification interval : 2000 s
Invalid-register notification interval   : 60000 s
```

```
New-neighbor notification interval      : 0 s
Mrt-limit notification interval         : never
```

Table 10-126 Description of the **display pim mib-notification interval** command output

Item	Description
Neighbor-loss notification interval	Interval for sending the notification messages about the neighbor loss
Invalid-join-prune notification interval	Interval for sending the notification messages about invalid Join/Prune messages
RP-mapping-change notification interval	Interval for sending the notification messages about RP-mapping changes
Interface-election notification interval	Interval for sending the notification messages about interface election
Invalid-register notification interval	Interval for sending the notification messages about invalid Register messages
New-neighbor notification interval	Interval for sending trap messages about neighbor addition.
Mrt-limit notification interval	Interval for sending trap messages about the failure in joining multicast groups because the number of PIM entries reaches the upper limit.

10.11.3 display snmp-agent trap feature-name igmp all

Function

The **display snmp-agent trap feature-name igmp all** command displays whether the trap function is enabled for the IGMP module.

Format

display snmp-agent trap feature-name igmp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name igmp all** command to view the status of all IGMP traps when you want to monitor the current status of IGMP protocol events but are not sure whether the IGMP trap function is enabled.

Example

Display whether the trap function is enabled for the IGMP module.

```
<Huawei> display snmp-agent trap feature-name igmp all
-------------------------------------------------------------------------------
Feature name: IGMP
Trap number : 18
-------------------------------------------------------------------------------
Trap name                        Default switch status   Current switch status
IFLIMIT                          off                     off
IFLIMITCLR                       off                     off
INSLIMIT                         off                     off
GLBLIMIT                         off                     off
HWMGMDGMPGLOBALLIMITCLEAR        off                     off
HWMGMDGMPTOTALLIMITCLEAR         off                     off
JOINGRP                          off                     off
LEAVEGRP                         off                     off

hwMgmdTotalLimitThresholdExceed
                                 off                     off
hwMgmdTotalLimitThresholdExceedClear
                                 off                     off
hwMgmdHostStarGThresholdExceed   off                     off
hwMgmdHostStarGThresholdExceedClear
                                 off                     off
hwMgmdHostStarGExceed            off                     off
hwMgmdHostStarGExceedClear       off                     off
hwMgmdHostSGThresholdExceed      off                     off
hwMgmdHostSGThresholdExceedClear
                                 off                     off
hwMgmdHostSGExceed               off                     off
hwMgmdHostSGExceedClear          off                     off
```

Table 10-127 Description of the **display snmp-agent trap feature-name igmp all** command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap event types.

Item	Description
Trap name	Trap event type. The following types of trap events are defined: ● IFLIMIT: The number of IGMP entries on an interface reaches the limit. ● IFLIMITCLR: The number of IGMP entries on an interface falls below the limit. ● INSLIMIT: The number of IGMP entries in an instance reaches the limit. ● GLBLIMIT: The total number of the entries in all instances reaches the limit. ● HWMGMDGMPGLOBALLIMITCLEAR: The number of IGMP entries in a single instance falls below the limit. ● HWMGMDGMPTOTALLIMITCLEAR: The number of IGMP entries in all instances falls below the limit. ● JOINGRP: An IGMP Join message is received. ● LEAVEGRP: An IGMP Leave message is received or the group timer expires. ● hwMgmdTotalLimitThresholdExceed: a trap message indicating that the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed reaches the upper alarm threshold. ● hwMgmdTotalLimitThresholdExceed-Clear: a trap message indicating that the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed falls below the lower alarm threshold. ● hwMgmdHostStarGThresholdExceed: a trap message indicating that the total number of (*, G) entries of all instances reaches the specified upper alarm threshold. ● hwMgmdHostStarGThresholdExceed-Clear: a trap message indicating that the total number of (*, G) entries of all instances falls below the specified lower alarm threshold. ● hwMgmdHostStarGExceed: a trap message indicating that the total

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	number of (*, G) entries of all instances exceeds the maximum number allowed on the user-side IGMP/MLD device. • hwMgmdHostStarGExceedClear: a trap message indicating that the total number of (*, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device. • hwMgmdHostSGThresholdExceed: a trap message indicating that the total number of (S, G) entries of all instances reaches the specified upper alarm threshold. • hwMgmdHostSGThresholdExceed-Clear: a trap message indicating that the total number of (S, G) entries of all instances falls below the specified lower alarm threshold. • hwMgmdHostSGExceed: a trap message indicating that the total number of (S, G) entries of all instances exceeded the maximum number allowed on the user-side IGMP/MLD device. • hwMgmdHostSGExceedClear: a trap message indicating that the total number of (S, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device.
Default switch status	Default status of a trap function: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Current status of a trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

10.11.17 snmp-agent trap enable feature-name igmp

10.11.4 display snmp-agent trap feature-name mld all

Function

The **display snmp-agent trap feature-name mld all** command displays whether the trap function is enabled for the MLD module.

Format

display snmp-agent trap feature-name mld all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name mld all** command to view the status of all MLD traps when you want to monitor the current status of MLD protocol events but are not sure whether the MLD trap function is enabled.

Example

Display whether the trap function is enabled for the MLD module.

```
<Huawei> display snmp-agent trap feature-name mld all
-----------------------------------------------------------------------------
Feature name: MLD
Trap number : 8
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
IFLIMIT                      off                     off
IFLIMITCLR                   off                     off
INSLIMIT                     off                     off
GLBLIMIT                     off                     off
HWMGMDGMPGLOBALLIMITCLEAR    off                     off
HWMGMDGMPTOTALLIMITCLEAR     off                     off
JOINGRP                      off                     off
LEAVEGRP                     off                     off
```

Table 10-128 Description of the **display snmp-agent trap feature-name mld all** command output

Item	Description
Feature name	Name of the module

Item	Description
Trap number	Number of trap messages of a specific type
Trap name	Types of trap messages: ● IFLIMIT: a trap message indicating that the number of MLD entries on the interface reaches the limit value. ● IFLIMITCLR: the number of MLD entries on an interface falls below the limit value. ● INSLIMIT: a trap message indicating that the number of MLD entries in the instance reaches the limit value. ● GLBLIMIT: a trap message indicating that the total number of MLD entries of all instances reaches the limit value. ● HWMGMDGMPGLOBALLIMITCLEAR: a trap message indicates that the number of MLD entries in an instance has fallen below the limit. ● HWMGMDGMPTOTALLIMITCLEAR: a trap message indicating that the total number of MLD entries in all instances has fallen below the limit. ● JOINGRP: a trap message indicating that a MLD Join message is received ● LEAVEGRP: a trap message indicating that a MLD Leave message is received or the group timer expires
Default switch status	Status of the default trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Status of the current trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

10.11.18 snmp-agent trap enable feature-name mld

10.11.5 display snmp-agent trap feature-name mrm all

Function

The **display snmp-agent trap feature-name mrm all** command displays whether the trap function is enabled for the MRM module.

Format

display snmp-agent trap feature-name mrm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name mrm all** command to view the status of all MRM traps when you want to monitor the current status of MRM protocol events but are not sure whether the MRM trap function is enabled.

Example

Display whether the trap function is enabled for the MRM module.

```
<Huawei> display snmp-agent trap feature-name mrm all
-------------------------------------------------------------------------------
Feature name: MRM
Trap number : 4
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwIpMcastSGThresholdExceed      off                       off
hwIpMcastSGThresholdExceedClear
                             off                     off
hwIpMcastSGExceed              off                     off
hwIpMcastSGExceedClear         off                       off
```

Table 10-129 Description of the **display snmp-agent trap feature-name mrm all** command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap event types.

Item	Description
Trap name	Trap event type. The following types of trap events are defined: ● hwIpMcastSGThresholdExceed: The proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed exceeds the upper alarm threshold. ● hwIpMcastSGThresholdExceedClear: The proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed falls below the lower alarm threshold. ● hwIpMcastSGExceed: The number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed. ● hwIpMcastSGExceedClear: The number of (S, G) multicast forwarding entries created falls below the maximum number of (S, G) multicast forwarding entries allowed.
Default switch status	Default status of a trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Current status of a trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

10.11.19 snmp-agent trap enable feature-name mrm

10.11.6 display snmp-agent trap feature-name msdp all

Function

The **display snmp-agent trap feature-name msdp all** command displays the status of all MSDP traps.

Format

display snmp-agent trap feature-name msdp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name msdp all** command to view the status of all MSDP traps when you want to monitor the current status of MSDP protocol events but are not sure whether the MSDP trap function is enabled.

Example

Display whether the trap function is enabled for the MSDP module.

```
<Huawei> display snmp-agent trap feature-name msdp all
-----------------------------------------------------------------------------
Feature name: MSDP
Trap number : 2
-----------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
establish                off                     off
backward                 off                     off
```

Table 10-130 Description of the display snmp-agent trap feature-name msdp all command output

Item	Description
Feature name	Indicates the name of the module.
Trap number	Indicates the type number of a trap.
Trap name	Indicates the event type. The event types are as follows: ● establish: indicates that an MSDP peer is established. ● backward: indicates that an MSDP peer is removed.
Default switch status	Status of the default trap switch: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Status of the current trap switch: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

10.11.20 snmp-agent trap enable feature-name msdp

10.11.7 display snmp-agent trap feature-name pim all

Function

The **display snmp-agent trap feature-name pim all** command displays the status of all PIM traps.

Format

display snmp-agent trap feature-name pim all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display snmp-agent trap feature-name pim all** command to view the status of all PIM traps when you want to monitor the current status of PIM protocol events but are not sure whether the PIM trap function is enabled.

Example

Display whether the trap function is enabled for the PIM module.

```
<Huawei> display snmp-agent trap feature-name pim all
-----------------------------------------------------------------------------
Feature name: PIM
Trap number : 16
-----------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
neighbor-loss            off                     on
```

```
invalid-register              off                    on
invalid-join-prune            off                    on
rp-mapping-change             off                    on
interface-election            off                    on
new-neighbor                  off                    on
mrt-limit                     off                    on
HWPIMMRTLIMITCLEAR            off                    on
hwPimStarGThresholdExceed     off                    on
hwPimSGThresholdExceed        off                    on
hwPimStarGExceed              off                    on
hwPimSGExceed                 off                    on
hwPimStarGThresholdExceedClear  off                  on
hwPimSGThresholdExceedClear   off                    on
hwPimStarGExceedClear         off                    on
hwPimSGExceedClear            off                    on
```

Table 10-131 Description of the **display snmp-agent trap feature-name pim all** command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap event types.

Item	Description
Trap name	Trap event type. The following types of trap events are defined: ● neighbor-loss: A neighbor is lost. ● invalid-register: An invalid Register message is received. ● invalid-join-prune: An invalid Join/Prune message is received. ● rp-mapping-change: The RP-mapping changes. ● interface-election: An interface is elected as the DR. ● new-neighbor: A new neighbor appears. ● mrt-limit: The number of PIM entries exceeds the limit for the multicast routing table (MRT). ● HWPIMMRTLIMITCLEAR: The total number of PIM entries falls below the limit. ● hwPimStarGThresholdExceed: The proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed exceeds the upper alarm threshold. ● hwPimSGThresholdExceed: The proportion of PIM (S, G) entries created to the maximum PIM (S, G) entries allowed exceeds the upper alarm threshold. ● hwPimStarGExceed: The number of PIM (*, G) entries created exceeds the maximum number of PIM (*, G) entries allowed. ● hwPimSGExceed: The number of PIM (S, G) entries created exceeds the maximum number of PIM (S, G) entries allowed. ● hwPimStarGThresholdExceedClear: The proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed falls below the lower alarm threshold. ● hwPimSGThresholdExceedClear: The proportion of PIM (S, G) entries created to the maximum PIM (S, G)

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	entries allowed falls below the lower alarm threshold. ● hwPimStarGExceedClear: The number of PIM (*, G) entries created falls below the maximum number of PIM (*, G) entries allowed. ● hwPimSGExceedClear: The number of PIM (S, G) entries created falls below the maximum number of PIM (S, G) entries allowed.
Default switch status	Default status of a trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Current status of a trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

10.11.21 snmp-agent trap enable feature-name pim

10.11.8 display snmp-agent trap feature-name pim-std all

Function

The **display snmp-agent trap feature-name pim-std all** command displays the status of all PIM-STD traps.

Format

display snmp-agent trap feature-name pim-std all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display snmp-agent trap feature-name pim-std all** command to view the status of all PIM-STD MIB traps when you want to monitor the current status of the public PIM protocol events but are not sure whether the PIM-STD MIB trap function is enabled.

Example

View the status of all PIM-STD MIB traps.

```
<Huawei> display snmp-agent trap feature-name pim-std all
-------------------------------------------------------------------------------
Feature name: pim-std
Trap number : 5
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
pimneighborloss                off                     on
piminvalidregister            off                     on
piminvalidjoinprune            off                     on
pimrpmappingchange               off                     on
piminterfaceelection           off                     on
```

Table 10-132 Description of the display snmp-agent trap feature-name pim-std all command output

Item	Description
Feature name	Feature name
Trap number	Number of trap message types
Trap name	Types of trap messages: ● pimneighborloss: A neighbor relationship is lost. ● piminvalidregister: An invalid Register message is received. ● piminvalidjoinprune: An invalid Join or Prune message is received. ● pimrpmappingchange: RP-Mapping changes. ● piminterfaceelection: The interface is elected as the DR.
Default switch status	Default status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Current status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

10.11.22 snmp-agent trap enable feature-name pim-std

10.11.9 igmp trap-interval limit

Function

The **igmp trap-interval limit** command configures the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit.

The **undo igmp trap-interval limit** command deletes the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit. When the joining failure event occurs, a trap message is sent immediately.

By default, the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit is not limited

Format

igmp trap-interval limit *min-interval*

undo igmp trap-interval limit

Parameters

Parameter	Description	Value
min-interval	Specifies the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.

Views

Multicast MIB view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When the interval is configured to 0 by using the **igmp trap-interval limit** command, the interval for IGMP to send trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit is not limited; otherwise, the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit should be equal to or longer than the configured one.

Example

Set the interval for sending trap messages of the failure of IGMP joining because the number of the IGMP entries exceeds the limit to 50 seconds.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] igmp trap-interval limit 50
```

10.11.10 mgmd total-number threshold-alarm

Function

The **mgmd total-number threshold-alarm** command sets the upper and lower alarm thresholds for IGMP/MLD entries.

The **undo mgmd total-number threshold-alarm** command restores the default alarm thresholds for IGMP/MLD entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

mgmd total-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mgmd total-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for IGMP/MLD entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for IGMP/MLD entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of IGMP/MLD entries. After the number of IGMP/MLD entries reaches the maximum value, no more IGMP/MLD entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operation and maintenance, configure the upper and lower alarm thresholds for IGMP/MLD entries. IGMP/MLD entry alarms and clear alarms help you learn IGMP/MLD entry usage in a timely manner. The **mgmd total-number threshold-alarm** command allows you to flexibly adjust the alarm thresholds for IGMP/MLD entries based on service requirements. Note that:

- If the proportion of existing IGMP/MLD entries to the maximum number reaches *upper-limit-value*, an IGMP/MLD entry alarm is reported for all VPN instances. This alarm is informational only and does not affect creation of new IGMP/MLD entries.
- If the proportion of existing IGMP/MLD entries to the maximum number falls below *lower-limit-value*, an IGMP/MLD entry clear alarm is reported for all VPN instances.

Prerequisites

This command only configures the alarm thresholds for IGMP/MLD entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name igmp trap-name** { **hwmgmdtotallimitthresholdexceed** | **hwmgmdtotallimitthresholdexceedclear** } command twice to enable the device to report IGMP/MLD entry alarms and clear alarms.

Precautions

If the **mgmd total-number threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for IGMP/MLD entries.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] mgmd total-number threshold-alarm upper-limit 88 lower-limit 77
```

10.11.11 mgmd host threshold-alarm

Function

The **mgmd host threshold-alarm** command configures the upper and lower alarm thresholds for the multicast entry usage of all instances on a user-side IGMP/MLD device.

The **undo mgmd host threshold-alarm** command restores the default upper and lower alarm thresholds.

 Copyright © Huawei Technologies Co., Ltd.

By default, the upper and lower alarm thresholds are 80% and 75%, respectively.

Format

mgmd host { **star-group-number** | **source-group-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo mgmd host { **star-group-number** | **source-group-number** } **threshold-alarm**

Parameters

Parameter	Description	Value
star-group-number	Enables you to configure the upper and lower alarm thresholds for the (*, G) entry usage of all instances.	-
source-group-number	Enables you to configure the upper and lower alarm thresholds for the (S, G) entry usage of all instances.	-
upper-limit *upper-limit-value*	Configures an upper alarm threshold for the multicast entry usage of all instances, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Configures a lower alarm threshold for the multicast entry usage of all instances, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user-side IGMP/MLD device has an upper limit for the number of multicast entries. When this upper limit is reached, the device cannot create new entries, so it will reject new multicast service requests. To resolve this issue and facilitate device maintenance, run the **mgmd host threshold-alarm** command to configure the upper and lower alarm thresholds for the multicast entry usage on a user-side IGMP/MLD device, enabling you to learn the multicast entry usage status. After the **mgmd host threshold-alarm** command is run:

- When the value of *upper-limit-value* is reached, the device triggers a multicast entry usage alarm. Such an alarm is a notification only, and the device can

still create new multicast entries before the multicast entry usage reaches 100%.

- When the multicast entry usage falls below the value specified by *lower-limit-value*, the device triggers a clear alarm for the multicast entry usage alarm.

Prerequisites

The **mgmd host threshold-alarm** command works with the **snmp-agent trap enable feature-name igmp trap-name** { **hwmgmdhoststargthresholdexceed** | **hwmgmdhoststargthresholdexceedclear** | **hwmgmdhostsgthresholdexceed** | **hwmgmdhostsgthresholdexceedclear** } command. The former one configures the upper and lower alarm thresholds, while the latter one enables or disables the function to report alarms.

Precautions

If the **mgmd host threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

Example

Configure the upper and lower alarm thresholds for the (*, G) entry usage of all instances.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] mgmd host star-group-number threshold-alarm upper-limit 88 lower-limit 77
```

Configure the upper and lower alarm thresholds for the (S, G) entry usage of all instances.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] mgmd host source-group-number threshold-alarm upper-limit 88 lower-limit 77
```

10.11.12 multicast forwarding-table source-group-number threshold-alarm

Function

The **multicast forwarding-table source-group-number threshold-alarm** command configures the upper and lower alarm thresholds for multicast forwarding entries.

The **undo multicast forwarding-table source-group-number threshold-alarm** command restores the default alarm thresholds for multicast forwarding entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

multicast forwarding-table source-group-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo multicast forwarding-table source-group-number threshold-alarm

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold for multicast forwarding entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold for multicast forwarding entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of multicast forwarding entries. After the number of multicast forwarding entries reaches the maximum value, no more multicast forwarding entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operation and maintenance, configure the upper and lower alarm thresholds for multicast forwarding entries. Multicast forwarding entry alarms and clear alarms help you learn IGMP/MLD entry usage in a timely manner. The **multicast forwarding-table source-group-number threshold-alarm** command allows you to flexibly adjust the alarm thresholds for multicast forwarding entries based on service requirements. Note that:

- If the proportion of existing multicast forwarding entries to the maximum number reaches *upper-limit-value*, a multicast forwarding entry alarm is reported. This alarm is informational only and does not affect creation of new multicast forwarding entries.
- If the proportion of existing multicast forwarding entries to the maximum number falls below *lower-limit-value*, a multicast forwarding entry clear alarm is reported.

Prerequisites

This command only configures the alarm thresholds for multicast forwarding entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name mrm trap-name** { **hwipmcastsgthresholdexceed** | **hwipmcastsgthresholdexceedclear** } command twice to enable the device to report multicast forwarding entry alarms and clear alarms.

Precautions

If the **multicast forwarding-table source-group-number threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for multicast forwarding entries.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] multicast forwarding-table source-group-number threshold-alarm upper-limit 88
lower-limit 77
```

10.11.13 multicast mib-notification join-leave frequency

Function

The **multicast mib-notification join-leave frequency** command sets the maximum number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.

The **undo multicast mib-notification join-leave frequency** command restores the default number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.

By default, the system does not send any trap message when IGMP/MLD joining or leaving events occur.

Format

multicast mib-notification join-leave frequency *count*

undo multicast mib-notification join-leave frequency

Parameters

Parameter	Description	Value
count	Specifies the maximum number of trap messages sent by the system per second when IGMP/MLD joining or leaving events occur.	The value is an integer that ranges from 0 to 240. The unit is in packets per second. The default value is 0.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum number of trap messages sent by the system per second to 30 when IGMP/MLD joining or leaving events occur.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] multicast mib-notification join-leave frequency 30
```

10.11.14 multicast-mib

Function

The **multicast-mib** command enables the multicast MIB and displays the multicast MIB view.

The **undo multicast-mib** command deletes all configurations in the multicast MIB view.

By default, the multicast MIB is not enabled.

Format

multicast-mib

undo multicast-mib

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **undo multicast-mib** command to delete all configurations in the multicast MIB view.

NOTICE

In using the **undo multicast-mib** command, you need to enter Y or N to confirm the action. This command will clear global multicast MIB configurations. So, use this command with caution.

Example

Enable multicast MIB and enter the multicast MIB view.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib]
```

10.11.15 pim mib-notification interval

Function

The **pim mib-notification interval** command sets the interval for PIM to send trap messages about various events.

The **undo pim mib-notification interval** command restores the default interval for PIM to send various trap messages.

By default, an alarm is generated only when a neighbor loss event or a neighbor addition event occurs. No alarm is generated when the other events occur.

Format

pim mib-notification interval { **interface-election-dr** *election-value* | **invalid-join-prune** *jp-value* | **invalid-register** *register-value* | **neighbor-loss** *loss-value* | **new-neighbor** *new-value* | **rp-mapping-change** *change-value* | **mrt-limit** *mrt-value* }

undo pim mib-notification interval { **all** | **interface-election-dr** | **invalid-join-prune** | **invalid-register** | **neighbor-loss** | **new-neighbor** | **rp-mapping-change** | **mrt-limit** }

Parameters

Parameter	Description	Value
interface-election-dr *election-value*	Specifies the minimum interval for sending trap messages about DR election.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 65535 seconds.
invalid-join-prune *jp-value*	Specifies the minimum interval for sending trap messages about invalid Join/Prune messages.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 65535 seconds.
invalid-register *register-value*	Specifies the minimum interval for sending trap messages about invalid Register messages.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 65535 seconds.
mrt-limit *mrt-value*	Specifies the minimum interval for sending trap messages about the failure in joining multicast groups because the number of PIM entries reaches the upper limit.	The value is an integer that ranges from 10 to 65535, in seconds. By default, the value is 65535 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
neighbor-loss *loss-value*	Specifies the minimum interval for sending trap messages about neighbor loss.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.
new-neighbor *new-value*	Specifies the minimum interval for sending trap messages about neighbor addition.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 0 seconds.
rp-mapping-change *change-value*	Specifies the minimum interval for sending trap messages about the RP-mapping change.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 65535 seconds.
all	Restore the default interval for PIM to send all trap messages.	-

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

The **pim mib-notification interval** command sets the interval for sending trap messages. When an event occurs, if the period since the last time for sending the trap message is shorter than the configured interval, the system does not send any trap message.

- If the default interval is 0, it indicates that a trap message is sent immediately after an event occurs.
- If the default interval is 65535, it indicates that no trap message is sent after an event occurs. Then run this command to adjust the interval to a smaller value so that a trap message can be sent after an event occurs.

Example

Set the interval for PIM to send trap messages about invalid Join/Prune messages.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] pim mib-notification interval invalid-join-prune 50
```

10.11.16 pim threshold-alarm

Function

The **pim threshold-alarm** command configures the upper and lower alarm thresholds for PIM entries.

The **undo pim threshold-alarm** command restores the default alarm thresholds for PIM entries.

By default, the upper and lower alarm thresholds are 80% and 75% respectively.

Format

pim { **star-group-number** | **source-group-number** } **threshold-alarm upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*

undo pim { **star-group-number** | **source-group-number** } **threshold-alarm**

Parameters

Parameter	Description	Value
star-group-number	Sets the alarm thresholds for PIM (*, G) entries.	-
source-group-number	Sets the alarm thresholds for PIM (S, G) entries.	-
upper-limit *upper-limit-value*	Specifies the upper alarm threshold value for PIM entries, in percentage.	The value is an integer ranging from 1 to 100.
lower-limit *lower-limit-value*	Specifies the lower alarm threshold value for PIM entries, in percentage.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

Multicast MIB view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device supports a limited number of PIM entries. After the number of PIM entries reaches the maximum value, no more PIM entries can be created. As a result, some multicast traffic cannot be forwarded. To facilitate network operation and maintenance, configure the upper and lower alarm thresholds for PIM entries.

 Copyright © Huawei Technologies Co., Ltd.

PIM entry alarms and clear alarms help you learn PIM entry usage in a timely manner. The **pim threshold-alarm** command allows you to flexibly adjust the alarm thresholds for PIM entries based on service requirements. Note that:

- If the proportion of existing PIM entries to the maximum number reaches *upper-limit-value*, a PIM entry alarm is reported. This alarm is informational only and does not affect creation of new PIM entries.
- If the proportion of existing PIM entries to the maximum number falls below *lower-limit-value*, a PIM entry clear alarm is reported.

Prerequisites

This command only configures the alarm thresholds for PIM entries. To enable the configured alarm thresholds to take effect, run the **snmp-agent trap enable feature-name pim trap-name** { **hwpimsgthresholdexceed** | **hwpimsgthresholdexceedclear** | **hwpimstargthresholdexceed** | **hwpimstargthresholdexceedclear** } command twice to enable the device to report PIM entry alarms and clear alarms.

Precautions

If the **pim threshold-alarm** command is executed multiple times, only the latest configuration takes effect.

Example

Configure the upper and lower alarm thresholds for PIM (*, G) entries.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] pim star-group-number threshold-alarm upper-limit 88 lower-limit 77
```

Configure the upper and lower alarm thresholds for PIM (S, G) entries.

```
<Huawei> system-view
[Huawei] multicast-mib
[Huawei-mcast-mib] pim source-group-number threshold-alarm upper-limit 88 lower-limit 77
```

10.11.17 snmp-agent trap enable feature-name igmp

Function

The **snmp-agent trap enable feature-name igmp** command enables the trap function for the IGMP module.

The **undo snmp-agent trap enable feature-name igmp** command disables the trap function for the IGMP module.

By default, the trap function for IGMP events is disabled.

Format

snmp-agent trap enable feature-name igmp [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** | **hwmgmdtotallimitthresholdexceed** | **hwmgmdtotallimitthresholdexceedclear** | **hwmgmdhoststargthresholdexceed** | **hwmgmdhoststargthresholdexceedclear** | **hwmgmdhoststargexceed** | **hwmgmdhoststargexceedclear** | **hwmgmdhostsgthresholdexceed** |

hwmgmdhostsgthresholdexceedclear | **hwmgmdhostsgexceed** | **hwmgmdhostsgexceedclear** }]

undo snmp-agent trap enable feature-name igmp [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** | **hwmgmdtotallimitthresholdexceed** | **hwmgmdtotallimitthresholdexceedclear** | **hwmgmdhoststargthresholdexceed** | **hwmgmdhoststargthresholdexceedclear** | **hwmgmdhoststargexceed** | **hwmgmdhoststargexceedclear** | **hwmgmdhostsgthresholdexceed** | **hwmgmdhostsgthresholdexceedclear** | **hwmgmdhostsgexceed** | **hwmgmdhostsgexceedclear** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap for a specified type of IGMP event.	-
glblimit	Enables the trap for the event indicating that the total number of the IGMP entries of all instances reaches the limit.	-
iflimit	Enables the trap for the event indicating that the number of IGMP entries on an interface reaches the limit.	-
iflimitclr	Enables the trap for the event indicating that the number of IGMP entries on an interface falls below the limit.	-
inslimit	Enables the trap for the event indicating that the number of IGMP entries in an instance reaches the limit.	-
joingrp	Enables the trap for the event indicating that an IGMP Join message is received.	-
leavegrp	Enables the trap for the event indicating that an IGMP Leave message is received or the group timer expires.	-
hwmgmdgmptotallimitclear	Enables the trap for the event indicating that the number of IGMP entries in all instances falls below the upper threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwmgmdgmpgloballimitclear	Enables the trap for the event indicating that the number of IGMP entries a single instance falls below the upper threshold.	-
hwmgmdtotallimitthresholdexceed	Generates an alarm when the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed reaches the upper alarm threshold.	-
hwmgmdtotallimitthresholdexceedclear	Generates a clear alarm when the proportion of global IGMP/MLD entries created to the maximum global IGMP/MLD entries allowed falls below the lower alarm threshold.	-
hwmgmdhoststargthresholdexceed	Generates an alarm when the (*, G) entry usage of all instances reaches the specified upper alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhoststargthresholdexceedclear	Generates a clear alarm when the (*, G) entry usage of all instances falls below the specified lower alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhoststargexceed	Generates an alarm when the number of (*, G) entries of all instances exceeds the maximum number allowed on the user-side IGMP/MLD device.	-
hwmgmdhoststargexceedclear	Generates a clear alarm when the number of (*, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwmgmdhostsgthresholdexceed	Generates an alarm when the (S, G) entry usage of all instances reaches the specified upper alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhostsgthresholdexceedclear	Generates a clear alarm when the (S, G) entry usage of all instances falls below the specified lower alarm threshold on the user-side IGMP/MLD device.	-
hwmgmdhostsgexceed	Generates an alarm when the number of (S, G) entries of all instances exceeds the maximum number allowed on the user-side IGMP/MLD device.	-
hwmgmdhostsgexceedclear	Generates a clear alarm when the number of (S, G) entries of all instances falls below the maximum number allowed on the user-side IGMP/MLD device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for a specific type of event, specify **trap-name**. To enable the trap function for multiple types of events, run this command multiple times.

Example

Enable the trap for the event indicating that an IGMP Join message is received.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name igmp trap-name joingrp
```

Disable the trap for the event indicating that an IGMP Join message is received.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name igmp trap-name joingrp
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

10.11.3 display snmp-agent trap feature-name igmp all

10.11.18 snmp-agent trap enable feature-name mld

Function

The **snmp-agent trap enable feature-name mld** command enables the trap function for the MLD module.

The **undo snmp-agent trap enable feature-name mld** command disables the trap function for the MLD module.

By default, the trap function for MLD events is disabled.

Format

snmp-agent trap enable feature-name mld [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** }]

undo snmp-agent trap enable feature-name mld [**trap-name** { **glblimit** | **iflimit** | **iflimitclr** | **inslimit** | **joingrp** | **leavegrp** | **hwmgmdgmptotallimitclear** | **hwmgmdgmpgloballimitclear** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap of MLD events of specified types.	-
glblimit	Enables the trap that the total number of the MLD entries of all instances reaches the limit value.	-
iflimit	Enables the trap that the number of MLD entries on an interface reaches the limit value.	-
iflimitclr	Enables the trap that the number of MLD entries on an interface falls below the limit value.	-
inslimit	Enables the trap that the number of MLD entries in an instance reaches the limit value.	-
joingrp	Enables the trap of the event that an MLD Join message is received.	-
leavegrp	Enables the trap of the event that an MLD Leave message is received or the group timer expires.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwmgmdgmptotallimitclear	Generates an alarm when the number of MLD entries in all instances falls below the upper threshold.	-
hwmgmdgmpgloballimitclear	Generates an alarm when the number of MLD entries in a single instance falls below the upper threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function of one or more types of trap messages, specify **trap-name**.

Example

Enable the trap of the event that an MLD Join message is received.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mld trap-name joingrp
```

Disable the trap of the event that an MLD Join message is received.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name mld trap-name joingrp
```

Related Topics

10.11.4 display snmp-agent trap feature-name mld all

10.11.19 snmp-agent trap enable feature-name mrm

Function

The **snmp-agent trap enable feature-name mrm** command enables the trap function for the Multicast Routing Management (MRM) module.

The **undo snmp-agent trap enable feature-name mrm** command disables the trap function for the MRM module.

By default, the trap function for MRM events is disabled.

Format

snmp-agent trap enable feature-name mrm [**trap-name** { **hwipmcastsgexceed** | **hwipmcastsgexceedclear** | **hwipmcastsgthresholdexceed** | **hwipmcastsgthresholdexceedclear** }]

undo snmp-agent trap enable feature-name mrm [**trap-name** { **hwipmcastsgexceed** | **hwipmcastsgexceedclear** | **hwipmcastsgthresholdexceed** | **hwipmcastsgthresholdexceedclear** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap for a specified type of MRM event.	-
hwipmcastsgexceed	Enables the trap for the event indicating that the number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed.	-
hwipmcastsgexceedclear	Enables the trap for the event indicating that the number of (S, G) multicast forwarding entries created falls below the maximum number of (S, G) multicast forwarding entries allowed.	-
hwipmcastsgthresholdexceed	Enables the trap for the event indicating that the proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed exceeds the upper alarm threshold.	-
hwipmcastsgthresholdexceedclear	Enables the trap for the event indicating that the proportion of (S, G) multicast forwarding entries created to the maximum (S, G) multicast forwarding entries allowed falls below the lower alarm threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for a specific type of event, specify **trap-name**. To enable the trap function for multiple types of events, run this command multiple times.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enables the trap for the event indicating that the number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mrm trap-name hwipmcastsgexceed
```

Disable the trap for the event indicating that the number of (S, G) multicast forwarding entries created exceeds the maximum number of (S, G) multicast forwarding entries allowed.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name mrm trap-name hwipmcastsgexceed
```

Related Topics

10.11.5 display snmp-agent trap feature-name mrm all

10.11.20 snmp-agent trap enable feature-name msdp

Function

The **snmp-agent trap enable feature-name msdp** command enables the traps function for the MSDP module.

The **undo snmp-agent trap enable feature-name msdp** command disables the traps function for the MSDP module.

By default, the trap function for MSDP events is disabled.

Format

snmp-agent trap enable feature-name msdp [**trap-name** { **establish** | **backward** }]

undo snmp-agent trap enable feature-name msdp [**trap-name** { **establish** | **backward** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of MSDP events of specified types.	-
establish	Enables the trap of the setup of the MSDP peer relationship.	-
backward	Enables the trap of the deletion of the MSDP peer relationship.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the traps of one or more events, you can specify **trap-name**.

Example

Enable the trap of the setup of the MSDP peer relationship in the system view.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name msdp trap-name establish
```

Disable the trap of the setup of the MSDP peer relationship in the system view.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name msdp trap-name establish
```

Related Topics

10.11.6 display snmp-agent trap feature-name msdp all

10.11.21 snmp-agent trap enable feature-name pim

Function

The **snmp-agent trap enable feature-name pim** command enables the trap function for PIM events.

The **undo snmp-agent trap enable feature-name pim** command disables the trap function for PIM events.

By default, the trap function for PIM events is disabled.

Format

snmp-agent trap enable feature-name pim [**trap-name** { **neighbor-loss** | **invalid-join-prune** | **rp-mapping-change** | **interface-election** | **invalid-register** | **new-neighbor** | **mrt-limit** | **hwpimmrtlimitclear** | **hwpimsgexceed** | **hwpimsgexceedclear** | **hwpimsgthresholdexceed** | **hwpimsgthresholdexceedclear** | **hwpimstargexceed** | **hwpimstargexceedclear** | **hwpimstargthresholdexceed** | **hwpimstargthresholdexceedclear** }]

undo snmp-agent trap enable feature-name pim [**trap-name** { **neighbor-loss** | **invalid-join-prune** | **rp-mapping-change** | **interface-election** | **invalid-register** | **new-neighbor** | **mrt-limit** | **hwpimmrtlimitclear** | **hwpimsgexceed** | **hwpimsgexceedclear** | **hwpimsgthresholdexceed** | **hwpimsgthresholdexceedclear** | **hwpimstargexceed** | **hwpimstargexceedclear** | **hwpimstargthresholdexceed** | **hwpimstargthresholdexceedclear** }]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name	Enables the trap for a specified type of PIM event.	-
neighbor-loss	Enables the trap for the PIM neighbor loss event.	-
invalid-join-prune	Enables the trap for the event indicating that an invalid Join/Prune message is received.	-
rp-mapping-change	Enables the trap for the PIM RP-mapping change event.	-
interface-election	Enables the trap for the event indicating that a PIM interface is elected as the DR.	-
invalid-register	Enables the trap for the event indicating that an invalid Register message is received.	-
new-neighbor	Enables the trap for the event indicating that a new PIM neighbor appears.	-
mrt-limit	Enables the trap for the event indicating that the number of PIM entries exceeds the limit.	-
hwpimmrtlimitclear	Enables the trap for the event indicating that the total number of PIM entries falls below the limit.	-
hwpimsgexceed	Enables the trap for the event indicating that the number of PIM (S, G) entries created exceeds the maximum number of PIM (S, G) entries allowed.	-
hwpimsgexceedclear	Enables the trap for the event indicating that the number of PIM (S, G) entries created falls below the maximum number of PIM (S, G) entries allowed.	-
hwpimsgthresholdexceed	Enables the trap for the event indicating that the proportion of PIM (S, G) entries created to the maximum PIM (S, G) entries allowed exceeds the upper alarm threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwpimsgthresholdexceedclear	Enables the trap for the event indicating that the proportion of PIM (S, G) entries created to the maximum PIM (S, G) entries allowed falls below the lower alarm threshold.	-
hwpimstargexceed	Enables the trap for the event indicating that the number of PIM (*, G) entries created exceeds the maximum number of PIM (*, G) entries allowed.	-
hwpimstargexceedclear	Enables the trap for the event indicating that the number of PIM (*, G) entries created falls below the maximum number of PIM (*, G) entries allowed.	-
hwpimstargthresholdexceed	Enables the trap for the event indicating that the proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed exceeds the upper alarm threshold.	-
hwpimstargthresholdexceedclear	Enables the trap for the event indicating that the proportion of PIM (*, G) entries created to the maximum PIM (*, G) entries allowed falls below the lower alarm threshold.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for a specific type of event, specify **trap-name**. To enable the trap function for multiple types of events, run this command multiple times.

Example

Enable the trap for the PIM neighbor loss event in the system view.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name pim trap-name neighbor-loss
```

Disable the trap for the PIM neighbor loss event in the system view.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name pim trap-name neighbor-loss
```

Related Topics

10.11.7 display snmp-agent trap feature-name pim all

10.11.15 pim mib-notification interval

10.11.22 snmp-agent trap enable feature-name pim-std

Function

The **snmp-agent trap enable feature-name pim-std** command enables PIM-STD traps.

The **undo snmp-agent trap enable feature-name pim-std** command disables related PIM-STD traps.

By default, the trap function for PIM-STD MIB events is disabled.

Format

snmp-agent trap enable feature-name pim-std [**trap-name** { **pimneighborloss** | **piminvalidregister** | **piminvalidjoinprune** | **pimrpmappingchange** | **piminterfaceelection** }]

undo snmp-agent trap enable feature-name pim-std [**trap-name** { **pimneighborloss** | **piminvalidregister** | **piminvalidjoinprune** | **pimrpmappingchange** | **piminterfaceelection** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for specific events.	-
pimneighborloss	Enables the trap function for the PIM-STD MIB events of neighbor loss.	-
piminvalidregister	Enables the trap function for the PIM-STD MIB events of invalid Register messages.	-
piminvalidjoinprune	Enables the trap function for the PIM-STD MIB events of invalid Join/Prune messages.	-
pimrpmappingchange	Enables the trap function for the PIM-STD MIB events of RP-Mapping change.	-
piminterfaceelection	Enables the trap function for the PIM-STD MIB events of interface election.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

At present, the defined public PIM-STD MIB traps events include neighbor loss, invalid Join/Prune messages, RP-mapping change, interface election, and invalid Register messages. You can run the **snmp-agent trap enable feature-name pim-std** command to enable the trap function for PIM-STD MIB events when you need to monitor the current status of PIM protocol events.

Precautions

When using the **snmp-agent trap enable feature-name pim-std**, note the following points:

- Run the **snmp-agent trap enable feature-name pim-std** command directly to enable the trap function for all PIM-STD MIB events.
- Specify **trap-name** to enable the trap function for a specified type of PIM-STD MIB events.

Example

Enable the trap function for the PIM-STD MIB events of neighbor loss.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name pim-std trap-name pimneighborloss
```

Enable the trap function for all PIM-STD MIB events.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name pim-std
```

Disable the trap function for the PIM-STD MIB events of neighbor loss.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name pim-std trap-name pimneighborloss
```

Related Topics

10.11.8 display snmp-agent trap feature-name pim-std all

 Copyright © Huawei Technologies Co., Ltd.

11 MPLS Commands

About This Chapter

NOTE

The AR100&AR120&AR150&AR160&AR200 do not support MPLS.

11.1 Basic MPLS Configuration Commands

11.2 MPLS TE Configuration Commands

11.1 Basic MPLS Configuration Commands

11.1.1 apply lsp public

Function

The **apply lsp public** command specifies an LSP for forwarding the public network packets that meet the filtering rules.

The **undo apply lsp public** command restores the default setting.

By default, the policy-based routing (PBR) is not used for forwarding public network packets.

Format

apply lsp public *pe-address* [*p-address* | *interface-type interface-number* | **secondary**]

undo apply lsp public *pe-address*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
pe-address	Specifies the IP address of the peer PE.	-
p-address	Specifies the IP address of the P. *p-address* and *pe-address* together specify the next P that an LSP passes through.	-
interface-type interface-number	Specifies the next outbound interface of an LSP, together with *pe-address*. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary	Indicates the backup LSP generated through LDP fast reroute (FRR). When **secondary** is not configured, only the primary LSP forwards packets. When **secondary** is configured, only the backup LSP forwards packets.	-

Views

Policy-Based-Route view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **apply lsp public** command to specify an LSP for forwarding services on an MPLS network.

Prerequisites

You have configured a route-policy using the **policy-based-route** command.

Precautions

After configuring a PBR to the PE address and the P address, if there is no reachable LSP to them, the PBR is ineffective.

Example

Specify the LSP of the PE with IP address 10.1.1.1 for forwarding the public network packets that match ACL 2000.

```
<Huawei> system-view
[Huawei] policy-based-route map1 permit node 10
[Huawei-policy-based-route-map1-10] if-match acl 2000
[Huawei-policy-based-route-map1-10] apply lsp public 10.1.1.1
```

Related Topics

9.11.44 policy-based-route

11.1.2 authentication exclude

Function

The **authentication exclude** command configures LDP peers in a batch that a local device does not authenticate after LDP keychain or LDP MD5 is configured to authenticate all LDP peers or LDP peers in a specified group.

The **undo authentication exclude** command enables a local device to authenticate all LDP peers using LDP keychain or LDP MD5.

By default, a local device is enabled to authenticate all LDP peers using LDP keychain or LDP MD5.

Format

authentication exclude peer *peer-id*

undo authentication exclude peer *peer-id*

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the ID of an LDP peer.	This value is in dotted decimal notation.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a local device is enabled to authenticate all LDP peers using LDP keychain or LDP MD5 after LDP keychain or LDP MD5 is configured for a peer group or all LDP peers. To disable the local device from authenticating some LDP peers, run the **authentication exclude** command.

Precautions

The following commands are mutually exclusive for a specified LDP peer:

- **authentication key-chain peer** *peer-id* **name** *keychain-name*
- **md5-password** { **plain** | **cipher** } *peer-lsr-id password*

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable a local device from authenticating an LDP peer with IP address **4.4.4.4** after LDP keychain or MD5 is configured for all LDP peers or LDP peers in a specified group.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] authentication exclude peer 4.4.4.4
```

11.1.3 authentication key-chain

Function

The **authentication key-chain** command enables Label Distribution Protocol (LDP) keychain authentication.

The **undo authentication key-chain** command disables Label Distribution Protocol (LDP) keychain authentication.

By default, LDP keychain authentication is disabled.

Format

authentication key-chain peer *peer-id* **name** *keychain-name*

undo authentication key-chain peer *peer-id*

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the ID of an LDP peer enabled with LDP keychain. The parameter is specified in the **mpls lsr-id** command.	The value is in dotted decimal notation.
name *keychain-name*	Specifies the keychain name. The keychain name is specified in the **keychain** command.	The value is an existing keychain name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

Information spoofing may occur during an LDP session. To enhance security of an LDP session, configure keychain authentication for a TCP connection over which an LDP session is created.

During keychain authentication, a group of passwords are defined to form a password string, and each password is specified with the encryption and decryption algorithms such as MD5 and SHA-1, and is configured with a validity period. When sending or receiving a packet, the system selects a valid password based on the user's configuration. Within the password validity period, the system either uses the encryption algorithm matching the password to encrypt the packet before sending it or uses the decryption algorithm matching the password to decrypt the packet before receiving it. In addition, the system automatically uses a new password after the previous one expires, preventing the password from being decrypted.

The keychain authentication password, the encryption and decryption algorithms, and password validity period that construct a keychain configuration node are configured using different commands. A keychain configuration node requires at least one password along with encryption and decryption algorithms.

To reference a keychain configuration node, specify the required peer and the node name in the MPLS-LDP view. In this manner, an LDP session is encrypted. Different peers can reference the same keychain configuration node.

Keychain authentication involves a set of passwords. It uses a new password when the previous one expires. Keychain authentication is complex to configure and is therefore recommended only for networks requiring high security.

Prerequisites

You have performed the following operations:

- Enable MPLS LDP globally using the **mpls ldp (system view)** command.
- Configure keychain authentication globally using the **keychain** command.

Precautions

- If a neighbor has been configured to be authenticated using MD5 algorithm by running the **md5-password** command, you cannot configure keychain authentication for the neighbor again.
- Configuring LDP keychain authentication causes the reestablishment of LDP sessions.

Example

Configure LDP keychain authentication for the peer with an LSR ID of **2.2.2.2**. The referenced keychain name is **kc1**.

```
<Huawei> system-view
[Huawei] keychain kc1 mode absolute
[Huawei-keychain-kc1] quit
[Huawei] mpls ldp
[Huawei-mpls-ldp] authentication key-chain peer 2.2.2.2 name kc1
```

Related Topics

11.1.82 mpls ldp (system view)
11.1.72 md5-password

11.1.4 authentication key-chain all

Function

The **authentication key-chain all** command enables keychain authentication in a batch for all LDP peers.

The **undo authentication key-chain all** command disables keychain authentication in a batch for all LDP peers.

By default, keychain authentication in a batch is disabled for all LDP peers. LDP keychain authentication is recommended to ensure security.

Format

authentication key-chain all name *keychain-name*

undo authentication key-chain all

Parameters

Parameter	Description	Value
name *keychain-name*	Specifies a keychain name. The keychain name is configured using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. The string does not contain question marks or spaces. The string can contain spaces if it is enclosed with double quotation marks ('').

Views

MPLS-LDP view

Default Level

2: Configuration level

Task Name and Operations

Task Name	Operations
mpls-ldp	write

Usage Guidelines

Usage Scenario

To help improve LDP session security, keychain authentication can be configured for a TCP connection over which an LDP session has been established. If a great number of LDP peers are configured, run the **authentication key-chain all** command to enable keychain authentication in a batch for all LDP peers.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A keychain has been configured using the **keychain** command.

Configuration Impact

After the **authentication key-chain all** command is run, the referenced keychain is applied to all LDP peers. If keychain authentication fails, an LDP session fails to be established.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1. Keychain authentication takes effect on other peers.
- Configuring LDP keychain authentication causes the reestablishment of LDP sessions.

Example

Configure LDP keychain authentication for all LDP peers and use the keychain named **kc1**.

```
<Huawei> system-view
[Huawei] keychain kc1 mode absolute
[Huawei-keychain-kc1] key-id 1
[Huawei-keychain-kc1-keyid-1] algorithm md5
[Huawei-keychain-kc1-keyid-1] key-string abcDEF-13579
[Huawei-keychain-kc1-keyid-1] send-time utc 14:30 2008-10-10 to 14:50 2008-10-10
[Huawei-keychain-kc1-keyid-1] receive-time utc 14:40 2008-10-10 to 14:50 2008-10-10
[Huawei-keychain-kc1-keyid-1] default send-key-id
[Huawei-keychain-kc1-keyid-1] quit
[Huawei-keychain-kc1] quit
[Huawei] mpls ldp
[Huawei-mpls-ldp] authentication key-chain all name kc1
```

11.1.5 authentication key-chain peer-group

Function

The **authentication key-chain peer-group** command enables keychain authentication in a batch for a specified LDP peer group.

The **undo authentication key-chain peer-group** command disables keychain authentication in a batch for a specified LDP peer group.

By default, keychain authentication in a batch is disabled for all peer groups. LDP keychain authentication is recommended to ensure security.

Format

authentication key-chain peer-group *ip-prefix-name* **name** *keychain-name*

undo authentication key-chain peer-group

Parameters

Parameter	Description	Value
ip-prefix-name	Specifies the name of an IP prefix list. The IP prefix list name is configured using the **ip ip-prefix** command.	The value is a string of 1 to 169 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks ('').
name *keychain-name*	Specifies a keychain name. The keychain name is configured using the **keychain** command.	The value is a string of 1 to 47 case-insensitive characters. The string does not contain question marks or spaces. The string can contain spaces if it is enclosed with double quotation marks ('').

Views

MPLS-LDP view

Default Level

2: Configuration level

Task Name and Operations

Task Name	Operations
mpls-ldp	write

Usage Guidelines

Usage Scenario

To help improve LDP session security, keychain authentication can be configured for a TCP connection over which an LDP session has been established. If a great number of LDP peers are configured, run the **authentication key-chain peer-group** command to enable keychain authentication in a batch for LDP peers in a specified peer group. An IP prefix list can be specified to define the range of IP addresses in a group.

Prerequisites

The following steps have been performed:

- An IP prefix list has been configured using the **ip ip-prefix** command.
- A keychain has been configured using the **keychain** command.

Configuration Impact

After the **authentication key-chain peer-group** command is run, the referenced Keychain authentication is applied to a specified peer. If keychain authentication fails, an LDP session fails to be established.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.
- Configuring LDP keychain authentication causes the reestablishment of LDP sessions.

Example

Enable LDP keychain authentication for LDP peers with IP addresses matching the IP prefix list named **list1** in a specified peer group and use a keychain named **kc1**.

```
<Huawei> system-view
[Huawei] keychain kc1 mode absolute
[Huawei-keychain-kc1] key-id 1
[Huawei-keychain-kc1-keyid-1] algorithm md5
[Huawei-keychain-kc1-keyid-1] key-string abcDEF-13579
[Huawei-keychain-kc1-keyid-1] send-time utc 14:30 2008-10-10 to 14:50 2008-10-10
[Huawei-keychain-kc1-keyid-1] receive-time utc 14:40 2008-10-10 to 14:50 2008-10-10
[Huawei-keychain-kc1-keyid-1] default send-key-id
[Huawei-keychain-kc1-keyid-1] quit
[Huawei-keychain-kc1] quit
[Huawei] ip ip-prefix list1 permit 4.4.4.4 32
[Huawei] mpls ldp
[Huawei-mpls-ldp] authentication key-chain peer-group list1 name kc1
```

11.1.6 auto-frr lsp-trigger

Function

The **auto-frr lsp-trigger** command configures a policy for triggering LDP to establish backup LSPs based on backup routes.

The **undo auto-frr lsp-trigger** command restores the default setting.

By default, LDP uses backup routes with 32-bit addresses to establish backup LSPs.

Format

auto-frr lsp-trigger { **all** | **host** | **ip-prefix** *ip-prefix-name* | **none** }

undo auto-frr lsp-trigger

Parameters

Parameter	Description	Value
all	Specifies all backup routes to trigger LDP to establish backup LSPs.	-
host	Specifies backup routes with 32-bit addresses to trigger LDP to establish backup LSPs.	-
ip-prefix *ip-prefix-name*	Specifies IP prefix list to trigger LDP to establish backup LSPs.	The value is an existing IP prefix list name.
none	Specifies no backup routes to trigger LDP to establish backup LSPs.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network with the active/standby link, run the **auto-frr lsp-trigger** command to quickly switch traffic to the backup LDP LSP within 50 ms upon a fault on the active link.

Auto LDP FRR depends on the automatic reroute function of IGP. Auto LDP FRR is automatically enabled after IGP automatic reroute is enabled using the **frr (IS-IS)** or **frr (OSPF)** command. To change the policy for triggering LDP to establish backup LSPs, run the **auto-frr lsp-trigger** command.

NOTE

During LDP GR, changing the policy for triggering the setup of backup LSPs is not allowed.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command in the system view.

Precautions

If both the **auto-frr lsp-trigger** command and the **lsp-trigger** command are run, the established backup LSPs are controlled by both the policy for triggering LDP LSP establishment and the policy for triggering backup LDP LSP establishment. For example, if the policy for triggering LDP LSP establishment is **none** and that for triggering backup LDP LSP establishment is **all**, the backup LDP LSP is established using the **none** policy.

 Copyright © Huawei Technologies Co., Ltd.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all backup routes trigger backup LDP LSP establishment.

Example

#Configure the policy for specifying no backup routes to trigger LDP to establish backup LSPs.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] auto-frr lsp-trigger none
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.67 lsp-trigger

11.1.7 backoff timer

Function

The **backoff timer** command sets the initial and maximum values for an Exponential backoff timer.

The **undo backoff timer** command restores the default settings.

By default, the initial value is 15 and the maximum value is 120, in seconds.

Format

backoff timer *init max*

undo backoff timer

Parameters

Parameter	Description	Value
init	Specifies the initial value of an Exponential backoff timer.	The value is an integer ranging from 5 to 2147483, in seconds.
max	Specifies the maximum value of an Exponential backoff timer.	The value is an integer ranging from 5 to 2147483, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After an LSR fails to process an LDP Initialization message or is informed that the peer LSR rejects the received LDP Initialization message, the LSR starts the Exponential backoff timer and periodically resends an LDP Initialization message to initiate an LDP session before the Exponential backoff timer expires.

When the Exponential backoff timer starts, the active role waits a period of time equal to the initial value of the Exponential backoff timer to attempt to set up an LDP session for the first time. Subsequently, the active role waits a period of time twice as long as the previous one to attempt to set up an LDP session. When the waiting period reaches the maximum value of the Exponential backoff timer, the active role waits a period of time equal to the maximum value of the Exponential backoff timer to attempt to set up an LDP session.

Run the **backoff timer** command to change the interval at which the active role attempts to set up a session.

By setting the initial value and maximum value for the Exponential backoff timer, you can flexibly control the reestablishment of sessions in different network environments.

- When a device is being upgraded, increase the initial and maximum values to set a large interval at which the active role attempts to set up a session.
- When a device that is transmitting services is prone to intermittent disconnections, reduce the initial and maximum values to set a small interval at which the active role attempts to set up a session.

NOTE

The initial value for the Exponential backoff timer cannot be smaller than 15, and the maximum value cannot be smaller than 120.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

If a session is disconnected after the **backoff timer** command is run, the device attempts to set up a session based on the set initial and maximum values of the Exponential backoff timer.

Example

Set the initial value to 20s and the maximum value to 160s for the Exponential backoff timer.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] backoff timer 20 160
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.8 bfd bind ldp-lsp

Function

The **bfd bind ldp-lsp** command creates a bidirectional forwarding detection (BFD) session for detecting LDP LSPs.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is created for detecting LDP LSPs.

Format

bfd *cfg-name* **bind ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* [**interface** *interface-type interface-number*]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	The value is in dotted decimal notation.
nexthop *ip-address*	Specifies the next hop IP address of the detected LSP.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Specifies the outbound interface that is bound to a BFD session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

A dynamic LSP is established using LDP on an MPLS network. It takes an interface a long period of time to detect a link fault. After a static BFD session is bound to the LDP LSP, the interface can quickly detect faults on LDP LSPs. This method applies to small networks.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

- When the IP address of the outbound interface of the detected LSP is lent or borrowed, an outbound interface must be specified.
- When the LDP LSP is deleted but the LDP session exists, the BFD session is in Down state, but the configuration of the BFD session bound to the LDP session is not deleted.

Example

Create a BFD session to detect the LDP LSP with the egress IP address being 4.4.4.4, the next hop IP address being 1.1.1.1, and the outbound interface being GE1/0/0.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd 1to4 bind ldp-lsp peer-ip 4.4.4.4 nexthop 1.1.1.1 interface gigabitethernet 1/0/0
[Huawei-bfd-lsp-session-1to4]
```

Related Topics

18.5.2 bfd
18.5.19 display bfd configuration

11.1.9 bfd bind static-lsp

Function

The **bfd bind static-lsp** command creates a BFD session to detect static LSPs.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is created to detect static LSPs.

Format

bfd *cfg-name* **bind static-lsp** *lsp-name*

undo bfd *cfg-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cfg-name	Specifies the BFD configuration name.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
lsp-name	Specifies the name of the static LSP bound to the BFD session.	The value is an existing static LSP name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can deploy MPLS services by manually configuring static LSPs on small networks with simple topology and stable performance. It takes an interface a long period of time to detect a link fault. After a static BFD session is bound to the LDP LSP, the interface can quickly detect faults on LDP LSPs.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

- If the specified static LSP does not exist or the BFD configuration name exists, the BFD session cannot be created.
- The **commit** command must be run to make the configured BFD parameters take effect before a BFD session is created.
- When the status of the static LSP is Down, a BFD session cannot be created.

Example

Create a BFD session to detect the static LSP named **1to4**.

```
<Huawei> system-view
[Huawei] bfd bfd1to4 bind static-lsp 1to4
[Huawei-bfd-lsp-session-bfd1to4]
```

Related Topics

18.5.2 bfd

11.1.120 static-lsp ingress

11.1.119 static-lsp egress
18.5.19 display bfd configuration

11.1.10 capability-announcement

Function

The **capability-announcement** command enables the LDP dynamic capability announcement function.

The **undo capability-announcement** command disables the LDP dynamic capability announcement function.

By default, the LDP dynamic capability announcement function is disabled.

Format

capability-announcement

undo capability-announcement

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a certain LDP feature is enabled after an LDP session has been created, the LDP session and the LSP associated with the session will be interrupted and re-negotiated.

The **capability-announcement** command can be run to dynamically enable or disable an LDP feature that supports the LDP dynamic capability announcement function without interrupting an LDP session. This feature ensures the stability of the LSP associated with the LDP session.

NOTE

It is recommended that you enable the dynamic LDP advertisement capability announcement function immediately after LDP is enabled globally. This function does not affect other existing LDP functions.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- If you enable the dynamic LDP advertisement capability announcement function after an LDP session is established, the LDP session is reestablished.
- This command is valid only for LDP supporting the dynamic LDP advertisement capability announcement function.

Example

Enable the LDP dynamic capability announcement function.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] capability-announcement
Warning: All the related sessions will be deleted if the operation is performed
!Continue? (y/n)y
```

Related Topics

11.1.82 mpls ldp (system view)
11.1.111 reset mpls ldp

11.1.11 diffserv-mode

Function

The **diffserv-mode** command configures a DiffServ mode for MPLS L3VPN labels to implement end-to-end QoS.

The **undo diffserv-mode** command restores the default DiffServ mode of an MPLS network.

By default, the uniform mode is used for MPLS L3VPN labels.

Format

diffserv-mode { **pipe mpls-exp** *mpls-exp* | **short-pipe mpls-exp** *mpls-exp* | **uniform** }

undo diffserv-mode

Parameters

Parameter	Description	Value
pipe	Indicates that the DiffServ mode of an MPLS network is pipe.	-
short-pipe	Indicates that the DiffServ mode of an MPLS network is short pipe.	-
uniform	Indicates that the DiffServ mode of an MPLS network is uniform.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mpls-exp *mpls-exp*	Specifies the EXP priority in the private label, which is mapped to the outer EXP priority in the public network LSP or outer DSCP priority in the public GRE tunnel. This parameter is valid only when the DiffServ mode on the ingress PE is set to pipe or short pipe. It is invalid on the egress PE. When the *mpls-exp* parameter is set to a large value, the packets have high priority and packet forwarding quality is high.	The value is an integer that ranges from 0 to 7.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To differentiate priorities of different services on an MPLS VPN, run this command to set the DiffServ mode to uniform. If priorities of services in a VPN do not need to be differentiated and priorities of services in different VPNs need to be differentiated, run this command to set the DiffServ mode to pipe or short pipe and specify the priority in the private label. Then map the EXP priority in the public LSP or DSCP priority in the public GRE tunnel.

NOTE

L3VPN supports LSPs, GRE tunnels, and MPLS TE tunnels.

Precautions

On the ingress, all the three modes can be set. On the egress, only the short pipe mode can be set.

The **diffserv-mode** command takes effect only for the new LSPs and private network routings. To make the command take effect for the existing LSPs and private network routings, run the **reset mpls ldp** and **reset bgp vpn-instance** *vpn-instance-name* **ipv4-family all** command to reestablish LSPs.

Example

In VPN instance **vrf1**, set the MPLS DiffServ mode to pipe and the value of *mpls-exp* to 3.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] diffserv-mode pipe mpls-exp 3
```

Related Topics

11.1.111 reset mpls ldp

11.1.12 display default-parameter mpls ldp

Function

The **display default-parameter mpls ldp** command displays the default configurations of MPLS LDP.

Format

display default-parameter mpls ldp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS LDP, run the **display default-parameter mpls ldp** command.

Example

Display the default configurations of MPLS LDP.

```
<Huawei> display default-parameter mpls ldp

 LDP Default Values:
 ----------------------------------------------------------
        Protocol version              : V1
        Graceful restart              : Off
          Neighbor liveness(sec)      : 600
          FT reconnect timer(sec)     : 300
          Recovery timer(sec)         : 300
        MTU signaling                 : On
        Label retention mode          : Liberal
        Label distribution mode       : Ordered
        Label advertisement           : DU
        Local hello-hold timer(sec)   : 15
        Remote hello-hold timer(sec)  : 45
        Keepalive-hold timer(sec)     : 45
        Backoff timer init(sec)       : 15
        Backoff timer max(sec)        : 120
        IGP-Sync delay timer(sec)     : 10
        Graceful delete               : Off
          Graceful delete timer(sec)  : 5
        Capability-announcement       : Off
        mLDP MBB Capability           : Off
```

```
    Wait-ack timer(sec)          : 10
    Switch-delay timer(ms)       : 100
  mLDP P2MP Capability           : Off
  mLDP MP2MP Capability          : Off
  Label withdraw-delay           : Off
    Withdraw-delay timer(sec)    : 5
  Send LSP down reason           : Off
  Ingress LSP Load-balance Num   : 64
  Transit LSP Load-balance Num   : 64
  Smart-policy Ingress           : Off
  Smart-policy Auto-dod-request : Off
        Label default-route      : Off
-------------------------------------------------------------
```

Table 11-1 Description of the **display default-parameter mpls ldp** command output

Item	Description
Protocol version	LDP version number.
Graceful restart	LDP GR capability status. ● On: LDP GR is enabled. ● Off: LDP GR is disabled. By default, LDP GR is disabled. You can configure the LDP GR capability status using the **graceful-restart** command.
Neighbor liveness(sec)	Value of the neighbor-liveness timer, in seconds. The default value is 600s. You can set this value using the **graceful-restart timer neighbor-liveness** command.
FT reconnect timer(sec)	Value of the reconnect timer of an LDP session, in seconds. The default value is 300s. You can set this value using the **graceful-restart timer reconnect** command.
Recovery timer(sec)	Value of the recovery timer of an LDP LSP, in seconds. The default value is 300s. You can set this value using the **graceful-restart timer recovery** command.
MTU signaling	MTU TLV status. ● On: MTU TLV is enabled. ● Off: MTU TLV is disabled. By default, MTU TLV is enabled.
Label retention mode	LDP label retention modes include: ● Liberal: free mode ● Conservative: conservative mode. The default label retention mode is liberal.
Label distribution mode	LDP label distribution mode. Currently, only the ordered mode is supported.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Label advertisement	LDP label advertisement modes include: ● DU: downstream unsolicited mode. ● DOD: downstream on demand mode. The default label advertisement mode is DU. You can set the LDP label advertisement mode using the **mpls ldp advertisement** command.
Local hello-hold timer(sec)	Value of the local Hello hold timer, in seconds. The default value is 15s. You can set this value using the **mpls ldp timer hello-hold** command.
Remote hello-hold timer(sec)	Value of the remote Hello hold timer, in seconds. The default value is 45s. You can set this value using the **mpls ldp timer hello-hold** command.
Keepalive-hold timer(sec)	Value of the keepalive hold timer for the local and remote LDP sessions, in seconds. The default value is 45s. You can set this value using the **mpls ldp timer keepalive-hold** command.
Backoff timer init(sec)	Initial value of the Exponential backoff timer, in seconds. The default value is 15s. You can set this value using the **backoff timer** command.
Backoff timer max(sec)	Maximum value of the Exponential backoff timer, in seconds. The default value is 120s. You can set this value using the **backoff timer** command.
IGP-Sync delay timer(sec)	Value of the LDP-IGP association timer, in seconds. The default value is 10s. You can set this value using the **mpls ldp timer igp-sync-delay** command.
Graceful delete	Graceful deletion. This function is disabled and not supported currently.
Graceful delete timer(sec)	Value of the graceful deletion timer, in seconds. The default value is 5s.
Capability-announcement	Dynamic capability announcement status can be: ● On: The dynamic capability announcement function is enabled. ● Off: The dynamic capability announcement function is disabled. By default, dynamic capability announcement is disabled.
mLDP MBB Capability	Whether the mLDP make-before-break capability is enabled. The default value is "Off", indicating that mLDP make-before-break is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wait-ack timer(sec)	Whether the multipoint extensions for LDP (mLDP) make-before-break capability is enabled. The default value is "Off", indicating that mLDP make-before-break is disabled.
Switch-delay timer(ms)	The default value of the time for waiting for an MBB ACK Notification message.
mLDP P2MP Capability	Whether mLDP P2MP is enabled global. The default value is "Off", indicating that LDP P2MP is disabled globally.
mLDP MP2MP Capability	Whether mLDP multipoint-to-multipoint (MP2MP) is enabled global. The default value is "Off", indicating that mLDP MP2MP is disabled globally.
Label withdraw-delay	Whether the label withdraw delay function is enabled. The default value is "Off", indicating that this function is disabled.
Withdraw-delay timer(sec)	Default value of the label withdraw delay timer (in seconds).
Send LSP down reason	Whether a node is enabled to report the fault location and cause to the ingress. The default value is "Off", indicating that the faulty node is disabled from reporting the fault cause to the ingress.
Ingress LSP Load-balance Num	Default maximum number of equal-cost LDP LSPs that can be established on the ingress.
Transit LSP Load-balance Num	Default maximum number of equal-cost LDP LSPs that can be established on a transit node.
Smart-policy Ingress	Smart LDP ingress policy
Smart-policy Auto-dod-request	Smart LDP request policy

Related Topics

11.1.7 backoff timer
11.1.50 graceful-restart (MPLS-LDP view)
11.1.51 graceful-restart timer neighbor-liveness
11.1.52 graceful-restart timer reconnect
11.1.53 graceful-restart timer recovery
11.1.81 mpls ldp advertisement
11.1.86 mpls ldp timer hello-hold
11.1.88 mpls ldp timer igp-sync-delay
11.1.89 mpls ldp timer keepalive-hold

 Copyright © Huawei Technologies Co., Ltd.

11.1.13 display default-parameter mpls management

Function

The **display default-parameter mpls management** command displays default configurations of the MPLS management module.

Format

display default-parameter mpls management

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the default configurations of MPLS management module, run the **display default-parameter mpls management** command.

Example

Display the default configurations of the MPLS management module.

```
<Huawei> display default-parameter mpls management

 Global Information:
 ------------------------------------------------------------
        BFD detect-multiplier        : 3
        BFD min-tx-interval(ms)      : 1000
        BFD min-rx-interval(ms)      : 1000
        Label advertisement mode     : Implicit null
        LSP trigger mode             : Host
        LDP LSP number threshold-alarm upper limit  : 80
        LDP LSP number threshold-alarm lower limit  : 75
        BGP LSP number threshold-alarm upper limit  : 80
        BGP LSP number threshold-alarm lower limit  : 75
        BGP V6 LSP number threshold-alarm upper limit  : 80
        BGP V6 LSP number threshold-alarm lower limit  : 75
        Dynamic Label number threshold-alarm upper limit  : 80
        Dynamic Label number threshold-alarm lower limit  : 70
        RSVP LSP number threshold-alarm upper limit  : 80
        RSVP LSP number threshold-alarm lower limit  : 75
        Total LSP number threshold-alarm upper limit  : 80
        Total LSP number threshold-alarm lower limit  : 75
        Total CR LSP number threshold-alarm upper limit  : 80
        Total CR LSP number threshold-alarm lower limit  : 75
        Ingress LDP LSP number threshold-alarm upper limit  : 80
        Ingress LDP LSP number threshold-alarm lower limit  : 75
        Transit LDP LSP number threshold-alarm upper limit  : 80
        Transit LDP LSP number threshold-alarm lower limit  : 75
```

 Copyright © Huawei Technologies Co., Ltd.

```
    Egress LDP LSP number threshold-alarm upper limit  : 80
    Egress LDP LSP number threshold-alarm lower limit  : 75
    Ingress BGP LSP number threshold-alarm upper limit  : 80
    Ingress BGP LSP number threshold-alarm lower limit  : 75
    Egress BGP LSP number threshold-alarm upper limit  : 80
    Egress BGP LSP number threshold-alarm lower limit  : 75
    Egress BGP V6 LSP number threshold-alarm upper limit  : 80
    Egress BGP V6 LSP number threshold-alarm lower limit  : 75
    Ingress RSVP LSP number threshold-alarm upper limit  : 80
    Ingress RSVP LSP number threshold-alarm lower limit  : 75
    Transit RSVP LSP number threshold-alarm upper limit  : 80
    Transit RSVP LSP number threshold-alarm lower limit  : 75
    Egress RSVP LSP number threshold-alarm upper limit  : 80
    Egress RSVP LSP number threshold-alarm lower limit  : 75
    Total ingress LSP number threshold-alarm upper limit  : 80
    Total ingress LSP number threshold-alarm lower limit  : 75
    Total transit LSP number threshold-alarm upper limit  : 80
    Total transit LSP number threshold-alarm lower limit  : 75
    Total egress LSP number threshold-alarm upper limit  : 80
    Total egress LSP number threshold-alarm lower limit  : 75
    Total ingress CR LSP number threshold-alarm upper limit  : 80
    Total ingress CR LSP number threshold-alarm lower limit  : 75
    Total transit CR LSP number threshold-alarm upper limit  : 80
    Total transit CR LSP number threshold-alarm lower limit  : 75
    Total egress CR LSP number threshold-alarm upper limit  : 80
    Total egress CR LSP number threshold-alarm lower limit  : 75
    Auto bypass tunnel interface number threshold-alarm upper limit  : 80
    Auto bypass tunnel interface number threshold-alarm lower limit  : 75
    P2MP auto tunnel interface number threshold-alarm upper limit  : 80
    P2MP auto tunnel interface number threshold-alarm lower limit  : 75
    TE dynamic bfd number threshold-alarm upper limit  : 80
    TE dynamic bfd number threshold-alarm lower limit  : 75
    LDP dynamic bfd number threshold-alarm upper limit  : 80
    LDP dynamic bfd number threshold-alarm lower limit  : 75
    Total MLDP tree number threshold-alarm upper limit  : 80
    Total MLDP tree number threshold-alarm lower limit  : 75
    Total MLDP branch number threshold-alarm upper limit  : 80
    Total MLDP branch number threshold-alarm lower limit  : 75
    Total LDP remote adjacency number threshold-alarm upper limit  : 80
    Total LDP remote adjacency number threshold-alarm lower limit  : 75
        Total LDP local adjacency number threshold-alarm upper limit  : 80
    Total LDP local adjacency number threshold-alarm lower limit  : 75
    Total CSPF node number threshold-alarm upper limit  : 80
    Total CSPF node number threshold-alarm lower limit  : 75
    Total CSPF link number threshold-alarm upper limit  : 80
    Total CSPF link number threshold-alarm lower limit  : 75
    Total CSPF network-lsa number threshold-alarm upper limit  : 80
    Total CSPF network-lsa number threshold-alarm lower limit  : 75
    Total CSPF SRLG number threshold-alarm upper limit  : 80
    Total CSPF SRLG number threshold-alarm lower limit  : 75
    RSVP peer number threshold-alarm upper limit  : 80
    RSVP peer number threshold-alarm lower limit  : 75
-------------------------------------------------------------
```

Table 11-2 Description of the display default-parameter mpls management command output

Item	Description
BFD detect-multiplier	BFD detection multiplier. The default value is 3. You can set this value using the **mpls bfd** command.

Item	Description
BFD min-tx-interval(ms)	Interval for sending BFD packets. You can set this value using the **mpls bfd** command. By default, the interval for sending BFD packets is 1000 ms.
BFD min-rx-interval(ms)	Interval for receiving BFD packets. You can set this value using the **mpls bfd** command. By default, the interval for receiving BFD packets is 1000 ms.
Label advertisement mode	Mode in which the egress node assigns labels to the penultimate hop. ● Implicit null: The egress node assigns an implicit empty label to the penultimate hop. The value of the label is 3. ● Explicit null: The egress node assigns an explicit empty label to the penultimate hop. The value of the label is 0. ● Non null: The egress node assigns a label to the penultimate hop properly. The value of the label is not smaller than 16. By default, the implicit null mode is used. You can set the label advertisement mode using the **label advertise** command.
LSP trigger mode	Policy for triggering LSP setup. ● All: All static routes and IGP routing entries trigger the setup of LSPs. ● Host: The IP route of the 32-bit address host triggers the setup of LSPs. ● Ip-prefix: Only FECs that match entries in the IP address prefix list trigger the setup of LSPs. ● None: The setup of LSPs is not triggered. The default trigger policy is **Host**. You can set the LSP trigger mode using the **lsp-trigger** command.
LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for LDP LSPs.
LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for LDP LSPs.
BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for BGP LSPs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for BGP LSPs.
BGP V6 LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for BGP IPv6 LSPs.
BGP V6 LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for BGP IPv6 LSPs.
Dynamic Label number threshold-alarm upper limit	Upper limit of the alarm threshold for dynamic label usage. You can set the LSP trigger mode using the **mpls dynamic-label-number threshold-alarm** command.
Dynamic Label number threshold-alarm lower limit	Lower limit of the alarm threshold for dynamic label usage. You can set the LSP trigger mode using the **mpls dynamic-label-number threshold-alarm** command.
RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for RSVP LSPs.
RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for RSVP LSPs.
Total LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total LSPs.
Total LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total LSPs.
Total CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total CR-LSPs.
Total CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total CR-LSPs.
Ingress LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress LDP LSP.
Ingress LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress LDP LSP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Transit LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for transit LDP LSP.
Transit LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for transit LDP LSP.
Egress LDP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress LDP LSP.
Egress LDP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress LDP LSP.
Ingress BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress BGP LSP.
Ingress BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress BGP LSP.
Egress BGP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress BGP LSP.
Egress BGP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress BGP LSP.
Egress BGP V6 LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress BGP V6 LSP.
Egress BGP V6 LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress BGP V6 LSP.
Ingress RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for ingress RSVP LSP.
Ingress RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for ingress RSVP LSP.
Transit RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for transit RSVP LSP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Transit RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for transit RSVP LSP.
Egress RSVP LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for egress RSVP LSP.
Egress RSVP LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for egress RSVP LSP.
Total ingress LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total ingress LSP.
Total ingress LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total ingress LSP.
Total transit LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total transit LSP.
Total transit LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total transit LSP.
Total egress LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total egress LSP.
Total egress LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total egress LSP.
Total ingress CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total ingress CR-LSP.
Total ingress CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total ingress CR-LSP.
Total transit CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total transit CR-LSP.
Total transit CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total transit CR-LSP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total egress CR LSP number threshold-alarm upper limit	Upper limit of the alarm threshold for total egress CR-LSP.
Total egress CR LSP number threshold-alarm lower limit	Lower limit of the alarm threshold for total egress CR-LSP.
Auto bypass tunnel interface number threshold-alarm upper limit	Upper limit of the alarm threshold for auto bypass tunnel interface.
Auto bypass tunnel interface number threshold-alarm lower limit	Lower limit of the alarm threshold for auto bypass tunnel interface.
P2MP auto tunnel interface number threshold-alarm upper limit	Upper limit of the alarm threshold for P2MP auto tunnel interface.
P2MP auto tunnel interface number threshold-alarm lower limit	Lower limit of the alarm threshold for P2MP auto tunnel interface.
TE dynamic bfd number threshold-alarm upper limit	Upper limit of the alarm threshold for TE dynamic bfd.
TE dynamic bfd number threshold-alarm lower limit	Lower limit of the alarm threshold for TE dynamic bfd.
LDP dynamic bfd number threshold-alarm upper limit	Upper limit of the alarm threshold for LDP dynamic bfd.
LDP dynamic bfd number threshold-alarm lower limit	Lower limit of the alarm threshold for LDP dynamic bfd.
Total MLDP tree number threshold-alarm upper limit	Upper limit of the alarm threshold for total MLDP tree.
Total MLDP tree number threshold-alarm lower limit	Lower limit of the alarm threshold for total MLDP tree.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total MLDP branch number threshold-alarm upper limit	Upper limit of the alarm threshold for total MLDP branch.
Total MLDP branch number threshold-alarm lower limit	Lower limit of the alarm threshold for total MLDP branch.
Total LDP remote adjacency number threshold-alarm upper limit	Upper limit of the alarm threshold for total LDP remote adjacency.
Total LDP remote adjacency number threshold-alarm lower limit	Lower limit of the alarm threshold for total LDP remote adjacency.
Total LDP local adjacency number threshold-alarm upper limit	Upper limit of the alarm threshold for total LDP local adjacency.
Total LDP local adjacency number threshold-alarm lower limit	Lower limit of the alarm threshold for total LDP local adjacency.
Total CSPF node number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF node.
Total CSPF node number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF node.
Total CSPF link number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF link.
Total CSPF link number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF link.
Total CSPF network-lsa number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF network-lsa.
Total CSPF network-lsa number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF network-lsa.
Total CSPF SRLG number threshold-alarm upper limit	Upper limit of the alarm threshold for total CSPF SRLG.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total CSPF SRLG number threshold-alarm lower limit	Lower limit of the alarm threshold for total CSPF SRLG
RSVP peer number threshold-alarm upper limit	Upper limit of the alarm threshold for RSVP peer.
RSVP peer number threshold-alarm lower limit	Lower limit of the alarm threshold for RSVP peer.

Related Topics

11.1.78 mpls bfd
11.1.60 label advertise
11.1.67 lsp-trigger

11.1.14 display isis ldp-sync interface

Function

The **display isis ldp-sync interface** command displays information about LDP and IS-IS synchronization on an interface.

Format

display isis [*process-id* | **vpn-instance** *vpn-instance-name*] **ldp-sync interface**

Parameters

Parameter	Description	Value
process-id	Specifies the IS-IS process ID.	The value is an integer ranging from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the VPN instance name.	The value is an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

For all the interfaces that are enabled with LDP and IS-IS synchronization, run the **display isis ldp-sync** command to view information about LDP and IS-IS synchronization.

Example

Display information about LDP and IS-IS synchronization on an interface.

```
<Huawei> display isis ldp-sync interface

                 Ldp Sync interface information for ISIS(1)
                 -----------------------------------------
Interface    HoldDownTimer    HoldMaxCostTimer   LDP State   Sync State
GE1/0/0      10               10                 Down        Init
```

Table 11-3 Description of the display isis ldp-sync interface command output

Item	Description
Interface	Interface connected to neighbors.
HoldDownTimer	Interval during which the interface waits for the LDP session establishment and does not create the IS-IS neighbor relationship. The default value is 10 seconds. You can set this value using the **isis timer ldp-sync hold-down** command.
HoldMaxCostTimer	Interval for IS-IS to notify the local device of the maximum metric in the link state PDU (LSP). The default value is 10 seconds. You can set this value using the **isis timer ldp-sync hold-max-cost** command. **NOTE** If the value of this field is **infinite**, IS-IS permanently notifies the local device of the maximum metric in the LSP before an LDP session is established.
LDP State	LDP session status, which can be: ● Up: The LDP session is normal. ● Down: The LDP session is disconnected. ● GR: The LDP session is in GR state. If the interface is maintaining the session before GR, the LDP status is displayed as GR state during GR.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Sync State	Status of synchronization between LDP and IS-IS: • Sync-Achieved: The creation of an LDP session and establishment of the IS-IS neighbor relationship are synchronized. • HoldDown: indicates the state in which the interface waits to create an LDP session without creating the IS-IS neighbor relationship. • HoldMaxCost: indicates the state in which IS-IS advertises the maximum metric in LSPs sent by the local device. • Init: indicates the initial state.

Related Topics

11.1.58 isis timer ldp-sync hold-down
11.1.59 isis timer ldp-sync hold-max-cost

11.1.15 display lspv configuration

Function

The **display lspv configuration** command displays the current configuration of LSPV.

Format

display lspv configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display lspv configuration** command to check the current LSPV configurations.

Example

Display the current configuration of LSPV.

```
<Huawei> display lspv configuration
lspv packet filter 2100
undo lspv mpls-lsp-ping echo enable
```

Table 11-4 Description of the **display lspv configuration** command output

Item	Description
lspv packet filter 2100	Filters the LSPV packet with the specific source address according to ACL 2100.
undo lspv mpls-lsp-ping echo enable	Disables the response to MPLS Ping packets.

Related Topics

11.1.68 lspv mpls-lsp-ping echo enable

11.1.69 lspv packet-filter

11.1.16 display lspv statistics

Function

The **display lspv statistics** command displays LSPV statistics.

Format

display lspv statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In MPLS network management, the **ping lsp** or **tracert lsp** command can be used for LSP detection.

If the LSP detection fails, you can run the **display lspv statistics** command to view statistics about MPLS packets sent and received on the local device. If the number of MPLS packets that the local device sends is the same as the number of MPLS packets that the local device receives, but the ping or trace operation fails, the detection failure is caused by the fault of the local device, not the LSP.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display LSPV statistics on the device.

```
<Huawei> display lspv statistics
Total sent: 0 packet(s)
Total received: 0 packet(s)
MPLS echo request sent: 0 packet(s), received: 0 packet(s)
MPLS echo reply sent: 0 packet(s), received: 0 packet(s)
-----------------------------------------------------------------------
Statistcs base on ReturnCode:
0 - No return code,1 - Malformed echo request received,2 - One or more
of the TLVs was not understood,3 - Replying router is an egress for
the FEC at stack-depth, 4 - Replying router has no mapping for the FEC
at stack-depth,5 - Downstream Mapping Mismatch, 6 - Upstream Interface
Index Unknown, 7 - Reserved, 8 - Label switched at stack-depth,9 -
Label switched but no MPLS forwarding at stack-depth,10 - Mapping for
this FEC is not the given label at stack-depth,11 - No label entry at
stack-depth,12 - Protocol not associated with interface at FEC
stack-epth,13 - Premature termination of ping due to label stack
hrinking to a single label.:
-----------------------------------------------------------------------
Value     SendNum     RecvNum     Value     SendNum     RecvNum
   0         0           0         1         0           0
   2         0           0         3         0           0
   4         0           0         5         0           0
   6         0           0         7         0           0
   8         0           0         9         0           0
  10         0           0        11         0           0
  12         0           0        13         0           0
-----------------------------------------------------------------------
```

Table 11-5 Description of the **display lspv statistics** command output

Item	Description
Total sent	Total number of sent MPLS Echo Request and MPLS Echo Reply packets
Total received	Total number of received MPLS Echo Request and MPLS Echo Reply packets
MPLS echo request sent: x packet(s), received: x packet(s)	Number of sent MPLS Echo Request packets is x, Number of received MPLS Echo Request packets is x
MPLS echo reply sent: x packet(s), received: x packet(s)	Number of sent MPLS Echo Reply packets is x, Number of received MPLS Echo Reply packets is x

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Statistcs base on ReturnCode	Statistcs base on ReturnCode: ● 0: No return code ● 1: Malformed echo request received ● 2: One or more of the TLVs was not understood ● 3: Replying router is an egress for the FEC at stack-depth ● 4: Replying router has no mapping for the FEC at stack-depth ● 5: Downstream Mapping Mismatch ● 6: Upstream Interface Index Unknown ● 7: Reserved ● 8: Label switched at stack-depth ● 9: Label switched but no MPLS forwarding at stack-depth ● 10: Mapping for this FEC is not the given label at stack-depth ● 11: No label entry at stack-depth ● 12: Protocol not associated with interface at FEC stack-epth ● 13: Premature termination of ping due to label stack shrinking to a single label
Value	The value of ReturnCode in sent or received LSP verification packets.
SendNum	Number of sent packets with this ReturnCode.
RecvNum	Number of received packets with this ReturnCode.

11.1.17 display mpls bfd session

Function

The **display mpls bfd session** command displays information about BFD sessions, including the BFD session for LDP LSPs and the BFD session for TE CR-LSPs.

Format

display mpls bfd session [**fec** *fec-address* | **monitor** | **nexthop** *ip-address* | **outgoing-interface** *interface-type interface-number* | **statistics** | **verbose**]

display mpls bfd session protocol ldp [**fec** *fec-address* [**verbose**]]

display mpls bfd session protocol { **cr-static** | **rsvp-te** } [**lsp-id** *ingress-lsr-id session-id lsp-id* [**verbose**]]

Parameters

Parameter	Description	Value
fec *fec-address*	Displays information about the BFD session of a specified FEC.	The value is in dotted decimal notation.
monitor	Displays monitoring information of BFD sessions.	-
nexthop *ip-address*	Displays information about the BFD session of a specified next hop.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Displays information about the BFD session of the LSP with a specified outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
protocol	Indicates the type of the protocol.	-
cr-static	Displays information about the BFD session for static CR-LSP.	-
ldp	Displays information about the BFD session for LDP.	-
rsvp-te	Displays information about the BFD session for RSVP-TE.	-
statistics	Displays statistics about BFD sessions such as the total number of BFD sessions.	-
verbose	Displays detailed information about BFD sessions.	-
lsp-id *ingress-lsr-id*	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer ranging from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer ranging from 0 to 65535.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls bfd session** command to view information about a BFD session and the LSP detected by BFD, including the destination address and outbound interface of the LSP, the local discriminator of the BFD session, and the status of an MPLS BFD session.

Example

Display information about the BFD session.

```
<Huawei> display mpls bfd session
-----------------------------------------------------------------------
              BFD Information: LDP  LSP
-----------------------------------------------------------------------
FEC           DISC  OUT-IF      NEXTHOP        TUNNEL         STATE
3.3.3.3       8     GE1/0/0   10.1.1.2       Tunnel0/0/1        Up
-----------------------------------------------------------------------
```

Table 11-6 Description of the display mpls bfd session command output

Item	Description
FEC	Forwarding equivalence class.
DISC	Local discriminator of a BFD session.
OUT-IF	Outbound interface.
NEXTHOP	IP address of the next hop.
TUNNEL	Name of a tunnel.
STATE	Status of an MPLS BFD session. ● Up ● Down

Display detailed information about a BFD session with the specified protocol type and LSP ID.

```
<Huawei> display mpls bfd session protocol rsvp-te lsp-id 3.3.3.3 3 1 verbose
-----------------------------------------------------------------------
              BFD Information: TE TUNNEL
-----------------------------------------------------------------------
 No                      :  1
 LspIndex                :  6157
 Protocol                :  RSVP-TE
 Tunnel-Interface        :  Tunnel0/0/1
 Fec                     :  2.2.2.2
 Nexthop                 :  10.2.3.2

 Bfd-Discriminator       :  8195
 TEMIB Tunn Table Index  :  3
 SessionTunnelID         :  3
```

```
LocalLspId              :  1
PrevSessionTunnelID     :  -
NextSessionTunnelID     :  12
ActTx                   :  2200
ActRx                   :  2200
ActMulti                :  -
Bfd-State               :  Down
Time                    :  2559 sec
```

Table 11-7 Description of the display mpls bfd session protocol rsvp-te verbose command output

Item	Description
No	Serial number.
LspIndex	Index number of an LSP.
Protocol	Protocol type.
Tunnel-Interface	Name of a tunnel interface.
Fec	Forwarding equivalence class.
Nexthop	IP address of the next hop.
Bfd-Discriminator	Local discriminator of a BFD session.
TEMIB Tunn Table Index	Index of the tunnel entry to which an LSP corresponds.
SessionTunnelID	BFD session ID.
LocalLspId	ID of a local LSP.
PrevSessionTunnelID	Tunnel ID mapping the previous LSP to which a BFD session is bound.
NextSessionTunnelID	Tunnel ID mapping the next LSP to which a BFD session is bound.
ActTx	Actual interval for sending BFD packets, in milliseconds.
ActRx	Actual interval for receiving BFD packets, in milliseconds.
ActMulti	Actual local detection multiple of a BFD session.
Bfd-State	Status of the BFD session. ● Up ● Down
Time	Period from the time when the BFD session is created or updated till now, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

11.1.18 display mpls graceful-restart

Function

The **display mpls graceful-restart** command displays graceful restart (GR) information about all protocols related to MPLS.

Format

display mpls graceful-restart

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When MPLS is used together with other protocols, run the **display mpls graceful-restart** command to view GR information about protocols related to MPLS, including the GR status, GR start time, and GR type.

Example

Display GR information related to all protocols.

```
<Huawei> display mpls graceful-restart
Protocol       GR state       GR start time          GR type
LDP            Normal         -                      -
CRLDP          Normal         -                      -
RSVP           Normal         -                      -
BGP            Normal         -                      -
L3VPN          Normal         -                      -
STATIC         Normal         -                      -
CRSTATIC       Normal         -                      -
BGP IPV6       Normal         -                      -
STATIC HA      Normal         -                      -
L3VPN IPV6     Normal         -                      -
STATIC TP      Normal         -                      -
```

Table 11-8 Description of the display mpls graceful-restart command output

Item	Description
Protocol	Protocol type: LDP, CRLDP, RSVP, BGP, L3VPN, STATIC, CRSTATIC, BGP IPV6, STATIC HA, L3VPN IPV6, and STATIC TP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
GR state	GR status of a protocol: ● Restarting: The protocol is in the GR process. ● Normal: The protocol is not in the GR process.
GR start time	Time when the GR process starts When the GR process does not start, a hyphen (-) is displayed.
GR type	GR type: ● System restart: indicates the system GR. ● Protocol restart: indicates the protocol GR. When the GR process does not start, a hyphen (-) is displayed.

Related Topics

11.1.50 graceful-restart (MPLS-LDP view)

11.1.19 display mpls interface

Function

The **display mpls interface** command displays information about all MPLS-enabled interfaces.

Format

display mpls interface [*interface-type interface-number*] [**verbose**]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-
verbose	Displays detailed information about the interface enabled with MPLS.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After enabling MPLS functions, run the **display mpls interface** command to view information about the interface enabled with MPLS.

Example

Display information about all MPLS-enabled interfaces.

```
<Huawei> display mpls interface
Interface          Status   TE Attr   LSP Count  CRLSP Count Effective MTU
GE1/0/0             Up       Dis       2          0           1500
```

Table 11-9 Description of the display mpls interface command output

Item	Description
Interface	Type and number of the interface enabled with MPLS.
Status	Interface status: ● Up ● Down
TE Attr	Status of the TE attributes on an interface: ● Dis: MPLS TE is disabled on the interface. ● En: MPLS TE is enabled on the interface.
LSP Count	Number of LSPs established on an interface.
CRLSP Count	Number of CR-LSPs established on an interface.
Effective MTU	MPLS MTU used during data forwarding: ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.

Display detailed information about a specified MPLS-enabled interface.

```
<Huawei> display mpls interface gigabitethernet 1/0/0 verbose
No                  :  1
Interface           :  GE1/0/0
Status              :  Up
TE Attribute        :  Disable
Static LSPCount     :  0
Static CR-LSPCount  :  0
LDP LSPCount        :  0
RSVP LSPCount       :  0
MPLS MTU            :  -
Interface MTU       :  1500
Effective MTU       :  1500
TE FRR              :  Disable
Interface Index     :  0xd1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 11-10 Description of the display mpls interface verbose command output

Item	Description
No	Serial number.
Interface	Type and number of the interface enabled with MPLS.
Status	Interface status: ● Up ● Down
TE Attribute	Status of the TE attributes on the interface: ● Disable: MPLS TE is disabled on the interface. ● Enable: MPLS TE is enabled on the interface.
Static LSPCount	Number of static LSPs established on the interface.
Static CR-LSPCount	Number of static CR-LSPs established on the interface.
LDP LSPCount	Number of LDP LSPs created on the interface.
RSVP LSPCount	Number of RSVP-TE LSPs established on the interface.
MPLS MTU	MPLS MTU value configured using the **mpls mtu** command. When no MPLS MTU is set, a hyphen (-) is displayed.
Interface MTU	MTU value configured on an interface.
Effective MTU	MPLS MTU used during data forwarding: ● If no MPLS MTU is set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.
TE FRR	Whether the TE FRR is enabled or disabled on the interface: ● Disable: No bypass tunnel is set up in manual FRR mode to protect the interface. ● Enable: A bypass tunnel is set up in manual FRR mode to protect the interface.
Interface Index	Interface index value.

Related Topics

11.1.76 mpls (interface view)

11.1.20 display mpls label static available

Function

The **display mpls label static available** command displays information about labels available for transmitting static services.

Format

display mpls label static available [[**label-from** *label-index*] **label-number** *label-number*]

Parameters

Parameter	Description	Value
label-from *label-index*	Specifies the start label value.	The value is an integer ranging from 16 to 1023.
label-number *label-number*	Specifies the number of the required labels.	The value is an integer ranging from 1 to 1008.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

By default, the system reserves separate label spaces for dynamic and static services, allowing labels for dynamic and static services to be stored in separate spaces.

Before specifying a label for static services, ensure that the specified label is available. You can run the **display mpls label static available** command to view labels for static services.

In the command output, a dash is used to specify a range. For example, labels 1000, 1001, and 1002 are displayed as 1000-1002.

Follow-up Procedure

Labels displayed in the command output can be allocated for static services.

Example

Display information about labels available for transmitting static services.

```
<Huawei> display mpls label static available
16-1023
```

11.1.21 display mpls label-stack ilm inlabel

Function

The **display mpls label-stack ilm inlabel** command displays information about the label stack for packets with a specified incoming label.

Format

display mpls label-stack ilm inlabel *in-label*

Parameters

Parameter	Description	Value
in-label	Specifies the incoming label for the packets about which label-stack information is to be displayed.	The value is an integer ranging from 16 to 1048575.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to query information about the outgoing label stack for packets based on the incoming label. The supported public network tunnels include static LSP tunnels, LDP LSPs, dynamic TE tunnels, and static TE tunnels. This command cannot be used in the following situations:

- Tunnels overlap.
- Tunnels load-balance traffic.
- The primary and secondary SPE egresses are used.

Example

Display the outgoing label, outbound interface, and tunnel type in the packets with the incoming label value of 1028.

```
<Huawei> display mpls label-stack ilm inlabel 1028
Label-stack  : 1
Level        : 1
Type         : LDP
Label        : 1025
OutInterface : Vlanif111
```

Table 11-11 Description of the **display mpls label-stack ilm inlabel** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
OutInterface	Outbound interface

11.1.22 display mpls last-info lsp-down

Function

The **display mpls last-info lsp-down** command displays information about LSPs in Down state.

Format

display mpls last-info lsp-down [**protocol ldp**] [**verbose**]

Parameters

Parameter	Description	Value
protocol ldp	Displays information about LSPs in Down state.	-
verbose	Displays detailed information about LDP LSPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If LSPs fail and enter the Down state, run the **display mpls last-info lsp-down** command to view the faults that cause the latest 64 LSPs to go Down.

Example

Display brief information about LDP LSPs that just enter the Down state.

```
<Huawei> display mpls last-info lsp-down
-------------------------------------------------------------------------------
                 LDP LSP Information: Host Address
-------------------------------------------------------------------------------
FEC               In/Out Label  Out Interface       Down Reason
12.12.12.12/32    1029/3        Eth2/0/1            route changed
12.12.12.12/32    NULL/3        Eth2/0/1            route changed
11.11.11.11/32    1034/3        Eth2/0/0            cannot recovery from GR
11.11.11.11/32    NULL/3        Eth2/0/0            cannot recovery from GR
11.11.11.11/32    1033/3        Eth2/0/0            DS lost
11.11.11.11/32    NULL/3        Eth2/0/0            DS lost
```

Table 11-12 Description of the display mpls last-info lsp-down command output

Item	Description
FEC	Forwarding equivalence class.
In/Out Label	Values of the incoming and outgoing labels.
Out Interface	Outbound interface.
Down Reason	LSPs go Down due to the following causes: ● route changed: A route was changed. ● adjacency changed: An adjacency was changed. ● cannot recovery from GR: The LDP LSP failed to be reestablished during GR. ● recv release msg: A Release message was received. ● recv withdraw msg: A Withdraw message was received. ● US lost: The session with the upstream node went Down. ● DS lost: The session with the downstream node went Down. ● policy changed: The policy to establish LSPs was changed (Generally, configurations of the policy was changed). ● reach paf limit: PAF resources are insufficient. ● GR aging: The LSP aged after GR. ● others

Display detailed information about LDP LSPs that just enter the Down state.

```
<Huawei> display mpls last-info lsp-down protocol ldp verbose
-------------------------------------------------------------------------------
                 LDP LSP Information: Host Address
-------------------------------------------------------------------------------
 No                 :  1
 VrfIndex           :
 Fec                :  1.1.1.1/32
 Nexthop            :  127.0.0.1
 In-Label           :  3
 Out-Label          :  NULL
 Out-Interface      :  InLoopBack0
 LspIndex           :  6144
 Token              :  0x0
 LsrType            :  Egress
 Outgoing token     :  0x0
 Label Operation    :  POP
 Down Time          :  2011/11/08 16:39:59
 Exist time         :  14sec
 Down Reason        :  policy changed

 No                 :  2
 VrfIndex           :
 Fec                :  2.2.2.2/32
```

```
Nexthop          :  100.1.2.2
In-Label         :  NULL
Out-Label        :  3
Out-Interface    :  InLoopBack0
LspIndex         :  6146
Token            :  0x1
LsrType          :  Ingress
Outgoing token   :  0x0
Label Operation  :  PUSH
Down Time        :  2011/11/08 16:51:26
Exist time       :  5sec
Down Reason      :  route changed
```

Table 11-13 Description of the display mpls last-info lsp-down protocol ldp verbose command output

Item	Description
No	Sequence number.
VrfIndex	Index of a VRF instance.
Fec	Forwarding equivalence class.
Nexthop	Next hop IP address.
In-Label	Value of the incoming label.
Out-Label	Value of the outgoing label.
Out-Interface	Outbound interface.
LspIndex	Index of an LSP.
Token	Token value, in the hexadecimal format.
LsrType	Type of an LSR on an LSP, which can be ingress, transit, or egress.
Outgoing token	Outgoing token value, in the hexadecimal format.
Label Operation	Label operation, which can be PUSH, POP, SWAP, or SWAPPUSH.
Down Time	Time when an LSP goes Down.
Exist time	Existing period of an LDP LSP, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Down Reason	LSPs go Down due to the following causes: ● route changed: A route was changed. ● adjacency changed: An adjacency was changed. ● cannot recovery from GR: The LDP LSP failed to be reestablished during GR. ● recv release msg: A Release message was received. ● recv withdraw msg: A Withdraw message was received. ● US lost: The session with the upstream node went Down. ● DS lost: The session with the downstream node went Down. ● policy changed: The policy to establish LSPs was changed (Generally, configurations of the policy was changed). ● reach paf limit: PAF resources are insufficient. ● GR aging: The LSP aged after GR. ● others

11.1.23 display mpls ldp

Function

The **display mpls ldp** command displays global LDP configurations.

Format

display mpls ldp [**all**] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all LDP information.	-
verbose	Displays detailed information about the LDP protocol and the LSR.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After global MPLS is enabled, run the **display mpls ldp** command to view LDP configurations, including configurations of the GR timer, label distribution, and label management.

Example

Display global LDP configurations.

```
<Huawei> display mpls ldp

                    LDP Global Information
 ------------------------------------------------------------------------------
 Protocol Version        : V1            Neighbor Liveness     : 600 Sec
 Graceful Restart        : Off           FT Reconnect Timer    : 300 Sec
 MTU Signaling           : On            Recovery Timer        : 300 Sec
 Capability-Announcement : Off           Longest-match         : Off
 mLDP P2MP Capability    : Off           mLDP MBB Capability   : Off
 mLDP MP2MP Capability   : Off
                    LDP Instance Information
 ------------------------------------------------------------------------------
 Instance ID             : 0             VPN-Instance          :
 Instance Status         : Active        LSR ID                : 1.2.3.4
 Loop Detection          : Off           Path Vector Limit     : 32
 Label Distribution Mode : Ordered
 Label Retention Mode    : Liberal(DU)/Conservative(DOD)
 Instance Deleting State : No            Instance Reseting State : No
 Graceful-Delete         : Off           Graceful-Delete Timer : 5 Sec
 ------------------------------------------------------------------------------
```

Table 11-14 Description of the display mpls ldp command output

Item	Description
LDP Global Information	Global LDP information.
Protocol Version	LDP protocol version.
Neighbor Liveness	Timeout period of the GR Neighbor-liveness timer.
Graceful Restart	Whether LDP is enabled with GR: ● On: GR is enabled. ● Off: GR is disabled.
FT Reconnect Timer	Timeout period of the GR reconnect timer.
MTU Signaling	Whether the MTU signaling is enabled: ● On: The private MTU TLV is sent. ● Off: The MTU TLV is not supported. ● On(apply-tlv): The MTU TLV is sent according to RFC.
Recovery Timer	Timeout period of the GR Recovery timer.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Capability-Announcement	Status of the LDP dynamic capability announcement function: ● On: LDP dynamic capability announcement is enabled. ● Off: LDP dynamic capability announcement is disabled.
Longest-match	Status of LDP extension for inter-area LSP: ● On: LDP extension for inter-area LSP is enabled. ● Off: LDP extension for inter-area LSP is disabled.
mLDP P2MP Capability	Whether mLDP P2MP is globally enabled: ● On: mLDP P2MP is enabled globally. ● Off: mLDP P2MP is disabled globally. **NOTE** The device does not support this parameter.
mLDP MBB Capability	Whether the mLDP make-before-break capability is enabled: ● On: mLDP make-before-break is enabled. ● Off: mLDP make-before-break is disabled. **NOTE** The device does not support this parameter.
LDP Instance Information	Information about the LDP multi-instance.
Instance ID	ID of a VPN instance in the integer format.
VPN-Instance	Name of a VPN instance. The default name is **null**. **NOTE** The router does not support this parameter.
Instance Status	Status of an instance: ● Active: The instance is in the Active state. ● NotInService: The instance is in the NotInService state temporarily due to certain operations. For example, after the **reset mpls ldp** or **graceful-restart** command is used, the instance is unavailable temporarily. ● Destroy: The instance is in the Destroy state. For example, after the **undo mpls ldp** command is used, the instance is in the Destroy state.
LSR ID	LSR ID of an LDP instance.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Loop Detection	Loop detection status: ● On: Loop detection is enabled. ● Off: Loop detection is disabled.
Path Vector Limit	Path vector limit for loop detection.
Label Distribution Mode	Label distribution mode: ● Ordered ● Independent Currently, the router supports only the ordered mode.
Label Retention Mode	● If label advertisement mode is DU, label retention mode will be Liberal. ● If label advertisement mode is DOD, label retention mode will be Conservative.
Instance Deleting State	Deletion status of an instance: ● Yes: The instance is being deleted. ● No: The instance is not being deleted.
Instance Reseting State	Resetting status of an instance: ● Yes: The instance is being reset. ● No: The instance is not being reset.
Graceful-Delete	Whether graceful deletion is enabled: ● On: enables graceful deletion. ● Off: disables graceful deletion. **NOTE** The devices does not support this parameter.
Graceful-Delete Timer	Value of the Graceful-delete Timer, in seconds.

Related Topics

11.1.82 mpls ldp (system view)

11.1.24 display mpls ldp adjacency

Function

The **display mpls ldp adjacency** command displays information about LDP adjacencies.

Format

display mpls ldp adjacency [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**]

display mpls ldp adjacency all [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about the LDP adjacency of a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
remote	Displays information about the LDP adjacency of a specified remote end.	-
peer *peer-id*	Displays information about the LDP adjacency of a specified peer.	The value is in dotted decimal notation.
verbose	Displays detailed information about LDP adjacencies.	-
all	Displays information about all the LDP adjacencies.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an LDP session is established, run the **display mpls ldp adjacency** command to view real-time information about LDP adjacencies, for example, the number of received Hello messages.

Example

Display information about LDP adjacencies.

```
<Huawei> display mpls ldp adjacency

 LDP Adjacency Information in Public Network
 Codes: R: Remote Adjacency, L: Local Adjacency
 A '*' before an adjacency means the adjacency is being deleted.
 ------------------------------------------------------------------------------
 SN   SourceAddr      PeerID          VrfID AdjAge(DDDD:HH:MM) RcvdHello Type
 ------------------------------------------------------------------------------
  1   10.1.2.2        2.2.2.2          0      0000:00:22        527       L
  2   10.2.3.3        3.3.3.3          0      0000:00:20        254       L
  3   3.3.3.3         3.3.3.3          0      0000:00:18        79        R
 ------------------------------------------------------------------------------
 TOTAL: 3 Record(s) found.
```

Table 11-15 Description of the display mpls ldp adjacency command output

Item	Description
SN	Serial number.
SourceAddr	Source address of the Hello message received by an LDP adjacency.
PeerID	LSR ID of an LDP peer.
VrfID	ID of a VPN instance.
AdjAge(DDDD:HH:MM)	Time elapsed since the LDP adjacency was created, in DDDD:HH:MM format.
RcvdHello	Number of Hello messages received by an LDP adjacency.
Type	Type of an LDP adjacency: ● L: local LDP adjacency. ● R: remote LDP adjacency.

Display detailed information about the LDP adjacency of the remote peer with the LSR ID of 3.3.3.3/32.

```
<Huawei> display mpls ldp adjacency remote peer 3.3.3.3 verbose

 LDP Adjacency Information in Public Network
 ------------------------------------------------------------------------------
                        LDP Peer ID : 3.3.3.3
                   VPNInstance name : -
                         CreateDate : 2005-07-27
                         CreateTime : 11:15:41 00:00
                      Adjacency Age : 0000:03:44
                      AdjacencyType : Remote Adjacency
                   Discovery-Source : -
                 UDP Source Address : 3.3.3.3
                     UDP Socket ID : 33
                       Sequence No. : 0
  Configuration Hello Hold Timer(sec) : 45
                 Hello Message Rcvd : 899
          Adjacency Deletion Status : No
 ------------------------------------------------------------------------------
 TOTAL: 1 Adjacency(s) found.
```

Table 11-16 Description of the display mpls ldp adjacency remote peer command output

Item	Description
LDP Peer ID	LSR ID of an LDP peer.
VPNInstance name	Name of a VPN instance. **NOTE** The router does not support this parameter.
CreateDate	Creation date of an LDP adjacency.

Item	Description
CreateTime	Creation time of an LDP adjacency.
Adjacency Age	Time elapsed since the LDP adjacency was created, in DDDD:HH:MM format.
AdjacencyType	Type of an LDP adjacency: ● Local Adjacency. ● Remote Adjacency.
Discovery-Source	Discovery source of an LDP adjacency: ● Interface: a discovery source of the local LDP adjacency. ● Null: a discovery source of the remote LDP adjacency.
UDP Source Address	Source address of the UDP packet contained in the Hello message received by an LDP adjacency.
UDP Socket ID	Socket ID of the LDP adjacency to receive Hello message.
Sequence No	Serial number carried in the received Hello message. The default value is 0.
Configuration Hello Hold Timer(sec)	Hello hold timer configured on the peer, in seconds: ● Link Hello hold timer: maintains the local LDP adjacency. The default value is 15. ● Target Hello hold timer: maintains the remote LDP adjacency. The default value is 45.
Hello Message Rcvd	Number of Hello messages received by an LDP adjacency.
Adjacency Deletion Status	Deletion status of an LDP adjacency: ● Yes: The LDP adjacency is being deleted. ● No: The LDP adjacency is not being deleted.

Related Topics

11.1.35 display mpls ldp peer

11.1.25 display mpls ldp adjacency statistics

Function

The **display mpls ldp adjacency statistics** command displays statistics about LDP adjacencies.

Format

display mpls ldp adjacency statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls ldp adjacency statistics** command to view the number of LDP adjacencies that are classified into local and remote LDP adjacencies.

Example

Display statistics about LDP adjacencies.

```
<Huawei> display mpls ldp adjacency statistics

 LDP Adjacency Statistics Information
 ---------------------------------------------------
 AdjacencyType          Local   Remote   Total
 ---------------------------------------------------
 AdjacencyNumber         1       2        3
 ---------------------------------------------------
```

Table 11-17 Description of the display mpls ldp adjacency statistics command output

Item	Description
AdjacencyType	Type of LDP adjacencies.
AdjacencyNumber	Number of LDP adjacencies.
Local	Number of local LDP adjacencies.
Remote	Number of remote LDP adjacencies.
Total	Total number of LDP adjacencies.

Related Topics

11.1.24 display mpls ldp adjacency

 Copyright © Huawei Technologies Co., Ltd.

11.1.26 display mpls ldp error packet

Function

The **display mpls ldp error packet** command displays information about LDP-related error messages.

Format

display mpls ldp error packet { **tcp** | **udp** } [*number*]

Parameters

Parameter	Description	Value
tcp	Displays information about TCP error messages related to LDP sessions.	-
udp	Displays information about UDP error messages related to LDP sessions.	-
number	Specifies the number of LDP-related error messages to be displayed.	The value is an integer ranging from 1 to 100.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an exception occurs on an MPLS network, run the **display mpls ldp error packet** command to view information about LDP-related error messages such as the number of received error messages.

Example

Displays information about error UDP packets related to LDP.

```
<Huawei> display mpls ldp error packet udp

  LDP Error UDP Packet
  Total received error packet number: 58
  Record error packet number        : 10
  Max Record error packet number    : 10
------------------- Number 1 ----------------------
  Date&Time         : 2011-11-08 16:39:59+08:00
  Error Reason      : unknown
  Interface         : GigabitEthernet1/0/0
  Instance ID       : 0
  Length            : 34
  Packet content    :
```

```
01 64 00 14 00 00 00 32 04 00 00 04 00 0f 00 00
04 01 00 04 01 01 01 01 00 00 00 00 00 00 00 00
00 00
```

Table 11-18 Description of the **display mpls ldp error packet** command output

Item	Description
Total received error packet number	Number of received error messages related to LDP sessions.
Record error packet number	Number of recorded error messages related to LDP sessions.
Max Record error packet number	Maximum number of error messages that can be recorded.
Date&Time	Date and time when an error message was received.
Error Reason	Cause for an error.
Interface	An interface that receives the message.
Instance ID	ID of an LDP instance to which the error message belongs.
Length	Length of the error message
Packet content	Contents of the error message in the binary format.

Related Topics

11.1.27 display mpls ldp error packet state

11.1.27 display mpls ldp error packet state

Function

The **display mpls ldp error packet state** command displays the record status of LDP-related error messages.

Format

display mpls ldp error packet state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an exception occurs on an MPLS network, run the **display mpls ldp error packet state** command to view the record status of error messages related to LDP sessions.

Example

Display the record status of LDP-related error messages.

```
<Huawei> display mpls ldp error packet state
-------------------------------------------
  Error UDP packet state            : ON
  Max UDP error packet number       : 100
  Current UDP error packet number   : 0
  Error TCP packet state            : ON
  Max TCP error packet number       : 100
  Current TCP error packet number   : 0
  Error L2VPN packet state          : ON
  Max L2VPN error packet number     : 100
  Current L2VPN error packet number : 0
-------------------------------------------
```

Table 11-19 Description of the display mpls ldp error packet state command output

Item	Description
Error UDP packet state	Whether or not UDP error messages can be detected and recorded: ● ON: UDP error message detection is enabled. ● OFF: UDP error message detection is disabled.
Max UDP error packet number	Maximum number of UDP error messages that can be recorded.
Current UDP error packet number	Number of recorded UDP error messages.
Error TCP packet state	Whether or not TCP error messages can be detected and recorded: ● ON: TCP error message detection is enabled. ● OFF: TCP error message detection is disabled.
Max TCP error packet number	Maximum number of TCP error messages that can be recorded.
Current TCP error packet number	Number of recorded TCP error messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Error L2VPN packet state	Whether or not L2VPN error messages can be detected and recorded: ● ON: L2VPN error message detection is enabled. ● OFF: L2VPN error message detection is disabled.
Max L2VPN error packet number	Maximum number of L2VPN error messages that can be recorded.
Current L2VPN error packet number	Number of recorded L2VPN error messages.

Related Topics

11.1.26 display mpls ldp error packet

11.1.28 display mpls ldp event adjacency-down

Function

The **display mpls ldp event adjacency-down** command displays events that LDP adjacencies go Down.

Format

display mpls ldp event adjacency-down [**interface** *interface-type interface-number* | **remote**] [**peer** *peer-id*] [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays events that LDP adjacencies on a specified interface go Down. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
remote	Indicates the remote LDP peer.	-
peer *peer-id*	Specifies the LSR ID of an LDP peer.	The value is in dotted decimal notation.
verbose	Displays details about events that LDP adjacencies go Down.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Run the **display mpls ldp event adjacency-down** command to view the event that an LDP adjacency went Down. The information includes the time, reason, and the duration of the LDP adjacency.

Precautions

A maximum of 1024 events can be displayed.

Example

Display the events that LDP adjacencies go Down.

```
<Huawei> display mpls ldp event adjacency-down

 LDP Adjacency Down Information
 ---------------------------------------------------------------------------
 PeerID          Down      Down                Duration      Reason
                 Date      Time                Time
 ---------------------------------------------------------------------------
 2.2.2.2:0       2012-04-24 17:08:59 00:00       0h44m54s      C
 2.2.2.2:0       2012-04-26 15:43:54 00:00       46h34m54s     A
 ---------------------------------------------------------------------------
 TOTAL: 2 Record(s) Found.
 A : The Adjacency is down because Hello Timer Expired.
 C : The administrator configuration to trigger.
 D : The Adjacency is down because delay-deleting timer expired.
 P : The Adjacency is down because the peer is being deleted.
 O : Other reason.
```

Table 11-20 Description of the display mpls ldp event adjacency-down command output

Item	Description
PeerID	LSR ID of an LDP peer.
Down Date	Date when an LDP adjacency went Down.
Down Time	Time when an LDP adjacency went Down.
Duration Time	Time elapsed since an LDP adjacency established.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Causes for the LDP adjacency Down event: ● A: The Hello timer expires. ● C: The configuration is changed. ● D: The delay deleting timer expires. ● P: The peer is deleted. ● O: other causes.

Display detailed information that LDP adjacencies go Down.

```
<Huawei> display mpls ldp event adjacency-down verbose

 LDP Adjacency-Down Information
 ---------------------------------------------------------------------------
 SN                                : 1
 PeerID                             : 2.2.2.2
 VrfID                             : 0
 DownDate                               : 2012-04-24
 DownTime                               : 17:08:59  00:00
 DurationTime                           : 0h44m54s
 MaxInterval(sec)                       : 5
 Reason                              : configuration to trigger
 Type                              : Local Adjacency
 DiscoverySource                        : GigabitEthernet0/0/1
 -----------------------------------------------------------------------------
 SN                                : 2
 PeerID                             : 2.2.2.2
 VrfID                             : 0
 DownDate                               : 2012-04-26
 DownTime                               : 15:43:54  00:00
 DurationTime                           : 46h34m54s
 MaxInterval(sec)                       : 6
 Reason                              : Hello Timer Expired
 Type                              : Local Adjacency
 DiscoverySource                        : GigabitEthernet0/0/1
 -----------------------------------------------------------------------------
  TOTAL: 2 Record(s) Found.
```

Table 11-21 Description of the display mpls ldp event adjacency-down verbose command output

Item	Description
SN	Serial number.
PeerID	LSR ID of an LDP peer.
VrfID	ID of a VPN instance.
DownDate	Date when an LDP adjacency went Down.
DownTime	Time when an LDP adjacency went Down.

Item	Description
DurationTime	Time elapsed since an LDP adjacency established.
MaxInterval (sec)	Maximum interval for sending a Hello message.
Reason	Reason for the LDP adjacency Down event: ● A: The Hello timer expires. ● C: The configuration is changed. ● D: The delay deleting timer expires. ● P: The peer is deleted. ● O: other causes.
Type	Adjacency type: ● Local Adjacency: Directly connected adjacency. ● Remote Adjacency: Indirectly connected adjacency.
DiscoverySource	Interface where an LDP peer is discovered.

11.1.29 display mpls ldp event gr-helper

Function

The **display mpls ldp event gr-helper** command displays GR Helper information.

Format

display mpls ldp event gr-helper [**all** | *peer-id*]

Parameters

Parameter	Description	Value
all	Displays information about all GR Helpers.	-
peer-id	Displays information about a GR Helper on a specified LDP peer.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If GR Helpers are configured, run the **display mpls ldp event gr-helper** command to view GR Helper information.

Example

Display GR Helper information.

```
<Huawei> display mpls ldp event gr-helper
 LDP GR-Helper Peer Info
 ----------------------------------------------------------------------
 LDP InstanceId            : 0          Vpn Instance Name:
 Peer ID                   : 1.1.1.1
 Label Advertisement Mode   : Downstream Unsolicited
 Timer State               :
 Recovery Timer Left        : 229(s)
 Peer Gr Timer Configuration:
 Reconnect Timer            : 300(s)     Recovery Timer   : 300(s)
 Stale Lsp State            :
 USCB Counter               : 3          DSCB Counter     : 3
 ----------------------------------------------------------------------
 Total GR Peer Counter: 1
```

Table 11-22 Description of the display mpls ldp event gr-helper command output

Item	Description
LDP InstanceId	LDP instance name.
Vpn Instance Name	VPN instance name. **NOTE** The device does not support this parameter.
Peer ID	LSR ID of an LDP peer.
Label Advertisement Mode	Mode used by LDP to advertise labels.
Timer State	Status of the timer.
Recovery Timer Left	Remaining time before an LSP starts to be reestablished.
Peer Gr Timer Configuration	Configuration of the GR timers.
Reconnect Timer	Value of the LDP session reconnection timer.
Recovery Timer	Value of the LSP recovery timer.
Stale Lsp State	Status of the primary LSP.
USCB Counter	Number of upstream control blocks (USCBs).
DSCB Counter	Number of downstream control blocks (DSCBs).

 Copyright © Huawei Technologies Co., Ltd.

11.1.30 display mpls ldp event session-down

Function

The **display mpls ldp event session-down** command displays events that LDP sessions go Down.

Format

display mpls ldp event session-down

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp event session-down** command to view events that LDP sessions go Down, including the cause and time.

Example

Display events that LDP sessions go Down.

```
<Huawei> display mpls ldp event session-down

LDP Session Down Information
--------------------------------------------------------------------------------
PeerID      Down       Down            Duration   Flag Reason
          Date       Time            Time
--------------------------------------------------------------------------------
10.1.2.9:0  2011-12-15 10:14:11 00:00  0h6m15s    L    Recv Noti(0x000a)

10.1.2.9:0  2011-12-15 10:14:26 00:00  0h6m34s    L    Recv Noti(0x000a)

--------------------------------------------------------------------------------
TOTAL: 2 Record(s) Found.
R: Remote peer.
L: Local peer.
B: Both of local and remote peer.
G: Graceful Restart Session.
```

Table 11-23 Description of the display mpls ldp event session-down command output

Item	Description
PeerID	LSR ID of an LDP peer.

Item	Description
Down Date	Date when an LDP session went down.
Down Time	Time when an LDP session went down.
Duration Time	Time elapsed since an LDP adjacency established.
Flag	Peer type. ● R: Remote peer, indicating that a remote session has been established. ● L: Local peer, indicating that a local session has been established. ● B: Both of local and remote peer, indicating that both local and remote sessions have been established. ● G: Graceful Restart Session.
Reason	Description of the cause.

11.1.31 display mpls ldp interface

Function

The **display mpls ldp interface** command displays information about LDP-enabled interfaces.

Format

display mpls ldp interface [*interface-type interface-number* | [**all**] [**verbose**]]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. If the parameter is specified, the configurations of a specified LDP-enabled interface are displayed.	-
all	Displays information about all LDP-enabled interfaces.	-
verbose	Displays detailed information about LDP-enabled interfaces.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp interface** command to view configurations of LDP-enabled interfaces and some real-time information, such as the number of sent and received Hello messages.

Example

Display information about LDP-enabled interfaces.

```
<Huawei> display mpls ldp interface

 LDP Interface Information in Public Network
 Codes:LAM(Label Advertisement Mode), IFName(Interface name)
 A '*' before an interface means the entity is being deleted.
 ------------------------------------------------------------------------------
 IFName          Status       LAM   TransportAddress   HelloSent/Rcv
 ------------------------------------------------------------------------------
GE1/0/0        Active       DU    1.1.1.1            29574/29539
 ------------------------------------------------------------------------------
```

Table 11-24 Description of the display mpls ldp interface command output

Item	Description
IFName	Name of an LDP-enabled interface.
Status	Status of the local LSR: ● Active ● Inactive
LAM	Label advertisement mode: ● DU: downstream unsolicited mode. ● DoD: downstream on demand mode.
TransportAddress	IP address of a node that initiates a TCP connection for an LDP session.
HelloSent/Rcv	Number of sent and received Hello messages.

Display detailed information about LDP-enabled interfaces.

```
<Huawei> display mpls ldp interface verbose

 LDP Interface Information in Public Network
 ------------------------------------------------------------------------------
 Interface Name :GigabitEthernet1/0/0
 LDP ID          : 1.1.1.1:0             Transport Address : 1.1.1.1
 Entity Status  : Active                 Effective MTU : 1500

 Configured Hello Hold Timer     : 15 Sec
 Negotiated Hello Hold Timer     : 15 Sec
```

```
Configured Hello Send Timer     : 2 Sec
Configured Keepalive Hold Timer : 45 Sec
Configured Keepalive Send Timer : 3 Sec
Configured Delay Timer          : 10 Sec
Label Advertisement Mode        : Downstream Unsolicited
Hello Message Sent/Rcvd         : 29913/29878 (Message Count)
Entity Deletion Status          : No
mLDP P2MP Capability            : Disable
-------------------------------------------------------------------------------
```

Table 11-25 Description of the display mpls ldp interface verbose command output

Item	Description
Interface Name	Name of an LDP-enabled interface.
LDP ID	LDP identifier.
Transport Address	IP addresses used in the TCP connection of a session.
Entity Status	Status of this entity: ● Active ● Inactive
Effective MTU	MTU value used for creating an LSP.
Configured Hello Hold Timer	Timeout period of the configured Hello hold timer.
Negotiated Hello Hold Timer	Negotiated value of the Hello hold timer, which is the smaller value of the Hello hold timers configured on the local and remote LDP peers.
Configured Hello Send Timer	Timeout period of the configured Hello send timer.
Configured Keepalive Hold Timer	Timeout period of the configured Keepalive hold timer.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer.
Configured Delay Timer	Timeout period of the Delay timer, which, in LDP and IGP synchronization, is the time that an interface waits to establish an LSP after an LDP session is established.
Label Advertisement Mode	Label advertisement mode: ● Downstream Unsolicited ● Downstream on Demand
Hello Message Sent/Rcvd	Number of sent and received Hello messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Entity Deletion Status	Deletion status of an instance: • Yes: The instance is being deleted. • No: The instance is not being deleted.
mLDP P2MP Capability	Whether mLDP P2MP is enabled: • Enable • Disable

Related Topics

11.1.83 mpls ldp (interface view)
11.1.19 display mpls interface

11.1.32 display mpls label all summary

Function

The **display mpls label all summary** displays allocation information about all MPLS labels.

Format

display mpls label all summary

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a session is established, the system collects statistics on label usage, including the allocation range and protocol type. You can use the **display mpls label all summary** command to view the allocation of label space and the corresponding protocol type.

Example

Display allocation information about MPLS labels.

```
<Huawei> display mpls label all summary
TableType      MinValue    MaxValue    AvailableNum
```

```
Reserved          0        15          16
Static           16      1023         989
Dynamic        1024    100000       98970
Block        100001    102049        2049
```

Table 11-26 Description of the **display mpls label all summary** command output

Item	Description
TableType	Label type. ● Reserved ● Static ● Dynamic ● Block
MinValue	Minimum label value.
MaxValue	Maximum label value.
AvailableNum	Number of labels that can be allocated.

11.1.33 display mpls ldp lsp

Function

The **display mpls ldp lsp** command displays information about an LDP LSP.

Format

display mpls ldp lsp [**all** | *destination-address mask-length*] [**peer** *peer-id*]

display mpls ldp lsp inbound-policy

Parameters

Parameter	Description	Value
all	Displays information about all LDP LSPs.	-
destination-address	Specifies the destination IPv4 address of an LDP LSP.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the specified IPv4 address.	The value is an integer ranging from 0 to 32.
peer *peer-id*	Specifies the peer ID.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
inbound-policy	Displays information about the LSPs that have passed an inbound policy, in addition to information about the LSPs that are established without applying the inbound policy.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After LDP LSPs are set up, run the **display mpls ldp lsp** command to view detailed information about LSPs such as the outbound interfaces, next hop addresses, total number, and types.

By configuring the parameter **inbound-policy**, you can view information about LDP LSPs that have passed the inbound policy. If no inbound policy is configured, information about all LDP LSPs is displayed.

Example

Display information about LSPs.

```
<Huawei> display mpls ldp lsp

 LDP LSP Information
 -------------------------------------------------------------------------------
 DestAddress/Mask   In/OutLabel    UpstreamPeer    NextHop         OutInterface
 -------------------------------------------------------------------------------
 3.3.3.3/32         3/NULL         4.4.4.9         127.0.0.1       InLoop0
 3.3.3.9/32         3/NULL         4.4.4.9         127.0.0.1       InLoop0
*3.3.3.9/32         Liberal/1024                   DS/4.4.4.9
 4.4.4.9/32         NULL/3         -               162.1.1.2       GE1/0/0
 4.4.4.9/32         1029/3         4.4.4.9         162.1.1.2       GE1/0/0
 -------------------------------------------------------------------------------
 TOTAL: 4 Normal LSP(s) Found.
 TOTAL: 1 Liberal LSP(s) Found.
 TOTAL: 0 Frr LSP(s) Found.
 A '*' before an LSP means the LSP is not established
 A '*' before a Label means the USCB or DSCB is stale
 A '*' before a UpstreamPeer means the session is stale
 A '*' before a DS means the session is stale
 A '*' before a NextHop means the LSP is FRR LSP
```

Table 11-27 Description of the display mpls ldp lsp command output

Item	Description
DestAddress/Mask	Destination address and mask of an LSP.

Item	Description
In/OutLabel	Values of the incoming and outgoing labels. An asterisk (*) before In/OutLabel indicates that the LSP is in the Stale state and needs to be restored.
UpstreamPeer	Upstream peer of an LSP. An asterisk (*) before UpstreamPeer indicates that the session is in the GR state.
NextHop	Next hop IP address. An asterisk (*) before NextHop indicates that the LSP is a FRR LSP. DS is short for DownStream. The address next to DS/ is the LSR ID of a downstream peer.
OutInterface	Name of an outbound interface.

Related Topics

11.1.40 display mpls lsp
11.1.55 inbound peer fec

11.1.34 display mpls ldp lsp statistics

Function

The **display mpls ldp lsp statistics** command displays statistics about LDP LSPs.

Format

display mpls ldp lsp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls ldp lsp statistics** command displays the statistics about an LDP LSP, whereas the **display mpls lsp statistics** command displays the statistics about all types of LSPs.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics about LDP LSPs.

```
<Huawei> display mpls ldp lsp statistics

 LDP LSP Statistics Information
 A '*' before a number means the LSP is for longest-match
 ------------------------------------------------------------------------------
 VPNInstanceName   Total   Ingress   Transit   Egress   Liberal  FRR
 ------------------------------------------------------------------------------
 -                  14       4         4         3        3       0
                    *0      *0        *0        *0       *-      *0
 ------------------------------------------------------------------------------
```

Table 11-28 Description of the display mpls ldp lsp statistics command output

Item	Description
VPNInstanceName	Name of a VPN instance: ● A hyphen (-) indicates a public network instance. ● If LDP multi-instance is configured, the name of the created VPN instance is displayed. **NOTE** The router does not support this parameter.
Total	Number of LDP LSPs in an instance.
Ingress	Number of ingress LSPs in an instance.
Transit	Number of transit LSPs in an instance.
Egress	Number of egress LSPs in an instance.
Liberal	Number of liberal LSPs in an instance.
FRR	Number of FRR LSPs in an instance.

Related Topics

11.1.41 display mpls lsp statistics

11.1.35 display mpls ldp peer

Function

The **display mpls ldp peer** command displays information about LDP peers.

Format

display mpls ldp peer [[**all**] [**verbose**] | *peer-id*]

Parameters

Parameter	Description	Value
verbose	Displays detailed information about LDP peers.	-
peer-id	Displays information about a specified LDP peer.	The value is in dotted decimal notation.
all	Displays information about all LDP peers.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If an LDP LSP fails to be established, run the **display mpls ldp peer** command to view the **DiscoverySource** field and check the interface through which the peer relationship is established.

The system supports the coexistent local and remote LDP peers. When you run the **display mpls ldp peer** command, information about both local and remote LDP peers is displayed.

You can set the *peer-id* parameter to specify a peer.

Precautions

You can view information about LDP peers only after the peers have been established using the **mpls ldp (interface view)** or **remote-ip** command.

Example

Display information about LDP peers.

```
<Huawei> display mpls ldp peer

 LDP Peer Information in Public network
 A '*' before a peer means the peer is being deleted.
 ------------------------------------------------------------------------------
 PeerID              TransportAddress   DiscoverySource
 ------------------------------------------------------------------------------
 2.2.2.2:0           2.2.2.2            Remote Peer : rtb
 3.3.3.3:0           3.3.3.3            GigabitEthernet1/0/0
 ------------------------------------------------------------------------------
 TOTAL: 2 Peer(s) Found.
```

Table 11-29 Description of the display mpls ldp peer command output

Item	Description
PeerID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● Non-0: per-interface label space.
TransportAddress	Transport address of an LDP peer. The transport address is used to set up TCP connections.
DiscoverySource	Discovery source of an LDP peer: ● Interface name: indicates the source that discovers the local LDP peer. ● Remote LDP peer name: indicates the source that discovers the remote LDP peer.

Display detailed information about LDP peers.

```
<Huawei> display mpls ldp peer verbose

 LDP Peer Information in Public network
 ------------------------------------------------------------------------------
 Peer LDP ID          : 2.2.2.2:0
 Peer Max PDU Length : 4096          Peer Transport Address   : 2.2.2.2
 Peer Loop Detection : Off           Peer Path Vector Limit   : ----
 Peer FT Flag         : Off          Peer Keepalive Timer     : 45 Sec
 Recovery Timer       : ----         Reconnect Timer          : ----
 Peer Type            :Remote

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source          : remote peer: rtb
 Peer Deletion Status           : No
 Capability-Announcement        : Off
 Peer mLDP P2MP Capability      : Off
 Peer mLDP MBB Capability       : Off
 ------------------------------------------------------------------------------
 Peer LDP ID          : 3.3.3.3:0
 Peer Max PDU Length : 4096          Peer Transport Address   : 3.3.3.3
 Peer Loop Detection : Off           Peer Path Vector Limit   : ----
 Peer FT Flag         : Off          Peer Keepalive Timer     : 45 Sec
 Recovery Timer       : ----         Reconnect Timer          : ----
 Peer Type            : Local

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source          : GigabitEthernet1/0/0
 Peer Deletion Status           : No
 Capability-Announcement        : Off
 Peer mLDP P2MP Capability      : Off
 Peer mLDP MBB Capability       : Off
 ------------------------------------------------------------------------------
```

Table 11-30 Description of the display mpls ldp peer verbose command output

Item	Description
Peer LDP ID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● Non-0: per-interface label space.
Peer Max PDU Length	Maximum size of a PDU sent by an LDP peer.
Peer Transport Address	Transport address of an LDP peer. The transport address is used to set up TCP connections.
Peer Loop Detection	Whether loop detection of an LDP peer is enabled: ● On: Loop detection is enabled. ● Off: Loop detection is disabled.
Peer Path Vector Limit	Indicates the upper limit of the Path Vector for an LDP peer.
Peer FT Flag	GR FT flag of an LDP peer: ● On: LDP GR is enabled. ● Off: LDP GR is disabled. The flag can only be set after an Initialization message containing an FT TLV is received.
Peer Keepalive Timer	Configured value of the Keepalive timer on an LDP peer.
Recovery Timer	Timeout period of the Recovery timer of an LDP peer. The value of the Recovery Timer field is not null only when the Peer FT Flag field is On.
Reconnect Timer	Timeout period of the Reconnect timer of an LDP peer. The value of the Recovery Timer field is not null only when the Peer FT Flag field is On.
Peer Type	Type of an LDP peer: ● Local ● Remote ● Local&Remote

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Peer Label Advertisement Mode	Indicates the label advertisement mode of an LDP peer: ● Downstream Unsolicited ● Downstream on Demand The router supports the Downstream Unsolicited (DU) mode.
Peer Discovery Source	Discovery source of an LDP peer: ● If the interface is displayed, the source of the local LDP peer is the local interface. ● If the configuration name of the remote peer is displayed, the source end of the remote LDP peer is the remote peer.
Peer Deletion Status	Deletion status of an LDP peer: ● Yes: LDP peer is being deleted. ● No: LDP peer is not being deleted.
Capability-Announcement	Status of the LDP dynamic capability announcement function: ● On: LDP dynamic capability announcement is enabled. ● Off: LDP dynamic capability announcement is disabled.
Peer mLDP P2MP Capability	Whether the LDP peer supports mLDP P2MP: ● On: The LDP peer supports mLDP P2MP. ● Off: The LDP peer does not support mLDP P2MP.
Peer mLDP MBB Capability	Whether the LDP peer supports make-before-break: ● On: The LDP peer supports mLDP make-before-break. ● Off: The LDP peer does not support mLDP make-before-break.

Related Topics

11.1.83 mpls ldp (interface view)
11.1.107 remote-ip
11.1.37 display mpls ldp remote-peer
11.1.38 display mpls ldp session
11.1.24 display mpls ldp adjacency

 Copyright © Huawei Technologies Co., Ltd.

11.1.36 display mpls ldp peer statistics

Function

The **display mpls ldp peer statistics** command displays statistics about LDP peers.

Format

display mpls ldp peer statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp peer statistics** command to view the number of local LDP peers, remote LDP peers, and coexistent local and remote LDP peers.

Example

Display statistics about LDP peers.

```
<Huawei> display mpls ldp peer statistics

 LDP Peer Statistics Information
 -------------------------------------------------------
 PeerType        Local   Remote   Local&Remote   Total
 -------------------------------------------------------
 PeerNumber      0       1        1              2
 -------------------------------------------------------
```

Table 11-31 Description of the display mpls ldp peer statistics command output

Item	Description
PeerType	Type of LDP peers.
PeerNumber	Number of LDP peers.
Local	Number of local LDP peers.
Remote	Number of remote LDP peers.
Local&Remote	Number of coexistent local and remote LDP peers.
Total	Total number of all types of LDP peers.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

11.1.35 display mpls ldp peer

11.1.37 display mpls ldp remote-peer

Function

The **display mpls ldp remote-peer** command displays information about a remote LDP peer.

Format

display mpls ldp remote-peer [*remote-peer-name* | **peer-id** *lsr-id*]

Parameters

Parameter	Description	Value
remote-peer-name	Specifies the name of a remote LDP peer.	The value is an existing remote LDP peer.
peer-id *lsr-id*	Specifies the LSR ID of a remote LDP peer.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Remote LDP peers are used to set up remote LDP sessions to transmit VPN services.

To view information about the configured remote LDP peers, run the **display mpls ldp remote-peer** command.

Example

Display information about remote LDP peers.

```
<Huawei> display mpls ldp remote-peer

                    LDP Remote Entity Information
 ------------------------------------------------------------------------------
 Remote Peer Name  : lsrc
 Remote Peer IP    : 3.3.3.9          LDP ID        : 1.1.1.9:0
 Transport Address : 1.1.1.9          Entity Status : Active
```

```
Configured Keepalive Hold Timer : 45 Sec
Configured Keepalive Send Timer : ---
Configured Hello Hold Timer     : 45 Sec
Negotiated Hello Hold Timer     : 45 Sec
Configured Hello Send Timer     : ---
Configured Delay Timer          : 10 Sec
Hello Packet sent/received      : 61/59
Label Advertisement Mode        : Downstream Unsolicited
Remote Peer Deletion Status     : No
Auto-config                     : ---
--------------------------------------------------------------------------------
TOTAL: 1 Peer(s) Found.
```

Table 11-32 Description of the **display mpls ldp remote-peer** command output

Item	Description
Remote Peer Name	Name of a remote LDP peer.
Remote Peer IP	IP address of a remote LDP peer.
LDP ID	Local LDP ID.
Transport Address	Transport address, which is used to set up the LDP session between the local and remote peers.
Entity Status	Status of a remote LDP peer: ● Active ● Inactive
Configured Keepalive Hold Timer	Timeout period of the configured Keepalive hold timer.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer.
Configured Hello Hold Timer	Timeout period of the configured Hello hold timer.
Negotiated Hello Hold Timer	Timeout period of the negotiated Hello hold timer.
Configured Hello Send Timer	Timeout period of the configured Hello send timer.
Configured Delay Timer	Timeout period of the Delay timer, which, in LDP and IGP synchronization, is the time that an interface waits to establish an LSP after an LDP session is established.
Hello Packet sent/received	Number of sent and received Hello packets.
Label Advertisement Mode	Label advertisement mode in an LDP session. The default mode is DU.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote Peer Deletion Status	Deletion status of an LDP peer: ● Yes: The LDP peer is being deleted. ● No: The LDP peer is not being deleted.
Auto-config	Whether the remote peer is created by BGP AD.

Related Topics

11.1.35 display mpls ldp peer
11.1.38 display mpls ldp session
11.1.107 remote-ip

11.1.38 display mpls ldp session

Function

The **display mpls ldp session** command displays information about LDP sessions.

Format

display mpls ldp session [*peer-id* | [**all**] [**verbose**]]

Parameters

Parameter	Description	Value
peer-id	Displays information about LDP sessions of a specified LSR ID.	The value is in dotted decimal notation.
all	Displays information about all LDP sessions.	-
verbose	Displays detailed information about LDP sessions.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After creating an LDP session, run the **display mpls ldp session** command to verify that the LDP session is created successfully and view information about the LDP session, such as the number of sent or received Keepalive messages.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about all LDP sessions.

```
<Huawei> display mpls ldp session

 LDP Session(s) in Public Network
 Codes: LAM(Label Advertisement Mode), SsnAge Unit(DDDD:HH:MM)
 A '*' before a session means the session is being deleted.
 ------------------------------------------------------------------------------
 PeerID            Status      LAM  SsnRole  SsnAge       KASent/Rcv
 ------------------------------------------------------------------------------
 2.2.2.2:0         Operational DU   Passive  0000:01:36   387/386
 3.3.3.3:0         Operational DU   Passive  0000:01:30   361/361
 ------------------------------------------------------------------------------
 TOTAL: 2 session(s) Found.
```

Table 11-33 Description of the display mpls ldp session command output

Item	Description
PeerID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.
Status	Status of an LDP session: ● NonExistent: LDP peers at both ends of the LDP session exchange Hello messages to negotiate a TCP connection. After the TCP connection is established, the LDP session enters the Initialized state. The Non-Existent state is the initial state in the LDP session state machine. ● Initialized: The LDP session is in the initialization state. ● Open Sent: The LSR playing the active role in the LDP session sends an Initialization message to the LSR playing the passive role and waits for a reply during initialization. ● Open Recv: LDP peers at both ends of the LDP session wait for receiving a Keepalive message from each other during initialization. If they receive a Keepalive message from each other, the LDP session enters the Operational state. ● Operational: An LDP session is established successfully.
LAM	Label advertisement mode of an LDP peer. The default mode is DU.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SsnRole	Role that an LSR plays in an LDP session: ● Active: an LSR with a larger LSR ID between two LSRs. ● Passive: an LSR with a smaller LSR ID between two LSRs.
SsnAge	Time elapsed since an LDP session was set up in DDDD:HH:MM format.
KASent/Rcv	Number of Keepalive messages sent and received by an LDP session.

Display detailed information about all LDP sessions.

```
<Huawei> display mpls ldp session verbose

 LDP Session(s) in Public Network
 ------------------------------------------------------------------------------
 Peer LDP ID      : 2.2.2.2:0            Local LDP ID    : 1.1.1.1:0
 TCP Connection   : 1.1.1.1 <- 2.2.2.2
 Session State    : Operational          Session Role    : Passive
 Session FT Flag  : Off                  MD5 Flag        : Off
 Reconnect Timer  : ---                  Recovery Timer  : ---
 Keychain Name    : kc1

 Negotiated Keepalive Hold Timer   : 45 Sec
 Configured Keepalive Send Timer   : 3 Sec
 Keepalive Message Sent/Rcvd       : 438/438 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Session Age                       : 0000:01:49 (DDDD:HH:MM)
 Session Deletion Status           : No

 Capability:
  Capability-Announcement           : On
  mLDP P2MP Capability              : Off
  mLDP MBB Capability               : Off

 Outbound&Inbound Policies applied :
 outbound peer all split-horizon

 Addresses received from peer: (Count: 3)
 10.1.1.2            2.2.2.2             10.1.2.1
 ------------------------------------------------------------------------------
```

Table 11-34 Description of the display mpls ldp session verbose command output

Item	Description
Peer LDP ID	LDP identifier of the peer in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.

Item	Description
Local LDP ID	Local LDP identifier in the format of <LSR ID>:<label space>. The value of a label space can be either of the following: ● 0: per-platform label space. ● 1: per-interface label space.
TCP Connection	TCP connection of an LDP session: ● The LSR with a larger LSR ID value plays an active role in establishing the TCP connection. ● The LSR with a smaller LSR ID value plays a passive role in establishing the TCP connection.
Session State	Status of an LDP session: ● NonExistent: LDP peers at both ends of the LDP session exchange Hello messages to negotiate a TCP connection. After the TCP connection is established, the LDP session enters the Initialized state. The Non-Existent state is the initial state in the LDP session state machine. ● Initialized: The LDP session is in the initialization state. ● Open Sent: The LSR playing the active role in the LDP session sends an Initialization message to the LSR playing the passive role and waits for a reply during initialization. ● Open Recv: LDP peers at both ends of the LDP session wait for receiving a Keepalive message from each other during initialization. If they receive a Keepalive message from each other, the LDP session enters the Operational state. ● Operational: An LDP session is established successfully.
Session Role	Role that an LSR plays in an LDP session: ● Active: an LSR with a larger LSR ID between two LSRs. ● Passive: an LSR with a smaller LSR ID between two LSRs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Session FT Flag	Negotiated LDP GR capability: ● On: Negotiated LDP GR capability is enabled. ● Off: Negotiated LDP GR capability is disabled.
MD5 Flag	MD5 authentication flag: ● On: MD5 authentication is enabled during the TCP connection establishment. ● Off: MD5 authentication is disabled during the TCP connection establishment.
Reconnect Timer	Negotiated timeout period of the Reconnect timer. The value of the Recovery Timer field is not null only when the Session FT Flag field is On.
Recovery Timer	Negotiated timeout period of the Recovery timer. The value of the Recovery Timer field is not null only when the Session FT Flag field is On.
Keychain Name	Referenced keychain authentication name.
Negotiated Keepalive Hold Timer	Negotiated value of the Keepalive hold timer, which is the smallest value of the Keepalive hold timers configured on the local and remote LDP peers.
Configured Keepalive Send Timer	Timeout period of the configured Keepalive send timer.
Keepalive Message Sent/Rcvd	Number of Keepalive messages sent and received by an LDP session.
Label Advertisement Mode	Label advertisement mode: ● Downstream Unsolicited ● Downstream on Demand The default mode is Downstream Unsolicited (DU).
Label Resource Status(Peer/Local)	Label resource status of the remote and local peers.
Session Age	Time elapsed since an LDP session was set up.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Session Deletion Status	Deletion status of an LDP session: ● Yes: The LDP session is being deleted. ● No: The LDP session is not being deleted.
Capability	LDP capability.
Capability-Announcement	LDP dynamic capability announcement function: ● On: LDP dynamic capability announcement is enabled. ● Off: LDP dynamic capability announcement is disabled.
mLDP P2MP Capability	Whether mLDP P2MP is supported after a session is negotiated: ● On: mLDP P2MP is supported. ● Off: mLDP P2MP is not supported. **NOTE** The router does not support this parameter.
mLDP MBB Capability	Whether mLDP make-before-break is supported after a session is negotiated: ● On: mLDP make-before-break is supported. ● Off: mLDP make-before-break is not supported. **NOTE** The router does not support this parameter.
Outbound&Inbound Policies applied	Outbound and inbound policies on the local node.
Addresses received from peer	Contents of an Address message sent by an LDP peer. The contents include the LSR ID of the peer and the IP address of the LDP-enabled interface.

Related Topics

11.1.33 display mpls ldp lsp
11.1.35 display mpls ldp peer
11.1.37 display mpls ldp remote-peer

11.1.39 display mpls ldp session statistics

Function

The **display mpls ldp session statistics** command displays statistics about sessions between LDP peers.

Format

display mpls ldp session statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls ldp session statistics** command to view the number of sessions between LDP peers. Statistics are collected based on the session type and status. The session type can be local, remote, or coexistent local and remote. The session status can be Not Operational or Operational.

Example

Display statistics about LDP sessions.

```
<Huawei> display mpls ldp session statistics

 LDP Session Statistics Information
 ------------------------------------------------------------
 SessionType         Local   Remote   Local&Remote   Total
 ------------------------------------------------------------
 Not Operational     0       0        0              0
 Operational         0       1        1              2
 ------------------------------------------------------------
 SessionStatistics   0       1        1              2
 ------------------------------------------------------------
```

Table 11-35 Description of the display mpls ldp session statistics command output

Item	Description
SessionType	Type of LDP sessions.
Local	Number of local LDP sessions.
Remote	Number of remote LDP sessions.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Local&Remote	Number of coexistent local and remote LDP sessions.
Total	Total number of sessions.
Not Operational	Number of sessions in the Not Operational state.
Operational	Number of sessions in the Operational state.
SessionStatistics	Total number of local sessions, remote sessions, and coexistent local and remote sessions.

Related Topics

11.1.38 display mpls ldp session

11.1.40 display mpls lsp

Function

The **display mpls lsp** command displays information about LSPs.

The **display mpls lsp lsp-id** command displays information about CR-LSPs only.

Format

display mpls lsp lsp-id *ingress-lsr-id session-id lsp-id* [**verbose**]

display mpls lsp [[**vpn-instance** *vpn-instance-name* [**ipv4-family** | **ipv6-family**]] [**protocol** { **bgp** | **bgp-ipv6** | **rsvp-te** | **static** | **static-cr** }] | **asbr**] [{ **exclude** | **include** } *ip-address mask-length*] [**incoming-interface** *interface-type interface-number*] [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp [**vpn-instance** *vpn-instance-name* [**ipv4-family** | **ipv6-family**]] **protocol ldp** [{ **exclude** | **include** } *ip-address mask-length*] [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp stale-incoming-interface *interface-index* [**outgoing-interface** *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

display mpls lsp stale-outgoing-interface *interface-index* [**in-label** *in-label-value*] [**out-label** *out-label-value*] [**nexthop** *ip-address*] [**lsr-role** { **egress** | **ingress** | **transit** }] [**verbose**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
lsp-id	Specifies the LSP ID.	The value is an integer ranging from 0 to 65535.
ingress-lsr-id	Specifies the ID of the ingress LSR.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer ranging from 0 to 65535.
vpn-instance *vpn-instance-name*	Displays detailed configurations of LSPs of a specified VPN instance.	The value is an existing VPN instance name.
ipv4-family	Indicates the IPv4 unicast address-family.	-
ipv6-family	Indicates the IPv6 unicast address-family.	-
protocol	Displays information about LSPs of a specified type.	-
ldp	Indicates LDP.	-
bgp	Indicates BGP.	-
bgp-ipv6	Indicates BGP IPv6.	-
rsvp-te	Indicates RSVP-TE.	-
static	Indicates Static.	-
static-cr	Indicates Static-CR.	-
asbr	Displays information about LSPs of a specified ASBR.	-
exclude	Displays information about LSPs, excluding information about the specific FEC.	-
include	Displays information about LSPs, including information about the specific FEC.	-
ip-address	Displays information about LSPs of a specified IPv4 address or a specified IPv6 address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mask-length	Specifies the mask length of the specified IPv4 address or a specified IPv6 address.	The value is an integer ranging from 0 to 32. Alternatively, it specifies the mask length of the specified IPv6 address. The value is an integer ranging from 0 to 128.
incoming-interface *interface-type interface-number*	Specifies the type and number of an inbound interface. You can view the configuration of an LSP on a specified interface.	-
outgoing-interface *interface-type interface-number*	Indicates the type and number of an outbound interface. You can view the configuration of an LSP on a specified interface.	-
in-label *in-label-value*	Displays information about LSPs of a specified incoming label.	The value is an integer ranging from 0 to 1048575.
out-label *out-label-value*	Displays information about LSPs of a specified outgoing label.	The value is an integer ranging from 0 to 1048575.
nexthop *ip-address*	Displays information about LSPs of a specified IPv4 or IPv6 next hop address.	The value is in dotted decimal notation.
lsr-role	Displays information about all LSPs on the current LSR that plays a specified role.	-
egress	Displays information about LSPs of an egress LSR.	-
ingress	Displays information about LSPs of an ingress LSR.	-
transit	Displays information about LSPs of a transit LSR.	-
verbose	Displays detailed information about LSPs.	-
stale-incoming-interface	Displays information about the stale inbound interface of an LSP.	-
stale-outgoing-interface	Displays information about the stale outbound interface of an LSP.	-
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer ranging from 1 to FFFFFFFE.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify a parameter, information about all LSPs is displayed.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

Display information about all types of LSPs.

```
<Huawei> display mpls lsp
-------------------------------------------------------------------------------
                LSP Information: RSVP LSP
-------------------------------------------------------------------------------
 FEC              In/Out Label  In/Out IF                      Vrf Name
 10.2.2.9/32        NULL/11264    -/GE1/0/0
-------------------------------------------------------------------------------
                LSP Information: LDP LSP
-------------------------------------------------------------------------------
 FEC              In/Out Label  In/Out IF                      Vrf Name

 10.2.2.9/32        NULL/3        -/GE1/0/0
 10.2.2.9/32        1024/3        -/GE1/0/0
 10.3.3.9/32        NULL/3        -/GE2/0/0
 10.3.3.9/32        1025/3        -/GE2/0/0
```

Display information about all LSPs with the next hop of 192.168.1.1.

```
<Huawei> display mpls lsp nexthop 192.168.1.1
-------------------------------------------------------------------------------
           LSP Information: L3VPN Label-Per-Nexthop LSP
-------------------------------------------------------------------------------
IndirectID  NextHop          In/Out Label  In/Out IF      Vrf Name
0x1         192.168.1.1      13312/13312   -/-            ASBR LSP
```

Display detailed information about all types of LSPs.

```
<Huawei> display mpls lsp verbose
-------------------------------------------------------------------------------
                LSP Information: RSVP LSP
-------------------------------------------------------------------------------

 No                 :  1
 SessionID          :  300
 IngressLsrID       :  10.1.1.9
 LocalLspID         :  1
 Tunnel-Interface   :  Tunnel0/0/1
 Fec                :  10.2.2.9/32
 TunnelTableIndex   :  0x1
 Nexthop            :  10.5.1.2
 In-Label           :  NULL
 Out-Label          :  11264
 In-Interface       :  ----------
 Out-Interface      :  GE1/0/0
 LspIndex           :  3072
 Token              :  0x8002008
```

```
 LsrType            :  Ingress
 Mpls-Mtu           :  1500
 TimeStamp          :  1171sec
 Bfd-State          :  ---
 CBfd-Event         :  0x0
 Bed-State          :  ---
 Bed-LastNotifyValue :  ---
 Bed-LastNotifyLspId :  ---

-------------------------------------------------------------------------------
                LSP Information: LDP LSP
-------------------------------------------------------------------------------
 No                 :  2
 Vrf Name           :
 Fec                :  10.2.2.2/32
 Nexthop            :  10.1.1.2
 In-Label           :  NULL
 Out-Label          :  3
 In-Interface       :  ----------
 Out-Interface      :  GE1/0/0
 LspIndex           :  9217
 Token              :  0x802009
 FrrToken           :  0x0
 LsrType            :  Ingress
 Outgoing token     :  0x0
 Label Operation    :  PUSH
 Mpls-Mtu           :  ------
 TimeStamp          :  21086sec
 Bfd-State          :  ---
 BGPKey             :  -----

 No                 :  3
 Vrf Name           :
 Fec                :  10.2.2.2/32
 Nexthop            :  10.2.1.2
 In-Label           :  NULL
 Out-Label          :  3
 In-Interface       :  ----------
 Out-Interface      :  GE2/0/0
 LspIndex           :  9218
 Token              :  0x80200a
 FrrToken           :  0x0
 LsrType            :  Ingress
 Outgoing token     :  0x0
 Label Operation    :  PUSH
 Mpls-Mtu           :  ------
 TimeStamp          :  19569sec
 Bfd-State          :  ---
 BGPKey             :  -----
```

Table 11-36 Description of the display mpls lsp command output

Item	Description
LSP Information	LSP information: ● STATIC LSP: manually created. ● LDP LSP: created using LDP. ● STATIC CR-LSP: a static MPLS TE tunnel created manually. ● RSVP LSP: an MPLS TE tunnel created using RSVP-TE. ● BGP LSP: an LSP created using BGP based on private or public IPv4 BGP routes. ● L3VPN LSP: an LSP based on IPv4 VPN routes received by means of BGP.
FEC/Fec	Forwarding equivalence class. Usually, the value is the destination address of an LSP.
In/Out Label	Values of the incoming and outgoing labels.
In/Out IF	Names of the incoming and outbound interfaces.
Vrf Name	Name of a VPN instance.
IndirectID	Index of the next hop of a BGP route.
No	Serial number of an LSP.
SessionID	Session ID of a CR-LSP.
IngressLsrID	Ingress LSR ID of a CR-LSP.
LocalLspID	Local LSP ID of a CR-LSP.
Tunnel-Interface	Tunnel interface.
Vrf Name	Index of a VPN instance. This value is available for only non-CR-LSPs.
Nexthop	IP address of the next hop of an LSP.
TunnelTableIndex	Index of a tunnel table.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Name of an inbound interface.
Out-Interface	Name of an outbound interface.
LspIndex	Index number of an LSP, which uniquely identifies an LSP that is established using a specific protocol.
Token	LSP token. It guides the packet forwarding.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FrrToken	Token of a standby LDP LSP. This value is available for only non-CR-LSPs.
LsrType	Role of an LSR on an LSP: ● Ingress ● Transit ● Egress
Outgoing token	Token that guides the packet forwarding, which is available for only non-CR-LSPs.
Label Operation	Type of a label operation, which is available for only non-CR-LSPs: ● PUSH ● SWAP ● POP ● SWAPPUSH
Mpls-Mtu	Maximum transmission unit (MTU) of an interface of an LSP.
TimeStamp	Time elapsed since an LSP was set up.
Bfd-State	BFD status.
CBfd-Event	Error code event that BFD reports to the RSVP LSP on the ingress node.
Bed-State	Error code status of an RSVP LSP on the ingress node.
Bed-LastNotifyValue	Error code association of which the RSVP LSP notifies BFD on the egress node.
Bed-LastNotifyLspId	ID of the reversed LSP that corresponds to the error code association event on the egress node. The association event is notified of BFD by the RSVP LSP.
BGPKey	Index of BGP.

Related Topics

11.1.43 display mpls static-lsp

11.1.41 display mpls lsp statistics

Function

The **display mpls lsp statistics** command displays statistics about the LSPs that are in the Up state and the number of the LSPs that are activated on the ingress, transit, and egress nodes.

Format

display mpls lsp statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display mpls lsp statistics** command to view statistics about the LSPs and CR-LSPs that are in the Up state.

To view detailed information about the LSPs and CR-LSPs, run the **display mpls lsp** command.

Example

Display statistics about LSPs.

```
<Huawei> display mpls lsp statistics
Lsp Type        Total     Ingress   Transit   Egress
STATIC LSP      0         0         0         0
STATIC CRLSP    0         0         0         0
LDP LSP         4         3         0         1
RSVP CRLSP      0         0         0         0
BGP LSP         1         0         0         1
ASBR LSP        0         0         0         0
BGP IPV6 LSP    0         0         0         0
L3VPN IPV6 LSP 0          0         0         0
-----------------------------------------------------------------------
LSP             5         3         0         2
CRLSP           0         0         0         0
-----------------------------------------------------------------------
Lsp Type        IngressLspBypassState          TransitLspBypassState
                ExistNotUsed   InUse           ExistNotUsed   InUse
RSVP CRLSP      0              0               0              0
-----------------------------------------------------------------------
```

Table 11-37 Description of the display mpls lsp statistics command output

Item	Description
Lsp Type	Type of an LSP: ● STATIC LSP: a static LSP. ● STATIC CRLSP: a static CR-LSP. ● LDP LSP: created using LDP. ● RSVP CRLSP: an MPLS TE tunnel created using RSVP-TE. ● BGP LSP: an LSP created using BGP based on private or public IPv4 BGP routes. ● ASBR LSP: created using BGP based on received IPv4 VPN route. ● BGP IPV6 LSP: an LSP created using BGP based on private IPv6 routes. ● L3VPN IPV6 LSP: created using BGP based on received IPv6 VPN routes. ● LSP: Label Switched Path. ● CRLSP: Constraint-based Routed Label Switched Path.
Total	Number of LSPs of a specific type.
Ingress	Number of LSPs on the local ingress LSR.
Transit	Number of LSPs on the local transit LSR.
Egress	Number of LSPs on the local egress LSR.
IngressLspBypassState	State of the ingress LSP enabled with FRR: ● ExistNotUsed: Bypass LSP that is bound to the primary LSP but has no traffic. ● InUse: Traffic switched to the bypass LSP.
TransitLspBypassState	State of the Transit LSP enabled with FRR: ● ExistNotUsed: Bypass LSP that is bound to the primary LSP but has no traffic. ● InUse: Traffic switched to the bypass LSP.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

11.1.40 display mpls lsp

11.1.42 display mpls route-state

Function

The **display mpls route-state** command displays routing information about a dynamic LSP.

Format

display mpls route-state [{ **exclude** | **include** } { **idle** | **ready** | **settingup** } * | *destination-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
exclude	Displays routing information excluding the specified route.	-
include	Displays information about a specified route.	-
idle	Indicates that a route is not used to establish an LSP.	-
ready	Indicates that a route has been used to establish an LSP.	-
settingup	Indicates that a signaling protocol is creating an LSP.	-
destination-address	Specifies the destination address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a specified destination address.	The value is an integer ranging from 0 to 32.
verbose	Displays detailed routing information about an LSP.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After completing LDP LSP configurations, run the **display mpls ldp lsp** command to view information about an LDP LSP. If the command output displays no information about the LDP LSP, run the **display mpls route-state** command to view LDP LSP routing information.

Example

Display detailed information about routes of dynamic LSPs.

```
<Huawei> display mpls route-state verbose

Codes: B(BGP), I(IGP), L(Public Label BGP), O(Original BGP), U(Unknown)
-------------------------------------------------------------------------------
Dest/Mask        Next-Hop       Out-Interface        State    LSP   VRF Type
-------------------------------------------------------------------------------
10.21.21.21/32    10.22.22.21    GigabitEthernet1/0/0          READY    2     0   I
    LspIndex: 30720     InLabel: NULL      OutLabel: 3
    LspIndex: 32728     InLabel: 1024      OutLabel: 3
10.0.0.6/32       10.21.22.21    GigabitEthernet1/0/0          READY    1     0   I
    LspIndex: 33053     InLabel: NULL      OutLabel: 3338
```

Table 11-38 Description of the display mpls route-state verbose command output

Item	Description
Dest/Mask	Destination IP address and mask length.
Next-Hop	Next hop IP address.
Out-Interface	Outbound interface.
State	Routing state of the MPLS control plane: ● IDLE: The route is not used to establish an LSP. ● SETTINGUP: A signaling protocol is creating an LSP. ● READY: The route has been used to establish an LSP. Static LSPs are only in READY state.
LSP	Number of LSPs reachable to the destination address. If the displayed value is not 0, there are LSPs reachable to the destination address and LSP information about these LSPs is also displayed.
VRF	Index of a VPN instance. The value 0 indicates the public network.
Type	Route type: ● B: BGP routes ● I: IGP routes ● L: labeled BGP routes of a public network ● O: original BGP routes ● U: unidentified routes (such as multicast routes)
LspIndex	Index of an LSP established using the route.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
InLabel	Incoming label of an LSP established using the route. If NULL is displayed, the current node is the ingress node of the LSP; if a number is displayed, the current node is the transit or egress node of the LSP.
OutLabel	Outgoing label of an LSP established using the route.

11.1.43 display mpls static-lsp

Function

The **display mpls static-lsp** command displays information about static LSPs.

Format

display mpls static-lsp [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is an existing static LSP name.
include	Displays information about LSPs, including information about the specific FEC.	-
exclude	Displays information about LSPs, excluding information about the specific FEC.	-
ip-address	Specifies the destination IPv4 address.	The value is in dotted decimal notation.
mask-length	Specifies the length of an IPv4 mask.	The value is an integer ranging from 0 to 32.
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Static LSPs are configured locally, so you need to run the **ping lsp** command to check whether the static LSP can work normally. If the static LSP cannot work normally, run the **display mpls static-lsp** command to view information about static LSPs.

Example

Display brief information about static LSPs.

```
<Huawei> display mpls static-lsp
TOTAL          : 1       STATIC LSP(S)
UP             : 1       STATIC LSP(S)
DOWN           : 0       STATIC LSP(S)
Name       FEC              I/O Label  I/O If              Status
lsp1       3.3.3.9/32       NULL/100   -/GE1/0/0           Up
```

Table 11-39 Description of the display mpls static-lsp command output

Item	Description
TOTAL	Total number of static LSPs.
UP	Number of static LSPs that are in the Up state.
DOWN	Number of static LSPs that are in the Down state.
Name	Name of an LSP.
FEC	Destination IP address and mask length of an LSP.
I/O Label	Incoming and outgoing labels.
I/O If	Incoming and outbound interfaces.
Status	Current status of an LSP: ● Up ● Down

Display detailed information about static LSPs.

```
<Huawei> display mpls static-lsp verbose
No             : 1
LSP-Name       : lsp1
LSR-Type       : Ingress
FEC            : 3.3.3.9/32
In-Label       : NULL
Out-Label      : 100
In-Interface   : -
Out-Interface  : GigabitEthernet1/0/0
NextHop        : 30.1.1.2
Static-Lsp Type: Normal
Lsp Status     : Up
```

 Copyright © Huawei Technologies Co., Ltd.

Table 11-40 Description of the display mpls static-lsp verbose command output

Item	Description
No	Serial number.
LSP-Name	Name of an LSP.
LSR-Type	Role of the current LSR on a static LSP: ● Ingress ● Transit ● Egress
FEC	Destination IP address and mask length of an LSP.
In-Label	Incoming label.
Out-Label	Outgoing label.
In-Interface	Inbound interface.
Out-Interface	Outbound interface.
NextHop	Next hop IP address.
Static-Lsp Type	Type of a static LSP.
Lsp Status	LSP status: ● Up ● Down

Related Topics

11.1.104 ping lsp

11.1.44 display ospf ldp-sync interface

Function

The **display ospf ldp-sync interface** command displays the status of LDP and OSPF synchronization on an interface.

Format

display ospf ldp-sync interface { **all** | *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays information about the synchronization status on all interfaces enabled with LDP and OSPF synchronization.	-

Parameter	Description	Value
interface-type interface-number	Displays information about the synchronization status on a specified interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

For all interfaces that are enabled with LDP and OSPF synchronization, run the **display ospf ldp-sync interface** command to view information about the status of LDP and OSPF synchronization.

Example

Display information about the status of LDP and OSPF synchronization on a specified interface.

```
<Huawei> display ospf ldp-sync interface gigabitethernet 1/0/0
 Interface GigabitEthernet1/0/0
 HoldDown Timer: 9          HoldMaxCost Timer: 50
 LDP State: Up              OSPF Sync State: Sync-Achieved
```

Table 11-41 Description of the display ospf ldp-sync interface command output

Item	Description
Interface	Interface connected to neighbors.
HoldDown Timer	Interval at which the interface waits to create an LDP session without creating the OSPF neighbor relationship. The default interval is 10 seconds.
HoldMaxCost Timer	Interval at which OSPF advertises the maximum metric in LSAs sent by the local device. The default interval is 10 seconds. **NOTE** If the value of this field is **infinite**, OSPF keeps advertising the maximum metric value in LSAs sent by the local device before the LDP session is reestablished.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
LDP State	Status of an LDP session: ● Up ● Down
OSPF Sync State	Status of LDP and OSPF synchronization: ● Sync-Achieved: The creation of an LDP session and establishment of the OSPF neighbor relationship are synchronized. ● HoldDown: The interface is waiting to create an LDP session without creating the OSPF neighbor relationship. ● HoldMaxCost: OSPF advertises the maximum metric in LSAs or LSPs sent by the local device. ● Init: the initial state.

Related Topics

11.1.99 ospf timer ldp-sync hold-down

11.1.100 ospf timer ldp-sync hold-max-cost

11.1.45 display snmp-agent trap feature-name ldp all

Function

The **display snmp-agent trap feature-name ldp all** command displays the status of all traps on the MPLS LDP module.

Format

display snmp-agent trap feature-name ldp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display snmp-agent trap feature-name ldp all** command to view the status of all traps on the LDP module. The status can be configured using the **snmp-agent trap enable feature-name ldp** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display all trap messages on the MPLS LDP module.

```
<Huawei> display snmp-agent trap feature-name ldp all
-------------------------------------------------------------------------------
Feature name: ldp
Trap number : 4
-------------------------------------------------------------------------------
Trap name              Default switch status     Current switch status
Session-Retry          off                       on
Session-PVL            off                       on
Session-Up-MIB           off                       on
Session-Down-MIB           off                       on
```

Table 11-42 Description of the display snmp-agent trap feature-name ldp all command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the MPLS LDP module: ● Session-Retry: An LDP session is reestablished. ● Session-PVL: PathVectorLimitMismatch event of an LDP session, which indicates that the maximal vector value in the received message is different from the one in the local setting. ● Session-Up-MIB: An LDP session goes Up through the MIB. ● Session-Down-MIB: An LDP session goes Down through the MIB.
Default switch status	Default status of the trap function: ● on: The trap function is enabled by default. ● off: The trap function is disabled by default.
Current switch status	Current status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

11.1.116 snmp-agent trap enable feature-name ldp

11.1.46 display snmp-agent trap feature-name mpls_lspm all

Function

The **display snmp-agent trap feature-name mpls_lspm all** command displays all trap messages on the MPLS LSPM module.

Format

display snmp-agent trap feature-name mpls_lspm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display snmp-agent trap feature-name mpls_lspm all** command to view the status of all traps on the MPLS LSPM module. The status can be configured using the **snmp-agent trap enable feature-name mpls_lspm** command.

Example

Display all trap messages on the MPLS LSPM module.

```
<Huawei> display snmp-agent trap feature-name mpls_lspm all
-----------------------------------------------------------------------------
Feature name: MPLS_LSPM
Trap number : 85
-----------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
mplsXCUp                       off                     off
mplsXCDown                     off                     off
hwMplsStaticLspUp              off                     off
hwMplsStaticLspDown            off                     off
hwMplsLdpVirtualTunnelUp       off                     off
hwMplsLdpVirtualTunnelDown     off                     off
hwMplsLspThresholdExceed       off                     off
hwMplsLspThresholdExceedClear  off                     off
hwMplsLspTotalCountExceed      off                     off
hwMplsLspTotalCountExceedClear off                     off
hwMplsDynamicLabelThresholdExceed
                               off                     off
hwMplsDynamicLabelThresholdExceedClear
                               off                     off
hwMplsDynamicLabelTotalCountExceed
                               off                     off
hwMplsDynamicLabelTotalCountExceedClear
                               off                     off
hwMplsResourceThresholdExceed  off                     off
hwMplsResourceThresholdExceedClear
                               off                     off
hwMplsResourceTotalCountExceed off                     off
hwMplsResourceTotalCountExceedClear
                               off                     off
mplsTunnelUp                   off                     off
mplsTunnelDown                 off                     off
hwMplsStaticCRLspUp            off                     off
hwMplsStaticCRLspDown          off                     off
mplsTunnelReoptimized          off                     off
```

```
mplsTunnelRerouted              off                    off
hwMplsTeFrrSwitch               off                    off
hwMplsTeFrrResume               off                    off
hwMplsTunnelHSBSwitch           off                    off
hwMplsTunnelHSBResume           off                    off
hwMplsTunnelOBSwitch            off                    off
hwMplsTunnelOBResume            off                    off
hwMplsTeFrrProtAval             off                    off
hwMplsTeFrrProtNotAval          off                    off
hwmplsTunnelChangeBW            off                    off
hwMplsOamLoss                   off                    off
hwMplsOamLossRecovery           off                    off
hwMplsOamAis                    off                    off
hwMplsOamAisRecovery            off                    off
hwMplsOamRdi                    off                    off
hwMplsOamRdiRecovery            off                    off
hwMplsOamMeg                    off                    off
hwMplsOamMegRecovery            off                    off
hwMplsOamMep                    off                    off
hwMplsOamMepRecovery            off                    off
hwMplsOamSF                     off                    off
hwMplsOamSFRecovery             off                    off
hwMplsOamPeriod                 off                    off
hwMplsOamPeriodRecovery         off                    off
hwMplsOamSDRecovery             off                    off
hwMplsOamLck                    off                    off
hwMplsOamLckRecovery            off                    off
hwMplsOamExcess                 off                    off
hwMplsOamExcessRecovery         off                    off
hwMplsOamMisMatch               off                    off
hwMplsOamMisMatchRecovery       off                    off
hwMplsOamMisMerge               off                    off
hwMplsOamMisMergeRecovery       off                    off
hwMplsOamUnknown                off                    off
hwMplsOamUnknownRecovery        off                    off
hwMplsOamBDI                    off                    off
hwMplsOamBDIRecovery            off                    off
hwMplsOamFail                   off                    off
hwMplsOamFailRecovery           off                    off
hwMplsTunnelPrimaryUp           off                    off
hwMplsTunnelPrimaryDown         off                    off
hwMplsTunnelHotstandbyUp        off                    off
hwMplsTunnelHotstandbyDown      off                    off
hwMplsTunnelOrdinaryUp          off                    off
hwMplsTunnelOrdinaryDown        off                    off
hwMplsTunnelBesteffortUp        off                    off
hwMplsTunnelBesteffortDown      off                    off
hwMplsTeAutoTunnelDownClear     off                    off
hwMplsTeAutoTunnelPrimaryDownClear
                                off                    off
hwMplsTunnelBBSwitch            off                    off
hwMplsTunnelBBResume            off                    off
hwMplsExtTunnelDown             off                    off
hwMplsExtTunnelDownClear        off                    off
hwMplsOamLocalLock              off                    off
hwMplsOamLocalLockRecovery      off                    off
hwMplsTunnelDelete              off                    off
hwMplsTunnelHotstandbySwitch    off                    off
hwMplsTunnelHotstandbyResume    off                    off
hwMplsTunnelBfdPathMismatch     off                    off
hwMplsTunnelBfdPathMismatchClear
                                off                    off
hwMplsTeLspBfdDown              off                    off
hwMplsTeLspBfdDownClear         off                    off
```

Table 11-43 Description of the **display snmp-agent trap feature-name mpls_lspm all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Name of a trap message of the MPLS LSPM module: ● mplsXCUp: Enables the trap of the event that an LSP goes Up. ● mplsXCDown: Enables the trap of the event that an LSP goes Down. ● hwMplsStaticLspUp: Enables the private trap of the event that a static LSP goes Up. ● hwMplsStaticLspDown: Enables the private trap of the event that a static LSP goes Down. ● hwMplsLdpVirtualTunnelUp: Enables the trap of the event that an LDP virtual tunnel goes Up. ● hwMplsLdpVirtualTunnelDown: Enables the trap of the event that an LDP virtual tunnel goes Down. ● hwMplsLspThresholdExceed: Enables the function to generate an alarm if the number of LSPs exceeds the alarm threshold. ● hwMplsLspThresholdExceedClear: Enables the function to clear an alarm if the number of LSPs falls below the alarm threshold. ● hwMplsLspTotalCountExceed: Enables the function to generate an alarm if the number of LSPs exceeds the maximum limit. ● hwMplsLspTotalCountExceedClear: Enables the function to clear an alarm if the number of LSPs falls below the maximum limit. ● hwMplsDynamicLabelThresholdExceed: Dynamic label usage reached the upper limit. ● hwMplsDynamicLabelThresholdExceedClear: Dynamic label usage reached the lower limit. ● hwMplsDynamicLabelTotalCountExceed: Dynamic label usage reached 100%. ● hwMplsDynamicLabelTotalCountExceedClear: Dynamic label usage fell to 95%. ● hwMplsResourceThresholdExceed: Enables the function to generate an alarm if the number of used MPLS resources exceeds the alarm threshold. ● hwMplsResourceThresholdExceedClear: Enables the function to clear an alarm if the number of used MPLS resources falls below the alarm threshold. ● hwMplsResourceTotalCountExceed: Enables the function to generate an alarm if the number of used MPLS resources exceeds the maximum limit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• hwMplsResourceTotalCountExceedClear: Enables the function to clear an alarm if the number of used MPLS resources falls below the maximum limit. • mplsTunnelUp: Enables the trap of the event that a tunnel goes Up. • mplsTunnelDown: Enables the trap of the event that a tunnel goes Down. • hwMplsStaticCRLspUp: Enables the private trap of the event that a static CR-LSP goes Up. • hwMplsStaticCRLspDown: Enables the private trap of the event that a static CR-LSP goes Down. • mplsTunnelReoptimized: Enables the trap of the tunnel reoptimization event. • mplsTunnelRerouted: Enables the trap of the tunnel reroute event. • hwMplsTeFrrSwitch: Enables the private trap of the event of TE FRR protection switching. • hwMplsTeFrrResume: Enables the private trap of the event of TE FRR fault recovery. • hwMplsTunnelHSBSwitch: Enables the private trap of the event that traffic switches from the primary CR-LSP to the hot-standby CR-LSP. • hwMplsTunnelHSBResume: Enables the private trap of the event that traffic switches from the hot-standby CR-LSP to the primary CR-LSP. • hwMplsTunnelOBSwitch: Enables the private trap of the event that traffic switches from the primary CR-LSP to the ordinary backup CR-LSP. • hwMplsTunnelOBResume: Enables the private trap of the event that traffic switches from the ordinary backup CR-LSP to the primary CR-LSP. • hwMplsTeFrrProtAval: Enables the trap of the TE FRR bypass tunnel binding event. • hwMplsTeFrrProtNotAval: Enables the trap of the TE FRR bypass tunnel unbinding event. • hwmplsTunnelChangeBW: Enables the private trap of the event that the tunnel bandwidth changes. • hwMplsOamLoss: Enables the trap of the event that the tunnel receives a loss of continuity (LOC) alarm. • hwMplsOamLossRecovery: Enables the trap of the event that the LOC alarm received by the tunnel is cleared.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• hwMplsOamAis: Enables the trap of the event that the tunnel receives an alarm indication signal (AIS) alarm. • hwMplsOamAisRecovery: Enables the trap of the event that the AIS alarm received by the tunnel is cleared. • hwMplsOamRdi: Enables the trap of the event that the tunnel receives a remote defect indication (RDI) alarm. • hwMplsOamRdiRecovery: Enables the trap of the event that the RDI alarm received by the tunnel is cleared. • hwMplsOamMeg: Enables the trap of the event that the tunnel receives an unexpected MEG alarm. • hwMplsOamMegRecovery: Enables the trap of the event that the unexpected MEG alarm received by the tunnel is cleared. • hwMplsOamMep: Enables the trap of the event that the tunnel receives an unexpected MEP alarm. • hwMplsOamMepRecovery: Enables the trap of the event that the unexpected MEP alarm received by the tunnel is cleared. • hwMplsOamSF: Enables the trap of the event that the tunnel receives a local signal deterioration threshold 2 alarm. • hwMplsOamSFRecovery: Enables the trap of the event that the local signal deterioration threshold 2 alarm received by the tunnel is cleared. • hwMplsOamPeriod: Enables the trap of the event that the tunnel receives an unexpected period alarm. • hwMplsOamPeriodRecovery: Enables the trap of the event that the unexpected period alarm received by the tunnel is cleared. • hwMplsOamSDRecovery: Enables the trap of the event that the local signal degrade threshold 1 alarm received by the tunnel is cleared. • hwMplsOamLck: Enables the trap of the event that the tunnel receives an LCK alarm. • hwMplsOamLckRecovery: Enables the trap of the event that the LCK alarm received by the tunnel is cleared. • hwMplsOamExcess: Enables the trap of the event that the tunnel receives an Excess alarm.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• hwMplsOamExcessRecovery: Enables the trap of the event that the Excess alarm received by the tunnel is cleared. • hwMplsOamMisMatch: Enables the trap of the event that the tunnel receives a MisMatch alarm. • hwMplsOamMisMatchRecovery: Enables the trap of the event that the MisMatch alarm received by the tunnel is cleared. • hwMplsOamMisMerge: Enables the trap of the event that the tunnel receives a MisMerge alarm. • hwMplsOamMisMergeRecovery: Enables the trap of the event that the MisMerge alarm received by the tunnel is cleared. • hwMplsOamUnknown: Enables the trap of the event that the tunnel receives an unknown alarm. • hwMplsOamUnknownRecovery: Enables the trap of the event that the unknown alarm received by the tunnel is cleared. • hwMplsOamBDI: Enables the trap of the event that the tunnel receives a backward defect indication (BDI) alarm. • hwMplsOamBDIRecovery: Enables the trap of the event that the BDI alarm received by the tunnel is cleared. • hwMplsOamFail: Enables the trap of the event that the tunnel receives an OAMFAIL alarm. • hwMplsOamFailRecovery: Enables the trap of the event that the OAMFAIL alarm received by the tunnel is cleared. • hwMplsTunnelPrimaryUp: Enables the trap of the event that the primary LSP of the tunnel changes to Up. • hwMplsTunnelPrimaryDown: Enables the trap of the event that the primary LSP of the tunnel changes to Down. • hwMplsTunnelHotstandbyUp: Enables the trap of the event that the hot-standby LSP of the tunnel changes to Up. • hwMplsTunnelHotstandbyDown: Enables the trap of the event that the hot-standby LSP of the tunnel changes to Down. • hwMplsTunnelOrdinaryUp: Enables the trap of the event that the ordinary LSP of the tunnel changes to Up.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• hwMplsTunnelOrdinaryDown: Enables the trap of the event that the ordinary LSP of the tunnel changes to Down. • hwMplsTunnelBesteffortUp: Enables the trap of the event that the best-effort LSP of the tunnel changes to Up. • hwMplsTunnelBesteffortDown: Enables the trap of the event that the best-effort LSP of the tunnel changes to Down. • hwMplsTeAutoTunnelDownClear: Enables the trap of the event that the TE Auto tunnel Down alarm was cleared. • hwMplsTeAutoTunnelPrimaryDownClear: Enables the trap of the event that the Down alarm about the primary LSP in the TE Auto tunnel was cleared. • hwMplsTunnelBBSwitch: enables the alarm for switchover from the primary LSP to the bypass LSP in common backup mode (BBK). • hwMplsTunnelBBResume: Enables the trap of main LSP of tunnel resumes from backup LSP in BBK. • hwMplsExtTunnelDown: Enables the trap of the event that the TE tunnel changes to Down. • hwMplsExtTunnelDownClear: Enables the trap of the event that the TE tunnel Down alarm was cleared. • hwMplsOamLocalLock: Enables the trap of the event that the tunnel receives a LOCK alarm. • hwMplsOamLocalLockRecovery: Enables the trap of the event that the LOCK alarm received by the tunnel is cleared. • hwMplsTunnelDelete: Enables the function to generate an alarm if an MPLS TE tunnel is deleted. • hwMplsTunnelHotstandbySwitch: • hwMplsTunnelHotstandbyResume: • hwMplsTunnelBfdPathMismatch: • hwMplsTunnelBfdPathMismatchClear: • hwMplsTeLspBfdDown: • hwMplsTeLspBfdDownClear:
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Current status of the trap function: ● on: The trap function is enabled. ● off: The trap function is disabled.

Related Topics

11.1.117 snmp-agent trap enable feature-name mpls_lspm

11.1.47 display static-route ldp-sync

Function

The **display static-route ldp-sync** command displays information about the outbound interface of a static route configured with synchronization between LDP and static routes.

Format

display static-route ldp-sync [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run the **display static-route ldp-sync** command to view synchronization between LDP and static routes to diagnose faults in static routes.

- If no outbound interface is specified, information about all outbound interfaces of the static routes configured with synchronization between LDP and static routes is displayed.
- If an outbound interface is specified, information about the specified outbound interface of the static routes configured with synchronization between LDP and static routes is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about the outbound interface of the static route configured with synchronization between LDP and static routes.

```
<Huawei> display static-route ldp-sync
Total number of routes enable Ldp-Sync: 2
-----------------------------------------------------
Interface GigabitEthernet0/0/1
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer: 20s
Sync state: Normal
Dest = 4.4.4.4, Mask = 32, NextHop = 10.1.1.1.
-----------------------------------------------------
Interface GigabitEthernet0/0/2
Enable ldp-sync static routes number: 1
Static-route ldp-sync holddown timer: 10s
Sync state: Normal
Dest = 4.4.4.4, Mask = 32, NextHop = 20.1.1.1.
-----------------------------------------------------
```

Table 11-44 Description of the display static-route ldp-sync command output

Item	Description
Total number of routes enable Ldp-Sync	Number of static routes configured with synchronization between LDP and static routes.
Interface GigabitEthernet0/0/1	Outbound interface of the static route configured with synchronization between LDP and static routes.
Enable ldp-sync static routes number	Number of static routes enabled with synchronization between LDP and static routes, with an outbound interface of GE1/0/0.
Static-route ldp-sync holddown timer	Time during which the static route remains inactive and waits for an LDP session to be established.
Sync state	Status of synchronization between LDP and static routes: ● Normal ● HoldDown
Dest	Destination address of the static route.
Mask	Mask length of the destination address of the static route.
NextHop	Next hop address of the static route.

Related Topics

9.1.3 ip route-static
9.1.6 ip route-static vpn-instance

11.1.122 static-route timer ldp-sync hold-down

11.1.48 fec-list

Function

The **fec-list** command creates a FEC list used in dynamic BFD for LDP LSP.

The **undo fec-list** command deletes a FEC list.

By default, no FEC list is created.

Format

fec-list *list-name*

undo fec-list *list-name*

Parameters

Parameter	Description	Value
list-name	Specifies the name of a FEC list.	The value is a string of 1 to 31 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a BFD session is established based on the FEC list, run the **fec-list** command to create a FEC list. Run the **fec-node** command to specify a host route to trigger the establishment of BFD sessions.

Only a single FEC list can be configured globally.

Example

Create FEC list 1.

```
<Huawei> system-view
[Huawei] fec-list 1
```

Related Topics

11.1.79 mpls bfd-trigger

11.1.49 fec-node

 Copyright © Huawei Technologies Co., Ltd.

11.1.49 fec-node

Function

The **fec-node** command adds a FEC node.

The **undo fec-node** command deletes a FEC node.

By default, no FEC node is created.

Format

fec-node *ip-address* [**nexthop** *ip-address* | **outgoing-interface** [*interface-type interface-number*]]*

undo fec-node *ip-address* [**nexthop** *ip-address* | **outgoing-interface** [*interface-type interface-number*]]*

Parameters

Parameter	Description	Value
ip-address	Specifies the FEC address.	The value is in dotted decimal notation.
nexthop *ip-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the outbound interface. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-

Views

FEC-list view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the establishment of BFD sessions is triggered in FEC list mode, the system sets up BFD sessions for the added FEC nodes.

Prerequisites

Before FEC nodes are added, a FEC list must be created.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create FEC nodes in the FEC list.

```
<Huawei> system-view
[Huawei] fec-list 1
[Huawei-fec-list-1] fec-node 2.2.2.2 nexthop 3.3.3.3 outgoing-interface gigabitethernet 1/0/0
```

Related Topics

11.1.48 fec-list

11.1.50 graceful-restart (MPLS-LDP view)

Function

The **graceful-restart** command enables LDP GR.

The **undo graceful-restart** command disables LDP GR.

By default, LDP GR is disabled.

Format

graceful-restart

undo graceful-restart

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LDP GR must be enabled on both the GR Restarter and Helper.

In LDP GR mode, when AMB/SMB switchover or protocol restart occurs on the neighboring device of the local device, the local device (GR helper) helps the device (restarter) to restart without interrupting packet forwarding.

If LDP GR is not enabled, during the AMB/SMB switchover or upgrade, the neighboring device deletes the LSP because the session is in the Down state. As a result, the traffic is interrupted in a short time. If LDP GR is enabled, the labels before and after unexpected AMB/SMB switchover or protocol restart can be consistent, and uninterrupted MPLS forwarding is ensured.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Currently, LDP supports only GR helper.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp(system view)** command in the system view.

Precautions

Enabling or disabling GR causes the reestablishment of all LDP sessions.

Example

Enable LDP GR.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Related Topics

11.1.82 mpls ldp (system view)
11.1.51 graceful-restart timer neighbor-liveness
11.1.53 graceful-restart timer recovery
11.1.38 display mpls ldp session
11.1.35 display mpls ldp peer

11.1.51 graceful-restart timer neighbor-liveness

Function

The **graceful-restart timer neighbor-liveness** command sets the value of the Neighbor-liveness timer.

The **undo graceful-restart timer neighbor-liveness** command restores the default setting.

By default, the value of the Neighbor-liveness timer is 600 seconds.

Format

graceful-restart timer neighbor-liveness *time*

undo graceful-restart timer neighbor-liveness

Parameters

Parameter	Description	Value
time	Specifies the value of the Neighbor-liveness timer.	The value is an integer ranging from 3 to 3600, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The value of the neighbor-liveness timer defines the LDP GR period.

During LDP GR, the reestablishment time of the LDP session is negotiated as the smaller value between the value of the neighbor-liveness timer on the GR helper and the value of the Reconnect timer on the GR restarter.

In general, the default value of the timer is recommended. When the number of LSPs on a network is small, you can set a smaller value for the neighbor-liveness timer to shorten the GR period.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the neighbor-liveness timer causes the reestablishment of all the LDP sessions.

Example

Set the value of the Neighbor-liveness timer to 500 seconds.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[Huawei-mpls-ldp] graceful-restart timer neighbor-liveness 500
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Related Topics

11.1.50 graceful-restart (MPLS-LDP view)

11.1.53 graceful-restart timer recovery

11.1.52 graceful-restart timer reconnect

Function

The **graceful-restart timer reconnect** command sets the value of the Reconnect timer of an LDP session.

The **undo graceful-restart timer reconnect** command restores the default setting.

 Copyright © Huawei Technologies Co., Ltd.

By default, the Reconnect timer is set to 300 seconds.

NOTE

Only the AR3260 supports this command.

Format

graceful-restart timer reconnect *time*

undo graceful-restart timer reconnect

Parameters

Parameter	Description	Value
time	Specifies the value of a Reconnect timer of an LDP session.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the GR restarter performs the active/standby switchover, the GR helper detects that the LDP session with the GR restarter fails, and then starts the Reconnect timer and waits for the reestablishment of the LDP session.

- If no LDP session between the GR helper and the GR restarter has been established after the Reconnect timer times out, the GR helper immediately deletes the MPLS forwarding entries associated with the GR restarter and exits from the GR help process.
- If the LDP session between the GR helper and the GR restarter is established before the Reconnect timer times out, the GR helper deletes the timer and starts the Recovery timer.

During LDP GR, when the reestablishment time of the LDP session is negotiated, the value of the Reconnect timer that actually takes effect on the local end is the smaller value between the value of the neighbor-liveness timer on the GR helper and the value of the Reconnect timer on the GR restarter.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Changing the value of the Reconnect timer causes the reestablishment of all the LDP sessions.

Example

Set the time of the Reconnect timer of an LDP session to 270 seconds.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[Huawei-mpls-ldp] graceful-restart timer reconnect 270
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Related Topics

11.1.50 graceful-restart (MPLS-LDP view)

11.1.51 graceful-restart timer neighbor-liveness

11.1.53 graceful-restart timer recovery

11.1.53 graceful-restart timer recovery

Function

The **graceful-restart timer recovery** command sets the value of the LSP Recovery timer.

The **undo graceful-restart timer recovery** command restores the default setting.

By default, the LSP Recovery timer is set to 300 seconds.

Format

graceful-restart timer recovery *time*

undo graceful-restart timer recovery

Parameters

Parameter	Description	Value
time	Specifies the value of an LSP Recovery timer.	The value is an integer ranging from 3 to 3600, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the LDP session is reestablished, the GR helper starts the Recovery timer and waits for the recovery of the LSP.

- If the Recovery timer times out, the GR helper considers that the GR process is complete on the GR restarter and deletes the unrecovered LSPs.
- If all the LSPs recover before the Recovery timer times out, the GR helper considers that the GR process is complete on the GR restarter only after the Recovery timer times out.

When a network with a large number of routes is faulty, run the **graceful-restart timer recovery** command to increase the value of the Recovery timer to ensure that all the LSPs recover within the timeout period of the timer.

During the LDP GR process, the value of the LSP Recovery timer that actually takes effect on the local end is negotiated as the smaller one of the values of the LSP Recovery timers configured on both ends of an LDP session.

Prerequisites

MPLS and MPLS LDP have been enabled globally.

LDP GR has been enabled globally.

Precautions

Changing the value of the LSP Recovery timer causes the reestablishment of all the LDP sessions.

Example

Set the value of the LSP Recovery timer to 330 seconds.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] graceful-restart
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
[Huawei-mpls-ldp] graceful-restart timer recovery 330
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Related Topics

11.1.50 graceful-restart (MPLS-LDP view)
11.1.52 graceful-restart timer reconnect

11.1.54 gtsm peer valid-ttl-hops

Function

The **gtsm peer valid-ttl-hops** command configures the generalized TTL security mechanism (GTSM) on a specified LDP peer.

The **undo gtsm** command deletes the GTSM on all LDP peers or a specified LDP peer.

By default, no LDP peer is configured with the GTSM.

Format

gtsm peer *ip-address* **valid-ttl-hops** *hops*

undo gtsm { **all** | **peer** *ip-address* }

Parameters

Parameter	Description	Value
peer *ip-address*	Specifies the transport address of an LDP peer.	The value is in dotted decimal notation.
valid-ttl-hops *hops*	Specifies the maximum number of valid hops permitted by the GTSM.	The value is an integer ranging from 1 to 255.
all	Indicates all LDP peers.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The GTSM checks TTL values to verify packets and protect devices against attacks. LDP peers are configured with the GTSM and a valid TTL range to check TTLs in LDP packets exchanged between them. If the TTL in an LDP packet is out of the valid range, this LDP packet is considered invalid and discarded. The GTSM defends against CPU-based attacks initiated using a large number of forged packets and protects upper-layer protocols.

If the value of *hops* is set to the maximum number of valid hops permitted by GTSM, when the TTL values carried in the packets sent by an LDP peer are within the range [255 - Number of hops +1, 255], the packets are received; otherwise, the packets are discarded.

NOTE

Configuring the GTSM on both ends of an LDP session is recommended.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

The valid TTL range is from 1 to 255 or from 1 to 64, depending on the specific vendor. If a Huawei device is connected to a non-Huawei device, set *hops* to a value in a valid range that both devices support; otherwise, the Huawei device will discard packets sent by the non-Huawei device, resulting in LDP session interruption.

 Copyright © Huawei Technologies Co., Ltd.

Example

On the LSR, set valid TTL values carried in LDP packets sent by the peer with transport address 2.2.2.9 to 254 and 255.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] gtsm peer 2.2.2.9 valid-ttl-hops 2
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.55 inbound peer fec

Function

The **inbound peer fec** command configures an inbound policy, which allows the LSR to receive Label Mapping messages for IGP routes only from a specified peer.

The **undo inbound peer fec** command restores the default setting.

By default, no inbound policy is configured.

Format

inbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec** { **none** | **host** | **ip-prefix** *prefix-name* }

undo inbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec**

Parameters

Parameter	Description	Value
peer-id	Specifies the ID of an LDP peer.	The value is in dotted decimal notation.
peer-group *peer-group-name*	Specifies the name of a peer group.	The value is an existing peer group name.
all	Indicates all LDP peers.	-
none	Forbids all Label Mapping messages. After the parameter **none** is configured, the specified LSR does not receive Label Mapping messages for IGP routes from its peers.	-
host	Allows only Label Mapping messages for host routes. After the parameter **host** is configured, the specified LSR receives only Label Mapping messages for host routes from its peers.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip-prefix *prefix-name*	Allows only Label Mapping messages for IGP routes that are defined in the IP prefix list. After the parameter **ip-prefix** is configured, the specified LSR receives Label Mapping messages only for IGP routes that are defined in the IP prefix list by its peers.	The value is an existing IP prefix list name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an LSR receives Label Mapping messages from all LDP peers to speed up LDP LSP convergence. This leads to establishment of a great number of unwanted LSPs, which wastes resources. To reduce the number of LSPs and save memory resources, configure an outbound or inbound policy to filter out LDP LSPs not matching the policy.

When running the **inbound peer fec** command to specify the peer ID and FEC of the IGP route, configure the peer to receive only Label Mapping messages for specified IGP routes.

To apply a policy associated with the same FEC range to an LDP peer group or all LDP peers receiving Label Mapping messages, configure either **peer-group** *peer-group-name* or **all** in the command.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

If multiple inbound policies are configured for a specified LDP peer, the earliest configuration takes effect. For example, the following two inbound policies are configured:

```
inbound peer 2.2.2.2 fec host
inbound peer peer-group group1 fec none
```

As group1 also contains an LDP peer with *peer-id* of 2.2.2.2, the following inbound policy takes effect:

```
inbound peer 2.2.2.2 fec host
```

If two inbound policies are configured in sequence and the **peer** parameters in the two commands are the same, the second command overrides the first one. For example, the following two outbound policies are configured:

```
inbound peer 2.2.2.2 fec host
inbound peer 2.2.2.2 fec none
```

 Copyright © Huawei Technologies Co., Ltd.

The second configuration overrides the first one. This means that the following inbound policy takes effect on the LDP peer with *peer-id* of 2.2.2.2:

```
inbound peer 2.2.2.2 fec none
```

Creating a peer group before it is referenced is recommended. By default, nonexistent peer groups cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is referenced using the current command, the current command applies to all LDP peers.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device receives Label Mapping messages of all LDP FECs from the specified peer.

Example

Configure all LSRs to receive Label Mapping messages only for host routes from peers.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] inbound peer all fec host
```

Related Topics

11.1.102 outbound peer fec

11.1.101 outbound peer bgp-label-route

11.1.103 outbound peer split-horizon

11.1.56 isis ldp-sync

Function

The **isis ldp-sync** command enables synchronization between LDP and IS-IS on an interface.

The **undo isis ldp-sync** command disables synchronization between LDP and IS-IS on an interface.

By default, synchronization between LDP and IS-IS is disabled on an interface.

Format

isis ldp-sync

undo isis ldp-sync

Parameters

None

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LDP convergence speed depends on the convergence speed of IS-IS routes. To enable MPLS LDP on a network with the primary and backup links, the following problems may occur:

- Upon a fault on the primary link, IS-IS routes and ISP are both switched to the backup link using LDP FRR. When the primary link recovers, IS-IS routes are switched back to the primary link earlier than LDP traffic because IGP route convergence is faster than LDP convergence. As a result, LSP traffic is lost.
- If a fault occurs on the LDP session between nodes on the primary link where the IS-IS routes are working properly, the IS-IS routes still use the primary link and the LSP on the primary link is deleted. No IS-IS route exists on the backup link; therefore, no LSP can be established on the backup link. LSP traffic is lost.

Run the **isis ldp-sync** command to enable synchronization between LDP and IS-IS to prevent traffic loss in the preceding problems. Run this command on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

All interfaces excluding the loopback interface, null0 interface, and Layer 2 Ethernet interface support this command.

Example

Enable synchronization between LDP and IS-IS on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis ldp-sync
```

Related Topics

9.6.56 isis

9.6.68 isis enable

11.1.58 isis timer ldp-sync hold-down

11.1.59 isis timer ldp-sync hold-max-cost

 Copyright © Huawei Technologies Co., Ltd.

11.1.57 isis ldp-sync block

Function

The **isis ldp-sync block** command blocks synchronization between LDP and IS-IS on an interface.

The **undo isis ldp-sync block** command restores the default setting.

By default, synchronization between LDP and IS-IS is not blocked on an interface.

Format

isis ldp-sync block

undo isis ldp-sync block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ldp-sync enable** command is run in an IGP process, Synchronization between LDP and IGP is enabled on the interfaces on which the neighbor status is Up. If the interfaces on a device carrying key services, ensure that the backup path does not pass through this device. In addition, you can block synchronization between LDP and IGP on a specified interface of the router.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

The **isis ldp-sync block** command can be run on all interfaces, except loopback, NULL0, and Layer 2 Ethernet interfaces.

Example

Block synchronization between LDP and IS-IS on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis ldp-sync block
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

9.6.56 isis

9.6.68 isis enable

11.1.59 isis timer ldp-sync hold-max-cost

11.1.58 isis timer ldp-sync hold-down

Function

The **isis timer ldp-sync hold-down** command sets the interval during which an interface waits for creating an LDP session before setting up the IS-IS neighbor relationship.

The **undo isis timer ldp-sync hold-down** command restores the default setting.

By default, the interval is 10 seconds.

Format

isis timer ldp-sync hold-down *value*

undo isis timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the interval during which an interface waits for creating an LDP session before setting up the IS-IS neighbor relationship.	The value is an integer ranging from 0 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the physical link with LDP and IS-IS synchronization enabled recovers, IS-IS enters the Hold-down state and starts the Hold-down timer to wait for the establishment of an LDP session. LDP and IS-IS are both switched back to the backup link.

Run the **isis timer ldp-sync hold-down** command to set the value of the Hold-down timer.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

All interfaces excluding the loopback interface, null0 interface, and Layer 2 Ethernet interface support this command.

Example

Set the value of the Hold-down timer for GE1/0/0 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the IS-IS neighbor relationship.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis timer ldp-sync hold-down 15
```

Related Topics

11.1.56 isis ldp-sync

11.1.14 display isis ldp-sync interface

11.1.59 isis timer ldp-sync hold-max-cost

Function

The **isis timer ldp-sync hold-max-cost** command sets the interval during which IS-IS sends LSPs to advertise the maximum metric on the local device.

The **undo isis timer ldp-sync hold-max-cost** command restores the default setting.

By default, the interval is 10 seconds.

Format

isis timer ldp-sync hold-max-cost { *value* | **infinite** }

undo isis timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
value	Specifies the interval during which IS-IS sends LSPs to advertise the maximum metric on the local device.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that IS-IS keeps advertising the maximum metric in LSPs on the local device before an LDP session is reestablished.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the primary LSP recovers from a fault, run the **isis timer ldp-sync hold-max-cost** command to set the interval during which traffic is still transmitted along the backup LSP before the LDP session of the primary LSP is reestablished.

Select the parameters based on network requirements.

- If IS-IS carries only LDP services, configure the parameter **infinite** to ensure that the selected IS-IS routes are always the same as the LDP LSPs.
- If IS-IS carries multiple types of services including LDP services, set the parameter *value* to ensure that the teardown of LDP sessions does not affect IS-IS route selection or other services.

Prerequisites

The IS-IS process has been started using the **isis enable** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

The **isis ldp-sync** command can be run on all interfaces, except for loopback, NULL0 and Layer 2 Ethernet interfaces.

Example

Set the interval to 8 seconds, during which IS-IS sends LSPs to advertise the maximum metric on the local device.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] isis enable 1
[Huawei-GigabitEthernet1/0/0] isis timer ldp-sync hold-max-cost 8
```

Related Topics

11.1.56 isis ldp-sync

11.1.14 display isis ldp-sync interface

11.1.60 label advertise

Function

The **label advertise** command enables the egress node to advertise labels of a specified type to the penultimate hop.

 Copyright © Huawei Technologies Co., Ltd.

The **undo label advertise** command restores the default setting.

By default, the egress node assigns implicit null labels to the penultimate hop.

Format

label advertise { **explicit-null** | **implicit-null** | **non-null** }

undo label advertise

Parameters

Parameter	Description	Value
explicit-null	Disables Penultimate Hop Popping (PHP) and enables the egress node to assign explicit null labels to the penultimate hop.	The value of the explicit null label is 0.
implicit-null	Enables PHP and enables the egress node to assign implicit null labels to the penultimate hop.	The value of the implicit null label is 3.
non-null	Disables PHP and enable the egress node to assign normal labels to the penultimate hop.	The value is equal to or greater than 16.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **label advertise** command to configure the type of labels assigned to the penultimate hop on the egress node. The default configuration **implicit-null** is recommended. The setting eases the forwarding burden on the egress node, improving the forwarding efficiency.

You can choose a type as required.

- **implicit-null** supports PHP, which allows the LSR at the penultimate hop to pop out the label from an MPLS packet and send the packet to the egress node. After receiving the packet, the egress node directly forwards the unlabeled IP packet or the single-labeled packet. PHP helps reduce the burden on the egress node.
- **non-null** and **explicit-null** do not support PHP. The setting is resource consuming and is therefore not recommended.

  explicit-null supports MPLS QoS.

 Copyright © Huawei Technologies Co., Ltd.

For LDP LSPs, run the **reset mpls ldp** command in the user view on the local LSR to validate the modification.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command in the system view.

Precautions

The **label advertise** command takes effect only after the following requirements are met:

- A master/slave MPU switchover is performed.
- Users perform the following operations:
  - Run the **reset mpls ldp** command to restart the LDP instance of the public network.
  - Change the policy for triggering LDP LSP establishment and increase the route range used to trigger the LSP establishment.
    - Change the policy for triggering LDP LSP establishment from **none** to **all**. The policy can trigger the establishment of all LDP LSPs.
    - Change the policy for triggering LDP LSP establishment from **host** to **all**. The policy can trigger the establishment of LDP LSPs using all routes except for host routes.

Example

Configure the egress node to assign explicit null labels to the penultimate hop.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] label advertise explicit-null
```

Related Topics

11.1.111 reset mpls ldp

11.1.61 label distribution control-mode

Function

The **label distribution control-mode** command configures an LDP label distribution control mode.

The **undo label-type** command restores the default LDP label distribution control mode.

The default LDP label distribution control mode is ordered.

Format

label distribution control-mode { **independent** | **ordered** }

undo label distribution control-mode

Parameters

Parameter	Description	Value
ordered	Sets the LDP label distribution control mode to ordered.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the LDP label distribution control mode is ordered. In the ordered mode, an LSR advertises the mapping between a label and an FEC to its upstream LSR only when this LSR is the outgoing node of the FEC or receives the Label Mapping message of the next hop for the FEC. If you want to quickly deploy services, you can set the LDP label distribution control mode to independent. In the independent mode, a local LSR can distribute a label bound to an FEC and then inform the upstream LSR, without waiting for the label distributed by the downstream LSR.

However, in the independent mode, an LSP cannot be established if the local LSR does not receive the label for the FEC distributed by the downstream LSR. The ingress node cannot detect an LSP establishment failure and keeps on forwarding service packets. When service packets reach the LSR, the LSR fails to forward the packets to its downstream LSR, causing service interruption. For example, services cannot be switched from the primary LSP to the backup LSP, resulting in service interruption.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Example

Set the LDP label distribution control mode to independent.

```
<Huawei> system-view
[Huawei] mpls
[Huawei] mpls ldp
[Huawei-mpls-ldp] label distribution control-mode independent
```

11.1.62 label-withdraw-delay

Function

The **label-withdraw-delay** command enables a node to delay sending Label Withdraw messages.

 Copyright © Huawei Technologies Co., Ltd.

The **undo label-withdraw-delay** command disables a node from delaying sending Label Withdraw messages.

By default, the label withdraw delay function is disabled.

Format

label-withdraw-delay

undo label-withdraw-delay

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The label withdraw delay function prevents downstream LSP flapping from spreading to upstream nodes. For example, an LSP on a local node flaps because an LDP session between the node and its downstream peer flaps, a route flaps, or an LDP policy is modified. The local node repeatedly sends Label Withdraw and Label Mapping messages in sequence to upstream nodes. This causes the upstream nodes to repeatedly tear down and reestablish LSPs. As a result, the entire LDP LSP flaps. The label withdraw delay function can be enabled on each node of the LDP LSP to suppress the spread of LSP flapping.

Follow-up Procedure

Use the default delay time of 5s or run the **label-withdraw-delay timer** command to set the delay time.

Example

Enable the label withdraw delay function.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] label-withdraw-delay
```

11.1.63 label-withdraw-delay timer

Function

The **label-withdraw-delay timer** command sets the delay time before a node sends a Label Withdraw message.

 Copyright © Huawei Technologies Co., Ltd.

The **undo label-withdraw-delay timer** command restores the default delay time.

The default delay time is 5 seconds.

Format

label-withdraw-delay timer *time*

undo label-withdraw-delay timer

Parameters

Parameter	Description	Value
time	Specifies the delay time before a Label Withdraw message can be sent.	The value is an integer ranging from 1 to 65535, in seconds.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The label withdraw delay function prevents downstream LSP flapping from spreading to upstream nodes. For example, an LSP on a local node flaps because an LDP session between the node and its downstream peer flaps, a route flaps, or an LDP policy is modified. The local node repeatedly sends Label Withdraw and Label Mapping messages in sequence to upstream nodes. This causes the upstream nodes to repeatedly tear down and reestablish LSPs. As a result, the entire LDP LSP flaps. To suppress the spread of LSP flapping, run the **label-withdraw-delay** command to enable the label withdraw delay function on each node and the **label-withdraw-delay timer** command to set the delay time before a node sends a Label Withdraw message to its upstream node.

Prerequisites

The label withdraw delay function has been enabled using the **label-withdraw-delay** command.

Example

Enable the label withdraw delay function on the node and set the delay time to 10s.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] label-withdraw-delay
[Huawei-mpls-ldp] label-withdraw-delay timer 10
```

 Copyright © Huawei Technologies Co., Ltd.

11.1.64 ldp-sync enable

Function

The **ldp-sync enable** command enables synchronization between LDP and IS-IS on all interfaces in an IS-IS process.

The **undo ldp-sync enable** command disables synchronization between LDP and IS-IS on all interfaces in an IS-IS process.

By default, synchronization between LDP and IS-IS is disabled on all interfaces in an IS-IS process.

Format

ldp-sync enable [**mpls-binding-only**]

undo ldp-sync enable

Parameters

Parameter	Description	Value
mpls-binding-only	Synchronization between LDP and IS-IS can only be enabled on MPLS LDP-enabled interfaces.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Synchronization between LDP and IGP reduces LSP traffic loss on a network with both primary and backup LSPs. Traffic loss occurs in either of the following situations:

- The primary LSP works properly and an LDP session between two nodes on the primary LSP fails. IGP guides traffic still through the primary LSP even though a primary/backup LSP switchover is performed.
- If a link on the primary LSP or the primary LSP recovers, IGP routes converge. IGP routes associated with the primary LSP become reachable earlier than the primary LSP because IGP routes converge faster than LDP routes. IGP routes guide traffic through the primary LSP before the primary LSP recovers.

Synchronization between LDP and IGP delays IGP route advertisement so that the LDP session and IGP route can converge simultaneously.

The **ldp-sync enable** command run in the IS-IS view can enable synchronization between LDP and IS-IS on all interfaces within a specified IS-IS process.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **isis ldp-sync block** command to disable synchronization between LDP and IGP on desired IS-IS interfaces.

Precautions

Although the **undo ldp-sync enable** command has been run, synchronization between LDP and IS-IS configured using the **isis ldp-sync** command still takes effect on an IS-IS interface.

Example

Enable synchronization between LDP and IS-IS on all interfaces in an IS-IS instance.

```
<Huawei> system-view
[Huawei] isis 100
[Huawei-isis-100] ldp-sync enable
```

11.1.65 longest-match

Function

The **longest-match** command configures inter-domain LDP extension capability and enable LDP to search for routes to establish LSPs based on the longest match rule.

The **undo longest-match** command restores the default setting.

By default, LDP searches for routes to establish LSPs based on the exact matching rule.

Format

longest-match

undo longest-match

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large network, multiple IGP areas need to be configured for flexible network deployment and fast route convergence. In this situation, when advertising routes

 Copyright © Huawei Technologies Co., Ltd.

between IGP areas, to prevent a large number of routes from consuming too many resources, an Area Border Router (ABR) needs to aggregate the routes in an area and then advertise the aggregated route to neighbor IGP areas. By default, when establishing LSPs, LDP searches the routing table for the route that exactly matches the forwarding equivalence class (FEC) carried in the received Label Mapping message. For aggregated routes, only liberal LDP LSPs, not inter-area LDP LSPs, can be set up.

In this case, run the **longest-match** command to enable LDP to search for routes or establishing inter-area LDP LSPs based on the longest match rule.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

Configuring this command is not allowed during LDP GR.

Example

Enable LDP to search for routes for establishing LDP LSPs based on the longest match rule.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] longest-match
```

11.1.66 lsp-trigger bgp-label-route

Function

The **lsp-trigger bgp-label-route** command enables LDP to allocate labels to labeled BGP routes on the public network.

The **undo lsp-trigger bgp-label-route** command restores the default setting.

By default, LDP does not allocate labels to labeled BGP routes on the public network.

NOTE

The AR100&AR120&AR150&AR160&AR200 does not support this command.

Format

lsp-trigger bgp-label-route [**ip-prefix** *ip-prefix-name*]

undo lsp-trigger bgp-label-route

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the labeled BGP routes on the public network to set up LDP LSPs.	The value is an existing IP prefix list name.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Both the **lsp-trigger bgp-label-route** command and the **lsp-trigger** command can be used to configure policies to trigger the establishment of LDP LSPs. The former command is used for labeled BGP routes on the public network, and the latter command is used for static routes and IGP routes.

NOTE

Modifying the LSP-triggering policy during the LDP GR period is invalid.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all public-network labeled BGP routes trigger LDP LSP establishment.

Example

Trigger the establishment of LDP LSPs according to labeled BGP routes on the public network.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] lsp-trigger bgp-label-route
```

Related Topics

11.1.67 lsp-trigger

11.1.67 lsp-trigger

Function

The **lsp-trigger** command sets a policy for establishing LDP LSPs.

The **undo lsp-trigger** command restores the default setting.

By default, LDP uses IP host routes with 32-bit addresses to establish LSPs.

Format

lsp-trigger { **all** | **host** | **ip-prefix** *ip-prefix-name* | **none** }

undo lsp-trigger

Parameters

Parameter	Description	Value
all	Indicates that all static and IGP routes trigger the establishment of LSPs.	-
host	Indicates that IP host routes with 32-bit addresses trigger the establishment of LSPs.	-
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the establishment of LSPs.	The value is an existing IP prefix list name.
none	Indicates that the establishment of an LSP is not triggered.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MPLS LDP is enabled, LSPs are automatically established. If no policy is configured, an increasing number of LSPs are established, wasting resources.

The **lsp-trigger** command configures a policy to allow LDP to use specified routes to establish LSPs. This setting prevents unwanted LSPs from being established and helps reduce resource wastes.

The **lsp-trigger** command and the **lsp-trigger bgp-label-route** command are used to configure policies for triggering the LDP LSP establishment. The former command is used for static and IGP routes; the latter command is used for labeled public BGP routes.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The **lsp-trigger all** command is not recommended. If this command is run, LDP uses all IGP routes to establish LSPs, causing a large number of unwanted LSPs to be established and wasting system resources. Before using this command, configure a policy for filtering out routes unnecessary for the LSP establishment. The policy helps reduce the number of LSPs to be established and save system resources.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

- Modifying the LSP-triggering policy during the LDP GR period is invalid.
- The **lsp-trigger** command can be used to configure policies only for ingress and egress LSPs on the public network and ingress and egress LSPs on the private network that are established using IGP routes. To configure a policy for triggering the transit LSP establishment, run the **propagate mapping** command.
- The **lsp-trigger host** command can be run on either of the following nodes to provide a specific function:
  - Ingress: This command enables the ingress to use all routes with a 32-bit mask to establish LDP LSPs.
  - Egress: This command enables the egress to use local routes with a 32-bit mask to establish LDP LSPs.

  The **lsp-trigger** { **all** | **ip-prefix** *ip-prefix-name* } command can be used to establish proxy egress LSPs. The **lsp-trigger host** command, however, cannot be used to establish proxy egress LSPs.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all static and IGP routes trigger LDP LSP establishment.

Example

Trigger the establishment of LSPs based on all static and IGP routes.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] lsp-trigger all
```

Related Topics

11.1.105 propagate mapping

11.1.66 lsp-trigger bgp-label-route

11.1.68 lspv mpls-lsp-ping echo enable

Function

The **lspv mpls-lsp-ping echo enable** command enables a device to respond to MPLS Echo Request packets.

The **undo lspv mpls-lsp-ping echo enable** command disables a device from responding to MPLS Echo Request packets.

By default, a device is enabled to respond to MPLS Echo Request packets.

Format

lspv mpls-lsp-ping echo enable

undo lspv mpls-lsp-ping echo enable

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ping and trace tests use ICMP packets to locate faulty nodes on a forwarding path. When an LSP fails, IP forwarding-based ICMP packets cannot be used to detect the faulty node.

In this case, the **ping lsp** and **tracert lsp** command can be used to locate the faulty node on the LSP. These commands use MPLS Echo Request and MPLS Echo Reply packets to detect the connectivity of an LSP. Both MPLS Echo Request and MPLS Echo Reply packets are encapsulated into UDP packets and transmitted through port 3503. The receiver distinguishes MPLS Echo Request and MPLS Echo Reply packets based on the port number. An MPLS Echo Request packet carries FEC information to be detected, and is sent along the same LSP as other packets with the same FEC information. In this manner, the connectivity of the LSP is checked. MPLS Echo Request packets are transmitted to the destination through MPLS, whereas MPLS Echo Reply packets are transmitted to the source through IP.

For network security or management, you can run the **lspv mpls-lsp-ping echo enable** command to enable a device to respond to MPLS Echo Request packets or run the **undo lspv mpls-lsp-ping echo enable** command to disable the device from responding to MPLS Echo Request packets. This function is implemented by enabling or disabling port 3503. By default, port 3503 is enabled.

After you run the **ping lsp** and **tracert lsp** command to detect the connectivity of an LSP, it is recommended that you run the **undo lspv mpls-lsp-ping echo enable** command to disable the device from responding to MPLS Echo Request packets to avoid occupation of system resources.

Precautions

If you run the **undo lspv mpls-lsp-ping echo enable** command to disable a device from responding to MPLS Echo Request packets, this device does not

 Copyright © Huawei Technologies Co., Ltd.

respond to the **ping lsp** and **tracert lsp** command. As a result, the ping or trace test with the address of the device as the destination address times out.

Example

Disable a device to respond to MPLS Echo Request packets.

```
<Huawei> system-view
[Huawei] undo lspv mpls-lsp-ping echo enable
```

11.1.69 lspv packet-filter

Function

The **lspv packet-filter** command enables the filtering of MPLS Echo Request packets based on source addresses. Filtering rules are defined in ACL configurations.

The **undo lspv packet-filter** command disables the filtering of MPLS Echo Request packets based on source addresses.

By default, the filtering of MPLS Echo Request packets based on source addresses is disabled.

Format

lspv packet-filter *acl-number*

undo lspv packet-filter

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The ACL number is a decimal integer that ranges from 2000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The **lspv packet-filter** command often runs on the destination device of the LSPV check. In the case that the filtering of MPLS Echo Request packets based on source addresses is enabled, upon receiving MPLS Echo Request packets, the device matches the source addresses of the packets with a specified ACL. The packets permitted by the ACL are processed; those denied by the ACL are discarded.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the filtering of the MPLS Echo Request packets based on source addresses based on ACL 2100.

```
<Huawei> system-view
[Huawei] lspv packet-filter 2100
```

11.1.70 lsr-id

Function

The **lsr-id** command sets the LSR ID of an LDP instance.

The **undo lsr-id** command restores the default setting.

By default, the LSR ID of an LDP instance is the LSR ID of the LSR where the LDP instance is configured

Format

lsr-id *lsr-id*

undo lsr-id

Parameters

Parameter	Description	Value
lsr-id	Specifies the LSR ID of an LDP instance.	The value is in dotted decimal notation.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the LSR ID of an LDP instance is the same as the MPLS LSR ID configured using the **mpls lsr-id** command. On some networks such as the BGP/MPLS VPNs to which VPN instances apply, if the VPN address space and the public network address space overlap, configure LSR IDs for LDP instances to ensure the correct establishment of TCP connections.

Prerequisites

- MPLS has been enabled globally using the **mpls (system view)** command.
- MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Modifying or deleting the LSR ID of an LDP instance causes the reestablishment of all sessions in the LDP instance.

Example

Set the LSR ID of an LDP instance to 2.2.2.3.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls ldp
[Huawei-mpls-ldp] lsr-id 2.2.2.3
Warning: All the related sessions will be deleted if the operation is performed! Continue? (y/n)y
```

Related Topics

11.1.92 mpls lsr-id

11.1.71 maintain-session received-error-message

Function

The **maintain-session received-error-message** command disables LDP from tearing down a session after error packets are received.

The **undo maintain-session received-error-message** command restores the default configuration.

By default, LDP tears down a session after error packets are received.

Format

maintain-session received-error-message

undo maintain-session received-error-message

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

LDP should tear down a session after error TCP packets are received. This processing mode causes the LDP session to frequently flap and L2VPN services carried on the LDP session to be frequently interrupted. To disable LDP from tearing down a session after error packets are received, run the **maintain-session**

received-error-message command. LDP then ignores error packets and keeps the session connected. This is beneficial to service maintenance and can also be used for LDP fault recovery.

Example

Disable LDP from tearing down a session after error packets are received.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] maintain-session received-error-message
```

11.1.72 md5-password

Function

The **md5-password** command sets the password that is used by a TCP connection during the creation of an LDP session.

The **undo md5-password** command disables MD5 authentication.

By default, MD5 authentication is disabled during the creation of an LDP session.

Format

md5-password { **plain** | **cipher** } *peer-lsr-id password*

undo md5-password [**plain** | **cipher**] *peer-lsr-id*

Parameters

Parameter	Description	Value
plain	Displays the password in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. In this case, users at a lower level can easily obtain the password by viewing the configuration file. This brings security risks. Therefore, it is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Displays the password in cipher text.	-
peer-lsr-id	Specifies the LSR ID of the peer, which identifies the peer LSR.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the password.	The value is a string of characters, spaces not supported. For a plain password, the string is 1 to 255 characters. For an encrypted password, the string is 20 to 392 characters. When double quotation marks are used around the string, spaces are allowed in the string.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. Note that the peers of an LDP session can be configured with different encryption modes (plain or cipher text mode), but must be configured with a single password.

LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

A password can be set either in cipher text or plain text. A plain text password is a character string that is pre-configured and directly recorded in a configuration file. A cipher text password is a character string that is recorded in a configuration file after being encrypted using a specified algorithm.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

- MD5 authentication and keychain authentication cannot be configured together on one peer. Note that MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.
- If the password on a peer changes, the LDP session is reestablished and the LSP associated with the original LDP session is deleted.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the local node to perform MD5 authentication when it establishes an LDP session with its peer.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] md5-password cipher 2.2.2.2 Huawei-123
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.73 md5-password all

Function

The **md5-password all** command enables LDP MD5 authentication in a batch for all LDP peers.

The **undo md5-password all** command disables LDP MD5 authentication in a batch for all LDP peers.

By default, MD5 authentication in a batch is disabled for all LDP peers. LDP MD5 authentication is recommended to ensure security.

Format

md5-password { **plain** | **cipher** } **all** *password*

undo md5-password all

Parameters

Parameter	Description	Value
plain	Indicates a simple text password. A simple text password is saved in simple text in a configuration file. This format poses risks. A ciphertext password is recommended. To improve device security, periodically modify the password.	-
cipher	Indicates a ciphertext password.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies an authentication password.	A password must not contain spaces. A simple text password is a string of 1 to 255 characters. A ciphertext password is a string of 1 to 255 characters. An MD5 ciphertext password is 20 bits to 392 bits long. The string can contain spaces if it is enclosed with double quotation marks ('').

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

If a great number of LDP peers are configured, run the **md5-password all** command to enable MD5 authentication in a batch for all LDP peers.

Configuration Impact

After the **md5-password all** command is run, MD5 authentication takes effect on all LDP peers. If MD5 authentication fails, an LDP session fails to be established.

Precautions

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.
- The session is not re-established if the passwords on both ends are the same. If the interval between password settings on both ends exceeds the session Keepalive time and the passwords become different, the sessions is disconnected due to a timeout, causing an LSP to be deleted.

 Copyright © Huawei Technologies Co., Ltd.

- Note that the peers of an LDP session can be configured with different authentication modes (simple text or ciphertext), but must be configured with a single password.

Example

Enable LDP MD5 authentication for all LDP peers.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] md5-password cipher all Huawei-123
```

11.1.74 md5-password peer-group

Function

The **md5-password peer-group** command enables LDP MD5 authentication in a batch for a specified LDP peer group.

The **undo md5-password peer-group** command disables LDP MD5 authentication in a batch for a specified LDP peer group.

By default, MD5 authentication in a batch is disabled for all peer groups. LDP MD5 authentication is recommended to ensure security.

Format

md5-password { **plain** | **cipher** } **peer-group** *ip-prefix-name password*

undo md5-password peer-group

Parameters

Parameter	Description	Value
plain	Indicates a simple text password. A simple text password is saved in simple text in a configuration file. This format poses risks. A ciphertext password is recommended. To improve device security, periodically modify the password.	-
cipher	Indicates a ciphertext password.	-
ip-prefix-name	Specifies the name of an IP prefix list. The IP prefix list name is configured using the **ip ip-prefix** command.	The value is a string of 1 to 169 case-sensitive characters, spaces not supported. The string can contain spaces if it is enclosed with double quotation marks ('').

Parameter	Description	Value
password	Specifies an authentication password.	A password must not contain spaces. A simple text password is a string of 1 to 255 characters. A ciphertext password is a string of 1 to 255 characters. An MD5 ciphertext password is 20 bits to 392 bits long. The string can contain spaces if it is enclosed with double quotation marks ('').

Views

MPLS-LDP view

Default Level

2: Configuration level

Task Name and Operations

Task Name	Operations
mpls-ldp	write

Usage Guidelines

Usage Scenario

MD5 authentication can be configured for a TCP connection over which an LDP session is established, improving security. LDP MD5 authentication generates a unique digest for an information segment to prevent LDP packets from being modified. LDP MD5 authentication is stricter than common checksum verification for TCP connections.

If a great number of LDP peers are configured, run the **md5-password peer-group** command to enable MD5 authentication in a batch for LDP peers in a specified peer group. An IP prefix list can be specified to define the range of IP addresses in a group.

Prerequisites

An IP prefix list has been configured using the **ip ip-prefix** command.

Configuration Impact

After the **md5-password peer-group** command is run, MD5 authentication takes effect on a specified LDP peer group. If MD5 authentication fails, an LDP session fails to be established.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- LDP authentication configurations are prioritized in descending order: for a single peer, for a specified peer group, for all peers. Keychain and MD5 configurations of the same priority are mutually exclusive. Keychain authentication and MD5 authentication can be configured simultaneously for a specified LDP peer, for this LDP peer in a specified peer group, and for all LDP peers. The configuration with a higher priority takes effect. For example, if MD5 authentication is configured for Peer1 and then keychain authentication is configured for all LDP peers, MD5 authentication takes effect on Peer1.
- The session is not re-established if the passwords on both ends are the same. If the interval between password settings on both ends exceeds the session Keepalive time and the passwords become different, the sessions is disconnected due to a timeout, causing an LSP to be deleted.
- Note that the peers of an LDP session can be configured with different authentication modes (simple text or ciphertext), but must be configured with a single password.

Before a peer group is referenced, create it. By default, a nonexistent peer group cannot be specified in this command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is specified in this command, a local device performs MD5 authentication for each LDP session connected to each LDP peer.

Example

Enable LDP MD5 authentication for LDP peers with IP addresses matching the IP prefix list named **list1**.

```
<Huawei>system-view
[Huawei] ip ip-prefix list1 permit 4.4.4.4 32
[Huawei] mpls ldp
[Huawei-mpls-ldp] md5-password cipher peer-group list1 Huawei-123
```

11.1.75 mpls (system view)

Function

The **mpls** command enables MPLS on the local node and displays the MPLS view.

The **undo mpls** command deletes all MPLS configurations.

By default, no node is enabled with MPLS.

Format

mpls

undo mpls

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **mpls** command on a network where MPLS services are to be deployed.

You can run MPLS-related commands only after running the **mpls** command.

Prerequisites

The LSR ID has been configured using the **mpls lsr-id** command.

Precautions

The **undo mpls** command run in the system view deletes all MPLS configurations in the system view and interface view, except the MPLS LSR-ID.

Example

Enable MPLS.

```
<Huawei> system-view
[Huawei] mpls lsr-id 10.1.1.1
[Huawei] mpls
Info: Mpls starting, please wait... OK!
```

Related Topics

11.1.92 mpls lsr-id

11.1.76 mpls (interface view)

Function

The **mpls** command enables MPLS on an interface.

The **undo mpls** command disables MPLS on an interface.

By default, no interface is enabled with MPLS.

Format

mpls

undo mpls

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, XGE interface view, Serial interface view, Eth-trunk interface view, Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS services are deployed, after enabling MPLS on a node, enable MPLS on the interfaces of the node before performing other MPLS configurations.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

Running the **undo mpls** command in the interface view deletes all MPLS configurations on the interface.

Example

Enable MPLS on the interface GE1/0/0.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
```

Related Topics

11.1.75 mpls (system view)

11.1.77 mpls bfd enable

Function

The **mpls bfd enable** command enables dynamic creation of BFD sessions on the ingress node of an LDP LSP.

The **undo mpls bfd enable** command disables the dynamic creation of BFD sessions on the ingress node of an LDP LSP.

By default, an ingress cannot dynamically create BFD sessions for monitoring LDP LSPs.

Format

mpls bfd enable

undo mpls bfd enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network, use LDP to dynamically create LSP tunnels. Upon a fault on the link, the convergence is slow. Configure BFD to detect LDP LSP connectivity to speed up convergence.

To dynamically establish a BFD session, run the **mpls bfd enable** command on the source end of the LDP LSP.

NOTE

After the **mpls bfd enable** command is used, no BFD session is set up.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Example

Enable the dynamic creation of BFD sessions on the ingress node of an LDP LSP.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls bfd enable
```

Related Topics

11.1.94 mpls-passive

11.1.78 mpls bfd

Function

The **mpls bfd** command sets the parameters of BFD sessions.

The **undo mpls bfd** command deletes the parameters of BFD sessions.

By default, no parameter of BFD sessions is set.

Format

mpls bfd { **min-tx-interval** *interval* | **min-rx-interval** *interval* | **detect-multiplier** *multiplier* } *

undo mpls bfd { **min-tx-interval** *interval* | **min-rx-interval** *interval* | **detect-multiplier** *multiplier* } *

undo mpls bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

Parameters

Parameter	Description	Value
min-tx-interval *interval*	Specifies the interval at which BFD packets are sent.	The value is an integer that ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
min-rx-interval *interval*	Specifies the interval at which BFD packets are received.	The value is an integer that ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. By default, the value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

On an MPLS network, use BFD to detect LSP connectivity to increase the link fault detection speed. Users can change the values of BFD parameters based on actual networking. On an unstable link, if the BFD parameters are set small, the BFD session may flap. You can increase the values of BFD parameters.

Actual interval for the local device to send BFD packets = max { interval for sending BFD packets on the local end, interval for receiving BFD packets on the peer end }; actual interval for the local device to receive BFD packets = max { interval for sending BFD packets on the peer end, interval for receiving BFD packets on the local end }; and local BFD detection time = actual interval for receiving BFD packets on the local end x BFD detection multiplier on the peer end.

If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval at which BFD packets are sent to 200 ms.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls bfd min-tx-interval 200
```

Related Topics

11.1.77 mpls bfd enable

11.1.79 mpls bfd-trigger

Function

The **mpls bfd-trigger** command configures a trigger policy for an LDP BFD session.

The **undo mpls bfd-trigger** command deletes a trigger policy for an LDP BFD session.

By default, no trigger policy for an LDP BFD session is configured.

Format

mpls bfd-trigger [**host** [**nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number*] * | **fec-list** *list-name*]

undo mpls bfd-trigger [**host** [**nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number*] * | **fec-list** *list-name*]

Parameters

Parameter	Description	Value
host	Indicates that all host addresses are used to create LDP BFD sessions.	-
nexthop *next-hop-address*	Specifies the next hop address on an LSP.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outbound interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-
fec-list *list-name*	Specifies the name of a FEC list, by which the creation of an LDP BFD session is triggered.	The value is an existing FEC list name.

 Copyright © Huawei Technologies Co., Ltd.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The trigger policy for LDP BFD has two types: the host address and FEC list.

If you want all host addresses to trigger the establishment of BFD sessions, use the host trigger mode. Specify the LSPs that can set up BFD sessions by specifying the next hop address and the outbound interface.

If you only want part of hosts to trigger the establishment of BFD sessions, use the FEC list trigger mode to specify the corresponding host addresses. Before specifying the FEC list triggering mode, run the **fec-list** and **fec-node** commands to configure a FEC list.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Example

Configure the host trigger policy of BFD sessions in the MPLS view.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls bfd enable
[Huawei-mpls] mpls bfd-trigger host
```

Related Topics

18.5.2 bfd

11.1.77 mpls bfd enable

11.1.48 fec-list

11.1.49 fec-node

11.1.80 mpls dynamic-label-number threshold-alarm

Function

The **mpls dynamic-label-number threshold-alarm** command sets alarm thresholds of dynamic label usage.

The **undo mpls dynamic-label-number threshold-alarm** command restores the default settings.

By default, the upper limit is 80%, and the lower limit is 70%.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls dynamic-label-number threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls dynamic-label-number threshold-alarm

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper limit of dynamic label usage.	The value is a percent integer ranging from 1 to 100. Using a value larger than 95 is not recommended. Using the default value 80 is recommended.
lower-limit *lower-limit-value*	Specifies the lower limit of dynamic label usage.	The value is a percent integer ranging from 1 to 100. The lower limit must be less than the upper limit. Using the default value 70 is recommended.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If dynamic labels run out but the system receives new dynamic label requests, the system fails to satisfy the requests because the dynamic labels are insufficient. As a result, the module that fails to be assigned labels works abnormally. The modules that apply for labels including MPLS TE, MPLS LDP, BGP, L3VPN and L2VPN. To facilitate operation and maintenance, run **mpls dynamic-label-number threshold-alarm** command to set alarm thresholds of dynamic label usage. The system can alert users to the issue that dynamic labels will exhaust.

This command enables the system to generate an alarm in either of the following situations:

- *upper-limit-value*: a percent indicating the upper limit of dynamic labels. If dynamic label usage reaches the upper limit, an alarm is generated.
- *lower-limit-value*: a percent indicating the lower limit of dynamic labels. If dynamic label usage falls below the lower limit, a clear alarm can be generated.

Precautions

If the **mpls dynamic-label-number threshold-alarm** command is run more than once, the latest configuration overrides the previous one.

 Copyright © Huawei Technologies Co., Ltd.

The **mpls dynamic-label-number threshold-alarm** command only configures the trigger conditions for an alarm and its clear alarm. Although trigger conditions are met, the alarm and its clear alarm can be generated only after the **snmp-agent trap enable feature-name mpls_lspm trap-name** { **hwmplsdynamiclabelthresholdexceed** | **hwmplsdynamiclabelthresholdexceedclear** } command is run to enable the device to generate a dynamic label insufficiency alarm and its clear alarm.

Example

Set the thresholds for triggering dynamic label alarms.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls dynamic-label-number threshold-alarm upper-limit 90 lower-limit 60
```

11.1.81 mpls ldp advertisement

Function

The **mpls ldp advertisement** command configures the label advertisement mode.

The **undo mpls ldp advertisement** command restores the default setting.

By default, the label advertisement mode is downstream unsolicited (DU).

Format

mpls ldp advertisement { **dod** | **du** }

undo mpls ldp advertisement

Parameters

Parameter	Description	Value
dod	Indicates the downstream on demand (DoD) mode. After the upstream requests the downstream for a label, the downstream sends a Label Mapping message to the upstream.	-
du	Indicates the DU mode. Without a request, the downstream voluntarily sends a Label Mapping message to the upstream.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, downstream LSRs unsolicitedly send Label Mapping messages to upstream LSRs. Establishing a large number of LSPs burdens an LSR such as a DSLAM (a low-performance access device) deployed on an MPLS network. On a large network, run the **mpls ldp advertisement dod** command. This setting allows a DSLAM to send Label Mapping messages to upstream LSRs only after receiving requests for labels. This setting helps minimize the number of unwanted MPLS forwarding entries forwarded by the DSLAM.

Prerequisites

MPLS LDP has been enabled on the interface using the **mpls ldp (interface view)** command.

Precautions

- When multiple links exist between neighbors, all interfaces must use the same label advertisement mode.
- Modifying the label advertisement mode causes reestablishment of LDP sessions.

Example

Set the label advertisement mode to DoD.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls ldp
[Huawei-GigabitEthernet1/0/0] mpls ldp advertisement dod
Warning: All the related sessions will be deleted if the operation is performed!
Continue? (y/n)y
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.82 mpls ldp (system view)

Function

The **mpls ldp** command enables LDP on the local node and displays the MPLS-LDP view.

The **undo mpls ldp** command deletes all LDP configurations.

By default, LDP is not enabled on a node.

Format

mpls ldp

undo mpls ldp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS LDP needs to be deployed, run the **mpls ldp** command to enable MPLS LDP globally and create a public network instance running LDP.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Follow-up Procedure

You can perform other LDP configurations.

Precautions

Running the **undo mpls ldp** command in the system view deletes all MPLS LDP configurations in the system and interface views.

Example

Enable LDP.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls ldp
[Huawei-mpls-ldp]
```

Related Topics

11.1.75 mpls (system view)

11.1.83 mpls ldp (interface view)

Function

The **mpls ldp** command enables MPLS LDP function on an interface.

The **undo mpls ldp** command disables MPLS LDP function on an interface.

By default, no interface is enabled with MPLS LDP function.

Format

mpls ldp

undo mpls ldp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, Serial interface view, Eth-trunk interface view, Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where MPLS LDP needs to be deployed, enable MPLS LDP function on an interface before configuring other LDP configurations.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

MPLS has been enabled on the interface using the **mpls** command in the interface view.

NOTE

To enable MPLS LDP on an interface in the tunnel interface view, you must set the parameter in the **tunnel-protocol** command to **gre p2mp** or **gre**.

Follow-up Procedure

You can perform other MPLS LDP configurations.

Precautions

Running the **undo mpls ldp** command in the interface view deletes all MPLS LDP configurations on the interface.

Example

Enable MPLS LDP function on GE1/0/0.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls ldp
[Huawei-mpls-ldp] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls ldp
```

Related Topics

11.1.82 mpls ldp (system view)
11.1.76 mpls (interface view)

11.1.84 mpls ldp frr nexthop

Function

The **mpls ldp frr nexthop** command enables LDP FRR on an interface.

The **undo mpls ldp frr** command disables LDP FRR on an interface.

By default, no interface is enabled with LDP FRR.

Format

mpls ldp frr nexthop *nexthop-address* [**ip-prefix** *ip-prefix-name*] [**priority** *priority*]

undo mpls ldp frr [**nexthop** *nexthop-address*] [**ip-prefix** *ip-prefix-name*] [**priority** *priority*]

Parameters

Parameter	Description	Value
nexthop *nexthop-address*	Specifies the next hop address on a backup LSP.	The value is in dotted decimal notation.
ip-prefix *ip-prefix-name*	Specifies the IP prefix name. Only the FEC that matches the specified IP prefix can trigger the generation of a backup LSP.	The value is an existing IP prefix name.
priority *priority*	Specifies the priority of a backup LSP. The greater the value is, the lower priority the backup LSP has.	The value is an integer ranging from 1 to 65535. By default, the value is 50.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traditional IP FRR technology cannot effectively protect the traffic on an MPLS network. The device provides the LDP FRR function and the solution to port protection.

In the manual LDP FRR mode, you need to configure a backup LSP by specifying the outbound interfaces or the next hops. This mode applies to simple-structured networks.

 Copyright © Huawei Technologies Co., Ltd.

When running the **mpls ldp frr nexthop** command to configure the next hop IP address, note that:

- You can configure multiple next hops on one interface. This allows you to configure multiple backup LSPs with different outbound interfaces for the primary LSP.
- You can configure different prefix lists for the same next hop on one interface.
  - If no prefix list is specified, LDP FRR tries to establish backup LSPs along the path specified by *nexthop-address* for all primary LSPs on the interface.
  - If only the DENY item is in a specified prefix list, no backup LSP is allowed to set up along the path specified by *nexthop-address* for the primary LSP mapping to the FEC denied by the interface.
  - If only PERMIT item is in the specified prefix list, backup LSPs are allowed to set up along the path specified by *nexthop-address* only for the primary LSPs mapping to the FEC permitted by the interface.
  - If both PERMIT and DENY items are in the prefix list, only the PERMIT item is effective. That is, backup LSPs are allowed to set up along the path specified by *nexthop-address* only for the primary LSPs mapping to the FEC permitted by the interface.
- A single interface supports LDP FRR with a maximum of 10 priorities. Only a single backup LSP is generated.

Precautions

- If the **undo mpls ldp** command is run in the system view or the **undo mpls ldp** command is run in the interface view to disable LDP functions, the LDP FRR configuration in the interface remains but does not take effect. During the LDP FRR configuration, the LSP that functions as the backup LSP must be in the liberal state. For a backup LSP, the routing status of the backup LSP from the ingress node to the egress node must be Inactive Adv.
- LDP FRR cannot be enabled or disabled during LDP GR.
- When both LDP FRR and IP FRR are enabled, IP FRR takes effect.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, backup LSPs are established for all LDP LSPs on the local interface along the path to the specified next-hop IP address.

Example

Enable LDP FRR on GE1/0/0, and set the next hop IP address of the backup LSP to 10.1.1.2.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls ldp frr nexthop 10.1.1.2
```

Related Topics

11.1.82 mpls ldp (system view)
11.1.83 mpls ldp (interface view)

11.1.85 mpls ldp remote-peer

Function

The **mpls ldp remote-peer** command creates a remote peer and displays the remote peer view.

The **undo mpls ldp remote-peer** command deletes a remote peer.

By default, no remote peer is created.

Format

mpls ldp remote-peer *remote-peer-name*

undo mpls ldp remote-peer *remote-peer-name*

Parameters

Parameter	Description	Value
remote-peer-name	Specifies the name of a remote LDP peer.	A string of 1 to 32 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A remote LDP session is used to allocate inner L2VPN labels. If a Martini VLL or VPLS connection is to be established between two LSRs, the remote LDP session must be established between the LSRs to allocate inner labels.

A remote LDP session can be established between two indirectly connected LSRs or two directly connected LSRs.

A local and a remote LDP session can be established together between two LSRs.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Follow-up Procedure

An IP address can be assigned to the LDP remote peer.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When configuring a remote LDP peer, run the **mpls ldp remote-peer** command on the local LDP and remote LDP peers.

Example

Create a remote peer.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] quit
[Huawei] mpls ldp remote-peer BJI
[Huawei-mpls-ldp-remote-bji]
```

Related Topics

11.1.37 display mpls ldp remote-peer

11.1.107 remote-ip

11.1.110 remote-peer pwe3

11.1.86 mpls ldp timer hello-hold

Function

The **mpls ldp timer hello-hold** command sets the value of a Hello Hold timer.

The **undo mpls ldp timer hello-hold** command restores the default value.

By default, the link Hello Hold timer is 15 seconds and the target Hello Hold timer is 45 seconds.

Format

mpls ldp timer hello-hold *interval*

undo mpls ldp timer hello-hold

Parameters

Parameter	Description	Value
interval	Specifies the value of a Hello Hold timer.	The value is an integer ranging from 3 to 65535, in seconds. Value 65535 indicates that the timer never expires.

Views

Interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Two LDP peers periodically exchange Hello messages to maintain the Hello adjacency. If no Hello message is received after the target Hello hold timer expires, the Hello adjacency is deleted.

The default value of the timer is recommended. On a network where the link status is unstable or a large number of packets are sent, increase the value of the timer to prevent the session flapping.

Hello hold timers are classified into the following types:

- Link-Hello hold timer: maintains the local adjacency. The **mpls ldp timer hello-hold** command in the interface view sets a value of the timer.
- Target-Hello hold timer: maintains the remote adjacency. The **mpls ldp timer hello-hold** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the timer that actually takes effect is the smaller one between the two Hello holder timers configured on both ends of an LDP session. If the value is smaller than 9, the Hello hold timer is 9.

Example

Set the value of the link Hello hold timer to 30 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls ldp
[Huawei-GigabitEthernet1/0/0] mpls ldp timer hello-hold 30
```

Set the value of the target Hello hold timer to 60 seconds.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer bji
[Huawei-mpls-ldp-remote-bji] mpls ldp timer hello-hold 60
```

Related Topics

11.1.85 mpls ldp remote-peer

11.1.87 mpls ldp timer hello-send

Function

The **mpls ldp timer hello-send** command sets the value of a Hello send timer.

The **undo mpls ldp timer hello-send** command restores the default setting.

By default, the value of a Hello send timer is one third the value of a Hello hold timer.

Format

mpls ldp timer hello-send *interval*

undo mpls ldp timer hello-send

Parameters

Parameter	Description	Value
interval	Specifies the value of a Hello send timer.	The value is an integer ranging from 1 to 65535, in seconds.

Views

Interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends Hello messages to the neighboring LSR to advertise its presence on the network and sets up the Hello adjacency. The Hello messages are sent at an interval specified by the Hello send timer.

The default value of the Hello send timer is recommended. On a network with poor performance, you can reduce the value of the Hello send timer, enabling the network to recover from faults as soon as possible.

Hello send timers are classified into the following types:

- Link-Hello send timer: maintains the local adjacency. The **mpls ldp timer hello-send** command in the interface view sets a value of the timer.
- Target-Hello send timer: maintains the remote adjacency. The **mpls ldp timer hello-send** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the Hello send timer that takes effect is not necessarily the same as the set value. If the value of the Hello send timer is greater than one third of the value of the Hello hold timer, the value of the Hello send timer that takes effect is equal to one third of the value of the link-Hello hold timer. Run the **mpls ldp timer hello-hold** command to set the value for the Hello hold timer.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the link Hello send timer to 10 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls ldp
[Huawei-GigabitEthernet1/0/0] mpls ldp timer hello-send 10
```

Set the value of the target Hello send timer to 20 seconds.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer bji
[Huawei-mpls-ldp-remote-bji] mpls ldp timer hello-send 20
```

Related Topics

11.1.86 mpls ldp timer hello-hold

11.1.88 mpls ldp timer igp-sync-delay

Function

The **mpls ldp timer igp-sync-delay** command sets the interval during which an LSP is being set up after an LDP session is created.

The **undo mpls ldp timer igp-sync-delay** command restores the default setting.

By default, the interval is 10 seconds.

Format

mpls ldp timer igp-sync-delay *value*

undo mpls ldp timer igp-sync-delay

Parameters

Parameter	Description	Value
value	Specifies the interval, during which an LSP is being set up after an LDP session is created.	The value is an integer ranging from 0 to 65535, in seconds.

Views

Interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an LDP session is reestablished on a faulty link, LDP starts the igp-sync-delay timer to wait for the establishment of an LSP.

 Copyright © Huawei Technologies Co., Ltd.

After the igp-sync-delay timer times out, LDP notifies the IGP that synchronization is complete.

Precautions

The **isis ldp-sync** command can be run on all interfaces, except for loopback, null0, and Layer 2 interfaces.

Example

After the LDP session is established on GE1/0/0, the interval is set to 15 seconds, during which the LSP is being set up.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls ldp
[Huawei-GigabitEthernet1/0/0] mpls ldp timer igp-sync-delay 15
```

After the LDP session is established in the remote MPLS LDP peer view, the interval is set to 15 seconds, during which the LSP is being set up.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer rta
[Huawei-mpls-ldp-remote-rta] mpls ldp timer igp-sync-delay 15
```

Related Topics

11.1.31 display mpls ldp interface

11.1.89 mpls ldp timer keepalive-hold

Function

The **mpls ldp timer keepalive-hold** command sets the value of a Keepalive hold timer.

The **undo mpls ldp timer keepalive-hold** command restores the default setting.

By default, the value of the Keepalive-hold timers of both local and remote sessions is 45 seconds.

Format

mpls ldp timer keepalive-hold *interval*

undo mpls ldp timer keepalive-hold

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a Keepalive hold timer.	The value is an integer ranging from 30 to 65535, in seconds.

Views

Interface view or remote MPLS LDP peer view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

LDP peers exchange LDP PDUs over session connections to maintain LDP sessions. If a node does not receive any LDP PDU after the Keepalive hold timer expires, the node closes the connection to terminate the session.

The default value of the Keepalive hold timer is recommended. On a network with unstable links, increase the value of a Keepalive hold timer, preventing the session flapping.

Keepalive hold timers are classified into the following types:

- Keepalive hold timer of the local session: maintains the local LDP session. The **mpls ldp timer keepalive-hold** command in the interface view sets a value of the timer.
- Keepalive hold timer of the remote session: maintains the remote LDP session. The **mpls ldp timer keepalive-hold** command in the remote MPLS LDP peer view sets a value of the timer.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

- The value of the Keepalive hold timer that takes effect is the smaller one between the two Keepalive hold timers configured on both ends of an LDP session.
- If more than one LDP link exists between two LSRs, the values of the Keepalive hold timers set for the links must be the same; otherwise, the LDP sessions may be unstable.
- Changing the value of a Keepalive hold timer causes the reestablishment of related LDP sessions.

Example

Set the value of the Keepalive hold timer for a local session to 60 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls ldp
[Huawei-GigabitEthernet1/0/0] mpls ldp timer keepalive-hold 60
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Set the value of the Keepalive hold timer for a remote session to 50 seconds.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer bji
[Huawei-mpls-ldp-remote-bji] mpls ldp timer keepalive-hold 50
Warning: All the related sessions will be deleted if the operation is performed!Continue? (y/n)y
```

Related Topics

11.1.85 mpls ldp remote-peer

11.1.90 mpls ldp timer keepalive-send

Function

The **mpls ldp timer keepalive-send** command sets the value of a Keepalive send timer.

The **undo mpls ldp timer keepalive-send** command restores the default setting.

By default, the value of a Keepalive send timer is one third the value of a Keepalive hold timer.

Format

mpls ldp timer keepalive-send *interval*

undo mpls ldp timer keepalive-send

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a Keepalive send timer.	The value is an integer ranging from 1 to 65535, in seconds.

Views

Interface view, remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an LDP session is set up, LSRs on the two ends of the session periodically exchange Keepalive messages to maintain the LDP session.

The default value of the Keepalive send timer is recommended. On a network with poor performance, reduce the value of the Keepalive send timer, enabling the network to recover as soon as possible.

Keepalive send timers are classified into the following types:

- Keepalive send timer of the local LDP session: controls the interval at which Keepalive messages are sent to the peer end of the local session. The **mpls ldp timer keepalive-send** command in the interface view sets a value of this timer.
- Keepalive send timer of the remote LDP session: controls the interval at which Keepalive messages are sent to the peer end of the remote session. The **mpls ldp timer keepalive-send** command in the remote MPLS LDP peer view sets a value of the timer.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The remote LDP peer has been configured or MPLS LDP has been enabled on the interface.

Precautions

The value of the Keepalive send timer that actually takes effect may be different from the configured one. If the value of the Keepalive send timer is greater than one third of the value of the Keepalive hold timer, the value of the Keepalive send timer that actually takes effect is equal to one third of the value of the Keepalive hold timer.

Example

Set the value of the Keepalive send timer for setting up a local LDP session to 10 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls ldp
[Huawei-GigabitEthernet1/0/0] mpls ldp timer keepalive-send 10
```

Set the value of the Keepalive send timer for setting up a remote LDP session to 20 seconds.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer bji
[Huawei-mpls-ldp-remote-bji] mpls ldp timer keepalive-send 20
```

Related Topics

11.1.89 mpls ldp timer keepalive-hold

11.1.91 mpls ldp transport-address

Function

The **mpls ldp transport-address** command configures an LDP transport address.

The **undo mpls ldp transport-address** command restores the default setting.

By default, the transport address for a node on a public network is the LSR ID of the node, and the transport address for a node on a private network is the primary IP address of an interface on the node.

Format

mpls ldp transport-address { *interface-type interface-number* | **interface** }

undo mpls ldp transport-address

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. LDP uses the address of the interface as the TCP transport address.	-

Parameter	Description	Value
interface	Indicates that LDP uses the IP address of the current interface as the TCP transport address.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before two LSRs establish an LDP session, the two LSRs need to establish a TCP connection to exchange label messages. Run the **mpls ldp transport-address** command to set the address (the LDP transport address) for the TCP connection.

The transport address is used to establish a TCP connection between the local node and its peer. The peer must have a reachable route to this transport address. The default transport address is the loopback interface address (an LSR ID). When the address of the loopback interface is a public network address, configure different transport addresses for LSRs so that LSRs can set up connections with private network addresses.

You can run the **mpls ldp transport-address** command in the interface view to set the transport address for a TCP connection. When more than one link exists between two LSRs, and the links are bound to VPN instances, the default transport address is the IP address of an interface rather than the LSR ID of an LSR.

NOTE

- If LDP sessions are to be established over multiple links connecting two LSRs, LDP-enabled interfaces of either LSR must use the default transport address or the same transport address. If interfaces on either of the LSRs are assigned different transport addresses, a single transport address can be used and a single LDP session can be established.
- When the LDP transport address changes, the session is not interrupted immediately. The session is interrupted after the Hello hold timer times out.

Prerequisites

MPLS LDP has been enabled on the interface using the **mpls ldp (interface view)** command.

An IP address must be assigned to the specified interface. If no IP address is assigned, 0.0.0.0 is used as a transport address, causing a failure to establish an LDP session.

Precautions

Changing an LDP transport address interrupts an LDP session. Exercise caution when running the **mpls ldp transport-address** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the transport address for link Hello messages to the current interface address.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls ldp
[Huawei-GigabitEthernet1/0/0] mpls ldp transport-address interface
```

Related Topics

11.1.92 mpls lsr-id

11.1.83 mpls ldp (interface view)

11.1.92 mpls lsr-id

Function

The **mpls lsr-id** command sets an LSR ID.

The **undo mpls lsr-id** command deletes an LSR ID.

By default, no LSR ID is set.

Format

mpls lsr-id *lsr-id*

undo mpls lsr-id

Parameters

Parameter	Description	Value
lsr-id	Specifies the LSR ID of a device, which identifies the LSR.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR ID identifies an LSR on a network. On a network where MPLS services are deployed, you must configure the LSR IDs for devices.

An LSR does not have the default LSR ID, and you must configure an LSR ID for it. To enhance network reliability, you are advised to use the IP address of a loopback interface on the LSR as the LSR ID.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

You can configure MPLS and associated services.

Precautions

Before changing or deleting a configured LSR ID, you must run the **undo mpls** command in the system view to delete all MPLS configurations. Exercise caution when you run the **undo mpls** command.

Example

Set the LSR ID to 1.1.1.1.

```
<Huawei> system-view
[Huawei] mpls lsr-id 1.1.1.1
```

Related Topics

11.1.75 mpls (system view)

11.1.93 mpls mtu

Function

The **mpls mtu** command configures the MTU of MPLS packets on an interface.

The **undo mpls mtu** command restores the default setting.

By default, the MTU of MPLS packets is equal to the interface MTU.

Format

mpls mtu *mtu*

undo mpls mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MPLS MTU of an interface.	The value range varies according to the interface type.

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

An MTU value determines the maximum number of bytes that can be sent each time. If the size of packets exceeds the MTU supported by a transit node or a receiver, the transit node or receiver fragments the packets or even discards them, increasing the network transmission load. MTU values must be correctly negotiated between LSRs to enable packets to successfully reach the receiver.

To calculate the MPLS MTU, an LSR on the path to a specified FEC compares all MTUs advertised by downstream devices with the interface MTU of its own, and adds the smaller MTU (the MPLS MTU) to the MTU TLV field in the Label Mapping message, and send the Label Mapping message upstream.

If an MTU value changes (for example when the local outbound interface or its configuration changes), an LSR recalculates the MTU value and sends a Label Mapping message carrying the new MTU value to all upstream devices.

The relationships between the MPLS MTU and the interface MTU are as follows:

- If no MPLS MTU is configured on an interface, the interface MTU is used to control forwarding of MPLS packets.
- If both an MPLS MTU and an interface MTU are configured on an interface, the smaller value between the two MTUs is used to control forwarding of MPLS packets.

Prerequisites

MPLS has been enabled on the interface using the **mpls (interface view)** command.

Precautions

After the **mpls mtu** command is run, LDP compares the MPLS MTU and the interface MTU, and uses the smaller value between the two MTUs.

Example

Set the MPLS MTU to 1500 bytes on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls mtu 1500
```

Related Topics

11.1.19 display mpls interface

11.1.94 mpls-passive

Function

The **mpls-passive** command enables the egress node of an LSP to passively create a BFD session.

The **undo mpls-passive** command disables the egress node of an LSP from passively creating a BFD session.

 Copyright © Huawei Technologies Co., Ltd.

By default, the egress node of an LSP cannot passively create a BFD session.

Format

mpls-passive

undo mpls-passive

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a unidirectional LSP, the ingress node creates a BFD session, which triggers the sending of an LSP ping packet. After the egress node receives the ping packet, a BFD session can be automatically created on the egress node. Run the **mpls-passive** command to enable the BFD session to be created passively on the egress node of an LSP. If the feature is disabled, the egress node cannot automatically create a BFD session.

Prerequisites

BFD has been enabled globally using the **bfd** command.

Precautions

You need to run the **mpls-passive** command on the egress node. Then, the egress node can create a BFD session in an opposite direction after receiving an LSP ping request packet carrying a BFD TLV.

Example

Enable the egress node of an LSP to automatically and passively create a BFD session.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] mpls-passive
```

Related Topics

11.1.77 mpls bfd enable

11.1.95 mpls ping interval

Function

The **mpls ping interval** command sets the interval at which LSP ping packets are sent in a dynamic BFD session.

The **undo mpls ping interval** command restores the default setting.

By default, the interval at which LSP ping packets are sent in a dynamic BFD session is 60 seconds.

Format

mpls ping interval *interval*

undo mpls ping interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending LSP ping packets.	The value is an integer ranging from 30 to 600, in seconds. The default value is 60.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an LSP, when the active role (the ingress node) creates a dynamic BFD session, an LSP ping request packet carrying a BFD TLV is sent. After receiving the LSP ping request packet, the passive role (the egress node) replies with an LSP ping response packet carrying the BFD TLV. Then, a BFD session is established. The egress node can automatically create the BFD session only after receiving the LSP ping packet. To set the interval for sending the LSP ping packet by dynamic BFD, run the **mpls ping interval** command.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

A small interval for sending LSP ping packets imposes a heady burden on links.

 Copyright © Huawei Technologies Co., Ltd.

Set the interval for sending the L SP ping packet according to the actual networking because the egress node can establish a BFD session only after receiving an LSP ping packet.

Example

Set the interval to 80 seconds for sending LSP ping packets in a dynamic BFD session.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] mpls ping interval 80
```

11.1.96 mtu-signalling

Function

The **mtu-signalling** command enables the router to send Label Mapping messages carrying the MTU TLV.

The **undo mtu-signalling** command disables the router to send Label Mapping messages carrying the MTU TLV.

By default, the router sends Label Mapping messages carrying the Huawei private MTU TLV.

Format

mtu-signalling [**apply-tlv**]

undo mtu-signalling [**apply-tlv**]

Parameters

Parameter	Description	Value
apply-tlv	Sends Label Mapping messages carrying the MTU TLV, as defined in RFC3988. If this parameter is not configured, Label Mapping messages carry a Huawei proprietary MTU TLV.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An MPLS MTU value determines the maximum size of a Label Mapping message exchanged between two devices on a network. Before packet transmission, devices calculate the MPLS MTU value to prevent packet fragmentation during the

transmission, relieving the load on the network. The MPLS MTU value advertised between devices is carried in the MTU TLV field of the Label Mapping message.

After the **mpls ldp** command is run, an MPLS LDP-enabled LSR by default sends a Huawei proprietary MTU TLV different from the MTU TLV defined in RFC3988.

- The default MTU setting is recommended.
- To ensure the communication with non-Huawei devices, run the **mtu-signalling apply-tlv** command to enable LSRs to send Label Mapping messages carrying the MTU TLV defined in RFC3988.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

- The MPLS MTU is a parameter to be negotiated during the LDP LSP establishment. If a Huawei device is connected to a non-Huawei device, run the **mtu-signalling apply-tlv** command; otherwise, the user-defined MPLS MTU does not take effect.
- The **mtu-signalling** command must be run before the **mpls ldp** command is run; otherwise, the number of network packets increases abruptly.
- Running the **undo mtu-signalling** command initiates the LDP session.

Example

Enable LDP to send Label Mapping messages carrying the MTU TLV, as defined in RFC3988.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] mtu-signalling apply-tlv
Warning: All the related sessions will be deleted if the operation is performed!
Continue? (y/n)y
```

Related Topics

11.1.23 display mpls ldp

11.1.97 no-renegotiate session-parameter-change graceful-restart

Function

The **no-renegotiate session-parameter-change graceful-restart** command disables a device from re-establishing existing LDP sessions when LDP GR status or a GR parameter is changed.

The **undo no-renegotiate session-parameter-change graceful-restart** command restores the default configuration.

By default, a device re-establishes LDP sessions when LDP GR status or a GR parameter is changed.

 Copyright © Huawei Technologies Co., Ltd.

Format

no-renegotiate session-parameter-change graceful-restart

undo no-renegotiate session-parameter-change graceful-restart

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

To disable a device from re-establishing existing LDP sessions when LDP GR status or a GR parameter is changed, run the **no-renegotiate session-parameter-change graceful-restart** command.

After the **no-renegotiate session-parameter-change graceful-restart** command is run, running the following commands does not affect the existing LDP sessions.

- **graceful-restart (MPLS-LDP view)**
- **graceful-restart timer neighbor-liveness**
- **graceful-restart timer reconnect**
- **graceful-restart timer recovery**

Example

Disable a device from re-establishing existing LDP sessions when LDP GR status or a GR parameter is changed.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] no-renegotiate session-parameter-change graceful-restart
```

11.1.98 ospf ldp-sync

Function

The **ospf ldp-sync** command enables synchronization between LDP and OSPF on an interface.

The **undo ospf ldp-sync** command disables synchronization between LDP and OSPF on an interface.

By default, synchronization between LDP and OSPF is disabled on an interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

ospf ldp-sync

undo ospf ldp-sync

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LDP convergence speed depends on the convergence speed of OSPF routes. To enable MPLS LDP on a network with the primary and backup links, the following problems may occur:

- Upon a fault on the active link, OSPF routes and ISP are switched to the backup link using LDP FRR. When the primary link recovers, OSPF routes are switched back to the primary link earlier than LDP traffic because IGP route convergence is faster than LDP convergence. As a result, LSP traffic is lost.
- If a fault occurs on the LDP session between nodes on the primary link where the OSPF routes are working properly, the OSPF routes still use the primary link and the LSP on the primary link is deleted. No OSPF route exists on the backup link; therefore, no LSP can be established on the backup link. LSP traffic is lost.

Run the **ospf ldp-sync** command to enable synchronization between LDP and OSPF to prevent traffic loss in the preceding problems. Run this command on the interfaces on both ends of the link between the node where the primary LSP and the backup LSP diverge from each other and its LDP peer on the primary LSP.

Precautions

The **ospf ldp-sync** command can be run on all interfaces, except for loopback, null0, and Layer 2 interfaces.

Example

Enable synchronization between LDP and OSPF on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf ldp-sync
```

Related Topics

11.1.99 ospf timer ldp-sync hold-down

11.1.100 ospf timer ldp-sync hold-max-cost

11.1.99 ospf timer ldp-sync hold-down

Function

The **ospf timer ldp-sync hold-down** command sets the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship.

The **undo ospf timer ldp-sync hold-down** command restores the default setting.

By default, the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship is 10 seconds.

Format

ospf timer ldp-sync hold-down *value*

undo ospf timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the interval during which an interface waits for creating an LDP session before setting up the OSPF neighbor relationship.	The value is an integer ranging from 0 to 65535, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is configured, OSPF routes are not immediately switched to the primary link after the primary link is restored and before the LDP session is established. LSP traffic is transmitted through the backup link in a period of time specified by this command.

Prerequisites

LDP and OSPF synchronization has been enabled using the **ospf ldp-sync** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

 Copyright © Huawei Technologies Co., Ltd.

The **isis ldp-sync** command can be run on all interfaces, except for loopback, null0, and Layer 2 interfaces.

Example

Set the value of the Hold-down timer for GE1/0/0 to 15 seconds, during which the interface waits for the establishment of an LDP session before setting up the OSPF neighbor relationship.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf timer ldp-sync hold-down 15
```

Related Topics

11.1.98 ospf ldp-sync

11.1.44 display ospf ldp-sync interface

11.1.100 ospf timer ldp-sync hold-max-cost

Function

The **ospf timer ldp-sync hold-max-cost** command sets the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device.

The **undo ospf timer ldp-sync hold-max-cost** command restores the default setting.

By default, the interval is 10 seconds.

Format

ospf timer ldp-sync hold-max-cost { *value* | **infinite** }

undo ospf timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
value	Specifies the interval for sending OSPF LSAs to advertise the maximum metric on the local device.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that OSPF always advertises the maximum metric in LSAs on the local device before an LDP session is reestablished.	-

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the primary LSP recovers from a fault, run the **ospf timer ldp-sync hold-max-cost** command to set the interval during which traffic is still transmitted along the backup LSP before the LDP session of the primary LSP is reestablished.

You can choose different parameters as required.

- When OSPF carries only LDP services, to ensure that OSPF routing is always consistent with the LDP LSP, specify **infinite**.
- When OSPF carries multiple services including LDP services, to ensure that OSPF route selection and other services still run properly in case the LDP session of the primary LSP fails, specify *value*.

Prerequisites

LDP and OSPF synchronization has been enabled using the **ospf ldp-sync** command in the interface view.

Precautions

This command is circular in nature, and the latest configuration overrides the previous configurations.

The **ospf ldp-sync** command can be run on all interfaces, except for loopback, null0, and Layer 2 interfaces.

Example

Set the interval at which OSPF LSAs are sent to advertise the maximum metric on the local device to 8 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ospf ldp-sync
[Huawei-GigabitEthernet1/0/0] ospf timer ldp-sync hold-max-cost 8
```

Related Topics

11.1.98 ospf ldp-sync

11.1.44 display ospf ldp-sync interface

11.1.101 outbound peer bgp-label-route

Function

The **outbound peer bgp-label-route** command configures an outbound policy to send Label Mapping messages to a specified peer based on the specified BGP labeled route.

The **undo outbound peer bgp-label-route** command restores the default configuration.

By default, no outbound policy is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

outbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **bgp-label-route** { **none** | **ip-prefix** *prefix-name* }

undo outbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **bgp-label-route**

Parameters

Parameter	Description	Value
peer-id	Specifies the ID of an LDP peer. By default, the peer ID is specified by the **mpls lsr-id** command. If the **lsr-id** command has been configured, the peer ID is specified by the **lsr-id** command.	The value is in dotted decimal notation.
peer-group *peer-group-name*	Specifies the name of a peer group. The parameter is specified by the **ip ip-prefix** command.	The value is an existing peer group name.
all	Indicates all LDP peers.	-
none	Forbids Label Mapping messages for all FECs. After the parameter **none** is configured, the LSR does not send Label Mapping messages for labeled BGP routes to the specified peer.	-
ip-prefix *prefix-name*	Allows only Label Mapping messages for labeled BGP routes that are defined in the IP prefix list. After the parameter **ip-prefix** is configured on an LSR, the LSR sends only Label Mapping messages for labeled BGP routes that are defined in the IP prefix list to a specified peer. The parameter is specified by the **ip ip-prefix** command.	The value is an existing IP prefix list name.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends Label Mapping messages to both upstream and downstream LDP peers by default, speeding up LDP LSP convergence. This leads to the establishment of a great number of unwanted LSPs, wasting resources. To reduce the number of LSPs and save memory resources, configure an outbound or inbound policy to filter out LDP LSPs not matching the policy.

 Copyright © Huawei Technologies Co., Ltd.

To trigger the egress LSP using the BGP labeled route, run the **outbound peer bgp-label-route** command. You can specify the peer ID and FEC of the BGP labeled route in the command to configure the peer to receive only Label Mapping messages with specified BGP labeled routes, limiting the number of Label Mapping messages to be sent.

To apply a policy associated with a single FEC range to an LDP peer group or all LDP peers that send Label Mapping messages, configure either the **peer-group** *peer-group-name* or **all** parameter in the command.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

If multiple outbound policies are configured for a specified LDP peer, the first configured one takes effect. For example, the following two outbound policies are configured:

```
outbound peer 2.2.2.2 bgp-label-route ip-prefix prefix1
outbound peer peer-group group1 bgp-label-route none
```

As group1 also contains an LDP peer with *peer-id* of 2.2.2.2, the following outbound policy takes effect:

```
outbound peer 2.2.2.2 bgp-label-route ip-prefix prefix1
```

If two outbound policies are configured in sequence and the **peer** *peer-id* parameters in the two commands are the same, the second command overrides the first one. For example, the following two outbound policies are configured:

```
outbound peer 2.2.2.2 bgp-label-route ip-prefix prefix1
outbound peer 2.2.2.2 bgp-label-route none
```

The second configuration overrides the first one. This means that the following outbound policy takes effect on the LDP peer with *peer-id* of 2.2.2.2:

```
outbound peer 2.2.2.2 bgp-label-route none
```

Creating a peer group before it is referenced is recommended. By default, nonexistent peer groups cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is referenced using the current command, the current command applies to all LDP peers.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the route-policy nonexistent-config-check disable command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device advertises Label Mapping messages of all public-network BGP labeled routes to the specified peer.

Example

Configure an LSR to send Label Mapping messages for labeled BGP routes defined in IP prefix list named **prefix1** to all peers.

```
<Huawei> system-view
[Huawei] ip ip-prefix prefix1 permit 2.2.2.2 24
[Huawei] mpls ldp
[Huawei-mpls-ldp] outbound peer all bgp-label-route ip-prefix prefix1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

11.1.55 inbound peer fec

11.1.102 outbound peer fec

11.1.103 outbound peer split-horizon

11.1.102 outbound peer fec

Function

The **outbound peer fec** command configures an outbound policy to send Label Mapping messages to a specified peer based on the specified IGP route.

The **undo outbound peer fec** command restores the default configuration.

By default, no outbound policy is configured to allow label mapping messages carrying a specified IGP route to be sent to a specified peer.

Format

outbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec** { **none** | **host** | **ip-prefix** *prefix-name* }

undo outbound peer { *peer-id* | **peer-group** *peer-group-name* | **all** } **fec**

Parameters

Parameter	Description	Value
peer-id	Specifies the ID of an LDP peer. By default, the peer ID is specified by the **mpls lsr-id** command. If the **lsr-id** command has been configured, the peer ID is specified by the **lsr-id** command.	The value is in dotted decimal notation.
peer-group *peer-group-name*	Specifies the name of a peer group.	The name is a string of 1 to 169 characters without spaces. It is case-sensitive.
all	Indicates all LDP peers.	-
none	Prohibits Label Mapping messages carrying routes mapped to all FECs from passing the policy. After the parameter **none** is configured, no Label Mapping messages carrying IGP routes mapped to all FECs are sent to a specified peer.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host	Allows Label Mapping messages carrying the host routes mapped to FECs to pass the policy. After the parameter **host** is configured, Label Mapping messages carrying host routes mapped to all FECs are sent to a specified peer.	-
ip-prefix *prefix-name*	Allows Label Mapping messages carrying IGP routes that are defined in the IP prefix list and mapped to FECs to pass the policy. After the parameter **ip-prefix** is configured, Label Mapping messages carrying IGP routes that are defined in the IP prefix list and mapped to FECs are sent to a specified peer. The parameter is specified by the **ip ip-prefix** command.	The name is a string of 1 to 169 characters without spaces. It is case-sensitive.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends label mapping messages to both upstream and downstream LDP peers by default, speeding up LDP LSP convergence. This leads to the establishment of a great number of unwanted LSPs, wasting resources. To reduce the number of LSPs and save memory resources, configure an outbound or inbound policy to filter out LDP LSPs not matching the policy.

When running the **outbound peer fec** command to specify the peer ID and FEC of the IGP route, configure the peer to receive only label mapping messages for specified IGP routes. This setting helps reduce the number of Label Mapping messages to be sent.

To apply a policy associated with a single FEC range to an LDP peer group or all LDP peers that send Label Mapping messages, configure either the **peer-group** *peer-group-name* or **all** parameter in the command.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

If multiple outbound policies are configured for a specified LDP peer, the first configured one takes effect. For example, the following two outbound policies are configured:

 Copyright © Huawei Technologies Co., Ltd.

```
outbound peer 2.2.2.2 fec host
outbound peer peer-group group1 fec none
```

As group1 also contains an LDP peer with *peer-id* of 2.2.2.2, the following outbound policy takes effect:

```
outbound peer 2.2.2.2 fec host
```

If two outbound policies are configured in sequence and the **peer** parameters in the two commands are the same, the second command overrides the first one. For example, the following two outbound policies are configured:

```
outbound peer 2.2.2.2 fec host
outbound peer 2.2.2.2 fec none
```

The second configuration overrides the first one. This means that the following outbound policy takes effect on the LDP peer with *peer-id* of 2.2.2.2:

```
outbound peer 2.2.2.2 fec none
```

NOTE

To delete all outbound policies in batches, run the **undo outbound peer all fec** command.

Creating a peer group before it is referenced is recommended. By default, nonexistent peer groups cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent peer group is referenced using the current command, the current command applies to all LDP peers.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device advertises Label Mapping messages of all LDP FECs to the specified peer.

Example

Configure an LSR to send Label Mapping messages carrying host routes to all peers.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] outbound peer all fec host
```

Related Topics

11.1.55 inbound peer fec

11.1.101 outbound peer bgp-label-route

11.1.103 outbound peer split-horizon

11.1.103 outbound peer split-horizon

Function

The **outbound peer split-horizon** command enables split horizon on an LSR to allow the LSR to distribute labels only to its upstream LDP peers.

The **undo outbound peer split-horizon** command restores the default setting.

By default, split horizon is not enabled, which means that an LSR distributes labels to both upstream and downstream LDP peers.

 Copyright © Huawei Technologies Co., Ltd.

Format

outbound peer { *peer-id* | **all** } **split-horizon**

undo outbound peer { *peer-id* | **all** } **split-horizon**

Parameters

Parameter	Description	Value
peer-id	Specifies the LSR ID of an LDP peer.	The value is in dotted decimal notation.
all	Indicates all LDP peers.	-

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An LSR sends Label Mapping messages to both upstream and downstream LDP peers by default, speeding up LDP LSP convergence. This leads to the establishment of a great number of unwanted LSPs, wasting resources. To reduce the number of LSPs and saving memory resources, run the **outbound peer** { *peer-id* | **all** } **split-horizon** command to configure an LDP split horizon policy, enabling the LSR to send Label Mapping messages only to upstream LDP peers.

In the **outbound peer split-horizon** command, configure either of the following parameters to prevent an LSR from distributing labels to specified downstream peers:

- *peer-id*: prevents the LSR from distributing labels to a specified downstream peer.
- **all**: prevents the LSR from distributing labels to all downstream peers.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

The **all** parameter takes preference over the *peer-id* parameter. For example, the **outbound peer all split-horizon** and then **outbound peer 2.2.2.2 split-horizon** commands are run, the **outbound peer all split-horizon** command can be saved in the configuration file and take effect, not the **outbound peer 2.2.2.2 split-horizon** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable split horizon for all LDP peers.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] outbound peer all split-horizon
```

11.1.104 ping lsp

Function

The **ping lsp** command checks the LSP connectivity and LSP forwarding status.

Format

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **ip** *destination-address mask-length* [*ip-address*] [**nexthop** *nexthop-address* | **draft6**]

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **te tunnel** *interface-number* [**hot-standby** | **primary**] [**draft6**] [**compatible-mode**]

ping lsp [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *interval* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * **vpn-instance** *vpn-name* **remote** *remote-address mask-length* [**vpn-frr-path**]

Parameters

Parameter	Description	Value
-a *source-ip*	Specifies the source IP address of MPLS Echo Request packets to be sent. If the source IP address is not specified, the IP address of the outbound interface from which MPLS Echo Request packets are sent is used as the source IP address.	-
-c *count*	Specifies the number of MPLS Echo Request packets to be sent. In the case of poor network quality, you can set this parameter to a comparatively large value to check the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-exp *exp-value*	Specifies the EXP value of MPLS Echo Request packets to be sent.	The value is an integer that ranges from 0 to 7. The default value is 0.

Parameter	Description	Value
-h *ttl-value*	Specifies the value of the TTL. Each time the **ping lsp** command is run, an MPLS Echo Request packet carrying a sequence number is sent. The sequence number of the MPLS Echo Request packet starts from 1 and is increased by 1. By default, a maximum of five MPLS Echo Request packets are sent. You can set the number of MPLS Echo Request packets to be sent through the parameter *ttl-value*. If the destination is reachable, the source can receive five MPLS Echo Reply packets from the destination, with sequence numbers corresponding to those of MPLS Echo Request packets. If the TTL field is decreased to 0 during packet forwarding, the router that the packet reaches sends an MPLS timeout packet to the source, indicating that the destination is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 64.
-m *interval*	Specifies the time to wait before sending the next MPLS Echo Request packet. Each time the source sends an MPLS Echo Request packet using the **ping lsp** command, the source waits a period of time (2000 ms by default) before sending the next MPLS Echo Request packet. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *interval*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets.	The value is an integer that ranges from 1 to 4. The default value is 2. ● 1: The peer does not return MPLS Echo Reply packets. ● 2: The peer end responds to MPLS Echo Reply packets with IPv4 or IPv6 User Datagram Protocol (UDP) packets. ● 3: The peer end responds to MPLS Echo Reply packets with IPv4 or IPv6 UDP packets containing the Router alert option. ● 4: The peer end responds to MPLS Echo Reply packets through the control channel on the application plane.
-s *packet-size*	Indicates the length of the payload in a packet, excluding the IP header and UDP header.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100. The configured value must be smaller than the MTU of the interface. The value must be smaller than the MTU value of the interface.
-t *time-out*	Indicates the timeout period to wait for an MPLS Echo Reply packet after an MPLS Echo Request packet is sent.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-v	Displays MPLS Echo Reply packets not for the local user. By default, only MPLS Echo Reply packets for the local user are displayed. ● If **-v** is not specified, the system displays only the MPLS Echo Reply packets received by the local user. ● If **-v** is specified, the system displays all received MPLS Echo Reply packets.	By default, the system displays only the MPLS Echo Reply packets received by the local user.
ip *destination-address mask-length*	Specifies the IPv4 address and mask length of the destination.	The destination IPv4 address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.
ip-address	Specifies the destination IP address carried in the IP header of an MPLS Echo Request packet.	The value is in dotted decimal notation. By default, the destination IP address carried in the IP header of an MPLS Echo Request packet is 127.0.0.1.
nexthop *nexthop-address*	Specifies the IP address of the next hop.	The value is in dotted decimal notation.
draft6	Specifies the version of the **ping lsp** command. If this parameter is specified, the ping operation is performed according to "draft-ietf-mpls-lsp-ping-06".	-
compatible-mode	Indicates that the compatible mode is specified for protocols used in the LSP ping.	-
te tunnel *interface-number*	Specifies the number of a tunnel interface.	-
hot-standby	Indicates that the hot-standby CR-LSP is to be detected.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
primary	Indicates that the primary CR-LSP is to be monitored.	-
vpn-instance *vpn-name*	Specifies the name of a VPN instance.	The value is an existing VPN instance name.
remote *remote-address mask-length*	Specifies the IP address of the device to be detected. By default, the system searches for the IP address of the next hop based on the PW on the local PE. In the case of the MS-PW, if the ping operation is performed in control word mode, the IP address of the destination must be specified; if the ping operation is performed in MPLS Router Alert mode, the IP address of the destination or any transit node can be specified. When the Echo Request packet reaches the destination, an Echo Reply packet is returned and the Echo Request packet is no longer forwarded.	The IP address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.
vpn-frr-path	Indicates that the connectivity of the backup VPN FRR LSP will be checked.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

On an MPLS network, you can run the **ping lsp** command to check LSP connectivity after an LSP is established.

The LSP ping can be used to monitor the following types of links:

- LDP LSP Ping: Run the **ping lsp ip** *destination-address mask-length* command on the ingress node to ping the egress node to monitor the connectivity of the LSP.
- TE Tunnel Ping: If a tunnel exists, run the **ping lsp te tunnel** *interface-number* command on the ingress node to ping the egress node to monitor the connectivity of the tunnel.
- L3VPN LSP Ping: After a VPN is correctly configured, run the **ping lsp vpn-instance** *vpn-name* **remote** *remote-address mask-length* command on the

ingress node to ping the egress node to monitor the connectivity of the VPN LSP established using BGP.

If the **ping lsp** command detects a fault on an LSP that packets transmitted along this LSP cannot reach the egress node, you can run the **tracert lsp** command to locate the fault.

Prerequisites

Before running the **ping lsp** command, ensure that the MPLS module is working properly.

Precautions

When you detect a L3VPN LSP, if the destination of the ping operation is a CE address, the ping can be successful even when the link between the CE and PE is faulty. This is because the end-to-end link between PEs is detected.

To prevent the egress node from forwarding the received MPLS Echo Request packet to other nodes, the destination address in the IP header of the Echo Request packet is set to 127.0.0.1/8 (the local loopback address), and the TTL value contained in the IP header is set to 1.

Example

Ping 4.4.4.9/32 by sending ten 200-byte MPLS Echo Request packets.

```
<Huawei> ping lsp -c 10 -s 200 ip 4.4.4.9 32
  LSP PING FEC: IPV4 PREFIX 4.4.4.9/32/ : 200 data bytes, press CTRL_C to break
    Reply from 4.4.4.9: bytes=200 Sequence=1 time = 11 ms
    Reply from 4.4.4.9: bytes=200 Sequence=2 time = 6 ms
    Reply from 4.4.4.9: bytes=200 Sequence=3 time = 6 ms
    Reply from 4.4.4.9: bytes=200 Sequence=4 time = 6 ms
    Reply from 4.4.4.9: bytes=200 Sequence=5 time = 12 ms
    Reply from 4.4.4.9: bytes=200 Sequence=6 time = 9 ms
    Reply from 4.4.4.9: bytes=200 Sequence=7 time = 12 ms
    Reply from 4.4.4.9: bytes=200 Sequence=8 time = 9 ms
    Reply from 4.4.4.9: bytes=200 Sequence=9 time = 12 ms
    Reply from 4.4.4.9: bytes=200 Sequence=10 time = 12 ms

  --- FEC: IPV4 PREFIX 4.4.4.9/32 ping statistics ---
    10 packet(s) transmitted
    10 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 6/10/12 ms
```

Ping an MPLS TE tunnel.

```
<Huawei> ping lsp te tunnel 0/0/1
  LSP PING FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1 : 100 data bytes, press CTRL_C to break
    Reply from 20.1.1.2: bytes=100 Sequence=1 time = 50 ms
    Reply from 20.1.1.2: bytes=100 Sequence=2 time = 28 ms
    Reply from 20.1.1.2: bytes=100 Sequence=3 time = 33 ms
    Reply from 20.1.1.2: bytes=100 Sequence=4 time = 52 ms
    Reply from 20.1.1.2: bytes=100 Sequence=5 time = 8 ms
  --- FEC: TE TUNNEL IPV4 SESSION QUERY Tunnel0/0/1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 8/34/52 ms
```

Ping 3.3.3.3/32 and output detailed information.

```
<Huawei> ping lsp -v ip 3.3.3.3 32
  LSP PING FEC: IPV4 PREFIX 3.3.3.3/32 : 100 data bytes, press CTRL_C to break
    Reply from 3.3.3.3: bytes=100 Sequence=1 time = 4 ms Return Code 3, Subcode 1
    Reply from 3.3.3.3: bytes=100 Sequence=2 time = 4 ms Return Code 3, Subcode 1
```

```
  Reply from 3.3.3.3: bytes=100 Sequence=3 time = 4 ms Return Code 3, Subcode 1
  Reply from 3.3.3.3: bytes=100 Sequence=4 time = 4 ms Return Code 3, Subcode 1
  Reply from 3.3.3.3: bytes=100 Sequence=5 time = 5 ms Return Code 3, Subcode 1
--- FEC: IPV4 PREFIX 3.3.3.3/32 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 4/4/5 ms
```

Table 11-45 Description of the **ping lsp** command output

Item	Description
Reply from	IP address in an Echo Reply packet.
bytes	Length of an Echo Reply packet.
Sequence	Serial number of an Echo Reply packet.
time	RTT of an Echo Reply packet.
Return Code	Return code. The meaning of each value is as follows: ● 0: No return code is received. ● 1: Incorrect request is received. ● 2: An unknown TLV is received. ● 3: There is the outbound interface of one LSP. ● 4: No mapping between the request device and the replying device exists. ● 5: The mapping does not match that on the downstream device. ● 6: An unknown upstream interface exists. ● 7: The return code is reserved. ● 8: indicates label switching. ● 9: indicates label switching without MPLS forwarding. ● 10: indicates mapping without labels. ● 11: indicates the entity without labels. ● 12: No protocol is loaded on the interface. ● 13: The ping operation is ended ahead of schedule because of shortened labels.
Subcode	Number of labels. Usually, the value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
xxx ping statistics	Statistics collected after the ping test. The statistics include the following information: • packet(s) transmitted: indicates the number of sent ICMP Echo Request messages. • packet(s) received: indicates the number of received ICMP Echo Reply messages. • % packet loss: indicates the percentage of unresponded messages to total sent messages. • round-trip min/avg/max: indicates the minimum, average, and maximum RTTs. The unit is ms.

Related Topics

11.1.125 tracert lsp

11.1.105 propagate mapping

Function

The **propagate mapping for ip-prefix** command allows the system to filter out the received routes using an IP prefix list. LDP uses routes that match the addresses in the prefix list to establish a LSP.

The **undo propagate mapping** command restores the default setting.

By default, when LDP establishes a LSP, LDP does not filter out received routes.

Format

propagate mapping for ip-prefix *ip-prefix-name*

undo propagate mapping

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list used to filter out routes.	The value is an existing IP prefix list name.

Views

MPLS-LDP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MPLS LDP is enabled, LDP LSPs are automatically established, leading to a large number of LSPs and wasting resources. Run the **propagate mapping** command to configure a policy for establishing a LSP, allowing LDP to use routes that match the specified conditions to establish LSPs.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp (system view)** command.

Precautions

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, the device does not filter received routes.

Example

Allow routes that match the IP prefix list named **policy1** to set up a LSP.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] propagate mapping for ip-prefix policy1
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.67 lsp-trigger

11.1.106 proxy-egress disable

Function

The **proxy-egress disable** command disables a device from establishing proxy egress LSPs.

The **undo proxy-egress disable** command enables a device to establish proxy egress LSPs.

By default, a device is enabled to establish proxy egress LSPs.

Format

proxy-egress disable

undo proxy-egress disable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a policy allows a device to use all static and IGP routes to establish LSPs or use an IP address prefix list to establish LSPs, the policy also triggers proxy egress LSP establishment. However, the proxy egress LSPs may be unavailable, which wastes system resources. To prevent this problem, run the **proxy-egress disable** command to disable a device from establishing such proxy egress LSPs.

Prerequisites

MPLS has been enabled using the **11.1.75 mpls (system view)** command.

Example

Disable a device from establishing proxy egress LSPs in the MPLS view.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] proxy-egress disable
```

Related Topics

11.1.67 lsp-trigger

11.1.107 remote-ip

Function

The **remote-ip** command allows you to assign an IP address to a remote LDP peer.

The **undo remote-ip** command deletes the configuration.

By default, the IP address of the remote LDP peer is not configured.

Format

remote-ip *ip-address* [**pwe3**]

undo remote-ip [**pwe3**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a remote peer.	The value is in decimal notation. The IPv4 address of a local interface is not supported.
pwe3	Prohibits labels from being distributed to a specified remote peer.	-

Views

Remote MPLS LDP peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a remote LDP peer is configured, to assign an IP address to the remote LDP peer, run the **remote-ip** command in the remote MPLS LDP peer view.

The IP address must be the LSR ID of the remote LDP peer. When the LDP LSR ID and the MPLS LSR ID are different, the LDP LSR ID takes effect.

The remote peer uses the LSR ID as the transport address to create a TCP connection.

PEs on both ends of an MPLS L2VPN that runs LDP signaling can establish a remote LDP session. The MPLS L2VPN can be a Martini VLL network. The remote LDP session is expected to transmit Label Mapping messages carrying VC labels, not LDP labels. By default, the PE distributes LDP labels to its peer. To disable the PE from distributing LDP labels to its peer, run either of the following commands, which helps prevent LDP label wastes and minimize memory usage.

- **remote-ip** *ip-address* **pwe3** command: prevents the LSR from distributing labels to a specified remote peer.
- **remote-peer** **pwe3** command: prevents the LSR from distributing labels to all remote peers.

Prerequisites

Remote LDP peers have been configured.

Precautions

- Modifying or deleting the configured IP address of a remote peer leads to the deletion of a remote LDP session.

 Copyright © Huawei Technologies Co., Ltd.

- After a remote peer IP address is specified using the **remote-ip** *ip-address* command, *ip-address* cannot be used as a local interface IP address. If it is used as a local interface IP address, the remote LDP session is interrupted.

Example

Configure the address for a remote peer.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer bji
[Huawei-mpls-ldp-remote-bji] remote-ip 10.3.3.3
```

Prohibit labels from being distributed to the remote peer at 10.1.1.1/32.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer rtc
[Huawei-mpls-ldp-remote-rtc] remote-ip 10.1.1.1 pwe3
```

Related Topics

11.1.85 mpls ldp remote-peer

11.1.110 remote-peer pwe3

11.1.108 remote-ip auto-dod-request

Function

The **remote-ip auto-dod-request** command configures automatic triggering of a request to a specified downstream remote LDP peer for a Label Mapping message in DoD mode.

The **undo remote-ip auto-dod-request** command restores the default setting.

By default, the configuration of the **remote-peer auto-dod-request** command is inherited.

Format

remote-ip auto-dod-request [**block**]

undo remote-ip auto-dod-request [**block**]

Parameters

Parameter	Description	Value
block	Disables the automatic triggering of a request to a downstream node for a Label Mapping message associated with a remote LDP peer of a specified LSR ID in DoD mode.	-

Views

Remote MPLS LDP peer view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale network, to reduce the burden on edge devices, use the DoD mode. Because edge devices cannot learn the accurate route to the remote peer, an LDP LSP cannot be set up even if LDP extensions for inter-area LSPs are configured. You can configure the DoD mode in which the local LSR requests a Label Mapping message from a specified downstream LSR or all LSRs to set up an LDP LSP.

To block this function, run the **remote-ip auto-dod-request block** command.

Prerequisites

Before running the **remote-ip auto-dod-request** command, ensure that the following operations has been performed:

- Configure a remote LDP session.
- Run the **longest-match** command to configure LDP extensions for inter-area LSPs.
- Run the **mpls ldp advertisement dod** command to set the DoD mode.

Example

Enable automatic triggering of a request to a downstream specified remote LDP peer for a Label Mapping message in DoD mode.

```
<Huawei> system-view
[Huawei] mpls ldp remote-peer lsrc
[Huawei-mpls-ldp-remote-lsrc] remote-ip 4.4.4.4
[Huawei-mpls-ldp-remote-lsrc] remote-ip auto-dod-request
```

Related Topics

11.1.65 longest-match

11.1.81 mpls ldp advertisement

11.1.109 remote-peer auto-dod-request

11.1.109 remote-peer auto-dod-request

Function

The **remote-peer auto-dod-request** command configures automatic triggering of a request to all downstream remote LDP peers for a Label Mapping message in DoD mode.

The **undo remote-peer auto-dod-request** command restores the default setting.

By default, this function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

remote-peer auto-dod-request

undo remote-peer auto-dod-request

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a large-scale network, to reduce the burden on edge devices, use the DoD mode. Because edge devices cannot learn the accurate route to the remote peer, an LDP LSP cannot be set up even if LDP extensions for inter-area LSPs are configured. You can configure the DoD mode in which the local LSR requests a Label Mapping message from a specified downstream LSR or all LSRs to set up an LDP LSP.

Prerequisites

Before running the **remote-peer auto-dod-request** command, ensure that the following operations have been performed:

- Configure a remote LDP session.
- Run the **longest-match** command to configure LDP extensions for inter-area LSPs.
- Run the **mpls ldp advertisement dod** command to set the DoD mode.

Example

Enable automatic triggering of a request to all downstream remote LDP peers for a Label Mapping message in DoD mode.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] remote-peer auto-dod-request
Warning: The operation will affect all the remote peers on which the attribute is not manually configured.
Continue? [Y/N]: y
```

Related Topics

11.1.108 remote-ip auto-dod-request

11.1.110 remote-peer pwe3

Function

The **remote-peer pwe3** command prevents public network labels from being distributed to all remote peers.

The **undo remote-peer pwe3** command restores the default setting.

By default, an LSR is permitted to distribute public network labels to all remote peers.

Format

remote-peer pwe3

undo remote-peer pwe3

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

PEs on both ends of an MPLS L2VPN that runs LDP signaling can establish a remote LDP session. The MPLS L2VPN can be a Martini VLL network. The remote LDP session is expected to transmit Label Mapping messages carrying VC labels, not LDP labels.

By default, the PE distributes LDP labels to its peer. To disable the PE from distributing LDP labels to its peer, run either of the following commands, which helps prevent LDP label wastes and minimize memory usage.

- The **remote-peer pwe3** command prohibits an LSR from distributing labels to all remote peers.
- The **remote-ip** *ip-address* **pwe3** command in the remote MPLS LDP peer view prohibits an LSR from distributing labels to a specified remote peer.

When you create a remote LDP session, run the **remote-peer pwe3** or **remote-ip** *ip-address* **pwe3** command to prevent public network labels from being distributed to remote peers. If you do not run either of the preceding commands, the command configuration may affect system performance.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

The configuration will take effect on all remote LDP peers, including existing remote peers.

Example

Prevent public network labels from being distributed to all remote peers.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] remote-peer pwe3
Warning: The modification has impact on all remote peers including the existing ones. Continue? [Y/N]: y
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.107 remote-ip

11.1.111 reset mpls ldp

Function

The **reset mpls ldp** command resets LDP instances of the public network.

The **reset mpls ldp all** command resets all LDP instances.

Format

reset mpls ldp [**peer** *peer-id*]

reset mpls ldp all

Parameters

Parameter	Description	Value
peer *peer-id*	Specifies the LSR ID of a peer.	Expressed in dotted decimal notation
all	Specifies all LDP instances.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When there is a new LDP configuration, to validate the configuration, you can run the **reset mpls ldp** command.

Run the **reset mpls ldp peer** command to reset sessions, and LSPs of a specified peer.

Precautions

The **reset mpls ldp** command cannot be run during GR.

Example

Reset the global LDP function.

```
<Huawei> reset mpls ldp
```

Reset all LDP instances.

```
<Huawei> reset mpls ldp all
```

Reset the peer.

```
<Huawei> reset mpls ldp peer 2.2.2.9
```

Related Topics

11.1.82 mpls ldp (system view)

11.1.112 reset mpls ldp error packet

Function

The **reset mpls ldp error packet** command deletes information about LDP-related error messages.

Format

reset mpls ldp error packet { **tcp** | **udp** | **all** }

Parameters

Parameter	Description	Value
tcp	Deletes information about TCP error messages.	-
udp	Deletes information about UDP error messages.	-
all	Deletes information about all LDP-related error messages.	-

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

By default, the system records information about LDP-related error messages. To delete the information, run the **reset mpls ldp error packet** command.

Example

Delete information about LDP-related TCP error messages.

```
<Huawei> reset mpls ldp error packet tcp
```

11.1.113 reset mpls ldp event adjacency-down

Function

The **reset mpls ldp event adjacency-down** command deletes the recorded events that LDP adjacencies go Down.

Format

reset mpls ldp event adjacency-down

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records the events that LDP adjacencies go Down. To delete the recorded events, run the **reset mpls ldp event adjacency-down** command.

Example

Delete the recorded events that LDP adjacencies go Down.

```
<Huawei> reset mpls ldp event adjacency-down
```

11.1.114 reset mpls ldp event session-down

Function

The **reset mpls ldp event session-down** command deletes the recorded events that LDP sessions go Down.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset mpls ldp event session-down

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

By default, the system records events that LDP sessions go Down. To delete the recorded events, run the **reset mpls ldp event session-down** command.

Example

Delete the recorded events that LDP sessions go Down.

```
<Huawei> reset mpls ldp event session-down
```

11.1.115 route recursive-lookup tunnel

Function

The **route recursive-lookup tunnel** command enables tunnel iteration.

The **undo route recursive-lookup tunnel** command disables tunnel iteration.

By default, tunnel iteration is disabled.

Format

route recursive-lookup tunnel [**only**] [**ip-prefix** *ip-prefix-name*]

undo route recursive-lookup tunnel

Parameters

Parameter	Description	Value
only	Iterates unlabeled public routes only to LSPs.	-
ip-prefix *ip-prefix-name*	Specifies the name of an IP-prefix list.	The value is an existing IP-prefix list name.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an unlabeled BGP public network route or a static route can only be iterated to the outbound interface and next hop, but not a tunnel. After tunnel iteration is enabled, this route is preferentially iterated to an LSP. If no LSP exists, the route can also be iterated to the outbound interface and next hop.

After **ip-prefix** *ip-prefix-name* is set, only the unlabeled BGP routes or static routes that match the specified IP prefix list are iterated to LSPs.

If the **ip-prefix** *ip-prefix-name* parameter is not set, all static routes and non-labeled public BGP routes will be preferentially iterated to LSP tunnels.

After the **route recursive-lookup tunnel** command is run, non-labeled public routes can be iterated to both LSPs and IP routes. Therefore, two equal-cost routes are available to balance traffic. If the link over the IP route fails, packets forwarded along the IP route are discarded, causing a service interruption. To prevent this problem, configure **only** in the command so that non-labeled public routes are iterated only to LSPs. If no LSPs are available, non-labeled public routes are not iterated.

Precautions

If the **route recursive-lookup tunnel** command is run for several times, the latest configuration overrides the previous one.

Example

Iterate the unlabeled public routes to the LSP tunnel.

```
<Huawei> system-view
[Huawei] route recursive-lookup tunnel
```

11.1.116 snmp-agent trap enable feature-name ldp

Function

The **snmp-agent trap enable feature-name ldp** command enables the trap for the MPLS LDP module.

The **undo snmp-agent trap enable feature-name ldp** command disables the trap for the MPLS LDP module.

By default, the trap is disabled for the MPLS LDP module.

 Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent trap enable feature-name ldp trap-name { **session-down-mib** | **session-pvl** | **session-retry** | **session-up-mib** }

undo snmp-agent trap enable feature-name ldp trap-name { **session-down-mib** | **session-pvl** | **session-retry** | **session-up-mib** }

Parameters

Parameter	Description	Value
trap-name	Enables the trap of MPLS LDP events of a specified type.	-
session-down-mib	Enables the trap of the event that an LDP session goes Down in the MIB.	-
session-pvl	Enables the trap of the PathVectorLimitMismatch event of an LDP session. The maximum path vector value in the received message is different from the one in the local setting.	-
session-retry	Enables the trap of the event that an LDP session is reestablished.	-
session-up-mib	Enables the trap of the event that an LDP session goes Up in the MIB.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **snmp-agent trap enable feature-name ldp** command to enable the LDP session trap. Currently, all traps of the MPLS LDP module are non-excessive trap. The frequent LDP session status changes do not trigger a large number of traps.

Example

Enable the trap of the event that an LDP session is reestablished.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name ldp trap-name session-retry
```

Related Topics

11.1.45 display snmp-agent trap feature-name ldp all

11.1.117 snmp-agent trap enable feature-name mpls_lspm

Function

The **snmp-agent trap enable feature-name mpls_lspm** command enables the trap for the MPLS LSPM module.

The **undo snmp-agent trap enable feature-name mpls_lspm** command disables the trap for the MPLS LSPM module.

By default, the trap is disabled for the MPLS LSPM module.

Format

snmp-agent trap enable feature-name mpls_lspm [**trap-name** *trapname*]

undo snmp-agent trap enable feature-name mpls_lspm [**trap-name** *trapname*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name *trapname*	Enables the trap of MPLS events of a specified type.	• hwmplsdynamiclabelthresholdexceed: Dynamic label usage reached the upper limit. • hwmplsdynamiclabelthresholdexceedclear: Dynamic label usage reached the lower limit. • hwmplsdynamiclabeltotalcountexceed: Dynamic label usage reached 100%. • hwmplsdynamiclabeltotalcountexceedclear: Dynamic label usage fell to 95%. • hwmplsexttunneldown: Enables the trap of the event that the TE tunnel changes to Down. • hwmplsexttunneldownclear: Enables the trap of the event that the TE tunnel Down alarm was cleared. • hwmplsldpvirtualtunneldown: Enables the trap of the event that an LDP virtual tunnel goes Down. • hwmplsldpvirtualtunnelup: Enables the trap of the event that an LDP virtual tunnel goes Up. • hwmplslspthresholdexceed: Enables the function to generate an alarm if the number of LSPs exceeds the alarm threshold. • hwmplslspthresholdexceedclear: Enables the function to clear an alarm if the number of LSPs falls below the alarm threshold. • hwmplslsptotalcountexceed: Enables the function to generate an alarm if the number of LSPs exceeds the maximum limit. • hwmplslsptotalcountexceedclear: Enables the function to clear an alarm if the number of LSPs falls below the maximum limit. • hwmplsoamais: Enables the trap of the event that the tunnel receives an alarm indication signal (AIS) alarm. • hwmplsoamaisrecovery: Enables the trap of the event that the AIS alarm received by the tunnel is cleared. • hwmplsoambdi: Enables the trap of the event that the tunnel receives a backward defect indication (BDI) alarm.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• hwmplsoambdirecovery: Enables the trap of the event that the BDI alarm received by the tunnel is cleared. • hwmplsoamexcess: Enables the trap of the event that the tunnel receives an Excess alarm. • hwmplsoamexcessrecovery: Enables the trap of the event that the Excess alarm received by the tunnel is cleared. • hwmplsoamfail: Enables the trap of the event that the tunnel receives an OAMFAIL alarm. • hwmplsoamfailrecovery: Enables the trap of the event that the OAMFAIL alarm received by the tunnel is cleared. • hwmplsoamlck: Enables the trap of the event that the tunnel receives an LCK alarm. • hwmplsoamlckrecovery: Enables the trap of the event that the LCK alarm received by the tunnel is cleared. • hwmplsoamlocallock: Enables the trap of the event that the tunnel receives a LOCK alarm. • hwmplsoamlocallockrecovery: Enables the trap of the event that the LOCK alarm received by the tunnel is cleared. • hwmplsoamloss: Enables the trap of the event that the tunnel receives a loss of continuity (LOC) alarm. • hwmplsoamlossrecovery: Enables the trap of the event that the LOC alarm received by the tunnel is cleared. • hwmplsoammeg: Enables the trap of the event that the tunnel receives an unexpected MEG alarm. • hwmplsoammegrecovery: Enables the trap of the event that the unexpected MEG alarm received by the tunnel is cleared. • hwmplsoammep: Enables the trap of the event that the tunnel receives an unexpected MEP alarm. • hwmplsoammeprecovery: Enables the trap of the event that the unexpected MEP alarm received by the tunnel is cleared. • hwmplsoammismatch: Enables the trap of the event that the tunnel receives a MisMatch alarm.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• hwmplsoammismatchrecovery: Enables the trap of the event that the MisMatch alarm received by the tunnel is cleared. • hwmplsoammismerge: Enables the trap of the event that the tunnel receives a MisMerge alarm. • hwmplsoammismergerecovery: Enables the trap of the event that the MisMerge alarm received by the tunnel is cleared. • hwmplsoamperiod: Enables the trap of the event that the tunnel receives an unexpected period alarm. • hwmplsoamperiodrecovery: Enables the trap of the event that the unexpected period alarm received by the tunnel is cleared. • hwmplsoamrdi: Enables the trap of the event that the tunnel receives a remote defect indication (RDI) alarm. • hwmplsoamrdirecovery: Enables the trap of the event that the RDI alarm received by the tunnel is cleared. • hwmplsoamsdrecovery: Enables the trap of the event that the local signal degrade threshold 1 alarm received by the tunnel is cleared. • hwmplsoamsf: Enables the trap of the event that the tunnel receives a local signal deterioration threshold 2 alarm. • hwmplsoamsfrecovery: Enables the trap of the event that the local signal deterioration threshold 2 alarm received by the tunnel is cleared. • hwmplsoamunknown: Enables the trap of the event that the tunnel receives an unknown alarm. • hwmplsoamunknownrecovery: Enables the trap of the event that the unknown alarm received by the tunnel is cleared. • hwmplsresourcethresholdexceed: Enables the function to generate an alarm if the number of used MPLS resources exceeds the alarm threshold. • hwmplsresourcethresholdexceedclear: Enables the function to clear an alarm if the number of used MPLS resources falls below the alarm threshold.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• hwmplsresourcetotalcountexceed: Enables the function to generate an alarm if the number of used MPLS resources exceeds the maximum limit. • hwmplsresourcetotalcountexceedclear: Enables the function to clear an alarm if the number of used MPLS resources falls below the maximum limit. • hwmplsstaticcrlspdown: Enables the private trap of the event that a static CR-LSP goes Down. • hwmplsstaticcrlspup: Enables the private trap of the event that a static CR-LSP goes Up. • hwmplsstaticlspdown: Enables the private trap of the event that a static LSP goes Down. • hwmplsstaticlspup: Enables the private trap of the event that a static LSP goes Up. • hwmplsteautotunneldownclear: Enables the trap of the event that the TE Auto tunnel Down alarm was cleared. • hwmplsteautotunnelprimarydownclear: Enables the trap of the event that the Down alarm about the primary LSP in the TE Auto tunnel was cleared. • hwmplstefrrprotaval: Enables the trap of the TE FRR bypass tunnel binding event. • hwmplstefrrprotnotaval: Enables the trap of the TE FRR bypass tunnel unbinding event. • hwmplstefrrresume: Enables the private trap of the event of TE FRR fault recovery. • hwmplstefrrswitch: Enables the private trap of the event of TE FRR protection switching. • hwmplstunnelbbresume: Enables the trap of main LSP of tunnel resumes from backup LSP in BBK. • hwmplstunnelbbswitch: Enables the trap of main LSP of tunnel switches to backup LSP in BBK. • hwmplstunnelbesteffortdown: Enables the trap of the event that the best-effort LSP of the tunnel changes to Down. • hwmplstunnelbesteffortup: Enables the trap of the event that the best-effort LSP of the tunnel changes to Up.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• hwmplstunnelchangebw: Enables the private trap of the event that the tunnel bandwidth changes. • hwmplstunneldelete: Enables the function to generate an alarm if an MPLS TE tunnel is deleted. • hwmplstunnelhotstandbydown: Enables the trap of the event that the hot-standby LSP of the tunnel changes to Down. • hwmplstunnelhotstandbyup: Enables the trap of the event that the hot-standby LSP of the tunnel changes to Up. • hwmplstunnelhsbresume: Enables the private trap of the event that traffic switches from the hot-standby CR-LSP to the primary CR-LSP. • hwmplstunnelhsbswitch: Enables the private trap of the event that traffic switches from the primary CR-LSP to the hot-standby CR-LSP. • hwmplstunnelobresume: Enables the private trap of the event that traffic switches from the ordinary backup CR-LSP to the primary CR-LSP. • hwmplstunnelobswitch: Enables the private trap of the event that traffic switches from the primary CR-LSP to the ordinary backup CR-LSP. • hwmplstunnelordinarydown: Enables the trap of the event that the ordinary LSP of the tunnel changes to Down. • hwmplstunnelordinaryup: Enables the trap of the event that the ordinary LSP of the tunnel changes to Up. • hwmplstunnelprimarydown: Enables the trap of the event that the primary LSP of the tunnel changes to Down. • hwmplstunnelprimaryup: Enables the trap of the event that the primary LSP of the tunnel changes to Up. • mplstunneldown: Enables the trap of the event that a tunnel goes Down. • mplstunnelreoptimized: Enables the trap of the tunnel reoptimization event.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• mplstunnelrerouted: Enables the trap of the tunnel reroute event. • mplstunnelup: Enables the trap of the event that a tunnel goes Up. • mplsxcdown: Enables the trap of the event that an LSP goes Down. • mplsxcup: Enables the trap of the event that an LSP goes Up.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **snmp-agent trap enable feature-name mpls_lspm** command to enable the MPLS LSPM module trap. Except **mplsxcup** and **mplsxcdown**, all traps of the MPLS LSPM module are non-excessive trap messages.

Example

Enables the trap of the event that a tunnel goes Up.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mpls_lspm trap-name mplstunnelup
```

11.1.118 snmp-agent trap suppress feature-name lsp

Function

The **snmp-agent trap suppress feature-name lsp** command configures the interval for suppressing the display of excessive LSP traps.

The **undo snmp-agent trap suppress feature-name lsp** command deletes the interval for suppressing the display of excessive LSP traps.

By default, the interval for suppressing the display of excessive LSP traps is 300 seconds, and a maximum of 3 LSP traps can be sent in the suppression interval.

Format

snmp-agent trap suppress feature-name lsp trap-name { **mplsxcup** | **mplsxcdown** } **trap-interval** *trap-interval* [**max-trap-number** *max-trap-number*]

undo snmp-agent trap suppress feature-name lsp trap-name { **mplsxcup** | **mplsxcdown** } **trap-interval**

Parameters

Parameter	Description	Value
mplsxcup	Indicates the excessive traps generated when an LSP goes Up.	-
mplsxcdown	Indicates the excessive traps generated when an LSP goes Down.	-
trap-interval *trap-interval*	Specifies the interval for suppressing the display of excessive LSP traps.	The value is an integer ranging from 0 to 65535, in seconds. By default, the value is 300.
max-trap-number *max-trap-number*	Sets the maximum number of traps to be sent during the suppression interval.	An integer ranging from 1 to 65535. If this parameter is not specified, three LSP trap can be sent in the suppression interval.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To prevent excessive traps from being displayed because of frequent LSP status changes, run the **snmp-agent trap suppress feature-name lsp** command to set the interval for suppressing the display of excessive LSP traps. During a specified suppression interval, a trap of a specified type is displayed only once. This setting reduces traps to be displayed.

For example, when the interval for suppressing the display of excessive traps when the LSP goes Down is set to 60s, only one trap indicating that the LSP goes Down is displayed every 60s. Within this interval, no other trap of the same type is displayed, but the number of the same traps generated is logged. During the next 60s, another trap indicating that an LSP goes Down can be displayed.

Example

Set the interval for suppressing the display of excessive traps when an LSP goes Up to 80s.

```
<Huawei> system-view
[Huawei] snmp-agent trap suppress feature-name lsp trap-name mplsxcup trap-interval 80
```

11.1.119 static-lsp egress

Function

The **static-lsp egress** command configures the egress node for a static LSP.

The **undo static-lsp egress** command deletes the configuration.

By default, no static LSP is configured for the egress node.

Format

static-lsp egress *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*]

undo static-lsp egress *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the inbound interface of an LSP. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
in-label	Specifies the value of an incoming label.	The value is an integer ranging from 16 to 1023.
lsrid *ingress-lsr-id*	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id *tunnel-id*	Specifies the ID of a tunnel.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Run the **static-lsp egress** command on the egress node to configure a static LSP.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify **incoming-interface** *interface-type interface-number* or **in-label** *in-label*, run the **static-lsp egress** command to set a new value. You do not need to run the **undo static-lsp egress** command before changing a configured value.

Example

Configure the local LSR as the egress node of the static LSP **bj-sh**, with the inbound interface of GE1/0/0 and incoming label of 233.

```
<Huawei> system-view
[Huawei] static-lsp egress bj-sh incoming-interface gigabitethernet 1/0/0 in-label 233
```

Related Topics

11.1.43 display mpls static-lsp

11.1.120 static-lsp ingress

11.1.121 static-lsp transit

11.1.120 static-lsp ingress

Function

The **static-lsp ingress** command configures the ingress node for a static LSP.

The **undo static-lsp ingress** command deletes the configuration.

By default, no static LSP is configured for the ingress node.

Format

static-lsp ingress *lsp-name* **destination** *ip-address* { *mask-length* | *mask* } { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label*

undo static-lsp ingress *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
destination *ip-address*	Specifies the destination IP address.	It is in dotted decimal notation.
mask-length	Specifies the mask length of the destination IP address.	An integer ranging from 0 to 32.
mask	Specifies the mask of the IP address.	It is in dotted decimal notation.
nexthop *next-hop-address*	Specifies the next-hop address.	It is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-
out-label *out-label*	Specifies the value of an outgoing label.	An integer ranging from 16 to 1048575.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp ingress** command on the ingress node to configure a static LSP.

NOTE

The local IP address cannot be designated as the next hop address.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify the parameter **destination** *destination-address*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, or **out-label** *out-label*, run the **static-lsp ingress** command to set a new value. You do not need to run the **undo static-lsp ingress** command before changing a configured value.

When configuring a static LSP, ensure that the route of the static LSP exactly matches the routing information. For example:

- If you specify a next hop when configuring a static LSP, specify a next hop when configuring a static IP route. If you do not specify a next hop, the static LSP cannot be set up. For example:

```
[Huawei] ip route-static 10.1.0.0 16 10.1.1.2
[Huawei] static-lsp ingress staticlsp1 destination 10.1.0.0 16 nexthop 10.1.1.2 out-label 100
```

- If a dynamic routing protocol applies to the link between LSRs, the next-hop IP address along the LSP must be the same as the IP address of the next hop in the routing table.

Precautions

If **outgoing-interface** is configured and *next-hop-address* is not configured, Ethernet forwarding failures occur.

Example

Configure the local LSR as the ingress node of the static LSP whose destination address is 10.25.38.1, next hop IP address is 10.55.25.33, and outgoing label is 237.

```
<Huawei> system-view
[Huawei] static-lsp ingress bj-sh destination 10.25.38.1 24 nexthop 10.55.25.33 out-label 237
```

Related Topics

11.1.43 display mpls static-lsp
11.1.119 static-lsp egress
11.1.121 static-lsp transit

11.1.121 static-lsp transit

Function

The **static-lsp transit** command configures the transit node for the static LSP.

The **undo static-lsp transit** command deletes the configuration.

By default, the transit node for the static LSP is not configured.

Format

static-lsp transit *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* }* **out-label** *out-label*

undo static-lsp transit *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface	Specifies the inbound interface.	-
interface-type interface-number	Specifies the type and number of an interface.	-
next-hop-address	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface	Specifies the outbound interface.	-
in-label	Specifies the value of an incoming label.	The value is an integer ranging from 16 to 1023.
out-label	Specifies the value of an outgoing label.	The value is an integer ranging from 16 to 1048575.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **static-lsp transit** command on the transit node to configure a static LSP.

After configuring a static LSP, run the **display mpls static-lsp** command to verify that the static LSP is established successfully.

Precautions

To modify the parameter **incoming-interface** *interface-type interface-number*, **in-label** *in-label*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, or **out-label** *out-label*, run the **static-lsp transit** command to set a new value. You do not need to run the **undo static-lsp transit** command before changing a configured value.

If **outgoing-interface** is configured and *next-hop-address* is not configured, Ethernet forwarding failures occur.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the LSR, with the inbound interface of GE1/0/0, the incoming label of 123, and the outgoing label of 253, as the transit node of a static LSP named **bj-sh**.

```
<Huawei> system-view
[Huawei] static-lsp transit bj-sh incoming-interface gigabitethernet 1/0/0 in-label 123 nexthop
10.1.2.3 out-label 253
```

Related Topics

11.1.43 display mpls static-lsp

11.1.119 static-lsp egress

11.1.120 static-lsp ingress

11.1.122 static-route timer ldp-sync hold-down

Function

The **static-route timer ldp-sync hold-down** command sets the time during which a static route remains inactive and waits for the establishment of an LDP session.

The **undo static-route timer ldp-sync hold-down** command restores the default setting.

By default, the time during which a static route remains inactive and waits for the establishment of an LDP session is 10 seconds.

Format

static-route timer ldp-sync hold-down { *timer* | **infinite** }

undo static-route timer ldp-sync hold-down

Parameters

Parameter	Description	Value
timer	Specifies the time during which a static route remains inactive and waits for an LDP session to be established.	The value is an integer ranging from 0 to 65535, in seconds.
infinite	Indicates that the Hold-down timer never expires. A static route becomes active only after an LDP session is established.	-

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

On an MPLS network with primary and backup links, LSRs establish LSPs based on static routes. When the LDP session of the primary link becomes faulty (the fault is not caused by a link failure) or the primary link recovers, configuring synchronization between LDP and static routes minimizes traffic loss during traffic switchover and switchback. After synchronization between LDP and static routes is enabled, and the **static-route timer ldp-sync hold-down** command is run, the recovered static route becomes temporarily inactive. It waits for the establishment of an LDP session before the Hold-down timer expires, which synchronizes LDP and the static route.

If the Hold-down timer expires, the static route becomes active regardless of whether an LDP session has been established.

- If the Hold-down timer is set to 0 seconds, synchronization between LDP and static routes is disabled on an interface.
- If the Hold-down timer is set to **infinite**, the timer never expires. In this case, the static route becomes active and MPLS traffic is switched only after an LDP session is established.

Precautions

The Hold-down timer cannot be set on loopback interfaces, Layer 2 Ethernet interfaces, or null interfaces.

Example

Set the time during which a static route remains inactive and waits for the establishment of an LDP session to 20 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] static-route timer ldp-sync hold-down 20
```

11.1.123 timer ldp-sync hold-down

Function

The **timer ldp-sync hold-down** command sets the Hold-down time for all IS-IS interfaces within an IS-IS process so that these interfaces remain in the Hold-down state before LDP sessions are established.

The **undo timer ldp-sync hold-down** command restores the default Hold-down time.

The default Hold-down time is 10 seconds.

Format

timer ldp-sync hold-down *value*

undo timer ldp-sync hold-down

Parameters

Parameter	Description	Value
value	Specifies the period of time during which all IS-IS interfaces within an IS-IS process remain in the Hold-down state before LDP sessions are established.	The value is an integer ranging from 0 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an active link between two devices enabled with synchronization between LDP and IS-IS recovers from a fault, the IS-IS module enters the Hold-down state and starts a Hold-down timer. This timer allows the devices to create an LDP session and set up an IS-IS neighbor relationship at the same time. Traffic can be switched back to the active link over a reachable IS-IS route for an established LDP LSP.

To set the Hold-down time for all interfaces within an IS-IS process, run the **timer ldp-sync hold-down** command.

Precautions

If both the **timer ldp-sync hold-down** command and the **isis timer ldp-sync hold-down** command in the interface view are executed, the **isis timer ldp-sync hold-down** command takes effect.

Example

Set the Hold-down time for all interfaces within an IS-IS process to **15** seconds.

```
<Huawei> system-view
[Huawei] isis 100
[Huawei-isis-100] timer ldp-sync hold-down 15
```

11.1.124 timer ldp-sync hold-max-cost

Function

The **timer ldp-sync hold-max-cost** command sets the Hold-max-cost time during which all interfaces enabled with synchronization between LDP and IS-IS advertise link state PDUs (LSPs) carrying the maximum route cost.

The **undo timer ldp-sync hold-max-cost** command restores the default setting.

The default Hold-max-cost time is 10 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

timer ldp-sync hold-max-cost { **infinite** | *interval* }

undo timer ldp-sync hold-max-cost

Parameters

Parameter	Description	Value
infinite	Enables IS-IS to advertise LSPs carrying the maximum route cost before LDP sessions are reestablished.	-
interval	Specifies the Hold-max-cost time during which IS-IS advertises LSPs carrying the maximum route cost on a local device.	The value is an integer ranging from 0 to 65535, in seconds.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After synchronization between LDP and IS-IS is enabled, if the LDP session over the active link fails but the IS-IS route for the active link is reachable, IS-IS advertises the LSPs carrying the maximum route cost so that the IS-IS route and LDP session over a standby link can become reachable at the same time.

To set the Hold-max-cost time, run the **timer ldp-sync hold-max-cost** command.

Select parameters based on networking requirements:

- If an IGP carries only LDP services, configure the parameter **infinite** to ensure that a selected IGP route is kept consistent with the LDP LSP.
- If an IGP carries multiple types of services including LDP services, set the value of the parameter *interval* to ensure that a teardown of LDP sessions does not affect IGP route selection or other services.

Precautions

- If the **timer ldp-sync hold-max-cost infinite** command is executed and the LDP session is Down, interfaces enabled with LDP and IS-IS synchronization keep advertising LSPs carrying the maximum route cost, which affects IS-IS routing.
- If both the **timer ldp-sync hold-max-cost** command and the **isis timer ldp-sync hold-max-cost** command in the interface view are executed, the **isis timer ldp-sync hold-max-cost** command takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure IS-IS to keep advertising the maximum cost by sending Link State PDUs until the LSP is established.

```
<Huawei> system-view
[Huawei] isis 100
[Huawei-isis-100] timer ldp-sync hold-max-cost infinite
```

11.1.125 tracert lsp

Function

The **tracert lsp** command detects the gateways along the LSP from the source to the destination.

Format

tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out* | **-v**] * **ip** *destination-address mask-length* [*ip-address*] [**nexthop** *nexthop-address* | **draft6**]

tracert lsp [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* | **-t** *time-out*] * **te tunnel** *interface-number* [**hot-standby** | **primary**] [**draft6**] [**compatible-mode**]

Parameters

Parameter	Description	Value
-a *source-ip*	Specifies the source IP address of Echo Request packets to be sent. If no source IP address is specified, the IP address of the outbound interface through which Echo Request packets are sent is used as a source IP address.	-
-exp *exp-value*	Specifies the EXP value of Echo Request packets to be sent. The EXP value represents the priority of Echo Request packets.	An integer that ranges from 0 to 7. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-h *ttl-value*	Specifies the TTL value of MPLS Echo Request packets to be sent. The TTL field indicates the lifetime of the MPLS Echo Request packet and specifies the maximum number of hops that the packet can pass through. The TTL value is set on the source and reduced by 1 each time the packet passes through a hop. When the TTL value is reduced to 0, the packet is discarded. At the same time, an ICMP Timeout message is sent to notify the source host.	An integer that ranges from 1 to 255. The default value is 30.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets.	An integer that ranges from 1 to 4. The default value is 2. The meaning of each value is as follows: ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated into IPv4 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated into IPv4 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are responded using the control channels on the application plane. If the value of *reply-mode* is 1, the initiator starts a unidirectional test. If the test succeeds, the initiator prompts that the test times out; if the test fails, the initiator prompts that the LSP does not exist.
-t *time-out*	Specifies the period of time for waiting for an MPLS Echo Reply packet.	An integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet. This parameter is used when public network labels need to be displayed after tracert is initiated on the PE.	-
ip *destination-address mask-length*	Specifies the destination IPv4 address and the mask length.	The destination IPv4 address is in dotted decimal notation. The mask length is an integer that ranges from 0 to 32.
ip-address	Specifies the destination IP address carried in the IP header of an MPLS Echo Request packet.	The value is in dotted decimal notation. By default, the destination IP address carried in the IP header of an MPLS Echo Request packet is 127.0.0.1.
nexthop *nexthop-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
draft6	Specifies the version of the **tracert lsp** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". By default, the tracert operation is performed according to RFC 4379.	-
compatible-mode	Indicates that the compatible mode is specified for protocols used in the LSP ping.	-
te tunnel *interface-number*	Specifies the number of the TE tunnel interface.	-
hot-standby	Indicates that the hot-standby CR-LSP is to be monitored.	-
primary	Indicates that the primary CR-LSP is to be monitored.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When a fault occurs on the LSPs of an MPLS network, you can run the **ping lsp** command to check the LSP connectivity based on the reply packet, and then run the **tracert lsp** command to locate the fault.

The LSP tracert can be used to monitor the following types of links:

- LDP LSP Tracert: Run the **tracert lsp ip** *destination-address mask-length* command on the ingress node to trace the egress node to detect the fault on the LSP.
- TE Tunnel Tracert: You can run the **tracert lsp te tunnel** *interface-number* command on the ingress node to trace the egress node to check the connectivity of a tunnel.
  - To check the connectivity of a hot-standby tunnel, run the **tracert lsp te tunnel** *interface-number* **hot-standby** command.

Prerequisites

- The UDP module of each node is working properly; otherwise, the tracert operation fails.
- The MPLS module of each node is enabled and is working properly.
- The ICMP module of each node is working properly; otherwise, three asterisks (* * *) are displayed.

Procedure

The execution process of the **tracert lsp** command is as follows:

- The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
- The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
- The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
- The preceding process proceeds until the MPLS Echo Request packet reaches the destination.

When the device on the destination hop receives the MPLS Echo Request packet, it returns an MPLS Echo Reply packet, indicating the end of the tracert. The purpose behind this is to record the source of each ICMP Timeout packet to provide a trace of the path the packet took to reach the destination.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When you run the **tracert lsp te tunnel** *interface-number* command to detect a tunnel, if a transit node is not enabled with LDP, a packet is returned, indicating that the destination is unreachable.

To prevent the egress node from forwarding the received MPLS Echo Request packet to other nodes, you can set the destination address in the IP header of the Echo Request packet to a loopback address with the prefix being 127.0.0.1/8.

Example

Tracert the LSP to 8.4.4.9/32.

```
<Huawei> tracert lsp ip 8.4.4.9 32
 LSP Trace Route FEC: IPV4 PREFIX 8.4.4.9/32 , press CTRL_C to break.
 TTL   Replier          Time    Type      Downstream
 0                        Ingress   9.1.2.2/[1028 ]
 1     9.1.2.2          94 ms   Transit   8.4.4.9/[3 ]
 2     8.4.4.9          94 ms   Egress
```

Tracert the LSP to 7.3.3.9/32 and configure the packets to carry the MTU value.

```
<Huawei> tracert lsp -v ip 7.3.3.9 32
 LSP Trace Route FEC: IPV4 PREFIX 7.3.3.9/32 , press CTRL_C to break.
 TTL   Replier          Time    Type      Downstream/Label/MTU
 0                        Ingress   11.11.11.11/[3 ]/1500
 1     7.3.3.9          20 ms   Egress
```

Table 11-46 Description of the tracert lsp command output

Item	Description
TTL	Indicates the TTL value in an Echo Request packet. It represents the number of hops of the tunnel an Echo Request packet passes.
Replier	IP address of a switching node that returns an MPLS Echo Reply packet.
Time	RTT, in milliseconds.
Type	Type of a node. Available node types: ● Ingress node ● Transit node ● Egress node
Downstream	Address of a downstream device.
Label	Label of a downstream device.
MTU	Link Maximum Transmission Unit.

Related Topics

11.1.104 ping lsp

11.1.126 ttl expiration pop

Function

The **ttl expiration pop** command enables a device to use the local IP route to forward ICMP response packets after the MPLS TTL expires.

The **undo ttl expiration pop** command disables this function. Therefore, ICMP response packets are sent along LSPs.

By default, the LSR returns an ICMP packet using the local IP route if the received MPLS TTL-expired packet contains one label.

Format

ttl expiration pop

undo ttl expiration pop

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On an MPLS network, when an LSR receives MPLS packets with the TTL value of 1, the LSR generates an ICMP TTL-expired message.

The LSR returns the TTL-expired message to the sender in the following ways:

- If the LSR has a reachable route to the sender, it directly sends the TTL-expired message to the sender through the IP route.
- If the LSR has no reachable route to the sender, it forwards the TTL-expired message along the LSP. The egress node forwards the TTL-expired message to the sender.

In most cases, the received MPLS packet contains only one label and the LSR responds to the sender with the TTL-expired message using the first method. If the MPLS packet contains multiple labels, the LSR uses the second method.

The MPLS VPN packets may contain only one label when they arrive at an autonomous system boundary router (ASBR) on the MPLS VPN, or a superstratum PE (SPE) device in HoVPN networking. These devices have no IP routes to the sender, so they use the second method to reply to the TTL-expired messages.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The **undo mpls (system view)** command deletes all configurations of the **ttl expiration pop** command.

Example

Forward ICMP packets through an LSP after the MPLS TTL expires.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] undo ttl expiration pop
```

11.1.127 ttl propagate

Function

The **ttl propagate** command sets the TTL propagate mode of MPLS packets to uniform.

The **undo ttl propagate** command sets the TTL propagate mode of MPLS packets to pipe.

By default, the TTL propagate function is enabled and the MPLS TTL processing mode is uniform.

Format

ttl propagate

undo ttl propagate

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TTL processing modes include uniform and pipe:

- Uniform

  When IP packets reach the ingress node of an MPLS network, the IP TTL decreases by one and is mapped to the MPLS TTL field. In this manner, packets are processed in the standard mode used on the MPLS network. On the egress node, the MPLS TTL decreases by one and is mapped to the IP TTL field. The traceroute output shows the path that the packets pass by.

 Copyright © Huawei Technologies Co., Ltd.

- Pipe

  On an MPLS network, the IP TTL does not decrease by one at each hop. The traceroute output hides all the hops on the MPLS backbone network, as if the ingress node is directly connected to the egress node.

In MPLS VPN applications, the MPLS backbone network needs to be hidden to ensure network security. The pipe mode is recommended for private network packets.

Precautions

The **ttl propagate** command only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Example

Set the TTL propagate mode of MPLS packets to uniform.

```
<Huawei> system-view
[Huawei] ttl propagate
```

Related Topics

11.1.11 diffserv-mode

11.1.128 ttl propagate public

Function

The **ttl propagate public** command enables IP TTL propagation for MPLS packets of the public network.

The **undo ttl propagate public** command disables IP TTL propagation for MPLS packets of the public network.

By default, IP TTL propagation for MPLS packets of the public network is enabled.

Format

ttl propagate public

undo ttl propagate public

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **ttl propagate public** and **undo ttl propagate public** commands only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

Example

Enable the IP TTL propagation for MPLS packets of the public network.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] ttl propagate public
```

Related Topics

11.1.126 ttl expiration pop

11.1.129 ttl propagate vpn

Function

The **ttl propagate vpn** command enables IP TTL propagation for MPLS packets of the VPN.

The **undo ttl propagate vpn** command disables IP TTL propagation for MPLS packets of the VPN.

By default, IP TTL propagation is disabled for VPN packets.

Format

ttl propagate vpn

undo ttl propagate vpn

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **ttl propagate vpn** and **undo ttl propagate vpn** commands only take effect on LSPs that are to be set up. Before using the function on LSPs that have been set up, run the **reset mpls ldp** command to reestablish the LSPs.

 Copyright © Huawei Technologies Co., Ltd.

Configure the IP TTL propagation consistently on all PEs. If you enable the IP TTL propagation only on some PEs, the traceroute output may not reflect the real network situation.

Example

Enable the IP TTL propagation for MPLS packets of the VPN.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] ttl propagate vpn
```

Related Topics

11.1.126 ttl expiration pop

11.1.130 undo outbound peer all

Function

The **undo outbound peer all** command deletes all outbound policies.

Format

undo outbound peer all

Parameters

None

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before MPLS LDP is used, the **outbound peer fec**, **outbound peer bgp-label-route**, and **outbound peer split-horizon** commands need to be executed to configure an outbound policy to control LDP LSP establishments. If multiple outbound policies have been configured, run the **undo outbound peer all** command to simultaneously delete all the outbound policies.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

Precautions

Running the **undo outbound peer all** command deletes all outbound policies. Therefore, exercise caution when running this command.

Example

Delete all outbound policies.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] undo outbound peer all
```

Related Topics

11.1.102 outbound peer fec

11.1.101 outbound peer bgp-label-route

11.1.103 outbound peer split-horizon

11.1.131 undo inbound peer all

Function

The **undo inbound peer all** command deletes all inbound policies.

Format

undo inbound peer all

Parameters

None.

Views

MPLS-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To delete all inbound policies in batches, run the **undo inbound peer all** command.

Before MPLS LDP is used, the **inbound peer fec** command needs to be executed to configure an inbound policy to control LDP LSP establishments. If multiple inbound policies have been configured, run the **undo inbound peer all** command to simultaneously delete all the inbound policies.

Prerequisites

MPLS LDP has been enabled globally using the **mpls ldp** command in the system view.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Running the **undo inbound peer all** command deletes all inbound policies. Therefore, exercise caution when running this command.

Example

Delete all inbound policies.

```
<Huawei> system-view
[Huawei] mpls ldp
[Huawei-mpls-ldp] undo inbound peer all
```

Related Topics

11.1.55 inbound peer fec

11.2 MPLS TE Configuration Commands

11.2.1 add hop

Function

The **add hop** command adds a specified node on an MPLS TE explicit path.

Format

add hop *ip-address1* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**] { **after** | **before** } *ip-address2*

Parameters

Parameter	Description	Value
ip-address1	Specifies the IP address of the added node.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Specifies the node with an IP address *ip-address1* on the explicit path. • **strict**: indicates that the node is added in **strict** mode. The node of *ip-address1* is directly connected to the node of *ip-address2*. • **loose**: indicates that the node is added in **loose** mode. The node of *ip-address1* may not be directly connected to the node of *ip-address2*. • **incoming**: indicates that the *ip-address1* is the IP address of an inbound interface of a new-added node. • **outgoing**: indicates that the *ip-address1* is the IP address of an outbound interface of a new-added node.	By default, an explicit path is added in **include strict** mode.
exclude	Excludes the node of *ip-address1* from the explicit path.	-
after	Indicates that the node of *ip-address1* is added after the node of *ip-address2*.	-
before	Indicates that the node of *ip-address1* is added before the node of *ip-address2*.	-
ip-address2	Specifies the IP address of an interface or the Router ID of a node on the explicit path.	The value is in dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Prerequisites

The **next hop** command must have been run to specify a next-hop IP address before the **add hop** command is run.

Precautions

A node can be added to an explicit path using the **add hop** command only when the following conditions are met:

- *ip-address2* is the IP address of a node that exists on the explicit path.
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

Exclude the next hop of 10.2.2.2 after 10.1.1.1 from the explicit path named **p1**.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] quit
[Huawei] explicit-path p1
[Huawei-explicit-path-p1] next hop 10.1.1.1
[Huawei-explicit-path-p1] add hop 10.2.2.2 exclude after 10.1.1.1
```

Related Topics

11.2.134 next hop

11.2.7 display explicit-path

11.2.51 list hop

11.2.52 modify hop

11.2.3 delete hop

11.2.2 bfd bind mpls-te

Function

The **bfd bind mpls-te** command configures BFD to monitor TE tunnels, or the primary or backup LSP bound to a TE tunnel.

The **undo bfd** command deletes a specified BFD session.

By default, no TE tunnel applies BFD.

Format

bfd *cfg-name* **bind mpls-te interface tunnel** *interface-number* [**te-lsp** [**backup**]]

undo bfd *cfg-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cfg-name	Specifies the BFD configuration name.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface tunnel *interface-number*	Specifies the interface number of the TE tunnel bound to a BFD session.	-
te-lsp [**backup**]	Indicates that BFD monitors the LSP bound to the TE tunnel. ● If **backup** is not selected, BFD monitors the primary LSP bound to the TE tunnel. ● If **backup** is selected, BFD monitors the backup LSP bound to the TE tunnel.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **bfd bind mpls-te** command to configure BFD to monitor TE tunnels, or the primary or backup LSP bound to a TE tunnel.

Prerequisites

Before configuring BFD to monitor TE tunnels, the following tasks must have been completed:

- BFD has been enabled globally using the **bfd** command.
- An MPLS TE tunnel interface has been configured.

Precautions

BFD can monitor a TE tunnel and the primary or backup LSP bound to the TE tunnel.

- If BFD is configured to monitor the primary or backup LSP bound to a TE tunnel, a BFD session cannot be created if the LSP status is Down.

 Copyright © Huawei Technologies Co., Ltd.

- If the tunnel status is Down when BFD is configured to monitor a TE tunnel, the BFD session can still be created, but its status is Down.

  Multiple LSPs can be bound to a TE tunnel. When BFD detects the tunnel, the BFD session will go Down only if all LSPs bound to the TE tunnel fail.

Example

Configure BFD to detect the primary LSP bound to the TE tunnel.

```
<Huawei> system-view
[Huawei] bfd 1to4rsvp bind mpls-te interface Tunnel 0/0/1 te-lsp
[Huawei-bfd-lsp-session-1to4rsvp]
```

Configure BFD to detect the backup LSP bound to the TE tunnel.

```
<Huawei> system-view
[Huawei] bfd 1to4backup bind mpls-te interface Tunnel 0/0/1 te-lsp backup
[Huawei-bfd-lsp-session-1to4backup]
```

11.2.3 delete hop

Function

The **delete hop** command deletes a specified node from an MPLS TE explicit path.

Format

delete hop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an interface on a node.	In dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Precautions

A node can be deleted from an explicit path using the **delete hop** command only when the following conditions are met:

- The node must exist on the explicit path
- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

Delete the node of 10.10.10.10 from the MPLS TE explicit path.

```
<Huawei> system-view
[Huawei] explicit-path p1
[Huawei-explicit-path-p1] list hop
 Path Name : p1        Path Status : Enabled
 1      2.2.2.2          Strict      Include
 2      10.10.10.10       Strict      Include
 3      10.20.20.20       Strict      Include
[Huawei-explicit-path-p1] delete hop 10.10.10.10
[Huawei-explicit-path-p1] list hop
 Path Name : p1        Path Status : Enabled
 1      2.2.2.2          Strict      Include
 2      10.20.20.20       Strict      Include
```

Related Topics

11.2.1 add hop

11.2.50 explicit-path

11.2.51 list hop

11.2.134 next hop

11.2.52 modify hop

11.2.7 display explicit-path

11.2.4 display default-parameter mpls rsvp-te

Function

The **display default-parameter mpls rsvp-te** command displays the default parameters of MPLS RSVP-TE.

Format

display default-parameter mpls rsvp-te

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display default MPLS RSVP-TE parameters.

```
<Huawei> display default-parameter mpls rsvp-te
  RSVP-TE View Default Configurations:
  ----------------------------------------
  Resv Confirmation Request  : Disabled
  RSVP Hello Extension       : Disabled
  GR Capability              : Disabled
  GR Basic-Restart-Time      : 90000 ms
  Hello Interval             : 3000 ms
  Max Times Of Hello Misses  : 3
  Path/Resv Message Refresh Interval    : 30000 ms
  Path/Resv Message Refresh Retry Times : 3
  Challenge Retransmission Interval     : 1000 ms
  Max Times Of Challenge Lost           : 3
  Soft Preemption Timeout               : 30 s

  Interface View Default Configurations:
  ----------------------------------------
  SRefresh Feature           : Disabled
  Authentication Feature     : Disabled
  BFD Feature                : Disabled
  Hello Feature              : Disabled
  BFD Min-Tx                 : 1000
  BFD Min-Rx                 : 1000
  BFD Detect-Multi           : 3
  MPLS MTU                   : 1500
  SRefresh Interval          : 30000 ms
  SRefresh Retransmission Interval        : 5000 ms
  SRefresh Retransmission Increment Value : 1
  Authentication Life Time                : 1800000 ms
```

Table 11-47 Description of the display default-parameter mpls rsvp-te command output

Item	Description
Resv Confirmation Request	Whether or not the request for reservation confirmation is enabled.
RSVP Hello Extension	Whether or not the Hello extension is enabled.
GR Capability	RSVP GR capability.
GR Basic-Restart-Time	Basic RSVP GR time.
Hello Interval	Interval of Hello message.
Max Times Of Hello Misses	Maximum number of Hello messages that consecutively fail to be received.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Path/Resv Message Refresh Interval	Interval for refreshing Path or Resv messages.
Path/Resv Message Refresh Retry Times	Interval for retrying refreshing Path or Resv messages.
Challenge Retransmission Interval	Interval for resending Challenge messages.
Max Times Of Challenge Lost	Maximum number of Challenge messages that consecutively fail to be received.
Soft Preemption Timeout	The timeout of soft preemption
SRefresh Feature	Whether or not Srefresh is enabled.
Authentication Feature	Whether or not authentication is enabled.
BFD Feature	Whether or not BFD is enabled.
Hello Feature	Whether or not the Hello feature is enabled.
BFD Min-Tx	Actual interval for sending BFD packets.
BFD Min-Rx	Actual interval for receiving BFD packets.
BFD Detect-Multi	Actual local BFD detection multiplier.
MPLS MTU	Actual MTU value used for MPLS forwarding.
SRefresh Interval	Srefresh interval.
SRefresh Retransmission Interval	Srefresh retransmission interval.
SRefresh Retransmission Increment Value	Increment value of Srefresh retransmission.
Authentication Life Time	Authentication lifetime.

11.2.5 display default-parameter mpls te cspf

Function

The **display default-parameter mpls te cspf** command displays the default CSPF configurations.

Format

display default-parameter mpls te cspf

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the default CSPF configurations.

```
<Huawei> display default-parameter mpls te cspf
-----------------------------------------------
        CSPF Default Configuration
-----------------------------------------------
        Preferred-IGP : OSPF
        Failed-link Interval(Sec): 10
```

Table 11-48 Description of the display default-parameter mpls te cspf command output

Item	Description
Preferred-IGP	The IGP type whose database is in CSPF TEDB and that will be preferred for path calculation.
Failed-link Interval(Sec)	The default value of the failed link timer.

Related Topics

11.2.102 mpls te cspf preferred-igp

11.2.103 mpls te cspf timer failed-link

11.2.6 display default-parameter mpls te management

Function

The **display default-parameter mpls te management** command displays the default configurations of the MPLS TE management module.

Format

display default-parameter mpls te management

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the default configurations of the MPLS TE management module.

```
<Huawei> display default-parameter mpls te management

  Global Information
  ------------------------------------------------------------
  DS-TE MODE                          : NON-IETF
  Bandwidth constraint model              : RDM
  Switch-delay time(ms)                 : 5000
  Delete-delay time(ms)                 : 7000
  Auto-bandwidth timer(sec)               : 300
  FRR timer(sec)                      : 300
  Path metric-type                      : TE
  Tie-breaking                        : Random
  ------------------------------------------------------------

  Interface Information
  ------------------------------------------------------------
  Administrative group value              : 0
  TE metric value                     : 0
  Bandwidth change thresholds up          : 10
  Bandwidth change thresholds down        : 10
  ------------------------------------------------------------

  Tunnel Interface Information
  ------------------------------------------------------------
  Retry timer(sec)                      : 30
  Set priority                        : 7
  Hold priority                       : 7
  Default signal protocol                 : Rsvp
  Default resv-style                    : SE
  Default classtype                     : CT0
  Reoptimization frequency(sec)           : 3600
  Auto-bandwidth adjustment frequency(sec) : 86400
  Auto-bandwidth max-bw                   : 4294901760
  Auto-bandwidth min-bw                   : 0
  Auto-bandwidth threshold                : 0
  Hop-limit                           : 32
  Diffserv-mode                         : Uniform
  ------------------------------------------------------------

  Explicit-path Information
  ------------------------------------------------------------
  Default type                        : include strict
  ------------------------------------------------------------

  Default TEClass Mapping
  ------------------------------------------------------------
  TE-Class      ID      Class Type      Priority
  TE-Class      0       0               0
  TE-Class      1       1               0
```

```
TE-Class      2       2            0
TE-Class      3       3            0
TE-Class      4       0            7
TE-Class      5       1            7
TE-Class      6       2            7
TE-Class      7       3            7
-------------------------------------------------------------
```

Table 11-49 Description of the display default-parameter mpls te management command output

Item	Description
DS-TE MODE	DS-TE mode: ● IETF: indicates DS-TE in IETF mode. ● NON-IETF: indicates DS-TE in non-IETF mode.
Bandwidth constraint model	Bandwidth Constraints model: ● RDM: indicates the Russian Dolls Model. ● MAM: indicates the Maximum Allocation Model. ● Extended MAM: indicates the extended Maximum Allocation Model.
Switch-delay time(ms)	Delay time before switching TE traffic from the primary CR-LSP to the modified CR-LSP in milliseconds.
Delete-delay time(ms)	Delay before deleting the primary CR-LSP after TE traffic is switched to the modified CR-LSP, in milliseconds.
Auto-bandwidth timer(sec)	Time interval at which the output rate of each tunnel configured with automatic bandwidth adjustment is sampled, in seconds.
FRR timer(sec)	FRR switching time.
Path metric-type	Link metric type for path selection for tunnels.
Tie-breaking	Rule for selecting a route to the destination if multiple routes of equal cost are available.
Administrative group value	Administrative-group attribute.
TE metric value	TE metric of a link.
Bandwidth change thresholds up	Upper threshold of the bandwidth of an MPLS TE tunnel to be flooded.
Bandwidth change thresholds down	Lower threshold of the bandwidth of an MPLS TE tunnel to be flooded.
Retry timer(sec)	Time interval between attempts to establish a tunnel, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Set priority	Setup priority.
Hold priority	Holding priority.
Default signal protocol	Signaling protocol used to set up an LSP.
Default resv-style	Resource reservation style.
Default classtype	Class type.
Reoptimization frequency(sec)	Time interval between attempts of re-optimization, in seconds.
Auto-bandwidth adjustment frequency(sec)	Time interval between attempts of automatic bandwidth adjustment, in seconds.
Auto-bandwidth max-bw	Maximum bandwidth allowed by automatic bandwidth adjustment.
Auto-bandwidth min-bw	Minimum bandwidth allowed by automatic bandwidth adjustment.
Auto-bandwidth threshold	Indicates the threshold of the difference between the new and existing bandwidth. The value is expressed in percentage.
Hop-limit	Maximum number of hops.
Diffserv-mode	DiffServ mode.
Default type	Default type.
TE-Class ID	TE-class ID. The value is an integer that ranges from 0 to 7.
Class Type	Service type. When the TE-class is not configured, "--" is displayed.
Priority	Preemption priority of a tunnel. The value is an integer that ranges from 0 to 7. The smaller the value, the higher tunnel preemption priority.

11.2.7 display explicit-path

Function

The **display explicit-path** command displays information about an explicit path and the tunnels using it.

Format

display explicit-path [[**name**] *path-name*] [**tunnel-interface** | **verbose**]

Parameters

Parameter	Description	Value
name	Displays information about the specified explicit path.	-
path-name	Specifies the explicit path name.	The value is an existing explicit path name.
tunnel-interface	Displays information about the interface of the tunnel that uses the explicit path.	-
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no path name is specified, information about all explicit paths is displayed.

Example

Display detailed information about the explicit path named p1.

```
<Huawei> display explicit-path p1 verbose
Path Name : p1          Path Status : Enabled
 1      1.1.1.1          Strict      Include
 2      2.2.2.2          Strict      Exclude
 3      3.3.3.3          Loose       Include            Outgoing
 4      4.4.4.4          Strict      Include            Incoming
 List of p2p tunnels using this path:
    Tunnel0/0/1
 Number of p2p tunnels using this path: 1
 List of lsp-attributes referring this path:
 Number of lsp-attributes referring this path: 0
```

Table 11-50 Description of the display explicit-path verbose command output

Item	Description
Path Name	Name of an explicit path.
Path Status	Status of an explicit path. ● Enabled ● Disabled

Item	Description
Strict	The address is a strict next hop. The address is the ingress address or the address of the node that is connected directly to the previous node.
Loose	The address is a loose next hop.
Include	The explicit path contains the node of this IP address.
Exclude	The explicit path does not contain the node of this IP address.
Incoming or Outgoing	Type of an interface to which the IP address belong: ● Incoming ● Outgoing If this field is not displayed, the IP address belongs to either an outbound interface or an inbound interface.
List of p2p tunnels using this path	List of tunnels using the path.
Number of p2p tunnels using this path	Number of tunnels using the path.
List of lsp-attributes referring this path	List of CR-LSP attribute templates using the path.
Number of lsp-attributes referring this path	Number of CR-LSP attribute templates using the path. **NOTE** You cannot configure CR-LSP attribute templates on the device. Therefore, 0 is displayed.

Related Topics

11.2.50 explicit-path
11.2.1 add hop
11.2.3 delete hop
11.2.52 modify hop
11.2.134 next hop

11.2.8 display mpls lsp attribute

Function

The **display mpls lsp attribute** command displays information about the local bypass LSP attributes.

Format

display mpls lsp attribute { **bypass-inuse** { **exists-not-used** | **inuse** | **not-exists** } | **bypass-tunnel** *tunnel-name* }

Parameters

Parameter	Description	Value
bypass-inuse	Displays the attribute of the bypass LSPs in use.	-
exists-not-used	Displays the attributes of the existing bypass LSPs that are not in use.	-
inuse	Displays the attribute of the bypass LSPs in use.	-
not-exists	Displays the attributes of the bypass LSPs that are not in use.	-
bypass-tunnel	Displays the attribute of the specified bypass tunnel.	-
tunnel-name	Specifies the name of the bypass tunnel.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls lsp attribute** command to view information about attributes of local bypass LSPs in the TE FRR scenarios.

Example

Display information about attributes of the existing bypass LSPs that are not in use.

```
<Huawei> display mpls lsp attribute bypass-inuse exists-not-used
-------------------------------------------------------------------------------
                 LSP Information: RSVP LSP
-------------------------------------------------------------------------------

  No                  :  1
  SessionID           :  300
  IngressLsrID        :  3.3.3.9
  LocalLspID          :  5
  Tunnel-Interface    :  Tunnel0/0/1
  Fec                 :  1.1.1.9/32
  TunnelTableIndex    :  0x1
```

```
Nexthop            :  -------
In-Label           :  3
Out-Label          :  NULL
In-Interface       :  GigabitEthernet1/0/0
Out-Interface      :  ----------
LspIndex           :  2049
Token              :  0x0
LsrType            :  Egress
Mpls-Mtu           :  ------
TimeStamp          :  333sec
Bfd-State          :  ---
CBfd-Event         :  ---
Bed-State          :  ---
Bed-LastNotifyValue :  ---
Bed-LastNotifyLspId :  ---
```

Table 11-51 Description of the display mpls lsp attribute command output

Item	Description
No	Sequence number of an LSP.
SessionID	Session ID of a CR-LSP.
IngressLsrID	Ingress LSR ID of a CR-LSP.
LocalLspID	Local LSP ID of a CR-LSP.
Tunnel-Interface	Tunnel interface.
Fec	Forwarding Equivalence Class, which is destination address of an LSP.
TunnelTableIndex	Index of a tunnel table.
Nexthop	IP address of the next hop of an LSP.
In-Label	Value of an incoming label.
Out-Label	Value of an outgoing label.
In-Interface	Name of an incoming interface.
Out-Interface	Name of an outgoing interface.
LspIndex	Index number of an LSP, which uniquely identifies an LSP that is established using a specified protocol.
Token	LSP token, which guides the packet forwarding.
LsrType	Role of an LSR on an LSP: ● Ingress ● Transit ● Egress
Mpls-Mtu	Maximum transmission unit (MTU) of an interface of an LSP.
TimeStamp	Time elapsed since an LSP was set up.

Item	Description
Bfd-State	BFD status.
CBfd-Event	BFD-reported error code event received on the ingress of an RSVP LSP.
Bed-State	Error code status received on the ingress of an RSVP LSP.
Bed-LastNotifyValue	Event of association relationship related to error codes informed on the egress of an RSVP LSP.
Bed-LastNotifyLspId	ID of a reverse LSP when an event of association relationship related to error codes is informed on the egress of an RSVP LSP.

Related Topics

11.1.40 display mpls lsp

11.2.9 display mpls rsvp-te

Function

The **display mpls rsvp-te** command displays the RSVP-TE configurations.

Format

display mpls rsvp-te

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display information about RSVP-TE.

```
<Huawei> display mpls rsvp-te
 LSR ID: 1.1.1.9
 RSVP-TE Function Capability: Enable
```

```
Resv Confirmation Request: DISABLE
RSVP Hello Extension: ENABLE
Hello interval: 3 sec        Max Hello misses: 3
Path and Resv message refresh interval: 30 sec
Path and Resv message refresh retries count: 3
Blockade Multiplier: 4
Graceful-Restart Capability: GR-Support GR-Self
Restart Time:  90000 Millisecond
Recovery Time: 0 Millisecond
Bfd Enabled: DISABLE                Bfd Min-Tx: 1000
Bfd Min-Rx: 1000                    Bfd Detect-Multi: 3
Soft Preemption Timeout: 30 sec
```

Table 11-52 Description of the display mpls rsvp-te command output

Item	Description
LSR ID	LSR ID in the format X.X.X.X.
RSVP-TE Function Capability	Whether or not RSVP-TE is enabled. To enable the RSVP-TE function, run the **mpls rsvp-te** command.
Resv Confirmation Request	Whether or not reservation confirmation is requested. To enable the reservation confirmation mechanism, run the **mpls rsvp-te resvconfirm** command.
RSVP Hello Extension	Whether or not the RSVP Hello extension is enabled. To enable the RSVP Hello extension, run the **mpls rsvp-te hello** command.
Hello interval	The interval at which Hello messages are sent, in seconds. To specify the interval, run the **mpls rsvp-te timer hello** command.
Max Hello misses	Maximum number of times for the consecutively lost Hello messages. To specify the maximum number, run the **mpls rsvp-te hello-lost** command.
Path and Resv message refresh interval	Time interval at which the Path and Resv messages are refreshed, in seconds. To specify the interval, run the **mpls rsvp-te timer refresh** command.
Path and Resv message refresh retries count	Number of retry times allowed for refreshing the Path and Resv messages. To specify the number, run the **mpls rsvp-te keep-multiplier** command.
Blockade Multiplier	Multiplier for keeping the blocked state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Graceful-Restart Capability	RSVP GR capability of a device: • GR-Support GR-Self: indicates that the RSVP GR on the local node is enabled and the RSVP GR of the neighbor is supported. • GR-Self: indicates that the RSVP GR is enabled only on the local node. • GR-Support: indicates that the RSVP GR of the neighbor is supported. • DISABLE: indicates that the RSVP GR is disabled. To enable the RSVP GR capability, run the **mpls rsvp-te hello support-peer-gr** command or**mpls rsvp-te hello full-gr** command.
Restart Time	Start time of the GR process, in milliseconds. It is displayed only after the command **mpls rsvp-te hello basic-restart-time** is run.
Recovery Time	Time spent on recovering all LSPs, in milliseconds. It is displayed only after the command **mpls rsvp-te hello basic-restart-time** is run.
Bfd Enabled	Whether or not the BFD for RSVP is enabled globally in the MPLS view: • ENABLE: indicates that BFD for RSVP is globally enabled in the MPLS view. • DISABLE: indicates that BFD for RSVP is globally disabled in the MPLS view. To enable the BFD for RSVP function, run the **mpls rsvp-te bfd all-interfaces enable** command.
Bfd Min-Tx	Local interval at which BFD packets are sent, in milliseconds. To specify the interval, run the **mpls rsvp-te bfd all-interfaces** command.
Bfd Min-Rx	Local interval at which BFD packets are received, in milliseconds. To specify the interval, run the **mpls rsvp-te bfd all-interfaces** command.
Bfd Detect-Multi	Local BFD detection multiplier. To specify the multiplier, run the **mpls rsvp-te bfd all-interfaces** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Soft Preemption Timeout	The timeout of soft preemption

Related Topics

11.2.54 mpls rsvp-te
11.2.75 mpls rsvp-te resvconfirm
11.2.67 mpls rsvp-te hello
11.2.79 mpls rsvp-te timer hello
11.2.66 mpls rsvp-te hello-lost
11.2.80 mpls rsvp-te timer refresh
11.2.72 mpls rsvp-te keep-multiplier

11.2.10 display mpls rsvp-te bfd session

Function

The **display mpls rsvp-te bfd session** command displays information about the BFD session for RSVP.

Format

display mpls rsvp-te bfd session { **all** | **interface** *interface-type interface-number* | **peer** *ip-address* } [**verbose**]

Parameters

Parameter	Description	Value
all	Displays information about all the BFD sessions for RSVP.	-
interface *interface-type interface-number*	Displays information about the BFD session for RSVP on the specified interface.	-
peer *ip-address*	Displays information about the BFD session for RSVP of the specified peer.	The value is in dotted decimal notation.
verbose	Displays detailed information about a BFD session for RSVP.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display information about a BFD session for RSVP.

```
<Huawei> display mpls rsvp-te bfd session all
Total Nbrs/Rsvp triggered sessions : 1/1
--------------------------------------------------------------------------
Local      Remote     Local          Peer           Interface      Session
Discr      Discr      Addr           Addr           Name           State
--------------------------------------------------------------------------
8192       8192       10.1.1.1       10.1.1.2       GE1/0/0        UP
```

Display detailed information about a BFD session for RSVP.

```
<Huawei> display mpls rsvp-te bfd session all verbose
Total Nbrs/Rsvp triggered sessions : 1/1
--------------------------------------------------------------------------
  Local Discriminator      :  8192
  Remote Discriminator     :  8192
  Local Address            :  10.1.1.1
  Peer Address             :  10.1.1.2
  Interface Name           :  GE1/0/0
  ActTx                    :  1000
  ActRx                    :  1000
  ActMulti                 :  3
  Session State            :  UP
```

Table 11-53 Description of the display mpls rsvp-te bfd session command output

Item	Description
Total Nbrs/Rsvp triggered sessions	Number of BFD neighbors or RSVP-triggered sessions in the system or interface view.
Local Discr/Local Discriminator	Local discriminator of a BFD session. The value 0 indicates an invalid discriminator. To specify a local discriminator of a BFD session, run the **discriminator** command.
Remote Discr/ Remote Discriminator	Remote discriminator of a BFD session. The value 0 indicates an invalid discriminator. To specify a remote discriminator of a BFD session, run the **discriminator** command.
Local Addr/Local Address	IP address of the local node in a BFD session.
Peer Addr/Peer Address	IP address of the peer in a BFD session.
Interface Name	Outgoing interface of a BFD session.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ActTx/ActRx/ActMulti	Parameters of a BFD session: To specify parameters of a BFD session, run the **mpls rsvp-te bfd all-interfaces** command. • ActTx: indicates the actual interval at which BFD packets are sent, in milliseconds. • ActRx: indicates the actual interval at which BFD packets are received, in milliseconds. • ActMulti: indicates the actual local detection multiplier. The default value is 3.
Session State	Status of a BFD session: • UP: indicates that the BFD session is Up. • DOWN: indicates that the BFD session is Down. • NONE: indicates that no BFD session is created. • ADMIN DOWN: indicates that the administrator manually closes the BFD session. • INITIAL: indicates the BFD session is in the Initial state.

Related Topics

11.2.61 mpls rsvp-te bfd all-interfaces enable

11.2.11 display mpls rsvp-te established

Function

The **display mpls rsvp-te established** command displays information about RSVP resource reservation based on an interface, and about the RSVP-TE LSPs that pass through the interface.

Format

display mpls rsvp-te established [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of an interface on the RSVP peer connected to the local device.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an interface is specified, information about the establishment of the RSVP-TE LSP on this interface is displayed.

Example

Display information about the establishment of the RSVP-TE LSPs of all interfaces.

```
<Huawei> display mpls rsvp-te established
Interface: Outgoing-Interface at the Egress
 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 1.1.1.9           Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4              Session Tunnel ID: 301
 Next Hop Addr:  -----
 Upstream Label: 3

 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 1.1.1.9           Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4              Session Tunnel ID: 300
 Next Hop Addr:  -----
 Upstream Label: 3

 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 3.3.3.9           Ingress LSR ID: 1.1.1.9
 Local LSP ID: 3              Session Tunnel ID: 300
 Next Hop Addr: 172.1.1.2
 Upstream Label: NULL             Downstream Label: 1040

 Token Bucket Rate: 0.00          Peak Data Rate: 0.00
 Tunnel Addr: 3.3.3.9           Ingress LSR ID: 1.1.1.9
 Local LSP ID: 2              Session Tunnel ID: 301
 Next Hop Addr: 172.1.1.2
 Upstream Label: NULL             Downstream Label: 1038
```

 Copyright © Huawei Technologies Co., Ltd.

Table 11-54 Description of the display mpls rsvp-te established command output

Item	Description
Interface: Outgoing-Interface at the Egress	Information about RSVP resource reservation based on the outgoing interface on the egress node and about the RSVP LSPs that pass through the interface.
Token Bucket Rate	Token bucket rate, in byte/s.
Peak Data Rate	Peak data rate, in byte/s.
Tunnel Addr	Tunnel address in the format X.X.X.X.
Ingress LSR ID	LSR ID on the ingress in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Session Tunnel ID	Tunnel ID.
Next Hop Addr	Next-hop address in the format X.X.X.X.
Upstream Label	Value of an incoming label.
Downstream Label	Value of an outgoing label.

Related Topics

11.2.54 mpls rsvp-te

11.2.12 display mpls rsvp-te graceful-restart

Function

The **display mpls rsvp-te graceful-restart** command displays the status of RSVP GR.

Format

display mpls rsvp-te graceful-restart

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None.

Example

Display the status of RSVP-TE GR.

```
<Huawei> display mpls rsvp-te graceful-restart
Display Mpls Rsvp te graceful restart information
 LSR ID: 1.1.1.9
 Graceful-Restart Capability:   GR-Self GR-Support
 Restart Time:  90000 Milli Second
 Recovery Time: 0 Milli Second
 GR Status:  Gracefully Restart Not going on
 Number of Restarting neighbors: 0
 Number of LSPs recovered: 0
 Received Gr Path message count: 0
 Send Gr Path message count: 0
 Received RecoveryPath message count: 0
 Send RecoveryPath message count: 0
```

Table 11-55 Description of the display mpls rsvp-te graceful-restart command output

Item	Description
LSR ID	LSR ID.
Graceful-Restart Capability	RSVP GR capability of a device.
Restart Time	Restart time for a device, in milliseconds. To set the restart time, run the **mpls rsvp-te hello basic-restart-time** command.
Recovery Time	Time spent on recovering all LSPs, in milliseconds. To set the restart time, run the **mpls rsvp-te hello basic-restart-time** command.
GR Status	RSVP GR status of the local device: • Gracefully Restart Not going on: indicates that the protocol is not entering the GR process. • Gracefully Restart on going restarting: indicates that the protocol has entered the GR process. • Gracefully Restart on going recovery: indicates that the configurations are being restored.
Number of Restarting neighbors	Number of supporting nodes.
Number of LSPs recovered	Number of recovered LSPs.
Received Gr Path message count	Number of Path messages received by restarting nodes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Send Gr Path message count	Number of Path messages sent by supporting nodes.
Received RecoveryPath message count	Number of Recovery Path messages received by restarting nodes.
Send RecoveryPath message count	Number of Recovery Path messages sent by supporting nodes.

Related Topics

11.2.13 display mpls rsvp-te graceful-restart peer

11.2.69 mpls rsvp-te hello full-gr

11.2.68 mpls rsvp-te hello basic-restart-time

11.2.13 display mpls rsvp-te graceful-restart peer

Function

The **display mpls rsvp-te graceful-restart peer** command displays the status of RSVP GR on a neighbor.

Format

display mpls rsvp-te graceful-restart peer [{ **interface** *interface-type interface-number* | **node-id** } [*ip-address*]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the RSVP GR status of a neighbor on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
node-id	Displays the RSVP GR status of a manually-configured neighbor.	-
ip-address	Specifies the IP addresses of a neighbor.	The value is in dotted decimal notation.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the RSVP-TE GR status of the neighbor.

```
<Huawei> display mpls rsvp-te graceful-restart peer
 Neighbor on Interface GigabitEthernet1/0/0
 Neighbor Addr: 1.1.1.1              Last Attribute: Added Usually
 SrcInstance: 0x7C832B3D               NbrSrcInstance: 0x6A48E0F5
 Neighbor Capability:
                  Can Do Self GR
                  Can Support GR
 GR Status:          Normal
 Restart Time:  90000 Millisecond
 Recovery Time: 0 Millisecond
 Stored GR message number: 0
 PSB Count: 0                        RSB Count: 1
 Total to be Recover PSB Count: 0     Recovered PSB Count: 0
 Total to be Recover RSB Count: 0     Recovered RSB Count: 0
 P2MP PSB Count: 0                    P2MP RSB Count: 0
 Total to be Recover P2MP PSB Count: 0     Recovered P2MP PSB Count: 0
 Total to be Recover P2MP RSB Count: 0     Recovered P2MP RSB Count: 0
```

Table 11-56 Description of the display mpls rsvp-te graceful-restart peer command output

Item	Description
Neighbor Addr	IP address of a neighbor.
Last Attribute	Neighbor attribute: ● Added Usually: indicates the neighbor is discovered based on an interface. ● Added by Node-Id: indicates the neighbor is discovered based on the configured node ID. ● To be deleted: indicates the neighbor that is to be deleted because of the Hello timeout. ● Add by Frr: indicates an FRR neighbor.
SrcInstance	Source instance.
NbrSrcInstance	Source instance of a neighbor.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Neighbor Capability	GR capability of a neighbor: ● Can Do Self GR: indicates that the neighbor can perform GR. ● Can Support GR: indicates that the neighbor has the capability of supporting GR. ● Can Transmit Recovery Path Messages: indicates that the neighbor can send Recovery Path messages. ● No Gr capabilities: indicates that the neighbor does not have the capability of supporting GR.
GR Status	GR status of a neighbor: ● Normal: indicates that the neighbor does not perform GR. ● Supporting: indicates that the neighbor is supporting the local node of performing GR. ● Restarting: indicates that the neighbor is supporting the local node of the restart.
Restart Time	Restart time of a neighbor, in milliseconds.
Recovery Time	Recovery time of a neighbor, in milliseconds.
Stored GR message number	Number of GR messages stored on the supporting node.
PSB Count	Number of PSBs.
RSB Count	Number of RSBs.
Total to be Recover PSB Count	Total number of the PSBs to be recovered.
Recovered PSB Count	Number of the recovered PSBs.
Total to be Recover RSB Count	Total number of the RSBs to be recovered.
Recovered RSB Count	Number of recovered RSBs.
P2MP PSB Count	Number of P2MP PSBs
P2MP RSB Count	Number of P2MP RSBs
Total to be Recover P2MP PSB Count	Number of P2MP PSBs to be restored after the GR process is complete
Recovered P2MP PSB Count	Number of P2MP PSBs that have been restored after the GR process is complete
Total to be Recover P2MP RSB Count	Number of P2MP RSBs to be restored after the GR process is complete

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Recovered P2MP RSB Count	Number of P2MP RSBs that have been restored after the GR process is complete

Related Topics

11.2.12 display mpls rsvp-te graceful-restart
11.2.68 mpls rsvp-te hello basic-restart-time
11.2.71 mpls rsvp-te hello support-peer-gr

11.2.14 display mpls rsvp-te interface

Function

The **display mpls rsvp-te interface** command displays the RSVP-TE configurations on an interface.

Format

display mpls rsvp-te interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and number. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the type and number of an interface is not specified, the **display mpls rsvp-te interface** command displays the RSVP-TE information of all RSVP TE-enabled interfaces.

Example

Display information about RSVP-TE of a specified interface.

```
<Huawei> display mpls rsvp-te interface gigabitethernet 1/0/0
Interface: GigabitEthernet1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Interface Address: 11.11.11.11
Interface state: UP                Interface Index: 0x4
Total-BW: 0                       Used-BW: 0
Hello configured: NO               Num of Neighbors: 0
SRefresh feature: DISABLE            SRefresh Interval: 30 sec
Mpls Mtu: 1500                     Retransmit Interval: 5000 msec
Increment Value: 1
Authentication: DISABLE
Bfd Enabled: DISABLE               Bfd Min-Tx: 400
Bfd Min-Rx: 300                   Bfd Detect-Multi: 4
```

Table 11-57 Description of the display mpls rsvp-te interface command output

Item	Description
Interface	Name of a tunnel interface.
Interface Address	IP address of an interface.
Interface state	Interface status: ● UP ● DOWN
Interface Index	Index of an interface.
Total-BW	Total available bandwidth of an interface, in kbit/s.
Used-BW	Total bandwidth of an interface in use, in kbit/s.
Hello configured	Whether or not the Hello feature is configured on an interface: ● YES: indicates that the Hello feature is configured. ● NO: indicates that the Hello feature is not configured.
Num of Neighbors	Number of neighbor devices of the local node.
SRefresh feature	Whether or not the Srefresh feature is enabled. To enable the Srefresh feature, run the **mpls rsvp-te srefresh** command in the interface view.
SRefresh Interval	Value of the Srefresh timer, in seconds. To specify the value of the Srefresh timer, run the **mpls rsvp-te timer refresh** command.
Mpls Mtu	MTU value used in MPLS forwarding.
Retransmit Interval	Value of the Retransmit timer, in milliseconds. To specify the value of the Retransmit timer, run the **mpls rsvp-te timer retransmission** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Increment Value	Retransmission increment. To specify the retransmission increment, run the **mpls rsvp-te timer retransmission** command.
Authentication	Whether or not the authentication function is enabled: ● ENABLE: indicates that the authentication function is enabled. ● DISABLE: indicates that the authentication function is disabled. To enable the authentication function, run the **mpls rsvp-te authentication** command.
Bfd Enabled	Whether or not BFD for RSVP is enabled on the interface: ● ENABLE: indicates that BFD for RSVP is enabled on the interface. ● DISABLE: indicates that BFD for RSVP is not enabled on the interface. To enable BFD for RSVP, run the **mpls rsvp-te bfd enable** command.
Bfd Min-Tx	Local interval at which BFD packets are sent, in milliseconds. To specify the local minimum interval at which BFD packets are sent, run the **mpls rsvp-te bfd** command.
Bfd Min-Rx	Local interval at which BFD packets are received, in milliseconds. To specify the local minimum interval at which BFD packets are received, run the **mpls rsvp-te bfd** command.
Bfd Detect-Multi	Local BFD detection multiplier. To specify the local BFD detection multiplier, run the **mpls rsvp-te bfd** command.

11.2.15 display mpls rsvp-te nsr status

Function

The **display mpls rsvp-te nsr status** command displays statistics on backup messages of RSVP-TE during NSR.

Format

display mpls rsvp-te nsr status

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

After configuring NSR, you need to back up data on the master main control board to the slave main control board to ensure data consistency. You can run the **display mpls rsvp-te nsr status** command to check whether the messages on the master and slave main control boards are the same.

Example

Display statistics on backup messages of RSVP-TE during NSR.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] display mpls rsvp-te nsr status
 NSR Capability: Disable
 Current Phase:  RealtimeBackup
 Backup Message Statistics:
 Total Send: 0                    Total Receive: 0
 Send Create LSP: 0               Receive Create LSP: 0
 Send Delete LSP: 0               Receive Delete LSP: 0
 Send Update LSP: 0               Receive Update LSP: 0
 Send Interface Event: 0          Receive Interface Event: 0
 Send Background End: 0           Receive Background End: 0
 Send Pseud MP Event: 0           Receive Pseud MP Event: 0
 Send Batch Nbr: 0                Receive Batch Nbr: 0
 Send Delete Nbr: 0               Receive Delete Nbr: 0
 Send Nbr Lost Event: 0           Receive Nbr Lost Event: 0
 Send Restart Timeout: 0          Receive Restart Timeout: 0
 Send Recover Timeout: 0          Receive Recover Timeout: 0
 Send Aging Timeout: 0            Receive Aging Timeout: 0
 Send Hello: 0                    Receive Hello: 0
 Send BFD Event: 0                Receive BFD Event: 0
 Send Auth Info: 0                Receive Auth Info: 0
 Send BFD Operate: 0              Receive BFD Operate: 0
 Send Delete FRR Node: 1          Receive Delete FRR Node: 0
 Send Pseud PLR Event: 1          Receive Pseud PLR Event: 0
```

Table 11-58 Description of the **display mpls rsvp-te nsr status** command output

Item	Description
NSR Capability	NSR capability: ● Enable: indicates that NSR is enabled. ● Disable: indicates that NSR is disabled.

Item	Description
Current Phase	Current backup status of the master and slave main control boards: ● RealtimeBackup: indicates the real-time backup. ● BatchBackup: indicates the batch backup. ● Smooth: indicates smoothing.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Backup Message Statistics	Statistics on backup messages between the master and slave main control boards: ● Total Send: indicates the total number of sent messages. ● Total Receive: indicates the total number of received messages. ● Send Create LSP: indicates the number of sent Create LSP messages. ● Receive Create LSP: indicates the number of received Create LSP messages. ● Send Delete LSP: indicates the number of sent Delete LSP messages. ● Receive Delete LSP: indicates the number of received Delete LSP messages. ● Send Update LSP: indicates the number of sent Update LSP messages. ● Receive Update LSP: indicates the number of received Update LSP messages. ● Send Interface Event: indicates the number of sent Interface Event messages. ● Receive Interface Event: indicates the number of received Interface Event messages. ● Send Background End: indicates the number of sent Background End messages. ● Receive Background End: indicates the number of received Background End messages. ● Send Pseud MP Event: indicates the number of sent Pseud MP Event messages. ● Receive Pseud MP Event: indicates the number of received Pseud MP Event messages. ● Send Batch Nbr: indicates the number of sent Batch Nbr messages. ● Receive Batch Nbr: indicates the number of received Batch Nbr messages ● Send Delete Nbr: indicates the number of sent Delete Nbr messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Receive Delete Nbr: indicates the number of received Delete Nbr messages. • Send Nbr Lost Event: indicates the number of sent Nbr Lost Event messages. • Receive Nbr Lost Event: indicates the number of received Nbr Lost Event messages. • Send Restart Timeout: indicates the number of sent Restart Timeout messages. • Receive Restart Timeout: indicates the number of received Restart Timeout messages. • Send Recover Timeout: indicates the number of sent Recover Timeout messages. • Receive Recover Timeout: indicates the number of received Recover Timeout messages. • Send Aging Timeout: indicates the number of sent Aging Timeout messages. • Receive Aging Timeout: indicates the number of received Aging Timeout messages. • Send Hello: indicates the number of sent Hello messages. • Receive Hello: indicates the number of received Hello messages. • Send BFD Event: indicates the number of sent BFD Event messages. • Receive BFD Event: indicates the number of received BFD Event messages. • Send Auth Info: indicates the number of sent Auth Info messages. • Receive Auth Info: indicates the number of received Auth Info messages. • Send BFD Operate: indicates the number of sent BFD Operate messages. • Receive BFD Operate: indicates the number of received BFD Operate messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Send Delete FRR Node: indicates the number of sent Delete FRR Node messages. • Receive Delete FRR Node: indicates the number of received Delete FRR Node messages. • Send Pseud PLR Event: indicates the number of sent Pseud PLR Event messages. • Receive Pseud PLR Event: indicates the number of received Pseud PLR Event messages.

11.2.16 display mpls rsvp-te peer

Function

The **display mpls rsvp-te peer** command displays information about RSVP-TE neighbor devices on an RSVP-TE-enabled interface.

Format

display mpls rsvp-te peer [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about RSVP-TE of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface is specified, information about RSVP-TE neighbors of all interfaces is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about RSVP-TE neighbors of all interfaces.

```
<Huawei> display mpls rsvp-te peer
 Remote Node id Neighbor
 Neighbor Addr:  -----
 SrcInstance: 0x3A76A0FA            NbrSrcInstance: 0x0
 PSB Count: 2                    RSB Count: 2
 Hello Type Sent: REQ
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL

Interface: GigabitEthernet1/0/0
 Neighbor Addr: 1.1.1.1
 SrcInstance: 0x3A76A0FA            NbrSrcInstance: 0x22A6B5C2
 PSB Count: 2                    RSB Count: 2
 Hello Type Sent: REQ               Neighbor Hello Extension: ENABLE
 SRefresh Enable: NO
 Last valid seq # rcvd: NULL
```

Table 11-59 Description of the display mpls rsvp-te peer command output

Item	Description
Neighbor Addr	Neighboring device address.
SrcInstance	Source instance.
NbrSrcInstance	Source instance of a neighbor device.
PSB Count	Number of Path State Blocks (PSBs).
RSB Count	Number of Reservation State Blocks (RSBs).
Hello Type Sent	Type of Hello message sent to the neighbor device: ● REQ ● ACK ● NONE
Neighbor Hello Extension	Whether or not the Hello extension feature of the neighboring device is enabled.
SRefresh Enable	Whether or not the Srefresh mechanism is enabled: ● YES ● NO
Last valid seq # rcvd	Serial number of the valid RSVP message last received.

Related Topics

11.2.54 mpls rsvp-te

11.2.17 display mpls rsvp-te psb-content

Function

The **display mpls rsvp-te psb-content** command displays information about an RSVP TE Path State Block (PSB).

Format

display mpls rsvp-te psb-content [*ingress-lsr-id tunnel-id lsp-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all RSVP-TE PSBs is displayed.

Example

Display information about the PSB.

```
<Huawei> display mpls rsvp-te psb-content 1.1.1.9 100 7
=============================================================
                    The PSB Content
=============================================================
 Tunnel Addr: 4.4.4.9                    Exist time: 17h 12m 57s
 Tunnel ExtID: 1.1.1.9                   Session ID: 100
 Ingress LSR ID: 1.1.1.9                 Local LSP ID: 7
 Previous Hop : 172.1.1.1/0x2d     Next Hop : 172.2.1.2
 Incoming / Outgoing Interface: GigabitEthernet1/0/0  / GigabitEthernet2/0/0
 InLabel : 1028                        OutLabel : 1028
 Send Message ID : 30                      Recv Message ID : 0
 Refresh Timer : 510224684                 Cleanup Timer : 408260940
 Session Attribute-
  SetupPrio: 7         HoldPrio: 7
  SessionAttrib: Local Protect desired. Node Protect desired. Label Recording de
sired. SE Style desired.
 LSP Type: -
```

```
FRR Flag : Will be MP                    Local RRO Flag : 0x1
ERO Information-
    L-Type         ERO-IPAddr       ERO-PrefixLen
  ERHOP_STRICT    172.2.1.2            32
  ERHOP_STRICT    172.3.1.1            32
  ERHOP_STRICT    172.3.1.2            32
Bypass ERO Information-
    L-Type         ERO-IPAddr       ERO-PrefixLen
  ERHOP_STRICT    3.3.3.9              32
  ERHOP_STRICT    172.3.1.1            32
  ERHOP_STRICT    172.3.1.2            32
RRO Information-
  RRO-CType: IPV4   IPAddress: 172.1.1.1         PrefixLen: 32  Flag: 0x9
  RRO-CType: IPV4   IPAddress: 1.1.1.9           PrefixLen: 32  Flag: 0x20
SenderTspec Information-
 Token bucket rate: 0.00
 Token bucket size: 1000.00
 Peak data rate: 0.00
 Minimum policed unit: 0
 Maximum packet size: 1500
CT-BandWidth Information:
CT0 BandWidth(Bytes/sec): 625000.00    CT1 BandWidth(Bytes/sec): 625000.00
CT2 BandWidth(Bytes/sec): -            CT3 BandWidth(Bytes/sec): -
CT4 BandWidth(Bytes/sec): -            CT5 BandWidth(Bytes/sec): -
CT6 BandWidth(Bytes/sec): -            CT7 BandWidth(Bytes/sec): -
Path Message arrive on GigabitEthernet1/0/0 from PHOP 172.1.1.1
Path Message sent to NHOP 172.2.1.2  on GigabitEthernet2/0/0
Resource Reservation OK

LSP Statistics Information:
  SendPacketCounter: 3623        RecvPacketCounter: 3648
  SendPathCounter: 1794          RecvPathCounter: 1791
  SendResvCounter: 1829          RecvResvCounter: 1857
```

Table 11-60 Description of the display mpls rsvp-te psb-content command output

Item	Description
Tunnel Addr	Tunnel address in the format X.X.X.X.
Exist time	Duration that an LSP has been established.
Tunnel ExtID	Tunnel extended ID.
Session ID	RSVP session ID
Ingress LSR ID	Ingress address in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Previous Hop	Previous-hop address in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Incoming / Outgoing Interface	Incoming or outgoing interface through which a tunnel passes on the local device.
InLabel	Value of an incoming label.
OutLabel	Value of an outgoing label.
Send Message ID	ID of the sent refresh reduction message.
Recv Message ID	ID of the received refresh reduction message.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Refresh Timer	Refresh timer.
Cleanup Timer	Timeout timer.
Session Attribute	Attribute of an RSVP session.
SetupPrio	Setup priority of an RSVP session.
HoldPrio	Holding priority of an RSVP session.
SessionAttrib	RSVP session attributes, such as resource reservation style.
LSP Type	Type of LSP.
FRR Flag	State of MPLS TE FRR
Local RRO Flag	Flag bit of the local RRO.
ERO Information	Information about the Explicit Route Object (ERO).
L-Type	Types of the explicit route.
ERO-IPAddr	Explicit route address.
ERO-PrefixLen	Explicit route prefix length.
RRO Information	Information about the Record Route Object (RRO).
RRO-CType	RRO of the C type, IPv4 or label.
IPAddress	IP address of a record route.
PrefixLen	Prefix length of a recorded route.
Flag	Flag bit of a recorded route.
SenderTspec Information	Information about the traffic specification of the sender.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size.
CT-BandWidth Information	Bandwidth information corresponding to each CT.
CT0 - CT7 Bandwidth	Bandwidth values of LSPs of CT0 to CT7.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Path Message arrive on	Incoming interfaces and previous-hop addresses of messages.
Path Message sent to NHOP	Next-hop addresses and outgoing interfaces of messages.
Resource Reservation OK	Ready state of resource reservation that is displayed only when the resource reserved flag is set.
LSP Statistics Information	Statistics of LSPs.
SendPacketCounter	Number of sent packets.
RecvPacketCounter	Number of received packets.
SendPathCounter	Number of sent Path messages.
RecvPathCounter	Number of received Path messages.
SendResvCounter	Number of sent Resv messages.
RecvResvCounter	Number of received Resv messages.

Related Topics

11.2.20 display mpls rsvp-te rsb-content

11.2.18 display mpls rsvp-te request

Function

The **display mpls rsvp-te request** command displays information about the RSVP-TE request messages on interfaces.

Format

display mpls rsvp-te request [**interface** *interface-type interface-number peer-ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about RSVP TE request messages on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of a neighbor device.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays information about the RSVP-TE request information of all RSVP-TE-enabled interfaces.

Example

Display information about the RSVP-TE request information.

```
<Huawei> display mpls rsvp-te request
Interface: Incoming-Interface at the Ingress
 Tunnel Addr: 3.3.3.9              Ingress LSR ID: 1.1.1.9
 Local LSP ID: 3                   Session Tunnel ID: 300
 NextHopAddr: 10.1.1.2
 SessionAttrib: SE Style desired.
 Token bucket rate: 0.00           Token bucket size: 1000.00
 Out Interface: GigabitEthernet2/0/0

 Tunnel Addr: 1.1.1.9              Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4                   Session Tunnel ID: 300
 NextHopAddr:  -----
 SessionAttrib: SE Style desired.
 Token bucket rate: 0.00           Token bucket size: 1000.00
 Out Interface: -----
```

Table 11-61 Description of the display mpls rsvp-te request command output

Item	Description
Interface	Name of the interface that is enabled with RSVP-TE.

Item	Description
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local identifier of an LSP.
Session Tunnel ID	Tunnel ID
NextHopAddr	Next-hop address in the format X.X.X.X.
SessionAttrib	Session attribute: ● Local protection desired ● Label record desired ● Resource reservation style
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.
Out Interface	Outgoing interface of an LSP.

Related Topics

11.2.54 mpls rsvp-te

11.2.19 display mpls rsvp-te reservation

Function

The **display mpls rsvp-te reservation** command displays RSVP-TE resource reservation information of an interface enabled with RSVP-TE.

Format

display mpls rsvp-te reservation [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the RSVP-TE reservation information of the interface that is not in stale state. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
peer-ip-address	Specifies the IP address of an RSVP-TE neighbor device.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays the resource reservation information of all RSVP-TE-enabled interfaces.

Example

Display information about the RSVP-TE resource reservation information of all interfaces.

```
<Huawei> display mpls rsvp-te reservation
Interface: Outgoing-Interface at the Egress
 Tunnel Addr: 1.1.1.9            Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4               Session Tunnel ID: 301
 Upstream Label: 3
 Token bucket rate: 0.00          Token bucket size: 1000.00

 Tunnel Addr: 1.1.1.9            Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4               Session Tunnel ID: 300
 Upstream Label: 3
 Token bucket rate: 0.00          Token bucket size: 1000.00

 Tunnel Addr: 3.3.3.9            Ingress LSR ID: 1.1.1.9
 Local LSP ID: 3               Session Tunnel ID: 300
 Upstream Label: NULL
 Token bucket rate: 0.00          Token bucket size: 1000.00

 Tunnel Addr: 3.3.3.9            Ingress LSR ID: 1.1.1.9
 Local LSP ID: 2               Session Tunnel ID: 301
 Upstream Label: NULL
 Token bucket rate: 0.00          Token bucket size: 1000.00
```

Table 11-62 Description of the display mpls rsvp-te reservation command output

Item	Description
Interface	Name of the interface that is enabled with RSVP-TE
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.

Item	Description
Local LSP ID	Local identifier of an LSP.
Session Tunnel ID	Tunnel ID.
Upstream Label	Incoming label.
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.

Related Topics

11.2.54 mpls rsvp-te

11.2.20 display mpls rsvp-te rsb-content

Function

The **display mpls rsvp-te rsb-content** command displays information about the RSVP TE Reserve State Block (RSB).

Format

display mpls rsvp-te rsb-content [*ingress-lsr-id tunnel-id lsp-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all RSVP TE RSBs are displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about the RSVP TE Reserve State Block.

```
<Huawei> display mpls rsvp-te rsb-content 1.1.1.9 300 3
==============================================================
                    The RSB Content
==============================================================
 Tunnel Addr: 3.3.3.9                Session Tunnel ID: 300
 Tunnel ExtID: 1.1.1.9
 Next Hop: 172.1.1.2                 Reservation Style: SE Style
 Reservation Incoming Interface: GigabitEthernet1/0/0
 Reservation Interface: GigabitEthernet1/0/0
 Filter Spec Information-
   The filter number: 1
   Ingress LSR ID: 1.1.1.9         Local LSP ID: 3       OutLabel: 1040
   Cleanup Timer : 504613260
   RRO Information-
     RRO-CType: IPV4   RRO-IPAddress: 172.1.1.2        RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1040
     RRO-CType: IPV4   RRO-IPAddress: 2.2.2.9          RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1040
     RRO-CType: IPV4   RRO-IPAddress: 172.2.1.1        RRO-IPPrefixLen: 32
     RRO-CType: IPV4   RRO-IPAddress: 172.2.1.2        RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 3
     RRO-CType: IPV4   RRO-IPAddress: 3.3.3.9          RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 3
   Message ID : 0
 FlowSpec Information-
   Token bucket rate: 0.00
   Token bucket size: 1000.00
   Peak data rate: 0.00
   Minimum policed unit: 0
   Maximum packet size: 1500
   Bandwidth guarantees: 0.00
   Delay guarantees: 0
   Qos Service is Controlled
 Resv Message arrive on GigabitEthernet1/0/0 from NHOP 172.1.1.2
```

Table 11-63 Description of the display mpls rsvp-te rsb-content command output

Item	Description
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Session Tunnel ID	Tunnel ID.
Tunnel ExtID	Tunnel extension ID (ingress LSR ID) in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Reservation Style	Reservation style: ● SE ● FF
Reservation Incoming Interface	Incoming interface for the reservation message.
Reservation Interface	Name of the interface on which bandwidth is reserved.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Message ID	ID of the Refresh Reduction message.
Filter Spec Information	Filtering conditions.
The filter number	Total number of filters.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local identifier of an LSP.
OutLabel	Outgoing label.
Cleanup Timer	Timeout timer.
RRO Information	Information about the RRO.
RRO-CType	Class type in the RRO: ● IPv4 ● Label
RRO-IPAddress	IP address in the RRO, in the format X.X.X.X.
RRO-IPPrefixLen	Length of the route prefix in the RRO.
RRO-Label	Label information in the RRO
FlowSpec Information	Traffic information including flow specifications.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size.
Bandwidth guarantees	Bandwidth guarantee.
Delay guarantees	Delay guarantee.
Qos Service	QoS guarantee/control.
Resv Message	Reservation message received on an interface.

Related Topics

11.2.17 display mpls rsvp-te psb-content

11.2.21 display mpls rsvp-te sender

Function

The **display mpls rsvp-te sender** command displays information about an RSVP-TE enabled interface as an RSVP-TE sender.

Format

display mpls rsvp-te sender [**interface** *interface-type interface-number peer-ip-address*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface receiving Path messages. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
peer-ip-address	Specifies the IP address of the outgoing interface on the previous hop sending Path messages.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no interface name is specified, the command displays the information about all RSVP-TE enabled interfaces as RSVP-TE senders.

Example

Display information about all RSVP-TE enabled interfaces as RSVP-TE senders.

```
<Huawei> display mpls rsvp-te sender
Interface: Incoming-Interface at the Ingress
 Tunnel Addr: 3.3.3.9              Ingress LSR ID: 1.1.1.9
 Local LSP ID: 3                  Session Tunnel ID: 300
 Session Name: Tunnel0/0/1
 Previous Hop Address:  -----
 Token bucket rate: 0.00           Token bucket size: 1000.00

 Tunnel Addr: 1.1.1.9              Ingress LSR ID: 3.3.3.9
 Local LSP ID: 4                  Session Tunnel ID: 300
 Session Name: Tunnel0/0/1
 Previous Hop Address: 10.1.1.2
 Token bucket rate: 0.00           Token bucket size: 1000.00
```

Table 11-64 Description of the display mpls rsvp-te sender command output

Item	Description
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Session Tunnel ID	Tunnel ID.
Session Name	Name of a session.
Previous Hop Address	Previous-hop address in the format X.X.X.X.
Token bucket rate	Token bucket rate.
Token bucket size	Token bucket size.
Interface: Incoming-Interface at the Ingress	Information about the RSB functioning as the ingress on the local node.

Related Topics

11.2.54 mpls rsvp-te

11.2.22 display mpls rsvp-te session

Function

The **display mpls rsvp-te session** command displays all information about any specified RSVP session.

Format

display mpls rsvp-te session *ingress-lsr-id tunnel-id egress-lsr-id*

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
tunnel-id	Specifies the tunnel ID.	The value is an integer that ranges from 0 to 65535.
egress-lsr-id	Specifies the egress LSR ID.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about the RSVP session includes information about the Path State Block (PSB), Reservation State Block (RSB), and ReFresh State Block (RFSB).

Example

Display all information about the RSVP session between nodes 1.1.1.9 and 3.3.3.9 (Tunnel ID is 300).

```
<Huawei> display mpls rsvp-te session 1.1.1.9 300 3.3.3.9
==============================================================
  Display PSB, RSB and RFSB information in session table
==============================================================
==============================================================
                    The PSB Content
==============================================================
 Tunnel Addr: 3.3.3.9                    Exist time: 1h 1m 4s
 Tunnel ExtID: 1.1.1.9                   Session ID: 300
 Ingress LSR ID: 1.1.1.9                 Local LSP ID: 4
 Previous Hop :  ----- /0x0     Next Hop : 172.1.1.2
 Incoming / Outgoing Interface: -----  / GigabitEthernet1/0/0
 InLabel : NULL                          OutLabel : 1042
 Send Message ID : 29                    Recv Message ID : 0
 Refresh Timer : 504613692               Cleanup Timer : ---
 Session Attribute-
  SetupPrio: 0         HoldPrio: 0
  SessionAttrib: Local Protect desired. Node Protect desired. Label Recording de
sired. SE Style desired.
 LSP Type: -
 FRR Flag : No protection                Local RRO Flag : 0x0
 ERO Information-
     L-Type         ERO-IPAddr       ERO-PrefixLen
   ERHOP_STRICT    172.1.1.2            32
   ERHOP_STRICT    172.2.1.1            32
   ERHOP_STRICT    172.2.1.2            32
 RRO Information-
    -----
 SenderTspec Information-
  Token bucket rate: 0.00
  Token bucket size: 1000.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 4294967295
 CT-BandWidth Information:
 CT0 BandWidth(Bytes/sec): 625000.00    CT1 BandWidth(Bytes/sec): 625000.00
 CT2 BandWidth(Bytes/sec): -            CT3 BandWidth(Bytes/sec): -
 CT4 BandWidth(Bytes/sec): -            CT5 BandWidth(Bytes/sec): -
 CT6 BandWidth(Bytes/sec): -            CT7 BandWidth(Bytes/sec): -
 Path Message arrive on ----- from PHOP  -----
 Path Message sent to NHOP 172.1.1.2  on GigabitEthernet1/0/0
 Resource Reservation OK

 LSP Statistics Information:
   SendPacketCounter: 106         RecvPacketCounter: 115
   SendPathCounter: 106           RecvPathCounter: 0
   SendResvCounter: 0             RecvResvCounter: 115
```

```
=============================================================
                    The RSB Content
=============================================================
 Tunnel Addr: 3.3.3.9                Session Tunnel ID: 300
 Tunnel ExtID: 1.1.1.9
 Next Hop: 172.1.1.2                 Reservation Style: SE Style
 Reservation Incoming Interface: GigabitEthernet1/0/0
 Reservation Interface: GigabitEthernet1/0/0
 Message ID : 0
 Filter Spec Information-
   The filter number: 1
   Ingress LSR ID: 1.1.1.9        Local LSP ID: 4       OutLabel: 1042
   Cleanup Timer : 504613800
   RRO Information-
     RRO-CType: IPV4   RRO-IPAddress: 172.1.1.2        RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1042
     RRO-CType: IPV4   RRO-IPAddress: 2.2.2.9          RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 1042
     RRO-CType: IPV4   RRO-IPAddress: 172.2.1.1        RRO-IPPrefixLen: 32
     RRO-CType: IPV4   RRO-IPAddress: 172.2.1.2        RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 3
     RRO-CType: IPV4   RRO-IPAddress: 3.3.3.9          RRO-IPPrefixLen: 32
     RRO-CType: Label    RRO-Label: 3
 FlowSpec Information-
   Token bucket rate: 0.00
   Token bucket size: 1000.00
   Peak data rate: 0.00
   Minimum policed unit: 0
   Maximum packet size: 1500
   Bandwidth guarantees: 0.00
   Delay guarantees: 0
   Qos Service is Controlled
 Resv Message arrive on GigabitEthernet1/0/0 from NHOP 172.1.1.2
```

Table 11-65 Description of the display mpls rsvp-te session command output

Item	Description
The PSB Content	Contents of the PSB.
Tunnel Addr	Tunnel destination address in the format X.X.X.X.
Exist time	Time elapsed since the PSB is created.
Tunnel ExtID	Tunnel extension ID (ingress LSR ID) in the format X.X.X.X.
Session ID/ Session Tunnel ID	Tunnel ID.
Ingress LSR ID	LSR ID of the ingress node in the format X.X.X.X.
Local LSP ID	Local LSP ID.
Previous Hop	Previous-hop address in the format X.X.X.X.
Next Hop	Next-hop address in the format X.X.X.X.
Incoming / Outgoing Interface	Name of the incoming or outgoing interface.

Item	Description
InLabel	Value of an incoming label.
OutLabel	Value of an outgoing label.
Send Message ID	ID of the sent refresh reduction message.
Recv Message ID	ID of the received refresh reduction message.
Refresh Timer	ID of the Refresh timer.
Cleanup Timer	ID of the Cleanup timer.
Session Attribute	Attribute of a session.
SetupPrio	Setup priority of a session.
HoldPrio	Holding priority of a session.
SessionAttrib	Session attributes, including required local protection, bandwidth protection, node protection, label record, and reservation style.
LSP Type	Type of an LSP.
FRR Flag	Flag bit of FRR: ● No protection: indicates no FRR protection. ● PLR in use: provides protection on the Point of Local Repair. ● MP in use: provides protection on the Merge Point. ● Under protecting: provides FRR protection.
Local RRO Flag	Flag bit of the local RRO.
ERO Information	Information about the Explicit Route Object (ERO).
L-Type	Types of the explicit route: ● ERHOP_STRICT ● ERHOP_LOOSE
ERO-IPAddr	Explicit route address.
ERO-PrefixLen	Explicit route prefix length.
RRO Information	Information about the Record Route Object (RRO).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RRO-CType	Recording Class C routes, including IPv4 or IPv6 addresses and labels.
RRO-IPAddress	IPv4 or IPv6 address of the recorded route.
RRO-IPPrefixLen	Prefix length of a recorded route.
RRO-Label	Label information in the RRO.
SenderTspec Information	Information about the traffic specification of the sender.
Token bucket rate	Token bucket rate, in byte/s.
Token bucket size	Token bucket size.
Peak data rate	Peak data rate, in byte/s.
Minimum policed unit	Minimum policed unit.
Maximum packet size	Maximum packet size, in bytes.
CT-BandWidth Information	Bandwidth information corresponding to each CT.
CT0 - CT7 Bandwidth	Bandwidth values of LSPs of CT0 to CT7.
Path Message arrive on	Pre-hop addresses and incoming interfaces of messages.
Path Message sent to	Next-hop addresses and outgoing interfaces of messages.
Resource Reservation OK	Displayed only when the resource reservation flag is set.
LSP Statistics Information	Statistics of LSPs.
SendPacketCounter	Number of sent packets.
RecvPacketCounter	Number of received packets.
SendPathCounter	Number of sent Path messages.
RecvPathCounter	Number of received Path messages.
SendResvCounter	Number of sent Resv messages.
RecvResvCounter	Number of received Resv messages.
The RSB Content	Number of Reservation State Blocks (RSBs).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reservation Style	Reservation style: ● SE: Shared Explicit Style ● FF: Fixed-Filter Style
Reservation Incoming Interface	Incoming interface for the reservation message.
Reservation Interface	Name of the interface on which bandwidth is reserved.
Message ID	Message ID locally allocated, used in the Srefresh feature and reliability.
Filter Spec Information	Filtering conditions.
The filter number	Total number of filters.
FlowSpec Information	Information about flow specifications.
Bandwidth guarantees	Bandwidth guarantee.
Delay guarantees	Delay guarantee.
Qos Service is Controlled	QoS guarantee.
Resv Message arrive on	Incoming interfaces and previous-hop addresses of messages.

11.2.23 display mpls rsvp-te statistics

Function

The **display mpls rsvp-te statistics** command displays statistics on RSVP-TE.

Format

display mpls rsvp-te statistics { **global** | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Displays the global statistics on RSVP-TE.	-
interface	Displays statistics on RSVP-TE on all interface that enabled RSVP-TE function.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Displays statistics on RSVP-TE on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the global RSVP-TE statistics.

```
<Huawei> display mpls rsvp-te statistics global
 LSR ID: 10.1.1.1                    LSP Count: 0
 PSB Count: 0                        RSB Count: 0
 RFSB Count: 0

Total Statistics Information:
 PSB CleanupTimeOutCounter: 0         RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 0                 RecPacketCounter: 0
 SendCreatePathCounter: 0             RecCreatePathCounter: 0
 SendRefreshPathCounter: 0            RecRefreshPathCounter: 0
 SendCreateResvCounter: 0             RecCreateResvCounter: 0
 SendRefreshResvCounter: 0            RecRefreshResvCounter: 0
 SendResvConfCounter: 0               RecResvConfCounter: 0
 SendHelloCounter: 0                  RecHelloCounter: 0
 SendAckCounter: 0                    RecAckCounter: 0
 SendPathErrCounter: 0                RecPathErrCounter: 0
 SendResvErrCounter: 0                RecResvErrCounter: 0
 SendPathTearCounter: 0               RecPathTearCounter: 0
 SendResvTearCounter: 0               RecResvTearCounter: 0
 SendSrefreshCounter: 0               RecSrefreshCounter: 0
 SendAckMsgCounter: 0                 RecAckMsgCounter: 0
 SendChallengeMsgCounter: 0           RecChallengeMsgCounter: 0
 SendResponseMsgCounter: 0            RecResponseMsgCounter: 0
 SendErrMsgCounter: 0                 RecErrMsgCounter: 0
 SendRecoveryPathMsgCounter: 0        RecRecoveryPathMsgCounter: 0
 SendGRPathMsgCounter: 0              RecGRPathMsgCounter: 0
 ResourceReqFaultCounter: 0           RecGRPathMsgFromLSPMCounter: 0
 Bfd neighbor count: 0                Bfd session count: 0
```

Table 11-66 Description of the display mpls rsvp-te statistics command output

Item	Description
LSR ID	Local LSR ID.
PSB Count	Number of PSBs.

Item	Description
RSB Count	Number of RSBs.
RFSB Count	Number of RFSBs.
LSP Count	Number of LSPs established through RSVP TE.
Total Statistics Information	Total statistics information.
PSB CleanupTimeOutCounter	Number of times that the PSB is reset after the timer expires.
RSB CleanupTimeOutCounter	Number of times that the RSB is reset after the timer expires.
SendPacketCounter	Number of sent packets.
RecPacketCounter	Number of received packets.
SendCreatePathCounter	Number of sent CreatePath messages.
RecCreatePathCounter	Number of received CreatePath messages.
SendRefreshPathCounter	Number of sent RefreshPath messages.
RecRefreshPathCounter	Number of received RefreshPath messages.
SendCreateResvCounter	Number of sent CreateResv messages.
RecCreateResvCounter	Number of received CreateResv messages.
SendRefreshResvCounter	Number of sent RefreshResv messages.
RecRefreshResvCounter	Number of received RefreshResv messages.
SendResvConfCounter	Number of sent ResvConf messages.
RecResvConfCounter	Number of received ResvConf messages.
SendHelloCounter	Number of sent Hello messages.
RecHelloCounter	Number of received Hello messages.
SendAckCounter	Number of sent Ack messages.
RecAckCounter	Number of received Ack messages.
SendPathErrCounter	Number of sent PathErr messages.
RecPathErrCounter	Number of received PathErr messages.
SendResvErrCounter	Number of sent ResvErr messages.
RecResvErrCounter	Number of received ResvErr messages.
SendPathTearCounter	Number of sent PathTear messages.
RecPathTearCounter	Number of received PathTear messages.
SendResvTearCounter	Number of sent ResvTear messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RecResvTearCounter	Number of received ResvTear messages.
SendSrefreshCounter	Number of sent Srefresh messages.
RecSrefreshCounter	Number of received Srefresh messages.
SendAckMsgCounter	Number of sent Msg_ID_ACK messages.
RecAckMsgCounter	Number of received Msg_ID_ACK messages.
SendChallengeMsgCounter	Number of sent Challenge messages.
RecChallengeMsgCounter	Number of received Challenge messages.
SendResponseMsgCounter	Number of sent Response messages.
RecResponseMsgCounter	Number of received Response messages.
SendErrMsgCounter	Number of sent Msg_ID_NACK messages.
RecErrMsgCounter	Number of received Msg_ID_NACK messages.
SendRecoveryPathMsg-Counter	Number of sent Recovery Path messages.
RecRecoveryPathMsgCount-er	Number of received Recovery Path messages.
SendGRPathMsgCounter	Number of sent GR Path messages.
RecGRPathMsgCounter	Number of received GR Path messages.
ResourceReqFaultCounter	Number of failed attempts to request resources.
RecGRPathMsgFromLSPM-Counter	Number of GR Path messages received from the LSPM module.
Bfd neighbor count	Number of upstream or downstream BFD peers through which at least one LSP in the Up state passes.
Bfd session count	Number of BFD sessions.

Related Topics

11.2.139 reset mpls rsvp-te statistics

11.2.24 display mpls rsvp-te statistics fast-reroute

Function

The **display mpls rsvp-te statistics fast-reroute** command displays the CR-LSP statistics on the local node serving as a Point of Local Repair (PLR) or Merge Point (MP).

Format

display mpls rsvp-te statistics fast-reroute

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can be used to check the following information:

- Number of CR-LSPs in the PLR Available state
- Number of CR-LSPs in the PLR Inuse state
- Number of CR-LSPs in the MP Available state
- Number of CR-LSPs in the MP Inuse state

Example

Display CR-LSP statistics information on the local node serving as PLR or MP.

```
<Huawei> display mpls rsvp-te statistics fast-reroute
FRR statistics information:
 PLR AvailLsps: 0                PLR InuseLsps: 0
 MP AvailLsps: 0                 MP InuseLsps: 0
```

Table 11-67 Description of the display mpls rsvp-te statistics fast-reroute command output

Item	Description
PLR AvailLsps	Number of CR-LSPs whose local node is the PLR in the PLR Available state (the CR-LSPs are bound to the bypass tunnel but FRR does not occur on the PLR).
PLR InuseLsps	Number of CR-LSPs whose local node is the PLR in the PLR Inuse state.
MP AvailLsps	Number of CR-LSPs whose local node is the MP in the MP Available state (the CR-LSPs are bound to the bypass tunnel but FRR does not occur on the MP).
MP InuseLsps	Number of CR-LSPs whose local node is the MP in the MP Inuse state.

 Copyright © Huawei Technologies Co., Ltd.

11.2.25 display mpls static-cr-lsp

Function

The **display mpls static-cr-lsp** command displays information about a static CR-LSP.

Format

display mpls static-cr-lsp [*lsp-name*] [{ **include** | **exclude** } *ip-address mask-length*] [**verbose**]

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of an LSP.	The value is an existing LSP name.
exclude	Displays information about the CR-LSPs without specified destination IP addresses.	-
include	Displays information about the CR-LSPs of specified destination IP addresses.	-
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of a destination address.	The value is an integer that ranges from 0 to 32.
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display brief information about static CR-LSPs.

```
<Huawei> display mpls static-cr-lsp
TOTAL         : 2     STATIC CRLSP(S)
UP            : 2     STATIC CRLSP(S)
DOWN          : 0     STATIC CRLSP(S)
Name            FEC               I/O Label    I/O If            Status
```

```
Tunnel0/0/1      3.3.3.3/32      NULL/20      -/GE1/0/0       Up
Tunnel0/0/2      3.3.3.3/32      NULL/20      -/GE1/0/0       Up
```

Table 11-68 Description of the display mpls static-cr-lsp command output

Item	Description
TOTAL	Total number of static CR-LSPs.
UP	Number of the static CR-LSPs in the Up state.
DOWN	Number of the static CR-LSPs in the DOWN state.
Name	Name of a static CR-LSP.
FEC	Destination IP address and mask length.
I/O Label	Incoming and outgoing labels.
I/O If	Incoming and outgoing interfaces.
Status	Current status of a CR-LSP.

Display detailed information about static CR-LSPs.

```
<Huawei> display mpls static-cr-lsp verbose
No             : 1
LSP-Name       : tunnel0/0/1
LSR-Type       : Transit
FEC            : -/-
In-Label       : 20
Out-Label      : 30
In-Interface   : GigabitEthernet1/0/0
Out-Interface  : GigabitEthernet2/0/0
NextHop        : 10.1.3.2
Lsp Status     : Up
```

Table 11-69 Description of the display mpls static-cr-lsp verbose command output

Item	Description
No	Sequence number of a static CR-LSP.
LSP-Name	Name of a static CR-LSP.
LSR-Type	Type of a static CR-LSP: ● Ingress ● Transit ● Egress
FEC	Destination address and mask length. "-/-" is displayed for the transit node and egress node.
In-Label	Value of an incoming label.

Item	Description
Out-Label	Value of an outgoing label.
In-Interface	Incoming interface.
Out-Interface	Outgoing interface.
NextHop	Next-hop address in the format X.X.X.X.
Lsp Status	Status of a static CR-LSP: ● Up: indicates that the static CR-LSP is successfully established. ● Down: indicates that the static CR-LSP fails to be established.

Related Topics

11.1.40 display mpls lsp

11.2.26 display mpls stale-interface

Function

The **display mpls stale-interface** command displays information about MPLS interfaces in the Stale state.

Format

display mpls stale-interface [*interface-index*] [**verbose**]

Parameters

Parameter	Description	Value
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer ranging from 1 to FFFFFFFE.
verbose	Displays detailed information about an interface, for example, whether FRR is configured. If FRR is configured, information about the bound tunnels is also displayed.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The outbound interface of the primary tunnel protected by TE FRR becomes a stale interface in one of the following situations:

- The interface board where the interface resides is removed.
- MPLS is disabled on the interface when the primary tunnel is in the FRR In-used state.

The **display mpls stale-interface** command displays information about the stale interfaces.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

Display information about all MPLS interfaces in the Stale state.

```
<Huawei> display mpls stale-interface
Stale-Interface      Status    TE Attr   LSP Count  CRLSP Count Effective MTU
0x81a                Up        Dis       0          1           1500
```

Table 11-70 Description of the display mpls stale-interface command output

Item	Description
Stale-Interface	Index of an MPLS interface in the Stale state.
Status	Status of the stale interface. ● Up ● Down
TE Attr	Whether MPLS TE is enabled on an interface: ● Dis: MPLS TE is not enabled on the interface. ● En: MPLS TE is enabled on the interface.
LSP Count	Number of LSPs on an interface.
CRLSP Count	Number of CR-LSPs on an interface.
Effective MTU	MTU value used in the MPLS forwarding. ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.

Display detailed information about all MPLS interfaces in the Stale state.

```
<Huawei> display mpls stale-interface verbose
No                  : 1
```

```
Interface          :  0x81a
Status             :  Up
TE Attribute       :  Disable
Static LSPCount    :  0
Static CR-LSPCount :  0
LDP LSPCount       :  0
RSVP LSPCount      :  1
MPLS MTU           :  -
Interface MTU      :  -
Effective MTU      :  1500
TE FRR             :  Enable
Manual Bypass      :  Tun0/0/1
Interface State    :  Stale
```

Table 11-71 Description of the display mpls stale-interface verbose command output

Item	Description
No	Serial number.
Interface	Index of an MPLS interface in the Stale state.
Status	Status of the stale interface, which is the Up state in this example.
TE Attribute	Whether MPLS TE is enabled on the interface: ● Disable: MPLS TE is disabled. ● Enable: MPLS TE is enabled.
Static LSPCount	Number of static LSPs created on the interface.
Static CR-LSPCount	Number of static CR-LSPs created on the interface.
LDP LSPCount	Number of LDP LSPs created on the interface.
RSVP LSPCount	Number of RSVP-TE LSPs created on the interface.
MPLS MTU	MPLS MTU set using the **mpls mtu** command. When the interface is in the Stale state, a hyphen (-) is displayed.
Interface MTU	MTU configured on the interface.
Effective MTU	MTU value used in the MPLS forwarding. ● If the MPLS MTU is not set, the interface MTU takes effect. ● If the MPLS MTU is set, the smaller one between the MPLS MTU and the interface MTU takes effect.
TE FRR	Whether MPLS TE is enabled on the interface: ● Disable: No bypass tunnel is set up in manual FRR mode to protect the interface. ● Enable: A bypass tunnel is set up in manual FRR mode to protect the interface.
Manual Bypass	Name of a bypass tunnel set up in manual FRR mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface State	Interface status. Stale indicates that the interface is to be deleted.

Related Topics

11.2.140 reset mpls stale-interface

11.2.27 display mpls te cspf destination

Function

The **display mpls te cspf destination** command helps you check whether the specified path is available or not. You can specify relevant parameters in the command to set constraint conditions.

Format

display mpls te cspf destination *ip-address* [**affinity** *properties* [**mask** *mask-value*] | **bandwidth** { **ct0** *ct0-bandwidth* | **ct1** *ct1-bandwidth* | **ct2** *ct2-bandwidth* | **ct3** *ct3-bandwidth* | **ct4** *ct4-bandwidth* | **ct5** *ct5-bandwidth* | **ct6** *ct6-bandwidth* | **ct7** *ct7-bandwidth* } * | **explicit-path** *path-name* | **hop-limit** *hop-limit-number* | **metric-type** { **igp** | **te** } | **priority** *setup-priority* | **srlg-strict** *exclude-path-name* | **tie-breaking** { **random** | **most-fill** | **least-fill** }] * [**hot-standby** [**explicit-path** *path-name* | **overlap-path** | **affinity** *properties* [**mask** *mask-value*] | **hop-limit** *hop-limit-number* | **srlg** { **preferred** | **strict** }] *]

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the destination IP address of an MPLS TE tunnel.	The value is in dotted decimal notation.
affinity *properties*	Specifies the affinity property of an MPLS TE tunnel.	The value is a hexadecimal number that ranges from 0 to FFFFFFFF.
mask *mask-value*	Specifies the value of the affinity property mask.	The value is a hexadecimal number that ranges from 0 to FFFFFFFF.
bandwidth	Specifies the required bandwidth of an MPLS TE tunnel.	-
ct0 *ct0-bandwidth* - **ct7** *ct7-bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT7.	The value is an integer that ranges from 1 to 4000000000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
explicit-path *path-name*	Specifies the explicit path of an MPLS TE tunnel.	The value is an existing explicit path name.
hop-limit *hop-limit-number*	Specifies the maximum number of hops on an MPLS TE tunnel.	The value is an integer that ranges from 1 to 32. By default, the maximum number of hops is 32.
metric-type	Specifies the metric type for the CSPF calculation.	-
igp	Specifies the metric type as IGP.	-
te	Specifies the metric type as TE.	-
priority *setup-priority*	Specifies the setup priority of an MPLS TE tunnel.	The value is an integer that ranges from 0 to 7.
srlg-strict *exclude-path-name*	Specifies the path of a specified SRLG.	The value is an existing explicit path name.
tie-breaking	Configures a tie-breaking mode for CSPF.	-
random	Configures the random mode.	-
most-fill	Configures the most-fill mode, meaning the path with the highest ratio of used bandwidth to maximum reservable bandwidth is selected.	-
least-fill	Configures the least-fill mode, meaning the path with the lowest ratio of used bandwidth to the maximum capacity of reservable bandwidth is selected.	-
hot-standby	Configures hot-standby path excluding primary path.	-
overlap-path	Specifies that if a completely disjoint path is not available, a maximally disjoint path should be computed for the Hot-standby.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
srlg preferred	Specifies that the SRLG attribute is an optional constraint used by CSPF to calculate the path for the hot-standby CR-LSP. If CSPF fails to calculate the path for the hot-standby CR-LSP based on the SRLG attribute, CSPF recalculates the path, regardless of the SRLG attribute.	-
srlg strict	Specifies that the SRLG attribute is a required constraint used by CSPF to calculate the path for the hot-standby CR-LSP. The links of the hot-standby CR-LSP and the primary CR-LSP cannot be in the same SRLG.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Prerequisites

Before running this command, the CSPF function must have been enabled by using the **mpls te cspf** command.

Precautions

When this command is run, the device uses CSPF to check whether or not there is a path satisfying the specified constraints. If such a path exists, its information is displayed; otherwise, the display is empty.

Example

Display the path with the destination address being 3.3.3.9 by performing the CSPF calculation.

```
<Huawei> display mpls te cspf destination 3.3.3.9
Path for the given constraints is:
1.1.1.9                 Include      LSR-ID
10.1.1.1                Include
10.1.1.2                Include
2.2.2.9                 Include      LSR-ID
10.2.1.1                Include
10.2.1.2                Include
3.3.3.9                 Include      LSR-ID
The total metrics of the calculated path is :  2
```

Display the explicit path named path1 with the destination address being 3.3.3.9 by performing the CSPF calculation.

```
<Huawei> display mpls te cspf destination 3.3.3.9 explicit-path path1
Path for the given constraints is:
1.1.1.9                 Include       LSR-ID
10.1.1.1                Include
10.1.1.2                Include
2.2.2.9                 Include       LSR-ID
10.2.1.1                Include
10.2.1.2                Include
3.3.3.9                 Include       LSR-ID
The total metrics of the calculated path is :   2
```

Display the hot standby path with the destination address being 3.3.3.9 by performing the CSPF calculation.

```
<Huawei> display mpls te cspf destination 3.3.3.9 hot-standby
Path for the given constraints is:
1.1.1.9                 Include       LSR-ID
10.1.1.1                Include
10.1.1.2                Include
2.2.2.9                 Include       LSR-ID
10.2.1.1                Include
10.2.1.2                Include
3.3.3.9                 Include       LSR-ID
The total metrics of the calculated path is :   2

Hot-standby path for the given constraints is:
1.1.1.9                 Include       LSR-ID
10.4.1.1                Include
10.4.1.2                Include
6.6.6.9                 Include       LSR-ID
10.5.1.1                Include
10.5.1.2                Include
3.3.3.9                 Include       LSR-ID
Complete disjoint path computed and the total metrics of the calculated path is :    2
```

Display the hot standby path with the destination address being 4.4.4.9 and partial overlapping by performing the CSPF calculation.

```
<Huawei> display mpls te cspf destination 4.4.4.9 hot-standby overlap-path
Main path for the given constraints is:
1.1.1.9                 Include       LSR-ID
10.1.1.1                Include
10.1.1.2                Include
2.2.2.9                 Include       LSR-ID
10.2.1.1                Include
10.2.1.2                Include
3.3.3.9                 Include       LSR-ID
10.3.1.1                Include
10.3.1.2                Include
4.4.4.9                 Include       LSR-ID
The total metrics of the calculated path is :   3

Hot-standby path for the given constraints is:
1.1.1.9                 Include       LSR-ID
10.6.1.1                Include
10.6.1.2                Include
6.6.6.9                 Include       LSR-ID
10.7.1.1                Include
10.7.1.2                Include
3.3.3.9                 Include       LSR-ID
10.3.1.1                Include
10.3.1.2                Include
4.4.4.9                 Include       LSR-ID
Partial Overlap path computed and the total metrics of the calculated path is :
  3
```

Table 11-72 Description of the display mpls te cspf destination command output

Item	Description
Path for the given constraints is	Path calculated by CSPF. If * is displayed, it indicates the node does not exist on the explicit path calculated by CSPF. If * is not displayed, it indicates that the node exists on the path calculated by CSPF.
1.1.1.9 Include LSR-ID	Path information. 1.1.1.9 is the next hop address, Include is the node name, and LSR-ID indicates that the LSR ID is used as the address.
The total metrics of the calculated path is	Calculated metric value of a path.
Main path for the given constraints is	Path for the main request, when both main and hot-standby is requested.
Hot-standby path for the given constraints is	Path calculated by CSPF for the hot-standby.
Complete disjoint path computed and the total metrics of the calculated path is	CSPF has calculated complete disjoint path from main path for hot-standby.
Partial Overlap path computed and the total metrics of the calculated path is	CSPF has calculated partial overlap path from main path for hot-standby.

Related Topics

11.2.100 mpls te cspf

11.2.28 display mpls te cspf tedb

Function

The **display mpls te cspf tedb** command displays the CSPF TEBD information based on specified conditions.

Format

display mpls te cspf tedb { **all** | **area** { *area-id* | *area-id-ip* } | **interface** *ip-address* | **network-lsa** | **node** [*router-id*] | **srlg** *srlg-number* | **overload-node** }

Parameters

Parameter	Description	Value
all	Displays information about all TEDB nodes.	-
area *area-id*	Specifies the ID of an area.	For an OSPF area, the value is an integer that ranges from 0 to 4294967295. For an IS-IS area, the value is 1 or 2.
area *area-id-ip*	Specifies the ID of an area in IP address format.	For an OSPF area, the value is in dotted decimal notation.
interface *ip-address*	Specifies the IP address of an interface	The value is in dotted decimal notation.
network-lsa	Displays information about all network LSAs.	-
node	Displays information about a node.	-
router-id	Specifies the router ID.	The value is in dotted decimal notation.
srlg *srlg-number*	Specifies the SRLG number.	The value is an integer that ranges from 0 to 4294967295.
overload-node	Displays information of all the overload-nodes.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display information about network LSAs in a TEDB.

```
<Huawei> display mpls te cspf tedb network-lsa
Maximum Network LSA Supported    : 512
Current Total Network LSA Number : 6

ID : 1
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 2.2.2.9
   DR-Address : 172.1.1.2
   Area : 0
```

```
  DR-OSPF-Router-ID : 2.2.2.9
    NBR-Router-ID      NBR-OSPF-Router-ID
    2.2.2.9            2.2.2.9
    1.1.1.9            1.1.1.9

ID : 2
  IGP-Type: OSPF
  Process-ID: 1
  DR-Router-ID : 2.2.2.9
  DR-Address : 172.2.1.1
  Area : 0
  DR-OSPF-Router-ID : 2.2.2.9
    NBR-Router-ID      NBR-OSPF-Router-ID
    2.2.2.9            2.2.2.9
    3.3.3.9            3.3.3.9

ID : 3
  IGP-Type: ISIS
  Process-ID: 1
  DR-Router-ID : 1.1.1.9
  DR-Address : 172.1.1.1
  Area : Level-2
  DR-ISIS-System-ID : 0000.0000.0001.01
    NBR-Router-ID      NBR-ISIS-System-ID
    1.1.1.9            0000.0000.0001.00
    2.2.2.9            0000.0000.0002.00

ID : 4
  IGP-Type: ISIS
  Process-ID: 1
  DR-Router-ID : 1.1.1.9
  DR-Address : 172.1.1.1
  Area : Level-1
  DR-ISIS-System-ID : 0000.0000.0001.01
    NBR-Router-ID      NBR-ISIS-System-ID
    1.1.1.9            0000.0000.0001.00
    2.2.2.9            0000.0000.0002.00

ID : 5
  IGP-Type: ISIS
  Process-ID: 1
  DR-Router-ID : 3.3.3.9
  DR-Address : 172.2.1.2
  Area : Level-1
  DR-ISIS-System-ID : 0000.0000.0003.01
    NBR-Router-ID      NBR-ISIS-System-ID
    3.3.3.9            0000.0000.0003.00
    2.2.2.9            0000.0000.0002.00

ID : 6
  IGP-Type: ISIS
  Process-ID: 1
  DR-Router-ID : 3.3.3.9
  DR-Address : 172.2.1.2
  Area : Level-2
  DR-ISIS-System-ID : 0000.0000.0003.01
    NBR-Router-ID      NBR-ISIS-System-ID
    3.3.3.9            0000.0000.0003.00
    2.2.2.9            0000.0000.0002.00
```

Table 11-73 Description of the display mpls te cspf tedb network-lsa command output

Item	Description
Maximum Network LSA Supported	Maximum network LSAs supported.

Item	Description
Current Total Network LSA Number	Current total number of network LSAs.
IGP-Type	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
ID	Sequence number.
DR-Router-ID	DR Router ID.
DR-Address	Interface address of the DR.
Area	Area to which the device belongs.
DR-OSPF-Router-ID	OSPF router ID of a DR.
DR-ISIS-System-ID	IS-IS system ID of a DR.
NBR-Router-ID	Neighbor Router ID.
NBR-OSPF-Router-ID	Neighbor OSPF router ID.
NBR-ISIS-System-ID	Neighbor IS-IS system ID.

Display information about all TEDBs.

```
<Huawei> display mpls te cspf tedb all
Maximum Nodes Supported: 1024   Current Total Node Number: 6
Maximum Links Supported: 2048   Current Total Link Number: 12
Maximum SRLGs supported: 5120   Current Total SRLG Number: 0
ID     Router-ID       IGP     Process-ID     Area          Link-Count
1      1.1.1.9         OSPF    1              0             1
2      2.2.2.9         OSPF    1              0             2
3      3.3.3.9         OSPF    1              0             1
4      1.1.1.9         ISIS    1              Level-1,2     2
5      2.2.2.9         ISIS    1              Level-1,2     4
6      3.3.3.9         ISIS    1              Level-1,2     2
```

Table 11-74 Description of the **display mpls te cspf tedb all** command output

Item	Description
Maximum Nodes Supported	Maximum number of nodes supported.
Maximum Links Supported	Maximum number of links supported.
Maximum SRLGs supported	Maximum SRLGs supported.
Current Total Node Number	Current total number of nodes.
Current Total Link Number	Current total number of links.
Current Total SRLG Number	Current total number of SRLGs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
Area	Area to which the device belongs.
Link-Count	Total number of connected links with a specified IGP and process ID.

Display TEDB information of a specified area.

```
<Huawei> display mpls te cspf tedb area 0
 Router Node Information for Area 0:
ID     Router-ID        IGP      Process-ID     Area           Link-Count
1      1.1.1.9          OSPF     1              0              1
2      2.2.2.9          OSPF     1              0              2
3      3.3.3.9          OSPF     1              0              1

Network LSA Information for Area 0:

ID : 1
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 2.2.2.9
   DR-Address : 172.1.1.2
   Area : 0
   DR-OSPF-Router-ID : 2.2.2.9
     NBR-Router-ID       NBR-OSPF-Router-ID
     2.2.2.9             2.2.2.9
     1.1.1.9             1.1.1.9

ID : 2
   IGP-Type: OSPF
   Process-ID: 1
   DR-Router-ID : 2.2.2.9
   DR-Address : 172.2.1.1
   Area : 0
   DR-OSPF-Router-ID : 2.2.2.9
     NBR-Router-ID       NBR-OSPF-Router-ID
     2.2.2.9             2.2.2.9
     3.3.3.9             3.3.3.9
```

Table 11-75 Description of the display mpls te cspf tedb area command output

Item	Description
Router Node Information for Area 0	Router node information for area 0.
Network LSA Information for Area 0	Network LSA information for area 0.

Item	Description
Link-Count	Total number of connected links with a specified IGP and process ID.
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
IGP-Type	IGP type: ● OSPF ● IS-IS
Process-ID	IGP process ID.
DR-Router-ID	Router ID of the DR.
DR-Address	Interface address of the DR.
Area	Area to which the device belongs.
DR-OSPF-Router-ID	OSPF router ID of the designated router.
NBR-Router-ID	Router ID of a neighbor router.
NBR-OSPF-Router-ID	OSPF router ID of a neighbor device.

Display TEDB information of a specified node.

```
<Huawei> display mpls te cspf tedb node 1.1.1.9
 Router ID: 1.1.1.9
 IGP Type: OSPF      Process ID: 1
  MPLS-TE Link Count: 1
  Link[1]:
    OSPF Router ID: 1.1.1.9                Opaque LSA ID: 1.0.0.1
    Interface IP Address: 172.1.1.1
    DR Address: 172.1.1.2
    IGP Area: 0
    Link  Type: Multi-access  Link Status: Active
    IGP Metric: 1               TE Metric: 1           Color: 0x0
    Bandwidth Allocation Model : Russian Dolls Model
    Maximum Link Bandwidth: 40000 (kbps)
    Maximum Reservable Bandwidth: 40000 (kbps)
    Bandwidth Constraints:          Local Overbooking Multiplier:
        BC[0]:      40000 (kbps)           LOM[0]:          1
        BC[1]:      30000 (kbps)           LOM[1]:          1
        BC[2]:      20000 (kbps)           LOM[2]:          1
        BC[3]:          0 (kbps)           LOM[3]:          1
        BC[4]:          0 (kbps)           LOM[4]:          1
        BC[5]:          0 (kbps)           LOM[5]:          1
        BC[6]:          0 (kbps)           LOM[6]:          1
        BC[7]:          0 (kbps)           LOM[7]:          1
    BW Unreserved:
        Class  ID:
        [0]:          0 (kbps),            [1]:          0 (kbps)
        [2]:          0 (kbps),            [3]:          0 (kbps)
```

```
      [4]:        0 (kbps),          [5]:        0 (kbps)
      [6]:        0 (kbps),          [7]:        0 (kbps)
Router ID: 1.1.1.9
IGP Type: ISIS      Process ID: 1
 MPLS-TE Link Count: 2
 Link[1]:
   ISIS System ID: 0000.0000.0001.00      Opaque LSA ID: 0.0.0.0
   Interface IP Address: 172.1.1.1
   DR Address: 172.1.1.1
   DR ISIS System ID: 0000.0000.0001.01
   IGP Area: Level-2
   Link  Type: Multi-access  Link Status: Active
   IGP Metric: 10             TE Metric: 10         Color: 0x0
   Bandwidth Allocation Model : Russian Dolls Model
   Maximum Link Bandwidth: 40000 (kbps)
   Maximum Reservable Bandwidth: 40000 (kbps)
   Bandwidth Constraints:         Local Overbooking Multiplier:
       BC[0]:      40000 (kbps)          LOM[0]:         1
       BC[1]:      30000 (kbps)          LOM[1]:         1
       BC[2]:      20000 (kbps)          LOM[2]:         1
       BC[3]:          0 (kbps)          LOM[3]:         1
       BC[4]:          0 (kbps)          LOM[4]:         1
       BC[5]:          0 (kbps)          LOM[5]:         1
       BC[6]:          0 (kbps)          LOM[6]:         1
       BC[7]:          0 (kbps)          LOM[7]:         1
   BW Unreserved:
       Class  ID:
       [0]:        0 (kbps),          [1]:        0 (kbps)
       [2]:        0 (kbps),          [3]:        0 (kbps)
       [4]:        0 (kbps),          [5]:        0 (kbps)
       [6]:        0 (kbps),          [7]:        0 (kbps)
```

Table 11-76 Description of the display mpls te cspf tedb node command output

Item	Description
Router ID	Router ID in the format X.X.X.X.
IGP Type	IGP type: ● OSPF ● IS-IS
Process ID	IGP Process ID.
MPLS-TE Link Count	Number of MPLS TE link.
OSPF Router ID	OSPF Route ID.
ISIS System ID	IS-IS system ID.
Interface IP Address	Interface IP address.
DR Address	DR address.
DR ISIS System ID	IS-IS system ID of the DR.
IGP Area	IGP area.
Link Type	Link type.
Link Status	Link status.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Link [x]	Link information, with "x" being the link number.
IGP Metric	IGP metric of a link.
TE Metric	TE metric of a link.
Color	Color of a link.
Maximum Link Bandwidth	Maximum bandwidth of a link.
Maximum Reservable Bandwidth	Maximum capacity of reserved bandwidth for a link.
Bandwidth Allocation Model	Bandwidth allocation model.
Bandwidth Constraints	Bandwidth constraints.
Local Overbooking Multiplier	Local overbooking multiplier.
BC	Bandwidth constraints.
LOM	Local overbooking multiplier.
BW Unreserved	Unreserved bandwidth for LSPs.
Class ID: [x]:	Class 0 to Class 7.

Display information about overloaded nodes in a TEDB.

```
<Huawei> display mpls te cspf tedb overload-node
Current Total Overload Node Number : 4
ID     Router-ID      IGP     Process-ID   Area       IGP_ID
1      3.3.3.3        ISIS    1            Level-1    3333.3333.3333.00
2      1.1.1.1        ISIS    1            Level-1    1111.1111.1111.00
3      1.1.1.1        ISIS    2            Level-1    1111.1111.1112.00
4      2.2.2.2        ISIS    1            Level-1    2222.2222.2222.00
```

Table 11-77 Description of the display mpls te cspf tedb overload-node command output

Item	Description
ID	Sequence number.
Router-ID	Router ID in dotted decimal notation.
IGP	IGP type: ● OSPF ● IS-IS
Process-ID	IGP Process ID.
Area	Area to which a device belongs.

Item	Description
IGP_ID	• OSPF router ID of a neighbor device. • IS-IS system ID of a neighbor device.

Related Topics

11.2.100 mpls te cspf

11.2.29 display mpls te ds-te

Function

The **display mpls te ds-te** command displays information about DS-TE.

Format

display mpls te ds-te { **summary** | **te-class-mapping** [**default** | **config** | **verbose**] }

Parameters

Parameter	Description	Value
summary	Displays DS-TE configurations in the current system.	-
te-class-mapping	Displays information about the TE-class mapping table.	-
default	Displays information about the default TE-class mapping table.	-
config	Displays information about the configured TE-class mapping table.	-
verbose	Displays detailed information about the TE-class mapping table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DS-TE is configured, you can run this command to view related DS-TE configurations.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about DS-TE.

```
<Huawei> display mpls te ds-te summary
DS-TE IETF Supported :YES
DS-TE MODE           :IETF
Bandwidth Constraint Model  :RDM
TEClass Mapping (default):
TE-Class ID    Class Type     Priority
TE-Class 0     0              0
TE-Class 1     1              0
TE-Class 2     2              0
TE-Class 3     3              0
TE-Class 4     0              7
TE-Class 5     1              7
TE-Class 6     2              7
TE-Class 7     3              7
```

Table 11-78 Description of the display mpls te ds-te summary command output

Item	Description
DS-TE IETF Supported	Whether or not the current system supports the DS-TE IETF mode.
DS-TE MODE	DS-TE mode: ● IETF: indicates the DS-TE mode that is defined by the IETF. ● NON-IETF: indicates the DS-TE mode that is not defined by the IETF. To set the DS-TE mode, run the **mpls te ds-te mode** command.
Bandwidth Constraint Model	Bandwidth Constraints Model: ● RDM: indicates the Russian Dolls Model. ● MAM: indicates the Maximum Allocation Model. ● Extended MAM: indicates the extended Maximum Allocation Model. To set the Bandwidth Constraints Model, run the **mpls te ds-te bcm** command.
TEClass Mapping	TE-class mapping.
TE-Class ID	TE-class ID. The value ranges from 0 to 7.
Class Type	Service type. When the TE-class is not configured, "--" is displayed.
Priority	Preemption priority of a tunnel. The value ranges from 0 to 7. The smaller the value, the higher the preemption priority of the tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Display information about the configured TE-class mapping table in IETF mode on the local device.

```
<Huawei> display mpls te ds-te te-class-mapping config
  TE-Class ID        Class Type     Priority       Description
  TE-Class0          0              0              -
  TE-Class1          1              0              -
  TE-Class2          2              0              -
  TE-Class3          3              0              -
  TE-Class4          0              7              -
  TE-Class5          1              7              -
  TE-Class6          2              7              -
  TE-Class7          3              7              -
```

Display information about the default TE-class mapping table in IETF mode.

```
<Huawei> display mpls te ds-te te-class-mapping default
  TE-Class ID        Class Type     Priority       Description
  TE-Class0          0              0              -
  TE-Class1          1              0              -
  TE-Class2          2              0              -
  TE-Class3          3              0              -
  TE-Class4          0              7              -
  TE-Class5          1              7              -
  TE-Class6          2              7              -
  TE-Class7          3              7              -
```

Display detailed information about the TE-class mapping table in DS-TE IETF mode on the local device.

```
<Huawei> display mpls te ds-te te-class-mapping verbose
  TE-Class0  : <CT0,0>     Description  : -
  -------------------------------------------------------------
  Lsp Type       Total       Ingress     Transit     Egress
  STATIC CRLSP   0           0           0           0
  RSVP LSP       2           1           0           1

  TE-Class1  : <CT1,0>     Description  : -
  -------------------------------------------------------------
  Lsp Type       Total       Ingress     Transit     Egress
  STATIC CRLSP   0           0           0           0
  RSVP LSP       0           0           0           0

  TE-Class2  : <CT2,0>     Description  : -
  -------------------------------------------------------------
  Lsp Type       Total       Ingress     Transit     Egress
  STATIC CRLSP   0           0           0           0
  RSVP LSP       0           0           0           0

  TE-Class3  : <CT3,0>     Description  : -
  -------------------------------------------------------------
  Lsp Type       Total       Ingress     Transit     Egress
  STATIC CRLSP   0           0           0           0
  RSVP LSP       0           0           0           0

  TE-Class4  : <CT0,0>     Description  : -
  -------------------------------------------------------------
  Lsp Type       Total       Ingress     Transit     Egress
  STATIC CRLSP   0           0           0           0
  RSVP LSP       2           1           0           1

  TE-Class5  : <CT1,0>     Description  : -
  -------------------------------------------------------------
  Lsp Type       Total       Ingress     Transit     Egress
  STATIC CRLSP   0           0           0           0
  RSVP LSP       0           0           0           0

  TE-Class6  : <CT2,0>     Description  : -
  -------------------------------------------------------------
```

```
Lsp Type       Total       Ingress     Transit     Egress
STATIC CRLSP   0           0           0           0
RSVP LSP       0           0           0           0

TE-Class7  : <CT3,0>     Description  : -
-------------------------------------------------------------
Lsp Type       Total       Ingress     Transit     Egress
STATIC CRLSP   0           0           0           0
RSVP LSP       0           0           0           0
```

Table 11-79 Description of the display mpls te ds-te te-class-mapping verbose command output

Item	Description
Description	Description message.
TE-Class0 : <CT0,0>	TE-class mapping.
Lsp Type	LSP type. ● STATIC CRLSP: indicates static CR-LSP. ● RSVP LSP: indicates dynamic CR-LSP.
Total	Number of LSPs.
Ingress	Total number of LSPs on which the local LSR functions as the ingress node.
Transit	Total number of LSPs on which the local LSR functions as the transit node.
Egress	Total number of LSPs on which the local LSR functions as the egress node.

Related Topics

11.2.149 te-class-mapping

11.2.105 mpls te ds-te mode

11.2.30 display mpls te hot-standby state

Function

The **display mpls te hot-standby state** command displays the hot-standby status of all tunnels or a specified tunnel.

Format

display mpls te hot-standby state { **all** [**verbose**] | **interface tunnel** *interface-number* }

Parameters

Parameter	Description	Value
all	Displays the status of all hot-standby tunnels.	-
verbose	Displays detailed information about hot-standby tunnels.	-
interface tunnel *interface-number*	Displays the status of a specified hot-standby tunnel.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When running the **display mpls te hot-standby state** command, note the following issues:

- The command displays the status of only hot-standby TE tunnels.
- If a tunnel interface is deleted or traffic switches from the tunnel to an ordinary backup tunnel, no command output is displayed.

Example

Display the hot-standby status of Tunnel 0/0/1.

```
<Huawei> display mpls te hot-standby state interface tunnel 0/0/1
(s): same path
-----------------------------------------------------------------
Verbose information about the Tunnel0/0/1 hot-standby state
-----------------------------------------------------------------
session id                          : 300
main LSP token                      : 0x9
hot-standby LSP token               : 0x0
HSB switch result                   : Primary LSP
HSB switch reason                   : -
WTR config time                     : 10s
WTR remain time                     : -
using overlapped path               : -
```

Table 11-80 Description of the display mpls te hot-standby state command output

Item	Description
session id	Session ID, which is the configured tunnel ID.
main LSP token	Index of the primary CR-LSP.
hot-standby LSP token	Index of the hot-standby CR-LSP.

Item	Description
HSB switch result	Result of a switchover: ● Primary LSP: indicates that data is switched to the primary CR-LSP. ● Hot-standby LSP: indicates that data is switched to the hot-standby CR-LSP. ● Ordinary LSP: indicates that data is switched to the ordinary CR-LSP. ● Best-Effort LSP: indicates that data is switched to the best-effort path.
HSB switch reason	Reason why traffic is switched to the hot-standby LSP.
WTR config time	WTR time. If a primary CR-LSP recovers from a fault, the system waits for a period of time, or the WTR time, to switch data from the hot-standby CR-LSP or best-effort path to the primary LSP.
WTR remain time	WTR remain time.
using overlapped path	Whether or not the path of the primary tunnel and the path of the backup tunnel overlap: ● yes: indicates that they overlap. ● no: indicates that they do not overlap. ● -: indicates that the system does not check whether or not they overlap.

Display the hot-standby status of all hot-standby tunnels.

```
<Huawei> display mpls te hot-standby state all
(s): same path----------------------------------------------------------------
No.       tunnel name        session id     switch result                overlap
-----------------------------------------------------------------------
1         Tunnel0/0/1          3            Best-Effort LSP     no
2         Tunnel0/0/2          9            Primary LSP         no
```

Table 11-81 Description of the display mpls te hot-standby state all command output

Item	Description
No.	Sequence number.
tunnel name	Name of a tunnel.

Item	Description
session id	Session ID, which is the configured tunnel ID.
switch result	Result of a switchover: • Primary LSP: indicates that data is switched to the primary CR-LSP. • Hot-standby LSP: indicates that data is switched to the hot-standby CR-LSP. • Ordinary LSP: indicates that data is switched to the ordinary CR-LSP. • Best-Effort LSP: indicates that data is switched to the best-effort path.

Related Topics

11.2.87 mpls te backup

11.2.31 display mpls te link-administration admission-control

Function

The **display mpls te link-administration admission-control** command displays CR-LSP information received by all links, including bandwidth and priority.

Format

display mpls te link-administration admission-control [**interface** *interface-type interface-number* | **stale-interface** *interface-index*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about admission control of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
stale-interface *interface-index*	Displays information about admission control of a stale interface. *interface-index* specifies the index of the stale interface.	The value is a hexadecimal integer that ranges from 0x1 to 0xFFFFFFFE.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mpls stale-interface** command without specifying any parameter to view the index of a stale interface.

Example

Display information about the admission control of all MPLS TE links.

```
<Huawei> display mpls te link-administration admission-control
LspID                  In/Out IF                S/H Prio CT BW(kbps)
10.3.3.9:300:4           GE1/0/0 / ---            0 /0     -  -
10.1.1.9:300:3           --- / GE1/0/0            0 /0     -  -
```

Display information about admission control of a stale interface.

```
<Huawei> display mpls te link-administration admission-control stale-interface 18000106
LspID                  In/Out IF            S/H Prio  CT        BW (kbps)
10.1.1.1:600:1        --- / 0x18000106        0 /0      0          0
```

Table 11-82 Description of the display mpls te link-administration admission-control command output

Item	Description
LspID	LSP ID, uniquely identified in the form of <Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID>.
In/Out IF	Incoming and outgoing interfaces.
S/H Prio	Setup and holding priorities.
CT	Class type.
BW	Bandwidth.

11.2.32 display mpls te link-administration bandwidth-allocation

Function

The **display mpls te link-administration bandwidth-allocation** command displays information about bandwidth allocation of a specified MPLS TE interface or all MPLS TE interfaces.

Format

display mpls te link-administration bandwidth-allocation [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about bandwidth allocation of a specified interface. ● *interface-type*: indicates the interface type. ● *interface-number*: indicates the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display information about the bandwidth allocation of all MPLS TE interfaces.

```
<Huawei> display mpls te link-administration bandwidth-allocation
  Link ID:  GigabitEthernet0/0/1
  Bandwidth Constraint Model   :  Russian Dolls Model (RDM)
  Physical Link Bandwidth(Kbits/sec)          :  1000000
  Maximum Link Reservable Bandwidth(Kbits/sec):  1000000
  Reservable Bandwidth BC0(Kbits/sec)         :  500000
  Reservable Bandwidth BC1(Kbits/sec)         :  4000
  Downstream Bandwidth (Kbits/sec)            :  0
  IPUpdown Link Status                        :  UP
  PhysicalUpdown Link Status                  :  UP
  GracefulUpdown Link Status                  :  DOWN
  ----------------------------------------------------------------------
  TE-CLASS  CT    PRIORITY   BW RESERVED   BW AVAILABLE   DOWNSTREAM
                            (Kbit/sec)     (Kbit/sec) RSVPLSPNODE COUNT
  ----------------------------------------------------------------------
    0      0        0          0            500000          0
    1      0        1          0            500000          0
    2      0        2          0            500000          0
    3      0        3          0            500000          0
    4      0        4          0            500000          0
    5      0        5          0            500000          0
    6      0        6          0            500000          0
    7      0        7          0            500000          0
    8      1        0          0            4000            0
    9      1        1          0            4000            0
    10     1        2          0            4000            0
    11     1        3          0            4000            0
    12     1        4          0            4000            0
```

```
  13    1     5     0     4000     0
  14    1     6     0     4000     0
  15    1     7     0     4000     0
-----------------------------------------------------------------------
```

Table 11-83 Description of the display mpls te link-administration bandwidth-allocation command output

Item	Description
Link ID	MPLS TE interface number.
Bandwidth Constraint Model	Bandwidth Constraints Model used by a TE tunnel: ● RDM: Russian Dolls Model ● MAM: Maximum Allocation Model ● Extended MAM: Extended Maximum Allocation Model To set the Bandwidth Constraints Model, run the **mpls te ds-te bcm** command.
Physical Link Bandwidth(Kbits/sec)	Indicates the capacity of bandwidth for a physical link.
Maximum Link Reservable Bandwidth(Kbits/sec)	Maximum capacity of reserved bandwidth for a link. To set the maximum capacity of reserved bandwidth for a link, run the **mpls te bandwidth max-reservable-bandwidth** command.
Reservable Bandwidth BCi(0≤i≤7)(Kbits/sec)	Bandwidth that is reserved for BCi. To set the bandwidth that is reserved for BCi, run the **mpls te bandwidth** command.
Downstream Bandwidth (Kbits/sec)	Bandwidth of an outgoing interface.
IPUpdown Link Status	IP link status of an interface: ● UP: IP link is available. ● DOWN: IP link is unavailable.
PhysicalUpdown Link Status	Physical link status of an interface: ● UP: The physical link is available. ● DOWN: The physical link is unavailable.
GracefulUpdown Link Status	Graceful link status of an interface: ● UP: The graceful link is available. ● DOWN: The graceful link is unavailable.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TE-CLASS	TE class. To set the TE class, run the **te-class** command.
CT	Class type.
PRIORITY	Preemption priority of an MPLS TE tunnel. To set the preemption priority of an MPLS TE tunnel, run the **mpls te priority** command.
BW RESERVED (Kbit/sec)	Reserved bandwidth for LSPs of the CT.
BW AVAILABLE (Kbit/sec)	Available bandwidth for LSPs of the CT.
DOWNSTREAM RSVPLSPNODE COUNT	Number of downstream RSVP LSP nodes.

11.2.33 display mpls te link-administration srlg-information

Function

The **display mpls te link-administration srlg-information** command displays SRLG(s) to which the interface belongs.

Format

display mpls te link-administration srlg-information [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After configuring the SRLG in the interface view, you can run the **display mpls te link-administration srlg-information** command to check the configuration.

Example

Display the SLRG(s) to which GE1/0/0 belongs to.

```
<Huawei> display mpls te link-administration srlg-information interface gigabitethernet1/0/0

 SRLGs on GigabitEthernet1/0/0 :
          2            3            9
```

Table 11-84 Description of the display mpls te link-administration srlg-information command output

Item	Description
SRLGs on GigabitEthernet1/0/0	SRLG number to which an interface belongs.

Related Topics

11.2.127 mpls te srlg

11.2.34 display mpls te session-entry

Function

The **display mpls te session-entry** command displays detailed information about LSP sessions of tunnels.

Format

display mpls te session-entry [*ingress-lsr-id tunnel-id egress-lsr-id*]

Parameters

Parameter	Description	Value
ingress-lsr-id	Specifies the LSR ID of the ingress.	In dotted decimal notation.
tunnel-id	Specifies the ID of a tunnel.	The value is an integer that ranges from 0 to 65535.
egress-lsr-id	Specifies the LSR ID of the egress.	The value is in dotted decimal notation.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display detailed information about LSP sessions of a tunnel in IETF mode.

```
<Huawei> display mpls te session-entry

  Ingress-ID                 :  3.3.3.9
  Tunnel-ID                  :  300
  Egress-ID                  :  1.1.1.9
  Crlsp num                  :  1
  First TunnelTable index    :  4
  LSP No.      :  1
  LSP ID       :  3.3.3.9:300:6
  In/Out IF    :  GE2/0/0/-
  Bandwidth(Kbit/sec):
    CT0 : 5000        CT1 : 5000        CT2 : 0           CT3 : 0
    CT4 : 0           CT5 : 0           CT6 : 0           CT7 : 0
```

Display detailed information about LSP sessions of a tunnel in non-IETF mode.

```
<Huawei> display mpls te session-entry

  Ingress-ID                 :  1.1.1.9
  Tunnel-ID                  :  300
  Egress-ID                  :  3.3.3.9
  Crlsp num                  :  1
  First TunnelTable index    :  4
  LSP No.      :  1
  LSP ID       :  1.1.1.9:300:6
  In/Out IF    :  -/GE2/0/0
  Bandwidth(Kbit/sec):
    CT0 : 500         CT1 : 0
```

Table 11-85 Description of the display mpls te session-entry command output

Item	Description
Ingress-ID	LSR ID of the ingress.
Tunnel-ID	Tunnel ID, which is the session ID.
Egress-ID	LSR ID of the egress.
Crlsp num	Number of CR-LSPs of the session entry.
First TunnelTable index	Index of the first CR-LSP of the session entry.
LSP No	Sequence number of a CR-LSP.
LSP ID	LSP ID, uniquely identified in the form of <Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID>.

Item	Description
In/Out IF	Incoming and outgoing interface through which the CR-LSP passes on the local node.
Bandwidth(Kbit/sec)	Bandwidth, in kbit/s.
CT0	Bandwidth value of CR-LSPs of CT0.
CT1	Bandwidth value of CR-LSPs of CT1.
CT2	Bandwidth value of CR-LSPs of CT2.
CT3	Bandwidth value of CR-LSPs of CT3.
CT4	Bandwidth value of CR-LSPs of CT4.
CT5	Bandwidth value of CR-LSPs of CT5.
CT6	Bandwidth value of CR-LSPs of CT6.
CT7	Bandwidth value of CR-LSPs of CT7.

11.2.35 display mpls te srlg

Function

The **display mpls te srlg** command displays the Shared Risk Link Group (SRLG) configurations and the interfaces that belong to it.

Format

display mpls te srlg { *srlg-number* | **all** }

Parameters

Parameter	Description	Value
srlg-number	Specifies the number of the SRLG to which an interface belongs.	The value is an integer that ranges from 0 to 4294967295.
all	Displays information about all SRLGs on the node and the interfaces that belong to the SRLG groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the configuring the SRLG on an interface, you can run the **display mpls te srlg** command to check the configuration.

The **display mpls te srlg** command displays the following information:

- Maximum of SRLGs that a node can support
- Number of SRLGs that are configured on the node
- Member interfaces of each SRLG

Example

Display information about all SRLGs on the node.

```
<Huawei> display mpls te srlg all
Total SRLG supported : 32
Total SRLG configured : 1
SRLG  239:          GE1/0/0
```

Table 11-86 Description of the display mpls te srlg all command output

Item	Description
Total SRLG supported	Total SRLGs supported.
Total SRLG configured	Total SRLGs configured.
SRLG	Shared risk link group.

Related Topics

11.2.127 mpls te srlg

11.2.36 display mpls te te-class-tunnel

Function

The **display mpls te te-class-tunnel** command displays TE tunnels associated with the TE-class.

Format

display mpls te te-class-tunnel { **all** | { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* }

Parameters

Parameter	Description	Value
all	Displays TE tunnels associated with all TE-classes.	-
ct0 - **ct7**	Specifies the CT in the TE-class.	-

Parameter	Description	Value
priority *priority*	Specifies the tunnel priority of a TE-class.	The value is an integer that ranges from 0 to 7.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DS-TE in IETF mode is configured, you can run this command to view TE tunnels associated with all TE-classes.

Example

Display TE tunnels associated with all TE-classes.

```
<Huawei> display mpls te te-class-tunnel all
-----------------------------------------------------------------------------
No.        CT  priority  status        tunnel name        tunnel commit
-----------------------------------------------------------------------------
1          0   7         Not Valid     Tunnel0/0/1        Yes
2          0   7         Not Valid     Tunnel0/0/2        No
```

Table 11-87 Description of the display mpls te te-class-tunnel command output

Item	Description
No.	Entry number.
CT	Service type.
priority	Holding priority of an MPLS TE tunnel. To set the holding priority of an MPLS TE tunnel, run the **mpls te priority** command.
status	Whether or not the TE-class is valid: • Valid: indicates that TE-class is valid. • Not Valid: indicates that TE-class is invalid.
tunnel name	Name of a TE tunnel corresponding to the CT.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
tunnel commit	Whether or not the tunnel interface configurations are committed: • Yes: indicates that the tunnel interface configurations are committed. • No: indicates that the tunnel interface configurations are not committed.

Related Topics

11.2.149 te-class-mapping

11.2.37 display mpls te tunnel-interface

Function

The **display mpls te tunnel-interface** command displays information about tunnel interfaces on the local LSR.

Format

display mpls te tunnel-interface [**tunnel** *interface-number* | **auto-bypass-tunnel** [*tunnel-name*]]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the number of a tunnel interface on the local LSR.	-
auto-bypass-tunnel *tunnel-name*	Specifies the name of an MPLS TE tunnel. If the *tunnel-name* parameter is configured, information about the specified Auto bypass tunnel is displayed. If this parameter is not configured, information about all Auto bypass tunnels is displayed.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If you do not specify any parameters, information about all tunnel interfaces is displayed.

Example

Display information about Tunnel 0/0/1.

```
<Huawei> display mpls te tunnel-interface tunnel 0/0/1
  -------------------------------------------------------------------
                         Tunnel0/0/1
  -------------------------------------------------------------------
  Tunnel State Desc   :  GRACEFUL SWITCH
  Active LSP          :  Best-Effort LSP
  Traffic Switch      :  Best-Effort LSP -> Ordinary LSP
  Session ID          :  50
  Ingress LSR ID      :  1.1.1.1          Egress LSR ID:  2.2.2.2
  Admin State         :  UP               Oper State   :  UP
  Primary LSP State      : DOWN
    Main LSP State       : SETTING UP
  Hot-Standby LSP State  : UP
    Main LSP State       : READY             LSP ID  : 32799
    Modify LSP State     : SETTING UP
  Ordinary LSP State     : UP
    Main LSP State       : READY             LSP ID  : 32782
  Best-Effort LSP State  : UP
    Main LSP State       : READY             LSP ID  : 32780
```

Table 11-88 Description of the display mpls te tunnel-interface command output

Item	Description
Tunnel State Desc	Tunnel status: ● UP: indicates that the tunnel is successfully set up. ● DOWN: indicates that the tunnel fails to be set up. ● GRACEFUL SWITCH: indicates that the tunnels are switched through GR. ● GRACEFUL DELETE: indicates that during the GR process a type of LSP is deleted.
Active LSP	Type of CR-LSP in use: ● Primary LSP: indicates the primary CR-LSP. ● Hot-Standby LSP: indicates the hot-standby CR-LSP. ● Ordinary LSP: indicates the ordinary backup CR-LSP. ● Best-Effort LSP: indicates the best-effort path.
Traffic Switch	Traffic switching status.
Session ID	Session ID of a CR-LSP.
Ingress LSR ID	LSR ID of the ingress.
Egress LSR ID	LSR ID of the egress.
Admin State	Administrative status.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Oper State	Operating status.
Primary LSP State	Status of a primary CR-LSP: ● UP: indicates that the primary CR-LSP is successfully set up. ● DOWN: indicates that no primary CR-LSP is set up. ● GRACEFUL SWITCH: indicates that the primary CR-LSP is being switched to the Modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the primary CR-LSP is deleted.
Main LSP State	Status of the primary CR-LSP: ● READY: indicates that the primary CR-LSP is successfully set up. ● SETTING UP: indicates that the primary CR-LSP is being set up.
Hot-Standby LSP State	Status of a hot-standby CR-LSP: ● UP: indicates that a hot-standby CR-LSP is successfully set up. ● DOWN: indicates that no hot-standby CR-LSP is set up. ● GRACEFUL SWITCH: indicates that the primary CR-LSP is being switched to the Modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the primary CR-LSP is deleted.
Modify LSP State	Status of a modified CR-LSP: ● READY: indicates that the Modified CR-LSP is successfully set up. ● SETTING UP: indicates that the Modified CR-LSP is being set up.
Ordinary LSP State	Status of an ordinary backup CR-LSP: ● UP: indicates that the ordinary backup CR-LSP is successfully set up. ● DOWN: indicates that no ordinary backup CR-LSP is set up. ● GRACEFUL SWITCH: indicates that the main CR-LSP is being switched to the modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the main CR-LSP is deleted.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Best-Effort LSP State	Status of a best-effort path: ● UP: indicates that the best-effort path is successfully set up. ● DOWN: indicates that no best-effort path is set up. ● GRACEFUL SWITCH: indicates that the main CR-LSP is being switched to the Modified CR-LSP. ● GRACEFUL DELETE: indicates that during the GR process, the main CR-LSP is deleted.
LSP ID	LSP ID.

11.2.38 display mpls te tunnel-interface failed

Function

The **display mpls te tunnel-interface failed** command displays the MPLS TE tunnels that fail to be set up or that are being set up.

Format

display mpls te tunnel-interface failed

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring multiple MPLS TE tunnels, you can use the **display mpls te tunnel-interface failed** command to check whether or not there are any tunnels that fail to be set up or are still being set up.

Example

Display the MPLS TE tunnels that fail to be set up or that are being set up.

```
<Huawei> display mpls te tunnel-interface failed
  Tunnel name       SessionId       State Desc
  ------------------------------------------------------------
  Tunnel0/0/1          39              DOWN
```

Table 11-89 Description of the display mpls te tunnel-interface failed command output

Item	Description
Tunnel name	Name of a tunnel interface.
SessionId	Session ID, which is the tunnel ID.
State Desc	Description of the tunnel status: ● UP: The tunnel is in Up state. ● DOWN: The tunnel is in Down state.

11.2.39 display mpls te tunnel-interface last-error

Function

The **display mpls te tunnel-interface last-error** command displays the last errors of a tunnel interface on the local node.

Format

display mpls te tunnel-interface last-error [*tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-name	Displays the last errors of a specified tunnel interface.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mpls te tunnel-interface last-error** command on the ingress to view the error of a local node or the error carried in an RSVP PathErr message sent by a downstream node. The errors can be as follows:

- CSPF computation fails.
- RSVP times out.
- One or more LSPs are deleted during RSVP GR smooth.

 Copyright © Huawei Technologies Co., Ltd.

- One or more LSPs are deleted during RSVP aging.
- RSVP GR fails to be triggered.

Precautions

The **display mpls te tunnel-interface last-error** command shows the last 20 recorded errors of each TE tunnel and LSP on which the errors occur, including errors about the primary CR-LSP, modified LSP, and backup CR-LSP.

If an RSVP PathErr message sent by a downstream node carries the error information, the Error Info field in the command output shows the IP address of the faulty downstream node and the cause of the error. If an error occurs on the ingress, the command output only shows the cause of the error.

Example

Display information about the last errors of Tunnel0/0/1.

```
<Huawei> display mpls te tunnel-interface last-error Tunnel0/0/1
  Tunnel name: Tunnel0/0/1


    Error No.  : 1
    LSP Type   : Hot-Standby LSP            LSP ID     : 1.1.1.9:300:32776
    Error Code : 0x3e8                    Occur Time : 2013/01/07 14:42:23
    Error Info : Link 172.2.1.2 is excluded, IGP: ISIS Process-ID: 1 Area: Level
-1.

    Error No.  : 2
    LSP Type   : Primary LSP               LSP ID     : 1.1.1.9:300:1
    Error Code : 0x5080007                  Occur Time : 2013/01/07 11:13:45
    Error Info : error node = 172.1.1.1    error lsrid = 1.1.1.9
                 BKGD error SHUTDOWN IF

    Error No.  : 3
    LSP Type   : Primary LSP               LSP ID     : 1.1.1.9:300:1
    Error Code : 0x3e8                    Occur Time : 2013/01/07 09:55:06
    Error Info : Cannot find the same IGP type and process ID for 1.1.1.9 and 17
2.1.1.2 (inter area scenario).

    Error No.  : 4
    LSP Type   : Primary LSP               LSP ID     : 1.1.1.9:300:1
    Error Code : 0x3e8                    Occur Time : 2013/01/07 09:43:06
    Error Info : Cspf failed to calculate a path for Tunnel.

    Error No.  : 5
    LSP Type   : Primary LSP               LSP ID     : 1.1.1.9:300:1
    Error Code : 0x3e8                    Occur Time : 2013/01/07 08:43:06
    Error Info:  error node = 172.1.1.1    error lsrid = 1.1.1.9
    Routing Problem: No route available toward destination.

    Error No.  : 6
    LSP Type   : Primary LSP               LSP ID     : 1.1.1.9:300:1
    Error Code : 0x180001                  Occur Time : 2013/01/07 07:47:19
    Error Info : error node = 172.1.1.2    error lsrid = 0.0.0.0
                 Routing Problem Bad EXPLICIT_ROUTE object

    Error No.  : 7
    LSP Type   : Primary LSP               LSP ID     : 1.1.1.9:300:1
    Error Code : 0x5080002                  Occur Time : 2013/01/6 20:03:05
    Error Info : error node = 0.0.0.0    error lsrid = 1.1.1.9
                 BKGD error TEAR ALL LSP
```

Table 11-90 Description of the display mpls te tunnel-interface last-error command output

Item	Description
Tunnel name	Name of an MPLS TE tunnel.
Error No	Number of errors.
LSP Type	Type of LSP: ● Modified LSP: indicates the LSP which is in modified state. ● Primary LSP: indicates the primary LSP. ● Backup LSP: indicates the backup LSP. ● Hot-Standby LSP: indicates the hot-standby LSP.
LSP ID	LSP ID, uniquely identified in the form of Ingress-LSR-ID:Tunnel-ID:Local-LSP-ID.
Error Code	Returned code, which specifies a unique type of error. The value is an integer in hexadecimal notation.
Occur Time	Time when an error occurred.
Error Info	Error description.
error node	Node on which an error occurs.
error lsrid	LSR ID of the node on which an error occurred.
Routing Problem	Error information carried in a received RSVP PathErr message: ● No route available toward destination: indicates that no route to the destination address of the tunnel is available. ● Bad EXPLICIT_ROUTE object: indicates that an unknown EXPLICIT_ROUTE object is received. ● bad strict node: indicates that a certain node cannot be found on the strict explicit path.
Cspf failed to calculate a path for Tunnel	CSPF computation failure.

 Copyright © Huawei Technologies Co., Ltd.

11.2.40 display mpls te tunnel-interface traffic-state

Function

The **display mpls te tunnel-interface traffic-state** command displays information about the traffic on the tunnel interface of the local LSR.

Format

display mpls te tunnel-interface traffic-state [*tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-name	Specifies a tunnel name.	The value is an existing tunnel name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the traffic protection mode, traffic state, and traffic switchover reasons of a tunnel interface on a local LSR, run the **display mpls te tunnel-interface traffic-state** command.

Example

Display information about the traffic on the tunnel interface of the local LSR.

```
<Huawei> display mpls te tunnel-interface traffic-state
 Protect Config: HSB - Hot-Standby,       OBK - Ordinary Backup
                 FRR - Fast Reroute,      BBK - Best-Effort Backup
                 PS  - Protection Switch

 ------------------------------------------------------------------------------
 Tunnel Interface    Protect Config   Traffic State          Switch Reason
 ------------------------------------------------------------------------------
 Tunnel0/0/1            OBK              Primary LSP            --
 Tunnel0/0/2            HSB              Primary LSP            Signal Fail
```

Table 11-91 Description of the display mpls te tunnel-interface traffic-state command output

Item	Description
Tunnel Interface	Tunnel interface name.

Item	Description
Protect Config	Protection modes. The protection modes are displayed using short names. If two protection modes are performed, both the two protection modes are displayed. ● HSB: indicates the hot standby. ● OBK: indicates ordinary backup. ● BBK: indicates the best-effort path. ● FRR: indicates FRR. ● PS: indicates the tunnel protection group.
Traffic State	Traffic protection state, including the following types: ● Hot-Standby LSP: Traffic is switched to the hot-standby LSP. ● Primary LSP FRR In Use: Traffic is on the primary LSP that is in the FRR in use state. ● Best-Effort LSP: Traffic is on the best-effort LSP. ● Ordinary LSP: Traffic is on the ordinary backup LSP. ● Protection Tunnel: Traffic is on the protection tunnel. ● Primary LSP: Traffic is on the primary LSP, and no switchover is performed.
Switch Reason	Reason why traffic is not on the primary LSP. If the traffic is on the primary LSP, or the traffic is on the primary LSP which is in the FRR in use state, this field is not displayed. If multiple reasons exist, only one reason with the highest priority is displayed. Following are the reasons listed in descending order of priorities: ● Manual Command: The user uses a command to enable a switchover. ● Signal Fail: The signaling protocol or detection protocol is Down. ● Signal Degrade: The detection protocol signal degrades. This field is also displayed when bit errors occur. ● Wait To Restore (WTR): The system waits for WTR period and then switch traffic back to the primary LSP. ● Do Not Revertive: Traffic is not switched back to the primary LSP even if the primary LSP recovers.

 Copyright © Huawei Technologies Co., Ltd.

11.2.41 display mpls te tunnel

Function

The **display mpls te tunnel** command displays information about an MPLS TE tunnel.

Format

display mpls te tunnel [**destination** *ip-address*] [**lsp-id** *ingress-lsr-id session-id local-lsp-id*] [**lsr-role** { **all** | **egress** | **ingress** | **remote** | **transit** }] [**name** *tunnel-name*] [{ **incoming-interface** | **interface** | **outgoing-interface** } *interface-type interface-number*] [**te-class0** | **te-class1** | **te-class2** | **te-class3** | **te-class4** | **te-class5** | **te-class6** | **te-class7**] [**verbose**]

display mpls te tunnel { **stale-incoming-interface** | **stale-interface** | **stale-outgoing-interface** } *interface-index* [**verbose**]

Parameters

Parameter	Description	Value
destination *ip-address*	Displays information about an MPLS TE tunnel with a specified destination address.	-
lsp-id	Displays information about an MPLS TE tunnel with a specified LSP ID.	-
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer that ranges from 0 to 65535.
local-lsp-id	Specifies the local LSP ID.	The value is an integer that ranges from 0 to 65535.
lsr-role	Displays information about an MPLS TE tunnel according to the specified role of the local LSR.	-
all	Displays information of all MPLS TE tunnels.	-
egress	Displays information about an MPLS TE tunnel with the local LSR as the egress.	-
ingress	Displays information about an MPLS TE tunnel with the local LSR as the ingress.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remote	Displays information about an MPLS TE tunnel with the local LSR as the egress or the transit node.	-
transit	Displays information about an MPLS TE tunnel with the local LSR as a transit node.	-
name *tunnel-name*	Displays the MPLS TE tunnel whose name is specified.	*tunnel-name* must be the name of an existing tunnel and its format, including the upper and lower casing, and blank spaces, must be consistent with that of the configuration file. For example, when the tunnel interface in a configuration file is named "interface Tunnel0/0/1", the tunnel name to be specified must also be Tunnel0/0/1. "tunnel0/0/1" or "Tunnel 0/0/1" is incorrect.
incoming-interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with a specified incoming interface.	-
interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with an outgoing or incoming interface of the specified type and number.	-
outgoing-interface *interface-type interface-number*	Displays information about all MPLS TE tunnels with a specified outgoing interface.	-
te-class0 - **te-class7**	Displays information about MPLS TE tunnels with a specified TE-class.	-
verbose	Displays detailed information.	-
stale-incoming-interface	Displays information about MPLS TE tunnels with a specified incoming interface in the stale state.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
stale-interface	Displays information about MPLS TE tunnels on an interface in the stale state.	-
stale-outgoing-interface	Displays information about MPLS TE tunnels with a specified outgoing interface in the stale state.	-
interface-index	Specifies the index of a specified stale interface.	The value is a hexadecimal integer that ranges from 0x1 to 0xfffffffe.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When **verbose** is configured, the command output varies with the signaling protocol used by the MPLS TE tunnel.

Example

Display information about an MPLS TE tunnel.

```
<Huawei> display mpls te tunnel
-------------------------------------------------------------------------------
Ingress LsrId    Destination      LSPID   In/Out Label     R  Tunnel-name
-------------------------------------------------------------------------------
1.1.1.9          3.3.3.9          6       --/1027          I  Tunnel0/0/1
```

Table 11-92 Description of the display mpls te tunnel command output

Item	Description
Ingress LsrId	Ingress LSR ID.
Destination	Destination IP address.
LSPID	LSP ID of the ingress.
In/Out Label	Incoming and outgoing labels.
R	The LSR role, including: ● I: Ingress ● T: Transit ● E: Egress

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tunnel-name	Tunnel name.

Display detailed information about an MPLS TE tunnel.

```
<Huawei> display mpls te tunnel verbose
  No                    :  1
  Tunnel-Name           :  Tunnel0/0/1
  Tunnel Interface Name   :  Tunnel0/0/1
  TunnelIndex           :  0          LSP Index        :  2049
  Session ID            :  100        LSP ID           :  6
  LSR Role              :  Ingress    LSP Type         :  Primary
  Ingress LSR ID        :  1.1.1.9
  Egress LSR ID         :  3.3.3.9
  In-Interface          :  -
  Out-Interface         :  GE0/0/2
  Sign-Protocol         :  RSVP TE    Resv Style       :  SE
  IncludeAnyAff         :  0x0        ExcludeAnyAff    :  0x0
  IncludeAllAff         :  0x0
  LspConstraint         :  -
  ER-Hop Table Index    :  -          AR-Hop Table Index:  0
  C-Hop Table Index     :  0
  PrevTunnelIndexInSession:  -          NextTunnelIndexInSession:  -
  PSB Handle            :  8195
  Created Time          :  2012/02/16 20:38:05
  RSVP LSP Type         :  -
  --------------------------------
          DS-TE Information
  --------------------------------
  Bandwidth Reserved Flag :  Unreserved
  CT0 Bandwidth(Kbit/sec) :  0          CT1 Bandwidth(Kbit/sec):  0
  CT2 Bandwidth(Kbit/sec) :  0          CT3 Bandwidth(Kbit/sec):  0
  CT4 Bandwidth(Kbit/sec) :  0          CT5 Bandwidth(Kbit/sec):  0
  CT6 Bandwidth(Kbit/sec) :  0          CT7 Bandwidth(Kbit/sec):  0
  Setup-Priority        :  7          Hold-Priority    :  7
  --------------------------------
           FRR Information
  --------------------------------
  Primary LSP Info
  TE Attribute Flag     :  0x63       Protected Flag   :  0x0
  Bypass In Use         :  Not Exists
  Bypass Tunnel Id      :  -
  BypassTunnel          :  -
  Bypass LSP ID         :  -          FrrNextHop       :  -
  ReferAutoBypassHandle   :  -
  FrrPrevTunnelTableIndex :  -          FrrNextTunnelTableIndex:  -
  Bypass Attribute(Not configured)
  Setup Priority        :  -          Hold Priority    :  -
  HopLimit              :  -          Bandwidth        :  -
  IncludeAnyGroup       :  -          ExcludeAnyGroup  :  -
  IncludeAllGroup       :  -
  Bypass Unbound Bandwidth Info(Kbit/sec)
  CT0 Unbound Bandwidth   :  -        CT1 Unbound Bandwidth:  -
  CT2 Unbound Bandwidth   :  -        CT3 Unbound Bandwidth:  -
  CT4 Unbound Bandwidth   :  -        CT5 Unbound Bandwidth:  -
  CT6 Unbound Bandwidth   :  -        CT7 Unbound Bandwidth:  -
  --------------------------------
           BFD Information
  --------------------------------
  NextSessionTunnelIndex  :  -          PrevSessionTunnelIndex:  -
  NextLspId             :  -          PrevLspId        :  -
```

Table 11-93 Description of the display mpls te tunnel verbose command output

Item	Description
No	Number of an MPLS TE tunnel.
Tunnel-Name	Name of an MPLS TE tunnel.
Tunnel Interface Name	Interface name of an MPLS TE tunnel.
TunnelIndex	Index of an MPLS TE tunnel.
LSP Index	Index of an LSP.
Session ID	Session ID, which is the tunnel ID.
LSP ID	LSP ID.
LSR Role	Role of the LSR: ● Ingress: indicates the node is the ingress of the tunnel. ● Egress: indicates the node is the egress of the tunnel. ● Transit: indicates the node is the transit of the tunnel.
LSP Type	Type of an LSP: ● Primary: indicates the primary CR-LSP. ● Hot-Standby: indicates the hot-standby CR-LSP. ● Ordinary: indicates the ordinary backup CR-LSP. ● Best-Effort: indicates the best-effort path.
Ingress LSR ID	LSR ID of the ingress.
Egress LSR ID	LSR ID of the egress.
In-Interface	Incoming interface of the LSP on the local node.
Out-Interface	Outgoing interface of the LSP on the local node.
Sign-Protocol	Tunnel protocol: ● Static: indicates Static LSP. ● Static CR: indicates Static CR-LSP. ● RSVP TE: uses RSVP TE signaling.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Resv Style	Style of resource reservation. For a static CR-LSP, no resource reservation style is displayed. For an RSVP-TE tunnel, shared explicit (SE) or fixed filter (FF) is displayed.
IncludeAnyAff	Valid affinity property. The default value is 0x0.
ExcludeAnyAff	Invalid affinity property. The default value is 0x0.
IncludeAllAff	The affinity property need to be included. The default value is 0x0.
LspConstraint	Sequence number of the constraint used by an LSP.
ER-Hop Table Index	Index of an explicit routing table.
AR-Hop Table Index	Index of the actual explicit routing table.
C-Hop Table Index	Routing table index that is calculated by CSPF.
PrevTunnelIndexInSession	Index of the previous tunnel entry in the same session.
NextTunnelIndexInSession	Index of the next tunnel entry in the same session.
PSB Handle	Handle of the PSB.
Created Time	Amount of time an MPLS TE tunnel is created for.
RSVP LSP Type	LSP type. ● Primary: indicates that the LSP is a primary LSP. ● Hot-Standby: indicates that the LSP is a hot-standby LSP. **NOTE** This field is displayed as "-" because the device does not support the error code switching function.
Bandwidth Reserved Flag	Bandwidth reservation flag: ● Unreserved: indicates that no bandwidth is reserved for CTs. ● Reserved: indicates that the bandwidth is reserved for one or multiple CTs.
CT0 Bandwidth(Kbit/sec) - CT7 Bandwidth(Kbit/sec)	Value of the bandwidth that is reserved for CT0 to CT7.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Setup-Priority	Setup priority of an MPLS TE tunnel.
Hold-Priority	Holding priority of an MPLS TE tunnel.
Primary LSP Info	Information about the primary LSP.
TE Attribute Flag	Flag of the TE tunnel attribute.
Protected Flag	Flag of the primary tunnel of the protection group.
Bypass In Use	LSP ID of the bypass tunnel. "Not Exists" indicates that the primary tunnel is not bound to a bypass tunnel.
Bypass Tunnel Id	Tunnel ID of the bypass tunnel.
BypassTunnel	Name of the bypass tunnel.
Bypass LSP ID	LSP ID of the bypass tunnel.
FrrNextHop	Next hop of the redirect route.
ReferAutoBypassHandle	Handle of the automatic bypass tunnel.
FrrPrevTunnelTableIndex	Index value of the previous tunnel entry in FRR.
FrrNextTunnelTableIndex	Index value of the next tunnel entry in FRR.
Bypass Attribute	Attributes of a bypass tunnel. "(Not configured)" indicates that no such attribute is configured and the bypass tunnel inherits the attributes of the primary tunnel.
Setup Priority	Setup priority of a bypass tunnel.
Hold Priority	Holding priority of a bypass tunnel.
HopLimit	Maximum number of hops along a bypass tunnel.
Bandwidth	Bandwidth of a bypass tunnel.
IncludeAnyGroup	Valid affinity property of a bypass tunnel.
ExcludeAnyGroup	Invalid affinity property of a bypass tunnel.
IncludeAllGroup	The affinity property of a bypass tunnel need to be included.
Bypass Unbound Bandwidth Info	Information about the bandwidth that is not bound to a bypass tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CT0 Unbound Bandwidth - CT7 Unbound Bandwidth	Bandwidth that is able to be reserved, but not for CT0 to CT7.
NextSessionTunnelIndex	Next index of a bypass tunnel entry.
PrevSessionTunnelIndex	Previous index of a bypass tunnel entry.
NextLspId	Value of the next bypass LSP ID.
PrevLspId	Value of the previous bypass LSP ID.

11.2.42 display mpls te tunnel c-hop

Function

The **display mpls te tunnel c-hop** command displays the path computation results of tunnels.

Format

display mpls te tunnel c-hop [*tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*]

Parameters

Parameter	Description	Value
tunnel-name	Displays the path computation result of the specified tunnel.	The value is an existing tunnel name.
lsp-id	Displays the path computation result of the specified tunnel based on the LSP ID.	-
ingress-lsr-id	Specifies the ingress LSR ID.	The value is in dotted decimal notation.
session-id	Specifies the session ID.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Tunnels are established based on path computation results. When a tunnel cannot be established successfully, run the **display mpls te tunnel c-hop** command to view the path computation results for locating causes on a per-hop basis.

Example

Display the path computation result of a tunnel.

```
<Huawei> display mpls te tunnel c-hop
 Tunnel Interface Name : Tunnel0/0/1
 Lsp ID : 2.2.2.2 :1 :10958
 CHop Information:
  Hop 0   2.3.0.2
  Hop 1   2.3.0.3
```

Display the path computation result of the specified tunnel based on the LSP ID.

```
<Huawei> display mpls te tunnel c-hop lsp-id 2.2.2.2 1 10958
 Tunnel Interface Name : Tunnel0/0/1
 Lsp ID : 2.2.2.2 :1 :10958
 CHop Information:
  Hop 0   2.3.0.2
  Hop 1   2.3.0.3
```

Table 11-94 Description of the display mpls te tunnel c-hop command output

Item	Description
Tunnel Interface Name	Interface name of a tunnel.
Lsp ID	LSP ID of a tunnel, in the Ingress-Lsr-Id:Tunnel-Id:LSP-Id format.
CHop Information	Information about CSPF path computation. **Hop** specifies the IPv4 address of each hop in the path computation result.

Related Topics

11.2.100 mpls te cspf

11.2.43 display mpls te tunnel path

Function

The **display mpls te tunnel path** command displays the path of an MPLS TE tunnel.

Format

display mpls te tunnel path [[[**tunnel-name**] *tunnel-name*] [**lsp-id** *ingress-lsr-id session-id lsp-id*] | **fast-reroute** { **local-protection-available** | **local-protection-inuse** } | **lsr-role** { **ingress** | **transit** | **egress** }]

display mpls te tunnel path expanded tunnel-name *tunnel-name* [**lsp-id** *ingress-lsr-id session-id lsp-id*]

display mpls te tunnel path expanded lsp-id *ingress-lsr-id session-id lsp-id*

Parameters

Parameter	Description	Value
tunnel-name *tunnel-name*	Specifies the name of an MPLS TE tunnel. If the **mpls te signalled tunnel-name** command has been used to configure a tunnel name, this specified name is used.	The value is an existing tunnel name.
ingress-lsr-id	Specifies the LSR ID of the ingress.	The value is in dotted decimal notation.
session-id	Specifies the ID of a session.	The value is an integer that ranges from 0 to 65535.
lsp-id	Specifies the LSP ID.	The value is an integer that ranges from 0 to 65535.
fast-reroute local-protection-available	Specifies the available path for local protection of FRR.	-
fast-reroute local-protection-inuse	Specifies the path in use for local protection of FRR.	-
lsr-role { **ingress** | **transit** | **egress** }	Indicates the role of an LSR. • **ingress**: indicates the ingress LSR. • **transit**: indicates the transit LSR. • **egress**: indicates the egress LSR.	-
expanded	Displays the expanded LSP path information by completing the RRO information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display mpls te tunnel path** command displays information about the path of an MPLS TE tunnel.

If no tunnel name is specified, information about all MPLS TE tunnels' path attributes is displayed.

When a Huawei device is interconnected with a non-Huawei device and the RRO information carried in the packet sent by the non-Huawei device is incomplete, the RRO information can be complemented using the **display mpls te tunnel path expanded** command on the Huawei device to display the information about the entire LSP path.

Precautions

The system can record and display the paths only after the **mpls te record-route** command is configured.

Example

Display information about path attributes of all MPLS TE tunnels.

```
<Huawei> display mpls te tunnel path
Tunnel Interface Name : Tunnel0/0/1
 Lsp ID : 1.1.1.9 :100 :34
 Hop Information
  Hop 0   10.1.1.1 Local-Protection available | node
  Hop 1   10.1.1.2  Label 1055
  Hop 2   2.2.2.9  Label 1055
  Hop 3   10.2.1.1 Local-Protection available
  Hop 4   10.2.1.2  Label 1063
  Hop 5   3.3.3.9  Label 1063
  Hop 6   10.3.1.1
  Hop 7   10.3.1.2  Label 3
  Hop 8   4.4.4.9  Label 3
```

Display path attributes of the MPLS TE tunnel with the ingress IP address being 1.1.1.9, the session ID being 300, and the LSP ID being 4.

```
<Huawei> display mpls te tunnel path lsp-id 1.1.1.9 300 4
 Tunnel Interface Name : Tunnel0/0/1
 Lsp ID : 1.1.1.9 :300 :4
 Hop Information
  Hop 0   10.1.1.1
  Hop 1   10.1.1.2  Label 1043
  Hop 2   2.2.2.9  Label 1043
  Hop 3   10.2.1.1
  Hop 4   10.2.1.2  Label 4
  Hop 5   3.3.3.9  Label 4
```

Display path attributes of a tunnel named **LSRAtoLSRC**.

```
<Huawei> display mpls te tunnel path tunnel-name LSRAtoLSRC
 Tunnel Interface Name : LSRAtoLSRC
 Lsp ID : 1.1.1.9 :1 :2
 Hop Information
  Hop 0   11.1.1.1  Local-Protection in use
  Hop 1   11.1.1.2  Label 3
  Hop 2   2.2.2.9
```

Display path attributes of a tunnel named **A2** using the command which expanded the information about the path.

```
<Huawei> display mpls te tunnel path expanded tunnel-name A2
 Tunnel Interface Name : A2
 Lsp ID : 1.1.1.9 :300 :4
```

 Copyright © Huawei Technologies Co., Ltd.

```
Hop Information
 Hop 0   1.1.1.9   Local-Protection available | bandwidth
 Hop 1   10.1.1.1
 Hop 2   10.1.1.2  Label 1042
 Hop 3   2.2.2.9  Label 1042
 Hop 4   10.2.1.1
 Hop 5   10.2.1.2  Label 3
 Hop 6   3.3.3.9  Label 3
```

Table 11-95 Description of the display mpls te tunnel path command output

Item	Description
Tunnel Interface Name	Name of a tunnel interface.
Lsp ID	LSP ID on the ingress.
Hop Information	Number and IP address of each hop.
Local-Protection available	Link protection provided by the bypass tunnel.
Local-Protection available | bandwidth	Bandwidth protection provided by the bypass tunnel.
Local-Protection available | node	Node protection provided by the bypass tunnel.
Local-Protection in use	The bypass tunnel in use.

Related Topics

11.2.119 mpls te record-route

11.2.44 display mpls te tunnel statistics

Function

The **display mpls te tunnel statistics** command displays the number and status of MPLS TE tunnels.

Format

display mpls te tunnel statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the number and status of MPLS TE tunnels.

```
<Huawei> display mpls te tunnel statistics
Ingress:    84 Tunnels     83 Up,     83 CRLSPs Up
            0 Modified,    0 In-Progress,    1 Failed
Transit:     2 Up
Egress :     3 Up
```

Table 11-96 Description of the display mpls te tunnel statistics command output

Item	Description
Ingress	Number and status of MPLS TE tunnels on the local LSR functioning as the ingress node: ● Tunnel: indicates the number of primary tunnels. ● Up: indicates the number of MPLS TE tunnels in the Up state. ● CRLSPs Up: indicates the number of CR-LSPs in the Up state. ● Modified: indicates the number of tunnels in the reestablishing state. **NOTE** The possible causes that an MPLS TE tunnel is in the Modified state are as follows: ● Configurations of the MPLS TE tunnel are manually modified. ● The MPLS TE tunnel is being re-optimized. ● The MPLS TE tunnel is in the FRR inuse state. ● The MPLS TE tunnel is in the Backup state. ● In-Progress: indicates the number of MPLS TE tunnels in the establishing process. At the moment, these tunnels do not go Up. ● Failed: indicates the number of MPLS TE tunnels in the Down state.
Transit	Number of MPLS TE tunnels, which are in the Up state, on the local LSR functioning as a transit node.
Egress	Number of MPLS TE tunnels, which are in the Up state, on the local LSR functioning as the egress node.

 Copyright © Huawei Technologies Co., Ltd.

11.2.45 display ospf mpls-te

Function

The **display ospf mpls-te** command displays information about TE LSAs in an LSDB.

Format

display ospf [*process-id*] **mpls-te** [**area** *area-id*] [**self-originated**]

Parameters

Parameter	Description	Value
process-id	Specifies the OSPF process ID.	The value ranges from 1 to 65535.
area *area-id*	Displays information about the area with a specified ID. The value can be a decimal integer or in the IP address format.	The integer value ranges from 0 to 4294967295.
self-originated	Displays information about the self originated TE LSAs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view information about LSAs of a specific process or area by specifying parameters.

Example

Display information about all TE LSAs in the LSDB.

```
<Huawei> display ospf mpls-te

        OSPF Process 1 with Router ID 5.5.5.5

 Area ID                  : 0.0.0.0

 Traffic Engineering LSAs of the database

 ----------------------------------------------

 LSA [ 1 ]

 ----------------------------------------------
```

```
  Lsa  Type                : Opq-Area
  Opaque Type              : 1
  Opaque Id                : 4
  Advertising Router Id    : 2.2.2.2
  Lsa  age                 : 1765
  Length                   : 200
  Lsa  Options             : E
  LS Seq Number            : 80000044
  CheckSum                 : 74B4

  Link Type                : MultiAccess
  Link ID                  : 3.3.3.3
  Local Interface Address  : 3.1.1.1
  Remote Interface Address : 3.1.1.2
  TE Metric                : 1
  Maximum Bandwidth        : 0 bytes/sec
  Maximum Reservable BW    : 0 bytes/sec
  Admin Group              : 0X0

Global Pool                :
  Unreserved BW [ 0] =   0  bytes/sec
  Unreserved BW [ 1] =   0  bytes/sec
  Unreserved BW [ 2] =   0  bytes/sec
  Unreserved BW [ 3] =   0  bytes/sec
  Unreserved BW [ 4] =   0  bytes/sec
  Unreserved BW [ 5] =   0  bytes/sec
  Unreserved BW [ 6] =   0  bytes/sec
  Unreserved BW [ 7] =   0  bytes/sec
  Sub Pool                 :
  Unreserved BW [ 8] =   0  bytes/sec
  Unreserved BW [ 9] =   0  bytes/sec
  Unreserved BW [10] =   0  bytes/sec
  Unreserved BW [11] =   0  bytes/sec
  Unreserved BW [12] =   0  bytes/sec
  Unreserved BW [13] =   0  bytes/sec
  Unreserved BW [14] =   0  bytes/sec
  Unreserved BW [15] =   0  bytes/sec

  DS-TE Mode: Non-Standard IETF Mode

  Bandwidth Constraint Model: RDM

Bandwidth Constraints

            BC [ 0] =   0  bytes/sec            BC [ 1] =   0  bytes/sec

Local OverBooking Multipliers

           LOM [ 0] =   1                 LOM [ 1] =   1


-----------------------------------------------

LSA [ 2 ]

-----------------------------------------------
  Lsa  Type                : Opq-Area
  Opaque Type              : 1
  Opaque Id                : 2
  Advertising Router Id    : 2.2.2.2
  Lsa  age                 : 102
  Length                   : 192
  Lsa  Options             : E
  LS Seq Number            : 80000046
  CheckSum                 : CC4D

  Link Type                : MultiAccess
  Link ID                  : 3.2.1.2
  Local Interface Address  : 3.2.1.1
```

```
  Remote Interface Address : 3.2.1.2
  TE Metric                : 1
  Maximum Bandwidth        : 0 bytes/sec
  Maximum Reservable BW    : 0 bytes/sec
  Admin Group              : 0X0

Global Pool                :
  Unreserved BW [ 0] =   0  bytes/sec
  Unreserved BW [ 1] =   0  bytes/sec
  Unreserved BW [ 2] =   0  bytes/sec
  Unreserved BW [ 3] =   0  bytes/sec
  Unreserved BW [ 4] =   0  bytes/sec
  Unreserved BW [ 5] =   0  bytes/sec
  Unreserved BW [ 6] =   0  bytes/sec
  Unreserved BW [ 7] =   0  bytes/sec

  DS-TE Mode: Standard IETF Mode

  Bandwidth Constraint Model: RDM

Bandwidth Constraints

          BC [ 0] =   0  bytes/sec          BC [ 1] =   0  bytes/sec

          BC [ 2] =   0  bytes/sec          BC [ 3] =   0  bytes/sec

          BC [ 4] =   0  bytes/sec          BC [ 5] =   0  bytes/sec

          BC [ 6] =   0  bytes/sec          BC [ 7] =   0  bytes/sec

Local OverBooking Multipliers

          LOM [ 0] =   1              LOM [ 1] =   1

          LOM [ 2] =   1              LOM [ 3] =   1

          LOM [ 4] =   1              LOM [ 5] =   1

          LOM [ 6] =   1              LOM [ 7] =   1

...
```

Table 11-97 Description of the display ospf mpls-te command output

Item	Description
OSPF Process 1 with Router ID 5.5.5.5	OSPF process 1 with Router ID being 5.5.5.5.
Area ID	ID of the OSPF area enabled with TE.
Traffic Engineering LSAs of the database	TE LSAs in an LSDB.
Lsa Type	LSA type: ● Opq-Link: indicates Type 9 LSAs that can only be spread on a specified interface. ● Opq-Area: indicates Type 10 LSAs that can only be spread within a specified area. ● Opq-As: indicates Type 11 LSAs that can be spread the same as Type 5 LSAs in the entire AS, except for the stub and NSSA areas.

Item	Description
Opaque Type	Application type of LSAs. For example, when LSAs are applied to traffic engineering, the value of the LSA type is 1. When LSAs are applied to the OSPF graceful restart, the value of the LSA type is 3.
Opaque Id	LSAs that are applied to the same application type. Opaque type and Opaque ID in an LSA header together specify the link status ID.
Advertising Router Id	Device that generates the LSA.
Lsa age	Aging time of the LSA. It is in the header of Opaque LSA, in seconds.
Length	Length of the Opaque LSA, including the LSA header, in bytes.
Lsa Options	LSA options: ● E: floods AS-external-LSAs. ● MC: forwards IP multicast packets. ● N/P: processes Type 7 LSAs. ● DC: processes required links.
LS Seq Number	LSA sequence, according to which other devices can identify the latest LSAs.
CheckSum	Checksum of LSA fields except for the LS age field.
Link Type	Link type: ● Point-to-point ● Point-to-multi-point (P2MP) ● Broadcast
Link ID	Link ID in the IP address format: ● Point-to-point: indicates the router ID of an OSPF neighbor. ● P2MP or broadcast: indicates the IP address of the DR interface.
Local Interface Address	IP address of the local interface.
Remote Interface Address	IP address of the peer interface: ● Point-to-point: indicates that the IP address of the peer is used. ● P2MP or broadcast: indicates that 0.0.0.0 is used or the IP address is omitted.
TE Metric	TE metric.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximum Bandwidth	Maximum bandwidth.
Maximum Reservable BW	Maximum capacity of reserved bandwidth.
Admin Group	Administration group.
Global Pool	Global address pool.
Unreserved BW [0] to [7]	Available bandwidth of eight levels.
Sub Pool	Sub-address pool. It is only applied to DS-TE LSAs.
Unreserved BW [8] to [15]	Available bandwidth of eight levels in the sub-address pool.
DS-TE Mode	DS-TE mode: ● Standard IETF mode ● Non-standard IETF mode
Bandwidth Constraint Model	Bandwidth Constraints model of LSAs: ● RDM ● MAM ● Extended-MAM
Bandwidth Constraints	Bandwidth constraints, which are only applied to DS-TE LSAs.
BC [0] - [7]	Eight bandwidth constraints, which are only applied to DS-TE LSAs.
Local OverBooking Multipliers	Local overbooking multiplier.
LOM [0] LOM [1]	Local overbooking multipliers for BC0 or BC1. It is applied only to DS-TE LSAs.

11.2.46 display ospf traffic-adjustment

Function

The **display ospf traffic-adjustment** command displays OSPF process-specific tunnel information relevant to traffic adjustment (through IGP shortcut and forwarding adjacency).

Format

display ospf [*process-id*] **traffic-adjustment**

Parameters

Parameter	Description	Value
process-id	Specifies the OSPF process ID. If you do not specify a process ID, information about all OSPF processes is displayed.	The value is an integer ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you want to look up the OSPF process-specific tunnel information relevant to traffic adjustment, you can run this command.

Example

Display tunnel information, which is relevant to traffic adjustment, of OSPF process 100.

```
<Huawei> display ospf 100 traffic-adjustment

        OSPF Process 100 with Router ID 1.1.1.9
                Traffic adjustment

 Interface: 1.1.1.9 (Tunnel0/0/1)
 Type: Forwarding Adjacency
 Neighbor ID: 3.3.3.9           Cost: 1
 Configuration:
  Neighbor ip address: 3.3.3.9
  Cost     :1
  Cost Type: Absolute
  Hold Time: 0
```

Table 11-98 Description of the display ospf traffic-adjustment command output

Item	Description
Interface	Name and IP address of a tunnel interface
Type	Whether or not a tunnel is applied to IGP shortcut or forwarding adjacency
Neighbor ID	Router ID of a neighbor device
Cost	Cost
Neighbor ip address	IP address of a neighbor device

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Cost Type	Cost type: • Relative • Absolute
Hold Time	Time elapsed since the tunnel has been created

Related Topics

11.2.49 enable traffic-adjustment
11.2.110 mpls te igp shortcut

11.2.47 display snmp-agent trap feature-name mpls_rsvp all

Function

The **display snmp-agent trap feature-name mpls_rsvp all** command displays the status of whether all trap functions of the MPLS RSVP module are enabled.

Format

display snmp-agent trap feature-name mpls_rsvp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

Example

Display all trap messages of the MPLS RSVP module.

```
<Huawei> display snmp-agent trap feature-name mpls_rsvp all
-----------------------------------------------------------------------------
```

```
Feature name: MPLS_RSVP
Trap number : 8
--------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwRsvpTeHelloLost              off                     on
hwRsvpTeHelloLostRecovery      off                     on
hwRsvpTeAuthFail               off                     on
hwRsvpTeAuthSuccess            off                     on
hwRsvpTeIfNbrThresholdExceed   off                     on
hwRsvpTeIfNbrThresholdExceedClear
                               off                     on
hwRsvpTeIfNbrTotalCountExceed  off                     on
hwRsvpTeIfNbrTotalCountExceedClear
                               off                     on
```

Table 11-99 Description of the **display snmp-agent trap feature-name mpls_rsvp all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs
Trap number	Number of trap messages
Trap name	Name of a trap message of the MPLS RSVP module: ● hwRsvpTeHelloLost: The RSVP neighbor relationship was interrupted. ● hwRsvpTeHelloLostRecovery: The device is restored from the status of interruption of RSVP neighbor relationship. ● hwRsvpTeAuthFail: RSVP authentication failed. ● hwRsvpTeAuthSuccess: RSVP authentication succeeded. ● hwRsvpTeIfNbrThresholdExceed: The proportion of configured RSVP neighbors to RSVP neighbors supported by a device reaches the upper alarm threshold. ● hwRsvpTeIfNbrThresholdExceedClear: The proportion of configured RSVP neighbors to RSVP neighbors supported by a device falls below the lower threshold. ● hwRsvpTeIfNbrTotalCountExceed: The number of configured RSVP neighbors on a device reaches the maximum number of RSVP neighbors supported by the device. ● hwRsvpTeIfNbrTotalCountExceedClear: The number of configured RSVP neighbors on a device falls below the maximum limit of RSVP neighbors.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default switch status	Default status of the trap function: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Current status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

11.2.143 snmp-agent trap enable feature-name mpls_rsvp

11.2.48 display snmp-agent trap feature-name tunnel-te all

Function

The **display snmp-agent trap feature-name tunnel-te all** command displays whether all trap functions of the Tunnel-TE module are enabled.

Format

display snmp-agent trap feature-name tunnel-te all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display all trap messages of the Tunnel-TE module.

```
<Huawei> display snmp-agent trap feature-name tunnel-te all
-------------------------------------------------------------------------------
Feature name: TUNNEL-TE
Trap number : 8
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwMplsPsSwitchWtoP              off                     off
hwMplsPsSwitchPtoW              off                     off
hwMplsApsMismatch               off                     off
hwMplsApsMismatchRecovery       off                     off
hwMplsApsLost                   off                     off
hwMplsApsLostRecovery           off                     off
hwMplsApsOutage                 off                     off
hwMplsApsOutageRecovery         off                     off
```

Table 11-100 Description of the **display snmp-agent trap feature-name tunnel-te all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs
Trap number	Number of trap messages
Trap name	Name of a trap message of the Tunnel-TE module: ● hwMplsPsSwitchWtoP: The protection group switched from the work tunnel to the protection tunnel. ● hwMplsPsSwitchPtoW: The protection group switched from the protection tunnel back to the work tunnel. ● hwMplsApsMismatch: APS information on the local end of a bidirectional tunnel was inconsistent with that on the remote end. ● hwMplsApsMismatchRecovery: APS information on the local end of a bidirectional tunnel was inconsistent with that on the remote end has been recovered. ● hwMplsApsLost: No APS frame was transmitted on the protect tunnel in the tunnel protection group. ● hwMplsApsLostRecovery: APS frames were transmitted on the protect tunnel in the tunnel protection group. ● hwMplsApsOutage: A tunnel protection group went faulty. ● hwMplsApsOutageRecovery: The tunnel protection group recovered from a fault.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default switch status	Default status of the trap function: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Current status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

11.2.144 snmp-agent trap enable feature-name tunnel-te

11.2.49 enable traffic-adjustment

Function

The **enable traffic-adjustment** command enables the IGP shortcut function.

The **enable traffic-adjustment advertise** command enables the forwarding adjacency function.

The **undo enable traffic-adjustment** command disables the IGP shortcut function.

The **undo enable traffic-adjustment advertise** command disables the forwarding adjacency function.

By default, the IGP shortcut function and the forwarding adjacency function are disabled.

Format

enable traffic-adjustment [**advertise**]

undo enable traffic-adjustment [**advertise**]

Parameters

None.

Views

OSPF view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After the configuration of a command, all TE tunnels are involved in the SPF calculation and flooding.

Example

Enable the forwarding adjacency function of the OSPF process.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] enable traffic-adjustment advertise
```

11.2.50 explicit-path

Function

The **explicit-path** command configures an explicit path of a tunnel.

The **undo explicit-path** command deletes a configured explicit path.

By default, no explicit path of a tunnel is configured.

Format

explicit-path *path-name*

undo explicit-path *path-name*

Parameters

Parameter	Description	Value
path-name	Indicates the name of an explicit path.	The value is a string of 1 to 31 case-insensitive characters, spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You must enable MPLS TE before running the **explicit-path** command.

The addresses of the hops along the explicit path must be different, without loops. If a loop exists, CSPF detects the loop and fails to compute a path.

If the explicit path is in use, the **undo explicit-path** command cannot be run to delete the explicit path.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an explicit path named path1.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] quit
[Huawei] explicit-path path1
[Huawei-explicit-path-path1] quit
```

Related Topics

11.2.134 next hop
11.2.1 add hop
11.2.3 delete hop
11.2.52 modify hop
11.2.7 display explicit-path
11.2.51 list hop
11.2.114 mpls te path explicit-path

11.2.51 list hop

Function

The **list hop** command displays information about nodes along an explicit path of an MPLS TE tunnel.

Format

list hop [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a node.	The value is in dotted decimal notation.

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

None.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about nodes along an explicit path of an MPLS TE tunnel.

```
<Huawei> system-view
[Huawei] explicit-path path1
[Huawei-explicit-path-path1] list hop
 Path Name : path1     Path Status : Enabled
 1     10.1.1.1        Strict     Include
 2     10.2.2.2        Strict     Exclude
 3     10.3.3.3        Loose      Include          Outgoing
 4     10.4.4.4        Strict     Include          Incoming
```

Related Topics

11.2.50 explicit-path

11.2.1 add hop

11.2.3 delete hop

11.2.134 next hop

11.2.52 modify hop

11.2.52 modify hop

Function

The **modify hop** command modifies the IP address of a hop on an explicit path.

Format

modify hop *ip-address1 ip-address2* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**]

Parameters

Parameter	Description	Value
ip-address1 ip-address2	Changes *ip-address1* to *ip-address2* on an explicit path.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Indicates that the explicit path must pass through the modified node on the explicit path. • **strict**: indicates the strict explicit path. The modified node must be directly connected to the previous node. • **loose**: indicates the loose explicit path. The modified node can be not directly connected to the previous node. • **incoming**: indicates that the *ip-address2* is the IP address of an inbound interface of the modified node. • **outgoing**: indicates that the *ip-address2* is the IP address of an outbound interface of the modified node.	By default, a node is added to an explicit path in **include strict** mode.
exclude	Indicates that the LSP set up along an explicit path excludes the modified link or node.	-

Views

Explicit path view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following commands are used to adjust nodes on a created explicit path:

- The **add hop** command is used to add a node to the explicit path.
- The **modify hop** command is used to delete a node from the explicit path and replace the node with a specified node.
- The **delete hop** command is used to delete a node from the explicit path.

Prerequisites

A next-hop IP address has been configured using the **next hop** command.

Precautions

A node can be modified on an explicit path using the **modify hop** command only when the following conditions are met:

- *ip-address2* must not be a next-hop IP address of an existing node on the explicit path.

 Copyright © Huawei Technologies Co., Ltd.

- If an explicit path over which a TE tunnel has been established is modified, the make-before-break mechanism is triggered, and a CR-LSP is reestablished without traffic loss.

Example

Modify IP address of a node along the explicit path from 1.1.1.9 to 2.2.2.9.

```
<Huawei> system-view
[Huawei] explicit-path p1
[Huawei-explicit-path-p1] next hop 1.1.1.9
[Huawei-explicit-path-p1] modify hop 1.1.1.9 2.2.2.9
```

Related Topics

11.2.1 add hop

11.2.3 delete hop

11.2.51 list hop

11.2.114 mpls te path explicit-path

11.2.134 next hop

11.2.53 mpls-te enable

Function

The **mpls-te enable** command enables the MPLS TE feature in the current OSPF area.

The **undo mpls-te** command disables the MPLS TE feature in the current OSPF area.

OSPF area does not support MPLS TE by default.

Format

mpls-te enable [**standard-complying**]

undo mpls-te

Parameters

Parameter	Description	Value
standard-complying	Accepts only LSAs in the standard format. This means that an LSA is rejected if it has more than one Top level TLV.	-

Views

OSPF area view

Default Level

2: Configuration level

Usage Guidelines

MPLS TE can only be enabled in an OSPF area after the OSPF process is enabled with the Opaque LSA function.

Example

Enable TE in OSPF area 1.

```
<Huawei> system-view
[Huawei] ospf 100
[Huawei-ospf-100] opaque-capability enable
[Huawei-ospf-100] area 1
[Huawei-ospf-100-area-0.0.0.1] mpls-te enable
```

Related Topics

9.4.68 opaque-capability enable

11.2.54 mpls rsvp-te

Function

The **mpls rsvp-te** command enables the RSVP-TE function on an interface or globally.

The **undo mpls rsvp-te** command disables the RSVP-TE function.

RSVP-TE is disabled by default.

Format

mpls rsvp-te

undo mpls rsvp-te

Parameters

None

Views

MPLS view, interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

You must run the **mpls (system view)** and **mpls te** commands to enable MPLS and MPLS TE before running the **mpls rsvp-te** command in the MPLS view.

You must run the **mpls (interface view)** and **mpls te** commands to enable MPLS and MPLS TE before running the **mpls rsvp-te** command in the interface view.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

In the MPLS view, the command disables RSVP-TE enabled on all interfaces.

NOTE

Before enabling the RSVP-TE function on an interface, you need to run this command in the MPLS view to enable the RSVP-TE function globally.

Example

Enable RSVP-TE globally.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls rsvp-te
```

Enable RSVP-TE on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
```

Related Topics

11.2.82 mpls te

11.2.55 mpls rsvp-te authentication

Function

The **mpls rsvp-te authentication** command run in the interface or neighbor view enables authentication and set an authentication key.

The **undo mpls rsvp-te authentication** command run in the interface or neighbor view disables authentication.

Authentication is disabled by default.

Format

mpls rsvp-te authentication { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* }

undo mpls rsvp-te authentication

Parameters

Parameter	Description	Value
cipher	Indicates that the key is displayed in cipher text.	-

Parameter	Description	Value
plain	Indicates that the key is displayed in plain text. **NOTICE** If **plain** is selected, the password is saved in the configuration file in plain text. In this case, users at a lower level can easily obtain the password by viewing the configuration file. This brings security risks. Therefore, it is recommended that you select **cipher** to save the password in cipher text.	-
auth-key	Specifies the password.	A string of case-sensitive characters, spaces not supported. When the key is displayed in plaintext, its length ranges from 1 to 255; when the key is displayed in MD5 cipher text, its length ranges from 20 to 392. When double quotation marks are used around the string, spaces are allowed in the string.
keychain *keychain-name*	Specifies the keychain name, which is configured by running the **keychain** command.	The value is the name of an existing keychain.

Views

Interface view, MPLS RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

RSVP authentication can be configured to improve network reliability and security and prevent attacks initiated using messages modified or forged by unauthorized users.

RSVP authentication can prevent the setup of an illegal RSVP neighbor relationship using the following methods and protect the local node against attacks (such as malicious reservation of a larger number of bandwidth resources):

- An unauthorized node attempts to set up an RSVP neighbor relationship with the local node.
- A remote node generates and sends forged RSVP messages to set up a neighbor relationship with the local node.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The **mpls rsvp-te** command is run to enable RSVP-TE in the MPLS view and interface view.

Precautions

The **mpls rsvp-te authentication** command run in either of the following views produces a specific result:

- If this command is run in the interface view, RSVP authentication takes effect on packets received by the interface. The interface sends RSVP-TE packets all carrying authentication information that is calculated using the key of the configured authentication mode, and authenticates all received RSVP-TE packets based on the configured key.
- If this command is run in the MPLS RSVP-TE neighbor view, RSVP authentication takes effect on packets received by the local RSVP-TE neighbor. The RSVP-TE packets sending by neighbor node all carry authentication information that is calculated using the key of the configured authentication mode, and authenticates all RSVP-TE packets sending to the neighbor node based on the configured key.

Parameters are optional for configuring HMAC-MD5 or keychain authentication:

- **cipher**: indicates HMAC-MD5 authentication with the key displayed in cipher text.
- **plain**: indicates HMAC-MD5 authentication with the key displayed in plain text.
- **keychain**: indicates keychain authentication with a globally configured keychain.

Note that HMAC-MD5 encryption algorithm cannot ensure security. Keychain authentication is recommended.

Example

Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<Huawei> system-view
[Huawei] keychain kc1 mode absolute
[Huawei-keychain-kc1] quit
[Huawei] mpls rsvp-te peer 10.1.2.3
[Huawei-mpls-rsvp-te-peer-10.1.2.3] mpls rsvp-te authentication keychain kc1
```

Configure keychain authentication for the peer. The referenced keychain name is **kc1**.

```
<Huawei> system-view
[Huawei] keychain kc1 mode absolute
[Huawei-keychain-kc1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te authentication keychain kc1
```

Related Topics

11.2.73 mpls rsvp-te peer

11.2.56 mpls rsvp-te authentication handshake

Function

The **mpls rsvp-te authentication handshake** command configures the RSVP-TE handshake mechanism.

The **undo mpls rsvp-te authentication handshake** command deletes the RSVP-TE handshake mechanism configuration.

By default, no RSVP-TE handshake mechanism is configured.

Format

mpls rsvp-te authentication handshake

undo mpls rsvp-te authentication handshake

Parameters

None

Views

Interface view, MPLS RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication handshake** command can be used to configure the RSVP-TE handshake mechanism to prevent anti-replay and improve network security.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* } command in the interface view or the MPLS RSVP-TE neighbor view.

Example

Configure the RSVP-TE handshake mechanism.

```
<Huawei> system-view
[Huawei] mpls rsvp-te peer 10.1.2.3
[Huawei-mpls-rsvp-te-peer-10.1.2.3] mpls rsvp-te authentication cipher beijing123
[Huawei-mpls-rsvp-te-peer-10.1.2.3] mpls rsvp-te authentication handshake
```

Configure the RSVP-TE handshake mechanism.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te authentication cipher beijing123
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te authentication handshake
```

Related Topics

11.2.55 mpls rsvp-te authentication

11.2.57 mpls rsvp-te authentication lifetime

11.2.58 mpls rsvp-te authentication window-size

11.2.57 mpls rsvp-te authentication lifetime

Function

The **mpls rsvp-te authentication lifetime** command sets the RSVP-TE authentication lifetime.

The **undo mpls rsvp-te authentication lifetime** command restores the default RSVP-TE authentication lifetime.

By default, the RSVP-TE authentication lifetime is 30 minutes.

Format

mpls rsvp-te authentication lifetime *lifetime*

undo mpls rsvp-te authentication lifetime

Parameters

Parameter	Description	Value
lifetime	Specifies the authentication lifetime.	The value ranges from 00:00:01 to 23:59:59 in the format of HH:MM:SS. The default value is 00:30:00.

Views

Interface view, MPLS RSVP-TE neighbor view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSVP lifetime functions are as follows:

- When no CR-LSP exists between RSVP neighbors, the RSVP adjacency remains until the RSVP authentication lifetime expires. The configuration of the RSVP authentication time does not affect the status of existing CR-LSPs.
- This function can avoid continuous RSVP authentication. For example, when RSVP authentication is enabled between RTA and RTB, but the key is damaged because the RSVP messages sent from RTA to RTB are incorrect, RTB receives and discards the messages. This can cause RTA to continuously send RTB the faulty RSVP messages and RTB to continuously discard these RSVP messages. The authentication relationship between the neighbors, however, cannot be torn down. In this case, the authentication lifetime needs to be configured. When a neighbor is able to receive a valid RSVP message within the lifetime, the RSVP authentication lifetime resets. Otherwise, the authentication relationship between RSVP-TE neighbors is deleted after the authentication lifetime expires.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* } command in the interface view or the MPLS RSVP-TE neighbor view.

Example

Set the authentication lifetime to 40 minutes.

```
<Huawei> system-view
[Huawei] mpls rsvp-te peer 10.1.2.3
[Huawei-mpls-rsvp-te-peer-10.1.2.3] mpls rsvp-te authentication cipher beijing123
[Huawei-mpls-rsvp-te-peer-10.1.2.3] mpls rsvp-te authentication lifetime 00:40:00
```

Set the authentication lifetime to 20 minutes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te authentication cipher beijing123
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te authentication lifetime 00:20:00
```

Related Topics

11.2.55 mpls rsvp-te authentication

11.2.56 mpls rsvp-te authentication handshake

11.2.58 mpls rsvp-te authentication window-size

Function

The **mpls rsvp-te authentication window-size** command specifies the maximum number of RSVP authentication messages that can be received out of sequence.

The **undo mpls rsvp-te authentication window-size** command restores the default configuration.

By default, the maximum number of RSVP authentication messages that can be received out of sequence is 1.

Format

mpls rsvp-te authentication window-size *window-size*

undo mpls rsvp-te authentication window-size

Parameters

Parameter	Description	Value
window-size	Specifies the size of a message window.	The value is an integer that ranges from 1 to 64. The default size is 1.

Views

Interface view, MPLS RSVP-TE neighbor view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Enhanced RSVP authentication can be configured to improve the system security and the capability to authenticate users in the unfavorable environment such as network congestion. Enhanced RSVP authentication functions are as follows:

- Sets the sliding window size for RSVP authentication messages.
- Configures the RSVP-TE handshake mechanism.

Traditional RSVP authentication is used to prevent an unauthorized remote node from setting up a neighbor relationship with the local node. It also prevents attacks (such as maliciously reserving a large number of bandwidth resources) initiated by a remote node after the remote node constructs pseudo RSVP messages to set up an RSVP neighbor relationship with the local node. Traditional RSVP authentication, however, cannot prevent anti-replay attacks or prevent the problem of neighbor relationship termination due to RSVP message disorder.

In an unfavorable environment, the **mpls rsvp-te authentication window-size** command can be used to set the maximum number of RSVP authentication

 Copyright © Huawei Technologies Co., Ltd.

messages that can be received. This setting prevents authentication termination due to RSVP message disorder.

Prerequisites

The RSVP authentication function must have been enabled by running the **mpls rsvp-te authentication** { { **cipher** | **plain** } *auth-key* | **keychain** *keychain-name* } command in the interface view or the MPLS RSVP-TE neighbor view.

Precautions

Setting the window size to a value greater than 32 is recommended. If the size of a sliding window is small, the RSVP messages may be dropped and the RSVP neighbor relationship may be terminated. If the size of a sliding window is set to 1, all the RSVP authentication messages that are received out of sequence are dropped.

Example

Set the size of the message window to 64.

```
<Huawei> system-view
[Huawei] mpls rsvp-te peer 10.1.2.3
[Huawei-mpls-rsvp-te-peer-10.1.2.3] mpls rsvp-te authentication cipher beijing123
[Huawei-mpls-rsvp-te-peer-10.1.2.3] mpls rsvp-te authentication window-size 64
```

Set the size of the message window to 1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te authentication cipher beijing123
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te authentication window-size 1
```

Related Topics

11.2.55 mpls rsvp-te authentication
11.2.56 mpls rsvp-te authentication handshake

11.2.59 mpls rsvp-te bfd

Function

The **mpls rsvp-te bfd** command sets parameters of a BFD session for RSVP on a specified interface.

The **undo mpls rsvp-te bfd** command restores the default configuration.

By default, no parameter of a BFD session for RSVP on a specified interface is set.

Format

mpls rsvp-te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls rsvp-te bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls rsvp-te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Actual local interval at which BFD packets are sent = MAX { Local interval at which BFD packets are sent, Remote interval at which BFD packets are received }; Actual local interval at which BFD packets are received = MAX { Remote interval at which BFD packets are sent, Local interval at which BFD packets are received }; Local detection period = Actual interval at which BFD packets are received x Remote BFD detection multiplier.

For example:

- The local sending interval is 200 ms, while the local receiving interval is 300 ms, and the detection multiplier is 4.
- The remote sending interval is 100 ms, while the remote receiving interval is 600 ms, and the detection multiplier is 5.

Then,

- The actual local sending interval is 600 ms (MAX { 200 ms, 600 ms }), while the local receiving interval is 300 ms (MAX { 100 ms, 300 ms }), and the detection period is 1500 ms (300 ms x 5).
- The actual remote sending interval is 300 ms (MAX { 100 ms, 300 ms }), while the receiving interval is 600 ms (MAX { 200 ms, 600 ms }), and the detection period is 2400 ms (600 ms x 4).

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the parameters for the BFD session on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te bfd min-tx-interval 50 detect-multiplier 5
```

Related Topics

11.2.10 display mpls rsvp-te bfd session
11.2.60 mpls rsvp-te bfd all-interfaces

11.2.60 mpls rsvp-te bfd all-interfaces

Function

The **mpls rsvp-te bfd all-interfaces** command sets session parameters on all RSVP-TE interfaces.

The **undo mpls rsvp-te bfd all-interfaces** command restores the default configuration.

By default, no session parameters on all RSVP-TE interfaces is set.

Format

mpls rsvp-te bfd all-interfaces { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls rsvp-te bfd all-interfaces { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls rsvp-te bfd all-interfaces { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

 Copyright © Huawei Technologies Co., Ltd.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Actual local interval at which BFD packets are sent = MAX { Local interval at which BFD packets are sent, Remote interval at which BFD packets are received }; Actual local interval at which BFD packets are received = MAX { Remote interval at which BFD packets are sent, Local interval at which BFD packets are received }; Local detection period = Actual interval at which BFD packets are received x Remote BFD detection multiplier.

For example:

- The local sending interval is 200 ms, while the local receiving interval is 300 ms, and the detection multiplier is 4.
- The remote sending interval is 100 ms, while the remote receiving interval is 600 ms, and the detection multiplier is 5.

Then,

- The actual local sending interval is 600 ms (MAX { 200 ms, 600 ms }), while the local receiving interval is 300 ms (MAX { 100 ms, 300 ms }), and the detection period is 1500 ms (300 ms x 5).
- The actual remote sending interval is 300 ms (MAX { 100 ms, 300 ms }), while the receiving interval is 600 ms (MAX { 200 ms, 600 ms }), and the detection period is 2400 ms (600 ms x 4).

Example

Set the session parameters of all RSVP-TE interfaces.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te bfd all-interfaces min-tx-interval 500 min-rx-interval 400
```

Related Topics

11.2.61 mpls rsvp-te bfd all-interfaces enable
11.2.10 display mpls rsvp-te bfd session

11.2.61 mpls rsvp-te bfd all-interfaces enable

Function

The **mpls rsvp-te bfd all-interfaces enable** command globally enables BFD for RSVP.

The **undo mpls rsvp-te bfd all-interfaces enable** command restores the default configuration.

By default, BFD for RSVP is disabled.

Format

mpls rsvp-te bfd all-interfaces enable

undo mpls rsvp-te bfd all-interfaces enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd all-interfaces enable** command enables the capability of creating BFD sessions on all interfaces that are not blocked from BFD for RSVP.

Example

Enable BFD for RSVP globally.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te bfd all-interfaces enable
```

Related Topics

11.2.10 display mpls rsvp-te bfd session

11.2.62 mpls rsvp-te bfd block

11.2.63 mpls rsvp-te bfd enable

11.2.62 mpls rsvp-te bfd block

Function

The **mpls rsvp-te bfd block** command blocks the BFD for RSVP capability on an interface.

The **undo mpls rsvp-te bfd block** command restores the default configuration.

By default, the BFD for RSVP capability on an interface is not blocked.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls rsvp-te bfd block

undo mpls rsvp-te bfd block

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd block** command and the **mpls rsvp-te bfd enable** command are mutually exclusive.

The **mpls rsvp-te bfd block** command is similar to the **undo mpls rsvp-te bfd enable** command. Their differences are as follows:

- When the **undo mpls rsvp-te bfd enable** command is run to disable BFD for RSVP on an RSVP interface, the interface can obtain the BFD for RSVP capability after you configure the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view.
- When the **mpls rsvp-te bfd block** command is run on an interface, the interface cannot obtain the BFD for RSVP capability even if the **mpls rsvp-te bfd all-interfaces enable** command is run in the MPLS view.

NOTE

- To enable the BFD for RSVP capability on a majority of interfaces, you can run the **mpls rsvp-te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for RSVP. Then, you can run the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view to enable the BFD for RSVP capability for the desired majority.
- To enable BFD for RSVP capability on a few interfaces, you can run the **mpls rsvp-te bfd enable** command on these specific interfaces. In addition, you can run the **undo mpls rsvp-te bfd enable** command or the **mpls rsvp-te bfd block** command to disable BFD for RSVP on these interfaces.

Example

Disable BFD for RSVP on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te bfd block
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

11.2.63 mpls rsvp-te bfd enable

11.2.63 mpls rsvp-te bfd enable

Function

The **mpls rsvp-te bfd enable** command enables the BFD for RSVP capability on an interface.

The **undo mpls rsvp-te bfd enable** command restores the default configuration.

By default, the BFD for RSVP capability on an interface is disabled.

Format

mpls rsvp-te bfd enable

undo mpls rsvp-te bfd enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls rsvp-te bfd enable** command and the **mpls rsvp-te bfd block** command are mutually exclusive. When using these commands, note the following:

- If the **undo mpls rsvp-te bfd enable** command is run to disable BFD for RSVP on an RSVP interface, the interface can still obtain the BFD for RSVP capability after you configure the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view.
- If the **mpls rsvp-te bfd block** command is run on an interface, the interface cannot obtain the BFD for RSVP capability even if the **mpls rsvp-te bfd all-interfaces enable** command is run in the MPLS view.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- To enable the BFD for RSVP capability on a majority of interfaces, you can run the **mpls rsvp-te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for RSVP. Then, you can run the **mpls rsvp-te bfd all-interfaces enable** command in the MPLS view to enable the BFD for RSVP capability for the desired majority.
- To enable BFD for RSVP capability on a few interfaces, you can run the **mpls rsvp-te bfd enable** command on these specific interfaces. In addition, you can run the **undo mpls rsvp-te bfd enable** command or the **mpls rsvp-te bfd block** command to disable BFD for RSVP on these interfaces.

Example

Enable the BFD for RSVP capability on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te bfd enable
```

Related Topics

11.2.62 mpls rsvp-te bfd block

11.2.64 mpls rsvp-te challenge-lost

Function

The **mpls rsvp-te challenge-lost** command sets the maximum number of times that the authenticator allows itself to retransmits Challenge messages during RSVP authentication.

The **undo mpls rsvp-te challenge-lost** command restores the default setting.

By default, the number of times for retransmitting Challenge messages is 3.

Format

mpls rsvp-te challenge-lost *max-miss-times*

undo mpls rsvp-te challenge-lost

Parameters

Parameter	Description	Value
max-miss-times	Specifies the number of times for retransmitting Challenge messages.	The value is an integer that ranges from 1 to 10. The default value is 3.

Views

MPLS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Assume node A and node B are RSVP neighbors and they need to authenticate each other. Node A authenticates node B as follows:

- Node A sends an RSVP message carrying an Integrity object to node B.
- When node B receives the message and detects that the key ID of node A is different from that in the Integrity object, node B sends a Challenge message to node A and starts a timer determining the time interval at which the Challenge message will be periodically retransmitted, and records the number of retries.
- When node A receives the Challenge message from node B, it directly copies the Challenge object in a message and adds its Integrity object to the message to generate a Response message to be sent to node B.
- When node B receives the Response message from node A, it checks whether or not the Challenge object in the Response message is consistent with the local Challenge object.
  - If the Challenge objects are consistent, node B stops and resets the timer for sending Challenge messages. Then, the authentication is successful.
  - If the Challenge message timer expires before node B receives the Response message, the authentication fails.

You can run the **mpls rsvp-te challenge-lost** command to change the maximum number of times for sending Challenge messages. In addition, you can use the **mpls rsvp-te retrans-timer challenge** command to change the interval for retransmitting Challenge messages.

Example

Set the number of times for retransmitting Challenge messages to 5.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te challenge-lost 5
```

Related Topics

11.2.55 mpls rsvp-te authentication

11.2.76 mpls rsvp-te retrans-timer challenge

11.2.65 mpls rsvp-te fast-reroute-bandwidth compatible

Function

The **mpls rsvp-te fast-reroute-bandwidth compatible** command configures the bandwidth of FRR objects to be saved in the integer mode.

The **undo mpls rsvp-te fast-reroute-bandwidth compatible** command restores the default configuration.

By default, the bandwidth of FRR objects is saved in the float point mode.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls rsvp-te fast-reroute-bandwidth compatible

undo mpls rsvp-te fast-reroute-bandwidth compatible

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

When Huawei devices communicate with devices from other vendors whose saving mode of the bandwidth of FRR objects is set to the integer mode, you need to run this command to set the saving mode of the bandwidth of FRR objects to the integer mode.

Example

Configure the saving mode of the bandwidth of FRR objects as the integer mode.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te fast-reroute-bandwidth compatible
```

Related Topics

11.2.84 mpls te auto-frr (MPLS view)

11.2.66 mpls rsvp-te hello-lost

Function

The **mpls rsvp-te hello-lost** command sets the maximum number of times for the consecutively lost Hello messages.

The **undo mpls rsvp-te hello-lost** command restores the default configuration.

By default, a maximum of three Hello messages can be lost consecutively.

Format

mpls rsvp-te hello-lost *times*

undo mpls rsvp-te hello-lost

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
times	Specifies the maximum number of times for the consecutively lost Hello messages.	The value is an integer that ranges from 3 to 10. The default value is 3.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the RSVP Hello extension function is enabled, you can run this command to set the maximum number of times for the consecutively lost Hello messages. If the number of times a node does not receive Hello messages consecutively exceeds the maximum value, it is considered that the link fails.

Prerequisites

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command in the MPLS view.

Example

Set the maximum number of times for the consecutively lost Hello messages to 5.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te hello
[Huawei-mpls] mpls rsvp-te hello-lost 5
```

Related Topics

11.2.67 mpls rsvp-te hello

11.2.79 mpls rsvp-te timer hello

11.2.67 mpls rsvp-te hello

Function

The **mpls rsvp-te hello** command enables the RSVP Hello extension function globally or on an interface.

The **undo mpls rsvp-te hello** command disables the RSVP Hello extension function globally or on an interface.

By default, the RSVP Hello extension function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls rsvp-te hello

undo mpls rsvp-te hello

Parameters

None

Views

MPLS view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RSVP Hello extension mechanism provides fast detection on the reachability between RSVP nodes. The function increases network costs. Therefore, you need to determine whether to enable this function based on network requirements.

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

Precautions

The **undo mpls rsvp-te hello** command in the MPLS view disables the Hello function from all interfaces and disables GR Helper on the local node.

You can run the **mpls rsvp-te hello** command in the MPLS view to enable the Hello function globally. After that, you can run the **mpls rsvp-te hello** command in the interface view to enable the Hello function on an interface.

The **undo mpls rsvp-te hello** command in the interface view is used to disable the Hello function on the interface. The **undo mpls rsvp-te hello** command in the MPLS view is used to disable the Hello function globally.

Example

Enable the RSVP Hello extension function globally.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls rsvp-te
[Huawei-mpls] mpls rsvp-te hello
```

Enable the RSVP Hello extension function on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te hello
```

Related Topics

11.2.79 mpls rsvp-te timer hello

11.2.66 mpls rsvp-te hello-lost

11.2.68 mpls rsvp-te hello basic-restart-time

Function

The **mpls rsvp-te hello basic-restart-time** command changes the basic time of RSVP GR.

The **undo mpls rsvp-te hello basic-restart-time** command restores the default setting.

By default, the basic time of RSVP GR is 90 seconds.

NOTE

Only the AR3260 supports this command.

Format

mpls rsvp-te hello basic-restart-time *basic-restart-time*

undo mpls rsvp-te hello basic-restart-time

Parameters

Parameter	Description	Value
basic-restart-time	Specifies the basic time of RSVP GR.	The value is an integer that ranges from 30 to 1200, in seconds.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

At the beginning of the AMB/SMB switchover, an RSVP-TE GR node enters a period during which the data plane can forward data but the control plane is not restored. A Restart timer starts following this phase. The restart time is relevant to the basic time, the number of ingress LSPs and the number of non-ingress LSPs.

 Copyright © Huawei Technologies Co., Ltd.

The default basic time is 90 seconds. You can use the **mpls rsvp-te hello basic-restart-time** command to change the value of the basic time.

After the Restart timer expires, the node starts a Recovery timer. The recovery time is relevant to the restart time and total number of LSPs.

Prerequisites

RSVP GR has been enabled by running the **mpls rsvp-te hello full-gr** command in the MPLS view.

Example

Set the basic time of RSVP GR to 39 seconds.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te hello basic-restart-time 39
```

Related Topics

11.2.69 mpls rsvp-te hello full-gr

11.2.12 display mpls rsvp-te graceful-restart

11.2.13 display mpls rsvp-te graceful-restart peer

11.2.69 mpls rsvp-te hello full-gr

Function

The **mpls rsvp-te hello full-gr** command enables RSVP GR and RSVP GR Helper.

The **undo mpls rsvp-te hello full-gr** command restores the default configurations.

By default, RSVP GR and RSVP GR Helper are disabled.

NOTE

Only the AR3260 supports this command.

Format

mpls rsvp-te hello full-gr

undo mpls rsvp-te hello full-gr

Parameters

None

Views

MPLS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command.

Example

Enable RSVP GR and RSVP GR Helper.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te
[Huawei-mpls] mpls rsvp-te hello
[Huawei-mpls] mpls rsvp-te hello full-gr
```

Related Topics

11.2.54 mpls rsvp-te

11.2.67 mpls rsvp-te hello

11.2.71 mpls rsvp-te hello support-peer-gr

11.2.70 mpls rsvp-te hello nodeid-session

Function

The **mpls rsvp-te hello nodeid-session** command establishes a Hello session between a PLR node and an MP node and specifies the ID of a single-hop or multi-hop node.

The **undo mpls rsvp-te hello nodeid-session** command restores the default configuration.

By default, no Hello session is established between a PLR node and an MP node.

Format

mpls rsvp-te hello nodeid-session *ip-address*

undo mpls rsvp-te hello nodeid-session [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a neighbor.	The value is in dotted decimal notation.

Views

MPLS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

On a TE FRR network, to ensure the protection of the primary tunnel when FRR and RSVP GR simultaneously occur, run the **mpls rsvp-te hello nodeid-session** command to establish a Hello session between a PLR node and an MP node.

Example

Establish a Hello session between the PLR and MP along the bypass tunnel.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te hello
[Huawei-mpls] mpls rsvp-te hello nodeid-session 10.0.0.1
```

Related Topics

11.2.67 mpls rsvp-te hello

11.2.71 mpls rsvp-te hello support-peer-gr

Function

The **mpls rsvp-te hello support-peer-gr** command enables RSVP GR Helper.

The **undo mpls rsvp-te hello support-peer-gr** command restores the default configuration.

By default, RSVP GR Helper is disabled.

Format

mpls rsvp-te hello support-peer-gr

undo mpls rsvp-te hello support-peer-gr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command.

Precautions

If the **mpls rsvp-te hello full-gr** command is run on an RSVP node, this node has the capability of RSVP GR Helper. If a node is a GR supporter rather than a GR node, run the **mpls rsvp-te hello support-peer-gr** command.

To change a node from a GR node to a GR supporter, you must run the **undo mpls rsvp-te hello full-gr** command, then run the **mpls rsvp-te hello support-peer-gr** command.

Example

Enable RSVP GR Helper.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te
[Huawei-mpls] mpls rsvp-te hello
[Huawei-mpls] mpls rsvp-te hello support-peer-gr
```

Related Topics

11.2.54 mpls rsvp-te

11.2.67 mpls rsvp-te hello

11.2.69 mpls rsvp-te hello full-gr

11.2.72 mpls rsvp-te keep-multiplier

Function

The **mpls rsvp-te keep-multiplier** command sets the number of retry times allowed for RSVP Refresh messages.

The **undo mpls rsvp-te keep-multiplier** command restores the default settings.

The number of retry times allowed for RSVP Refresh messages is 3 by default.

Format

mpls rsvp-te keep-multiplier *keep-multiplier-number*

undo mpls rsvp-te keep-multiplier

Parameters

Parameter	Description	Value
keep-multiplier-number	Specifies the number of retry times allowed for RSVP Refresh messages.	The value is an integer that ranges from 3 to 255. The default value is 3.

 Copyright © Huawei Technologies Co., Ltd.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a node does not receive any Refresh message about PSB or RSB within a specified time period, the node deletes the state. You can run this command to modify the number of retry times for Refresh messages to change of the timeout period.

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

Precautions

The timeout period is calculated by using the following formula:

Timeout period = (*keep-multiplier-number* + 0.5) x 1.5 x *refresh-interval*.

In the formula, *keep-multiplier-number* specifies the number of retry times allowed for RSVP Refresh messages; *refresh-interval* specifies the interval at which RSVP Refresh messages are sent. To set these two parameters, run the **mpls rsvp-te timer refresh** command.

Example

Set the number of retry times for RSVP Refresh messages to 5.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te keep-multiplier 5
```

Related Topics

11.2.80 mpls rsvp-te timer refresh

11.2.54 mpls rsvp-te

11.2.73 mpls rsvp-te peer

Function

The **mpls rsvp-te peer** command sets up an RSVP neighbor node and displays the MPLS RSVP-TE neighbor view.

The **undo mpls rsvp-te peer** command deletes an RSVP neighbor node.

No RSVP neighbor node is set up by default.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls rsvp-te peer *ip-address*

undo mpls rsvp-te peer *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a neighbor interface or the LSR ID. The LSR ID is specified in the **mpls lsr-id** command.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command in the MPLS view.

Precautions

You can run this command on two neighboring devices to configure neighbor nodes. Then you can configure these neighbors with other functions such as authentication and handshake. The command functions differ according to the values of *ip-address*.

- When *ip-address* is the LSR-ID of a neighbor, the command takes effect on an entire device.
- When *ip-address* is the IP address of a neighbor interface, the command takes effect only on the single interface.

NOTE

If a neighbor node is identified by its LSR-ID, CSPF must be enabled on two neighboring devices where RSVP authentication is required.

Example

Set up an RSVP neighbor node and displays the MPLS RSVP-TE neighbor view.

```
<Huawei> system-view
[Huawei] mpls rsvp-te peer 10.1.2.3
[Huawei-mpls-rsvp-te-peer-10.1.2.3]
```

Related Topics

11.2.54 mpls rsvp-te

 Copyright © Huawei Technologies Co., Ltd.

11.2.74 mpls rsvp-te resv-rro

Function

The **mpls rsvp-te resv-rro** command configures record route objects (RROs) carried in Resv messages.

The **undo mpls rsvp-te resv-rro** command restores the default setting.

By default, the labels carried in the transit LSP RRO in turn are inbound interface address with upstream label, LSR ID with upstream label, and outbound interface address. The labels carried in the egress LSP RRO in turn are inbound interface address with upstream label, LSR ID with upstream label.

Format

mpls rsvp-te resv-rro transit { { **incoming** | **incoming-with-label** } | { **routerid** | **routerid-with-label** } | { **outgoing** | **outgoing-with-label** } } *

mpls rsvp-te resv-rro egress { { **incoming** | **incoming-with-label** } | { **routerid** | **routerid-with-label** } } *

undo mpls rsvp-te resv-rro transit

undo mpls rsvp-te resv-rro egress

Parameters

Parameter	Description	Value
transit	Indicates a transit node.	-
incoming	Indicates an inbound interface address.	-
incoming-with-label	Indicates an inbound interface address and upstream label.	-
routerid	Indicates an LSR ID.	-
routerid-with-label	Indicates an LSR ID and an upstream label.	-
outgoing	Indicates an outbound interface address.	-
outgoing-with-label	Indicates an outbound interface address and a downstream label.	-
egress	Indicates an egress.	-

Views

MPLS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Two devices of different types must have the same RRO configuration to ensure that they can communicate with each other. You can run the **mpls rsvp-te resv-rro** command to configures RROs carried in Resv messages.

Precautions

The modification takes effect only for new LSPs.

Example

Configure the transit LSP RRO to carry the following labels: LSR ID with upstream label, inbound interface address, and outbound interface address with downstream label.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te resv-rro transit routerid-with-label incoming outgoing-with-label
```

Configure the egress LSP RRO to carry the following labels: LSR ID with upstream label, and inbound interface address.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te resv-rro egress routerid-with-label incoming
```

11.2.75 mpls rsvp-te resvconfirm

Function

The **mpls rsvp-te resvconfirm** command enables the reservation confirmation mechanism on a node.

The **undo mpls rsvp-te resvconfirm** command disables the reservation confirmation mechanism.

The mechanism is disabled on a node by default.

Format

mpls rsvp-te resvconfirm

undo mpls rsvp-te resvconfirm

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **mpls rsvp-te resvconfirm** command is configured on the egress of the TE tunnel.

Example

Enable the reservation confirmation mechanism on the local node.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te resvconfirm
```

11.2.76 mpls rsvp-te retrans-timer challenge

Function

The **mpls rsvp-te retrans-timer challenge** command configures the interval at which a Challenge message is retransmitted.

The **undo mpls rsvp-te retrans-timer challenge** command restores the default value.

The interval at which a Challenge message is retransmitted is set to 1000 milliseconds by default.

Format

mpls rsvp-te retrans-timer challenge *retransmission-interval*

undo mpls rsvp-te retrans-timer challenge

Parameters

Parameter	Description	Value
retransmission-interval	Specifies the interval at which a Challenge message is retransmitted.	An integer ranging from 500 to 10000 in milliseconds. The value is 1000 milliseconds by default.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Assume node A and node B are RSVP neighbors and they need to authenticate each other. Node A authenticates node B as follows:

- Node A sends an RSVP message carrying an Integrity object to node B.

 Copyright © Huawei Technologies Co., Ltd.

- When node B receives the message and detects that the key ID of node A is different from that in the Integrity object, node B sends a Challenge message to node A and starts a timer determining the time interval at which the Challenge message will be periodically retransmitted, and records the number of retries.
- When node A receives the Challenge message from node B, it directly copies the Challenge object in a message and adds its Integrity object to the message to generate a Response message to be sent to node B.
- When node B receives the Response message from node A, it checks whether or not the Challenge object in the Response message is consistent with the local Challenge object.
  - If the Challenge objects are consistent, node B stops and resets the timer for sending Challenge messages. Then, the authentication is successful.
  - If the Challenge message timer expires before node B receives the Response message, the authentication fails.

You can run the **mpls rsvp-te challenge-lost** command to change the maximum number of attempts to send Challenge messages. In addition, you can use the **mpls rsvp-te retrans-timer challenge** command to change the interval at which a Challenge message is retransmitted.

Example

Set the interval for retransmitting a Challenge message to 800 ms.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te retrans-timer challenge 800
```

Related Topics

11.2.55 mpls rsvp-te authentication

11.2.64 mpls rsvp-te challenge-lost

11.2.77 mpls rsvp-te send-message

Function

The **mpls rsvp-te send-message** command configures the formats of objects in a sent message.

The **undo mpls rsvp-te send-message** command restores the default configuration.

By default, the formats of objects in the sent message are not configured.

Format

mpls rsvp-te send-message { **suggest-label** | **extend-class-type value-length-type** | **session-attribute without-affinity** | **down-reason** }

undo mpls rsvp-te send-message { **suggest-label** | **extend-class-type value-length-type** | **session-attribute without-affinity** | **down-reason** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
suggest-label	Indicates that an RSVP message carries the suggest-label object.	-
extend-class-type value-length-type	Indicates that the encoding format of the extend-class-type object in an RSVP message is value-length-type.	-
session-attribute without-affinity	Indicates that the session-attribute in an RSVP message does not carry the affinity attribute.	-
down-reason	Indicates that RSVP messages carry the down-reason object.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls rsvp-te send-message** command controls the formats of objects in the messages sent by nodes. If required, you can use this command to adjust the transmission of messages so that downstream nodes can use the carried object format in processing.

When a Huawei device attempts to communicate with a non-Huawei device, RSVP messages sent by the non-Huawei device may not support the affinity attribute, causing a communication failure. To allow successful communication, run the **mpls rsvp-te send-message session-attribute without-affinity** command to allow the Huawei device to receive RSVP messages without the affinity attribute.

If you want an ingress to learn RSVP-TE tunnel Down causes of the transit and egress nodes, run the **mpls rsvp-te send-message down-reason** command on the transit and egress nodes, facilitating fault locating.

Precautions

The modification takes effect only for new LSPs.

Configurations of the four formats of objects in a sent message can take effect simultaneously.

Example

Include the suggest-label object from a message.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te send-message suggest-label
```

 Copyright © Huawei Technologies Co., Ltd.

Set the encoding format of the extend-class-type object in an RSVP message to value-length-type.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te send-message extend-class-type value-length-type
```

Allow a message to carry the session-attribute object without the affinity attribute.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te send-message session-attribute without-affinity
```

Configure RSVP messages to carry the down-reason object.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls rsvp-te send-message down-reason
```

11.2.78 mpls rsvp-te srefresh

Function

The **mpls rsvp-te srefresh** command enables the summary refresh (Srefresh) function on an interface or globally.

The **undo mpls rsvp-te srefresh** command disables the Srefresh function.

The Srefresh function is disabled by default.

Format

mpls rsvp-te srefresh

undo mpls rsvp-te srefresh

Parameters

None

Views

MPLS view, interface view

Default Level

2: Configuration level

Usage Guidelines

Each RSVP session needs to generate, send, receive, and process RSVP Path messages and Resv message within the refresh period. With an increasing number of RSVP sessions, a large amount of Refresh messages are generated to maintain the RSVP soft state. When an RSVP message, not an RSVP Refresh message, is dropped, reliability is deteriorated and causes delay. The Srefresh extension can solve the preceding problems. The summary refresh mechanism reduces the required number of Refresh messages and improves reliability of RSVP messages and efficiency of resource usage.

 Copyright © Huawei Technologies Co., Ltd.

After the Srefresh function is enabled in the MPLS view, the Srefresh function is enable globally. In addition, the interface enabled with the Srefresh function can refresh the path status and the reservation status by sending Srefresh messages, rather than Path or Resv messages.

Example

Enable the Srefresh function globally.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls rsvp-te
[Huawei-mpls] mpls rsvp-te srefresh
```

Enable the Srefresh function on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te srefresh
```

Related Topics

11.2.54 mpls rsvp-te

11.2.79 mpls rsvp-te timer hello

Function

The **mpls rsvp-te timer hello** command sets an interval at which Hello messages are sent.

The **undo mpls rsvp-te timer hello** command restores the default setting.

The interval at which Hello messages are sent is 3 seconds by default.

Format

mpls rsvp-te timer hello *interval*

undo mpls rsvp-te timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval at which Hello messages are sent.	The value is an integer that ranges from 1 to 25, in seconds. The default value is 3s.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

The RSVP Hello extension function has been enabled by running the **mpls rsvp-te hello** command in the MPLS view.

NOTE

If the interval at which Hello messages are sent is changed, the new interval can only take effect after the previous Hello timer expires.

Example

Set the interval at which Hello messages are sent to 5s.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls rsvp-te
[Huawei-mpls] mpls rsvp-te hello
[Huawei-mpls] mpls rsvp-te timer hello 5
```

Related Topics

11.2.67 mpls rsvp-te hello

11.2.66 mpls rsvp-te hello-lost

11.2.80 mpls rsvp-te timer refresh

Function

The **mpls rsvp-te timer refresh** command sets an interval at which RSVP Refresh messages are sent.

The **undo mpls rsvp-te timer refresh** command restores the default setting.

The time interval is 30 seconds by default.

Format

mpls rsvp-te timer refresh *refresh-interval*

undo mpls rsvp-te timer refresh

Parameters

Parameter	Description	Value
refresh-interval	Specifies the interval at which RSVP Refresh messages are sent.	An integer ranging from 10 to 65535 in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

RSVP-TE has been enabled by running the **mpls rsvp-te** command.

NOTE

If the interval at which RSVP Refresh messages are sent is changed, the new interval can only take effect after the previous refreshing timer expires. Therefore, you are not recommended to set an excessively long refreshing interval, or frequently change a refreshing interval.

Example

Set the interval at which RSVP Refresh messages are sent to 60s.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls rsvp-te
[Huawei-mpls] mpls rsvp-te timer refresh 60
```

Related Topics

11.2.72 mpls rsvp-te keep-multiplier

11.2.23 display mpls rsvp-te statistics

11.2.54 mpls rsvp-te

11.2.81 mpls rsvp-te timer retransmission

Function

The **mpls rsvp-te timer retransmission** command adjusts retransmission-related parameters on an interface.

The **undo mpls rsvp-te timer retransmission** command restores the default settings.

By default, the retransmission incremental is 1 and the timeout period of a retransmission timer is 5000 ms.

Format

mpls rsvp-te timer retransmission { **increment-value** *increment* | **retransmit-value** *interval* } *

undo mpls rsvp-te timer retransmission [**increment-value** [*increment*] | **retransmit-value** [*interval*]] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
increment-value *increment*	Specifies the retransmission incremental value.	The value is an integer that ranges from 1 to 10. The default value is 1.
retransmit-value *interval*	Specifies the timeout period of a retransmission timer.	The value is an integer that ranges from 500 to 5000, in milliseconds. The default value is 5000 ms.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The relationship between *increment* and *interval*: Next retransmission *interval* = Current retransmission *interval* x (1 + *increment*)

Prerequisites

The Srefresh function has been enabled by running the **mpls rsvp-te srefresh** command in the MPLS view.

Example

Set the timeout period of the retransmission timer to 500 ms and the increment to 2 on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te
[Huawei-GigabitEthernet1/0/0] mpls rsvp-te timer retransmission retransmit-value 500 increment-value 2
```

Related Topics

11.2.78 mpls rsvp-te srefresh

11.2.82 mpls te

Function

The **mpls te** command enables MPLS TE.

The **undo mpls te** command disables MPLS TE.

MPLS TE is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls te

undo mpls te

Parameters

None

Views

MPLS view, interface view

Default Level

2: Configuration level

Usage Guidelines

When running the **mpls te** command in the MPLS view, you can globally enable MPLS TE. When running the **mpls te** command in the interface view, you can enable MPLS TE on a specified interface. MPLS TE can only be enabled on interfaces after the function is enabled globally.

NOTICE

When the MPLS TE is disabled in the interface view, all the CR-LSPs on the current interface change to Down.

When the MPLS TE is disabled in the MPLS view, the MPLS TE on each interface is disabled, and all CR-LSPs are deleted.

Example

Enable MPLS TE globally.

```
<Huawei> system-view
[Huawei] mpls lsr-id 1.1.1.9
[Huawei] mpls
[Huawei-mpls] mpls te
```

Enable MPLS TE on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
```

11.2.83 mpls te affinity property

Function

The **mpls te affinity property** command configures the affinity property for an MPLS TE tunnel.

 Copyright © Huawei Technologies Co., Ltd.

The **undo mpls te affinity property** command restores the default settings.

By default, both the affinity value and the affinity mask are 0x0 for an MPLS TE tunnel.

Format

mpls te affinity property *properties* [**mask** *mask-value*] [**secondary** | **best-effort**]

undo mpls te affinity property [**secondary** | **best-effort**]

undo mpls te affinity property *properties* [**mask** *mask-value*] { **secondary** | **best-effort** }

Parameters

Parameter	Description	Value
properties	Specifies the affinity property of links that carry a tunnel.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF. The default value is 0x0.
mask *mask-value*	Specifies the link property to be checked.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF. The default value is 0x0.
secondary	Indicates the affinity property of a backup CR-LSP.	-
best-effort	Indicates the affinity property of the best-effort path.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Affinity property masks determine the link properties that should be checked by a device.

To ensure that a link can be used by a tunnel, for the bits that are 1 in a mask, it is required that at least one bit in the administrative group and the corresponding

 Copyright © Huawei Technologies Co., Ltd.

bit in the affinity property be 1. In addition, if the bits in the affinity property are 0, the corresponding bits in the administrative group cannot be 1.

After an affinity property for the MPLS TE tunnel is changed and the new configuration is committed, the established LSPs can be affected, and the path of the TE tunnel is recalculated.

Example

Set the affinity property of Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te affinity property a04 mask e0c
[Huawei-Tunnel0/0/1] mpls te commit
```

Set the affinity property of the backup CR-LSP and the best-effort path.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te backup hot-standby
[Huawei-Tunnel0/0/1] mpls te backup ordinary best-effort
[Huawei-Tunnel0/0/1] mpls te affinity property a04 mask e0c secondary
[Huawei-Tunnel0/0/1] mpls te affinity property a04 mask e0c best-effort
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.111 mpls te link administrative group

11.2.84 mpls te auto-frr (MPLS view)

Function

The **mpls te auto-frr** command globally enables the TE Auto FRR function.

The **undo mpls te auto-frr** command globally disables the TE Auto FRR function.

TE Auto FRR is disabled by default.

Format

mpls te auto-frr

undo mpls te auto-frr

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **mpls te auto-frr** command to globally enable the TE Auto FRR function.

Precautions

After the TE Auto FRR function is enabled globally, all MPLS TE-enabled interfaces use node protection by default.

If TE Auto FRR is enabled globally, all interfaces that are enabled with MPLS TE on the device are automatically configured with the **mpls te auto-frr default** command by default. To disable TE Auto FRR on certain interfaces, run the **mpls te auto-frr block** command on these interfaces.

Example

Enable the TE Auto FRR function.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te auto-frr
```

Disable the TE Auto FRR function.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] undo mpls te auto-frr
```

Related Topics

11.2.85 mpls te auto-frr (interface view)

11.2.85 mpls te auto-frr (interface view)

Function

The **mpls te auto-frr** command configures the TE Auto FRR function in the interface view.

The **undo mpls te auto-frr** command restores the default configuration.

The TE Auto FRR function is disabled on an interface by default.

Format

mpls te auto-frr { **default** | **link** | **node** | **block** }

undo mpls te auto-frr { **block** | **link** | **node** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
default	Indicates that the configuration of the TE Auto FRR function in the MPLS view is used by default. Only node protection is provided.	-
link	Indicates that only link protection is provided.	-
node	Indicates that node protection is provided. When the topology does not meet the requirement to set up a bypass CR-LSP for node protection, the penultimate hop (but not other hops) on the primary CR-LSP attempts to set up a bypass CR-LSP for link protection.	-
block	Disables the TE Auto FRR function in the interface view.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the TE Auto FRR function is enabled globally, all MPLS TE-enabled interfaces can use the TE Auto FRR configuration configured in the MPLS view.

To disable the TE Auto FRR function on a specified interface, you must run the **mpls te auto-frr block** command. To enable link protection on a specified interface, you must run the **mpls te auto-frr link** command.

Prerequisites

MPLS TE has been enabled by running the **mpls te** command in the interface view.

Precautions

After the **mpls te auto-frr block** command is run on an interface, the interface does not have the TE Auto FRR capability, regardless of whether or not TE Auto FRR is already enabled or reenabled globally.

After the command **mpls te auto-frr** is configured in the MPLS view, the device provides only node protection when you run the **mpls te auto-frr default** or **mpls te auto-frr node** command on an interface. When the topology does not meet the requirement to set up a bypass CR-LSP for node protection, the penultimate hop (but not other hops) on the primary CR-LSP attempts to set up a bypass CR-LSP for link protection.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable TE Auto FRR that provides link protection on the interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te auto-frr link
```

Disable the TE Auto FRR function in the interface view.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te auto-frr block
```

Related Topics

11.2.84 mpls te auto-frr (MPLS view)

11.2.86 mpls te auto-frr reoptimization

Function

The **mpls te auto-frr reoptimization** command enables auto bypass tunnel re-optimization.

The **undo mpls te auto-frr reoptimization** command disables auto bypass tunnel re-optimization.

By default, auto bypass tunnel re-optimization is disabled.

Format

mpls te auto-frr reoptimization [**frequency** *interval*]

undo mpls te auto-frr reoptimization

Parameters

Parameter	Description	Value
frequency *interval*	Indicates the re-optimization interval. Paths are recalculated at the *interval* based on auto bypass tunnel constraints. If an optimal path to the same destination is available, the system re-optimizes the auto bypass tunnel.	The value is an integer ranging from 60 to 604800, in seconds. The default value is 3600s (one hour).

Views

MPLS view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network changes often cause the changes in optimal paths. Run the **mpls te auto-frr reoptimization** to allow paths to be recalculated at certain intervals for an auto bypass tunnel. If an optimal path to the same destination is found due to some reasons, such as the changes in the cost, a new auto bypass tunnel will be set up over this optimal path. In this manner, network resources are optimized.

Auto bypass tunnel re-optimization can be classified into the following modes:

- Automatic re-optimization: Auto bypass tunnels are re-optimized at intervals, requiring no manual intervention. The **mpls te auto-frr reoptimization** command can be used to implement the function, and this command takes effect on the auto bypass tunnels that have been already set up successfully.
- Manual re-optimization: After the **mpls te auto-frr reoptimization** command is run, run the **mpls te reoptimization (user view)** command to re-optimize auto bypass tunnels manually.

Prerequisites

MPLS TE has been enabled using the **mpls te** command.

Example

Configure auto bypass tunnel re-optimization at 8939-second intervals.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls te auto-frr reoptimization frequency 8939
```

Related Topics

11.2.120 mpls te reoptimization (user view)

11.2.87 mpls te backup

Function

The **mpls te backup** command specifies the backup mode of an existing tunnel.

The **undo mpls te backup** command restores the default configuration.

By default, no tunnel is backed up.

Format

mpls te backup ordinary [**best-effort**]

mpls te backup hot-standby [**mode** { **revertive** [**wtr** *interval*] | **non-revertive** } | **dynamic-bandwidth**] *

mpls te backup hot-standby wtr *interval* [**dynamic-bandwidth**]

mpls te backup hot-standby dynamic-bandwidth wtr *interval*

undo mpls te backup { **hot-standby** [**mode** { **revertive** [**wtr** [*interval*]] | **non-revertive** } | **dynamic-bandwidth**] * | **ordinary** }

Parameters

Parameter	Description	Value
ordinary	Enables the ordinary backup mode. In ordinary backup mode, an ordinary backup CR-LSP is created only after the primary CR-LSP fails.	-
hot-standby	Enables the hot-standby mode. In hot-standby mode, both the primary and backup CR-LSP are set up. If the primary CR-LSP fails, traffic is immediately switched to the hot-standby CR-LSP.	-
dynamic-bandwidth	Enables the dynamic bandwidth function for a hot-standby CR-LSP.	-
wtr *interval*	Specifies the wait-to-restore (WTR) time in hot standby.	The value is an integer that ranges from 0 to 2592000, in seconds. The default value is 10 seconds.
best-effort	Enables the best-effort path mode. When both the primary and backup CR-LSPs fail, the system triggers the establishment of a best-effort path.	-
mode { **revertive** | **non-revertive** }	Specifies the revertive mode. ● **revertive**: The current mode can be switched to the original mode. ● **non-revertive**: The current mode cannot be switched to the original mode.	The default mode is **revertive**.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help enhance the reliability of a CR-LSP, you are recommended to set up a backup CR-LSP to protect traffic on the primary CR-LSP.

You can select the following CR-LSP backup modes as required:

- Hot-standby mode: A hot-standby backup CR-LSP is set up over a separate path immediately after the primary CR-LSP is set up. When the CR-LSP transmitting services fails, traffic can be immediately switched to the other CR-LSP. However, additional bandwidth is needed in hot-standby mode.
- Ordinary backup mode: The system attempts to set up an ordinary backup CR-LSP over a new explicit path, only when the primary CR-LSP fails. No additional bandwidth is needed in ordinary backup mode. In the case that the primary CR-LSP fails, this mode provides a traffic switchover slower than that of the hot-standby mode.
- Best-effort path mode: When both the primary and backup CR-LSP fail, the system establishes a best-effort path. There are few constraints on the establishment of best-effort path; therefore, it is easy to set up. In best-effort path mode, packet loss is decreased, and certain QoS requirements may not be guaranteed.

Prerequisites

A tunnel ID has been configured by running the **mpls te tunnel-id** command.

Precautions

After tunnel backup is enabled, the route recording function is automatically enabled, regardless of whether or not the **mpls te record-route** command is run.

Tunnel backup and the function configured by running the **mpls te resv-style ff** command are mutually exclusive.

The **mpls te backup ordinary** command and the **mpls te backup ordinary best-effort** command cannot be configured together; otherwise, the previous configuration overrides the later one.

After initiating the dynamic bandwidth function for a hot-standby CR-LSP, the hot-standby CR-LSP does not occupy any bandwidth when bearing no traffic. If the primary CR-LSP fails, the system re-establishes a hot-standby CR-LSP with the expected bandwidth according to the Make-Before-Break mechanism. The new hot-standby CR-LSP now transmits traffic. The system then deletes the hot-standby CR-LSP with the bandwidth being 0 bit/s.

Example

Enable hot standby for the current CR-LSP.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te backup hot-standby
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.88 mpls te backup frr-in-use

11.2.89 mpls te backup hot-standby overlap-path

11.2.88 mpls te backup frr-in-use

Function

The **mpls te backup frr-in-use** command allows a device to start a bypass CR-LSP if a primary CR-LSP becomes faulty (when the primary CR-LSP is in the FRR-in-use state), and to attempt to set up a backup CR-LSP while the system is restoring the primary CR-LSP.

The **undo mpls te backup frr-in-use** command restores the default configuration.

If the primary CR-LSP is faulty, the system starts the bypass CR-LSP and attempts to restore the primary CR-LSP, but does not set up a backup CR-LSP by default.

Format

mpls te backup frr-in-use

undo mpls te backup frr-in-use

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the primary CR-LSP is faulty, the system starts the bypass CR-LSP and tries to restore the primary CR-LSP the same time it sets up a backup CR-LSP.

Prerequisites

End-to-end protection in hot standby or ordinary backup mode has been enabled by running the **mpls te backup** { **hot-standby** | **ordinary** } command, and local protection of TE FRR has been enabled by running the **mpls te fast-reroute** command.

Precautions

If only the best-effort path is configured, rather than another end-to-end protection mode, the **mpls te backup frr-in-use** command cannot take effect.

After the **mpls te backup frr-in-use** command is run and if the primary CR-LSP is faulty:

 Copyright © Huawei Technologies Co., Ltd.

- If ordinary backup is configured, the system tries to set up a backup CR-LSP when the traffic is switched to the bypass CR-LSP and also attempts to restore the primary CR-LSP. If the backup CR-LSP is set up successfully and the primary CR-LSP is not restored, traffic is switched to the backup CR-LSP.
- If hot standby is configured and the backup CR-LSP is in the Up state, the traffic is switched to the bypass CR-LSP and then immediately to the backup CR-LSP while the system attempts to restore the primary CR-LSP. If the backup CR-LSP is in the Down state, the solution is the same as that in ordinary backup.

It is recommended that ordinary backup be configured together with the **mpls te backup frr-in-use** command. This saves bandwidth resources and improves tunnel security.

Example

Configure the system to set up a backup CR-LSP the same time it starts the bypass CR-LSP and tries to restore the primary CR-LSP after the primary CR-LSP is faulty.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te backup ordinary
[Huawei-Tunnel0/0/1] mpls te fast-reroute
[Huawei-Tunnel0/0/1] mpls te backup frr-in-use
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.87 mpls te backup
11.2.106 mpls te fast-reroute

11.2.89 mpls te backup hot-standby overlap-path

Function

The **mpls te backup hot-standby overlap-path** command enables the path partially overlapping function for hot-standby CR-LSPs.

The **undo mpls te backup hot-standby overlap-path** command disables the path overlapping function for hot-standby CR-LSPs.

By default, the path partially overlapping function is disabled for hot-standby CR-LSPs.

Format

mpls te backup hot-standby overlap-path

undo mpls te backup hot-standby overlap-path

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After the path overlapping function is configured, the path of a hot-standby CR-LSP can partially overlap the path of the primary CR-LSP when primary CR-LSP is not excluded by the system in path calculation.

Example

Enable the path overlapping function for hot-standby CR-LSPs.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te backup hot-standby
[Huawei-Tunnel0/0/1] mpls te backup hot-standby overlap-path
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.87 mpls te backup

11.2.90 mpls te bandwidth (interface view)

Function

The **mpls te bandwidth** command sets the BC bandwidth for a link.

The **undo mpls te bandwidth** command restores the default setting.

By default, no BC bandwidth is configured for a link.

Format

- In non-IETF mode:

  mpls te bandwidth { **bc0** *bc0-bw-value* | **bc1** *bc1-bw-value* } *

- In IETF mode:

  mpls te bandwidth { **bc0** *bc0-bw-value* | **bc1** *bc1-bw-value* | **bc2** *bc2-bw-value* | **bc3** *bc3-bw-value* | **bc4** *bc4-bw-value* | **bc5** *bc5-bw-value* | **bc6** *bc6-bw-value* | **bc7** *bc7-bw-value* } *

- To restore the default configuration, run the following command:

  undo mpls te bandwidth

Parameters

Parameter	Description	Value
bc0 *bc0-bw-value*	Specifies the bandwidth of BC0.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc1 *bc1-bw-value*	Specifies the bandwidth of BC1.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc2 *bc2-bw-value*	Specifies the bandwidth of BC2.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc3 *bc3-bw-value*	Specifies the bandwidth of BC3.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc4 *bc4-bw-value*	Specifies the bandwidth of BC4.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc5 *bc5-bw-value*	Specifies the bandwidth of BC5.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc6 *bc6-bw-value*	Specifies the bandwidth of BC6.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.
bc7 *bc7-bw-value*	Specifies the bandwidth of BC7.	The value is an integer that ranges from 1 to 4000000000, in kbit/s. The default value is 1.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In real-world situations, the bandwidth value is set on outbound interfaces along links of a TE tunnel that requires sufficient bandwidth.

The relationship between the maximum BC bandwidth and the maximum reservable link bandwidth (*max-reservable-bandwidth*) is as follows:

- In the RDM: *bc7-bw-value* ≤ *bc6-bw-value* ≤ *bc5-bw-value* ≤ *bc4-bw-value* ≤ *bc3-bw-value* ≤ *bc2-bw-value* ≤ *bc1-bw-value* ≤ *bc0-bw-value* ≤ *max-reservable-bandwidth*

 Copyright © Huawei Technologies Co., Ltd.

- In the MAM: *bc0-bw-value* + *bc1-bw-value* + *bc2-bw-value* + *bc3-bw-value* + *bc4-bw-value* + *bc5-bw-value* + *bc6-bw-value* + *bc7-bw-value* ≤ *max-reservable-bandwidth*
- In the Extended-MAM: The relationship is the same as that in the MAM.

Precautions

To change bandwidth BC values, reconfigure the **mpls te bandwidth** command. The last configured BC bandwidth value overrides the previous one.

One or multiple BC bandwidth values can be set in a single command in a random order.

NOTE

- The DS-TE non-IETF mode supports only BC0 and BC1; the DS-TE IETF mode supports BC0 to BC7.
- After the non-IETF mode is switched to the IETF mode, the bandwidth values of BC0 and BC1 are unchanged; after the IETF mode is switched to the non-IETF mode, the bandwidth values of other BCs are cleared except the bandwidth values of BC0 and BC1.

A BC bandwidth value can be changed only to a value greater than or equal to the set one. For example, the BC0 bandwidth of 10 Mbit/s can be changed to 10 or a larger value.

NOTE

To implement accurate bandwidth control, bandwidth of BCi (0≤i≤7) along a link must be larger than 125% of the total bandwidth of CTi (0≤i≤7) on this link.

Example

Set the maximum reservable bandwidth to 10000 kbit/s, the bandwidth of BC0 to 1000 kbit/s on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 10000
[Huawei-GigabitEthernet1/0/0] mpls te bandwidth bc0 1000
```

11.2.91 mpls te bandwidth (tunnel interface view)

Function

The **mpls te bandwidth** command sets the bandwidth of an MPLS TE tunnel.

The **undo mpls te bandwidth** command restores the default settings.

By default, the bandwidth of an MPLS TE tunnel is not set.

Format

- In non-IETF mode:

  mpls te bandwidth { **ct0** *ct0-bw-value* | **ct1** *ct1-bw-value* }

  undo mpls te bandwidth { **all** | **ct0** [*ct0-bw-value*] | **ct1** [*ct1-bw-value*] }

- In IETF mode:

  mpls te bandwidth { **ct0** *ct0-bw-value* | **ct1** *ct1-bw-value* | **ct2** *ct2-bw-value* | **ct3** *ct3-bw-value* | **ct4** *ct4-bw-value* | **ct5** *ct5-bw-value* | **ct6** *ct6-bw-value* | **ct7** *ct7-bw-value* } *

  undo mpls te bandwidth { **all** | { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } * }

  undo mpls te bandwidth { **all** | { **ct0** *ct0-bw-value* | **ct1** *ct1-bw-value* | **ct2** *ct2-bw-value* | **ct3** *ct3-bw-value* | **ct4** *ct4-bw-value* | **ct5** *ct5-bw-value* | **ct6** *ct6-bw-value* | **ct7** *ct7-bw-value* } * }

Parameters

Parameter	Description	Value
ct0 *ct0-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT0.	*ct0-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct1 *ct1-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT1.	*ct1-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct2*ct2-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT2.	*ct2-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct3 *ct3-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT3.	*ct3-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct4 *ct4-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT4.	*ct4-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct5 *ct5-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT5.	*ct5-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct6 *ct6-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT6.	*ct6-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
ct7 *ct7-bw-value*	Specifies the bandwidth reserved for a TE tunnel of CT7.	*ct7-bw-value* is an integer that ranges from 1 to 4000000000, in kbit/s.
all	Deletes bandwidth for all CTs.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CT bandwidth can be set in either non-IETF or IETF mode. The non-IETF mode only supports the CT0 and CT1 configuration; the IETF mode supports one or multiple CTs.

Precautions

A static TE tunnel does not support the multi-CT configuration.

On a single TE tunnel interface, the multi-CT bandwidth cannot be configured with the following features:

- CSPF tie-breaking
- Bypass tunnel attributes

The **undo mpls te bandwidth** command is used to restore the default settings of all CTs or specified CTs:

- **undo mpls te bandwidth all**: deletes all configured bandwidth.
- **undo mpls te bandwidth** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } *: deletes the bandwidth of one or more CTs configured on the current TE tunnel.

NOTE

After modification, the TE-class mapping table contains items CT4 to CT7.

Example

Set the bandwidth required by Tunnel0/0/1. The bandwidth of CT0 is 2000 kbit/s.

```
<Huawei> system-view
[Huawei] mpls lsr-id 10.1.1.1
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] quit
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 10.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te bandwidth ct0 2000
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.82 mpls te

11.2.92 mpls te bandwidth change thresholds

Function

The **mpls te bandwidth change thresholds** command sets the percentage threshold of the physical link bandwidth used by an MPLS TE tunnel for flooding link information.

The **undo mpls te bandwidth change thresholds** command restores the default settings.

 Copyright © Huawei Technologies Co., Ltd.

If the ratio of the reserved (or released) bandwidth for a tunnel to the remaining bandwidth in a Traffic Engineering Database (TEDB) is equal to or greater than 10%, an IGP floods link information and CSPF updates the TEDB by default.

Format

mpls te bandwidth change thresholds { **down** | **up** } *percent*

undo mpls te bandwidth change thresholds { **down** | **up** }

Parameters

Parameter	Description	Value
down	Indicates the flooding threshold of the bandwidth used by an MPLS TE tunnel. If the ratio of the bandwidth used by an MPLS TE tunnel to the remaining link bandwidth in a TEDB is equal to or greater than the threshold, an IGP floods link information and CSPF updates the TEDB.	-
up	Indicates the flooding threshold of the bandwidth released by an MPLS TE tunnel. If the ratio of the bandwidth released by an MPLS TE tunnel to the remaining link bandwidth in a TEDB is equal to or greater than the threshold, an IGP floods link information and CSPF updates the TEDB.	-
percent	Specifies the threshold as a percentage.	The value is an integer that ranges from 0 to 100. The default value is 10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When the bandwidth changes slightly, flooding the bandwidth wastes network resources. For example, the bandwidth of a link is 100 Mbit/s. During the creation of 100 TE tunnels each with the bandwidth being 1 Mbit/s, the bandwidth of all TE tunnels needs to be flooded 100 times. If the flooding threshold is set to 10%, the first nine tunnels are created without flooding. When the tenth tunnel is created, the 10 Mbit/s bandwidth that is used by the preceding 10 tunnels is flooded. The tunnels from the eleventh tunnel to the eighteenth are created without flooding. When the nineteenth tunnel is created, the bandwidth is flooded, and so on.

 Copyright © Huawei Technologies Co., Ltd.

Example

On GE1/0/0, when the link bandwidth reserved for the MPLS TE tunnel exceeds 10% of the overall bandwidth or the bandwidth released by the MPLS TE tunnel exceeds 25% of the overall bandwidth, the link information is flooded.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te bandwidth change thresholds up 25
[Huawei-GigabitEthernet1/0/0] mpls te bandwidth change thresholds down 10
```

11.2.93 mpls te bandwidth max-reservable-bandwidth

Function

The **mpls te bandwidth max-reservable-bandwidth** command sets or modifies the maximum reservable bandwidth of a link.

The **undo mpls te bandwidth max-reservable-bandwidth** command restores the default configuration.

The maximum reservable bandwidth of a link is not configured by default.

Format

mpls te bandwidth max-reservable-bandwidth *bw-value*

undo mpls te bandwidth max-reservable-bandwidth

Parameters

Parameter	Description	Value
bw-value	Specifies the maximum reservable bandwidth of a link.	The value is an integer that ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

In practical applications, the **mpls te bandwidth max-reservable-bandwidth** command can be configured for a TE tunnel on an outgoing interface of the link through which the tunnel passes.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum reservable bandwidth of the link to 10000 kbit/s on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te bandwidth max-reservable-bandwidth 10000
```

11.2.94 mpls te bfd

Function

The **mpls te bfd** command sets the parameters of a BFD session for TE.

The **undo mpls te bfd** command restores the default configuration.

By default, no parameters of a BFD session for TE is set.

Format

mpls te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

undo mpls te bfd { **min-tx-interval** | **min-rx-interval** | **detect-multiplier** } *

undo mpls te bfd { **min-tx-interval** *tx-interval* | **min-rx-interval** *rx-interval* | **detect-multiplier** *multiplier* } *

Parameters

Parameter	Description	Value
min-tx-interval *tx-interval*	Specifies the interval at which BFD packets are sent.	The value ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
min-rx-interval *rx-interval*	Specifies the interval at which BFD packets are received.	The value ranges from 10 to 2000, in milliseconds. By default, the value is 1000.
detect-multiplier *multiplier*	Specifies the local detection multiplier value of a BFD session.	An integer ranging from 3 to 50. The value is 3 by default.

Views

MPLS view, tunnel interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

If **min-tx-interval** *tx-interval* configured on the local end is different from **min-rx-interval** *rx-interval* configured on the peer, the larger value is used as the actual session parameter.

The used **detect-multiplier** *multiplier* is the value set on the peer.

If the **mpls te bfd** command is configured in the MPLS view, it takes effect globally. If the command is configured in the tunnel interface view, it only takes effect on the current tunnel interface, and the parameters of the BFD session for TE set in the MPLS view are overridden.

Example

Set the parameters of the BFD session.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te bfd min-tx-interval 200 detect-multiplier 5
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.95 mpls te bfd block
11.2.96 mpls te bfd enable

11.2.95 mpls te bfd block

Function

The **mpls te bfd block** command blocks the BFD capability on a specified tunnel interface of a CR-LSP.

The **undo mpls te bfd block** command restores the default configuration.

The BFD capability is not blocked on a tunnel interface by default.

Format

mpls te bfd block

undo mpls te bfd block

Parameters

None.

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te bfd block** command and the **mpls te bfd enable** command are mutually exclusive.

The differences between the **mpls te bfd block** command and the **undo mpls te bfd enable** command in the tunnel interface view are as follows:

- When the **undo mpls te bfd enable** command is run on a tunnel interface, the interface can still obtain the BFD for TE capability after you configure the **mpls te bfd enable** command in the MPLS view.
- When the **mpls te bfd block** command is run on a tunnel interface, the interface cannot obtain the BFD for TE capability even if the **mpls te bfd enable** command is run in the MPLS view.

NOTE

To enable the BFD for TE capability on a majority of interfaces, you can run the **mpls te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for TE. Then, you can run the **mpls te bfd enable** command in the MPLS view to enable the BFD for TE capability on the other interfaces.

To enable BFD for TE capability on a few interfaces, you can run the **mpls te bfd enable** command on these interfaces. After, you can run the **undo mpls te bfd enable** command or the **mpls te bfd block** command to disable BFD for TE from these interfaces.

Example

Block the BFD capability on Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te bfd block
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.96 mpls te bfd enable

11.2.96 mpls te bfd enable

Function

The **mpls te bfd enable** command enables BFD for TE.

The **undo mpls te bfd enable** command restores the default configuration.

BFD for TE is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls te bfd enable

undo mpls te bfd enable

Parameters

None.

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If the **mpls te bfd enable** command is configured in the MPLS view, all TE tunnel interfaces are enabled with BFD for TE, except those configured with the **mpls te bfd block** command, blocking BFD for TE.

If this command is configured in the tunnel interface view, it only takes effect on the single tunnel interface.

The differences between the **undo mpls te bfd enable** command and the **mpls te bfd block** command configured in the tunnel interface view are as follows:

- When the **undo mpls te bfd enable** command is run on a tunnel interface, the interface can still obtain the BFD for TE capability after you configure the **mpls te bfd enable** command in the MPLS view.
- When the **mpls te bfd block** command is run on a tunnel interface, the interface cannot obtain the BFD for TE capability even if the **mpls te bfd enable** command is run in the MPLS view.

NOTE

- To enable the BFD for TE capability on a majority of interfaces, you can run the **mpls te bfd block** command on a minority of interfaces that do not need to be enabled with BFD for TE. Then, you can run the **mpls te bfd enable** command in the MPLS view to enable the BFD for TE capability for the other interfaces.
- To enable BFD for TE capability on a few interfaces, you can run the **mpls te bfd enable** command on these interfaces. After, you can run the **undo mpls te bfd enable** command or the **mpls te bfd block** command to disable BFD for TE from these interfaces.

Example

Enable BFD for TE globally.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls te bfd enable
```

Enable BFD for TE on the tunnel interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te bfd enable
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.95 mpls te bfd block

11.2.97 mpls te bypass-attributes

Function

The **mpls te bypass-attributes** command configures the bypass tunnel attributes in the MPLS TE Auto FRR feature.

The **undo mpls te bypass-attributes** command restores the default settings.

By default, no bypass tunnel attributes in the MPLS TE Auto FRR feature is configured.

Format

mpls te bypass-attributes [**bandwidth** *bandwidth*] [**priority** *setup-priority* [*hold-priority*]]

undo mpls te bypass-attributes

Parameters

Parameter	Description	Value
bandwidth *bandwidth*	Specifies the bandwidth.	The value is an integer that ranges from 1 to 4000000000, in kbit/s.
setup-priority	Specifies the setup priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. The value is 7 by default.
hold-priority	Specifies the holding priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. The value is 7 by default.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

Before running the **mpls te bypass-attributes** command, you must run the **mpls te fast-reroute bandwidth** command to enable FRR function. The bandwidth of a bypass tunnel cannot be greater than that of the primary tunnel.

Precautions

The setup priority of a bypass tunnel cannot be higher than the holding priority. Both cannot be higher than the priorities of the primary tunnel.

On the same TE tunnel interface, the **mpls te bypass-attributes** command cannot be configured together with the **mpls te bandwidth (tunnel interface view)** command.

Example

Set the bandwidth of the bypass tunnel to 2048 kbit/s, the setup priority to 3, and the holding priority to 3.

```
<Huawei> system-view
[Huawei] mpls lsr-id 1.1.1.1
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] quit
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te bandwidth ct0 10000
[Huawei-Tunnel0/0/1] mpls te priority 3 3
[Huawei-Tunnel0/0/1] mpls te fast-reroute bandwidth
[Huawei-Tunnel0/0/1] mpls te bypass-attributes bandwidth 2048 priority 3 3
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.106 mpls te fast-reroute

11.2.37 display mpls te tunnel-interface

11.2.98 mpls te bypass-tunnel

Function

The **mpls te bypass-tunnel** command specifies the bypass tunnel for MPLS TE Auto FRR.

The **undo mpls te bypass-tunnel** command deletes the bypass tunnel configuration.

By default, no bypass tunnel for MPLS TE Auto FRR is specified.

Format

mpls te bypass-tunnel

undo mpls te bypass-tunnel

Parameters

None.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The total bandwidth of LSPs protected by the bypass tunnel is not more than the bandwidth of the primary tunnel. When multiple bypass tunnels exist, the system selects a single bypass tunnel through the best-fit algorithm.

If global Srefresh needs to be enabled on the bypass PLR and MP node, configure the MPLS LSR ID of the destination peer FRR MP node as the destination address of the bypass tunnel.

NOTE

The **mpls te bypass-tunnel** command cannot be configured simultaneously with the following commands on the same tunnel interface:

- **mpls te fast-reroute**
- **mpls te backup**

Example

Configure the bypass tunnel on Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te bypass-tunnel
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.106 mpls te fast-reroute

11.2.87 mpls te backup

11.2.99 mpls te commit

Function

The **mpls te commit** command commits the tunnel configurations to the system for processing.

Format

mpls te commit

Parameters

None.

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The configurations of an MPLS TE tunnel can only take effect after the **mpls te commit** command is run. The destination and tunnel ID must be configured; otherwise, the commitment fails, and you need to configure both of them and then commit the configuration again. If the MPLS TE configuration changes, you must run the **mpls te commit** command to validate the modification.

NOTE

Each time the MPLS TE tunnel configuration is changed, the **mpls te commit** command must be run to make the modification take effect. If this command is not run, the changed configuration can be saved in the configuration file but cannot take effect.

Example

Configure an MPLS TE tunnel and then commit the configuration.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.9
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.133 mpls te tunnel-id

11.2.100 mpls te cspf

Function

The **mpls te cspf** command enables CSPF.

The **undo mpls te cspf** command disables CSPF.

CSPF is disabled by default.

Format

mpls te cspf

undo mpls te cspf

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

You must enable MPLS TE in the MPLS view before enabling CSPF.

CSPF provides a mechanism for selecting a path in an MPLS domain. You must enable CSPF before configuring CSPF functions.

Example

Enable CSPF.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls te cspf
```

11.2.101 mpls te cspf disable

Function

The **mpls te cspf disable** command disables CSPF calculation when an LSP is being established in a TE tunnel.

The **undo mpls te cspf disable** command enables CSPF calculation when an LSP is being established in a TE tunnel.

By default, CSPF calculation is enabled when an LSP is being established in a TE tunnel.

Format

mpls te cspf disable

undo mpls te cspf disable

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After CSPF is enabled globally, CSPF calculation is triggered each time an LSP is being established in a TE tunnel. In the inter-AS VPN-OptionC scenario, no IGP is configured between two ASs, causing the TEDB to fail to be generated. As a result, CSPF calculation fails to be performed, and inter-area TE tunnels fail to be set up. Run the **mpls te cspf disable** command on the configured TE tunnel interface to disable CSPF calculation in the TE tunnel, and set up inter-area TE tunnels using direct routes or static routes.

Precautions

After the **mpls te cspf disable** command is run, CR-LSP selection functions, such as hop limit, CSPF tie-breaking, and SRLG, will become invalid.

Example

Disable CSPF calculation when an LSP is being established in a TE tunnel.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te cspf disable
[Huawei-Tunnel0/0/1] mpls te commit
```

11.2.102 mpls te cspf preferred-igp

Function

The **mpls te cspf preferred-igp** command specifies a preferred IGP for the CSPF calculation.

The **undo mpls te cspf preferred-igp** command restores the default settings.

The TEDB generated by OSPF is preferred by default.

Format

mpls te cspf preferred-igp { **isis** [*isis-process-id* [**level-1** | **level-2**]] | **ospf** [*ospf-process-id* [**area** { *area-id-1* | *area-id-2* }]] }

undo mpls te cspf preferred-igp

Parameters

Parameter	Description	Value
isis	Indicates that the TEDB generated by IS-IS is preferred.	-
isis-process-id	Specifies the process ID.	The value is an integer that ranges from 1 to 65535.

Parameter	Description	Value
level-1	Indicates that the TEDB generated by a Level-1 IS-IS device is preferred.	-
level-2	Indicates that the TEDB generated by a Level-2 IS-IS device is preferred.	-
ospf	Indicates that the TEDB generated by OSPF is preferred.	-
ospf-process-id	Specifies the ID of an OSPF process.	The value is an integer that ranges from 1 to 65535.
area *area-id-1*	Specifies a preferred OSPF area configured in number format.	The value is an integer that ranges from 0 to 4294967295.
area *area-id-2*	Specifies a preferred OSPF area configured in IP address format.	The value is in dotted decimal notation.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

When selecting a path, CSPF prefers the TEDB generated by OSPF to calculate a CR-LSP by default. When the OSPF TEDB can be used to calculate a path, the IS-IS TEDB is not used. If the calculation based on the OSPF TEDB fails, recalculation based on the IS-IS TEDB is performed.

You can run the **mpls te cspf preferred-igp** command to configure CSPF to prefer the TEDB generated by IS-IS when calculating a CR-LSR. In this case, the OSPF TEDB is only used to calculate a path when the path calculation based on the IS-IS TEDB fails.

Example

Configure CSPF to prefer the TEDB generated by OSPF when calculating a CR-LSP.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te cspf
[Huawei-mpls] mpls te cspf preferred-igp ospf
```

Related Topics

11.2.100 mpls te cspf

11.2.103 mpls te cspf timer failed-link

Function

The **mpls te cspf timer failed-link** command sets the timeout period of a failed-link timer.

The **undo mpls te cspf timer failed-link** command restores the default setting.

By default, the timeout period of the failed-link timer is 10 seconds.

Format

mpls te cspf timer failed-link *interval*

undo mpls te cspf timer failed-link

Parameters

Parameter	Description	Value
interval	Specifies the timeout period of a failed-link timer.	The value is an integer ranges from 1 to 300, in seconds. The default value is 10.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A failed-link timer starts when a link goes Down.

- If an IGP deletes or modifies the link before the timer expires, CSPF is informed of the change. Then CSPF updates the link in the Traffic Engineering DataBase (TEDB) and terminates the timer.
- If IGP does not delete the link after the timer expires, the link goes Up.

Prerequisites

The CSPF function has been enabled by running the **mpls te cspf** command.

Example

Set the timeout period of the failed-link timer to 50 seconds.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te cspf
[Huawei-mpls] mpls te cspf timer failed-link 50
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

11.2.100 mpls te cspf

11.2.104 mpls te ds-te bcm

Function

The **mpls te ds-te bcm** command sets a DS-TE Bandwidth Constraints model.

The **undo mpls te ds-te bcm** command restores the default configuration.

By default, the DS-TE Bandwidth Constraints model is RDM.

Format

- In non-IETF mode:
  mpls te ds-te bcm { **mam** | **rdm** }
  undo mpls te ds-te bcm
- In IETF mode:
  mpls te ds-te bcm { **extend-mam** | **mam** | **rdm** }
  undo mpls te ds-te bcm

Parameters

Parameter	Description	Value
extend-mam	Indicates that the DS-TE Bandwidth Constraints model is the extended-MAM.	-
mam	Indicates that the DS-TE Bandwidth Constraints model is the MAM.	-
rdm	Indicates that the DS-TE Bandwidth Constraints model is the RDM.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If preemption for CT bandwidth is enabled, you are recommended to use the RDM, which effectively uses bandwidth. If preemption for CT bandwidth is disabled on a network, you are recommended to use the MAM or the extended-MAM.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The DS-TE non-IETF mode does not support the extended-MAM.

When the non-IETF mode is switched to the IETF mode, the Bandwidth Constraints model remains unchanged. When the IETF mode is switched to the non-IETF mode, the system changes the extended-MAM to the MAM if the Bandwidth Constraints model is extended-MAM. Other models will remain unchanged.

Example

Set the DS-TE Bandwidth Constraints model of the local device to extended-MAM.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te ds-te mode ietf
[Huawei-mpls] mpls te ds-te bcm extend-mam
```

Related Topics

11.2.105 mpls te ds-te mode

11.2.105 mpls te ds-te mode

Function

The **mpls te ds-te mode** command sets the DS-TE mode.

The **undo mpls te ds-te mode** command restores the default configuration.

The non-IETF mode is used by default.

Format

mpls te ds-te mode { **ietf** | **non-ietf** }

undo mpls te ds-te mode

Parameters

Parameter	Description	Value
ietf	Indicates the standard DS-TE mode supported by the system, or IETF mode.	-
non-ietf	Indicates the non-standard DS-TE mode supported by the system, or non-IETF mode.	-

Views

MPLS view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The IETF mode and the non-IETF mode can be switched to each other on the device. Take care when switching the DS-TE modes. Before and after the switching, the TE-class mapping table and the Bandwidth Constraints model may have changed and certain LSPs may have been deleted. When devices of difference vendors are connected, an abnormality may occur.

Example

Set the DS-TE mode of the local device to the standard DS-TE mode.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te ds-te mode ietf
```

11.2.106 mpls te fast-reroute

Function

The **mpls te fast-reroute** command enables FRR.

The **undo mpls te fast-reroute** command disables FRR.

By default, FRR is disabled.

Format

mpls te fast-reroute [**bandwidth**]

undo mpls te fast-reroute

Parameters

Parameter	Description	Value
bandwidth	Indicates that bandwidth protection is needed.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

When FRR is enabled on a tunnel interface, the record route flag is automatically set as "record reroute with label", irrespective of the configuration of the **mpls te record-route label** command.

You must disable FRR If run the **mpls te record-route** or **undo mpls te record-route** command.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The **mpls te fast-reroute** command and the **mpls te resv-style ff** command cannot be configured together.
- The **mpls te fast-reroute** command and the **mpls te bypass-tunnel** command cannot be configured on the same tunnel interface.
- The **mpls te fast-reroute** command and the **mpls te protected-interface** command cannot be configured on the same tunnel interface.

Example

Enable FRR on Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] mpls te fast-reroute
[Huawei-Tunnel0/0/1] mpls te commit
```

Enable FRR on Tunnel0/0/1 and allow the bandwidth protection.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te fast-reroute bandwidth
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.122 mpls te resv-style

11.2.98 mpls te bypass-tunnel

11.2.119 mpls te record-route

11.2.118 mpls te protected-interface

11.2.107 mpls te hop-limit

Function

The **mpls te hop-limit** command limits the maximum number of hops of a CR-LSP.

The **undo mpls te hop-limit** command restores the default setting.

By default, the maximum number of hops of a CR-LSP is 32.

Format

mpls te hop-limit *hop-limit-value* [**best-effort** | **secondary**]

undo mpls te hop-limit [**best-effort** | **secondary**]

undo mpls te hop-limit *hop-limit-value* { **secondary** | **best-effort** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hop-limit-value	Specifies the value of the hop limit.	The value is an integer that ranges from 1 to 32. The default value is 32.
best-effort	Indicates the hop limit of a best-effort path.	-
secondary	Indicates the hop limit of a backup CR-LSP.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After a CR-LSP is configured with a hop limit, the hop limit acts as one of routing conditions such as the link bandwidth and affinity property when the CR-LSP is created. After the hop limit is set, the number of hops of a CR-LSP cannot exceed this limit.

Example

Set the maximum number of hops of the primary CR-LSP, bypass CR-LSP, and best-effort path in hot-standby to 10.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te hop-limit 10
[Huawei-Tunnel0/0/1] mpls te hop-limit 10 secondary
[Huawei-Tunnel0/0/1] mpls te hop-limit 10 best-effort
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.100 mpls te cspf

11.2.108 mpls te igp advertise

Function

The **mpls te igp advertise** command configures forwarding adjacency to take an MPLS TE tunnel as a virtual link and advertise the virtual link to an IGP network.

The **undo mpls te igp advertise** command restores the default configuration.

By default, forwarding adjacency to take an MPLS TE tunnel as a virtual link and advertise the virtual link to an IGP network is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls te igp advertise [**hold-time** *interval*]

undo mpls te igp advertise

Parameters

Parameter	Description	Value
hold-time *interval*	Specifies the interval between the time when a TE tunnel goes Down and when the network is notified of the change.	The value is an integer that ranges from 0 to 4294967295 in milliseconds. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te igp advertise** command and the **mpls te igp shortcut** command cannot be configured simultaneously.

Example

Configure the forwarding adjacency and use the default hold time.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te igp advertise
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.110 mpls te igp shortcut

11.2.109 mpls te igp metric

Function

The **mpls te igp metric** command specifies the MPLS TE tunnel metric for the SPF calculation in IGP shortcut or forwarding adjacency mode.

The **undo mpls te igp metric** command restores the default settings.

The TE tunnel metric is equal to the IGP metric of the TE tunnel by default.

Format

mpls te igp metric { **absolute** *absolute-value* | **relative** *relative-value* }

 Copyright © Huawei Technologies Co., Ltd.

undo mpls te igp metric

Parameters

Parameter	Description	Value
absolute *absolute-value*	Specifies the absolute metric mode.	The value is an integer that ranges from 1 to 65535.
relative *relative-value*	Specifies the relative metric mode, indicating the difference compared with the IGP metric.	The value is an integer that ranges from -10 to 10. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

In IGP shortcut or SPF calculation for forwarding adjacency scenarios, to set a metric for an MPLS TE tunnel, run the **mpls te igp metric** command in the tunnel interface view. The TE tunnel metric affects IGP path selection.

Example

Set the MPLS TE tunnel metric to the IGP metric minus 1 in the SPF calculation.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te igp metric relative -1
[Huawei-Tunnel0/0/1] mpls te commit
```

11.2.110 mpls te igp shortcut

Function

The **mpls te igp shortcut** command configures an IGP to use MPLS TE tunnels in the Up state for performing the enhanced SPF calculation.

The **undo mpls te igp shortcut** command restores the default configuration.

By default, an IGP does not use MPLS TE tunnels for performing the enhanced SPF calculation.

Format

mpls te igp shortcut [**isis** | **ospf**]

undo mpls te igp shortcut

Parameters

Parameter	Description	Value
isis	Indicates the IS-IS protocol.	-
ospf	Indicates the OSPF protocol.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te igp shortcut** command and the **mpls te igp advertise** command cannot be configured simultaneously.

Example

Configure OSPF or IS-IS to use Tunnel 0/0/1 in the enhanced SPF calculation if this tunnel is Up.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te igp shortcut
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.108 mpls te igp advertise

11.2.111 mpls te link administrative group

Function

The **mpls te link administrative group** command sets the value of the administrative-group attribute for an interface.

The **undo mpls te link administrative group** command restores the default setting.

The default administrative-group attribute is 0x0.

Format

mpls te link administrative group *value*

undo mpls te link administrative group

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
value	Specifies the link attributes compared with affinity bits during the selection of a path.	The value is in hexadecimal notation and is of 32 bits with each bit representing an attribute. The value ranges from 0x0 to 0xFFFFFFFF.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

After being advertised globally, interface attributes can work as a standard for the ingress of a tunnel to select a path.

The modification on the administrative-group attributes takes effect only on the LSPs created after the modification and does not affect the established LSPs.

The **mpls te link administrative group** command can be run on the outgoing interface of the link through which a TE tunnel passes.

Example

Set the administrative-group attribute to 0x0101 on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te link administrative group 101
```

Related Topics

11.2.83 mpls te affinity property

11.2.112 mpls te loop-detection

Function

The **mpls te loop-detection** command enables loop detection function while a tunnel is being set up.

The **undo mpls te loop-detection** command disables this function.

Loop detection function is disabled by default.

Format

mpls te loop-detection

undo mpls te loop-detection

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable loop detection when an MPLS TE tunnel is being set up.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te loop-detection
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.82 mpls te

11.2.113 mpls te metric

Function

The **mpls te metric** command configures the TE metric value of a link.

The **undo mpls te metric** command restores the default configuration.

The IGP metric value of a link is used as the TE metric value by default.

Format

mpls te metric *value*

undo mpls te metric

Parameters

Parameter	Description	Value
metric *value*	Specifies the TE metric of a link.	An integer ranging from 1 to 16777215.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

If the IGP is OSPF and the current device is a stub router, the **mpls te metric** command does not take effect.

Example

Set the TE metric of the link to 20 on interface GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te metric 20
```

Related Topics

11.2.115 mpls te path metric-type

11.2.114 mpls te path explicit-path

Function

The **mpls te path explicit-path** command configures an explicit path for a tunnel.

The **undo mpls te path** command deletes a configured explicit path.

By default, no explicit path for a tunnel is configured.

Format

mpls te path explicit-path *path-name* [**secondary**]

undo mpls te path [**secondary**]

undo mpls te path explicit-path *path-name* **secondary**

Parameters

Parameter	Description	Value
path-name	Specifies the name of the explicit path for a tunnel.	The value is an existing explicit path name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
secondary	Indicates that the explicit path is configured for a backup tunnel. The parameter is applied only to configuring a backup CR-LSP using the **mpls te backup** command.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te path explicit-path** command can be run successfully only after an explicit path is set up by running the **explicit-path** command in the system view, and the nodes on the path are specified.

Example

Apply the explicit path named path1 to Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] explicit-path path1
[Huawei-explicit-path-path1] next hop 2.2.2.9
[Huawei-explicit-path-path1] quit
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te path explicit-path path1
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.50 explicit-path

11.2.115 mpls te path metric-type

Function

The **mpls te path metric-type** command specifies a link metric type used to select a path for a tunnel without any metric type.

The **undo mpls te path metric-type** command restores the default settings.

The TE metric is used to select a path for a tunnel by default.

Format

mpls te path metric-type { **igp** | **te** }

undo mpls te path metric-type

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
igp	Indicates that the IGP metric is used.	-
te	Indicates that the TE metric is used.	-

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

If the **mpls te path metric-type** command is not configured in the tunnel interface view, the metric type set in the MPLS view is used. Otherwise, the metric type set in the tunnel interface view will be used.

Example

Adopt the IGP metric that is used to select a path for the tunnel that is not configured with any metric type.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te path metric-type igp
```

Adopt the TE metric that is used to select a path for Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te path metric-type te
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.113 mpls te metric

11.2.116 mpls te path-selection overload

Function

The **mpls te path-selection overload** command associates CR-LSP establishment with the IS-IS overload setting. This association allows CSPF to calculate paths excluding overloaded IS-IS nodes.

The **undo mpls te path-selection** command restores the default configuration.

By default, CR-LSP establishment is not associated with the IS-IS overload setting.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls te path-selection overload

undo mpls te path-selection

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrator can run the **set-overload** command to mark a node overloaded if the node is transmitting a large number of services or its CPU is overburdened. If there are overloaded nodes on an MPLS TE network, associate CR-LSP establishment with the IS-IS overload setting to ensure that CR-LSPs are established over paths excluding overloaded nodes. This configuration prevents overloaded nodes from being further burdened and improves CR-LSP reliability.

Prerequisites

The route record has been enabled using the **mpls te record-route** command.

Precautions

The **mpls te path-selection overload** command has the following influences on the CR-LSP establishment:

- CSPF recalculates paths excluding overloaded nodes for established CR-LSPs.

  NOTE

  Traffic travels through an existing CR-LSP before a new CR-LSP is established. After the new CR-LSP is established, traffic switches to the new CR-LSP and the original CR-LSP is deleted. This traffic switchover is performed based on the Make-Before-Break mechanism. Traffic is not dropped during the switchover.

- CSPF calculates paths excluding overloaded nodes for new CR-LSPs.

This command does not take effect on bypass tunnels.

If the ingress or egress is marked overloaded, the **mpls te path-selection overload** command does not take effect. The established CR-LSPs associated with the ingress or egress will not be reestablished and new CR-LSPs associated with the ingress or egress will also not be established.

Example

Associate CR-LSP establishment with the IS-IS overload setting.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls te path-selection overload
```

Related Topics

11.2.82 mpls te

11.2.117 mpls te priority

Function

The **mpls te priority** command configures the setup priority and holding priority for an MPLS TE tunnel.

The **undo mpls te priority** command restores the default settings.

The default setup and holding priority for an MPLS TE tunnel are both 7.

Format

mpls te priority *setup-priority* [*hold-priority*]

undo mpls te priority

Parameters

Parameter	Description	Value
setup-priority	Specifies the setup priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority.
hold-priority	Specifies the holding priority.	The value is an integer that ranges from 0 to 7. The smaller the value, the higher the priority. Its value is the same as the setup priority by default.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If bandwidth resources on a link cannot satisfy the requirements for establishing all CR-LSPs, you can specify the setup and holding priorities for certain CR-LSPs. In this manner, the CR-LSPs with higher priorities can be established by preempting bandwidth resources of CR-LSPs with lower priorities before transmitting certain user services.

 Copyright © Huawei Technologies Co., Ltd.

Priorities of a CR-LSP consist of the setup priority and holding priority, representing the preemption relationship between a CR-LSP to be established and an established CR-LSP. If the setup priority of a CR-LSP to be established is higher than the holding priority of an established CR-LSP, the CR-LSP to be established can preempt the bandwidth resources of the established one.

The default setup and holding priorities of CR-LSPs are 7, the lowest priority value. Default priorities take effect on all CR-LSPs if no priorities are specified. These CR-LSPs with the default priorities are at the risk of being preempted by those with higher priorities.

Precautions

During the planning of a network, it is recommended that the setup and holding priorities of all CR-LSPs be strictly planned. To preferentially transmit services over a CR-LSP, you can set the higher setup and holding priorities for the CR-LSP, preventing unwanted bandwidth preemption. The same setup and holding priorities are set for CR-LSPs which are transmitting services with the same priority, also preventing bandwidth preemption.

In addition, on one TE tunnel, its setup priority must be less than or equal to its holding priority. This ensures that CR-LSPs in the tunnel can be successfully set up, and prevents CR-LSP flapping caused by bandwidth preemption between CR-LSPs.

NOTICE

After the priorities of an existing CR-LSP have been changed, the existing CR-LSP will be deleted and a new one will be established. Therefore, back up CR-LSPs with lower priorities before setting higher priorities for a certain CR-LSP.

Example

Set the setup priority and the holding priority to 1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te priority 1
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.82 mpls te

11.2.118 mpls te protected-interface

Function

The **mpls te protected-interface** command specifies an interface to be protected by a bypass tunnel.

The **undo mpls te protected-interface** command delete an interface protected by a bypass tunnel.

By default, no interface to be protected by a bypass tunnel is specified.

Format

mpls te protected-interface *interface-type interface-number*

undo mpls te protected-interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface to be protected. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te protected-interface** command must be configured together with the **mpls te bypass-tunnel** command on the same tunnel interface. Otherwise, the configured **mpls te protected-interface** command cannot take effect.

Currently, a bypass tunnel can protect up to six interfaces that must be enabled with MPLS TE.

NOTE

If a tunnel interface is configured with the **mpls te protected-interface** command, it cannot be configured with the **mpls te backup** or **mpls te fast-reroute** command.

Example

Use Tunnel 0/0/1 as a bypass tunnel of GE 1/0/0.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te protected-interface gigabitethernet 1/0/0
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.98 mpls te bypass-tunnel

11.2.87 mpls te backup

11.2.106 mpls te fast-reroute

 Copyright © Huawei Technologies Co., Ltd.

11.2.119 mpls te record-route

Function

The **mpls te record-route** command enables the route and label recording function during tunnel establishment.

The **undo mpls te record-route** command disables the route and label recording function during tunnel establishment.

By default, the route and label recording function is disabled during tunnel establishment.

Format

mpls te record-route [**label**]

undo mpls te record-route

Parameters

Parameter	Description	Value
label	Indicates that a label is also recorded during route recording.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an MPLS TE tunnel is not established over an explicit path, the system does not record detailed path information. In this case, to view detailed path information about the tunnel, run this command on a tunnel interface. After the configuration, RROs are carried in Path and Resv messages and record the IP address of each hop along the tunnel. In addition, the keyword **label** can be configured to record the label of each hop along the tunnel.

Precautions

After the **mpls te record-route** command is configured and the MPLS TE tunnel is established, the **display mpls te tunnel path** command can be run to display detailed path information about the tunnel.

Do not run the **mpls te record-route** command on a large-scale network. On such a network, a large number of hops exist along a tunnel. Running this command allows the Path and Resv messages to carry RROs that record the IP address of each hop along the tunnel. As a result, the Path or Resv message will be oversized, lowering the system performance.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

After the **mpls te fast-reroute**, **mpls te backup**, or **mpls te bypass-tunnel** command has been configured on a tunnel interface, the route record function is automatically enabled.

Example

Enable the route and label recording function during tunnel establishment.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te record-route label
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.43 display mpls te tunnel path

11.2.116 mpls te path-selection overload

11.2.120 mpls te reoptimization (user view)

Function

The **mpls te reoptimization** command immediately triggers re-optimization for an MPLS TE tunnel that is enabled with automatic re-optimization.

Format

mpls te reoptimization [**tunnel** *interface-number*]

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies a tunnel that needs immediate re-optimization.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The manual re-optimization function is used in either of the following situations:

- After the network topology is modified manually, a new optimal path will be calculated. The new optimal path needs to be immediately used by the TE tunnel.

- TE tunnels need to be immediately optimized in batches, optimizing resources of these TE tunnels in time.

If you run the **mpls te reoptimization** command without specifying the **tunnel** *interface-number* parameter, all TE tunnels on which the automatic re-optimization is enabled are optimized. If you run the **mpls te reoptimization** command and specify the **tunnel** *interface-number* parameter, the specified TE tunnels on which the automatic re-optimization is enabled are optimized.

Re-optimization of a TE tunnel can be performed in either of the following modes:

- Automatic re-optimization: means that the TE tunnel is periodically optimized, saving manpower. To enable automatic re-optimization, run the **mpls te reoptimization (tunnel interface view)** command in the tunnel interface view. In addition, this command takes effect only on an established TE tunnel.
- Manual re-optimization: means that the TE tunnel is immediately optimized. To immediately optimize the TE tunnel, run the **mpls te reoptimization** command in the user view.

Prerequisites

Periodic re-optimization has been enabled by running the **mpls te reoptimization (tunnel interface view)** command.

Precautions

- If the re-optimization function is configured after an explicit path is configured and a new path fails to meet the explicit path constraints, the re-optimization function will not take effect.
- After a TE tunnel is configured with the re-optimization function, the tie breading in most-fill mode will not be supported.
- The **mpls te reoptimization** command cannot be run together with the following commands:
  - **mpls te route-pinning**
  - **mpls te resv-style ff**

Example

Immediately re-optimize all the TE tunnels that are configured with periodic re-optimization on the local device.

```
<Huawei> mpls te reoptimization
```

Related Topics

11.2.121 mpls te reoptimization (tunnel interface view)

11.2.121 mpls te reoptimization (tunnel interface view)

Function

The **mpls te reoptimization** command enables automatic re-optimization for a TE tunnel.

The **undo mpls te reoptimization** command restores the default setting.

By default, automatic re-optimization for a TE tunnel is disabled.

Format

mpls te reoptimization [**frequency** *interval*]

undo mpls te reoptimization

Parameters

Parameter	Description	Value
frequency *interval*	Specifies the interval for re-optimization. The system calculates the path for a TE tunnel based on constraints at the intervals of *interval*. If a better path to the same destination is calculated, the TE tunnel will be re-established over the better path.	The value is an integer that ranges from 60 to 604800, in seconds. By default, the interval is 3600 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a better path is calculated, to allow a TE tunnel to be automatically re-established over the better path, the **mpls te reoptimization** command needs to be run in the tunnel interface view. In this manner, after a better path to the same destination has been calculated for a certain reason such as the change of the cost, the TE tunnel can be automatically re-established, optimizing the resources on the network.

Re-optimization of a TE tunnel can be performed in either of the following modes:

- Automatic re-optimization: means that the TE tunnel is periodically optimized, saving manpower. To enable automatic re-optimization, run the **mpls te reoptimization** command in the tunnel interface view. In addition, this command takes effect only on an established TE tunnel.
- Manual re-optimization: means that the TE tunnel is immediately optimized. To immediately optimize the TE tunnel, run the **mpls te reoptimization** command in the user view.

Prerequisites

CSPF has been enabled by running the **mpls te cspf** command.

Precautions

- If the re-optimization function is configured after an explicit path is configured and a new path fails to meet the explicit path constraints, the re-optimization function will not take effect.
- After a TE tunnel is configured with the re-optimization function, the tie breading in most-fill mode will not be supported.
- The **mpls te reoptimization** command cannot be run together with the following commands:
  - **mpls te route-pinning**
  - **mpls te resv-style ff**

Example

Enable periodic re-optimization for a TE tunnel named Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te reoptimization frequency 43200
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.120 mpls te reoptimization (user view)

11.2.100 mpls te cspf

11.2.122 mpls te resv-style

Function

The **mpls te resv-style** command specifies a reservation style.

The **undo mpls te resv-style** command restores the default setting.

The default reservation style is SE.

Format

mpls te resv-style { **ff** | **se** }

undo mpls te resv-style

Parameters

Parameter	Description	Value
ff	Indicates the style of fixed filter.	-
se	Indicates the style of shared explicit.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

RSVP-TE only supports two resources reservation styles: FF and SE.

NOTE

The **mpls te resv-style ff** command cannot be configured simultaneously with the following commands: **mpls te fast-reroute**, **mpls te backup**, and **mpls te reoptimization (tunnel interface view)**.

Example

Set up a CR-LSP with the resource reservation style being FF.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te signal-protocol rsvp-te
[Huawei-Tunnel0/0/1] mpls te resv-style ff
[Huawei-Tunnel0/0/1] mpls te commit
```

11.2.123 mpls te route-pinning

Function

The **mpls te route-pinning** command enables the route pinning function.

The **undo mpls te route-pinning** command disables this function.

Route pinning is disabled by default.

Format

mpls te route-pinning

undo mpls te route-pinning

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

The **mpls te route-pinning** command cannot be configured simultaneously the **mpls te reoptimization (tunnel interface view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable route pinning function.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te route-pinning
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.119 mpls te record-route

11.2.124 mpls te signal-protocol

Function

The **mpls te signal-protocol** command specifies a signaling protocol to set up an LSP.

The **undo mpls te signal-protocol** command deletes the signaling protocol to set up an LSP.

The default signaling protocol used to set up an LSP is RSVP-TE.

Format

mpls te signal-protocol { **cr-static** | **rsvp-te** }

undo mpls te signal-protocol cr-static

Parameters

Parameter	Description	Value
cr-static	Uses static CR-LSPs to establish TE tunnels.	-
rsvp-te	Uses RSVP-TE as the signaling protocol.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

When configuring MPLS TE, you can run this command to specify a signaling protocol to set up a tunnel.

- When configuring an static MPLS TE tunnel, the signaling protocol used is **cr-static**.
- When configuring an dynamic MPLS TE tunnel, the signaling protocol used is **rsvp-te**.

 Copyright © Huawei Technologies Co., Ltd.

Example

Use RSVP-TE as the signaling protocol for MPLS TE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te signal-protocol rsvp-te
[Huawei-Tunnel0/0/1] mpls te commit
```

Related Topics

11.2.119 mpls te record-route

11.2.125 mpls te signaling-delay-trigger enable

Function

The **mpls te signaling-delay-trigger enable** command enables the RSVP signaling delay-trigger function.

The **undo mpls te signaling-delay-trigger enable** command disables the RSVP signaling delay-trigger function.

The RSVP signaling delay-trigger function is disabled by default.

Format

mpls te signaling-delay-trigger enable

undo mpls te signaling-delay-trigger enable

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a fault occurs on an MPLS network and a large number of RSVP CR-LSPs need to be re-established, a large amount of system resources may be required. In this case, after the RSVP signaling delay-trigger function is configured, the interval between re-establishments of a CR-LSP is prolonged so that system resources are saved.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

Before running the **mpls te signaling-delay-trigger enable** command, the **mpls te** command must be run in the MPLS view.

Precautions

Use caution when configuring the RSVP signaling delay-trigger function because it causes the delay of CR-LSP convergence. The default settings are recommended.

Example

Enable the RSVP signaling delay-trigger function.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls te signaling-delay-trigger enable
```

Related Topics

11.2.82 mpls te

11.2.126 mpls te signalled tunnel-name

Function

The **mpls te signalled tunnel-name** command configures the name of a TE tunnel.

The **undo mpls te signalled tunnel-name** command deletes the configured name of the TE tunnel.

By default, the name of a TE tunnel is not configured.

Format

mpls te signalled tunnel-name *tunnel-name*

undo mpls te signalled tunnel-name

Parameters

Parameter	Description	Value
tunnel-name	Specifies the name of a TE tunnel.	A string of 1 to 63 case-sensitive characters, spaces or slashes (/) not supported. The initial character must be an underscore (_) or an English letter, not a digit.

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A tunnel interface name is used as a tunnel name by default, for example, Tunnel0/0/1. Alternatively, if you want to customize a name for a TE tunnel, the **mpls te signalled tunnel-name** command can be used to configure a TE tunnel name. For example, a TE tunnel from LSR A to LSR C is named LSRAtoLSRC.

Precautions

A TE tunnel name must be unique on an entire device.

If a TE tunnel name is specified, RSVP signaling messages will carry the specified name. If a configured TE tunnel name is deleted or no TE tunnel name is specified, RSVP signaling messages will carry the TE tunnel interface name as the TE tunnel name.

The **mpls te signalled tunnel-name** command or its undo form takes effect on a TE tunnel established using only RSVP signaling, not a static route.

Example

Name a TE tunnel **LSRAtoLSRC**.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te signalled tunnel-name LSRAtoLSRC
[Huawei-Tunnel0/0/1] mpls te commit
```

11.2.127 mpls te srlg

Function

The **mpls te srlg** command configures an interface as an SRLG member.

The **undo mpls te srlg** command deletes an interface from an SRLG.

No interface is added to any SRLG by default.

Format

mpls te srlg *srlg-number*

undo mpls te srlg { *srlg-number* | **all** }

Parameters

Parameter	Description	Value
srlg-number	Specifies the number of the SRLG to which an interface belongs.	The value is an integer that ranges from 0 to 4294967295.
all	Indicates that all SRLG configurations are deleted from an interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SRLG, like the bandwidth and affinity property, is a constraint in path calculation. If SRLG is configured for links, an IGP floods the TE link information along with the SRLG membership information to all devices in an IGP area. The SRLG membership information is also added into the TEDB.

Prerequisites

Before running the **mpls te srlg** command, the **mpls te** command must be run in the interface view.

Precautions

If SRLG is configured for links and the **mpls te srlg path-calculation** command is configured on the ingress of the primary tunnel, when calculating the path of a bypass tunnel or a hot-standby tunnel, CSPF determines whether or not the SRLG attribute is used as a constraint according to the configured SRLG calculation mode.

One interface can join multiple SRLGs.

Example

Add GE1/0/0 to SRLG 1 and SRLG 2.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls
[Huawei-GigabitEthernet1/0/0] mpls te
[Huawei-GigabitEthernet1/0/0] mpls te srlg 1
[Huawei-GigabitEthernet1/0/0] mpls te srlg 2
```

Related Topics

11.2.128 mpls te srlg path-calculation

11.2.152 undo mpls te srlg all-config

11.2.35 display mpls te srlg

11.2.33 display mpls te link-administration srlg-information

11.2.128 mpls te srlg path-calculation

Function

The **mpls te srlg path-calculation** command configures an SRLG-based path calculation mode.

 Copyright © Huawei Technologies Co., Ltd.

The **undo mpls te srlg path-calculation** command deletes an SRLG-based path calculation mode.

By default, when calculating a path, CSPF does not consider an SRLG constraint or check whether or not the primary CR-LSP and a Bypass CR-LSP or a hot-standby CR-LSP are in the same SRLG.

Format

mpls te srlg path-calculation [**strict** | **preferred**]

undo mpls te srlg path-calculation

Parameters

Parameter	Description	Value
strict	Indicates that CSPF must calculate a bypass CR-LSP or a hot-standby CR-LSP according to the SRLG attribute. The link that the primary path uses and the link that the bypass CR-LSP or hot-standby CR-LSP uses cannot be in the same SRLG. **NOTE** After you specify this parameter, all the links on the primary CR-LSP regardless of whether the SRLG attribute is configured cannot be used for calculation of the bypass or hot-standby CR-LSP. However, nodes on the primary CR-LSP can be used in CSPF calculation.	-
preferred	Indicates that CSPF prefers the SRLG attribute the first time it calculates a Bypass CR-LSP or hot-standby CR-LSP. If the initial calculation fails, the CSPF does not use the SRLG attribute as a constraint. **NOTE** If no path calculation mode is specified in the **mpls te srlg path-calculation** command, SRLG-based path calculation is performed in preferred mode by default.	-

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the TE FRR or hot standby scenario, to enable CSPF to calculate a path for a Bypass CR-LSP or a hot-standby CR-LSP based on the SRLG attribute, you must run the **mpls te srlg path-calculation** command on the ingress of the tunnel.

The SRLG, like the bandwidth and affinity property, is a constraint in path calculation. If SRLG is configured for links and the **mpls te srlg path-calculation**

command is configured on the ingress of the primary CR-LSP, when calculating the path of a Bypass CR-LSP or a hot-standby tunnel, CSPF determines whether or not the SRLG attribute is used as a constraint according to the configured SRLG calculation mode.

Precautions

If **strict** is configured, CSPF always considers SRLG as a constraint.

If **preferred** is configured, the first time that CSPF calculates a path is according to the SRLG attribute. If the calculation fails, CSPF tries to calculate again without considering SRLG.

Example

Enable path calculation in **strict** mode.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te srlg path-calculation strict
```

Related Topics

11.2.127 mpls te srlg

11.2.152 undo mpls te srlg all-config

11.2.35 display mpls te srlg

11.2.33 display mpls te link-administration srlg-information

11.2.129 mpls te switch-delay

Function

The **mpls te switch-delay** command sets the switching and deletion delays for a TE tunnel.

The **undo mpls te switch-delay** command restores the default settings.

By default, the switching delay is 5000 milliseconds and the deletion delay is 7000 milliseconds.

Format

mpls te switch-delay *switch-time* **delete-delay** *delete-time*

undo mpls te switch-delay *switch-time* **delete-delay** *delete-time*

Parameters

Parameter	Description	Value
switch-delay *switch-time*	Specifies the time period that the TE traffic is switched from the primary CR-LSP to the Modified CR-LSP.	The value is an integer that ranges from 0 to 600000, in milliseconds. The default value is 5000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
delete-delay *delete-time*	Specifies the delay for deleting the primary CR-LSP after the TE traffic is switched to a Modified CR-LSP.	The value is an integer that ranges from 0 to 600000, in milliseconds. The default value is 7000.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MPLS TE uses the Make-Before-Break mechanism. When the attributes of an MPLS TE tunnel such as bandwidth and path change, a new CR-LSP with new attributes, also called Modified CR-LSP, must be established.

On the same modified CR-LSP, when a downstream LSR is too busy but the upstream LSR is not as busy, the Modified CR-LSP may go Up earlier on the upstream LSR than on the downstream LSR. The upstream LSR switches traffic to the Modified CR-LSP but the Modified CR-LSP is not Up on the downstream LSR. This causes a momentary traffic interruption. You can set a suitable switching delay time to avoid the traffic interruption.

If a modified CR-LSP fails, the failed node sends PathErr messages to its upstream LSRs and deletes the Modified CR-LSP, and traffic should be switched back to the primary CR-LSP. In applications, when detecting the fault, the upstream LSRs of the failed node are too occupied to forward the PathErr messages. This causes a traffic interruption on the failed node because the primary CR-LSP is deleted on the failed node. You can set a suitable deletion delay time to prevent the traffic interruption.

Prerequisites

MPLS TE has been enabled globally by running the **mpls te** command.

Example

Set the switching delay of the TE tunnel to 3000 milliseconds and the deletion delay of the TE tunnel to 8000 milliseconds.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te
[Huawei-mpls] mpls te switch-delay 3000 delete-delay 8000
```

Related Topics

11.2.37 display mpls te tunnel-interface

11.2.130 mpls te tie-breaking

Function

The **mpls te tie-breaking** command configures a rule for selecting a route among multiple available equal-cost routes to the destination.

The **undo mpls te tie-breaking** command restores the default settings.

By default, tie-breaking policy is random.

Format

mpls te tie-breaking { **least-fill** | **most-fill** | **random** }

undo mpls te tie-breaking

Parameters

Parameter	Description	Value
least-fill	Selects the route with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.	-
most-fill	Selects the route with the largest ratio of the occupied bandwidth to the maximum reservable bandwidth.	-
random	Selects a route randomly.	-

Views

MPLS view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The route is selected based on the ratio of the occupied available bandwidth to the maximum reservable bandwidth. If **least-fill** is configured, the route with the smallest ratio is selected; if **most-fill** is configured, the route with the largest ratio is selected.

Prerequisites

MPLS TE has been enabled by running the **mpls te** command.

Precautions

Note that the link is selected according to a ratio through the tie-breaking mechanism. In the case that the ratios are the same when the reservable bandwidth is not used or the same reservable bandwidth is used on the links, the

 Copyright © Huawei Technologies Co., Ltd.

first found link is used regardless of whether or not **least-fill** or **most-fill** is configured.

NOTE

A tunnel prefers the route-selecting rule configured in the local tunnel interface view. If no rule is configured in the tunnel interface view, the rule configured in the MPLS view is used.

Example

Select the path with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te tie-breaking least-fill
[Huawei-Tunnel0/0/1] mpls te commit
```

Select the path with the smallest ratio of the occupied bandwidth to the maximum reservable bandwidth.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te tie-breaking least-fill
```

Related Topics

11.2.100 mpls te cspf

11.2.131 mpls te timer fast-reroute

Function

The **mpls te timer fast-reroute** command sets the interval at which the binding between a bypass CR-LSP and a primary CR-LSP is refreshed.

The **undo mpls te timer fast-reroute** command restores the default configuration.

By default, the time weight used to calculate the interval is 300. And the actual interval at which the binding between a bypass CR-LSP and a primary LSP is refreshed depends on device performance and the maximum number of LSPs that can be established on the device.

Format

mpls te timer fast-reroute [*weight*]

undo mpls te timer fast-reroute

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
weight	Specifies the weight value used to calculate the interval at which the binding between a bypass CR-LSP and a primary LSP is refreshed.	The value is an integer that ranges from 0 to 604800. **NOTE** If *weight* is not specified, the default weight value is 300.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After TE FRR is configured, a PLR refreshes the binding between a bypass CR-LSP and a primary CR-LSP at a specified interval. The PLR searches for the optimal bypass CR-LSP and binds it to a primary CR-LSP. To set the interval at which the binding between a bypass CR-LSP and a primary CR-LSP is refreshed, run the **mpls te timer fast-reroute** command.

The PLR calculates the interval using the value of *weight*. And the actual interval depends on device performance and the maximum number of LSPs that can be established on the device

Prerequisites

RSVP-TE has been enabled by running the **mpls rsvp-te** command in the MPLS view.

Example

Set the weight of the interval at which binding between a bypass CR-LSP and a primary LSP is refreshed to **120**.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] mpls te timer fast-reroute 120
```

Related Topics

11.2.54 mpls rsvp-te

11.2.132 mpls te timer retry

Function

The **mpls te timer retry** command sets the interval for re-establishing a tunnel.

 Copyright © Huawei Technologies Co., Ltd.

The **undo mpls te timer retry** command restores the default setting.

The default interval is 30 seconds.

Format

mpls te timer retry *interval*

undo mpls te timer retry [*interval*]

Parameters

Parameter	Description	Value
interval	Specifies the interval for resetting up tunnels.	The value is an integer ranges from 10 to 65535, in seconds. The default value is 30 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a TE tunnel has been established, the TE tunnel is kept Up by periodically sending a Path message from the local node to its neighbor and receiving a Resv message from the neighbor. If no Resv message is received after the specified interval at which a tunnel is re-established, the local node considers the tunnel Down and reattempts to establish the tunnel. You can run this command to modify the interval for re-establishing a tunnel.

Precautions

A rather smaller interval imposes heavy burden of message processing on the system, causing network flapping; a rather large interval deteriorates the efficiency of RSVP CR-LSP convergence. Therefore, the default interval, 30 seconds, is recommended.

Example

Set the interval for setting up tunnels to 20 seconds.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te timer retry 20
[Huawei-Tunnel0/0/1] mpls te commit
```

 Copyright © Huawei Technologies Co., Ltd.

11.2.133 mpls te tunnel-id

Function

The **mpls te tunnel-id** command specifies the ID for a tunnel.

Format

mpls te tunnel-id *tunnel-id*

Parameters

Parameter	Description	Value
tunnel-id	Specifies the ID for a tunnel.	The value is an integer that ranges from 1 to 4096.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ID for a tunnel is a number that uniquely identifies an MPLS TE tunnel to facilitate tunnel planning and management.

Precautions

A tunnel ID must be set for a tunnel; otherwise, the tunnel fails to be established.

Example

Create a tunnel interface, configure MPLS TE as a tunnel protocol, set the tunnel ID to 100, and assign a tunnel destination address 2.2.2.2 to the interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te tunnel-id 100
[Huawei-Tunnel0/0/1] destination 2.2.2.2
[Huawei-Tunnel0/0/1] mpls te commit
```

 Copyright © Huawei Technologies Co., Ltd.

11.2.134 next hop

Function

The **next hop** command specifies the next-hop address on an explicit path, and creates an MPLS TE tunnel through nodes in the order in which they are configured.

The **undo next hop** command restores the default configuration.

By default, no next-hop address on an explicit path is specified.

Format

next hop *ip-address* [**include** [[**loose** | **strict**] | [**incoming** | **outgoing**]] * | **exclude**]

undo next hop *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the next-hop IP address on an explicit path.	The value is in dotted decimal notation.
include [[**loose** | **strict**] | [**incoming** | **outgoing**]] *	Specifies the IP address of a node included on an explicit path. ● **strict**: indicates that the node is added in **strict** mode. The node of *ip-address* is directly connected to the previous hop. ● **loose**: indicates that the node is added in **loose** mode. The node of *ip-address* may not be directly connected to the previous hop. ● **incoming**: indicates that the *ip-address* is the IP address of an inbound interface of a next-hop node. ● **outgoing**: indicates that the *ip-address* is the IP address of an outbound interface of a next-hop node.	By default, a node is added to an explicit path in **include strict** mode.
exclude	Excludes the IP address from an explicit path.	-

Views

Explicit path view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **next hop** command is used to plan nodes for an explicit path.

Precautions

The **include strict** parameters are used by default, meaning the tunnel must pass through a specified node.

Example

Exclude the IP address 10.0.0.125 from the MPLS TE explicit path.

```
<Huawei> system-view
[Huawei] explicit-path p1
[Huawei-explicit-path-p1] next hop 10.0.0.125 exclude
```

Related Topics

11.2.7 display explicit-path

11.2.51 list hop

11.2.1 add hop

11.2.50 explicit-path

11.2.135 notify neighbor-down

Function

The **notify neighbor-down** command configures a BFD session to notify the upper layer protocol when the BFD session detects a neighbor Down event.

The **undo notify neighbor-down** command restores the default configuration.

By default, when the BFD detection time expires or a BFD session detects a neighbor Down event, the BFD session notifies the upper layer protocol.

Format

notify neighbor-down

undo notify neighbor-down

Parameters

None

Views

BFD-LSP session view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

In most cases, when you use a BFD session to detect link faults, the BFD session notifies the upper layer protocol of a link fault in the following scenarios:

- When the BFD detection time expires, the BFD session notifies the upper layer protocol. BFD sessions must be configured on both ends. If the BFD session on the local end does not receive any BFD packets from the remote end within the detection time, the BFD session on the local end concludes that the link fails and notifies the upper layer protocol of the link fault.
- When a BFD session detects a neighbor Down event, the BFD session notifies the upper layer protocol. If the BFD session on the local end detects a neighbor Down event within the detection time, the BFD session on the local end directly notifies the upper layer protocol of the neighbor Down event.

When you use a BFD session to detect faults on an LSP, you need only be concerned about whether a fault occurs on the link from the local end to remote end. In this situation, run the **notify neighbor-down** command to configure the BFD session to notify the upper layer protocol only when the BFD session detects a neighbor Down event. This configuration prevents the BFD session from notifying the upper layer protocol when the BFD detection time expires and ensures that services are not interrupted.

Example

Configure the BFD session to notify the upper layer protocol when the BFD session detects a neighbor Down event.

```
<Huawei> system-view
[Huawei] bfd atob bind ldp-lsp peer-ip 10.1.2.1 nexthop 10.1.1.2 interface vlanif 100
[Huawei-bfd-lsp-session-atob] discriminator local 1
[Huawei-bfd-lsp-session-atob] discriminator remote 2
[Huawei-bfd-lsp-session-atob] notify neighbor-down
[Huawei-bfd-lsp-session-atob] commit
```

Related Topics

18.5.2 bfd

11.2.136 opaque-capability enable

Function

The **opaque-capability enable** command enables the Opaque-LSA capability so that an OSPF process can generate Opaque LSAs, and receive Opaque LSAs from neighbors.

The **undo opaque-capability** command disables the Opaque-LSA capability.

By default, the Opaque-LSA capability is disabled.

Format

opaque-capability enable

undo opaque-capability

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

OSPF view

Default Level

2: Configuration level

Usage Guidelines

Enabling or disabling the Opaque-LSA capability function can delete and reestablish all sessions and instances.

Example

Enable OSPF Opaque.

```
<Huawei> system-view
[Huawei] ospf
[Huawei-ospf-1] opaque-capability enable
```

Related Topics

9.4.69 ospf

11.2.137 qos te queue-profile

Function

The **qos te queue-profile** command applies a queue profile to an MPLS TE interface.

The **undo qos te queue-profile** command deletes a queue profile from an MPLS TE interface.

Format

qos te queue-profile *queue-profile-name*

undo qos te queue-profile

Parameters

Parameter	Description	Value
queue-profile-name	Specifies the name of a queue profile.	The value is a string of 1 to 31 case-insensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A queue profile is a set of queue parameters that determine the scheduling modes, lengths, weights, and traffic shaping rates of queues. After a queue profile is applied to an interface, different services can be provided for queues on the interface.

After creating a queue profile, bind the queue profile to an interface so that the scheduling modes, lengths, weights, and traffic shaping rates of queues take effect on the interface.

Prerequisites

A queue profile has been created using the **qos queue-profile (system view)** command.

Precautions

When you modify the configuration of the queue profile bound to an interface, the modification is synchronized to the interface and takes effect immediately if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

Example

Create a queue profile hello-world and apply it to GE1/0/0.

```
<Huawei> system-view
[Huawei] qos queue-profile hello-world
[Huawei-qos-queue-profile-hello-world] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] qos te queue-profile hello-world
```

Related Topics

20.4.9 qos queue-profile (system view)

11.2.138 reset mpls rsvp-te

Function

The **reset mpls rsvp-te** command resets RSVP-TE process.

Format

reset mpls rsvp-te

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can delete and re-establish a CR-LSP by running the **reset mpls rsvp-te** command. This command is used to verify the working process of RSVP-TE in special cases. Generally, this command is not needed.

Example

Reset RSVP-TE.

```
<Huawei> reset mpls rsvp-te
```

Related Topics

11.2.54 mpls rsvp-te

11.2.139 reset mpls rsvp-te statistics

Function

The **reset mpls rsvp-te statistics** command clears the operational statistics on RSVP-TE.

Format

reset mpls rsvp-te statistics { **global** | **interface** [*interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Clears the global operational statistics on RSVP-TE.	-
interface	Clears the operational statistics on RSVP-TE on the interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Clears the operational statistics on RSVP-TE on the specifies interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	If no type or number of an interface is specified, statistics about all RSVP-TE interfaces are cleared.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When you run this command to clear the running information about RSVP-TE, the system displays the statistics from after the previous information is cleared.

Example

Clear the global operational statistics on RSVP-TE.

```
<Huawei> reset mpls rsvp-te statistics global
```

Related Topics

11.2.23 display mpls rsvp-te statistics

11.2.140 reset mpls stale-interface

Function

The **reset mpls stale-interface** command deletes information about MPLS interfaces in the Stale state.

Format

reset mpls stale-interface [*interface-index*]

Parameters

Parameter	Description	Value
interface-index	Specifies the index of a specified stale interface.	A hexadecimal integer ranging from 1 to FFFFFFFE.

Views

User view

Default Level

3: Management level

Usage Guidelines

If the configuration of an interface is deleted, or MPLS is disabled on an interface, the interface status becomes Stale. Run the **reset mpls stale-interface** command to delete information about a stale interface.

Run the **display mpls stale-interface** command without specifying a parameter to view the index of a stale interface.

Example

Delete information about a specified stale interface.

```
<Huawei> reset mpls stale-interface 9d
```

Delete information about all stale interfaces.

```
<Huawei> reset mpls stale-interface
```

Related Topics

11.2.26 display mpls stale-interface

11.2.141 reset mpls te auto-frr

Function

The **reset mpls te auto-frr** command resets a specified Auto bypass tunnel.

NOTE

After the Auto FRR function is enabled, you can use this command to recreate a bypass tunnel.

Format

reset mpls te auto-frr { **lsp-id** *ingress-lsr-id tunnel-id* | **name** *bypass-tunnel-name* }

Parameters

Parameter	Description	Value
lsp-id	Specifies the ID of a LSP.	-
ingress-lsr-id	Specifies the LSR ID of the ingress.	In dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tunnel-id	Specifies the ID of a tunnel.	The value is an integer and its ranges from 0 to 65535.
name *bypass-tunnel-name*	Specifies the name of a bypass tunnel.	The value is a string of 1 to 63 characters.

Views

User view

Default Level

3: Management level

Usage Guidelines

None.

Example

Reset the bypass tunnel with the ingress address being 1.1.1.1 and the tunnel ID being 10.

```
<Huawei> reset mpls te auto-frr lsp-id 1.1.1.1 10
```

Related Topics

11.2.85 mpls te auto-frr (interface view)

11.2.142 reset mpls te tunnel-interface tunnel

Function

The **reset mpls te tunnel-interface tunnel** command resets a TE tunnel interface and re-establishes a TE tunnel.

Format

reset mpls te tunnel-interface tunnel *interface-number*

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the number of a TE tunnel.	-

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

To validate the configurations of an MPLS TE tunnel, you can run the **mpls te commit** command in the tunnel interface view, and then run the **reset mpls te tunnel-interface tunnel** command in the user view.

If you do not run the **mpls te commit** command after modifying the configuration of a TE tunnel in the tunnel interface view, the system prompts a fault after the **reset mpls te tunnel-interface tunnel** command is run.

Example

Reset Tunnel 0/0/1.

```
<Huawei> reset mpls te tunnel-interface tunnel 0/0/1
```

Related Topics

11.2.37 display mpls te tunnel-interface

11.2.143 snmp-agent trap enable feature-name mpls_rsvp

Function

The **snmp-agent trap enable feature-name mpls_rsvp** command enables the trap for the MPLS RSVP module.

The **undo snmp-agent trap enable feature-name mpls_rsvp** command disables the trap for the MPLS RSVP module.

By default, the trap is disabled for the MPLS RSVP module.

Format

snmp-agent trap enable feature-name mpls_rsvp [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name mpls_rsvp [**trap-name** *trap-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name *trap-name*	Enables or disables a trap of the specified name. **NOTE** If *trap-name* is not specified, all traps of the MPLS RSVP module will be enabled or disabled.	The value can be: • hwrsvpteauthfail: RSVP authentication failed. • hwrsvpteauthsuccess: RSVP authentication succeeded. • hwrsvptehellolost: The RSVP neighbor relationship was interrupted. • hwrsvptehellolostrecovery: The device is restored from the status of interruption of RSVP neighbor relationship. • hwrsvpteifnbrthresholdexceed: The proportion of configured RSVP neighbors to RSVP neighbors supported by a device reaches the upper alarm threshold. • hwrsvpteifnbrthresholdexceedclear: The proportion of configured RSVP neighbors to RSVP neighbors supported by a device falls below the lower threshold. • hwrsvpteifnbrtotalcountexceed: The number of configured RSVP neighbors on a device reaches the maximum number of RSVP neighbors supported by the device. • hwrsvpteifnbrtotalcountexceedclear: The number of configured RSVP neighbors on a device falls below the maximum limit of RSVP neighbors.

Views

System view

Default Level

3: Management level

Usage Guidelines

None.

Example

Enable the trap of the event that RSVP authentication failed.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mpls_rsvp trap-name hwrsvpteauthfail
```

Related Topics

11.2.47 display snmp-agent trap feature-name mpls_rsvp all

11.2.144 snmp-agent trap enable feature-name tunnel-te

Function

The **snmp-agent trap enable feature-name tunnel-te** command enables the trap for the Tunnel-TE module.

The **undo snmp-agent trap enable feature-name tunnel-te** command disables the trap for the Tunnel-TE module.

By default, the trap is disabled for the Tunnel-TE module.

Format

snmp-agent trap enable feature-name tunnel-te [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name tunnel-te [**trap-name** *trap-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name *trap-name*	Enables or disables a trap of the specified name. **NOTE** If *trap-name* is not specified, all traps of the Tunnel-TE module will be enabled or disabled.	The value can be: ● hwmplsapslost: No APS frame was transmitted on the protect tunnel in the tunnel protection group. ● hwmplsapslostrecovery: APS frames were transmitted on the protect tunnel in the tunnel protection group. ● hwmplsapsmismatch: APS information on the local end of a bidirectional tunnel was inconsistent with that on the remote end. ● hwmplsapsmismatchrecovery: APS information on the local end of a bidirectional tunnel was inconsistent with that on the remote end has been recovered. ● hwmplsapsoutage: A tunnel protection group went faulty. ● hwmplsapsoutagerecovery: The tunnel protection group recovered from a fault. ● hwmplspsswitchptow: The protection group switched from the protection tunnel back to the work tunnel. ● hwmplspsswitchwtop: The protection group switched from the work tunnel to the protection tunnel. ● hwmplsapsdegradedrecovery: The faulty working or protection tunnel in an APS protection group recovered. ● hwmplsapsdegraded: A tunnel in an APS protection group failed, which decreased the usability of the APS protection group.

Views

System view

Default Level

3: Management level

Usage Guidelines

None.

Example

Enable all traps of the Tunnel-TE module.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name tunnel-te
```

Related Topics

11.2.48 display snmp-agent trap feature-name tunnel-te all

11.2.145 static-cr-lsp egress

Function

The **static-cr-lsp egress** command configures a static CR-LSP on the egress LSR.

The **undo static-cr-lsp egress** command deletes a static CR-LSP from the egress LSR.

By default, no static CR-LSP on the egress LSR is configured.

Format

static-cr-lsp egress *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*]

undo static-cr-lsp egress *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the name of a CR-LSP.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the type and number of an inbound interface.	-
in-label *in-label*	Specifies the value of an incoming label.	The value is an integer ranges from 16 to 1023.
lsrid *ingress-lsr-id*	Specifies the ingress LSR ID.	-
tunnel-id *tunnel-id*	Specifies the ID of a tunnel.	The value is an integer ranges from 1 to 65535.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When configuring the egress of the CR-LSP, you can run the command **static-cr-lsp egress**. Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

To modify the value of **incoming-interface** *interface-type interface-number* and **in-label** *in-label*, run the **static-cr-lsp egress** command to set a new value. There is no need to run the **undo static-cr-lsp egress** command before changing a configured value.

Example

Configure the static CR-LSP named tunnel34 with the inbound interface being GE1/0/0, and the incoming label being 233 on the egress LSR.

```
<Huawei> system-view
[Huawei] static-cr-lsp egress tunnel34 incoming-interface gigabitethernet 1/0/0 in-label 233
```

Related Topics

11.2.146 static-cr-lsp ingress

11.2.147 static-cr-lsp transit

11.2.146 static-cr-lsp ingress

Function

The **static-cr-lsp ingress** command configures a static CR-LSP on the ingress LSR.

The **undo static-cr-lsp ingress** command deletes a static CR-LSP from the ingress LSR.

By default, no static CR-LSP on the ingress LSR is configured.

Format

static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* } **destination** *destination-address* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* [**bandwidth** [**ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7**] *bandwidth*]

undo static-cr-lsp ingress { **tunnel-interface tunnel** *interface-number* | *tunnel-name* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tunnel-interface tunnel *interface-number*	Specifies the tunnel interface of a static CR-LSP. *interface-number* indicates the tunnel interface number.	-
tunnel-name	Specifies the name of a CR-LSP.	The name is a string of 1 to 19 case-sensitive characters, spaces and abbreviation not supported. If you use the **interface Tunnel 0/0/1** command to create a tunnel interface for a static CR-LSP, the tunnel name in the **static-cr-lsp ingress** command must be formatted as "Tunnel0/0/1", otherwise, the tunnel cannot be created. There is no such a limit for the transit node and egress node.
destination *destination-address*	Specifies the destination IP address of a static CR-LSP.	The value is in dotted decimal notation.
nexthop *next-hop-address*	Specifies the next-hop IP address of a static CR-LSP.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the type and number of an outgoing interface. This parameter is only applicable to a P2P link.	-
out-label *out-label*	Specifies the value of an outgoing label.	The value is an integer ranges from 16 to 1048575.
bandwidth ct0 - **ct7** *bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT7.	The value is an integer ranges from 0 to 4000000000, in kbit/s. The default value is 0.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Run the this command on the ingress node to configure a static CR-LSP.

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

Precautions

To modify parameters including **destination** *destination-address*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, and **out-label** *out-label*, run the **static-cr-lsp ingress** command to set a new value. There is no need to run the **undo static-cr-lsp ingress** command before changing a configured value.

When configuring a static CR-LSP ensure that the route of the static CR-LSP exactly matches the routing information. For example:

- If you specify a next hop when configuring a static CR-LSP, specify a next hop when configuring a static IP route. If you do not specify a next hop, the static LSP cannot be set up. For example:

```
[Huawei] ip route-static 10.1.3.0 24 10.1.1.2
[Huawei] static-cr-lsp ingress Tunnel0/0/1 destination 10.1.3.1 nexthop 10.1.1.2 out-label 237
```

- If a dynamic routing protocol applies to the link between LSRs, the next-hop IP address along the LSP must be the same as the IP address of the next hop in the routing table.

Example

Configure the static CR-LSP named Tunnel0/0/1, with the destination IP address being 10.1.3.1, the next-hop address being 10.1.1.2, the outgoing label being 237, and the required bandwidth being 20 kbit/s from CT1 on the ingress.

```
<Huawei> system-view
[Huawei] static-cr-lsp ingress Tunnel0/0/1 destination 10.1.3.1 nexthop 10.1.1.2 out-label 237
bandwidth ct1 20
```

Related Topics

11.2.147 static-cr-lsp transit

11.2.145 static-cr-lsp egress

11.2.147 static-cr-lsp transit

Function

The **static-cr-lsp transit** command configures a static CR-LSP on a transit LSR.

The **undo static-cr-lsp transit** command deletes a static CR-LSP from the transit LSR.

By default, no static CR-LSP on a transit LSR is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

static-cr-lsp transit *lsp-name* [**incoming-interface** *interface-type interface-number*] **in-label** *in-label* { **nexthop** *next-hop-address* | **outgoing-interface** *interface-type interface-number* } * **out-label** *out-label* [**bandwidth** [**ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7**] *bandwidth*] [**description** *description*]

undo static-cr-lsp transit *lsp-name*

Parameters

Parameter	Description	Value
lsp-name	Specifies the CR-LSP name.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
incoming-interface *interface-type interface-number*	Specifies the incoming interface of the CR-LSP. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
in-label *in-label*	Specifies the value of an incoming label.	The value is an integer that ranges from 16 to 1023.
nexthop *next-hop-address*	Specifies the next-hop address.	The value is in dotted decimal notation.
outgoing-interface *interface-type interface-number*	Specifies the name of an outgoing interface.	-
out-label *out-label*	Specifies the value of an outgoing label.	The value is an integer that ranges from 16 to 1048575.
bandwidth ct0 - **ct7** *bandwidth*	Specifies the bandwidth values of CR-LSPs of CT0 to CT7.	The value is an integer ranges from 0 to 4000000000, in kbit/s. The default value is 0.
description *description*	Specifies the description information.	The value is a string of 1 to 63 case-sensitive characters with spaces.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Before setting up an MPLS TE tunnel through a static CR-LSP, configure a static route or an IGP to ensure connectivity between LSRs, and enable basic MPLS and MPLS TE functions. After setting up a static CR-LSP, you can run the **display mpls static-cr-lsp** command to ensure that the static CR-LSP is established successfully.

To modify parameters including **incoming-interface** *interface-type interface-number*, **in-label** *in-label*, **nexthop** *next-hop-address*, **outgoing-interface** *interface-type interface-number*, and **out-label** *out-label*, run the **static-cr-lsp transit** command to set a new value for each parameter. There is no need to run the **undo static-cr-lsp transit** command before modifying a value.

Example

Configure the static CR-LSP named tunnel39 with the incoming interface being GE1/0/0, the incoming label being 123, the outgoing interface being GE2/0/0, the outgoing label as 253, the required CT0 bandwidth being 20 kbit/s on the transit node.

```
<Huawei> system-view
[Huawei] static-cr-lsp transit tunnel39 incoming-interface gigabitethernet 1/0/0 in-label 123 outgoing-interface gigabitethernet 2/0/0 out-label 253 bandwidth ct0 20
```

Related Topics

11.2.146 static-cr-lsp ingress

11.2.145 static-cr-lsp egress

11.2.148 te-class

Function

The **te-class** command configures a TE-class.

The **undo te-class** command deletes a TE-class.

By default, TE-class is configured.

Format

te-class0 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

te-class1 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

te-class2 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

te-class3 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

 Copyright © Huawei Technologies Co., Ltd.

te-class4 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

te-class5 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

te-class6 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

te-class7 { **class-type** { **ct0** | **ct1** | **ct2** | **ct3** | **ct4** | **ct5** | **ct6** | **ct7** } **priority** *priority* [**description** *description-info*] | **description** *description-info* }

undo { **te-class0** | **te-class1** | **te-class2** | **te-class3** | **te-class4** | **te-class5** | **te-class6** | **te-class7** } [**description**]

Parameters

Parameter	Description	Value
class-type	Indicates the service type.	The IETF mode supports eight service types, CT0 to CT7.
ct0 - **ct7**	Indicates the value of a service type.	-
priority *priority*	Specifies the priority. It is the priority of CR-LSP preemption rather than the value of the EXP field in an MPLS packet header.	The value is an integer ranges from 0 to 7. The smaller the value, the higher preemption priority.
description-info	Specifies the description of a TE-class.	The value is a string of 1 to 31 case-sensitive characters with spaces.

Views

TE-class mapping view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

Before running the **te-class** command, a TE-class mapping table must have been created in the system view using the **te-class-mapping** command.

Precautions

The relationships among a CT, priorities, and LSP preemption are as follows:

- In the MAM and extended-MAM, a CR-LSP of higher priority can only preempt bandwidth of CR-LSPs of lower priorities that belong to the same CT.

 Copyright © Huawei Technologies Co., Ltd.

CR-LSPs of different CTs, however, do not preempt bandwidth from each other.

- In the RDM, if 0 ≤ m < n ≤7 and 0 ≤ i < j ≤ 7, CTi of priority m can preempt bandwidth of both CTi of priority n and of CTj of priority n. The total bandwidth of CTi of all CR-LSPs is less than or equal to that of BCi.

A CR-LSP can only be set up when both the combination of its CT and setup priority (<CT, setup-priority>) and the combination of its CT and holding priority (<CT, holding-priority>>) exist in a TE-class mapping table. Assume the TE-class mapping table of a certain node contains only TE-Class [0] = <CT0, 6> and TE-Class [1] = <CT0, 7>. Only the following types of CR-LSPs can be set up successfully. (The combination of setup-priority (6) and hold-priority (7) cannot exist because the setup priority of the CR-LSP cannot be higher than the holding priority of the CR-LSP.):

- Class-Type = CT0, setup-priority = 6, holding-priority = 6
- Class-Type = CT0, setup-priority = 7, holding-priority = 6
- Class-Type = CT0, setup-priority = 7, holding-priority = 7

When the **undo mpls** command is run in the system view, or the **undo mpls te** command is run in the MPLS view, all configured TE-Class are deleted. When the **undo te-class-mapping** command is run in the system view to delete a configured TE-class mapping table, the configurations of all TE-classes are also deleted from the mapping table.

Example

Configure the TE-class mapping table and configure three CTs: CT0, CT1, and CT2 with their preemption priorities of 0, 1, and 2, respectively.

```
<Huawei> system-view
[Huawei] te-class-mapping
[Huawei-te-class-mapping] te-class0 class-type ct0 priority 0 description For-EF
[Huawei-te-class-mapping] te-class1 class-type ct1 priority 1 description For-AF
[Huawei-te-class-mapping] te-class2 class-type ct2 priority 2 description For-BE
```

Related Topics

11.2.149 te-class-mapping

11.2.149 te-class-mapping

Function

The **te-class-mapping** command creates a TE-class mapping table or displays the TE-class mapping view.

The **undo te-class-mapping** command deletes the configured TE-class mapping table.

By default, no TE-class mapping table is created but their is a **default TE-class mapping table**.

Format

te-class-mapping

undo te-class-mapping

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The TE-class mapping table is only valid in IETF mode. In non-IETF mode, the TE-class mapping table can be configured, but cannot take effect.

You need to run the **te-class-mapping** command to create a TE-class mapping table before configuring it.

When the **undo mpls** command is run in the system view, or the **undo mpls te** command is run in the MPLS view, the configured TE-class mapping table is deleted.

In IETF mode, the system has one TE-class mapping table by default.

Table 11-101 Default TE-class mapping table

TE-class	CT	Priority
TE-class [0]	0	0
TE-class [1]	1	0
TE-class [2]	2	0
TE-class [3]	3	0
TE-class [4]	0	7
TE-class [5]	1	7
TE-class [6]	2	7
TE-class [7]	3	7

Example

Create a TE-class mapping table.

```
<Huawei> system-view
[Huawei] te-class-mapping
[Huawei-te-class-mapping]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

11.2.148 te-class

11.2.150 te-set-subtlv

Function

The **te-set-subtlv** command sets the TLV types for different sub-TLVs that carry DS-TE parameters.

The **undo te-set-subtlv** command restores the default settings.

Sub-TLVs of **bw-constraint**, **lo-multiplier**, and **unreserve-bw-sub-pool** are set to 252, 253, and 251 respectively, by default.

Format

te-set-subtlv { **bw-constraint** *bw-constraint-value* | **lo-multiplier** *lo-multiplier-value* | **unreserve-bw-sub-pool** *unreserve-bw-sub-pool-value* } *

undo te-set-subtlv { **bw-constraint** [*bw-constraint-value*] | **lo-multiplier** [*lo-multiplier-value*] | **unreserve-bw-sub-pool** [*unreserve-bw-sub-pool-value*] } *

Parameters

Parameter	Description	Value
bw-constraint *bw-constraint-value*	Sets the value of a bandwidth constraint sub-TLV.	The value is an integer that ranges from 19 to 254.
lo-multiplier *lo-multiplier-value*	Sets the value of the Local Overbooking Multiplier (LOM) sub-TLV.	The value is an integer that ranges from 19 to 254.
unreserve-bw-sub-pool *unreserve-bw-sub-pool-value*	Sets the value of the unreserved bandwidth sub-pool sub-TLV.	The value is an integer that ranges from 19 to 254.

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Because the standard of the DS-TE sub-TLV types is unavailable, set the value of sub-TLVs when devices of different vendors are connected. After the configuration, the TEDB can be generated again, and the TE tunnel is re-established.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the types of sub-TLVs of IS-IS process 1.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] te-set-subtlv bw-constraint 200 lo-multiplier 201 unreserve-bw-sub-pool 202
Warning: This will cause ISIS TE to be reset. Are you sure?[Y/N]y
```

Related Topics

11.2.105 mpls te ds-te mode

11.2.151 traffic-eng

Function

The **traffic-eng** command enables TE features on a specified level for an IS-IS process.

The **undo traffic-eng** command restores the default settings.

By default, TE features are disabled for an IS-IS process.

Format

traffic-eng [**level-1** | **level-2** | **level-1-2**]

undo traffic-eng [**level-1** | **level-2** | **level-1-2**]

Parameters

Parameter	Description	Value
level-1	Enables IS-IS TE on Level-1.	-
level-2	Enables IS-IS TE on Level-2.	-
level-1-2	Enables IS-IS TE on Level-1-2. **NOTE** If no level is specified, TE is enabled on Level-1-2.	-

Views

IS-IS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

When you deploy MPLS TE on the MPLS backbone network where IS-IS is used to advertise routes, run this command to enable TE features on a specified level for an IS-IS process.

Prerequisites

The **cost-style** command has been executed to set the cost type of IS-IS packets to wide, compatible, or wide-compatible.

Precautions

The IS-IS level in this command must be the same as that on the MPLS backbone network.

Example

Enable TE on level-2 for IS-IS process 1.

```
<Huawei> system-view
[Huawei] isis 1
[Huawei-isis-1] cost-style compatible
[Huawei-isis-1] traffic-eng level-2
```

Related Topics

9.6.35 display isis traffic-eng advertisements

9.6.11 cost-style

11.2.152 undo mpls te srlg all-config

Function

The **undo mpls te srlg all-config** command deletes the member interfaces of all SRLGs on an MPLS TE node.

Format

undo mpls te srlg all-config

Parameters

None

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

If an MPLS TE node is configured with the **undo mpls te srlg all-config** command, the **mpls te srlg** command is deleted from all the interfaces of an

 Copyright © Huawei Technologies Co., Ltd.

MPLS TE node, while the **mpls te srlg path-calculation** command configured in the MPLS view is not deleted.

Example

Delete the SRLG configuration from all the interfaces of the MPLS TE node.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls te srlg 1
[Huawei-GigabitEthernet1/0/0] mpls te srlg 2
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] mpls te srlg 1
[Huawei-GigabitEthernet2/0/0] mpls te srlg 2
[Huawei-GigabitEthernet2/0/0] quit
[Huawei] mpls
[Huawei-mpls] undo mpls te srlg all-config
```

Related Topics

11.2.127 mpls te srlg

11.2.128 mpls te srlg path-calculation

11.2.35 display mpls te srlg

11.2.33 display mpls te link-administration srlg-information

 Copyright © Huawei Technologies Co., Ltd.

12 VPN Commands

About This Chapter

12.1 L2TP Configuration Commands
12.2 L2TPv3 Configuration Commands
12.3 GRE Configuration Commands
12.4 SVPN Configuration Commands
12.5 DSVPN Configuration Commands
12.6 IPSec Configuration Commands
12.7 A2A VPN Configuration Commands
12.8 SSL VPN Configuration Commands
12.9 BGP/MPLS IP VPN Configuration Commands
12.10 EVPN Configuration Commands
12.11 VLL Configuration Commands
12.12 PWE3 Configuration Commands
12.13 VPLS Configuration Commands
12.14 VXLAN Configuration Commands

12.1 L2TP Configuration Commands

NOTE

AR161EW-M1, AR169EGW-L, AR161EW and AR169EW do not support LAC and LNS, but support L2TP Client.

 Copyright © Huawei Technologies Co., Ltd.

12.1.1 allow l2tp

Function

The **allow l2tp** command specifies a virtual interface template and the name of an LAC tunnel that are used by the LNS to accept an L2TP connection request.

The **undo allow** command rejects an L2TP connection request.

By default, an L2TP connection request is rejected.

Format

allow l2tp virtual-template *virtual-template-number* [**remote** *remote-name* [**vpn-instance** *vpn-instance-name*]]

undo allow

Parameters

Parameter	Description	Value
virtual-template *virtual-template-number*	Specifies the number of a virtual interface template used when the LNS accepts a call connection request.	The value is an integer that ranges from 0 to 1023.
remote *remote-name*	Specifies the name of a remote tunnel end. You can use the **tunnel name** command to configure the name on an LAC in the L2TP group view. When the L2TP group number is not 1, you must specify *remote-name*.	The value is a string of 1 to 30 case-sensitive characters.
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which the IP address of the L2TP connection belongs. The LNS searches for the corresponding L2TP group based on the VPN instance name and *remote-name*. Route information to LACs exists in the routing table of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters.

Views

L2TP group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **allow l2tp** command is used on the LNS side to establish an L2TP connection between the LAC and LNS. After receiving an L2TP connection request, the LNS accepts the L2TP connection request and initiates a PPP negotiation on the specified virtual tunnel template (which also used as an L2TP tunnel interface) if the tunnel name contained in the connection request is consistent with the name specified by the **allow l2tp** command.

When L2TP group 1 is used and the tunnel name is not specified, the default L2TP group receives L2TP connection requests sent by any remote end and the tunnel name on the LAC side is not checked. This method can be used when the name of a remote tunnel end is unknown to the LNS.

Precautions

When specify the name of the remote tunnel end, ensure that the name is consistent with the tunnel name configured on the LAC side.

Example

Configure the device to receive L2TP tunnel connection requests sent by the LAC device named **lac**. Create a virtual interface template **virtual-template 1**.

```
<Huawei> system-view
[Huawei] l2tp-group 2
[Huawei-l2tp2] allow l2tp virtual-template 1 remote lac
```

Set L2TP group 1 as the default L2TP group, configure the device to receive L2TP tunnel connection requests sent by any remote end, and create a virtual interface template **virtual-template 1**.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] allow l2tp virtual-template 1
```

Configure the device to receive L2TP tunnel connection requests sent by the LAC device named **lac** that belongs to **vpn1**. Create a virtual interface template **virtual-template 1**.

```
<Huawei> system-view
[Huawei] l2tp-group 2
[Huawei-l2tp2] allow l2tp virtual-template 1 remote lac vpn-instance vpn1
```

Related Topics

12.1.9 l2tp-group
12.1.19 tunnel name

12.1.2 display l2tp session

Function

The **display l2tp session** command displays information about L2TP sessions established on the current device.

Format

display l2tp session [**destination-ip** *d-ip-address* | **session-item** *session-id* | **source-ip** *s-ip-address*]

Parameters

Parameter	Description	Value
destination-ip *d-ip-address*	Specifies the IP address of the L2TP tunnel remote end used to view session information.	The value is in dotted decimal notation.
session-item *session-id*	Specifies IDs of local sessions, and displays session used to view tunnel information.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 1 to 16 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 ● AR2220, AR2220E, AR2240C: 1 to 512 ● AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024
source-ip *s-ip-address*	Specifies the IP address of the L2TP tunnel local end and displays session information.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After L2TP sessions are established, you can use this command to view the number of L2TP sessions that are established on the current device, and the session IDs.

You can view statistics of L2TP sessions by the IP address of the L2TP tunnel remote end or local end.

 Copyright © Huawei Technologies Co., Ltd.

If local session IDs are specified, you can view information about L2TP sessions and the tunnel.

Prerequisites

L2TP sessions have been established.

Example

Display information about L2TP sessions.

```
<Huawei> display l2tp session

 Total session : 1
 LocalSID  RemoteSID  LocalTID  Interface            LclTAddr       RmtTAddr       LclSAddr       RmtSAddr
 1         1          4         Virtual-Template0:1  3.3.40.132     3.3.40.140     5.5.5.1        5.5.5.201
```

Table 12-1 Description of the display l2tp session command output

Item	Description
Total session	Total number of sessions established on the local end.
LocalSID	Local session ID.
RemoteSID	Remote session ID.
LocalTID	Local tunnel ID.
Interface	Name of the virtual interface for the local L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
LclTAddr	Local tunnel IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
RmtTAddr	Remote tunnel IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
LclSAddr	Local session IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.
RmtSAddr	Remote session IP address in the L2TP session. **NOTE** This parameter is supported in V200R010C10 and later versions.

Display information about L2TP sessions of the tunnel with the destination IP address as 3.3.40.140.

```
<Huawei> display l2tp session destination-ip 3.3.40.140

 Total session : 1
 LocalSID  RemoteSID  LocalTID  Interface            LclTAddr       RmtTAddr       LclSAddr       RmtSAddr
 1         1          4         Virtual-Template0:1  3.3.40.132     3.3.40.140     5.5.5.1        5.5.5.201
```

Display information about L2TP sessions of the tunnel with the local session ID as 1.

```
<Huawei> display l2tp session session-item 1
  -----------------------------------------------------------
    Call id              :1
    Remote Call id       :1
    Call State           :Up
    Remote tunnel name  :lac
    Remote Address       :10.1.2.3    port : 1701
    Local tunnel name   :lns
    Local Address        :10.1.2.4    port : 1701
    Call serial number  :1
    Session username     : NULL
    Sequencing is        :off
    Source Interface     :Routing
  -----------------------------------------------------------
```

Table 12-2 Description of the **display l2tp session** command output

Item	Description
Call id	Local session ID.
Remote Call id	Remote session ID.
Call State	Call status. The value is **Up** after an L2TP session is established.
Remote tunnel name	Remote tunnel name.
Remote Address	Remote tunnel address.
Local tunnel name	Local tunnel name.
Local Address	Local IP address.
Call serial number	Call serial number.
Session username	Session username: ● Client: The user name is displayed. ● Sever: **NULL**is displayed.
Sequencing is	Sequencing function. The default value is **off**.
Source Interface	Outbound interface of the tunnel. ● When multiple equal cost routes exist between the local and remote ends, the name of the access-side interface is displayed. ● When no equal cost routes exist between the local and remote ends, **Routing** is displayed.

Related Topics

12.1.3 display l2tp tunnel

12.1.3 display l2tp tunnel

Function

The **display l2tp tunnel** command displays information about the current L2TP tunnel.

Format

display l2tp tunnel [**tunnel-item** *tunnel-id* | **tunnel-name** *tunnel-name*]

Parameters

Parameter	Description	Value
tunnel-item *tunnel-id*	Specifies the tunnel ID used to view tunnel information.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 1 to 16 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 • AR2220, AR2220E, AR2240C: 1 to 512 • AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024
tunnel-name *tunnel-name*	Specifies the name of the tunnel remote end used to view tunnel information.	The value is a string of 1 to 30 characters.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After L2TP tunnels are established, you can use this command to view the number of L2TP tunnels that are established on the current device, the tunnel IDs, and tunnel addresses.

You can view detailed information about a specified L2TP tunnel by local tunnel ID or remote tunnel name.

Prerequisites

L2TP sessions have been established.

Example

Display information about the current L2TP tunnel.

```
<Huawei> display l2tp tunnel

 Total tunnel : 1
 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         10.1.2.4         1701   1        lns
```

NOTE

If a large number of sessions are carried over a tunnel, the sessions may still exist when you tear down the tunnel.

Table 12-3 Description of the display l2tp tunnel command output

Item	Description
Total tunnel	Total number of tunnels established on the local end.
LocalTID	Local tunnel ID.
RemoteTID	Remote tunnel ID.
RemoteAddress	Remote tunnel IP address.
Port	Remote port number. The value is 1701 in general.
Sessions	Number of sessions that an L2TP tunnel carries.
Remote Name	Name of the tunnel remote end.

Display detailed information about L2TP tunnel **1**.

```
<Huawei> display l2tp tunnel tunnel-item 1
  -----------------------------------------------------------
    Tunnel id            :1
    Remote Tunnel id     :1
    Tunnel State         :Up
    Remote tunnel name  :lns
    Remote Address       :10.1.2.4    port : 1701
    ReCall Address       :10.1.2.4
    Local tunnel name   :lac
    Local Address        :10.1.2.3    port : 1701
    active sessions      :1
```

```
  Session Limit       :4294967295
  Control Ns          :170
  Control Nr          :169
  Retransmission      :5
  Timeout             :2
  Hello Interval      :60
  Local RWS           :4
  Remote RWS          :128
  OuterDscp           :0xff
  Source Interface    :Routing
-------------------------------------------------------------
```

Table 12-4 Description of the **display l2tp tunnel** command output

Item	Description
Tunnel id	Local tunnel ID.
Remote Tunnel id	Remote tunnel ID.
Tunnel State	Tunnel status. The tunnel status is **Up** after the L2TP tunnel is successfully set up.
Remote tunnel name	Name of the tunnel remote end.
Remote Address	Remote port number and IP address. The port number is 1701 in general.
ReCall Address	Recall address.
Local tunnel name	Name of the tunnel local end.
Local Address	Local port number and IP address. The port number is 1701 in general.
active sessions	Number of sessions established in the current L2TP tunnel.
Session Limit	Maximum number of sessions that can be established in the L2TP tunnel.
Control Ns	Number of control packets sent over the tunnel.
Control Nr	Number of control packets received over the tunnel.
Retransmission	Number of retransmission times after the transmission of control packets fails.
Timeout	Aging time of control packets.
Hello Interval	Interval for sending Hello packets.
Local RWS	Size of the local receiving window.
Remote RWS	Size of the remote receiving window.
OuterDscp	Priority of packets after L2TP encapsulation. This parameter is used in QoS deployment.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Source Interface	Outbound interface of the L2TP tunnel ● When multiple equal cost routes exist between the local and remote ends, the name of the access-side interface is displayed. ● When no equal cost routes exist between the local and remote ends, **Routing** is displayed.

Related Topics

12.1.2 display l2tp session

12.1.4 display l2tp-group

Function

The **display l2tp-group** command displays configurations of the L2TP group on the device.

Format

display l2tp-group [*group-number*]

Parameters

Parameter	Description	Value
group-number	Specifies an L2TP group.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 1 to 16 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 ● AR2220, AR2220E, AR2240C: 1 to 512 ● AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the L2TP group and its number.

You can also use this command to view L2TP configurations of a specified group to rectify a fault or check the configurations.

Example

Display the L2TP group existing on the device currently.

```
<Huawei> display l2tp-group
----------------------------------------
 L2TP-GROUP    GROUP-NUMBER
----------------------------------------
 1             1
 2             2
 4             4
----------------------------------------
```

Table 12-5 Description of the display l2tp-group command output

Item	Description
L2TP-GROUP	L2TP group identified by a group number.
GROUP-NUMBER	L2TP group number.

Display the configurations of the L2TP group **1**.

```
<Huawei> display l2tp-group 1
 ----------------------------------------------
 L2tp-index        :    1
 GroupType         :    ACCEPT_DIALIN_L2TP
 TunnelAuth        :    Use tunnel authentication
 LocalName         :    lns
 Encrypt           :   0
 Hello             :   60
 Retransmit        :   5
 Timeout           :   2
 IfIndex           :   4294967295
 SrcIp             :   255.255.255.255
 VtNum             :   1
 RemoteName        :   lac1
 ForceChap         :   0
 LcpReg            :   0
 LcpMismatch       :   0
 tunnel each user  :   0
 ----------------------------------------------
```

Table 12-6 Description of the display l2tp-group command output

Item	Description
L2tp-index	L2TP group number.
GroupType	L2TP group type. ● REQUEST_DIALIN_L2TP: The device functions as the LAC to receive dial-up calls and initiate L2TP connections to the LNS. ● ACCEPT_DIALIN_L2TP: The device functions as the LNS to receive the L2TP connection requests from the LAC. ● VPDNGROUPTYPE_NONE: The L2TP group function is not configured.
TunnelAuth	Whether tunnel authentication is enabled.
LocalName	Name of the tunnel local end.
Encrypt	Whether the authentication password is configured for tunnel encapsulation. ● 0: no ● 1: yes
Hello	Interval for sending Hello messages (the default interval is 60 seconds).
Retransmit	Number of retransmission times after the transmission of control packets fails (the default number of retransmissions is 5).
Timeout	Aging time of control packets (the default aging time is 2 seconds).
IfIndex	Interface index bound to the tunnel.
SrcIp	IP address of the tunnel source interface.
VtNum	Number of the virtual interface template.
RemoteName	Name of the tunnel remote end.
ForceChap	Whether mandatory CHAP authentication is enabled. ● 0: no ● 1: yes
LcpReg	Whether LCP renegotiation is enabled. ● 0: no ● 1: yes

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
LcpMismatch	Whether mandatory LCP renegotiation is enabled when the PPP authentication mode on the LAC is different from that on the LNS. ● 0: no ● 1: yes
tunnel each user	Whether an L2TP user exclusively occupies an L2TP tunnel. ● 0: no ● 1: yes

12.1.5 display l2tp statistics tunnel

Function

The **display l2tp statistics tunnel** command displays L2TP packet statistics.

Format

display l2tp statistics tunnel [**local-id** *tunnel-id*]

Parameters

Parameter	Description	Value
local-id *tunnel-id*	Specifies the local tunnel ID of an L2TP tunnel.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 1 to 16 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 ● AR2220, AR2220E, AR2240C: 1 to 512 ● AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When L2TP users go online, there are packet exchanges of multiple protocols. You can run the **display l2tp statistics tunnel** command to check L2TP packet statistics.

Prerequisites

A tunnel is established successfully before you run the **display l2tp statistics tunnel local-id** *tunnel-id* command. You can run the **display l2tp tunnel** command to check the value of **local-id**.

Example

Display L2TP packet statistics of the device.

```
<Huawei> display l2tp statistics tunnel

                SEND         RESEND          RCVD
          ==========     ==========     ==========
SCCRQ              0            0            9
SCCRP              9           30            0
SCCCN              0            0            2
StopCCN            7            0            0
ICRQ               0            0            2
ICRP               2            0            0
ICCN               0            0            2
CDN                0            0            0
Hello              5            0            5
Total             23           30           20
```

Display L2TP packet statistics of tunnel 1.

```
<Huawei> display l2tp tunnel

 Total tunnel : 1
 LocalTID RemoteTID RemoteAddress    Port   Sessions RemoteName
 1        1         10.1.2.4         1701   1        lns
<Huawei> display l2tp statistics tunnel local-id 1
Tunnel LocalID: 1
Tunnel RemoteID: 1
Local Address: 10.1.1.1
Remote Address: 10.1.1.2

                SEND         RESEND          RCVD
          ==========     ==========     ==========
SCCRQ              0            0            1
SCCRP              1            0            0
SCCCN              0            0            1
StopCCN            0            0            0
ICRQ               0            0            1
ICRP               1            0            0
ICCN               0            0            1
CDN                0            0            0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Hello          5          0          5
Total          7          0          9
```

Table 12-7 Description of the **display l2tp statistics tunnel** command output

Item	Description
Tunnel LocalID	Local ID of the L2TP tunnel.
Tunnel RemoteID	Remote ID of the L2TP tunnel.
Local Address	Local IP address of the L2TP tunnel.
Remote Address	Remote IP address of the L2TP tunnel.
SEND	Number of sent L2TP packets.
RESEND	Number of resent L2TP packets.
RCVD	Number of received L2TP packets.
SCCRQ	Start control connection request packet.
SCCRP	Start control connection reply packet.
SCCCN	Start control connection connected packet.
StopCCN	Stop control connection notification packet.
ICRQ	Incoming call request packet.
ICRP	Incoming call reply packet.
ICCN	Incoming call connected packet.
CDN	Call disconnection packet.
Hello	Hello packet.
Total	Total number of sent, resent, and received packets of various types.

NOTE

The device only receives SCCRQ, SCCCN, ICRQ, and ICCN packets.
The device only sends and resends SCCRP and ICRP packets.
The device only sends and receives StopCCN, CDN, and Hello packets.

Related Topics

12.1.3 display l2tp tunnel

12.1.6 l2tp aging

Function

The **l2tp aging** command sets the LNS locking duration.

The **undo l2tp aging** command restores the default value.

By default, the LNS locking duration is 30 seconds.

Format

l2tp aging *time*

undo l2tp aging

Parameters

Parameter	Description	Value
time	Specifies the LNS aging time.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device attempts to set up a tunnel to an LNS but the LNS runs abnormally, the device marks the LNS as unusable and does not set up a tunnel to the LNS in a period. This period is the LNS locking duration. After the locking duration, the device attempts to set up a tunnel to the LNS again.

Example

Set the LNS aging time to 60 seconds.

```
<Huawei> system-view
[Huawei] l2tp aging 60
```

12.1.7 l2tp enable

Function

The **l2tp enable** command enables L2TP globally.

The **undo l2tp enable** command disables L2TP.

By default, L2TP is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

l2tp enable

undo l2tp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TheL2TP function enables remote users to dial up to access resources in the enterprise headquarters. You can complete L2TP configurations and then enable L2TP. You can also enable L2TP first and then complete L2TP configurations.

Precautions

The L2TP configurations take effect only after you run the **l2tp enable** command. If you run the **undo l2tp enable** command, the L2TP configurations do not take effect.

Example

Enable L2TP on the router.

```
<Huawei> system-view
[Huawei] l2tp enable
```

12.1.8 l2tp-auto-client enable

Function

The **l2tp-auto-client enable** command enables a virtual PPP user on the device to initiate an L2TP connection request.

The **undo l2tp-auto-client enable** command disables a virtual PPP user on the device from initiating an L2TP connection request.

By default, a virtual PPP user cannot initiate an L2TP connection request.

Format

l2tp-auto-client enable

undo l2tp-auto-client enable

Parameters

None

Views

VT interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An L2TP connection request is initiated in the following cases:

- The LAC receives a dial-up call from a remote user, and then initiates an L2TP connection request.
- A virtual PPP user on the L2TP Client automatically dials up, and the L2TP Client initiates an L2TP connection request.

In auto L2TP Client-initiated mode, users in the branch do not need to be managed by the headquarters in a centralized manner. Instead, the LNS in the headquarters authenticates only the gateway in the branch. The branch gateway functions as the L2TP Client on which virtual PPP users are created. The virtual users automatically dial up to initiate L2TP connections to the LNS. No additional devices or configurations are required for branch users to access the headquarters resources.

Prerequisites

L2TP has been enabled globally by running the **l2tp enable** command on the LAC or L2TP Client.

Example

Enable a virtual PPP user to initiate an L2TP tunnel.

```
<Huawei> system-view
[Huawei] l2tp enable
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] l2tp-auto-client enable
```

Related Topics

12.1.7 l2tp enable

12.1.9 l2tp-group

Function

The **l2tp-group** command creates an L2TP group or displays an L2TP group with a specified group number.

The **undo l2tp-group** command deletes an L2TP group.

 Copyright © Huawei Technologies Co., Ltd.

By default, no L2TP group is created.

Format

l2tp-group *group-number*

undo l2tp-group *group-number*

Parameters

Parameter	Description	Value
group-number	Specifies the L2TP group number.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 1 to 16 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 ● AR2220, AR2220E, AR2240C: 1 to 512 ● AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An L2TP tunnel is established after the LAC and LNS negotiate L2TP parameters successfully. These L2TP parameters are set in the L2TP group view. An L2TP group is an end of a tunnel. A local end and a remote end constitute an L2TP tunnel.

When the group number is 1, it is the default group. When the default group is configured on the LNS and no remote tunnel name is specified, the LNS accepts any L2TP connection request initiated by the LAC.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

L2TP has been enabled by running the **l2tp enable** command in the system view.

Follow-up Procedure

Configure L2TP parameters on the LAC or LNS.

Precautions

After you run the **undo l2tp-group** command to delete an L2TP group, all information about this group is deleted.

If an L2TP tunnel with the group as one end exists, this group cannot be deleted. Run the **reset l2tp tunnel** { **local-id** *local-id* | **peer-name** *peer-name* } command in the user view to forcibly disconnect the L2TP tunnel based on the tunnel ID or remote tunnel name, and then delete the L2TP group.

Example

Create L2TP group 2 and enter the L2TP group 2 view.

```
<Huawei> system-view
[Huawei] l2tp-group 2
[Huawei-l2tp2]
```

Related Topics

12.1.1 allow l2tp

12.1.16 start l2tp

12.1.14 reset l2tp tunnel

12.1.10 mandatory-chap

Function

The **mandatory-chap** command enables the LNS to perform mandatory CHAP authentication on remote users.

The **undo mandatory-chap** command disables mandatory CHAP authentication.

By default, mandatory CHAP authentication is disabled on the LNS.

Format

mandatory-chap

undo mandatory-chap

Parameters

None

Views

L2TP group view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Mandatory CHAP authentication is enabled on networks that demand high security. The LNS authenticates remote users using CHAP authentication. If PAP authentication mode is configured on the LAC, the LNS will not perform PPP negotiation with the LAC immediately after receiving the authentication success message. Instead, the LNS requires that the remote user initiates secondary CHAP authentication.

Prerequisites

The **l2tp-group** *l2tp-group* command has been executed to create an L2TP group and enter the L2TP group view.

Precautions

Some PPP clients may not support the second authentication. In this case, the L2TP connection fails if mandatory CHAP authentication is enabled.

When LCP renegotiation and mandatory CHAP authentication are configured simultaneously in an L2TP group, the LCP renegotiation takes effect.

Example

Enable mandatory CHAP authentication.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] mandatory-chap
```

Related Topics

12.1.11 mandatory-lcp

12.1.11 mandatory-lcp

Function

The **mandatory-lcp** command enables LCP renegotiation on the LNS.

The **undo mandatory-lcp** command disables LCP renegotiation.

By default, LCP renegotiation is disabled on the LNS.

Format

mandatory-lcp

undo mandatory-lcp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On networks that demand high security, the LNS does not trust the authentication result on remote users performed by the LAC. In this case, enable LCP renegotiation to perform second authentication on remote users. L2TP tunnels can be set up after PPP renegotiation between the LNS and remote users succeeds.

Prerequisites

The **l2tp-group** *l2tp-group* command has been executed to create an L2TP group and enter the L2TP group view.

Precautions

Some PPP clients may not support the second authentication. In this case, the L2TP connection fails when LCP renegotiation is enabled.

When LCP renegotiation and mandatory CHAP authentication are configured simultaneously in an L2TP group, the LCP renegotiation takes effect.

Example

Enable LCP renegotiation.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] mandatory-lcp
```

Related Topics

12.1.10 mandatory-chap

12.1.12 multichassis-mp enable

Function

The **multichassis-mp enable** command enables Multi-Chassis Multilink PPP (MMP) for an L2TP group.

The **undo multichassis-mp enable** command disables MMP for an L2TP group.

By default, MMP is disabled for an L2TP group.

 Copyright © Huawei Technologies Co., Ltd.

Format

multichassis-mp enable

undo multichassis-mp enable

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

MMP allows multiple dialup requests sent by the same branch device to multiple access servers to be terminated in the same bundle through L2TP, which increases bandwidth of the branch device. In MMP scenarios, run the **multichassis-mp enable** command for an L2TP group on the access server (LAC/LNS).

The access server processes ISDN requests from the branch device as follows:

- If an MP bundle has been created, the access server adds ISDN requests to the MP bundle and does not initiate L2TP dialup.
- If no MP bundle is created, the access server initiates L2TP dialup according to user information and searches an MP bundle on another access server.

  If an MP bundle exists on another access server, the access server adds ISDN requests to the MP bundle. If no MP bundle is created, the access server creates an MP bundle and adds ISDN requests to the MP bundle so that ISDN users can connect to the ISDN.

Precautions

Before disabling MMP, ensure that the triggering condition of initiating calls is not specified when the local end serves as the L2TP LAC end. If the triggering condition has been specified, run the **undo start** command to delete the triggering condition.

Example

Enable MMP.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] multichassis-mp enable
```

Related Topics

12.1.11 mandatory-lcp

12.1.13 reset l2tp session

Function

The **reset l2tp session** command forcibly disconnects a specified L2TP session.

Format

reset l2tp session session-id *session-id*

Parameters

Parameter	Description	Value
session-id *session-id*	Specifies the session ID of the L2TP tunnel local end.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 1 to 16 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 ● AR2220, AR2220E, AR2240C: 1 to 512 ● AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A session can be set up only after a tunnel is created successfully. An L2TP session corresponds to a remote dial-up user.

When a security problem occurs or when you locate a fault, run the **reset l2tp session** command to forcibly disconnect the specified L2TP session to force the specified remote user to go offline.

When the remote user calls in again, the session can be reestablished.

Precautions

The **reset l2tp session** command disconnects the specified L2TP session. Exercise caution before you run this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disconnect the L2TP session **1**.

```
<Huawei> reset l2tp session session-id 1
```

Related Topics

12.1.2 display l2tp session

12.1.14 reset l2tp tunnel

Function

The **reset l2tp tunnel** command forcibly disconnects a specified tunnel connection and all sessions in the tunnel.

Format

reset l2tp tunnel { **peer-name** *remote-name* | **local-id** *tunnel-id* }

Parameters

Parameter	Description	Value
peer-name *remote-name*	Specifies the remote tunnel name of the L2TP tunnel.	The value is a string of 1 to 30 characters.
local-id *tunnel-id*	Specifies the remote tunnel ID of the L2TP tunnel.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 1 to 16 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 ● AR2220, AR2220E, AR2240C: 1 to 512 ● AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no L2TP remote user exists, a fault occurs on the network, or the L2TP tunnel is not required, you can use this command to disconnect a tunnel connection and all sessions in the tunnel.

If the specified remote tunnel name does not exist, the command has no effect on the current tunnel connection. If multiple tunnels with the same specified remote tunnel name exist, all these tunnel connections and sessions are disconnected. If a tunnel ID is specified, only the specified tunnel connection is disconnected.

When the remote user calls in again, the tunnel can be reestablished.

Follow-up Procedure

You can change parameters of an L2TP group or delete the L2TP group after the L2TP tunnel is disconnected and before a new L2TP tunnel is established.

Precautions

The **reset l2tp tunnel** command disconnects the specified L2TP tunnel and all sessions in the tunnel. Exercise caution when you run this command.

Example

Disconnect the L2TP tunnel with a remote tunnel named **lac**.

```
<Huawei> reset l2tp tunnel peer-name lac
 Clear tunnel remote name = lac
```

Related Topics

12.1.3 display l2tp tunnel

12.1.15 reset l2tp statistics tunnel

Function

The **reset l2tp statistics tunnel** command resets L2TP packet statistics.

Format

reset l2tp statistics tunnel [**local-id** *tunnel-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
local-id *tunnel-id*	Specifies the local tunnel ID of an L2TP tunnel.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 1 to 16 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, AR2204: 1 to 128 ● AR2220, AR2220E, AR2240C: 1 to 512 ● AR2204XE, AR2204XE-DC, AR2240, AR3200, and AR3600 (using SRUX5) series: 1 to 1024

Views

User view

Default Level

2: Configuration level

Usage Guidelines

To view statistics on L2TP packets within a period of time, you can run the **reset l2tp statistics tunnel** command to clear the existing packet statistics.

Example

Reset L2TP packet statistics of the device.

```
<Huawei> reset l2tp statistics tunnel
  Info: Reset tunnel Statistics success.
```

Reset L2TP packet statistics of tunnel 1.

```
<Huawei> reset l2tp statistics tunnel local-id 1
  Info: Reset tunnel Statistics success, LocID = 1.
```

 Copyright © Huawei Technologies Co., Ltd.

12.1.16 start l2tp

Function

The **start l2tp** command specifies the triggering condition of initiating calls when the local end functions as the LAC.

The **undo start** command deletes the triggering condition.

By default, no triggering condition is configured.

Format

start l2tp ip *ip-address* &<1-4> { **domain** *domain-name* | **fullusername** *user-name* | **interface** *interface-type interface-number* | **vpn-instance** *vpn-instance-name* **fullusername** *user-name* }

start l2tp host *hostname* { **domain** *domain-name* | **fullusername** *user-name* }

undo start

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IP address of the LNS. You can specify a maximum of four IP addresses in the primary and secondary LNSs scenario. The IP addresses are in descending order of priorities, that is, the IP address configured first has the highest priority.	-
host *hostname*	Specifies the LNS domain name.	The value is a string of 1 to 255 case-sensitive characters
domain *domain-name*	Specifies the domain name that triggers the L2TP connection request. **NOTE** Run the **domain** *domain-name* command to create a domain first. Otherwise, the domain name cannot be specified.	The value is a string of 1 to 20 case-insensitive characters.
vpn-instance *vpn-instance-name*	Specifies the VPN instance to which the IP address of the L2TP connection belongs. Route information to LNSs exists in the routing table of the VPN instance.	The value is a string of 1 to 31 case-sensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
fullusername *user-name*	Specifies the full user name that triggers the L2TP connection request.	The value is a string of 1 to 64 case-insensitive characters.
interface *interface-type interface-number*	Specifies the name of an interface that triggers L2TP connection requests. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run the **start l2tp** command on the LAC. L2TP connection requests are triggered on the device in the following situations:

- Triggered based on the domain name. For example, you can specify users with the domain name **huawei.com** as VPDN users.
- Triggered based on the full user name. For example, you can specify users with the full name **user@huawei.com** as VPDN users. L2TP connections are triggered only after the device receives requests from a user with full name **user@huawei.com**.
- The device searches for a route to the LNS based on the VPN instance, such as **VPN1**. The device can initiate an L2TP connection only after an available route is found.
- Triggered based on the interface name. User requests are added to an MP bundle.

  In MMP scenarios, the access server functions as both the LAC and LNS.

After the LAC receives call requests from remote users, it performs the following operations:

- Triggered based on the domain name, VPN attribute, or full user name.

  If the call initiator is a VPDN user, the LAC sends L2TP connection requests to LNSs according to the sequence in which the LNSs were configured. If the LAC receives a response packet from the LNS, this LNS will function as the remote end of the L2TP tunnel. If the LAC receives no response from the LNS, the LAC sends an L2TP connection request to another LNS.

 Copyright © Huawei Technologies Co., Ltd.

- Initiates L2TP connection requests based on the interface name.

  After receiving ISDN requests from users, the access server where no MP bundle is configured initiates an L2TP tunnel setup request to the LNSs and searches for an MP bundle. After receiving a response from the first LNS, the access server uses the LNS as the remote end of the L2TP tunnel and adds user requests to the MP bundle. If the access server does not receive responses from any LNS, it creates an MP bundle and adds user requests to the MP bundle so that users can connect to the ISDN.

Prerequisites

The **multichassis-mp enable** command has been executed to enable MMP when the LAC initiates L2TP connection requests based on the interface name.

Example

Determine VPDN users based on the domain name **huawei.com** with the IP address of the LNS in the headquarters as 10.1.2.3.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] start l2tp ip 10.1.2.3 domain huawei.com
```

Determine VPDN users based on the domain name **huawei.com** with the domain name of the LNS in the headquarters as **www.huawei.com**.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] start l2tp host www.huawei.com domain huawei.com
```

Find a route to the LNS in the routing table of **VPN1** and establish an L2TP connection to the LNS in the headquarters with the IP address 10.1.2.3.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] start l2tp ip 10.1.2.3 vpn-instance vpn1 fullusername huawei
```

In an MMP scenario, initiate L2TP connection requests to other access servers according to Serial1/0/0.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] multichassis-mp enable
[Huawei-l2tp1] start l2tp ip 10.1.2.3 interface serial 1/0/0
```

12.1.17 tunnel authentication

Function

The **tunnel authentication** command enables L2TP tunnel authentication.

The **undo tunnel authentication** command disables L2TP tunnel authentication.

By default, tunnel authentication is enabled.

Format

tunnel authentication

undo tunnel authentication

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure data security, L2TP tunnel authentication is enabled by default. In case of network connectivity test or receiving a connection request sent by an unknown remote end, disable L2TP tunnel authentication. It is recommended that you enable L2TP tunnel authentication.

The tunnel authentication request can be initiated by the LAC or the LNS. As soon as one end is enabled with tunnel authentication, the identity authentication is performed in the tunnel setup process. The tunnel can be set up only if the passwords of both ends are the same and not empty. Otherwise, the local end automatically disconnects itself from the tunnel. If tunnel authentication is disabled on both ends, the authentication password does not take effect.

Follow-up Procedure

Run the **tunnel password** command to configure an authentication password. Configure the same authentication password on the LAC and LNS.

Precautions

By default, tunnel authentication is enabled, but no authentication password is configured. When the default configuration is used to set up an L2TP tunnel, tunnel authentication fails and the tunnel cannot be set up.

Example

Disable tunnel authentication.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] undo tunnel authentication
```

Related Topics

12.1.20 tunnel password

12.1.18 tunnel avp-hidden

Function

The **tunnel avp-hidden** command configures Attribute Value Pair (AVP) data to be transmitted in cipher text.

 Copyright © Huawei Technologies Co., Ltd.

The **undo tunnel avp-hidden** command restores the default transmission mode of AVP data.

By default, AVP data is transmitted in plain text.

Format

tunnel avp-hidden

undo tunnel avp-hidden

Parameters

None

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AVP data carries some parameters of the L2TP protocol. For the purpose of security, run this command to configure AVP data to be transmitted in cipher text.

Prerequisites

The following operations have been performed:

1. Run the **l2tp-group** command to create an L2TP group and enter the L2TP group view.
2. Run the **tunnel authentication** command to enable tunnel authentication function. By default, tunnel authentication is enabled.
3. Run the **tunnel password** command to configure the authentication password.

Precautions

If AVP data is transmitted in plain text, the leakage of the user name and password occurs when L2TP packets are intercepted.

When you configure the AVP parameter encryption, enable tunnel authentication on the LAC and LNS, and configure the same authentication password on the two ends.

Example

Configure AVP data to be transmitted in cipher text.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel authentication
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-l2tp-1] tunnel password cipher huawei
[Huawei-l2tp-1] tunnel avp-hidden
```

12.1.19 tunnel name

Function

The **tunnel name** command specifies the local name of a tunnel.

The **undo tunnel name** command restores the default tunnel name.

By default, the local name of a tunnel is the device name.

Format

tunnel name *tunnel-name*

undo tunnel name

Parameters

Parameter	Description	Value
tunnel-name	Specifies the name of the local end of a tunnel.	The value is a string of 1 to 30 case-sensitive characters.

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

When you create an L2TP group, the local name of a tunnel is initialized to be the device name. Run the **tunnel name** command to specify another name as the local name. When the configured local tunnel name is the same as the initial host name of the device, the configured local tunnel name will take effect but will not be displayed during the query of configuration.

You can create multiple L2TP groups and establish multiple L2TP tunnels on a device. Specify a tunnel name for each tunnel to differentiate the tunnels. The tunnel name of the LAC end must be specified for the LNS to accept a connection request. It is recommended that you configure the tunnel name on the LAC end.

Example

Set the local tunnel name to **huawei**.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel name huawei
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.1.1 allow l2tp

12.1.20 tunnel password

Function

The **tunnel password** command specifies a password for tunnel authentication.

The **undo tunnel password** command deletes the password.

By default, tunnel authentication is enabled, but no authentication password is configured.

Format

tunnel password { **simple** | **cipher** } *password*

undo tunnel password

Parameters

Parameter	Description	Value
simple	Indicates the password in plain text. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the password in cipher text. The password is displayed in cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the password for tunnel authentication.	The password is a string of case-sensitive characters. The password cannot contain command line characters such as spaces and question marks (?). • If **simple** is specified, the password must be in plain text and contain 1 to 16 characters. • If **cipher** is specified, the password can be either in cipher or plain text, depending on what is entered. The password in plain text contains 1 to 16 characters, such as 1234567. The password in cipher mode must be a string of 24/32/48 bytes, for example, _(TT8F]Y\5SQ=^Q`MAF4<1!!.

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can decide whether to enable tunnel authentication before creating the tunnel connection. After tunnel authentication is enabled, run the **tunnel password** command to configure an authentication password. To ensure tunnel security, it is recommended that you enable tunnel authentication.

Prerequisites

The **l2tp-group** command has been executed to create an L2TP group and enter the L2TP group view.

Tunnel authentication has been enabled by running the **tunnel authentication** command. By default, tunnel authentication is enabled.

Precautions

If tunnel authentication is enabled on the LAC or the LNS, it must also be enabled on the other end. Configure the same authentication password on the LAC and LNS.

Example

Set the password for tunnel authentication to **huawei** in cipher text.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel password cipher huawei
```

Related Topics

12.1.17 tunnel authentication

12.1.21 tunnel timer hello

Function

The **tunnel timer hello** command sets the interval for sending Hello packets.

The **undo tunnel timer hello** command restores the interval to the default value.

By default, Hello packets are sent every 60s.

Format

tunnel timer hello *interval*

undo tunnel timer hello

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending Hello packets.	The value is an integer that ranges from 0 to 1000, in seconds. If the value is 0, no Hello packet is sent.

Views

L2TP group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

L2TP uses Hello packets to check tunnel connectivity. The LAC and LNS periodically send Hello packets to each other. If no response packet is received within a specified period, they retransmit Hello packets. If Hello packets are retransmitted for five times but no response packet is received, the L2TP tunnel is disconnected.

When the network is unstable, set a shorter interval for sending Hello packets to detect tunnel status. When the network is stable, set the interval to a longer value. Different intervals can be set on the LNS and LAC.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

Hello packets are sent periodically, which increases network burdens. If the interval is set to a smaller value, network burdens increase.

Example

Set the interval for sending Hello packets to 99s.

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp-1] tunnel timer hello 99
```

Related Topics

12.1.9 l2tp-group

12.2 L2TPv3 Configuration Commands

12.2.1 encapsulation l2tpv3

Function

The **encapsulation l2tpv3** command sets the tunnel type to static L2TPv3.

The **undo encapsulation l2tpv3** command deletes the specified tunnel type.

By default, the tunnel type is not specified.

Format

encapsulation l2tpv3 [**static**]

undo encapsulation l2tpv3

Parameters

Parameter	Description	Value
static	Sets the tunnel type to static L2TPv3.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want the device to directly forward data without packet negotiation, run the **encapsulation l2tpv3** command to set the tunnel type to static L2TPv3.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command on the LCCE. A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.

Precautions

The **encapsulation l2tpv3** and **svpn-proposal** commands cannot be configured simultaneously. A tunnel can be bound only to one protocol.

If you run the **undo encapsulation l2tpv3** command, cookie and session of the tunnel, the tunnel source address and the tunnel destination address, as well as the binding between a tunnel and an AC configured using the **link-bridge** command.

Example

Set the tunnel type to static L2TPv3.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
```

Related Topics

12.2.2 l2tpv3 enable
12.3.21 tunnel-protocol

12.2.2 l2tpv3 enable

Function

The **l2tpv3 enable** command enables the L2TPv3 function globally.

The **undo l2tpv3 enable** command disables the L2TPv3 function.

By default, the L2TPv3 function is disabled.

Format

l2tpv3 enable

undo l2tpv3 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an enterprise wants Layer 2 data to be transparently transmitted on a Layer 3 network without changing the IP network, the L2TPv3 service can be deployed to implement communication between branches or between the headquarters and branches.

Precautions

The L2TPv3 function takes effect only after you run the **l2tpv3 enable** command.

Example

Enable the L2TPv3 function globally.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
```

12.2.3 l2tpv3 local cookie

Function

The **l2tpv3 local cookie** command configures the local cookie key.

The **undo l2tpv3 local cookie** command deletes the local cookie key.

By default, the local cookie key is not configured.

Format

l2tpv3 local cookie { **key cipher** *cipher* | **length 4 plain lower-value** *local-lower-value1* | **length 8 plain lower-value** *local-lower-value2* **upper-value** *local-high-value* }

undo l2tpv3 local cookie

Parameters

Parameter	Description	Value
key cipher *cipher*	Specifies the cookie in cipher text. The local cookie is saved in cipher text. **NOTE** If the parameter is not specified, the cookie is saved in plain text which is not secure. You are advised to select **key cipher** to save the cookie in cipher text.	The value is a string of 1 to 8 case-sensitive bytes without spaces. If the cookie is in cipher text, the key is a string of 1 to 8 bytes and the encrypted password contains 48 bytes. If the cookie is in plain text, the plain-text password contains 4 or 8 bytes.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
length 4 plain lower-value *local-lower-value1*	Specifies a 4-byte cookie in plain text.	The value is a decimal integer that ranges from 0 to 4294967295.
length 8 plain lower-value *local-lower-value2*	Specifies the rightmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.
upper-value *local-high-value*	Specifies the leftmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 local cookie** command is used to configure the local cookie key.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

The **l2tpv3 local cookie** configured on the local device must be the same as the **l2tpv3 remote cookie** configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the local cookie key to **abc** in cipher text.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
```

```
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 local cookie key ciper abc
```

Related Topics

12.2.5 l2tpv3 remote cookie

12.2.4 l2tpv3 local session-id

Function

The **l2tpv3 local session-id** command configures the local session ID.

The **undo l2tpv3 local session-id** command deletes the local session ID.

By default, the local session ID is not configured.

Format

l2tpv3 local session-id *local-session-id*

undo l2tpv3 local session-id

Parameters

Parameter	Description	Value
local-session-id	Specifies the local session ID.	The value is a decimal integer that ranges from 1 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 local session-id** command is used to configure the local session ID.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

- The local session IDs are different for different tunnel interfaces.
- The *local-session-id* configured on the local device must be the same as the *remote session-id* configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the local session ID to 2.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 local session-id 2
```

Related Topics

12.2.6 l2tpv3 remote session-id

12.2.5 l2tpv3 remote cookie

Function

The **l2tpv3 remote cookie** command configures the remote cookie key.

The **undo l2tpv3 remote cookie** command deletes the remote cookie key.

By default, the remote cookie key is not configured.

Format

l2tpv3 remote cookie { **key cipher** *cipher* | **length 4 plain lower-value** *remote-lower-value1* | **length 8 plain lower-value** *remote-lower-value2* **upper-value** *remote-high-value* }

undo l2tpv3 remote cookie

Parameters

Parameter	Description	Value
key cipher *cipher*	Specifies the cookie in cipher text. The remote cookie is saved in cipher text. **NOTE** If the parameter is not specified, the cookie is saved in plain text which is not secure. You are advised to select **key cipher** to save the cookie in cipher text.	The value is a string of 1 to 8 case-sensitive bytes without spaces. If the cookie is in cipher text, the key is a string of 1 to 8 bytes and the encrypted password contains 48 bytes. If the cookie is in plain text, the plain-text password contains 4 or 8 bytes.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
length 4 plain lower-value *remote-lower-value1*	Specifies a 4-byte key in plain text.	The value is a decimal integer that ranges from 0 to 4294967295.
length 8 plain lower-value *remote-lower-value2*	Specifies the rightmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.
upper-value *remote-high-value*	Specifies the leftmost four bytes in the 8-byte key.	The value is a decimal integer that ranges from 0 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 remote cookie** command is used to configure the remote cookie key.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

The **l2tpv3 remote cookie** configured on the local device must be the same as the **l2tpv3 local cookie** configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the remote cookie key to **abc** in cipher text.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
```

```
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 remote cookie key ciper abc
```

Related Topics

12.2.3 l2tpv3 local cookie

12.2.6 l2tpv3 remote session-id

Function

The **l2tpv3 remote session-id** command configures the remote session ID.

The **undo l2tpv3 remote session-id** command deletes the remote session ID.

By default, the remote session ID is not specified.

Format

l2tpv3 remote session-id *remote-session-id*

undo l2tpv3 remote session-id

Parameters

Parameter	Description	Value
remote-session-id	Specifies the remote session ID.	The value is a decimal integer that ranges from 1 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. Ensure that parameters of a local tunnel interface are complete and match the parameters configured on the remote device. The **l2tpv3 remote session-id** command is used to configure the remote session ID.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The *remote session-id* configured on the local device must be the same as the *local-session-id* configured on the remote device. Traffic can be forwarded through a tunnel when they are the same. If they are different, traffic cannot be forwarded even though a tunnel is established.

Example

Set the remote session ID to 2.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] l2tpv3 remote session-id 2
```

Related Topics

12.2.4 l2tpv3 local session-id

12.2.7 link-bridge

Function

The **link-bridge** command binds an AC interface to a tunnel interface.

The **undo link-bridge** command unbinds an AC interface from a tunnel interface.

By default, an AC interface is not bound to a tunnel interface.

Format

link-bridge tunnel *slot-number* [**vc-id** *vc-id*] { **tagged** | **raw** }

undo link-bridge tunnel *slot-number*

Parameters

Parameter	Description	Value
tunnel *slot-number*	Specifies a tunnel interface bound to an AC interface.	-
tagged	Reserves the service-delimiting tag (SD-tag) of a packet. This parameter can be set only if the AC is an Ethernet link.	-
raw	Deletes the SD-tag of a packet. This parameter can be set only if the AC is an Ethernet link.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vc-id *vc-id*	Specifies a vc-id.	The value is an integer that ranges from 1 to 4294967295.

Views

AC interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The LCCE devices can transparently transmit only Layer 3 packets when they are connected through an IP network. After Layer 2 packets enter an AC interface on an LCCE device, you can run the **link-bridge** command to bind the AC interface to a tunnel interface. After that, the AC interface encapsulates the Layer 2 packets based on parameters for the tunnel interface and transparently transmits the packets over the IP network based on routing information.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

- The link bridge function can be configured only on the Layer 3 interface.
- An AC interface can be bound only to one tunnel interface.
- After you run the **link-bridge** command to bind an AC interface to a tunnel interface, the physical status of the interfaces become Standby. After the tunnel is established, the Standby status is changed to Up.

Example

Bind Ethernet0/0/1 and Tunnel0/0/1 in tagged mode.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] quit
[Huawei] interface ethernet0/0/1
[Huawei-Ethernet0/0/1] link-bridge tunnel 0/0/1 tagged
```

 Copyright © Huawei Technologies Co., Ltd.

12.2.8 tunnel-destination

Function

The **tunnel-destination** command configures a destination address for a tunnel interface.

The **undo tunnel-destination** command deletes the destination address of a tunnel interface.

By default, no destination address is configured for a tunnel interface.

Format

tunnel-destination [**vpn-instance** *vpn-instance*] *dest-ip-address*

undo tunnel-destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. **NOTE** You are advised to use the existing VPN instance; otherwise, a tunnel cannot be established.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks ("), the string can contain spaces.
dest-ip-address	Specifies the destination address for a tunnel.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. After creating the tunnel interfaces, run the **tunnel-destination** command to configure destination addresses for the tunnel interfaces.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.

 Copyright © Huawei Technologies Co., Ltd.

- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

- The destination IP address of the local device must be a reachable IP address and be the same as the IP address of the PW interface on the remote device (the source IP address of the remote device).
- The source IP addresses, destination IP addresses, and VPN instances for different tunnel interfaces cannot be exactly the same.
- If you want to set **tunnel-destination** to **vpn-instance**, run the **ip vpn-instance** command to create a VPN instance first. A tunnel cannot be established if a VPN instance that does not exist is used.

Example

Set the destination address for Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel 0/0/1] tunnel-protocol svpn
[Huawei-Tunnel 0/0/1] encapsulation l2tpv3
[Huawei-Tunnel 0/0/1] tunnel-destination 10.1.1.2
```

Set the destination address for Tunnel0/0/1 to 10.1.1.1 of vpn1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] tunnel-destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.2.9 tunnel-source

12.2.9 tunnel-source

Function

The **tunnel-source** command configures a source address for a tunnel interface.

The **undo tunnel-source** command deletes the source address of a tunnel interface.

By default, no source address is configured for a tunnel interface.

Format

tunnel-source [*source-ip-address* | *interface-type interface-number*]

undo tunnel-source

Parameters

Parameter	Description	Value
source-ip-address	Specifies the source IP address for a tunnel interface.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the interface type for a tunnel interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	Only the Ethernet, GigabitEthernet, and VLANIF interfaces are supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before establishing a tunnel, you need to create tunnel interfaces. After creating the tunnel interfaces, run the **tunnel-source** command to configure source addresses for the tunnel interfaces.

Prerequisites

- The L2TPv3 function has been enabled globally using the **l2tpv3 enable** command.
- A tunnel protocol has been configured on tunnel interfaces using the **tunnel-protocol** command.
- The tunnel type has been set to static L2TPv3 using the **encapsulation l2tpv3** command.

Precautions

- The source IP address of a tunnel interface must be the same as the IP address of the PW interface on the local device. The IP address can be directly configured or be obtained from the Layer 3 interface for which an IP address has been configured.
- The source IP address of the local device must be the same as the destination IP address of the remote device.
- The source IP addresses, destination IP addresses, and VPN instances for different tunnel interfaces cannot be exactly the same.

Example

Set the source address for Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel 0/0/1] tunnel-protocol svpn
[Huawei-Tunnel 0/0/1] encapsulation l2tpv3
[Huawei-Tunnel 0/0/1] tunnel-source 10.1.1.1
```

Set the source address of Tunnel0/0/1 to the IP address of Ethernet0/0/1.

```
<Huawei> system-view
[Huawei] l2tpv3 enable
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] encapsulation l2tpv3
[Huawei-Tunnel0/0/1] tunnel-source ethernet0/0/1
```

Related Topics

12.2.8 tunnel-destination

12.3 GRE Configuration Commands

12.3.1 description (tunnel interface view)

Function

The **description** command sets the description of the current tunnel interface.

The **undo description** command deletes the description of the current tunnel interface.

By default, the description of a tunnel interface is "HUAWEI, AR Series, Tunnel *interface-number* Interface".

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a tunnel interface.	The value is a string of 1 to 242 case-sensitive characters, with spaces supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After using the **interface tunnel** command to create a tunnel interface, you can run the **description** command to configure a description of the tunnel interface to facilitate later query.

To check the description of a tunnel interface, run the **display this interface** command in the tunnel interface view or the **display interface tunnel** command.

Example

Configure the description of Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] description This is a tunnel from 10.1.1.1 to 10.2.2.2
```

Delete the description of Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] undo description
```

Related Topics

12.3.10 interface tunnel

12.3.3 display interface tunnel

12.3.2 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE tunnel or IPSec tunnel, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a GRE, IPv4 over IPv6, IPSec, MPLS TE, manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, MPLS TE, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. Normally, two tunnel interfaces in a system cannot have the same encapsulation mode, source address, and destination address.

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

On the IPSec, IPv6 over IPv4, IPv4 over IPv6, or GRE tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface by the **source** command, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Set the destination address of the GRE tunnel Tunnel 0/0/1 to 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] destination 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

Set the destination address of the GRE tunnel Tunnel 0/0/0 to 10.1.1.1 that belongs to vpn1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre
[Huawei-Tunnel0/0/0] destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.3.10 interface tunnel

12.3.18 source

12.3.21 tunnel-protocol

12.3.3 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the details of the tunnel interface.

```
<Huawei> display interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Tunnel0/0/2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1), destination 10.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-08-09 18:53:47
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    15 seconds input rate 0 bits/sec, 0 packets/sec
    15 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
    Input bandwidth utilization  : 0%
    Output bandwidth utilization : 0%
```

Table 12-8 Description of the display interface tunnel command output

Item	Description
Tunnel0/0/2 current state	Physical layer status of the Tunnel0/0/2 interface: ● UP: The interface is in normal state. ● Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status of the Tunnel0/0/2 interface: ● UP: The link layer protocol of the tunnel interface works normally. ● DOWN: The link layer protocol of the tunnel interface is abnormal.
Description	Description of the tunnel interface.
Route Port,The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Internet protocol processing: disabled	IP protocol is disabled.
Encapsulation is TUNNEL	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1)	The source address of the tunnel is 10.10.10.1. That is, the IP address of the GigabitEthernet 0/0/1 interface sending packets at the source side is 10.10.10.1.
destination	Destination address of the tunnel.
Tunnel protocol/transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● IPSec: indicates tunnel mode of IPSec to protect data stream. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● SVPN: encapsulates packets into SVPN packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive disabled	The keepalive function of GRE is not enabled.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
300 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
300 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
15 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface during the last query period.
15 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface during the last query period.
0 packets input, 0 bytes 0 input error	Total packets and bytes received on the interface and the total number of defective packets.
0 packets output, 0 bytes 0 output error	Total packets and bytes sent through the interface and the total number of defective packets.
Input bandwidth utilization	Input bandwidth usage.
Output bandwidth utilization	Output bandwidth usage.

Related Topics

12.3.11 keepalive

12.3.4 display keepalive packets count

Function

The **display keepalive packets count** command displays the number of Keepalive packets and Keepalive response packets sent and received by the local GRE tunnel interface.

Format

display keepalive packets count

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a tunnel is a GRE tunnel, you can enable the Keepalive function to check the link connectivity. If the function is disabled, service packets are continuously forwarded through this tunnel interface when the link fails, resulting in a tunnel black hole and loss of service data.

The **display keepalive packets count** command allows you to view the number of Keepalive packets and Keepalive response packets sent and received through the GRE tunnel interface.

Prerequisites

1. The tunnel interface view has been displayed using the **interface tunnel** command.
2. The tunnel type has been set to GRE using the **tunnel-protocol gre** command.
3. The Keepalive function has been enabled for the GRE tunnel using the **keepalive** command.

Follow-up Procedure

Run the **reset keepalive packets count** command to reset the Keepalive packet statistics.

Example

View the Keepalive packet statistics of GRE tunnel interface 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] keepalive
[Huawei-Tunnel0/0/1] display keepalive packets count
Send 10 keepalive packets to peers, Receive 10 keepalive response packets from
peers
Receive 8 keepalive packets from peers, Send 8 keepalive response packets to
peers.
```

Table 12-9 Description of the display keepalive packets count command output

Item	Description
Send 10 keepalive packets to peers	Ten Keepalive packets are sent to the remote end.
Receive 10 keepalive response packets from peers	Ten Keepalive response packets are received from the remote end.
Receive 8 keepalive packets from peers	Eight Keepalive packets are received from the remote end.
Send 8 keepalive response packets to peers	Eight Keepalive response packets are sent to the remote end.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.3.11 keepalive

12.3.17 reset keepalive packets count

12.3.5 display tunnel-info

Function

The **display tunnel-info** command displays the tunnel information.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display tunnel-info { **tunnel-id** *tunnel-id* | **all** | **statistics** [**slots**] }

Parameters

Parameter	Description	Value
tunnel-id *tunnel-id*	Specifies the tunnel ID. If the specified ID does not exist, the system prompts errors.	A hexadecimal integer ranging from 1 to FFFFFFFE.
all	Displays information about all the tunnels.	-
statistics	Displays statistics about all tunnels.	-
slots	Displays tunnel statistics in the order of interface boards.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display tunnel-info all** command displays existing tunnel IDs, tunnel types, destination IP addresses, and Token information about all tunnels.

The **display tunnel-info tunnel-id** *tunnel-id* command displays detail information about a tunnel when you only know the tunnel ID.

The **display tunnel-info statistics** command displays the number of tunnels configured on the router.

 Copyright © Huawei Technologies Co., Ltd.

Example

View information about the GRE tunnel.

```
<Huawei> display tunnel-info tunnel-id 10003
Tunnel ID:                0x10003
Tunnel Token:               3
Type:                     gre
Destination:                10.1.1.1
Out Slot:                 0
Instance ID:                0
Interface:                Tunnel0/0/1
```

Table 12-10 Description of the display tunnel-info command output

Item	Description
Tunnel ID	Tunnel ID in hexadecimal notation that is assigned by the system.
Tunnel Token	Token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.
Type	Type of a tunnel, such as GRE, LSP, or CR-LSP. The command output varies according to the tunnel type.
Destination	Destination IP address of the tunnel.
Out Slot	Number of the slot that is used when the router sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.

Display all tunnel information.

```
<Huawei> display tunnel-info all
* -> Allocated VC Token
Tunnel ID          Type              Destination          Token
-----------------------------------------------------------------------
0x1800800          lsp               3.3.3.3              0
0x1800801          lsp               2.2.2.2              1
0x41804bb8         lsp               192.168.2.0          3000
```

Display tunnel statistics.

```
<Huawei> display tunnel-info statistics
LSP/32bit LSP :                    3/3
GRE :                              0
CRLSP :                            2
LOCAL IFNET :                      0
MPLS LOCAL IFNET :                 0
VPN QOS LSP :                      0
Reserved :                         0
```

Table 12-11 Description of the display tunnel-info statistics command output

Item	Description
LSP/32bit LSP	Number of LSP tunnels created in the system view/Number of LSP tunnels triggered by the route of host with the 32-bit mask address.
GRE	Number of tunnel IDs allocated to the GRE tunnels.
CRLSP	Number of tunnel IDs allocated to the CR-LSP tunnels.
LOCAL IFNET	Number of tunnels used by the VPN internal module.
MPLS LOCAL IFNET	Number of tunnels used by the MPLS internal module.
VPN QOS LSP	Number of the tunnel ID allocated to the LSP used in VPN QoS.
Reserved	Number of the tunnel ID allocated to the product.

Display tunnel statistics in the order of interface boards.

```
<Huawei> display tunnel-info statistics slots
-----------------------------------------------------------------
Slot            LSP     CR      GRE     LCL     MPLS-L  VPN
Num                     LSP             IFNET   IFNET   QOS
-----------------------------------------------------------------
0               0       0       0       0       0       0
Logic Slot: 0                   Total:  0
-----------------------------------------------------------------
TOTAL           0       0       0       0       0       0
                                Total:  0
-----------------------------------------------------------------
```

Table 12-12 Description of the display tunnel-info statistics slots command output

Item	Description
Slot Num	Slot number used by the device to send packets.
LSP	Total LSP tunnels set up by the device.
CR LSP	Number of CR-LSPs created on the device.
GRE	Number of GRE tunnels created on the device.
LCL IFNET	Number of tunnels used by the VPN module.
MPLS-L IFNET	Number of tunnels used by the MPLS module.
VPN QOS	Number of tunnels used for VPN QoS.

12.3.6 gre checksum

Function

The **gre checksum** command enables the end-to-end checksum function between both ends of a GRE tunnel.

The **undo gre checksum** command disables the end-to-end checksum function.

By default, the checksum function is disabled on the GRE tunnel.

Format

gre checksum

undo gre checksum

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure an end-to-end check between both ends of a GRE tunnel to improve the GRE tunnel security. This mechanism prevents the device from incorrectly identifying and receiving invalid packets.

You can configure the checksum function on the two ends of the tunnel as required to determine whether to trigger the checksum function.

Prerequisites

The tunnel interface view has been displayed using the **interface tunnel** command.

The tunnel type has been set to GRE using the **tunnel-protocol gre** command.

Precautions

After this command is executed, the integrity of packets can be checked.

If the checksum function is configured on the local end:

- The local end calculates the checksum according to the GRE header and payload.
- The local end sends a packet containing the checksum to the remote end.

 Copyright © Huawei Technologies Co., Ltd.

- The remote end calculates the checksum based on the packet and then compares the result with the checksum contained in the packet.
  - If the two checksum values are the same, the packet is processed.
  - If the two checksum values are different, the packet is discarded.

If the checksum function is enabled on the local end and disabled on the remote end, the local end does not perform checksum on received packets, but performs checksum on locally transmitted packets. If the checksum function is disabled on the local end and enabled on the remote end, the local end performs checksum on received packets, but does not perform checksum on locally transmitted packets.

Example

Enable checksum on the GRE Tunnel0/0/1 on the local device.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] gre checksum
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.3.7 gre df-bit

Function

The **gre df-bit** command specifies the don't fragment (DF) flag bit for GRE packets.

By default, the DF flag bit for GRE packets uses the clear mode.

Format

gre df-bit { **clear** | **set** | **copy** }

Parameters

Parameter	Description	Value
clear	Sets the DF flag bit to 0, indicating that packets can be fragmented.	-
set	Sets the DF flag bit to 1, indicating that packets cannot be fragmented.	-
copy	Uses the DF flag bit of original packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After original packets are encapsulated using GRE, the packet length may exceed the maximum transmission unit (MTU) allowed by the device outbound interface. In this case, you need to fragment the packets by running the **gre df-bit clear** command to prevent packet loss.

Precautions

If you run the **gre df-bit** command multiple times, only the latest configuration takes effect.

Example

Set the DF flag bit for GRE packets to clear.

```
<Huawei> system-view
[Huawei] gre df-bit clear
```

12.3.8 gre key

Function

The **gre key** command sets the key number of a GRE tunnel.

The **undo gre key** command deletes the key number of a GRE tunnel.

By default, the GRE key number is not configured.

Format

gre key { **plain** *key-number* | [**cipher**] *plain-cipher-text* }

undo gre key

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
plain *key-number*	Specifies a plaintext key. **NOTICE** If **plain** is selected, the key is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the key in cipher text.	The value is an integer that ranges from 0 to 4294967295.
[**cipher**] *plain-cipher-text*	Specifies that a ciphertext key is displayed.	You can specify a plaintext key (integer) ranging from 0 to 4294967295 or a ciphertext key of 32 or 48 bits.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure key numbers for both ends of a GRE tunnel to improve GRE tunnel security. This security mechanism ensures that a device accepts only packets sent from the valid tunnel interface and discards invalid packets.

Prerequisites

The tunnel interface view has been displayed using the **interface tunnel** command.

The tunnel type has been set to GRE using the **tunnel-protocol gre** command.

Precautions

Packets pass authentication only when the key numbers set on both ends of the tunnel are consistent. Otherwise, the packets are discarded.

When you run the **gre key** command several times, the latest configuration overrides the previous configurations.

Example

Configure the GRE key number for the ends of a tunnel is 123.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] gre key cipher 123
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.3.10 interface tunnel
12.3.21 tunnel-protocol

12.3.9 gre map virtual-ethernet forward-broadcast disable

Function

The **gre map virtual-ethernet forward-broadcast disable** command disables a VE interface from forwarding broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

The **undo gre map virtual-ethernet forward-broadcast disable** command enables a VE interface to forward broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

By default, a VE interface can forward broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

Format

gre map virtual-ethernet forward-broadcast disable

undo gre map virtual-ethernet forward-broadcast disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If branch CPE fails to obtain the MAC address of the HQ CPE, it will send broadcast, multicast, and unknown unicast packets to the VE interface bound to the tunnel interface of the HQ CPE. The VE interface then forwards the packets to other CPEs in the same VLAN. This consumes large network bandwidth, increases the workload of the HQ CPE, and may lead to drop of normal packets. To prevent this problem, you can configure the **gre map virtual-ethernet forward-broadcast disable** command on the HQ CPE to disable the VE interface from forwarding broadcast, multicast, and unknown unicast packets to other CPEs in the same VLAN.

Example

Disable a VE interface from forwarding broadcast, multicast, and unknown unicast packets to devices in the same VLAN.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] gre map virtual-ethernet forward-broadcast disable
```

12.3.10 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface with format "slot/subslot/number".	The slot, subslot, or interface number is an integer. The value range of the slot or subslot number varies according to the device type. The value of the interface number ranges. ● AR100&AR120&AR150&AR160&AR200 series: 0 to 255 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204E, AR2204E-D: 0 to 255 ● AR2220, AR2220E: 0 to 1023 ● AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80), AR2240C, AR3200 (using SRU40, SRU60, or SRU80) series: 0 to 2047 ● AR2240 (using SRU200, or SRU200E, or SRU400), AR3200 (using SRU200, or SRU200E, or SRU400) series: 0 to 4095 ● AR3600 (using SRUX5) series: 0 to 4095

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- IPSec
- GRE
- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPSec, IPv4 over IPv6, or IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

If a tunnel is being used, services transmitted over the tunnel will be affected after the tunnel interface is deleted. Exercise caution when running the **undo interface tunnel** command.

Example

Create a tunnel interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1]
```

12.3.11 keepalive

Function

The **keepalive** command enables the Keepalive function of GRE tunnels.

The **undo keepalive** command disables the Keepalive function of GRE tunnels.

By default, the Keepalive function of a GRE tunnel is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

keepalive [**period** *period* [**retry-times** *retry-times*]]

undo keepalive

Parameters

Parameter	Description	Value
period *period*	Specifies the interval for sending Keepalive packets.	The value is an integer that ranges from 1 to 32767, in seconds. The default value is 5 seconds.
retry-times *retry-times*	Specifies the parameter of the unreachable counter.	The value is an integer that ranges from 1 to 255. The default value is 3.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you configure a tunnel policy and set the VPN tunnel type to GRE, you need to enable the Keepalive function. After Keepalive is enabled, the VPN cannot choose a tunnel with an unreachable remote end, preventing data loss.

When Keepalive is disabled on a local end, the tunnel interface status of the local end might be Up even if the remote end is unreachable. After Keepalive is enabled on the local end, the tunnel interface status of the local end changes to Down if the remote end is unreachable. Therefore, when the remote end is unreachable, the VPN cannot choose the GRE tunnel, preventing data loss.

The Keepalive function takes effect uni-directionally. To enable the Keepalive function on both ends of a tunnel, run the **keepalive** command on each end of the tunnel. The Keepalive configuration takes effect on one end even if the function is disabled on the other end. However, it is recommended that you enable the Keepalive function on both ends.

After the Keepalive function is enabled on a GRE tunnel, the tunnel periodically sends Keepalive packets. The unreachable counter increases by one each time a packet is sent. If no response packet is received when the value of the counter reaches the value of *retry-times*, the remote end is considered unreachable.

Prerequisites

The **keepalive** command can be used only when the encapsulation mode has been set to GRE on an interface.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When you run the **keepalive** command several times, the latest configuration overrides the previous configurations.

Follow-up Procedure

Run the **display keepalive packets count** command to display the number of Keepalive packets and Keepalive response packets sent and received by the local GRE tunnel interface.

Example

Enable the Keepalive function for the GRE tunnel using default parameters.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] keepalive
```

Enable the Keepalive function for the GRE tunnel. Set the interval for sending Keepalive packets to 12 seconds and **retry-times** to 4.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] keepalive period 12 retry-times 4
```

Related Topics

12.3.4 display keepalive packets count

12.3.17 reset keepalive packets count

12.3.12 link-bridge

Function

The **link-bridge** command binds an inbound interface to an outbound interface, so that packets received from the specified inbound interface can only be sent through the specified outbound interface.

The **undo link-bridge** command deletes the binding between inbound and outbound interfaces.

By default, inbound and outbound interfaces are not bound.

Format

link-bridge *tag-id* **interface** *interface-type interface-number* **out-interface** *interface-type interface-number* [**untagged** | **tagged** *vlan-id*]

undo link-bridge *tag-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tag-id	Indicates the tag ID of a link bridge.	The value is an integer that ranges from 1 to 65535.
interface *interface-type interface-number*	Indicates the inbound interface of the link bridge. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	For FR, HDLC, or PPP packets, the inbound interface of a link bridge can only be a serial interface. For Ethernet packets, the inbound interface of a link bridge can only be an Ethernet, a GE, a XGE, Ethernet sub-interface, GE sub-interface, XGE sub-interface, or a VLANIF.
out-interface *interface-type interface-number*	Indicates the outbound interface of the link bridge. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	Currently, the outbound interface of a link bridge can only be a tunnel interface.
untagged	Indicates that Ethernet packets do not carry tags.	-
tagged *vlan-id*	Specifies that the AR adds a VLAN tag to Ethernet packets before sending them over a tunnel.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customers want to use GRE to transparently transmit FR, HDLC, PPP, or Ethernet packets over networks of a different network layer protocol, such as the IPv4 network. To transmit FR, HDLC, PPP, or Ethernet packets over a GRE tunnel, they need to configure the link bridge function to bind a serial, an Ethernet, a GE, a XGE, or a VLANIF interface with a tunnel interface, so that packets received from the serial, Ethernet, GE, XGE, or VLANIF interface can be directly sent out from the tunnel interface bound to it.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A serial, Ethernet, GE, XGE, or VLANIF interface is available and a tunnel interface has been configured using the **interface** command.

Precautions

- After you configure this command, the protocol status of the inbound interface which is a serial interface turns Down and network-layer configurations on the inbound interface do not take effect. The inbound interface only functions as a bridge.
- After link bridge is bound to an interface, the interface does not support QoS. The inbound interface to which link bridge is bound supports traffic policy, traffic policing, traffic statistics collection, and mapping between 802.1p and DSCP priorities.
- Two link bridges must be configured with different tag IDs. The tag ID of a link bridge must be globally unique. If the tag ID of two link bridges is the same, an error message is displayed.
- Only one link bridge can be configured on a physical interface. If two link bridges are configured on the same physical interface, an error message is displayed.
- Only one link bridge can be configured on a tunnel interface. If two link bridges are configured on the same tunnel interface, an error message is displayed.
- If you specify the untagged mode, Ethernet packets transmitted over a GRE tunnel do not contain VLAN tags; otherwise, packets contain VLAN tags. You can determine whether to configure the untagged mode based on your actual networking to ensure normal traffic transmission over a tunnel. The following table describes the packet transmission rules.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
Layer 2 Ethernet interface	From an Ethernet interface to a tunnel interface	The interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.

 Copyright © Huawei Technologies Co., Ltd.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
	From a tunnel interface to an Ethernet interface	The interface transparently transmits the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface transparently transmits the packet.
Layer 3 Ethernet interface	From an Ethernet interface to a tunnel interface	The interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.
	From a tunnel interface to an Ethernet interface	The interface transparently transmits the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface transparently transmits the packet.

 Copyright © Huawei Technologies Co., Ltd.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
VLANIF interface	From a VLANIF interface to a tunnel interface	If the VLAN ID in the packet is the same as the PVID, the interface removes the tag; otherwise, the interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.
	From a tunnel interface to a VLANIF interface	The device checks whether the VLAN ID in the packet is the same as that of the VLANIF interface. If so, the interface sends the packet; otherwise, the interface discards the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface adds the VLAN ID of the VLANIF interface to the packet before sending the packet.
Ethernet sub-interface	From an Ethernet sub-interface to a tunnel interface	The interface transparently transmits the packet.	The interface adds an outer tag to the packet before sending the packet.	If the packet contains a tag, the interface removes the tag before sending the packet.

 Copyright © Huawei Technologies Co., Ltd.

Interface Type	Traffic Flow	Default Processing on Ethernet Packet	With Tag	Without Tag (Untagged)
	From a tunnel interface to an Ethernet sub-interface	The device checks whether the VLAN ID in the packet is the same as that of the Dot1q or QinQ sub-interface. If so, the interface sends the packet; otherwise, the interface discards the packet.	If the tag differs from the specified one, the interface discards the packet. Otherwise, the interface removes the outer tag before sending the packet.	The interface adds the VLAN ID of the Dot1q or QinQ sub-interface to the packet before sending the packet.

Example

Configure the link bridge function when the inbound interface is a serial interface.

```
<Huawei> system-view
[Huawei] link-bridge 2 interface serial 1/0/0 out-interface tunnel 0/0/1
```

Configure the link bridge function when the inbound interface is a GE interface.

```
<Huawei> system-view
[Huawei] link-bridge 2 interface gigabitethernet 1/0/0 out-interface tunnel 0/0/1
```

12.3.13 map interface virtual-ethernet

Function

The **map interface virtual-ethernet** command binds a Layer 2 virtual Ethernet (VE) interface to a physical Ethernet interface or tunnel interface.

The **undo map interface virtual-ethernet** command deletes the binding relationship.

By default, no Layer 2 VE interface is bound to a physical Ethernet interface or tunnel interface.

Format

map interface virtual-ethernet *ve-number*

undo map interface virtual-ethernet *ve-number*

Parameters

Parameter	Description	Value
ve-number	Specifies a VE interface number. The value is in slot number/card ID/sequence number format.	The VE interface number must already exist.

Views

Ethernet interface view, GE interface view, XGE interface view, tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customers want to use GRE to transparently transmit Ethernet packets over networks of a different network layer protocol, such as the IPv4 network. Ethernet over GRE can be configured to transparently transmit Ethernet packets over a GRE tunnel. After you run the **map interface virtual-ethernet** command to bind Layer 2 VE interfaces to the LAN-side physical Ethernet interface and WAN-side tunnel interface of a device, Ethernet packets received from the LAN-side interface are forwarded by the VE interfaces to the WAN-side tunnel interface. The WAN-side tunnel interface encapsulates the packets using GRE and transparently transmits the packets over a GRE tunnel.

Prerequisites

- A VE interface has been created by using the **interface virtual-ethernet** *ve-number* command, and the VE interface has been changed from Layer 3 mode to Layer 2 mode by using the **portswitch** command.
- The tunnel protocol of a tunnel interface has been set to GRE or mGRE by using the **tunnel-protocol gre** [**p2mp**] command in the tunnel interface view.

Precautions

- One VE interface can be bound to only one physical Ethernet interface or tunnel interface.
- The physical Ethernet interface and VE interface added to the same VLAN cannot communicate with each other.
- After a VE interface is bound to a physical Ethernet interface, other services on the Ethernet interface become invalid. After a VE interface is bound to a tunnel interface, the MTU value configured by using the **mtu** command does not take effect for Layer 2 traffic.
- This command can be configured only in the Layer 3 physical Ethernet interface view and tunnel interface view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind VE0/0/1 to GE0/0/2.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
[Huawei-Virtual-Ethernet0/0/1] quit
[Huawei] interface gigabitethernet 0/0/2
[Huawei-GigabitEthernet0/0/2] map interface virtual-ethernet 0/0/1
```

Bind VE0/0/2 to Tunnel0/0/2.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/2
[Huawei-Virtual-Ethernet0/0/2] portswitch
[Huawei-Virtual-Ethernet0/0/2] quit
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
[Huawei-Tunnel0/0/2] map interface virtual-ethernet 0/0/2
```

Related Topics

5.20.12 interface virtual-ethernet

12.3.15 portswitch (VE interface view)

12.3.10 interface tunnel

12.3.14 mtu (tunnel interface view)

Function

The **mtu** command sets the Maximum Transmission Unit (MTU) of a tunnel interface.

The **undo mtu** command restores the default value.

By default, the MTU is 1500 bytes on a tunnel interface.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a tunnel interface.	An integer ranging from 128 to 9202, in bytes.

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU.

If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Precautions

Set the MTU for a tunnel interface based on actual networking. The default value is recommended. If a small MTU is used but the packet size is large, packets may be divided into many fragments. Then the packets are discarded by QoS queues. If a large MTU is used, packets may be transmitted at a low rate.

If IPv6 is run on a tunnel interface and the MTU set using the **mtu** command on the interface is smaller than 1280, IPv6 works abnormally on this interface. To prevent this problem, set the MTU of a tunnel interface to a value greater than or equal to 1280 if IPv6 runs on the tunnel interface.

After running the **mtu** command, run the **shutdown** and then **undo shutdown** commands on the interface. The set MTU then can take effect.

On a network with IPv4 over IPv6 tunnels, if a tunnel interface is Down, the MTU value of the tunnel interface 64000 does not take effect. After the tunnel interface goes Up, the system dynamically refreshes the MTU value of the tunnel interface based on the Path_MTU of the tunnel and IPv6 MTU of the tunnel outbound interface. If the Path_MTU does not exist, the system adopts the MTU of the tunnel outbound interface as the MTU of the tunnel interface.

On a network with Ethernet over GRE tunnels, the MTU configured on a tunnel interface takes effect for Layer 3 traffic but not Layer 2 traffic.

The **mtu** *mtu* command configuration on a TE tunnel interface takes effect for packets sent by hosts only in the following scenarios:

- In an L3VPN over TE scenario, if the length of a packet that a host sends exceeds the configured MTU value, the packet is fragmented based on the MTU value at the IP layer before being forwarded.
- In a TE tunnel scenario, the length of a tunnel detection packet must be less than the configured MTU value.

Example

Set the MTU of Tunnel 0/0/1 to 1492.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] mtu 1492
[Huawei-Tunnel0/0/1] shutdown
[Huawei-Tunnel0/0/1] undo shutdown
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.3.3 display interface tunnel

12.3.15 portswitch (VE interface view)

Function

The **portswitch** command changes the working mode of a virtual Ethernet (VE) interface from Layer 3 mode to Layer 2 mode.

The **undo portswitch** command changes the working mode of a VE interface from Layer 2 mode to Layer 3 mode.

By default, a VE interface works in Layer 3 mode.

Format

portswitch

undo portswitch

Parameters

None.

Views

VE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VE interface on the device works in Layer 3 mode. To enable Layer 2 forwarding on the VE interface, run the **portswitch** command to change the working mode to Layer 2 mode.

Precautions

- The command cannot be executed on an interface that has any other configurations except attributes. Delete these configurations before you run this command.
- After changing the working mode of a VE interface, wait at least 30 seconds if you want to change the working mode again.

Example

Change VE0/0/1 to Layer 2 mode.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 0/0/1
[Huawei-Virtual-Ethernet0/0/1] portswitch
```

 Copyright © Huawei Technologies Co., Ltd.

12.3.16 qos pre-classify

Function

The **qos pre-classify** command enables pre-extraction of original IP packets.

The **undo qos pre-classify** command disables pre-extraction of original IP packets.

By default, pre-extraction of original IP packets is disabled.

Format

qos pre-classify

undo qos pre-classify

Parameters

None

Views

Tunnel interface view, Efficient VPN policy view, Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, GDOI policy view, BD view, VBDIF interface view, VPN instance view, Virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In tunnel mode, QoS parameters such as the packet header and protocol type in original packets are hidden after IP packets are encapsulated through GRE, VXLAN, L2TP, and IPSec. Although GRE, VXLAN, L2TP, and IPSec uses the DSCP field in original packets as the DSCP field in the IP packet header, some QoS solutions require quintuple information. The encryption device can pre-extract quintuple information including the source address, destination address, protocol type, source port number, and destination port number to facilitate refined QoS management on GRE, VXLAN, L2TP, and IPSec packets.

In an A2A VPN solution, the device uses the IP header of original packets as the IP header for encapsulated A2A VPN packets. Therefore, you do not need to configure this command if the device classifies packets based on the source address, destination address, or protocol type only.

Follow-up Procedure

After pre-extraction of original IP packets is enabled, run the **if-match acl** { *acl-number* | *acl-name* } command in the traffic classifier view to configure a matching rule based on the ACL.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable pre-extraction of original IP packets in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos pre-classify
```

Related Topics

12.6.104 ipsec policy (interface view)

12.6.106 ipsec policy-template

12.6.107 ipsec profile (interface view)

12.6.98 ipsec efficient-vpn (system view)

12.3.17 reset keepalive packets count

Function

The **reset keepalive packets count** command clears the statistics on Keepalive packets sent and received by a GRE tunnel interface.

Format

reset keepalive packets count

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Keepalive function is enabled on a GRE tunnel, the VPN cannot choose a tunnel with an unreachable remote end, preventing data loss. You can run the **display keepalive packets count** command to view the statistics on Keepalive packets and Keepalive response packets sent and received by the GRE tunnel interface, and the running status of the GRE tunnel.

The **reset keepalive packets count** command resets the statistics of Keepalive packets and Keepalive response packets sent and received by the GRE tunnel interface. You can monitor the running status of the GRE tunnel.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The cleared packet statistics cannot be restored. Exercise caution when you run the command.

Example

Reset the Keepalive packet statistics of GRE tunnel interface 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] reset keepalive packets count
 Info: Succeeded in resetting tunnel keepalive packets count.
```

Related Topics

12.3.11 keepalive

12.3.4 display keepalive packets count

12.3.18 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel.	-

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured

 Copyright © Huawei Technologies Co., Ltd.

with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

12.3.19 statistic enable (Tunnel interface view)

Function

The **statistic enable** command enables traffic statistics collection on a Tunnel interface.

The **undo statistic enable** command disables traffic statistics collection on a Tunnel interface.

By default, traffic statistics collection is disabled on a Tunnel interface.

Format

statistic enable { **inbound** | **outbound** }

undo statistic enable { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables incoming traffic statistics collection.	-
outbound	Enables outgoing traffic statistics collection.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check the network status or locate network faults, you can use the **statistic enable** command to enable traffic statistics collection on Tunnel interfaces. The device then collect traffic statistics on the Tunnel interfaces.

Precautions

After running the **statistic enable** command on an interface, you can run the **display interface tunnel** command to view the traffic statistics on the interface. The traffic statistics help you diagnose the fault of a tunnel.

Example

Enable incoming traffic statistics collection on a Tunnel interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] statistic enable inbound
```

Related Topics

12.3.3 display interface tunnel

12.3.20 tunnel route-via

Function

The **tunnel route-via** command specifies the routing outbound interface for a GRE tunnel or mGRE tunnel.

The **undo tunnel route-via** command restores the default configuration.

By default, a GRE tunnel or mGRE tunnel does not have a routing outbound interface.

Format

tunnel route-via *interface-type interface-number* { **mandatory** | **preferred** }

undo tunnel route-via *interface-type interface-number* { **mandatory** | **preferred** }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Parameter	Description	Value
mandatory	Configures traffic to be strictly forwarded through the specified routing outbound interface.	-
preferred	Configures traffic to be preferentially forwarded through the specified routing outbound interface.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

GRE packets are forwarded based on routing tables. If there are multiple equal-cost routes to the destination address, GRE packets are shared among these routes. In some situations, the actual routing outbound interface of GRE packets transmitted over a GRE tunnel may be the routing outbound interface for another GRE tunnel. If Unicast Reverse Path Forwarding (URPF) is enabled on the next hop device, this device checks the source addresses of these GRE packets to identify their outbound interface and then determines whether the outbound interface for these packets are the same as the actual interface that receives these packets. After the device finds that the outbound interface for these packets is different from the actual interface that receives these packets, the device drops these packets. To solve this problem, run the **tunnel route-via** command to specify the routing outbound interface for each GRE tunnel.

If multiple equal-cost routes exist between a Spoke or Hub site and the GRE tunnel destination address for an mGRE tunnel but you want GRE packets to be forwarded through a specified physical outbound interface, run the **tunnel route-via** command in the mGRE tunnel interface view to specify the routing outbound interface.

Prerequisites

The **tunnel-protocol gre** command has been run in the tunnel interface view.

Configuration Impact

If you configure **mandatory** when running the **tunnel route-via** command, traffic is strictly forwarded through the specified routing outbound interface. Specifically, if the available routing outbound interfaces for GRE packets transmitted over a GRE tunnel do not include the routing outbound interface specified for the tunnel, packets cannot be forwarded. The mGRE tunnel status is not affected. If you configure **preferred** when running the **tunnel route-via** command, traffic is preferentially forwarded through the specified routing outbound interface. Specifically, if the available routing outbound interfaces for GRE packets transmitted over a GRE or mGRE tunnel do not include the routing outbound interface specified for the tunnel, packets can still be forwarded through available routing outbound interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify the routing outbound interface for a GRE tunnel and configure traffic to be strictly forwarded through the specified interface.

```
<Huawei> system-view
[Huawei] interface Tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] tunnel route-via GigabitEthernet 0/0/1 mandatory
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.3.21 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. ● **p2p**: indicates the P2P SVPN tunnel protocol. ● **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

12.4 SVPN Configuration Commands

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact Huawei technical support personnel.

12.4.1 authentication

Function

The **authentication** command configures the user name and password for authentication in Hub-Spoke mode.

The **undo authentication** command cancels the user name and password.

By default, no user name or password is configured.

Format

authentication user-name *user-name* **password cipher** *cipher-string*

undo authentication

Parameters

Parameter	Description	Value
user-name *user-name*	Specifies a user name for authentication.	The value is a string of 1 to 32 case-sensitive characters without spaces.
password cipher *cipher-string*	Specifies the authentication password in cipher text.	The value is a string of case-sensitive characters without spaces. It can contain 1 to 16 characters in plain text or 32or 48 characters in cipher text.

Views

SVPN proposal view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To improve security in Hub-Spoke mode, two communicating parties authenticate each other before establishing an SVPN tunnel between them. An SVPN tunnel can be established only after the two parties pass authentication.

Example

Set the authentication user name and password to **Huawei** and **Huawei@1234**.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] authentication user-name Huawei password cipher Huawei@1234
```

12.4.2 cmi-method (service view)

Function

The **cmi-method** command configures a composite measure indicator (CMI) calculation formula for the service flow forwarding path.

The **undo cmi-method** command restores the default configuration.

By default, the CMI calculation formula is CMI = 9000 - (D + J + L), where, D presents the delay; J presents the jitter; L represents the packet loss rate.

Format

cmi-method *cmi-method-formula*

undo cmi-method

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cmi-method-formula	Specifies the CMI calculation formula. ● The CMI calculation formula is CMI = 9000 - *cmi-method*. You can define how *cmi-method* is calculated based on service requirements, and the default value is D + J + L. ● In the CMI calculation formula, if there is a coefficient before D, J, or L, the product of D, J, or L and the coefficient must be smaller than or equal to 5000, 3000, and 1000 respectively. If the product is larger than the maximum values (5000, 3000, and 1000), the maximum values are used. For example, when the formula CMI = 9000 - (10 x D + 10 x J + 10 x L) is used, and the D, J, and L are 1000 ms, 100 ms, and 10‰ respectively, the CMI is calculated as follows: CMI = 9000 - (5000 + 1000 + 100) = 2900. This is because 10 x D is 10000, which exceeds the maximum value 5000 and can only be calculated as 5000.	The value is a string of 1 to 20 characters. The value contains only digits, plus sign (+), asterisk (*), slash (/), and letters (D, d, L, l, J, or j). Only the plus operator (+) can be used among parameters D, J, and L. These parameters can be multiplied or divided by a positive integer. For example: ● 10 x D ● D x 10 + J/10 ● D x 100 + J x 10 + L/10 **NOTE** D or d indicates the delay; J or j indicates the jitter; and L or l indicates the packet loss rate.

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to customize the CMI calculation formula based on service requirements. SVPN determines link quality based on the CMI value and selects an optimal link to forward service data.

Precautions

After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to modify the CMI calculation formula for the service flow forwarding path.

Example

Set the CMI calculation formula for the service flow forwarding path to CMI = 9000 - (D + J).

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] cmi-method d+j
```

Related Topics

12.4.3 cmi-threshold (service view)

12.4.3 cmi-threshold (service view)

Function

The **cmi-threshold** command configures a composite measure indicator (CMI) threshold for the service flow forwarding path.

The **undo cmi-threshold** command restores the default configuration.

By default, the CMI, delay, jitter, and packet loss rate thresholds are 0, 5000 ms, 3000 ms, and 1000‰ respectively.

Format

cmi-threshold { **cmi** *cmi-threshold-value* | **delay** *delay-threshold-value* | **jitter** *jitter-threshold-value* | **loss** *loss-threshold-value* } *

undo cmi-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cmi *cmi-threshold-value*	Specifies a CMI threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 9000.
delay *delay-threshold-value*	Specifies a delay threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 5000, in milliseconds.
jitter *jitter-threshold-value*	Specifies a jitter threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 3000, in milliseconds.
loss *loss-threshold-value*	Specifies a packet loss rate threshold for a service flow forwarding path.	The value is an integer that ranges from 0 to 1000, in ‰.

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- CMI is the composite measure indicator of a link. Many services have requirements for link delay, jitter, and packet loss rate. Therefore, users need to configure the correct CMI calculation formula according to service requirements and use the **cmi-threshold** command set the CMI threshold. When the calculated CMI value is lower than the configured CMI threshold, SVPN determines that the link CMI does not meet service requirements.
- The service delay threshold is the maximum service delay allowed by services on a link. If services require a short delay, this threshold needs to be set.
- The service jitter threshold is the maximum service jitter allowed by services on a link. If services require a low jitter, this threshold needs to be set.
- The packet loss rate threshold is the maximum packet loss rate allowed by services on a link. If services require a low packet loss rate, this threshold needs to be set.

If either of the following occurs, the path does not meet the requirement.

- The CMI value calculated using the CMI calculation formula is smaller than the configured CMI threshold.
- The path delay is larger than the configured delay threshold.

 Copyright © Huawei Technologies Co., Ltd.

- The path jitter is larger than the configured delay threshold.
- The packet loss rate value of a path is larger than the configured packet loss rate threshold.

Precautions

After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to modify the CMI threshold for the service traffic forwarding path.

If you run the **cmi-threshold** command multiple times, only the latest configuration takes effect.

Example

Set the CMI threshold for an SVPN service flow forwarding path to 7000.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] cmi-threshold cmi 7000
```

Related Topics

12.4.2 cmi-method (service view)

12.4.4 encapsulation (SVPN proposal view)

Function

The **encapsulation** command configures the encapsulation type for SVPN packets.

The **undo encapsulation** command restores the default configuration.

By default, the encapsulation type of SVPN packets is NULL.

Format

encapsulation gre

undo encapsulation

Parameters

Parameter	Description	Value
gre	Specifies the GRE encapsulation type for packets.	-

Views

SVPN proposal view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You do not need to set the encapsulation type for SVPN packets to GRE when the device works in Lone Ranger mode. If the encapsulation type is set to GRE, you need to configure the SVPN function on the peer device and configure the peer device to work in Lone Ranger mode. Otherwise, service flows cannot be transmitted between the two devices.

In Hub-Spoke mode, you can use either of the following methods to set the encapsulation type for SVPN packets to GRE:

- Run the **encapsulation** command to set the encapsulation type for SVPN packets to GRE. Packets on all service flow forwarding paths in the SVPN proposal use the GRE encapsulation type. If you want to set the GRE encapsulation type for packets on some service flow forwarding paths, use the following method.
- Specify the **encapsulation gre** parameter when you run the **source (SVPN proposal view)** command to configure a forwarding path for the service flow. In this way, the encapsulation type for packets on the specified forwarding path is set to GRE.

Example

Set the encapsulation type for SVPN packets to GRE.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] encapsulation gre
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.5 destination (SVPN proposal view)

Function

The **destination** command configures the destination address for a service flow forwarding path.

The **undo destination** command deletes the destination address of a service flow forwarding path.

By default, no destination address is configured for a service flow forwarding path.

Format

destination *dest-ip-address*

undo destination

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dest-ip-address	Specifies a destination address for a service flow forwarding path.	The value is in dotted decimal notation.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an SVPN proposal is created, you need to configure service flow forwarding paths for the SVPN proposal to direct packet forwarding. You can use the following methods to configure a service flow forwarding path.

- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } **destination** *dest-ip-address* { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } * command to configure the source address/interface and destination address for a service flow forwarding path.
- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } * or **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } command to configure the source address or source interface for a service flow forwarding path, and then run the **destination** *dest-ip-address* command to configure the destination address for the path.

Precautions

If you configure a service flow forwarding path using the **source (service view)** command without **destination** *dest-ip-address* specified or the **source (SVPN proposal view)** command, you must run the this command to configure the destination address for the path. Otherwise, the path cannot be used to forward SVPN packets.

Example

Set the destination address of a service flow forwarding path to 2.2.2.9.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] destination 2.2.2.9
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.14 source (SVPN proposal view)
12.4.15 source (service view)

12.4.6 svpn-proposal (system view)

Function

The **svpn-proposal** command creates an SVPN proposal and enters the SVPN proposal view.

The **undo svpn-proposal** command deletes an SVPN proposal.

By default, no SVPN proposal is created on the device.

Format

svpn-proposal *svpn-proposal-name*

undo svpn-proposal *svpn-proposal-name*

Parameters

Parameter	Description	Value
svpn-proposal-name	Specifies the name of an SVPN proposal.	The value is a string of 1 to 31 case-sensitive characters without spaces or hyphens (-). When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SVPN binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers. When the SVPN function is required, you can run this command to create an SVPN proposal.

Precautions

After you run the **undo svpn-proposal** command to delete an SVPN proposal, all configurations in the SVPN proposal are deleted.

Follow-up Procedure

After creating an SVPN proposal, you need to perform a series of configurations for the SVPN proposal. The mandatory operations are as follows:

- Creating an SVPN service: Only after you run the **service (SVPN proposal view)** command to create an SVPN service, you can set other parameters for the service. The parameters include the forwarding path and scheduling mode for a service flow, and the packet matching mode.
- Binding an SVPN proposal to an SVPN tunnel interface: Run the **svpn-proposal (tunnel interface view)** command to bind an SVPN proposal to an SVPN tunnel interface. After the SVPN proposal is bound to a tunnel interface, packets received by this interface are forwarded along the path for SVPN service packets.

Example

Create an SVPN proposal **p1**.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1]
```

Related Topics

12.4.7 svpn-proposal (tunnel interface view)

12.4.7 svpn-proposal (tunnel interface view)

Function

The **svpn-proposal** command binds an SVPN proposal to an SVPN tunnel interface.

The **undo svpn-proposal** command unbinds an SVPN proposal from an SVPN tunnel interface.

By default, no SVPN proposal is bound to a tunnel interface.

Format

svpn-proposal *svpn-proposal-name*

undo svpn-proposal *svpn-proposal-name*

Parameters

Parameter	Description	Value
svpn-proposal-name	Specifies the name of an SVPN proposal.	The value is an existing SVPN proposal name.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an SVPN proposal is created, you need to bind the SVPN proposal to an SVPN tunnel interface. After the SVPN proposal is bound to a tunnel interface, packets received by this interface are forwarded along the path for SVPN service packets.

Prerequisite

An SVPN proposal has been created by using the **svpn-proposal (system view)** command and the tunnel protocol type has been set to SVPN by using the **tunnel-protocol svpn** [**p2p** | **p2mp**] command.

Precautions

One SVPN proposal can be bound to only one tunnel interface. If you want to bind the SVPN proposal to another tunnel interface, unbind the SVPN proposal from the previous tunnel interface first.

All configurations in the SVPN proposal that has been bound to an SVPN tunnel interface cannot be modified. To modify the configurations, unbind the SVPN proposal from the tunnel interface.

Example

Bind the SVPN proposal **p1** to Tunnel0/0/1.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 5 permit ip
[Huawei-acl-adv-3000] quit
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] encapsulation gre
[Huawei-svpn-proposal-p1] source 1.1.1.9 destination 2.2.2.9 bandwidth 1024
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] schedule-type overflow
[Huawei-svpn-proposal-p1-service-s1] match acl 3000
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9
[Huawei-svpn-proposal-p1-service-s1] quit
[Huawei-svpn-proposal-p1] quit
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn p2p
[Huawei-Tunnel0/0/1] svpn-proposal p1
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.8 svpn-zone

Function

The **svpn-zone** command configures an SVPN zone for a tunnel interface.

The **undo svpn-zone** command restores the default configuration.

By default, a tunnel interface belongs to SVPN zone 0.

 Copyright © Huawei Technologies Co., Ltd.

Format

svpn-zone *zone-number*

undo svpn-zone

Parameters

Parameter	Description	Value
zone-number	Specifies an SVPN zone.	The value is an integer that ranges from 1 to 1000. The default value is 0.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple SVPN tunnel interfaces are configured on a device in an SVPN scenario, you need to run this command to configure different SVPN zones for these interfaces to ensure proper data forwarding.

Prerequisite

The tunnel protocol type has been set to SVPN by using the **tunnel-protocol** command.

Precautions

After an SVPN proposal is bound to a tunnel interface, you cannot modify the SVPN zone of the interface. To modify the SVPN zone of the interface, unbind the SVPN proposal from the interface first.

The SVPN zones of SVPN tunnel interfaces on a device must differ from one another, regardless of whether the device works in Lone Ranger or Hub-Spoke mode. If the device works in Hub-Spoke mode, the Hub and Spoke devices must be configured with the same SVPN zone. If the device works in Lone Ranger mode and uses the GRE encapsulation type, the connected devices must be configured with the same SVPN zone.

Example

Set the SVPN zone of Tunnel0/0/1 to 1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol svpn
[Huawei-Tunnel0/0/1] svpn-zone 1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.4.6 svpn-proposal (system view)

12.4.9 match (service view)

Function

The **match** command configures an ACL rule or an application protocol type for matching service flows.

The **undo match** command deletes an ACL rule or an application protocol type for matching service flows.

By default, service flows do not match any rule.

Format

match { **acl** *acl-number* | **application** *protocol-name* }

undo match { **acl** *acl-number* | **application** *protocol-name* }

Parameters

Parameter	Description	Value
acl *acl-number*	Indicates that the device matches service flows by ACL rule.	The value is an integer that ranges from 2000 to 3999.
application *protocol-name*	Indicates that the device matches service flows by application protocol type.	The value is a character string without spaces and varies with the feature library.

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

SVPN distinguishes different service flows by matching ACL rules or application protocol types.

If no matching ACL rule or application protocol type is configured for SVPN service flows, all the service flows sent to the SVPN tunnel interface can be forwarded. SVPN randomly selects an available forwarding path.

Example

Distinguish the service flow **s1** by matching the ACL rule 3000.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] acl number 3000
[Huawei-acl-adv-3000] rule 5 permit ip
[Huawei-acl-adv-3000] quit
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] match acl 3000
```

Related Topics

12.4.13 service (SVPN proposal view)

12.4.10 recovery-delay

Function

The **recovery-delay** command configures the delay for switching a service flow between forwarding paths when the scheduling mode is Priority.

The **undo recovery-delay** command restores the default configuration.

By default, the delay for switching a service flow between forwarding paths is 5s.

Format

recovery-delay *delay-time*

undo recovery-delay

Parameters

Parameter	Description	Value
delay-time	Specifies the switching delay.	The value is an integer that ranges from 0 to 30000, in seconds. The default value is 5s.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

In an SVPN scenario, when the scheduling mode is set to Priority, the device usually switches a service flow to the optimal path in 5seconds when it detects that a better path is available. When a network is unstable, the service flow may be frequently switched between different paths, resulting in data loss. You can run this command to set an appropriate switching delay.

Example

Set the delay for switching service flow between forwarding paths to 60s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] recovery-delay 60
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.11 reorder-window

Function

The **reorder-window** command configures the size of the receive or transmit buffer for SVPN packets.

The **undo reorder-window** command restores the default configuration.

By default, the size of the receive or transmit buffer for SVPN packets is 64.

Format

reorder-window *window-size*

undo reorder-window

Parameters

Parameter	Description	Value
window-size	Specifies the size of the receive or transmit buffer for SVPN packets.	The value is an integer, which can be 32, 64, or 128.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When SVPN binds multiple WAN access lines and the scheduling mode for a service flow is set to Overflow, packets in the service flow may be forwarded through multiple paths. As a result, the receiver end may receive mis-sequencing packets, leading to communication quality deterioration. You can run this command to adjust the size of the receive or transmit buffer for SVPN packets to reduce packet mis-sequencing.

Precautions

You are advised to specify the *window-size* parameter under the supervision of the technical support personnel.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the size of the receive or transmit buffer for SVPN packets to 128.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] reorder-window 128
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.12 schedule-type (service view)

Function

The **schedule-type** command configures a mode for scheduling a service flow to one or more forwarding paths.

The **undo schedule-type** command deletes the mode for scheduling a service flow to one or more forwarding paths.

By default, no mode is configured for scheduling a service flow.

Format

schedule-type { **overflow** | **priority** }

undo schedule-type

Parameters

Parameter	Description	Value
overflow	Indicates that a service flow is scheduled based on the path bandwidth.	-
priority	Indicates that a service flow is scheduled based on the path priority.	-

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the SVPN function, the device needs to distinguish different types of service flows. Multiple forwarding paths may be available for one type of service flow. You can run this command to configure a mode for scheduling a service flow to one or more forwarding paths.

 Copyright © Huawei Technologies Co., Ltd.

- Overflow mode: The device schedules the service flow based on the path bandwidth. Packets of one service flow can be transmitted over different paths. If the bandwidth of the first available path is occupied, packets are scheduled to a second available path, and so on.

  You can run the **source index (service view)** command to manually sequence the paths.

- Priority mode: The device schedules the service flow based on the path priority. Packets of one service flow can be transmitted over only one optimal path. When selecting the optimal path, the device calculates forwarding paths that meet the criteria using link detection (associated NQA instances or the default link quality measurement method) and then selects the first available path from these paths.

  Multiple forwarding paths may meet the link quality criteria. To select the first available path from these paths, run the **source index (service view)** command to manually sequence the paths.

Precautions

Ensure that the **schedule-type** command is configured in the service view before you bind an SVPN proposal to an SVPN tunnel interface. After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to modify the mode for scheduling a service flow.

Example

Set the mode for scheduling a service flow to Overflow.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] schedule-type overflow
```

Related Topics

12.4.13 service (SVPN proposal view)

12.4.13 service (SVPN proposal view)

Function

The **service** command creates an SVPN service and displays the service view.

The **undo service** command deletes an SVPN service.

By default, no SVPN service is created.

Format

service *service-name* [**id** *service-id*]

undo service *service-name*

Parameters

Parameter	Description	Value
service-name	Specifies the name of an SVPN service.	The value is a string of 1 to 31 case-sensitive characters without spaces or hyphens (-). The total length of the names of the SVPN service and SVPN proposal must be within 56 case-sensitive characters.
id *service-id*	Specifies the ID of an SVPN service.	The value is an integer that ranges from 1 to 8.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an SVPN service is created, you can configure other parameters for the SVPN service to implement the SVPN function. The parameters include the forwarding path and scheduling mode for a service flow, and the packet matching mode.

Precautions

You must specify the **id** parameter when you create an SVPN service for the first time. The SVPN service ID is unique in an SVPN proposal and the created service ID cannot be modified.

After an SVPN service is created, you do not need to specify the **id** parameter in the service view.

If the device works in Hub-Spoke mode, the Hub and Spoke devices must be configured with the same *service-id*.

Example

Create an SVPN service named **s1** with the ID 1.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1]
```

Related Topics

12.4.6 svpn-proposal (system view)

12.4.14 source (SVPN proposal view)

Function

The **source** command configures one or more forwarding paths for a service flow.

The **undo source** command deletes the forwarding paths of a service flow.

By default, no forwarding path is configured for a service flow.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } [**destination** *dest-ip-address*] { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } *

undo source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified source address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
source-ip-address	Specifies a source address for a service flow forwarding path.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of the source interface for a service flow forwarding path. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
destination *dest-ip-address*	Specifies a destination address for a service flow forwarding path.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bandwidth { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* }	Specifies the link bandwidth of a forwarding path. ● **up**: indicates the uplink bandwidth. ● **down**: indicates the downlink bandwidth. ● If neither **up** or **down** is specified, this parameter indicates the uplink bandwidth and downlink bandwidth. **NOTE** If this parameter is not specified, the bandwidth of the forwarding path is equal to the actual physical bandwidth of the source interface.	The value is an integer that ranges from 0 to 4000000000, in kbit/s.
encapsulation gre	Specifies the GRE encapsulation type for packets on a forwarding path.	-
track nqa *admin-name test-name*	Specifies the name of the administrator of the NQA test instance and the name of the test instance associated with a service flow forwarding path. **NOTE** If this parameter is not specified, the default link quality measurement method is used to calculate the delay and packet loss rate of the forwarding path.	The value of *admin-name* or *test-name* is a string of 1 to 32 case-sensitive characters without spaces.

Views

SVPN proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an SVPN proposal is created, you need to configure service flow forwarding paths for the SVPN proposal to direct packet forwarding. You can use the following methods to configure a service flow forwarding path.

- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } **destination** *dest-ip-address* { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track**

nqa *admin-name test-name* } * command to configure the source address/interface and destination address for a service flow forwarding path.

- Run the **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } { **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* } | **encapsulation gre** | **track nqa** *admin-name test-name* } * or **source** { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } command to configure the source address or source interface for a service flow forwarding path, and then run the **destination** *dest-ip-address* command to configure the destination address for the path.

After multiple forwarding paths are configured using this command, SVPN supports the following modes for scheduling service flows:

- Overflow mode: The device schedules the service flow based on the path bandwidth. Packets of one service flow can be transmitted over different paths. If the bandwidth of the first available path is occupied, packets are scheduled to a second available path, and so on. You can run the **source index (service view)** command to manually sequence the paths.

  When the Overflow mode is used:

  - You can specify **bandwidth** to configure the bandwidth for a forwarding path. If **bandwidth** is not specified, the actual physical bandwidth of the source interface is used. In practice, SVPN adjusts the bandwidth of the forwarding paths based on the packet loss rate calculated using link detection (associated the default link quality measurement method) in real time to provide a better service.
  - If the link detection result shows that the delay of a second available path is much larger than the delay of the first available path, SVPN does not use this path but searches for another path that meets the link quality requirement.
- Priority mode: The device schedules the service flow based on the path priority. Packets of one service flow can be transmitted over only one optimal path. When this mode is used, SVPN can select a path using either of the following methods:

  - Associate with NQA instances by specifying **track nqa** to calculate forwarding paths that meet the criteria and then select the first available path from these paths.
  - Use the default link quality measurement method to calculate forwarding paths that meet the criteria and then select the first available path from these paths.

  Multiple forwarding paths may meet the link quality criteria. To select the first available path from these paths, run the **source index (service view)** command to manually sequence the paths.

  NOTE

  When this mode is used, the **bandwidth** parameter does not take effect even if it is specified for service flow forwarding path.

Precautions

- A maximum of eight forwarding paths can be created for an SVPN proposal. You can run this command to configure one or more forwarding paths or run

the **source (service view)** command to configure a new forwarding path for the SVPN service.

- If you run this command multiple times, the latest configuration for the following parameters overrides the previous configuration. The parameters that are overridden include **destination** *dest-ip-address*, **bandwidth** { { **up** *bw-value* | **down** *bw-value* } * | *bw-value* }, and **track nqa** *admin-name test-name*.
- Generally, the GRE encapsulation type is not required when you configure forwarding paths for a device working in Lone Ranger mode. If the encapsulation type is set to GRE, you need to configure the SVPN function on the peer device and configure the peer device to work in Lone Ranger mode. Otherwise, service flows cannot be transmitted between the two devices. In Hub-Spoke mode, you can use either of the following methods to set the encapsulation type for SVPN packets to GRE:
  - Set the encapsulation type to GRE by specifying the **encapsulation gre** parameter in this command.
  - Run the **encapsulation (SVPN proposal view)** command to set the encapsulation type for SVPN packets to GRE. Packets on all service flow forwarding paths in the SVPN proposal use the GRE encapsulation type. If you want to set the GRE encapsulation type for packets on some service flow forwarding paths, use the first method.
- When you delete a forwarding path that has been referenced by the SVPN service, the forwarding path still exists in the service view as a newly created path.

Example

Configure a forwarding path for the SVPN proposal **p1**, whose source address, destination address, and bandwidth are 1.1.1.9, 2.2.2.9, and 1024 kbit/s respectively.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] source 1.1.1.9 destination 2.2.2.9 bandwidth 1024
```

Related Topics

12.4.16 source index (service view)

12.4.15 source (service view)

Function

The **source** command configures one or more service flow forwarding paths for the SVPN service.

The **undo source** command deletes one or more service flow forwarding paths for the SVPN service.

By default, no service flow forwarding path is configured for the SVPN service.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified source address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
source-ip-address	Specifies a source address for a service flow forwarding path.	The value is in dotted decimal notation.
interface-type interface-number	Specifies the type and number of the source interface for a service flow forwarding path. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After service flow forwarding paths are configured for an SVPN proposal, you can run this command to apply an existing forwarding path to the SVPN service. You can also run this command and the **destination (SVPN proposal view)** command to create a service flow forwarding path for the SVPN service.

Precautions

If you run this command to create a service flow forwarding path, the path uses the default link quality measurement method, actual physical bandwidth of the source interface, and packet encapsulation type configured for the SVPN proposal.

 Copyright © Huawei Technologies Co., Ltd.

Currently, a maximum of eight forwarding paths can be configured for a service flow.

Example

Apply the existing forwarding path with the source address 1.1.1.9, destination address 2.2.2.9, and packet encapsulation type GRE to the SVPN service s1.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
[Huawei-svpn-proposal-p1] source 1.1.1.9 destination 2.2.2.9 encapsulation gre
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9
```

Related Topics

12.4.14 source (SVPN proposal view)

12.4.5 destination (SVPN proposal view)

12.4.16 source index (service view)

Function

The **source index** command adjusts the sequence of forwarding paths for a service flow in the SVPN service.

By default, forwarding paths are sequenced according to the configuration time.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* } **index** *path-index*

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the specified source address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
source-ip-address	Specifies a source address for a service flow forwarding path.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface for a service flow forwarding path. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
path-index	Specifies an index for a service flow forwarding path. **NOTE** The index cannot be larger than the total number of forwarding paths currently configured.	The value is an integer that ranges from 1 to 8.

Views

Service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After forwarding paths are configured for an SVPN service flow, you can run this command to adjust the sequence of the forwarding paths.

Prerequisite

Before adjusting the sequence of the forwarding paths for a service flow, you need to run the **source (SVPN proposal view)** command to create a forwarding path and the **source (service view)** command to reference this forwarding path, or run the **source (service view)** command to create a forwarding path.

Precautions

After an SVPN proposal is bound to an SVPN tunnel interface, you need to unbind the SVPN proposal from the interface if you want to adjust the sequence of the forwarding paths.

When you adjust the sequence of the forwarding paths, the specified **source** related parameters must be the same as those of the forwarding path to be adjusted.

Example

Set the index of the forwarding path with the source addresses of 1.1.1.9 to 2.

```
<Huawei> system-view
[Huawei] svpn-proposal p1
```

```
[Huawei-svpn-proposal-p1] destination 2.2.2.9
[Huawei-svpn-proposal-p1] service s1 id 1
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9
[Huawei-svpn-proposal-p1-service-s1] source 3.3.3.9
[Huawei-svpn-proposal-p1-service-s1] source 4.4.4.9
[Huawei-svpn-proposal-p1-service-s1] source 1.1.1.9 index 2
[Huawei-svpn-proposal-p1-service-s1] display this
#
 service s1 id 1
  source 3.3.3.9
  source 1.1.1.9
  source 4.4.4.9
#
return
```

Related Topics

12.4.14 source (SVPN proposal view)

12.4.15 source (service view)

12.4.17 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. • **p2p**: indicates the P2P SVPN tunnel protocol. • **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

12.5 DSVPN Configuration Commands

12.5.1 display nhrp peer

Function

The **display nhrp peer** command displays NHRP peer entries.

Format

display nhrp peer { **interface tunnel** *interface-number* [**dynamic** | **static** | *ip-address*] | *ip-address* }

display nhrp peer { **dynamic** | **static** } [*ip-address*]

display nhrp peer all

Parameters

Parameter	Description	Value
interface tunnel *interface-number*	Displays NHRP peer entries on the specified interface. *interface-number* specifies the interface number.	The interface number must already exist.
dynamic	Displays dynamic NHRP peer entries.	-
static	Displays static NHRP peer entries.	-
ip-address	Displays NHRP peer entry information based on the subnet IP address of the NHRP peer.	The value is in dotted decimal notation.
all	Displays all NHRP peer entries.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To determine whether a spoke has successfully registered, run the **display nhrp peer** command on the Hub to check whether NHRP peer entries of the spoke are generated. When a communication fault occurs between two spokes, run the **display nhrp peer** command on a spoke to check whether NHRP peer entries of the destination spoke are generated.

Example

Display all NHRP peer entries.

```
<Huawei> display nhrp peer all
-------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type          Flag
-------------------------------------------------------------------------------
1.2.1.2         32    2.2.1.1        1.2.1.2         registered     up|unique
-------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 19:00:27
Expire time     : 01:59:34
-------------------------------------------------------------------------------
Protocol-addr   Mask  NBMA-addr      NextHop-addr    Type          Flag
-------------------------------------------------------------------------------
1.2.1.1         32    3.2.1.1        1.2.1.1         registered     up|no-unique
-------------------------------------------------------------------------------
Tunnel interface: Tunnel0/0/0
Created time    : 17:12:23
Expire time     : 01:59:54

Number of nhrp peers: 2
```

Table 12-13 Description of the **display nhrp peer all** command output

Item	Description
Protocol-addr	Subnet address or tunnel interface address of the NHRP peer.
Mask	Subnet address mask or tunnel interface address mask of the NHRP peer.
NBMA-addr	Public address of the NHRP peer, which corresponds to the source tunnel interface address of the NHRP peer.
NextHop-addr	Address of the next hop pointing to the protocol address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Type of the NHRP peer table. ● hub: indicates a static entry with the **register** parameter. ● static: indicates a static entry without the **register** parameter. ● local: indicates an entry whose peer is itself. ● registered: indicates a dynamically generated branch registration entry. ● remote: indicates a dynamically generated entry in which the remote address is a tunnel interface address. ● remote-network: indicates a dynamically generated entry in which the remote address is a subnet address. If branches save only summarized routes to the headquarters, the source branch can dynamically learn the subnet address of the destination branch.
Flag	NHRP peer entry status: ● up: indicates that the NHRP peer entry is Up. ● down: indicates that the NHRP peer entry is Down. ● unique: indicates that conflicting NHRP peer entries are not overwritten during NHRP registration. ● no-unique: indicates that conflicting NHRP peer entries are overwritten during NHRP registration. **NOTE** up/down and unique/no-unique can be displayed simultaneously.
Tunnel interface	Tunnel interface number.
Before NAT NBMA-addr	NBMA address before NAT is implemented.
Created time	Time when an NHRP peer entry is created.
Expire time	Time when an NHRP peer entry expires.
Number of nhrp peers	Total number of NHRP peer entries generated currently.

12.5.2 display nhrp peer maximum-history

Function

The **display nhrp peer maximum-history** command displays historical statistics on NHRP peer entries and sites.

Format

display nhrp peer maximum-history

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view history statistics on NHRP peer entries and sites.

Example

Display history statistics on NHRP peer entries and sites.

```
<Huawei> display nhrp peer maximum-history
 ---------------------------------------------------------------------------
 Total peers                          :    0
 Maximum of total peers in history          :    0
 Begin time of total peers                  :    2016-10-18 20:22:30
 Maximum time of total peers                :    2016-10-18 20:22:30

 Total sites                          :    0
 Maximum of total sites in history          :    0
 Begin time of total sites                  :    2016-10-18 20:22:30
 Maximum time of total sites                :    2016-10-18 20:22:30
 ---------------------------------------------------------------------------
```

Table 12-14 Description of the **display nhrp peer maximum-history** command output

Item	Description
Total peers	Total number of NHRP peer entries.
Maximum of total peers in history	Maximum number of NHRP peer entries in the history.
Begin time of total peers	Time when collection of statistics on NHRP peer entries begins.
Maximum time of total peers	Time when the number of NHRP peer entries reaches the maximum value.
Total sites	Total number of sites.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximum of total sites in history	Maximum number of sites in the history.
Begin time of total sites	Time when collection of site statistics begins.
Maximum time of total sites	Time when the number of sites reaches the maximum value.

12.5.3 display nhrp statistics

Function

The **display nhrp statistics** command displays NHRP packet statistics.

Format

display nhrp statistics interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface tunnel *interface-number*	Displays NHRP packet statistics on the specified interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays NHRP packet statistics to help locate DSVPN-related faults.

Example

Display NHRP packet statistics on the interface tunnel 0/0/0.

```
<Huawei> display nhrp statistics interface tunnel 0/0/0
RegisterRequestSendSuccess        :0
RegisterRequestSendFail           :0
RegisterRequestCorrectRecv        :1024
```

```
RegisterRequestErrRecv          :0
RegisterRequestTransf           :0
RegisterReplySendSuccess        :1024
RegisterReplySendFail           :0
RegisterReplyCorrectRecv        :0
RegisterReplyErrRecv            :0
RegisterReplyTransf             :0
ResolutionRequestSendSuccess    :0
ResolutionRequestSendFail       :0
ResolutionRequestCorrectRecv    :0
ResolutionRequestErrRecv        :0
ResolutionRequestTransf         :0
ResolutionReplySendSuccess      :0
ResolutionReplySendFail         :0
ResolutionReplyCorrectRecv      :0
ResolutionReplyErrRecv          :0
ResolutionReplyTransf           :0
PurgeRequestSendSuccess         :0
PurgeRequestSendFail            :0
PurgeRequestCorrectRecv         :0
PurgeRequestErrRecv             :0
PurgeRequestTransf              :0
PurgeReplySendSuccess           :0
PurgeReplySendFail              :0
PurgeReplyCorrectRecv           :0
PurgeReplyErrRecv               :0
PurgeReplyTransf                :0
RedirectIndicationSendSuccess   :0
RedirectIndicationSendFail      :0
RedirectIndicationCorrectRecv   :0
RedirectIndicationErrRecv       :0
RedirectIndicationTransf        :0
ErrIndicationSendSuccess        :0
ErrIndicationSendFail           :0
ErrIndicationCorrectRecv        :0
ErrIndicationErrRecv            :0
ErrIndicationTransf             :0
AuthenticationFail              :0
LoopdetectFail                  :0
```

Table 12-15 Description of the **display nhrp statistics** command output

Item	Description
RegisterRequest-SendSuccess	Number of NHRP Registration Request packets that are sent successfully.
RegisterRequest-SendFail	Number of NHRP Registration Request packets that fail to be sent.
RegisterRequestCor-rectRecv	Number of NHRP Registration Request packets that are received successfully.
RegisterRequestErr-Recv	Number of NHRP Registration Request packets that fail to be received.
RegisterRequest-Transf	Number of NHRP Registration Request packets that are forwarded.
RegisterReplySend-Success	Number of NHRP Registration Reply packets that are sent successfully.
RegisterReplySend-Fail	Number of NHRP Registration Reply packets that fail to be sent.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RegisterReplyCorrectRecv	Number of NHRP Registration Reply packets that are received successfully.
RegisterReplyErrRecv	Number of NHRP Registration Reply packets that fail to be received.
RegisterReplyTransf	Number of NHRP Registration Reply packets that are forwarded.
ResolutionRequestSendSuccess	Number of NHRP Resolution Request packets that are sent successfully.
ResolutionRequestSendFail	Number of NHRP Resolution Request packets that fail to be sent.
ResolutionRequestCorrectRecv	Number of NHRP Resolution Request packets that are received successfully.
ResolutionRequestErrRecv	Number of NHRP Resolution Request packets that fail to be received.
ResolutionRequestTransf	Number of NHRP Resolution Request packets that are forwarded.
ResolutionReplySendSuccess	Number of NHRP Resolution Reply packets that are sent successfully.
ResolutionReplySendFail	Number of NHRP Resolution Reply packets that fail to be sent.
ResolutionReplyCorrectRecv	Number of NHRP Resolution Reply packets that are received successfully.
ResolutionReplyErrRecv	Number of NHRP Resolution Reply packets that fail to be received.
ResolutionReplyTransf	Number of NHRP Resolution Reply packets that are forwarded.
PurgeRequestSendSuccess	Number of NHRP Purge Request packets that are sent successfully.
PurgeRequestSendFail	Number of NHRP Purge Request packets that fail to be sent.
PurgeRequestCorrectRecv	Number of NHRP Purge Request packets that are received successfully.
PurgeRequestErrRecv	Number of NHRP Purge Request packets that fail to be received.
PurgeRequestTransf	Number of NHRP Purge Request packets that are forwarded.
PurgeReplySendSuccess	Number of NHRP Purge Reply packets that are sent successfully.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PurgeReplySendFail	Number of NHRP Purge Reply packets that fail to be sent.
PurgeReplyCorrectRecv	Number of NHRP Purge Reply packets that are received successfully.
PurgeReplyErrRecv	Number of NHRP Purge Reply packets that fail to be received.
PurgeReplyTransf	Number of NHRP Purge Reply packets that are forwarded.
RedirectIndicationSendSuccess	Number of NHRP Redirect Indication packets that are sent successfully.
RedirectIndicationSendFail	Number of NHRP Redirect Indication packets that fail to be sent.
RedirectIndicationCorrectRecv	Number of NHRP Redirect Indication packets that are received successfully.
RedirectIndicationErrRecv	Number of NHRP Redirect Indication packets that fail to be received.
RedirectIndicationTransf	Number of NHRP Redirect Indication packets that are forwarded.
ErrIndicationSendSuccess	Number of NHRP Error Indication packets that are sent successfully.
ErrIndicationSendFail	Number of NHRP Error Indication packets that fail to be sent.
ErrIndicationCorrectRecv	Number of NHRP Error Indication packets that are received successfully.
ErrIndicationErrRecv	Number of NHRP Error Indication packets that fail to be received.
ErrIndicationTransf	Number of NHRP Error Indication packets that are forwarded.
AuthenticationFail	Number of packets that fail to be authenticated.
LoopdetectFail	Number of loopback packets.

Related Topics

12.5.15 reset nhrp statistics

12.5.4 nhrp authentication

Function

The **nhrp authentication** command configures an NHRP authentication string.

The **undo nhrp authentication** command deletes an NHRP authentication string.

By default, no NHRP authentication string is configured.

Format

nhrp authentication { **simple** *string* | **cipher** *cipher-string* }

undo nhrp authentication

Parameters

Parameter	Description	Value
simple	Indicates the plain text password. You can enter a plain text password. When you want to view the configuration file, the password is displayed in plain text mode. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
string	Specifies the NHRP authentication string.	The value is a string of 1 to 8 case-sensitive characters. The value can contain special characters except the question mark (?) and space. **NOTE** To improve security, it is recommended that the NHRP authentication string contains at least two types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.
cipher	Indicates the cipher text password. You can enter a plain or cipher text password. When you want to view the configuration file, the password is displayed in cipher text mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher-string	Specifies the NHRP authentication string. The value is a string of encrypted or unencrypted characters.	An unencrypted password is a string of 1 to 8 case-sensitive characters, and an encrypted password is a string of 48 case-sensitive characters. The value can contain special characters except the question mark (?) and space. **NOTE** To improve security, it is recommended that the NHRP authentication string contains at least two types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command configures the NHRP authentication string on a spoke and the hub. This command enables the hub to reject the illegal registration of a spoke.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

After this command is executed on a spoke and the hub, the spoke sends an NHRP Registration Request packet to the hub, and the hub decides whether to process this packet based on the NHRP authentication string in the packet. If this NHRP authentication string is different from that configured on the hub, the hub does not process this packet. If the two NHRP authentication strings are the same, the hub processes this packet.

Precautions

If the NHRP authentication string is configured on the spoke but not on the hub, the NHRP authentication string cannot be used for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the NHRP authentication string to huawei@1 in cipher text.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp authentication cipher huawei@1
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.5 nhrp entry

12.5.5 nhrp entry

Function

The **nhrp entry** command adds static NHRP peer entries to the local NHRP mapping table.

The **undo nhrp entry** command deletes static NHRP peer entries from the local NHRP mapping table.

By default, no static NHRP peer entry is added to the local NHRP mapping table.

Format

nhrp entry *protocol-address* { *dns-name* | *nbma-address* } [**register** [**preference** *preference-value*]] [**track apn** *apn-name*]

undo nhrp entry *protocol-address* { *dns-name* | *nbma-address* } [**register** [**preference** *preference-value*]] [**track apn** *apn-name*]

Parameters

Parameter	Description	Value
protocol-address	Specifies the tunnel interface address of an NHRP peer device.	The value is in dotted decimal notation.
dns-name	Specifies the domain name of the NHRP peer device.	The value is a string of 1 to 255 case-sensitive characters without spaces.
nbma-address	Specifies the NBMA address of the NHRP peer device.	The value is in dotted decimal notation.
register	Configures a spoke to register with the hub to generate NHRP peer entries on the hub.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
preference *preference-value*	Specifies the hub priority. When multiple static NHRP peer entries are configured on a branch device and NHRP fails to determine the hub based on the next hop in private routes, the device selects an active hub based on the hub priority.	The value is an integer that ranges from 1 to 255. The default value is 60. A smaller value indicates a higher priority.
track apn	Binds NHRP peer information with the APN profile.	-
apn-name	Specifies the APN profile name.	The value is the name of an existing APN profile.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command configures mapping between the tunnel interface address of the NHRP peer device (the hub) and the NBMA address or mapping between the tunnel interface address and the host name.

When the spoke registers with the hub, the hub generates mapping between the tunnel interface address of the spoke and the NBMA address, so that the spoke and the hub communicate with each other through a VPN tunnel.

In a LTE scenario, you can bind NHRP peer information with the APN profile configured on the cellular interface if the source interface of the mGRE tunnel is a cellular interface. The NHRP peer information takes effect when the associated APN profile is in use. This flexibly controls mGRE tunnel setup.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

After this command is executed on the spoke, a local NHRP peer entry is generated and takes effect regardless of whether the hub receives Registration

 Copyright © Huawei Technologies Co., Ltd.

Request packets or not. If the spoke forwards packets based on this entry but the hub cannot receive the packets, a black hole is generated.

Precautions

The Domain Name Server (DNS) provides static mappings between domain names and IP addresses. When IP addresses change, DNS cannot dynamically update mappings. Therefore, administrators should configure the **nhrp peer** or **shutdown** and **undo shutdown** command to specify the next mGRE interface.

If NHRP peer information is associated with the APN profile, whether the NHRP peer entry takes effect depends on the APN status. If the APN is valid, the NHRP peer entry takes effect; otherwise, the configuration is saved but the NHRP peer entry does not take effect.

Example

Configure mapping between tunnel interface address 10.10.10.10 and NBMA address 1.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry 10.10.10.10 1.1.1.1
```

Configure mapping between the static address 10.10.10.10 and domain name **www.huawei.com**, and set the hub priority to 40.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry 10.10.10.10 www.huawei.com register preference 40
```

Related Topics

12.3.10 interface tunnel
12.3.21 tunnel-protocol

12.5.6 nhrp entry holdtime

Function

The **nhrp entry holdtime** command sets the aging time of NHRP peer entries.

The **undo nhrp entry holdtime** command restores the aging time of NHRP peer entries to the default value.

By default, the aging time of NHRP peer entries is 7200 seconds.

Format

nhrp entry holdtime seconds *seconds*

undo nhrp entry holdtime seconds

Parameters

Parameter	Description	Value
seconds *seconds*	Specifies the aging time of NHRP peer entries.	The value is an integer that ranges from 5 to 31845, in seconds. It is recommended that the aging time of NHRP peer entries be larger than 120s.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the aging time. The aging time is notified by the local device to the remote end so that the remote end can learn how long local NHRP peer entries can be retained. When a network exception occurs, the remote end deletes local NHRP peer entries based on the configured aging time. After the network recovers, a spoke registers with the hub to generate new NHRP peer entries.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

When you run this command to change the aging time of NHRP peer entries:

- If the value is too large, the device cannot delete NHRP peer entries in time.
- If the value is too small, a smaller interval for sending Registration packets must be configured on the peer device. This results in frequent sending of Registration packets, wasting network resources.

Precautions

The value of *seconds* must be larger than the value configured using the **nhrp registration interval** command so that the hub can receive re-registration packets from a spoke within the entry hold time.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the aging time of NHRP peer entries to 1800 seconds.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry holdtime seconds 1800
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.10 nhrp registration interval

12.5.7 nhrp entry multicast dynamic

Function

The **nhrp entry multicast dynamic** command enables the Hub to add dynamically registered Spokes to the NHRP multicast member table.

The **undo nhrp entry multicast dynamic** command disables the Hub to add dynamically registered Spokes from the NHRP multicast member table.

By default, no dynamically registered Spoke is added to the NHRP multicast member table.

Format

nhrp entry multicast dynamic

undo nhrp entry multicast dynamic

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the RIP or OSPF protocol is deployed on the DSVPN network, run the **nhrp entry multicast dynamic** command to enable the Hub to add dynamically registered Spokes to the multicast member table. This allows Spokes to learn routes from each other. After receiving routing multicast packets sent from Spokes, the Hub copies these routing multicast packets and forwards them to the

 Copyright © Huawei Technologies Co., Ltd.

destination Spoke based on the NHRP multicast member table. This allows routing multicast packets to be exchanged between Spokes.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

When a network has multiple Spokes and the Hub learns all the routes to these Spokes, the Hub consumes large CPU resources. In this case, you can configure a shortcut mode of DSVPN and the route summarization function to allow Spokes to directly communicate with each other.

Precautions

Run this command on the hub in both the shortcut and non-shortcut mode of DSVPN.

Example

Configure the Spoke registered on Tunnel0/0/0 to be dynamically added to the NHRP multicast member table of the Hub.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp entry multicast dynamic
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.5 nhrp entry

12.5.8 nhrp network-id

Function

The **nhrp network-id** command specifies the NHRP domain for a local mGRE interface.

The **undo nhrp network-id** command restores the default NHRP domain of the local mGRE interface.

By default, the local mGRE interface belongs to NHRP domain 0.

Format

nhrp network-id *number*

undo nhrp network-id

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies an NHRP domain. This domain takes effect only on the local device.	The value is an integer ranging from 1 to 4294967295.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **nhrp network-id** command specifies NHRP domains for mGRE interfaces to isolate various mGRE interfaces into different NHRP domains. A VPN tunnel is set up between two devices to forward NHRP packets. The network IDs of the inbound and outbound mGRE interfaces determine whether to set up a tunnel.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

If the inbound and outbound interfaces for NHRP packets are both mGRE interfaces, compare the network IDs of the two interfaces. The configuration impact on different types of NHRP packets is as follows:

- NHRP Registration Request packet and NHRP Registration Reply packet

  The NHRP module does not forward NHRP Registration packets. Therefore, it has no impact on the NHRP registration process.
- NHRP Resolution Request packet

  If the inbound and outbound mGRE interfaces for the NHRP packets have different network IDs, the NHRP module discards the packet and sends an NHRP Resolution Reply packet to the source peer device.
- NHRP Resolution Reply packet, Purge Request packet, Purge Reply packet and Redirect packet

  If the inbound and outbound mGRE interfaces for the NHRP packets have different network IDs, the NHRP module discards the packet.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After network IDs are changed, the NHRP peer learned by the device is not affected and the existing IPSec tunnel will not be changed.

Example

Set the network ID of an NHRP domain to 100.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp network-id 100
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.9 nhrp redirect

Function

The **nhrp redirect** command enables the NHRP redirect function.

The **undo nhrp redirect** command disables the NHRP redirect function.

By default, the NHRP redirect function is disabled.

Format

nhrp redirect

undo nhrp redirect

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the shortcut scenario, enable the NHRP redirect function on the hub. The hub sends NHRP Redirect packets to the source spoke while forwarding data flows within the NHRP domain. After receiving the NHRP Redirect packets, the source spoke sends NHRP Resolution Request packets and then establishes a tunnel to communicate with the destination spoke.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

After you run this command on the hub, it takes effect no matter the NHRP shortcut function is enabled on a spoke or not. When you disable the NHRP shortcut function on spoke, the hub sends an NHRP Redirect packet whenever a data packet is received, this cause the wasting of CPU and network resources. Enabling the NHRP shortcut function on a spoke solves this problem.

Precautions

To allow two branches to directly communicate by establishing a tunnel, you must also enable the **nhrp shortcut** function on spokes.

Example

Enable the NHRP redirect function on Tunnel0/0/0.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp redirect
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.12 nhrp shortcut

12.5.10 nhrp registration interval

Function

The **nhrp registration interval** command sets the interval at which a spoke registers with the hub.

The **undo nhrp registration interval** command restores the interval to the default value.

By default, a spoke registers with the hub at an interval of 1800 seconds.

Format

nhrp registration interval *seconds*

undo nhrp registration interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
seconds	Specifies the interval at which a spoke registers with the hub.	The value is an integer that ranges from 5 to 31845, in seconds. The default value is 1800 seconds.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the tunnel address and public network address of a spoke change or the NHRP peer entry of the hub ages, the hub may fail to update the NHRP peer entry in time. In this case, run the **nhrp registration interval** command on the spoke to set the interval at which a spoke registers with the hub to a value smaller than the aging time of NHRP peer entries.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

When you run this command to change the interval at which a spoke registers with the hub:

- If the interval is too long, the spoke fails to immediately inform the hub of the latest branch information.
- If the interval is too short, the spoke frequently registers with the hub, wasting network resources.

Precautions

NOTICE

The value of the parameter *seconds* cannot be larger than the aging time of NHRP peer entries configured by using the **nhrp entry holdtime** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a spoke to register with the hub at an interval of 600 seconds.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp registration interval 600
```

Related Topics

12.3.10 interface tunnel

12.5.6 nhrp entry holdtime

12.3.21 tunnel-protocol

12.5.11 nhrp registration no-unique

Function

The **nhrp registration no-unique** command configures the device to send NHRP packets that carry the no-unique flag to instruct the remote end to overwrite conflicting NHRP peer entries.

The **undo nhrp registration no-unique** command configures the device to send NHRP packets that do not carry the no-unique flag to instruct the remote end not to overwrite conflicting NHRP peer entries.

By default, the device sends NHRP packets that do not carry the no-unique flag to instruct the remote end not to overwrite conflicting NHRP peer entries.

Format

nhrp registration no-unique

undo nhrp registration no-unique

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can only be configured on branch devices. When a branch device sends an NHRP Registration Reply packet to a headquarters device, whether this packet carries the no-unique flag determines whether the headquarters device overrides conflicting NHRP peer entries of this branch device.

 Copyright © Huawei Technologies Co., Ltd.

When a branch device performs NHRP registration with a headquarters device, the headquarters device generates an NHRP peer entry for this branch device. If the branch device performs NHRP registration again after its public IP address changes, by default, the NHRP registration packet sent by this branch device does not carry the no-unique flag. After the headquarters device receives this packet, it does not override the conflicting NHRP peer entry of this branch device and rejects this NHRP registration. If the headquarters device needs to save the latest branch device information and overrides the conflicting NHRP peer entry, run the **nhrp registration no-unique** command on the branch device to enable the NHRP registration packet sent by this branch device to carry the no-unique flag.

If a branch device dynamically obtains an IP address, for example, in an LTE scenario, you are advised to run the **nhrp registration no-unique** command on the branch device to send NHRP packets that carry the no-unique flag, instructing the headquarters device to overwrite the conflicting NHRP peer entry. Otherwise, the branch device cannot re-register with the headquarters device successfully.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Configuration Impact

The following situations occur when the spoke re-registers with the hub after the public address of the spoke is changed:

- If the **nhrp registration no-unique** command is used on the spoke, the device overrides existing NHRP peer entries with new NHRP peer entries.
- If the **nhrp registration no-unique** command is not configured on a spoke node, new NHRP peer entries will not override existing NHRP peer entries on a hub node and new registration entries will be discarded. New registration entries can successfully register only when old NHRP peer entries are aged out.

Example

Configure the device to send NHRP packets that carry the no-unique flag to instruct the remote end to overwrite conflicting NHRP peer entries.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp registration no-unique
```

Related Topics

12.3.10 interface tunnel
12.3.21 tunnel-protocol

12.5.12 nhrp shortcut

Function

The **nhrp shortcut** command enables the NHRP shortcut function.

The **undo nhrp shortcut** command disables the NHRP shortcut function.

By default, the NHRP shortcut function is disabled.

Format

nhrp shortcut

undo nhrp shortcut

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The hub sends NHRP Redirect packets to the source spoke while forwarding data flows within the NHRP domain. Run the **nhrp shortcut** command on the spoke to allow it to send NHRP Resolution Request packets to the destination spoke after it receives NHRP Redirect packets sent from the hub. A tunnel is directly established between two branches.

Prerequisites

The following operations have been performed:

1. Run the **interface tunnel** command to create a tunnel interface and display the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the tunnel encapsulation mode to mGRE.

Precautions

The NHRP shortcut function must work with the NHRP redirect function. Therefore, the NHRP redirect function must be enabled on the hub using the **nhrp redirect** command.

Example

Enable the NHRP shortcut function on Tunnel0/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp shortcut
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.5.9 nhrp redirect

12.5.13 nhrp tunnel-if-state related

Function

The **nhrp tunnel-if-state related** command associates the mGRE interface status of a Spoke with the Hub status.

The **undo nhrp tunnel-if-state related** command cancels associating the mGRE interface status of a Spoke with the Hub status.

By default, the mGRE interface status of a Spoke is not associated with the Hub status.

Format

nhrp tunnel-if-state related

undo nhrp tunnel-if-state related

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a DSVPN scenario, when a Spoke detects that the Hub status goes Down, the Spoke reports an alarm to the NMS to alert network administrators. If the intermediate network experiences a fault, the Spoke detects that the status of all Hubs goes Down; however, network administrators cannot view the network fault on the NMS monitor topology. To solve this problem, associate the mGRE interface status of the Spoke with the Hub status for rapid fault detection on the monitor topology. That is, the mGRE interface becomes Down when the Hub status is Down. Additionally, enable the system to send an email to instruct network

 Copyright © Huawei Technologies Co., Ltd.

administrators to rectify faults in a timely manner when the mGRE interface becomes Down. To associate the mGRE interface status of the Spoke with the Hub status, run the **nhrp tunnel-if-state related** command.

Prerequisites

Before executing this command, perform the following operations:

1. Run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface view.
2. Run the **tunnel-protocol gre p2mp** command to set the encapsulation mode of a tunnel interface to mGRE.

Example

Associate the mGRE interface status of a Spoke with the Hub status.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] nhrp tunnel-if-state related
```

12.5.14 reset nhrp peer maximum-history

Function

The **reset nhrp peer maximum-history** command clears the history statistics on NHRP peer entries.

Format

reset nhrp peer maximum-history

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear the history statistics on NHRP peer entries.

Example

Clear the history statistics on NHRP peer entries.

```
<Huawei> reset nhrp peer maximum-history
```

Related Topics

12.5.2 display nhrp peer maximum-history

12.5.15 reset nhrp statistics

Function

The **reset nhrp statistics** command clears NHRP packet statistics on a specified tunnel interface.

Format

reset nhrp statistics interface tunnel *interface-number*

Parameters

Parameter	Description	Value
interface tunnel *interface-number*	Specifies the interface number.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command clears NHRP packet statistics on a specified tunnel interface. This helps you locate DSVPN faults quickly.

Configuration Impact

This command clears NHRP packet statistics on a specified tunnel interface.

Precautions

NOTICE

Statistics cannot be restored after being cleared. Therefore, confirm the action before you run the command.

Example

Clear NHRP packet statistics on Tunnel0/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei>reset nhrp statistics interface tunnel 0/0/0
```

Related Topics

12.5.3 display nhrp statistics

12.5.16 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

12.5.17 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. ● **p2p**: indicates the P2P SVPN tunnel protocol. ● **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.

 Copyright © Huawei Technologies Co., Ltd.

- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.3.10 interface tunnel

12.5.18 undo nhrp peer

Function

The **undo nhrp peer** command deletes dynamically negotiated NHRP peer entries.

Format

undo nhrp peer [*protocol-address* [*mask*]]

Parameters

Parameter	Description	Value
protocol-address [*mask*]	Specifies the network layer protocol address and mask.	-

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command deletes dynamically negotiated NHRP peer entries before the entries age out. This prevents the existing NHRP peer entries from affecting the diagnosis result.

Configuration Impact

Dynamically negotiated NHRP peer entries are deleted from the local device and no entry will be generated before the peer device registers with the local device.

Precautions

NOTICE

- Deleting dynamically negotiated NHRP peer entries may result in communication interruption.
- Run this command only on the mGRE interface.

Example

Delete an NHRP peer entry with an IP address 10.10.10.10 and a 24-bit mask.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/0] undo nhrp peer 10.10.10.10 24
```

Related Topics

12.5.1 display nhrp peer
12.3.21 tunnel-protocol

12.6 IPSec Configuration Commands

12.6.1 aaa authorization

Function

The **aaa authorization** command configures AAA RADIUS server authorization.

The **undo aaa authorization** command cancels AAA RADIUS server authorization.

By default, AAA RADIUS server authorization is not configured.

Format

aaa authorization [**domain** *domain-name*]

undo aaa authorization

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name.	The domain name must already exist.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the remote device establishes an IKE SA with the server, you can run this command on the server to enable AAA RADIUS server authorization. If the **domain** parameter is specified, the remote device obtains authorization information using the specified **domain**. If the **domain** parameter is not specified, the remote device obtains authorization information using the domain name it sends to the server. The domain name is specified using the **service-scheme** command in the Efficient VPN policy view.

Prerequisite

A domain has been created using the **domain (AAA view)** command.

Precautions

After you configure this command on the server, the **service-scheme** command does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the domain name for AAA RADIUS server authorization to **abc**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain abc
[Huawei-aaa-domain-abc] quit
[Huawei] ike peer p1
[Huawei-ike-peer-p1] aaa authorization domain abc
```

12.6.2 alias

Function

The **alias** command sets an alias of an IPSec policy or IPSec policy template.

The **undo alias** command restores the default alias of an IPSec policy or IPSec policy template.

By default, the alias of an IPSec policy or IPSec policy template is the combination of its name and ID. If the default alias has been used by another IPSec policy or IPSec policy template, the system defines the default alias of the IPSec policy or IPSec policy template by combining the current time with its name and ID.

Format

alias *alias*

undo alias

Parameters

Parameter	Description	Value
alias	Specifies an alias for an IPSec policy or IPSec policy template.	The value is a string of 1 to 127 case-sensitive characters. It can contain special characters, such as !, @, #, $, and %, but cannot contain question marks.

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In real-world applications, multiple IPSec policies or IPSec policy templates are often configured in an IPSec policy group. In this case, you can use the **alias** command to configure alias to identify these IPSec policies or IPSec policy templates. It is recommended that you configure meaningful alias that are easy to remember.

Precautions

The alias of each IPSec policy or IPSec policy template must be unique. Otherwise, the system displays a configuration failure message.

Example

Configure the alias **huawei** for the IPSec policy **policy1** with the ID of 1.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] alias huawei
```

12.6.3 ah authentication-algorithm

Function

The **ah authentication-algorithm** command configures the AH authentication algorithm.

The **undo ah authentication-algorithm** command restores the default AH authentication algorithm.

By default, the AH authentication algorithm is SHA2-256.

Format

ah authentication-algorithm { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo ah authentication-algorithm

Parameters

Parameter	Description	Value
md5	Uses the message digest algorithm 5 (MD5) authentication algorithm.	-
sha1	Uses the Secure Hash Algorithm 1 (SHA-1) authentication algorithm.	-
sha2-256	Uses the SHA2-256 authentication algorithm.	-
sha2-384	Uses the SHA2-384 authentication algorithm.	-
sha2-512	Uses the SHA2-512 authentication algorithm.	-
sm3	Uses the SM3 authentication algorithm.The algorithm can be used only in IKEv1 negotiation.When the SM3 algorithm is used, the padding mode of RSA signing cannot be PSS.	-

 Copyright © Huawei Technologies Co., Ltd.

NOTE

AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The AH protocol only authenticates packets and does not provide the encryption function.

Authentication algorithms that can be used in an IPSec proposal include the following (listed in descending order of security level): **sha2-512** > **sha2-384** > **sha2-256** > **sha1** > **md5**.

Prerequisites

ah or **ah-esp** has been specified in the **transform** command.

Precautions

Both ends of an IPSec tunnel must use the same authentication algorithm.

Authentication algorithms **sha2-256**, **sha2-384**, and **sha2-512** are recommended for security purpose. **md5** and **sha1** are not recommended.

Example

Specify the SHA2-256 algorithm for the AH protocol in the IPSec proposal **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform ah
[Huawei-ipsec-proposal-newprop1] ah authentication-algorithm sha2-256
```

Related Topics

12.6.40 display ipsec proposal (All views)

12.6.4 ah authentication-algorithm (ipsec-proto-protect-proposal view)

Function

The **ah authentication-algorithm** command configures the authentication algorithm for Authentication Header (AH).

The **undo ah authentication-algorithm** command restores the default authentication algorithm for AH.

By default, the authentication algorithm SHA2-256 is used for AH.

Format

ah authentication-algorithm { **md5** | **sha1** | **sha2-256** }

undo ah authentication-algorithm

Parameters

Parameter	Description	Value
md5	Configures MD5 as the authentication algorithm for AH. **NOTE** To ensure high security, do not use the MD5 algorithm as the AH authentication algorithm.	-
sha1	Configures Secure Hash Algorithm-1 (SHA1) as the authentication algorithm for AH. **NOTE** To ensure high security, do not use the SHA1 algorithm as the AH authentication algorithm.	-
sha2-256	Configures SHA2-256 as the authentication algorithm for AH.	-

Views

IPSec proto-protect proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH is used to prevent packets from being intercepted or modified and implement data origin authentication during data transmission. AH implements the Hash algorithm on the sending and receiving parties and checks data integrity and authenticity.

 Copyright © Huawei Technologies Co., Ltd.

AH currently supports MD5, SHA-1 and SHA2-256 authentication algorithms.

- MD5: generates a 128-bit message summary for an input message of any length
- SHA-1: generates a 160-bit message summary for an input message of less than 2^{64} bits
- SHA2-256: generates a 256-bit message summary for an input message of less than 2^{64} bits

MD5 is faster than SHA-1, but is less secure.

Prerequisite

The **transform** command has been configured to select AH before the authentication algorithm for AH is configured.

Precautions

The authentication algorithms on both IPSec peers must be identical.

Example

Set the authentication algorithm to SHA-1 for AH.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform ah
[Huawei-ipsec-proto-protect-proposal-prop1] ah authentication-algorithm sha1
```

12.6.5 anti-replay window

Function

The **anti-replay window** command sets the anti-replay window size for an IPSec tunnel.

The **undo anti-replay window** command restores the default anti-replay window size of an IPSec tunnel.

By default, the anti-replay window size of a single IPSec tunnel is not set. The global value is used.

Format

anti-replay window *window-size*

undo anti-replay window

Parameters

Parameter	Description	Value
window-size	Specifies the anti-replay window size of an IPSec tunnel.	The value can be 32, 64, 128, 256, 512, or 1024, in bits.

 Copyright © Huawei Technologies Co., Ltd.

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Configuration Impact

You may need to change the anti-replay window size for an IPSec tunnel in some situations. For example, if QoS is performed for packets passing an IPSec tunnel, sequence numbers of service data packets may be different from those in common data packets. As a result, these service data packets are dropped as replay attack packets. To prevent such packets from being dropped incorrectly, you can disable the anti-replay function or increase the anti-replay window size for the IPSec tunnel.

Prerequisites

The anti-replay function is enabled for the IPSec tunnel. By default, the anti-replay function is enabled (through **ipsec anti-reply enable** command).

Precautions

When both **anti-replay window** and **ipsec anti-replay window** are configured, the **anti-replay window** configuration takes effect. When **anti-replay window** is not configured, the **ipsec anti-replay window** configuration takes effect.

Example

Set the IPSec anti-replay window size to 128 bits.

```
<Huawei> system-view
[Huawei] ipsec policy poli 10 isakmp
[Huawei-ipsec-policy-isakmp-poli-10] anti-replay window 128
```

Related Topics

12.6.93 ipsec anti-replay window

12.6.34 display ipsec policy (all views)

12.6.36 display ipsec policy-template (all views)

12.6.38 display ipsec profile (all views)

12.6.30 display ipsec efficient-vpn

12.6.6 authentication-algorithm

Function

The **authentication-algorithm** command configures an authentication algorithm for IKEv1 negotiation.

The **undo authentication-algorithm** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, the SHA2-256 authentication algorithm is used for IKEv1 negotiation.

Format

authentication-algorithm { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo authentication-algorithm

Parameters

Parameter	Description	Value
md5	Uses the message digest algorithm 5 (MD5) authentication algorithm.	-
sha1	Uses the Secure Hash Algorithm 1 (SHA-1) authentication algorithm.	-
sha2-256	Uses the SHA2-256 authentication algorithm.	-
sha2-384	Uses the SHA2-384 authentication algorithm.	-
sha2-512	Uses the SHA2-512 authentication algorithm.	-
sm3	Uses the SM3 authentication algorithm.The algorithm can be used only in IKEv1 negotiation.When the SM3 algorithm is used, the padding mode of RSA signing cannot be PSS.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

An authentication algorithm is required for IKEv1 negotiation. Authentication algorithms that can be used for IKEv1 negotiation include the following (listed in descending order of security level): **sha2-512** > **sha2-384** > **sha2-256** > **sha1** > **md5**.

NOTE

md5 and **sha1** are not recommended because they cannot provide high security.

Example

Specify the SHA2-384 authentication algorithm for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] authentication-algorithm sha2-384
```

Related Topics

12.6.22 display ike proposal (All views)

12.6.7 authentication-method

Function

The **authentication-method** command specifies the authentication method used in IKE negotiation.

The **undo authentication-method** command restores the default authentication method.

By default, pre-shared key authentication is used in IKE negotiation.

Format

authentication-method { **pre-share** | **rsa-signature** }

undo authentication-method

Parameters

Parameter	Description	Value
pre-share	Uses pre-shared key authentication.	-
rsa-signature	Uses RSA signature authentication.	-

Views

IKE proposal view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a protection mechanism that ensures secure data transmission on an insecure network. This command configures an identity authentication method.

Precautions

The authentication methods in the IKE proposals used by the IKE peer must be the same. Otherwise, IKE negotiation fails.

For IKEv1, the **authentication-method** command does not take effect in the Efficient VPN policy view.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

- If **pre-share** is specified, run the **pre-shared-key** command to specify an authentication key.
- If **rsa-signature** is specified, configure a local certificate.

Example

Configure pre-shared key authentication in IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] authentication-method pre-share
```

Configure pre-shared key authentication for Efficient VPN policy **vpn1**.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn vpn1 mode client
[Huawei-ipsec-efficient-vpn-vpn1] authentication-method pre-share
```

Related Topics

12.6.76 ike proposal
12.6.22 display ike proposal (All views)
12.6.30 display ipsec efficient-vpn
12.6.98 ipsec efficient-vpn (system view)

12.6.8 certificate peer-name

Function

The **certificate peer-name** command enables IKEv1 digital envelope negotiation to use the peer certificate file imported to the PKI.

The **undo certificate peer-name** command disables IKEv1 digital envelope negotiation from using the peer certificate file imported to the PKI.

By default, the system does not use the peer certificate file imported to the PKI for IKEv1 digital envelope negotiation.

Format

certificate peer-name *peer-name*

undo certificate peer-name

Parameters

Parameter	Description	Value
peer-name *peer-name*	Specifies the name of the digital certificate of an IKE peer.	The digital certificate must have been imported to the PKI.

Views

IKE peer view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

If the authentication method is digital envelope (**digital-envelope**), you can use the peer digital certificate imported to the PKI. IKEv1 obtains the certificate public key through the peer digital certificate for digital envelope negotiation.

Example

Import the peer digital certificate **aa.pem** and reference it in the IKE peer.

```
<Huawei> system-view
[Huawei] pki import-certificate peer abcd pem filename aa.pem
[Huawei] ike peer a
[Huawei-ike-peer-a] certificate peer-name abcd
```

Related Topics

12.6.7 authentication-method

12.6.9 certificate-check disable

Function

The **certificate-check disable** command disables validity verification on certificates of an IKE peer.

The **undo certificate-check disable** command restores the default configuration.

By default, the device verifies certificates of an IKE peer.

Format

certificate-check disable

undo certificate-check disable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IPSec uses certificate authentication, users cannot update certificates after they become invalid, leading to unavailable certificates and IPSec authentication failure. If users still want to use these invalid certificates, run the **certificate-check disable** command to disable validity verification on certificates of an IKE peer. If users do not want to verify certificates of all IKE peers, run the **12.6.65 ike certificate-check disable** command.

Precautions

Disabling validity verification on certificates will lead to security risks.

Example

Configure the device not to verify certificates of an IKE peer.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] certificate-check disable
```

Related Topics

12.6.20 display ike peer (all views)

12.6.10 certificate-request empty-payload enable

Function

The **certificate-request empty-payload enable** command configures a router to send certificate requests with empty payload.

The **undo certificate-request empty-payload enable** command restores the default configuration.

By default, certificate requests sent from a router carries CA information in the payload.

Format

certificate-request empty-payload enable

undo certificate-request empty-payload enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a router acting as a gateway in the headquarters uses an IPSec policy configured using a policy template and authenticates branches by digital certificates, you can run the **certificate-request empty-payload enable** command to send certificate requests with empty payload, allowing access from branches using certificates issued by different CAs. The router can then perform certificate authentication based on certificate information provided by each branch.

Precautions

Do not configure this command if access devices cannot process certificate request packets with an empty authentication and authorization field. Otherwise, IKE negotiation fails.

Example

Configure the router to send certificate requests with empty payload.

```
<Huawei> system-view
[Huawei] ike peer a20
[Huawei-ike-peer-a20] certificate-request empty-payload enable
```

12.6.11 config-exchange

Function

The **config-exchange** command enables the device to request or set subnet route information.

The **undo config-exchange** command disables the device from requesting or setting subnet route information.

By default, the device cannot request or set subnet route information.

Format

config-exchange { **request** | **set** { **accept** | **send** } }

undo config-exchange { **request** | **set** [**accept** | **send**] }

Parameters

Parameter	Description	Value
request	Enables the device to request subnet route information from a remote device.	-

Parameter	Description	Value
set { **accept** | **send** }	Enables the device to accept subnet route information from a remote device or send local subnet route information.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A headquarters gateway sets up an IPSec tunnel with a branch gateway in virtual tunnel mode. In this case, you can run the **config-exchange** command to enable the gateways to request or set subnet route information.

1. The **config-exchange request** command can only be used on the initiator to enable it to request subnet information from the responder.
2. The **config-exchange set** { **accept** | **send** } command can be configured on both the initiator and the responder.
   - The **config-exchange set accept** command enables the local device to accept subnet route information sent by the remote device.
   - The **config-exchange set send** command enables the local device to send subnet route information to the remote device.

   If the **config-exchange set send** command is configured on the local device, the **config-exchange set accept** command must be configured on the remote device.

Prerequisites

Before you configure the **config-exchange set send** command to enable the local device to send subnet route information, the following operations must have been completed in the AAA service scheme.

- Run the **route set acl** *acl-number* command to configure local subnet route information.
- Run the **route set interface** command to configure interface addresses to which the IPSec profile is applied.

Precautions

This command is supported by IKEv2 only.

 Copyright © Huawei Technologies Co., Ltd.

If the **config-exchange set accept** command is configured on the local device, the **route accept** command must also be configured before the local device can accept subnet route information sent by the remote device and generate routes.

Example

Enable the IKE peer named **peer1** to accept subnet route information from the remote device.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] config-exchange set accept
```

Related Topics

12.6.75 ike peer

12.6.149 route accept

12.6.12 connect track

Function

The **connect track** command configures the device to control IPSec tunnel setup according to the NQA test instance, NQA group, BFD session, or BFD group status.

The **undo connect track** command cancels the configuration.

By default, the device is configured not to control IPSec tunnel setup according to the NQA test instance, NQA group, BFD session, or BFD group status.

Format

connect track { **nqa** *admin-name test-name* | **nqa-group** *nqa-group-name* | **bfd-session** *bfd-session-name* | **bfd-session-group** *bfd-group-name* } { **up** | **down** }

undo connect track { **nqa** | **nqa-group** | **bfd-session** | **bfd-session-group** }

Parameters

Parameter	Description	Value
nqa *admin-name test-name*	Configures the device to control IPSec tunnel setup according to the NQA test instance status. *admin-name* and *test-name* specify the administrator name and name of the NQA test instance respectively.	The administrator name or name of an NQA test instance must have been created.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
nqa-group *nqa-group-name*	Configures the device to control IPSec tunnel setup according to the NQA group status. *nqa-group-name* specifies the name of the NQA group.	The value is a string of 1 to 32 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.
bfd-session *bfd-session-name*	Configures the device to control IPSec tunnel setup according to the BFD session status. *bfd-session-name* specifies the name of the BFD session.	The BFD session name must have been created.
bfd-session-group *bfd-group-name*	Configures the device to control IPSec tunnel setup according to the BFD group status. *bfd-group-name* specifies the name of the BFD group.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.
up	Indicates that an IPSec tunnel is set up when the NQA test instance, NQA group, BFD session, or BFD group status is Up.	-
down	Indicates that an IPSec tunnel is set up when the NQA test instance, NQA group, BFD session, or BFD group status is Down.	-

Views

View of the IPSec policy established in ISAKMP mode

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, to improve network reliability, a branch gateway connects to the headquarters using multiple links. The branch gateway needs to determine on which link an IPSec tunnel is established. You can associate IPSec with NQA or BFD so that the branch gateway controls IPSec tunnel setup according to the NQA test instance, NQA group, BFD session, or BFD group status, which ensures that only one link is available at any time.

Prerequisites

- An NQA test instance has been created using the **nqa** command and the NQA test instance type has been set to ICMP using the **test-type** command if **nqa** *admin-name test-name* is specified.
- A BFD session has been created using the **bfd bind peer-ip** command and the BFD session has been set the local and remote discriminators using the **discriminator** command if **bfd-session** *bfd-session-name* is specified.

Precautions

- The device supports only association between IPSec and the NQA test instance of ICMP.
- The NQA test instance, NQA group, BFD session, and BFD group cannot be configured simultaneously in this scenario. That is, the device controls IPSec tunnel setup using a specified IPSec policy according to one of the NQA test instance, NQA group, BFD session, BFD group, and VRRP group status.
- When **nqa-group** *nqa-group-name* is specified, you do not need to create an NQA group first. However, the configuration takes effect only when the NQA group is created and configured using the **nqa-group** and **nqa (nqa-group view)** commands respectively.
- When **bfd-session-group** *bfd-group-name* is specified, you do not need to create a BFD group first. However, the configuration takes effect only when the BFD group is created and configured using the **bfd-group** and **track bfd** commands respectively.
- **connect track** needs to be used with **disconnect track** to implement link redundancy control.

Example

Configure the device to establish an IPSec tunnel when the NAQ test instance (administrator name **admin** and instance name **test**) status is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type icmp
[Huawei-nqa-admin-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] connect track nqa admin test up
```

Configure the device to establish an IPSec tunnel when the status of the NAQ group **ngroup** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] connect track nqa-group ngroup down
```

Configure the device to establish an IPSec tunnel when the status of the BFD session **test** is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 10.1.1.1 255.255.255.0
[Huawei-Ethernet2/0/0] quit
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ip 10.1.1.2 interface ethernet 2/0/0
[Huawei-bfd-session-test] discriminator local 10
[Huawei-bfd-session-test] discriminator remote 20
[Huawei-bfd-session-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] connect track bfd-session test up
```

Configure the device to establish an IPSec tunnel when the status of the BFD group **bfd-group1** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] connect track bfd-session-group bfd-group1 down
```

12.6.13 description

Function

The **description** command configures the description for an IKE user.

The **undo description** command deletes the description of an IKE user.

By default, the description of an IKE user is not configured.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an IKE user.	The value is a string of 1 to 63 case-sensitive characters.

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

To identify IKE users, run the **description** command to configure the description for the IKE users. For example, you can describe branches corresponding to IKE users,

Example

Configure the description for an IKE user.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] description user1
```

Related Topics

12.6.27 display ike user-table (all views)

12.6.14 dh

Function

The **dh** command specifies a Diffie-Hellman (DH) group used for IKE negotiation.

The **undo dh** command restores the default DH group for IKE negotiation.

By default, group14 is used for IKE negotiation.

Format

dh { **group1** | **group2** | **group5** | **group14** | **group19** | **group20** | **group21** }

undo dh

Parameters

Parameter	Description	Value
group1	Uses the 768-bit DH group in IKE negotiation phase 1.	-
group2	Uses the 1024-bit DH group in IKE negotiation phase 1.	-
group5	Uses the 1536-bit DH group in IKE negotiation phase 1.	-
group14	Uses the 2048-bit DH group in IKE negotiation phase 1.	-
group19	Uses the 256-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-
group20	Uses the 384-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group21	Uses the 521-bit Elliptic Curve Groups modulo a Prime (ECP) DH group in IKE negotiation phase 1.	-

Views

IKE proposal view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DH algorithm is a public key algorithm. Two communicating parties calculate a shared key based on data exchanged between them, without transmitting the key. A third party (such as a hacker) cannot calculate the actual key even if it obtains all exchanged data for key calculation.

Precautions

- Both ends of an IPSec tunnel must be configured with the same DH group. Otherwise, the negotiation fails.
- The security level order of the DH groups is: **group21** > **group20** > **group19** > **group14** > **group5** > **group2** > **group1**.
- The **group1**, **group2**, and **group5** have potential security risks. The other DH groups are recommended.

Example

Specify the 2048-bit DH group for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] dh group14
```

Specify the 2048-bit DH group for the IPSec Efficient VPN policy.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] dh group14
```

Related Topics

12.6.22 display ike proposal (All views)

12.6.30 display ipsec efficient-vpn

12.6.15 disconnect track

Function

The **disconnect track** command configures the device to control IPSec tunnel teardown according to the NQA test instance, NQA group, BFD session, or BFD group status.

 Copyright © Huawei Technologies Co., Ltd.

The **undo disconnect track** command cancels the configuration.

By default, the device is configured not to control IPSec tunnel teardown according to the NQA test instance, NQA group, BFD session, or BFD group status.

Format

disconnect track { **nqa** *admin-name test-name* | **nqa-group** *nqa-group-name* | **bfd-session** *bfd-session-name* | **bfd-session-group** *bfd-group-name* } { **up** | **down** }

undo disconnect track { **nqa** | **nqa-group** | **bfd-session** | **bfd-session-group** }

Parameters

Parameter	Description	Value
nqa *admin-name test-name*	Configures the device to control IPSec tunnel teardown according to the NQA test instance status. *admin-name* and *test-name* specify the administrator name and name of the NQA test instance respectively.	The administrator name or name of an NQA test instance must have been created.
nqa-group *nqa-group-name*	Configures the device to control IPSec tunnel teardown according to the NQA group status. *nqa-group-name* specifies the name of the NQA group.	The value is a string of 1 to 32 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.
bfd-session *bfd-session-name*	Configures the device to control IPSec tunnel teardown according to the BFD session status. *bfd-session-name* specifies the name of the BFD session.	The BFD session name must have been created.
bfd-session-group *bfd-group-name*	Configures the device to control IPSec tunnel teardown according to the BFD group status. *bfd-group-name* specifies the name of the BFD group.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

up	Indicates that an IPSec tunnel is torn down when the NQA test instance, NQA group, BFD session, or BFD group status is Up.	-
down	Indicates that an IPSec tunnel is torn down when the NQA test instance, NQA group, BFD session, or BFD group status is Down.	-

Views

View of the IPSec policy established in ISAKMP mode

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, to improve network reliability, a branch gateway connects to the headquarters using multiple links. The link where an IPSec tunnel is established needs to be determined. You can associate IPSec with NQA or BFD so that the branch gateway controls IPSec tunnel teardown according to the NQA test instance, NQA group, BFD session, or BFD group status, which ensures that only one link is available at any time.

Prerequisites

- An NQA test instance has been created using the **nqa** command and the NQA test instance type has been set to ICMP using the **test-type** command if **nqa** *admin-name test-name* is specified.
- A BFD session has been created using the **bfd bind peer-ip** command and the BFD session has been set the local and remote discriminators using the **discriminator** command if **bfd-session** *bfd-session-name* is specified.

Precautions

- The device supports only association between IPSec and the NQA test instance of ICMP.
- When **nqa-group** *nqa-group-name* is specified, you do not need to create an NQA group first. However, the configuration takes effect only when the NQA group is created and configured using the **nqa-group** and **nqa (nqa-group view)** commands respectively.
- When **bfd-session-group** *bfd-group-name* is specified, you do not need to create a BFD group first. However, the configuration takes effect only when

the BFD group is created and configured using the **bfd-group** and **track bfd** commands respectively.

- **disconnect track** needs to be used with **connect track** to implement link redundancy control.

Example

Configure the device to terminate an IPSec tunnel when the NAQ test instance (administrator name **admin** and instance name **test**) status is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type icmp
[Huawei-nqa-admin-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] disconnect track nqa admin test up
```

Configure the device to terminate an IPSec tunnel when the status of the NAQ group **ngroup** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] disconnect track nqa-group ngroup down
```

Configure the device to terminate an IPSec tunnel when the status of the BFD session **test** is Up in the view of the IPSec policy **policy1** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 10.1.1.1 255.255.255.0
[Huawei-Ethernet2/0/0] quit
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ip 10.1.1.2 interface ethernet 2/0/0
[Huawei-bfd-session-test] discriminator local 10
[Huawei-bfd-session-test] discriminator remote 20
[Huawei-bfd-session-test] quit
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] disconnect track bfd-session test up
```

Configure the device to terminate an IPSec tunnel when the status of the BFD group **bfd-group1** is Down in the view of the IPSec policy **policy2** established in ISAKMP mode.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 200 isakmp
[Huawei-ipsec-policy-isakmp-policy2-200] disconnect track bfd-session-group bfd-group1 down
```

12.6.16 display ike error-info

Function

The **display ike error-info** command displays information about IPSec tunnel negotiation failures using IKE.

Format

display ike error-info [**verbose**] [**peer** *remote-address*]

Parameters

Parameter	Description	Value
verbose	Displays details about IPSec tunnel negotiation failures using IKE.	-
peer *remote-address*	Displays information about IPSec tunnel negotiation failures using IKE with a specified remote IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output contains information of the latest 200 IPSec tunnel negotiation failures using IKE.

Example

Display information about IPSec tunnel negotiation failures using IKE.

```
<Huawei> display ike error-info

 current info Num :2
 Ike error information:
 current ike Error-info number :2
  -------------------------------------------------------------------------------
  peer      port      error-reason                version     error-time
  -------------------------------------------------------------------------------
10.1.1.1   500       phase1 proposal mismatch     v1          2013-08-26
13:42:37
10.1.1.1   500       phase1 proposal mismatch     v1          2013-08-26 13:08:45
```

Display details about IPSec tunnel negotiation failures using IKE.

```
<Huawei> display ike error-info verbose

  current info Num :1
  Ike error information:
  current ike Error-info number :1
-------------------------------------------------------------------------------
Peer       : 10.1.1.1
Port       : 500
version    : v1
Reason     : phase1 proposal mismatch
Detail     : phase1 proposal mismatch
Error-time : 2013-08-26 12:02:37
-------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-16 Description of the **display ike error-info** command output

Item	Description
current info Num	Current information number.
Ike error information	Information about IPSec tunnel negotiation failures using IKE.
current ike Error-info number	Number of IPSec tunnel negotiation failures using IKE.
peer or Peer	Remote IP address.
port or Port	Peer UDP port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
error-reason or Reason	Causes for IPSec tunnel negotiation failures using IKE: ● phase1 proposal mismatch: IKE proposal parameters of the two ends do not match. ● phase2 proposal or pfs mismatch: IPSec proposal parameters, pfs algorithm, or security ACL of the two ends do not match. ● responder dh mismatch: The DH algorithm of the responder does not match. ● initiator dh mismatch: The DH algorithm of the initiator does not match. ● encapsulation mode mismatch: The encapsulation mode does not match. ● flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match. ● version mismatch: The IKE version number of the two ends does not match. ● peer address mismatch: The IKE peer address of the two ends does not match. ● config ID mismatch: The IKE peer of the specified ID is not found. ● exchange mode mismatch: The negotiation mode of the two ends does not match. ● authentication fail: Identity authentication fails. ● construct local ID fail: The local ID fails to be constructed. ● rekey no find old sa: The old SA is not found during re-negotiation. ● rekey fail: The old SA is going offline during re-negotiation. ● first packet limited: The rate of the first packet is limited. ● unsupported version: The IKE version number is not supported. ● malformed message: Malformed message. ● malformed payload: Malformed payload. ● critical drop: Unidentified critical payload. ● cookie mismatch: Cookie mismatch. ● invalid cookie: Invalid cookie. ● invalid length: Invalid packet length. ● unknown exchange type: Unknown negotiation mode. ● uncritical drop: Unidentified non-critical payload. ● route limit: The number of injected routes has reached the upper limit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• ip assigned fail: IP address allocation fails. • local address mismatch: The local IP address in IKE negotiation and interface IP address do not match. • dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit. • ipsec tunnel number reaches limitation: The number of IPSec tunnels reaches the upper limit. • netmask mismatch: The mask does not match the configured mask after the IPSec mask filtering function is enabled. • flow confict: A data flow conflict occurs. • proposal mismatch or use sm in ikev2: IPSec proposals at both ends of the IPSec tunnel do not match or IKEv2 uses the SM algorithm. • ikev2 not support sm in ipsec proposal ikev2: IKEv2 does not support the SM algorithm used in the IPSec proposal. • no policy applied on interface: No policy is applied to an interface. • nat detection fail: NAT detailed failed. • fragment packet limit: Fragment packets exceed the limit. • fragment packet reassemble timeout: Fragment packet reassembly times out. • proposal mismatch or use sm in ikev2: The received IPSec proposal parameters do not match the local parameters or IKEv2 uses the SM algorithm.
version	IKE version.
Error-time/error-time	Time of IPSec tunnel negotiation failures using IKE.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Detail	Details about IPSec tunnel negotiation failures using IKE. ● phase1 proposal mismatch: IKE proposal parameters of the two ends do not match. ● phase2 proposal or pfs mismatch: IPSec proposal parameters, pfs algorithm, or security ACL of the two ends do not match. ● responder dh mismatch: The DH algorithm of the responder does not match. ● initiator dh mismatch: The DH algorithm of the initiator does not match. ● encapsulation mode mismatch: The encapsulation mode does not match. ● flow or peer mismatch: The security ACL or IKE peer address of the two ends does not match. ● version mismatch: The IKE version number of the two ends does not match. ● peer address mismatch: The IKE peer address of the two ends does not match. ● config ID mismatch: The IKE peer of the specified ID is not found. ● exchange mode mismatch: The negotiation mode of the two ends does not match. ● authentication fail: Identity authentication fails. ● construct local ID fail: The local ID fails to be constructed. ● rekey no find old sa: The old SA is not found during re-negotiation. ● rekey fail: The old SA is going offline during re-negotiation. ● first packet limited: The rate of the first packet is limited. ● unsupported version: The IKE version number is not supported. ● malformed message: Malformed message. ● malformed payload: Malformed payload. ● critical drop: Unidentified critical payload. ● cookie mismatch: Cookie mismatch. ● invalid cookie: Invalid cookie. ● invalid length: Invalid packet length. ● unknown exchange type: Unknown negotiation mode. ● uncritical drop: Unidentified non-critical payload. ● route limit: The number of injected routes has reached the upper limit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• ip assigned fail: IP address allocation fails. • local address mismatch: The local IP address in IKE negotiation and interface IP address do not match. • dynamic peers number reaches limitation: The number of IKE peers reaches the upper limit. • ipsec tunnel number reaches limitation: The number of IPSec tunnels reaches the upper limit. • netmask mismatch: The mask does not match the configured mask after the IPSec mask filtering function is enabled. • flow confict: A data flow conflict occurs. • proposal mismatch or use sm in ikev2: IPSec proposals at both ends of the IPSec tunnel do not match or IKEv2 uses the SM algorithm. • ikev2 not support sm in ipsec proposal ikev2: IKEv2 does not support the SM algorithm used in the IPSec proposal. • no policy applied on interface: No policy is applied to an interface. • nat detection fail: NAT detailed failed. • fragment packet limit: Fragment packets exceed the limit. • fragment packet reassemble timeout: Fragment packet reassembly times out. • proposal mismatch or use sm in ikev2: The received IPSec proposal parameters do not match the local parameters or IKEv2 uses the SM algorithm. • receive phase1 proposal mismatch: The received IKE proposal parameters do not match the local parameters. • receive phase2 proposal mismatch: The received IPSec proposal parameters do not match the local parameters. • phase2 proposal mismatch: IPSec proposal parameters on both ends do not match. • receive flow or peer mismatch: The received security ACL or IKE peer address does not match the local one. • (peer local or tunnel local or interface) address mismatch: The peer's local IP address, local tunnel IP address or interface IP address does not match the local one. • remote auth method mismatch: The peer authentication method does not match. • proc cert fail or inband cert validate fail: Failed to process or verify the certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	● outband cert validate fail(rsa-signature): Certificate verification failed during RSA signature authentication. ● hash value not equal(pre-share-key): The hash values are different during pre-shared key authentication. ● hash value not equal(digital-envelope): The hash values are different during digital signature authentication. ● verify sig data fail(rsa-signature): Failed to verify the signature. ● proc auth payload fail(pre-share-key): Failed to process the authentication payload during pre-shared key authentication. ● proc auth payload fail(rsa-signature): Failed to process the authentication payload during RSA signature authentication. ● recv peer auth fail notification: An authentication failure notification from the peer end is received. ● recv peer auth fail notification(pre-share-key): An authentication failure notification from the peer end is received during pre-shared key authentication. ● recv peer auth fail notification(rsa-signature): An authentication failure notification from the peer end is received during RSA signature authentication. ● recv peer auth fail notification(digital-envelope): An authentication failure notification from the peer end is received during digital signature authentication. ● proc and auth ID payload fail(pre-share-key): The peer ID fails to be authenticated during pre-shared key authentication. ● proc and auth ID payload fail(rsa-signature): The peer ID fails to be authenticated during RSA signature authentication. ● can not find key by cert: Failed to obtain the key pair corresponding to the certificate. ● the cert is not valid: The certificate is invalid. ● cert revoked by CRL: The certificate is revoked by the CRL. ● unable to get issuer cert: The issuer cannot be found. ● ocsp valid fail: Failed to check the certificate online. ● cert filter check mismatch: The certificate filtering verification does not match. ● no corresponding CRL: No corresponding CRL exists. ● inband cert validate fail: Failed to verify the certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• receive proposal mismatch or use sm in ikev2: The received IPSec proposal parameters do not match the local parameters or IKEv2 uses the SM algorithm.

12.6.17 display ike global config

Function

The **display ike global config** command displays the global IKE configuration.

Format

display ike global config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the global IKE configuration, such as the local name used in IKE negotiation, interval at which an IKE SA sends a heartbeat packet, timeout interval of heartbeat packets, and interval at which an IKE SA sends an NAT keepalive packet.

Example

Display the global IKE configuration.

```
<Huawei> display ike global config
IKE Global Config:
-------------------------------------------------------------
  IKE local-name                    : huawei
  IKE heartbeat-timer interval      : 30
  IKE heartbeat-timer timeout       : 100
  IKE nat-keepalive-timer interval : 52
  IKE sm-encryption-key-length      : disable
  IKE certificate-check             : disable
  IKEv2 prf aes-xcbc-128 compatible: enable
-------------------------------------------------------------
```

Table 12-17 Description of the **display ike global config** command output

Item	Description
IKE Global Config	Global configuration of IKE.
IKE local-name	Local name used in IKE negotiation. To set the local name used in IKE negotiation, run the **ike local-name** command. If **ike local-name** is not configured on the local end, the name specified by the **sysname** command is used for IKE negotiation.
IKE heartbeat-timer interval	Interval at which an IKE SA sends a heartbeat packet, in seconds. To set the interval at which an IKE SA sends a heartbeat packet, run the **ike heartbeat-timer interval** command.
IKE heartbeat-timer timeout	Timeout interval of heartbeat packets, in seconds. To set the timeout interval of heartbeat packets, run the **ike heartbeat-timer timeout** command.
IKE nat-keepalive-timer interval	Interval at which an IKE SA sends an NAT keepalive packet, in seconds. To set the interval at which an IKE SA sends an NAT keepalive packet, run the **ike nat-keepalive-timer interval** command.
IKE sm-encryption-key-length	Whether IKE negotiation packets carry the SM encryption key length when IKE uses a digital envelope for authentication. • enable • disable
IKE certificate-check	Whether validity verification on certificates of all IKE peers is enabled. • enable • disable To configure this function, run the **12.6.65 ike certificate-check disable** command.
IKEv2 prf aes-xcbc-128 compatible	Whether the IKEv2 PRF AES-XCBC-128 algorithm is a non-standard RFC algorithm: • enable • disable This function is configured using the **12.6.84 ikev2 prf aes-xcbc-128 compatible** command. **NOTE** V200R010C10 and later versions support this parameter.

12.6.18 display ike offline-info

Function

The **display ike offline-info** command displays information about deleted IPSec tunnels established through IKE negotiation.

Format

display ike offline-info [**peer** *remote-address*]

Parameters

Parameter	Description	Value
peer *remote-address*	Displays information about deleted IPSec tunnels with a specified remote IP address and established through IKE negotiation.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The command output contains the possible causes and time of the latest 200 IPSec tunnel deletions.

Example

Display information about deleted IPSec tunnels established through IKE negotiation.

```
<Huawei> display ike offline-info

  Current info Num :3
  Ike offline information:
-------------------------------------------------------------------------------
  peer              offline-reason       version     offline-time
-------------------------------------------------------------------------------------------------------
  10.10.10.10         dpd-timeout          v2          2015/08/01  16:05:55
  3.3.3.3             dpd-timeout          v2          2015/08/01  16:05:55
  10.2.2.2            hardware-timeout     v2          2015/08/01  15:05:55
-------------------------------------------------------------------------------------------------------
```

Table 12-18 Description of the **display ike offline-info** command output

Item	Description
Current info Num	Current number of information records.
peer	Peer IP address of a deleted IPSec tunnel.

Item	Description
offline-reason	Causes for deletion of IPSec tunnels established through IKE negotiation: ● dpd timeout: Dead peer detection (DPD) times out. ● peer request: The remote end has sent a message, asking the local end to tear down the tunnel. ● config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted. ● phase1 hard expiry: Hard lifetime expires in phase 1 (no new SA negotiation success message is received). ● phase2 hard expiry: Hard lifetime expires in phase 2. ● heartbeat timeout: heartbeat detection times out. ● modecfg address soft expiry: The IP address lease applied by the remote end from the server expires. ● re-auth timeout: An SA is deleted due to reauthentication timeout. ● aaa cut user: The AAA module disconnects users. ● peer address switch: An SA is deleted due to change of the peer address. ● hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. ● kick old sa with same flow: The old SA is deleted for the same incoming flow. ● spi conflict: An SPI conflict occurs. ● phase1 sa replace: The new IKE SA replaces the old IKE SA. ● phase2 sa replace: The new IPSec SA replaces the old IPsec SA. ● nhrp notify: NHRP notifies the device that the SA needs to be deleted. ● disconnect track nqa/bfd/vrrp: The IPSec tunnel is torn down based on the NQA test instance, NQA group, VRRP, BFD session, or BFD group status. ● receive invalid spi notify: The device receives an invalid SPI notification. ● dns resolution status change: DNS resolution status changes. ● ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPSec SA when deleting an IKEv1 SA.
version	IKE version.
offline-time	IPSec tunnel deletion time.

 Copyright © Huawei Technologies Co., Ltd.

12.6.19 display ike identity

Function

The **display ike identity** command displays information about an identity filter set.

Format

display ike identity [**name** *identity-name*]

Parameters

Parameter	Description	Value
name *identity-name*	Specifies the name of the identity filter set.	The value is an existing identity filter name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to display information about an identity filter set.

Example

Display information about all identity filter sets.

```
<Huawei> display ike identity

Number of identity: 2

IKE identity: identity1
 FQDN       : R1
 DN         : c=cn,st=jiangsu,l=nanjing,o=huawei,ou=vpn,cn=ipsec
 User-FQDN  : liming@huawei.com
 User-FQDN  : zhangsan@huawei.com
 IP address : 1.1.1.0 255.255.255.0
 IP address : 2.2.2.0 255.255.255.0
 IP address : 3.3.3.0 255.255.255.0

IKE identity: 1
 FQDN       : R2
 IP address : 4.1.1.0 255.255.255.0
 IP address : 4.1.2.0 255.255.255.0
```

Display information about the identity filter set named **identity1**.

```
<Huawei> display ike identity name identity1
```

 Copyright © Huawei Technologies Co., Ltd.

```
IKE identity: identity1
 FQDN       : R1
 DN         : c=cn,st=jiangsu,l=nanjing,o=huawei,ou=vpn,cn=ipsec
 User-FQDN  : liming@huawei.com
 User-FQDN  : zhangsan@huawei.com
 IP address : 1.1.1.0 255.255.255.0
 IP address : 2.2.2.0 255.255.255.0
 IP address : 3.3.3.0 255.255.255.0
 IP address : 6.6.6.0 255.255.255.0
```

Table 12-19 Description of the display ike identity command output

Item	Description
IKE identity	Name of the identity filter set. To set this parameter, run the **12.6.70 ike identity** command.
Name	Name of the allowed peer for IKE negotiation. To set this parameter, run the **12.6.62 fqdn** command.
DN	DN of the allowed peer. To set this parameter, run the **12.6.49 dn** command.
User-FQDN	User-FQDN of the allowed peer. To set this parameter, run the **12.6.182 user-fqdn** command.
IP address	IP address of the allowed peer. To set this parameter, run the **12.6.90 ip address** command.

Related Topics

12.6.70 ike identity

12.6.20 display ike peer (all views)

Function

The **display ike peer** command displays the IKE peer configuration.

Format

display ike peer [**brief** | **name** *peer-name*]

Parameters

Parameter	Description	Value
brief	Displays brief information about IKE peers.	-

Parameter	Description	Value
name *peer-name*	Displays detailed information about the IKE peer with a specified name.	The value must be an existing IKE peer name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ike peer** command output contains the following information:

- Name of the IKE peer
- Negotiation mode
- Authentication key
- IKE proposal
- Type of the local ID
- IP address of the IKE peer
- Name of the IKE peer
- Whether NAT traversal is enabled

Example

Display brief configuration of the IKE peer.

```
<Huawei> display ike peer brief
Current ike peer number: 3

-------------------------------------------------------------------------------
Peer name        Version  Exchange-mode   Proposal   Id-type   RemoteAddr
-------------------------------------------------------------------------------
1                v1v2     main            11         IP
peer1            v1v2     main            12         IP
huawei           v1v2     main            13         IP
```

Table 12-20 Description of the **display ike peer brief** command output

Item	Description
Current ike peer number	Current number of IKE peers that have been configured.
Peer name	Number of an IKE peer. To configure an IKE peer, run the **12.6.75 ike peer** command.

Item	Description
Version	IKE version of the IKE peer: ● v1: IKEv1 is enabled. ● v2: IKEv2 is enabled. ● v1v2: Both IKEv1 and IKEv2 are enabled. To configure an IKE version, run the **12.6.180 version** command.
Exchange-mode	IKEv1 negotiation mode: ● main ● aggressive ● -: not supported. The value is displayed when the IKE peer uses only IKEv2. To configure a negotiation mode, run the **exchange-mode** command.
Proposal	Name of the referenced IKE proposal. To configure an IKE proposal, run the **ike-proposal** command.
Id-type	Local ID type in IKE negotiation. To set the local ID type, run the **local-id-type** command.
RemoteAddr	IP address of the remote IKE peer. To configure an IP address of the remote IKE peer, run the **12.6.134 remote-address (IKE peer view)** command.

Display configuration of the IKE peer.

```
<Huawei> display ike peer

Number of IKE peers: 1
-----------------------------------------
  Peer name                          : 1
  IKE version                        : v1v2
  VPN instance                       : vpn1
  Remote IP                          : 1.1.1.1
  Remote IP                          : 2.2.2.2
  Authentic IP address               : -
  Proposal                           : 1
  Pre-shared-key                     : %^%#G7(t:%yFw/PVF>Jsva;"zx]oL!sw-8z\C;I}%%RY%^%#
  Local ID type                      : IP
  Local ID                           : -
  Remote ID type                     : any
  Remote ID                          : -
  certificate peer-name              : abc
  PKI realm                          : test
  Inband OCSP                        : Enable
  Inband CRL                         : Disable
  cert-request empty-payload         : Enable
```

```
  VPN instance bound to the SA          : vpna
  NAT-traversal                         : Enable
  Service-scheme name                   : a
  Re-authentication interval(s)         : 333
  IKE user-table                        : 1
  AAA authorization domain              : a
  DSCP                                  : -
  Lifetime-notification-message         : Enable
  DPD                                   : Enable
  DPD type                              : on-demand
  DPD retry-limit                       : 3
  DPD retransmit-interval(s)            : 30
  DPD idle-time(s)                      : 60
  DPD msg                               : seq-hash-notify
  RSA encryption-padding                : PKCS1
  RSA signature-padding                 : PKCS1
  ipsec sm4 version                     : standard
  Certificate-check                     : Disable
  Resource acl                          : -
  Local ID Certificate Preference       : Enable
  IKEv2 Local ID Reflect                : Enable
-----------------------------------------
```

Table 12-21 Description of the **display ike peer** command output

Item	Description
Number of IKE peers	Number of IKE peers that have been configured.
Peer name	Name of an IKE peer. To configure an IKE peer, run the **12.6.75 ike peer** command.
IKE version	IKE version of the IKE peer: ● v1: IKEv1 is enabled. ● v2: IKEv2 is enabled. ● v1v2: Both IKEv1 and IKEv2 are enabled. To configure an IKE version, run the **12.6.180 version** command.
VPN instance	VPN instance name. To configure a VPN instance name, run the **12.6.134 remote-address (IKE peer view)** command.
Remote IP	IP address of the remote IKE peer. To configure an IP address of the remote IKE peer, run the **12.6.134 remote-address (IKE peer view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentic IP address	IP address used for IKE negotiation authentication before NAT translation. To configure the IP address used for IKE negotiation authentication before NAT translation, run the **12.6.134 remote-address (IKE peer view)** command.
Proposal	Referenced IKE proposal. This parameter is available only when the IKE proposal has been configured using the **12.6.78 ike-proposal** command.
Pre-shared-key	Pre-shared key used for authentication. When an IKE proposal referenced by an IKE peer uses pre-shared key authentication, the pre-shared key is used for identity authentication. To configure a pre-shared key, run the **pre-shared-key** command.
Local ID type	Local ID type in IKE negotiation. To set the local ID type, run the **local-id-type** command.
Local ID	Local ID used in IKE negotiation. To set the local ID used in IKE negotiation, run the **ike local-name** or **12.6.118 local-id** command.
Remote ID type	Remote ID type in IKE negotiation. To set the remote ID type, run the **remote-id-type** command.
Remote ID	Remote ID used in IKE negotiation. To configure the remote ID used in IKE negotiation, run the **12.6.136 remote-id** command.
certificate peer-name	Peer name in the specified certificate.
PKI realm	PKI realm bound to the IKE peer. To bind a PKI realm to an IKE peer, run the **12.6.124 pki realm** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Inband OCSP	Whether IKEv2 is used to transmit Online Certificate Status Protocol (OCSP) requests and responses: ● Enable ● Disable To this function, run the **inband ocsp** command.
Inband CRL	Whether IKEv2 is used to transmit certificate revocation list (CRL) requests and responses: ● Enable ● Disable To this function, run the **inband crl** command.
cert-request empty-payload	Whether the certificate request payload is empty: ● Enable ● Disable To configure the device to send certificate requests with empty payload, run the **12.6.10 certificate-request empty-payload enable** command.
VPN instance bound to the SA	Name of the VPN instance bound to the IPSec tunnel. To bind a VPN instance to an IPSec tunnel, run the **12.6.155 sa binding vpn-instance** command.
NAT-traversal	Whether NAT traversal is enabled: ● Enable ● Disable To enable NAT traversal, run the **nat traversal** command.
Service-scheme name	AAA scheme referenced by an IKE peer. To configure an AAA scheme, run the **12.6.168 service-scheme** command.
Re-authentication interval(s)	IKEv2 re-authentication interval. To configure an IKEv2 re-authentication interval, run the **12.6.133 re-authentication interval** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IKE user-table	IKE user table referenced by an IKE peer. To configure an IKE user table, run the **12.6.179 user-table** command.
AAA authorization domain	AAA authorization domain referenced by an IKE peer. To configure an AAA authorization domain, run the **12.6.1 aaa authorization** command.
DSCP	DSCP value of IKE packets of an IKE peer. To configure a DSCP value, run the **12.6.53 dscp** command.
Lifetime-notification-message	Whether the device is enabled to send notification messages of the IKE SA lifetime: ● Enable ● Disable To enable this function, run the **12.6.115 lifetime-notification-message enable** command.
DPD	Whether the DPD function is enabled: ● Enable ● Disable
DPD type	DPD mode of an IKE peer. ● on-demand: DPD is performed on demand. ● periodic: DPD is performed periodically. To specify a DPD mode, run the **12.6.52 dpd type** command.
DPD retry-limit	Number of times that an IKE peer can retransmit DPD packets. To specify the number of retransmission times, run the **12.6.50 dpd** command.
DPD retransmit-interval(s)	Interval at which an IKE peer retransmits DPD packets. To configure the retransmission interval, run the **12.6.50 dpd** command.
DPD idle-time(s)	DPD idle time of an IKE peer. To configure a DPD idle time, run the **12.6.50 dpd** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DPD msg	Sequence of the payload in DPD packets. ● seq-hash-notify: indicates that in a DPD packet, the hash payload is before the notify payload. ● seq-notify-hash: indicates that in a DPD packet, the notify payload is before the hash payload. To configure the sequence of the payload, run the **12.6.51 dpd msg** command.
RSA encryption-padding	Padding mode of RSA encryption.
RSA signature-padding	Padding mode of an RSA signature. To specify the padding mode, run the **12.6.152 rsa signature-padding** command.
ipsec sm4 version	Version of the SM4 algorithm.
Certificate-check	Whether validity verification on certificates of an IKE peer is enabled: ● Enable ● Disable To disable validity verification on certificates of an IKE peer, run the **12.6.9 certificate-check disable** command.
Resource acl	ACL information to be pushed by the headquarters device to the branch. To configure ACL information, run the **12.6.148 resource acl** command.
Local ID Certificate Preference	Whether to enable the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation: ● Enable ● Disable To enable this function, run the **12.6.119 local-id-preference certificate enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IKEv2 Local ID Reflect	Whether the local ID of the responder is used as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation: ● Enable ● Disable To enable this function, run the **12.6.120 local-id-reflect enable** command.

12.6.21 display ike peer ctrl-plane

Function

The **display ike peer ctrl-plane** command displays the IKE peer configuration on control plane.

Format

display ike peer [**brief** | **name** *peer-name*] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about the IKE peer.	-
name *peer-name*	Specifies the name of IKE peer.	The value is an existing ike peer name.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

The output of the **display ike peer ctrl-plane** command is as follows:

- Name of the IKE peer
- Negotiation mode
- Authentication key

 Copyright © Huawei Technologies Co., Ltd.

- IKE proposal
- Type of the local ID
- IP address of the peer
- Name of the peer
- Whether NAT traversal is enabled

Example

Display configuration of the IKE peer.

```
<Huawei> display ike peer ctrl-plane
Number of IKE peers: 1
-----------------------------------------
  Peer name                          : 1
  IKE version                        : v1v2
  VPN instance                       : vpn1
  Remote IP                          : 1.1.1.1
  Remote IP                          : 2.2.2.2
  Authentic IP address               : -
  Proposal                           : 1
  Pre-shared-key                     : %^%#G7(t:%yFw/PVF>Jsva;"zx]oL!sw-8z\C;I}%%RY%^%#
  Local ID type                      : IP
  Local ID                           : -
  Remote ID type                     : any
  Remote ID                          : -
  certificate peer-name              : abc
  PKI realm                          : test
  Inband OCSP                        : Enable
  Inband CRL                         : Disable
  cert-request empty-payload         : Enable
  VPN instance bound to the SA       : vpna
  NAT-traversal                      : Enable
  Service-scheme name                : a
  Re-authentication interval(s)      : 333
  IKE user-table                     : 1
  AAA authorization domain           : a
  DSCP                               : -
  Lifetime-notification-message      : Enable
  DPD                                : Enable
  DPD type                           : on-demand
  DPD retry-limit                    : 3
  DPD retransmit-interval(s)         : 30
  DPD idle-time(s)                   : 60
  DPD msg                            : seq-hash-notify
  RSA encryption-padding             : PKCS1
  RSA signature-padding              : PKCS1
  ipsec sm4 version                  : standard
  Certificate-check                  : Disable
  Resource acl                       : -
  Local ID Certificate Preference    : Enable
  IKEv2 Local ID Reflect             : Enable
-----------------------------------------
```

Display brief configuration of the IKE peer.

```
<Huawei> display ike peer brief ctrl-plane
Current ike peer number: 3

-----------------------------------------------------------------------------
Peer name        Version  Exchange-mode   Proposal   Id-type   RemoteAddr
-----------------------------------------------------------------------------
1                v1v2     main            11         IP
peer1            v1v2     main            12         IP
huawei           v1v2     main            13         IP
```

Table 12-22 Description of the **display ike peer ctrl-plane** command output

Item	Description
Number of IKE peers	Number of IKE peers that have been configured.
Peer name	Name of the IKE peer.
IKE version/Version	IKE version of the IKE peer: ● v1: IKEv1 is enabled. ● v2: IKEv2 is enabled. ● v1v2: Both IKEv1 and IKEv2 are enabled.
VPN instance	VPN instance name.
Exchange-mode	IKEv1 negotiation mode: ● main ● aggressive ● -: not supported. The value is displayed when the IKE peer uses only IKEv2.
Remote IP/RemoteAddr	IP address of the remote IKE peer.
Authentic IP address	IP address used for IKE negotiation authentication before NAT translation.
Proposal	Name of the IKE proposal.
Pre-shared-key	Pre-shared key used in pre-shared key authentication.
Local ID type/Id-type	Local ID type in IKE negotiation.
Local ID	Local ID used in IKE negotiation.
Remote ID type	Remote ID type in IKE negotiation.
Remote ID	Remote ID used in IKE negotiation.
certificate peer-name	Peer name in the specified certificate.
PKI realm	PKI domain bound to the IKE peer.
Inband OCSP	Whether the IKEv2 for Online Certificate Status Protocol (OCSP) requests and responses is enabled for the IKE peer.
Inband CRL	Whether IKEv2 for certificate revocation list (CRL) requests and responses is enabled for an IKE peer.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
cert-request empty-payload	Whether the certificate request payload carries CA information.
VPN instance bound to the SA	Name of the VPN instance bound to the IPSec tunnel.
NAT-traversal	Whether NAT traversal is enabled.
Service-scheme name	AAA scheme referenced by an IKE peer.
Re-authentication interval(s)	IKEv2 re-authentication interval.
IKE user-table	IKE user table referenced by an IKE peer.
AAA authorization domain	AAA authorization domain referenced by an IKE peer.
DSCP	DSCP value of IKE packets of an IKE peer.
Lifetime-notification-message	Whether the device is enabled to send notification messages of the IKE SA lifetime.
DPD	Whether the DPD function is enabled.
DPD type	DPD mode of an IKE peer. ● on-demand: DPD is performed on demand. ● periodic: DPD is performed periodically.
DPD retry-limit	Number of times that an IKE peer can retransmit DPD packets.
DPD retransmit-interval(s)	Interval at which an IKE peer retransmits DPD packets.
DPD idle-time(s)	DPD idle time of an IKE peer.
DPD msg	Sequence of the payload in DPD packets. ● seq-hash-notify ● seq-notify-hash
RSA encryption-padding	Padding mode of RSA encryption.
RSA signature-padding	Padding mode of a RSA signature.
ipsec sm4 version	Version of the SM4 algorithm.
Certificate-check	Whether validity verification on certificates of an IKE peer is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Resource acl	ACL information to be pushed by the headquarters device to the branch.
Local ID Certificate Preference	Whether to enable the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation. ● Enable ● Disable To enable this function, run the **12.6.119 local-id-preference certificate enable** command.
IKEv2 Local ID Reflect	Whether the local ID of the responder is used as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation. ● Enable ● Disable To enable this function, run the **12.6.120 local-id-reflect enable** command.

12.6.22 display ike proposal (All views)

Function

The **display ike proposal** command displays the IKE proposal configuration.

Format

display ike proposal [**number** *proposal-number*]

display ike proposal default

Parameters

Parameter	Description	Value
number *proposal-number*	Specifies the number of an IKE proposal. A smaller IKE proposal number indicates a higher priority.	The value is an integer that ranges from 1 to 99.
default	Displays a default IKE proposal information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

IKE proposals are displayed in ascending order of IKE proposal number.

Example

Display the configuration of all IKE proposals.

```
<Huawei> display ike proposal

Number of IKE Proposals: 2

-------------------------------------------
 IKE Proposal: 1
   Authentication Method      : PRE_SHARED
   Authentication Algorithm   : SHA2-256
   Encryption Algorithm       : AES-256
   Diffie-Hellman Group       : MODP-2048
   SA Duration(Seconds)       : 86400
   Integrity Algorithm        : HMAC-SHA2-256
   Prf Algorithm              : HMAC-SHA2-256
-------------------------------------------
```

```
-----------------------------------------
IKE Proposal: Default
  Authentication Method      : PRE_SHARED
  Authentication Algorithm   : SHA2-256
  Encryption Algorithm       : AES-256
  Diffie-Hellman Group       : MODP-1024
  SA Duration(Seconds)       : 86400
  Integrity Algorithm        : HMAC-SHA2-256
  Prf Algorithm              : HMAC-SHA2-256
-----------------------------------------
```

Table 12-23 Description of the **display ike proposal** command output

Item	Description
Number of IKE Proposals	Number of the IKE proposal.
IKE Proposal	IKE proposal number. To configure an IKE proposal, run the **ike proposal** command.
Authentication Method	Authentication method used in the IKE proposal: ● PRE_SHARED: pre-shared key authentication ● RSA-SIGNATURE: RSA signature authentication To configure an authentication method, run the **authentication-method** command.
Authentication Algorithm	Authentication algorithm used in the IKE proposal: ● MD5: uses a 128-bit key. ● SHA1: uses a 160-bit key. ● SHA2-256: uses a 256-bit key. ● SHA2-384: uses a 384-bit key. ● SHA2-512: uses a 512-bit key. To configure an authentication algorithm, run the **authentication-algorithm** command. **NOTE** The MD5 and SHA-1 algorithms have potential security risks. The SHA2 algorithm is recommended.
Encryption Algorithm	Encryption algorithm used in the IKE proposal: ● 3DES: 168-bit 3DES-CBC encryption algorithm ● AES-128: 128-bit AES encryption algorithm ● AES-192: 192-bit AES encryption algorithm ● AES-256: 256-bit AES encryption algorithm ● DES: DES-CBC encryption algorithm To configure an encryption algorithm, run the **encryption-algorithm** command. **NOTICE** The DES and 3DES algorithms have potential security risks. The AES algorithm is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Diffie-Hellman Group	DH group in the IKE proposal: • MODP-768: 768-bit Diffie-Hellman group • MODP-1024: 1024-bit Diffie-Hellman group • MODP-1536: 1536-bit Diffie-Hellman group • MODP-2048: 2048-bit Diffie-Hellman group • ECP-256: 256-bit ECP Diffie-Hellman group • ECP-384: 384-bit ECP Diffie-Hellman group • ECP-521: 521-bit ECP Diffie-Hellman group To configure a DH group, run the **dh** command.
SA Duration(Seconds)	IKE SA lifetime. To set the IKE SA lifetime, run the **sa duration** command.
Integrity Algorithm	Integrity algorithm in the IKE proposal: • AES-XCBC-96: AES-XCBC-96 algorithm • HMAC-MD5-96: HMAC-MD5-96 algorithm • HMAC-SHA1-96: HMAC-SHA1-96 algorithm • HMAC-SHA2-256: HMAC-SHA2-256 algorithm • HMAC-SHA2-384: HMAC-SHA2-384 algorithm • HMAC-SHA2-512: HMAC-SHA2-512 algorithm Only IKEv2 negotiation requires the integrity algorithm. To configure an integrity algorithm, run the **integrity-algorithm** command. **NOTE** The HMAC-MD5-96 and HMAC-SHA1-96 algorithms have potential security risks. The HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512 algorithm is recommended.
Prf Algorithm	Algorithm used to generate a pseudo random number in the IKE proposal: • AES-XCBC-128: AES-XCBC-128 algorithm • HMAC-MD5: HMAC-MD5 algorithm • HMAC-SHA1: HMAC-SHA1 algorithm • HMAC-SHA2-256: HMAC-SHA2-256 algorithm • HMAC-SHA2-384: HMAC-SHA2-384 algorithm • HMAC-SHA2-512: HMAC-SHA2-512 algorithm Only IKEv2 requires the PRF algorithm. To specify an algorithm used to generate a pseudo random number, run the **prf** command. **NOTE** The HMAC-MD5 and HMAC-SHA1 algorithms have potential security risks. The AES-XCBC-128, HMAC-SHA2-256, HMAC-SHA2-384, or HMAC-SHA2-512 algorithm is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.6.76 ike proposal
12.6.78 ike-proposal

12.6.23 display ike proposal ctrl-plane

Function

The **display ike proposal ctrl-plane** command displays the IKE proposal configuration on control plane.

Format

display ike proposal [**number** *proposal-number*] **ctrl-plane**

Parameters

Parameter	Description	Value
number *proposal-number*	Specifies the number of an IKE proposal. A smaller IKE proposal number indicates a higher priority.	The value is an integer that ranges from 1 to 99.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the configuration of all IKE proposals.

```
<Huawei> display ike proposal number 10 ctrl-plane
-------------------------------------------
 IKE Proposal: 10
   Authentication Method      : PRE_SHARED
   Authentication Algorithm   : SHA2-256
   Encryption Algorithm       : AES-256
   Diffie-Hellman Group       : MODP-1024
   SA Duration(Seconds)       : 86400
   Integrity Algorithm        : HMAC-SHA2-256
   Prf Algorithm              : HMAC-SHA2-256
-------------------------------------------
```

Table 12-24 Description of the **display ike proposal ctrl-plane** command output

Item	Description
IKE Proposal	IKE proposal number.
Authentication Method	Authentication mode in the IKE proposal: ● PRE_SHARED: pre-shared key authentication. ● RSA-SIGNATURE: RSA signature authentication. ● DIGITAL-ENVELOPE: digital envelope authentication.
Authentication Algorithm	Authentication algorithm in the IKE proposal: ● MD5: uses a 128-bit key. ● SHA1: uses a 160-bit key. ● SHA2-256: uses a 256-bit key. ● SHA2-384: uses a 384-bit key. ● SHA2-512: uses a 512-bit key.
Encryption Algorithm	Encryption algorithm in the IKE proposal: ● 3DES: 168-bit 3DES-CBC encryption algorithm. ● AES-128: 128-bit AES encryption algorithm. ● AES-192: 192-bit AES encryption algorithm. ● AES-256: 256-bit AES encryption algorithm. ● DES: DES-CBC encryption algorithm.
Diffie-Hellman Group	DH group in the IKE proposal: ● MODP-768: 768-bit Diffie-Hellman group. ● MODP-1024: 1024-bit Diffie-Hellman group. ● MODP-1536: 1536-bit Diffie-Hellman group. ● MODP-2048: 2048-bit Diffie-Hellman group. ● MODP-3072: 3072-bit Diffie-Hellman group. ● MODP-4096: 4096-bit Diffie-Hellman group.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA Duration(Seconds)	ISAKMP SA Duration used in the IKE proposal.
Integrity Algorithm	Integrity algorithm in the IKE proposal: ● AES-XCBC-96: AES-XCBC-96 algorithm. ● HMAC-MD5-96: HMAC-MD5-96 algorithm. ● HMAC-SHA1-96: HMAC-SHA1-96 algorithm. ● HMAC-SHA2-256: HMAC-SHA2-256 algorithm. ● HMAC-SHA2-384: HMAC-SHA2-384 algorithm. ● HMAC-SHA2-512: HMAC-SHA2-512 algorithm.
Prf Algorithm	Algorithm used to generate a pseudo random number in the IKE proposal: ● AES-XCBC-128: AES-XCBC-128 algorithm. ● HMAC-MD5: HMAC-MD5 algorithm. ● HMAC-SHA1: HMAC-SHA1 algorithm. ● HMAC-SHA2-256: HMAC-SHA2-256 algorithm. ● HMAC-SHA2-384: HMAC-SHA2-384 algorithm. ● HMAC-SHA2-512: HMAC-SHA2-512 algorithm.

12.6.24 display ike sa

Function

The **display ike sa** command displays information about SAs established through IKE negotiation.

Format

display ike sa [**remote** *ipv4-address*]

display ike sa [**remote-id-type** *remote-id-type*] **remote-id** *remote-id*

display ike sa verbose { **remote** *ipv4-address* | **connection-id** *connection-id* | [**remote-id-type** *remote-id-type*] **remote-id** *remote-id* }

Parameters

Parameter	Description	Value
remote *ipv4-address*	Specifies the IPv4 address of the remote peer.	The value is in dotted decimal notation.
remote-id-type *remote-id-type*	Specifies a remote ID type.	The remote ID type can be ip, dn, key-id, fqdn, or user-fqdn.
remote-id *remote-id*	Specifies the remote ID.	The remote ID must be an existing one.
verbose	Displays detailed information about SAs.	-
connection-id *connection-id*	Specifies the connection ID of an SA.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ike sa** command to check the following SA information: connection ID, peer IP address, VPN instance name, SA phase, remote ID type, remote ID, and SA status.

NOTE

After an IPSec tunnel is established successfully, the **display ike sa** command does not display the latest local ID or remote ID until the IPSec tunnel is re-negotiated if the local ID or remote ID is modified.

Example

Display IKE SAs and IPSec SAs.

```
<Huawei> display ike sa
IKE SA information :
  Conn-ID      Peer            VPN   Flag(s)   Phase   RemoteType  RemoteID
 -------------------------------------------------------------------------------
  117477244    10.100.1.1:4500 vrf1  RD|M      v2:2    IP          10.100.1.1
  117477243    10.100.1.1:4500 vrf1  RD|M      v2:2    IP          10.100.1.1
  117477242    10.100.1.1:4500 vrf1  RD|M      v2:1    IP          10.100.1.1

  Number of IKE SA : 3
```

```
-------------------------------------------------------------------------------

Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Table 12-25 Description of the **display ike sa** command output

Item	Description
IKE SA information	Configuration of SAs.
Conn-ID	Connection ID of an SA.
Peer	IP address and UDP port number of the peer.
VPN	VPN instance bound to the interface where the IPSec policy was applied to.
Flag(s)	SA status: ● RD--READY: The SA has been established successfully. ● ST--STAYALIVE: This end is the initiator of tunnel negotiation. ● RL--REPLACED: This SA has been replaced by a new one and will be deleted after a period of time. ● FD--FADING: A soft timeout has occurred, but the SA is still in use. The SA will be deleted when the hard lifetime expires. ● TO--TIMEOUT: This SA has not received any heartbeat packet after the last heartbeat timeout. The SA will be deleted if it still does not receive any heartbeat packet till the next heartbeat timeout. ● HRT--HEARTBEAT: The local IKE SA sends heartbeat packets. ● LKG--LAST KNOWN GOOD SEQ NO: It is the last known sequence number. ● BCK--BACKED UP: The SA is backed up. ● M--ACTIVE: The IPSec policy group is in active state. ● S--STANDBY: The IPSec policy group is in standby state. ● A--ALONE: The IPSec policy group is not backed up. ● NEG--NEGOTIATING: The devices are negotiating an SA. ● Empty: IKE SA negotiation is being performed because the settings at the two ends of the tunnel are inconsistent.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Phase	Phases of the SA: ● v1:1 or v2:1: v1 and v2 are IKE versions. The digit 1 indicates the phase during which a security channel, that is IKE SA, is established. ● v1:2 or v2:2: v1 and v2 are IKE versions. The digit 2 indicates the phase during which a security service, that is IPSec SA, is negotiated.
RemoteType	Remote ID type.
RemoteID	Remote ID.

Display detailed information about established IKE SAs and IPSec SAs when the peers use IKEv1 to negotiate IPSec SAs.

```
<Huawei> display ike sa verbose remote 10.100.1.1

IKE SA information :
-----------------------------------------------
Ike Sa phase   : 2
Establish Time : 2015-09-18 18:58:24
PortCfg Index  : 0xe
IKE Peer Name  : zhe
Connection Id  : 67126707
Version        : v1
Flow VPN       :
Peer VPN       :
-----------------------------------------------
Intiator Cookie         : 0x a7b1c107a7a67b1
Responder Cookie        : 0xf70b111e391f79a9
Local Address           : 10.2.1.1
Remote Address          : 10.1.1.1:4500
PFS                     : dh-group14
Flags                   : RD|ST|S
-----------------------------------------------

-----------------------------------------------
Ike Sa phase   : 1
Establish Time :
PortCfg Index  : 0xe
IKE Peer Name  : zhe
Connection Id  : 67125326
Version        : v1
Exchange Mode  : Main
Flow VPN       :
Peer VPN       :
-----------------------------------------------
Intiator Cookie                : 0x a7b1c107a7a67b1
Responder Cookie               : 0xf70b111e391f79a9
Local Address                  : 10.2.1.1
Remote Address                 : 10.1.1.1:4500
Encryption Algorithm           : AES-256
Authentication Algorithm       : SHA2-256
Authentication Method          : Pre-Shared key
DPD Capability                 : Yes
DPD Enable                     : Yes
Remaining Duration             : 11168
Reference Counter              : 60
Flags                          : RD|ST|S
Remote Id Type                 : IP
```

```
Remote Id                    : 10.136.24.108
DH Group                     : group14
NAT Traversal Version        : RFC3947
ModeCfg IP                   : 10.10.1.36
-------------------------------------------------

  Number of IKE SA : 2
-------------------------------------------------

 Flag Description:
 RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
 HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
 M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Display detailed information about established IKE SAs and IPSec SAs when the peers use IKEv2 to negotiate IPSec SAs.

```
<Huawei> display ike sa verbose remote 10.100.1.1

Ike sa verbose information :
-------------------------------------------------
Ike Sa phase   : 2
Establish Time : 2015-09-18 18:58:24
PortCfg Index  : 0x4
IKE Peer Name  : ptest
Connection Id  : 117440514
Version        : v2
Flow VPN       :
Peer VPN       :
-------------------------------------------------
Intiator Cookie         : 0x10dbb95cdb031726
Responder Cookie        : 0x4ba2840bddcf74fd
Local Address           : 10.2.1.1
Remote Address          : 10.1.1.1:4500
PFS                     : dh-group14
Flags                   : RD|ST|A
-------------------------------------------------

-------------------------------------------------
Ike Sa phase   : 1
Establish Time : 2015-09-18 18:58:24
PortCfg Index  : 0x4
IKE Peer Name  : ptest
Connection Id  : 117440513
Version        : v2
Flow VPN       :
Peer VPN       :
-------------------------------------------------
Intiator Cookie                     : 0x10dbb95cdb031726
Responder Cookie                    : 0x4ba2840bddcf74fd
Local Address                       : 10.2.1.1
Remote Address                      : 10.1.1.1:4500
Encryption Algorithm                : AES-256
Authentication Method               : Pre-Shared key
Integrity Algorithm                 : hmac-sha2-256
Prf Algorithm                       : hmac-sha2-256
DPD Capability                      : Yes
DPD Enable                          : Yes
Remaining Duration                  : 11168
Reference Counter                   : 1
Flags                               : RD|ST|A
Remote Id Type                      : IP
Remote Id                           : 10.136.24.108
DH Group                            : group2
Re-authentication remaining time (sec) : -
ModeCfg IP                          : 10.10.1.36
-------------------------------------------------

  Number of IKE SA : 2
-------------------------------------------------
```

```
Flag Description:
RD--READY   ST--STAYALIVE   RL--REPLACED   FD--FADING   TO--TIMEOUT
HRT--HEARTBEAT   LKG--LAST KNOWN GOOD SEQ NO.   BCK--BACKED UP
M--ACTIVE   S--STANDBY   A--ALONE  NEG--NEGOTIATING
```

Table 12-26 Description of the **display ike sa verbose** command output

Item	Description
Ike Sa phase	Phases of the SA: ● 1: IKE peers establish an IPSec tunnel. An IKE SA is established in this phase. ● 2: IKE peers negotiate security services. An IPSec SA is established in this phase.
Establish Time	Time when the SA was created.
PortCfg Index	Index of the interface where the IPSec policy was applied to.
IKE Peer Name	IKE peer name. To configure an IKE peer, run the **12.6.75 ike peer** command.
Connection Id	Connection ID of an SA.
Version	IKE version of the IKE peer: ● v1: IKEv1 is enabled. ● v2: IKEv2 is enabled. ● v1v2: Both IKEv1 and IKEv2 are enabled. To configure an IKE version, run the **12.6.180 version** command.
Exchange Mode	Negotiation mode of the IKEv1 phase 1. ● Main: main mode. ● Aggressive: aggressive mode. To configure the negotiation mode, run the **12.6.61 exchange-mode** command.
Flow VPN	VPN to which the data flow belongs, run the **12.6.155 sa binding vpn-instance** command.
Peer VPN	VPN to which the peer belongs, run the **12.6.155 sa binding vpn-instance** command.
Intiator Cookie	Cookie of the initiator.
Responder Cookie	Cookie of the responder.
Local Address	Local IP address of an IPSec tunnel. To configure the local IP address of an IPSec tunnel, run the **12.6.174 tunnel local** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote Address	Remote IP address and UDP port number of an IPSec tunnel. To configure the remote IP address of an IPSec tunnel, run the **12.6.175 tunnel remote** command.
Encryption Algorithm	Encryption algorithm in the IKE proposal. To configure an encryption algorithm, run the **12.6.56 encryption-algorithm** command.
Authentication Algorithm	Authentication algorithm in the IKE proposal. To configure an authentication algorithm, run the **12.6.6 authentication-algorithm** command.
Authentication Method	Authentication method in the IKE proposal. To configure an authentication method, run the **12.6.7 authentication-method** command.
Integrity Algorithm	Integrity algorithm used in an IKEv2 proposal. To configure an integrity algorithm, run the **12.6.87 integrity-algorithm** command.
Prf Algorithm	Pseudo-random function (PRF) used in an IKEv2 proposal. To configure a PRF algorithm, run the **12.6.128 prf** command.
DPD Capability	Whether DPD capability is successfully negotiated. ● Yes ● No
DPD Enable	Whether the DPD function is enabled. ● Yes ● No To enable this function, run the **12.6.52 dpd type** command.
Remaining Duration	Remaining lifetime of an SA.
Reference Counter	Number of IPSec SAs negotiated by the IKE SA.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Flags	SA status: • RD--READY: The SA has been established successfully. • ST--STAYALIVE: This end is the initiator of tunnel negotiation. • RL--REPLACED: This SA has been replaced by a new one and will be deleted after a period of time. • FD--FADING: A soft timeout has occurred, but the SA is still in use. The SA will be deleted when the hard lifetime expires. • TO--TIMEOUT: This SA has not received any heartbeat packet after the last heartbeat timeout. The SA will be deleted if it still does not receive any heartbeat packet till the next heartbeat timeout. • HRT--HEARTBEAT: The local IKE SA sends heartbeat packets. • LKG--LAST KNOWN GOOD SEQ NO.: It is the last known sequence number. • BCK--BACKED UP: The SA is backed up. • M--ACTIVE: The IPSec policy group is in active state. • S--STANDBY: The IPSec policy group is in standby state. • A--ALONE: The IPSec policy group is not backed up. • NEG--NEGOTIATING: The devices are negotiating an SA. • Empty: IKE SA negotiation is being performed because the settings at the two ends of the tunnel are inconsistent.
PFS	Perfect Forward Secrecy (PFS) when the local end initiates negotiation. To enable this function, run the **12.6.123 pfs** command.
Remote Id Type	Remote ID type. To configure the remote ID type, run the **12.6.137 remote-id-type** command.
Remote Id	Remote ID for IKE negotiation. To configure the remote ID, run the **12.6.136 remote-id** command.
DH Group	DH group in the IKE proposal. To configure a DH group, run the **dh** command.
NAT Traversal Version	Version of NAT traversal. • draft-ietf-ipsec-nat-t-ike-00 • draft-ietf-ipsec-nat-t-ike-02 • RFC3947

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Re-authentication remaining time (sec)	Remaining time for IKEv2 to initiate re-authentication, in seconds. When the IKEv2 re-authentication interval is set on the device and the device functions as the responder, it does not initiate IKEv2 re-authentication. Therefore, the remaining time for IKEv2 to initiate re-authentication displays - in the command output. You can view the remaining time on the initiator.
ModeCfg IP	IP address allocated through mode configuration.
Number of IKE SA	Total number of IKE SAs and IPSec SAs.

12.6.25 display ike statistics

Function

The **display ike statistics** command displays IKE statistics.

Format

display ike statistics { **v1** | **v2** }

Parameters

Parameter	Description	Value
v1	Displays IKEv1 statistics.	-
v2	Displays IKEv2 statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs on the IPSec tunnel that is established through IKE negotiation, you can check statistics about IKE peers, IKE SAs, and DPD packets to diagnose and locate the fault.

Example

Display IKEv1 statistics.

```
<Huawei> display ike statistics v1
-------------------------------------------------------------------------------
 IKE V1 statistics information

 Number of total peers                      : 7
 Maximum of total peers in history          : 0
 Begin time of total peers                  : 2015-04-08 21:23:10
 Maximum time of total peers                : 2015-04-08 21:23:10
 Number of proposals                        : 4
 Number of established V1 phase 1 SAs       : 0
 Number of established V1 phase 2 SAs       : 0
 Number of total V1 phase 1 SAs             : 0
 Number of total V1 phase 2 SAs             : 0
 Number of total SAs                        : 0
 Maximum of V1 phase 1 SAs in history       : 0
 Begin time of V1 phase 1 SAs               : 2015-04-08 21:23:10
 Maximum time of V1 phase 1 SAs             : 2015-04-08 21:23:10
 Maximum of V1 phase 2 SAs in history       : 0
 Begin time of V1 phase 2 SAs               : 2015-04-08 21:23:10
 Maximum time of V1 phase 2 SAs             : 2015-04-08 21:23:10
 Maximum of total SAs in history            : 0
 Begin time of total SAs                    : 2015-04-08 21:23:10
 Maximum time of total SAs                  : 2015-04-08 21:23:10
 Number of messages in V1 fast queue        : 0
 Number of messages in V1 slow queue        : 0
 Number of DPD request sent                 : 0
 Number of DPD ack received                 : 0
 Number of DPD request received             : 0
 Number of DPD ack sent                     : 0
-------------------------------------------------------------------------------
```

Display IKEv2 statistics.

```
<Huawei> display ike statistics v2
-------------------------------------------------------------------------------
 IKE V2 statistics information

 Number of total peers                      : 0
 Maximum of total peers in history          : 0
 Begin time of total peers                  : 2015-04-08 21:23:10
 Maximum time of total peers                : 2015-04-08 21:23:10
 Number of proposals                        : 4
 Number of established V2 phase 1 SAs       : 0
 Number of established V2 phase 2 SAs       : 0
 Number of total V2 phase 1 SAs             : 0
 Number of total V2 phase 2 SAs             : 0
 Number of total SAs                        : 0
 Maximum of V2 phase 1 SAs in history       : 0
 Begin time of V2 phase 1 SAs               : 2015-04-08 21:23:10
 Maximum time of V2 phase 1 SAs             : 2015-04-08 21:23:10
 Maximum of V2 phase 2 SAs in history       : 0
 Begin time of V2 phase 2 SAs               : 2015-04-08 21:23:10
 Maximum time of V2 phase 2 SAs             : 2015-04-08 21:23:10
 Maximum of total SAs in history            : 0
 Begin time of total SAs                    : 2015-04-08 21:23:10
 Maximum time of total SAs                  : 2015-04-08 21:23:10
 Number of messages in V2 fast queue        : 0
 Number of messages in V2 slow queue        : 0
 Number of DPD request sent                 : 0
 Number of DPD ack received                 : 0
 Number of DPD request received             : 0
 Number of DPD ack sent                     : 0
-------------------------------------------------------------------------------
```

Table 12-27 Description of the **display ike statistics** command output

Item	Description
IKE V1 statistics information	IKEv1 statistics.
IKE V2 statistics information	IKEv2 statistics.
Number of total peers	Total number of peers.
Maximum of total peers in history	Historical maximum number of IKE peers.
Begin time of total peers	Time when the system started to count the number of IKE peers.
Maximum time of total peers	Time when the total number of IKE peers reached the maximum value.
Number of proposals	Number of IKE proposals.
Number of established V1/V2 phase 1 SAs	Total number of IKE SAs that have been established successfully.
Number of established V1/V2 phase 2 SAs	Total number of IPSec SAs that have been established successfully.
Number of total V1/V2 phase 1 SAs	Total number of IKE SAs.
Number of total V1/V2 phase 2 SAs	Total number of IPSec SAs.
Number of total SAs	Total number of SAs.
Maximum of V1/V2 phase 1 SAs in history	Maximum number of IKE SAs in the history.
Begin time of V1/V2 phase 1 SAs	Time when the system started to count the number of IKE SAs.
Maximum time of V1/V2 phase 1 SAs	Time when the total number of IKE SAs reaches the maximum value.
Maximum of V1/V2 phase 2 SAs in history	Maximum number of IPSec SAs in the history.
Begin time of V1/V2 phase 2 SAs	Time when the system started to count the number of IPSec SAs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximum time of V1/V2 phase 2 SAs	Time when the total number of IPSec SAs reached the maximum value.
Maximum of total SAs in history	Maximum number of total SAs in the history.
Begin time of total SAs	Time when the system started to count the total number of SAs.
Maximum time of total SAs	Time when the total number of SAs reached the maximum value.
Number of messages in V1/V2 fast queue	Number of IKE messages in high-priority queues.
Number of messages in V1/V2 slow queue	Number of IKE messages in low-priority queues.
Number of DPD request sent	Number of DPD request packets sent from the local end.
Number of DPD ack received	Number of DPD ack packets received by the local end.
Number of DPD request received	Number of DPD request packets received by the local end.
Number of DPD ack sent	Number of DPD ack packets sent from the local end.

12.6.26 display ikev2 statistics

Function

The **display ikev2 statistics** command displays statistics on IPSec tunnels negotiated using IKEv2.

Format

display ikev2 statistics { **eap** | **error** | **notify-info** | **packet** | **sa** }

Parameters

Parameter	Description	Value
eap	Displays EAP statistics on IPSec tunnels negotiated using IKEv2.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
error	Displays error statistics on IPSec tunnels negotiated using IKEv2.	-
notify-info	Displays notification message statistics on IPSec tunnels negotiated using IKEv2.	-
packet	Displays packet statistics on IPSec tunnels negotiated using IKEv2.	-
sa	Displays SA statistics on IPSec tunnels negotiated using IKEv2.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view error, packet, SA, EAP, and notification message statistics on IPSec tunnels negotiated using IKEv2.

Example

Display EAP statistics on IPSec tunnels negotiated using IKEv2.

```
<Huawei> display ikev2 statistics eap

Ikev2 eap and modecfg statistics:
-------------------------------------------------------------------------------
Eap user auth success                                   :0
Eap auth timeout                                        :0
Eap auth fail                                           :0
Eap user get authorized IP address                      :0
Eap user go online number                               :0
Eap user go offline number                              :0
Eap user cut message                                    :0
Send ip address allocation request                      :0
Send ip address allocation request timeout              :0
Receive ip address allocation request ack               :0
Receive ip address allocation request nack              :0
Send ip address release request                         :0
Receive ip address release request nack                 :0
Fail to process the ip address allocation               :0
Ip address allocated fail to save                       :0
Ip address allocated exist but receive duplicate ip request :0
-------------------------------------------------------------------------------
```

Table 12-28 Description of the **display ikev2 statistics eap** command output

Item	Description
Ikev2 eap and modecfg statistics	IKEv2 EAP and mode configuration statistics.
Eap user auth success	EAP users pass the authentication successfully.
Eap auth timeout	EAP authentication timed out.
Eap auth fail	EAP authentication failed.
Eap user get authorized IP address	EAP users obtained authorized IP addresses.
Eap user go online number	Number of times EAP users go online.
Eap user go offline number	Number of times EAP users go offline.
Eap user cut message	Number of times EAP users are forced offline.
Send ip address allocation request	The device sends an IP address allocation request message.
Send ip address allocation request timeout	The IP address request message times out.
Receive ip address allocation request ack	The device receives an ACK message for the IP address allocation request.
Receive ip address allocation request nack	The device receives an NACK message for the IP address allocation request.
Send ip address release request	The device sends an IP address release request message.
Receive ip address release request nack	The device receives an NACK message for the IP address release request.
Fail to process the ip address allocation	The device fails to process the reply message for the IP address allocation request.
Ip address allocated fail to save	The allocated IP address is not saved in the SA.
Ip address allocated exist but receive duplicate ip request	The device receives a duplicate IP address request message.

 Copyright © Huawei Technologies Co., Ltd.

Display error statistics on IPSec tunnels negotiated using IKEv2.

```
<Huawei> display ikev2 statistics error

Error statistics:
-------------------------------------------------------------------------------
Config error:
Version error            :0
Peer address can not match with any ike peer config                  :0
Phase1 proposal mismatch :0           Phase2 proposal or pfs mismatch:0
Responder dh mismatch    :0           Initiator dh mismatch          :0
Flow mismatch            :1
ID can not match with any ike peer config                            :0
Construct local id fail                                        :0
Authentication fail (may be pre-shared-key error)                    :0
Peer's flow netmask range is too wide                                :0
-------------------------------------------------------------------------------
Packet or payload error:
Invalid length           :0
Message-id unordered     :0
Unknown exchange type    :0
Invalid cookie           :6
Shortpacket              :0
Malformed message        :4
Malformed payload        :0
Rekey, not find old child:0           Rekey, old child close         :14
Exchange-type or role(initiator or responder) mismatch               :0
Unexpected critical payload, drop                                    :0
Unexpected uncritical payload, ignore                                :0
-------------------------------------------------------------------------------
Maybe ddos attack:
Responder request IKEV2_COOKIE                                       :0
Responder receive invalid cookie for IKEV2_COOKIE request            :0
Responder receive no cookie for IKEV2_COOKIE request                 :0
-------------------------------------------------------------------------------
System abnormal:
Fail decrypt             :0           Fail encrypt                   :0
Fail integrity check     :0
No memory, fail send packet                                          :0
No memory, fail process packet                                       :0
-------------------------------------------------------------------------------
System limited:
First packet speed limited :0                License limited         :0
-------------------------------------------------------------------------------
```

Table 12-29 Description of the **display ikev2 statistics error** command output

Item	Description
Error statistics	Error statistics.
Config error	Configurations are incorrect.
Version error	The IKE version does not match.
Peer address can not match with any ike peer config	The corresponding IKE peer is not found based on the peer address.
Phase1 proposal mismatch	The phase 1 IPSec proposal does not match.
Phase2 proposal or pfs mismatch	The phase 2 IPSec proposal or PFS does not match.

Item	Description
Responder dh mismatch	DH group match on the responder failed. (If a matching DH group is available in the algorithm list of the initiator, the responder will send an information message to the initiator to instruct the initiator to start negotiation using the matching DH group. If the initiator accepts the information message, the negotiation succeeds.)
Initiator dh mismatch	DH group match on the initiator failed. (The initiator failed to process the message requesting a matching DH group.)
Flow mismatch	The data flow does not match.
ID can not match with any ike peer config	The peer ID does not match that configured in the IKE peer.
Construct local id fail	Local ID construction failed.
Authentication fail (may be pre-shared-key error)	Authentication failed. The possible cause is that the pre-shared key does not match.
Peer's flow netmask range is too wide	The mask length of the peer flow is too large.
Packet or payload error	Incorrect packet or payload.
Invalid length	Invalid length.
Message-id unordered	Message ID out of order.
Unknown exchange type	Unknown exchange type.
Invalid cookie	Invalid cookie: ● The corresponding SA does not exist in the received IKEv2 message that does not trigger negotiation. ● The cookie in the IKEv2 message that triggers negotiation is 0.
Shortpacket	The packet is too short.
Malformed message	Invalid message.
Malformed payload	Invalid payload.
Rekey, not find old child	The old IPSec SA is not found for re-negotiation.
Rekey, old child close	The old IPSec SA is offline for re-negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Exchange-type or role(initiator or responder) mismatch	The exchange type or role (initiator or responder) does not match.
Unexpected critical payload, drop	The unidentified key payload is dropped.
Unexpected uncritical payload, ignore	The unidentified key payload is ignored.
Maybe ddos attack	Maybe DDoS attacks occur.
Responder request IKEV2_COOKIE	The device requests a cookie when the SA in negotiation status exceeds the threshold.
Responder receive invalid cookie for IKEV2_COOKIE request	The received cookie is invalid.
Responder receive no cookie for IKEV2_COOKIE request	No cookie is received.
System abnormal	The system is abnormal.
Fail decrypt	Decryption failed.
Fail encrypt	Encryption failed.
Fail integrity check	Integrity check failed.
No memory, fail send packet	Packet sending failed due to insufficient memory.
No memory, fail process packet	Packet parsing failed due to insufficient memory.
System limited	System restriction.
First packet speed limited	The rate of the first packet is limited.
License limited	License restriction.

Display notification message statistics on IPSec tunnels negotiated using IKEv2.

```
<Huawei> display ikev2 statistics notify-info

Ikev2 notification statistics:
-------------------------------------------------------------------------------
Notification:
INVALID_IKE_SPI notification              send:0          receive:0
```

```
INVALID_MAJOR_VERSION notification          send:0          receive:0
INVALID_SYNTAX notification                 send:0          receive:0
INVALID_IPSEC_SPI notification              send:0          receive:0
INVALID_KE_PAYLOAD notification             send:0          receive:0
SINGLE_PAIR_REQUIRED notification           send:0          receive:0
NO_ADDITIONAL_SA notification               send:0          receive:0
TS_UNACCEPTABLE notification                send:0          receive:0
INVALID_IPSEC_SELECTORS notification        send:0          receive:0
INITIAL_CONTACT payload                     send:0          receive:0
SET_WINDOW_SIZE payload                     send:0          receive:0
NAT_DETECTION_SOURCE_IP payload             send:0          receive:0
NAT_DETECTION_DESTINATION_IP payload        send:0          receive:0
USE_TRANSPORT_MODE notification             send:0          receive:0
REKEY_SA notification                       send:0          receive:0
ESP_TFC_PADDING_NOT_SUPPORTED payload       send:0          receive:0
AUTH_LIFETIME payload                       send:0          receive:0
REDIRECT payload                            send:0          receive:0
DELETE_OLD_CHILDSA notification             send:0          receive:0
DSCP payload                                send:0          receive:0
-------------------------------------------------------------------------------
```

Table 12-30 Description of the **display ikev2 statistics notify-info** command output

Item	Description
Ikev2 notification statistics	IKEv2 notification message statistics.
Notification	IKEv2 notification message.
INVALID_IKE_SPI notification	Invalid IKE SPI notification message.
INVALID_MAJOR_VERSION notification	Invalid Major version number notification message.
INVALID_SYNTAX notification	Invalid syntax notification message.
INVALID_IPSEC_SPI notification	Invalid IPSec SPI notification message.
INVALID_KE_PAYLOAD notification	Incorrect KE payload.
SINGLE_PAIR_REQUIRED notification	Single_Pair_Required notification message.
NO_ADDITIONAL_SA notification	No additional SA notification message.
TS_UNACCEPTABLE notification	Invalid TS payload.
INVALID_IPSEC_SELECTORS notification	Invalid IPSec Selectors notification message.
INITIAL_CONTACT payload	Initial_Contact notification message.

Item	Description
SET_WINDOW_SIZE payload	Set_Window_Size notification message.
NAT_DETECTION_SOURCE_IP payload	NAT source IP notification message.
NAT_DETECTION_DESTINATION_IP payload	NAT destination IP notification message.
USE_TRANSPORT_MODE notification	Transport mode notification message.
REKEY_SA notification	SA re-negotiation notification message.
ESP_TFC_PADDING_NOT_SUPPORTED payload	ESP_TFC_Padding_Not_Supported notification message.
AUTH_LIFETIME payload	Auth_Lifetime notification message.
REDIRECT payload	Redirection notification message.
DELETE_OLD_CHILD SA notification	Delete_Old_ChildSa notification message.
DSCP payload	DSCP notification message.
send	Number of sent messages.
receive	Number of received messages.

Display packet statistics on IPSec tunnels negotiated using IKEv2.

```
<Huawei> display ikev2 statistics packet

Packet statistics:
-------------------------------------------------------------------------------
Ike_init request send    :33          Ike_init response send   :0
Ike_init request recv    :10          Ike_init response recv   :0
Ike_auth request send    :10          Ike_auth response send   :0
Ike_auth request recv    :10          Ike_auth response recv   :0
Create_child req send    :91          Create_child resp send   :147
Create_child req recv    :87          Create_child resp recv   :147
Ike_info request send    :210         Ike_info response send   :31
Ike_info request recv    :0           Ike_info response recv   :31
Del_info request send    :209         Del_info response send   :26
Del_info request recv    :0           Del_info response recv   :31
Dpd_info request send    :4           Dpd_info response send   :0
Dpd_info request recv    :0           Dpd_info response recv   :0
-------------------------------------------------------------------------------
```

Table 12-31 Description of the **display ikev2 statistics packet** command output

Item	Description
Packet statistics	IPSec packet statistics.
Ike_init request send	Number of sent IKE SA initialization exchange (ike_init) request packets.
Ike_init response send	Number of sent ike_init response packets.
Ike_init request recv	Number of received ike_init request packets.
Ike_init response recv	Number of received ike_init response packets.
Ike_auth request send	Number of sent IKE authentication exchange (ike_auth) request packets.
Ike_auth response send	Number of sent ike_auth response packets.
Ike_auth request recv	Number of received ike_auth request packets.
Ike_auth response recv	Number of received ike_auth response packets.
Create_child req send	Number of sent IPSec SA for sub-tunnel creation (create_child) request packets.
Create_child resp send	Number of sent create_child response packets.
Create_child req recv	Number of received create_child request packets.
Create_child resp recv	Number of received create_child response packets.
Ike_info request send	Number of sent IKE notification exchange (ike_info) request packets.
Ike_info response send	Number of sent ike_info response packets.
Ike_info request recv	Number of received ike_info request packets.
Ike_info response recv	Number of received ike_info response packets.
Del_info request send	Number of sent tunnel information deletion (del_info) request packets.
Del_info response send	Number of sent del_info response packets.
Del_info request recv	Number of received del_info request packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Del_info response recv	Number of received del_info response packets.
Dpd_info request send	Number of sent DPD information (dpd_info) request packets.
Dpd_info response send	Number of sent dpd_info response packets.
Dpd_info request recv	Number of received dpd_info request packets.
Dpd_info response recv	Number of received dpd_info response packets.

Display SA statistics on IPSec tunnels negotiated using IKEv2.

```
<Huawei> display ikev2 statistics sa

Sa establish and offline statistic:
-------------------------------------------------------------------------------
Establish:
Initiator request phase1 negotiation                    :33
Initiator request phase2 negotiation                    :16
Initiator request and success phase1 negotiation          :10
Initiator request and success phase2 negotiation          :41
Responder response phase1 negotiation                    :0
Responder response phase2 negotiation                    :0
Responder response and success phase1 negotiation          :0
Responder response and success phase2 negotiation          :0
Offline:
Receive delete info      :1          Config modify          :0
Manual reset             :1          Dpd timeout            :0
Phase1 hardware expire   :0          Phase2 hardware expire   :0
Phase1 replace           :0          Phase2 replace         :0
Aaa cut user             :0          Reauth timeout         :0
Flow overlap             :0          IP address syn failed  :0
Port mismatch            :0          Kick old SA            :0
CPU table updated        :0          SPI conflict           :0
EAP delete old sa        :0
-------------------------------------------------------------------------------
```

Table 12-32 Description of the **display ikev2 statistics sa** command output

Item	Description
Sa establish and offline statistic	SA establishment and deletion information.
Establish	Statistics on established IPSec tunnels.
Initiator request phase1 negotiation	Number of times that the initiator requests phase 1 negotiation.
Initiator request phase2 negotiation	Number of times that the initiator requests phase 2 negotiation.

Item	Description
Initiator request and success phase1 negotiation	Number of times that the initiator succeeds in requesting phase 1 negotiation.
Initiator request and success phase2 negotiation	Number of times that the initiator succeeds in requesting phase 2 negotiation.
Responder response phase1 negotiation	Number of times that the responder responds to phase 1 negotiation.
Responder response phase2 negotiation	Number of times that the responder responds to phase 2 negotiation.
Responder response and success phase1 negotiation	Number of times that the responder succeeds in responding to phase 1 negotiation.
Responder response and success phase2 negotiation	Number of times that the responder succeeds in responding to phase 2 negotiation.
Offline	Statistics on deleted IPSec tunnels.
Receive delete info	Number of times that the device receives tunnel deletion messages.
Config modify	Number of times that the tunnel is deleted by modifying the configuration.
Manual reset	Number of times that the tunnel is deleted manually.
Phase1 hardware expire	Number of times that the phase 1 tunnel is deleted due to hard timeout.
Phase2 hardware expire	Number of times that the phase 2 tunnel is deleted due to hard timeout.
Phase1 replace	Number of phase 1 tunnel re-negotiation times.
Phase2 replace	Number of phase 2 tunnel re-negotiation times.
Aaa cut user	Number of tunnel deletion times caused by forced user offline.
Dpd timeout	Number of tunnel deletion times caused by DPD timeout.
Reauth timeout	Number of tunnel deletion times caused by re-authentication timeout.
Flow overlap	Number of tunnel deletion times caused by the conflict between the IP address in the encrypted flow and remote IP address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IP address syn failed	Number of tunnel deletion times caused by the failure to synchronize IP addresses.
Port mismatch	Number of tunnel deletion times caused by the UDP port mismatch.
Kick old SA	Number of tunnel deletion times caused by a flow conflict.
CPU table updated	Number of tunnel deletion times caused by a CPU table update.
SPI conflict	Number of tunnel deletion times caused by an SPI conflict.
EAP delete old sa	Number of times the device deletes the old SA during EAP authentication.

12.6.27 display ike user-table (all views)

Function

The **display ike user-table** command displays IKE user table information.

Format

display ike user-table [**number** *user-table-id* [**user-name** *user-name*]]

Parameters

Parameter	Description	Value
number *user-table-id*	Specifies the ID of an IKE user table. If this parameter is not specified, the command displays information about all IKE user tables.	The value must be an existing IKE user table ID.
user-name *user-name*	Specifies a user name.	The value must be a user name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the user ID type, user ID, pre-shared key, and user description in an IKE user table.

Example

Display information about all IKE user tables.

```
<Huawei> display ike user-table
Number of IKE User-tables: 1

-----------------------------------------------------------------------------
 IKE User-table: 10, Number of users: 1
-----------------------------------------------------------------------------

  User Name             : user1
  User ID-type          : IP
  User ID               : 1.1.1.1
  Pre-shared-key        : %^%#D,Ul0!:u2RM;giQtp4KDzkbm*)=Y[NYF[N6s)SMQ%^%#
  VPN instance          : vrf1
  Description           : USER1
  Interface-assign      : Tunnel0/0/1
```

Table 12-33 Description of the **display ike user-table** command output

Item	Description
Number of IKE User-tables	Number of IKE user tables.
Number of users	Number of IKE users.
IKE User-table	ID of an IKE user table.
User Name	IKE user name. To configure the IKE user name, run the **12.6.178 user** command.
User ID-type	Remote ID type of the IKE peer. • ANY: The remote ID type of the IKE peer is of any type. • ESN: The remote ID type of the IKE peer is an ESN. • FQDN: The remote ID type of the IKE peer is a name. • IP: The remote ID type of the IKE peer is an IP address. • USER-FQDN: The remote ID type of the IKE peer is a user domain name. To configure the remote ID type of an IKE peer, run the **12.6.63 id-type** command.
User ID	Remote ID of the IKE peer. To configure the remote ID of an IKE peer, run the **12.6.63 id-type** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pre-shared-key	Pre-shared key. To configure the pre-shared key, run the **12.6.127 pre-shared-key (IKE user view)** command.
VPN instance	Name of the VPN instance. To configure the name of a VPN instance, run the **12.6.181 vpn-instance-traffic (IKE user view)** command.
Description	Description of the IKE user table. To configure the description of an IKE user table, run the **12.6.13 description** command.
Interface-assign	Interface with which an IKE user associates. To specify an interface, run the **12.6.88 interface-assign** command.

12.6.28 display ike user-table ctrl-plane

Function

The **display ike user-table ctrl-plane** command displays IKE user table information on control plane.

Format

display ike user-table [**number** *user-table-id* [**user-name** *user-name*]] **ctrl-plane**

Parameters

Parameter	Description	Value
number *user-table-id*	Specifies the ID of an IKE user table. If the name of an IKE user table is not specified, information about all IKE user tables is displayed.	The ID of an IKE user table must already exist.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the user ID type, user ID, pre-shared key, and user description in an IKE user table.

Example

Display information about all IKE user tables.

```
<Huawei> display ike user-table ctrl-plane
Number of IKE User-tables: 1

-----------------------------------------------------------------------------
 IKE User-table: 10, Number of users: 1
-----------------------------------------------------------------------------

  User Name              : user1
  User ID-type           : IP
  User ID                : 1.1.1.1
  Pre-shared-key         : %^%#D,Ul0!:u2RM;giQtp4KDzkbm*)=Y[NYF[N6s)SMQ%^%#
  VPN instance           : vrf1
  Description            : USER1
```

Table 12-34 Description of the **display ike user-table ctrl-plane** command output

Item	Description
Number of IKE User-tables	Number of IKE user tables.
Number of users	Number of IKE users.
IKE User-table	ID of an IKE user table.
User Name	IKE user name.
User ID-type	Remote ID type of the IKE peer.
User ID	Remote ID of the IKE peer.
Pre-shared-key	Pre-shared key.
VPN instance	Name of the VPN instance.
Description	Description of the IKE user table.

12.6.29 display interface tunnel-template

Function

The **display interface tunnel-template** command displays information about a tunnel template interface.

Format

display interface tunnel-template [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of a tunnel template.	The number must be an existing tunnel template.
main	Displays information about only a tunnel template interface. If a tunnel template interface has no sub-interface, the information about the tunnel template interface is displayed regardless of whether the **main** parameter is specified.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Displays information about Tunnel template 0.

```
<Huawei> display interface tunnel-template 0
Tunnel-Template0 current state : UP
Line protocol current state : DOWN
Description:ith
Route Port,The Maximum Transmit Unit is 1500
Internet Address is unnumbered, using address of LoopBack0(1.1.1.1/32)
Encapsulation is TUNNEL, loopback not set
Tunnel protocol IPSEC
Current system time: 2013-10-24 14:58:00
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    0 seconds input rate 0 bits/sec, 0 packets/sec
    0 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
```

 Copyright © Huawei Technologies Co., Ltd.

```
  0 packets output,  0 bytes
  0 output error
  Input bandwidth utilization  : --
  Output bandwidth utilization : --
```

Table 12-35 Description of the **display interface tunnel-template** command output

Item	Description
Tunnel-Template0 current state	Physical status of the tunnel template interface: ● **UP**: The physical status of the tunnel template interface is Up. ● **DOWN**: The physical status of the tunnel template interface is Down.
Line protocol current state	Link layer protocol status of the tunnel template interface: ● **UP**: The link layer protocol status of the tunnel template interface is Up. ● **DOWN**: The link layer protocol of the tunnel template interface is Down or no IP address is assigned to the tunnel template interface.
Description	Description of the tunnel template interface.
Route Port	Indicates that the interface is a Layer 3 interface.
The Maximum Transmit Unit is 1500	MTU of the tunnel template interface. The default MTU is 1500 bytes. If the length of a packet is greater than the MTU, it is fragmented before being sent. If fragmentation is disabled, the packet is discarded.
Internet Address is unnumbered, using address of LoopBack0 (1.1.1.1/32)	Indicates that the interface IP address is borrowed from Loopback 0 (1.1.1.1/32).
Encapsulation is TUNNEL	Indicates that the tunnel template interface encapsulates packets in tunnel mode.
loopback not set	Indicates that the loopback mode is not set for the tunnel-template interface.
Tunnel protocol IPSEC	Indicates that the tunnel encapsulation protocol is IPsec.
Current system time	Current time of the system. If a time zone is configured and the daylight saving time begins, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC±HH:MM DST.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
300 seconds input rate 0 bits/sec, 0 packets/sec	Receive bit and packet rates on the tunnel template interface within the first 300 seconds. You can run the **set flow-stat interval** command to change the interval at which traffic statistics are collected. The interval must be an integer multiple of 10 and range from 10 to 600, in seconds.
300 seconds output rate 0 bits/sec, 0 packets/sec	Send bit and packet rates on the tunnel template interface within the first 300 seconds. You can run the **set flow-stat interval** command to change the interval at which traffic statistics are collected. The interval must be an integer multiple of 10 and range from 10 to 600, in seconds.
0 seconds input rate 0 bits/sec, 0 packets/sec	Receive bit and packet rates within the interval between two queries.
0 seconds output rate 0 bits/sec, 0 packets/sec	Send bit and packet rates within the interval between two queries.
0 packets input, 0 bytes	Total numbers of packets and bytes received by the tunnel template interface.
0 input error	Number of error packets received by the tunnel template interface.
0 packets output, 0 bytes	Total numbers of packets and bytes sent by the tunnel template interface.
0 output error	Number of error packets sent by the tunnel template interface.
Input bandwidth utilization	"--" indicates that this item is not supported.
Output bandwidth utilization	"--" indicates that this item is not supported.

Related Topics

12.6.89 interface tunnel-template

12.6.30 display ipsec efficient-vpn

Function

The **display ipsec efficient-vpn** command displays Efficient VPN policy information.

Format

display ipsec efficient-vpn [**brief** | **capability** | **name** *efficient-vpn-name* | **remote**]

Parameters

Parameter	Description	Value
brief	Displays brief information about Efficient VPN policies.	-
capability	Displays the IPSec configuration supported by an Efficient VPN policy.	-
name *efficient-vpn-name*	Displays information about a specified Efficient VPN policy.	The value is an existing Efficient VPN policy name.
remote	Displays the running status of remote devices. **remote** only takes effect on the server.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Efficient VPN policy is configured, you can run this command to know the configuration information of the Efficient VPN policy, such as the name, interface, authentication method, IKE version, DH algorithm, and PFS algorithm of the Efficient VPN.

Example

Display brief information about Efficient VPN policies.

```
<Huawei> display ipsec efficient-vpn brief
 Total number of IPSec efficient-vpn: 1

 Efficient-vpn name      Efficient-vpn mode
 ------------------------------------------
 v1                      client
```

Display information about the Efficient VPN policy named **easyvpn_1**.

```
<Huawei> display ipsec efficient-vpn name easyvpn_1
=========================================
IPSec efficient-vpn name: easyvpn_1
Using interface        : GigabitEthernet1/0/0
=========================================
 IPSec Efficient-vpn Name  : easyvpn_1
 IPSec Efficient-vpn Mode  : 3 (1:Client 2:Network 3:Network-plus 4:Network-auto-cfg)
 ACL Number                :
 Auth Method               : 8 (8:PSK 9:RSA)
 VPN name                  :
 Local ID Type             : 1 (1:IP 2:Name 3:User-fqdn 9:DN 11:Key-id)
 IKE Version               : 1 (1:IKEv1 2:IKEv2)
 Remote Address            : 1.1.1.1
 Pre Shared Key            :
 DH Group                  : DH group 14
 PFS Type                  : DH group 14
 Remote Name               :
 PKI Object                :
 Re-auth interval          : 300 seconds
 Anti-replay window size   : 32
 Qos pre-classify          : 0 (0:Disable 1:Enable)
 Qos group                 : -
 Service-scheme name       : scheme
 DPD Msg Type
 Sim-based-username Type   : IMEI
 RSA signature-padding     : PKCS1
 Interface loopback        : LoopBack100
 Interface loopback IP     : 1.2.1.1/25
 Dns server IP             : 2.2.2.2, 2.2.2.3
 Wins server IP            : 3.3.3.2, 3.3.3.3
 Dns default domain name   : mydomain.com.cn
 Auto-update url           :
 Auto-update version       :
 IP pool                   : 10.1.1.0/255.255.255.0
 Resource acl list         : 1
   IP address/mask         : 5.1.1.2/255.255.255.255
   Source port number      : 0
   Destination port number : 0
   Protocol ID             : 0
 Resource acl list         : 2
   IP address/mask         : 6.1.1.0/255.255.255.0
   Source port number      : 0
   Destination port number : 0
   Protocol ID             : 0
```

Table 12-36 Description of the **display ipsec efficient-vpn** command output

Item	Description
IPSec Efficient-vpn Name/ Efficient-vpn name	Name of the Efficient VPN policy. To configure an Efficient VPN policy, run the **ipsec efficient-vpn (system view)** command.
Using interface	Interface to which an Efficient VPN policy is applied.

Item	Description
IPSec Efficient-vpn Mode/ Efficient-vpn mode	Mode used by the Efficient VPN policy. ● 1: client ● 2: network ● 3: network-plus ● 4: network-auto-cfg To configure an Efficient VPN policy, run the **ipsec efficient-vpn (system view)** command.
ACL Number	ACL used by the Efficient VPN policy. To configure an ACL referenced by an Efficient VPN policy, run the **security acl** command.
Auth Method	Authentication mode used by the Efficient VPN policy: ● 8: pre-shared key authentication ● 9: RSA signature authentication To configure an authentication mode, run the **authentication-method** command.
VPN name	Name of the VPN instance bound to the Efficient VPN policy. To bind a VPN instance to an Efficient VPN policy, run the **sa binding vpn-instance (Efficient VPN policy view)** command.
Local ID Type	Local ID type in IKE negotiation, to set the local ID type, run the **local-id-type** command.
IKE Version	Configured IKE version: ● 1: IKEv1 ● 2: IKEv2
Remote Address	IP address of the remote IKE peer. To configure the remote IP address, run the **remote-address** command.
Pre Shared Key	Pre-shared key. To configure a pre-shared key, run the **pre-shared-key** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DH Group	DH group used in IKE negotiation: ● DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify a DH group, run the **dh** command.
PFS Type	Perfect Forward Secrecy (PFS) used in IKE negotiation: ● DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify a PFS, run the **pfs** command.
Remote Name	Remote name used in IKE negotiation. To configure the remote name used in IKE negotiation, run the **remote-name** command. When the **local-id-type name** command is used, the local and remote names are used for IKE negotiation. If **ike local-name** is not configured on the remote end, the name specified by the **sysname** command is used for IKE negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PKI Object	PKI domain bound to the Efficient VPN policy. To bind a PKI domain to an Efficient VPN policy, run the **12.6.124 pki realm** command.
Re-auth interval	IKEv2 re-authentication interval. To configure IKEv2 re-authentication interval, run the **12.6.133 re-authentication interval** command.
Anti-replay window size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **ipsec anti-replay window** command. When the value is 0, the IPSec anti-replay function is enabled in the system view. To enable this function, run the **12.6.92 ipsec anti-replay enable** command.
Qos pre-classify	Whether pre-extraction of original IP packets is enabled: ● 0: Pre-extraction of original IP packets is enabled. ● 1: Pre-extraction of original IP packets is disabled. To enable pre-extraction of original IP packets, run the **qos pre-classify** command.
Qos group	QoS group to which IPSec packets belong. To configure the QoS group, run the **qos group** command. - indicates that no QoS group is specified for IPSec packets.
Service-scheme name	Name of the bound service scheme. To configure the name of the bound service scheme, run the **12.6.169 service-scheme (Efficient VPN policy view)** command.
DPD Msg Type	Sequence of the payload in DPD packets. ● seq-notify-hash ● seq-hash-notify To configure the sequence of the payload, run the **12.6.51 dpd msg** command.
Sim-based-username Type	Type of the SIM card user name. ● IMEI: international mobile equipment identity. ● IMSI: international mobile subscriber identity.
RSA signature-padding	Padding mode of an RSA signature. To specify the padding mode, run the **12.6.152 rsa signature-padding** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface loopback	Number of the loopback interface. The loopback interface is dynamically created on the remote device and is used to establish an IPSec tunnel with the Efficient VPN server.
Interface loopback IP	IP address of the loopback interface, which is allocated by the Efficient VPN server to the remote device.
Dns server IP	DNS server IP address. To configure a DNS server IP address, run the **dns** command.
Wins server IP	WINS server IP address. To configure a WINS server IP address, run the **wins** command.
Dns default domain name	DNS domain name. To configure a DNS domain name, run the **dns-name** command.
Auto-update url	URL of the file used to upgrade a remote device. To configure the URL of the file used to upgrade a remote device, run the **auto-update url** command.
Auto-update version	Version number of the version file. To configure the version number of the version file, run the **auto-update url** command.
IP pool	IP address obtained from the address pool.
Resource acl list	Delivered ACL list. The value is the number of configured ACL rules. This field is available only when ACL delivery is enabled using the **resource acl** command.
IP address/mask	Delivered IP address or mask. To specify an IP address or port number, run the **rule (advanced ACL view)** command.
Source port number	Delivered source port number. To specify a source port number, run the **rule (advanced ACL view)** command.
Destination port number	Delivered destination port number. To specify a destination port number, run the **rule (advanced ACL view)** command.
Protocol ID	Delivered protocol ID. To specify a protocol ID, run the **rule (advanced ACL view)** command.

Display the IPSec configuration supported by an Efficient VPN policy.

```
<Huawei> display ipsec efficient-vpn capability

 IKEv1 Global Supported Algorithms
```

```
-------------------------------------------------------
  Supported DH Groups:
    DH_GROUP1 | DH_GROUP2 | DH_GROUP5 | DH_GROUP14 | DH_GROUP19 | DH_GROUP20 |
DH_GROUP21
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256
  Supported Authentication Algorithms:
    MD5 | SHA1 | SHA2-256 | SHA2-384 | SHA2-512
  Supported Authentication Methods:
    Pre Shared Key | RSA_SIG

  IKEv2 Global Supported Algorithms
-------------------------------------------------------
  Supported DH Groups:
    DH_GROUP1 | DH_GROUP2 | DH_GROUP5 | DH_GROUP14 | DH_GROUP19 | DH_GROUP20 |
DH_GROUP21
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256
  Supported Integrity Algorithms:
    MD5 | SHA1 | AES-XCBC-96 | SHA2-256 | SHA2-384 | SHA2-512
  Supported PRF:
    PRF-MD5 | PRF-SHA1 | PRF-AES-XCBC-128 | PRF-SHA2-256 | PRF-SHA2-384 |
    PRF-SHA2-512

  IPSEC Global Supported Algorithms
-------------------------------------------------------
  Supported Security Protocols:
    ESP
  Supported Encapsulation Modes:
    TUNNEL
  Supported Authentication Algorithms:
    MD5 | SHA1 | SHA256 | SHA384 | SHA512 | NULL
  Supported Encryption Algorithms:
    DES | 3DES | AES128 | AES192 | AES256 | NULL
```

NOTE

- The MD5 and SHA-1 authentication algorithms have security risks; therefore, you are advised to use SHA-2 preferentially.
- The DES and 3DES encryption algorithms have security risks; therefore, you are advised to use AES preferentially.
- The PRF-MD5 and PRF-SHA1 algorithms have security risks; therefore, you are advised to use PRF-AES-XCBC-128 or SHA-2 preferentially.

Table 12-37 Description of the **display ipsec efficient-vpn capability** command output

Item	Description
IKEv1 Global Supported Algorithms	Supported algorithms when IKEv1 is specified in the Efficient VPN policy. The server can use only the supported algorithms to negotiate with the remote device.
Supported DH Groups	Supported DH groups when IKEv1 or IKEv2 is used. To configure a DH group on the server, run the **dh** command.

Item	Description
Supported Encryption Algorithms	Supported encryption algorithms when IKEv1 or IKEv2 is used. To configure an authentication algorithm on the server, run the **authentication-algorithm** command.
Supported Authentication Algorithms	Supported authentication algorithms when IKEv1 is used. To configure an authentication algorithm on the server, run the **authentication-algorithm** command.
Supported Authentication Methods	Supported authentication algorithms when IKEv1 is used: ● Pre Shared Key: pre-shared key authentication ● RSA_SIG: RSA signature authentication To configure an authentication mode on the server, run the **authentication-method** command.
IKEv2 Global Supported Algorithms	Supported algorithms when IKEv2 is specified in the Efficient VPN policy. The server can use only the supported algorithms to negotiate with the remote device.
Supported Integrity Algorithms	Supported integrity algorithms when IKEv2 is used. To configure an integrity algorithm on the server, run the **12.6.87 integrity-algorithm** command.
Supported PRF	Supported PRF algorithms when IKEv2 is used. To configure a PRF algorithm on the server, run the **prf** command.
IPSEC Global Supported Algorithms	Algorithms supported by the system.
Supported Security Protocols	Security protocol supported by IPSec: ESP. To configure a security protocol, run the **transform** command.
Supported Encapsulation Modes	Encapsulation mode supported by IPSec: tunnel mode. To configure an encapsulation mode, run the **encapsulation-mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Supported Authentication Algorithms	Authentication algorithm supported by IPSec. To configure an authentication algorithm on the server, run the **esp authentication-algorithm** command.
Supported Encryption Algorithms	Encryption algorithm supported by IPSec. To configure an encryption algorithm on the server, run the **esp encryption-algorithm** command.

Display running status of remote devices.

```
<Huawei> display ipsec efficient-vpn remote
 Total number of remote : 1

 Local interface         : GigabitEthernet0/0/2
 Client IP address       : 10.1.1.1:500
 Client system MAC       : 5489-98f4-78f4
 Client description      :
 Client alloc address    : 10.1.1.254
 Client version ID       : 2
 Client last upgrade info: Failed to get the upgrade information.
```

Table 12-38 Description of the **display ipsec efficient-vpn remote** command output

Item	Description
Total number of remote	Number of remote devices.
Local interface	Interface bound to an IPSec policy on the server. To bind an IPSec policy group to an interface, run the **12.6.104 ipsec policy (interface view)** command.
Client IP address	IP address of the remote device.
Client system MAC	MAC address of the remote device.
Client description	Device information and version information about the remote device.
Client alloc address	IP address delivered by the Efficient VPN server to the remote device.
Client version ID	Version number of the version file delivered from the server to the remote device.
Client last upgrade info	Information about the last automatic upgrade on the remote device.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.6.98 ipsec efficient-vpn (system view)
12.6.97 ipsec efficient-vpn (interface view)

12.6.31 display ipsec history record

Function

The **display ipsec history record** command displays history information about IPSec tunnels.

Format

display ipsec history record [**remote-address** *remote-address*]

Parameters

Parameter	Description	Value
remote-address *remote-address*	Displays history information about the IPSec tunnel with the specified remote IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipsec history record** command to view the reason and time of the last teardown of the IPSec tunnel.

Example

Display history information about IPSec tunnels.

```
<Huawei> display ipsec history record
IPSec history record:
==============================
Interface             : GigabitEthernet1/0/1
remote-address          : 2.1.1.1
remote-port            : 500
VPN-name               : huawei
flow-source            : 10.1.1.1/255.255.255.255
flow-destination       : 10.2.2.2/255.255.255.255
last-offline-reason    : peer request
```

```
last-offline-time      : 2017-07-17 20:25:31
offline-times-in-24Hour: 1
```

Table 12-39 Description of the **display ipsec history record** command output

Item	Description
IPSec history record	Display history information about IPSec tunnels.
Interface	Interface to which an IPSec policy is applied.
remote-address	Remote IP address of an IPSec tunnel.
remote-port	Remote UDP port number.
VPN-name	Name of a VPN instance.
flow-source	Source address segment of data flows.
flow-destination	Destination address segment of data flows.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
last-offline-reason	Reason of the last teardown of an IPSec tunnel. ● dpd timeout: Dead peer detection (DPD) times out. ● peer request: The remote end has sent a message, asking the local end to tear down the tunnel. ● config modify or manual offline: An SA is deleted due to configuration modification or an SA is manually deleted. ● phase1 hard expiry: Hard lifetime expires in phase 1 (no new SA negotiation success message is received). ● phase2 hard expiry: Hard lifetime expires in phase 2. ● heartbeat timeout: heartbeat detection times out. ● modecfg address soft expiry: The IP address lease applied by the remote end from the server expires. ● re-auth timeout: An SA is deleted due to reauthentication timeout. ● aaa cut user: The AAA module disconnects users. ● peer address switch: An SA is deleted due to change of the peer address. ● hard expiry triggered by port mismatch: A hard timeout occurs due to mismatch NAT port number. ● kick old sa with same flow: The old SA is deleted for the same incoming flow. ● spi conflict: An SPI conflict occurs. ● phase1 sa replace: The new IKE SA replaces the old IKE SA. ● phase2 sa replace: The new IPSec SA replaces the old IPsec SA. ● nhrp notify: NHRP notifies the device that the SA needs to be deleted. ● disconnect track nqa/bfd/vrrp: The IPSec tunnel is torn down based on the NQA test instance, NQA group, VRRP, BFD session, or BFD group status. ● receive invalid spi notify: The device receives an invalid SPI notification. ● dns resolution status change: DNS resolution status changes. ● ikev1 phase1-phase2 sa dependent offline: The device deletes the associated IPSec SA when deleting an IKEv1 SA.
last-offline-time	Last time an IPSec tunnel was torn down.
offline-times-in-24Hour	Number of times an IPSec tunnel was torn down within 24 hours.

 Copyright © Huawei Technologies Co., Ltd.

12.6.32 display ipsec global config

Function

The **display ipsec global config** command displays IPSec global configurations.

Format

display ipsec global config

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view IPSec global configurations, run the **display ipsec global config** command. The global configurations include the global SA lifetime and whether the anti-replay function is enabled.

Example

Display IPSec global configurations.

```
<Huawei> display ipsec global config
IPSec Global Config:
-------------------------------------------------------------
  IPSec sa global-duration time-based(seconds)        : 3600
  IPSec sa global-duration traffic-based(kbytes)      : 1843200
  IPSec anti-replay                                   : enable
  IPSec df-bit                                        : copy
  IPSec fragmentation                                 : disable
  IPSec nat-traversal source-port                     : 8000
  IPSec invalid-spi-recovery                          : disable
  IPSec netmask source                                : 24
  IPSec netmask destination                           : 24
-------------------------------------------------------------
```

Table 12-40 Description of the **display ipsec global config** command output

Item	Description
IPSec Global Config	IPSec global configurations.
IPSec sa global-duration time-based(seconds)	Time-based global SA lifetime, in seconds. To set the time-based global SA lifetime, run the **ipsec sa global-duration time-based** command.

Item	Description
IPSec sa global-duration traffic-based(kbytes)	Traffic-based global SA lifetime, in kilobytes. To set the traffic-based global SA lifetime, run the **ipsec sa global-duration traffic-based** command.
IPSec anti-replay	Whether the anti-replay function is enabled. To configure the anti-replay function, run the **12.6.92 ipsec anti-replay enable** command.
IPSec df-bit	IPSec tunnel don't fragment (DF) bit: ● clear: The DF bit is set to 0, allowing packets to be fragmented. ● set: The DF bit is set to 1, prohibiting packets from being fragmented. ● copy: The DF bit is that of original packets. To set the DF bit, run the **12.6.96 ipsec df-bit** command.
IPSec fragmentation	IPSec tunnel packet fragmentation mode: ● enable: Fragmentation before IPSec encryption. ● disable: Fragmentation after IPSec encryption To set the fragmentation mode, run the **12.6.99 ipsec fragmentation before-encryption** command.
IPSec nat-traversal source-port	Port number used for IPSec NAT traversal. To configure the port number used for IPSec NAT traversal, run the **12.6.101 ipsec nat-traversal source-port** command.
IPSec invalid-spi-recovery	Whether the invalid SPI recovery function is enabled: ● enable ● disable To configure the invalid SPI recovery function, run the **12.6.100 ipsec invalid-spi-recovery enable** command.
IPSec netmask source	Source address mask of data flows. To configure the source address mask of data flows, run the **12.6.102 ipsec netmask** command. When the source address mask is not configured, the mask length is 0.
IPSec netmask destination	Destination address mask of data flows. To configure the destination address mask of data flows, run the **12.6.102 ipsec netmask** command. When the destination address mask is not configured, the mask length is 0.

 Copyright © Huawei Technologies Co., Ltd.

12.6.33 display ipsec interface brief

Function

The **display ipsec interface brief** command displays IPSec policies bound to an interface.

Format

display ipsec interface brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an IPSec policy is bound to an interface, you can run this command to view information about the bound IPSec policy, such as the policy name and interface to which the policy is bound.

Example

Display IPSec policies bound to an interface.

```
<Huawei> display ipsec interface brief
-----------------------------------------------
  IPSec policy        : policy1
  Using interface     : GigabitEthernet1/0/0
  IPSec policy number : 10
  IPSec policy Type   : policy
-----------------------------------------------
```

Table 12-41 Description of the **display ipsec interface brief** command output

Item	Description
IPSec policy	Sequence number of the IPSec policy bound to the interface. Name of the IPSec policy bound to an interface. To apply an IPSec policy to an interface, run the **ipsec policy (interface view)**, **ipsec profile (interface view)**, or **ipsec efficient-vpn (interface view)** command.
Using interface	Interface to which an IPSec policy is applied.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec policy number	Sequence number of the IPSec policy bound to the interface. To configure an IPSec policy, run the **ipsec policy (system view)** or **ipsec profile (system view)** command.
IPSec policy Type	Type of the IPSec policy bound to an interface: • policy: IPSec policy in manual or IKE negotiation mode • profile: IPSec profile • template: IPSec policy template • efficient-vpn: Efficient VPN policy

12.6.34 display ipsec policy (all views)

Function

The **display ipsec policy** command displays IPSec policy information.

Format

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]]

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec policies.	-
name *policy-name*	Displays detailed information about an IPSec policy with a specified name.	The value must be an existing IPSec policy name.
seq-number	Displays detailed information about an IPSec policy with a specified sequence number.	The value must be an existing IPSec policy sequence number.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If no parameter is specified, this command displays detailed information about all IPSec policies.

You can use the **display ipsec policy brief** command to check brief information about all IPSec policies, including:

- Name and sequence number
- Negotiation mode
- ACL number
- IKE peer
- Local address
- Remote address

Using the **name** parameter, you can view details on the specified IPSec policy. In this case, the information is displayed in detailed format. If you specify **name** *policy-name* and do not specify *seq-number*, the command displays detailed information about an IPSec policy group.

Example

Display brief information about all the IPSec policies.

```
<Huawei> display ipsec policy brief
Number of policies group : 1
Number of policies       : 1

Policy name          Mode     ACL        Peer name   Local address    Remote address
-------------------------------------------------------------------------------------------
policy1-100          isakmp   3002/IPv4  peer1
```

Table 12-42 Description of the **display ipsec policy brief** command output

Item	Description
Number of policies group	Number of IPSec policy groups. An IPSec policy is identified by its name and sequence number, and multiple IPSec policies with the same name constitute an IPSec policy group.
Number of policies	Number of IPSec policies.
Policy name	Name and sequence number of an IPSec policy. To configure an IPSec policy, run the **ipsec policy (system view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Mode in which an IPSec policy is created: ● isakmp: The IPSec policy is created in IKE negotiation mode. ● template: The IPSec policy is created using an IPSec policy template. ● manual: The IPSec policy is created manually. To configure IPSec policy creation mode, run the **ipsec policy (system view)** command.
ACL	ACL referenced in the IPSec policy. To reference an ACL in an IPSec policy, run the **security acl** command.
Peer name	Name of the IKE peer referenced in the IPSec policy. To configure an IKE peer, run the **ike-peer** command.
Local address	Local IP address used in IPSec negotiation. To configure the local IP address used in IPSec negotiation, run the **12.6.174 tunnel local** command.
Remote address	Remote IP address used in IPSec negotiation. To configure the remote IP address used in IPSec negotiation, run the **12.6.175 tunnel remote** command.

Display information about all IPSec policies.

```
<Huawei> display ipsec policy
===========================================
IPSec policy group: "10"
Using interface: GigabitEthernet6/0/0
===========================================
    Sequence number: 10
    Policy Alias: map1-10
    Security data flow: 3000/IPv4
    Peer name    :  rut2
    Perfect forward secrecy: DH group 14
    Proposal name:  prop1
    IPSec SA local duration(time based): 3600 seconds
    IPSec SA local duration(traffic based): 1843200 kilobytes
    SA trigger mode: Traffic-based
    Route inject: None
    Route inject state: -
    Route inject nexthop: -
    Route inject preference: -
    Policy state: Enable
    Anti-replay window size: 1024
    Fragment before-encryption: Disable
```

```
  Respond-only: Enable
  Policy status  : Inactive
  Qos pre-classify: Disable
  Qos group: -
  Sa keep-holding-to hard-duration : Disable
```

Table 12-43 Description of the **display ipsec policy** command output

Item	Description
IPSec policy group	Name of an IPSec policy group. To configure an IPSec policy group, run the **ipsec policy (system view)** command.
Using interface	Interface to which an IPSec policy group is applied.
Sequence number	Sequence number of an IPSec policy. To configure a sequence number, run the **ipsec policy (system view)** command.
Policy Alias	Alias of the IPSec policy. To configure an alias for an IPSec policy, run the **12.6.2 alias** command.
Security data flow	ACL referenced in the IPSec policy. To reference an ACL in an IPSec policy, run the **security acl** command.
Peer name	IKE peer referenced in the IPSec policy. To configure an IKE peer, run the **ike-peer** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used in IKE negotiation: ● DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To configure the PFS used in IKE negotiation, run the **pfs** command.
Proposal name	IPSec proposal referenced in the IPSec policy. To reference an IPSec proposal, run the **proposal** command.
IPSec SA local duration(time based)	Time-based IPSec SA lifetime. To set the time-based lifetime of the local SA, run the **sa duration time-based** command in the IPSec policy view.
IPSec SA local duration(traffic based)	Traffic-based IPSec SA lifetime. To set the traffic-based lifetime of the local SA, run the **sa duration traffic-based** command in the IPSec policy view.
SA trigger mode	SA trigger mode: ● Automatic ● Traffic-based To configure an SA trigger mode, run the **sa trigger-mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Route inject state	Route injection status: ● Dynamic, Preference: Dynamic route injection is enabled and a priority is configured for the static routes generated through route injection. ● Static, Preference: Static route injection is enabled and a priority is configured for the static routes generated through route injection. ● None: Route injection is disabled. ● Dynamic: Dynamic route injection is enabled. ● Static: Static route injection is enabled. To configure route injection, run the **route inject** command.
Route inject nexthop	Next hop of a generated route. To configure route injection, run the **route inject** command.
Route inject preference	Priority of a generated route. To configure route injection, run the **route inject** command.
Policy state	Policy status: ● Enable ● Disable
Anti-replay window size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **12.6.5 anti-replay window** command.
Fragment before-encryption	IPSec fragmentation mode: ● Enable: IPSec packets are fragmented before encryption. ● Disable: IPSec packets are fragmented after encryption. To configure an IPSec fragmentation mode, run the **12.6.99 ipsec fragmentation before-encryption** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Respond-only	Whether the local end is enabled to initiate IPSec negotiation when an IPSec policy in ISAKMP mode is used to create an IPSec tunnel. ● Enable: The local end functions as the IPSec responder and does not initiate IPSec negotiation. ● Disable: The local end initiates IPSec negotiation.
Policy status	IPSec policy status: ● Active ● Inactive To set an IPSec policy to the active state, run the **12.6.125 policy enable** command.
Qos pre-classify	Pre-extraction of original IP packets. To configure pre-extraction of original IP packets, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which the IPSec packets belong. To configure the QoS group, run the **12.6.131 qos group** command.
Sa keep-holding-to hard-duration	Whether the device deletes the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation. ● Enable: The device will delete the original IPSec SA after the hard lifetime expires. ● Disable: The device deletes the original IPSec SA immediately. To configure the device to delete the original IPSec SA after the hard lifetime expires, run the **12.6.161 sa keep-holding-to hard-duration** command.

12.6.35 display ipsec policy ctrl-plane

Function

Using the **display ipsec policy ctrl-plane** command, you can view information about the IPSec policy on control plane.

Format

display ipsec policy [**brief** | **name** *policy-name* [*seq-number*]] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about all the IPSec policies.	-
name *policy-name*	Specifies the name of an IPSec policy.	The value is an existing IPSec policy name.
seq-number	Specifies the sequence number of an IPSec policy	The value is an existing IPSec policy number.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

If the policy name or the sequence number is not specified, detailed information about all IPSec policies is displayed.

Using the **display ipsec policy brief ctrl-plane** command, you can view the following brief information about all IPSec policies. In this case, the information is displayed in brief format.

- Name and sequence number
- Negotiation mode
- ACL number
- IKE peer
- Local address
- Remote address

Using the **name** parameter, you can view details on the specified IPSec policy. In this case, the information is displayed in detailed format. If you specify **name** *policy-name* and do not specify *seq-number*, the command displays detailed information about an IPSec policy group.

Example

Display brief information about all the IPSec policies.

```
<Huawei> display ipsec policy brief ctrl-plane
Number of policies group : 1
```

```
Number of policies       : 1

Policy name          Mode     ACL   Peer name   Local address    Remote address
-------------------------------------------------------------------------------
policy1-100          isakmp   3002  peer1       60.1.1.1         60.1.1.2
```

Table 12-44 Description of the **display ipsec policy brief ctrl-plane** command output

Item	Description
Number of policies group	Number of IPSec policy groups. An IPSec policy is identified by its name and sequence number and multiple IPSec policies with the same IPSec policy name constitute an IPSec policy group.
Number of policies	Number of IPSec policies.
Policy name	Name and sequence number of an IPSec policy.
Mode	Mode in which an IPSec policy is created: ● isakmp: An IPSec policy is created in IKE negotiation mode. ● template: An IPSec policy is created using an IPSec policy template. ● manual: An IPSec policy is created manually.
ACL	ACL referenced by the IPSec policy.
Peer name	Name of the IKE peer referenced by the IPSec policy.
Local address	Local IP address used in IKE negotiation (Only the manual mode IPSec policies display the local address).
Remote address	Remote IP address used in IKE negotiation (Only the manual mode IPSec policies display the remote address).

View the information about the security policy.

```
<Huawei> display ipsec policy ctrl-plane
==========================================
IPSec policy group: "10"
Using interface: {GigabitEthernet6/0/0}
==========================================
    Policy Alias: map1-10
    Security data flow: 3000
```

```
Peer name    :  rut2
Perfect forward secrecy: None
Proposal name:  prop1
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
SA trigger mode: Traffic-based
Route inject: None
Policy state: Enable
Anti-replay: -
Anti-replay window size: 1024
Fragment before-encryption: Disable
Respond-only: Disable
Policy status  : Inactive
Qos pre-classify: Disable
Qos group: -
```

Table 12-45 Description of the **display ipsec policy ctrl-plane** command output

Item	Description
IPsec policy group	Name of an IPSec policy group.
Using interface	Interface to which the IPSec policy group is applied.
sequence number	sequence number of an IPSec policy.
Security data flow	ACL used by an IPSec policy.
Peer name	IKE peer end used in the IPSec policy.
Perfect forward secrecy	DH group used by the PFS function: ● DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 14: 2014-bit Diffie-Hellman group is used during IKE negotiation. ● None: PFS is not used during IKE negotiation.
Proposal name	IPSec proposal used by an IPSec policy.
IPSec SA local duration(time based)	Time-based IPSec SA duration.
IPSec SA local duration(traffic based)	traffic-based IPSec SA duration.
SA trigger mode	SA trigger mode: ● Automatic. ● Traffic-based.

Route inject	Route injection status: ● Dynamic, Preference: Dynamic route injection is enabled and a priority is configured for the static route generated through route injection. ● Static, Preference: Static route injection is enabled and a priority is configured for the static route generated through route injection. ● None: Route injection is disabled.
Policy state	Policy status: ● Enable. ● Disable.

Anti-replay	Whether the Anti-replay function is enabled.
Anti-replay window size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled.
Fragment before-encryption	IPSec fragment mode: ● Enable: fragment before encryption. ● Disable: Fragment after encryption.
Respond-only	Whether the local end is enabled to initiate IPSec negotiation when an IPSec policy in ISAKMP mode is used to create an IPSec tunnel. ● Enable: The local end functions as the IPSec responder and does not initiate IPSec negotiation. ● Disable: The local end initiates IPSec negotiation.
Policy status	IPSec policy status: ● Active. ● Inactive.
Qos Pre-classify	Pre-extraction of original IP packets.
Qos group	QoS group to which the IPSec packets belong.

12.6.36 display ipsec policy-template (all views)

Function

The **display ipsec policy-template** command displays IPSec policy template information.

Format

display ipsec policy-template [**brief** | **name** *policy-template-name* [*seq-number*]]

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec policy templates.	-
name *policy-template-name*	Displays detailed information about the IPSec policy template with a specified name.	The value must be an existing IPSec policy template name.
seq-number	Displays detailed information about the IPSec policy template with a specified sequence number.	The value must be an existing IPSec policy template sequence number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, this command displays detailed information about all IPSec policy templates.

You can use the **display ipsec policy-template brief** command to check the following brief information about all IPSec policy templates, including:

- Template name and sequence number
- ACL number
- IKE Peer

If **name** is specified, the command displays detailed information about the IPSec policy template. If you specify **name** and do not specify *seq-number*, the command displays detailed information about an IPSec policy template group.

Example

Display brief information about all IPSec policy templates.

```
<Huawei> display ipsec policy-template brief
Number of templates group : 1
Number of templates       : 1

Policy template name     ACL          Peer name
-------------------------------------------------------
temp1-10                 3001/IPv4    rut3
```

Table 12-46 Description of the **display ipsec policy-template brief** command output

Item	Description
Number of templates group	Number of IPSec policy template groups. An IPSec policy template is identified by its name and sequence number. Multiple IPSec policy templates with the same IPSec policy template name constitute an IPSec policy template group.
Number of templates	Number of IPSec policy templates.
Policy template name	Name and sequence number of an IPSec policy template. To configure an IPSec policy template, run the **ipsec policy-template** command.
ACL	ACL referenced in the IPSec policy template. To reference an ACL in an IPSec policy template, run the **security acl** command.
Peer name	Name of the IKE peer referenced in the IPSec policy template. To reference an IKE peer, run the **ike-peer** command.

Display information about a specified IPSec policy template group.

```
<Huawei> display ipsec policy-template name tem3

===============================================
IPSec policy template group: "tem3"
===============================================

  Sequence number: 1
  Policy Alias: tem3-1
  Security data flow: 3001/IPv4
  Peer name    :  zc3
  Perfect forward secrecy: DH group 14
  Proposal name:  3
  IPSec SA local duration(time based): 3600 seconds
  IPSec SA local duration(traffic based): 1843200 kilobytes
  Anti-replay window size: 1024
  Fragment before-encryption: Disable
  Route inject state: -
  Route inject nexthop: -
  Route inject preference: -
  Policy state: Enable
  Qos pre-classify: Enable
```

```
Qos group: -
Sa keep-holding-to hard-duration : Disable
```

Table 12-47 Description of the **display ipsec policy-template name** command output

Item	Description
IPSec policy template group	Name of an IPSec policy template. To configure an IPSec policy template, run the **ipsec policy-template** command.
Sequence number	Sequence number of an IPSec policy template. To configure an IPSec policy template, run the **ipsec policy-template** command.
Policy Alias	Alias of an IPSec policy template. To configure an alias, run the **12.6.2 alias** command.
Security data flow	ACL referenced in the IPSec policy template. To reference an ACL referenced in an IPSec policy template, run the **security acl** command.
Peer name	Name of the IKE peer referenced in the IPSec policy template. To reference an IKE peer, run the **ike-peer** command.
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used in IKE negotiation: • DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. • DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. • DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. • DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. • DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. • DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify an algorithm used to generate a pseudo random number, run the **pfs** command.
Proposal name	Name of an IPSec proposal referenced in the IPSec policy template. To reference an IPSec proposal, run the **proposal** command.
IPSec SA local duration(time based)	Time-based lifetime of the local SA. To set the time-based lifetime of the local SA, run the **sa duration time-based** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec SA local duration(traffic based)	Traffic-based lifetime of the local SA. To set the traffic-based lifetime of the local SA, run the **sa duration traffic-based** command.
Anti-replay window size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **ipsec anti-replay window** command.
Fragment before-encryption	Packet fragmentation mode for an IPSec tunnel: ● Enable: IPSec packets are fragmented before encryption. ● Disable: IPSec packets are fragmented after encryption. To configure a packet fragmentation mode for an IPSec tunnel, run the **12.6.99 ipsec fragmentation before-encryption** command.
Route inject state	Route injection status. Dynamic: Dynamic route injection is enabled To configure route injection, run the **route inject** command.
Route inject nexthop	Next hop of a generated route. To configure route injection, run the **route inject** command.
Route inject preference	Priority of a generated route. To configure route injection, run the **route inject** command.
Policy state	Status of the IPSec policy that references the IPSec policy template: ● Enable: The IPSec policy is enabled. ● Disable: The IPSec policy is disabled. To set an IPSec policy to the state, run the **12.6.125 policy enable** command.
Qos pre-classify	Pre-extraction of original IP packets. To configure pre-extraction of original IP packets, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which the IPSec packets belong. To configure the QoS group, run the **12.6.131 qos group** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Sa keep-holding-to hard-duration	Whether the device deletes the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation. ● Enable: The device will delete the original IPSec SA after the hard lifetime expires. ● Disable: The device deletes the original IPSec SA immediately. To configure the device to delete the original IPSec SA after the hard lifetime expires, run the **12.6.161 sa keep-holding-to hard-duration** command.

12.6.37 display ipsec policy-template ctrl-plane

Function

The **display ipsec policy-template ctrl-plane** command displays information about the IPSec policy template on control plane.

Format

display ipsec policy-template [**brief** | **name** *policy-template-name* [*seq-number*]] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about all the IPSec policy templates.	-
name *policy-template-name*	Specifies the name of an IPSec policy template.	The value is an existing IPSec policy template name.
seq-number	Specifies the sequence number of an IPSec policy template.	The value is an existing IPSec policy template number.

Views

User view

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If the no parameter is not specified, detailed information about all IPSec policy templates is displayed.

If **brief** is specified, you can view the following brief information about the IPSec policy template. In this case, the information is displayed in brief format.

- Template name and sequence number
- ACL number
- IKE Peer

If **name** is specified, the command displays detailed information about the IPSec policy template.

Example

Display information about all the IPSec policy template.

```
<Huawei> display ipsec policy-template brief ctrl-plane
Number of templates group : 1
Number of templates       : 1

Policy template name     ACL          Peer name
-------------------------------------------------------
temp1-10                              rut3
```

Table 12-48 Description of the **display ipsec policy-template brief ctrl-plane** command output

Item	Description
Number of templates group	Number of IPSec policy template groups. An IPSec policy template is identified by its name and sequence number and multiple IPSec policy templates with the same IPSec policy template name constitute an IPSec policy template group.
Number of templates	Number of IPSec policy templates.
Policy template name	Name and sequence number of an IPSec policy template.
ACL	ACL used by an IPSec policy template.
Peer name	IKE peer involved.

Display information about a specified IPSec policy template.

```
<Huawei> display ipsec policy-template name tem3 ctrl-plane

===============================================
IPSec policy template group: "tem3"
===============================================
```

```
Sequence number: 1
Policy Alias: tem3-1
Security data flow: 0
Peer name    :  zc3
Perfect forward secrecy: None
Proposal name:  3
IPSec SA local duration(time based): 3600 seconds
IPSec SA local duration(traffic based): 1843200 kilobytes
Anti-replay: -
Anti-replay window size: 1024
Fragment before-encryption: Disable
Route inject: None
Policy state: Enable
Qos pre-classify: Enable
Qos group: -
```

Table 12-49 Description of the **display ipsec policy-template name tem3 ctrl-plane** command output

Item	Description
IPSec policy template group	Name of an IPSec policy template.
Sequence number	Sequence number in the IPSec policy template.
Policy Alias	Alias of the IPSec policy template.
Security data flow	ACL referenced by the IPSec policy template.
Peer name	Name of the IKE peer referenced by the IPSec policy template.
Perfect forward secrecy	Perfect Forward Secrecy (PFS) used in IKE negotiation: ● DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 14: 2014-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. ● None: PFS is not used during IKE negotiation.
Proposal name	Name of an IPSec proposal referenced by the IPSec policy template.
IPSec SA local duration(time based)	Time-based lifetime of the local SA.

Item	Description
IPSec SA local duration(traffic based)	Traffic-based lifetime of the local SA.
Anti-replay	Whether IPSec anti-replay is enabled in an IPSec policy template: ● Enable: IPSec anti-replay is enabled. ● -: IPSec anti-replay is disabled for an IPSec tunnel. The global IPSec anti-replay function is used.
Anti-replay window size	IPSec anti-replay window size.
Fragment before-encryption	Packet fragmentation mode for an IPSec tunnel: ● Enable: IPSec packets are fragmented before encryption. ● Disable: IPSec packets are fragmented after encryption.
Route inject	Route injection status: ● Dynamic , Preference: Dynamic route injection is enabled and a priority is configured for the route generated through route injection. ● Static , Preference: Dynamic route injection is enabled and a priority is configured for the route generated through route injection. ● None: Route injection is disabled.
Policy state	Status of the IPSec policy that references the IPSec policy template: ● Enable: The IPSec policy is enabled. ● Disable: The IPSec policy is disabled.
Qos Pre-classify	Pre-extraction of original IP packets.
Qos group	QoS group to which the IPSec packets belong.

12.6.38 display ipsec profile (all views)

Function

The **display ipsec profile** command displays IPSec profile information.

Format

display ipsec profile [**brief** | **name** *profile-name*]

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec profiles.	-
name *profile-name*	Displays information about the specified IPSec profile.	The value must be an existing IPSec profile name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, you can view information about all IPSec profiles.

If the **brief** parameter is specified, you can view brief information about all IPSec policies.

If the **name** parameter is specified, you can view detailed information about the specified IPSec policy.

Example

Display brief information about all IPSec profiles.

```
<Huawei> display ipsec profile brief
 Total number of IPSec profile: 1
 Profile name       Peer name
 ---------------------------------
 a                  spub
```

Table 12-50 Description of the **display ipsec profile brief** command output

Item	Description
Total number of IPSec profile	Number of IPSec profiles on a device.
Profile name	Name of an IPSec profile. To configure an IPSec profile, run the **ipsec profile (system view)** command.
Peer name	Name of the IKE peer referenced by the IPSec profile. To reference an IKE peer, run the **ike-peer** command.

Display information about IPSec profile **a**.

```
<Huawei> display ipsec profile name a
=========================================
IPSec profile  : a
Using interface: Tunnel0/0/1
=========================================
 IPSec Profile Name        : a
 Peer Name                 : -
 PFS   Group               : DH group 14
 SecondsFlag               : 0 (0:Global 1:Local)
 SA Life Time Seconds      : 3600
 KilobytesFlag             : 0 (0:Global 1:Local)
 SA Life Kilobytes         : 1843200
 Anti-replay Window Size   : 1024
 Fragment Before-encryption: Disable
 Number of IPSec Proposals : 0
 IPSec Proposals Name      : -
 IKE Identity Name         : identity1
 Qos Pre-classify          : 0 (0:Disable 1:Enable)
 Qos group                 : -
```

Table 12-51 Description of the **display ipsec profile name** command output

Item	Description
IPSec profile	Name of an IPSec profile. To configure an IPSec profile, run the **ipsec profile (system view)** command.
Using interface	Interface to which an IPSec profile is applied.
IPSec Profile Name	Name of an IPSec profile. To configure an IPSec profile, run the **ipsec profile (system view)** command.
Peer Name	Name of the IKE peer referenced by the IPSec profile. To reference an IKE peer, run the **ike-peer** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PFS Group	Perfect Forward Secrecy (PFS) used in IKE negotiation: ● DH group 1: 768-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 2: 1024-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 5: 1536-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 14: 2048-bit Diffie-Hellman group is used during IKE negotiation. ● DH group 19: 256-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 20: 384-bit ECP Diffie-Hellman group is used during IKE negotiation. ● DH group 21: 521-bit ECP Diffie-Hellman group is used during IKE negotiation. To specify the PFS, run the **pfs** command.
SecondsFlag	Flag bit indicating aging of the SA. ● 0: The SA ages based on the time. The flag bit takes effect globally. To configure a global time-based SA lifetime, run the **ipsec sa global-duration time-based** command. ● 1: The SA ages based on the time. The flag bit takes effect in specified views only.
SA Life Time Seconds	Time-based IPSec SA lifetime.
KilobytesFlag	Flag bit indicating aging of the SA. ● 0: The SA ages based on the traffic. The flag bit takes effect globally. To configure a global traffic-based SA lifetime, run the **ipsec sa global-duration traffic-based** command. ● 1: The SA ages based on the traffic.
SA Life Kilobytes	Traffic-based IPSec SA lifetime.
Anti-replay Window Size	IPSec anti-replay window size. This field is valid only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **12.6.5 anti-replay window** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Fragment Before-encryption	Packet fragmentation mode. • Enable: IPSec packets are fragmented before encryption. • Disable: IPSec packets are fragmented after encryption. To configure a packet fragmentation mode, run the **12.6.99 ipsec fragmentation before-encryption** command.
Number of IPSec Proposals	Number of IPSec proposals referenced by an IPSec profile.
IPSec Proposals Name	Name of the referenced IPSec proposal. To configure an IPSec proposal, run the **proposal** command.
IKE Identity Name	Name of the referenced IKE identity. To referenced an IKE identity, run the **match ike-identity** command.
Qos Pre-classify	Pre-extraction of original IP packets. To configure pre-extraction of original IP packets, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which the IPSec packets belong. To configure the QoS group, run the **12.6.131 qos group** command.

12.6.39 display ipsec profile ctrl-plane

Function

The **display ipsec profile ctrl-plane** command displays information about an IPSec profile on the ctrl-plane.

Format

display ipsec profile [**brief** | **name** *profile-name*] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec profiles.	-

Parameter	Description	Value
name *profile-name*	Displays information about the specified IPSec profile.	The value is an existing IPSec profile name.

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, information about all IPSec profiles is displayed.

If the **brief** parameter is specified, you can view brief information about all IPSec policies.

If the **name** parameter is specified, you can view detailed information about the specified IPSec policy.

Example

View information about the **a** IPSec profile.

```
<Huawei> display ipsec profile name a ctrl-plane
=========================================
IPSec profile  : a
Using interface:
=========================================
 IPSec Profile Name        :a
 Peer Name                 :
 PFS   Group               :DH group 14
 SecondsFlag               :0 (0:Global 1:Local)
 SA Life Time Seconds      :3600
 KilobytesFlag             :0 (0:Global 1:Local)
 SA Life Kilobytes         :1843200
 Anti-replay               :-
 Anti-replay Window Size   :1024
 Fragment Before-encryption:Disable
 Number of IPSec Proposals :0
 IPSec Proposals Name      :
 IKE Identity Name         :identity1
 Qos Pre-classify          :0 (0:Disable 1:Enable)
 Qos group                 : -
```

Table 12-52 Description of the **display ipsec profile name a ctrl-plane** command output

Item	Description
IPSec profile	Name of an IPSec profile
Using interface	Interface to which an IPSec profile is applied

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSec Profile Name	Name of an IPSec profile
Peer name	Name of the IKE peer referenced by the IPSec profile.
PFS Group	Perfect Forward Secrecy (PFS) used in IKE negotiation: ● DH group 1: Indicates the 768-bit Diffie-Hellman group during negotiation. ● DH group 2: Indicates the 1024-bit Diffie-Hellman group during negotiation. ● DH group 5: Indicates the 1536-bit Diffie-Hellman group during negotiation. ● DH group 14: Indicates the 2048-bit Diffie-Hellman group during negotiation.
SecondsFlag	Flag bits that the SA ages by time: ● 0: Global configurations aged by time ● 1: Local configurations aged by time
SA Life Time Seconds	Time-based IPSec SA duration.
KilobytesFlag	Flag bits that the SA ages by traffic: ● 0: Global configurations aged by traffic ● 1: Local configurations aged by traffic
SA Life Kilobytes	traffic-based IPSec SA duration.
Anti-replay	Whether the IPSec anti-replay function is enabled.
Anti-replay Window Size	IPSec anti-replay window size. This field is available only when the IPSec anti-replay function is enabled.
Fragment Before-encryption	IPSec fragment mode: ● Enable: fragment before encryption ● Disable: Fragment after encryption
Number of IPSec Proposals	Proposals referenced by the IPSec profile.
IPSec Proposals Name	Name of an IPSec proposal
IKE Identity Name	Name of the referenced IKE identity.
Qos Pre-classify	pre-extraction of original IP packets.
Qos group	QoS group to which the IPSec packets belong.

 Copyright © Huawei Technologies Co., Ltd.

View brief information about all IPSec profiles.

```
<Huawei> display ipsec profile brief ctrl-plane
 Total number of IPSec profile: 1
 Profile name      Peer name
 ---------------------------------
 a                 spub
```

Table 12-53 Description of the **display ipsec profile brief ctrl-plane** command output

Item	Description
Total number of IPSec profile	Number of IPSec profiles on a device
Profile name	Name of an IPSec profile
Peer name	Name of the IKE peer referenced by the IPSec profile.

12.6.40 display ipsec proposal (All views)

Function

The **display ipsec proposal** command displays IPSec proposal information.

Format

display ipsec proposal [**brief** | **name** *proposal-name*]

Parameters

Parameter	Description	Value
brief	Displays brief information about IPSec proposals.	-
name *proposal-name*	Displays detailed information about an IPSec proposal with a specified name.	The value must be an existing IPSec proposal name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipsec proposal** command to view the following information:

- Name of the IPSec proposal
- Encapsulation mode
- Security protocol
- Authentication and encryption algorithms defined in the security protocol

If no parameter is specified, this command displays detailed information about all IPSec proposals.

Example

Display detailed information about all IPSec proposals.

```
<Huawei> display ipsec proposal

Number of proposals: 2

IPSec proposal name: 1
 Encapsulation mode: Tunnel
 Transform          : esp-new
 ESP protocol       : Authentication SHA2-HMAC-256
                      Encryption AES-256

IPSec proposal name: 2
 Encapsulation mode: Tunnel
 Transform          : ah-esp-new
 AH protocol        : Authentication SHA2-HMAC-256
 ESP protocol       : Authentication SHA2-HMAC-256
                      Encryption     AES-256
```

Display brief information about all IPSec proposals.

```
<Huawei> display ipsec proposal brief

Current ipsec proposal number: 5
 -------------------------------------------------------
 Proposal Name     Encapsulation mode    Transform
 -------------------------------------------------------
 1                 Tunnel                esp-new
 2                 Tunnel                ah-esp-new
 3                 Tunnel                ah-esp-new
 4                 Tunnel                esp-new
 prop1               Tunnel                esp-new
```

Table 12-54 Description of the **display ipsec proposal** command output

Item	Description
Number of proposals/Current ipsec proposal number	Current total number of IPSec proposals.
IPSec proposal name/Proposal Name	Name of the IPSec proposal. To configure an IPSec proposal, run the **ipsec proposal** command.

Item	Description
Encapsulation mode	Encapsulation mode in the IPSec proposal, which can be transport or tunnel. To configure an encapsulation mode, run the **12.6.54 encapsulation-mode** command.
Transform	Security protocol in the IPSec proposal. The value can be: ● ah-new ● esp-new ● ah-esp-new To configure a security protocol, run the **12.6.172 transform** command.
ESP protocol	Authentication and encryption algorithms used by ESP. To configure authentication and encryption algorithms, run the **12.6.57 esp authentication-algorithm** and **12.6.59 esp encryption-algorithm** commands.

12.6.41 display ipsec proposal ctrl-plane

Function

The **display ipsec proposal ctrl-plane** command displays information about the IPSec proposal on the ctrl-plane.

Format

display ipsec proposal [**brief** | **name** *proposal-name*] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about the IPSec proposal.	-
name *proposal-name*	Specifies the name of the proposal.	The value is an existing IPSec proposal name.

Views

User view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The output of the **display ipsec proposal ctrl-plane** command is as follows:

- Name of the IPSec proposal
- Adopted encapsulation mode
- Adopted security protocol
- Authentication and encryption algorithms defined in the security protocol

If the name of the IPSec proposal is not specified, all proposals are displayed.

Example

Display detailed information about all IPSec proposals.

```
<Huawei> display ipsec proposal ctrl-plane
Number of proposals: 3

IPSec proposal name: newprop1
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption AES-256

IPSec proposal name: prop1
 Encapsulation mode: Tunnel
 Transform         : ah-new
 AH protocol       : Authentication SHA2-HMAC-256

IPSec proposal name: prop
 Encapsulation mode: Tunnel
 Transform         : esp-new
 ESP protocol      : Authentication SHA2-HMAC-256
                   Encryption AES-256
```

Display brief information about all IPSec proposals.

```
<Huawei> display ipsec proposal brief ctrl-plane
Current ipsec proposal number: 1
-----------------------------------------------------
Proposal Name      Encapsulation mode      Transform
-----------------------------------------------------
prop1              Tunnel                  esp-new
```

Table 12-55 Description of the **display ipsec proposal ctrl-plane** command output

Item	Description
Number of proposals/Current ipsec proposal number	Total number of IPSec proposals in the current system.
IPsec proposal name/Proposal Name	Name of the proposal
Encapsulation mode	Modes used by the proposal, including transport mode and tunnel mode

Item	Description
Transform	Security protocols used by the proposal, including AH and ESP
AH protocol	Authentication and encryption algorithms used by AH
ESP protocol	Authentication and encryption algorithms used by ESP

12.6.42 display ipsec proto-protect proposal

Function

The **display ipsec proto-protect proposal** command displays information about security proposals.

Format

display ipsec proto-protect proposal [**name** *proposal-name*]

Parameters

Parameter	Description	Value
name *proposal-name*	Specifies the name of a security proposal.	The value is a string of 1 to 15 case-insensitive characters.

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

After IPSec is configured, when valid packets are dropped between IPSec peers, you can run the **display ipsec proto-protect proposal** command to check whether the security proposal configurations on both IPSec peers are identical.

IPSec ensures security using the security proposal. You can run the **display ipsec proto-protect proposal** command to view the following information:

- Name of the IPSec security proposal
- Encapsulation mode defined in the security proposal

 Copyright © Huawei Technologies Co., Ltd.

- Security protocol defined in the security proposal
- Authentication and encryption algorithms defined in the security proposal

Example

Display information about all security proposals.

```
<Huawei> display ipsec proto-protect proposal
 Total IP security proposal number: 2

 IP security proposal name: proposal1
   encapsulation mode: transport
   transform: esp-new
   ESP protocol: authentication SHA1-HMAC-96, encryption 256-aes

 IP security proposal name: proposal2
   encapsulation mode: transport
   transform: ah-new
   AH protocol: authentication SHA1-HMAC-96
```

Table 12-56 Description of the **display ipsec proto-protect proposal** command output

Item	Description
Total IP security proposal number	Number of security proposals created
IP security proposal name	Name of a security proposal
encapsulation mode	Encapsulation mode: ● transport ● tunnel **NOTE** Currently only **transport** mode is supported.
transform	Security protocol defined in the security proposal: ● esp-new: specifies the Encapsulating Security Payload (ESP). ● ah-new: specifies the Authentication Header (AH).
ESP protocol	ESP configuration.
AH protocol	AH configuration.

12.6.43 display ipsec proposal (User view)

Function

The **display ipsec proposal** command displays information about the IPSec proposal.

Format

display ipsec proposal [**brief** | **name** *proposal-name*] **ctrl-plane**

Parameters

Parameter	Description	Value
brief	Displays brief information about the IPSec proposal.	-
name *proposal-name*	Specifies the name of the proposal.	The value is an existing IPSec proposal name.
ctrl-plane	Displays information about the IPSec profiles on the ctrl-plane.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

The output of the **display ipsec proposal** command is as follows:

- Name of the IPSec proposal
- Adopted encapsulation mode
- Adopted security protocol
- Authentication and encryption algorithms defined in the security protocol

If the name of the IPSec proposal is not specified, all proposals are displayed.

Example

Display detailed information about all IPSec proposals.

```
<Huawei> display ipsec proposal ctrl-plane

Number of proposals: 2

IPSec proposal name: 1
 Encapsulation mode: Tunnel
 Transform          : esp-new
 ESP protocol       : Authentication SHA2-HMAC-256
                      Encryption AES-256

IPSec proposal name: 2
 Encapsulation mode: Tunnel
 Transform          : ah-esp-new
 AH protocol        : Authentication SHA2-HMAC-256
 ESP protocol       : Authentication SHA2-HMAC-256
                      Encryption     AES-256
```

Display brief information about all IPSec proposals.

```
<Huawei> display ipsec proposal brief ctrl-plane

Current ipsec proposal number: 5
 -------------------------------------------------------
 Proposal Name     Encapsulation mode    Transform
 -------------------------------------------------------
 1                 Tunnel                esp-new
 2                 Tunnel                ah-esp-new
 3                 Tunnel                ah-esp-new
 4                 Tunnel                esp-new
 prop1               Tunnel                esp-new
```

Table 12-57 Description of the **display ipsec proposal** command output

Item	Description
Number of proposals/Current ipsec proposal number	Current total number of IPSec proposals.
IPSec proposal name/Proposal Name	Name of the IPSec proposal. To configure an IPSec proposal, run the **ipsec proposal** command.
Encapsulation mode	Encapsulation mode in the IPSec proposal, which can be transport or tunnel. To configure an encapsulation mode, run the **12.6.54 encapsulation-mode** command.
Transform	Security protocol in the IPSec proposal. The value can be: ● ah-new ● esp-new ● ah-esp-new To configure a security protocol, run the **12.6.172 transform** command.
ESP protocol	Authentication and encryption algorithms used by ESP. To configure authentication and encryption algorithms, run the **12.6.57 esp authentication-algorithm** and **12.6.59 esp encryption-algorithm** commands.

12.6.44 display ipsec sa

Function

The **display ipsec sa** command displays IPSec SA information.

Format

display ipsec sa [**brief** | **duration** | **efficient-vpn** *efficient-vpn-name* | **policy** *policy-name* [*seq-number*] | **profile** *profile-name* | **remote** *ipv4-address*]

Parameters

Parameter	Description	Value
brief	Displays brief information about all IPSec SAs.	-
duration	Displays detailed information about IPSec SAs with specified lifetime.	-
efficient-vpn *efficient-vpn-name*	Displays SA information of an Efficient VPN policy with a specified name.	The value is an existing Efficient VPN policy name.
policy *policy-name*	Displays detailed information about IPSec SAs established using an IPSec policy with a specified name.	The value must be an existing IPSec policy name.
seq-number	Displays detailed information about IPSec SAs established using an IPSec policy with a specified sequence number.	The value must be an existing IPSec policy sequence number.
profile *profile-name*	Displays detailed information about IPSec SAs established using a specified IPSec profile.	The value must be an existing IPSec profile name.
remote *ipv4-address*	Displays detailed information about IPSec SAs with the specified remote IPv4 address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no parameter is specified, detailed information about all IPSec SAs is displayed.

If **duration** is specified, the command displays information about global IPSec SAs with specified time-based or traffic-based lifetime. For details, see the **12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)** command.

Example

Display brief information about all IPSec SAs.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ipsec sa brief
IPSec SA information:

  Src address    Dst address   SPI     VPN   Protocol    Algorithm
-------------------------------------------------------------------------------
  10.3.1.1       10.3.1.10     123456  vrf1  AH          A:SHA2_256_128
  10.3.1.1       10.3.1.10     754321  vrf1  ESP         E:AES-256 A:SHA2_256_128
  10.3.1.10      10.3.1.1      123457  vrf1  ESP         E:AES-256 A:SHA2_256_128
  10.3.1.10      10.3.1.1      654321  vrf1  AH          A:SHA2_256_128

Number of IPSec SA: 4
-------------------------------------------------------------------------------
```

Display information about all IPSec SAs in the IPSec policy mode.

```
<Huawei> display ipsec sa
ipsec sa information:
===============================
Interface: GigabitEthernet2/0/10
===============================
 ----------------------------
  IPSec policy name: "pc2"
  Sequence number  : 1
  Acl group        : 3061
  Acl rule         : 5
  Mode             : Template
  ----------------------------
    Connection ID     : 67108879
    Encapsulation mode: Tunnel
    Holding time      : 0d 0h 4m 29s
    Tunnel local      : 10.0.0.1:500
    Tunnel remote     : 10.0.0.2:500
    Flow source       : 10.0.0.1/255.255.255.255 17/1701
    Flow destination  : 10.0.0.2/255.255.255.255 17/39725
    Flow dscp         : af11

    [Outbound ESP SAs]
      SPI: 4055669516 (0xf1bc9b0c)
      Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 5242880/3355
      Outpacket count       : 0
      Outpacket encap count : 0
      Outpacket drop count  : 0
      Slice Failure: 0
      Max sent sequence-number: 2377
      UDP encapsulation used for NAT traversal: N

    [Inbound ESP SAs]
      SPI: 1050491168 (0x3e9d3920)
      Proposal: ESP-ENCRYPT-3DES-192 SHA2-256-128
      SA remaining key duration (kilobytes/sec): 5242880/3355
      Inpacket count        : 0
      Inpacket decap count  : 0
      Inpacket drop count   : 0
      Authentication Failure: 0
      Replay Failure: 0
      Decrypt Check Failure: 0
      Max received sequence-number: 0
      UDP encapsulation used for NAT traversal: N
      Anti-replay : Enable
      Anti-replay window size: 1024

===============================
Interface: Tunnel0/0/2
===============================

  ----------------------------
  IPSec profile name: "1"
  Mode             : PROF-ISAKMP
  ----------------------------
    Connection ID     : 232
```

```
  Encapsulation mode: Tunnel
  Holding time      : 0d 0h 4m 29s
  Tunnel local      : 3.1.1.1:500
  Tunnel remote     : 2.1.1.1:500
  Flow source       : 10.0.0.1/255.255.255.255 47/0-65535
  Flow destination  : 10.0.0.2/255.255.255.255 47/0-65535

  [Outbound AH SAs]
    SPI: 12306225 (0xbbc731)
    Proposal: AH-SHA2-256-128
    SA remaining key duration (kilobytes/sec): 5242880/3355
    Outpacket count       : 1
    Outpacket encap count : 1
    Outpacket drop count  : 0
    Slice Failure: 0
    Max sent sequence-number: 1
    UDP encapsulation used for NAT traversal: N

  [Inbound AH SAs]
    SPI: 2513644 (0x265aec)
    Proposal: AH-SHA2-256-128
    SA remaining key duration (kilobytes/sec): 5242880/3355
    Inpacket count        : 0
    Inpacket decap count  : 0
    Inpacket drop count   : 0
    Authentication Failure: 0
    Replay Failure: 0
    Decrypt Check Failure: 0
    Max received sequence-number: 0
    UDP encapsulation used for NAT traversal: N
    Anti-replay : Enable
    Anti-replay window size: 1024
```

Table 12-58 Description of the **display ipsec sa** command output

Item	Description
ipsec sa information	Information about the IPSec SA.
Interface	Interface to which the IPSec policy is applied.
IPSec policy name	Name of the IPSec policy. To configure an IPSec policy, run the **ipsec policy (system view)** command.
IPSec profile name	Name of the IPSec profile. To configure an IPSec profile, run the **12.6.108 ipsec profile (system view)** command.
Sequence number	Sequence number of the IPSec policy. To configure an IPSec policy, run the **ipsec policy (system view)** command.
Acl group	ACL number used in the IPSec policy. To configure an ACL referenced by an IPSec policy, run the **security acl** command.
Acl rule	ID of the matched ACL rule. The ACL rule ID is not displayed if the IPSec tunnel is created manually.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Mode in which an IPSec policy is created: ● template: An IPSec policy is created using an IPSec policy template. ● isakmp: An IPSec policy is created in ISAKMP mode. ● manual: An IPSec policy is created manually. To configure an IPSec policy, run the **ipsec policy (system view)** command.
Connection ID	ID of the IPSec SA connection.
Encapsulation mode	Encapsulation mode in an IPSec proposal. **tunnel** indicates that the encapsulation mode is tunnel mode, and **transport** indicates that the encapsulation mode is transport mode. To configure an encapsulation mode, run the **12.6.54 encapsulation-mode** command.
Holding time	Time elapsed since an IPSec tunnel was created.
Tunnel local	IP address and NAT traversal port of the local interface. To configure the IP address and NAT traversal port of the local interface, run the **12.6.174 tunnel local** and **12.6.101 ipsec nat-traversal source-port** command.
Tunnel remote	IP address and NAT traversal port of the remote interface. To configure the IP address and NAT traversal port of the remote interface, run the **12.6.175 tunnel remote**/ **12.6.134 remote-address (IKE peer view)** and **12.6.101 ipsec nat-traversal source-port** command.
Flow source	Source IP address segment of the data flow sent from the local end and the protocol number and port number of the ACL.
Flow destination	Destination IP address segment of the data flow sent from the local end and the protocol number and port number of the ACL.
Flow dscp	DSCP value of the data flow sent from the local end.
Outbound ESP SAs	Outbound IPSec SA information using ESP.
SPI	SPI of an SA. To configure the SPI for the SA created using a manually configured IPSec policy, run the **sa spi** command. The SPI is automatically generated when an IPSec policy is created in IKE negotiation mode.
Proposal	Name of an IPSec proposal referenced by the IPSec policy. To reference an IPSec proposal, run the **proposal** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA remaining key duration (kilobytes/sec)	Hard remaining lifetime of an SA, in kilobytes or seconds. To set the SA lifetime, run the **12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)** command.
Outpacket count	Number of packets that can be encrypted with the IPSec SA.
Outpacket encap count	Number of sent packets that are successfully encrypted.
Outpacket drop count	Number of discarded packets during encryption.
Max sent sequence-number	Maximum sequence number of sent packets. The sequence number increases during communication and is used for anti-replay.
Slice Failure	Number of packets that fail to be fragmented.
UDP encapsulation used for NAT traversal	Whether NAT traversal is enabled: ● Y ● N To enable NAT traversal, run the **nat traversal** command.
Inbound ESP SAs	Inbound IPSec SA information using ESP.
Inpacket count	Number of packets that can be decrypted with the IPSec SA.
Inpacket decap count	Number of received packets that are successfully decrypted.
Inpacket drop count	Number of discarded packets during decryption.
Authentication Failure	Number of packets that fail to be authenticated.
Replay Failure	Number of packets discarded by the anti-replay function.
Decrypt Check Failure	Number of packets discarded because of a failure in IPSec check.
Max received sequence-number	Maximum sequence number of received packets.
Anti-replay	Whether the anti-replay function is enabled for an IPSec tunnel: ● Enable ● disable To configure the anti-replay function for an IPSec tunnel, run the **12.6.92 ipsec anti-replay enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Anti-replay window size	IPSec anti-replay window size. This field is valid only when the IPSec anti-replay function is enabled. To set the IPSec anti-replay window size, run the **12.6.5 anti-replay window** or **12.6.93 ipsec anti-replay window** command.
Src address	IP address of the local interface. To configure the IP address of the local interface, run the **12.6.174 tunnel local** command.
Dst address	IP address of the remote interface. To configure the IP address of the remote interface, run the **12.6.175 tunnel remote** or **12.6.134 remote-address (IKE peer view)** command.
VPN	VPN instance that the IPSec tunnel belongs to. To configure a VPN instance that the IPSec tunnel belongs to, run the **12.6.155 sa binding vpn-instance** command.
Protocol	Security protocol used by the IPSec SA: ● AH: AH is used. ● AH-ESP: AH and ESP are used. ● ESP: ESP is used. To configure a security protocol, run the **12.6.172 transform** command.
Algorithm	Authentication and encryption algorithms used by a security protocol. A indicates the authentication algorithm, and E indicates the encryption algorithm. To configure an authentication algorithm, run the **12.6.3 ah authentication-algorithm** or **12.6.57 esp authentication-algorithm** command. To configure an encryption algorithm, run the **12.6.59 esp encryption-algorithm** command.

12.6.45 display ipsec proto-protect sa

Function

The **display ipsec proto-protect sa** command displays information about a Security Association (SA).

Format

display ipsec proto-protect sa [**name** *sa-name*] [**brief**]

Parameters

Parameter	Description	Value
name *sa-name*	Specifies the SA name.	The value is an existing IPSec Security Association name.
brief	Displays brief information of the SA, such as the SA name and the Security Parameter Index (SPI) value.	-

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

You can run the **display ipsec proto-protect sa** command to check whether the SA configurations for outgoing packets on the local end are identical with those for incoming packets on the peer end. The **display ipsec proto-protect sa** command output displays the following information:

- SA name
- Security proposal applied to the SA
- Number of times the SA is applied
- SA configurations for incoming Authentication Header (AH) packets
- SA configurations for outgoing AH packets
- SA configurations for incoming Encapsulating Security Payload (ESP) packets
- SA configurations for outgoing ESP packets

Example

Display configurations of the SA.

```
<Huawei> display ipsec proto-protect sa
IP security association name: sa1
Number of references: 0
  proposal name: p1
  inbound AH setting:
     AH spi: 267 (0x10b)
     AH string-key:
     AH authentication hex key: %^%#'RCZaI8Z:_E!Q8T!3,AO_OKZ>\U!O]*>(U(9CS9!%^%#
  inbound ESP setting:
     ESP spi: 789 (0x315)
     ESP string-key: DN]I8$];]3+Q=^Q`MAF4<1!!
     ESP encryption hex key:
     ESP authentication hex key:
  outbound AH setting:
     AH spi: 267 (0x10b)
```

```
  AH string-key:
  AH authentication hex key: %^%#'RCZaI8Z:_E!Q8T!3,AO_OKZ>\U!O]*>(U(9CS9!%^%#
outbound ESP setting:
  ESP spi: 789 (0x315)
  ESP string-key: DN]I8$];]3+Q=^Q`MAF4<1!!
  ESP encryption hex key:
  ESP authentication hex key:
```

Table 12-59 Description of the **display ipsec proto-protect sa** command output

Item	Description
IP security association name	SA name
Number of references	Number of times the SA is applied
proposal name	Security proposal applied to the SA
inbound AH setting	SA configurations for incoming AH packets
AH spi	SPI for AH
AH string-key	Authentication key for AH in the string format displayed in cipher text
AH authentication hex key	Authentication key for AH in cipher text
inbound ESP setting	SA configurations for incoming ESP packets
ESP spi	SPI for ESP
ESP string-key	Authentication key for ESP in the string format displayed in cipher text
ESP encryption hex key	Encryption key for ESP in cipher format
ESP authentication hex key	Authentication key for ESP in cipher text
outbound AH setting	SA configurations for outgoing AH packets
outbound ESP setting	SA configurations for outgoing ESP packets

12.6.46 display ipsec statistics

Function

The **display ipsec statistics** command displays IPSec packet statistics.

Format

display ipsec statistics [**tunnel-number**]

Parameters

None.

Parameter	Description	Value
tunnel-number	Displays the number of IPSec tunnels.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display ipsec statistics** command to view IPSec packet statistics, including statistics about incoming or outgoing packets that are protected, statistics about encrypted and decrypted packets, detailed statistics about discarded packets that are protected, and statistics about IKE negotiation related packets. The IPSec packet statistics facilitate IPSec fault diagnosis and maintenance.

Precautions

The **display ipsec statistics** command only displays the number of plaintext bytes.

Example

Display statistics about all IPSec packets.

```
<Huawei> display ipsec statistics
 IPSec statistics information:
 Number of IPSec tunnels: 1
 Number of standby IPSec tunnels: 0
 the security packet statistics:
   input/output security packets: 0/0
   input/output security bytes: 0/0
   input/output dropped security packets: 0/0
   the encrypt packet statistics:
     send chip: 0, recv chip: 0, send err: 0
     local cpu: 0, other cpu: 0, recv other cpu: 0
     intact packet: 0, first slice: 0, after slice: 0
   the decrypt packet statistics:
     send chip: 0, recv chip: 0, send err: 0
     local cpu: 0, other cpu: 0, recv other cpu: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
    reass  first slice: 0, after slice: 0
  dropped security packet detail:
    can not find SA: 0, wrong SA: 0
    authentication: 0, replay: 0
    front recheck: 0, after recheck: 0
    change cpu enc: 0, dec change cpu: 0
    fib search: 0, output l3: 0
    flow err: 0, slice err: 0, byte limit: 0
  negotiate about packet statistics:
    IKE fwd packet ok: 0, err: 0
    IKE ctrl packet inbound ok: 0, outbound ok: 0
    SoftExpr: 0, HardExpr: 0, DPDOper: 0
    trigger ok: 0, switch sa: 0, sync sa: 0
    recv IKE nat keepalive: 0, IKE input: 0
```

Display the number of IPSec tunnels.

```
<Huawei> display ipsec statistics tunnel-number
  IPSec tunnel totals: 0
  IPSec tunnel specifications: 4000
```

Table 12-60 Description of the **display ipsec statistics** command output

Item	Description
IPSec statistics information	Statistics about IPSec packets.
Number of IPSec tunnels	Number of the IPSec tunnels.
Number of standby IPSec tunnels	Number of the standby IPSec tunnels.
the security packet statistics	Statistics about packets that are protected.
input/output security packets	Number of incoming or outgoing packets that are protected.
input/output security bytes	Number of incoming or outgoing bytes that are protected.
input/output dropped security packets	Number of discarded incoming or outgoing packets that are protected.
the encrypt packet statistics	Statistics about encrypted packets.
send chip	Number of packets sent to the hardware for encryption and decryption.
recv chip	Number of packets encrypted and decrypted by hardware.
send err	Number of packets that fail to be sent to hardware for encryption and decryption.
local cpu	Number of packets encrypted and decrypted by the local CPU.
other cpu	Number of packets forwarded to another CPU for encryption and decryption.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
recv other cpu	Number of packets received from another CPU for encryption and decryption.
intact packet	Number of non-fragmented encrypted packets.
first slice	Number of initial fragmented packets.
after slice	Number of non-initial fragmented packets.
the decrypt packet statistics	Statistics about decrypted packets.
reass first slice	Number of initial packets that are reassembled.
after slice	Number of non-initial packets that are reassembled.
dropped security packet detail	Detailed statistics about discarded packets that are protected.
can not find SA	Number of packets for which SAs are not found.
wrong SA	Number of packets with invalid SAs.
authentication	Number of packets that fail to be authenticated.
replay	Number of discarded packets due to replay check.
front recheck	Number of discarded packets due to IPSec pre-check.
after recheck	Number of discarded packets due to IPSec post-check.
change cpu enc	Number of encrypted packets that fail to be forwarded.
dec change cpu	Number of decrypted packets that fail to be forwarded.
fib search	Number of encrypted packets that are discarded due to route searching failure.
output l3	Number of encrypted packets that fail to be sent.
flow err	Number of packets discarded because negotiation is triggered.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
slice err	Number of IPSec packets that fail to be fragmented.
byte limit	Number of discarded packets due to traffic limit.
negotiate about packet statistics	Statistics about IKE negotiation packets.
IKE fwd packet ok	Number of IKE packets sent to the IKE process.
err	Number of IKE packets that fail to be sent to the IKE process.
IKE ctrl packet inbound ok	Number of IKE packets received by the control plane.
outbound ok	Number of IKE packets sent by the control plane.
SoftExpr	Number of traffic soft timeouts.
HardExpr	Number of traffic hard timeouts.
DPDOper	Number of times DPD is performed in on-demand DPD mode.
trigger ok	Number of times that negotiation is triggered.
switch sa	Number of times the local device receives data encrypted with the new SA and instructs the IKE process to replace the SA.
sync sa	Number of times the active device notifies the IKE process that the SA triplet (remote address, SPI, protocol ID) does not exist on the standby device.
recv IKE nat keepalive	Number of received IKE nat keepalive packets.
IKE input	Number of received IKE packets.
IPSec tunnel totals	Number of IPSec tunnels.
IPSec tunnel specifications	IPSec tunnel specifications.

Related Topics

12.6.144 reset ipsec statistics

12.6.47 display ipsec statistics route

Function

The **display ipsec statistics route** command displays IPSec route injection statistics.

Format

display ipsec statistics route

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

In an IPSec route injection scenario, you can run the **display ipsec statistics route** command to view IPSec route injection statistics for fault location.

Example

Display IPSec route injection statistics.

```
<Huawei> display ipsec statistics route
IPSec route statistics information:

Route add                    send:1          receive:1
Route del                    send:0          receive:0
Route syn                    send:674        receive:674
Route syn  round             send:674        receive:674
Route syn                    add :0          del    :0
Route send to route module    add :2          del    :1
Route send to ipsec module    add :1          del    :0
Route msg ipc send error          :0
Route msg process error           :0
Route add:
  dest addr equal with peer addr          :0
  add no memery                           :0
  same route same slot                    :0
  same route diff slot or interface down  :1
  cpu not exist                           :0
  vrf invalid                             :0
Route del:
  route not exist                         :0
  not delete state                        :0
  same route send by other slot           :0

HA data
Route HA send num                         :675
```

```
Route HA receive num                :0
Route HA send error num              :0
```

Table 12-61 Description of the **display ipsec statistics route** command output

Item	Description
IPSec route statistics information	IPSec route statistics.
Route add	Routes are added from the LPU to MPU: ● send: indicates the number of routes sent by the LPU. ● receive: indicates the number of routes received by the MPU.
Route del	Routes are deleted by the LPU from the MPU: ● send: indicates the number of routes sent by the LPU. ● receive: indicates the number of routes received by the MPU.
Route syn	Routes are synchronized by the LPU with the MPU: ● send: indicates the number of routes sent by the LPU. ● receive: indicates the number of routes received by the MPU. ● add: indicates the number of routes added by the MPU because routes do not exist. ● del: indicates the number of routes deleted by the MPU due to residual routing entries.
Route syn round	Number of times the LPU synchronizes routes with the MPU: ● send: indicates the number of times the LPU sends routes to the MPU. ● receive: indicates the number of times the MPU receives routes from the LPU.
Route send to route module	Routes are added to or deleted from the routing module: ● add: indicates the number of added routes. ● del: indicates the number of deleted routes.
Route send to ipsec module	Routes are added to or deleted from the IPSec module: ● add: indicates the number of added routes. ● del: indicates the number of deleted routes.
Route msg ipc send error	Number of times IPC fails to send routing information.
Route msg process error	Number of times the LPU fails to process routing information.
Route add	Added routes.

Item	Description
dest addr equal with peer addr	Number of times the route destination address is consistent with the peer address specified in intelligent path selection during route addition.
add no memery	Number of failures to apply for memory during route addition.
same route same slot	Number of times the same slot has the same routes during route addition.
same route diff slot or interface down	Number of times boards in different slots have the same routes or have interfaces in Down state during route addition.
cpu not exist	Number of times the CPU does not exist during route addition.
vrf invalid	Number of times the VPN instance becomes invalid during route addition.
Route del	Deleted routes.
route not exist	Number of routes that do not exist during route deletion.
not delete state	Number of routes that do not exist in the routing table during route deletion.
same route send by other slot	Number of the same routes that boards in other slots send to the MPU during route deletion.
HA data	Active/standby backup data.
Route HA send num	Number of routes sent by the active device during active/standby backup.
Route HA receive num	Number of routes received by the standby device during active/standby backup.
Route HA send error num	Number of routes that fail to be sent by the active device during active/standby backup.

12.6.48 display ipsec proto-protect statistics

Function

Using the **display ipsec proto-protect statistics** command, you can view the statistics about packets processed by IPSec.

Format

display ipsec proto-protect statistics [**sa-name** *sa-name*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing IPSec Security Association name.

Views

All views

Default Level

1: Monitoring Level

Usage Guidelines

Usage Scenario

After IPSec protection is configured for a routing protocol, you can run the **display ipsec proto-protect statistics** command to view information about transmitted packets and dropped packets. The details are as follows:

- Number of received and sent packets
- Number of received and sent bytes
- Number of dropped incoming and outgoing packets
- Detailed information about dropped packets

Example

Display statistics about packets processed by IPSec.

```
<Huawei> display ipsec proto-protect statistics
  IPv6 security packet statistics:
    input/output security packets: 0/0
    input/output security bytes: 0/0
    input/output dropped security packets: 0/0
    dropped security packet detail:
      memory process problem: 0
      can't find SA: 0
      queue is full: 0
      authentication is failed: 0
      wrong length: 0
      replay packet: 0
      too long packet: 0
      invalid SA: 0
      policy deny: 0
  the normal packet statistics:
    input/output dropped normal packets: 0/0

  IPv4 security packet statistics:
    input/output security packets: 0/0
    input/output security bytes: 0/0
    input/output dropped security packets: 0/0
    dropped security packet detail:
      memory process problem: 0
      can't find SA: 0
      queue is full: 0
      authentication is failed: 0
      wrong length: 0
```

```
    replay packet: 0
    too long packet: 0
    invalid SA: 0
    policy deny: 0
the normal packet statistics:
  input/output dropped normal packets: 0/0
```

Table 12-62 Description of the **display ipsec proto-protect statistics** command output

Item	Description
input/output security packets	Indicates the number of received and sent packets
input/output security bytes	Indicates the number of received and sent bytes
input/output dropped security packets	Indicates the number of dropped incoming and outgoing packets
dropped security packet detail	Detailed information about dropped packets
memory process problem	Indicates the number of packets that are dropped due to a memory fault
can't find SA	Indicates the number of packets that are dropped because no SA is found
queue is full	Indicates the number of packets that are dropped because the queue is full
authentication is failed	Indicates the number of packets that are dropped due to authentication failure
wrong length	Indicates the number of packets that are dropped due to a packet length fault
replay packet	Indicates the number of packets that are dropped due to repeated transmission
too long packet	Indicates the number of packets that are dropped due to excess packet length
invalid SA	Indicates the number of packets that are dropped due to an invalid SA
policy deny	Indicates the number of packets that are dropped due to a deny action in the policy
the normal packet statistics	Statistics about normal packets
input/output dropped normal packets	Indicates the number of received/sent normal packets that are dropped

 Copyright © Huawei Technologies Co., Ltd.

12.6.49 dn

Function

The **dn** command specifies the distinguished name (DN) of an allowed peer for IKE negotiation.

The **undo dn** command deletes the DN of an allowed peer.

By default, no DN of allowed peer for IKE negotiation is configured.

Format

dn *name*

undo dn *name*

Parameters

Parameter	Description	Value
name	Specifies the DN of an allowed peer for IKE negotiation.	The value is a string of 1 to 255 case-sensitive characters without spaces.

Views

Identity filter set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify an allowed peer based on the DN (PKI domain configuration referenced in the IKE peer configured on a remote device) in the identity filter set for IKE negotiation.

Precautions

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

If you run this command in the same view multiple times, the latest configuration does not override earlier ones.

Example

Set the name of the allowed peer for IKE negotiation to **huawei**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] dn c=cn,st=jiangsu,l=nanjing,o=huawei,ou=vpn,cn=ipsec
```

Related Topics

12.6.70 ike identity

12.6.50 dpd

Function

The **dpd** command configures the dead peer detection (DPD) idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on the specified IKE peer.

The **undo dpd** command restores the default DPD idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on the specified IKE peer.

By default, the DPD idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on an IKE peer are 30s, 15s, and 3 respectively.

Format

dpd { **idle-time** *interval* | **retransmit-interval** *interval* | **retry-limit** *times* }

undo dpd { **idle-time** | **retransmit-interval** | **retry-limit** }

Parameters

Parameter	Description	Value
idle-time *interval*	Specifies the DPD idle time.	The value is an integer that ranges from 10 to 3600, in seconds.
retransmit-interval *interval*	Specifies the DPD packet retransmission interval.	The value is an integer that ranges from 2 to 60, in seconds.
retry-limit *times*	Specifies the maximum number of DPD packet retransmissions.	The value is an integer that ranges from 3 to 10.

Views

IKE peer view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When peers implement IPSec communication, the heartbeat mechanism can detect peer faults to avoid traffic loss. However, the periodic heartbeat message exchanges consume CPU resources on the two ends. The DPD mechanism enables a device to send DPD messages for peer detection only when the device does not receive IPSec packets from the peer within a period. This mechanism can detect peer faults and save CPU resources.

The device sets the DPD mode and enables the DPD function based on the **dpd type** command. Two DPD modes are available:

- On-demand DPD

  When the local end needs to send IPSec packets to the remote end, the local end sends a DPD request packet to the remote end for DPD detection.
- Periodic DPD

  If the local end does not receive IPSec packets or a DPD request packet from the remote end after the DPD idle time expires, it periodically sends a DPD request packet to the remote end.

The local end retransmits DPD request packets if it does not receive any DPD response packet from the remote end within the retransmission interval. If the local end still does not receive any DPD response packet within the retransmission interval after the maximum number of retransmissions is reached, the local end considers that the remote end is offline and deletes the involved IKE SA and IPSec SA.

Precautions

- The **dpd** command must be used with the **dpd type** and **dpd msg** commands.
- Parameters in the **dpd** command can be configured for each IKE peer separately and do not need to be the same as the parameters on the peer device.

Example

Set the DPD idle time, DPD packet retransmission interval, and maximum number of DPD packet retransmissions on the IKE peer **test** to 300s, 10s, and 4.

```
<Huawei> system-view
[Huawei] ike peer test
[Huawei-ike-peer-test] dpd idle-time 300
[Huawei-ike-peer-test] dpd retransmit-interval 10
[Huawei-ike-peer-test] dpd retry-limit 4
```

Related Topics

12.6.51 dpd msg

12.6.52 dpd type

12.6.75 ike peer

12.6.51 dpd msg

Function

The **dpd msg** command configures the payload sequence of DPD packets on the specified IKE peer.

The **undo dpd msg** command restores the default payload sequence of DPD packets on the specified IKE peer.

By default, the payload sequence of DPD packets on an IKE peer is **seq-notify-hash**.

Format

dpd msg { **seq-hash-notify** | **seq-notify-hash** }

undo dpd msg

Parameters

Parameter	Description	Value
seq-hash-notify	Indicates that in a DPD packet, the hash payload is before the notify payload.	-
seq-notify-hash	Indicates that in a DPD packet, the notify payload is before the hash payload.	-

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

DPD packets carrying the notify payload and hash payload are exchanged bidirectionally. The notify payload sent by the initiator carries an R-U-THERE message equivalent to a Hello packet, and the notify payload sent by the responder carries an R-U-THERE-ACK message equivalent to an ACK packet.

The payload sequence of DPD packets sent by different devices may be different. IKE peers on both ends must send DPD packets with the same payload sequence; otherwise, DPD does not take effect. You can use the **dpd msg** command to set the same payload sequence of DPD packets on the two ends.

Precautions

This command applies only when an IKE peer uses IKEv1.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the payload sequence of DPD packets to **hash-notify** on the IKE peer **huawei**.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] dpd msg seq-hash-notify
```

Related Topics

12.6.52 dpd type
12.6.34 display ipsec policy (all views)
12.6.36 display ipsec policy-template (all views)
12.6.38 display ipsec profile (all views)
12.6.30 display ipsec efficient-vpn

12.6.52 dpd type

Function

The **dpd type** command configures the DPD mode on an IKE peer.

The **undo dpd type** command deletes the DPD mode on an IKE peer.

By default, the DPD mode is not configured on an IKE peer.

Format

dpd type { **on-demand** | **periodic** }

undo dpd type

Parameters

Parameter	Description	Value
on-demand	Configures on-demand DPD.	-
periodic	Configures periodic DPD.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When peers implement IPSec communication, the heartbeat mechanism can detect peer faults to avoid traffic loss. However, the periodic heartbeat message exchanges consume CPU resources on the two ends. The DPD mechanism enables a device to send DPD messages for peer detection only when the device does not receive IPSec packets from the peer within a period. This mechanism can detect peer faults and save CPU resources.

The device sets the DPD mode and enables the DPD function based on the **dpd type** command. Two DPD modes are available:

- On-demand DPD

  When the local end needs to send IPSec packets to the remote end, the local end sends a DPD request packet to the remote end for DPD detection.
- Periodic DPD

  If the local end does not receive IPSec packets or a DPD request packet from the remote end after the DPD idle time expires, it periodically sends a DPD request packet to the remote end.

The local end retransmits DPD request packets if it does not receive any DPD response packet from the remote end within the retransmission interval. If the local end still does not receive any DPD response packet within the retransmission interval after the maximum number of retransmissions is reached, the local end considers that the remote end is offline and deletes the involved IKE SA and IPSec SA.

Precautions

The sequence of the payload in DPD packets configured on IKE peers using the **dpd msg** command must be the same. Otherwise, DPD does not take effect.

When multiple branches are connected to the headquarters, you are advised not to set the DPD mode of the headquarters to periodic detection. This is because an IPSec tunnel will frequently flap, causing high CPU usage, if the network is unstable. You are advised to set the DPD mode of the headquarters to on-demand detection or not to configure the DPD mode.

Example

Configure on-demand DPD.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] dpd type on-demand
```

Related Topics

12.6.50 dpd
12.6.51 dpd msg
12.6.75 ike peer

12.6.53 dscp

Function

The **dscp** command sets the DSCP priority of IKE packets on a specified IKE peer.

The **undo dscp** command cancels the DSCP priority configuration.

By default, the DSCP priority of IKE packets on a specified IKE peer is 0.

Format

dscp *dscp-value*

undo dscp

Parameters

Parameter	Description	Value
dscp-value	Specifies the DSCP priority of IKE packets.	The value can be an integer or a string of characters. That is, the value can be an integer that ranges from 0 to 63, or a string of AF11 to AF13, AF21 to AF23, AF31 to AF33, AF41 to AF43, CS1 to CS7, EF, or default.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IKE packets are used for IKE SA and IPSec SA negotiation or DPD. When IKE packets are lost during transmission, IPSec SAs may fail to be negotiated. As a result, packets that need to be protected by IPSec are not protected. The DSCP priority of IKE packets can be improved so that IKE packets are processed preferentially. IKE packet transmission reliability is therefore improved.

To configure the DSCP priority for IKE packets of an IKE peer, run this command.

Precautions

The DSCP priority of IKE packets can be configured in the IKE peer view or system view. The system preferentially uses the DSCP priority configured in the IKE peer view. If the DSCP priority is not configured in the IKE peer view, the system uses the global DSCP priority.

Example

Set the DSCP priority of IKE packets to CS2 for the IKE peer **ik1**.

```
<Huawei> system-view
[Huawei] ike peer ik1
[Huawei-ike-peer-ik1] dscp cs2
```

 Copyright © Huawei Technologies Co., Ltd.

12.6.54 encapsulation-mode

Function

The **encapsulation-mode** command sets the IPSec encapsulation mode.

The **undo encapsulation-mode** command restores the default IPSec encapsulation mode.

By default, the tunnel mode is used.

Format

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

Parameters

Parameter	Description	Value
transport	Encapsulates IP packets in transport mode.	-
tunnel	Encapsulates IP packets in tunnel mode.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec encapsulates IP packets by adding an AH or ESP header and ESP tail to original IP packets for authentication and encryption. The following two IPSec encapsulation modes are available:

- Tunnel mode

  In tunnel mode, IPSec adds a new IP header to an IP packet. The source and destination addresses of the new IP header are the IP addresses of two ends of a tunnel. The tunnel mode is more secure than the transport mode. In terms of performance, the tunnel mode consumes more bandwidth than the transport mode.

  The tunnel mode is often used between two security gateways. The packets encrypted by one security gateway can only be decrypted by the other security gateway.
- Transport mode

  In transport mode, IPSec does not add a new header to an IP packet. The source and destination addresses of the original packet are the IP addresses of

 Copyright © Huawei Technologies Co., Ltd.

two ends of a tunnel. In transport mode, the two devices that encrypt and decrypt packets must be the original packet sender and final receiver respectively.

Since most data traffic between two security gateways is not communication traffic of the two gateways, the transport mode is not used between security gateways. The transport mode is suited for the communication between two hosts or between a host and a security gateway; however, the transport mode is not recommended because it provides low security.

Precautions

The two IPSec tunnel ends must use the same encapsulation mode.

When IKEv2 is used, the encapsulation mode in all the IPSec proposals configured on the IKE negotiation initiator must be the same; otherwise, IKE negotiation fails.

Example

Set the IPSec encapsulation mode to the transport mode.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] encapsulation-mode transport
```

12.6.55 encapsulation-mode (ipsec-proto-protect-proposal view)

Function

The **encapsulation-mode** command sets the encapsulation mode for IP packets.

The **undo encapsulation-mode** command restores the default encapsulation mode for IP packets.

By default, the encapsulation mode is set to **tunnel**.

Format

encapsulation-mode { **transport** | **tunnel** }

undo encapsulation-mode

Parameters

Parameter	Description	Value
transport	Sets the encapsulation mode to **transport**.	-
tunnel	Sets the encapsulation mode to **tunnel**.	-

Views

IPSec proto-protect proposal view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure Authentication Header (AH) or Encapsulating Security Payload (ESP) to ensure security based on data confidentiality. If AH is configured, an AH header is generated; if ESP is configured, an ESP header, an ESP tail, and an ESP authentication field are generated. Two encapsulation modes are available for IPSec: transport and tunnel.

- The transport mode is applicable to a scenario in which two hosts, or a host and a security gateway (such as a gateway workstation and a router), are communicating with each other. In transport mode, the two devices encrypting and decrypting packets must be the original packet sender and the final receiver, respectively.
- The tunnel mode is generally applied to a scenario in which two security gateways (routers) are communicating with each other. The packets that are encrypted on the local security gateway can be decrypted only on the peer security gateway. Therefore, an IP packet must be encapsulated using the tunnel mode and an IP header embed. After arriving at the peer security gateway, the IP packet can be decrypted.

Precautions

The encapsulation modes on both IPSec peers must be identical.

Example

Set the encapsulation mode to **transport** in the security proposal named **prop2**.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop2
[Huawei-ipsec-proto-protect-proposal-prop2] encapsulation-mode transport
```

12.6.56 encryption-algorithm

Function

The **encryption-algorithm** command configures an encryption algorithm for IKE negotiation.

The **undo encryption-algorithm** command restores the default configuration.

By default, the AES-256 encryption algorithm is used for IKE negotiation.

Format

encryption-algorithm { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }

undo encryption-algorithm

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
des	Configures the 56-bit Data Encryption Standard (DES) algorithm in Cipher Block Chaining (CBC) mode.	-
3des	Configures the 168-bit Triple Data Encryption Standard (3DES) algorithm in CBC mode.	-
aes-128	Configures the 128-bit AES algorithm in CBC mode.	-
aes-192	Configures the 192-bit AES algorithm in CBC mode.	-
aes-256	Configures the 256-bit AES algorithm in CBC mode.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

The following encryption algorithms used in IKE proposals are listed in descending order of security level: **aes-256** > **aes-192** > **aes-128** > **3des** > **des**.

NOTE

The **3des** and **des** algorithms provide low security and so are not recommended.

Example

Set the AES-192 algorithm for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] encryption-algorithm aes-192
```

12.6.57 esp authentication-algorithm

Function

The **esp authentication-algorithm** command configures the Encapsulating Security Payload (ESP) authentication algorithm.

The **undo esp authentication-algorithm** command configures ESP not to authenticate packets.

By default, the ESP authentication algorithm is Secure Hash Algorithm SHA2-256.

Format

esp authentication-algorithm { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

 Copyright © Huawei Technologies Co., Ltd.

undo esp authentication-algorithm

Parameters

Parameter	Description	Value
md5	Specifies MD5 as the ESP authentication algorithm.	-
sha1	Specifies SHA1 as the ESP authentication algorithm.	-
sha2-256	Specifies SHA2-256 as the ESP authentication algorithm.	-
sha2-384	Specifies SHA2-384 as the ESP authentication algorithm.	-
sha2-512	Specifies SHA2-512 as the ESP authentication algorithm.	-

NOTE

AR100&AR120 series, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S, AR169W, AR169W-P-M9, AR169RW-P-M9, AR169EW, AR169EGW-L, AR1220C, AR1220-8GE, AR2204-27GE, AR2204E-D-27GE, AR2204-24GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2204XE, and AR2204XE-DC do not support SHA2-384 and SHA2-512 authentication algorithms.

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ESP supports the following encryption and authentication modes: both, encryption-only, authentication-only, and none. In the efficient VPN scenario, do not configure encryption or authentication algorithm for ESP when the remote device does not support IPSec encryption or authentication.

NOTE

When ESP is not used to encrypt or authenticate packets, the IKEV2 version of the IPSec tunnel cannot be established.

Prerequisites

esp or **ah-esp** has been specified in the **transform** command.

Precautions

ESP authentication algorithms in the IPSec proposals referenced in the IPSec policies configured at both ends of an IPSec tunnel must be the same.

 Copyright © Huawei Technologies Co., Ltd.

The **undo esp authentication-algorithm** command sets the ESP authentication algorithm to blank (non-authentication) and takes effect only when an ESP authentication algorithm has been specified.

The following algorithms are listed in descending order of security level: **sha2-512** > **sha2-384** > **sha2-256** > **sha1** > **md5**.

The **sha2-256**, **sha2-384**, and **sha2-512** algorithms are recommended for security purposes. The **md5** and **sha1** algorithms are not recommended.

Example

Set ESP and SHA2-256 in the IPSec proposal **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform esp
[Huawei-ipsec-proposal-newprop1] esp authentication-algorithm sha2-256
```

Related Topics

12.6.40 display ipsec proposal (All views)

12.6.58 esp authentication-algorithm (ipsec-proto-protect-proposal view)

Function

The **esp authentication-algorithm** command configures the authentication algorithm for Encapsulating Security Payload (ESP).

The **undo esp authentication-algorithm** command cancels the authentication algorithm for ESP.

By default, the authentication algorithm SHA2-256 is used for ESP.

Format

esp authentication-algorithm { **md5** | **sha1** | **sha2-256** }

undo esp authentication-algorithm

Parameters

Parameter	Description	Value
md5	Indicates that the authentication algorithm MD5 is used for ESP. **NOTE** To ensure high security, do not use the MD5 algorithm as the ESP authentication algorithm.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sha1	Indicates that the authentication algorithm Secure Hash Algorithm-1 (SHA-1) is used for ESP. **NOTE** To ensure high security, do not use the SHA-1 algorithm as the ESP authentication algorithm.	-
sha2-256	Indicates the authentication algorithm SHA-2 256 is used for ESP.	-

Views

IPSec proto-protect proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec can use Authentication Header (AH) or ESP to authenticate packets, preventing packets from being intercepted or modified. When ESP is used, the authentication and encryption algorithms must be configured. You can run the **transform** command to configure AH or ESP. When ESP is used, you can run the **esp authentication-algorithm** command to specify an authentication algorithm for ESP.

ESP currently supports MD5, SHA-1 and SHA2-256 authentication algorithms.

- MD5: generates a 128-bit message summary for an input message of any length.
- SHA-1: generates a 160-bit message summary for an input message of less than 2^{64} bits.
- SHA2-256: generates a 256-bit message summary for an input message of less than 2^{64} bits

MD5 is faster than SHA-1, but is less secure.

NOTE

The **undo esp authentication-algorithm** command functions differently from the **undo ah authentication-algorithm** command. The **undo esp authentication-algorithm** command configures ESP not to authenticate packets, whereas the **undo ah authentication-algorithm** command restores the default authentication algorithm for AH.

Prerequisite

IPSec ensures security using AH or ESP. An authentication algorithm can be configured only after AH or ESP is specified. Therefore, you can configure an ESP authentication algorithm only after running the **transform** command to specify ESP.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The encryption algorithm and authentication algorithm cannot be both set to **NULL** for ESP.

The authentication algorithms on both IPSec peers must be identical.

Example

Set the authentication algorithm to SHA-1 for ESP.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform esp
[Huawei-ipsec-proto-protect-proposal-prop1] esp authentication-algorithm sha1
```

12.6.59 esp encryption-algorithm

Function

The **esp encryption-algorithm** command configures the ESP encryption algorithm.

The **undo esp encryption-algorithm** command sets the ESP encryption algorithm to blank (non-encryption).

By default, the ESP encryption algorithm is Advanced Encryption Standard AES-256.

Format

esp encryption-algorithm { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }

undo esp encryption-algorithm

Parameters

Parameter	Description	Value
des	Configures the 56-bit Data Encryption Standard (DES) algorithm in Cipher Block Chaining (CBC) mode.	-
3des	Configures the 168-bit Triple Data Encryption Standard (3DES) algorithm in CBC mode.	-
aes-128	Configures the 128-bit AES algorithm in CBC mode.	-
aes-192	Configures the 192-bit AES algorithm in CBC mode.	-
aes-256	Configures the 256-bit AES algorithm in CBC mode.	-

Views

IPSec proposal view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ESP supports the following encryption and authentication modes: both, encryption-only, authentication-only, and none. In the efficient VPN scenario, do not configure encryption or authentication algorithm for ESP when the remote device does not support IPSec encryption or authentication.

NOTE

When ESP is not used to encrypt or authenticate packets, the IKEV2 version of the IPSec tunnel cannot be established.

Prerequisites

esp or **ah-esp** has been specified in the **transform** command.

Precautions

ESP encryption algorithms in the IPSec proposals referenced in the IPSec policies configured at both ends of an IPSec tunnel must be the same.

The **undo esp encryption-algorithm** command sets the ESP encryption algorithm to blank (non-encryption) and takes effect only when an ESP encryption algorithm has been specified.

The following encryption algorithms are listed in descending order of security level: **aes-256** > **aes-192** > **aes-128** > **3des** > **des**.

The **aes-256**, **aes-192**, and **aes-128** algorithms are recommended for security purposes. The **3des** and **des** algorithms are not recommended.

Example

Set ESP and AES-128 in the IPSec proposal **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform esp
[Huawei-ipsec-proposal-newprop1] esp encryption-algorithm aes-128
```

Related Topics

12.6.40 display ipsec proposal (All views)

12.6.60 esp encryption-algorithm (ipsec-proto-protect-proposal view)

Function

The **esp encryption-algorithm** command configures the encryption algorithm for Encapsulating Security Payload (ESP).

The **undo esp encryption-algorithm** command configures ESP not to encrypt packets.

By default, the encryption algorithm AES 128 is used for ESP.

Format

esp encryption-algorithm { **des** | **3des** | **aes** [**128** | **192** | **256**] }

undo esp encryption-algorithm

Parameters

Parameter	Description	Value
des	Indicates that ESP uses DES algorithm to encrypt packets. To ensure high security, do not use the DES algorithm as the ESP encryption algorithm.	-
3des	Indicates that ESP uses 3DES algorithm to encrypt packets.	-
aes	Indicates that ESP uses Advanced Encryption Standard (AES) algorithm to encrypt packets. By default, If 128, 192 and 256 are not configured, AES 128 bits algorithm is used for ESP to encrypt packets.	-
128	Indicates that ESP uses AES 128 bits algorithm to encrypt packets.	-
192	Indicates that ESP uses AES 192 bits algorithm to encrypt packets.	-
256	Indicates that ESP uses AES 256 bits algorithm to encrypt packets.	-

Views

IPSec proto-protect proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec uses authentication and encryption algorithms to protect IP packet transmission, preventing packets from being intercepted or modified. Therefore, specify an encryption algorithm before using ESP to ensure security.

 Copyright © Huawei Technologies Co., Ltd.

- DES: uses a 56-bit key to encrypt a 64-bit packet in plain text.
- 3DES: uses three 56-bit keys (in effect, a 168-bit key) to encrypt a packet in plain text.
- AES: uses 128, 192, 256-bit keys respectively to encrypt a packet in plain text.

3DES is CPU incentive and encrypts packets slowly, but provides a more secure service than DES. AES is more secure and performance is also better than 3DES.

Prerequisite

You can configure an encryption algorithm only after ESP is used.

Precautions

The **undo esp encryption-algorithm** command does not restore the default encryption algorithm but configures ESP not to encrypt packets.

The encryption algorithm and authentication algorithm cannot be both set to **NULL** for ESP.

The encryption algorithms on both IPSec peers must be identical.

NOTE

You cannot setup a peer with ESP encryption algorithm configuration.

Example

Set the encryption algorithm to 3DES for ESP.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform esp
[Huawei-ipsec-proto-protect-proposal-prop1] esp encryption-algorithm 3des
```

Set the encryption algorithm to AES 128 bits for ESP.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform esp
[Huawei-ipsec-proto-protect-proposal-prop1] esp encryption-algorithm aes 128
```

12.6.61 exchange-mode

Function

The **exchange-mode** command configures the IKEv1 phase 1 negotiation mode.

The **undo exchange-mode** command restores the default IKEv1 phase 1 negotiation mode.

By default, the main mode is used.

Format

exchange-mode { **aggressive** | **main** }

undo exchange-mode

Parameters

Parameter	Description	Value
aggressive	Configures the aggressive mode.	-
main	Configures the main mode.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Two key exchange and negotiation modes are defined in IKEv1 phase 1:

- In main mode, key exchange information is separated from identity and authentication information to protect identity information.
- In aggressive mode, only three messages are exchanged. Therefore, IKE SAs can be set up more quickly in aggressive mode. However, the first two messages exchanged in aggressive mode are not encrypted, and identity authentication is transmitted in plain text. This brings security risks.

When selecting a negotiation mode, you can determine the main or aggressive mode based on network requirements:

- In the scenario where multiple pre-shared keys are configured in the IKE user table, if the IP address of the negotiation initiator is unknown or unstable and the two ends expect to set up SAs using the pre-shared key, only the aggressive mode can be used.
- If the initiator knows the policy of the responder, IKE SAs can be set up more quickly in aggressive mode.

Example

Configure the aggressive IKE negotiation mode for the IKE peer **peer1**.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] exchange-mode aggressive
```

Related Topics

12.6.20 display ike peer (all views)

12.6.62 fqdn

Function

The **fqdn** command specifies the name of an allowed peer for IKE negotiation.

The **undo fqdn** command deletes the name of an allowed peer.

By default, no name of allowed peer for IKE negotiation is configured.

Format

fqdn *fqdn-name*

undo fqdn *fqdn-name*

Parameters

Parameter	Description	Value
fqdn-name	Specifies the name of an allowed peer.	The value is a string of 1 to 255 case-sensitive characters without spaces.

Views

Identity filter set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify an allowed peer based on the name (configured on a remote device using the **ike local-name** command) in the identity filter set for IKE negotiation.

Precautions

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

If you run this command in the same view multiple times, the latest configuration does not override earlier ones.

Example

Set the name of the allowed peer for IKE negotiation to **huawei**.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] fqdn huawei
```

Related Topics

12.6.70 ike identity

12.6.71 ike local-name

 Copyright © Huawei Technologies Co., Ltd.

12.6.63 id-type

Function

The **id-type** command configures the IKE user ID type and ID.

The **undo id-type** command deletes the IKE user ID type and ID.

By default, the IKE user ID type and ID are not configured.

Format

id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ipv4-address* | **user-fqdn** *remote-user-fqdn* }

undo id-type

Parameters

Parameter	Description	Value
any *any-id*	Indicates that the remote ID type of an IKE peer can be any type and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).
fqdn *remote-fqdn*	Uses the name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).
ip *ipv4-address*	Uses the IPv4 address as the remote ID of an IKE peer and configures the remote ID.	The value is in dotted decimal notation.
user-fqdn *remote-user-fqdn*	Uses the domain name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters, an IPSec policy is created using an IPSec policy template, and the VPN gateway receives IPSec connection setup requests of different branches. When the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak. To prevent this problem, you are advised to run the **id-type** and **pre-shared-key** commands in the view of the IKE user in the IKE user table.

An IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references an IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys.

Precautions

- After an IKE peer references an IKE user table, the ID configured using this command can be used to find required resources, for example, the pre-shared key can be found based on the configured ID.
- When IKEv1 in main mode and pre-shared key authentication is used, the value of **id-type** must be set to **ip**. In NAT traversal scenarios, *ipv4-address* should be set to the IP address that is translated using NAT.

Example

Configure the IKE user ID type and ID.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] id-type ip 1.1.1.1
```

Related Topics

12.6.127 pre-shared-key (IKE user view)

12.6.137 remote-id-type

12.6.136 remote-id

12.6.27 display ike user-table (all views)

12.6.64 ike call admission limit in-negotiation-sa

Function

The **ike call admission limit in-negotiation-sa** command specifies the maximum number of IKE SAs waiting in a queue.

The **undo ike call admission limit in-negotiation-sa** command restores the default maximum number of IKE SAs waiting in a queue.

By default, the maximum number of IKE SAs waiting in a queue is 800 on a CPU.

Format

ike call admission limit in-negotiation-sa *limit-value*

 Copyright © Huawei Technologies Co., Ltd.

undo ike call admission limit in-negotiation-sa

Parameters

Parameter	Description	Value
limit-value	Specifies the maximum number of IKE SAs waiting in a queue.	The value is an integer that ranges from 1 to 800.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the maximum number of IKE SAs waiting in a queue to defend against DOS attacks.

Example

Set the maximum number of IKE SAs waiting in a queue to 100.

```
<Huawei> system-view
[Huawei] ike call admission limit in-negotiation-sa 100
```

12.6.65 ike certificate-check disable

Function

The **ike certificate-check disable** command disables validity verification on certificates of all IKE peers.

The **undo ike certificate-check disable** command restores the default configuration.

By default, the device verifies certificates of all IKE peers.

Format

ike certificate-check disable

undo ike certificate-check disable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IPSec uses certificate authentication, users cannot update certificates after they become invalid, leading to unavailable certificates and IPSec authentication failure. If users still want to use these invalid certificates, run the **ike certificate-check disable** command to disable validity verification on certificates of all IKE peers. If users only want to disable validity verification on certificates of a specified IKE peer, run the **12.6.9 certificate-check disable** command.

Precautions

Disabling validity verification on certificates will lead to security risks.

Example

Configure the device not to verify certificates of all IKE peers.

```
<Huawei> system-view
[Huawei] ike certificate-check disable
```

Related Topics

12.6.17 display ike global config

12.6.66 ike dscp

Function

The **ike dscp** command sets a global DSCP priority of IKE packets.

The **undo ike dscp** command cancels the DSCP priority configuration.

By default, the global DSCP priority of IKE packets is 0.

Format

ike dscp *dscp-value*

undo ike dscp

Parameters

Parameter	Description	Value
dscp-value	Specifies the global DSCP priority of IKE packets.	The value can be an integer or a string of characters. That is, the value can be an integer that ranges from 0 to 63, or a string of AF11 to AF13, AF21 to AF23, AF31 to AF33, AF41 to AF43, CS1 to CS7, EF, or default.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IKE packets are used for IKE SA and IPSec SA negotiation or DPD. When IKE packets are lost during transmission, IPSec SAs may fail to be negotiated. As a result, packets that need to be protected by IPSec are not protected. The DSCP priority of IKE packets can be improved so that IKE packets are processed preferentially. IKE packet transmission reliability is therefore improved.

To configure the DSCP priority for IKE packets of all IKE peers, run this command.

Precautions

The DSCP priority of IKE packets can be configured in the IKE peer view or system view. The system preferentially uses the DSCP priority configured in the IKE peer view. If the DSCP priority is not configured in the IKE peer view, the system uses the global DSCP priority.

Example

Set a global DSCP priority of IKE packets to CS2.

```
<Huawei> system-view
[Huawei] ike dscp cs2
```

12.6.67 ike heartbeat

Function

The **ike heartbeat** command sets heartbeat parameters.

The **undo ike heartbeat** command restores the default configuration.

By default, a heartbeat packet uses old type sequence number mechanism and does not carry the SPI list.

Format

ike heartbeat { **seq-num** { **new** | **old** } | **spi-list** }

undo ike heartbeat { **seq-num** | **spi-list** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
seq-num { **new** | **old** }	Configures the sequence number mechanism for heartbeat packets. ● **new**: The sequence number mechanism conforms to draft-ietf-ipsec-heartbeats-00.txt. ● **old**: The sequence number mechanism conforms to the standard that before draft-ietf-ipsec-heartbeats-00.txt emerges.	-
spi-list	Configures heartbeat packets to carry the SPI list.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In IPSec communication, if the local end becomes faulty and the remote end does not detect the fault because of system failures, the remote end still sends IPSec packets to the local end, causing traffic loss. Heartbeat detection solves this problem. After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status.

Precautions

The two ends must use the same heartbeat parameters.

If you run the **ike heartbeat** { **seq-num** { **new** | **old** } | **spi-list** } command multiple times, only the latest configuration takes effect.

Example

Configure the sequence number mechanism for heartbeat packets to **new**.

```
<Huawei> system-view
[Huawei] ike heartbeat seq-num new
```

12.6.68 ike heartbeat-timer interval

Function

The **ike heartbeat-timer interval** command sets the interval for sending heartbeat packets through an IKE SA.

The **undo ike heartbeat-timer interval** command cancels the configuration.

By default, an IKE SA does not send heartbeat packets.

Format

ike heartbeat-timer interval *interval*

undo ike heartbeat-timer interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending heartbeat packets through an IKE SA.	The value is an integer that ranges from 20 to 28800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status. This command sets the interval for sending heartbeat packets through an IKE SA.

The interval at which heartbeat packets are sent (configured using the **ike heartbeat-timer timeout** command) at the local end must be used with the

timeout interval of heartbeat packets (configured using the **ike heartbeat-timer timeout** command) at the remote end. If the remote end does not receive any heartbeat packet within the timeout interval, it deletes the IKE SA with a timeout tag along with its corresponding IPSec SA. If the IKE SA does not have a timeout tag, it is marked as timeout.

Precautions

When the **ike heartbeat-timer interval** command is configured at one end, the **ike heartbeat-timer timeout** command must be used at the other end.

The timeout interval of heartbeat packets must be longer than the interval at which heartbeat packets are sent. On a network, packet loss seldom occurs more than three consecutive times. Therefore, it is recommended that the timeout interval of heartbeat packets be three times the interval at which heartbeat packets are sent.

Example

Set the interval for sending heartbeat packets to 20 seconds.

```
<Huawei> system-view
[Huawei] ike heartbeat-timer interval 20
```

12.6.69 ike heartbeat-timer timeout

Function

The **ike heartbeat-timer timeout** command sets the timeout interval during which an IKE SA waits for a heartbeat packet.

The **undo ike heartbeat-timer timeout** command cancels the configuration.

By default, the timeout interval during which an IKE SA waits for a heartbeat packet is not configured.

Format

ike heartbeat-timer timeout *seconds*

undo ike heartbeat-timer timeout

Parameters

Parameter	Description	Value
seconds	Specifies the timeout interval during which an IKE SA waits for a heartbeat packet.	The value is an integer that ranges from 30 to 28800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After heartbeat detection is enabled, the local end periodically sends detection packets to the remote end. If the remote end does not receive packets after the heartbeat timer expires, the remote end considers the local end faulty. IKE can send heartbeat packets to detect IKE peer faults and maintain the IKE SA link status. This command sets the timeout interval during which an IKE SA waits for a heartbeat packet.

Precautions

When the **ike heartbeat-timer interval** command is configured at one end, the **ike heartbeat-timer timeout** command must be used at the other end.

The timeout interval of heartbeat packets must be longer than the interval at which heartbeat packets are sent. On a network, packet loss seldom occurs more than three consecutive times. Therefore, it is recommended that the timeout interval of heartbeat packets be three times the interval at which heartbeat packets are sent.

Example

Set the timeout interval during which an IKE SA waits for a heartbeat packet to 60 seconds.

```
<Huawei> system-view
[Huawei] ike heartbeat-timer timeout 60
```

12.6.70 ike identity

Function

The **ike identity** command creates an identity filter set and enter the identity filter set view.

The **undo ike identity** command deletes an identity filter set.

By default, no identity filter set is configured.

Format

ike identity *identity-name*

undo ike identity *identity-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
identity-name	Specifies the name of the identity filter set.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to control user access. The remote peer parameters defined in an identity filter set include the name, DN, IP address of the peer. Only initiators that match the identity filter set can establish an IPSec tunnel with the device, improving access security.

Follow-up Procedure

Configure an allowed peer in the identity filter set view and reference this identity filter set with **match ike-identity** command in the policy template view or IPSec profile view.

Precautions

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

Example

Configure an identity filter set named **identity1**.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1]
```

Related Topics

12.6.121 match ike-identity

12.6.71 ike local-name

Function

The **ike local-name** command configures the local name for IKE negotiation.

The **undo ike local-name** command deletes the local name for IKE negotiation.

By default, no local name is configured for IKE negotiation.

Format

ike local-name *local-name*

undo ike local-name

Parameters

Parameter	Description	Value
local-name	Specifies a local name for IKE negotiation.	The value is a string of 1 to 255 case-sensitive characters without question marks (?).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When identity authentication, If the ID type of an IKE peer is domain name, fully qualified domain name (FQDN), or USER-FQDN, the IKE peer uses the name for identity authentication. You can use the following methods to configure the local name:

- Run the **local-id** command in the IKE peer view. After this command is used, only the IKE peer uses the configured name for identity authentication.
- Run the **local-id** command in the system view. After this command is used, all IKE peers use the configured name for identity authentication.

The local name configured using the **local-id** command has a higher priority than that configured using the **ike local-name** command.

Example

Set the local ID for IKE negotiation to **Huawei**.

```
<Huawei> system-view
[Huawei] ike local-name Huawei
```

12.6.72 ike nat-keepalive-timer interval

Function

The **ike nat-keepalive-timer interval** command configures the interval for sending NAT Keepalive packets.

The **undo ike nat-keepalive-timer interval** command restores the default setting.

By default, the interval for sending NAT Keepalive packets is 20 seconds.

Format

ike nat-keepalive-timer interval *interval*

undo ike nat-keepalive-timer interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for sending NAT Keepalive packets.	The value is an integer that ranges from 5 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an NAT gateway exists between two IKE peers, to prevent NAT entries from being aged, the device on the private network side of the NAT gateway sends NAT Keepalive packets to its peer at a certain interval to maintain the NAT session.

Prerequisites

NAT traversal has been enabled using the **nat traversal** command.

Example

Configure the interval for sending NAT Keepalive packets to 30 seconds.

```
<Huawei> system-view
[Huawei] ike nat-keepalive-timer interval 30
```

12.6.73 ike sm-encryption-key-length enable

Function

The **ike sm-encryption-key-length enable** command enables IKE negotiation packets to carry the SM encryption key length.

The **undo ike sm-encryption-key-length enable** command disables IKE negotiation packets from carrying the SM encryption key length.

By default, IKE negotiation packets do not carry the SM encryption key length.

Format

ike sm-encryption-key-length enable

undo ike sm-encryption-key-length enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a digital envelop is used for IKE negotiation, the negotiation fails if packets sent by the initiator carry the SM encryption key length but the responder cannot process the SM encryption key length. To solve this problem, run the **undo ike sm-encryption-key-length enable** command on the IKE initiator to disable IKE negotiation packets from carrying the SM encryption key length.

Example

Enable IKE negotiation packets to carry the SM encryption key length.

```
<Huawei> system-view
[Huawei] ike sm-encryption-key-length enable
```

Related Topics

12.6.17 display ike global config

12.6.74 ike user-table

Function

The **ike user-table** command creates an IKE user table and displays the IKE user table view, or directly displays the view of an existing IKE user table.

The **undo ike user-table** command deletes an IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

By default, no IKE user table is configured.

Format

ike user-table *user-table-id*

undo ike user-table *user-table-id*

Parameters

Parameter	Description	Value
user-table-id	Specifies the ID of an IKE user table.	The value is an integer and the value range depends on device types. ● AR120&150&160&200 series: 1 to 7. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204E: 1 to 200. ● AR2220, AR2240 (using SRU40 or SRU60), AR2240C, AR3200 (using SRU40 or SRU60) series: 1 to 400. ● AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100, SRU200, SRU200E or SRU400), AR3200 (using SRU80, SRU100, SRU200, SRU200E or SRU400), AR3600 (using SRUX5) series: 1 to 600.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters, an IPSec policy is created using an IPSec policy template, and the VPN gateway receives IPSec connection setup requests of different branches. Some parameters (for example, pre-shared key and VPN instance) of IKE peers are configured on the headquarters gateway that connect to branch gateways, and the parameters are used by all branches. In this case, services of branches cannot be distinguished, and there are even security risks. When the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak.

You are advised to configure an IKE user table to prevent this problem. The IKE user table records the mapping between remote IDs of IKE peers and other parameters. After an IKE peer references the IKE user table, the device searches for the parameters matching the remote ID of the IKE peer in the IKE user table during IKE negotiation. By doing this, branches use different services.

Follow-up Procedure

Run the **12.6.179 user-table** command in the IKE peer view to reference the IKE user table.

Precautions

The IKE user table that has been referenced by an IKE peer cannot be deleted.

Example

Create an IKE user table **10** and enter its view.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10]
```

Related Topics

12.6.179 user-table

12.6.27 display ike user-table (all views)

12.6.75 ike peer

Function

The **ike peer** command creates an IKE peer and displays the IKE peer view.

The **undo ike peer** command deletes the specified IKE peer.

By default, no IKE peer is configured.

Format

ike peer *peer-name*

undo ike peer *peer-name*

Parameters

Parameter	Description	Value
peer-name	Specifies the name of an IKE peer.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **ike peer** command to enter the IKE peer view and then define all parameters for the IKE peer, including:

- Negotiation mode
- ID type
- NAT traversal
- Pre-shared key
- Remote address
- Peer name

Follow-up Procedure

Run the **ike-peer** command to reference the IKE peer.

Example

Create an IKE peer named **peer1** and enter the IKE peer view.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1]
```

12.6.76 ike proposal

Function

The **ike proposal** command creates an IKE proposal and displays the IKE proposal view.

The **undo ike proposal** command deletes the IKE proposal.

By default, an IKE proposal **Default** with the lowest priority is available.

Table 12-63 describes the default configuration of an IKE proposal.

 Copyright © Huawei Technologies Co., Ltd.

Table 12-63 Default configurations of an IKE proposal

Parameter	Default Configuration
Authentication method	Pre-shared key authentication
Encryption algorithm	AES-256
Diffie-Hellman (DH) group parameter	DH14
IKE SA lifetime	86400 seconds
IKEv1 authentication algorithm	SHA2-256
IKEv2 pseudo-random function algorithm	SHA2-256
IKEv2 integrity function algorithm	SHA2-256

Format

ike proposal *proposal-number*

ike proposal default

undo ike proposal *proposal-number*

Parameters

Parameter	Description	Value
proposal-number	Specifies the number of an IKE proposal. A smaller value indicates a higher priority.	The value is an integer that ranges from 1 to 99.
default	Specifies the default IKE proposal.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An IKE proposal is a component of an IKE peer and defines IKE negotiation parameters, including the encryption algorithm, authentication method, authentication algorithm, DH group, and SA lifetime.

A smaller IKE proposal number indicates a higher priority. You can create multiple IKE proposals with different priorities. The negotiation succeeds if any IKE proposal is matched.

 Copyright © Huawei Technologies Co., Ltd.

You can configure multiple IKE proposals for each IKE peer. The proposals will be tried in descending order of security level until a matching proposal is found. During an IKE negotiation, the initiator sends its IKE proposal to the remote end, and the remote end uses its IKE proposals starting from the highest priority to match the received proposal before a match is found. The matched IKE proposal will be used to create an IKE IPSec tunnel.

The negotiation mode of an IKE proposal varies depending on the IKE negotiation mode:

- Main mode

  In main mode, if an IKE proposal is specified in the IKE peer that initiates IKE negotiation, only the specified IKE proposal is sent during IKE negotiation. The responder searches for only the IKE proposal matching with that specified by the initiator. If such IKE proposal cannot be found, the negotiation fails.

  If no IKE proposal is specified in the IKE peer that initiates IKE negotiation, all IKE proposals are sent during IKE negotiation. The responder searches for the IKE proposals matching with these proposals sent by the initiator one by one.
- Aggressive mode

  In aggressive mode, if an IKE proposal is specified in the IKE peer that initiates IKE negotiation, the case is the same as that in main mode.

  If no IKE proposal is specified in the IKE peer that initiates IKE negotiation, only the default IKE proposal is sent during IKE negotiation. The responder also matches this IKE proposal with the default IKE proposal.

Follow-up Procedure

Run the **ike-proposal** command in the IKE peer view to reference the IKE proposal.

Example

Configure IKE proposal 10 and enter the IKE proposal view.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10]
```

12.6.77 ike-peer

Function

The **ike-peer** command references an IKE peer in an IPSec policy.

The **undo ike-peer** command cancels the configuration.

By default, no IKE peer is referenced.

Format

ike-peer *peer-name*

undo ike-peer

Parameters

Parameter	Description	Value
peer-name	Specifies the name of the referenced IKE peer.	The value is an existing IKE peer name.

Views

ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure IKE negotiation, you need to reference an IKE peer in the specified view.

The remote IP address of the IKE peer referenced in an IPSec policy must be unique. You are recommended to configure the remote address range of the IKE peer in an IPSec policy template.

Prerequisites

An IKE peer has been created using the **ike peer** command.

Follow-up Procedure

Run the **12.6.78 ike-proposal** command to reference a configured IKE proposal and run the **12.6.134 remote-address (IKE peer view)** command to configure the remote address or domain name.

Example

Reference the IKE peer **peer1** in the IPSec policy **policy1**.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] ike-peer peer1
```

Reference the IKE peer **peer1** in the IPSec profile **profile1**.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] ike-peer peer1
```

12.6.78 ike-proposal

Function

The **ike-proposal** command configures an IKE proposal for an IKE peer.

The **undo ike-proposal** command cancels the configuration.

By default, an IKE peer does not reference an IKE proposal.

Format

ike-proposal *proposal-number*

undo ike-proposal

Parameters

Parameter	Description	Value
proposal-number	Specifies the number of the IKE proposal to be used. A smaller value indicates a higher priority.	The value is an integer that ranges from 1 to 99.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Configure an IKE proposal using the **ike proposal** command before using this command.

IKE proposal negotiation complies with the following principles:

- If a configured IKE proposal is referenced in the IKE peer view, only the referenced proposal is sent during IKE negotiation, and the responder searches its IKE proposals for a match. If no match is found, the negotiation fails.
- If no IKE proposal is referenced in the IKE peer view (for example, pre-shared and certificate authentication modes are both supported), within the device specifications, a maximum 255 IKE proposals can be carried for IKE negotiation. The responder searches its IKE proposals for a match.

Example

Configure IKE peer **peer1** to reference an IKE proposal **10**.

```
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] ike-proposal 10
```

12.6.79 ikev1 phase1-phase2 sa dependent

Function

The **ikev1 phase1-phase2 sa dependent** command enables dependency between IPSec SA and IKE SA during IKEv1 negotiation.

The **undo ikev1 phase1-phase2 sa dependent** command cancels dependency between IPSec SA and IKE SA during IKEv1 negotiation.

By default, no dependency exists between IPSec SA and IKE SA during IKEv1 negotiation.

Format

ikev1 phase1-phase2 sa dependent

undo ikev1 phase1-phase2 sa dependent

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During IKEv1 negotiation, an IKE SA is established during phase 1, and an IPSec SA is established during phase 2. By default, no dependency exists between IPSec SA and IKE SA, that is, the two SAs can be deleted separately. If the IKE SA is deleted but the corresponding IPSec SA still exists, traffic forwarding will be effected. To prevent this problem, you can run this command to enable dependency between IPSec SA and IKE SA.

Example

Enable dependency between IPSec SA and IKE SA during IKEv1 negotiation.

```
<Huawei> system-view
[Huawei] ikev1 phase1-phase2 sa dependent
```

12.6.80 ikev2 authentication sign-hash

Function

The **ikev2 authentication sign-hash** command configures the certificate signature algorithm used by IKEv2.

The **undo ikev2 authentication sign-hash** command restores the default configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, the certificate signature algorithm used by IKEv2 is SHA2-256.

NOTE

Only V200R010C10 and later version support this command.

Format

ikev2 authentication sign-hash { **md5** | **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo ikev2 authentication sign-hash

Parameters

Parameter	Description	Value
md5	Specifies the certificate signature algorithm as MD5.	-
sha1	Specifies the certificate signature algorithm as SHA1.	-
sha2-256	Specifies the certificate signature algorithm as SHA2-256.	-
sha2-384	Specifies the certificate signature algorithm as SHA2-384.	-
sha2-512	Specifies the certificate signature algorithm as SHA2-512.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an IKEv2 certificate authentication scenario, if the device functions as the sender, it uses the configured algorithm to sign the certificate. If the decryption algorithm used by the receiver is different from that used by the sender, the signature verification of the receiver fails. As a result, IKEv2 negotiation between the two ends fails. If the device functions as the receiver, it searches for a matching algorithm to verify the signature of packets. The device searches for the matching algorithm in the following sequence: **sha2-256** algorithm, configured algorithm, and then other algorithms. If no matching algorithm is found, the signature verification fails, and IKEv2 negotiation between the two ends fails. To prevent this problem, ensure that the certificate signature algorithms used on the two ends are the same.

Precautions

The following certificate signature algorithms are listed in descending order of security level: **sha2-512**, **sha2-384**, **sha2-256**, **sha1**, and **md5**.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the certificate signature algorithm used by IKEv2 as SHA2-256.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] ikev2 authentication sign-hash sha2-256
```

12.6.81 ikev2 cookie-challenge

Function

The **ikev2 cookie-challenge** command sets the maximum number of half-open connections allowed by IKEv2.

The **undo ikev2 cookie-challenge** command restores the default setting.

By default, the maximum number of half-open connections allowed by IKEv2 is 25000.

Format

ikev2 cookie-challenge *number*

undo ikev2 cookie-challenge

Parameters

Parameter	Description	Value
number	Specifies the maximum number of half-open connections allowed by IKEv2.	The value is an integer that ranges from 1 to 1000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

IKEv2 initial exchange messages are transmitted in plaintext. If an attack forges massive IKE_INIT_SA requests, the resources of the responder will be exhausted, causing DoS attacks.

Cookie exchange is defined in IKEv2. After receiving the first message from the sender, the responder replies an unprotected notify payload. In follow-up communications, the responder accepts only the IKE negotiation initiated by the sender of cookie-carrying notify payloads.

You can run this command for the device to determine whether and when to enable attack defense.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the device to start attack defense when the number of half-open connections allowed by IKEv2 exceeds 200.

```
<Huawei> system-view
[Huawei] ikev2 cookie-challenge 200
```

12.6.82 ikev2 initial-contact enable

Function

The **ikev2 initial-contact enable** command enables the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

The **undo ikev2 initial-contact enable** command disables the device from sending the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

By default, the device is disabled to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

Format

ikev2 initial-contact enable

undo ikev2 initial-contact enable

Parameters

None

Views

System View

Default Level

2: Configuration level

Usage Guidelines

The INITIAL_CONTACT notify payload asserts that an IKE SA is the only active IKE SA between a pair of IKE peers. By default, the device will delete the old IKE SA without the INITIAL_CONTACT notify payload after the new IKE SA is created. When the remote end requires the INITIAL_CONTACT notify payload to delete the old IKE SA, configure this command.

When the local device restarts or expects to use the current IKE SA for establishing an IPSec tunnel only, run this command to enable the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request so that the remote device deletes the old IKE SA.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the device to send the INITIAL_CONTACT notify payload in the first IKE_AUTH request.

```
<Huawei> system-view
[Huawei] ikev2 initial-contact enable
```

12.6.83 ikev2 id-match-certificate enable

Function

The **ikev2 id-match-certificate enable** command enables the device to check certificate identity information of the remote device during IKEv2 certificate negotiation.

The **undo ikev2 id-match-certificate enable** command disables the device from checking certificate identity information of the remote device during IKEv2 certificate negotiation.

By default, the device does not check certificate identity information of the remote device during IKEv2 certificate negotiation.

Format

ikev2 id-match-certificate enable

undo ikev2 id-match-certificate enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device does not check certificate identity information of the remote device, such as the IP address, fully qualified domain name (FQDN), and email during IKEv2 certificate negotiation. If the certificate of a branch gateway is used by another device, it can establish an IPSec tunnel with the headquarters, causing security risks.

To prevent security risks, you can run the **ikev2 id-match-certificate enable** command to enable the local device to check certificate identity information of the remote device. If the information differs from the ID (IP address, FQDN, or User-FQDN) of the remote device, IKEv2 negotiation fails.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

You can run the **19.17.28 display pki certificate** command to view certificate identity information. The Subject field in the certificate corresponds to the DN, and the email corresponds to the User-FQDN.

Example

Enable the device to check certificate identity information of the remote device during IKEv2 certificate negotiation.

```
<Huawei> system-view
[Huawei] ikev2 id-match-certificate enable
```

12.6.84 ikev2 prf aes-xcbc-128 compatible

Function

The **ikev2 prf aes-xcbc-128 compatible** command configures the IKEv2 PRF AES-XCBC-128 algorithm as a non-standard RFC algorithm.

The **undo ikev2 prf aes-xcbc-128 compatible** command restores the default configuration.

By default, the IKEv2 PRF AES-XCBC-128 algorithm is a standard RFC algorithm.

NOTE

This command is supported in V200R010C10 and later versions.

Format

ikev2 prf aes-xcbc-128 compatible

undo ikev2 prf aes-xcbc-128 compatible

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device is connected to a device running V200R007 or an earlier version, if both ends use the IKEv2 PRF AES-XCBC-128 algorithm, run the **ikev2 prf aes-xcbc-128 compatible** command on the local device to configure the IKEv2 PRF AES-XCBC-128 algorithm as a non-standard RFC algorithm. Otherwise, the two ends cannot establish an IPSec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the IKEv2 PRF AES-XCBC-128 algorithm as a non-standard RFC algorithm.

```
<Huawei> system-view
[Huawei] ikev2 prf aes-xcbc-128 compatible
```

12.6.85 inband crl

Function

The **inband crl** command configures the device to validate the remote certificate based on the CRL sent from the remote device when IKEv2 uses RSA signature authentication.

The **undo inband crl** command restores the default configuration.

By default, the device does not validate the remote certificate based on the CRL sent from the remote device when IKEv2 uses RSA signature authentication.

Format

inband crl

undo inband crl

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IKEv2 uses RSA signature authentication and the CRL is used for certificate validation, if the CA server is located in the private network of the headquarters, the branch cannot directly communicate with the CA server to obtain the CRL. As a result, the branch cannot use the latest CRL to validate the certificate in the headquarters. To enable the branch to obtain the CRL of the headquarters through IKEv2, run the **inband crl** command on the branch. After receiving the CRL sent from the headquarters through IKEv2, the branch uses this CRL to validate the certificate in the headquarters. If the certificate is not in the CRL, the certificate is considered valid and identity authentication succeeds. The branch can negotiate with the headquarters to establish an IPSec tunnel.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

When you run both the **inband crl** and **12.6.86 inband ocsp** commands, the certificate is considered valid only when it passes the validity check in both OCSP and CRL modes.

The IKEv2 protocol defines the payload length as 2 bytes (that is, the maximum length is 65535). Therefore, when the CRL length exceeds 65535, IKEv2 cannot construct the CRL payload. As a result, the certificate validity check fails.

Example

Configure the device to validate the remote certificate based on the CRL sent from the remote device when IKEv2 uses RSA signature authentication.

```
<Huawei> system-view
[Huawei] ike peer mypeer
[Huawei-ike-peer-mypeer] version 2
[Huawei-ike-peer-mypeer] inband crl
```

12.6.86 inband ocsp

Function

The **inband ocsp** command configures the device to validate the remote certificate based on the OCSP validation result sent from the remote device when IKEv2 uses RSA signature authentication.

The **undo inband ocsp** command restores the default configuration.

By default, the device does not validate the remote certificate based on the OCSP validation result sent from the remote device when IKEv2 uses RSA signature authentication.

Format

inband ocsp

undo inband ocsp

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

When IKEv2 uses RSA signature authentication and OCSP is used for certificate validation, if the OCSP server is located in the private network of the headquarters, the branch cannot directly communicate with the OCSP server to

validate the certificate in the headquarters. To enable the branch to obtain the OCSP validation result of the headquarters through IKEv2, run the **inband ocsp** command on the branch. After receiving the OCSP validation result sent from the headquarters through IKEv2, the branch uses the OCSP validation result to validate the certificate in the headquarters. If the OCSP validation result is valid, the certificate is considered valid and identity authentication succeeds. The branch can negotiate with the headquarters to establish an IPSec tunnel.

When you run both the **inband ocsp** and **12.6.85 inband crl** commands, the certificate is considered valid only when it passes the validity check in both OCSP and CRL modes.

Example

Configure the device to validate the remote certificate based on the OCSP validation result sent from the remote device when IKEv2 uses RSA signature authentication.

```
<Huawei> system-view
[Huawei] ike peer mypeer
[Huawei-ike-peer-mypeer] version 2
[Huawei-ike-peer-mypeer] inband ocsp
```

12.6.87 integrity-algorithm

Function

The **integrity-algorithm** command configures an integrity algorithm for IKEv2 negotiation.

The **undo integrity-algorithm** command restores the default configuration.

By default, the HMAC-SHA2-256 integrity algorithm is used for IKEv2 negotiation.

Format

integrity-algorithm { **aes-xcbc-96** | **hmac-md5-96** | **hmac-sha1-96** | **hmac-sha2-256** | **hmac-sha2-384** | **hmac-sha2-512** }

undo integrity-algorithm

Parameters

Parameter	Description	Value
aes-xcbc-96	Indicates that the integrity algorithm is AES-XCBC-96.	-
hmac-md5-96	Indicates that the integrity algorithm is HMAC-MD5-96.	-
hmac-sha1-96	Indicates that the integrity algorithm is HMAC-SHA1-96.	-
hmac-sha2-256	Indicates that the integrity algorithm is HMAC-SHA2-256.	-
hmac-sha2-384	Indicates that the integrity algorithm is HMAC-SHA2-384.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hmac-sha2-512	Indicates that the integrity algorithm is HMAC-SHA2-512.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The integrity algorithms are listed as follows from the highest security level to the lowest security level: **hmac-sha2-512** > **hmac-sha2-384** > **hmac-sha2-256** > **aes-xcbc-96** > **hmac-sha1-96** > **hmac-md5-96**.

Precautions

On the device running a version earlier than V200R008, the **authentication-algorithm** command serves the same function as the **integrity-algorithm** command.

Example

Set the integrity algorithm to be used in IKEv2 proposal **10** to HMAC-SHA2-384.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] integrity-algorithm hmac-sha2-384
```

12.6.88 interface-assign

Function

The **interface-assign** command assigns an interface associated with an IKE user.

The **undo interface-assign** command deletes an interface associated with an IKE user.

By default, no interface on the device is associated with the IKE user.

Format

interface-assign *interface-type interface-number*

undo interface-assign

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. Currently, the interface can only be a tunnel interface.	-

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters. The IKE user table in the headquarters contains multiple IKE users for managing parameters for interconnection between the headquarters and branches, such as the pre-shared key. If one IPSec profile in the headquarters is applied to multiple tunnel interfaces, IPSec negotiation may fail because the IKE peer in the headquarters fails to match the tunnel interface of each branch. In this case, you can run the **interface-assign** command to assign a tunnel interface associated with an IKE user, so that IKE users can successfully match tunnel interfaces of branches.

Example

Assign an interface associated with the IKE user.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei] quit
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] interface-assign tunnel 0/0/1
```

Related Topics

12.6.27 display ike user-table (all views)

12.6.89 interface tunnel-template

Function

The **interface tunnel-template** command creates a tunnel template interface and enters the tunnel template interface view.

The **undo interface tunnel-template** command deletes the tunnel template interface.

 Copyright © Huawei Technologies Co., Ltd.

By default, no tunnel template interface exists.

Format

interface tunnel-template *interface-number*

undo interface tunnel-template *interface-number*

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel template interface.	The value range depends on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A virtual tunnel template interface is similar to a virtual tunnel interface. You can create a tunnel template interface on the headquarters gateway and then apply an IPSec profile to the tunnel template interface and the tunnel interface of the branch gateway respectively to enable the gateways to send or accept subnet route information.

Follow-up Procedure

After creating a tunnel template interface, run the **tunnel-protocol ipsec** command to set the encapsulation mode of the tunnel template interface to IPSec.

Example

Create a tunnel template interface.

```
<Huawei> system-view
[Huawei] interface tunnel-template 1
[Huawei-Tunnel-Template1]
```

Related Topics

12.6.29 display interface tunnel-template

12.6.90 ip address

Function

The **ip address** command specifies the IP address of an allowed peer for IKE negotiation.

The **undo ip address** command deletes the IP address of an allowed peer.

By default, no IP address of allowed peer for IKE negotiation is configured.

Format

ip address *ip-address* { *mask* | *mask-length* }

undo ip address *ip-address* { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
ip-address { *mask* | *mask-length* }	Specifies the IP address of an allowed peer. • *ip-address* specifies the IP address. • *mask* specifies the mask of the IP address. • *mask-length* specifies the mask length of IP address.	• The value of *ip-address* is in dotted decimal notation. • The value of *mask* is in dotted decimal notation. • The value of *mask-length* is an integer that ranges from 0 to 32.

Views

Identity filter set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify an allowed peer based on the IP address (configured on a remote device for establishing an IPSec tunnel) in the identity filter set for IKE negotiation.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

An IPSec tunnel can be established only when the remote end matches one or more parameters in the identity filter set and the IPSec negotiation parameters at both ends are consistent.

If you run this command in the same view multiple times, the latest configuration does not override earlier ones.

Example

Configure the IP address **10.1.1.1** of an allowed peer for IKE negotiation.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] ip address 10.1.1.1 24
```

Related Topics

12.6.70 ike identity

12.6.117 local-id-type

12.6.91 ip address ike-negotiated

Function

The **ip address ike-negotiated** command configures an IKE peer to request an IP address for an IPSec tunnel interface through IKEv2 negotiation.

The **undo ip address ike-negotiated** command cancels the configuration.

By default, an IKE peer does not request an IP address for an IPSec tunnel interface through IKEv2 negotiation.

Format

ip address ike-negotiated

undo ip address ike-negotiated

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ip address ike-negotiated** command is used in scenarios where many branches connect to the headquarters, the headquarters pushes the IP address of

 Copyright © Huawei Technologies Co., Ltd.

the IPSec tunnel interface. This reduces the configuration and maintenance workload of branches.

Prerequisites

The tunneling protocol has been configured as IPSec on the IPSec tunnel interface using the **tunnel-protocol ipsec command.**

Precautions

If the **ip address** command has been used to configure an IP address for the IPSec tunnel interface, when you run the **ip address ike-negotiated** command, the system displays a message indicating a conflict. If the **ip address ike-negotiated** command has been configured on the IPSec tunnel interface, the **ip address** command executed later will take effect.

Example

Configure an IKE peer to request an IP address for Tunnel0/0/1 through IKEv2 negotiation.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipsec
[Huawei-Tunnel0/0/1] ip address ike-negotiated
```

Related Topics

12.3.21 tunnel-protocol

12.6.92 ipsec anti-replay enable

Function

The **ipsec anti-replay enable** command enables the anti-replay function globally.

The **undo ipsec anti-replay enable** command disables the anti-replay function globally.

By default, the anti-replay function is enabled globally.

Format

ipsec anti-replay enable

undo ipsec anti-replay enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Replayed packets refer to the packets that have been processed by the device. IPSec uses the sliding window (anti-replay window) to detect replayed packets. AH and ESP packet headers carry 32-bit sequence numbers. The sequence numbers carried in the AH or ESP packet headers of the same SA are in ascending order. If the sequence number of an authenticated packet is the same as that of a decapsulated packet or the sequence number is outside the sliding window, the packet is considered a replayed packet.

Decapsulating replayed packets consumes many resources and makes system performance deteriorate. Therefore, attackers may use replayed packets to initiate a DoS attack. After the anti-replay function is enabled, the system discards replayed packets to save system resources.

Precautions

Only SAs established in IKE negotiation mode support the anti-replay function. Manually configured SAs do not support the anti-replay function.

In some situations, for example, network congestion occurs or QoS is performed for packets, the sequence numbers of some service data packets may be different from those in common data packets. The device that has IPSec anti-replay enabled considers the packets replayed and discards them. You can disable global IPSec anti-replay to prevent packets from being discarded incorrectly or adjust the IPSec anti-replay window size to meet service requirements.

Example

Enable the anti-replay function globally.

```
<Huawei> system-view
[Huawei] ipsec anti-replay enable
```

Related Topics

12.6.93 ipsec anti-replay window

12.6.93 ipsec anti-replay window

Function

The **ipsec anti-replay window** command sets the global IPSec anti-replay window size.

The **undo ipsec anti-replay window** command restores the default global IPSec anti-replay window size.

By default, the global IPSec anti-replay window size is 1024 bits.

 Copyright © Huawei Technologies Co., Ltd.

Format

ipsec anti-replay window *window-size*

undo ipsec anti-replay window

Parameters

Parameter	Description	Value
window-size	Specifies the global IPSec anti-replay window size.	The value can be 32, 64, 128, 256, 512, or 1024, in bits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some situations, for example, network congestion occurs or QoS is performed for packets, the sequence numbers of some service data packets may be unusual. The device that has IPSec anti-replay enabled considers the packets replayed and discards them. To prevent packets from being discarded incorrectly, you can disable global IPSec anti-replay or adjust the IPSec anti-replay window size to meet service requirements.

Prerequisites

The anti-replay function has been enabled. By default, the anti-replay function is enabled (through **ipsec anti-reply enable** command).

Precautions

When both **anti-replay window** and **ipsec anti-replay window** are used, the **anti-replay window** command takes effect. When **anti-replay window** is not configured, the **ipsec anti-replay window** command takes effect.

Example

Set the global IPSec anti-replay window size to 128 bits.

```
<Huawei> system-view
[Huawei] ipsec anti-replay window 128
```

Related Topics

12.6.92 ipsec anti-replay enable

 Copyright © Huawei Technologies Co., Ltd.

12.6.94 ipsec authentication sha2 compatible enable

Function

The **ipsec authentication sha2 compatible enable** command enables SHA-2 to be compatible with RFC standard algorithm versions.

The **undo ipsec authentication sha2 compatible enable** command disables SHA-2 from being compatible with RFC standard algorithm versions.

By default, the SHA-2 algorithm is not compatible with RFC standard algorithm versions.

Format

ipsec authentication sha2 compatible enable

undo ipsec authentication sha2 compatible enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IPSec uses the SHA-2 algorithm, if the devices on two ends of an IPSec tunnel are from different vendors or run different software versions, they may use different encryption and decryption methods. In this situation, traffic between devices is interrupted.

To solve this problem, run the **ipsec authentication sha2 compatible enable** command to enable SHA-2 to be compatible with RFC standard algorithm versions.

Precautions

When AR routers are interconnected, ensure that the configuration are the same; otherwise, IPSec traffic fails to be transmitted.

This function takes effect only after you run the **reset ike sa** command.

Example

Enable the SHA-2 algorithm to be compatible with RFC standard algorithm versions.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ipsec authentication sha2 compatible enable
```

12.6.95 ipsec decrypt check

Function

The **ipsec decrypt check** command enables a device to check decrypted IPSec packets.

The **undo ipsec decrypt check** command disables a device from checking decrypted IPSec packets.

By default, the device does not check decrypted IPSec packets.

Format

ipsec decrypt check

undo ipsec decrypt check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

In tunnel mode, the IP header in the decrypted IPSec packet of the inbound SA may be not defined in an ACL, for example, the IP header of attack packets may be out of the range defined in the ACL. Therefore, the device checks whether the IP header of the decrypted IPSec packet is in the range defined by the ACL. If the decrypted IPSec packet matches the permit clause, the device continues to process the IPSec packet. If the decrypted IPSec packet does not match the permit clause, the device discards the IPSec packet. The device discards the IPSec packets failing the ACL check to improve network security.

When establishing an IPSec tunnel using a tunnel interface, if the **ipsec decrypt check** command is executed in the system view, packets decrypted by IPSec are check based on the ACL rule. Note the following points:

- When the encapsulation mode is set to IPSec, the source and destination addresses in the ACL are both any, indicating that all data flows destined for the IPSec tunnel interface are protected.
- When the encapsulation mode is set to GRE, the source and destination addresses in the ACL are the source and destination addresses of the IPSec tunnel interface respectively.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the device from checking decrypted IPSec packets.

```
<Huawei> system-view
[Huawei] undo ipsec decrypt check
```

12.6.96 ipsec df-bit

Function

The **ipsec df-bit** command sets the don't fragment (DF) flag bit in an IPSec or a A2A VPN packet.

By default, the DF flag bit in an IPSec or a A2A VPN packet is the flag bit of original packets.

Format

ipsec df-bit { **clear** | **set** | **copy** }

Parameters

Parameter	Description	Value
clear	Sets the DF flag bit to 0, indicating that IP packets can be fragmented.	-
set	Sets the DF flag bit to 1, indicating that IP packets cannot be fragmented.	-
copy	Uses the flag bit of original packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an original packet is encapsulated, the packet length may exceed the MTU of the device outbound interface. To prevent packet loss, fragment the packets.

Precautions

If you run the **ipsec df-bit** command multiple times, only the latest configuration takes effect.

Example

Set the DF flag bit to 0 in an IPSec or a A2A VPN packet.

```
<Huawei> system-view
[Huawei] ipsec df-bit clear
```

Related Topics

12.6.99 ipsec fragmentation before-encryption

12.6.97 ipsec efficient-vpn (interface view)

Function

The **ipsec efficient-vpn** command binds an Efficient VPN policy to an interface.

The **undo ipsec efficient-vpn** command deletes the Efficient VPN policy from an interface.

By default, no Efficient VPN policy is applied to an interface.

Format

ipsec efficient-vpn *efficient-vpn-name*

undo ipsec efficient-vpn

Parameters

Parameter	Description	Value
efficient-vpn-name	Specifies the name of an Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many branches and traveling staff connect to the headquarters over IPSec tunnels, similar or duplicate IPSec configurations and other network resource

 Copyright © Huawei Technologies Co., Ltd.

configurations must be configured on the branch and headquarters gateways. The Efficient VPN solution uses centralized IPSec configurations on the headquarters gateway and simplified IPSec configuration on each branch gateway. This solution reduces the manual configuration workload, and facilitates IPSec VPN configuration and maintenance.

Prerequisites

An Efficient VPN policy has been created using the **ipsec efficient-vpn (system view)** command.

Precautions

If an Efficient VPN policy is used to establish an IPSec tunnel between the enterprise branch and headquarters, apply the Efficient VPN policy to the branch gateway and use an IPSec policy template on the headquarters gateway to create an IPSec policy.

Example

Apply the Efficient VPN policy named **evpn** to **Ethernet 1/0/2**.

```
<Huawei> system-view
[Huawei] interface ethernet 1/0/2
[Huawei-Ethernet1/0/2] ipsec efficient-vpn evpn
```

Related Topics

12.6.30 display ipsec efficient-vpn

12.6.98 ipsec efficient-vpn (system view)

12.6.98 ipsec efficient-vpn (system view)

Function

The **ipsec efficient-vpn** command creates an IPSec Efficient VPN policy and displays the IPSec Efficient VPN policy view.

The **undo ipsec efficient-vpn** command deletes an IPSec Efficient VPN policy.

By default, no IPSec Efficient VPN policy is created in the system.

Format

ipsec efficient-vpn *efficient-vpn-name* [**mode** { **client** | **network** | **network-auto-cfg** | **network-plus** }]

undo ipsec efficient-vpn *efficient-vpn-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
efficient-vpn-name	Specifies the name of an Efficient VPN policy.	The value is a string of 1 to 12 case-sensitive characters without question marks (?) or spaces.
mode	Specifies the mode of the Efficient VPN policy.	-
client	Indicates the client mode.	-
network	Indicates the network mode.	-
network-auto-cfg	Indicates the network-auto-cfg mode. The Network-auto-cfg mode is supported in IKEv1 only.	-
network-plus	Indicates the network-plus mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many branches and traveling staff connect to the headquarters over IPSec tunnels, similar or duplicate IPSec configurations and other network resource configurations must be configured on the branch and headquarters gateways. The Efficient VPN solution uses centralized IPSec configurations on the headquarters gateway and simplified IPSec configuration on each branch gateway. This solution reduces the manual configuration workload, and facilitates IPSec VPN configuration and maintenance.

The Efficient VPN policy has the following modes:

- Client mode

  When a remote device requests an IP address from the Efficient VPN server, a loopback interface is dynamically created on the remote device and the IP address obtained from the server is assigned to the loopback interface. The

remote device automatically enables NAT to translate its original IP address into the obtained IP address, and then uses this IP address to establish an IPSec tunnel with the headquarters.

The client mode applies to scenarios where traveling staff or small-scale branches connect to the headquarters network through private networks. In client mode, devices connected to the Efficient VPN server or remote devices can use the same IP address. However, the number of devices allowed depends on the number of IP addresses assigned by the Efficient VPN server.

- Network mode

  In network mode, a remote device does not apply to the Efficient VPN server for an IP address. Instead, the remote device uses the original IP address to establish an IPSec tunnel with the headquarters. Therefore, NAT is not automatically enabled in network mode.

  The network mode applies to scenarios where IP addresses of the headquarters and branches are planned uniformly. Ensure that IP addresses do not conflict.

- Network-plus mode

  Compared with the network mode, the remote device applies to the Efficient VPN server for an IP address in network-plus mode. IP addresses of branches and headquarters are configured beforehand. A remote device applies to the Efficient VPN server for an IP address. The Efficient VPN server uses the IP address to perform ping, Telnet, or other management and maintenance operations on the remote device. NAT is not automatically enabled on the remote device.

- Network-auto-cfg mode

  Compared with the network-plus mode, the remote device applies to the Efficient VPN server for an IP address pool in network-auto-cfg mode. The IP address pool is used for allocating addresses to users.

Follow-up Procedure

Configure negotiation parameters of Efficient VPN in the Efficient VPN policy view, and use the **ipsec efficient-vpn (interface view)** command to bind the Efficient VPN policy to an interface.

Example

Create the Efficient VPN policy named **vpn1** in client mode.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn vpn1 mode client
[Huawei-ipsec-efficient-vpn-vpn1]
```

Related Topics

12.6.30 display ipsec efficient-vpn

12.6.97 ipsec efficient-vpn (interface view)

12.6.99 ipsec fragmentation before-encryption

Function

The **ipsec fragmentation before-encryption** command sets the fragmentation mode of packets to fragmentation before encryption for all IPSec tunnels or a A2A VPN.

The **undo ipsec fragmentation before-encryption** command restores the default packet fragmentation mode.

By default, the packet fragmentation mode for all IPSec tunnels or a A2A VPN is fragmentation after encryption.

Format

ipsec fragmentation before-encryption

undo ipsec fragmentation before-encryption

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an original packet is encapsulated, the packet length may exceed the MTU of the device outbound interface. To prevent packet loss, the device fragments the packets. Two fragmentation modes are available:

- Fragmentation before encryption: Before encapsulation, the encryption device calculates the predicted encapsulated packet length. If the packet length is larger than the MTU of the outbound interface, the encryption device fragments packets, and then encrypts the packets. In this situation, the decryption device requests the terminal to reassemble the packets, reducing the CPU usage on the decryption device.
- Fragmentation after encryption: If the size of the encapsulated VPN packets exceeds the MTU of the outbound interface, the encryption device fragments the packets based on the MTU of the outbound interface. In this case, the peer decryption device assembles and decrypts VPN fragments and then sends decrypted packets to the terminal host.

Precautions

Before IPSec packets can be fragmented, the **ipsec df-bit** command must be configured to permit IPSec packet fragmentation.

This command just specifies how the IPSec tunnels process packets. However, whether a packet is fragmented depends on:

 Copyright © Huawei Technologies Co., Ltd.

- The DF bit in IP header of the original packet if the fragmentation before encryption mode is selected
- The DF bit in IPSec header if the fragmentation after encryption mode is selected

For the established IPSec tunnels, you need to restart them after running this command. Otherwise, the command function does not take effect.

Example

Set the fragmentation mode of IPSec or a A2A VPN packets to fragmentation before encryption.

```
<Huawei> system-view
[Huawei] ipsec fragmentation before-encryption
```

12.6.100 ipsec invalid-spi-recovery enable

Function

The **ipsec invalid-spi-recovery enable** command enables the invalid SPI recovery function.

The **undo ipsec invalid-spi-recovery enable** command disables the invalid SPI recovery function.

By default, the invalid SPI recovery function is disabled.

Format

ipsec invalid-spi-recovery enable

undo ipsec invalid-spi-recovery enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the IPSec SA is lost on Gateway_1 at one end of an IPSec tunnel, the corresponding IKE SA still exists on Gateway_1. However, Gateway_2 at the other end of the IPSec tunnel still maintains the IPSec SA. If Gateway_1 receives IPSec packets encapsulated by Gateway_2 using the IPSec SA, Gateway_1 discards the

 Copyright © Huawei Technologies Co., Ltd.

packets because it cannot find the corresponding IPSec SA. At the same time, Gateway_1 sends a DELETE SA INFORMATIONAL message to Gateway_2 by default. After receiving the message, Gateway_2 immediately deletes the IPSec SA matching the invalid SPI. When Gateway_2 continues sending IPSec packets to Gateway_1, the two ends re-negotiate an IPSec SA to restore the IPSec service.

However, when neither IKE SA nor IPSec SA exists on Gateway_1, Gateway_1 does not send a DELETE SA INFORMATIONAL message to Gateway_2 until dead peer detection (DPD) shows that the IPSec SA is invalid or the SA lifetime has expired. This causes lengthy IPSec service interruption. In this case, you can enable the invalid SPI recovery function to solve the problem. When Gateway_1 sends IPSec packets to Gateway_2, the two ends re-negotiate an IPSec SA to restore the IPSec service.

Precautions

The invalid SPI recovery function may lead to denial of service (DoS) attacks.

When the device uses an IPSec policy configured using an IPSec policy template or has the **12.6.147 respond-only enable** command configured, the **ipsec invalid-spi-recovery enable** command does not take effect.

Example

Enable the invalid SPI recovery function.

```
<Huawei> system-view
[Huawei] ipsec invalid-spi-recovery enable
```

Related Topics

12.6.32 display ipsec global config

12.6.25 display ike statistics

12.6.101 ipsec nat-traversal source-port

Function

The **ipsec nat-traversal source-port** command configures a UDP port number for IPSec NAT traversal.

The **undo ipsec nat-traversal source-port** command restores the default UDP port number for IPSec NAT traversal.

By default, the UDP port number for IPSec NAT traversal is 4500.

Format

ipsec nat-traversal source-port *port-number*

undo ipsec nat-traversal source-port

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number for IPSec NAT traversal.	The value is an integer that ranges from 4501 to 49151.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, IPSec NAT traversal uses UDP port 4500. If you want to use another UDP port for IPSec NAT traversal, run the **ipsec nat-traversal source-port** command.

Example

Set a UDP port number for IPSec NAT traversal.

```
<Huawei> system-view
[Huawei] ipsec nat-traversal source-port 4510
```

Related Topics

12.6.32 display ipsec global config

12.6.102 ipsec netmask

Function

The **ipsec netmask** command configures the IPSec mask filtering function.

The **undo ipsec netmask** command deletes the IPSec mask filtering function.

By default, IPSec mask filtering is not configured in the system.

Format

ipsec netmask { **source** *source-mask* | [**source** *source-mask*] **destination** *destination-mask* }

undo ipsec netmask [**source** | **destination**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
source *source-mask*	Specifies the source IPv4 address mask of data flows.	The value is an integer in the range from 1 to 32.
destination *destination-mask*	Specifies the destination IPv4 address mask of data flows.	The value is an integer in the range from 1 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where branches connect to the headquarters, if a branch has a too large protection data flow range configured, traffic of other branches may be incorrectly diverted to the branch. In this case, you can run the **ipsec netmask** command to check and restrict the access of flow information negotiated by the IPSec tunnel. After this function is configured, the device checks the source and destination IP address masks of the peer device. If the mask values are greater than or equal to the configured values, subsequent negotiation continues. Otherwise, the IPSec SA negotiation fails.

Precautions

The device checks and restricts the access of flow information only when it adopts the IPSec policy template.

Example

Configure the IPSec mask filtering function.

```
<Huawei> system-view
[Huawei] ipsec netmask source 24 destination 24
```

Related Topics

12.6.32 display ipsec global config

 Copyright © Huawei Technologies Co., Ltd.

12.6.103 ipsec policy shared

Function

The **ipsec policy shared** command configures a security policy as a multi-link shared security policy.

The **undo ipsec policy shared** command cancels configuring a security policy as a multi-link shared security policy.

By default, no security policy is configured as a multi-link shared security policy.

Format

ipsec policy *policy-name* **shared local-interface loopback** *interface-number*

undo ipsec policy *policy-name* **shared**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a security policy. The security policy must have been configured in the system view.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) or spaces.
local-interface loopback *interface-number*	Specifies the loopback interface number. The loopback interface must have been created.	The value is an integer that ranges from 0 to 1023.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve network reliability, the enterprise gateway often connects to the Internet Service Provider (ISP) through two egress links, which work in backup or load balancing mode. When two outbound interfaces are configured with IPSec policies with the same parameter settings, services need to be smoothly switched between the two links corresponding to the two outbound interfaces. The two outbound interfaces negotiate with their peers to establish IPSec SAs respectively. When one interface alternates between Up and Down states and an active/standby switchover occurs, the two peers need to perform IKE negotiate again to

 Copyright © Huawei Technologies Co., Ltd.

generate IPSec SAs. The IKE re-negotiation causes IPSec service interruption in a short time.

You can configure a multi-link shared security policy and use a loopback interface on the local device to establish an IPSec tunnel with the remote device. When an active/standby switchover occurs, IPSec services are not interrupted. The two IPSec-enabled physical interfaces share the same IPSec SA. When services are switched between links corresponding to the physical interfaces, the IPSec SA is not deleted as long as the loopback interface status remains unchanged. In addition, IKE re-negotiation is not required because the same IPSec SA is used to protect IPSec services.

In an A2A VPN scenario, a GDOI policy can also be configured as a multi-link shared security policy. GMs then register with the KS using loopback interfaces and negotiate to generate one KEK SA. In this manner, multiple interfaces to which the GDOI policy is applied share the same KEK SA.

Precautions

One loopback interface maps to only one multi-link shared security policy.

Example

Configure an IPSec policy as a multi-link shared security policy.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] quit
[Huawei] ipsec policy policy1 11 isakmp
[Huawei-ipsec-policy-isakmp-policy1-11] quit
[Huawei] ipsec policy policy1 shared local-interface loopback 0
```

Configure a GDOI policy as a multi-link shared security policy.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] quit
[Huawei] ipsec policy policy2 12 gdoi
[Huawei-ipsec-policy-gdoi-policy2-12] quit
[Huawei] ipsec policy policy2 shared local-interface loopback 1
```

12.6.104 ipsec policy (interface view)

Function

The **ipsec policy** command binds an IPSec policy group to an interface.

The **undo ipsec policy** command unbinds an IPSec policy group from an interface.

By default, no IPSec policy group is bound to an interface.

Format

ipsec policy *policy-name*

undo ipsec policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPSec policy group bound to an interface.	The value must be the name of an existing IPSec policy group on the device.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can bind an IPSec policy group to a physical or logical interface to protect data flows. In addition to physical interfaces such as serial interfaces and Ethernet interfaces, you can bind an IPSec policy group to virtual interfaces such as Tunnel interfaces. IPSec policy groups can be used according to actual networking requirements. If an IPSec policy group is unbound from an interface, the interface cannot provide IPSec functions.

After an IPSec policy group is bound to an interface, all IPSec policies in the group are bound to the interface to protect different data flows.

When sending a packet, an interface matches the packet with IPSec policies in an IPSec policy group in ascending order of sequence number. If the packet matches the ACL referenced by an IPSec policy, the packet is processed based on the IPSec policy. If the packet does not match an IPSec policy, it searches for the next policy. If no matching ACL is found after all IPSec policies are checked, the interface sends the packet directly without IPSec protection.

Precautions

IPSec policy group can not be bound to VLANIF interface and loopback interface.

Only one IPSec policy group can be bound to an interface, and an IPSec policy group can be bound to only one interface. To bind a new IPSec policy group to an interface, remove the previous one first.

When an IPSec policy group contains both an IPSec policy configured using an IPSec policy template and an IPSec policy in ISAKMP mode, to match the IPSec policy in ISAKMP mode, ensure that the sequence number of the IPSec policy in ISAKMP mode is smaller than that of the IPSec policy configured using an IPSec policy template.

In an IPSec policy group, if multiple policies are bound to different IKE peers, the remote addresses specified in the IKE peers cannot be the same. Otherwise, IKE negotiation of some IPSec policies fails.

 Copyright © Huawei Technologies Co., Ltd.

If multiple IPSec policies are bound to the same IKE peer in an IPSec policy group, the same tunnel local address must be configured for these IPSec policies. Otherwise, IKE negotiation of some IPSec policies fails.

When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the **undo ipsec policy** command is run. After all the SAs are cleared, the CPU usage restores to the normal range.

In the PPPoE scenario, the application of IPSec policies on the VT interface of the PPPoE server is not supported.

A tunnel interface and the source interface that is referenced by the tunnel interface cannot be both bound to IPSec policies.

Example

Apply the IPSec policy group **policy1** to Eth1/0/2.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] quit
[Huawei] interface ethernet 1/0/2
[Huawei-Ethernet1/0/2
] ipsec policy policy1
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.105 ipsec policy (system view)

Function

The **ipsec policy** command creates an IPSec policy and displays the IPSec policy view.

The **undo ipsec policy** command deletes an IPSec policy.

By default, no IPSec policy is configured.

Format

ipsec policy *policy-name seq-number* [**manual** | **isakmp** [**template** *template-name*]]

undo ipsec policy *policy-name* [*seq-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPSec policy.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) and spaces.
seq-number	Specifies the sequence number of an IPSec policy.	The value is an integer that ranges from 1 to 10000. A smaller value indicates a higher IPSec policy priority.
manual	Indicates that an IPSec SA is created manually.	-
isakmp	Indicates that an IPSec policy is established in IKE negotiation mode.	-
template *template-name*	Indicates that an IPSec policy is established by referencing an IPSec policy template.	The value must be an existing IPSec policy template name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec policy is uniquely defined by its name and sequence number. IPSec policies with the same name belong to one IPSec policy group.

- Manual mode

  IPSec parameters including the authentication/encryption key and SPI on IPSec peers must mirror each other. That is, IPSec parameters of the inbound SA at the local end must be the same as those of the outbound SA at the remote end, and IPSec parameters of the outbound SA at the local end must be the same as those of the inbound SA at the remote end.

- IKE negotiation mode

  IPSec parameters are automatically negotiated through IKE. This mode is classified into ISAKMP and IPSec policy template:

- ISAKMP

  Negotiated IPSec parameters are defined in the IPSec policy view, and the initiator and responder must use the same IPSec parameters.

  Devices use the ISAKMP policy can be an initiator or a responder.

- IPSec policy template

  An IPSec policy template defines negotiated parameters. The initiator determines optional parameters, and the responder accepts the parameters delivered by the initiator.

  An IPSec policy template can reduce the workload of establishing multiple IPSec tunnels. The IPSec policy template is applicable to specific scenarios, for example, scenario where the remote IP address is variable or unknown (for example, the remote end obtains an IP address using PPPoE) and the remote device is allowed to initiate negotiation to the local end.

  ACLs in this mode are optional. If no ACL is configured, the responder uses the ACL configured on the initiator to protect data flows.

Follow-up Procedure

Define negotiated IPSec parameters in the IPSec policy view and run the **ipsec policy (interface view)** command to bind the IPSec policy to an interface.

Precautions

- The end where an IPSec policy template is configured can only function as the responder to receive negotiation requests.
- One IPSec policy group can have only one IPSec policy template.
- When creating an IPSec policy, you must specify the SA creation mode. If you have entered the IPSec policy view, you do not need to enter the SA creation mode.
- Before modifying the negotiation mode of a created IPSec policy, delete the IPSec policy and create an IPSec policy again.

Example

Set an IPSec policy using the ISAKMP negotiation mode. The IPSec policy name is **policy1** and the sequence number is **1**.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1]
```

Set an IPSec policy using the manual negotiation mode. The IPSec policy name is **policy2** and the sequence number is **1**.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 1 manual
[Huawei-ipsec-policy-manual-policy2-1]
```

Related Topics

12.6.104 ipsec policy (interface view)
12.6.34 display ipsec policy (all views)

12.6.106 ipsec policy-template

Function

The **ipsec policy-template** command creates an IPSec policy template and displays the IPSec policy template view.

The **undo ipsec policy-template** command deletes an IPSec policy template group or an IPSec policy template from the group.

By default, no IPSec policy template is created.

Format

ipsec policy-template *template-name seq-number*

undo ipsec policy-template *template-name* [*seq-number*]

Parameters

Parameter	Description	Value
template-name	Specifies the name of the policy template.	It is a string of 1 to 15 case sensitive characters and cannot contain the hyphen (-).
seq-number	Specifies the sequence number of the IPSec policy.	It is an integer that ranges from 1 to 10000. The smaller the value is, the higher the priority is.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Negotiated IPSec parameters are defined in the IPSec policy template view. The initiator determines optional parameters, and the responder accepts the parameters delivered by the initiator. If an IPSec policy template is configured at the local end, the local end can only function as the responder to receive negotiation requests.

An IPSec policy template can be used to configure multiple IPSec policies, reducing the workload of establishing multiple IPSec tunnels. An IPSec policy template is applicable to specific scenarios, for example, scenario where the remote IP address is variable or unknown and the remote peers are allowed to initiate negotiation to the local end.

 Copyright © Huawei Technologies Co., Ltd.

ACLs in this mode are optional. If no ACL is configured, the responder uses the ACL configured on the initiator to protect data flows.

Follow-up Procedure

Run the **ipsec policy** *policy-name seq-number* **isakmp template** *template-name* command to reference the created template.

Precautions

The IPSec policy template name must be different from the IPSec policy name.

Example

Create an IPSec policy template with the name **policy1** and the sequence number **1**.

```
<Huawei> system-view
[Huawei] ipsec policy-template policy1 1
[Huawei-ipsec-policy-templet-policy1-1]
```

Related Topics

12.6.36 display ipsec policy-template (all views)
12.6.105 ipsec policy (system view)

12.6.107 ipsec profile (interface view)

Function

The **ipsec profile** command applies an IPSec profile to a tunnel interface.

The **undo ipsec profile** command unbinds the IPSec profile from a tunnel interface.

By default, no IPSec profile is applied to a tunnel interface.

Format

ipsec profile *profile-name*

undo ipsec profile

NOTE

V200R010 does not support the shared parameter. That is, the same physical outbound interface cannot be specified for multiple tunnel interfaces.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an IPSec profile.	The value is an existing IPSec profile name.

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

An IPSec profile has been created using the **ipsec profile (system view)** command.

A tunnel interface has been created using the **12.3.10 interface tunnel** command, and the encapsulation mode of the tunnel interface has been set to GRE or IPSec using the **12.3.21 tunnel-protocol** command.

Precautions

- A tunnel interface can be bound to only one IPSec profile. An IPSec profile can be applied to only one tunnel interface.
- A tunnel template interface can be bound to only one IPSec profile. An IPSec profile can be applied to only one tunnel template interface.
- When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the **undo ipsec profile** command is run. After all the SAs are cleared, the CPU usage restores to the normal range.
- A tunnel interface and the source interface that is referenced by the tunnel interface cannot be both bound to IPSec profiles.

Example

Bind the IPSec profile **profile1** to tunnel interface **tunnel 0/0/1**.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipsec
[Huawei-Tunnel0/0/1] source 10.1.1.1
[Huawei-Tunnel0/0/1] ipsec profile profile1
```

Related Topics

12.3.10 interface tunnel

12.3.21 tunnel-protocol

12.6.108 ipsec profile (system view)

12.6.38 display ipsec profile (all views)

12.6.108 ipsec profile (system view)

Function

The **ipsec profile** command creates an IPSec profile and enters the IPSec profile view.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ipsec profile** command deletes an IPSec profile.

By default, no IPSec profile is configured.

Format

ipsec profile *profile-name*

undo ipsec profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an IPSec profile.	The value is a string of 1 to 32 case-sensitive characters without question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec profile is similar to an IPSec policy. However, different from an IPSec policy, an IPSec profile is identified by its name, and can only be configured in IKE negotiation mode. The IPSec profile does not support ACL configuration. The IPSec profile can be applied to only an IPSec tunnel interface. An IPSec profile defines IPSec proposals used to protect data flows, IKE negotiation parameters for SA setup, SA lifetime, and PFS status. After an IPSec profile is applied to an IPSec tunnel interface, only one IPSec tunnel is created. The IPSec tunnel protects all the data flows routed to the IPSec tunnel interface, simplifying IPSec policy management.

Follow-up Procedure

Define negotiated IPSec parameters in the IPSec profile view and run the **12.6.107 ipsec profile (interface view)** command to apply the IPSec profile to an interface.

Precautions

You do not need to specify the local and remote addresses for the IKE peer that is referenced by an IKE profile. Even if the local and remote addresses are specified for the IKE peer that is referenced by an IKE profile, the local and remote addresses are invalid. This is because the source and destination addresses of the IPSec tunnel interfaces are used as local and remote addresses when the IPSec profile performs IKE negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an IPSec profile named **profile1**.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1]
```

Related Topics

12.6.38 display ipsec profile (all views)

12.6.107 ipsec profile (interface view)

12.6.109 ipsec proposal

Function

The **ipsec proposal** command creates an IPSec proposal and displays the IPSec proposal view.

The **undo ipsec proposal** command deletes an IPSec proposal.

By default, no IPSec proposal is configured.

Format

ipsec proposal *proposal-name*

undo ipsec proposal *proposal-name*

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of an IPSec proposal.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) and spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec proposal is a part of an IPSec policy or an IPSec profile. It defines IPSec protection methods and security parameters for IPSec SA negotiation. The parameters include the security protocol, encryption and authentication algorithms, and encapsulation mode.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

1. Configure security parameters including the security protocol, encryption and authentication algorithms, and encapsulation mode.
2. Run the **proposal** command to reference the IPSec proposal in an IPSec policy.

Precautions

Both ends of an IPSec tunnel must be configured with the same parameters.

Example

Create an IPSec proposal named **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1]
```

Related Topics

12.6.172 transform
12.6.3 ah authentication-algorithm
12.6.57 esp authentication-algorithm
12.6.59 esp encryption-algorithm
12.6.54 encapsulation-mode
12.6.40 display ipsec proposal (All views)
12.6.129 proposal

12.6.110 ipsec proto-protect proposal

Function

The **ipsec proto-protect proposal** command creates a security proposal and displays the security proposal view.

The **undo ipsec proto-protect proposal** command deletes a security proposal.

By default, no security proposal is created.

Format

ipsec proto-protect proposal *proposal-name*

undo ipsec proto-protect proposal *proposal-name*

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of a security proposal.	The value is a string of 1 to 15 case-insensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A security proposal defines the security protocol and authentication or encryption algorithm. Therefore, run the **ipsec proto-protect proposal** command to create a security proposal before configuring IPSec.

Follow-up Procedure

Configure the security protocol, authentication or encryption algorithm, and encapsulation mode.

Precautions

You cannot delete the security proposal applied on a Security Association (SA). However, you can apply the same proposal on different SA's. To delete a security proposal, run the **undo proposal** command to remove a security proposal from the SA.

Example

Configure a security proposal named **newprop1**.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal newprop1
```

12.6.111 ipsec remote traffic-identical accept

Function

The **ipsec remote traffic-identical accept** command allows branch or other users to quickly access the headquarters network.

The **undo ipsec remote traffic-identical accept** command disables quick access to the headquarters network.

By default, the device allows branch or other users to quickly access the headquarters network after their IP addresses are changed.

Format

ipsec remote traffic-identical accept

undo ipsec remote traffic-identical accept

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a branch and headquarters of a company establish an IPSec tunnel, the IP address of the branch gateway interface to which an IPSec policy group is applied changes due to the link status change or other reasons. For example, the branch gateway connects to the Internet through dialup and establishes an IPSec tunnel with the headquarters. As a result, the established IPSec tunnel between the headquarters and branch becomes unavailable. However, this IPSec tunnel still exists before timeout.

If quick access to the headquarters network is disabled, when a branch gateway initiates IPSec negotiation again, the headquarters retains the original IPSec tunnel before the tunnel expires. As a result, the data flows transmitted over the new negotiated IPSec tunnel are the same as those on the original IPSec tunnel, causing a conflict. In this case, the branch and headquarters cannot establish a new IPSec tunnel in a short period of time.

If quick access to the headquarters network is enabled, when a branch gateway initiates IPSec negotiation again, the headquarters deletes the original IPSec tunnel immediately so that the branch and headquarters can establish a new IPSec tunnel quickly.

Prerequisites

- The headquarters gateway functions as the responder and uses an IPSec policy template to establish an IPSec tunnel with the branch gateway.
- The ACL referenced by the IPSec policy does not change before and after the IPSec tunnel becomes unavailable.
- The interface that the branch uses to connect to the headquarters gateway does not change before and after the IPSec tunnel becomes unavailable.

Example

Allow the branch or other users to quickly access the headquarters network.

```
<Huawei> system-view
[Huawei] ipsec remote traffic-identical accept
```

12.6.112 ipsec sa

Function

The **ipsec sa** command creates a Security Association (SA) and displays the SA view.

The **undo ipsec sa** command deletes an SA.

By default, no SA is created.

Format

ipsec sa *sa-name*

undo ipsec sa *sa-name*

Parameters

Parameter	Description	Value
sa-name	Specifies the name of an SA.	It is a string of 1 to 15 case-insensitive characters, spaces not supported. The characters can be letters or numbers. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IPSec uses an SA to ensure security during data transmission. When configuring IPSec, run the **ipsec sa** command to create an SA and configure SA parameters.

Follow-up Procedure

Run the **proposal** command to import a security proposal; run the **sa spi** command to configure the SPI; run the **sa string-key**, **sa authentication-hex** or **sa encryption-hex** command to configure the authentication key.

Precautions

An SA is unidirectional. Incoming packets and outgoing packets are processed by different SAs.

An SA can be configured with only one security protocol.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an SA.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
```

12.6.113 ipsec sa global-duration

Function

The **ipsec sa global-duration** command sets the global hard lifetime of IPSec SAs.

The **undo ipsec sa global-duration** command restores the default global hard lifetime of IPSec SAs.

By default, the global time-based SA hard lifetime is 3600 seconds and the global traffic-based SA hard lifetime is 1843200 Kbytes.

Format

ipsec sa global-duration { **time-based** *interval* | **traffic-based** *size* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

Parameters

Parameter	Description	Value
time-based *interval*	Specifies the time-based global IPSec SA hard lifetime. When a large number of IPSec tunnels are established between two devices, you are advised to set the global IPSec SA hard lifetime to a value larger than or equivalent to 1800s.	It is an integer that ranges from 30 to 604800, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
traffic-based *size*	Specifies the traffic-based global IPSec SA hard lifetime. It is recommended that the traffic volume be equal to or larger than the size of IPSec traffic forwarded in 1 hour.	The value is 0 or an integer from 256 to 200000000, in Kbytes. ● IKEv1 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function. ● IKEv2 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, the local device disables the traffic timeout function. During IPSec negotiation between a Huawei device and a Cisco device using IKEv1: ● If the Huawei device functions as the initiator and the traffic hard lifetime is set to 0, the traffic hard lifetime value pushed by the Cisco device takes effect on the local end. ● If the Huawei device functions as the responder and the traffic hard lifetime is set to 0, the value 0 takes effect on the local end.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a dynamic SA, configure the SA hard lifetime so that the SA can be updated in real time, reducing the crash risk and improving security.

There are two methods to measure the lifetime:

- Time-based lifetime

  The period from when an SA is set up to when the SA is expired.
- Traffic-based lifetime

  The maximum volume of traffic that this SA can process.

The lifetime is classified as follows:

- Hard lifetime: specifies the lifetime of an IPSec SA.

  When two devices negotiate an IPSec SA, the actual hard lifetime is the smaller of the two values configured on the two devices.

- Soft lifetime: specifies the time after which a new IPSec SA is negotiated so that the new IPSec SA will be ready before the hard lifetime of the original IPSec SA expires.

  Table 12-64 lists the default soft lifetime values.

Table 12-64 Soft lifetime values

Soft Lifetime Type	Description
Time-based soft lifetime (soft timeout period)	The value is 70% of the actual hard lifetime (hard timeout period).
Traffic-based soft lifetime (soft timeout traffic)	• For IKEv1, the value is 70% of the actual hard lifetime (hard timeout traffic). • For IKEv2, the value is 65% to 75% of the actual hard lifetime (hard timeout traffic) plus or minus a random value.

Before an IPSec SA becomes invalid, IKE negotiates a new IPSec SA for the remote end. The remote end uses the new IPSec SA to protect IPSec communication immediately after the new IPSec SA is negotiated. If service traffic is transmitted, the original IPSec SA is deleted immediately. If no service traffic is transmitted, the original IPSec SA will be deleted after 10s or the hard lifetime expires.

If the time-based lifetime and traffic-based lifetime are both set for an IPSec SA, the IPSec SA becomes invalid when either lifetime expires.

Precautions

You only need to specify the SA lifetime for the SA setup through the IKE negotiation. That is, it is invalid to the SA manually set up. The manually set up SA is effective permanently.

The SA lifetime can be configured globally or based on an IPSec policy or profile. If no SA lifetime is configured for the IPSec policy or profile, the global lifetime is used. If both the global SA lifetime and lifetime based on the IPSec policy or profile are configured, the latter one takes effect.

During IKEv1 negotiation:

- The responder cannot initiate IPSec SA renegotiation after the IPSec SA soft lifetime expires.
- The initiator cannot initiate IPSec SA renegotiation when its IKE SA is deleted and the IPSec SA soft lifetime expires.

During IKEv2 negotiation, the initiator or responder cannot initiate IPSec SA renegotiation if the IKE SA is deleted and the IPSec SA soft lifetime expires.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the time-based global SA hard lifetime to 7200s.

```
<Huawei> system-view
[Huawei] ipsec sa global-duration time-based 7200
```

Set the traffic-based global SA hard lifetime to 10 MB.

```
<Huawei> system-view
[Huawei] ipsec sa global-duration traffic-based 10240
```

Related Topics

12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)

12.6.114 ipsec sm4 version

Function

The **ipsec sm4 version** command sets an SM4 algorithm version for IKE negotiation.

The **undo ipsec sm4 version** command restores the default SM4 algorithm version for IKE negotiation.

By default, the SM4 algorithm version **draft-standard** is used.

Format

ipsec sm4 version { **draft-standard** | **standard** }

undo ipsec sm4 version

Parameters

Parameter	Description	Value
draft-standard	Sets the SM4 algorithm version to that released in 2013. The attribute value of the SM4 algorithm is 127.	-
standard	Sets the SM4 algorithm version to that released in 2014. The attribute value of the SM4 algorithm is 129.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

For IKE negotiation during interconnection with non-Huawei devices, if the SM4 algorithm versions used by devices of different vendors differ from each other, the

 Copyright © Huawei Technologies Co., Ltd.

IKE negotiation fails. In this case, run the **ipsec sm4 version** command to set the SM4 algorithm version consistent with that on non-Huawei devices.

Example

Set the SM4 algorithm version used for IKE negotiation to **standard**.

```
<Huawei> system-view
[Huawei] ike peer p1
[Huawei-ike-peer-p1] ipsec sm4 version standard
```

Related Topics

12.6.20 display ike peer (all views)

12.6.115 lifetime-notification-message enable

Function

The **lifetime-notification-message enable** command enables a device to send IKE SA lifetime notification messages.

The **undo lifetime-notification-message enable** command disables a device from sending IKE SA lifetime notification messages.

By default, the device does not send IKE SA lifetime notification messages.

Format

lifetime-notification-message enable

undo lifetime-notification-message enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **12.6.157 sa duration (IKE proposal view)** command to configure an IKE SA lifetime in an IKE proposal. If the IKE SA lifetimes of two ends are different, the two ends use the smaller IKE SA lifetime for IKE negotiation.

- When a Huawei device (responder) wants to set up an IPSec tunnel with a Cisco systems VPN client (initiator) and the IKE SA lifetimes configured at two

ends are different, you can run this command to enable the Huawei device to send IKE SA lifetime notification messages to the Cisco device to ensure successful IKE negotiation between them. If the Huawei device is disabled from sending IKE SA lifetime notification messages to the peer, the IKE negotiation fails.

- You can also run this command when two Huawei devices need to set up an IPSec tunnel. However, the configuration takes effect on the responder only. If you cannot determine which end is the initiator, you are advised to configure this command on devices at both ends.

Precautions

This command is supported by IKEv1 only.

Example

Enable the IKE peer named **peer1** to send IKE SA lifetime notification messages.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] undo version 2
[Huawei-ike-peer-peer1] lifetime-notification-message enable
```

Related Topics

12.6.75 ike peer

12.6.157 sa duration (IKE proposal view)

12.6.116 local-address

Function

The **local-address** command assigns an IP address to the local end of IKE negotiation.

The **undo local-address** command cancels the configuration.

By default, the system selects an outbound interface according to a route and uses the IP address of the outbound interface as the local IP address.

Format

local-address *ip-address*

undo local-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the local end of IKE negotiation.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **local-address** command assigns an IP address to the local end of IKE negotiation.

When the local end and remote end establish an IPSec tunnel, the local IP address does not need to be configured during IKE negotiation. By default, the system selects an outbound interface according to a route and uses the IP address of the outbound interface as the local IP address.

- If the IP address of an interface bound to an IPSec policy is variable or unknown, run the **local-address** command to specify the IP address of another interface such as a loopback interface as the local IP address.
- If an interface bound to an IPSec policy is configured with one primary IP address and multiple secondary IP addresses, run the **local-address** command to specify one IP address as the local IP address.
- If the local and remote ends have equal-cost routes, run the **local-address** command to specify the local IP address so that IPSec packets can be sent out from the specified interface.

Precautions

The **local-address** at the local end must be the same as the **remote-address** at the remote end.

You do not need to specify **local-address** for an IKE peer referenced by an IPSec profile. During IKE negotiation, the IPSec profile uses the source addresses of the IPSec tunnel interface.

In a multi-link shared IPSec policy group scenario, the IP address of the local end cannot be the secondary IP address of a loopback interface. Otherwise, an IPSec tunnel cannot be established.

Example

Configure an IP address for the local end of IKE negotiation in the IKE peer view.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] local-address 10.10.10.1
```

Related Topics

12.6.75 ike peer

12.6.20 display ike peer (all views)

 Copyright © Huawei Technologies Co., Ltd.

12.6.117 local-id-type

Function

The **local-id-type** command sets the type of the local ID used in IKE negotiation.

The **undo local-id-type** command restores the default type of the local ID used in IKE negotiation.

By default, the local ID type used by IKE negotiation is IP.

Format

local-id-type { **dn** | **fqdn** | **ip** [**ip-configurable**] | **key-id** | **user-fqdn** }

undo local-id-type

Parameters

Parameter	Description	Value
dn	Specifies the Distinguished Name (DN) as the local ID.	-
fqdn	Specifies the name as the local ID.	-
ip	Specifies the IP address as the local ID.	-
ip-configurable	Indicates that the IP address used as the local ID is configurable. This IP address can be configured using the **local-id** command. The IP address is the local IP address used for IKE negotiation by default. This parameter takes effect only in the IKE peer view.	-
key-id	Specifies the key-id as the local ID. This parameter takes effect only in the Efficient VPN policy view.	-
user-fqdn	Specifies the USER-FQDN as the local ID.	-

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a protection mechanism for IKE negotiation. The device ensures security by confirming identities of communication parties. IKE peers can

 Copyright © Huawei Technologies Co., Ltd.

use different types. This command configures the type of the local ID of an IKE peer.

Precautions

- The local ID type can be different from the remote ID type. You can use commands to specify the local and remote ID types.
- If IKEv1 is used, pre-shared key authentication requires the local ID on the local end to be the same as the remote ID on the remote end. If IKEv2 is used, pre-shared key authentication requires the local ID type or local ID on the local end to be the same as the remote ID type or remote ID on the remote end.
- For RSA signature authentication, the remote ID type or remote ID on the local end must be consistent with corresponding fields in the local certificate on the remote end.

Different authentication methods support different ID types, as shown in **Table 12-65**.

 Copyright © Huawei Technologies Co., Ltd.

Table 12-65 Relationship between local IKE ID types, local ID, and authentication methods

Authentication Method	IP	DN	FQDN	USER-FQDN	key-id
pre-share	Supported The ID is the local IP address used for IKE negotiation by default. Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication.	Not supported	Supported Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication. The ID specified by the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication. The ID specified by the **local-id** command has a higher priority than the one specified by the **ike local-name** command.	Supported Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication. Set an ID using the **ike local-name** command, indicating that all peers on the device use this ID for identity authentication. The ID specified by the **local-id** command has a higher priority than the one specified by the **ike local-name** command.	Supported This parameter is often used when the device using the Efficient VPN policy functions as a remote end to communicate with Cisco devices.

 Copyright © Huawei Technologies Co., Ltd.

Authentication Method	IP	DN	FQDN	USER-FQDN	key-id
rsa-signature	Supported The ID is the local IP address used for IKE negotiation by default. Set an ID using the **local-id** command, indicating that the IKE peer uses this ID for identity authentication.	Supported Use the default ID in the certificate. No configuration is required.	Supported Use the default ID in the certificate. No configuration is required.	Supported Use the default ID in the certificate. No configuration is required.	Supported This parameter is often used when the device using the Efficient VPN policy functions as a remote end to communicate with Cisco devices.

Example

Set the local ID type of IKE peer **peer1** to FQDN.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id-type fqdn
```

Related Topics

12.6.20 display ike peer (all views)

12.6.30 display ipsec efficient-vpn

12.6.118 local-id

Function

The **local-id** command specifies the local ID for IKE negotiation.

The **undo local-id** command deletes the local ID for IKE negotiation.

By default, the local ID is not configured for IKE negotiation.

Format

local-id *id*

undo local-id

Parameters

Parameter	Description	Value
id	Specifies the local ID used in IKE negotiation	The value is a string of 1 to 255 case-sensitive characters.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

If the ID type of the IKE peer is **IP**, **FQDN**, or **USER-FQDN**, you can configure the local end identity in the system view or IKE peer view.

The **local-id** command sets an ID, indicating that the IKE peer uses this ID for authentication. If the ID type is FQDN or User-FQDN, the **12.6.71 ike local-name** command sets an ID, indicating that all peers on the device use this ID for authentication. The ID specified by the **local-id** command has a higher priority than the one specified by the **12.6.71 ike local-name** command.

Example

Set the local ID to be **huawei** in IKE negotiation.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id huawei
```

Related Topics

12.6.117 local-id-type

12.6.71 ike local-name

12.6.119 local-id-preference certificate enable

Function

The **local-id-preference certificate enable** command enables the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation.

The **undo local-id-preference certificate enable** command disables the device from preferentially obtaining the local ID from a field in a certificate when IKE uses certificate negotiation.

By default, the device does not preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Format

local-id-preference certificate enable

undo local-id-preference certificate enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When IKE uses certificate negotiation, the device can obtain its local ID from a field (IP address, FQDN, or email address) in the certificate, removing the need to configure the local ID.

After the **local-id-preference certificate enable** command is configured, the device preferentially obtains its local ID from a field in the certificate. If this method fails, it obtains its local ID based on the local configuration. If this method also fails, IKE negotiation fails.

Precautions

Before V500R005C00, the **local-id-preference certificate enable** command is supported only after a required patch is installed. By default, this command is disabled. In V500R005C00, this command is supported by default but is not displayed in the IKE peer view. In versions earlier than V5R5C20SPC500, this command is supported and displayed by default.

This command is not supported when the certificate negotiation mode is set to digital envelope authentication using the **authentication-method** command.

In IKEv2 negotiation scenarios, when both the **local-id-preference certificate enable** and **12.6.120 local-id-reflect enable** commands are configured, the **12.6.120 local-id-reflect enable** command takes effect.

You can run the **19.17.28 display pki certificate** command to view certificate identity information. The email address in the certificate corresponds to User-FQDN.

Example

Enable the device to preferentially obtain the local ID from a field in a certificate when IKE uses certificate negotiation.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei&gt; system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id-preference certificate enable
```

Related Topics

12.6.20 display ike peer (all views)

12.6.118 local-id

12.6.120 local-id-reflect enable

Function

The **local-id-reflect enable** command enables the function of using the local ID of the responder as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation.

The **undo local-id-reflect enable** command disables the function of using the local ID of the responder as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation.

By default, during IKEv2 negotiation, the local ID of the responder is not used as the remote ID carried in the IKE packets sent by the initiator.

Format

local-id-reflect enable

undo local-id-reflect enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During IKEv2 negotiation, if the user does not know the remote ID configured for the initiator, run the **local-id-reflect enable** command on the responder. When the responder receives an IKE packet from the initiator, the responder uses the IDr payload (remote ID) in the received packet as its local ID. If the responder does not obtain the IDr payload, it obtains its local ID based on the local configuration.

Precautions

This command is not supported when IKEv2 uses a digital envelope for authentication during certificate negotiation.

 Copyright © Huawei Technologies Co., Ltd.

When both the **local-id-reflect enable** and **12.6.119 local-id-preference certificate enable** commands are configured, the **local-id-reflect enable** command takes effect.

Currently, the ID type can only be IP address, FQDN, or User-FQDN.

Example

Enable the function of using the local ID of the responder as the remote ID carried in the IKE packets sent by the initiator during IKEv2 negotiation.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] local-id-reflect enable
```

Related Topics

12.6.20 display ike peer (all views)

12.6.118 local-id

12.6.136 remote-id

12.6.121 match ike-identity

Function

The **match ike-identity** command references an identity filter set.

The **undo match ike-identity** command removes the referenced identity filter set.

By default, no identity filter set is referenced.

Format

match ike-identity *identity-name*

undo match ike-identity

Parameters

Parameter	Description	Value
identity-name	Specifies the name of the identity filter set.	The value is an existing identity filter name.

Views

IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

1. During IKE negotiation, a device specifies the peer based on the identity filter set referenced in the policy template or IPSec profile.

   When the device functions as a responder, it can specify the peer allowed to connect to it to improve security.

2. In an IPSec over DSVPN application, multiple mGRE tunnel interfaces are configured on the hub which provides only one IP address for spoke access. The mGRE tunnel interfaces use the same source address or source interface; therefore, the hub cannot identify IKE packets from different mGRE tunnel interfaces. To solve this problem, set parameters in the identity filter set to specify the mGRE tunnel interface of each IKE packet.

   For details about DSVPN, see DSVPN Configuration.

Prerequisites

An identity filter set with a specific *identity-name* has been created using the **12.6.70 ike identity** command.

Precautions

- If you configure multiple IPSec policy templates and apply them to multiple interfaces on the same device, the parameters in the identity filter set referenced in different policy templates cannot be the same.
- If you configure multiple IPSec profiles and apply them to multiple tunnel interfaces on the same device, the parameters in the identity filter set referenced in different IPSec profiles cannot be the same.

If a remote device matches one parameter or more parameters in different identity filter sets in the local device, the access request of the remote device will be denied.

Example

Reference an identity filter set in the IPSec profile view.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] fqdn peer1
[Huawei-ike-identity-identity1] quit
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] match ike-identity identity1
```

Related Topics

12.6.70 ike identity

12.6.106 ipsec policy-template

12.6.108 ipsec profile (system view)

12.6.122 nat traversal

 Copyright © Huawei Technologies Co., Ltd.

Function

The **nat traversal** command enables NAT traversal.

The **undo nat traversal** command disables NAT traversal.

By default, the NAT traversal is enabled.

Format

nat traversal

undo nat traversal

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, if the initiator is located on a private network and the responder is located on the public network side. To ensure that an IPSec tunnel can be set up when the NAT device exists, NAT traversal needs to be configured.

NAT traversal allows ESP packets to pass through the NAT gateway during IKE negotiation.

Precautions

If NAT traversal is enabled, the IPSec proposal (**ipsec proposal**) supports only ESP.

Example

Enable NAT traversal in IKE peer named **peer1**.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] nat traversal
```

Related Topics

12.6.75 ike peer

12.6.20 display ike peer (all views)

12.6.123 pfs

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pfs** command enables Perfect Forward Secrecy (PFS) when the local end initiates negotiation.

The **undo pfs** command disables PFS when the local end initiates negotiation.

By default, PFS is not used when the local end initiates negotiation.

Format

pfs { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** | **dh-group19** | **dh-group20** | **dh-group21** }

undo pfs

Parameters

Parameter	Description	Value
dh-group1	Uses the 768-bit DH group.	-
dh-group2	Uses the 1024-bit DH group.	-
dh-group5	Uses the 1536-bit DH group.	-
dh-group14	Uses the 2048-bit DH group.	-
dh-group19	Uses the 256-bit Elliptic Curve Groups modulo a Prime (ECP) DH group.	-
dh-group20	Uses the 384-bit ECP DH group.	-
dh-group21	Uses the 521-bit ECP DH group.	-

Views

ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the local end initiates negotiation, there is an additional DH exchange in IKEv1 phase 2 or IKEv2 CREATE_CHILD_SA exchange. The additional DH exchange ensures security of the IPSec SA key and improves communication security.

Precautions

The **dh-group1**, **dh-group2**, and **dh-group5** have potential security risks. The other DH groups are recommended.

Table 12-66 describes the requirement for consistency of the PFS DH groups configured on the local and remote ends when the PFS function is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Table 12-66 Description of PFS DH groups

Security Policy Mode on the Local and Remote Ends	Description
IPSec policy in ISAKMP mode on both ends	The DH groups specified on the two ends must be the same; otherwise, the IPSec SA negotiation fails.
IPSec policy in ISAKMP mode on one end and IPSec policy configured using an IPSec policy template on the other end	• If PFS is enabled in the IPSec policy template: The DH groups specified on the two ends must be the same; otherwise, the IPSec SA negotiation fails. • If PFS is disabled in the IPSec policy template: The IPSec SA negotiation may succeed when the DH groups specified on the two ends are different. The responder uses the DH group on the initiator.
IPSec profile on both ends	The DH groups specified on the two ends must be the same; otherwise, the IPSec SA negotiation fails.

Example

Use PFS when the IPSec policy named **policy1** is used in negotiation.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] pfs dh-group14
```

Enable the PFS feature in the IPSec Efficient VPN policy **evpn**.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] pfs dh-group14
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.98 ipsec efficient-vpn (system view)

12.6.30 display ipsec efficient-vpn

12.6.34 display ipsec policy (all views)

12.6.124 pki realm

Function

The **pki realm** command binds a public key infrastructure (PKI) realm to an IKE peer or an Efficient VPN policy.

The **undo pki realm** command unbinds a PKI realm from an IKE peer or an Efficient VPN policy.

By default, no PKI realm is bound to an IKE peer or an Efficient VPN policy.

Format

pki realm *realm-name*

undo pki realm

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The PKI realm must already exist.

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A PKI realm is a set of identity information required when a PKI entity enrolls a certificate.

After a PKI realm is bound to an IKE peer or an Efficient VPN policy, the IKE peer can obtain the CA certificate and local certificate based on the PKI realm configuration.

Prerequisites

A PKI realm has been created using the **pki realm** command in the system view. And the CA certificate and local certificate have been imported in the PKI realm.

Example

Bind the PKI realm **test** to the IKE peer.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] pki realm test
```

Bind the PKI realm **test1** to the Efficient VPN policy.

```
<Huawei> system-view
[Huawei] pki realm test1
[Huawei-pki-realm-test1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] pki realm test1
```

Related Topics

12.6.75 ike peer

12.6.98 ipsec efficient-vpn (system view)

12.6.125 policy enable

Function

The **policy enable** command enables a policy in an IPSec policy group.

The **undo policy enable** command disables a policy in an IPSec policy group.

By default, all the policies in an IPSec policy group are enabled.

Format

policy enable

undo policy enable

Parameters

None

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

After you disable a policy, the policy is not used for tunnel establishment.

Example

Disable policy 1 in the IPSec policy group.

```
<Huawei> system-view
[Huawei] ipsec policy map1 1 isakmp
[Huawei-ipsec-policy-isakmp-map1-1] undo policy enable
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **pre-shared-key** command configures the pre-shared key used by IKE peers to perform pre-shared key authentication.

The **undo pre-shared-key** command deletes the pre-shared key used by IKE peers to perform pre-shared key authentication.

By default, the pre-shared key used by IKE peers to perform pre-shared key authentication is not configured.

Format

pre-shared-key { **simple** | **cipher** } *key*

undo pre-shared-key

Parameters

Parameter	Description	Value
simple	Indicates the pre-shared key in plain text. The pre-shared key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the pre-shared key in cipher text. You can enter a pre-shared key in plain text or cipher text, but the pre-shared key is displayed in cipher text in the configuration file.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key	Specifies the pre-shared key used by IKE peers to perform pre-shared key authentication.	The value is a string of case-sensitive characters without spaces. A plaintext key contains 1 to 128 characters, and a ciphertext key contains 48 to 188 characters. If the character string is enclosed in double quotation marks (" "), the character string can contain spaces. **NOTE** For security purposes, it is recommended that the pre-shared key contains at least 3 types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During IKE negotiation, IPSec can use pre-shared key authentication to verify identities of communication parties. After pre-shared key authentication is configured, the initiator encrypts data using the pre-shared key before transmitting the data, and the receiver decrypts the data using the same pre-shared key. If the receiver succeeds in data decryption, the initiator passes the identity verification.

Prerequisites

Pre-shared key authentication has been specified in an IKE proposal or in an Efficient VPN policy.

Precautions

Both ends of IKE negotiation must be configured with the same pre-shared key.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the pre-shared key used by IKE peers to perform pre-shared key authentication as **Test!123**.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] pre-shared-key cipher Test!123
```

Configure pre-shared key authentication in the Efficient VPN policy **evpn** and set the pre-shared key to **huawei@123** in cipher text.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] authentication-method pre-share
[Huawei-ipsec-efficient-vpn-evpn] pre-shared-key cipher huawei@123
```

Related Topics

12.6.75 ike peer

12.6.98 ipsec efficient-vpn (system view)

12.6.20 display ike peer (all views)

12.6.30 display ipsec efficient-vpn

12.6.127 pre-shared-key (IKE user view)

Function

The **pre-shared-key** command configures the pre-shared key used by IKE users when IKE peers use pre-shared key authentication during IKE negotiation.

The **undo pre-shared-key** command cancels the configuration.

By default, the pre-shared key used by IKE peers is not configured when IKE peers use pre-shared key authentication during IKE negotiation.

Format

pre-shared-key *key*

undo pre-shared-key

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key	Specifies the pre-shared key used by IKE users when IKE peers use pre-shared key authentication during IKE negotiation.	The value is a string of case-sensitive characters without spaces. A plaintext key contains 1 to 128 characters, and a ciphertext key contains 48 to 188 characters. If the character string is quoted by double quotation marks (" "), the character string can contain spaces. **NOTE** For security purposes, it is recommended that the pre-shared key contains at least 3 types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 6 characters.

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a point-to-multipoint scenario, the device functions as the VPN gateway of the headquarters, an IPSec policy is created using an IPSec policy template, and the VPN gateway receives IPSec connection setup requests of different branches. When the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak. To prevent this problem, you are advised to run the **id-type** and **pre-shared-key** commands in the view of the IKE user in the IKE user table.

An IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references an IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- After an IKE peer references an IKE user table, the pre-shared key configured by this command takes precedence over the pre-shared key configured by the **12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)** command.
- Pre-shared key authentication has been specified in an IKE proposal when IKE peers are configured.
- Both ends of IKE negotiation must use the same pre-shared key.

Example

Configure the pre-shared key as **Test!123** for IKE users.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] pre-shared-key Test!123
```

Related Topics

12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)

12.6.63 id-type

12.6.27 display ike user-table (all views)

12.6.128 prf

Function

The **prf** command configures the pseudo-random function (PRF) algorithm used in IKEv2 negotiation.

The **undo prf** command restores the default configuration.

By default, the HMAC-SHA2-256 PRF algorithm is used in IKEv2 negotiation.

Format

prf { **aes-xcbc-128** | **hmac-md5** | **hmac-sha1** | **hmac-sha2-256** | **hmac-sha2-384** | **hmac-sha2-512** }

undo prf

Parameters

Parameter	Description	Value
aes-xcbc-128	Indicates that the PRF algorithm is AES-XCBC-128. This algorithm applies only to IKEv2 negotiation.	-
hmac-md5	Indicates that the PRF algorithm is HMAC-MD5.	-
hmac-sha1	Indicates that the PRF algorithm is HMAC-SHA1.	-
hmac-sha2-256	Indicates that the PRF algorithm is HMAC-SHA2-256.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hmac-sha2-384	Indicates that the PRF algorithm is HMAC-SHA2-384.	-
hmac-sha2-512	Indicates that the PRF algorithm is HMAC-SHA2-512.	-

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

The PRF algorithm is required in IKEv2 negotiation. The PRFs are listed as follows from the highest security level to the lowest security level: **hmac-sha2-512** > **hmac-sha2-384** > **hmac-sha2-256** > **aes-xcbc-128** > **hmac-sha1** > **hmac-md5**.

If you run the **prf** command multiple times, only the latest configuration takes effect.

NOTE

hmac-md5 and **hmac-sha1** are not recommended due to their low security.

Example

Set hmac-sha2-256 as the PRF algorithm for IKEv2 proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] prf hmac-sha2-256
```

Related Topics

12.6.76 ike proposal

12.6.129 proposal

Function

The **proposal** command references an IPSec proposal.

The **undo proposal** command deletes the referenced IPSec proposal.

By default, no IPSec proposal is referenced.

Format

Manual IPSec policy view:

proposal *proposal-name*

undo proposal

 Copyright © Huawei Technologies Co., Ltd.

ISAKMP IPSec policy view, IPSec policy template view, and IPSec profile view:

proposal *proposal-name*

undo proposal [*proposal-name*]

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of the proposals.	It is a string of 1 to 15 case-insensitive characters.

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec proposal defines IPSec protection methods and takes effect only after an IPSec policy or profile references the IPSec proposal.

Prerequisites

An IPSec proposal has been created using the **ipsec proposal** command.

Precautions

A manual IPSec policy can only reference one IPSec proposal.

An ISAKMP IPSec policy, an IPSec policy template, or IPSec profile can reference a maximum of 12 IPSec proposals. When devices at both ends of an IPSec tunnel perform IKE negotiation, they search for IPSec proposals in sequence where IPSec proposals were configured until a matching IPSec proposal is found. If no matching IPSec proposal is found, an SA cannot be set up and packets to be protected are discarded.

Example

Set a proposal named **prop1**, and apply this proposal to the IPSec policy in manual mode named **policy1**.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] proposal prop1
```

Related Topics

12.6.109 ipsec proposal

12.6.105 ipsec policy (system view)
12.6.106 ipsec policy-template
12.6.108 ipsec profile (system view)

12.6.130 proposal (SA view)

Function

The **proposal** command applies a security proposal to a Security Association (SA).

The **undo proposal** command removes a security proposal from an SA.

By default, no security proposal is created.

Format

proposal *proposal-name*

undo proposal

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of a security proposal.	The value is a string of 1 to 15 case-insensitive characters.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SA defines a protection policy, and a security proposal defines a protection method. Data protection can be implemented only after a security proposal is applied to an SA.

Prerequisite

The **ipsec proto-protect proposal** *proposal-name* command has been run to create a security proposal before the **proposal** command is run. If no security proposal has been created, an error message will be displayed when the **proposal** command is run.

Configuration Impact

After the **proposal** command is run, the security proposal is applied to an SA and cannot be deleted.

 Copyright © Huawei Technologies Co., Ltd.

Example

Apply the security proposal named **prop1** to the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform ah
[Huawei-ipsec-proto-protect-proposal-prop1] quit
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] proposal prop1
```

12.6.131 qos group

Function

The **qos group** command configures the QoS group to which the IPSec packets belong.

The **undo qos group** command deletes the QoS group to which the IPSec packets belong.

By default, no QoS group is configured.

Format

qos group *qos-group-value*

undo qos group

Parameters

Parameter	Description	Value
qos-group-value	Specifies the ID of the QoS group.	The value is an integer that ranges from 1 to 99.

Views

Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, Efficient VPN policy view, GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both an IPSec policy and a QoS policy are used on an interface, you can run this command to specify the QoS group to which the IPSec packets belong to facilitate QoS management.

Precautions

This command takes effect in the packet encapsulation process but not the packet decapsulation process. That is, the command takes effect only for incoming packets.

Follow-up Procedure

After QoS for IPSec packets is enabled, run the **if-match qos-group** *qos-group-value* command in the traffic classifier view to configure a matching rule based on the QoS group.

Example

Configure the QoS group to which the IPSec packets belong in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos group 30
```

Related Topics

12.6.104 ipsec policy (interface view)

12.6.106 ipsec policy-template

12.6.107 ipsec profile (interface view)

12.6.98 ipsec efficient-vpn (system view)

12.6.132 qos pre-classify

Function

The **qos pre-classify** command enables pre-extraction of original IP packets.

The **undo qos pre-classify** command disables pre-extraction of original IP packets.

By default, pre-extraction of original IP packets is disabled.

Format

qos pre-classify

undo qos pre-classify

Parameters

None

Views

Tunnel interface view, Efficient VPN policy view, Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, GDOI policy view, BD view, VBDIF interface view, VPN instance view, Virtual template interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In tunnel mode, QoS parameters such as the packet header and protocol type in original packets are hidden after IP packets are encapsulated through GRE, VXLAN, L2TP, and IPSec. Although GRE, VXLAN, L2TP, and IPSec uses the DSCP field in original packets as the DSCP field in the IP packet header, some QoS solutions require quintuple information. The encryption device can pre-extract quintuple information including the source address, destination address, protocol type, source port number, and destination port number to facilitate refined QoS management on GRE, VXLAN, L2TP, and IPSec packets.

In an A2A VPN solution, the device uses the IP header of original packets as the IP header for encapsulated A2A VPN packets. Therefore, you do not need to configure this command if the device classifies packets based on the source address, destination address, or protocol type only.

Follow-up Procedure

After pre-extraction of original IP packets is enabled, run the **if-match acl** { *acl-number* | *acl-name* } command in the traffic classifier view to configure a matching rule based on the ACL.

Example

Enable pre-extraction of original IP packets in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos pre-classify
```

Related Topics

12.6.104 ipsec policy (interface view)

12.6.106 ipsec policy-template

12.6.107 ipsec profile (interface view)

12.6.98 ipsec efficient-vpn (system view)

12.6.133 re-authentication interval

Function

The **re-authentication interval** command sets the IKEv2 re-authentication interval.

The **undo re-authentication interval** command cancels the configuration.

By default, the device does not perform IKEv2 re-authentication.

Format

re-authentication interval *interval*

undo re-authentication interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the IKEv2 re-authentication interval. When about 70% of the time interval has elapsed, the device initiates IKEv2 re-authentication.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the remote access scenario, third-party attacks may occur during communications of peers. To improve IPSec network security, you can run this command to enable the peers to periodically re-authenticate each other.

Precautions

Only IKEv2 supports re-authentication.

Example

Set the re-authentication interval of an IKE peer to 400 seconds.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] re-authentication interval 400
```

Set the re-authentication interval to 400 seconds in the IPSec Efficient VPN policy.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] re-authentication interval 400
```

12.6.134 remote-address (IKE peer view)

Function

The **remote-address** command configures an IP address or domain name for the remote IKE peer during IKE negotiation.

The **undo remote-address** command cancels the configuration.

By default, no IP address or domain name is configured for the remote IKE peer during IKE negotiation.

Format

remote-address { [**vpn-instance** *vpn-instance-name*] { *ipv4-address* | **host-name** *host-name* } [**track** { **nqa** *admin-name test-name* | **bfd-session** *session-name* } { **up** | **down** }] | **authentication-address** *start-ipv4-address* [*end-ipv4-address*] }

undo remote-address [*ipv4-address* | **host-name** *host-name* | **authentication-address**]

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name. IPv4 multi-instance is supported.
ipv4-address	Specifies the IP address of the remote IKE peer.	The value is an IPv4 address in dotted decimal notation.
host-name *host-name*	Specifies the domain name of the remote IKE peer.	The value is an existing remote IKE peer domain name.
track	Specifies association between IKE and NQA or BFD.	-
nqa *admin-name test-name*	Configures association between IKE negotiation and NQA so that the device can determine whether the remote address of the peer is valid according to the NQA test instance status. *admin-name* specifies the administrator name of an NQA test instance, and *test-name* specifies the name of an NQA test instance.	The administrator name or name of an NQA test instance must have been created.
bfd-session *session-name*	Specifies association between IKE and BFD so that the peer address depends on the BFD session status. *bfd-session-name* specifies the name of the BFD session.	The BFD session name must have been created.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
up	Indicates that the local address is used as the peer address for negotiation when the NQA test instance or BFD session status is Up.	-
down	Indicates that the local address is used as the peer address for negotiation when the NQA test instance or BFD session status is Down.	-
authentication-address *start-ipv4-address* [*end-ipv4-address*]	Specifies the IP address before NAT as the authentication address. ● *start-ipv4-address*: Specifies the start IP address of the remote end. ● *end-ipv4-address*: Specifies the end IP address of the remote end.	The value is an IPv4 address in dotted decimal notation.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The remote address negotiated by the IKE peers has two types: IP address and domain name.

When the configured remote address is an IP address and the remote gateway IP address is fixed, set **remote-address** to a fixed IP address. When an IPSec policy template is used and the remote gateway address is not fixed, set **remote-address** to an IP address segment.

When a domain name is configured as the remote address, the device obtains the remote address in either of the following modes:

- Static mode: The device obtains the remote address based on the manually configured mapping between the domain name and IP address.
- Dynamic mode: The device obtains the remote address from the DNS server.

To improve network reliability, the headquarters provides four devices for branch gateways to access. In an IPSec policy, two remote IP addresses or domain names of the IKE peer can be configured on the branch gateway. The branch gateway attempts to use the first IP address or domain name to establish an IKE connection with the headquarters gateway. If the connection fails, the branch gateway uses the second IP address or domain name to establish an IKE connection, and so on.

If the IP address of the first IKE peer is unreachable in the scenario that two IP addresses are configured, the branch gateway uses the second IP address to establish an IKE connection only when establishing an IKE connection fails or the dead peer detection (DPD) fails. It takes a long time. To reduce the time required and determine validity of the IKE peer address in real time, configuring association between IKE negotiation and NQA or BFD to detect the link status and check validity of the IKE peer address based on the detection result.

In NAT traversal scenarios, when two ends use IKEv2, you can run the **remote-address authentication-address** *start-ipv4-address* [*end-ipv4-address*] command to specify the pre-NAT IP address or IP address segment as the authentication address if IP addresses need to be verified.

Prerequisites

- The VPN instance has been created using the **ip vpn-instance** command and the route distinguisher (RD) has been configured for the VPN instance using the **route-distinguisher** command if **vpn-instance** *vpn-instance-name* is specified.
- An NQA test instance has been created using the **nqa** command and the NQA test instance type has been set to ICMP using the **test-type** command if **nqa** *admin-name test-name* is specified.
- A BFD session has been created using the **bfd bind peer-ip** command and the BFD session has been set the local and remote discriminators using the **discriminator** command if **bfd-session** *bfd-session-name* is specified.

Precautions

- When an IPSec policy is used, if the local device functions as the initiator, run the **remote-address** command so that the initiator can use this address to search for the responder. Because both ends may be the initiator, run the **remote-address** command at both ends. The **remote-address** command is not required when the IKE peer functions as the responder and uses an IPSec policy template to establish an IPSec policy.
- You do not need to specify the **12.6.174 tunnel local** (local address) for the IKE peer referenced in an IPSec profile, because the local address is the source address of the GRE, mGRE or IPSec virtual tunnel interface. For the IKE peer referenced in an IPSec profile, **12.6.174 tunnel local** does not take effect.
- When applying an IPSec policy to a tunnel interface and running the **12.3.18 source** command to specify an IP address for the interface, you must run the **12.6.174 tunnel local** command to configure a tunnel local address. Otherwise, IKE negotiation will fail.

- When an IPSec profile is used, the destination address of the IPSec tunnel interface configured using the **destination** command is preferentially used as the remote address for IKE negotiation. When the **remote-address** and **destination** commands are configured at the same time, ensure that the configured IP addresses are the same; otherwise, IKE negotiation will fail. To implement IKE peer redundancy, do not configure the **destination** command on the IPSec tunnel interface. Instead, configure the **remote-address** command on the IKE peer referenced by the IPSec profile.
- The remote IP address (**remote-address**) at the local end must be the same as the local IP address (**local-address**) at the remote end.
- The VPN instance specified by *vpn-instance-name* must be the same as the VPN instance that is configured by the **ip binding vpn-instance** command and bound to the physical interface negotiating IPSec tunnel setup.
- If more than one remote IP address or domain name is configured, the specified *vpn-instance-name* must be the same.
- If multiple remote IP addresses are configured, the device with redundant addresses must function as the IKE negotiation initiator.

Example

Set the remote IP address of IKE peer **peer1** to 10.1.1.1.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] remote-address 10.1.1.1
```

Configure association between the IKE peer **huawei** with NQA and specify IP address 10.1.1.1 as the peer address for IKE negotiation when the NQA test instance (administrator name **admin** and instance name **test**) status is Up.

```
<Huawei> system-view
[Huawei] nqa test-instance admin test
[Huawei-nqa-admin-test] test-type icmp
[Huawei-nqa-admin-test] destination-address ipv4 10.1.1.1
[Huawei-nqa-admin-test] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] remote-address 10.1.1.1 track nqa admin test up
```

Configure association between the IKE peer **huawei** and BFD and use the IP address 10.1.1.2 as the peer address for IKE negotiation when the status of the BFD session **test** is Up.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] ip address 10.1.1.1 255.255.255.0
[Huawei-GigabitEthernet0/0/1] quit
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ip 10.1.1.2 interface gigabitethernet 0/0/1
[Huawei-bfd-session-test] discriminator local 10
[Huawei-bfd-session-test] discriminator remote 20
[Huawei-bfd-session-test] commit
[Huawei-bfd-session-test] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] remote-address 10.1.1.2 track bfd-session test up
```

Related Topics

12.6.75 ike peer
21.7.56 nqa

21.7.95 test-type
18.5.3 bfd bind peer-ip
18.5.18 discriminator
12.6.171 switch-back enable

12.6.135 remote-address (Efficient VPN policy view)

Function

The **remote-address** command configures an IP address or domain name for the remote IKE peer during IKE negotiation.

The **undo remote-address** command deletes an IP address or domain name for the remote IKE peer during IKE negotiation.

By default, no IP address or domain name is configured for the remote IKE peer during IKE negotiation.

Format

remote-address { *ip-address* | **host-name** *host-name* } { **v1** | **v2** }

undo remote-address [*ip-address* | **host-name** *host-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the remote IKE peer.	The value is in dotted decimal notation.
host-name *host-name*	Specifies the domain name of the remote IKE peer.	The value is an existing remote IKE peer domain name.
v1	Indicates that both ends use IKEv1.	-
v2	Indicates that both ends use IKEv2.	-

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **remote-address** command configures an IP address or domain name for the remote IKE peer in an Efficient VPN policy. If the domain name is configured for the remote IKE peer, the IP address of the remote IKE peer is obtained in either of the following modes:

- Static mode: The IP address of the remote IKE peer is obtained based on the mapping between the domain name and IP address.
- Dynamic mode: The IP address of the remote IKE peer is obtained from the DNS server.

To improve network reliability, two devices can be deployed at the headquarters to connect to the branch gateway. In an Efficient VPN solution, two IP addresses or domain names of the remote IKE peer can be configured on the branch gateway. The branch gateway first attempts to use the first configured IP address or domain name to establish an IKE connection with the headquarters gateway. If establishing an IKE connection fails, the branch gateway uses the second IP address or domain name to establish an IKE connection.

Precautions

When you configure IP addresses or domain names for two remote IKE peers, ensure that the value type of **remote-address** and the IKE version are respectively the same. Generally, only one device is deployed at the headquarters to connect to the branch gateway. Therefore, only one remote address is configured.

Example

Assign the IP addresses 10.1.1.1 and 10.1.2.1 to the remote peer in the Efficient VPN policy view.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] remote-address 10.1.1.1 v1
[Huawei-ipsec-efficient-vpn-evpn] remote-address 10.1.2.1 v1
```

Set the domain name of the remote peer to **mypeer** in the Efficient VPN policy view.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] remote-address host-name mypeer v1
```

Related Topics

12.6.98 ipsec efficient-vpn (system view)
12.6.30 display ipsec efficient-vpn

12.6.136 remote-id

Function

The **remote-id** command specifies the remote ID for IKE negotiation.

The **undo remote-id** command deletes the remote ID for IKE negotiation.

By default, the remote ID for IKE negotiation is not configured.

Format

remote-id *id*

undo remote-id

Parameters

Parameter	Description	Value
id	Specifies the remote ID.	The value is a string of 1 to 255 case-sensitive characters including special characters, such as the exclamation point (!), at sign (@), number sign (#), dollar sign ($), and percent (%).

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the remote ID type of the IKE peer is IP, DN, FQDN, or USER-FQDN, you can run this command to set a value for the remote ID.

During IKE negotiation, you can run the **remote-id-type** and **remote-id** commands to configure the remote ID type and remote ID for authentication.

Precautions

- In IKEv1, the configured remote ID is used to authenticate only the peer.
- In IKEv2, the configured remote ID can be sent to the peer to check whether the local ID of the peer is the same as this remote ID.

Example

Set the remote ID of IKE peer **peer1** when pre-shared key authentication is used and the remote ID type is FQDN or USER-FQDN.

```
# Set the remote end of the tunnel.
<Huawei_A> system-view
[Huawei_A] ike local-name device_A
# Set the local end of the tunnel.
<Huawei_B> system-view
[Huawei_B] ike peer peer1
[Huawei_B-ike-peer-peer1] remote-id device_A
```

 Copyright © Huawei Technologies Co., Ltd.

Set the remote ID of IKE peer **peer1** when digital signature authentication is used.

- If the remote ID type is **DN**, set the remote ID as follows:

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] remote-id /C=CN/ST=beijing
```

  If **remote-id** is set to the **subject** field in the certificate entity, the format is as follows: "/"+"subject". Note that spaces in the **subject** field are omitted and the comma is replaced by slash (/). For example, if the **subject** field is C=CN, ST=beijing, the command is **remote-id /C=CN/ST=beijing**.

- If the remote ID type is **FQDN**, set the remote ID as follows:

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] remote-id www.hw.com
```

- If the remote ID type is **USER-FQDN**, set the remote ID as follows:

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] remote-id user@hw.com
```

Set the remote peer name to **Huawei** in the Efficient VPN policy view.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn name mode client
[Huawei-ipsec-efficient-vpn-name] remote-id Huawei
```

Related Topics

12.6.20 display ike peer (all views)

12.6.30 display ipsec efficient-vpn

12.6.137 remote-id-type

Function

The **remote-id-type** command configures the remote ID type for IKE negotiation.

The **undo remote-id-type** command cancels the remote ID type.

By default, no remote ID type is configured.

Format

remote-id-type { **any** | **dn** | **fqdn** | **ip** | **user-fqdn** | **none** }

undo remote-id-type

Parameters

Parameter	Description	Value
any	Specifies that the remote ID can be of any type.	-
dn	Specifies the distinguished name (DN) as the remote ID.	-
fqdn	Specifies the host name of the remote end as the remote ID.	-

Parameter	Description	Value
ip	Specifies the IP address of the remote end as the remote ID.	-
user-fqdn	Specifies the user domain name of the remote end as the remote ID.	-
none	Specifies the remote ID type of an IKE peer as none. After this parameter is specified, the remote ID type and remote ID are not checked during IKE negotiation.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a protection mechanism for IKE negotiation. This mechanism ensures device security by confirming identities of communication parties. IKE peers can use different types of IDs. This command configures the remote ID type of an IKE peer.

Precautions

- The local ID type can be different from the remote ID type. You can use commands to specify the local and remote ID types.
- If IKEv1 is used, pre-shared key authentication requires the local ID on the local end to be the same as the remote ID on the remote end. If IKEv2 is used, pre-shared key authentication requires the local ID type or local ID on the local end to be the same as the remote ID type or remote ID on the remote end.
- For RSA signature authentication, the remote ID type or remote ID on the local end must be consistent with corresponding fields in the local certificate on the remote end.

Support for remote ID types and their configuration methods differ depending on the authentication modes. **Table 12-67** describes the details.

 Copyright © Huawei Technologies Co., Ltd.

Table 12-67 Relationships among the remote ID type, remote ID, and authentication mode

Authentication Mode	IP	DN	FQDN	USER-FQDN
Pre-shared key authentication (**pre-share**)	Supported To set a remote ID, run the **12.6.134 remote-address (IKE peer view)** command.	Not supported	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses this ID for identity authentication.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses this ID for identity authentication.
RSA signature authentication (**rsa-signature**)	Supported To set a remote ID, run the **12.6.134 remote-address (IKE peer view)** command.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses the ID of the corresponding field in the certificate for identity authentication.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses the ID of the corresponding field in the certificate for identity authentication.	Supported To set a remote ID, run the **remote-id** command. The remote IKE peer uses the ID of the corresponding field in the certificate for identity authentication.

Example

Set the remote ID type of IKE peer **peer1** to **FQDN** for pre-shared key authentication.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] remote-id-type fqdn
```

12.6.138 reset ike error-info

Function

The **reset ike error-info** command clears information about IPSec tunnel negotiation failures using IKE.

Format

reset ike error-info

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

You can run the **display ike error-info** command to view information about IPSec tunnel negotiation failures using IKE.

Example

Clear information about IPSec tunnel negotiation failures using IKE.

```
<Huawei> reset ike error-info
```

12.6.139 reset ike offline-info

Function

The **reset ike offline-info** command clears information about deleted IPSec tunnels established through IKE negotiation.

Format

reset ike offline-info

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

You can run the **display ike offline-info** command to check the reasons why IPSec tunnels established through IKE negotiation have been deleted.

Example

Clear information about deleted IPSec tunnels established using IKE negotiation.

```
<Huawei> reset ike offline-info
```

12.6.140 reset ike sa

Function

The **reset ike sa** command clears information about SAs established through IKE negotiation.

Format

reset ike sa [**conn-id** *conn-id* | **remote** *ipv4-address*]

Parameters

Parameter	Description	Value
conn-id *conn-id*	Specifies the connection ID of an SA.	The value is an integer that ranges from 1 to 4294967295.
remote *ipv4-address*	Specifies the IPv4 address of the remote end.	The value is in dotted decimal notation.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To clear an IPSec tunnel established through IKE negotiation, run the **reset ike sa** command to clear the IKE SA that is used to negotiate the IPSec tunnel.

There are two types of SAs established by IKE negotiation: IKE SAs in phase 1 and IPSec SAs in phase 2. IKE SAs in phase 1 are used for IKE negotiation. Under the protection of these IKE SAs, IPSec SAs in phase 2 are used to protect data flows.

- If the specified *conn-id* parameter corresponds to an IKE SA in phase 1, IKE peers do not automatically negotiate an IKE SA after the IKE SA is cleared. The IKE peers re-negotiate an IKE SA in phase 1 only when data flows match ACL rules in the IPSec policy again.
- If the specified *conn-id* parameter corresponds to an IPSec SA in phase 2, either of the following will occur:
  - Automatic triggering mode: The IKE peers re-negotiate an IPSec SA in phase 2 under the protection of the IKE SA in phase 1 after the IPSec SA is cleared.
  - Traffic-based triggering mode: The IKE peers do not automatically negotiate an IPSec SA after the IPSec SA is cleared. They re-negotiate an IPSec SA in phase 2 under the protection of the IKE SA in phase 1 only when data flows match ACL rules in the IPSec policy again.
- If the *conn-id* parameter is not specified, all IKE SAs in phase 1 are cleared, and IKE negotiation process is similar to that described above.

Precautions

When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the command is run. After all the SAs are cleared, the CPU usage restores to the normal range.

After dependency between IPSec SA and IKE SA during IKEv1 negotiation is disabled using the **undo ikev1 phase1-phase2 sa dependent** command, running the **reset ike sa** *conn-id* command to delete an IKE SA will also delete the corresponding IPSec SA.

Example

Clear IKE SAs in both phases.

```
<Huawei> reset ike sa
```

Related Topics

12.6.24 display ike sa

12.6.141 reset ike statistics

Function

The **reset ike statistics** command clears IKE statistics.

Format

reset ike statistics

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored after being cleared.

To diagnose and locate faults of IPSec tunnels established using IKE, you can collect IKE statistics in a given period of time. You can run the **reset ike statistics** command to clear historical IKE statistics before starting statistics collection. You can then run the **display ike statistics** command to check IKE statistics.

Example

Clear IKE statistics.

```
<Huawei> reset ike statistics
```

12.6.142 reset ipsec history record

Function

The **reset ipsec history record** command clears history information about IPSec tunnels.

Format

reset ipsec history record

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored once being cleared.

You can run the **12.6.31 display ipsec history record** command to view history information about the current IPSec tunnel.

Example

Clear history information about IPSec tunnels.

```
<Huawei> reset ipsec history record
```

12.6.143 reset ipsec sa

Function

The **reset ipsec sa** command deletes IPSec SAs.

Format

reset ipsec sa [**remote** *ipv4-address* | **policy** *policy-name* [*seq-number*] | **parameters** *ipv4-address* { **ah** | **esp** } *spi* | **efficient-vpn** *efficient-vpn-name* | **profile** *profile-name*]

Parameters

Parameter	Description	Value
remote *ipv4-address*	Specifies the IPv4 address of the remote end.	The value is in dotted decimal notation.
policy *policy-name* [*seq-number*]	Specifies the name and sequence number of an IPSec policy. If *sequence-number* is not specified, all the IPSec policies in the IPSec policy group with the specified name are used.	The value must be an existing IPSec policy name or sequence number.
profile *profile-name*	Specifies the name of an IPSec profile. If **profile** is not specified, IPSec SAs established using all IPSec profiles are deleted.	The value must be an existing IPSec profile name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
parameters *ipv4-address* { **ah** | **esp** } *spi*	Specifies the three elements that uniquely identify an IPSec SA. The three elements are *ipv4-address* (destination address), *protocol* (AH or ESP), and Security Parameter Index (SPI). To reset an SA, the three elements must be specified. If **parameters** is not specified, IPSec SAs established using any security protocol are deleted.	The three elements are described as follows: • *ipv4-address*: IPv4 address. • *protocol*: AH or ESP. • *spi*: an integer that ranges from 256 to 4294967295.
efficient-vpn *efficient-vpn-name*	Specifies the name of an Efficient VPN policy.	The value is an existing Efficient VPN policy name.

Views

User view

Default Level

3: Management level

Usage Guidelines

When you run the **reset ipsec sa** command to delete IPSec SAs, note the following points:

- When the number of IPSec tunnels is larger than 50% of the maximum limit, high CPU usage alarms may be generated in a short period of time after the command is run. After all the SAs are cleared, the CPU usage restores to the normal range.
- If no parameter is specified, all IPSec SAs are deleted.
- If **parameters** is specified, the IPSec SAs in two directions are deleted simultaneously.
- If a manually created IPSec SA is deleted, the IKE peers automatically create a new IPSec SA based on the manually configured parameters.
- To delete IPSec SAs established through IKE negotiation, you must run the **reset ipsec sa** and **12.6.140 reset ike sa** commands in sequence. Otherwise, IPSec SAs established through IKE negotiation fail to be deleted. After the IPSec SAs are deleted, IKE peers re-negotiate IPSec SAs only when packets trigger IKE negotiation.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete all the IPSec SAs.

```
<Huawei> reset ipsec sa
```

Delete the IPSec SA with remote IP address 10.1.1.2.

```
<Huawei> reset ipsec sa remote 10.1.1.2
```

Delete all IPSec SAs created through IPSec policy group **policy1**.

```
<Huawei> reset ipsec sa policy policy1
```

Delete the IPSec SA with IPSec policy name **policy1** and sequence number 10.

```
<Huawei> reset ipsec sa policy policy1 10
```

Delete the IPSec SA whose remote IP address is 10.1.1.2, security protocol is AH, and SPI is 10000.

```
<Huawei> reset ipsec sa parameters 10.1.1.2 ah 10000
```

Delete the IPSec SA established through IPSec profile **profile1**.

```
<Huawei> reset ipsec sa profile profile1
```

Related Topics

12.6.44 display ipsec sa

12.6.144 reset ipsec statistics

Function

The **reset ipsec statistics** command deletes statistics about IPSec packets.

Format

reset ipsec statistics

Parameters

None.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics about IPSec packets within a given period of time, run this command to delete existing statistics.

Precautions

The deleted statistics about IPSec packets cannot be restored. Exercise caution when you run this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete statistics about all IPSec packets.

```
<Huawei> reset ipsec statistics
```

Related Topics

12.6.46 display ipsec statistics

12.6.145 reset ipsec statistics route

Function

The **reset ipsec statistics route** command clears IPSec route injection statistics.

Format

reset ipsec statistics route

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

NOTICE

Statistics cannot be restored once being cleared.

When locating IPSec route injection problems, you can collect the IPSec route injection statistics only within a specified period for fault location. Before collecting the statistics, run the **reset ipsec statistics route** command to clear the historical statistics and then run the **12.6.47 display ipsec statistics route** command to view IPSec route statistics.

Example

Clear IPSec route injection statistics.

```
<Huawei> reset ipsec statistics route
```

 Copyright © Huawei Technologies Co., Ltd.

12.6.146 reset ipsec proto-protect statistics

Function

The **reset ipsec proto-protect statistics** command clears statistics about packets processed by IPSec.

Format

reset ipsec proto-protect statistics [**sa-name** *sa-name*]

Parameters

Parameter	Description	Value
sa-name *sa-name*	Specifies the IPSec Security Association (SA) name.	The value is an existing IPSec Security Association name.

Views

User view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Before collecting statistics about packets processed by IPSec in a specified length of time, you can run the **reset ipsec proto-protect statistics** command to clear the original statistics.

Follow-up Procedure

Run the **display ipsec proto-protect statistics** command to check statistics about packets processed by IPSec.

Precautions

The statistics cannot be restored after being cleared. Therefore, confirm the action before running this command.

Example

Clear statistics about packets processed by IPSec.

```
<Huawei> reset ipsec proto-protect statistics
```

12.6.147 respond-only enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **respond-only enable** command configures the local end as the IPSec responder that does not initiate IPSec negotiation.

The **undo respond-only enable** command cancels the configuration.

By default, if the local end establishes an IPSec tunnel using the ISAKMP IPSec policy, the local end initiates IPSec negotiation.

Format

respond-only enable

undo respond-only enable

Parameters

None

Views

ISAKMP IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

If the IPSec peers establish IPSec tunnels using the ISAKMP IPSec policy, both ends initiate negotiation. You can configure one end as the responder that does not initiate negotiation, which can help you check the packet processing, and therefore diagnose and locate IPSec faults.

Example

Configure the peer in ISAKMP IPSec policy **policy1** with sequence number 100 as the responder for IPSec negotiation.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] respond-only enable
```

12.6.148 resource acl

Function

The **resource acl** command defines subnet information of the headquarters on the Efficient VPN server.

The **undo resource acl** command cancels the configuration.

By default, no subnet information of the headquarters is defined on the Efficient VPN server.

 Copyright © Huawei Technologies Co., Ltd.

Format

resource acl *acl-number*

undo resource acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an advanced ACL.	The value is an integer that ranges from 3000 to 3999.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Efficient VPN server delivers headquarters network information defined in an ACL to the remote device. The ACL defines the headquarters subnets that branches can access. Traffic not destined for the subnets specified in the ACL is directly forwarded to the Internet. Such traffic does not pass through the IPSec tunnel.

When an Efficient VPN policy is configured, this command is used on the Efficient VPN server. You can reference the IKE peer on the Efficient VPN server to implement ACL delivery.

Prerequisites

An advanced ACL has been created.

Precautions

This command is only valid for IKEv1.

The sum of ACL rules pushed by the headquarters and ACL rules configured on the branch cannot exceed 512. Otherwise, the IPSec tunnels cannot be established.

Example

Configure ACL 3100 that defines headquarters subnet information on the IPSec Efficient VPN server.

```
<Huawei> system-view
[Huawei] acl 3100
[Huawei-acl-adv-3100] rule 5 permit ip source 10.1.1.0 0.0.0.255
[Huawei-acl-adv-3100] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] resource acl 3100
```

12.6.149 route accept

Function

The **route accept** command configures the device to generate routes based on the received subnet route information and define the priority and tag value for the routes.

The **undo route accept** command disables the function that generates routes based on the received subnet route information.

By default, the device does not generate routes based on the received subnet route information.

Format

route accept [**preference** *preference-number*] [**tag** *tag-value*]

undo route accept

Parameters

Parameter	Description	Value
preference *preference-number*	Specifies the priority for the route generated based on the received subnet route information.	The value is an integer that ranges from 1 to 255.
tag *tag-value*	Specifies the tag value for the route generated based on the received subnet route information.	The value is an integer that ranges from 1 to 4294967295.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When virtual tunnel interfaces are used for IPSec tunnel setup, you can run this command to allow the local device to accept subnet route information sent by the remote device.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The local device can accept subnet route information sent by the remote device only when both the **route accept** command and the **config-exchange set accept** command are configured.

NOTE

This command is supported by IKEv2 only.

Example

Configure the IKE peer named **peer1** to accept subnet route information sent by the remote device and set the priority and tag value of the generated route to 20 and 256 respectively.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] route accept preference 20 tag 256
```

Related Topics

12.6.75 ike peer

12.6.11 config-exchange

12.6.150 route inject

Function

The **route inject** command configures route injection.

The **undo route inject** command cancels the configuration.

By default, route injection is not configured.

Format

route inject [**nexthop** *ipv4-address*] { **static** | **dynamic** } [**preference** *preference*]

undo route inject

Parameters

Parameter	Description	Value
nexthop *ipv4-address*	Specifies the next-hop IPv4 address to the remote end.	The value is in dotted decimal notation.
static	Enables static route injection. The parameter is only available in the ISAKMP IPSec policy view.	-
dynamic	Enables dynamic route injection.	-

Parameter	Description	Value
preference *preference*	Specifies the priority of a static route generated through route injection.	The value is an integer that ranges from 1 to 255. The default value is 60.

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an enterprise headquarters and its branch establish an IPSec tunnel, a static route to the branch subnet needs to be configured on the headquarters gateway. If there are many branch subnets, a large number of static routes need to be configured on the headquarters gateway. When branch subnets change, the static route configuration needs to be modified on the headquarters gateway, causing a difficulty in network maintenance. Route injection injects routes to branch subnets to the headquarters gateway based on IPSec tunnel information, which reduces manual configuration and improves configuration correctness. Route injection can also inject routes to headquarters subnets to the branch gateway based on IPSec tunnel information, implementing association between IPSec tunnel subnet information and routes.

Route injection works in two modes:

- Static mode: The generated static route is added to the local device immediately, and is independent of IPSec tunnel status change.
- Dynamic mode: If the IPSec tunnel is Up, the generated static route can be added to the local device. If the IPSec tunnel is Down, the generated static route can be deleted from the local device.

  Compared with static route injection, dynamic route injection is relevant to the IPSec tunnel status. Dynamic route injection prevents IPSec peers from sending IPSec packets over the IPSec tunnel in Down state, reducing packet loss.

You can configure a priority for the static route generated through route injection. For example, when there is another route to the same destination as the static route, specify the same priority for the routes so that traffic can be load balanced. If different priorities are specified for the routes, the routes can back up each other.

Precautions

Only IPSec SAs established in IKE negotiation mode support the route injection function. Manually configured IPSec SAs do not support the route injection function.

 Copyright © Huawei Technologies Co., Ltd.

The device does not support the route injection function when a Layer 2 interface is added to an IPSec policy group.

After the next hop is specified using the **route inject nexthop** command, the generated route is not used for IPSec packet forwarding if the IPSec tunnel remote address is not within the destination network segment of the injected route.

Example

Set the priority of a static route generated through route injection to 10.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] route inject static preference 10
```

Related Topics

12.6.105 ipsec policy (system view)
12.6.106 ipsec policy-template

12.6.151 rsa encryption-padding

Function

The **rsa encryption-padding** command configures a padding mode for RSA encryption.

The **undo rsa encryption-padding** command restores the default padding mode for RSA encryption.

By default, the padding mode of RSA encryption is OAEP.

Format

rsa encryption-padding { **oaep** | **pkcs1** }

undo rsa encryption-padding

Parameters

Parameter	Description	Value
oaep	Set the padding mode of RSA encryption to Optimal Asymmetric Encryption Padding (OAEP).	-
pkcs1	Sets the padding mode of RSA encryption to Public-Key Cryptography Standards 1 (PKCS1).	-

Views

IKE peer view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

On an IPSec-enabled network, identity authentication can be performed using an RSA digital envelope. When the padding mode of RSA encryption is set to PKCS1, there are security risks. To improve network security, run the **rsa encryption-padding** command to set the padding mode of RSA encryption to OAEP.

Example

Set the padding mode of RSA encryption to OAEP.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] rsa encryption-padding oaep
```

Related Topics

12.6.20 display ike peer (all views)

12.6.152 rsa signature-padding

Function

The **rsa signature-padding** command configures a padding mode for the RSA signature.

The **undo rsa signature-padding** command restores the default padding mode for the RSA signature.

By default, the padding mode of the RSA signature is PSS.

Format

rsa signature-padding { **pkcs1** | **pss** }

undo rsa signature-padding

Parameters

Parameter	Description	Value
pkcs1	Sets the padding mode of the RSA signature to Public-Key Cryptography Standards 1 (PKCS1).	-
pss	Sets the padding mode of the RSA signature to Probabilistic Signature Scheme (PSS).	-

Views

IKE peer view, Efficient VPN policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

On an IPSec-enabled network, identity authentication can be performed using an RSA signature or digital envelope. When the padding mode of the RSA signature in the certificate is set to PKCS1, there are security risks. To improve network security, run the **rsa signature-padding** command to set the padding mode of the RSA signature to PSS.

Example

Set the padding mode of the RSA signature to PSS.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] rsa signature-padding pss
```

Related Topics

12.6.20 display ike peer (all views)

12.6.153 sa authentication-hex

Function

The **sa authentication-hex** command configures an authentication key for an IPSec SA in hexadecimal notation.

The **undo sa authentication-hex** command cancels the configuration.

By default, the authentication key is not configured for an IPSec SA.

Format

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } { **simple** | **cipher** } *hex-string*

undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Sets an authentication key for the inbound IPSec SA. IPSec uses the inbound IPSec SA to process incoming packets.	-
outbound	Sets an authentication key for the outbound IPSec SA. IPSec uses the outbound IPSec SA to process outgoing packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ah	Sets an authentication key using the AH protocol. If the IPSec proposal referenced in an IPSec policy uses the AH protocol, the authentication key is set based on the *ah* keyword.	-
esp	Sets an authentication key using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-
simple	Indicates plain text authentication key. Type in an authentication key in plain text. The authentication key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the cipher authentication key. You can enter an authentication key in plain text or cipher text. The authentication key is displayed in cipher text in the configuration file.	-
hex-string	Sets an authentication key for the IPSec SA.	The value is in the hexadecimal format. ● If MD5 is used, the key length is 16 bytes. ● If SHA1 is used, the key length is 20 bytes. ● If SHA2-256 is used, the key length is 32 bytes. ● If SHA2-384 is used, the key length is 48 bytes. ● If SHA2-512 is used, the key length is 64 bytes.

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When manually configuring an IPSec policy, you must configure an authentication key for the inbound/outbound IPSec SA. The authentication key can be a hexadecimal number or a character string.

- The **sa authentication-hex** command sets an authentication key in hexadecimal notation.
- The **sa string-key** command sets a character string as the authentication key.

If two keys in different formats are configured, the key configured later takes effect.

Precautions

The inbound authentication key on the local end must be the same as the outbound authentication key on the remote end. The outbound authentication key on the local end must be the same as the inbound authentication key on the remote end.

The authentication key on both ends of an IPSec tunnel must use the same format. For example, an IPSec SA cannot be established if the authentication key on one end is a character string but that on the other end is a hexadecimal number.

Example

In IPSec policy **policy1** using AH and SHA2-256 on the local device, set the SPI and authentication key of the inbound IPSec SA to 10000 and 0x112233445566778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00; set the SPI and authentication key of the outbound IPSec SA to 20000 and 0xaabbccddeeff001100aabbccddeeff0011223344556677889 9aabbccddeeff00.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex inbound ah cipher
112233445566778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex outbound ah cipher
aabbccddeeff001100aabbccddeeff0011223344556677889 9aabbccddeeff00
```

In IPSec policy **policy1** using AH and SHA2-256 on the remote device, set the SPI and authentication key of the inbound IPSec SA to 20000 and 0xaabbccddeeff001100aabbccddeeff0011223344556677889 9aabbccddeeff00; set the SPI and authentication key of the outbound IPSec SA to 10000 and 0x112233445566778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
```

```
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex inbound ah cipher
aabbccddeeff001100aabbccddeeff00112233445566778899aabbccddeeff00
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa authentication-hex outbound ah cipher
112233445566778899aabbccddeeff00aabbccddeeff001100aabbccddeeff00
```

Related Topics

12.6.105 ipsec policy (system view)

12.6.164 sa string-key

12.6.154 sa authentication-hex (SA view)

Function

The **sa authentication-hex** command sets an authentication in hexadecimal format or cipher text for Security Associations (SAs).

The **undo sa authentication-hex** command deletes an authentication key from SAs.

By default, no authentication key is created.

Format

sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] { *hex-plain-key* | *hex-cipher-key* }

undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa authentication-hex** command.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa authentication-hex** command.	-
cipher	Indicates the ciphertext used for authentication.	-
hex-plain-key	Sets the authentication password to be in plaintext format.	The value is in hexadecimal notation. ● If authentication algorithm Message Digest 5 (MD5) is used, the length of the key is 16 bytes. ● If authentication algorithm Secure Hash Algorithm-1 (SHA-1) is used, the length of the key is 20 bytes. ● If authentication algorithm SHA2-256 is used, the length of the key is 32 bytes.
hex-cipher-key	Sets the authentication password to be in ciphertext format.	The value is a string of case-insensitive characters, spaces not supported. ● If authentication algorithm MD5 is used, the length of the key is 68. ● If authentication algorithm SHA-1 is used, the length of the key is88. ● If authentication algorithm SHA2-256 is used, the length of the key is108.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH and ESP can use either MD5, SHA-1, or SHA-2 that require an authentication key in the string or hexadecimal format. If an authentication key in the hexadecimal format is required, run the **sa authentication-hex** command.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

SA parameters on both IPSec peers must be identical. The authentication key for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

The authentication key can be in the hexadecimal or string format. To configure an authentication key in the string format, run the **sa string-key** command. If multiple authentication keys are configured, the latest one takes effect. The formats of authentication keys on both IPSec peers must be identical. If an authentication key in the string format is configured on one end and an authentication key in the hexadecimal format on another end, the two ends cannot communicate.

Example

Configure an authentication key in the hexadecimal format for the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] sa authentication-hex inbound ah abcdeF1234567891abcdeF1234567891
```

12.6.155 sa binding vpn-instance

Function

The **sa binding vpn-instance** command binds a VPN instance to an IPSec tunnel.

The **undo sa binding vpn-instance** command deletes a VPN instance from an IPSec tunnel.

By default, no VPN instance is bound to an IPSec tunnel.

Format

sa binding vpn-instance *vpn-instance-name*

undo sa binding vpn-instance

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance to be bound to an IPSec tunnel.	The value must be an existing VPN instance name.

Views

IKE peer view, manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When multiple branches connected to the headquarters network across the Internet using IPSec, you can run the **sa binding vpn-instance** command to bind each VPN instance to an IPSec tunnel, thereby isolating traffic of different branches.

When configuring IPSec multi-instance, note the following points:

- If an IPSec policy is created using IKE and no VPN instance is specified, run the **sa binding vpn-instance** command in the IKE peer view to specify the VPN instance bound to the IPSec tunnel. The bound domain must be the same as the domain bound to the virtual interface that is generated during VPN instance creation.
- If an IPSec policy is created manually, run the **sa binding vpn-instance** command in the manual IPSec policy view to specify the VPN instance bound to the IPSec tunnel.
- In IPsec multi-instance, the security zone of decapsulated packets shall be identified with the decrypted packets inspection function. Therefore, the decrypted packets inspection function shall be enabled.

Prerequisites

The VPN instance has been created using the **ip vpn-instance** command and the route distinguisher (RD) has been configured for the VPN instance using the **route-distinguisher** command.

Precautions

The VPN instance specified by the **sa binding vpn-instance** command must be the same as the VPN instance bound to the ACL referenced by the IPSec tunnel.

Example

Configure the VPN instance **vpna** that IPSec tunnel traffic belongs to in the IPSec policy in manual mode.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpna
[Huawei-vpn-instance-vpna] ipv4-family
[Huawei-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpna-af-ipv4] quit
[Huawei-vpn-instance-vpna] quit
[Huawei] ipsec policy policy1 100 manual
[Huawei-ipsec-policy-manual-policy1-100] sa binding vpn-instance vpna
```

Related Topics

12.6.34 display ipsec policy (all views)

12.6.20 display ike peer (all views)

12.6.156 sa binding vpn-instance (Efficient VPN policy view)

Function

The **sa binding vpn-instance** command binds a VPN instance to an IPSec tunnel.

The **undo sa binding vpn-instance** command unbinds a VPN instance from an IPSec tunnel.

By default, no VPN instance is bound to an IPSec tunnel.

Format

sa binding vpn-instance *vpn-instance-name*

undo sa binding vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance bound to an IPSec tunnel.	The value is an existing VPN instance name.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Applicable environment

On an MPLS VPN with small VPN sites, if CEs and PEs are connected through the Internet but not leased lines, hosts connected to a CE can access resources on another VPN site only through the insecure Internet. To enhance access security,

 Copyright © Huawei Technologies Co., Ltd.

these hosts can connect to the backbone network of the MPLS VPN through an IPSec tunnel.

This command specifies the VPN that the remote end of the IPSec tunnel belongs to. The tunnel initiator then can obtain the outbound interface and send packets through the outbound interface.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

A route distinguisher (RD) for the VPN instance has been configured using the **route-distinguisher** command.

Example

Bind the VPN instance **vpna** to the Efficient VPN policy **evpn**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpna
[Huawei-vpn-instance-vpna] ipv4-family
[Huawei-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpna-af-ipv4] vpn-target 100:100
[Huawei-vpn-instance-vpna-af-ipv4] quit
[Huawei-vpn-instance-vpna] quit
[Huawei] ipsec efficient-vpn evpn mode client
[Huawei-ipsec-efficient-vpn-evpn] sa binding vpn-instance vpna
```

Related Topics

12.6.98 ipsec efficient-vpn (system view)

12.6.30 display ipsec efficient-vpn

12.6.157 sa duration (IKE proposal view)

Function

The **sa duration** command specifies the IKE SA hard lifetime for an IKE proposal.

The **undo sa duration** command restores the default IKE SA hard lifetime.

By default, the IKE SA hard lifetime is 86400 seconds.

Format

sa duration *seconds*

undo sa duration

Parameters

Parameter	Description	Value
seconds	Specifies the IKE SA hard lifetime. IKE SA is automatically updated after the hard lifetime expires.	The value is an integer that ranges from 60 to 604800, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

IKE proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the SA lifetime is set, SAs are updated in real time and difficult to decipher, enhancing security.

The IKE SA lifetime is classified as follows:

- Hard lifetime (hard timeout period): specifies the lifetime of an IKE SA.

  When two devices negotiate an IKE SA, the actual hard lifetime is the smaller of the two values configured on the two devices.
- Soft lifetime (soft timeout period): refers to the time after which a new IKE SA is negotiated so that the new IKE SA will be ready before the hard lifetime of the original IKE SA expires.

  Table 12-68 lists the default soft lifetime values.

  Table 12-68 Soft lifetime values

IKE Protocol Type	Description
IKEv1	70% of the actual hard SA lifetime
IKEv2	65% to 75% of the actual hard SA lifetime

Before an IKE SA becomes invalid, IKE negotiates a new IKE SA for the remote end. The remote end uses the new IKE SA to protect IPSec communication immediately after the new IKE SA is negotiated. If service traffic is transmitted, the original IKE SA is deleted immediately. If no service traffic is transmitted, the original IKE SA will be deleted after 10s or the hard lifetime expires.

Precautions

IKE negotiation requires DH calculation, which takes a long time. Therefore, you are advised to set the IKE SA hard lifetime to a value longer than 10 minutes to make sure that the update of IKE SAs does not affect secure communication.

During IKEv1 negotiation, the responder cannot initiate IKE SA renegotiation after the IKE SA soft lifetime expires.

Example

Set the IKE SA hard lifetime to 600 seconds for IKE proposal 10.

```
<Huawei> system-view
[Huawei] ike proposal 10
[Huawei-ike-proposal-10] sa duration 600
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.6.22 display ike proposal (All views)

12.6.158 sa duration (ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view)

Function

The **sa duration** command sets the hard lifetime of IPSec SAs in an IPSec policy or profile.

The **undo sa duration** command restores the default configuration.

By default, the hard lifetime of IPSec SAs is not configured in an IPSec policy or profile. The system uses the global hard lifetime of IPSec SAs.

Format

sa duration { **traffic-based** *kilobytes* | **time-based** *seconds* }

undo sa duration { **traffic-based** | **time-based** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
traffic-based *kilobytes*	Specifies the traffic-based SA hard lifetime. It is recommended that the traffic volume be equal to or larger than the size of IPSec traffic forwarded in 1 hour.	The value is 0 or an integer from 256 to 200000000, in Kbytes. ● IKEv1 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, both the local and remote devices disable the traffic timeout function. ● IKEv2 for IPSec negotiation: If the traffic hard lifetime is set to 0 on either device, the local device disables the traffic timeout function. During IPSec negotiation between a Huawei device and a Cisco device using IKEv1: ● If the Huawei device functions as the initiator and the traffic hard lifetime is set to 0, the traffic hard lifetime value pushed by the Cisco device takes effect on the local end. ● If the Huawei device functions as the responder and the traffic hard lifetime is set to 0, the value 0 takes effect on the local end.
time-based *seconds*	Specifies the time-based SA hard lifetime. When a large number of IPSec tunnels are established between two devices, you are advised to set the IPSec SA hard lifetime to a value larger than or equivalent to 1800s.	The value is an integer that ranges from 30 to 604800, in seconds.

Views

ISAKMP IPSec policy view, IPSec policy template view, IPSec profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For a dynamic SA, configure the SA hard lifetime so that the SA can be updated in real time, reducing the crash risk and improving security.

There are two methods to measure the lifetime:

- Time-based lifetime

  The period from when an SA is set up to when the SA is expired.
- Traffic-based lifetime

  The maximum volume of traffic that this SA can process.

The lifetime is classified as follows:

- Hard lifetime: specifies the lifetime of an IPSec SA.

  When two devices negotiate an IPSec SA, the actual hard lifetime is the smaller of the two values configured on the two devices.
- Soft lifetime: specifies the time after which a new IPSec SA is negotiated so that the new IPSec SA will be ready before the hard lifetime of the original IPSec SA expires.

  Table 12-69 lists the default soft lifetime values.

Table 12-69 Soft lifetime values

Soft Lifetime Type	Description
Time-based soft lifetime (soft timeout period)	The value is 70% of the actual hard lifetime (hard timeout period).
Traffic-based soft lifetime (soft timeout traffic)	• For IKEv1, the value is 70% of the actual hard lifetime (hard timeout traffic). • For IKEv2, the value is 65% to 75% of the actual hard lifetime (hard timeout traffic) plus or minus a random value.

Before an IPSec SA becomes invalid, IKE negotiates a new IPSec SA for the remote end. The remote end uses the new IPSec SA to protect IPSec communication immediately after the new IPSec SA is negotiated. If service traffic is transmitted, the original IPSec SA is deleted immediately. If no service traffic is transmitted, the original IPSec SA will be deleted after 10s or the hard lifetime expires.

If the time-based lifetime and traffic-based lifetime are both set for an IPSec SA, the IPSec SA becomes invalid when either lifetime expires.

Precautions

The SA lifetime can be configured globally (**12.6.113 ipsec sa global-duration**) or based on an IPSec policy or profile. If no SA lifetime is configured for the IPSec policy or profile, the global lifetime is used. If both the global SA lifetime and lifetime based on the IPSec policy or profile are configured, the latter one takes effect.

 Copyright © Huawei Technologies Co., Ltd.

You only need to specify the SA lifetime for the SA setup through the IKE negotiation. That is, it is invalid to the SA manually set up. The manually set up SA is effective permanently.

During IKEv1 negotiation:

- The responder cannot initiate IPSec SA renegotiation after the IPSec SA soft lifetime expires.
- The initiator cannot initiate IPSec SA renegotiation when its IKE SA is deleted and the IPSec SA soft lifetime expires.

During IKEv2 negotiation, the initiator or responder cannot initiate IPSec SA renegotiation if the IKE SA is deleted and the IPSec SA soft lifetime expires.

Example

Set the IPSec SA hard lifetime in IPSec policy **policy1** to 7200 seconds.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] sa duration time-based 7200
```

Set the IPSec SA hard lifetime in IPSec policy **policy2** to 20000 KB.

```
<Huawei> system-view
[Huawei] ipsec policy policy2 1 isakmp
[Huawei-ipsec-policy-isakmp-policy2-1] sa duration traffic-based 20000
```

Set the IPSec SA hard lifetime in IPSec profile **profile1** to 7200 seconds.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] sa duration time-based 7200
```

Set the IPSec SA hard lifetime in IPSec profile **profile1** to 20000 KB.

```
<Huawei> system-view
[Huawei] ipsec profile profile1
[Huawei-ipsec-profile-profile1] sa duration traffic-based 20000
```

12.6.159 sa encryption-hex

Function

The **sa encryption-hex** command configures an encryption key for an IPSec SA.

The **undo sa encryption-hex** command cancels the configuration.

By default, the encryption key is not configured for an IPSec SA.

Format

sa encryption-hex { **inbound** | **outbound** } **esp** { **simple** | **cipher** } *hex-string*

undo sa encryption-hex { **inbound** | **outbound** } **esp**

Parameters

Parameter	Description	Value
inbound	Sets an encryption key for the inbound IPSec SA. IPSec uses the inbound IPSec SA to process incoming packets.	-
outbound	Sets an encryption key for the outbound IPSec SA. IPSec uses the outbound IPSec SA to process outgoing packets.	-
esp	Sets an encryption key using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-
simple	Indicates the encryption key in plain text. The encryption key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the encryption key in cipher text. You can enter an authentication key in plain text or cipher text. The encryption key is displayed in cipher text in the configuration file.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hex-string	Sets an encryption key for the IPSec SA.	The value is a hexadecimal number. ● If DES is used, the key length is 8 bytes. ● If 3DES is used, the key length is 24 bytes ● If AES-128 is used, the key length is 16 bytes. ● If AES-192 is used, the key length is 24 bytes. ● If AES-256 is used, the key length is 32 bytes. ● If SM4 is used, the key length is 16 bytes.

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **sa encryption-hex** command applies to manually created IPSec policies only. You do not need to set an encryption key for an IPSec SA established through IKE negotiation, because IKE peers automatically negotiate the encryption key.

Precautions

When configuring manual IPSec policies, you must set encryption keys for the IPSec SAs in **inbound** and **outbound** directions. The inbound encryption key on the local end must be the same as the outbound encryption key on the remote end. The outbound encryption key on the local end must be the same as the inbound encryption key on the remote end.

Example

In IPSec policy **policy1** using ESP and AES-256, set the SPI and encryption key of the inbound IPSec SA to 10000 and 0x1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef; set the SPI and encryption key of the outbound IPSec SA to 20000 and 0xabcdefabcdef1234abcdefabcdef1234abcdefabcdef1234abcdefabcdef1234.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
```

```
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] proposal prop1
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound esp 10000
[Huawei-ipsec-policy-manual-policy1-1] sa encryption-hex inbound esp cipher
1234567890abcdef1234567890abcdef1234567890abcdef1234567890abcdef
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound esp 20000
[Huawei-ipsec-policy-manual-policy1-1] sa encryption-hex outbound esp cipher
abcdefabcdef1234abcdefabcdef1234abcdefabcdef1234abcdefabcdef1234
```

12.6.160 sa encryption-hex (SA view)

Function

The **sa encryption-hex** command configures an encryption key for manual Security Association (SA) in hexadecimal format.

The **undo sa encryption-hex** command deletes an encryption key for manual SA configured in hexadecimal format.

By default, no encryption key is created.

Format

sa encryption-hex { **inbound** | **outbound** } **esp** [**cipher**] { *hex-plain-key* | *hex-cipher-key* }

undo sa encryption-hex { **inbound** | **outbound** } **esp**

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa encryption-hex** command.	-
cipher	Indicates the ciphertext used for encryption.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hex-plain-key	Sets the authentication password to be in plaintext format.	The value is in hexadecimal notation. ● If encryption algorithm Data Encryption Standard (DES) is used, the length of the key is 8 bytes. ● If encryption algorithm Triple Data Encryption Standard (3DES) is used, the length of the key is 24 bytes. ● If encryption algorithm Advanced Encryption Standard 128 (AES-128) is used, the length of the key is 16 bytes. ● If encryption algorithm AES-192 is used, the length of the key is 24 bytes. ● If encryption algorithm AES-256 is used, the length of the key is 32 bytes.
hex-cipher-key	Sets the authentication password to be in ciphertext format.	The value is a string of case-insensitive characters, spaces not supported. ● If encryption algorithm DES is used, the length of the key is 48. ● If encryption algorithm 3DES is used, the length of the key is 88. ● If encryption algorithm AES-128 is used, the length of the key is 68. ● If encryption algorithm AES-192 is used, the length of the key is 88. ● If encryption algorithm AES-256 is used, the length of the key is 108.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ESP security protocol support encryption of IP packets. The algorithm used for encryption/decryption is either DES, 3DES or AES. These algorithms need a key either in hexadecimal format to operate. The hexadecimal key to be used for encryption is configured using the **sa encryption-hex** command.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If **sa encryption-hex** command is configured, then the encryption key configured using **sa string-key** command is deleted automatically.

Example

Configure an encryption key in the hexadecimal format for the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] sa encryption-hex inbound esp abcdabcdabcdabcd
```

12.6.161 sa keep-holding-to hard-duration

Function

The **sa keep-holding-to hard-duration** command configures the device to delete the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation.

The **undo sa keep-holding-to hard-duration** command configures the device to delete the original IPSec SA immediately after it uses the new IPSec SA to transmit data during IPSec SA re-negotiation.

By default, during IPSec SA re-negotiation, the device deletes the original IPSec SA immediately after using the new IPSec SA to transmit data.

Format

sa keep-holding-to hard-duration

undo sa keep-holding-to hard-duration

Parameters

None

Views

ISAKMP IPSec policy view, IPSec policy template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a new IPSec SA is negotiated, if the peer device still uses the original IPSec SA to transmit data while the local device deletes the original IPSec SA immediately after using the new IPSec SA to transmit data, the IPSec SAs on the two devices will be different. This will cause IPSec traffic interruption. In this case, you are advised to run the **sa keep-holding-to hard-duration** command to enable the local device to delete the original IPSec SA after the hard lifetime expires.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

This command takes effect only for IPSec SAs established through IKEv1 negotiation.

Example

Configure the device to delete the original IPSec SA after the hard lifetime expires during IPSec SA re-negotiation.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 isakmp
[Huawei-ipsec-policy-isakmp-policy1-1] sa keep-holding-to hard-duration
```

Related Topics

12.6.34 display ipsec policy (all views)
12.6.36 display ipsec policy-template (all views)

12.6.162 sa spi

Function

The **sa spi** command configures a Security Parameter Index (SPI) for an IPSec SA.

The **undo sa spi** command cancels the configuration.

By default, the SPI of an IPSec SA is not configured.

Format

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Sets an SPI for the inbound IPSec SA.	-
outbound	Sets an SPI for the outbound IPSec SA.	-
ah	Sets an SPI using the AH protocol. If the IPSec proposal referenced in an IPSec policy uses the AH protocol, the authentication key is set based on the *ah* keyword.	-
esp	Sets an SPI using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
spi-number	Sets an SPI for the IPSec SA.	The value is an integer that ranges from 256 to 4294967295.

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec SA is uniquely identified by a triplet, including the SPI, destination IP address, and security protocol number (AH or ESP). The receiver uses the SPI to identify the binding between a data flow and an IPSec SA.

When manually configuring an IPSec policy, you must specify the SPIs for inbound and outbound SAs. The inbound SPI on the local end must be the same as the outbound SPI on the remote end. The outbound SPI on the local end must be the same as the inbound SPI on the remote end.

Precautions

This command applies to manually created IPSec policies only. You do not need to set an SPI for an IPSec SA established through IKE negotiation, because IKE peers automatically negotiate the SPI.

Example

In IPSec policy **policy1** using AH and SHA2-256 on the local device, set the SPI of the inbound IPSec SA to 10000; set the SPI of the outbound IPSec SA to 20000.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 20000
```

In IPSec policy **policy1** using AH and SHA2-256 on the remote device, set the SPI of the inbound IPSec SA to 20000; set the SPI of the outbound IPSec SA to 10000.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 10000
```

12.6.163 sa spi (SA view)

Function

The **sa spi** command configures the Security Parameter Index (SPI) for a Security Association (SA).

The **undo sa spi** command deletes the SPI from an SA.

By default, no SPI is configured.

Format

sa spi { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa spi** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa spi** command.	-
spi-number	Specifies the SPI.	The value is an integer ranging from 256 to 4294967295.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

SPI uniquely identifies an SA. When an SPI is configured for an SA, the SPI is carried in each sent packet. The receiver checks the packet authenticity based on

 Copyright © Huawei Technologies Co., Ltd.

the SPI. When the **ipsec sa** *sa-name* command is used to create an SA, run the **sa spi** command to configure the SPI.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

The SPI for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

Example

Set the SPI for the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] sa spi inbound ah 10000
[Huawei-ipsec-sa-sa1] sa spi outbound ah 20000
```

12.6.164 sa string-key

Function

The **sa string-key** command configures a character string as an authentication key for an IPSec SA.

The **undo sa string-key** command cancels the configuration.

By default, the authentication key is not configured for an IPSec SA.

Format

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } { **simple** | **cipher** } *string-key*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Sets an authentication key for the inbound IPSec SA.	-
outbound	Sets an authentication key for the outbound IPSec SA.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ah	Sets an authentication key using the AH protocol. If the IPSec proposal referenced in an IPSec policy uses the AH protocol, the authentication key is set based on the *ah* keyword.	-
esp	Sets an authentication key using the ESP protocol. If the IPSec proposal referenced in an IPSec policy uses the ESP protocol, the authentication key is set based on the *esp* keyword.	-
simple	Indicates plain text authentication key. Type in an authentication key in plain text. The authentication key is displayed in plain text in the configuration file. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the cipher authentication key. You can enter an authentication key in plain text or cipher text. The authentication key is displayed in cipher text in the configuration file.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
string-key	Sets an authentication key for the IPSec SA.	The value is a string of case-sensitive characters without question marks (?) and spaces. The value is a string of 1 to 255 characters in plain text or 48 to 348 characters in cipher text. **NOTE** To ensure security, the authentication key must meet the minimum complexity requirement. That is, the authentication key must be a combination of three of the following: uppercase letters, lowercase letters, digits, and special characters (such as !, @, #, $, and %).

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an authentication algorithm is specified in the IPSec proposal referenced by a manually created IPSec policy, you must configure an authentication key for the inbound/outbound SA. The inbound authentication key on the local end must be the same as the outbound authentication key on the remote end. The outbound authentication key on the local end must be the same as the inbound authentication key on the remote end.

The authentication key can be a hexadecimal number or a character string.

- The **sa string-key** command sets a character string as the authentication key.
- The **sa authentication-hex** command sets an authentication key in hexadecimal notation.

If two keys in different formats are configured, the key configured later takes effect.

Precautions

The **sa string-key** command applies to manually created IPSec policies only. You do not need to set an authentication key for an IPSec SA established through IKE negotiation, because IKE peers automatically negotiate the authentication key.

The authentication key on both ends of an IPSec tunnel must use the same format. For example, an IPSec SA cannot be established if the authentication key on one end is a character string but that on the other end is a hexadecimal number.

Example

In IPSec policy **policy1** using AH and SHA2-256 on the local device, set the SPI and authentication key of the inbound IPSec SA to 10000 and **Test@123**; set the SPI and authentication key of the outbound IPSec SA to 20000 and **Test@456**.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key inbound ah cipher Test@123
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key outbound ah cipher Test@456
```

In IPSec policy **policy1** using AH and SHA2-256 on the remote device, set the SPI and authentication key of the inbound IPSec SA to 20000 and **Test@456**; set the SPI and authentication key of the outbound IPSec SA to 10000 and **Test@123**.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] transform ah
[Huawei-ipsec-proposal-prop1] ah authentication-algorithm sha2-256
[Huawei-ipsec-proposal-prop1] quit
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] sa spi inbound ah 20000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key inbound ah cipher Test@456
[Huawei-ipsec-policy-manual-policy1-1] sa spi outbound ah 10000
[Huawei-ipsec-policy-manual-policy1-1] sa string-key outbound ah cipher Test@123
```

12.6.165 sa string-key (SA view)

Function

The **sa string-key** command configures an authentication key in the string format.

The **undo sa string-key** command deletes an authentication key from Security Associations (SAs).

By default, no authentication key is created.

Format

sa string-key { **inbound** | **outbound** } { **ah** | **esp** } [**cipher**] *string-cipher-key*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

Parameters

Parameter	Description	Value
inbound	Specifies SA parameters for incoming packets.	-
outbound	Specifies SA parameters for outgoing packets.	-
ah	Specifies SA parameters for Authentication Header (AH). If the security proposal applied to an SA uses AH, **ah** must be configured in the **sa string-key** command.	-
esp	Specifies SA parameters for Encapsulating Security Payload (ESP). If the security proposal applied to an SA uses ESP, **esp** must be configured in the **sa string-key** command.	-
cipher	Indicates the ciphertext used for authentication.	-
string-cipher-key	Specifies the ciphertext key.	The value is a string of case-sensitive characters that can be letters or digits. The authentication password can be a string of 1 to 127 characters in simple text or a string of 20 to 392 characters in encrypted text. Except the question mark (?) and space. However, when quotation marks (") are used around the string, spaces are allowed in the string.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AH and ESP can use either Message Digest 5 (MD5), Secure Hash Algorithm 1 (SHA-1) or SHA-2, that require an authentication key in the string or hexadecimal format. If an authentication key in the string format is required, run the **sa string-key** command.

Precautions

Set parameters for both **inbound** and **outbound** SAs.

SA parameters on both IPSec peers must be identical. The authentication key for incoming packets on the local end must be identical with that for outgoing packets on the peer end and vice versa.

The authentication key can be in the hexadecimal or string format. To configure an authentication key in the hexadecimal format, run the **sa authentication-hex** command. If multiple authentication keys are configured, the latest one takes effect. The formats of authentication keys on both IPSec peers must be identical. If an authentication key in the string format is configured on one end and an authentication key in the hexadecimal format on another end, the two ends cannot communicate.

Example

Set an authentication key in the string format for the SA named **sa1**.

```
<Huawei> system-view
[Huawei] ipsec sa sa1
[Huawei-ipsec-sa-sa1] sa string-key inbound esp Hello-13579
[Huawei-ipsec-sa-sa1] sa string-key outbound esp Huawei-13579
```

12.6.166 sa trigger-mode

Function

The **sa trigger-mode** command configures a mode in which IPSec tunnel setup is triggered.

The **undo sa trigger-mode** command restores the default mode in which IPSec tunnel setup is triggered.

By default, the IPSec tunnel trigger mode is **auto**.

Format

sa trigger-mode { **auto** | **traffic-based** }

undo sa trigger-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
auto	Indicates that IPSec tunnel setup is triggered automatically.	-
traffic-based	Indicates that IPSec tunnel setup is triggered by traffic.	-

Views

ISAKMP IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

If **auto** is specified, IPSec tunnel setup is triggered automatically. If **traffic-based** is specified, an IPSec tunnel is triggered by outgoing data flows matching the IPSec policy.

Example

Set the mode in which IPSec tunnel setup is triggered to **traffic-based**.

```
<Huawei> system-view
[Huawei] ipsec policy test 10 isakmp
[Huawei-ipsec-policy-isakmp-test-10] sa trigger-mode traffic-based
```

12.6.167 security acl

Function

The **security acl** command specifies an ACL to be referenced in an IPSec policy or IPSec policy template.

The **undo security acl** command cancels the configuration.

By default, an IPSec policy or IPSec policy template does not reference an ACL.

Format

security acl *acl-number* [**dynamic-source**]

undo security acl

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.
dynamic-source	Indicates that the IP address of the applied interface in the IPSec policy replaces the source IP address in its referenced ACL. This parameter is only valid in IPSec policy view.	-

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **security acl** command references an ACL that defines data flows to be protected by IPSec. In practice, you need to configure rules in an ACL to define data flows to be protected and apply the ACL to an IPSec policy to protect the data flows.

When an IPSec policy is created using an IPSec policy template, you can determine whether to define data flows to be protected by IPSec on the responder.

- If data flows to be protected by IPSec are not specified on the responder, the responder accepts the range of data flows to be protected by IPSec defined on the initiator.
- If data flows to be protected by IPSec are specified on the responder, the configuration on the responder must mirror that on the initiator or the range of protected data flows on the responder must contain the range of protected data flows on the initiator.

Precautions

To reference an ACL in an IPSec policy, ensure that rules must be configured in this ACL view and the number of rules configured in this ACL view does not exceed 256. Otherwise, this ACL cannot be referenced in this IPSec policy.

After an IPSec tunnel has been established, if both permit and deny actions are configured in an ACL rule in the IPSec policy template view, the deny action does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Reference ACL 3100 in a manually created IPSec policy.

```
<Huawei> system-view
[Huawei] acl number 3100
[Huawei-acl-adv-3100] rule permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.1.2 0.0.0.0
[Huawei-acl-adv-3100] quit
[Huawei] ipsec policy policy1 100 manual
[Huawei-ipsec-policy-manual-policy1-100] security acl 3100
```

Reference ACL 3101 in an Efficient VPN policy.

```
<Huawei> system-view
[Huawei] acl number 3101
[Huawei-acl-adv-3101] rule permit tcp source 10.1.1.1 0.0.0.0 destination 10.1.1.2 0.0.0.0
[Huawei-acl-adv-3101] quit
[Huawei] ipsec efficient-vpn name mode network
[Huawei-ipsec-efficient-vpn-name] security acl 3101
```

12.6.168 service-scheme

Function

The **service-scheme** command specifies a service scheme referenced by an IKE peer.

The **undo service-scheme** command deletes a service scheme referenced by an IKE peer.

By default, an IKE peer does not reference any service scheme.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme.	The service scheme name must already exist.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an Efficient VPN scenario, the customer wants to deploy network resources including the DNS domain name, DNS server address, WINS server address, and IP

addresses on the server end (headquarters gateway). The server end pushes network resource information to remote ends (branch gateways) to simplify configuration and maintenance of network resources on them. In this case, run the **service-scheme** command to specify a service scheme referenced by an IKE peer. After this command is configured, remote ends are authorized based on network resource information pushed by the server end.

Prerequisites

A service scheme has been created by running the **service-scheme** *service-scheme-name* command.

Example

Configure the service scheme **service** referenced by an IKE peer.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme service
[Huawei-aaa-service-service] quit
[Huawei-aaa] quit
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] service-scheme service
```

Related Topics

12.6.20 display ike peer (all views)

12.6.169 service-scheme (Efficient VPN policy view)

Function

The **service-scheme** command configures a server-end service scheme in an Efficient VPN policy.

The **undo service-scheme** command deletes a server-end service scheme from an Efficient VPN policy.

By default, no server-end service scheme is configured in an Efficient VPN policy.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme on the server end.	The service scheme name must already exist.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

In an Efficient VPN scenario, the customer wants to deploy network resources including the DNS domain name, DNS server address, WINS server address, and IP addresses on the server end (headquarters gateway). The server end pushes network resource information to remote ends (branch gateways) to simplify configuration and maintenance of network resources on them.

Remote ends are authorized based on network resource information pushed by the server end or the server-end AAA service scheme specified in an Efficient VPN policy. To use the AAA service scheme, run the **service-scheme** command to configure a server-end service scheme in an Efficient VPN policy and run the **local-id-type** command to specify the **key-id** parameter. Otherwise, the configuration does not take effect.

Example

Configure the server-end service scheme **service** in an Efficient VPN policy.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn name mode network
[Huawei-ipsec-efficient-vpn-name] service-scheme service
```

Related Topics

12.6.30 display ipsec efficient-vpn

12.6.170 sim-based-username

Function

The **sim-based-username** command configures the user name and password of the remote device for authentication by the RADIUS server.

The **undo sim-based-username** command deletes the user name and password of the remote device for authentication by the RADIUS server.

By default, the user name and password of the remote device for authentication by the RADIUS server are not configured.

Format

sim-based-username type { **imei** | **imsi** } **password** *password*

undo sim-based-username

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
type { **imei** | **imsi** }	Obtains the corresponding user name by the type. ● **imei**: indicates that the type of the user name is International Mobile Equipment Identity (IMEI). ● **imsi**: indicates that the type of the user name is International Mobile Subscriber Identity (IMSI).	-
password *password*	Sets the password of the remote device for authentication by the RADIUS server.	The value is a string of case-sensitive characters. It cannot contain question marks (?) or spaces. The *password* is in plain text containing 9 to 32 characters or in cipher text containing 48 to 68 characters. **NOTE** To improve the security, it is recommended that the certificate revocation password contains at least two types of lowercase letters, uppercase letters, digits, and special characters, and contains at least 9 characters.

Views

Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

When the remote device establishes an IKE SA with the RADIUS server, the remote device needs to be authenticated and authorized by the RADIUS server. The remote device needs to send the user name and password to the RADIUS server. The remote device can obtain the user name based on the user name type configured using this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the user name type and password of the remote device for authentication by the RADIUS server to **IMSI** and **Huawei@1234**.

```
<Huawei> system-view
[Huawei] ipsec efficient-vpn evpn mode network-auto-cfg
[Huawei-ipsec-efficient-vpn-evpn] sim-based-username type imsi password Huawei@1234
```

12.6.171 switch-back enable

Function

The **switch-back enable** command enables revertive switching of an IKE peer.

The **undo switch-back enable** command disables revertive switching of an IKE peer.

By default, revertive switching of an IKE peer is disabled.

Format

switch-back enable

undo switch-back enable

Parameters

None

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a live network, to improve network reliability, the headquarters provides two devices to connect to the branch. On the branch gateway, two IP addresses or domain names are configured for an IKE peer to establish connections with the headquarters. Normally, the branch gateway connects to the primary headquarters gateway. When the primary headquarters gateway becomes unreachable, the branch gateway connects to the secondary headquarters gateway to prevent traffic loss. After the primary headquarters gateway recovers, you need to run the **switch-back enable** command to enable revertive switching to the primary headquarters gateway.

Precautions

The **12.6.134 remote-address (IKE peer view)** command must also be executed to configure an IKE peer to perform redundancy switching according to the NQA test instance status or the BFD session status. The switching function takes effect

 Copyright © Huawei Technologies Co., Ltd.

based on the NQA test instance status change or BFD session status change instead of based on the detection result.

Example

Configure revertive switching of the IKE peer **huawei**.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] switch-back enable
```

12.6.172 transform

Function

The **transform** command specifies a security protocol used in an IPSec proposal.

The **undo transform** command restores the default configuration.

By default, an IPSec proposal uses the ESP protocol.

Format

transform { **ah** | **ah-esp** | **esp** }

undo transform

Parameters

Parameter	Description	Value
ah	Indicates that the IPSec proposal uses the Authentication Header (AH) protocol.	-
ah-esp	Indicates that the IPSec proposal encapsulates packets through ESP, then through AH.	-
esp	Indicates that the IPSec proposal uses the ESP protocol.	-

Views

IPSec proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Three security modes are available and their differences are as follows:

- In the AH mode, devices only authenticate packets.
- In the ESP mode, devices provide packet authentication, encryption, or both functions.
- In the AH-ESP mode, devices use the AH protocol to authenticate packets and the ESP protocol to encrypt packets. During IPSec encapsulation, devices encapsulate packets using ESP and then AH. During IPSec decapsulation, devices decapsulate packets using AH and then ESP.

AH prevents data tampering but cannot prevent data from being listened to, so it applies only to the transmission of non-confidential data. ESP provides authentication service inferior to that of AH, but it can encrypt packet payloads.

Precautions

The IPSec proposals configured on both ends of an IPSec tunnel must use the same security protocol.

Example

Set the security protocol used in IPSec proposal **newprop1** to AH.

```
<Huawei> system-view
[Huawei] ipsec proposal newprop1
[Huawei-ipsec-proposal-newprop1] transform ah
```

12.6.173 transform (ipsec-proto-protect-proposal view)

Function

The **transform** command configures the security protocol in a security proposal.

The **undo transform** command restores the default security protocol.

By default, the Encapsulating Security Payload (ESP) protocol is used, as defined in RFC 2406.

Format

transform { **ah** | **esp** }

undo transform

Parameters

Parameter	Description	Value
ah	Configures Authentication Header (AH) as the security protocol.	-
esp	Configures ESP as the security protocol.	-

Views

IPSec proto-protect proposal view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on packet encryption and authentication at the IP layer, IPSec ensures the integrity, authenticity, and confidentiality of packets transmitted on networks. IPSec uses two protocols, AH and ESP, for data authentication and encryption.

- AH: provides data origin and integrity authentication.
- ESP: provides data origin and integrity authentication and data encryption.

Configuration Impact

When multiple security proposals are configured, the latest configuration takes effect, and the default authentication and encryption algorithms will be restored.

NOTE

AH uses the authentication algorithm SHA2-256 by default. ESP uses the authentication algorithm SHA2-256 and the encryption algorithm AES 128 by default.

Follow-up Procedure

Configure the authentication algorithm for AH when AH is used.

Configure the authentication and encryption algorithms for ESP when ESP is used.

Precautions

The security protocols on both IPSec peers must be identical.

Example

Configure AH for the security proposal named **prop**.

```
<Huawei> system-view
[Huawei] ipsec proto-protect proposal prop1
[Huawei-ipsec-proto-protect-proposal-prop1] transform ah
```

12.6.174 tunnel local

Function

The **tunnel local** command specifies the local address of an IPSec tunnel.

The **undo tunnel local** command cancels the configuration.

By default, no local IP address is configured for the IPSec tunnel.

Format

tunnel local { *ipv4-address* | **applied-interface** }

undo tunnel local

Parameters

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address for the local end of an IPSec tunnel.	The value is in dotted decimal notation.
applied-interface	Indicates the primary IP address of the IPSec-enabled interface is used as the local address of an IPSec tunnel. **NOTE** This parameter takes effect only in the ISAKMP IPSec policy view.	-

Views

Manual IPSec policy view, ISAKMP IPSec policy view, IPSec policy template view, Efficient VPN policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify a start point for an IPSec tunnel.

For a manually created IPSec policy, you must run the **tunnel local** *ipv4-address* command to configure an IP address for the local end before you can create an SA. Only after correct IP addresses are configured for the local end (start point) and remote end (end point), an IPSec tunnel can be established between the two ends.

For the IKE negotiation mode, you do not need to configure an IP address for the local end of an IPSec tunnel. During SA negotiation, the device will select a proper address based on route information. The local address needs to be configured in the following situations:

- If the IP address of the interface to which an IPSec policy is applied varies or is unknown, run the **tunnel local** *ipv4-address* command to specify the IP address of another interface (such as the loopback interface) on the device as the IP address for the local end of an IPSec tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the IP address of the interface to which an IPSec policy is applied as the local address of an IPSec tunnel.
- If the interface to which an IPSec policy is applied has multiple IP addresses (one primary IP address and several secondary IP addresses), run the **tunnel local** *ipv4-address* command to specify one of these IP addresses as the IP address for the local end of an IPSec tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the primary IP address of the interface as the local address of an IPSec tunnel.
- If equal-cost routes exist between the local and remote ends, run the **tunnel local** command to specify a local IP address for an IPSec tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- If an IPSec policy is created manually, **tunnel local** on the local end must be the same as the **tunnel remote** on the remote end.
- If an IPSec policy is created in IKE negotiation mode, the **tunnel local** on the local end must be the same as **12.6.134 remote-address (IKE peer view)** that the remote end references from the IKE peer.
- You do not need to specify the **12.6.174 tunnel local** (local address) for the IKE peer referenced in an IPSec profile, because the local address is the source address of the GRE, mGRE or IPSec virtual tunnel interface. For the IKE peer referenced in an IPSec profile, **12.6.174 tunnel local** does not take effect.
- When applying an IPSec policy to a tunnel interface and running the **12.3.18 source** command to specify an IP address for the interface, you must run the **12.6.174 tunnel local** command to configure a tunnel local address. Otherwise, IKE negotiation will fail.
- In an IPSec hot standby scenario, **tunnel local** must be set to a virtual IP address.

Example

Set the local IP address of the IPSec tunnel to 10.1.1.1 in the manual IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 100 manual
[Huawei-ipsec-policy-manual-policy1-100] tunnel local 10.1.1.1
```

Set the primary IP address of the interface to which the IPSec policy in IKE negotiation mode is applied as the local IP address of the IPSec tunnel.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 100 isakmp
[Huawei-ipsec-policy-isakmp-policy1-100] tunnel local applied-interface
```

12.6.175 tunnel remote

Function

The **tunnel remote** command specifies the remote address of an IPSec tunnel.

The **undo tunnel remote** command cancels the configuration.

By default, no remote IP address is configured for the IPSec tunnel.

Format

tunnel remote *ip-address*

undo tunnel remote

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address for the remote end of an IPSec tunnel.	The value is in dotted decimal notation.

Views

Manual IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to specify an end point for an IPSec tunnel.

For a manually created IPSec policy, you must run the **tunnel remote** *ip-address* command to configure an IP address for the remote end before you can create an SA. Only after correct IP addresses are configured for the local end (start point) and remote end (end point), an IPSec tunnel can be established between the two ends.

Precautions

If an IPSec policy is created manually, **tunnel remote** on the local end must be the same as **tunnel local** on the remote end.

Example

Set the remote IP address in IPSec policy **policy1** to 10.1.1.2.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 manual
[Huawei-ipsec-policy-manual-policy1-1] tunnel remote 10.1.1.2
```

12.6.176 tunnel pathmtu enable

Function

The **tunnel pathmtu enable** command enables the device to learn the maximum transmission unit (MTU) of packets allowed on an IPSec tunnel.

The **undo tunnel pathmtu enable** command disables the device from learning the MTU of packets allowed on an IPSec tunnel.

By default, the device cannot learn the MTU of packets allowed on an IPSec tunnel.

Format

tunnel pathmtu enable

undo tunnel pathmtu enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Tunnel interface view, Tunnel-Template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the local device sends IPSec packets along a created IPSec tunnel, the IPSec packets are discarded if the packet MTU exceeds the MTU allowed on the IPSec tunnel and the local device receives an ICMP Unreachable packet.

The local device uses the MTU in the ICMP Unreachable packet and the Security Parameter Index (SPI) of the SA, and then automatically adjusts the interface MTU to a proper value to allow IPSec packets to pass.

Prerequisites

This command takes effect only when the encapsulation mode of the tunnel interface has been set to **IPSec** or **GRE** using the **tunnel-protocol** command or the **destination** command has been configured on the tunnel interface.

The Don't Fragment (DF) field of the IPSec tunnel has been set to 1 using the **ipsec df-bit set** command, indicating that packet fragmentation is not allowed on the IPSec tunnel.

Precautions

If there is a firewall on the network, this command cannot take effect because the firewall blocks ICMP packets.

If devices have the NAT traverse function enabled, this command cannot take effect because the format of IPSec packets has changed after the NAT traverse and the devices cannot identify the SPI values of SAs.

Example

Enable the device to learn the MTU allowed on an IPSec tunnel on a virtual tunnel interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipsec
[Huawei-Tunnel0/0/1] tunnel pathmtu enable
```

12.6.177 user (IKE user table view)

Function

The **user** command configures IKE user information.

The **undo user** command deletes IKE user information.

By default, no IKE user information is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **vpn-instance** *vpn-instance-name*

user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **pre-shared-key** *key* [**description** *description*]

undo user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **vpn-instance**

undo user id-type { **any** *any-id* | **fqdn** *remote-fqdn* | **ip** *ip-address* | **user-fqdn** *remote-user-fqdn* } **pre-shared-key**

Parameters

Parameter	Description	Value
id-type	Specifies the remote ID type and remote ID of an IKE peer.	-
any *any-id*	Indicates that the remote ID of an IKE peer can be of any type and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?) and spaces.
fqdn *remote-fqdn*	Specifies the name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?) and spaces.
ip *ip-address*	Specifies the IP address as the remote ID of an IKE peer and configures the remote ID.	The value is in dotted decimal notation.
user-fqdn *remote-user-fqdn*	Specifies the domain name as the remote ID of an IKE peer and configures the remote ID.	The value is a string of 1 to 255 case-sensitive characters without question marks (?) and spaces.
vpn-instance *vpn-instance-name*	Specifies a VPN instance name.	The value is the name of an existing VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pre-shared-key *key*	Specifies a pre-shared key.	The value is a string of 1 to 128 case-sensitive characters in plaintext or 48 to 188 case-sensitive characters in ciphertext. When the value contains the question mark (?) or space, you must enclose the value with double quotation marks ("").
description *description*	Specifies the description of an IKE user.	The value is a string of 1 to 63 case-sensitive characters without question marks (?).

Views

IKE user table view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device functions as the headquarters gateway, an IPSec policy is created using an IPSec policy template, and the gateway receives IPSec connection requests of different branches. If the pre-shared key is used for identity authentication and all branches use the same ID and pre-shared key, there are security risks. That is, if the ID and pre-shared key of one branch leak, the ID and pre-shared key of all branches leak. The IKE user table can prevent this problem.

The IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references the IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys for identity authentication.

In addition, on an MPLS VPN with small VPN sites, if CEs and PEs are connected through the Internet but not leased lines, hosts connected to a CE can access the resources on another VPN site only through the insecure Internet. To enhance access security, these hosts can connect to the backbone network of the MPLS VPN through an IPSec tunnel.

After you run this command, the device determines the VPN instance to which site traffic passing through the IPSec tunnel belongs by the user type, isolating traffic from different sites.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The VPN instance has been created using the **ip vpn-instance** command and the route distinguisher (RD) has been configured for the VPN instance using the **route-distinguisher** command.

Precautions

- After an IKE peer references an IKE user table, the pre-shared key configured by this command takes precedence over the pre-shared key configured using the **pre-shared-key** command.
- After an IKE peer references an IKE user table, the VPN instance configured by this command takes precedence over the VPN instance configured using the **sa binding vpn-instance** command.
- If IKEv1 in main mode is used, **id-type** must be set to **ip**. In NAT traversal scenarios, *ip-address* must be the IP address translated by the NAT device.

Example

Configure user information in IKE user table 10, and set the remote ID type, remote ID, and pre-shared key to **IP**, 10.1.1.1, and **Test!123** respectively.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user id-type ip 10.1.1.1 pre-shared-key Test!123
```

Configure user information in IKE user table 10, and bind it to VPN instance **vpna**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpna
[Huawei-vpn-instance-vpna] ipv4-family
[Huawei-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpna-af-ipv4] quit
[Huawei-vpn-instance-vpna] quit
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user id-type ip 10.1.1.1 vpn-instance vpna
```

Related Topics

12.6.74 ike user-table

12.6.178 user

Function

The **user** command creates an IKE user and displays the IKE user view, or directly displays the view of an existing IKE user.

The **undo user** command deletes the created IKE user.

By default, no IKE user is created in an IKE user table.

Format

user *user-name*

undo user *user-name*

Parameters

Parameter	Description	Value
user-name	Specifies the name of an IKE user.	The value is a string of 1 to 63 case-sensitive characters without spaces and question marks (?).

Views

IKE user table view

Default Level

2: Configuration level

Usage Guidelines

After the **ike user-table** command is used to create an IKE user table and enter the IKE user table view, run the **user** command to create an IKE user and enter the IKE user view. You can define the pre-shared key, user ID, IP address, DNS server address, and VPN instance in the IKE user view.

Example

Create an IKE user in the IKE user table.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1]
```

Related Topics

12.6.74 ike user-table

12.6.63 id-type

12.6.127 pre-shared-key (IKE user view)

12.6.181 vpn-instance-traffic (IKE user view)

12.6.27 display ike user-table (all views)

12.6.179 user-table

Function

The **user-table** command references an IKE user table in an IKE peer.

The **undo user-table** command deletes the referenced IKE user table.

By default, the IKE peer does not reference an IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

Format

user-table *user-table-id*

undo user-table

Parameters

Parameter	Description	Value
user-table-id	Specifies the ID of an IKE user table.	The value must be an existing IKE user table ID.

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IKE user table records the mapping between remote IDs of IKE peers and pre-shared keys. After an IKE peer references an IKE user table, the device searches for the pre-shared key matching the remote ID of the IKE peer in the IKE user table to complete identity authentication during IKE negotiation. In this manner, branches use different IDs and pre-shared keys.

Prerequisites

An IKE user table has been created using the **ike user-table** command.

Precautions

After an IKE peer references an IKE user table, the pre-shared key configured using the **12.6.127 pre-shared-key (IKE user view)** command takes precedence over that configured using the **12.6.126 pre-shared-key (IKE peer view, Efficient VPN policy view)** command.

Example

Reference IKE user table 10 in IKE peer **peer1**.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] quit
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] user-table 10
```

Related Topics

12.6.74 ike user-table

 Copyright © Huawei Technologies Co., Ltd.

12.6.180 version

Function

The **version** command sets the IKE version number of an IKE peer.

The **undo version** command cancels the configuration.

By default, IKEv1 and IKEv2 are enabled.

Format

version { **1** | **2** }

undo version { **1** | **2** }

Parameters

Parameter	Description	Value
1	Indicates that the IKE version number is 1.	-
2	Indicates that the IKE version number is 2.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

IKEv1 and IKEv2 cannot be disabled simultaneously.

If IKEv1 and IKEv2 are enabled simultaneously, the initiator uses IKEv2, and the responder can use IKEv1 or IKEv2.

Example

Configure IKE peer **peer1** to initiate negotiation using IKEv1.

```
<Huawei> system-view
[Huawei] ike peer peer1
[Huawei-ike-peer-peer1] undo version 2
```

12.6.181 vpn-instance-traffic (IKE user view)

Function

The **vpn-instance-traffic** command configures a VPN instance corresponding to user traffic of the IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

The **undo vpn-instance-traffic** command deletes a VPN instance corresponding to user traffic of the IKE user table.

By default, the VPN instance corresponding to user traffic of the IKE user table is not configured.

Format

vpn-instance-traffic { **public** | **name** *vpn-instance-name* }

undo vpn-instance-traffic

Parameters

Parameter	Description	Value
public	Indicates that user traffic of the IKE user table is public network traffic.	-
name *vpn-instance-name*	Specifies the name of a VPN instance.	The value must be an existing VPN instance name.

Views

IKE user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where multiple branches connect to the headquarters, you can run the **sa binding vpn-instance** command to specify the VPN instance that IPSec tunnel traffic belongs to, thereby isolating traffic of different branches. When the device functions as the headquarters gateway and an IPSec policy is created using an IPSec policy template, the headquarters gateway cannot distinguish VPNs of different branches. You can run the **vpn-instance-traffic** command to specify VPNs for different branches.

Prerequisites

1. A VPN instance has been created using the **12.9.35 ip vpn-instance** command.
2. An RD has been configured using the **12.9.50 route-distinguisher** command.

Precautions

After an IKE user table is referenced by an IKE peer, the VPN instance configured by this command takes precedence over the VPN instance configured by the **sa binding vpn-instance** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a VPN instance named **vrf1** corresponding to user traffic of the IKE user table.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] route-distinguisher 22:1
[Huawei-vpn-instance-vrf1-af-ipv4] quit
[Huawei-vpn-instance-vrf1] quit
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] user user1
[Huawei-ike-user-table-10-user1] vpn-instance-traffic name vrf1
```

Related Topics

12.9.35 ip vpn-instance

12.9.50 route-distinguisher

12.6.27 display ike user-table (all views)

12.6.182 user-fqdn

Function

The **user-fqdn** command configures the user domain name of an allowed peer for IKE negotiation.

The **undo user-fqdn** command deletes the user domain name of the allowed peer.

By default, no user domain name of allowed peer for IKE negotiation is configured.

Format

user-fqdn *fqdn-name*

undo user-fqdn *fqdn-name*

Parameters

Parameter	Description	Value
fqdn-name	Specifies the user domain name of the peer for IKE negotiation.	The value is an existing user domain name of the peer for IKE negotiation.

Views

Identity filter set view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can run this command to configure a user domain name in the identity filter set to specify the allowed peer.

Precautions

An IPSec tunnel can be established only when the peer matches one or more attributes in the identity filter set and IPSec negotiation parameters on two ends are the same.

You can run this command in the same view multiple times to specify multiple user domain names.

Example

Set the user domain name of the allowed peer for IKE negotiation to **liming@huawei.com**.

```
<Huawei> system-view
[Huawei] ike identity identity1
[Huawei-ike-identity-identity1] user-fqdn liming@huawei.com
```

Related Topics

12.6.121 match ike-identity

12.7 A2A VPN Configuration Commands

12.7.1 anti-replay time-based enable

Function

The **anti-replay time-based enable** command enables the time-based anti-replay function for the A2A VPN.

The **undo anti-replay time-based enable** command disables the time-based anti-replay function for the A2A VPN.

By default, the time-based anti-replay function is disabled for the A2A VPN.

Format

anti-replay time-based enable

undo anti-replay time-based enable

Parameters

None

Views

GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized users from stealing A2A VPN packets for DoS attacks, the A2A VPN provides the time-based anti-replay function to detect replayed packets (processed packets) according to the time mechanism.

After this function is enabled for the A2A VPN, the KS generates a pseudo timestamp (PTs) based on the GM and sends the pseudo timestamp and time-based anti-replay window (Tw) to GMs. During communication between GMs, the pseudo timestamp and time-based anti-replay window are used to prevent replayed packets. The detailed process is as follows:

1. When sending a packet, GM_1 adds the encryption time t1 to the encrypted packet. The formula for calculating t1 is as follows: t1 = Pseudo timestamp (PTs1) + Packet sending time (ts) - GM_1 registration time (tr1).
2. After receiving the packet, GM_2 generates the time t2, extracts the encryption time t1 from the packet, and compares t1 and t2. The formula for calculating t2 is as follows: t2 = Pseudo timestamp (PTs2) + Time when the packet is received (tsr) - GM_2 registration time (tr2). If the difference between t1 and t2 is within the range (-Tw to +Tw), the packet is accepted; otherwise, the packet is dropped.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Enable the time-based anti-replay function for the A2A VPN.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] anti-replay time-based enable
```

Related Topics

12.7.2 anti-replay time-based window

12.7.3 display gdoi ks group

12.7.2 anti-replay time-based window

Function

The **anti-replay time-based window** command sets the size of the A2A VPN time-based anti-replay window.

The **undo anti-replay time-based window** command restores the size of the A2A VPN time-based anti-replay window to the default value.

The default size of the A2A VPN time-based anti-replay window is 5 seconds.

Format

anti-replay time-based window *seconds*

undo anti-replay time-based window

Parameters

Parameter	Description	Value
seconds	Specifies the size of the A2A VPN time-based anti-replay window.	The value is an integer that ranges from 1 to 100, in seconds.

Views

GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the time-based anti-replay function is enabled, you can adjust the time-based anti-replay window size based on the actual scenario. For example, in the case of a large network delay, the service packets received by the receiver are regarded as replayed packets and thus are discarded. In this instance, you can disable the time-based anti-replay function or expand the anti-replay window size to prevent incorrect packet dropping.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the size of the A2A VPN time-based anti-replay window to 6 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] anti-replay time-based window 6
```

Related Topics

12.7.1 anti-replay time-based enable

12.7.3 display gdoi ks group

12.7.3 display gdoi ks group

Function

The **display gdoi ks group** command displays configuration information about a GDOI group of a KS.

Format

display gdoi ks group [**brief** | **name** *group-name*]

Parameters

Parameter	Description	Value
brief	Displays brief configuration information about a given GDOI group.	-
name *group-name*	Displays detailed configuration information about a given GDOI group. If **name** is not specified, the configuration information about all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When deploying the A2A VPN, you can run this command to check the configuration information about the GDOI groups of the KS, such as the group ID,

encryption algorithm used for rekey messages, signature hash algorithm used for rekey messages, transmission mode of rekey messages, RSA key pair used for rekey messages, retransmission interval of rekey messages, number of times for retransmitting rekey messages, time-based anti-replay function, and anti-replay window size.

Example

Display brief configuration information about a GDOI group.

```
<Huawei> display gdoi ks group brief
Number of GDOI group : 1

GDOI group name                    identity number
-------------------------------------------------------
test                               33
```

Display configuration information about all GDOI groups.

```
<Huawei> display gdoi ks group
===============================================
GDOI group: test
===============================================
  Group identity number          : 10
  SA mode                        : normal
  Rekey encrypt algorithm        : AES-128
  Rekey sig-hash-algorithm       : SHA2-512
  Rekey transport type           : multicast
  Source address                 : 3.1.1.1
  Rekey destination address      : 239.0.1.2
  Rekey rsa key pair             : keytest
  Rekey lifetime (secs)          : 86400
  Rekey retry interval (secs)    : 10
  Rekey retry limit              : 3
  User-table                     : 10
  Local-id                       : -
  Local-id-type                  : ip
  Group policy numbers           : 1

  GDOI policy seq                : 5
   Proposal name                         : tran1
   Security acl                          : 3001
   SA lifetime (secs)                    : 3600
   Anti-replay time-based                : enable
   Anti-replay time-based window size(secs) : 5
```

Table 12-70 Description of the **display gdoi ks group** command output

Item	Description
Number of GDOI group	Number of GDOI groups.
GDOI group name/GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
identity number/Group identity number	GDOI group identity number. To configure this parameter, run the **12.7.13 group identity number** command.

Item	Description
SA mode	SA mode: ● receive-only: The GM sends only plaintext packets but can receive both plaintext and ciphertext packets. ● normal: The GM sends and receives only ciphertext packets. To configure this parameter, run the **12.7.38 sa receive-only** command.
Rekey encrypt algorithm	Encryption algorithm used for rekey messages: ● DES ● 3DES ● AES-128 ● AES-192 ● AES-256 To configure this parameter, run the **12.7.25 rekey encryption-algorithm** command.
Rekey sig-hash-algorithm	Signature hash algorithm used for rekey messages: ● SHA1 ● SHA2-256 ● SHA2-384 ● SHA2-512 To configure this parameter, run the **12.7.28 rekey sig-hash-algorithm** command.
Rekey transport type	Transmission mode of rekey messages: ● unicast ● multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
Source address	IP address of a KS. To configure this parameter, run the **12.7.40 source address (GDOI Group View)** command.
Rekey destination address	Destination IP address of rekey messages. To configure this parameter, run the **12.7.24 rekey destination address** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rekey rsa key pair	RSA key pair used for rekey messages. To configure this parameter, run the **12.7.23 rekey authentication public-key rsa** command.
Rekey lifetime (secs)	KEK SA lifetime, in seconds. To configure this parameter, run the **12.7.27 rekey sa duration time-based** command.
Rekey retry interval (secs)	Interval for retransmitting rekey messages, in seconds. To configure this parameter, run the **12.7.26 rekey retry** command.
Rekey retry limit	Number of times for retransmitting rekey messages. To configure this parameter, run the **12.7.26 rekey retry** command.
User-table	IKE user table referenced in the GDOI group. To configure this parameter, run the **12.7.42 user-table (GDOI Group View)** command.
Local-id	Local ID used in A2A VPN negotiation. To configure this parameter, run the **12.7.21 local-id (GDOI Group View)** command.
Local-id-type	Local ID type used in A2A VPN negotiation: • fqdn: The local ID type used in A2A VPN negotiation is in the name format. • ip: The local ID type used in A2A VPN negotiation is in the IP address format. • user-fqdn: The local ID type used in A2A VPN negotiation is in the user +domain name format. To configure this parameter, run the **12.7.20 local-id-type (GDOI Group View)** command.
Group policy numbers	Number of GDOI IPSec policies.
GDOI policy seq	GDOI group IPSec policy sequence number. To configure this parameter, run the **12.7.15 ipsec** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Proposal name	IPSec proposal referenced in GDOI IPSec policies. To configure this parameter, run the **12.7.22 proposal (GDOI group IPSec policy View)** command.
Security acl	ACL referenced in GDOI IPSec policies. To configure this parameter, run the **12.7.39 security acl** command.
SA lifetime (secs)	TEK SA lifetime, in seconds. To configure this parameter, run the **12.7.37 sa duration time-based** command.
Anti-replay time-based	Time-based anti-replay function: ● enable: The time-based anti-replay function is enabled. ● disable: The time-based anti-replay function is disabled. To configure this parameter, run the **12.7.1 anti-replay time-based enable** command.
Anti-replay time-based window size (secs)	Size of the time-based anti-replay window, in seconds. To configure this parameter, run the **12.7.2 anti-replay time-based window** command.

12.7.4 display gdoi ks members

Function

The **display gdoi ks members** command displays information about GDOI group members of a KS.

Format

display gdoi ks members [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Displays information about members in a specified GDOI group. If **group** is not specified, the information about members in all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a GM registers with the KS successfully, you can run this command to view information about GDOI group members, such as the number of GMs, transmission mode of rekey messages, IP address of the GM, IP address of the KS, and sequence number of rekey messages.

Example

Display information about members in all GDOI groups of the KS.

```
<Huawei> display gdoi ks members
===============================================
 GDOI group    : test
 GM number     : 1
 Rekey transport type          : unicast
===============================================

   GM ID                        : 10.2.1.1
   Key server ID                : 10.3.1.1
   Current seq of rekey         : 0
   Acked seq of rekey           : 0
   Number of rekey sent         : 0
   Number of rekey unacked      : 0
```

Table 12-71 Description of the **display gdoi ks members** command output

Item	Description
GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
GM number	Number of GDOI group members.

Item	Description
Rekey transport type	Transmission mode of rekey messages: ● unicast ● multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
GM ID	IP address of the GM.
Key server ID	IP address of the KS. To configure this parameter, run the **12.7.40 source address (GDOI Group View)** command.
Current seq of rekey	Current sequence number of rekey messages.
Acked seq of rekey	Sequence number of unicast rekey ACK messages.
Number of rekey sent	Number of sent rekey messages.
Number of rekey unacked	Number of unicast rekey ACK messages that are not received.

Related Topics

12.7.31 reset gdoi ks members

12.7.5 display gdoi ks members history record

Function

The **display gdoi ks members history record** command displays historical information about GDOI group members of a KS.

Format

display gdoi ks members history record [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Displays historical information about members in a specified GDOI group. If **group** is not specified, the historical information about members in all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a GM fails to register with the KS or goes offline abnormally, you can run this command to check the reason for quick fault location.

Example

Display historical information about members in all GDOI groups.

```
<Huawei> display gdoi ks members history record
==============================================================================
GDOI GM history record:
remote address                  : 10.2.1.1
source address                  : 10.10.10.1
group name                      : test
group id                        : 33
offline reason                  : Failed to verify rekey ack message of a group member
offline time                    : 2018-05-28 10:06:43

==============================================================================
GDOI GM history record:
remote address                  : 10.2.1.2
source address                  : 10.10.10.1
group name                      : test
group id                        : 33
register failure reason         : No TEK
register failure time           : 2018-05-28 11:06:43
```

Table 12-72 Description of the **display gdoi ks members history record** command output

Item	Description
GDOI GM history record	Historical information about a GM in a GDOI group.
remote address	IP address of the GM.
source address	IP address of the KS.
group name	GDOI group name.
group id	GDOI group ID.
offline reason	Reason why the GM goes offline. Failed to verify rekey ack message of a group member: Failed to verify the rekey ACK message of the GM.
offline time	Time when the GM goes offline.
register failure reason	Reason why the GM fails to register with the KS: ● Can not find GDOI group: The GDOI group cannot be found. ● Invalid hash_1 payload received: The KS receives an invalid hash payload. ● Invalid group id received: The KS receives an invalid group ID. ● Number of group members reached maximum: The number of GMs has reached the upper limit. ● No KEK: The KEK SA does not exist. ● No TEK: The TEK SA does not exist. ● No permit rules: All rules in the ACL referenced by the KS are Deny. ● Invalid hash_3 payload received: The KS receives an invalid hash payload. ● Send sequence failed: Failed to send the sequence number payload of the KEK SA. ● Invalid TEK key: The TEK key is invalid. ● Invalid KEK key: The KEK key is invalid. ● Deletion in progress: The GDOI group is being deleted.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
register failure time	Time when the GM fails to register with the KS.

Related Topics

12.7.32 reset gdoi ks members history record

12.7.6 display gdoi ks rekey statistics

Function

The **display gdoi ks rekey statistics** command displays statistics about the rekey messages on a KS.

Format

display gdoi ks rekey statistics [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Displays statistics about the rekey messages of a specified GDOI group. If **group** is not specified, statistics about the rekey messages of all GDOI groups are displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the KS performs rekey, you can run this command to view statistics about rekey messages received and sent by the KS, which helps you quickly locate faults.

Example

Display statistics about rekey messages of all GDOI groups.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display gdoi ks rekey statistics
===============================================
GDOI group: test
===============================================
  Rekey transport type          : unicast
  Number of rekey sent          : 28
  Number of rekey retransmitted  : 21
  Number of rekey acked         : 0
  Number of rekey missed        : 13
```

Table 12-73 Description of the **display gdoi ks rekey statistics** command output

Item	Description
GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
Rekey transport type	Transmission mode of rekey messages: ● unicast ● multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
Number of rekey sent	Number of sent rekey messages.
Number of rekey retransmitted	Number of retransmitted rekey messages.
Number of rekey acked	Number of unicast rekey ACK messages.
Number of rekey missed	Number of discarded unicast rekey ACK messages.

Related Topics

12.7.33 reset gdoi ks rekey statistics

12.7.7 display gdoi ks sa

Function

The **display gdoi ks sa** command displays SA information about the GDOI groups of a KS.

Format

display gdoi ks sa [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Displays SA information about a specified GDOI group. If **group** is not specified, the SA information about all GDOI groups is displayed.	The value must be the name of an existing GDOI group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a GM registers with the KS successfully, you can run this command to view the SA information about the GDOI groups of the KS, such as the group name, encryption algorithm used for rekey messages, signature hash algorithm used for rekey messages, transmission mode of rekey messages, RSA key pair used for rekey messages, KEK SA lifetime, TEK SA lifetime, time-based anti-replay function, and anti-replay window size.

Example

Display SA information about all GDOI groups.

```
<Huawei> display gdoi ks sa
===============================================
GDOI group: bzh
===============================================
  KEK SA
   SPI : 0x2ba0dacd87f2dd0a573a281e0599c65b
   Rekey transport type        : multicast
   Encrypt algorithm           : 3DES
   Encrypt iv length (bits)    : 64
   Encrypt key length (bits)   : 192
   Signature hash algorithm    : SHA1
   Signature key length (bits) : 4096
   Signature algorithm         : SIG_ALG_RSA
   Rekey current sequence      : 0
   Rekey next sequence         : 4
   SA lifetime (secs)          : 600
   SA remaining lifetime (secs): 104
   Next rekey time (secs)      : 34

  TEK SA
   SPI          : 3327227442 (0xc6517632)
   Security acl : 3001
   Proposal     : ESP-ENCRYPT-AES-256 ESP-AUTH-SHA2-256-128
   Encrypt key length (bits)   : 256
```

```
Auth key length (bits)      : 256
Anti-replay (time-based)    : enable
Window size (secs)          : 99
Replay value (secs)         : 102813.30
SA lifetime (secs)          : 3600
SA remaining lifetime (secs): 391
Next rekey time (secs)      : 261
```

Table 12-74 Description of the **display gdoi ks sa** command output

Item	Description
GDOI group	GDOI group name. To configure this parameter, run the **12.7.10 gdoi ks group** command.
KEK SA	Information about the KEK SA.
SPI	SPI value of the KEK SA or TEK SA.
Rekey transport type	Transmission mode of rekey messages: ● unicast ● multicast To configure this parameter, run the **12.7.29 rekey transport-type** command.
Encrypt algorithm	Encryption algorithm. To configure this parameter, run the **12.7.25 rekey encryption-algorithm** command.
Encrypt iv length (bits)	Length of the encryption IV, in bits.
Encrypt key length (bits)	Length of the encryption key, in bits.
Signature hash algorithm	Signature hash algorithm: ● SHA1 ● SHA2-256 ● SHA2-384 ● SHA2-512 To configure this parameter, run the **12.7.28 rekey sig-hash-algorithm** command.
Signature key length (bits)	Length of the signature key, in bits.
Signature algorithm	Signature algorithm.
Rekey current sequence	Sequence number used by the current rekey message.
Rekey next sequence	Sequence number used by the next rekey message.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA lifetime (secs)	KEK SA or TEK SA lifetime, in seconds. To configure this parameter, run the **12.7.27 rekey sa duration time-based** or **12.7.37 sa duration time-based** command.
SA remaining lifetime (secs)	Remaining lifetime of the KEK SA or TEK SA, in seconds.
Next rekey time (secs)	Next rekey time, in seconds.
TEK SA	Information about the TEK SA.
Security acl	ACL used in the TEK SA. To configure this parameter, run the **12.7.39 security acl** command.
Proposal	Algorithm of the IPSec proposal. To configure this parameter, run the **12.7.22 proposal (GDOI group IPSec policy View)** command.
Auth key length (bits)	Length of the authentication key, in bits.
Anti-replay (time-based)	Time-based anti-replay function: ● enable: The time-based anti-replay function is enabled. ● disable: The time-based anti-replay function is disabled. To configure this parameter, run the **12.7.1 anti-replay time-based enable** command.
Window size (secs)	Size of the time-based anti-replay window, in seconds. To configure this parameter, run the **12.7.2 anti-replay time-based window** command.
Replay value (secs)	Replay pseudo timestamp, in seconds.

Related Topics

12.7.30 reset gdoi ks group

12.7.8 display ipsec gdoi-policy

Function

The **display ipsec gdoi-policy** command displays GDOI policy information.

Format

display ipsec gdoi-policy [*policy-name* [*seq-number*]]

Parameters

Parameter	Description	Value
policy-name	Displays detailed information about the GDOI policy with a specified name. If *policy-name* is not specified, information about all GDOI policies is displayed.	The value must be an existing GDOI policy name.
seq-number	Displays information about the GDOI policy with a specified sequence number.	The value must be an existing GDOI policy sequence number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After registering with the KS successfully, a GM obtains the TEK and KEK security policies from the KS, such as the data flow to be protected, SA mode, IPSec proposal, and encryption algorithm of rekey messages. You can run this command to view information about security policies or information about the locally-configured security policies.

Example

Display detailed GDOI policy information.

```
<Huawei> display ipsec gdoi-policy
==========================================
Gdoi policy group: "map1"
Using interface: GigabitEthernet1/0/0
==========================================
  Sequence number: 10
  Group identity : 10
  Qos pre-classify: Disable
  Qos group: -
  Key server ID  : 3.1.1.1(active)
  Peer name      : spub
  Local acl      :
```

```
  GM reregister  : 2018-06-05 14:34:39
  Rekey received :
  Rekey received cumulative : 0
  Rekey received after register : 0
  Rekey ack sent : 0

  ACL Downloaded From KS 3.1.1.1:
   Protocol: 0/permit
   Flow source      : 10.1.1.0/255.255.255.0/0
   Flow destination : 10.1.2.0/255.255.255.0/0

  TEK POLICY:
   SA mode : normal
   SPI: 2529860581 (0x96ca9be5)
   Encapsulation mode: Tunnel
   Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
   SA remaining lifetime (secs) : 3206
   Anti-replay (time based) : enable
   Window size (secs): 5
   Reply value (secs): 3689.31

  KEK POLICY:
   Rekey transport type        : multicast
   SPI: 0x2ad569a935d15b75174446fbb0feaf5b
   Received rekey seqno        : 100
   Lifetime (secs)             : 71733
   Encrypt algorithm           : AES
   Encrypt key size            : 128
   Signature hash algorithm    : HMAC_AUTH_SHA2_512
   Signature key length (bits) : 2160
   Signature algorithm         : SIG_ALG_RSA

==========================================
Gdoi policy group: "po1"
Shared interface: LoopBack0
Using interface: GigabitEthernet1/0/1
                 GigabitEthernet1/0/2
==========================================
  Sequence number: 10
  Group identity : 10
  Qos pre-classify: Disable
  Qos group: -
  Key server ID  : 3.1.1.1(active)
  Peer name      : spub
  Local acl      :

  GM reregister  : 2018-06-05 14:34:39
  Rekey received :
  Rekey received cumulative : 0
  Rekey received after register : 0
  Rekey ack sent : 0

  ACL Downloaded From KS 3.1.1.1:
   Protocol: 0/permit
   Flow source      : 10.1.1.0/255.255.255.0/0
   Flow destination : 10.1.2.0/255.255.255.0/0

  TEK POLICY:
   SA mode : normal
   SPI: 2529860581 (0x96ca9be5)
   Encapsulation mode: Tunnel
   Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
   SA remaining lifetime (secs) : 3206
   Anti-replay (time based) : enable
   Window size (secs): 5
   Reply value (secs): 3689.31

  KEK POLICY:
   Rekey transport type        : multicast
```

```
SPI: 0x2ad569a935d15b75174446fbb0feaf5b
Received rekey seqno        : 100
Lifetime (secs)             : 71733
Encrypt algorithm           : AES
Encrypt key size            : 128
Signature hash algorithm    : HMAC_AUTH_SHA2_512
Signature key length (bits) : 2160
Signature algorithm         : SIG_ALG_RSA
```

Table 12-75 Description of the **display ipsec gdoi-policy** command output

Item	Description
Gdoi policy group	Name of the GDOI policy group. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
Shared interface	Multi-link shared interface. To configure a multi-link shared interface, run the **12.6.103 ipsec policy shared** command.
Using interface	Interface to which a GDOI policy is applied. To apply a GDOI policy to an interface, run the **12.7.19 ipsec policy (interface view)** command.
Sequence number	Sequence number of the applied IPSec policy. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
Group identity	GDOI group ID.
Qos pre-classify	Whether to pre-extract original packet information: ● Enable: Pre-extraction is enabled. ● Disable: Pre-extraction is disabled. To enable pre-extraction, run the **12.6.132 qos pre-classify** command.
Qos group	QoS group to which A2A VPN packets belong. To configure a QoS group, run the **12.6.131 qos group** command.
Key server ID	IP address of the KS.
Peer name	Name of the referenced IKE peer. To create an IKE peer, run the **12.6.77 ike-peer** command.
Local acl	Number of a local ACL. To reference an ACL, run the **12.6.167 security acl** command.
GM reregister	Time at which a GM registers with the KS.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rekey received	Time at which a GM receives rekey messages.
Rekey received cumulative	Total number of rekey messages received by a GM.
Rekey received after register	Number of rekey messages received by a GM after it registers with the KS.
Rekey ack sent	Number of responses to unicast rekey messages sent by a GM.
ACL Downloaded From KS	ACL downloaded from the KS by the GM.
Protocol	Number of the protocol data flows of which are protected by the SA.
Flow source	Source address of encryption data flows. ● The value 10.0.0.0 indicates the network segment address of the source IP address. ● The value 255.0.0.0 indicates the network mask. ● The value 0/0 indicates the ACL number and port number.
Flow destination	Destination address of encryption data flows. ● The value 10.1.0.0 indicates the network segment address of the destination IP address. ● The value 255.0.0.0 indicates the network mask. ● The value 0/0 indicates the ACL number and port number.
TEK POLICY	Policy for the traffic encryption key.
SA mode	TEK SA mode.
SPI	Security parameter index.
Encapsulation mode	TEK SA encapsulation mode. ● Tunnel: tunnel mode. ● Transport: transport mode.
Proposal	Encryption and authentication algorithms of A2A VPN Security proposal.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SA remaining lifetime (secs)	Remaining lifetime of the TEK SA in seconds.
Anti-replay (time based)	Time-based anti-replay: ● enable: The time-based anti-replay function is enabled. ● disable: The time-based anti-replay function is disabled.
Window size (secs)	Size of the time-based anti-replay window, in seconds.
Reply value (secs)	Replay pseudo timestamp, in seconds.
KEK POLICY	Policy for key encryption key.
Rekey transport type	Type of the received rekey message. ● unicast ● multicast
Received rekey seqno	Received Rekey message sequence number.
Lifetime (secs)	Remaining lifetime of the KEK SA in seconds.
Encrypt algorithm	Encryption algorithm used in a GDOI policy.
Encrypt key size	Private key of the encryption algorithm.
Signature hash algorithm	Hash algorithm used to calculate a signature.
Signature key length (bits)	Private key length of the signature in bits.
Signature algorithm	Signature algorithm used in a GDOI policy.

12.7.9 display ipsec gdoi-sa

Function

The **display ipsec gdoi-sa** command displays GDOI SA information.

Format

display ipsec gdoi-sa [*policy-name* [*seq-number*]]

Parameters

Parameter	Description	Value
policy-name	Displays the SA established through a specified GDOI policy. If *policy-name* is not specified, all GDOI SA information is displayed.	The value must be an existing GDOI policy name.
seq-number	Specifies the sequence number of the GDOI policy.	The value must be an existing GDOI policy sequence number.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the TEK SA and KEK SA are generated by the GM, you can run this command to view information about the TEK SA and KEK SA, such as the data flows to be protected, inbound/outbound packet statistics, SA mode, transmission mode of rekey messages, encryption algorithm of rekey messages, and signature hash algorithm of rekey messages.

Example

Display detailed information about the SA established through a GDOI policy.

```
<Huawei> display ipsec gdoi-sa
================================
Interface: GigabitEthernet1/0/0
 Path MTU: 1500
================================
  ---------------------------------
  Gdoi policy name          : "map1"
  Sequence number           : 10
  ---------------------------------
    [TEK SA]
    Protected vrf : 0
    Protocol: 0/permit
    Flow source      : 10.1.1.0/255.255.255.0/0
    Flow destination : 10.1.2.0/255.255.255.0/0

    Inpacket count             : 0
    Inpacket decap count       : 0
    Outpacket count            : 0
    Outpacket encap count      : 0
    Inpacket drop count        : 0
    Outpacket drop count       : 0
    Anti-replay drop count     : 0
```

```
    SA mode : normal
    SPI: 99152831 (0x5e8f3bf)
    Encapsulation mode: Tunnel
    Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
    SA remaining lifetime (secs) : 2873
    Anti-replay (time based) : enable
    Window size (secs): 5
    Replay value (secs): 6342.88

    [KEK POLICY]
    Rekey transport type        : multicast
    SPI: 0x2ad569a935d15b75174446fbb0feaf5b
    Received rekey seqno        : 8
    Lifetime (secs)             : 81811
    Encrypt algorithm           : AES
    Encrypt key size            : 128
    Signature hash algorithm    : HMAC_AUTH_SHA2_512
    Signature key length (bits) : 2160
    Signature algorithm         : SIG_ALG_RSA

===============================
 Shared interface: LoopBack0
 Using interface: GigabitEthernet1/0/1
                  GigabitEthernet1/0/3
===============================
  ---------------------------------
  Gdoi policy name         : "map1"
  Sequence number          : 10
  ---------------------------------
    [TEK SA]
    Protected vrf : 0
    Protocol: 0/permit
    Flow source      : 10.1.1.0/255.255.255.0/0
    Flow destination : 10.1.2.0/255.255.255.0/0

    Inpacket count            : 0
    Inpacket decap count      : 0
    Outpacket count           : 0
    Outpacket encap count     : 0
    Inpacket drop count       : 0
    Outpacket drop count      : 0
    Anti-replay drop count    : 0

    SA mode : normal
    SPI: 99152831 (0x5e8f3bf)
    Encapsulation mode: Tunnel
    Proposal : ESP-ENCRYPT-AES-128 ESP-AUTH-SHA2-256-128
    SA remaining lifetime (secs) : 2873
    Anti-replay (time based) : enable
    Window size (secs): 5
    Replay value (secs): 6342.88

    [KEK POLICY]
    Rekey transport type        : multicast
    SPI: 0x2ad569a935d15b75174446fbb0feaf5b
    Received rekey seqno        : 8
    Lifetime (secs)             : 81811
    Encrypt algorithm           : AES
    Encrypt key size            : 128
    Signature hash algorithm    : HMAC_AUTH_SHA2_512
    Signature key length (bits) : 2160
    Signature algorithm         : SIG_ALG_RSA
```

Table 12-76 Description of the **display ipsec gdoi-sa** command output

Item	Description
Interface	Interface to which a GDOI policy is applied. To apply a GDOI policy to an interface, run the **12.7.19 ipsec policy (interface view)** command.
Path MTU	MTU of the interface.
Shared interface	Multi-link shared interface. To configure a multi-link shared interface, run the **12.6.103 ipsec policy shared** command.
Using interface	Interface to which a GDOI policy is applied. To apply a GDOI policy to an interface, run the **12.7.19 ipsec policy (interface view)** command.
Gdoi policy name	Name of the applied GDOI policy. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
Sequence number	Sequence number of the applied GDOI policy. To create a GDOI policy, run the **12.7.18 ipsec policy (system view)** command.
TEK SA	SA of the traffic encryption key.
Protected vrf	VPN instance protected by A2A VPN. To specify the VPN instance bound to A2A VPN, run the **sa binding vpn-instance** command.
Protocol	Number of the protocol data flows of which are protected by the SA.
Flow source	Source address of encryption data flows. • The value 10.1.1.0 indicates the network segment address of the source IP address. • The value 255.255.255.0 indicates the network mask. • The value 0/0 indicates the ACL number and port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Flow destination	Destination address of encryption data flows. ● The value 10.1.2.0 indicates the network segment address of the destination IP address. ● The value 255.255.255.0 indicates the network mask. ● The value 0/0 indicates the ACL number and port number.
Inpacket count	Number of incoming Security packets.
Inpacket decap count	Number of times that the device decapsulates incoming packets.
Outpacket count	Number of outgoing Security packets.
Outpacket encap count	Number of times that the device encapsulates outgoing packets.
Inpacket drop count	Number of discarded incoming packets.
Outpacket drop count	Number of discarded outgoing packets.
Anti-replay drop count	Number of packets dropped during anti-replay.
SA mode	TEK SA mode.
SPI	Security parameter index.
Encapsulation mode	TEK SA encapsulation mode. ● Tunnel: tunnel mode. ● Transport: transport mode.
Proposal	Encryption and authentication algorithms of A2A VPN Security proposal.
SA remaining lifetime (secs)	Remaining lifetime of the TEK SA in seconds.
Anti-replay (time based)	Time-based anti-replay: ● enable: The time-based anti-replay function is enabled. ● disable: The time-based anti-replay function is disabled.
Window size (secs)	Size of the time-based anti-replay window, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Replay value (secs)	Replay pseudo timestamp, in seconds.
KEK POLICY	Policy for the traffic encryption key.
Rekey transport type	Type of the received rekey message. ● unicast ● multicast
Received rekey seqno	Received Rekey message sequence number.
Lifetime (secs)	Remaining lifetime of the KEK SA in seconds.
Encrypt algorithm	Encryption algorithm used in a GDOI policy.
Encrypt key size	Private key length of the encryption algorithm.
Signature hash algorithm	Hash algorithm used by a signature.
Signature key length (bits)	Private key length of the signature in bits.
Signature algorithm	Signature algorithm used in a GDOI policy.

12.7.10 gdoi ks group

Function

The **gdoi ks group** command creates a GDOI group for a KS and displays the GDOI group view.

The **undo gdoi ks group** command deletes the ID of a GDOI group.

By default, no GDOI group is created for a KS.

Format

gdoi ks group *group-name*

undo gdoi ks group *group-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a GDOI group.	The value is a string of 1 to 31 case-sensitive characters, with the exception of spaces or question marks (?).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After registering with the KS successfully, a GM obtains the TEK and KEK policies from the KS that are configured in a GDOI group. For this reason, you need to run the **gdoi ks group** command first to create a GDOI group, and then set parameters for the GDOI group, such as the group ID, group IP address, IKE user table, signature algorithm and key pair of rekey messages, and GDOI IPSec policies.

Example

Create a GDOI group for the KS.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1]
```

Related Topics

12.7.3 display gdoi ks group

12.7.11 gdoi ks rekey

Function

The **gdoi ks rekey** command is used to manually trigger a KS to send rekey messages.

Format

gdoi ks rekey group *group-name*

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

After modifying the configuration in a GDOI group, you can run this command to manually trigger the KS to send rekey messages without waiting for the KEK SA or TEK SA to age out.

Example

Manually trigger the KS to send rekey messages.

```
<Huawei> gdoi ks rekey group gr1
```

12.7.12 gdoi sa direction receive-option

Function

The **gdoi sa direction receive-option** command sets the SA mode to Receive_Option. In this mode, the device can receive both cipher text and plain text packets but can send only cipher text packets.

Format

gdoi sa direction receive-option

Parameters

None

Views

User view

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When you deploy A2A VPN on an existing network, a GM that has joined a group such as GM_1 can only send and receive cipher text packets, but the other GMs that have not joined the group can only send and receive plain text packets. In this case, the other GMs will discard encrypted packets from GM_1 because they cannot decrypt them, and GM_1 will discard plain text packets from the other GMs, resulting in service interruption. After you run this command on the GMs, A2A VPN can be deployed in several stages, preventing service interruption.

Example

Set the SA mode to Receive_Option.

```
<Huawei> gdoi sa direction receive-option
```

12.7.13 group identity number

Function

The **group identity number** command configures an ID for a GDOI group.

The **undo group identity number** command deletes the ID of a GDOI group.

By default, a GDOI group has no ID.

Format

group identity number { *group-number* | *ip-address* }

undo group identity number

Parameters

Parameter	Description	Value
group-number	Specifies the GDOI group ID.	The value is an integer that ranges from 0 to 4294967295.
ip-address	Specifies the IP address of the GDOI group.	The value is in dotted decimal notation.

Views

GDOI policy view, GDOI group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can run this command to configure an ID for a GDOI group in the A2A VPN. The KS determines the GDOI group to which a GM is to be added based on the group ID submitted by the GM.

Precautions

You can configure either a group ID or an IP address for a GDOI group at one time. If you run the command multiple times, only the latest configuration takes effect.

When the group ID for a GDOI group is modified, the GDOI group-related TEK SA and KEK SA are deleted. As a result, services between the KS and GM are interrupted until the GM re-registers with the KS after the TEK SA of the GM ages out.

Example

Configure an ID for a GDOI group in the GDOI policy view.

```
<Huawei> system-view
[Huawei] ipsec policy mypolicy 4 gdoi
[Huawei-ipsec-policy-gdoi-mypolicy-4] group identity number 10
```

Configure an ID for a GDOI group in the GDOI group view.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] group identity number 10
```

12.7.14 ike-peer

Function

The **ike-peer** command references an IKE peer.

The **undo ike-peer** command cancels the configuration.

By default, no IKE peer is referenced.

Format

ike-peer *peer-name*

undo ike-peer

Parameters

Parameter	Description	Value
peer-name	Specifies the name of the referenced IKE peer.	The value must be an existing IKE peer name.

 Copyright © Huawei Technologies Co., Ltd.

Views

GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure IKE negotiation, you need to reference an IKE peer in the specified view.

Prerequisites

An IKE peer has been created using the **ike peer** command in the system view.

Example

Reference the IKE peer **mypeer** in the GDOI policy.

```
<Huawei> system-view
[Huawei] ike peer mypeer
[Huawei-ike-peer-mypeer] quit
[Huawei] ipsec policy map2 4 gdoi
[Huawei-ipsec-policy-gdoi-map2-4] ike-peer mypeer
```

Related Topics

12.7.18 ipsec policy (system view)

12.7.15 ipsec

Function

The **ipsec** command creates a GDOI group IPSec policy and displays the GDOI group IPSec policy view.

The **undo ipsec** deletes the created GDOI group IPSec policy.

By default, no GDOI group IPSec policy is created.

Format

ipsec *policy-num*

undo ipsec *policy-num*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-num	Specifies the sequence number of a GDOI group IPSec policy.	The value is an integer that ranges from 1 to 65,535.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After registering with the KS successfully, a GM receives the TEK policies pushed by the KS. The TEK policies are used for generating TEK SAs on the GMs to encrypt inter-GM data flows. To generate a TEK policy on the KS, you need to run the **ipsec** command to configure a GDOI group IPSec policy.

Follow-up Tasks

You need to set parameters for the GDOI group IPSec policy, for example, referencing the IPSec proposal and security ACL.

Precautions

When a GDOI group IPSec policy is added, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

When the GDOI group IPSec policy is deleted, the KS immediately sends out rekey messages.

Example

Create a GDOI group IPSec policy and enter the GDOI group IPSec policy view.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2]
```

Related Topics

12.7.3 display gdoi ks group

 Copyright © Huawei Technologies Co., Ltd.

12.7.16 ipsec gdoi anti-replay force 32-bit enable

Function

The **ipsec gdoi anti-replay force 32-bit enable** command enables an A2A VPN Group Member (GM) device to use the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

The **undo ipsec gdoi anti-replay force 32-bit enable** command disables an A2A VPN GM device from using the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

By default, an A2A VPN GM device does not use the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

NOTE

This function is supported in V200R010C10 and later versions.

Format

ipsec gdoi anti-replay force 32-bit enable

undo ipsec gdoi anti-replay force 32-bit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as an A2A VPN GM device to connect to a non-Huawei device, you need to run the **ipsec gdoi anti-replay force 32-bit enable** command to enable

the Huawei GM device to use the least significant 32 bits to add timestamps to encrypted packets, if the Key Server (KS) advertises 64-bit timestamps of encrypted packets but the non-Huawei GM device supports only 32-bit timestamps of encrypted packets. This command ensures normal interconnection with the non-Huawei device.

Example

Enable an A2A VPN GM device to use the least significant 32 bits of the timestamp to add a timestamp to encrypted packets.

```
<Huawei> system-view
[] ipsec gdoi anti-replay force 32-bit enable
```

12.7.17 ipsec gdoi multicast-rekey ip

Function

The **ipsec gdoi multicast-rekey ip** command configures an IP address for multicast Rekey messages.

The **undo ipsec gdoi multicast-rekey ip** command deletes an IP address for multicast Rekey messages.

By default, no IP address is configured for multicast Rekey messages.

Format

ipsec gdoi multicast-rekey ip *ip-address*

undo ipsec gdoi multicast-rekey ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for multicast Rekey messages.	The value ranges from 224.0.1.0 to 239.255.255.255, in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an IP address for multicast Rekey messages is configured, GMs with this IP address and a UDP port number 848/4500 update TEK SAs or KEK SAs based on the multicast Rekey messages.

Precautions

The IP address for multicast Rekey messages configured on the GM must be the same as that configured on the KS.

After you configure this command, the following commands must be configured; otherwise, the configuration does not take effect.

- Run the **multicast routing-enable** command to enable the multicast routing function.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **pim dm** command to enable the PIM-DM function on an interface.
- Run the **igmp static-group** command to configure a static multicast group on an interface.

Example

Set the IP address for multicast Rekey messages to 225.0.0.1.

```
<Huawei> system-view
[Huawei] ipsec gdoi multicast-rekey ip 225.0.0.1
```

12.7.18 ipsec policy (system view)

Function

The **ipsec policy** command creates an IPSec policy and displays the IPSec policy view.

The **undo ipsec policy** command deletes an IPSec policy.

By default, no IPSec policy is configured.

Format

ipsec policy *policy-name seq-number* **gdoi**

undo ipsec policy *policy-name* [*seq-number*]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an IPSec policy.	The value is a string of 1 to 15 case-sensitive characters without question marks (?) or spaces.
seq-number	Specifies the sequence number of an IPSec policy.	The value is an integer that ranges from 1 to 4. A smaller value indicates a higher IPSec policy priority.
gdoi	Indicates that an IPSec SA is established in GDOI mode.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IPSec policy is a prerequisite to creating SAs and determines the methods used to protect specified data flows. An IPSec policy is identified by its name and sequence number, and multiple IPSec policies with the same IPSec policy name constitute an IPSec policy group.

On an A2A VPN network with many branches, a large number of multicast services need to be encrypted; therefore, the IPSec policy in GDOI mode is recommended.

Follow-up Procedure

Define negotiated IPSec parameters in the IPSec policy view and run the **ipsec policy (interface view)** command to apply the IPSec policy to an interface.

Example

Create an IPSec policy **policy1** whose sequence number is 3, and set the SA creation mode to GDOI.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 3 gdoi
[Huawei-ipsec-policy-gdoi-policy1-3]
```

Related Topics

12.7.19 ipsec policy (interface view)

12.7.39 security acl

12.7.14 ike-peer

12.7.8 display ipsec gdoi-policy

12.7.19 ipsec policy (interface view)

Function

The **ipsec policy** command applies an IPSec policy group to an interface.

The **undo ipsec policy** command deletes the IPSec policy group from an interface so that it is no longer protected by IPSec.

By default, no IPSec policy is applied to an interface.

Format

ipsec policy *policy-name*

undo ipsec policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the IPSec policy applied to an interface.	The value must be an existing IPSec policy name.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect data flows from an A2A VPN network on an interface, you need to apply a GDOI policy group to the interface. If the GDOI policy group is deleted from the interface, the interface no longer provides the encryption protection function.

After a GDOI policy group is applied to an interface, all GDOI policies in the group are applied to the interface to protect different data flows.

When sending a data flow, an interface matches the data flow with the GDOI policies in the GDOI policy group in ascending order of sequence numbers. If the data flow matches an ACL rule in a GDOI policy, the interface processes the data flow according to the GDOI policy; if the data flow does not match an ACL rule, the interface matches the data flow with another GDOI policy; if the data flow does not match any ACL rule in all the GDOI policies, the interface forwards the data flow directly without encryption protection.

Precautions

Only one GDOI policy group can be applied on an interface. A GDOI policy group can be applied to only one interface. To apply a new GDOI policy group to the interface, remove the previous one first.

In a GDOI policy group, if multiple policies are bound to different IKE peers, the remote addresses specified in the IKE peers cannot be the same. Otherwise, IKE negotiation of some GDOI policies fails.

Example

Bind an GDOI policy group named **policy1** to GE 1/0/2.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 1 gdoi
[Huawei-ipsec-policy-isakmp-policy1-1] quit
[Huawei] interface gigabitethernet 1/0/2
[Huawei-Gigabitethernet1/0/2] ipsec policy policy1
```

Related Topics

12.7.18 ipsec policy (system view)

12.7.20 local-id-type (GDOI Group View)

Function

The **local-id-type** command sets the local ID type for a GDOI group.

The **undo local-id-type** command restores the default local ID type of a GDOI group.

The default local ID type of a GDOI group is in the IP address format.

Format

local-id-type { **fqdn** | **ip** | **user-fqdn** }

undo local-id-type

Parameters

Parameter	Description	Value
fqdn	Sets the local ID type used in IKE negotiation to the name format.	-
ip	Sets the local ID type used in IKE negotiation to the IP address format.	-
user-fqdn	Sets the local ID type used in IKE negotiation to the user +domain name format.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Identity authentication is a self-protection mechanism for A2A VPN negotiation. It ensures security by confirming the identities of both communication parties. The identity types for the KS and GM can be different. You can use this command to set the identity type of the local end in a GDOI group, which is also called the local ID type.

Precautions

In pre-shared key authentication, the local ID type and local ID set for the local end must be the same as the peer ID type and peer ID set for the peer end.

 Copyright © Huawei Technologies Co., Ltd.

The method of setting the local ID type and local ID varies according to the identity authentication mode, as shown in **Table 12-77**.

Table 12-77 Relationship between the identity authentication mode, local ID type, and local ID

Authentication Mode	IP	FQDN	User-FQDN
Pre-shared key authentication (**pre-share**)	Supported The IP address is set using the **12.7.40 source address (GDOI Group View)** command.	Supported The ID is set using the **12.7.21 local-id (GDOI Group View)** command, indicating that this ID is used for identity authentication.	Supported The ID is set using the **12.7.21 local-id (GDOI Group View)** command, indicating that this ID is used for identity authentication.
RSA signature authentication (**rsa-signature**)	Not supported	Not supported	Not supported

Example

Set the local ID type of a GDOI group to the name format.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] local-id-type fqdn
```

Related Topics

12.7.21 local-id (GDOI Group View)

12.7.3 display gdoi ks group

12.7.21 local-id (GDOI Group View)

Function

The **local-id** command specifies a local ID for a GDOI group.

The **undo local-id** command deletes the local ID of a GDOI group.

By default, no local ID is specified for a GDOI group.

Format

local-id *id*

undo local-id

Parameters

Parameter	Description	Value
id	Specifies the local ID of a GDOI group.	The value is a string of 1 to 255 case-sensitive characters, with the exception of question marks (?).

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

When using the **12.7.20 local-id-type (GDOI Group View)** command to set the local ID type to FQDN or user-FQDN, you also need to run the **local-id** command to specify a local ID, which is used for identity authentication.

Example

Set the local ID of a GDOI group to **huawei**.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] local-id huawei
```

Related Topics

12.7.20 local-id-type (GDOI Group View)

12.7.3 display gdoi ks group

12.7.22 proposal (GDOI group IPSec policy View)

Function

The **proposal** command references an IPSec proposal in a GDOI group IPSec policy.

The **undo proposal** command cancels the preceding configuration.

By default, no IPSec proposal is referenced in a GDOI group IPSec policy.

Format

proposal *proposal-name*

undo proposal

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
proposal-name	Specifies the name of an IPSec proposal.	The value must be an existing IPSec proposal name.

Views

GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After using the **12.7.15 ipsec** command to create a GDOI group IPSec policy, you need to configure an IPSec proposal to define the IPSec protection method, for example, an encryption/authentication algorithm. The IPSec proposal takes effect only after being referenced in the GDOI group IPSec policy. After registering with the KS successfully, a GM obtains the IPSec proposal from the KS for further negotiating TEK SA establishment with other GMs.

Prerequisites

An IPSec proposal has been configured using the **12.6.109 ipsec proposal** command.

Precautions

The A2A VPN supports only the ESP protocol and the tunnel encapsulation mode.

When the IPSec proposal is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

When the IPSec proposal is added or deleted, the KS sends rekey messages immediately.

Example

Set an IPSec proposal named **prop1**, and reference this proposal to a GDOI group IPSec policy.

```
<Huawei> system-view
[Huawei] ipsec proposal prop1
[Huawei-ipsec-proposal-prop1] quit
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] proposal prop1
```

Related Topics

12.7.3 display gdoi ks group

 Copyright © Huawei Technologies Co., Ltd.

12.7.23 rekey authentication public-key rsa

Function

The **rekey authentication public-key rsa** command configures an RSA key pair used by rekey messages.

The **undo rekey authentication public-key rsa** command deletes the RSA key pair used by rekey messages.

By default, no RSA key pair is configured for rekey messages.

Format

rekey authentication public-key rsa *key-pair-name*

undo rekey authentication public-key rsa

Parameters

Parameter	Description	Value
key-pair-name	Specifies the RSA key pair name.	The value must be an existing RSA key pair name.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For security purposes, the KS signs the encrypted rekey messages. That is, the KS uses its own RSA private key to encrypt the data obtained using the hash algorithm from the encrypted rekey messages. After receiving the rekey messages, GMs use the RSA public key, hash algorithm, and encryption algorithm of the KS to decrypt them. The RSA public key, hash algorithm, and encryption algorithm are sent by the KS to registered GMs.

You can run the **rekey authentication public-key rsa** command to configure an RSA key pair used by rekey messages.

Prerequisite

An RSA key pair has been created using the **19.17.106 pki rsa local-key-pair create** command, or an RSA key pair has been imported to the device memory using the **19.17.95 pki import rsa-key-pair** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Configure an RSA key pair used by rekey messages.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create keytest modulus 2048 exportable
 Info: The name of the new key-pair will be: keytest
 Generating key-pairs...
.+++
......+++
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey authentication public-key rsa keytest
```

Related Topics

12.7.3 display gdoi ks group

12.7.24 rekey destination address

Function

The **rekey destination address** command configures a destination IP address used by multicast rekey messages.

The **undo rekey destination address** command deletes the destination IP address used by multicast rekey messages.

By default, no destination IP address is configured for multicast rekey messages.

Format

rekey destination address *ip-address*

undo rekey destination address

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address used by multicast rekey messages.	The value is in dotted decimal notation in a range from 224.0.0.0 to 239.255.255.255, excluding reserved multicast addresses.

 Copyright © Huawei Technologies Co., Ltd.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In multicast rekey mode, a GM registers with the KS and joins a specific multicast group. The KS sends rekey messages to all the GMs that join the group in multicast mode. In this scenario, you need to run the **rekey destination address** command to configure a destination IP address used by rekey messages in advance. Otherwise, the KS cannot send multicast rekey messages.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the destination IP address of multicast rekey messages to 239.10.1.1.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey destination address 239.10.1.1
```

Related Topics

12.7.3 display gdoi ks group

12.7.25 rekey encryption-algorithm

Function

The **rekey encryption-algorithm** command configures an encryption algorithm for rekey messages.

The **undo rekey encryption-algorithm** command restores the default encryption algorithm used by rekey messages.

The default encryption algorithm used by rekey messages is AES-256.

Format

rekey encryption-algorithm { **des** | **3des** | **aes-128** | **aes-192** | **aes-256** }

undo rekey encryption-algorithm

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
des	Specifies the 56-bit DES-CBC encryption algorithm.	-
3des	Specifies the 168-bit 3DES-CBC encryption algorithm.	-
aes-128	Specifies the 128-bit AES-CBC encryption algorithm.	-
aes-192	Specifies the 192-bit AES-CBC encryption algorithm.	-
aes-256	Specifies the 256-bit AES-CBC encryption algorithm.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For security purposes, the KS signs the encrypted rekey messages. That is, the KS uses its own RSA private key to encrypt the data obtained using the hash algorithm from the encrypted rekey messages. After receiving the rekey messages, GMs use the RSA public key, hash algorithm, and encryption algorithm of the KS to decrypt them. The RSA public key, hash algorithm, and encryption algorithm are sent by the KS to registered GMs.

You can run the **rekey encryption-algorithm** command to configure the encryption algorithm for rekey messages.

Precautions

The DES and 3DES algorithms are not secure and therefore not recommended.

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the encryption algorithm for rekey messages to AES-192.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey encryption-algorithm aes-192
```

Related Topics

12.7.3 display gdoi ks group

12.7.26 rekey retry

Function

The **rekey retry** command configures the number of retransmissions and retransmission interval for rekey messages.

The **undo rekey retry** command restores the default number of retransmissions and retransmission interval of rekey messages.

By default, the number of retransmissions of rekey messages is 3 and the retransmission interval is 10 seconds.

Format

rekey retry limit *limit* **interval** *interval*

undo rekey retry

Parameters

Parameter	Description	Value
limit *limit*	Specifies the number of times for retransmitting rekey messages.	The value is an integer that ranges from 1 to 6.
interval *interval*	Specifies the interval at which rekey messages are retransmitted.	The value is an integer that ranges from 5 to 20, in seconds.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

After a GM registers with the KS successfully, the KS periodically sends rekey messages to the GM to update the TEK and KEK policies. When the network is unstable, the GM fails to receive rekey messages and thereby cannot update these policies in a timely manner, causing service interruption.

To solve this problem, the A2A VPN provides a mechanism for retransmitting rekey messages.

- Unicast rekey

  If the KS does not receive a response from the GM within a specified period after sending a rekey message, the KS retransmits the rekey message until the number of retransmissions reaches the specified value.
- Multicast rekey

  After sending a rekey message, the KS periodically retransmits it until the number of retransmissions reaches the specified value.

You can run the **rekey retry** command to change the number of retransmissions and retransmission interval of rekey messages based on actual scenarios. For example, you can increase the number of retransmissions when network congestion occurs.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the number of retransmissions of rekey messages to 4 and the retransmission interval to 8 seconds.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey retry limit 4 interval 8
```

Related Topics

12.7.3 display gdoi ks group

12.7.27 rekey sa duration time-based

Function

The **rekey sa duration time-based** command configures the KEK SA hard lifetime.

The **undo rekey sa duration time-based** command restores the default KEK SA hard lifetime.

The default KEK SA hard lifetime is 86,400 seconds.

Format

rekey sa duration time-based *seconds*

 Copyright © Huawei Technologies Co., Ltd.

undo rekey sa duration time-based

Parameters

Parameter	Description	Value
seconds	Specifies the KEK SA hard lifetime.	The value is an integer that ranges from 600 to 604,800, in seconds.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The KEK SA lifetime is used to periodically update the KEK SA, which reduces the risk of KEK SA cracking and improves security.

The KEK SA lifetime falls into the following types:

- Hard lifetime (hard timeout period): defines the number of seconds until the KEK SA expires.
- Soft lifetime (soft timeout period): defines the number of seconds until the IKE process is informed that the KEK SA is about to expire. This is to provide enough time for the creation of a new KEK SA before the hard lifetime is reached.

When the soft lifetime expires, the KS generates a new KEK SA and sends it to GMs through rekey messages. After receiving the rekey messages, GMs delete the old KEK SA and use the new one when the hard lifetime expires.

The value of the soft lifetime is related to the transmission mode, number of retransmissions, and retransmission interval of rekey messages. **Table 12-78** shows the detailed calculation methods.

Table 12-78 Soft lifetime values

Transmission Mode of Rekey Messages	Soft Lifetime Value
Unicast rekey	Hard lifetime - (30 + (Number of retransmissions + 1) x Retransmission interval + 5 x Number of GMs in the group/50)

 Copyright © Huawei Technologies Co., Ltd.

Transmission Mode of Rekey Messages	Soft Lifetime Value
Multicast rekey	Hard lifetime - (30 + (Number of retransmissions + 1) x Retransmission interval)

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the KEK SA hard lifetime to 3600 seconds.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey sa duration time-based 3600
```

Related Topics

12.7.3 display gdoi ks group

12.7.28 rekey sig-hash-algorithm

Function

The **rekey sig-hash-algorithm** command configures the signature hash algorithm for rekey messages.

The **undo rekey sig-hash-algorithm** command restores the default signature hash algorithm for rekey messages.

The default signature hash algorithm for rekey messages is SHA2-256.

Format

rekey sig-hash-algorithm { **sha1** | **sha2-256** | **sha2-384** | **sha2-512** }

undo rekey sig-hash-algorithm

Parameters

Parameter	Description	Value
sha1	Sets the signature hash algorithm for rekey messages to SHA1.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sha2-256	Sets the signature hash algorithm for rekey messages to SHA2-256.	-
sha2-384	Sets the signature hash algorithm for rekey messages to SHA2-384.	-
sha2-512	Sets the signature hash algorithm for rekey messages to SHA2-512.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

For security purposes, the KS signs the encrypted rekey messages. That is, the KS uses its own RSA private key to encrypt the data obtained using the hash algorithm from the encrypted rekey messages. After receiving the rekey messages, GMs use the RSA public key, hash algorithm, and encryption algorithm of the KS to decrypt them. The RSA public key, hash algorithm, and encryption algorithm are sent by the KS to registered GMs.

You can run the **rekey sig-hash-algorithm** command to configure the signature hash algorithm for rekey messages.

Precautions

The SHA1 algorithm is not secure and therefore not recommended.

When the KS connects to a GM, you need to confirm the signature hash algorithm supported by the GM. For example, the GM running a software version earlier than V200R010C00 supports only the SHA1 algorithm.

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the signature hash algorithm for rekey messages to SHA2-384.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey sig-hash-algorithm sha2-384
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.7.3 display gdoi ks group

12.7.29 rekey transport-type

Function

The **rekey transport-type** command configures the transmission mode of rekey messages.

The **undo rekey transport-type** command restores the default transmission mode of rekey messages.

The default transmission mode of rekey messages is multicast.

Format

rekey transport-type { **multicast** | **unicast** }

undo rekey transport-type

Parameters

Parameter	Description	Value
multicast	Sets the transmission mode to multicast.	-
unicast	Sets the transmission mode to unicast.	-

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

After GMs register with the KS, the KS periodically sends new TEK SAs or KEK SAs to GMs through rekey messages to improve security. A rekey message carries parameters such as information about the data flows to be protected, encryption algorithm, key, and SA lifetime.

The KS supports two modes for transmitting rekey messages:

- Multicast mode

  The KS sends rekey messages to GMs in the multicast group using the multicast address as the destination IP address. After successfully registering with the KS, GMs join a specific multicast group. All GMs in the group will receive the rekey messages.

 Copyright © Huawei Technologies Co., Ltd.

In multicast mode, GM entries on the KS do not age. If a GM keeps changing its IP address to register with the KS, the number of GM entries on the KS exceeds the maximum value. As a result, new GMs cannot register with the KS. In this instance, you need to run the **12.7.30 reset gdoi ks group** command to clear GM entries.

- Unicast mode

  The KS sends a rekey message to each GM using the GM address as the destination IP address. After receiving the rekey message, each GM sends an ACK message to the KS. The KS updates the current active GM list based on the received ACK messages and sends rekey messages only to active GMs.

  In unicast mode, the KS sends a rekey message to each GM. If there are too many GMs that may bring heavy load to the KS, the multicast mode is recommended.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the transmission mode of rekey messages to unicast.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] rekey transport-type unicast
```

Related Topics

12.7.3 display gdoi ks group

12.7.30 reset gdoi ks group

Function

The **reset gdoi ks group** command clears the TEK SA and KEK SA related to a given GDOI group of a KS.

Format

reset gdoi ks group *group-name*

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

After this command is executed, the TEK SA and KEK SA related to a given GDOI group of the KS are deleted. As a result, services between the KS and GM are interrupted until the GM re-registers with the KS after the TEK SA of the GM ages out.

Example

Clear the TEK SA and KEK SA related to a KS GDOI group.

```
<Huawei> reset gdoi ks group gr1
```

Related Topics

12.7.7 display gdoi ks sa

12.7.31 reset gdoi ks members

Function

The **reset gdoi ks members** command clears statistics about GDOI group members of a KS.

Format

reset gdoi ks members group *group-name*

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

NOTE

After this command is executed, cleared statistics cannot be restored.

When diagnosing and locating GM registration problems, you can collect statistics only within a given length of time for fault location. You need to run the **reset gdoi ks members** command to clear historical GDOI group member statistics before statistics collection, and then run the **12.7.4 display gdoi ks members** command to view the current statistics about GDOI group members.

Example

Clear statistics about GDOI group members of a KS.

```
<Huawei> reset gdoi ks members group gr1
```

12.7.32 reset gdoi ks members history record

Function

The **reset gdoi ks members history record** command clears historical information about the GDOI group members of a KS.

Format

reset gdoi ks members history record [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group. If **group** is not specified, the historical information about members in all GDOI groups is cleared.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

NOTE

After this command is executed, cleared statistics cannot be restored.

When diagnosing and locating a GM registration failure or abnormal logout, you can collect statistics only within a given length of time for fault location. You need

to run the **reset gdoi ks members history record** command to clear historical statistics before statistics collection, and then run the **12.7.6 display gdoi ks rekey statistics** command to view the current statistics about the rekey messages on the KS.

Example

Clear historical information about the GMs in GDOI group **gr1**.

```
<Huawei> reset gdoi ks members history record group gr1
```

12.7.33 reset gdoi ks rekey statistics

Function

The **reset gdoi ks rekey statistics** command clears statistics about the rekey messages on a KS.

Format

reset gdoi ks rekey statistics [**group** *group-name*]

Parameters

Parameter	Description	Value
group *group-name*	Specifies the name of a GDOI group. If **group** is not specified, statistics about the rekey messages of all GDOI groups are cleared.	The value must be the name of an existing GDOI group.

Views

User view

Default Level

3: Configuration level

Usage Guidelines

NOTE

After this command is executed, cleared statistics cannot be restored.

When diagnosing and locating rekey messages problems, you can collect statistics only within a given length of time for fault location. You need to run the **reset gdoi ks rekey statistics** command to clear historical statistics before statistics collection, and then run the **12.7.6 display gdoi ks rekey statistics** command to view the current statistics about the rekey messages on the KS.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear statistics about the rekey messages of GDOI group **gr1**.

```
<Huawei> reset gdoi ks rekey statistics group gr1
```

12.7.34 qos group

Function

The **qos group** command configures the QoS group to which the IPSec packets belong.

The **undo qos group** command deletes the QoS group to which the IPSec packets belong.

By default, no QoS group is configured.

Format

qos group *qos-group-value*

undo qos group

Parameters

Parameter	Description	Value
qos-group-value	Specifies the ID of the QoS group.	The value is an integer that ranges from 1 to 99.

Views

Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, Efficient VPN policy view, GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When both an IPSec policy and a QoS policy are used on an interface, you can run this command to specify the QoS group to which the IPSec packets belong to facilitate QoS management.

Precautions

This command takes effect in the packet encapsulation process but not the packet decapsulation process. That is, the command takes effect only for incoming packets.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

After QoS for IPSec packets is enabled, run the **if-match qos-group** *qos-group-value* command in the traffic classifier view to configure a matching rule based on the QoS group.

Example

Configure the QoS group to which the IPSec packets belong in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos group 30
```

Related Topics

12.6.104 ipsec policy (interface view)
12.6.106 ipsec policy-template
12.6.107 ipsec profile (interface view)
12.6.98 ipsec efficient-vpn (system view)

12.7.35 qos pre-classify

Function

The **qos pre-classify** command enables pre-extraction of original IP packets.

The **undo qos pre-classify** command disables pre-extraction of original IP packets.

By default, pre-extraction of original IP packets is disabled.

Format

qos pre-classify

undo qos pre-classify

Parameters

None

Views

Tunnel interface view, Efficient VPN policy view, Manual IPSec policy view, IPSec policy view, IPSec policy template view, IPSec profile view, GDOI policy view, BD view, VBDIF interface view, VPN instance view, Virtual template interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In tunnel mode, QoS parameters such as the packet header and protocol type in original packets are hidden after IP packets are encapsulated through GRE,

 Copyright © Huawei Technologies Co., Ltd.

VXLAN, L2TP, and IPSec. Although GRE, VXLAN, L2TP, and IPSec uses the DSCP field in original packets as the DSCP field in the IP packet header, some QoS solutions require quintuple information. The encryption device can pre-extract quintuple information including the source address, destination address, protocol type, source port number, and destination port number to facilitate refined QoS management on GRE, VXLAN, L2TP, and IPSec packets.

In an A2A VPN solution, the device uses the IP header of original packets as the IP header for encapsulated A2A VPN packets. Therefore, you do not need to configure this command if the device classifies packets based on the source address, destination address, or protocol type only.

Follow-up Procedure

After pre-extraction of original IP packets is enabled, run the **if-match acl** { *acl-number* | *acl-name* } command in the traffic classifier view to configure a matching rule based on the ACL.

Example

Enable pre-extraction of original IP packets in the IPSec policy view.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 10 isakmp
[Huawei-ipsec-policy-isakmp-policy1-10] qos pre-classify
```

Related Topics

12.6.104 ipsec policy (interface view)

12.6.106 ipsec policy-template

12.6.107 ipsec profile (interface view)

12.6.98 ipsec efficient-vpn (system view)

12.7.36 reset ipsec gdoi-sa

Function

The **reset ipsec gdoi-sa** command deletes TEK SAs and KEK SAs of all created GDOI policies.

Format

reset ipsec gdoi-sa [**policy** *policy-name* [*seq-number*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy *policy-name* [*seq-number*]	Specifies the name and sequence number of a GDOI policy. The *seq-number* parameter is optional. If *seq-number* is not specified, all the TEK SAs and KEK SAs in the GDOI policy group specified by *policy-name* are deleted. This parameter is specified by running the **12.6.105 ipsec policy (system view)** command.	The value must be an existing GDOI policy name and sequence number.

Views

User view

Default Level

3: Management level

Usage Guidelines

When running the **reset ipsec gdoi-sa** command, pay attention to the following:

- If no parameter is specified, the TEK SAs and KEK SAs of all GDOI policies are deleted.
- If both **policy** and *seq-number* are specified, the TEK SAs and KEK SAs of the GDOI policy with the specified name and sequence is deleted. If only **policy** is specified, all the TEK SAs and KEK SAs in the specified GDOI policy group are deleted.

Example

Delete the TEK SAs and KEK SAs of all GDOI policies.

```
<Huawei> reset ipsec gdoi-sa
```

Delete all the TEK SAs and KEK SAs in the GDOI policy group **policy1**.

```
<Huawei> reset ipsec gdoi-sa policy policy1
```

Delete the TEK SA and KEK SA of the GDOI policy with the name **policy1** and sequence number 4.

```
<Huawei> reset ipsec gdoi-sa policy policy1 4
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.7.9 display ipsec gdoi-sa

12.7.37 sa duration time-based

Function

The **sa duration time-based** configures the TEK SA hard lifetime.

The **undo sa duration time-based** restores the TEK SA hard lifetime to the default value.

The default TEK SA hard lifetime is 3600 seconds.

Format

sa duration time-based *seconds*

undo sa duration time-based

Parameters

Parameter	Description	Value
seconds	Specifies the hard lifetime of a TEK SA.	The value is an integer that ranges from 600 to 604,800, in seconds.

Views

GDOI IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The TEK SA lifetime is used to update the TEK SA periodically, which reduces the risk of TEK SA cracking and improves security.

The TEK SA lifetime falls into the following types:

- Hard lifetime (hard timeout period): defines the number of seconds until the TEK SA expires.
- Soft lifetime (soft timeout period): defines the number of seconds until the IKE process is informed that the TEK SA is about to expire. This is to provide enough time for the creation of a new TEK SA before the hard lifetime is reached.

 Copyright © Huawei Technologies Co., Ltd.

When the soft lifetime expires, the KS generates a new TEK SA and sends it to GMs through rekey messages. After receiving the rekey messages, GMs use the new TEK SA 30 seconds prior to hard lifetime expiry. When the hard lifetime expires, the old TEK SA is deleted.

The value of the soft lifetime is related to the transmission mode, number of retransmissions, and retransmission interval of rekey messages. **Table 12-79** shows the detailed calculation methods.

Table 12-79 Soft lifetime values

Transmission Mode of Rekey Messages	Soft Lifetime Value
Unicast rekey	Hard lifetime - (90 + (Number of retransmissions + 1) x Retransmission interval + 5 x Number of GMs in the group/50)
Multicast rekey	Hard lifetime - (90 + (Number of retransmissions + 1) x Retransmission interval)

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the TEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the TEK SA hard lifetime to 7200 seconds.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] sa duration time-based 7200
```

Related Topics

12.7.3 display gdoi ks group

12.7.38 sa receive-only

Function

The **sa receive-only** command sets the SA mode to Receive_Only. In this mode, the GM can send only plaintext packets but can receive both plaintext and ciphertext packets.

The **undo sa receive-only** command restores the default SA mode.

By default, the SA mode is Normal. In this mode, the GM sends and receives only ciphertext packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

sa receive-only

undo sa receive-only

Parameters

None

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If SA modes cannot be configured in stages when you deploy the A2A VPN on an existing network (such as the MPLS VPN), services will be interrupted because a GM that joins a group can send and receive only ciphertext packets but the GM that has not joined the group can send and receive only plaintext packets. In this case, you need to set the SA mode on the GM and KS to implement the phased deployment of the A2A VPN.

The procedure is as follows:

1. Set the SA mode to Receive_Only on the KS. The KS will deliver this SA mode to GMs.
2. Deploy GMs on the A2A VPN one by one. The registered GMs work in Receive_Only mode, so they can communicate with the newly deployed GMs that haven't registered with the KS.
3. After all the GMs are deployed, set the SA mode to Receive_Option on the GMs. A GM in Receive_Option mode can still communicate with a GM in Receive_Only mode.
4. After all the GMs are switched to Receive_Option mode, set the SA mode to Normal on the KS.

Precautions

When the SA mode is changed, the KS immediately sends rekey messages.

When the SA mode is switched on the KS, traffic between GMs is interrupted for a short period of time.

Example

Set the SA mode to Receive_Only.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] sa receive-only
```

Related Topics

12.7.12 gdoi sa direction receive-option
12.7.3 display gdoi ks group

12.7.39 security acl

Function

The **security acl** command references an ACL.

The **undo security acl** command cancels the configuration.

By default, no ACL is referenced.

Format

security acl *acl-number*

undo security acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.

Views

GDOI policy view, GDOI group IPSec policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a GM registers with the KS, the GM obtains security policies including the ACL rules from the KS. The ACL rules configured on the KS determine data flows to be encrypted and data flows to be forwarded in plain text. The GM matches received data flows with the ACL rules obtained from the KS. If the matched ACL rule defines a permit action, the GM encrypts the data flows and forwards them; if the matched ACL rule defines a deny action, the GM forwards the data flows in plain text. If a data flow matches an ACL rule that defines a permit action, but the GM wants to forward the data flow in plain text, you can configure a local ACL rule to define data flows not to be protected. When a device forwards a data flow, it matches the data flow with the local ACL rule first. If the data flow matches the local ACL rule, the device forwards the data flow in plain text. If not, the device matches the data flow with the ACL rules obtained from the KS.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The ACL rule configured in a GDOI policy can only be set to deny.

If no ACL rule is configured in a GDOI policy or all ACL rules configured in a GDOI policy are set to deny, a GM will fail to register with the KS.

If the KS sends more than 100 ACL rules to a GM, only 100 ACL rules take effect. If more than 100 ACL rules are configured on a GM, only 100 ACL rules take effect.

When configuring an ACL on the KS, you must deploy ACL rules based on the encrypted data flows to prevent some unencrypted packets from being discarded by IPSec verification, for example, rekey packets and IKE packets. When the ACL range is large, you must configure "deny" ACL rules for the packets that are not encrypted and should not be discarded. This ensures that such packets will not be dropped by IPSec verification.

When an ACL rule is modified in the GDOI group IPSec policy, the KS immediately sends rekey messages. If there are multiple GDOI IPSec policies in a GDOI group, the KS immediately sends out rekey messages when deleting the ACL in a GDOI group IPSec policy. If there is only one GDOI group IPSec policy in a GDOI group, the KS fails to send out rekey messages when deleting the ACL in the GDOI group IPSec policy.

Only the following optional parameters are supported for a security ACL rule: **source**, **destination**, **source-port eq**, and **destination-port eq**.

Example

Reference ACL 3101 in a GDOI policy.

```
<Huawei> system-view
[Huawei] acl number 3101
[Huawei-acl-adv-3101] rule deny ip destination 10.1.1.2 0.0.0.0
[Huawei-acl-adv-3101] quit
[Huawei] ipsec policy policy1 4 gdoi
[Huawei-ipsec-policy-gdoi-policy1-4] security acl 3101
```

Reference ACL 3101 in a GDOI group IPSec policy.

```
<Huawei> system-view
[Huawei] acl number 3101
[Huawei-acl-adv-3101] rule permit ip destination 10.1.1.2 0.0.0.0
[Huawei-acl-adv-3101] quit
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] ipsec 2
[Huawei-gdoi-group-gr1-ipsec-2] security acl 3101
```

Related Topics

12.7.8 display ipsec gdoi-policy
12.7.3 display gdoi ks group

12.7.40 source address (GDOI Group View)

Function

The **source address** command configures an IP address for a KS.

The **undo source address** command deletes the configured IP address of a KS.

By default, no IP address is configured for a KS.

Format

source address *ip-address*

undo source address

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a KS.	The value is in dotted decimal notation.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GM registers with the KS, the GM carries the specified KS IP address to perform IKE SA negotiation with the KS. If the IP address configured for the KS is different from that carried by the GM, the IKE SA negotiation between the two ends fails, causing a GM registration failure. After the GM registers successfully, the KS sends a rekey message to the GM using the KS IP address as the source IP address of the rekey message.

Precautions

When the configuration is modified, the KS does not send rekey messages immediately until the KEK SA soft lifetime expires. To make the modified configuration take effect immediately, enter the **12.7.11 gdoi ks rekey** command to manually trigger the KS to send out rekey messages.

Example

Set the IP address of a KS to 10.1.1.1.

```
<Huawei> system-view
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] source address 1.1.1.1
```

Related Topics

12.7.3 display gdoi ks group

 Copyright © Huawei Technologies Co., Ltd.

12.7.41 tunnel local

Function

The **tunnel local** command configures an IP address for the local end of an A2A VPN tunnel.

The **undo tunnel local** command deletes the IP address of the local end of an A2A VPN tunnel.

By default, no IP address is configured for the local end of an A2A VPN tunnel.

Format

tunnel local { *ip-address* | **applied-interface** }

undo tunnel local

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address for the local end of an A2A VPN tunnel.	THe value is a valid IPv4 address in dotted decimal notation.
applied-interface	Specifies the primary address of the interface to which the IPSec policy is applied as the IP address for the local end of an A2A VPN tunnel.	-

Views

GDOI policy view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to specify a start point for an A2A VPN tunnel.

For a manually created IPSec policy, run the **tunnel local** *ip-address* command to configure an IP address for the local end before you can create an SA. Only after correct IP addresses are configured for the local end (start point) and remote end (end point), an A2A VPN tunnel can be established between the two ends.

For a GDOI policy, you do not need to configure a local address for A2A VPN because the device will select an appropriate local address based on routing

 Copyright © Huawei Technologies Co., Ltd.

information during SA negotiation. However, you need to configure a local address in the following cases:

- If the IP address of the interface to which an IPSec policy is applied varies or is unknown, run the **tunnel local** *ip-address* command to specify the IP address of another interface (such as the loopback interface) on the device as the IP address for the local end of an A2A VPN tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the IP address of the interface as the IP address for the local end of an A2A VPN tunnel.
- If the interface to which an IPSec policy is applied has multiple IP addresses (one primary IP address and several secondary IP addresses), run the **tunnel local** *ip-address* command to specify one of these IP addresses as the IP address for the local end of an A2A VPN tunnel. Otherwise, run the **tunnel local applied-interface** command to specify the IP address of the interface as the IP address for the local end of an A2A VPN tunnel.
- If equal-cost routes exist between the local and remote ends, run the **tunnel local** { *ip-address* | **applied-interface** } command to configure an IP address for the local end of an A2A VPN tunnel.

Example

Configure the primary address of the interface to which the GDOI policy is applied as the IP address for the local end.

```
<Huawei> system-view
[Huawei] ipsec policy policy1 3 gdoi
[Huawei-ipsec-policy-gdoi-policy1-3] tunnel local applied-interface
```

Related Topics

12.7.18 ipsec policy (system view)

12.7.42 user-table (GDOI Group View)

Function

The **user-table** command references an IKE user table in a GDOI group.

The **undo user-table** command cancels the reference of an IKE user table.

By default, no IKE user table is referenced in a GDOI group.

Format

user-table *user-table-id*

undo user-table

Parameters

Parameter	Description	Value
user-table-id	Specifies the ID of an IKE user table.	The value must be the ID of an existing IKE user table.

 Copyright © Huawei Technologies Co., Ltd.

Views

GDOI group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a GM registers with the KS, the KS and GM use pre-shared key authentication to authenticate each other. The initiator uses the pre-shared key to encrypt the data to be transmitted. The receiver uses the same pre-shared key to decrypt the data. If the decryption succeeds, the initiator passes the authentication.

The IKE user table records the mappings between the GM IDs and pre-shared keys. After a GDOI group references an IKE user table, the KS sends the pre-shared key to a GM based on the GM ID. During identity authentication, the KS searches the IKE user table for the pre-shared key corresponding to the GM ID to complete identity authentication.

Prerequisites

An IKE user table has been created using the **12.6.74 ike user-table** command.

Precautions

Each GDOI group can reference only one IKE user table.

Example

Reference IKE user table 10 in a GDOI group.

```
<Huawei> system-view
[Huawei] ike user-table 10
[Huawei-ike-user-table-10] quit
[Huawei] gdoi ks group gr1
[Huawei-gdoi-group-gr1] user-table 10
```

Related Topics

12.7.3 display gdoi ks group

12.8 SSL VPN Configuration Commands

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact Huawei technical support personnel.

 Copyright © Huawei Technologies Co., Ltd.

12.8.1 background-color

Function

The **background-color** command configures the background color of the virtual gateway web GUI.

The **undo background-color** command restores the default setting.

The RGB color model of the default background color on the virtual gateway web GUI is **#F6F6F6**.

Format

background-color *color-value*

undo background-color

Parameters

Parameter	Description	Value
color-value	Background color of the virtual gateway web GUI.	The RGB color model is used. The value format is #*H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **background-color** command to configure the background color on the virtual gateway web GUI.

Precautions

If you run the **background-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the RGB color model of the background color of the virtual gateway web GUI to **#EE0000**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] background-color #EE0000
```

Related Topics

12.8.21 max-user

12.8.2 banner-color

Function

The **banner-color** command configures the banner color of the virtual gateway web GUI.

The **undo banner-color** command restores the default setting.

The RGB color model of the default banner color on the virtual gateway web GUI is **#EEEEEE**.

Format

banner-color *color-value*

undo banner-color

Parameters

Parameter	Description	Value
color-value	Banner color of the virtual gateway web GUI.	The RGB color model is used. The value format is #*H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **banner-color** command to configure the banner color on the virtual gateway web GUI.

Precautions

If you run the **banner-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the RGB color model of the banner color of the virtual gateway web GUI to **#000011**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] banner-color #000011
```

Related Topics

12.8.21 max-user

12.8.3 bind acl

Function

The **bind acl** command binds an ACL to the IP forwarding service.

The **undo bind acl** command unbinds an ACL from the IP forwarding service.

By default, no ACL is bound to the IP forwarding service.

Format

bind acl *acl-number*

undo bind acl

Parameters

Parameter	Description	Value
acl-number	ACL number that you want to bind to the IP forwarding service.	The value is an integer ranging from 3000 to 3999.

Views

IP forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSL VPN gateway allows remote terminals to communicate with internal servers at the network layer. For example, remote terminals and internal servers implement file sharing.

Remote users are not allowed to access confidential data on the intranet. After an ACL is bound to the IP forwarding service, the SSL VPN gateway filters remote users' IP packets based on this ACL to limit the remote users access rights. For example, if you want remote users to access only internal server 1.1.1.1, bind an ACL to the IP forwarding service to permit only the IP packets destined for 1.1.1.1 and discard other IP packets.

Prerequisites

The ACL that you want to bind to the IP forwarding service has been created.

Precaution

If you run the **bind acl** command multiple times in the same IP forwarding service view, only the latest configuration takes effect.

Example

Bind an ACL to the IP forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] bind acl 3001
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.4 bind domain

Function

The **bind domain** command binds an AAA domain to a virtual gateway.

The **undo bind domain** command unbinds an AAA domain from a virtual gateway.

By default, no AAA domain is bound to a virtual gateway.

Format

bind domain *domain-name*

undo bind domain

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
domain-name	Name of an AAA domain.	The value is the name of an existing AAA domain.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent unauthorized remote users from accessing internal resources and protect intranet security, each virtual gateway must authenticate login remote users. After being bound to an AAA domain, a virtual gateway performs AAA authentication for all login remote users. Only the authenticated remote users are allowed to access internal resources.

Prerequisites

The AAA domain that you want to bind to the virtual gateway has been created.

Precautions

The virtual gateway supports only two authentication methods: local authentication and RADIUS authentication.

If you need to modify the bound AAA domain after the basic SSL VPN functions are enabled, use the **undo enable** command to disable the basic SSL VPN functions first.

Example

Bind the AAA domain **admin** to the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] bind domain admin
```

Related Topics

12.8.21 max-user

12.8.5 bind ip-pool

Function

The **bind ip-pool** command binds an IP address pool to the IP forwarding service.

The **undo bind ip-pool** command unbinds an IP address pool from the IP forwarding service.

By default, no IP address pool is bound to the IP forwarding service.

Format

bind ip-pool *pool-name*

undo bind ip-pool

Parameters

Parameter	Description	Value
pool-name	IP address pool that you want to bind to the IP forwarding service.	The value is the name of an existing ip address pool.

Views

IP forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IP forwarding function allows remote terminals to communicate with internal servers at the network layer.

When a remote user starts the IP forwarding service, the remote host automatically downloads the client software on the web page. The client software then installs a virtual network adapter on the remote host. The client software is responsible for setting up an SSL connection between the terminal and gateway, requesting an IP address for the virtual network adapter, and creating a route with the virtual network adapter as outbound interface.

After an IP address pool is bound to the IP forwarding service, an IP address is allocated from the IP address pool to the virtual network adapter.

Prerequisites

The IP address pool that you want to bind to the IP forwarding service has been created.

Precautions

If you want to configure the rental period of an IP address pool, the rental period must be longer than the maximum online duration of the SSL VPN remote user.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **bind ip-pool** command multiple times in the same IP forwarding service view, only the latest configuration takes effect.

Example

Bind the IP address pool **pool1** to the IP forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] bind ip-pool pool1
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

8.3.83 ip pool (system view)

12.8.6 cut user

Function

The **cut user** command forcibly disconnects remote users from a virtual gateway.

Format

cut user { **name** *user-name* | **id** *user-id* | **all** }

Parameters

Parameter	Description	Value
name *user-name*	Specifies the name of the remote user that you want to disconnect from a virtual gateway.	The value is the name of an existing remote user.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
id *user-id*	Specifies the ID of the remote user that you want to disconnect from a virtual gateway. After a user goes online, the virtual gateway automatically allocates an ID for the remote user. To view the IDs of all online remote users, run the **display sslvpn gateway access-user** command.	The value is an integer and the value range depends on device types. • AR100&AR120&AR150&AR160&AR200 series: 0 to 9 • AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 0 to 49 • AR2220E, AR2220, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 0 to 99 • AR2204XE, AR2204XE-DC, AR2240 (using SRU80, or SRU100E, SRU200, or SRU200E, or SRU400), AR3200 (using SRU80, or SRU100E, SRU200, or SRU200E, or SRU400), AR3600 (using SRUX5) series: 0 to 199
all	Disconnects all remote users from a virtual gateway.	-

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can disconnect a remote user by specifying the remote user's name or ID or disconnect all remote users from a virtual gateway. The virtual gateway still stores information about the disconnected remote users.

Follow-up Procedure

Run the **display sslvpn gateway access-user** command to view remote users' status.

Example

Disconnect the user **jackson** from the virtual gateway.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] cut user name jackson
```

Related Topics

12.8.21 max-user

12.8.9 display sslvpn gateway access-user

12.8.7 description

Function

The **description** command configures the description of a service on a virtual gateway.

The **undo description** command deletes the service description on a virtual gateway.

By default, the services on a virtual gateway do not have description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Service description on a virtual gateway.	The value is a string of 1 to 80 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Web proxy service view, port forwarding service view, or IP forwarding service view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the service description on a virtual gateway, such as, the usage or use scenario of a service. The service description is used to differentiate services.

Precautions

If you run the **description** command multiple times in the same service view, only the latest configuration takes effect.

Example

Configure the description for the port forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type port-forwarding resource pres1
[Huawei-sslvpn-users-pf-res-presl] description this service is used to access the ftp server
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.8 display sslvpn gateway

Function

The **display sslvpn gateway** command displays virtual gateway information.

Format

display sslvpn gateway [*gateway-name*]

Parameters

Parameter	Description	Value
gateway-name	Displays information about a specified virtual gateway. If this parameter is not specified, the system displays information about all virtual gateways.	The value is the name of an existing virtual gateway.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users
 ------------------------------------------------------------------------------
  Gateway name                 :   users
  Status                       :   enable
  Intranet interface           :   Ethernet1/0/0
  Intranet IP                  :   10.1.17.1
  Domain                       :   default
  Max-user                     :   200
  Max-onlinetime(minute)       :   120
  Web-proxy resources          :   2
  Port-forwarding resources    :   1
  Ip-forwarding  resources     :   1
  Total online users           :   15
  ------------------------------------------------------------------
```

Table 12-80 Description of the display sslvpn gateway command output

Item	Description
Gateway name	Virtual gateway name. To configure the virtual gateway name, run the **sslvpn gateway** *gateway-name* command.
Status	Status of the virtual gateway: ● enable ● disable To enable basic functions of a virtual gateway, run the **enable** command.
Intranet interface	Intranet interface of the virtual gateway. To configure an intranet interface of a virtual gateway, run the **intranet interface** *interface-type interface-number* command.
Intranet IP	IP address of the intranet interface.
Domain	AAA domain bound to the virtual gateway. To bind a domain to a virtual gateway, run the **bind domain** *domain-name* command.

Item	Description
Max-user	Maximum number of online remote users allowed by the virtual gateway. To set the maximum number of online remote users allowed by a virtual gateway, run the **max-user** *number* command. The maximum number of online remote users is limited by the maximum numbers of online remote users provided by the device. The actual maximum number of online remote users is the smallest value between the maximum numbers configured by the administrator and provided by the device.
Max-onlinetime(minute)	Maximum online duration of a remote user allowed by the virtual gateway. To set the maximum online duration of a remote user allowed by a virtual gateway, run the **max-online-time** *number* command.
Web-proxy resources	Number of web proxy resources.
Port-forwarding resources	Number of port forwarding resources.
Ip-forwarding resources	Number of IP forwarding resources.
Total online users	Total number of online remote users.

12.8.9 display sslvpn gateway access-user

Function

The **display sslvpn gateway access-user** command displays remote access user information on a virtual gateway.

Format

display sslvpn gateway *gateway-name* **access-user** [*user-name*]

Parameters

Parameter	Description	Value
gateway-name	Indicates the virtual gateway name.	The value is the name of an existing virtual gateway.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-name	Displays details about the specified remote user on the virtual gateway.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain a space or question mark (?).

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about online remote users on the virtual gateway, namely, access remote user information, run the **display sslvpn gateway access-user** command.

Example

Display information about all remote access users on a virtual gateway.

```
<Huawei> display sslvpn gateway gate0 access-user
Total access-user number of this gateway: 1
  --------------------------------------------------------------------------------
  User name                        User ID          Auth method
  --------------------------------------------------------------------------------
  admin@domain1                      0                LOCAL
  --------------------------------------------------------------------------------
```

Display information about the remote user **fag**.

```
<Huawei> display sslvpn gateway gate0 access-user fag
  --------------------------------------------------------------------------------
  User name                  :   admin@domain1
  User ID                    :   0
  Auth Method                :   LOCAL
  Max-onlinetime(minute)     :   120
  Current-onlinetime(minute) :   25
  --------------------------------------------------------------------------------
```

Table 12-81 Description of the display sslvpn gateway command output

Item	Description
User name	User name of the remote access user.
User ID	User ID of the remote access user.

Item	Description
Auth Method	Authentication method of the remote access user: ● LOCAL: local authentication ● RADIUS: RADIUS authentication
Max-onlinetime(minute)	Maximum online duration of the remote user. To set the maximum online duration of a remote user allowed by a virtual gateway, run the **max-online-time** *number* command.
Current-onlinetime(minute)	Current online duration of the remote user.

Related Topics

12.8.21 max-user

12.8.10 display sslvpn gateway resource

Function

The **display sslvpn gateway resource** command displays resource information on a virtual gateway.

Format

display sslvpn gateway *gateway-name* **resource class** { **web-proxy** | **port-forwarding** | **ip-forwarding** }

Parameters

Parameter	Description	Value
gateway-name	Displays resource information on a virtual gateway.	The value is the name of an existing virtual gateway.
class web-proxy	Displays resource information of the web proxy service.	-
class port-forwarding	Displays resource information of the port forwarding service.	-
class ip-forwarding	Displays resource information of the IP forwarding service.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view resource information on a virtual gateway, run the **display sslvpn gateway resource** command.

Example

Display web proxy resource information on the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users resource class web-proxy
The total number of resources is : 2
  --------------------------------------------------------------------------------
  Resource name                Url                        Type
  --------------------------------------------------------------------------------
  liyue                      http://192.168.1.65/        web-proxy
  test                       http://192.168.1.65/        web-proxy
  --------------------------------------------------------------------------------
```

Display port forwarding resource information on the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users resource class port-forwarding

The total number of resources is : 1
  --------------------------------------------------------------------------------
  Resource name                Server            Port       Type
  --------------------------------------------------------------------------------
  liyue                      192.168.1.65        3389       port-forwarding
  --------------------------------------------------------------------------------
```

Display IP forwarding resource information on the virtual gateway **users**.

```
<Huawei> display sslvpn gateway users resource class ip-forwarding
  --------------------------------------------------------------------------------
  Resource name        :   liyue
  Pool name            :   liyue
  Route-mode           :   full
  Acl                  :   3001
  Type                 :   ip-forwarding
  --------------------------------------------------------------------------------
```

Table 12-82 Description of the display sslvpn gateway resource command output

Item	Description
The total number of resources	Number of resources on the virtual gateway
Resource name	Resource name. To configure a resource name, run the **service-type** { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name* command.

Item	Description
Url	URLs in the web proxy service. To configure a URL of an internal web server, run the **link** *url* [**web-tunnel**] command.
Type	Resource type: ● web-proxy: web proxy service ● port-forwarding: port forwarding service ● ip-forwarding: IP forwarding service To configure an SSL VPN service, run the **service-type** { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name* command.
Server Port	IP address for the port forwarding service. Port number for the port forwarding service. To configure the IP address and port number for the port forwarding service, run the **server ip-address** *ip-address* **port** *port-number* command.
Pool name	IP address pool name bound to the IP forwarding service. To bind an IP address pool to the IP forwarding service, run the **bind ip-pool** *pool-name* command.
Route-mode	Routing mode used by the IP forwarding service: ● full ● split To configure a routing mode used by the IP forwarding service, run the **route-mode** { **full** | **split** } command.
Acl	ACL number bound to the IP forwarding service. To bind an ACL to the IP forwarding service, run the **bind acl** *acl-number* command.

12.8.11 display sslvpn user statistics

Function

The **display sslvpn user statistics** command displays history statistics on remote users.

Format

display sslvpn user statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view history statistics on remote users.

Example

Display history statistics on remote users.

```
<Huawei> display sslvpn user statistics
  ------------------------------------------------------------------------------
  Maximum of total online users in history      :    0
  Begin time of total online users              :    2013-10-18 20:22:05
  Maximum time of total online users            :    2013-10-18 20:22:05
  ------------------------------------------------------------------------------
```

Table 12-83 Description of the **display sslvpn user statistics** command output

Item	Description
Maximum of total online users in history	Maximum number of total online remote users in the history.
Begin time of total online users	Time when collection of statistics on online remote users begins.
Maximum time of total online users	Time when the total number of online remote users reaches the maximum value.

Related Topics

12.8.23 reset sslvpn user statistics

12.8.12 display sslvpn server port

Function

The **display sslvpn server port** command displays information about the listening port number used by the SSL VPN service.

Format

display sslvpn server port

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about the listening port number used by the SSL VPN service.

```
<Huawei> display sslvpn server port
  sslvpn server port : 443    (default:443)
```

Table 12-84 Description of the display sslvpn server port command output

Item	Description
sslvpn server port	Listening port number used by the SSL VPN service.
default	Default listening port number used by the SSL VPN service.

Related Topics

12.8.30 sslvpn server port

12.8.13 enable

Function

The **enable** command enables the basic SSL VPN functions for a virtual gateway.

The **undo enable** command disables the basic SSL VPN functions for a virtual gateway.

By default, the basic SSL VPN functions are disabled.

Format

enable

undo enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use a device as an SSL VPN gateway, you must configure and enable the basic SSL VPN functions.

Pay attention to the following points when using the basic SSL VPN functions:

- After you configure the basic SSL VPN functions, you must use the **enable** command to make the function effective.
- If you disable the basic SSL VPN functions using the **undo enable** command, all online users are forcibly disconnected from the virtual gateway.

Prerequisites

The configurations of basic SSL VPN functions have been complete on the virtual gateway. The configurations of basic SSL VPN functions include:

- Intranet interfaces
- AAA domain

Example

Enable the basic SSL VPN functions on the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] enable
```

Related Topics

12.8.21 max-user

12.8.14 intranet interface

Function

The **intranet interface** command configures an intranet interface for a virtual gateway.

The **undo intranet interface** command deletes the intranet interface from a virtual gateway.

By default, no intranet interface exists on a virtual gateway.

Format

intranet interface *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

undo intranet interface

Parameters

Parameter	Description	Value
interface-type interface-number	Type and number of the intranet interface.	The *interface-type* value is a Layer 3 interface type; the *interface-number* value depends on the interface type and slot ID.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The intranet hosts or servers connect to the intranet interfaces of the SSL VPN gateway. When configuring a virtual gateway, the administrator needs to set the interface connecting the SSL VPN gateway to the internal server to the intranet interface of the virtual gateway. The interface enables the communication between the virtual gateway and the internal server.

Precautions

The intranet interface must be a Layer 3 interface and have an IP address.

If you need to modify the intranet interface after the basic SSL VPN functions are enabled, use the **undo enable** command to disable the basic SSL VPN functions first.

Example

Configure the intranet interface for the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] intranet interface gigabitethernet 2/0/0
```

Related Topics

12.8.21 max-user

 Copyright © Huawei Technologies Co., Ltd.

12.8.15 link

Function

The **link** command configures a URL of an internal web server and a mode in which the web proxy service is implemented.

The **undo link** command deletes a URL of an internal web server and a mode in which the web proxy service is implemented.

By default, the URL of an internal web server is not configured on a virtual gateway and URL rewriting mode is used.

Format

link *url* [**web-tunnel**]

undo link

Parameters

Parameter	Description	Value
url	Specifies the URL of an internal web server.	The value is a string of 1 to 200 case-sensitive characters. The string cannot contain the following characters: < > [ ]. **NOTE** ● A URL supports the IP address and domain name formats. ● An HTTP port number can also be specified in the URL. If no port number is specified, the URL uses the default port number 80.
web-tunnel	Indicates that users access the internal web server in web-tunnel mode.	-

Views

Web proxy service view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The web proxy service is based on the HTTPS protocol. Users access the internal web server through the SSL VPN gateway. The SSL VPN gateway functions as a proxy that forwards data between users and the internal web server. This function helps ensure that access to the internal web server is secure.

The URL for the internal web server must be specified so that remote users can access the web server.

The web proxy service can be implemented in the following modes:

- URL rewriting: this mode is often used.

  The internal website resource URL displayed by the SSL VPN gateway to remote users is a rewritten URL. After remote users click the website resource URL, the SSL VPN gateway changes the URL to the URL pointing to the SSL VPN gateway. The SSL VPN gateway must rewrite the URL on each page responded by the internal web server to remote users and retain other contents unchanged.
- Web-tunnel: this mode is implemented through port forwarding.

  After a remote user logs in to the SSL VPN gateway, the Java plug-in is automatically installed on the remote terminal, and the internal website resource URL displayed to the remote user is the actual intranet URL. After the user clicks the URL, the Java plug-in automatically adds a header containing a destination address (address of the SSL VPN gateway) to the packet, and sends the packet to the SSL VPN gateway using HTTP request. The SSL VPN gateway converts the packet to the original HTTP request and sends it to the internal web server.

Precautions

Only one URL can be configured for a web proxy service. If there are multiple internal web servers, multiple web proxy services can be configured.

If you run the **link** command multiple times in the same web proxy service view, only the latest configuration takes effect.

Example

Configure a URL for an internal web server.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type web-proxy resource wpres1
[Huawei-sslvpn-users-wp-res-wpres1] link http://10.0.0.1/
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.16 login-help

Function

The **login-help** command configures the help information on the bottom of the virtual gateway web GUI.

The **undo login-help** command restores the default setting.

The default help information on the bottom of the virtual gateway web GUI is **Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.**

Format

login-help *help-info*

undo login-help

Parameters

Parameter	Description	Value
help-info	Help information on the bottom of the virtual gateway web GUI.	The value is a string of 1 to 200 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The Unicode can be used to represent Chinese characters or special characters.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

An enterprise may want to display the enterprise address and phone number to customers. To meet this requirement, the administrator can display the information as the help information on the bottom of the virtual gateway web GUI.

Precautions

If you run the **login-help** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the help information on the bottom of the virtual gateway web GUI to **Tel:123456**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-help Tel:123456
```

Related Topics

12.8.21 max-user

12.8.17 login-message

Function

The **login-message** command configures the greeting on the virtual gateway web GUI.

The **undo login-message** command restores the default setting.

The default greeting on the virtual gateway web GUI is **Welcome to login:**.

Format

login-message *welcome-info*

undo login-message

Parameters

Parameter	Description	Value
welcome-info	Greeting on the virtual gateway web GUI.	The value is a string of 1 to 128 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The Unicode can be used to represent Chinese characters or special characters.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

An enterprise may require the virtual gateway web GUI to display specified greetings for specified customers or holidays. Run the **login-message** command to configure the greeting on the virtual gateway web GUI.

Precautions

If you run the **login-message** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the greeting on the virtual gateway web GUI to **Welcome**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-message Welcome
```

Set the greeting on the virtual gateway web GUI to **Welcome**. (Unicode indicates Chinese Characters.)

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-message %u6B22%u8FCE%u8BBF%u95EE%u672C%u516C%u53F8
```

Related Topics

12.8.21 max-user

12.8.18 login-photo

Function

The **login-photo** command configures the background picture in the login dialog box of the virtual gateway web GUI.

The **undo login-photo** command deletes the configured background picture from the login dialog box of the virtual gateway web GUI.

By default, the background picture in the login dialog box of the virtual gateway web GUI is light gray.

Format

login-photo *login-photo-file*

undo login-photo

Parameters

Parameter	Description	Value
login-photo-file	Background picture in the login dialog box of the virtual gateway web GUI. **NOTE** The background picture must be a GIF file of a maximum of 6 KB.	The value is a string of 1 to 64 characters in the format of *[path] [file-name]*.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **login-photo** command to change the background picture in the login dialog box of the virtual gateway web GUI.

Precautions

- The recommended picture pixels are 35 x 35.
- If you run the **login-photo** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the background picture in the login dialog box of the virtual gateway web GUI to **Login.gif**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] login-photo flash:/Login.gif
```

Related Topics

12.8.21 max-user

12.8.19 logo

Function

The **logo** command configures the enterprise logo on the enterprise gateway web GUI.

The **undo logo** command deletes the configured enterprise logo from the enterprise gateway web GUI.

Format

logo *logo-file*

undo logo

Parameters

Parameter	Description	Value
logo-file	File name of the enterprise logo on the enterprise gateway web GUI.	The value is a string of 1 to 64 characters in the format of *[path] [file-name]*. **NOTE** The enterprise logo must be a GIF file of a maximum of 6 KB.

 Copyright © Huawei Technologies Co., Ltd.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Generally, enterprises have their own logos. If an enterprise requires the virtual gateway web GUI to display the enterprise logo, run the **logo** command to configure the enterprise logo on the enterprise gateway web GUI.

Precautions

- The recommended picture pixels are 50 x 50.
- If you run the **logo** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the enterprise logo on the enterprise gateway web GUI to **iHappy.gif**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] logo flash:/iHappy.gif
```

Related Topics

12.8.21 max-user

12.8.20 max-online-time

Function

The **max-online-time** command configures the maximum online duration of a remote user allowed by the virtual gateway.

The **undo max-online-time** command restores the default duration.

By default, the maximum online duration of remote users allowed by a virtual gateway is 120 minutes.

Format

max-online-time *number*

undo max-online-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Maximum online duration of a remote user allowed by the virtual gateway.	The value is an integer ranging from 5 to 480, in minutes.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an online remote user does not use services for a long time, the remote user still occupies resources. To avoid a waste of resources, configure the maximum online duration for remote users. A remote user whose online duration exceeds the limit is logged off forcibly. The virtual gateway still stores information about the disconnected remote users.

Follow-up Procedure

Run the **display sslvpn gateway access-user** command to view the maximum online duration of remote users.

Example

Configure the maximum online duration of a remote user allowed by the virtual gateway.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] max-online-time 200
```

Related Topics

12.8.21 max-user

12.8.9 display sslvpn gateway access-user

12.8.21 max-user

Function

The **max-user** command configures the maximum number of online users allowed by the virtual gateway.

The **undo max-user** command restores the default value.

By default, the maximum number of online users allowed by the virtual gateway is:

- AR120&AR150&AR160&AR200 series: 10
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 50
- AR2220, AR2220E, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 100
- AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100E, SRU200, SRU200E, SRU400), AR3200 (using SRU80, SRU100E, SRU200, SRU200E, SRU400), AR3600 (using SRU5X) series: 200

The maximum number of online remote users is limited by the maximum numbers of online remote users provided by the device. The actual maximum number of online remote users is the smallest value between the maximum numbers configured by the administrator and provided by the device.

Format

max-user *number*

undo max-user

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Maximum number of online users allowed by the virtual gateway.	The value is an integer and the value range depends on device types. ● AR100&AR120&AR150&AR160&AR200 series: 0 to 10 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 0 to 50 ● AR2220, AR2220E, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 0 to 100 ● AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100E, SRU200, SRU200E, or SRU400), AR3200 (using SRU80, SRU100E, SRU200, SRU200E, or SRU400), AR3600 (using SRU5X) series: 0 to 200

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **max-user** command limits the number of online remote users. When the number of online remote users on the virtual gateway exceeds the limit, no more remote user can log in.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

When you configure the maximum number of online remote users for multiple virtual gateways, the sum of the maximum numbers cannot exceed the maximum number supported by the device.

Example

Set the maximum number of online users on the virtual gateway **users** to 10.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] max-user 10
```

Related Topics

12.8.21 max-user

12.8.22 organization

Function

The **organization** command configures the enterprise name on the enterprise gateway web GUI.

The **undo organization** command restores the default setting.

The default enterprise name on the virtual gateway web GUI is **SSL VPN**.

Format

organization *organization-name*

undo organization

Parameters

Parameter	Description	Value
organization-name	Enterprise name on the enterprise gateway web GUI.	The value is a string of 1 to 200 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The Unicode can be used to represent Chinese characters or special characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Generally, enterprises have their own names. If an enterprise requires the virtual gateway web GUI to display the enterprise name, run the **organization** command to configure the enterprise name on the enterprise gateway web GUI.

Precautions

If you run the **organization** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the enterprise name on the enterprise gateway web GUI to **iHappy**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] organization iHappy
```

Related Topics

12.8.21 max-user

12.8.23 reset sslvpn user statistics

Function

The **reset sslvpn user statistics** command clears history statistics on remote users.

Format

reset sslvpn user statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run this command to clear history statistics on remote users.

NOTICE

Statistics cannot be restored after being cleared. Therefore, confirm the action before you run the command.

Example

Clear history statistics on remote users.

```
<Huawei> reset sslvpn user statistics
```

Related Topics

12.8.11 display sslvpn user statistics

12.8.24 route-mode

Function

The **route-mode** command configures a routing mode for the IP forwarding service.

The **undo route-mode** command restores the default routing mode.

By default, the routing mode is full.

Format

route-mode { **full** | **split** }

undo route-mode

Parameters

Parameter	Description	Value
full	Sets the routing mode to full.	-
split	Sets the routing mode to split.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

IP forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSL VPN gateway allows remote terminals to communicate with internal servers at the network layer. For example, remote terminals and internal servers implement file sharing.

The IP forwarding service can be implemented in the following modes:

- Full routing mode

  The SSL VPN gateway adds a default route with the next hop address as the virtual network adapter's IP address (intranet IP address allocated to the virtual network adapter by the SSL VPN gateway) to the routing table of a remote terminal. The remote terminal can communicate with servers on the specified network segment through the SSL VPN gateway.
- Split routing mode

  The SSL VPN gateway adds the route in split mode to the routing table of a remote terminal. The remote terminal can communicate with only servers on the specified internal network segment. This mode controls internal servers that remote terminals can communicate in a fine-grained manner.

Precaution

If you run the **route-mode** command multiple times in the same IP forwarding service view, only the latest configuration takes effect.

Follow-up Procedure

If you choose the Split mode, you must use the **route-split** command to specify the network segment that users can access.

Example

Set the routing mode to Split.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] route-mode split
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.25 route-split

12.8.25 route-split

Function

The **route-split** command specifies the accessible network segment for remote users when the split routing mode is used.

The **undo route-split** command cancels the configuration.

By default, no accessible network segment is specified.

Format

route-split ip address *ip-address* **mask** { *mask-length* | *mask* }

undo route-split ip address *ip-address* **mask** { *mask-length* | *mask* }

Parameters

Parameter	Description	Value
ip address *ip-address*	Specifies the destination IP address of the route to the internal network segment. This is a private IP address.	The value is in dotted decimal notation.
mask *mask-length*	Specifies the mask length of the route to the internal network segment.	The value is an integer ranging from 1 to 32.
mask *mask*	Specifies the mask of the route to the internal network segment.	The value is in dotted decimal notation.

Views

IP forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The SSL VPN gateway allows remote terminals to communicate with internal servers at the network layer. For example, remote terminals and internal servers implement file sharing.

The IP forwarding service can be implemented in full routing mode and split routing mode. In split routing mode, the SSL VPN gateway adds the route in split

 Copyright © Huawei Technologies Co., Ltd.

mode to the routing table of a remote terminal. The remote terminal can communicate with only servers on the specified internal network segment. This mode controls internal servers that remote terminals can communicate in a fine-grained manner.

The **route-split** command limits the network segment that users can access by specifying the route destination IP address and mask.

Prerequisites

The **route-mode** command has been executed to set the routing mode to Split.

Precautions

A maximum of 10 user routes in Split routing mode can be configured in the same IP forwarding service view.

Example

Specify the network segment that users can access.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type ip-forwarding resource ifres1
[Huawei-sslvpn-users-if-res-ifres1] route-mode split
[Huawei-sslvpn-users-if-res-ifres1] route-split ip address 1.1.1.0 mask 24
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.24 route-mode

12.8.26 server ip-address

Function

The **server ip-address** command configures the IP address and port number for the port forwarding service.

The **undo server ip-address** command deletes the IP address and port number for the port forwarding service.

By default, no IP address or port number is configured for the port forwarding service.

Format

server ip-address *ip-address* **port** *port-number*

undo server ip-address

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	IP address for the port forwarding service.	The value is in dotted decimal notation.
port *port-number*	Port number for the port forwarding service.	The value is an integer ranging from 1 to 65535.

Views

Port forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The port forwarding function allows applications to access internal servers using TCP. Remote users can access the TCP-based services on the internal network. The typical port forwarding services include Telnet login, desktop sharing, and mailing. The IP address and port number of the internal application server must be specified so that remote users can access the application server.

Precautions

The IP address and port number specified in a command must match.

If you run the **server ip-address** command with different IP addresses and port numbers multiple times in the same port forwarding service view, only the latest configuration takes effect.

Example

Specify the IP address and port number for the port forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type port-forwarding resource wpres1
[Huawei-sslvpn-users-pf-res-wpres1] server ip-address 1.1.1.1 port 23
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.27 server name

 Copyright © Huawei Technologies Co., Ltd.

12.8.27 server name

Function

The **server name** command configures the domain name and port number for the port forwarding service.

The **undo server name** command deletes the domain name and port number for the port forwarding service.

By default, the domain name and port number are not configured for the port forwarding service.

Format

server name *name* **port** *port-number*

undo server name

Parameters

Parameter	Description	Value
name	Specifies the domain name for the port forwarding service.	The value is a string of 1 to 200 case-sensitive characters without spaces or the following characters: < > [ ]. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
port *port-number*	Specifies the port number for the port forwarding service.	The value is an integer ranging from 1 to 65535.

Views

Port forwarding service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The port forwarding function allows applications to access internal servers using TCP. Users can access the TCP-based services on the internal network. The typical port forwarding services include Telnet login, desktop sharing, and mailing.

 Copyright © Huawei Technologies Co., Ltd.

Compared with an IP address, the domain name is easy to remember. When configuring the port forwarding service, the administrator can specify the domain name and port number of the internal server that can be accessed.

Prerequisites

The SSL VPN gateway has been configured as the DNS client.

Precautions

When you run this command to configure the domain name and port number for the port forwarding service, the domain name and port number must correspond to each other.

If you run the **server name** command with different values of the *name* or *port-number* parameter multiple times in the same port forwarding service view, only the latest configuration takes effect.

Example

Configure the domain name and port number for the port forwarding service.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type port-forwarding resource wpres1
[Huawei-sslvpn-users-pf-res-wpres1] server name www.iHappy.com.cn port 23
```

Related Topics

12.8.21 max-user

12.8.28 service-type resource

12.8.26 server ip-address

12.8.28 service-type resource

Function

The **service-type resource** command creates a service on the virtual gateway and enters the service view or enters an existing service view.

The **undo service-type resource** command deletes a service from the virtual gateway.

By default, no service exists on a virtual gateway.

Format

service-type { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name*

undo service-type { **web-proxy** | **port-forwarding** | **ip-forwarding** } **resource** *resource-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
web-proxy	Indicates a web proxy service.	-
port-forwarding	Indicates a port forwarding service.	-
ip-forwarding	Indicates an IP forwarding service.	-
resource-name	Indicates the service name.	The value is a string of 1 to 31 case-sensitive characters without spaces When double quotation marks are used around the string, spaces are allowed in the string.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

The device supports three service types as an SSL VPN gateway: web proxy, port forwarding, and IP forwarding.

The services on the SSL VPN gateway are created and configured in the virtual gateway view.

Example

Create the web proxy service **wpres1** and enter its view.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] service-type web-proxy resource wpres1
[Huawei-sslvpn-users-wp-res-wpres1]
```

Related Topics

12.8.21 max-user

12.8.29 sslvpn gateway

Function

The **sslvpn gateway** command creates a virtual gateway and enters its view or enters an existing virtual gateway view.

The **undo sslvpn gateway** command deletes a virtual gateway.

By default, no virtual gateway exists.

Format

sslvpn gateway *gateway-name*

undo sslvpn gateway *gateway-name*

Parameters

Parameter	Description	Value
gateway-name	Indicates the virtual gateway name.	The value is a string of 1 to 31 case-sensitive characters without spaces. The string cannot contain the following characters: ? < > [ ].

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Based on the HTTPS protocol, SSL VPN uses the data encryption, user identify authentication, and message integrity check mechanisms of the SSL protocol to ensure secure remote access to enterprises' intranets.

An SSL VPN gateway can function as multiple virtual gateways, and the administrator manage users and configures services for each virtual gateway. To deploy the SSL VPN function on a device, the administrator creates multiple virtual gateways on the device, and configures the basic SSL VPN functions, SSL VPN services, and personalized web GUI and manage SSL VPN users on each virtual gateway.

Precautions

The numbers of virtual gateways that can be created on devices are as follows:

 Copyright © Huawei Technologies Co., Ltd.

- AR100&AR120&AR150&AR160&AR200 series: 1
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204: 2
- AR2220, AR2220E, AR2240 (using SRU40 or SRU60), AR3200 (using SRU40 or SRU60) series: 4
- AR2204XE, AR2204XE-DC, AR2240 (using SRU80, SRU100, SRU100E, SRU200, or SRU200E, or SRU400), AR3200 (using SRU80, SRU100, SRU100E, SRU200, or SRU200E, or SRU400) series, AR3600 (using SRUX5): 8

Example

Create the virtual gateway **users**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users]
```

Related Topics

12.8.28 service-type resource

12.8.30 sslvpn server port

Function

The **sslvpn server port** command configures the listening port number of the SSL VPN service.

The **undo sslvpn server port** command restores the default setting.

The default listening port number of the SSL VPN service is 443.

Format

sslvpn server port *port*

undo sslvpn server port

Parameters

Parameter	Description	Value
port	Listening port number of the SSL VPN service.	The value is an integer that can be 443 or range from 1025 to 51200.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default listening port number of the SSL VPN service is 443. When port 443 is used by another service, such as web-based network management service, run the **sslvpn server port** command to configure another listening port number for the SSL VPN service.

Precautions

- Before configuring the listening port number of the SSL VPN service, the administrator must ensure that all virtual gateways on the SSL VPN gateway are disabled. To disable a virtual gateway, run the **undo enable** command in the virtual gateway view.
- After the administrator changes the listening port number, users must enter the URL containing the new port number to log in to the SSL VPN gateway.

  For example, the URL of the SSL VPN gateway is https://1.1.1.1/gateway1. When the listening port number is changed to 1025, remote users must enter the URL https://1.1.1.1:1025/gateway1.

Example

Set the listening port number of the SSL VPN service to 1025.

```
<Huawei> system-view
[Huawei] sslvpn server port 1025
```

12.8.31 table-color

Function

The **table-color** command configures the table header color of the virtual gateway web GUI.

The **undo table-color** command restores the default setting.

The RGB color model of the default table header color on the virtual gateway web GUI is **#CDCDCD**.

Format

table-color *color-value*

undo table-color

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
color-value	Table header color of the virtual gateway web GUI.	The RGB color model is used. The value format is #*H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **table-color** command to configure the table header color on the virtual gateway web GUI.

Precautions

If you run the **table-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

Example

Set the RGB color model of the table header color of the virtual gateway web GUI to **#00EEFF**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] table-color #00EEFF
```

Related Topics

12.8.21 max-user

12.8.32 text-color

Function

The **text-color** command configures the text color of the virtual gateway web GUI.

The **undo text-color** command restores the default setting.

The RGB color model of the default text color on the virtual gateway web GUI is **#333333**.

Format

text-color *color-value*

undo text-color

Parameters

Parameter	Description	Value
color-value	Text color of the virtual gateway web GUI.	The RGB color model is used. The value format is #*H*, in which *H* is a 3-digit or 6-digit hexadecimal number. Each digit ranges from 0 to F.

Views

Virtual gateway view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device supports personalized GUI elements. Enterprise users can customize elements on the web GUI of a virtual gateway to meet diversified enterprise requirements.

Run the **text-color** command to configure the text color on the virtual gateway web GUI.

Precautions

If you run the **text-color** command multiple times in the same virtual gateway view, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the RGB color model of the text color of the virtual gateway web GUI to **#00EEFF**.

```
<Huawei> system-view
[Huawei] sslvpn gateway users
[Huawei-sslvpn-users] text-color #00EEFF
```

Related Topics

12.8.21 max-user

12.9 BGP/MPLS IP VPN Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not supports BGP/MPLS IP VPN, only supports MCE.

12.9.1 apply tunnel-policy (tunnel-selector view)

Function

The **apply tunnel-policy** command applies a tunnel policy to routes filtered by the **if-match** clause.

The **undo apply tunnel-policy** command cancels the setting.

By default, no tunnel policy is configured for filtered routes.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

apply tunnel-policy *tunnel-policy-name*

undo apply tunnel-policy

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of a tunnel policy to be applied to the routes that match the **if-match** clause.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel selector view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, by default, LSPs are selected for VPNv4 and BGP labeled routes without performing load balancing. If you want to select other types of tunnels or configure load balancing for VPNv4 or BGP labeled routes, run the **apply tunnel-policy** command to apply a tunnel policy. The **apply tunnel-policy** command can be used in the following situations:

- The ASBR in VPN Option B networking needs to apply a tunnel policy to VPNv4 routes learned from PEs.
- The RR on the backbone network of a VPN needs to apply a tunnel policy to VPNv4 routes learned from PEs.
- The PE in VPN Option C networking needs to apply a tunnel policy to received BGP labeled routes.

If you want to apply a tunnel policy to only specific VPNv4 or BGP labeled routes in the situations mentioned above, first use the **if-match** clause to filter routes. The **if-match** commands that can be used are listed below:

- **if-match ip next-hop (tunnel-selector view)**

  The command filters IPv4 routes by next hop.
- **if-match rd-filter**

  The command filters routes by RD.

Prerequisite

The **tunnel-selector** command is run to create a tunnel selector; **if-match** clauses are configured as needed.

Follow-up Procedure

If the tunnel policy specified in the **apply tunnel-policy** command does not exist in the system, run the **tunnel-policy** command to create the tunnel policy.

Example

Select policy1 for the VPN routes that are filtered by RD in the tunnel selector view.

```
<Huawei> system-view
[Huawei] tunnel-policy policy1
[Huawei-tunnel-policy-policy1] tunnel select-seq cr-lsp lsp load-balance-number 1
[Huawei-tunnel-policy-policy1] quit
[Huawei] tunnel-selector tps permit node 10
[Huawei-tunnel-selector] if-match rd-filter 1
[Huawei-tunnel-selector] apply tunnel-policy policy1
```

Related Topics

12.9.63 tunnel-policy (system view)

12.9.2 apply-label per-instance

Function

The **apply-label per-instance** command sets the label allocation mode to one label per instance. In this mode, all the routes of the VPN instance address family destined for the remote PE are assigned the same label.

The **undo apply-label per-instance** command restores the default configuration.

By default, the label allocation mode is one label per route, that is, each route of the VPN instance address family destined for the remote PE is assigned a label.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

apply-label per-instance

undo apply-label per-instance

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, if VPN routes on PE are numerous but MPLS label resources are insufficient, the **apply-label per-instance** command can be run to minimize MPLS label consumption on PE.

By default, each route of the VPN instance IPv4 or IPv6 address family is assigned a specified label. To change the label allocation mode to one label per instance, run the **apply-label per-instance** command. For example, a PE is configured with two VPN instances that have 20000 routes in total. By default, the PE will allocate 20000 MPLS labels to the routes. After the **apply-label per-instance** command is configured for the two VPN instances, the PE will allocate only two labels for the two VPN instances.

When a large number of routes of the VPN instance IPv4 or IPv6 address family need to apply for labels, the **apply-label per-instance** command saves label resources of PEs and lowers the requirements for PE capacities.

 Copyright © Huawei Technologies Co., Ltd.

You can run the **display fib statistics** command to check the number of VPN routes.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to enter the IPv4 or IPv6 VPN instance address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The change of the label allocation mode leads to the re-advertising of VPN routes. The services may be interrupted temporarily. Therefore, use the **apply-label per-instance** and **undo apply-label per-instance** commands with caution.

Example

Assign one label to all routes of the IPv4 address family of the VPN instance named vpn1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn1-af-ipv4] apply-label per-instance
```

Related Topics

12.9.35 ip vpn-instance

12.9.14 display ip vpn-instance

12.9.36 ipv4-family (VPN instance view)

12.9.50 route-distinguisher

12.9.3 apply-label per-nexthop

Function

The **apply-label per-nexthop** command enables the ASBR to allocate labels for IPv4 VPN routes based on the next hop.

The **undo apply-label per-nexthop** command disables the ASBR from allocating labels for IPv4 VPN routes based on the next hop.

By default, next-hop-based label allocation for VPN routes is disabled on the ASBR, and a label is allocated to each VPNv4 or VPNv6 route.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

apply-label per-nexthop

undo apply-label per-nexthop

Parameters

None

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In inter-AS VPN Option B or HoVPN networking, if MPLS label resources on the ASBR or SPE are insufficient for the advertised VPNv4 routes to use, the **apply-label per-nexthop** command can be run to minimize MPLS label consumption on the ASBR or SPE.

By default, the ASBR or SPE allocates a label to each VPNv4 route when advertising it to an MP-BGP peer. If the **apply-label per-nexthop** command is run, the ASBR or SPE will allocate one label to all the routes with the same next hop and outgoing label. To make the routes learned from the same next hop have the same outgoing label, run the **apply-label per-instance** command on the PE. Otherwise, the effect of the **apply-label per-nexthop** command will be affected.

You can run the **display fib statistics** command to check the number of VPN routes.

Configuration Impact

After next-hop-based label allocation is enabled or disabled, the label allocated by the ASBR or SPE to a route changes, which leads to a transient loss of VPN packets.

Example

In the BGP-VPNv4 view, enable the ASBR to allocate labels to IPv4 VPN routes based on the next hop.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] apply-label per-nexthop
```

Related Topics

12.9.2 apply-label per-instance

 Copyright © Huawei Technologies Co., Ltd.

12.9.4 apply-label per-route

Function

The **apply-label per-route** command enables the one-label-per-route mode. The VPN instance address family assigns a unique label to each route to be sent to the peer PE.

The **undo apply-label per-route** command disables the one-label-per-route mode.

By default, the label allocation mode is one label per route, that is, each route of the VPN instance address family destined for the remote PE is assigned a label.

Format

apply-label per-route

undo apply-label per-route

Parameters

None

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only a small number of VPN routes exists on the PE and MPLS label resources are sufficient, you can run the **apply-label per-route** command to improve system security. In this way, downstream devices can load balance VPN traffic based on the inner labels of packets.

Prerequisite

The **route-distinguisher** command is run to configure an RD for the VPN instance enabled with the IPv4 or IPv6 address family.

Configuration Impact

The change of the label allocation mode leads to the re-advertising of VPN routes. The services may be interrupted temporarily. Exercise caution when running the **apply-label per-route** or **undo apply-label per-route** command.

The **apply-label per-instance** and **apply-label per-route** commands are mutually exclusive. If both commands are run, the latest configuration overrides the previous one.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the one-label-per-route mode for routes of **vpn1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn1-af-ipv4] apply-label per-route
```

Related Topics

12.9.36 ipv4-family (VPN instance view)

12.9.37 ipv6-family (VPN instance view)

12.9.50 route-distinguisher

12.9.5 apply lsp vpn

Function

The **apply lsp vpn** command enables a specified LSP to forward VPN packets that meet the PBR filtering conditions.

The **undo apply lsp vpn** command disables a specified LSP from forwarding VPN packets that meet the PBR filtering conditions.

By default, the PBR is not used for forwarding VPN packets.

Format

apply lsp vpn *vpn-instance-name ce-address* [*pe-address* [*p-address* | *interface-type* | **secondary**]]

undo apply lsp vpn *vpn-instance-name ce-address*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance name.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ce-address	Specifies the IP address of the destination CE.	The address is in dotted decimal notation.
pe-address	Specifies the IP address of the peer PE that resides on the LSP.	The address is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
p-address	Specifies the IP address of the P. *p-address* and *pe-address* together specify the next P through which the LSP passes.	The address is in dotted decimal notation.
interface-type interface-number	Specifies, together with *pe-address*, the next outbound interface of an LSP.	-
secondary	Indicates the backup LSP generated through LDP fast reroute (FRR). When **secondary** is not configured, only the primary LSP forwards packets. When **secondary** is configured, only the backup LSP forwards packets.	-

Views

Policy-Based-Route view

Default Level

2: Configuration level

Usage Guidelines

After configuring a PBR to the PE address and the P address, if there is no reachable LSP to them, the PBR is ineffective.

Example

Configure the LSP destined for the CE with IP address 20.1.1.1 to forward the VPN packets that match ACL 3000.

```
<Huawei> system-view
[Huawei] policy-based-route map1 permit node 10
[Huawei-policy-based-route-map1-10] if-match acl 3000
[Huawei-policy-based-route-map1-10] apply lsp vpn vpn1 20.1.1.1
```

12.9.6 as-number

Function

The **as-number** command configures an AS number for a VPN instance.

The **undo as-number** command restores the default setting.

By default, a VPN instance uses the AS number of BGP.

Format

as-number { *as-number-plain* | *as-number-dot* }

undo as-number

Parameters

Parameter	Description	Value
as-number-plain	Integral AS number	The value is an integer ranging from 1 to 4294967295.
as-number-dot	AS number in dotted notation	The value is in the format of *x.y*, where *x* and *y* are integers that range from 1 to 65535 and from 0 to 65535, respectively.

Views

BGP-VPN instance IPv4 address family view, BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During network transfer or service identification, a device needs to be simulated as multiple BGP devices logically. In this case, you can run the **as-number** command to configure an AS number for each VPN instance.

After the **as-number** command is used:

- BGP peer relationships in the VPN instance are established by using the configured AS number.
- The configured AS number is used to generate the aggregator attribute during route aggregation.
- When advertising routes to an EBGP peer, the local device carries the AS number configured in the VPN instance.

Prerequisites

If a BGP peer or a BGP peer group is configured in the VPN instance, you need to delete the configuration of the BGP peer or peer group before configuring or deleting an AS number.

Precautions

A VPN instance configured with an AS number cannot be configured with BGP confederation. Conversely, a VPN instance configured with BGP confederation cannot be configured with an AS number.

NOTE

The AS number configured in the BGP-VPN instance view cannot be the same as the AS number configured in the BGP view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the AS number of the VPN instance named **vpna** to 65001.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpn-instance vpna
[Huawei-bgp-vpna] as-number 65001
```

12.9.7 description (VPN instance view)

Function

The **description** command specifies the description of the current VPN instance.

The **undo description** command deletes the description of the current VPN instance.

By default, no description is specified for a VPN instance.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of a VPN instance.	The value is a string of 1 to 242 case-sensitive characters with spaces.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To record the purpose of creating a VPN instance and the CEs with which the VPN instance is associated, you can run the **description** command to specify the description of the VPN instance.

To check the description of a VPN instance, run the **display ip vpn-instance** command.

Precautions

If you run the **description** command several times, the latest configuration overrides the previous configurations.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify the description of a VPN instance named vpn1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] description OnlyForAB
```

Related Topics

12.9.14 display ip vpn-instance

12.9.8 description (tunnel interface view)

Function

The **description** command sets the description of the current tunnel interface.

The **undo description** command deletes the description of the current tunnel interface.

By default, the description of a tunnel interface is "HUAWEI, AR Series, Tunnel *interface-number* Interface".

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of a tunnel interface.	The value is a string of 1 to 242 case-sensitive characters, with spaces supported.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

After using the **interface tunnel** command to create a tunnel interface, you can run the **description** command to configure a description of the tunnel interface to facilitate later query.

To check the description of a tunnel interface, run the **display this interface** command in the tunnel interface view or the **display interface tunnel** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the description of Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] description This is a tunnel from 10.1.1.1 to 10.2.2.2
```

Delete the description of Tunnel 0/0/1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] undo description
```

Related Topics

12.9.32 interface tunnel

12.9.16 display interface tunnel

12.9.9 description (tunnel-policy view)

Function

The **description** command configures the description of the current tunnel policy.

The **undo description** command cancels the setting.

By default, a tunnel policy does not have a description.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

description *description-information*

undo description

Parameters

Parameter	Description	Value
description-information	Specifies the description of the tunnel policy.	The value is a string of 1 to 80 case-sensitive characters with spaces.

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

After using the **12.9.63 tunnel-policy (system view)** command to create a tunnel policy, you can run the **description** command to configure a description of the tunnel policy to facilitate later query.

Example

Configure the description of the tunnel policy named test1.

```
<Huawei> system-view
[Huawei] tunnel-policy test1
[Huawei-tunnel-policy-test1] description two TE tunnels are used
```

12.9.10 destination

Function

The **destination** command specifies the destination IP address of a tunnel interface.

The **undo destination** command deletes the destination IP address of a tunnel interface.

By default, no destination address is configured.

Format

destination [**vpn-instance** *vpn-instance-name*] *dest-ip-address*

undo destination

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the destination address of a tunnel belongs to. When the tunnel interface uses GRE tunnel or IPSec tunnel, you can specify **vpn-instance** *vpn-instance-name*.	The value is the name of an existing VPN instance.
dest-ip-address	Specifies the destination IP address of a tunnel interface.	The value is in dotted decimal notation.

Views

Tunnel interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When configuring a GRE, IPv4 over IPv6, IPSec, MPLS TE, manual IPv6 over IPv4 tunnel, create a tunnel interface. After a tunnel interface is created, run the **destination** command to specify the destination IP address for the tunnel interface.

When using the **destination** command on a PE to specify the destination address of a GRE tunnel bound for a CE, you need to set **vpn-instance** *vpn-instance-name* in the command to specify the name of the VPN instance to which the destination address belongs.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, MPLS TE, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. Normally, two tunnel interfaces in a system cannot have the same encapsulation mode, source address, and destination address.

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

On the IPSec, IPv6 over IPv4, IPv4 over IPv6, or GRE tunnel, the destination address of the local tunnel interface is the source address of the remote tunnel interface by the **source** command, and the source address of the local tunnel interface is the destination address of the remote tunnel interface.

Example

Set the destination address of the GRE tunnel Tunnel 0/0/1 to 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol gre
[Huawei-Tunnel0/0/1] destination 10.1.1.1
```

Set the destination address of the GRE tunnel Tunnel 0/0/0 to 10.1.1.1 that belongs to vpn1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/0
[Huawei-Tunnel0/0/0] tunnel-protocol gre
[Huawei-Tunnel0/0/0] destination vpn-instance vpn1 10.1.1.1
```

Related Topics

12.9.32 interface tunnel

12.9.55 source

12.9.64 tunnel-protocol

12.9.11 display default-parameter l3vpn

Function

The **display default-parameter l3vpn** command displays the default configuration of L3VPN during initialization.

Format

display default-parameter l3vpn

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Scenario

You can run this command to check the default configuration of L3VPN during initialization, for example, default label allocation mode in a VPN instance.

Precautions

This command displays only the default configuration of L3VPN during initialization. The command output shows the default configuration of L3VPN during initialization even when the default configuration is changed.

Example

Display the default configuration of L3VPN during initialization.

```
<Huawei> display default-parameter l3vpn
 Apply label mode          :
    IPv4-family          : label per route
    IPv6-family          : label per route
```

Table 12-85 Description of the display default-parameter l3vpn command output

Item	Description
Apply label mode	Default label allocation mode.
IPv4-family	IPv4 address family.
IPv6-family	IPv6 address family.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
label per route	The default label allocation mode is label per route.

12.9.12 display ip prefix-limit statistics

Function

The **display ip prefix-limit statistics** command displays the statistics of the prefix limits of VPN instances.

Format

display ip prefix-limit { **all-vpn-instance** | **vpn-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ip prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified VPN instance.

Example

Display the statistics of the prefix limits of all VPN instances.

```
<Huawei> display ip prefix-limit all-vpn-instance statistics
-------------------------------------------------------------------------------
VPN instance name: vrf1
        DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0              0             0
STATIC        0              0           0              0             0
UNR           0              0           0              0             0
```

```
OSPF          11            3          1            0            5
IS-IS        106            0          1            0            5
RIP           98            0          1            1            5
BGP            2            0          1            1            5
MSR            0            0          0            0            0
------------------------------------------------------------------------------
VPN instance name: VPN1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT         0            0          0            0            0
STATIC         0            0          0            0            0
UNR            0            0          0            0            0
OSPF          11            3          1            0            5
IS-IS        106            0          1            0            5
RIP           98            0          1            1            5
BGP            2            0          1            1            5
MSR            0            0          0            0            0
```

Display the statistics of the prefix limit of the VPN instance named **vrf1**.

```
<Huawei> display ip prefix-limit vpn-instance vrf1 statistics
------------------------------------------------------------------------------
VPN instance name: vrf1
         DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT         0            0          0            0            0
STATIC         0            0          0            0            0
UNR            0            0          0            0            0
OSPF          11            3          1            0            5
IS-IS        106            0          1            0            5
RIP           98            0          1            1            5
BGP            2            0          1            1            5
MSR            0            0          0            0            0
```

Table 12-86 Description of the display ip prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

12.9.13 display ipv6 prefix-limit statistics

Function

The **display ipv6 prefix-limit statistics** command displays the statistics of the prefix limits of IPv6 VPN instances.

Format

display ipv6 prefix-limit { **all-vpn-instance** | **vpn-instance** *vpn-instance-name* } **statistics**

Parameters

Parameter	Description	Value
all-vpn-instance	Indicates all IPv6 VPN instances.	-
vpn-instance *vpn-instance-name*	Specifies the name of an IPv6 VPN instance.	The value is the name of an existing IPv6 VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ipv6 prefix-limit statistics** command to view the number of times that a protocol re-adds or deletes routes according to the prefix limit of a specified IPv6 VPN instance.

Example

Display the statistics of the prefix limits of all IPv6 VPN instances.

```
<Huawei> display ipv6 prefix-limit all-vpn-instance statistics
-------------------------------------------------------------------------------
IPv6 VPN instance name: vrf1
        DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0             0             0
STATIC        0              0           0             0             0
UNR           0              0           0             0             0
OSPFv3       11              3           1             0             5
IS-IS       106              0           1             0             5
RIPng        98              0           1             1             5
BGP           2              0           1             1             5
-------------------------------------------------------------------------------
IPv6 VPN instance name: VPN123
        DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0           0             0             0
STATIC        0              0           0             0             0
UNR           0              0           0             0             0
OSPFv3       11              3           1             0             5
IS-IS       106              0           1             0             5
RIPng        98              0           1             1             5
BGP           2              0           1             1             5
```

Display the statistics of the prefix limit of the IPv6 VPN instance named **vrf1**.

```
<Huawei> display ipv6 prefix-limit vpn-instance vrf1 statistics
-------------------------------------------------------------------------------
```

```
IPv6 VPN instance name: vrf1
        DenyAdd TryAddInDelState NotifyDelAll NotifyDelFinish NotifyAddRoute
DIRECT        0              0          0             0             0
STATIC        0              0          0             0             0
UNR           0              0          0             0             0
OSPFv3       11              3          1             0             5
IS-IS       106              0          1             0             5
RIPng        98              0          1             1             5
BGP           2              0          1             1             5
```

Table 12-87 Description of the display ipv6 prefix-limit statistics command output

Item	Description
DenyAdd	Number of routes that the protocol fails to add to the RIB because of the prefix limit.
TryAddInDelState	Number of routes that the protocol fails to add to the RIB because the RIB is in the process of deleting routes.
NotifyDelAll	Number of times that the RIB notifies the protocol of deleting routes when the prefix limit is decreased.
NotifyDelFinish	Number of times that the protocol notifies the RIB of completion of deleting routes.
NotifyAddRoute	Number of times that the RIB notifies the protocol of re-adding routes.

12.9.14 display ip vpn-instance

Function

The **display ip vpn-instance** command displays configurations of VPN instances.

Format

display ip vpn-instance [**verbose**] [*vpn-instance-name*]

display ip vpn-instance [*vpn-instance-name*] **interface**

display ip vpn-instance [*vpn-instance-name*] **tunnel-info**

Parameters

Parameter	Description	Value
verbose	Displays detailed information about VPN instances.	-
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.

Parameter	Description	Value
interface	Displays information about the interfaces bound to the VPN instance.	-
tunnel-info	Displays information about the LSP associated with the VPN instance.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you want to check the configurations of VPN instances, interfaces bound to them, and LSPs associated with them, run the **display ip vpn-instance** command. Since VPN instances support both IPv4 and IPv6 address families, the **display ip vpn-instance** command displays the information of different address families separately.

If *vpn-instance-name* is not specified, the **display ip vpn-instance** command displays information about all configured VPN instances on the device.

If **interface** is specified, the display ip vpn-instance command displays all interfaces bound to the specified VPN instance.

If **tunnel-info** is specified, the **display ip vpn-instance** command displays information about the LSPs to which the routes of the VPN instance enabled with the IPv4 or IPv6 address family are iterated (in other words, information about the LSPs between PEs). If the tunnels between PEs are not LSPs, the **display ip vpn-instance** command does not display tunnel information.

Precautions

If the VPN instance to be displayed is not created, the system prompts that the VPN instance does not exist.

Example

Display brief information about all VPN instances.

```
<Huawei> display ip vpn-instance
 Total VPN-Instances configured      : 3
 Total IPv4 VPN-Instances configured : 2
 Total IPv6 VPN-Instances configured : 0

  VPN-Instance Name            RD                  Address-family
  vpn1
  vpna                      100:1               IPv4
  vpnb                      100:2               IPv4
```

Table 12-88 Description of the display ip vpn-instance command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name	Name of the VPN instance.
RD	RD of the VPN instance IPv4 address family or IPv6 address family.
Address-family	Address family enabled for the VPN instance. The address family can be: ● Null, if no address family is enabled. ● IPv4, if only the IPv4 address family is enabled. ● IPv6, if only the IPv6 address family is enabled.

Display detailed information about all VPN instances.

```
<Huawei> display ip vpn-instance verbose
 Total VPN-Instances configured      : 1
 Total IPv4 VPN-Instances configured : 1
 Total IPv6 VPN-Instances configured : 1

 VPN-Instance Name and ID : vpna, 6
  Description : vpna-1
  Service ID : 12
  Interfaces : GigabitEthernet1/0/0
 Address family ipv4
  Create date : 2012/12/3 15:36:20
  Up time : 6 days, 04 hours, 41 minutes and 57 seconds
  Route Distinguisher : 100:1
  Export VPN Targets :  1:1
  Import VPN Targets :  1:1
  Label Policy : label per instance
  Per-Instance Label : 1024
  IP FRR Route Policy : 20
  VPN FRR Route Policy : 12
  Import Route Policy : 10
  Export Route Policy : 20
  Tunnel Policy : bindTE

  Maximum Routes Limit : 2000
  Threshold Routes Limit : 80%
  Maximum Prefixes Limit : 1024
  Threshold Prefixes Limit : 50%
  Install Mode : route-unchanged
  Log Interval : 10
```

```
Address family ipv6
 Create date : Create date : 2012/12/3 15:36:40
 Up time : 6 days, 04 hours, 41 minutes and 57 seconds
 Log Interval : 5
```

Table 12-89 Description of the display ip vpn-instance verbose command output

Item	Description
Total VPN-Instances configured	Total number of VPN instances configured on the local end.
Total IPv4 VPN-Instances configured	Total number of locally configured VPN instances for which IPv4 address families are enabled.
Total IPv6 VPN-Instances configured	Total number of locally configured VPN instances for which IPv6 address families are enabled.
VPN-Instance Name and ID	Name and ID of the VPN instance. The ID is assigned by the system, which facilitates indexing.
Description	Description of the VPN instance. This field is displayed in the command output only when the **description (VPN instance view)**command is used.
Service ID	Service ID of the VPN instance. This item is displayed only after the **service-id (VPN instance view)** command is run in the VPN instance view.
Interfaces	Interfaces bound to the VPN instance. This field is displayed only after the **ip binding vpn-instance** command is configured on these interfaces.
Address family ipv4	Information about the IPv4 address family enabled for the VPN instance.
Address family ipv6	Information about the IPv6 address family enabled for the VPN instance.
Create date	Time when the VPN instance is created.
Up time	Period during which the VPN instance maintains in the Up state.
Route Distinguisher	RD of the VPN instance IPv4 address family or IPv6 address family

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Export VPN Targets	Route Target list in the outbound direction. To set the VPN target, run the **vpn-target** command.
Import VPN Targets	Route Target list in the inbound direction. To set the VPN target, run the **vpn-target** command.
Label Policy	Label policy: ● label per instance: indicates that the same label is allocated to routes of a VPN instance. This field is displayed in the command output only when the **apply-label per-instance** command is run in the VPN instance view. ● label per route: indicates that each route of a VPN instance is assigned a label.
Per-Instance Label	Label value used when all VPN routes of the VPN instance address family share one label. This field is displayed only after the **apply-label per-instance** command is run in the VPN instance address family view.
IP FRR Route Policy	IP FRR route policy used for the address family. This item is displayed only after the **ip frr** command is run in the VPN instance IPv4 address family view.
VPN FRR Route Policy	VPN FRR route policy used for the address family. This item is displayed only after the **vpn frr** command is run in the VPN instance IPv4 address family view.
Import Route Policy	Import Route-Policy applied to the VPN instance. This field is displayed only after the **import route-policy** command is run in the VPN instance address family view.
Export Route Policy	Export Route-Policy applied to the VPN instance. This field is displayed only after the **export route-policy** command is run in the VPN instance address family view.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tunnel Policy	Tunnel policy applied to the VPN instance. This field is displayed only after the **tnl-policy** command is run in the VPN instance address family view.
Maximum Routes Limit	Maximum number of routes supported by the current address family. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Threshold Routes Limit	Percentage of the maximum number of routes specified for the current address family. When the maximum number of routes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **routing-table limit** command is run in the VPN instance address family view.
Maximum Prefixes Limit	Maximum number of prefixes supported by the current address family of the VPN instance. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Threshold Prefixes Limit	Percentage of the maximum number of prefixes specified for the current address family of the VPN instance. When the maximum number of prefixes reaches the percentage threshold, an alarm is generated. This field is displayed only after the **prefix limit** command is run in the VPN instance address family view.
Install Mode	Method of processing routes. The **prefix limit** command can be used to specify the route processing method when the threshold is lowered due to the number of route prefixes exceeding the upper threshold. • If **route-unchanged** is configured, routes in the routing information base (RIB) table remain unchanged. • If **route-unchanged** is not configured, all routes in the RIB table are deleted and the routes are re-installed in the RIB table.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Log Interval	Interval for displaying log messages when the number of VPN instance routes exceeds the maximum value. The default interval is 5 seconds. The value can be set by the command **limit-log-interval**.

Display information about the interface bound to the VPN instance named **vrf1**.

```
<Huawei> display ip vpn-instance vrf1 interface
 VPN-Instance Name and ID : vrf1, 6
  Interface Number : 1
  Interface list : GigabitEthernet1/0/0
```

Table 12-90 Description of the display ip vpn-instance interface command output

Item	Description
Interface Number	Number of interfaces bound to the VPN instance
Interface list	List of interfaces bound to the VPN instance

Display information about the LSP associated with the vrf1 VPN instance.

```
<Huawei> display ip vpn-instance vrf1 tunnel-info

 VPN-Instance Name and ID : vrf1, 1
 Address family ipv4
  Nexthop Address              Tunnel ID
  1.1.1.1                    0x3
 Address family ipv6
```

Table 12-91 Description of the display ip vpn-instance tunnel-info command output

Item	Description
Nexthop Address	Indicates the next-hop address of the route learned by the VPN instance from the peer PE.
Tunnel ID	Indicates the ID of the LSP corresponding to the next-hop address of the route learned by the VPN instance from the peer PE.

Related Topics

12.9.35 ip vpn-instance
12.9.7 description (VPN instance view)
12.9.33 ip binding vpn-instance

12.9.50 route-distinguisher
12.9.69 vpn-target
12.9.2 apply-label per-instance
12.9.30 import route-policy
12.9.26 export route-policy
12.9.65 tnl-policy
12.9.51 routing-table limit
12.9.48 prefix limit
12.9.38 limit-log-interval

12.9.15 display ip vpn-instance import-vt

Function

The **display ip vpn-instance import-vt** command displays all VPN instances with the specified import vpn-target attribute.

Format

display ip vpn-instance import-vt *ivt-value*

Parameters

Parameter	Description	Value
ivt-value	Specifies the value of the import VPN-target attribute. The forms of VPN targets are as follows: • 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. • IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. • Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. • 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If a PE is configured with multiple VPN instances, the **display ip vpn-instance import-vt** command can be run on the PE to check into which VPN instances a VPNv4 route with a specified VPN target can be imported.

The VPN target controls route learning between VPN instances. A VPN target may be either an import VPN target or an export VPN target. An export VPN target is contained in a VPNv4 route to be advertised to a remote MP-BGP peer. Receiving a VPNv4 route, an MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 route can be added to the routing table of the local VPN instance IPv4 address family.

Precautions

At present, this command cannot be used to view the VPN instance with multiple import VPN-target attributes specified.

Example

Display the VPN instance with the import VPN-target attribute being 1:1.

```
<Huawei> display ip vpn-instance import-vt 1:1
The number of ipv4-family matched the import-vt : 3
 VPN-Instance Name and ID : vrf1, 1
 VPN-Instance Name and ID : vrf4, 5
 VPN-Instance Name and ID : vrf5, 4
```

Table 12-92 Description of the display ip vpn-instance import-vt command output

Item	Description
The number of ipv4-family matched the import-vt	Number of VPN instances with the specified import VPN-target attribute in the VPN instance IPv4 address family view.
VPN-Instance Name and ID	Name and ID of the VPN instance.

Related Topics

12.9.35 ip vpn-instance

12.9.69 vpn-target

12.9.16 display interface tunnel

Function

The **display interface tunnel** command displays details of the tunnel interface.

Format

display interface tunnel [*interface-number* | **main**]

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface. If this parameter is not specified, the command displays information about all tunnel interfaces.	The value must be the number a tunnel interface that has been created.
main	Displays status and traffic statistics about main interface. The interface has no sub-interfaces. Status and traffic statistics about the interface are displayed whether you specify the main parameter or not.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the details of the tunnel interface.

```
<Huawei> display interface tunnel 0/0/2
Tunnel0/0/2 current state : UP
Line protocol current state : UP
```

```
Description:HUAWEI, AR Series, Tunnel0/0/2 Interface
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1), destination 10.1.1.1
Tunnel protocol/transport GRE/IP, key disabled
keepalive disabled
Checksumming of packets disabled
Current system time: 2012-08-09 18:53:47
    300 seconds input rate 0 bits/sec, 0 packets/sec
    300 seconds output rate 0 bits/sec, 0 packets/sec
    15 seconds input rate 0 bits/sec, 0 packets/sec
    15 seconds output rate 0 bits/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
    Input bandwidth utilization  : 0%
    Output bandwidth utilization : 0%
```

Table 12-93 Description of the display interface tunnel command output

Item	Description
Tunnel0/0/2 current state	Physical layer status of the Tunnel0/0/2 interface: ● UP: The interface is in normal state. ● Administratively DOWN: The network administrator executes the **shutdown** command on the interface. After a tunnel interface is created, its physical layer status is Up.
Line protocol current state	Link protocol status of the Tunnel0/0/2 interface: ● UP: The link layer protocol of the tunnel interface works normally. ● DOWN: The link layer protocol of the tunnel interface is abnormal.
Description	Description of the tunnel interface.
Route Port,The Maximum Transmit Unit is 1500	MTU of tunnel interfaces, which is 1500 bytes by default. Any packet larger than the MTU is fragmented before being sent. If non-fragmentation is configured, the packet is discarded.
Internet protocol processing: disabled	IP protocol is disabled.
Encapsulation is TUNNEL	Encapsulation type of packets on a tunnel interface. Packet encapsulation protects a whole IP packet.
loopback not set	The tunnel interface does not support a loopback test.
Tunnel source 10.10.10.1 (GigabitEthernet0/0/1)	The source address of the tunnel is 10.10.10.1. That is, the IP address of the GigabitEthernet 0/0/1 interface sending packets at the source side is 10.10.10.1.
destination	Destination address of the tunnel.

Item	Description
Tunnel protocol/ transport GRE/IP, key disabled	The tunnel encapsulation protocol is the GRE protocol, and the transport protocol is the IP protocol. Encapsulation protocol types of a tunnel are as follows: ● GRE: indicates Generic Routing Encapsulation. ● IPSec: indicates tunnel mode of IPSec to protect data stream. ● MPLS: encapsulates packets into MPLS packets. ● IPv6 over IPv4: encapsulates IPv6 packets into IPv4 packets. ● IPv4 over IPv6: encapsulates IPv4 packets into IPv6 packets. ● SVPN: encapsulates packets into SVPN packets. ● none: indicates no encapsulation. This is the default mode of the tunnel interface. key disabled: the key word recognition function of GRE is not enabled.
keepalive disabled	The keepalive function of GRE is not enabled.
Checksumming of packets disabled	The check sum function of GRE is not enabled.
300 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
300 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface in the last 300 seconds. **NOTE** If the tunnel encapsulation protocol is SVPN, this field is not supported.
15 seconds input rate 0 bits/sec, 0 packets/sec	Rate of bits and packets received on the interface during the last query period.
15 seconds output rate 0 bits/sec, 0 packets/sec	Rate of bits and packets sent through the interface during the last query period.
0 packets input, 0 bytes 0 input error	Total packets and bytes received on the interface and the total number of defective packets.
0 packets output, 0 bytes 0 output error	Total packets and bytes sent through the interface and the total number of defective packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input bandwidth utilization	Input bandwidth usage.
Output bandwidth utilization	Output bandwidth usage.

Related Topics

12.3.11 keepalive

12.9.17 display l3vpn vpn-list tunnel-policy

Function

The **display l3vpn vpn-list tunnel-policy** command displays all the VPN instances to which a specified tunnel policy is applied.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display l3vpn vpn-list tunnel-policy *tunnel-policy-name*

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of a tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To have its routes iterated to tunnels, a VPN instance needs to apply a tunnel policy. If the tunnel policy used by a VPN instance is changed or the status of tunnels selected based on the tunnel policy changes, the iterated tunnels may change. The **display l3vpn vpn-list tunnel-policy** command displays all the VPN instances to which a specified tunnel policy is applied. The command output will show the VPN instances that will be affected by changes in the tunnel policy.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the referential relationship between a tunnel policy and a VPN instance.

```
<Huawei> display l3vpn vpn-list tunnel-policy p1
Codes: *(Tunnel policy is not configured)
Tunnel Policy Name: p1
Total VPN Instance(s) number: 1
VPN(s) using the tunnel policy:
vrf1
```

Table 12-94 Description of the **display l3vpn vpn-list tunnel-policy** command output

Item	Description
Codes	Comments
Tunnel Policy Name	Name of a tunnel policy
Total VPN Instance(s) number	Number of VPN instances specified with tunnel policies
VPN(s) using the tunnel policy	Name of VPN instances specified with tunnel policies

12.9.18 display mpls label-stack vpn-instance

Function

The **display mpls label-stack vpn-instance** command displays information about L3VPN label stacks.

Format

display mpls label-stack vpn-instance *vpn-instance-name ip-address*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
ip-address	Specifies a private IPv4 address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

In a non-inter-AS L3VPN scenario, this command allows you to query label stack information on PEs based on VPN instance names and private IP addresses.

Example

Display label stack information about the VPN instance named **vpna**.

```
<Huawei> display mpls label-stack vpn-instance vpna 10.12.12.1
Label-stack  : 1
Level        : 1
Type         : VPN
Label        : 1033
Level        : 2
Type         : LDP
Label        : 1041
OutInterface : Vlanif100
```

Table 12-95 Description of the **display mpls label-stack vpn-instance** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

12.9.19 display snmp-agent trap feature-name l3vpn all

Function

The **display snmp-agent trap feature-name l3vpn all** command displays whether the trap function is enabled for the L3VPN module and the excessive trap flag.

Format

display snmp-agent trap feature-name l3vpn all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display snmp-agent trap feature-name l3vpn all** command displays the following information:

- Trap names supported by the L3VPN module. The trap names are the same as the trap names specified by the **snmp-agent trap enable feature-name l3vpn** command. Each trap name corresponds to a network element abnormality.
- Trap status of the L3VPN module. You can check whether the trap is reported based on the trap name.

Example

Display whether the trap function is enabled for the L3VPN module and the excessive trap flag.

```
<Huawei> display snmp-agent trap feature-name l3vpn all
-------------------------------------------------------------------------------
Feature name: l3vpn
Trap number : 6
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
L3VPN_MIB_TRAP_VRF_UP          off                     off
L3VPN_MIB_TRAP_VRF_DOWN        off                     off
L3VPN_MIB_TRAP_THRESH_CLEARED  off                     off
L3VPN_MIB_TRAP_THRESH_EXCEED   off                     off
L3VPN_MIB_TRAP_MID_THRESH_EXCEED
                               off                     off
L3VPN_MIB_TRAP_TUNNEL_UPDOWN_EVENT
                               off                     off
```

Table 12-96 Description of the display snmp-agent trap feature-name l3vpn all command output

Item	Description
Feature name	Name of the module.
Trap number	Number of trap messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Types of trap messages: ● L3VPN_MIB_TRAP_MID_THRESH_EXCEED: The number of VPN routes exceeds the maximum number of route prefixes allowed. ● L3VPN_MIB_TRAP_THRESH_CLEARED: The number of VPN routes falls below the threshold. ● L3VPN_MIB_TRAP_THRESH_EXCEED: The number of VPN routes exceeds the threshold. ● L3VPN_MIB_TRAP_TUNNEL_UPDOWN_EVENT: The status of the tunnel used by a VPN changed. ● L3VPN_MIB_TRAP_VRF_DOWN: a trap message indicating a VRF Down event. ● L3VPN_MIB_TRAP_VRF_UP: a trap message indicating a VRF Up event.
Default switch status	Default status of a trap message: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of a trap message: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

12.9.54 snmp-agent trap enable feature-name l3vpn

12.9.20 display traffic-statistics vpn-instance

Function

The **display traffic-statistics vpn-instance** command displays the traffic statistics about the specified VPN instance.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display traffic-statistics vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Run this command to view the statistics about traffic of the specified VPN instance.

Example

Display the statistics about the VPN instance named **vpna**.

```
<Huawei> display traffic-statistics vpn-instance vpna
 vpn-instance name: vpna
 Statistics last cleared: 0000-00-00 00:00:00
 Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
 Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
 Input: 0 bytes, 0 packets
 Output: 0 bytes, 0 packets
 Input:
   Unicast: 0 packets, Multicast: 0 packets
   Broadcast: 0 packets
 Output:
   Unicast: 0 packets, Multicast: 0 packets
   Broadcast: 0 packets
```

Table 12-97 Description of the **display traffic-statistics vpn-instance** command output

Item	Description
vpn-instance name	Name of a VPN instance
Statistics last cleared	Time when statistics are cleared last time
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds
Input	Total number of received bytes and packets

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Output	Total number of sent bytes and packets
Unicast	Number of unicast packets
Multicast	Number of multicast packets
Broadcast	Number of broadcast packets

Related Topics

12.9.49 reset traffic-statistics vpn-instance

12.9.21 display tunnel-info

Function

The **display tunnel-info** command displays the tunnel information.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display tunnel-info { **tunnel-id** *tunnel-id* | **all** | **statistics** [**slots**] }

Parameters

Parameter	Description	Value
tunnel-id *tunnel-id*	Specifies the tunnel ID. If the specified ID does not exist, the system prompts errors.	A hexadecimal integer ranging from 1 to FFFFFFFE.
all	Displays information about all the tunnels.	-
statistics	Displays statistics about all tunnels.	-
slots	Displays tunnel statistics in the order of interface boards.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display tunnel-info all** command displays existing tunnel IDs, tunnel types, destination IP addresses, and Token information about all tunnels.

The **display tunnel-info tunnel-id** *tunnel-id* command displays detail information about a tunnel when you only know the tunnel ID.

The **display tunnel-info statistics** command displays the number of tunnels configured on the router.

Example

View information about the GRE tunnel.

```
<Huawei> display tunnel-info tunnel-id 10003
Tunnel ID:                0x10003
Tunnel Token:               3
Type:                     gre
Destination:                10.1.1.1
Out Slot:                 0
Instance ID:               0
Interface:                Tunnel0/0/1
```

Table 12-98 Description of the display tunnel-info command output

Item	Description
Tunnel ID	Tunnel ID in hexadecimal notation that is assigned by the system.
Tunnel Token	Token value used for MPLS forwarding that is a part of tunnel ID and is assigned by the system.
Type	Type of a tunnel, such as GRE, LSP, or CR-LSP. The command output varies according to the tunnel type.
Destination	Destination IP address of the tunnel.
Out Slot	Number of the slot that is used when the router sends packets.
Instance ID	VPN instance ID (0 indicates that a tunnel is a public network tunnel).
Interface	Local tunnel interface.

Display all tunnel information.

```
<Huawei> display tunnel-info all
* -> Allocated VC Token
Tunnel ID          Type              Destination          Token
-----------------------------------------------------------------------
0x1800800          lsp                3.3.3.3              0
0x1800801          lsp                2.2.2.2              1
0x41804bb8          lsp                192.168.2.0            3000
```

Display tunnel statistics.

```
<Huawei> display tunnel-info statistics
LSP/32bit LSP :                    3/3
GRE :                              0
CRLSP :                            2
LOCAL IFNET :                      0
MPLS LOCAL IFNET :                 0
VPN QOS LSP :                      0
Reserved :                         0
```

Table 12-99 Description of the display tunnel-info statistics command output

Item	Description
LSP/32bit LSP	Number of LSP tunnels created in the system view/Number of LSP tunnels triggered by the route of host with the 32-bit mask address.
GRE	Number of tunnel IDs allocated to the GRE tunnels.
CRLSP	Number of tunnel IDs allocated to the CR-LSP tunnels.
LOCAL IFNET	Number of tunnels used by the VPN internal module.
MPLS LOCAL IFNET	Number of tunnels used by the MPLS internal module.
VPN QOS LSP	Number of the tunnel ID allocated to the LSP used in VPN QoS.
Reserved	Number of the tunnel ID allocated to the product.

Display tunnel statistics in the order of interface boards.

```
<Huawei> display tunnel-info statistics slots
-----------------------------------------------------------------
Slot          LSP    CR     GRE    LCL    MPLS-L  VPN
Num                  LSP           IFNET  IFNET   QOS
-----------------------------------------------------------------
0             0      0      0      0      0       0
Logic Slot: 0                  Total:  0
-----------------------------------------------------------------
TOTAL         0      0      0      0      0       0
                             Total:  0
-----------------------------------------------------------------
```

Table 12-100 Description of the display tunnel-info statistics slots command output

Item	Description
Slot Num	Slot number used by the device to send packets.
LSP	Total LSP tunnels set up by the device.
CR LSP	Number of CR-LSPs created on the device.

Item	Description
GRE	Number of GRE tunnels created on the device.
LCL IFNET	Number of tunnels used by the VPN module.
MPLS-L IFNET	Number of tunnels used by the MPLS module.
VPN QOS	Number of tunnels used for VPN QoS.

12.9.22 display tunnel-policy

Function

The **display tunnel-policy** command displays the configurations of tunnel policies.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display tunnel-policy [*tunnel-policy-name*]

Parameters

Parameter	Description	Value
tunnel-policy-name	Specifies the name of tunnel policy. If *policy-name* is specified, information about the specified tunnel policy is displayed.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display tunnel-policy** command, you can check the configured tunnel policy and information about a tunnel policy before applying it.

Example

Display information about all the tunnel policies.

```
<Huawei> display tunnel-policy
Total   tunnel policy num:          2
```

```
Sel-Seq tunnel policy num:            1
Binding tunnel policy num:            1
Invalid tunnel policy num:            0
Tunnel Policy Name  Select-Seq                    Load balance No
-----------------------------------------------------------------
po2                 CR-LSP LSP                    1

Tunnel Policy Name  Destination     Tunnel Intf                 Ignore-dest-check   Down switch
-----------------------------------------------------------------------------------------------
po1                 1.1.1.1         Tunnel0/0/2                 Disable             Disable
```

Table 12-101 Description of the display tunnel-policy command output

Item	Description
Total tunnel policy num	Total number of tunnel policies.
Sel-Seq tunnel policy num	Total number of tunnel policies in select-sequence mode.
Binding tunnel policy num	Total number of tunnel policies in tunnel binding mode.
Invalid tunnel policy num	Total number of invalid tunnel policies.
Tunnel Policy Name	Name of tunnel policies.
Select-Seq	Priorities of tunnel types in descending order.
Load balance No	Number of tunnels for load balancing. The default value is 1.
Destination	Destination IP addresses of the bound tunnels, that is, IP addresses of the peer interfaces that receive packets.
Tunnel Intf	Local tunnel interface of the bound tunnel.
Ignore-dest-check	Check is disabled regardless of whether the destination IP address specified in a tunnel policy is consistent with the actual destination address of the tunnel to be bound to the tunnel policy.
Down switch	Tunnel switch over status: ● Enable indicates that the function is enabled ● Disable indicates that the function is disabled

Display information about the tunnel policy.

```
<Huawei> display tunnel-policy p1
The number of binding:2
Tunnel Policy Name                  Destination     Tunnel Intf       Ignore-dest-check   Down Switch
-------------------------------------------------------------------------------------------------------
tep                                 2.2.2.2         Tunnel0/0/2       Enable              Disable
                                                    Tunnel0/0/3
                                    3.3.3.3         Tunnel0/0/2       Enable              Disable
                                                    Tunnel0/0/3
```

Table 12-102 Description of the display tunnel-policy tunnel-policy-name command output

Item	Description
The number of binding	Number of the bound destination addresses.

Related Topics

12.9.63 tunnel-policy (system view)

12.9.23 display tunnel-policy-config

Function

The **display tunnel-policy-config** command displays the configuration of tunnel policies.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display tunnel-policy-config [*tunnel-policy-name*]

Parameters

Parameter	Description	Value
tunnel-policy-name	Indicates the name of the tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After tunnel policies are configured, you can view the configuration of a tunnel policy by using the **display tunnel-policy-config** command. If you do not specify the tunnel policy to be displayed, the configurations of all tunnel policies are displayed.

Example

Display the configurations of all tunnel policies.

```
<Huawei> display tunnel-policy-config
#
tunnel-policy sel-1
 tunnel select-seq cr-lsp lsp load-balance-number 1
#
tunnel-policy bind-1 tunnel binding destination 1.1.1.1 te Tunnel0/0/1 down-switch
#
return
```

Display the configuration of the tunnel policy named p1.

```
<Huawei> display tunnel-policy-config p1
#
tunnel-policy p1
 tunnel select-seq cr-lsp lsp load-balance-number 1
#
return
```

Related Topics

12.9.63 tunnel-policy (system view)

12.9.24 display tunnel-policy subscriber statistics

Function

The **display tunnel-policy subscriber statistics** command displays the number of times a tunnel policy is used by external services.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display tunnel-policy *tunnel-policy-name* **subscriber statistics**

Parameters

Parameter	Description	Value
tunnel-policy-name	Specify the name of a tunnel policy.	The value is the name of an existing tunnel policy.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

A system has many tunnel policies that can be used by different services. The **display tunnel-policy subscriber statistics** command can be used to view the

number of times a tunnel policy is used by external services. This prevents the tunnel policy from being deleted mistakenly.

Example

View the number of times a tunnel policy is used by external services.

```
<Huawei> display tunnel-policy nms-vrf-vpna subscriber statistics
The specified tunnel policy does not exist.
Total 200 applications subscribed the tunnel policy.
```

View the number of times a tunnel policy is used by external services.

```
<Huawei> display tunnel-policy nms-vrf-vpna subscriber statistics
The specified tunnel policy does not exist.
Total 0 applications subscribed the tunnel policy.
```

View the number of times a tunnel policy is used by external services.

```
<Huawei> display tunnel-policy nms-vrf-vpna subscriber statistics
Total 200 applications subscribed the tunnel policy.
```

Table 12-103 Description of the **display tunnel-policy subscriber statistics** command output

Item	Description
The specified tunnel policy does not exist. Total 200 applications subscribed the tunnel policy.	The tunnel policy does not exist and is used by 200 applications.
The specified tunnel policy does not exist. Total 0 applications subscribed the tunnel policy.	The tunnel policy does not exist and is not used by applications.
Total 200 applications subscribed the tunnel policy.	The tunnel policy exists and is used by 200 applications.

12.9.25 display tunnel-selector

Function

The **display tunnel-selector** command displays the configurations of tunnel selectors of a system.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

display tunnel-selector [*tunnel-selector-name*]

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel selector.	The value is the name of an existing tunnel selector.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If *tunnel-selector-name* is not specified in the command, the command displays the configurations of all the tunnel selectors of the system.

Example

Display information about a tunnel selector named tps.

```
<Huawei> display tunnel-selector tps
Tunnel-selector : tps
  permit : 10 (matched counts: 0)
    Match clauses :
      if-match ip next-hop ip-prefix ipv4prefix
    Apply clauses :
      apply tunnel-policy policy1
```

Table 12-104 Description of the **display tunnel-selector** command output

Item	Description
Tunnel-selector	Name of a tunnel selector
permit : 10	Matching mode and number of the node of the tunnel selector
Match clauses	**if-match** clauses
Apply clauses	**apply** causes

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.9.59 tunnel-selector (system view)

12.9.26 export route-policy

Function

The **export route-policy** command associates the current VPN instance address family with an export Route-Policy.

The **undo export route-policy** command disassociates the current VPN instance address family from the export Route-Policy.

By default, the current VPN instance address family is not associated with any export Route-Policy.

Format

export route-policy *policy-name*

undo export route-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the export Route-Policy to be associated with the VPN instance address family.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can implement a more accurate advertisement of the routes of the VPN instance address family based on the export Route-Policy than that based on the extended community attribute. The export Route-Policy is used to filter the routing information and to set the routing attributes of the routes that pass the filtering.

The **export route-policy** command advertises local routes of the VPN instance address family to other VPN instances address family. The **peer route-policy**

 Copyright © Huawei Technologies Co., Ltd.

command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

In local cross scenarios, you can run the **export route-policy** command to filter out locally crossed routes and set the attributes of these routes. Locally crossed routes include both locally imported routes and routes learned from VPN peers.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The current VPN instance address family can be associated with only one export Route-Policy. If the **export route-policy** command is run several times, the latest configuration overrides the previous configurations.

If the route policy does not exist, you need to configure the route policy.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the route-policy nonexistent-config-check disable command is run in the system view and a nonexistent route-policy is referenced using the current command in the VPN instance view or BGP-VPN instance IPv4 address family view, all routes in the VPN instance address family can be crossed to the VPNv4 address family. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command in the BGP-VPN instance IPv6 address family view, all routes in the BGP-VPN instance IPv6 address family can be crossed to the VPNv6 address family.

Example

Apply an export Route-Policy named poly-1 to the IPv4 address family of the VPN instance named vrf1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] export route-policy poly-1
```

Related Topics

12.9.30 import route-policy

12.9.27 if-match ip next-hop (tunnel-selector view)

Function

The **if-match ip next-hop** command configures route filtering based on the next hop.

The **undo if-match ip next-hop** command cancels the setting.

By default, route filtering based on the next hop is not configured.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

if-match ip next-hop { **acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name* }

undo if-match ip next-hop [**acl** { *acl-number* | *acl-name* } | **ip-prefix** *ip-prefix-name*]

Parameters

Parameter	Description	Value
acl *acl-number*	Specifies the number of a basic ACL.	The value is an integer ranging from 2000 to 2999.
acl *acl-name*	Specifies the name of a named ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command can be run in the tunnel selector view in the following scenarios:

- The ASBR or SPE in inter-AS VPN Option B or HVPN networking needs to apply a tunnel policy to VPNv4 routes to, for example, have the VPNv4 routes iterated to MPLS TE tunnels.
- The PE in inter-AS VPN Option C networking needs to apply a tunnel policy to BGP-IPv4 labeled routes to, for example, have the BGP-IPv4 labeled routes iterated to MPLS TE tunnels.

The **if-match ip next-hop** command is used to apply a tunnel policy to the VPNv4 or BGP-IPv4 labeled routes with a specified next hop, not all VPNv4 or BGP-IPv4 labeled routes.

Either an ACL or IP prefix list can be used to filter routes by next hop.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisite

The **12.9.59 tunnel-selector (system view)** command is run to create a tunnel selector.

An IP prefix list is configured using the **ip ip-prefix** command, or an ACL is configured using the **acl** command in the system view or the **acl name** command to specify the next hop.

Follow-up Procedure

Run the **12.9.1 apply tunnel-policy (tunnel-selector view)** command in the tunnel selector view to apply a tunnel policy to the routes that pass the filtering.

Precautions

Creating an ACL before it is referenced is recommended. If a nonexistent ACL is referenced using the command, all routes match the ACL.

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all routes match the IP prefix list.

Example

Configure route filtering based on the next hop.

```
<Huawei> system-view
[Huawei] tunnel-selector abc permit node 10
[Huawei-tunnel-selector] if-match ip next-hop acl 2000
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

12.9.1 apply tunnel-policy (tunnel-selector view)

9.9.47 ip ip-prefix

12.9.59 tunnel-selector (system view)

12.9.28 if-match ip-prefix (tunnel-selector view)

Function

The **if-match ip-prefix** command configures a tunnel selector to use an IP prefix list as a route filtering rule.

The **undo if-match ip-prefix** command restores the default configuration.

By default, a tunnel selector does not use any IP prefix list as a route filtering rule.

Format

if-match ip-prefix *ip-prefix-name*

undo if-match ip-prefix *ip-prefix-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of an IP prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Tunnel-selector view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to match routes against a specified IP prefix list and determine whether to permit or deny the routes based on matching results, run the **if-match ip-prefix** command to configure a tunnel selector to use the IP prefix list as a route filtering rule.

The **if-match ip-prefix** command must be used with the **ip ip-prefix** command. For example:

- If the **if-match ip-prefix aa** command is configured but the **ip ip-prefix aa** command is not configured, all routes will be permitted.
- If the **if-match ip-prefix aa** and **ip ip-prefix aa permit 1.1.1.1 32** commands are both configured, BGP routes with IP prefix 1.1.1.1/32 will be permitted.

Prerequisites

A tunnel selector has been configured using the **tunnel-selector** command.

Configuration Impact

Routes are filtered by IP prefix. Only routes matching the specified IP prefix list are permitted.

Example

Configure a tunnel selector to use IP prefix list **p1** as a route filtering rule.

```
<Huawei> system-view
[Huawei] tunnel-selector policy permit node 10
[Huawei-tunnel-selector] if-match ip-prefix p1
```

 Copyright © Huawei Technologies Co., Ltd.

12.9.29 if-match ipv6 next-hop (tunnel-selector view)

Function

The **if-match ipv6 next-hop** command configures the filtering of IPv6 routes based on the next hop.

The **undo if-match ipv6 next-hop** command cancels the setting.

By default, the filtering of IPv6 routes based on the next hop is not configured.

Format

if-match ipv6 next-hop prefix-list *ipv6-prefix-name*

undo if-match ipv6 next-hop prefix-list *ipv6-prefix-name*

Parameters

Parameter	Description	Value
prefix-list *ipv6-prefix-name*	Specifies the name of an IPv6 prefix list.	The name is a string of 1 to 169 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

tunnel selector view

Default Level

2: Configuration level

Usage Guidelines

You can run the **if-match ipv6 next-hop** command if it is required to filter IPv6 routes based on the next hop. When you run the **if-match ipv6 next-hop** command in the tunnel selector view, you can use an **apply** clause to apply a tunnel policy to the IPv6 routes filtered based on the next hop.

The next hop can be specified by the IPv6 prefix list.

Example

Configure filtering of IPv6 routes based on the next hop.

```
<Huawei> system-view
[Huawei] tunnel-selector abc permit node 10
[Huawei-tunnel-selector] if-match ipv6 next-hop prefix-list ipv6prefix
```

Related Topics

9.9.48 ip ipv6-prefix

 Copyright © Huawei Technologies Co., Ltd.

12.9.30 import route-policy

Function

The **import route-policy** command associates the current VPN instance address family with an import Route-Policy.

The **undo import route-policy** command disassociates the current VPN instance address family from an import Route-Policy.

By default, the current VPN instance address family is not associated with any import Route-Policy.

Format

import route-policy *policy-name*

undo import route-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the import Route-Policy to be associated with the VPN instance address family.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When no import Route-Policy is configured, routes that match the export VPN target attribute of the received routes and the import VPN target attribute of the local VPN instance address family are added to the VPN instance address family. To control the import of the routes into the VPN instance address family more accurately, you can use the import Route-Policy. The import Route-Policy is used to filter the imported routing information and to set the routing attributes of the routes that pass the filtering.

The **import route-policy** command controls the VPN routes that are cross added to the VPN instance address family. The **peer route-policy** command or the **filter-policy** command run in the BGP VPN instance address family view filters routes of the VPN instance address family advertised to or received from CE neighbors.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

The current VPN instance address family can be associated with only one import Route-Policy. If the **import route-policy** command is run several times, the latest configuration overrides the previous configurations.

If the route policy to be associated with the VPN instance address family does not exist, you need to configure the route policy.

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command in the VPN instance view or BGP-VPN instance IPv4 address family view, all routes in the VPNv4 address family can be crossed to the VPN instance address family. If the route-policy nonexistent-config-check disable command is run in the system view and a nonexistent route-policy is referenced using the current command in the BGP-VPN instance IPv6 address family view, all routes in the VPNv6 address family can be crossed to the VPN instance address family.

Example

Apply an import Route-Policy named poly-1 to the IPv4 address family of the VPN instance named vrf1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] import route-policy poly-1
```

Related Topics

12.9.26 export route-policy

12.9.31 ingress-lsp trigger

Function

The **ingress-lsp trigger** command specifies a routing policy to control the creation of ingress LSPs based on labeled BGP IPv4 routes.

The **undo ingress-lsp trigger** command restores the default setting.

By default, ingress LSPs are created based on all received BGP labeled routes.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

ingress-lsp trigger route-policy *route-policy-name*

undo ingress-lsp trigger

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of a routing policy to be used to create ingress LSPs based on BGP labeled routes.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a MAN where the hybrid access mode is used, a large number of BGP labeled routes are used to establish end-to-end LSPs. On certain intermediate nodes where VPN services do not need to be supported, excessive ingress LSPs are created, causing the waste of network resources. In this case, you can run the **ingress-lsp trigger** command to create ingress LSPs based on a routing policy to save network resources.

Configuration Impact

If the **ingress-lsp trigger** command is run more than once, the latest configuration overrides the previous ones.

Follow-up Procedure

If the routing policy specified in the **ingress-lsp trigger** command does not exist, you need to configure the routing policy by using the **route-policy** command.

Example

Specify a routing policy named test-policy to control the creation of ingress LSPs based on labeled IPv4 routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] ingress-lsp trigger route-policy test-policy
```

Related Topics

9.9.53 route-policy

12.9.32 interface tunnel

Function

The **interface tunnel** command creates a tunnel interface.

The **undo interface tunnel** command deletes the configured tunnel interface.

By default, no tunnel interface is configured.

Format

interface tunnel *interface-number*

undo interface tunnel *interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-number	Specifies the number of the tunnel interface with format "slot/subslot/number".	The slot, subslot, or interface number is an integer. The value range of the slot or subslot number varies according to the device type. The value of the interface number ranges. ● AR100&AR120&AR150&AR160&AR200 series: 0 to 255 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204E, AR2204E-D: 0 to 255 ● AR2220, AR2220E: 0 to 1023 ● AR2204XE, AR2204XE-DC, AR2240 (using SRU40, SRU60, or SRU80), AR2240C, AR3200 (using SRU40, SRU60, or SRU80) series: 0 to 2047 ● AR2240 (using SRU200, or SRU200E, or SRU400), AR3200 (using SRU200, or SRU200E, or SRU400) series: 0 to 4095 ● AR3600 (using SRUX5) series: 0 to 4095

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To forward data over a tunnel, ensure that the tunnel has been created. The system supports the following types of tunnels:

- LSP (Static LSP, BGP LSP, LDP LSP)
- MPLS TE
- IPSec
- GRE
- IPv6 over IPv4
- IPv4 over IPv6

You must use the **interface tunnel** command to create a tunnel interface when creating a tunnel except for LSP tunnels.

Precautions

After a tunnel interface is created, you need to configure an IP address and encapsulation type for the tunnel interface.

To save IP addresses, run the **ip address unnumbered** command to configure the tunnel interface to borrow an IP address of another interface.

The **tunnel-protocol** command configures an encapsulation protocol for the tunnel interface. Then basic configurations are performed based on the encapsulation protocol:

- On an MPLS TE tunnel, run the **destination**, **mpls te tunnel-id**, **mpls te signal-protocol**, and **mpls te commit** commands.
- On the GRE, IPSec, IPv4 over IPv6, or IPv6 over IPv4 tunnel, run the **source** and **destination** commands.

Tunnel interface numbers are valid on the local device only. You can configure different numbers for the tunnel interfaces on the two ends.

If a tunnel is being used, services transmitted over the tunnel will be affected after the tunnel interface is deleted. Exercise caution when running the **undo interface tunnel** command.

Example

Create a tunnel interface.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1]
```

12.9.33 ip binding vpn-instance

Function

The **ip binding vpn-instance** command associates an interface on a PE with a VPN instance.

The **undo ip binding vpn-instance** command disables the association between a VPN instance and an interface.

By default, an interface is a public network interface and is not associated with any VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip binding vpn-instance *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of the VPN instance that is associated with the interface.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a VPN instance is created, you need to associate the PE interface connecting to the VPN with the VPN instance. Then, the interface is used as a private network interface on which a private network address and a private network routing protocol can be configured.

Prerequisites

The **ip vpn-instance** command has been executed to create a VPN instance

Precautions

The binding relationship between an interface and a VPN instance with a BFD session bound is removable using the **undo ip binding vpn-instance** command only after the bound BFD session is removed.

Binding an interface to a VPN instance or deleting the binding will result in the deletion of the IP address of the interface, Layer 3 features, and IP-related routing protocols. These features must be re-configured if needed.

An interface cannot be bound to any VPN instance that is not enabled with any address family.

Using the **undo ipv4-family** or **undo ipv6-family** command to disable the IPv4 or IPv6 address family also deletes the IPv4 or IPv6 configurations of the interfaces bound to the VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

Example

Associate the VLANIF 10 interface with the VPN instance named **vrf1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] quit
[Huawei-vpn-instance-vrf1] quit
[Huawei] interface vlanif 10
[Huawei-Vlanif10] ip binding vpn-instance vrf1
Info: All IPv4 related configurations on this interface are removed!
Info: All IPv6 related configurations on this interface are removed!
```

Related Topics

12.9.14 display ip vpn-instance

12.9.34 ip frr (VPN instance view)

Function

The **ip frr** command enables IP FRR of a private network in the VPN instance IPv4 address family view.

The **undo ip frr** command disables IP FRR of a private network in the VPN instance IPv4 address family view.

By default, IP FRR of a private network is disabled in the VPN instance IPv4 address family view.

Format

ip frr route-policy *route-policy-name*

undo ip frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Enables IP FRR for the private routes matching the specified route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When there are private network routes generated by multiple types of routing protocols in a VPN instance enabled with the IPv4 address family, the **ip frr** command can be used to enable IP FRR to immediately switch traffic among routes and ensure the normal forwarding of traffic if certain routes are faulty. The following example shows how IP FRR works:

There are two routes to 1.1.1.1. One is a BGP route with priority 150, and the other one is a static route with priority 60. When IP FRR is not enabled, the static route is preferred. After IP FRR is enabled, the static route functions as the primary route, and the BGP route functions as the backup route. If the static route fails, the system immediately switches traffic to the BGP route to ensure the normal forwarding of traffic.

Precautions

The **ip frr** command must be used together with the **apply backup-interface** and **apply backup-nexthop** commands.

Only one route-policy can be configured every time you use the **ip frr** command. If you run the command multiple times, only the latest configuration takes effect. The configuration in the system view is independent of the configuration in the VPN instance view.

Example

Specify a backup outbound interface and a backup next hop in route-policy **ip_frr_rp** and enable IP FRR for private routes in the VPN instance view.

```
<Huawei> system-view
[Huawei] route-policy ip_frr_rp permit node 10
[Huawei-route-policy] apply backup-interface gigabitethernet 1/0/0
[Huawei-route-policy] apply backup-nexthop 192.168.20.2
[Huawei-route-policy] quit
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ip frr route-policy ip_frr_rp
```

12.9.35 ip vpn-instance

Function

The **ip vpn-instance** command creates a VPN instance and displays the VPN instance view.

The **undo ip vpn-instance** command deletes a specified VPN instance.

By default, no VPN instance is configured.

Format

ip vpn-instance *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When private network data needs to travel across a public network, you need to configure a VPN instance on the PE of the public network. The public network mentioned here is an MPLS backbone network.

VPN instances are required for all L3VPN configurations.

Precautions

After the ip vpn-instance command is run, a virtual routing table is created on the PE and consumes resources on the PE.

A VPN instance with a BFD session bound can be deleted using the **undo ip vpn-instance** command only after the bound BFD session is deleted.

After the **undo ip vpn-instance** command is used to delete a VPN instance, all configurations of this VPN instance are deleted.

Follow-up Procedure

After creating a VPN instance, perform the following configurations in the VPN instance view:

- Enable the IPv4 or IPv6 address family for the VPN instance. A VPN instance supports both the IPv4 and IPv6 address families. You need to run the **ipv4-family (VPN instance view)** or **ipv6-family (VPN instance view)** command to enable the IPv4 or IPv6 address family based on the type of the protocol stack used to advertise VPN routes in the VPN instance.
- Configure an RD for the IPv4 or IPv6 address family of the VPN instance. You are allowed to perform VPN configurations in the address family view only after using the **route-distinguisher** command to configure an RD for the address family.
- Configure a VPN target for the VPN instance using the **vpn-target** command. The VPN target controls route learning between VPN instances.

 Copyright © Huawei Technologies Co., Ltd.

- Bind the VPN instance to the PE or MCE interface connected to the VPN using the **ip binding vpn-instance** command. After an interface is bound to a VPN instance, the interface becomes a part of the VPN. Packets entering the interface will be forwarded based on the VRF table of the VPN.

Example

Create a VPN instance named **vrf1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1]
```

Related Topics

12.9.50 route-distinguisher

12.9.36 ipv4-family (VPN instance view)

12.9.37 ipv6-family (VPN instance view)

12.9.69 vpn-target

12.9.14 display ip vpn-instance

12.9.36 ipv4-family (VPN instance view)

Function

The **ipv4-family** command enables the IPv4 address family for a VPN instance and displays the VPN instance IPv4 address family view.

The **undo ipv4-family** command disables the IPv4 address family for a VPN instance.

By default, VPN instances are disabled with the IPv4 address family.

Format

ipv4-family

undo ipv4-family

Parameters

None.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IP VPN networking, after running the **ip vpn-instance** command to create a VPN instance, you can run the **ipv4-family** command to enable the IPv4 address family for the VPN instance and perform VPN configurations in the address family view if you want to have IPv4 VPN routes advertised and IPv4 VPN data forwarded.

Follow-up Procedure

Run the **route-distinguisher** command to configure an RD for the IPv4 address family of the VPN instance. VPN configurations can be performed in the IPv4 address family view only after an RD is configured for the IPv4 address family of the VPN instance.

Precautions

Configurations of the commands run in the VPN instance view, except the **description** command, are automatically synchronized to the VPN instance IPv4 address family view.

The IPv4 address family for a VPN instance with a BFD session bound can be disabled using the **undo ipv4-family** command only after the bound BFD session is deleted.

Example

Enable the IPv4 address family for a VPN instance.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4]
```

12.9.37 ipv6-family (VPN instance view)

Function

The **ipv6-family** command enables the IPv6 address family for a VPN instance and displays the VPN instance IPv6 address family view.

The **undo ipv6-family** command disables the IPv6 address family for a VPN instance.

By default, the IPv6 address family is disabled for a VPN instance.

Format

ipv6-family

undo ipv6-family

Parameters

None

Views

VPN instance view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In BGP/MPLS IPv6 VPN networking, after running the **ip vpn-instance** command to create a VPN instance, you can run the **ipv6-family** command to enable the IPv6 address family for the VPN instance and perform VPN configurations in the address family view if you want to have IPv6 VPN routes advertised and IPv6 VPN data forwarded.

Follow-up Procedure

Run the **route-distinguisher** command to configure an RD for the IPv6 address family of the VPN instance. VPN configurations can be performed in the IPv6 address family view only after an RD is configured for the IPv6 address family of the VPN instance.

Precautions

The IPv6 address family for a VPN instance with a BFD session bound can be disabled using the **undo ipv6-family** command only after the bound BFD session is deleted.

Example

Enable the IPv6 address family for the VPN instance named vrf1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv6-family
[Huawei-vpn-instance-vrf1-af-ipv6]
```

Related Topics

12.9.35 ip vpn-instance

12.9.38 limit-log-interval

Function

The **limit-log-interval** command configures the interval for displaying logs when the number of routes exceeds the threshold.

The **undo limit-log-interval** command restores the default setting.

By default, the interval for displaying logs when the number of routes exceeds the threshold is 5 seconds.

Format

limit-log-interval *interval*

undo limit-log-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the interval for displaying logs when the number of routes exceeds the threshold.	An integer ranging from 1 to 60, in seconds.

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the routes or prefixes in the IPv4 or IPv6 address family of a VPN instance reach the maximum, the system will generate logs at intervals (defaulting to 5 seconds). To prevent logs from being displayed frequently, run the **limit-log-interval** command to prolong the interval of log generation.

The maximum number of routes or prefixes that the IPv4 or IPv6 address family of a VPN instance supports can be configured using the **routing-table limit** or **prefix limit** command.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** or **ipv6-family** command has been executed to create a VPN instance and enter the VPN instance IPv4 or IPv6 address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

If a log is generated to record the event that routes or prefixes in the IPv4 address family of a VPN instance reach the maximum, no more routes can be added to the routing table of the IPv4 address family of the VPN instance. Instead, the routes will be discarded.

Example

Set the interval for displaying logs to 8 seconds when the number of routes in the IPv4 address family of the VPN instance named vpn1 exceeds the threshold.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn1-af-ipv4] limit-log-interval 8
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.9.51 routing-table limit
12.9.48 prefix limit
12.9.14 display ip vpn-instance
9.10.9 display ip routing-table limit

12.9.39 lsp-trigger bgp-label-route

Function

The **lsp-trigger bgp-label-route** command enables LDP to allocate labels to labeled BGP routes on the public network.

The **undo lsp-trigger bgp-label-route** command restores the default setting.

By default, LDP does not allocate labels to labeled BGP routes on the public network.

NOTE

The AR100&AR120&AR150&AR160&AR200 does not support this command.

Format

lsp-trigger bgp-label-route [**ip-prefix** *ip-prefix-name*]

undo lsp-trigger bgp-label-route

Parameters

Parameter	Description	Value
ip-prefix *ip-prefix-name*	Specifies the name of the IP prefix list that triggers the labeled BGP routes on the public network to set up LDP LSPs.	The value is an existing IP prefix list name.

Views

MPLS view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Both the **lsp-trigger bgp-label-route** command and the **lsp-trigger** command can be used to configure policies to trigger the establishment of LDP LSPs. The former command is used for labeled BGP routes on the public network, and the latter command is used for static routes and IGP routes.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Modifying the LSP-triggering policy during the LDP GR period is invalid.

Prerequisites

MPLS has been enabled globally using the **mpls (system view)** command.

Precautions

Creating an IP prefix list before it is referenced is recommended. By default, nonexistent IP prefix lists cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent IP prefix list is referenced using the current command, all public-network labeled BGP routes trigger LDP LSP establishment.

Example

Trigger the establishment of LDP LSPs according to labeled BGP routes on the public network.

```
<Huawei> system-view
[Huawei] mpls
[Huawei-mpls] lsp-trigger bgp-label-route
```

Related Topics

11.1.67 lsp-trigger

12.9.40 mpls te reserved-for-binding

Function

The **mpls te reserved-for-binding** command reserves an MPLS TE tunnel for VPN binding.

The **undo mpls te reserved-for-binding** command removes the configuration.

By default, an MPLS TE tunnel can be selected based on any type of tunnel policy.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

mpls te reserved-for-binding

undo mpls te reserved-for-binding

Parameters

None

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a VPN has high requirements for bandwidth, you can apply a tunnel binding policy to the VPN to have the routes of the VPN iterated to MPLS TE tunnels. Before applying that tunnel binding policy to the VPN, you need to run the **mpls te reserved-for-binding** command to reserve MPLS TE tunnels for VPN binding.

Prerequisites

MPLS TE tunnels are available in the system.

Configuration Impact

After the **mpls te reserved-for-binding** command is configured on an MPLS TE tunnel, the tunnel can be selected based on a tunnel binding policy only. Even if no tunnel binding policy is configured, a tunnel type prioritizing policy created using the **tunnel select-seq** command will not select the MPLS TE tunnel for which the **mpls te reserved-for-binding** command has been configured.

Follow-up Procedure

Run the **tunnel-policy** command to create a tunnel policy and the **tunnel binding** command to bind the policy to the MPLS TE tunnel.

Example

Reserve Tunnel0/0/1 for VPN binding.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol mpls te
[Huawei-Tunnel0/0/1] mpls te reserved-for-binding
```

Delete the configuration of a tunnel that is reserved for VPN binding.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] undo mpls te reserved-for-binding
```

Related Topics

12.9.58 tunnel binding

12.9.41 mtu (tunnel interface view)

Function

The **mtu** command sets the Maximum Transmission Unit (MTU) of a tunnel interface.

The **undo mtu** command restores the default value.

By default, the MTU is 1500 bytes on a tunnel interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

mtu *mtu*

undo mtu

Parameters

Parameter	Description	Value
mtu	Specifies the MTU of a tunnel interface.	An integer ranging from 128 to 9202, in bytes.

Views

Tunnel interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The size of data frames is limited at the network layer. Any time the IP layer receives an IP packet to be sent, it checks to which local interface the packet needs to be sent and obtains the MTU configured on the interface. Then the IP layer compares the MTU with the packet length. If the packet length is longer than the MTU, the IP layer fragments the packet into smaller packets, which are shorter than or equal to the MTU.

If unfragmentation is configured, some packets may be discarded during data transmission at the IP layer. To ensure jumbo packets are not dropped during transmission, you need to configure forcible fragmentation. In this case, you can run the **mtu** command to set the size of a fragment.

Precautions

Set the MTU for a tunnel interface based on actual networking. The default value is recommended. If a small MTU is used but the packet size is large, packets may be divided into many fragments. Then the packets are discarded by QoS queues. If a large MTU is used, packets may be transmitted at a low rate.

If IPv6 is run on a tunnel interface and the MTU set using the **mtu** command on the interface is smaller than 1280, IPv6 works abnormally on this interface. To prevent this problem, set the MTU of a tunnel interface to a value greater than or equal to 1280 if IPv6 runs on the tunnel interface.

After running the **mtu** command, run the **shutdown** and then **undo shutdown** commands on the interface. The set MTU then can take effect.

On a network with IPv4 over IPv6 tunnels, if a tunnel interface is Down, the MTU value of the tunnel interface 64000 does not take effect. After the tunnel interface goes Up, the system dynamically refreshes the MTU value of the tunnel interface

 Copyright © Huawei Technologies Co., Ltd.

based on the Path_MTU of the tunnel and IPv6 MTU of the tunnel outbound interface. If the Path_MTU does not exist, the system adopts the MTU of the tunnel outbound interface as the MTU of the tunnel interface.

On a network with Ethernet over GRE tunnels, the MTU configured on a tunnel interface takes effect for Layer 3 traffic but not Layer 2 traffic.

The **mtu** *mtu* command configuration on a TE tunnel interface takes effect for packets sent by hosts only in the following scenarios:

- In an L3VPN over TE scenario, if the length of a packet that a host sends exceeds the configured MTU value, the packet is fragmented based on the MTU value at the IP layer before being forwarded.
- In a TE tunnel scenario, the length of a tunnel detection packet must be less than the configured MTU value.

Example

Set the MTU of Tunnel 0/0/1 to 1492.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] mtu 1492
[Huawei-Tunnel0/0/1] shutdown
[Huawei-Tunnel0/0/1] undo shutdown
```

Related Topics

12.9.16 display interface tunnel

12.9.42 peer default-originate vpn-instance

Function

The **peer default-originate vpn-instance** command configures BGP to advertise all default routes related to the specified VPN instance to the specified VPNv4 peer or peer group.

The **undo peer default-originate vpn-instance** command removes the configuration.

By default, BGP does not advertise its default route to the VPNv4 peer or peer group.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

peer { *ipv4-address* | *group-name* } **default-originate vpn-instance** *vpn-instance-name*

undo peer { *ipv4-address* | *group-name* } **default-originate vpn-instance** *vpn-instance-name*

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vpn-instance-name	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HoVPN refers to a hierarchical VPN, with multiple PEs functioning as different roles to form a hierarchical architecture and provide functions of a single PE. In this manner, the performance requirement on PEs is lowered. If the **peer default-originate vpn-instance** command is used, SPE sends the default route with the address of the next hop as the local address, regardless of whether there is a default route in the local routing table. The UPE then only needs to maintain the local VPN routes, whereas all remote routes are replaced by the default route. The workload of the UPE is reduced.

Precautions

If an SPE does not have an active default route, either of the following methods can be used to generate a default route on the SPE and allow the SPE to advertise the route to the UPE:

- Method 1: Run the **peer default-originate vpn-instance** command to enable the SPE to automatically generate a default route and advertise it to the UPE.
- Method 2: Run the **ip route-static vpn-instance** command to configure a default route on the SPE, run the **default-route imported** command to enable the SPE to import the default route to the BGP routing table, and then run the **import-route static** or **network** command in the BGP-VPN instance IPv4 address family view to import the default route to the BGP IPv4 VPN instance routing table.

Either of the preceding methods can be used to advertise a default route to the UPE. The priority of the default route generated through method 1 is higher than

 Copyright © Huawei Technologies Co., Ltd.

that generated through method 2. If method 1 is used, the default route generated through method 2 will be suppressed, and no Update messages will be sent for a route change or withdrawal. If the SPE has an active default route, the SPE can advertise the route to the UPE without the need for either of the preceding methods.

Example

Advertise default routes of vpn1 to VPNv4 peer 1.1.1.1.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.1 as-number 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] peer 1.1.1.1 enable
[Huawei-bgp-af-vpnv4] peer 1.1.1.1 upe
[Huawei-bgp-af-vpnv4] peer 1.1.1.1 default-originate vpn-instance vpn1
```

Related Topics

12.9.44 peer upe

9.8.24 default-route imported

12.9.43 peer mpls-local-ifnet disable

Function

The **peer mpls-local-ifnet disable** command disables EBGP peers from establishing an MPLS local IFNET tunnel between them.

The **undo peer mpls-local-ifnet disable** command enables EBGP peers to establish an MPLS local IFNET tunnel between them.

By default, EBGP peers can automatically establish MPLS local IFNET tunnels between them if one of the following conditions is met:

- EBGP peers are enabled to exchange labeled routes.
- EBGP peers are configured in the BGP-VPNv4 address family.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

undo peer { *group-name* | *ipv4-address* } **mpls-local-ifnet disable**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	The value is in dotted decimal notation.

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the IPv4 VPN Option C scenario, EBGP peer relationships are established between BGP peers. The BGP peers can be endpoint PEs in the VPN Option C scenario. These EBGP peers automatically establish MPLS local IFNET tunnels between them. The E2E MPLS local IFNET tunnel fails to transmit traffic if the two peers are indirectly connected.

If a fault occurs on a tunnel between the two EBGP peers, traffic is iterated to the MPLS local IFNET tunnel, not an FRR bypass tunnel. As the MPLS local IFNET tunnel cannot forward traffic, traffic is interrupted. To prevent the traffic interruption, run this command to disable the establishment of an MPLS local IFNET tunnel between the EBGP peers.

Prerequisites

The EBGP peer relationship must be in the Established between PEs.

Example

Disable EBGP peers from establishing an MPLS local IFNET tunnel.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 10.1.1.1 as-number 200
[Huawei-bgp] peer 10.1.1.1 mpls-local-ifnet disable
```

12.9.44 peer upe

Function

The **peer upe** command specifies a BGP peer or peer group as UPE of HoVPN.

The **undo peer upe** command cancels the configuration.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

peer { *group-name* | *ipv4-address* } **upe**

undo peer { *group-name* | *ipv4-address* } **upe**

Parameters

Parameter	Description	Value
group-name	Specifies the name of the peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	-

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a UPE is specified on the SPE through the **peer upe** command, the SPE does not send a specific route to the UPE. If the **peer route-policy export** command is run on the SPE to configure routing policies for the UPE and certain specific routes can pass the filtration of routing policies, these specific routes can be sent to the UPE.

Prerequisites

Before you run the peer upe command, the **peer as-number** command should be used to create a peer or peer group.

Precautions

If an SPE does not have an active default route, either of the following methods can be used to generate a default route on the SPE and allow the SPE to advertise the route to the UPE:

- Method 1: Run the **peer default-originate vpn-instance** command to enable the SPE to automatically generate a default route and advertise it to the UPE.

- Method 2: Run the **ip route-static vpn-instance** command to configure a default route on the SPE, run the **default-route imported** command to enable the SPE to import the default route to the BGP routing table, and then run the **import-route static** or **network** command in the BGP-VPN instance IPv4 address family view to import the default route to the BGP IPv4 VPN instance routing table.

Either of the preceding methods can be used to advertise a default route to the UPE. The priority of the default route generated through method 1 is higher than that generated through method 2. If method 1 is used, the default route generated through method 2 will be suppressed, and no Update messages will be sent for a route change or withdrawal. If the SPE has an active default route, the SPE can advertise the route to the UPE without the need for either of the preceding methods.

The BGP peer relationship is interrupted after you run the **peer upe** command. So, confirm the action before you use the command.

Follow-up Procedure

After the **peer upe** command is configured, to send the default route 0.0.0.0 to the UPE, you need to run the **peer default-originate vpn-instance** command on the SPE.

Example

Specify the peer 1.1.1.2 as UPE.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.2 as-number 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] peer 1.1.1.2 enable
[Huawei-bgp-af-vpnv4] peer 1.1.1.2 upe
```

Related Topics

9.8.135 peer route-policy
12.9.42 peer default-originate vpn-instance

12.9.45 peer soo

Function

The **peer soo** command configures the Source of Origin (SoO) attribute for an EBGP peer in a BGP VPN instance.

The **undo peer soo** command deletes the SoO.

By default, no SoO attribute is configured for an EBGP peer in a BGP VPN instance.

Format

peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo** *site-of-origin*

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **soo**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a BGP peer.	It is in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a BGP peer.	The address is in the format of X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Site-of-origin	Specifies the SoO attribute, which is a BGP extended community attribute and can be expressed in any of the following formats: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a SoO cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a SoO cannot be 0.0:0.	-

Views

BGP-VPN instance IPv4 address family view or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. As a result, different sites of the same VPN cannot communicate. The **peer substitute-**

as command can be used to enable AS number substitution on PEs to address this problem.

Enabling AS number substitution will cause another problem. Several CEs at a VPN site may establish EBGP connections with different PEs of a BGP/MPLS IP VPN backbone network, and a routing protocol has been configured on the CEs. If AS number substitution is enabled on PEs, the AS numbers carried by VPN routes of this site will be replaced on the PEs. As a result, routes advertised from a CE to a PE may be re-advertised to this VPN site after the routes traverse the backbone network, causing a routing loop. The **peer soo** command can be run on the PEs to address this problem.

After the **peer soo** command is run on a PE to configure the SoO attribute for a specified CE, the PE adds the attribute to a route sent from the CE and advertises the route to the remote PE. The remote PE checks the SoO attribute of the route before sending it to its attached CE. If the SoO attribute is the same as the local SoO attribute on the remote PE, the remote PE does not send the route to its attached CE, preventing a routing loop in a VPN site.

Precautions

The **peer soo** command is used only in the scenarios where PEs and CEs establish EBGP peer relationships.

Example

Configure the SoO attribute for EBGP peers in a BGP VPN instance.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpn-instance vpna
[Huawei-bgp-vpna] peer 192.168.15.2 soo 10.2.2.2:45
```

Related Topics

12.9.46 peer substitute-as

12.9.46 peer substitute-as

Function

The **peer substitute-as** command enables AS number substitution. This command enables a device to replace the AS number of the peer specified in the AS_Path attribute with the local AS number.

The **undo peer substitute-as** command disables AS number substitution.

By default, AS number substitution is disabled.

Format

peer { *group-name* | *ipv4-address* } **substitute-as**

undo peer { *group-name* | *ipv4-address* } **substitute-as**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	It is in dotted decimal notation.

Views

BGP-VPN instance IPv4 address family view or BGP-VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a BGP/MPLS IP VPN scenario, if the ASs to which two VPN sites belong use private AS numbers, the AS numbers of the two VPN sites may be the same. If a CE in a VPN site sends a VPN route to the connected PE using EBGP and the PE then sends the route to the remote PE, the remote CE will discard the route because the AS number carried by the route is the same as the local AS number. As a result, different sites of the same VPN cannot communicate. The **peer substitute-as** command can be used on the PE to enable AS number substitution to address this problem. After that, the PE replaces the AS number carried in the VPN route with the local AS number. As a result, the remote CE will not discard the route due to identical AS numbers.

Pre-configuration Tasks

Run the **9.8.101 peer as-number** command to create a peer or configure an AS number for a specified peer group.

Precautions

Enabling BGP AS number substitution may cause route loops in a CE multi-homing network. The **peer soo** command must be run to prevent a routing loop in a VPN site.

Example

Configure a device to replace the AS number of a specified peer in the AS_Path of a route with the local AS number.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpn-instance vpn1
```

```
[Huawei-bgp-vpn1] peer 10.1.1.2 as-number 200
[Huawei-bgp-vpn1] peer 10.1.1.2 substitute-as
```

Related Topics

12.9.45 peer soo

12.9.47 policy vpn-target

Function

The **policy vpn-target** command configures a device to implement VPN target-based filtering for received routes.

The **undo policy vpn-target** command cancels VPN target-based filtering.

By default, the VPN-Target filtering is enabled.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the networking of BGP/MPLS IP VPN, VPN target attributes are used to filter received VPN routes or label blocks. If VPN target attributes are not configured, received VPN routes or label blocks are discarded.

VPNs and VPN target attributes are not configured on the following devices in certain networking scenarios:

- RRs in BGP/MPLS IP VPN
- ASBRs (not functioning as PEs) in inter-AS BGP/MPLS IP VPN OptionB

In this case, VPN routes or label blocks are not saved on the RRs or ASBRs.

 Copyright © Huawei Technologies Co., Ltd.

The RRs or ASBRs, however, need to save all VPN routes or label blocks sent from PEs. Therefore, the **undo policy vpn-target** command can be configured on the RRs or ASBRs to disable the filtering of VPN routes or label blocks.

Precautions

Running the **undo policy vpn-target** makes all VPN routes or label blocks from PEs received. Therefore, this command is configured only on devices of particular roles (RRs or ASBRs)

Example

Configure a device to implement VPN target-based filtering for received VPNv4 routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] policy vpn-target
```

12.9.48 prefix limit

Function

The **prefix limit** command sets a limit on the maximum number of prefixes supported in the existing VPN instance address family, preventing the PE from importing excessive VPN route prefixes.

The **undo prefix limit** command restores the default setting.

By default, the maximum number of VPN route prefixes is not limited.

Format

prefix limit *number* { *alert-percent* [**route-unchanged**] | **simply-alert** }

undo prefix limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of prefixes supported in the VPN instance address family. **NOTE** The maximum number of unicast prefixes allowed on a PE is determined by the license but is not specified through the **prefix limit** command. The total number of VPN route prefixes and public network route prefixes cannot exceed *number*. If the total number exceeds *number*, the route management module denies the subsequent route prefixes and generates an alarm.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
alert-percent	Specifies the proportion of the alarm threshold to the maximum number of prefixes. When the number of prefixes in the VPN instance address family exceeds *number* x *alert-percent*/100, alarms are displayed. The VPN route prefixes, however, can still join the VPN routing table. When the number of the prefixes exceeds the *number*, the subsequent prefixes are discarded.	The value is an integer ranging from 1 to 100.
route-unchanged	Indicates that the routing table remains unchanged. By default, **route-unchanged** is not configured. When the number of prefixes in the routing table is greater than the value of the parameter number, routes are processed as follows: ● If **route-unchanged** is configured, routes in the routing table remain unchanged. ● If **route-unchanged** is not configured, all routes in the routing table are deleted and then re-added.	-
simply-alert	Indicates that when the number of VPN route prefixes exceeds *number*, prefixes can still join the VPN routing table and alarms are displayed. On the device, however, the subsequent VPN route prefixes are discarded after the total number of the unicast prefixes of the private network and the public network reaches the upper limit.	-

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many useless route prefixes imported into a VPN instance constitute a large proportion of the route prefixes on a device, run the **prefix limit** command to set a limit on the maximum number of prefixes supported by the VPN instance. After the **prefix limit** command is run in the current VPN instance address family, if the number of route prefixes reaches the set limit, the system will generate an alarm to instruct the user to check the validity of route prefixes of the VPN instance.

Prerequisites

The **12.9.50 route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

After the command is run, the excess route prefixes of the current VPN instance address family will be discarded.

If the number of route prefixes exceeds the set limit and the **undo prefix limit** command is run, the system will receive the route prefixes from routing tables generated by protocols to create a private network routing table.

The **prefix limit** command can prevent the routing table of the current VPN instance address family on a PE from importing too many route prefixes, but cannot prevent the PE from importing excessive route prefixes from other PEs. Therefore, configuring both the **prefix limit** and **peer route-limit** commands is recommended.

Do not run both the **routing-table limit** (the command restricts the number of routes) and **prefix limit** (the command restricts the number of route prefixes) commands in the current VPN instance address family. Configure either one of them based on your need.

When the number of prefixes exceeds the upper limit, the **prefix limit** command with **simply-alert** specified enables the device to display only alarms and allows the device to add prefixes to the routing table.

Example

Configure the system to only generate alarms when the number of prefixes exceeds the maximum number 1000 in the VPN instance named vpn1.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn1-af-ipv4] prefix limit 1000 simply-alert
```

Related Topics

9.8.134 peer route-limit

12.9.51 routing-table limit

12.9.14 display ip vpn-instance

9.10.9 display ip routing-table limit

12.9.49 reset traffic-statistics vpn-instance

Function

The **reset traffic-statistics vpn-instance** command clears traffic statistics about the specified VPN instance.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

reset traffic-statistics vpn-instance { **name** *vpn-instance-name* | **all** }

Parameters

Parameter	Description	Value
name *vpn-instance-name*	Specifies the name of a VPN instance.	The value is the name of an existing VPN instance.
all	Clears the traffic statistics about all VPN instances.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run this command to clear L3VPN traffic statistics when you need to collect new traffic statistics.

Precautions

Statistics cannot be restored after being cleared. Therefore, use this command with caution.

Example

Clear statistics about traffic of the VPN instance with the name of **vpn1**.

```
<Huawei> reset traffic-statistics vpn-instance name vpn1
```

Clear statistics about traffic of all the VPN instances.

```
<Huawei> reset traffic-statistics vpn-instance all
Warning: Traffic-statistics information will be cleared! Continue? [Y/N]:y
```

Related Topics

12.9.20 display traffic-statistics vpn-instance

12.9.50 route-distinguisher

Function

The **route-distinguisher** command configures a route distinguisher (RD) for a VPN instance address family.

 Copyright © Huawei Technologies Co., Ltd.

By default, no RD is configured for the VPN instance address family.

Format

route-distinguisher *route-distinguisher*

Parameters

Parameter	Description	Value
route-distinguisher	Specifies the value of an RD. The forms of RD are as follows: ● 2-byte AS number:4-byte user-defined number, for example, 101:3. An AS number ranges from 0 to 65535. A user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot be 0s at the same time. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● IPv4-address:2-byte user-defined number, for example, 192.168.122.15:1. An IP address ranges from 0.0.0.0 to 255.255.255.255. A user-defined number ranges from 0 to 65535.	-

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VPN instance and enable the address family, run this command to configure an RD for the VPN instance address family.

Different VPN instances may have the same route prefix. To allow a PE to determine to which VPN instance a route belongs, run the **route-distinguisher** command to configure an RD for an address family of a VPN instance on the PE. After the configuration, the PE will add an RD to the route received from the VPN instance, and then the route prefix becomes a globally unique VPN IPv4 or IPv6 route.

Precautions

Execution of this command will also enable the IPv4 address family.

When the CE is dual-homed, the RDs on the PEs must be globally unique to ensure routing.

Once the RD is configured for the VPN instance address family, it cannot be modified or deleted. To change an RD, you need to delete the VPN instance identified by the RD or disable the VPN instance address family. Then, reconfigure the VPN instance and its RD.

Example

Configure an RD for the VPN instance named **vpn1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 22:1
```

Related Topics

12.9.35 ip vpn-instance
12.9.14 display ip vpn-instance

12.9.51 routing-table limit

Function

The **routing-table limit** command sets the maximum number of routes that the current VPN instance address family supports.

The **undo routing-table limit** command restores the maximum number of routes that the current VPN instance address family can support to the default setting.

By default, there is no limit on the maximum number of routes that the current VPN instance address family can support, but the total number of private network and public network routes on a device cannot exceed the allowed maximum number of unicast routes.

Format

routing-table limit *number* { *alert-percent* | **simply-alert** }

undo routing-table limit

Parameters

Parameter	Description	Value
number	Specifies the maximum number of routes supported by a VPN instance.	The value is an integer, and the minimum value is 1. The maximum number is determined by the license file.
alert-percent	Specifies the percentage of the maximum number of routes. When the maximum number of routes that join the VPN instance is up to the value (*number*alert-percent*)/100, the system prompts alarms. The VPN routes can be still added to the routing table, but after the number of routes reaches *number*, the subsequent routes are dropped.	An integer ranging from 1 to 100.
simply-alert	Indicates that when VPN routes exceed *number*, routes can still be added into the routing table, but the system prompts alarms. However, after the total number of VPN routes and network public routes reaches the unicast route limit specified in the License, the subsequent VPN routes are dropped.	-

Views

VPN instance view, VPN instance IPv4 address family view or VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many useless routes imported into a VPN instance constitute a large proportion of the routes on a device, run the **routing-table limit** command to set a limit on the maximum number of routes supported by the VPN instance. After the **routing-table limit** command is run in the current VPN instance address family, if the number of routes of the VPN instance reaches the set limit, the system will generate an alarm to instruct the user to check the validity of routes of the VPN instance.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.

 Copyright © Huawei Technologies Co., Ltd.

2. The **ipv4-family** command has been executed to enter the VPN instance IPv4 address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

Using the **routing-table limit** command prevents the routing table of the current VPN instance address family on a PE from importing too many routes, but cannot prevent the PE from importing excessive routes from other PEs. Therefore, configuring both the **routing-table limit** and **peer route-limit** commands is recommended.

Do not run both the **routing-table limit** (the command restricts the number of routes) and **prefix limit** (the command restricts the number of route prefixes) commands in the current VPN instance address family. Configure either one of them based on your need.

Follow-up Procedure

When the number of routes reaches the upper limit, run the **undo routing-table limit** command to allow the system to receive routes from routing tables of various protocols and to establish a private IP routing table.

If the remote cross routes learned using MP-IBGP and the BGP routes learned from CEs failed to be added to the routing table, the system automatically refreshes the routing table to add these routes.

Example

Configure the maximum number of routes for the IPv4 address family of the VPN instance named vpn1 to 1000, and when VPN routes exceed 1000, routes can still be added into the routing table, but the system prompts alarms.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn1-af-ipv4] routing-table limit 1000 simply-alert
```

Related Topics

9.8.134 peer route-limit

12.9.48 prefix limit

12.9.14 display ip vpn-instance

9.10.9 display ip routing-table limit

12.9.52 rr-filter

Function

The **rr-filter** command creates a reflection policy for the route reflectors.

The **undo rr-filter** command removes the configuration.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

By default, no reflection policy for a route reflectors is created.

Format

rr-filter { *extcomm-filter-number* | *extcomm-filter-name* }

undo rr-filter

Parameters

Parameter	Description	Value
extcomm-filter-number	specifies the number of the extended community filter supported by the route-reflector group. You can specify only one extended community filter each time.	It is an integer that ranges from 1 to 399.
extcomm-filter-name	specifies the name of the extended community filter supported by the route-reflector group. You can specify only one extended community filter each time.	The name is a string of 1 to 51 characters without any space. It is case-sensitive. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-VPNv4 address family view or BGP-MDT address family view

Default Level

2: Configuration level

Usage Guidelines

Full-mesh connections need to be established between IBGP peers in an AS to ensure the connectivity between the IBGP peers. When there are many IBGP peers, it is costly to establish a fully-meshed network. An RR or a confederation can be used to solve the problem. Only the IBGP route of which route-target extended community attribute meets the matching rules can be reflected. This allows load balancing among RRs.

Example

Create a route-reflector group, and enable the automatic filtering for VPNv4 route updates on the outbound interface. The group should be created on the basis of the permitted route target extended community attributes.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpnv4
[Huawei-bgp-af-vpnv4] rr-filter 10
```

12.9.53 service-id (VPN instance view)

Function

The **service-id** command sets a service ID for a VPN instance.

The **undo service-id** command deletes the service ID of a VPN instance.

By default, no service ID is set for a VPN instance.

Format

service-id *service-id*

undo service-id

Parameters

Parameter	Description	Value
service-id	Specifies the service ID of a VPN instance.	An integer ranging from 1 to 4294967295.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A service ID set in the view of a VPN instance identifies an L3VPN service, which facilitates later service query using the NMS.

A service ID is unique on a device. It distinguishes a VPN service from other VPN services on the network. A service ID used by a VPN instance cannot be allocated to other VPN instances.

Configuration Impact

If the **service-id** command is run repeatedly, the last configuration overrides the previous ones.

Example

Set a service ID for a VPN instance.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] service-id 123
```

12.9.54 snmp-agent trap enable feature-name l3vpn

Function

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for the L3VPN module.

The **undo snmp-agent trap enable feature-name l3vpn** command disables the trap function for the L3VPN module.

By default, the trap function for the L3VPN module is disabled.

Format

snmp-agent trap enable feature-name l3vpn [**trap-name** { **l3vpn_mib_trap_mid_thresh_exceed** | **l3vpn_mib_trap_thresh_cleared** | **l3vpn_mib_trap_thresh_exceed** | **l3vpn_mib_trap_tunnel_updown_event** | **l3vpn_mib_trap_vrf_down** | **l3vpn_mib_trap_vrf_up** }]

undo snmp-agent trap enable feature-name l3vpn [**trap-name** { **l3vpn_mib_trap_mid_thresh_exceed** | **l3vpn_mib_trap_thresh_cleared** | **l3vpn_mib_trap_thresh_exceed** | **l3vpn_mib_trap_tunnel_updown_event** | **l3vpn_mib_trap_vrf_down** | **l3vpn_mib_trap_vrf_up** }]

Parameters

Parameter	Description	Value
trap-name	Enables the traps of L3VPN events of specified types.	-
l3vpn_mib_trap_mid_thresh_exceed	Enables the trap of the event indicating that the number of private route prefixes exceeds the middle threshold which is set by the **prefix limit** command.	-
l3vpn_mib_trap_thresh_cleared	Enables the trap of the event indicating that the number of private route prefixes falls below the threshold which is set by the **prefix limit** command.	-
l3vpn_mib_trap_thresh_exceed	Enables the trap of the event indicating that the number of private route prefixes exceeds the upper limit which is set by the **prefix limit** command.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
l3vpn_mib_trap_tunnel_updown_event	Enables the trap of the event indicating that the status of the tunnel used by a VPN changed.	-
l3vpn_mib_trap_vrf_down	Enables the trap of VRF Down event.	-
l3vpn_mib_trap_vrf_up	Enables the trap of VRF Up event.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

The **snmp-agent trap enable feature-name l3vpn** command enables the trap function for L3VPN modules.

Precautions

To enable the trap function of one or more types of trap messages, specify **trap-name**.

Example

Enable the trap of VRF Down event in the system view.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_vrf_down
```

Disable the trap of VRF Down event in the system view.

```
<Huawei> system-view
[Huawei] undo snmp-agent trap enable feature-name l3vpn trap-name l3vpn_mib_trap_vrf_down
```

Related Topics

12.9.19 display snmp-agent trap feature-name l3vpn all

12.9.55 source

Function

The **source** command configures the source address or source interface of the tunnel.

The **undo source** command deletes the configured source address or source interface.

The source address and source interface of a tunnel are not specified by default.

Format

source { [**vpn-instance** *vpn-instance-name*] *source-ip-address* | *interface-type interface-number* }

undo source

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance that the source address of a tunnel belongs to. **NOTE** You can specify the parameter only when the encapsulation mode of a tunnel interface is set to IPSec or mGRE.	The value is the name of an existing VPN instance.
source-ip-address	Specifies the source address of a tunnel interface. If a tunnel interface works in IPv4-IPv6 mode, specify an IPv6 address as the source address of the tunnel interface.	The IPv4 address is in dotted decimal notation. The IPv6 address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
interface-type interface-number	Specifies the type and the number of the source interface of the tunnel.	-

Views

Tunnel interface view, Tunnel-Template interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring a tunnel, you must create a tunnel interface. After a tunnel interface is created, run the **source** command to specify the source IP address for the tunnel interface.

Prerequisites

A tunnel interface has been created using the **interface tunnel** command, and the encapsulation mode is set to GRE, IPSec, IPv4 over IPv6, or IPv6 over IPv4 of manual mode using the **tunnel-protocol** command.

Precautions

Two tunnel interfaces with the same encapsulation mode, source address, and destination address cannot be configured simultaneously.

IPv6 over IPv4, IPv4 over IPv6, and GRE tunnels are bidirectional tunnels. The source address of the local tunnel interface is the destination address of the remote tunnel interface by the **destination** command, and the destination address of the local tunnel interface is the source address of the remote tunnel interface.

Two or more tunnel interfaces that use the same encapsulation protocol cannot be configured with the same source and destination addresses. Two or more GRE tunnel interfaces in a system can have the same source address and same destination address. The system uses GRE keys to identify these GRE tunnel interfaces. When two or more tunnel interfaces on a P2MP tunnel are configured with the same source address, run the **gre key** command to set the key number of each tunnel interface.

You can also specify VPN instance parameters while specifying the source address for an IPSec tunnel or an mGRE tunnel in IPSec/mGRE over VPN scenarios.

Example

Set the tunnel type of Tunnel0/0/1 to IPv6 over IPv4 manual tunnel and configure the source IP address of Tunnel0/0/1 as 10.1.1.1.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] tunnel-protocol ipv6-ipv4
[Huawei-Tunnel0/0/1] source 10.1.1.1
```

Configure Tunnel0/0/2 of mGRE and use Loopback0 address as the interface address.

```
<Huawei> system-view
[Huawei] interface loopback 0
[Huawei-LoopBack0] ip address 10.2.1.1 32
[Huawei-LoopBack0] quit
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
[Huawei-Tunnel0/0/2] source loopback 0
```

 Copyright © Huawei Technologies Co., Ltd.

12.9.56 supernet label-route advertise

Function

The **supernet label-route advertise disable** command disables a BGP device from advertising BGP supernet labeled routes.

The **undo supernet label-route advertise disable** or **supernet label-route advertise enable** command restores the default configuration.

By default, BGP supernet labeled routes can be preferentially selected and advertised.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

supernet label-route advertise disable

supernet label-route advertise enable

undo supernet label-route advertise disable

Parameters

None

Views

BGP view, BGP-IPv4 unicast address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BGP supernet route has the same destination address and next hop address or has a more detailed destination address than the next hop address. Any route that meets one of the following conditions is a BGP supernet route.

- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are the same, and the destination address mask is greater than or equal to the next hop address mask.
- If you perform bitwise AND operations on the destination address mask with the destination address and next hop address, respectively, the calculated network addresses are different. However, if you perform bitwise AND operations on the next hop address mask with the destination address and next hop address, respectively, the calculated network addresses are the same.

 Copyright © Huawei Technologies Co., Ltd.

For example, the route destined for 10.6.6.6 in the following command output is a BGP supernet route.

```
<Huawei> display bgp routing-table
 BGP Local router ID is 10.1.1.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total Number of Routes: 1
      Network          NextHop       MED       LocPrf    PrefVal Path/Ogn
  *>i  10.6.6.6/32       10.6.6.6       0          100       0       ?
```

BGP supernet routes include BGP supernet labeled routes and BGP supernet unicast routes. In V2R3C00 or earlier, a BGP device does not advertise received BGP supernet labeled routes. After the BGP device is upgraded to a later version, the BGP device can advertise received BGP supernet labeled routes to other BGP peers. This advertisement may change the traffic path on the network before and after the upgrade. To ensure that the traffic path remains unchanged, run the **supernet label-route advertise disable** command to disable the BGP device from advertising BGP supernet labeled routes.

Example

Disable a BGP device from advertising BGP supernet labeled routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] supernet label-route advertise disable
```

12.9.57 traffic-statistics enable

Function

The **traffic-statistics enable** command enables traffic statistics for a VPN instance family.

The **undo traffic-statistics enable** command disables traffic statistics for a VPN instance family.

By default, traffic statistics is disabled for a VPN instance family.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

traffic-statistics enable

undo traffic-statistics enable

Parameters

None

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you want to collect statistics about the traffic received or sent by a VPN instance family as a basis for VPN traffic monitoring or accounting, run the **traffic-statistics enable** command to enable traffic statistics for the VPN instance family.

Follow-up Procedure

After running the **traffic-statistics enable** command, you can use the **display traffic-statistics vpn-instance** command to view statistics about the traffic of the VPN instance family.

The **reset traffic-statistics vpn-instance** command can be used to clear the collected traffic statistics.

Example

Enable traffic statistics for the family of a VPN instance named **vpna**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpna
[Huawei-vpn-instance-vpna] traffic-statistics enable
```

Related Topics

12.9.20 display traffic-statistics vpn-instance

12.9.49 reset traffic-statistics vpn-instance

12.9.58 tunnel binding

Function

The **tunnel binding** command binds a specified tunnel to the destination IP address. Therefore, the tunnel can be used by a specified VPN.

The **undo tunnel binding** command cancels the binding.

By default, a tunnel is not bound to any IP address.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel binding destination *dest-ip-address* **te** { **tunnel** *interface-number* } &<1-16> [**ignore-destination-check**] [**down-switch**]

undo tunnel binding destination *dest-ip-address*

Parameters

Parameter	Description	Value
dest-ip-address	Specifies the destination address of the tunnel.	-
interface-number	Specifies the interface number of the bound tunnel interface.	-
ignore-destination-check	Specifies whether to ignore destination consistency check. If this parameter is enabled, a tunnel policy selects a TE tunnel for route iteration even if the destination address of that TE tunnel is different from the destination address specified in the tunnel policy.	-
down-switch	Indicates that the tunnel switchover is enabled. After this parameter is configured, an available tunnel, with the priority as LSP, CR-LSP, and then GRE, is adopted when the bound TE tunnel fails.	-

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A tunnel policy determines the selection of proper tunnels for VPN services. There are two types of tunnel policies. Only one policy type can be configured in the tunnel policy view.

- Tunnel type prioritizing policy: Such a policy specifies the sequence in which different types of tunnels are selected. The **tunnel select-seq** command is used to configure a tunnel type prioritizing policy.
- Tunnel binding policy: Such a policy binds a tunnel to a VPN for service transmission. The **tunnel binding** command is used to configure a tunnel binding policy.

Only MPLS TE tunnels can be bound to VPNs. The **tunnel binding** command can specify the MPLS TE tunnels that are used for VPN binding, facilitating QoS deployment. If some VPN services have high requirements for QoS, run the **tunnel binding** command to use specific MPLS TE tunnels to transmit these VPN services.

Prerequisites

The **tunnel-policy** command is run to create a tunnel policy.

The **mpls te reserved-for-binding** command is run in the view of the tunnel interface to be bound to an MPLS TE tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The **tunnel binding** command can be run repeatedly in the tunnel policy view so long as the value of *dest-ip-address* varies.

Apply the tunnel binding policy to the VPN instance so that the VPN instance can have its routes iterated to the bound MPLS TE tunnel.

Example

Bind the IP address of the remote PE, 10.2.2.9, to the local tunnel interface Tunnel0/0/1 in the tunnel policy view.

```
<Huawei> system-view
[Huawei] tunnel-policy tnlpolicyname
[Huawei-tunnel-policy-tnlpolicyname] tunnel binding destination 10.2.2.9 te tunnel 0/0/1
```

Related Topics

12.9.40 mpls te reserved-for-binding

12.9.63 tunnel-policy (system view)

12.9.61 tunnel select-seq

12.9.59 tunnel-selector (system view)

Function

The **tunnel-selector** command creates a tunnel selector and displays the tunnel selector view.

The **undo tunnel-selector** command cancels the setting.

By default, no tunnel selector is created.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel-selector *tunnel-selector-name* { **permit** | **deny** } **node** *node*

undo tunnel-selector *tunnel-selector-name* [**node** *node*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel selector.	The value is a string of 1 to 40 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
permit	Specifies the matching mode of the tunnel selector to **permit**. If a route matches all the **if-match** clauses of a node, the route matches the node and all the actions defined by the **apply** clause are performed on the route. If a route does not match one **if-match** clause of a node, the route continues to match the next node.	-
deny	Specifies the matching mode of the tunnel selector to **deny**. If a route matches all the **if-match** clauses of a node, the route is denied and does not match the next node.	-
node *node*	Specifies the index of the node of the tunnel selector. The route first matches the node with a smaller index value.	The value is an integer ranging from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **tunnel-selector** command is often used in BGP/MPLS IP VPN networking. A tunnel selector needs to be created in the following scenarios:

- The ASBR in the VPN Option B networking needs to apply a tunnel policy to VPNv4 routes that are received from PEs although VPN instances are not configured on it.
- The SPE in the HoVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.

 Copyright © Huawei Technologies Co., Ltd.

- The PE in the VPN Option C networking needs to apply a tunnel policy to BGP labeled routes advertised to remote PEs.

Follow-up Procedure

Configure the following clauses after creating a tunnel selector (each node of the tunnel selector consists of two parts):

- **if-match** clause: sets filtering conditions on a node. To filter routes by RD, run the **if-match rd-filter** command. To filter routes by next hop, run the **if-match ip next-hop** command.
- **apply** clause: applies a tunnel policy to the routes filtered by the **if-match** clause using the **12.9.1 apply tunnel-policy (tunnel-selector view)** command.

In addition, the system will have routes iterated to expected tunnels only after applying a tunnel selector. The **12.9.60 tunnel-selector (BGP view)** command can be run in the BGP view for the application of a tunnel selector.

Precautions

A change in the tunnel selector may cause VPN services to be interrupted because BGP-VPNv4 or BGP labeled routes may fail to be iterated to tunnels.

Example

Create a tunnel selector named tps, and set the node number to 10 and the matching mode to **permit**.

```
<Huawei> system-view
[Huawei] tunnel-selector tps permit node 10
[Huawei-tunnel-selector]
```

Related Topics

12.9.25 display tunnel-selector

12.9.60 tunnel-selector (BGP view)

Function

The **tunnel-selector** command applies a tunnel selector to BGP-VPNv4 or BGP labeled routes.

The **undo tunnel-selector** command cancels the configuration.

By default, no tunnel selector is applied to BGP-VPNv4 or BGP labeled routes. BGP-VPNv4 or BGP labeled routes are only iterated to LSPs.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel-selector *tunnel-selector-name*

undo tunnel-selector

Parameters

Parameter	Description	Value
tunnel-selector-name	Specifies the name of a tunnel policy selector.	The value is a string of 1 to 40 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP view, BGP-IPv4 unicast address family view or BGP-VPNv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **tunnel-selector** command is often used in BGP/MPLS IP VPN networking. It can be used in the following scenarios to apply a tunnel selector to BGP-VPNv4 or BGP labeled routes:

- The ASBR in the VPN Option B networking needs to apply a tunnel policy to VPNv4 routes that are received from PEs although VPN instances are not configured on it.
- The SPE in the HVPN networking needs to apply a tunnel policy to VPNv4 routes that are received from UPEs.
- The PE in the VPN Option C networking needs to apply a tunnel policy to BGP labeled routes advertised to remote PEs.

Prerequisites

The **12.9.59 tunnel-selector (system view)** command is run to create a tunnel selector.

Precautions

Deleting the tunnel selector applied to BGP-VPNv4 or BGP labeled routes may cause VPN service interruption because the BGP-VPNv4 or BGP labeled routes may fail to be iterated to tunnels.

Example

Apply a tunnel selector to BGP labeled routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family unicast
[Huawei-bgp-af-ipv4] tunnel-selector tps
```

 Copyright © Huawei Technologies Co., Ltd.

12.9.61 tunnel select-seq

Function

The **tunnel select-seq** command specifies the priority sequence of the tunnels taking part in load balancing.

The **undo tunnel select-seq load-balance-number** command restores the default setting.

By default, only LDP LSPs, BGP LSP or static LSPs are selected and no load balancing is performed.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel select-seq { **gre** | **lsp** | **cr-lsp** } * **load-balance-number** *load-balance-number*

undo tunnel select-seq

Parameters

Parameter	Description	Value
gre	Specifies a GRE tunnel.	-
lsp	Specifies the LDP LSPs, BGP LSP or static LSPs.	-
cr-lsp	Specifies the CR-LSP tunnel.	-
load-balance-number	Specifies the number of tunnels taking part in load balancing.	• The value of this parameter can only range from 1 to 4 on the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204E, AR2204E-D, and AR2204. • The value of this parameter can only range from 1 to 8 on the AR2220, AR2220E, AR2240, AR2240C, AR3200, and AR3600 series.

Views

Tunnel policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VPN instance uses LSPs for service transmission on the backbone network. To use other types of tunnels or configure load balancing for service transmission of the VPN instance, you need to apply a tunnel policy to the VPN instance.

Precautions

A tunnel policy determines the selection of proper tunnels for VPN services. There are two types of tunnel policies.

- Tunnel type prioritizing policy: Such a policy specifies the sequence in which different types of tunnels are selected. The **tunnel select-seq** command is used to configure a tunnel type prioritizing policy.
- Tunnel binding policy: Such a policy binds a tunnel to a VPN for service transmission. The **tunnel binding** command is used to configure a tunnel binding policy.

If the **tunnel select-seq** command is run, the VPN instance preferably selects the tunnel type with the highest priority according to the specified sequence. For example, after the **tunnel select-seq cr-lsp lsp load-balance-number 2** command is run in the tunnel policy view, the VPN instance will select CR-LSPs to transmit services on the backbone network.

- If two or more CR-LSPs are available on the network, the VPN instance randomly selects two of them for service transmission.
- If no CR-LSP or only one CR-LSP is available on the network, the VPN instance selects LSPs as substitutes with the existing CR-LSP for service transmission.
- If the number of tunnels used by the VPN instance is reduced to 1, the VPN instance uses the tunnel policy to re-select tunnels.

If **lsp** is specified in the command, three types of LSPs can serve as candidate tunnels: LDP LSP, BGP LSP, and static LSP. The priority sequence of these LSPs taking part in load balancing is LDP LSP > BGP LSP > static LSP. For example, if the **tunnel select-seq lsp cr-lsp load-balance-number 3** command is configured for the tunnel policy:

- If three or more LDP LSPs are available on the network, the VPN instance randomly selects three of them for service transmission.
- If less than three LDP LSPs are available on the network, the VPN instance selects BGP LSPs as substitutes to ensure that three LSPs work in load balancing mode to transmit services.
- If the total number of LDP and BGP LSPs available on the network is less than 3, the VPN instance selects static LSPs as substitutes to ensure that three LSPs work in load balancing mode to transmit services.

After the **tunnel select-seq** command is executed, apply the configured tunnel policy to the VPN instance so that the VPN instance can select tunnels based on the tunnel policy and have its services load-balanced across tunnels.

Example

Configure a tunnel policy that only LDP LSPs, BGP LSP or static LSPs can be used. Set the number of tunnels taking part in load balancing to 2.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] tunnel-policy l2
[Huawei-tunnel-policy-l2] tunnel select-seq lsp load-balance-number 2
```

Related Topics

12.9.58 tunnel binding

12.9.63 tunnel-policy (system view)

12.9.62 tunnel-policy nonexistent-config-check

Function

The **tunnel-policy nonexistent-config-check** command configures whether a nonexistent tunnel policy can be specified in a command.

The **undo tunnel-policy nonexistent-config-check disable** command configures only an existing tunnel policy can be specified in a command.

By default, only an existing tunnel policy can be specified in a command.

Format

tunnel-policy nonexistent-config-check { **disable** | **enable** }

undo tunnel-policy nonexistent-config-check disable

Parameters

Parameter	Description	Value
disable	Indicates that a nonexistent tunnel policy can be specified in a command.	-
enable	Indicates that only an existing tunnel policy can be specified in a command.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, if you specify a nonexistent tunnel policy in a command, the command does not take effect.

If you need the nonexistent tunnel policy can be specified in a command, run the **tunnel-policy nonexistent-config-check disable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

# Indicates that a nonexistent tunnel policy can be specified in a command.

```
<Huawei> system-view
[Huawei] tunnel-policy nonexistent-config-check disable
```

12.9.63 tunnel-policy (system view)

Function

The **tunnel-policy** command creates a tunnel policy and displays the tunnel policy view.

The **undo tunnel-policy** command deletes the specified tunnel policy.

By default, no tunnel policy is created in the system.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tunnel-policy *policy-name*

undo tunnel-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Displays the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a VPN instance selects LSPs without performing load balancing based on the default tunnel policy. If you want to make a change, run the **tunnel-policy** command to create a tunnel policy.

There are two types of tunnel policies:

- Tunnel type prioritizing policy: It specifies the sequence in which different types of tunnels are selected and the number of tunnels taking part in load balancing.
- Tunnel binding policy: It binds a tunnel to a destination address. In this manner, the VPN traffic bound for the destination address enters the bound tunnel only, and as a result, QoS is guaranteed for the VPN traffic.

Precautions

If you change the tunnel policy in a VPN instance, VPN services may be interrupted due to a possibility of iteration failures.

Run one of the following commands to perform further configuration on the created tunnel policy:

- To configure the tunnel policy as a tunnel type prioritizing policy, run the **tunnel select-seq** command.
- To configure the tunnel policy as a tunnel binding policy, run the **tunnel binding** command.

The system can select tunnels for a VPN instance based on a tunnel policy only after the tunnel policy is applied to the VPN instance. The mode in which a tunnel policy is applied to a VPN instance varies according to the VPN type.

Example

Create a tunnel policy named policy1 and enter the tunnel policy view.

```
<Huawei> system-view
[Huawei] tunnel-policy policy1
[Huawei-tunnel-policy-policy1]
```

Related Topics

12.9.22 display tunnel-policy

12.9.58 tunnel binding

12.9.61 tunnel select-seq

12.9.64 tunnel-protocol

Function

The **tunnel-protocol** command configures the tunnel protocol on a tunnel interface.

The **undo tunnel-protocol** command restores the tunnel protocol to the default configuration.

By default, no tunnel protocol is used on a tunnel interface.

Format

tunnel-protocol { **gre** [**p2mp**] | **ipsec** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv4-ipv6** | **mpls te** | **svpn** [**p2p** | **p2mp**] | **none** }

undo tunnel-protocol

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
gre	Indicates that the GRE tunnel protocol is configured on a tunnel interface.	-
gre p2mp	Indicates that the mGRE tunnel protocol is configured on a tunnel interface. If this parameter is not used, the tunnel protocol configured on a tunnel interface is a traditional point-to-point GRE.	-
ipsec	Indicates that the IPSec tunnel protocol is configured on a tunnel interface.	-
ipv4-ipv6	Indicates that the IPv4 to IPv6 tunnel protocol is configured on a tunnel interface.	-
ipv6-ipv4	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses a manual IPv6 over IPv4 tunnel.	-
ipv6-ipv4 6to4	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using 6to4.	-
ipv6-ipv4 auto-tunnel	Configures the tunnel protocol of the tunnel interface as ipv6-ipv4 and uses an automatic IPv6 over IPv4 tunnel.	-
ipv6-ipv4 isatap	Indicates that the IPv6 to IPv4 tunnel protocol is configured on a tunnel interface using isatap.	-
mpls te	Indicates that the MPLS TE tunnel protocol is configured on a tunnel interface. **NOTE** The AR100&AR120&AR150&AR160&AR200 does not support this parameter.	-
svpn [**p2p** | **p2mp**]	Indicates that the SVPN tunnel protocol is configured on a tunnel interface. ● **p2p**: indicates the P2P SVPN tunnel protocol. ● **p2mp**: indicates the P2MP SVPN tunnel protocol.	-
none	Indicates that no tunnel protocol is configured on a tunnel interface.	-

Views

Tunnel interface view, Tunnel-Template interface view

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The tunnel template interface view supports the **ipsec** and **none** parameters only.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a tunnel interface using the **interface tunnel** command, run the **tunnel-protocol** command to configure the tunnel encapsulation mode for the tunnel interface.

The following tunnel encapsulation modes are available:

- GRE: encapsulates packets of some network layer protocols such as IP or IPX to enable these encapsulated packets to be transmitted on networks running other protocols such as IP. When the **p2mp** parameter is specified following **gre**, you can set the tunnel encapsulation mode to P2MP GRE. The destination address of a P2MP GRE tunnel does not need to be manually configured. Instead, the destination address of this tunnel can either be defined by a protocol (for example, NHRP in a DSVPN scenario) or be dynamically learned.
- IPSec: protects the security of data transmitted on the Internet by establishing tunnels using the IPSec protocol.
- IPv4-IPv6: creates tunnels on the IPv6 networks to connect IPv4 isolated sites so that IPv4 isolated sites can access other IPv4 networks through the IPv6 public network.
- IPv6-IPv4: creates tunnels on the IPv4 networks to connect IPv6 isolated sites so that IPv6 packets can be transmitted on IPv4 networks.
- MPLS TE: integrates the MPLS technology with traffic engineering. It can reserve resources by setting up LSP tunnels for a specified path in an attempt to avoid network congestion and balance network traffic.
- SVPN: binds multiple WAN access lines to provide high bandwidth and highly reliable networks for customers.
  - When the SVPN mode is set to Hub-Spoke, specify **p2p** on the Spoke and **p2mp** on the hub when configuring a tunnel protocol.
  - When the SVPN mode is set to Lone Ranger, you must not specify **p2p** or **p2mp**.

Precautions

- The **none** mode indicates the initial configuration, that is, no tunnel encapsulation mode is configured. In practice, you must select another tunnel encapsulation mode.
- You must configure the tunnel encapsulation mode before setting the source IP address or other parameters for a tunnel interface. Changing the encapsulation mode of a tunnel interface deletes other parameters of the tunnel interface. When an SVPN proposal is bound to a tunnel interface, you cannot modify the tunnel encapsulation mode.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the tunnel encapsulation mode of Tunnel0/0/2 to mGRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre p2mp
```

Set the tunnel encapsulation mode of Tunnel0/0/2 to GRE.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/2
[Huawei-Tunnel0/0/2] tunnel-protocol gre
```

Related Topics

12.9.32 interface tunnel

12.9.65 tnl-policy

Function

The **tnl-policy** command associates a tunnel policy with the current VPN instance address family.

The **undo tnl-policy** command dissociates the current VPN instance address family from a tunnel policy.

By default, no tunnel policy is associated with the VPN instance address family. By default, a tunnel is selected for a VPN in the sequence of the LSP, CR-LSP, and Local_IfNet, and no load balancing is performed.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the tunnel policy to be associated with the VPN instance address family.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, a device only uses an LSP tunnel to forward data on the backbone network and cannot implement multi-path load balancing at the same time. To ensure transmission quality of services and specify a TE tunnel to transmit VPN services, or to improve transmission efficiency and implement load balancing, run the **tunnel-policy** command to configure a tunnel policy and run the **tnl-policy** command to reference the tunnel policy in the VPN address family view.

Prerequisites

1. The **ip vpn-instance** command has been executed to create a VPN instance and enter the VPN instance view.
2. The **ipv4-family** command has been executed to create a VPN instance and enter the VPN instance IPv4 address family view.
3. The **route distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

If the tunnel policy associated with a VPN instance enabled with the address family cannot match an existing tunnel on the network, the routes in the VPN instance enabled with the address family will have routes iterated to tunnels based on the default tunnel policy. If the iteration fails, services will be interrupted.

If the address family of a VPN instance changes or the associated tunnel policy is deleted, VPN services will be interrupted for a short time even if tunnels matching the tunnel policy are available on the network. Therefore, use the **tnl-policy** command with caution.

Follow-up Procedure

If the associated tunnel policy does not exist, run the **tunnel-policy** command to create the tunnel policy.

Example

Associate a tunnel policy named **po1** with the VPN instance named *vpn2*.

```
<Huawei> system-view
[Huawei] tunnel-policy po1
[Huawei-tunnel-policy-po1] tunnel select-seq lsp load-balance-number 2
[Huawei-tunnel-policy-po1] quit
[Huawei] ip vpn-instance vpn2
[Huawei-vpn-instance-vpn2] ipv4-family
[Huawei-vpn-instance-vpn2-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn2-af-ipv4] tnl-policy po1
```

Related Topics

12.9.63 tunnel-policy (system view)

12.9.14 display ip vpn-instance

12.9.66 transit-vpn

Function

The **transit-vpn** command ensures that the status of a VRF (VPN Routing and Forwarding table) obtained from MIB is always Up, no matter whether this VRF is bound to interfaces.

The **undo transit-vpn** command restores the default setting.

By default, the status of a VRF obtained from MIB is Up only if it is bound to at least one interface in the Up state.

Format

transit-vpn

undo transit-vpn

Parameters

None.

Views

VPN instance view or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The status of a VRF obtained from MIB is Up only if it is bound to at least one interface in the Up state. In the HoVPN networking, however, a VRF does not need to be bound to any interface. If the VRF is not bound to an interface in this networking, the status of the VRF obtained from MIB is Down by default.

In this case, you can run the **transit-vpn** command to ensure that the status of a VRF obtained from MIB is always Up.

Prerequisites

The **route-distinguisher** command has been executed to set the RD of the VPN instance.

Example

Configure the status of the VRF vpna obtained from MIB to be always Up, no matter whether the VRF is bound to interfaces.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpna
```

```
[Huawei-vpn-instance-vpna] ipv4-family
[Huawei-vpn-instance-vpna-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpna-af-ipv4] transit-vpn
```

12.9.67 undo vpn frr all

Function

Using the **undo vpn frr all** command, you can disable VPN FRR in all the VPN instances.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

undo vpn frr all

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When running the **undo vpn frr all** command in the system view, you can disable VPN FRR in all the VPN instances.

Example

Disable VPN FRR of all the VPN instances in the system view.

```
<Huawei> system-view
[Huawei] undo vpn frr all
```

Related Topics

12.9.70 vpn frr

12.9.68 vpn-route cross multipath

Function

The **vpn-route cross multipath** command adds multiple VPNv4 routes to a VPN instance with a different RD from these routes' RDs.

The **undo vpn-route cross multipath** command restores the default configuration.

By default, if the RDs of multiple VPNv4 routes are different from the RD of a VPN instance, only the optimal route is added to the VPN instance.

Format

vpn-route cross multipath

undo vpn-route cross multipath

Parameters

None

Views

BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, if the RD of the VPN instance on the local PE is different from the RDs of the VPN instances on multiple remote PEs, and the RDs of the VPN instances on remote PEs are the same, the local PE adds only the optimal route to the VPN instance after receiving VPNv4 routes with the same destination address from the remote PEs. As a result, load balancing or VPN FRR does not take effect. To resolve this problem, run the **vpn-route cross multipath** command on the local PE.

Configuration Impact

After you run the **vpn-route cross multipath** command, the local PE adds multiple VPNv4 routes to a VPN instance with a different RD from these routes' RDs. The number of VPNv4 routes that can be added to the VPN instance depends on whether load balancing or VPN FRR is configured.

- If no load balancing is configured, a maximum of two VPNv4 routes can be added to the VPN instance.
- If you set the maximum number of equal-cost routes for load balancing to *n* using the **maximum load-balancing** command, *n* VPNv4 routes can be added to the VPN instance.

Example

Add multiple VPNv4 routes to a VPN instance with a different RD from these routes' RDs.

```
<Huawei> system-view
[Huawei] bgp 100
```

```
[Huawei-bgp] ipv4-family vpn-instance vrf1
[Huawei-bgp-vrf1] vpn-route cross multipath
```

12.9.69 vpn-target

Function

The **vpn-target** command configures the export or import VPN target extended community attribute for the VPN instance address family.

The **undo vpn-target** command deletes the setting.

By default, no export or import VPN target extended community list is configured for the VPN instance address family.

Format

vpn-target *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-target	Specifies the VPN target extended community attribute to be added to the VPN target extended community list of the VPN instance address family. The forms of VPN targets are as follows: ● 2-byte AS number: 4-byte user-defined number, for example, 1:3. The AS number ranges from 0 to 65535. The user-defined number ranges from 0 to 4294967295. The AS number and the user-defined number cannot both be 0. That is, a VPN target cannot be 0:0. ● IPv4-address: 2-byte user-defined number, for example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255. The user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that range from 0 to 65535 and from 0 to 65535, respectively. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, a VPN target cannot be 0.0:0.	-
both	Adds the VPN target extended community attribute to the export and import VPN target extended community lists of the VPN instance address family. If none of **both**, **export-extcommunity**, or **import-extcommunity** is specified, **both** is adopted by default.	-
export-extcommunity	Adds the VPN target extended community attribute to the export VPN target extended community lists of the VPN instance address family.	-
import-extcommunity	Adds the VPN target extended community attribute to the import VPN target extended community lists of the VPN instance address family.	-
all	Delete all the VPN targets of the VPN instance IPv4 address family.	-

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a VPN instance is configured on a PE, the **vpn-target** command must be used to configure a VPN target for the IPv4 or IPv6 address family of the VPN instance.

The VPN target controls route learning between VPN sites. A VPN target may be either an import VPN target or an export VPN target. An export VPN target is contained in a VPNv4 route to be advertised to a remote MP-BGP peer. After receiving a VPNv4 or IPv6 route, an MP-BGP peer compares the received export VPN target with the local import VPN target to determine whether the VPNv4 route can be added to the routing table of the local VPN instance enabled with the IPv4 or IPv6 address family.

Prerequisites

The **12.9.50 route-distinguisher** command has been executed to set the RD of the VPN instance.

Precautions

A VPN target configured using the **vpn-target** command will not overwrite any previously configured VPN target. If the number of configured VPN targets has reached the maximum limit, no VPN target can be added by using the **vpn-target** command.

After a VPN target is configured for the IPv4 or IPv6 address family of a VPN instance, only the routes that match the VPN target will be accepted by the IPv4 or IPv6 address family of the VPN instance.

If all the VPN targets of the IPv4 or IPv6 address family of a VPN instance are deleted using the **undo vpn-target** command, all routes learned by the IPv4 or IPv6 address family of the VPN instance from other VPN instances will be deleted.

Multiple VPN targets can be configured for the IPv4 or IPv6 address family of a VPN instance. One **vpn-target** command can configure a maximum of eight VPN targets at a time. If you want to configure more VPN targets in the VPN instance IPv4 or IPv6 address family view, run the **vpn-target** command multiple times. When VPN routes are advertised between VPN instances, if one of the VPN targets carried in the VPNv4 or IPv6 routes matches the import VPN target of the IPv4 or IPv6 address family of a local VPN instance, the routes will be added to the routing table of the local VPN instance.

Example

Add 3:3 to the export VPN target extended community list and 4:4 to the import VPN target extended community list of the VPN instance named *vrf1*.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] vpn-target 3:3 export-extcommunity
[Huawei-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.9.14 display ip vpn-instance

12.9.70 vpn frr

Function

Using the **vpn frr** command, you can enable VPN FRR.

Using the **undo vpn frr** command, you can disable VPN FRR.

By default, VPN FRR is disabled.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

vpn frr route-policy *route-policy-name*

undo vpn frr

Parameters

Parameter	Description	Value
route-policy *route-policy-name*	Specifies the name of the route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view, VPN instance IPv4 address family view, VPN instance IPv6 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a PE is connected to two other PEs, running the **vpn frr** command in the VPN instance address family view of the PE enables VPN FRR and improves network reliability. After VPN FRR is configured, traffic can switch to the secondary LSP immediately after the primary LSP becomes faulty.

The **undo vpn frr all** command is run in the system view, and the **undo vpn frr** command is run in the VPN instance view.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When running the **undo vpn frr all** command in the system view, you can disable VPN FRR in all the VPN instances.

Prerequisites

The **12.9.50 route-distinguisher** command has been executed to set the RD of the VPN instance.

Example

Specify the IP address of the backup next hop in the route-policy named **vpn_frr_rp**, and enable VPN FRR in the VPN instance view.

```
<Huawei> system-view
[Huawei] route-policy vpn_frr_rp permit node 10
[Huawei-route-policy] apply backup-nexthop 2.2.2.9
[Huawei-route-policy] quit
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vpn1-af-ipv4] vpn frr route-policy vpn_frr_rp
[Huawei-vpn-instance-vpn1-af-ipv4] quit
```

Related Topics

12.9.67 undo vpn frr all

12.10 EVPN Configuration Commands

NOTE

Only the AR100, AR120, AR150, AR160 (except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L), AR200, AR1200series, AR2220E support EVPN.

12.10.1 advertise l2vpn evpn

Function

The **advertise l2vpn evpn** command enables a VPN instance to advertise IP routes to a BGP EVPN address family.

The **undo advertise l2vpn evpn** command restores the default configuration.

By default, a VPN instance is disabled from advertising IP routes to a BGP EVPN address family.

Format

advertise l2vpn evpn

undo advertise l2vpn evpn

Parameters

None

Views

BGP-VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

If IP prefix routes are used to establish tunnels between VXLAN tunnel endpoints (VTEPs) and advertise host routes, run the **advertise l2vpn evpn** command in the BGP-VPN instance IPv4 address family view to enable a VPN instance to advertise IP routes to the BGP EVPN address family. This configuration allows the host routes collected by the VPN instance to be sent to the BGP EVPN address family and then sent to the remote VTEPs through EVPN BGP peer relationships.

Example

Enable a VPN instance named **vpna** to advertise IP routes to the BGP EVPN address family.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] ipv4-family vpn-instance vpna
[Huawei-bgp-vpna] advertise l2vpn evpn
```

12.10.2 display bgp evpn routing-table

Function

The **display bgp evpn routing-table** command displays information about EVPN routes.

Format

display bgp evpn all routing-table [**statistics**]

display bgp evpn { **all** | **route-distinguisher** *route-distinguisher* } **routing-table** { **inclusive-route** [*inclusive-route*] | **mac-route** [*mac-route*] | **prefix-route** [*prefix-route*] }

Parameters

Parameter	Description	Value
all	Displays information about EVPN routes of all EVPN instances.	-
statistics	Displays statistics about EVPN routes.	-

Parameter	Description	Value
route-distinguisher *route-distinguisher*	Displays information about EVPN routes with a specified route distinguisher (RD).	RD has the following four formats: ● 16-bit AS number:32-bit user-defined number. For example, 101:3. The AS number is an integer ranging from 0 to 65535, and the user-defined number is an integer ranging from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295, and a user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that both range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, an RD cannot be 0.0:0. ● 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535.
inclusive-route	Displays information about inclusive multicast routes.	-
inclusive-route	Specifies an inclusive multicast route.	The value is in the format of M:L:X.X.X.X, where: ● M is fixed at 0. ● X.X.X.X indicates the source address configured for the device originating the route. ● L indicates the mask length of the source address configured for the device originating the route.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-route	Displays information about MAC advertisement routes.	-
mac-route	Specifies a MAC advertisement route.	The value is in the format of E:M:H-H-H:L:X.X.X.X, where: ● E indicates the ID of the VLAN to which the MAC address belongs. ● M is fixed at 48, indicating the length of the MAC address. ● H-H-H indicates the MAC address. Each H represents a 4-bit hexadecimal number. The system prefixes the number with zeros if fewer than four bits are entered. For example, if you enter e0, 00e0 is displayed. ● L is fixed at 32, indicating the mask length of the IP address corresponding to the MAC address. ● X.X.X.X indicates the IP address corresponding to the MAC address.
prefix-route	Displays information about IP prefix routes.	-
prefix-route	Specifies an IP prefix route.	The value is in the format of L:X.X.X.X:M, where: ● L is fixed at 0. ● X.X.X.X indicates the IP address of host routes. ● M indicates the mask length of host routes.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Information about specified EVPN routes can be displayed by specifying different parameters.

Example

Display information about all EVPN routes.

```
<Huawei> display bgp evpn all routing-table
Local AS number :100

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete


 EVPN address family:
 Number of Mac Routes : 2
 Route Distinguisher: 1:1


        Network(EthTagId/MacAddrLen/MacAddr/IpAddrLen/IpAddr)   NextHop
 *>      0:48:a4dc-be0f-99a6:0:0.0.0.0                          9.9.9.9
 *>      0:48:a4dc-be0f-99a6:32:9.9.9.9                          9.9.9.9

 VPN-Instance vpn1, Router ID 1.1.1.1:

 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

   i  9.9.9.9/32         9.9.9.9                   100        0      ?

 EVPN address family:
 Number of Inclusive Multicast Routes : 1
 Route Distinguisher: 1:1


        Network(EthTagId/IpAddrLen/OriginalIp)                 NextHop
 *>      0:32:9.9.9.9                                       9.9.9.9

 EVPN address family:
 Number of Ip Prefix Routes : 1
 Route Distinguisher: 1:1


        Network(EthTagId/IpPrefix/IpPrefixLen)                 NextHop
 *>      0:9.9.9.0:24                                       9.9.9.9

 VPN-Instance vpn1, Router ID 1.1.1.1:

 Total Number of Routes: 1
      Network            NextHop        MED        LocPrf    PrefVal Path/Ogn

   i  9.9.9.0/24         9.9.9.9         0          100        0        ?
```

Table 12-105 Description of the **display bgp evpn all routing-table** command output

Item	Description
Local AS number	Local AS number of the EVPN routes
BGP Local router ID	Router ID of the local BGP device
Number of Mac Routes	Number of MAC advertisement routes
Route Distinguisher	RD of the EVPN routes

Item	Description
Network	Reachable address
NextHop	Next hop address
VPN-Instance	VPN instance name
Router ID	ID of a router
Total Number of Routes	Total number of EVPN routes
MED	Metric of the EVPN routes
LocPrf	Local preference of the EVPN routes
PrefVal	Preferred value of a routing protocol
Path/Ogn	Path and Origin attributes of the AS of the EVPN routes
Number of Inclusive Multicast Routes	Number of inclusive multicast routes
Number of Ip Prefix Routes	Number of IP prefix routes

12.10.3 display bgp evpn update-peer-group

Function

The **display bgp evpn update-peer-group** command displays information about BGP update peer-groups in the EVPN address family.

Format

display bgp evpn update-peer-group [**index** *update-peer-group-index*]

Parameters

Parameter	Description	Value
index *update-peer-group-index*	Specifies the index of a BGP update peer-group.	The value is an integer.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When a VXLAN network is deployed using BGP EVPN, to view information about the update peer-group with a specified index in the EVPN address family, run the **display bgp evpn update-peer-group** command.

Example

Display information about all BGP update peer-groups in the EVPN address family.

```
<Huawei> display bgp evpn update-peer-group

  The EVPN instance's update peer group number : 1
  Keep buffer update peer group number : 0
  BGP Version : 4

  Group ID : 0
  Group Type : internal
  Addr Family : L2-EVPN
  AdvMinTimeVal : 0
  Total Peers : 2
  Leader Peer : 5.5.5.5
  Peers List : 5.5.5.5          4.4.4.4
```

Display information about the BGP update peer-group with the index 0 in the EVPN address family.

```
<Huawei> display bgp evpn update-peer-group index 0

  Group ID : 0
  BGP Version : 4
  Group Type : internal
  Addr Family : L2-EVPN
  AdvMinTimeVal : 0
  Total Peers : 1
  Leader Peer : 1.1.1.1

  Total format packet number : 85
  Total send packet number : 85
  Total replicate packet number : 0
  The replication percentages(%) : 0

  Peers List : 1.1.1.1
```

Table 12-106 Description of the **display bgp evpn update-peer-group** command output

Item	Description
The EVPN instance's update peer group number	Number of update peer-groups in the EVPN instance
Keep buffer update peer group number	Number of update peer-groups stored in the buffer
BGP Version	BGP version
Group ID	ID of the BGP update peer-group

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Group Type	Type of a BGP update peer-group: ● external: EBGP update peer-group ● internal: IBGP update peer-group ● external-confed: EBGP update peer-group in the confederation ● internal-confed: IBGP update peer-group in the confederation ● unknown: unknown update peer-group
Addr Family	Address family
AdvMinTimeVal	Minimum interval at which Update messages with the same route prefix are sent, in seconds
Total Peers	Total number of BGP peers in the update peer-group
Leader Peer	Leader peer in the update peer-group
Total format packet number	Number of Update messages of a single peer sends in the update peer-group
Total send packet number	Number of Update messages sent to all BGP peers in the update peer-group
Total replicate packet number	Absolute value of the difference between Total send packet number and Total format packet number, that is, absolute value of the difference between the number of Update messages that are sent to all peers in the update peer-group and the number of Update messages sent to a single peer in the update peer-group
The replication percentages(%)	Percentage of the number of replicated Update messages to the total number of sent Update messages, that is, (Total send packet number – Total format packet number)/Total send packet number
Peers List	BGP peer list, displaying the IP addresses of all peers in the update peer-group

 Copyright © Huawei Technologies Co., Ltd.

12.10.4 export route-policy evpn

Function

The **export route-policy evpn** command associates the VPN instance IPv4 address family with an export route-policy to filter the EVPN routes that the VPN instance IPv4 address family advertises to the EVPN address family.

The **undo export route-policy evpn** command dissociates the VPN instance IPv4 address family from an export route-policy.

By default, the VPN instance IPv4 address family is not associated with any export route-policy.

Format

export route-policy *policy-name* **evpn**

undo export route-policy *policy-name* **evpn**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the export route-policy with which the VPN instance IPv4 address family is associated.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VPN instance view or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the VPN instance IPv4 address family adds all EVPN-VPN targets in the export EVPN-VPN target list to routes when advertising the routes to the EVPN address family. To control route advertisement more precisely, run the **export route-policy** *policy-name* **evpn** command to associate the VPN instance IPv4 address family with an export route-policy and set attributes for eligible routes.

Prerequisites

An RD has been configured for the VPN instance IPv4 address family using the **route-distinguisher** *route-distinguisher* command.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

The VPN instance IPv4 address family can be associated with only one export route-policy. If the **export route-policy evpn** command is run more than once, the latest configuration overrides the previous one.

Configuration of the **export route-policy evpn** command does not affect the export route-policy applied to a VPN instance using the **export route-policy** *policy-name* command.

Precautions

If the route-policy with which the VPN instance IPv4 address family is associated does not exist, run the **route-policy** command to configure the route-policy.

Example

Associate a VPN instance named **vrf1** with an export route-policy named **policy-2** to filter EVPN routes that the VPN instance IPv4 address family advertises to other VPN instances.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] export route-policy policy-2 evpn
```

12.10.5 import route-policy evpn

Function

The **import route-policy evpn** command associates the VPN instance IPv4 address family with an import route-policy that is used to filter the EVPN routes imported from the EVPN address family.

The **undo import route-policy evpn** command dissociates the VPN instance IPv4 address family from an import route-policy.

By default, the VPN instance IPv4 address family is not associated with any import route-policy.

Format

import route-policy *policy-name* **evpn**

undo import route-policy *policy-name* **evpn**

Parameters

Parameter	Description	Value
policy-name	Specifies the name of the import route-policy with which the VPN instance IPv4 address family is associated.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Views

VPN instance view or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the VPN instance IPv4 address family matches the export EVPN-VPN targets of received routes against its import EVPN-VPN targets to determine whether to import these routes. To control route import more precisely, run the **import route-policy** *policy-name* **evpn** command to associate the VPN instance IPv4 address family with an import route-policy and set attributes for eligible routes.

Prerequisites

An RD has been configured for the VPN instance IPv4 address family using the **route-distinguisher** *route-distinguisher* command.

Configuration Impact

The VPN instance IPv4 address family can be associated with only one import route-policy. If the **import route-policy evpn** command is run more than once, the latest configuration overrides the previous one.

Configuration of the **import route-policy evpn** command does not affect the import route-policy applied to a VPN instance using the **import route-policy** *policy-name* command.

Precautions

If the route-policy with which the VPN instance IPv4 address family is associated does not exist, run the **route-policy** command to configure the route-policy.

Example

Associate a VPN instance named **vrf1** with an import route-policy named **policy-1** to filter EVPN routes imported from other VPN instances to the VPN instance IPv4 address family.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] import route-policy policy-1 evpn
```

12.10.6 peer advertise

Function

The **peer advertise** command enables a device to advertise ARP or IRB routes to a BGP EVPN peer.

 Copyright © Huawei Technologies Co., Ltd.

The **undo peer advertise** command restores the default configuration.

By default, a device does not advertise ARP or IRB routes to a BGP EVPN peer.

Format

peer { *ipv4-address* | *group-name* } **advertise** { **arp** | **irb** }

undo peer { *ipv4-address* | *group-name* } **advertise** { **arp** | **irb** }

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP peer.	The value is in dotted decimal notation.
group-name	Specifies the name of a peer group.	The value is a string of 1 to 47 case-sensitive characters, spaces not supported.
arp	Advertises ARP routes.	-
irb	Advertises IRB routes.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable a device to advertise ARP or IRB routes to a BGP EVPN peer, run the **peer advertise** command. Advertising ARP or IRB routes allows a VXLAN tunnel to be established between VTEPs and suppresses ARP flooding on the network. Advertising IRB routes additionally allows the advertisement of host routes between the VTEPs.

Precautions

The **arp** and **irb** parameters are mutually exclusive in the BGP-EVPN address family view.

Example

Enable a device to advertise ARP routes to a BGP EVPN peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 1.1.1.1 advertise arp
```

 Copyright © Huawei Technologies Co., Ltd.

12.10.7 peer advertise route-reoriginated

Function

The **peer advertise route-reoriginated** command enables a device to advertise IP prefix routes re-encapsulated by the EVPN address family to a BGP EVPN peer.

The **undo peer advertise route-reoriginated** command restores the default configuration.

By default, the local device does not advertise IP prefix routes re-encapsulated by the EVPN address family to a BGP EVPN peer.

Format

peer { *ipv4-address* | *group-name* } **advertise route-reoriginated evpn ip**

undo peer { *ipv4-address* | *group-name* } **advertise route-reoriginated evpn ip**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP EVPN peer.	The value is in dotted decimal notation.
group-name	Specifies the name of a BGP EVPN peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
evpn	Re-encapsulates the received EVPN routes.	-
ip	Re-encapsulates the IP prefix routes in the received EVPN routes.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Task Name and Operations

Task Name	Operations
bgp	write

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In three-segment VXLAN scenarios, to re-encapsulate EVPN routes received from a DC into IP prefix routes and then send them to the BGP EVPN peer in another DC, run the **peer advertise route-reoriginated** command. This configuration allows communication between VMs in different DCs.

During EVPN route re-encapsulation, a border leaf node receives an EVPN route from a DC and changes the route next hop to the VTEP address of the leaf node. Additionally, the leaf node replaces the source MAC address in the gateway MAC attribute of the host route with its own MAC address and the L3VNI with that of an L3VPN instance.

Prerequisites

The device has been enabled to add a regeneration flag to the routes received from BGP EVPN peers using the **peer** { *ipv4-address* | *group-name* } **import reoriginate** command.

Example

Enable a device to advertise regenerated IP prefix routes to a BGP EVPN peer.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 2.2.2.2 as-number 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 2.2.2.2 enable
[Huawei-bgp-af-evpn] peer 2.2.2.2 import reoriginate
[Huawei-bgp-af-evpn] peer 2.2.2.2 advertise route-reoriginated evpn ip
```

12.10.8 peer import reoriginate

Function

The **peer import reoriginate** command enables a device to add a regeneration flag to the routes received from BGP EVPN peers.

The **undo peer import reoriginate** command restores the default configuration.

By default, a device does not add a regeneration flag to the routes received from BGP EVPN peers.

Format

peer { *ipv4-address* | *group-name* } **import reoriginate**

undo peer { *ipv4-address* | *group-name* } **import reoriginate**

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a BGP EVPN peer.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group-name	Specifies the name of a BGP EVPN peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Task Name and Operations

Task Name	Operations
bgp	write

Usage Guidelines

Usage Scenario

In a three-segment VXLAN scenario, an edge node that connects to a carrier network does not re-encapsulate the routes received from BGP EVPN peers, causing the EVPN routes to be terminated on the edge node. As a result, the EVPN routes from one DC cannot be advertised to the BGP EVPN peers of another DC. To address this problem, run the **peer import reoriginate** command to enable the edge node to add a regeneration flag to the routes received from BGP EVPN peers. The edge node then re-encapsulates the EVPN routes received from one DC before sending them to another DC for inter-DC VM communication.

Prerequisites

A device has been enabled to exchange routes with a specified peer or peer group using the **peer** { *group-name* | *ipv4-address* } **enable** command.

Example

Enable a device to add a regeneration flag to the routes received from BGP EVPN peers.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.1 as-number 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 1.1.1.1 enable
[Huawei-bgp-af-evpn] peer 1.1.1.1 import reoriginate
```

 Copyright © Huawei Technologies Co., Ltd.

12.10.9 l2vpn-family evpn

Function

The **l2vpn-family evpn** command enables the BGP-EVPN address family and displays the BGP-EVPN address family view.

The **undo l2vpn-family evpn** command deletes the BGP-EVPN address family view.

By default, the BGP-EVPN address family is disabled, and the BGP-EVPN address family is not displayed.

NOTE

Only AR121, AR129, AR129CV, AR129CVW, AR129CGVW-L, AR160 series (except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L, AR161W, AR169W, and AR169CGVW-L), AR200 series, AR1220E, AR1220EV, AR1220EVW, AR1220F, and AR2220E support this command.

Format

l2vpn-family evpn

undo l2vpn-family evpn

Parameters

None

Views

BGP view

Default Level

2: Configuration level

Usage Guidelines

Before you perform configurations in the BGP-EVPN address family view, run the **l2vpn-family evpn** command to enable the BGP-EVPN address family and display the BGP-EVPN address family view.

Example

Enable the BGP-EVPN address family and display the BGP-EVPN address family view.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn]
```

Related Topics

9.8.12 bgp

 Copyright © Huawei Technologies Co., Ltd.

12.10.10 peer mac-limit

Function

The **peer mac-limit** command configures the maximum number of MAC advertisement routes allowed to be received from a peer.

The **undo peer mac-limit** command restores the default configuration.

By default, the number of MAC advertisement routes allowed to be received from a peer is not limited.

Format

peer { *group-name* | *ipv4-address* } **mac-limit** *mac-limit* [**idle-forever** | **idle-timeout** *times*]

undo peer { *group-name* | *ipv4-address* } **mac-limit**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of a peer.	The value is in dotted decimal notation.
mac-limit	Specifies the maximum number of MAC advertisement routes allowed to be received from each peer.	-
idle-forever	Indicates that a connection that is interrupted after the maximum number of routes allowed have been received cannot be automatically re-established.	-
idle-timeout *times*	Specifies a timer for re-establishing a connection if the connection is interrupted after the maximum number of routes allowed have been received. Before the timer expires, the system does not re-establish a connection.	The value is an integer ranging from 1 to 1200, in minutes.

Views

BGP-EVPN address family view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an EVPN instance imports many invalid MAC advertisement routes from peers and these routes occupy a large proportion of the total number of MAC advertisement routes, run the **peer mac-limit** command to configure the maximum number of MAC advertisement routes allowed to be received from each peer.

Configuration Impact

After this command is run, excess route prefixes of the BGP-EVPN address family may be discarded.

If the **undo peer mac-limit** command is run after the number of received MAC advertisement routes exceeds the specified maximum number, the system receives route prefixes from PEs again to construct the EVPN BGP routing table.

Example

Set the maximum number of MAC advertisement routes allowed to be received from the peer 2.2.2.2 to 1000.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 2.2.2.2 mac-limit 1000
```

12.10.11 peer route-policy (BGP-EVPN address family view)

Function

route-policy

The **undo peer route-policy** deletes a specified route-policy.

By default, no route-policy is specified to filter routes received from an EVPN BGP peer or peer group or routes to be advertised to an EVPN BGP peer or peer group.

Format

peer { *group-name* | *ipv4-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* } **route-policy** *route-policy-name* { **import** | **export** }

Parameters

Parameter	Description	Value
group-name	Specifies the name of an EVPN BGP peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ipv4-address	Specifies the IPv4 address of an EVPN BGP peer.	The value is in dotted decimal notation.
route-policy-name	Specifies the name of a route-policy.	The name is a string of 1 to 40 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
import	Applies a route-policy to routes received from an EVPN BGP peer or peer group.	-
export	Applies a route-policy to routes advertised to an EVPN BGP peer or peer group.	-

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a route-policy is created, you can run the **peer route-policy** command to apply the route-policy to an EVPN BGP peer or peer group so that the routes advertised to or received from the peer or peer group can be controlled. To be specific, only the necessary routes are advertised to or received from the peer or peer group. This configuration streamlines route management, reduces the routing table scale, and minimizes network resource consumption.

Prerequisites

EVPN BGP peers or peer groups have been enabled to exchange route information using the **peer** { *group-name* | *ipv4-address* } **enable** command.

Configuration Impact

If a route-policy is specified for an EVPN BGP peer group, all the members in the group inherit this configuration.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Creating a route-policy before it is referenced is recommended. By default, nonexistent route-policies cannot be referenced using the command. If the **route-policy nonexistent-config-check disable** command is run in the system view and a nonexistent route-policy is referenced using the current command, all routes are advertised to the specified peer, or all routes received from the specified peer are accepted.

Example

Apply a route-policy named **test-rp** to the routes received from the EVPN BGP peer 1.1.1.9.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] peer 1.1.1.9 as-number 200
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] peer 1.1.1.9 enable
[Huawei-bgp-af-evpn] peer 1.1.1.9 route-policy test-rp import
```

12.10.12 policy vpn-target (BGP-EVPN address family view)

Function

The **policy vpn-target** command enables EVPN-VPN target-based filtering for received EVPN routes.

The **undo policy vpn-target** command disables EVPN-VPN target-based filtering for received EVPN routes.

By default, EVPN-VPN target-based filtering is enabled for received EVPN routes.

Format

policy vpn-target

undo policy vpn-target

Parameters

None

Views

BGP-EVPN address family view

Default Level

2: Configuration level

Usage Guidelines

To enable EVPN-VPN target-based filtering for EVPN routes, run the **policy vpn-target** command. This configuration allows received EVPN routes to be filtered based on an EVPN-VPN target. For example, if an export EVPN-VPN target in the

 Copyright © Huawei Technologies Co., Ltd.

received EVPN routes matches the local import EVPN-VPN target, the EVPN routes is accepted.

Example

Enable EVPN-VPN target-based filtering for received EVPN routes.

```
<Huawei> system-view
[Huawei] bgp 100
[Huawei-bgp] l2vpn-family evpn
[Huawei-bgp-af-evpn] policy vpn-target
```

12.10.13 refresh bgp evpn

Function

The **refresh bgp evpn** command configures EVPN BGP soft reset to allow EVPN BGP connections to be softly reset.

Format

refresh bgp evpn { **all** | *ipv4-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

Parameters

Parameter	Description	Value
all	Softly resets all EVPN BGP connections.	-
ipv4-address	Specifies the IPv4 address of an EVPN BGP peer.	The value is in dotted decimal notation.
group *group-name*	Specifies an EVPN peer group.	The name is a string of 1 to 47 case-sensitive characters, with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
external	Specifies the EVPN peer of an EBGP connection.	-
internal	Specifies the EVPN peer of an IBGP connection.	-
export	Softly resets EVPN BGP connections in the outbound direction.	-
import	Softly resets EVPN BGP connections in the inbound direction.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To softly reset EVPN BGP connections, run the **refresh bgp evpn** command. EVPN BGP soft reset allows the system to refresh an EVPN BGP routing table without tearing down the EVPN BGP connections and to apply a new filtering policy.

With a delay configured for BGP to apply a route-policy,

- If an import policy is configured to filter the routes learned from a peer or peer group using the **peer route-policy import** command, BGP applies the import policy immediately when the **refresh bgp evpn all** command is run.
- If an export policy is configured to filter the routes to be sent to a peer or peer group using the **peer route-policy export** command, BGP does not apply the export policy even if the **refresh bgp evpn all** command is run.

Prerequisites

The route-refresh function has been enabled for EVPN BGP peers.

Example

Softly reset all EVPN BGP connections in the inbound direction so that new configurations can take effect.

```
<Huawei> refresh bgp evpn all import
```

Related Topics

9.8.121 peer keep-all-routes

12.10.11 peer route-policy (BGP-EVPN address family view)

12.10.14 vpn-target evpn

Function

The **vpn-target evpn** command configures EVPN-VPN targets for the VPN instance IPv4 address family.

The **undo vpn-target evpn** command deletes the EVPN-VPN targets configured for the VPN instance IPv4 address family.

By default, no EVPN-VPN targets are configured for the VPN instance IPv4 address family.

 Copyright © Huawei Technologies Co., Ltd.

Format

vpn-target { *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] } **evpn**

undo vpn-target { **all** | *vpn-target* &<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] } **evpn**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-target	Specifies the EVPN-VPN targets to be added to the EVPN-VPN target list of the VPN instance IPv4 address family.	The value can be in one of the following four formats: ● 16-bit AS number:32-bit user-defined number. For example, 1:3. The AS number is an integer ranging from 0 to 65535, and the user-defined number is an integer ranging from 0 to 4294967295. The AS number and user-defined number cannot be both 0s. That is, the EVPN-VPN target value cannot be 0:0. ● 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1. The IP address ranges from 0.0.0.0 to 255.255.255.255, and the user-defined number ranges from 0 to 65535. ● Integral 4-byte AS number:2-byte user-defined number, for example, 65537:3. An AS number ranges from 65536 to 4294967295, and a user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, the EVPN-VPN target value cannot be 0:0. ● 4-byte AS number in dotted notation:2-byte user-defined number, for example, 0.0:3 or 0.1:0. A 4-byte AS number in dotted notation is in the format of *x.y*, where *x* and *y* are integers that both range from 0 to 65535. A user-defined number ranges from 0 to 65535. The AS number and user-defined number cannot be both 0s. That is, the EVPN-VPN target value cannot be 0.0:0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
both	Adds specified EVPN-VPN targets to both the import and export EVPN-VPN target lists of the VPN instance IPv4 address family. If you do not specify **both**, **export-extcommunity**, or **import-extcommunity**, EVPN-VPN targets are added to both the import and export EVPN-VPN target lists by default.	-
export-extcommunity	Adds specified EVPN-VPN targets to the export EVPN-VPN target list of the VPN instance IPv4 address family.	-
import-extcommunity	Adds specified EVPN-VPN targets to the import EVPN-VPN target list of the VPN instance IPv4 address family.	-
all	Deletes all the EVPN-VPN targets of the VPN instance IPv4 address family.	-

Views

VPN instance view or VPN instance IPv4 address family view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VPN instance-configured device, to configure import or export EVPN-VPN targets for the VPN instance IPv4 address family, run the **vpn-target evpn** command.

The EVPN-VPN targets control EVPN route learning between VPN instances. An EVPN-VPN target may be either import or export. An export EVPN-VPN target is contained in an EVPN route to be advertised to a remote EVPN peer. Upon receipt of the EVPN route, the remote EVPN peer compares the received export EVPN-VPN target with the local import EVPN-VPN target to determine whether the

 Copyright © Huawei Technologies Co., Ltd.

EVPN route can be added to the routing table of the local VPN instance IPv4 address family.

Prerequisites

An RD has been configured for the VPN instance IPv4 address family using the **route-distinguisher** command.

Configuration Impact

An EVPN-VPN target configured using the **vpn-target evpn** command does not overwrite any previously configured EVPN-VPN target. If the number of configured EVPN-VPN targets has reached the maximum limit, subsequent EVPN-VPN targets cannot be added any more.

Precautions

Multiple EVPN-VPN targets can be configured for the VPN instance IPv4 address family. One **vpn-target evpn** command can configure a maximum of eight EVPN-VPN targets at a time. To configure more EVPN-VPN targets for a VPN instance, run the **vpn-target evpn** command several times. When EVPN routes are advertised between VPN instances, if one of the EVPN-VPN targets carried in the EVPN routes matches the import EVPN-VPN target of the local VPN instance IPv4 address family, the EVPN routes will be added to the EVPN routing table of the local VPN instance.

Example

Add an EVPN-VPN target with the value 3:3 to the export EVPN-VPN target list and an EVPN-VPN target with the value 4:4 to the import EVPN-VPN target list for the IPv4 address family of VPN instance named **vrf1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] ipv4-family
[Huawei-vpn-instance-vrf1-af-ipv4] route-distinguisher 100:1
[Huawei-vpn-instance-vrf1-af-ipv4] vpn-target 3:3 export-extcommunity evpn
[Huawei-vpn-instance-vrf1-af-ipv4] vpn-target 4:4 import-extcommunity evpn
```

12.11 VLL Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support VLL.

12.11.1 bfd bind pw

Function

The **bfd bind pw** command configures a BFD session to detect a PW.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is configured to detect a PW.

Format

bfd *cfg-name* **bind pw interface** *interface-type interface-number* [**secondary**]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of the BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the type and number of the interface where the PW to be detected resides, namely, the AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary	Indicates that the BFD session detects the secondary PW.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a transmission device exists on a direct link, BFD detects a link fault faster than a link detection mechanism on an interface. On networks demanding fast fault detection, run the **bfd bind pw** command to configure a BFD session to detect a PW.

Prerequisites

- A PW has been configured on an AC interface by running the **mpls l2vc** command.
- BFD has been enabled globally by running the **bfd** command.
- A single-segment or multi-segment PW has been configured.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- When detecting a PW, BFD sessions must be bound to the source and destination ends of a PW.
- You need to create a BFD session to detect primary and secondary PWs separately.

NOTE

When running the **bfd bind pw** command to detect a multi-segment PW, ensure that the first-segment PW is a VLL PW configured on a non-SPE node.

When running the **bfd bind pw** command to detect a single-segment PW, ensure that the single-segment PW is configured on a non-SPE node.

Example

Create a BFD session to detect a PW.

```
<Huawei> system-view
[Huawei] bfd pe2 bind pw interface vlanif 10
```

12.11.2 ccc interface out-interface

Function

The **ccc interface out-interface** command creates a local CCC connection between two CEs connected to the same PE.

The **undo ccc** command deletes the CCC connection.

By default, no local CCC connection is created.

Format

ccc *ccc-connection-name* **interface** *interface-type1 interface-number1* [**raw** | **tagged**] **out-interface** *interface-type2 interface-number2* [**raw** | **tagged**]

undo ccc *ccc-connection-name*

Parameters

Parameter	Description	Value
ccc-connection-name	Specifies a CCC connection name, which uniquely identifies a CCC connection on a PE.	The value is a string of 1 to 20 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Parameter	Description	Value
interface *interface-type1 interface-number1*	Specifies the type and number of the interface connected to the first CE. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
out-interface *interface-type2 interface-number2*	Specifies the type and number of the interface connected to the second CE. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-
raw	Sets the inbound interface to raw mode. When packets arrive at the inbound interface in raw mode, the system deletes the provider tags (P-tags) of packets.	By default, the tagged mode is used.
tagged	Sets the inbound interface to tagged mode. When packets arrive at the inbound interface in tagged mode, the system retains the sprovider tags (P-tags) of packets.	By default, the tagged mode is used.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When two CEs connect to the same PE, use the **ccc interface out-interface** command to create a local CCC connection between the CEs.

Precautions

An interface cannot serve as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, the Layer 3 features such as the IP address and routing protocol configured on this interface become invalid. After the interface is bound to a CCC connection, its sub-interfaces no longer transmit Layer 3 traffic.

A CCC connection is bidirectional; therefore, only one connection is needed. Do not configure the name of a CCC connection as **type**; otherwise, you cannot view information about the CCC connection by running the **display vll ccc** command.

Example

Create a local CCC connection between two CEs connected to the same PE device.

```
<Huawei> system-view
[Huawei] mpls lsr-id 1.1.1.1
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls l2vpn
[Huawei-l2vpn] quit
[Huawei] ccc ccc-connect-1 interface vlanif 10 out-interface vlanif 11
```

Related Topics

12.11.16 display vll ccc

12.11.3 display l2vpn ccc-interface vc-type

Function

The **display l2vpn ccc-interface vc-type** command displays information about the interface used by an L2VPN connection.

Format

display l2vpn ccc-interface vc-type { **all** | *vc-type* } [**down** | **up**]

Parameters

Parameter	Description	Value
all	Displays information about all interfaces of L2VPN connections.	-
vc-type	Specifies the type of the L2VPN connection.	The following types of the L2VPN connection are available: • ccc: Cross Circuit Connection • ldp-vc: L2VPN connection in the Martini mode • static-vc: L2VPN connection in the SVC mode • vpls-vc: VPLS connection
down	Displays information about interfaces of L2VPN connection in the Down state.	-
up	Displays information about interfaces of L2VPN connection in the Up state.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating L2VPN faults, you can use the **display l2vpn ccc-interface vc-type** command to view information about the AC interface of the current L2VPN connection, the total number of AC interfaces of various L2VPN connections, interface status, interface encapsulation type, and L2VPN connection types.

Example

Display information about all the interfaces of L2VPN.

```
<Huawei> display l2vpn ccc-interface vc-type all
Total ccc-interface of CCC : 2
up (2), down (0)
Interface                 Encap Type        State    VC Type
GigabitEthernet0/0/2          ethernet           up       ccc
GigabitEthernet0/0/1          ethernet           up       ccc
```

Table 12-107 Description of the **display l2vpn ccc-interface vc-type** command output

Item	Description
Total ccc-interface of CCC : 2 up (2), down (0)	Total number of L2VPN connections is 2. Two connections is Up. No connection is Down.
Interface	Interface connected to the L2VPN connection on the router.
Encap Type	Encapsulation type of the L2VPN connection. The encapsulation type can be VLAN encapsulation or Ethernet encapsulation.
State	Current status of the L2VPN connection. The status can be Up or Down.
VC Type	Type of the L2VPN connection: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● vpls-vc: VPLS connection

Related Topics

12.11.4 display mpls l2vc

12.11.12 display mpls static-l2vc

12.11.4 display mpls l2vc

Function

The **display mpls l2vc** command displays information about virtual circuits (VCs) in LDP mode.

Format

display mpls l2vc [*vc-id* | **interface** *interface-type interface-number* | **remote-info** [*vc-id* | **verbose**] | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface connected to the CE. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
remote-info	Displays information about the VC on the remote end.	-
vc-id	Displays static PW information with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays the detailed information about the VC on the remote end.	-
state { **down** | **up** }	Displays VC information based on the VC status. • **down**: Displays information about the VC in Down state. • **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display mpls l2vc** command displays information about the VCs in LDP signaling mode, including the Martini VC and PWE3 VC.

- If the interface is specified, information about VCs on the specified AC interface is displayed.
- If **remote-info** is specified but *vc-id* is not specified, information about all VCs set up by the remote and local peers is displayed.

Example

Display information about all the LDP VCs configured on the router.

```
<Huawei> display mpls l2vc
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW        : no
  session state           : up
  AC status               : up
  Ignore AC state         : disable
  VC state                : up
  Label state             : 0
  Token state             : 0
  VC ID                   : 101
  VC type                 : VLAN
  destination             : 10.3.3.9
  local VC label          : 1026         remote VC label      : 1026
  control word            : disable
  remote control word     : disable
  forwarding entry        : exist
  local group ID          : 0
  remote group ID         : 0
  local AC OAM State      : up
  local PSN OAM State     : up
  local forwarding state : forwarding
  local status code       : 0x0
  remote AC OAM state     : up
  remote PSN OAM state    : up
  remote forwarding state: forwarding
  remote status code      : 0x0
  ignore standby state    : no
  BFD for PW              : unavailable
  VCCV State              : up
  manual fault            : not set
  active state            : active
  link state              : up
  local VC MTU            : 1500         remote VC MTU        : 1500
  local VCCV              : alert ttl lsp-ping bfd
  remote VCCV             : alert ttl lsp-ping bfd
  tunnel policy name      : --
  PW template name        : --
  primary or secondary    : primary
  load balance type       : flow
  Access-port             : false
  Switchover Flag         : false
  VC tunnel/token info    : 1 tunnels/tokens
    NO.0  TNL type        : lsp   , TNL ID : 0x48000020
    Backup TNL type       : lsp   , TNL ID : 0x0
  create time             : 0 days, 0 hours, 6 minutes, 50 seconds
  up time                 : 0 days, 0 hours, 6 minutes, 34 seconds
  last change time        : 0 days, 0 hours, 6 minutes, 34 seconds
  VC last up time         : 2013/09/24 18:23:35
  VC total up time        : 0 days, 0 hours, 6 minutes, 34 seconds
  CKey                    : 16
```

 Copyright © Huawei Technologies Co., Ltd.

```
NKey                    : 15
PW redundancy mode      : frr
AdminPw interface       : --
AdminPw link state      : --
Diffserv Mode           : uniform
Service Class           : be
Color                   : --
DomainId                : --
Domain Name             : --
```

Table 12-108 Description of the **display mpls l2vc** command output

Item	Description
Total LDP VC	Total number of established LDP VCs, including the number of LDP VCs in Up and Down state.
client interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface. This field can be displayed as **yes** or **no**. Currently, mPW is not supported on the device.
session state	Status of the LDP session established between both ends of the VC: ● up: The LDP session has been established. ● down: The LDP session is not established.
AC status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
Ignore AC state	Whether to ignore the impact of AC status changes on the active/standby PWE3 service status is enabled: ● enable ● disable
VC state	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Token state	Token status: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
VC ID	ID of the VC, which uniquely identifies a VC. **NOTE** If the VC IDs on both ends are different, run the **mpls l2vc** command in the interface view to change the VC ID on one end to be the same as that on the other end.
VC type	Encapsulation type of the VC: ● VLAN ● Ethernet The PW can go Up only when the local and remote encapsulation types are the same.
destination	LSR ID of the VC peer device.
local VC label	Local VC label.
remote VC label	Remote VC label.
control word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.
forwarding entry	Whether forwarding entries exist.
local group ID	Local group ID.
remote group ID	Remote group ID.
manual fault	Whether a PW fault is simulated.
active state	Whether the PW is in active state. A PW in active state can forward packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link state	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● Status of the mPW associated with service PWs ● Status of the BFD session associated with service PWs ● PW state code ● PW status detected by VCCV ● OAM status
local VC MTU	MTU of the local VC.
remote VC MTU	MTU of the remote VC.
tunnel policy name	Name of the tunnel policy.
PW template name	Name of the PW template.
primary or secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
Switchover Flag	Whether a switchover has occurred.
create time	How long the VC has been created.
up time	How long the VC keeps the Up state. If the current PW status is Down, the value is 0.
last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AdminPw interface	AC interface on which the mPW is bound to the PW. The AC interface must be a loopback interface. This field is displayed only when the PW is not an mPW: ● Name of the loopback interface. ● --: indicates that the PW is not bound to an mPW.
AdminPw link state	Status of the mPW bound to the PW. This field is displayed only when the PW is not an mPW. This field can be displayed as: ● Up ● Down ● --: indicates that the PW is not bound to an mPW.
Diffserv Mode	QoS DiffServ mode.
Service Class	QoS service class.
Color	QoS color.
DomainId	ID of a domain.
Domain Name	Name of a domain.

Display LDP VC information about the AC interface.

```
<Huawei> display mpls l2vc interface ethernet 1/0/0
 *client interface       : Ethernet1/0/0 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 101
  VC type                : Ethernet
  destination            : 10.3.3.9
  local group ID         : 0            remote group ID      : 0
  local VC label         : 1024         remote VC label      : 1024
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x0
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  forwarding entry       : exist
  link state             : up
```

```
local VC MTU           : 1500         remote VC MTU        : 1500
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable      remote control word  : disable
tunnel policy name     : --
PW template name       : --
primary or secondary   : primary
load balance type      : flow
Access-port            : false
Switchover Flag        : false
VC tunnel/token info   : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x5
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 29 minutes, 47 seconds
up time                : 0 days, 0 hours, 4 minutes, 54 seconds
last change time       : 0 days, 0 hours, 4 minutes, 54 seconds
VC last up time        : 2011/09/26 15:29:03
VC total up time       : 0 days, 0 hours, 4 minutes, 54 seconds
CKey                   : 5
NKey                   : 4
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : uniform
Service Class          : --
Color                  : --
DomainId               : --
Domain Name            : --
```

Table 12-109 Description of the **display mpls l2vc interface** command output

Item	Description
local AC OAM State	OAM status of the local AC. ● up ● down
local PSN OAM State	Status of the local device on the Packet Switch Network (PSN) side. ● up ● down
local forwarding state	Status of the local forwarding table. ● forwarding ● down
local status code	Status code of the local PW: ● 0x0: indicates that the local PW functions as the master PW and is in Up state. ● 0x20: indicates that the local PW functions as the backup PW and is in Up state. ● 0x1: indicates that the local PW functions as the master PW and is in Down state. ● 0x21: indicates that the local PW functions as the backup PW and is in Down state.

Item	Description
remote AC OAM state	OAM status of the remote AC. ● up ● down
remote PSN OAM state	Status of the remote device on the PSN side. ● up ● down
remote forwarding state	Status of the remote forwarding table. ● forwarding ● down
remote status code	Status code of the remote PW: ● 0x0: indicates that the remote PW functions as the master PW and is in Up state. ● 0x20: indicates that the remote PW functions as the backup PW and is in Up state. ● 0x1: indicates that the remote PW function as the master PW and is in Down state. ● 0x21: indicates that the remote PW function as the backup PW and is in Down state.
BFD for PW	Whether BFD for PW is enabled: ● available ● unavailable
VCCV State	Whether Virtual Circuit Connectivity Verification (VCCV) is enabled.
local VCCV	Type of VCCV supported on the local device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
remote VCCV	Type of VCCV supported on the remote device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
local control word	Whether the control word is enabled on the local device: ● Disable ● Enable
remote control word	Whether the control word is enabled on the remote device: ● Disable ● Enable
ignore standby state	Whether the status of the secondary PW is ignored.
VC Tunnel/token info: 1 tunnels/tokens	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
TNL type	Type of the tunnel used by the PW.
TNL ID	ID of the tunnel used by the PW.
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
PW redundancy mode	PW redundancy mode. By default, the mode is FRR. ● Independent: indicates that the PW is in negotiation mode. ● frr: indicates that the PW is in FRR mode. ● --: indicates that the PW is in master/slave mode.

Display the LDP VC information received from the remote peer.

```
<Huawei> display mpls l2vc remote-info
Total remote ldp vc : 1

Transport  Group      Peer           Remote        Remote     C   MTU/  N   S
VC ID      ID         Addr           Encap         VC Label   Bit CELLS Bit Bit
```

```
101        0          10.3.3.9        ethernet       1024       0   1500  0   0
```

Display the detailed LDP VC information received from the remote peer.

```
<Huawei> display mpls l2vc remote-info verbose
Total remote LDP VC : 1

VC ID              : 101
VC Type            : ethernet
VC Label           : 1024
Peer Address       : 10.3.3.9
Group ID           : 0
MTU                : 1500
Control Word       : 0
Notification       : 0
Status Code        : 0
Match Local VC     : MATCH
Max ATM CELLS      : --
TDM RTP Header     : --
TDM Encap Num      : --
TDM Bit Rate       : --
```

Table 12-110 Description of the **display mpls l2vc remote-info** command output

Item	Description
Total remote ldp vc	Total number of created remote LDP VCs.
Transport VC ID	VC ID, which uniquely identifies a VC.
Group ID	ID of the group to which the L2VPN belongs. The default value is 0.
Peer Addr and Peer Address	IP address of the remote peer.
Remote Encap	Encapsulation type of the remote VC. ● vlan ● ethernet
Remote VC Label	Remote VC label.
C Bit	Whether the control word is enabled: ● 1: indicates that the control word is enabled. ● 0: indicates that the control word is disabled.
MTU/CELLS	MTU of the L2VPN.
N Bit and Notification	Whether the Notification message is supported: ● 1: indicates the message is supported. ● 0: indicates the message is not supported.
S Bit and Status Code	Status code: ● 0: indicates the forwarding state. ● 1: indicates the non-forwarding state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Match Local VC	Whether the local VC ID matches the remote VC ID: ● MATCH ● NOT-MATCH
Max ATM CELLS	Maximum number of ATM cells that can be transmitted. If ATM encapsulation is used, the value ranges from 1 to 28, and the default value is 28. If non-ATM encapsulation is used, double hyphens (--) are displayed.
TDM RTP Header	Whether the RTP-header option is enabled: ● enable: The RTP header is added to TDM packets to be transparently transmitted. ● disable: The RTP header is not added to TDM packets to be transparently transmitted. This is the default value. ● --: Non-TDM encapsulation is used.
TDM Encap Num	Number of frames in a TDM packet. If TDM encapsulation is used, the value is 8, 16, 24, 32 or 40, and the default value is 32. If non-TDM encapsulation is used, double hyphens (--) are displayed.
TDM Bit Rate	Number of timeslots in a TDM packet. Number of timeslots in a TDM packet = Number of bytes in a TDM packet/Number of frames in a TDM packet

Display information about the VCs in Up state.

```
<Huawei> display mpls l2vc state up
 Total LDP VC : 1     1 up       0 down

 *client interface       : Ethernet1/0/0 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 100
  VC type                : Ethernet
  destination            : 10.2.2.9
  local VC label         : 1024         remote VC label      : 1024
  control word           : disable
  remote control word    : disable
  forwarding entry       : exist
  local group ID         : 0
  remote group ID        : 0
```

```
 local AC OAM State     : up
 local PSN OAM State    : up
 local forwarding state : forwarding
 local status code      : 0x0
 remote AC OAM state    : up
 remote PSN OAM state   : up
 remote forwarding state: forwarding
 remote status code     : 0x0
 ignore standby state   : no
 BFD for PW             : unavailable
 VCCV State             : up
 manual fault           : not set
 active state           : active
 link state             : up
 local VC MTU           : 1500         remote VC MTU        : 1500
 local VCCV             : alert ttl lsp-ping bfd
 remote VCCV            : alert ttl lsp-ping bfd
 tunnel policy name     : --
 PW template name       : --
 primary or secondary   : primary
 load balance type      : flow
 Access-port            : false
 Switchover Flag        : false
 VC tunnel/token info   : 1 tunnels/tokens
   NO.0  TNL type       : lsp   , TNL ID : 0x12
   Backup TNL type      : lsp   , TNL ID : 0x0
 create time            : 0 days, 1 hours, 0 minutes, 17 seconds
 up time                : 0 days, 0 hours, 24 minutes, 56 seconds
 last change time       : 0 days, 0 hours, 24 minutes, 56 seconds
 VC last up time        : 2013/10/10 14:29:39
 VC total up time       : 0 days, 0 hours, 24 minutes, 56 seconds
 CKey                   : 10
 NKey                   : 9
 PW redundancy mode     : frr
 AdminPw interface      : --
 AdminPw link state     : --
 Diffserv Mode          : uniform
 Service Class          : --
 Color                  : --
 DomainId               : --
 Domain Name            : --
```

Display information about the dynamic VC on the TDM interface.

```
<Huawei> display mpls l2vc interface serial 2/0/0
*client interface       : Serial2/0/0 is up
 Administrator PW       : no
 session state          : up
 AC status              : up
 Ignore AC state        : disable
 VC state               : up
 Label state            : 0
 Token state            : 0
 VC ID                  : 100
 VC type                : CESoPSN basic mode
 destination            : 10.3.3.9
 local group ID         : 0            remote group ID      : 0
 local VC label         : 1039         remote VC label      : 1045
 local TDM Encap Num    : 8            remote TDM Encap Num : 0
 jitter-buffer          : 8
 idle-code              : ff
 local rtp-header       : disable      remote rtp-header    : disable
 local bit-rate         : 0            remote bit-rate      : 0
 local AC OAM State     : up
 local PSN OAM State    : up
 local forwarding state : forwarding
 local status code      : 0x0
 remote AC OAM state    : up
 remote PSN OAM state   : up
 remote forwarding state: forwarding
 remote status code     : 0x0
```

```
ignore standby state   : no
BFD for PW             : unavailable
VCCV State             : up
manual fault           : not set
active state           : active
forwarding entry       : exist
link state             : up
local VC MTU           : --          remote VC MTU        : --
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable     remote control word  : disable
tunnel policy name     : --
PW template name       : pe2pe
primary or secondary   : primary
load balance type      : flow
Access-port            : false
Switchover Flag        : false
VC tunnel/token info   : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x5
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 1 minutes, 36 seconds
up time                : 0 days, 0 hours, 1 minutes, 36 seconds
last change time       : 0 days, 0 hours, 1 minutes, 36 seconds
VC last up time        : 2013/11/02 09:30:04
VC total up time       : 0 days, 0 hours, 1 minutes, 36 seconds
CKey                   : 9
NKey                   : 8
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : pipe
Service Class          : ef
Color                  : green
DomainId               : --
Domain Name            : --
```

Table 12-111 Description of the **display mpls l2vc interface** command output

Item	Description
local TDM Encap Num	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application of the local VC.
remote TDM Encap Num	Number of encapsulated TDM frames in CESoPSN or SAToP packets in the TDMoPSN application of the remote VC. **NOTE** This field is displayed as 0 when the AC interface is a serial interface.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
local rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the local end.

Item	Description
remote rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the remote end.
local bit-rate	Bit rate of the local VC.
remote bit-rate	Bit rate of the remote VC.

Related Topics

12.11.20 mpls l2vc
12.11.7 display mpls l2vpn forwarding-info

12.11.5 display mpls l2vc brief

Function

The **display mpls l2vc brief** command displays brief information about LDP Layer 2 virtual circuits (L2VCs) on the device.

Format

display mpls l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc brief** command is recommended when many L2VCs are configured on a device. The command output is more concise than that of the **display mpls l2vc** command.

Example

Display brief information about all LDP L2VCs on the device.

```
<Huawei> display mpls l2vc brief
 Total LDP VC : 1      1 up       0 down

 *Client Interface     : Vlanif1111
  Administrator PW     : no
  AC status            : up
```

```
VC state          : up
Label state        : 0
Token state        : 0
VC ID             : 116119
VC Type           : VLAN
session state      : up
Destination        : 10.6.6.6
link state        : up
```

Table 12-112 Description of the **display mpls l2vc brief** command output

Item	Description
Total LDP VC	Total number of LDP VCs, including the number of LDP VCs in Up and Down state.
Client Interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface.
AC status	Status of the AC: ● up ● down
VC state	Status of the VC: ● up ● down
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
Token state	Token status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
session state	Status of the session between peers: ● up ● down
Destination	Peer address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link state	Status of the VC: ● up ● down

Related Topics

12.11.20 mpls l2vc

12.11.7 display mpls l2vpn forwarding-info

12.11.6 display mpls l2vc oam-mapping

Function

The **display mpls l2vc oam-mapping** command displays status of an L2VPN AC established by using the LDP signaling and information about the OAM mapping table at the PSN side.

Format

display mpls l2vc oam-mapping [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number. If this parameter specified, OAM mapping information on the specified VC interface using the LDP signaling is displayed. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display mpls l2vc oam-mapping** command, either the following situation will occur:

- If an interface name is specified, detailed OAM mapping information on this interface is displayed.

 Copyright © Huawei Technologies Co., Ltd.

- If no interface name is specified, basic about the OAM mapping information on all interfaces is displayed.

Example

Display OAM mapping information on the VC interface using the LDP signaling.

```
<Huawei> display mpls l2vc oam-mapping
 Interface                Active VC-ID     VC-status AC-OAM  BFD-for-PW
GigabitEthernet0/0/1        No    100       Primary   Enable  Disable
GigabitEthernet0/0/1        No    101       Secondary Enable  Disable
```

Table 12-113 Description of the **display mpls l2vc oam-mapping** command output

Item	Description
Interface	Type and number of the AC interface.
Active	Whether the PW is in the active state: ● Yes: indicates that the PW is in active state. ● No: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist.
VC-ID	ID of the local VC.
VC-status	Status of the local PW: ● Primary: indicates the primary PW. ● Secondary: indicates the secondary PW.
AC-OAM	Whether the local PE reports an AC fault to the remote PE through OAM: ● Enable: indicates that the local PE reports an AC fault to the remote PE through OAM. ● Disable: indicates that the local PE does not report an AC fault to the remote PE through OAM.
BFD-for-PW	Whether BFD for PW is enabled on the local PE: ● Enable ● Disable

Display OAM mapping information on GE1/0/0.

```
<Huawei> display mpls l2vc oam-mapping interface gigabitethernet 1/0/0
 AC OAM Info:
```

```
 EOAM Type      : 802.3ah
 AC OAM State   : Up
 OAM-mapping    : Enable
PSN info:
 VC-ID          : 100
 VC status      : Primary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
 VC-ID          : 101
 VC status      : Secondary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
```

Table 12-114 Description of the **display mpls l2vc oam-mapping interface** command output

Item	Description
AC OAM Info	Information about AC OAM to be displayed in the following lines.
ACFD Index	Index of the AC forwarding information.
EOAM Type	Type of the protocol used for fault detection and notification.
AC OAM State	Fault detection status on the local AC: ● Up: indicates that AC fault detection is disabled or that AC fault detection is enabled but no AC fault is detected. ● Down: indicates that AC fault detection is enabled and an AC fault is detected. ● Invalid: indicates that AC fault detection is disabled, and the AC OAM state field is invalid.
OAM-mapping	Whether OAM mapping is enabled on the local PE: ● Enable ● Disable
PSN info	Information about the PW.
VC-ID	ID of the VC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VC status	Status of the PW: ● Primary: indicates the primary PW. ● Secondary: indicates the secondary PW. ● Bypass: indicates the inter-chassis PW. ● PW-Bypass: indicates the inter-chassis PW used to protect PW-side links. ● AC-Bypass: indicates the inter-chassis PW used to protect AC-side links.
Active state	Whether the PW is in the active state: ● Active: indicates that the PW is in active state. ● Inactive: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist. When an AC interface is configured with only one PW, the PW is in active state. If an AC interface is configured with primary and secondary PWs, the primary PW is in active state and the secondary PW is in inactive state. When the primary PW fails, the secondary PW becomes active and the primary PW becomes inactive.
Link State	Link status of the AC interface. ● Up: indicates that the interface is Up. ● Down: indicates that the interface is Down.
BFD for PW	Whether BFD for PW is enabled on the local PE.
BFD for LSP	Whether BFD is used to detect a tunnel: ● zero: indicates that BFD is not used to detect a tunnel. ● non-zero: indicates that BFD is used to detect a tunnel.
TunnelNum	Number of tunnels detected by BFD.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSN State	• When the tunnel is not detected by BFD, the default status of the tunnel is Up. • When the PW uses the tunnel not detected by BFD, the PSN state is Up.

Related Topics

12.11.24 mpls l2vpn oam-mapping

12.11.7 display mpls l2vpn forwarding-info

Function

The **display mpls l2vpn forwarding-info** command displays MPLS L2VPN forwarding information.

Format

display mpls l2vpn forwarding-info [*vc-label*] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
vc-label	Specifies L2VPN VC label.	The value is a decimal integer that ranges from 16 to 1048575.
interface *interface-type interface-number*	Specifies the type and number of the interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display mpls l2vpn forwarding-info** command displays:

- Private network data carrying the specified label is forwarded from which tunnel.
- Whether the data supports the connectivity verification.
- Whether the data carry the control word.

Example

Display MPLS L2VPN forwarding information.

```
<Huawei> display mpls l2vpn forwarding-info interface vlanif 10
 The Main PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
--------------------------------------------------------------------------------
35841   LSP            SEND      ACTIVE   UP       UP    FALSE   2  a  0x1
  1   Record(s) Found.

 The Second PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
--------------------------------------------------------------------------------
  0   Record(s) Found.
```

Table 12-115 Description of the display mpls l2vpn forwarding-info interface command output

Item	Description
The Main PW Forward Information :	Forwarding information about the primary PW.
VCLABEL	Label of the VC bound to the interface.
TNLTYPE	Types of public network tunnels used by the VC.
ENTRYTYPE	Type of forwarding entries: ● SEND: forwarding entries of L2VPN except CCC ● LOCAL: forwarding entries of the local connection ● INVALID: invalid forwarding entries
PWSTATE	PW state used for guiding packet forwarding: active or inactive. The primary PW and the secondary PW are mutually exclusive and both cannot be in the active state simultaneously.
BFDSTATE	BFD state used for guiding packet forwarding. If BFD is not configured, this flag bit is Up by default. If BFD is configured and the BFD session is Down (not Admin Down), this flag bit is Down and packets cannot be forwarded.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ADMIN	Whether the primary or secondary PW fault is configured manually: ● Up: indicates that the primary or secondary PW fault is not configured manually. ● Down: indicates that the primary or secondary PW fault is configured manually.
CTLWORD	Whether the control word is enabled on the local end: ● FALSE: indicates that the control word is disabled. ● TRUE: indicates that the control word is enabled.
CC	Connection channel of the VCCV: Control word Label alert.
CV	Connectivity verification.
TNLID	ID of the public tunnel used by the VC, which is a hexadecimal integer.
Record (s) Found	Number of VC forwarding entries on the local interface.
The Second PW Forward Information :	Forwarding information about the secondary PW.

Display MPLS L2VPN forwarding information with VC label as 35842.

```
<Huawei> display mpls l2vpn forwarding-info 35842 interface vlanif 10
 The Main PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
--------------------------------------------------------------------------------
35842   LSP            SEND      ACTIVE   UP       UP    FALSE   0  0  0x1
   1   Record(s) Found.

 The Second PW Forward Information :
VCLABEL TNLTYPE        ENTRYTYPE PWSTATE  BFDSTATE ADMIN CTLWORD CC CV TNLID
--------------------------------------------------------------------------------
   0   Record(s) Found.
```

Related Topics

12.11.4 display mpls l2vc

12.11.8 display mpls l2vpn label-space

Function

The **display mpls l2vpn label-space** command displays information about label space distribution and different types of labels in the label cache.

Format

display mpls l2vpn label-space

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After L2VPN is enabled, run the **display mpls l2vpn label-space** command and you can view information about label space distribution and different types of labels in the label cache.

Example

Display information about label space distribution when L2VPN is enabled and the cache contains labels.

```
<Huawei> display mpls l2vpn label-space
 there are 0 labels or label blocks in label-space.
 ------------------------------------------------------------
 label(s) released in SVC connection:              0
 label(s) released in LDP connection:              1
 label block(s) released in BGP connection:        0
 label(s) released in VPLS LDP connection:         0
 label block(s) released in VPLS BGP connection:   0
 ------------------------------------------------------------
```

Table 12-116 Description of the **display mpls l2vpn label-space** command output

Item	Description
Label	Indicates the value of the label in the label cache.
Label (s) released in SVC connection	Indicates the total number of labels in the label cache for the VLL SVC connections.
Label (s) released in LDP connection	Indicates the total number of labels in the label cache for the VLL LDP connections.
Label block (s) released in BGP connection	Indicates the total number of label blocks in the label cache for the VLL BGP connections.
Label (s) released in VPLS LDP connection	Indicates the total number of labels in the label cache for the VPLS LDP connections.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Label blocks (s) released in VPLS BGP connection	Indicates the total number of labels in the label cache for the VPLS BGP connections.

12.11.9 display mpls l2vpn resource

Function

The **display mpls l2vpn resource** command displays MPLS L2VPN specifications and usage information.

Format

display mpls l2vpn resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check MPLS L2VPN specifications and usage information in routine maintenance, run the **display mpls l2vpn resource** command.

Example

Display MPLS L2VPN specifications and usage information.

```
<Huawei> display mpls l2vpn resource

 Public Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN AC Number                      512                 0
 L2VPN VC Number                      512                 1

 VPWS Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN Local CCC Number               256                 0
 L2VPN SVC Number                     256                 0
 L2VPN LDP VC Number                  256                 1
 L2VPN Switch VC Number               256                 0

 VPLS Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN VSI Number                     512                 0
```

```
L2VPN VSI VC Number          512          0
L2VPN VSI PWG Number          8000          0
```

Table 12-117 Description of the **display mpls l2vpn resource** command output

Item	Description
Public Capacity Statistics	MPLS L2VPN capacity statistics
Statistics Item	Statistics item
Supported Number	Maximum number allowed
Used Number	Number already used
L2VPN AC Number	Number of L2VPN AC interfaces, including the maximum number allowed and number already used
L2VPN VC Number	Number of L2VPN VCs, including the maximum number allowed and number already used
VPWS Capacity Statistics	VPWS capacity statistics
L2VPN Local CCC Number	Number of VLLs in local CCC mode, including the maximum number allowed and number already used
L2VPN SVC Number	Number of VLLs in SVC mode, including the maximum number allowed and number already used
L2VPN LDP VC Number	Number of LDP VLLs, including the maximum number allowed and number already used
L2VPN Switch VC Number	Number of Switch VC, including the maximum number allowed and number already used
VPLS Capacity Statistics	VPLS capacity statistics
L2VPN VSI Number	Number of VSIs, including the maximum number allowed and number already used
L2VPN VSI VC Number	Number of VSI VCs, including the maximum number allowed and number already used
L2VPN VSI PWG Number	Number of protection groups for a VSI, including the maximum number allowed and number already used

12.11.10 display mpls l2vpn vpws

Function

The **display mpls l2vpn vpws** command displays information about the VPWS service.

Format

display mpls l2vpn vpws [**interface** *interface-type interface-number* [**verbose**]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
verbose	Displays detailed VPWS service information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When configuring or commissioning VPWS, you can run the **display mpls l2vpn vpws** command to check whether VPWS service configurations are correct.

Note the following points when using the **display mpls l2vpn vpws** command:

- If **interface** *interface-type interface-number* is specified, only VPWS service information on a specified AC interface is displayed.
- If **verbose** is also specified, detailed information about the VPWS service on a specified AC interface is displayed.

Prerequisites

VPLS configurations are complete on the local end.

Example

Display VPWS service information.

```
<Huawei> display mpls l2vpn vpws

Pri : Primary          Sec : Secondary          Byp : Bypass
PWb : PW-bypass        ACb : AC-bypass

Access Circuit              Virtual Circuit              States Active   Role
                    3.3.3.9:200                 Up     Active   Pri
                         2.2.2.9:201                 Up     Inactive Sec
```

Table 12-118 Description of the display mpls l2vpn vpws command output

Item	Description
Access Circuit	Access circuit.
Virtual Circuit	Virtual circuit.
States	VC status, which can be: ● Up ● Down
Active	Activation status of a VC, which can be: ● Active ● Inactive
Role	Role of a PW, which can be: ● Pri: Primary PW ● Sec: Secondary PW ● PWb: PW-bypass ● ACb: AC-bypass ● Byp: Bypass

Display the detailed information about the VPWS service on a specified AC interface.

```
<Huawei> display mpls l2vpn vpws interface gigabitethernet  verbose

Access circuit     : GigabitEthernet
Interface state    : Up
Protect mode       : FRR

Members:
Virtual Circuit              States Active   Role
3.3.3.9:200                  Up     Active   Primary
2.2.2.9:201                  Up     Inactive Secondary

Primary:
 VC type                : LDP VC
 VC state               : up
 Peer IP                : 3.3.3.9
 VC ID                  : 200
 Encapsulation type     : Ethernet
 LDP session state      : up
 VC information (Local / Remote)
  Label                 : 1025 / 1024
  MTU                   : 1500 / 1500
  Control word          : enable / enable
  Status code           : 0x0 / 0x0
  Group ID              : 0 / 0
  VCCV status           : cw alert ttl lsp-ping bfd / cw alert ttl lsp-ping bfd
 VC last up time        : 2013/12/21 16:42:51
 VC total up time       : 0 days, 6 hours, 20 minutes, 0 seconds

Secondary:
 VC type                : LDP VC
 VC state               : up
 Peer IP                : 2.2.2.9
 VC ID                  : 201
```

```
Encapsulation type     : Ethernet
LDP session state      : up
VC information (Local / Remote)
 Label                 : 1026 / 1025
 MTU                   : 1500 / 1500
 Control word          : enable / enable
 Status code           : 0x0 / 0x0
 Group ID              : 0 / 0
 VCCV status           : cw alert ttl lsp-ping bfd / cw alert ttl lsp-ping bfd
VC last up time        : 2013/12/21 14:57:13
VC total up time       : 0 days, 20 hours, 44 minutes, 40 seconds
```

Table 12-119 Description of the display mpls l2vpn vpws command output

Item	Description
Access Circuit	Access circuit.
Protect mode	Protection mode, which can be FRR, independent, or master.
Members	PW member.
Virtual Circuit	Virtual circuit.
States	VC status
Active	Activation status of a VC, which can be:
Role	Role of a PW, which can be: ● Pri: Primary PW ● Sec: Secondary PW ● PWb: PW-bypass ● ACb: AC-bypass ● Byp: Bypass
Primary	Information about the primary PW.
VC type	The type of a VC.
VC state	VC status.
Peer IP	IP address of a peer.
VC ID	ID of a VC. The value is an integer in decimal notation. The default value is 0.
Encapsulation type	Encapsulation type of a VC.
LDP session state	Status of an LDP session.
VC information (Local / Remote)	VC information (local/remote).
Label	VC label.
MTU	Maximum transmission unit of a VC interface.
Control word	Whether the control word is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status code	Status code, which can be: ● 0x0: indicates the forwarding state. ● 0x1: indicates the non-forwarding state. ● 0x06: indicates the ACOAM fault. ● 0x18: indicates the public network fault. ● 0x20: indicates the standby state.
Group ID	Group ID.
VCCV status	VCCV status.
VC last up time	Time when the VC last goes Up.
VC total up time	Total Up time of a VC.
Secondary	Information about the secondary PW.

12.11.11 display mpls label-stack vll interface

Function

The **display mpls label-stack vll interface** command displays information about label stacks in VLL networking.

Format

display mpls label-stack vll interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about label stacks in VLL networking, run the **display mpls label-stack vll interface** command.

Example

Display information about the label stack on VLANIF100 in VLL networking.

```
<Huawei> display mpls label-stack vll interface vlanif 100
Label-stack  : 1
Level        : 1
Type         : VLL primary
Label        : 1027
Level        : 2
Type         : LDP
Label        : --
OutInterface : Vlanif1024
```

Table 12-120 Description of the **display mpls label-stack vll interface** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of labels
Type	Tunnel type
Label	Value of the outgoing label
OutInterface	Outbound interface

12.11.12 display mpls static-l2vc

Function

The **display mpls static-l2vc** command displays information about static VCs on the device.

Format

display mpls static-l2vc [*vc-id* | **interface** *interface-type interface-number* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
vc-id	Displays information about a static VC with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about all static PWs on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you run the **display mpls static-l2vc** command with the interface name specified, information about static VCs on the interface connected to a CE is displayed. If no interface is specified, information about static VCs on all interfaces is displayed.

Example

Display information about static VCs on the device.

```
<Huawei> display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy Name   : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
```

```
VC tunnel/token info : 1 tunnels/tokens
NO.0  TNL type       : lsp    , TNL ID : 0x800802
Backup TNL type      : lsp    , TNL ID : 0x0
Create time          : 0 days, 1 hours, 44 minutes, 19 seconds
UP time              : 0 days, 1 hours, 44 minutes, 19 seconds
Last change time     : 0 days, 1 hours, 44 minutes, 19 seconds
VC last up time      : 2011/09/22 15:48:06
VC total up time     : 0 days, 1 hours, 44 minutes, 19 seconds
CKey                 : 10
NKey                 : 9
BFD for PW           : unavailable
```

Table 12-121 Description of the **display mpls static-l2vc** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up ● down
VC State	Status of the VC: ● up ● down
VC ID	ID of the VC, which uniquely identifies a VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Label Status	Whether the label can be used: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token Status	Whether the token can be used: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Control Word	Whether the control word function is enabled: ● enable ● disable
VCCV Capability	Whether VCCV is enabled.
active state	Whether the PW is in active state. A PW in active state can forward packets. ● active ● inactive
Link State	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● OAM status
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
VC Tunnel/token info	Displays information about the VC tunnel or token ("1 tunnels/tokens" indicates that the PW uses one tunnel or token).
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
NO.0 TNL Type	Type of the tunnel used by the PW
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured.

Display information about static VCs on Ethernet1/0/0.

```
<Huawei> display mpls static-l2vc interface ethernet 1/0/0
 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capabilty       : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy        : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x3
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 1 hours, 55 minutes, 52 seconds
  UP time              : 0 days, 1 hours, 55 minutes, 52 seconds
  Last change time     : 0 days, 1 hours, 55 minutes, 52 seconds
  VC last up time      : 2011/09/22 15:48:06
  VC total up time     : 0 days, 1 hours, 55 minutes, 52 seconds
  CKey                 : 10
  NKey                 : 9
  Diffserv Mode        : uniform
  Service Class        : --
  Color                : --
  DomainId             : --
  Domain Name          : --
  BFD for PW           : unavailable
```

Table 12-122 Description of the **display mpls static-l2vc interface** command output

Item	Description
Client Interface	AC interface and its status.

Item	Description
AC Status	Status of the link between the PE and its directly connected CE.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	VC label sent by the local device.
Receive VC Label	VC label received by the local device.
Control Word	Whether the control word function is enabled.
VCCV Capabilty	Whether VCCV is enabled.
Tunnel Policy	Name of the tunnel policy. The value -- indicates that no tunnel policy is configured.
PW Template Name	Name of the PW template. The value -- indicates that no PW template is configured.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
VC tunnel/token info	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Diffserv Mode	QoS DiffServ mode for VLL services.
Service Class	QoS service class for VLL services.
Color	QoS color for VLL services.
DomainId	ID of a domain.
Domain Name	Name of a domain.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured.

Display information about SVCs in Up state between peers.

```
<Huawei> display mpls static-l2vc state up
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy Name   : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x56
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 1 hours, 56 minutes, 1 seconds
  UP time              : 0 days, 1 hours, 56 minutes, 1 seconds
  Last change time     : 0 days, 1 hours, 56 minutes, 1 seconds
  VC last up time      : 2011/09/22 15:48:06
  VC total up time     : 0 days, 1 hours, 56 minutes, 1 seconds
  CKey                 : 10
  NKey                 : 9
  BFD for PW           : unavailable
```

Table 12-123 Description of the **display mpls static-l2vc state** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.

Item	Description
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured.

Display information about the static VC configured on TDM interface.

```
<Huawei> display mpls static-l2vc
 Total svc connections:  1,  0 up,  1 down

 *Client Interface     : Serial2/0/0 is up
  AC Status            : up
  VC State             : down
  VC ID                : 112
  VC Type              : CESoPSN basic mode
  Destination          : 1.1.1.9
  Transmit VC Label    : 115
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : inactive
  Link State           : down
  Tunnel Policy Name   : --
  PW Template Name     : --
  TDM encapsulation number : 8
  jitter-buffer        : 8
  idle-code            : ff
  rtp-header           : disable
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
```

```
VC tunnel/token info : 0 tunnels/tokens
Backup TNL Type      : lsp   , TNL ID : 0x0
Create time          : 0 days, 0 hours, 0 minutes, 9 seconds
UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
Last change time     : 0 days, 0 hours, 0 minutes, 9 seconds
VC last up time      : 0000/00/00 00:00:00
VC total up time     : 0 days, 0 hours, 0 minutes, 0 seconds
CKey                 : 4
NKey                 : 3
BFD for PW           : unavailable
```

Table 12-124 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Whether the RTP header is added to the transparently transmitted TDM frame.

Related Topics

12.11.28 mpls static-l2vc

12.11.13 display mpls static-l2vc brief

12.11.13 display mpls static-l2vc brief

Function

The **display mpls static-l2vc brief** command displays brief information about static VCs on the device.

Format

display mpls static-l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls static-l2vc brief** command is recommended when a large number of static VCs are configured on the device.

Example

Display brief information about static VCs on the device.

```
<Huawei> display mpls static-l2vc brief
Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID               : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
```

Table 12-125 Description of the **display mpls static-l2vc brief** command output

Item	Description
Total SVC Connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
VC ID	ID of the static VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	IPv4 address of the peer. Generally, the value is the loopback address of the peer.

Display brief information about the static VC configured on a TDM interface.

```
<Huawei> display mpls static-l2vc brief
 Total svc connections:  1,  0 up,  1 down
```

```
*Client Interface     : Serial2/0/0 is up
 AC Status            : up
 VC State             : down
 VC ID                : 112
 VC Type              : CESoPSN basic mode
 Destination          : 1.1.1.9
 TDM encapsulation number : 8
 jitter-buffer            : 8
 idle-code                : ff
 rtp-header               : disable
```

Table 12-126 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Indicates Whether the RTP header is added to the transparently transmitted TDM frames.

Related Topics

12.11.28 mpls static-l2vc

12.11.7 display mpls l2vpn forwarding-info

12.11.14 display snmp-agent trap feature-name l2vpn all

Function

The **display snmp-agent trap feature-name l2vpn all** command displays all trap messages about the L2VPN module.

Format

display snmp-agent trap feature-name l2vpn all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used on TCP/IP networks. It uses a central computer (a network management station) that runs network management software to manage network elements. The management agent on the network element automatically reports traps to the network management station. After that, the network administrator immediately takes measures to resolve the problem.

The **display snmp-agent trap feature-name l2vpn all** command displays whether all trap functions of the L2VPN module are enabled.

Example

Display all trap messages about the L2VPN module.

```
<Huawei> display snmp-agent trap feature-name l2vpn all
-----------------------------------------------------------------------------
Feature name: L2VPN
Trap number : 14
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwCCCVcDown                     off                     on
hwCCCVcUp                     off                     on
hwPWVcDeleted                   off                     on
hwPWVcDown                      off                     on
hwPWVcUp                      off                     on
hwPWVcSwitchWtoP                off                     on
hwPWVcSwitchPtoW                off                     on
hwSvcDeleted                  off                     on
hwSvcDown                     off                     on
hwSvcUp                     off                     on
hwPWVcBackup                    off                     on
hwSvcSwitchWtoP                 off                     on
hwSvcSwitchPtoW                 off                     on
hwPWVcStatusChange              off                     on
```

Table 12-127 Description of the **display snmp-agent trap feature-name l2vpn all** command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.

Item	Description
Trap name	Name of a trap message about the L2VPN module: ● hwCCCVcDown: indicates a Huawei private trap in case the status of the CCC VC changes to Down. ● hwCCCVcUp: indicates a Huawei private trap in case the status of the CCC VC changes to Up. ● hwPWVcDeleted: indicates a Huawei-specific trap in the event that a PWE3 VC is deleted. ● hwPWVcDown: indicates a Huawei private trap in case the status of the PWE3 VC changes to Down. ● hwPWVcUp: indicates a Huawei private trap in case the status of the PWE3 VC changes to Up. ● hwPWVcSwitchWtoP: indicates a Huawei private trap in case the primary PWE3 PW is switched to the secondary PW. ● hwPWVcSwitchPtoW: indicates a Huawei private trap in case the secondary PWE3 PW is switched to the primary PW. ● hwSvcDeleted: indicates a Huawei-specific trap in the event that an SVC is deleted. ● hwSvcDown: indicates a Huawei private trap in case the status of the SVC changes to Down. ● hwSvcUp: indicates a Huawei private trap in case the status of the SVC changes to Up. ● hwPWVcBackup: indicates a Huawei private trap in case the status of the PWE3 VC changes to Backup. ● hwSvcSwitchWtoP: indicates that an SVC PW changes from the secondary state to the primary state. ● hwSvcSwitchPtoW: indicates that an SVC PW changes from the primary state to the secondary state. ● hwPWVcStatusChange: indicates that the status of the PWE3 VC change.
Default switch status	Default status of the trap function: ● on: indicates that the trap default function is enabled. ● off: indicates that the trap default function is disabled.
Current switch status	Current status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.11.30 snmp-agent trap enable feature-name l2vpn

12.11.15 display virtual-ethernet ve-group

Function

The **display virtual-ethernet ve-group** command displays the binding relationship between Virtual Ethernet (VE) interfaces and a VE-Group.

Format

display virtual-ethernet ve-group [*ve-group-id*]

Parameters

Parameter	Description	Value
ve-group-id	Specifies the ID of a VE-Group.	The value is an integer that ranges from 1 to 8192.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a device is configured with many VE-Groups, you can use the command to view the relationship between VE interfaces and VE-Groups.

Example

Display the binding relationship between all VE interfaces and VE-Groups on a Router.

```
<Huawei>display virtual-ethernet ve-group
 Ve-groupID    TerminateVE              AccessVE
 1             Virtual-Ethernet1/0/0(L2)  Virtual-Ethernet1/0/1(L3)
 5             Virtual-Ethernet2/0/0(L2)  Virtual-Ethernet2/0/1(L3)
Total 2, 2 printed
```

Table 12-128 Description of the **display virtual-ethernet ve-group** command output

Item	Description
Ve-groupID	Number of a VE-Group
TerminateVE	L2VE interface terminating the L2VPN

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AccessVE	L3VE interface accessing an L3VPN

Related Topics

5.20.12 interface virtual-ethernet

12.11.32 ve-group

12.11.16 display vll ccc

Function

The **display vll ccc** command displays information about a CCC connection.

Format

display vll ccc [*ccc-name* | **type local**]

Parameters

Parameter	Description	Value
ccc-name	Specifies the connection name.	The value is an existing connection name.
type	Specifies the CCC connection type.	-
local	Displays local CCC connections.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a CCC connection is configured, you can use the **display vll ccc** command to see whether the configuration is successful.

If you do not specify a connection name or type, information about all the existing CCC connections is displayed.

Example

Display a specified CCC connection.

```
<Huawei> display vll ccc CE1-CE2
name: CE1-CE2, type: local, state: up
```

```
intf1: GigabitEthernet0/0/1 (up ethernet),access-port: false

intf2: GigabitEthernet0/0/2 (up ethernet),access-port: false
no control word
VC last up time : 2012/09/10 14:28:24
VC total up time: 0 days, 0 hours, 1 minutes, 41 seconds
```

Display information about all the CCC connections.

```
<Huawei> display vll ccc
total  ccc vc : 1
local  ccc vc : 1,  1 up
remote ccc vc : 0,  0 up

name: CE1-CE2, type: local, state: up,
intf1: GigabitEthernet0/0/1 (up), access-port: false

intf2: GigabitEthernet0/0/2 (up), access-port: false
VC last up time : 2012/09/10 14:28:24
VC total up time: 0 days, 0 hours, 0 minutes, 10 seconds
```

Table 12-129 Description of the display vll ccc command output

Item	Description
total ccc vc	Total number of CCC local connections and remote connections at the local end.
local ccc vc	The number of CCC local connections at the local end.
remote ccc vc	The number of CCC remote connections at the local end.
name	Name of CCC connection in a character string.
type	Types of CCC connections. ● local: connection between two CEs that are connected to the same PE. ● remote: connection between CEs that are connected to two different PEs.
state	Status of a CCC connection: ● down: indicates that the CCC connection fails because the configuration is incorrect or the associated interface is Down. ● up: indicates that the CCC connection is set up successfully.
intf	Interface connected to the CCC connection.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Access-port	Whether the interface supports the access-port attribute. ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
VC last up time	Indicates the last time the VC was Up.
VC total up time	Indicates the total duration the VC is Up.

Display information about all the local CCC connections.

```
<Huawei> display vll ccc type local
total local  ccc vc : 1,  1 up

name: CE1-CE2, type: local, state: up,
intf1: GigabitEthernet0/0/2 (up),  access-port: false

intf2: GigabitEthernet0/0/1 (up),  access-port: false
VC last up time : 2011/09/21 22:17:44
VC total up time: 0 days, 0 hours, 8 minutes, 43 seconds
```

Related Topics

12.11.2 ccc interface out-interface

12.11.3 display l2vpn ccc-interface vc-type

12.11.17 l3ve track oam-state

Function

The **l3ve track oam-state** command enables the association between the L3VE interface status and the OAM status.

The **undo l3ve track oam-state** command disables the association between the L3VE interface status and the OAM status.

By default, the association between the L3VE interface status and the OAM status is disabled.

Format

l3ve track oam-state

undo l3ve track oam-state

Parameters

None

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In L2VPN accessing L3VPN scenarios in which PW protection is configured, if OAM (BFD, MPLS OAM, or MPLS-TP OAM) detects that services are interrupted between routers, OAM does not trigger the L3VE interface to withdraw reverse routes. Therefore, reverse traffic is still forwarded along the faulty PW until route convergence is complete, which causes traffic loss. To resolve this problem, run the **l3ve track oam-state** command to enable the association between the L3VE interface status and the OAM status. The L3VE interface then can identify the OAM status and have its status consistent with the OAM status. This prevents traffic loss.

Precautions

The **l3ve track oam-state** command applies only to the 1:1 mode and not to the N:1 mode.

- In 1:1 mode, one L2VE sub-interface is bound to one L3VE interface.
- In N:1 mode, N L2VE sub-interfaces are bound to one L3VE interface.

Example

Enable the association between the L3VE interface status and the OAM status.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 3/0/1.1
[Huawei-Virtual-Ethernet3/0/1.1] l3ve track oam-state
```

Related Topics

12.12.29 pw-template

12.11.18 l3ve track pw-state

12.11.18 l3ve track pw-state

Function

The **l3ve track pw-state** command associates the L3VE interface status with the PW status.

The **undo l3ve track pw-state** command disassociates the L3VE interface status from the PW status.

By default, the L3VE interface status is not associated with the PW status.

 Copyright © Huawei Technologies Co., Ltd.

Format

l3ve track pw-state

undo l3ve track pw-state

Parameters

None

Views

VE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the L2VPN access L3VPN solution, if the primary and secondary PWs have been established and corresponding L3VE interfaces have gone Up when the primary router recovers, the downstream traffic may switch back to the primary router. However, if the downstream traffic switches back to the primary router before the primary/secondary PW switchover is complete, the downstream traffic may be temporarily dropped. To solve this problem, run the **l3ve track pw-state** command to associate the L3VE interface status with the PW status.

The **l3ve track pw-state** command associates the L3VE interface status with the PW status. Then, the L3VE interface can keep its status consistent with the PW status by detecting the active/standby status of the PW so that the traffic on the RNC can be properly switched between the master and backup routers.

Precautions

This command can be configured only on the VE sub-interface.

Example

Associate the L3VE interface status with the PW status.

```
<Huawei> system-view
[Huawei] interface Virtual-Ethernet 3/0/1.1
[Huawei-Virtual-Ethernet3/0/1.1] l3ve track pw-state
```

Related Topics

12.12.29 pw-template

12.11.19 manual-set pw-ac-fault

Function

The **manual-set pw-ac-fault** command simulates a fault on the primary or secondary PW.

The **undo manual-set pw-ac-fault** command cancels the fault that is simulated on a primary or secondary PW.

By default, no fault is simulated on a PW.

Format

manual-set pw-ac-fault [**secondary**]

undo manual-set pw-ac-fault [**secondary**]

Parameters

Parameter	Description	Value
secondary	Simulates a fault on the secondary PW. If this parameter is not specified, a fault is simulated on the primary PW.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where the primary and secondary PWs need to be configured, you can run the **manual-set pw-ac-fault** command to simulate a fault on the primary or secondary PW to check whether services can be switched between the primary and secondary PWs.

Prerequisites

A VC has been created.

Example

Simulate a fault on the PW.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] mpls l2vc 2.2.2.2 100
[Huawei-Vlanif10] manual-set pw-ac-fault
```

 Copyright © Huawei Technologies Co., Ltd.

12.11.20 mpls l2vc

Function

The **mpls l2vc** command creates a Martini VLL.

The **undo mpls l2vc** command deletes the Martini VLL from an interface.

By default, no Martini L2VPN connection is created.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc [**secondary**]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies a L2VC ID.	The value is an integer that ranges from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tunnel-policy *policy-name*	Specifies a tunnel policy name for the L2VC. If no name is specified for a tunnel policy, the default tunnel policy is used. The LSP tunnel is preferred and only one LSP is used for load balancing in the default tunnel policy. If the name of the tunnel policy is specified but no tunnel policy is configured, the default tunnel policy is still used.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Removes the service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
secondary	Indicates that the VC is a secondary VC. If this parameter is not specified, a primary VC is created. You can configure a secondary VC only when the primary VC exists on the local device.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Martini VLL networking, you can run this command to create a VC connection for a Martini VLL.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You must create dynamic VCs on PEs at both ends of a PW to connect the PEs. The destination address of a VC is the LSR ID of the peer PE.
- You can set attributes for a PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring an LDP PW, you can directly apply the PW template without specifying attributes for the PW. After setting attributes for a PW template, you can update the PW template at any time. The modified PW template takes effect only after the **reset pw** command is run.
- If a PW attribute is specified in the **mpls l2vc** command, the corresponding PW attribute in the same PW template is invalid.
- If you do not specify a tunnel policy for a Martini connection, the default tunnel policy is used. By default, the LSP tunnel is preferentially selected and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- The parameters **raw** and **tagged** can be used only for Ethernet links.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the router and other devices.
- You must configure the primary PW before configuring the secondary PW and delete the secondary PW before deleting the primary PW.
- When creating VCs dynamically, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

Example

Create a Martini connection on the VLANIF interface.

```
<Huawei> system-view
[Huawei] vlan batch 10
[Huawei] interface vlanif 10
[Huawei-Vlanif10] mpls l2vc 10.2.2.9 100
```

Related Topics

12.11.4 display mpls l2vc
12.11.7 display mpls l2vpn forwarding-info

12.11.21 mpls l2vpn

Function

The **mpls l2vpn** command enables MPLS L2VPN and displays the MPLS L2VPN view.

The **undo mpls l2vpn** command disables MPLS L2VPN and deletes all the L2VPN configurations.

By default, the MPLS L2VPN function is disabled.

Format

mpls l2vpn

undo mpls l2vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MPLS L2VPN functions or perform configurations in the MPLS L2VPN view on the MPLS L2VPN network, run the **mpls l2vpn** command to enable MPLS L2VPN and enter the MPLS L2VPN view.

Prerequisites

Basic MPLS functions have been configured. For details, see the **mpls lsr-id** and **mpls** commands.

Precautions

When the command is configured, a P device does not need to be enabled with the MPLS L2VPN function.

After the **mpls l2vpn** command is executed:

- If MPLS L2VPN is disabled on the device, MPLS L2VPN is enabled and the MPLS L2VPN view is displayed.

 Copyright © Huawei Technologies Co., Ltd.

- If MPLS L2VPN is enabled on the device, the MPLS L2VPN view is displayed.

Example

Enable MPLS L2VPN.

```
<Huawei> system-view
[Huawei] mpls lsr-id 10.1.1.1
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls l2vpn
[Huawei-l2vpn]
```

12.11.22 mpls l2vpn default martini

Function

The **mpls l2vpn default martini** command configures the dynamic VC signaling not to carry status information.

The **undo mpls l2vpn default martini** command restores the default configuration.

By default, the dynamic VC signaling carries status information.

Format

mpls l2vpn default martini

undo mpls l2vpn default martini

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

To configure the dynamic VC signaling not to carry status information in VLL scenarios, run the **mpls l2vpn default martini** command. In other scenarios, do not run this command.

NOTE

- If the dynamic VC signaling carries status information, the local end can send Notification messages to the peer end. For details about Notification messages, see Chapter "PWE3 Principles" in the "PWE3 Configuration".
- Before using the **mpls l2vpn default martini** command, you must delete the configurations of VCs (including PWE3 VCs and VPLS VCs) that support Notification messages.

Example

Configure the dynamic VC signaling not to carry status information.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn default martini
```

Restore the default dynamic VC signaling configuration.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] undo mpls l2vpn default martini
```

Related Topics

12.11.21 mpls l2vpn

12.11.23 mpls l2vpn frag

Function

The **mpls l2vpn frag** command enables fragmentation of L2VPN IPv4 packets.

The **undo mpls l2vpn frag** command disables fragmentation of L2VPN IPv4 packets.

By default, fragmentation of L2VPN IPv4 packets is disabled.

Format

mpls l2vpn frag

undo mpls l2vpn frag

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AR router communicates with another device, packet transmission between them may fail if the AR does not fragment packets, in which case the packet length may exceed the MTU value of the other device. To ensure normal packet transmission, configure the **mpls l2vpn frag** command to fragment packets.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

MPLS L2VPN has been enabled on the interface.

Precautions

After the **mpls l2vpn frag** command is executed, the AR fragments IPv4 packets based on the MTU value on the tunnel's public network interface.

Example

Enable the packet fragmentation function.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vpn frag
```

12.11.24 mpls l2vpn oam-mapping

Function

The **mpls l2vpn oam-mapping** command enables the mapping between the AC status and the Packet Switching Network (PSN) status.

The **undo mpls l2vpn oam-mapping** command disables the mapping between the AC status and the PSN status.

By default, the mapping between the AC status and the PSN status is disabled.

Format

mpls l2vpn oam-mapping 3ah

undo mpls l2vpn oam-mapping

Parameters

Parameter	Description	Value
3ah	Enables fault detection and fault notification defined in IEEE 802.3ah.	-

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLL FRR or PWE3 FRR scenarios, PEs and CEs do not advertise their primary/secondary status and link status to each other. PW OAM and AC OAM need to be configured to monitor PW and AC status respectively. OAM mapping is enabled on the PEs to associate PW OAM with AC OAM.

After the **mpls l2vpn oam-mapping** command is configured on a PE, the system generates the mapping table between the AC status and the PSN status. If a fault occurs on an AC, the local PE will notify the remote PE of the AC fault. If a fault occurs on a PW, the local PE will notify the local CE of the fault. Timely fault notification allows PEs and CEs to coordinate with each other to implement end-to-end FRR.

Prerequisites

OAM fault detection and notification have been configured for the corresponding AC.

Configuration Impact

After the mapping between the AC status and the PSN status is enabled, if a fault occurs on the local AC:

- If BFD for PW is enabled, the local AC notifies the remote PE of the AC fault using BFD and the signaling protocol.
- If BFD for PW is disabled, the local AC notifies the remote PE of the AC fault using the signaling protocol.

Follow-up Procedure

After configuring this command, run the **display mpls l2vc interface** command to check the AC link status. The AC link status is displayed in the **Local AC OAM State** field of the command output.

Example

Enable fault detection and notification defined in IEEE 802.3ah on an Ethernet interface.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.1 101
[Huawei-GgiabitEthernet1/0/0] mpls l2vpn oam-mapping 3ah
```

Related Topics

12.11.6 display mpls l2vc oam-mapping

12.11.25 mpls l2vpn reroute

Function

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

The **undo mpls l2vpn reroute** command restores the default revertive switchover policy.

By default, delayed revertive switchover is configured in FRR or PW redundancy master/slave mode.

Format

mpls l2vpn reroute { { **delay** *delay-time* | **immediately** } [**resume** *resume-time*] | **never** }

undo mpls l2vpn reroute

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies the revertive switchover policy for the primary and secondary PWs as delayed revertive switchover, and sets the duration for delayed switchover.	The value is an integer that ranges from 10 to 1800, in seconds. The default value is 30.
immediately	Specifies the revertive switchover policy for the primary and secondary PWs as immediate revertive switchover.	-
resume *resume-time*	Specifies a delay after which the local device notifies the peer PE on the secondary PW of the recovery. You can set this parameter only in VLL FRR mode.	The value is an integer that ranges from 0 to 600, in seconds. The default value is 10.
never	Specifies the revertive switchover policy for the primary and secondary PWs to none revertive switchover. After the primary PW recovers, traffic is not switched to it until the secondary PW is faulty.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

Prerequisites

The primary and secondary PWs have been configured in FRR or PW redundancy master/slave mode. The revertive switchover policy cannot be configured for PW redundancy independent mode.

Precautions

In VLL FRR mode and in PW redundancy master/slave mode, the PW revertive switchover policy is classified into the following modes:

- Immediate revertive switchover: When the primary PW recovers from a fault, the local PE switches traffic back to the primary PW immediately and notifies

the peer PE on the secondary PW of the fault. In FRR mode, the local PE notifies the peer PE on the secondary PW of the recovery after a delay of *resume-time*. In PW redundancy master/slave mode, the parameter *resume-time* is not supported.

This revertive switchover applies to scenarios in which users hope traffic to be restored as soon as possible.

- Delayed revertive switchover: When the primary PW recovers from a fault, traffic is switched back to the primary PW after a period specified by *delay-time*. After traffic is switched back, the local device immediately notifies the peer device on the secondary PW of the fault. If *resume-time* is configured in FRR mode, the local device notifies the peer device on the secondary PW of the recovery after a delay of *resume-time*.

  On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.

- None revertive switchover: When the primary PW recovers from a fault, traffic is not switched back to the primary PW until the secondary PW becomes faulty.

  If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive switchover.

In a CE asymmetrical networking, if the Ethernet OAM function is configured on a PE interface connected to a CE, and a revertive switchover policy is configured, the value of *resume-time* cannot be 0 seconds. The value must be equal to or greater than 1 second.

Example

Configure the device to switch traffic back to the primary PW 15 seconds after the primary PW recovers from a fault, notify the peer PE on the secondary PW of the fault when a switchover is performed, and notify the peer PE of the secondary PW of the recovery 20 seconds later.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.9 100
[Huawei-GigabitEthernet1/0/0] mpls l2vc 2.2.2.9 200 secondary
[Huawei-GigabitEthernet1/0/0] mpls l2vpn reroute delay 15 resume 20
```

Related Topics

12.11.20 mpls l2vc

12.11.26 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL service.

The **undo mpls l2vpn service-name** command deletes the configured L2VPN service name.

By default, no L2VPN service name is configured in the system.

Format

mpls l2vpn service-name *service-name*

undo mpls l2vpn service-name

Parameters

Parameter	Description	Value
service-name	Specifies the name of an L2VPN service. This parameter uniquely identifies an L2VPN service on a PE.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an SVC or Martini VLL service is uniquely identified by the combination of the VC ID and VC type, which are hard to remember and make maintenance complex. When a service name is used to uniquely identify an L2VPN service, the name can be defined based on requirements and the NMS operator can maintain the L2VPN service by clicking the name on the NMS graphical user interface (GUI). This simplifies operation and maintenance.

Prerequisites

An SVC or Martini VLL service has been configured on a service interface. A primary PW and a secondary PW can be configured for a Martini VLL or PWE3 service.

Precautions

On each PE, an L2VPN service name is unique. If an L2VPN service name has been used by a PW, it cannot be configured for another PW, or the system will display an error message.

If an L2VPN service already has a service name, this service name will be overwritten when a new name is configured for the L2VPN service. Therefore, when changing an L2VPN service name, you can directly configure a new service name without deleting the original one.

- Because the primary and secondary PWs are configured on the same interface, they are regarded as one PW, and a service name is configured for both of them.

 Copyright © Huawei Technologies Co., Ltd.

- On each PE, an L2VPN service name is unique.
- The **mpls l2vpn service-name** command cannot be run on a loopback interface.

Example

Set an L2VPN service name to **pw1** on a service interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 10.1.1.1 1
[Huawei-GigabitEthernet1/0/0] mpls l2vpn service-name pw1
```

Related Topics

12.11.2 ccc interface out-interface

12.11.27 mpls l2vpn vccv bfd-cv-negotiation fault-detection-only

Function

The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type for BFD CV packets to be sent to remote peers.

The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default configuration.

By default, the device sends BFD CV packets with the encapsulation type 0x08 to all remote peers.

Format

mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address* { **enable** | **disable** }]

undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address*]

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the IP address of a remote peer.	The value is in dotted decimal notation.
enable	Sets the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
disable	Set the encapsulation type 0x08 for BFD CV packets to be sent to a specified remote peer.	-

Views

MPLS L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Virtual Circuit Connectivity Verification (VCCV) is a mechanism to detect and diagnose end-to-end faults on PWs. VCCV provides a control channel between a PW's ingress and egress over which connectivity verification (CV) messages can be sent. A VCCV message includes a BFD control packet encapsulated as specified by the CV type. A BFD CV packet can be transmitted over a VCCV control channel after being encapsulated using BFD IP/UDP. BFD IP/UDP encapsulation for BFD CV packets are classified into two types:

- 0x04: used only for PW fault detection.
- 0x08: used for PW fault detection and AC/PW status signaling.

To control the encapsulation type of BFD CV packets to be sent to remote peers, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command.

- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to all remote peers.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default encapsulation type 0x08 for BFD CV packets to be sent to all remote peers.
- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **enable** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to a specified remote peer.
- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **disable** command sets the encapsulation type to 0x08 for BFD CV packets to be sent to a specified remote peer.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* command restores the global encapsulation type for BFD CV packets to be sent to a specified remote peer.

Dynamic PWs support VCCV by default, and can use LDP signaling to advertise local attributes to remote peers. The default encapsulation type of BFD CV packets is 0x08. If a remote peer supports the encapsulation type 0x04 and BFD is used for communication, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-**

only peer *peer-address* **enable** command to change the encapsulation type of BFD CV packets to be sent to this peer to 0x04.

Precautions

After this command is run, PWs may be re-established, which causes a short service interruption.

Example

Set the encapsulation type 0x04 for BFD CV packets to be sent to remote peers.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only
```

Set the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer 10.10.10.1 enable
```

12.11.28 mpls static-l2vc

Function

The **mpls static-l2vc** command creates a static VC.

The **undo mpls static-l2vc** command deletes the static VCs.

By default, no static VC is created.

Format

mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

undo mpls static-l2vc [**secondary**]

undo mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.

Parameter	Description	Value
pw-template *pw-template-name*	Specifies the name of a static PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.
transmit-vpn-label *transmit-label-value*	Specifies the value of a transmit label.	The value is an integer that ranges from 0 to 1048575.
receive-vpn-label *receive-label-value*	Specifies the value of a receive label.	The value is an integer that ranges from 16 to 1023.
tunnel-policy *tnl-policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word | **no-control-word**	Enables or disables the control word function. By default, the control word function is disabled.	-
raw	Removes the service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
idle-code *idle-code-value*	Specifies the idle code that is filled in manually when a jitter buffer underflow occurs. This parameter is required when the AC is a TDM link.	The value ranges from 00 to FF, in hexadecimal notation. The default value is FF.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
jitter-buffer *depth*	Specifies the depth of the jitter buffer, that is, the allowed maximum jitter delay. This parameter is required when the AC is a TDM link.	The value is an integer that ranges from 4 to 64, in milliseconds. The default value is 8 ms.
tdm-encapsulation *number*	Specifies the number of TDM frames encapsulated in a CESoPSN packet. This parameter is required when the AC is a TDM link.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.
tdm-sequence-number	Sets the sequence number of the first frame encapsulated for TDM transparent transmission to 1. This parameter is required when the AC is a TDM link.	-
secondary	Configures the PW as a static secondary PW. By default, a created PW is a primary PW.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an L2VPN networking, you can use this command to create a static VC between two PEs connected to CEs.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You can set attributes for a static PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring a static PW, you can directly use the static PW template without specifying attributes for the PW. After setting attributes for a static PW template, you can update the static PW template at any time. The modified static PW template takes effect only after the **reset pw** command is run.
- Static VCs must be created on PEs at both ends. The destination address of a VC is the LSR ID of the peer PE. The transmit label of the PE at one end is the receive label of the PE at the other end. If the labels do not match, traffic may fail to be forwarded even though the **static-l2vc** field is displayed as Up.
- If no tunnel policy is specified, the default tunnel policy is used. The default policy specifies that traffic is forwarded along the LSP and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- When configuring a static VC, note that the value of the transmit label ranges from 0 to 1048575. This ensures the communication between the device and different types of devices.
- When creating static VCs, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

Example

Configure a static VC. Set the LSR ID of the peer device to 1.1.1.1, transmit label to 100, and receive label to 100.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100 receive-vpn-label 100
```

Delete a static VC.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] undo mpls static-l2vc
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.11.12 display mpls static-l2vc
12.11.21 mpls l2vpn

12.11.29 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** [**remote** *remote-ip-address peer-pw-id* | **draft6**] * [**ttl** *ttl-value*] [**uniform**]

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word remote** *remote-ip-address peer-pw-id* **sender** *sender-address* [**ttl** *ttl-value*] [**uniform**]

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address* | **draft6**] * [**uniform**]

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **normal** [**no-control-word**] [**remote** *remote-ip-address peer-pw-id*] [**ttl** *ttl-value*] [**uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
-c *echo-number*	Specifies the number of Echo Request messages to be sent. If the network works unstably, you can set this parameter to a larger value to test network quality based on the packet loss ratio.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-m *time-value*	Specifies the interval for sending Echo Request messages. Each time after the source sends an Echo Request message by using the **ping vc** command, it waits a period of time (2000 ms by default) before sending the next Echo Request message. You can set the interval for sending Echo Request messages through the parameter *time-value*. If the network works unstably, the value should be larger than or equal to 2000 ms.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-s *data-bytes*	Specifies the number of bytes of the sent Echo Request messages.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100. The value must be smaller than the MTU value of the interface.
-t *timeout-value*	Specifies the timeout period for sending Echo Request messages.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-exp *exp-value*	Specifies the EXP value of the sent Echo Request messages.	The value is an integer that ranges from 0 to 7. The default value is 0.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply messages. ● 1: No MPLS Echo Reply message is returned. ● 2: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply messages are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-v	Displays the detailed information.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-control-word	Disables the control word function.	-
control-word	Enables the control word function. The switching node along a multi-segment PW does not transmit ping packets. When the control word function is enabled, you can ping only the termination node of the PW. Before using the control word to ping the PW, you must enable the control word for a PW.	-
remote	Specifies information about the PW on the remote PE. Information specified by the remote PE is finally encapsulated into the ping packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the ping packets is the information about the PW on the local end, which applies to single-segment PWs.	-
peer-pw-id	Specifies the ID of the PW on the peer.	The value is an integer that ranges from 1 to 4294967295. By default, the peer PW ID is the same as the local PW ID.
draft6	Specifies the version of the **ping vc** command. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06".	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. In the case of a multi-segment PW, if the ping operation is performed in control word mode, the IP address of the termination node must be specified. In MPLS router alert mode, the IP address of any switching node or the termination node can be specified. Then, the Echo Request message is sent to the peer and then sent back.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
label-alert	Specifies the label alert mode. The switching node along a multi-segment PW sends ping packets forcibly. In MPLS router alert mode, you can ping any switching node along the PW.	-
normal	Specifies the normal mode, that is, the TTL detection mode. In this mode, control word and router alert are not encapsulated in to MPLS Echo Request messages, and TTL values are used to detect PW connectivity.	-
ttl *ttl-value*	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default value is 64.
sender *sender-address*	Specifies a source address. For end-to-end detection of a multi-segment PW, a source IP address needs to be specified for a public network device that communicates with the remote PE. Generally, the source IP address is the address of the adjacent SPE or UPE.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. The **ping vc** command can be used to check a PW in the following scenarios:

VLL networking

Based on VLL types, the VLL PW ping can be classified into the following types:

- PWE3 VLL PW ping: In a PWE3 VLL networking, a PW ping is initiated to check the connectivity of a PW. A PWE3 VLL PW ping can be performed in control word mode, TTL mode, or label alert mode. In a ping test, a local PE sends an Echo Request message to the peer PE. After receiving the message, the peer PE abstracts and sends FEC information to the L2VPN module to determine whether the message has reached the egress. If so, the peer PE returns an Echo Reply message.

If a PW fault is detected by using the **ping vc** command, the **tracert vc** command can be used to locate the fault. Both the **ping vc** command and the **tracert vc** command can properly check the connectivity of PWs and locate faults.

Prerequisites

The MPLS module has been enabled on the device and works properly.

Precautions

control-word is recommended to detect an entire PW. Even though **label-alert** can be used to check the entire PW, the whole process is the same as the forwarding process only when **control-word** is used.

The execution of the **ping vc** command terminates when either of the following situations occurs:

- The ping packet reaches the egress.
- The TTL value of the ping packet reaches the upper threshold.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

Run the **ping vc** command in label alert mode on the device to check the connectivity of an Ethernet PW.

```
<Huawei> ping vc ethernet 100 -c 10 -m 10 -s 65 -t 100 -v label-alert remote 2.2.2.2
  Reply from 2.2.2.2: bytes=65 Sequence=1 time = 31 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=2 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=3 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=4 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=5 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=6 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=7 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=8 time = 16 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=9 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=10 time = 32 ms Return Code 3, Subcode 1

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics
  10 packet(s) transmitted
  10 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/21/32 ms
```

Related Topics

12.11.31 tracert vc

12.11.30 snmp-agent trap enable feature-name l2vpn

Function

The **snmp-agent trap enable feature-name l2vpn** command enables the trap function for the L2VPN module.

The **undo snmp-agent trap enable feature-name l2vpn** command disables the trap function for the L2VPN module.

By default, the trap function is disabled for the L2VPN module.

Format

snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

undo snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

Parameters

Parameter	Description	Value
trap-name	Indicates the traps of L2VPN events of specified types.	-
hwcccvcdown	Enables or disables the trap indicating that the status of a CCC VC changes to Down.	-
hwcccvcup	Enables or disables the trap indicating that the status of a CCC VC changes to Up.	-
hwpwvcbackup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Backup.	-
hwpwvcdeleted	Enables or disables the trap indicating that a PWE3 VC is deleted.	-
hwpwvcdown	Enables or disables the trap indicating that the status of a PWE3 VC changes to Down.	-
hwpwvcstatuschange	Enables or disables the trap indicating that the status of a PWE3 VC changes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwpwvcswitchptow	Enables or disables the trap indicating that a PWE3 PW changes from the secondary state to the primary state.	-
hwpwvcswitchwtop	Enables or disables the trap indicating that a PWE3 PW changes from the primary state to the secondary state.	-
hwpwvcup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Up.	-
hwsvcdeleted	Enables or disables the trap indicating that an SVC is deleted.	-
hwsvcdown	Enables or disables the trap indicating that the status of an SVC changes to Down.	-
hwsvcswitchptow	Enables or disables the trap indicating that an SVC PW changes from the secondary state to the primary state.	-
hwsvcswitchwtop	Enables or disables the trap indicating that an SVC PW changes from the primary state to the secondary state.	-
hwsvcup	Enables or disables the trap indicating that the status of an SVC changes to Up.	-
hwVpwsPwRedundancyDegraded	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS degrades.	-
hwVpwsPwRedundancyDegradedClear	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS recovers.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

The L2VPN module is not configured with the function of excessive traps. To enable the traps of one or more events, specify **trap-name**.

Example

Enable the system to generate an alarm when a VC in CCC mode goes Down.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name l2vpn trap-name hwcccvcdown
```

Related Topics

12.11.14 display snmp-agent trap feature-name l2vpn all

12.11.31 tracert vc

Function

The **tracert vc** command detects the status of a PW or locates a faulty node on a PW in Down state.

Format

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-ip-address* [**ptn-mode** | **full-lsp-path**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-pw-id* **draft6** [**full-lsp-path**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**uniform**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0.	The value is an integer that ranges from 0 to 7.
-f *first-ttl*	Specifies the initial Time-to-Live (TTL).	The value is an integer that ranges from 1 to 255, and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from 1 to 255, and must be larger than the value of *first-ttl*. The default value is 30.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets. ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated in IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated in IPv4/IPv6 /IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4.
-t *timeout-value*	Specifies the timeout interval of an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
control-word	Indicates that the control word is encapsulated in the MPLS Echo Request packet.	-
label-alert	Indicates that the router alert label is encapsulated in the MPLS Echo Request packet.	-
no-control-word	Indicates that the control word is not encapsulated in the MPLS Echo Request packet.	-
normal	Indicates the normal mode where the router alert label and control word are not encapsulated in the MPLS Echo Request packet.	-
remote	Specifies information about the PW on the remote PE.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. If **label-alert** is configured, you can specify the IP address of any switching node or the termination node.	-
remote-pw-id	Specifies the ID of the remote PW. By default, the ID of the local PW is used. If the tracert operation is performed in control word mode for a multi-segment PW, the IP address of the termination node must be specified.	-
ptn-mode	Specifies the PTN mode.	-
full-lsp-path	Displays the responses from all nodes along the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, only the responses from the PW nodes along the LSP are displayed.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
draft6	Specifies the version of the **tracert vc** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". **NOTE** Tracert VC based on **draft6** is applied only to VLL over LDP scenarios.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a fault occurs on the PW, the **ping vc** command can be used to check the connectivity of the network, and the **tracert vc** command can be used to locate the fault and provide reference for fault diagnosis. If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. If a PW is down, the **tracert vc** command must be used to locate the faulty node on the PW.

Prerequisite

- The UDP module of each node works properly; otherwise, the tracert operation will fail.
- The MPLS module has been enabled on each node and works properly.
- The ICMP module of each node works properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert vc** command is as follows:

1. The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
2. The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
3. The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
4. The preceding steps continue until the MPLS Echo Request packet reaches the destination.

 Copyright © Huawei Technologies Co., Ltd.

When the device on each hop receives the MPLS Echo Request packet, it will respond with an MPLS Echo Reply packet, indicating that the tracert test ends. In the command output information of the source device, you can view the path that the packet passes through.

Configuration Impact

In control word mode, if a transit node receives an MPLS Echo Request packet whose TTL does not time out, it does not send the packet to the CPU. In this mode, the source obtains only a little PW information and cannot obtain information about the downstream devices of the transit node. This mode is recommended when the traffic volume is heavy.

In router alert mode, a transit node sends the received MPLS Echo Request packets to the CPU. In this mode, the source obtains a lot of PW information; therefore, device performance is affected when the traffic volume is heavy. This mode is recommended when the traffic volume is light.

Information specified by **remote** is encapsulated in MPLS Echo Request packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the MPLS Echo Request packets is about the PW on the local PE. This applies to single-segment PWs.

Precautions

- When the probe packet reaches the egress or the TTL reaches the upper threshold, the PW tracert is terminated.
- You can press **Ctrl + C** to terminate the execution of the **tracert vc** command.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

Trace a multi-segment PW. The encapsulation type, local PW ID, and remote PW ID of the PW is ethernet, 100, and 200.

```
<Huawei> tracert vc ethernet 100 control-word remote 200 draft6 full-lsp-path
 TTL   Replier          Time    Type      Downstream
 0                        Ingress   10.1.1.2/[1025 ]
 1     10.1.1.2         230 ms  Transit   10.2.1.2/[3 ]
 2     10.2.1.2         230 ms  Transit   10.3.1.2/[3 ]
 3     10.3.1.2         100 ms  Transit   10.4.1.2/[3 ]
 4     10.4.1.2         150 ms  Egress
```

Table 12-130 Description of the **tracert vc** command output

Item	Description
TTL	TTL value in an Echo Request packet. It represents the number of hops along the path through which an Echo Request packet passes.

Item	Description
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time when the packet is processed.
Type	Node type. The value can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

Related Topics

12.11.29 ping vc

12.11.32 ve-group

Function

The **ve-group** command sets a VE interface to work in multi-service access mode and binds the VE interface to a specified VE-Group.

The **undo ve-group** command sets a VE interface to common mode.

By default, VE interfaces work in common mode.

Format

ve-group *ve-group-id* { **l2-terminate** | **l3-access** }

undo ve-group

Parameters

Parameter	Description	Value
ve-group-id	Specifies the number of a VE-Group.	The value is an integer that ranges from 1 to 8192.
l2-terminate	Sets the VE interface as an L2VE that terminates the VLL.	-
l3-access	Sets the VE interface as an L3VE interface that accesses the MPLS L3VPN.	-

Views

VE interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Before using the **ve-group** command, if a VE interface is bound to a Permanent Virtual Circuit (PVC) that carries IPoEoA, you must disconnect the binding.

In L2VPN access to L3VPN scenarios:

- To change a VE interface to an L2VE interface, run the **ve-group** *ve-group-id* **l2-terminate** command on the VE interface.
- To change a VE interface to an L3VE interface, run the **ve-group** *ve-group-id* **l3-access** command on the VE interface.

In L2VPN access to L3VPN scenarios, a VE group has only one L2VE interface and one L3VE interface. L2VE interfaces can only work in Dot1q termination mode, L3VE interfaces can work in QinQ termination and Dot1q termination mode. L2VE and L3VE interfaces can have multiple sub-interfaces created for different VLAN services.

Example

Set VE 1/0/0 as an L2VE.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 1/0/0
[Huawei-Virtual-Ethernet1/0/0] ve-group 1 l2-terminate
```

Set the VE 1/0/1 as an L3VE.

```
<Huawei> system-view
[Huawei] interface virtual-ethernet 1/0/1
[Huawei-Virtual-Ethernet1/0/1] ve-group 1 l3-access
```

Related Topics

5.20.12 interface virtual-ethernet

12.12 PWE3 Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support PWE3.

12.12.1 bfd bind pw

Function

The **bfd bind pw** command configures a BFD session to detect a PW.

The **undo bfd** command deletes a specified BFD session.

By default, no BFD session is configured to detect a PW.

Format

bfd *cfg-name* **bind pw interface** *interface-type interface-number* [**secondary**]

undo bfd *cfg-name*

Parameters

Parameter	Description	Value
cfg-name	Specifies the name of the BFD session.	The value is a string of 1 to 15 case-insensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
interface *interface-type interface-number*	Specifies the type and number of the interface where the PW to be detected resides, namely, the AC interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
secondary	Indicates that the BFD session detects the secondary PW.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a transmission device exists on a direct link, BFD detects a link fault faster than a link detection mechanism on an interface. On networks demanding fast fault detection, run the **bfd bind pw** command to configure a BFD session to detect a PW.

Prerequisites

- A PW has been configured on an AC interface by running the **mpls l2vc** command.
- BFD has been enabled globally by running the **bfd** command.
- A single-segment or multi-segment PW has been configured.

Precautions

- When detecting a PW, BFD sessions must be bound to the source and destination ends of a PW.

 Copyright © Huawei Technologies Co., Ltd.

- You need to create a BFD session to detect primary and secondary PWs separately.

NOTE

When running the **bfd bind pw** command to detect a multi-segment PW, ensure that the first-segment PW is a VLL PW configured on a non-SPE node.

When running the **bfd bind pw** command to detect a single-segment PW, ensure that the single-segment PW is configured on a non-SPE node.

Example

Create a BFD session to detect a PW.

```
<Huawei> system-view
[Huawei] bfd pe2 bind pw interface vlanif 10
```

12.12.2 control-word

Function

The **control-word** command enables the control word in a PW template.

The **undo control-word** command disables the control word in a PW template.

By default, the control word is disabled in a PW template.

Format

control-word

undo control-word

Parameters

None

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

When load balancing is used, packets may be out of sequence when reaching the destination. The control word function can be used to put the packets into the correct order.

Example

Enable the control word in the PW template named **pwt**.

```
<Huawei> system-view
[Huawei] pw-template pwt
[Huawei-pw-template-pwt] control-word
```

Disable the control word in the PW template named **pwt**.

```
<Huawei> system-view
[Huawei] pw-template pwt
[Huawei-pw-template-pwt] undo control-word
```

Related Topics

12.12.29 pw-template

12.12.3 display mpls l2vc

Function

The **display mpls l2vc** command displays information about virtual circuits (VCs) in LDP mode.

Format

display mpls l2vc [*vc-id* | **interface** *interface-type interface-number* | **remote-info** [*vc-id* | **verbose**] | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface connected to the CE. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
remote-info	Displays information about the VC on the remote end.	-
vc-id	Displays static PW information with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays the detailed information about the VC on the remote end.	-
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc** command displays information about the VCs in LDP signaling mode, including the Martini VC and PWE3 VC.

- If the interface is specified, information about VCs on the specified AC interface is displayed.
- If **remote-info** is specified but *vc-id* is not specified, information about all VCs set up by the remote and local peers is displayed.

Example

Display information about all the LDP VCs configured on the router.

```
<Huawei> display mpls l2vc
 Total LDP VC : 1     1 up       0 down

 *client interface       : Vlanif1111 is up
  Administrator PW        : no
  session state           : up
  AC status               : up
  Ignore AC state         : disable
  VC state                : up
  Label state             : 0
  Token state             : 0
  VC ID                   : 101
  VC type                 : VLAN
  destination             : 10.3.3.9
  local VC label          : 1026         remote VC label      : 1026
  control word            : disable
  remote control word     : disable
  forwarding entry        : exist
  local group ID          : 0
  remote group ID         : 0
  local AC OAM State      : up
  local PSN OAM State     : up
  local forwarding state : forwarding
  local status code       : 0x0
  remote AC OAM state     : up
  remote PSN OAM state    : up
  remote forwarding state: forwarding
  remote status code      : 0x0
  ignore standby state    : no
  BFD for PW              : unavailable
  VCCV State              : up
  manual fault            : not set
  active state            : active
  link state              : up
  local VC MTU            : 1500         remote VC MTU        : 1500
  local VCCV              : alert ttl lsp-ping bfd
  remote VCCV             : alert ttl lsp-ping bfd
  tunnel policy name      : --
  PW template name        : --
  primary or secondary    : primary
  load balance type       : flow
  Access-port             : false
```

```
Switchover Flag        : false
VC tunnel/token info   : 1 tunnels/tokens
  NO.0  TNL type       : lsp    , TNL ID : 0x48000020
  Backup TNL type      : lsp    , TNL ID : 0x0
create time            : 0 days, 0 hours, 6 minutes, 50 seconds
up time                : 0 days, 0 hours, 6 minutes, 34 seconds
last change time       : 0 days, 0 hours, 6 minutes, 34 seconds
VC last up time        : 2013/09/24 18:23:35
VC total up time       : 0 days, 0 hours, 6 minutes, 34 seconds
CKey                   : 16
NKey                   : 15
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : uniform
Service Class          : be
Color                  : --
DomainId               : --
Domain Name            : --
```

Table 12-131 Description of the **display mpls l2vc** command output

Item	Description
Total LDP VC	Total number of established LDP VCs, including the number of LDP VCs in Up and Down state.
client interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface. This field can be displayed as **yes** or **no**. Currently, mPW is not supported on the device.
session state	Status of the LDP session established between both ends of the VC: ● up: The LDP session has been established. ● down: The LDP session is not established.
AC status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
Ignore AC state	Whether to ignore the impact of AC status changes on the active/standby PWE3 service status is enabled: ● enable ● disable
VC state	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token state	Token status: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
VC ID	ID of the VC, which uniquely identifies a VC. **NOTE** If the VC IDs on both ends are different, run the **mpls l2vc** command in the interface view to change the VC ID on one end to be the same as that on the other end.
VC type	Encapsulation type of the VC: ● VLAN ● Ethernet The PW can go Up only when the local and remote encapsulation types are the same.
destination	LSR ID of the VC peer device.
local VC label	Local VC label.
remote VC label	Remote VC label.
control word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.
forwarding entry	Whether forwarding entries exist.
local group ID	Local group ID.
remote group ID	Remote group ID.
manual fault	Whether a PW fault is simulated.
active state	Whether the PW is in active state. A PW in active state can forward packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link state	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● Status of the mPW associated with service PWs ● Status of the BFD session associated with service PWs ● PW state code ● PW status detected by VCCV ● OAM status
local VC MTU	MTU of the local VC.
remote VC MTU	MTU of the remote VC.
tunnel policy name	Name of the tunnel policy.
PW template name	Name of the PW template.
primary or secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
Switchover Flag	Whether a switchover has occurred.
create time	How long the VC has been created.
up time	How long the VC keeps the Up state. If the current PW status is Down, the value is 0.
last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AdminPw interface	AC interface on which the mPW is bound to the PW. The AC interface must be a loopback interface. This field is displayed only when the PW is not an mPW: ● Name of the loopback interface. ● --: indicates that the PW is not bound to an mPW.
AdminPw link state	Status of the mPW bound to the PW. This field is displayed only when the PW is not an mPW. This field can be displayed as: ● Up ● Down ● --: indicates that the PW is not bound to an mPW.
Diffserv Mode	QoS DiffServ mode.
Service Class	QoS service class.
Color	QoS color.
DomainId	ID of a domain.
Domain Name	Name of a domain.

Display LDP VC information about the AC interface.

```
<Huawei> display mpls l2vc interface ethernet 1/0/0
 *client interface       : Ethernet1/0/0 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 101
  VC type                : Ethernet
  destination            : 10.3.3.9
  local group ID         : 0            remote group ID      : 0
  local VC label         : 1024         remote VC label      : 1024
  local AC OAM State     : up
  local PSN OAM State    : up
  local forwarding state : forwarding
  local status code      : 0x0
  remote AC OAM state    : up
  remote PSN OAM state   : up
  remote forwarding state: forwarding
  remote status code     : 0x0
  ignore standby state   : no
  BFD for PW             : unavailable
  VCCV State             : up
  manual fault           : not set
  active state           : active
  forwarding entry       : exist
  link state             : up
```

```
local VC MTU           : 1500         remote VC MTU        : 1500
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable      remote control word  : disable
tunnel policy name     : --
PW template name       : --
primary or secondary   : primary
load balance type      : flow
Access-port            : false
Switchover Flag        : false
VC tunnel/token info   : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x5
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 29 minutes, 47 seconds
up time                : 0 days, 0 hours, 4 minutes, 54 seconds
last change time       : 0 days, 0 hours, 4 minutes, 54 seconds
VC last up time        : 2011/09/26 15:29:03
VC total up time       : 0 days, 0 hours, 4 minutes, 54 seconds
CKey                   : 5
NKey                   : 4
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : uniform
Service Class          : --
Color                  : --
DomainId               : --
Domain Name            : --
```

Table 12-132 Description of the **display mpls l2vc interface** command output

Item	Description
local AC OAM State	OAM status of the local AC. ● up ● down
local PSN OAM State	Status of the local device on the Packet Switch Network (PSN) side. ● up ● down
local forwarding state	Status of the local forwarding table. ● forwarding ● down
local status code	Status code of the local PW: ● 0x0: indicates that the local PW functions as the master PW and is in Up state. ● 0x20: indicates that the local PW functions as the backup PW and is in Up state. ● 0x1: indicates that the local PW functions as the master PW and is in Down state. ● 0x21: indicates that the local PW functions as the backup PW and is in Down state.

Item	Description
remote AC OAM state	OAM status of the remote AC. ● up ● down
remote PSN OAM state	Status of the remote device on the PSN side. ● up ● down
remote forwarding state	Status of the remote forwarding table. ● forwarding ● down
remote status code	Status code of the remote PW: ● 0x0: indicates that the remote PW functions as the master PW and is in Up state. ● 0x20: indicates that the remote PW functions as the backup PW and is in Up state. ● 0x1: indicates that the remote PW function as the master PW and is in Down state. ● 0x21: indicates that the remote PW function as the backup PW and is in Down state.
BFD for PW	Whether BFD for PW is enabled: ● available ● unavailable
VCCV State	Whether Virtual Circuit Connectivity Verification (VCCV) is enabled.
local VCCV	Type of VCCV supported on the local device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
remote VCCV	Type of VCCV supported on the remote device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
local control word	Whether the control word is enabled on the local device: ● Disable ● Enable
remote control word	Whether the control word is enabled on the remote device: ● Disable ● Enable
ignore standby state	Whether the status of the secondary PW is ignored.
VC Tunnel/token info: 1 tunnels/tokens	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
TNL type	Type of the tunnel used by the PW.
TNL ID	ID of the tunnel used by the PW.
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
PW redundancy mode	PW redundancy mode. By default, the mode is FRR. ● Independent: indicates that the PW is in negotiation mode. ● frr: indicates that the PW is in FRR mode. ● --: indicates that the PW is in master/slave mode.

Display the LDP VC information received from the remote peer.

```
<Huawei> display mpls l2vc remote-info
Total remote ldp vc : 1

Transport  Group      Peer          Remote        Remote     C   MTU/  N   S
VC ID      ID         Addr          Encap         VC Label   Bit CELLS Bit Bit
```

```
101        0          10.3.3.9        ethernet       1024       0   1500  0   0
```

Display the detailed LDP VC information received from the remote peer.

```
<Huawei> display mpls l2vc remote-info verbose
Total remote LDP VC : 1

VC ID              : 101
VC Type            : ethernet
VC Label           : 1024
Peer Address       : 10.3.3.9
Group ID           : 0
MTU                : 1500
Control Word       : 0
Notification       : 0
Status Code        : 0
Match Local VC     : MATCH
Max ATM CELLS      : --
TDM RTP Header     : --
TDM Encap Num      : --
TDM Bit Rate       : --
```

Table 12-133 Description of the **display mpls l2vc remote-info** command output

Item	Description
Total remote ldp vc	Total number of created remote LDP VCs.
Transport VC ID	VC ID, which uniquely identifies a VC.
Group ID	ID of the group to which the L2VPN belongs. The default value is 0.
Peer Addr and Peer Address	IP address of the remote peer.
Remote Encap	Encapsulation type of the remote VC. ● vlan ● ethernet
Remote VC Label	Remote VC label.
C Bit	Whether the control word is enabled: ● 1: indicates that the control word is enabled. ● 0: indicates that the control word is disabled.
MTU/CELLS	MTU of the L2VPN.
N Bit and Notification	Whether the Notification message is supported: ● 1: indicates the message is supported. ● 0: indicates the message is not supported.
S Bit and Status Code	Status code: ● 0: indicates the forwarding state. ● 1: indicates the non-forwarding state.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Match Local VC	Whether the local VC ID matches the remote VC ID: ● MATCH ● NOT-MATCH
Max ATM CELLS	Maximum number of ATM cells that can be transmitted. If ATM encapsulation is used, the value ranges from 1 to 28, and the default value is 28. If non-ATM encapsulation is used, double hyphens (--) are displayed.
TDM RTP Header	Whether the RTP-header option is enabled: ● enable: The RTP header is added to TDM packets to be transparently transmitted. ● disable: The RTP header is not added to TDM packets to be transparently transmitted. This is the default value. ● --: Non-TDM encapsulation is used.
TDM Encap Num	Number of frames in a TDM packet. If TDM encapsulation is used, the value is 8, 16, 24, 32 or 40, and the default value is 32. If non-TDM encapsulation is used, double hyphens (--) are displayed.
TDM Bit Rate	Number of timeslots in a TDM packet. Number of timeslots in a TDM packet = Number of bytes in a TDM packet/Number of frames in a TDM packet

Display information about the VCs in Up state.

```
<Huawei> display mpls l2vc state up
 Total LDP VC : 1     1 up       0 down

 *client interface       : Ethernet1/0/0 is up
  Administrator PW       : no
  session state          : up
  AC status              : up
  Ignore AC state        : disable
  VC state               : up
  Label state            : 0
  Token state            : 0
  VC ID                  : 100
  VC type                : Ethernet
  destination            : 10.2.2.9
  local VC label         : 1024         remote VC label      : 1024
  control word           : disable
  remote control word    : disable
  forwarding entry       : exist
  local group ID         : 0
  remote group ID        : 0
```

```
 local AC OAM State     : up
 local PSN OAM State    : up
 local forwarding state : forwarding
 local status code      : 0x0
 remote AC OAM state    : up
 remote PSN OAM state   : up
 remote forwarding state: forwarding
 remote status code     : 0x0
 ignore standby state   : no
 BFD for PW             : unavailable
 VCCV State             : up
 manual fault           : not set
 active state           : active
 link state             : up
 local VC MTU           : 1500         remote VC MTU        : 1500
 local VCCV             : alert ttl lsp-ping bfd
 remote VCCV            : alert ttl lsp-ping bfd
 tunnel policy name     : --
 PW template name       : --
 primary or secondary   : primary
 load balance type      : flow
 Access-port            : false
 Switchover Flag        : false
 VC tunnel/token info   : 1 tunnels/tokens
   NO.0  TNL type       : lsp   , TNL ID : 0x12
   Backup TNL type      : lsp   , TNL ID : 0x0
 create time            : 0 days, 1 hours, 0 minutes, 17 seconds
 up time                : 0 days, 0 hours, 24 minutes, 56 seconds
 last change time       : 0 days, 0 hours, 24 minutes, 56 seconds
 VC last up time        : 2013/10/10 14:29:39
 VC total up time       : 0 days, 0 hours, 24 minutes, 56 seconds
 CKey                   : 10
 NKey                   : 9
 PW redundancy mode     : frr
 AdminPw interface      : --
 AdminPw link state     : --
 Diffserv Mode          : uniform
 Service Class          : --
 Color                  : --
 DomainId               : --
 Domain Name            : --
```

Display information about the dynamic VC on the TDM interface.

```
<Huawei> display mpls l2vc interface serial 2/0/0
*client interface       : Serial2/0/0 is up
 Administrator PW       : no
 session state          : up
 AC status              : up
 Ignore AC state        : disable
 VC state               : up
 Label state            : 0
 Token state            : 0
 VC ID                  : 100
 VC type                : CESoPSN basic mode
 destination            : 10.3.3.9
 local group ID         : 0            remote group ID      : 0
 local VC label         : 1039         remote VC label      : 1045
 local TDM Encap Num    : 8            remote TDM Encap Num : 0
 jitter-buffer          : 8
 idle-code              : ff
 local rtp-header       : disable      remote rtp-header    : disable
 local bit-rate         : 0            remote bit-rate      : 0
 local AC OAM State     : up
 local PSN OAM State    : up
 local forwarding state : forwarding
 local status code      : 0x0
 remote AC OAM state    : up
 remote PSN OAM state   : up
 remote forwarding state: forwarding
 remote status code     : 0x0
```

```
ignore standby state   : no
BFD for PW             : unavailable
VCCV State             : up
manual fault           : not set
active state           : active
forwarding entry       : exist
link state             : up
local VC MTU           : --          remote VC MTU        : --
local VCCV             : alert ttl lsp-ping bfd
remote VCCV            : alert ttl lsp-ping bfd
local control word     : disable     remote control word  : disable
tunnel policy name     : --
PW template name       : pe2pe
primary or secondary   : primary
load balance type      : flow
Access-port            : false
Switchover Flag        : false
VC tunnel/token info   : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x5
  Backup TNL type      : lsp   , TNL ID : 0x0
create time            : 0 days, 0 hours, 1 minutes, 36 seconds
up time                : 0 days, 0 hours, 1 minutes, 36 seconds
last change time       : 0 days, 0 hours, 1 minutes, 36 seconds
VC last up time        : 2013/11/02 09:30:04
VC total up time       : 0 days, 0 hours, 1 minutes, 36 seconds
CKey                   : 9
NKey                   : 8
PW redundancy mode     : frr
AdminPw interface      : --
AdminPw link state     : --
Diffserv Mode          : pipe
Service Class          : ef
Color                  : green
DomainId               : --
Domain Name            : --
```

Table 12-134 Description of the **display mpls l2vc interface** command output

Item	Description
local TDM Encap Num	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application of the local VC.
remote TDM Encap Num	Number of encapsulated TDM frames in CESoPSN or SAToP packets in the TDMoPSN application of the remote VC. **NOTE** This field is displayed as 0 when the AC interface is a serial interface.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
local rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the local end.

Item	Description
remote rtp-header	Whether the RTP header is added to the transparently transmitted TDM frames on the remote end.
local bit-rate	Bit rate of the local VC.
remote bit-rate	Bit rate of the remote VC.

Related Topics

12.12.15 mpls l2vc
12.11.7 display mpls l2vpn forwarding-info

12.12.4 display mpls l2vc brief

Function

The **display mpls l2vc brief** command displays brief information about LDP Layer 2 virtual circuits (L2VCs) on the device.

Format

display mpls l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls l2vc brief** command is recommended when many L2VCs are configured on a device. The command output is more concise than that of the **display mpls l2vc** command.

Example

Display brief information about all LDP L2VCs on the device.

```
<Huawei> display mpls l2vc brief
 Total LDP VC : 1      1 up       0 down

 *Client Interface     : Vlanif1111
  Administrator PW     : no
  AC status            : up
```

```
VC state          : up
Label state        : 0
Token state        : 0
VC ID             : 116119
VC Type           : VLAN
session state      : up
Destination        : 10.6.6.6
link state        : up
```

Table 12-135 Description of the **display mpls l2vc brief** command output

Item	Description
Total LDP VC	Total number of LDP VCs, including the number of LDP VCs in Up and Down state.
Client Interface	AC interface and its status.
Administrator PW	Whether the PW is an mPW. The PW can be an mPW only when the AC interface is a loopback interface.
AC status	Status of the AC: ● up ● down
VC state	Status of the VC: ● up ● down
Label state	Label status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
Token state	Token status: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirming failed.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
session state	Status of the session between peers: ● up ● down
Destination	Peer address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
link state	Status of the VC: ● up ● down

Related Topics

12.12.15 mpls l2vc

12.11.7 display mpls l2vpn forwarding-info

12.12.5 display mpls l2vc oam-mapping

Function

The **display mpls l2vc oam-mapping** command displays status of an L2VPN AC established by using the LDP signaling and information about the OAM mapping table at the PSN side.

Format

display mpls l2vc oam-mapping [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface type and number. If this parameter specified, OAM mapping information on the specified VC interface using the LDP signaling is displayed. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display mpls l2vc oam-mapping** command, either the following situation will occur:

- If an interface name is specified, detailed OAM mapping information on this interface is displayed.

 Copyright © Huawei Technologies Co., Ltd.

- If no interface name is specified, basic about the OAM mapping information on all interfaces is displayed.

Example

Display OAM mapping information on the VC interface using the LDP signaling.

```
<Huawei> display mpls l2vc oam-mapping
 Interface                Active VC-ID     VC-status AC-OAM  BFD-for-PW
GigabitEthernet0/0/1        No    100       Primary   Enable  Disable
GigabitEthernet0/0/1        No    101       Secondary Enable  Disable
```

Table 12-136 Description of the **display mpls l2vc oam-mapping** command output

Item	Description
Interface	Type and number of the AC interface.
Active	Whether the PW is in the active state: ● Yes: indicates that the PW is in active state. ● No: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist.
VC-ID	ID of the local VC.
VC-status	Status of the local PW: ● Primary: indicates the primary PW. ● Secondary: indicates the secondary PW.
AC-OAM	Whether the local PE reports an AC fault to the remote PE through OAM: ● Enable: indicates that the local PE reports an AC fault to the remote PE through OAM. ● Disable: indicates that the local PE does not report an AC fault to the remote PE through OAM.
BFD-for-PW	Whether BFD for PW is enabled on the local PE: ● Enable ● Disable

Display OAM mapping information on GE1/0/0.

```
<Huawei> display mpls l2vc oam-mapping interface gigabitethernet 1/0/0
 AC OAM Info:
```

```
 EOAM Type      : 802.3ah
 AC OAM State   : Up
 OAM-mapping    : Enable
PSN info:
 VC-ID          : 100
 VC status      : Primary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
 VC-ID          : 101
 VC status      : Secondary
 Active State   : Inactive
 Link State     : Down
 BFD for PW     : Disable
 BFD for LSP    : 0    TunnelNum: 0    PSN State : up
```

Table 12-137 Description of the **display mpls l2vc oam-mapping interface** command output

Item	Description
AC OAM Info	Information about AC OAM to be displayed in the following lines.
ACFD Index	Index of the AC forwarding information.
EOAM Type	Type of the protocol used for fault detection and notification.
AC OAM State	Fault detection status on the local AC: ● Up: indicates that AC fault detection is disabled or that AC fault detection is enabled but no AC fault is detected. ● Down: indicates that AC fault detection is enabled and an AC fault is detected. ● Invalid: indicates that AC fault detection is disabled, and the AC OAM state field is invalid.
OAM-mapping	Whether OAM mapping is enabled on the local PE: ● Enable ● Disable
PSN info	Information about the PW.
VC-ID	ID of the VC.

Item	Description
VC status	Status of the PW: ● Primary: indicates the primary PW. ● Secondary: indicates the secondary PW. ● Bypass: indicates the inter-chassis PW. ● PW-Bypass: indicates the inter-chassis PW used to protect PW-side links. ● AC-Bypass: indicates the inter-chassis PW used to protect AC-side links.
Active state	Whether the PW is in the active state: ● Active: indicates that the PW is in active state. ● Inactive: indicates that the PW is in inactive state. This field is valid only when primary and secondary PWs coexist. When an AC interface is configured with only one PW, the PW is in active state. If an AC interface is configured with primary and secondary PWs, the primary PW is in active state and the secondary PW is in inactive state. When the primary PW fails, the secondary PW becomes active and the primary PW becomes inactive.
Link State	Link status of the AC interface. ● Up: indicates that the interface is Up. ● Down: indicates that the interface is Down.
BFD for PW	Whether BFD for PW is enabled on the local PE.
BFD for LSP	Whether BFD is used to detect a tunnel: ● zero: indicates that BFD is not used to detect a tunnel. ● non-zero: indicates that BFD is used to detect a tunnel.
TunnelNum	Number of tunnels detected by BFD.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSN State	• When the tunnel is not detected by BFD, the default status of the tunnel is Up. • When the PW uses the tunnel not detected by BFD, the PSN state is Up.

Related Topics

12.12.18 mpls l2vpn oam-mapping

12.12.6 display mpls l2vpn interface performance

Function

The **display mpls l2vpn interface performance** command displays PW performance information on a TDM interface.

Format

display mpls l2vpn interface *interface-type interface-number* **performance**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After configuring a TDM-encapsulated PW at the AC side, you can run the **display mpls l2vpn interface performance** command to view PW performance information.

Prerequisites

A static or dynamic PW has been configured on the ATM or TDM interface.

Precautions

- The **interface** *interface-type interface-number* parameter specifies the AC interface on which PW performance information is displayed.
- This command can be used only to display performance information of a primary PW.
- PW performance information is updated every 15 minutes. Therefore, only PW performance information updated for the latest 15 minutes is displayed when you run this command.

Example

Display PW performance information on a TDM interface.

```
<Huawei> display mpls l2vpn interface serial 2/0/0  performance
Client interface                          : Serial2/0/0
Number of missing packets                 : 0
Number of times the jitter buffer was overrun  : 0
Number of times the jitter buffer was underrun : 0
Number of misorder packets                : 0
Number of malformed packets               : 0
Number of misconnected packets            : 0
Number of error seconds                   : 0
Number of severely error seconds          : 0
Number of unavailable seconds             : 0
```

Table 12-138 Description of the **display mpls l2vpn interface performance** command output

Item	Description
Client interface	AC interface and its status.
Number of missing packets	Number of lost packets.
Number of times the jitter buffer was overrun	Number of times that a jitter buffer overflow occurs.
Number of times the jitter buffer was underrun	Number of times that a jitter buffer underflow occurs.
Number of misorder packets	Number of lost packets caused by packet disorder.
Number of malformed packets	Number of malformed packets.
Number of misconnected packets	Number of misconnected packets during the detection period.
Number of error seconds	Number of errored seconds, indicating the period during which a TDM-encapsulated PW discards packets or receives error packets. Any malformed packet or disorder packet is considered as an error packet.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Number of severely error seconds	Number of severely errored seconds.
Number of unavailable seconds	Number of unavailable seconds. When the SES is larger than 10 seconds, a TDM encapsulated PW is considered as unavailable. The number of unavailable seconds is counted when a severe error begins.

Related Topics

12.12.19 mpls l2vpn pw performance disable

12.12.7 display mpls static-l2vc

Function

The **display mpls static-l2vc** command displays information about static VCs on the device.

Format

display mpls static-l2vc [*vc-id* | **interface** *interface-type interface-number* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
vc-id	Displays information about a static VC with a specified VC ID.	The value is an integer that ranges from 1 to 4294967295.
interface *interface-type interface-number*	Displays information about all static PWs on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
state { **down** | **up** }	Displays VC information based on the VC status. • **down**: Displays information about the VC in Down state. • **up**: Displays information about the VC in Up state.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you run the **display mpls static-l2vc** command with the interface name specified, information about static VCs on the interface connected to a CE is displayed. If no interface is specified, information about static VCs on all interfaces is displayed.

Example

Display information about static VCs on the device.

```
<Huawei> display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy Name   : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL type       : lsp   , TNL ID : 0x800802
  Backup TNL type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 1 hours, 44 minutes, 19 seconds
  UP time              : 0 days, 1 hours, 44 minutes, 19 seconds
  Last change time     : 0 days, 1 hours, 44 minutes, 19 seconds
  VC last up time      : 2011/09/22 15:48:06
  VC total up time     : 0 days, 1 hours, 44 minutes, 19 seconds
  CKey                 : 10
  NKey                 : 9
  BFD for PW           : unavailable
```

Table 12-139 Description of the **display mpls static-l2vc** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.

Item	Description
AC Status	Status of the AC: ● up ● down
VC State	Status of the VC: ● up ● down
VC ID	ID of the VC, which uniquely identifies a VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Label Status	Whether the label can be used: ● 0: The label can be used. ● 1: Wait for the SMB to confirm the label status. ● 2: The label is released. ● 3: SMB confirmation failed.
Token Status	Whether the token can be used: ● 0: The token can be used. ● 1: Wait for the SMB to confirm the token status. ● 2: The token is released. ● 3: SMB confirmation failed.
Control Word	Whether the control word function is enabled: ● enable ● disable
VCCV Capability	Whether VCCV is enabled.
active state	Whether the PW is in active state. A PW in active state can forward packets. ● active ● inactive

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Link State	Integrative PW status: ● up ● down If any of the following status is Down, the PW link state is Down: ● Service PW status ● OAM status
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
load balance type	Load balancing mode of Martini VLL: ● flow: indicates flow-based load balancing. ● packet: indicates packet-based load balancing.
Access-port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
VC Tunnel/token info	Displays information about the VC tunnel or token ("1 tunnels/tokens" indicates that the PW uses one tunnel or token).
Backup TNL Type	Type of the backup tunnel when PW over LDP FRR is used.
NO.0 TNL Type	Type of the tunnel used by the PW
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured.

 Copyright © Huawei Technologies Co., Ltd.

Display information about static VCs on Ethernet1/0/0.

```
<Huawei> display mpls static-l2vc interface ethernet 1/0/0
 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capabilty       : alert ttl lsp-ping bfd
  active state         : active
  Link State           : up
  Tunnel Policy        : --
  PW Template Name     : --
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 1 tunnels/tokens
  NO.0  TNL Type       : lsp   , TNL ID : 0x3
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 1 hours, 55 minutes, 52 seconds
  UP time              : 0 days, 1 hours, 55 minutes, 52 seconds
  Last change time     : 0 days, 1 hours, 55 minutes, 52 seconds
  VC last up time      : 2011/09/22 15:48:06
  VC total up time     : 0 days, 1 hours, 55 minutes, 52 seconds
  CKey                 : 10
  NKey                 : 9
  Diffserv Mode        : uniform
  Service Class        : --
  Color                : --
  DomainId             : --
  Domain Name          : --
  BFD for PW           : unavailable
```

Table 12-140 Description of the **display mpls static-l2vc interface** command output

Item	Description
Client Interface	AC interface and its status.
AC Status	Status of the link between the PE and its directly connected CE.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	VC label sent by the local device.
Receive VC Label	VC label received by the local device.
Control Word	Whether the control word function is enabled.
VCCV Capabilty	Whether VCCV is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tunnel Policy	Name of the tunnel policy. The value -- indicates that no tunnel policy is configured.
PW Template Name	Name of the PW template. The value -- indicates that no PW template is configured.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
VC tunnel/token info	Information about the tunnel or token used by the VC. The value **1 tunnels/tokens** indicates that the PW uses one tunnel or token.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Diffserv Mode	QoS DiffServ mode for VLL services.
Service Class	QoS service class for VLL services.
Color	QoS color for VLL services.
DomainId	ID of a domain.
Domain Name	Name of a domain.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured.

Display information about SVCs in Up state between peers.

```
<Huawei> display mpls static-l2vc state up
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
  Destination          : 3.3.3.9
  Transmit VC Label    : 100
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Disable
  VCCV Capability      : alert ttl lsp-ping bfd
  active state         : active
```

```
Link State           : up
Tunnel Policy Name   : --
PW Template Name     : --
Main or Secondary    : Main
load balance type    : flow
Access-port          : false
VC tunnel/token info : 1 tunnels/tokens
NO.0  TNL Type       : lsp   , TNL ID : 0x56
Backup TNL Type      : lsp   , TNL ID : 0x0
Create time          : 0 days, 1 hours, 56 minutes, 1 seconds
UP time              : 0 days, 1 hours, 56 minutes, 1 seconds
Last change time     : 0 days, 1 hours, 56 minutes, 1 seconds
VC last up time      : 2011/09/22 15:48:06
VC total up time     : 0 days, 1 hours, 56 minutes, 1 seconds
CKey                 : 10
NKey                 : 9
BFD for PW           : unavailable
```

Table 12-141 Description of the **display mpls static-l2vc state** command output

Item	Description
Total svc connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC.
VC State	Status of the VC.
VC ID	ID of the VC, which uniquely identifies a VC.
VC Type	Encapsulation type of the VC.
Destination	LSR ID of the remote end on the VC.
Transmit VC Label	Local VC label.
Receive VC Label	Remote VC label.
Control Word	Whether the control word function is enabled.
VCCV Capability	Whether VCCV is enabled.
Tunnel Policy Name	Name of the tunnel policy.
PW Template Name	Name of the PW template.
Main or Secondary	Whether the VC is a primary VC or a secondary VC.
Create time	How long the VC has been created.
UP time	How long the VC keeps the Up state.
Last change time	How long the VC status remains unchanged.
VC last up time	Last time when the VC became Up.
VC total up time	Total duration of the VC in Up state.
CKey	Index of the public tunnel for VPN QoS.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
NKey	Index of the public tunnel.
BFD for PW	Whether BFD is configured. ● unavailable: indicates that BFD is not configured. ● available: indicates that BFD is configured.

Display information about the static VC configured on TDM interface.

```
<Huawei> display mpls static-l2vc
 Total svc connections:  1,  0 up,  1 down

 *Client Interface     : Serial2/0/0 is up
  AC Status            : up
  VC State             : down
  VC ID                : 112
  VC Type              : CESoPSN basic mode
  Destination          : 1.1.1.9
  Transmit VC Label    : 115
  Receive VC Label     : 200
  Label Status         : 0
  Token Status         : 0
  Control Word         : Enable
  VCCV Capability      : cw alert ttl lsp-ping bfd
  active state         : inactive
  Link State           : down
  Tunnel Policy Name   : --
  PW Template Name     : --
  TDM encapsulation number : 8
  jitter-buffer        : 8
  idle-code            : ff
  rtp-header           : disable
  Main or Secondary    : Main
  load balance type    : flow
  Access-port          : false
  VC tunnel/token info : 0 tunnels/tokens
  Backup TNL Type      : lsp   , TNL ID : 0x0
  Create time          : 0 days, 0 hours, 0 minutes, 9 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 9 seconds
  VC last up time      : 0000/00/00 00:00:00
  VC total up time     : 0 days, 0 hours, 0 minutes, 0 seconds
  CKey                 : 4
  NKey                 : 3
  BFD for PW           : unavailable
```

Table 12-142 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Whether the RTP header is added to the transparently transmitted TDM frame.

Related Topics

12.12.24 mpls static-l2vc

12.12.8 display mpls static-l2vc brief

12.12.8 display mpls static-l2vc brief

Function

The **display mpls static-l2vc brief** command displays brief information about static VCs on the device.

Format

display mpls static-l2vc brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display mpls static-l2vc brief** command is recommended when a large number of static VCs are configured on the device.

Example

Display brief information about static VCs on the device.

```
<Huawei> display mpls static-l2vc brief
Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet1/0/0 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : Ethernet
```

```
Destination          : 3.3.3.9
```

Table 12-143 Description of the **display mpls static-l2vc brief** command output

Item	Description
Total SVC Connections	Number of established SVCs, including the number of SVCs in Up and Down states.
Client Interface	AC interface and its status.
AC Status	Status of the AC: ● up: An AC has been established. ● down: An AC is not established.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.
VC ID	ID of the static VC. If you run the **mpls static-l2vc** command without the VC ID specified, the value of this field is displayed as 0.
VC Type	Encapsulation type of the VC: ● VLAN ● Ethernet
Destination	IPv4 address of the peer. Generally, the value is the loopback address of the peer.

Display brief information about the static VC configured on a TDM interface.

```
<Huawei> display mpls static-l2vc brief
 Total svc connections:  1,  0 up,  1 down

 *Client Interface     : Serial2/0/0 is up
  AC Status            : up
  VC State             : down
  VC ID                : 112
  VC Type              : CESoPSN basic mode
  Destination          : 1.1.1.9
  TDM encapsulation number : 8
  jitter-buffer            : 8
  idle-code                : ff
  rtp-header               : disable
```

Table 12-144 Description of the **display mpls static-l2vc** command output

Item	Description
TDM encapsulation number	Number of encapsulated TDM frames in Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packets in the TDMoPSN application.
jitter-buffer	Depth of the jitter buffer, that is, the maximum allowed jitter delay.
idle-code	Idle code that is filled manually when a jitter buffer underflow occurs.
rtp-header	Indicates Whether the RTP header is added to the transparently transmitted TDM frames.

Related Topics

12.12.24 mpls static-l2vc

12.11.7 display mpls l2vpn forwarding-info

12.12.9 display mpls switch-l2vc

Function

The **display mpls switch-l2vc** command displays information about PW switching, including static, dynamic, and mix PW switching.

Format

display mpls switch-l2vc [*ip-address vc-id* **encapsulation** *encapsulation-type* | **state** { **down** | **up** }]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of the peer PE.	-
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.
encapsulation *encapsulation-type*	Specifies the PW encapsulation type.	Currently, the device supports the following types encapsulation types: **ethernet**, **vlan**, **satop-e1**, and **cesopsn-basic**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
state { **down** | **up** }	Displays VC information based on the VC status. ● **down**: Displays information about the VC in Down state. ● **up**: Displays information about the VC in Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If parameters in the **display mpls switch-l2vc** command are not specified, information about all PW switching is displayed.

Example

Display information about the specified PW switching.

```
<Huawei> display mpls switch-l2vc 1.1.1.9 100 encapsulation ethernet
*Switch-l2vc type            : SVC<---->SVC
 Peer IP Address             : 3.3.3.9, 1.1.1.9
 VC ID                       : 100, 100
 VC Type                     : Ethernet
 VC State                    : up
 In/Out Label                : 200/200, 100/100
 InLabel Status              : 0 , 0
 Control Word                : Disable, Disable
 VCCV Capability             : alert ttl lsp-ping bfd, alert ttl lsp-ping bfd
 Switch-l2vc tunnel info     :
                             1 tunnels for peer 5.5.5.9
                             NO.0  TNL Type : lsp   , TNL ID : 0x11
                             1 tunnels for peer 1.1.1.9
                             NO.0  TNL Type : lsp   , TNL ID : 0xb
 CKey                        : 44, 1
 NKey                        : 43, 3
 Tunnel policy               : --,--
 Control-Word transparent    : YES
 Create time                 : 0 days, 0 hours, 7 minutes, 2 seconds
 UP time                     : 0 days, 0 hours, 7 minutes, 2 seconds
 Last change time            : 0 days, 0 hours, 7 minutes, 2 seconds
 VC last up time             : 2013/11/24 14:31:31
 VC total up time            : 0 days, 2 hours, 12 minutes, 51 seconds
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-145 Description of the **display mpls switch-l2vc** command output (SVC-SVC)

Item	Description
Switch-l2vc Type	Switching type: ● LDP-LDP ● LDP-SVC ● SVC-SVC When primary/secondary PWs and PW switching are configured, the value of this field must be LDP-LDP. ● LDP: indicates a dynamic PW. ● SVC: indicates a static PW.
Peer ip address	IP addresses of the peers at two ends of a switching PW, which are displayed in left and right columns respectively.
VC ID	ID of the VC, which uniquely identifies a VC. Here, the field indicates the two switched VC IDs.
VC Type	Encapsulation type of the VC.
VC State	Status of the VC: ● Up: A VC has been established. ● Down: A VC is not established.
In/Out Label	Incoming or outgoing label.
InLabel Status	Status of the inner label.
Control Word	Whether the control word function is enabled on both ends: ● Disable ● Enable
VCCV Capability	Type of VCCV supported on the local device. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Switch-l2vc tunnel info: 1 tunnels for peer 3.3.3.9 NO.0 TNL Type : lsp , TNL ID : 0x11	Information about the tunnels on both ends: ● TNL Type: indicates the type of the tunnel. ● TTNL ID: indicates the tunnel ID.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Tunnel policy	Name of the tunnel policy.
Control-Word transparent	Whether transparent transmission of the control word is enabled: ● yes ● no
Create Time	How long the VC has been created.
Up Time	How long the VC keeps the Up state.
Last Change Time	How long the VC status remains unchanged.
VC last up time	Last time when the AC became Up.
VC total up time:	Total duration when the AC interface is Up.

Display information about the switched L2VCs in Up state between peers.

```
<Huawei> display mpls switch-l2vc state up
Total Switch VC : 1, 1 up, 0 down
*Switch-l2vc type            : LDP<---->LDP
 Peer IP Address             : 5.5.5.9, 1.1.1.9
 VC ID                       : 200, 100
 VC Type                     : Ethernet
 VC State                    : up
 VC StatusCode               |PSN |OAM | FW |    |PSN |OAM | FW |
                 -Local VC :| UP | UP | UP |    | UP | UP |DOWN|
                 -Remote VC:| UP | UP |DOWN|    | UP | UP | UP |
 Session State               : up, up
 Local/Remote Label          : 1025/1024, 1024/1025
 InLabel Status              : 0 , 0
 Local/Remote MTU            : 1500/1500, 1500/1500
 Local/Remote Control Word    : Disable/Disable, Disable/Disable
 Local/Remote VCCV Capability : alert ttl lsp-ping bfd /alert ttl lsp-ping bfd, alert ttl lsp-ping bfd/alert ttl lsp-
ping bfd
 Switch-l2vc tunnel info      :
                             1 tunnels for peer 5.5.5.9
                             NO.0  TNL Type : lsp   , TNL ID : 0x12
                             1 tunnels for peer 1.1.1.9
                             NO.0  TNL Type : lsp   , TNL ID : 0x15
 CKey                        : 44, 1
 NKey                        : 43, 3
 Tunnel policy               : --, --
 Control-Word transparent     : YES
 Create time                 : 0 days, 0 hours, 3 minutes, 54 seconds
 UP time                     : 0 days, 0 hours, 3 minutes, 12 seconds
 Last change time            : 0 days, 0 hours, 3 minutes, 12 seconds
 VC last up time             : 2013/11/24 14:31:31
 VC total up time            : 0 days, 2 hours, 12 minutes, 51 seconds
```

Table 12-146 Description of the **display mpls switch-l2vc** command output (LDP-LDP)

Item	Description
VC StatusCode	VC status code: ● PSN: indicates the fault status at the public network side. ● OAM: indicates the fault status at the AC side. ● FW: indicates the forwarding status. -Local VC: indicates the local VC status. -Remote VC: indicates the remote VC status.
Session State	Status of the session: ● Up: indicates that the session is successfully set up. ● Down: indicates that the session is not set up. ● None: indicates that no session exists.
Local/Remote Label	Incoming or outgoing label.
Local/Remote MTU	Local and remote MTU values of the PWs on two ends: ● For LDP, both the local and remote MTU values are displayed. ● For SVC, only the local MTU value is displayed.
Local/Remote Control Word	Whether the control word is enabled on both ends: ● disable: indicates that the control word is disabled. ● enable: indicates that the control word is enabled.
Local/Remote VCCV Capability	Whether VCCV is enabled on both ends: ● CC: specifies the control channel type, which can be CW, alert, or TTL. ● CV: specifies the connectivity verification mode, which can be LSP ping or BFD.
Control-Word transparent	Whether transparent transmission of the control word is enabled: ● yes ● no

Display information about all the switched L2VCs between peers.

```
<Huawei> display mpls switch-l2vc
Total Switch VC : 1, 1 up, 0 down

*Switch-l2vc type            : LDP<---->SVC
 Peer IP Address             : 1.1.1.9, 5.5.5.9
 VC ID                       : 100, 200
 VC Type                     : Ethernet
 VC State                    : up
 Session State               : up, None
 Local(In)/Remote(Out) Label  : 1027/1028, 100/200
 InLabel Status              : 0 , 0
 Local/Remote MTU            : 1500/1500, 1500
 Local/Remote Control Word    : Disable/Disable, Disable
 Local/Remote VCCV Capability : alert ttl lsp-ping bfd /alert ttl lsp-ping bfd, alert ttl lsp-ping bfd
 Switch-l2vc tunnel info      :
                               1 tunnels for peer 1.1.1.9
                               NO.0  TNL Type : lsp   , TNL ID : 0x9
                               1 tunnels for peer 5.5.5.9
                               NO.0  TNL Type : lsp   , TNL ID : 0xa
 CKey                        : 44, 1
 NKey                        : 43, 3
 Tunnel policy               : --, --
 Create time                 : 0 days, 0 hours, 3 minutes, 48 seconds
 UP time                     : 0 days, 0 hours, 3 minutes, 48 seconds
 Last change time            : 0 days, 0 hours, 3 minutes, 48 seconds
 VC last up time             : 2013/11/24 14:31:31
 VC total up time            : 0 days, 2 hours, 12 minutes, 51 seconds
```

Related Topics

12.12.25 mpls switch-l2vc

12.12.10 display mpls switch-l2vc brief

Function

The **display mpls switch-l2vc brief** command displays brief information about all switching PWs, including static, dynamic, and mixed switching PWs.

Format

display mpls switch-l2vc brief

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When many switching PWs are configured on the device, you can run this command to view brief information about the switching PWs. The command

output of the **display mpls switch-l2vc brief** command is more concise than that of the **display mpls switch-l2vc** command.

Example

Display brief information about switching PWs.

```
<Huawei> display mpls switch-l2vc brief
 Total Switch VC : 3, 0 up, 3 down

*Switch-l2vc type            : LDP<---->LDP
 Peer IP Address             : 2.2.2.2, 3.3.3.9
 VC ID                     : 18, 180
 VC Type                     : SAT E1 over Packet
 VC State                    : up
 Session State               : up, up

*Switch-l2vc type            : LDP<---->SVC
 Peer IP Address             : 3.3.3.3, 4.4.4.9
 VC ID                     : 19, 119
 VC Type                     : Ethernet
 VC State                    : up
 Session State               : up, up

*Switch-l2vc type            : SVC<---->SVC
 Peer IP Address             : 1.1.1.1, 2.2.2.9
 VC ID                     : 113, 1123
 VC Type                     : CESoPSN basic mode
 VC State                    : up
 In/Out Label                : 16/10, 17/150
```

Table 12-147 Description of the display mpls switch-l2vc brief command output

Item	Description
Total Switch VC	Number of established Martini VCs (using the LDP signaling), including the number of Martini VCs in Up and Down states.
Switch-l2vc Type	Switching type, which can be LDP-LDP, LDP-SVC, or SVC-SVC. If the primary and secondary switching VCs are configured, the switching types of these VCs can only be LDP-LDP. ● LDP: indicates a dynamic PW. ● SVC: indicates a static PW.
Peer IP Address	IP address of the peer.
VC ID	ID of the VC, which uniquely identifies a VC. Here, the field indicates the two switched VC IDs.
VC Type	Encapsulation type of the VC.
VC State	Status of the VC: ● up: A VC has been established. ● down: A VC is not established.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Session state	Status of the session between peers: ● up: indicates that the session is successfully set up. ● down: indicates that the session is not set up. ● none: indicates that no session exists.

Related Topics

12.12.25 mpls switch-l2vc

12.12.11 display pw-template

Function

The **display pw-template** command displays information about PW templates.

Format

display pw-template [*pw-template-name*]

Parameters

Parameter	Description	Value
pw-template-name	Specifies the PW template name. If this parameter is not specified, information about all PW templates is displayed.	The value is an existing PW template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display information about all PW templates.

```
<Huawei> display pw-template
Total PW template number : 1
  PW Template Name : p2
  PeerIP           : --
  Tnl Policy Name  : --
```

```
CtrlWord          : Disable
MTU               : 1500
Max Atm Cells     : 28
ATM Pack Overtime: 1000
Seq-Number        : Disable
Transmit ATM Cells       : --
TDM Encapsulation Number: 8
Jitter-Buffer            : 8
Jitter-Buffer-Cep        : 1000
Payload-Compression DBA : --
Idle-Code                : ff
Rtp-Header               : Disable
VCCV Capability  : alert ttl lsp-ping bfd
Total PW          : 0, Static PW : 0, LDP PW : 0
```

Table 12-148 Description of the **display pw-template** command output

Item	Description
Total PW template number	Total number of PW templates.
PW Template Name	PW template name.
PeerIP	Peer IP address.
Tnl Policy Name	Name of the public network tunnel policy applied to the PW.
CtrlWord	Whether the control word is enabled in the PW template. ● Disable ● Enable
MTU	Maximum transmission unit.
Max ATM cells	Maximum number of transmitted ATM cells.
ATM pack overtime	Delay in packaging ATM cells.
Seq-Number	Sequence number in the control word of the PW: ● If the sequence number function is enabled, the device checks the sequence number of each packet and discards any packet with an incorrect sequence number. ● If the sequence number function is disabled, the device does not check the sequence number when processing packets.
Transmit ATM Cells	Number of ATM cells sent by the local device.
TDM Encapsulation Number	Number of encapsulated TDM frames.
Jitter-Buffer	Maximum jitter buffer depth for TDM.
Jitter-Buffer-Cep	Maximum jitter buffer depth for TDM (with CEP encapsulation).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Payload-Compression DBA	Payload compression dynamic bandwidth allocation (DBA): ● UNEQ: Send DBA packets when unequipped circuit indications are detected. ● --: Payload compression DBA is not configured.
Idle-Code	Idle code that is filled when a jitter buffer underflow occurs.
Rtp-Header	Whether the RTP header is added to the transparently transmitted TDM frame.
VCCV Capability	VC connection verification mode. ● By default, the VCCV type is **alert ttl lsp-ping bfd**, indicating that the control word function is disabled and LSP ping and BFD are supported for the alert channel. ● If the control word function is enabled, the VCCV type is **cw alert ttl lsp-ping bfd**, indicating that LSP ping and BFD are supported for both the control word channel and the alert channel.
Total PW	Total number of PWs using this PW template, including static and dynamic PWs.

Related Topics

12.12.29 pw-template

12.12.12 idle-code

Function

The **idle-code** command sets the idle code that is filled when a jitter buffer underflow occurs.

The **undo idle-code** command deletes the idle code that is filled when a jitter buffer underflow occurs.

By default, the system sets the idle code to FF when a jitter buffer underflow occurs.

Format

idle-code *idle-code-value*

undo idle-code

Parameters

Parameter	Description	Value
idle-code-value	Specifies the value of the idle code that is filled when a jitter buffer underflow occurs.	The value is a hexadecimal number that ranges from 00 to FF. The default value is FF.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to set the value of the idle code that is filled when a jitter buffer underflow occurs. A jitter buffer underflow occurs when the device needs to read packets but there are not sufficient packets in the buffer. The idle code has no significance, and can be set randomly.

Prerequisite

A PW template has been created and the PW template view is displayed by running the **pw-template** command in the system view.

Follow-up Procedure

After running the **idle-code** command, run the **reset pw** command to apply the attributes in the PW template to the PW. To check whether the idle code has taken effect on the PW, run the **display mpls l2vc** command to view the **idle-code** field.

Precautions

If you specify the **idle-code** parameter in the **mpls l2vc** command and run the **idle-code** command in the PW template view simultaneously, the idle code specified in the **mpls l2vc** command takes effect.

Example

Set the idle code to 0 when a jitter buffer underflow occurs.

```
<Huawei> system-view
[Huawei] pw-template tdmpw
[Huawei-pw-template-tdmpw] idle-code 0
```

Related Topics

12.12.13 jitter-buffer depth
12.12.29 pw-template

12.12.13 jitter-buffer depth

Function

The **jitter-buffer depth** command sets the depth of the jitter buffer in the TDMoPSN application.

The **undo jitter-buffer depth** command restores the default maximum depth of the TDM jitter buffer.

By default, the depth of the jitter buffer is 8 ms.

Format

jitter-buffer depth *depth*

undo jitter-buffer depth

Parameters

Parameter	Description	Value
depth *depth*	Specifies the depth of the jitter buffer, that is, the allowed maximum jitter delay.	The value is an integer that ranges from 4 to 64, in milliseconds. The default value is 8 ms.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A jitter buffer is designed to smooth the transmission jitter. The jitter buffer receives TDM services at different rates, buffers TDM frames, and then sends the frames to the next hop at a certain rate. In this manner, the transmission jitter is smoothed. The **jitter-buffer depth** command can be run on TDM AC interfaces only.

The shallower the jitter buffer is, the weaker the anti-jitter capabilities are. The deeper the jitter buffer is, the stronger the anti-jitter capabilities are, but a long transmission delay will be introduced when data flows are reconstructed. If the jitter buffer is set to a too large or too small value, service transmission quality will be affected.

Therefore, during the configuration, you need to set a proper depth for the jitter buffer by considering the network bandwidth, jitter, and sensitivity of various services to the delay.

 Copyright © Huawei Technologies Co., Ltd.

- An 8 ms-deep jitter buffer is recommended for voice services because they are sensitive to the delay. The depth can be increased for video and data services.
- If the network topology is complex and the jitter of link transmission is large, you can increase the depth of the jitter buffer. If the network topology is simple and the jitter of link transmission is small, you can decrease the depth of the jitter buffer.
- If the initial wait delay is long, you can decrease the depth of the jitter buffer.

For a PSN, you need to pre-set the depth of the jitter buffer. More importantly, you need to monitor the jitter prevention effects of the jitter buffer with different depths and adjust the depth of the jitter buffer accordingly. In this manner, you can determine the depth of the jitter buffer based on service requirements.

Prerequisites

A PW template has been created and the PW template view is displayed by running the **pw-template** command in the system view.

Follow-up Procedure

After running the **jitter-buffer depth** command, run the **reset pw** command to apply the attributes in the PW template to the PW. To check whether the jitter buffer depth has taken effect on the PW, run the **display mpls l2vc** command to view the **jitter-buffer** field.

Precautions

If you specify the **jitter-buffer** parameter in the **mpls l2vc** command and run the **jitter-buffer depth** command in the PW template view simultaneously, the jitter buffer depth specified in the **mpls l2vc** command takes effect.

Example

Set the depth of the jitter buffer to 4 ms.

```
<Huawei> system-view
[Huawei] pw-template tdmpw
[Huawei-pw-template-tdmpw] jitter-buffer depth 4
```

Related Topics

12.12.12 idle-code

12.12.29 pw-template

12.12.32 tdm-encapsulation-number

12.12.14 manual-set pw-ac-fault

Function

The **manual-set pw-ac-fault** command simulates a fault on the primary or secondary PW.

The **undo manual-set pw-ac-fault** command cancels the fault that is simulated on a primary or secondary PW.

By default, no fault is simulated on a PW.

Format

manual-set pw-ac-fault [**secondary**]

undo manual-set pw-ac-fault [**secondary**]

Parameters

Parameter	Description	Value
secondary	Simulates a fault on the secondary PW. If this parameter is not specified, a fault is simulated on the primary PW.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network where the primary and secondary PWs need to be configured, you can run the **manual-set pw-ac-fault** command to simulate a fault on the primary or secondary PW to check whether services can be switched between the primary and secondary PWs.

Prerequisites

A VC has been created.

Example

Simulate a fault on the PW.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] mpls l2vc 2.2.2.2 100
[Huawei-Vlanif10] manual-set pw-ac-fault
```

12.12.15 mpls l2vc

Function

The **mpls l2vc** command creates a Martini VLL.

The **undo mpls l2vc** command deletes the Martini VLL from an interface.

By default, no Martini L2VPN connection is created.

Format

mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc { *ip-address* | **pw-template** *pw-template-name* } * *vc-id* [[**tunnel-policy** *policy-name*] | [{ **control-word** | **no-control-word** }] | [{ **raw** | **tagged** }] | [**secondary**]] *

undo mpls l2vc [**secondary**]

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies a L2VC ID.	The value is an integer that ranges from 1 to 4294967295.
tunnel-policy *policy-name*	Specifies a tunnel policy name for the L2VC. If no name is specified for a tunnel policy, the default tunnel policy is used. The LSP tunnel is preferred and only one LSP is used for load balancing in the default tunnel policy. If the name of the tunnel policy is specified but no tunnel policy is configured, the default tunnel policy is still used.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
raw	Removes the service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
control-word	Enables the control word function.	-
no-control-word	Disables the control word function.	-
secondary	Indicates that the VC is a secondary VC. If this parameter is not specified, a primary VC is created. You can configure a secondary VC only when the primary VC exists on the local device.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a Martini VLL networking, you can run this command to create a VC connection for a Martini VLL.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You must create dynamic VCs on PEs at both ends of a PW to connect the PEs. The destination address of a VC is the LSR ID of the peer PE.
- You can set attributes for a PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring an LDP PW, you can directly apply the PW template without specifying attributes for the PW. After setting attributes for a PW template, you can update the PW template at any time. The modified PW template takes effect only after the **reset pw** command is run.

- If a PW attribute is specified in the **mpls l2vc** command, the corresponding PW attribute in the same PW template is invalid.
- If you do not specify a tunnel policy for a Martini connection, the default tunnel policy is used. By default, the LSP tunnel is preferentially selected and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- The parameters **raw** and **tagged** can be used only for Ethernet links.
- The MTU value is specified when you create Martini or PWE3 VLLs and is used for interconnection between the router and other devices.
- You must configure the primary PW before configuring the secondary PW and delete the secondary PW before deleting the primary PW.
- When creating VCs dynamically, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

Example

Create a Martini connection on the VLANIF interface.

```
<Huawei> system-view
[Huawei] vlan batch 10
[Huawei] interface vlanif 10
[Huawei-Vlanif10] mpls l2vc 10.2.2.9 100
```

Related Topics

12.12.3 display mpls l2vc

12.11.7 display mpls l2vpn forwarding-info

12.12.16 mpls l2vpn

Function

The **mpls l2vpn** command enables MPLS L2VPN and displays the MPLS L2VPN view.

The **undo mpls l2vpn** command disables MPLS L2VPN and deletes all the L2VPN configurations.

By default, the MPLS L2VPN function is disabled.

Format

mpls l2vpn

undo mpls l2vpn

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure MPLS L2VPN functions or perform configurations in the MPLS L2VPN view on the MPLS L2VPN network, run the **mpls l2vpn** command to enable MPLS L2VPN and enter the MPLS L2VPN view.

Prerequisites

Basic MPLS functions have been configured. For details, see the **mpls lsr-id** and **mpls** commands.

Precautions

When the command is configured, a P device does not need to be enabled with the MPLS L2VPN function.

After the **mpls l2vpn** command is executed:

- If MPLS L2VPN is disabled on the device, MPLS L2VPN is enabled and the MPLS L2VPN view is displayed.
- If MPLS L2VPN is enabled on the device, the MPLS L2VPN view is displayed.

Example

Enable MPLS L2VPN.

```
<Huawei> system-view
[Huawei] mpls lsr-id 10.1.1.1
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls l2vpn
[Huawei-l2vpn]
```

12.12.17 mpls l2vpn no-request-message

Function

The **mpls l2vpn no-request-message** command disables the device from sending L2VPN label request messages to a specified peer.

The **undo mpls l2vpn no-request-message** command re-enables the device to send L2VPN label request messages to a specified peer.

 Copyright © Huawei Technologies Co., Ltd.

By default, the system sends L2VPN label request messages to all its peers.

Format

mpls l2vpn no-request-message peer *ip-address*

undo mpls l2vpn no-request-message peer *ip-address*

Parameters

Parameter	Description	Value
peer *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

When a Huawei device and a non-Huawei device need to set up a PW using LDP but the non-Huawei device cannot process L2VPN label request messages, use this command to enable the two devices to communicate. Do not use this command in other conditions.

Example

Disable the device from sending L2VPN label request messages to a peer with the LSR ID being 2.2.2.9.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn no-request-message peer 2.2.2.9
```

12.12.18 mpls l2vpn oam-mapping

Function

The **mpls l2vpn oam-mapping** command enables the mapping between the AC status and the Packet Switching Network (PSN) status.

The **undo mpls l2vpn oam-mapping** command disables the mapping between the AC status and the PSN status.

By default, the mapping between the AC status and the PSN status is disabled.

Format

mpls l2vpn oam-mapping 3ah

 Copyright © Huawei Technologies Co., Ltd.

undo mpls l2vpn oam-mapping

Parameters

Parameter	Description	Value
3ah	Enables fault detection and fault notification defined in IEEE 802.3ah.	-

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In VLL FRR or PWE3 FRR scenarios, PEs and CEs do not advertise their primary/secondary status and link status to each other. PW OAM and AC OAM need to be configured to monitor PW and AC status respectively. OAM mapping is enabled on the PEs to associate PW OAM with AC OAM.

After the **mpls l2vpn oam-mapping** command is configured on a PE, the system generates the mapping table between the AC status and the PSN status. If a fault occurs on an AC, the local PE will notify the remote PE of the AC fault. If a fault occurs on a PW, the local PE will notify the local CE of the fault. Timely fault notification allows PEs and CEs to coordinate with each other to implement end-to-end FRR.

Prerequisites

OAM fault detection and notification have been configured for the corresponding AC.

Configuration Impact

After the mapping between the AC status and the PSN status is enabled, if a fault occurs on the local AC:

- If BFD for PW is enabled, the local AC notifies the remote PE of the AC fault using BFD and the signaling protocol.
- If BFD for PW is disabled, the local AC notifies the remote PE of the AC fault using the signaling protocol.

Follow-up Procedure

After configuring this command, run the **display mpls l2vc interface** command to check the AC link status. The AC link status is displayed in the **Local AC OAM State** field of the command output.

Example

Enable fault detection and notification defined in IEEE 802.3ah on an Ethernet interface.

```
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.1 101
[Huawei-GgiabitEthernet1/0/0] mpls l2vpn oam-mapping 3ah
```

Related Topics

12.12.5 display mpls l2vc oam-mapping

12.12.19 mpls l2vpn pw performance disable

Function

The **mpls l2vpn pw performance disable** command disables the function of PW performance information collection on a TDM interface.

The **undo mpls l2vpn pw performance disable** command restores the default setting.

By default, the function of PW performance information collection is enabled on a TDM interface.

Format

mpls l2vpn pw performance disable

undo mpls l2vpn pw performance disable

Parameters

None

Views

TDM interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PW is configured on a TDM interface, the function of PW performance information collection is automatically enabled on the TDM interface. The system collects statistics about the packets sent and received by the primary PW at an interval of 15 minutes. If other performance statistics collection methods are available or you want to further improve system performance, you can run the **mpls l2vpn pw performance disable** command to disable the function of PW performance information collection.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A PW has been configured on the interface because this command needs to be associated with a PW.

NOTE

This command applies to only static PWs and dynamic LDP PWs.

Follow-up Procedure

If the function of PW performance information collection is enabled, you can run the **display mpls l2vpn interface performance** command to view PW performance statistics collected during the latest 15 minutes to obtain the current working status of the primary PW.

Precautions

The **mpls l2vpn pw performance disable** and **undo mpls l2vpn pw performance disable** commands apply to only primary PWs.

Example

Disable PW performance information collection on Serial2/0/0.

```
<Huawei> system-view
[Huawei] interface serial 2/0/0
[Huawei-Serial2/0/0] mpls l2vpn pw performance disable
```

Related Topics

12.12.6 display mpls l2vpn interface performance

12.12.20 mpls l2vpn reroute

Function

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

The **undo mpls l2vpn reroute** command restores the default revertive switchover policy.

By default, delayed revertive switchover is configured in FRR or PW redundancy master/slave mode.

Format

mpls l2vpn reroute { { **delay** *delay-time* | **immediately** } [**resume** *resume-time*] | **never** }

undo mpls l2vpn reroute

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delay *delay-time*	Specifies the revertive switchover policy for the primary and secondary PWs as delayed revertive switchover, and sets the duration for delayed switchover.	The value is an integer that ranges from 10 to 1800, in seconds. The default value is 30.
immediately	Specifies the revertive switchover policy for the primary and secondary PWs as immediate revertive switchover.	-
resume *resume-time*	Specifies a delay after which the local device notifies the peer PE on the secondary PW of the recovery. You can set this parameter only in VLL FRR mode.	The value is an integer that ranges from 0 to 600, in seconds. The default value is 10.
never	Specifies the revertive switchover policy for the primary and secondary PWs to none revertive switchover. After the primary PW recovers, traffic is not switched to it until the secondary PW is faulty.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls l2vpn reroute** command configures the revertive switchover policy for the primary and secondary PWs in FRR or PW redundancy master/slave mode.

Prerequisites

The primary and secondary PWs have been configured in FRR or PW redundancy master/slave mode. The revertive switchover policy cannot be configured for PW redundancy independent mode.

Precautions

In VLL FRR mode and in PW redundancy master/slave mode, the PW revertive switchover policy is classified into the following modes:

- Immediate revertive switchover: When the primary PW recovers from a fault, the local PE switches traffic back to the primary PW immediately and notifies the peer PE on the secondary PW of the fault. In FRR mode, the local PE

 Copyright © Huawei Technologies Co., Ltd.

notifies the peer PE on the secondary PW of the recovery after a delay of *resume-time*. In PW redundancy master/slave mode, the parameter *resume-time* is not supported.

This revertive switchover applies to scenarios in which users hope traffic to be restored as soon as possible.

- Delayed revertive switchover: When the primary PW recovers from a fault, traffic is switched back to the primary PW after a period specified by *delay-time*. After traffic is switched back, the local device immediately notifies the peer device on the secondary PW of the fault. If *resume-time* is configured in FRR mode, the local device notifies the peer device on the secondary PW of the recovery after a delay of *resume-time*.

  On a large-scale network, packet loss caused by incomplete route convergence may occur during the switchback. To prevent this problem, configure traffic to be switched back after a delay.

- None revertive switchover: When the primary PW recovers from a fault, traffic is not switched back to the primary PW until the secondary PW becomes faulty.

  If you do not want traffic to be frequently switched between the primary and secondary PWs, you can use the non-revertive switchover.

In a CE asymmetrical networking, if the Ethernet OAM function is configured on a PE interface connected to a CE, and a revertive switchover policy is configured, the value of *resume-time* cannot be 0 seconds. The value must be equal to or greater than 1 second.

Example

Configure the device to switch traffic back to the primary PW 15 seconds after the primary PW recovers from a fault, notify the peer PE on the secondary PW of the fault when a switchover is performed, and notify the peer PE of the secondary PW of the recovery 20 seconds later.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.9 100
[Huawei-GigabitEthernet1/0/0] mpls l2vc 2.2.2.9 200 secondary
[Huawei-GigabitEthernet1/0/0] mpls l2vpn reroute delay 15 resume 20
```

Related Topics

12.12.15 mpls l2vc

12.12.21 mpls l2vpn service-name

Function

The **mpls l2vpn service-name** command sets the name of an SVC or Martini VLL service.

The **undo mpls l2vpn service-name** command deletes the configured L2VPN service name.

By default, no L2VPN service name is configured in the system.

 Copyright © Huawei Technologies Co., Ltd.

Format

mpls l2vpn service-name *service-name*

undo mpls l2vpn service-name

Parameters

Parameter	Description	Value
service-name	Specifies the name of an L2VPN service. This parameter uniquely identifies an L2VPN service on a PE.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an SVC or Martini VLL service is uniquely identified by the combination of the VC ID and VC type, which are hard to remember and make maintenance complex. When a service name is used to uniquely identify an L2VPN service, the name can be defined based on requirements and the NMS operator can maintain the L2VPN service by clicking the name on the NMS graphical user interface (GUI). This simplifies operation and maintenance.

Prerequisites

An SVC or Martini VLL service has been configured on a service interface. A primary PW and a secondary PW can be configured for a Martini VLL or PWE3 service.

Precautions

On each PE, an L2VPN service name is unique. If an L2VPN service name has been used by a PW, it cannot be configured for another PW, or the system will display an error message.

If an L2VPN service already has a service name, this service name will be overwritten when a new name is configured for the L2VPN service. Therefore, when changing an L2VPN service name, you can directly configure a new service name without deleting the original one.

- Because the primary and secondary PWs are configured on the same interface, they are regarded as one PW, and a service name is configured for both of them.

 Copyright © Huawei Technologies Co., Ltd.

- On each PE, an L2VPN service name is unique.
- The **mpls l2vpn service-name** command cannot be run on a loopback interface.

Example

Set an L2VPN service name to **pw1** on a service interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 10.1.1.1 1
[Huawei-GigabitEthernet1/0/0] mpls l2vpn service-name pw1
```

Related Topics

12.11.2 ccc interface out-interface

12.12.22 mpls l2vpn stream-dual-receiving

Function

The **mpls l2vpn stream-dual-receiving** command configures an interface to receive packets from both the primary and secondary PWs.

The **undo mpls l2vpn stream-dual-receiving** command disables an interface from receiving packets from both the primary and secondary PWs.

By default, an interface cannot receive packets from the secondary PW.

Format

mpls l2vpn stream-dual-receiving

undo mpls l2vpn stream-dual-receiving

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network configured with PWE3 FRR, the **mpls l2vpn stream-dual-receiving** command must be run on a PE to which the CE is single homed, so that the PE can receive packets from both the primary and secondary PWs. This prevents packet loss during the PW switchover process.

 Copyright © Huawei Technologies Co., Ltd.

If the command is not run, the PE receives packets only from the primary PW. This causes packet loss during a traffic switchover. After the primary PW recovers and a traffic switchover is triggered, the secondary PW on the PE becomes the primary PW and the PE notifies the peer of the status change. A delay in signaling transmission causes the peer PE to send packets along the secondary PW. After the PE receiving packets from the secondary PW, the PE discards the packets, resulting in packet loss.

Prerequisites

Primary and secondary PWs have been configured.

Precautions

The **mpls l2vpn stream-dual-receiving** command applies to only PWE3 L2VPN.

Example

Enable the device to receive packets from both the primary and secondary PWs on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] mpls l2vc 1.1.1.1 1
[Huawei-GigabitEthernet1/0/0] mpls l2vc 2.2.2.2 2 secondary
[Huawei-GigabitEthernet1/0/0] mpls l2vpn stream-dual-receiving
```

Related Topics

12.11.20 mpls l2vc

12.12.23 mpls l2vpn vccv bfd-cv-negotiation fault-detection-only

Function

The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type for BFD CV packets to be sent to remote peers.

The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default configuration.

By default, the device sends BFD CV packets with the encapsulation type 0x08 to all remote peers.

Format

mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address* { **enable** | **disable** }]

undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only [**peer** *peer-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the IP address of a remote peer.	The value is in dotted decimal notation.
enable	Sets the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.	-
disable	Set the encapsulation type 0x08 for BFD CV packets to be sent to a specified remote peer.	-

Views

MPLS L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Virtual Circuit Connectivity Verification (VCCV) is a mechanism to detect and diagnose end-to-end faults on PWs. VCCV provides a control channel between a PW's ingress and egress over which connectivity verification (CV) messages can be sent. A VCCV message includes a BFD control packet encapsulated as specified by the CV type. A BFD CV packet can be transmitted over a VCCV control channel after being encapsulated using BFD IP/UDP. BFD IP/UDP encapsulation for BFD CV packets are classified into two types:

- 0x04: used only for PW fault detection.
- 0x08: used for PW fault detection and AC/PW status signaling.

To control the encapsulation type of BFD CV packets to be sent to remote peers, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command.

- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to all remote peers.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only** command restores the default encapsulation type 0x08 for BFD CV packets to be sent to all remote peers.
- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **enable** command sets the encapsulation type to 0x04 for BFD CV packets to be sent to a specified remote peer.

 Copyright © Huawei Technologies Co., Ltd.

- The **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **disable** command sets the encapsulation type to 0x08 for BFD CV packets to be sent to a specified remote peer.
- The **undo mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* command restores the global encapsulation type for BFD CV packets to be sent to a specified remote peer.

Dynamic PWs support VCCV by default, and can use LDP signaling to advertise local attributes to remote peers. The default encapsulation type of BFD CV packets is 0x08. If a remote peer supports the encapsulation type 0x04 and BFD is used for communication, run the **mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer** *peer-address* **enable** command to change the encapsulation type of BFD CV packets to be sent to this peer to 0x04.

Precautions

After this command is run, PWs may be re-established, which causes a short service interruption.

Example

Set the encapsulation type 0x04 for BFD CV packets to be sent to remote peers.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only
```

Set the encapsulation type 0x04 for BFD CV packets to be sent to a specified remote peer.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn vccv bfd-cv-negotiation fault-detection-only peer 10.10.10.1 enable
```

12.12.24 mpls static-l2vc

Function

The **mpls static-l2vc** command creates a static VC.

The **undo mpls static-l2vc** command deletes the static VCs.

By default, no static VC is created.

Format

mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

undo mpls static-l2vc [**secondary**]

undo mpls static-l2vc { { **destination** *ip-address* | **pw-template** *pw-template-name vc-id* } * | **destination** *ip-address vc-id* } **transmit-vpn-label** *transmit-label-*

value **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tnl-policy-name* | [**control-word** | **no-control-word**] | [**raw** | **tagged**] | **idle-code** *idle-code-value* | **jitter-buffer** *depth* | **tdm-encapsulation** *number* | **tdm-sequence-number** | **secondary**] *

Parameters

Parameter	Description	Value
destination *ip-address*	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
pw-template *pw-template-name*	Specifies the name of a static PW template.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
vc-id	Specifies the VC ID.	The value is an integer that ranges from 1 to 4294967295.
transmit-vpn-label *transmit-label-value*	Specifies the value of a transmit label.	The value is an integer that ranges from 0 to 1048575.
receive-vpn-label *receive-label-value*	Specifies the value of a receive label.	The value is an integer that ranges from 16 to 1023.
tunnel-policy *tnl-policy-name*	Specifies the name of a tunnel policy.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
control-word | **no-control-word**	Enables or disables the control word function. By default, the control word function is disabled.	-
raw	Removes the service-delimiting (SD) tag from a packet. This parameter is required when the AC is an Ethernet link.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tagged	Retains the SD tag in a packet. This parameter is required when the AC is an Ethernet link.	-
idle-code *idle-code-value*	Specifies the idle code that is filled in manually when a jitter buffer underflow occurs. This parameter is required when the AC is a TDM link.	The value ranges from 00 to FF, in hexadecimal notation. The default value is FF.
jitter-buffer *depth*	Specifies the depth of the jitter buffer, that is, the allowed maximum jitter delay. This parameter is required when the AC is a TDM link.	The value is an integer that ranges from 4 to 64, in milliseconds. The default value is 8 ms.
tdm-encapsulation *number*	Specifies the number of TDM frames encapsulated in a CESoPSN packet. This parameter is required when the AC is a TDM link.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.
tdm-sequence-number	Sets the sequence number of the first frame encapsulated for TDM transparent transmission to 1. This parameter is required when the AC is a TDM link.	-
secondary	Configures the PW as a static secondary PW. By default, a created PW is a primary PW.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an L2VPN networking, you can use this command to create a static VC between two PEs connected to CEs.

Precautions

- An interface cannot function as an L2VPN AC interface and L3VPN AC interface at the same time. After an interface is bound to an L2VPN, Layer 3 features such as the IP address and routing protocol on this interface become invalid.
- You can set attributes for a static PW template, including the remote peer, tunnel policy, control word, and VCCV. When configuring a static PW, you can directly use the static PW template without specifying attributes for the PW. After setting attributes for a static PW template, you can update the static PW template at any time. The modified static PW template takes effect only after the **reset pw** command is run.
- Static VCs must be created on PEs at both ends. The destination address of a VC is the LSR ID of the peer PE. The transmit label of the PE at one end is the receive label of the PE at the other end. If the labels do not match, traffic may fail to be forwarded even though the **static-12vc** field is displayed as Up.
- If no tunnel policy is specified, the default tunnel policy is used. The default policy specifies that traffic is forwarded along the LSP and only one tunnel is used for load balancing. If a tunnel policy name is specified but the tunnel policy is not configured, the default tunnel policy is used.
- When configuring a static VC, note that the value of the transmit label ranges from 0 to 1048575. This ensures the communication between the device and different types of devices.
- When creating static VCs, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *tnl-policy-name*, **control-word**, **no-control-word**, **idle-code** *idle-code-value*, **jitter-buffer**, **tdm-encapsulation** *number*, and **tdm-sequence-number**.

NOTE

- If a sub-interface is bound to a VLL, the sub-interface can be deleted only after the sub-interface is unbound from the VLL.
- If a sub-interface is bound to a VLL, you cannot change the encapsulation type of the main interface.
- To configure TDM PWE3, run the **link-protocol tdm** command to set the link layer protocol to TDM before you run this command to configure a PW.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a static VC. Set the LSR ID of the peer device to 1.1.1.1, transmit label to 100, and receive label to 100.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100 receive-vpn-label 100
```

Delete a static VC.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] undo mpls static-l2vc
```

Related Topics

12.12.7 display mpls static-l2vc

12.12.16 mpls l2vpn

12.12.25 mpls switch-l2vc

Function

The **mpls switch-l2vc** command configures PW switching on the SPE to implement multi-segment PWs.

The **undo mpls switch-l2vc** command deletes PW switching.

The default policy is used for PW switching. In the default policy, LSP tunnels are used and the number of routes for load balancing is 1.

Format

Static PW

mpls switch-l2vc *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**control-word-transparent**]

Dynamic PW

mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**control-word-transparent**]

Mixed PW

 Copyright © Huawei Technologies Co., Ltd.

mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**timeslotnum** *timeslotnum*] [**tdm-encapsulation** *number*] [**control-word-transparent**]

undo mpls switch-l2vc *ip-address vc-id* [**tunnel-policy** *policy-name*] **between** *ip-address vc-id* **trans** *trans-label* **recv** *received-label* [**tunnel-policy** *policy-name*] **encapsulation** *encapsulation-type* [**mtu** *mtu-value*] [**control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**] | [**no-control-word**] [**cc alert cv lsp-ping**]] [**timeslotnum** *timeslotnum*] [**tdm-encapsulation** *number*] [**control-word-transparent**]

undo mpls switch-l2vc { *ip-address vc-id* **encapsulation** *encapsulation-type* | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies the LSR ID of a peer device on the PW.	The value is in dotted decimal notation.
vc-id	Specifies the L2VC ID.	The value is an integer that ranges from 1 to 4294967295.
trans *trans-label*	Specifies the static label for sending packets.	The value is an integer that ranges from 0 to 1048575.
recv *received-label*	Specifies the static label for receiving packets.	The value is an integer that ranges from 16 to 1023.
tunnel-policy *policy-name*	Specifies a tunnel policy name for the L2VC. If no name is specified for a tunnel policy, the default tunnel policy is used. The LSP tunnel is preferred and only one LSP is used for load balancing in the default tunnel policy. If the name of the tunnel policy is specified but no tunnel policy is configured, the default tunnel policy is used.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
between	Specifies the switching PW that corresponds to the PW	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
encapsulation *encapsulation-type*	Specifies the encapsulation type of a static PW.	The encapsulation types supported by PW switching are **ethernet**, **vlan**, **satop-e1**, and **cesopsn-basic**.
mtu *mtu-value*	Specifies the MTU for negotiating dynamic PW signaling. If the non-default MTU is set when you configure a dynamic PW, you need to set the MTU manually when configuring mixed PW switching; otherwise, the signaling negotiation at the dynamic PW side may fail.	The value is an integer that ranges from 46 to 9600.
control-word	Enables the control word function. By default, the control word function is disabled.	-
no-control-word	Disable the control word function.	-
cw	Indicates the mode in which the control word function is enabled.	-
alert	Indicates the label alert tunnel for VCCV ping.	-
cv	Indicates connectivity verification, which is enabled by default.	-
lsp-ping	Indicates connectivity verification in LSP ping mode for VCs, which is enabled by default.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
control-word-transparent	Enables transparent transmission of the control word. In the scenario where a PE is dual homed to SPEs and BFD for PW is enabled, transparent transmission of the control word must be enabled on the SPEs; otherwise, the BFD negotiation fails. By default, transparent transmission of the control word is disabled.	-
timeslotnum *timeslotnum*	Specifies the number of timeslots in TDM PWE3.	The value is an integer. ● If the encapsulation type of a non-channelized interface is **satop-e1**, you do not need to set the number of timeslots and the total number of supported timeslots is used by default. ● If the encapsulation type of a channelized interface is **cesopsn-basic**, you need to set this number and the value ranges from 1 to 32.
tdm-encapsulation *number*	Specifies the number of TDM frames encapsulated in a packet.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.
all	Deletes all PW switching.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **mpls switch-l2vc** command configures PW switching on the SPE to implement multi-segment PWs.

PW switching can be classified into dynamic mode, static mode, and mixed mode. You can create PW switching of different types using different commands to meet site requirements:

- **Configuring static PW switching**: The two PW segments connected by an SPE are both static PWs. Static PW switching apples when static PWs are used on the entire network.
- **Configuring dynamic PW switching**: The two PW segments connected by an SPE are both dynamic PWs. Dynamic PW switching applies when dynamic PWs are used on the entire network.
- **Configuring mixed PW switching**: A mixed PW switching applies when an SPE connects a dynamic PW and a static PW.

Precautions

You need to configure the PW label for the static PW switching and for the static PW in the mixed PW switching.

The configuration of static PW switching is simple. The remote label is sent from two neighboring ends (UPE or SPE) to the SPE through signaling. The CW and the VCCV are sent from two UPE nodes to the SPE through signaling.

When you configure mixed PW switching, the value of *ip-address vc-id* before **between** in the command is for the dynamic PW, and the value of *ip-address vc-id* after **between** in the command is for the static PW. The two values cannot be interchanged.

When you configure static PW switching, the parameters that can be configured vary with the PW encapsulation type and the details are as follows:

- If *encapsulation-type* is set to **ethernet** or **vlan**, the following parameters can be specified: **control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**], and [**no-control-word**] [**cc alert cv lsp-ping**].
- If *encapsulation-type* is set to **satop-e1**, the following parameters can be specified: [**no-control-word**] [**cc alert cv lsp-ping**].
- If *encapsulation-type* is set to **cesopsn-basic**, the following parameters can be specified: **control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**], and [**no-control-word**] [**cc alert cv lsp-ping**].

 Copyright © Huawei Technologies Co., Ltd.

When you configure mixed PW switching, the parameters that can be configured vary with the PW encapsulation type and the details are as follows:

- If *encapsulation-type* is set to **ethernet** or **vlan**, the following parameters can be specified: **mtu** *mtu-value*, **control-word** [**cc** { **alert** | **cw** } * **cv lsp-ping**], and [**no-control-word**] [**cc alert cv lsp-ping**].
- If *encapsulation-type* is set to **satop-e1**, the following parameters can be specified: **mtu** *mtu-value*, **control-word**, **no-control-word**, and **tdm-encapsulation** *number*.
- If *encapsulation-type* is set to **cesopsn-basic**, the following parameters can be specified: **mtu** *mtu-value*, **control-word**, **no-control-word**, **timeslotnum** *timeslotnum*, and **tdm-encapsulation** *number*.

  The **timeslotnum** *timeslotnum* must be configured.

NOTE

- The VC IDs for PW switching can be different.
- The combination of the PW ID and PW type must be unique on each node. The PW IDs at two ends of PW switching can be the same.
- When creating PW switching, the latest configurations of some parameters override the previous ones. The parameters include **tunnel-policy** *policy-name*, **control-word-transparent**, **control-word**, **no-control-word**, **tdm-encapsulation** *number*, **timeslotnum** *timeslotnum*, and **mtu** *mtu-value*.

Example

Configure dynamic PW switching.

```
<Huawei> system-view
[Huawei] mpls switch-l2vc 1.1.1.9 100 between 3.3.3.9 100 encapsulation vlan
```

Configure static PW switching.

```
<Huawei> system-view
[Huawei] mpls switch-l2vc 1.1.1.9 100 trans 100 recv 100 between 3.3.3.9 100 trans 200 recv 200
encapsulation vlan
```

Configure mixed PW switching.

```
<Huawei> system-view
[Huawei] mpls switch-l2vc 1.1.1.9 100 between 3.3.3.9 100 trans 200 recv 200 encapsulation vlan mtu
1500
```

Delete PW switching.

```
<Huawei> system-view
[Huawei] undo mpls switch-l2vc 1.1.1.9 100 encapsulation vlan
```

Related Topics

12.12.9 display mpls switch-l2vc
12.11.21 mpls l2vpn

12.12.26 mtu (PW template view)

Function

The **mtu** command specifies the MTU in a PW template.

The **undo mtu** command restores the default setting.

By default, the MTU in a PW template is 1500.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU in a PW template.	The value is an integer that ranges from 46 to 9600.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When creating a PW template, run the **mtu** command to specify the MTU for the PW template.

Precautions

When creating a Martini VLL or PWE3 VLL, if you set the MTU value by specifying **mtu** *mtu-value* in the **mpls l2vc** command. If you do not specify **mtu** *mtu-value*, the MTU in the PW template takes effect. If you do not specify **mtu** *mtu-value* in the **mpls l2vc** command and do not set the MTU in the PW template, the device uses the default MTU value 1500.

Example

Configure the MTU for the PW template **pw1**.

```
<Huawei> system-view
[Huawei] pw-template pw1
[Huawei-pw-template-pw1] mtu 1600
```

Related Topics

12.12.29 pw-template

12.12.27 peer-address

Function

The **peer-address** command assigns a remote IP address to a PW template.

The **undo peer-address** command deletes the remote IP address assigned to a PW template.

By default, a PW template is not configured with a remote IP address.

Format

peer-address *ip-address*

undo peer-address

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of the peer. Generally, *ip-address* is a loopback address of the peer and needs be the same as the destination address of the tunnel.	The value is in dotted decimal notation.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

ip-address in this command is the same as that in the **mpls l2vc** command. You can update the IP address of the peer in real time. After updating the IP address, run the **reset pw** command to make it take effect if the PW is used. If the PW is not used, you do not need to restart the PW after updating the IP address.

Example

Assign a remote IP address to a PW template.

```
<Huawei> system-view
[Huawei] pw-template pwt
[Huawei-pw-template-pwt] peer-address 1.1.1.1
```

Modify a remote IP address in a PW template.

```
<Huawei> system-view
[Huawei] pw-template pwt
[Huawei-pw-template-pwt] undo peer-address
[Huawei-pw-template-pwt] peer-address 2.2.2.2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.12.29 pw-template

12.12.28 ping vc

Function

The **ping vc** command detects the status of a PW.

Format

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word** [**remote** *remote-ip-address peer-pw-id* | **draft6**] * [**ttl** *ttl-value*] [**uniform**]

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **control-word remote** *remote-ip-address peer-pw-id* **sender** *sender-address* [**ttl** *ttl-value*] [**uniform**]

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address* | **draft6**] * [**uniform**]

ping vc *pw-type pw-id* [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-exp** *exp-value* | **-r** *reply-mode* | **-v**] * **normal** [**no-control-word**] [**remote** *remote-ip-address peer-pw-id*] [**ttl** *ttl-value*] [**uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the encapsulation type of a local PW.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the ID of a local PW.	The value is an integer that ranges from 1 to 4294967295.
-c *echo-number*	Specifies the number of Echo Request messages to be sent. If the network works unstably, you can set this parameter to a larger value to test network quality based on the packet loss ratio.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-m *time-value*	Specifies the interval for sending Echo Request messages. Each time after the source sends an Echo Request message by using the **ping vc** command, it waits a period of time (2000 ms by default) before sending the next Echo Request message. You can set the interval for sending Echo Request messages through the parameter *time-value*. If the network works unstably, the value should be larger than or equal to 2000 ms.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.
-s *data-bytes*	Specifies the number of bytes of the sent Echo Request messages.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100. The value must be smaller than the MTU value of the interface.
-t *timeout-value*	Specifies the timeout period for sending Echo Request messages.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-exp *exp-value*	Specifies the EXP value of the sent Echo Request messages.	The value is an integer that ranges from 0 to 7. The default value is 0.
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply messages. ● 1: No MPLS Echo Reply message is returned. ● 2: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply messages are encapsulated into IPv4/IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply messages are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-v	Displays the detailed information.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-control-word	Disables the control word function.	-
control-word	Enables the control word function. The switching node along a multi-segment PW does not transmit ping packets. When the control word function is enabled, you can ping only the termination node of the PW. Before using the control word to ping the PW, you must enable the control word for a PW.	-
remote	Specifies information about the PW on the remote PE. Information specified by the remote PE is finally encapsulated into the ping packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the ping packets is the information about the PW on the local end, which applies to single-segment PWs.	-
peer-pw-id	Specifies the ID of the PW on the peer.	The value is an integer that ranges from 1 to 4294967295. By default, the peer PW ID is the same as the local PW ID.
draft6	Specifies the version of the **ping vc** command. If this parameter is specified, the ping operation is performed based on "draft-ietf-mpls-lsp-ping-06".	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. In the case of a multi-segment PW, if the ping operation is performed in control word mode, the IP address of the termination node must be specified. In MPLS router alert mode, the IP address of any switching node or the termination node can be specified. Then, the Echo Request message is sent to the peer and then sent back.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
label-alert	Specifies the label alert mode. The switching node along a multi-segment PW sends ping packets forcibly. In MPLS router alert mode, you can ping any switching node along the PW.	-
normal	Specifies the normal mode, that is, the TTL detection mode. In this mode, control word and router alert are not encapsulated in to MPLS Echo Request messages, and TTL values are used to detect PW connectivity.	-
ttl *ttl-value*	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default value is 64.
sender *sender-address*	Specifies a source address. For end-to-end detection of a multi-segment PW, a source IP address needs to be specified for a public network device that communicates with the remote PE. Generally, the source IP address is the address of the adjacent SPE or UPE.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. The **ping vc** command can be used to check a PW in the following scenarios:

VLL networking

Based on VLL types, the VLL PW ping can be classified into the following types:

- PWE3 VLL PW ping: In a PWE3 VLL networking, a PW ping is initiated to check the connectivity of a PW. A PWE3 VLL PW ping can be performed in control word mode, TTL mode, or label alert mode. In a ping test, a local PE sends an Echo Request message to the peer PE. After receiving the message, the peer PE abstracts and sends FEC information to the L2VPN module to determine whether the message has reached the egress. If so, the peer PE returns an Echo Reply message.

If a PW fault is detected by using the **ping vc** command, the **tracert vc** command can be used to locate the fault. Both the **ping vc** command and the **tracert vc** command can properly check the connectivity of PWs and locate faults.

Prerequisites

The MPLS module has been enabled on the device and works properly.

Precautions

control-word is recommended to detect an entire PW. Even though **label-alert** can be used to check the entire PW, the whole process is the same as the forwarding process only when **control-word** is used.

The execution of the **ping vc** command terminates when either of the following situations occurs:

- The ping packet reaches the egress.
- The TTL value of the ping packet reaches the upper threshold.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

Example

Run the **ping vc** command in label alert mode on the device to check the connectivity of an Ethernet PW.

```
<Huawei> ping vc ethernet 100 -c 10 -m 10 -s 65 -t 100 -v label-alert remote 2.2.2.2
  Reply from 2.2.2.2: bytes=65 Sequence=1 time = 31 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=2 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=3 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=4 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=5 time = 32 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=6 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=7 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=8 time = 16 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=9 time = 15 ms Return Code 3, Subcode 1
  Reply from 2.2.2.2: bytes=65 Sequence=10 time = 32 ms Return Code 3, Subcode 1

--- FEC: FEC 128 PSEUDOWIRE (NEW). Type = ethernet, ID = 100 ping statistics
  10 packet(s) transmitted
  10 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 15/21/32 ms
```

Related Topics

12.12.34 tracert vc

12.12.29 pw-template

Function

The **pw-template** command creates a PW template. In the PW template, you can set attributes for a PW, such as the peer, control word, and tunnel policy.

The **undo pw-template** command deletes a PW template.

By default, no PW template is created.

Format

pw-template *pw-template-name*

undo pw-template *pw-template-name*

Parameters

Parameter	Description	Value
pw-template-name	Specifies the PW template name.	The value is a string of 1 to 19 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Importing a PW template simplifies the configuration of PWs with similar attributes.

Prerequisites

L2VPN has been enabled by running the command.

Precautions

- If a PW template is applied to a PW, the PW template cannot be deleted.
- When a PW template is applied to a PW, the PW uses the PW attributes specified on the interface if the PW attributes specified on the interface are different from those specified in the template.
- When modifying attributes in a PW template, run the **reset pw** command to make the modification take effect. This may cause PW disconnection and reconnection.
- After a PW is bound to a link detection protocol, the remote IP address in the PW template cannot be changed. To change the remote IP address, unbind the PW from the link detection protocol.

Example

Create a PW template named **pwt1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pw-template pwt1
[Huawei-pw-template-pwt1]
```

Related Topics

12.12.2 control-word
12.12.26 mtu (PW template view)
12.12.11 display pw-template
12.12.27 peer-address
12.12.33 tnl-policy (PW template view)
12.12.30 reset pw

12.12.30 reset pw

Function

The **reset pw** command re-creates a PW or a PW template.

Format

reset pw { *pw-id pw-type* | **pw-template** *pw-template-name* }

Parameters

Parameter	Description	Value
pw-id	Specifies the ID of a VC connected to L2VPN.	The value is an integer that ranges from 1 to 4294967295.
pw-type	Specifies the encapsulation type of a PW.	Currently, PWs of the following types are supported: **ethernet**, **vlan**, **satop-e1**, and **cesopsn-basic**.
pw-template	Re-creates all PWs in the PW template.	-
pw-template-name	Specifies the PW template name.	The value is an existing PW template name.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After changing the parameters in a PW template, you need to run the **reset pw pw-template** command to make the modification take effect. The configuration

on the PW template applies to all PWs using this PW template. You can configure the attributes of a PW by using a PW template or commands. The attributes configured by using commands take precedence over those configured by using the template. If you configure PW attributes by using commands, the corresponding attributes in the PW template do not take effect. Therefore, if you run the **reset pw pw-template** and **reset pw** *pw-id* commands, the PW attributes remain unchanged. To change a PW attribute, configure the attribute in the PW template but do not configure attribute by using a command.

Example

Re-create a PW by specifying the VC ID and VC type.

```
<Huawei> reset pw 100 vlan
```

Re-create all PWs that use the PW template named **pwt1**.

```
<Huawei> reset pw pw-template pwt1
```

Related Topics

12.12.29 pw-template

12.12.31 snmp-agent trap enable feature-name l2vpn

Function

The **snmp-agent trap enable feature-name l2vpn** command enables the trap function for the L2VPN module.

The **undo snmp-agent trap enable feature-name l2vpn** command disables the trap function for the L2VPN module.

By default, the trap function is disabled for the L2VPN module.

Format

snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

undo snmp-agent trap enable feature-name l2vpn [**trap-name** { **hwcccvcdown** | **hwcccvcup** | **hwpwvcbackup** | **hwpwvcdeleted** | **hwpwvcdown** | **hwpwvcstatuschange** | **hwpwvcswitchptow** | **hwpwvcswitchwtop** | **hwpwvcup** | **hwsvcdeleted** | **hwsvcdown** | **hwsvcswitchptow** | **hwsvcswitchwtop** | **hwsvcup** | **hwVpwsPwRedundancyDegraded** | **hwVpwsPwRedundancyDegradedClear** }]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trap-name	Indicates the traps of L2VPN events of specified types.	-
hwcccvcdown	Enables or disables the trap indicating that the status of a CCC VC changes to Down.	-
hwcccvcup	Enables or disables the trap indicating that the status of a CCC VC changes to Up.	-
hwpwvcbackup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Backup.	-
hwpwvcdeleted	Enables or disables the trap indicating that a PWE3 VC is deleted.	-
hwpwvcdown	Enables or disables the trap indicating that the status of a PWE3 VC changes to Down.	-
hwpwvcstatuschange	Enables or disables the trap indicating that the status of a PWE3 VC changes.	-
hwpwvcswitchptow	Enables or disables the trap indicating that a PWE3 PW changes from the secondary state to the primary state.	-
hwpwvcswitchwtop	Enables or disables the trap indicating that a PWE3 PW changes from the primary state to the secondary state.	-
hwpwvcup	Enables or disables the trap indicating that the status of a PWE3 VC changes to Up.	-
hwsvcdeleted	Enables or disables the trap indicating that an SVC is deleted.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwsvcdown	Enables or disables the trap indicating that the status of an SVC changes to Down.	-
hwsvcswitchptow	Enables or disables the trap indicating that an SVC PW changes from the secondary state to the primary state.	-
hwsvcswitchwtop	Enables or disables the trap indicating that an SVC PW changes from the primary state to the secondary state.	-
hwsvcup	Enables or disables the trap indicating that the status of an SVC changes to Up.	-
hwVpwsPwRedundancyDegraded	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS degrades.	-
hwVpwsPwRedundancyDegradedClear	Indicates a Huawei-specific trap reported when the primary or secondary PW for PW APS recovers.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The L2VPN module is not configured with the function of excessive traps. To enable the traps of one or more events, specify **trap-name**.

Example

Enable the system to generate an alarm when a VC in CCC mode goes Down.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name l2vpn trap-name hwcccvcdown
```

Related Topics

12.11.14 display snmp-agent trap feature-name l2vpn all

12.12.32 tdm-encapsulation-number

Function

The **tdm-encapsulation-number** command configures the number of TDM frames encapsulated in a Circuit Emulation Services over Packet Switch Network (CESoPSN) or Structure-Agnostic Time Division Multiplexing over Packet (SAToP) packet in the TDMoPSN application.

The **undo tdm-encapsulation-number** command restores the default number of TDM frames encapsulated in a CESoPSN or SAToP packet.

By default, the number of encapsulated TDM frames in a CESoPSN or SAToP packet is 8.

Format

tdm-encapsulation-number *number*

undo tdm-encapsulation-number

Parameters

Parameter	Description	Value
number	Specifies the number of TDM frames encapsulated in a CESoPSN or SAToP packet.	The value is an integer, which can be 8, 16, 24, 32, or 40. The default value is 8. When the interface card where the AC interface locates is 8SA, 8E1T1-M or 8E1T1-F, the interface can encapsulate a maximum of 16 TDM frames in a packet. If the value is larger than 16, the interface only encapsulates 16 TDM frames in a packet.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a dynamic PW is configured on a TDM interface, three parameters need to be negotiated between the two ends of the PW. The parameters are the RTP header, time slot number, and time slot number x number of encapsulated frames.

 Copyright © Huawei Technologies Co., Ltd.

You can configure the number of TDM frames encapsulated in each PW packet. The smaller the number of frames encapsulated in a packet, the shorter the transmission delay but the larger the encapsulation overhead. The larger the number of frames encapsulated in a packet, the higher the bandwidth utilization but the longer the encapsulation delay.

Prerequisite

A PW template has been created and the PW template view is displayed by running the **pw-template** command in the system view.

Configuration Impact

After the **tdm-encapsulation-number** command is run, the two ends of a PW will negotiate the number of frames encapsulated in each packet. If the values at two ends of a PW are different, the PW cannot go Up.

Follow-up Procedure

After running the **tdm-encapsulation-number** command, run the **reset pw** command to enable the attributes in the PW template to take effect on the PW. To check whether the configuration of the number of TDM frames encapsulated in each packet has taken effect on the PW, run the **display mpls l2vc** command to view the **local TDM Encap Num** field.

Precautions

The **mpls l2vc** command can also be used to configure the number of TDM frames encapsulated in each packet if **tdm-encapsulation** is specified in the command. If both the **mpls l2vc** command and the **tdm-encapsulation-number** command are used to configure the number of TDM frames encapsulated in each packet, the value specified by the **mpls l2vc** command takes precedence over the **tdm-encapsulation-number** effect.

Example

Set the number of the TDM frames encapsulated in a CESoPSN or SAToP packet to 16.

```
<Huawei> system-view
[Huawei] pw-template tdmpw
[Huawei-pw-template-tdmpw] tdm-encapsulation-num 16
```

Related Topics

12.12.13 jitter-buffer depth

12.12.29 pw-template

12.12.33 tnl-policy (PW template view)

Function

The **tnl-policy** command configures a tunnel policy for a PW template.

The **undo tnl-policy** command deletes the tunnel policy configured for a PW template.

By default, no tunnel policy is configured for a PW template.

 Copyright © Huawei Technologies Co., Ltd.

Format

tnl-policy *policy-name*

undo tnl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the tunnel policy name of a PW.	The value is a string of 1 to 39 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

PW template view

Default Level

2: Configuration level

Usage Guidelines

The **tnl-policy** command specifies the a PWE3 tunnel policy based on which a PW selects a tunnel to be associated with.

If no policy is configured, an LSP tunnel is selected and load balancing is not performed.

Example

Configure a tunnel policy named **policy1** for a PW template named **pwt**.

```
<Huawei> system-view
[Huawei] pw-template pwt
[Huawei-pw-template-pwt] tnl-policy policy1
```

Related Topics

12.12.29 pw-template

12.12.34 tracert vc

Function

The **tracert vc** command detects the status of a PW or locates a faulty node on a PW in Down state.

Format

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word** [**draft6**] [**full-lsp-path**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-ip-address* [**ptn-mode** | **full-lsp-path**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **control-word remote** *remote-pw-id* **draft6** [**full-lsp-path**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **label-alert** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**uniform**]

tracert vc *pw-type pw-id* [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **normal** [**no-control-word**] [**remote** *remote-ip-address*] [**full-lsp-path**] [**draft6**] [**uniform**]

Parameters

Parameter	Description	Value
pw-type	Specifies the PW type.	Currently, PWs of the following types are supported: **ethernet**, **vlan**.
pw-id	Specifies the local PW ID.	The value is an integer that ranges from 1 to 4294967295.
-exp *exp-value*	Specifies the EXP value in the outer label of an MPLS Echo Request packet. The default value is 0.	The value is an integer that ranges from 0 to 7.
-f *first-ttl*	Specifies the initial Time-to-Live (TTL).	The value is an integer that ranges from 1 to 255, and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from 1 to 255, and must be larger than the value of *first-ttl*. The default value is 30.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-r *reply-mode*	Specifies the mode in which the peer returns MPLS Echo Reply packets. ● 1: No MPLS Echo Reply packet is returned. ● 2: The MPLS Echo Reply packet is encapsulated in IPv4/IPv6 UDP packets. ● 3: MPLS Echo Reply packets are encapsulated in IPv4/IPv6 /IPv6 UDP packets carrying the Router Alert option. ● 4: MPLS Echo Reply packets are returned through the control channel of the application plane.	The value is an integer that ranges from 1 to 4.
-t *timeout-value*	Specifies the timeout interval of an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
control-word	Indicates that the control word is encapsulated in the MPLS Echo Request packet.	-
label-alert	Indicates that the router alert label is encapsulated in the MPLS Echo Request packet.	-
no-control-word	Indicates that the control word is not encapsulated in the MPLS Echo Request packet.	-
normal	Indicates the normal mode where the router alert label and control word are not encapsulated in the MPLS Echo Request packet.	-
remote	Specifies information about the PW on the remote PE.	-
remote-ip-address	Specifies the remote IP address. By default, the system searches for the IP address of the next hop based on the PW on the local PE. If **label-alert** is configured, you can specify the IP address of any switching node or the termination node.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remote-pw-id	Specifies the ID of the remote PW. By default, the ID of the local PW is used. If the tracert operation is performed in control word mode for a multi-segment PW, the IP address of the termination node must be specified.	-
ptn-mode	Specifies the PTN mode.	-
full-lsp-path	Displays the responses from all nodes along the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, only the responses from the PW nodes along the LSP are displayed.	-
uniform	Specifies the uniform mode. The IP TTL of the probe packet is reduced by one each time it passes through one hop in the MPLS domain.	-
draft6	Specifies the version of the **tracert vc** command. If this parameter is specified, the tracert operation is performed according to "draft-ietf-mpls-lsp-ping-06". **NOTE** Tracert VC based on **draft6** is applied only to VLL over LDP scenarios.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If a fault occurs on the PW, the **ping vc** command can be used to check the connectivity of the network, and the **tracert vc** command can be used to locate the fault and provide reference for fault diagnosis. If a PW is Up, the **ping vc** command can be used to locate the fault on the PW. For example, a forwarding entry is abnormally lost or incorrect. If a PW is down, the **tracert vc** command must be used to locate the faulty node on the PW.

Prerequisite

- The UDP module of each node works properly; otherwise, the tracert operation will fail.

 Copyright © Huawei Technologies Co., Ltd.

- The MPLS module has been enabled on each node and works properly.
- The ICMP module of each node works properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert vc** command is as follows:

1. The source sends an MPLS Echo Request packet with the TTL being 1. After the TTL times out, the first hop sends an MPLS Echo Reply packet to the source.
2. The source sends an MPLS Echo Request packet with the TTL being 2. After the TTL times out, the second hop sends an MPLS Echo Reply packet to the source.
3. The source sends an MPLS Echo Request packet with the TTL being 3. After the TTL times out, the third hop sends an MPLS Echo Reply packet to the source.
4. The preceding steps continue until the MPLS Echo Request packet reaches the destination.

When the device on each hop receives the MPLS Echo Request packet, it will respond with an MPLS Echo Reply packet, indicating that the tracert test ends. In the command output information of the source device, you can view the path that the packet passes through.

Configuration Impact

In control word mode, if a transit node receives an MPLS Echo Request packet whose TTL does not time out, it does not send the packet to the CPU. In this mode, the source obtains only a little PW information and cannot obtain information about the downstream devices of the transit node. This mode is recommended when the traffic volume is heavy.

In router alert mode, a transit node sends the received MPLS Echo Request packets to the CPU. In this mode, the source obtains a lot of PW information; therefore, device performance is affected when the traffic volume is heavy. This mode is recommended when the traffic volume is light.

Information specified by **remote** is encapsulated in MPLS Echo Request packets. The PW can be searched on the remote PE based on the specified information. By default, information contained in the MPLS Echo Request packets is about the PW on the local PE. This applies to single-segment PWs.

Precautions

- When the probe packet reaches the egress or the TTL reaches the upper threshold, the PW tracert is terminated.
- You can press **Ctrl + C** to terminate the execution of the **tracert vc** command.

When a PE is single-homed to an SPE and two multi-segment PWs are deployed for PW redundancy, end-to-end detection cannot be performed for the secondary PW if services are transmitted over the primary PW. If services are transmitted over the secondary PW, the primary PW can only be detected segment by segment.

 Copyright © Huawei Technologies Co., Ltd.

Example

Trace a multi-segment PW. The encapsulation type, local PW ID, and remote PW ID of the PW is ethernet, 100, and 200.

```
<Huawei> tracert vc ethernet 100 control-word remote 200 draft6 full-lsp-path
 TTL   Replier          Time    Type      Downstream
 0                        Ingress   10.1.1.2/[1025 ]
 1     10.1.1.2         230 ms  Transit   10.2.1.2/[3 ]
 2     10.2.1.2         230 ms  Transit   10.3.1.2/[3 ]
 3     10.3.1.2         100 ms  Transit   10.4.1.2/[3 ]
 4     10.4.1.2         150 ms  Egress
```

Table 12-149 Description of the **tracert vc** command output

Item	Description
TTL	TTL value in an Echo Request packet. It represents the number of hops along the path through which an Echo Request packet passes.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time when the packet is processed.
Type	Node type. The value can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

Related Topics

12.12.28 ping vc

12.13 VPLS Configuration Commands

NOTE

The AR100&AR120&AR150&AR160&AR200 series routers do not support VPLS.

12.13.1 description (VSI view)

Function

The **description** command configures the description of a Virtual Switch Instance (VSI).

The **undo description** command deletes the description of a VSI.

By default, no description of the VSI is configured.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a VSI.	The value is a string of 1 to 64 case-sensitive characters with spaces.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

The **description** command can be used to identify different VSIs or describe the functions of VSIs.

Example

Configure the description of the current VSI.

```
<Huawei> system-view
[Huawei] vsi v100
[Huawei-vsi-v100] description vsi for company1
```

Related Topics

12.13.48 vsi

12.13.2 display l2vpn ccc-interface vc-type

Function

The **display l2vpn ccc-interface vc-type** command displays information about the interface used by an L2VPN connection.

Format

display l2vpn ccc-interface vc-type { **all** | *vc-type* } [**down** | **up**]

Parameters

Parameter	Description	Value
all	Displays information about all interfaces of L2VPN connections.	-
vc-type	Specifies the type of the L2VPN connection.	The following types of the L2VPN connection are available: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● vpls-vc: VPLS connection
down	Displays information about interfaces of L2VPN connection in the Down state.	-
up	Displays information about interfaces of L2VPN connection in the Up state.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When locating L2VPN faults, you can use the **display l2vpn ccc-interface vc-type** command to view information about the AC interface of the current L2VPN connection, the total number of AC interfaces of various L2VPN connections, interface status, interface encapsulation type, and L2VPN connection types.

Example

Display information about all the interfaces of L2VPN.

```
<Huawei> display l2vpn ccc-interface vc-type all
Total ccc-interface of CCC : 2
up (2), down (0)
Interface                    Encap Type          State    VC Type
GigabitEthernet0/0/2            ethernet             up       ccc
GigabitEthernet0/0/1            ethernet             up       ccc
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-150 Description of the **display l2vpn ccc-interface vc-type** command output

Item	Description
Total ccc-interface of CCC : 2 up (2), down (0)	Total number of L2VPN connections is 2. Two connections is Up. No connection is Down.
Interface	Interface connected to the L2VPN connection on the router.
Encap Type	Encapsulation type of the L2VPN connection. The encapsulation type can be VLAN encapsulation or Ethernet encapsulation.
State	Current status of the L2VPN connection. The status can be Up or Down.
VC Type	Type of the L2VPN connection: ● ccc: Cross Circuit Connection ● ldp-vc: L2VPN connection in the Martini mode ● static-vc: L2VPN connection in the SVC mode ● vpls-vc: VPLS connection

Related Topics

12.11.4 display mpls l2vc
12.11.12 display mpls static-l2vc

12.13.3 display mpls l2vpn resource

Function

The **display mpls l2vpn resource** command displays MPLS L2VPN specifications and usage information.

Format

display mpls l2vpn resource

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check MPLS L2VPN specifications and usage information in routine maintenance, run the **display mpls l2vpn resource** command.

Example

Display MPLS L2VPN specifications and usage information.

```
<Huawei> display mpls l2vpn resource

 Public Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN AC Number                      512                0
 L2VPN VC Number                      512                1

 VPWS Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN Local CCC Number             256                 0
 L2VPN SVC Number                  256                 0
 L2VPN LDP VC Number                256                 1
 L2VPN Switch VC Number             256                 0

 VPLS Capacity Statistics
 Statistics Item                Supported Number     Used Number
 L2VPN VSI Number                     512                0
 L2VPN VSI VC Number                512                 0
 L2VPN VSI PWG Number               8000                 0
```

Table 12-151 Description of the **display mpls l2vpn resource** command output

Item	Description
Public Capacity Statistics	MPLS L2VPN capacity statistics
Statistics Item	Statistics item
Supported Number	Maximum number allowed
Used Number	Number already used
L2VPN AC Number	Number of L2VPN AC interfaces, including the maximum number allowed and number already used
L2VPN VC Number	Number of L2VPN VCs, including the maximum number allowed and number already used
VPWS Capacity Statistics	VPWS capacity statistics
L2VPN Local CCC Number	Number of VLLs in local CCC mode, including the maximum number allowed and number already used
L2VPN SVC Number	Number of VLLs in SVC mode, including the maximum number allowed and number already used

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
L2VPN LDP VC Number	Number of LDP VLLs, including the maximum number allowed and number already used
L2VPN Switch VC Number	Number of Switch VC, including the maximum number allowed and number already used
VPLS Capacity Statistics	VPLS capacity statistics
L2VPN VSI Number	Number of VSIs, including the maximum number allowed and number already used
L2VPN VSI VC Number	Number of VSI VCs, including the maximum number allowed and number already used
L2VPN VSI PWG Number	Number of protection groups for a VSI, including the maximum number allowed and number already used

12.13.4 display mpls label-stack vpls vsi

Function

The **display mpls label-stack vpls vsi** command displays information about label stacks in a VPLS scenario.

Format

display mpls label-stack vpls vsi *vsi-name* **peer** *peer-ip-address* **vc-id** *vc-id*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-ip-address*	Specifies the IP address of a peer.	The value is in dotted decimal notation.
vc-id *vc-id*	Specifies the VPLS PW ID.	The value is an integer ranging from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To view PW traffic forwarding information in a Martini VPLS scenario, run the **display mpls label-stack vpls vsi** command.

Example

Display stack label information in a Martini VPLS scenario with the peer IP address **1.1.1.9** and PW ID **11**.

```
<Huawei> display mpls label-stack vpls vsi a1 peer 1.1.1.9 vc-id 11
Label-stack  : 1
Level        : 1
Type         : VPLS
Label        : 1028
Level        : 2
Type         : LDP
Label        : --
OutInterface : Vlanif1024
```

Table 12-152 Description of the **display mpls label-stack vpls vsi** command output

Item	Description
Label-stack	Number of label stacks
Level	Number of label layers
Type	Tunnel type
Label	Outgoing label value
OutInterface	Outbound interface name

12.13.5 display traffic-statistics vsi

Function

The **display traffic-statistics vsi** command displays public network traffic statistics on all PWs of a specified VSI.

Format

display traffic-statistics vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After VPLS configurations are complete, you can run this command to view public network traffic statistics on all PWs of a specified VSI, so that you can learn the running status of all PWs of the specified VSI.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics enable** command in the VSI-LDP view to enable statistics collection on public network traffic of all PWs.

Precautions

Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

Display the statistics about the traffic on all VPLS PWs in a specified VSI.

```
<Huawei> display traffic-statistics vsi newvsi
vsi-name: newvsi
Peer-address: 10.22.33.20
Negotiation-vc-id: 2
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 12-153 Description of the **display traffic-statistics vsi** command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Negotiation-vc-id	VC ID of the PW.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

Related Topics

12.13.37 reset traffic-statistics vsi name

12.13.44 traffic-statistics enable (VSI-LDP view)

12.13.6 display traffic-statistics vsi peer

Function

The **display traffic-statistics vsi peer** command displays public network traffic statistics on a specified PW of a specified VSI.

Format

display traffic-statistics vsi *vsi-name peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-
negotiation-vc-id *vc-id*	Specifies the VC ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

After VPLS configurations are complete, you can run this command to view public network traffic statistics on a specified PW of a specified VSI, so that you can learn the running status of the PW of the specified VSI.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics peer enable** command in the VSI-LDP view to enable statistics collection on public network traffic of specified PWs.

Precautions

Within five minutes, if a PW goes Down, traffic before the PW is Down cannot be used to compute the traffic rate in the five minutes.

Example

Display the statistics about the traffic on the specified VPLS PW.

```
<Huawei> display traffic-statistics vsi newvsi peer 10.22.33.20
vsi-name: newvsi
Peer-address: 10.22.33.20
Statistics last cleared: never
Last 300 seconds input rate : 0 bytes/sec, 0 packets/sec
Last 300 seconds output rate: 0 bytes/sec, 0 packets/sec
Input: 0 bytes, 0 packets
Output: 0 bytes, 0 packets
```

Table 12-154 Description of the **display traffic-statistics vsi peer** command output

Item	Description
vsi-name	VSI name.
Peer-address	IP address of the remote peer.
Statistics last cleared	Last time when statistics are cleared.
Last 300 seconds input rate	Rate of incoming traffic in the last 300 seconds.
Last 300 seconds output rate	Rate of outgoing traffic in the last 300 seconds.
Input	Number of packets received by the PW from the AC.
Output	Number of packets sent from the PW to the AC.

Related Topics

12.13.38 reset traffic-statistics vsi name peer
12.13.45 traffic-statistics peer enable

12.13.7 display vpls connection

Function

The **display vpls connection** command displays the VPLS connection.

Format

display vpls connection [**ldp** | **vsi** *vsi-name*] [**down** | **up**] [**verbose**]

Parameters

Parameter	Description	Value
ldp	Displays information about LDP signaling connections.	-
vsi *vsi-name*	Displays information about connections of the specified VSI.	The value is an existing VSI.
down	Displays information about connections in Down state.	-
up	Displays information about connections in Up state.	-
verbose	Displays detailed information about connections.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After VPLS services are configured, you can run the **display vpls connection** command with different keywords or parameters to view information about specific VPLS connections.

Precautions

If no keyword or parameter is specified, information about all VPLS connections in Up state is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about the connections of all VSIs.

```
<Huawei> display vpls connection

1 total connections,
connections: 1 up, 0 down, 1 ldp, 0 bgp, 0 bgpad

VSI Name: a2                          Signaling: ldp
VsiID     EncapType            PeerAddr        InLabel   OutLabel  VCState
2         vlan                 3.3.3.9         18        18        up
```

Table 12-155 Description of the **display vpls connection** command output

Item	Description
VSI Name	Name of the VSI. To set the value, run the **vsi** command.
Signaling	Signaling mode: LDP. To set the value, run the **pwsignal** command.
VsiID	VSI ID. To set the value, run the **vsi-id** command.
EncapType	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC. To set the value, run the **encapsulation** command.
PeerAddr	IP addresses of the peer.
InLabel	VC label distributed locally.
OutLabel	Local outgoing label, namely, the VC label distributed by the peer.
VCState	Status of the VC.

Display the detailed information about all VSI connections.

```
<Huawei> display vpls connection verbose
VSI Name: a2                          Signaling: ldp
  **Remote Vsi ID   : 2
    VC State        : up
    Encapsulation   : vlan
    Group ID        : 0
    MTU             : 1500
    Peer Ip Address : 3.3.3.9
    PW Type         : label
    Local VC Label  : 1026
    Remote VC Label : 1025
    Tunnel Policy   : --
    Tunnel ID       : 0x10x0000000001004c4be1
```

Table 12-156 Description of the **display vpls connection verbose** command output

Item	Description
VSI Name	Name of the VSI. To set the value, run the **vsi** command.
Signaling	Signaling mode: LDP. To set the value, run the **pwsignal** command.
Remote Vsi ID	Remote VSI ID that is consistent with the local VSI ID.
VC State	Status of the VC, which can be Up or Down.
Encapsulation	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC. The encapsulation type is VLAN or Ethernet. To set the value, run the **encapsulation** command.
Group ID	Group identifier.
MTU	Maximum transmission unit. To set the value, run the **mtu** command.
Peer Ip Address	IP addresses of the peer.
PW Type	Type of the PW.
Local VC Label	Local VC label.
Remote VC Label	Remote VC label.
Tunnel Policy	Tunnel policy that is used by the L2VPN.
Tunnel ID	Tunnel ID.

Related Topics

12.11.3 display l2vpn ccc-interface vc-type

12.13.48 vsi

12.13.8 display vpls forwarding-info

Function

The **display vpls forwarding-info** command displays forwarding information of all VSIs.

Format

display vpls forwarding-info [**vsi** *vsi-name* [**peer** *peer-address* [**negotiation-vc-id** *vc-id* | **remote-site** *site-id*]] | **state** { **up** | **down** }] [**verbose**]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Displays forwarding information of a specified VSI.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the VC ID of the PW.	The value is an integer that ranges from 1 to 4294967295.
remote-site *site-id*	Specifies the remote site ID.	The value is an integer that ranges from 0 to 65534.
state	Displays the forwarding information about VSIs based on the PW status.	-
up	Displays the forwarding information about the VSIs whose PWs are in Up state.	-
down	Displays the forwarding information about the VSIs whose PWs are in Down state.	-
verbose	Displays detailed forwarding information of the VSI.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the VPLS is configured, you can run the **display vpls forwarding-info** command to view the forwarding information of all VSIs.

Precautions

- The **display vpls forwarding-info vsi** *vsi-name* command is used to display forwarding information of a specified VSI.

 Copyright © Huawei Technologies Co., Ltd.

- The **display vpls forwarding-info vsi** *vsi-name* **peer** *peer-address* [**negotiation-vc-id** *vc-id*] command is used to display forwarding information of a specified PW in the Martini VSI.

Example

Display brief forwarding information of all PWs in all VSIs.

```
<Huawei> display vpls forwarding-info
Total Number   : 2,       2  up,  0  down

Vsi-Name                    PeerIP         VcOrSiteId  PwState
a2                        3.3.3.9        2          UP
vplsad1                     3.3.3.9        0          UP
```

Display brief information about the VSI PWs in Up state.

```
<Huawei> display vpls forwarding-info state up
Total Number   : 2,       2  up,  0  down

Vsi-Name                    PeerIP         VcOrSiteId  PwState
a2                        3.3.3.9        2          UP
vplsad1                     3.3.3.9        0          UP
```

Table 12-157 Description of the **display vpls forwarding-info** command output

Item	Description
Total Number	The number of VSI.
Vsi-Name	Name of the VSI.
PeerIP	Peer IP address of the PW in the VSI.
VcOrSiteId	VSI ID for the Martini VSI.
PwState	PW status: ● UP ● DOWN

Display detailed forwarding information of all PWs in all VSIs.

```
<Huawei> display vpls forwarding-info verbose
Total Number   : 2,       2  up,  0  down

**Vsi-Name      : a2
  Vsi Index     : 0                       PwState      : UP
  Peer IP       : 3.3.3.9                 VcOrSiteId   : 2
  InVcLabel     : 1026                      OutVcLabel   : 1025
  BroadTunnelID : 0x1                         OutInterface : Vlanif1025
  MainPwToken   : 0x1                         SlavePwToken : 0x0
  NKey          : 0x9                     CKey         : 0xa

**Vsi-Name      : vplsad1
  Vsi Index     : 2                       PwState      : UP
  Peer IP       : 3.3.3.9                 VcOrSiteId   : 0
  InVcLabel     : 1036                      OutVcLabel   : 1031
  BroadTunnelID : 0x1                         OutInterface : Vlanif1025
  MainPwToken   : 0x1                         SlavePwToken : 0x0
  NKey          : 0x9                     CKey         : 0x1b
```

Display the detailed forwarding information about the VSI PWs in Up state.

```
<Huawei> display vpls forwarding-info state up verbose
Total Number   : 2,        2  up,  0  down

**Vsi-Name      : a2
  Vsi Index     : 0                        PwState      : UP
  Peer IP       : 3.3.3.9                  VcOrSiteId   : 2
  InVcLabel     : 1026                       OutVcLabel   : 1025
  BroadTunnelID : 0x1                          OutInterface : Vlanif1025
  MainPwToken   : 0x1                          SlavePwToken : 0x0
  NKey          : 0x9                      CKey         : 0xa

**Vsi-Name      : vplsad1
  Vsi Index     : 2                        PwState      : UP
  Peer IP       : 3.3.3.9                  VcOrSiteId   : 0
  InVcLabel     : 1036                       OutVcLabel   : 1031
  BroadTunnelID : 0x1                          OutInterface : Vlanif1025
  MainPwToken   : 0x1                          SlavePwToken : 0x0
  NKey          : 0x9                      CKey         : 0x1b
```

Table 12-158 Description of the **display vpls forwarding-info verbose** command output

Item	Description
Total Number	The number of VSI.
Vsi-Name	Name of the VSI.
Vsi Index	VSI index.
PwState	PW status: ● UP ● DOWN
Peer IP	Peer IP address of the PW in the VSI.
VcOrSiteId	VSI ID for the Martini VSI.
InVcLabel	Incoming label of the VC.
OutVcLabel	Outgoing label of the VC.
BroadTunnelID	ID of the tunnel used for broadcast.
OutInterface	Outbound interface.
MainPwToken	Token of the master PW.
SlavePwToken	Token of the slave PW.
NKey	Network key. Each NKey corresponds to one peer + tunnel policy.
CKey	User key. Each CKey corresponds to a PW.

 Copyright © Huawei Technologies Co., Ltd.

12.13.9 display vpls-ping statistics

Function

The **display vpls-ping statistics** command displays the statistics on the number of sent and received VPLS MAC Ping packets.

Format

display vpls-ping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls-ping statistics** command, you can view the statistics on the number of sent and received VPLS MAC Ping packets on the device.

Example

Display the statistics on the number of VPLS MAC Ping packets.

```
<Huawei> display vpls-ping statistics
Vpls-ping statistics:
Total sent: 104797 packet (s)
Total received: 104792 packet (s)
vpls-ping request sent: 13 packet (s), received: 104784 packet (s)
vpls-ping reply sent: 104784 packet (s), received: 8 packet (s)
```

Table 12-159 Description of the **display vpls-ping statistics** command output

Item	Description
Total sent	Total number of sent VPLS MAC Ping packets.
Total received	Total number of received VPLS MAC Ping packets.
vpls-ping request sent	Number of sent VPLS Ping Request packets.
vpls-ping reply sent	Number of sent VPLS Ping Reply packets.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.13.33 ping vpls mac vsi
12.13.39 reset vpls-ping statistics

12.13.10 display vpls-trace statistics

Function

The **display vpls-trace statistics** command displays the statistics on the number of sent and received VPLS MAC Trace packets.

Format

display vpls-trace statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Using the **display vpls-trace statistics** command, you can view the statistics on the number of sent and received VPLS MAC Trace packets on the device.

Example

Display the statistics on the number of VPLS MAC Trace packets.

```
<Huawei> display vpls-trace statistics
Vpls-trace statistics:
Total sent : 4 packet (s)
Total received : 4 packet (s)
vpls-trace request sent: 4 packet (s), received: 0 packet (s)
vpls-trace reply sent: 0 packet (s), received: 4 packet (s)
```

Table 12-160 Description of the **display vpls-trace statistics** command output

Item	Description
Total sent	Total number of sent VPLS MAC Trace packets.
Total received	Total number of received VPLS MAC Trace packets.
vpls-trace request sent	Number of sent VPLS MAC Trace Request packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
vpls-trace reply sent	Number of sent VPLS MAC Trace Reply packets.

Related Topics

12.13.42 trace vpls mac vsi
12.13.40 reset vpls-trace statistics

12.13.11 display vsi

Function

The **display vsi** command displays information about a VSI.

Format

display vsi [**name** *vsi-name*] [**verbose**]

display vsi [**name** *vsi-name*] **peer-info** [**statistics**]

display vsi name *vsi-name* **peer-info** *peer-ip* [**verbose**]

Parameters

Parameter	Description	Value
name *vsi-name*	Displays the name of a specified VSI.	The value is an existing VSI.
verbose	Displays detailed information about the VSI.	-
peer-info	Displays detailed information or statistics about the PW status of peers.	-
statistics	Displays statistics about the PW status of peers.	-
peer-ip	Displays detailed information about the PW status of the peer with a specified IP address.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When you run the **display vsi** command:

- The **display vsi** command displays information about VSIs. By default, information of all VSIs is displayed.
- The **display vsi peer-info** command displays detailed information about the PW status of peers of all VSIs.
- The **display vsi name** *vsi-name* **peer-info** command displays detailed information about the PW status of peers to a specified VSI.
- The **display vsi name** *vsi-name* **peer-info** *peer-ip* command displays detailed information about the PW status of a specific peer to a specified VSI.
- The **display vsi peer-info statistics** command displays statistics about the PW status of peers of all VSIs.
- The **display vsi name** *vsi-name* **peer-info statistics** command displays statistics about the PW status of peers to a specified VSI.

Example

Display information about the VSI named **a2**.

```
<Huawei> display vsi name a2
Vsi                     Mem    PW    Mac       Encap     Mtu   Vsi
Name                      Disc   Type  Learn     Type      Value State
-------------------------------------------------------------------------------
a2                      static ldp   unqualify vlan      1500  up
```

Table 12-161 Description of the **display vsi** command output

Item	Description
Vsi Name	Name of the VSI. To set the value, run the **vsi** command.
Mem Disc	Member discovery mode. Currently, only static member discovery is supported.
PW Type	PW type.
Mac Learn	Mode of learning the MAC address.
Encap Type	Encapsulation type. • vlan • ethernet If the PW encapsulation types on both ends are different, run the **encapsulation** { **ethernet** | **vlan** } command in the VSI view to change the encapsulation type on one end to be the same as that on the other end.
Mtu Value	Maximum transmission unit. To set the value, run the **mtu** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Vsi State	Status of the VSI: ● up: The VSI is in Up state. ● down: The VSI is in Down state. ● *down: The VSI is in Down state. The network administrator has run the **shutdown** command on this interface.

Display detailed information about all VSIs.

```
<Huawei> display vsi verbose

 ***VSI Name                : a2
    Administrator VSI       : no
    Isolate Spoken          : disable
    VSI Index               : 0
    PW Signaling            : ldp
    Member Discovery Style : static
    PW MAC Learn Style      : unqualify
    Encapsulation Type      : vlan
    MTU                     : 1500
    Diffserv Mode           : uniform
    Service Class           : --
    Color                   : --
    DomainId                : 255
    Domain Name             :
    Ignore AcState          : disable
    P2P VSI                 : disable
    Create Time             : 0 days, 0 hours, 3 minutes, 57 seconds
    VSI State               : down

    VSI ID                  : 2
    LDP MAC-WITHDRAW        : mac-withdraw Enable
   *Peer Router ID          : 3.3.3.9
    Negotiation-vc-id       : 2
    primary or secondary    : primary
    ignore-standby-state    : no
    VC Label                : 1025
    Peer Type               : dynamic
    Session                 : up
    Tunnel ID               : 0x7
    Broadcast Tunnel ID     : 0x7
    Broad BackupTunnel ID   : 0x0
    CKey                    : 4
    NKey                    : 3
    Stp Enable              : 0
    PwIndex                 : 0
    Control Word            : disable
    BFD for PW              : unavailable

    Interface Name          : Ethernet0/0/2
    State                   : up
    Access Port             : false
    Last Up Time            : 2017/07/13 11:27:13
    Total Up Time           : 2 days, 2 hours, 6 minutes, 36 seconds

  **PW Information:

   *Peer Ip Address         : 3.3.3.9
    PW State                : up
    Local VC Label          : 1025
    Remote VC Label         : 1025
```

```
Remote Control Word    : disable
PW Type                : label
Local  VCCV            : alert lsp-ping bfd
Remote VCCV            : alert lsp-ping bfd
Tunnel ID              : 0x7
Broadcast Tunnel ID    : 0x7
Broad BackupTunnel ID  : 0x0
Ckey                   : 0x4
Nkey                   : 0x3
Main PW Token          : 0x0
Slave PW Token         : 0x0
Tnl Type               : LSP
OutInterface           :
Backup OutInterface    :
Stp Enable             : 0
PW Last Up Time        : 2017/07/13 11:31:24
PW Total Up Time       : 2 days, 2 hours, 2 minutes, 25 seconds
```

Table 12-162 Description of the **display vpls vsi verbose** command output

Item	Description
VSI Name	Name of the VSI.
Administrator VSI	Whether the VSI is an administrator VSI: ● yes ● no
Isolate Spoken	Whether the forwarding isolation function is enabled: ● enable ● disable
VSI Index	Index of the VSI.
PW Signaling	Type of the PW signaling. To set the value, run the **pwsignal** command.
Member Discovery Style	Member discovery mode.
PW MAC Learn Style	Mode of MAC address learning of the PW.
Encapsulation Type	VPLS encapsulation type of the VSI, namely, the encapsulation type of the packets transmitted over the VC: ● vlan ● ethernet
MTU	Maximum transmission unit. If the MTU values on both ends are different, run the **mtu** *mtu-value* command in the VSI view to change the MTU value on one end to be the same as that on the other end.
Diffserv Mode	VSI QoS mode.
Service Class	QoS service class of a VSI.

Item	Description
Color	QoS packet color of a VSI.
DomainId	ID of a domain.
Domain Name	Domain name.
Ignore AcState	Whether the **vpls ignore-ac-state** command is used to prevent the status of a VSI from being affected by the status of the Attachment Circuit (AC).
P2P VSI	A P2P VSI identifier, which can be: ● enable: indicates that the VSI is a P2P VSI. ● disable: indicates that the VSI is not a P2P VSI.
Create Time	Time when the VSI is created.
VSI State	Status of the VSI: ● up ● down ● administratively down
VSI ID	VSI ID If the VSI IDs or negotiation IDs on both ends are different, run the **vsi-id** *vsi-id* or **peer (VSI-LDP view)** command in the VSI-LDP view to change the VSI ID or negotiation ID on one end to be the same as that on the other end.
LDP MAC-WITHDRAW	Whether the MAC withdraw function is enabled.
Peer Router ID	ID of the peer device.
Negotiation-vc-id	VC ID for negotiation.
primary or secondary	Whether the PW is a primary PW or a secondary PW.
ignore-standby-state	Whether the PW ignores the secondary state sent from the peer device. ● yes: Ignore the secondary state sent from the peer device. ● no: Do not ignore the secondary state sent from the peer device.
VC Label	Label value of the VC.
Peer Type	PW type of the peer.
Session	Status of the session between the local end and its peer. The status can be Up or Down.
Tunnel ID	Tunnel ID that is displayed only when the Martini VPLS is configured.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Broadcast Tunnel ID	Tunnel ID (for broadcast).
Broad BackupTunnel ID	ID of the selected backup broadcast tunnel.
CKey	Index of the public tunnel for VPN QoS.
NKey	Index of the public tunnel.
Stp Enable	Whether STP for PW is enabled: ● 0: disabled ● 1: enabled
PwIndex	PW index.
Control Word	Whether the control word is enabled for the local end on the PW: ● enable: The control word is enabled. ● disable: The control word is disabled.
BFD for PW	Whether BFD is configured: ● unavailable: BFD is not configured. ● available: BFD is configured. ● timeout: BFD session creation timed out.
Interface Name	Name of the interface bound to the VSI.
State	Status of the AC bound to the VSI. ● up ● down
Access Port	Whether the interface supports the access-port attribute: ● true: indicates that the interface supports the access-port attribute. ● false: indicates that the interface does not support the access-port attribute.
Last Up Time	Last time when the AC interface goes Up.
Total Up Time	Total time when the AC interface is Up.
PW Information	Information about the PW.
Peer Ip Address	IP addresses of the peer.
PW State	Status of the PW. ● up ● down
Local VC Label	VC label distributed locally.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote VC Label	VC label distributed by the peer.
Remote Control Word	Whether the control word is enabled for the remote end on the PW: ● enable: The control word is enabled. ● disable: The control word is disabled.
PW Type	Type of the PW.
Local VCCV	VCCV mode supported by the local end: ● **alert lsp-ping bfd** (default value): VCCV is implemented by sending LSP ping and BFD packets in label alert mode when the control word function is disabled. ● **cw alert lsp-ping bfd**: VCCV is implemented by sending LSP ping and BFD packets in control word, label alert mode when the control word function is enabled. ● **--**: VCCV is disabled.
Remote VCCV	VCCV mode supported by the remote end: ● **alert lsp-ping bfd** (default value): VCCV is implemented by sending LSP ping and BFD packets in label alert mode when the control word function is disabled. ● **cw alert lsp-ping bfd**: VCCV is implemented by sending LSP ping and BFD packets in control word, label alert mode when the control word function is enabled. ● **--**: VCCV is disabled. ● **none**: The remote PW does not exist.
Main PW Token	Token of the master PW.
Slave PW Token	Token of the slave PW.
Tnl Type	Type of a tunnel. ● LSP ● CR-LSP ● Other
OutInterface	Outbound interface.
Backup OutInterface	Outbound interface of the selected backup broadcast tunnel.
PW Last Up Time	Last time when the PW goes Up.
PW Total Up Time	Total time when the PW is Up.

 Copyright © Huawei Technologies Co., Ltd.

Display detailed information of PW status of peers to all VSIs.

```
<Huawei> display vsi peer-info

VSI Name: a2                                    Signaling: ldp
-----------------------------------------------------------------
Peer            Transport       Local      Remote      VC
Addr             VC ID/TAII      VC Label   VC Label    State
-----------------------------------------------------------------
3.3.3.9          2               1025       1025        up
```

Display detailed information of PW status of a specific peer to a specified VSI.

```
<Huawei> display vsi name a2 peer-info 3.3.3.9

VSI Name: a2                                    Signaling: ldp
-----------------------------------------------------------------
Peer            Transport       Local      Remote      VC
Addr             VC ID/TAII      VC Label   VC Label    State
-----------------------------------------------------------------
3.3.3.9          2               1025       1025        up
```

Table 12-163 Description of the **display vsi peer-info** command output

Item	Description
Vsi Name	Name of the VSI.
Signaling	Type of the PW signaling.
Peer Addr	IP addresses of the peer.
Transport VC ID/TAII	● VC ID for an LDP PW ● TAII for a BGP-AD PW
Local VC Label	VC label distributed locally.
Remote VC Label	VC label distributed by the peer.
VC State	Status of the PW. ● up ● down

Display statistics about PW status of peers to all VSIs.

```
<Huawei> display vsi peer-info statistics
Total Local Peers: 1          1 Up          0 Down
-------------------------------------------------------
Vsi Name                    Up Peers       Down Peers
-------------------------------------------------------
a2                          1              0
```

Display statistics about PW status of peers to a specified VSI.

```
<Huawei> display vsi name a2 peer-info statistics
Vsi Name                    Up Peers       Down Peers
-------------------------------------------------------
a2                          1              0
```

Table 12-164 Description of the **display vsi peer-info statistics** command output

Item	Description
Total Local Peers	Total number of remote peers to the local end, that is, total number of PWs.
Up	Total number of PWs in Up state.
Down	Total number of PWs in Down state.
Vsi Name	Name of the VSI.
Up Peers	Total number of PWs in Up state in a specified VSI.
Down Peers	Total number of PWs in Down state in a specified VSI.

Related Topics

12.13.14 display vsi remote
12.13.48 vsi

12.13.12 display vsi mac-withdraw loop-detect

Function

The **display vsi mac-withdraw loop-detect** command displays information about MAC withdraw loop detection.

Format

display vsi [**name** *vsi-name*] **mac-withdraw loop-detect**

Parameters

Parameter	Description	Value
name *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you enable MAC withdraw loop detection, run the **display vsi mac-withdraw loop-detect** command to view information about MAC withdraw loop

detection. If you specify **name** *vsi-name*, the command output shows information about MAC withdraw loop detection in a specified VSI. If you do not specify **name** *vsi-name*, the command output shows information about MAC withdraw loop detection in all VSIs.

Example

Display information about MAC withdraw loop detection in all VSIs.

```
<Huawei> display vsi mac-withdraw loop-detect
Total number of vsi detect loop is 2.
Support max hop 255.

Vsi name        : VSI1
Last loop type  : detect loop
Send peer       : 10.5.5.5
Receive peer    : 10.2.2.2
Last loop time  : 2012/10/26 11:35:59

Vsi name        : VSI2
Last loop type  : exceed max hop
Send peer       : 10.5.5.5
Receive peer    : 10.3.3.3
Last loop time  : 2012/10/26 11:35:59
```

Display information about MAC withdraw loop detection in VSI1.

```
<Huawei> display vsi name VSI1 mac-withdraw loop-detect
Vsi name        : VSI1
Last loop type  : detect loop
Send peer       : 10.5.5.5
Receive peer    : 10.2.2.2
Last loop time  : 2012/10/26 11:35:59
```

Table 12-165 Description of the **display vsi mac-withdraw loop-detect** command output

Item	Description
Total number of vsi detect loop	Number of MAC Withdraw message loops.
Support max hop 255	Indicates that the maximum number of hops supported by MAC Withdraw loop detection is 255.
Vsi name	Name of the VSI in which a MAC Withdraw message loop occurred.
Last loop type	Type of the MAC Withdraw message loop. The values are as follows: • **detect loop**: The PE detects that a MAC Withdraw message loop occurs. • **exceed max hop**: The number of hops for forwarding MAC Withdraw messages exceeds the maximum number of hops.
Send peer	Peer to which MAC Withdraw messages are sent.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Receive peer	Peer from which MAC Withdraw messages are received.
Last loop time	Time when the MAC Withdraw message loop occurs.

Related Topics

12.13.47 vpls mac-withdraw loop-detect enable

12.13.13 display vsi pw out-interface

Function

The **display vsi pw out-interface** command displays information about the outgoing interface of a VSI PW.

Format

display vsi pw out-interface [**vsi** *vsi-name*]

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display vsi pw out-interface** command to view information about the actual outgoing interface of the PW.

Precautions

This command applies to the Martini VPLS PW only.

Example

Display information about the outgoing interface of the VSI PW.

```
<Huawei> display vsi pw out-interface
Total: 1
-------------------------------------------------------------------------------
Vsi Name                    peer          vcid      interface
-------------------------------------------------------------------------------
a2                        3.3.3.9        2         GigabitEthernet2/0/0
```

Table 12-166 Description of the **display vsi pw out-interface** command output

Item	Description
Vsi Name	VSI name.
peer	VSI peer.
vcid	VC ID.
interface	Outgoing interface of a VSI PW.

Related Topics

12.13.11 display vsi

12.13.14 display vsi remote

Function

The **display vsi remote** command displays information about a remote VSI.

Format

display vsi remote ldp [**router-id** *ip-address*] [**pw-id** *pw-id*]

display vsi remote ldp verbose

Parameters

Parameter	Description	Value
ldp	Displays information about remote VSIs using LDP signaling.	-
route-id *ip-address*	Displays information about remote VSIs of specified peers.	*ip-address* specifies the IPv4 address of the peer.
pw-id *pw-id*	Displays information about remote VSIs of a specified PW.	*pw-id* specifies the number of a VC. It is a decimal integer that ranges from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Display details about the remote VSIs using LDP signaling.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about remote VSIs, configure one of the following parameters in the **display vsi remote ldp** command:

Example

Display information about the remote VSIs using LDP signaling.

```
<Huawei> display vsi remote ldp
Vsi        Peer          VC      Group   Encap      MTU    Vsi    State
ID         RouterID      Label   ID      Type       Value  Index  Code
2          10.3.3.9      1025    0       vlan       1500   0      FORWARD
```

Table 12-167 Description of the **display vsi remote ldp** command output

Item	Description
Vsi ID	ID of a remote VSI.
Peer RouterID	Remote peer address.
VC Label	Remote VC label.
Group ID	Remote group ID. The default value is 0.
Encap Type	Remote VC encapsulation type. ● vlan ● ethernet
MTU Value	MTU of a remote VC.
Vsi Index	Index of a remote VSI.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State Code	Status of a remote VC: ● FORWARD: The remote VC is in the forwarding state. ● STANDBY: The remote VC is in the standby state. ● AC FAULT: The remote AC interface is faulty. ● PSN FAULT: The remote VC is faulty. ● NO FORWARD: The remote VC cannot forward packets owing to other reasons. ● -: The negotiated communication mode is Martini.

Display detailed information about remote VSIs using LDP signaling.

```
<Huawei> display vsi remote ldp verbose
Total remote LDP VC : 1

VSI ID            : 2
VSI Index         : 0
VC Type           : vlan
VC Label          : 1025
Peer Address      : 10.3.3.9
Group ID          : 0
MTU               : 1500
Status Code       : FORWARD
Match Local VC    : MATCH
Control Word      : disable
```

Table 12-168 Description of the **display vsi remote ldp verbose** command output

Item	Description
Total remote LDP VC	Indicates the total number of remote LDP VC.
VSI ID	ID of a remote VSI.
VSI Index	Index of a remote VSI.
VC Type	Remote VC encapsulation type.
VC Label	Remote VC label.
Peer Address	Remote peer address.
Group ID	Remote group ID. The default value is 0.
MTU	MTU of a remote VC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status Code	Status of a remote VC: ● FORWARD: The remote VC is in the forwarding state. ● STANDBY: The remote VC is in the standby state. ● AC FAULT: The remote AC interface is faulty. ● PSN FAULT: The remote VC is faulty. ● NO FORWARD: The remote VC cannot forward packets owing to other reasons.
Match Local VC	Whether a VC matching the remote VC ID exists on the local end: ● MATCH: A VC matching the remote VC ID exists on the local end. ● NOT-MATCH: No VC matching the remote VC ID exists on the local end.
Control Word	Whether the control word is enabled: ● enable: The control word is enabled. ● disable: The control word is disabled.

Related Topics

12.13.11 display vsi

12.13.15 display vsi services

Function

The **display vsi services** command displays information about the AC interface associated with the VSI.

Format

display vsi services { **all** | *vsi-name* | **interface** *interface-type interface-number* | **vlan** *vlan-id* }

Parameters

Parameter	Description	Value
all	Displays the information about AC interfaces associated with all VSIs.	-
vsi-name	Displays the information about AC interfaces associated with the specified VSI.	The value is an existing VSI.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the AC interface associated with the VSI. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
vlan *vlan-id*	Displays information about the specified VLAN AC interface associated with the VSI.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vsi services** command displays status of the AC interface associated with the VSI, and can be used for fault diagnosis.

Example

Display information about the AC interfaces associated with all VSIs.

```
<Huawei> display vsi services all
Total: 1
Code: AS(Admin Status), PS(Physical Status)
--------------------------------------------------------------------------------
Interface                    Vsi Name                    AS    PS
--------------------------------------------------------------------------------
GigabitEthernet0/0/1              1                       up    up
--------------------------------------------------------------------------------
```

Table 12-169 Description of the **display vsi services** command output

Item	Description
Interface	Name of the interface.
Vsi Name	Name of the VSI that is bound to the interface.
AS	Status of the VSI that is bound to the interface: ● up: The VSI is in Up state. ● down: The VSI is in Down state. ● *down: The VSI is in Down state. The network administrator has run the **shutdown** command on this interface.

Item	Description
PS	Physical status of the interface: • up: The physical status of the interface is Up. • down: The physical status of the interface is Down.

Related Topics

12.13.11 display vsi

12.13.16 encapsulation (VSI view)

Function

The **encapsulation** command configures the encapsulation type of the interface in the VSI view.

The **undo encapsulation** command restores the default encapsulation type of the interface in the VSI view.

By default, the encapsulation type is VLAN.

Format

encapsulation { **ethernet** | **vlan** }

undo encapsulation ethernet

Parameters

Parameter	Description	Value
ethernet	Indicates that the encapsulation type is Ethernet.	-
vlan	Indicates the VLAN encapsulation format that meets the 802.1Q standard.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure the VPLS function, run the **encapsulation** command to configure the encapsulation type of the interface.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Example

Configure the encapsulation type of the current VSI as Ethernet.

```
<Huawei> system-view
[Huawei] vsi a2 static
[Huawei-vsi-a2] pwsignal ldp
[Huawei-vsi-a2-ldp] vsi-id 101
[Huawei-vsi-a2-ldp] quit
[Huawei-vsi-a2] encapsulation ethernet
```

Related Topics

12.13.48 vsi

12.13.17 ignore-ac-state

Function

The **ignore-ac-state** command enables a VSI to retain in Up state regardless of the Attachment Circuit (AC) state.

The **undo ignore-ac-state** command restores the default setting.

By default, the VSI state changes with the AC state.

Format

ignore-ac-state

undo ignore-ac-state

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

To verify whether a VSI can work normally on the new network before a VPLS network migration, run the **ignore-ac-state** command in the VSI view on the new device. This command enables the VSI to retain in Up state on the new device before the AC-side device is connected to the new device. When the AC interface is Down and the PW is Up, the VSI is Up. When the AC interface is Up and the PW is Down, the VSI is still Up.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable a VSI to retain in Up state regardless of the AC state.

```
<Huawei> system-view
[Huawei] vsi vsi1
[Huawei-vsi-vsi1] pwsignal ldp
[Huawei-vsi-vsi1-ldp] vsi-id 2
[Huawei-vsi-vsi1-ldp] quit
[Huawei-vsi-vsi1] ignore-ac-state
```

Related Topics

12.13.46 vpls ignore-ac-state

12.13.18 interface-parameter-type vccv (VSI-LDP-PW view)

Function

The **interface-parameter-type vccv** command restores the default setting.

The **undo interface-parameter-type vccv** command deletes the VCCV byte right after the interface parameter in the Mapping packet.

By default, a mapping packet carries the VCCV byte.

Format

interface-parameter-type vccv

undo interface-parameter-type vccv

Parameters

None

Views

VSI-LDP-PW view

Default Level

2: Configuration level

Usage Guidelines

If the router communicates with the devices of VRP V300R001 and all branching versions, and the LDP VPLS is configured, run the **undo interface-parameter-type vccv** command.

Example

When configuring the VPLS in LDP mode, delete the VCCV byte from the Mapping packet.

```
<Huawei1> system-view
[Huawei] vsi vsi1 static
```

```
[Huawei-vsi-vsi1] pwsignal ldp
[Huawei-vsi-vsi1-ldp] vsi-id 100
[Huawei-vsi-vsi1-ldp] peer 2.2.2.2
[Huawei-vsi-vsi1-ldp] peer 2.2.2.2 pw pw1
[Huawei-vsi-vsi1-ldp-pw-pw1] undo interface-parameter-type vccv
```

12.13.19 interface-status-change mac-withdraw enable

Function

The **interface-status-change mac-withdraw enable** command enables the PEs to send LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

The **undo interface-status-change mac-withdraw enable** command disables the PEs from sending LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

By default, a PE does not send LDP MAC Withdraw messages when the status of the AC interface bound to the VSI changes.

Format

interface-status-change mac-withdraw enable

undo interface-status-change mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On enterprise networks, you can configure this command on the PE to enable the PE to update the MAC address entry when the AC link is in Down state. In this way, the PE sends LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

Precautions

If the local end sends MAC-Withdraw messages, the remote VSI clears local MAC addresses and learns new MAC addresses.

After you run the **interface-status-change mac-withdraw enable** command, the PE sends LDP MAC-Withdraw messages to all peers if the status of the interface bound to the VSI changes:

- From Down to Up.
- From Up to Down.

The **interface-status-change mac-withdraw enable** takes effect only when the **mac-withdraw enable** is configured.

Example

Enable the PE to send LDP MAC Withdraw messages to all peers when the status of the AC interface bound to the VSI changes.

```
<Huawei> system-view
[Huawei] vsi v1 static
[Huawei-vsi-v1] pwsignal ldp
[Huawei-vsi-v1-ldp] interface-status-change mac-withdraw enable
```

Related Topics

12.13.24 mac-withdraw enable

12.13.20 l2 binding

Function

The **l2 binding** command binds an interface to a VSI.

The **undo l2 binding** command unbinds an interface to a VSI.

By default, the interface is not bound to any VSI.

Format

l2 binding vsi *vsi-name*

undo l2 binding vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi *vsi-name*	Specifies the name of the VSI to be bound with an interface.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

GE interface view, Ethernet interface view, GE sub-interface view, Ethernet sub-interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In the VPLS, run the **l2 binding** command on the PE to bind the interface that is connected to the CE to the corresponding VSI.

Prerequisites

A VSI has been created by using the **vsi** command, and a VSI instance ID has been configured by using the **vsi-id** *vsi-id* command.

Precautions

When an interface is bound to a VSI, the MTU can be configured in the interface view but does not take effect. The MTU configured in the VSI is used for PW MTU negotiation.

In the VPLS application, different CEs are transparently connected to each other in the same network segment of a LAN through VSIs, and the IP addresses of the CEs must be different.

NOTE

- If a sub-interface is bound to a VSI, you can delete the sub-interface only after unbinding it from the VSI.
- A sub-interface cannot be bound to the VSI instance that uses Ethernet encapsulation.
- Before running the **l2 binding** command on a sub-interface, add the main interface to a VLAN.
- The **l2 binding** command and the **ip address** command cannot be configured on the CE-side interface of the PE at the same time.

Example

Bind a Gigabitethernet sub-interface to a VSI.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp] vsi-id 100
[Huawei-vsi-company1-ldp] quit
[Huawei-vsi-company1] quit
[Huawei] interface gigabitethernet 0/0/1.1
[Huawei-GigabitEthernet0/0/1.1] dot1q termination vid 10
[Huawei-GigabitEthernet0/0/1.1] l2 binding vsi company1
```

Related Topics

12.13.11 display vsi

12.13.14 display vsi remote

12.13.21 mac-address blackhole vsi

Function

The **mac-address blackhole vsi** command configures a blackhole MAC address entry.

The **undo mac-address blackhole vsi** command deletes a blackhole MAC address entry.

 Copyright © Huawei Technologies Co., Ltd.

By default, no blackhole MAC address entry is configured.

Format

mac-address blackhole *mac-address* **vsi** *vsi-name*

undo mac-address blackhole [*mac-address*] **vsi** *vsi-name*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in a blackhole MAC address entry.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The MAC address cannot be FFFF-FFFF-FFFF or a multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI in a blackhole MAC address entry. The VSI must have been created.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To protect a device or network against MAC address attacks, configure MAC addresses of untrusted users as blackhole MAC addresses. The device then directly discards the received packets of which the source or destination MAC addresses match the blackhole MAC address entries.

Precautions

- If you configure a blackhole MAC address entry when the MAC address table is full, the device processes the MAC address entry as follows:
  - If a dynamic MAC address entry with the same MAC address and VLAN ID or VSI name exists in the MAC address table, the blackhole MAC address entry replaces the dynamic MAC address entry.
  - If no dynamic MAC address entry with the same MAC address and VLAN ID or VSI name exists in the MAC address table, the blackhole MAC address entry cannot be added to the MAC address table.

 Copyright © Huawei Technologies Co., Ltd.

- You can run the **mac-address blackhole** command multiple times to configure multiple blackhole MAC address entries.

Example

Add a blackhole MAC address entry to the MAC address table in the VSI named **vsi1**. In the blackhole MAC address entry, the MAC address is 0004-0004-0004.

```
<Huawei> system-view
[Huawei] mac-address blackhole 0004-0004-0004 vsi vsi1
```

Related Topics

6.1.3 display mac-address

6.1.5 display mac-address blackhole

12.13.22 mac-address static vsi

Function

The **mac-address static vsi** command configures a static MAC address entry. The outgoing interface in this entry is bound to a specified VSI.

The **undo mac-address static vsi** command deletes a static MAC address entry.

By default, the system does not configure any static MAC address entry.

Format

mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name* [**pe-vid** *pe-vid* [**ce-vid** { *ce-vid* | **any** }]]

undo mac-address static *mac-address interface-type interface-number* **vsi** *vsi-name* [**pe-vid** *pe-vid* [**ce-vid** { *ce-vid* | **any** }]]

undo mac-address static vsi *vsi-name* [*interface-type interface-number*]

Parameters

Parameter	Description	Value
mac-address	Specifies the unicast MAC address in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The MAC address cannot be a broadcast MAC address (FFFF-FFFF-FFFF) or a multicast MAC address (the eighth bit is 1).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	The interface can be an Ethernet interface, an Ethernet sub-interface, a GE interface, or a GE sub-interface. The interface in this command is a Layer 3 interface bound to a VSI.
vsi *vsi-name*	Specifies the name of a specified VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
pe-vid *pe-vid*	Specifies the outer VLAN tag of user packets.	The value is a decimal integer that ranges from 1 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN tag of user packets. When you specify **ce-vid** *ce-vid*, the corresponding interface must be a sub-interface. QinQ termination is configured on the sub-interface, and a VSI is bound to the sub-interface.	The value is a decimal integer that ranges from 1 to 4094.
any	Specifies that the inner VLAN tag can be of any value. If **any** is specified, the VLAN ID in the inner tag is ignored to reduce configurations and system resource consumption.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The VPLS provides reachability through MAC address learning. Each PE maintains a MAC address table.

The device learns source MAC addresses and then creates the MAC address table. However, the device cannot identify whether the packets are from authorized users or hackers, which brings security threats. If a hacker sets the source MAC address of attack packets to the MAC address of an authorized user and connects to another interface of the device, the device learns an incorrect MAC address entry. The packets that should be forwarded to the authorized user are forwarded to the hacker.

To improve interface security, the network administrator can manually create MAC address entries to bind MAC addresses of authorized users to specified interfaces using the **mac-address static vsi** command. This prevents hackers from intercepting data of authorized users.

Prerequisites

The network administrator is familiar with the MAC addresses of the devices on the network that need to use static MAC address entries for communications; otherwise, the configuration will interrupt authorized users' communications.

In the **mac-address static vsi** command, the interface must be a Layer 3 interface bound to a VSI.

Precautions

After being created, the static MAC address entries will not be aged. When receiving a frame of a specific MAC address, the device forwards the frame through the outgoing interface directly. After being configured and saved, the MAC address entries are still stored in the table even if the system is reset or the LPU is hot swapped.

Manually created MAC address entries take precedence over automatically created MAC address entries. Static MAC address entries and blackhole MAC address entries take precedence over dynamic MAC address entries.

If the user service changes, specify a new VSI bound to the interface. In this way, data of the user is not forwarded through the previously configured static MAC address entries. You need to configure new MAC address entries on the device or enable the device to learn dynamic MAC address entries to forward the data.

Example

Add a static MAC address entry to the VSI named **abc**. When the destination MAC address of a received frame is 0011-2233-4455, the frame is forwarded in the VSI named **abc**.

```
<Huawei> system-view
[Huawei] vsi abc static
[Huawei-vsi-abc] pwsignal ldp
[Huawei-vsi-abc-ldp] vsi-id 1
[Huawei-vsi-abc-ldp] quit
[Huawei-vsi-abc] quit
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] undo portswitch
[Huawei-GigabitEthernet0/0/1] l2 binding vsi abc
[Huawei-GigabitEthernet0/0/1] quit
[Huawei] mac-address static 0011-2233-4455 gigabitethernet 0/0/1 vsi abc
```

GE 1/0/0.1 is configured with a dot1q termination sub-interface and accesses the VPLS. Configure a static MAC address entry on this sub-interface. When a frame that belongs to VLAN 10 and has the destination MAC address

0011-2233-4455 is received, its tag is deleted and it is forwarded in the VSI named **abc**.

```
<Huawei> system-view
[Huawei] vsi abc static
[Huawei-vsi-abc] pwsignal ldp
[Huawei-vsi-abc-ldp] vsi-id 1
[Huawei-vsi-abc-ldp] quit
[Huawei-vsi-abc] quit
[Huawei] interface gigabitethernet 1/0/0.1
[Huawei-GigabitEthernet1/0/0.1] dot1q termination vid 10
[Huawei-GigabitEthernet1/0/0.1] l2 binding vsi abc
[Huawei-GigabitEthernet1/0/0.1] quit
[Huawei] mac-address static 0011-2233-4455 gigabitethernet 1/0/0.1 vsi abc pe-vid 10
```

Related Topics

6.1.3 display mac-address

12.13.23 mac-learning

Function

The **mac-learning enable** command enables MAC address learning for a VSI.

The **mac-learning disable** command disables MAC address learning of a VSI.

The **undo mac-learning disable** command enables MAC address learning for a VSI.

By default, MAC address learning is enabled for a VSI.

Format

mac-learning { **enable** | **disable** }

undo mac-learning disable

Parameters

Parameter	Description	Value
enable	Enables a VSI to learn MAC addresses.	-
disable	Disables a VSI to learn MAC addresses.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To disable MAC address learning in a VSI on a VPLS network, run the **mac-learning disable** command. The VPLS network then functions similarly to a VPWS network. For example, if there are only two PEs with each connecting to one CE, disabling MAC address learning in a VSI on a PE reduces the PE's pressure.

Configuration Impact

After the **mac-learning disable** command is run for a VSI, the VSI can no longer automatically learn MAC addresses, causing packets to be broadcast on the network. Therefore, exercise caution when running this command.

Example

Disable MAC address learning on the current VSI.

```
<Huawei> system-view
[Huawei] vsi company1
[Huawei-vsi-company1] mac-learning disable
```

Related Topics

12.13.24 mac-withdraw enable

12.13.24 mac-withdraw enable

Function

The **mac-withdraw enable** command enables a VSI to delete the local MAC address and inform all the remote peers of the deletion.

The **undo mac-withdraw enable** command disables a VSI to delete the local MAC address and inform all the remote peers of the deletion.

By default, the MAC-withdraw function is disabled.

Format

mac-withdraw enable

undo mac-withdraw enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In this case, the local end is unaware of an AC fault. The VSI remains Up and does not delete the corresponding MAC address entries in time. As a result, the remote end cannot receive data streams sent by the local end. After the **mac-withdraw enable** command is executed, the VSI deletes the local MAC address and informs all the remote peers of the deletion when an AC fault occurs and the VSI remains Up. This solves the preceding problem.

Precautions

The **mac-withdraw enable** command must be used together with the **interface-status-change mac-withdraw enable** command.

Example

Configure a VSI named v100 to delete the local MAC addresses and inform all the remote peers of the deletion when an AC fault occurs and the VSI remains Up.

```
<Huawei> system-view
[Huawei] vsi v100 static
[Huawei-vsi-v100] pwsignal ldp
[Huawei-vsi-v100-ldp] mac-withdraw enable
```

Related Topics

12.13.19 interface-status-change mac-withdraw enable

12.13.25 mpls l2vpn default vlan

Function

The **mpls l2vpn default vlan** sets the default VLAN of an interface to VLAN 0.

The **undo mpls l2vpn default vlan** command deletes the default VLAN of an interface.

By default, no default VLAN is configured for an interface.

Format

mpls l2vpn default vlan

undo mpls l2vpn default vlan

Parameters

None

Views

GE interface view, Ethernet interface view, GE sub-interface view, Ethernet sub-interface view

Default Level

2: Configuration level

Usage Guidelines

When the following conditions are met, you can run the **mpls l2vpn default vlan** command to specify the default VLAN on an interface:

- The VSI using VLAN encapsulation is configured on the two PEs.
- The remote PE accepts only the tagged packets.
- The local PE is connected to a computer by using the Ethernet interface or GE interface as the AC interface.

  In this scenario, the computer sends and receives only untagged packets. After the default VLAN is specified on the interface, the local PE performs the following operations:

  – The local PE adds VLAN tags to the packets sent by the computer. The VLAN tags are encapsulated in the user packets, and are transparently transmitted to the remote PE.

  – The local PE removes the VLAN tags from the packets sent by the remote PE, and forwards the packets to the computer.

Example

Configure the default VLAN of primary interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] mpls l2vpn default vlan
```

12.13.26 mpls l2vpn vsi-pw limit threshold-alarm

Function

The **mpls l2vpn vsi-pw limit threshold-alarm** command configures the upper and lower alarm thresholds for VPLS VCs.

The **undo mpls l2vpn vsi-pw limit threshold-alarm** command restores the default settings.

By default, the upper and lower alarm thresholds are 80% and 70% respectively.

Format

mpls l2vpn vsi-pw limit threshold-alarm upper-limit *upper-limit-value* **lower-limit** *lower-limit-value*

undo mpls l2vpn vsi-pw limit threshold-alarm [**upper-limit** *upper-limit-value* **lower-limit** *lower-limit-value*]

Parameters

Parameter	Description	Value
upper-limit *upper-limit-value*	Specifies the upper alarm threshold.	The value is an integer ranging from 1 to 100.

Parameter	Description	Value
lower-limit *lower-limit-value*	Specifies the lower alarm threshold.	The value is an integer ranging from 1 to 100. *lower-limit-value* must be smaller than *upper-limit-value*.

Views

MPLS-L2VPN view

Default Level

2: Configuration Level

Usage Guidelines

A device supports only a limited number of VPLS VCs. If a device has too many VPLS VCs, the device performance deteriorates. The **mpls l2vpn vsi-pw limit threshold-alarm** command allows you to flexibly adjust the upper and lower alarm thresholds for VPLS VCs to control VPLS VC usage.

- *upper-limit-value* specifies the upper alarm threshold for VPLS VCs. If the proportion of VPLS VCs created to the maximum VPLS VCs allowed reaches this threshold, a VPLS VC threshold-crossing alarm is reported.
- *lower-limit-value* specifies the lower alarm threshold for VPLS VCs. If the proportion of VPLS VCs created to the maximum VPLS VCs allowed falls below this threshold, a VPLS VC threshold-crossing clear alarm is reported.

Example

Configure the upper and lower alarm thresholds for VPLS VCs as 90% and 70% respectively.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] mpls l2vpn vsi-pw limit threshold-alarm upper-limit 90 lower-limit 70
```

Related Topics

12.11.9 display mpls l2vpn resource

12.13.27 mtu (VSI view)

Function

The **mtu** command sets the MTU of a VSI.

The **undo mtu** command restores the default value.

The default MTU of a VSI is 1500.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the MTU of a VSI.	The value is an integer that ranges from 328 to 65535.

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the MTUs of the same VSI on two PEs are different, the two PEs cannot exchange information or establish a connection. In this case, you can run the **mtu** command to set the MTU of a VSI so that VSIs created on different PEs for the same VPLS have the same MTU.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

When configuring MTUs, note that the MTUs of the VSIs created for the same VPLS on different PEs must be the same.

Example

Set the MTU of the VSI named **company1** as 1600.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp] vsi-id 100
[Huawei-vsi-company1-ldp] quit
[Huawei-vsi-company1] mtu 1600
```

12.13.28 oam-detecting enable

Function

The **oam-detecting enable** command enables the L2VPN OAM detection on the PSN tunnel.

The **undo oam-detecting enable** command disables the L2VPN OAM detection on the PSN tunnel.

By default, the L2VPN OAM detection on the PSN tunnel is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

oam-detecting enable

undo oam-detecting enable

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

After the L2VPN OAM detection on the PSN tunnel is enabled, you can:

Detect and locate the MPLS network faults swiftly and efficiently.

Report and process the faults.

Enable the VSI to sense the Down state of the LSP and then the VSI deletes the MAC address.

Example

Enable the L2VPN OAM detection on the PSN tunnel.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] oam-detecting enable
```

12.13.29 peer (VSI-LDP view)

Function

The **peer** command configures a peer for a VSI.

The **undo peer** command deletes the peer of a VSI.

By default, no peer is configured for a VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*]

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the peer. Generally, it is specified as the loopback address of the peer.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the VSI ID of another local VSI, or be the same as another VSI ID specified by another local **negotiate-vc-id**. In other words, *vc-id* must be an unused one. *vc-id* is a decimal integer that ranges from 1 to 4294967295.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you configure Martini VPLS, you need to run the **peer** command to configure a peer for the VSI.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

To configure a VLL to access a VPLS network, you can adopt one of the following configurations to create a PW:

- Configure the VSI ID on the VPLS network to be the same as the VC ID of the VLL peer.
- Configure the value of **negotiation-vc-id** *vc-id* to be the same as the VC ID of the VLL peer.

Precautions

After you run the **undo peer** command, all PW configurations created by the peer are deleted.

If the value of **negotiation-vc-id** *vc-id* is different from the value of *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer** command to delete the VSI peer. Otherwise, the system prompts that the VSI peer cannot be deleted.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the peer for the current VSI.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp] vsi-id 1
[Huawei-vsi-company1-ldp] peer 10.3.3.3 negotiation-vc-id 10
```

Delete the peer of a VSI.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp] vsi-id 1
[Huawei-vsi-company1-ldp] peer 10.3.3.3 negotiation-vc-id 10
[Huawei-vsi-company1-ldp] undo peer 10.3.3.3 negotiation-vc-id 10
```

Related Topics

12.13.49 vsi-id

12.13.30 peer pw

Function

The **peer pw** creates a PW and displays the PW view.

The **undo peer pw** deletes the created PW.

By default, no PW is created.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*] **pw**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the IPv4 address of the peer. Generally, it is specified as the loopback address of the peer.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the VSI ID of another local VSI, or be the same as another VSI ID specified by another local **negotiate-vc-id**. In other words, *vc-id* must be an unused one. *vc-id* is a decimal integer that ranges from 1 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pw *pw-name*	Specifies the name of a PW. The PW name is used to distinguish the PW from other PWs, and must be unique in the same VSI. Nevertheless, the PW name can be used in other VSIs.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Martini VPLS, you need to run the **peer pw** command to configure a PW after specifying a peer.

Prerequisites

The IP address of the peer has been specified using the **peer** *peer-address* command.

Precautions

If the value of **negotiation-vc-id** *vc-id* is different from the value of *vsi-id* configured using the **vsi-id** command, you must configure **negotiation-vc-id** *vc-id* when running the **undo peer pw** command to delete the PW. Otherwise, the PW cannot be deleted.

Example

Create the PW view.

```
<Huawei> system-view
[Huawei] vsi aa static
[Huawei-vsi-aa] pwsignal ldp
[Huawei-vsi-aa-ldp] vsi-id 1
[Huawei-vsi-aa-ldp] peer 10.1.1.1
[Huawei-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[Huawei-vsi-aa-ldp-pw-pw1]
```

Delete the PW.

```
<Huawei> system-view
[Huawei] vsi aa static
[Huawei-vsi-aa] pwsignal ldp
[Huawei-vsi-aa-ldp] vsi-id 1
[Huawei-vsi-aa-ldp] peer 10.1.1.1
[Huawei-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[Huawei-vsi-aa-ldp-pw-pw1] quit
[Huawei-vsi-aa-ldp] undo peer 10.1.1.1 pw
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

12.13.29 peer (VSI-LDP view)

12.13.31 peer static-npe

Function

The **peer static-npe** command configures the static NPE peer of the VSI in the Hierarchical Virtual Private LAN Service (HVPLS).

The **undo peer static-npe** command deletes the static NPE peer of the VSI in the HVPLS.

By default, the HVPLS has no static NPE peer of the VSI.

Format

peer *peer-address* [**negotiation-vc-id** *vc-id*] **static-npe trans** *transmit-label* **recv** *receive-label*

undo peer *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
peer-address	Specifies the IPv4 address of the static NPE peer. It is generally specified as the loopback address of the peer.	The value is in dotted decimal notation.
negotiation-vc-id *vc-id*	Specifies the ID of a VC, which uniquely identifies the VC. Generally, this parameter is specified when the two ends with different VSI IDs need to interconnect.	*vc-id* cannot be the same as the VSI ID of another local VSI, or be the same as another VSI ID specified by another local **negotiate-vc-id**. In other words, *vc-id* must be an unused one. *vc-id* is a decimal integer that ranges from 1 to 4294967295.
trans *transmit-label*	Indicates the outer label that is manually configured and sent from the local device to its peer. It is the outgoing label of the static Layer 2 VC.	The value is an integer ranging from 0 to 1048575.
recv *receive-label*	Indicates the outer label that is manually configured and sent from the peer to the local device. It is the incoming label of the static Layer 2 VC.	The value is an integer that ranges from 16 to 1023.

 Copyright © Huawei Technologies Co., Ltd.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On the VPLS network, you can run the **peer static-upe** command on the local device to configure a static NPE peer.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

If you specify **negotiation-vc-id** *vc-id* when you configure the peer of the VSI, and the specified *vc-id* and that in the configured **vsi-id** command are inconsistent, to delete the peer of the VSI, you must use the **undo peer** command with **negotiation-vc-id** *vc-id*. Otherwise, the peer cannot be deleted.

Example

Configure the static NPE peer of the current VSI. Configure the received and sent outer labels are 100.

```
<Huawei> system-view
[Huawei] vsi company1
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp] vsi-id 101
[Huawei-vsi-company1-ldp] peer 3.3.3.3 static-npe trans 100 recv 100
```

Related Topics

12.13.29 peer (VSI-LDP view)

12.13.30 peer pw

12.13.32 ping vpls

Function

The **ping vpls** command detects the status of the PW and reachability of the peer.

Format

ping vpls [**-c** *echo-number* | **-m** *time-value* | **-s** *data-bytes* | **-t** *timeout-value* | **-r** *reply-mode* | **-exp** *exp-value* | **-v**] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
-c *echo-number*	Specifies the number of sent Echo Request packets.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the time to wait before sending the next packet.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000 ms.
-s *data-bytes*	Specifies the number of bytes of an Echo Request packet to be sent.	The value is an integer that ranges from 65 to 8100, in bytes. The default value is 100 bytes.
-t *timeout-value*	Specifies the timeout period of sending Echo Request packets.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-r *reply-mode*	Specifies the mode in which the peer sends MPLS Echo Reply packets. The value is a decimal integer. The values are as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 UDP datagram carrying a router alert label. ● 4: indicates a reply through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-exp *exp-value*	Specifies the EXP value of an Echo Request packet to be sent.	The value is an integer that ranges from 0 to 7.
-v	Displays detailed information.	-
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
peer *peer-address*	Specifies the IP address of the peer PE.	-
negotiate-vc-id *vc-id*	Specifies the ID of the local PW.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

After VPLS configurations are complete, you can run the **ping vpls** command to check the PW status and reachability of the peer.

Precautions

The timeout period specified by **-t** is less than the waiting time specified by **-m**.

Note the following points when configuring VPLS:

- If **negotiate-vc-id** is not specified in the **peer** command, *vc-id* is unique and equal to *vsi-id*. To perform the ping operation, you do not need to specify *vc-id* because the VC is unique when **vsi** *vsi-name* and **peer** *peer-address* are specified. In the same case, however, if **negotiate-vc-id** is specified and it is not equal to the actual *vc-id* (that is, *vsi-id*), an error message is displayed.
- If **negotiate-vc-id** (multiple VC IDs can be specified) in the **peer** command, you need to specify **negotiate-vc-id** in addition to **vsi** *vsi-name* and **peer** *peer-address* when performing the ping. If **negotiate-vc-id** is not found or specified, an error message is displayed.

Example

Run the **ping vpls** command on the PE to check the connectivity of a PW in the Martini VPLS.

```
<Huawei> ping vpls vsi a2 peer 10.2.2.2
  Reply from 10.2.2.2: bytes=100 Sequence=1 time=3 ms
  Reply from 10.2.2.2: bytes=100 Sequence=2 time=6 ms
  Reply from 10.2.2.2: bytes=100 Sequence=3 time=6 ms
  Reply from 10.2.2.2: bytes=100 Sequence=4 time=6 ms
  Reply from 10.2.2.2: bytes=100 Sequence=5 time=6 ms

 --- FEC: FEC 128 PSEUDOWIRE (NEW). Type = vlan, ID = 10 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 3/4/6 ms
```

Table 12-170 Description of the **ping vpls** command output

Item	Description
Reply from x.x.x.x	Response from the destination host to each Echo Request packet: ● bytes: indicates the length of the response packet. ● sequence: indicates the sequence number of the response packet. ● time: indicates the response time, in ms. If no response packet is received after the timeout period, the message "Request time out" is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FEC: FEC 128 PSEUDOWIRE	Check on FEC 128, namely, check on a Martini VPLS PW.
Type = vlan	VLAN encapsulation on packets.
ID = 10	The VSI ID being 10.

Related Topics

12.13.48 vsi
12.13.43 tracert vpls
12.13.33 ping vpls mac vsi

12.13.33 ping vpls mac vsi

Function

The **ping vpls mac vsi** command checks the connectivity of Layer 2 forwarding links on the VPLS network.

Format

ping vpls mac *mac-address* **vsi** *vsi-name* [**vlan** *vlan-id* | **-c** *count* | **-m** *time-value* | **-s** *packsize* | **-t** *timeout* | **-exp** *exp* | **-r** *replymode* | **-h** *ttl*] *

ping vpls mac *mac-address* **vsi** *vsi-name* **rapid** [**vlan** *vlan-id* | **-c** *count_rapid* | **-s** *packsize* | **-t** *timeout* | **-exp** *exp* | **-r** *replymode* | **-h** *ttl*] *

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the unicast destination MAC address of the VPLS MAC ping, expressed in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The value cannot be a broadcast or multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
vlan *vlan-id*	Specifies the ID of a VLAN	*vlan-id* specifies the VLAN ID, which is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-c *count*	Specifies the number of VPLS MAC Ping Request packets to be sent.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-m *time-value*	Specifies the time to wait before sending the next VPLS MAC Ping Request packet.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000 ms.
-s *packsize*	Specifies the size of the VPLS MAC Ping Request packet.	The value is an integer that ranges from 142 to 1442, in bytes. The default value is 142 bytes.
-t *timeout*	Specifies the timeout period for waiting for a Reply packet in response to a VPLS MAC Ping Request packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-exp *exp*	Specifies the priority.	The value is an integer that ranges from 0 to 7. The default value is 0.
-r *replymode*	Specifies the reply mode, that is, the Reply packet is sent from the control layer or the data layer. ● 1: indicates that the peer end does not respond to MPLS MAC Trace Request packets. ● 2: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets. ● 3: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets containing the Router Alert TLV option. ● 4: indicates that the peer end responds to MPLS MAC Trace Request packets through the control channel of the application program grade. ● 5: indicates that the peer end responds to MPLS MAC Trace Request packets with VPLS IPv4 UDP packets.	Enumerated type. At present, only mode 1, 2, and 5 are supported. When mode 2 is adopted, reply packets are sent from the control layer; when mode 5 is adopted, reply packets are sent from the data layer. The default value is 5.
-h *ttl*	Specifies the TTL value of an Echo Request packet to be sent.	The value is an integer that ranges from 1 to 255. The default value is 30.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rapid	Indicates that VPLS MAC ping packets are sent in **rapid** mode. This parameter can be used if each response message is not concerned and multiple ping operations need to be performed within a shot period of time. This configuration allows all packets to be sent at the same time, and only summary statistics are displayed.	-
-c *count_rapid*	Specifies the number of VPLS MAC Ping Request packets to be sent.	The value is an integer that ranges from 1 to 1000. The default value is 5.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Using the **ping vpls mac vsi** command, you can check the connectivity of Layer 2 forwarding links on the VPLS network.

Example

On the VPLS network, check whether the device with the MAC address of 00e0-5952-6f01 is reachable.

```
<Huawei> ping vpls mac 00e0-5952-6f01 vsi v123
Ping mac 00e0-5952-6f01 vsi v123 : 100 data bytes , press CTRL_C to break
    Reply from 10.1.1.1 : bytes=100 sequence=1 time = 1ms
    Reply from 10.1.1.1 : bytes=100 sequence=2 time = 1ms
    Reply from 10.1.1.1 : bytes=100 sequence=3 time = 2ms
    Reply from 10.1.1.1 : bytes=100 sequence=4 time = 3ms
    Reply from 10.1.1.1 : bytes=100 sequence=5 time = 2ms
    The IP address of the PE is 5.5.5.9 and the interface on the PE is GigabitEthernet0/0/1.

  --- vsi : v123 00e0-5952-6f01 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/2/3 ms
```

Related Topics

12.13.48 vsi

12.13.32 ping vpls

 Copyright © Huawei Technologies Co., Ltd.

12.13.34 pw

Function

The **pw** command displays the PW view.

The **undo pw** command deletes the PW view.

By default, the PW view is not displayed.

Format

pw *pw-name*

undo pw *pw-name*

Parameters

Parameter	Description	Value
pw-name	Specifies the name of a PW.	The value is a string of 1 to 15 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a PW is created, you can run the **pw** *pw-name* command to enter the PW view.

Prerequisites

A PW has been created using the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] **pw** *pw-name* command.

Precautions

The PW name must be unique in a VSI, and the PW name can be the same in different VSIs.

Example

Enter the PW view.

```
<Huawei> system-view
[Huawei] vsi aa static
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-vsi-aa] pwsignal ldp
[Huawei-vsi-aa-ldp] vsi-id 1
[Huawei-vsi-aa-ldp] peer 10.1.1.1
[Huawei-vsi-aa-ldp] peer 10.1.1.1 pw pw1
[Huawei-vsi-aa-ldp-pw-pw1] quit
[Huawei-vsi-aa-ldp] pw pw1
```

Related Topics

12.13.30 peer pw

12.13.35 pwsignal

Function

The **pwsignal** command configures the signaling mode for a VSI.

By default, no signaling mode is configured for a VSI.

Format

pwsignal ldp

Parameters

Parameter	Description	Value
ldp	Uses the LDP signaling mode.	-

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring the Martini VPLS, you need to run the **pwsignal** command to configure a signaling mode for a VSI or displays the VSI-LDP view.

Precautions

If the member discovery mode of the VSI is static, the signaling mode must be LDP.

After the signaling mode is configured successfully for the VSI, it cannot be modified. If you want to change the signaling mode, you must delete the VSI and re-create VSI.

Example

Configure the signaling mode of the VSI as LDP.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp]
```

Related Topics

12.13.48 vsi

12.13.36 reset traffic-statistics vsi all

Function

The **reset traffic-statistics vsi all** command clears the statistics about all VPLS PW traffic.

Format

reset traffic-statistics vsi all

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When the **reset traffic-statistics vsi all** command is run successfully, confirm whether to proceed with the operation. If yes, enter **Y**. If no, enter **N**.

Example

Reset the statistics about all VPLS PW traffic in the user view.

```
<Huawei> reset traffic-statistics vsi all
Warning: Traffic-statistics information will be cleared! Continue? [Y/N]Y
```

Related Topics

12.13.5 display traffic-statistics vsi

12.13.6 display traffic-statistics vsi peer

12.13.37 reset traffic-statistics vsi name

Function

The **reset traffic-statistics vsi name** command clears the statistics about the public traffic on all VPLS PWs in the specified VSI.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset traffic-statistics vsi name *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the VPLS configuration is complete, you can run the **display traffic-statistics vsi** command to view statistics about all PW traffic in the VSI. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name** command to clear the previous statistics.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics enable** command in the VSI-LDP view to enable statistics collection on public network traffic of all PWs.

Precautions

After you run this command, statistics about all VPLS PW traffic in the VSI are cleared.

Example

Clear the statistics about all VPLS PW traffic in the specified VSI in the user view.

```
<Huawei> reset traffic-statistics vsi name newvsi
```

Related Topics

12.13.5 display traffic-statistics vsi

12.13.44 traffic-statistics enable (VSI-LDP view)

 Copyright © Huawei Technologies Co., Ltd.

12.13.38 reset traffic-statistics vsi name peer

Function

The **reset traffic-statistics vsi name peer** command clears public network traffic statistics on a specified PW of a specified VSI.

Format

reset traffic-statistics vsi name *vsi-name* **peer** *peer-address* [**negotiation-vc-id** *vc-id*]

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of the VSI in which traffic statistics are cleared.	The value is an existing VSI.
peer *peer-address*	Specifies the peer IP address of the PW.	-
negotiation-vc-id *vc-id*	Specifies the VC ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the VPLS configuration is complete, you can run the **display traffic-statistics vsi peer** command to view statistics about the traffic of the PW. To view the statistics about the traffic in a specified period, you can run the **reset traffic-statistics vsi name peer** command to clear the previous statistics.

Prerequisites

The following operations have been performed before this command is used:

Run the **traffic-statistics peer enable** command in the VSI-LDP view to enable statistics collection on public network traffic of specified PWs.

Precautions

After you run this command, statistics about the traffic on the corresponding VPLS PW are cleared.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear the statistics about the traffic on the VPLS PW in the user view.

```
<Huawei> reset traffic-statistics vsi name newvsi peer 10.1.1.1
```

Related Topics

12.13.6 display traffic-statistics vsi peer

12.13.45 traffic-statistics peer enable

12.13.39 reset vpls-ping statistics

Function

The **reset vpls-ping statistics** command clears the statistics about the number of VPLS MAC Ping packets.

Format

reset vpls-ping statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset vpls-ping statistics** command clears the statistics about the number of sent and received VPLS MAC Ping packets.

Example

Clear the statistics about the number of VPLS MAC Ping packets.

```
<Huawei> reset vpls-ping statistics
```

Related Topics

12.13.9 display vpls-ping statistics

12.13.33 ping vpls mac vsi

 Copyright © Huawei Technologies Co., Ltd.

12.13.40 reset vpls-trace statistics

Function

The **reset vpls-trace statistics** command clears the statistics about the number of VPLS MAC Trace packets.

Format

reset vpls-trace statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset vpls-trace statistics** command clears the statistics about the number of sent and received VPLS MAC Trace packets.

Example

Clear the statistics about the number of VPLS MAC Trace packets.

```
<Huawei> reset vpls-trace statistics
```

Related Topics

12.13.10 display vpls-trace statistics

12.13.42 trace vpls mac vsi

12.13.41 shutdown (VSI view)

Function

The **shutdown** command disables a VSI.

The **undo shutdown** command enables a VSI.

By default, a VSI is enabled.

Format

shutdown

undo shutdown

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

VSI view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For service management such as service debugging or service halting, you can disable a VSI temporarily, and add, cancel, or adjust VSI functions.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command.

Precautions

The **shutdown** command mainly affects PW connections of a VSI. After the command is run, the AC is Down and the Layer 2 forwarding table is deleted.

Example

Disable the current VSI.

```
<Huawei> system-view
[Huawei] vsi company1
[Huawei-vsi-company1] shutdown
```

Enable the current VSI.

```
<Huawei> system-view
[Huawei] vsi company1
[Huawei-vsi-company1] undo shutdown
```

Related Topics

12.13.48 vsi

12.13.35 pwsignal

12.13.49 vsi-id

12.13.42 trace vpls mac vsi

Function

The **trace vpls mac vsi** command checks PE and P devices on the VPLS network which packets pass through from the source to the destination. This command is used to check the connectivity of Layer 2 forwarding links and locate faults on the network.

 Copyright © Huawei Technologies Co., Ltd.

Format

trace vpls mac *mac-address* **vsi** *vsi-name* [**vlan** *vlan-id*] [**-t** *timeout* | **-f** *first-ttl* | **-m** *max-ttl* | **-exp** *exp* | **-r** *replymode*] *

Parameters

Parameter	Description	Value
mac *mac-address*	Specifies the unicast destination MAC address of the VPLS MAC trace, expressed in the format of H-H-H.	An H is a hexadecimal number of 1 to 4 bits, such as 00e0 and fc01. If you enter less than four digits, 0s are padded before the input digits. For example, if e0 is entered, 00e0 is displayed. The value cannot be a broadcast or multicast MAC address.
vsi *vsi-name*	Specifies the name of a VSI.	The value is an existing VSI.
vlan *vlan-id*	Specifies the ID of a VLAN	*vlan-id* specifies the VLAN ID, which is an integer that ranges from 1 to 4094.
-t *timeout*	Specifies the timeout period for waiting for a Reply packet in response to a VPLS MAC Trace Request packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000 ms.
-f *first-ttl*	Specifies the initial TTL.	The value is an integer that ranges from 1 to *max-ttl.* The default value is 1.
-m *max-ttl*	Specifies the maximum TTL.	The value is an integer that ranges from *first-ttl* to 255. The default value is 30.
-exp *exp*	Specifies the priority.	The value is an integer that ranges from 0 to 7. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-r *replymode*	Specifies the reply mode, that is, the Reply packet is sent from the control layer or the data layer. ● 1: indicates that the peer end does not respond to MPLS MAC Trace Request packets. ● 2: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets. ● 3: indicates that the peer end responds to MPLS MAC Trace Request packets with IPv4 or IPv6 UDP packets containing the Router Alert TLV option. ● 4: indicates that the peer end responds to MPLS MAC Trace Request packets through the control channel of the application program grade. ● 5: indicates that the peer end responds to MPLS MAC Trace Request packets with VPLS IPv4 UDP packets.	Enumerated type. At present, only mode 1, 2, and 5 are supported. When mode 2 is adopted, reply packets are sent from the control layer; when mode 5 is adopted, reply packets are sent from the data layer. The default value is 5.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Using the **trace vpls mac vsi** command, you can check the connectivity of Layer 2 forwarding links on the VPLS network, analyze roles of devices, and locate faults on the network.

Prerequisites

Before running this command, ensure that a VSI is configured and the VSI is in the Up state.

Example

On the VPLS network, trace the device with the MAC address of 781d-ba56-355e.

```
<Huawei> trace vpls mac 781d-ba56-355e vsi a2
 Traceroute to mac 781d-ba56-355e vsi a2, 30 hops max, press CTRL_C to break
 TTL  Num     Replier          Time     Type     Downstream              Hit
            LSR-ID          Out Interface
 ---------------------------------------------------------------------------
 0    1                                Ingress  10.1.1.2/[3]           N
            1.1.1.9          GigabitEthernet2/0/0
 1    1       192.168.1.1        8 ms     Egress                          Y
            3.3.3.9
Info: Succeed in tracing the destination address 781d-ba56-355e.
```

Table 12-171 Description of the **trace vpls mac** command output

Item	Description
TTL	Time to live.
Num	Sequence number of the packet sent at each hop.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time the packet is processed, that is, period from the time the Request packet is sent from the source node to the time a Reply packet is received by the source node.
Type	Type of the device that sends the Reply packet, which can be: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	Address and label of the next hop. For example, 192.168.1.1/[3] indicates that the IP address of the next hop is 192.168.1.1 and the label allocated to the next hop is 3.
Hit	Whether the Request packet reaches the destination. ● Y: The Request packet reaches the destination. ● N: The Request packet does not reach the destination.
LSR-ID	ID of the LSR.
Out Interface	Outbound interface through which packets are forwarded.

Related Topics

12.13.33 ping vpls mac vsi

12.13.43 tracert vpls

Function

The **tracert vpls** command detects the status of a PW or locates an abnormal node on a PW in Down state.

Format

tracert vpls [**-exp** *exp-value* | **-f** *first-ttl* | **-m** *max-ttl* | **-r** *reply-mode* | **-t** *timeout-value*] * **vsi** *vsi-name* **peer** *peer-address* [**negotiate-vc-id** *vc-id*] [**full-lsp-path**]

Parameters

Parameter	Description	Value
-exp *exp-value*	Specifies the value of the EXP field in the outer label of an MPLS Echo Request packet.	The value is an integer that ranges from 0 to 7.
-f *first-ttl*	Specifies an initial TTL.	The value is an integer that ranges from 1 to 255 and must be smaller than the value of *max-ttl*. The default value is 1.
-m *max-ttl*	Specifies a maximum TTL.	The value is an integer that ranges from 1 to 255 and must be greater than the value of *first-ttl*. The default value is 30.
-r *reply-mode*	Specifies the mode for the peer end to return MPLS Echo Reply packets. The values are as follows: ● 1: indicates no reply. ● 2: indicates a reply with an IPv4 or IPv6 UDP datagram. ● 3: indicates a reply with an IPv4 or IPv6 UDP datagram carrying a router alert label. ● 4: indicates a reply through the control channel of the application plane.	The value is an integer that ranges from 1 to 4. The default value is 2.
-t *timeout-value*	Specifies the timeout period for waiting for an MPLS Echo Reply packet.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5.
vsi *vsi-name*	Specifies the VPN name.	The value is an existing VSI.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
peer *peer-address*	Specifies the IP address of the peer PE.	-
negotiate-vc-id *vc-id*	Specifies the ID of the local PW.	The value is an integer that ranges from 1 to 4294967295.
full-lsp-path	Displays the responses from all nodes on the LSP that the MPLS Echo Request packets pass through. If this parameter is not specified, the responses from only the PW nodes along the LSP are displayed.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

After the VPLS network is configured, if the VSI is in the Down state, you can run the **tracert vpls** command to locate the faulty device on the PW.

Example

Perform the tracert operation on the VPLS link.

```
<Huawei> tracert vpls vsi a1 peer 10.2.2.2
 TTL   Replier          Time    Type      Downstream
 0                        Ingress   10.1.1.2/[1025 3 ]
 1     10.2.2.2         30 ms   Egress
```

Table 12-172 Description of the **tracert vpls** command output

Item	Description
TTL	TTL in an MPLS Echo Request packet. It indicates the number of hops through which an MPLS Echo Request packet passes from the source node to this node.
Replier	IP address of the node sending MPLS Echo Reply packets.
Time	Time that the packet is processed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	Type of a node: ● Ingress: indicates an ingress node. ● Transit: indicates a transmit node. ● Egress: indicates an egress node.
Downstream	IP address and label of the downstream node.

Related Topics

12.13.32 ping vpls

12.13.44 traffic-statistics enable (VSI-LDP view)

Function

The **traffic-statistics enable** command enables the statistics about the public traffic on all Martini VPLS PWs.

The **undo traffic-statistics enable** command disables the statistics about the public traffic on all Martini VPLS PWs.

By default, the statistics function is disabled.

Format

traffic-statistics enable

undo traffic-statistics enable

Parameters

None

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **traffic-statistics enable** command to enable statistics about the traffic on all PWs.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Precautions

After this command is executed and the statistics reach the upper limit, a peer can still be configured, but the traffic statistics function does not take effect on this peer. When the configuration needs to be restored after the system is restarted, configured the peer first. If the statistics exceed the upper limit after the **traffic-statistics enable** is executed, the configuration cannot be restored.

The **traffic-statistics enable** command cannot be used together with the **traffic-statistics peer enable** command in the VSI-LDP view.

Example

Enable the statistics on all PWs in the VSI 1.

```
<Huawei> system-view
[Huawei] vsi vsi1
[Huawei-vsi-vsi1] pwsignal ldp
[Huawei-vsi-vsi1-ldp] vsi-id 1
[Huawei-vsi-vsi1-ldp] traffic-statistics enable
```

Related Topics

12.13.45 traffic-statistics peer enable

12.13.37 reset traffic-statistics vsi name

12.13.5 display traffic-statistics vsi

12.13.45 traffic-statistics peer enable

Function

The **traffic-statistics peer enable** command enables the statistics about the public traffic on a specified Martini VPLS PW.

The **undo traffic-statistics peer enable** command disables the statistics about the public traffic on a specified Martini VPLS PW.

By default, the statistics function is disabled.

Format

traffic-statistics peer *peer-address* [**negotiation-vc-id** *vc-id*] **enable**

undo traffic-statistics peer *peer-address* [**negotiation-vc-id** *vc-id*] **enable**

Parameters

Parameter	Description	Value
peer *peer-address*	Specifies the peer IP address of the PW.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
negotiation-vc-id *vc-id*	Specifies the ID of the PW.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI-LDP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Martini VPLS network is configured, you can run the **traffic-statistics peer enable** command to enable statistics about the traffic on the specified PW. You can specify *peer-address* to enable the statistics about the traffic on the corresponding PW.

Prerequisites

The VSI ID has been configured using the **vsi-id** *vsi-id* command in the VSI-LDP view.

Precautions

After you enable the statistics about the public traffic on the specified Martini VPLS PW, run the **display traffic-statistics vsi peer** command to view the statistics about the public traffic on the specified PW.

The **traffic-statistics peer enable** command cannot be used together with the **traffic-statistics enable** command in the VSI-LDP view.

Example

Enable the statistics about the public traffic on the specified Martini VPLS PW.

```
<Huawei> system-view
[Huawei] vsi newvsi static
[Huawei-vsi-newvsi] pwsignal ldp
[Huawei-vsi-newvsi-ldp] vsi-id 1
[Huawei-vsi-newvsi-ldp] traffic-statistics peer 10.22.33.20 negotiation-vc-id 2 enable
```

Related Topics

12.13.44 traffic-statistics enable (VSI-LDP view)
12.13.38 reset traffic-statistics vsi name peer
12.13.6 display traffic-statistics vsi peer

12.13.46 vpls ignore-ac-state

Function

The **vpls ignore-ac-state** command prevents the status of a VSI from being affected by the status of the Attachment Circuit (AC).

The **undo vpls ignore-ac-state** command restores the default setting.

By default, changes in the status of the AC affect the VSI status.

Format

vpls ignore-ac-state

undo vpls ignore-ac-state

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **vpls ignore-ac-state** command is used only before a service switchover between a new network and an old one. Before the devices on an old VPLS network switch to a new network, if you want to check whether the VSI on the new VPLS network can work normally, you can run this command to configure the VSI to ignore the AC status so that the VSI maintains the Up state before the switchover.

Precautions

After the **vpls ignore-ac-state** command is executed, a VSI can keep Up if the VSI PW is Up, and the VSI status is not affected by the AC status.

The AC status refers to the status of the physical or logical interface bound to the VSI.

After the devices on the old network switch to a new network, run the **undo vpls ignore-ac-state** command to restore the default setting.

Example

Configure a VSI to ignore the AC status.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] vpls ignore-ac-state
```

12.13.47 vpls mac-withdraw loop-detect enable

Function

The **vpls mac-withdraw loop-detect enable** command enables MAC withdraw loop detection.

The **undo vpls mac-withdraw loop-detect enable** command disables MAC withdraw loop detection.

By default, MAC withdraw loop detection is disabled.

Format

vpls mac-withdraw loop-detect enable

undo vpls mac-withdraw loop-detect enable

Parameters

None

Views

MPLS-L2VPN view

Default Level

2: Configuration level

Usage Guidelines

On a dual-homing VPLS network, MAC withdraw messages can be forwarded between hub and spoke PWs and between spoke PWs. Incorrect configurations may cause a MAC withdraw message loop, which results in traffic loss. If the loop involves a large number of MAC withdraw messages, denial of service (DoS) attacks may occur. To resolve these problems, run the **vpls mac-withdraw loop-detect enable** command to enable MAC withdraw loop detection. After you enable MAC withdraw loop detection, a PE immediately discards MAC withdraw message when it detects a MAC withdraw message loop.

Example

Enable MAC withdraw loop detection.

```
<Huawei> system-view
[Huawei] mpls l2vpn
[Huawei-l2vpn] vpls mac-withdraw loop-detect enable
```

 Copyright © Huawei Technologies Co., Ltd.

12.13.48 vsi

Function

The **vsi** command creates a VSI or displays the VSI view.

The **undo vsi** command deletes a VSI.

By default, no VSI is created.

Format

vsi *vsi-name* [**static**]

undo vsi *vsi-name*

Parameters

Parameter	Description	Value
vsi-name	Specifies the name of a VSI.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Names of the VSIs on one device cannot be identical.
static	Indicates that the static member discovery mode is used in the VSI. You must specify this parameter when creating a VSI.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure VPLS, run the **vsi** *vsi-name* **static** command to create a VSI first. Each device in a VPLS domain needs to be configured with a VSI that belongs to the domain.

Prerequisites

MPLS L2VPN has been enabled by using the **mpls l2vpn** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Note the following points when configuring VSIs in a VPLS domain:

- VSIs on different PEs can have different names.
- A VSI on a PE must be configured with a unique VSI ID.
- Multiple peers can be specified for a VSI on a PE.

If the specified VSI exists, you can use the **vsi** *vsi-name* [**static**] command to enter the VSI view.

After VPLS configurations are complete, VPLS packets are forwarded based on VSIs. Exercise caution when using the **undo vsi** command because VPLS traffic will be interrupted.

Example

Create a Martini VPLS VSI named **company1**.

```
<Huawei> system-view
[Huawei] mpls lsr-id 10.1.1.1
[Huawei] mpls
[Huawei-mpls] quit
[Huawei] mpls l2vpn
[Huawei-l2vpn] quit
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
```

Related Topics

12.13.11 display vsi

12.13.14 display vsi remote

12.13.49 vsi-id

12.13.49 vsi-id

Function

The **vsi-id** command sets an ID for a VSI.

By default, no VSI ID is set.

Format

vsi-id *vsi-id*

Parameters

Parameter	Description	Value
vsi-id	Specifies the unique ID of a VSI.	The value is an integer that ranges from 1 to 4294967295.

Views

VSI-LDP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VSI in the Martini VPLS and use the LDP as the PW signaling protocol, run the **vsi-id** command to configure the VSI ID. Other parameters can be configured only after the VSI ID is configured.

Precautions

Different VSIs have different IDs.

VSI IDs on all devices in the same VPLS domain must be the same.

The VSI ID cannot be changed after being set. If you want to change the VSI ID, you need to delete the VSI and re-create a VSI.

Example

Set the ID of the current VSI to 101.

```
<Huawei> system-view
[Huawei] vsi company1 static
[Huawei-vsi-company1] pwsignal ldp
[Huawei-vsi-company1-ldp] vsi-id 101
```

Related Topics

12.13.11 display vsi

12.13.14 display vsi remote

12.13.48 vsi

12.13.35 pwsignal

12.14 VXLAN Configuration Commands

NOTE

Only the AR100, AR120, AR150, AR160, AR200, AR1200 series, AR2220E, AR2240, and AR3260 support VXLAN. AR2220E, AR2240, and AR3260 need to run the **portswitch** command to change the working mode of all interfaces on the SRU200, SRU400, 4GECS, and 2X10GL from Layer 3 mode to Layer 2 mode. The interfaces that change the working mode to layer 2 only support VXLAN. Only the 8FE1GE, 24GE, and 24ES2GP ethernet LAN card support VXLAN.

12.14.1 arp static vni

Function

The **arp static vni** command configures a static ARP entry for a VXLAN tunnel.

The **undo arp static vni** command deletes the static ARP entry of a VXLAN tunnel.

By default, a static MAC address entry of a VXLAN tunnel is not configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

arp static *ip-address mac-address* **vni** *vni-id* **source-ip** *source-ip-address* **peer-ip** *peer-ip-address*

undo arp static *ip-address mac-address* **vni** *vni-id* **source-ip** *source-ip-address* **peer-ip** *peer-ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address mapping the destination IP address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vni *vni-id*	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.
source-ip *source-ip-address*	Specifies the IP address of the source VTEP.	The value is in dotted decimal notation.
peer-ip *peer-ip-address*	Specifies the IP address of the destination VTEP.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static ARP entries are manually configured and maintained. They cannot be aged and overridden by dynamic ARP entries. Running the **arp static vni** command on a Layer 3 VXLAN gateway to configure static ARP entries increases communication security. Static ARP entries ensure communication between the local device and a specified device by using a specified MAC address so that attackers cannot modify mappings between IP addresses and MAC addresses in static ARP entries.

Prerequisites

A VXLAN tunnel and a Layer 3 gateway have been configured.

Precautions

The IP address specified by the *ip-address* command must be in the same network segment as the IP address of the outbound interface specified by the **interface** *interface-type interface-number* command.

 Copyright © Huawei Technologies Co., Ltd.

If a static ARP entry to be created exists, the system updates the entry.

Example

Configure a static ARP entry for the VXLAN tunnel with the IP address 10.2.2.10 and MAC address 0011-0022-0033.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] vxlan vni 1010
[Huawei-bd10] quit
[Huawei] interface vbdif 10
[Huawei-Vbdif10] ip address 10.2.2.2 255.255.255.0
[Huawei-Vbdif10] quit
[Huawei] interface nve 1
[Huawei-Nve1] source 1.1.1.1
[Huawei-Nve1] vni 1010 head-end peer-list 2.2.2.2
[Huawei-Nve1] quit
[Huawei] arp static 10.2.2.10 0011-0022-0033 vni 1010 source-ip 1.1.1.1 peer-ip 2.2.2.2
```

12.14.2 arp static vni interface

Function

The **arp static vni interface** command configures static ARP entries.

The **undo arp static vni interface** command deletes static ARP entries.

By default, no static ARP entry is configured.

Format

arp static *ip-address mac-address* **vni** *vni-id* [**vid** *vlan-id* [**cevid** *ce-vid*]] **interface** *interface-type interface-number*

undo arp static *ip-address mac-address* **vni** *vni-id* [**vid** *vlan-id* [**cevid** *ce-vid*]] **interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
mac-address	Specifies the destination MAC address mapping the destination IP address.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.
vni *vni-id*	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.
vid *vlan-id*	Specifies the ID of the VLAN to which a static ARP entry belongs.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cevid *ce-vid*	Specifies the ID of the inner VLAN to which a static ARP entry belongs.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Specifies the outbound interface of a static ARP packet. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. Only Layer 2 Ethernet interface or Layer 2 sub-interface is supported.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Static ARP entries are manually configured and maintained. They cannot be aged and overridden by dynamic ARP entries. Running the **arp static vni interface** command on a VXLAN network to configure static ARP entries increases communication security. Static ARP entries ensure communication between the local device and a specified device by using a specified MAC address so that attackers cannot modify mappings between IP addresses and MAC addresses in static ARP entries.

Prerequisites

An access-side VXLAN deployment mode and a Layer 3 gateway have been configured.

Precautions

The IP address specified by the *ip-address* command must be in the same network segment as the IP address of the outbound interface specified by the **interface** *interface-type interface-number* command.

If a static ARP entry to be created exists, the system updates the entry.

- On a Layer 2 Ethernet interface, run the **arp static** *ip-address mac-address* **vni** *vni-id* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries.
- On a Layer 2 sub-interface:

- If the traffic encapsulation type is **dot1q**, run the **arp static** *ip-address mac-address* **vni** *vni-id* **vid** *vlan-id* **interface** *interface-type interface-number* command to configure static ARP entries. The value of **vid** *vlan-id* in this command must be the same as that in the **encapsulation dot1q vid** *pe-vid* command.
- If the traffic encapsulation type is **qinq**, run the **arp static** *ip-address mac-address* **vni** *vni-id* **vid** *vlan-id* **cevid** *ce-vid* **interface** *interface-type interface-number* command to configure static ARP entries. The values of **vid** *vlan-id* and **cevid** *ce-vid* in this command must be the same as the values in the **encapsulation qinq vid** *vlan-vid* **ce-vid** *ce-vid* command.
- If the traffic encapsulation type is **untag**, run the **arp static** *ip-address mac-address* **vni** *vni-id* **interface** *interface-type interface-number* command to configure static ARP entries.

Example

Configure a static ARP entry with IP address 10.3.3.10, MAC address 0031-0032-0033, VLAN ID 300, and outbound interface GE0/0/3.

```
<Huawei> system-view
[Huawei] vlan 300
[Huawei-vlan300] quit
[Huawei] bridge-domain 30
[Huawei-bd30] vxlan vni 3010
[Huawei-bd30] l2 binding vlan 300
[Huawei-bd30] quit
[Huawei] interface gigabitethernet 0/0/3
[Huawei-GigabitEthernet0/0/3] port link-type access
[Huawei-GigabitEthernet0/0/3] port default vlan 300
[Huawei-GigabitEthernet0/0/3] quit
[Huawei] interface vbdif 30
[Huawei-Vbdif30] ip address 10.3.3.2 255.255.255.0
[Huawei-Vbdif30] quit
[Huawei] arp static 10.3.3.10 0031-0032-0033 vni 3010 vid 300 interface gigabitethernet 0/0/3
```

Configure a static ARP entry with IP address 10.1.1.10, MAC address 0011-0012-0013, VLAN ID 100, and outbound interface GE0/0/1.1.

```
<Huawei> system-view
[Huawei] bridge-domain 20
[Huawei-bd20] vxlan vni 2010
[Huawei-bd20] quit
[Huawei] interface gigabitethernet 0/0/1.1 mode l2
[Huawei-GigabitEthernet0/0/1.1] encapsulation dot1q vid 100
[Huawei-GigabitEthernet0/0/1.1] bridge-domain 20
[Huawei-GigabitEthernet0/0/1.1] quit
[Huawei] interface vbdif 20
[Huawei-Vbdif20] ip address 10.1.1.2 255.255.255.0
[Huawei-Vbdif20] quit
[Huawei] arp static 10.1.1.10 0011-0012-0013 vni 2010 vid 100 interface gigabitethernet 0/0/1.1
```

12.14.3 bridge-domain (Layer 2 sub-interface view)

Function

The **bridge-domain** command associates a Layer 2 sub-interface with a BD.

The **undo bridge-domain** command restores the default settings.

By default, no Layer 2 sub-interface is associated with a BD.

Format

bridge-domain *bd-id*

undo bridge-domain [*bd-id*]

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of the BD that is associated with a Layer 2 sub-interface.	The BD ID must exist.

Views

Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

On the access side, two methods are available for creating a large Layer 2 BD.

- Based on VLAN: You can associate one or multiple VLANs with a BD to add users in these VLANs to the BD. This VLAN-based mode implements larger-granularity control, but is easy to configure. It applies to VXLAN deployment on a live network.
- Based on encapsulation mode: The device sends packets of different encapsulation modes to different Layer 2 sub-interfaces based on the VLAN tags contained in the packets. You can bind a Layer 2 sub-interface to a BD to add specified users to the BD. This mode implements refined and flexible control but requires more complex configuration. It applies to VXLAN deployment on a new network.

To create a BD based on encapsulation mode, create a Layer 2 sub-interface first. Then run the **encapsulation (Layer 2 sub-interface view)** command to configure a supported encapsulation mode on the sub-interface. After you run the **bridge-domain (Layer 2 sub-interface view)** command to associate a Layer 2 sub-interface with a BD, packets containing the same VLAN tag from different LANs can communicate at Layer 2.

Prerequisites

A BD has been created using the **12.14.4 bridge-domain (system view)** command in the system view.

Precautions

One Layer 2 sub-interface can be associated with only one BD.

 Copyright © Huawei Technologies Co., Ltd.

For the BD that bind to the Layer 2 sub-interfaces which use **dot1q** encapsulation, the VBDIF interface of this BD cannot be created on the device.

Example

Associate Layer 2 sub-interface Eth2/0/0.1 with BD 10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface ethernet 2/0/0.1 mode l2
[Huawei-Ethernet2/0/0.1] bridge-domain 10
```

12.14.4 bridge-domain (system view)

Function

The **bridge-domain** command creates a bridge domain (BD) and displays the BD view, or directly displays the view of an existing BD view.

The **undo bridge-domain** command deletes a BD.

By default, no BD is created.

Format

bridge-domain *bd-id*

undo bridge-domain *bd-id*

Parameters

Parameter	Description	Value
bd-id	Specifies the ID of a BD.	The value is an integer. The value ranges are as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-64 ● AR1200 series: 1-128 ● AR2220E: 1-256

Views

System view

Default Level

2: Configuration level

Usage Guidelines

BDs are Layer 2 bridge domains on a large Layer 2 network constructed using VXLAN. VXLAN packets can be forwarded at Layer 2 within a BD through a VXLAN tunnel.

 Copyright © Huawei Technologies Co., Ltd.

After you run the **bridge-domain** command to create a BD, you can complete other VXLAN configurations in the BD.

Example

Create BD 10 and enter the view of BD 10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10]
```

12.14.5 description (BD view)

Function

The **description** command configures the description of a bridge domain (BD).

The **undo description** command deletes the description of a BD.

By default, no description is configured for a BD.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the BD description.	The value is a string of 1 to 80 case-sensitive characters without spaces.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

If you have configured multiple BDs using the **bridge-domain (system view)** command, run the **description** command in the corresponding BD view to configure the description for each BD. BD description helps you quickly understand the function of each BD, facilitating service management.

Example

Configure description **vxlan** for BD 10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] description vxlan
```

 Copyright © Huawei Technologies Co., Ltd.

12.14.6 display bridge-domain

Function

The **display bridge-domain** command displays the BD configuration.

Format

display bridge-domain [*bd-id* [**brief** | **verbose**]]

Parameters

Parameter	Description	Value
bd-id	Displays the configuration of a specified BD. If this parameter is not specified, the device displays the configuration of all BDs.	The BD ID must exist.
brief	Displays brief BD configuration.	-
verbose	Displays detailed BD configuration.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After BDs are created on a device, you can run the **display bridge-domain** command to view the configuration of a specified BD or all BDs.

Example

Display the configuration of all BDs.

```
<Huawei> display bridge-domain
-------------------------------------------------------------------------------

BDID     State      Description
-------------------------------------------------------------------------------
10       down       vxlan
20       up         vxlan
-------------------------------------------------------------------------------
The total number of bridge-domains is : 2
```

Display the detailed configuration of BD 10.

```
<Huawei> display bridge-domain 10 verbose
Bridge-domain ID   :10
Description        :vxlan
State              :Down
```

```
--------------------------------------------------------------------------------
Interface                          State
--------------------------------------------------------------------------------
Ethernet2/0/0.1                      down
--------------------------------------------------------------------------------
VLAN                               State
--------------------------------------------------------------------------------
2                                 down
3                                 down
10                                 down
--------------------------------------------------------------------------------
```

Table 12-173 Description of the **display bridge-domain** command output

Item	Description
BDID/Bridge-domain ID	ID of a BD. To set the BD ID, run the **12.14.4 bridge-domain (system view)** command in the system view.
State	BD status: ● up: The BD is bound to a Layer 2 sub-interface, VLAN, or VNI, and at least one of the bound Layer 2 sub-interface, VLAN, and VNI is Up. ● down: The BD is not bound to a Layer 2 sub-interface, VLAN, or VNI; alternatively, the BD is bound to a Layer 2 sub-interface, VLAN, or VNI and the bound Layer 2 sub-interface, VLAN, and VNI are Down.
Description	BD description. To configure the description of a BD, run the **description (BD view)** command.
The total number of bridge-domains is	Total number of BDs on the device.
Interface State	Member interface in a BD and its status. ● up: The link layer protocol of the interface is in the Up state. ● down: The link layer protocol of the interface is Down.
VLAN State	Status of the VLAN associated with the BD. ● up ● down The status of a VLAN is determined by the status of member interfaces in the VLAN. A VLAN is Up only when at least one member interface in the VLAN is Up.

 Copyright © Huawei Technologies Co., Ltd.

12.14.7 display interface nve

Function

The **display interface nve** command displays NVE interface information.

Format

display interface nve [*nve-number* | **main**]

Parameters

Parameter	Description	Value
nve-number	Specifies the number of an NVE interface. If *nve-number* is not specified, information about all NVE interfaces is displayed.	The value is 1.
main	Displays the running status and statistics of the main interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To monitor the NVE interface status or locate an NVE interface fault on the VXLAN network, run the **display interface nve** command to check the running status and statistics of the NVE interface.

Example

Display the running status of the NVE interface.

```
<Huawei> display interface nve 1
Nve1 current state : UP
Line protocol current state : UP
Description:HUAWEI, AR Series, Nve1 Interface
Route Port,The Maximum Transmit Unit is 1500
Current system time: 2016-09-21 17:05:06
```

Table 12-174 Description of the **display interface nve** command output

Item	Description
Nve1 current state	Indicates the physical status of the NVE interface. The physical status of the successfully created NVE interface is always Up.
Line protocol current state	Link layer protocol status of the NVE interface. The link layer protocol status of the successfully created NVE interface is always Up.
Description	Description of the NVE interface.
Current system time	System time. If a time zone is configured and the daylight saving time is used, the time is displayed in the format of YYYY/MM/DD HH:MM:SS UTC ±HH:MM DST.

12.14.8 display mac-address bridge-domain

Function

The **display mac-address bridge-domain** command displays MAC address entries of a BD.

Format

display mac-address [*mac-address*] **bridge-domain** *bd-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits, such as 00e0 and fc01. The MAC address cannot be the broadcast MAC address (FFFF-FFFF-FFFF), multicast MAC address (the eighth bit is 1), or MAC address of all 0s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bd-id	Displays MAC address entries of a specified BD.	The value is an integer. The value ranges are as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-64 ● AR1200 series: 1-128 ● AR2220E: 1-256

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The MAC address table needs to be updated constantly because the network topology always changes. To learn about MAC address entries of a BD in a timely manner, run the **display mac-address bridge-domain** command.

NOTE

The device supports only query of MAC address entries based on a BD.

Example

Display all MAC address entries of BD 10.

```
<Huawei> display mac-address bridge-domain 10
MAC_Address    VLAN/Bridge/VSI/BD        Learned-From              Type
0003-0002-0003 -/-/-/10                  Ethernet0/0/1.1           static
Total items: 1
```

Display the MAC address entry with the MAC address of 0004-0003-0004 in BD 20.

```
<Huawei> display mac-address 0004-0003-0004 bridge-domain 20
MAC_Address    VLAN/Bridge/VSI/BD        Learned-From              Type
0004-0003-0004 -/-/-/20                  2.2.2.2                   static
Total items: 1
```

Table 12-175 Description of the **display mac-address bridge-domain** command output

Item	Description
MAC_Address	Destination MAC address.

Item	Description
VLAN/ Bridge/VSI/BD	• VLAN: VLAN associated with the interface • Bridge: bridge that the interface belongs to • VSI: VSI associated with the interface • BD: BD associated with the interface **NOTE** BD information is displayed only on the VXLAN-enabled device.
Learned-From	• LAN side: Layer 2 sub-interface that joins a BD • VXLAN side: IP address of the remote VTEP
Type	Type of a MAC address: • **static**: indicates the static MAC address entry. A static MAC address entry is manually configured and will not be aged out. • **dynamic**: indicates the MAC address entry learned by the device based on the source MAC address. Dynamic MAC address entries have the aging time and can be aged.
Total items	Total number of MAC address entries that match the filtering condition.

Related Topics

12.14.19 mac-address static bridge-domain

12.14.9 display vxlan encapsulation

Function

The **display vxlan encapsulation** command displays VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface.

Format

display vxlan encapsulation interface *interface-type interface-number* [**bridge-domain** *bd-id* | **default** | **dot1q** [**vid** *pe-vid*] | **qinq** [**vid** *vlan-vid* [**ce-vid** *ce-vid*]] | **untag**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays VXLAN encapsulation information about a specified Layer 2 sub-interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
bridge-domain *bd-id*	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by BD ID.	The BD ID must exist.
default	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **default**.	-
dot1q	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **Dot1q**.	-
vid *pe-vid*	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by VLAN ID in packets with the flow encapsulation mode **Dot1q**.	The VLAN ID must exist.
qinq	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **QinQ**.	-
vid *vlan-vid* [**ce-vid** *ce-vid*]	Displays VXLAN encapsulation information about Layer 2 sub-interfaces by VLAN ID in packets with the flow encapsulation mode **QinQ**. ● *vlan-vid* specifies the outer VLAN ID. ● *ce-vid* specifies the inner VLAN ID.	The VLAN ID must exist.
untag	Displays VXLAN encapsulation information about Layer 2 sub-interfaces for the flow encapsulation mode **untag**.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display vxlan encapsulation** command to view VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface as well as the bindings between the sub-interface and BD.

Example

Display VXLAN encapsulation information about Layer 2 sub-interfaces of a main interface.

```
<Huawei> display vxlan encapsulation interface ethernet 1/0/1
-----------------------------------------------------------------------------------------------
Interface              EncapType        PeVid        CeVid        BD-ID
-----------------------------------------------------------------------------------------------
Ethernet1/0/1.1          QinQ            4093         4093         16000
-----------------------------------------------------------------------------------------------
Total number to display is 1.
```

Table 12-176 Description of the **display vxlan encapsulation** command output

Item	Description
Interface	Name of the Layer 2 sub-interface.
EncapType	Flow encapsulation type of the Layer 2 sub-interface. • QinQ • Dot1q • Default • Untag To configure the flow encapsulation type, run the **12.14.13 encapsulation (Layer 2 sub-interface view)** command.
PeVid	VLAN ID of packets with the flow encapsulation type **Dot1q** or outer VLAN ID of packets with the flow encapsulation type **QinQ**. To configure the VLAN ID, run the **12.14.13 encapsulation (Layer 2 sub-interface view)** command.
CeVid	Inner VLAN ID of packets with the flow encapsulation type **QinQ**. To configure the VLAN ID, run the **12.14.13 encapsulation (Layer 2 sub-interface view)** command.
BD-ID	BD. To configure the BD, run the **12.14.3 bridge-domain (Layer 2 sub-interface view)** command.
Total number to display is	Total number of encapsulation data records about Layer 2 sub-interfaces of a main interface.

 Copyright © Huawei Technologies Co., Ltd.

12.14.10 display vxlan peer

Function

The **display vxlan peer** command displays the IP address of the destination virtual tunnel end point (VTEP) of a Virtual Network Identifier (VNI).

Format

display vxlan peer [**vni** *vni-id*]

Parameters

Parameter	Description	Value
vni *vni-id*	Displays the IP address of the destination VTEP of a specified VNI.	The VNI ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After completing VXLAN configuration, you can run the **display vxlan peer** command to view information about the source and destination IP address bound to the VNI.

Precautions

Before running the **display vxlan peer** command, ensure that the device has been configured with VNIs. Otherwise, the command output is meaningless.

Example

Display the IP address of the destination VTEP of a specified VNI.

```
<Huawei> display vxlan peer
 Vni ID      Source            Destination          Type
 ------------------------------------------------------------
 10          10.1.1.2          10.1.1.3             static
 10          10.1.1.2          10.1.1.4             static
 ------------------------------------------------------------
 Number of peers :
 Total: 2   Static: 2   L3 dynamic: 0
```

Table 12-177 Description of the **display vxlan peer** command output

Item	Description
Vni ID	ID of a VNI. To configure or modify a VNI ID, run the **12.14.23 vxlan vni (BD view)** command.
Source	IP address of the source VTEP. To configure or modify the IP address of the source VTEP, run the **12.14.21 source (NVE interface view)** command.
Destination	IP address of the destination VTEP. To configure or modify the IP address of the destination VTEP, run the **vni head-end peer-list** command.
Type	IP address configuration mode of the destination VTEP: ● static: The IP address is manually configured. ● l3 dynamic: Layer 3 VXLAN tunnel IP addresses are dynamically generated through the BGP protocol. To configure the IP address configuration mode, run the **vni head-end peer-list** command.
Number of peers	Number of IP addresses of destination VTEPs on the device: ● Total: indicates the number of IP addresses of destination VTEPs. ● Static: indicates the number of IP addresses of static destination VTEPs. ● L3 dynamic: indicates the number of IP addresses of Layer 3 dynamic destination VTEPs.

12.14.11 display vxlan tunnel

Function

The **display vxlan tunnel** command displays information about VXLAN tunnels.

Format

display vxlan tunnel [*tunnel-id*] [**verbose**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tunnel-id	Displays information about the VXLAN tunnel with a specified ID. If this parameter is not specified, the device displays information about all VXLAN tunnels.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays detailed VXLAN tunnel information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After VXLAN tunnels are established, you can run the **display vxlan tunnel** command to view VXLAN tunnel information.

Example

Display VXLAN tunnel information.

```
<Huawei> display vxlan tunnel
 Tunnel ID       Source            Destination       State     Type
 --------------------------------------------------------------------------
 4026531841      10.1.1.2          10.1.1.4          up        static
 4026531842      10.1.1.1          10.1.1.3          up        l3 dynamic
 --------------------------------------------------------------------------
 Number of vxlan tunnel :
 Total: 2   Static: 1   L3 dynamic: 1
```

Display detailed VXLAN tunnel information.

```
<Huawei> display vxlan tunnel verbose
 Tunnel ID       : 4026531841
 Source          : 10.1.1.2
 Destination     : 10.1.1.4
 State           : up
 Type            : static

 Tunnel ID       : 4026531842
 Source          : 10.1.1.1
 Destination     : 10.1.1.3
 State           : up
 Type            : l3 dynamic
 --------------------------------------------------------------------------
 Number of vxlan tunnel :
 Total: 2   Static: 1   L3 dynamic: 1
```

 Copyright © Huawei Technologies Co., Ltd.

Table 12-178 Description of the **display vxlan tunnel** command output

Item	Description
Tunnel ID	ID of a VXLAN tunnel. After a VXLAN tunnel is established, the ID is automatically generated by the device.
Source	Source IP address of the VXLAN tunnel. To configure the source IP address, run the **source (NVE interface view)** command.
Destination	Destination IP address of the VXLAN tunnel.
State	Status of the VXLAN dynamic tunnel: ● up: The VXLAN tunnel is reachable. ● down: The VXLAN tunnel is unreachable. Status of the VXLAN static tunnel: ● up: The destination route exists. ● down: The destination route not exists.
Type	Status of the VXLAN tunnel, which is determined by the **peer-list** parameter in the **vni head-end peer-list** command. ● static: The peer list is configured manually. ● l3 dynamic: The peer list is learned by a dynamic routing protocol.
Number of vxlan tunnel	Total number of VXLAN tunnels on the device. ● Total: indicates the number of VXLAN tunnels. ● Static: indicates the number of static VXLAN tunnels. ● L3 dynamic: indicates the number of Layer 3 dynamic VXLAN tunnels.

12.14.12 display vxlan vni

Function

The **display vxlan vni** command displays the VXLAN configuration of a specified VNI or all VNIs.

Format

display vxlan vni [*vni-id* [**verbose**]]

Parameters

Parameter	Description	Value
vni-id	Displays VXLAN information about a specified VNI. If this parameter is not specified, the device displays VXLAN configuration of all VNIs.	The VNI ID must exist.
verbose	Displays detailed VXLAN information about a specified VNI.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Applications

After VXLAN is configured, you can run the **display vxlan vni** command to view information about BDs associated with VNIs, VPN instances bound to the VNIs, and VNI status.

Precautions

Before running the **display vxlan vni** command, ensure that the device has been configured with VNIs. Otherwise, the command output is meaningless.

Example

Display VXLAN information about all VNIs.

```
<Huawei> display vxlan vni
 VNI              BD-ID            State
 ----------------------------------------
 10               10               up
 50               50               up
 ----------------------------------------
 Number of vxlan vni bound to BD is : 2

 VNI              VRF-ID
 ----------------------------------------
 20               5
 ----------------------------------------
 Number of vxlan vni bound to VPN is : 1
```

Display detailed VXLAN information about VNI 10.

```
<Huawei> display vxlan vni 10 verbose
 BD ID              :10
 State              :up
 Source             :10.1.1.2
```

```
UDP Port          :4789
Peer List         :10.1.1.1 10.1.1.3
```

Display detailed VXLAN information about VNI 20.

```
<Huawei> display vxlan vni 20 verbose
 VRF-ID            :5
```

Table 12-179 Description of the **display vxlan vni** command output

Item	Description
VNI	ID of a VNI. To configure or modify a VNI ID, run the **vxlan vni** command.
BD-ID (BD ID)	ID of the BD associated with a VNI. To configure or modify a BD ID, run the **bridge-domain (system view)** command.
State	VNI status: ● up ● down To ensure that the VNI status is up, the corresponding VXLAN tunnel must exist and be up for the VNI. If the VNI status is down, check whether **Source** and **Peer List** in this command output are the same as **Source** and **Destination** in the output of the **display vxlan tunnel** command. ● If they are different, no VXLAN tunnel exists for the specified VNI. Run the **source (NVE interface view)** or **vni head-end peer-list** command to change the source or destination IP address of the VXLAN tunnel to ensure that the corresponding VXLAN tunnel exists for the VNI. ● If they are the same, collect related configuration and contact technical support personnel.
VRF-ID	VPN instance ID.
Number of vxlan vni bound to VPN is	Number of existing VNIs bound to VPN instances.
Source	IP address of the source VTEP. To configure the IP address of the source VTEP, run the **source (NVE interface view)** command.
Source IPv6 Address	IPv6 address of the source VTEP. To configure the IP address of the source VTEP, run the **source (NVE interface view)** command.
UDP Port	Destination UDP port. The port number is fixed as 4789.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Peer List	IP address of the destination VTEP. To configure the IP address of the destination VTEP, run the **vni head-end peer-list** command.
IPv6 Peer List	IPv6 address of the destination VTEP. To configure the IP address of the destination VTEP, run the **vni head-end peer-list** command.

12.14.13 encapsulation (Layer 2 sub-interface view)

Function

The **encapsulation** command configures the encapsulation mode of packets allowed to pass a Layer 2 sub-interface.

The **undo encapsulation** command deletes the encapsulation mode of packets allowed to pass a Layer 2 sub-interface.

By default, the encapsulation mode of packets allowed to pass a Layer 2 sub-interface is not configured.

Format

encapsulation { **dot1q vid** *pe-vid* | **default** | **untag** | **qinq vid** *vlan-vid* **ce-vid** *ce-vid* }

undo encapsulation { **dot1q vid** *pe-vid* | **default** | **untag** | **qinq vid** *vlan-vid* **ce-vid** *ce-vid* }

Parameters

Parameter	Description	Value
dot1q	Sets encapsulation mode of packets allowed to pass a Layer 2 sub-interface to Dot1q. This mode enables a Layer 2 sub-interface to receive packets with a VLAN tag.	-
vid *pe-vid*	Specifies the outer VLAN ID in packets allowed to pass a Layer 2 sub-interface in Dot1q encapsulation mode.	The value is an integer that ranges from 2 to 4094.
default	Sets the encapsulation mode of packets allowed to pass a Layer 2 sub-interface to default. This mode enables a Layer 2 sub-interface to receive all packets, regardless of whether they contain VLAN tags.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
untag	Sets the encapsulation mode of packets allowed to pass a Layer 2 sub-interface to untag. This mode enables a Layer 2 sub-interface to receive packets without VLAN tags.	-
qinq	Sets encapsulation mode of packets allowed to pass a Layer 2 sub-interface to QinQ. This mode enables a Layer 2 sub-interface to receive packets with double VLAN tags.	-
vid *vlan-vid*	Specifies the outer VLAN ID in double-tagged packets allowed to pass a Layer 2 sub-interface in QinQ encapsulation mode.	The value is an integer that ranges from 2 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN ID in double-tagged packets allowed to pass a Layer 2 sub-interface in QinQ encapsulation mode.	The value is an integer that ranges from 1 to 4094.

Views

Layer 2 sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VXLAN network, a Layer 2 sub-interface functions as a VXLAN service access point to forward data packets in a BD.

Packets passing through a physical interface may contain one or two VLAN tags or no VLAN tag. After you run the **encapsulation** command in a Layer 2 sub-interface view to configure the encapsulation mode, the sub-interface can forward only specified types of packets.

Precautions

When configuring an encapsulation mode on a Layer 2 sub-interface, pay attention to the following points:

- The VLAN ID in **dot1q** mode or outer VLAN ID in **qinq** mode cannot be the same as the allowed VLAN of the corresponding main interface or the global VLAN.
- On the same main interface, the VLAN ID in **dot1q** mode and the outer VLAN ID in **qinq** mode must be different.
- After NAC authentication is configured on the main interface, the traffic encapsulation type on a Layer 2 sub-interface cannot be set to **default**.

 Copyright © Huawei Technologies Co., Ltd.

- When the encapsulation mode of a Layer 2 sub-interface is **default**, the corresponding main interface cannot be added to any VLAN, including VLAN 1.
- Before the encapsulation mode of a Layer 2 sub-interface is set to **default**, the main interface has only one sub-interface.
- After the encapsulation mode of a Layer 2 sub-interface is set to **default**, no other sub-interface can be created on the main interface.
- When the encapsulation mode of a Layer 2 sub-interface is set to **untag**, other sub-interfaces of the main interface cannot be set to **untag**.
- You can configure only one encapsulation mode for each Layer 2 sub-interface. If an encapsulation mode has been configured for a Layer 2 sub-interface, run the **undo encapsulation** command to delete the original mode before you configure another mode.
- When the device functions as a Layer 3 VXLAN gateway, the traffic encapsulation type on a Layer 2 sub-interface cannot be set to **default**.

Example

Set the encapsulation mode of packets allowed to pass Layer 2 sub-interface Eth2/0/0.1 to Dot1q and the outer VLAN ID in the packets to 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0.1 mode l2
[Huawei-Ethernet2/0/0.1] encapsulation dot1q vid 10
```

Related Topics

12.14.9 display vxlan encapsulation

12.14.14 interface mode l2

Function

The **interface mode l2** command creates a Layer 2 sub-interface and displays the Layer 2 sub-interface view.

The **undo interface** command deletes the created Layer 2 sub-interface.

By default, no Layer 2 sub-interface is created.

NOTE

Only 8FE1GE, 24GE, and 24ES2GP ethernet LAN card support this function.

Format

interface *interface-type interface-number.subinterface-number* **mode l2**

undo interface *interface-type interface-number.subinterface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number.subinterface-number	Specifies the type and number of a Layer 2 sub-interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a VXLAN network, you need to configure VXLAN service access points on a VXLAN network edge node. On the device, VXLAN service access points can be configured through a Layer 2 sub-interface or binding between VLANs and bridge domains (BDs).

When VXLAN service access points are configured through a Layer 2 sub-interface, the **interface mode l2** command needs to be used to configure the Layer 2 sub-interface first. After the Layer 2 sub-interface is created, you can run the **bridge-domain** *bd-id* command to add the Layer 2 sub-interface to a BD so that service packets are forwarded in the BD.

Precautions

The Layer 2 sub-interface can only join a BD but cannot directly connect to a Layer 3 network. Each Layer 2 sub-interface belongs to only one BD.

After the **interface mode l2** command is used to create a Layer 2 sub-interface, you can run the **interface** *interface-type interface-number.subinterface-number* **mode l2** or **interface** *interface-type interface-number.subinterface-number* command to enter the Layer 2 sub-interface view.

Example

Create Eth0/0/1.1.

```
<Huawei> system-view
[Huawei] interface ethernet 0/0/1.1 mode l2
```

12.14.15 interface nve

Function

The **interface nve** command creates a Network Virtualization Edge (NVE) interface and displays the NVE interface view.

The **undo interface nve** command deletes a specified NVE interface.

By default, no NVE interface is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

interface nve *nve-number*

undo interface nve *nve-number*

Parameters

Parameter	Description	Value
nve-number	Specifies the number of an NVE interface.	The value is 1.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make full use of advantages of server virtualization, you can deploy Virtual eXtensible Local Area Network (VXLAN) to connect to multiple tenants. VXLAN tunnel information needs to be configured on an NVE interface, so the **interface nve** command needs to be executed to create the NVE interface.

Precautions

After a VXLAN tunnel is configured, running the **undo interface nve** command will delete the specified NVE interface and all the configuration of the NVE interface.

Example

Create an NVE interface.

```
<Huawei> system-view
[Huawei] interface nve 1
```

12.14.16 interface vbdif

Function

The **interface vbdif** command creates a VBDIF interface and displays the VBDIF interface view.

The **undo interface vbdif** command deletes a VBDIF interface.

By default, no VBDIF interface is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

interface vbdif *bd-id*

undo interface vbdif *bd-id*

Parameters

Parameter	Description	Value
bd-id	Specifies a BD ID.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP routes are required for communication between VXLANs on different network segments and between VXLANs and non-VXLANs.

To allow communication between these networks, run the **vxlan vni** command to map VXLAN Network Identifiers (VNIs) to BDs in 1:1 mode, run the **interface vbdif** command to create a VBDIF interface for the BD, and configure an IP address for the BD. As a VBDIF interface is a Layer 3 logical interface similar to a VLANIF interface, it can have an IP address configured.

Prerequisites

A BD has been created by running the **bridge-domain** command.

Follow-up Procedure

Run the **ip address** command to configure an IP address for the VBDIF interface.

Example

Create VBDIF10.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface vbdif 10
```

 Copyright © Huawei Technologies Co., Ltd.

12.14.17 l2 binding vlan

Function

The **l2 binding vlan** command associates a specified VLAN with a BD.

The **undo l2 binding vlan** command restores the default settings.

By default, a VLAN is associated with no BD.

Format

l2 binding vlan *vlan-id*

undo l2 binding vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

On the access side, two methods are available for creating a large Layer 2 BD.

- Based on VLAN: You can associate one or multiple VLANs with a BD to add users in these VLANs to the BD. This VLAN-based mode implements larger-granularity control, but is easy to configure. It applies to VXLAN deployment on a live network.
- Based on encapsulation mode: The device sends packets of different encapsulation modes to different Layer 2 sub-interfaces based on the VLAN tags contained in the packets. You can bind a Layer 2 sub-interface to a BD to add specified users to the BD. This mode implements refined and flexible control but requires more complex configuration. It applies to VXLAN deployment on a new network.

After you run this command to associate specified VLANs with a BD, different VLANs associated with the same BD form a large Layer 2 network. Users belong to these VLANs can communicate at Layer 2 through VXLAN tunnels.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The VLAN to be bound to the BD has been created using the **6.3.43 vlan** command.

Precautions

- One VLAN can be associated with only one BD, but one BD can be associated with multiple VLANs.
- After a global VLAN is associated with a BD, you need to add corresponding interfaces to the VLAN. An Eth-Trunk cannot be added to the VLAN.

Example

Associate VLAN 10 with BD 10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] bridge-domain 10
[Huawei-bd10] l2 binding vlan 10
```

12.14.18 mac-address (VBDIF interface view)

Function

The **mac-address** command configures a MAC address for a VBDIF interface.

The **undo mac-address** command restores the default MAC address of a VBDIF interface.

By default, the MAC address of a VBDIF interface is the system MAC address.

Format

mac-address *mac-address*

undo mac-address

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a VBDIF interface.	The value is in the format of H-H-H. Each H is a 4-digit hexadecimal number, such as 00e0 or fc01. If you enter fewer than four digits, the system pads 0s before the input digits. For example, if you enter e0, 00e0 is displayed. The MAC address cannot be FFFF-FFFF-FFFF, all 0s, or a multicast MAC address.

Views

VBDIF interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

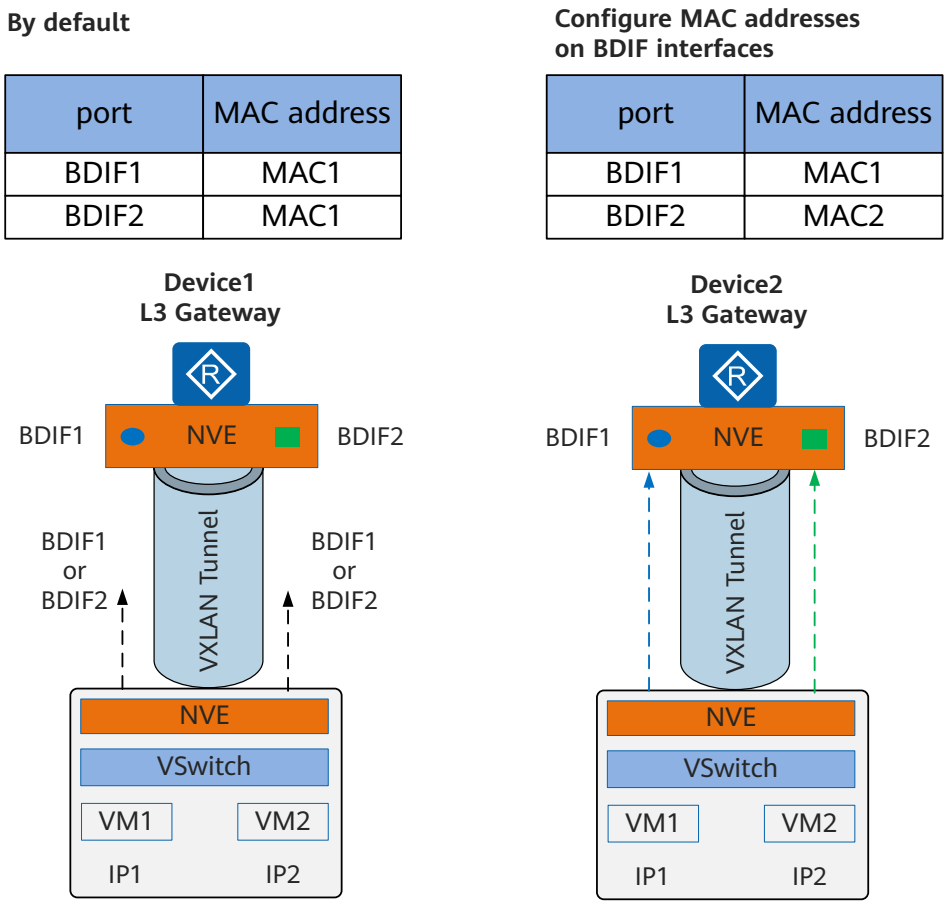
Usage Guidelines

Usage Scenario

In **Figure 12-1**, the VBDIF interface on both Layer 3 VXLAN gateways uses the system MAC address as its MAC address.

In a distributed gateway or centralized all-active gateway scenario, multiple Layer 3 gateways are simulated into one gateway. You need to configure the **mac-address** command to configure the same MAC address for the VBDIF interface on these Layer 3 gateways to ensure normal traffic forwarding and VM migration. Using the same MAC address, the Layer 3 gateways act like one gateway for terminals.

Figure 12-1 Default MAC addresses of VBDIF interfaces



Configuration Impact

After the MAC address of a VBDIF interface is changed, the device proactively sends gratuitous ARP packets to update ARP entries on the remote device.

Example

Set the MAC address of VBDIF 10 to 0001-2345-abcd.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface vbdif 10
[Huawei-Vbdif10] mac-address 0001-2345-abcd
```

12.14.19 mac-address static bridge-domain

Function

The **mac-address static bridge-domain** command configures a static MAC address entry based on a bridge domain (BD). The static MAC address entry guides data forwarding.

The **undo mac-address static** command deletes a static MAC address entry based on a BD.

By default, no static MAC address entry based on a BD is configured.

Format

mac-address static *mac-address interface-type interface-number.subnum* **bridge-domain** *bd-id* { **default** | **untag** | **vid** *vid* }

undo mac-address [*mac-address*] **bridge-domain** *bd-id*

undo mac-address { **static** | **dynamic** } **bridge-domain** *bd-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits, such as 00e0 and fc01. The MAC address cannot be the broadcast MAC address (FFFF-FFFF-FFFF), multicast MAC address (the eighth bit is 1), or MAC address of all 0s.
interface-type interface-number.subnum	Specifies the type and number of a Layer 2 sub-interface that joins a BD.	The interface type must be Ethernet.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bd-id	Specifies the ID of a BD.	The value is an integer. The value ranges are as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-64 ● AR1200 series: 1-128 ● AR2220E: 1-256
default	Indicates that the flow encapsulation mode of a Layer 2 sub-interface is default. All packets are transparently transmitted, without any VLAN tag processing.	-
untag	Indicates that the flow encapsulation mode of a Layer 2 sub-interface is untag. Packets are forwarded after VLAN tags are removed from the packets.	-
vid *vid*	Specifies the outer VLAN ID in packets received by a Layer 2 sub-interface.	The value is an integer that ranges from 1 to 4094.
dynamic	Deletes dynamic MAC address entries, that is, MAC address entries learned by an interface based on its source MAC address.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the VXLAN-enabled device forwards BUM packets to the user side, the following issues may occur:

- MAC address table attacks

  When an attack source sends packets with variable MAC addresses, the network device receives the packets and learns source MAC addresses. Because the size of the MAC address table is limited, the device cannot learn MAC addresses of packets after the number of MAC address entries reaches the maximum. During Layer 2 forwarding, these packets will be broadcast in a BD. This seriously affects the network bandwidth and affects the downstream hosts connected to the device.
- MAC address entry attacks

  When the device creates a MAC address table by learning source MAC addresses, the device cannot distinguish packets from authorized and unauthorized users. This threatens network security. If an unauthorized user uses the MAC address of an authorized user as the source MAC address of attack packets and connects to another interface of the device, the device learns an incorrect MAC address entry. The device incorrectly forwards the packets to the unauthorized user. Actually, the packets should be forwarded to the authorized user.

To improve interface security, the network administrator can run the **mac-address static bridge-domain** command to manually add a static MAC address entry to the MAC address table. The static MAC address entry binds the MAC address of an authorized user to a specified interface, which prevents unauthorized users from intercepting data of authorized users.

Prerequisites

Ensure that the following operations have been performed:

- The network administrator is familiar with MAC addresses of devices that need to use static MAC address entries for communication on a network; otherwise, communication of authorized users will be interrupted.
- A Layer 2 sub-interface has been created and joined a BD, and the flow encapsulation mode of the Layer 2 sub-interface has been configured.

Configuration Notes

Manually created MAC address entries take precedence over automatically created MAC address entries. Manually created static MAC address entries and blackhole MAC address entries are not overridden by dynamic MAC address entries, but dynamic MAC address entries can be overridden by static MAC address entries and blackhole MAC address entries.

 Copyright © Huawei Technologies Co., Ltd.

The created static MAC address entries never age out. When the device receives a frame with a specific MAC address, it forwards the frame through the outbound interface. After the configuration is saved, MAC address entries are not lost during system reset or hot swapping of cards.

Example

Configure the device to use Eth0/0/1.1 to forward the received packets that have the destination MAC address of 0003-0002-0003 and belong to BD 10. Eth0/0/1.1 uses dot1q encapsulation.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] quit
[Huawei] interface ethernet0/0/1.1 mode l2
[Huawei-Ethernet0/0/1.1] bridge-domain 10
[Huawei-Ethernet0/0/1.1] encapsulation dot1q vid 10
[Huawei-Ethernet0/0/1.1] quit
[Huawei] mac-address static 0003-0002-0003 ethernet0/0/1.1 bridge-domain 10 vid 10
```

12.14.20 mac-address static vni

Function

The **mac-address static vni** command configures a static MAC address entry of a VXLAN tunnel.

The **undo mac-address static** command deletes a static MAC address entry of a VXLAN tunnel.

By default, a static MAC address entry of a VXLAN tunnel is not configured.

Format

mac-address static *mac-address* **bridge-domain** *bd-id* **source** *source-ip-address* **peer** *peer-ip-address* **vni** *vni-id*

undo mac-address [*mac-address*] **bridge-domain** *bd-id*

undo mac-address { **static** | **dynamic** } **bridge-domain** *bd-id*

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits, such as 00e0 and fc01. The MAC address cannot be the broadcast MAC address (FFFF-FFFF-FFFF), multicast MAC address (the eighth bit is 1), or MAC address of all 0s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bridge-domain *bd-id*	Specifies the ID of a BD associated with a VNI.	The value is an integer. The value ranges are as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-64 ● AR1200 series: 1-128 ● AR2220E: 1-256
source *source-ip-address*	Specifies the IP address of the local VTEP.	The value is in dotted decimal notation.
peer *peer-ip-address*	Specifies the IP address of the remote VTEP.	The value is in dotted decimal notation.
vni-id	Specifies the VNI ID.	The value is an integer that ranges from 0 to 16777215.
dynamic	Deletes dynamic MAC address entries, that is, MAC address entries learned by an interface based on its source MAC address.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving a broadcast, unknown unicast, and multicast (BUM) packet, the VXLAN tunnel ingress replicates the packet based on the VTEP list and forwards it to all the VTEPs with the same VNI. To reduce broadcast traffic and improve network security, run the **mac-address static vni** command to configure a static MAC address entry to specify the forwarding path. This prevents unauthorized users from using the source MAC address of attack packets and intercepting data of authorized users.

Prerequisites

A VXLAN tunnel has been configured successfully.

Precautions

The network administrator must be familiar with MAC addresses of devices that need to use static MAC address entries for communication on a network; otherwise, communication of authorized users will be interrupted.

Example

Configure a static MAC address entry with the destination MAC address of 0004-0003-0004 for a VXLAN tunnel.

```
<Huawei> system-view
[Huawei] bridge-domain 20
[Huawei-bd20] vxlan vni 5000
[Huawei-bd20] quit
[Huawei] interface nve 1
[Huawei-Nve1] source 1.1.1.1
[Huawei-Nve1] vni 5000 head-end peer-list 2.2.2.2
[Huawei-Nve1] quit
[Huawei] mac-address static 0004-0003-0004 bridge-domain 20 source 1.1.1.1 peer 2.2.2.2 vni 5000
```

12.14.21 source (NVE interface view)

Function

The **source** command configures an IP address for a source VXLAN Tunnel Endpoint (VTEP).

The **undo source** command deletes the IP address of the source VTEP.

By default, no IP address is configured for a source VTEP.

Format

source *ip-address*

undo source [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the IPv4 address of a source VTEP.	The value is in dotted decimal notation.

Views

NVE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VXLAN needs to be deployed on a downlink interface to provide access services and an uplink interface to establish a VXLAN tunnel.

To establish a VXLAN tunnel, configure IP addresses for the source and destination VTEPs.

To configure an IP address for a source VTEP, run this command. When access service packets reach a Network Virtualization Edge (NVE), the VTEP encapsulates the packets based on the IP addresses of source and destination VTEPs and forwards them.

Precautions

- You can specify the IP address of a physical interface or a loopback interface as the IP address of the source VTEP. The address of a loopback interface is recommended.
- Generally, the NVE interfaces of different devices must be configured with different VTEP addresses; otherwise, traffic forwarding errors may occur.
- The IP address of a VBDIF interface cannot be configured as the IP address of the source VTEP of a VXLAN tunnel.

Follow-up Procedure

Run the **vni head-end peer-list** command to configure an IP address for a destination VTEP.

Example

Set the IP address of the source VTEP to 10.1.1.2.

```
<Huawei> system-view
[Huawei] interface nve 1
[Huawei-Nve1] source 10.1.1.2
```

12.14.22 vni head-end peer-list

Function

The **vni head-end peer-list** command configures an ingress replication list that contains the IP addresses of those remote VTEPs for a VXLAN network identifier (VNI).

The **undo vni head-end peer-list** command deletes the ingress replication list of a VNI.

By default, no ingress replication list is configured for any VNI.

Format

vni *vni-id* **head-end peer-list** *ip-address* &<1-10>

undo vni *vni-id* [**head-end peer-list** *ip-address* &<1-10>]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.
ip-address	Specifies the IPv4 address of a remote VTEP.	The value is in dotted decimal notation.

Views

NVE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the ingress of a VXLAN tunnel receives broadcast, unknown unicast, and multicast (BUM) packets, it replicates these packets and sends a copy to each VTEP in the ingress replication list. The ingress replication list is a collection of remote VTEP IP addresses to which the ingress of a VXLAN tunnel should send replicated BUM packets.

If a source VTEP on a VXLAN connects to multiple remote VTEPs on the same VXLAN segment, run the **vni head-end peer-list** command to configure an ingress replication list that contains the IP addresses of those remote VTEPs. After the source NVE receives BUM packets, the local VTEP sends a copy of the BUM packets to every VTEP in the list.

Precautions

- You need to run the **vni head-end peer-list** command to configure the corresponding VTEP address even if the source VTEP matches only one destination VTEP.
- Run the **ping** command to check whether a reachable route exists between two ends of the tunnel. If there is a reachable route, the tunnel can be established and packets can be normally forwarded. If the two devices have a route to each other but the route is unreachable, the tunnel can still go Up but packets cannot be forwarded.

Example

Configure an ingress replication list for VNI 10, with the remote VTEPs' IP addresses being 10.1.1.1 and 10.1.1.3.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] vxlan vni 10
```

```
[Huawei-bd10] quit
[Huawei] interface nve 1
[Huawei-Nve1] vni 10 head-end peer-list 10.1.1.1 10.1.1.3
```

Related Topics

12.14.10 display vxlan peer

12.14.23 vxlan vni (BD view)

Function

The **vxlan vni** command associated a specified VNI with a BD.

The **undo vxlan vni** command restores the default settings.

By default, no VNI is associated with a BD.

Format

vxlan vni *vni-id*

undo vxlan vni *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 0 to 16777215.

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Similar to VLAN ID, VNI is used to distinguish VXLAN segments.

On the VXLAN network, one VXLAN segment is a large Layer 2 BD; therefore, VNI and BD have a one-to-one mapping relationship.

You can run this command to configure the mapping relationship between VNIs and BDs. In this way, the VTEP can forward received packets through a correct VXLAN tunnel based on the mapping between BDs and VNIs.

Example

Set the mapping between VNI 10 and BD 10.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] bridge-domain 10
[Huawei-bd10] vxlan vni 10
```

12.14.24 vxlan vni (VPN instance view)

Function

The **vxlan vni** command binds a VXLAN Network Identifier (VNI) to a Virtual Private Network (VPN) instance.

The **undo vxlan vni** command deletes the binding between the VNI and VPN instance.

By default, a VNI is not bound to any VPN instance.

Format

vxlan vni *vni-id*

undo vxlan vni *vni-id*

Parameters

Parameter	Description	Value
vni-id	Specifies a VNI ID.	The value is an integer that ranges from 1 to 16777215.

Views

VPN instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Generally, VPN is used to isolate Layer 3 routes.

On a network with distributed VXLAN gateways deployed, a Layer 2 VNI needs to be allocated for each subnet and a Layer 3 VNI needs to be allocated for each tenant (VPN instance) on a Layer 3 gateway to implement communication over the Layer 3 gateway. After a Layer 3 VNI is bound to a VPN instance, the remote Layer 3 gateway can identify VPN information based on the tenant's VNI ID in packets received from the VXLAN tunnel. In this way, tenants belonging to the same VPN can communicate, while tenants in different VPNs are isolated.

Precautions

Currently, one VNI can be bound to only one VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

The VNI bound to a VPN instance by running the **vxlan vni** command cannot be the same as the VNI configured in the BD.

Example

Bind VNI 50 to VPN instance **huawei**.

```
<Huawei> system-view
[Huawei] ip vpn-instance huawei
[Huawei-vpn-instance-huawei] vxlan vni 50
```

 Copyright © Huawei Technologies Co., Ltd.

13 WLAN-FAT AP Commands

About This Chapter

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW provide WLAN Fat AP functions.

AR109W, AR109GW-L, AR129CVW, AR129CGVW-L, AR169CVW, AR169CVW-4B4S do not support WAPI security policy.

13.1 WLAN Service Configuration Commands

13.2 WLAN QoS Configuration Commands

13.3 WLAN Security Configuration Commands

13.4 WLAN Radio Resource Management Configuration Commands

13.1 WLAN Service Configuration Commands

13.1.1 80211n a-mpdu enable (for FAT AP)

Function

The **80211n a-mpdu enable** command enables aggregation of MPDUs.

The **undo 80211n a-mpdu enable** command disables aggregation of MPDUs.

By default, aggregation of MPDUs is enabled.

Format

80211n a-mpdu enable

 Copyright © Huawei Technologies Co., Ltd.

undo 80211n a-mpdu enable

Parameters

None

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce cost, 802.11n uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Enable aggregation of MPDUs.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile id 1 name rp01
[Huawei-wlan-radio-prof-rp01] 80211n a-mpdu enable
```

Related Topics

13.1.56 radio-profile (WLAN view) (for FAT AP)

13.1.27 display radio-profile

13.1.2 80211n a-mpdu (for FAT AP)

Function

The **80211n a-mpdu** command sets the maximum length of an aggregated MPDU (A-MPDU). MPDU stands for MAC protocol data unit.

The **undo 80211n a-mpdu** command restores the maximum length of an A-MPDU to the default value.

By default, the index for the maximum length of an A-MPDU is 3. The maximum length of the A-MPDU is 65535 bytes.

Format

80211n a-mpdu max-length-exponent *length-capability-index*

undo 80211n a-mpdu max-length-exponent

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-length-exponent *length-capability-index*	Indicates the index for the maximum length of the A-MPDU.	The value is an integer that ranges from 0 to 3. ● 0: indicates that the maximum length of the A-MPDU is 8191 bytes. ● 1: indicates that the maximum length of the A-MPDU is 16383 bytes. ● 2: indicates that the maximum length of the A-MPDU is 32767 bytes. ● 3: indicates that the maximum length of the A-MPDU is 65535 bytes.

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11n uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Set the maximum length of an A-MPDU to 32767 bytes in radio profile rp01.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile id 1 name rp01
[Huawei-wlan-radio-prof-rp01] 80211n a-mpdu max-length-exponent 2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

13.1.56 radio-profile (WLAN view) (for FAT AP)
13.1.27 display radio-profile

13.1.3 80211bg basic-rate (for FAT AP)

Function

The **80211bg basic-rate** command configures a basic rate set of the 802.11bg protocol in the radio profile.

The **undo 80211bg basic-rate** command restores the default basic rate set of the 802.11bg protocol in the radio profile.

By default, the basic rate set of the 802.11bg protocol includes rates 1 Mbps and 2 Mbps in the radio profile.

Format

80211bg basic-rate [*80211bg-rate-value* &<1-12> | **all**]

undo 80211bg basic-rate

Parameters

Parameter	Description	Value
80211bg-rate-value	Specifies an 802.11bg basic rate set.	Enumerated type: • 1: 1 Mbps • 2: 2 Mbps • 5: 5.5 Mbps • 6: 6 Mbps • 9: 9 Mbps • 11: 11 Mbps • 12: 12 Mbps • 18: 18 Mbps • 24: 24 Mbps • 36: 36 Mbps • 48: 48 Mbps • 54: 54 Mbps
all	Supports all basic rates.	-

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The rates specified in the basic rate set must be supported by both the AP and STA; otherwise, the STA cannot associate with the AP. For example, if you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command to configure a basic rate set in the radio profile, bind the radio profile to the AP's 2.4 GHz radio. If a STA associates with the AP in 802.11bg mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

Configuration Precautions

This configuration applies only to STAs associated with an AP in 802.11bg mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

If no parameter is specified in the command, the basic rate set contains no rate settings.

Example

Configure the 802.11bg basic rate set to contain rates 6 Mbps and 9 Mbps in the radio profile.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name radiopf
[Huawei-wlan-radio-prof-radiopf] 80211bg basic-rate 6 9
```

Related Topics

13.1.4 80211bg supported-rate (for FAT AP)

13.1.4 80211bg supported-rate (for FAT AP)

Function

The **80211bg supported-rate** command configures a supported rate set of the 802.11bg protocol in the radio profile.

The **undo 80211bg supported-rate** command restores the default supported rate set of the 802.11bg protocol in the radio profile.

By default, the supported rate set of the 802.11bg protocol in the radio profile includes rates 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.

 Copyright © Huawei Technologies Co., Ltd.

Format

80211bg supported-rate [*80211bg-rate-value* &<1-12> | **all**]

undo 80211bg supported-rate

Parameters

Parameter	Description	Value
80211bg-rate-value	Specifies an 802.11bg supported rate set.	Enumerated type: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all rates.	-

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP except the basic rates. The AP and STA can transmit data at all rates specified by the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP,

 Copyright © Huawei Technologies Co., Ltd.

the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command to configure a supported rate set in the radio profile, bind the radio profile to the AP's 2.4 GHz radio. If a STA associates with the AP in 802.11bg mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

Configuration Precautions

This configuration applies only to STAs associated with an AP in 802.11bg mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

If no parameter is specified in the command, the supported rate set contains no rate settings.

Example

Configure the 802.11bg supported rate set to contain rates 6 Mbps and 9 Mbps in the radio profile.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name radiopf
[Huawei-wlan-radio-prof-radiopf] 80211bg supported-rate 6 9
```

Related Topics

13.1.3 80211bg basic-rate (for FAT AP)

13.1.5 ap-manufacturer-config (for FAT AP)

Function

The **ap-manufacturer-config** command restores the factory settings of APs.

NOTE

Only the AR1220W, AR1220EVW and AR1220VW support this command.

Format

ap-manufacturer-config

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When a configuration error occurs on the AP, you can run this command to clear AP configurations.

NOTICE

After restoring factory settings, the AP is reset and configurations are restored to factory settings.

Example

Restore the factory settings of the AP.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] ap-manufacturer-config
```

13.1.6 ap-reset (for FAT AP)

Function

The **ap-reset** command resets an AP.

NOTE

Only the AR1220W, AR1220EVW and AR1220VW support this command.

Format

ap-reset

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After the command is run, the AP restarts and the latest configuration file saved on the router takes effect for the AP after startup.

Example

Reset the AP.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] ap-reset
```

13.1.7 ap-sysname (for FAT AP)

Function

The **ap-sysname** command changes the system name of an AP.

The **undo ap-sysname** command restores the default system name of an AP.

By default, the system name of an AP is ap-*ap-id*.

NOTE

Only the AR1220W, AR1220EVW and AR1220VW support this command.

Format

ap-sysname *ap-sysname*

undo ap-sysname

Parameters

Parameter	Description	Value
ap-sysname	Specifies the system name of an AP.	The value is a string of 1 to 31 characters. The value cannot contain question marks (?) or spaces and cannot start or end with double quotation marks (" ").

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap-sysname** command to change the AP system name or restore the default name.

 Copyright © Huawei Technologies Co., Ltd.

Example

Change the system name of AP to **ap_01**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] ap-sysname ap_01
```

Related Topics

13.1.17 display ap (for FAT AP)

13.1.8 ap-threshold

Function

Using the **ap-threshold** command, you can set the alarm thresholds of the memory usage, and temperature for an AP.

Using the **undo ap-threshold** command, you can restore the default alarm thresholds of the memory usage, and temperature for an AP.

By default, the memory usage alarm threshold is 90%; the lower temperature alarm threshold is 1°C; the upper temperature alarm threshold is 80°C.

NOTE

Only the AR1220W, AR1220EVW and AR1220VW support this command.

Format

ap-threshold memory-usage *threshold-value*

ap-threshold temperature *high-value* [*low-value*]

undo ap-threshold { **memory-usage** | **temperature** }

Parameters

Parameter	Description	Value
memory-usage *threshold-value*	Specifies the memory usage alarm threshold.	The value is an integer ranging from 1 to 100, in percentage (%). The default value is 90.
temperature *high-value*	Specifies the upper temperature alarm threshold.	The value is an integer ranging from 1 to 100, in °C. The default value is 80.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
temperature *low-value*	Specifies the lower temperature alarm threshold.	The value is an integer ranging from 1 to 100, in °C. The default value is 1.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can set the alarm thresholds of memory usage, and temperature for an AP as required. When the memory usage, or temperature exceeds the alarm threshold, the AP generates an alarm. The AP saves alarm messages in logs to record the AP status. To view the logs, run the **display trapbuffer** command.

Example

Set the memory usage alarm threshold to 70%.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] ap-threshold memory-usage 70
```

Related Topics

13.1.21 display ap-threshold

13.1.9 association-timeout (for FAT AP)

Function

The **association-timeout** command configures an association aging time for STAs.

The **undo association-timeout** command restores the default association aging time.

By default, the association aging time is 5 minutes.

Format

association-timeout *association-timeout*

undo association-timeout

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
association-timeout	Specifies the association aging time of STAs.	The value is an integer that ranges from 1 to 30, in minutes.

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

The administrator can run the **association-timeout** command to set the association aging time for STAs. If the AP receives no data packet from a STA in a specified time, the STA goes offline after the association aging time expires.

Example

Create a service set named **ChinaNet** and set the association aging time of STAs to 15 minutes.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] association-timeout 15
```

13.1.10 auto-off service radio

Function

The **auto-off service radio** command disables radios as scheduled.

The **undo auto-off service radio** command cancels the setting.

By default, radios are not disabled as scheduled.

Format

auto-off service radio interface *wlan-radio* **start-time** *start-time* **end-time** *end-time*

undo auto-off service radio interface *wlan-radio*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *wlan-radio*	Specifies a wlan-radio interface.	-
start-time *start-time*	Specifies the time when a radio starts to be disabled.	The time is in hh:mm:ss format. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59.
end-time *end-time*	Specifies the time when a radio stops being disabled.	The time is in hh:mm:ss format. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

At midnight when the user service traffic volume is low, you can run this command to disable radios on specified APs, reducing power consumption.

Configuration Precautions

- The **auto-off service radio** command takes effect only when radios have been enabled using the **13.1.54 radio enable (for FAT AP)** command. If radios are disabled using the **undo 13.1.54 radio enable (for FAT AP)** command, the **auto-off service radio** command does not take effect.
- If a radio is enabled using the **13.1.54 radio enable (for FAT AP)** command, you can run the **auto-off service radio** command to configure the radio to be automatically disabled as scheduled. In the scheduled time, the radio is

disabled and cannot be enabled using the **13.1.54 radio enable (for FAT AP)** command. To enable the radio, run the **undo auto-off service radio** command.

- The start time must be 60 seconds earlier than the end time.
- If the **auto-off** command is configured on a radio interface, you cannot configure the status (enabled or disabled) of the radio on the interface using a MIB.
- This function does not allow for the configuration of multiple time ranges. If the command is executed for multiple times, only the latest time range configuration takes effect.

Example

Configure radio 0 on AP to be disabled from 01:00:00 to 07:00:00.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] auto-off service radio interface wlan-radio0/0/0 start-time 1:00:00 end-time
7:00:00
```

Related Topics

13.1.28 display radio status (for FAT AP)

13.1.11 available-antenna-number (for Fat AP)

Function

The **available-antenna-number** command sets the number of available antennas on a radio.

The **undo available-antenna-number** command restores the default number of available antennas on a radio.

By default, all antennas on a radio are available.

Format

available-antenna-number { **all** | *available-antenna-number* }

undo available-antenna-number

Parameters

Parameter	Description	Value
all	Indicates that all antennas are available.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
available-antenna-number	Specifies the number of available antennas.	The value is an integer. The value range varies according to the AP type. Antennas here refer to the antennas that can receive and send signals. For the number of antennas supported by a device, see "MIMO mode (Tx x Rx)" in the *Huawei AR Series Access Routers Get to Know the Product-Hardware Description-Chassis-Interface Description-Wi-Fi Antenna Interface*.

Views

WLAN-radio interface view

Default Level

2: Configuration level

Usage Guidelines

- The value of available antennas must be less than or equal to the number of antennas on a radio.
- You can run this command to shut down excess antennas to save power.

Example

Set the number of available antennas on a radio to 1.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] available-antenna-number 1
```

13.1.12 beacon-interval (for FAT AP)

Function

The **beacon-interval** command sets the interval for sending Beacon frames.

The **undo beacon-interval** restores the default interval for sending Beacon frames.

By default, the interval for sending Beacon frames is 100 ms.

Format

beacon-interval *beacon-interval*

undo beacon-interval

Parameters

Parameter	Description	Value
beacon-interval	Specifies the interval for sending Beacon frames.	The value is an integer that ranges from 20 to 1000, in ms.

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

An AP broadcasts Beacon frames at intervals to notify STAs of an existing 802.11 network. After receiving a Beacon frame, a STA can modify parameters used to connect to the 802.11 network.

A long interval for sending Beacon frames lengthens the dormancy time of STAs, while a short interval for sending Beacon frames increases air interface costs. Therefore, you are advised to set the interval for sending Beacon frames for an AP based on the VAP quantity. The following intervals for sending Beacon frames are recommended for APs with different VAP quantities on a single radio:

- No more than 4 VAPs: about 100 ms
- 5 to 8 VAPs: about 200 ms
- 9 to 12 VAPs: about 300 ms
- 13 to 16 VAPs: about 400 ms

Example

Set the interval for sending Beacon frames to 200 ms in the radio profile named **802.11b**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name 80211b
[Huawei-wlan-radio-prof-80211b] beacon-interval 200
```

13.1.13 channel (for FAT AP)

Function

The **channel** command configures a channel for a radio.

The **undo channel** command restores the default channel of a radio.

The default working channel of a radio is selected based on the country code and radio frequency band.

- The radio frequency band varies according to AP models.
- The default working channel of each AP radio varies according to different country codes.

You can run the **13.1.16 display actual channel-power (for FAT AP)** command to check the channel in use on a radio.

Format

channel { **20mhz** | **40mhz-minus** | **40mhz-plus** | **80mhz** } *channel*

undo channel { **20mhz** | **40mhz-minus** | **40mhz-plus** | **80mhz** }

Parameters

Parameter	Description	Value
20mhz	Indicates that the channel bandwidth is 20 MHz.	-
40mhz-minus	Indicates that the channel bandwidth is 40 MHz Minus.	-
40mhz-plus	Indicates that the channel bandwidth is 40 MHz Plus.	-
80mhz	Indicates that the channel bandwidth is 80 MHz. **NOTE** Only the 5 GHz radio of the AR129CVW, AR129CGVW-L, AR169CVW-4B4S, AR169CVW, AR169EGW-L, AR169EW, AR161EW, AR161EW-M1, AR169W-P-M9 and AR169RW-P-M9 supports this parameter.	-
channel	Specifies the working channel for a radio. The channel is selected based on the country code and radio mode.	The parameter is an enumeration value. The value range is determined according to the country code and radio mode.

 Copyright © Huawei Technologies Co., Ltd.

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different radios use different channels. Channels for radios also vary in different countries and regions. Select channels based on the actual situations.

NOTE

- The configured channel IDs must match the radio frequency band. For details about mappings between channel IDs and frequency bands, see Country codes & Channels compliance status.
- The 2.4 GHz radio does not support the 40 MHz Minus and 40 MHz Plus bandwidth in FCC compliance regions (including America).
- The channels you configure must be supported by the terminals; otherwise, the terminals cannot discover wireless signals. For example, when the country code is set to China, 5 GHz channels 36, 40, 44, 48, 52, 56, 60, and 64 can be configured. However, most terminals do not support these channels currently. If these channels are configured, the terminals cannot discover wireless signals. In this case, you can configure 5 GHz channels 149, 153, 157, 161, and 165, which are supported by the terminals.
- If an AP detects radar signals on a channel, the channel cannot be configured as the radio channel of the AP in 30 minutes.

Prerequisites

The channel mode has been set to fixed using the **channel-mode fixed** command.

Example

Configure the channel for radio of interface 0/0/0 as 6.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] channel 20mhz 6
```

Configure the channel for radio of interface 0/0/1 as 40.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/1
[Huawei-Wlan-Radio0/0/1] channel 80mhz 40
```

13.1.14 channel-mode (for FAT AP)

Function

The **channel-mode** command sets the channel mode in a radio profile.

The **undo channel-mode** command restores the default channel mode in a radio profile.

By default, the channel of a radio can be automatically adjusted.

Format

channel-mode { **auto** | **fixed** }

undo channel-mode

Parameters

Parameter	Description	Value
auto	Indicates the automatic mode, in which the channels of radios bound to the radio profile can be automatically adjusted.	-
fixed	Indicates the fixed mode, in which radios bound to the radio profile use fixed channels.	-

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

Two channel working modes are available:

- Automatic mode: Channels are automatically selected to adapt to the radio environment.
- Fixed mode: Channels must be manually specified for radios.

The automatic mode is recommended because you do not need to specify a channel for each radio. The fixed mode provides an alternative way. You can use this mode if you want to avoid frequent channel adjustment, which may cause intermittent service interruption.

If an AP needs radio calibration, the channel mode must be set to automatic mode in the AP's radio profile.

Example

Set the channel mode in radio profile 802.11b to automatic mode.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name 80211b
[Huawei-wlan-radio-prof-80211b] channel-mode auto
```

 Copyright © Huawei Technologies Co., Ltd.

13.1.15 conflict-rate-threshold (for FAT AP)

Function

The **conflict-rate-threshold** command sets the collision rate threshold in a radio profile.

The **undo conflict-rate-threshold** command restores the default collision rate threshold in a radio profile.

By default, the collision rate threshold is 60.

Format

conflict-rate-threshold *conflict-rate-threshold*

undo conflict-rate-threshold

Parameters

Parameter	Description	Value
conflict-rate-threshold	Specifies the collision rate threshold.	The value is an integer that ranges from 20 to 80, in percentage (%).

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

If the MAC layer of a radio does not receive any ACK packet after sending a packet at the lowest rate, a collision occurs.

The collision rate threshold and the packet loss ratio threshold determine whether the radio environment is good. When the collision rate or packet loss ratio of a radio reaches the threshold, the system considers that the radio environment deteriorates. When this occurs, the system may start radio calibration or take measures to avoid signal interference.

Example

Set the collision rate threshold to 70% in radio profile 802.11b.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name 80211b
[Huawei-wlan-radio-prof-80211b] conflict-rate-threshold 70
```

13.1.16 display actual channel-power (for FAT AP)

Function

The **display actual channel-power** command displays the channel and power of a radio.

Format

display actual channel-power interface wlan-radio *wlan-radio-number*

Parameters

Parameter	Description	Value
interface wlan-radio *wlan-radio-number*	Specifies the WLAN radio interface. **NOTE** You do not need to enter a space between **wlan-radio** and *wlan-radio-number*.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view the channel used by a radio and power of the radio, run this command.

The power in the command output is the sum of the maximum transmit power of the radio interface and the antenna gain. If MIMO is supported, the MIMO gain should also be added. The maximum power displayed should comply with laws and regulations corresponding to the country code.

Example

Display the current channel and power.

```
<Huawei> display actual channel-power interface wlan-radio0/0/0
 -------------------------------------------------------
  RADIO  CHANNEL POWER-LEVEL POWER(dBm) CHANNEL-BANDWIDTH
 -------------------------------------------------------
  0/0    1       0           20      20MHz
 -------------------------------------------------------
```

Table 13-1 Description of the display actual channel-power command output

Item	Description
RADIO	Radio identified by the AP ID and radio ID.

Item	Description
CHANNEL	Current channel of a radio.
POWER-LEVEL	Current transmit power level of a radio.
POWER(dBm)	Current transmit power of the radio, in dBm, which is determined by the power level.
CHANNEL-BANDWIDTH	Channel bandwidth.

13.1.17 display ap (for FAT AP)

Function

The **display ap** command displays AP information.

Format

display ap

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about APs, run this command.

Example

Display information about an AP.

```
<Huawei> display ap
  AP detail information:
  ------------------------------------------------------------------------------
  AP type: AR169W
  State: normal
  AP performance-statistic cycle: 15 minutes
  AP access priority mode: Priority Access 5GHz Radio
  Dynamic-blacklist : disable
  Dynamic-blacklist aging-duration(s) : 600
  Attack detection flood interval(s) : 60
  Attack detection flood times : 300
  Attack detection psk interval(s) : 60
  Attack detection psk times : 20
  Flood attack detection quiet time(s)   : 600
```

```
Psk attack detection quiet time(s)     : 600
Weak iv attack detection quiet time(s) : 600
Spoof attack detection quiet time(s)   : 600
Maximum station number: 128
-----------------------------------------------------------------------------
```

Table 13-2 Description of the **display ap** command output

Item	Description
AP Type	Type of an AP.
State	Status of an AP. ● normal: The AP is in normal state. ● committing: The WLAN service configuration is being committed. ● commit-failed: The WLAN service configuration fails to be committed.
AP performance-statistic cycle	Interval at which performance statistics on an AP are collected, in minutes.
AP access priority mode	Access mode of a STA. ● normal: Users select the SSID configured on a 2.4 GHz radio to access the AP. ● 5g: Users select the SSID configured on a 5 GHz radio to access the AP.
Dynamic-blacklist	Status of the dynamic blacklist.
Dynamic-blacklist aging-duration(s)	Aging time of the dynamic blacklist.
Attack detection flood interval(s)	Interval for flood attack detection.
Attack detection flood times	Upper threshold for the number of packets of the same type received by an AP at an interval.
Attack detection psk interval(s)	Interval for PSK attack detection.
Attack detection psk times	Upper threshold for the number of failed authentications at an interval.
Maximum station number	Maximum number of STAs supported by the AP.

Related Topics

13.1.7 ap-sysname (for FAT AP)

13.1.18 display ap configurable channel (for FAT AP)

Function

The **display ap configurable channel** command displays the configurable channels supported by the AP.

Format

display ap configurable channel

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Different countries or regions use different wireless channels and powers. Setting country and area codes can specify channels that can be used on WLANs of different countries. The **display ap configurable channel** command displays the configurable channels supported by a AP.

Example

Display the configurable channels supported by the AP.

Table 13-3 Description of the **display ap configurable channel** command output

Item	Description
2.4G 20M	Channels configurable on an AP when the AP works on the 2.4 GHz frequency band in 802.11b/g/n mode. These channels work at a bandwidth of 20 MHz.
2.4G 40M+	Channels configurable on an AP when the AP works on the 2.4 GHz frequency band in 802.11n mode. These channels work at a bandwidth of 40 MHz.
2.4G 40M-	Channels configurable on an AP when the AP works on the 2.4 GHz frequency band in 802.11n mode. These channels work at a bandwidth of 40 MHz.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
5G 20M	Channels configurable on an AP when the AP works on the 5 GHz frequency band in 802.11g/n mode. These channels work at a bandwidth of 20 MHz.
5G 40M+	Channels configurable on an AP when the AP works on the 5 GHz frequency band in 802.11n mode. These channels work at a bandwidth of 40 MHz.
5G 40M-	Channels configurable on an AP when the AP works on the 5 GHz frequency band in 802.11n mode. These channels work at a bandwidth of 40 MHz.

Related Topics

13.1.77 wlan global country-code

13.1.19 display ap-performance-statistic (for FAT AP)

Function

The **display ap-performance-statistic** command displays performance statistics on an AP to monitor AP performance.

NOTE

Only the AR1220W, AR1220EVW and AR1220VW support this command.

Format

display ap-performance-statistic

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ap-performance-statistic** command displays the following information: performance statistics items, memory usage, CPU usage, available space in the flash memory, temperature, number of online users.

Example

Display performance statistics on the AP.

```
<Huawei> display ap-performance-statistic
 AP performance statistic information:
 ---------------------------------------------------------------------------
 Memory use rate: 78 %
 CPU use rate: 7 %
 Flash free size: 19296 KB
 Temperature: 47 °C
 Online user number: 0
 ---------------------------------------------------------------------------
```

Table 13-4 Description of the **display ap-performance-statistic** command output

Item	Description
Memory use rate	Memory usage (%).
CPU use rate	CPU usage (%).
Flash free size	Available space in the flash memory, in KB.
Temperature	Operating temperature.
Online user number	Number of online users.

13.1.20 display ap-run-info (for FAT AP)

Function

The **display ap-run-info** command displays the running status of an AP. You can run this command to monitor an AP in real time.

NOTE

Only the AR1220W, AR1220EVW and AR1220VW support this command.

Format

display ap-run-info

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to monitor an AP in real time.

Prerequisites

The AP works properly.

Example

Display the running status of the AP.

```
<Huawei> display ap-run-info
  AP run information:
  ------------------------------------------------------------------------------
  Software version: V200R003C00
  Hardware version: R0A
  Country code: CN
  CPU type: CN5010
  CPU frequency: 300 MHZ
  Memory type: HY5PS1G1631CFP-Y5
  Memory size: 128 MB
  Flash size: 48 MB
  Run time: 160354 S
  ------------------------------------------------------------------------------
```

Table 13-5 Description of the display ap-run-info command output

Item	Description
Software version	Software version that the AP is running.
Hardware version	Hardware version of the AP.
CPU type	CPU type of the AP.
CPU frequency	CPU frequency of the AP.
Memory type	Memory type of the AP.
Country code	Region where the AP is located.
Memory size	Size of the memory.
Flash size	Size of the flash memory.
Run time	How long the AP has been running, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

13.1.21 display ap-threshold

Function

Using the **display ap-threshold** command, you can view the alarm thresholds of the memory usage, and temperature on an AP.

NOTE

Only the AR1220W, AR1220EVW and AR1220VW support this command.

Format

display ap-threshold [**memory-usage** | **temperature**]

Parameters

Parameter	Description	Value
memory-usage	Displays the memory usage alarm threshold.	-
temperature	Displays the temperature alarm threshold.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ap-threshold** command shows the alarm thresholds of the memory usage, and temperature on an AP. You can specify a keyword to view the specified alarm threshold or view all alarm thresholds at one time. If none of alarm thresholds is configured, this command displays the default alarm thresholds.

Example

Display the memory usage alarm threshold of the AP.

```
<Huawei> display ap-threshold
 AP threshold memory-usage     : 90 %
 AP threshold temperature high : 80 C
 AP threshold temperature low  : 1 C
```

 Copyright © Huawei Technologies Co., Ltd.

Table 13-6 Description of the display ap-threshold command output

Item	Description
AP threshold memory-usage	Memory usage alarm threshold of the AP. When the AP memory usage exceeds the threshold, an alarm is generated.
AP threshold temperature high	Temperature alarm upper threshold of the AP. When the AP temperature exceeds the upper threshold, an alarm is generated.
AP threshold temperature low	Temperature alarm lower threshold of the AP. When the AP temperature exceeds the lower threshold, an alarm is generated.

Related Topics

13.1.8 ap-threshold

13.1.22 display ap around-ssid-list (for FAT AP)

Function

The **display ap around-ssid-list** command displays SSIDs of neighbors of a specified AP.

Format

display ap around-ssid-list

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view SSIDs of neighbors of a specified AP.

Example

Display SSIDs of neighbors of AP.

```
<Huawei> display ap around-ssid-list
 Own AP(2.4G):
 ---------------------------------------------------
  SSID
 ---------------------------------------------------
  huawei
 ---------------------------------------------------
  Total: 1

 Uncontrol AP(2.4G):
 ---------------------------------------------------
  SSID
 ---------------------------------------------------
  huawei1
  company
 ---------------------------------------------------
  Total: 2
```

Table 13-7 Description of the display ap around-ssid-list command output

Item	Description
Own AP(2.4G)	SSIDs of authorized neighbors.
Uncontrol AP(2.4G)	SSIDs of unauthorized neighbors.

13.1.23 display binding radio-profile (for FAT AP)

Function

The **display binding radio-profile** command displays radios to which a specified radio profile is bound.

Format

display binding radio-profile { **id** *profile-id* | **name** *profile-name* }

Parameters

Parameter	Description	Value
id *profile-id*	Specifies the radio profile ID.	The radio profile ID must exist.
name *profile-name*	Specifies the name of a radio profile.	The radio profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the radios to which a specified radio profile is bound.

Prerequisites

When using this command, ensure that the specified radio profile exists.

Example

Display the radios to which radio profile 0 is bound.

```
<Huawei> display binding radio-profile id 0
 ---------------------------------------------------
  AP  RADIO
 ---------------------------------------------------
  0    0
 ---------------------------------------------------
  Total: 1
```

Table 13-8 Description of the display binding radio-profile command output

Item	Description
AP	ID of an AP.
RADIO	Radio ID.

13.1.24 display channel country-code (for FAT AP)

Function

The **display channel country-code** command displays 2.4 GHz and 5 GHz channels corresponding to a specified country code.

Format

display channel country-code *country-code*

Parameters

Parameter	Description	Value
country-code	Specifies the AP country code.	The value is a string of characters. For specific values, see **Table 13-9**.

 Copyright © Huawei Technologies Co., Ltd.

Table 13-9 Country codes supported by APs

Country Code	Country/Region
AE	UNITED ARAB EMIRATES
AM	ARMENIA
AR	ARGENTINA
AT	AUSTRIA
AU	AUSTRALIA
AZ	AZERBAIJAN
BE	BELGIUM
BG	BULGARIA
BH	BAHRAIN
BN	BRUNEI DARUSSALAM
BO	BOLIVIA
BR	BRAZIL
BY	BELARUS
BZ	BELIZE
CA	CANADA
CH	SWITZERLAND
CL	CHILE
CN	CHINA (Default)
CO	COLOMBIA
CR	COSTA RICA
CY	CYPRUS
CZ	CZECH REPUBLIC
DE	GERMANY
DK	DENMARK
DO	DOMINICAN REPUBLIC
EC	ECUADOR
EE	ESTONIA
EG	EGYPT
ES	SPAIN

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
FI	FINLAND
FR	FRANCE
GB	UNITED KINGDOM
GE	GEORGIA
GR	GREECE
GT	GUATEMALA
HK	HONG KONG, SPECIAL ADMINISTRATIVE REGION OF CHINA
HN	HONDURAS
HR	CROATIA
HU	HUNGARY
ID	INDONESIA
IE	IRELAND
IL	ISRAEL
IN	INDIA
IQ	IRAQ
IR	IRAN
IS	ICELAND
IT	ITALY
JO	JORDAN
JP	JAPAN
KP	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA
KR	REPUBLIC OF KOREA
KW	KUWAIT
KZ	KAZAKHSTAN
LB	LEBANON
LI	LIECHTENSTEIN
LK	SRI LANKA
LT	LITHUANIA
LU	LUXEMBOURG

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
LV	LATVIA
MA	MOROCCO
MC	MONACO
MK	MACEDONIA
MO	MACAU, SPECIAL ADMINISTRATIVE REGION OF CHINA
MT	MALTA
MX	MEXICO
MY	MALAYSIA
NG	NIGERIA
NL	NETHERLANDS
NO	NORWAY
NZ	NEW ZEALAND
OM	OMAN
PA	PANAMA
PE	PERU
PH	PHILIPPINES
PK	PAKISTAN
PL	POLAND
PR	PUERTO RICO
PT	PORTUGAL
QA	QATAR
RO	ROMANIA
RU	RUSSIA
SA	SAUDI ARABIA
SE	SWEDEN
SG	SINGAPORE
SI	SLOVENIA
SK	SLOVAKIA
SV	EL SALVADOR
SY	SYRIA

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
TH	THAILAND
TN	TUNISIA
TR	TURKEY
TT	TRINIDAD & TOBAGO
TW	TAIWAN, PROVINCE OF CHINA
UA	UKRAINE
US	UNITED STATES
UY	URUGUAY
UZ	UZBEKISTAN
VE	VENEZUELA
VN	VIET NAM
YE	YEMEN
ZA	SOUTH AFRICA
ZW	ZIMBABWE

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display channel country-code** command to view 2.4 GHz and 5 GHz channels corresponding to a specified country code.

Example

Display 2.4 GHz and 5 GHz channels corresponding to the country code **CN**.

```
<Huawei> display channel country-code CN
  2.4G 20M : 1,2,3,4,5,6,7,8,9,10,11,12,13.
  2.4G 40M+: 1,2,3,4,5,6,7.
  2.4G 40M-: 5,6,7,8,9,10,11.
  5G   20M : 36,40,44,48,52,56,60,64,149,153,157,161,165.
  5G   40M+: 36,44,52,60,149,157.
  5G   40M-: 40,48,56,64,153,161.
  5G   80M : 36,40,44,48,52,56,60,64,149,153,157,161.
```

 Copyright © Huawei Technologies Co., Ltd.

Table 13-10 Description of the **display channel country-code** command output

Parameter	Description
2.4G 20M : 1,2,3,4,5,6,7,8,9,10,11,12,13 **NOTE** Description is only provided for the first line of the command output. The description about the rest lines is similar.	**2.4G** indicates the frequency band of a radio; **20M** indicates the channel bandwidth; **1,2,3,4,5,6,7,8,9,10,11,12,13** are IDs of channels at the 2.4 GHz frequency band. See *Country Code & Channel Compliance Table* for the relationship between the channel IDs and frequency band.

13.1.25 display power-level (for FAT AP)

Function

The **display power-level** command displays the radio power level and corresponding power.

Format

display power-level interface *wlan-radio*

Parameters

Parameter	Description	Value
interface *wlan-radio*	Specifies a wlan-radio interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display power-level** command displays the radio power level and corresponding power. The radio power level and corresponding power vary according to AP radios.

The power in the command output is the sum of the maximum transmit power of the radio interface and the antenna gain. If MIMO is supported, the MIMO gain

 Copyright © Huawei Technologies Co., Ltd.

should also be added. The maximum power displayed should comply with laws and regulations corresponding to the country code.

Example

Display the power level and corresponding power of radio0/0/0.

```
<Huawei> display power-level interface wlan-radio0/0/0
 power-level num: 20
 level 0: 20.00 dBm
 level 1: 19.00 dBm
 level 2: 18.00 dBm
 level 3: 17.00 dBm
 level 4: 16.00 dBm
 level 5: 15.00 dBm
 level 6: 14.00 dBm
 level 7: 13.00 dBm
 level 8: 12.00 dBm
 level 9: 11.00 dBm
 level 10: 10.00 dBm
 level 11: 9.00 dBm
 level 12: 8.00 dBm
 level 13: 7.00 dBm
 level 14: 6.00 dBm
 level 15: 5.00 dBm
 level 16: 5.00 dBm
 level 17: 5.00 dBm
 level 18: 5.00 dBm
 level 19: 5.00 dBm
```

NOTE

The displayed information is for reference only and varies according to the actual device.

Table 13-11 Description of the display power-level command output

Item	Description
power-level num	Radio power level.
level 0: 20.00 dBm	Power corresponding to power level 0.

13.1.26 display radio config (for FAT AP)

Function

The **display radio config** command displays the configuration of a radio.

Format

display radio config interface wlan-radio *wlan-radio-number*

Parameters

Parameter	Description	Value
interface wlan-radio *wlan-radio-number*	Specifies the WLAN radio interface. **NOTE** You do not need to enter a space between **interface wlan-radio** and *wlan-radio-number*.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the radio profile bound to a radio, and the radio parameters, administrative status, channel, and power specified in the radio profile.

Example

Display the current configuration of the 2.4 GHz radio.

```
<Huawei> display radio config interface wlan-radio0/0/0
  ---------------------------------------------------------------------
  Administrate status                    :enable
  Channel                          :1
  Channel bandwidth                      :20MHz
  Power level                        :0
  Power(dBm)                         :20
  Available antenna number               :all
  Attack Detect                      :-
  Radio frequency                    :2.4G
  Antenna gain(dbi)                  :2
  Profile ID                       :0
  Profile name                       :radiof
  Channel mode                       :auto
  Power mode                         :auto
  PER threshold(%)                   :30
  Conflict rate threshold(%)         :60
  RTS/CTS threshold(Byte)            :2347
  Support short preamble             :support
  DTIM interval (Beacon interval numbers):1
  Beacon interval(ms)                :100
  WMM profile ID                     :0
  WMM profile name                   :wmmf
  RTS/CTS mode                       :CTS-TO-SELF
  Guard interval mode                :normal
  802.11n A-MPDU length limit        :3
  Legacy station access              :enable
  80211bg basic rate                 :1 2
  80211bg support rate               :1 2 5 6 9 11 12 18 24 36 48 54
  80211a basic rate                  :6 12 24
  80211a support rate                :6 9 12 18 24 36 48 54
  Multicast rate 2g                  :11
```

```
Multicast rate 5g                    :6
-----------------------------------------------------------------------
```

Display the current configuration of the 5 GHz radio.

```
<Huawei> display radio config interface wlan-radio0/0/1
-----------------------------------------------------------------------
Administrate status                  :enable
Channel                              :149
Channel bandwidth                    :20MHz
Power level                          :0
Power(dBm)                           :20
Available antenna number             :all
Attack Detect                        :-
Radio frequency                      :5G
Antenna gain(dbi)                    :3
Profile ID                           :0
Profile name                         :radiof
Channel mode                         :auto
Power mode                           :auto
PER threshold(%)                     :30
Conflict rate threshold(%)           :60
RTS/CTS threshold(Byte)              :2347
Support short preamble               :support
DTIM interval (Beacon interval numbers):1
Beacon interval(ms)                  :100
WMM profile ID                       :0
WMM profile name                     :wmmf
RTS/CTS mode                         :CTS-TO-SELF
Guard interval mode                  :normal
802.11n A-MPDU length limit          :3
802.11ac A-MPDU length limit         :7
Legacy station access                :enable
80211bg basic rate                   :1 2
80211bg support rate                 :1 2 5 6 9 11 12 18 24 36 48 54
80211a basic rate                    :6 12 24
80211a support rate                  :6 9 12 18 24 36 48 54
80211ac mcs                          :9 9 9
Multicast rate 2g                    :11
Multicast rate 5g                    :6
A-MSDU send switch                   :disable
A-MSDU send max-subframes            :2
-----------------------------------------------------------------------
```

NOTE

The preceding command output is an example when a radio profile is bound to the radio interface. The command output varies according to the frequency band supported by the device.

Table 13-12 Description of the display radio config command output

Item	Description
Administrate status	Administrative status of the radio.
Channel	Channel used by the radio.
Channel bandwidth	Bandwidth of a channel.
Power level	Power level of the radio.
Power(dBm)	Power of the radio, in dBm.
Available antenna number	Number of available antennas.

Item	Description
Attack Detect	Attack detection mode.
Radio frequency	Frequency of the radio.
Antenna gain(dbi)	Antenna gain, in dBi.
Profile ID	ID of the radio profile bound to the radio.
Profile name	Name of the radio profile bound to the radio.
Channel mode	Channel mode of the radio.
Power mode	Whether the power of the radio is adjusted automatically.
PER threshold(%)	Packet error rate threshold of the radio, in percentage (%).
Conflict rate threshold(%)	Collision rate threshold of the radio, in percentage (%).
RTS/CTS threshold(Byte)	Request To Send/Clear To Send (RTS/CTS) threshold of the radio, in bytes.
Support short preamble	Whether the radio supports the short preamble.
DTIM interval (Beacon interval numbers)	Delivery traffic indication message (DTIM) interval, which is the number of Beacon intervals.
Beacon interval (ms)	Unit of the Beacon interval.
WMM profile ID	ID of the Wi-Fi Multimedia (WMM) profile applied to the radio.
WMM profile name	Name of the WMM profile.
RTS/CTS mode	RTS/CTS working mode.
Guard interval mode	Guard interval (GI) mode
802.11n A-MPDU length limit	The maximum length of an aggregated MPDU
802.11ac A-MPDU length limit	Maximum length of an 802.11ac A-MPDU. This parameter is displayed only for the 5 GHz frequency band.
Legacy station access	Whether to permit access of legacy terminals. To set this parameter, run the **13.1.48 legacy-station enable (for FAT AP)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
80211bg basic rate	80211bg basic rate set. To set this parameter, run the **13.1.3 80211bg basic-rate (for FAT AP)** command.
80211bg support rate	802.11bg supported rate set. To set this parameter, run the **13.1.4 80211bg supported-rate (for FAT AP)** command.
80211a basic rate	802.11a basic rate set.
80211a support rate	802.11a supported rate set.
80211ac mcs	802.11ac MCS. This parameter is displayed only for the 5 GHz frequency band.
Multicast rate 2g	Multicast rate of wireless packets on the 2.4 GHz radio. To set this parameter, run the **multicast-rate 2g** command.
Multicast rate 5g	Multicast rate of wireless packets on the 5 GHz radio. To set this parameter, run the **multicast-rate 5g** command.
A-MSDU send switch	Whether to enable the function of sending 802.11 packets in A-MSDU mode. This parameter is displayed only for the 5 GHz frequency band.
A-MSDU send max-subframes	Maximum number of subframes that can be aggregated into an A-MSDU at one time. This parameter is displayed only for the 5 GHz frequency band.

13.1.27 display radio-profile

Function

The **display radio-profile** command displays the configuration of a radio profile.

Format

display radio-profile { **all** | **id** *profile-id* | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays configurations of all radio profiles.	-
id *profile-id*	Specifies the radio profile ID.	The radio profile ID must exist.
name *profile-name*	Specifies the radio profile name.	The radio profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the configuration of radio profile named **huawei**.

```
<Huawei> display radio-profile name huawei
-----------------------------------------------------------------------
  Profile ID                          :5
  Profile name                        :huawei
  Channel mode                        :auto
  Power mode                          :auto
  PER threshold(%)                    :30
  Conflict rate threshold(%)          :60
  RTS/CTS threshold(Byte)             :2347
  Fragmentation threshold(Byte)       :2346
  Support short preamble              :support
  DTIM interval (Beacon interval numbers):1
  Beacon interval(ms)                 :100
  WMM profile ID                      :0
  WMM profile name                    :wmmf
  RTS/CTS mode                        :CTS-TO-SELF
  802.11n guard interval mode         :normal
  802.11n A-MPDU length limit         :3
  Legacy station access               :enable
  80211bg basic rate                  :1 2
  80211bg support rate                :1 2 5 6 9 11 12 18 24 36 48 54
  Multicast rate 2g                   :11
  -----------------------------------------------------------------------
```

Display configurations of all radio profiles.

```
<Huawei> display radio-profile all
  ---------------------------------------------------
   ID     Name
  ---------------------------------------------------
   0      lw
```

```
 1     t
-----------------------------------------------------
 Total: 2
```

Table 13-13 Description of the display radio-profile command output

Item	Description
Profile ID	Profile ID.
Profile name	Profile name.
Channel mode	Channel mode.
Power mode	Power mode.
PER threshold(%)	Packet error rate threshold, in percentage (%).
Conflict rate threshold(%)	Collision rate threshold, in percentage (%).
RTS/CTS threshold(Byte)	Request To Send/Clear To Send (RTS/CTS) threshold.
Fragmentation threshold(Byte)	Packet fragmentation threshold. **NOTE** V200R007C00 does not support fragmentation threshold.
Support short preamble	Whether short preamble is supported.
DTIM interval (Beacon interval numbers)	DTIM interval.
Beacon interval(ms)	Interval for sending Beacon frames.
WMM profile ID	ID of the Wi-Fi Multimedia (WMM) profile bound to the radio profile.
WMM profile name	Name of the WMM profile bound to the radio profile.
RTS/CTS mode	RTS/CTS working mode.
802.11n guard interval mode	Guard-interval Mode.
802.11n A-MPDU length limit	Maximum length of an A-MPDU.
ID	Profile ID.
Name	Profile name.
Total	Number of profiles.
Legacy station access	Whether to permit access of legacy terminals. To set this parameter, run the **legacy-station enable** command.

Item	Description
80211bg basic rate	802.11bg basic rate set. To set this parameter, run the **80211bg basic-rate** command.
80211bg support rate	802.11bg supported rate set. To set this parameter, run the **80211bg supported-rate** command.
Multicast rate 2g	Multicast rate of wireless packets on the 2.4 GHz radio. To set this parameter, run the **multicast-rate 2g** command.

13.1.28 display radio status (for FAT AP)

Function

The **display radio status** command displays status of a specified AP radio.

Format

display radio status interface wlan-radio *wlan-radio-number*

Parameters

Parameter	Description	Value
interface wlan-radio *wlan-radio-number*	Specifies the WLAN radio interface. **NOTE** You do not need to enter a space between **wlan-radio** and *wlan-radio-number*.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display radio status** command can display status of specified AP radios, which facilitates AP radio management.

Example

Display the status of wlan-radio0/0/0.

```
<Huawei> display radio status interface wlan-radio0/0/0
  Radio status
 ------------------------------------------------------------------------
  Radio status: on
 ------------------------------------------------------------------------
```

Table 13-14 Description of the display radio status command output

Item	Description
radio-status	Radio status. ● on: enabled ● off: disabled

13.1.29 display service-set (for FAT AP)

Function

The **display service-set** command displays service set information.

Format

display service-set { **all** | **id** *service-set-id* | **name** *service-set-name* | **ssid** *ssid* }

Parameters

Parameter	Description	Value
all	Displays information about all service sets.	-
id *service-set-id*	Specifies the ID of a service set.	The value must be an existing service set ID.
name *service-set-name*	Specifies the name of a service set.	The value must be an existing service set name.
ssid *ssid*	Specifies the SSID of a service set.	The value must be an existing SSID.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information service set information.

Example

Display information about all service sets.

```
<Huawei> display service-set all
  ------------------------------------------------------------------------------
  ID      Name                          SSID
  0       lw                          abc
  1       lw2                          abcd
  ------------------------------------------------------------------------------
  Total: 2
```

Display information about service set 1.

```
<Huawei> display service-set id 1
  ------------------------------------------------------------------------------
  Service-set ID                  : 1
  Service-Set name                : lw2
  SSID                          : l00129796_93002
  Hide SSID                       : disable
  Type                          : service
  Maximum number of user          : 32
  Association timeout(min)        : 5
  Traffic profile name            : lw
  Security profile name           : lw
  Wlan-bss interface              : Wlan-bss1
  Igmp mode                       : off
  ------------------------------------------------------------------------------
```

Display information about service set with the SSID of abcd.

```
<Huawei> display service-set ssid abcd
  Service-set List:
  ------------------------------------------------------------------------------
  ID      Name
  1       abcd
  ------------------------------------------------------------------------------
  Total: 1
```

Table 13-15 Description of the **display service-set** command output

Item	Description
ID	ID of a service set.
Name	Name of a service set.
SSID	SSID character string of a service set.
Hide SSID	Whether the SSID is hidden.
Type	Type of a service set, which can be service or ap-management.

Item	Description
Maximum number of user	Maximum number of users allowed by a service set.
Association timeout(min)	Association timeout period.
Traffic profile name	Name of the traffic profile bound to a service set.
Security profile name	Name of the security profile bound to a service set.
Wlan-bss interface	Number of a WLAN-BSS interface.
Igmp mode	IGMP mode, which can be snooping or off.
Service-set ID	ID of a service set.
Service-Set name	Name of a service set.

13.1.30 display station assoc-info (for FAT AP)

Function

The **display station assoc-info** command displays information about associated STAs.

Format

display station assoc-info { **sta** *mac-address* | **interface wlan-radio** *wlan-radio-number* [**service-set** *service-set-id*] }

Parameters

Parameter	Description	Value
sta *mac-address*	Displays information about a STA with a specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
interface wlan-radio *wlan-radio-number*	Displays information about STAs connected to WLAN-Radio. **NOTE** You do not need to enter a space between **wlan-radio** and *wlan-radio-number*.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
service-set *service-set-id*	Displays information about STAs in a specified service set.	• AR150 series, AR160 series and AR200 series: 0 to 7

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about associated STAs.

- To view information about a specified STA, ensure that the STA has been associated with an AP.
- To view information about all STAs associated with a service set on WLAN-Radio, ensure that the service set has been bound to WLAN-Radio.

Example

Display information about an associated STA with MAC address 4016-9f14-f25d.

```
<Huawei> display station assoc-info sta 4016-9f14-f25d
 -------------------------------------------------------------------------------
  Station mac-address                    : 4016-9f14-f25d
  Associated SSID                        : huawei-wzk
  Station's AP ID                        : 0
  Station's Radio ID                     : 0
  Station's Authentication Method        : OPEN
  Station's Cipher Type                  : NO CIPHER
  Station's User Name                    : 88e3abeb97a4
  Station's Vlan ID                      : 100
  Station's asso BSSID                   : 00fe-a1b1-4043
  Station's state                        : Asso with auth
  ---------------------------------------------------------------------
```

Table 13-16 Description of the **display station assoc-info** command output

Item	Description
Station mac-address	MAC address of a STA.
Associated SSID	SSID of a service set with which a STA is associated.
Station's AP ID	ID of the AP that a STA associates with.
Station's Radio ID	Radio ID of a STA.

Item	Description
Station's Authentication Method	Authentication mode of a STA.
Station's Cipher Type	Encryption mode of a STA.
Station's User Name	User name of a STA.
Station's Vlan ID	VLAN ID of a STA.
Station's Channel Band-width	Channel bandwidth of a STA.
Station's asso BSSID	BSSID that the STA associates with.
Station's state	Status of the STA.

13.1.31 display station assoc-num (for FAT AP)

Function

The **display station assoc-num** command displays the number of STAs associated with a specified service set.

Format

display station assoc-num [**service-set** *service-set-id*]

Parameters

Parameter	Description	Value
service-set *service-set-id*	Specifies the number of STAs associated with a specified service set.	• AR150 series, AR160 series and AR200 series: 0 to 7

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If no service set is specified, the number of STAs associated with all service sets is displayed. To specify a service set, ensure that the service set has been created.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the number of STAs associated with service set 0.

```
<Huawei> display station assoc-num service-set 0
  Number of station: 1
```

Table 13-17 Description of the display station assoc-num command output

Item	Description
Number of station	Number of associated STAs.

13.1.32 display station roam-track (for FAT AP)

Function

The **display station roam-track** command displays the roaming track of a STA.

Format

display station roam-track sta *mac-address*

Parameters

Parameter	Description	Value
sta *mac-address*	Specifies the MAC address of the specified STA.	The value is in H-H-H format. An H is a hexadecimal number of four digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During the roaming process of a STA, the AC records the STA's roaming track (that is, information about the APs that the STA connects to). You can run the **display station roam-track** command to view the roaming track of the STA.

Example

Display the roaming track of the STA with the MAC address 0011-43c7-d73e.

```
<Huawei> display station roam-track sta 0011-43c7-d73e
 Access SSID:huawei1            Rx/Tx:Rx-Rate/Tx-Rate Mbps
 ------------------------------------------------------------------------------
 L2/L3     AC IP
 AP/Radio  BSSID          TIME                 In Rx/Tx   RSSI Out Rx/Tx    RSSI
 ------------------------------------------------------------------------------
 --        192.168.109.1
 1/0       dcd2-fc9d-0bb0 2014/01/03 11:46:12    61/61    -51     46/13    -48
 L2        192.168.109.1
 1/0       e468-a34d-afb0 2014/01/03 11:48:17    61/61    -58      -/-     -
 ------------------------------------------------------------------------------
 Number of roam track: 1
```

Table 13-18 Description of the display station roam-track command output

Item	Description
Access SSID	SSID associated with an STA.
Rx/Tx	Negotiated rate between the STA and AP.
L2/L3	Roaming mode.
AC IP	IP address of an AC that the STA has associated with.
AP/Radio	ID of a radio or an AP that the STA has associated with.
BSSID	BSSID of an AP that the STA has associated with.
TIME	Time duration when the STA has associated with an AP.
In Rx/Tx	Negotiated rate of the STA when it goes online on an AP.
RSSI	Signal strength of the STA when it goes online on an AP.
Out Rx/Tx	Negotiated rate of the STA when it disconnects from an AP.
RSSI	Signal strength of the STA when it disconnects from an AP.
Number of roam track	Number of STA roaming tracks.

13.1.33 display station statistics (for FAT AP)

Function

The **display station statistics** command displays statistics information about STAs.

Format

display station statistics [**sta** *mac-address*]

Parameters

Parameter	Description	Value
sta *mac-address*	Displays statistics information about a STA with a specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of four digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When you run the **display station statistics** command to check the statistics information about STAs,

- If no parameter is specified, statistics information about all STAs associated with the device is displayed.
- If **sta** is specified, the number of packets exchanged between the specified STA and device and the corresponding rate are displayed.

Prerequisites

To view statistics information about a specified STA, ensure that the STA has been associated with an AP.

Example

Display traffic statistics on a STA.

```
<Huawei> display station statistics sta 0025-86aa-0d1c
 --------------------------------------------------------------------------------
 Count of sent packets to the station                  : 2
 Count of received packets from the station            : 3846
 Count of sent bytes to the station                    : 110
 Count of received bytes from the station              : 170549
 Wireless data rate sent to the station(kbps)          : 0
 Wireless data rate received from the station(kbps)    : 0
 --------------------------------------------------------------------------------
```

Table 13-19 Description of the display station statistics command output

Item	Description
Count of sent packets to the station	Number of packets sent to the STA.
Count of received packets from the station	Number of packets received by the STA.
Count of sent bytes to the station	Number of bytes sent to the STA.
Count of received bytes from the station	Number of bytes received by the STA.
Wireless data rate sent to the station(kbps)	Rate at which packets are sent to the STA, in kbit/s.
Wireless data rate received from the station(kbps)	Rate at which packets are received by the STA, in kbit/s.

Display statistics information about all STAs.

```
<Huawei> display station statistics
  ------------------------------------------------------------------------------
  Total stations online time(seconds)                                :639
  Count of successful association and reassociation request          :1
  Count of stations associated with the AP                           :1
  Count of association request                                       :1
  Count of reject association request                                :0
  Count of failed association request                                :3
  Count of reassociation request                                     :0
  Count of successful reassociation request                          :0
  Count of reject reassociation request                              :0
  Count of failed reassociation request                              :3
  Count of disassociations because of users notified                 :0
  Count of disassociations because of users left without notification:3
  Count of disassociations because of other reasons                  :0
  Count of disassociations because of linkauthfail                   :0
  Count of authentication request                                    :6
  Count of deauth request                                            :0
  Count of AC auth successful                                        :1
  Count of AC auth failed because of password error                  :0
  Count of AC auth failed because of invalid calc                    :0
  Count of AC auth failed because of timeout                         :0
  Count of AC auth failed because of refused                         :0
  Count of AC auth failed because of other reasons                   :0
  ------------------------------------------------------------------------------
```

Table 13-20 Description of the **display station statistics** command output

Item	Description
Total stations online time(seconds)	Total online duration of all STAs, in seconds.

Item	Description
Count of successful association and reassociation request	Number of successful associations between STAs and the AP. If a STA successfully associates with the AP multiple times, STA association is counted multiple times.
Count of stations associated with the AP	Number of STAs that are being associated with the AP.
Count of association request	Number of association requests sent to the AP.
Count of reject association request	Number of association requests denied by the AP.
Count of failed association request	Number of failed associations.
Count of reassociation request	Number of reassociation requests sent to the AP.
Count of successful reassociation request	Number of successful reassociations.
Count of reject reassociation request	Number of reassociation requests rejected by the AP.
Count of failed reassociation request	Number of failed reassociations.
Count of disassociations because of users notified	Number of times STAs are disassociated from the AP because users go offline.
Count of disassociations because of users left without notification	Number of times STAs are disassociated from the AP because users go offline abnormally.
Count of disassociations because of other reasons	Number of times STAs are disassociated from the AP for other reasons.
Count of disassociations because of linkauthfail	Number of times STAs are disassociated from the AP due to link authentication failures.
Count of authentication request	Number of link authentication request packets.
Count of deauth request	Number of link deauthentication request packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Count of AC auth successful	Total number of successful link authentications on the AP. Every time a STA initiates a link authentication request and passes the authentication, the counter is incremented by 1. If the same STA initiates multiple authentication requests and passes all authentications, the counter is incremented cumulatively.
Count of AC auth failed because of password error	Number of STAs that fail to be authenticated due to incorrect passwords.
Count of AC auth failed because of invalid calc	Number of STAs that fail to be authenticated due to an invalid authentication algorithm.
Count of AC auth failed because of timeout	Number of STAs that fail to be authenticated due to timeout.
Count of AC auth failed because of refused	Number of STAs that fail to be authenticated because the AC rejects the associate requests.
Count of AC auth failed because of other reasons	Number of STAs that fail to be authenticated due to other reasons.

13.1.34 display statistics sta (for FAT AP)

Function

The **display statistics sta** command displays authentication statistics on a specified STA.

Format

display statistics sta *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a STA.	The value is in H-H-H format. An H is a hexadecimal number of four digits.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view authentication statistics on a STA by specifying the MAC address of a STA. This command displays the authentication mode used by the STA and authentication statistics.

Example

View statistics on the STA with MAC address 000b-c002-95c9, which uses Wireless LAN Authentication and Privacy Infrastructure (WAPI) authentication.

```
<Huawei> display statistics sta 000b-c002-95c9
  STA MAC address                    : 000b-c002-95c9
  Authentication method              : WAPI PSK
  WAPI Version                       : 1
  Status of Controlled Port          : Open
  Selected unicast cipher            : SMS4
  WPI Replay Counters                : 0
  WPI Decryptable Errors             : 0
  WPI MIC Errors                     : 0
  WAI Signature Errors               : 0
  WAI HMAC Errors                    : 0
  WAI Discard Counters               : 0
  WAI Timeout Counters               : 1
  WAI Format Errors                  : 0
  WAI Authentication Result Failures : 0
  WAI Certificate Handshake Failures : 0
  WAI Unicast Handshake Failures     : 0
  WAI Multicast Handshake Failures   : 0
```

Table 13-21 Description of the display statistics sta command output (WAPI authentication)

Item	Description
STA MAC address	MAC address of a STA.
Authentication method	Authentication mode. The following authentication modes are supported: WAPI certificate authentication, WAPI pre-shared key authentication, WPA1 802.1x authentication, WPA1 pre-shared key authentication, WPA2 802.1x authentication, WPA2 pre-shared key authentication, pre-shared key authentication, and open system authentication.
WAPI Version	WAPI version.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status of Controlled Port	Status of the controlled port, which can be open or closed.
Selected unicast cipher	Unicast key used in authentication.
WPI Replay Counters	Number of WPI MAC protocol data units (MPDUs) discarded by the anti-replay function.
WPI Decryptable Errors	Number of WPI-SMS4 decryption errors caused by lack of valid key.
WPI MIC Errors	Number of WPI-SMS4 decryption errors caused by incorrect message integrity codes (MICs).
WAI Signature Errors	Number of WAI packets with incorrect signatures.
WAI HMAC Errors	Number of WAI packets with incorrect message authentication codes (MACs).
WAI Discard Counters	Number of discarded WAI packets.
WAI Timeout Counters	Number of WAI packets that time out.
WAI Format Errors	Number of WAI packets with incorrect formats.
WAI Authentication Result Failures	Number of WAI authentication failures.
WAI Certificate Handshake Failures	Number of WAI certificate authentication failures.
WAI Unicast Handshake Failures	Number of WAI unicast key negotiation failures.
WAI Multicast Handshake Failures	Number of WAI multicast key negotiation failures.

View statistics on the STA with MAC address 0011-F321-D2C3, which uses Wired Equivalent Privacy (WEP) authentication.

```
<Huawei> display statistics sta 0011-F321-D2C3
  STA MAC Address          : 0011-F321-D2C3
  Authentication Method    : Share key
  Selected Unicast Cipher : WEP-40
```

Table 13-22 Description of the display statistics sta command output (WEP authentication)

Item	Description
STA MAC Address	MAC address of a STA.
Authentication Method	Authentication mode specified in the security profile.
Selected Unicast Cipher	Unicast key used in authentication.

View statistics on the STA with MAC address 0011-F321-D2C3, which uses WPA authentication.

```
<Huawei> display statistics sta 0011-F321-D2C3
STA MAC address                    : 0011-F321-D2C3
Authentication method              : WPA  PSK
Dot11RSNAStatsVersion              : 0
Status of Controlled Port          : Closed
Selected unicast cipher            : TKIP
```

Table 13-23 Description of the display statistics sta command output (WPA authentication)

Item	Description
STA MAC address	MAC address of a STA.
Authentication method	Authentication mode specified in the security profile.
Status of Controlled Port	Status of the controlled port.
Selected unicast cipher	Unicast key used in authentication.
Dot11RSNAStatsVersion	Latest RSNA version that the STA supports.

13.1.35 display statistics radio (for FAT AP)

Function

The **display statistics radio** command displays frame statistics on the MAC layer of a specified radio, including the number of frames sent and received by the radio.

Format

display statistics radio interface wlan-radio *wlan-radio-number*

Parameters

Parameter	Description	Value
interface wlan-radio *wlan-radio-number*	Specifies the WLAN radio interface. **NOTE** You do not need to enter a space between **interface wlan-radio** and *wlan-radio-number*.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

View frame statistics on the MAC layer of a radio to monitor the service operating status on the radio.

Example

Display frame statistics on the MAC layer of the radio interface.

```
<Huawei> display statistics radio interface wlan-radio0/0/0
 ---------------------------------------------------------------------------
   Wireless received frames                          :0
   Wireless received bytes                           :0
   Wireless transmitted frames                       :0
   Wireless transmitted bytes                        :0
   Wireless transmitted RTS successes                :0
   Wireless transmitted unicast frames               :0
   Wireless transmitted broadcast frames             :0
   Wireless transmitted failure frames               :0
   Wireless received error frames                    :0
   Wireless received physical layer error frames     :0
   Wireless received FCS error frames                :0
   Wireless received MIC error frames                :0
   Wireless received private key and decrypt fail frames :0
   Wireless retry frames                             :0
   Wireless down-stream MAC error frames             :0
   Wireless PER(%)                                   :0
   Wireless PER of the last statistic period(%)      :100
   Wireless channel utilization(%)                   :0
   Wireless received signal strength(dBm)            :-79.00
   Wireless receive power(dBm)                       :-79.00
 ---------------------------------------------------------------------------
```

Table 13-24 Description of the **display statistics radio** command output

Item	Description
Wireless received frames	Number of frames received by the radio.

Item	Description
Wireless received bytes	Number of bytes received by the radio.
Wireless transmitted frames	Number of frames sent by the radio.
Wireless transmitted bytes	Number of bytes sent by the radio.
Wireless transmitted RTS successes	Number of Request to Send (RTS) frames that are successfully sent by the radio.
Wireless transmitted unicast frames	Number of unicast frames sent by the radio.
Wireless transmitted broadcast frames	Number of broadcast frames sent by the radio.
Wireless transmitted failure frames	Number of frames that the radio fails to send.
Wireless received error frames	Number of errored frames received by the radio.
Wireless received physical layer error frames	Number of errored frames received at the physical layer of the radio.
Wireless received FCS error frames	Number of frames with incorrect frame check sequence (FCS) received by the radio.
Wireless received MIC error frames	Number of frames with message integrity code (MIC) received by the radio.
Wireless received private key and decrypt fail frames	Number of frames with incorrect keys received by the radio.
Wireless retry frames	Number of frames that are retransmitted by the radio.
Wireless down-stream MAC error frames	Number of downstream errored frames received by the MAC layer of the radio.
Wireless PER(%)	Packet error rate of the radio.
Wireless PER of the last statistic period(%)	Packet error rate in the last statistical period.
Wireless channel utilization(%)	Channel usage on the radio.
Wireless received signal strength(dBm)	Strength of signals received by the radio.
Wireless receive power(dBm)	Receiving optical power of the radio.

 Copyright © Huawei Technologies Co., Ltd.

13.1.36 display station online-fail-record (for FAT AP)

Function

The **display station online-fail-record** command displays STA online failure records.

Format

display station online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays online failure records of all STAs.	-
mac *mac-address*	Displays online failure records of the STA with the specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If a STA fails to go online, you can run the command to check the failure reason, which helps locate the fault.

After the number of STA online failure records reaches the maximum that can be stored, new records overwrites existing ones.

Example

Displays online failure records of all STAs.

```
<Huawei> display station online-fail-record all
  AP/Rf/WLAN: AP ID/Radio ID/WLAN ID
  -------------------------------------------------------------------------------
  STA MAC         AP/Rf/WLAN    Last fail time       Reason
  -------------------------------------------------------------------------------
  14cf-9208-9abf  0/0/1         2014-06-17/14:06:57  Succeed in matching the glo
bal STA blacklist.
  -------------------------------------------------------------------------------
  Total stations: 1 Total records: 1
```

Table 13-25 Description of the **display station online-fail-record** command output

Item	Description
STA MAC	MAC address of the STA that fails to go online.
AP/Rf/WLAN	ID of the AP/radio/VAP that the STA fails to connect to.
Last fail time	Time of the STA online failure.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Reason for the STA online failure. ● 802.1X authentication failed: 802.1x authentication fails. ● ap max user: The number of connected STAs has reached the maximum on the AP. ● Authentication failed or Esap cut STA: The authentication fails or the AP automatically disconnects from the STA. ● Authentication times out: Authentication times out. ● Failed to check the association and reassociation request packets: Association or reassociation packet check fails. ● Failed to decrypt WEP challenge phrases: Decryption of the challenge phrase in WEP encryption fails. ● Failed to match the global STA whitelist: The STA is not in the global whitelist. ● Failed to match the VAP STA whitelist: The STA is not in the VAP whitelist. ● Incompatible STA: The AP is not compatible with the STA. ● Insufficient resources allocated to the STA: Too many STAs associate with the AP, and resources are insufficient. ● Inner application reason: The STA online failure is caused by internal application problems. ● Invalid encryption field: The encryption field is invalid. ● Low rssi: The signals of the STAs are too weak. ● MAC address authentication failed: MAC address authentication fails. ● No response from the STA: The STA is aged out or forced offline. ● Static ip: The IP address of the STA is an unauthorized IP address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Succeed in matching the dynamic blacklist: The STA is in the dynamic blacklist. • Succeed in matching the global STA blacklist: The STA is in the global dynamic blacklist. • Succeed in matching the VAP STA blacklist: The STA is in the VAP blacklist. • The AP supports only 802.11n access: The VAP supports only the 802.11n access mode but the STA does not work in the 802.11n access mode. • The maximum number of access STAs is exceeded: The number of STAs reaches the maximum. • The rate set does not support negotiation: The AP does not support the rate of the STA. • The STA is disconnected or VAP is disabled: The STA is forced offline on the AP or the VAP state becomes down. • The STA is not associated: The STA fails to associate with the AP but sends a data packet to the AP. After the AP receives the data packet, it does not send the packet to an upstream device but sends a disassociation packet to the STA. • The STA is not authenticated before association: The STA directly connects to the AP but is not authenticated; therefore, it is rejected by the AP. • The STA is not authenticated: The STA sends a data packet to the AP but does not pass the authentication. After the AP receives the data packet, it does not send the packet to an upstream device but sends a disassociation packet to the STA. • Uac channel util: The channel usage of the radio exceeds the threshold.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• Uac user num: The number of STAs connected to the radio has reached the maximum. • vap max user: The number of STAs connected to the VAP has reached the maximum. • WAPI authentication failed: WAPI authentication fails. • WAPI authentication times out: WAPI authentication times out. • WEP authentication packet sequence error: There is a sequence error in the WEP authentication packet. • WEP encryption error: A WEP encryption error occurs. • WPA authentication failed: WPA authentication fails. • WPA authentication times out: WPA authentication times out. • WPA MIC failed: The PSK is incorrect. • WPA/WPA2/WAPI encryption error: A WPA/WPA2/WAPI encryption error occurs. • Inconsistent SSIDs before and after the roaming: The STA associates with different VAP SSIDs before and after intra-AP roaming.

Related Topics

13.1.59 reset station online-fail-record (for FAT AP)

13.1.37 display uncontrol ap (for FAT AP)

Function

The **display uncontrol ap** command displays information about uncontrolled APs.

Format

display uncontrol ap { **all** | **bssid** *bssid* }

Parameters

Parameter	Description	Value
bssid *bssid*	Specifies the basic service set identifier (BSSID) of an AP that is not controlled by the local AC.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
all	Displays information about all APs that are not controlled by the local AC.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about all uncontrolled APs or an uncontrolled AP with a specified BSSID. The command output includes ID of the controlled AP closest to the uncontrolled AP and the strength of signals that the controlled AP received from the uncontrolled AP.

Example

View information about all APs that are not controlled by the local AC.

```
<Huawei> display uncontrol ap all
---------------------------------------------
 BSSID          NEAREST-AP  CHANNEL  RSSI(dBm)
---------------------------------------------
 00e0-1234-5678 5           6        3.50
 00e0-5678-1234 6           11       5.00
---------------------------------------------
 Total: 2
```

View information about uncontrolled AP with the BSSID of 00e0-5678-1234.

```
<Huawei> display uncontrol ap bssid 00e0-5678-1234
 ----------------------------------------------------
  BSSID          NEAREST-AP  CHANNEL  RSSI(dBm)  SSID
 ----------------------------------------------------
  00e0-5678-1234 6           11       -42.00     busonline
 ----------------------------------------------------
```

Table 13-26 Description of the display uncontrol ap command output

Item	Description
BSSID	BSSID of an uncontrolled AP.

Item	Description
NEAREST-AP	ID of the controlled AP that is closest to the uncontrolled AP.
CHANNEL	Channel on which the uncontrolled AP is detected. If a rogue AP is detected on multiple channels, the channel with the strongest signal strength is displayed.
RSSI(dBm)	Strength of signals that the closest controlled AP receives from the uncontrolled AP, in dBm.
SSID	SSID of an uncontrolled AP.

13.1.38 display vap (for FAT AP)

Function

The **display vap** command displays parameter settings of virtual access points (VAPs).

Format

display vap { **all** | **service-set** { **id** *service-set-id* | **name** *service-set-name* } }

Parameters

Parameter	Description	Value
all	Displays parameter settings of all VAPs.	-
service-set id *service-set-id*	Displays parameter settings of the VAP with a specified SSID.	• AR150 series, AR160 series and AR200 series: 0 to 7
service-set name *service-set-name*	Displays parameter settings of the VAP with a specified service set name.	The value is a string of 1 to 31 characters without question marks (?) or spaces. It cannot begin or end with double quotation marks (" ").

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vap** command displays parameter settings of a specified VAP or all VAPs.

Example

Display parameter settings of all VAPs.

```
<Huawei> display vap all
  All VAP Information(Total-1):
  ---------------------------------------------------------------------
  Radio ID  SS ID   WLAN ID  BSSID           SS name
  0         0       1        00E0-FC03-0205  vap0
  ---------------------------------------------------------------------
  Total: 1
```

Display parameter settings of the VAP with a specified SSID.

```
<Huawei> display vap service-set id 0
  ---------------------------------------------------------------------
  Radio ID  SS ID   WLAN ID  BSSID           SS name
  0         1       1        707B-E8E9-D32A  test
  ---------------------------------------------------------------------
  Total: 1
```

Table 13-27 Description of the display vap command output

Item	Description
Radio ID	ID of the radio.
SS ID	Identifier of the service set bound to the radio.
WLAN ID	ID of the WLAN to which a VAP is applied.
BSSID	BSSID of a VAP, which is the unique identifier of the VAP.
SS name	Name of a service set.

13.1.39 display wlan global

Function

The **display wlan global** command displays global parameters of an AP.

Format

display wlan global

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display wlan global** command shows settings of global parameters.

Prerequisites

The AP country code has been configured using the **13.1.77 wlan global country-code** command.

Example

Display global parameters of an AP.

```
<Huawei> display wlan global
 ------------------------------------------------------------
 Country code      : CN
 AP Network Element: -
 ------------------------------------------------------------
```

Table 13-28 Description of the display wlan global command output

Item	Description
Country code	Country code of the AP. To configure the country code of the AP, run the **13.1.77 wlan global country-code** command.
AP Network Element	NE ID.

Related Topics

13.1.77 wlan global country-code

 Copyright © Huawei Technologies Co., Ltd.

13.1.40 display wlan record

Function

The **display wlan record** command displays information about the Probe Request and Beacon frames collected by the device.

NOTE

The AR1220W, AR1220EVW and AR1220VW do not support this command.

Format

display wlan record { **all** | **probe** | **beacon** } [**interface wlan-radio** *wlan-radio-number*]

Parameters

Parameter	Description	Value
all	Displays information about the Probe Request and Beacon frames collected by the device.	-
probe	Displays information about the Probe Request frames collected by the device.	-
beacon	Displays information about the Beacon frames collected by the device.	-
interface wlan-radio *wlan-radio-number*	Specifies the WLAN radio interface. **NOTE** You do not need to enter a space between **wlan-radio** and *wlan-radio-number*.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the function of collecting Probe Request and Beacon frames is enabled on the device, you can run the **display wlan record** command to check information about the Probe Request and Beacon frames collected by the device, including the MAC address and RSSI of the STA or Fat AP.

Precautions

The aging time of all statistics entries is 5 minutes. That is, if the device does not receive a Probe Request frame from a STA or a Beacon frame from a Fat AP within 5 minutes, the device deletes statistics entries of the STA or Fat AP when the aging time expires.

Example

Display information about the Probe Request and Beacon frames collected by the device.

```
<Huawei> display wlan record all
MY MAC:  9c28-efcb-44a9
--------------------------------------------------------------------------------
-----------------------------------------------------------------
 STA MAC            First time            Last time            DurTime FirRSSI
LaRSSI  DType     DManu        DModelName       DModelNum        DeviceName
--------------------------------------------------------------------------------
-----------------------------------------------------------------------
 7014-a6**-d157     14:19:11 2015/08/01     14:19:11 2015/08/01        0     -91
  -91    0
 9404-9c**-74f0     14:18:35 2015/08/01     14:19:21 2015/08/01       46     -62
  -58    1
 38bc-1a**-8dd2     14:19:00 2015/08/01     14:19:11 2015/08/01       11     -89
  -89    0
 acf7-f3**-3942     14:19:19 2015/08/01     14:19:19 2015/08/01        0     -82
  -83    0      "Xiaomi"     "MI 2"     "MI 2"     "aries"
 1834-51**-6fb9     14:19:13 2015/08/01     14:19:16 2015/08/01        3     -75
  -76    0
 18c5-8a**-8b5f     14:19:25 2015/08/01     14:19:25 2015/08/01        0     -83
  -83    1
 0046-4b**-1fa0     14:18:49 2015/08/01     14:18:49 2015/08/01        0     -87
  -87    0
 581f-28**-f450     14:18:51 2015/08/01     14:19:26 2015/08/01       35     -79
  -85    0
 9cc1-72**-1014     14:19:22 2015/08/01     14:19:23 2015/08/01        1     -89
  -83    0      "HUAWEI"     "HUAWEI P7-L07"     "HUAWEI P7-L07"     "P7-L07"
 f8df-a8**-71ce     14:18:44 2015/08/01     14:19:14 2015/08/01       30     -65
  -71    0      "nubia"     "NX40X"     "NX40X"     "NX40X"
 0046-4b**-68cf     14:18:35 2015/08/01     14:19:26 2015/08/01       51     -87
  -86    0

Total Records: 11
```

Table 13-29 Description of the **display wlan record** command output

Item	Description
MY MAC	MAC address of the device.
STA MAC	MAC address of the STA or Fat AP.
First time	First time when the device receives a Probe Request frame or Beacon frame.

Item	Description
Last time	Last time when the device receives a Probe Request frame or Beacon frame.
DurTime	Duration when the device receives Probe Request frames or Beacon frames.
FirRSSI	RSSI of the STA or Fat AP that is collected for the first time.
LaRSSI	RSSI of the STA or Fat AP that is collected for the last time.
DType	Whether the device sending packets is a STA or Fat AP. ● 0: The device is a STA, such as a mobile phone or a tablet. ● 1: The device is a Fat AP, such as a router.
DManu	Manufacturer of the STA. **NOTE** A maximum of 32 bytes can be displayed.
DModelName	Model of the STA. **NOTE** A maximum of 32 bytes can be displayed.
DModelNum	Sequence number of the STA. **NOTE** A maximum of 32 bytes can be displayed.
DeviceName	Name of the STA. **NOTE** A maximum of 32 bytes can be displayed.

Related Topics

13.1.63 set wlan record enable

13.1.60 reset wlan record

13.1.41 display workmode wlan

Function

The **display workmode wlan** command displays the current WLAN mode and the configured WLAN mode of a device.

Format

display workmode wlan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the current WLAN mode and the configured WLAN mode of a device. The configured WLAN mode takes effect after the device is restarted.

Example

Display the current WLAN mode of the device.

```
<Huawei> display workmode wlan
 Wlan Current WorkMode = ap
 Wlan Config WorkMode  = ac
```

Table 13-30 Description of the display workmode wlan command output

Item	Description
Wlan Current WorkMode	Current WLAN mode of a device. ● ap: Fat AP mode ● ac: AC mode
Wlan Config WorkMode	Configured WLAN mode, which takes effect after the device is restarted. ● ap: Fat AP mode ● ac: AC mode

Related Topics

13.1.69 set workmode wlan (for FAT AP)

13.1.42 dtim-interval (for FAT AP)

Function

The **dtim-interval** command sets the delivery traffic indication map (DTIM) interval in a radio profile.

The **undo dtim-interval** command restores the default DTIM interval in a radio profile.

By default, the DTIM interval is 1.

Format

dtim-interval *dtim-interval*

undo dtim-interval

Parameters

Parameter	Description	Value
dtim-interval	Specifies the DTIM interval.	The value is an integer that ranges from 1 to 255, in Beacons.

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

DTIM refers to delivery traffic indication map. After a STA enters the dormancy mode, the associated AP saves the broadcast and multicast frames for the STA. When a Beacon frame sent to the STA by the AP contains DTIM, the saved broadcast and multicast frames will be transmitted to the STA. The DTIM interval refers to the number of Beacon frames sent before the Beacon frame that contains the DTIM. To set the interval for sending Beacon frames in a radio profile, run the **beacon-interval** command.

- When the STA is in the dormancy status, the AP saves data transmitted to the STA and notifies the STA with a bit in broadcast Beacon frames. The STA receives data according to this bit. You can run this command to set the DTIM interval in the specified radio profile.
- The DTIM interval specifies how many Beacon frames are sent before the Beacon frame that contains the DITM. A long DTIM interval lengthens the dormancy time of the STA and saves power, but degrades the transmission capability of the STA. A short interval helps transmitting data in a timely manner, but the STA is waken up frequently, causing high power consumption.

Example

Set the interval for sending DTIM to 5 in radio profile **80211b**.

```
<Huawei> system-view
[Huawei] wlan
```

```
[Huawei-wlan-view] radio-profile name 80211b
[Huawei-wlan-radio-prof-80211b] dtim-interval 5
```

13.1.43 forward-mode (for FAT AP)

Function

The **forward-mode** command sets the data forwarding mode in a service set.

The **undo forward-mode** command restores the default data forwarding mode in a service set.

By default, the data forwarding mode is direct-forward in the service set.

NOTE

The AR1220W and AR1220VW do not support this command.

Format

forward-mode { **direct-forward** | **gre-tunnel** }

undo forward-mode

Parameters

Parameter	Description	Value
direct-forward	Indicates the direct forwarding mode.	-
gre-tunnel	Indicates the GRE tunnel forwarding mode.	-

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

You can run the **forward-mode** command to configure the data forwarding mode in a service set.

Precautions

- When Wi-Fi and GRE both exist, you must configure the DHCP server and GRE tunnel on different devices but not on the same device.
- GRE tunnel forwarding is used only in Wi-Fi + GRE scenarios. In other scenarios, direct forwarding is recommended.

 Copyright © Huawei Technologies Co., Ltd.

- In GRE tunnel forwarding mode, remote 802.1x authentication is not supported, and the local and remote ends cannot share one address pool.
- In GRE tunnel forwarding mode, an access device (Fat AP) and the upper-layer network (Internet) at the same end of a GRE tunnel cannot communicate at Layer 2 or Layer 3.
- When a WLAN-BSS interface with GRE tunnel forwarding configured is isolated from a WLAN-BSS without GRE tunnel forwarding configured, they cannot communicate with each other. You need to configure the same data forwarding mode on the interfaces to enable communication between them.

Example

Create the service set **ChinaNet** and set the data forwarding mode to GRE tunnel forwarding.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] forward-mode gre-tunnel
```

Related Topics

13.1.29 display service-set (for FAT AP)

13.1.44 guard-interval-mode (for FAT AP)

Function

The **guard-interval-mode** command configures the guard interval (GI) mode.

The **undo guard-interval-mode** command restores the default GI mode.

By default, the GI mode is normal.

Format

guard-interval-mode { **short** | **normal** }

undo guard-interval-mode

Parameters

Parameter	Description	Value
short	Indicates a short interval.	-
normal	Indicates a common interval.	-

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

A wireless device does not receive and send data all the time. An interval between data receiving and sending improves transmission performance. This interval is called GI.

The GI mode consists of the short interval and common interval. The common interval is 800 ns whereas the short interval is 400 ns. The short interval is applicable to 802.11n specifications, which can raise the transmission rate of 802.11n packets.

NOTE

The **guard-interval-mode** command supports only 802.11n.

Example

Set the GI mode of radio profile **80211n** to normal.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name 80211n
[Huawei-wlan-radio-prof-80211n] guard-interval-mode normal
```

Related Topics

13.1.56 radio-profile (WLAN view) (for FAT AP)
13.1.27 display radio-profile

13.1.45 igmp-mode snooping (for FAT AP)

Function

The **igmp-mode snooping** command enables the function of converting multicast packets to unicast packets in the service set view.

The **undo igmp-mode** command disables the function of converting multicast packets to unicast packets.

By default, the function of converting multicast packets to unicast packets is disabled.

Format

igmp-mode snooping

undo igmp-mode

Parameters

None

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

You can enable the function of converting multicast packets to unicast packets in scenarios that have high requirements on multicast stream transmission, such as a high-definition video on-demand scenario.

After the function is enabled, an AP listens on Report and Leave packets to maintain multicast-to-unicast entries. When sending multicast packets to the client, the AP converts the multicast packets to unicast packets based on the multicast-to-unicast entries to improve multicast stream transmission efficiency.

Example

Enable the function of converting multicast packets to unicast packets.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name huawei
[Huawei-wlan-service-set-huawei] igmp-mode snooping
```

Related Topics

13.1.29 display service-set (for FAT AP)

13.1.46 interface wlan-bss

Function

Using the **interface wlan-bss** command, you can create a WLAN-BSS interface.

Using the **undo interface wlan-bss** command, you can delete a WLAN-BSS interface.

By default, no WLAN-BSS interface is created.

Format

interface wlan-bss *wlan-bss-number*

undo interface wlan-bss *wlan-bss-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
wlan-bss-number	Specifies the number of a WLAN-BSS interface.	The value is an integer. The value range varies according to devices: ● AR150 series, AR200 series, AR161FGW-L, AR161FGW-La, AR161FGW-Lc, AR161FW, AR161FW-P-M5, AR161W, AR169FGW-L, AR169FGVW-L, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S and AR169JFVW-2S: 0 to 7 ● AR1200 series, AR161EW, AR161EW-M1, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR169W-P-M9 and AR169RW-P-M9: 0 to 15

Views

System view

Default Level

2: Configuration level

Usage Guidelines

- A WLAN-BSS interface is configured with parameters such as the interface priority and authentication mode.
- After you create a WLAN-BSS interface, bind this interface to a service set.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create WLAN-BSS 1.

```
<Huawei> system-view
[Huawei] interface wlan-bss 1
[Huawei-Wlan-Bss1]
```

13.1.47 interface wlan-radio

Function

The **interface wlan-radio** command displays the radio interface view.

NOTE

In the radio interface view, modifying the WLAN configuration may cause STAs associated with the current radio to go offline.

Format

interface wlan-radio *wlan-radio-number*

Parameters

Parameter	Description	Value
wlan-radio-number	Displays the specified radio interface view.	Enumerated type. The values are as follows: ● 0/0/0: indicates the 2.4-GHz radio interface. ● 0/0/1: indicates the 5-GHz radio interface. Only the AR169W-P-M9, AR169RW-P-M9, AR129CVW, AR129CGVW-L, AR169CVW, AR169CVW-4B4S, AR161EW, AR161EW-M1, AR169EW, AR169EGW-L support 0/0/0 and 0/0/1. Other models support only 0/0/0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

- You can configure the radio after entering the radio interface.
- you can create a VAP by binding a service set to radio interface.

Example

Display the view of Wlan-Radio0/0/0.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0]
```

13.1.48 legacy-station enable (for FAT AP)

Function

The **legacy-station enable** command permits access of legacy terminals.

The **undo legacy-station enable** command denies access of legacy terminals.

By default, access of legacy terminals is permitted.

Format

legacy-station enable

undo legacy-station enable

Parameters

None

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Legacy terminals support only 802.11a, 802.11b, or 802.11g, and provide a rate far smaller than 802.11n terminals. If the legacy terminals access the wireless network, data transmission rate of the 802.11n terminals will be reduced. To prevent transmission rate of 802.11n terminals from being affected, run the **undo legacy-station enable** command to deny access of legacy terminals.

Configuration Impact

After the **undo legacy-station enable** command is run, legacy terminals supporting only 802.11a, 802.11b, or 802.11g cannot access the wireless network.

Precautions

The **undo legacy-station enable** and **undo wmm enable** commands cannot be configured at the same time, otherwise, any STA cannot access the WLAN.

Example

Deny access of legacy terminals.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name radiopf
[Huawei-wlan-radio-prof-radiopf] undo legacy-station enable
```

13.1.49 max-user-number (for FAT AP)

Function

The **max-user-number** command sets the maximum number of successfully associated STAs in a service set.

The **undo max-user-number** command restores the default maximum number of successfully associated STAs in a service set.

By default, a service set allows for a maximum of 32 successfully associated STAs.

Format

max-user-number *max-user-number*

undo max-user-number

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of successfully associated STAs in the specified service set.	The value is an integer that ranges from 1 to 128. For the AR109GW-L, AR109W, AR129CGVW-L, AR129CVW, AR169CVW, and AR169CVW-4B4S, the maximum number of associated STAs is 32 on each VAP.

 Copyright © Huawei Technologies Co., Ltd.

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

The **max-user-number** *max-user-number* command sets the maximum number of successfully associated STAs in the specified service set.

Example

Create a service set named **ChinaNet** and set the maximum number of successfully associated STAs for the service set to 50.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] max-user-number 50
```

13.1.50 multicast-rate (for FAT AP)

Function

The **multicast-rate** command configures the multicast rate of wireless packets for a radio.

The **undo multicast-rate** command restores the default multicast rate of wireless packets for a radio.

By default, the multicast rate of wireless packets is 11 Mbps for the 2.4 GHz radio and 6 Mbps for the 5 GHz radio.

Format

multicast-rate { **2g** *2g-multicast-rate* | **5g** *5g-multicast-rate* }

undo multicast-rate { **2g** | **5g** }

Parameters

Parameter	Description	Value
2g *2g-multicast-rate*	Specifies the multicast rate of wireless packets for the 2.4 GHz radio.	Enumerated type: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
5g *5g-multicast-rate*	Specifies the multicast rate of wireless packets for the 5 GHz radio. **NOTE** Only the AR169W-P-M9, AR169RW-P-M9, AR129CVW, AR129CGVW-L, AR169CVW, AR169CVW-4B4S, AR161EW, AR161EW-M1, AR169EW, AR169EGW-L support the 5 GHz radio.	Enumerated type: ● 6: 6 Mbps ● 9: 9 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

After this command is run, the multicast rate of wireless packets is the configured value and irrelevant to the STA access mode.

If the configured multicast rate is not in the basic rate set and the STA does not support this rate, the STA cannot receive multicast data.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the multicast rate of 2.4GHz radio packets to 54 Mbps.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name radiopf
[Huawei-wlan-radio-prof-radiopf] multicast-rate 2g 54
```

13.1.51 per-threshold (for FAT AP)

Function

The **per-threshold** command sets the packet loss or packet error rate threshold in a radio profile.

The **undo per-threshold** command restores the default packet loss or packet error rate threshold in a radio profile.

The default packet loss or packet error rate threshold in a radio profile is 30%.

Format

per-threshold *per-threshold*

undo per-threshold

Parameters

Parameter	Description	Value
per-threshold	Specifies the packet loss or packet error rate threshold.	The value is an integer that ranges from 3 to 50, in percentage.

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

After the MAC layer sends out a packet at the lowest rate, a packet loss or an error packet is recorded if no ACK message or an NACK message is received after the retransmission threshold is exceeded.

Example

Set the packet loss or packet error rate threshold to 15% in radio profile **radio1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name radio1
[Huawei-wlan-radio-prof-radio1] per-threshold 15
```

13.1.52 power-level (for FAT AP)

Function

The **power-level** command sets the power level for a radio.

The **undo power-level** command restores the default power level of a radio.

By default, the power level of a radio is 0, indicating full power. The actual power is determined by an AP type.

Format

power-level *power-level*

undo power-level

Parameters

Parameter	Description	Value
power-level	Specifies the power level of a radio.	The value is an integer that ranges from 0 to 12. A larger value indicates a higher power level and a low transmit power of a radio.

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The configured power level must be supported by the radio, and is subject to different channels as well as laws and regulations corresponding to the country code.

If the configured power level exceeds the maximum power level supported by the AP, the configuration is saved but the actual power is determined by the

maximum power level supported by the AP. You can run the **display actual channel-power** command to check the actual channel and power information about the AP radio.

Prerequisites

The radio power mode has been set to fixed using the **power-mode fixed** command.

Example

Set the power level of radio 0/0/0 to 1.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] power-level 1
```

Related Topics

13.1.16 display actual channel-power (for FAT AP)

13.1.53 power-mode (for FAT AP)

Function

The **power-mode** command sets the power mode in a radio profile.

The **undo power-mode** command restores the default power mode in a radio profile.

By default, the automatic mode is used.

Format

power-mode { **auto** | **fixed** }

undo power-mode

Parameters

Parameter	Description	Value
auto	Indicates the automatic mode. The power of the radio bound to the radio profile can be automatically adjusted.	-
fixed	Indicates the fixed mode. The power of the radio bound to the radio profile is fixed at the set value.	-

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

The power mode can be set to the automatic or fixed mode. In the automatic mode, the radio output power is automatically selected according to the radio environment. In the fixed mode, the radio output power must be specified.

If an AP needs radio calibration, the power mode must be set to automatic mode in the AP's radio profile.

Example

Set the power mode in radio profile **802.11b** to **auto**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name 80211b
[Huawei-wlan-radio-prof-80211b] power-mode auto
```

13.1.54 radio enable (for FAT AP)

Function

The **radio enable** command enables a specified radio.

The **undo radio enable** command disables a specified radio.

By default, a radio is enabled.

Format

radio enable

undo radio enable

Parameters

None

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enable or disable a specified radio.

Example

Enable radio 0/0/0 on the WLAN-radio interface.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] radio enable
```

13.1.55 radio-frequency (for FAT AP)

Function

The **radio-frequency** command configures the frequency band of a radio.

The **undo radio-frequency** command restores the default frequency band of a radio.

By default, a radio works at the 2.4 GHz frequency band.

NOTE

Only the AR201VW-P and AR207VW support this command.

Format

radio-frequency { **2.4g** | **5g** }

undo radio-frequency

Parameters

Parameter	Description	Value
2.4g	Indicates that the radio works at the 2.4 GHz frequency band.	-
5g	Indicates that the radio works at the 5 GHz frequency band.	-

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

When the device works in Fat AP mode, it can switch between 2.4 GHz and 5 GHz.

NOTE

Changing the working radio of Wlan-Radio0/0/0 will delete channel, power, and antenna gain configurations on Wlan-Radio0/0/0.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the radio to work at the 5 GHz frequency band.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] radio-frequency 5g
  Warning: Modify radio frequency may delete configuration of the Radio, are you
 sure to continue?[Y/N]:y
```

13.1.56 radio-profile (WLAN view) (for FAT AP)

Function

The **radio-profile** command creates or enters an radio profile view.

The **undo radio-profile** command is used to delete a radio profile.

By default, the radio profile named **radiof** exists in the system.

Format

radio-profile { **id** *profile-id* | **name** *profile-name* } *

undo radio-profile { **all** | **id** *profile-id* | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Deletes all radio profiles.	-
id *profile-id*	Specifies the ID of a radio profile, which identifies a radio profile.	The value is an integer ranging from 0 to 15.
name *profile-name*	Specifies the name of a radio profile, which identifies a radio profile.	The value is a string of 1 to 31 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to create or delete a radio profile or enter the radio profile mode to configure the profile. If the specified profile ID or profile name does not exist, this command creates a radio profile and displays the view of this radio profile, and all parameters in this radio profile use default values. You can also change values of these parameters. For default values of parameters, see parameter descriptions of configuration commands.

NOTE

A radio profile name is mandatory for creating a radio profile.

Example

Create radio profile **802.11b**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name 802.11b
[Huawei-wlan-radio-prof-802.11b]
```

Related Topics

13.1.27 display radio-profile

13.1.57 radio-profile (Radio interface view) (for FAT AP)

Function

The **radio-profile** command binds a radio profile to a specified radio of an AP for creating VAPs.

The **undo radio-profile** unbinds a radio profile from a specified radio.

By default, no radio profile is bound to a radio.

Format

radio-profile { **id** *profile-id* | **name** *profile-name* }

undo radio-profile

Parameters

Parameter	Description	Value
id *profile-id*	Specifies the ID of a radio profile, which identifies a radio profile.	The radio profile ID must exist.
name *profile-name*	Specifies the name of a radio profile, which identifies a radio profile.	The radio profile name must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a radio profile is bound to a radio, parameters defined in the radio profile are applied to the radio. A radio profile defines the following parameters: radio type, radio rate, channel mode, radio power mode, calibration interval, packet loss threshold, error packet threshold, packet conflict threshold, package fragmentation threshold, Request To Send/Clear To Send (RTS/CTS) threshold, maximum retransmission attempts for long/short frames, whether short preamble is supported, delivery traffic indication message (DTIM) interval, beacon frame interval, WMM profile name or ID, GI mode, and A-MPDU parameters. To set these parameters, run the **13.1.27 display radio-profile** command.

When a radio profile is bound to a radio, some parameters may be restored to the default values.

Precautions

A radio profile to be bound to a radio must exist and all parameters are set.

Example

Bind radio profile **huawei** to a radio.

```
<Huawei> system-view
[Huawei] interface wlan-radio0/0/0
[Huawei-Wlan-Radio0/0/0] radio-profile name huawei
```

Related Topics

13.1.38 display vap (for FAT AP)

13.1.56 radio-profile (WLAN view) (for FAT AP)

13.1.27 display radio-profile

13.1.58 reset radio statistics (for FAT AP)

Function

The **reset radio statistics** command clears statistics at the MAC layer of a specified radio

Format

reset radio statistics

Parameters

None

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Clear statistics on the MAC layer of the radio interface.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] reset radio statistics
```

Related Topics

13.1.35 display statistics radio (for FAT AP)

13.1.59 reset station online-fail-record (for FAT AP)

Function

The **reset station online-fail-record** command clears STA online failure records.

Format

reset station online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears online failure records of all STAs.	-
mac *mac-address*	Clears online failure records of the STA with the specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

To re-collect records about STA online failures, run this command to clear existing records.

The cleared records cannot be restored.

Example

Clear online failure records of all STAs.

```
<Huawei> reset station online-fail-record all
```

Related Topics

13.1.36 display station online-fail-record (for FAT AP)

13.1.60 reset wlan record

Function

The **reset wlan record** command clears information about the Probe Request and Beacon frames collected by the device.

NOTE

The AR1220W, AR1220EVW and AR1220VW do not support this command.

Format

reset wlan record

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To re-collect information about Probe Request and Beacon frames collected by the device, run the **reset wlan record** command to clear the existing information first.

Prerequisites

The function of collecting Probe Request and Beacon frames has been enabled.

Example

Clear information about the Probe Request and Beacon frames collected by the device.

```
<Huawei> reset wlan record
```

Related Topics

13.1.63 set wlan record enable

13.1.40 display wlan record

13.1.61 rts-cts-threshold (for FAT AP)

Function

The **rts-cts-threshold** command sets the RTS or CTS threshold in a radio profile.

The **undo rts-cts-threshold** command restores the default RTS or CTS threshold in a radio profile.

The default RTS/CTS alarm threshold is 2347 bytes.

Format

rts-cts-threshold *rts-cts-threshold*

undo rts-cts-threshold

Parameters

Parameter	Description	Value
rts-cts-threshold	Specifies the RTS or CTS threshold. If the length of a frame to be sent by the MAC Layer exceeds this threshold, an RTS frame needs to be sent before this frame.	The value is an integer that ranges from 64 to 2347, in bytes.

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

The IEEE 802.11 MAC protocol provides an RTS/CTS handshake protocol to prevent conflicts between channels and failure to transmit data. STA A sends an RTS frame

 Copyright © Huawei Technologies Co., Ltd.

before sending data to STA B. STA A can send data after receiving a CTS frame from STA B. If multiple STAs send RTS frames to an STA, only the STA that receives a CTS frame can send data, and other STAs have channel conflicts by default and must wait and send RTS frames again.

If STAs implement RTS/CTS handshakes before sending data, the channel bandwidth is consumed by too much RTS frames. You can set an RTS threshold to specify the length of frames to be sent. When the length of frames to be sent by the STA is smaller than the RTS threshold, no RTS/CTS handshake is implemented.

Example

Set the RTS/CTS threshold in radio profile **radio** to 1500 bytes.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name radio
[Huawei-wlan-radio-prof-radio] rts-cts-threshold 1500
```

13.1.62 set wlan collisionrate threshold

Function

The **set wlan collisionrate threshold** command specifies the collision rate threshold for the radio channel.

The **undo set wlan collisionrate threshold** command restores the default collision rate threshold for the radio channel.

The default collision rate threshold is 60%.

NOTE

This command is supported only by models that support the WLAN Fat AP function (that is, the models containing W in their names), excluding the AR109W, AR109GW-L, AR129CVW, AR129CGVW-L, AR169CVW, AR169CVW-4B4S, AR1220W, AR1220EVW, and AR1220VW.

Format

set wlan collisionrate threshold *threshold-value*

undo set wlan collisionrate threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the collision rate threshold for the radio channel.	The value is an integer that ranges from 1 to 100, in percentages.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the MAC layer of a radio does not receive any ACK packet after sending a packet at the lowest rate, it considers that an error occurs. When severe signal interference exists around the AP, you can run the **set wlan collisionrate threshold** command to set the collision rate threshold for the radio channel. When detecting that the collision rate of the radio channel exceeds the threshold, the AP automatically performs radio calibration to switch to a channel with less interference to transmit and receive data, improving AP performance.

Example

Set the collision rate threshold for the radio channel to 70%.

```
<Huawei> system-view
[Huawei] set wlan collisionrate threshold 70
```

13.1.63 set wlan record enable

Function

The **set wlan record enable** command enables the function of collecting Probe Request and Beacon frames on the device.

The **undo set wlan record enable** command disables the function of collecting Probe Request and Beacon frames on the device.

By default, the function of collecting Probe Request and Beacon frames is disabled on the device.

NOTE

The AR1220W, AR1220EVW and AR1220VW do not support this command.

Format

set wlan record { **all** [**log**] | **probe log** | **beacon log** } **enable**

undo set wlan record [**log**] **enable**

Parameters

Parameter	Description	Value
all [**log**]	Collects both Probe Request and Beacon frames. If **log** is specified, the information about the collected Probe Request and Beacon frames is saved to the flash memory in .txt file.	-
probe log	Collects Beacon and Probe Request frames and saves the information about the collected Probe Request frames to the flash memory in .txt file.	-
beacon log	Collects Beacon and Probe Request frames and saves the information about the collected Beacon frames to the flash memory in .txt file.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device functions as a Fat AP to build a wireless network, it receives Probe Request frames from nearby STAs and Beacon frames from nearby Fat APs. These frames contain information about the STAs and Fat APs, such as their MAC addresses and RSSIs.

To analyze and know wireless environments around the device, you can enable the function of collecting Probe Request and Beacon frames on the device using the **set wlan record enable** command.

Precautions

The information about the Beacon and Probe Request frames collected by the device is first saved to the **wlan_probe.txt** file in the flash memory. After ten

saving intervals, the device moves the **wlan_probe.txt** file to the **wlan_probe** folder in the flash memory and names the **wlan_probe.txt** file in the format of **ESN+Time stamp**, for example, **21500101633GE4000288_20150803131429.txt**.

The **wlan_probe** folder can contain a maximum of 50 files. If the number of files exceeds 50, the device deletes the earliest files.

Example

Enable the function of collecting Probe Request and Beacon frames on the device and configure the device to save the information about the collected frames.

```
<Huawei> system-view
[Huawei] set wlan record all log enable
```

Related Topics

13.1.40 display wlan record

13.1.60 reset wlan record

13.1.64 set wlan falsecca threshold

Function

The **set wlan falsecca threshold** command specifies the threshold for the number of clear channel assessment (CCA) detection errors.

The **undo set wlan falsecca threshold** command restores the default threshold for the number of CCA detection errors.

By default, the threshold for the number of CCA detection errors is 3000.

NOTE

This command is supported only by the AR109W, AR109GW-L, AR129CVW, AR129CGVW-L, AR169CVW, and AR169CVW-4B4S.

Format

set wlan falsecca threshold *threshold-value*

undo set wlan falsecca threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the threshold for the number of CCA detection errors.	The value is an integer that ranges from 1 to 10000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CCA mechanism enables the WLAN chip to determine whether the channel is idle before transmitting signals to the air interface. If so, the chip transmits signals. If not, the chip waits until the channel is idle. The CCA threshold allows the WLAN chip to evaluate whether the channel is idle. When the noise strength of the channel exceeds the threshold, the current channel is considered busy. Otherwise, the current channel is considered idle.

When severe signal interference exists around the AP, the physical layer of the AP may encounter an error when performing CCA detection. In this case, you can run the **set wlan falsecca threshold** command to set the threshold for the number of CCA detection errors. When the number of CCA detection errors exceeds the threshold, the AP automatically performs radio calibration to switch to the channel with less interference to transmit and receive data, improving AP performance.

Example

Set the threshold for the number of CCA detection errors to 200.

```
<Huawei> system-view
[Huawei] set wlan falsecca threshold 200
```

13.1.65 set wlan utmost-power

Function

The **set wlan utmost-power enable** command enables the device to send packets at maximum power.

The **set wlan utmost-power disable** command disables the device from sending packets at maximum power.

By default, the device is enabled to send packets at maximum power.

NOTE

This command is supported only by the AR109W, AR109GW-L, AR129CVW, AR129CGVW-L, AR169CVW, and AR169CVW-4B4S.

Format

set wlan utmost-power enable

set wlan utmost-power disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is valid for all country codes. After the **set wlan utmost-power enable** command is run, the device sends packets at maximum power. After the **set wlan utmost-power disable** command is run, the device sends packets at the power based on the country code.

Example

Disable the device from sending packets at maximum power.

```
<Huawei> system-view
[Huawei] set wlan utmost-power disable
```

13.1.66 security-profile (service set view) (for FAT AP)

Function

The **security-profile** command binds a security profile to a specified service set.

The **undo security-profile** command deletes a security profile from a specified service set.

By default, the security profile named **secf** is bound to a service set.

Format

security-profile { **name** *profile-name* | **id** *profile-id* }

undo security-profile

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a security profile.	The security profile name must exist.
id *profile-id*	Specifies the ID of a security profile.	The security profile ID must exist.

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

The administrator can run this command to bind a security profile to a service set. The security profile then applies to all users using this service set.

Example

Create a service set named **ChinaNet**, specify an SSID **ChinaNet-1** for the service set, and bind traffic profile **traffic01** and security profile **security01** to the service set.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] ssid ChinaNet-1
[Huawei-wlan-service-set-ChinaNet] traffic-profile name traffic01
[Huawei-wlan-service-set-ChinaNet] security-profile name security01
```

Related Topics

13.3.21 security-profile (for FAT AP)
13.1.29 display service-set (for FAT AP)

13.1.67 service-set (for FAT AP)

Function

The **service-set** command adds a service set.

The **undo service-set** command deletes one or multiple service sets.

By default, there is no service set in the system.

Format

service-set { **name** *service-set-name* | **id** *service-set-id* } *

undo service-set { **id** *service-set-id* | **name** *service-set-name* }

undo service-set batch id { *service-set-id* [**to** *service-set-id*] } &<1-10>

Parameters

Parameter	Description	Value
name *service-set-name*	Specifies the name of a service set.	The value is a string of 1 to 31 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
batch	Deletes multiple service sets.	The value is a string of 1 to 31 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
id *service-set-id*	Specifies the ID of a service set.	• AR150 series, AR160 series and AR200 series: 0 to 7

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before providing services to a user, create a service set and bind it to a radio. A service set defines service parameters and virtual access point (VAP) attributes. After the service set is bound to a specified radio on an AP, its service parameters are applied to a WLAN service entity, namely, a VAP. The AP then provides users with differentiated WLAN services based on these service parameters.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

A radio profile name is mandatory for creating a radio profile.

Example

Create a service set named **ChinaNet**, specify an SSID **ChinaNet-1** for the service set, and bind traffic profile **traffic01**, and security profile **security01**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] ssid ChinaNet-1
[Huawei-wlan-service-set-ChinaNet] traffic-profile name traffic01
[Huawei-wlan-service-set-ChinaNet] security-profile name security01
```

Related Topics

13.1.29 display service-set (for FAT AP)

13.1.68 service-set (Radio interface view)

Function

Using the **service-set** command, you can bind a service set to a specified ratio of Wlan-Radio to create a VAP.

Using the **undo service-set** command, you can unbind a service set from a specified radio.

By default, no service set is bound to any radio.

Format

service-set { **name** *service-set-name* | **id** *service-set-id* } [**wlan** *wlan-id*]

undo service-set { **id** *service-set-id* | **name** *service-set-name* }

Parameters

Parameter	Description	Value
name *service-set-name*	Specifies the name of a service set.	The service set name must exist.
id *service-set-id*	Specifies the ID of a service set.	The service set ID must exist.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wlan *wlan-id*	Specifies the WLAN index. **NOTE** • If you set a WLAN ID when creating a VAP, the WLAN ID is the ID of a VAP. • If you do not set a WLAN ID when creating a VAP, the system assigns an ID to the VAP.	The value is an integer. The value range varies according to devices: • AR150 series, AR160 series and AR200 series: 1 to 8 • AR1200 series: 1 to 16

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- A service set defines service parameters and VAP attributes. After the service set is bound to a specified radio on Wlan-Radio, its service parameters are applied to a WLAN service entity, namely, a VAP. Wlan-Radio then provides users with differentiated WLAN services based on these service parameters.
- The **service-set** command binds a service set to a specified ratio of Wlan-Radio to create a VAP.

Prerequisite

A traffic profile, security profile, and WLAN-BSS interface have been bound to the service set, and an SSID has been configured.

A radio profile has been bound to the radio interface.

Precautions

Each wlan-radio interface can bind multiple service sets.

Example

Bind a service set **ChinaNet** and WLAN 1 to Wlan-Radio 0/0/0.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-wlan-radio0/0/0] service-set name ChinaNet wlan 1
```

Related Topics

13.1.38 display vap (for FAT AP)
13.1.67 service-set (for FAT AP)
13.1.29 display service-set (for FAT AP)

13.1.69 set workmode wlan (for FAT AP)

Function

The **set workmode wlan** command configures the WLAN mode of the device.

By default, the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW work in AP mode and other devices work in AC mode.

Format

set workmode wlan { **ap** | **ac** }

Parameters

Parameter	Description	Value
ap	Indicates that the device works in Fat AP mode.	-
ac	Indicates that the device works in AC mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Fat AP mode, the device functions as an access point (AP) to provide access control, authentication, data encryption, and QoS functions.

In AC mode, the device functions as the access controller (AC) to deploy and control APs. The AC implements functions including mobility management,

 Copyright © Huawei Technologies Co., Ltd.

identity verification, VLAN assignment, radio resource management, wireless Intrusion Detection System (IDS), and data packet forwarding. APs only send and receive wireless data, simplifying AP management and configuration. APs can even work without any configuration.

Example

Configure the device to work in AP mode.

```
<Huawei> system-view
[Huawei] set workmode wlan ap
Warning: The WorkMode Change will be activated after board reboot. Continue? [y/n]:y
[Huawei] quit
<Huawei> reboot fast
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

13.1.70 short-preamble (for FAT AP)

Function

The **short-preamble** command determines whether the short preamble is supported in a specified radio profile.

The **undo short-preamble** command restores the default settings.

By default, the short preamble is supported in a specified radio profile.

Format

short-preamble { **enable** | **disable** }

undo short-preamble disable

Parameters

Parameter	Description	Value
enable	Indicates that the short preamble is supported.	-
disable	Indicates that the short preamble is not supported.	-

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

The preamble is a section of bits in the header of a data frame. It synchronizes signals transmitted between the sender and receiver. The preamble is classified

into the long preamble and short preamble. The short preamble ensures better synchronization performance and therefore is recommended. The long preamble is usually used for compatibility with earlier network adapters of clients.

Example

Configure radio profile **80211b** to support the short preamble.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name 80211b
[Huawei-wlan-radio-prof-80211b] short-preamble enable
```

13.1.71 smart-carrier-sense enable

Function

The **smart-carrier-sense enable** command enables smart carrier receiver sensitivity adjustment.

The **undo smart-carrier-sense enable** command disables smart carrier receiver sensitivity adjustment.

By default, smart carrier receiver sensitivity adjustment is enabled.

NOTE

Only the AR109W, AR109GW-L, AR129CGVW-L, AR129CVW, AR169CVW-4B4S, and AR169CVW support this command.

Format

smart-carrier-sense enable

undo smart-carrier-sense enable

Parameters

None

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of wireless interference sources exist in the surroundings of AP, the access rate of STAs is decreased. After you run the **smart-carrier-sense enable** command, carrier receiver sensitivity can be adjusted smartly to improve the anti-interference capability of the device.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- The smart carrier receiver sensitivity adjustment function is valid only on the 2.4 GHz frequency band but invalid on the 5 GHz frequency band.
- Modifying parameters of the radio profile will cause online users on the profile to go offline.

Example

Enable carrier receiver sensitivity adjustment.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] radio-profile name rds
[Huawei-wlan-radio-prof-rds] smart-carrier-sense enable
```

Related Topics

13.1.56 radio-profile (WLAN view) (for FAT AP)

13.1.72 ssid (for FAT AP)

Function

The **ssid** command sets a service set identifier (SSID) for a service set.

The **undo ssid** command deletes the SSID of a service set.

By default, no SSID is configured.

Format

ssid *ssid*

undo ssid

Parameters

Parameter	Description	Value
ssid	Specifies the name of an SSID.	The value is a string of 1 to 32 case-insensitive characters. The value cannot contain question marks (?) and cannot start or end with double quotation marks (" ").

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

An SSID specifies a wireless network. When you search for available wireless networks on your laptop, SSIDs are displayed to identify the available wireless networks.

Example

Set the SSID of service set ss1 to company.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ss1
[Huawei-wlan-service-set-ss1] ssid company
```

13.1.73 ssid-hide (for FAT AP)

Function

The **ssid-hide** command hides an SSID in a Beacon frame.

The **undo ssid-hide** command cancels the configuration.

By default, no SSID is hidden in a Beacon frame.

Format

ssid-hide

undo ssid-hide

Parameters

None

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

A STA listens on the Beacon frames that an AP periodically sends in each channel to obtain AP information. The STA can obtain SSIDs from Beacon frames that contain the SSIDs.

The STA can actively send a probe frame with a specified SSID or send a broadcast probe frame without an SSID. When a broadcast probe frame is sent, the STA can join any WLAN network.

After the **ssid-hide** command is executed, an AP periodically sends Beacon frames that contain empty SSID character strings and does not reply to the broadcast probe requests sent from STAs.

After the **undo ssid-hide** command is executed, an AP periodically sends Beacon frames that contain valid SSID character strings and replies to the broadcast probe requests sent from STAs.

Example

Create a service set **ChinaNet** and configure the AP to hide the SSID in Beacon frames.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] ssid-hide
```

13.1.74 ssid-catch (for FAT AP)

Function

The **ssid-catch** command uses Equipment Serial Number (ESN) to form an SSID.

The **undo ssid-catch** command cancels using ESN to form an SSID.

By default, the device directly uses the SSID configured using the **ssid** command but does not use ESN to form an SSID.

Format

ssid-catch device-esn [**length** *esn-len*]

undo ssid-catch

Parameters

Parameter	Description	Value
device-esn	Uses part of ESN to form an SSID.	-

Parameter	Description	Value
length *esn-len*	Specifies the length of ESN to form an SSID. ● If this parameter is not specified, the device uses the whole ESN to form an SSID. For example, if the SSID **huawei** is configured using the **ssid** command, the ESN of the device is 21020000012345000678 9, and *esn-len* is not specified, the device uses the whole ESN to form an SSID (new SSID: **huawei-21020000012345000678 9**). ● If this parameter is specified, the device uses the ESN with the specified *esn-len* to form an SSID. For example, if the SSID **huawei** is configured using the **ssid** command, the ESN of the device is 21020000012345000678 9, and *esn-len* is set to 5, the device uses the last five digits to form an SSID (new SSID: **huawei-06789**).	The value is an integer that ranges from 1 to 32.

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When devices are deployed in batches, the same configuration file is loaded on the devices. As a result, different devices are configured with the same SSID (configured using the **ssid** command), which may affect normal management, operation, and maintenance (O&M) of WLANs.

After the **ssid-catch** command is run, the device uses part of or the whole ESN to form a new SSID. In this way, each device has a unique SSID, meeting management and O&M requirements.

Precautions

An SSID contains a maximum of 32 characters; therefore, the length of the SSID formed using ESN cannot exceed 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the function of using ESN to form an SSID and set the length of ESN to be used to 7.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ss1
[Huawei-wlan-service-set-ss1] ssid-catch device-esn length 7
```

Related Topics

13.1.72 ssid (for FAT AP)

13.1.75 traffic-profile (service set view) (for FAT AP)

Function

The **traffic-profile** command binds a traffic profile to a specified service set.

The **undo traffic-profile** command deletes a traffic profile from a specified service set.

By default, the traffic profile named **traf** is bound to a service set.

Format

traffic-profile { **name** *profile-name* | **id** *profile-id* }

undo traffic-profile

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a traffic profile.	The traffic profile name must exist.
id *profile-id*	Specifies the ID of a traffic profile.	The traffic profile ID must exist.

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

You can run the **traffic-profile** command to bind a traffic profile to a service set. The traffic profile then applies to all users using the service set.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a service set **ChinaNet**, and bind a traffic profile **traffic01** to the service set.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] traffic-profile name traffic01
```

Related Topics

13.2.7 traffic-profile (WLAN view) (for FAT AP)
13.1.29 display service-set (for FAT AP)

13.1.76 wlan (for FAT AP)

Function

The **wlan** command displays the WLAN view.

NOTE

In the WLAN view, modifying the WLAN configuration may cause STAs associated with the current radio to go offline.

Format

wlan [**ap**]

Parameters

Item	Description	Value
ap	FAT AP mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before performing WLAN configurations, run the **wlan** command to enter the WLAN view. All WLAN configuration commands need to be used in the WLAN view or WLAN sub-view. When the **wlan** or **wlan ap** command is executed, you enter the WLAN view in FAT AP mode.

Example

Enter the WLAN view in FAT AP mode.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ap
[Huawei-wlan-view]
```

13.1.77 wlan global country-code

Function

Using the **wlan global country-code** command, you can set a country code for an AP.

The **undo wlan global country-code** command restores the country code to the default values.

By default, the country code of the AP is CN.

Format

wlan global country-code *country-code*

undo wlan global country-code

Parameters

Parameter	Description	Value
country-code	Specifies the AP country code.	The value is a string of characters. Enumerated type. For specific values, see **Table 13-31**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Table 13-31 Country codes supported by APs

Country Code	Country/Region
AE	UNITED ARAB EMIRATES
AM	ARMENIA
AR	ARGENTINA

Country Code	Country/Region
AT	AUSTRIA
AU	AUSTRALIA
AZ	AZERBAIJAN
BE	BELGIUM
BG	BULGARIA
BH	BAHRAIN
BN	BRUNEI DARUSSALAM
BO	BOLIVIA
BR	BRAZIL
BY	BELARUS
BZ	BELIZE
CA	CANADA
CH	SWITZERLAND
CL	CHILE
CN	CHINA (Default)
CO	COLOMBIA
CR	COSTA RICA
CY	CYPRUS
CZ	CZECH REPUBLIC
DE	GERMANY
DK	DENMARK
DO	DOMINICAN REPUBLIC
EC	ECUADOR
EE	ESTONIA
EG	EGYPT
ES	SPAIN
FI	FINLAND
FR	FRANCE
GB	UNITED KINGDOM
GE	GEORGIA

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
GR	GREECE
GT	GUATEMALA
HK	HONG KONG, SPECIAL ADMINISTRATIVE REGION OF CHINA
HN	HONDURAS
HR	CROATIA
HU	HUNGARY
ID	INDONESIA
IE	IRELAND
IL	ISRAEL
IN	INDIA
IQ	IRAQ
IR	IRAN
IS	ICELAND
IT	ITALY
JO	JORDAN
JP	JAPAN
KP	DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA
KR	REPUBLIC OF KOREA
KW	KUWAIT
KZ	KAZAKHSTAN
LB	LEBANON
LI	LIECHTENSTEIN
LK	SRI LANKA
LT	LITHUANIA
LU	LUXEMBOURG
LV	LATVIA
MA	MOROCCO
MC	MONACO
MK	MACEDONIA

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
MO	MACAU, SPECIAL ADMINISTRATIVE REGION OF CHINA
MT	MALTA
MX	MEXICO
MY	MALAYSIA
NG	NIGERIA
NL	NETHERLANDS
NO	NORWAY
NZ	NEW ZEALAND
OM	OMAN
PA	PANAMA
PE	PERU
PH	PHILIPPINES
PK	PAKISTAN
PL	POLAND
PR	PUERTO RICO
PT	PORTUGAL
QA	QATAR
RO	ROMANIA
RU	RUSSIA
SA	SAUDI ARABIA
SE	SWEDEN
SG	SINGAPORE
SI	SLOVENIA
SK	SLOVAKIA
SV	EL SALVADOR
SY	SYRIA
TH	THAILAND
TN	TUNISIA
TR	TURKEY
TT	TRINIDAD & TOBAGO

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
TW	TAIWAN, PROVINCE OF CHINA
UA	UKRAINE
US	UNITED STATES
UY	URUGUAY
UZ	UZBEKISTAN
VE	VENEZUELA
VN	VIET NAM
YE	YEMEN
ZA	SOUTH AFRICA
ZW	ZIMBABWE

NOTE

After the AP country code is modified, all VAPs are automatically deleted and all STAs get offline.

Example

Set the country code of the AP to **CN**.

```
<Huawei> system-view
[Huawei] wlan global country-code CN
```

13.1.78 wlan record log timer

Function

The **wlan record log timer** command sets the interval for saving information about Probe Request and Beacon frames.

The **undo wlan record log timer** command restores the default setting.

By default, the device saves information about the Probe Request and Beacon frames every 10 seconds.

NOTE

The AR1220W, AR1220EVW and AR1220VW do not support this command.

Format

wlan record log timer *interval*

undo wlan record log timer

Parameters

Parameter	Description	Value
interval	Specifies the interval for saving information about Probe Request and Beacon frames.	It is an integer that ranges from 1 to 2592000, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you enable the function of collecting Probe Request and Beacon frames on the device and configure the device to save information about the collected frames to the flash memory using the **set wlan record enable** command, the device saves the collected information every 10 seconds by default. You can run the **wlan record log timer** command to set the interval for saving information about Probe Request and Beacon frames.

Example

Set the interval for saving information about Probe Request and Beacon frames to 100s.

```
<Huawei> system-view
[Huawei] wlan record log timer 100
```

Related Topics

13.1.63 set wlan record enable

13.1.79 wlan-bss (service set view)

Function

Using the **wlan-bss** command, you can bind a WLAN-BSS interface to a service set.

Using the **undo wlan-bss** command, you can unbind a WLAN-BSS interface from a service set.

By default, no WLAN-BSS interface is bound to any service set.

Format

wlan-bss *wlan-bss-number*

undo wlan-bss

Parameters

Parameter	Description	Value
wlan-bss-number	Specifies the number of the WLAN-BSS interface to be bound to a service set.	The value is an integer. The value range varies according to devices: ● AR150 series, AR200 series, AR161FGW-L, AR161FGW-La, AR161FGW-Lc, AR161FW, AR161FW-P-M5, AR161W, AR169FGW-L, AR169FGVW-L, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S and AR169JFVW-2S: 0 to 7 ● AR1200 series, AR161EW, AR161EW-M1, AR169CVW, AR169CVW-4B4S, AR169EW, AR169EGW-L, AR169W-P-M9 and AR169RW-P-M9: 0 to 15

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

Attributes such as the authentication mode and interface priority set on a WLAN-BSS interface take effect only after the interface is bound to a service set.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a service set **ChinaNet** and bind WLAN-BSS interface 1 to it.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] wlan-bss 1
```

13.1.80 wmm-profile (WLAN view) (for FAT AP)

Function

The **wmm-profile** command creates a Wi-Fi Multimedia (WMM) profile and displays the WMM profile view. If the specified WMM profile exists, you can directly enter the specified WMM profile view.

The **undo wmm-profile** command deletes a WMM profile.

By default, the WMM profile named **wmmf** exists in the system.

Format

wmm-profile { **id** *profile-id* | **name** *profile-name* } *

undo wmm-profile { **all** | **id** *profile-id* | **name** *profile-name* }

Parameters

Parameter	Description	Value
id *profile-id*	Specifies the ID of a WMM profile.	The value is an integer. The value range varies according to devices: ● AR150 series, AR200 series: 0 to 7 ● AR100 series, AR120 series and AR160 series: 0 to 15 ● AR1200 series: 0 to 15

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
name *profile-name*	Specifies the name of a WMM profile.	The value is a string of 1 to 31 case-sensitive characters without spaces or question marks (?) and cannot begin or end with double quotation marks (" ").
all	Deletes all WMM profiles	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure a Wi-Fi Multimedia (WMM) profile to implement the WMM protocol that guarantees preferential transmission of packets with a high priority, which ensures better quality for voice and video services on a wireless network.

The **wmm-profile** command applies to the following situations:

- To apply WMM functions to a radio, create a WMM profile and bind it to a radio profile.
- To change WMM functions of a radio, enter the WMM profile view of the radio profile to modify the required parameters.

After a WMM profile is created, the profile retains the default settings.

Follow-up Procedure

Run the **wmm-profile** command to bind the specified WMM profile to a radio profile.

Precautions

A WMM profile cannot be deleted if it is bound to a radio profile.

- The profile name is mandatory when you create a WMM profile. The profile ID is optional. If you do not specify a profile ID, an ID is automatically allocated.
- When entering the created WMM profile view, you can specify either the profile name or profile ID. If you specify both the profile name and profile ID, you can enter the specified WMM profile view only when both the profile

 Copyright © Huawei Technologies Co., Ltd.

name and profile ID are correct. You can specify a profile name or profile ID to delete the specified WMM profile.

Example

Create a WMM profile **p1** and enter the WMM profile view.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] wmm-profile name p1
[Huawei-wlan-wmm-prof-p1]
```

Related Topics

13.1.81 wmm-profile (radio profile view) (for FAT AP)

13.1.81 wmm-profile (radio profile view) (for FAT AP)

Function

The **wmm-profile** command binds a specified Wi-Fi Multimedia (WMM) profile to a radio profile.

The **undo wmm-profile** command unbinds a specified WMM profile from a radio profile.

By default, the WMM profile named **wmmf** is bound to the radio profile named **radiof**.

Format

wmm-profile { **id** *profile-id* | **name** *profile-name* }

undo wmm-profile

Parameters

Parameter	Description	Value
id *profile-id*	Specifies the ID of a WMM profile.	The value is an integer. The value range varies according to devices: • AR150 series, AR200 series: 0 to 7 • AR100 series, AR120 series and AR160 series: 0 to 15 • AR1200 series: 0 to 15

Parameter	Description	Value
name *profile-name*	Specifies the name of a WMM profile.	The value is a string of 1 to 31 case-insensitive characters without question marks (?) and spaces. The value cannot start or end with double quotation marks (" ").

Views

Radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To apply WMM functions to a radio, create an MM profile and bind it to a radio profile.

Prerequisites

A WMM profile has been created using the **13.1.80 wmm-profile (WLAN view) (for FAT AP)** command.

Example

Bind WMM profile **p1** to radio profile **802.11b**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] wmm-profile name p1
[Huawei-wlan-wmm-prof-p1] quit
[Huawei-wlan-view] radio-profile name 802.11b
[Huawei-wlan-radio-prof-802.11b] wmm-profile name p1
```

Related Topics

13.1.80 wmm-profile (WLAN view) (for FAT AP)

13.1.27 display radio-profile

13.2 WLAN QoS Configuration Commands

13.2.1 8021p (for FAT AP)

Function

The **8021p** command sets mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets when data packets are sent from STAs to an AP.

The **undo 8021p** command restores the default mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets when data packets are sent from STAs to an AP.

By default, mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets are shown in **Table 13-32**.

Table 13-32 Default mappings from user priorities of 802.11 packets to 802.1p priorities of 802.3 packets

User-Priority	802.1p
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Format

8021p designate *value*

8021p up-mapping *value0 value1 value2 value3 value4 value5 value6 value7*

undo 8021p

Parameters

Parameter	Description	Value
designate *value*	Indicates that user priorities of all 802.11 packets are mapped to a specified 802.1p priority of 802.3 packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
up-mapping	Indicates that user priorities of 802.11 packets are mapped to different 802.1p priorities of 802.3 packets.	-
value0	Specifies the 802.1p priority that maps user priority 0.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value1	Specifies the 802.1p priority that maps user priority 1.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value2	Specifies the 802.1p priority that maps user priority 2.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value3	Specifies the 802.1p priority that maps user priority 3.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value4	Specifies the 802.1p priority that maps user priority 4.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value5	Specifies the 802.1p priority that maps user priority 5.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value6	Specifies the 802.1p priority that maps user priority 6.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value7	Specifies the 802.1p priority that maps user priority 7.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 packets use different fields to identify their priorities. 802.11 packets sent from WMM-capable STAs carry user priorities (user priority field) and 802.3 VLAN packets transmitted on the Ethernet carry 802.1p priorities (CoS field). When STAs send 802.11 packets to an AP, the AP converts the 802.11 packets into 802.3 packets. To ensure the service quality for 802.3 packets, user priorities in 802.11 packets must be mapped to 802.1p priorities in 802.3 packets to provide differentiated services to packets of different priorities.

Use either of the following methods to set the mapping mode.

- If you want to distinguish service priorities of 802.3 packets, run the **8021p up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* command to map user priorities of 802.11 packets to different 802.1p priorities of 802.3 packets.
- If you do not want to distinguish service priorities of 802.3 packets, run the **8021p designate** *value* command to map user priorities of all 802.11 packets to a specified 802.1p priority of 802.3 packets.

Example

Set the 802.1p priority in traffic profile **p1** to a specified value.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] 8021p designate 7
```

Set mappings from user priorities to 802.1p priorities in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] 8021p up-mapping 7 6 5 4 3 2 1 0
```

Related Topics

13.2.7 traffic-profile (WLAN view) (for FAT AP)

13.2.3 display traffic-profile (for FAT AP)

13.2.2 8021p-map-up (for FAT AP)

Function

The **8021p-map-up** command sets mappings from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets when data packets are sent from the Internet to an AP.

 Copyright © Huawei Technologies Co., Ltd.

The **undo 8021p-map-up** command restores the default mappings from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets when data packets are sent from the Internet to an AP.

By default, mappings from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets are shown in **Table 13-33**.

Table 13-33 Mappings from 802.1p priorities of 802.3 packets to user priorities of 802.11 packets

802.1p	User-Priority
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Format

8021p-map-up *value0 value1 value2 value3 value4 value5 value6 value7*

undo 8021p-map-up

Parameters

Parameter	Description	Value
value0	Specifies the user priority that maps 802.1p priority 0.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value1	Specifies the user priority that maps 802.1p priority 1.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
value2	Specifies the user priority that maps 802.1p priority 2.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value3	Specifies the user priority that maps 802.1p priority 3.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value4	Specifies the user priority that maps 802.1p priority 4.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value5	Specifies the user priority that maps 802.1p priority 5.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value6	Specifies the user priority that maps 802.1p priority 6.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
value7	Specifies the user priority that maps 802.1p priority 7.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 packets use different fields to identify their priorities. 802.11 packets sent from WMM-capable STAs carry user priorities (user priority field) and 802.3 VLAN packets transmitted on the Ethernet carry 802.1p priorities (CoS field). When data packets are sent from upper-layer network to APs, 802.3 packets must

 Copyright © Huawei Technologies Co., Ltd.

be converted into 802.11 packets. You can run the **8021p-map-up** command to map 802.1p priorities of 802.3 packets to user priorities of 802.11 packets.

Example

Configure mappings from 802.1p priorities to user priorities in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] 8021p-map-up 7 6 5 4 3 2 1 0
```

Related Topics

13.2.7 traffic-profile (WLAN view) (for FAT AP)
13.2.3 display traffic-profile (for FAT AP)

13.2.3 display traffic-profile (for FAT AP)

Function

The **display traffic-profile** command displays the traffic profile configuration.

Format

display traffic-profile { **all** | **id** *profile-id* | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays the configurations of all traffic profiles.	-
id *profile-id*	Displays the configuration of a traffic profile with a specified ID.	The traffic profile ID must exist.
name *profile-name*	Displays the configuration of a traffic profile with a specified name.	The traffic profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the default configuration of a new traffic profile or the configuration of a configured traffic profile.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the configuration of traffic profile 0.

```
<Huawei> display traffic-profile id 0
  Profile ID          : 0
  Profile name        : lw
  Client Limit Rate  : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  VAP Limit Rate     : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  802.1p Mapping Mode: mapping
  ----------------------------
  User-priority  802.1p
  0              0
  1              1
  2              2
  3              3
  4              4
  5              5
  6              6
  7              7
  ----------------------------
  802.1p to User-priority Mapping List:
  ----------------------------
  802.1p  User-priority
  0       0
  1       1
  2       2
  3       3
  4       4
  5       5
  6       6
  7       7
  ----------------------------
  Service-set bind the traffic-profile:
  -----------------------------------------------------
    0
  -----------------------------------------------------
  Total: 1
```

Table 13-34 Description of the display traffic-profile command output

Item	Description
Profile ID	Traffic profile ID. To set the traffic profile ID, run the **13.2.7 traffic-profile (WLAN view) (for FAT AP)** command.
Profile name	Traffic profile name. To set the traffic profile name, run the **13.2.7 traffic-profile (WLAN view) (for FAT AP)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Client Limit Rate	Rate limit configured for STAs. ● up: indicates rate limit for upstream packets of the STAs. ● down: indicates rate limit for downstream packets of the STAs. To set the rate limit for STAs, run the **13.2.6 rate-limit client (for FAT AP)** command.
VAP Limit Rate	Rate limit configured for VAPs. ● up: indicates rate limit for upstream packets of the VAPs. ● down: indicates rate limit for downstream packets of the VAPs. To set the rate limit for VAPs, run the **13.2.5 rate-limit vap (for FAT AP)** command.
802.1p Mapping Mode	Mappings from user priorities to 802.1p priorities. ● designate(x): maps user priorities to a specified 802.1p priority. x indicates the 802.1p priorities. ● mapping: maps user priorities to different 802.1p priorities. To mappings from user priorities to 802.1p priorities, run the **13.2.1 8021p (for FAT AP)** command.
802.1p to User-priority Mapping List	Mappings from 802.1p priorities to user priorities. To mappings from 802.1p priorities to user priorities, run the **13.2.2 8021p-map-up (for FAT AP)** command.
Service-set bind the traffic-profile	ID of a service set bound to the traffic profile. To set the ID of a service set bound to the traffic profile, run the **traffic-profile** command.

Display the configurations of all traffic profiles.

```
<Huawei> display traffic-profile all
  --------------------------------------------------
  ID     Name
 --------------------------------------------------
  0      lw
```

```
-----------------------------------------------------
 Total: 1
```

Table 13-35 Description of the display traffic-profile all command output

Item	Description
ID	Traffic profile ID. To set the traffic profile ID, run the **13.2.7 traffic-profile (WLAN view) (for FAT AP)** command.
Name	Traffic profile name. To set the traffic profile name, run the **13.2.7 traffic-profile (WLAN view) (for FAT AP)** command.

Related Topics

13.2.7 traffic-profile (WLAN view) (for FAT AP)

13.2.4 display wmm-profile (for FAT AP)

Function

The **display wmm-profile** command displays the WMM profile configuration.

Format

display wmm-profile { **all** | **id** *profile-id* | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays the configurations of all WMM profiles.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
id *profile-id*	Displays the configuration of a WMM profile with a specified ID.	The value is an integer. The value range varies according to devices: ● AR150 series, AR200 series: 0 to 7 ● AR100 series, AR120 series and AR160 series: 0 to 15 ● AR1200 series: 0 to 15
name *profile-name*	Displays detailed information about a WMM profile with a specified name.	The value of *profile-name* is a character string of 1 to 31 characters without spaces or question marks (?). The character string cannot start or end with a quotation mark ('').

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the default configuration of a new WMM profile or the configuration of a configured WMM profile.

Example

Display detailed information about WMM profile 0.

```
<Huawei> display wmm-profile id 0
  Profile ID      : 0
  Profile name    : lw
  WMM switch      : enable
  Mandatory switch: disable
  Client EDCA parameters:
  --------------------------------------------------
        ECWmax  ECWmin  AIFSN  TXOPLimit
```

```
AC_VO  3      2      2     47
AC_VI  4      3      2     94
AC_BE  10     4      3     0
AC_BK  10     4      7     0
--------------------------------------------------
AP EDCA parameters:
--------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO  3      2      1     47         normal
AC_VI  4      3      1     94         normal
AC_BE  6      4      3     0          normal
AC_BK  10     4      7     0          normal
--------------------------------------------------
Radio-profile(s) bind the wmm-profile:
--------------------------------------------------
  0       1       2       3
--------------------------------------------------
Total: 4
```

Table 13-36 Description of the display wmm-profile command output

Item	Description
Profile ID	WMM profile ID. To set the WMM profile ID, run the **13.1.80 wmm-profile (WLAN view) (for FAT AP)** command.
Profile name	WMM profile name. To set the WMM profile name, run the **13.1.80 wmm-profile (WLAN view) (for FAT AP)** command.
WMM switch	Whether WMM is enabled. To enable WMM, run the **13.2.10 wmm enable (for FAT AP)** command.
Mandatory switch	Whether STAs that do not support WMM are allowed to connect to a WMM-capable AP To allow STAs that do not support WMM to connect to a WMM-capable AP, run the **13.2.11 wmm mandatory enable (for FAT AP)** command.
Client EDCA parameters	EDCA parameters for STAs. To set EDCA parameters for STAs, run the **13.2.9 wmm edca client (for FAT AP)** command.
AP EDCA parameters	EDCA parameters for APs. To set EDCA parameters for APs, run the **13.2.8 wmm edca ap (for FAT AP)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AC_VO	Voice access category. To set the voice access category, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.
AC_VI	Video access category. To set the video access category, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.
AC_BE	Best effort access category. To set the best effort access category, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.
AC_BK	Background access category. To set the background access category, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.
ECWmax	Exponent form of the maximum contention window. To set the exponent form of the maximum contention window, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.
ECWmin	Exponent form of the minimum contention window. To set the exponent form of the minimum contention window, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.
AIFSN	Arbitration inter frame spacing number. To set the arbitration inter frame spacing number, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TXOPLimit	Transmission opportunity limit. To set the transmission opportunity limit, run the **13.2.9 wmm edca client (for FAT AP)** and **13.2.8 wmm edca ap (for FAT AP)** commands.
Ack-Policy	ACK policy. To set the ACK policy, run the **13.2.8 wmm edca ap (for FAT AP)** command.
Radio-profile(s) bind the wmm-profile	ID of a radio profile bound to the WMM profile. To set the ID of a radio profile bound to the WMM profile, run the **13.1.81 wmm-profile (radio profile view) (for FAT AP)** command.

Display the configurations of all WMM profiles.

```
<Huawei> display wmm-profile all
  -----------------------------------------------------
   ID     Name
  -----------------------------------------------------
   0      lw
  -----------------------------------------------------
   Total: 1
```

Table 13-37 Description of the display wmm-profile all command output

Item	Description
ID	WMM profile ID. To set the WMM profile ID, run the **13.1.80 wmm-profile (WLAN view) (for FAT AP)** command.
Name	WMM profile name. To set the WMM profile name, run the **13.1.80 wmm-profile (WLAN view) (for FAT AP)** command.

Related Topics

13.1.80 wmm-profile (WLAN view) (for FAT AP)

 Copyright © Huawei Technologies Co., Ltd.

13.2.5 rate-limit vap (for FAT AP)

Function

The **rate-limit vap** command sets the rate limit for upstream and downstream traffic on all STAs in a VAP.

The **undo rate-limit vap** command restores the default rate limit for upstream and downstream traffic on all STAs in a VAP.

By default, the rate limit for upstream and downstream traffic on all STAs in a VAP is 4294967295, in kbit/s.

Format

rate-limit vap { **up** | **down** } *rate-limit-value*

undo rate-limit vap { **up** | **down** }

Parameters

Parameter	Description	Value
up	Limits the rate of upstream traffic in a VAP.	-
down	Limits the rate of downstream traffic in a VAP.	-
rate-limit-value	Specifies the limit rate of traffic.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **rate-limit vap** command to limit the rate of upstream and downstream traffic on all STAs in a VAP to protect network bandwidth resources.

Precautions

The rate limit set using the **rate-limit vap** command must be not smaller than that set using the **13.2.6 rate-limit client (for FAT AP)** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the rate limit of upstream traffic on all STAs in a VAP bound to traffic profile **p1** to 64 kbit/s.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] rate-limit vap up 64
```

Related Topics

13.2.7 traffic-profile (WLAN view) (for FAT AP)

13.2.3 display traffic-profile (for FAT AP)

13.2.6 rate-limit client (for FAT AP)

Function

The **rate-limit client** command sets the rate limit for upstream and downstream traffic on each STA in a VAP.

The **undo rate-limit client** command restores the default rate limit for upstream and downstream traffic on each STA in a VAP.

By default, the rate limit for upstream and downstream traffic on each STA in a VAP is 4294967295, in kbit/s.

Format

rate-limit client { **up** | **down** } *rate-limit-value*

undo rate-limit client { **up** | **down** }

Parameters

Parameter	Description	Value
up	Limits the rate of upstream traffic on a STA.	-
down	Limits the rate of downstream traffic on a STA.	-
rate-limit-value	Specifies the limit rate of traffic.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.

Views

Traffic profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **rate-limit client** command to limit the rate of upstream and downstream traffic on each STA in a VAP to protect network bandwidth resources.

Precautions

The rate limit set using the **rate-limit client** command cannot be larger than that set using the **13.2.5 rate-limit vap (for FAT AP)** command.

Example

Set the rate limit of upstream traffic on each STA in a VAP bound to traffic profile **p1** to 64 kbit/s.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] rate-limit client up 64
```

Related Topics

13.2.7 traffic-profile (WLAN view) (for FAT AP)

13.2.3 display traffic-profile (for FAT AP)

13.2.7 traffic-profile (WLAN view) (for FAT AP)

Function

The **traffic-profile** command creates a traffic profile and displays the traffic profile view. If the specified traffic profile exists, you can directly enter the specified traffic profile view.

The **undo traffic-profile** command deletes a traffic profile. The traffic profile bound to a service set cannot be deleted.

By default, the traffic profile named **traf** exists in the system.

Format

traffic-profile { **name** *profile-name* | **id** *profile-id* } *

undo traffic-profile { **all** | **name** *profile-name* | **id** *profile-id* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
id *profile-id*	Specifies the ID of a traffic profile.	The value is an integer that ranges from 0 to 15.
name *profile-name*	Specifies the name of a traffic profile.	The value is a string of 1 to 31 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all traffic profiles.	–

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

- The **traffic-profile** command applies to the following situations:
  - To apply the priority mapping and traffic suppression functions to a VAP, create a traffic profile and bind the traffic profile to a service set.
  - To change the priority mapping and traffic suppression functions of a VAP, enter the traffic profile view of the VAP to modify the required parameters. When a traffic profile is not required, delete it.
- After a traffic profile is created, the profile retains the default settings. For details about the default settings, see the **rate-limit client**, **rate-limit vap**, **8021p**, and **8021p-map-up** commands.

NOTE

- The profile name is mandatory when you create a traffic profile. The profile ID is optional. If you do not specify a profile ID, an ID is automatically allocated.
- When entering the created traffic profile view, you can specify either the profile name or profile ID. If you specify both the profile name and profile ID, you can enter the specified traffic profile view only when both the profile name and profile ID are correct.
- You can specify a profile name or profile ID to delete the specified profile.
- The traffic profile bound to a service set cannot be deleted.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a traffic profile **p1** and enter the traffic profile view.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1]
```

Related Topics

13.2.3 display traffic-profile (for FAT AP)

13.2.6 rate-limit client (for FAT AP)

13.2.5 rate-limit vap (for FAT AP)

13.2.1 8021p (for FAT AP)

13.2.2 8021p-map-up (for FAT AP)

13.2.8 wmm edca ap (for FAT AP)

Function

The **wmm edca ap** command sets EDCA parameters and ACK policies for an AP.

The **undo wmm edca ap** command restores the default EDCA parameters and ACK policies for an AP.

Table 13-38 lists the default EDCA parameter settings and ACK policy for APs.

Table 13-38 Default EDCA parameter settings and ACK policy for APs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	3	2	1	47	normal
AC_VI	4	3	1	94	normal
AC_BE	6	4	3	0	normal
AC_BK	10	4	7	0	normal

Format

wmm edca ap { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *

undo wmm edca ap

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the AIFSN, which determines the channel idle time.	The value is an integer that ranges from 1 to 15.
ecwmin *ecwmin-value*	Specifies the ECWmin. ECWmin and ECWmax determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be smaller than the ECWmax value.
ecwmax *ecwmax-value*	Specifies the ECWmax. ECWmax and ECWmin determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be larger than the ECWmin value.
txoplimit *txoplimit-value*	Specifies the TXOPLimit. The value determines the maximum duration in which an AP or a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the TXOPLimit value is 0, the STA can send only one data frame every time it occupies a channel.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ack-policy { **normal** | **noack** }	Specifies an ACK policy. • **normal**: During 802.11 packet exchange, The receiver must return an ACK packet each time it receives a packet from the sender. • **noack**: The receiver does not need to send an ACK message when it receives a packet from the sender. The **noack** is applicable to scenarios with good communication quality and little interference.	-

Views

WMM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide different priorities to the packets. In this way, APs have different capabilities to compete for channels and provide differentiated services.

Precautions

- EDCA parameters of the four ACs take effect only after WMM is enabled using the **13.2.10 wmm enable (for FAT AP)** command.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.

Example

Set EDCA parameters and an ACK policy for the AC_VO queue of an AP in WMM profile **p1**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] wmm-profile name p1
[Huawei-wlan-wmm-prof-p1] wmm edca ap ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0 ack-policy normal
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

13.2.4 display wmm-profile (for FAT AP)

13.2.9 wmm edca client (for FAT AP)

Function

The **wmm edca client** command sets EDCA parameters for a STA.

The **undo wmm edca client** command restores the default EDCA parameters for a STA.

Table 13-39 lists the default EDCA parameter settings for STAs.

Table 13-39 Default EDCA parameter settings for STAs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit
AC_VO	3	2	2	47
AC_VI	4	3	2	94
AC_BE	10	4	3	0
AC_BK	10	4	7	0

Format

wmm edca client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo wmm edca client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the AIFSN, which determines the channel idle time.	The value is an integer that ranges from 1 to 15.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ecwmin *ecwmin-value*	Specifies the ECWmin. ECWmin and ECWmax determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be smaller than the ECWmax value.
ecwmax *ecwmax-value*	Specifies the ECWmax. ECWmax and ECWmin determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be larger than the ECWmin value.
txoplimit *txoplimit-value*	Specifies the TXOPLimit. The value determines the maximum duration in which an AP or a STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is 32 microseconds. **NOTE** If the TXOPLimit value is 0, the STA can send only one data frame every time it occupies a channel.

Views

WMM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide different priorities to the packets. In this way, STAs have different capabilities to compete for channels and provide differentiated services.

Table 13-40 describes the EDCA parameters.

 Copyright © Huawei Technologies Co., Ltd.

Table 13-40 EDCA parameter description

Parameter	Meaning
Arbitration Inter Frame Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.
Exponent form of CWmin (ECWmin) and Exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. They determine the average backoff time. Large ECWmin and ECWmax values mean that the average backoff time for the STA is long and the STA priority is low.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can send only one data frame every time it preempts a channel.

Precautions

- EDCA parameters of the four ACs take effect only after WMM is enabled using the **13.2.10 wmm enable (for FAT AP)** command.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.

Example

Set EDCA parameters for the AC_VO queue of a STA in WMM profile **p1**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] wmm-profile name p1
[Huawei-wlan-wmm-prof-p1] wmm edca client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0
```

Related Topics

13.2.4 display wmm-profile (for FAT AP)

13.2.10 wmm enable (for FAT AP)

Function

The **wmm enable** command enables WMM in a WMM profile.

The **undo wmm enable** command disables WMM from a WMM profile.

By default, WMM is enabled.

Format

wmm enable

undo wmm enable

Parameters

None

Views

WMM profile view

Default Level

2: Configuration level

Usage Guidelines

Precautions

Parameters in a WMM profile can be set only after WMM is enabled in the WMM profile using the **wmm enable** command.

The **undo legacy-station enable** and **undo wmm enable** commands cannot be configured at the same time, otherwise, any STA cannot access the WLAN.

Example

Enable WMM in WMM profile **p1**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] wmm-profile name p1
[Huawei-wlan-wmm-prof-p1] wmm enable
```

Related Topics

13.1.80 wmm-profile (WLAN view) (for FAT AP)
13.2.4 display wmm-profile (for FAT AP)

13.2.11 wmm mandatory enable (for FAT AP)

Function

The **wmm mandatory enable** disables STAs that do not support WMM from connecting to a WMM-enabled AP.

The **undo wmm mandatory enable** allows STAs that do not support WMM to connect to a WMM-enabled AP.

By default, STAs that do not support WMM are allowed to connect to a WMM-enabled AP.

 Copyright © Huawei Technologies Co., Ltd.

Format

wmm mandatory enable

undo wmm mandatory enable

Parameters

None

Views

WMM profile view

Default Level

2: Configuration level

Usage Guidelines

On a WLAN, wireless channels are open and all STAs have the same chance to occupy a channel. You can configure WMM to distinguish high-priority packets and enable the high-priority packets to preempt channels. You can also disable STAs that do not support WMM from connecting to a WMM-enabled AP, which prevents those STAs from preempting channels of WMM-capable STAs.

Example

Disable STAs that do not support WMM to connect to a WMM-enabled AP.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] wmm-profile name p1
[Huawei-wlan-wmm-prof-p1] wmm mandatory enable
```

Related Topics

13.2.4 display wmm-profile (for FAT AP)

13.3 WLAN Security Configuration Commands

13.3.1 attack detection enable (for FAT AP)

Function

The **attack detection enable** command enables attack detection on a specified AP radio interface.

The **undo attack detection enable** command disables attack detection on a specified AP radio interface.

By default, attack detection is disabled on an AP radio interface.

Format

attack detection enable { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

undo attack detection enable { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

Parameters

Parameter	Description	Value
all	Indicates that all attack detection functions are enabled.	-
flood	Indicates that flood attack detection is enabled.	-
weak-iv	Indicates that weak IV attack detection is enabled.	-
spoof	Indicates that spoofing attack detection is enabled.	-
wpa-psk	Indicates that detection of brute force password cracking is enabled for WPA-PSK authentication.	-
wpa2-psk	Indicates that detection of brute force password cracking is enabled for WPA2-PSK authentication.	-
wapi-psk	Indicates that detection of brute force password cracking is enabled for WAPI-PSK authentication.	-
wep-share-key	Indicates that detection of brute force password cracking is enabled for shared key authentication.	-

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To detect malicious or unintentional attacks on WLANs in real time, network administrators can enable the following attack detection functions based on actual requirements and monitor or prevent these attacks:

 Copyright © Huawei Technologies Co., Ltd.

- flood: detects whether an AP receives a large number of packets of a certain type in a short period.
- weak-iv: detects whether weak IV is used on a WLAN that is currently configured with a WEP security policy.
- spoof: detects whether a potential attacker forges an AP to send broadcast packets to disassociate a client from the authentication server and an AP from the AC.
- wpa-psk, wpa2-psk, wapi-psk, wep-share-key: If WPA-PSK, WPA2-PSK, WAPI-PSK, and WEP-SK security policies are configured on a WLAN, detection of brute force password cracking can be enabled to increase the time required for password cracking and improve password security.

Follow-up Procedure

Run the **13.3.15 dynamic-blacklist enable (for FAT AP)** command to enable the dynamic blacklist function.

Example

Enable flood attack detection on radio interface 0/0/0.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] attack detection enable flood
```

Related Topics

13.3.10 display wlan ids attack-detected (for FAT AP)

13.3.2 attack detection flood (for FAT AP)

Function

The **attack detection flood** command specifies the interval for flood attack detection and the maximum number of packets of the same type that an AP can receive within the interval.

The **undo attack detection flood** command restores the interval for flood attack detection and the maximum number of packets of the same type that an AP can receive within the interval to the default values.

By default, the interval for flood attack detection is 60 seconds and an AP can receive a maximum of 300 packets of the same type within the interval.

Format

attack detection flood interval *intvalue* **times** *timesvalue*

undo attack detection flood

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval *intvalue*	Specifies the interval for flood attack detection.	The value is an integer that ranges from 10 to 120, in seconds.
times *timesvalue*	Specifies the number of packets of the same type that an AP receives within the detection interval.	The value is an integer that ranges from 1 to 1000.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a flood attack, an AP receives a large number of packets of the same type in a short period and it is too busy with the flood attack packets to process packets sent from authorized STAs.

In flood attack detection included in the Wireless Intrusion Detection System (WIDS) attack detection, an AP continuously monitors the number of packets of the same type that are sent to it from each STA and compares the number with the value specified using the **attack detection flood** command. If the number of received packets exceeds the value, the AP determines that the STA is attacking. When the packet number exceeds the maximum number tolerable, the AP considers that the STA intends to launch a flood attack and locks the STA. If the dynamic blacklist function is enabled, the STA is added to the dynamic blacklist.

Follow-up Procedure

Run the **13.3.15 dynamic-blacklist enable (for FAT AP)** command to enable the dynamic blacklist function.

Example

Set the interval for flood attack detection to 120 seconds and the maximum number of packets of the same type that an AP can receive within the interval to 350.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] attack detection flood interval 120 times 350
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

13.1.17 display ap (for FAT AP)
13.3.1 attack detection enable (for FAT AP)
13.3.15 dynamic-blacklist enable (for FAT AP)

13.3.3 attack detection psk (for FAT AP)

Function

The **attack detection psk** command specifies the interval for brute force preshared key (PSK) cracking detection and the number of key negotiation attempts allowed within the interval.

The **undo attack detection psk** command restores the interval for brute force PSK cracking detection and the number of key negotiation attempts allowed within the interval to the default values.

By default, the interval for brute force PSK cracking detection is 60 seconds and an AP allows a maximum of 20 key negotiation attempts within the interval.

Format

attack detection psk interval *intvalue* **times** *timesvalue*

undo attack detection psk

Parameters

Parameter	Description	Value
interval *intvalue*	Specifies the interval for brute force PSK cracking detection.	The value is an integer that ranges from 10 to 120, in seconds.
times *timesvalue*	Specifies the number of key negotiation attempts within the interval.	The value is an integer that ranges from 1 to 100.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Brute force PSK cracking means that an attacker tries all possible PSK combinations one by one and finally obtains the right key. To improve key security,

 Copyright © Huawei Technologies Co., Ltd.

enable defense against brute force PSK cracking to prolong the time used to decrypt passwords.

An AP checks whether the number of key negotiation attempts during WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key authentication exceeds the threshold configured using the **attack detection psk** command. If so, the AP considers that a user is using the brute force method to decrypt the password. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets of the user until the dynamic blacklist entry ages.

Follow-up Procedure

Run the **13.3.15 dynamic-blacklist enable (for FAT AP)** command to enable the dynamic blacklist function.

Example

Set the interval for brute force PSK cracking detection is 60 seconds and an AP allows a maximum of 60 key negotiation attempts within the interval.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] attack detection psk interval 60 times 60
```

Related Topics

13.1.17 display ap (for FAT AP)

13.3.1 attack detection enable (for FAT AP)

13.3.15 dynamic-blacklist enable (for FAT AP)

13.3.4 attack detection quiet-time (for FAT AP)

Function

The **attack detection quiet-time** command sets the quiet time for an AP to report attack records.

The **undo attack detection quiet-time** command restores the default quiet time.

By default, the quiet time is 600 seconds.

Format

attack detection { **flood** | **weak-iv** | **spoof** | **psk** } **quiet-time** *quiet-time-value*

undo attack detection { **flood** | **weak-iv** | **spoof** | **psk** } **quiet-time**

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time.	The value is an integer that ranges from 60 to 36000, in seconds.

Parameter	Description	Value
flood	Indicates flood attack detection.	-
weak-iv	Indicates weak IV attack detection.	-
spoof	Indicates spoofing attack detection.	-
psk	Indicates PSK brute force attack detection.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If a attack source launches attacks repeatedly, a large number of repetitive attacks are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Example

Set the quiet time for reporting flood attacks to 300 seconds.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] attack detection flood quiet-time 300
```

Related Topics

13.1.17 display ap (for FAT AP)

13.3.5 display security-profile (for FAT AP)

Function

The **display security-profile** command displays the security profile configuration.

Format

display security-profile { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] }

Parameters

Parameter	Description	Value
all	Displays configurations of all security profiles.	-
id *profile-id*	Specifies the ID of a security profile.	The security profile ID must exist.
name *profile-name*	Specifies the name of a security profile.	The security profile name must exist.
detail	Displays detailed information about a security profile.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

- You can run this command to view the configuration of access security.
- When there is a large amount of configuration information, output information is displayed on multiple screens.

Example

Display configurations of all security profiles.

```
<Huawei> display security-profile all
  -----------------------------------------------------------
  ID          Name
  0           lw
  1           ttt
  -----------------------------------------------------------
  Total: 2
```

Display brief information about security profile 0.

```
<Huawei> display security-profile id 0
  -----------------------------------------------------------
  Profile name                    : lw
  Profile ID                      : 0
  Authentication                  : Share key
  Encryption                      : WEP-40
  -----------------------------------------------------------
  Service-set ID                  SSID
  0                               l00129796_9300
```

```
1                              l00129796_93002
-----------------------------------------------------------------
```

Display detailed information about security profile 0.

```
<Huawei> display security-profile id 0 detail
  -----------------------------------------------------------------
  Profile name                      : test
  Profile ID                        : 0
  Authentication                    : Open system
  Encryption                        : -
  -----------------------------------------------------------------
  Service-set ID                    SSID
  0                              service-set
  -----------------------------------------------------------------
  WEP's configuration
  Authentication                    : Open system
  Encryption                        : -
  Key 0                             : *****
  Key 1                             : Empty
  Key 2                             : Empty
  Key 3                             : Empty
  Default key ID                    : 0
  -----------------------------------------------------------------
  WPA's configuration
  Authentication                    : WPA  PSK
  Encryption                        : CCMP
  -----------------------------------------------------------------
  WPA2's configuration
  Authentication                    : WPA2 PSK
  Encryption                        : CCMP
  -----------------------------------------------------------------
  WAPI's configuration
  CA certificate filename           : -
  ASU certificate filename          : -
  Certificate filename              : -
  Private key filename              : -
  Authentication server IP          : -
  Authentication method             : WAPI certificate
  WAI timeout(s)                    : 60
  BK update interval(s)             : 43200
  BK lifetime threshold(%)          : 70
  USK update interval(s)            : 86400
  USK update packet(k)              : 10
  MSK update interval(s)            : 86400
  MSK update packet(k)              : 10
  Cert auth retrans count           : 3
  USK negotiate retrans count       : 3
  MSK negotiate retrans count       : 3
  USK update method                 : Time-based
  MSK update method                 : Time-based
  -----------------------------------------------------------------
```

Table 13-41 Description of the **display security-profile** command output

Item	Description
Profile name	Name of the security profile.
Profile ID	ID of the security profile.

Item	Description
Authentication	Authentication mode. The following authentication modes are supported: WLAN Authentication and Privacy Infrastructure (WAPI) certificate authentication, WAPI pre-shared key authentication, Wi-Fi Protected Access (WPA) 802.1x authentication, WPA pre-shared key authentication, WPA2 802.1x authentication, WPA2 pre-shared key authentication, shared key authentication, and open system authentication.
Encryption	Encryption mode. The following encryption mode is supported: Temporal Key Integrity Protocol (TKIP), CTR with CBC-MAC Protocol (CCMP), and Wired Equivalent Privacy (WEP) using a 40-bit or 104-bit key.
SSID	Service set identifier that identifies a WLAN.
Key X	Key ID.
Default key ID	Default key ID.
CA certificate filename	CA certificate file name.
ASU certificate filename	File name of the authentication server unit (ASU) certificate.
Certificate filename	Certificate file name.
Private key filename	Private key file name.
Authentication server IP	IP address of the ASU certificate server.
Authentication method	Authentication mode.
WAI timeout(s)	Timeout period of an association.
BK update interval(s)	Interval for updating the base key (BK).
BK lifetime threshold(%)	Threshold for triggering BK update.
USK update interval(s)	Time-based interval for updating the unicast session key (USK).
USK update packet(k)	Packet count-based interval for updating the USK.
MSK update interval(s)	Time-based interval for updating the MBMS service key (MSK).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MSK update packet(k)	Packet count-based interval for updating the MSK.
Cert auth retrans count	Number of retransmissions of certificate authentication packets.
USK negotiate retrans count	Number of retransmissions of USK negotiation packets.
MSK negotiate retrans count	Number of retransmissions of MSK negotiation packets.
USK update method	Whether the USK is updated based on a time interval or a packet count.
MSK update method	Whether the MSK is updated based on a time interval or a packet count.

13.3.6 display sta-access-mode (for FAT AP)

Function

Using the **display sta-access-mode** command, you can check whether the blacklist or whitelist function is enabled, which determines the STA access control mode.

Format

display sta-access-mode

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the blacklist function is enabled, STAs in the blacklist cannot connect to the WLAN.

After the whitelist function is enabled, only the STAs in the whitelist can connect to the WLAN.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the STA access control mode.

```
<Huawei> display sta-access-mode
 Station access control mode: disable
```

Table 13-42 Description of the **display sta-access-mode** command output

Item	Description
Station access control mode	STA access control mode: ● disable ● white list: The whitelist is used. ● black list: The blacklist is used. You can run the **13.3.22 sta-access-mode (for FAT AP)** command to set STA access control mode.

Related Topics

13.3.22 sta-access-mode (for FAT AP)

13.3.7 display sta-blacklist (for FAT AP)

Function

The **display sta-blacklist** command displays the STA blacklist.

Format

display sta-blacklist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **13.3.22 sta-access-mode (for FAT AP)** command to enable the blacklist function, STAs in the blacklist cannot connect to the WLAN.

You can use the **display sta-blacklist** command to view MAC addresses of STAs in the blacklist.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display information about the STA blacklist.

```
<Huawei> display sta-blacklist
  Station mac global black list information:
  ---------------------------------------------------------------------------
  ID        MAC
  ---------------------------------------------------------------------------
  0         0026-0000-90a1
  1         0026-0000-909f
  ---------------------------------------------------------------------------
  Total number: 2
```

Table 13-43 Description of the **display sta-blacklist** command output

Item	Description
ID	STA ID in the blacklist.
MAC	MAC address of a STA in the blacklist.
Total number	Total number of STAs in the blacklist.

13.3.8 display sta-whitelist (for FAT AP)

Function

The **display sta-whitelist** command displays the STA whitelist.

Format

display sta-whitelist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **13.3.22 sta-access-mode (for FAT AP)** command to enable the whitelist function, only STAs in the whitelist can connect to the WLAN.

You can run the **display sta-whitelist** command to view MAC addresses of STAs in the whitelist.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the STA whitelist.

```
<Huawei> display sta-whitelist
  Station mac global white list information:
  ---------------------------------------------------------------------------
  ID        MAC
  ---------------------------------------------------------------------------
  0         0025-9e26-b9bd
  1         001e-907a-b6a6
  2         0026-0000-90a1
  ---------------------------------------------------------------------------
  Total number: 3
```

Table 13-44 Description of the **display sta-whitelist** command output

Item	Description
ID	ID of a STA.
MAC	MAC address of a STA.
Total number	Total number of STAs in the whitelist.

13.3.9 display wapi certificate (for FAT AP)

Function

The **display wapi certificate** command displays the content of a certificate file.

Format

display wapi certificate file-name *file-name*

Parameters

Parameter	Description	Value
file-name *file-name*	Specifies a certificate file name.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) or spaces and cannot start or end with double quotation marks (" ").

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view content of certificate files imported to the device.

In the command, *file-name* must specify the complete path of a certificate file. For example, if the certificate file **as.cer** is saved in the flash memory, run **display wapi certificate file-name flash:/as.cer** command.

Example

Display content of certificate file **as.cer**.

```
<Huawei> display wapi certificate file-name flash:/as.cer
  Certificate:
  Data:
    Version: V3
    Serial Number:
      4B 05 3B F4
    Signature Algorithm: sha256ECDSA192
    Issuer:
      OU = iwncomm
      CN = iwncomm
    Validity:
      Not Before: 2009-11-19 12:37:08 UTC
      Not After : 2029-11-19 12:37:08 UTC
    Subject:
      OU = iwncomm
      CN = iwncomm
    Subject Public Key Info:
      Public Key Algorithm: ECC
      Public Key: (392 bit)
      04 69 5C B1 3F 52 A1 D6 6C DD 5A 4C E7 5D 5D C8
      2B 83 BF 22 A2 F2 63 B1 FA 5F 6E 87 A8 F2 F6 31
      12 D3 A4 D4 9B 34 F9 30 35 2A 70 5B 43 48 47 47
      7D
```

Table 13-45 Description of the **display wapi certificate** command output

Item	Description
Version	Version of the X.509 certificate.
Serial Number	Serial number of the certificate.
Signature Algorithm	Algorithm used to calculate the signature.
Issuer	Certificate issuer.
Validity	Valid period of the certificate, specified by the start date and end date.
Subject	Subject of the certificate.
Subject Public Key Info	Information about the public key of the certificate.

 Copyright © Huawei Technologies Co., Ltd.

13.3.10 display wlan ids attack-detected (for FAT AP)

Function

The **display wlan ids attack-detected** command displays information about the attacking devices detected.

Format

display wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all types of attacking devices.	-
flood	Displays information about devices launching flood attacks.	-
spoof	Displays information about devices launching spoofing attacks.	-
wapi-psk	Displays information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays information about devices launching weak IV attacks.	-
wep-share-key	Displays information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays information about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run the **display wlan ids attack-detected** command to view the information list of attacking devices.

Prerequisites

Attack detection has been enabled on the AP radio using the **13.3.1 attack detection enable (for FAT AP)** command.

Precautions

When the AR169W-P-M9 and AR169RW-P-M9 work on the 5G frequency band, they can defend against attacks that STAs launch using Action, EAPoL Logoff, EAPoL start, and null data frames. However, the AR169W-P-M9 and AR169RW-P-M9 cannot display the attacking devices and attack times and do not add the STAs to the blacklist.

Example

Display information of all current attacking devices.

```
<Huawei> display wlan ids attack-detected all
Total Number Of Entries: 4
 act = Action Frame          asr = Association Request
 aur = Authentication Request daf = Deauthentication Frame
 dar = Disassociation Request ndf = Null Data Frame
 pbr = Probe Request         rar = Reassociation Request
 eaps = EAPOL Start Frame     eapl = EAPOL Logoff Frame
 saf = Spoofed Disassociation Frame
 sdf = Spoofed Deauthentication Frame
 wiv = Weak IV Detected       nqf = Null Qos Frame
 wep = Wep Share-key          wpa = WPA
 wpa2 = WPA2                  wapi = WAPI
 #AP = number of active APs detecting, AT = Last Detcted Attack Type
 Ch = Channel Number
 Attacking Device(s) Table
--------------------------------------------------------------------------------
 MAC address     AT     Ch   Last Detected Time     #AP
--------------------------------------------------------------------------------
 0010-1000-0031  saf    1    2013-07-27/16:41:55    1
 0010-1000-0030  wiv    1    2013-07-27/16:41:55    2
 0010-1000-002f  asr    1    2013-07-27/16:41:55    2
 0010-1000-002e  saf    1    2013-07-27/16:41:55    2
--------------------------------------------------------------------------------
```

Table 13-46 Description of the **display wlan ids attack-detected all** command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of attack type.
Ch	Channel in which the last attack is detected.
Last Detected Time	Last time at which an attack is detected.
#AP	Number of APs which detect this attack.

Display information of attacking device by specifying its MAC address.

```
<Huawei> display wlan ids attack-detected mac-address dcd2-fc1c-77ef
 act = Action Frame          asr = Association Request
 aur = Authentication Request daf = Deauthentication Frame
 dar = Disassociation Request ndf = Null Data Frame
 pbr = Probe Request         rar = Reassociation Request
 eaps = EAPOL Start Frame     eapl = EAPOL Logoff Frame
 saf = Spoofed Disassociation Frame
 sdf = Spoofed Deauthentication Frame
 wiv = Weak IV Detected       nqf = Null Qos Frame
 wep = Wep Share-key          wpa = WPA
 wpa2 = WPA2                  wapi = WAPI
 #AP = number of active APs detecting, AT = Last Detcted Attack Type
 Ch = Channel Number
 Attacking Device(s) Table
-----------------------------------------------------------------------------
 MAC address                        : dcd2-fc1c-77ef
 Number of detected APs                 : 1
 Channel                            : 1
 Reported AP 1:
        AP ID                       : 13
        Flood attack type                : asr,aur,pbr
        First detected time(Flood)          : 2012-10-25/16:51:59
        Spoof attack type                : saf,sdf
        First detected time(Spoof)          : 2012-10-25/16:46:37
        First detected time(Weak-iv)        : -
        First detected time(Wep)            : -
        First detected time(WPA)            : -
        First detected time(WPA2)           : -
        First detected time(WAPI)           : -
-----------------------------------------------------------------------------
```

Table 13-47 Description of the **display wlan ids attack-detected mac-address** *mac-address* command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
Number of detected APs	Number of APs which detect this attack.
Channel	Channel in which the last attack is detected.
Reported AP	Information of AP which detect the attack.
AP ID	ID of the AP which detects the attack.
Flood attack type	The type of flood attacking detected by the AP.
Spoof attack type	The type of spoof attacking detected by the AP.
First detected time	The first time of each attacking which AP detects.

13.3.11 display wlan ids attack-detected statistics (for FAT AP)

Function

The **display wlan ids attack-detected statistics** command displays the number of attacks detected.

Format

display wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run the **display wlan ids attack-detected statistics** command to view the total number of all types of attacks.

Prerequisites

Attack detection has been enabled on the AP radio using the **13.3.1 attack detection enable (for FAT AP)** command.

Precautions

When the AR169W-P-M9 and AR169RW-P-M9 work on the 5G frequency band, they can defend against attacks that STAs launch using Action, EAPoL Logoff, EAPoL start, and null data frames. However, the AR169W-P-M9 and AR169RW-P-M9 cannot display the attacking devices and attack times and do not add the STAs to the blacklist.

Example

Display the number of attacks detected.

```
<Huawei> display wlan ids attack-detected statistics
Attack tracking since: 2012-07-27/16:16:06
-------------------------------------------------------------------------------
 Type                                        Total
-------------------------------------------------------------------------------
 Probe Request Frame Flood Attack                    : 7
 Authentication Request Frame Flood Attack           : 0
 Deauthentication Frame Flood Attack                 : 0
 Association Request Frame Flood Attack              : 1
 Disassociation Request Frame Flood Attack           : 8
 Reassociation Request Frame Flood Attack            : 0
 Action Frame Flood Attack                           : 0
 Null Data Frame Flood Attack                        : 0
 Null Qos Frame Flood Attack                         : 0
 EAPOL Start Frame Flood Attack                      : 0
 EAPOL Logoff Frame Flood Attack                     : 0
 Weak IVs Detected                                   : 21
 Spoofed Deauthentication Frame Attack               : 0
 Spoofed Disassociation Frame Attack                 : 2
 WEP Share-key Attack                                : 0
 WPA Attack                                          : 0
 WPA2 Attack                                         : 0
 WAPI Attack                                         : 0
-------------------------------------------------------------------------------
```

Table 13-48 Description of the display wlan ids attack-detected statistics command output

Item	Description
Type	Attack type: ● Probe Request Frame Flood Attack ● Authentication Request Frame Flood Attack ● Deauthentication Frame Flood Attack ● Association Request Frame Flood Attack ● Disassociation Request Frame Flood Attack ● Reassociation Request Frame Flood Attack ● Action Frame Flood Attack ● Null Data Frame Flood Attack ● Null Qos Frame Flood Attack ● EAPOL Start Frame Flood Attack ● EAPOL Logoff Frame Flood Attack ● Weak IVs Detected ● Spoofed Deauthentication Frame Attack ● Spoofed Disassociation Frame Attack ● WEP Share-key Attack: brute force cracking attack in WEP-SK authentication mode ● WPA Attack: brute force cracking attack in WPA-PSK authentication mode ● WPA2 Attack: brute force cracking attack in WPA2-PSK authentication mode ● WAPI Attack: brute force cracking attack in WPAI authentication mode
Total	Total number of attacks detected.

 Copyright © Huawei Technologies Co., Ltd.

13.3.12 display wlan ids attack-history (for FAT AP)

Function

The **display wlan ids attack-history** command displays historical records about the attacking devices detected.

Format

display wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays historical records about all types of attacking devices.	-
flood	Displays historical records about devices launching flood attacks.	-
spoof	Displays historical records about devices launching spoofing attacks.	-
wapi-psk	Displays historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays historical records about devices launching weak IV attacks.	-
wep-share-key	Displays historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, information about the detected attacking devices is saved in the attacking device list. If an attacking device no longer launches an attack, the device is removed from the attacking device list and saved to the historical attacking device list. You can run the **display wlan ids attack-history** command to check historical records about the attacking devices detected.

Prerequisites

Attack detection has been enabled on the AP radio using the **13.3.1 attack detection enable (for FAT AP)** command.

Example

Display historical records of all attacking devices.

```
<Huawei> display wlan ids attack-history all
Total Number Of Entries: 4
 act = Action Frame          asr = Association Request
 aur = Authentication Request daf = Deauthentication Frame
 dar = Disassociation Request ndf = Null Data Frame
 pbr = Probe Request         rar = Reassociation Request
 eaps = EAPOL Start Frame     eapl = EAPOL Logoff Frame
 saf = Spoofed Disassociation Frame
 sdf = Spoofed Deauthentication Frame
 wiv = Weak IV Detected       nqf = Null Qos Frame
 wep = Wep Share-key          wpa = WPA
 wpa2 = WPA2                  wapi = WAPI
 AP = Detector AP ID
 AT = Attack Type, Ch = Channel Number, AR = Average RSSI
 Attack History Table
--------------------------------------------------------------------------------
 MAC address   AT     Ch   AR(dBm)  Last Detected Time     AP
--------------------------------------------------------------------------------
 1010-1000-0031  saf    1    -10       2013-05-11/16:41:55  2
 1010-1000-0030  wiv    1    -10       2013-05-11/16:41:55  2
 1010-1000-002f  asr    1    -10       2013-05-11/16:41:55  2
 1010-1000-002e  saf    1    -10       2013-05-11/16:41:55  2
--------------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 13-49 Description of the **display wlan ids attack-history all** command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of attack type.
Ch	Channel in which the last attack is detected.
AR	Average received signal strength indicator (RSSI) of the attack frames detected.
Last Detected Time	Last time at which an attack is detected.
AP	SSID of the AP that detects attacks.

13.3.13 display wlan ids dynamic-blacklist (for FAT AP)

Function

The **display wlan ids dynamic-blacklist** command displays information about devices in the dynamic blacklist.

Format

display wlan ids dynamic-blacklist { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all devices in the dynamic blacklist.	-
mac-address *mac-address*	Displays information about attacking devices with a specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An AP uses attack detection and dynamic blacklist functions to add an attacking device detected to the dynamic blacklist, and rejects packets sent from this device until the device entry in the dynamic blacklist ages. You can run the **display wlan ids dynamic-blacklist** command to view information about devices in the dynamic blacklist.

Prerequisites

- Attack detection has been enabled on the AP radio using the **13.3.1 attack detection enable (for FAT AP)** command.
- Dynamic blacklist is enabled on the AP radio using the **13.3.15 dynamic-blacklist enable (for FAT AP)** command.

Precautions

When the AR169W-P-M9 and AR169RW-P-M9 work on the 5G frequency band, they can defend against attacks that STAs launch using Action, EAPoL Logoff, EAPoL start, and null data frames. However, the AR169W-P-M9 and AR169RW-P-M9 cannot display the attacking devices and attack times and do not add the STAs to the blacklist.

Example

Display information about all devices in the dynamic blacklist.

```
<Huawei> display wlan ids dynamic-blacklist all
Total number of entries : 2
--------------------------------------------------------------------------------
 #AP = number of active APs detecting
 MAC address       Last Updated Since    Reason   #AP
--------------------------------------------------------------------------------
 0010-1000-0002    2005-07-27/16:53:40   asr      1
 0010-1000-0005    2005-07-27/16:53:40   asr      1
--------------------------------------------------------------------------------
```

Table 13-50 Description of the display wlan ids dynamic-blacklist all command output

Item	Description
MAC address	MAC address of the device in the dynamic blacklist.
Last Updated Since	Latest time of device attack detection.

Item	Description
Reason	Reason why the device is added to the dynamic blacklist. The values here are the acronyms of attack types. For details, see **13.3.10 display wlan ids attack-detected (for FAT AP)**.
#AP	The number of AP that detects the device and adds it to the dynamic blacklist.

Display information about specified devices in the dynamic blacklist.

```
<Huawei> display wlan ids dynamic-blacklist mac-address 1010-1000-0005
-------------------------------------------------------------------------------
 MAC address                        : 1010-1000-0005
 Reported AP 0:
  AP name                          : ap-0
  reason                          : asr
  Last Detected time                : 2012-07-27/16:53:40
-------------------------------------------------------------------------------
```

Table 13-51 Description of the display wlan ids dynamic-blacklist mac-address command output

Item	Description
Reported AP 0	AP that adds the device to the dynamic blacklist.
AP name	Name of the monitoring AP.
Last Detected time	Last time at which the device is detected.

Related Topics

13.3.1 attack detection enable (for FAT AP)

13.3.15 dynamic-blacklist enable (for FAT AP)

13.3.14 dynamic-blacklist aging-duration (for FAT AP)

Function

The **dynamic-blacklist aging-duration** command sets an aging time for the dynamic blacklist.

The **undo dynamic-blacklist aging-duration** command restores the aging time for the dynamic blacklist to the default value.

By default, the aging time for the dynamic blacklist is 600 seconds.

Format

dynamic-blacklist aging-duration *duration*

undo dynamic-blacklist aging-duration

Parameters

Parameter	Description	Value
duration	Specifies the aging time at the expiry of which a specified MAC address is removed from the dynamic blacklist.	The value is an integer that ranges from 180 to 3600, in seconds.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

The dynamic blacklist function is enabled using the **13.3.15 dynamic-blacklist enable (for FAT AP)** command. When detecting attacks from a STA, the AP adds the STA to the dynamic blacklist to disable the STA from getting online and to reject any packets sent from the STA. As long as the STA is blacklisted, it cannot go online again even if it no longer launches attacks. To avoid that, you can run the **dynamic-blacklist aging-duration** command to set the aging time of the dynamic blacklist. If the set aging time expires and the AP detects no attack from the STA, the STA is once again allowed to go online.

Example

Set the aging time for the dynamic blacklist to 300 seconds.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] dynamic-blacklist aging-duration 300
```

Related Topics

13.1.26 display radio config (for FAT AP)

13.3.15 dynamic-blacklist enable (for FAT AP)

13.3.15 dynamic-blacklist enable (for FAT AP)

Function

The **dynamic-blacklist enable** command enables the dynamic blacklist function.

 Copyright © Huawei Technologies Co., Ltd.

The **undo dynamic-blacklist enable** command disables the dynamic blacklist function.

By default, the dynamic blacklist function is disabled.

Format

dynamic-blacklist enable

undo dynamic-blacklist enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled using the **13.3.1 attack detection enable (for FAT AP)** command, you can run the **dynamic-blacklist enable** command to enable the dynamic blacklist function. When detecting attacks from a device, an AP adds the device to the dynamic blacklist to reject any packets sent from the device until the dynamic blacklist entry ages.

An AP can use the dynamic blacklist to filter out the blacklisted wireless devices to avoid malicious attacks.

Follow-up Procedure

Run the **13.3.14 dynamic-blacklist aging-duration (for FAT AP)** command to set an aging time for the dynamic blacklist.

Example

Enable the dynamic blacklist function.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] dynamic-blacklist enable
```

Related Topics

13.1.26 display radio config (for FAT AP)

13.3.14 dynamic-blacklist aging-duration (for FAT AP)

13.3.16 reset wlan ids attack-detected (for FAT AP)

Function

The **reset wlan ids attack-detected** command deletes information about the attacking devices detected.

Format

reset wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes information about all types of attacking devices.	-
flood	Deletes information about devices launching flood attacks.	-
spoof	Deletes information about devices launching spoofing attacks.	-
wapi-psk	Deletes information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes information about devices launching weak IV attacks.	-
wep-share-key	Deletes information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes information about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After attack detection is enabled, information about attacking devices detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-detected** command to delete the information.

Prerequisites

Attack detection has been enabled on the AP radio interface using the **13.3.1 attack detection enable (for FAT AP)** command.

Example

Delete information about all the current attacking devices.

```
<Huawei> reset wlan ids attack-detected all
```

Related Topics

13.3.1 attack detection enable (for FAT AP)

13.3.10 display wlan ids attack-detected (for FAT AP)

13.3.17 reset wlan ids attack-detected statistics (for FAT AP)

Function

The **reset wlan ids attack-detected statistics** command deletes the number of attacks detected.

Format

reset wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After attack detection is enabled, the number of attacks detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-detected statistics** command to delete the information.

Prerequisites

Attack detection has been enabled on the AP radio using the **13.3.1 attack detection enable (for FAT AP)** command.

Example

Delete the number of attacks detected.

```
<Huawei> reset wlan ids attack-detected statistics
```

Related Topics

13.3.1 attack detection enable (for FAT AP)

13.3.11 display wlan ids attack-detected statistics (for FAT AP)

13.3.18 reset wlan ids attack-history (for FAT AP)

Function

The **reset wlan ids attack-history** command deletes historical records about the attacking devices detected.

Format

reset wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes historical records about all types of attacking devices.	-
flood	Deletes historical records about devices launching flood attacks.	-
spoof	Deletes historical records about devices launching spoofing attacks.	-
wapi-psk	Deletes historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes historical records about devices launching weak IV attacks.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wep-share-key	Deletes historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes historical records about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After attack detection is enabled, historical records about attacking devices detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-history** command to delete the historical records information about the attacking devices detected.

Prerequisites

Attack detection has been enabled on the AP radio using the **13.3.1 attack detection enable (for FAT AP)** command.

Example

Delete historical records about all the current attacking devices.

```
<Huawei> reset wlan ids attack-history all
```

Related Topics

13.3.1 attack detection enable (for FAT AP)

13.3.12 display wlan ids attack-history (for FAT AP)

13.3.19 reset wlan ids dynamic-blacklist (for FAT AP)

Function

The **reset wlan ids dynamic-blacklist** command deletes information about devices in the dynamic blacklist.

Format

reset wlan ids dynamic-blacklist { **mac-address** *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address *mac-address*	Deletes devices with a specified MAC address from the dynamic blacklist.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Deletes all information in the dynamic blacklist.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset wlan ids dynamic-blacklist** command is applicable to the following scenarios:

- To re-collect the dynamic blacklist information, run the **reset wlan ids dynamic-blacklist all** command to delete all information in the dynamic blacklist. After that, the AP re-collects the information.
- If an unintentional rogue device has restored to its normal state but the dynamic blacklist entry has not aged, run the **reset wlan ids dynamic-blacklist mac-address** command to remove the MAC address of the device from the dynamic blacklist. After that, information sent from the device is not rejected.

Precautions

After you run the **reset wlan ids dynamic-blacklist** command to delete the information in the dynamic blacklist, packet receipt of APs is affected. Therefore, confirm the action before running this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Remove the client with MAC address 78AC-C0C1-C1FC from the dynamic blacklist.

```
<Huawei> reset wlan ids dynamic-blacklist mac-address 78ac-c0c1-c1fc
```

13.3.20 security-policy (for FAT AP)

Function

The **security-policy** command configures the security policy that a profile used.

The **undo security-policy** command restores the default security policy that a profile used.

By default, the **wep** security policy is used.

Format

security-policy { **wep** | **wpa** | **wpa2** | **wapi** }

undo security-policy

Parameters

Parameter	Description	Value
wep	Indicates a WEP security policy. By default, open system authentication +non-encryption is used.	-
wpa	Indicates a WPA security policy. By default, 802.1X, the Protected Extensible Authentication Protocol (PEAP) authentication, and TKIP encryption are used.	-
wpa2	Indicates a WPA2 security policy. By default, 802.1X, PEAP authentication, and CCMP encryption are used.	-
wapi	Indicates a WAPI security policy. By default, the WAPI-CERT authentication and WPI encryption are used.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can select security policies on a WLAN based on the security level. WEP is a security policy used earlier and has security risks. It can be used in open scenarios that do not require high security, such as airports and railway stations. WPA and WAPI can provide higher security for devices.

- Before running this command, ensure that a security profile has been configured. You can specify a security policy in the security profile.
- Security policies need later configurations such as shared keys and certificates.
- You need to run this command together with the **13.1.47 interface wlan-radio** and **13.1.67 service-set (for FAT AP)** commands.

Example

Create a security profile named **p1** and set the security policy to WPA2.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] security-policy wpa2
```

Related Topics

13.3.5 display security-profile (for FAT AP)

13.3.21 security-profile (for FAT AP)

Function

The **security-profile** command creates a security profile or enters the security profile view.

The **undo security-profile** command deletes a security profile according to the ID or name.

By default, the security profile named **secf** exists in the system.

Format

security-profile { **id** *profile-id* | **name** *profile-name* } *

undo security-profile { **all** | **id** *profile-id* | **name** *profile-name* }

Parameters

Parameter	Description	Value
id *profile-id*	Specifies the ID of a security profile.	The value is an integer. The value range varies according to devices: ● AR150 series and AR200 series: 0 to 7 ● AR100 series, AR120 series and AR160 series: 0 to 15 ● AR1200 series: 0 to 15
name *profile-name*	Specifies the name of a security profile.	The value is a string of 1 to 31 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Indicates all security profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure access security. A security profile must be configured before you specify an authentication mode in the profile. To delete a security profile, run the **undo security-profile** command.

The system configures the new profile with the following default values:

- WEP: no authentication and no encryption
- WPA: 802.1X+PEAP authentication and TKIP encryption

 Copyright © Huawei Technologies Co., Ltd.

- WPA2: 802.1X+PEAP authentication and CCMP encryption
- WAPI: WAPI certificate encryption

NOTE

- If you enter only a name, the system checks whether the specified profile exists according to the name. If so, you enter the profile view. If not, the profile is created.
- If you enter only an ID, the system checks whether the specified profile exists according to the ID. If so, you enter the profile view. If not, an error message is displayed and no profile is created.
- If the name and ID you enter exist in the profile and match, you can enter the profile view. If the name and ID do not exist, the profile using the specified ID is created and you enter the profile view.

Example

Configure a security profile named **p1**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
```

Related Topics

13.3.5 display security-profile (for FAT AP)

13.3.22 sta-access-mode (for FAT AP)

Function

Using the **sta-access-mode** command, you can check whether the blacklist or whitelist function is enabled, which determines the STA access control mode.

The **undo sta-access-mode** command disables the blacklist or whitelist function.

By default, the blacklist or whitelist function is disabled.

Format

sta-access-mode { **blacklist** | **whitelist** | **disable** }

undo sta-access-mode { **blacklist** | **whitelist** | **disable** }

Parameters

Parameter	Description	Value
blacklist	Enables the blacklist function.	-
whitelist	Enables the whitelist function.	-
disable	Disables the blacklist or whitelist function.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

- The blacklist configured using the **13.3.23 sta-blacklist (for FAT AP)** command takes effect only after the blacklist function is enabled using the **sta-access-mode** command.
- The whitelist configured using the **13.3.24 sta-whitelist (for FAT AP)** command takes effect only after the whitelist function is enabled using the **sta-access-mode** command.

Example

Enable the blacklist function on the AP.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] sta-access-mode blacklist
```

13.3.23 sta-blacklist (for FAT AP)

Function

The **sta-blacklist** command adds a STA's MAC address to the STA blacklist.

The **undo sta-blacklist** command deletes the created blacklist.

By default, no blacklist is created.

Format

sta-blacklist *mac-address*

undo sta-blacklist { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in the blacklist.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
all	Deletes all MAC addresses from the blacklist.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Users whose MAC addresses are in the blacklist cannot be associated with APs and cannot access resources on WLAN networks.

The configured blacklist can take effect only after the blacklist function is enabled by using the **13.3.22 sta-access-mode (for FAT AP)** command.

Example

Add a STA's MAC address to the STA blacklist.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] sta-blacklist 0014-2261-2a43
```

Related Topics

13.3.7 display sta-blacklist (for FAT AP)

13.3.22 sta-access-mode (for FAT AP)

13.3.24 sta-whitelist (for FAT AP)

Function

The **sta-whitelist** command adds a STA's MAC address to the STA whitelist.

The **undo sta-whitelist** command deletes STA's MAC address from the STA whitelist.

By default, no STA whitelist created.

Format

sta-whitelist *mac-address*

undo sta-whitelist { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address in the whitelist.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Deletes all MAC addresses from the whitelist.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Users whose MAC addresses are in the whitelist can be associated with APs and access resources on WLAN networks.

The configured whitelist can take effect only after the whitelist function is enabled by using the **13.3.22 sta-access-mode (for FAT AP)** command. After the configured whitelist takes effect, users whose MAC addresses are not in the whitelist cannot access network resources.

NOTE

If the STA whitelist is configured but no MAC address is added to the whitelist, any STA can access WLAN network resources.

Example

Add a STA's MAC address to the STA whitelist.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] sta-whitelist 0011-43c7-d73e
```

Related Topics

13.3.8 display sta-whitelist (for FAT AP)

13.3.22 sta-access-mode (for FAT AP)

13.3.25 user-isolate (for FAT AP)

Function

The **user-isolate** command enables Layer 2 user isolation.

The **undo user-isolate** command disables Layer 2 user isolation.

By default, Layer 2 user isolation is disabled.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When working in WLAN Fat mode, the AR109W, AR109GW-L, AR129CVW, AR129CGVW-L, AR169CVW, and AR169CVW-4B4S support Layer 2 user isolation in V200R010C10 and later versions.

Format

user-isolate

undo user-isolate

Parameters

None

Views

Service set view

Default Level

2: Configuration level

Usage Guidelines

When multiple wireless users associate with the same VAP, one of the users with security risks may send a large number of broadcast packets to the other users, which impacts data services of the other users. After Layer 2 user isolation is enabled, wireless users associated with the same VAP can only forward packets at Layer 3 through the gateway but cannot implement Layer 2 data forwarding. This ensures secure data transmission between users.

Example

Create a service set **ChinaNet** and configure Layer 2 user isolation.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] service-set name ChinaNet
[Huawei-wlan-service-set-ChinaNet] user-isolate
```

13.3.26 wapi asu (for FAT AP)

Function

The **wapi asu** command specifies an IP address for an authentication server unit (ASU) server.

The **undo wapi asu** command deletes the IP address of the ASU server.

By default, no IP address is specified for the ASU server.

Format

wapi asu ip *ip-address*

undo wapi asu ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the ASU server.	The value is in dotted decimal notation.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If WAPI certificate authentication is configured, an AP sends WAPI authentication packets to the ASU server at the specified IP address.

Prerequisites

If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi asu** command to specify an IP address for the ASU server.

Precautions

The **wapi asu** command helps to determine to which ASU server WAPI packets are sent. Users must ensure the correctness of both ASU certificates and ASU servers; otherwise, they may fail in user authentication.

Example

Specify IP address 10.164.10.10 for the ASU server.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi asu ip 10.164.10.10
```

13.3.27 wapi authentication-method (for FAT AP)

Function

The **wapi authentication-method** command configures the WAPI authentication mode.

 Copyright © Huawei Technologies Co., Ltd.

The **undo wapi authentication-method** command restores the default WAPI authentication mode.

By default, WAPI certificate authentication is used.

Format

wapi authentication-method psk { **pass-phrase** | **hex** } **cipher** *cipher-key*

wapi authentication-method certificate

undo wapi authentication-method

Parameters

Parameter	Description	Value
certificate	Configures WAPI certificate authentication.	-
psk	Configures WAPI pre-shared key authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommend.	-
cipher *cipher-key*	Specifies a password in cipher text.	In pass-phrase mode, the key is a string of 8 to 64 characters in plain text or 32 to 108 characters in cipher text. In hex mode, the key is a string of 8 to 32 hexadecimal numbers, in which case the length of the string must be an even, or a string of 32 to 68 characters in cipher text.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI supports two authentication modes: certificate authentication and pre-shared key authentication. When pre-shared key authentication is used, a pre-shared key must be configured.

- If WAPI authentication is specified as a security policy in a security profile, you can run the **wapi authentication-method** command to configure the WAPI authentication mode.
- The **wapi authentication-method** command determines the WAPI authentication and key management mode. When certificate authentication and key management are configured, authentication involves identity authentication and key negotiation, and the authentication server and certificate need to be configured. When pre-shared key authentication is configured, a pre-shared key needs to be configured, and STAs also need to know the pre-shared key. In this situation, authentication just involves key negotiation.

Example

Set the WAPI authentication mode to pre-shared key authentication and specify the key.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi authentication-method psk pass-phrase cipher huawei@123
```

13.3.28 wapi bk (for FAT AP)

Function

The **wapi bk** command sets the interval for updating a BK and the BK lifetime percentage.

The **undo wapi bk** command restores the default interval for updating a BK and the BK lifetime percentage.

By default, the interval for updating a BK is 43200s, and the BK lifetime percentage is 70%.

Format

wapi { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-update-interval* }

undo wapi { **bk-threshold** | **bk-update-interval** }

Parameters

Parameter	Description	Value
bk-threshold *bk-threshold*	Specifies the BK lifetime percentage.	The value is an integer that ranges from 1 to 100.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bk-update-interval *bk-update-interval*	Specifies the interval for updating a BK.	The value is an integer that ranges from 600 to 604800, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can set the intervals for updating a BK and an MSK to ensure security.

Example

Set the interval for updating a BK to 10000s and the BK lifetime percentage to 80%.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi bk-update-interval 10000
[Huawei-wlan-sec-prof-p1] wapi bk-threshold 80
```

13.3.29 wapi import certificate (for FAT AP)

Function

The **wapi import certificate** command imports the AP certificate file, certificate of the AP certificate issuer, and ASU certificate file.

The **undo wapi certificate** command deletes the imported AP certificate file, certificate of the AP certificate issuer, or ASU certificate file.

By default, the AP certificate file, certificate of the AP certificate issuer, and ASU certificate file are not imported.

Format

wapi import certificate { **ap** | **asu** | **issuer** } **file-name** *file-name* [**password cipher** *password*]

undo wapi certificate { **issuer** | **ap** | **asu** }

Parameters

Parameter	Description	Value
issuer	Specifies the certificate of the AP certificate issuer.	-
ap	Specifies the AP certificate.	-
asu	Specifies the ASU certificate.	-
file-name *file-name*	Specifies a certificate file name, which the complete path of a certificate file must be specified.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) or spaces and cannot start or end with double quotation marks (" ").
password cipher *password*	Specifies the certificate key.	● The password can be in plain text or cipher text. – A plain text password is a string of 1 to 32 characters. – A cipher text password is a string of 32 to 68 characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi import certificate** command to specify the AP certificate, certificate of the AP certificate issuer, and ASU certificate. STAs will fail to be authenticated if you do not run this command. The issuer certificate helps to check whether the AP certificate is modified.
- Before using this command, store the AP certificate and ASU certificate to the storage of the device, and import the certificates and private key using TFTP. Certificates must be X509 V3 certificates and comply with the WAPI standard. Otherwise, certificates cannot be imported.

 Copyright © Huawei Technologies Co., Ltd.

- After this command is run:
  - When an issuer certificate is configured, the system checks correctness of the AP certificate.
  - If the authentication system uses only two certificates, the issuer certificate and ASU certificate have the same certificate file name and are the same certificate. If the authentication system uses three certificates, the issuer certificate and ASU certificate are different from each other and both must be imported.

NOTE

- The ASU certificate and issuer certificate must be imported.
- Certificates to be imported must be valid and correct.
- If the certificate with the same name but different contents has been imported by other security profiles, delete the earlier certificate first.

Example

Import the AP certificate.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi import certificate ap file-name flash:/local_ap.cer
```

13.3.30 wapi cert-retrans-count (for FAT AP)

Function

The **wapi cert-retrans-count** command sets the number of retransmissions of certificate authentication packets.

The **undo wapi cert-retrans-count** command restores the default number of retransmissions of certificate authentication packets.

By default, the number of retransmissions is 3.

Format

wapi cert-retrans-count *cert-count*

undo wapi cert-retrans-count

Parameters

Parameter	Description	Value
cert-count	Specifies the number of retransmissions of certificate authentication packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

If WAPI authentication is specified as a security policy using the **13.3.20 security-policy (for FAT AP)** command, run the **wapi cert-retrans-count** command to set the number of retransmissions of certificate authentication packets.

Example

Set the number of retransmissions of certificate authentication packets to 5.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi cert-retrans-count 5
```

13.3.31 wapi msk (for FAT AP)

Function

The **wapi msk** command sets the interval for updating an MSK, number of packets that will trigger MSK update, and number of retransmissions of MSK negotiation packets.

The **undo wapi msk** command restores the default interval for updating an MSK, number of packets that will trigger MSK update, and number of retransmissions of MSK negotiation packets.

By default, the interval for updating an MSK is 86400s; the number of packets that will trigger MSK update is 10; the number of retransmissions of MSK negotiation packets is 3.

Format

wapi { **msk-update-interval** *msk-interval* | **msk-update-packet** *msk-packet* | **msk-retrans-count** *msk-count* }

undo wapi { **msk-update-interval** | **msk-update-packet** | **msk-retrans-count** }

Parameters

Parameter	Description	Value
msk-update-interval *msk-interval*	Specifies the interval for updating an MSK. When the MSK update mode is set to time-based update using the **13.3.34 wapi key-update (for FAT AP)** command, the interval for updating an MSK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
msk-update-packet *msk-packet*	Specifies the number of packets that will trigger MSK update. When the MSK update mode is set to packet count-based update using the **13.3.34 wapi key-update (for FAT AP)** command, the number of packets that will trigger MSK update needs to be set.	The value is an integer that ranges from 1 to 4294967295.
msk-retrans-count *msk-count*	Specifies the number of retransmissions of MSK negotiation packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends. To enhance security, WAPI provides the following key update mechanisms:

- Time-based key update: periodically updates a key.
- Packet-based key update: updates a key when the number of packets encrypted using the key reaches the specified value.

Example

Set the interval for updating an MSK to 10000s, number of packets that will trigger MSK update to 1200, and number of retransmissions of MSK negotiation packets to 5.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi msk-update-interval 10000
[Huawei-wlan-sec-prof-p1] wapi msk-update-packet 1200
[Huawei-wlan-sec-prof-p1] wapi msk-retrans-count 5
```

13.3.32 wapi import private-key (for FAT AP)

Function

The **wapi import private-key** command imports the AP private key file.

The **undo wapi private-key** command deletes the imported AP private key file.

By default, no AP private key file is imported.

Format

wapi import private-key file-name *file-name* [**password cipher** *cipher-password*]

undo wapi private-key

Parameters

Parameter	Description	Value
file-name *file-name*	Specifies the name of a private key file.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) or spaces and cannot start or end with double quotation marks (" ").
password	Specifies the AP private key.	-
cipher *cipher-password*	Specifies a password in cipher text.	The password can be in plain text or cipher text. ● A plain text password is a string of 1 to 32 characters. ● A cipher text password is a string of 32 to 68 characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi import private-key** command to specify the private key file for the AP certificate.
- Before using this command, store the AP private key file to the storage of the device, and import the private key file using TFTP.

- After this command is used, the system obtains the private key file and establishes the mapping between the certificate and private key.

NOTE

The certificate and private key to be imported must be valid and correct.

Example

Import the AP private key file **ap_key.key**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi import private-key file-name flash:/ap_key.key
```

Related Topics

13.3.5 display security-profile (for FAT AP)

13.3.33 wapi sa-timeout (for FAT AP)

Function

The **wapi sa-timeout** command sets the timeout period of a security association (SA) of key encryption.

The **undo wapi sa-timeout** command restores the default timeout period of a SA for key encryption.

By default, the timeout period for a SA is 60s.

Format

wapi sa-timeout *sa-time*

undo wapi sa-timeout

Parameters

Parameter	Description	Value
sa-time	Specifies the timeout period of an SA.	The value is an integer that ranges from 1 to 255, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can prolong the WAPI timeout period to increase the authentication success ratio.

Example

Set the timeout period of an SA to 100s.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi sa-timeout 100
```

13.3.34 wapi key-update (for FAT AP)

Function

The **wapi key-update** command sets the USK and MSK update mode.

The **undo wapi key-update** command restores the default USK and MSK update mode.

By default, USKs and MSKs are updated based on time.

Format

wapi { **usk** | **msk** } **key-update** { **disable** | **time-based** | **packet-based** | **timepacket-based** }

undo wapi { **usk** | **msk** } **key-update**

Parameters

Parameter	Description	Value
usk	Indicates USK update.	-
msk	Indicates MSK update.	-
disable	Disables key update.	-
time-based	Indicates time-based update. You can run the **13.3.31 wapi msk (for FAT AP)** and **13.3.35 wapi usk (for FAT AP)** commands to respectively set the intervals for updating an MSK and a USK.	-
packet-based	Indicates packet count-based update. You can run the **13.3.31 wapi msk (for FAT AP)** and **13.3.35 wapi usk (for FAT AP)** commands to set the number of packets that will trigger MSK update and USK update.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
timepacket-based	Indicates time-based update and packet count-based update. You can run the **13.3.31 wapi msk (for FAT AP)** and **13.3.35 wapi usk (for FAT AP)** commands to set the intervals for updating an MSK and a USK and number of packets that will trigger MSK update and USK update.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- To ensure network security, update keys in a timely manner. There are several key update modes. To change the WAPI key update mode, run the **wapi key-update** command.
- The **wapi key-update** command sets the USK and MSK update mode. If the interval for updating an MSK or a USK is too long or the number of packets that will trigger MSK or USK update is too large, key security cannot be ensured.
- If **disable** is specified, keys will not be updated.

Example

Set the USK update mode to packet count-based update.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi usk key-update packet-based
```

13.3.35 wapi usk (for FAT AP)

Function

The **wapi usk** command sets the interval for updating a USK, number of packets that will trigger USK update, and number of retransmissions of USK negotiation packets.

The **undo wapi usk** command restores the default interval for updating a USK, number of packets that will trigger USK update, and number of retransmissions of USK negotiation packets.

 Copyright © Huawei Technologies Co., Ltd.

By default, the interval for updating a USK is 86400s; the number of packets that will trigger USK update is 10; the number of retransmissions of USK negotiation packets is 3.

Format

wapi { **usk-update-interval** *usk-interval* | **usk-update-packet** *usk-packet* | **usk-retrans-count** *usk-count* }

undo wapi { **usk-update-interval** | **usk-update-packet** | **usk-retrans-count** }

Parameters

Parameter	Description	Value
usk-update-interval *usk-interval*	Specifies the interval for updating a USK. When the USK update mode is set to time-based update using the **13.3.34 wapi key-update (for FAT AP)** command, the interval for updating a USK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.
usk-update-packet *usk-packet*	Specifies the number of packets that will trigger USK update. When the USK update mode is set to packet count-based update using the **13.3.34 wapi key-update (for FAT AP)** command, the number of packets that will trigger USK update needs to be set.	The value is an integer that ranges from 1 to 4294967295.
usk-retrans-count *usk-count*	Specifies the number of retransmissions of USK negotiation packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends. To enhance security, WAPI provides the following key update mechanisms:

- Time-based key update: periodically updates a key.
- Packet-based key update: updates a key when the number of packets encrypted using the key reaches the specified value.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval for updating a USK to 10000s, number of packets that will trigger USK update to 1200, and number of retransmissions of USK negotiation packets to 5.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wapi usk-update-interval 10000
[Huawei-wlan-sec-prof-p1] wapi usk-update-packet 1200
[Huawei-wlan-sec-prof-p1] wapi usk-retrans-count 5
```

13.3.36 wep authentication-method (for FAT AP)

Function

The **wep authentication-method** command configures the WEP authentication mode.

The **undo wep authentication-method** command restores the default WEP authentication mode.

By default, open system authentication is used.

Format

wep authentication-method { **open-system** [**data-encrypt**] | **share-key** }

undo wep authentication-method

Parameters

Parameter	Description	Value
open-system	Sets the WEP authentication mode to open system authentication.	-
share-key	Sets the WEP authentication mode to pre-shared key authentication.	-
data-encrypt	Sets the WEP authentication mode to open system authentication and data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can select security policies on a WLAN based on the security level. WEP is a security policy used earlier and has security risks. It can be used in open scenarios that do not require high security, such as airports and railway stations. You can run this command to set the WEP authentication mode to open system authentication or pre-shared key authentication.

Table 13-52 Comparison between open system authentication and pre-shared key authentication

Authentication Mode	Advantage	Disadvantage
open-system	Wireless devices can connect to a network without authentication.	STA identities are not checked, bringing security risks.
share-key	A pre-shared key is used to enhance security.	• A long key string must be configured on each device and is difficult to expand. • A static key is used, which is easy to decipher.

Precautions

- If the authentication mode is set to **share-key**, run the **13.3.38 wep key (for FAT AP)** command to configure a pre-shared key.
- If the authentication mode is set to **open-system** without **data-encrypt**, the WEP pre-shared key configured in the profile cannot take effect.
- If the authentication mode is set to **open-system** with **data-encrypt**, run the **13.3.38 wep key (for FAT AP)** command to configure a pre-shared key.

Example

Create security profile **p1** and set the authentication mode to **share-key**.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wep authentication-method share-key
```

13.3.37 wep default-key (for FAT AP)

Function

The **wep default-key** command sets the default key ID for WEP authentication or encryption.

The **undo wep default-key** command restores the default key ID for WEP authentication or encryption.

By default, key 0 is used for WEP authentication or encryption.

Format

wep default-key *key-id*

undo wep default-key

Parameters

Parameter	Description	Value
key-id	Specifies the default key ID.	The value is an integer that ranges from 0 to 3.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- A maximum of four WEP keys can be configured, and only one WEP key is used for authentication and encryption. This command specifies which key to use.
- After a key ID is specified, the specified key is used for authentication or encryption.

Example

Set the default key ID to 1.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wep default-key 1
```

Related Topics

13.3.38 wep key (for FAT AP)

13.3.38 wep key (for FAT AP)

Function

The **wep key** command sets a WEP key.

 Copyright © Huawei Technologies Co., Ltd.

The **undo wep key** command deletes the specified key.

By default, the device does not set a WEP key.

Format

wep key { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id* **cipher** *cipher-key-value*

undo wep key *key-id*

Parameters

Parameter	Description	Value
wep-40	Configures WEP-40 authentication.	-
wep-104	Configures WEP-104 authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number.	-
key-id	Specifies the key ID.	The value is an integer that ranges from 0 to 3.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-key-value*	Specifies a password in cipher text.	The password can be in plain text or cipher text. ● A plain text password is a string of case-sensitive characters. – If WEP-40 is used, the WEP key is 10 hexadecimal characters (select **hex**) or 5 ASCII characters (select **pass-phrase**). – If WEP-104 is used, the WEP key is 26 hexadecimal characters or 13 ASCII characters. ● The password is a character string in cipher text. You are advised to enter a password in plain text and then use the password displayed in cipher text as the cipher text password.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

To connect to a WLAN device in WEP shared-key authentication mode or open system authentication+data encryption mode, run the **wep key** command to set a WEP key.

NOTE

If the key is in hexadecimal notation, you can enter hexadecimal numbers without entering 0x.

Example

Configure a WEP key and its ID.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] wep key wep-40 hex 1 cipher 1234567890
```

Related Topics

13.3.37 wep default-key (for FAT AP)

13.3.39 authentication-method dot1x encryption-method (for FAT AP)

Function

The **authentication-method dot1x encryption-method** command configures 802.1X authentication and encryption for WPA and WPA2.

The **undo authentication-method** command disables WPA and WPA2 authentication and encryption.

By default, WPA uses 802.1X authentication+TKIP encryption, WPA2 uses 802.1X authentication+CCMP encryption.

Format

{ **wpa** | **wpa2** } **authentication-method dot1x encryption-method** { **tkip** | **ccmp** }

undo { **wpa** | **wpa2** } **authentication-method**

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
tkip	Configures TKIP encryption.	-
ccmp	Configures CCMP encryption.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WPA/WPA2 authentication includes WPA/WPA2 pre-shared key authentication and 802.1X authentication, which are also called WPA/WPA2 personal edition and WPA/WPA2 enterprise edition respectively. 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 802.1X authentication, run the **authentication-method dot1x encryption-method** command. CCMP encryption is recommended. TKIP encryption and WEP encryption both use the RC4 algorithm, providing low security.

Example

Configure WPA authentication (802.1x and TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] security-policy wpa
[Huawei-wlan-sec-prof-p1] wpa authentication-method dot1x encryption-method tkip
```

Configure WPA2 authentication (802.1x and TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] security-policy wpa2
[Huawei-wlan-sec-prof-p1] wpa2 authentication-method dot1x encryption-method tkip
```

13.3.40 authentication-method psk encryption-method (for FAT AP)

Function

The **authentication-method psk encryption-method** command configures pre-shared key authentication and encryption for WPA and WPA2.

The **undo authentication-method** command disables WPA and WPA2 authentication and encryption.

By default, WPA uses 802.1X authentication+TKIP encryption, WPA2 uses 802.1X authentication+CCMP encryption.

 Copyright © Huawei Technologies Co., Ltd.

Format

{ **wpa** | **wpa2** } **authentication-method psk** { **pass-phrase** | **hex** } **cipher** *cipher-key* **encryption-method** { **tkip** | **ccmp** }

undo { **wpa** | **wpa2** } **authentication-method**

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommend.	-
cipher *cipher-key*	Specifies a password in cipher text.	The value is of 8 to 63 characters in plain text, 64 hexadecimal characters in plain text, or 32 to 108 characters in cipher text.
tkip	Configures TKIP encryption.	-
ccmp	Configures CCMP encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

To access a WLAN device using WPA or WPA2 pre-shared key authentication, run the **wpa authentication-method psk encryption-method** command. CCMP encryption is recommended. TKIP encryption and WEP encryption both use the RC4 algorithm, providing low security.

NOTE

If the key is in hexadecimal notation, you can enter hexadecimal numbers without entering 0x.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure WPA pre-shared key authentication and the authentication key.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] security-policy wpa
[Huawei-wlan-sec-prof-p1] wpa authentication-method psk pass-phrase cipher huawei@123
encryption-method ccmp
```

Configure WPA2 pre-shared key authentication and the authentication key.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] security-profile id 10 name p1
[Huawei-wlan-sec-prof-p1] security-policy wpa2
[Huawei-wlan-sec-prof-p1] wpa2 authentication-method psk pass-phrase cipher huawei@123
encryption-method ccmp
```

13.4 WLAN Radio Resource Management Configuration Commands

13.4.1 calibrate channel-set (for FAT AP)

Function

The **calibrate channel-set** command configures a calibration channel set.

The **undo calibrate channel-set** command restores the default calibration channel set.

By default, a global calibration channel set contains channels corresponding to global country codes.

NOTE

The default calibration channels corresponding to the country code China do not include channels 36 to 64.

Format

calibrate { **2.4g** | **5g** } **channel-set** *channel-value*

undo calibrate { **2.4g** | **5g** } **channel-set**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
2.4g | **5g**	Specifies the frequency band on which radio calibration is performed. ● **2.4g**: Radios work on the 2.4 GHz frequency band. ● **5g**: Radios work on the 5 GHz frequency band.	-
channel-set *channel-value*	Specifies the calibration channel set.	The value is a character string. You can select calibration channels as prompted. If you select multiple channels, use commas (,) to separate channel names.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to specify a calibration channel set for an AP. The device selects channels from the channel set to calibrate. This reduces the burden on the AP.

NOTE

To ensure a good calibration effect, you are advised to configure at least three calibration channels.

The 5 GHz frequency band has richer spectrum resources. In addition to 20 MHz channels, APs working on the 5 GHz frequency band support 40 MHz channels. Larger-bandwidth channels mean higher transmission rates. However, at least three channels are required in radio calibration to achieve the optimal calibration effect. When configuring the calibration bandwidth, ensure that enough calibration channels are available for use.

To specify a 40 MHz calibration channel, you need to specify two consecutive 20 MHz channels. To specify an 80 MHz calibration channel, you need to specify four consecutive 20 MHz channels. The combinations of 20 MHz channels making up the 40 MHz and 80 MHz channels are fixed. For details, see *Access Routers Configuration Guide*–Radio Resource Management–Radio Calibration.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When configuring a radio calibration set, avoid using radar channels.

The channels you configure must be supported by the terminals; otherwise, the terminals cannot discover wireless signals. For example, when the country code is set to China, 5 GHz channels 36, 40, 44, 48, 52, 56, 60, and 64 can be configured. However, most terminals do not support these channels currently. If these channels are configured, the terminals cannot discover wireless signals. In this case, you can configure 5 GHz channels 149, 153, 157, 161, and 165, which are supported by the terminals.

Example

Configure a global calibration channel set composed of 40 MHz channels 149, 153, 157, and 161 on the 5 GHz frequency band.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] calibrate 5g channel-set 149,153,157,161
```

13.4.2 calibrate sensitivity (for FAT AP)

Function

The **calibrate sensitivity** command configures the radio calibration sensitivity for a device.

The **undo calibrate sensitivity** command restores the default radio calibration sensitivity.

By default, the radio calibration sensitivity of the device is set to **medium**.

Format

calibrate sensitivity { **low** | **medium** | **high** }

undo calibrate sensitivity

Parameters

Parameter	Description	Value
low	Indicates low radio calibration sensitivity.	-
medium	Indicates medium radio calibration sensitivity.	-
high	Indicates high radio calibration sensitivity.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

The following table describes the radio calibration sensitivity of the device.

Sensitivity	2.4 GHz	5 GHz
high	0 dB	x dB
medium	4*x dB	6*x dB
low	5*x dB	5*x dB

NOTE

x depends on the number of APs engaged in radio calibration and is calculated according to the formula:

x = (Number of APs/8 + 1)

The default value is recommended.

Example

Set the radio calibration sensitivity to high.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] calibrate sensitivity high
```

13.4.3 calibrate enable { auto | manual | schedule time } (for FAT AP)

Function

The **calibrate enable** { **auto** | **manual** | **schedule time** } command configures the radio calibration mode.

The **undo calibrate enable** command disables calibration.

The default radio calibration mode is **manual**.

Format

calibrate enable { **auto** [**interval** *interval-value* [**start-time** *start-time*]] | **manual** | **schedule time** *time-value* }

undo calibrate enable

Parameters

Parameter	Description	Value
auto	Sets the radio calibration mode to auto.	-
interval *interval-value*	Specifies the radio calibration interval in auto mode.	The value is an integer that ranges from 30 to 1440, in minutes. If **interval** is not specified, the radio calibration interval in auto mode is 60 minutes.
start-time *start-time*	Specifies the start time for radio calibration in automatic mode.	The value is in the format of hh:mm:ss. ● hh: indicates the hour. The value is an integer that ranges from 0 to 23. ● mm: indicates the minute. The value is an integer that ranges from 0 to 59. ● ss: indicates the second. The value is an integer that ranges from 0 to 59.
manual	Sets the radio calibration mode to manual.	-
schedule	Sets the radio calibration mode to schedule.	-
time *time-value*	Specifies the time for triggering the scheduled radio calibration.	The value is in the format of hh:mm:ss. ● hh: indicates the hour. The value is an integer that ranges from 0 to 23. ● mm: indicates the minute. The value is an integer that ranges from 0 to 59. ● ss: indicates the second. The value is an integer that ranges from 0 to 59.

Views

WLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

There are three radio calibration modes:

- Auto mode: The device periodically implements radio calibration at certain intervals (the interval is specified by **interval** and the default interval is 60 minutes).
- Manual mode: Radio calibration is not automatically implemented by the device but manually triggered through the **13.4.4 calibrate manual startup (for FAT AP)** command.
- Schedule mode: The device triggers radio calibration at the time specified by the parameter **time**.

The three modes cannot be configured simultaneously. You can choose any of the modes as required.

Example

Set the radio calibration mode to auto.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] calibrate enable auto
```

Set the radio calibration mode to schedule and set the time for scheduled radio calibration to 20:30:00.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] calibrate enable schedule time 20:30:00
```

Related Topics

13.4.4 calibrate manual startup (for FAT AP)

13.4.4 calibrate manual startup (for FAT AP)

Function

The **calibrate manual startup** command triggers radio calibration.

Format

calibrate manual startup

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

To manually trigger radio calibration, run the **calibrate enable manual** command to set the radio calibration mode to manual and then run the **calibrate manual startup** command. The device implements radio calibration only after the **calibrate manual startup** command is executed.

Example

Manually trigger radio calibration.

```
<Huawei> system-view
[Huawei] wlan
[Huawei-wlan-view] calibrate enable manual
[Huawei-wlan-view] calibrate manual startup
```

Related Topics

13.4.3 calibrate enable { auto | manual | schedule time } (for FAT AP)

13.4.5 display calibrate channel-set (for FAT AP)

Function

The **display calibrate channel-set** command displays the calibration channels and bandwidth that take effect.

Format

display calibrate channel-set

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the radio calibration function, you can run the **display calibrate channel-set** command to check the calibration channels and bandwidth that take effect.

Example

Display the calibration channels and bandwidth that take effect globally.

```
<Huawei> display calibrate channel-set
Country-code: CN
```

 Copyright © Huawei Technologies Co., Ltd.

```
-----------------------------------------------------------------------------
Radio Frequency  Bandwidth  Channel Set
-----------------------------------------------------------------------------
2.4G             20MHz      1,6,11
5G               40MHz      149,153,157,161
-----------------------------------------------------------------------------
```

Table 13-53 Description of the **display calibrate channel-set** command output

Item	Description
Country-code	Country code.
Radio Frequency	Radio type.
Bandwidth	Calibration bandwidth that takes effect.
Channel Set	Calibration channel set that takes effect.

Related Topics

13.4.1 calibrate channel-set (for FAT AP)

13.4.6 display neighbor (for FAT AP)

Function

The **display neighbor** command displays information about neighbors of a radio.

Format

display neighbor interface *wlan-radio-num*

Parameters

Parameter	Description	Value
interface *wlan-radio-num*	Displays information about neighbors of a specified radio interface.	The value is determined based on radio interfaces supported by the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

APs' neighbor information reflects the APs' locations and neighbor relationships, helping you plan the network.

Example

Display information about neighbors of radio interface 0/0/0.

```
<Huawei> display neighbor interface wlan-radio0/0/0
 Uncontrol AP:
 ----------------------------------------------------
  BSSID          CHANNEL  RSSI(dBm)  SSID
 ----------------------------------------------------
  dcd2-fc9a-2070 1        -65.00     B1-5F-01-49
 ----------------------------------------------------
 Total: 1
```

Table 13-54 Description of the display neighbor command output

Item	Description
BSSID	BSSID of a neighboring radio.
CHANNEL	Channel of a neighboring radio.
RSSI(dBm)	Strength of signals received from a neighboring radio, in dBm.
SSID	SSID of a neighboring radio.

13.4.7 display statistics calibrate (for FAT AP)

Function

The **display statistics calibrate** command displays radio calibration statistics.

Format

display statistics calibrate interface wlan-radio *wlan-radio-number*

Parameters

Parameter	Description	Value
interface wlan-radio [*wlan-radio-number*]	Displays radio calibration statistics on the specified radio interface. **NOTE** You do not need to enter a space between **wlan-radio** and *wlan-radio-number*.	The value is determined based on radio interfaces supported by the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display statistics calibrate** command to view radio calibration statistics, helping check whether the radio environment is stable.

Example

Display radio calibration statistics on radio interface 0/0/0.

```
<Huawei> display statistics calibrate interface wlan-radio0/0/0
 ---------------------------------------------------------------------------
  Signal environment deterioration :1
  Power calibration                :1
  Channel calibration              :0
 ---------------------------------------------------------------------------
```

Table 13-55 Description of the display statistics calibrate command output

Item	Description
Signal environment deterioration	Number of times the radio environment deteriorates.
Power calibration	Number of times the power of the radio is calibrated.
Channel calibration	Number of times the channel of the radio is calibrated.

13.4.8 reset statistics calibrate (Radio interface view)

Function

The **reset statistics calibrate** command clears radio calibration statistics.

Format

reset statistics calibrate

Parameters

None

Views

Radio interface view

Default Level

2: Configuration level

Usage Guidelines

Run the **reset statistics calibrate** command to clear radio calibration statistics, including the number of times the radio environment deteriorates and number of times the radio channel and power are calibrated.

Example

Clear radio calibration statistics.

```
<Huawei> system-view
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] reset statistics calibrate
```

Related Topics

13.4.7 display statistics calibrate (for FAT AP)

 Copyright © Huawei Technologies Co., Ltd.

14 WLAN-AC Commands

About This Chapter

14.1 WLAN Service Configuration Commands
14.2 WLAN Radio Resource Management Configuration Commands
14.3 WLAN Roaming Commands
14.4 WLAN Security Configuration Commands
14.5 WLAN WDS Configuration Commands
14.6 WLAN Reliability Commands

14.1 WLAN Service Configuration Commands

14.1.1 ac sysnetid

Function

The **ac sysnetid** command configures an NE name for an AC.

The **undo ac sysnetid** command deletes the NE name of an AC.

By default, no NE name is configured for an AC.

Format

ac sysnetid *ac-sysnetid*

undo ac sysnetid

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ac-sysnetid	Specifies the NE name of an AC.	The value is a string of 1 to 32 case-sensitive characters. The value beginning and ending with double quotation marks (" ") can contain spaces. The value can contain digits, letters, and special characters such as the asterisk (*) and number sign (#).

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrator can run the **ac sysnetid** command to configure a unique NE name for an AC. This facilitates AC management.

Configuration Impact

If you run the **ac sysnetid** command multiple times, only the latest configuration takes effect.

Example

Set the NE name of an AC to **ABC123**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ac sysnetid ABC123
```

Related Topics

14.1.69 display ac global configuration

14.1.2 access-user syslog-restrain enable

Function

The **access-user syslog-restrain enable** command enables system log suppression.

The **undo access-user syslog-restrain enable** command disables system log suppression.

By default, system log suppression is enabled.

Format

access-user syslog-restrain enable

undo access-user syslog-restrain enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a STA passes authentication or successfully associates with the AP, the AP sends system logs to the NMS server. A system log contains MAC addresses of the STA, AC, and AP, AP and AC name and current time, and authentication result.

If a STA fails to associate with an AP or fails authentication, the STA attempts to go online continuously. The AP sends a large number of duplicate logs to the AC in a short period, which wastes resources and deteriorates system performance. To prevent this problem, enable system log suppression.

Example

Enable system log suppression.

```
<Huawei> system-view
[Huawei] access-user syslog-restrain enable
```

14.1.3 access-user syslog-restrain period

Function

The **access-user syslog-restrain period** command sets the period of system log suppression.

The **undo access-user syslog-restrain period** command restores the default period of system log suppression.

By default, the period of system log suppression is 300s.

Format

access-user syslog-restrain period *period*

undo access-user syslog-restrain period

Parameters

Parameter	Description	Value
period	Specifies the period of system log suppression.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a STA is authenticated or successfully associates with an AP, the AP sends system logs to the NMS server. A system log contains MAC addresses of the STA, AP, and AC, AP name and current time, AC name and current time, and authentication result.

A STA retries continuously after it fails to associate with an AP or pass the authentication. When this occurs, the AC sends a large number of logs in a short time. This results in a high statistics failure rate and degrades the NMS performance. The system log suppression function reduces impact of such logs on the NMS.

Example

Set the period of system log suppression to 600s.

```
<Huawei> system-view
[Huawei] access-user syslog-restrain period 600
```

14.1.4 active-dull-client enable

Function

The **active-dull-client enable** command enables the function of preventing terminals from entering energy-saving mode.

The **undo active-dull-client enable** command disables the function.

By default, the function of preventing terminals from entering energy-saving mode is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

active-dull-client enable

undo active-dull-client enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Due to individual reasons, some terminals may not run services normally when entering energy-saving mode. You can run the **active-dull-client enable** command to enable the function of preventing terminals from entering energy-saving mode. After that, an AP frequently sends null data frames to these terminals to prevent them from entering energy-saving mode, ensuring normal services.

Precautions

After the function is enabled, the terminals consume more power and extra bandwidth. If no terminal enters an abnormal energy-saving state, you are advised to disable the function.

Example

Enable the function of preventing terminals from entering energy-saving mode.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] active-dull-client enable
```

Related Topics

14.1.118 display ssid-profile

14.1.5 alarm-restriction disable

Function

The **alarm-restriction disable** command disables alarm suppression for an AP.

The **undo alarm-restriction disable** command enables alarm suppression for an AP.

 Copyright © Huawei Technologies Co., Ltd.

By default, alarm suppression is enabled for an AP.

Format

alarm-restriction disable

undo alarm-restriction disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a STA cannot go online due to security type mismatch, UAC, or access user upper limit exceeding, the STA will automatically re-connect to the AP. During this period, the AP sends a large number of STA association failure alarms to the AC, which degrades the system performance.

To solve this problem, enable alarm suppression for the AP. The AP then does not report alarms repeatedly in the alarm suppression period, preventing alarm storms.

Example

Disable alarm suppression for an AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] alarm-restriction disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.6 alarm-restriction period

Function

The **alarm-restriction period** command configures the period of alarm suppression on an AP.

The **undo alarm-restriction period** command restores the default period of alarm suppression for an AP.

The default alarm suppression period is 60 seconds on an AP.

Format

alarm-restriction period *period*

undo alarm-restriction period

Parameters

Parameter	Description	Value
period	Specifies the period of alarm suppression for an AP.	The value is an integer that ranges from 10 to 300, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap alarm-restriction period** command to configure the period of alarm suppression for an AP. The AP reports an alarm only one time in the specified period if the alarm is repeatedly generated.

Example

Set the period of alarm suppression to 200 seconds for an AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] alarm-restriction period 200
```

Related Topics

14.1.98 display ap-system-profile

14.1.7 antenna-gain

Function

(AP group radio view) The **antenna-gain** command configures the antenna gain for all specified radios in an AP group.

(AP group radio view) The **undo antenna-gain** command restores the default antenna gain for all specified radios in an AP group.

(AP radio view) The **antenna-gain** command configures the antenna gain for an AP radio.

 Copyright © Huawei Technologies Co., Ltd.

(AP radio view) The **undo antenna-gain** command cancels the configuration of the antenna gain on an AP radio. The antenna gain on the AP radio is then determined by that configured in the AP group radio view.

By default, no antenna gain is configured for AP radios.

The antenna gain of AP radios depends on AP types and working channels of AP radios. You can run the **display ap-type** { **id** *type-id* | **type** *ap-type* } command to check default antenna gains of radios of different AP types.

Format

antenna-gain *antenna-gain*

undo antenna-gain

Parameters

Parameter	Description	Value
antenna-gain	Specifies the antenna gain.	The value is an integer that ranges from 0 to 30, in dB.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The antenna gain is the ratio of the power density produced by an antenna to the power density that should be obtained at the same point if the power accepted by the antenna were radiated equally. It can measure the capability for an antenna to receive and send signals in a specified direction, which is one of the most important parameters to select a BTS antenna. In the same condition, if the antenna gain is high, the wave travels far.

Precautions

The antenna gain of an AP radio configured using the command must be consistent with the gain of the antenna connected to the AP.

The antenna gain of an AP radio configured using the command takes effect only for external antennas. When an AP uses an external antenna, configure the antenna gain for the AP radio to be consistent with the gain of the external antenna connected to the AP.

The maximum antenna gain should comply with laws and regulations of the corresponding country. For details, see the *Country Code & Channel Compliance Table*.

 Copyright © Huawei Technologies Co., Ltd.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the antenna gain to 4 for radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] antenna-gain 4
```

14.1.8 anti-attack broadcast-flood blacklist enable

Function

The **anti-attack broadcast-flood blacklist enable** command enables the broadcast flood blacklist function.

The **undo anti-attack broadcast-flood blacklist enable** command disables the broadcast flood blacklist function.

By default, the broadcast flood blacklist function is disabled.

Format

anti-attack broadcast-flood blacklist enable

undo anti-attack broadcast-flood blacklist enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the broadcast flood blacklist function is enabled, the device considers traffic with a rate higher than that specified in **14.1.10 anti-attack broadcast-flood sta-rate-threshold** a broadcast flood attack and adds the STA to the blacklist.

Prerequisites

The broadcast flood detection function has been enabled using the **undo anti-attack broadcast-flood disable** command.

Example

Enable the broadcast flood blacklist function.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name profile1
[Huawei-wlan-vap-prof-profile1] anti-attack broadcast-flood blacklist enable
```

Related Topics

14.1.9 anti-attack broadcast-flood disable
14.1.10 anti-attack broadcast-flood sta-rate-threshold

14.1.9 anti-attack broadcast-flood disable

Function

The **anti-attack broadcast-flood disable** command disables the broadcast flood detection function.

The **undo anti-attack broadcast-flood disable** command enables the broadcast flood detection function.

By default, the broadcast flood detection function is enabled.

Format

anti-attack broadcast-flood disable

undo anti-attack broadcast-flood disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

If a large number of broadcast packets are sent to a device in a short time, the device becomes busy processing the packets and cannot process normal services. To prevent broadcast flood attacks, you can configure broadcast flood detection.

Example

Disable the broadcast flood detection function.

```
<Huawei> system-view
[Huawei] wlan ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] vap-profile name profile1
[Huawei-wlan-vap-prof-profile1] anti-attack broadcast-flood disable
```

Related Topics

14.1.10 anti-attack broadcast-flood sta-rate-threshold

14.1.10 anti-attack broadcast-flood sta-rate-threshold

Function

The **anti-attack broadcast-flood sta-rate-threshold** command sets the broadcast flood threshold.

The **undo anti-attack broadcast-flood sta-rate-threshold** command restores the default broadcast flood threshold.

By default, the broadcast flood threshold is 10 pps.

Format

anti-attack broadcast-flood sta-rate-threshold *sta-rate-threshold*

undo anti-attack broadcast-flood sta-rate-threshold

Parameters

Parameter	Description	Value
sta-rate-threshold	Specifies the rate threshold of broadcast traffic from STAs.	The value is an integer that ranges from 5 to 5000, in pps.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the broadcast flood detection function is enabled, you can set the broadcast traffic threshold.

When the traffic rate exceeds the threshold, the device considers a broadcast flood attack from the STA and discards the broadcast traffic. This prevents the upper-layer network from being affected by the broadcast flood.

 Copyright © Huawei Technologies Co., Ltd.

If the broadcast flood blacklist function is enabled using the **14.1.8 anti-attack broadcast-flood blacklist enable** command, the device adds broadcast flood STAs to the blacklist.

Prerequisites

The broadcast flood detection function has been enabled using the **undo anti-attack broadcast-flood disable** command.

Example

Set the broadcast flood threshold to 100 pps.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name profile1
[Huawei-wlan-vap-prof-profile1] anti-attack broadcast-flood sta-rate-threshold 100
```

Related Topics

14.1.9 anti-attack broadcast-flood disable

14.1.8 anti-attack broadcast-flood blacklist enable

14.1.11 ap auth-mode

Function

The **ap auth-mode** command configures the AP authentication mode.

The **undo ap auth-mode** command restores the default AP authentication mode.

The default AP authentication mode is MAC address authentication.

Format

ap auth-mode { **mac-auth** | **no-auth** | **sn-auth** }

undo ap auth-mode

Parameters

Parameter	Description	Value
mac-auth	Indicates the MAC address authentication mode.	-
no-auth	Indicates the non-authentication mode.	-
sn-auth	Indicates the SN authentication mode.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After the **ap auth-mode** command is executed, the AC authenticates the AP using the configured mode.

NOTE

The non-authentication mode brings security risks. You are advised to set the authentication mode to MAC address authentication or SN authentication, which is more secure.

Example

Change the AP authentication mode to MAC address authentication.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap auth-mode mac-auth
```

Related Topics

14.1.77 display ap global configuration

14.1.12 ap blacklist

Function

The **ap blacklist** command adds an AP to an AP blacklist.

The **undo ap blacklist** command deletes an AP from an AP blacklist.

By default, no AP is in an AP blacklist.

Format

ap blacklist mac *ap-mac1* [**to** *ap-mac2*]

undo ap blacklist mac *ap-mac1* [**to** *ap-mac2*]

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the AP MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
to *ap-mac2*	Specifies the end MAC address. This parameter is used when you want to add multiple MAC addresses to the blacklist. The value must be larger than *ap-mac1*. *ap-mac1* and *ap-mac2* identify a range. The maximum number of MAC addresses that can be added to the blacklist in batches is 128.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the AP's MAC address is in the blacklist, the AP cannot go online. If the MAC address of an online AP is in the blacklist, the AP is forced to log out.

Precautions

The AP blacklist and whitelist can be configured at the same time. However, the MAC address of an AP cannot be added to the AP blacklist and whitelist at the same time.

If AP whitelist and blacklist are all configured, check whether an AP is on the blacklist first.

Example

Add the AP with the MAC address of 0025-9e07-8280 to the AP blacklist.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap blacklist mac 0025-9e07-8280
```

Add MAC addresses from 0025-9e07-8270 to 0025-9e07-8276 to the AP blacklist.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap blacklist mac 0025-9e07-8270 to 0025-9e07-8276
```

Related Topics

14.1.30 ap-confirm
14.1.73 display ap blacklist

14.1.13 ap data-collection enable

Function

The **ap data-collection enable** command enables an AC to buffer AP data.

The **undo ap data-collection enable** command restores the default settings.

By default, an AC is disabled from buffering AP data.

Format

ap data-collection enable

undo ap data-collection enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

The NMS needs to periodically query performance statistics (including AP and radio performance statistics and information about users on an AP) from an AC that queries the information from the AP.

Data caching is a method to improve query performance, in which an AC periodically queries performance statistics and caches the data. When the NMS requires the data, the NMS queries the data from the buffer but not from the AP.

You are advised to enable an AC to buffer AP data when you use the NMS to query AP statistics. When NMS query expires, the NMS can obtain AP data from the AC.

Example

Enable an AC to buffer AP data.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap data-collection enable
```

Related Topics

14.1.14 ap data-collection interval

14.1.77 display ap global configuration

 Copyright © Huawei Technologies Co., Ltd.

14.1.14 ap data-collection interval

Function

The **ap data-collection interval** command sets the data buffer duration.

The **undo ap data-collection interval** command restores the default data buffer duration.

By default, an AC buffers AP data for 5 minutes.

Format

ap data-collection interval *interval*

undo ap data-collection interval

Parameters

Parameter	Description	Value
interval	Specifies the buffer duration.	The value is an integer that ranges from 5 to 60, in minutes.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can run the **ap data-collection interval** command to set the buffer duration.

Example

Enable an AC to buffer AP data and set the buffer duration.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap data-collection enable
[Huawei-wlan-view] ap data-collection interval 57
```

Related Topics

14.1.13 ap data-collection enable

14.1.77 display ap global configuration

 Copyright © Huawei Technologies Co., Ltd.

14.1.15 ap lldp enable

Function

The **ap lldp enable** command enables LLDP in the WLAN view.

The **undo ap lldp enable** command disables LLDP in the WLAN view.

By default, LLDP is disabled in the WLAN view.

Format

ap lldp enable

undo ap lldp enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Link Layer Discovery Protocol (LLDP) is a Layer 2 discovery protocol defined in the IEEE 802.1ab standard. Using LLDP, the Central AP or NMS can obtain Layer 2 information about the connected RRUs, including RRUs' interfaces and connections with other devices. Additionally, the Central AP or NMS can obtain details about network topology and interface changes. To view the Layer 2 link status between RRUs, and between RRUs and switch or analyze the network topology, enable WLAN LLDP.

Precautions

WLAN LLDP can be enabled in the system view and the RRU wired port link profile view.

- An RRU can send and receive LLDP packets only after LLDP is enabled in both the WLAN view and the RRU wired port link profile view.
- After LLDP is disabled in the WLAN view, the commands for enabling and disabling LLDP on the RRU wired port link profile view do not take effect.

Example

Enable LLDP in the WLAN view.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap lldp enable
```

Related Topics

14.1.77 display ap global configuration

14.1.160 lldp enable

14.1.16 ap manufacturer-config

Function

The **ap manufacturer-config** command restores the factory settings of APs.

Format

ap manufacturer-config { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP, factory settings of which need to be restored.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP, factory settings of which need to be restored.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP, factory settings of which need to be restored.	The AP ID must already exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When a configuration error occurs on the AP, you can run this command to clear AP configurations.

NOTICE

After restoring factory settings, the AP is reset and configurations are restored to factory settings.

 Copyright © Huawei Technologies Co., Ltd.

Example

Restore the factory settings of AP **N1-2**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap manufacturer-config ap-name N1-2
Warning: Reset AP to the manufacturing default configuration, continue?[Y/N]:y
```

14.1.17 ap modify

Function

The **ap modify** command changes the MAC address of an AP.

Format

ap modify *ap-id* **mac** *ap-mac*

Parameters

Parameter	Description	Value
ap-id	Specifies the ID of the AP to be replaced.	The AP ID must exist.
mac *ap-mac*	Specifies the MAC address of a new AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When AP hardware needs to be replaced, you can change the MAC address of the AP to that of a new AP to prevent repetitive data configurations. After the change, the new AP goes online using the ID of the original AP, and all data configurations of the original AP take effect on the new AP.

By default, you can run the **display ap** { **all** | **ap-group** *ap-group* } command to check the MAC address of an AP.

Precautions

Replacing an AP enables the new AP to go online on the AC but will interrupt services of the original AP.

Example

Replace the AP with the ID **0** with the AP with the MAC address **0002-1110-0120**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap modify 0 mac 0002-1110-0120
Warning: Modify AP will influence the service that has published in AP, Whether to continue? [Y/N]y
```

Related Topics

14.1.70 display ap

14.1.18 ap update ftp-server

Function

The **ap update ftp-server** command configures basic FTP information, including the FTP server IP address, FTP server user name and password.

The **undo ap update ftp-server** command restores default FTP settings.

By default, no FTP server IP address is configured, The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

ap update ftp-server ip-address *server-ip-address* **ftp-username** *ftp-username* **ftp-password cipher** *ftp-password*

undo ap update ftp-server

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the FTP server.	The value is in dotted decimal notation.
ftp-username *ftp-username*	Specifies the FTP server user name.	The value is a string of 1 to 31 characters. The value cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ") or spaces.
ftp-password	Specifies the password for logging in to the FTP server.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher	Specifies the password in cipher text.	-
ftp-password	Specifies the FTP server password.	The value is a string of characters without question marks (?) or spaces. It cannot start or end with double quotation marks (" ") or spaces. *ftp-password* contains 48 or 68 characters in cipher text, such as %^%#A<g;&zQR7P3TF+,[MxQ1X%4[2~Gb]Vp#(e<y:~)/%^%#. *ftp-password* also can be a string of 1 to 31 characters in plain text, such as **huawei123**.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- The FTP configuration is used when the automatic upgrade and online upgrade modes are FTP. In the automatic upgrade or online upgrade, the AC sends basic FTP information to the AP, and the AP requests the FTP server for upgrade based on FTP information.
- After running the **ap update ftp-server** command, you can perform the following operations:
  a. Run the **ap update mode** command to set the upgrade mode to ftp-mode.
  b. Run the **ap update multi-load** command to upgrade APs in batches.

Precautions

- It is recommended that you use an external FTP server to upgrade APs. If the AC functions as the FTP server, a maximum of five APs can be upgraded simultaneously.
- The FTP server user name cannot contain the double quotation marks ("). Ensure that the FTP server user name and unencrypted password configured on the AC do not contain the preceding characters. Otherwise, FTP upgrade fails.

Example

Configure the FTP server IP address, FTP server user name and password.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update ftp-server ip-address 192.168.1.100 ftp-username admin ftp-password
cipher wlanadmin
```

Related Topics

14.1.21 ap update mode

14.1.22 ap update multi-load

14.1.91 display ap update configuration

14.1.19 ap update ftp-server max-connect-number

Function

The **ap update ftp-server** command configures the maximum number of APs that can be upgraded simultaneously in FTP mode.

The **undo ap update ftp-server** command restores the default maximum number of APs that can be upgraded simultaneously in FTP mode.

By default, a maximum of 50 APs can be upgraded simultaneously in FTP mode.

Format

ap update ftp-server max-connect-number *max-connect-number*

undo ap update ftp-server max-connect-number

Parameters

Parameter	Description	Value
max-connect-number	Specifies the maximum number of APs that can be upgraded simultaneously.	The value is an integer that ranges from 1 to 64.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in FTP mode, you can configure the value of *max-connect-number* to change the maximum number of APs that can be upgraded simultaneously.

- If the number of APs to be upgraded is equal to or smaller than *max-connect-number*, all APs can be upgraded simultaneously.
- If the number of APs to be upgraded is larger than *max-connect-number*, only the specified number of APs can be upgraded simultaneously. After the specified number of APs are upgraded, the remaining APs are upgraded automatically until all APs are upgraded. The number of APs that are upgraded at a time cannot exceed the value of *max-connect-number*.

Precautions

An external FTP server can be used, which is recommended. The AC can also function as the FTP server.

- When an external FTP server is used, the maximum number of APs that can be upgraded simultaneously is the configured *max-connect-number*.
- If an AC is used as the FTP server, a maximum of five APs can be upgraded simultaneously even if the specified number is larger than five.

  When the AC functions as the FTP server, run the **ap update ftp-server max-connect-number** *max-connect-number* command to set the maximum number of APs that can be upgraded simultaneously. The value of *max-connect-number* is an integer ranging from 1 to 5. During the upgrade, a maximum of 1 to 5 APs can be upgraded at a time until all APs are upgraded. If the configured number of APs to be upgraded simultaneously is larger than 5, an error message will be displayed after the first 5 APs are upgraded. The remaining APs cannot be automatically upgraded. You have to repeat the command until all APs are upgraded.

Example

Set the maximum number of APs that can be upgraded simultaneously in FTP mode to 10.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update ftp-server max-connect-number 10
```

Related Topics

14.1.21 ap update mode
14.1.22 ap update multi-load
14.1.91 display ap update configuration

14.1.20 ap update load

Function

The **ap update load** command upgrades a specified AP.

The **undo ap update load** command cancels AP upgrade.

Format

ap update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name*

undo ap update load { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP to be upgraded.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP to be upgraded.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP to be upgraded.	The AP ID must already exist.
update-filename *update-file-name*	Specifies the AP upgrade file.	The upgrade file name must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in batches based on AP types, if the new version fails, the version rollback takes a long period. Therefore, you can update a single AP to check whether faults occur on the version, ensuring successful upgrades in batches.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

If the FTP or SFTP mode is used, the AP upgrade file has been uploaded to the FTP server or SFTP server.

The AP is in normal or vmiss state.

Follow-up Procedure

Run the **ap update reset** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } command to restart the AP to make the upgrade take effect.

Precautions

The **undo ap update load** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } command cancels AP upgrade. However, if the AP system software has been written to the flash memory during the upgrade, the command does not take effect. You can run the **display ap update status** { **ap-name** *ap-name* | **ap-id** *ap-id* } command to check AP upgrade progress.

Example

Upgrade the AP **N1-2** using the upgrade file **fitap6x10xn_v200r006c10.bin**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update load ap-name N1-2 update-filename fitap6x10xn_v200r006c10.bin
```

Related Topics

14.1.24 ap update reset

14.1.92 display ap update status

14.1.21 ap update mode

Function

The **ap update mode** command configures the AP upgrade mode.

The **undo ap update mode** command restores the default AP upgrade mode.

The default upgrade mode is **ftp-mode**.

Format

ap update mode { **ftp-mode** | **sftp-mode** }

undo ap update mode

Parameters

Parameter	Description	Value
ftp-mode	Indicates the FTP mode. The AC delivers the FTP configuration to APs using the **14.1.18 ap update ftp-server** command, and APs download the upgrade version file from the FTP server.	-

Parameter	Description	Value
sftp-mode	Indicates the SFTP mode. The AC delivers the SFTP configuration to APs using the **14.1.25 ap update sftp-server** command, and APs download the upgrade version file from the SFTP server.	-

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

- The AC, FTP or SFTP upgrade mode must be preset on the AP for automatic upgrade and online upgrade.
- Run the **ap update multi-load** command to upgrade the AP.

Example

Set the AP upgrade mode to **sftp-mode**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update mode sftp-mode
Info:Changing AP update mode causes an AP update failure, continue?[Y/N]:Y
```

Related Topics

14.1.91 display ap update configuration

14.1.22 ap update multi-load

Function

The **ap update multi-load** command upgrades APs of the same type in batches.

The **undo ap update multi-load** command cancels batch upgrade of APs with the same type.

Format

ap update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

ap update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

undo ap update multi-load ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

undo ap update multi-load ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to 255.
ap-group *group-name*	Specifies an AP group.	The AP group must exist.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ap update multi-load ap-type** *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] command to upgrade APs of the same type in batches in the online upgrade mode.

- If **ap-group** *group-name* is specified, only APs of the same type and in the specified AP group are upgraded.
- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs of the specified type and with the specified AP name or AP ID are upgraded
- If none of the **ap-group** *group-name*, **ap-name** *ap-name*, and **ap-id** *ap-id* parameters are specified, all APs of the specified type are upgraded.
- If the type of APs specified by **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from **ap-type** *type-id*, the APs cannot be upgraded.

You can run the **ap update multi-load ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] command to batch upgrade APs in the specified AP group online.

- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs with the specified name or ID in the specified AP group are upgraded.

- If neither **ap-name** *ap-name* nor **ap-id** *ap-id* is specified, all APs in the specified AP group are upgraded.
- If APs specified by **ap-name** *ap-name* and **ap-id** *ap-id* are in different AP groups, the APs cannot be upgraded.

Prerequisites

AP upgrade files have been configured in batches using the **ap update update-filename** command.

Follow-up Procedure

Run the **ap update multi-reset** command to reset APs in batches to make AP upgrade take effect.

Precautions

The **undo ap update multi-load** command cancels batch upgrade of APs with the same type. However, if the AP system software has been written to the flash memory during the upgrade, the command does not take effect. You can run the **display ap update status all** command to check AP upgrade progress.

Example

Upgrade APs with *type-id* 19 in batches online.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update multi-load ap-type 19
```

Upgrade all APs in AP group **ap-group1** in batches online.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update multi-load ap-group ap-group1
```

Related Topics

14.1.27 ap update update-filename

14.1.23 ap update multi-reset

14.1.92 display ap update status

14.1.23 ap update multi-reset

Function

The **ap update multi-reset** command resets APs of the same type in batches.

Format

ap update multi-reset ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>]

ap update multi-reset ap-group *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>]

Parameters

Parameter	Description	Value
ap-type *type-id*	Resets APs of the specified type ID.	The AP type ID must exist.
ap-group *group-name*	Resets APs in the specified AP group.	The AP group must exist.
ap-name *ap-name*	Resets APs with the specified AP name.	The AP name must exist.
ap-id *ap-id*	Resets APs with the specified AP ID.	The AP ID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

This command resets APs of the same type in batches and can be used only after APs are upgraded in batches.

ap update multi-reset ap-type *type-id* [**ap-group** *group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } &<1-10>] command to batch reset APs of the specified type online.

- If **ap-group** *group-name* is specified, only APs of the specified type and in the specified AP group are reset.
- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs of the specified type and with the specified AP name or ID are reset.
- If none of the **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* parameters are specified, all APs of the specified type are reset.
- If the type of APs specified by **ap-group** *group-name*, **ap-name** *ap-name*, or **ap-id** *ap-id* is different from **ap-type** *type-id*, the APs cannot be reset.

You can run the **ap update multi-reset ap-group** *group-name* [{ **ap-name** *ap-name* } &<1-10> | { **ap-id** *ap-id* } &<1-10>] command to batch reset APs in the specified AP group online.

- If **ap-name** *ap-name* or **ap-id** *ap-id* is specified, only APs with the specified name or ID in the specified AP group are reset.
- If neither **ap-name** *ap-name* nor **ap-id** *ap-id* is specified, all APs in the specified AP group are reset.
- If APs specified by **ap-name** *ap-name* and **ap-id** *ap-id* are in different AP groups, the APs cannot be reset.

 Copyright © Huawei Technologies Co., Ltd.

Example

Reset APs with **type-id** 19 in batches.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update multi-reset ap-type 19
```

14.1.24 ap update reset

Function

The **ap update reset** command restarts a specified AP.

Format

ap update reset { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of the AP to be restarted.	The AP name must already exist.
ap-mac *ap-mac*	Specifies the MAC address of the AP to be restarted.	The AP's MAC address must already exist.
ap-id *ap-id*	Specifies the ID of the AP to be restarted.	The AP ID must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a single AP has been upgraded, run the **ap update reset** command to restart the AP and make the AP upgrade take effect.

Prerequisites

The AP is in normal or vmiss state.

The specified AP has been upgraded using the **ap update load** { **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* } **update-filename** *update-file-name* command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Restart AP **N1-2** after the upgrade.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update load ap-name N1-2 update-filename huawei.bin
[Huawei-wlan-view] ap update reset ap-name N1-2
```

Related Topics

14.1.20 ap update load

14.1.25 ap update sftp-server

Function

The **ap update sftp-server** command configures basic sftp information, including the sftp server IP address, sftp server user name and password.

The **undo ap update sftp-server** command restores default sftp settings.

By default, no SFTP server IP address is configured, The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

ap update sftp-server ip-address *server-ip-address* **sftp-username** *sftp-username* **sftp-password cipher** *sftp-password*

undo ap update sftp-server

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies an IPv4 address for the sftp server.	The value is in dotted decimal notation.
sftp-username *sftp-username*	Specifies the sftp server user name.	The value is a string of 1 to 31 characters. The value cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ") or spaces.
sftp-password	Specifies the password for logging in to the sftp server.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher	Specifies the password in cipher text.	-
sftp-password	Specifies the sftp server password.	The value is a string of characters without question marks (?) or spaces. It cannot start or end with double quotation marks (" ") or spaces. *sftp-password* can be up to 68 characters in cipher text, such as %^%#A<g;&zQR7P3TF+,[MxQ1X%4[2~Gb]Vp#(e<y:~)/%^%#. *sftp-password* also can be a string of 1 to 31 characters in plain text, such as **huawei123**.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

- The sftp configuration is used when the automatic upgrade and online upgrade modes are sftp. In the automatic upgrade or online upgrade, the AC sends basic sftp information to the AP, and the AP requests the sftp server for upgrade based on sftp information.
- After running the **ap update sftp-server** command, you can perform the following operations:
  a. Run the **ap update mode** command to set the upgrade mode to sftp-mode.
  b. Run the **ap update multi-load** command to upgrade APs in batches.

Precautions

- It is recommended that you use an external sftp server to upgrade APs. If the AC functions as the sftp server, a maximum of five APs can be upgraded simultaneously.
- APs do not support the following characters: ". Ensure that the sftp server user name and unencrypted password configured on the AC do not contain the preceding characters. Otherwise, sftp upgrade fails.

Example

Configure the sftp server IP address, sftp server user name and password.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update sftp-server ip-address 192.168.1.100 sftp-username admin sftp-
password cipher wlanadmin
```

Related Topics

14.1.21 ap update mode

14.1.22 ap update multi-load

14.1.91 display ap update configuration

14.1.26 ap update sftp-server max-connect-number

Function

The **ap update sftp-server max-connect-number** command configures the maximum number of APs that can be upgraded simultaneously in SFTP mode.

The **undo ap update sftp-server** command restores the default maximum number of APs that can be upgraded simultaneously in SFTP mode.

By default, a maximum of 50 APs can be upgraded simultaneously in SFTP mode.

Format

ap update sftp-server max-connect-number *max-connect-number*

undo ap update sftp-server max-connect-number

Parameters

Parameter	Description	Value
max-connect-number	Specifies the maximum number of APs that can be upgraded simultaneously.	The value is an integer that ranges from 1 to 64.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When APs are upgraded in SFTP mode, you can configure the value of *max-connect-number* to change the maximum number of APs that can be upgraded simultaneously.

- If the number of APs to be upgraded is equal to or smaller than *max-connect-number*, all APs can be upgraded simultaneously.
- If the number of APs to be upgraded is larger than *max-connect-number*, only the specified number of APs can be upgraded simultaneously. After the specified number of APs are upgraded, the remaining APs are upgraded automatically until all APs are upgraded. The number of APs that are upgraded at a time cannot exceed the value of *max-connect-number*.

Precautions

An external SFTP server can be used, which is recommended. The AC can also function as the SFTP server.

- When an external SFTP server is used, the maximum number of APs that can be upgraded simultaneously is the configured *max-connect-number*.
- If an AC is used as the SFTP server, a maximum of five APs can be upgraded simultaneously even if the specified number is larger than five.

  When the AC functions as the SFTP server, run the **ap update sftp-server max-connect-number** *max-connect-number* command to set the maximum number of APs that can be upgraded simultaneously. The value of *max-connect-number* is an integer ranging from 1 to 5. During the upgrade, a maximum of 1 to 5 APs can be upgraded at a time until all APs are upgraded.

  If *max-connect-number* is set larger than 5, an error message will be displayed after the first five APs are upgraded. The remaining APs cannot be automatically upgraded. You have to repeat the command until all APs are upgraded.

Example

Set the maximum number of APs that can be upgraded simultaneously in SFTP mode to 10.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update sftp-server max-connect-number 10
```

Related Topics

14.1.21 ap update mode
14.1.22 ap update multi-load
14.1.91 display ap update configuration

14.1.27 ap update update-filename

Function

The **ap update update-filename** command configures the upgrade file name for APs of a specified type.

The **undo ap update update-filename** command deletes the upgrade file name for APs of a specified type.

Format

ap update update-filename *filename* **ap-type** *type-id* [**ap-group** *ap-group-name*]

undo ap update update-filename ap-type *type-id* [**ap-group** *ap-group-name*]

Parameters

Parameter	Description	Value
ap-type *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to 255.
filename	Specifies the AP upgrade file name.	The value is a string of 1 to 255 case-sensitive characters. Ensure that the file name is the same as the actual upgrade file name and has the extension .bin.
ap-group *ap-group-name*	Specifies an AP group.	The AP group must already exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

If you specify **ap-group** *ap-group-name*, the command configures the upgrade file name only for APs of the specified type and in the specified group.

Run the **ap update multi-load ap-type** command to upgrade APs of the same type in batches.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the upgrade file name for APs with the type ID 19 to **fitap6x10xn_v200r006c10.bin**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap update update-filename fitap6x10xn_v200r006c10.bin ap-type 19
```

Related Topics

14.1.22 ap update multi-load

14.1.28 ap username

Function

The **ap username** command sets the user name and password for AP login.

The **undo ap username** command restores the default user name and password for AP login.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

ap username *username* **password cipher**

undo ap username

Parameters

Parameter	Description	Value
username	Specifies the user name for AP login.	The value is a string of 4-31 characters. It can contain letters, underlines, and digits. The character string must start with letters.
password	Specifies the password for AP login.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher	Indicates the cipher text password.	The password can be entered in plain or cipher text: ● In plain text, the password is a string of 8 to 32 case-sensitive characters. It must contain at least one uppercase letter, one lowercase letter, and one digit except the question mark (?). ● In cipher text, the password is a string of 48 or 68 characters. It must contain at least one uppercase letter, one lowercase letter, and one digit.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Unauthorized users may use the default user name and password to log in to APs, causing security risk to APs. You can use the **ap username** command to change the user name and password to improve security for APs.

NOTE

It is recommended that you change the user name and password in a timely manner to ensure device security.

The password cannot be the same as the user name or the mirror user name.

Example

Set the user name to **huawei** and password to **Zz123456**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap username huawei password cipher
Enter the password (plain-text password of 8-32 characters or cipher-text passwo
rd of 48 or 68 characters that must contain at least one lowercase letter, one uppercase letter, and one
digit):
Confirm password:
```

Related Topics

14.1.77 display ap global configuration

14.1.93 display ap username

14.1.29 ap whitelist

Function

The **ap whitelist** command adds an AP to an AP whitelist.

The **undo ap whitelist** command deletes an AP from an AP whitelist.

By default, no AP is in an AP whitelist.

Format

ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }

undo ap whitelist { **mac** *ap-mac1* [**to** *ap-mac2*] | **sn** *ap-sn1* [**to** *ap-sn2*] }

Parameters

Parameter	Description	Value
mac *ap-mac1*	Specifies the AP MAC address.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
to *ap-mac2*	Specifies the end MAC address. This parameter is used when you want to add multiple MAC addresses to the whitelist. The value must be larger than *ap-mac1*. *ap-mac1* and *ap-mac2* identify a range.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
sn *ap-sn1*	Specifies the SN of an AP.	The value is a string of 1 to 31 characters.
to *ap-sn2*	Specifies the end SN. This parameter is used when you want to add multiple SNs to the whitelist. It must be larger than *ap-sn1*. *ap-sn1* and *ap-sn2* identify a range.	The value is a string of 1 to 31 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- When the AP authentication mode is set to MAC address authentication using the **14.1.11 ap auth-mode** command, if the MAC address of an online AP exists in the whitelist, the AP is automatically added to the AC. If the MAC address of an AP is not in the whitelist, the AP can go online only after its identity is confirmed by the user using the **14.1.30 ap-confirm** command.
- When the AP authentication mode is set to SN authentication using the **14.1.11 ap auth-mode** command, if the SN of an online AP exists in the whitelist, the AP is automatically added to the AC. If the SN of an AP is not in the whitelist, the AP can go online only after its identity is confirmed by the user using the **14.1.30 ap-confirm** command.

Prerequisites

The AP authentication mode has been set to MAC address or SN authentication using the **14.1.11 ap auth-mode** command.

Precautions

When adding multiple SNs to the whitelist, ensure that the start SN length and the end SN length are the same.

Example

Add AP MAC address 0025-9e07-8280 to the whitelist.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap whitelist mac 0025-9e07-8280
```

Add the MAC addresses from 0025-9e07-8270 to 0025-9e07-8290 to the AP whitelist.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap whitelist mac 0025-9e07-8270 to 0025-9e07-8290
```

Add SN 08PE56430071 to the AP whitelist.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap whitelist sn 08PE56430071
```

Add SNs from 08PE56430076 to 08PE56430081 to the AP whitelist.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap whitelist sn 08PE56430076 to 08PE56430081
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.95 display ap whitelist
14.1.11 ap auth-mode
14.1.30 ap-confirm

14.1.30 ap-confirm

Function

The **ap-confirm** command confirms unauthenticated APs and allows them to go online.

Format

ap-confirm { **all** | **mac** *ap-mac* | **sn** *ap-sn* }

Parameters

Parameter	Description	Value
all	Confirms all APs.	-
mac *ap-mac*	Confirms the AP with the specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
sn *ap-sn*	Confirms the AP with the specified SN.	The value is a string of 1 to 31 characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After viewing unauthenticated APs using the **14.1.89 display ap unauthorized record** command, you can run the **ap-confirm** command to confirm these unauthenticated APs if you want to connect them to the AC. After confirmation, the APs are allowed to go online, added to the default region, and bound to the default AP profile.

Example

Confirm the AP with MAC 0025-9e07-8270.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-confirm mac 0025-9e07-8270
```

Confirm all APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-confirm all
```

Related Topics

14.1.70 display ap

14.1.95 display ap whitelist

14.1.77 display ap global configuration

14.1.31 ap-group

Function

The **ap-group** command creates an AP group and displays the AP group view, or displays the view of an existing AP group.

The **undo ap-group** command deletes an AP group.

By default, the system provides the AP group **default**.

Format

ap-group name *group-name*

undo ap-group { **name** *group-name* | **all** }

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of an AP group.	The value is a string of 1 to 35 characters. It does not contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ").
all	Deletes all AP groups.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same configuration on multiple APs, add the APs to an AP group and perform the configuration in the AP group. The configuration takes effect on all APs of the group. This prevents repetitive configuration.

Follow-up Procedure

Run the **14.1.32 ap-group (AP view)** or **14.1.38 ap-regroup** command to add APs to an AP group.

Precautions

- If the configuration of an AP in the AP view is different from that in the AP group view, the configuration in the AP view is preferentially used.
- The device supports a maximum of 256 AP groups.
- The AP group that has APs cannot be deleted. The AP group **default** cannot be deleted either.
- By default, an AP group has the following profiles bound: AP system profile **default**, 2G radio profile **default**, 5G radio profile **default**, regulatory domain profile **default**, WIDS profile **default**, and AP wired port profile **default**.

Example

Create the AP group **group1** and display the AP group view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1]
```

Related Topics

14.1.32 ap-group (AP view)

14.1.38 ap-regroup

14.1.97 display ap-group

14.1.32 ap-group (AP view)

Function

The **ap-group** command configures an AP group.

The **undo ap-group** command restores the default AP group.

By default, no AP group is configured.

Format

ap-group *ap-group*

undo ap-group

Parameters

Parameter	Description	Value
ap-group	Specifies an AP group.	The AP group must exist.

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to perform the same configuration on multiple APs, add the APs to an AP group and perform the configuration in the AP group. The configuration takes effect on all APs of the group. This prevents you from configuring each AP one by one.

Each AP must be added to an AP group. If no AP group is configured for an AP, the AP automatically joins the AP group **default**.

Example

Configure the AP group **ap-new-group** for an AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 0
[Huawei-wlan-ap-0] ap-group ap-new-group
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
```

14.1.33 ap-id

Function

The **ap-id** command adds an AP offline or displays the AP view.

By default, no AP is added offline.

Format

ap-id *ap-id* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-mac** *ap-mac*] [**ap-sn** *ap-sn*]

Parameters

Parameter	Description	Value
ap-id	Specifies the AP ID.	The value is an integer. The value range varies according to devices: ● AR150 series: 0 to 15 ● AR100series, AR120 series and AR160 series: 0 to 15 ● AR200 series: 0 to 15 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D and AR2204E: 0 to 31 ● AR2220, AR2220E, AR2230: 0 to 63 ● AR2204XE and AR2204XE-DC: 0 to 255 ● AR2240 and AR3200 series: – SRU40: 0 to 127 – SRU60: 0 to 127 – SRU80: 0 to 255 – SRU100E: 0 to 255 – SRU200 and SRU200E: 0 to 255 – SRU400: 0 to 511 ● AR2240C: 0 to 127 ● AR3600 series: 0 to 255
type-id *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to 255.
ap-type *ap-type*	Specifies the AP type.	The value is a string of 1 to 31 characters.
ap-mac *ap-mac*	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
ap-sn *ap-sn*	Specifies the sequence number (SN) of an AP.	The value is a string of 1 to 31 characters, and can only contain letters and digits.

Views

WLAN view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP is successfully added to an AC, you can configure parameters for the AP offline. When the AP goes online, it uses the configured parameters.

Precautions

To add an AP, enter the MAC address of the AP if the AP authentication mode is MAC address authentication. If the AP authentication mode is SN authentication, enter the SN of the AP.

To enter the AP view, you only need to enter the AP ID.

Example

Create an AP with ID **11**, type ID **19**, and MAC address **0025-9e07-8270**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 11 type-id 19 ap-mac 0025-9e07-8270
```

Related Topics

14.1.70 display ap

14.1.34 ap-mac

Function

The **ap-mac** command adds an AP offline or displays the AP view.

By default, no AP is added offline.

Format

ap-mac *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*]

Parameters

Parameter	Description	Value
ap-mac	Specifies the MAC address of an AP.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
type-id *type-id*	Specifies the AP type ID.	The value is an integer that ranges from 0 to 255.
ap-type *ap-type*	Specifies the AP type.	The value is a string of 1 to 31 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ap-id *ap-id*	Specifies the AP ID.	The value is an integer. The value range varies according to devices: ● AR150 series: 0 to 15 ● AR100series, AR120 series and AR160 series: 0 to 15 ● AR200 series: 0 to 15 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D and AR2204E: 0 to 31 ● AR2220, AR2220E, AR2230: 0 to 63 ● AR2204XE and AR2204XE-DC: 0 to 255 ● AR2240 and AR3200 series: – SRU40: 0 to 127 – SRU60: 0 to 127 – SRU80: 0 to 255 – SRU100E: 0 to 255 – SRU200 and SRU200E: 0 to 255 – SRU400: 0 to 511 ● AR2240C: 0 to 127 ● AR3600 series: 0 to 255
ap-sn *ap-sn*	Specifies the sequence number (SN) of an AP.	The value is a string of 1 to 31 characters, and can only contain letters and digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an AP is successfully added to an AC, you can configure parameters for the AP offline. When the AP goes online, it uses the configured parameters.

Precautions

When adding an AP, you need to enter the MAC address of the AP. If the AP authentication mode is SN authentication, you also need to enter the SN of the AP.

To enter the AP view, you only need to enter the MAC address of the AP. If the entered MAC address does not exist, the system adds a new AP and displays the AP view.

The **ap-mac** *ap-mac* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-id** *ap-id*] [**ap-sn** *ap-sn*] and **ap-id** *ap-id* [**type-id** *type-id* | **ap-type** *ap-type*] [**ap-mac** *ap-mac*] [**ap-sn** *ap-sn*] commands have the same function. You can use either one according to the actual situation.

Example

Add the AP with the MAC address **0025-9e07-8260**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-mac 0025-9e07-8260
```

Related Topics

14.1.70 display ap

14.1.35 ap-name

Function

The **ap-name** command displays the AP view.

Format

ap-name *ap-name*

Parameters

Parameter	Description	Value
ap-name	Specifies the AP name.	The AP name must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After entering the AP view, you can perform personalized configuration on an AP.

Example

Display the view of the AP named **area_1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-name area_1
[Huawei-wlan-area_1]
```

Related Topics

14.1.70 display ap

14.1.36 ap-name (AP view)

Function

The **ap-name** command configures an AP name.

The **undo ap-name** command restores the default AP name.

By default, no AP name is configured for an AP.

Format

ap-name *ap-name*

undo ap-name

Parameters

Parameter	Description	Value
ap-name	Specifies an AP name.	The value is a string of 1 to 31 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Views

AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To facilitate AP maintenance, management, and differentiation, you can name the AP according to actual situations.

Precautions

The new AP name cannot be the same as the existing AP name.

 Copyright © Huawei Technologies Co., Ltd.

Example

Change the AP name to **AP-N1-2**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 0
[Huawei-wlan-ap-0] ap-name AP-N1-2
```

14.1.37 ap-ping

Function

The **ap-ping** command uses a specified AP to ping a network device and displays the returned result.

Format

ap-ping { **ap-name** *ap-name* | **ap-id** *ap-id* } [**-c** *count* | **-s** *packetsize* | **-m** *time* | **-t** *timeout*] * *host*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP used to ping other network devices.	The AP name must already exist.
ap-id *ap-id*	Specifies the ID of an AP used to ping other network devices.	The AP ID must already exist.
-c *count*	Specifies the number of ICMP Echo Request packets to be sent.	The value is an integer that ranges from 1 to 10. The default value is 4.
-s *packetsize*	Specifies the length of an Echo Request packet excluding the IP header and ICMP header.	The value is an integer that ranges from 20 to 8100, in bytes. The default value is 56 bytes.
-m *time*	Specifies the time to wait before sending the next ICMP Request packet.	The value is an integer that ranges from 1 to 5000, in milliseconds. The default value is 2000 ms.
-t *timeout*	Specifies the timeout period for an ICMP Echo Response packet.	The value is an integer that ranges from 0 to 10000, in milliseconds. The default value is 2000 ms.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host	Specifies the domain name or IP address of the destination host.	The value is a string of 1 to 20 characters.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- You can run this command to check the connectivity between an AP and network device by pinging a network device from an AP.
- The prerequisite is that the AP is online and has been configured with an IP address.

Precautions

- This command may cost much time because the parameters such as waiting time affects the command running.
- Only one AP can perform the ping operation at a time.

Example

Use the AP **N1-2** to perform a ping operation.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-ping ap-name N1-2 192.168.0.1
Warning: This operation maybe takes several minutes, continue?[Y/N]:y
[Huawei-wlan-view]
  AP ping result
    Success count        : 4
    Failure count        : 0
    Average response time: 1 ms
    Minimum response time: 1 ms
    Maximum response time: 1 ms
```

14.1.38 ap-regroup

Function

The **ap-regroup** command changes the group that an AP joins.

Format

ap-regroup { **ap-name** *ap-name* | **ap-id** *ap-id* } **new-group** *new-group-name*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
new-group *new-group-name*	Specifies the name of the new group to which the AP is added.	The AP group must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the current AP group is not applicable to an AP or the AP is added to an incorrect group, you can run this command to delete the AP from the current AP group and add the AP to a new AP group.

Prerequisites

The AP group has been created using the **14.1.31 ap-group** command.

Configuration Impact

Changing the group of an AP will restart the AP and interrupt services. Exercise caution when you run the command.

Example

Change the group that an AP joins to the AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] quit
[Huawei-wlan-view] ap-regroup ap-name 1047-80b1-56a0 new-group group1
Warning: This operation may cause AP reset. If the country code changes, it will clear channel, power and antenna gain configuration
s of the radio, Whether to continue? [Y/N]:y
```

Related Topics

14.1.31 ap-group

14.1.70 display ap

14.1.39 ap-rename

Function

The **ap-rename** command changes the name of an AP.

Format

ap-rename { **ap-name** *name* | **ap-mac** *ap-mac-address* | **ap-id** *ap-id* } **new-name** *ap-new-name*

Parameters

Parameter	Description	Value
ap-name *name*	Specifies the old name of an AP.	The AP name must exist.
ap-mac *ap-mac-address*	Specifies the MAC address of an AP.	The AP's MAC address must exist.
ap-id *ap-id*	Specifies the ID of an AP.	The AP ID must exist.
new-name *ap-new-name*	Specifies the new name of an AP.	The value is a string of 1 to 31 case-sensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

If the name of an AP conflicts with that of another or an AP requires a more proper name, you can run this command to change the name of the AP.

Example

Change the AP name from **N1-2** to **N2-2**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-rename ap-name N1-2 new-name N2-2
```

Related Topics

14.1.70 display ap

14.1.40 ap-reset

Function

The **ap-reset** command resets an AP.

Format

ap-reset { **all** | **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* | **ap-group** *ap-group* | **ap-type** { **type** *type-name* | **type-id** *type-id* } }

Parameters

Parameter	Description	Value
all	Resets all APs.	-
ap-name *ap-name*	Resets the AP with the specified AP name.	The AP name must exist.
ap-mac *ap-mac*	Resets the AP with the specified MAC address.	The AP's MAC address must exist.
ap-id *ap-id*	Resets the AP with the specified AP ID.	The AP ID must exist. The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) or hyphens (-) to separate AP IDs. For example, **5,8,10-13,20** indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.
ap-group *ap-group*	Resets APs in the specified AP group.	The AP group must exist.
ap-type	Resets APs of the specified AP type.	-
type *type-name*	Resets APs of the specified type name.	The AP type name must exist.

Parameter	Description	Value
type-id *type-id*	Resets APs of the specified type ID.	The AP type ID must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After in-service upgrade of APs is complete, you can run the **ap-reset** command to reset the APs. After the command is run, the APs restart with the upgraded software version. You can also use the command to restart APs for other reasons.

Prerequisites

An AP exists on the AC.

Example

Reset the AP **N1-2**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-reset ap-name N1-2
Warning: Reset AP(s), continue?[Y/N]:y
```

14.1.41 ap-system-profile (WLAN view)

Function

The **ap-system-profile** command creates an AP system profile and displays the AP system profile view, or displays the view of an existing AP system profile.

The **undo ap-system-profile** command deletes an AP system profile.

By default, the system provides the AP system profile **default**.

Format

ap-system-profile name *profile-name*

undo ap-system-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP system profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all AP system profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To manage and maintain multiple APs in a centralized manner, add the APs in an AP group, configure parameters in an AP system profile, and apply the AP system profile to the AP group.

To manage and maintain an AP independently, configure parameters in an AP system profile and apply the AP system profile to the AP specific profile.

Follow-up Procedure

Run the **14.1.42 ap-system-profile (AP group view and AP view)** command to bind the AP system profile to an AP or AP group so that the AP system profile can take effect.

Precautions

- The AP system profile **default** cannot be deleted.
- The AP system profile referenced by an AP or AP group cannot be deleted. To delete the AP system profile, unbind it from the AP or AP group first.

Example

Create the AP system profile **ap-system1** and display the AP system profile view.

```
<Huawei> system-view
[Huawei] wlan ac
```

```
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1]
```

Related Topics

14.1.42 ap-system-profile (AP group view and AP view)

14.1.98 display ap-system-profile

14.1.42 ap-system-profile (AP group view and AP view)

Function

The **ap-system-profile** command binds an AP system profile to an AP or AP group.

The **undo ap-system-profile** command unbinds an AP system profile from an AP or AP group.

By default, the AP system profile **default** is bound to an AP group, but no AP system profile is bound to an AP.

Format

ap-system-profile *profile-name*

undo ap-system-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP system profile.	The AP system profile must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP system profile using the **14.1.41 ap-system-profile (WLAN view)** command, bind it to an AP or AP group so that the AP system profile can take effect.

Precautions

After an AP system profile is bound to an AP or AP group, parameter settings in the AP system profile apply to all APs using the profile.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create the AP system profile **ap-system1** and bind it to AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] ap-system-profile ap-system1
```

Related Topics

14.1.31 ap-group

14.1.41 ap-system-profile (WLAN view)

14.1.108 display references ap-system-profile

14.1.43 association-timeout

Function

The **association-timeout** command configures an association aging time for STAs.

The **undo association-timeout** command restores the default association aging time.

By default, the association aging time is 5 minutes.

Format

association-timeout *association-timeout*

undo association-timeout

Parameters

Parameter	Description	Value
association-timeout	Specifies the association aging time of STAs.	The value is an integer that ranges from 1 to 30, in minutes.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The administrator can run the **association-timeout** command to set the association aging time for STAs. If the AP receives no data packet from a STA in a specified time, the STA goes offline after the association aging time expires.

Precautions

Changing the association aging time of a STA may interrupt the STA services.

Example

Set the association aging time of STAs to 15 minutes in the SSID profile **ssid1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] association-timeout 15
Warning: This action may cause service interruption. Continue?[Y/N]y
```

Related Topics

14.1.118 display ssid-profile

14.1.44 beacon-2g-rate

Function

The **beacon-2g-rate** command sets the transmit rate of 2.4 GHz Beacon frames.

The **undo beacon-2g-rate** command restores the default transmit rate of 2.4 GHz Beacon frames.

By default, the transmit rate of 2.4 GHz Beacon frames is 1 Mbit/s.

Format

beacon-2g-rate *beacon-2g-rate*

undo beacon-2g-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
beacon-2g-rate	Specifies the transmit rate of Beacon frames.	Enumerated type: • 1: 1 Mbit/s • 2: 2 Mbit/s • 5.5: 5.5 Mbit/s • 6: 6 Mbit/s • 9: 9 Mbit/s • 11: 11 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Beacon frames occupy a large number of wireless resources. To reduce wireless resource occupation of Beacon frames and improve channel usage efficiency, you can run the **beacon-2g-rate** command to set a large transmit rate for 2.4 GHz Beacon frames.

Precautions

Modifying the transmit rate of Beacon frames will affect the association experience of STAs. Exercise caution when running the command.

The 802.11b protocol supports only 1 Mbit/s, 2 Mbit/s, 5.5 Mbit/s, and 11 Mbit/s. If you set the transmit rate of Beacon frames to a rate not supported by the 802.11b protocol, STAs supporting only 802.11b cannot connect to the wireless network.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, *beacon-2g-rate* that takes effect on the 2 GHz radio of the AP has a fixed value of 1 Mbit/s, and *beacon-2g-rate* configured in the SSID profile view does not take effect on the AP.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the transmit rate of 2.4 GHz Beacon frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] beacon-2g-rate 18
```

Related Topics

14.1.118 display ssid-profile

14.1.188 radio-type (2G radio profile view)

14.1.45 beacon-5g-rate

Function

The **beacon-5g-rate** command sets the transmit rate of 5 GHz Beacon frames.

The **undo beacon-5g-rate** command restores the default transmit rate of 5 GHz Beacon frames.

By default, the transmit rate of 5 GHz Beacon frames is 6 Mbit/s.

Format

beacon-5g-rate *beacon-5g-rate*

undo beacon-5g-rate

Parameters

Parameter	Description	Value
beacon-5g-rate	Specifies the transmit rate of Beacon frames.	Enumerated type: • 6: 6 Mbit/s • 9: 9 Mbit/s • 12: 12 Mbit/s • 18: 18 Mbit/s • 24: 24 Mbit/s • 36: 36 Mbit/s • 48: 48 Mbit/s • 54: 54 Mbit/s

Views

SSID profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Beacon frames occupy a large number of wireless resources. To reduce wireless resource occupation of Beacon frames and improve channel usage efficiency, you can run the **beacon-5g-rate** command to set a large transmit rate for 5 GHz Beacon frames.

Precautions

Modifying the transmit rate of Beacon frames will affect the association experience of STAs. Exercise caution when running the command.

Example

Set the transmit rate of 5 GHz Beacon frames to 18 Mbit/s in the SSID profile **ssid1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] beacon-5g-rate 18
```

Related Topics

14.1.118 display ssid-profile

14.1.46 beacon-interval

Function

The **beacon-interval** command sets the interval for sending Beacon frames.

The **undo beacon-interval** restores the default interval for sending Beacon frames.

By default, the interval for sending Beacon frames is 100 ms.

Format

beacon-interval *beacon-interval*

undo beacon-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
beacon-interval	Specifies the interval for sending Beacon frames.	The value is an integer that ranges from 60 ms to 1000 ms

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

An AP broadcasts Beacon frames at intervals to notify STAs of an existing 802.11 network. After receiving a Beacon frame, a STA can modify parameters used to connect to the 802.11 network.

Example

Set the interval for sending Beacon frames to 200 ms in the 2G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] beacon-interval 200
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.47 capwap control-link-priority

Function

The **capwap control-link-priority** command configures the priority of CAPWAP management packets.

The **undo capwap control-link-priority** command restores the default priority of CAPWAP management packets.

By default, the priority of CAPWAP management packets is 7.

Format

capwap control-link-priority { **local** | **remote** } *priority-value*

undo capwap control-link-priority { **local** | **remote** }

Parameters

Parameter	Description	Value
local	Indicates the priority of CAPWAP management packets from an AC to an AP. The priority of CAPWAP management packets determines the reliability of the link between an AC and an AP.	-
remote	Indicates the priority of CAPWAP management packets from an AP to an AC. The priority of CAPWAP management packets determines the reliability of the link between an AP and an AC.	-
priority-value	Specifies the priority of CAPWAP management packets.	The value is an integer that ranges from 0 to 7. The value 0 indicates the lowest priority, and the value 7 indicates the highest priority.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **capwap control-link-priority** command to configure the DSCP priority of CAPWAP management packets. A higher priority indicates a more reliable link between the AC and AP.

The configuration of the priority of CAPWAP management packets from an AC to an AP takes effect immediately. After the priority of CAPWAP management packets from an AP to an AC is changed, if the AP is online, the priority is sent to the AP in the Echo packet. If the AP is not online, the priority is delivered to the AP in the Echo packet when the AP goes online. The new priority takes effect once the AP receives it.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

NOTICE

Configure priority 4 to 7 for CAPWAP management packets from an AC to an AP, preventing the CAPWAP management tunnel from being interrupted due to large traffic.

Example

Set the priority of CAPWAP management packets from an AC to an AP to 6.

```
<Huawei> system-view
[Huawei] capwap control-link-priority local 6
```

Related Topics

14.1.100 display capwap configuration

14.1.48 capwap dtls control-link encrypt

Function

The **capwap dtls control-link encrypt** command enables the function of encrypting the CAPWAP control tunnel using Datagram Transport Layer Security (DTLS).

The **undo capwap dtls control-link encrypt** command disables the function of encrypting the CAPWAP control tunnel using DTLS.

By default, the function of encrypting the CAPWAP control tunnel using DTLS is enabled.

Format

capwap dtls control-link encrypt

undo capwap dtls control-link encrypt

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the Discovery phase of the CAPWAP tunnel establishment between the AP and the AC, the AP obtains the AC IP address using the discovery mechanism. Then in

 Copyright © Huawei Technologies Co., Ltd.

the DTLS negotiation phase, the CAPWAP tunnel encrypts UDP packets using DTLS.

After this command is run, the CAPWAP control packets between the AP and AC are encrypted using DTLS, and the AP and AC use the PSK to perform DTLS negotiation. If the DTLS negotiation fails, the CAPWAP tunnel cannot be established.

Configuration Impact

After this command is run, the AP and AC reestablish a CAPWAP tunnel.

Precautions

When APs are being upgraded, the status of DTLS encryption cannot be changed.

Example

Enable the function of encrypting the CAPWAP control tunnel using DTLS.

```
<Huawei> system-view
[Huawei] capwap dtls control-link encrypt
```

Related Topics

14.1.100 display capwap configuration

14.1.49 capwap dtls psk

Function

The **capwap dtls psk** command configures a pre-shared key used for DTLS encryption.

The **undo capwap dtls psk** command restores the default pre-shared key used for DTLS encryption.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

capwap dtls psk *psk-value*

undo capwap dtls psk

Parameters

Parameter	Description	Value
psk-value	Specifies the pre-shared key used for DTLS encryption.	The value is string of characters. The pre-shared key contains 48 or 68 characters in cipher text, for example, %^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#, or contains 6 to 32 characters in plain text, for example, a1234567. The password must contain at least two types of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

During the CAPWAP tunnel establishment between an AP and an AC, the AP performs a DTLS session with the AC as soon as the AP is associated with the AC. DTLS supports PSK encryption. When the pre-shared key is used for DTLS encryption, the **capwap dtls psk** command can be used to manually change the value in the DTLS session on the AC.

NOTE

It is recommended that you change the pre-shared key in a timely manner to ensure device security.

Follow-up Procedure

Run the **capwap dtls control-link encrypt** command to enable the function of encrypting the CAPWAP control tunnel using Datagram Transport Layer Security (DTLS).

Precautions

After the configuration is complete, the new pre-shared key will be automatically synchronized to online APs. However, the old pre-shared key takes effect on the APs. The new pre-shared key takes effect only after the APs goes offline and goes online again.

Example

Configure the pre-shared key for DTLS encryption as **z0020011@11**.

```
<Huawei> system-view
[Huawei] capwap dtls psk z0020011@11
Deliver DTLS PSK to devices using CAPWAP connections. It may take a few mi
nutes.
 ------------------------------------------------------------------------------
 CAPWAP DTLS PSK deliver result
 Deliver Number : 0
 Success Number : 0
 Failed  Number : 0
------------------------------------------------------------------------------
```

Related Topics

14.1.48 capwap dtls control-link encrypt

14.1.50 capwap dtls psk-mandatory-match enable

14.1.100 display capwap configuration

14.1.50 capwap dtls psk-mandatory-match enable

Function

The **capwap dtls psk-mandatory-match enable** command enables an AP to establish a Datacom Transport Layer Security (DTLS) session with an AC using the default pre-shared key.

The **undo capwap dtls psk-mandatory-match enable** command disables an AP to establish a Datacom Transport Layer Security (DTLS) session with an AC using the default pre-shared key.

By default, an AP is not allowed to establish a DTLS session with an AC using the default pre-shared key.

Format

capwap dtls psk-mandatory-match enable

undo capwap dtls psk-mandatory-match enable

Parameters

None.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a new AP is added to the WLAN or the passwords of the AP and AC are different (for example, the password of the AC is changed but the AP is not online), you can enable the AP to perform DTLS sessions with the AC using the default pre-shared key. After three DTLS session failures, the AP notifies the AC of DTLS sessions using the default pre-shared key. In this way, a CAPWAP tunnel is established between the AP and the AC.

Example

Enable the AP to establish a DTLS session with the AC using the default pre-shared key.

```
<Huawei> system-view
[Huawei] capwap dtls psk-mandatory-match enable
```

Related Topics

14.1.100 display capwap configuration

14.1.51 capwap echo

Function

The **capwap echo** command sets the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections.

The **undo capwap echo** command restores the default CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections.

By default, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 6.

By default, if dual-link backup is enabled, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 3.

Format

capwap echo { **interval** *interval-value* | **times** *times-value* } *

undo capwap echo { **interval** | **times** }

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the CAPWAP heartbeat detection interval, the interval at which two detection packets are sent.	The value is an integer ranging from 20 to 300, in seconds.
times *times-value*	Specifies the number of CAPWAP heartbeat detections. If no response is received after the specified number of times, the link is considered disconnected.	The value is an integer ranging from 3 to 120.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined by CAPWAP, an AP and an AC send handshake packets periodically to maintain the data channel and management channel. If the AP does not receive packets from the AC within the heartbeat detection interval, it considers that the link between them is disconnected. Then the AP resets and releases its IP address, and reestablishes a link. If the AC does not receive packets from the AP within the heartbeat detection interval, it disconnects the link between the AC and the AP and reports an error message to the AP.

Precautions

If dual-link backup is enabled, the CAPWAP heartbeat detection interval is 25s and the number of CAPWAP heartbeat detections is 3. When the Wireless Distribution System (WDS) is required in dual-link backup configuration, the WDS link may be unstable and users may not access the network. You need to run this command to set the interval for CAPWAP heartbeat detection to 25 seconds and the number of CAPWAP heartbeat detections to 6.

After the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections are configured, the interval and the number of times for sending Echo packets are configured.

Radio traffic statistics packets are sent and received together with Echo packets.

If you set the CAPWAP heartbeat detection interval and the number of CAPWAP heartbeat detections smaller than the default values, the CAPWAP link reliability is degraded. Exercise caution when you set the values. The default values are recommended. If an AP goes offline unexpectedly, you can set a larger CAPWAP

 Copyright © Huawei Technologies Co., Ltd.

heartbeat detection interval and a larger number of CAPWAP heartbeat detections.

Example

Set the CAPWAP heartbeat detection interval to 30s and the number of CAPWAP heartbeat detections to 3.

```
<Huawei> system-view
[Huawei] capwap echo interval 30 times 3
```

Related Topics

14.1.47 capwap control-link-priority

14.1.100 display capwap configuration

14.1.52 capwap ipv6 enable

Function

The **capwap ipv6 enable** command enables CAPWAP tunnels to support IPv6 functions.

The **undo capwap ipv6 enable** command disables CAPWAP tunnels from supporting IPv6 functions.

By default, CAPWAP tunnels are disabled from supporting IPv6 functions.

Format

capwap ipv6 enable

undo capwap ipv6 enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, CAPWAP tunnels are disabled from supporting IPv6 functions. You can run the **capwap ipv6 enable** command to enable CAPWAP tunnels to support IPv6 functions.

Example

Enable CAPWAP tunnels to support IPv6 functions.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] capwap ipv6 enable
```

14.1.53 capwap message-integrity psk

Function

The **capwap message-integrity psk** command configures a pre-shared key (PSK) for checking integrity of CAPWAP packets.

The **undo capwap message-integrity psk** command deletes the PSK for checking integrity of CAPWAP packets.

By default, no PSK is configured for checking integrity of CAPWAP packets.

Format

capwap message-integrity psk *psk-value*

undo capwap message-integrity psk

Parameters

Parameter	Description	Value
psk-value	Specifies the PSK for checking integrity of CAPWAP packets.	The value can be a string of 48 or 68 characters in cipher text (for example, %^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#) or a string of 6 to 32 characters in plain text (for example, a1234567). The key must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

CAPWAP packets are transmitted between the AC and APs. This command is used to configure a PSK for checking integrity of CAPWAP packets to prevent the packets from being forged or tampered with and prevent malformed packet attacks.

NOTE

After the command is executed, all APs connected to the AC are restarted.

Example

Set the PSK for checking integrity of CAPWAP packets to **z0020011@11**.

```
<Huawei> system-view
[Huawei] capwap message-integrity psk z0020011@11
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

Related Topics

14.1.54 capwap message-integrity psk-mandatory-match enable

14.1.54 capwap message-integrity psk-mandatory-match enable

Function

The **capwap message-integrity psk-mandatory-match enable** command enables CAPWAP packets to reach the AC without integrity check.

The **undo capwap message-integrity psk-mandatory-match enable** command disables CAPWAP packets without integrity check from reaching the AC.

By default, CAPWAP packets without integrity check cannot be successfully sent to the AC.

Format

capwap message-integrity psk-mandatory-match enable

undo capwap message-integrity psk-mandatory-match enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

APs in earlier versions cannot receive the pre-shared key (PSK) for checking packet integrity from the AC. This command is used to control whether CAPWAP packets from APs in earlier versions can be successfully sent to the AC without integrity check.

NOTE

If this command is not executed, the APs that do not support packet integrity check cannot get online on the AC.

Example

Enable CAPWAP packets to reach the AC without integrity check.

```
<Huawei> system-view
[Huawei] capwap message-integrity psk-mandatory-match enable
```

Related Topics

14.1.53 capwap message-integrity psk

14.1.55 capwap sensitive-info psk

Function

The **capwap sensitive-info psk** command modifies the pre-shared key (PSK) for encrypting sensitive information.

The **undo capwap sensitive-info psk** command restores the default PSK for encrypting sensitive information.

By default, the default PSK is used for encrypting sensitive information.

Format

capwap sensitive-info psk *psk-value*

undo capwap sensitive-info psk

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
psk-value	Specifies the PSK for encrypting sensitive information.	The value can be a string of 48 or 68 characters in cipher text (for example, %^%#u(Oz:BL,QKYZw%-JWC*P8aGC,="C&M'OI*Gmt.V(%^%#) or a string of 6 to 32 characters in plain text (for example, a1234567). The key must contain at least two of the following: uppercase letters, lowercase letters, digits, and special characters except the question mark (?) and space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Sensitive information may be exchanged between the AC and APs, for example, FTP user name/password, AP login user name/password, and service configuration PSK. By default, a PSK is used for encrypting sensitive information. This command allows users to manually modify the PSK.

NOTE

After the command is executed, all APs connected to the AC are restarted.

Precautions

In dual-link backup and HSB scenarios, the PSK for encryption must be set to the same value on the active and standby ACs. Otherwise, APs cannot set up a CAPWAP tunnel with the standby AC.

 Copyright © Huawei Technologies Co., Ltd.

Example

Modify the PSK for encrypting sensitive information to **z0020011@11**.

```
<Huawei> system-view
[Huawei] capwap sensitive-info psk z0020011@11
Warning: This operation may cause devices using CAPWAP connections to reset or go offline. Continue? [Y/N]:y
```

14.1.56 capwap source interface

Function

The **capwap source interface** command configures the source interface that the AC uses to establish a CAPWAP tunnel with an access device.

The **undo capwap source interface** command restores the source interface that the AC uses to establish a CAPWAP tunnel with an access device to the default setting.

By default, no source interface is configured for the AC to establish a CAPWAP tunnel with the access device.

Format

capwap source interface { **loopback** *loopback-number* | **vlanif** *vlan-id* }

undo capwap source interface { **loopback** *loopback-number* | **vlanif** *vlan-id* }

Parameters

Parameter	Description	Value
loopback *loopback-number*	Configures a loopback interface as the source interface.	The value is an integer that ranges from 0 to 1023.
vlanif *vlan-id*	Configures a VLANIF interface as the source interface.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AC uses the IP address of the specified interface as the source IP address. All access devices connected to the AC can learn this IP address and use the IP address to communicate with the AC.

Prerequisites

A loopback interface or VLANIF interface has been created and has an IP address configured. If the loopback or VLANIF interface uses an IPv6 address, the IPv6 address can only be configured manually.

Example

Configure a loopback interface as the source interface.

```
<Huawei> system-view
[Huawei] interface loopback 20
[Huawei-LoopBack20] ip address 192.168.10.1 24
[Huawei-LoopBack20] quit
[Huawei] capwap source interface loopback 20
```

Related Topics

14.1.100 display capwap configuration

14.1.57 channel

Function

(AP group radio view) The **channel** command configures the working bandwidth and channel for all specified radios in an AP group.

(AP group radio view) The **undo channel** command restores the default working bandwidth and channel for all specified radios in an AP group.

(AP radio view) The **channel** command configures the working bandwidth and channel for an AP radio.

(AP radio view) The **undo channel** command cancels the configuration of the working bandwidth and channel on an AP radio. The working bandwidth and channel on the AP radio are then determined by those configured in the AP group radio view.

By default, the working bandwidth of a radio is 20 MHz, and no working channel is configured for a radio.

You can run the **14.1.74 display ap config-info** command to check the channel in use on a radio.

Format

channel { **20mhz** | **40mhz-minus** | **40mhz-plus** | **80mhz** | **160mhz** } *channel*

channel 80+80mhz *channel1 channel2*

undo channel

Parameters

Parameter	Description	Value
20mhz	Sets the working bandwidth of a radio to 20 MHz.	-
40mhz-minus	Sets the working bandwidth of a radio to 40 MHz Minus.	-
40mhz-plus	Sets the working bandwidth of a radio to 40 MHz Plus.	-
80mhz	Sets the working bandwidth of a radio to 80 MHz.	-
160mhz	Sets the working bandwidth of a radio to 160 MHz.	-
80+80mhz	Sets the working bandwidth of a radio to 80+80 MHz.	-
channel/ channel1/ channel2	Specifies the working channel for a radio. The channel is selected based on the country code and radio mode.	The parameter is an enumeration value. The value range is determined according to the country code and radio mode.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different radios use different channels. Channels for radios also vary in different countries and regions. Select channels based on the actual situations.

Precautions

The configured channel parameters must match the radio frequency band. For details about mappings between channel parameters and frequency bands, see *Country Codes & Channels Compliance*.

The 2.4 GHz radio does not support the 40 MHz Minus, 40 MHz Plus and 80 MHz bandwidth in FCC compliance regions (including America).

The channels you configure must be supported by the terminals; otherwise, the terminals cannot discover wireless signals. For example, when the country code is

 Copyright © Huawei Technologies Co., Ltd.

set to China, 5 GHz channels 36, 40, 44, 48, 52, 56, 60, and 64 can be configured. However, most terminals do not support these channels currently. If these channels are configured, the terminals cannot discover wireless signals. In this case, you can configure 5 GHz channels 149, 153, 157, 161, and 165, which are supported by the terminals.

If an AP detects radar signals on a channel, the channel cannot be configured as the radio channel of the AP in 30 minutes. However, the channel can be configured as the radio channel of other APs not detecting radar signals on it.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

NOTE

- The 80 MHz, 160 MHz, and 80+80 MHz working bandwidths are only supported in the 5G radio view.
- Only APs that support 802.11ac support the 80 MHz parameters.

Example

Set the working bandwidth to 20 MHz and channel to 6 for radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] channel 20mhz 6
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.58 channel-switch announcement disable

Function

The **channel-switch announcement disable** command disables an AP from sending an announcement when the channel is switched.

The **undo channel-switch announcement disable** command enables an AP to send an announcement when the channel is switched.

By default, the AP send an announcement when the channel is switched.

Format

channel-switch announcement disable

undo channel-switch announcement disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

When the AP works on a Depth First Select (DFS) channel, a radar detection is performed. The AP automatically switches to another channel because the DFS channel frequency may interfere with the radar frequency.

After the **undo channel-switch announcement disable** command is run, if the AP channel switches, the AP sends an Action frame to instruct STAs to switch channels after multiple Beacon intervals. The AP also switches the channel after the same intervals. The AP and STAs switch channels at the same time to prevent STA reassociations and ensure rapid service recovery.

NOTE

The channel switching announcement function must be supported by both the AP and STA.

Example

Disable the AP from sending an announcement after the channel is switched.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] channel-switch announcement disable
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.59 commit (WLAN view)

Function

The **commit** command commits configurations of a specified AP or all APs.

Format

commit { **all** | **ap-name** *ap-name* | **ap-id** { *ap-id1* [**to** *ap-id2*] } &<1-10> }

Parameters

Parameter	Description	Value
all	Commits configurations of all APs.	-

Parameter	Description	Value
ap-name *ap-name*	Commits configurations of a specified AP.	The AP name must exist.
ap-id *ap-id1*	Commits configurations of an AP with a specified ID.	The AP ID must exist.
to *ap-id2*	Specifies the end AP ID in a batch operation. The *ap-id2* value must be larger than the *ap-id1* value.	The AP ID must exist.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

You can configure attributes for APs on the AC. The configurations are delivered to APs only after you run the **commit** command to commit the configurations.

NOTE

If you commit configurations to a large number of APs simultaneously, some of the APs may fail to receive the configurations. In this case, you are advised to commit the configurations again.

Example

Commit the configuration of a specified AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] commit ap-name ap-1
Warning: Committing configuration may cause service interruption, continue?[Y/N]:y
```

Commit configurations of all APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] commit all
Warning: Committing configuration may cause service interruption, continue?[Y/N]:y
```

14.1.60 console disable

Function

The **console disable** command disables a user from logging in to the AP through a console interface.

The **undo console disable** command enables a user from logging in to the AP through a console interface.

By default, a user can log in to the AP through a console interface.

Format

console disable

undo console disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When a user cannot telnet or stelnet to the AP, the user can log in to the AP through a console interface to manage and configure the AP.

After the **console disable** command is run, unauthorized users cannot log in to the AP through the console interface to perform operations.

Example

Disable a user to log in to the AP through a console interface.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] console disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.61 country-code

Function

The **country-code** command configures a country code.

The **undo country-code** command restores the default country code.

By default, the country code **CN** is configured.

Format

country-code *country-code*

undo country-code

Parameters

Parameter	Description	Value
country-code	Specifies a country code.	The value is a string of characters. For specific values, see **Table 14-1**.

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Table 14-1 Country codes supported by ACs

Country Code	Country/Region
AE	United Arab Emirates
AM	Armenia
AR	Argentina
AT	Austria
AU	Australia
AZ	Azerbaijan
BE	Belgium
BG	Bulgaria
BH	Bahrain
BN	Brunei Darussalam
BO	Bolivia
BR	Brazil
BY	Belarus
BZ	Belize
CA	Canada
CH	Switzerland
CL	Chile

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
CN	China (default)
CO	Colombia
CR	Costa Rica
CY	Cyprus
CZ	Czech Republic
DE	Germany
DK	Denmark
DO	Dominican Republic
EC	Ecuador
EE	Estonia
EG	Egypt
ES	Spain
FI	Finland
FR	France
GB	United Kingdom
GE	Georgia
GR	Greece
GT	Guatemala
HK	Hong Kong, Special Administrative Region of China
HN	Honduras
HR	Croatia
HU	Hungary
ID	Indonesia
IE	Ireland
IL	Israel
IN	India
IQ	Iraq
IR	Iran
IS	Iceland
IT	Italy

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
JO	Jordan
JP	Japan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KW	Kuwait
KZ	Kazakhstan
LB	Lebanon
LI	Liechtenstein
LK	Sri Lanka
LT	Lithuania
LU	Luxembourg
LV	Latvia
MA	Morocco
MC	Monaco
MK	North Macedonia
MO	Macao, Special Administrative Region of China
MT	Malta
MX	Mexico
MY	Malaysia
NG	Nigeria
NL	Netherlands
NO	Norway
NZ	New Zealand
OM	Oman
PA	Panama
PE	Peru
PH	Philippines
PK	Pakistan
PL	Poland
PR	Puerto Rico

 Copyright © Huawei Technologies Co., Ltd.

Country Code	Country/Region
PT	Portugal
QA	Qatar
RO	Romania
RU	Russia
SA	Saudi Arabia
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SV	El Salvador
SY	Syria
TH	Thailand
TN	Tunisia
TR	Turkey
TT	Trinidad & Tobago
TW	Taiwan, Province of China
UA	Ukraine
US	United States
UY	Uruguay
UZ	Uzbekistan
VE	Venezuela
VN	Vietnam
YE	Yemen
ZA	South Africa
ZW	Zimbabwe

Usage Scenario

When an AC controls APs in different countries or regions, different country codes can be configured based on the regulatory domain profile to meet different radio requirements in different countries or regions, such as power requirements and channel requirements.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

Modifying the country code in a regulatory domain profile will restart APs using the profile.

Example

Set the country code to US in the regulatory domain profile **region1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] regulatory-domain-profile name region1
[Huawei-wlan-regulate-domain-region1] country-code us
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the
radio and reset the AP. Continu
e?[Y/N]:y
```

Related Topics

14.1.117 display regulatory-domain-profile

14.1.62 coverage distance

Function

(AP group radio view) The **coverage distance** command configures the radio coverage distance parameter for all specified radios in an AP group.

(AP group radio view) The **undo coverage distance** command restores the default radio coverage distance parameter for all specified radios in an AP group.

(AP radio view) The **coverage distance** command configures the radio coverage distance parameter for an AP radio.

(AP radio view) The **undo coverage distance** command cancels the configuration of the radio coverage distance parameter on an AP radio. The radio coverage distance parameter on the AP radio is then determined by that configured in the AP group radio view.

By default, the radio coverage distance parameter is 3 (unit: 100 m) for all radios.

Format

coverage distance *distance*

undo coverage distance

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
distance	Specifies the radio coverage distance parameter. Each distance parameter corresponds to a group of slottime, acktimeout, and ctstimeout values. You can configure the distance parameter based on the AP distance. APs adjust the values of slottime, acktimeout, and ctstimeout values based on the distance parameter.	The value is an integer that ranges from 1 to 400, in 100 meters.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In actual application scenarios, two APs may be connected over dozens of meters to dozens of kilometers. Due to different AP distances, the time to wait for ACK packets from the peer AP varies. A proper acktimeout value can improve data transmission efficiency between APs.

You can configure the radio coverage distance parameter based on distances between APs and the APs automatically adjust the values of slottime, acktimeout, and ctstimeout based on the configured distance parameter to improve data transmission efficiency.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the radio coverage distance parameter to 2 for radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] coverage distance 2
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.63 cpu-usage threshold

Function

The **cpu-usage threshold** command configures a CPU usage alarm threshold for APs.

The **undo cpu-usage threshold** command restores the default CPU usage alarm threshold.

By default, the CPU usage alarm threshold of APs is 90.

Format

cpu-usage threshold *threshold*

undo cpu-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies the CPU usage alarm threshold of APs.	The value is an integer that ranges from 50 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **cpu-usage threshold** command to configure the CPU usage alarm threshold in the AP system profile view. The configuration is delivered to all APs using the profile.

- When the CPU usage of an AP exceeds the alarm threshold, the AP sends an alarm message to the AC, and the AC displays the alarm information.
- When the CPU usage of an AP falls below the alarm threshold, the AP sends a clear alarm message to the AC, and the AC displays the clear alarm information.

Example

Set the CPU usage alarm threshold to 60.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] cpu-usage threshold 60
```

 Copyright © Huawei Technologies Co., Ltd.

14.1.64 crc-alarm enable

Function

The **crc-alarm enable** command enables the alarm function for CRC errors on the AP wired interface and specifies the alarm threshold and clear alarm threshold.

The **undo crc-alarm enable** command disables the alarm function for CRC errors on the AP wired interface and restores the alarm threshold and clear alarm threshold to the default values.

By default, the alarm function for CRC errors is disabled on the AP wired interface. The alarm threshold for CRC errors is 50 and the clear alarm threshold is 20.

Format

crc-alarm enable [**high-threshold** *high-threshold-value* | **low-threshold** *low-threshold-value*]*

undo crc-alarm enable

Parameters

Parameter	Description	Value
high-threshold *high-threshold-value*	Specifies the alarm threshold for CRC errors on the AP wired interface.	The value is an integer ranging from 1 to 100. The unit is 1/10000. The value of *high-threshold-value* must be larger than the value of *low-threshold-value*.
low-threshold *low-threshold-value*	Specifies the clear alarm threshold for CRC errors on the AP wired interface.	The value is an integer ranging from 1 to 100.

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

When the AP detects that the number of CRC errors exceeds the configured upper alarm threshold in a specified period, it sends an alarm message to the AC. To

 Copyright © Huawei Technologies Co., Ltd.

prevent the AP from frequently sending alarm messages or alarm clearance messages to the AC, you need to configure the lower threshold for clearing the alarm. The AP sends an alarm clearance message to the AC only when the AP detects that the number of CRC errors is lower than the configured lower threshold.

Example

Enable the alarm function for CRC errors on the AP's wired interface.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1] crc-alarm enable
```

Related Topics

14.1.104 display port-link-profile

14.1.65 deny-broadcast-probe enable

Function

The **deny-broadcast-probe enable** command configures an AP not to respond to broadcast Probe Request frames.

The **undo deny-broadcast-probe enable** command configures an AP to respond to broadcast Probe Request frames.

By default, an AP responds to broadcast Probe Request frames.

Format

deny-broadcast-probe enable

undo deny-broadcast-probe enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Probe Response frames occupy a large number of wireless resources. To reduce wireless resource occupation of the frames and improve channel usage efficiency, you can run the **deny-broadcast-**

probe enable command to configure an AP not to respond to broadcast Probe Request frames.

Precautions

Configuring an AP not to respond to broadcast Probe Request frames may reduce channel scan efficiency of some STAs.

Example

Configure an AP not to respond to broadcast Probe Request frames.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] deny-broadcast-probe enable
```

Related Topics

14.1.118 display ssid-profile

14.1.66 description (AP wired port profile view)

Function

The **description** command configures the description of an AP wired port.

The **undo description** command restores the default description of an AP wired port.

By default, the port has no description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the AP interface description.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

To manage AP interfaces conveniently, run this command to set AP interface descriptions. The description of an AP interface helps you identify the AP interface and know its functions.

Example

Change the description of the AP's wired interface to **poe-power**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1] description poe-power
```

Related Topics

14.1.128 display wired-port-profile

14.1.67 dhcp trust port

Function

The **dhcp trust port** command configures a DHCP trusted interface on an AP.

The **undo dhcp trust port** command cancels the configuration.

By default, the DHCP trusted interface is disabled in the VAP profile view and enabled on the AP's uplink interface in the AP wired port profile view.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

Views

VAP profile view, AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a bogus DHCP server is deployed at the user side, STAs may obtain incorrect IP addresses and network configuration parameters and cannot communicate properly. After the **dhcp trust port** command is executed in the VAP profile view, an AP discards the DHCP OFFER, ACK, and NAK packets sent by the bogus DHCP

server and reports to the AC about the IP address of the unauthorized DHCP server.

Before WLAN services are delivered to an AP, run the **dhcp trust port** command in the AP wired port profile view. After the command is run, the AP receives the DHCP OFFER, ACK, and NAK packets sent by the authorized DHCP server and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

The **undo dhcp trust port** command configured in the AP wired port profile view takes effect only in direct forwarding mode, but not the tunnel forwarding mode.

Precautions

When executed in the AP wired port, this command takes effect only on uplink interfaces of an RRU.

Example

Create the VAP profile **vap1** and configure a DHCP trusted interface on the AP in the VAP profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] dhcp trust port
```

Related Topics

14.1.127 display vap-profile

14.1.98 display ap-system-profile

14.1.68 dai enable (AP wired port profile view)

Function

The **dai enable** command enables dynamic ARP inspection (DAI) on an AP's wired interface.

The **undo dai enable** command disables DAI on an AP's wired interface.

By default, DAI is disabled on an AP's wired interface.

Format

dai enable

undo dai enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable DAI using this command to prevent Man in The Middle (MITM) attacks and theft on authorized user information. When a device receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN ID of the ARP packet with DHCP snooping binding entries. If the ARP packet matches a binding entry, the device allows the packet to pass through. If the ARP packet does not match any binding entry, the device discards the packet.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on ARP packets transmitted on an AP's wired interface.

The AP wired interfaces added to an Eth-trunk interface do not support this function.

Example

Enable DAI on an AP's wired interface.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] dai enable
```

Related Topics

14.1.128 display wired-port-profile

14.1.69 display ac global configuration

Function

The **display ac global configuration** command displays AC global configuration.

Format

display ac global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display AC global configuration.

```
<Huawei> display ac global configuration
-------------------------------------------------------------------------------
AC sysnetid                    : AC
-------------------------------------------------------------------------------
```

Table 14-2 Description of the **display ac global configuration** command output

Item	Description
AC sysnetid	NE name of an AC. To configure the NE name for an AC, run the **14.1.1 ac sysnetid** command.

Related Topics

14.1.1 ac sysnetid

14.1.70 display ap

Function

The **display ap** command displays AP information.

Format

display ap { **all** | **ap-group** *ap-group* }

display ap [**ap-group** *ap-group*] **by-ssid** *ssid*

display ap by-state *state* [**ap-group** *ap-group*]

Parameters

Parameter	Description	Value
all	Displays information about all APs.	-

Parameter	Description	Value
ap-group *ap-group*	Specifies the group to which an AP belongs.	The AP group must exist.
by-ssid *ssid*	Specifies an SSID.	The value must be an existing SSID.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
by-state *state*	Specifies the status of the AP.	Enumerated type. • **commit-failed**: Displays information about APs in configuration commitment failed state. • **committing**: Displays information about APs in configuration committing state. • **config**: Displays information about APs in configuration initialization state. • **config-failed**: Displays information about APs in initialization failed state. • **download**: Displays information about APs in system software downloading state. • **fault**: Displays information about APs in faulty state. • **idle**: Displays information about APs in idle state. • **name-conflicted**: Displays information about APs having duplicate names.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• **normal**: Displays information about APs in normal state. • **standby**: Displays information about APs in standby AC state. • **ver-mismatch**: Displays information about APs with versions that do not match the AC version.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view information about APs, run this command.

Example

Display information about all APs.

```
<Huawei> display ap all
Total AP information:
nor  : normal          [2]
-------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP             Type           State STA Uptime
-------------------------------------------------------------------------------------
0    dcd2-fcf6-76a0 area_1 ap-group1 192.168.120.254 AP6010DN-AGN    nor   0   4H:49M:11S
1    60de-4474-9640 area_2 ap-group1 192.168.120.253 AP5010DN-AGN    nor   0   6H:3M:40S
-------------------------------------------------------------------------------------
Total: 2
```

Display information about APs bound to SSID **hw-wlan**.

```
<Huawei> display ap by-ssid hw-wlan
Total AP information:
nor  : normal          [2]
-------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP             Type           State STA Uptime
-------------------------------------------------------------------------------------
0    dcd2-fcf6-76a0 area_1 ap-group1 192.168.120.254 AP6010DN-AGN    nor   0   4H:49M:11S
1    60de-4474-9640 area_2 ap-group1 192.168.120.253 AP5010DN-AGN    nor   0   6H:3M:40S
-------------------------------------------------------------------------------------
Total: 2
```

 Copyright © Huawei Technologies Co., Ltd.

Display information about APs in normal state.

```
<Huawei> display ap by-state normal
AP information(State-normal):
-----------------------------------------------------------------------------------------------
ID   MAC            Name   Group     IP             Type           State          STA Uptime
-----------------------------------------------------------------------------------------------
0    dcd2-fcf6-76a0 area_1 ap-group1 192.168.120.254 AP6010DN-AGN    nor            0   4H:50M:55S
1    60de-4474-9640 area_2 ap-group1 192.168.120.253 AP5010DN-AGN    nor            0   6H:5M:24S
-----------------------------------------------------------------------------------------------
Total: 2
```

Table 14-3 Description of the **display ap** command output

Item	Description
ID	AP ID.
MAC	MAC address of an AP.
Name	AP name.
Group	AP group.
IP	AP IP address.
Type	AP type.
State	State of an AP. ● commit-failed: WLAN service configuration commitment fails. ● committing: WLAN service configuration is being committed. ● config: The AP is initializing configuration. ● config-failed: The AP fails to initialize the configuration. ● download: The AP is downloading the upgrade software. ● fault: The AP is faulty. ● idle: The AP is in idle state. ● name-conflicted: APs' names conflict. ● nor: The AP is in normal state. ● standby: The AP is on the standby AC. ● ver-mismatch: Versions of the AP and AC do not match.
STA	Number of STAs connected to an AP.
Uptime	Online duration of an AP.

Related Topics

14.1.33 ap-id
14.1.34 ap-mac

14.1.71 display ap around-ssid-list

Function

The **display ap around-ssid-list** command displays SSIDs of neighbors of a specified AP.

Format

display ap around-ssid-list { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view SSIDs of neighbors of a specified AP. Neighbors of an AP include authorized and unauthorized neighbors. Authorized neighbors are other APs managed by the same AC. APs that are managed by other ACs are unauthorized neighbors.

Example

Display SSIDs of neighbors of AP **huawei**.

```
<Huawei> display ap around-ssid-list ap-name huawei
In control AP(2.4G):
--------------------------------------------------
SSID
--------------------------------------------------
test1
--------------------------------------------------
Total: 1
Uncontrol AP(2.4G):
--------------------------------------------------
```

```
SSID
-----------------------------------------------------
test2
-----------------------------------------------------
Total: 1
In control AP(5G):
-----------------------------------------------------
SSID
-----------------------------------------------------
test3
-----------------------------------------------------
Total: 1
Uncontrol AP(5G):
-----------------------------------------------------
SSID
-----------------------------------------------------
test4
-----------------------------------------------------
Total: 1
```

Table 14-4 Description of the **display ap around-ssid-list** command output

Item	Description
In control AP	SSIDs of authorized neighbors.
Uncontrol AP	SSIDs of unauthorized neighbors.

14.1.72 display ap asyn-message err-info

Function

The **display ap asyn-message err-info** command displays records about AP restart failures.

Format

display ap asyn-message err-info { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays records about restart failures of all APs.	-
ap-name *ap-name*	Displays records about restart failures of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays records about restart failures of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you use commands on the AC to restart an AP manually, during an upgrade, or to restore its factory settings, the restart message delivered by the AC may get lost due to transmission failures. Therefore, APs are not restarted. If an AP does not receive the restart message, the AP is still connected to the AC, which makes the AC incorrectly consider that the AP is restarted successfully. This command displays records about AP restart failures, helping you check whether the AP is restarted successfully. If the AP restart fails, restart the AP.

Example

Display records about restart failures of all APs.

```
<Huawei> display ap asyn-message err-info all
-------------------------------------------------------------------------------
AP Name MAC            Time                  Reason
-------------------------------------------------------------------------------
hw1     dcd2-fcf4-6600 2015-1-19 14:41:59    update
hw2     dcd2-fcf4-8800 2015-1-19 14:45:56    clear config
-------------------------------------------------------------------------------
Total: 2
```

Table 14-5 Description of the **display ap asyn-message err-info** command output

Item	Description
AP Name	Name of an AP.
MAC	MAC address of an AP.
Time	Time when AP restart fails.
Reason	Type of AP restart failures. ● update: The AP fails to be restarted during an upgrade. ● clear config: The AP fails to be restarted when restoring factory settings. ● other: The AP fails to be restarted manually.

14.1.73 display ap blacklist

Function

The **display ap blacklist** command displays the AP blacklist.

Format

display ap blacklist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays APs in the blacklist. These APs are not allowed to go online on the AC. If an AP is online on the AC but is in the blacklist, the AP is forced to log out.

Example

Display the AP blacklist.

```
<Huawei> display ap blacklist
--------------------------------------------------------------------------------
ID     MAC
--------------------------------------------------------------------------------
0      0001-0002-0001
--------------------------------------------------------------------------------
Total: 1
```

Table 14-6 Description of the **display ap blacklist** command output

Item	Description
ID	ID of the MAC address in the AP blacklist. The ID is generated automatically when the MAC address is specified.
MAC	MAC addresses of the APs that are not allowed to connect to the AC. To add MAC addresses to the AP blacklist, run the **14.1.12 ap blacklist** command.

Related Topics

14.1.12 ap blacklist

14.1.74 display ap config-info

Function

The **display ap config-info** command displays AP configuration.

Format

display ap config-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays configuration of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays configuration of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap config-info** command to view AP configuration information, including the basic configuration, radio configuration, VAP configuration, and profile configuration.

Example

Display configuration of AP **huawei**.

```
<Huawei> display ap config-info ap-name huawei
-------------------------------------------------------------------------------
AP MAC                        : dcd2-fcf6-76a0
AP SN                        : 210235419610D2000097
AP type                      : AP6010DN-AGN
AP name                       : huawei
AP group                     : default
Country code                  : CN
-------------------------------------------------------------------------------
Radio 0 configurations:
 Radio enable                 : yes
 WDS  mode                     : -
 Radio band                   : 2.4G
 Radio type                   : bgn
 Config channel/bandwidth       : -/20M
 Actual channel/bandwidth       : 1/20M
 Config EIRP                  : 127
```

```
 Actual EIRP                    : 27
 Maximum EIRP                   : 27

 VAP configurations:
  WLAN ID 1:
   SSID                         : HUAWEI-WLAN
   Authen mode                  : Open
   Encrypt mode                 : -
-------------------------------------------------------------------------------
Radio 1 configurations:
 Radio enable                   : yes
 WDS  mode                      : -
 Radio band                     : 5G
 Radio type                     : an
 Config channel/bandwidth       : -/20M
 Actual channel/bandwidth       : 157/20M
 Config EIRP                    : 127
 Actual EIRP                    : 28
 Maximum EIRP                   : 28

 VAP configurations:
  WLAN ID 1:
   SSID                         : HUAWEI-WLAN
   Authen mode                  : Open
   Encrypt mode                 : -
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
AP system profile          : default
Regulatory domain profile  : default
WIDS profile               : default
AP wired port profile
 Interface FE0             : default
 Interface FE1             : default
 Interface FE2             : default
 Interface FE3             : default
 Interface GE0             : default
 Interface GE1             : default
 Interface GE2             : default
 Interface GE3             : default
 Interface GE4             : default
 Interface GE5             : default
 Interface GE6             : default
 Interface GE7             : default
 Interface GE8             : default
 Interface GE9             : default
 Interface GE10            : default
 Interface GE11            : default
 Interface GE12            : default
 Interface GE13            : default
 Interface GE14            : default
 Interface GE15            : default
 Interface GE16            : default
 Interface GE17            : default
 Interface GE18            : default
 Interface GE19            : default
 Interface GE20            : default
 Interface GE21            : default
 Interface GE22            : default
 Interface GE23            : default
 Interface GE24            : default
 Interface GE25            : default
 Interface GE26            : default
 Interface GE27            : default
 Interface Eth-trunk0      : default
Radio 0
 Radio 2.4G profile        : default
 Radio 5G profile          :
 VAP profile
  WLAN  1                  : default
```

```
 WDS profile              :
 WDS whitelist profile     :
 Radio switch             : enable
 Channel                  : -
 Channel bandwidth         : 20mhz
 EIRP(dBm)                : 127
 Antenna gain(dB)          : -
 Coverage distance(100 m)  : 3
 Radio frequency           : 2.4G
 WIDS attack detect        : -
Radio 1
 Radio 2.4G profile       :
 Radio 5G profile          : default
 VAP profile
  WLAN  1                 : default
 WDS profile              :
 WDS whitelist profile     :
 Radio switch             : enable
 Channel                  : -
 Channel bandwidth         : 20mhz
 EIRP(dBm)                : 127
 Antenna gain(dB)          : -
 Coverage distance(100 m)  : 3
 Radio frequency           : 5G
 WIDS attack detect        : -
-------------------------------------------------------------------------------
```

Table 14-7 Description of the **display ap config-info** command output

Item	Description
AP MAC	MAC address of an AP.
AP SN	SN of an AP.
AP type	AP type.
AP name	AP name. To configure the parameter, run the **14.1.36 ap-name (AP view)** or **14.1.39 ap-rename** command.
AP group	AP group. To configure the parameter, run the **14.1.32 ap-group (AP view)** or **14.1.38 ap-regroup** command.
Country code	Country code. To configure the parameter, run the **14.1.61 country-code** command.
Radio 0 configurations/Radio 1 configurations	Radio configuration.
Radio enable	Radio status. To configure the parameter, run the **14.1.183 radio disable** command.

Item	Description
WDS mode	WDS mode. To configure the parameter, run the **14.5.18 wds-mode** command.
Radio band	Frequency band of a radio. To configure the parameter, run the **14.1.143 frequency** command.
Radio type	Protocol type of a radio.
Config channel/bandwidth	Configured AP channel and bandwidth. To configure the parameter, run the **14.1.57 channel** command.
Actual channel/bandwidth	Actual AP channel and bandwidth.
Config EIRP	Transmit power of a radio configured in the radio profile. To configure the parameter, run the **14.1.140 eirp** command.
Actual EIRP	Actual transmit power of a radio.
Maximum EIRP	Maximum transmit power of a radio.
VAP configurations	VAP configuration. VAP configuration is displayed only after a VAP profile is referenced by the AP.
WLAN ID 1	WLAN ID of a VAP. To configure the parameter, run the **14.1.234 vap-profile** command.
SSID	SSID name. To configure the parameter, run the **14.1.214 ssid** command.
Authen mode	Authentication mode.
Encrypt mode	Encryption mode.
AP system profile	Name of the referenced AP system profile. To configure the parameter, run the **14.1.42 ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Name of the referenced regulatory domain profile. To configure the parameter, run the **14.1.193 regulatory-domain-profile** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WIDS profile	Name of the referenced WIDS profile. To configure the parameter, run the **14.4.57 wids-profile (AP group view and AP view)** command.
AP wired port profile	Name of the referenced AP wired port profile. To configure the parameter, run the **14.1.241 wired-port-profile (AP group view and view)** command.
Interface *interface-name*	Interface name and number.
Radio 0/Radio 1	Radio frequency.
Radio 2.4G profile	Name of the referenced 2G radio profile. To configure the parameter, run the **14.1.185 radio-2g-profile** command.
Radio 5G profile	Name of the referenced 5G radio profile. To configure the parameter, run the **14.1.187 radio-5g-profile** command.
VAP profile	Name of the referenced VAP profile. To configure the parameter, run the **14.1.234 vap-profile** command.
WLAN 1	VAP profile name. To configure the parameter, run the **14.1.234 vap-profile** command.
WDS profile	Name of the referenced WDS profile. To configure the parameter, run the **14.5.21 wds-profile radio** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure the parameter, run the **14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)** command.
Radio switch	Radio status. To configure the parameter, run the **14.1.183 radio disable** command.
Channel	Working channel of a radio. To configure the parameter, run the **14.1.57 channel** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Channel bandwidth	Working bandwidth of a radio. To configure the parameter, run the **14.1.57 channel** command.
EIRP(dBm)	Transmit power of a radio, in dBm. To configure the parameter, run the **14.1.140 eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dBm. To configure the parameter, run the **14.1.7 antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter, in 100 m. To configure the parameter, run the **14.1.62 coverage distance** command.
Radio frequency	Working frequency band of a radio. To configure the parameter, run the **14.1.143 frequency** command.
WIDS attack detect	Whether attack detection is enabled. To configure the parameter, run the **14.4.55 wids attack detect enable** command.

14.1.75 display ap configurable channel

Function

The **display ap configurable channel** command displays the configurable channels supported by a specified AP.

Format

display ap configurable channel { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays configurable channels supported by the AP with the specified name.	The AP name must exist.
ap-id *ap-id*	Displays configurable channels supported by the AP with the specified ID.	The AP ID must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Different countries or regions use different wireless channels and powers. Setting country and area codes can specify channels that can be used on WLANs of different countries. The **display ap configurable channel** command displays the configurable channels supported by a specified AP.

Example

Display configurable channels supported by AP **huawei**.

```
<Huawei> display ap configurable channel ap-name huawei
2.4G 20M : 1,2,3,4,5,6,7,8,9,10,11,12,13.
2.4G 40M+: 1,2,3,4,5,6,7.
2.4G 40M-: 5,6,7,8,9,10,11.
5G   20M : 36,40,44,48,52,56,60,64,149,153,157,161,165.
5G   40M+: 36,44,52,60,149,157.
5G   40M-: 40,48,56,64,153,161.
5G   80M : 36,40,44,48,52,56,60,64,149,153,157,161.
```

Table 14-8 Description of the **display ap configurable channel** command output

Item	Description
2.4G 20M	Configurable 20 MHz channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 2.4 GHz frequency band.
2.4G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 2.4 GHz frequency band.
5G 20M	Configurable 20 MHz channels supported by the AP on the 5 GHz frequency band.
5G 40M+	Configurable 40 MHz Plus channels supported by the AP on the 5 GHz frequency band.
5G 40M-	Configurable 40 MHz Minus channels supported by the AP on the 5 GHz frequency band.
5G 80M	Configurable 80 MHz channels supported by the AP on the 5 GHz frequency band.

 Copyright © Huawei Technologies Co., Ltd.

14.1.76 display ap elabel

Function

The **display ap-elabel** command displays electronic label information about a specified AP.

Format

display ap elabel { **ap-name** *ap-name* | **ap-id** *ap-id* | all }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays electronic label information about the AP with the specified name.	The AP name must exist.
ap-id *ap-id*	Displays electronic label information about the AP with the specified ID.	The AP ID must exist.
all	Displays electronic label information of all APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view electronic label information about an AP. An electronic label is also called permanent configuration data or information and is written in the storage device during AP testing or commissioning. An electronic label includes the AP name, serial number, manufacture date and manufacturer information.

Example

Display electronic label information about AP **huawei**.

```
<Huawei> display ap elabel ap-name huawei
/$[ArchivesInfo Version]
/$ArchivesInfoVersion=3.0


[Board Properties]
```

```
BoardType=AP6310SN-GN-CN
BarCode=210235449210CB000011
Item=02354492
Description=AP6310SN-GN Bundle(11n,Distributed AP Indoor,Single Frequency,AC/DC
adapter(CN))
Manufactured=2012-11-27
VendorName=Huawei
IssueNumber=00
CLEICode=
BOM=
```

Table 14-9 Description of the **display ap elabel** command output

Item	Description
ArchivesInfo Version	Electronic label version.
BoardType	AP type.
BarCode	Bar code of an AP.
Item	BOM code of an AP.
Description	English description of an AP.
Manufactured	Production date of an AP.
VendorName	Vendor name.
IssueNumber	Issue number of an AP.
CLEICode	CLEI code of an AP.
BOM	Sales BOM code of an AP.

Display electronic label information of all APs.

```
<Huawei> display ap elabel all
Info: This operation may take a few seconds. Please wait for a moment.done.
Total AP elabel information:
--------------------------------------------------------------------------------
ID   MAC            Name     Type         SN                   Item
--------------------------------------------------------------------------------
1    dcd2-fc04-b500 L1_001   AP7110DN-AGN 210235555310CC000094 -
2    dcd2-fc9d-0bb0 1        AP7110SN-GN  210235568010D1000032 -
--------------------------------------------------------------------------------
Total: 2
```

Table 14-10 display ap elabel all command output

Item	Description
ID	AP ID.
MAC	MAC address of an AP.
Name	AP name.
Type	AP type.

SN	SN of an AP.
Item	BOM code of an AP.

14.1.77 display ap global configuration

Function

The **display ap global configuration** command displays AP global configuration.

Format

display ap global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display AP global configuration.

```
<Huawei> display ap global configuration
-------------------------------------------------------------------------------
AP auth-mode                      : MAC-auth
AP LLDP swtich                    : disable
AP username/password              : -/******
AP data collection                : disable
AP data collection interval(minute): 5
-------------------------------------------------------------------------------
```

Table 14-11 Description of the **display ap global configuration** command output

Item	Description
AP auth-mode	AP authentication mode. To configure the parameter, run the **14.1.11 ap auth-mode** command.

Item	Description
AP LLDP swtich	Whether LLDP is enabled on an AP. To configure the parameter, run the **14.1.15 ap lldp enable** command.
AP username/password	User name and password for AP login. To configure the parameter, run the **14.1.28 ap username** command.
AP data collection	Whether data buffering is enabled on an AP. To configure the parameter, run the **14.1.13 ap data-collection enable** command.
AP data collection interval(minute)	AP data buffering duration. To configure the parameter, run the **14.1.14 ap data-collection interval** command.

Related Topics

14.1.11 ap auth-mode
14.1.15 ap lldp enable
14.1.28 ap username
14.1.13 ap data-collection enable
14.1.14 ap data-collection interval

14.1.78 display ap lldp neighbor

Function

The **display ap lldp neighbor** command displays LLDP neighbor information on a specified AP.

Format

display ap lldp neighbor { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**interface** *interface-type interface-number*] | **brief** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays LLDP neighbor information of the AP with a specified name.	The AP name must exist.

Parameter	Description	Value
ap-id *ap-id*	Displays LLDP neighbor information of the AP with a specified ID.	The AP ID must exist.
interface *interface-type interface-number*	Displays LLDP neighbor information on a specified AP interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
brief	Displays brief LLDP neighbor information of APs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view LLDP neighbor information on a specified AP, including the number of LLDP neighbors, device ID, interface ID, system name, system description, and management address of each neighbor. The LLDP neighbor information is reported by an AP to the connected AC.

If no parameter is specified, LLDP neighbor information about all AP interfaces is displayed.

Example

Display LLDP neighbor information on all APs.

```
<Huawei> display ap lldp neighbor brief
-------------------------------------------------------------------------------
Hostname  Neighbor device  Management address  Local intf  Neighbor intf        TTL
-------------------------------------------------------------------------------
huawei    Quidway          10.10.10.3          GE0         GigabitEthernet0/0/16  119
-------------------------------------------------------------------------------
Total: 1
```

Table 14-12 Description of the **display ap lldp neighbor** command output

Item	Description
Hostname	AP name.
Neighbor device	System name of an AP neighbor.
Management address	Management address of an AP neighbor.
Local intf	Local interface of the AP.
Neighbor intf	Interface of an AP neighbor.
TTL	Time to live (TTL) of the local AP information stored on a neighboring device

Display LLDP neighbor information about GE0/0/0 of AP **huawei**.

```
<Huawei> display ap lldp neighbor ap-name huawei interface gigabitethernet 0
-------------------------------------------------------------------------------
AP 1 Port 0 has 1 neighbor(s):

Neighbor index               : 1
Host Name                    : huawei
Chassis ID type              : macAddress
Chassis ID                   : 5489-9876-b7d7
Port ID type                 : interfaceName
Port ID                      : GigabitEthernet0/0/2
Time to live                 : 120s
Port description             : GigabitEthernet0/0/2
System name                  : Quidway
System description           : AR1200
                    Huawei Versatile Routing Platform Software
                    VRP (R) software,Version 5.110 (AR1200 V200R009C00)
                    Copyright (C) 2007 Huawei Technologies Co., Ltd.
System capabilities supported: wlanAccessPoint telephone
System capabilities enabled  : wlanAccessPoint telephone
Management address type      : IPv4
Management address           : 10.10.10.5
-------------------------------------------------------------------------------
```

Table 14-13 Description of the **display ap lldp neighbor ap-name** *ap-name* **interface** *interface-type interface-number* command output

Item	Description
Neighbor index	Index of a neighbor.
Host Name	AP name

Item	Description
Chassis ID type	ID subtype of a neighbor device. ● chassisComponent: chassis alias ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● interfaceName: name of the interface ● local: name of the local device
Chassis ID	ID of the neighbor device. ● A MAC address is displayed when the neighbor device ID subtype is macAddress. ● An IP address is displayed when the neighbor device ID subtype is networkAddress. ● A character string is displayed when the neighbor device ID subtype is neither macAddress nor networkAddress.
Port ID type	ID subtype of the neighbor interface. ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● interfaceName: name of the interface ● agentCircuitID: loopback interface ID of the DHCP relay ● local: name of the local device

 Copyright © Huawei Technologies Co., Ltd.

Port ID	ID of the neighbor interface. ● A MAC address is displayed when the neighbor interface ID subtype is macAddress. ● An IP address is displayed when the neighbor interface ID subtype is networkAddress. ● A character string is displayed when the neighbor interface ID subtype is neither macAddress nor networkAddress.
Time to live	Time to live (TTL) of the local device information stored on the neighbor device.
Port description	Description of the neighbor interface.
System name	System name.
System description	System description of the neighbor.
System capabilities supported	Capabilities of the neighbor device. ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station
System capabilities enabled	Capabilities enabled on the neighbor device. ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station

 Copyright © Huawei Technologies Co., Ltd.

Management address type	Management address type of the neighbor.
Management address	Management address of the neighbor.

Related Topics

14.1.15 ap lldp enable

14.1.79 display ap neighbor

Function

The **display ap neighbor** command displays information about neighbors of a radio, including authorized and unauthorized neighbors.

Format

display ap neighbor { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
radio *radio*	Specifies radio ID of an AP.	The value is an integer that ranges from 0 to 2.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

APs' neighbor information reflects the APs' locations and neighbor relationships, helping you plan the network.

Information about authorized neighbors includes forward channel attenuation and backward channel attenuation:

- Forward channel attenuation: indicates the attenuation from the local AP to the neighboring AP.
- Backward channel attenuation: indicates the attenuation from the neighboring AP to the local AP.

If a neighboring AP is an unauthorized one, the system displays only the power of signals received from the neighboring AP.

Example

Display neighbor information of AP **huawei**.

```
<Huawei> display ap neighbor ap-name huawei
Radio: Radio ID of AP
In control AP:
-----------------------------------------------------------
Radio  AP ID   AP name    Channel Front(db)  Back(db)
-----------------------------------------------------------
0      1       ap-14      1       44         45
1      2       ap-14      2       44         45
-----------------------------------------------------------
Total: 2

Uncontrol AP:
-----------------------------------------------------------
Radio  BSSID          Channel  RSSI(dBm)  SSID
-----------------------------------------------------------
0      0020-1306-0680 1        -79        b
1      cc53-b5ee-3d00 5        -60        test
-----------------------------------------------------------
Total: 2
```

Table 14-14 Description of the **display ap neighbor** command output

Item	Description
In control AP	Authorized neighboring AP.
Uncontrol AP	Unauthorized neighboring AP.
Radio	Neighboring AP detected on an AP radio.
AP ID	ID of a neighboring AP.
AP name	Name of a neighboring AP.
Channel	Channel that the authorized neighboring AP uses. **NOTE** The device displays only information about neighboring APs detected on the current channel.
Front(db)	Forward channel attenuation, in dB. The value is the attenuation from the local AP to the neighboring AP.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Back(db)	Backward channel attenuation, in dB. The value is the attenuation from the neighboring AP to the local AP.
BSSID	Basic service set identifier (BSSID) of an unauthorized neighbor.
Channel	Channel that the unauthorized neighboring AP uses.
RSSI(dBm)	Power of signals received from the neighboring AP, in dBm.
SSID	Service set identifier (SSID) of an unauthorized neighbor.

14.1.80 display ap offline-record

Function

The **display ap offline-record** command displays AP offline records.

Format

display ap offline-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays offline records of all APs.	-
mac *mac-address*	Displays offline records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays AP offline records, helping the maintenance personnel manage and maintain the APs.

 Copyright © Huawei Technologies Co., Ltd.

After the number of AP offline records reaches the maximum that can be stored, new records overwrite existing ones.

Example

Display all AP offline records.

```
<Huawei> display ap offline-record all
--------------------------------------------------------------------------------
MAC              Last offline time      Reason
--------------------------------------------------------------------------------
0023-0024-0080   2015-01-31/16:21:50   Reboot by ap-reset command
60de-4476-e360   2015-01-31/14:02:35   Reboot by ap update reset command
1047-80b1-56a0   2015-01-31/13:52:35   Reboot by ap update reset command
--------------------------------------------------------------------------------
Total records: 3
```

Table 14-15 Description of the **display ap offline-record** command output

Item	Description
MAC	AP's MAC address.
Last offline time	Last offline time of an AP.
Reason	AP offline reason.

Related Topics

14.1.195 reset ap offline-record

14.1.81 display ap online-fail-record

Function

The **display ap online-fail-record** command displays AP online failure records.

Format

display ap online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays online failure records of all APs.	-
mac *mac-address*	Displays online failure records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If an AP fails to go online on the AC, you can run the command to check the failure reason, which helps locate the fault.

After the number of AP online failure records reaches the maximum that can be stored, new records overwrites existing ones.

Example

Display online failure records about the AP with the MAC address 1047-80b1-56a0.

```
<Huawei> display ap online-fail-record mac 1047-80b1-56a0
-------------------------------------------------------------------------------
MAC             Last fail time       Reason
-------------------------------------------------------------------------------
1047-80b1-56a0  2015-01-20/15:48:06  In blacklist
-------------------------------------------------------------------------------
Total records: 1
```

Table 14-16 Description of the **display ap online-fail-record** command output

Item	Description
MAC	MAC address of the AP that fails to go online.
Last fail time	Time of the AP online failure.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Reason for the AP online failure. • Lack of license. • Not in SN whitelist. • Not in MAC whitelist. • return "In blacklist". • MAC and SN mismatched. • Negotiation DTLS failed. • Negotiation CAPWAP tunnel failed. • Data batching. • AP IP address mismatch. • AP auto update fail. • Create link failed. • Config timeout. • Config failed. • Version mismatch. • Unsupported AP type, AC version may need to be upgraded. • Name conflict. • AP reaches the upper limit. • Capwap psk mismatch. • CAPWAP message-integrity PSK mismatch. • Forcibly disconnected in certain situations. • AP type mismatch. • DTLS negotiation failed, because of negotiation timeout or inconsistent PSKs on two ends. • Other reasons.

Related Topics

14.1.196 reset ap online-fail-record

14.1.82 display ap optical-info

Function

The **display ap optical-info** command displays optical module information.

Format

display ap optical-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays optical module information of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays optical module information of the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view optical module information, including the optical module type, transmit optical power, and receive optical power.

Prerequisites

The AP has been online. You can run the **display ap** command to check the AP status.

The AP supports optical modules. You can run the **display ap-type** command to view the AP model.

NOTE

Currently, only the AP6610DN-AGN, AP6610DN-AGN-US, AP8030DN and AP8130DN support optical modules.

Example

Display optical module information of AP **huawei**.

```
<Huawei> display ap optical-info ap-name huawei
-------------------------------------------------------------------------------
Common information:
  Transceiver Type                :1000_BASE_LX
  Connector Type                  :LC
  Wavelength(nm)                  :1310
  Transfer Distance(m)            :10000(9um)
  Copper Link Length(m)           :0
  Digital Diagnostic Monitoring   :NO
```

```
  Vendor Name                      :FINISAR CORP.
  Vendor Part Number               :FTLF1318P2BTL-HW
  Vendor IEEE Company ID           :36965
  Vendor Revision Level            :A
  Nominal Bit Rate(MBits/sec)      :1200
-------------------------------------------------------------------------------
Manufacture information:
  Manu. Serial Number              :PMK2K62
  Manufacturing Date               :2012-05-09
  Vendor Name                      :FINISAR CORP.
-------------------------------------------------------------------------------
Diagnostic information:
  Temperature(degree C)            :49
  Temp High Threshold(degree C)    :90
  Temp Low Threshold(degree C)     :-45
  Voltage(0.1mV)                   :33161
  Volt High Threshold(0.1mV)       :37000
  Volt Low Threshold(0.1mV)        :29000
  Bias Current(mA)                 :19
  Bias High Threshold(mA)          :25430
  Bias Low Threshold(mA)           :1929
  RX Power(0.1uw)                  :0
  RX Power High Threshold(0.1uw)   :5012
  RX Power Low Threshold(0.1uw)    :126
  TX Power(0.1uw)                  :2886
  TX Power High Threshold(0.1uw)   :6310
  TX Power Low Threshold(0.1uw)    :708
-------------------------------------------------------------------------------
```

Table 14-17 Description of the **display ap optical-info** command output

Item	Description
Transceiver Type	Type of the optical module.
Connector Type	Interface type.
Wavelength(nm)	Optical wavelength, in nm.
Transfer Distance(m)	Transmission distance, in meters.
Copper Link Length(m)	Length of the copper cable, in meters.
Digital Diagnostic Monitoring	Whether diagnostic information about the optical module is monitored.
Vendor Name	Name of the vendor.
Vendor Part Number	Product code provided by the vendor.
Vendor IEEE Company ID	Version number provided by the vendor.
Vendor Revision Level	Product serial number provided by the vendor.
Nominal Bit Rate(MBits/sec)	Bit rate of the optical module, in Mbit/s.
Manu. Serial Number	Vendor sequence number of the optical module.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Manufacturing Date	Manufacturing date of the optical module.
Temperature(degree C)	Current temperature of the optical module, in °C.
Temp High Threshold(degree C)	The upper threshold for the temperature of the optical module, in °C.
Temp Low Threshold(degree C)	The lower threshold for the temperature of the optical module, in °C.
Voltage(0.1mV)	Current voltage of the optical module, in 0.1mV.
Volt High Threshold(0.1mV)	The upper threshold for the voltage of the optical module, in 0.1mV.
Volt Low Threshold(0.1mV)	The lower threshold for the voltage of the optical module, in 0.1mV.
Bias Current(mA)	Bias current of the optical module, in mA.
Bias High Threshold(mA)	Upper threshold for the bias current of the optical module, in mA.
Bias Low Threshold(mA)	Lower threshold for the bias current of the optical module, in mA.
RX Power(0.1uw)	Receive power of the optical module, in 0.1uw.
RX Power High Threshold(0.1uw)	Upper receive power threshold for the optical module, in 0.1uw.
RX Power Low Threshold(0.1uw)	Lower receive power threshold for the optical module, in 0.1uw.
TX Power(0.1uw)	Transmit power of the optical module, in 0.1uw.
TX Power High Threshold(0.1uw)	Upper transmit power threshold for the optical module, in 0.1uw.
TX Power Low Threshold(0.1uw)	Lower transmit power threshold for the optical module, in 0.1uw.

 Copyright © Huawei Technologies Co., Ltd.

14.1.83 display ap performance statistics

Function

The **display ap performance statistics** command displays performance statistics about an AP.

Format

display ap performance statistics { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays performance statistics about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays performance statistics about the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap performance statistics** command to view AP performance statistics to monitor AP performance.

Example

Display performance statistics about AP **huawei**.

```
<Huawei> display ap performance statistics ap-name huawei
-------------------------------------------------------------------------------
Memory usage(%)                  : 58
Memory average usage(%)          : 58
CPU usage(%)                     : 4
CPU average usage(%)             : 4
Available space size(KB)         : 1192
Temperature(degree C)            : 54
Online user number               : 0
Upstream traffic(wireless)(KB)   : 23 KB
Wireless port drop frames(RX)    : 0
Wireless port drop frames(TX)    : 0
Wireless port total bytes(RX)    : 0
Wireless port total bytes(TX)    : 0
Wireless port unicast frames(RX): 0
GigabitEthernet port 0
  port drop frames(RX)           : 0
```

```
  port drop frames(TX)          : 0
  port total Bytes(RX)          : 0
  port total Bytes(TX)          : 0
  port unknown frames(RX)       : 0
  port error frames(TX)         : 0
  port updown counts            : 0
  port up rate(Kbps)            : 0
  port down rate(Kbps)          : 0
GigabitEthernet port 1
  port drop frames(RX)          : 0
  port drop frames(TX)          : 0
  port total Bytes(RX)          : 61210
  port total Bytes(TX)          : 38218
  port unknown frames(RX)       : 0
  port error frames(TX)         : 0
  port updown counts            : 0
  port up rate(Kbps)            : 0
  port down rate(Kbps)          : 0
-------------------------------------------------------------------------------
```

Table 14-18 Description of the **display ap performance statistics** command output

Item	Description
Memory usage(%)	Memory usage (%).
Memory average usage(%)	Average memory usage (%).
CPU usage(%)	CPU usage (%).
CPU average usage(%)	Average CPU usage (%).
Available space size(KB)	Available space size (KB).
Temperature(degree C)	AP's internal temperature (°C). **NOTE** The temperature cannot be viewed on the AP2010DN, AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP3010DN-AGN, AP3010DN-V2, AP5010SN-GN and AP5010DN-AGN. The value is displayed as "-".
Online user number	Number of online users.
Upstream traffic(wireless)(KB)	Traffic volume on the wireless upstream interface in a specified period, in KB.
Wireless port drop frames(RX)	Number of discarded data frames that are received by the wireless interface.
Wireless port drop frames(TX)	Number of discarded data frames that are sent by the wireless interface.
Wireless port total bytes(RX)	Number of bytes received by the wireless interface.
Wireless port total bytes(TX)	Number of bytes sent by the wireless interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wireless port unicast frames(RX)	Number of unicast data frames received by the wireless interface.
GigabitEthernet port x	ID of the wired-side interface.
port drop frames(RX)	Number of discarded data frames that are received by the wired interface.
port drop frames(TX)	Number of discarded data frames that are sent by the wired interface.
port total Bytes(RX)	Number of bytes received by the wired interface.
port total Bytes(TX)	Number of bytes sent by the wired-side interface.
port unknown frames(RX)	Number of unknown protocol packets received by the wired interface.
port error frames(TX)	Number of error data frames sent by the wired interface.
port updown counts	Number of times the wired interface alternates between Up and Down.
port up rate(Kbps)	Upstream rate on the wired interface, in kbit/s.
port down rate(Kbps)	Downstream rate on the wired interface, in kbit/s.

14.1.84 display ap port

Function

The **display ap port** command displays the AP port status and traffic information.

Format

display ap port { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **ap-mac** *ap-mac* }

Parameters

Parameter	Description	Value
all	Displays port status and traffic information of all APs.	-

Parameter	Description	Value
ap-name *ap-name*	Displays port status and traffic information of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays port status and traffic information of the AP with a specified ID.	The AP ID must exist.
ap-mac *ap-mac*	Displays port status and traffic information of the AP with a specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap port** command to check port status and traffic information of online APs, which facilitates AP port maintenance and management.

Example

Display port status and traffic information of all APs.

```
<Huawei> display ap port all
Info: Waiting for AP response.
-----------------------------------------------------------------------------------------------------------------------------------
AP-ID Port      State Speed Duplex TX-Packets      Tx-ErrorPackets  TX-Rate(Kbps) RX-Packets      RX-
DropPackets   RX-Rate(Kbps)
-----------------------------------------------------------------------------------------------------------------------------------
0     GE0       up    1000  full   9178           0               0            12857           0               1
-----------------------------------------------------------------------------------------------------------------------------------
Total: 1
```

Table 14-19 Description of the **display ap performance statistics** command output

Parameter	Description
AP-ID	AP ID.
Port	AP port.

Parameter	Description
State	Status of the AP port. ● down: The AP port is Down. ● up: The AP port is Up. ● *down: indicates that the interface is shut down.
Speed	Speed of the AP port, in Mbit/s.
Duplex	Duplex mode of the AP port, which includes the half-duplex and full-duplex modes.
TX-Packets	Number of data frames sent by the AP port.
Tx-ErrorPackets	Number of error data frames sent by the AP port.
TX-Rate(Kbps)	Uplink rate of the AP port.
RX-Packets	Number of data frames received by the AP port.
RX-DropPackets	Number of discarded data frames that are received by the AP port.
RX-Rate(Kbps)	Downlink rate of the AP port.

14.1.85 display ap run-info

Function

The **display ap run-info** command displays running status of an AP.

Format

display ap run-info { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays running status of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays running status of the AP with a specified ID.	The AP ID must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays AP running status. You can run this command to monitor an AP in real time.

Prerequisites

The AP works properly.

Example

Display running status of AP **huawei**.

```
<Huawei> display ap run-info ap-name huawei
-------------------------------------------------------------------------------
AP type                      : AP7030DE
Country code                 : CN
Software version             : V200R007C00
Hardware version             : Ver.A
BIOS version                 : 271
BOM version                  : 001
Memory size(MB)              : 256
Flash size(MB)               : 64
Manufacture                  : Huawei Technologies Co., Ltd.
Software vendor              : Huawei Technologies Co., Ltd.
Online time(ddd:hh:mm:ss)    : 6H:56M:26S
Run time(ddd:hh:mm:ss)       : 6H:59M:51S
IP address                   : 192.168.109.252
IP mask                      : 255.255.255.0
Gateway                      : 192.168.109.1
DNS server                   : 0.0.0.0
GigabitEthernet port 0
  Port speed(Mbps)           : 1000
  Port speed mode            : auto
  Port duplex                : full
  Port duplex mode           : auto
  Port state                 : down
  STP down recovery time(ddd:hh:mm:ss)       : -
GigabitEthernet port 1
  Port speed(Mbps)           : 1000
  Port speed mode            : auto
  Port duplex                : full
  Port duplex mode           : auto
  Port state                 : up
  STP down recovery time(ddd:hh:mm:ss)       : -
IoT card status              : slot 1: -, slot 2: -, slot 3: -
-------------------------------------------------------------------------------
```

Table 14-20 Description of the **display ap run-info** command output

Item	Description
AP type	AP type.

Item	Description
Country code	Country code.
Software version	Software version of an AP.
Hardware version	Hardware version of an AP.
BIOS version	BIOS version of an AP.
BOM version	BOM version of an AP.
Memory size(MB)	Memory size of an AP, in MB.
Flash size(MB)	Flash memory size of an AP, in MB.
Manufacture	Manufacturer of an AP.
Software vendor	AP software manufacturer.
Online time(ddd:hh:mm:ss)	AP online duration.
Run time(ddd:hh:mm:ss)	Running duration of an AP.
IP address	IP address of an AP.
IP mask	Mask of an AP.
Gateway	Gateway IP address of an AP.
DNS server	IP address of the DNS server.
GigabitEthernet port *number*	ID of the AP's Ethernet interface.
Port speed(Mbps)	Rate on the upstream Ethernet interface, in Mbit/s.
Port speed mode	Rate mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.
Port duplex	Duplex type of the upstream Ethernet interface, including full duplex and half duplex.
Port duplex mode	Duplex mode of the upstream Ethernet interface, including automatic and non-automatic negotiation modes.
Port state	AP interface status. ● down: indicates that the interface is disabled. ● up: indicates that the interface is enabled. ● *down: indicates that the interface is shut down.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
STP down recovery time(ddd:hh:mm:ss)	Remaining recovery time of the STP.
IoT card status	IoT card status. ● -: indicates that the IoT card is not in position. ● present: indicates that the IoT card is in position.

14.1.86 display ap service-config acl

Function

The **display ap service-config acl** command displays the ACL configuration on a specified AP.

Format

display ap service-config acl { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the ACL configuration on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the ACL configuration on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can determine which ACLs have been delivered to the AP based on the command output, which helps locate and troubleshoot faults about user rights.

Example

Display ACL configuration on AP **huawei**.

```
<Huawei> display ap service-config acl ap-name huawei
-----------------------------------------------------------------------------------------
Index          ACL number
-----------------------------------------------------------------------------------------
1              3000
2              3002
3              3015
4              3022
5              3030
-----------------------------------------------------------------------------------------
Total: 5
```

Table 14-21 Description of the **display ap service-config acl** command output

Item	Description
Index	Index.
ACL number	ACL number configured on an AP.

14.1.87 display ap sta-signal strength

Function

The **display ap sta-signal strength** command displays the average signal strength of STAs connected to an AP.

Format

display ap sta-signal strength { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the average signal strength of STAs connected to the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the average signal strength of STAs connected to the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays the average signal strength of STAs connected to a specified AP radio.	The value is an integer that ranges from 0 to 2.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the average signal strength of STAs connected to an AP.

Example

Display the average signal strength of STAs connected to AP **huawei**.

```
<Huawei> display ap sta-signal strength ap-name huawei
Station signal strength(%): 0
```

Table 14-22 Description of the **display ap sta-signal strength** command output

Item	Description
Station signal strength(%)	Average signal strength of STAs.

14.1.88 display ap traffic statistics wireless

Function

The **display ap traffic statistics wireless** command displays statistics about packets with the specified SSID on the radio of an AP.

Format

display ap traffic statistics wireless { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* [**ssid** *ssid*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.
radio *radio-id*	Specifies the radio ID.	The value is an integer that ranges from 0 to 2.
ssid *ssid*	Specifies the SSID that STAs associate with.	The value must be an existing SSID.

 Copyright © Huawei Technologies Co., Ltd.

Views

ALL views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap traffic statistics wireless** command to view statistics about packets with the specified SSID on the radio of an AP.

Example

Display statistics about packets with the SSID **cmcc** on radio 0 of AP **huawei**.

```
<Huawei> display ap traffic statistics wireless ap-name huawei radio 0 ssid cmcc
-----------------------------------------------------------------
Wireless bytes(RX)           : 14583149
Wireless error frames(RX)    : 10
Wireless frames(RX)          : 97419
Wireless unicast frames(RX)  : 16
Wireless dropped frames(RX)  : 0
Wireless bytes(TX)           : 1725974
Wireless error frames(TX)    : 6
Wireless frames(TX)          : 9704
Wireless unicast frames(TX)  : 9680
Wireless dropped frames(TX)  : 6
Wireless retransmitted frames: 32674
Current accessed STA number  : 0
-----------------------------------------------------------------
```

Table 14-23 Description of the **display ap traffic statistics wireless ap-name** *ap-name* **radio** *radio-id* **ssid** *ssid* command output

Item	Description
Wireless bytes(RX)	Total number of received bytes.
Wireless error frames(RX)	Total number of received error frames.
Wireless frames(RX)	Total number of received frames.
Wireless unicast frames(RX)	Total number of received unicast frames.
Wireless dropped frames(RX)	Total number of received frames that are discarded.
Wireless bytes(TX)	Total number of transmitted bytes.
Wireless error frames(TX)	Total number of transmitted error frames.
Wireless frames(TX)	Total number of transmitted frames.
Wireless unicast frames(TX)	Total number of transmitted unicast frames.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wireless dropped frames(TX)	Total number of transmitted frames that are discarded.
Wireless retransmitted frames	Total number of retransmitted frames.
Current accessed STA number	Number of STAs that connect to the AP normally.

Display packet statistics on Radio 0 of the AP **huawei**.

```
<Huawei> display ap traffic statistics wireless ap-name huawei radio 0
-----------------------------------------------------------------------
Wireless frames(RX)                                  :506379
Wireless bytes(RX)                                   :76567129
Wireless error frames(RX)                            :113998
Wireless physical layer error frames(RX)             :0
Wireless MIC error frames(RX)                        :0
Wireless private key and decrypt fail frames(RX)     :0
Wireless signal strength(dBm)(RX)                    :-
Wireless power(dBm)(RX)                              :-
Wireless unicast frames(RX)                          :30
Wireless management frames(RX)                       :506379
Wireless control frames(RX)                          :0
Wireless data frames(RX)                             :0
Wireless maximal signal strength(dBm)(RX)            :0
Wireless minimal signal strength(dBm)(RX)            :0
Wireless average signal strength(dBm)(RX)            :0
Wireless frames(TX)                                  :4949
Wireless bytes(TX)                                   :855879
Wireless RTS successes(TX)                           :0
Wireless unicast frames(TX)                          :4587
Wireless broadcast frames(TX)                        :355
Wireless failure frames(TX)                          :3406
Wireless management frames(TX)                       :4725
Wireless control frames(TX)                          :0
Wireless data frames(TX)                             :0
Wireless noise(dBm)                                  :-100
Wireless port up rate(Kbps)                          :40
Wireless port down rate(Kbps)                        :1
Wireless port drop rate(%)                           :42
Wireless port PS-Poll Frames                         :0
Wireless port Association Request                    :0
Wireless port Association Response                   :0
Wireless port ReAssociation Request                  :0
Wireless port ReAssociation Response                 :0
Wireless port Disassociation Frames                  :0
Wireless port DisAuth Frames                         :0
Wireless retry frames                                :515
Wireless PER(%)                                      :0
Wireless PER of the last statistic period(%)         :7
Wireless channel utilization(%)                      :96
WMM AC_BE retry ratio(%)                             :0
WMM AC_BK retry ratio(%)                             :0
WMM AC_VI retry ratio(%)                             :0
WMM AC_VO retry ratio(%)                             :0
WMM AC_BE PER(%)                                     :0
WMM AC_BK PER(%)                                     :0
WMM AC_VI PER(%)                                     :0
WMM AC_VO PER(%)                                     :0
-----------------------------------------------------------------------
```

Table 14-24 Description of the **display ap traffic statistics wireless ap-name** *ap-name* **radio** *radio-id* command output

Item	Description
Wireless frames(RX)	Number of frames received by the radio.
Wireless bytes(RX)	Number of bytes received by the radio.
Wireless error frames(RX)	Number of error frames received by the radio.
Wireless physical layer error frames(RX)	Number of error frames received at the physical layer of the radio.
Wireless MIC error frames(RX)	Number of frames with message integrity code (MIC) received by the radio.
Wireless private key and decrypt fail frames(RX)	Number of frames with incorrect keys received by the radio.
Wireless signal strength(dBm)(RX)	Strength of signals received by the radio.
Wireless power(dBm)(RX)	Receive optical power of the radio.
Wireless unicast frames(RX)	Number of unicast frames received by the radio.
Wireless management frames(RX)	Number of management frames received on the radio.
Wireless control frames(RX)	Number of control frames received on the radio.
Wireless data frames(RX)	Number of data frames received on the radio.
Wireless maximal signal strength(dBm)(RX)	Maximum strength of signals received by the radio, in dBm.
Wireless minimal signal strength(dBm)(RX)	Minimum strength of signals received by the radio, in dBm.
Wireless average signal strength(dBm)(RX)	Average strength of signals received by the radio, in dBm.
Wireless frames(TX)	Number of transmitted frames received by the radio.
Wireless bytes(TX)	Number of transmitted bytes received by the radio.
Wireless RTS successes(TX)	Number of Request to Send (RTS) frames that are successfully sent by the radio.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wireless unicast frames(TX)	Number of transmitted unicast frames received by the radio.
Wireless broadcast frames(TX)	Number of broadcast frames sent by the radio.
Wireless failure frames(TX)	Number of frames that the radio fails to send.
Wireless management frames(TX)	Number of management frames sent from the radio.
Wireless control frames(TX)	Number of control frames sent from the radio.
Wireless data frames(TX)	Number of data frames sent from the radio.
Wireless noise(dBm)	Radio noise level (dBm).
Wireless port up rate(Kbps)	Upstream rate on the radio, kbit/s.
Wireless port down rate(Kbps)	Downstream rate on the radio, kbit/s.
Wireless port drop rate(%)	Packet loss ratio on the radio, in percentage (%).
Wireless port PS-Poll Frames	Number of data frames sent by the STA working in power saving mode.
Wireless port Association Request	Number of Association Request frames.
Wireless port Association Response	Number of Association Response frames.
Wireless port ReAssociation Request	Number of Reassociation Request frames.
Wireless port ReAssociation Response	Number of Reassociation Response frames.
Wireless port Disassociation Frames	Number of Disassociation frames.
Wireless port DisAuth Frames	Number of Deauthentication frames.
Wireless retry frames	Number of frames that are retransmitted by the radio.
Wireless PER(%)	Packet error rate of the radio.
Wireless PER of the last statistic period(%)	Packet error rate in the last statistical period.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wireless channel utilization(%)	Channel usage on the radio. **NOTE** When the working mode of an AP radio is the monitor mode, this parameter is displayed as **-**.
WMM AC_BE retry ratio(%)	Retransmission ratio of AC_BE packets in the WMM queue.
WMM AC_BK retry ratio(%)	Retransmission ratio of AC_BK packets in the WMM queue.
WMM AC_VI retry ratio(%)	Retransmission ratio of AC_VI packets in the WMM queue.
WMM AC_VO retry ratio(%)	Retransmission ratio of AC_VO packets in the WMM queue.
WMM AC_BE PER(%)	PER of AC_BE packets in the WMM queue.
WMM AC_BK PER(%)	PER of AC_BK packets in the WMM queue.
WMM AC_VI PER(%)	PER of AC_VI packets in the WMM queue.
WMM AC_VO PER(%)	PER of AC_VO packets in the WMM queue.

14.1.89 display ap unauthorized record

Function

The **display ap unauthorized record** command displays information about unauthenticated APs.

Format

display ap unauthorized record

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the MAC authentication or SN authentication mode is configured for an AP but the AP is neither added offline nor added to the whitelist, the AC does not allow this AP to access. You can run the **display ap unauthorized record** command to view information about unauthenticated APs.

Example

Display information about unauthenticated APs.

```
<Huawei> display ap unauthorized record
Unauthorized AP record:
Total number: 1
-------------------------------------------------------------------------------
AP type: AP7110SN-GN
AP SN: 210235568010D1000032
AP MAC address: dcd2-fc9d-0bb0
AP IP address: 192.168.109.252
Record time: 2015-01-22 17:23:17
-------------------------------------------------------------------------------
```

Table 14-25 Description of the **display ap unauthorized record** command output

Item	Description
Unauthorized AP record	Records about unauthenticated APs.
Total number	Total number of unauthenticated APs.
AP type	Type of an unauthenticated AP.
AP SN	Serial number of an unauthenticated AP.
AP MAC address	MAC address of an unauthenticated AP.
AP IP address	IP address of an unauthenticated AP.
Record time	Time when an unauthorized AP is recorded.

14.1.90 display ap uncontrol all

Function

The **display ap uncontrol all** command displays information about all APs that are not controlled by the local AC.

Format

display ap uncontrol all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about all uncontrolled APs. The command output includes channel of the controlled AP closest to the uncontrolled AP and the strength of signals that the controlled AP received from the uncontrolled AP.

Example

View information about all APs that are not controlled by the local AC.

```
<Huawei> display ap uncontrol all
-------------------------------------------------------
BSSID          NEAREST-AP      CHANNEL  RSSI(dBm)   SSID
-------------------------------------------------------
1047-80af-9970 ap-13           149      -68         test
-------------------------------------------------------
Total: 1
```

Table 14-26 Description of the **display ap uncontrol all** command output

Item	Description
BSSID	BSSID of an uncontrolled AP.
NEAREST-AP	Name of the controlled AP that is closest to the uncontrolled AP.
CHANNEL	Channel on which the uncontrolled AP is detected. If a rogue AP is detected on multiple channels, the channel with the strongest signal strength is displayed.
RSSI(dBm)	Strength of signals that the closest controlled AP receives from the uncontrolled AP, in dBm.
SSID	SSID of an uncontrolled AP.

 Copyright © Huawei Technologies Co., Ltd.

14.1.91 display ap update configuration

Function

The **display ap update configuration** command displays AP upgrade configuration.

Format

display ap update configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the display ap update configuration command to view AP upgrade configuration, including the upgrade mode, FTP server configuration, and SFTP server configuration.

Example

Display AP upgrade configuration.

```
<Huawei> display ap update configuration
--------------------------------------------------------------------------------
AP update mode          : ftp-mode
FTP configuration
 FTP IP                 : -
 FTP username           : anonymous
 FTP password           : ******
 FTP max number         : 50
SFTP configuration
 SFTP IP                : -
 SFTP username          : anonymous
 SFTP password          : ******
 SFTP max number        : 50
AP type/AP-group update filename
 AP6010DN-AGN           : FitAP6X10XN_V200R008C00.bin
--------------------------------------------------------------------------------
```

Table 14-27 Description of the **display ap update configuration** command output

Item	Description
AP update mode	AP upgrade mode. ● FTP-mode: indicates the FTP mode. ● SFTP-mode: indicates the SFTP mode. To configure the parameter, run the **14.1.21 ap update mode** command.
FTP configuration	FTP server configuration.
FTP IP	IP address of the FTP server. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
FTP username	User name for logging in to the FTP server. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
FTP password	Password for logging in to the FTP server. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
FTP max number	Maximum number of APs that can be upgraded simultaneously in FTP mode. To configure the parameter, run the **14.1.18 ap update ftp-server** command.
SFTP configuration	SFTP server configuration.
SFTP IP	IP address of the SFTP server. To configure the parameter, run the **14.1.25 ap update sftp-server** command.
SFTP username	User name for logging in to the SFTP server. To configure the parameter, run the **14.1.25 ap update sftp-server** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
SFTP password	Password for logging in to the SFTP server. To configure the parameter, run the **14.1.25 ap update sftp-server** command.
SFTP max number	Maximum number of APs that can be upgraded simultaneously in SFTP mode. To configure the parameter, run the **14.1.25 ap update sftp-server** command.
AP type/AP-group update filename	Name of the upgrade file for a specified AP type or group. To configure the parameter, run the **14.1.27 ap update update-filename** command.

14.1.92 display ap update status

Function

The **display ap update status** command displays AP upgrade progress.

Format

display ap update status { **all** | **downloading** | **failed** | **succeed** | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays upgrade progress of all APs.	-
downloading	Displays APs that are upgrading.	-
failed	Displays APs that failed to be upgraded.	-
succeed	Displays APs that have been successfully upgraded.	-
ap-name *ap-name*	Displays upgrade progress of the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays upgrade progress of the AP with a specified ID.	The AP ID must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to check upgrade progress of all APs or a specified AP, and check information about APs in specified upgrade status.

Example

Display upgrade progress of all APs.

```
<Huawei> display ap update status all
-------------------------------------------------------------------------------
ID   Name   Type                AP MAC          Update Status
-------------------------------------------------------------------------------
0    hw0    AP6010DN-AGN        60de-4476-e320  succeed
1    hw1    AP6010DN-AGN        60de-4476-e340  downloading(progress: 80%/0%)
2    hw2    AP6010DN-AGN        60de-4476-e360  downloading(progress: 100%/50%)
3    hw3    AP6010DN-AGN        60de-4476-e380  -
4    hw4    AP6010DN-AGN        60de-4476-e3a0  -
5    hw5    AP6010DN-AGN        60de-4476-e3c0  -
-------------------------------------------------------------------------------
Total: 6
```

Table 14-28 Description of the **display ap update status all** command

Item	Description
ID	AP ID.
Name	AP name.
Type	AP type.
AP MAC	MAC address of the AP.

Update Status	AP upgrade progress. • downloading (progress: 80%/0%): The AP is downloading the system software package, with 80% downloaded. • downloading (progress: 100%/50%): The system software package is successfully downloaded and is being written to the flash memory, with 50% written. • failed(AC global caching): The upgrade failed. When an AP is downloading system software package during an in-service upgrade, the system displays this message if the AP starts automatic upgrade which triggers a new process for downloading the software package. When multiple RRUs automatically upgrade at the same time, this message may also be displayed. In this situation, the actual RRU upgrade result depends on that displayed in the **display ap update status all** command output. • failed(alloc memory for file): The upgrade failed because the AP failed to apply for memory resources. • failed(analyze the version by upgrade filename): The upgrade failed because the device failed to analyze the version number in the file name. • failed(AP type in the EFS mismatch): The upgrade failed because the AP type in the EFS file trailer of the current AP version does not match the AP. • failed(AP type mismatch batch upgrade AP type): The upgrade failed because the AP type is different from the batch upgrade AP type. • failed(AP wait file timeout): The upgrade failed because the time that the AP waits for fragment data expired.

 Copyright © Huawei Technologies Co., Ltd.

	• failed(can not get AP type): The upgrade failed because the AC failed to obtain the AP type. • failed(change to standby): The upgrade failed due a revertive switchover failure. • failed(cut upgrade filename): The upgrade failed because the AC failed to process the upgrade file name. • failed(fail to download the file): The upgrade failed because the system software failed to be downloaded. • failed(file content error): The upgrade failed due to incorrect system software file contents. • failed(file version inconsistent): The upgrade failed because the AP type in the EFS file trailer does not match the AP type contained in the system software package name. • failed(invalid file name): The upgrade failed because the name of the AP version file is incorrect. • failed(link down): The upgrade failed because the AP failed to communicate with the AC. • failed(mode changed): The upgrade failed because the AP upgrade mode is changed during AP automatic upgrade. • failed(nospace in AP memory): The upgrade failed because the AP memory resources were insufficient. • failed(not receive update result): The upgrade failed because the AC receives no AP upgrade result. • failed(over max upgrade time): The upgrade failed because the upgrade duration exceeds the maximum upgrade time allowed. • failed(read file): The upgrade failed because no upgrade file is available in the flash memory. • failed(receive file failed): The upgrade failed because fragments failed to be received.

 Copyright © Huawei Technologies Co., Ltd.

	• failed(retransfer over times): The upgrade failed because the number of fragment retransmissions exceeds the threshold. • failed(send first file failed): The upgrade failed because the first fragment failed to be sent. • failed(send upgrade configuration): The upgrade failed because the upgrade configuration failed to be sent. • failed(send upgrade request): The upgrade failed because the upgrade request failed to be sent. • failed(unknown error): The upgrade failed due to an unknown error. • failed(upgrade configuration response error): The upgrade failed because there was an error in the AP's upgrade response. • failed(upgrade timeout): The upgrade timed out and failed. • failed(user canceled): The upgrade failed because the user cancels the upgrade. • failed(waited for next batch): The upgrade failed. The AP has to wait for the next upgrade. • failed(write flash error): The upgrade failed because the system software package failed to be written to the flash memory. • failed(age time out): The upgrade failed because the state machine aged out. • succeed: The upgrade succeeded. • succeed(auto resetting): The upgrade failed, and the AP is being restarted. • succeed(need reset): The upgrade succeeded. The AP must be restarted. • succeed(no need to update): The upgrade succeeded. There is no need to upgrade the AP. • -: The AP requires no upgrade.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.20 ap update load
14.1.22 ap update multi-load

14.1.93 display ap username

Function

The **display ap username** command displays the user name for logging in to an AP.

Format

display ap username [**ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays the user name for logging in to the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays the user name for logging in to the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ap username ap-name** *ap-name* command displays the user name for logging in to a specified AP.

Example

Display the user name for logging in to AP **huawei**.

```
<Huawei> display ap username ap-name huawei
-------------------------------------------------------------------------------
AP username: admin
AP password: ******
-------------------------------------------------------------------------------
```

Table 14-29 Description of the **display ap username** command output

Item	Description
AP username	User name for logging in to the AP. To configure the parameter, run the **14.1.28 ap username** command.
AP password	Password for logging in to the AP. To configure the parameter, run the **14.1.28 ap username** command.

Related Topics

14.1.28 ap username

14.1.94 display ap version

Function

The **display ap version** command displays AP version information.

Format

display ap version { **all** | { **ap-group** *ap-group-name* | **version-name** *version-name* } * }

Parameters

Parameter	Description	Value
all	Displays version information about all APs.	-
ap-group *ap-group-name*	Displays version information about all APs of a specified AP group.	The AP group must exist.
version-name *version-name*	Displays version information about a specified AP.	The value is string of 11 to 17 characters, in the format of **VxxxRxxxCxxx** or **VxxxRxxxCxxxSPCxxx**. For example, V200R006C00 or V200R005C10SPC200.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap version** command to view AP version information.

Example

Display version information about all APs.

```
<Huawei> display ap version all
Compatible version : V200R010
-------------------------------------------------------------------------------
ID    Name            Group   Type            Version            state
-------------------------------------------------------------------------------
0     60de-4476-e360 default AP6010DN-AGN     V200R007C00         normal
1     1047-80b1-56a0 default AP6310SN-GN      V200R007C00         normal
2     Huawei          default AP7030DE        V200R007C00         normal
3     AP4             gjg1                    _                   idle
4     48f8-dbc9-4a40 default AP4050DE-M-S     V200R010C00SPC500   normal
-------------------------------------------------------------------------------
Total: 5, printed: 5
```

Table 14-30 Description of the **display ap version** command output

Item	Description
Compatible version	Compatible version. Only the latest compatible version of the AP is displayed.
ID	AP ID.
Name	AP name.
Group	AP group name.
Type	AP type.
Version	AP version name.

Item	Description
state	State of an AP. ● commit-failed: WLAN service configuration commitment fails. ● committing: WLAN service configuration is being committed. ● config: The AP is initializing configuration. ● config-failed: The AP fails to initialize the configuration. ● download: The AP is downloading the upgrade software. ● fault: The AP is faulty. ● idle: The AP is in idle state. ● name-conflicted: APs' names conflict. ● nor: The AP is in normal state. ● standby: The AP is on the standby AC. ● ver-mismatch: Versions of the AP and AC do not match.

14.1.95 display ap whitelist

Function

The **display ap whitelist** command displays information about an AP whitelist.

Format

display ap whitelist { **mac** | **sn** }

Parameters

Parameter	Description	Value
sn	Displays serial numbers (SNs) in the AP whitelist.	-
mac	Displays MAC addresses in the AP whitelist.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the AP authentication mode is set to MAC authentication or SN authentication using the **14.1.11 ap auth-mode** command, you can run the **14.1.29 ap whitelist** command to configure an AP whitelist. Only APs on the whitelist are allowed to go online. To check information about APs in the whitelist, run the **display ap whitelist** command.

Example

Display MAC addresses in the AP whitelist.

```
<Huawei> display ap whitelist mac
-----------------------------------------------------------------------------
Index  MAC
-----------------------------------------------------------------------------
0      1047-80b1-56a0
1      0023-0024-0080
2      dcd2-fc9d-0bb0
-----------------------------------------------------------------------------
Total: 3
```

Table 14-31 Description of the **display ap whitelist mac** command output

Item	Description
Index	Index.
MAC	MAC address of an AP. To add a MAC address to the AP whitelist, run the **ap whitelist mac** *ap-mac1* [**to** *ap-mac2*] command.

Display SNs in the AP whitelist.

```
<Huawei> display ap whitelist sn
-----------------------------------------------------------------------------
Index  SN
-----------------------------------------------------------------------------
0      210235449210CB000011
1      S0001
2      210235568010D1000032
-----------------------------------------------------------------------------
Total: 3
```

Table 14-32 Description of the **display ap whitelist sn** command output

Item	Description
Index	Index.

Item	Description
SN	SN of an AP. To add an SN to the AP whitelist, run the **ap whitelist sn** *ap-sn1* [**to** *ap-sn2*] command.

Related Topics

14.1.29 ap whitelist

14.1.96 display ap wired-port

Function

The **display ap wired-port** command displays AP wired interface configuration.

Format

display ap wired-port *interface-type interface-number* { **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an AP wired interface.	The interface type and number need to be selected according to the actual device.
ap-name *ap-name*	Specifies an AP name.	The AP name must exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view configurations on the AP wired interface.

Example

Display GE interface configuration of AP **huawei**.

```
<Huawei> display ap wired-port gigabitethernet 0 ap-name huawei
--------------------------------------------------------------------------------
Wired port number             : 0
Wired port type               : GigabitEthernet
Wired port description        :
Wired port STP                : disable
Wired port user isolate       : disable
Wired port PVID VLAN          : -
Wired port VLAN tagged        : -
Wired port VLAN untagged      : -
Wired port Eth-trunk          : -
Wired port LLDP               : enable
Wired port LLDP basic TLV management address: enable
Wired port LLDP basic TLV port description  : enable
Wired port LLDP basic TLV system capability : enable
Wired port LLDP basic TLV system description: enable
Wired port LLDP basic TLV system name       : enable
Wired port CRC warn switch    : No
Wired port CRC warn high threshold : 50
Wired port CRC warn low threshold  : 20
Wired port IPv4 inbound ACL number : -
Wired port IPv4 outbound ACL number: -
--------------------------------------------------------------------------------
```

Table 14-33 Description about the **display ap wired-port gigabitethernet 0 ap-name huawei** command output

Item	Description
Wired port number	Number of the wired interface.
Wired port type	Type of the wired interface.
Wired port description	Description of the wired interface.
Wired port STP	Whether to enable STP on the wired interface.
Wired port user isolate	Whether to enable user isolation on the wired interface.
Wired port PVID VLAN	PVID of the wired interface.
Wired port VLAN tagged	VLAN to which the interface is added in tagged mode.
Wired port VLAN untagged	VLAN to which the interface is added in untagged mode.
Wired port Eth-trunk	Trunk ID to which the wired interface is bound.
Wired port LLDP	Whether to enable LLDP on the wired interface.
Wired port LLDP basic TLV management address	Management IP address of the wired interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wired port LLDP basic TLV port description	Wired interface description.
Wired port LLDP basic TLV system capability	Wired interface capability set.
Wired port LLDP basic TLV system description	Wired interface system description.
Wired port LLDP basic TLV system name	Wired interface system name.
Wired port CRC warn switch	Whether to enable the alarm function for CRC errors on the wired interface.
Wired port CRC warn high threshold	Upper alarm threshold for CRC errors on the wired interface.
Wired port CRC warn low threshold	Lower alarm threshold for CRC errors on the wired interface.
Wired port IPv4 inbound ACL number	IPv4-based ACL in the inbound direction.
Wired port IPv4 outbound ACL number	IPv4-based ACL in the outbound direction.

Display Eth-trunk interface configuration of AP **huawei**.

```
<Huawei> display ap wired-port eth-trunk 0 ap-name huawei
-------------------------------------------------------------------------------
Eth-trunk ID                        : 0
Eth-trunk description               : -
STP                               : disable
User isolate                        : disable
PVID VLAN                           : -
VLAN tagged                         : -
VLAN untagged                       : -
Wired port IPv4 Inbound ACL Number  : -
Wired port IPv4 Outbound ACL Number : -
-------------------------------------------------------------------------------
```

Table 14-34 Description about the **display ap wired-port eth-trunk 0 ap-name huawei** command output

Item	Description
Eth-trunk ID	ID of the Eth-trunk interface.
Eth-trunk description	Description of the Eth-trunk interface.
STP	Whether to enable STP on the Eth-trunk interface.

Item	Description
User isolate	Whether to enable user isolation on the Eth-trunk interface.
PVID VLAN	PVID of the Eth-trunk interface.
VLAN tagged	VLAN to which the Eth-trunk interface is added in tagged mode.
VLAN untagged	VLAN to which the Eth-trunk interface is added in untagged mode.
Wired port IPv4 Inbound ACL Number	IPv4-based ACL in the inbound direction.
Wired port IPv4 Outbound ACL Number	IPv4-based ACL in the outbound direction.

14.1.97 display ap-group

Function

The **display ap-group** command displays configuration and reference information about an AP group.

Format

display ap-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP groups.	-
name *group-name*	Displays information about a specified AP group.	The AP group must exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display ap-group** command to view configuration and reference information about an AP group.

Example

Display information about all AP groups.

```
<Huawei> display ap-group all
-------------------------------------------------------------
Name                          APs
-------------------------------------------------------------
default                       1
ap-group1                       0
-------------------------------------------------------------
Total: 2
```

Table 14-35 Description of the **display ap-group all** command output

Item	Description
Name	Name of an AP group.
APs	Number of APs in an AP group.

Display information of the AP group **default**.

```
<Huawei> display ap-group name default
-------------------------------------------------------------------------------
AP system profile          : default
Regulatory domain profile  : default
WIDS profile               : default
AP wired port profile
 Interface FE0             : default
 Interface FE1             : default
 Interface FE2             : default
 Interface FE3             : default
 Interface GE0             : default
 Interface GE1             : default
 Interface GE2             : default
 Interface GE3             : default
 Interface GE4             : default
 Interface GE5             : default
 Interface GE6             : default
 Interface GE7             : default
 Interface GE8             : default
 Interface GE9             : default
 Interface GE10            : default
 Interface GE11            : default
 Interface GE12            : default
 Interface GE13            : default
 Interface GE14            : default
 Interface GE15            : default
 Interface GE16            : default
 Interface GE17            : default
 Interface GE18            : default
 Interface GE19            : default
 Interface GE20            : default
 Interface GE21            : default
 Interface GE22            : default
 Interface GE23            : default
 Interface GE24            : default
```

```
 Interface GE25          : default
 Interface GE26          : default
 Interface GE27          : default
 Interface Eth-trunk0     : default
Radio 0
 Radio 2.4G profile       : default
 Radio 5G profile         : default
 VAP profile             :
 WDS profile             : default
 WDS whitelist profile    :
 Radio switch            : enable
 Channel                 : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)               : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m)  : 3
 Radio frequency          : 2.4G
 WIDS attack detect       : -
Radio 1
 Radio 5G profile         : default
 VAP profile             :
 WDS profile             :
 WDS whitelist profile    :
 Radio switch            : enable
 Channel                 : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)               : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m)  : 3
 Radio frequency          : 5G
 WIDS attack detect       : -
Radio 2
 Radio 5G profile         : default
 VAP profile             :
  WLAN  1                : default
 WDS profile             :
 WDS whitelist profile    :
 Radio switch            : enable
 Channel                 : -
 Channel bandwidth        : 20mhz
 EIRP(dBm)               : 127
 Antenna gain(dB)         : -
 Coverage distance(100 m)  : 3
 Radio frequency          : 5G
 WIDS attack detect       : -
```

Table 14-36 Description of the **display ap-group name** command output

Item	Description
AP system profile	AP system profile referenced by an AP group. To configure the parameter, run the **14.1.42 ap-system-profile (AP group view and AP view)** command.
Regulatory domain profile	Regulatory domain profile referenced by an AP group. To configure the parameter, run the **14.1.193 regulatory-domain-profile** command.

Item	Description
WIDS profile	WIDS profile referenced by an AP group. To configure the parameter, run the **14.4.57 wids-profile (AP group view and AP view)** command.
AP wired port profile	AP wired port profile referenced by an AP group. To configure the parameter, run the **14.1.241 wired-port-profile (AP group view and view)** command.
Interface *Interface-name*	Interface name.
Radio 0/Radio 1/Radio 2	Radio ID.
Radio 2.4G profile	2G radio profile referenced by an AP group. To configure the parameter, run the **14.1.185 radio-2g-profile** command.
Radio 5G profile	5G radio profile referenced by an AP group. To configure the parameter, run the **14.1.187 radio-5g-profile** command.
VAP profile	VAP profile referenced by an AP group. To configure the parameter, run the **14.1.234 vap-profile** command.
WDS profile	WDS profile referenced by an AP group. To configure the parameter, run the **14.5.21 wds-profile radio** command.
WDS whitelist profile	WDS whitelist profile referenced by an AP group. To configure the parameter, run the **14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)** command.
Radio switch	Whether a radio is enabled. To configure the parameter, run the **14.1.183 radio disable** command.
Channel	Working channel of a radio. To configure the parameter, run the **14.1.57 channel** command.
Channel bandwidth	Operating bandwidth of a radio. To configure the parameter, run the **14.1.57 channel** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EIRP(dBm)	Transmit power of a radio, in dBm. To configure the parameter, run the **14.1.140 eirp** command.
Antenna gain(dB)	Antenna gain of a radio, in dBm. To configure the parameter, run the **14.1.7 antenna-gain** command.
Coverage distance(100 m)	Radio coverage distance parameter (unit: 100 m). To configure the parameter, run the **14.1.62 coverage distance** command.
Radio frequency	Working frequency of a radio. To configure the parameter, run the **14.1.143 frequency** command.
WIDS attack detect	Whether attack detection is enabled. To configure the parameter, run the **14.4.55 wids attack detect enable** command.

Related Topics

14.1.31 ap-group

14.1.98 display ap-system-profile

Function

The **display ap-system-profile** command displays reference and configuration information about an AP system profile.

Format

display ap-system-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP system profiles.	-
name *profile-name*	Displays information about a specified AP system profile.	The AP system profile must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap-system-profile** command to view configuration and reference information about an AP system profile.

Example

Display information about all AP system profiles.

```
<Huawei> display ap-system-profile all
-------------------------------------------------------------
Profile name                    Reference
-------------------------------------------------------------
default                       1
ap-system1                      0
-------------------------------------------------------------
Total: 2
```

Table 14-37 Description of the **display ap-system-profile all** command output

Item	Description
Profile name	Name of an AP system profile.
Reference	Number of times an AP system profile is referenced.

Display information about the AP system profile **default**.

```
<Huawei> display ap-system-profile name default
-------------------------------------------------------------------------------
AC priority                    : -
Protect AC IP address          : -
AP management VLAN             : -
Temporary management switch    : disable
STA access mode                : disable
STA whitelist profile          : -
STA blacklist profile          : -
EAPOL start mode               : multicast
EAPOL start transform          : equal-bssid
EAPOL response mode            : unicast learning
EAPOL response transform       : equal-bssid
AP LLDP message transmission delay time(s): 2
AP LLDP message transmission hold multiplier: 4
AP LLDP message transmission interval time(s): 30
AP LLDP restart delay time(s) : 2
AP LLDP admin status           : txrx
AP LLDP report interval time(s): 30
AP high temperature threshold(degree C): -
AP low temperature threshold(degree C): -
AP CPU usage threshold(%)      : 90
AP memory usage threshold(%)   : 80
```

```
Alarm restriction            : enable
Alarm restriction period(s)   : 60
Log server IP address         : -
Ethernet port MTU(byte)       : 1500
Telnet                      : enable
STelnet server               : enable
SFTP server                  : enable
Console                     : enable
Led                        : on
Report disassoc request       : enable
Dynamic blacklist aging time(s): 600
--------------------------------------------------------------------------------
```

Table 14-38 Description of the **display ap-system-profile name** *profile-name* command output

Item	Description
AC priority	AC priority. To configure the parameter, run the **14.6.7 priority** command.
Protect AC IP address	IP address of the standby AC. To configure the parameter, run the **14.6.8 protect-ac** command.
AP management VLAN	Management VLAN of an AP. To configure the parameter, run the **14.1.169 management-vlan** command.
Temporary management switch	Status of management VAP and antenna alignment VAP for offline APs. To configure the parameter, run the **14.1.220 temporary-management enable (AP system profile view)** command.
STA access mode	STA access mode. To configure the parameter, run the **14.4.38 sta-access-mode** command.
STA whitelist profile	Name of a STA whitelist profile referenced by an AP system profile. To configure the parameter, run the **14.4.38 sta-access-mode** command.
STA blacklist profile	Name of a STA blacklist profile referenced by an AP system profile. To configure the parameter, run the **14.4.38 sta-access-mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EAPOL start mode	Eapol-start packet encapsulation mode. To configure the parameter, run the **14.1.139 eapol-start dest-address transform-to** command.
EAPOL start transform	Eapol-start packet conversion mode. To configure the parameter, run the **14.1.138 eapol-start dest-address transform-condition** command.
EAPOL response mode	Eapol-response packet encapsulation mode. To configure the parameter, run the **14.1.137 eapol-response dest-address transform-to** command.
EAPOL response transform	Eapol-response packet conversion mode. To configure the parameter, run the **14.1.136 eapol-response dest-address transform-condition** command.
AP LLDP message transmission delay time(s)	Delay for an AP to send LLDP packets to neighbors. To configure the parameter, run the **14.1.161 lldp message-transmission delay (AP system profile view)** command.
AP LLDP message transmission hold multiplier	Hold time multiplier of AP information on neighbors. To configure the parameter, run the **14.1.162 lldp message-transmission hold-multiplier (AP system profile view)** command.
AP LLDP message transmission interval time(s)	Interval at which an AP sends LLDP packets to neighbors. To configure the parameter, run the **14.1.163 lldp message-transmission interval (AP system profile view)** command.
AP LLDP restart delay time(s)	Delay in re-enabling LLDP. To configure the parameter, run the **14.1.165 lldp restart-delay** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AP LLDP admin status	LLDP mode on an AP. • tx: The AP sends but does not receive LLDP packets. • rx: The AP receives but does not send LLDP packets. • txrx: The AP sends and receives LLDP packets. To configure the parameter, run the **14.1.159 lldp admin-status** command.
AP LLDP report interval time(s)	Interval at which an AP reports LLDP neighbor information to an AC. To configure the parameter, run the **14.1.164 lldp report-interval** command.
AP high temperature threshold(degree C)	High temperature alarm threshold of an AP. To configure the parameter, run the **14.1.145 high-temperature threshold** command.
AP low temperature threshold(degree C)	Low temperature alarm threshold of an AP. To configure the parameter, run the **14.1.168 low-temperature threshold** command.
AP CPU usage threshold(%)	CPU usage alarm threshold of an AP. To configure the parameter, run the **14.1.63 cpu-usage threshold** command.
AP memory usage threshold(%)	Memory usage alarm threshold of an AP. To configure the parameter, run the **14.1.171 memory-usage threshold** command.
Alarm restriction	Alarm suppression status of an AP. To configure the parameter, run the **14.1.5 alarm-restriction disable** command.
Alarm restriction period(s)	Alarm suppression period of an AP. To configure the parameter, run the **14.1.6 alarm-restriction period** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Log server IP address	IP address of the log server. To configure the parameter, run the **14.1.167 log-server** command.
Ethernet port MTU(byte)	MTU of Ethernet interfaces. To configure the parameter, run the **14.1.172 mtu** command.
Telnet	Whether AP Telnet login is enabled. To configure the parameter, run the **14.1.219 telnet enable** command.
STelnet server	STelnet server status of an AP. To configure the parameter, run the **14.1.218 stelnet server disable** command.
SFTP server	SFTP server status of an AP. To configure the parameter, run the **14.1.210 sftp server disable** command.
Console	Whether AP console port login is enabled. To configure the parameter, run the **14.1.60 console disable** command.
Led	Whether AP indicators are allowed to turn on. ● on: The AP indicators are allowed to turn on. ● off: The AP indicators are forbidden to turn on. To configure the parameter, run the **14.1.157 led off** command.
Report disassoc request	Whether an AP is enabled to report disassociation request packets of STAs to the AC. To configure the parameter, run the **14.1.194 report-disassoc-request disable** command.
Dynamic blacklist aging time(s)	Aging time of a dynamic blacklist entry. To configure the parameter, run the **14.4.22 dynamic-blacklist aging-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.41 ap-system-profile (WLAN view)

14.1.99 display ap-type

Function

The **display ap-type** command displays AP type information.

Format

display ap-type { **all** | **id** *type-id* | **type** *ap-type* }

Parameters

Parameter	Description	Value
all	Displays all supported AP types.	-
id *type-id*	Specifies the AP type ID.	The AP type ID must exist.
type *ap-type*	Specifies the AP type name.	The AP type name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ap-type** command to view all AP types supported by the device and information about an AP of the specified type.

Example

Display all AP types supported by the device.

```
<Huawei> display ap-type all
--------------------------------------------------------------------------------
ID     Type
--------------------------------------------------------------------------------
17     AP6010SN-GN
19     AP6010DN-AGN
21     AP6310SN-GN
23     AP6510DN-AGN
25     AP6610DN-AGN
27     AP7110SN-GN
28     AP7110DN-AGN
29     AP5010SN-GN
```

 Copyright © Huawei Technologies Co., Ltd.

```
30    AP5010DN-AGN
31    AP3010DN-AGN
33    AP6510DN-AGN-US
34    AP6610DN-AGN-US
35    AP5030DN
36    AP5130DN
37    AP7030DE
38    AP2010DN
39    AP8130DN
40    AP8030DN
42    AP9330DN
43    AP4030DN
44    AP4130DN
45    AP3030DN
46    AP2030DN
47    AP9131DN
48    AP9132DN
49    AP5030DN-S
50    AP3010DN-V2
51    AP4030DN-E
56    AP6050DN
57    AP6150DN
58    AP7050DE
59    AP7050DN-E
60    AP4030TN
61    AP4050DN-E
62    AP4050DN-HD
64    AP430-E
68    AP1010SN
69    AP2050DN
70    AP2050DN-E
71    AP8130DN-W
73    AP2050DN-S
75    AP4050DN
76    AP4051DN
77    AP4151DN
78    AP4050DN-S
79    AP4051DN-S
80    AP8050DN
81    AP8150DN
82    AP8050DN-S
85    AP1050DN-S
86    AP4051TN
87    AP6052DN
88    AP7052DN
89    AP7052DE
90    AP3050DE
91    AP7152DN
92    AP8050TN-HD
93    AP8082DN
94    AP8182DN
97    AP2051DN
98    AP2051DN-S
99    AP2051DN-E
100    AP7060DN
101    AP5050DN-S
102    AP2030DN-S
103    AP4050DE-M
104    AP4050DE-M-S
105    AP100EC
106    AP200EC
107    AP300EC
108    WA375DD-CE
109    AP4050DE-B-S
110    AP5510-W-GP
111    AP2051DN-L-S
--------------------------------------------------------------------------------
Total: 74
```

NOTE

APs with the IDs of 90, 100, and 103 to 111 are supported only in the V200R010C00SPC600 version.

Table 14-39 Description of the **display ap-type all** command output

Item	Description
ID	ID of an AP.
Type	Type of an AP.

Display information about AP type 19.

```
<Huawei> display ap-type id 19
-------------------------------------------------------------------------------
Type                                : AP6010DN-AGN
AP wired port number                    : 1
AP wired port 0 type                  : GE
Radio number                          : 2
Radio 0 type                        : 802.11bgn
  Maximal spatial streams             : 2
  Maximal antenna number                : 2
  Maximal VAP number                  : 16
  Antenna gain                      : 4
Radio 1 type                        : 802.11an
  Maximal spatial streams             : 2
  Maximal antenna number                : 2
  Maximal VAP number                  : 16
  Antenna gain                      : 5
Maximum station number                  : 128
AP high temperature threshold(degree C): 102
AP low temperature threshold(degree C) : -13
Outdoor                             : N
-------------------------------------------------------------------------------
```

Table 14-40 Description of the **display ap-type id** command output

Item	Description
Type	AP type.
AP wired port number	Number of wired interfaces.
AP wired port 0 type	Type of wired interfaces.
Radio number	Number of radios.
Radio 0 type	Type of the radio. The value 0 indicates the radio ID.
Maximal spatial streams	Maximum number of spatial streams on the radio.
Maximal antenna number	Maximum number of antennas on the radio.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximal VAP number	Maximum number of VAPs of the radio.
Antenna gain	Antenna gain of the radio, in dB.
Maximum station number	Maximum number of STAs supported by the AP type.
AP high temperature threshold(degree C)	High temperature alarm threshold.
AP low temperature threshold(degree C)	Low temperature alarm threshold.
Outdoor	Type of an AP. ● Y: Outdoor AP. ● N: Indoor AP.

14.1.100 display capwap configuration

Function

The **display capwap configuration** command displays the CAPWAP configuration.

Format

display capwap configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the interval for sending Keepalive packets, number of times for sending Keepalive packets, and priority of CAPWAP management packets.

Example

Display the CAPWAP configuration.

```
<Huawei> display capwap configuration
  ------------------------------------------------------------
  Source interface                        : -
  Source ip-address                       : -
  Echo interval(seconds)                  : 25
  Echo times                              : 6
  Control priority(server to client)      : 7
  Control priority(client to server)      : 7
  Control-link DTLS encrypt               : enable
  DTLS PSK value                          : ******
  PSK mandatroy match switch              : disable
  IPv6 status                             : disable
  ------------------------------------------------------------
```

Table 14-41 Description of the **display capwap configuration** command output

Item	Description
Source interface	AC's source interface. To configure the parameter, run the **capwap source interface** command.
Source ip-address	IP address of the AC's source interface.
Echo interval(seconds)	Interval for sending Keepalive packets. To specify the interval for sending Keepalive packets, run the **capwap echo interval** command.
Echo times	Number of times for sending Keepalive packets. If the APs or AC receive no response from each other after the Keepalive packets are sent for the specified number of times, the APs or AC consider that they are disconnected from their peer devices. To specify the number of times for sending Keepalive packets, run the **capwap echo times** command.
Control priority(server to client)	Priority of CAPWAP management packets from an AC to an AP. To configure the priority of CAPWAP management packets from an AC to an AP, run the **capwap control-link-priority local** *priority-value* command.
Control priority(client to server)	Priority of CAPWAP management packets from an AP to an AC. To configure the priority of CAPWAP management packets from an AP to an AC, run the **capwap control-link-priority remote** *priority-value* command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Control-link DTLS encrypt	Whether CAPWAP control tunnel using DTLS is enabled. To enable CAPWAP control tunnel using DTLS, run the **capwap dtls control-link encrypt** command.
DTLS PSK value	Pre-shared key for DTLS encryption. To configure the pre-shared key for DTLS encryption, run the **capwap dtls psk** command.
PSK mandatroy match switch	Whether an AP is enabled to perform DTLS sessions with the AC using the default pre-shared key. To enable an AP to perform DTLS sessions with the AC using the default pre-shared key, run the **capwap dtls psk-mandatory-match enable** command.
IPv6 status	Whether the CAPWAP tunnel supports the IPv6 function. To configure this parameter, run the **capwap ipv6 enable** command.

Related Topics

14.1.47 capwap control-link-priority
14.1.48 capwap dtls control-link encrypt
14.1.49 capwap dtls psk
14.1.50 capwap dtls psk-mandatory-match enable
14.1.51 capwap echo

14.1.101 display channel switch-record

Function

The **display channel switch-record** command displays channel switching records on the device.

Format

display channel switch-record { **all** | **ap-name** *ap-name* **radio** *radio-id* | **ap-id** *ap-id* **radio** *radio-id* | **reason** *reason* }

Parameters

Parameter	Description	Value
all	Displays all channel switching records.	-
ap-name *ap-name*	Displays channel switching records of the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays channel switching records of a specified AP radio.	The radio ID must exist.
ap-id *ap-id*	Displays channel switching records of the AP with a specified ID.	The AP ID must exist.
reason *reason*	Displays records of channel switching caused by a specified reason.	The enumerated values are: ● calibration: channel switching caused by radio calibration ● configuration: channel switching caused by configuration ● dfs: channel switching performed to avoid radar channels ● unsupported: channel switching performed because the AP does not support the channel delivered from the AC ● wds: channel switching caused by channel negotiation on a WDS network

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command enables you to view channel switching records on a device.

Example

Display all channel switching records.

```
<Huawei> display channel switch-record all
Old/New: Old channel/New channel
RfID   : Radio ID
-----------------------------------------------------------------------------------------
AP name  RfID      Old/New  Switch reason  Switch time
-----------------------------------------------------------------------------------------
L2-4f     0        1/6      wds            11:03:30 2014/9/28
-----------------------------------------------------------------------------------------
Total : 1, printed : 1
```

Table 14-42 Description of the **display channel switch-record** command output

Item	Description
AP name	Name of an AP where channel switching has occurred.
RfID	Radio ID.
Old/New	Channels used before and after switching.
Switch reason	Reason for channel switching.
Switch time	Time when channel switch occurred.

Related Topics

14.1.198 reset channel switch-record

14.1.102 display mac-address ap-all

Function

The **display mac-address ap-all** command displays MAC address entries on all APs.

Format

display mac-address *mac-address* [**verbose**] **ap-all**

Parameters

Parameter	Description	Value
mac-address	Displays MAC address entries on all APs.	The value is in H-H-H format, where H is a hexadecimal number of 1 to 4 digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Displays detailed information of the dynamic entries. If *verbose* is not specified, brief information of the dynamic entries is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When errors or attacks occur on the network, you can run the **display mac-address ap-all** command to locate the attack sources based on the displayed MAC addresses.

Example

Display dynamic MAC address entries of all APs.

```
<Huawei> display mac-address 00e0-fc09-bcf9 ap-all
Info: Waiting for AP response...done.
--------------------------------------------------------------------------------
MAC Address    VLAN/VSI       Learned-From              Type       AP ID
--------------------------------------------------------------------------------
00e0-fc09-bcf9    1/-         GigabitEthernet0/0/0      dynamic    1
00e0-fc09-bcf9    1/-         GigabitEthernet0/0/0      dynamic    0
--------------------------------------------------------------------------------
Total: 2
```

Table 14-43 Description of the **display mac-address** *mac-address* **ap-all** command output

Item	Description
MAC Address	MAC address.
VLAN/VSI	VLAN or VSI to which the device belongs.
Learned-From	Interface that learns a MAC address.
Type	Type of a MAC address entry.
AP ID	AP ID.

 Copyright © Huawei Technologies Co., Ltd.

14.1.103 display mac-address { ap-id | ap-name }

Function

The **display mac-address** { **ap-id** | **ap-name**} command displays all dynamic MAC address entries on an AP's wired interface.

Format

display mac-address { **ap-id** *ap-id* | **ap-name** *ap-name* } *interface-type interface-number*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays all dynamic MAC address entries on wired interfaces of the AP with the specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays all dynamic MAC address entries on wired interfaces of the AP with the specified name.	The AP name must exist.
interface-type interface-number	Displays dynamic MAC address entries on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the number of the outbound interface.	Currently, only Ethernet interfaces are supported.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display mac-address** { **ap-id** | **ap-name**} command to check all dynamic MAC address entries on an AP's wired interface, including the MAC addresses and VLANs that the AP learns on specified interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display dynamic MAC address entries on wired interfaces of the AP with ID 1.

```
<Huawei> display mac-address ap-id 1 ethernet 0
-------------------------------------------------------------
MAC Address    VLAN/VSI   Learned-From        Type
-------------------------------------------------------------
1051-7254-5a80 1/-        Ethernet0/0/0       dynamic
-------------------------------------------------------------
Total: 1
```

Table 14-44 Description of the **display mac-address ap-id** *ap-id interface-type interface-number* command output

Item	Description
MAC Address	MAC address.
VLAN/VSI	VLAN or VSI to which the device belongs.
Learned-From	Interface on which the MAC address is learned.
Type	Type of a MAC address entry.

Related Topics

14.1.199 reset mac-address { ap-id | ap-name }

14.1.104 display port-link-profile

Function

The **display port-link-profile** command displays reference and configuration information about an AP wired port link profile.

Format

display port-link-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP wired port link profiles.	-
name *profile-name*	Displays information about a specified AP wired port link profile.	The AP wired port link profile must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display port-link-profile** command to view configuration and reference information about an AP wired port link profile.

Example

Display information about all AP wired port link profiles.

```
<Huawei> display port-link-profile all
-------------------------------------------------------------
Profile name                    Reference
-------------------------------------------------------------
default                       1
port-link-profile-1             0
-------------------------------------------------------------
Total: 2
```

Table 14-45 Description of the **display port-link-profile all** command output

Item	Description
Profile name	Name of an AP wired port link profile.
Reference	Number of times an AP wired port link profile is referenced.

Display information about the AP wired port link profile **default**.

```
<Huawei> display port-link-profile name default
-----------------------------------------------------------------------------
LLDP enable                 : enable
Management address          : enable
Port description            : enable
System capability           : enable
System description          : enable
System name                 : enable
CRC error alarm             : disable
CRC error high threshold(%): 50
CRC error Low threshold(%) : 20
Shutdown switch             : disable
-----------------------------------------------------------------------------
```

Table 14-46 Description of the **display port-link-profile name** *profile-name* command output

Item	Description
LLDP enable	Whether LLDP is enabled on an AP's wired interface. To configure the parameter, run the **14.1.160 lldp enable** command.
Management address	Whether an AP's wired interface is allowed to advertise the Management-address TLV. To configure the parameter, run the **14.1.166 lldp tlv-enable (AP wired port link profile view)** command.
Port description	Whether an AP's wired interface is allowed to advertise the Port-description TLV. To configure the parameter, run the **14.1.166 lldp tlv-enable (AP wired port link profile view)** command.
System capability	Whether an AP's wired interface is allowed to advertise the System-capability TLV. To configure the parameter, run the **14.1.166 lldp tlv-enable (AP wired port link profile view)** command.
System description	Whether an AP's wired interface is allowed to advertise the System-description TLV. To configure the parameter, run the **14.1.166 lldp tlv-enable (AP wired port link profile view)** command.
System name	Whether an AP's wired interface is allowed to advertise the System-name TLV. To configure the parameter, run the **14.1.166 lldp tlv-enable (AP wired port link profile view)** command.
CRC error alarm	Whether the alarm function for CRC errors is enabled on an AP's wired interface. To configure the parameter, run the **14.1.64 crc-alarm enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CRC error high threshold(%)	Alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **14.1.64 crc-alarm enable** command.
CRC error Low threshold(%)	Clear alarm threshold for CRC errors on an AP's wired interface. To configure the parameter, run the **14.1.64 crc-alarm enable** command.
Shutdown switch	Whether the AP's wired interface function is disabled. To configure the parameter, run the **14.1.212 shutdown (AP wired port link profile view)** command.

Related Topics

14.1.64 crc-alarm enable
14.1.160 lldp enable
14.1.166 lldp tlv-enable (AP wired port link profile view)
14.1.174 port-link-profile (WLAN view)

14.1.105 display radio

Function

The **display radio** command displays AP radio information.

Format

display radio { **all** | **ap-group** *ap-group-name* | **ap-name** *ap-name* | **ap-id** *ap-id* }

Parameters

Parameter	Description	Value
all	Displays radio information about all APs.	-
ap-group *ap-group-name*	Displays radio information about all APs in a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays radio information about the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays radio information about the AP with a specified ID.	The AP ID must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display radio** command to view current working status of an AP radio.

Example

Display radio information about all APs.

```
<Huawei> display radio all
CH/BW:Channel/Bandwidth
CE:Current EIRP (dBm)
ME:Max EIRP (dBm)
CU:Channel utilization
ST:Status
---------------------------------------------------------------------------
AP ID Name    RfID  Band  Type    ST  CH/BW        CE/ME   STA    CU
---------------------------------------------------------------------------
0     L1_003  0     2.4G  bgn     on  6/20M        27/27   0      71%
0     L1_003  1     5G    an      on  149/20M      28/28   0      39%
---------------------------------------------------------------------------
Total:2
```

Table 14-47 Description of the **display radio** command output

Item	Description
AP ID	AP ID.
Name	AP name.
RfID	Radio ID of an AP.
Band	Working frequency of an AP radio.
Type	Protocol type of an AP radio.
ST	Working status of an AP radio.
CH/BW	Channel/Bandwidth of an AP radio.
CE/ME	Current power of an AP radio/ Maximum power of an AP radio.
STA	Number of STAs connected to an AP radio.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CU	Channel usage. **NOTE** When the working mode of an AP radio is the monitor mode, this parameter is displayed as **-**.

14.1.106 display radio-2g-profile

Function

The **display radio-2g-profile** command displays configuration and reference information about a 2G radio profile.

Format

display radio-2g-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all 2G radio profiles.	-
name *profile-name*	Displays information about a specified 2G radio profile.	The 2G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display radio-2g-profile** command to view configuration and reference information about a 2G radio profile.

Example

Display information about all 2G radio profiles.

```
<Huawei> display radio-2g-profile all
-------------------------------------------------------
Profile name                Reference
-------------------------------------------------------
```

```
default                    1
-----------------------------------------------------------
Total: 1
```

Table 14-48 Description of the **display radio-2g-profile all** command output

Item	Description
Profile name	Name of a 2G radio profile.
Reference	Number of times a 2G radio profile is referenced.

Display information of the 2G radio profile **default**.

```
<Huawei> display radio-2g-profile name default
-----------------------------------------------------------------
Radio type                          : 802.11n
Power auto adjust                   : disable
Beacon interval(ms)                 : 100
Support short preamble              : support
Channel switch announcement         : enable
Guard interval mode                 : normal
HT A-MPDU switch                    : enable
HT A-MPDU length limit              : 3
RTS-CTS-mode                        : cts-to-self
RTS-CTS-threshold                   : 2347
802.11bg basic rate                 : 1 2
802.11bg support rate               : 1 2 5 6 9 11 12 18 24 36 48 54
Multicast rate 2.4G                 : 11
Interference detect switch          : disable
Co-channel frequency interference threshold(%)      : 50
Adjacent-channel frequency interference threshold(%)  : 50
Station interference threshold      : 32
WMM switch                          : enable
Mandatory switch                    : disable
Wifi-light mode                     : signal-strength
Utmost power switch                 : enable
Rrm-profile                         : default
Air-scan-profile                    : default
-----------------------------------------------------------------
AP EDCA parameters:
--------------------------------------------------
      ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO  3      2      1      47         normal
AC_VI  4      3      1      94         normal
AC_BE  6      4      3      0          normal
AC_BK  10     4      7      0          normal
--------------------------------------------------
```

Table 14-49 Description of the **display radio-2g-profile name** command output

Item	Description
Radio type	Radio type. To configure the parameter, run the **14.1.188 radio-type (2G radio profile view)** command.

Item	Description
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure the parameter, run the **14.2.33 power auto-adjust enable** command.
Beacon interval(ms)	Interval at which an AP sends Beacon frames, in ms. To configure the parameter, run the **14.1.46 beacon-interval** command.
Support short preamble	Whether the short preamble is supported. To configure the parameter, run the **14.1.211 short-preamble disable** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure the parameter, run the **14.1.58 channel-switch announcement disable** command.
Guard interval mode	GI mode. To configure the parameter, run the **14.1.144 guard-interval-mode** command.
HT A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure the parameter, run the **14.1.146 ht a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure the parameter, run the **14.1.147 ht a-mpdu max-length-exponent** command.
RTS-CTS-mode	RTS/CTS mode. To configure the parameter, run the **14.1.206 rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure the parameter, run the **14.1.207 rts-cts-threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
802.11bg basic rate	802.11bg basic rate set. To configure the parameter, run the **14.1.133 dot11bg basic-rate** command.
802.11bg support rate	802.11bg supported rate set. To configure the parameter, run the **14.1.134 dot11bg supported-rate** command.
Multicast rate 2.4G	Multicast rate of wireless packets on the 2.4GHz radio. To configure the parameter, run the **14.1.173 multicast-rate** command.
Interference detect switch	Whether interference detection is enabled. To configure the parameter, run the **14.2.30 interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure the parameter, run the **14.2.29 interference co-channel threshold** command.
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure the parameter, run the **14.2.28 interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure the parameter, run the **14.2.31 interference station threshold** command.
WMM switch	Whether the WMM function is enabled. To configure the parameter, run the **14.1.243 wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure the parameter, run the **14.1.246 wmm mandatory enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Wifi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure the parameter, run the **14.1.239 wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure the parameter, run the **14.2.36 rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure the parameter, run the **14.2.3 air-scan-profile (radio profile view)** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure the parameter, run the **14.1.232 utmost-power disable** command.
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VO	AC_VO packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BE	AC_BE packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BK	AC_BK packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an STA can occupy a channel. A larger value indicates a longer duration. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
Ack-Policy	ACK policy. It includes: • **normal**: During 802.11 packet exchange, the receiver sends an ACK packet to confirm the receiving of a packet from the sender. • **noack**: The receiver sends no ACK packet to confirm the receiving of a packet from the sender. It applies to scenarios where communication quality is good and interference is low. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

14.1.107 display radio-5g-profile

Function

The **display radio-5g-profile** command displays configuration and reference information about a 5G radio profile.

Format

display radio-5g-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all 5G radio profiles.	-
name *profile-name*	Displays information about a specified 5G radio profile.	The 5G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display radio-5g-profile** command to view configuration and reference information about a 5G radio profile.

Example

Display information about all 5G radio profiles.

```
<Huawei> display radio-5g-profile all
-----------------------------------------------------------
Profile name                    Reference
-----------------------------------------------------------
default                         1
-----------------------------------------------------------
Total: 1
```

Table 14-50 Description of the **display radio-5g-profile all** command output

Item	Description
Profile name	Name of a 5G radio profile.
Reference	Number of times a 5G radio profile is referenced.

Display information of the 5G radio profile **default**.

```
<Huawei> display radio-5g-profile name default
-----------------------------------------------------------
Radio type                          : 802.11ac
Power auto adjust                   : disable
Beacon interval(ms)                 : 100
Beamforming switch                  : disable
Support short preamble              : not support
Channel switch announcement         : support
Guard interval mode                 : normal
```

```
HT A-MPDU switch                    : disable
HT A-MPDU length limit               : 3
VHT A-MPDU length limit              : 7
VHT A-MSDU switch                   : disable
VHT A-MSDU Max frame number          : 2
RTS-CTS-mode                        : CTS-TO-SELF
RTS-CTS-threshold                   : 2347
802.11a basic rate                  : 6 12 24
802.11a support rate                : 6 9 12 18 24 36 48 54
Multicast rate 5G                   : 6
VHT mcs                             : 9 9 9
Interference detect switch          : disable
Co-channel frequency interference threshold(%)       : 50
Adjacent-channel frequency interference threshold(%)  : 50
Station interference threshold       :32
WMM switch                          : enable
Mandatory switch                    : disable
Auto-off start time                 : -
Auto-off end time                   : -
WiFi-light mode                     : signal-strength
Utmost power switch                 : enable
Rrm-profile                         : default
Air-scan-profile                    : default
------------------------------------------------------------
AP EDCA parameters:
----------------------------------------------------
      ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO  3       2       1      47         normal
AC_VI  4       3       1      94         normal
AC_BE  6       4       3      0          normal
AC_BK  10      4       7      0          normal
----------------------------------------------------
```

Table 14-51 Description of the **display radio-5g-profile name** command output

Item	Description
Radio type	Radio type. To configure the parameter, run the **14.1.189 radio-type (5G radio profile view)** command.
Power auto adjust	Whether automatic per packet power adjustment is enabled. To configure the parameter, run the **14.2.33 power auto-adjust enable** command.
Beacon interval(ms)	Interval at which an AP sends Beacon frames, in ms. To configure the parameter, run the **14.1.46 beacon-interval** command.
Beamforming switch	Whether the beamforming function is enabled. When the WLAN mode is AC, this parameter cannot be set.

Item	Description
Support short preamble	Whether the short preamble is supported. To configure the parameter, run the **14.1.211 short-preamble disable** command.
Channel switch announcement	Whether channel switch announcement is enabled. To configure the parameter, run the **14.1.58 channel-switch announcement disable** command.
Guard interval mode	GI mode. To configure the parameter, run the **14.1.144 guard-interval-mode** command.
HT A-MPDU switch	Whether the MPDU aggregation function is enabled. To configure the parameter, run the **14.1.146 ht a-mpdu disable** command.
HT A-MPDU length limit	Maximum length of the aggregated MPDU frame. To configure the parameter, run the **14.1.147 ht a-mpdu max-length-exponent** command.
VHT A-MPDU length limit	Maximum length of the frame aggregated in A-MSDU mode. To configure the parameter, run the **14.1.235 vht a-mpdu max-length-exponent** command.
VHT A-MSDU switch	Whether to enable the function of sending 802.11 packets in A-MSDU mode. To configure the parameter, run the **14.1.236 vht a-msdu enable** command.
VHT A-MSDU Max frame number	Maximum number of subframes that can be aggregated into an A-MSDU. To configure the parameter, run the **14.1.237 vht a-msdu max-frame-num** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RTS-CTS-mode	RTS/CTS mode. To configure the parameter, run the **14.1.206 rts-cts-mode** command.
RTS-CTS-threshold	RTS/CTS threshold. To configure the parameter, run the **14.1.207 rts-cts-threshold** command.
802.11a basic rate	802.11a basic rate set. To configure the parameter, run the **14.1.131 dot11a basic-rate** command.
802.11a support rate	802.11a supported rate set. To configure the parameter, run the **14.1.132 dot11a supported-rate** command.
Multicast rate 5G	Multicast rate of wireless packets on the 5 GHz radio. To configure the parameter, run the **14.1.173 multicast-rate** command.
VHT mcs	Maximum MCS value corresponding to a specific number of 802.11ac spatial streams. To configure the parameter, run the **14.1.238 vht mcs-map** command.
Interference detect switch	Whether interference detection is enabled. To configure the parameter, run the **14.2.30 interference detect-enable** command.
Co-channel frequency interference threshold(%)	Alarm threshold for co-channel interference. To configure the parameter, run the **14.2.29 interference co-channel threshold** command.
Adjacent-channel frequency interference threshold(%)	Alarm threshold for adjacent-channel interference. To configure the parameter, run the **14.2.28 interference adjacent-channel threshold** command.
Station interference threshold	Alarm threshold for STA interference. To configure the parameter, run the **14.2.31 interference station threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WMM switch	Whether the WMM function is enabled. To configure the parameter, run the **14.1.243 wmm disable** command.
Mandatory switch	Whether to allow STAs that do not support WMM to connect to a WMM-enabled AP. To configure the parameter, run the **14.1.246 wmm mandatory enable** command.
Auto-off start time	Start time for scheduled VAP auto-off.
Auto-off end time	End time for scheduled VAP auto-off.
WiFi-light mode	Information reflected by the blinking frequency of the Wireless LED. To configure the parameter, run the **14.1.239 wifi-light** command.
Rrm-profile	Name of the RRM profile referenced by a radio profile. To configure the parameter, run the **14.2.36 rrm-profile (radio profile view)** command.
Air-scan-profile	Name of the air scan profile referenced by a radio profile. To configure the parameter, run the **14.2.3 air-scan-profile (radio profile view)** command.
Utmost power switch	Whether a radio is enabled to send packets at maximum power. To configure the parameter, run the **14.1.232 utmost-power disable** command.
AP EDCA parameters	EDCA parameters and ACK policy on an AP. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VO	AC_VO packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AC_BE	AC_BE packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BK	AC_BK packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an STA can occupy a channel. A larger value indicates a longer duration. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
Ack-Policy	ACK policy. It includes: • **normal**: During 802.11 packet exchange, the receiver sends an ACK packet to confirm the receiving of a packet from the sender. • **noack**: The receiver sends no ACK packet to confirm the receiving of a packet from the sender. It applies to scenarios where communication quality is good and interference is low. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

14.1.108 display references ap-system-profile

Function

The **display references ap-system-profile** command displays reference information about an AP system profile.

Format

display references ap-system-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP system profile.	The AP system profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references ap-system-profile** command to view reference information about an AP system profile.

Example

Display reference information of the AP system profile **default**.

```
<Huawei> display references ap-system-profile name default
-----------------------------------------------------------------------
Reference type              Reference name
-----------------------------------------------------------------------
AP group                    ap-group1
-----------------------------------------------------------------------
Total: 1
```

Table 14-52 Description of the **display references ap-system-profile** command output

Item	Description
Reference type	Type of the profile by which an AP system profile is referenced.

Item	Description
Reference name	Name of the profile by which an AP system profile is referenced.

14.1.109 display references port-link-profile

Function

The **display references port-link-profile** command displays reference information about an AP wired port link profile.

Format

display references port-link-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP wired port link profile.	The AP wired port link profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references port-link-profile** command to view reference information about an AP wired port link profile.

Example

Display reference information about the AP wired port link profile **default**.

```
<Huawei> display references port-link-profile name default
-----------------------------------------------------------------
Reference type                Reference name
-----------------------------------------------------------------
AP wiredport profile           wired-port1
-----------------------------------------------------------------
Total:1
```

Table 14-53 Description of the **display references port-link-profile** command output

Item	Description
Reference type	Type of the profile by which an AP wired port link profile is referenced.
Reference name	Name of the profile by which an AP wired port link profile is referenced.

14.1.110 display references radio-2g-profile

Function

The **display references radio-2g-profile** command displays reference information about a 2G radio profile.

Format

display references radio-2g-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified 2G radio profile.	The 2G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references radio-2g-profile** command to view reference information about a 2G radio profile.

Example

Display reference information about the 2G radio profile **default**.

```
<Huawei> display references radio-2g-profile name default
-----------------------------------------------------------------
Reference type              Reference name
-----------------------------------------------------------------
AP-group                    ap-group1
```

```
-----------------------------------------------------------------
Total:1
```

Table 14-54 Description of the **display references radio-2g-profile** command output

Item	Description
Reference type	Type of the profile by which a 2G radio profile is referenced.
Reference name	Name of the profile by which a 2G radio profile is referenced.

14.1.111 display references radio-5g-profile

Function

The **display references radio-5g-profile** command displays reference information about a 5G radio profile.

Format

display references radio-5g-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified 5G radio profile.	The 5G radio profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references radio-5g-profile** command to view reference information about a 5G radio profile.

Example

Display reference information about the 5G radio profile **default**.

```
<Huawei> display references radio-5g-profile name default
-----------------------------------------------------------------
```

```
Reference type              Reference name
-----------------------------------------------------------------
AP-group                    ap-group1
-----------------------------------------------------------------
Total:1
```

Table 14-55 Description of the **display references radio-5g-profile** command output

Item	Description
Reference type	Type of the profile by which a 5G radio profile is referenced.
Reference name	Name of the profile by which a 5G radio profile is referenced.

14.1.112 display references regulatory-domain-profile

Function

The **display references regulatory-domain-profile** command displays reference information about a regulatory domain profile.

Format

display references regulatory-domain-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified regulatory domain profile.	The regulatory domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references regulatory-domain-profile** command to view reference information about a regulatory domain profile.

Example

Display reference information about the regulatory domain profile **default**.

```
<Huawei> display references regulatory-domain-profile name default
-----------------------------------------------------------
Reference type          Reference name
-----------------------------------------------------------
AP-group                default
AP-group                hw
-----------------------------------------------------------
Total: 2
```

Table 14-56 Description of the **display references regulatory-domain-profile** command output

Item	Description
Reference type	Type of the profile by which a regulatory domain profile is referenced.
Reference name	Name of the profile by which a regulatory domain profile is referenced.

14.1.113 display references ssid-profile

Function

The **display references ssid-profile** command displays reference information about an SSID profile.

Format

display references ssid-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified SSID profile.	The SSID profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references ssid-profile** command to view reference information about an SSID profile.

Example

Display reference information about the SSID profile **default**.

```
<Huawei> display references ssid-profile name default
-----------------------------------------------------------------
Reference type                Reference name
-----------------------------------------------------------------
VAP profile                   vap-profile1
-----------------------------------------------------------------
Total:1
```

Table 14-57 Description of the **display references ssid-profile** command output

Item	Description
Reference type	Type of the profile by which an SSID profile is referenced.
Reference name	Name of the profile by which an SSID profile is referenced.

14.1.114 display references traffic-profile

Function

The **display references traffic-profile** command displays the reference information of a traffic profile.

Format

display references traffic-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays the reference information of a specified traffic profile.	The traffic profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the VAP profiles by which a specified traffic profile is referenced.

Example

Display the reference information of the traffic profile **p1**.

```
<Huawei> display references traffic-profile name p1
--------------------------------------------------
Reference type     Reference name
--------------------------------------------------
VAP profile        default
VAP profile        wlan-vap
VAP profile        jsl
VAP profile        test
VAP profile        wlan-vap1
VAP profile        huawei
VAP profile        2
--------------------------------------------------
Total: 7
```

Table 14-58 Description of the **display references traffic-profile** command output

Item	Description
Reference type	Type of the profile that references a traffic profile.
Reference name	Name of the profile that references a traffic profile.

14.1.115 display references vap-profile

Function

The **display references vap-profile** command displays reference information about a VAP profile.

Format

display references vap-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified VAP profile.	The VAP profile must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references vap-profile** command to view reference information about a VAP profile.

Example

Display reference information about the VAP profile **default**.

```
<Huawei> display references vap-profile name default
-------------------------------------------------------------------------------
Reference type     Reference name                    Reference radio  WLAN ID
-------------------------------------------------------------------------------
AP group           group1                            Radio-0          1
-------------------------------------------------------------------------------
Total: 1
```

Table 14-59 Description of the **display references vap-profile** command output

Item	Description
Reference type	Type of the profile by which a VAP profile is referenced.
Reference name	Name of the profile by which a VAP profile is referenced.
Reference radio	AP radio by which a VAP profile is referenced.
WLAN ID	WLAN ID of a VAP.

14.1.116 display references wired-port-profile

Function

The **display references wired-port-profile** command displays reference information about an AP wired port profile.

Format

display references wired-port-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified AP wired port profile.	The AP wired port profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wired-port-profile** command to view reference information about an AP wired port profile.

Example

Display reference information about the AP wired port profile **default**.

```
<Huawei> display references wired-port-profile name default
-----------------------------------------------------------------------------
Reference type     Reference name                    Reference port
-----------------------------------------------------------------------------
AP group           huawei                            Ethernet0
-----------------------------------------------------------------------------
Total: 1
```

Table 14-60 Description of the **display references wired-port-profile** command output

Item	Description
Reference type	Type of the profile by which an AP wired port profile is referenced.
Reference name	Name of the profile by which an AP wired port profile is referenced.
Reference port	Interface by which an AP wired port profile is referenced.

14.1.117 display regulatory-domain-profile

Function

The **display regulatory-domain-profile** command displays configuration information about a regulatory domain profile.

Format

display regulatory-domain-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all regulatory domain profiles.	-
name *profile-name*	Displays information about a specified regulatory domain profile.	The regulatory domain profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display regulatory-domain-profile** command to view configuration information about a regulatory domain profile.

Example

Display information about all regulatory profiles.

```
<Huawei> display regulatory-domain-profile all
-----------------------------------------------------------
Profile name        Reference
-----------------------------------------------------------
default             6
-----------------------------------------------------------
Total: 1
```

Table 14-61 Description of the **display regulatory-domain-profile all** command output

Item	Description
Profile name	Regulatory domain profile name.
Reference	Number of times a regulatory domain profile is referenced.

Display information about the regulatory domain profile **default**.

```
<Huawei> display regulatory-domain-profile name default
-----------------------------------------------------------
```

```
Profile name          : default
Country code          : CN
2.4G dca channel-set  : 1,6,11
5G dca bandwidth      : 20mhz
5G dca channel-set    : 149,153,157,161,165
-------------------------------------------------------------
```

Table 14-62 Description of the **display regulatory-domain-profile name** command output

Item	Description
Profile name	Regulatory domain profile name.
Country code	Country code. To configure the parameter, run the **14.1.61 country-code** command.
2.4G dca channel-set	2.4G radio calibration channel set. To configure the parameter, run the **14.2.16 dca-channel channel-set** command.
5G dca bandwidth	5G radio calibration bandwidth. To configure the parameter, run the **14.2.15 dca-channel bandwidth** command.
5G dca channel-set	5G radio calibration channel set. To configure the parameter, run the **14.2.16 dca-channel channel-set** command.

Related Topics

14.1.61 country-code

14.2.15 dca-channel bandwidth

14.2.16 dca-channel channel-set

14.1.118 display ssid-profile

Function

The **display ssid-profile** command displays configuration and reference information about an SSID profile.

Format

display ssid-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all SSID profiles.	-
name *profile-name*	Displays information about a specified SSID profile.	The SSID profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display ssid-profile** command to view configuration and reference information about an SSID profile.

Example

Display information about all SSID profiles.

```
<Huawei> display ssid-profile all
-------------------------------------------------------
Profile name                Reference
-------------------------------------------------------
default                     1
ssid-profile-1              0
-------------------------------------------------------
Total: 2
```

Table 14-63 Description of the **display ssid-profile all** command output

Item	Description
Profile name	SSID profile name.
Reference	Number of times an SSID profile is referenced.

Display information about the SSID profile **default**.

```
<Huawei> display ssid-profile name default
-----------------------------------------------------------------
Profile ID                  : 0
SSID                        : HUAWEI-WLAN
SSID hide                   : disable
Association timeout(min)    : 5
Max STA number              : 64
Reach max STA SSID hide     : enable
```

```
Legacy station              : enable
DTIM interval               : 1
beacon-2g-rate              : 1
beacon-5g-rate              : 6
deny-broadcast-probe        : disable
probe-response-retry num    : 1
Active dull client          : disable
-----------------------------------------------------------------
WMM EDCA client parameters:
-----------------------------------------------------------------
      ECWmax  ECWmin  AIFSN  TXOPLimit
AC_VO  3       2       2      47
AC_VI  4       3       2      94
AC_BE  10      4       3      0
AC_BK  10      4       7      0
-----------------------------------------------------------------
```

Table 14-64 Description of the **display ssid-profile name** command output

Item	Description
Profile ID	ID of an SSID profile.
SSID	SSID name. To configure the parameter, run the **14.1.214 ssid** command.
SSID hide	SSID hiding. To configure the parameter, run the **14.1.215 ssid-hide enable** command.
Association timeout(min)	Association timeout period. To configure the parameter, run the **14.1.43 association-timeout** command.
Max STA number	Maximum number of users. To configure the parameter, run the **14.1.170 max-sta-number (SSID profile view)** command.
Reach max STA SSID hide	Whether to automatically hide SSIDs when the number of users reaches the maximum. To configure the parameter, run the **14.1.191 reach-max-sta hide-ssid disable** command.
Legacy station	Whether to permit access of legacy terminals. To configure the parameter, run the **14.1.158 legacy-station disable** command.
DTIM interval	DTIM interval. To configure the parameter, run the **14.1.135 dtim-interval** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
beacon-2g-rate	Rate at which 2.4 GHz Beacon frames are sent. To configure the parameter, run the **14.1.44 beacon-2g-rate** command.
beacon-5g-rate	Rate at which 5 GHz Beacon frames are sent. To configure the parameter, run the **14.1.45 beacon-5g-rate** command.
deny-broadcast-probe	Whether an AP is configured not to respond to broadcast Probe Request frames. To configure the parameter, run the **14.1.65 deny-broadcast-probe enable** command.
probe-response-retry num	Number of times Probe Response packets are retransmitted. To configure the parameter, run the **14.1.181 probe-response-retry** command.
Active dull client	Whether the function of preventing terminals from entering energy-saving mode is enabled. To configure the parameter, run the **14.1.4 active-dull-client enable** command.
AC_VO	AC_VO packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_VI	AC_VI packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BE	AC_BE packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AC_BK	AC_BK packets. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ECWmax	Exponent form of the maximum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
ECWmin	Exponent form of the minimum contention window. ECWmin and ECWmax determine the average backoff time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
AIFSN	Arbitration inter frame spacing number (AIFSN), which determines the channel idle time. To configure the parameter, run the **14.1.244 wmm edca-ap** command.
TXOPLimit	Transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an STA can occupy a channel. A larger value indicates a longer duration. To configure the parameter, run the **14.1.244 wmm edca-ap** command.

14.1.119 display station

Function

The **display station** command displays STA access information.

Format

display station { **ap-group** *ap-group-name* | **ap-name** *ap-name* | **ap-id** *ap-id* | **ssid** *ssid* | **sta-mac** *sta-mac-address* | **vlan** *vlan-id* | **all** }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays STA access information about a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays STA access information of the AP with a specified name.	The AP name must exist.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ap-id *ap-id*	Displays STA access information of the AP with a specified ID.	The AP ID must exist.
ssid *ssid*	Displays STA access information about a specified SSID.	The SSID must exist.
sta-mac *sta-mac-address*	Displays access information about a STA with the specified MAC address.	The STA's MAC address must exist.
vlan *vlan-id*	Displays STA access information about a specified VLAN.	The VLAN ID must exist.
all	Displays access information about all STAs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display station** command to view STA access information.

Example

Display access information about all STAs.

```
<Huawei> display station all
Rf/WLAN: Radio ID/WLAN ID
Rx/Tx: link receive rate/link transmit rate(Mbps)
-----------------------------------------------------------------------------------------------------------------------------
-
STA MAC          AP ID AP name  Rf/WLAN  Band  Type  Rx/Tx     RSSI  VLAN  IPv4 address   SSID       IPv6
address
-----------------------------------------------------------------------------------------------------------------------------
-
84db-ac68-2017   0     area_1   0/1      2.4G  11n   64/64     -50   100   192.168.20.173 wlan-net
FE80::86DB:ACFF:FE68:2017
b863-4d02-c617   0     area_1   1/1      5G    11n   97/114    -38   100   192.168.20.31  wlan-net5g
FE80::4:F75D:620C:FA02
-----------------------------------------------------------------------------------------------------------------------------
-
Total: 2 2.4G: 1 5G: 1
```

Table 14-65 Description of the **display station all** command output

Item	Description
STA MAC	STA's MAC address.

Item	Description
AP ID	AP ID.
AP name	AP name.
Rf/WLAN	Radio ID/WLAN ID of a VAP.
Band	Frequency band of a radio.
Type	Protocol type of a radio.
Rx/Tx	Rate at which the AP receives packets from the STA/Rate at which the AP sends packets to the STA.
RSSI	RSSI of a STA.
VLAN	VLAN ID of a STA.
IPv4 address	IPv4 address of a STA.
SSID	SSID name.
IPv6 address	IPv6 address of a STA.

Display access information about a specified STA.

```
<Huawei> display station sta-mac b878-2eb4-2689
-------------------------------------------------------------------------------
Station MAC-address                        : b878-2eb4-2689
Station IP-address                         : 2.2.2.1
                                           : FE80::C87:23F4:A6D:8D03
Station gateway                            : 2.2.2.2
Associated SSID                            : jsldoc
Station online time(ddd:hh:mm:ss)          : 000:00:03:14
The upstream SNR(dB)                       : 80.0
The upstream aggregate receive power(dBm) : -28.0
Station connect rate(Mbps)                 : 61
Station connect channel                    : 36
Station inactivity time(ddd:hh:mm:ss)      : 000:00:00:00
Station current state
  Authorized for data transfer             : YES
  QoS enabled                              : YES
  ERP enabled                              : No
  HT rates enabled                         : YES
  Power save mode enabled                  : YES
  Auth reference held                      : No
  This is an ATH node                      : No
  WDS workaround req                       : No
  WDS link                                 : No
  PMF negotiation                          : No
Station's HT capability                    : WQ
Station ERP element                        : 0
Station capabilities                       : E
Station PMF capabilities                   : PMFC=0,PMFR=0
Station VHT capabilities
  256QAM capabilities                      :No
  VHT Explicit Beamforming capabilities   :No
Station's RSSI(dBm)                        : -28
Station's Noise(dBm)                       : -108
Station's radio mode                       : 11n
Station's AP Name                          : area_3
```

```
Station's Radio ID                      : 1
Station's Authentication Method           : OPEN
Station's Cipher Type                    : NO CIPHER
Station's User Name                       : b8782eb42689
Station's Vlan ID                       : 22
Station's Channel Band-width              : 20MHz
Station's asso BSSID                     : dcd2-fc04-b513
Station's state                        : Asso with auth
Station's QoS Mode                        : WMM
Station's HT Mode                        : HT20
Station's MCS value                      : 7
Station's Short GI                      : nonsupport
Station's roam state                     : No
Station supported band                    : Dual Band
Station support 802.11k                  : Yes
Station support 802.11v                  : No
Available to trigger roam                : Yes
Is sticky client now                    : No
Trigger aimless roam while sticky         : Yes
Neighbor list:
-----------------------------------------
AP name            RfID  SNR     RCPI
-----------------------------------------
-----------------------------------------
--------------------------------------------------------------------------------
```

Table 14-66 Description of the **display station sta-mac** *sta-mac-address* command output

Item	Description
Station MAC-address	MAC address of a STA.
Station IP-address	IP address of a STA.
Station gateway	Gateway address of a STA. **NOTE** If the device obtains the STA's gateway address through DHCP, the parameter displays as the obtained gateway address; otherwise, the parameter displays as 0.0.0.0.
Associated SSID	SSID of a service set with which a STA is associated.
Station online time(ddd:hh:mm:ss)	Online duration of a STA, in the format of ddd:hh:mm:ss.
The upstream SNR(dB)	Upstream signal noise ratio of a STA, in dB.
The upstream aggregate receive power(dBm)	Upstream receive power of a STA, in dBm.
Station connect rate(Mbps)	Connection rate of a STA, in Mbit/s.
Station connect channel	Channel used by a STA.
Station inactivity time(ddd:hh:mm:ss)	Idle duration of a STA, in the format of ddd:hh:mm:ss.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Station current state	Current status of a STA.
Authorized for data transfer	Whether a STA is authenticated.
QoS enabled	Whether QoS is enabled on a STA.
ERP enabled	Whether Effective radiated power (ERP) is enabled on a STA to increase the physical-layer transmission speed.
HT rates enabled	Whether 802.11n is enabled on a STA.
Power save mode enabled	Whether the power saving mode is enabled on a STA.
Auth reference held	Whether the authentication reference flag is set.
This is an ATH node	Whether the wireless network adapter uses the atheros chip.
WDS workaround req	Whether a patch is used to fix bugs of atheros owl series chips in WDS scenarios.
WDS link	STA that is a node on the WDS link.
PMF negotiation	Whether a STA implements the PMF negotiation.
Station's HT capability	HT capability of a STA.
Station ERP element	ERP of a STA, in dBm.
Station capabilities	Capabilities of a STA.
Station PMF capabilities	PMF capability of a STA.
Station VHT capabilities	VHT capability of a STA.
256QAM capabilities	Whether a STA supports 802.11ac.
VHT Explicit Beamforming capabilities	Whether a STA supports 802.11ac explicit Beamforming.
Station's RSSI(dBm)	Received signal strength indicator (RSSI) of a STA, in dBm.
Station's Noise(dBm)	Interference signal strength of a STA, in dBm.
Station's radio mode	Radio mode of a STA.
Station's AP Name	Name of the AP which a STA associates with.
Station's Radio ID	Radio ID of a STA.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Station's Authentication Method	Authentication mode of a STA.
Station's Cipher Type	Encryption mode of a STA.
Station's User Name	User name of a STA.
Station's Vlan ID	VLAN ID of a STA.
Station's Channel Band-width	Channel bandwidth of a STA.
Station's asso BSSID	BSSID that the STA associates with.
Station's state	Status of the STA.
Station's QoS Mode	QoS mode of the STA.
Station's HT Mode	HT mode of the STA.
Station's MCS value	MCS value of the STA.
Station's Short GI	Whether the STA supports the short GI.
Station's roam state	Roaming state of a STA.
Station supported band	Bandwidth supported by a STA.
Station support 802.11k	Whether a STA supports 802.11k.
Station support 802.11v	Whether a STA supports 802.11v.
Available to trigger roam	Whether a STA can trigger the roaming process.
Is sticky client now	Whether a STA is a sticky terminal.
Trigger aimless roam while sticky	Whether a STA is forced to roam aimlessly.
Neighbor list	Neighboring AP list of a STA.
AP name	Name of a STA's neighboring AP.
RfID	Radio ID of a STA's neighboring AP.
SNR	SNR of a STA's neighboring AP.
RCPI	RCPI of a STA's neighboring AP.

14.1.120 display station assoc-info ap-offline-record

Function

The **display station assoc-info ap-offline-record** command displays information about STAs that connect to the APs in fault state.

Format

display station assoc-info ap-offline-record { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Displays information about STAs that connect to all APs in fault state.	-
ap-name *ap-name*	Displays information about STAs that go online on the AP with a specified name in fault state.	The AP name must exist.
ap-id *ap-id*	Displays information about STAs that go online on the AP with a specified ID in fault state.	The AP ID must exist.
radio *radio-id*	Displays information about STAs that connect to a specified radio of an AP in fault state.	The radio ID must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When link faults occur between the APs and AC, the APs in fault state allow access of new STAs and log the STA information. When the link between the APs and AC is re-established, the APs disconnect these STAs and send the STA information to the AC. You can run the **display station assoc-info ap-offline-record** command on the AC to check information about the STAs that connect to the APs in fault state.

Example

Display information about STAs that connect to all APs in fault state.

```
<Huawei> display station assoc-info ap-offline-record all
Offline Station information list:
-------------------------------------------------------------------------------
STA MAC          AP name   RADIO ID  SSID
-------------------------------------------------------------------------------
286E-D488-B74F   Huawei    0         SSID_MYWLAN
-------------------------------------------------------------------------------
Total: 1
```

Table 14-67 Description of the **display station assoc-info ap-offline-record** command output

Item	Description
STA MAC	MAC address of a STA.
AP name	Name of the AP that the STA connects to.
RADIO ID	ID of the radio that the STA connects to.
SSID	SSID that the STA connects to.

Related Topics

14.1.200 reset station assoc-info ap-offline-record

14.1.121 display station online-fail-record

Function

The **display station online-fail-record** command displays STA online failure records.

Format

display station online-fail-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac-address* }

Parameters

Parameter	Description	Value
all	Displays online failure records of all STAs.	-
ap-name *ap-name*	Displays online failure records of STAs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays online failure records of STAs on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac-address*	Displays online failure records of the STA with the specified MAC address.	The STA's MAC address must exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

If a STA fails to go online, you can run the command to check the failure reason, which helps locate the fault.

After the number of STA online failure records reaches the maximum that can be stored, new records overwrite existing ones.

Example

Displays online failure records of all STAs.

```
<Huawei> display station online-fail-record all
Rf/WLAN: Radio ID/WLAN ID
-------------------------------------------------------------------------------
STA MAC         AP ID Ap name  Rf/WLAN    Last record time
                Reason
-------------------------------------------------------------------------------
14cf-9202-13dc  0     area_11  0/1       2015-03-11/15:53:18
                The STA is in the VAP's blacklist.
-------------------------------------------------------------------------------
Total stations: 1 Total records: 1
```

Table 14-68 Description of the **display station online-fail-record** command output

Item	Description
Radio ID/WLAN ID	Radio/VAP that the STA fails to connect to.
STA MAC	MAC address of the STA that fails to go online.
AP ID	ID of the AP on which the STA fails to go online.
Ap name	Name of the AP on which the STA fails to go online.
Last record time	Time of the STA online failure.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reason	Reason for the STA online failure. ● A user has gone offline unexpectedly. ● STA association request error. ● Incorrect encryption mode. ● The STA needs to send an authentication request before associating with the network. ● The authentication request is not approved. ● The AP does not support the rate set specified in the association request packet of the STA. ● Incorrect encryption mode in the authentication frame. ● Failed to decrypt the challenge packet. ● The radio mode does not match. ● The number of STAs exceeds the maximum allowed by the AP. ● The terminal capability set does not match the capabilities configured for the VAP. The WMM capabilities do not match. ● The terminal capability set does not match the capabilities configured for the VAP. The network type flag carried by the terminal is incorrect. ● The terminal capability set does not match the capabilities configured for the VAP. The terminal does not support short slot time. ● The terminal capability set does not match the capabilities configured for the VAP. In the 802.11h only mode, the terminal does not support dynamic frequency selection. ● The number of associated STAs exceeds the maximum allowed by the AC. ● The STA is not in the global whitelist. ● The STA is in the global blacklist.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• The STA is not in the VAP's whitelist. • The STA is in the VAP's blacklist. • The STA is in the dynamic blacklist. • The association or reassociation packet check fails. • The number of users exceeds the maximum allowed on the VAP. • The STA uses a static IP address. • The STA's SNR is below the specified threshold. • The number of STAs of the radio has reached the upper threshold. • The channel utilization of the radio has reached the upper threshold. • The number of STAs exceeds the maximum allowed by the radio. • The number of STAs exceeds the maximum allowed in the VAP. • Failed to decrypt the challenge packet. • The key is incorrect or the STA uses the cached PMK. • Time to wait for the STA's handshake packet (2/4) expires. • Time to wait for the STA's handshake packet (4/4) expires. • WAPI authentication times out. • Authentication fails. • Reauthentication fails.

Related Topics

14.1.202 reset station online-fail-record

14.1.122 display station offline-record

Function

The **display station offline-record** command displays STA offline records.

Format

display station offline-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac* }

Parameters

Parameter	Description	Value
all	Displays all STA offline records.	-
ap-name *ap-name*	Displays STA offline records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays STA offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Displays logout records of a specified STA.	The STA's MAC address must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a STA goes offline, you can use this command to check the reason why the STA goes offline.

Example

Display all STA offline records.

```
<Huawei> display station offline-record all
Rf/WLAN: Radio ID/WLAN ID
--------------------------------------------------------------------------------
STA MAC         AP ID Ap name        Rf/WLAN    Last record time
                Reason
--------------------------------------------------------------------------------
14cf-9208-9abf  0     area_1         0/2        2015-09-18/09:38:50
                The VAP goes down because the configuration is modified.
14cf-9202-13dc  1     60de-4474-9640 0/1        2015-09-18/09:28:52
                The VAP goes down because the configuration is modified.
--------------------------------------------------------------------------------
Total stations: 2 Total records: 2
```

Table 14-69 Description of the **display station offline-record** command output

Item	Description
STA MAC	MAC address of a STA.
AP ID	AP ID.

Item	Description
Ap name	AP name.
Radio ID/WLAN ID	ID of the radio or WLAN ID of the VAP from which a STA goes offline.
Last record time	Time when the STA went offline last time.
Reason	Reason why the STA went offline.
Total stations	Total number of STAs.
Total records	Total number of STA offline records.

Related Topics

14.1.201 reset station offline-record

14.1.123 display station statistics

Function

The **display station statistics** command displays statistics information about STAs.

Format

display station statistics [**sta-mac** *sta-mac-address* | **ap-name** *ap-name* | **ap-id** *ap-id*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Displays statistics information about a STA with a specified MAC address.	The STA's MAC address must exist.
ap-name *ap-name*	Displays statistics information about STAs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays statistics information about STAs on the AP with a specified ID.	The AP ID must exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can run this command to view statistics information about STAs.

- If no parameter is specified, statistics information about all STAs associated with the AC is displayed.
- If an AP is specified, the number of STAs associated with, disassociated from, and reassociated with the AP is displayed.
- If a STA is specified, the number of packets and packet transmission rate between the STA and an AP.

Prerequisites

- To view statistics information about a specified STA, ensure that the STA has been associated with an AP.
- To view statistics information about STAs associated with a specified AP, ensure that the AP has been added to the AC and is in normal state.

Example

Display statistics information about all STAs.

```
<Huawei> display station statistics
-------------------------------------------------------------------------------
  AC auth successful                                    :0
  AC roaming                                           :0
  AC auth failed because of password error                      :0
  AC auth failed because of invalid calc                      :0
  AC auth failed because of timeout                           :0
  AC auth failed because of being refused                       :0
  AC auth failed because of other reasons                       :0
  Sticky clients detected                               :0
  Stations supporting dual band                             :0
  Online stations                                      :0
     Stations associated with 2.4G band                       :0
     Stations associated with 5G band                         :0
-------------------------------------------------------------------------------
```

Table 14-70 Description of the **display station statistics** command output

Item	Description
AC auth successful	Total number of successful link authentications on the AC. Every time a STA initiates a link authentication request and passes the authentication, the counter is incremented by 1. If the same STA initiates multiple authentication requests and passes all authentications, the counter is incremented cumulatively.
AC roaming	Total number of times that roaming occurs on the AC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AC auth failed because of password error	Number of STAs that fail to be authenticated due to incorrect passwords.
AC auth failed because of invalid calc	Number of STAs that fail to be authenticated due to an invalid authentication algorithm.
AC auth failed because of timeout	Number of STAs that fail to be authenticated due to timeout.
AC auth failed because of being refused	Number of STAs that fail to be authenticated because the AC rejects the associate requests.
AC auth failed because of other reasons	Number of STAs that fail to be authenticated due to other reasons.
Sticky clients detected	Number of sticky STAs.
Stations supporting dual band	Number of STAs that support only dual bands.
Online stations	Number of online STAs.
Stations associated with 2.4G band	Number of STAs associated with the 2.4 GHz band.
Stations associated with 5G band	Number of STAs associated with the 5 GHz band.

Display statistics information about a STA with MAC address 0025-86aa-0d1c.

```
<Huawei> display station statistics sta-mac 0025-86aa-0d1c
-----------------------------------------------------------------
  Packets sent to the station                          : 7
  Packets received from the station                    : 40
  Bytes sent to the station                            : 1170
  Bytes received from the station                      : 3911
  Wireless data rate sent to the station(kbps)         : 0
  Wireless data rate received from the station(kbps)   : 0
  STA power save percent                               : 0%
-----------------------------------------------------------------------------
```

Table 14-71 Description of the **display station statistics sta-mac** *sta-mac-address* command output

Item	Description
Packets sent to the station	Number of packets sent to the STA.
Packets received from the station	Number of packets sent by the STA.
Bytes sent to the station	Number of bytes sent to the STA.
Bytes received from the station	Number of bytes sent by the STA.

Item	Description
Wireless data rate sent to the station(kbps)	Rate at which packets are sent to the STA, in kbit/s.
Wireless data rate received from the station(kbps)	Rate at which packets are received from the STA, in kbit/s.
STA power save percent	Percentage of power saved on the STA.

Display STA statistics information of a specified AP.

```
<Huawei> display station statistics ap-name N1-2
-------------------------------------------------------------------------------
  Total stations online time(seconds)                          :2713
  Stations associated with the AP                              :1
  Association request                                          :5
  Successful association request                               :5
  Reject association request                                   :0
  Failed association request                                   :0
  Reassociation request                                        :0
  Successful reassociation request                             :0
  Reject reassociation request                                 :0
  Failed reassociation request                                 :0
  Disassociations because of users notified                    :3
  Disassociations because of users roam                        :0
  Disassociations because of users left without notification   :0
  Disassociations because of other reasons                     :0
  Disassociations because of linkauthfail                      :0
  Authentication request                                       :5
  Deauth request                                               :0
  Average rate of all stations(kbps)                           :63476
  Stations work in power save mode                             :0
  Stations work in HT mode                                     :1
  Stations work in B mode                                      :0
  Stations work in G mode                                      :0
  Stations work in A mode                                      :0
  Stations work in N mode                                      :1
  Stations work in AC mode                                     :0
  Stations only support 2.4G band                              :1
  Stations only support 5G band                                :0
  Stations support dual band                                   :0
     Stations associated with 2.4G band                        :1
     Stations associated with 5G band                          :0
  Load balancing status between dual band                      :Balanced
  Detected as sticky clients                                   :0
  Online stations                                              :0
-------------------------------------------------------------------------------
```

Table 14-72 Description of the **display station statistics ap-name** *ap-name* command output

Item	Description
Total stations online time(seconds)	Total online duration of all STAs, in seconds.
Stations associated with the AP	Number of STAs currently associated with the AP, not including the number of STAs in aging status.

Item	Description
Association request	Number of association requests sent to the AP.
Successful association request	Number of successful associations.
Reject association request	Number of association requests denied by the AP.
Failed association request	Number of failed associations.
Reassociation request	Number of reassociation requests sent to the AP.
Successful reassociation request	Number of successful reassociations.
Reject reassociation request	Number of reassociation requests rejected by the AP.
Failed reassociation request	Number of failed reassociations.
Disassociations because of users notified	Number of times STAs are disassociated from the AP because users go offline.
Disassociations because of users roam	Number of times STAs are disassociated from the AP because users roam to other regions.
Disassociations because of users left without notification	Number of times STAs are disassociated from the AP because users go offline abnormally.
Disassociations because of other reasons	Number of times STAs are disassociated from the AP for other reasons.
Disassociations because of linkauthfail	Number of times STAs are disassociated from the AP due to link authentication failures.
Authentication request	Number of link authentication request times.
Deauth request	Number of disassociation times.
Average rate of all stations(kbps)	Average rate of all STAs, in kbit/s.
Stations work in power save mode	Number of STAs working in power saving mode.
Stations work in HT mode	Number of STAs working in HT mode.
Stations work in B mode	Number of STAs working in 802.11b mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Stations work in G mode	Number of STAs working in 802.11g mode.
Stations work in A mode	Number of STAs working in 802.11a mode.
Stations work in N mode	Number of STAs working in 802.11n mode.
Stations work in AC mode	Number of STAs working in 802.11ac mode.
Stations only support 2.4G band	Number of STAs that support only the 2.4 GHz frequency band.
Stations only support 5G band	Number of STAs that support only the 5 GHz frequency band.
Stations support dual band	Number of STAs that support both 2.4 GHz and 5 GHz frequency bands.
Stations associated with 2.4G band	Number of STAs that associate with the 2.4 GHz frequency band.
Stations associated with 5G band	Number of STAs that associate with the 5 GHz frequency band.
Load balancing status between dual band	Status of load balancing between the 2.4 GHz and 5 GHz frequency bands.
Detected as sticky clients	Number of the detected sticky terminals.
Online stations	Number of online STAs.

14.1.124 display traffic-profile

Function

The **display traffic-profile** command displays configuration information about a traffic profile.

Format

display traffic-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays configuration information about all traffic profiles.	-
name *profile-name*	Displays configuration information about a specified traffic profile.	The value is a string of 1 to 35 characters without spaces and question marks (?). It cannot begin or end with double quotation marks (" ").

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display traffic-profile** command to check default configurations of a new traffic profile or configurations of an existing traffic profile.

Example

The user priority of 802.11e packets is mapped to DSCP priority in the CAPWAP header when packets are sent from an AP to an AC.

```
<Huawei> display traffic-profile name p1
-------------------------------------------------------
Profile ID                    : 1
Priority map downstream trust : DSCP
User isolate mode             : disable
Rate limit client up(Kbps)    : 4294967295
Rate limit client down(Kbps)  : 4294967295
Rate limit VAP up(Kbps)       : 4294967295
Rate limit VAP down(Kbps)     : 4294967295
Traffic optimize sta bridge forward : enable
IGMP snooping                 : enable
IGMP snooping report suppress : disable
Traffic optimize broadcast suppression(pps): -
Traffic optimize multicast suppression(pps): -
Traffic optimize unicast suppression(pps): -
Traffic optimize multicast to unicast: disable
Priority map upstream trust   : 8021e
CAPWAP priority upstream map mode: 802.11e map DSCP
                              0 map 0
                              1 map 8
                              2 map 16
                              3 map 24
                              4 map 32
                              5 map 40
```

```
                                6 map 48
                                7 map 56
WMM priority downstream map mode: DSCP map 802.11e
                               0-7 map 0
                               8-15 map 1
                               16-23 map 2
                               24-31 map 3
                               32-39 map 4
                               40-47 map 5
                               48-55 map 6
                               56-63 map 7
-----------------------------------------------------
```

The DSCP priority of 802.11e packets is mapped to the user priority of tunnel packets when packets are sent to APs.

```
<Huawei> display traffic-profile name p1
-----------------------------------------------------
Priority map downstream trust : DSCP
User isolate mode             : disable
Rate limit client up(Kbps)    : 4294967295
Rate limit client down(Kbps)  : 4294967295
Rate limit VAP up(Kbps)       : 4294967295
Rate limit VAP down(Kbps)     : 4294967295
Traffic optimize sta bridge forward : enable
IGMP snooping                 : enable
IGMP snooping report suppress : disable
Traffic optimize broadcast suppression(pps): -
Traffic optimize multicast suppression(pps): -
Traffic optimize unicast suppression(pps): -
Traffic optimize multicast to unicast: disable
Priority map upstream trust   : DSCP
WMM priority downstream map mode: DSCP map 802.11e
                               0-7 map 0
                               8-15 map 1
                               16-23 map 2
                               24-31 map 3
                               32-39 map 4
                               40-47 map 5
                               48-55 map 6
                               56-63 map 7
priority upstream map mode: DSCP map DSCP
                          0 map 0
                          1 map 1
                          2 map 2
                          3 map 3
                          4 map 4
                          5 map 5
                          6 map 6
                          7 map 7
                          8 map 8
                          9 map 9
                          10 map 10
                          11 map 11
                          12 map 12
                          13 map 13
                          14 map 14
                          15 map 15
                          16 map 16
                          17 map 17
                          18 map 18
                          19 map 19
                          20 map 20
                          21 map 21
                          22 map 22
                          23 map 23
                          24 map 24
                          25 map 25
                          26 map 26
                          27 map 27
```

```
                    28 map 28
                    29 map 29
                    30 map 30
                    31 map 31
                    32 map 32
                    33 map 33
                    34 map 34
                    35 map 35
                    36 map 36
                    37 map 37
                    38 map 38
                    39 map 39
                    40 map 40
                    41 map 41
                    42 map 42
                    43 map 43
                    44 map 44
                    45 map 45
                    46 map 46
                    47 map 47
                    48 map 48
                    49 map 49
                    50 map 50
                    51 map 51
                    52 map 52
                    53 map 53
                    54 map 54
                    55 map 55
                    56 map 56
                    57 map 57
                    58 map 58
                    59 map 59
                    60 map 60
                    61 map 61
                    62 map 62
                    63 map 63
--------------------------------------------------
```

Table 14-73 Description of the **display traffic-profile** command output

Item	Description
Profile ID	Traffic profile ID
Priority map downstream trust	Mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11e user priority when 802.3 packets are sent to an AP from upper-layer devices. To configure the parameter, run the **14.1.177 priority-map downstream trust** command.
User isolate mode	User isolation. To configure the parameter, run the **14.5.14 user-isolate (traffic profile view)** command.
Rate limit client up(Kbps)	Indicates upstream rate limit configured for STAs. To configure the parameter, run the **14.1.190 rate-limit** command.

Item	Description
Rate limit client down(Kbps)	Indicates downstream rate limit configured for STAs. To configure the parameter, run the **14.1.190 rate-limit** command.
Rate limit VAP up(Kbps)	Indicates upstream rate limit configured for VAPs. To configure the parameter, run the **14.1.190 rate-limit** command.
Rate limit VAP down(Kbps)	Indicates downstream rate limit configured for VAPs. To configure the parameter, run the **14.1.190 rate-limit** command.
Traffic optimize sta bridge forward	Function of forbidding STA bridging packet forwarding.
IGMP snooping	IGMP snooping.
IGMP snooping report suppress	IGMP message suppression time.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume allowed on an interface. To configure the parameter, run the **14.1.223 traffic-optimize broadcast-suppression** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume allowed on an interface. To configure the parameter, run the **14.1.224 traffic-optimize multicast-suppression** command.
Traffic optimize unicast suppression(pps)	Maximum unicast traffic volume allowed on an interface. To configure the parameter, run the **14.1.227 traffic-optimize unicast-suppression** command.
Traffic optimize multicast to unicast	Function of converting multicast packets to unicast packets. To configure the parameter, run the **14.1.225 traffic-optimize multicast-unicast enable** command.
CAPWAP priority upstream map mode	Mapping from WMM to the DSCP priority of the upstream CAPWAP tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Priority map upstream trust	Mapping from the 802.11e user priority or DSCP priority of 802.3 packets to the user priority of tunnel packets. To configure the parameter, run the **14.1.180 priority-map tunnel-upstream trust** command.
WMM priority downstream map mode	Mapping from the DSCP priority to the WMM of downstream packets.

Display configurations of all traffic profiles.

```
<Huawei> display traffic-profile all
-----------------------------------------------------
Profile name                    Reference
-----------------------------------------------------
default                          3
1                               1
p1                               0
-----------------------------------------------------
Total: 3
```

Table 14-74 Description of the **display traffic-profile all** command output

Item	Description
Profile name	Profile name. To configure the parameter, run the **14.1.229 traffic-profile (WLAN view)** command.
Reference	Number of times a location profile is referenced.

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.125 display vap

Function

The **display vap** command displays information about service VAPs.

Format

display vap { **ap-group** *ap-group-name* | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } [**ssid** *ssid*]

display vap { **all** | **ssid** *ssid* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all service VAPs in a specified AP group.	The AP group must exist.
ap-name *ap-name*	Displays information about service VAPs on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Displays information about service VAPs on the AP with a specified ID.	The AP ID must exist.
radio *radio-id*	Displays information about service VAPs of a specified AP radio.	The value is an integer that ranges from 0 to 2.
ssid *ssid*	Displays information about service VAPs of a specified SSID.	The SSID must exist.
all	Displays information about all service VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vap** command to view information about service VAPs.

Example

Display information about all service VAPs.

```
<Huawei> display vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name       RfID WID  BSSID          Status  Auth type  STA   SSID
--------------------------------------------------------------------------------
3     ap1           0    1    0023-0024-0080 ON      Open       0     ag
--------------------------------------------------------------------------------
Total: 1
```

Table 14-75 Description of the **display vap** command output

Item	Description
AP ID	AP ID.

Item	Description
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
SSID	SSID name.
BSSID	MAC address of a VAP.
Status	Current status of a VAP. ● ON: The VAP service is enabled. ● OFF: The VAP service is disabled.
Auth type	Authentication mode of a VAP.
STA	Number of terminals connected to a VAP.

14.1.126 display vap create-fail-record

Function

The **display vap create-fail-record** command displays records about VAP creation failures.

Format

display vap create-fail-record { **ap-mac** *ap-mac* | **all** }

Parameters

Parameter	Description	Value
ap-mac *ap-mac*	Displays records about VAP creation failures on an AP with the specified MAC address.	The specified MAC address must exist.
all	Displays records about VAP creation failures on an AP with the specified MAC address.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vap create-fail-record all** command to check records about VAP creation failures.

Example

Display all records about VAP creation failures.

```
<Huawei> display vap create-fail-record all
Rf/WLAN: Radio ID/WLAN ID
--------------------------------------------------------------------------------
AP MAC          Rf/WLAN  Profile Name  Source Type  Source Name
VAP Type        Reason
--------------------------------------------------------------------------------
e468-a350-8a60  0/4      1             ap-group     default
Service         Preshared key is not configured.
e468-a350-8a60  1/4      1             ap-group     default
Service         Preshared key is not configured.
e468-a350-8a60  0/6      1             ap-group     1
Service         Preshared key is not configured.
e468-a350-8a60  1/6      1             ap-group     1
Service         Preshared key is not configured.
--------------------------------------------------------------------------------
Total records: 4
```

Table 14-76 Description of the **display vap create-fail-record all** command output

Item	Description
AP MAC	MAC address of the AP.
Rf/WLAN	Radio ID/WLAN ID.
Profile Name	VAP profile name.
Source Type	Object to which the VAP is bound, including: ● ap-group: AP group ● ap-id: AP
Source Name	Name of the object to which the VAP is bound.
VAP Type	VAP type, including ● Service: Service VAP ● WDS: WDS VAP
Reason	Reason why the VAP fails to be created.

 Copyright © Huawei Technologies Co., Ltd.

14.1.127 display vap-profile

Function

The **display vap-profile** command displays configuration and reference information about a VAP profile.

Format

display vap-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all VAP profiles.	-
name *profile-name*	Displays information about a specified VAP profile.	The VAP profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vap-profile** command to view configuration and reference information about a VAP profile.

Example

Display information about all VAP profiles.

```
<Huawei> display vap-profile all
-------------------------------------------------------
Profile name                Reference
-------------------------------------------------------
default                     1
vap-profile-1               0
-------------------------------------------------------
Total: 2
```

Table 14-77 Description of the **display vap-profile all** command output

Item	Description
Profile name	VAP profile name.

Item	Description
Reference	Number of times a VAP profile is referenced.

Display information about the VAP profile **default**.

```
<Huawei> display vap-profile name default
-------------------------------------------------------------------------------
Type                          : service
Forward mode                  : direct-forward
Offline management            : disable
Service VLAN ID               : 1
Learn client address          : enable
Learn client DHCP strict      : disable
Learn client DHCP blacklist   : disable
IP source check               : disable
DHCP trust port               : disable
SSID profile                  : default
Security profile              : default
Traffic profile               : default
Authentication profile        :
-------------------------------------------------------------------------------
```

Table 14-78 Description of the **display vap-profile name** *profile-name* command output

Item	Description
Type	VAP type. ● service: indicates the service type. ● ap-management: indicates the management AP type. To configure the parameter, run the **14.1.230 type (VAP profile view)** command.
Forward mode	Data forwarding mode. ● direct-forward: Indicates direct forwarding. ● tunnel: Indicates tunnel forwarding. To configure the parameter, run the **14.1.142 forward-mode** command.
Offline management	Whether to enable management VAP and antenna alignment VAP for offline APs. To configure the parameter, run the **14.1.221 temporary-management enable (VAP profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Service VLAN ID	Service VLAN ID. To configure the parameter, run the **14.1.208 service-vlan** command.
Learn client address	Status of STA address learning. To configure the parameter, run the **14.1.155 learn-client-address disable** command.
Learn client DHCP strict	Status of strict STA IP address learning through DHCP. To configure the parameter, run the **14.1.154 learn-client-address dhcp-strict** command.
Learn client DHCP blacklist	Whether to add STAs with bogus IP addresses to a dynamic blacklist. To configure the parameter, run the **14.1.154 learn-client-address dhcp-strict** command.
IP source check	Status of IP source guard. To configure the parameter, run the **14.1.150 ip source check user-bind enable** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **14.1.67 dhcp trust port** command.
SSID profile	Name of the SSID profile referenced by a VAP profile. To configure the parameter, run the **14.1.217 ssid-profile (VAP profile view)** command.
Security profile	Name of the security profile referenced by a VAP profile. To configure the parameter, run the **14.4.36 security-profile (VAP profile view)** command.
Traffic profile	Name of the traffic profile referenced by a VAP profile. To configure the parameter, run the **14.1.228 traffic-profile (VAP profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication profile	Name of the authentication profile referenced by a VAP profile.

Related Topics

14.1.233 vap-profile (WLAN view)

14.1.128 display wired-port-profile

Function

The **display wired-port-profile** command displays reference and configuration information about an AP wired port profile.

Format

display wired-port-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all AP wired port profiles.	-
name *profile-name*	Displays information about a specified AP wired port profile.	The AP wired port profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wired-port-profile** command to view configuration and reference information about an AP wired port profile.

Example

Display information about all AP wired port profiles.

```
<Huawei> display wired-port-profile all
-------------------------------------------------------
Profile name                Reference
-------------------------------------------------------
```

```
default                    1
wired-port-profile-1          0
-------------------------------------------------------------
Total: 2
```

Table 14-79 Description of the **display wired-port-profile all** command output

Item	Description
Profile name	Name of an AP wired port profile.
Reference	Number of times an AP wired port profile is referenced.

Display information about the AP wired port profile **default** (Eth-trunk is not configured).

```
<Huawei> display wired-port-profile name default
-----------------------------------------------------------------------------
Port link profile            : default
Description                  :
Port work mode                : -
Port Tagged VLAN              : -
Port untagged VLAN            : 1
Port PVID VLAN                : -
User isolate mode             : disable
DHCP trust port               : enable
IPSG switch                  : disable
DAI switch                   : disable
Learn client address switch   : disable
Traffic optimize broadcast suppression(pps)    : -
Traffic optimize unicast suppression(pps)      : -
Traffic optimize multicast suppression(pps)    : -
-----------------------------------------------------------------------------
```

Display information about the AP wired port profile **dj** (Eth-trunk is configured).

```
<Huawei> display wired-port-profile name dj
-----------------------------------------------------------------------------
Port link profile            : default
Description                  :
Ethernet trunk ID             : 0
-----------------------------------------------------------------------------
```

Table 14-80 Description of the **display wired-port-profile name** *profile-name* command output

Item	Description
Port link profile	Name of the AP wired port link profile referenced by an AP wired port profile. To configure the parameter, run the **14.1.175 port-link-profile (AP wired port profile view)** command.

Item	Description
Description	Interface description. To configure the parameter, run the **14.1.66 description (AP wired port profile view)** command.
Port work mode	Working mode of a wired interface. ● root: indicates the root mode. ● endpoint: indicates the endpoint mode. ● middle: indicates the middle mode. ● -: indicates that the working mode of wired interfaces is not changed. To configure the parameter, run the **14.5.8 mode (AP wired port profile view)** command.
Port Tagged VLAN	VLAN to which a wired interface is added in tagged mode. To configure the parameter, run the **14.5.17 vlan (AP wired port profile view)** command.
Port untagged VLAN	VLAN to which a wired interface is added in untagged mode. To configure the parameter, run the **14.5.17 vlan (AP wired port profile view)** command.
Port PVID VLAN	PVID of a wired interface. To configure the parameter, run the **14.5.17 vlan (AP wired port profile view)** command.
User isolate mode	User isolation status on a wired interface. To configure the parameter, run the **14.5.13 user-isolate (AP wired port profile view)** command.
DHCP trust port	Status of the DHCP trusted interface function. To configure the parameter, run the **14.1.67 dhcp trust port** command.
Ethernet trunk ID	ID of the Eth-Trunk interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IPSG switch	Whether IP source guard (IPSG) is enabled on an AP's wired interface. To configure the parameter, run the **14.1.151 ipsg enable (AP wired port profile view)** command.
DAI switch	Whether DAI is enabled on an AP's wired interface. To configure the parameter, run the **14.1.68 dai enable (AP wired port profile view)** command.
Learn client address switch	Whether terminal address learning is enabled on an AP's wired interface. To configure the parameter, run the **14.1.156 learn-client-address enable (AP wired port profile view)** command.
Traffic optimize broadcast suppression(pps)	Maximum broadcast traffic volume allowed on an AP's wired interface. To configure the parameter, run the **14.1.222 traffic-optimize (AP wired port profile view)** command.
Traffic optimize unicast suppression(pps)	Maximum unknown unicast traffic volume allowed on an AP's wired interface. To configure the parameter, run the **14.1.222 traffic-optimize (AP wired port profile view)** command.
Traffic optimize multicast suppression(pps)	Maximum multicast traffic volume allowed on an AP's wired interface. To configure the parameter, run the **14.1.222 traffic-optimize (AP wired port profile view)** command.

Related Topics

14.1.240 wired-port-profile (WLAN view)

14.1.129 display wlan config-errors

Function

The **display wlan config-errors** command displays WLAN configuration errors.

Format

display wlan config-errors

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check WLAN configuration errors.

Example

Display WLAN configuration errors.

```
<Huawei> display wlan config-errors
--------------------------------------------------------------------------------
Profile                                  Error
--------------------------------------------------------------------------------
vap-profile 1                              The authentication type specifie
d in the authentication-profile 1 does not match that in the security-profile 1.
--------------------------------------------------------------------------------
Total: 1
```

Table 14-81 Description of the **display wlan config-errors** command output

Item	Description
Profile	Profile name.
Error	Cause of a configuration error.

14.1.130 display workmode wlan

Function

The **display workmode wlan** command displays the current WLAN mode and the configured WLAN mode of a device.

Format

display workmode wlan

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the current WLAN mode and the configured WLAN mode of a device. The configured WLAN mode takes effect after the device is restarted.

Example

Display the current WLAN mode of the device.

```
<Huawei> display workmode wlan
 Wlan Current WorkMode = ap
 Wlan Config WorkMode  = ac
```

Table 14-82 Description of the display workmode wlan command output

Item	Description
Wlan Current WorkMode	Current WLAN mode of a device. ● ap: Fat AP mode ● ac: AC mode
Wlan Config WorkMode	Configured WLAN mode, which takes effect after the device is restarted. ● ap: Fat AP mode ● ac: AC mode

Related Topics

14.1.209 set workmode wlan

14.1.131 dot11a basic-rate

Function

The **dot11a basic-rate** command configures a basic rate set of the 802.11a protocol in a 5G radio profile.

The **undo dot11a basic-rate** command restores the default basic rate set of the 802.11a protocol in a 5G radio profile.

By default, a basic rate set of the 802.11a protocol in a 5G radio profile includes rates 6 Mbps, 12 Mbps, and 24 Mbps.

Format

dot11a basic-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a basic-rate

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies an 802.11a basic rate set.	Enumerated type: ● 6: 6 Mbps ● 9: 9 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all basic rates.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The rates specified in the basic rate set must be supported by both the AP and STA; otherwise, the STA cannot associate with the AP. For example, if you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command to configure a basic rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11a mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

Example

Configure the 802.11a basic rate set to contain rates 6 Mbps and 9 Mbps in the 5G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] dot11a basic-rate 6 9
```

Related Topics

14.1.107 display radio-5g-profile

14.1.132 dot11a supported-rate

14.1.132 dot11a supported-rate

Function

The **dot11a supported-rate** command configures a supported rate set of the 802.11a protocol in a 5G radio profile.

The **undo dot11a supported-rate** command restores the default supported rate set of the 802.11a protocol in a 5G radio profile.

By default, the supported rate set of the 802.11a protocol in a 5G radio profile includes rates 6 Mbps, 9 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.

Format

dot11a supported-rate { *dot11a-rate-value* &<1-8> | **all** }

undo dot11a supported-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dot11a-rate-value	Specifies an 802.11a supported rate set.	Enumerated type: ● 6: 6 Mbps ● 9: 9 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all rates.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP except the basic rates. The AP and STA can transmit data at all rates specified by the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command to configure a supported rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11a mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This configuration applies only to STAs associated with an AP in 802.11a mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

Example

Configure the 802.11a supported rate set to contain rates 6 Mbps and 9 Mbps in the 5G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] dot11a supported-rate 6 9
```

Related Topics

14.1.107 display radio-5g-profile

14.1.131 dot11a basic-rate

14.1.133 dot11bg basic-rate

Function

The **dot11bg basic-rate** command configures a basic rate set of the 802.11bg protocol in a 2G radio profile.

The **undo dot11bg basic-rate** command restores the default basic rate set of the 802.11bg protocol in a 2G radio profile.

By default, the basic rate set of the 802.11bg protocol includes rates 1 Mbps and 2 Mbps in a 2G radio profile.

Format

dot11bg basic-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg basic-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies an 802.11bg basic rate set.	Enumerated type: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all basic rates.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The rates specified in the basic rate set must be supported by both the AP and STA; otherwise, the STA cannot associate with the AP. For example, if you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and deliver the configuration to an AP, only STAs supporting the two rates can associate with the AP. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

After you run this command to configure a basic rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in 802.11bg mode, the STA must support all rates specified by the basic rate set; otherwise, the STA cannot associate with the AP.

Precautions

This configuration applies only to STAs associated with an AP in 802.11bg mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the 802.11bg basic rate set to contain rates 6 Mbps and 9 Mbps in the 2G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] dot11bg basic-rate 6 9
```

Related Topics

14.1.106 display radio-2g-profile

14.1.134 dot11bg supported-rate

14.1.134 dot11bg supported-rate

Function

The **dot11bg supported-rate** command configures a supported rate set of the 802.11bg protocol in a 2G radio profile.

The **undo dot11bg supported-rate** command restores the default supported rate set of the 802.11bg protocol in a 2G radio profile.

By default, the supported rate set of the 802.11bg protocol in a 2G radio profile includes rates 1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, and 54 Mbps.

Format

dot11bg supported-rate { *dot11bg-rate-value* &<1-12> | **all** }

undo dot11bg supported-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dot11bg-rate-value	Specifies an 802.11bg supported rate set.	Enumerated type: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps
all	Supports all rates.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The supported rate set contains rates supported by the AP except the basic rates. The AP and STA can transmit data at all rates specified by the supported rate set. The AP and STA select a rate from the basic rate set or the supported rate set to transmit packets.

When a STA supports rates specified in the basic rate set, the STA can associate with the AP regardless of whether the STA supports rates specified in the supported rate set. In this case, the AP and STA can only select a rate from the basic rate set to transmit packets. For example, assume that you configure the basic rate set to contain rates 6 Mbps and 9 Mbps and the supported rate set to contain rates 48 Mbps and 54 Mbps. After you deliver the configurations to an AP, the STA supporting 6 Mbps and 9 Mbps can associate with the AP, and select either of the two rates to transmit packets with the AP. However, if the STA supports 6 Mbps, 9 Mbps, and 54 Mbps, the STA and AP select any of the three rates to transmit packets after the STA associates with the AP.

After you run this command to configure a supported rate set in a radio profile, bind the radio profile to an AP or AP group. If a STA associates with the AP in

802.11bg mode, the AP and STA select a rate from the basic rate set or supported rate set to transmit packets.

Precautions

This configuration applies only to STAs associated with an AP in 802.11bg mode but does not take effect on STAs associated with the AP in other modes.

The basic rate set and supported rate set cannot be empty simultaneously.

Example

Configure the 802.11bg supported rate set to contain rates 6 Mbps and 9 Mbps in the 2G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] dot11bg supported-rate 6 9
```

Related Topics

14.1.106 display radio-2g-profile
14.1.133 dot11bg basic-rate

14.1.135 dtim-interval

Function

The **dtim-interval** command sets the delivery traffic indication map (DTIM) interval in an SSID profile.

The **undo dtim-interval** command restores the default DTIM interval in an SSID profile.

By default, the DTIM interval is 1.

Format

dtim-interval *dtim-interval*

undo dtim-interval

Parameters

Parameter	Description	Value
dtim-interval	Specifies the DTIM interval.	The value is an integer that ranges from 1 to 255, in Beacons.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

DTIM refers to delivery traffic indication map. After a STA enters the dormancy mode, the associated AP saves the broadcast and multicast frames for the STA. When a Beacon frame sent to the STA by the AP contains DTIM, the saved broadcast and multicast frames will be transmitted to the STA. The DTIM interval refers to the number of Beacon frames sent before the Beacon frame that contains the DTIM. To set the interval for sending Beacon frames in an SSID profile, run the **beacon-interval** command.

- When the STA is in the dormancy status, the AP saves data transmitted to the STA and notifies the STA with a bit in broadcast Beacon frames. The STA receives data according to this bit. You can run this command to set the DTIM interval in the specified SSID profile.
- The DTIM interval specifies how many Beacon frames are sent before the Beacon frame that contains the DITM. A long DTIM interval lengthens the dormancy time of the STA and saves power, but degrades the transmission capability of the STA. A short interval helps transmitting data in a timely manner, but the STA is waken up frequently, causing high power consumption.

Example

Set the DTIM interval to 5 in the SSID profile **ssid1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] dtim-interval 5
```

Related Topics

14.1.118 display ssid-profile

14.1.136 eapol-response dest-address transform-condition

Function

The **eapol-response dest-address transform-condition** command specifies the EAPOL-Response packets to be encapsulated by an AP.

The **undo eapol-response dest-address transform-condition** command restores the default settings.

By default, an AP encapsulates only the EAPOL-Response packets with the destination MAC addresses being the AP's BSSID.

Format

eapol-response dest-address transform-condition { **always** | **equal-bssid** }

undo eapol-response dest-address transform-condition

Parameters

Parameter	Description	Value
always	Configures the AP to encapsulate all EAPOL-Response packets.	-
equal-bssid	Configures the AP to encapsulate only the EAPOL-Response packets with the destination MAC address being the AP's BSSID.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

The destination MAC addresses of the EAPOL-Response packets sent by some STAs are APs' BSSIDs, but the destination MAC addresses of the EAPOL-Response packets sent by other STAs are not APs' BSSIDs. You need to run this command to specify the EAPOL-Response packets to be encapsulated.

Example

Configure the AP to encapsulate all EAPOL-Response packets.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] eapol-response dest-address transform-condition always
```

Related Topics

14.1.98 display ap-system-profile

14.1.137 eapol-response dest-address transform-to

Function

The **eapol-response dest-address transform-to** command configures an AP to encapsulate EAPOL-Response packets into broadcast, multicast, or unicast packets.

The **undo eapol-response dest-address transform-to** command restores the default settings.

 Copyright © Huawei Technologies Co., Ltd.

By default, an AP encapsulates EAPOL-Response packets into unicast packets and actively learns the destination MAC address.

Format

eapol-response dest-address transform-to { **broadcast** | **multicast** | **mac** *mac-address* | **learning** }

undo eapol-response dest-address transform-to

Parameters

Parameter	Description	Value
broadcast	Configures an AP to encapsulate EAPOL-Response packets into broadcast packets.	-
multicast	Configures an AP to encapsulate EAPOL-Response packets into multicast packets.	-
mac *mac-address*	Configures an AP to encapsulate EAPOL-Response packets into unicast packets with a specified destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
learning	Configures an AP to encapsulate EAPOL-Response packets into unicast packets and actively learn the destination MAC address.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

- If the authentication server can only process EAP multicast packets, configure the AP to encapsulate EAPOL-Response packets into multicast packets.
- If the authentication server can only process EAP broadcast packets, configure the AP to encapsulate EAPOL-Response packets into broadcast packets.

 Copyright © Huawei Technologies Co., Ltd.

- If the authentication server can only process EAP unicast packets, configure the AP to encapsulate EAPOL-Response packets into unicast packets. When the AP is configured to encapsulate EAPOL-Response packets into unicast packets, a unicast MAC address must be configured.

Example

Configure an AP to encapsulate EAPOL-Response packets into broadcast packets.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] eapol-response dest-address transform-to broadcast
```

Related Topics

14.1.98 display ap-system-profile

14.1.138 eapol-start dest-address transform-condition

Function

The **eapol-start dest-address transform-condition** command specifies the EAPOL-Start packets to be encapsulated by an AP.

The **undo eapol-start dest-address transform-condition** command restores the default settings.

By default, an AP encapsulates only the EAPOL-Start packets with the destination MAC addresses being the AP's BSSID.

Format

eapol-start dest-address transform-condition { **always** | **equal-bssid** }

undo eapol-start dest-address transform-condition

Parameters

Parameter	Description	Value
always	Configures the AP to encapsulate all EAPOL-Start packets.	-
equal-bssid	Configures the AP to encapsulate only the EAPOL-Start packets with the destination MAC address being the AP's BSSID.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The destination MAC addresses of the EAPOL-Start packets sent by some STAs are APs' BSSIDs, but the destination MAC addresses of the EAPOL-Start packets sent by other STAs are not APs' BSSIDs. You need to run this command to specify the EAPOL-Start packets to be encapsulated.

Precautions

The packet types specified by the **eapol-start dest-address transform-condition** and **14.1.139 eapol-start dest-address transform-to** commands must be the same.

Example

Configure the AP to encapsulate all EAPOL-Start packets.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] eapol-start dest-address transform-condition always
```

Related Topics

14.1.98 display ap-system-profile

14.1.139 eapol-start dest-address transform-to

Function

The **eapol-start dest-address transform-to** command configures an AP to encapsulate EAPOL-Start packets into broadcast, multicast, or unicast packets.

The **undo eapol-start dest-address transform-to** command restores the default settings.

By default, an AP encapsulates EAPOL-Start packets into multicast packets.

Format

eapol-start dest-address transform-to { **broadcast** | **multicast** | **mac** *mac-address* }

undo eapol-start dest-address transform-to

Parameters

Parameter	Description	Value
broadcast	Configures an AP to encapsulate EAPOL-Start packets into broadcast packets.	-
multicast	Configures an AP to encapsulate EAPOL-Start packets into multicast packets.	-
mac *mac-address*	Configures an AP to encapsulate EAPOL-Start packets into unicast packets.	The value is in H-H-H format. An H is a hexadecimal number of four digits.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

- If the authentication server can only process EAP multicast packets, configure the AP to encapsulate EAPOL-Start packets into multicast packets.
- If the authentication server can only process EAP broadcast packets, configure the AP to encapsulate EAPOL-Start packets into broadcast packets.
- If the authentication server can only process EAP unicast packets, configure the AP to encapsulate EAPOL-Start packets into unicast packets. When the AP is configured to encapsulate EAPOL-Start packets into unicast packets, a unicast MAC address must be configured.

Example

Configure an AP to encapsulate EAPOL-Start packets into broadcast packets.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] eapol-start dest-address transform-to broadcast
```

Related Topics

14.1.98 display ap-system-profile

14.1.140 eirp

Function

(AP group radio view) The **eirp** command configures the transmit power for all specified radios in an AP group.

(AP group radio view) The **undo eirp** command restores the default transmit power for all specified radios in an AP group.

(AP radio view) The **eirp** command configures the transmit power for an AP radio.

(AP radio view) The **undo eirp** command cancels the configuration of the transmit power on an AP radio. The transmit power on the AP radio is then determined by that configured in the AP group radio view.

By default, the transmit power of a radio is 127 dBm.

Format

eirp *eirp*

undo eirp

Parameters

Parameter	Description	Value
eirp	Specifies the transmit power.	The value is an integer that ranges from 1 to 127, in dBm.

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the transmit power for a radio based on actual network environments, enabling radios to provide the required signal strength and improving signal quality on WLANs.

Precautions

The value of *antenna-gain* in the **antenna-gain** *antenna-gain* command must be consistent with the gain of the antenna connected to an AP.

 Copyright © Huawei Technologies Co., Ltd.

The actual transmit power of an AP radio is determined by the configured transmit power of the radio, requirements of local laws and regulations, as well as the transmit power range supported by the AP. The actual transmit power of a radio cannot exceed the maximum transmit power required by local laws and regulations.

- If the configured transmit power of a radio is in compliance with local laws and regulations and within the transmit power range supported by the AP, the configured transmit power is the actual transmit power of the radio.
- If the configured transmit power of a radio is smaller than the minimum transmit power supported by the AP, the smaller one between the minimum transmit power supported by the AP and maximum transmit power required by local laws and regulations is the actual transmit power of the radio.
- If the configured transmit power of a radio is larger than the maximum transmit power supported by the AP, the smaller one between the maximum transmit power supported by the AP and maximum transmit power required by local laws and regulations is the actual transmit power of the radio.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the transmit power to 30 dBm for radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] eirp 30
```

Related Topics

14.1.74 display ap config-info

14.1.105 display radio

14.1.141 eth-trunk (AP wired port profile view)

Function

The **eth-trunk** command adds an AP interface to an Eth-Trunk.

The **undo eth-trunk** command removes an AP interface from an Eth-Trunk.

By default, an AP interface is not added to any Eth-Trunk.

Format

eth-trunk *trunk-id*

undo eth-trunk

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trunk-id	Specifies the ID of an Eth-Trunk.	The value is an integer, and the value is 0.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve the connection reliability and increase the bandwidth, you can run this command to bind multiple interfaces into an Eth-Trunk.

Prerequisite

The physical interface to be added to an Eth-Trunk cannot have other configurations. Before adding a physical interface to an Eth-Trunk, clear all configurations on it except the interface status, working mode, descriptions, LLDP function, and alarm function for CRC errors.

Precautions

APs that have only one physical network interface do not support this command.

Example

Add the AP interface to Eth-Trunk 0.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1] eth-trunk 0
```

Related Topics

14.1.128 display wired-port-profile

14.1.142 forward-mode

Function

The **forward-mode** command sets the data forwarding mode in a VAP profile.

The **undo forward-mode** command restores the default data forwarding mode in a VAP profile.

 Copyright © Huawei Technologies Co., Ltd.

By default, the forwarding mode is direct-forward in the VAP profile.

Format

forward-mode { **direct-forward** | **tunnel** }

undo forward-mode

Parameters

Parameter	Description	Value
direct-forward	Indicates the direct forwarding mode.	-
tunnel	Indicates the tunnel forwarding mode.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **forward-mode** command to configure the forwarding mode in a VAP profile. The forwarding modes of VAP profiles can be different.

Example

Create the VAP profile **vap1** and set the forwarding mode to tunnel forwarding in the profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] forward-mode tunnel
Warning: This action may cause service interruption. Continue?[Y/N]y
Info: This operation may take a few seconds, please wait.done.
```

Related Topics

14.1.127 display vap-profile

14.1.143 frequency

Function

(AP group radio view) The **frequency** command sets the working frequency of radios for all APs in an AP group.

(AP group radio view) The **undo frequency** command restores the default working frequency of radios for all APs in an AP group.

(AP radio view) The **frequency** command sets the working frequency of radios for an AP.

(AP radio view) The **undo frequency** command restores the working frequency of the radio on an AP to the working frequency configured in the AP group radio view.

By default, radio 0 works on the 2.4 GHz frequency band, and radio 2 work on the 5 GHz frequency band.

Format

frequency { 2.4g | 5g }

undo frequency

Parameters

Parameter	Description	Value
2.4g	Indicates that the radio works at the 2.4 GHz frequency band.	-
5g	Indicates that the radio works at the 5 GHz frequency band.	-

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Radio 0s of the AP2010DN and AP8130DN support 2.4 GHz and 5 GHz frequency bands but they can work on one frequency band at a time. You can configure the working frequency of the AP based on the frequency band of STAs.

Precautions

The configuration of the 5 GHz frequency band for radio 0 takes effect only on the AP2010DN and AP8130DN.

Changing the working frequency of radio 0 and radio 2 will delete the channel, power, and antenna gain configurations on radio 0 and radio 2. If an AP uses an external antenna, run the **antenna-gain** *antenna-gain* command to reconfigure the antenna gain to be consistent with the gain of the external antenna connected to the AP.

 Copyright © Huawei Technologies Co., Ltd.

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Set the working frequency to the 5 GHz frequency band for radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] frequency 5g
```

Related Topics

14.1.98 display ap-system-profile

14.1.144 guard-interval-mode

Function

The **guard-interval-mode** command configures the guard interval (GI) mode.

The **undo guard-interval-mode** command restores the default GI mode.

By default, the GI mode is normal.

Format

guard-interval-mode { **short** | **normal** }

undo guard-interval-mode

Parameters

Parameter	Description	Value
short	Sets the GI mode to short GI.	-
normal	Sets the GI mode to normal GI.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

During data transmission, the receive and transmit ends do not receive and send data at all times. There is an interval between the first and second data receiving or transmission or among multiple transmissions. The interval is called Guard Interval (GI) and can improve the transmission effect.

The GI mode consists of the short interval and common interval. The common interval is 800 ns whereas the short interval is 400 ns. The short interval is applicable to 802.11n and 802.11ac specifications, which can raise the transmission rate of 802.11n and 802.11ac packets.

Example

Set the GI mode to short.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] guard-interval-mode short
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.145 high-temperature threshold

Function

The **high-temperature threshold** command sets the upper temperature alarm threshold for APs.

The **undo high-temperature threshold** command restores the default upper temperature alarm threshold for APs.

Table 14-83 Default upper temperature alarm threshold for APs

AP Model	Default Value (°C)
AP5030DN/AP5130DN	87
AP6010SN-GN	85
AP6010DN-AGN	102
AP6310SN-GN	94
AP6510DN-AGN	88
AP6510DN-AGN-US	81
AP6610DN-AGN	104
AP6610DN-AGN-US	100
AP7110SN	76
AP7110DN	89
AP7030DE/AP8030DN/AP8130DN/AP9330DN	83
AP9131DN	84

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AP2010DN, AP2030DN, AP3010DN-AGN, AP5010SN-GN, AP5010DN-AGN, AP4030DN and AP4130DN do not support this command.

Format

high-temperature threshold *threshold*

undo high-temperature threshold

Parameters

Parameter	Description	Value
threshold	Specifies the upper temperature alarm threshold.	The value is an integer that ranges from 20 to 110, in °C.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the upper temperature alarm threshold for an AP. When an AP's temperature exceeds the upper threshold, the AP generates an alarm and a log, and notifies the AC of the high temperature.

Example

Set the upper temperature alarm threshold for APs to 65°C.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] high-temperature threshold 65
```

Related Topics

14.1.98 display ap-system-profile

14.1.146 ht a-mpdu disable

Function

The **ht a-mpdu disable** command disables aggregation of MPDUs.

The **undo ht a-mpdu disable** command enables aggregation of MPDUs.

By default, aggregation of MPDUs is enabled.

Format

ht a-mpdu disable

undo ht a-mpdu disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce cost, 802.11n uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Disable aggregation of MPDUs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] ht a-mpdu disable
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.147 ht a-mpdu max-length-exponent

Function

The **ht a-mpdu max-length-exponent** command sets the maximum length of an aggregated MPDU (A-MPDU) on the 802.11n radio. MPDU stands for MAC protocol data unit.

The **undo ht a-mpdu max-length-exponent** command restores the maximum length of an A-MPDU on the 802.11n radio to the default value.

By default, the index for the maximum length of an A-MPDU is 3. The maximum length of the A-MPDU is 65535 bytes.

 Copyright © Huawei Technologies Co., Ltd.

Format

ht a-mpdu max-length-exponent *max-length-exponent-index*

undo ht a-mpdu max-length-exponent

Parameters

Parameter	Description	Value
max-length-exponent-index	Indicates the index for the maximum length of the A-MPDU.	The value is an integer that ranges from 0 to 3. ● 0: indicates that the maximum length of the A-MPDU is 8191 bytes. ● 1: indicates that the maximum length of the A-MPDU is 16383 bytes. ● 2: indicates that the maximum length of the A-MPDU is 32767 bytes. ● 3: indicates that the maximum length of the A-MPDU is 65535 bytes.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11n uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Set the index of the maximum length of the A-MPDU to 2 in the 2G radio profile **default**. The index 2 corresponds to a maximum length of 32767 bytes.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] ht a-mpdu max-length-exponent 2
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.148 igmp-snooping enable (traffic profile view)

Function

The **igmp-snooping enable** command enables IGMP snooping in a traffic profile.

The **undo igmp-snooping enable** command disables IGMP snooping in a traffic profile.

By default, IGMP snooping is disabled in a traffic profile.

Format

igmp-snooping enable

undo igmp-snooping enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IGMP snooping is a basic Layer 2 multicast function that forwards and controls multicast traffic at the data link layer. IGMP snooping runs on a Layer 2 device and analyzes IGMP messages exchanged between a Layer 3 device and hosts to set up and maintain a Layer 2 multicast forwarding table. The Layer 2 device forwards multicast packets based on the Layer 2 multicast forwarding table.

After you disable IGMP snooping in a traffic profile using the **undo igmp-snooping enable** command, all IGMP snooping configurations on the device are deleted. When you run the **igmp-snooping enable** command to enable IGMP snooping again, all IGMP snooping configurations are restored to the default settings on the device.

Prerequisites

A traffic profile has been created.

Example

Enable IGMP snooping in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] igmp-snooping enable
```

14.1.149 igmp-snooping report-suppress

Function

The **igmp-snooping report-suppress** command configures IGMP Report message suppression in a traffic profile.

The **undo igmp-snooping report-suppress** command cancels configuration of IGMP Report and Leave message suppression in a traffic profile.

By default, IGMP Report and Leave message suppression is disabled in a traffic profile.

Format

igmp-snooping report-suppress

undo igmp-snooping report-suppress

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a Layer 2 device receives an IGMP Membership Report message (Report or Leave message) from a group member, the Layer 2 device forwards the message to the directly connected Layer 3 device. A group member host sends a Membership Report message in the following situations:

- When joining a multicast group, a host sends a Report message. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Report messages from the member hosts.
- When receiving an IGMP General Query message, a host sends a Report message. Hosts use a timer to suppress duplicate Report messages in the

same network segment. However, if the timer values on hosts are the same, the Layer 3 device can still receive duplicate Report messages.

- A host running IGMPv2 or IGMPv3 sends a Leave message when leaving a multicast group. When a multicast group has multiple members in a VLAN, the Layer 3 device receives duplicate Leave messages from the member hosts.

After this function is configured, a Layer 2 device forwards only one IGMP Membership Report message to the upstream device in the following scenarios: When the first member joins a multicast group or a host sends a Report message in response to an IGMP Query message, the Layer 2 device forwards a Report message to the upstream device. The upstream device then creates or maintains the matching forwarding entry based on the Report message. When the last member of a group leaves the group, the Layer 2 device forwards a Leave message to the upstream device. The upstream device then deletes the matching forwarding entry. This reduces the number of IGMP messages on the network.

Prerequisites

IGMP snooping has been enabled using the **igmp-snooping enable (traffic profile view)** command.

Example

Enable IGMP Report message suppression in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] igmp-snooping enable
[Huawei-wlan-traffic-prof-p1] igmp-snooping report-suppress
```

Related Topics

10.9.1 display igmp-snooping

14.1.148 igmp-snooping enable (traffic profile view)

10.9.17 igmp-snooping querier enable

10.9.31 igmp-snooping suppress-time

14.1.150 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP source guard on APs.

The **undo ip source check user-bind enable** command disables IP source guard on APs.

By default, IP source guard is disabled on APs.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Users can configure static IP addresses for their clients and connect to the Internet after passing 802.1X authentication. To defend against source IP address spoofing attacks, you need to enable IP source guard on APs.

To prevent IP packets of unauthorized users from entering external networks through an AP, enable IP source guard in a VAP profile and bind the VAP profile to an AP or AP group. The IP source guard function can filter incoming packets on an AP radio interface, preventing unauthorized packets from passing through the AP.

If STA address learning is enabled on an AP using the **undo learn-client-address disable** command, DHCP users are allowed to access the AP. Before the users who are assigned IP addresses statically access an AP, the administrator needs to manually configure static binding entries for the users. That is, the administrator configures an IP network segment and binds it to the MAC addresses of the users so that the users can access the AP.

Example

Enable IP source guard on APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] ip source check user-bind enable
```

Related Topics

14.1.127 display vap-profile

14.4.15 display station dynamic-blacklist

14.1.155 learn-client-address disable

14.1.151 ipsg enable (AP wired port profile view)

Function

The **ipsg enable** command enables IP source guard (IPSG) on an AP's wired interface.

The **undo ipsg enable** command disables IPSG on an AP's wired interface.

By default, IPSG is disabled on an AP's wired interface.

 Copyright © Huawei Technologies Co., Ltd.

Format

ipsg enable

undo ipsg enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Attackers often use packets with the source IP addresses or MAC addresses of authorized users to access or attack networks. As a result, authorized users cannot obtain stable and secure network services. You can enable the IPSG function to prevent the situation.

Prerequisites

Terminal address learning has been enabled on the AP's wired interface using the **learn-client-address enable** command.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

This command takes effect only on IP packets transmitted on an AP's wired interface.

The AP wired interfaces added to an Eth-trunk interface do not support this function.

Example

Enable IPSG on an AP's wired interface.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] ipsg enable
```

Related Topics

14.1.128 display wired-port-profile

14.1.152 keep-service enable

Function

The **keep-service enable** command configures the AP to continue providing data services after the CAPWAP link between the AP and AC is disconnected.

The **undo keep-service enable** command restores the default setting.

By default, all services on the AP are interrupted after the CAPWAP link between the AP and AC is disconnected.

Format

keep-service enable

undo keep-service enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In direct forwarding mode, you can run the **keep-service enable** command to configure the AP to continue providing data services after the CAPWAP link between the AP and AC is disconnected. The data services then no longer depends on the CAPWAP link, which enhances service forwarding robustness.

Precautions

The command does not take effect on a WDS network.

The offline management VAP function and service holding upon CAPWAP link disconnection are mutually exclusive. When the two functions are configured at the same time, the offline management VAP function cannot take effect.

Example

Configure the AP to continue providing data services after the CAPWAP link between the AP and AC is disconnected.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] keep-service enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.98 display ap-system-profile

14.1.153 keep-service enable allow new-access

Function

The **keep-service enable allow new-access** command enables the APs in fault state to allow access of new STAs.

The **undo keep-service enable** command disables the APs in fault state from allowing access of new STAs.

By default, the APs in fault state are disabled from allowing access of new STAs.

Format

keep-service enable allow new-access

undo keep-service enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The networks with low security requirements, which apply to hospitals or warehouses, require that the APs in fault state still allow access of new STAs when link faults occur between the APs and AC. After the **keep-service enable allow new-access** command is run, new STAs can still connect to the APs in fault state when the CAPWAP link between the APs and AC is disconnected.

Prerequisites

The security policy used by the APs must be WEP or WPA/WPA2-PSK.

Precautions

The command does not take effect on a WDS network.

Example

Enable the APs in fault state to allow access of new STAs.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] keep-service enable allow new-access
Info: This configuration is invalid for the WDS network.
```

14.1.154 learn-client-address dhcp-strict

Function

The **learn-client-address dhcp-strict** command enables strict STA IP address learning through DHCP.

The **undo learn-client-address dhcp-strict** command disables strict STA IP address learning through DHCP.

By default, strict STA IP address learning through DHCP is disabled.

Format

learn-client-address dhcp-strict [**blacklist enable**]

undo learn-client-address dhcp-strict

Parameters

Parameter	Description	Value
blacklist enable	Adds STAs with bogus IP addresses to a blacklist. By default, STAs with bogus IP addresses are not added to a blacklist.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a STA associates with an AP, the following situation occurs after strict STA IP address learning through DHCP is enabled:

- If the STA obtains an IP address through DHCP, the AP will automatically report the IP address to the AC. The STA IP address can be used to maintain the mapping between STA IP addresses and MAC addresses.
- For a STA using a static IP address:

  If **blacklist enable** is specified, the STA will be added to a dynamic blacklist of the AP and cannot associate with the AP before the blacklist entry ages.

If **blacklist enable** is not specified, the STA can associate with the AP but the AP does not learn the IP address of the STA.

Prerequisites

STA address learning has been enabled using the **undo learn-client-address disable** command.

Precautions

After strict STA IP address learning is enabled, it is recommended that you run the **14.1.150 ip source check user-bind enable** commands to enable IP source guard so that STAs cannot communicate with the network before obtaining an IP address through DHCP.

Example

Enable strict STA IP address learning through DHCP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] learn-client-address dhcp-strict
```

Related Topics

14.1.127 display vap-profile

14.1.150 ip source check user-bind enable

14.1.155 learn-client-address disable

Function

The **learn-client-address disable** command disables STA address learning.

The **undo learn-client-address disable** command enables STA address learning.

By default, STA address learning is enabled.

Format

learn-client-address disable

undo learn-client-address disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a STA associates with an AP that has STA address learning enabled and obtains an IP address, the AP automatically reports the STA IP address to the AC to maintain the STA' IP address and MAC address binding entry

Precautions

- Before disabling STA address learning, run the **undo learn-client-address dhcp-strict** command to disable strict STA IP address learning through DHCP.
- If a bridging device functions as a STA to connect to an AP enabled with STA address learning, the AP cannot learn IP addresses of users connected to the bridging device; therefore, the users cannot communicate with the network. In this situation, disable STA address learning.

Example

Disable STA address learning.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] learn-client-address disable
```

Related Topics

14.1.127 display vap-profile

14.1.156 learn-client-address enable (AP wired port profile view)

Function

The **learn-client-address enable** command enables terminal address learning on an AP's wired interface.

The **undo learn-client-address enable** command disables terminal address learning on an AP's wired interface.

By default, terminal address learning is disabled on an AP's wired interface.

Format

learn-client-address enable

undo learn-client-address enable

Parameters

None

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After terminal address learning is enabled on an AP's wired interface, if a wired terminal connected to the AP wired interface successfully obtains an IP address, the AP automatically reports the IP address of the terminal to the AC, helping to maintain the IP address and MAC address binding entries of wired terminals.

Prerequisites

The DHCP trusted interface has been enabled using the **undo dhcp trust port** command in the AP wired port profile view.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

The AP wired interfaces added to an Eth-trunk interface do not support this function.

If a bridging device functions as a STA to connect to an AP enabled with STA address learning, the AP cannot learn IP addresses of users connected to the bridging device; therefore, the users cannot communicate with the network. In this situation, disable STA address learning.

Example

Enable terminal address learning on an AP's wired interface.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] learn-client-address enable
```

Related Topics

14.1.128 display wired-port-profile

14.1.157 led off

Function

The **led off** command forbids AP indicators to turn on.

The **undo led off** command restores the default settings.

By default, the AP indicators are allowed to turn on.

Format

led off

undo led off

Parameters

None.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent AP indicators in hospitals and hotels from affecting people's rest at night, run the **led off** command to forbid AP indicators to turn on.

If you need to locate AP faults by observing AP indicator status, run the **undo led off** command to allow the AP indicators to turn on.

Example

Forbid AP indicators to turn on.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] led off
```

Related Topics

14.1.98 display ap-system-profile

14.1.158 legacy-station disable

Function

The **legacy-station disable** command denies access of legacy terminals.

The **undo legacy-station disable** command permits access of legacy terminals.

By default, access of legacy terminals is permitted.

Format

legacy-station disable

undo legacy-station disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Legacy terminals support only 802.11a, 802.11b, or 802.11g, and provide a rate far smaller than 802.11n and 802.11ac terminals. If the legacy terminals access the wireless network, data transmission rate of the 802.11n and 802.11ac terminals will be reduced. To prevent transmission rate of 802.11n and 802.11ac terminals from being affected, run the **legacy-station disable** command to deny access of legacy terminals.

Configuration Impact

After the **legacy-station disable** command is run, legacy terminals supporting only 802.11a, 802.11b, or 802.11g cannot access the wireless network.

Example

Deny access of legacy terminals.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] legacy-station disable
```

Related Topics

14.1.118 display ssid-profile

14.1.159 lldp admin-status

Function

The **lldp admin-status** command sets the LLDP operation mode for an AP.

The **undo lldp admin-status** command restores the default LLDP operation mode for an AP.

By default, the LLDP operation mode of an AP is TxRx.

Format

lldp admin-status { **rx** | **tx** | **txrx** }

undo lldp admin-status

Parameters

Parameter	Description	Value
rx	Specifies the LLDP operation mode as Rx. An AP only receives but does not send LLDP packets.	-
tx	Specifies the LLDP operation mode as Tx. An AP only sends but does not receive LLDP packets.	-
txrx	Specifies the LLDP operation mode as TxRx. An AP sends and receives LLDP packets.	-

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can configure the LLDP operation mode for an AP based on the site requirements. For example, if you set the LLDP operation mode of an AP to Tx, the AP sends LLDP packets but cannot receive LLDP packets from neighbors. In this situation, the AP cannot discover neighbors.

Example

Set the LLDP operation mode of an AP to Tx.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp admin-status tx
```

Related Topics

14.1.98 display ap-system-profile

14.1.160 lldp enable

Function

The **lldp enable** command enables LLDP on AP wired interfaces.

The **undo lldp enable** command disables LLDP on AP wired interfaces.

By default, LLDP is enabled on AP wired interfaces.

Format

lldp enable

undo lldp enable

Parameters

None.

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AP wired interfaces can exchange LLDP packets with neighbors to obtain neighbor status and transmit AP status to neighbors. The AP and neighbors save the received information to the Management Information Base (MIB) for an AC to query and determine the link status.

Prerequisite

The LLDP function has been enabled in the WLAN view using the **14.1.15 ap lldp enable** command.

Example

Enable LLDP on the AP wired interface.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap lldp enable
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1] lldp enable
```

Related Topics

14.1.15 ap lldp enable

14.1.104 display port-link-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.161 lldp message-transmission delay (AP system profile view)

Function

The **lldp message-transmission delay** command sets the LLDP packet transmission delay.

The **undo lldp message-transmission delay** command restores the default LLDP packet transmission delay.

The default LLDP packet transmission delay is 2 seconds.

Format

lldp message-transmission delay *delay*

undo lldp message-transmission delay

Parameters

Parameter	Description	Value
delay	Specifies the LLDP packet transmission delay.	The value is an integer that ranges from 1 to 8192, in seconds. The *delay* value depends on the parameter *interval* set by the **lldp message-transmission interval** command. The *delay* value must be smaller than or equal to a quarter of the *interval* value.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the AP sends an LLDP packet to the neighbor when the device status changes frequently.

 Copyright © Huawei Technologies Co., Ltd.

If the AP status changes frequently, extend the delay in preventing the AP from frequently sending packets to the neighbors. A delay suppresses the network topology flapping.

Configuration Impact

The LLDP packet transmission delay must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency when the local device status frequently changes. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time when the local device status frequently changes. However, if the value is too small, LLDP packets are exchanged frequently. This increases the system load and wastes resources.
- The default value is recommended.

Precautions

Consider the value of *interval* when adjusting the value of *delay* because it is restricted by the value of *interval*.

- Decreasing the value of *delay* is not restricted by the value of *interval*. *delay* can be any number from 1 to 8192.
- The *delay* value must be smaller than or equal to a quarter of the *interval* value. Therefore, if you want to set *delay* to be greater than a quarter of *interval*, first increase the *interval* value to at least four times the new *delay* value, and then increase the *delay* value.

NOTE

If the *interval* value is smaller than four times the *delay* value, the system displays an error message when you run the **undo lldp message-transmission delay** command. To run the **undo lldp message-transmission delay** command, increase the *interval* value to at least four times the *delay* value first.

Example

Set the LLDP packet transmission delay to 10 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp message-transmission delay 10
```

Related Topics

14.1.98 display ap-system-profile
14.1.163 lldp message-transmission interval (AP system profile view)

14.1.162 lldp message-transmission hold-multiplier (AP system profile view)

Function

The **lldp message-transmission hold-multiplier** command sets the hold time multiplier of device information stored on neighbors.

The **undo lldp message-transmission hold-multiplier** command restores the default hold time multiplier of device information stored on neighbors.

The default hold time multiplier is 4.

Format

lldp message-transmission hold-multiplier *hold*

undo lldp message-transmission hold-multiplier

Parameters

Parameter	Description	Value
hold	Specifies the hold time multiplier of device information stored on neighbors.	The value is an integer that ranges from 2 to 10.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The time multiplier is used to calculate how long a packet can be saved on a neighboring node. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the TTL.

The storage time calculation formula is: TTL = Min (65535, (*interval* x *hold*)).

TTL is the device information storage time. It is the smaller value between 65535 and (*interval* x *hold*).

interval indicates the interval at which the device sends LLDP packets to neighbors. This parameter is set by the **lldp message-transmission interval** command. *hold* indicates the hold time multiplier of device information stored on neighbors.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

The hold time multiplier of device information stored on neighbors must be set to a proper value.

- A large value of *delay* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *delay* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the hold time multiplier of AP information stored on neighbors to 5.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp message-transmission hold-multiplier 5
```

Related Topics

14.1.98 display ap-system-profile

14.1.163 lldp message-transmission interval (AP system profile view)

14.1.163 lldp message-transmission interval (AP system profile view)

Function

The **lldp message-transmission interval** command sets the LLDP packet transmission interval.

The **undo lldp message-transmission interval** command restores the default LLDP packet transmission interval.

The default LLDP packet transmission interval is 30 seconds.

Format

lldp message-transmission interval *interval*

undo lldp message-transmission interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the LLDP packet transmission interval.	The value is an integer that ranges from 5 to 32768, in seconds. The *interval* value depends on the parameter *delay* set by the **lldp message-transmission delay** command. The *interval* value must be larger than or equal to 4 times the *delay* value; otherwise, the system displays an error message when you run the **lldp message-transmission interval** command.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the LLDP status of the AP keeps unchanged or the AP does not discover new neighbors, the AP sends LLDP packets to the neighbors at a specified interval.

If you want to change the network topology detection frequency, run the **lldp message-transmission interval** command to change the LLDP packet transmission interval.

Configuration Impact

The LLDP transmission interval must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A short interval increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time. If the delay is too

 Copyright © Huawei Technologies Co., Ltd.

short, LLDP packets are exchanged frequently. This increases the system load and wastes resources.

- The default value is recommended.

Precautions

Consider the value of *delay* when adjusting the value of *interval* because it is restricted by the value of *interval*.

- Increasing the value of *interval* is not restricted by the value of *delay*. *interval* can be any number from 5 to 32768.
- The *interval* value must be larger than or equal to four times the *delay* value. Therefore, if you want to set *interval* to be smaller than four times the value of *delay*, first reduce the *delay* value to be smaller than or equal to a quarter of the new *interval* value, and then reduce the *interval* value.

NOTE

If the *delay* value is larger than a quarter of the *interval* value, the system displays an error message when you run the **undo lldp message-transmission interval** command. To run the **undo lldp message-transmission interval** command, reduce the *delay* value to be smaller than or equal to a quarter of the *interval* value first.

Example

Set the LLDP packet transmission interval to 60 second.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp message-transmission interval 60
```

Related Topics

14.1.98 display ap-system-profile

14.1.161 lldp message-transmission delay (AP system profile view)

14.1.164 lldp report-interval

Function

The **lldp report-interval** command sets the interval at which an AP reports LLDP neighbor information to an AC.

The **undo lldp report-interval** command restores the default interval at which an AP reports LLDP neighbor information to an AC.

By default, an AP reports LLDP neighbor information to an AC at an interval of 30 seconds.

Format

lldp report-interval *interval-time*

undo lldp report-interval

Parameters

Parameter	Description	Value
interval-time	Specifies the interval at which an AP reports LLDP neighbor information to an AC.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **lldp report-interval** command to adjust the interval at which an AP reports LLDP neighbor information to an AC. This prevents LLDP neighbor information from being frequently reported.

Example

Set the interval at which an AP reports LLDP neighbor information to an AC to 20 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp report-interval 20
```

Related Topics

14.1.98 display ap-system-profile

14.1.165 lldp restart-delay

Function

The **lldp restart-delay** command sets the delay in re-enabling LLDP on an AP.

The **undo lldp restart-delay** command restores the default LLDP operation mode for an AP.

By default, the delay in re-enabling LLDP on an AP is 2 seconds.

Format

lldp restart-delay *delay-time*

undo lldp restart-delay

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delay-time	Specifies the delay in re-enabling LLDP.	The value is an integer that ranges from 1 to 10, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When the LLDP status of an AP changes, the AP reports LLDP neighbor information to the connected AC. Setting the delay in re-enabling LLDP on the AP prevents the AP from frequently reporting LLDP neighboring information to the AC when the LLDP status of the AP frequently changes. This reduces the load on the AC and saves resources.

Example

Set the delay in re-enabling LLDP on an AP to 1 second.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] lldp restart-delay 1
```

Related Topics

14.1.98 display ap-system-profile

14.1.166 lldp tlv-enable (AP wired port link profile view)

Function

The **lldp tlv-enable** command specifies the types of TLVs that an AP wired interface.

The **undo lldp tlv-enable** command specifies the types of TLVs that an AP wired interface advertises is prohibited from advertising.

By default, an AP wired interface advertises all types of TLVs.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

 Copyright © Huawei Technologies Co., Ltd.

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

Parameters

Parameter	Description	Value
basic-tlv	Indicates basic TLVs to be advertised: ● Management-address TLV ● Port Description TLV ● System Capabilities TLV ● System Description TLV ● System Name TLV	-
all	● Configures the AP wired interface to advertise all types of TLVs when basic TLVs, TLVs defined by IEEE 802.1, and TLVs defined by IEEE 802.3 are configured.	-
management-address	Configures the AP wired interface to advertise Management-address TLVs.	-
port-description	Configures the AP wired interface to advertise Port Description TLVs.	-
system-capability	Configures the AP wired interface to advertise System Capabilities TLVs.	-
system-description	Configures the AP wired interface to advertise System Description TLVs.	-
system-name	Configures the AP wired interface to advertise System Name TLVs.	-

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs, TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the IEEE 802.1 format, TLVs in the IEEE 802.3 format.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

Prerequisites

The LLDP function is enabled globally and on interfaces.

Precautions

When the supported TLVs are basic TLVs, TLVs in the IEEE 802.1 format, and TLVs in the IEEE 802.3 format, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs.

If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.

Example

Configure the wired interface of AP to advertise Management-address TLVs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap lldp enable
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1] lldp tlv-enable basic-tlv management-address
```

Related Topics

14.1.15 ap lldp enable

14.1.160 lldp enable

14.1.167 log-server

Function

The **log-server** command configures the log server IP address in the AP system profile and enables log backup on the AP.

The **undo log-server** command restores the default configurations.

By default, the log server IP address is not configured in an AP system profile and log backup is disabled on an AP.

Format

log-server ip-address *server-ip-address*

undo log-server

Parameters

Parameter	Description	Value
ip-address *server-ip-address*	Specifies the IPv4 address of the log server.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the command to configure the log server IP address in the AP system profile and enable log backup on the AP. After log backup is enabled, the AP automatically sends logs to the log server with the specified IP address.

NOTICE

Modifying the attributes of an AP profile changes configurations of all APs using this profile.

Example

Set the IP address of the log server to 10.0.0.1 and enable log backup on the AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] log-server ip-address 10.0.0.1
```

14.1.168 low-temperature threshold

Function

The **low-temperature threshold** command sets the lower temperature alarm threshold for APs.

The **undo low-temperature threshold** command restores the default lower temperature alarm threshold for APs.

 Copyright © Huawei Technologies Co., Ltd.

Table 14-84 Default lower temperature alarm threshold for APs

AP Model	Default Value (°C)
AP6010SN-GN/AP6010DN-AGN/AP6310SN-GN/AP7110DN-AGN/AP7110SN-GN/AP9330DN	-13
AP6510DN-AGN/AP6610DN-AGN/AP6510DN-AGN-US/AP6610DN-AGN-US/AP8030DN/AP8130DN/AP9131DN	-43
AP5030DN/AP5130DN	-28
AP7030DE	-23

NOTE

The AP2010DN, AP2030DN, AP3010DN-AGN, AP5010SN-GN, AP5010DN-AGN, AP4030DN and AP4130DN do not support this command.

Format

low-temperature threshold *threshold*

undo low-temperature threshold

Parameters

Parameter	Description	Value
threshold	Specifies the lower temperature alarm threshold.	The value is an integer that ranges from -70 to 10, in °C.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to set the lower temperature alarm threshold for an AP. When an AP's temperature exceeds the lower threshold, the AP generates an alarm and a log, and notifies the AC of the low temperature.

Example

Set the lower temperature alarm threshold for APs to 5°C.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] low-temperature threshold 5
```

Related Topics

14.1.98 display ap-system-profile

14.1.169 management-vlan

Function

The **management-vlan** command configures a management VLAN for an AP.

The **undo management-vlan** command deletes a management VLAN of an AP.

By default, no management VLAN is configured for an AP.

Format

management-vlan *vlan-id*

undo management-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of the management VLAN.	The value is an integer that ranges from 1 to 4094.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the management packets of APs are untagged, and the access switch directly connected to the APs tag VLAN IDs on the management packets.

After the **management-vlan** command is executed, the management and control packets sent from APs to the AC contain the management VLAN tag. You can use this command according to the networking.

Precautions

The configured management VLAN takes effect only after the AP is restarted.

 Copyright © Huawei Technologies Co., Ltd.

In the following paragraphs, packets sent by the AP's wired interface refer to the management packets and service packets sent in the tunnel forwarding mode.

- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command, packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in untagged mode using the **vlan untagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command, the packets sent from the AP's wired interface are not tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in tagged mode using the **vlan tagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the PVID of the AP's wired interface is set to the management VLAN ID using the **vlan pvid** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.

Example

Set the management VLAN of the AP to VLAN 2 in the AP system profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] management-vlan 2
Warning: This operation will cause AP reset. Continue? [Y/N]:y
```

Related Topics

14.1.98 display ap-system-profile

14.5.15 vlan pvid (AP wired port profile view)

14.5.17 vlan (AP wired port profile view)

14.1.170 max-sta-number (SSID profile view)

Function

The **max-sta-number** command sets the maximum number of successfully associated STAs on a VAP.

The **undo max-sta-number** command restores the default maximum number of successfully associated STAs on a VAP.

By default, a VAP allows for a maximum of 64 successfully associated STAs.

Format

max-sta-number *max-sta-number*

undo max-sta-number

Parameters

Parameter	Description	Value
max-sta-number	Specifies the maximum number of successfully associated STAs on a specified VAP.	The value is an integer that ranges from 1 to 128.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

More access users on a VAP indicate fewer network resources that each user can occupy. To ensure Internet experience of users, you can run the **max-sta-number** command to set a proper maximum number of successfully associated STAs on a VAP.

Configuration Impact

After the number of successfully associated STAs on a VAP reaches the maximum, new users cannot connect to the VAP.

The **max-sta-number** *max-sta-number* command sets the maximum number of successfully associated STAs on a VAP.

Example

Set the maximum number of successfully associated STAs on a VAP to 50.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] max-sta-number 50
Warning: This action may cause service interruption. Continue?[Y/N]y
```

14.1.171 memory-usage threshold

Function

The **memory-usage threshold** command configures a memory usage alarm threshold for APs.

The **undo memory-usage threshold** command restores the default memory usage alarm threshold.

By default, the memory usage alarm threshold on an AP is 80.

Format

memory-usage threshold *threshold*

undo memory-usage threshold

Parameters

Parameter	Description	Value
threshold	Specifies the memory usage alarm threshold of an AP.	The value is an integer that ranges from 30 to 100.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **memory-usage threshold** command to configure the memory usage alarm threshold in the AP system profile view. The configuration is delivered to all APs using the profile.

- When the memory usage of an AP exceeds the alarm threshold, the AP sends an alarm message to the AC, and the AC displays the alarm information.
- When the memory usage of an AP falls below the alarm threshold, the AP sends a clear alarm message to the AC, and the AC displays the clear alarm information.

Example

Set the memory usage alarm threshold of AP to 60.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] memory-usage threshold 60
```

Related Topics

14.1.98 display ap-system-profile

14.1.172 mtu

Function

The **mtu** command changes the maximum transmission unit (MTU) of Ethernet ports in an AP system profile.

The **undo mtu** command restores the default MTU of Ethernet ports in an AP system profile.

The default the MTU of Ethernet ports in an AP system profile is 1500 bytes.

Format

mtu *mtu-value*

undo mtu

Parameters

Parameter	Description	Value
mtu-value	Specifies the maximum size of packets sent and received on an Ethernet port.	The value is an integer that ranges from 1500 to 1700, in bytes.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

The MTU value is the maximum size of packets sent and received on an Ethernet interface of the AP.

NOTICE

Modifying the attributes of an AP system profile changes configurations of all APs using this profile.

Precautions

- DHCP packets cannot be fragmented. When the MTU value set using the **mtu** command is smaller than the DHCP packet length, DHCP packets cannot be forwarded. Therefore, set a larger MTU value.
- If the MTU value is smaller than the DHCP packet length, the AP may be disconnected. In this case, restart the AP.

Example

Change the MTU of Ethernet ports to 1700 bytes in the AP system profile.

```
<Huawei> system-view
[Huawei] wlan ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] mtu 1700
```

Related Topics

14.1.98 display ap-system-profile

14.1.173 multicast-rate

Function

The **multicast-rate** command configures the multicast rate of wireless packets in a radio profile.

The **undo multicast-rate** command restores the default multicast rate of wireless packets in a radio profile.

By default, the multicast rate of wireless packets is 11 Mbps in a 2G radio profile and 6 Mbps in a 5G radio profile.

Format

multicast-rate *multicast-rate*

undo multicast-rate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
multicast-rate	Specifies the multicast rate of wireless packets in a radio profile.	Enumerated type. The values are as follows in a 2G radio profile: ● 1: 1 Mbps ● 2: 2 Mbps ● 5: 5.5 Mbps ● 6: 6 Mbps ● 9: 9 Mbps ● 11: 11 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps The values are as follows in a 5G radio profile: ● 6: 6 Mbps ● 9: 9 Mbps ● 12: 12 Mbps ● 18: 18 Mbps ● 24: 24 Mbps ● 36: 36 Mbps ● 48: 48 Mbps ● 54: 54 Mbps

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After this command is run, the multicast rate of wireless packets is the configured value and irrelevant to the STA access mode.

If the configured multicast rate is not in the basic rate set and the STA does not support this rate, the STA cannot receive multicast data.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, *multicast-rate* that takes effect on the 2 GHz radio of the AP is fixed as 1 Mbps, and *multicast-rate* configured in the 2G radio profile view does not take effect on the AP.

Example

Set the multicast rate of wireless packets to 54 Mbps in the 2.4G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] multicast-rate 54
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.188 radio-type (2G radio profile view)

14.1.174 port-link-profile (WLAN view)

Function

The **port-link-profile** command creates an AP wired port link profile and displays the AP wired port link profile view, or displays the view of an existing AP wired port link profile.

The **undo port-link-profile** command deletes an AP wired port link profile.

By default, the system provides the AP wired port link profile **default**.

Format

port-link-profile name *profile-name*

undo port-link-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP wired port link profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all AP wired port link profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP wired port link profile offers link-layer management and configuration on AP's wired interfaces.

Follow-up Procedure

After you create an AP wired port link profile, run the **14.1.175 port-link-profile (AP wired port profile view)** command to bind it to an AP wired port profile and then run the **14.1.241 wired-port-profile (AP group view and view)** command to bind the AP wired port profile to an AP or AP group. In this way, the AP wired port link profile can take effect.

Precautions

- The AP wired port link profile **default** cannot be deleted.
- The AP wired port link profile referenced by an AP or AP group cannot be deleted. To delete the AP wired port link profile, unbind it from the AP or AP group first.

Example

Create the AP wired port link profile **port-link1** and display the AP wired port link profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1]
```

Related Topics

14.1.104 display port-link-profile

14.1.175 port-link-profile (AP wired port profile view)

14.1.175 port-link-profile (AP wired port profile view)

Function

The **port-link-profile** command binds an AP wired port link profile to an AP wired port profile.

The **undo port-link-profile** command unbinds an AP wired port link profile from an AP wired port profile.

 Copyright © Huawei Technologies Co., Ltd.

By default, the AP wired port link profile **default** is bound to an AP wired port profile.

Format

port-link-profile *profile-name*

undo port-link-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port link profile.	The AP wired port link profile must exist.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP wired port link profile using the **14.1.174 port-link-profile (WLAN view)** command, bind it to an AP wired port profile so that the AP wired port link profile can take effect.

Precautions

After an AP wired port link profile is bound to an AP wired port profile, parameter settings in the AP wired port link profile apply to specified interfaces of all APs using the AP wired port profile.

Example

Create the AP wired port link profile **port-link1** and bind it to the AP wired port profile **wired-port1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1] quit
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1] port-link-profile port-link1
```

Related Topics

14.1.109 display references port-link-profile

14.1.128 display wired-port-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.174 port-link-profile (WLAN view)

14.1.176 priority-map downstream dscp

Function

The **priority-map downstream dscp** command configures mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets when packets are sent to an AP from upper-layer devices.

The **undo priority-map downstream** command restores the default mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets when packets are sent to an AP from upper-layer devices.

Table 14-85 describes the default mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets.

Table 14-85 Default mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets

DSCP	User-Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Format

priority-map downstream dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map downstream

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot11e *dot11e-value*	Specifies the 802.11e UP value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11e packets use different fields to identify their priorities. 802.11e packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and IP packets transmitted on an Ethernet carry the DSCP priority (also called the ToS field). When data packets are forwarded from the AC or upper-layer network to an AP, the AP needs to convert the 802.3 packets to 802.11e packets and map the ToS field in the IP packet header to the UP field of 802.11e packets. You can use the **priority-map downstream dscp** command to configure mapping from the DSCP priority of 802.3 packets to the 802.11e user priority of 802.11e packets.

Example

Configure mapping from DSCP priorities to user priorities in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map downstream dscp 0 to 6 dot11e 1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.229 traffic-profile (WLAN view)
14.1.124 display traffic-profile

14.1.177 priority-map downstream trust

Function

The **priority-map downstream trust** command configures mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11e user priority of 802.11 packets when packets are forwarded to APs from upper-layer network devices.

The **undo priority-map downstream trust** command restores the default mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11e user priority of 802.11 packets when packets are forwarded to APs from upper-layer network devices.

By default, the 802.1p or DSCP priorities are mapped to 802.11e user priorities.

Format

priority-map downstream trust { **dot1p** | **dscp** }

undo priority-map downstream trust

Parameters

Parameter	Description	Value
dot1p	Specifies mapping from the 802.1p priority to the 802.11e user priority.	-
dscp	Specifies mapping from the DSCP priority to the 802.11e user priority.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

802.3 and 802.11 packets use different fields to identify their priorities. 802.11 packets sent from a WMM-capable STA carry the user priority (also called the User Priority field), and VLAN tagged-802.3 packets transmitted on the Ethernet contain 802.1p priorities (also called the CoS field). When data packets are forwarded from the AC or upper-layer network to an AP, the AP needs to convert the 802.3 packets to 802.11 packets and map the 802.1p priority carried in the

 Copyright © Huawei Technologies Co., Ltd.

802.3 packet header to the user priority of 802.11 packets. You can use the **priority-map downstream trust** command to configure mapping from the 802.1p or DSCP priority of 802.3 packets to the 802.11e user priority of 802.11 packets.

Example

Configure mapping from the 802.1p priority to the 802.11e user priority in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map downstream trust dot1p
```

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

14.1.178 priority-map tunnel-upstream dot11e

Function

The **priority-map tunnel-upstream dot11e** command configures mapping from the 802.11e user priority to DSCP priority in the CAPWAP header when packets are sent from an AP to an AC.

The **undo priority-map tunnel-upstream** command restores the default mapping from the 802.11e user priority to DSCP priority in the CAPWAP header when packets are sent from an AP to an AC.

By default, the 802.11e user priority is mapped to the DSCP priority in the CAPWAP header, as shown in **Table 14-86**.

NOTE

The CAPWAP header refers to the tunnel header.

Table 14-86 Default mapping from the 802.11e user priority to DSCP priority in the CAPWAP header

802.11e UP	DSCP Priority in the CAPWAP Header
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

 Copyright © Huawei Technologies Co., Ltd.

Format

priority-map tunnel-upstream dot11e { *dot11e-value1* [**to** *dot11e-value2*] } &<1-10> **dscp** *dscp-value*

undo priority-map tunnel-upstream

Parameters

Parameter	Description	Value
dot11e *dot11e-value1*	Specifies the 802.11e UP value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
to *dot11e-value2*	Specifies the 802.11e UP value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.
dscp *dscp-value*	Specifies the DSCP priority in the CAPWAP header.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

Map 802.11e user priority 6 to DSCP priority 1 when packets are transmitted from an AP to an AC in the traffic profile **p1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map tunnel-upstream dot11e 6 dscp 1
```

Related Topics

14.1.124 display traffic-profile

14.1.229 traffic-profile (WLAN view)

14.1.179 priority-map tunnel-upstream dscp

Function

The **priority-map tunnel-upstream dscp** command configures mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets when packets are sent to an AP.

The **undo priority-map tunnel-upstream dscp** command restores the default mapping from the DSCP priority of 802.11 packets to the DSCP priority of tunnel packets.

By default, DSCP priority **1** of 802.11 packets maps DSCP priority **1** of tunnel packets, DSCP priority **2** of 802.11 packets maps DSCP priority **2** of tunnel packets, and so on. DSCP priority **63** of 802.11 packets maps DSCP priority **63** of tunnel packets.

Format

priority-map tunnel-upstream dscp { *dscp-value* [**to** *dscp-value1*] } &<1-10> **tunnel-dscp** *dscp-value2*

undo priority-map tunnel-upstream dscp

Parameters

Parameter	Description	Value
dscp *dscp-value*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value1*	Specifies the DSCP priority of 802.11 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tunnel-dscp *dscp-value2*	Specifies the DSCP priority of tunnel packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

The tunnel priority mapping is applicable to scenarios where data packets are sent in tunnel forwarding mode.

Example

Map DSCP priority 6 of 802.11 packets to DSCP priority 1 of tunnel packets when packets are sent to an AP in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map tunnel-upstream dscp 6 tunnel-dscp 1
```

Related Topics

14.1.124 display traffic-profile
14.1.229 traffic-profile (WLAN view)

14.1.180 priority-map tunnel-upstream trust

Function

The **priority-map tunnel-upstream trust** command configures mapping from the 802.11e user priority or DSCP priority of 802.3 packets to the user priority of tunnel packets.

The **undo priority-map tunnel-upstream trust** command restores the default mapping.

By default, the 802.11e user priority of 802.3 packets is mapped to the user priority of tunnel packets.

Format

priority-map tunnel-upstream trust { **dot11e** | **dscp** }

undo priority-map tunnel-upstream trust

Parameters

Parameter	Description	Value
dot11e	Maps the 802.11e user priority of 802.3 packets to the user priority of tunnel packets.	-
dscp	Maps the DSCP priority of 802.3 packets to the user priority of tunnel packets.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

To provide QoS guarantee for data packets of different users when packets are transmitted over a tunnel, configure a specific tunnel priority or priority mapping.

Example

Configure mapping from the DSCP priority to the user priority of tunnel packets in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] priority-map tunnel-upstream trust dscp
```

Related Topics

14.1.229 traffic-profile (WLAN view)
14.1.124 display traffic-profile

14.1.181 probe-response-retry

Function

The **probe-response-retry** command sets the number of times Probe Response packets are retransmitted.

The **undo probe-response-retry** command restores the default number of times Probe Response packets are retransmitted.

By default, the number of Probe Response retransmissions is 1.

Format

probe-response-retry *retry-time*

undo probe-response-retry

Parameters

Parameter	Description	Value
retry-time	Specifies the number of times Probe Response packets are retransmitted.	The value is an integer that ranges from 0 to 3. When the value is set to 0, Probe Response packets are not retransmitted.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In high-density wireless scenarios, too many Probe Response frames occupy a large number of wireless resources. To reduce wireless resource occupation of the frames and improve channel usage efficiency, you can run the **probe-response-retry** command to set a small number of or forbid Probe Response packet retransmissions.

Precautions

A small number of Probe Response packet retransmissions may reduce the channel scan efficiency of some STAs while a large number of Probe Response packet retransmissions may lower the wireless network performance.

Example

Set the number of times Probe Response packets are retransmitted to 0.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] probe-response-retry 0
```

Related Topics

14.1.118 display ssid-profile

14.1.182 radio

Function

The **radio** command displays the radio view.

Format

radio *radio-id*

Parameters

Parameter	Description	Value
radio-id	Specifies the radio ID.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The radio configuration in the AP group view or AP view takes effect on all radios at the same time. To perform configuration only on radio 0 or radio 1, enter the view of the corresponding radio to configure the radio parameters.

Precautions

After running the **radio** *radio-id* command in the AP group view to enter the radio view, you can perform configurations on all specified radios in the AP group; after running the **radio** *radio-id* command in the AP view to enter the radio view, you can perform configurations on the specified AP radio.

Example

Display the view of radio 0 on the AP with the ID 0

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 0
[Huawei-wlan-ap-0] radio 0
[Huawei-wlan-radio-0/0]
```

Related Topics

14.1.70 display ap

14.1.183 radio disable

Function

(AP group radio view) The **radio disable** command disables all specified radios in an AP group.

(AP group radio view) The **undo radio disable** command enables all specified radios in an AP group.

(AP radio view) The **radio disable** command disables an AP radio.

(AP radio view) The **undo radio disable** command cancels the status configuration of an AP radio. The status of the AP radio is then determined by the status configuration in the AP group radio view.

By default, all AP radios are enabled.

Format

radio disable

undo radio disable

Parameters

None

Views

AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to enable or disable a specified radio.

After a radio is disabled, coverage hole compensation is triggered for automatic optimization.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Example

Disable radio 0 of AP 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-id 1
```

```
[Huawei-wlan-ap-1] radio 0
[Huawei-wlan-radio-1/0] radio disable
Warning: This action may cause service interruption. Continue?[Y/N]y
```

14.1.184 radio-2g-profile (WLAN view)

Function

The **radio-2g-profile** command creates a 2G radio profile and displays the 2G radio profile view, or displays the view of an existing 2G radio profile.

The **undo radio-2g-profile** command deletes a 2G radio profile.

By default, the system provides the 2G radio profile **default**.

Format

radio-2g-profile name *profile-name*

undo radio-2g-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a 2G radio profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all 2G radio profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 2G radio profile is used to configure and optimize the 2G radio of an AP, but does not take effect on the 5G radio. Create a proper radio profile and apply it in

the AP view, AP group view, AP radio view, or AP group radio view. In this way, the AP provides better radio signal transmit and receive capabilities.

Follow-up Procedure

Run the **14.1.185 radio-2g-profile** command to apply the 2G radio profile in the AP view, AP group view, AP radio view, or AP group radio view so that the 2G radio profile can take effect.

Precautions

- The 2G radio profile **default** cannot be deleted.
- The 2G radio profile referenced in the AP view, AP group view, AP radio view, or AP group radio view cannot be deleted. To delete the 2G radio profile, unbind it in the AP view, AP group view, AP radio view, or AP group radio view first.

Usually, radio 0 and radio 1 of an AP work on the 2.4 GHz and 5 GHz frequency bands respectively. Only radio 0 of the AP2010DN and AP8130DN can be configured to work on the 2.4 GHz or 5 GHz frequency band using the **14.1.143 frequency** command.

Example

Create the 2G radio profile **radio-profile1** and display the view of the profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1]
```

Related Topics

14.1.106 display radio-2g-profile

14.1.186 radio-5g-profile (WLAN view)

14.1.185 radio-2g-profile

Function

The **radio-2g-profile** command binds a 2G radio profile to a 2G radio.

The **undo radio-2g-profile** command unbinds a 2G radio profile from a 2G radio.

By default, no 2G radio profile is applied in the AP view and AP radio view, but the 2G radio profile **default** is applied to the AP group view and AP group radio view.

Format

radio-2g-profile *profile-name* { **radio** { *radio-id* | **all** } }

undo radio-2g-profile { **radio** { *radio-id* | **all** } }

radio { *radio-id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 2G radio profile.	The 2G radio profile must exist.
radio *radio-id*	Specifies a radio ID.	The value is an integer that is 0 and 2.
radio all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 2G radio profile using the **14.1.184 radio-2g-profile (WLAN view)** command, bind it to a 2G radio so that the 2G radio profile can take effect.

Precautions

After a 2G radio profile is applied in the AP group view or AP view, the parameter settings in the profile take effect on all 2G radios in the AP group or the 2G radio of the AP.

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

Example

Create the 2G radio profile **radio-profile1** and bind it to AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] radio-2g-profile radio-profile1 radio 0
```

Related Topics

14.1.97 display ap-group

14.1.110 display references radio-2g-profile

14.1.184 radio-2g-profile (WLAN view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.186 radio-5g-profile (WLAN view)

Function

The **radio-5g-profile** command creates a 5G radio profile and displays the 5G radio profile view, or displays the view of an existing 5G radio profile.

The **undo radio-5g-profile** command deletes a 5G radio profile.

By default, the system provides the 5G radio profile **default**.

Format

radio-5g-profile name *profile-name*

undo radio-5g-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a 5G radio profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all 5G radio profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A 5G radio profile is used to configure and optimize the 5G radio of an AP, but does not take effect on the 2G radio. Create a proper radio profile and apply it in the AP view, AP group view, AP radio view, or AP group radio view. In this way, the AP provides better radio signal transmit and receive capabilities.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Run the **14.1.187 radio-5g-profile** command to apply the 5G radio profile in the AP view, AP group view, AP radio view, or AP group radio view so that the 5G radio profile can take effect.

Precautions

- The 5G radio profile **default** cannot be deleted.
- The 5G radio profile referenced in the AP view, AP group view, AP radio view, or AP group radio view cannot be deleted. To delete the 5G radio profile, unbind it in the AP view, AP group view, AP radio view, or AP group radio view first.

Usually, radio 0 and radio 1 of an AP work on the 2.4 GHz and 5 GHz frequency bands respectively. Only radio 0 of the AP2010DN and AP8130DN can be configured to work on the 2.4 GHz or 5 GHz frequency band using the **14.1.143 frequency** command.

Example

Create the 5G radio profile **radio-profile2** and display the view of the profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name radio-profile2
[Huawei-wlan-radio-5g-prof-radio-profile2]
```

Related Topics

14.1.107 display radio-5g-profile

14.1.184 radio-2g-profile (WLAN view)

14.1.187 radio-5g-profile

Function

The **radio-5g-profile** command binds a 5G radio profile to a 5G radio.

The **undo radio-5g-profile** command unbinds a 5G radio profile from a 5G radio.

By default, no 5G radio profile is applied in the AP view and AP radio view, but the 5G radio profile **default** is applied to the AP group view and AP group radio view.

Format

radio-5g-profile *profile-name* { **radio** { *id* | **all** } }

undo radio-5g-profile [**radio** { *id* | **all** }]

radio { *id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a 5G radio profile.	The 5G radio profile must exist.

Parameter	Description	Value
radio *id*	Specifies the radio ID.	The value is an integer that ranges from 0 to 2.
radio all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a 5G radio profile using the **14.1.186 radio-5g-profile (WLAN view)** command, bind it to a 5G radio so that the 5G radio profile can take effect.

Precautions

After a 5G radio profile is applied in the AP group view or AP view, the parameter settings in the profile take effect on all 5G radios in the AP group or the 5G radio of the AP.

The configuration in the AP view and AP radio view has a higher priority than that in the AP group view and AP group radio view.

Example

Create the 5G radio profile **radio-profile2** and bind it to AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name radio-profile2
[Huawei-wlan-radio-5g-prof-radio-profile2] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] radio-5g-profile radio-profile2 radio 1
```

Related Topics

14.1.97 display ap-group

14.1.111 display references radio-5g-profile

14.1.186 radio-5g-profile (WLAN view)

14.1.188 radio-type (2G radio profile view)

Function

The **radio-type** command sets the radio type in a 2G radio profile.

 Copyright © Huawei Technologies Co., Ltd.

The **undo radio-type** command restores the default radio type in a 2G radio profile.

By default, the radio type in a 2G radio profile is **dot11n**.

Format

radio-type { **dot11b** | **dot11g** | **dot11n** }

undo radio-type

Parameters

Parameter	Description	Value
dot11b	Specifies the 802.11b radio type.	-
dot11g	Specifies the 802.11b/g radio type.	-
dot11n	Specifies the 802.11b/g/n radio type.	-

Views

2G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **radio-type** command to set the radio type in a radio profile.

Precautions

If a rate in the basic rate set or supported rate set, or the multicast rate is not supported by the 802.11b protocol, the radio type cannot be set to **80211b**.

When the radio type is set to **dot11b** or **dot11g**, the function of denying access from legacy terminals becomes invalid.

If WDS-enabled radios are configured not to support 802.11n/ac, the air interface backhaul performance will be degraded.

If you run the **radio-type dot11b** command in the 2G radio profile view to set the radio type to **dot11b**, and the 2G radio profile is applied to an AP, the rates of Beacon frames and multicast packets that take effect on the 2 GHz radio of the AP are fixed as 1 Mbps, and the values configured using the **beacon-2g-rate** *beacon-2g-rate* and **multicast-rate** *multicast-rate* commands do not take effect on the AP.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the radio type to **dot11g** in a 2G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] radio-type dot11g
```

Related Topics

14.1.44 beacon-2g-rate

14.1.106 display radio-2g-profile

14.1.173 multicast-rate

14.1.189 radio-type (5G radio profile view)

Function

The **radio-type** command sets the radio type in a 5G radio profile.

The **undo radio-type** command restores the default radio type in a 5G radio profile.

By default, the radio type in a 5G radio profile is **dot11ac**.

Format

radio-type { **dot11a** | **dot11ac** | **dot11n** }

undo radio-type

Parameters

Parameter	Description	Value
dot11a	Specifies the 802.11a radio type.	-
dot11ac	Specifies the 802.11a/n/ac radio type.	-
dot11n	Specifies the 802.11a/n radio type.	-

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

You can run the **radio-type** command to set the radio type in a radio profile.

Precautions

When the radio type is set to **dot11a**, the function of denying access from legacy terminals becomes invalid.

If the configured radio type is not supported by an AP, the actual radio type supported by the AP takes effect. For example, if you set the 802.11ac radio type for an 802.11n AP, the 802.11n radio type takes effect on the AP.

If WDS-enabled radios are configured not to support 802.11n/ac, the air interface backhaul performance will be degraded.

Example

Set the radio type to **dot11n** in a 5G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] radio-type dot11n
```

Related Topics

14.1.107 display radio-5g-profile

14.1.190 rate-limit

Function

The **rate-limit** command configures rate limit for upstream and downstream packets of all STAs or each STA on a VAP.

The **undo rate-limit** command restores the default rate limit for upstream and downstream packets of all STAs or each STA on a VAP.

By default, the rate limit for upstream and downstream packets of all STAs on a VAP is 4294967295 kbit/s, and that of each STA is 4294967295 kbit/s.

Format

rate-limit { **client** | **vap** } { **up** | **down** } *rate-value*

undo rate-limit { **client** | **vap** } { **up** | **down** }

Parameters

Parameter	Description	Value
client	Specifies a STA on a VAP.	-
vap	Specifies all STAs on a VAP.	-
up	Specifies the rate limit for upstream packets on a VAP.	-

Parameter	Description	Value
down	Specifies the rate limit for downstream packets on a VAP.	-
rate-value	Specifies the limited rate of packets.	The value is an integer that ranges from 64 to 4294967295, in kbit/s.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **rate-limit** command to limit the rate of upstream and downstream packets for all STAs or each STA on a VAP to protect network bandwidth resources.

Precautions

The limited rate of upstream and downstream packets configured for all STAs on a VAP using the **rate-limit vap** command must be greater than or equal to that configured for each STA on a VAP using the **rate-limit client** command.

The limited rate of upstream and downstream packets configured for each STA on a VAP using the **rate-limit client** command cannot exceed that configured for all STAs on a VAP using the **rate-limit vap** command.

Example

Set the limited rate of upstream packets to 4294967295 kbit/s for all STAs on a VAP in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] rate-limit vap up 4294967295
```

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

14.1.191 reach-max-sta hide-ssid disable

Function

The **reach-max-sta hide-ssid disable** command disables automatic SSID hiding when the number of users reaches the maximum.

The **undo reach-max-sta hide-ssid disable** command enables automatic SSID hiding when the number of users reaches the maximum.

By default, automatic SSID hiding is enabled when the number of users reaches the maximum.

Format

reach-max-sta hide-ssid disable

undo reach-max-sta hide-ssid disable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

After automatic SSID hiding is enabled, SSIDs are automatically hidden when the number of users connected to the WLAN reaches the maximum, and SSIDs are unavailable for new users.

Example

Disable automatic SSID hiding when the number of users reaches the maximum.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] reach-max-sta hide-ssid disable
```

Related Topics

14.1.118 display ssid-profile

 Copyright © Huawei Technologies Co., Ltd.

14.1.192 regulatory-domain-profile (WLAN view)

Function

The **regulatory-domain-profile** command creates a regulatory domain profile and displays the regulatory domain profile view, or displays the view of an existing regulatory domain profile.

The **undo regulatory-domain-profile** command deletes a regulatory domain profile.

By default, the system provides the regulatory domain profile **default**.

Format

regulatory-domain-profile name *profile-name*

undo regulatory-domain-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a regulatory domain profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all regulatory domain profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A regulatory domain profile contains settings of the country code, calibration channel, and calibration bandwidth, which take effect on APs using the regulatory domain profile.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **14.1.193 regulatory-domain-profile** command to bind the regulatory domain profile to an AP or AP group so that the regulatory domain profile can take effect.

Precautions

- The regulatory domain profile **default** cannot be deleted.
- The regulatory domain profile referenced by an AP or AP group cannot be deleted. To delete the regulatory domain profile, unbind it from the AP or AP group first.

Example

Create the regulatory domain profile **domain1** and display the regulatory domain profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] regulatory-domain-profile name domain1
[Huawei-wlan-regulate-domain-domain1]
```

Related Topics

14.1.117 display regulatory-domain-profile

14.1.193 regulatory-domain-profile

14.1.193 regulatory-domain-profile

Function

The **regulatory-domain-profile** command binds a regulatory domain profile to an AP or AP group.

The **undo regulatory-domain-profile** command unbinds a regulatory domain profile from an AP or AP group.

By default, the regulatory domain profile **default** is bound to an AP group, but no regulatory domain profile is bound to an AP.

Format

regulatory-domain-profile *profile-name*

undo regulatory-domain-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a regulatory domain profile.	The regulatory domain profile must exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a regulatory domain profile using the **14.1.192 regulatory-domain-profile (WLAN view)** command, bind it to an AP or AP group so that the regulatory domain profile can take effect.

Precautions

After a regulatory domain profile is bound to an AP or AP group, parameter settings in the regulatory domain profile apply to all APs using the profile.

Example

Create the regulatory domain profile **domain1** and bind it to AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] regulatory-domain-profile name domain1
[Huawei-wlan-regulate-domain-domain1] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] regulatory-domain-profile domain1
Warning: Modifying the country code will clear channel, power and antenna gain configurations of the
radio and reset the AP. Continu
e?[Y/N]:y
```

Related Topics

14.1.97 display ap-group

14.1.112 display references regulatory-domain-profile

14.1.192 regulatory-domain-profile (WLAN view)

14.1.194 report-disassoc-request disable

Function

The **report-disassoc-request disable** command enables an AP to report disassociation request packets of STAs to the AC.

The **undo report-disassoc-request disable** command disables an AP from reporting disassociation request packets of STAs to the AC.

By default, an AP is enabled to report disassociation request packets of STAs to the AC.

Format

report-disassoc-request disable

 Copyright © Huawei Technologies Co., Ltd.

undo report-disassoc-request disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

If a large number of STAs disassociate from the network in a certain time, the APs need to report lots of disassociation request packets to the AC, impacting the AC performance. To alleviate the impact on the AC, you can disable APs from reporting disassociation request packets of STAs to the AC.

Example

Disable an AP from reporting disassociation request packets of STAs to the AC.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ab
[Huawei-wlan-ap-system-prof-ab] report-disassoc-request disable
```

14.1.195 reset ap offline-record

Function

The **reset ap offline-record** command clears AP offline records.

Format

reset ap offline-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears offline records of all APs.	-
mac *mac-address*	Clears offline records of the AP with specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect AP offline records, run this command to clear existing records.

Precautions

The cleared records cannot be restored.

Example

Clear offline records of all APs.

```
<Huawei> reset ap offline-record all
```

Related Topics

14.1.80 display ap offline-record

14.1.196 reset ap online-fail-record

Function

The **reset ap online-fail-record** command clears AP online failure records.

Format

reset ap online-fail-record { **all** | **mac** *mac-address* }

Parameters

Parameter	Description	Value
all	Clears online failure records of all APs.	-
mac *mac-address*	Clears online failure records of the AP with the specified MAC address.	The AP's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To re-collect records about AP online failures, run this command to clear existing records.

Precautions

The cleared records cannot be restored.

Example

Clear online failure records of all APs.

```
<Huawei> reset ap online-fail-record all
```

Related Topics

14.1.81 display ap online-fail-record

14.1.197 reset ap unauthorized record

Function

The **reset ap unauthorized record** command clears information about unauthenticated APs.

Format

reset ap unauthorized record

Parameters

None

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to clear information about unauthenticated APs so that removed APs or unauthenticated APs that are physically disconnected from the AC can be cleared. This facilitates collecting statistics and confirmation of unauthenticated APs.

Precautions

If an AP physically connects to the AC but has not been authenticated, the AP is added in the unauthenticated AP list after you run the **reset ap unauthorized record** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear information about unauthenticated APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] reset ap unauthorized record
Warning: Clear unauthorized AP record, continue?[Y/N]:y
```

Related Topics

14.1.89 display ap unauthorized record

14.1.198 reset channel switch-record

Function

The **reset channel switch-record** command deletes channel switching records on a device.

Format

reset channel switch-record all

Parameters

Parameter	Description	Value
all	Deletes all channel switching records.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing channel switching records so that the system can record new channel switching events.

Precautions

Deleted channel switching records cannot be restored.

Example

Delete all channel switching records.

```
<Huawei> reset channel switch-record all
```

Related Topics

14.1.101 display channel switch-record

14.1.199 reset mac-address { ap-id | ap-name }

Function

The **reset mac-address** { **ap-id** | **ap-name**} command clears all dynamic MAC address entries on an AP's wired interface.

Format

reset mac-address { **ap-id** *ap-id* | **ap-name** *ap-name* } *interface-type interface-number*

Parameters

Parameter	Description	Value
ap-id *ap-id*	Clears all dynamic MAC address entries on wired interfaces of the AP with the specified ID.	The AP ID must exist.
ap-name *ap-name*	Clears all dynamic MAC address entries on wired interfaces of the AP with the specified name.	The AP name must exist.
interface-type interface-number	Clears dynamic MAC address entries on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the number of the outbound interface.	Currently, only Ethernet interfaces are supported.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Clear dynamic MAC address entries on wired interfaces of the AP with ID 1.

```
<Huawei> reset mac-address ap-id 1 ethernet 0
```

Related Topics

14.1.103 display mac-address { ap-id | ap-name }

14.1.200 reset station assoc-info ap-offline-record

Function

The **reset station assoc-info ap-offline-record** command deletes information about STAs that connect to the APs in fault state.

Format

reset station assoc-info ap-offline-record { **all** | { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] }

Parameters

Parameter	Description	Value
all	Deletes information about all STAs that connect to APs in fault state from the AC.	-
ap-name *ap-name*	Clears information about STAs that go online on the AP with a specified name in fault state.	The AP name must exist.
ap-id *ap-id*	Clears information about STAs that go online on the AP with a specified ID in fault state.	The AP ID must exist.
radio *radio-id*	Deletes information about STAs that connect to the specified radio of the AP in fault state.	The radio ID must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before collecting statistics on the STAs that connect to the APs in fault state within a specific period, run the **reset station assoc-info ap-offline-record** command to delete the original STA information.

Function

The deleted STA information cannot be restored. Exercise caution when you run the **reset station assoc-info ap-offline-record** command.

Example

Delete information about all STAs that connect to APs in fault state from the AC.

```
<Huawei> reset station assoc-info ap-offline-record all
```

Related Topics

14.1.120 display station assoc-info ap-offline-record

14.1.201 reset station offline-record

Function

The **reset station offline-record** command deletes STA offline records.

Format

reset station offline-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac* }

Parameters

Parameter	Description	Value
all	Deletes all STA offline records.	-
ap-name *ap-name*	Deletes STA offline records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Deletes STA offline records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac*	Deletes offline records of a specified STA.	The specified STA MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to delete existing STA offline records so that the system can record new STA offline events.

Precautions

The deleted STA offline records cannot be restored.

Example

Delete all STA offline records.

```
<Huawei> reset station offline-record all
```

Related Topics

14.1.122 display station offline-record

14.1.202 reset station online-fail-record

Function

The **reset station online-fail-record** command clears STA online failure records.

Format

reset station online-fail-record { **all** | **ap-name** *ap-name* | **ap-id** *ap-id* | **sta-mac** *sta-mac-address* }

Parameters

Parameter	Description	Value
all	Clears online failure records of all STAs.	-
ap-name *ap-name*	Clears STA online failure records on the AP with a specified name.	The AP name must exist.
ap-id *ap-id*	Clears STA online failure records on the AP with a specified ID.	The AP ID must exist.
sta-mac *sta-mac-address*	Clears online failure records of the STA with the specified MAC address.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To re-collect records about STA online failures, run this command to clear existing records.

Precautions

The cleared records cannot be restored.

Example

Clear online failure records of all STAs.

```
<Huawei> reset station online-fail-record all
```

Related Topics

14.1.121 display station online-fail-record

14.1.203 reset station statistics

Function

The **reset station statistics** command deletes statistics about online STAs.

Format

reset station statistics [**sta-mac** *sta-mac-address*]

Parameters

Parameter	Description	Value
sta-mac *sta-mac-address*	Specifies the MAC address of an online STA.	The STA's MAC address must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about online STAs, run the command to clear the existing statistics.

Precautions

After the command is run, statistics about online STAs are cleared and cannot be restored.

Example

Delete statistics about the STA with MAC address 286e-d488-b74f.

```
<Huawei> reset station statistics sta-mac 286e-d488-b74f
```

Related Topics

14.1.123 display station statistics

14.1.204 reset statistics

Function

The **reset statistics** command clears device statistics.

Format

reset statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } [**ssid** *ssid*]

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears statistics about the AP with the specified name.	The AP name must exist.
ap-id *ap-id*	Clears statistics about the AP with the specified ID.	The AP ID must exist.
ssid *ssid*	Clears statistics about a specified SSID.	The SSID must exist.

Views

WLAN view

Default Level

3: Management level

Usage Guidelines

You can run the **reset statistics** command to clear device statistics.

Example

Clear AP statistics.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system view
[Huawei] wlan ac
[Huawei-wlan-view] reset statistics ap-name area1
```

14.1.205 rf-ping

Function

The **rf-ping** command enables an AC to automatically detect wireless link quality.

Format

rf-ping [**-m** *time* | **-c** *number*] * *mac-address*

Parameters

Parameter	Description	Value
-m *time*	Specifies the interval for sending probe data packets.	The value is an integer that ranges from 100 to 10000, in milliseconds. The default value is 1000.
-c *number*	Specifies the number of probe data packets sent by the AC.	The value is an integer that ranges from 1 to 1000. The default value is 1.
mac-address	MAC address of a STA.	The value is in H-H-H format. An H is a hexadecimal number of four digits.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

This command allows an AC to automatically detect wireless link quality based on link parameters, including the signal strength, data rate on air port, and delay in packet transmission.

Prerequisites

STAs have been associated with the APs and go online.

Example

Configure an AC to automatically detect quality of the link between the AP and STA with the MAC address 14cf-9202-13dc.

```
<Huawei> system-view
[Huawei] wlan ac
```

```
[Huawei-wlan-view] rf-ping 14cf-9202-13dc
 Tx rate=52.0 Mbps, Reply from 14cf-9202-13dc: RSSI=-58 dBm time < 1 ms
 1 packets transmitted, 1 received, 0% packet loss, time < 1 ms, RSSI -58 dBm
```

Table 14-87 Description of the **rf-ping** command output

Item	Description
Tx rate	Transmission rate.
RSSI	Received signal strength.
time	Packet transmission delay.

14.1.206 rts-cts-mode

Function

The **rts-cts-mode** command sets the request to send (RTS)-clear to send (CTS) operation mode in a radio profile.

The **undo rts-cts-mode** command restores the default RTS-CTS operation mode in a radio profile.

By default, the RTS-CTS operation mode is **cts-to-self**.

Format

rts-cts-mode { **cts-to-self** | **disable** | **rts-cts** }

undo rts-cts-mode

Parameters

Parameter	Description	Value
cts-to-self	Sets the RTS-CTS operation mode to cts-to-self.	-
disable	Disables RTS-CTS.	-
rts-cts	Sets the RTS-CTS operation mode to rts-cts.	-

Views

2G radio profile view, 5G radio profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

- In rts-cts mode, when an AP needs to send data to a STA, the AP sends an RTS packet to all STAs associated with it. After receiving the RTS packet, none of the devices within the AP's coverage area sends data within a specified period. After the destination STA receives the RTS packet, it sends a CTS packet. After receiving the CTS packet, none of the devices within the STA's coverage area sends data within a specified period. Using the rts-cts mode to avoid conflicts requires two packets (RTS and CTS packets), increasing packet overhead.
- In cts-to-self mode, when an AP needs to send data to STAs, it sends a CTS packet with its IP address as the source and destination addresses. Then none of the devices within the AP's coverage area sends data within a specified period. In cts-to-self mode, an AP only needs to send a CTS packet to avoid channel conflicts in most scenarios. However, if there is a device within the STA's coverage area but not within the AP's coverage area, a channel conflict may still occur.

Compared to the rts-cts mode, the cts-to-self mode reduces the number of control packets sent on the network. In some situations, however, a channel conflict may still occur when hidden nodes do not receive the CTS packet from the AP. Therefore, the rts-cts mode is more effective in avoiding channel conflicts than the cts-to-self mode.

To avoid a data transmission failure caused by channel conflicts, run the **rts-cts-mode** command to set the RTS-CTS operation mode in a radio profile according to networking requirements.

Example

Set the RTS-CTS operation mode to **rts-cts** in the 2G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] rts-cts-mode rts-cts
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.207 rts-cts-threshold

Function

The **rts-cts-threshold** command sets the RTS-CTS threshold in a radio profile.

The **undo rts-cts-threshold** command restores the default RTS-CTS threshold in a radio profile.

The default RTS-CTS alarm threshold is 2347 bytes.

 Copyright © Huawei Technologies Co., Ltd.

Format

rts-cts-threshold *rts-cts-threshold*

undo rts-cts-threshold

Parameters

Parameter	Description	Value
rts-cts-threshold	Specifies the RTS-CTS threshold. If the length of a frame to be sent by the MAC Layer exceeds this threshold, an RTS frame needs to be sent before this frame.	The value is an integer that ranges from 64 to 2347, in bytes.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

The IEEE 802.11 MAC protocol provides an RTS-CTS handshake protocol to prevent conflicts between channels and failure to transmit data. STA A sends an RTS frame before sending data to STA B. STA A can send data after receiving a CTS frame from STA B. If multiple STAs send RTS frames to an STA, only the STA that receives a CTS frame can send data, and other STAs have channel conflicts by default and must wait and send RTS frames again.

If STAs implement RTS-CTS handshakes before sending data, the channel bandwidth is consumed by too much RTS frames. You can set an RTS threshold to specify the length of frames to be sent. When the length of frames to be sent by the STA is smaller than the RTS threshold, no RTS/CTS handshake is implemented.

Example

Set the RTS-CTS threshold to 2300 bytes in the 2G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] rts-cts-threshold 2300
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.208 service-vlan

Function

The **service-vlan** command configures a service VLAN for a VAP.

The **undo service-vlan** command restores the default service VLAN of a VAP.

By default, VLAN 1 is the service VLAN of a VAP.

Format

service-vlan { **vlan-id** *vlan-id* }

undo service-vlan

Parameters

Parameter	Description	Value
vlan-id *vlan-id*	Sets the service VLAN of a VAP to a specific VLAN.	The value is an integer that ranges from 1 to 4094.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can specify a specific VLAN as the service VLAN of a VAP. Layer 2 data packets delivered from the VAP to an AP carry the service VLAN IDs.

- When a specific VLAN is configured as the service VLAN of a VAP, STAs connected to the VAP join the same VLAN.

Precautions

Modifying the service VLAN of a VAP will interrupt services of STAs connected to the VAP. Exercise caution when you run the command.

Example

Set the service VLAN to VLAN2 in the VAP profile **vap1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] service-vlan vlan-id 2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.127 display vap-profile

14.1.209 set workmode wlan

Function

The **set workmode wlan** command configures the WLAN mode of the device.

By default, the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW work in AP mode and other devices work in AC mode.

Format

set workmode wlan { **ap** | **ac** }

Parameters

Parameter	Description	Value
ap	Indicates that the device works in Fat AP mode.	-
ac	Indicates that the device works in AC mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Fat AP mode, the device functions as an access point (AP) to provide access control, authentication, data encryption, and QoS functions.

In AC mode, the device functions as the access controller (AC) to deploy and control APs. The AC implements functions including mobility management, identity verification, VLAN assignment, radio resource management, wireless Intrusion Detection System (IDS), and data packet forwarding. APs only send and

 Copyright © Huawei Technologies Co., Ltd.

receive wireless data, simplifying AP management and configuration. APs can even work without any configuration.

Example

Configure the device to work in AC mode.

```
<Huawei> system-view
[Huawei] set workmode wlan ac
Warning: The WorkMode Change will be activated after board reboot. Continue? [y/n]:y
[Huawei] quit
<Huawei> reboot fast
System will reboot! Continue ? [y/n]:y
Info: system is rebooting ,please wait...
```

14.1.210 sftp server disable

Function

The **sftp server disable** command disables the SFTP server function on an AP.

The **undo sftp server disable** command enables the SFTP server function on an AP.

By default, the SFTP server function is enabled on an AP.

Format

sftp server disable

undo sftp server disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to an SFTP-enabled AP from a user terminal for file management. Instead, you can log in to the SFTP-enabled AP through SFTP to manage files of the AP.

Example

Disable the SFTP server function on an AP.

```
<Huawei> system-view
[Huawei] wlan ac
```

```
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] sftp server disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.211 short-preamble disable

Function

The **short-preamble disable** command configures a radio profile not to support the short preamble.

The **undo short-preamble disable** command configures a radio profile to support the short preamble.

By default, a radio profile supports the short preamble.

Format

short-preamble disable

undo short-preamble disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

The preamble is a section of bits in the header of a data frame. It synchronizes signals transmitted between the sender and receiver. The preamble is classified into the long preamble and short preamble. The short preamble ensures better synchronization performance and therefore is recommended. The long preamble is usually used for compatibility with earlier network adapters of clients.

Example

Configure the 2G radio profile **default** not to support the short preamble.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] short-preamble disable
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.1.212 shutdown (AP wired port link profile view)

Function

The **shutdown** command shuts down an AP's wired interface.

The **undo shutdown** command enables an AP's wired interface.

By default, an AP's wired interface is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

AP wired port link profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If malicious users launch attacks to the network through an AP's wired interface, the administrator can deliver the **shutdown** command on the AC to shut down the interface.

Precautions

Data frames may be lost if you shut down an interface during data transmission. Exercise caution when you use the **shutdown** command.

The **shutdown** command still takes effect after an AP is restarted.

The **shutdown** command takes effect only on AP's wired interfaces working in **endpoint** or **middle** mode but not on those working in **root** mode.

Example

Shut down the AP's wired interface GE0.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] port-link-profile name port-link1
[Huawei-wlan-port-link-prof-port-link1] shutdown
Warning: The AP may become out of management after the port is disabled (if the port is an uplink port).
Continue?[Y/N]:y
```

Related Topics

14.1.104 display port-link-profile

14.1.213 snmp-agent trap enable feature-name wlan

Function

The **snmp-agent trap enable feature-name wlan** command enables the trap function for the WLAN module.

The **undo snmp-agent trap enable feature-name wlan** command disables the trap function for the WLAN module.

By default, the trap function is enabled for the WLAN module.

Format

snmp-agent trap enable feature-name wlan [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name wlan [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the name of a trap.	The value is a string and must be set according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can specify **trap-name** to enable the trap function for one or more events of the WLAN module.

Example

Enable the hwapfaulttrap trap.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name wlan trap-name hwapfaulttrap
```

 Copyright © Huawei Technologies Co., Ltd.

14.1.214 ssid

Function

The **ssid** command sets a service set identifier (SSID) for an SSID profile.

The **undo ssid** command deletes the SSID of an SSID profile.

By default, the SSID **HUAWEI-WLAN** is configured in an SSID profile.

Format

ssid *ssid*

undo ssid

Parameters

Parameter	Description	Value
ssid	Specifies the name of an SSID.	The value is in text format and can contain 1 to 32 case-sensitive characters. It does not support Chinese characters. **NOTE** You can only use a command editor of the UTF-8 encoding format to edit Chinese characters. SSIDs containing Chinese characters cannot be displayed on STAs that do not support the UTF-8 encoding format.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

An SSID specifies a wireless network. When you search for available wireless networks on your wireless terminal, SSIDs are displayed to identify the available wireless networks.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the SSID to **wlan-net** in the SSID profile **ssid1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] ssid wlan-net
Warning: This action may cause service interruption. Continue?[Y/N]y
```

Related Topics

14.1.118 display ssid-profile

14.1.215 ssid-hide enable

Function

The **ssid-hide enable** command enables SSID hiding in Beacon frames in an SSID profile.

The **undo ssid-hide enable** command disables SSID hiding in Beacon frames in an SSID profile.

By default, SSID hiding in Beacon frames is disabled in an SSID profile.

Format

ssid-hide enable

undo ssid-hide enable

Parameters

None

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

A STA listens on the Beacon frames that an AP periodically sends in each channel to obtain AP information. The STA can obtain SSIDs from Beacon frames that contain the SSIDs.

The STA can actively send a probe frame with a specified SSID, only the AP with the same SSID will respond to the STA. If the STA broadcasts a probe frame without an SSID, only the APs on which SSID hiding in Beacon frames is disabled will respond to the STA.

- After the **ssid-hide enable** command is used, an AP periodically sends Beacon frames that contain empty SSID character strings and does not reply to the

broadcast probe requests sent from STAs. The STAs can send probe frames with the AP's SSID to discover the SSID.

- After the **undo ssid-hide enable** command is used, an AP periodically sends Beacon frames that contain valid SSID character strings and replies to the broadcast probe requests sent from STAs. The STAs can send probe frames with the AP's SSID to discover the SSID.

Example

Configure SSID hiding in Beacon frames in the SSID profile **ssid1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] ssid-hide enable
```

Related Topics

14.1.118 display ssid-profile

14.1.216 ssid-profile (WLAN view)

Function

The **ssid-profile** command creates an SSID profile and displays the SSID profile view, or displays the view of an existing SSID profile.

The **undo ssid-profile** command deletes an SSID profile.

By default, the system provides the SSID profile **default**.

Format

ssid-profile name *profile-name*

undo ssid-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an SSID profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all SSID profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSID profile is mainly used to configure STA association and access parameters based on SSIDs, including the SSID name, STA association timeout period, and legacy terminal access.

Follow-up Procedure

Run the **14.1.217 ssid-profile (VAP profile view)** command to bind the SSID profile to a VAP profile and run the **14.1.234 vap-profile** command to bind the VAP profile to an AP group, AP, AP radio, or AP group radio so that the SSID profile can take effect.

Precautions

- The SSID profile **default** cannot be deleted.
- The SSID profile referenced by a VAP profile cannot be deleted. To delete the SSID profile, unbind it from the VAP profile first.
- If the VAP profile has been applied to an AP group or an AP, modifying the SSID profile will interrupt services.

  ```
  Warning: This action may cause service interruption. Continue?[Y/N]
  ```

Example

Create an SSID profile **ssid1** and enter the SSID profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1]
```

Related Topics

14.1.127 display vap-profile

14.1.217 ssid-profile (VAP profile view)

14.1.217 ssid-profile (VAP profile view)

Function

The **ssid-profile** command binds an SSID profile to a VAP profile.

The **undo ssid-profile** command unbinds an SSID profile from a VAP profile.

By default, the SSID profile **default** is bound to a VAP profile.

Format

ssid-profile *profile-name*

undo ssid-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an SSID profile.	The SSID profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an SSID profile using the **14.1.216 ssid-profile (WLAN view)** command, bind it to a VAP profile to make the SSID profile take effect.

Precautions

After an SSID profile is bound to a VAP profile, parameter settings in the SSID profile take effect on all APs using the VAP profile.

Example

Create the SSID profile **ssid1** and bind it to the VAP profile **vap1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name ssid1
[Huawei-wlan-ssid-prof-ssid1] quit
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] ssid-profile ssid1
```

Related Topics

14.1.113 display references ssid-profile

14.1.127 display vap-profile

14.1.216 ssid-profile (WLAN view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.218 stelnet server disable

Function

The **stelnet server disable** command disables the STelnet server function on an AP.

The **undo stelnet server disable** command enables the STelnet server function on an AP.

By default, the STelnet server function is enabled on an AP.

Format

stelnet server disable

undo stelnet server disable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to an STelnet-enabled AP from a user terminal to maintain it locally. Instead, you can log in to the STelnet-enabled AP through STelnet to remotely configure and maintain it.

Example

Disable the STelnet server function on an AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] stelnet server disable
```

Related Topics

14.1.98 display ap-system-profile

14.1.219 telnet enable

Function

The **telnet enable** command enables Telnet on an AP.

The **undo telnet enable** command disables Telnet on an AP.

By default, Telnet is disabled on an AP.

Format

telnet enable

undo telnet enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

You do not need to log in to a Telnet-enabled AP from a user terminal to maintain it locally. Instead, you can log in to the Telnet-enabled AP through Telnet to remotely configure and maintain it.

To improve login security, you are advised to run the **undo stelnet server disable** command to enable the STelnet server function and log in to the AP through STelnet.

Example

Enable Telnet on an AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] telnet enable
```

Related Topics

14.1.98 display ap-system-profile

14.1.218 stelnet server disable

14.1.220 temporary-management enable (AP system profile view)

Function

The **temporary-management enable** command enables offline management VAP and antenna alignment VAP functions.

The **undo temporary-management enable** command disables offline management VAP and antenna alignment VAP functions.

By default, offline management VAP and antenna alignment VAP functions are disabled.

Format

temporary-management enable

undo temporary-management enable

Parameters

None

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- APs are often installed in hidden places or at high positions. When an AP becomes faulty, it is inconvenient to connect to the AP through a console port or network cable to troubleshoot faults.

  After the offline management VAP function is enabled for an AP, the AP automatically generates a management VAP when it becomes faulty. The default SSID and password of the management VAP are **hw_manage_xxxx** and **hw_manage** respectively. **xxxx** indicates the last four bits of the AP's MAC address. To troubleshoot the AP fault, the maintenance personnel only need to set the IP address of the maintenance device to 169.254.2.x/16 (except 169.254.2.1. This IP address is used only to facilitate fault location and needs to be changed when fault location is completed), associate the device to the wireless network with SSID **hw_manage_xxxx**, and connect to the AP using Telnet. This prevents complex operations.
- After the antenna alignment VAP function is enabled for an AP, the AP automatically generates an antenna alignment VAP when it works properly. The default SSID and password of the management VAP are **hw_manage_xxxx** and **hw_manage** respectively. **xxxx** indicates the last four bits of the AP's MAC address. You can associate the mobile phone on which the antenna alignment APP is installed to the wireless network with SSID **hw_manage_xxxx** and use the phone to receive packets sent by the antenna alignment VAP to obtain RSSI information.

Precautions

- After the offline management VAP and antenna alignment VAP functions are enabled, the administrator needs to change the SSIDs and passwords of the

offline management VAP and antenna alignment VAP. Using the default values brings security threats. Any wireless user may use the default SSIDs and passwords to log in to the offline AP and perform unauthorized operations or receive packets sent by the antenna alignment APP. In actual applications, the maintenance personnel may enable the offline management VAP and antenna alignment VAP functions to facilitate AP maintenance. Using the default offline management VAP and antenna alignment VAP is not recommended. To ensure security, the administrator needs to configure a secure VAP profile, set new SSIDs and passwords, and run the **temporary-management enable** command in the VAP profile view to specify the VAPs generated after the VAP profile is bound to an AP group or AP as the offline management VAP and antenna alignment VAP to replace the default offline management VAP and antenna alignment VAP.

- The offline management VAP takes effect only when an AP goes offline unexpectedly.
- The offline management VAP works only on the 2.4 GHz radio. If the 2.4 GHz radio is occupied by the WDS bridge, the offline management VAP function cannot be used.
- Before using the offline management VAP function, ensure that the AP has enabled with Telnet services.
- The antenna alignment VAP is automatically deleted 24 hours after it is created. If you want to use an antenna alignment VAP after the deletion, run the **undo temporary-management enable** and then run the **temporary-management enable** commands in the AP profile view in succession to create a new antenna alignment VAP.
- After the offline management VAP function is enabled, an RRU automatically generates an offline management VAP when it is disconnected from the central AP. Packets of the offline management VAP are only processed on the RRU and wil not be forwarded to the central AP. If the link between the central AP and AC is disconnected, all online RRUs on the central AP will automatically generate an offline management VAP, and send packets of the VAPs to the central AP for processing. The central AP does not have radios and therefore do not generate an offline management VAP.

Example

Enable offline management VAP and antenna alignment VAP functions.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name apsys1
[Huawei-wlan-ap-system-prof-apsys1] temporary-management enable
```

Related Topics

14.1.98 display ap-system-profile
14.1.221 temporary-management enable (VAP profile view)

14.1.221 temporary-management enable (VAP profile view)

Function

The **temporary-management enable** command configures a VAP as the offline management VAP or antenna alignment VAP.

The **undo temporary-management enable** command restores a VAP to the default setting.

By default, a VAP is a service VAP.

Format

temporary-management enable

undo temporary-management enable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- After the offline management VAP function is enabled using the **temporary-management enable** command in the AP system profile view, an AP automatically generates a management VAP when it becomes faulty. The default SSID and password of the management VAP are **hw_manage_xxxx** and **hw_manage** respectively. **xxxx** indicates the last four bits of the AP's MAC address. The maintenance personnel can associate the maintenance device to the default VAP and log in to the AP using Telnet to troubleshoot the fault. However, using the default management VAP brings security risks. Any wireless user may use the default SSID and password to log in to the offline AP and perform unauthorized operations.
- After the antenna alignment VAP function is enabled using the **temporary-management enable** command in the AP system profile view, an AP automatically generates an antenna alignment VAP when it works properly. The default SSID and password of the management VAP are **hw_manage_xxxx** and **hw_manage** respectively. **xxxx** indicates the last four bits of the AP's MAC address. Using the default antenna alignment VAP also brings security risks.

To improve security of the offline management VAP and antenna alignment VAP, bind a security profile of a high security level to a VAP profile, set new SSIDs and

passwords, configure the VAPs generated by the VAP profile as the offline management VAP and antenna alignment VAP, and bind the VAP profile to an AP group or AP to replace the default offline management VAP and antenna alignment VAP.

Follow-up Procedure

Run the **temporary-management enable** command to enable the offline management VAP and antenna alignment VAP functions in the AP system profile view to make the offline management VAP and antenna alignment VAP in the VAP profile take effect.

Precautions

- If the VAPs are configured as the offline management VAP and antenna alignment VAP in a VAP profile, the security profile referenced by the VAP profile supports only the WEP or WPA/WPA2 PSK security policy.
- If the VAPs are configured as the offline management VAP and antenna alignment VAP in a VAP profile, VAPs generated by the VAP profile cannot be used as service VAPs for service transmission.
- The offline management VAP and antenna alignment VAP cannot be modified. To modify the VAPs, delete them first, and then modify the VAP attributes in the VAP profile view.
- The offline management VAP works only on the 2.4 GHz radio. If the 2.4 GHz radio is occupied by the WDS bridge, the offline management VAP function cannot be used.
- The offline management VAP function and service holding upon CAPWAP link disconnection are mutually exclusive. When the two functions are configured at the same time, the offline management VAP function cannot take effect.

Example

Configure VAPs generated by the VAP profile **vap1** as the offline management VAP and antenna alignment VAP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] temporary-management enable
```

Related Topics

14.1.98 display ap-system-profile

14.1.220 temporary-management enable (AP system profile view)

14.1.222 traffic-optimize (AP wired port profile view)

Function

The **traffic-optimize** command sets the maximum volume of broadcast, multicast, or unknown unicast traffic on an AP's wired interface.

The **undo traffic-optimize** command restores the default maximum volume of broadcast, multicast, or unknown unicast traffic on an AP's wired interface.

By default, the volume of broadcast, multicast, or unknown unicast traffic is not suppressed on an AP's wired interface.

Format

traffic-optimize { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** } **packets** *packets-rate*

undo traffic-optimize { **broadcast-suppression** | **multicast-suppression** | **unicast-suppression** }

Parameters

Parameter	Description	Value
broadcast-suppression	Specifies the maximum broadcast traffic volume allowed on an AP's wired interface.	-
multicast-suppression	Specifies the maximum multicast traffic volume allowed on an AP's wired interface.	-
unicast-suppression	Specifies the maximum unknown unicast traffic volume allowed on an AP's wired interface.	-
packets *packets-rate*	Specifies the maximum number of packets that can pass every second.	The value is an integer that ranges from 0 to 14881000, in pps.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of broadcast, multicast, and unknown unicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected. When the traffic volume of broadcast, multicast, and unknown unicast packets reaches the maximum on an AP's wired interface, the system discards excess packets to control the traffic volume in a proper range and prevent flooding attacks.

Follow-up Procedure

Bind the AP wired port profile to an AP group or AP.

Precautions

The uplink interfaces of RRUs do not support this command.

Example

Set the maximum broadcast traffic volume allowed on an AP's wired interface to 21600 pps.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wire1
[Huawei-wlan-wired-port-wire1] traffic-optimize broadcast-suppression packets 21600
```

Related Topics

14.1.128 display wired-port-profile

14.1.223 traffic-optimize broadcast-suppression

Function

The **traffic-optimize broadcast-suppression** command sets the maximum traffic volume of broadcast packets that can pass through a traffic profile.

The **undo traffic-optimize broadcast-suppression** command cancels the limit on the maximum traffic volume of broadcast packets that can pass through a traffic profile.

By default, broadcast packets are not suppressed on a traffic profile.

Format

traffic-optimize broadcast-suppression packets *packets-rate*

undo traffic-optimize broadcast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value is an integer that ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When a large number of broadcast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To prevent broadcast storms, you can run the **traffic-optimize broadcast-suppression** command to configure the maximum traffic volume of broadcast packets that can pass through a traffic profile. When the traffic volume of broadcast packets reaches the maximum in a traffic profile, the system discards excess broadcast packets to control the traffic volume in a proper range.

Example

Set the maximum traffic volume of broadcast packets that can pass through 21600 pps in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize broadcast-suppression packets 21600
```

14.1.224 traffic-optimize multicast-suppression

Function

The **traffic-optimize multicast-suppression** command sets the maximum traffic volume of multicast packets in a traffic profile.

The **undo traffic-optimize multicast-suppression** command cancels the limit on the maximum traffic volume of multicast packets in a traffic profile.

By default, multicast packets are not suppressed in a traffic profile.

Format

traffic-optimize multicast-suppression packets *packets-rate*

undo traffic-optimize multicast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

When a large number of multicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

To ensure normal service transmission on a network, you can run the **traffic-optimize multicast-suppression** command to configure the maximum multicast traffic volume in a traffic profile. When the traffic volume of multicast packets reaches the maximum, the system discards excess multicast packets to control the traffic volume in a proper range.

Example

Set the maximum traffic volume of multicast packets to 21600 pps in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize multicast-suppression packets 21600
```

14.1.225 traffic-optimize multicast-unicast enable

Function

The **traffic-optimize multicast-unicast enable** command enables the function of converting multicast packets to unicast packets in a traffic profile.

The **undo traffic-optimize multicast-unicast enable** command disables the function of converting multicast packets to unicast packets in a traffic profile.

By default, the function of converting multicast packets to unicast packets is disabled in a traffic profile.

Format

traffic-optimize multicast-unicast enable

undo traffic-optimize multicast-unicast enable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can enable the function of converting multicast packets to unicast packets in scenarios that have high requirements on multicast stream transmission, such as a high-definition video on-demand scenario.

After the function is enabled, an AP listens on Report and Leave packets to maintain multicast-to-unicast entries. When sending multicast packets to the client, the AP converts the multicast packets to unicast packets based on the multicast-to-unicast entries to improve multicast stream transmission efficiency.

Example

Enable the function of converting multicast packets to unicast packets in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize multicast-unicast enable
```

14.1.226 traffic-optimize sta-bridge-forward disable

Function

The **traffic-optimize sta-bridge-forward disable** command forbids an air interface to forward packets to bridging terminals.

The **undo traffic-optimize sta-bridge-forward disable** command cancels of the configuration of forbidding an air interface to forward packets to bridging terminals.

By default, an air interface is allowed to forward packets to bridging terminals.

Format

traffic-optimize sta-bridge-forward disable

undo traffic-optimize sta-bridge-forward disable

Parameters

None

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Some terminals on the wireless network can provide bridging functions. The terminals associate with APs with their MAC addresses and connect to multiple Layer 3 wired devices in the downlink direction. The connected Layer 3 wired devices can also obtain IP addresses and forward traffic through the APs. The APs

consider that the associated terminals have multiple IP addresses. You can run the command to forbid air interfaces to forward packets to bridging terminals. This can reduce the number of packets transmitted on the air interfaces and improve the air interface performance.

Example

Forbid an air interface to forward packets to bridging terminals in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize sta-bridge-forward disable
```

14.1.227 traffic-optimize unicast-suppression

Function

The **traffic-optimize unicast-suppression** command sets the maximum traffic volume of unknown unicast packets in a traffic profile.

The **undo traffic-optimize unicast-suppression** command cancels the limit on the maximum traffic volume of unknown unicast packets in a traffic profile.

By default, unknown unicast packets are not suppressed in a traffic profile.

Format

traffic-optimize unicast-suppression packets *packets-rate*

undo traffic-optimize unicast-suppression

Parameters

Parameter	Description	Value
packets *packets-rate*	Specifies the number of packets transmitted per second.	The value ranges from 0 to 14881000, in pps.

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

When a large number of unknown unicast packets are transmitted on a network, a lot of network resources are occupied, and services on the network are affected.

 Copyright © Huawei Technologies Co., Ltd.

To prevent broadcast storms, you can run the **traffic-optimize unicast-suppression** command to configure the maximum traffic volume of unknown unicast packets that can pass through an interface. When the traffic volume of unknown unicast packets reaches the maximum on an interface, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Example

Set the maximum traffic volume of unknown unicast packets to 21600 pps in the traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] traffic-optimize unicast-suppression packets 21600
```

14.1.228 traffic-profile (VAP profile view)

Function

The **traffic-profile** command binds a traffic profile to a VAP profile.

The **undo traffic-profile** command unbinds a traffic profile from a VAP profile.

By default, the traffic profile **default** is bound to a VAP profile.

Format

traffic-profile *profile-name*

undo traffic-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a traffic profile.	The traffic profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **traffic-profile** command to bind a traffic profile to a VAP profile. The traffic profile applies to all users using the VAP profile.

Prerequisites

The traffic profile has been created using the **14.1.229 traffic-profile (WLAN view)** command.

Example

Create VAP profile **p1** and bind traffic profile **u1** to the VAP profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name p1
[Huawei-wlan-vap-prof-p1] traffic-profile u1
```

Related Topics

14.1.229 traffic-profile (WLAN view)

14.1.124 display traffic-profile

14.1.229 traffic-profile (WLAN view)

Function

The **traffic-profile** command creates a traffic profile and displays the traffic profile view, or displays the view of an existing traffic profile.

The **undo traffic-profile** command deletes a traffic profile.

By default, the system provides the traffic profile **default**.

Format

traffic-profile name *profile-name*

undo traffic-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a traffic profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all traffic profiles.	–

 Copyright © Huawei Technologies Co., Ltd.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

- The **traffic-profile** command applies to the following situations:
  - To apply priority mapping and traffic suppression functions to a VAP, create a traffic profile and bind the traffic profile to the VAP profile.
  - To change priority mapping and traffic suppression functions of a VAP, enter the traffic profile view of the VAP to modify the required parameters. When a traffic profile is not required, delete it.
- After a traffic profile is created, parameters in the profile use default values.

NOTE

- The profile name is mandatory when you create a profile.
- The traffic profile referenced by a VAP profile cannot be deleted. To delete the traffic profile, unbind it from the VAP profile first.

Example

Create traffic profile **p1** and enter the traffic profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1]
```

Related Topics

14.1.124 display traffic-profile

14.1.230 type (VAP profile view)

Function

The **type** command sets the type for a VAP.

The **undo type** command restores the default VAP type.

By default, the type of a VAP is service.

Format

type { **ap-management** | **service** }

undo type

Parameters

Parameter	Description	Value
ap-management	Sets the type to AP management.	-
service	Sets the type to service.	-

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

- If the type of a VAP is set to **service**, STAs connected to the VAP can only access network resources but not APs. Service VAPs are used in regular WLAN deployment scenarios.
- If the type of a VAP is set to **ap-management**, STAs connected to the VAP can only access APs but not network resources. AP management VAPs are used in STA access and AP management scenarios.

Precautions

After the VAP type is configured in the VAP profile view, the VAPs generated by the VAP profile use the configured VAP type. The new VAP type will overwrite the old one.

If the type of a VAP is AP management, the VAP does not support portal, MAC address and 802.1X authentication using an external server.

After the VAP type is set to management AP, configure an IP address in the same network segment as the AP for a STA, so that the STA can access the AP.

Example

Create the VAP profile **vap1** and set the VAP type to AP management VAP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] type ap-management
```

Related Topics

14.1.127 display vap-profile

14.1.231 undo ap

Function

The **undo ap** command deletes an AP.

Format

undo ap { **ap-name** *ap-name* | **ap-id** *ap-list* | **ap-mac** *ap-mac* | **ap-group** *group-name* | **all** }

Parameters

Parameter	Description	Value
ap-name *ap-name*	Deletes the AP with the specified AP name.	The AP name must exist.
ap-id *ap-list*	Deletes APs with the specified IDs in a batch.	The value is a string of 1 to 255 characters. When multiple APs are selected, use commas (,) or hyphens (-) to separate AP IDs. For example, 5,8,10-13,20 indicates the list of APs with IDs 5, 8, 10, 11, 12, 13, and 20.
ap-mac *ap-mac*	Deletes the AP with the specified MAC address.	The AP's MAC address must exist.
ap-group *group-name*	Deletes the AP in a specified AP group.	The AP group must exist.
all	Deletes all APs.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

If you do not want a specified AP to go online on the AC, run the command to delete the AP from the AC. After the AP is deleted, the AP goes offline from the AC.

Configuration Impact

Deleting an AP will interrupt services of STAs connected to the AP.

Example

Delete the AP named **Area_1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] undo ap ap-name Area_1
Warning: Deleting the AP will interrupt user services. Continue?[Y/N]:y
```

Related Topics

14.1.70 display ap

14.1.232 utmost-power disable

Function

The **utmost-power disable** command disables radios from sending packets at maximum power.

The **undo utmost-power disable** command enables radios to send packets at maximum power.

By default, a radio can send packets at maximum power.

Format

utmost-power disable

undo utmost-power disable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command takes effect only for the country code CN. You can use the command to configure a radio to send packets at maximum power supported by

the radio or maximum power allowed by the country code. After a radio is disabled from sending packets at maximum power, the radio uses the maximum power allowed by the country code to send packets.

Except the country code CN, a radio can only send packets using the maximum power allowed by the country codes.

Precautions

Only radios of the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN can send packets at maximum power.

Example

Disable radios from sending packets at maximum power.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] utmost-power disable
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.233 vap-profile (WLAN view)

Function

The **vap-profile** command creates a VAP profile and displays the VAP profile view, or displays the view of an existing VAP profile.

The **undo vap-profile** command deletes a VAP profile.

By default, the system provides the VAP profile **default**.

Format

vap-profile name *profile-name*

undo vap-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a VAP profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all VAP profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a radio profile is applied in the AP group view, AP view, AP radio view, or AP group radio view, the AP can transmit and receive radio signals. After a VAP profile is applied in the AP group view, AP view, AP radio view, or AP group radio view, VAPs are generated and provide wireless access services for STAs. You can configure parameters in the VAP profile to enable APs to provide different wireless services.

Follow-up Procedure

Run the **14.1.234 vap-profile** command to apply the VAP profile in the AP group view, AP view, AP radio view, or AP group radio view so that the VAP profile can take effect.

Precautions

- The VAP profile **default** cannot be deleted.
- The VAP profile referenced in the AP group view, AP view, AP radio view, or AP group radio view cannot be deleted. To delete the VAP profile, unbind it from the AP group view, AP view, AP radio view, or AP group radio view first.
- By default, the SSID profile **default**, security profile **default**, and traffic profile **default** are bound to a VAP profile.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a VAP profile **vap1** and enter the VAP profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1]
```

Related Topics

14.1.127 display vap-profile

14.1.234 vap-profile

14.1.234 vap-profile

Function

The **vap-profile** command binds a VAP profile to a radio.

The **undo vap-profile** command unbinds a VAP profile from a radio.

By default, no VAP profile is bound to a radio.

Format

vap-profile *profile-name* **wlan** *wlan-id* { **radio** { *radio-id* | **all** } }

undo vap-profile *profile-name* **wlan** *wlan-id* { **radio** { *radio-id* | **all** } }

radio { *radio-id* | **all** } is supported only in the AP group view and AP view.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a VAP profile.	The VAP profile must exist.
wlan *wlan-id*	Specifies the WLAN ID of a VAP.	The value is an integer that ranges from 1 to 16.
radio	Specifies a radio.	-
radio-id	Specifies a radio ID.	The value is an integer that ranges from 0 to 2.
all	Specifies all radios.	-

Views

AP group view, AP view, AP radio view, AP group radio view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create a VAP profile using the **14.1.233 vap-profile (WLAN view)** command, bind it to a radio so that the VAP profile can take effect.

Precautions

After a VAP profile is bound to a radio, parameter settings in the VAP profile apply to the radio using the profile.

Example

Create the VAP profile **vap1** and bind it to AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name vap1
[Huawei-wlan-vap-prof-vap1] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] vap-profile vap1 wlan 1 radio 0
```

Related Topics

14.1.97 display ap-group

14.1.115 display references vap-profile

14.1.233 vap-profile (WLAN view)

14.1.235 vht a-mpdu max-length-exponent

Function

The **vht a-mpdu max-length-exponent** command sets the maximum length of an aggregated MPDU (A-MPDU) on the 802.11ac radio. MPDU stands for MAC protocol data unit.

The **undo vht a-mpdu max-length-exponent** command restores the maximum length of an A-MPDU on the 802.11ac radio to the default value.

By default, the index for the maximum length of an A-MPDU is 7. The maximum length of the A-MPDU is 1048575 bytes.

NOTE

Currently, only the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN support 802.11ac.

Format

vht a-mpdu max-length-exponent *max-length-exponent-index*

undo vht a-mpdu max-length-exponent

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-length-exponent-index	Indicates the index for the maximum length of the A-MPDU.	The value is an integer that ranges from 0 to 7. ● 0: indicates that the maximum length of the A-MPDU is 8191 bytes. ● 1: indicates that the maximum length of the A-MPDU is 16383 bytes. ● 2: indicates that the maximum length of the A-MPDU is 32767 bytes. ● 3: indicates that the maximum length of the A-MPDU is 65535 bytes. ● 4: indicates that the maximum length of the A-MPDU is 131071 bytes. ● 5: indicates that the maximum length of the A-MPDU is 262143 bytes. ● 6: indicates that the maximum length of the A-MPDU is 524287 bytes. ● 7: indicates that the maximum length of the A-MPDU is 1048575 bytes.

 Copyright © Huawei Technologies Co., Ltd.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

To reduce costs, 802.11ac uses frame aggregation technology that aggregates two or more frames into an A-MPDU to transmit.

Example

Set the index of the maximum length of the A-MPDU to 2 in the 5G radio profile **default**. The index 2 corresponds to a maximum length of 32767 bytes.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht a-mpdu max-length-exponent 2
```

Related Topics

14.1.107 display radio-5g-profile

14.1.236 vht a-msdu enable

Function

The **vht a-msdu enable** command enables the function of sending 802.11 frames in A-MSDU mode.

The **undo vht a-msdu enable** command disables the function of sending 802.11 frames in A-MSDU mode.

By default, the function of sending 802.11 frames in A-MSDU mode is disabled.

NOTE

Currently, only the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN support 802.11ac.

Format

vht a-msdu enable

undo vht a-msdu enable

Parameters

None

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Aggregated MAC Service Data Unit (A-MSDU) technology aggregates multiple MAC Service Data Units (MSDUs) into an MAC Protocol Data Unit (MPDU), which reduces MAC layer costs of the 802.11 packets and improves packet transmission efficiency especially when short MSDUs are aggregated.

Precautions

The function of sending 802.11 frames in A-MSDU mode can only be enabled on the 802.11ac radio.

Example

Enable the function of sending 802.11 frames in A-MSDU mode.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht a-msdu enable
```

Related Topics

14.1.107 display radio-5g-profile

14.1.237 vht a-msdu max-frame-num

Function

The **vht a-msdu max-frame-num** command sets the maximum number of subframes that can be aggregated into an A-MSDU at one time.

The **undo vht a-msdu max-frame-num** command restores the default maximum number of subframes that can be aggregated into an A-MSDU at one time.

By default, a maximum of two subframes can be aggregated into an A-MSDU at one time.

NOTE

Currently, only the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN support 802.11ac.

Format

vht a-msdu max-frame-num *max-frame-number*

undo vht a-msdu max-frame-num

Parameters

Parameter	Description	Value
max-frame-number	Specifies the maximum number of subframes that can be aggregated into an A-MSDU at one time.	The value is an integer ranging from 2 to 15.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A-MSDU technology aggregates multiple MSDUs into an MPDU, which reduces MAC layer costs of the 802.11 packets.

- When the wireless network quality is satisfactory, increase the maximum number of subframes that can be aggregated into an A-MSDU at one time to improve the network usage efficiency and wireless service performance.
- When the wireless network quality is unsatisfactory or delay-sensitive services, such as voice services are transmitted, reduce the maximum number of subframes that can be aggregated into an A-MSDU at one time to minimize the impact of packet loss on services and reduce packet transmission delay. Some STAs have restrictions on the number of subframes aggregated into a received A-MSDU. If the number of subframes sent by the AP exceeds the threshold, the STAs cannot receive the frames properly.

Prerequisite

The function of sending 802.11 frames in A-MSDU mode has been enabled using the **14.1.236 vht a-msdu enable** command.

Precautions

The function of sending 802.11 frames in A-MSDU mode can only be enabled on the 802.11ac radio.

Example

Set the maximum number of subframes that can be aggregated into an A-MSDU at one time to 3.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht a-msdu max-frame-num 3
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.1.236 vht a-msdu enable

14.1.107 display radio-5g-profile

14.1.238 vht mcs-map

Function

The **vht mcs-map** command configures the maximum MCS value corresponding to a specific number of 802.11ac spatial streams in the 5G radio profile.

The **undo vht mcs-map** command restores the default maximum MCS value corresponding to a specific number of 802.11ac spatial streams in the 5G radio profile.

By default, the maximum MCS value of the 802.11 ac radios is 9 in the 5G radio profile.

NOTE

Currently, only the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP8030DN, AP8130DN and AP9330DN support 802.11ac.

Format

vht mcs-map nss *nss-value* **max-mcs** *max-mcs-value*

undo vht mcs-map

Parameters

Parameter	Description	Value
nss *nss-value*	Specifies the number of spatial streams.	The value is an integer ranging from 1 to 4.
max-mcs *max-mcs-value*	Specifies the maximum MCS value corresponding to a specific number of spatial streams.	The value is an integer ranging from 7 to 9.

Views

5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Rates of 802.11ac radios depend on the index value of Modulation and Coding Scheme (MCS). A larger MCS value indicates a higher transmission rate.

- If *nss-value* is equal to or larger than the actual number of spatial streams supported by an AP, the maximum MCS value corresponding to all spatial streams of the AP is *max-mcs-value*.
- If *nss-value* is smaller than the actual number of spatial streams supported by an AP, only the maximum MCS value of configured spatial streams is *max-mcs-value*. The maximum MCS value of the other spatial streams does not take effect.

  For example, if *nss-value* is 2, and the AP supports 3 spatial streams. Only the maximum MCS value of spatial stream 1 and spatial stream 2 is *max-mcs-value*, and that of spatial stream 3 does not take effect.

Precautions

This configuration applies only to STAs associated with an AP in 802.11ac mode but does not take effect on STAs associated with the AP in other modes.

Example

Configure the maximum MCS value 8 for 802.11ac radios with two spatial streams in the 5G radio profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] vht mcs-map nss 2 max-mcs 8
```

Related Topics

14.1.107 display radio-5g-profile

14.1.239 wifi-light

Function

The **wifi-light** command specifies the parameter reflected by the blinking frequency of the Wireless LED on an AP.

The **undo wifi-light** command restores the default parameter reflected by the blinking frequency of the Wireless LED on an AP.

By default,

- If WDS is enabled on an AP, the blinking frequency of the Wireless LED reflects the strength of signals received from a WDS AP.
  - If the AP works in leaf mode, the blinking frequency of the Wireless LED reflects the strength of signals received from a middle AP.
  - If the AP works in middle mode, the blinking frequency of the Wireless LED reflects the strength of signals received from a root AP.
  - If the AP works in root mode, the blinking frequency of the Wireless LED reflects the weakest signal strength of middle APs.
- If the WDS functions are disabled on an AP, the blinking frequency of the Wireless LED reflects the service traffic volume on the radio.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only APs having Wireless LEDs support this command.

Format

wifi-light { **signal-strength** | **traffic** }

undo wifi-light

Parameters

Parameter	Description	Value
signal-strength	Sets the parameter reflected by the blinking frequency of the Wireless LED on an AP to signal strength. When the Wireless LED blinks fast, the signal strength is strong.	-
traffic	Sets the parameter reflected by the blinking frequency of the Wireless LED on an AP to service traffic volume. When the Wireless LED blinks fast, the service traffic volume is high.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During installation and commissioning of an AP that has the WDS function enabled, you need to adjust AP locations and antenna directions to obtain strong signals. If the blinking frequency of the Wireless LED shows the signal strength, onsite installation personnel can know the signal strength in real time. The **wifi-light** command allows you to specify the parameter reflected by the blinking frequency of the Wireless LED. For example, you can specify the parameter to signal strength during installation and service traffic volume after installation.

Precautions

This command takes effect only when the AP has the WDS function enabled. If the WDS functions are disabled on the AP, the Wireless LED always shows service traffic volume.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the parameter reflected by the blinking frequency of the Wireless LED on an AP to service traffic volume.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio-profile1
[Huawei-wlan-radio-2g-prof-radio-profile1] wifi-light traffic
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile

14.1.240 wired-port-profile (WLAN view)

Function

The **wired-port-profile** command creates an AP wired port profile and displays the AP wired port profile view, or displays the view of an existing AP wired port profile.

The **undo wired-port-profile** command deletes an AP wired port profile.

By default, the system provides the AP wired port profile **default**.

Format

wired-port-profile name *profile-name*

undo wired-port-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an AP wired port profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all AP wired port profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP wired port profile provides convenience for AP wired interface management and configuration. You can configure AP wired interface parameters in an AP wired port profile to manage APs.

Follow-up Procedure

Run the **14.1.241 wired-port-profile (AP group view and view)** command to bind the AP wired port profile to an AP or AP group so that the AP wired port profile can take effect.

Precautions

- The AP wired port profile**default** cannot be deleted.
- The AP wired port profile referenced by an AP or AP group cannot be deleted. To delete the AP wired port profile, unbind it from the AP or AP group first.

Example

Create the AP wired port profile **wired-port1** and display the AP wired port profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1]
```

Related Topics

14.1.128 display wired-port-profile

14.1.241 wired-port-profile (AP group view and view)

14.1.241 wired-port-profile (AP group view and view)

Function

The **wired-port-profile** command binds an AP wired port profile to an AP or AP group.

The **undo wired-port-profile** command unbinds an AP wired port profile from an AP or AP group.

By default, the AP wired port profile **default** is bound to an AP group, but no AP wired port profile is bound to an AP.

Format

wired-port-profile *profile-name interface-type interface-number*

undo wired-port-profile *interface-type interface-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an AP wired port profile.	The AP wired port profile must exist.
interface-type interface-number	Specifies the type and number of an AP wired interface.	-

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an AP wired port profile using the **14.1.240 wired-port-profile (WLAN view)** command, bind it to an AP or AP group so that the AP wired port profile can take effect.

Precautions

After an AP wired port profile is bound to an AP or AP group, parameter settings in the AP wired port profile apply to specified interfaces of all APs using the AP wired port profile.

Example

Create the AP wired port profile **wired-port1** and bind it to GE0 of APs in AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wired-port-profile name wired-port1
[Huawei-wlan-wired-port-wired-port1] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] wired-port-profile wired-port1 gigabitethernet 0
```

Related Topics

14.1.97 display ap-group

14.1.116 display references wired-port-profile

14.1.240 wired-port-profile (WLAN view)

 Copyright © Huawei Technologies Co., Ltd.

14.1.242 wlan

Function

The **wlan ac** command displays the WLAN view.

Format

wlan ac

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before performing WLAN configurations, run the **wlan** command to enter the WLAN view. All WLAN configuration commands need to be used in the WLAN view or WLAN sub-view.

Example

Enter the WLAN view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view]
```

14.1.243 wmm disable

Function

The **wmm disable** command disables the Wi-Fi Multimedia (WMM) function in a 2G or 5G radio profile.

The **undo wmm disable** command enables the WMM function in a 2G or 5G radio profile.

By default, the WMM function is enabled in a 2G or 5G radio profile.

Format

wmm disable

undo wmm disable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After the WMM function is enabled in a 2G or 5G radio profile, the AP radio to which the 2G or 5G radio profile is applied can use the WMM parameters.

Example

Enable the WMM function in 5G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] undo wmm disable
```

Related Topics

14.1.184 radio-2g-profile (WLAN view)

14.1.186 radio-5g-profile (WLAN view)

14.1.244 wmm edca-ap

Function

The **wmm edca-ap** command sets EDCA parameters and ACK policies for an AP.

The **undo wmm edca-ap** command restores the default EDCA parameters and ACK policies for an AP.

Table 14-88 lists the default EDCA parameter settings and ACK policies for APs.

Table 14-88 Default EDCA parameter settings and ACK policies for APs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit	ACK Policy
AC_VO	3	2	1	47	normal
AC_VI	4	3	1	94	normal
AC_BE	6	4	3	0	normal
AC_BK	10	4	7	0	normal

 Copyright © Huawei Technologies Co., Ltd.

Format

wmm edca-ap { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *

undo wmm edca-ap

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the AIFSN, which determines the channel idle time.	The value is an integer that ranges from 1 to 15.
ecwmin *ecwmin-value*	Specifies the *ecwmin-value*. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and cannot be greater than the *ecwmax-value* value.
ecwmax *ecwmax-value*	Specifies the *ecwmax-value*. *ecwmax-value* and *ecwmin-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and cannot be smaller than the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the *txoplimit-value*. The value determines the maximum duration in which an AP or a STA can occupy a channel. A larger *txoplimit-value* value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. The unit is microseconds. **NOTE** If the *txoplimit-value* value is 0, the STA can send only one data frame every time it occupies a channel.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ack-policy { **normal** | **noack** }	Specifies an ACK policy. ● **normal**: During 802.11 packet exchange, The receiver must return an ACK packet each time it receives a packet from the sender. ● **noack**: The receiver does not need to send an ACK message when it receives a packet from the sender. The **noack** is applicable to scenarios with good communication quality and little interference.	-

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide different priorities to the packets. In this way, APs have different capabilities to compete for channels and provide differentiated services.

Precautions

- The EDCA parameters configured for the four AC queues take effect only after the WMM function is enabled. By default, the WMM function is enabled in a 2G or 5G radio profile.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.

Example

Set EDCA parameters and ACK policies for AC_VO packets in 5G radio profile **default**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-5g-profile name default
[Huawei-wlan-radio-5g-prof-default] wmm edca-ap ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0
ack-policy normal
```

14.1.245 wmm edca-client (SSID profile view)

Function

The **wmm edca-client** command configures EDCA parameters for STAs.

The **undo wmm edca-client** command restores the default EDCA parameter settings of STAs.

Table 14-89 lists the default EDCA parameter settings for STAs.

Table 14-89 Default EDCA parameter settings for STAs

Packet Type	ECWmax	ECWmin	AIFSN	TXOPLimit
AC_VO	3	2	2	47
AC_VI	4	3	2	94
AC_BE	10	4	3	0
AC_BK	10	4	7	0

Format

wmm edca-client { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

undo wmm edca-client

Parameters

Parameter	Description	Value
ac-vo	Indicates AC_VO packets.	-
ac-vi	Indicates AC_VI packets.	-
ac-be	Indicates AC_BE packets.	-
ac-bk	Indicates AC_BK packets.	-
aifsn *aifsn-value*	Specifies the arbitration inter frame spacing number (AIFSN), which determines the channel idle time.	The value is an integer that ranges from 1 to 15.
ecwmin *ecwmin-value*	Specifies the exponent form of the minimum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be smaller than the *ecwmax-value* value.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ecwmax *ecwmax-value*	Specifies the exponent form of the maximum contention window. *ecwmin-value* and *ecwmax-value* determine the average backoff time.	The value is an integer that ranges from 0 to 15 and must be greater than the *ecwmin-value* value.
txoplimit *txoplimit-value*	Specifies the transmission opportunity limit (TXOPLimit), which determines the maximum duration in which an STA can occupy a channel. A larger TXOPLimit value indicates a longer duration to occupy a channel.	The value is an integer that ranges from 0 to 255. **NOTE** If the TXOPLimit value is 0, the STA can send only one data frame every time it occupies a channel.

Views

SSID profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WMM classifies data packets into the following access categories (ACs): AC_VO, AC_VI, AC_BE, and AC_BK. A set of EDCA parameters is set for each AC queue. These parameters determine the capabilities of a queue to occupy a channel. You can set EDCA parameters for packets of different ACs to provide differentiated priorities to the packets and different capabilities to compete for channels. In this way, differentiated services are implemented.

Table 14-90 describes the EDCA parameters.

Table 14-90 EDCA parameter description

Parameter	Meaning
Arbitration Interframe Spacing Number (AIFSN)	The DIFS has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value means that the STA must wait for a long time and has a low priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Meaning
Exponent form of CWmin (ECWmin) and exponent form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. Together, they determine the average backoff time. Large ECWmin and ECWmax values mean a long average backoff time for the STA and a low STA priority.
Transmission Opportunity Limit (TXOPLimit)	After preempting a channel, the STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value means that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can only send one data frame every time it preempts a channel.

Precautions

- The EDCA parameters configured for the four AC queues take effect only after the WMM function is enabled using the **14.1.243 wmm disable** command.
- By default, queues of AC_VO, AC_VI, AC_BE, and AC_BK are in descending order of priority. Priorities of the four queues are determined by their EDCA parameters.

Example

Set EDCA parameters for AC_VO packets of STAs in SSID profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ssid-profile name p1
[Huawei-wlan-ssid-prof-p1] wmm edca-client ac-vo aifsn 7 ecw ecwmin 4 ecwmax 10 txoplimit 0
```

Related Topics

14.1.118 display ssid-profile

14.1.246 wmm mandatory enable

Function

The **wmm mandatory enable** disables STAs that do not support WMM from connecting to a WMM-enabled AP.

The **undo wmm mandatory enable** allows STAs that do not support WMM to connect to a WMM-enabled AP.

By default, STAs that do not support WMM are allowed to connect to a WMM-enabled AP.

Format

wmm mandatory enable

undo wmm mandatory enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

On a WLAN, wireless channels are open and all STAs have the same chance to occupy a channel. You can configure WMM to distinguish high-priority packets and enable the high-priority packets to preempt channels. You can also disable STAs that do not support WMM from connecting to a WMM-enabled AP, which prevents those STAs from preempting channels of WMM-capable STAs.

Example

Disable STAs that do not support WMM to connect to a WMM-enabled AP.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name default
[Huawei-wlan-radio-2g-prof-default] wmm mandatory enable
```

14.2 WLAN Radio Resource Management Configuration Commands

14.2.1 amc-policy

Function

The **amc-policy** command configures an adaptive modulation and coding (AMC) algorithm for a radio.

The **undo amc-policy** command restores the default AMC algorithm for a radio.

By default, a radio uses the AMC algorithm **auto-balance**.

Format

amc-policy { **auto-balance** | **high-stability** | **high-throughput** }

undo amc-policy

Parameters

Parameter	Description	Value
auto-balance	Indicates the **auto-balance** algorithm.	-
high-stability	Indicates the **high-stability** algorithm.	-
high-throughput	Indicates the **high-throughput** algorithm.	-

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Radios need to adjust the AMC algorithm according to different scenarios to deliver the optimal user experience. Three AMC algorithms are available:

- **auto-balance**: applicable to most wireless scenarios
- **high-stability**: applicable to scenarios with continuous interference.
- **high-throughput**: applicable to scenarios with good wireless signals and non-continuous interference.

Example

Set the AMC algorithm of a radio to **high-stability**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] amc-policy high-stability
```

Related Topics

14.2.20 display rrm-profile

14.2.2 air-scan-profile

Function

The **air-scan-profile** command creates an air scan profile and displays the air scan profile view.

The **undo air-scan-profile** command deletes an air scan profile.

By default, the system provides the air scan profile **default**. You can run the **14.2.17 display air-scan-profile** command to view configuration of the air scan profile **default**.

Format

air-scan-profile name *profile-name*

undo air-scan-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an air scan profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all air scan profiles.	The air scan profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an air scan profile is created using the **air-scan-profile** command and bound to a radio profile, and scanning functions are enabled, such as radio calibration, and WIDS, the AP periodically scans surrounding radio signals and reports the collected information to an AC or a server. The information is used for radio calibration, or WIDS data analysis.

Follow-up Procedure

Run the **14.2.3 air-scan-profile (radio profile view)** command to bind the air scan profile to a 2G radio profile or 5G radio profile so that the air scan profile can take effect.

Example

Create the air scan profile **air-scan01**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] air-scan-profile name air-scan01
[Huawei-wlan-air-scan-prof-air-scan01]
```

Related Topics

14.2.3 air-scan-profile (radio profile view)

14.2.3 air-scan-profile (radio profile view)

Function

The **air-scan-profile** command binds an air scan profile to a radio profile.

The **undo air-scan-profile** command unbinds an air scan profile from a radio profile.

By default, the air scan profile **default** is bound to a radio profile.

Format

air-scan-profile *profile-name*

undo air-scan-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an air scan profile.	The air scan profile name must already exist.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After you create an air scan profile using the **14.2.2 air-scan-profile** command, bind it to a radio profile so that the air scan profile can take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind the air scan profile **air-scan01** to the radio profile **office01**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] air-scan-profile name air-scan01
[Huawei-wlan-air-scan-prof-air-scan01] quit
[Huawei-wlan-view] radio-2g-profile name office01
[Huawei-wlan-radio-2g-prof-office01] air-scan-profile air-scan01
```

Related Topics

14.2.2 air-scan-profile

14.2.4 band-steer balance gap-threshold

Function

The **band-steer balance gap-threshold** command sets the load difference threshold for load balancing between radios.

The **undo band-steer balance gap-threshold** command restores the default load difference threshold for load balancing between radios.

By default, the load difference threshold for load balancing between radios is 20%.

Format

band-steer balance gap-threshold *gap-threshold*

undo band-steer balance gap-threshold

Parameters

Parameter	Description	Value
gap-threshold	Specifies the load difference threshold for load balancing between radios.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **undo band-steer disable** command to configure the band steering function. If an AP and STAs connected to the AP can work at both 2.4 and

 Copyright © Huawei Technologies Co., Ltd.

5 GHz radios, the band steering function allows radios of the AP to load balance traffic. This helps minimize interference between STAs and improve user experience.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access users on each radio.

1. If the number of access users on the AP does not exceed **start-threshold** specified using the **14.2.5 band-steer balance start-threshold** command, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access users on the AP exceeds **start-threshold**, the AP determines the frequency band to which the STA connects based on radio load difference computed according to the formula:

   (Number of access users on the 5 GHz radio – Number of access users on the 2.4 GHz radio)/Number of access users on the 5 GHz radio x 100%

For example, if a STA requests to associate with the AP at the 2.4 GHz radio but the number of access users on the AP has exceeded **start-threshold**, the AP implements load balancing between the 2.4 GHz and 5 GHz radios according to their load difference. If the value obtained based on the preceding formula is greater than **gap-threshold**, the AP preferentially associates with the STA on the 2.4 GHz radio; otherwise, the AP preferentially associates with the STA on the 5 GHz radio.

Example

Set the load difference threshold to 25% in the RRM profile **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer balance gap-threshold 25
```

Related Topics

14.2.7 band-steer deny-threshold

14.2.5 band-steer balance start-threshold

14.2.5 band-steer balance start-threshold

Function

The **band-steer balance start-threshold** command sets the start threshold for load balancing between radios.

The **undo band-steer balance start-threshold** command restores the default start threshold for load balancing between radios.

By default, the start threshold for load balancing between radios is 10.

Format

band-steer balance start-threshold *start-threshold*

undo band-steer balance start-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start-threshold	Specifies the start threshold for load balancing between radios.	The value is an integer that ranges from 0 to 100.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

You can run the **undo band-steer disable** command to configure the band steering function. If an AP and STAs connected to the AP support both radios, the band steering function allows radios of the AP to load balance traffic. This helps minimize interference between STAs and improve user experience.

When a STA requests to connect to an AP radio, the AP enabled with band steering will collect statistics about access users on each radio.

1. If the number of access users on the AP does not exceed **start-threshold**, the STA can preferentially associate with the 5 GHz radio.
2. If the number of access users on the AP exceeds **start-threshold**, the AP determines the frequency band to which the STA connects based on radio load difference computed according to the formula: (Number of access users on the 5 GHz radio – Number of access users on the 2.4 GHz radio)/Number of access users on the 5 GHz radio * 100%

For example, if a STA requests to associate with the AP at the 2.4 GHz radio but the number of access users on the AP has exceeded **start-threshold**, the AP implements load balancing between the 2.4 GHz and 5 GHz radios according to their load difference. If the value obtained based on the formula (Number of access users on the 5 GHz radio – Number of access users on the 2.4 GHz radio)/Number of access users on the 5 GHz radio * 100% is greater than **gap-threshold** configured using the **14.2.4 band-steer balance gap-threshold** command, the AP preferentially associates with the STA on the 2.4 GHz radio; otherwise, the AP preferentially associates with the STA on the 5 GHz radio.

Example

Set the start threshold to 20 in the RRM profile **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer balance start-threshold 20
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.2.4 band-steer balance gap-threshold
14.2.7 band-steer deny-threshold

14.2.6 band-steer client-band-expire

Function

The **band-steer client-band-expire** command sets the aging condition for terminal band information.

The **undo band-steer client-band-expire** command restores the default aging condition for terminal band information.

By default, band information of a terminal will be aged out under conditions that an AP has consecutively received Probe frames of the terminal more than 35 times from the same frequency band.

Format

band-steer client-band-expire *probe-counters*

undo band-steer client-band-expire

Parameters

Parameter	Description	Value
probe-counters	Sets the aging condition of terminal band information to the number of times that an AP has consecutively received Probe frames of a terminal from the same frequency band.	The value is an integer that ranges from 10 to 300.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the band steering function is enabled on an AP, the AP records frequency band information of terminals so that the terminals can preferentially access the supported and lightly loaded frequency band.

Users may change terminals' configurations, which causes the supported frequency band of terminals to change. Therefore, the AP needs to update

 Copyright © Huawei Technologies Co., Ltd.

frequency band information of terminals in a timely manner. If the AP keeps receiving Probe frames of a terminal from a specific frequency band, and the number of receiving times exceeds a certain threshold, the AP updates the frequency band information of the terminal and considers that the terminal supports only the frequency band.

For example, the supported frequency bands of a terminal are 2.4 and 5 GHz frequency bands on an AP. If the AP only receives Probe frames of the terminal from the 2.4 GHz frequency band, and the number of times that the AP consecutively receives Probe frames from the 2.4 GHz frequency band exceeds the specified threshold, the AP considers that users change the terminal configuration and the terminal supports only the 2.4 GHz frequency band.

Precautions

If you set the aging condition to a large number of times that an AP consecutively receives Probe frames of a terminal from the same frequency band, the AP detects terminal band change more slowly. A smaller number indicates quicker response. Set the aging condition according to the difference in the number of Probe frames sent from the two frequency bands.

Example

Configure the supported band information of the terminal **huawei** to age out when the number of times that an AP consecutively receives Probe frames from a frequency band exceeds 80.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer client-band-expire 80
```

14.2.7 band-steer deny-threshold

Function

The **band-steer deny-threshold** command sets the maximum number of times an AP rejects association requests of a STA for band steering.

The **undo band-steer deny-threshold** command restores the default maximum number of times an AP rejects association requests of a STA for band steering.

By default, the maximum number of rejections is 2.

Format

band-steer deny-threshold *deny-threshold*

undo band-steer deny-threshold

Parameters

Parameter	Description	Value
deny-threshold	Specifies the maximum number of times an AP rejects association requests of a STA.	The value is an integer that ranges from 1 to 10.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

If a STA requests to associate with an AP from the 2.4 GHz frequency band but the AP steers the STA to the 5 GHz frequency band according to the band steering algorithm, the AP will reject the association. However, after the number of rejections exceeds the maximum value specified by the **band-steer deny-threshold** command, the AP allows the STA to associate from the 2.4 GHz frequency band.

Example

Set the maximum number of rejections to 8 for the terminal **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] band-steer deny-threshold 8
```

Related Topics

14.2.8 band-steer disable

14.2.8 band-steer disable

Function

The **band-steer disable** command disables the band steering function.

The **undo band-steer disable** command enables the band steering function.

By default, the band steering function is enabled.

Format

band-steer disable

undo band-steer disable

Parameters

None

Views

VAP profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with the 2.4 GHz frequency band, the 5 GHz frequency band has less interference and more available channels, and provides higher access capability.

Most STAs support both 5 GHz and 2.4 GHz frequency bands and usually associate with the 2.4 GHz radio by default when connecting to the Internet. To connect the STAs to the 5 GHz radio, you must manually select the 5 GHz radio. The band steering function frees you from the manual selection.

After you enable band steering for a specific SSID on the AC, the AP preferentially associates the terminals connected to the SSID with the 5 GHz frequency band. After the 5 GHz frequency band is fully loaded, the AP steers the terminals to the 2.4 GHz frequency band.

Configuration Impact

After the band steering function is enabled, it takes a long time for dual-band terminals to associate or roam. You are advised to disable band steering for delay-sensitive services.

Precautions

If both radios of an AP use the same VAP profile, the band steering function takes effect on both radios as long as the function is enabled for an SSID on one radio of the AP. For example, if band steering is enabled for the SSID **huawei** on the 2.4 GHz radio but not on the 5 GHz radio, the AP preferentially steers terminals associated with the SSID to the 5 GHz radio.

Single-radio devices do not support the band steering function.

The AP2010DN does not support the band steering function.

Example

Disable band steering.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name huawei
[Huawei-wlan-vap-prof-huawei] band-steer disable
```

Related Topics

14.1.127 display vap-profile

14.2.9 calibrate auto-channel-select disable

Function

The **calibrate auto-channel-select disable** command disables automatic channel selection.

The **undo calibrate auto-channel-select disable** command enables automatic channel selection.

By default, automatic channel selection is enabled.

Format

calibrate auto-channel-select disable

undo calibrate auto-channel-select disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Two channel selection modes are available:

- Automatic mode (enabling automatic channel selection): An AP automatically selects a proper channel based on the WLAN radio environment, removing the need to specify channels manually.
- Fixed mode (disabling automatic channel selection): Channels must be manually specified.

The automatic mode (automatic channel selection) is recommended because you do not need to specify a channel for each radio. The fixed mode provides users with an alternative way when they want to specify channels by themselves or to avoid frequent channel adjustment (this may cause intermittent service interruption).

If an AP needs radio calibration, automatic channel selection must be enabled in the AP's RRM profile.

NOTE

When automatic channel selection is enabled, the manually configured channels do not take effect to ensure that the radio works in the optimal channel environment.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable automatic channel selection in the RRM profile **802.11b**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name 802.11b
[Huawei-wlan-rrm-prof-802.11b] calibrate auto-channel-select disable
```

14.2.10 calibrate auto-txpower-select disable

Function

The **calibrate auto-txpower-select disable** command disables automatic transmit power selection.

The **undo calibrate auto-txpower-select disable** command enables automatic transmit power selection.

By default, automatic transmit power selection is enabled.

Format

calibrate auto-txpower-select disable

undo calibrate auto-txpower-select disable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Two power selection modes are available:

- Automatic mode (enabling automatic transmit power selection): An AP automatically selects or adjusts the transmit power based on the WLAN radio environment, removing the need to specify AP power manually.
- Fixed mode (disabling automatic transmit power selection): The transmit power must be manually specified.

If an AP needs radio calibration, automatic transmit power selection must be enabled in the AP's RRM profile.

Example

Disable automatic transmit power selection in the RRM profile **802.11b**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name 802.11b
[Huawei-wlan-rrm-prof-802.11b] calibrate auto-txpower-select disable
```

14.2.11 calibrate enable { auto | manual | schedule time }

Function

The **calibrate enable** { **auto** | **manual** | **schedule time** } command configures the radio calibration mode.

The **undo calibrate enable** command disables calibration.

By default, the radio calibration mode is **auto**, the radio calibration interval is 1440 minutes, and the start time for radio calibration is 00:00:00.

Format

calibrate enable { **auto** [**interval** *interval-value* [**start-time** *start-time*]] | **manual** | **schedule time** *time-value* }

undo calibrate enable

Parameters

Parameter	Description	Value
auto	Sets the radio calibration mode to auto.	-
interval *interval-value*	Specifies the radio calibration interval in auto mode.	The value is an integer that ranges from 30 to 1440, in minutes. If **interval** is not specified, the radio calibration interval in auto mode is 1440 minutes.
start-time *start-time*	Specifies the start time for radio calibration in automatic mode.	The value is in the format of hh:mm:ss. ● hh: indicates the hour. The value is an integer that ranges from 0 to 23. ● mm: indicates the minute. The value is an integer that ranges from 0 to 59. ● ss: indicates the second. The value is an integer that ranges from 0 to 59.
manual	Sets the radio calibration mode to manual.	-

Parameter	Description	Value
schedule	Sets the radio calibration mode to schedule.	-
time *time-value*	Specifies the time for triggering the scheduled radio calibration.	The value is in the format of hh:mm:ss. • hh: indicates the hour. The value is an integer that ranges from 0 to 23. • mm: indicates the minute. The value is an integer that ranges from 0 to 59. • ss: indicates the second. The value is an integer that ranges from 0 to 59.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

There are three radio calibration modes:

- Auto mode: The device periodically implements radio calibration at certain intervals (the interval is specified by **interval** and the default interval is 1440 minutes).
- Manual mode: Radio calibration is not automatically implemented by the device but manually triggered through the **14.2.13 calibrate manual startup** command.
- Schedule mode: The device triggers radio calibration at the time specified by the parameter **time**.

The three modes cannot be configured simultaneously. You can choose any of the modes as required.

In any mode, you can run the **calibrate manual startup** command to trigger the calibration. In **manual** mode, the device implements radio calibration only after the **calibrate manual startup** command is executed.

Example

Set the radio calibration mode to manual.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] calibrate enable manual
```

Set the radio calibration mode to schedule and set the time for scheduled radio calibration to 20:30:00.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] calibrate enable schedule time 20:30:00
```

Related Topics

14.2.13 calibrate manual startup

14.2.12 calibrate error-rate-threshold

Function

The **calibrate error-rate-threshold** command sets the packet error rate (PER) threshold in a radio profile.

The **undo calibrate error-rate-threshold** command restores the default PER threshold in a radio profile.

By default, the PER threshold is 60%.

Format

calibrate error-rate-threshold *error-rate-threshold*

undo calibrate error-rate-threshold

Parameters

Parameter	Description	Value
error-rate-threshold	Specifies the PER threshold.	The value is an integer that ranges from 20 to 80, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

If the MAC layer of a radio does not receive any ACK packet after sending a packet at the lowest rate, it considers that an error occurs.

The PER threshold determines whether the radio environment is normal. When the PER of a radio reaches the threshold, the system considers that the radio environment deteriorates. When this occurs, the system may start radio calibration or take measures to avoid signal interference.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the PER threshold to 70% in the RRM profile **80211b**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name 80211b
[Huawei-wlan-rrm-prof-80211b] calibrate error-rate-threshold 70
```

14.2.13 calibrate manual startup

Function

The **calibrate manual startup** command manually triggers radio calibration.

Format

calibrate manual startup

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

When you need to implement radio calibration instantly, run the **calibrate enable** { **auto** [**interval** *interval-value* [**start-time** *start-time*]] | **manual** | **schedule time** *time-value* } command to enable radio calibration and then run the **calibrate manual startup** command to manually trigger radio calibration.

Example

Manually trigger radio calibration.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] calibrate enable auto
[Huawei-wlan-view] calibrate manual startup
```

Related Topics

14.2.11 calibrate enable { auto | manual | schedule time }

14.2.14 calibrate sensitivity

Function

The **calibrate sensitivity** command configures the radio calibration sensitivity for a device.

The **undo calibrate sensitivity** command restores the default radio calibration sensitivity.

By default, the radio calibration sensitivity of the device is set to **medium**.

Format

calibrate sensitivity { **low** | **medium** | **high** }

undo calibrate sensitivity

Parameters

Parameter	Description	Value
low	Indicates low radio calibration sensitivity.	-
medium	Indicates medium radio calibration sensitivity.	-
high	Indicates high radio calibration sensitivity.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Radio calibration sensitivity of a device is described as follows:

- high: The device implements radio calibration when the current spectrum model is not as good as the estimated spectrum model.
- medium: The device implements radio calibration when the current spectrum model varies from the estimated spectrum model.
- low: The device implements radio calibration when the current spectrum model differs greatly from the estimated spectrum model.

The default value is recommended.

Example

Set the radio calibration sensitivity to high.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] calibrate sensitivity high
```

 Copyright © Huawei Technologies Co., Ltd.

14.2.15 dca-channel bandwidth

Function

The **dca-channel bandwidth** command configures the calibration bandwidth.

The **undo dca-channel bandwidth** command restores the default calibration bandwidth.

By default, the calibration bandwidth is 20 MHz.

Format

dca-channel 5g bandwidth { **20mhz** | **40mhz** | **80mhz** }

undo dca-channel 5g bandwidth

Parameters

Parameter	Description	Value
5g	Specifies the frequency band on which radio calibration is implemented.	-
20mhz | **40mhz** | **80mhz**	Specifies the calibration bandwidth.	-

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 5 GHz frequency band has richer spectrum resources. In addition to 20 MHz channels, APs working on the 5 GHz frequency band support 40 MHz and 80 MHz channels. Larger-bandwidth channels mean higher transmission rates. However, at least three channels are required in radio calibration to achieve the optimal calibration effect. When configuring the calibration bandwidth, ensure that enough calibration channels are available for use.

You can use the **dca-channel bandwidth** command to configure the calibration bandwidth and the **14.2.16 dca-channel channel-set** command to configure calibration channels as prompted.

Configuration Impact

 Copyright © Huawei Technologies Co., Ltd.

When the calibration bandwidth is changed, the device recalculates the calibration channels.

Precautions

Only the AP2030DN, AP3030DN, AP4030DN, AP4130DN, AP5030DN, AP5130DN, AP7030DE, AP9131DN, AP9330DN, AP8030DN, and AP8130DN support 80 MHz calibration bandwidth.

When configuring 40 MHz or 80 MHz calibration bandwidth, check whether channels of the corresponding bandwidth exist under the country code.

Example

Set the calibration bandwidth to 40 MHz.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] regulatory-domain-profile name huawei
[Huawei-wlan-regulate-domain-huawei] dca-channel 5g bandwidth 40mhz
```

Related Topics

14.2.16 dca-channel channel-set

14.1.117 display regulatory-domain-profile

14.2.16 dca-channel channel-set

Function

The **dca-channel channel-set** command configures a calibration channel set.

The **undo dca-channel channel-set** command restores the default calibration channel set.

By default, a calibration channel set contains channels 1, 6, and 11 on the 2.4G radio and contains all channels supported by the corresponding country code on the 5G radio. If the country code is China, the calibration channel set does not contain channels 36 to 64. When configuring the calibration channels, users can specify channels as prompted.

Format

dca-channel { **2.4g** | **5g** } **channel-set** *channel-value*

undo dca-channel { **2.4g** | **5g** } **channel-set**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
2.4g | **5g**	Specifies the frequency band on which radio calibration is performed. ● **2.4g**: Radios work on the 2.4 GHz frequency band. ● **5g**: Radios work on the 5 GHz frequency band.	-
channel-set *channel-value*	Specifies a calibration channel set.	The value is a character string. You can select calibration channels as prompted. If you select multiple channels, use commas (,) to separate channel names.

Views

Regulatory domain profile view

Default Level

2: Configuration level

Usage Guidelines

The 5 GHz frequency band has richer spectrum resources. In addition to 20 MHz channels, APs working on the 5 GHz frequency band support 40 MHz and 80 MHz channels. Larger-bandwidth channels mean higher transmission rates. However, at least three channels are required in radio calibration to achieve the optimal calibration effect. When configuring the calibration bandwidth, ensure that enough calibration channels are available for use.

You can run this command to specify a calibration channel set for an AP. The AP selects channels from the channel set to calibrate. This reduces the burden on the AP.

NOTE

To ensure a good calibration effect, you are advised to configure at least three calibration channels.

To prevent signal interference, ensure that adjacent APs work in non-overlapping channels. The 2.4 GHz frequency band has overlapping channels. When configuring calibration channels, you are advised to configure a non-overlapping calibration channel set containing channels 1, 6, and 11 or containing channels 1, 5, 9, and 13.

To specify a 40 MHz calibration channel, you need to specify two consecutive 20 MHz channels. To specify an 80 MHz calibration channel, you need to specify four consecutive 20 MHz channels. The combinations of 20 MHz channels making up

 Copyright © Huawei Technologies Co., Ltd.

the 40 MHz and 80 MHz channels are fixed. For details, see *Huawei AR Series Access Routers Configuration Guide*–Radio Resource Management–Radio Calibration.

You can also use the **14.2.15 dca-channel bandwidth** command to configure the calibration bandwidth and the **dca-channel channel-set** command to configure calibration channels as prompted.

If no calibration channel set is configured, the device probes channels based on the calibration channels corresponding to the country code.

NOTE

When configuring a calibration channel set, avoid using radar channels.

The channels you configure must be supported by the terminals; otherwise, the terminals cannot discover wireless signals. For example, when the country code is set to China, 5 GHz channels 36, 40, 44, 48, 52, 56, 60, and 64 can be configured. However, most terminals do not support these channels currently. If these channels are configured, the terminals cannot discover wireless signals. In this case, you can configure 5 GHz channels 149, 153, 157, 161, and 165, which are supported by the terminals.

Example

Configure a calibration channel set composed of 40MHz channels 149, 153, 157, and 161 on the 5 GHz frequency band.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] regulatory-domain-profile name huawei
[Huawei-wlan-regulate-domain-huawei] dca-channel 5g bandwidth 40mhz
[Huawei-wlan-regulate-domain-huawei] dca-channel 5g channel-set 149,153,157,161
```

Related Topics

14.1.61 country-code

14.2.15 dca-channel bandwidth

14.2.17 display air-scan-profile

Function

The **display air-scan-profile** command displays information about air scan profiles.

Format

display air-scan-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all air scan profiles.	-

Parameter	Description	Value
name *profile-name*	Displays information about a specified air scan profile.	The air scan profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display air-scan-profile** command to view information about air scan profiles.

Example

Display information about all air scan profiles.

```
<Huawei> display air-scan-profile all
-----------------------------------------------------------
Profile name        Reference
-----------------------------------------------------------
default             2
huawei              1
-----------------------------------------------------------
Total: 2
```

Table 14-91 Description of the **display air-scan-profile all** command output

Item	Description
Profile name	Name of an air scan profile.
Reference	Number of times that the air scan profile is referenced.

Display information about the air scan profile **huawei**.

```
<Huawei> display air-scan-profile name huawei
-----------------------------------------------------------
Scan period(ms)   : 80
Scan interval(ms) : 3000
Scan channel-set  : dca-channel
-----------------------------------------------------------
```

Table 14-92 Description of the **display air-scan-profile name** command output

Item	Description
Scan period(ms)	Air scan period. To set the air scan period, run the **14.2.39 scan-period** command.
Scan interval(ms)	Air scan interval. To set the air scan interval, run the **14.2.38 scan-interval** command.
Scan channel-set	Air scan channel set. To set the air scan channel set, run the **14.2.37 scan-channel-set** command.

Related Topics

14.2.39 scan-period
14.2.38 scan-interval
14.2.37 scan-channel-set

14.2.18 display references air-scan-profile

Function

The **display references air-scan-profile** command displays reference information about an air scan profile.

Format

display references air-scan-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified air scan profile.	The air scan profile name must already exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display references air-scan-profile** command to view reference information about an air scan profile.

Example

Display reference information about the air scan profile **huawei**.

```
<Huawei> display references air-scan-profile name huawei
-----------------------------------------------------------
Reference type              Reference name
-----------------------------------------------------------
radio-2g-profile            default
-----------------------------------------------------------
Total: 1
```

Table 14-93 Description of the **display references air-scan-profile** command output

Item	Description
Reference type	Type of the profile that references the air scan profile.
Reference name	Name of the profile that references the air scan profile.

14.2.19 display references rrm-profile

Function

The **display references rrm-profile** command displays reference information about an RRM profile.

Format

display references rrm-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified RRM profile.	The RRM profile name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references rrm-profile** command to view reference information about an RRM profile.

Example

Display reference information about the RRM profile **huawei**.

```
<Huawei> display references rrm-profile name huawei
-----------------------------------------------------------
Reference type          Reference name
-----------------------------------------------------------
radio-2g-profile        radio0
radio-5g-profile        radio1
-----------------------------------------------------------
Total: 2
```

Table 14-94 Description of the **display references rrm-profile** command output

Item	Description
Reference type	Type of the profile that references the RRM profile.
Reference name	Name of the profile that references the RRM profile.

14.2.20 display rrm-profile

Function

The **display rrm-profile** command displays information about an RRM profile.

Format

display rrm-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all RRM profiles.	-
name *profile-name*	Displays information about a specified RRM profile.	The RRM profile name must already exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display rrm-profile** command to view information about an RRM profile.

Example

Display information about all RRM profiles.

```
<Huawei> display rrm-profile all
-----------------------------------------------------------
Profile name  Reference
-----------------------------------------------------------
default       2
-----------------------------------------------------------
Total:1
```

Table 14-95 Description of the **display rrm-profile all** command output

Item	Description
Profile name	Name of an RRM profile.
Reference	Number of times an RRM profile is referenced.

Display information about the RRM profile **huawei**.

```
<Huawei> display rrm-profile name huawei
-----------------------------------------------------------
Auto channel select                                : enable
Auto transmit power select                         : enable
PER threshold for trigger channel/power select(%)      : 60
Airtime fairness schedule                          : disable
Dynamic adjust EDCA parameter                      : enable
Band steer deny threshold                          : 2
Band balance start threshold                       : 10
Band balance gap threshold(%)                      : 20
Client's band expire based on continuous probe counts  : 35
Station load balance                               : disable
Station load balance start threshold               : 10
Station load balance gap threshold(%)              : 20
-----------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-96 Description of the **display rrm-profile name** command output

Item	Description
Auto channel select	Whether to enable automatic channel selection. To enable automatic channel selection, run the **14.2.9 calibrate auto-channel-select disable** command.
Auto transmit power select	Whether to enable automatic transmit power selection. To enable automatic transmit power selection, run the **14.2.10 calibrate auto-txpower-select disable** command.
PER threshold for trigger channel/ power select(%)	PER threshold for triggering channel or power adjustment. To set the PER threshold, run the **14.2.12 calibrate error-rate-threshold** command.
Airtime fairness schedule	Whether to enable airtime fair scheduling.
Dynamic adjust EDCA parameter	Whether to enable dynamic EDCA parameter adjustment. To enable dynamic EDCA parameter adjustment, run the **14.2.26 dynamic-edca enable** command.
Band steer deny threshold	Maximum number of times that an AP rejects association requests of a STA for band steering. To configure the maximum number of rejections, run the **14.2.7 band-steer deny-threshold** command.
Band balance start threshold	Start threshold for load balancing between radios. To configure start threshold for load balancing between radios, run the **14.2.5 band-steer balance start-threshold** command.
Band balance gap threshold(%)	Load difference threshold for load balancing between radios. To configure load difference threshold for load balancing between radios, run the **14.2.4 band-steer balance gap-threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Client's band expire based on continuous probe counts	Aging condition of terminal band information, that is, the number of times that an AP has continuously received Probe frames of a terminal from the same frequency band. To set the aging condition of terminal band information, run the **14.2.6 band-steer client-band-expire** command.
Station load balance	Whether to enable the load balancing function. To configure the load balancing function, run the **14.2.40 sta-load-balance dynamic enable** command.
Station load balance start threshold	Start threshold for load balancing. To configure the start threshold for load balancing, run the **14.2.42 sta-load-balance dynamic start-threshold** command.
Station load balance gap threshold(%)	Load difference threshold for load balancing. To configure the load difference threshold for load balancing, run the **14.2.41 sta-load-balance dynamic gap-threshold** command.

Related Topics

14.2.9 calibrate auto-channel-select disable
14.2.10 calibrate auto-txpower-select disable
14.2.26 dynamic-edca enable
14.2.40 sta-load-balance dynamic enable
14.2.42 sta-load-balance dynamic start-threshold
14.2.41 sta-load-balance dynamic gap-threshold

14.2.21 display sta-load-balance static-group

Function

The **display sta-load-balance static-group** command displays information about a static load balancing group.

Format

display sta-load-balance static-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all static load balancing groups.	-
name *group-name*	Displays information about a specified static load balancing group.	The static load balancing group must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display sta-load-balance static-group** command to view information about a specified static load balancing group or all static load balancing groups.

Example

Display information about all static load balancing group.

```
<Huawei> display sta-load-balance static-group all
-----------------------------------------------------------
Index  Group name
-----------------------------------------------------------
0      cc
1      coco
-----------------------------------------------------------
Total: 2
```

Table 14-97 Description of the **display sta-load-balance static-group all** command output

Item	Description
Index	Index.
Group name	Name of a static load balancing group.

Display information about the static load balancing group **cc**.

```
<Huawei> display sta-load-balance static-group name cc
-----------------------------------------------------------
Group name           : cc
Load-balance status  : balance
Start threshold      : 5
```

```
Gap threshold(%)     : 40
-----------------------------------------------------------
RfID: Radio ID
CurEIRP: Current EIRP (dBm)
Act CH: Actual channel, Cfg CH: Config channel
-----------------------------------------------------------
AP ID  AP Name  RfID  Act CH/Cfg CH  CurEIRP/MaxEIRP  Client
-----------------------------------------------------------
2      area_2   0     6/-            28/28            0
2      area_2   1     153/-          29/29            0
3      area_3   0     1/-            28/28            0
3      area_3   1     149/-          29/29            0
-----------------------------------------------------------
Total: 4
```

Table 14-98 Description of the **display sta-load-balance static-group name** command output

Item	Description
Group name	Name of a static load balancing group.
Load-balance status	Load balancing status in a static load balancing group.
Start threshold	Start threshold for load balancing in a static load balancing group. To configure the parameter, run the **14.2.44 start-threshold** command.
Gap threshold(%)	Load difference threshold in a static load balancing group. To configure the parameter, run the **14.2.27 gap-threshold** command.
AP ID	ID of the AP that joins a static load balancing group.
AP Name	Name of the AP that joins a static load balancing group.
RfID	Radio that joins a static load balancing group.
Act CH/Cfg CH	Actual effective/configured channel of an AP.
CurEIRP/MaxEIRP	Current power of an AP radio/ Maximum power of an AP radio.
Client	Number of STAs connected to an AP radio.

Related Topics

14.2.44 start-threshold

14.2.27 gap-threshold

14.2.22 display station load-balance sta-mac

Function

The **display station load-balance sta-mac** command displays information about the dynamic load balancing group based on STAs.

Format

display station load-balance sta-mac *mac-address*

Parameters

Parameter	Description	Value
mac-address	Displays information about the dynamic load balancing group based on the STA with the specified MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After dynamic load balancing group configuration is complete, run the **display station load-balance sta-mac** command to check information about the group based on STAs.

Example

Display information about the dynamic load balancing group.

```
<Huawei> display station load-balance sta-mac a826-d9e5-6df3
Station load balance status: Balance
--------------------------------------------------------------------------------
AP name                         Radio ID
--------------------------------------------------------------------------------
ap1                             0
ap3                             0
--------------------------------------------------------------------------------
Total: 2
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-99 Description of the **display station load-balance sta-mac** command output

Item	Description
Station load balance status	Load balancing status in the dynamic load balancing group: ● Balance: the load is balanced. ● Not balance: the load is unbalanced.
AP name	Name of the AP in the load balancing group.
Radio ID	ID of the radio in the load balancing group.

14.2.23 display station rssi-rejected statistics

Function

The **display station rssi-rejected statistics** command displays information about rejected STAs by a specified VAP due to weak signal strength.

Format

display station rssi-rejected statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id* **vap-profile** *profile-name*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies an AP name.	The AP name must already exist.
ap-id *ap-id*	Specifies an AP ID.	The AP ID must already exist.
radio *radio-id*	Specifies the radio ID.	The value is an integer that ranges from 0 to 2.
vap-profile *profile-name*	Specifies the ID of a service set.	The VAP profile must already exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The **display station rssi-rejected statistics** command displays information about rejected STAs due to weak signal strength.

Example

Display the number of times a STA is rejected due to weak signal strength in the VAP profile **office** applied to radio 0 of AP **huawei**.

```
<Huawei> display station rssi-rejected statistics ap-name huawei radio 0 vap-profile office
  Total station numbers: 2
--------------------------------------------------------------------------------
  MAC               Times    Last reject time
  c46a-b72c-4100    2        2012-07-23/09:26:23
  38e7-d87c-48c1    478      2012-07-23/10:16:10
--------------------------------------------------------------------------------
```

Table 14-100 Description of the **display station rssi-rejected statistics** command output

Item	Description
Total station numbers	Total number of STAs that are rejected due to weak signal strength.
MAC	MAC address of the rejected STA.
Times	Total number of times the STA is rejected.
Last reject time	Time when the STA is rejected for the last time.

14.2.24 display wlan calibrate channel-set

Function

The **display wlan calibrate channel-set** command displays the effective calibration channels and bandwidth.

Format

display wlan calibrate channel-set ap-group { **name** *ap-group-name* | **all** }

Parameters

Parameter	Description	Value
ap-group name *ap-group-name*	Displays the effective calibration channels and bandwidth in a specified AP group.	The AP group must exist.
ap-group all	Displays the effective calibration channels and bandwidth in all AP groups.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the radio calibration function, you can run the **display wlan calibrate channel-set** command to check the effective calibration channels and bandwidth.

Example

Display the calibration channels and bandwidth that take effect globally.

```
<Huawei> display wlan calibrate channel-set ap-group all
AP group    : default
Country code: CN
-------------------------------------------------------------------------------
Radio band  Bandwidth  Channel Set
-------------------------------------------------------------------------------
2.4G        20MHz      1,6,11
5G          20MHz      149,153,157,161,165
-------------------------------------------------------------------------------

AP group    : mainland
Country code: CN
-------------------------------------------------------------------------------
Radio band  Bandwidth  Channel Set
-------------------------------------------------------------------------------
2.4G        20MHz      1,6,11
5G          20MHz      149,153,157,161,165
-------------------------------------------------------------------------------
```

Table 14-101 Description of the **display wlan calibrate channel-set** command output

Item	Description
AP group	Name of an AP group.
Country code	Country code.

Item	Description
Radio band	Radio type.
Bandwidth	Effective calibration bandwidth.
Channel Set	Effective calibration channel set.

Related Topics

14.2.15 dca-channel bandwidth
14.2.16 dca-channel channel-set

14.2.25 display wlan calibrate statistics

Function

The **display wlan calibrate statistics** command displays radio calibration statistics.

Format

display wlan calibrate statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Displays radio calibration statistics on the specified AP name. The AP name and radio ID identify a radio.	The AP name must already exist.
ap-id *ap-id*	Displays radio calibration statistics on the specified AP ID. The AP ID and radio ID identify a radio.	The AP ID must already exist.
radio *radio-id*	Displays radio calibration statistics on the specified radio.	The value is an integer that ranges from 0 to 2.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display wlan calibrate statistics** command to view radio calibration statistics, helping check whether the radio environment is stable.

Example

Display calibration statistics about radio 0 of AP **office**.

```
<Huawei> display wlan calibrate statistics ap-name office radio 0
-----------------------------------------------------------------------
Signal environment deterioration :1
Power calibration                :1
Channel calibration              :0
-----------------------------------------------------------------------
```

Table 14-102 Description of the **display wlan calibrate statistics** command output

Item	Description
Signal environment deterioration	Number of times the radio environment deteriorates.
Power calibration	Number of times the power of the radio is calibrated.
Channel calibration	Number of times the channel of the radio is calibrated.

Related Topics

14.2.34 reset wlan calibrate statistics

14.2.26 dynamic-edca enable

Function

The **dynamic-edca enable** command enables dynamic EDCA parameter adjustment.

The **undo dynamic-edca enable** command disables dynamic EDCA parameter adjustment.

By default, dynamic EDCA parameter adjustment is disabled.

Format

dynamic-edca enable

undo dynamic-edca enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

A WLAN has only three non-overlapping channels on the 2.4 GHz frequency band. When APs are deployed densely, multiple APs have to work in the same channel, resulting in co-channel interference. This interference degrades network performance.

The dynamic EDCA parameter adjustment function allows APs to adjust EDCA parameters flexibly to reduce the possibility of collision, improve the throughput, and enhance user experience.

Example

Enable dynamic EDCA parameter adjustment.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] dynamic-edca enable
```

Related Topics

14.2.20 display rrm-profile

14.2.27 gap-threshold

Function

The **gap-threshold** command sets the load difference threshold for a static load balancing group.

The **undo gap-threshold** command restores the default load difference threshold for a static load balancing group.

By default, the load difference threshold of a static load balancing group is 20%.

Format

gap-threshold *gap-threshold-value*

undo gap-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
gap-threshold-value	Specifies the load difference threshold.	The value is an integer that ranges from 1 to 100. It indicates the threshold of the load difference among radios in a load balancing group, in percentage. The load difference refers to the difference between the number of STAs on radios.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

After the load difference threshold is configured using the **gap-threshold** command, the AP implements load balancing based on the difference between the number of users on different radios. The load balancing algorithm is as follows:

The AC calculates the load percentage of each radio in a load balancing group using the formula: Load percentage of a radio = (Number of associated STAs on the radio/Maximum number of STAs allowed on the radio) x 100%. The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a STA requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold (configured using the *gap-threshold-value* command). If the load difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC rejects the association request of the STA. If the STA continues sending association requests to this AP, the AC allows the STA to associate with the AP when the number of consecutive association attempts of the STA exceeds the maximum value configured.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the load difference threshold to 40% for the static load balancing group **coco**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-load-balance static-group name coco
[Huawei-wlan-sta-lb-static-coco] gap-threshold 40
```

Related Topics

14.2.43 sta-load-balance static-group

14.2.28 interference adjacent-channel threshold

Function

The **interference adjacent-channel threshold** command configures the alarm threshold for adjacent-channel interference.

The **undo interference adjacent-channel threshold** command restores the default alarm threshold for adjacent-channel interference.

By default, the alarm threshold for adjacent-channel interference is 50%.

Format

interference adjacent-channel threshold *threshold-value*

undo interference adjacent-channel threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold, which is the percentage of the adjacent-channel interference power against the maximum power.	The value is an integer that ranges from 1 to 100, in percentage.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Two APs with different center frequencies have overlapping areas, resulting in adjacent-channel interference. When APs are placed too close to each other or have strong signals, more noise is produced, degrading network performance.

After the **14.2.30 interference detect-enable** command is executed to enable interference detection, an AP can detect adjacent-channel interference. When the AP detects that adjacent-channel interference exceeds the alarm threshold configured using the **interference adjacent-channel threshold** command, the AP sends an alarm to the AC an alarm is generated.

Example

Set the alarm threshold for adjacent-channel interference to 52%.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio0
[Huawei-wlan-radio-2g-prof-radio0] interference detect-enable
[Huawei-wlan-radio-2g-prof-radio0] interference adjacent-channel threshold 52
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.2.30 interference detect-enable

14.2.29 interference co-channel threshold

Function

The **interference co-channel threshold** command configures the alarm threshold for co-channel interference.

The **undo interference co-channel threshold** command restores the default alarm threshold for co-channel interference.

By default, the alarm threshold for co-channel interference is 50%.

Format

interference co-channel threshold *threshold-value*

undo interference co-channel threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold, which is the percentage of the co-channel interference power against the maximum power.	The value is an integer that ranges from 1 to 100, in percentage.

Views

2G radio profile view, 5G radio profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Two APs working in the same frequency band interfere with each other. For example, on a large-scale WLAN (a university campus network), different APs often use the same channel. When there are overlapping areas among these APs, co-channel interference exists, degrading network performance.

After the **14.2.30 interference detect-enable** command is executed to enable interference detection, an AP can detect adjacent-channel interference. When the AP detects that co-channel interference exceeds the alarm threshold configured using the **interference co-channel threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for co-channel interference to 60%.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio0
[Huawei-wlan-radio-2g-prof-radio0] interference detect-enable
[Huawei-wlan-radio-2g-prof-radio0] interference co-channel threshold 60
```

Related Topics

14.1.106 display radio-2g-profile
14.1.107 display radio-5g-profile
14.2.30 interference detect-enable

14.2.30 interference detect-enable

Function

The **interference detect-enable** command enables interference detection.

The **undo interference detect-enable** command disables interference detection.

By default, interference detection is disabled.

Format

interference detect-enable

undo interference detect-enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

WLAN wireless channels are vulnerable to interference in surrounding radio environments, and the service quality is therefore degraded. If interference detection is configured, a monitor AP can know the radio environment in real time and report alarms to the AC in a timely manner.

Interference detection enables an AP to detect AP co-channel interference, AP adjacent-channel interference, and STA interference.

- AP co-channel interference: Two APs working on the same frequency band interfere with each other. For example, on a large-scale WLAN (a university campus network), different APs often use the same channel. When there are overlapping areas among these APs, co-channel interference exists, degrading network performance.
- AP adjacent-channel interference: Two APs with different center frequencies have overlapping areas, resulting in adjacent-channel interference. Therefore, if APs are placed too close to each other or they have strong signals, more noise will be produced, degrading network performance.
- STA interference: If there are many STAs that are managed by other APs around an AP, services of the STAs managed by the local AP may be affected.

Example

Enable interference detection.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio0
[Huawei-wlan-radio-2g-prof-radio0] interference detect-enable
```

14.2.31 interference station threshold

Function

The **interference station threshold** command configures the alarm threshold for STA interference.

The **undo interference station threshold** command restores the default alarm threshold for STA interference.

By default, the alarm threshold for STA interference is 32.

Format

interference station threshold *threshold-value*

undo interference station threshold

Parameters

Parameter	Description	Value
threshold-value	Specifies the alarm threshold.	The value is an integer that ranges from 1 to 256.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

If there are many STAs that are managed by other APs around an AP, services of the STAs managed by the local AP may be affected.

After the **14.2.30 interference detect-enable** command is executed to enable interference detection, an AP can detect STAs that are managed by other APs. When the AP detects that the number of such STAs exceeds the alarm threshold configured using the **interference station threshold** command, the AP sends an alarm to the AC.

Example

Set the alarm threshold for STA interference to 50.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name radio0
[Huawei-wlan-radio-2g-prof-radio0] interference station threshold 50
```

Related Topics

14.1.106 display radio-2g-profile

14.1.107 display radio-5g-profile

14.2.30 interference detect-enable

14.2.32 member (static load balancing group view)

Function

The **member** command adds an AP radio to a static load balancing group.

The **undo member** command deletes an AP radio from a load balancing group.

By default, no AP radio is added to a static load balancing group.

Format

member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } &<1-16>

undo member { { **ap-name** *ap-name* | **ap-id** *ap-id* } [**radio** *radio-id*] } &<1-16>

Parameters

Parameter	Description	Value
ap-name *ap-name*	Specifies the name of an AP. The AP name and radio ID identify a radio.	The AP name must exist.
ap-id *ap-id*	Specifies the ID of an AP. The AP ID and radio ID identify a radio.	The AP ID must exist.
radio *radio-id*	Specifies a radio ID. The radio ID and AP name identify a radio.	The value is an integer that ranges from 0 to 2.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use this command to add an AP radio to or delete an AP radio from a static load balancing group. When a STA requests to connect to an AP radio in a static load balancing group, the AC compares the load of the radio and other working radios in the load balancing group and determines whether to allow the STA to connect to the radio according to a load balancing algorithm.

Precautions

- If dual-band APs are used, traffic is load balanced among APs working on the same frequency band.
- Each load balancing group supports a maximum of 16 AP radios.

Example

Add radio 0 of AP **office** to the static load balancing group **coco**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-load-balance static-group name coco
[Huawei-wlan-sta-lb-static-coco] member ap-name office radio 0
```

Related Topics

14.2.43 sta-load-balance static-group

14.2.33 power auto-adjust enable

Function

The **power auto-adjust enable** command enables signal-strength-based power adjustment for APs.

The **undo power auto-adjust enable** command disables signal-strength-based power adjustment for APs.

By default, signal-strength-based power adjustment is disabled for an AP.

Format

power auto-adjust enable

undo power auto-adjust enable

Parameters

None

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The traditional radio power control function sets the power of an AP to a fixed value to keep the power of all STAs connecting to the AP the same.

You can run the **power auto-adjust enable** command to enable signal-strength-based power adjustment. This function enables an AP to detect the signal strength of a STA in a timely manner. If the AP detects that the signal strength of the STA is strong (for example, the STA is near the AP), the AP reduces its transmit power when sending packets. If the AP detects that the signal strength of the STA is weak (for example, the STA is far from the AP), the AP uses the normal transmit power to send radio signals.

Prerequisites

The power mode has been set to automatic mode using the **undo calibrate auto-txpower-select disable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable signal-strength-based power adjustment for APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] radio-2g-profile name huawei
[Huawei-wlan-radio-2g-prof-huawei] power auto-adjust enable
```

Related Topics

14.2.10 calibrate auto-txpower-select disable

14.2.34 reset wlan calibrate statistics

Function

The **reset wlan calibrate statistics** command clears radio calibration statistics.

Format

reset wlan calibrate statistics { **ap-name** *ap-name* | **ap-id** *ap-id* } **radio** *radio-id*

Parameters

Parameter	Description	Value
ap-name *ap-name*	Clears radio calibration statistics on the AP with the specified AP name. The AP name and radio ID identify a radio.	The AP name must already exist.
ap-id *ap-id*	Clears radio calibration statistics on the AP with the specified AP ID. The AP ID and radio ID identify a radio.	The AP ID must already exist.
radio *radio-id*	Clears calibration statistics about the radio with the specified radio ID. The radio ID and AP name identify a radio.	The value is an integer that ranges from 0 to 2.

Views

User view

Default Level

3: Management level

Usage Guidelines

Run the **reset wlan calibrate statistics** command to clear radio calibration statistics, including the number of times the radio environment deteriorates and number of times the radio channel and power are calibrated.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear calibration statistics about radio 0 of AP **office**.

```
<Huawei> reset wlan calibrate statistics ap-name office radio 0
```

Related Topics

14.2.25 display wlan calibrate statistics

14.2.35 rrm-profile (WLAN view)

Function

The **rrm-profile** command creates an RRM profile and displays the RRM profile view.

The **undo rrm-profile** command deletes an RRM profile.

By default, the system provides the RRM profile **default**. You can run the **14.2.20 display rrm-profile** command to view configuration of the RRM profile **default**.

Format

rrm-profile name *profile-name*

undo rrm-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of an RRM profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all RRM profiles.	The RRM profile **default** can be modified but cannot be deleted.

Views

WLAN view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

WLAN technology uses radio signals (such as 2.4 GHz or 5 GHz radio waves) as transmission medium. Radio signals will attenuate when transmitted over the air, degrading service quality for wireless users. Radio resource management (RRM) enables a WLAN to adapt to changes in the radio environment by dynamically adjusting radio resources. This improves service quality for wireless users.

Follow-up Procedure

Run the **14.2.36 rrm-profile (radio profile view)** command to bind the RRM profile to a radio profile so that the RRM profile can take effect.

Example

Create the RRM profile **rrm01**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name rrm01
[Huawei-wlan-rrm-prof-rrm01]
```

Related Topics

14.2.36 rrm-profile (radio profile view)

14.2.36 rrm-profile (radio profile view)

Function

The **rrm-profile** command binds an RRM profile to a radio profile.

The **undo rrm-profile** command unbinds an RRM profile from a radio profile.

By default, the RRM profile **default** is bound to a radio profile.

Format

rrm-profile *profile-name*

undo rrm-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an RRM profile.	The RRM profile name must already exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

2G radio profile view, 5G radio profile view

Default Level

2: Configuration level

Usage Guidelines

After you create an RRM profile using the **14.2.35 rrm-profile (WLAN view)** command, bind the RRM profile to a radio profile so that the RRM profile can take effect.

Example

Bind the RRM profile **rrm01** to the radio profile **office01**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name rrm01
[Huawei-wlan-rrm-prof-rrm01] quit
[Huawei-wlan-view] radio-2g-profile name office01
[Huawei-wlan-radio-2g-prof-office01] rrm-profile rrm01
```

Related Topics

14.2.35 rrm-profile (WLAN view)

14.2.37 scan-channel-set

Function

The **scan-channel-set** command configures an air scan channel set.

The **undo scan-channel-set** command restores the default air scan channel set.

By default, an air scan channel set contains all channels supported by the country code of an AP.

Format

scan-channel-set { **country-channel** | **dca-channel** | **work-channel** }

undo scan-channel-set

Parameters

Parameter	Description	Value
country-channel	Specifies an air scan channel set that contains all channels supported by the country code of an AP.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dca-channel	Specifies a calibration channel set as the air scan channel set. To configure a calibration channel set, run the **14.2.16 dca-channel channel-set** command.	-
work-channel	Specifies an air scan channel set that contains working channels of APs.	-

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **scan-channel-set** command to specify an air scan channel set for an AP, the AP scans channels in the channel set. The collected information is reported to the AC or server for radio calibration, or WIDS data analysis.

Precautions

- If the air scan channel set you specified contains all channels supported by the country code of the AP, the AP scans data on many channels but the channel scanning lasts for a long time, which may affect real-time data analysis.
- If you specify a calibration channel set as the air scan channel set, the AP scans data on a few channels. This reduces the channel scanning time, increases the terminal location accuracy, and reduces burden on the device.
- If you add only working channels of an AP to the air scan channel set, the AP only scans the working channels. If the radio working mode is set to **monitor**, the AP scans all channels supported by the country code.

Example

Configure an air scan channel set that contains all calibration channels.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] air-scan-profile name huawei
[Huawei-wlan-air-scan-prof-huawei] scan-channel-set dca-channel
```

Related Topics

14.2.17 display air-scan-profile

14.2.38 scan-interval

Function

The **scan-interval** command sets an air scan interval.

The **undo scan-interval** command restores the default air scan profile.

By default, the air scan interval is 60000 ms.

Format

scan-interval *scan-time*

undo scan-interval

Parameters

Parameter	Description	Value
scan-time	Specifies an air scan interval.	The value is an integer that ranges from 300 to 600000, in milliseconds.

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an air scan interval is specified using the **scan-interval** command, APs scan channels at the specified intervals.

Precautions

The air scan interval also applies to radio calibration, and WIDS functions.

If the customer has high requirements on real-time data analysis, configure a small air scan interval using the **scan-interval** command to improve the scan frequency; however, higher scan frequency indicates much larger impact on the services.

Example

Set the air scan interval to 3000 ms for APs.

```
<Huawei> system-view
[Huawei] wlan ac
```

```
[Huawei-wlan-view] air-scan-profile name huawei
[Huawei-wlan-air-scan-prof-huawei] scan-interval 3000
```

Related Topics

14.2.17 display air-scan-profile

14.2.39 scan-period

Function

The **scan-period** command sets the air scan period.

The **undo scan-period** command restores the default air scan period.

By default, the air scan period is 60 ms.

Format

scan-period *scan-time*

undo scan-period

Parameters

Parameter	Description	Value
scan-time	Specifies the air scan period.	The value is an integer that ranges from 60 to 100, in milliseconds.

Views

Air scan profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the air scan period is configured using the **scan-period** command, an AP continuously scans surrounding radio signals in the configured period. After the period expires, the AP reports the collected information to an AC or server. The information is used for radio calibration, or WIDS data analysis.

Precautions

A longer air scan period indicates more collected data and a more accurate data analysis result. However, if the air scan period is set too large, WLAN services are affected. You are advised to use the default value.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the air scan period to 80 ms for APs.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] air-scan-profile name huawei
[Huawei-wlan-air-scan-prof-huawei] scan-period 80
```

Related Topics

14.2.17 display air-scan-profile

14.2.40 sta-load-balance dynamic enable

Function

The **sta-load-balance dynamic enable** command enables the dynamic load balancing function.

The **undo sta-load-balance dynamic enable** command disables the dynamic load balancing function.

By default, the dynamic load balancing function is disabled.

Format

sta-load-balance dynamic enable

undo sta-load-balance dynamic enable

Parameters

None

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

Static load balancing limits the maximum number of AP radios to 16 and allows only radios on the same frequency band to join a load balancing group. Additionally, a load balancing group needs to be manually specified. Dynamic load balancing overcomes the limitations of static load balancing.

In dynamic load balancing mode, a STA sends broadcast Probe Request frame to scan available APs. The APs that receive the Probe Request frame all report the STA information to the AC. The AC adds these APs to a load balancing group, and then uses a load balancing algorithm to determine whether to allow access from the STA.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable dynamic load balancing.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] sta-load-balance dynamic enable
```

14.2.41 sta-load-balance dynamic gap-threshold

Function

The **sta-load-balance dynamic gap-threshold** command sets the load difference threshold for dynamic load balancing.

The **undo sta-load-balance dynamic gap-threshold** command restores the default load difference threshold for dynamic load balancing.

By default, the dynamic load difference threshold for load balancing is 20%.

Format

sta-load-balance dynamic gap-threshold *gap-threshold*

undo sta-load-balance dynamic gap-threshold

Parameters

Parameter	Description	Value
gap-threshold	Specifies the load difference threshold for dynamic load balancing.	The value is an integer that ranges from 1 to 100, in percentage.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

In dynamic load balancing mode, an AC uses a load balancing algorithm to determine whether to allow a STA to associate with a radio. The load balancing algorithm is as follows:

When a STA requests to connect to an AP, the AP will count the total number of access users on all radios. If the total number of access users does not exceed **start-threshold** configured using the **14.2.42 sta-load-balance dynamic start-threshold** command, the AP does not implement dynamic load balancing. The AP

implements dynamic load balancing only when the total number of access users on all radios exceeds **start-threshold**.

When implementing dynamic load balancing, the AC calculates the load percentage of each radio in a load balancing group using the formula: Load percentage of a radio = (Number of associated STAs on the radio/Maximum number of STAs allowed on the radio) x 100%. The AC compares load percentages of all radios in the load balancing group and obtains the smallest load percentage value. When a STA requests to associate with an AP radio, the AC calculates the difference between the radio's load percentage and the smallest load percentage value and compares the load difference with the threshold. If the load difference is smaller than the threshold, the AC allows the STA to associate with the radio. If not, the AC rejects the association request of the STA.

Example

Set the load difference threshold to 25 in the RRM profile **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] sta-load-balance dynamic gap-threshold 25
```

Related Topics

14.2.42 sta-load-balance dynamic start-threshold

14.2.42 sta-load-balance dynamic start-threshold

Function

The **sta-load-balance dynamic start-threshold** command sets the start threshold for dynamic load balancing.

The **undo sta-load-balance dynamic start-threshold** command restores the default start threshold for dynamic load balancing.

By default, the start threshold for dynamic load balancing is 10.

Format

sta-load-balance dynamic start-threshold *start-threshold*

undo sta-load-balance dynamic start-threshold

Parameters

Parameter	Description	Value
start-threshold	Specifies the start threshold for dynamic load balancing.	The value is an integer that ranges from 1 to 40.

 Copyright © Huawei Technologies Co., Ltd.

Views

RRM profile view

Default Level

2: Configuration level

Usage Guidelines

When a STA requests to connect to an AP, the AP will count the total number of access users on all radios. If the number of access users on the requested radio does not exceed **start-threshold**, the AP does not implement dynamic load balancing. The AP implements dynamic load balancing only after the number of access users exceeds **start-threshold**.

Example

Set the start threshold to 20 in the RRM profile **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] rrm-profile name huawei
[Huawei-wlan-rrm-prof-huawei] sta-load-balance dynamic start-threshold 20
```

Related Topics

14.2.41 sta-load-balance dynamic gap-threshold

14.2.43 sta-load-balance static-group

Function

The **sta-load-balance static-group** command creates a static load balancing group and displays the static load balancing group view.

The **undo sta-load-balance static-group** command deletes a static load balancing group.

By default, no static load balancing group is configured.

Format

sta-load-balance static-group name *group-name*

undo sta-load-balance static-group { **name** *group-name* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name *group-name*	Specifies the name of a load balancing group.	The value is a string of 1 to 35 plain-text characters. It does not contain any question mark (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all static load balancing groups.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

In static load balancing mode, APs providing the same services are manually added to a load balancing group. When a STA needs to access a WLAN, it sends an Association Request packet to an AC through an AP. The AC determines whether to allow access from the STA according to the load balancing algorithm.

To configure static load balancing, run the **sta-load-balance static-group** command in the WLAN view to create a static load balancing group and **14.2.32 member (static load balancing group view)** command to add APs to the group.

Example

Configure the static load balancing group named **new**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-load-balance static-group name new
[Huawei-wlan-sta-lb-static-new]
```

Related Topics

14.2.21 display sta-load-balance static-group

14.2.44 start-threshold

Function

The **start-threshold** command sets the start threshold for load balancing in a static load balancing group.

The **undo start-threshold** command deletes the configured start threshold for load balancing in a static load balancing group.

By default, the start threshold for load balancing in a static load balancing group is 10.

Format

start-threshold *start-threshold-value*

undo start-threshold

Parameters

Parameter	Description	Value
start-threshold-value	Specifies the start threshold for load balancing in a static load balancing group.	The value is an integer that ranges from 1 to 40.

Views

Static load balancing group view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to set the start threshold for load balancing in a static load balancing group. If the load on a radio does not reach the start threshold, the device does not implement load balancing control on access STAs.

Example

Set the start threshold for load balancing to 5 for the static load balancing group **coco**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-load-balance static-group name coco
[Huawei-wlan-sta-lb-static-coco] start-threshold 5
```

Related Topics

14.2.43 sta-load-balance static-group

14.3 WLAN Roaming Commands

14.3.1 display station roam-track

Function

The **display station roam-track** command displays the roaming track of an STA.

Format

display station roam-track sta-mac *mac-address*

Parameters

Parameter	Description	Value
sta-mac *mac-address*	Specifies the MAC address of a specified STA.	The value is in H-H-H format. An H is a hexadecimal number of four digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

During the roaming process of an STA, the AC records the STA's roaming track (that is, information about the APs that the STA connects to). You can run the **display station roam-track** command to view the roaming track of the STA.

Example

Display the roaming track of the STA with the MAC address 0011-43c7-d73e.

```
<Huawei> display station roam-track sta-mac 0011-43c7-d73e
Access SSID:huawei  Rx/Tx:link receive rate/link transmit rate(Mbps)  Z:Zero Roam
--------------------------------------------------------------------------------
L2/L3          AC IP                AP name              Radio ID
BSSID          TIME                 In/Out RSSI          Out Rx/Tx
--------------------------------------------------------------------------------
--             192.168.109.1        Huawei1              1
dcd2-fc9d-0bb0  2015/01/12 16:52:58    -51/-48            46/13
L2             192.168.109.1        Huawei2              1
e468-a34d-afb0  2015/01/12 16:55:45    -58/-              -/-
--------------------------------------------------------------------------------
Number: 1
```

Table 14-103 Description of the **display station roam-track** command output

Item	Description
Access SSID	SSID associated with an STA.
Rx/Tx	Negotiated rate between the STA and AP.
Z	Zero Roam
L2/L3	Roaming mode.
AC IP	IP address of an AC that the STA has associated with.
AP name	Name of an AP that the STA has associated with.
Radio ID	ID of a radio that the STA has associated with.
BSSID	BSSID of an AP that the STA has associated with.
TIME	Time duration when the STA has associated with an AP.
In/Out RSSI	RSSI of the STA when it disconnects from an AP before roaming and goes online on an AP after roaming.
Out Rx/Tx	Negotiated rate of the STA when it disconnects from an AP.
Number	Number of STA roaming tracks.

14.4 WLAN Security Configuration Commands

14.4.1 brute-force-detect interval

Function

The **brute-force-detect interval** command sets the interval for brute force key cracking detection.

The **undo brute-force-detect interval** command restores the default interval for brute force key cracking detection.

By default, the interval for brute force key cracking detection is 60 seconds.

Format

brute-force-detect interval *interval*

undo brute-force-detect interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for brute force key cracking detection.	The value is an integer that ranges from 10 to 120, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a brute force key cracking attack, an attacker tries all possible key combinations one by one to obtain the correct password. To improve password security, enable defense against brute force key cracking to prolong the the time used to crack passwords.

An AP checks whether the number of key negotiation failures during WPA/WPA2-PSK, WAPI-PSK, or WEP-Share-Key authentication of a user exceeds the threshold configured using the **brute-force-detect threshold** command. If so, the AP considers that the user is using the brute force method to crack the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets from the user until the dynamic blacklist entry ages out.

Follow-up Procedure

Run the **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the interval for brute force key cracking detection to 100 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable wpa-psk
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] brute-force-detect interval 100
```

Related Topics

14.4.55 wids attack detect enable
14.4.3 brute-force-detect threshold
14.4.23 dynamic-blacklist enable

14.4.2 brute-force-detect quiet-time

Function

The **brute-force-detect quiet-time** command sets the quiet time for an AP to report brute force key attacks to an AC.

The **undo brute-force-detect quiet-time** command restores the default quiet time for an AP to report brute force key attacks to an AC.

By default, the quiet time for an AP to report brute force key attacks to an AC is 600 seconds.

Format

brute-force-detect quiet-time *quiet-time-value*

undo brute-force-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report brute force key attacks to an AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If a attack source launches attacks repeatedly, a large number of repetitive alarms are generated. To prevent this situation, configure the quiet time function for attack detection. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

 Copyright © Huawei Technologies Co., Ltd.

To obtain attack information in time, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to avoid frequent alarm reports.

Follow-up Procedure

Run the **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the quiet time for an AP to report brute force key attacks to an AC to 300 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable wpa-psk
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] brute-force-detect quiet-time 300
```

Related Topics

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.3 brute-force-detect threshold

Function

The **brute-force-detect threshold** command sets the maximum number of key negotiation failures allowed within a brute force key cracking attack detection period.

The **undo brute-force-detect threshold** command restores the default maximum number of key negotiation failures allowed within a brute force key cracking attack detection period.

By default, an AP allows a maximum of 20 key negotiation failures within a brute force key cracking attack detection period.

Format

brute-force-detect threshold *threshold*

undo brute-force-detect threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
threshold	Specifies the number of key negotiation failures within a detection period.	The value is an integer that ranges from 1 to 100.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a brute force key cracking attack, an attacker tries all possible key combinations one by one to obtain the correct password. To improve password security, enable defense against brute force key cracking to prolong the the time used to crack passwords.

An AP checks whether the number of key negotiation failures during WPA/WPA2-PSK, WAPI-PSK, or WEP-Share-Key authentication of a user exceeds the threshold configured using the **brute-force-detect threshold** command. If so, the AP considers that the user is using the brute force method to crack the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets from the user until the dynamic blacklist entry ages out. If the threshold is set to a small value, the AP may incorrectly add authorized users to the dynamic blacklist, causing the users unable to go online.

Follow-up Procedure

Run the **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the maximum number of key negotiation failures allowed within a brute force key cracking attack detection period to 60.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable wpa-psk
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] brute-force-detect threshold 60
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.4 device report-interval

Function

The **device report-interval** command sets the interval at which an AP reports incremental wireless device information.

The **undo device report-interval** command restores the default interval at which an AP reports incremental wireless device information.

By default, an AP reports incremental wireless device information to an AC at an interval of 300 seconds.

Format

device report-interval *interval*

undo device report-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an AP reports incremental wireless device information.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The monitoring AP buffers information about detected wireless devices at the interval set using the **device report-interval** command. When the interval is reached, the monitoring AP reports the information to the AC and then clear the reported information.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval at which an AP reports incremental wireless device information to 120 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-profile name office
[Huawei-wlan-wids-prof-office] device report-interval 120
```

14.4.5 device synchronization-interval

Function

The **device synchronization-interval** command sets the interval at which an AP reports all wireless device information.

The **undo device synchronization-interval** command restores the default interval at which an AP reports all wireless device information.

By default, an AP reports all wireless device information to an AC at an interval of 360 minutes.

Format

device synchronization-interval *interval*

undo device synchronization-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an AP reports all wireless device information.	The value is an integer that ranges from 120 to 360, in minutes.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An AP reports wireless device information in the following modes:

- Incremental reporting: The AP reports the added, changed, or deleted information to the AC in real time.

- All information reporting: The AP periodically reports all wireless device information to the AC.

To ensure that detected device information is consistent on the AP and AC, run the **device synchronization-interval** command to enable the AP to periodically synchronize wireless device information to the AC.

Example

Set the interval at which an AP reports all wireless device information to 120 minutes.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-profile name office
[Huawei-wlan-wids-prof-office] device synchronization-interval 120
```

14.4.6 display references wids-profile

Function

The **display references wids-profile** command displays reference information about a WIDS profile.

Format

display references wids-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS profile.	The WIDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-profile** command to view reference information about a WIDS profile.

Example

Display reference information about the WIDS profile **huawei**.

```
<Huawei> display references wids-profile name huawei
-----------------------------------------------------------------------
```

```
Reference type              Reference name
-----------------------------------------------------------------------------
AP group                    default
AP ID                       0
-----------------------------------------------------------------------------
Total: 2
```

Table 14-104 Description of the **display references wids-profile** command output

Item	Description
Reference type	Type of the object that references the WIDS profile.
Reference name	Name of the object that references the WIDS profile.

14.4.7 display references wids-spoof-profile

Function

The **display references wids-spoof-profile** command displays reference information about a WIDS spoof SSID profile.

Format

display references wids-spoof-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wids-spoof-profile** command to view reference information about a WIDS spoof SSID profile.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display reference information about the WIDS spoof SSID profile **huawei**.

```
<Huawei> display references wids-spoof-profile name huawei
Profile type                Reference name
-------------------------------------------------------------
wids-profile                huawei
-------------------------------------------------------------
Total: 1
```

Table 14-105 Description of the **display references wids-spoof-profile** command output

Item	Description
Profile type	Type of the profile that references the WIDS spoof SSID profile.
Reference name	Name of the profile that references the WIDS spoof SSID profile.

14.4.8 display wids-profile

Function

The **display wids-profile** command displays information about a WIDS profile.

Format

display wids-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS profiles.	-
name *profile-name*	Displays information about a specified WIDS profile.	The WIDS profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-profile** command to view information about a WIDS profile.

Example

Display information about all WIDS profiles.

```
<Huawei> display wids-profile all
-----------------------------------------------------------
Profile name                Reference
-----------------------------------------------------------
default                      3
huawei                        2
office                      0
office01                     0
-----------------------------------------------------------
Total: 4
```

Table 14-106 Description of the **display wids-profile all** command output

Item	Description
Profile name	Name of a WIDS profile.
Reference	Number of times a WIDS profile is referenced.

Display information about the WIDS profile **huawei**.

```
<Huawei> display wids-profile name huawei
-----------------------------------------------------------
Device report interval(s)           : 10
Device synchronization interval(m)   : 120
Brute force detect interval(s)       : 20
Brute force detect threshold         : 20
Brute force quiet time(s)           : 600
Flood detect interval(s)            : 10
Flood detect threshold               : 1
Flood quiet time(s)                 : 600
Weak IV quiet time(s)                : 600
Spoof quiet time(s)                 : 600
Dynamic blacklist                   : enable
WIDS spoof profile                   : huawei
-----------------------------------------------------------
```

Table 14-107 Description of the **display wids-profile name** command output

Item	Description
Device report interval(s)	Interval at which an AP reports the detected incremental wireless device information. To set the interval, run the **14.4.4 device report-interval** command.

Item	Description
Device synchronization interval(m)	Interval at which an AP reports all the detected wireless device information. To set the interval, run the **14.4.5 device synchronization-interval** command.
Brute force detect interval(s)	Interval for brute force key cracking detection. To set the interval, run the **14.4.1 brute-force-detect interval** command.
Brute force detect threshold	Maximum number of key negotiation failures allowed within a brute force key cracking detection period. To set the maximum number, run the **14.4.3 brute-force-detect threshold** command.
Brute force quiet time(s)	Quiet time for an AP to report the detected brute force attacks to the AC. To set the quiet time, run the **14.4.2 brute-force-detect quiet-time** command.
Flood detect interval(s)	Flood attack detection interval. To set the interval, run the **14.4.24 flood-detect interval** command.
Flood detect threshold	Flood attack detection threshold. To set the threshold, run the **14.4.26 flood-detect threshold** command.
Flood quiet time(s)	Quiet time for an AP to report the detected flood attacks to the AC. To set the quiet time, run the **14.4.25 flood-detect quiet-time** command.
Weak IV quiet time(s)	Quiet time for an AP to report the detected weak IV attacks to the AC. To set the quiet time, run the **14.4.52 weak-iv-detect quiet-time** command.
Spoof quiet time(s)	Quiet time for an AP to report the detected spoofing attacks to the AC. To set the quiet time, run the **14.4.37 spoof-detect quiet-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dynamic blacklist	Whether the dynamic blacklist function is enabled. To configure the function, run the **14.4.23 dynamic-blacklist enable** command.
WIDS spoof profile	WIDS spoof profile bound to the WIDS profile. To bind a WIDS spoof profile to a WIDS profile, run the **14.4.59 wids-spoof-profile (WIDS profile view)** command.

Related Topics

14.4.4 device report-interval
14.4.5 device synchronization-interval
14.4.1 brute-force-detect interval
14.4.3 brute-force-detect threshold
14.4.2 brute-force-detect quiet-time
14.4.24 flood-detect interval
14.4.26 flood-detect threshold
14.4.25 flood-detect quiet-time
14.4.52 weak-iv-detect quiet-time
14.4.37 spoof-detect quiet-time
14.4.23 dynamic-blacklist enable
14.4.59 wids-spoof-profile (WIDS profile view)

14.4.9 display wids-spoof-profile

Function

The **display wids-spoof-profile** command displays information about a WIDS spoof SSID profile.

Format

display wids-spoof-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WIDS spoof SSID profiles.	-
name *profile-name*	Displays information about a specified WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wids-spoof-profile** command to view information about a WIDS spoof SSID profile.

Example

Display information about all WIDS spoof SSID profiles.

```
<Huawei> display wids-spoof-profile all
-------------------------------------------------------------
Profile name                  Reference
-------------------------------------------------------------
huawei                          0
office1                       1
-------------------------------------------------------------
Total: 2
```

Table 14-108 Description of the **display wids-spoof-profile all** command output

Item	Description
Profile name	Name of a WIDS spoof SSID profile.
Reference	Number of times a WIDS spoof SSID profile is referenced.

Display information about the WIDS spoof SSID profile **huawei**.

```
<Huawei> display wids-spoof-profile name huawei
-------------------------------------------------------------
ID      Pattern rule
-------------------------------------------------------------
0       ^HUAWE[1l]$
-------------------------------------------------------------
Total: 1
```

Table 14-109 Description of the **display wids-spoof-profile name** command output

Item	Description
ID	Index.
Pattern rule	Matching rule for spoofing SSIDs.

14.4.10 display references security-profile

Function

The **display references security-profile** command displays reference information about a security profile.

Format

display references security-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified security profile.	The security profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a security profile.

Example

Display reference information about the security profile **security-profile1**.

```
<Huawei> display references security-profile name security-profile1
---------------------------------------------
Reference type          Reference name
---------------------------------------------
VAP profile             vap-profile1
---------------------------------------------
Total: 1
```

Table 14-110 Description of the **display references security-profile** command output

Item	Description
Reference type	Type of the profile that references a security profile.
Reference name	Name of the profile that references a security profile.

14.4.11 display references sta-blacklist-profile

Function

The **display references sta-blacklist-profile** command displays reference information about a STA blacklist profile.

Format

display references sta-blacklist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a STA blacklist profile.	The STA blacklist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a STA blacklist profile.

Example

Display reference information about the STA blacklist profile **sta-blacklist-profile1**.

```
<Huawei> display references sta-blacklist-profile name sta-blacklist-profile1
--------------------------------------------
Reference type          Reference name
--------------------------------------------
```

```
VAP profile          vap-profile1
---------------------------------------------
Total: 1
```

Table 14-111 Description of the **display references sta-blacklist-profile** command output

Item	Description
Reference type	Type of the profile that references the STA blacklist profile.
Reference name	Name of the profile that references the STA blacklist profile.

14.4.12 display references sta-whitelist-profile

Function

The **display references sta-whitelist-profile** command displays reference information about a STA whitelist profile.

Format

display references sta-whitelist-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a STA whitelist profile.	The STA whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view reference information about a STA whitelist profile.

Example

Display reference information about the STA whitelist profile **sta-whitelist-profile1**.

```
<Huawei> display references sta-whitelist-profile name sta-whitelist-profile1
--------------------------------------------------------------------------------
Reference type              Reference name
--------------------------------------------------------------------------------
AP system profile           ap-system-profile1
--------------------------------------------------------------------------------
Total: 1
```

Table 14-112 Description of the **display references sta-whitelist-profile** command output

Item	Description
Reference type	Type of the profile that references the STA whitelist profile.
Reference name	Name of the profile that references the STA whitelist profile.

14.4.13 display security-profile

Function

The **display security-profile** command displays configuration and reference information about a security profile.

Format

display security-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all security profiles.	-
name *profile-name*	Displays information about a specified security profile.	The security profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the command to view configuration and reference information about a specified security profile or all security profiles.

Example

Display configurations of all security profiles.

```
<Huawei> display security-profile all
-----------------------------------------------------------
Profile name                Reference
-----------------------------------------------------------
default                     1
default-wds                 1

security-profile1           0
-----------------------------------------------------------
Total: 3
```

Table 14-113 Description of the **display security-profile all** command output

Item	Description
Profile name	Name of the security profile.
Reference	Number of times a security profile is referenced.

Display information about the security profile **default**.

```
<Huawei> display security-profile name default
-----------------------------------------------------------
Security policy             : Open system
Encryption                  : -
-----------------------------------------------------------
WEP's configuration
Key 0                       : *****
Key 1                       : *****
Key 2                       : *****
Key 3                       : *****
Default key ID              : 0
-----------------------------------------------------------
WPA/WPA2's configuration
PTK update                  : disable
PTK update interval(s)      : 43200
-----------------------------------------------------------
WAPI's configuration
CA certificate filename     : -
ASU certificate filename    : -
AC certificate filename     : -
AC private key filename     : -
WAPI source interface       : -
Authentication server IP    : -
WAI timeout(s)              : 60
BK update interval(s)       : 43200
BK lifetime threshold(%)    : 70
USK update method           : Time-based
USK update interval(s)      : 86400
MSK update method           : Time-based
MSK update interval(s)      : 86400
Cert auth retrans count     : 3
USK negotiate retrans count : 3
MSK negotiate retrans count : 3
-----------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 14-114 Description of the **display security-profile name** command output

Item	Description
Security policy	Security policy. The following security policies are supported: ● Open system: open system authentication ● Share key: WEP Shared Key ● WPA 802.1X ● WPA2 802.1X ● WPA-WPA2 802.1X ● WPA PSK: WPA Pre-Shared Key ● WPA2 PSK: WPA2 Pre-Shared Key ● WPA-WPA2 PSK: WPA-WPA2 Pre-Shared Key ● WAPI PSK: WAPI Pre-Shared Key ● WAPI certificate To configure the parameter, run the **14.4.34 security wep**, **14.4.31 security dot1x**, **14.4.32 security psk** and **14.4.33 security wapi** commands.
Encryption	Encryption mode. The following encryption modes are supported: TKIP, AES, AES-TKIP, WEP-40, WEP-104, WEP-128, and SMS4. WAPI encryption uses SMS4. To configure the parameter, run the **14.4.54 wep key**, **14.4.31 security dot1x** and **14.4.32 security psk** commands.
Key *key-id*	Key ID. To configure the parameter, run the **14.4.54 wep key** command.
Default key ID	Default key ID. To configure the parameter, run the **14.4.53 wep default-key** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PTK update	Whether to enable periodic PTK update in WPA, WPA2 or WPA-WPA2 authentication and encryption. ● enable: Enables periodic PTK update. ● disable: Disables periodic PTK update. To configure the parameter, run the **14.4.60 wpa ptk-update enable** command.
PTK update interval(s)	The interval for updating PTKs in WPA, WPA2 or WPA-WPA2 authentication and encryption. The value is an integer in seconds. To configure the parameter, run the **14.4.61 wpa ptk-update ptk-update-interval** command.
CA certificate filename	CA certificate file name. To configure the parameter, run the **14.4.45 wapi import certificate** command.
ASU certificate filename	File name of the authentication server unit (ASU) certificate. To configure the parameter, run the **14.4.45 wapi import certificate** command.
AC certificate filename	AC certificate file name. To configure the parameter, run the **14.4.45 wapi import certificate** command.
AC private key filename	AC private key file name. To configure the parameter, run the **14.4.46 wapi import private-key** command.
WAPI source interface	WAPI source interface. To configure the parameter, run the **14.4.50 wapi source interface** command.
Authentication server IP	IP address of the ASU certificate server. To configure the parameter, run the **14.4.42 wapi asu** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
WAI timeout(s)	Timeout period of an association. To configure the parameter, run the **14.4.49 wapi sa-timeout** command.
BK update interval(s)	Interval for updating the base key (BK). To configure the parameter, run the **14.4.43 wapi bk** command.
BK lifetime threshold(%)	Threshold for triggering BK update. To configure the parameter, run the **14.4.43 wapi bk** command.
USK update method	Whether the USK is updated based on a time interval or a packet count. To configure the parameter, run the **14.4.47 wapi key-update** command.
USK update interval(s)	Time-based interval for updating the unicast session key (USK). To configure the parameter, run the **14.4.51 wapi usk** command.
MSK update method	Whether the MSK is updated based on a time interval or a packet count. To configure the parameter, run the **14.4.47 wapi key-update** command.
MSK update interval(s)	Time-based interval for updating the MBMS service key (MSK). To configure the parameter, run the **14.4.48 wapi msk** command.
Cert auth retrans count	Number of retransmissions of certificate authentication packets. To configure the parameter, run the **14.4.44 wapi cert-retrans-count** command.
USK negotiate retrans count	Number of retransmissions of USK negotiation packets. To configure the parameter, run the **14.4.51 wapi usk** command.
MSK negotiate retrans count	Number of retransmissions of MSK negotiation packets. To configure the parameter, run the **14.4.48 wapi msk** command.

 Copyright © Huawei Technologies Co., Ltd.

14.4.14 display sta-blacklist-profile

Function

The **display sta-blacklist-profile** command displays configuration and reference information about a STA blacklist profile.

Format

display sta-blacklist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all STA blacklist profiles.	-
name *profile-name*	Displays information about a specified STA blacklist profile.	The STA blacklist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring STA blacklists for VAPs, you can run this command to check whether a MAC address is in the blacklists.

Example

Display reference information about all STA blacklist profiles.

```
<Huawei> display sta-blacklist-profile all
-----------------------------------------------------------
Profile name                    Reference
-----------------------------------------------------------
sta-blacklist-profile1           1
-----------------------------------------------------------
Total: 1
```

Table 14-115 Description of the **display sta-blacklist-profile all** command output

Item	Description
Profile name	Name of a STA blacklist profile.

Item	Description
Reference	Number of times a STA blacklist profile is referenced.

Display information about the STA blacklist profile **sta-blacklist-profile1**.

```
<Huawei> display sta-blacklist-profile name sta-blacklist-profile1
-----------------------------------------------------------
Index      MAC
-----------------------------------------------------------
0          0021-1111-2222
-----------------------------------------------------------
Total: 1
```

Table 14-116 Description of the **display sta-blacklist-profile name** command output

Item	Description
Index	Blacklist index.
MAC	MAC address of a STA in the blacklist. To configure the parameter, run the **14.4.40 sta-mac** command.

Related Topics

14.4.40 sta-mac

14.4.15 display station dynamic-blacklist

Function

The **display station dynamic-blacklist** command displays the dynamic blacklist on an AP.

Format

display station dynamic-blacklist { **ap-id** *ap-id* | **ap-name** *ap-name* }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Displays information about STAs that are denied access on the AP with a specified ID.	The AP ID must exist.

Parameter	Description	Value
ap-name *ap-name*	Displays information about STAs that are denied access on the AP with a specified name.	The AP name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a STA dynamic blacklist on an AP. The blacklist helps control access of STAs, for example, forbidding STAs with bogus IP addresses to go online. If a STA is not allowed to go online, the STA is added to the dynamic blacklist. Before the dynamic blacklist entry ages out, the STA cannot associate with the AP. The aging time of the dynamic blacklist entries is 10 minutes. After the aging time is reached, the dynamic blacklist entries are automatically deleted. During this period, if the STA on an entry is added to the blacklist again, the aging time of the entry is updated and recalculated.

The administrator can run this command to check STAs in the blacklist and the reasons for adding the STAs to the blacklist.

Example

Display the dynamic blacklist on AP.

```
<Huawei> display station dynamic-blacklist ap-name huawei
Total: 1
--------------------------------------------------------------------------------
STA MAC          Time left(s)   Reason
--------------------------------------------------------------------------------
581f-28fc-7ead   160            static ip
--------------------------------------------------------------------------------
```

Table 14-117 Description of the **display station dynamic-blacklist** command output

Item	Description
STA MAC	MAC address of a STA.
Time left(s)	Remaining aging period, in seconds. To configure the parameter, run the **14.4.22 dynamic-blacklist aging-time** command.

Item	Description
Reason	STA access denial reason. • static ip: The AP is configured to deny access of STAs with bogus IP addresses, and the STA has a static IP address configured. • broadcast flood: The AP is configured to detect and defend against broadcast flood attacks, and the STA initiates a broadcast flood attack.

Related Topics

14.4.22 dynamic-blacklist aging-time

14.4.16 display sta-whitelist-profile

Function

The **display sta-whitelist-profile** command displays configuration and reference information about a STA whitelist profile.

Format

display sta-whitelist-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all STA whitelist profiles.	-
name *profile-name*	Displays information about a specified STA whitelist profile.	The STA whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After configuring a STA whitelist on a device, you can run this command to check whether a MAC address is in the whitelist.

Example

Display reference information about all STA whitelist profiles.

```
<Huawei> display sta-whitelist-profile all
-----------------------------------------------------------
Profile name                    Reference
-----------------------------------------------------------
sta-whitelist-profile1            1
-----------------------------------------------------------
Total: 1
```

Table 14-118 Description of the **display sta-whitelist-profile all** command output

Item	Description
Profile name	Name of a STA whitelist profile.
Reference	Number of times a STA whitelist profile is referenced.

Display information about the STA whitelist profile **sta-whitelist-profile1**.

```
<Huawei> display sta-whitelist-profile name sta-whitelist-profile1
-----------------------------------------------------------
Index      MAC
-----------------------------------------------------------
0          0021-1111-2222
-----------------------------------------------------------
Total: 1
```

Table 14-119 Description of the **display sta-whitelist-profile name** command output

Item	Description
Index	Whitelist index.
MAC	MAC address of a STA in the whitelist. To configure the parameter, run the **14.4.40 sta-mac** command.

Related Topics

14.4.40 sta-mac

14.4.17 display wlan ids attack-detected

Function

The **display wlan ids attack-detected** command displays information about the detected attacking devices.

Format

display wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all types of attacking devices.	-
flood	Displays information about devices launching flood attacks.	-
spoof	Displays information about devices launching spoofing attacks.	-
wapi-psk	Displays information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays information about devices launching weak IV attacks.	-
wep-share-key	Displays information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays information about the detected attacking devices with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run the **display wlan ids attack-detected** command to view information about the attacking devices.

Prerequisites

The attack detection functions of all types have been enabled using the **14.4.55 wids attack detect enable** command.

Example

Display information of all current attacking devices.

```
<Huawei> display wlan ids attack-detected all
#AP: Number of monitor APs that have detected the device
AT: Last detcted attack type
CH: Channel number
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
--------------------------------------------------------------------------------
MAC address     AT     CH   RSSI(dBm)  Last detected time     #AP
--------------------------------------------------------------------------------
000b-c002-9c81  pbr    165  -87        2014-11-20/15:51:13    1
0024-2376-03e9  pbr    165  -84        2014-11-20/15:52:13    1
0046-4b74-691f  act    165  -67        2014-11-20/15:43:33    1
00bc-71b7-171d  pbr    165  -88        2014-11-20/15:41:43    1
00bc-71b7-171f  act    165  -87        2014-11-20/15:44:03    1
--------------------------------------------------------------------------------
Total: 5, printed: 5
```

Table 14-120 Description of the **display wlan ids attack-detected all** command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of the attack type.

Item	Description
CH	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.
Last detected time	Last time at which an attack is detected.
#AP	Number of APs which detect this attack.

Display information of an attacking device with the specified MAC address.

```
<Huawei> display wlan ids attack-detected mac-address 8c70-5a47-aad0
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
--------------------------------------------------------------------------------
MAC address                        : 8c70-5a47-aad0
Number of detected APs             : 1
Channel                            : 165
RSSI(dBm)                          : -80
Reported AP 1
  AP name                          : ap-13
  Flood attack type                : pbr
  First detected time(Flood)       : 2014-11-20/15:50:33
  Spoof attack type                : -
  First detected time(Spoof)       : -
  First detected time(Weak-iv)     : -
  First detected time(WEP)         : -
  First detected time(WPA)         : -
  First detected time(WPA2)        : -
  First detected time(WAPI)        : -
--------------------------------------------------------------------------------
```

Table 14-121 Description of the **display wlan ids attack-detected mac-address** *mac-address* command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.

Item	Description
Number of detected APs	Number of APs which detect this attack.
Channel	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.
Reported AP	Information of the AP which detects the attack.
AP name	Name of the AP which detects the attack.
Flood attack type	Flood attacks detected by the AP.
Spoof attack type	Spoofing attacks detected by the AP.
First detected time	First time when an attack is detected by an AP.

Related Topics

14.4.55 wids attack detect enable

14.4.18 display wlan ids attack-detected statistics

Function

The **display wlan ids attack-detected statistics** command displays the number of attacks detected.

Format

display wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, you can run the **display wlan ids attack-detected statistics** command to view the total number of all types of attacks.

Prerequisites

The attack detection functions of all types have been enabled using the **14.4.55 wids attack detect enable** command.

Example

Display the number of attacks detected.

```
<Huawei> display wlan ids attack-detected statistics
Attack tracking since: 2015-01-27/12:02:11
-------------------------------------------------------------------------------
Type                                        Total
-------------------------------------------------------------------------------
Probe request frame flood attack                  : 0
Authentication request frame flood attack           : 0
Deauthentication frame flood attack                 : 0
Association request frame flood attack              : 0
Disassociation request frame flood attack           : 0
Reassociation request frame flood attack            : 0
Action frame flood attack                         : 0
EAPOL start frame flood attack                    : 0
EAPOL logoff frame flood attack                   : 0
Weak IVs detected                               : 0
Spoofed deauthentication frame attack               : 0
Spoofed disassociation frame attack               : 0
Other types of spoofing frame attack              : 0
WEP share-key attack                            : 0
WPA attack                                      : 0
WPA2 attack                                     : 0
WAPI attack                                     : 0
-------------------------------------------------------------------------------
```

Table 14-122 Description of the display wlan ids attack-detected statistics command output

Item	Description
Type	Attack type: • Probe request frame flood attack • Authentication request frame flood attack • Deauthentication frame flood attack • Association request frame flood attack • Disassociation request frame flood attack • Reassociation request frame flood attack • Action frame flood attack • EAPOL start frame flood attack • EAPOL logoff frame flood attack • Weak IVs detected • Spoofed deauthentication frame attack • Spoofed disassociation frame attack • Other types of spoofing frame attack • WEP share-key attack: brute force cracking attack in WEP-SK authentication mode • WPA attack: brute force cracking attack in WPA-PSK authentication mode • WPA2 attack: brute force cracking attack in WPA2-PSK authentication mode • WAPI attack: brute force cracking attack in WPAI authentication mode
Total	Total number of attacks detected.

Related Topics

14.4.55 wids attack detect enable

14.4.19 display wlan ids attack-history

Function

The **display wlan ids attack-history** command displays historical records about the attacking devices detected.

Format

display wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays historical records about all types of attacking devices.	-
flood	Displays historical records about devices launching flood attacks.	-
spoof	Displays historical records about devices launching spoofing attacks.	-
wapi-psk	Displays historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Displays historical records about devices launching weak IV attacks.	-
wep-share-key	Displays historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Displays historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Displays information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Displays historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After attack detection is enabled, information about the detected attacking devices is saved in the attacking device list. If an attacking device no longer launches an attack, the device is removed from the attacking device list and saved to the historical attacking device list. You can run the **display wlan ids attack-history** command to check historical records about the attacking devices detected.

Prerequisites

The attack detection functions of all types have been enabled using the **14.4.55 wids attack detect enable** command.

Example

Display historical records of all attacking devices.

```
<Huawei> display wlan ids attack-history all
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  wiv: Weak IV detected
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame      eapl: EAPOL logoff frame
saf: Spoofed disassociation frame
sdf: Spoofed deauthentication frame
otsf: Other types of spoofing frames
AP: Name of the monitor AP that has detected the device
AT: Attack type              CH: Channel number
--------------------------------------------------------------------------------
MAC address     AT     CH   RSSI(dBm)  Last detected time    AP
--------------------------------------------------------------------------------
2477-039a-37ec  pbr    165  -86        2014-11-20/15:51:43   ap-13
00bc-71b7-171d  pbr    165  -88        2014-11-20/15:41:43   ap-13
2477-039a-0bf4  pbr    165  -81        2014-11-20/15:41:53   ap-13
--------------------------------------------------------------------------------
Total: 3, printed: 3
```

Table 14-123 Description of the **display wlan ids attack-history all** command output

Item	Description
MAC address	• For spoofing attacks, this parameter indicates the basic service set identifier (BSSID) that forges the MAC address of an AP. • For other types of attacks, this parameter indicates the MAC address of the device launching attacks.
AT	Acronym of attack type.

Item	Description
CH	Channel in which the last attack is detected.
RSSI(dBm)	Average received signal strength indicator (RSSI) of the attack frames detected.
Last detected time	Last time at which an attack is detected.
AP	Name of the monitor AP.

Related Topics

14.4.55 wids attack detect enable

14.4.20 display wlan ids dynamic-blacklist

Function

The **display wlan ids dynamic-blacklist** command displays information about devices in the dynamic blacklist.

Format

display wlan ids dynamic-blacklist { **all** | **ap-id** *ap-id* | **ap-name** *ap-name* | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all devices in the dynamic blacklist.	-
ap-id *ap-id*	Displays information about attacking devices detected by the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about attacking devices detected by the AP with a specified name.	The AP name must exist.
mac-address *mac-address*	Displays information about attacking devices with a specified MAC address.	The MAC address must exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

An AP uses attack detection and dynamic blacklist functions to add a detected attacking device to the dynamic blacklist, and rejects packets sent from this device until the device entry in the dynamic blacklist ages. You can run the **display wlan ids dynamic-blacklist** command to view information about devices in the dynamic blacklist.

Prerequisites

- The dynamic blacklist function has been enabled using the **14.4.23 dynamic-blacklist enable** command.
- The attack detection functions of all types have been enabled using the **14.4.55 wids attack detect enable** command.

Example

Display information about all devices in the dynamic blacklist.

```
<Huawei> display wlan ids dynamic-blacklist all
#AP: Number of monitor APs that have detected the device
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame
--------------------------------------------------------------------------------
MAC address       Last detected time    Reason   #AP
--------------------------------------------------------------------------------
0020-1408-019f    2014-11-20/11:15:53   act      1
00bc-71b7-171f    2014-11-20/11:15:53   act      1
00d5-5862-641d    2014-11-20/11:15:43   pbr      1
--------------------------------------------------------------------------------
Total: 3, printed: 3
```

Table 14-124 Description of the **display wlan ids dynamic-blacklist all** command output

Item	Description
MAC address	MAC address of the device in the dynamic blacklist.
Last detected time	Latest time of device attack detection.
Reason	Reason why the device is added to the dynamic blacklist. The values here are the acronyms of attack types. For details, see **14.4.17 display wlan ids attack-detected**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
#AP	Number of the AP that detects the device and adds it to the dynamic blacklist.

Display information about all devices added to the dynamic blacklist by AP **huawei**.

```
<Huawei> display wlan ids dynamic-blacklist ap-name huawei
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame
--------------------------------------------------------------------------------
MAC address       Last detected time    Reason
--------------------------------------------------------------------------------
0020-1408-019f    2014-11-20/11:15:53   act
00bc-71b7-171f    2014-11-20/11:15:53   act
00d5-5862-641d    2014-11-20/11:15:43   pbr
--------------------------------------------------------------------------------
Total: 3, printed: 3
```

Display information about specified devices in the dynamic blacklist.

```
<Huawei> display wlan ids dynamic-blacklist mac-address e468-a350-8b3d
act: Action frame            asr: Association request
aur: Authentication request  daf: Deauthentication frame
dar: Disassociation request  eapl: EAPOL logoff frame
pbr: Probe request           rar: Reassociation request
eaps: EAPOL start frame
------------------------------------------------------------
 Last detected time    Reason
------------------------------------------------------------
 2014-11-20/11:15:53   act
 2014-11-20/11:15:53   act
 2014-11-20/11:15:43   pbr
------------------------------------------------------------
Total: 3, printed: 3
```

Table 14-125 Description of the **display wlan ids dynamic-blacklist mac-address** command output

Item	Description
Last detected time	Last time when the device is detected.
Reason	Reason why the device is added to the dynamic blacklist.

Related Topics

14.4.23 dynamic-blacklist enable

14.4.55 wids attack detect enable

14.4.21 display wlan wapi certificate

Function

The **display wlan wapi certificate** command displays the content of a certificate file.

Format

display wlan wapi certificate file-name *file-name*

Parameters

Parameter	Description	Value
file-name *file-name*	Specifies a certificate file name.	The value is a string of 1 to 255 visible characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ") or spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view content of certificate files imported to the device.

In the command, *file-name* must specify the complete path of a certificate file. For example, if the certificate file **as.cer** is saved in the flash memory, run **display wlan wapi certificate file-name flash:/as.cer** command.

Example

Display content of certificate file **as.cer**.

```
<Huawei> display wlan wapi certificate file-name flash:/as.cer
Certificate:
Data:
  Version: V3
  Serial number:
      50 FA CF CA
  Signature algorithm: sha256ECDSA192
```

```
Issuer:
    C = CN
    O = 0003
    OU = CUCC
    CN = as_test_1@ASU
Validity:
  Not before: 2013-01-19 16:54:34 UTC
  Not after : 2033-01-19 16:54:34 UTC
Subject:
    C = CN
    O = 0003
    OU = CUCC
    CN = as_test_1@ASU
Subject public key information:
  Public key algorithm: ECC
  Public key: (392 bit)
    04 31 AB F2 76 AE E4 BD EF E6 ED CA 93 C0 04 C8
    C9 C9 BF 6F A3 6A F9 A1 9E 35 3E 9B 08 21 EF 20
    5E 82 C1 42 2D A9 42 C3 CE 91 98 7F 21 83 7C 71
    3A
```

Table 14-126 Description of the **display wlan wapi certificate** command output

Item	Description
Version	Version of the X.509 certificate.
Serial number	Serial number of the certificate.
Signature algorithm	Algorithm used to calculate the signature.
Issuer	Certificate issuer.
Validity	Valid period of the certificate, specified by the start date and end date.
Subject	Subject of the certificate.
Subject public key information	Information about the public key of the certificate.

14.4.22 dynamic-blacklist aging-time

Function

The **dynamic-blacklist aging-time** command sets an aging time for a dynamic blacklist.

The **undo dynamic-blacklist aging-time** command restores the aging time of a dynamic blacklist to the default value.

By default, the aging time of a dynamic blacklist is 600 seconds.

Format

dynamic-blacklist aging-time *time*

undo dynamic-blacklist aging-time

Parameters

Parameter	Description	Value
time	Specifies the aging time at the expiry of which a specified MAC address is removed from the dynamic blacklist.	The value is an integer that ranges from 180 to 3600, in seconds.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

When detecting attacks from a STA, an AP reports the STA to the AC, forbids the STA to go online, and rejects any packets sent from the STA. As long as the STA is blacklisted, it cannot go online again even if it no longer launches attacks. To avoid that, you can run the **dynamic-blacklist aging-time** command to configure an aging time for the dynamic blacklist. If the configured aging time expires and the AP detects no attack from the STA, the STA is once again allowed to go online.

Example

Set the aging time of the dynamic blacklist to 300 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name huawei
[Huawei-wlan-ap-system-prof-huawei] dynamic-blacklist aging-time 300
```

Related Topics

14.4.23 dynamic-blacklist enable

14.4.23 dynamic-blacklist enable

Function

The **dynamic-blacklist enable** command enables the dynamic blacklist function.

The **undo dynamic-blacklist enable** command disables the dynamic blacklist function.

By default, the dynamic blacklist function is disabled.

Format

dynamic-blacklist enable

 Copyright © Huawei Technologies Co., Ltd.

undo dynamic-blacklist enable

Parameters

None

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **dynamic-blacklist enable** command to enable the dynamic blacklist function. When detecting flood attacks or brute force password cracking attacks from a device, an AP reports the device to the AC, and the AC adds the device to a dynamic blacklist. Any packets sent from the device are rejected until the dynamic blacklist entry ages.

An AP can use the dynamic blacklist to filter out the blacklisted wireless devices to avoid malicious attacks.

Follow-up Procedure

Run the **14.4.22 dynamic-blacklist aging-time** command to set an aging time for the dynamic blacklist.

Example

Enable the dynamic blacklist function.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] dynamic-blacklist enable
```

Related Topics

14.4.22 dynamic-blacklist aging-time

14.4.24 flood-detect interval

Function

The **flood-detect interval** command sets the flood attack detection interval.

The **undo flood-detect interval** command restores the default flood attack detection interval.

By default, the flood attack detection interval is 60 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

flood-detect interval *interval*

undo flood-detect interval

Parameters

Parameter	Description	Value
interval	Specifies the interval for flood attack detection.	The value is an integer that ranges from 10 to 120, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A flood attack occurs when an AP receives a large number of packets of the same type within a short period. As a result, the AP is flooded by too many attack packets to process service packets from authorized wireless terminals.

After the flood attack detection function is enabled, an AP counts the number of packets of the same type that it receives from a user at regular intervals. When the number exceeds a specified threshold, the AP considers that the user launches a flood attack. If the dynamic blacklist function is enabled, the user will be added to a dynamic blacklist.

Follow-up Procedure

Run the **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection interval to 120s.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable flood
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] flood-detect interval 120
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.25 flood-detect quiet-time

Function

The **flood-detect quiet-time** command sets the quiet time for an AP to report the detected flood attacks to the AC.

The **undo flood-detect quiet-time** command restores the quiet time for an AP to report the detected flood attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected flood attacks to the AC.

Format

flood-detect quiet-time *quiet-time-value*

undo flood-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected flood attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If a attack source launches attacks repeatedly, a large number of repetitive alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

 Copyright © Huawei Technologies Co., Ltd.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Follow-up Procedure

Run the **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the quiet time to 300 seconds for an AP to report the detected flood attacks to the AC.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable flood
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] flood-detect quiet-time 300
```

Related Topics

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.26 flood-detect threshold

Function

The **flood-detect threshold** command sets the flood attack detection threshold. A flood attack occurs when an AP receives a large number of packets of the same type within a short period.

The **undo flood-detect threshold** command restores the default flood attack detection threshold.

By default, the flood attack detection threshold is 300 seconds.

Format

flood-detect threshold *threshold*

undo flood-detect threshold

Parameters

Parameter	Description	Value
threshold	Specifies the flood attack detection threshold.	The value is an integer that ranges from 1 to 1000.

 Copyright © Huawei Technologies Co., Ltd.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A flood attack occurs when a device receives a large number of packets of the same type within a short period. As a result, the device is flooded by too many attack packets to process service packets from authorized wireless terminals.

After the flood attack detection function is enabled, a device counts the number of packets of the same type that it receives from a user at regular intervals. When the number exceeds a specified threshold, the device considers that the user launches a flood attack. If the dynamic blacklist function is enabled, the user will be added to a dynamic blacklist. If the threshold is set to a small value, the device may incorrectly add authorized users to the dynamic blacklist, causing the users unable to go online.

Follow-up Procedure

Run the **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Set the flood attack detection threshold to 350.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable flood
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] flood-detect threshold 350
```

Related Topics

14.4.55 wids attack detect enable

14.4.23 dynamic-blacklist enable

14.4.27 reset wlan ids attack-detected

Function

The **reset wlan ids attack-detected** command deletes information about the attacking devices detected.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset wlan ids attack-detected { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes information about all types of attacking devices.	-
flood	Deletes information about devices launching flood attacks.	-
spoof	Deletes information about devices launching spoofing attacks.	-
wapi-psk	Deletes information about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes information about devices launching weak IV attacks.	-
wep-share-key	Deletes information about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes information about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes information about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes information about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, information about attacking devices detected is recorded. When there is excessive information recorded or the recorded

information is useless, you can run the **reset wlan ids attack-detected** command to delete the information.

Example

Delete information about all the current attacking devices.

```
<Huawei> reset wlan ids attack-detected all
```

Related Topics

14.4.17 display wlan ids attack-detected

14.4.28 reset wlan ids attack-detected statistics

Function

The **reset wlan ids attack-detected statistics** command deletes the number of attacks detected.

Format

reset wlan ids attack-detected statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, the number of attacks detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-detected statistics** command to delete the information.

Example

Delete the number of attacks detected.

```
<Huawei> reset wlan ids attack-detected statistics
```

Related Topics

14.4.18 display wlan ids attack-detected statistics

14.4.29 reset wlan ids attack-history

Function

The **reset wlan ids attack-history** command deletes historical records about the attacking devices detected.

Format

reset wlan ids attack-history { **all** | **flood** | **spoof** | **wapi-psk** | **weak-iv** | **wep-share-key** | **wpa-psk** | **wpa2-psk** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Deletes historical records about all types of attacking devices.	-
flood	Deletes historical records about devices launching flood attacks.	-
spoof	Deletes historical records about devices launching spoofing attacks.	-
wapi-psk	Deletes historical records about devices that perform brute force cracking in WAPI-PSK authentication mode.	-
weak-iv	Deletes historical records about devices launching weak IV attacks.	-
wep-share-key	Deletes historical records about devices that perform brute force cracking in WEP-SK authentication mode.	-
wpa-psk	Deletes historical records about devices that perform brute force cracking in WPA-PSK authentication mode.	-
wpa2-psk	Deletes historical records about devices that perform brute force cracking in WPA2-PSK authentication mode.	-
mac-address *mac-address*	Deletes historical records about detected devices launching attacks with specified MAC addresses.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

After attack detection is enabled, historical records about attacking devices detected is recorded. When there is excessive information recorded or the recorded information is useless, you can run the **reset wlan ids attack-history** command to delete the information.

Example

Delete historical records about all the current attacking devices.

```
<Huawei> reset wlan ids attack-history all
```

Related Topics

14.4.19 display wlan ids attack-history

14.4.30 reset wlan ids dynamic-blacklist

Function

The **reset wlan ids dynamic-blacklist** command deletes information about devices in the dynamic blacklist.

Format

reset wlan ids dynamic-blacklist { **ap-id** *ap-id* | **ap-name** *ap-name* | **mac-address** *mac-address* | **all** }

Parameters

Parameter	Description	Value
ap-id *ap-id*	Deletes the dynamic blacklist information reported by the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Deletes the dynamic blacklist information reported by the AP with a specified name.	The AP name must exist.
mac-address *mac-address*	Deletes the device with a specified MAC address from the dynamic blacklist.	The MAC address must exist.
all	Deletes all information in the dynamic blacklist.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset wlan ids dynamic-blacklist** command is applicable to the following scenarios:

- To re-collect the dynamic blacklist information, run the **reset wlan ids dynamic-blacklist all** command to delete all information in the dynamic blacklist. After that, the AC re-collects the information.
- To remove an authorized device from the dynamic blacklist, run the **reset wlan ids dynamic-blacklist mac-address** command to remove the MAC address of the device from the dynamic blacklist. After that, information sent from the device is not rejected.

Precautions

Running the **reset wlan ids dynamic-blacklist** command affects packet receiving of APs. Exercise caution when running this command.

Example

Delete the device with MAC address **78AC-C0C1-C1FC** from the dynamic blacklist.

```
<Huawei> reset wlan ids dynamic-blacklist mac-address 78ac-c0c1-c1fc
```

14.4.31 security dot1x

Function

The **security dot1x** command configures pre-shared key authentication and encryption for WPA and WPA2.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

Format

security { **wpa** | **wpa2** | **wpa-wpa2** } **dot1x** { **aes** | **tkip** | **aes-tkip** }

undo security

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
wpa-wpa2	Configures WPA-WPA2 authentication. User terminals can be authenticated using WPA or WPA2.	-
aes	Configures AES encryption.	-
tkip	Configures TKIP encryption.	-
aes-tkip	Configures AES-TKIP encryption. After passing the authentication, user terminals can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WPA/WPA2 authentication includes WPA/WPA2 pre-shared key authentication and 802.1X authentication, which are also called WPA/WPA2 personal edition and WPA/WPA2 enterprise edition respectively. 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 802.1X authentication, run the **security dot1x** command. If multiple types of user terminals are available, you can configure the WPA-WPA2 and TKIP-CCMP security policy for authentication and data encryption.

NOTE

The following terminals do not support the WPA2 802.1X authentication and cannot access the AP. You must configure other security policies for the terminals.

- Nokia: N8
- HP: Pre 3

The authentication type in the security profile and authentication profile must both be set to 802.1X authentication. You can run the **display wlan config-errors** command to check whether error messages are generated for authentication type mismatch between the security profile and authentication profile.

The system displays the message only when the security profile has been bound to the other profiles.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure WPA authentication (802.1X and TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa dot1x tkip
```

Configure WPA2 authentication (802.1X and TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa2 dot1x tkip
```

Configure WPA-WPA2 authentication (802.1X authentication and AES-TKIP encryption).

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa-wpa2 dot1x aes-tkip
```

14.4.32 security psk

Function

The **security psk** command configures pre-shared key authentication and encryption for WPA and WPA2.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

Format

security { **wpa** | **wpa2** | **wpa-wpa2** } **psk** { **pass-phrase** | **hex** } *key-value* { **aes** | **tkip** | **aes-tkip** }

undo security

Parameters

Parameter	Description	Value
wpa	Configures WPA authentication.	-
wpa2	Configures WPA2 authentication.	-
wpa-wpa2	Configures WPA-WPA2 authentication. User terminals can be authenticated using WPA or WPA2.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-value	Specifies a password in cipher text.	The value is of 8 to 63 ASCII characters in plain text, 64 hexadecimal characters in plain text, or 48 or 68 or 88 or 108 characters in cipher text. The question mark (?) is supported, which you can enter by pressing **Ctrl+T**. In **pass-phrase** mode, the key must be a combination of at least two of the following: lowercase letters, uppercase letters, digits, and special characters.
aes	Configures AES encryption.	-
tkip	Configures TKIP encryption.	-
aes-tkip	Configures AES-TKIP encryption. After passing the authentication, user terminals can use the AES or TKIP algorithm for data encryption.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WPA/WPA2 authentication includes WPA/WPA2 pre-shared key authentication and 802.1X authentication, which are also called WPA/WPA2 personal edition and WPA/WPA2 enterprise edition respectively. 802.1X authentication is of high security and is applicable to enterprise networks.

To access a WLAN device using WPA or WPA2 pre-shared key authentication, run the **security psk** command. If multiple types of user terminals are available, you can configure the WPA-WPA2 and AES-TKIP security policy for authentication and data encryption.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If the key is in hexadecimal notation, you can enter hexadecimal characters without entering 0x.

If a security profile is bound to multiple VAP profiles, it will take a few minutes to configure WPA/WPA2 PSK authentication and encryption in the security profile.

The system displays the message only when the security profile has been bound to the other profiles.

Example

Configure WPA pre-shared key authentication and the authentication key.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa psk pass-phrase abcdfffffgF aes
```

Configure WPA2 pre-shared key authentication and the authentication key.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa2 psk pass-phrase abcdfffffgF aes
```

Configure WPA-WPA2 pre-shared key authentication and TKIP-CCMP encryption.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wpa-wpa2 psk pass-phrase abcdfffffgF aes-tkip
```

14.4.33 security wapi

Function

The **security wapi** command configures the WAPI authentication mode.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

Format

security wapi psk { **pass-phrase** | **hex** } *key-value*

security wapi certificate

undo security

Parameters

Parameter	Description	Value
certificate	Configures WAPI certificate authentication.	-

Parameter	Description	Value
psk	Configures WAPI pre-shared key authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number. The password of **hex** does not have enough complexity, so **pass-phrase** is recommend.	-
key-value	Specifies a password in cipher text.	In pass-phrase mode, the key is a string of 8 to 64 characters in plain text or 48 or 68 or 88 or 108 characters in cipher text. In hex mode, the key is a string of 8 to 32 hexadecimal numbers, in which case the length of the string must be an even, or a string of 48 or 68 or 88 or 108 characters in cipher text. The cipher-text characters must be a combination of at least two of the following: lowercase letters, uppercase letters, digits, and special characters.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI supports two authentication modes: certificate authentication and pre-shared key authentication. When pre-shared key authentication is used, a pre-shared key must be configured.

- If WAPI authentication is specified as a security policy in a security profile, you can run the **wapi authentication-method** command to configure the WAPI authentication mode.
- The **wapi authentication-method** command determines the WAPI authentication and key management mode. When certificate authentication and key management are configured, authentication involves identity authentication and key negotiation, and the authentication server and certificate need to be configured. When pre-shared key authentication is configured, a pre-shared key needs to be configured, and STAs also need to know the pre-shared key. In this situation, authentication just involves key negotiation.

The system displays the message only when the security profile has been bound to the other profiles.

Example

Set the WAPI authentication mode to pre-shared key authentication and specify the key.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wapi psk pass-phrase testpasswordF
```

14.4.34 security wep

Function

The **security wep** command configures the WEP authentication mode.

The **undo security** command restores the default security policy.

By default, the security policy is open system.

Format

security { **open** | **wep** [**share-key**] }

undo security

Parameters

Parameter	Description	Value
open	Sets the WEP authentication mode to open authentication.	-
share-key	Sets the WEP authentication mode to share-key authentication.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can select security policies on a WLAN based on the security level. WEP is a security policy used earlier and has security risks. It can be used in open scenarios that do not require high security. You can run this command to set the WEP authentication mode to open authentication or share-key authentication.

Table 14-127 Comparison between open system authentication and share-key authentication

Authentication Mode	Advantage	Disadvantage
open	Wireless devices can connect to a network without authentication.	STA identities are not checked, bringing security risks.
share-key	A share-key is used to enhance security.	• A long key string must be configured on each device and is difficult to expand. • A static key is used, which is easy to decipher.

Precautions

- If the authentication mode is set to **share-key**, run the **14.4.54 wep key** command to configure a share-key.
- If the authentication mode is set to **open**, the WEP share-key configured in the profile cannot take effect.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same. If a key index takes effect on a VAP, the key index cannot be applied to other VAPs.
- The system displays the message only when the security profile has been bound to the other profiles.

Example

Create security profile **p1** and set the authentication mode to **share-key**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] security wep share-key
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.54 wep key

14.4.35 security-profile

Function

The **security-profile** command creates a security profile or enters the security profile view.

The **undo security-profile** command deletes a security profile according to the ID or name.

By default, security profiles **default** and **default-wds** are available in the system.

Format

security-profile name *profile-name*

undo security-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a security profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all security profiles. **NOTE** Security profiles **default** and **default-wds** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run this command to configure access security. A security profile must be configured before you specify an authentication mode in the profile. To delete a security profile, run the **undo security-profile** command.

The system configures the new profile, the default value is no authentication and no encryption.

Example

Configure a security profile named **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1]
```

Related Topics

14.4.13 display security-profile

14.4.36 security-profile (VAP profile view)

Function

The **security-profile** command binds a security profile to a VAP profile.

The **undo security-profile** command unbinds a security profile from a VAP profile.

By default, the security profile **default** is bound to a VAP profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a security profile.	The security profile must exist.

Views

VAP profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can use this command to bind a security profile to a VAP profile. The security profile then applies to all users using this VAP profile.

Example

Create VAP profile **ChinaNet** and bind security profile **security-profile1** to the VAP profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] vap-profile name ChinaNet
[Huawei-wlan-vap-prof-ChinaNet] security-profile security-profile1
```

Related Topics

14.4.35 security-profile

14.1.127 display vap-profile

14.4.37 spoof-detect quiet-time

Function

The **spoof-detect quiet-time** command sets the quiet time for an AP to report the detected spoofing attacks to the AC.

The **undo spoof-detect quiet-time** command restores the default quiet time for an AP to report the detected spoofing attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected spoofing attacks to the AC.

Format

spoof-detect quiet-time *quiet-time-value*

undo spoof-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected spoofing attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repetitive alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Example

Set the quiet time to 300 seconds for an AP to report the detected spoofing attacks to the AC.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable spoof
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] spoof-detect quiet-time 300
```

Related Topics

14.4.55 wids attack detect enable

14.4.38 sta-access-mode

Function

The **sta-access-mode** command binds STA blacklist and STA whitelist profiles to AP system profiles.

The **undo sta-access-mode** command unbinds STA blacklist and STA whitelist profiles from AP system profiles.

By default, no STA blacklist and STA whitelist profiles are bound to an AP system profile.

Format

sta-access-mode { **blacklist** | **whitelist** } *profile-name*

undo sta-access-mode

Parameters

Parameter	Description	Value
blacklist	Specifies a STA blacklist profile.	-
whitelist	Specifies a STA whitelist profile.	-
profile-name	Specifies the names of STA blacklist and whitelist profiles.	The STA blacklist and whitelist profiles must exist.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

STA blacklists and whitelists configured by using the **14.4.40 sta-mac** command take effect only after the STA blacklist and whitelist profiles are bound to AP system profiles using the **sta-access-mode** command.

When STA blacklist and whitelist profiles are bound to different profiles, the effective scope of the STA blacklists and whitelists differs.

- AP system profile: The STA blacklist and whitelist take effect on the corresponding AP.

Example

Bind the STA blacklist profile **sta-blacklist-profile1** to the AP system profile **ap-system-profile1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system-profile1
[Huawei-wlan-ap-system-prof-ap-system-profile1] sta-access-mode blacklist sta-blacklist-profile1
```

Related Topics

14.4.40 sta-mac

14.4.39 sta-blacklist-profile

Function

The **sta-blacklist-profile** command creates a STA blacklist profile or displays the STA blacklist profile view.

The **undo sta-blacklist-profile** command deletes one or multiple STA blacklist profiles.

By default, no STA blacklist profile is created.

Format

sta-blacklist-profile name *profile-name*

undo sta-blacklist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a STA blacklist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all STA blacklist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the MAC address of a STA is in the blacklist, the STA cannot go online. If the STA blacklist profile is not referenced or the MAC address of a STA is not in the blacklist, the STA is allowed to go online.

The configured blacklist takes effect only after the STA blacklist profile is bound to an AP system profile using the **14.4.38 sta-access-mode** command.

If a STA is added to the blacklist, the system automatically disconnects the STA.

Example

Create the STA blacklist profile **sta-blacklist-profile1**.

```
<Huawei> system-view
[Huawei] wlan ac
```

```
[Huawei-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[Huawei-wlan-blacklist-prof-sta-blacklist-profile1]
```

Related Topics

14.4.38 sta-access-mode

14.4.14 display sta-blacklist-profile

14.4.40 sta-mac

Function

The **sta-mac** command adds the MAC addresses of a STA to the blacklist or whitelist.

The **undo sta-mac** command deletes a specified MAC address or all MAC addresses from the blacklist or whitelist.

By default, the MAC address of a STA is not added to the blacklist or whitelist.

Format

sta-mac *mac-address*

undo sta-mac { *mac-address* | **all** }

Parameters

Parameter	Description	Value
mac-address	Adds a MAC address to the blacklist or whitelist.	The value is in H-H-H format. An H is a hexadecimal number of four digits.
all	Deletes all MAC addresses from the blacklist or whitelist.	-

Views

Blacklist profile view, whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

If the blacklist function is enabled, all STAs in the blacklist cannot connect to the WLAN.

If the whitelist function is enabled, only STAs in the whitelist can connect to the WLAN.

 Copyright © Huawei Technologies Co., Ltd.

If a STA is added to the blacklist, the system automatically disconnects the STA.

Example

Add MAC address 2C27-D720-746B of a STA to blacklist **huawei**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-blacklist-profile name sta-blacklist-profile1
[Huawei-wlan-blacklist-prof-sta-blacklist-profile1] sta-mac 2C27-D720-746B
```

Related Topics

14.4.14 display sta-blacklist-profile
14.4.16 display sta-whitelist-profile

14.4.41 sta-whitelist-profile

Function

The **sta-whitelist-profile** command creates a STA whitelist profile for VAPs or displays the STA whitelist profile view.

The **undo sta-whitelist-profile** command deletes a specified STA whitelist profile or all STA whitelist profiles for VAPs.

By default, no STA whitelist profile is created.

Format

sta-whitelist-profile name *profile-name*

undo sta-whitelist-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a STA whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all STA whitelist profiles.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

The configured whitelist takes effect only after the STA whitelist profile is bound to an AP system profile using the **14.4.38 sta-access-mode** command.

If the configured whitelist takes effect, only STAs in the whitelist can access the WLAN.

Example

Create the STA whitelist profile **sta-whitelist-profile1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] sta-whitelist-profile name sta-whitelist-profile1
[Huawei-wlan-whitelist-prof-sta-whitelist-profile1]
```

Related Topics

14.4.38 sta-access-mode

14.4.16 display sta-whitelist-profile

14.4.42 wapi asu

Function

The **wapi asu** command specifies an IP address for an authentication server unit (ASU) server.

The **undo wapi asu** command deletes the IP address of the ASU server.

By default, no IP address is specified for the ASU server.

Format

wapi asu ip *ip-address*

undo wapi asu ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the ASU server.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If WAPI certificate authentication is configured, an AC sends WAPI authentication packets to the ASU server at the specified IP address.

Prerequisites

If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi asu** command to specify an IP address for the ASU server.

Precautions

The **wapi asu** command helps to determine to which ASU server WAPI packets are sent. Users must ensure the correctness of both ASU certificates and ASU servers; otherwise, they may fail in user authentication.

The system displays the message only when the security profile has been bound to the other profiles.

Example

Specify IP address 10.164.10.10 for the ASU server.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi asu ip 10.164.10.10
```

14.4.43 wapi bk

Function

The **wapi bk** command sets the interval for updating a BK and the BK lifetime percentage.

The **undo wapi bk** command restores the default interval for updating a BK and the BK lifetime percentage.

By default, the interval for updating a BK is 43200s, and the BK lifetime percentage is 70%.

Format

wapi { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-update-interval* }

undo wapi { **bk-threshold** | **bk-update-interval** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bk-threshold *bk-threshold*	Specifies the BK lifetime percentage.	The value is an integer that ranges from 1 to 100.
bk-update-interval *bk-update-interval*	Specifies the interval for updating a BK.	The value is an integer that ranges from 600 to 604800, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can set the intervals for updating a BK to ensure security.

The value obtained by multiplying the interval for updating a BK by the BK lifetime percentage should be greater than or equal to 300 seconds.

Example

Set the interval for updating a BK to 10000s and the BK lifetime percentage to 80%.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi bk-update-interval 10000
[Huawei-wlan-sec-prof-p1] wapi bk-threshold 80
```

14.4.44 wapi cert-retrans-count

Function

The **wapi cert-retrans-count** command sets the number of retransmissions of certificate authentication packets.

The **undo wapi cert-retrans-count** command restores the default number of retransmissions of certificate authentication packets.

By default, the number of retransmissions is 3.

Format

wapi cert-retrans-count *cert-count*

undo wapi cert-retrans-count

Parameters

Parameter	Description	Value
cert-count	Specifies the number of retransmissions of certificate authentication packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

If WAPI authentication is specified as a security policy, run the **wapi cert-retrans-count** command to set the number of retransmissions of certificate authentication packets.

Example

Set the number of retransmissions of certificate authentication packets to 5.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi cert-retrans-count 5
```

14.4.45 wapi import certificate

Function

The **wapi import certificate** command imports the AC certificate file, certificate of the AC certificate issuer, and ASU certificate file.

The **undo wapi certificate** command deletes the imported AC certificate file, certificate of the AC certificate issuer, or ASU certificate file.

By default, the AC certificate file, certificate of the AC certificate issuer, and ASU certificate file are not imported.

Format

wapi import certificate { **ac** | **asu** | **issuer** } **format pkcs12 file-name** *file-name* **password** *password*

wapi import certificate { **ac** | **asu** | **issuer** } **format pem file-name** *file-name*

undo wapi certificate { **ac** | **asu** | **issuer** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ac	Specifies the AC certificate.	-
asu	Specifies the ASU certificate.	-
issuer	Specifies the certificate of the AC certificate issuer.	-
format pkcs12	Imports a certificate in P12 format.	-
format pem	Imports a certificate in PEM format.	-
file-name *file-name*	Specifies a certificate file name, which the complete path of a certificate file must be specified.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ") or spaces.
password *password*	Specifies the key of the P12 certificate.	The password can be in plain text or cipher text. ● A plain text password is a string of 1 to 32 characters. ● A cipher text password is a string of 48 or 68 characters.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi import certificate** command to specify the AC certificate, certificate of the AC certificate issuer, and ASU certificate. STAs will fail to be authenticated if you do not run this command. The issuer certificate helps to check whether the AC certificate is modified.

 Copyright © Huawei Technologies Co., Ltd.

- Before using this command, store the AC certificate and ASU certificate to the storage of the device, and import the certificates and private key using TFTP. Certificates must be X509 V3 certificates and comply with the WAPI standard. Otherwise, certificates cannot be imported.
- After this command is run:
  - When an issuer certificate is configured, the system checks correctness of the AC certificate.
  - If the authentication system uses only two certificates, the issuer certificate and ASU certificate have the same certificate file name and are the same certificate. If the authentication system uses three certificates, the issuer certificate and ASU certificate are different from each other and both must be imported.

NOTE

- The ASU certificate and issuer certificate must be imported.
- Certificates to be imported must be valid and correct.
- If the certificate with the same name but different contents has been imported by other security profiles, delete the earlier certificate first.

Example

Import the AC certificate.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi import certificate ac format pem file-name flash:/local_ac.cer
Warning: This action may cause service interruption. Continue?[Y/N]y
```

14.4.46 wapi import private-key

Function

The **wapi import private-key** command imports the AC private key file.

The **undo wapi private-key** command deletes the imported AC private key file.

By default, no AC private key file is imported.

Format

wapi import private-key format pkcs12 file-name *file-name* **password** *password*

wapi import private-key format pem file-name *file-name*

undo wapi private-key

Parameters

Parameter	Description	Value
format pkcs12	Imports a private key file in P12 format.	-

Parameter	Description	Value
format pem	Imports a private key file in PEM format.	-
file-name *file-name*	Specifies the name of a private key file.	The value is a string of 1 to 255 characters. It cannot contain question marks (?) or spaces, and cannot start or end with double quotation marks (" ") or spaces.
password *password*	Specifies the password in the private key file of the P12 format.	The password can be in plain text or cipher text. ● A plain text password is a string of 1 to 32 characters. ● A cipher text password is a string of 48 or 68 characters.

Views

Security profile view

Default Level

3: Management level

Usage Guidelines

- If WAPI certificate authentication is specified as a security policy in a security profile, run the **wapi import private-key** command to specify the private key file for the AC certificate.
- Before using this command, store the AC private key file to the storage of the device, and import the private key file using TFTP.
- After this command is used, the system obtains the private key file and establishes the mapping between the certificate and private key.

NOTE

The certificate and private key to be imported must be valid and correct.

Example

Import the AC private key file **ac_key.key**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi import private-key format pem file-name flash:/ac_key.key
Warning: This action may cause service interruption. Continue?[Y/N]y
```

Related Topics

14.4.13 display security-profile

14.4.47 wapi key-update

Function

The **wapi key-update** command sets the USK and MSK update mode.

The **undo wapi key-update** command restores the default USK and MSK update mode.

By default, USKs and MSKs are updated based on time.

Format

wapi { **usk** | **msk** } **key-update** { **disable** | **time-based** }

undo wapi { **usk** | **msk** } **key-update**

Parameters

Parameter	Description	Value
usk	Indicates USK update.	-
msk	Indicates MSK update.	-
disable	Disables key update.	-
time-based	Indicates time-based update. You can run the **14.4.48 wapi msk** and **14.4.51 wapi usk** commands to respectively set the intervals for updating an MSK and a USK.	-

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- To ensure network security, update keys in a timely manner. There are several key update modes.

- The **wapi key-update** command sets the USK and MSK update mode. If the interval for updating an MSK or a USK is too long, key security cannot be ensured.
- If **disable** is specified, keys will not be updated.

Example

Set the USK update mode to time-based update.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi usk key-update time-based
```

Related Topics

14.4.48 wapi msk

14.4.51 wapi usk

14.4.48 wapi msk

Function

The **wapi msk** command sets the interval for updating an MSK, and number of retransmissions of MSK negotiation packets.

The **undo wapi msk** command restores the default interval for updating an MCK, and number of retransmissions of MSK negotiation packets.

By default, the interval for updating an MSK is 86400s; the number of retransmissions of MSK negotiation packets is 3.

Format

wapi { **msk-update-interval** *msk-interval* | **msk-retrans-count** *msk-count* }

undo wapi { **msk-update-interval** | **msk-retrans-count** }

Parameters

Parameter	Description	Value
msk-update-interval *msk-interval*	Specifies the interval for updating an MSK. When the MSK update mode is set to time-based update using the **14.4.47 wapi key-update** command, the interval for updating an MSK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.
msk-retrans-count *msk-count*	Specifies the number of retransmissions of MSK negotiation packets.	The value is an integer that ranges from 1 to 10.

 Copyright © Huawei Technologies Co., Ltd.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends.

Example

Set the interval for updating an MSK to 10000s, and number of retransmissions of MSK negotiation packets to 5.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi msk key-update time-based
[Huawei-wlan-sec-prof-p1] wapi msk-update-interval 10000
[Huawei-wlan-sec-prof-p1] wapi msk-retrans-count 5
```

Related Topics

14.4.47 wapi key-update

14.4.49 wapi sa-timeout

Function

The **wapi sa-timeout** command sets the timeout period of a security association (SA) of key encryption.

The **undo wapi sa-timeout** command restores the default timeout period of a SA for key encryption.

By default, the timeout period for a SA is 60s.

Format

wapi sa-timeout *sa-time*

undo wapi sa-timeout

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
sa-time	Specifies the timeout period of an SA.	The value is an integer that ranges from 1 to 255, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

You can prolong the WAPI timeout period to increase the authentication success ratio.

Example

Set the timeout period of an SA to 100s.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi sa-timeout 100
```

14.4.50 wapi source interface

Function

The **wapi source interface** command configures a source interface for an AC to communicate with an ASU server.

The **undo wapi source interface** command cancels the source interface for an AC to communicate with an ASU server.

By default, no source interface is configured for an AC to communicate with an ASU server.

Format

wapi source interface { **vlanif** *vlan-id* | **loopback** *loopback-number* }

undo wapi source interface

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlanif *vlan-id*	Configures a VLANIF interface as the source interface.	The value is an integer that ranges from 1 to 4094.
loopback *loopback-number*	Configures a loopback interface as the source interface.	The value is an integer that ranges from 0 to 1023.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In WLAN applications, to use WAPI authentication and enable socket communication between an AC and an ASU server, the AC needs a WAPI source IP address using which all packets are sent to the ASU server.

Prerequisites

An IP address has been assigned to the specified loopback or VLANIF interface.

Precautions

The IP address of the WAPI source interface on the AC must be on the same network segment as the IP address of the ASU server. If no WAPI source interface is configured, the IP address of the AC source interface is used as the source IP address for sending WAPI packets to the WAPI server by default.

Example

Configure a VLANIF interface as the source interface for the AC to communicate with the ASU server.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] ip address 192.168.10.1 24
[Huawei-Vlanif100] quit
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi source interface Vlanif 100
```

 Copyright © Huawei Technologies Co., Ltd.

14.4.51 wapi usk

Function

The **wapi usk** command sets the interval for updating a USK, and number of retransmissions of USK negotiation packets.

The **undo wapi usk** command restores the default interval for updating a USK, and number of retransmissions of USK negotiation packets.

By default, the interval for updating a USK is 86400s; the number of retransmissions of USK negotiation packets is 3.

Format

wapi { **usk-update-interval** *usk-interval* | **usk-retrans-count** *usk-count* }

undo wapi { **usk-update-interval** | **usk-retrans-count** }

Parameters

Parameter	Description	Value
usk-update-interval *usk-interval*	Specifies the interval for updating a USK. When the USK update mode is set to time-based update using the **14.4.47 wapi key-update** command, the interval for updating a USK needs to be set.	The value is an integer that ranges from 600 to 604800, in seconds.
usk-retrans-count *usk-count*	Specifies the number of retransmissions of USK negotiation packets.	The value is an integer that ranges from 1 to 10.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

WAPI defines a dynamic key negotiation mechanism, but there are still security risks if a STA uses the same encryption key for a long time. Both the USK and MSK have a lifetime. The USK or MSK needs to be updated when its lifetime ends.

Example

Set the interval for updating a USK to 10000s, and number of retransmissions of USK negotiation packets to 5.

```
<Huawei> system-view
[Huawei] wlan ac
```

```
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wapi usk key-update time-based
[Huawei-wlan-sec-prof-p1] wapi usk-update-interval 10000
[Huawei-wlan-sec-prof-p1] wapi usk-retrans-count 5
```

Related Topics

14.4.47 wapi key-update

14.4.52 weak-iv-detect quiet-time

Function

The **weak-iv-detect quiet-time** command sets the quiet time for an AP to report the detected weak IV attacks to the AC.

The **undo weak-iv-detect quiet-time** command restores the default quiet time for an AP to report the detected weak IV attacks to the AC.

By default, the quiet time is 600 seconds for an AP to report the detected weak IV attacks to the AC.

Format

weak-iv-detect quiet-time *quiet-time-value*

undo weak-iv-detect quiet-time

Parameters

Parameter	Description	Value
quiet-time-value	Specifies the quiet time for an AP to report the detected weak IV attacks to the AC.	The value is an integer that ranges from 60 to 36000, in seconds.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After attack detection is enabled on an AP, the AP reports alarms upon attack detection. If an attack source launches attacks repeatedly, a large number of repetitive alarms are generated. To prevent this situation, configure the quiet time for an AP to report alarms. When detecting attack sources of the same MAC address, the AP does not report alarms in the quiet time. However, if the AP still detects attacks from the attack source after the quiet time expires, the AP reports alarms. You can set the quiet time based on attack types.

 Copyright © Huawei Technologies Co., Ltd.

To obtain attack information in a timely manner, set the quiet time to a small value. If attack detection is enabled on many APs, and attacks are frequently detected, set the quiet time to a large value to prevent frequent alarm reports.

Example

Set the quiet time to 300 seconds for an AP to report the detected weak IV attacks to the AC.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable weak-iv
[Huawei-wlan-group-radio-office/0] quit
[Huawei-wlan-ap-group-office] quit
[Huawei-wlan-view] wids-profile name huawei
[Huawei-wlan-wids-prof-huawei] weak-iv-detect quiet-time 300
```

Related Topics

14.4.55 wids attack detect enable

14.4.53 wep default-key

Function

The **wep default-key** command sets the default key ID for WEP authentication or encryption.

The **undo wep default-key** command restores the default key ID for WEP authentication or encryption.

By default, key 0 is used for WEP authentication or encryption.

Format

wep default-key *key-id*

undo wep default-key

Parameters

Parameter	Description	Value
key-id	Specifies the default key ID.	The key ID must exist.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

- A maximum of four WEP keys can be configured, and only one WEP key is used for authentication and encryption. This command specifies which key to use.
- After a key ID is specified, the specified key is used for authentication or encryption.
- Each AP can have at most four key indexes configured. The key indexes used by different VAPs cannot be the same. If a key index takes effect on a VAP, the key index cannot be applied to other VAPs.
- The system displays the message only when the security profile has been bound to the other profiles.

Example

Set the default key ID to 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wep default-key 1
```

Related Topics

14.4.54 wep key

14.4.54 wep key

Function

The **wep key** command sets a WEP key.

The **undo wep key** command deletes the specified key.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

wep key *key-id* { **wep-40** | **wep-104** | **wep-128** } { **pass-phrase** | **hex** } *key-value*

undo wep key *key-id*

Parameters

Parameter	Description	Value
key-id	Specifies the key ID.	The value is an integer that ranges from 0 to 3.
wep-40	Configures WEP-40 authentication.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wep-104	Configures WEP-104 authentication.	-
wep-128	Configures WEP-128 authentication.	-
pass-phrase	Specifies the key phrase.	-
hex	Specifies a hexadecimal number.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-value	Specifies a password in cipher text.	The password can be in plain text or cipher text. ● A plain text password is a string of case-sensitive characters. – If WEP-40 is used, the WEP key is 10 hexadecimal characters or 5 ASCII characters. – If WEP-104 is used, the WEP key is 26 hexadecimal characters or 13 ASCII characters. – If WEP-128 is used, the WEP key is 32 hexadecimal characters or 16 ASCII characters. ● A cipher text password is a string of 48 or 68 characters. Here, ASCII characters contain only digits or letters. In **pass-phrase** mode, the key must be a combination of at least two of the following: lowercase letters, uppercase letters, and digits.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

To connect to a WLAN device in WEP shared-key authentication mode, run the **wep key** command to set a WEP key.

NOTE

If the key is in hexadecimal notation, you can enter hexadecimal characters without entering 0x.

The system displays the message only when the security profile has been bound to the other profiles.

Example

Configure a WEP key and its ID.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name p1
[Huawei-wlan-sec-prof-p1] wep key 1 wep-128 hex
12345678123456781234567812345 67a
Warning: This action may cause service interruption. Continue?
[Y/N]y
Info: This operation may take a few seconds, please wait.done.
```

Related Topics

14.4.53 wep default-key

14.4.55 wids attack detect enable

Function

(AP group radio view) The **wids attack detect enable** command enables attack detection on all specified radios in an AP group.

(AP group radio view) The **undo wids attack detect enable** command disables attack detection on all l specified radios in an AP group.

(AP radio view) The **wids attack detect enable** command enables attack detection on an AP radio.

(AP radio view) The **undo wids attack detect enable** command cancels the configuration of the attack detection function on an AP radio. The status of this function on the AP radio is then determined by the status of this function in the AP group radio view.

By default, attack detection is disabled on AP radios.

Format

wids attack detect enable { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

undo wids attack detect enable { **all** | **flood** | **weak-iv** | **spoof** | **wpa-psk** | **wpa2-psk** | **wapi-psk** | **wep-share-key** }

Parameters

Parameter	Description	Value
all	Enables all attack detection functions.	-
flood	Enables flood attack detection.	-
weak-iv	Enables weak IV attack detection.	-
spoof	Enables spoofing attack detection.	-
wpa-psk	Enables brute force attack detection for WPA-PSK authentication.	-
wpa2-psk	Enables brute force attack detection for WPA2-PSK authentication.	-
wapi-psk	Enables brute force attack detection for WAPI-PSK authentication.	-
wep-share-key	Enables brute force attack detection for shared key authentication.	-

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor and prevent malicious or unintentional attacks on WLANs in real time, network administrators can enable the following attack detection functions based on actual requirements:

- **flood**: indicates flood attack detection used to detect whether an AP receives a large number of packets of the same type in a short period.
- **weak-iv**: indicates weak IV attack detection used to detect whether weak IV is used for WEP encryption on a WLAN.
- **spoof**: indicates spoofing attack detection used to detect whether a potential attacker pretends to be an AP to broadcast Deauthentication and Disassociation packets.
- **wpa-psk**, **wpa2-psk**, **wapi-psk**, **wep-share-key**: indicates brute force attack detection. If the WPA-PSK, WPA2-PSK, WAPI-PSK, or WEP-SK security policy is configured on a WLAN, brute force attack detection can be enabled to

 Copyright © Huawei Technologies Co., Ltd.

increase the time required for password cracking and improve password security.

Precautions

The configuration in the AP radio view has a higher priority than that in the AP group radio view.

Follow-up Procedure

Run the **14.4.23 dynamic-blacklist enable** command to enable the dynamic blacklist function.

Example

Enable brute force attack detection for WPA-PSK authentication on radio 0 in AP group **office**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name office
[Huawei-wlan-ap-group-office] radio 0
[Huawei-wlan-group-radio-office/0] wids attack detect enable wpa-psk
```

Related Topics

14.4.23 dynamic-blacklist enable

14.4.56 wids-profile (WLAN view)

Function

The **wids-profile** command creates a WIDS profile and displays the WIDS profile view.

The **undo wids-profile** command deletes a WIDS profile.

By default, the system provides the WIDS profile **default**.

You can run the **14.4.8 display wids-profile** command to view configuration of the WIDS profile **default**.

Format

wids-profile name *profile-name*

undo wids-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all WIDS profiles.	The default WIDS profile **default** can be modified but cannot be deleted.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure the WIDS function on a device to detect attacks and add devices launching the attacks to a dynamic blacklist. Packets sent from the blacklisted devices will be rejected to protect authorized users.

After you create a WIDS profile using the **wids-profile** command, you can configure APs to detect attacks in the profile.

Follow-up Procedure

Run the **14.4.57 wids-profile (AP group view and AP view)** command to bind the WIDS profile to an AP group or AP so that the WIDS profile can take effect.

Example

Create the WIDS profile **office**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-profile name office
[Huawei-wlan-wids-prof-office]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

14.4.57 wids-profile (AP group view and AP view)

14.4.57 wids-profile (AP group view and AP view)

Function

The **wids-profile** command binds a WIDS profile to an AP group or AP.

The **undo wids-profile** command unbinds a WIDS profile from an AP group or AP.

By default, no WIDS profile is bound to an AP, but the WIDS profile **default** is bound to the AP group.

Format

wids-profile *profile-name*

undo wids-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a WIDS profile.	The WIDS profile must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

After you create a WIDS profile using the **14.4.56 wids-profile (WLAN view)** command, bind it to an AP group or AP to make the profile take effect.

Example

Bind the WIDS profile **office01** to AP group **AP-office01**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-profile name office01
[Huawei-wlan-wids-prof-office01] quit
[Huawei-wlan-view] ap-group name AP-office01
[Huawei-wlan-ap-group-AP-office01] wids-profile office01
```

Bind the WIDS profile **office01** to the AP with ID **1**.

```
<Huawei> system-view
[Huawei] wlan ac
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-wlan-view] wids-profile name office01
[Huawei-wlan-wids-prof-office01] quit
[Huawei-wlan-view] ap-id 1
[Huawei-wlan-ap-1] wids-profile office01
```

Related Topics

14.4.56 wids-profile (WLAN view)

14.4.58 wids-spoof-profile (WLAN view)

Function

The **wids-spoof-profile** command creates a WIDS spoof SSID profile and displays the WIDS spoof SSID profile view.

The **undo wids-spoof-profile** command deletes a WIDS spoof SSID profile.

By default, no WIDS spoof SSID profile exists in the system.

Format

wids-spoof-profile name *profile-name*

undo wids-spoof-profile { **name** *profile-name* | **all** }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WIDS spoof SSID profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all WIDS spoof SSID profiles.	-

Views

WLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Follow-up Procedure

Run the **14.4.59 wids-spoof-profile (WIDS profile view)** command to bind the WIDS spoof SSID profile to a WIDS profile to make the WIDS spoof SSID profile take effect.

Example

Create the WIDS spoof SSID profile **office**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-spoof-profile name office
[Huawei-wlan-wids-spoof-office]
```

Related Topics

14.4.59 wids-spoof-profile (WIDS profile view)

14.4.59 wids-spoof-profile (WIDS profile view)

Function

The **wids-spoof-profile** command binds a WIDS spoof SSID profile to a WIDS profile.

The **undo wids-spoof-profile** command unbinds a WIDS spoof SSID profile from a WIDS profile.

By default, no WIDS spoof SSID profile is bound to a WIDS profile.

Format

wids-spoof-profile *profile-name*

undo wids-spoof-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a WIDS spoof SSID profile.	The WIDS spoof SSID profile must already exist.

Views

WIDS profile view

Default Level

2: Configuration level

Usage Guidelines

After you create a WIDS spoof SSID profile using the **14.4.58 wids-spoof-profile (WLAN view)** command, bind it to a WIDS profile so that the WIDS spoof SSID profile can take effect.

Example

Bind the WIDS spoof SSID profile **office01** to the WIDS profile **office01**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wids-spoof-profile name office01
[Huawei-wlan-wids-spoof-office01] quit
[Huawei-wlan-view] wids-profile name office01
[Huawei-wlan-wids-prof-office01] wids-spoof-profile office01
```

Related Topics

14.4.58 wids-spoof-profile (WLAN view)

14.4.56 wids-profile (WLAN view)

14.4.60 wpa ptk-update enable

Function

The **wpa ptk-update enable** command enables periodic PTK update in WPA or WPA2 authentication and encryption.

The **undo wpa ptk-update enable** command disables periodic PTK update.

By default, periodic PTK update is disabled.

Format

wpa ptk-update enable

undo wpa ptk-update enable

Parameters

None

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In WPA or WPA2 authentication and encryption, a Pairwise Transient Key (PTK) is generated at the key negotiation stage to encrypt unicast radio packets. To ensure

 Copyright © Huawei Technologies Co., Ltd.

secure encryption, enable periodic PTK update so that the AP and STA use a new PTK to encrypt radio packets after a regular interval.

Precautions

When periodic PTK update is implemented, some terminals may go offline due to individual problems.

Follow-up Procedure

Run the **14.4.61 wpa ptk-update ptk-update-interval** command to configure the periodic PTK update interval.

Example

Enable the periodic PTK update function.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name huawei
[Huawei-wlan-sec-prof-huawei] wpa ptk-update enable
```

Related Topics

14.4.61 wpa ptk-update ptk-update-interval

14.4.61 wpa ptk-update ptk-update-interval

Function

The **wpa ptk-update ptk-update-interval** command configures an interval for updating PTKs in WPA or WPA2 authentication and encryption.

The **undo wpa ptk-update ptk-update-interval** command restores the default PTK update interval.

By default, the interval for updating PTKs is 43200 seconds.

Format

wpa ptk-update ptk-update-interval *ptk-rekey-interval*

undo wpa ptk-update ptk-update-interval

Parameters

Parameter	Description	Value
ptk-rekey-interval	Specifies the PTK update interval.	The value is an integer ranging from 30 to 86400, in seconds.

Views

Security profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure secure encryption during WPA or WPA2 authentication, enable periodic PTK update. You can run this command to configure the PTK update interval. A smaller interval indicates faster PTK update and more secure data encryption. However, if the PTK update interval is set too small, the STA and AP implement more negotiations, affecting the throughput.

Precautions

The configured periodic PTK update interval takes effect only after you enable the periodic PTK update function using the **14.4.60 wpa ptk-update enable** command.

Example

Set the periodic PTK update interval to 50,000 seconds.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name huawei
[Huawei-wlan-sec-prof-huawei] wpa ptk-update ptk-update-interval 50000
```

Related Topics

14.4.60 wpa ptk-update enable

14.5 WLAN WDS Configuration Commands

14.5.1 dhcp trust port (WDS profile view)

Function

The **dhcp trust port** command enables a DHCP trusted port in a WDS profile.

The **undo dhcp trust port** command disables a DHCP trusted port in a WDS profile.

By default, a DHCP trusted port is enabled in a WDS profile.

Format

dhcp trust port

undo dhcp trust port

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

After a DHCP trusted port is enabled in a WDS profile and the WDS profile is applied to an AP, the AP receives the DHCP OFFER, ACK, and NAK packets sent by authorized DHCP servers and forwards the packets to STAs so that the STAs can obtain valid IP addresses and go online.

Example

Enable a DHCP trusted port in the WDS profile **test**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] dhcp trust port
```

Related Topics

14.5.20 wds-profile

14.5.2 display references wds-profile

Function

The **display references wds-profile** command displays reference information about a WDS profile.

Format

display references wds-profile name *profile-name*

Parameters

Parameter	Description	Value
name *profile-name*	Displays reference information about a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display references wds-profile** command to check reference information about a WDS profile.

Example

Display reference information about the WDS profile **test**.

```
<Huawei> display references wds-profile name test
--------------------------------------------------------------------------------
Reference type     Reference name                    Reference radio  WLAN ID
--------------------------------------------------------------------------------
AP group           group-1                           Radio-0          13
AP group           group-1                           Radio-0          14
--------------------------------------------------------------------------------
Total: 2
```

Table 14-128 Description of the **display references wds-profile name** command output

Parameter	Description
Reference type	Type of the profile to which the WDS profile is bound.
Reference name	Name of the profile to which the WDS profile is bound. • Run the **14.5.21 wds-profile radio** command in the AP group view or view of the AP with a specified ID to apply a WDS profile. • Run the **14.5.22 wds-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view to apply a WDS profile.
Reference radio	AP radio to which the WDS profile is applied.
WLAN ID	WLAN ID to which the WDS profile is bound.

Related Topics

14.5.4 display wds-profile

14.5.21 wds-profile radio

14.5.22 wds-profile (AP group radio view or AP radio view)

 Copyright © Huawei Technologies Co., Ltd.

14.5.3 display references wds-whitelist-profile

Function

The **display references wds-whitelist-profile** command displays reference information about a WDS whitelist profile.

Format

display references wds-whitelist-profile name *whitelist-name*

Parameters

Parameter	Description	Value
name *whitelist-name*	Displays reference information about a specified WDS whitelist profile.	The WDS whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display references wds-whitelist-profile** command to check reference information about a specified WDS whitelist profile.

Example

Display reference information about the WDS whitelist profile **test**.

```
<Huawei> display references wds-whitelist-profile name test
-------------------------------------------------------------------------------
Reference type                Reference name
-------------------------------------------------------------------------------
AP group                      profile-1
AP group                      profile-2
-------------------------------------------------------------------------------
Total: 2
```

Table 14-129 Description of the **display references wds-whitelist-profile** command output

Parameter	Description
Reference type	Type of the profile to which the WDS whitelist profile is bound.

Parameter	Description
Reference name	Name of the profile to which the WDS whitelist profile is bound. Run the **14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)** command in the AP group radio view or AP radio view to apply a WDS whitelist profile.

Related Topics

14.5.5 display wds-whitelist-profile
14.5.23 wds-whitelist-profile
14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)

14.5.4 display wds-profile

Function

The **display wds-profile** command displays reference or configuration information about a WDS profile.

Format

display wds-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all WDS profiles.	-
name *profile-name*	Displays information about a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds-profile** command to view the number of times a WDS profile is referenced or configuration information of a specified WDS profile.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display reference information about all WDS profiles.

```
<Huawei> display wds-profile all
--------------------------------------------------------------------------------
Profile name                    Reference
--------------------------------------------------------------------------------
default                          0
test                            2
--------------------------------------------------------------------------------
Total: 2
```

Table 14-130 Description of the **display wds-profile all** command output

Item	Description
Profile name	WDS profile name. To create a WDS profile, run the **14.5.20 wds-profile** command.
Reference	Number of times a WDS profile is referenced.

Display information about the WDS profile **test**.

```
<Huawei> display wds-profile name test
--------------------------------------------------------------------------------
WDS name                  : HUAWEI-WLAN-WDS
WDS work mode               : root
Security profile          : test
DHCP trust port             : enable
Tagged vlan               : -
Priority map trust          : DSCP
Priority map mode           : DSCP map 802.11e
                          0-7 map 0
                          8-15 map 1
                          16-23 map 2
                          24-31 map 3
                          32-39 map 4
                          40-47 map 5
                          48-55 map 6
                          56-63 map 7
--------------------------------------------------------------------------------
```

Table 14-131 Description of the **display wds-profile name** command output

Item	Description
WDS name	WDS name. To set a WDS name, run the **14.5.19 wds-name** command.
WDS work mode	WDS working mode. To set the WDS working mode, run the **14.5.18 wds-mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Security profile	Security profile bound to a WDS profile. To bind a security profile to a WDS profile, run the **14.5.12 security-profile (WDS profile view)** command.
DHCP trust port	Whether to enable a DHCP trusted port in a WDS profile. ● enable: A DHCP trusted port is enabled. ● disable: A DHCP trusted port is disabled. To enable a DHCP trusted port in a WDS profile, run the **14.5.1 dhcp trust port (WDS profile view)** command.
Tagged vlan	VLAN configured in a WDS profile. To configure a VLAN in a WDS profile, run the **14.5.16 vlan tagged (WDS profile view)** command.
Priority map trust	Priority mapping trusted by the WDS air interface. To configure the parameter, run the **14.5.11 priority-map trust (WDS profile view)** command.
Priority map mode	Mapping from DSCP priorities to 802.11e user priorities on the WDS air interface. To configure the parameter, run the **14.5.10 priority-map dscp (WDS profile view)** command.

Related Topics

14.5.1 dhcp trust port (WDS profile view)
14.5.12 security-profile (WDS profile view)
14.5.16 vlan tagged (WDS profile view)
14.5.18 wds-mode
14.5.19 wds-name

 Copyright © Huawei Technologies Co., Ltd.

14.5.5 display wds-whitelist-profile

Function

The **display wds-whitelist-profile** command displays reference or configuration information about a WDS whitelist profile.

Format

display wds-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
all	Displays reference information about all WDS whitelist profiles.	-
name *whitelist-name*	Displays information about a specified WDS whitelist profile.	The WDS whitelist profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds-whitelist-profile** command to view the number of times a WDS whitelist profile is referenced or MAC addresses added in a specified WDS whitelist profile.

Example

Display reference information about all WDS whitelist profiles.

```
<Huawei> display wds-whitelist-profile all
-------------------------------------------------------------------------------
Profile name                    Reference
-------------------------------------------------------------------------------
default                          0
test                            2
-------------------------------------------------------------------------------
Total: 2
```

Table 14-132 Description of the **display wds-whitelist-profile all** command output

Item	Description
Profile name	Name of a WDS whitelist profile. To create a WDS whitelist profile, run the **14.5.23 wds-whitelist-profile** command.
Reference	Number of times a WDS whitelist profile is referenced.

Display information about the WDS whitelist profile **test**.

```
<Huawei> display wds-whitelist-profile name test
-----------------------------------------------------------------------------
WDS whitelist name: test
WDS whitelist MAC list information:
-----------------------------------------------------------------------------
Index     MAC
-----------------------------------------------------------------------------
0         1047-80b1-56a0
-----------------------------------------------------------------------------
Total: 1
```

Table 14-133 Description of the **display wds-whitelist-profile name** command output

Item	Description
Index	WDS whitelist ID in a WDS whitelist profile.
MAC	MAC address on a WDS whitelist. To add a MAC address to a WDS whitelist, run the **14.5.9 peer-ap mac (WDS whitelist profile view)** command.

Related Topics

14.5.23 wds-whitelist-profile

14.5.9 peer-ap mac (WDS whitelist profile view)

14.5.6 display wds vap

Function

The **display wds vap** command displays information about a WDS VAP.

Format

display wds vap { **ap-group** *ap-group-name* | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] } [**wds-name** *wds-name*]

display wds vap { **all** | **wds-name** *wds-name* }

Parameters

Parameter	Description	Value
ap-group *ap-group-name*	Displays information about all WDS VAPs in a specified AP group.	The AP group must exist.
ap-id *ap-id*	Displays information about WDS VAPs on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about WDS VAPs on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about WDS VAPs of a specified AP radio.	The radio ID must exist.
wds-name *wds-name*	Displays information about WDS VAPs of a specified WDS name.	The WDS name must exist.
all	Displays information about all WDS VAPs.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wds vap** command to display information about a WDS VAP.

Example

Display information about all WDS VAPs.

```
<Huawei> display wds vap all
WID : WLAN ID
--------------------------------------------------------------------------------
AP ID AP name      RfID WID       WDS name          BSSID         WDS links
--------------------------------------------------------------------------------
1     AP2          0  14          wds               60DE-4474-964D  0
1     AP2          0  13          wds               60DE-4474-964C  0
0     AP1          0  14          wds               60DE-4476-E36D  1
0     AP1          0  13          wds               60DE-4476-E36C  1
```

```
--------------------------------------------------------------------------------
Total: 4
```

Table 14-134 Description of the **display wds vap** command output

Item	Description
AP ID	AP ID.
AP name	AP name.
RfID	Radio ID.
WID	WLAN ID of a VAP.
WDS name	WDS name. To set a WDS name, run the **14.5.19 wds-name** command.
BSSID	MAC address of a VAP.
WDS links	Number of WDS links.

Related Topics

14.5.7 display wlan wds link

14.5.19 wds-name

14.5.7 display wlan wds link

Function

The **display wlan wds link** command displays information about a WDS link.

Format

display wlan wds link { **all** | **ap-id** *ap-id* [**radio** *radio-id*] | **ap-name** *ap-name* [**radio** *radio-id*] | **wds-profile** *profile-name* }

Parameters

Parameter	Description	Value
all	Displays information about all WDS links.	-
ap-id *ap-id*	Displays information about WDS links on the AP with a specified ID.	The AP ID must exist.
ap-name *ap-name*	Displays information about WDS links on the AP with a specified name.	The AP name must exist.
radio *radio-id*	Displays information about WDS links of a specified AP radio.	The radio ID must exist.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wds-profile *profile-name*	Displays information about WDS links in a specified WDS profile.	The WDS profile must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display wlan wds link** command to view information about a WDS link.

Example

Display information about all WDS links.

```
<Huawei> display wlan wds link all
Rf   : radio ID              Dis  : coverage distance(100m)
Ch   : channel               Per  : drop percent(%)
TSNR : total SNR(dB)         P-   : peer
WDS  : WDS mode              Re   : retry ratio(%)
RSSI : RSSI(dBm)             MaxR : max RSSI(dBm)
-----------------------------------------------------------------------------------------------------
APName  P-APName        Rf Dis   Ch   WDS     P-Status    RSSI  MaxR  Per  Re   TSNR  SNR(Ch0~2:dB)
-----------------------------------------------------------------------------------------------------
AP_1                 1  3    36   root    -          -77   -40   100  100  0    -/-/-
AP_2                 1  3    36   root    -          -72   -40   56   99   23   21/19/-
-----------------------------------------------------------------------------------------------------
Total: 2
```

Table 14-135 Description of the **display wlan wds link** command output

Item	Description
APName	Name of the local AP.
P-APName	Name of the peer AP.
Rf	Radio ID of the local AP.
Dis	Radio coverage distance parameter of the local AP.
Ch	Working channel of a WDS link.
WDS	WDS role of the local AP.
P-Status	Status of the peer AP.
RSSI	RSSI of the peer AP.

Item	Description
MaxR	Maximum RSSI threshold of a WDS link.
Per	Packet error ratio of a WDS link.
Re	Packet retransmission ratio of a WDS link.
TSNR	Total SNR of a WDS link.
SNR(Ch0~2:dB)	SNR of each spatial stream of a WDS link.

Related Topics

14.5.6 display wds vap

14.5.8 mode (AP wired port profile view)

Function

The **mode** command sets the working mode for an AP's wired interface.

The **undo mode** command restores the default working mode of an AP's wired interface.

By default, the GigabitEthernet interface of a common AP works in **root** mode, the Ethernet interface in **endpoint** mode, and the Eth-trunk interface in **root** mode.

NOTE

You cannot change the working mode of wired interfaces on the AP2010DN and AP2030DN.

Format

mode { **root** | **endpoint** | **middle** }

undo mode

Parameters

Parameter	Description	Value
root	Sets the working mode of an AP's wired interface to root, which can connect to an AC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
endpoint	Sets the working mode of an AP's wired interface to endpoint, which can connect to a computer or switch.	-
middle	Sets the working mode of an AP wired interface to middle, which can connect to an RRU.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When working as an uplink interface to connect to an AC, an AP's wired interface must work in root mode. In root mode, the AP's wired interface automatically joins service VLANs and user-specific VLANs (for example, VLANs assigned by the RADIUS server).

When working as a downlink interface to connect to a wired terminal, the AP's wired interface must work in endpoint mode. In endpoint mode, the AP's wired interface does not join any VLAN by default.

When the central AP connects to RRUs through downlink GigabitEthernet interfaces, the working mode of the downlink GigabitEthernet interfaces must be set to **middle**.

Configuration Impact

The AP's wired interface supports user isolation in endpoint mode, but not in root mode.

If the working mode of an AP's wired interface is set to **root** in the AP wired port profile, you cannot set the **vlan pvid** *vlan-id*. In turn, if you set the **vlan pvid** *vlan-id*, you cannot set the working mode of the AP's wired interface to **root**.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] quit
```

```
[Huawei-wlan-view] wired-port-profile name wired
[Huawei-wlan-wired-port-wired] mode endpoint
[Huawei-wlan-wired-port-wired] quit
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

Related Topics

14.1.240 wired-port-profile (WLAN view)

14.5.9 peer-ap mac (WDS whitelist profile view)

Function

The **peer-ap mac** command adds MAC addresses of neighboring APs that are allowed to connect to an AP to a WDS whitelist profile.

The **undo peer-ap mac** command deletes the MAC addresses of neighboring APs from a WDS whitelist profile.

By default, no MAC address of a neighboring AP is added to a WDS whitelist profile.

Format

peer-ap mac *mac-address*

undo peer-ap mac *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of a neighboring AP to be added to a WDS whitelist profile.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

Views

WDS whitelist profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS whitelist profile is created, you can run the **peer-ap mac** command to add neighboring APs' MAC addresses to the profile.

 Copyright © Huawei Technologies Co., Ltd.

If a WDS whitelist profile is bound to a WDS profile, only APs with MAC addresses in the WDS whitelist profile can access the local AP, and other APs are denied access.

Precautions

A maximum of six MAC addresses can be added to a WDS whitelist profile.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-whitelist-profile name whitelist
[Huawei-wlan-wds-whitelist-whitelist] peer-ap mac 0001-0001-0001
[Huawei-wlan-wds-whitelist-whitelist] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] radio 0
[Huawei-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

Related Topics

14.5.23 wds-whitelist-profile

14.5.10 priority-map dscp (WDS profile view)

Function

The **priority-map dscp** command configures the mapping from DSCP priorities to 802.11e user priorities on the WDS air interface.

The **undo priority-map dscp** command restores the default mapping from DSCP priorities to 802.11e user priorities on the WDS air interface.

Table 14-136 describes the mapping from DSCP priorities to 802.11e user priorities by default.

Table 14-136 Mapping from DSCP priorities to 802.11e user priorities

DSCP Priority	802.11e User Priority
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

 Copyright © Huawei Technologies Co., Ltd.

Format

priority-map dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **dot11e** *dot11e-value*

undo priority-map dscp

Parameters

Parameter	Description	Value
dscp *dscp-value1*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
to *dscp-value2*	Specifies the DSCP priority of 802.3 packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.
dot11e *dot11e-value*	Specifies the 802.11e user priority.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

On a WDS network, you can run this command to configure the mapping from DSCP priorities to 802.11e user priorities on the WDS air interface of an AP.

Example

Map DSCP priorities 0-6 to 802.11e user priority 0 on the WDS air interface.

```
<Huawei> system-view
[Huawei] wlan ac
```

```
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] priority-map dscp 0 to 6 dot11e 0
```

Related Topics

14.5.11 priority-map trust (WDS profile view)

14.5.11 priority-map trust (WDS profile view)

Function

The **priority-map trust** command configures the priority mapping to be trusted by the WDS air interface.

The **undo priority-map trust** command restores the default priority mapping to be trusted by the WDS air interface.

By default, the WDS air interface trusts the mapping from DSCP priorities to 802.11e user priorities.

Format

priority-map trust { **dot1p** | **dscp** }

undo priority-map trust

Parameters

Parameter	Description	Value
dot1p	Indicates that the WDS air interface trusts the mapping from 802.1p priorities to 802.11e user priorities.	-
dscp	Indicates that the WDS air interface trusts the mapping from DSCP priorities to 802.11e user priorities.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

On a WDS network, when 802.1p or DSCP priorities in data packets need to be mapped to 802.11e user priorities and the packets are transmitted through a WDS link, run this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the WDS air interface to trust the mapping from 802.1p priorities to 802.11e user priorities.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] priority-map trust dot1p
```

Related Topics

14.5.10 priority-map dscp (WDS profile view)

14.5.12 security-profile (WDS profile view)

Function

The **security-profile** command binds a security profile to a WDS profile.

The **undo security-profile** command restores the default security profile bound to a WDS profile.

By default, the security profile **default-wds** is bound to a WDS profile.

Format

security-profile *profile-name*

undo security-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the security profile bound to a WDS profile.	The security profile must exist and be configured with the security policy WPA2+PSK+AES.

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before a WDS profile is applied to an AP radio to set up WDS links, the WDS profile must have a security profile bound to ensure WDS link security.

Precautions

Currently, the WDS profile supports only the security policy WPA2+PSK+AES. After a security profile is bound to a WDS profile, the authentication policy and encryption mode in the security profile cannot be changed, but the authentication key can be changed.

A WDS profile can only have one security profile bound. If you run the command multiple times in the same WDS profile view, the latest configuration overwrites the old one.

Example

Create the security profile **sec** and set the security policy to WPA2+PSK+AES. Create the WDS profile **test** and bind the security profile to the WDS profile.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] security-profile name sec
[Huawei-wlan-sec-prof-sec] security wpa2 psk pass-phrase huawei@123 aes
[Huawei-wlan-sec-prof-sec] quit
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] security-profile sec
```

Related Topics

14.4.35 security-profile
14.5.20 wds-profile

14.5.13 user-isolate (AP wired port profile view)

Function

The **user-isolate** command enables user isolation on an AP's wired interface.

The **undo user-isolate** command disables user isolation on an AP's wired interface.

By default, user isolation is disabled on an AP's wired interface.

Format

user-isolate { **all** | **l2** }

undo user-isolate

Parameters

Parameter	Description	Value
all	Enables Layer 2 and Layer 3 user isolation.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
l2	Enables Layer 2 user isolation.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user isolation function prevents users on the same wired interface from communicating with each other. All user traffic on the wired interface is forwarded by the gateway. Therefore, this function ensures communication security on wired interfaces and allows uniform charging for users.

Precautions

Eth-Trunk member interfaces do not support the user isolation function.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint** and enable Layer 2 user isolation on GE0.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] quit
[Huawei-wlan-view] wired-port-profile name wired
[Huawei-wlan-wired-port-wired] mode endpoint
[Huawei-wlan-wired-port-wired] user-isolate l2
[Huawei-wlan-wired-port-wired] quit
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

Related Topics

14.1.240 wired-port-profile (WLAN view)

14.5.14 user-isolate (traffic profile view)

Function

The **user-isolate** command enables user isolation.

The **undo user-isolate** command disables user isolation.

By default, user isolation is disabled in a traffic profile.

Format

user-isolate l2

undo user-isolate

Parameters

Parameter	Description	Value
l2	Specifies Layer 2 user isolation.	-

Views

Traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The user isolation function prevents users in the same traffic profile from communicating with each other. All user traffic in the traffic profile is forwarded by the gateway. Therefore, this function ensures communication security on wired interfaces and allows uniform charging for users.

You can run the **user-isolate** command to enable user isolation on a traffic profile.

Example

Enable Layer 2 user isolation in traffic profile **p1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] traffic-profile name p1
[Huawei-wlan-traffic-prof-p1] user-isolate l2
Warning: This action may cause service interruption. Continue?[Y/N]y
```

14.5.15 vlan pvid (AP wired port profile view)

Function

The **vlan pvid** command sets the PVID for an AP wired interface.

The **undo vlan pvid** command deletes the PVID of an AP wired interface.

By default, no PVID is configured for an AP wired interface.

Format

vlan pvid *vlan-id*

undo vlan pvid

Parameters

Parameter	Description	Value
vlan-id	Specifies the PVID of an AP's wired interface.	The value is an integer that ranges from 1 to 4094.

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The APs on the WLAN WDS network only process tagged packets.

When receiving an untagged packet from a peer device, the AP wired interface adds a VLAN tag to the packet. After the PVID is configured on the wired interface, the interface adds the PVID to all the received untagged packets.

NOTE

In the following paragraphs, packets sent by the AP's wired interface refer to the management packets and service packets sent in the tunnel forwarding mode.

- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command, packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in untagged mode using the **vlan untagged** *vlan-id* command, the packets sent from the AP's wired interface are not tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in tagged mode using the **vlan tagged** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the PVID of the AP's wired interface is set to the management VLAN ID using the **vlan pvid** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.

Precautions

Eth-Trunk member interfaces do not support PVID setting.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint** and set the PVID of GE0 to VLAN 1.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] quit
[Huawei-wlan-view] wired-port-profile name wired
[Huawei-wlan-wired-port-wired] mode endpoint
[Huawei-wlan-wired-port-wired] vlan pvid 1
[Huawei-wlan-wired-port-wired] quit
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

Related Topics

14.1.240 wired-port-profile (WLAN view)

14.5.16 vlan tagged (WDS profile view)

Function

The **vlan tagged** command adds one or a group of VLANs to a WDS profile in tagged mode.

The **undo vlan tagged** command deletes VLANs from a WDS profile.

By default, no VLAN is configured in a WDS profile.

NOTE

Currently, VLANs can only be added to a WDS profile in tagged mode.

Format

vlan tagged { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan tagged { { *vlan-id1* [**to** *vlan-id2*] } &<1-10> | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the tagged VLAN ID. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be equal to or greater than the value of *vlan-id1*. The *vlan-id1* and *vlan-id2* parameters determine a VLAN range. If **to** *vlan-id2* is not specified, only the VLAN specified by *vlan-id1* is added to the WDS profile in tagged mode. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	• The value of *vlan-id1* is an integer that ranges from 1 to 4094. • The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes all tagged VLANs from a WDS profile.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Adding VLANs to a WDS profile is equivalent to adding hybrid interfaces to a VLAN. After one or a group of VLANs is added to a WDS profile, the WDS link forwards only the packets with these VLAN IDs from STAs and peer APs.

NOTE

A maximum of 256 VLANs can be added to a WDS profile.

Example

Create the WDS profile **test** and add VLANs 3, 4, 5, 6, 10, and 12 to the WDS profile in **tagged** mode.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] vlan tagged 3 to 6 10 12
```

Related Topics

14.5.20 wds-profile

14.5.17 vlan (AP wired port profile view)

Function

The **vlan** command configures the VLAN to which an AP wired interface belongs.

The **undo vlan** command deletes the VLAN to which an AP wired interface belongs.

By default, an AP wired interface is added to VLAN 1 in untagged mode.

NOTE

An AP's wired interface can be added to a maximum of 256 VLANs.

Format

vlan { **tagged** | **untagged** } { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo vlan { **all** | *vlan-id1* [**to** *vlan-id2*] &<1-10> }

Parameters

Parameter	Description	Value
tagged	Adds a wired interface to a VLAN in tagged mode.	-
untagged	Adds a wired interface to a VLAN in untagged mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan-id1 [**to** *vlan-id2*]	Specifies the ID of the VLAN to which the wired interface belongs. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If **to** *vlan-id2* is not specified, the wired interface is added to the VLAN specified by *vlan-id1*. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	● The value of *vlan-id1* is an integer that ranges from 1 to 4094. ● The value of *vlan-id2* is an integer that ranges from 1 to 4094.
all	Deletes the VLANs to which the AP wired interface belongs.	-

Views

AP wired port profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a wired interface connects to a PC or Layer 2 network, the interface is equivalent to a hybrid interface on a switch, and can forward the packets with multiple VLAN tags.

After the **vlan tagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command is executed to add the wired interface to one or more VLANs in tagged mode, the interface does not remove VLAN tags from the packets it forwarded.

After the **vlan untagged** { *vlan-id1* [**to** *vlan-id2*] } &<1-10> command is executed to add the wired interface to one or more VLANs in untagged mode, the interface removes VLAN tags from the packets it forwarded.

NOTE

In the following paragraphs, packets sent by the AP's wired interface refer to the management packets and service packets sent in the tunnel forwarding mode.

- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command, packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in untagged mode using the **vlan untagged** *vlan-id* command, the packets sent from the AP's wired interface are not tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the AP's wired interface is added to the management VLAN in tagged mode using the **vlan tagged** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.
- After the AP's management VLAN is configured using the **management-vlan** *vlan-id* command and the PVID of the AP's wired interface is set to the management VLAN ID using the **vlan pvid** *vlan-id* command, the packets sent from the AP's wired interface are tagged with the management VLAN ID.

Configuration Impact

Eth-Trunk member interfaces cannot be added to VLANs.

Example

Set the working mode of the AP's wired interface GE0 to **endpoint** and add GE0 to VLANs 3, 4, 5, and 10 in **tagged** mode and to VLANs 12, 13, 14, and 20 in **untagged** mode.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] quit
[Huawei-wlan-view] wired-port-profile name wired
[Huawei-wlan-wired-port-wired] mode endpoint
[Huawei-wlan-wired-port-wired] vlan tagged 3 to 5 10
[Huawei-wlan-wired-port-wired] vlan untagged 12 to 14 20
[Huawei-wlan-wired-port-wired] quit
[Huawei-wlan-view] ap-group name ap-group1
[Huawei-wlan-ap-group-ap-group1] wired-port-profile wired gigabitethernet 0
```

Related Topics

14.1.240 wired-port-profile (WLAN view)

14.5.18 wds-mode

Function

The **wds-mode** command sets the WDS mode in a WDS profile.

By default, the WDS mode in a WDS profile is **leaf**.

Format

wds-mode { **root** | **middle** | **leaf** }

Parameters

Parameter	Description	Value
root	Sets the WDS mode to root.	-
middle	Sets the WDS mode to middle.	-
leaf	Sets the WDS mode to leaf.	-

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To connect an AP to an AC through WDS links, use this command to set the WDS mode for an AP radio based on the location of the AP on a WDS network.

In the downlink direction, a root node can connect to a middle or leaf node, and a middle node can connect to a leaf node. A leaf node is the termination node of a WDS link.

Precautions

After changing the WDS mode in a WDS profile, reset the APs using the profile to make the changed WDS mode take effect.

Example

Create the WDS profile **test** and set the WDS mode of the profile to **middle**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] wds-mode middle
```

Related Topics

14.5.20 wds-profile

14.5.19 wds-name

Function

The **wds-name** command sets a WDS name for a WDS profile.

The **undo wds-name** command deletes the WDS name of a WDS profile.

By default, the WDS name of a WDS profile is **HUAWEI-WLAN-WDS**.

Format

wds-name *name*

undo wds-name

Parameters

Parameter	Description	Value
name	Specifies the character string that indicates the WDS name.	The value is a string of 1 to 32 case-sensitive characters. It does not contain question marks (?)or spaces, and cannot start or end with double quotation marks (" ").

Views

WDS profile view

Default Level

2: Configuration level

Usage Guidelines

A WDS name is similar to an SSID. On a WDS network, an AP radio discovers WDS services provided by other APs based on the WDS name.

Each WDS profile must have a WDS name. The default WDS name of a WDS profile is **HUAWEI-WLAN-WDS**. You can run the **14.5.19 wds-name** command to set a WDS name for a WDS profile.

Example

Create the WDS profile **test** and set the WDS name of the profile to **bridge**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] wds-name bridge
```

Related Topics

14.5.20 wds-profile

14.5.20 wds-profile

Function

The **wds-profile** command creates a WDS profile or displays the WDS profile view.

The **undo wds-profile** command deletes a WDS profile.

By default, the system provides the WDS profile **default**.

Format

wds-profile name *profile-name*

undo wds-profile { **all** | **name** *profile-name* }

Parameters

Parameter	Description	Value
name *profile-name*	Specifies the name of a WDS profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all WDS profiles. **NOTE** The WDS profile **default** cannot be deleted.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Each WDS profile must have a WDS name. The default WDS name of a WDS profile is **HUAWEI-WLAN-WDS**. You can run the **14.5.19 wds-name** command to set a WDS name for a WDS profile.

Example

Create the WDS profile **test** and set the WDS name of the profile to **bridge**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-profile name test
[Huawei-wlan-wds-prof-test] wds-name bridge
```

Related Topics

14.5.19 wds-name

14.5.21 wds-profile radio

Function

The **wds-profile radio** command binds a WDS profile to an AP group or AP.

The **undo wds-profile radio** command deletes a WDS profile from an AP group or AP.

By default, no WDS profile is bound to an AP group or AP.

Format

wds-profile *profile-name* **radio** { **all** | *radio-id* }

undo wds-profile radio { **all** | *radio-id* }

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the WDS profile bound to an AP or AP group.	The WDS profile must exist.
all	Binds a WDS profile to all AP radios.	-
radio-id	Binds a WDS profile to a specified AP radio.	The radio ID must exist.

Views

AP group view, AP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a WDS profile is bound to an AP or AP group, the AP radio will generate a WDS VAP to provide WDS services. The WDS VAP provides hidden SSIDs for WDS nodes to set up connections.

Prerequisites

A WDS profile has been created and configured properly.

Precautions

Among the VAPs created after a WDS profile is bound to an AP radio, the VAPs with the WLAN IDs 13 and 14 cannot be occupied.

An AP radio can only have one WDS profile bound.

Example

Bind the WDS profile **test** to radio **0** of APs in the AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] wds-profile test radio 0
```

Related Topics

14.5.20 wds-profile

14.5.22 wds-profile (AP group radio view or AP radio view)

Function

The **wds-profile** command binds a WDS profile to an AP radio.

The **undo wds-profile** command unbinds a WDS profile from an AP radio.

By default, no WDS profile is bound to an AP radio.

Format

wds-profile *profile-name*

undo wds-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the WDS profile bound to an AP radio.	The WDS profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After a WDS profile is bound to an AP radio, the radio will generate a WDS VAP to provide WDS services. The WDS VAP provides hidden SSIDs for WDS nodes to set up connections.

Prerequisites

A WDS profile has been created and configured properly.

Precautions

Among the VAPs created after a WDS profile is bound to an AP radio, the VAPs with the WLAN IDs 13 and 14 cannot be occupied.

An AP radio can only have one WDS profile bound.

This command has the same function as the **14.5.21 wds-profile radio** command. You can use either of them.

Example

Bind the WDS profile **test** to radio **0** of APs in the AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] radio 0
[Huawei-wlan-group-radio-group1/0] wds-profile test
```

Related Topics

14.5.20 wds-profile

14.5.21 wds-profile radio

14.5.23 wds-whitelist-profile

Function

The **wds-whitelist-profile** command creates a WDS whitelist profile or displays the WDS whitelist profile view.

The **undo wds-whitelist-profile** command deletes a WDS whitelist profile.

By default, no WDS whitelist profile is available in the system.

Format

wds-whitelist-profile name *whitelist-name*

undo wds-whitelist-profile { **all** | **name** *whitelist-name* }

Parameters

Parameter	Description	Value
name *whitelist-name*	Specifies the name of a WDS whitelist profile.	The value is a string of 1 to 35 case-insensitive characters. It does not contain question marks (?) or spaces, and cannot begin or end with double quotation marks (" ").
all	Deletes all WDS whitelist profiles.	-

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

After a WDS whitelist profile is created using the **wds-whitelist-profile** command, you can run the **14.5.9 peer-ap mac (WDS whitelist profile view)** command in the WDS whitelist profile view to add MAC addresses of peer APs that are allowed to set up WDS links with the local AP to the profile.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-whitelist-profile name whitelist
[Huawei-wlan-wds-whitelist-whitelist] peer-ap mac 0001-0001-0001
[Huawei-wlan-wds-whitelist-whitelist] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] radio 0
[Huawei-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

Related Topics

14.5.9 peer-ap mac (WDS whitelist profile view)

14.5.20 wds-profile

14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)

 Copyright © Huawei Technologies Co., Ltd.

14.5.24 wds-whitelist-profile (AP group radio view or AP radio view)

Function

The **wds-whitelist-profile** command binds a WDS whitelist profile to an AP radio.

The **undo wds-whitelist-profile** command unbinds a WDS whitelist profile from an AP radio.

By default, no WDS whitelist profile is bound to an AP radio.

Format

wds-whitelist-profile *whitelist-name*

undo wds-whitelist-profile

Parameters

Parameter	Description	Value
whitelist-name	Specifies the name of the WDS whitelist profile bound to an AP radio.	The WDS whitelist profile must exist.

Views

AP group radio view, AP radio view

Default Level

2: Configuration level

Usage Guidelines

After a WDS whitelist profile is applied to an AP radio, the AP radio can only set up WDS links with neighboring APs whose MAC addresses are in the WDS whitelist profile. If no WDS whitelist profile is bound to an AP radio, the AP radio can establish WDS links with any neighboring APs.

NOTE

On a WDS network, a root or middle node controls subnode access by MAC addresses added to the WDS whitelist profile. However, a leaf node does not require a whitelist.

An AP radio can only have one WDS whitelist profile bound. If you run the command multiple times on the same AP radio, the latest configuration overwrites the old one.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create the WDS whitelist profile **whitelist** and add the MAC address **0001-0001-0001** to the whitelist profile. Bind the WDS whitelist profile **whitelist** to radio **0** of APs in the AP group **group1**.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] wds-whitelist-profile name whitelist
[Huawei-wlan-wds-whitelist-whitelist] peer-ap mac 0001-0001-0001
[Huawei-wlan-wds-whitelist-whitelist] quit
[Huawei-wlan-view] ap-group name group1
[Huawei-wlan-ap-group-group1] radio 0
[Huawei-wlan-group-radio-group1/0] wds-whitelist-profile whitelist
```

Related Topics

14.5.20 wds-profile
14.5.23 wds-whitelist-profile

14.6 WLAN Reliability Commands

14.6.1 ac protect cold-backup kickoff-station

Function

The **ac protect cold-backup kickoff-station** command enables the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured.

The **undo ac protect cold-backup kickoff-station** command restores the default setting.

By default, STAs using open system authentication remain connected to APs when an active/standby AC switchover is implemented.

Format

ac protect cold-backup kickoff-station

undo ac protect cold-backup kickoff-station

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

An active/standby switchover between two ACs that have dual-link cold backup configured causes a short service interruption.

- STAs not using open system authentication are disconnected from APs and need to go online again after the active/standby switchover.
- By default, STAs using open system authentication remain connected to APs and do not need to go online again after the active/standby switchover. You can run the **ac protect cold-backup kickoff-station** command to configure the STAs to be disconnected when an active/standby AC switchover is implemented.

Example

Enable the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ac protect cold-backup kickoff-station
```

Related Topics

14.6.6 display ac protect

14.6.2 ac protect enable

Function

The **ac protect enable** command enables dual-link backup globally and disables N+1 backup.

The **undo ac protect enable** command disables dual-link backup globally and enables N+1 backup.

By default, dual-link backup is disabled globally, and N+1 backup is enabled.

Format

ac protect enable

undo ac protect enable

Parameters

None

Views

WLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To ensure service stability, an AP needs to establish connections with two ACs. The two ACs work in active/standby mode. The active AC provides services for APs, whereas the standby AC is a backup to the active AC.

Follow-up Procedure

After dual-link backup or N+1 backup is enabled globally, configure the AC priority and standby AC IP address to implement dual-link backup or N+1 backup.

Precautions

Ensure that active and standby ACs deliver the same WLAN service configuration to an AP that connects to the two ACs.

Example

Enable dual-link backup globally and disable N+1 backup.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ac protect enable
Warning: This operation maybe cause AP reset, continue?[Y/N]:y
```

Related Topics

14.6.6 display ac protect

14.6.3 ac protect priority

Function

The **ac protect priority** command configures the AC priority in the WLAN view.

The **undo ac protect priority** command restores the default AC priority in the WLAN view.

By default, the AC priority in the WLAN view is 0.

Format

ac protect priority *priority*

undo ac protect priority

Parameters

Parameter	Description	Value
priority	Specifies the AC priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP goes online, ACs deliver their priorities to the AP. The AP selects the AC with a higher priority as the active AC and establishes a CAPWAP tunnel with the active AC.

To implement dual-link backup on all the APs connected to an AC, configure the AC priority and standby AC IP address in the WLAN view to reduce the configuration workload.

Precautions

If the AC priority is configured in the WLAN view and AP system profile view before an AP goes online, the AC priority configured in the AP system profile view is delivered to the AP. If no AC priority is configured in the AP system profile view, the AC priority configured in the WLAN view is delivered to the AP.

Example

Set the AC priority to 3 in the WLAN view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ac protect priority 3
```

Related Topics

14.6.6 display ac protect
14.6.7 priority

14.6.4 ac protect protect-ac

Function

The **ac protect protect-ac** command configures the standby AC IP address in the WLAN view.

The **undo ac protect protect-ac** command restores the default standby AC IP address in the WLAN view.

By default, no standby AC IP address is configured in the WLAN view.

Format

ac protect protect-ac *ip-address*

undo ac protect protect-ac

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address for the standby AC.	The value is in dotted decimal notation.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement dual-link backup on all the APs connected to an AC, configure the AC priority and standby AC IP address in the WLAN view to reduce the configuration workload.

Precautions

If standby AC IP addresses are configured in both the WLAN view and AP system profile view before an AP goes online, the standby AC IP address configured in the AP system profile view is delivered to an AP. If no standby AC IP address is configured in the AP system profile view, the standby AC IP address configured in the WLAN view is delivered to an AP. If no standby AC IP address is configured in the WLAN view, dual-link backup is disabled.

Example

Set the standby AC IP address to 10.33.12.56 in the WLAN view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ac protect protect-ac 10.33.12.56
```

Related Topics

14.6.6 display ac protect
14.6.8 protect-ac

14.6.5 ac protect restore disable

Function

The **ac protect restore disable** command disables global revertive switching.

The **undo ac protect restore disable** command enables global revertive switching.

By default, global revertive switching is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

ac protect restore disable

undo ac protect restore disable

Parameters

None.

Views

WLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

AC1 is the active AC and AC2 is the standby AC. When the link between AC1 and an AP fails, AC2 takes the active role.

When the link between AC1 and the AP recovers, the AP detects that AC1 priority is higher than AC2 and instructs AC1 and AC2 to perform revertive switching. AC1 then becomes the active AC again.

Precautions

- The **undo wlan ac protect restore disable** command must be used before an AP goes online and dual-link backup is implemented. In this way, the AC delivers the revertive switching configuration to the AP when the AP goes online.
- If global revertive switching is disabled, traffic of an AP cannot be switched back to AC1 when the link between AC1 and the AP restores.
- The command takes effect after an AP restart.

Example

Disable global revertive switching.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ac protect restore disable
```

Related Topics

14.6.6 display ac protect

14.6.6 display ac protect

Function

The **display ac protect** command displays AC dual-link backup configuration.

Format

display ac protect

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays AC dual-link backup configuration.

Example

Display AC dual-link backup configuration.

```
<Huawei> display ac protect
-----------------------------------------------------------
Protect state            : disable
Protect AC               : -
Priority                 : 0
Protect restore          : enable
Coldbackup kickoff station: disable
-----------------------------------------------------------
```

Table 14-137 Description of the **display ac protect** command output

Item	Description
Protect state	Whether global dual-link backup and N+1 backup are enabled. ● disable: Global dual-link backup is disabled, and N+1 backup is enabled. ● enable: Global dual-link backup is enabled, and N+1 backup is disabled. To configure the parameter, run the **14.6.2 ac protect enable** command.
Protect AC	Standby AC IP address. To configure the parameter, run the **14.6.4 ac protect protect-ac** command.

 Copyright © Huawei Technologies Co., Ltd.

Priority	Priority of the local AC. To configure the parameter, run the **14.6.3 ac protect priority** command.
Protect restore	Whether global revertive switching is enabled on the AC. To configure the parameter, run the **14.6.5 ac protect restore disable** command.
Coldbackup kickoff station	Whether to enable the function of disconnecting STAs in open system authentication mode when an active/standby switchover is implemented between ACs that have dual-link cold backup configured. To configure the parameter, run the **14.6.1 ac protect cold-backup kickoff-station** command.

Related Topics

14.6.1 ac protect cold-backup kickoff-station
14.6.2 ac protect enable
14.6.3 ac protect priority
14.6.4 ac protect protect-ac
14.6.5 ac protect restore disable

14.6.7 priority

Function

The **priority** command sets the AC priority in the AP system profile view.

The **undo priority** command restores the AC priority to the default setting in the AP system profile view.

By default, no AC priority is configured in the AP system profile view.

Format

priority *priority-level*

undo priority

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
priority-level	Specifies the AC priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AP goes online, ACs deliver their priorities to the AP. The AP selects the AC with the highest priority as the active AC and establishes a CAPWAP tunnel with the active AC.

Precautions

If the AC priority is configured in the WLAN view and AP system profile view before an AP goes online, the AC priority configured in the AP system profile view is delivered to the AP. If no AC priority is configured in the AP system profile view, the AC priority configured in the WLAN view is delivered to the AP.

If ACs deliver the same priorities to the AP, the AP selects the AC with the lowest AP load as the active AC. If both AC priorities and AP load are the same, the AP selects the AC with the lowest STA load as the active AC. If AC priorities, AP load, and STA load are the same, the AP selects the AC with the smallest IP address as the active AC to establish a CAPWAP tunnel. The AP or STA load equals the number of allowed APs or STAs minus the number of existing APs or STAs.

Example

Set the AC priority to 3 in the AP system profile view.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] priority 3
```

Related Topics

14.1.98 display ap-system-profile

14.6.8 protect-ac

Function

The **protect-ac** command configures the standby AC's IP address in the AP system profile view.

The **undo protect-ac** command restores the standby AC's IP address to the default setting in the AP system profile view.

By default, no standby AC's IP address is configured in the AP system profile view.

Format

protect-ac ip-address *ip-address*

undo protect-ac

Parameters

Parameter	Description	Value
ip-address *ip-address*	Specifies an IPv4 address for the standby AC.	The value is in dotted decimal notation.

Views

AP system profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To connect an AP to two ACs (active and standby ACs) to implement dual-link backup, you can run the **protect-ac** command to configure the standby AC's IP address in the AP system profile view.

Precautions

If standby AC's IP addresses are configured in both the WLAN view and AP system profile view, the standby AC's IP address configured in the AP system profile view is delivered to an AP. If no standby AC's IP address is configured in the AP system profile view, the standby AC's IP address configured in the WLAN view is delivered to an AP.

Example

Set the standby AC's IP address to 10.3.3.3 in the AP system profile view.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] wlan ac
[Huawei-wlan-view] ap-system-profile name ap-system1
[Huawei-wlan-ap-system-prof-ap-system1] protect-ac ip-address 10.3.3.3
```

Related Topics

14.1.98 display ap-system-profile

 Copyright © Huawei Technologies Co., Ltd.

15 Energy Efficiency Commands

About This Chapter

NOTE

The feature is just for beta test, and is not for commercial use. If the feature is required in the test, contact Huawei technical support personnel.

Only the AR169RW-P-M9 supports Energy Efficiency Commands.

15.1 authentication mode

15.2 authentication passwd

15.3 authentication zigbee link-key

15.4 display channel-type zigbee status

15.5 display m2m-gateway configuration

15.6 display m2m-gateway long-latitude

15.7 display m2m-gateway statistics

15.8 display m2m-gateway status

15.9 display m2m-gateway task

15.10 display m2m-gateway task list group-task

15.11 display m2m-gateway task list optimal-task

15.12 display m2m-gateway task list statistics

15.13 display m2m-gateway task schedule

15.14 display m2m-gateway tsvr-server status

15.15 display m2m-gateway timer-join-network

15.16 display m2m-gateway upgrade current

15.17 display m2m-gateway upstream communication style

15.18 display m2m-gateway upstream statistics

 Copyright © Huawei Technologies Co., Ltd.

15.19 display m2m-gateway whitelist
15.20 display firmware process
15.21 display zigbee link-key-using
15.22 encrypt mode disable
15.23 encrypt type
15.24 firmware upgrade channel-type zigbee remote
15.25 firmware upgrade channel-type zigbee local
15.26 firmware upgrade channel-type zigbee erase flash
15.27 firmware upgrade stop
15.28 hes-bakserver
15.29 hes-server
15.30 longitude-latitude
15.31 m2m-gateway
15.32 reset m2m-gateway offline-device
15.33 reset m2m-gateway statistics
15.34 restore factory configuration
15.35 task delete
15.36 task update task-name
15.37 tsvr-server
15.38 upstream-cache cache-size wait-time
15.39 upstream-cache mode
15.40 upstream statistics threshold
15.41 zigbee-network dismiss
15.42 zigbee-network get-rssi
15.43 zigbee-network permit-join
15.44 zigbee-network permit-join whitelist
15.45 zigbee-network status refresh
15.46 zigbee-network timer-join-network
15.47 zigbee-network timer-join-network enable

 Copyright © Huawei Technologies Co., Ltd.

15.1 authentication mode

Function

The **authentication mode enable** command enables authentication between the device and AgileConnect.

The **authentication mode disable** command disables authentication between the device and AgileConnect.

By default, authentication between the device and AgileConnect is enabled.

Format

authentication mode { **enable** | **disable** }

Parameters

None

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

To prevent unauthorized devices from connecting to the AgileConnect or devices from connecting to the unauthorized AgileConnect, enable authentication between the device and AgileConnect. The device can communicate with the AgileConnect only when the passwords for authentication on them are the same.

NOTICE

You are advised to enable authentication between devices and the AgileConnect. If not, security risks exist.

Example

Enable authentication between the device and AgileConnect.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] authentication mode enable
Info: Set Auth Mode Enable Successfully!
```

Related Topics

15.2 authentication passwd

 Copyright © Huawei Technologies Co., Ltd.

15.2 authentication passwd

Function

The **authentication passwd** command configures the password for authentication between the device and AgileConnect.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

authentication passwd *password*

Parameters

Parameter	Description	Value
password	Specifies the password for authentication between the device and AgileConnect.	The value is a string of 6 to 31 case-sensitive characters without spaces.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

After authentication between the device and AgileConnect is enabled, run this command to configure the password for authentication. The device can communicate with the AgileConnect only when the passwords for authentication on them are the same.

Example

Set the password for authentication between the device and AgileConnect to Huawei@1234.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] authentication passwd Huawei@1234
Info: Update Passwd Successfully!
```

Related Topics

15.1 authentication mode

 Copyright © Huawei Technologies Co., Ltd.

15.3 authentication zigbee link-key

Function

The **authentication zigbee link-key** command configures the key for communication between the device and smart terminals.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

authentication zigbee link-key { **custom-key** *key* | **huawei-key** | **silabs-default-key** }

Parameters

Parameter	Description	Value
custom-key *key*	Specifies the user-defined key for communication between the device and smart terminals.	The value is a string of 6 to 16 case-sensitive characters without spaces.
huawei-key	Indicates the Huawei key for communication between the device and smart terminals.	-
silabs-default-key	Indicates the public key for communication between the device and smart terminals.	-

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

The public key silabs-default-key is often used on the ZigBee network, which can be easily attacked by third-party devices. There are potential security risks. To

 Copyright © Huawei Technologies Co., Ltd.

prevent malicious attacks by third-party devices, the device allows the key to be changed to the Huawei or user-defined key. This improves the network security.

After the key is changed on the device, the changed key needs to be synchronized on smart terminals.

NOTICE

During key switching, the ZigBee network will be re-established. Exercise caution when you run this command.

Example

Configure the user-defined key Huawei@123 for communication between the device and smart terminals.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] authentication zigbee link-key custom-key Huawei@123
Warning: Change Link-key will fromat the network. Are you sure to continue?
[Y/N]y
..........
Info: Set custom link key Successfully!
```

Related Topics

15.21 display zigbee link-key-using

15.4 display channel-type zigbee status

Function

The **display channel-type zigbee status** command displays the status of smart terminals on the ZigBee network.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

display channel-type zigbee status [**hwarc** | **hwbmcd** | **hwcc** | **hwdgcp** | **hwgem** | **hwirr** | **hwmvrdc** | **hwod** | **hwscd** | **hwsgcp** | **hwslc** | **hwss** | **hwtc** | **hwths** | **hwtls32a** | **unkonw**]

Parameters

Parameter	Description	Value
hwarc	Displays the status of the fresh air controller.	-

Parameter	Description	Value
hwbmcd	Displays the status of the brightness movement combo detector.	-
hwcc	Displays the status of the curtain controller.	-
hwdgcp	Displays the status of the two-way switch.	-
hwgem	Displays the status of the general expansion module.	-
hwirr	Displays the status of the infrared controller.	-
hwmvrdc	Displays the status of the ducted type air conditioner controller.	-
hwod	Displays the status of the object detector.	-
hwscd	Displays the status of the single-controller dimmer.	-
hwsgcp	Displays the status of the one-way switch.	-
hwslc	Displays the status of the street lamp controller.	-
hwss	Displays the status of the smart socket.	-
hwtc	Displays the status of the traffic counter.	-
hwths	Displays the status of the temperature and humidity sensor.	-
hwtls32a	Displays the status of the three-phase load switch (32 A).	-
unkonw	Displays the status of other smart terminals.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the smart terminal status including the smart terminal type, MAC address, online status, and logout cause on the ZigBee network, run this command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the status of smart sockets on the ZigBee network.

```
<Huawei> display channel-type zigbee status hwss
Firmware Version:001
PanId: 0x6325
RadioTxPower: 8
RadioChannel: 20
Zigbee Device-table:
Index Device Type      Mac     DeviceId          Status  OffReason Version      RSSI
-----------------------------------------------------------------------------------------------
1     HWSS             0x8635  1300B136CB000658    Online  Never     0x270a0114    40
-----------------------------------------------------------------------------------------------
Online count: 1                  Total count: 1
```

Table 15-1 Description of the **display channel-type zigbee status** command output

Item	Description
Firmware Version	EM357 firmware version.
PanId	ZigBee network ID.
RadioTxPower	EM357 transmit power.
RadioChannel	EM357 channel information.
Index	Index of the smart terminal.
Device Type	Type of the smart terminal.
Mac	MAC address of the smart terminal.
DeviceId	ID of the smart terminal.
Status	Whether the smart terminal is connected to the network: ● Online: The smart terminal is connected to the network. ● Offline: The smart terminal is disconnected from the network.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
OffReason	Reason why the smart terminal is disconnected from the network last time: ● SrvCtl: The CBEMS controls the network disconnection of the smart terminal. ● Detect: The gateway detects that the smart terminal is disconnected from the network through heartbeat packets. ● RepOff: The gateway receives logout messages reported by the smart terminal and then sets the smart terminal status to offline. ● RepIdChg: The communication address of the smart terminal changes. ● Never: The smart terminal has never been disconnected from the network after being connected to the network.
Version	Version of the smart terminal.
Online count	Number of smart terminals connected to the ZigBee network.
RSSI	RSSI of smart terminals.
Total count	Total number of smart terminals on the ZigBee network.

15.5 display m2m-gateway configuration

Function

The **display m2m-gateway configuration** command displays the configuration of the connection between the device and an AgileConnect system.

Format

display m2m-gateway configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the configuration of the connection between an energy efficiency gateway and a AgileConnect system.

```
<Huawei> display m2m-gateway configuration
[M2M Gateway Configuration]:
 Server IP       : 192.168.1.200
 Server Port     : 7001
 ServerBakIP     : 0.0.0.0
 DHCP            : off
 Local IP        : 0.0.0.0
 Local Netmask   : 0.0.0.0
 Local Gateway   : 0.0.0.0
 DNS             : 0.0.0.0
```

Table 15-2 Description of the **display m2m-gateway configuration** command output

Item	Description
M2M Gateway Configuration	Configuration of the connection between an energy efficiency gateway and an AgileConnect.
Server IP	IP address of the AgileConnect system connected to the energy efficiency gateway. To configure the IP address, run the **15.29 hes-server** command.
Server Port	Port number of the AgileConnect system connected to the energy efficiency gateway. To configure the IP address, run the **15.29 hes-server** command.
ServerBakIP	Backup IP address of the AgileConnect system connected to the energy efficiency gateway.
DHCP	DHCP is enabled. **NOTE** Currently, this parameter cannot be configured.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Local IP	Local IP address. **NOTE** Currently, this parameter cannot be configured.
Local Netmask	Local network mask. **NOTE** Currently, this parameter cannot be configured.
Local Gateway	Local gateway IP address. **NOTE** Currently, this parameter cannot be configured.
DNS	IP address of a DNS server. **NOTE** Currently, this parameter cannot be configured.

Related Topics

15.29 hes-server

15.6 display m2m-gateway long-latitude

Function

The **display m2m-gateway long-latitude** command displays the longitude and latitude of the device.

Format

display m2m-gateway long-latitude

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display m2m-gateway long-latitude** command to check whether the longitude and latitude of the device are correct.

Example

Display the longitude and latitude of the device.

```
<Huawei> display m2m-gateway long-latitude
long-latitude config:
longitude: east  129.542144
latitude : south  12.000000
```

Table 15-3 Description of the **display m2m-gateway long-latitude** command output

Item	Description
longitude	Configured longitude. To set the longitude, run the **15.30 longitude-latitude** command.
latitude	Configured latitude. To set the latitude, run the **15.30 longitude-latitude** command.

Related Topics

15.30 longitude-latitude

15.7 display m2m-gateway statistics

Function

The **display m2m-gateway statistics** command displays received and sent packet statistics and rate on the device functioning as an energy efficiency gateway.

Format

display m2m-gateway statistics

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

To check whether the device is busy processing energy efficiency services or to locate a fault, you can run the **display m2m-gateway statistics** command to view packet statistics and rate on the device.

Example

Display packet statistics on the device.

```
<Huawei> display m2m-gateway statistics
 M2M-Gateway Packet Statistics:
  Statistics From Server      : 0
  Statistics To Server        : 17
  Statistics From Zigbee      : 27
  Statistics To Zigbee        : 27

  Statistics failed to Zigbee : 0
  Statistics failed to Server : 0


 M2M-Gateway Packet Rate:
  Rate From Server            : 0
  Rate To Server              : 2
  Rate From Zigbee            : 2
  Rate To Zigbee              : 2
```

Table 15-4 Description of the **display m2m-gateway statistics** command output

Item	Description
M2M-Gateway Packet Statistics	Packet statistics on the device.
Statistics From Server	Statistics about the packets sent from an AgileConnect system to the device.
Statistics To Server	Statistics about the packets sent from the device to an AgileConnect system.
Statistics From Zigbee	Statistics about the packets sent from a smart terminal to the device through a ZigBee channel.
Statistics To Zigbee	Statistics about the packets sent from the device to a smart terminal through a ZigBee channel.
Statistics failed to Zigbee	Statistics about the packets that fail to be sent from the device to an smart terminal through a ZigBee channel.
Statistics failed to Server	Statistics about the packets that fail to be sent from the device to an AgileConnect system.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
M2M-Gateway Packet Rate	Packet rate on the device.
Rate From Server	Rate at which an AgileConnect system sends packets to the device.
Rate To Server	Rate at which the device sends packets to an AgileConnect system.
Rate From Zigbee	Rate at which a smart terminal sends packets to the device through a ZigBee channel.
Rate To Zigbee	Rate at which the device sends packets to a smart terminal through a ZigBee channel.

Related Topics

15.33 reset m2m-gateway statistics

15.8 display m2m-gateway status

Function

The **display m2m-gateway status** command displays the status of the connection between the device and an AgileConnect.

Format

display m2m-gateway status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the IP address and port number of an AgileConnect are configured on the device, you can run the **display m2m-gateway status** command to view the status of the connection between the device and the AgileConnect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the status of the connection between an energy efficiency gateway and an AgileConnect.

```
<Huawei> display m2m-gateway status
[M2MGateway System Version]:
V200R008C20B310

[M2M Gateway Information]:
 Gateway Id        : D6F00052AE468
 Auth Mode         : disabled
 Encrypt Mode      : disabled  NONE
 Upstream Mode     : enabled
 Upstream Max Size : 1024 KB
 Upstream Send Wait: 10 MS
 Connection State  : certified
 Reconnect Flag    : enabled
 Permit Join       : disabled
[SESSION LIST]:
[1] serverIp = 192.168.1.2, socketId = 1, connState = 7
```

Table 15-5 Description of the **display m2m-gateway status** command output

Item	Description
M2MGateway System Version	System software version of an energy efficiency gateway.
M2M Gateway Information	Connection information of the energy efficiency gateway.
Gateway Id	ID of the energy efficiency gateway.
Auth Mode	Whether authentication between the device and AgileConnect is enabled: ● enabled: Authentication between the device and AgileConnect is enabled. ● disabled: Authentication between the device and AgileConnect is disabled. To configure authentication between the device and AgileConnect, run the **15.1 authentication mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Encrypt Mode	Whether Encrypt tunnel between the device and AgileConnect is enabled, and the encrypt type. Encrypt mode: ● enabled: Encrypt tunnel between the device and AgileConnect is enabled. ● disabled: Encrypt tunnel between the device and AgileConnect is disabled. Encrypt type: ● AES256: AES256 encrypt. ● NONE: No encrypt.
Upstream Mode	Whether the uplink buffer of the device is enabled: ● enabled: The uplink buffer of the device is enabled. ● disabled: The uplink buffer of the device is disabled. To configure authentication between the device and AgileConnect, run the **15.39 upstream-cache mode** command.
Upstream Max Size	Size of the uplink buffer. To configure the size of the uplink buffer, run the **15.38 upstream-cache cache-size wait-time** command.
Upstream Send Wait	Interval for sending buffered data. To configure the interval for sending buffered data, run the **15.38 upstream-cache cache-size wait-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Connection State	Status of the connection between the energy efficiency gateway and an AgileConnect: ● init: The connection is initialized. ● disconnected: The connection is torn down. ● connecting: The connection is being set up. ● connected: The two devices have been connected. ● registering: The connection is being registered. ● registered: The connection is successfully registered. ● certified: The connection passes authentication. ● idle: The connection is idle.
Reconnect Flag	Reconnection flag of the energy efficiency gateway: ● enabled: reconnection ● disabled: non-reconnection
Permit Join	Whether authorized network access is enabled: ● enabled: Authorized network access is enabled. ● disabled: Authorized network access is disabled. To configure authorized network access, run the **15.43 zigbee-network permit-join** command.
SESSION LIST	Connection session list. Currently, only one session process is supported.
serverIp	IP address of the AgileConnect connected to the energy efficiency gateway. To configure the IP address, run the **15.29 hes-server** command.
socketId	Socket ID created for the connection between the energy efficiency gateway and an AgileConnect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
connState	Status code of the connection between the energy efficiency gateway and an AgileConnect: • 0: idle, indicating that the connection is idle • 1: init, indicating that the connection is initialized • 2: disconnected, indicating that the connection is torn down • 3: connecting, indicating that the connection is being set up • 4: connected, indicating that the two devices have been connected • 5: registering, indicating that the connection is being registered • 6: registered, indicating that the connection is registered successfully • 7: certified, indicating that the connection passes authentication

Related Topics

15.29 hes-server
15.43 zigbee-network permit-join
15.1 authentication mode
15.39 upstream-cache mode
15.38 upstream-cache cache-size wait-time

15.9 display m2m-gateway task

Function

The **display m2m-gateway task** command displays the local task configuration.

Format

display m2m-gateway task { **list** { **brief** | **detail** } | *task-id* }

Parameters

Parameter	Description	Value
list { **brief** | **detail** }	Displays the local task configuration. ● **brief**: displays brief information about all local tasks. ● **detail**: displays detailed information about all local tasks.	-
task-id	Displays the configuration of the specified local task.	The value is an integer that ranges from 0 to 9999999999999999999.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display m2m-gateway task** command to check whether the local task configuration is correct.

Example

Display brief information about all local tasks.

```
<Huawei> display m2m-gateway task list brief
Index TaskId          TaskName                Status    LastExtTime         SuccCnt    FailCnt
-----------------------------------------------------------------------------------------------------------------------

1     51              yzq201511               RUNNING   2015-11-03 10:14:12   1          0
2     41              AR169-4                 RUNNING   2015-11-03 10:14:13   1          0
3     31              AR169-3                 RUNNING   2015-11-03 10:14:14   1          0
4     20              AR169-2                 RUNNING   2015-11-03 10:14:16   1          0
5     120             AR169-1                 RUNNING   2015-11-03 10:14:17   1          0
-----------------------------------------------------------------------------------------------------------------------

 Task count: 5
```

Table 15-6 Description of the **display m2m-gateway task list brief** command output

Item	Description
Index	Index of the local task list.

Item	Description
TaskId	ID of the local task.
TaskName	Name of the local task.
Status	Status of the local task: ● DELETED: The task has been deleted. ● STOPED: The task has been stopped. ● RUNNING: The task is running. ● UPDATING: The task is being updated. ● READY: The task is ready.
LastExtTime	Last time the local task was executed.
SuccCnt	Number of times the local task was executed successfully.
FailCnt	Number of times the local task failed to be executed.
Task count	Number of local tasks.

Display detailed information about all local tasks.

```
<Huawei> display m2m-gateway task list detail
-------------------------------------------------------------------------------
TaskId          : 7
TaskName        : onlyYou
isBusy          : no
TaskType        : ONCE
 once.dt        : 2015-09-22 21:32:00
TaskNotify      : SimplyNotify
TaskPriority    : 2
Retrycount      : 3
RetryInterval   : 2 (s)
status          : READY
opscount        : 2
 operation  1
   devId        : 2A00216EFC000145
   opType       : getData
   idx          : 0
   delayTime    : 123
   payload      : 0x 03
 operation  2
   devId        : 2A00216EFC000145
   opType       : Control
   idx          : 1
   delayTime    : 300
   payload      : 0x 01 02 02 02
```

Table 15-7 Description of the **display m2m-gateway task list detail** command output

Item	Description
TaskId	ID of the local task.
TaskName	Name of the local task.
isBusy	Whether the local task is being executed: ● yes: The task is being executed. ● no: The task is not executed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TaskType	Type of the local task: ● ONCE: The local task is executed at one time. ● MINUTE: The local task is executed at an interval that is expressed in minutes within the specified time range. ● DAILY: The local task is executed at an interval that is expressed in days within the specified time range. ● W_D: The local task is executed in one or more days by week within the specified time range. For example, the local task is executed on Monday and Wednesday every two weeks. ● M_D: The local task is executed at the specified month and date within the specified time range. For example, the local task is executed on March 25. ● M_W_D: The local task is executed at the specified month, week, and day within the specified time range. For example, the local task is executed on Wednesday of the third week in March. ● LON_LAT_DAILY: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed by day within the specified time range. ● LON_LAT_W_D: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed in one or more days by week within the specified time range. ● LON_LAT_M_D: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed at the specified month and date within the specified time range. ● LON_LAT_M_W_D: The local task of calculating the sunrise and sunset

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	times based on the longitude and latitude is executed at the specified month, week, and day within the specified time range.
once.dt	Time the local task is executed. The parameter is available only when the value of **TaskType** is **ONCE**.
TaskNotify	Mode in which the local task execution result is notified. The value can be only **NoNotify**, indicating that the local task execution result is not notified.
TaskPriority	Priority of the local task. The value ranges from 0 to 10. A larger value indicates a higher priority of a local task.
Retrycount	Retry count after the local task fails to be executed.
RetryInterval	Retry interval after the local task fails to be executed.
status	Status of the local task: ● DELETED: The task has been deleted. ● STOPED: The task has been stopped. ● RUNNING: The task is running. ● UPDATING: The task is being updated. ● READY: The task is ready.
opscount	Number of operations in the local task.
operation N	Information about the executed *n*th operation in the local task.
devId	ID of the smart terminal on which the operation is performed.
opType	Operation type.
idx	Operation execution sequence.
delayTime	Delay between the current and next operations.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
payload	Operation payload.

Display the configuration of task 1.

```
<Huawei> display m2m-gateway task 1
--------------------------------------------------------------------------------
TaskId : 1
TaskName : month
isBusy : no
TaskType : MINITE
startDt : 2016-11-25 09:10:40
endDt : 2017-12-31 12:01:01
interval : 120 (s)
TaskNotify : NoNotify
TaskPriority : 1
Retrycount : 3
RetryInterval : 1000 (s)
status : RUNNING
opscount : 1
operation 1
devId : 2A006124A6000146
opType : Control
idx : 0
delayTime : 1000
payload : 0x 01 02 02 02
```

Table 15-8 Description of the **display m2m-gateway task** *task-id* command output

Item	Description
TaskId	ID of the local task.
TaskName	Name of the local task.
isBusy	Whether the local task is being executed: ● yes: The task is being executed. ● no: The task is not executed.

Item	Description
TaskType	Type of the local task: ● ONCE: The local task is executed at one time. ● MINUTE: The local task is executed at an interval that is expressed in minutes within the specified time range. ● DAILY: The local task is executed at an interval that is expressed in days within the specified time range. ● W_D: The local task is executed in one or more days by week within the specified time range. For example, the local task is executed on Monday and Wednesday every two weeks. ● M_D: The local task is executed at the specified month and date within the specified time range. For example, the local task is executed on March 25. ● M_W_D: The local task is executed at the specified month, week, and day within the specified time range. For example, the local task is executed on Wednesday of the third week in March. ● LON_LAT_DAILY: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed by day within the specified time range. ● LON_LAT_W_D: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed in one or more days by week within the specified time range. ● LON_LAT_M_D: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed at the specified month and date within the specified time range. ● LON_LAT_M_W_D: The local task of calculating the sunrise and sunset

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	times based on the longitude and latitude is executed at the specified month, week, and day within the specified time range.
startDt	Scheduled start time of the local task. The parameter is available only when the value of **TaskType** is not **ONCE**.
endDt	Scheduled end time of the local task. The parameter is available only when the value of **TaskType** is not **ONCE**.
execT	Time the local task is executed. The parameter is available only when the value of **TaskType** is not **ONCE**.
interval	Interval at which the local task is executed. The parameter is available only when the value of **TaskType** is not **ONCE**.
TaskNotify	Mode in which the local task execution result is notified. The value can be only **NoNotify**, indicating that the local task execution result is not notified.
TaskPriority	Priority of the local task. The value ranges from 0 to 10. A larger value indicates a higher priority of a local task.
Retrycount	Retry count after the local task fails to be executed.
RetryInterval	Retry interval after the local task fails to be executed.
status	Status of the local task: ● DELETED: The task has been deleted. ● STOPED: The task has been stopped. ● RUNNING: The task is running. ● UPDATING: The task is being updated. ● READY: The task is ready.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
opscount	Number of operations in the local task.
operation N	Information about the executed *n*th operation in the local task.
devId	ID of the smart terminal on which the operation is performed.
opType	Operation type.
idx	Operation execution sequence.
delayTime	Delay between the current and next operations.
payload	Operation payload.

Related Topics

15.36 task update task-name

15.10 display m2m-gateway task list group-task

Function

The **display m2m-gateway task list group-task** command displays the list of all conflicting tasks of the current day.

Format

display m2m-gateway task list group-task

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check the list of all conflicting tasks of the current day, including the task ID, ID of the smart terminal for which the task is executed, and group that the task belongs to.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the list of all conflicting tasks of the current day.

```
<Huawei> display m2m-gateway task list group-task
-----------------------------------------------------------------------
Task Group Id: 0
   Device Id: 0X1300B136CB000485
     Task Id: 3
     Task Id: 6
   Device Id: 0X1300B136CB000632
     Task Id: 3
     Task Id: 8
-----------------------------------------------------------------------
```

Table 15-9 Description of the **display m2m-gateway task list group-task** command output

Item	Description
Task Group Id	ID of the group that the conflicting task belongs to.
Device Id	ID of the smart terminal for which the conflicting task is executed.
Task Id	ID of the conflicting task.

15.11 display m2m-gateway task list optimal-task

Function

The **display m2m-gateway task list optimal-task** command displays the list of optimal tasks of the current day.

Format

display m2m-gateway task list optimal-task

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Among conflicting tasks of the current day, the task with the highest priority is the optimal task. You can run this command to check the list of optimal tasks of the

current day, including the task ID, ID of the smart terminal for which the task is executed, and group that the task belongs to.

Example

Display the task of optimal tasks of the current day.

```
<Huawei> display m2m-gateway task list optimal-task
-----------------------------------------------------------------------
Task Group Id: 0
   Device Id: 0X1300B136CB000485      Optimal Task Id: 9
   Device Id: 0X1300B136CB000632      Optimal Task Id: 9
```

Table 15-10 Description of the **display m2m-gateway task list optimal-task** command output

Item	Description
Task Group Id	ID of the group that the optimal task belongs to.
Device Id	ID of the smart terminal for which the optimal task is executed.
Task Id	ID of the optimal task.

15.12 display m2m-gateway task list statistics

Function

The **display m2m-gateway task list statistics** command displays statistics on local tasks.

Format

display m2m-gateway task list statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics on local tasks, including the number of created tasks and numbers of various scheduled tasks.

Example

Display statistics on local tasks.

```
<Huawei> display m2m-gateway task list statistics
 M2M-Gateway Task List Statistics:
  MaxLimit TaskCnt                          : 2096
  Total TaskCnt                             : 2
  Once PlanCnt                              : 0
  Minute PlanCnt                            : 0
  Daily PlanCnt                             : 2
  Week Day PlanCnt                          : 0
  Month Day PlanCnt                         : 0
  Month Week Day PlanCnt                    : 0
  Mutual Exclusion Daily PlanCnt            : 0
  Mutual Exclusion Week Day PlanCnt         : 0
  Mutual Exclusion Month Day PlanCnt        : 0
  Mutual Exclusion Month Week Day PlanCnt   : 0
  Longitude Latitude Day PlanCnt            : 0
  Longitude Latitude Week Day PlanCnt       : 0
  Longitude Latitude Month Day PlanCnt      : 0
  Longitude Latitude Month Week Day PlanCnt : 0
```

Table 15-11 Description of the **display m2m-gateway task list statistics** command output

Item	Description
M2M-Gateway Task List Statistics	Statistics on local tasks.
MaxLimit TaskCnt	Number of local tasks that can be created.
Total TaskCnt	Number of local tasks.
Once PlanCnt	Number of one-time tasks.
Minute PlanCnt	Number of scheduled tasks by minute.
Daily PlanCnt	Number of scheduled tasks by day.
Week Day PlanCnt	Number of scheduled tasks by day and week.
Month Day PlanCnt	Number of scheduled tasks by day and month.
Month Week Day PlanCnt	Number of scheduled tasks by day, week, and month.
Mutual Exclusion Daily PlanCnt	Number of conflicting scheduled tasks by day.
Mutual Exclusion Week Day PlanCnt	Number of conflicting scheduled tasks by day and week.
Mutual Exclusion Month Day PlanCnt	Number of conflicting scheduled tasks by day and month.
Mutual Exclusion Month Week Day PlanCnt	Number of conflicting scheduled tasks by day, week, and month.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Longitude Latitude Day PlanCnt	Number of LON_LAT_DAILY tasks. LON_LAT_DAILY: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed by day within the specified time range.
Longitude Latitude Week Day PlanCnt	Number of LON_LAT_W_D tasks. LON_LAT_W_D: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed in one or more days by week within the specified time range.
Longitude Latitude Month Day PlanCnt	Number of LON_LAT_M_D tasks. LON_LAT_M_D: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed at the specified month or date within the specified time range.
Longitude Latitude Month Week Day PlanCnt	Number of LON_LAT_M_W_D tasks. LON_LAT_M_W_D: The local task of calculating the sunrise and sunset times based on the longitude and latitude is executed at the specified month, week, or day within the specified time range.

Related Topics

15.9 display m2m-gateway task

15.13 display m2m-gateway task schedule

Function

The **display m2m-gateway task schedule** command displays scheduling information about local tasks.

Format

display m2m-gateway task schedule

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Each day is represented by 24 points and each point represents one hour; one hour is represented by 30 points and each point represents 120s. When you run the **display m2m-gateway task schedule** command to check scheduling information about local tasks, if the value of a point is 1, tasks need to be executed within the specified period. If the value of a point is 0, tasks do not need to be executed within the specified period.

Example

Display scheduling information about local tasks.

```
<Huawei> display m2m-gateway task schedule
--------------------------------------------------------------------------------
startDt         : 2015-10-22 19:38:02
curDt           : 2015-10-23 00:00:10
curHourProgress : 11
curMinProgress  : 0
HOUR POINTS: as follow(0x):
0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
MINUTE POINTS: as follow
00:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
01:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
02:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
03:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
04:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
05:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
06:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
07:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
08:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
09:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
10:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
11:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
12:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
13:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
14:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
15:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
16:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
17:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
18:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
19:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
20:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
21:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
22:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
23:00 | 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
--------------------------------------------------------------------------------
```

Table 15-12 Description of the **display m2m-gateway task schedule** command output

Item	Description
startDt	First time the task scheduling table was generated in the system.
curDt	First time the task scheduling table was generated in the current day.
curHourProgress	Point corresponding to the hour in the current time.
curMinProgress	Point corresponding to the minute in the current time.
HOUR POINTS: as follow(0x)	Whether tasks need to be executed in each hour of a day. The value 1 indicates that tasks need to be executed, and the value 0 indicates that tasks do not need to be executed. The first time on the left is 00:00, the second time is 01:00, and so on.
MINUTE POINTS: as follow	Whether tasks need to be executed at every 120s in each hour of a day. The value 1 indicates that tasks need to be executed, and the value 0 indicates that tasks do not need to be executed. The first time range on the left is 00:00-01:59, the second time is 02:00-03:59, and so on.

Related Topics

15.9 display m2m-gateway task

15.14 display m2m-gateway tsvr-server status

Function

The **display m2m-gateway tsvr-server status** command displays the status of all smart terminals on the network.

Format

display m2m-gateway tsvr-server status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check the status of smart terminals on the network, including their IDs, IP addresses, and port numbers, run this command.

Example

Display the status of smart terminals on the network.

```
<Huawei> display m2m-gateway tsvr-server status
[M2M Gateway Tsvr server status]:
 Tsvr Server Flag   : enable
 Tsvr Encrypt Mode  : enable
 Tsvr Server IP     : 10.138.138.201
 Tsvr Server Port   : 7001
 Tsvr Server Socket : 1
[SESSION LIST]:
[1] clientId = 8900000000000093, clientIp = 10.138.138.168, clientPort = 30204, socketId = 3,upflow = 54 B,
downflow = 27 B
```

Table 15-13 Description of the **display m2m-gateway tsvr-server status** command output

Item	Description
[M2M Gateway Tsvr server status]	Status of the device that functions as a TSVR server.
Tsvr Server Flag	Whether to enable TSVR. ● enable: TSVR is enabled. ● disable: TSVR is not enabled.
Tsvr Encrypt Mode	Whether to enable authentication between the device and smart terminals. ● enabled: Authentication between the device and smart terminals is enabled. ● disabled: Authentication between the device and AgileConnect is not enabled.
Tsvr Server IP	IP address of the TSVR server.
Tsvr Server Port	Port number of the TSVR server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Tsvr Server Socket	Socket used by the device to communicate with smart terminals through Ethernet.
[SESSION LIST]	Session list.
clientId	ID of the smart terminal.
clientIp	IP address of the smart terminal, which is used for communication with the device.
clientPort	Port number of the smart terminal, which is used for communication with the device.
socketId	Socket ID.
upflow	Volume of uplink traffic, which is transmitted from the smart terminal to the device.
downflow	Volume of downlink traffic, which is transmitted from the device to the smart terminal.

15.15 display m2m-gateway timer-join-network

Function

The **display m2m-gateway timer-join-network** command displays the configuration of scheduled authorized network access.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

display m2m-gateway timer-join-network

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After scheduled authorized network access is enabled, you can run this command to check the configuration.

Example

Display the configuration of scheduled authorized network access.

```
<Huawei> display m2m-gateway timer-join-network
TimerJoinNetwork config
timer : 12:12:12
time  : 240
status: enable
LastExecTime : 2015-09-27 12:44:02
```

Table 15-14 Description of the **display m2m-gateway timer-join-network** command output

Item	Description
timer	Time of scheduled authorized network access. To set the time of scheduled authorized network access, run the **15.46 zigbee-network timer-join-network** command.
time	Time range of scheduled authorized network access. To set the time range of scheduled authorized network access, run the **15.46 zigbee-network timer-join-network** command.
status	Scheduled authorized network access status: ● enable: Scheduled authorized network access is enabled. ● disable: Scheduled authorized network access is disabled.
LastExecTime	Last time scheduled authorized network access was enabled.

Related Topics

15.47 zigbee-network timer-join-network enable

15.46 zigbee-network timer-join-network

 Copyright © Huawei Technologies Co., Ltd.

15.16 display m2m-gateway upgrade current

Function

The **display m2m-gateway upgrade current** command displays information about remote upgrade tasks.

Format

display m2m-gateway upgrade current

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the AgileConnect to remotely upgrade smart terminals and run this command to check information about remote upgrade tasks, including the upgrade task status, upgrade file version, smart terminal ID, and upgrade progress.

Example

Display information about remote upgrade tasks.

```
<Huawei> display m2m-gateway upgrade current
-----------------------------------------------------------------------------------------------
UpgradeID : 31
UpgradeStatus : Finish
UpgradeVersion : 0x270a0133
DeviceID : 2E00216EFC000222 PercentProcess : 100 Result : STOP
-----------------------------------------------------------------------------------------------
UpgradeTask count: 1
-----------------------------------------------------------------------------------------------
```

Table 15-15 Description of the **display m2m-gateway upgrade current** command output

Item	Description
UpgradeID	ID of the upgrade task.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
UpgradeStatus	Upgrade status: ● Running: Smart terminals are being upgraded. ● Stop: The upgrade is terminated. ● Finish: The upgrade is successful. ● None: No smart terminal is upgraded.
UpgradeVersion	Version of the upgrade file.
DeviceID	ID of the smart terminal.
PercentProcess	Upgrade progress. The value ranges from 0 to 100.
Result	Upgrade result: ● NOT: No smart terminal is upgraded. ● RECIVECMD: Upgrade instructions are received. ● UPGRADING: Smart terminals are being upgraded. ● STOP: The upgrade is terminated. ● SUCCESS: The upgrade is successful. ● UNKNOW: The upgrade status is unknown.
UpgradeTask count	Number of upgrade tasks.

15.17 display m2m-gateway upstream communication style

Function

The **display m2m-gateway upstream communication style** command displays the type of communication between the device and AgileConnect.

Format

display m2m-gateway upstream communication style

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the uplink communication type of the device that processes energy efficiency services.

Example

Display the type of communication between the device and AgileConnect.

```
<Huawei> display m2m-gateway upstream communication style
Upstream communication style: none
```

Table 15-16 Description of the **display m2m-gateway upstream communication style** command output

Item	Description
Upstream communication style	Type of communication between the device serving as an energy efficiency gateway and the AgileConnect, which includes: ● none: The device is not connected to the AgileConnect. ● 3g-or-lte: The device communicates with the AgileConnect through 3G or LTE links. ● ethernet: The device communicates with the AgileConnect through Ethernet links.

15.18 display m2m-gateway upstream statistics

Function

The **display m2m-gateway upstream statistics** command displays statistics on traffic between the device and AgileConnect.

Format

display m2m-gateway upsteam { all | year | month | date } statistics

Parameters

Parameter	Description	Value
upsteam { all | year | month | date }	Specifies the time mode for collecting statistics on uplink traffic. **all** indicates statistics on all traffic, **year** indicates statistics on uplink traffic by year, **month** indicates statistics on uplink traffic by month, and **date** indicates statistics on uplink traffic by date.	_

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check statistics on uplink traffic of energy efficiency services processed by the device and the specified threshold.

Example

Display traffic statistics on the device.

```
<Huawei> display m2m-gateway upstream month statistics
 M2M-Gateway Upstream Flow Statistics:
  Month statistic      :
     Threshold        :      30000 KB
     2017-04          :   10405336 KB
     2017-03          :          0 KB
     2017-02          :          0 KB
     2017-01          :          0 KB
     2016-12          :          0 KB
     2016-11          :          0 KB
     2016-10          :          0 KB
     2016-09          :          0 KB
     2016-08          :          0 KB
     2016-07          :          0 KB
     2016-06          :          0 KB
     2016-05          :          0 KB
```

Table 15-17 Description of the **display m2m-gateway upstream statistics** command output

Item	Description
M2M-Gateway Upstream Flow Statistics	Statistics on uplink traffic of the energy efficiency gateway.
Month statistic	Traffic statistics by month.
Threshold	Monthly traffic threshold.
2017-04 : 10405336 KB	Month for which traffic statistics are collected and traffic volume (in KB).

Related Topics

15.33 reset m2m-gateway statistics

15.19 display m2m-gateway whitelist

Function

The **display m2m-gateway whitelist** command displays whitelist information.

Format

display m2m-gateway whitelist

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After smart terminals are added to a whitelist, you can run this command to check the smart terminal list in the whitelist.

Example

Display whitelist information.

```
<Huawei> display m2m-gateway whitelist
 WhiteList
```

```
-----------------------------------------------------------------------------
Index Device Type      Mac     DeviceId          Status
-----------------------------------------------------------------------------
1     HWSS           0x0000  1300B136CB000486    NotJoin
2     HWWS2           0xf753  240013917F300641    Online
3     HWMVRDC          0x0f70  2B0012F111000181    Online
4     HWSS           0x6ab4  1300B136CB000725    Online
5     HWSS           0x0000  1300B136CB000455    NotJoin
6     HWSS           0x716b  1300B136CB000475    Online
7     HWSS           0xb752  1300B136CB000485    Online
8     HWTLS32A         0x0000  0700B136CB001481    Offline
9     HWWS2           0x0000  240013917F303046    NotJoin
10    HWOD            0x5610  01001E71EE000091    Online
11    HWIRR           0x0000  280012F111000197    NotJoin
12    HWWS2           0x1771  240013917F300690    Online
13    HWBMCD           0x0000  260013917F304620    Offline
14    HWWS2           0xde67  240013917F302902    Online
-----------------------------------------------------------------------------
Online count: 8                Total count: 14
```

Table 15-18 Description of the **display m2m-gateway whitelist** command output

Item	Description
Whitelist	Whitelist that contains smart terminals.
Index	Index of the smart terminal in the whitelist.
Device Type	Type of the smart terminal in the whitelist.
Mac	MAC address of the smart terminal in the whitelist.
DeviceId	ID of the smart terminal in the whitelist. To add smart terminals to a whitelist, run the **15.44 zigbee-network permit-join whitelist** command.
Status	Status of the smart terminal in the whitelist: • Online: The smart terminal is online. • Offline: The smart terminal is offline. • NotJoin: The smart terminal is not connected to the network.
Online count	Number of online smart terminals in the whitelist.
Total count	Number of smart terminals in the whitelist.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

15.44 zigbee-network permit-join whitelist

15.20 display firmware process

Function

The **display firmware process** command displays the upgrade process of a smart terminal

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

display firmware process { *mac-address* | **hwarc** | **hwbmcd** | **hwdgcp** | **hwgem** | **hwirr** | **hwmvrdc** | **hwod** | **hwscd** | **hwsgcp** | **hwss** | **hwtc** | **hwths** | **hwtls32a** | **others** }

Parameters

Parameter	Description	Value
mac-address	Displays the upgrade process of a smart terminal with the specified MAC address.	The value is a hexadecimal integer that ranges from 0x1 to 0xFFFF.
hwarc	Displays the upgrade process of the air refresh controller.	-
hwbmcd	Displays the upgrade process of the brightness movement combo detector.	-
hwdgcp	Displays the upgrade process of the two-way switch.	-
hwgem	Displays the upgrade process of the general expansion module.	-
hwirr	Displays the upgrade process of the IR repeater.	-
hwmvrdc	Displays the upgrade process of the MVRD controller.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwod	Displays the upgrade process of the object detector.	-
hwscd	Displays the upgrade process of the single-controlled dimmer.	-
hwsgcp	Displays the upgrade process of the one-way switch.	-
hwss	Displays the upgrade process of the smart socket.	-
hwths	Displays the upgrade process of the temperature and humidity sensor.	-
hwtc	Displays the upgrade process of the traffic counter.	-
hwtls32a	Displays the upgrade process of the three-phase load switch (32 A).	-
others	Displays the upgrade process of other terminals.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the upgrade process of a smart terminal with the MAC address of 0x1234.

```
<Huawei> display firmware process 0x1234
Info: Upgrade FJ sta process 100% mac 0x1234

Info: Upgrade FJ sta mac 0x1234 complete!
```

Related Topics

15.24 firmware upgrade channel-type zigbee remote
15.27 firmware upgrade stop

15.21 display zigbee link-key-using

Function

The **display zigbee link-key-using** command displays the key for communication between the device and smart terminals.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

display zigbee link-key-using

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the key for communication between the device and smart terminals.

```
<Huawei> display zigbee link-key-using
current zigbee link-key type: Huawei
```

 Copyright © Huawei Technologies Co., Ltd.

Table 15-19 Description of the **display zigbee link-key-using** command output

Item	Description
current zigbee link-key type	Key for communication between the device and smart terminals, which can be **Huawei**, **Silabs Default**, or **Custom**. To configure the key for communication between the device and smart terminals, run the **15.3 authentication zigbee link-key** command.

Related Topics

15.3 authentication zigbee link-key

15.22 encrypt mode disable

Function

The **encrypt mode disable** command disables encryption of the tunnel between an AR and a AgileConnect.

By default, encryption of a tunnel is enabled.

Format

encrypt mode disable

Parameters

None

Views

m2m-gateway view

Default Level

3: Management level

Usage Guidelines

You can run the command to disable encryption of the tunnel between a gateway and the AgileConnect.

Example

Disable encryption of the tunnel between a gateway and the AgileConnect.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] encrypt mode disable
Info: Set Encryption Mode Disable Successfully!
```

15.23 encrypt type

Function

The **encrypt type** command specifies the encryption type of the communication between a gateway and the AgileConnect.

Format

encrypt type *type-name*

Parameters

Parameter	Description
type-name	

Views

m2m-gateway

Default Level

3: Management level

Usage Guidelines

Encryption is enabled on the tunnel between a gateway and the AgileConnect to protect data against theft. Currently only the AES256 encryption algorithm is supported.

Example

Set the encryption type of the communication between a gateway and the AgileConnect to AES256.

```
<Huawei> system
[Huawei] m2m-gateway
[Huawei-m2m-gateway] encrypt type aes256
Info: Set Encryption Type AES256 Successfully!
```

15.24 firmware upgrade channel-type zigbee remote

Function

The **firmware upgrade channel-type zigbee remote** command upgrades the remote smart terminal on the ZigBee network.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

firmware upgrade channel-type zigbee remote { **all** | *mac-address* } { **hwarc** | **hwbmcd** | **hwdgcp** | **hwgem** | **hwirr** | **hwmvrdc** | **hwod** | **hwscd** | **hwsgcp** | **hwss** | **hwtc** | **hwths** | **hwtls32a** | **others** } *file-name*

firmware upgrade channel-type zigbee remote *mac-address* &<1-10> { **hwarc** | **hwbmcd** | **hwdgcp** | **hwgem** | **hwirr** | **hwmvrdc** | **hwod** | **hwscd** | **hwsgcp** | **hwss** | **hwtc** | **hwths** | **hwtls32a** | **others** } *file-name*

Parameters

Parameter	Description	Value
all	Indicates all remote smart terminals.	-
mac-address	Specifies the MAC address of the remote smart terminal.	The value is a hexadecimal integer that ranges from 0x1 to 0xFFFF.
hwarc	Specifies the air refresh controller to be upgraded.	-
hwbmcd	Specifies the brightness movement combo detector to be upgraded.	-
hwdgcp	Specifies the two-way switch to be upgraded.	-
hwgem	Specifies the general expansion module to be upgraded.	-
hwirr	Specifies the IR repeater to be upgraded.	-
hwmvrdc	Specifies the MVRD controller to be upgraded.	-
hwod	Specifies the object detector to be upgraded.	-
hwscd	Specifies the single-controlled dimmer to be upgraded.	-
hwsgcp	Specifies the one-way switch to be upgraded.	-
hwss	Specifies the smart socket to be upgraded.	-
hwths	Specifies the temperature and humidity sensor to be upgraded.	-
hwtc	Specifies the traffic counter to be upgraded.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwtls32a	Specifies the three-phase load switch (32 A) to be upgraded.	-
others	Specifies another terminal to be upgraded.	-
file-name	Specifies the name of the software to be upgraded.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the version of the smart terminal is different from the version of the ZigBee subcard version on the device or needs to be upgraded, run this command.

Example

Upgrade the traffic counter with the MAC address of 0x1234 through the upgrade software V270A0115T0126.ota.

```
<Huawei> system-view
[Huawei] firmware upgrade channel-type zigbee remote 0x1234 hwtc V270A0115T0126.ota
Info: The succesfully upgraded device will reboot to make the upgrade take effect. Continue?[y/n]: y
Info: Do not power off or reboot the device during the upgrade in case of an unexpected
failure!

Info: Wait a moment while upgrading! Upgrade state 2
```

Related Topics

15.20 display firmware process

15.27 firmware upgrade stop

15.25 firmware upgrade channel-type zigbee local

Function

The **firmware upgrade channel-type zigbee local** command upgrades the ZigBee daughter card on the device.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

firmware upgrade channel-type zigbee local zigbee-ebl [*file-name*]

Parameters

Parameter	Description	Value
zigbee-ebl	The upgrade file of ZigBee daughter card.	-
file-name	Specifies the upgrade file name.	The value is a string of 1 to 64 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the ZigBee daughter card version on the device needs to be upgraded or does not match the version of Fenjin smart switches, you can use the **firmware upgrade channel-type** command.

Example

Upgrade the ZigBee daughter card version on the device.

```
<Huawei> system-view
[Huawei] firmware upgrade channel-type zigbee local zigbee-ebl
Info: The succesfully upgraded device will reboot to make the upgrade take effect. Continue?[y/n]: y
Info: Do not power off or reboot the device during the upgrade in case of an unexpected failure!

INFO: reading upg file...
```

15.26 firmware upgrade channel-type zigbee erase flash

Function

The **firmware upgrade channel-type zigbee erase flash** command erases the flash memory of smart terminals.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

firmware upgrade channel-type zigbee { **all** | **hwarc** | **hwbmcd** | **hwcc** | **hwdgcp** | **hwgem** | **hwirr** | **hwmvrdc** | **hwod** | **hwscd** | **hwsgcp** | **hwslc** | **hwss** | **hwtc** | **hwths** | **hwtls32a** | **others** | *mac-address* } **erase flash**

Parameters

Parameter	Description	Value
all	Erases the flash memory of smart terminals.	-
hwarc	Erases the flash memory of the fresh air controller.	-
hwbmcd	Erases the flash memory of the brightness movement combo detector.	-
hwcc	Erases the flash memory of the curtain controller.	-
hwdgcp	Erases the flash memory of the two-way switch.	-
hwgem	Erases the flash memory of the general expansion module.	-
hwirr	Erases the flash memory of the infrared controller.	-
hwmvrdc	Erases the flash memory of the ducted type air conditioner controller.	-
hwod	Erases the flash memory of the object detector.	-
hwscd	Erases the flash memory of the single-controller dimmer.	-
hwsgcp	Erases the flash memory of the one-way switch.	-
hwslc	Erases the flash memory of the street lamp controller.	-
hwss	Erases the flash memory of the smart socket.	-
hwtc	Erases the flash memory of the traffic counter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwths	Erases the flash memory of the temperature and humidity sensor.	-
hwtls32a	Erases the flash memory of the three-phase load switch (32A).	-
others	Erases the flash memory of other smart terminals.	-
mac-address	Erases the flash memory of a smart terminal with the specified MAC address.	The value is a 4-digit hexadecimal number ranging from 0x0001 to 0xFFFF.

Views

System view

Default Level

3: Management level

Usage Guidelines

The upgrade of a smart terminal may be stopped and failed due to causes such as network faults. When the smart terminal is required to be upgraded to another target version, it is recommended that the flash memory of the smart terminal be erased to delete remaining files due to upgrade failure. If the smart terminal is required to be upgraded to the original target version, this command is not required.

Example

Erase the flash memory of the smart socket.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] firmware upgrade channel-type zigbee hwss erase flash
Device 0x8635 erase flash success
```

15.27 firmware upgrade stop

Function

The **firmware upgrade stop** command stops the upgrade processes of all Fenjin smart switches.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

firmware upgrade stop

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When you find that the target version is incorrect after you run the **15.24 firmware upgrade channel-type zigbee remote** command to upgrade a Fenjin smart switch, you can run the **firmware upgrade stop** command to stop the upgrade process. After the upgrade process is stopped, the Fenjin smart switch uses the source version.

Example

Stop the upgrade processes of all Fenjin smart switches.

```
<Huawei> system-view
[Huawei] firmware upgrade stop
```

Related Topics

15.20 display firmware process

15.24 firmware upgrade channel-type zigbee remote

15.28 hes-bakserver

Function

The **hes-bakserver** command configures the IP address and port number of the standby AgileConnect.

The **undo hes-server** command restores the default IP address and port number of the standby AgileConnect.

By default, the IP address of the standby AgileConnect is not configured and the default port number is 7001.

 Copyright © Huawei Technologies Co., Ltd.

Format

hes-bakserver *ip-address* [**port** *port-num*]

undo hes-bakserver

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the standby AgileConnect.	The value is in dotted decimal notation. The value cannot be 0.0.0.0, or a broadcast or multicast address.
port *port-num*	Specifies the port number of the standby AgileConnect.	The value is an integer that ranges from 1 to 65535.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

You can configure the active and standby AgileConnects. When the device fails to connect to the current AgileConnect, the device will attempt to connect to another AgileConnect. This improves the reliability of the connection between the device and AgileConnect.

Example

Set the IP address and port number of the standby AgileConnect to 10.1.1.10 and 7001, respectively.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] hes-bakserver 10.1.1.10 port 7001
```

Related Topics

15.5 display m2m-gateway configuration

15.29 hes-server

Function

The **hes-server** command configures the IP address and port number of an AgileConnect.

The **undo hes-server** command restores the default settings.

By default, no IP address is configured for an AgileConnect. The default port number is 7001.

Format

hes-server *ip-address* [**port** *port-num*]

undo hes-server

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an AgileConnect.	The value is in dotted decimal notation. The IP address cannot be configured as 0.0.0.0, a broadcast address, or a multicast address.
port *port-num*	Specifies the port number of the AgileConnect.	The value is an integer that ranges from 1 to 65535.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

Before a device connects to an AgileConnect, the device needs to obtain the IP address and port number of the AgileConnect. The two devices can work together to monitor and manage electrical equipment. When the default port number 7001 has been used by another process, you can run the **hes-server** command on the device to configure a new idle port number of the AgileConnect and change the port number configured on the AgileConnect to be the same as that configured on the device.

You can run the **15.8 display m2m-gateway status** command to check whether the device has been connected to the AgileConnect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the IP address and port number of an AgileConnect to 10.1.1.10 and 7002.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] hes-server 10.1.1.10 port 7002
```

Related Topics

15.8 display m2m-gateway status

15.30 longitude-latitude

Function

The **longitude-latitude** command configures the longitude and latitude of the device.

By default, the longitude and latitude of the device are not configured.

Format

longitude-latitude { **longitude** { **east** | **west** } *longitude-value* | **latitude** { **north** | **south** } *latitude-value* }

Parameters

Parameter	Description	Value
longitude { **east** | **west** } *longitude-value*	Specifies the longitude. **east** indicates east longitude, and **west** indicates west longitude.	The value is a floating point number, accurate to the sixth decimal place. The value ranges from 0.000000 to 180.000000.
latitude { **north** | **south** } *latitude-value*	Specifies the latitude. **north** indicates north latitude, and **south** indicates south latitude.	The value is a floating point number, accurate to the sixth decimal place. The value ranges from 0.000000 to 180.000000.

Views

M2M gateway view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After the **longitude-latitude** command is used to configure the longitude and latitude of the device, the upper-layer application can calculate the sunrise and sunset times based on the longitude and latitude of the device and current date. Then policies are configured to control smart terminals based on sunrise and sunset times.

Example

Set the south latitude to 12 degrees and east longitude to 50 degrees for the device.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] longitude-latitude latitude south 12
[Huawei-m2m-gateway] longitude-latitude longitude east 50
```

Related Topics

15.6 display m2m-gateway long-latitude

15.31 m2m-gateway

Function

The **m2m-gateway** command displays the M2M gateway view.

Format

m2m-gateway

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To use functions of an energy efficiency gateway, perform related configurations in the M2M gateway view.

Example

Display the M2M gateway view.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway]
```

15.32 reset m2m-gateway offline-device

Function

The **reset m2m-gateway offline-device** command deletes the statistics about offline devices.

Format

reset m2m-gateway offline-device

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When there are many offline devices, you can run this command to clear the statistics about offline devices to facilitate the query of online device status.

Example

Clear the statistics about offline devices.

```
<Huawei> reset m2m-gateway offline-device
```

15.33 reset m2m-gateway statistics

Function

The **reset m2m-gateway statistics** command clears statistics about the packets received and sent by the device functioning as an energy efficiency gateway.

Format

reset m2m-gateway statistics

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Before collecting statistics about the packets received and sent by the device functioning as an energy efficiency gateway within a certain period, run the **reset m2m-gateway statistics** command to clear existing statistics.

Example

Clear packet statistics.

```
<Huawei> reset m2m-gateway statistics
```

Related Topics

15.7 display m2m-gateway statistics

15.34 restore factory configuration

Function

The **restore factory configuration** command restores factory settings.

After you run this command, the system automatically restarts and the command configuration takes effect.

Format

restore factory configuration type *type_val*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
type *type_val*	Specifies the types of settings to be restored.	The value can be 1 or 2. ● 1: M2M configurations including communication parameters ● 2: M2M configurations excluding communication parameters **NOTE** Communication parameters include the following: ● Bidirectional authentication mode ● Authentication key ● Channel encryption mode ● Channel encryption type ● AgileConnect IP address ● AgileConnect port number ● Backup IP address for communication with the AgileConnect ● Backup port number for communication with the AgileConnect ● DHCP ● Local IP ● Local Netmask ● Local Gateway ● DNS

Views

m2m-gateway view

Default Level

3: Management level

Usage Guidelines

If the M2M settings are incorrect, you can run the **restore factory configuration** command to restore the factory settings. After the command is executed, the device automatically restarts and restores the factory settings.

Table 15-20 Description of M2M factory settings

Item	Description of Factory Setting
Bidirectional authentication mode	Enabled
Authentication key	The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.
Channel encryption mode	Enabled
Channel encryption type	AES256
AgileConnect IP	0
AgileConnect port number	0
Backup IP address for communication with the AgileConnect	0
Backup port number for communication with the AgileConnect	0
DHCP	Off
Local IP	0
Local Netmask	0
Local Gateway	0
DNS	0
Whitelist	Empty
Local task	Empty
The longitude of the device	0
The latitude of the device	0
Scheduled authorized network access	Disabled
Time range of scheduled authorized network access	0
Time of scheduled authorized network access	0

 Copyright © Huawei Technologies Co., Ltd.

Item	Description of Factory Setting
Upstream-cache mode	Enabled
The size of the uplink buffer	256 KB
The interval for sending buffered data to the AgileConnect	10 ms
The key for communication between the device and smart terminals	huawei-key
broadcast-resend-times	0

Example

Restore all M2M factory settings including the communication parameter settings.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] restore factory configuration type 1
Warning: Restore gateway factory configuration then gateway will be reboot and current configuration will be lost. Are you sure to continue?[Y/N]Y
```

Related Topics

15.5 display m2m-gateway configuration

15.8 display m2m-gateway status

15.19 display m2m-gateway whitelist

15.6 display m2m-gateway long-latitude

15.35 task delete

Function

The **task delete** command deletes local tasks on the device.

Format

task delete { *task-id* | **all** }

Parameters

Parameter	Description	Value
task-id	Specifies the ID of a local task.	The value is an integer that ranges from 0 to 9999999999999999999.
all	Deletes all local tasks.	-

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

When the device cannot communicate with the upper-layer application system and cannot delete tasks through the upper-layer application system, run this command on the device to delete local tasks.

Example

Delete local task 102.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] task delete 102
Warning: This task will be deleted. Are you sure to continue?
[Y/N]y
Task delete success
```

Related Topics

15.9 display m2m-gateway task

15.36 task update task-name

Function

The **task update task-name** command changes the name of the local task.

Format

task update *task-id* **task-name** *task-name*

Parameters

Parameter	Description	Value
task-id	Specifies the ID of a local task.	The value is an integer that ranges from 0 to 9999999999999999999.

Parameter	Description	Value
task-name	Specifies the name of a local task.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

When the device cannot communicate with the upper-layer application and tasks cannot be modified through the upper-layer application, run this command on the device to change the name of a specified local task.

After the name of a local task is changed, you can run the **15.9 display m2m-gateway task list brief** command to check whether the name of a local task is successfully changed.

Example

Change the name of local task 102 to **TheDawn**.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] task update 102 task-name TheDawn
```

Related Topics

15.9 display m2m-gateway task

15.37 tsvr-server

Function

The **tsvr-server** command configures parameters for the device that functions as a smart terminal server.

The **undo tsvr-server** command restores the default IP address and port number of the TSVR server.

The **undo tsvr-server encrypt enable** command restores the default encryption mode between the device and smart terminals.

By default, no IP address is configured for the standby TSVR server, the port number is 7001, and encryption is enabled.

Format

tsvr-server { **encrypt enable** | *ip-address* [**port** *port-num*] }

undo tsvr-server [**encrypt enable**]

Parameters

Parameter	Description	Value
encrypt enable	Enables encryption between the device and smart terminals.	-
ip-address	Specifies the IP address of the TSVR server.	The value is in dotted decimal notation. The IP address cannot be set to 0.0.0.0, a broadcast address, or a multicast address.
port *port-num*	Specifies the port number of the TSVR server.	The value is an integer that ranges from 1 to 65535.

Views

M2M gateway view

Default Level

1: Monitoring level

Usage Guidelines

When a smart terminal accesses the device through Ethernet, you need to run this command to set the IP address, port number, and encryption mode for the device that functions as the TSVR server.

You can run the **display m2m-gateway tsvr-server status** command to check the configuration result.

Example

Set the IP address of tsvr-server to **10.1.1.10** and port number to **7002**.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] tsvr-server 10.1.1.10 port 7002
```

Related Topics

15.14 display m2m-gateway tsvr-server status

 Copyright © Huawei Technologies Co., Ltd.

15.38 upstream-cache cache-size wait-time

Function

The **upstream-cache cache-size wait-time** command sets the size of the uplink buffer and the interval for sending buffered data to the AgileConnect.

By default, the size of the uplink buffer is 256 KB and the interval for sending buffered data to the AgileConnect is 10 ms.

Format

upstream-cache cache-size *size* **wait-time** *time*

Parameters

Parameter	Description	Value
size	Specifies the size of the uplink buffer.	The value is an integer that ranges from 256 to 2048, in KB.
time	Specifies the interval for sending buffered data to the AgileConnect.	The value is an integer that ranges from 10 to 1000, in milliseconds.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

After the uplink buffer is enabled, data sent by smart terminals are cached on the device. After a while, the device attempts to send the data to the AgileConnect.

NOTE

After running this command, you need to restart the device to make the configuration take effect.

Example

Set the size of the uplink buffer to 2048 KB and the interval for sending buffered data to the AgileConnect to 100 ms.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] upstream-cache cache-size 2048 wait-time 100
```

```
Info: Set Cache Limited Size And Sended Wait Time Successfully, Reboot To Take
Effect!
```

Related Topics

15.39 upstream-cache mode

15.39 upstream-cache mode

Function

The **upstream-cache mode enable** command enables the uplink buffer.

The **upstream-cache mode disable** command disables the uplink buffer.

By default, the uplink buffer is enabled.

Format

upstream-cache mode { **enable** | **disable** }

Parameters

None

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

When the device constitutes the ZigBee network with smart terminals but does not connect to the AgileConnect, data reported by smart terminals cannot be sent to the AgileConnect. As a result, the data is discarded. After the uplink buffer is enabled, the device can cache data reported by smart terminals. The device sends the buffered data to the AgileConnect after establishing a connection with the AgileConnect.

Example

Enable the uplink buffer.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] upstream-cache mode enable
Info: Set Upstream Cache Mode Enable Successfully!
```

Related Topics

15.38 upstream-cache cache-size wait-time

 Copyright © Huawei Technologies Co., Ltd.

15.40 upstream statistics threshold

Function

The **upstream statistics threshold** command sets a threshold for statistics on upstream traffic between the device that functions as an energy efficiency gateway and the AgileConnect.

Format

upstream { **date** | **month** | **year** } **statistics threshold** *val*

Parameters

Parameter	Description	Value
upstream { **date** | **month** | **year** }	Specifies the time mode for collecting statistics on uplink traffic. **date** indicates traffic statistics by date, **month** indicates traffic statistics by month, and **year** indicates traffic statistics by year.	–
val	Specifies the threshold for statistics on uplink traffic.	The value is an integer that ranges from 0 to 4294967294, in KB.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

You can run this command to set a threshold for statistics on uplink traffic. If the traffic exceeds the threshold, the gateway will report an alarm.

Example

Set the threshold for uplink traffic statistics by month to 30000 KB.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] upstream month  statistics threshold 30000
Info: Set month flow control threshold success!
```

Related Topics

15.18 display m2m-gateway upstream statistics

15.41 zigbee-network dismiss

Function

The **zigbee-network dismiss** command dismisses the smart terminal from a ZigBee network.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

zigbee-network dismiss [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Dismiss the specified smart terminal from the ZigBee network.	The value is a 4-digit hexadecimal number ranging from 0x0000 to 0xFFFF.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

When the device incorrectly joins a ZigBee network, run the **zigbee-network dismiss** *mac-address* command to dismiss the smart terminal from the ZigBee network.

Example

Dismiss the smart terminal from the ZigBee network.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] zigbee-network dismiss
```

Related Topics

15.43 zigbee-network permit-join

 Copyright © Huawei Technologies Co., Ltd.

15.42 zigbee-network get-rssi

Function

The **zigbee-network get-rssi** command configures the device to obtain the RSSI of smart terminals.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

zigbee-network get-rssi { **all** | *mac-address* }

Parameters

Parameter	Description	Value
all	Obtains the RSSI of all smart terminals.	-
mac-address	Obtains the RSSI of a smart terminal with the specified MAC address.	The value is a 4-digit hexadecimal number ranging from 0x0000 to 0xFFFF.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

To obtain the RSSI of the connection between the device and smart terminals, run this command.

Example

Obtain the RSSI of the smart terminal 0x7db8.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] zigbee-network get-rssi 0x7db8
Firmware Version:001
PanId: 0x6325
RadioTxPower: 8
RadioChannel: 20
Zigbee Device-table:
```

```
Index Device Type      Mac     DeviceId          Status  OffReason Version      RSSI
-----------------------------------------------------------------------------------------------
1     HWSS            0x7db8  1300B136CB000485    Online  RepOff    0x270a0110    41
-----------------------------------------------------------------------------------------------
Online count: 1      Total count: 1
```

Table 15-21 Description of the **zigbee-network get-rssi** command output

Item	Description
Firmware Version	EM357 firmware version.
PanId	ZigBee network ID.
RadioTxPower	EM357 transmit power.
RadioChannel	EM357 channel information.
Index	Index of the smart terminal.
Device Type	Type of the smart terminal.
Mac	MAC address of the smart terminal.
DeviceId	ID of the smart terminal.
Status	Whether the smart terminal is connected to the network: ● Online: The smart terminal is connected to the network. ● Offline: The smart terminal is disconnected from the network.
OffReason	Reason why the smart terminal is disconnected from the network last time: ● SrvCtl: The CBEMS controls the network disconnection of the smart terminal. ● Detect: The gateway detects that the smart terminal is disconnected from the network through heartbeat packets. ● RepOff: The gateway receives logout messages reported by the smart terminal and then sets the smart terminal status to offline. ● RepIdChg: The communication address of the smart terminal changes. ● Never: The smart terminal has never been disconnected from the network after being connected to the network.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Version	Version of the smart terminal.
RSSI	RSSI of smart terminals.
Online count	Number of smart terminals connected to the ZigBee network.
Total count	Total number of smart terminals on the ZigBee network.

15.43 zigbee-network permit-join

Function

The **zigbee-network permit-join** command enables ZigBee network access.

The **zigbee-network permit-join** command disables ZigBee network access.

By default, ZigBee network access is disabled.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

zigbee-network permit-join { *time* | **permanent** } [**whitelist**]

undo zigbee-network permit-join

Parameters

Parameter	Description	Value
time	Specifies the ZigBee network access time.	The value is an integer that ranges from 1 to 254, in seconds.
permanent	Sets the ZigBee network access to permanent.	-
whitelist	Specifies that only devices in the whitelist can connect to the ZigBee network. If this parameter is not configured, all devices can connect to the ZigBee network.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

When connected smart devices need to be added to the ZigBee network, run the **zigbee-network permit-join** command to enable ZigBee network access. Then only devices in the whitelist or all smart devices can connect to the ZigBee network in the specified period or at any time.

Example

Enable smart devices in the whitelist to access the ZigBee network for 200 seconds.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] zigbee-network permit-join 200 whitelist
```

Related Topics

15.41 zigbee-network dismiss

15.44 zigbee-network permit-join whitelist

Function

The **zigbee-network permit-join whitelist** command configures a whitelist and adds a specified smart terminal to the whitelist.

The **undo zigbee-network permit-join whitelist** command deletes a smart terminal from a whitelist.

By default, no whitelist is configured on the device.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

zigbee-network permit-join whitelist *device-id* &<1-10>

undo zigbee-network permit-join whitelist [*device-id*] &<1-10>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
device-id	Specifies the ID of a smart terminal. When this parameter is not specified, the **undo zigbee-network permit-join whitelist** command deletes all smart terminals from a whitelist.	The value is in hexadecimal notation and ranges from 0000000000000001 to FFFFFFFFFFFFFFFF.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

After authorized network access is enabled, smart terminals can connect to the ZigBee network. In this case, it is difficult to manage the smart terminals that are connected to the ZigBee network. After the **zigbee-network permit-join whitelist** *device-id* command is used to add a specified smart terminal to a whitelist, only the smart terminal in the whitelist can connect to the ZigBee network. The device can effectively control the smart terminals that are connected to the ZigBee network.

A maximum of 256 smart terminals can be added to a whitelist.

Example

Add the device with the ID of ABCDEF0123456789 to a whitelist.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] zigbee-network permit-join whitelist ABCDEF0123456789
```

Related Topics

15.19 display m2m-gateway whitelist

15.45 zigbee-network status refresh

Function

The **zigbee-network status refresh** command configures the device to upgrade the status of smart terminals.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

zigbee-network status refresh

Parameters

None

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When some smart terminals on the ZigBee network are not online, run this command to update the status of the smart terminals so that they can be triggered to go online again.

Precautions

After this command is executed, the device broadcasts instructions to smart terminals on the ZigBee network. The command execution has a delay.

Example

Configure the device to upgrade the status of smart terminals.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] zigbee-network status refresh
```

15.46 zigbee-network timer-join-network

Function

The **zigbee-network timer-join-network** command sets the time and time range of scheduled authorized network access.

By default, the time and time range of scheduled authorized network access are not configured.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

zigbee-network timer-join-network *timer time*

Parameters

Parameter	Description	Value
timer	Specifies the time of scheduled authorized network access.	The value is in hh:mm:ss format. hh ranges from 0 to 24; mm ranges from 0 to 60; ss ranges from 0 to 60.
time	Specifies the time range of scheduled authorized network access.	The value is an integer that ranges from 1 to 254, in seconds.

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After scheduled authorized network access is enabled, you can run this command to set the time and time range of scheduled authorized network access.

Prerequisites

Scheduled authorized network access has been enabled using the **15.47 zigbee-network timer-join-network enable** command.

Example

Set the time and time range of scheduled authorized network access to 12:12:12 and 200s, respectively.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] zigbee-network timer-join-network enable
[Huawei-m2m-gateway] zigbee-network timer-join-network 12:12:12 200
```

Related Topics

15.47 zigbee-network timer-join-network enable

 Copyright © Huawei Technologies Co., Ltd.

15.15 display m2m-gateway timer-join-network

15.47 zigbee-network timer-join-network enable

Function

The **zigbee-network timer-join-network enable** command enables scheduled authorized network access.

The **undo zigbee-network timer-join-network enable** command disables scheduled authorized network access.

By default, scheduled authorized network access is disabled.

NOTE

Only AR502EGRz-Lc and AR502EGRz-L support this command.

Format

zigbee-network timer-join-network enable

undo zigbee-network timer-join-network enable

Parameters

None

Views

M2M gateway view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a fault on a smart terminal is rectified, the smart terminal can connect to the ZigBee network only when authorized network access is enabled manually. After scheduled authorized network access is enabled, the device automatically enables scheduled authorized network access at the specified time. The smart terminals where faults are rectified can automatically connect to the ZigBee network again with no manual operation, reducing maintenance costs.

Follow-up Procedure

Run the **15.46 zigbee-network timer-join-network** *timer time* command to set the time and time range of scheduled authorized network access.

Example

Enable scheduled authorized network access.

```
<Huawei> system-view
[Huawei] m2m-gateway
[Huawei-m2m-gateway] zigbee-network timer-join-network enable
```

Related Topics

15.46 zigbee-network timer-join-network

15.15 display m2m-gateway timer-join-network

 Copyright © Huawei Technologies Co., Ltd.

16 Voice Commands

About This Chapter

16.1 Voice Configuration Commands
16.2 Voice interface Commands
16.5 PBX Configuration Commands
16.6 SIP AG Commands
16.7 H.248 AG Commands

16.1 Voice Configuration Commands

16.1.1 Basic Voice Configuration Commands

16.1.1.1 debugging voice logserver

Function

Using the **debugging voice logserver** command, you can configure the IP address and port number of the log server, and the local IP address.

Format

debugging voice logserver ip *ip-address* **port** *port* **local-ip** *local-ip*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IP address of the log server.	The value is a string of 1 to 64 characters.
port *port*	Specifies the port number of the log server.	The value is an integer that ranges from 0 to 65535.
local-ip *local-ip*	Specifies the local IP address.	The value is a string of 1 to 64 characters. The local IP address must be in the signaling IP address pool.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

You can use this command to configure an IP address and a port number of the log server, and a local IP address, then use the Wireshark to capture logs.

Example

Configure the IP address and port number of the log server, and the local IP address.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose]debugging voice logserver ip 192.168.1.1 port 2000 local-ip 192.168.1.2
```

16.1.1.2 debugging voice module-name cmd

Function

The **debugging voice module-name cmd** command enables software debugging of each module.

Format

debugging voice module-name cmd *cmd-value* [**p1** *p1-value*] [**p2** *p2-value*] [**p3** p3-value] [**p4** p4-value] [**p5** *p5-value*] [**p6** *p6-value*]

Parameters

Parameter	Description	Value
module-name	Specifies the voice module of the debugging messages.	Enumerated type. The values are as follows: • **at0** • **bill** • **billserver** • **bin** • **ccm** • **conference** • **db** • **dss1** • **error** • **h323** • **innertrace** • **lm** • **ms** • **nm** • **pbxmp** • **pbxomshl** • **r2** • **r2rs** • **rm** • **scm** • **sdb** • **sip** • **sipdlg** • **sipem** • **sipmsg** • **sippa** • **siptk** • **ssm** • **sys** • **tam** • **tbcm** • **tkh** • **tpa** • **trace** • **transfer** • **trc**

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• **uam** • **ucbincli** • **userlocation** • **vcm** • **vpm** • **vrm** • **vsppdt** • **ioee** • **vu**
cmd *cmd-value*	Specifies the command value.	The value is an integer that ranges from 0 to 65535.
p1 *p1-value*	Specifies the value of parameter 1.	The value is an integer that ranges from 0 to 4294967295.
p2 *p2-value*	Specifies the value of parameter 2.	The value is an integer that ranges from 0 to 4294967295.
p3 *p3-value*	Specifies the value of parameter 3.	The value is an integer that ranges from 0 to 4294967295.
p4 *p4-value*	Specifies the value of parameter 4.	The value is an integer that ranges from 0 to 4294967295.
p5 *p5-value*	Specifies the value of parameter 5.	The value is a string of 1 to 64 characters.
p6 *p6-value*	Specifies the value of parameter 6.	The value is a string of 1 to 64 characters.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable software debugging for the CCM module.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] debugging voice ccm cmd 0
```

```
->CCM_DebugFunc: dwDebugCmd = 0, dwPara1 = 4294967295, dwPara2 = 4294967295, dwPara3 =
4294967295, dwPara4 = 4294967295
---------------------- CCM Debug Help ----------------------------------------
  0   : print debug help information .......................command parmeters:[-]

---------------------- CCM Block Debug Help ---------------------------------
  1   : show All CCM control block In Used..................command parameters:[-]
  2   : show content of CCM control block ..................command parameters:[p1:ccm no]

---------------------- CCM Timer Debug Help ---------------------------------
  11  : show timer switch of CCM ...........................command parameters:[-]
  12  : set timer switch of CCM ............................command parameters:[-]
  13  : show timer length of CCM ...........................command parameters:[-]
  14  : set ccm timer length to default ....................command parameters:[-]

---------------------- CCM Newservice Debug Help ----------------------------
  21   : show All ringsevice CB In Used.....................command parameters:[-]
  22   : show info of ringsevice CB ........................command parameters:[p1:ringservice no]
  23   : show PickupGroup Stack Info........................command parameters:[-]

---------------------- CCM Bill Debug Help ----------------------------------
  31   : generate bills.....................................command parameters:[P1:bills number(0-5000) P2-CCM No(0-132)]
  32   : show max number length the bill could display .....command parameters:[-]
  33   : modify max number length the bill could display ...command parameters:[p1:length]
  35   : show diameter info by ccm number...................command parameters:[p1:ccm no]
```

16.1.1.3 debugging voice module-name debug-level-value

Function

The **debugging voice module-name debug-level-value** command enables the debug log function for modules.

The **undo debugging voice module-name** command disables the debug log function for modules.

Format

debugging voice *module-name debug-level-value*

debugging voice msgtrace [**caller** *caller-telno*] *debug-level-value*

undo debugging voice *module-name*

undo debugging voice msgtrace

Parameters

Parameter	Description	Value
module-name	Specifies the voice module of the debugging messages.	Enumerated type. The values are as follows: • **at0** • **bill** • **billserver** • **bin** • **cs** • **ccm** • **conference** • **db** • **dss1** • **error** • **h248dmm** • **h248sp** • **h248pa** • **h323** • **innertrace** • **l2ua** • **lm** • **ms** • **nm** • **pbxmp** • **pbxomshl** • **r2** • **r2rs** • **rm** • **scm** • **sdb** • **sip** • **sipbcm** • **sipcc** • **sipcom** • **sipcp** • **sipdlg** • **sipdmm** • **sipem** • **sipmp** • **sipmpc**

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• **sipmsg** • **sippa** • **sipsl** • **siptk** • **snm** • **ssm** • **sys** • **ioee** • **tam** • **tbcm** • **tkh** • **tpa** • **trace** • **transfer** • **trc** • **uam** • **ucbincli** • **userlocation** • **vcm** • **volc** • **vpm** • **vrm** • **vu**
debug-level-value	Specifies the debug log level.	The value can be **error**, **event**, **trace**, or **all**. • error: error level • event: event level • trace: trace level • all: all levels

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the debug log function for the DSS1 module and set the debug log level to all.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] debugging voice dss1 all
```

16.1.1.4 display voice configuration

Function

Using the **display voice configuration** command, you can view global voice parameters.

Format

display voice configuration

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

View global voice parameters.

```
<Huawei> display voice configuration
  Country                  : China-mainland
  Stop initial ring        : Enable
  MWI mode                 : FSK without ring
  Flash hook upper         : 1000 ms
  Flash hook lower         : 100 ms
  Park feed                : Disable
  PCM                      : a law
  Ring frequency           : 25HZ
  Ring ac amplitude        : 45Vrms
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-1 Description of the **display voice configuration** command output

Item	Description
Country	Region identifier. The following identifiers are supported: ● brazil: Brazil version. ● britain-msfuk: Britain MSFUK version. ● britain-etsi: Britain ESTI version. ● bulgaria: Bulgaria version. ● china-hongkong: China Hongkong version. ● china-mainland: China mainland version. ● egypt: Egypt version. ● france: France version. ● singapore: Singapore version. ● thailand: Thailand version.
Stop initial ring	Stop initial ring
MWI mode	MWI mode
Flash hook upper	Flash hook upper
Flash hook lower	Flash hook lower
Park feed	Park feed
PCM	PCM
Ring frequency	Ring frequency
Ring ac amplitude	Specifies a ringing voltage.

16.1.1.5 display voice debugging

Function

The **display voice debugging** command displays the voice debugging status.

Format

display voice debugging *module-name*

Parameters

Parameter	Description	Value
module-name	Displays debugging messages of the specified voice module.	Enumerated type. The values are as follows: ● at0 ● bill ● billserver ● bin ● ccm ● conference ● db ● dss1 ● h323 ● innertrace ● lm ● ms ● msgtrace ● nm ● pbxmp ● pbxomshl ● r2 ● r2rs ● rm ● scm ● sdb ● sip ● sipdlg ● sipem ● sipmsg ● sippa ● siptk ● ssm ● sys ● tam ● tbcm ● tkh ● tpa ● trace ● transfer ● trc

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• uam • ucbincli • userlocation • vcm • vpm • vrm • vu • all

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

View debugging information about the DSS1 module.

```
<Huawei> display voice debugging dss1
 DSS1  current tracing is disabled.
```

16.1.1.6 display voice diagnostic-information

Function

The **display voice diagnostic-information** command displays the voice diagnostic information.

Format

display voice diagnostic-information

Parameters

None

Views

All view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the voice diagnostic information.

```
<Huawei> display voice diagnostic-information
 ================================================================
  ===============display voice service-mode===============
================================================================
 The voice service mode is PBX.
================================================================
  ===============display voice dsp statistic===============
================================================================
  Slotid/DSP-Index                11/2
  Total                         128
  Idle                          128
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                    0

  Sum of Sub-Board
  Total                         128
  Idle                          128
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                    0
================================================================
  ===============display voice dsp state 11/2===============
================================================================

  Symbol:
     0-idle $-G.711 busy A-All busy W-Wastage X-fault
     @-IP loopback *-PCM loopback #-prohibited

  Channel NO.  DSP channel state
  ---------------------------------------------------------------------
  0000-0049  00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
  0050-0099  00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
  0100-0127  00000 00000 00000 00000 00000 000

  Total:
     128 DSP channel
     128 idle, 0 G.711 Busy, 0 All Busy, 0 Wastage, 0 Fault,
     0   IP loopback, 0 PCM loopback, 0 prohibited
================================================================
```

16.1.1.7 display voice error

Function

The **display voice error** command displays error logs about latest call failures (including the current call).

Format

display voice error

Parameters

None

Views

All view

Default Level

2: Configuration level

Usage Guidelines

When a call fails, run the **display voice error** command to view the error log to rapidly troubleshoot the call failures caused by incorrect configurations.

Example

Display error logs about latest call failures.

```
<Huawei> display voice error
<Huawei> 2016/03/30-14:08:23 AR[N@18][CCM:1]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@53][CCM:2]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
```

16.1.1.8 display voice media-port

Function

The **display voice media-port** command displays the media port number range.

Format

display voice media-port

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the media port number range.

```
<Huawei> display voice media-port
 media-port start 59392 end 62724
```

Table 16-2 Description of the **display voice media-port** command output

Item	Description
media-port start 59392 end 62724	• Start port number • End port number

16.1.1.9 display voice mix-info

Function

The **display voice mix-info** command displays voice mixing information.

Format

display voice mix-info { **port** *slotid*|*dspindex*|*dspchannel* | **dsp** *slotid*|*subcardid*|*portid* }

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display voice mixing information.

```
<Huawei> display voice mix-info port 2/0/0
 media-port start 59392 end 62724
```

Table 16-3 Description of the **display voice mix-info** command output

Item	Description
media-port start 59392 end 62724	• Start port number • End port number

16.1.1.10 display voice online-info

Function

The **display voice online-info** command displays current online user information on the device.

Format

display voice online-info [**callee** *callee-number* | **caller***caller-number*]

Parameters

Parameter	Description	Value
callee *callee-number*	Displays information about called parties.	The value is a string of 1 to 32 characters.
caller *caller-number*	Displays information about calling parties.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display the current online user information on the device.

```
<Huawei> display voice online-info
 Online User Number : 2
 Online Call Information:
 Call type          : INNER
 Caller Service      : NORMAL
 Caller type         : SIPUE
 Caller info         : 214
 Caller DSP          : 0/0/17
```

```
Caller RTP          : 192.168.0.3:62565
Callee Service       : NORMAL
Callee type          : PSTN
Callee info          : 1/0/0
Callee DSP           : -
Callee RTP           : -
Callee CodecType     : G711U
Start time           : 2012-07-16 14:21:58
Call duration (s)    : 0:0:16

Codec                          : G711U
Packetization duration (ms)      : 20
Local IP address: port           : 192.168.0.3:62656
Remote IP address: port          : 192.168.0.1:10002
Total number of Rx RTP bytes     : 756
Total number of Tx RTP bytes     : 120000
Total number of Rx RTP packets   : 756
Total number of Tx RTP packets   : 750
Total number of lost RTP packets : 0
Maximum network jitter (ms)      : 29
Minimum network jitter (ms)      : 17
Maximum loop delay (ms)          : 0
Minimum loop delay (ms)          : 0
Maximum Drop packets Rate (%)    : 0
Minimum Drop packets Rate (%)    : 0
```

Table 16-4 Description of the display voice online-info command output

Item	Description
Online Users Number	Number of online users.
Call type	Call type. For details, see the parameter description in **16.5.1.5 call-type**.
Caller Service	Service type. For details, see the parameter description in **16.5.1.5 call-type**.
Caller type	Caller type.
Caller info	Caller terminal identifier.
Caller DSP	DSP used by the caller terminal.
Caller RTP	IP address and port number in RTP packets received and sent by the calling party.
Callee Service	Service type. For details, see the parameter description in **16.5.1.5 call-type**.
Callee type	Callee type.
Callee info	Callee terminal identifier.
Callee DSP	DSP used by the callee terminal.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Callee RTP	IP address and port number in RTP packets received and sent by the called party.
Callee CodecType	Codec type: ● G711U ● G726 ● G723 ● G711A ● G722 ● G728 ● G729 ● G723Low ● g726-16k ● g726-24k ● g726-32k ● g726-40k ● R2198 ● R2833 ● v150 ● clearmode ● T.38 ● T.38+2
Start time	Start time of a call.
Call duration (s)	Duration in which a call lasts.
Codec	-
Packetization duration (ms)	-
Local IP address: port	Local IP address and port number.
Remote IP address: port	Remote IP address and port number.
Total number of Rx RTP bytes	Total number of bytes received by the local end.
Total number of Tx RTP bytes	Total number of bytes sent by the local end.
Total number of Rx RTP packets	Total number of packets received by the local end.
Total number of Tx RTP packets	Total number of packets sent by the local end.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total number of lost RTP packets	Total number of discarded RTP packets.
Maximum network jitter (ms)	-
Minimum network jitter (ms)	-
Maximum loop delay (ms)	-
Minimum loop delay (ms)	-
Maximum Drop packets Rate (%)	Maximum packet loss ratio.
Minimum Drop packets Rate (%)	Minimum packet loss ratio.

16.1.1.11 display voice run-stat

Function

display voice run-stat command displays running state information of voice module.

Format

display voice run-stat{ **call-info** | **dsp** | **port** | **proxy-rtp** | **rtp** | **user** }

Parameters

Parameter	Description	Value
call-info	Call-relevant port info	-
dsp	State of dsp channel	-
port	State of port	-
proxy-rtp	RTP port info of media proxy	-
rtp	RTP port info	-

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

displays running state information of voice module

```
<Huawei> display voice run-stat call-info
 [DSP statistics]
  Total          DSP channel : 36
  Idle           DSP channel : 33
  Occupy         DSP channel : 1
  Fault          DSP channel : 0
  Waste          DSP channel : 2
  Prohibit       DSP channel : 0
  PCM loopback   DSP channel : 0
  IP loopback    DSP channel : 0

 [RTP port statistics]
  Total  RTP  port : 250
  Idle   RTP  port : 249
  Occupy RTP  port : 1
  Fault  RTP  port : 0

 [PORT statistics]
  Total  port      : 7
  Busy   port      : 0
  Idle   port      : 7
  Fault  port      : 0
  Locked port      : 0
  Other  port      : 0

 [Proxy RTP port statistics]
  Total  RTP  port : 250
  Idle   RTP  port : 250
  Occupy RTP  port : 0
```

Table 16-5 Description of the **display voice run-stat call-info** command output

Item	Description
[DSP statistics]	DSP statistics
Total DSP channel	Total DSP channel number
Idle DSP channel	Idle DSP channel number
Occupy DSP channel	Occupy DSP channel number
Fault DSP channel	Fault DSP channel number
Waste DSP channel	Waste DSP channel number
Prohibit DSP channel	Prohibit DSP channel number
PCM loopback DSP channel	PCM loopback DSP channel number
IP loopback DSP channel	IP loopback DSP channel number
[RTP port statistics]	RTP port statistics
Total RTP port	Total RTP port number

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Idle RTP port	Idle RTP port number
Occupy RTP port	Occupy RTP port number
Fault RTP port	Fault RTP port number
[PORT statistics]	PORT statistics
Total port	Total port number
Busy port	Busy port number
Idle port	Idle port number
Fault port	Fault port number
Locked port	Locked port number
Other port	Other port number
[Proxy RTP port statistics]	Proxy RTP port statistics
Total RTP port	Total RTP port number
Idle RTP port	Idle RTP port number
Occupy RTP port	Occupy RTP port number

16.1.1.12 display voice service-mode

Function

Using the **display voice service-mode** command, you can view the voice service mode.

Format

display voice service-mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The default voice service mode is SIPAG. When configuring voice functions, you must specify the voice service mode.

Example

View the current voice service mode.

```
<Huawei> display voice service-mode
 The voice service mode is PBX.
```

Table 16-6 Description of the **display voice service-mode** command output

Item	Description
The voice service mode is PBX.	Voice service mode. The device supports the following service modes: ● H248AG ● SIP AG ● PBX

16.1.1.13 display voice sip-reg-count-per-second

Function

The **display voice sip-reg-count-per-second** command displays the number of SIP register messages sent every second.

Format

display voice sip-reg-count-per-second

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display the number of SIP register messages sent every second.

```
<Huawei> display voice sip-reg-count-per-second
 Sip register message count per second is 10!
```

16.1.1.14 display voice trace

Function

The **display voice trace** command displays the latest log information about call failures, including error and call logs.

Format

display voice trace

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When a call fails, run the **display voice trace** command to view the call log to rapidly troubleshoot call failures.

Example

Display call logs about latest call failures, including error and call logs.

```
<Huawei> display voice trace
<Huawei> 2016/03/30-14:08:23 AR[N@18][CCM:1]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@53][CCM:2]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@49]------[CCM     :    2]  <-- SETUP             --  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@50]------[CCM     :    2]  -- SETUP_ACK          -->  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@51]------[CCM     :    2]  <-- INFORMATION        --  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@52]------[CCM     :    2]  caller(2003) called(69****412)
<Huawei> 2016/03/30-14:08:30 AR[N@53][CCM:2]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@54]------[CCM     :    2]  -- RELEASE            -->  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@55]------[UAM-SIP :    2]  <-- SETUP_ACK          --  [CCM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@56]------[UAM-SIP :    2]  <-- RELEASE            --  [CCM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@57]------[CCM     :    2]  <-- RELEASE_COMPLETE   --  [UAM     ]
```

16.1.1.15 display voice upgrade-info

Function

The **display voice upgrade-info** command displays the configuration that fails to be upgraded after version upgrade.

Format

display voice upgrade-info

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After version upgrade, you can run the **display voice upgrade-info** command to view the configuration that fails to be upgraded.

Example

Display upgrade information.

```
<Huawei> system-view
[Huawei]display voice upgrade-info
[Upgrade-info: Upgrade unsuccessful command]
telno country-code 86 area-code 571 telno-value 6005
[Upgrade-info: End]
```

16.1.1.16 display voice voip-address

Function

Using the **display voice voip-address** command, you can view the configuration of the signaling IP address pool and media IP address pool.

Format

display voice voip-address

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice voip-address** command shows the configuration of the signaling IP address pool and media IP address pool.

Example

Display the configuration of the signaling IP address pool and media IP address pool.

```
<Huawei> display voice voip-address

  IP type          : Media IP
  Method             : Static
  Interface        : GigabitEthernet0/0/1
  IP address       : 192.168.1.1

  IP type          : Signal IP
  Method             : Static
  Interface        : GigabitEthernet0/0/1
  IP address       : 192.168.1.1
```

Table 16-7 Description of the display voice voip-address command output

Item	Description
IP type	IP address pool type: ● Media IP: media IP address pool ● Signal IP: signaling IP address pool
Method	Mode in which an IP address pool is configured: ● Static: The IP address pool is configured statically. ● dynamic: The IP address pool is allocated dynamically.
Interface	Interface where an IP address pool is configured.
IP address	IP addresses in an IP address pool.

 Copyright © Huawei Technologies Co., Ltd.

16.1.1.17 eid-para signalling (PBX user view)

Function

Using the **eid-para signalling** command, you can set the signaling type for a PBX user on a BRA port.

Using the **undo eid-para signalling** command, you can restore the default signaling type of a PBX user on a BRA port.

By default, the signaling type of a PBX user on a BRA port is Digital Subscriber Signalling System No. 1 (DSS1).

Format

eid-para signalling *sigtype*

undo eid-para signalling

Parameters

Parameter	Description	Value
sigtype	Specifies the signaling type.	The value can be: ● dss1 ● qsig

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

You need to configure the signaling type only for PBX users on a BRA port:

- When the device functions as a user-side device and uses DSS1 to connect to a network, set the signaling type to **dss1**.
- When the device functions as a user-side device and uses Q signaling (QSIG) to connect to a network, set the signaling type to **qsig**.

Example

Set the signaling type of a PBX user to QSIG.

```
<system-view> system-view
[Huawei] voice
[Huawei-voice] pbxuser jack
[Huawei-voice-pbxuser-jack] eid-para signalling qsig
```

16.1.1.18 flash-hook lower

Function

Using the **flash-hook lower** command, you can set the lower threshold for hookflash pressing.

Using the **undo flash-hook lower** command, you can restore the default lower threshold for hookflash pressing.

By default, the lower threshold for hookflash pressing is 100 ms.

Format

flash-hook lower *lower-value*

undo flash-hook lower

Parameters

Parameter	Description	Value
lower-value	Specifies the lower hookflash threshold.	The value is an integer that ranges from 50 to 1400, in milliseconds. **NOTE** The value of *lower-value* plus 50 cannot be larger than the value of *upper-value*.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The hookflash can be pressed by a calling party or a called party:

- Hookflash pressed by a called party: If the called party user A wants to transfer an incoming call to user B or another phone, user A can press the hookflash and dial the number of user C.
- Hookflash pressed by a calling party: User A calls user B. User B answers the call and talks with user A. User A can press the hookflash and dial the number of user C after hearing a special dial tone.

After user A presses the hookflash, if user C is busy or does not respond for a long period of time, user A can press the hookflash and talk with user B. If the phone of user C rings, user A hangs up and user B hears the ringback tone. User C picks

 Copyright © Huawei Technologies Co., Ltd.

up the phone and talks with user B. Whether a called party can be transferred to a toll call is restricted by the outgoing right of the called party.

The hookflash function can support the multi-party call service that users on a local network apply for, such as call waiting, call hold, three-party service, and call conference. Centrex users can call only users in the Centrex group.

Example

Set the lower threshold for hookflash pressing to 200 ms on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] flash-hook lower 200
```

16.1.1.19 flash-hook upper

Function

Using the **flash-hook upper** command, you can set the upper threshold for hookflash pressing.

Using the **undo flash-hook upper**command, you can restore the default upper threshold for hookflash pressing.

By default, the upper threshold for hookflash pressing is 350 ms.

Format

flash-hook upper *upper-value*

undo flash-hook upper

Parameters

Parameter	Description	Value
upper-value	Specifies the upper threshold for hookflash pressing.	The value is an integer ranging from 50 to 1400, in milliseconds. **NOTE** The value that ranges from 100 to 1400 is supported by AR129CGVM-L.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The hookflash can be pressed by a calling party or a called party:

- Hookflash pressed by a called party: If the called party user A wants to transfer an incoming call to user B or another phone, user A can press the hookflash and dial the number of user C.
- Hookflash pressed by a calling party: User A calls user B. User B answers the call and talks with user A. User A can press the hookflash and dial the number of user C after hearing a special dial tone.

After user A presses the hookflash, if user C is busy or does not respond for a long period of time, user A can press the hookflash and talk with user B. If the phone of user C rings, user A hangs up and user B hears the ringback tone. User C picks up the phone and talks with user B. Whether a called party can be transferred to a toll call is restricted by the outgoing right of the called party.

The hookflash function can support the multi-party call service that users on a local network apply for, such as call waiting, call hold, three-party service, and call conference. Centrex users can call only users in the Centrex group.

Example

Set the upper threshold for hookflash pressing to 1200 ms on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] flash-hook upper 1200
```

16.1.1.20 load voice-package

Function

The **load voice-package** command loads the voice prompt file.

Format

load voice-package *filename*

Parameters

Parameter	Description	Value
filename	Specifies the voice prompt file to be loaded.	The value is a string of 1 to 64 case-insensitive characters. The file name extension is .res or .cc. The recommended format is drive name:/directory name/file name, for example, flash:/voicepacket.res.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A prompt tone is the voice prompt heard by the calling and called users when the calling user initiates a call. For example, when the calling user calls the called user, the calling user hears the prompt tone indicating that the called user is busy. A voice prompt file stores all voice prompt tones.

The system software has the default voice prompt file. Voice prompt tone rules and services (including three-way conversation, three-party service, teleconference, call transfer, and call waiting) have different usage scenarios in different countries. You can customize the voice prompt file according to service requirements. To make the voice prompt voice file take effect immediately, run the **load voice-package** command to load the files. After loading the voice prompt file, run the **display startup** command to check the loaded voice prompt file according to the Startup voice-files field.

Prerequisites

Before loading the voice prompt file, perform the following operations:

1. Make the voice prompt file and generate a file with file name extension .res or .cc.

   NOTE

   For details about generating the voice prompt file with file name extension .res or .cc, contact technical support personnel.

2. Upload or download the voice prompt file to the device's memory.

Precautions

- When you use the **load voice-package** command to load the voice prompt file, the file take effect immediately after being loaded and the voice prompt file for next startup is modified.
- To restore the default English language, run the **load voice-package** command to load the system software package (.cc file) used for the current startup.

Example

Load voice prompt file **voicepacket.res**.

```
<Huawei> load voice-package voicepacket.res
 Info: Succeeded in activating the file
<Huawei> display startup
 MainBoard:
  Startup system software:                flash:/ar_v2r2c00.cc
  Next startup system software:             flash:/ar_v2r2c00.cc
```

```
Backup system software for next startup:   null
Startup saved-configuration file:          flash:/vrpcfg.zip
Next startup saved-configuration file:     flash:/vrpcfg.zip
Startup license file:                      null
Next startup license file:                 null
Startup patch package:                     null
Next startup patch package:                null
Startup voice-files:                       flash:/voicepacket.res
Next startup voice-files:                  flash:/voicepacket.res
```

16.1.1.21 media-port

Function

The **media-port** command configures a media port number range.

The **undo media-port** command restores the default values of media port number range.

By default, the system allocates a media port number range.

Format

media-port start *start-port-value* **end** *end-port-value*

undo media-port

Parameters

Parameter	Description	Value
start *start-port-value*	Specifies the start media port number.	The value is an integer that ranges from 1025 to 65535. Compatible with older versions whose range for this port value is from 1025 to 65535. **NOTE** Four media port numbers constitute a group, so the start media port number must be a multiple of 4.
end *end-port-value*	Specifies the end media port number.	The value is an integer that ranges from 1025 to 65532.Compatible with older versions whose range for this port value is from 1025 to 65535. **NOTE** Four media port numbers constitute a group, so the end media port number must be a multiple of 4.

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

M indicates the maximum number of online users and N indicates the start media port number (N + M*4 <= 65535).

Example

Set the media port number range to 54000-64000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] media-port start 54000 end 64000
```

16.1.1.22 mwi-mode

Function

Using the **mwi-mode** command, you can set the message waiting indicator (MWI) mode.

Using the **undo mwi-mode** command, you can restore the default MWI mode.

By default, the MWI mode is **fsk-without-ring**, in which the FSK is sent but no ring message is sent.

Format

mwi-mode { **fsk-with-ring** | **fsk-without-ring** }

undo mwi-mode

Parameters

Parameter	Description	Value
fsk-with-ring	Indicates that the FSK and a ring message are sent.	-
fsk-without-ring	Indicates that the FSK is sent but no ring message is sent.	-

Views

Voice view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the MWI mode to **fsk-with-ring**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] mwi-mode fsk-with-ring
```

16.1.1.23 pcm

Function

Using the **pcm** command, you can set the codec mode for voice services.

Using the **undo pcm** command, you can restore the default codec mode for voice services.

By default, the codec mode for voice services is A law.

Format

pcm { **a-law** | **u-law** }

undo pcm

Parameters

Parameter	Description	Value
a-law	Indicates the a-law algorithm.	-
u-law	Indicates the u-law algorithm.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

G.711 defines two compression algorithms: A-law algorithm and u-law algorithm. G.711, also known as Pulse Code Modulation (PCM), is a commonly used

waveform codec. G.711 uses a sampling rate of 8,000 samples per second. Non-uniform quantization (logarithmic) with 8 bits is used to represent each sample, resulting in a 64 kbit/s bit rate.

G.711 defines two main compression algorithms, the μ-law algorithm (used in North America and Japan) and A-law algorithm (used in Europe and the rest of the world). A-law encoding takes a 13-bit signed linear audio sample as input. μ-law encoding takes a 15-bit signed linear audio sample as input.

Example

Set the codec mode to u-law on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pcm u-law
```

16.1.1.24 park-feed

Function

Using the **park-feed** command, you can enable the device to reduce the feed on locked ports or disable this function.

Using the **undo park-feed** command, you can cancel the configuration.

By default, the device reduces the feed on locked ports.

Format

park-feed { **enable** | **disable** }

undo park-feed

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The **park-feed enable** command configures the system to reduce the feed on a Foreign Exchange Station (FXS) port when the port is locked.

NOTE

This function takes effect only for FXS ports.

Example

Disable the device from reducing the feed on locked FXS ports.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] park-feed disable
```

16.1.1.25 save tracelog

Function

The **save tracelog** command saves logs in the error log buffer and call log buffer to the **tracelog.zip** file in the flash memory of the device.

Format

save tracelog

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When a call fails, it is slow to generate error and call logs on the console interface. You can run the **save tracelog** command to save error and call logs in the log buffer to the **flash:/tracelog.zip** file. Technical personnel can export the logs from the device to rapidly troubleshoot the call failure.

Example

Save logs in the error log buffer and call log buffer to the **tracelog.zip** file in the flash memory of the device.

```
<Huawei> save tracelog
```

16.1.1.26 service-mode

Function

Using the **service-mode** command, you can set the voice operation mode.

By default, the voice operation mode is SIPAG mode.

Format

service-mode { **h248ag** | **sipag** | **pbx**}

Parameters

Parameter	Description	Value
h248ag	Indicates the H248AG mode.	-
sipag	Indicates the SIP AG mode.	-
pbx	Indicates the PBX mode.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Before configuring voice functions, you must specify the voice operation mode on the device.

After running the **service-mode** command to switch the voice operation mode of the device, save the configuration and run the **reboot** command in the user view to restart the device.

Example

Set the service mode to PBX.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service-mode PBX
 The modification takes effect only after you save the data and reboot the device.
[Huawei-voice] quit
[Huawei] quit
<Huawei> save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.........
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Huawei> reboot
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.1.27 sip-reg-count-per-second

Function

The **sip-reg-count-per-second** command sets the number of SIP register messages sent every second.

The **undo sip-reg-count-per-second** command restores the default number of SIP register messages sent every second.

By default, five SIP register messages are sent every second.

Format

sip-reg-count-per-second *reg-count-value*

undo sip-reg-count-per-second

Parameters

Parameter	Description	Value
reg-count-value	Specifies the number of SIP register messages sent every second.	The value is an integer that ranges from 1 to 1024.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the number of SIP register messages sent every second to 3.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip-reg-count-per-second 3
```

16.1.1.28 startup voice-package

Function

The **startup voice-package** command specifies the voice prompt file for next startup.

 Copyright © Huawei Technologies Co., Ltd.

Format

startup voice-package *filename*

Parameters

Parameter	Description	Value
filename	Specifies the voice prompt file for next startup.	The value is a string of 1 to 64 case-insensitive characters. The file name extension is .res or .cc. The recommended format is drive name:/directory name/file name, for example, flash:/voicepacket.res.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A prompt tone is the voice prompt heard by the calling and called users when the calling user initiates a call. For example, when the calling user calls the called user, the calling user hears the prompt tone indicating that the called user is busy. A voice prompt file stores all voice prompt tones.

The system software has the default voice prompt file. Voice prompt tone rules and services (including three-way conversation, three-party service, teleconference, call transfer, and call waiting) have different usage scenarios in different countries. You can customize the voice prompt file according to service requirements. To make the current voice prompt file continue to take effect and the new voice prompt file file take effect during next startup, run the **startup voice-package** command to specify the voice prompt file for next startup. After loading the voice prompt file, run the **display startup** command to check the loaded voice prompt file according to the Next startup voice-files field.

Prerequisites

Before loading the voice prompt file, perform the following operations:

1. Make the voice prompt file and generate a file with file name extension .res or .cc.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

For details about generating the voice prompt file with file name extension .res or .cc, contact technical support personnel.

2. Upload or download the voice prompt file to the device's memory.

Follow-up Procedure

To make the configuration take effect, run the **reboot** command in the user view to restart the device.

Example

Specify the voice prompt file **voicepacket.res** for next startup.

```
<Huawei> startup voice-package flash:/voicepacket.res
 This operation will take several minutes, please wait.........................
 ..
 Info: Succeeded in setting the file for booting system
<Huawei> display startup
 MainBoard:
  Startup system software:                    flash:/ar_v2r2c00.cc
  Next startup system software:               flash:/ar_v2r2c00.cc
  Backup system software for next startup:    null
  Startup saved-configuration file:           flash:/vrpcfg.zip
  Next startup saved-configuration file:      flash:/vrpcfg.zip
  Startup license file:                       null
  Next startup license file:                  null
  Startup patch package:                      null
  Next startup patch package:                 null
  Startup voice-files:                        null
  Next startup voice-files:                   flash:/voicepacket.res
```

16.1.1.29 voice

Function

Using the **voice** command, you can enter the voice view.

Format

voice

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Voice configurations can be performed only in the voice view.

Example

Enter the voice view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]
```

16.1.1.30 voip-address media

Function

Using the **voip-address media** command, you can assign a media IP address pool to an interface.

Using the **undo voip-address media** command, you can delete the media IP address pool of an interface.

Format

voip-address media interface *interface-type interface-number* { *ip-address* | **dynamic** }

undo voip-address media interface *interface-type interface-number* { *ip-address* | **dynamic** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
dynamic	Obtains IP addresses dynamically.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When configuring a media IP address pool:

- To specify the *ip-address* parameter, ensure that an IP address has been configured for the specified interface.

- To specify the **dynamic** parameter, ensure that an IP address has been dynamically assigned to the specified interface.

Example

Assign the media IP address pool 192.168.1.1 to GigabitEthernet 0/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] voip-address media interface GigabitEthernet 0/0/0 192.168.1.1
```

Related Topics

16.1.1.31 voip-address signalling

16.1.1.31 voip-address signalling

Function

Using the **voip-address signalling** command, you can assign a signaling IP address pool to an interface.

Using the **undo voip-address signalling** command, you can delete the signaling IP address pool of an interface.

Format

voip-address signalling interface *interface-type interface-number* { *ip-address* | **dynamic** }

undo voip-address signalling interface *interface-type interface-number* { *ip-address* | **dynamic** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
dynamic	Obtains IP addresses dynamically.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When configuring a signaling IP address pool:

- To specify the *ip-address* parameter, ensure that an IP address has been configured for the specified interface.
- To specify the **dynamic** parameter, ensure that an IP address has been dynamically assigned to the specified interface.

Example

Assign the signaling IP address pool 192.168.1.1 to GigabitEthernet 0/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] voip-address signalling interface GigabitEthernet 0/0/0 192.168.1.1
```

Related Topics

16.1.1.30 voip-address media

16.1.1.32 voip-vpn-instance

Function

The **voip-vpn-instance** command specifies a VPN instance used by voice services.

The **undo voip-vpn-instance** command deletes the VPN instance used by voice services.

By default, no VPN instance is specified to be used by voice services.

Format

voip-vpn-instance *vpn-instance-name*

undo voip-vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The VPN instance must already exist.

Views

Voice view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the interfaces to which specified media IP addresses and signaling IP addresses belong are bound to a VPN instance, you can run the **voip-vpn-instance** command in the voice view to specify the VPN instance to be used by voice services.

Prerequisites

- The VPN instance used by voice services can be configured only when the router works in PBX mode. By default, a router works in PBX mode. If the router does not work in PBX mode, run the **service-mode** command in the voice view to change the work mode of the router to PBX.
- Before running the **voip-vpn-instance** command, run the **ip vpn-instance** command to create a VPN instance.

Precautions

- After a VPN instance is specified to be used by voice services, reset the SIP server and SIP trunk group.
- In the voice view, you can specify only one VPN instance to be used by voice services.

Example

Specify the VPN instance vpn1 to be used by voice services.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] voice
[Huawei-voice] voip-vpn-instance vpn1
```

Related Topics

12.9.35 ip vpn-instance

16.1.1.30 voip-address media

16.1.1.31 voip-address signalling

16.1.1.33 undo logserver

Function

Using the **undo logserver** command, you can disable the port for communicating with the log server to stop sending logs to the log server.

Format

undo logserver

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Disable the port for communicating with the log server to stop sending logs to the log server.

```
<Huawei> system-view
[Huawei] diag
[Huawei-diagnose]undo logserver
```

16.1.2 Clip Configuration Commands

16.1.2.1 clip offhook ack-fsk-interval

Function

Using the **clip offhook ack-fsk-interval** command, you can set the interval between the time when the ACK message is received and the time when the frequency-shift keying (FSK) is transmitted in offhook state.

Using the **undo clip offhook ack-fsk-interval** command, you can restore the default interval.

By default, the interval between the time when the ACK message is received and the time when the FSK is transmitted in offhook state is 50 ms.

Format

clip offhook ack-fsk-interval *ack-fsk-interval*

undo clip offhook ack-fsk-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ack-fsk-interval	Specifies the interval between the time when the ACK message is received and the time when the FSK is transmitted in offhook state.	The value is an integer that ranges from 0 to 1000, in milliseconds. The default value is 50.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the interval between the time when the ACK message is received and the time when the FSK is transmitted in offhook state to 200 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook ack-fsk-interval 200
```

16.1.2.2 clip offhook dtas-ack-interval

Function

Using the **clip offhook dtas-ack-interval** command, you can set the maximum duration between the time when the dual tone-alerting signal (DT-AS) is transmitted and the time when the ACK message is received in offhook state.

Using the **undo clip offhook dtas-ack-interval** command, you can restore the default maximum duration.

By default, the maximum duration is 160 ms.

Format

clip offhook dtas-ack-interval *dtas-ack-interval*

undo clip offhook dtas-ack-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-ack-interval	Specifies the maximum duration between the time when the DT-AS is transmitted and the time when the ACK message is received in offhook state.	The value is an integer that ranges from 0 to 1000, in milliseconds. The default value is 160 ms.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the maximum duration between the time when the DT-AS is transmitted and the time when the ACK message is received in offhook state to 500 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook dtas-ack-interval 500
```

16.1.2.3 clip offhook dtas-duration

Function

Using the **clip offhook dtas-duration** command, you can set the duration of the dual tone-alerting signal (DT-AS) in offhook state.

Using the **undo clip offhook dtas-duration** command, you can restore the default duration of the DT-AS in offhook state.

By default, the duration of the DT-AS in offhook state is 80 ms.

Format

clip offhook dtas-duration *dtas-dur-value*

undo clip offhook dtas-duration

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-dur-value	Specifies the duration of the DT-AS in offhook state.	The value is an integer ranging from 0 to 1000, in milliseconds. The default value is 80.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the duration of the DT-AS in offhook state to 200 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook dtas-duration 200
```

16.1.2.4 clip offhook dtas-level

Function

Using the **clip offhook dtas-level** command, you can configure the level of the dual tone-alerting signal (DT-AS) in offhook state.

Using the **undo clip offhook dtas-level** command, you can restore the default level of the DT-AS in offhook state.

By default, the level of the DT-AS in offhook state is 10, that is, -15.5 dBm0.

Format

clip offhook dtas-level *dtas-level*

undo clip offhook dtas-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-level	Specifies the level of the DT-AS in offhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 10.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the DT-AS in offhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook dtas-level 15
```

16.1.2.5 clip offhook fsk-level

Function

Using the **clip offhook fsk-level** command, you can configure the level of the frequency-shift keying (FSK) in offhook state.

Using the **undo clip offhook fsk-level** command, you can restore the default level of the FSK in offhook state.

By default, the level of the FSK in offhook state is 3, that is, -8.5 dBm0.

Format

clip offhook fsk-level *fsk-level*

undo clip offhook fsk-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
fsk-level	Specifies the level of the FSK in offhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 3.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the FSK in offhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook fsk-level 15
```

16.1.2.6 clip offhook mark-signal-bit

Function

Using the **clip offhook mark-signal-bit** command, you can set the number of bits of the FSK synchronization mask in offhook state.

Using the **undo clip offhook mark-signal-bit** command, you can restore the default number of bits of the FSK synchronization mask in offhook state.

By default, the number of bits of the FSK synchronization mask in offhook state is 80.

Format

clip offhook mark-signal-bit *mark-signal-bit*

undo clip offhook mark-signal-bit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mark-signal-bit	Specifies the number of bits of the FSK synchronization mask in offhook state.	The value is an integer that ranges from 0 to 1000. The default value is 80.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of bits of the FSK synchronization mask in offhook state to 200 on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook mark-signal-bit 200
```

16.1.2.7 clip onhook channel-seize-bit

Function

Using the **clip onhook channel-seize-bit** command, you can set the number of bits seized by a channel in onhook state.

Using the **undo clip onhook channel-seize-bit** command, you can restore the default number of bits seized by a channel in onhook state.

By default, the number of bits seized by a channel in onhook state is 300.

Format

clip onhook channel-seize-bit *channel-seize-bit*

undo clip onhook channel-seize-bit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
channel-seize-bit	Specifies the number of bits seized by a channel in onhook state.	The value is an integer that ranges from 0 to 1000. The default value is 300.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of bits seized by a channel in onhook state to 500 on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook channel-seize-bit 500
```

16.1.2.8 clip onhook dtas-duration

Function

Using the **clip onhook dtas-duration** command, you can set the duration of the DT-AS in onhook state.

Using the **undo clip onhook dtas-duration** command, you can restore the default duration of the DT-AS in onhook state.

By default, the duration of the DT-AS in onhook state is 100 ms.

Format

clip onhook dtas-duration *dtas-dur-value*

undo clip onhook dtas-duration

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-dur-value	Specifies the duration of the DT-AS in onhook state.	The value is an integer ranging from 0 to 1000, in milliseconds. The default value is 100.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the duration of the DT-AS in onhook state to 500 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook dtas-duration 500
```

16.1.2.9 clip onhook dtas-fsk-interval

Function

Using the **clip onhook dtas-fsk-interval** command, you can set the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state.

Using the **undo clip onhook dtas-fsk-interval** command, you can restore the default interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state.

By default, the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state is 250 ms.

Format

clip onhook dtas-fsk-interval *dtas-fsk-interval*

undo clip onhook dtas-fsk-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-fsk-interval	Specifies the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state.	The value is an integer ranging from 0 to 1000, in milliseconds. The default value is 250.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state to 500 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook dtas-fsk-interval 500
```

16.1.2.10 clip onhook dtas-level

Function

Using the **clip onhook dtas-level** command, you can configure the level of the DT-AS in onhook state.

Using the **undo clip onhook dtas-level** command, you can restore the default level of the DT-AS in onhook state.

By default, the level of the DT-AS in onhook state is 3, that is, -8.5 dBm0.

Format

clip onhook dtas-level *dtas-level*

undo clip onhook dtas-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-level	Specifies the level of the DT-AS in onhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 3.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the DT-AS in onhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook dtas-level 15
```

16.1.2.11 clip onhook fsk-level

Function

Using the **clip onhook fsk-level** command, you can configure the level of the FSK in onhook state.

Using the **undo clip onhook fsk-level** command, you can restore the default level of the FSK in onhook state.

By default, the level of the FSK in onhook state is 3, that is, -8.5 dBm0.

Format

clip onhook fsk-level *fsk-level*

undo clip onhook fsk-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
fsk-level	Specifies the level of the FSK in onhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 3.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the FSK in onhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook fsk-level 15
```

16.1.2.12 clip onhook mark-signal-bit

Function

Using the **clip onhook mark-signal-bit** command, you can set the number of bits of the FSK synchronization mask in onhook state.

Using the **undo clip onhook mark-signal-bit** command, you can restore the default number of bits of the FSK synchronization mask in onhook state.

By default, the number of bits of the FSK synchronization mask in onhook state is 180.

Format

clip onhook mark-signal-bit *marksignal-bit*

undo clip onhook mark-signal-bit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
marksignal-bit	Specifies the number of bits of the FSK synchronization mask in onhook state.	The value is an integer that ranges from 0 to 1000. The default value is 180.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of bits of the FSK synchronization mask in onhook state to 600.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook mark-signal-bit 600
```

16.1.2.13 display voice clip

Function

Using the **display voice clip** command, you can view Calling Line Identification Presentation (CLIP) parameters.

Format

display voice clip

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display CLIP parameters on the device.

```
<Huawei> display voice clip
 CLIP onhook parameters:
  DTAS level                  : -8.5dBm0
  FSK level                   : -8.5dBm0
  Channel seize bit           : 300
  Mark signal bit             : 180
  DTAS FSK interval(ms)       : 250
  DTAS duration(ms)           : 100

 CLIP offhook parameters:
  DTAS level                  : -15.5dBm0
  FSK level                   : -8.5dBm0
  Mark signal bit             : 80
  DTAS ack interval(ms)       : 160
  Ack FSK interval(ms)        : 50
  DTAS duration(ms)           : 80
```

Table 16-8 Description of the display voice clip command output

Item	Description
CLIP onhook parameters	CLIP parameters in onhook state.
DTAS level	Level of the DT-AS.
FSK level	Level of the FSK.
Channel seize bit	Number of bits seized by a channel.
Mark signal bit	Number of bits of the FSK synchronization mask.
DTAS FSK interval	Interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted.
DTAS duration	Duration of the DT-AS.
CLIP offhook parameters	CLIP parameters in offhook state.
Ack FSK interval	Interval between the time when the ACK message is received and the time when the FSK is transmitted.
DTAS ack interval	Maximum duration between the time when the DT-AS is transmitted and the time when the ACK message is received.

 Copyright © Huawei Technologies Co., Ltd.

16.1.3 Ring Configuration Commands

16.1.3.1 display voice user-defined-ring

Function

Using the **display voice user-defined-ring** command, you can view the user-defined ring information.

Format

display voice user-defined-ring [*ring-index*]

Parameters

Parameter	Description	Value
ring-index	Specifies the index of a user-defined ring.	The value is an integer that ranges from 0 to 15.

Views

All views

Default Level

3: Management level

Usage Guidelines

If *ring-index* is not specified, information about all user-defined rings is displayed.

Example

Display information about user-defined ring 1.

```
<Huawei> display voice user-defined-ring 1
      First-ring(ms)  Second-ring(ms) Third-ring(ms)
 Index Ring   Interval  Ring  Interval  Ring  Interval
 1     0      0         0     0         0     0
```

Display information about user-defined rings.

```
<Huawei> display voice user-defined-ring
       First-ring(ms)  Second-ring(ms) Third-ring(ms)
 Index Ring   Interval  Ring  Interval  Ring  Interval
 0     0      0         0     0         0     0
 1     0      0         0     0         0     0
 2     0      0         0     0         0     0
 3     0      0         0     0         0     0
 4     0      0         0     0         0     0
 5     0      0         0     0         0     0
 6     0      0         0     0         0     0
 7     0      0         0     0         0     0
```

 Copyright © Huawei Technologies Co., Ltd.

```
8    0     0       0    0       0    0
9    0     0       0    0       0    0
10   0     0       0    0       0    0
11   0     0       0    0       0    0
12   0     0       0    0       0    0
13   0     0       0    0       0    0
14   0     0       0    0       0    0
15   0     0       0    0       0    0
```

Table 16-9 Description of the display voice user-defined-ring command output

Item	Description
Index	Index of the user-defined ring.
First-ring	Duration of the first ring tone.
Second-ring	Duration of the second ring tone.
Third-ring	Duration of the third ring tone.
Ring	Ringing duration.
Interval	Duration after ringing stops.

16.1.3.2 ring frequency

Function

Using the **ring frequency** command, you can set the frequency of the ringing current.

Using the **undo ring frequency** command, you can restore the default frequency of the ringing current.

By default, the frequency of the ringing current is 25 Hz.

Format

ring frequency { **16hz** | **25hz** | **50hz** }

undo ring frequency

Parameters

Parameter	Description	Value
16hz	Indicates that the frequency of the ringing current is 16 Hz.	-
25hz	Indicates that the frequency of the ringing current is 25 Hz.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
50hz	Indicates that the frequency of the ringing current is 50 Hz.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

A higher frequency of the ringing current indicates a sharper ring tone.

Example

Set the frequency of the ringing current on the device to 16 Hz.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring frequency 16hz
```

16.1.3.3 ring voltage

Function

The **ring voltage** command configures the ringing voltage.

The **undo ring voltage** command restores the default ringing voltage.

By default, the ringing voltage is 45 Vrms. On the AR169FVW-8S, the default ringing voltage is 50 Vrms.

Format

ring voltage *voltage-value*

undo ring voltage

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
voltage-value	Specifies a ringing voltage.	Enumerated type. The value can be: • 65 Vrms • 53 Vrms • 50 Vrms • 45 Vrms **NOTE** Only 129CGVW-L, AR129CVW and AR129CV support 53 Vrms.

Views

Voice views

Default Level

2: Configuration level

Usage Guidelines

When the default ringing voltage cannot meet requirements, you can run the **ring voltage** command to change the ringing voltage as required. You can run the **display voice configuration** command to verify the current ringing voltage configured on a device.

Example

Set the ringing voltage to 50 Vrms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring voltage 50Vrms
```

Related Topics

16.1.1.4 display voice configuration

16.1.3.4 stop-initial-ring enable

Function

Using the **stop-initial-ring enable** command, you can disable the initial ringing function.

Using the **stop-initial-ring disable** command, you can enable the initial ringing function.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo stop-initial-ring** command, you can restore the default initial ringing function.

By default, the initial ringing function is disabled.

Format

stop-initial-ring { **enable** | **disable** }

undo stop-initial-ring

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the initial ringing function on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] stop-initial-ring disable
```

16.1.3.5 user-defined-ring

Function

Using the **user-defined-ring** command, you can set the cadence ratio of the specified user-defined ring type.

Using the **undo user-defined-ring** command, you can delete the cadence ratio of the specified user-defined ring type.

Format

user-defined-ring *ring-index* { **first-ring** *first-ring-period* | **first-interval** *first-interval* | **second-ring** *second-ring-period* | **second-interval** *second-interval* | **third-ring** *third-ring-period* | **third-interval** *third-interval* }*

undo user-defined-ring *ring-index* { **first-ring** | **first-interval** | **second-ring** | **second-interval** | **third-ring** | **third-interval** }*

Parameters

Parameter	Description	Value
ring-index	Specifies the index of the user-defined ring type.	The value is an integer that ranges from 0 to 15.
first-ring *first-ring-period*	Specifies the duration of the first ring tone.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds. The value 0 indicates that the first ring tone is canceled.
first-interval *first-interval*	Specifies the duration after the first ring stops.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
second-ring *second-ring-period*	Specifies the duration of the second ring tone.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
second-interval *second-interval*	Specifies the duration after the second ring stops.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
third-ring *third-ring-period*	Specifies the duration of the third ring tone.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
third-interval *third-interval*	Specifies the duration after the third ring stops.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can set different ring types based on the ringing duration.

The **ring-mode** command can reference the cadence ratio configured by the **user-defined-ring** command. The *cadencering-value* values 128 to 143 in the **ring-mode** command correspond to *index* values 0 to 15 in the **user-defined-ring**.

 Copyright © Huawei Technologies Co., Ltd.

The *initialring-value* values 144 to 159 in the **ring-mode** command correspond to *index* values 0 to 15 in the **user-defined-ring** command.

The device supports the following combinations:

- 1-segment ringing: **first-ring**
- 2-segment ringing: **first-ring** + **first-interval**
- 4-segment ringing: **first-ring** + **first-interval** + **second-ring** + **second-interval**
- 6-segment ringing: **first-ring** + **first-interval** + **second-ring**+**second-interval** + **third-ring** + **third-interval**

Example

Configure user-defined ring 0 as 6-segment ringing and set the cadence ratio to 200:200:200:200:200:200.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] user-defined-ring 0 first-ring 200 first-interval 200 second-ring 200 second-interval 200 third-ring 200 third-interval 200
```

16.1.4 Upward-bandwidth Configuration Commands

16.1.4.1 display voice media-bandwidth-control

Function

Using the **display voice media-bandwidth-control** command, you can view the call restriction configuration when the uplink bandwidth is insufficient.

Format

display voice media-bandwidth-control

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display voice media-bandwidth-control** command only after the **media-bandwidth-control enable** command is executed to enable the call restriction function when the uplink bandwidth is insufficient.

Example

Display the call restriction configuration when the uplink bandwidth is insufficient.

```
<Huawei> display voice media-bandwidth-control
 Upward bandwidth                          : disable
 The maximum upward bandwidth              : 100000 kbit/s
 The reserved bandwidth for emergency call : 1000 kbit/s
 The used normal bandwidth                 : 0 kbit/s
 The used bandwidth for emergency call     : 0 kbit/s
```

Table 16-10 Description of the display voice upward-bandwidth command output

Item	Description
Upward bandwidth	Whether call restriction is enabled when the uplink bandwidth is insufficient. ● enable: call restriction is enabled when the uplink bandwidth is insufficient. ● disable: call restriction is disabled when the uplink bandwidth is insufficient.
The maximum upward bandwidth	Maximum uplink bandwidth.
The reserved bandwidth for emergency call	Reserved bandwidth for emergency calls.
The used normal bandwidth	Used bandwidth.
The used bandwidth for emergency call	Used bandwidth for emergency calls.

16.1.4.2 media-bandwidth-control enable

Function

Using the **media-bandwidth-control enable** command, you can enable the call restriction function when the uplink bandwidth is insufficient or disable this function.

Using the **media-bandwidth-control disable** command, you can cancel the configuration.

By default, the call restriction function is disabled when the uplink bandwidth is insufficient.

Format

media-bandwidth-control enable

 Copyright © Huawei Technologies Co., Ltd.

media-bandwidth-control disable

Parameters

None

Views

Trunk-group view or sipserver view

Default Level

2: Configuration level

Usage Guidelines

Before running the **16.1.4.3 media-bandwidth-control max-bandwidth** command to set the maximum uplink bandwidth, you must run the **media-bandwidth-control enable** command.

Example

Enable the call restriction function when the uplink bandwidth is insufficient.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] media-bandwidth-control enable
```

16.1.4.3 media-bandwidth-control max-bandwidth

Function

Using the **media-bandwidth-control max-bandwidth** command, you can set the maximum uplink bandwidth.

Using the **undo media-bandwidth-control max-bandwidth** command, you can restore the default maximum uplink bandwidth.

By default, the maximum uplink bandwidth is 100000 kbit/s.

Format

media-bandwidth-control max-bandwidth *max-bandwidth*

undo media-bandwidth-control max-bandwidth

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-bandwidth	Specifies the maximum uplink bandwidth.	The value is an integer that ranges from 1 to 5000, in 100 kbit/s. The default value is 1000, that is, 100000 kbit/s.

Views

trunk-group view or sipserver view

Default Level

2: Configuration level

Usage Guidelines

Before running the **media-bandwidth-control max-bandwidth** command, you must run the **media-bandwidth-control enable** command to enable the call restriction function when the uplink bandwidth is insufficient.

When the common bandwidth is overloaded, calls of common users are rejected. Emergency calls can be resumed within the range of the reserved bandwidth. (Common bandwidth = Maximum uplink bandwidth - Reserved bandwidth for emergency calls)

NOTE

Even if the remaining bandwidth is insufficient, the system allows the last call to be connected.

Example

Set the maximum uplink bandwidth to 90000 kbit/s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]sipserver
[Huawei-voice-sipserver]media-bandwidth-control enable
[Huawei-voice-sipserver]media-bandwidth-control max-bandwidth 900
```

16.1.5 Sip Stack Configuration Commands

16.1.5.1 display voice sip

Function

Using the **display voice sip** command, you can view the configuration of Session Initiation Protocol (SIP) parameters.

Format

display voice sip

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the configuration of SIP parameters on the device.

```
<Huawei> display voice sip
 SIP stack parameter & timers:
  Server header field                    :
  Organization header field              :
  User-agent header field                :
  Max-forwards header field              : 70
  Headline folding flag                  : Disable
  T1 timer(ms)                           : 500
  T2 timer(ms)                           : 4000
  T4 timer(ms)                           : 5000
  TD timer(ms)                           : 32000
  Min-SE timer(s)                        : 90
  Session progress timer(s)              : 180
  Session reliable progress timer(s)     : 60
  Entity based session timer flag        : Disable
  To header strict check flag            : Disable
```

Table 16-11 Description of the display voice sip command output

Item	Description
SIP stack parameter & timers	SIP stack parameter and values of timers.
Server header field	Value of the Server header field.
Organization header field	Value of the Organization header field.
User-agent header field	Value of the User-agent header field.
Max-forwards header field	Value of the Max-forwards header field.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Headline folding flag	Header folding flag in the authentication header field.
Entity based session timer flag	Whether the session timer defined by RFC 4028 based on the user agent (UA) is started.
T1 timer(ms)	T1 timer, which defines the estimated round-trip timer (RTT) time. For details, see RFC 3261.
T2 timer(ms)	T2 timer, which defines the maximum interval at which non-INVITE request messages and INVITE response messages are retransmitted. For details, see RFC 3261.
T4 timer(ms)	T4 timer, which defines the maximum duration a message will remain on a network. For details, see RFC 3261.
TD timer(ms)	TD timer, which defines the waiting time for retransmitting response messages. For details, see RFC 3261.
Min-SE timer(s)	Minimum value for the session interval. For details, see RFC 4028.
Session progress timer(s)	Unreliable provisional response retransmission timer, which determines the frequency for retransmitting unreliable provisional responses. For details, see RFC 3261.
Session reliable progress timer(s)	Reliable provisional response retransmission timer, which determines the frequency for retransmitting reliable provisional responses. For details, see RFC 3261.
To header strict check flag	Whether the To header field of the SIP protocol is strictly checked.

16.1.5.2 entity-based-sessions-timer

Function

Using the **entity-based-sessions-timer** command, you can enable the session timer defined by RFC4028 based on the UA or disable this function.

undo entity-based-sessions-timer command, you can disable the session timer defined by RFC4028 based on the UA.

 Copyright © Huawei Technologies Co., Ltd.

By default, the session timer defined by RFC4028 based on the UA is disabled.

Format

entity-based-sessions-timer { **enable** | **disable** }

undo entity-based-sessions-timer

Parameters

None

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the session timer defined by RFC4028 based on the UA.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] entity-based-sessions-timer enable
```

16.1.5.3 field-header max-forwards

Function

Using the **field-header max-forwards** command, you can set the value of the Max-forwards header field.

Using the **undo field-header max-forwards** command, you can restore the default value of the Max-forwards header field.

By default, the value of the Max-forwards header field is 70.

Format

field-header max-forwards *max-forwards-value*

undo field-header max-forwards

Parameters

Parameter	Description	Value
max-forwards-value	Specifies the value of the Max-forwards header field.	The value is an integer that ranges from 0 to 255.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the Max-forwards header field to 90.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header max-forwards 90
```

16.1.5.4 field-header organization

Function

Using the **field-header organization** command, you can set the value of the Organization header field.

Using the **undo field-header organization** command, you can restore the default value of the Organization header field.

By default, the value of the Organization header field is empty.

Format

field-header organization *organization-head*

undo field-header organization

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
organization-head	Specifies the value of the Organization header field.	The value is a string of 1 to 64 characters. **NOTE** If the hyphen (-) is entered, the value of the Organization header field is deleted.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the Organization header field in the SIP stack to OrganizationTemp.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header organization OrganizationTemp
```

16.1.5.5 field-header server

Function

Using the **field-header server** command, you can set the value of the Server header field.

Using the **undo field-header server** command, you can restore the default value of the Server header field.

By default, the value of the Server header field is empty.

Format

field-header server *server-head*

undo field-header server

Parameters

Parameter	Description	Value
server-head	Specifies the value of the Server header field.	The value is a string of 1 to 64 characters. **NOTE** If the hyphen (-) is entered, the value of the Server header field is deleted.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the Server header field in the SIP stack to HuaweiServerV2.0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header server huaweiserverv2.0
```

16.1.5.6 field-header user-agent

Function

Using the **field-header user-agent** command, you can set the value of the User-agent header field.

Using the **undo field-header user-agent** command, you can restore the default value of the User-agent header field.

By default, the value of the User-agent header field is empty.

Format

field-header user-agent *user-agent-head*

undo field-header user-agent

Parameters

Parameter	Description	Value
user-agent-head	Specifies the value of the User-agent header field.	The value is a string of 1 to 64 characters. **NOTE** If the hyphen (-) is entered, the value of the User-agent header field is deleted.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the User-agent header field in the SIP stack to SoftPhone V2.0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header user-agent softphoneV2.0
```

16.1.5.7 header-folding

Function

Using the **header-folding** command, you can enable header folding in the authentication header field or disable this function.

Using the **undo header-folding** command, you can cancel the configuration.

By default, header folding in the authentication header field is disabled.

Format

header-folding { enable | disable }

undo header-folding

Parameters

None

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable header folding in the authentication header field.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] header-folding enable
```

16.1.5.8 min-se

Function

Using the **min-se** command, you can set the minimum value of the session timer.

Using the **undo min-se** command, you can restore the default minimum value of the session timer.

By default, the minimum value of the session timer is 90s.

Format

min-se *min-se-period*

undo min-se

Parameters

Parameter	Description	Value
min-se-period	Specifies the minimum value of the session timer.	The value is an integer that ranges from 90 to 86400, in seconds. The default value is 90.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the minimum value of the session timer to 90s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] min-se 90
```

16.1.5.9 session-progress

Function

Using the **session-progress** command, you can set the value of the unreliable provisional response retransmission timer.

Using the **undo session-progress** command, you can restore the default value of the unreliable provisional response retransmission timer.

By default, the value of the unreliable provisional response retransmission timer is 180s.

Format

session-progress *session-progress-period*

undo session-progress

Parameters

Parameter	Description	Value
session-progress-period	Specifies the value of the unreliable provisional response retransmission timer.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 180.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the value of the unreliable provisional response retransmission timer to 90s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] session-progress 90
```

16.1.5.10 session-rel-progress

Function

Using the **session-rel-progress** command, you can set the value of the reliable provisional response retransmission timer.

Using the **undo session-rel-progress** command, you can restore the default value of the reliable provisional response retransmission timer.

By default, the value of the reliable provisional response retransmission timer is 60s.

Format

session-rel-progress *session-rel-progress-period*

undo session-rel-progress

Parameters

Parameter	Description	Value
session-rel-progress-period	Specifies the value of the reliable provisional response retransmission timer.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 60.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the value of the reliable provisional response retransmission timer to 90s.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] sip
[Huawei-voice-sip] session-rel-progress 90
```

16.1.5.11 sip

Function

Using the **sip** command, you can enter the SIP view.

Format

sip

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

SIP stack parameters are set in the SIP view.

Example

Enter the SIP view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip]
```

16.1.5.12 to-header-check-flag

Function

The **to-header-check-flag** command enables or disables strict check on the To header in SIP.

Using the **undo to-header-check-flag** command, you can cancel the configuration.

By default, strict check on the To header in SIP is disabled.

Format

to-header-check-flag { **enable** | **disable** }

undo to-header-check-flag

Parameters

None

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable strict check on the To header in SIP.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] to-header-check-flag enable
```

16.1.5.13 t1

Function

Using the **t1** command, you can set the value of the T1 timer.

Using the **undo t1** command, you can restore the default value of the T1 timer.

By default, the value of the T1 timer is 500 ms.

Format

t1 *t1-period*

undo t1

Parameters

Parameter	Description	Value
t1-period	Specifies the value of the T1 timer.	The value is an integer that ranges from 200 to 10000, in milliseconds. The default value is 500 ms.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The T1 timer defines the estimated round-trip timer (RTT) time.

Example

Set the value of the T1 timer to 1000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] t1 1000
```

16.1.5.14 t2

Function

Using the **t2** command, you can set the value of the T2 timer.

Using the **undo t2** command, you can restore the default value of the T2 timer.

By default, the value of the T2 timer is 4000 ms.

Format

t2 *t2-period*

undo t2

Parameters

Parameter	Description	Value
t2-period	Specifies the value of the T2 timer.	The value is an integer that ranges from 200 to 10000, in milliseconds. The default value is 4000 ms.

Views

SIP view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The T2 timer defines the maximum interval at which non-INVITE request messages and INVITE response messages are retransmitted.

Example

Set the value of the T2 timer to 1000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] t2 1000
```

16.1.5.15 t4

Function

Using the **t4** command, you can set the value of the T4 timer.

Using the **undo t4** command, you can restore the default value of the T4 timer.

By default, the value of the T4 timer is 5000 ms.

Format

t4 *t4-period*

undo t4

Parameters

Parameter	Description	Value
t4-period	Specifies the value of the T4 timer.	The value is an integer that ranges from 200 to 10000, in milliseconds. The default value is 5000 ms.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The T4 timer defines the maximum duration a message will remain on a network.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the T4 timer to 6000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] t4 6000
```

16.1.5.16 td

Function

Using the **td** command, you can set the value of the TD timer.

Using the **undo td** command, you can restore the default value of the TD timer.

By default, the value of the TD timer is 32000 ms.

Format

td *td-period*

undo td

Parameters

Parameter	Description	Value
td-period	Specifies the value of the TD timer.	The value is an integer that ranges from 0 to 300000, in milliseconds. The default value is 32000 ms. **NOTE** If UDP is used, the value must be greater than or equal to 32000. If TCP/SCTP is used, the value is 0.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The TD timer defines the waiting time for retransmitting response messages.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the TD timer to 60000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] td 60000
```

16.1.6 Dsp Configuration Commands

16.1.6.1 display voice dsp state

Function

The **display voice dsp state** command displays the status of a digital signal processor (DSP) or DSP channel.

Format

display voice dsp state { *slot/dsp-index* | **channel***slot/dsp-index/channel* }

Parameters

Parameter	Description	Value
slot/dsp-index	Specifies the slot ID and index of a DSP.	The value is a string of 1 to 15 case-insensitive characters. For example, if the slot ID is 0 and the DSP index is 0, the value is 0/0.
channel*slot/dsp-index/channel*	Specifies the slot ID, DSP index, and DSP channel index.	The value is a string of 1 to 15 case-insensitive characters. For example, if the slot ID is 0, the DSP index is 0, and the DSP index is 5, the value is 0/0/5.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the status of DSP 0/0.

```
<Huawei> display voice dsp state 0/0

 Symbol:
    0-idle $-G.711 busy A-All busy W-Wastage X-fault
    @-IP loopback *-PCM loopback #-prohibited

 Channel NO.  DSP channel state
 ---------------------------------------------------------------------
 0000-0035  00000 00000 00000 00000 00000 00000 00000 0

 Total:
    36  DSP channel
    36  idle, 0 G.711 Busy, 0 All Busy, 0 Wastage, 0 Fault,
    0   IP loopback, 0 PCM loopback, 0 prohibited
```

Table 16-12 Description of the display voice dsp state command output

Item	Description
0-idle	0 indicates that the DSP channel is in idle state.
$-G.711	$ indicates that the DSP channel works in G.711 codec state.
A-All busy	A indicates that the DSP channel works in non-G.711 codec state, such as the G.729 and G.723 codec state.
W-Wastage	W indicates that the the DSP channel is in wastage state, for example, G.729 codec may consume extra DSP channels.
X-fault	X indicates that the DSP channel is in faulty state, and a call cannot be connected through the DSP channel.
@-IP loopback	@ indicates that the DSP channel works in IP loopback state.
*-PCM loopback	* indicates that the DSP channel works in PCM loopback state.
#-prohibited	# indicates that the DSP channel is in prohibited state.
Channel NO	Number of a channel.
DSP channel state	DSP channel status displayed in graphs.

The AR150/200 series has the DSP chip. The following figure lists the maximum number of calls supported by the DSP chip in each codec state and packetization duration.

Table 16-13 Maximum number of calls supported by the AR150/200 series DSP chip in each codec state and packetization duration

Codec	5 ms	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	8	8	8	8	8	8	8
G723	-	-	-	8	-	-	8
G726	-	8	8	8	8	8	8
G729	-	8	8	8	8	8	8

The AR1200 series has the DSP chip. The following figure lists the maximum number of calls supported by the DSP chip in each codec state and packetization duration.

Table 16-14 Maximum number of calls supported by the AR1200 series DSP chip in each codec state and packetization duration

Codec	5 ms	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	32	32	32	32	32	32	32
G723	-	-	-	12	-	-	12
G726	-	12	12	12	12	12	12
G729	-	32	32	32	32	32	32

A DSP slot on the AR2200 and AR3200 series supports up to 128-channel DSP chip. The following figure lists the maximum number of calls supported by the DSP chip in each codec state and packetization duration.

Table 16-15 Maximum number of calls supported by the 128-channel DSP chip in each codec state and packetization duration

Codec	5 ms	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	32	72	128	128	128	72	128
G723	-	-	-	36	-	-	36
G726	-	36	48	48	48	48	48
G729	-	32	32	32	32	32	32

NOTE

AR2201 and AR2202 do not support the voice feature because they have no DSP slot.

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.2 display voice dsp statistic

Function

Using the **display voice dsp statistic** command, you can view the DSP statistics.

Format

display voice dsp statistic [*slotid|dsp-index*]

Parameters

Parameter	Description	Value
slotid|dsp-index	Specifies the slot ID and index of a DSP.	The value is a string of 1 to 15 case-insensitive characters. For example, if the slot ID is 0 and the DSP index is 0, the value is 0/0.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the statistics about all DSPs.

```
<Huawei> display voice dsp statistic
  Slotid/DSP-Index                0/0
  Total                         108
  Idle                          108
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                      0
  Sum of Sub-Board
  Total                         108
  Idle                          108
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                      0
```

16.1.6.3 display voice dsp-attribute

Function

Using the **display voice dsp-attribute** command, you can view the configuration of DSP parameters.

Format

display voice dsp-attribute

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the configuration of DSP parameters.

```
<Huawei> display voice dsp-attribute
 DSP code type                                  : G711A
 DSP RTP packet interval(ms)                    : 20
 T30 redundancy parameter value of T38 fax      : 3
 T4 redundancy parameter value of T38 fax       : 3
 Fax ECM                                        : Enable
 Fax train mode                                 : E2E train
 Fax max train rate                             : V17
 Fax V8 negotiate                               : Disable
 DSP min adapted jitter buffer(ms)              : 2
 DSP max adapted jitter buffer(ms)              : 135
 DSP init adapted jitter buffer(ms)             : 2
 DSP adapted jitter buffer threshold(ms)        : 150
 DSP min fixed jitter buffer(ms)                : 2
 DSP max fixed jitter buffer(ms)                : 135
 DSP init fixed jitter buffer(ms)               : 60
 DSP redundancy payload value                   : 96
 DSP NTE payload value                          : 97
 DSP clearmode payload value                    : 100
 DSP G.726-16k payload value                    : 103
 DSP G.726-24k payload value                    : 104
 DSP G.726-32k payload value                    : 101
 DSP G.726-40k payload value                    : 105
 DSP VBD payload value                          : 102
 VQM                                            : Disable
 RTCP package send interval time(ms)            : 5000
 RTCPXR                                         : Enable
 Severe degrade second threshold                : 400
 DSP echo check                                 : On
```

```
DSP packet lose compensate                    : Off
DSP silence reduce                          : Off
DTMF negative twist value                     : 10, unit 0.1db
DTMF positive twist value                    : 40, unit 0.1db
DSP 2833 event volume adjustment mode         : disable
DSP 2833 event volume adjustment devia        :  0  dBm
 Workmode         Threshold1   Threshold2   Threshold3
 Normal
```

Table 16-16 Description of the display voice dsp-attribute command output

Item	Description
DSP code type	Default DSP channel code type: ● G711A ● G711u ● G723_1 ● G729 ● G726-16k ● G726-24k ● G726-32k ● G726-40k
DSP Rtp Packet interval (ms)	Interval for the DSP channel to packetize RTP packets, in milliseconds. ● 5 ms ● 10 ms ● 20 ms ● 30 ms
T30 redundancy parameter value of T38 fax	T.30 redundancy parameter value of the T.38 fax. The value ranges from 0 to 7.
T4 redundancy parameter value of T38 fax	T.4 redundancy parameter value of the T.38 fax. The value ranges from 0 to 3.
Fax ECM	Fax ECM mode: ● enable: ECM ● disable: NECM
Fax train Mode	Fax training mode: ● e2e: End-to-end training ● local: Local training This parameter takes effect only when the T.38 fax is used.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Fax Max train Rate	Maximum fax training rate: ● V17: negotiation using V.17 fax and a maximum fax training rate of 14.4 kbit/s. ● V29: negotiation using V.29 fax and a maximum fax training rate of 9.6 kbit/s. ● V27: negotiation using V.27 fax and a maximum fax training rate of 4.8 kbit/s.
Fax V8 Negotiate	Whether V.8 negotiation of the T.38 fax is enabled or disabled.
DSP min adapted jitter buffer (ms)	Minimum value of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP max adapted jitter buffer (ms)	Maximum value of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP init adapted jitter buffer (ms)	Initial value of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP adapted jitter buffer threshold (ms)	Alarm threshold of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP min fixed jitter buffer (ms)	Minimum value of the static jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP max fixed jitter buffer (ms)	Maximum value of the static jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP init fixed jitter buffer (ms)	Initial value of the static jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP redundancy payload value	Redundancy payload value of the DSP channel. The value ranges from 96 to 127.
DSP NTE payload value	NTE payload value of the DSP channel. The value ranges from 96 to 127.
DSP clearmode payload value	RTP payload value of the DSP channel. The value ranges from 96 to 127.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DSP G.726-16k payload value	G.726-16k payload value of the DSP channel. The value ranges from 96 to 127.
DSP G.726-24k payload value	G.726-24k payload value of the DSP channel. The value ranges from 96 to 127.
DSP G.726-32k payload value	G.726-32k payload value of the DSP channel. The value ranges from 96 to 127.
DSP G.726-40k payload value	G.726-40k payload value of the DSP channel. The value ranges from 96 to 127.
DSP VBD payload value	VBD payload value of the DSP channel. The value ranges from 96 to 127.
VQM	Whether voice quality monitor (VQM) is enabled. ● disable: VQM is disabled. ● enable: VQM is enabled.
RTCPXR	Whether RTP Control Protocol Extended Reports (RTCP XR) is enabled. ● disable: RTCP XR is disabled. ● enable: RTCP XR is enabled.
RTCP package send interval time (ms)	Interval for the DSP channel to send RTCP packets. The value can be 0 or in the range of 500 to 65535, in milliseconds.
Severe Degrade Second Threshold	Default threshold for the number of severe degrade seconds. The value ranges from 1 to 65535.
DSP echo check	Whether echo cancellation is enabled on the DSP channel. ● disable: Echo cancellation is disabled on the DSP channel. ● enable: Echo cancellation is enabled on the DSP channel.
DSP Packet Lose Compensate	Whether the Packet Loss Concealment (PLC) function is enabled on the DSP channel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DSP silence reduce	Whether silence compression is enabled on the DSP channel.
DTMF negative twist value	DTMF detection negative twist value, range 0~100, unit 0.1db
DTMF positive twist value	DTMF detection positive twist value, range 0~100, unit 0.1db
DSP 2833 event volume adjustment mode	The mode in which the DSP adjusts the volume of DTMF tones during RFC 2833 DTMF transmission. **NOTE** Only AR1200, AR2200, and AR3200 that support voice communication support this parameter.
DSP 2833 event volume adjustment devia	The value of the DSP adjusts the volume of DTMF tones in fixed mode during RFC 2833 DTMF transmission. **NOTE** Only AR1200, AR2200, and AR3200 that support voice communication support this parameter.

16.1.6.4 display voice tone

Function

The **display voice tone** command is used to verify the current configuration on a signal tone.

Format

display voice tone *tone-id*

Parameters

Parameter	Description	Value
tone-id	Display the configuration of the specified signal tone.	The value is an integer that ranges from 1 to 11.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

```
<Huawei> display voice tone 3
-----------------Parameter Tone ID: 3 ----------------
------------------------------------------------------------
 Frequency(Unit:hz)  Ampletude(Unit:dbm)
        450                  0.3
          0                  0.0
          0                  0.0
          0                  0.0
 Cadences(count:1)   On-time  Off-time Frequency-Base-Flag
 Sequence[1]          65535        0       1

---------Attributes for detect Tone--------
            Frequency_Low[hz] Frequency_High[hz] Low-Ampletude[dbm] High-Ampletude[dbm]
1st Frequency      420               480               0.0             0.0
2nd Frequency      0                 0                 0.0             0.0
             Time_Onlow[ms]   Time_OnHigh[ms]  Time_OffLow[ms]  Time_OffHigh[ms]
1st Cadence:        2000             0                0                0
2nd Cadence:          0              0                0                0
```

16.1.6.5 dsp

Function

Using the **dsp** command, you can enter the DSP resource management view.

Format

dsp *slot/dsp-index*

Parameters

Parameter	Description	Value
slot/dsp-index	Specifies the slot ID and index of a DSP.	The value is a string of 1 to 15 characters. For example, if the slot ID is 0 and the DSP index is 0, the value is 0/0.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

To manage DSP resources, run the **dsp** command to enter the DSP resource management view.

Example

Enter the view of DSP 0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp 0/0
```

16.1.6.6 dsp-attribute

Function

Using the **dsp-attribute** command, you can enter the DSP attribute view.

Format

dsp-attribute

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

DSP configurations can be performed only in the DSP attribute view.

Example

Enter the DSP attribute view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute]
```

16.1.6.7 dtmf-twist-value(dsp-attribute view)

Function

command **dtmf-twist-value** is used to configure dtmf detection twist values

command **undo dtmf-twist-value** restores the default dtmf detection twist values

Format

dtmf-twist-value negative-twist *negative-twist-value* **positive-twist** *positive-twist-value*

undo dtmf-twist-value

Parameters

parameter	description	value
negative-twist *negative-twist-value*	negative dtmf twist value	integer 0-100, unit 0.1db.
positive-twist *positive-twist-value*	positive dtmf twist value	integer 0-100, unit 0.1db.

Views

dsp-attribute view

Default Level

2: Configuration level

Usage Guidelines

To configure dtmf detection twist values, run **dtmf-twist-value** command.

Example

set the negative twist value of dtmf detection to 5 db, and positive twist value to 10db.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] dtmf-twist-value negative-twist 50 positive-twist 100
```

16.1.6.8 echo

Function

Using the **echo** command, you can enable echo cancelation on the DSP channel or disable this function.

Using the **undo echo** command, you can cancel the configuration.

By default, echo cancelation is disabled on the DSP channel.

Format

echo { **enable** | **disable** }

undo echo

Parameters

None

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **echo enable** command enables echo cancelation on an MGC.

Example

Disable echo cancelation.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] echo disable
```

16.1.6.9 fax ecm

Function

The **fax ecm** command enables T.38 Error Correction Mode (ECM) or disable this function.

The **undo fax ecm** command restores the default T.38 ECM setting.

By default, T.38 ECM is enabled.

Format

fax ecm { **enable** | **disable** }

undo fax ecm

Parameters

None

Views

DSP attribute view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

ECM takes effect only when T.38 is used. After ECM is enabled, fax quality is optimized but the rate of fax messages is reduced. To increase the rate of fax messages, disable ECM.

Example

Enable T.38 ECM.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax ecm enable
```

16.1.6.10 fax redundancy-t30

Function

Using the **fax redundancy-t30** command, you can set the T.30 redundancy parameter value of the T.38 fax.

Using the **undo fax redundancy-t30** command, you can restore the default T.30 redundancy parameter value of the T.38 fax.

By default, the T.30 redundancy parameter value of the T.38 fax is 3.

Format

fax redundancy-t30 *redundancy-t30-value*

undo fax redundancy-t30

Parameters

Parameter	Description	Value
redundancy-t30-value	Specifies the T.30 redundancy parameter value of the T.38 fax.	The value is an integer that ranges from 0 to 7. The default value is 3.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the T.30 redundancy parameter value of the T.38 fax to 5.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax redundancy-t30 5
```

16.1.6.11 fax redundancy-t4

Function

Using the **fax redundancy-t4** command, you can set the T.4 redundancy parameter value of the T.38 fax.

Using the **undo fax redundancy-t4** command, you can restore the default T.4 redundancy parameter value of the T.38 fax.

By default, the T.4 redundancy parameter value of the T.38 fax is 3.

Format

fax redundancy-t4 *redundancy-t4-value*

undo fax redundancy-t4

Parameters

Parameter	Description	Value
redundancy-t4-value	Specifies the T.4 redundancy parameter value of the T.38 fax.	The value is an integer that ranges from 0 to 3. The default value is 3.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the T.4 redundancy parameter value of the T.38 fax to 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax redundancy-t4 2
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.12 fax training-mode

Function

Using the **fax training-mode** command, you can set the fax training mode.

Using the **undo fax training-mode** command, you can restore the default fax training mode.

By default, end-to-end training is used.

Format

fax training-mode { **e2e** | **local** }

undo fax training-mode

Parameters

Parameter	Description	Value
e2e	Indicates the end-to-end training mode.	-
local	Indicates the local training mode.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The fax training mode takes effect only when the T.38 fax is used. End-to-end training and local training modes are distinguished based on rate training signals sent from the transmit gateway to the receive gateway:

- If rate training signals need to be sent to the peer end, end-to-end training is used.
- If the gateway terminates and generates training signals, local training is used.

To use the local training mode, consider the maximum rate of the gateway, which is represented by the maximum fax rate supported on the DSP channel. The training mode is invalid for high-rate fax and low-rate transparent transmission.

Example

Set the fax training mode to local training.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax training-mode local
```

16.1.6.13 fax training-rate

Function

Using the **fax training-rate** command, you can set the maximum fax training rate.

Using the **undo fax training-rate** command, you can restore the default maximum fax training rate.

By default, the maximum fax training rate is V17.

Format

fax training-rate { **v17** | **v29** | **v27** }

undo fax training-rate

Parameters

Parameter	Description	Value
v17	Indicates the negotiation using V.17 and a maximum fax training rate of 14.4 kbit/s.	-
v29	Indicates the negotiation using V.29 and a maximum fax training rate of 9.6 kbit/s.	-
v27	Indicates the negotiation using V.27 and a maximum fax training rate of 4.8 kbit/s.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The maximum fax training rate takes effect only when local training is used, and is invalid for fax in transparent transmission mode. When the rate of the fax

machine can be reduced and the network is not running properly, reduce the fax training rate.

Example

Set the maximum fax training rate to V29.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax training-rate v29
```

16.1.6.14 fax v8negotiate

Function

Using the **fax v8negotiate** command, you can enable V8 negotiation or disable this function.

Using the **undo fax v8negotiate** command, you can restore the V8 negotiation parameter setting.

By default, V8 negotiation is disabled.

Format

fax v8negotiate { **enable** | **disable** }

undo fax v8negotiate

Parameters

None

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

During communication between two fax machines, one fax machine supports the V.34 fax (high-speed fax) and the other fax machine supports only the low-speed fax. To prevent the two fax machines from performing high-speed fax negotiation, disable V8 negotiation so that the two fax machines implement low-speed fax.

Example

Enable V8 negotiation.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax v8negotiate enable
```

16.1.6.15 jitter-buffer adapt-jb-threshold

Function

Using the **jitter-buffer adapt-jb-threshold** command, you can set the alarm threshold of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer adapt-jb-threshold** command, you can restore the default alarm threshold of the dynamic jitter buffer of the DSP channel.

By default, the alarm threshold of the dynamic jitter buffer of the DSP channel is 150 ms.

Format

jitter-buffer adapt-jb-threshold *adapt-jb-threshold*

undo jitter-buffer adapt-jb-threshold

Parameters

Parameter	Description	Value
adapt-jb-threshold	Specifies the alarm threshold of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 150 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer

MinAdaptJitterBuffer < ThresholdJitterBuffer

Example

Set the alarm threshold of the dynamic jitter buffer of the DSP channel to 100 ms.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer adapt-jb-threshold 100
```

16.1.6.16 jitter-buffer init-adapt-jb

Function

Using the **jitter-buffer init-adapt-jb** command, you can set the initial value of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer init-adapt-jb** command, you can restore the default initial value of the dynamic jitter buffer of the DSP channel.

By default, the initial value of the dynamic jitter buffer of the DSP channel is 2 ms.

Format

jitter-buffer init-adapt-jb *init-adapt-jb-value*

undo jitter-buffer init-adapt-jb

Parameters

Parameter	Description	Value
init-adapt-jb-value	Specifies the initial value of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 2 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the

specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

Example

Set the initial value of the dynamic jitter buffer of the DSP channel to 30 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer init-adapt-jb 30
```

16.1.6.17 jitter-buffer init-fixed-jb

Function

Using the **jitter-buffer init-fixed-jb** command, you can set the initial value of the static jitter buffer of the DSP channel.

Using the **undo jitter-buffer init-fixed-jb** command, you can restore the default initial value of the static jitter buffer of the DSP channel.

By default, the initial value of the static jitter buffer of the DSP channel is 60 ms.

Format

jitter-buffer init-fixed-jb *init-fixed-jb-value*

undo jitter-buffer init-fixed-jb

Parameters

Parameter	Description	Value
init-fixed-jb-value	Specifies the initial value of the static jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 60 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately.

 Copyright © Huawei Technologies Co., Ltd.

The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= IinitFixedJitterBuffer <= MaxFixedJitterBuffer and the MinAdaptJitterBuffer

Example

Set the initial value of the static jitter buffer of the DSP channel to 90 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer init-fixed-jb 90
```

16.1.6.18 jitter-buffer max-adapt-jb

Function

Using the **jitter-buffer max-adapt-jb** command, you can set the maximum value of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer max-adapt-jb** command, you can restore the default maximum value of the dynamic jitter buffer of the DSP channel.

By default, the maximum value of the dynamic jitter buffer of the DSP channel is 135 ms.

Format

jitter-buffer max-adapt-jb *max-adapt-jb-value*

undo jitter-buffer max-adapt-jb

Parameters

Parameter	Description	Value
max-adapt-jb-value	Specifies the maximum value of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 135 ms.

Views

DSP attribute view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

Example

Set the maximum value of the dynamic jitter buffer of the DSP channel to 120 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer max-adapt-jb 120
```

16.1.6.19 jitter-buffer max-fixed-jb

Function

Using the **jitter-buffer max-fixed-jb** command, you can set the maximum value of the static jitter buffer of the DSP channel.

Using the **undo jitter-buffer max-fixed-jb** command, you can restore the default maximum value of the static jitter buffer of the DSP channel.

By default, the maximum value of the static jitter buffer of the DSP channel is 135 ms.

Format

jitter-buffer max-fixed-jb *max-fixed-jb-value*

undo jitter-buffer max-fixed-jb

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-fixed-jb-value	Specifies the maximum value of the static jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 135 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer

MinAdaptJitterBuffer < ThresholdJitterBuffer

Example

Set the maximum value of the static jitter buffer of the DSP channel to 120 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer max-fixed-jb 120
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.20 jitter-buffer min-adapt-jb

Function

Using the **jitter-buffer min-adapt-jb** command, you can set the minimum value of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer min-adapt-jb** command, you can restore the default minimum value of the dynamic jitter buffer of the DSP channel.

By default, the minimum value of the dynamic jitter buffer of the DSP channel is 2 ms.

Format

jitter-buffer min-adapt-jb *min-adapt-jb-value*

undo jitter-buffer min-adapt-jb

Parameters

Parameter	Description	Value
min-adapt-jb-value	Specifies the minimum value of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 2 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

 Copyright © Huawei Technologies Co., Ltd.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer

MinAdaptJitterBuffer < ThresholdJitterBuffer

Example

Set the minimum value of the dynamic jitter buffer of the DSP channel to 30 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer min-adapt-jb 30
```

16.1.6.21 jitter-buffer min-fixed-jb

Function

Using the **jitter-buffer min-fixed-jb** command, you can set the minimum value of the static jitter buffer of the DSP channel.

Using the **undo jitter-buffer min-fixed-jb** command, you can restore the default minimum value of the static jitter buffer of the DSP channel.

By default, the minimum value of the static jitter buffer of the DSP channel is 2 ms.

Format

jitter-buffer min-fixed-jb *min-fixed-jb-value*

undo jitter-buffer min-fixed-jb

Parameters

Parameter	Description	Value
min-fixed-jb-value	Specifies the minimum value of the static jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 2 ms.

Views

DSP attribute view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer and the MinAdaptJitterBuffer

Example

Set the minimum value of the static jitter buffer of the DSP channel to 5 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer min-fixed-jb 5
```

16.1.6.22 loop-back (DSP resource management view)

Function

Using the **loop-back** command, you can configure the loopback function on a DSP channel.

Using the **undo loop-back** command, you can disable the loopback function.

Format

loop-back *loop-back-typechannel*

undo loop-back

Parameters

Parameter	Description	Value
loop-back-type	Specifies the loopback type.	The value can be: ● pcm-side: performs a loopback test at the pulse code modulation (PCM) channel side. ● ip-side: performs a loopback test at the IP side.
channel	Specifies the index of the DSP channel where the loopback test is performed.	The value is an integer that ranges from 0 to the maximum DSP channel index.

Views

DSP resource management view

Default Level

2: Configuration level

Usage Guidelines

When using the **loop-back** command, pay attention to the following points:

- This command is invalid for DSP channels in Idle, Fault, Wastage, or Prohibited state.
- When the DSP channel between the calling party and called party cannot transmit signals or can transmit signals only in one direction, run this command to locate the fault. For example, if the calling party hears the echo in a PCM-side loopback test, the speech channel between the calling phone and the calling DSP channel is functioning properly. If the called party hears the echo in an IP-side loopback test, the speech channel between the called phone and the calling DSP channel is functioning properly.

When using the **undo loop-back** command, pay attention to the following points:

- This command is valid only on DSP channels with the loopback function configured.
- After disabling the loopback function, you can run the **display voice dsp state** command to check the status of the DSP channel.

Example

Perform a PCM-side loopback test on DSP channel 5 in DSP 0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp 0/0
[Huawei-voice-dsp0/0] loop-back pcm-side 5
```

16.1.6.23 nte2833-volume deviation

Function

The **nte2833-volume deviation** command specifies how much the DSP adjusts the volume of DTMF tones in fixed mode.

The **undo nte2833-volume deviation** command restores the default setting of how much the DSP adjusts the volume of DTMF tones in fixed mode.

The default value is 20, indicating that the DSP adjusts the volume of DTMF tones by 0 dBm.

NOTE

Only AR1200, AR2200, and AR3200 that support voice communication support this command.

Format

nte2833-volume deviation *deviation-value*

undo nte2833-volume deviation

Parameters

Parameter	Description	Value
deviation-value	Indicates how much the DSP adjusts the volume of DTMF tones.	The value is an integer ranging from 0 to 40. For example, the value 0 indicates that the DSP adjusts the volume of DTMF tones by 20 dBm, the value 1 indicates adjusting by 19 dBm, and the value 40 indicates adjusting by –20 dBm.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

When the value of *deviation-value* is 0, it indicates that the volume of DTMF tones is increased by 20 dBm. The value 0 is called configured adjustment value, and 20 dBm the actual adjustment value. The conversion between the two values is as follows: Actual adjustment value = 20 – Configured adjustment value

The original volume of DTMF tones plus the actual adjustment value is the adjusted volume of DTMF tones. If the actual adjustment value is larger than 0 dBm, the DSP increases the volume of DTMF tones. If the actual adjustment value is smaller than 0 dBm, the DSP reduces the volume of DTMF tones. The actual adjustment value 0 indicates that the DSP does not change the volume of DTMF tones.

Precautions

The **nte2833-volume deviation** command takes effect only when the mode in which the DSP adjusts the volume of DTMF tones is fixed. You can run the **nte2833-volume mode** command to configure the DSP's DTMF tone adjustment mode.

Example

Configure the DSP to adjust the volume of DTMF tones by –5 dBm.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] nte2833-volume deviation 25
```

Related Topics

16.1.6.3 display voice dsp-attribute

16.1.6.24 nte2833-volume mode

16.1.6.24 nte2833-volume mode

Function

The **nte2833-volume mode** command configures the mode in which the DSP adjusts the volume of DTMF tones.

The **undo nte2833-volume** command restores the default mode in which the DSP adjusts the volume of DTMF tones.

By default, the adjustment mode is disabled.

NOTE

Only AR1200, AR2200, and AR3200 that support voice communication support this command.

Format

nte2833-volume mode *mode-value*

undo nte2833-volume mode

Parameters

Parameter	Description	Value
mode-value	Indicates the mode in which the DSP adjusts the volume of DTMF tones.	Enumerated type. The value can be: • **auto_attenuation**: Automatic attenuation mode • **disable**: Disabled mode • **fixed_adjust**: Fixed mode

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

During RFC 2833 DTMF transmission, the volume of DTMF tones may be high or low and cannot be automatically adjusted by DSP gains. In this case, you can run the **nte2833-volume mode** command to configure the DSP's DTMF tone adjustment mode, and thereby enable the DSP to adjust the volume of DTMF tones to solve the problem.

Example

Set the mode in which the DSP adjusts the volume of DTMF tones to **auto_attenuation**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] nte2833-volume mode auto_attenuation
```

Related Topics

16.1.6.3 display voice dsp-attribute
16.1.6.23 nte2833-volume deviation

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.25 payload-type clear-mode

Function

Using the **payload-type clear-mode** command, you can set the RTP payload type value of the DSP channel.

Using the **undo payload-type clear-mode** command, you can restore the default RTP payload type value of the DSP channel.

By default, the RTP payload type value of the DSP channel is 100.

Format

payload-type clear-mode *clear-mode-value*

undo payload-type clear-mode

Parameters

Parameter	Description	Value
clear-mode-value	Specifies the RTP payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 100.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The RTP payload type values at both ends must be identical and unique.

Example

Set the RTP payload type value of the DSP channel to 120.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type clear-mode 120
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.26 payload-type g726-16k

Function

Using the **payload-type g726-16k** command, you can set the G.726-16k payload type value of the DSP channel.

Using the **undo payload-type g726-16k** command, you can restore the default G.726-16k payload type value of the DSP channel.

By default, the G.726-16k payload type value of the DSP channel is 103.

Format

payload-type g726-16k *g726-16k-value*

undo payload-type g726-16k

Parameters

Parameter	Description	Value
g726-16k-value	Specifies the G.726-16k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 103.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-16k payload type values at both ends must be identical and unique.

Example

Set the G.726-16k payload type value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-16k 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.27 payload-type g726-24k

Function

Using the **payload-type g726-24k** command, you can set the G.726-24k payload type value of the DSP channel.

Using the **undo payload-type g726-24k** command, you can restore the default G.726-24k payload type value of the DSP channel.

By default, the G.726-24k payload type value of the DSP channel is 104.

Format

payload-type g726-24k *g726-24k-value*

undo payload-type g726-24k

Parameters

Parameter	Description	Value
g726-24k-value	Specifies the G.726-24k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 104.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-24k payload type values at both ends must be identical and unique.

Example

Set the G.726-24k payload type value of the DSP channel to 101.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-24k 101
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.28 payload-type g726-32k

Function

Using the **payload-type g726-32k** command, you can set the G.726-32k payload type value of the DSP channel.

Using the **undo payload-type g726-32k** command, you can restore the default G.726-32k payload type value of the DSP channel.

By default, the G.726-32k payload type value of the DSP channel is 101.

Format

payload-type g726-32k *g726-32k-value*

undo payload-type g726-32k

Parameters

Parameter	Description	Value
g726-32k-value	Specifies the G.726-32k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 101.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-32k payload type values at both ends must be identical and unique.

Example

Set the G.726-32k payload type value of the DSP channel to 102.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-32k 102
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.29 payload-type g726-40k

Function

Using the **payload-type g726-40k** command, you can set the G.726-40k payload type value of the DSP channel.

Using the **undo payload-type g726-40k** command, you can restore the default G.726-40k payload type value of the DSP channel.

By default, the G.726-40k payload type value of the DSP channel is 105.

Format

payload-type g726-40k *g726-40k-value*

undo payload-type g726-40k

Parameters

Parameter	Description	Value
g726-40k-value	Specifies the G.726-40k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 105.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-40k payload type values at both ends must be identical and unique.

Example

Set the G.726-40k payload type value of the DSP channel to 103.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-40k 103
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.30 payload-type nte

Function

Using the **payload-type nte** command, you can set the NTE payload type value of the DSP channel.

Using the **undo payload-type nte** command, you can restore the default NTE payload type value of the DSP channel.

By default, the NTE payload type value of the DSP channel is 97.

Format

payload-type nte *nte-value*

undo payload-type nte

Parameters

Parameter	Description	Value
nte-value	Specifies the NTE payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 97.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The NTE payload type values at both ends must be identical and unique.

Example

Set the NTE payload value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type nte 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.31 payload-type redundancy

Function

Using the **payload-type redundancy** command, you can set the redundancy payload type value of the DSP channel.

Using the **undo payload-type redundancy** command, you can restore the default redundancy payload type value of the DSP channel.

By default, the redundancy payload type value of the DSP channel is 96.

Format

payload-type redundancy *redundancy-value*

undo payload-type redundancy

Parameters

Parameter	Description	Value
redundancy-value	Specifies the redundancy payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 96.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The redundancy payload type values at both ends must be identical and unique.

Example

Set the redundancy payload type value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type redundancy 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.32 payload-type vbd

Function

Using the **payload-type vbd** command, you can set the VBD payload type value of the DSP channel.

Using the **undo payload-type vbd** command, you can restore the default VBD payload type value of the DSP channel.

By default, the VBD payload type value of the DSP channel is 102.

Format

payload-type vbd *vbd-value*

undo payload-type vbd

Parameters

Parameter	Description	Value
vbd-value	Specifies the VBD payload value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 102.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The VBD payload type values at both ends must be identical and unique.

Example

Set the VBD payload value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type vbd 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.33 plc

Function

Using the **plc** command, you can enable the Packet Loss Concealment (PLC) function on the DSP channel or disable this function.

Using the **undo plc** command, you can cancel the configuration.

By default, the PLC function is disabled.

Format

plc { enable | disable }

undo plc

Parameters

Parameter	Description	Value
enable	Enable the Packet Loss Concealment (PLC) function on the DSP channel.	-
disable	Disable the Packet Loss Concealment (PLC) function on the DSP channel.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Packet loss makes the voice quality deteriorated. The PLC recovers the packet loss to minimize the effect of packet loss in digital communications.

Example

Enable the PLC function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] plc enable
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.34 prohibit

Function

Using the **prohibit** command, you can prohibit DSP channels.

Using the **undo prohibit** command, you can restore the prohibited DSP channels.

Format

prohibit *channel* [*count*]

undo prohibit *channel* [*count*]

Parameters

Parameter	Description	Value
channel	Specifies the index of a DSP channel.	The value is an integer that ranges from 0 to the maximum DSP channel index.
count	Specifies the number of DSP channels to be prohibited.	The value is an integer that ranges from 1 to the maximum number of DSP channels supported.

Views

DSP resource management view

Default Level

2: Configuration level

Usage Guidelines

DSP channels in Busy or Wastage state or unregistered DSP channels cannot be prohibited.

Example

Prohibit channel 5 in DSP 0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp 0/0
[Huawei-voice-dsp0/0] prohibit 5
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.6.35 resource-threshold

Function

Using the **resource-threshold** command, you can set the resource threshold in hierarchical control mode.

Using the **undo resource-threshold mode** command, you can restore the default resource threshold in hierarchical control mode.

Format

resource-threshold { **threshold1** *threshold1* | **threshold2** *threshold2* | **threshold3** *threshold3* }

undo resource-threshold { **threshold1** | **threshold2** | **threshold3** }

Parameters

Parameter	Description	Value
threshold1 *threshold1*	Specifies the resource threshold of common users (cat1).	The value is an integer that ranges from 0 to 100. The default value is 100.
threshold2 *threshold2*	Specifies the resource threshold of category 2 users (cat2).	The value is an integer that ranges from 0 to 100. The default value is 100.
threshold3 *threshold3*	Specifies the resource threshold of category 3 users (cat3).	The value is an integer that ranges from 0 to 100. The default value is 100.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The thresholds in the **resource-threshold** command are as follows: *threshold1-val* <= *threshold2-val* <= *threshold3-val*

When the DSP resource control mode is hierarchical control, DSP resource allocation is determined based on user levels. The resources that can be used are configured by the **resource-threshold** command.

Example

Set the resource threshold for an authorized user to 60.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] resource-threshold threshold 1 60
```

16.1.6.36 resource-threshold mode

Function

Using the **resource-threshold mode** command, you can set the DSP resource control mode.

Using the **undo resource-threshold mode** command, you can restore the default DSP resource control mode.

By default, the DSP resource control mode is normal.

Format

resource-threshold mode { **priority** | **normal** }

undo resource-threshold mode

Parameters

Parameter	Description	Value
priority	Indicates that the DSP resource control mode is hierarchical control.	-
normal	Indicates that the DSP resource control mode is normal.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

When the DSP resource control mode is hierarchical control, DSP resource allocation is determined based on user levels. The resources that can be used are configured by the **resource-threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

When the DSP resource control mode is normal, users at any level can occupy all DSP resources.

Example

Set the DSP resource control mode to hierarchical control.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] resource-threshold mode priority
```

16.1.6.37 rtcp rtcp-interval

Function

Using the **rtcp rtcp-interval** command, you can set the interval at which the DSP channel sends RTCP packets.

Using the **undo rtcp rtcp-interval** command, you can restore the default interval at which the DSP channel sends RTCP packets.

By default, the interval at which the DSP channel sends RTCP packets is 5000 ms.

Format

rtcp rtcp-interval *rtcp-interval*

undo rtcp rtcp-interval

Parameters

Parameter	Description	Value
rtcp-interval	Specifies the interval at which the DSP channel sends RTCP packets.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5000 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **rtcp rtcp-interval** command sets the interval at which the DSP channel sends RTCP packets on an MGC.

Example

Set the interval at which the DSP channel sends RTCP packets to 8000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp rtcp-interval 8000
```

16.1.6.38 rtcp rtcpxr

Function

Using the **rtcp rtcpxr** command, you can enable the RTP Control Protocol Extended Reports (RTCP XR) function or disable this function.

Using the **undo rtcp rtcpxr** command, you can cancel the configuration.

By default, the RTCP XR function is disabled.

Format

rtcp rtcpxr { enable | disable }

undo rtcp rtcpxr

Parameters

Parameter	Description	Value
enable	Enable the RTP Control Protocol Extended Reports function.	-
disable	Disable the RTP Control Protocol Extended Reports function.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the RTCP XR function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp rtcpxr enable
```

16.1.6.39 rtcp sev-degrade-threshold

Function

Using the **rtcp sev-degrade-threshold** command, you can set the threshold for the number of severe degrade seconds.

Using the **undo rtcp sev-degrade-threshold** command, you can restore the default threshold for the number of severe degrade seconds.

By default, the threshold for the number of severe degrade seconds is 400.

Format

rtcp sev-degrade-threshold *sev-degrade-thresholdval*

undo rtcp sev-degrade-threshold

Parameters

Parameter	Description	Value
sev-degrade-thresholdval	Specifies the threshold for the number of severe degrade seconds.	The value is an integer that ranges from 1 to 65535. The default value is 400.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the threshold for the number of severe degrade seconds to 1000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp sev-degrade-threshold 1000
```

16.1.6.40 rtcp vqm

Function

Using the **rtcp vqm** command, you can enable the Voice Quality Monitor (VQM) function or disable this function.

Using the **undo rtcp vqm** command, you can cancel the configuration.

By default, the VQM function is disabled.

Format

rtcp vqm { enable | disable }

undo rtcp vqm

Parameters

Parameter	Description	Value
enable	Enable the Voice Quality Monitor function.	-
disable	Disable the Voice Quality Monitor function.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the VQM function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp vqm enable
```

16.1.6.41 silence

Function

Using the **silence** command, you can enable silence compression on the DSP channel.

Using the **undo silence** command, you can cancel the configuration.

By default, silence compression is disabled on the DSP channel.

Format

silence { enable | disable }

undo silence

Parameters

Parameter	Description	Value
enable	Enable the silence compression on the DSP channel.	-
disable	Disable the silence compression on the DSP channel.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **silence enable** command enables silence compression on an MGC.

Example

Enable silence compression.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] silence enable
```

16.1.6.42 tone (Voice View)

Function

tone can be either used to enter a specific tone-id view or create a new tone-id view, and hence configure the parameters of that tone-id

undo tone deletes a tone id

 Copyright © Huawei Technologies Co., Ltd.

Format

tone *Tone-id*

undo tone *Tone-id*

Parameters

parameter	description	value
Tone-id	Tone id number	integer, ranging from 1 to 11

Views

voice view

Default Level

Configuration level

Usage Guidelines

In the past, tone parameters were customized by way of importing a particular tone file. The disadvantage of this approach is that once some parameters need to be modified, the tone file has to be remade and imported again. This tone command can alleviate the trouble of the above process by enabling users to make customizations on the commandline.

Example

#create a view for tone id 3

```
[Huawei-voice]tone 3
Welcome enter the tone configuration!
As a diagnose feature,you'd better make change with the guide of handbook and local standards! Be
careful!
[Huawei-voice-tone-3]
```

16.1.6.43 tone-frequency

Function

The **tone-frequency** command configures the frequency and amplitude of a signal tone.

The **undo tone-frequency** command cancels any configuration on a signal tone's frequency and amplitude.

Format

tone-frequency { **frequency-1** *freq1-value amplitude1-value* [**frequency-2** *freq2-value amplitude2-value* [**frequency-3** *freq3-value amplitude3-value* [**frequency-4** *freq4-value amplitude4-value*]]] }

undo tone-frequency

Parameters

Parameter	Description	Value
frequency-1 *freq1-value*	Specifies the frequency of the first frequency set.	Integer, range: 0-4000, unit: Hz
amplitude1-value	Specifies the first amplitude of the Nth frequency set.	Integer, range: 0-100, unit: 0.1 dBm
frequency-2 *freq2-value*	Specifies the frequency of the second frequency set.	Integer, range: 0-4000, unit: Hz
amplitude2-value	Specifies the amplitude of the second frequency set.	Integer, range: 0-100, unit: 0.1 dBm
frequency-3 *freq3-value*	Specifies the frequency of the third frequency set.	Integer, range: 0-4000, unit: Hz
amplitude3-value	Specifies the amplitude of third frequency set.	Integer, range: 0-100, unit: 0.1 dBm
frequency-4 *freq4-value*	Specifies the frequency of the fourth frequency set.	Integer, range: 0-4000, unit: Hz
amplitude4-value	Specifies the amplitude of the fourth frequency set.	Integer, range: 0-100, unit: 0.1 dBm

Views

Tone view

Default Level

Configuration level

Usage Guidelines

Usually users should only perform find-tune on the frequency and the amplitude. Radical changes on those parameters may have undesirable effect upon normal calls.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure tone 3, set the frequency to be 980 Hz and amplitude 0.3 dBm. After doing so, the dial-tone becomes sharper because of higher pitch and larger amplitude.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tone 3
[Huawei-voice-tone-3] tone-frequency frequency-1 980 3
```

16.1.6.44 tone-cadence

Function

tone-cadence sets the cadence.

undo tone-cadence restores the default cadence.

Format

tone-cadence continus *base-frequency-flag*

tone-cadence sequence { *ontime1-value offtime1-value base-frequency-flag1* } [{ *ontime2-value offtime2-value base-frequency-flag2* } [{ *ontime3-value offtime3-value base-frequency-flag3* } [{ *ontime4-value offtime4-value base-frequency-flag4* }]]]

undo tone-cadence

Parameters

parameter	description	value
continus *base-frequency-flag*	Frequency flag. Convert this number into a 4-bit binary number, and each of the 4 bits corresponds to a frequency set (See the **tone-frequency** command).	Integer, range: 1-6, 8-10, 12.
sequence	Sequential flag.	-
ontimeN-value	Length of playing time for the Nth cadence.	Integer, range: 0-65535, unit: ms.
offtimeN-value	Length of silence time for the Nth cadence.	Integer, range: 0-65535, unit: ms.
base-frequency-flagN	Frequency flag of the Nth cadence.	Integer, range: 1-6, 8-10, 12.

 Copyright © Huawei Technologies Co., Ltd.

Views

Tone view

Default Level

Configuration level

Usage Guidelines

Usually users should only perform find-tune on the cadence. Radical changes on those parameters may have undesirable effect upon normal calls.

Example

Scenario 1:

Configure the cadence on tone 3, making it play continuously with frequency 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tone 3
[Huawei-voice-tone-3] tone-cadence continus 1
```

Scenario 2:

```
[Huawei-voice-tone-3] tone-cadence sequence 400 200 1 500 200 2
```

Set up to 2 cadences. The first one plays 400 ms, then begins a silence period that lasts 200 ms; the second plays for 500 ms, and then begins a 200 ms' silence. The values '1' and '2' are base-frequency-flags, which should be converted to binary numbers as follows:

1 == 0001 frequency 1

2 == 0010 frequency 2

3 == 0011 frequency 1 and frequency 2

4 == 0100 frequency 3

5 == 0101 frequency 1 and frequency 3

.....

After the above configuration, the tone that comes out when one picks up the phone sounds almost the same as before, except that the cadence differs.

Restores the default cadence

```
[Huawei-voice-tone-3] undo tone-cadence
```

16.1.6.45 tone-detect-info

Function

tone-detect-info configure the detection on both the tone-id's frequency and cadence.

undo tone-detect-info cancels any tone-id detection that has been configured.

Format

tone-detect-info { **frequency-1** *freq-low-throld-value1 freq-high-throld-value1* | **amplitude-1** *amp-low-throld-value1 amp-high-throld-value1* }* [{ **frequency-2** *freq-low-throld-value2 freq-high-throld-value2* | **amplitude-2** *amp-low-throld-value2 amp-high-throld-value2* }*

tone-detect-info { **cadence-1** *cadence-ontime-low-throld-value1 cadence-ontime-high-throld-value1 cadence-offtime-low-throld-value1 cadence-offtime-high-throld-value1* | **cadence-2** *cadence-ontime-low-throld-value2 cadence-ontime-high-throld-value2 cadence-offtime-low-throld-value2 cadence-offtime-high-throld-value2* }*

Parameters

Parameter	Description	Integer
frequency-1	frequency detection on frequency set N.	-
freq-low-throld-value1	the low threshold of frequency detection on frequency set N.	Integer, range: 0-4000, unit: Hz
freq-high-throld-value1	the high threshold of frequency detection on frequency set N.	Integer, range: 0-4000, unit: Hz
cadence-1	amplitude detection on frequency set 1.	-
amplitude-1 *amp-low-throld-value1*	the low threshold of amplitude detection on frequency set 1.	Integer, range: 0-100, unit: 0.1 dBm
amp-high-throld-value1	the high threshold of amplitude detection on frequency set 1.	integer, range: 0-100, unit: 0.1 dBm
cadence-2 *cadence-ontime-low-throld-value2*	when to start detecting the play of cadence 1.	Integer, range: 0-65535, unit: ms
cadence-ontime-high-throld-value1	when to stop detecting the play of cadence 1.	Integer, range: 0-65535, unit: ms
cadence-offtime-low-throld-value1	when to start detecting the cadence 1's silence period.	Integer, range: 0-65535, unit: ms
cadence-offtime-high-throld-value1	when to stop detecting the cadence 1's silence period.	Integer, range: 0-65535, unit: ms

Views

tone-id view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

Configuration level

Usage Guidelines

Precautions

For now, tone detection only supports at most two cadences and two frequencies.

This command requires a device restart before it takes effect.

Example

Configure the detection on tone3 frequency.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tone 3
[Huawei-voice-tone-3] tone-detect-info frequency-1 440 460 amplitude-1 2 4
```

Set frequency detection on frequency 1 to be [440, 460]Hz, and detection on amplitude to be [2,4]. The detection on frequency set 2 uses its original detection values when it is not set here.

Configure the detection on tone3 cadence.

```
[Huawei-voice-tone-3] tone-detect-info cadence-1 400 500 200 300 cadence-2 480 520 320 360
```

Set the play time detection on cadence 1 to be [400, 500]ms, and silence detection at time [200, 300]ms. Set the play time detection on cadence 2 to be [480, 520]ms, and silence detection at [320,360]ms.

16.1.6.46 traffic-policy (DSP attribute view)

Function

The **traffic-policy** command applies a traffic policy to a DSP channel.

The **undo traffic-policy** command deletes a traffic policy from a DSP channel.

By default, no traffic policy is applied to a DSP channel.

Format

traffic-policy *policy-name* **inbound**

undo traffic-policy inbound

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value is a string of 1 to 31 case-sensitive characters without spaces and starts with a letter.
inbound	Applies a traffic policy to the inbound direction of a DSP channel.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The redirection function of the MQC is used for routing voice packets.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

A traffic policy supports only filtering and redirection.

NOTE

After a traffic policy is applied, you cannot directly delete the traffic policy or traffic classifiers or traffic behaviors in the traffic policy. If the traffic policy that you want to delete has been applied to a DSP channel, run the **undo traffic-policy** command to unbind the traffic policy. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction of a DSP channel.

```
<Huawei> system-view
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] voice
```

```
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] traffic-policy p1 inbound
```

16.1.7 Voice Diagnose Commands

NOTE

- The following product models support voice functions (such as the PBX, SIP AG, and H.248 AG):
  - AR120 series: AR129CV, AR129CVW, and AR129CGVW-L
  - AR150 series: AR157VW and AR158EVW
  - AR160 series: AR161, AR169FVW, AR169FVW-8S, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR161FV-1P, and AR169FGVW-L
  - AR200 series: AR201VW-P, AR207V, AR207VW, and AR207V-P
  - AR1200 series: AR1220V, AR1220VW, AR1220EV, and AR1220EVW
  - AR2200 series: AR2204, AR2220, AR2220L, AR2220E.
  - AR2240: For the equipped with SRU40, SRU60, SRU80, and SRU100.
  - AR3200 series: For the AR3260 equipped with SRU40, SRU60, SRU80, or SRU100, the same voice mode is set for the active and standby SRUs.

  The AR129CV, AR129CVW, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, and AR169CVW-4B4S only support the PBX and SIP AG, but not the H.248 AG.
- When an AR2204, AR2220L, or AR2220E router needs to provide voice services, install a DSP module and a voice subcard in the router. When an AR2220, AR2240, or AR3200 router needs to provide voice services, install a DSP module.
- To provide voice services to POTS users on the AR1200, AR2200, or AR3200, install the 4FXS1FXO, 16FXS, or 32FXS card. The AR1200 does not support the 32FXS card.
- To provide voice services to ISDN phone users on the AR1200, AR2200, or AR3200, install the 2BST card.
- To connect an AR1200, AR2200, or AR3200 router to a TDM PBX through the E1 interface, install the E1T1-M card.
- On the AR169FGVW-L, AR1220EV, and AR1220EVW, the AT0 trunk cannot be connected to the SIP server or SIP trunk.

16.1.7.1 clip port

Function

The **clip port** command is used to test the display of the POTS calling number.

Format

clip port *slot-id* { **transwhen** *transwhen-value* | **format** *format-value* | **reversepole-beforecid** *reversepole-before-cid-value* | **input-gain** *input-gain-value* | **output-gain** *output-gain-value* | **telno** *telno-value* | **telname** *telname-value* }*

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.
transwhen *transwhen-value*	Displays the time.	Enumerated type. The values are as follows: ● after-ring ● before-ring
format *format-value*	Displays the format.	Enumerated type. The values are as follows: ● SDMF ● MDMF ● DTMF ● ETSI ● R15
reversepole-beforecid *reversepole-before-cid-value*	Displays the polarity reversal tag before a number.	Enumerated type. The values are as follows: ● disable ● enable
input-gain *input-gain-value*	Indicates the input gain.	The value is an integer that ranges from 0 to 15.
output-gain *output-gain-value*	Indicates the output gain.	The value is an integer that ranges from 0 to 20.
telno *telno-value*	Displays the calling number.	The value is a string of 1 to 32 characters.
telname *telname-value*	Displays the calling name.	The value is a string of 1 to 32 characters.

Views

Voice Diagnostic view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Configure the tested POTS calling number to be displayed after ringing.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] clip port 1/0/0 transwhen after-ring
```

16.1.7.2 debugging voice-adapt

Function

the **debugging voice-adapt** command is used to configure debugging print level for voice-adapt-related modules.

Format

debugging voice-adapt { **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** } *debug-level-value*

undo debugging voice-adapt { **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** }

display voice-adapt debugging { **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** }

Parameters

Parameter	Description	Value
{ **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** }	Module name.	-
debug-level-value	Debugging print level.	Enumerated value: ● error ● event ● trace ● all

Views

Diagnostic views

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Switch on debugging print for voice-adapt-related modules. Used for troubleshooting.

Example

Set debugging print level for vproduct module to be all.

```
[Huawei-diagnose] debugging voice-adapt vproduct all
```

undo all debugging print from vom module.

```
[Huawei-diagnose] undo debugging voice-adapt vom
```

16.1.7.3 diagnose

Function

The **diagnose** command displays the Diagnostic view.

Format

diagnose

Parameters

None

Views

Voice view

Default Level

3: Management level

Usage Guidelines

None

Example

Enter the Diagnostic view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]
```

16.1.7.4 digit-trace

Function

The **digit-trace** command is used to enable POTS number diagnosis.

The **undo digit-trace** command is used to disable POTS number diagnosis.

Format

digit-trace *slotid/subcardid/portid*

undo digit-trace *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable POTS number diagnosis

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]digit-trace 1/0/0
```

16.1.7.5 display fe slot fe-id table port-map dsp-port base-port

Function

The **display fe slot fe-id table port-map dsp-port base-port** command displays voice portmap entries.

Format

display fe slot *slot-id* **fe-id** *fe-id* **table port-map dsp-port** *dsp-port-num* **base-port** *base-port-num*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value is the slot where the LPU is installed.
fe-id *fe-id*	Specifies the multicore forwarding engine number.	The value is an integer that ranges from 0 to 256.
dsp-port *dsp-port-num*	Specifies the DSP port number.	The value is an integer that ranges from 61440 to 65535.
base-port *base-port-num*	Specifies the BASE port number.	The value is an integer that ranges from 0 to 61440.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display voice portmap entries of BASE port 0 in DSP port 61440 of engine 0 in slot 0.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] display fe slot 0 fe-id 0 table port-map dsp-port 61440 base-port 0
memory data:
0000 0000
```

16.1.7.6 display fe slot fe-id table voice-mr dest-ip port protocol

Function

The **display fe slot fe-id table voice-mr dest-ip port protocol** command displays the VoiceMr table.

Format

display fe slot *slot-id* **fe-id** *fe-id* **table voice-mr dest-ip** *ip-address* **port** *port-num* **protocol** *protocol-num*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value is the slot where the LPU is installed.
fe-id *fe-id*	Specifies the multicore forwarding engine number.	The value is an integer that ranges from 0 to 256.
dest-ip *ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.
port *port-num*	Specifies the port number.	The value is an integer that ranges from 0 to 65535.
protocol *protocol-num*	Specifies the protocol number.	The value is an integer that ranges from 0 to 255.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the VoiceMr table of engine 0 in slot 0. Engine 0 has destination IP address 192.168.0.1, port number 10, and protocol number 0.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] display fe slot 0 fe-id 0 table voice-mr dest-ip 192.168.0.1 port 10 protocol 0
memory data:
0000 0000
```

16.1.7.7 display fe slot fe-id table voice-signal

Function

The **display fe slot fe-id table voice-signal** command displays voice signaling entries.

Format

display fe slot *slot-id* **fe-id** *fe-id* **table voice-signal** *ip-address port-num protocol-num*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value is the slot where the LPU is installed.
fe-id *fe-id*	Specifies the multicore forwarding engine number.	The value is an integer that ranges from 0 to 256.
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
port-num	Specifies the destination port number.	The value is an integer that ranges from 5000 to 5999.
protocol-num	Specifies the protocol number.	The value is an integer that ranges from 6 to 17.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the voice signaling entry of engine 0 in slot 0. Engine 0 has destination IP address 192.168.0.1, port number 5000, and protocol number 7.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] display fe slot 0 fe-id 0 table voice-signal 192.168.0.1 5000 7
memory data:
0000 0000
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.7.8 display pots loop-line-threshold

Function

The **display pots loop-line-threshold** command is used to check the POTS loop line detection threshold.

Format

display pots loop-line-threshold

Parameters

None

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Check the POTS loop line detection threshold.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]display pots loop-line-threshold
 ---------------------------------------------------------------------------
  Loop-line test threshold item                                    Value
 ---------------------------------------------------------------------------
  Touch the power line : AC voltage threshold(volt)                 55
  Loop-line mixed with others:DC voltage threshold(volt)             40
  Loop-line grounding: ground resistance threshold(ohm)             20000
  Off-hook: A-B resistance min. threshold(ohm)                     100
  Off-hook: A-B resistance max. threshold(ohm)                    100000
  Off-hook: loop resistance min. threshold(ohm)                   2000
  Off-hook: loop resistance max. threshold(ohm)                   2000
  Loop-line mixed with others: A-B resistance threshold(ohm)          2000
  A-B poor insulation:A-B resistance min. threshold(ohm)            2000
  A-B poor insulation:A-B resistance max. threshold(ohm)            20000
  Leakage: ground capacitance threshold(nF)                        700
  Normal: ground capacitance threshold 1(nF)                       200
  Normal: ground capacitance threshold 2(nF)                       350
  Normal: ground capacitance threshold 3(nF)                        50
 ---------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.7.9 display pots subcard-loopline-adjust

Function

The **display pots subcard-loopline-adjust** command is used to check the calibration value in the scenario of POTS user port disconnection and self-mixing.

Format

display pots subcard-loopline-adjust [**from** *startframeid* [**to** *endframeid*] | *frameid*]

Parameters

Parameter	Description	Value
from *startframeid*	Specifies the start frame ID.	The value is fixed at 0.
to *endframeid*	Specifies the end frame ID.	The value is fixed at 0.
frameid	Specifies a frame ID.	The value is fixed at 0.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Check the calibration value in the scenario of POTS user port disconnection and self-mixing.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]display pots subcard-loopline-adjust
  ------------------------------------------------------------
  FrameID    Adjust flag    CAB(nF)  CAG(nF)  CBG(nF)  RAB(ohm)
  ------------------------------------------------------------
      0          Null          -        -        -        -
  ------------------------------------------------------------
  Total: All 0, Capacitance 0, Resistance 0, Null 1
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.7.10 display voice device state

Function

The **display voice device state** command displays device voice status.

Format

display voice device state

Parameters

None

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View device voice status.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice device state
  pots user number          : 0
  bra user number           : 0
  sipue user number         : 252
  Sipat0 trunk number       : 250
  At0 trunk number          : 1
  Pra trunk circuit number : 32
  R2 trunk circuit number  : 0
  Sip trunk group number   : 2
  H323 trunk group number  : 0
  Active call number        : 0
  Max call number           : 80
```

16.1.7.11 display voice statistics module at0

Function

The **display voice statistics module at0** command displays statistical information about the AT0 module.

Format

display voice statistics module at0 [**srv** | **line** | **rm**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the AT0 module.	-
line	Specifies LINE statistical information about the AT0 module.	-
rm	Specifies RM statistical information about the AT0 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the AT0 module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module at0
  Srv Messages:
  Send_Alerting       : 0
  Send_CallProceeding : 0
  Send_Progress       : 0
  Send_Setup          : 0
  Send_Connect        : 0
  Send_SetupAck       : 0
  Send_Disconnect     : 0
  Send_Release        : 0
  Send_RestartAck     : 0
  Send_Facility       : 0
  Send_Notify         : 0

  Recv_Alerting       : 0
  Recv_CallProceeding : 0
  Recv_Progress       : 0
  Recv_Setup          : 0
  Recv_Connect        : 0
  Recv_SetupAck       : 0
  Recv_Disconnect     : 0
  Recv_Release        : 0
  Recv_RestartAck     : 0
  Recv_Facility       : 0
  Recv_Notify         : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Line Messages:
Send_OccupyTrunk      : 0
Send_ReleaseTrunk     : 0
Send_SendNumber       : 0
Send_SetActive        : 0
Send_SetA/MuLaw       : 0
Send_SetGain          : 0
Send_SetNumberType    : 0
Send_SetRecvDTMF      : 0
Send_SetDTMFPara      : 0
Send_SetPulsePara     : 0
Send_ResetChannel     : 0
Send_ResetBoard       : 0
Send_InquireVersion   : 0
Send_SetRingAttribute : 0
Send_SetFeedVoltage   : 0
Send_SetFeedCurrent   : 0
Send_SetImpedance     : 0
Send_TsLoop           : 0

Recv_OccupyConfirm      : 0
Recv_CallInCome         : 0
Recv_CallRelease        : 0
Recv_PolarityReverse    : 0
Recv_SecondDialNumber   : 0
Recv_CallerIdRecvEnd    : 0
Recv_SendNumberComplete : 0
Recv_UtdDetect          : 0
Recv_ChannelResetOk     : 1
Recv_ChannelResetFault  : 1

Rm Messages:
Send_Alloc            : 2
Send_Release          : 2
Send_Add              : 0
Send_Del              : 0
Send_HandleOpen       : 1
Send_HandleClose      : 0
Send_HandleSendTone   : 0
Send_HandleStopTone   : 0
Send_HandleSendFSK    : 0
Send_HandleInsertDTMF : 0

Recv_Alloc            : 2
Recv_Release          : 2
Recv_Add              : 0
Recv_Del              : 0
Recv_HandleOpen       : 1
Recv_HandleClose      : 0
Recv_HandleSendTone   : 0
Recv_HandleStopTone   : 0
Recv_HandleSendFSK    : 0
Recv_HandleInsertDTMF : 0
```

16.1.7.12 display voice statistics module h323

Function

The **display voice statistics module h323** command displays statistical information about the H323 module.

Format

display voice statistics module h323 [**srv** | **h225** | **h245** | **ras**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the H323 module.	-
h225	Specifies H225 statistical information about the H323 module.	-
h245	Specifies H245 statistical information about the H323 module.	-
ras	Specifies RAS statistical information about the H323 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the H323 module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module h323
  Srv Sent Messages:
  Send_Setup           : 0
  Send_SetupAck        : 0
  Send_Callproceeding  : 0
  Send_Alerting        : 0
  Send_Connect         : 0
  Send_ConnectAck      : 0
  Send_ReleaseComplete : 0
  Send_Progress        : 0
  Send_ProgressRsp     : 0
  Send_ProgressAck     : 0
  Send_Information     : 0
  Send_Facility        : 0
  Send_Bearinfo        : 0
  Send_BearinfoRsp     : 0
  Send_BearinfoAck     : 0
  Send_GRQ             : 0
  Send_GCF             : 0
  Send_GRJ             : 0
  Send_RRQ             : 0
  Send_RCF             : 0
  Send_RRJ             : 0
  Send_LRQ             : 0
  Send_LCF             : 0
  Send_LRJ             : 0
  Send_ARQ             : 0
```

```
Send_ACF            : 0
Send_ARJ            : 0
Send_URQ            : 0
Send_UCF            : 0
Send_URJ            : 0
Send_DRQ            : 0
Send_DCF            : 0
Send_DRJ            : 0

Srv received Messages:
Recv_Setup          : 0
Recv_SetupAck       : 0
Recv_Callproceeding  : 0
Recv_Alerting       : 0
Recv_Connect        : 0
Recv_ConnectAck     : 0
Recv_ReleaseComplete : 0
Recv_Progress       : 0
Recv_ProgressRsp    : 0
Recv_ProgressAck    : 0
Recv_Information    : 0
Recv_Facility       : 0
Recv_Bearinfo       : 0
Recv_BearinfoRsp    : 0
Recv_BearinfoAck    : 0
Recv_GRQ            : 0
Recv_GCF            : 0
Recv_GRJ            : 0
Recv_RRQ            : 0
Recv_RCF            : 0
Recv_RRJ            : 0
Recv_LRQ            : 0
Recv_LCF            : 0
Recv_LRJ            : 0
Recv_ARQ            : 0
Recv_ACF            : 0
Recv_ARJ            : 0
Recv_URQ            : 0
Recv_UCF            : 0
Recv_URJ            : 0
Recv_DRQ            : 0
Recv_DCF            : 0
Recv_DRJ            : 0

H225 Sent Messages:
Send_Setup                    : 0
Send_SetupAck                 : 0
Send_Callproceeding           : 0
Send_Alerting                 : 0
Send_Connect                  : 0
Send_ReleaseComplete          : 0
Send_FacilityTCSQequest       : 0
Send_FacilityTCSAck           : 0
Send_FacilityTCSReject        : 0
Send_FacilityOLCRequest       : 0
Send_FacilityOLCAck           : 0
Send_FacilityOLCReject        : 0
Send_FacilityMSDRequest       : 0
Send_FacilityMSDAck           : 0
Send_FacilityCLCRequest       : 0
Send_FacilityCLCAck           : 0
Send_FacilityRequestMode      : 0
Send_FacilityRequestModeAck   : 0
Send_FacilityRequestModeReject : 0
Send_Progress                 : 0

H225 received Messages:
Recv_Setup                    : 0
Recv_SetupAck                 : 0
```

```
Recv_Callproceeding            : 0
Recv_Alerting                  : 0
Recv_Connect                   : 0
Recv_ReleaseComplete           : 0
Recv_FacilityTCSQequest        : 0
Recv_FacilityTCSAck            : 0
Recv_FacilityTCSReject         : 0
Recv_FacilityOLCRequest        : 0
Recv_FacilityOLCAck            : 0
Recv_FacilityOLCReject         : 0
Recv_FacilityMSDRequest        : 0
Recv_FacilityMSDAck            : 0
Recv_FacilityCLCRequest        : 0
Recv_FacilityCLCAck            : 0
Recv_FacilityRequestMode       : 0
Recv_FacilityRequestModeAck    : 0
Recv_FacilityRequestModeReject : 0
Recv_Progress                  : 0

H245 sent Messages:
Send_TCSRequest        : 0
Send_TCSAck            : 0
Send_TCSReject         : 0
Send_OlcRequest        : 0
Send_OlcAck            : 0
Send_OlcReject         : 0
Send_MsdRequest        : 0
Send_MsdAck            : 0
Send_ClcRequest        : 0
Send_ClcAck            : 0
Send_StartH245         : 0
Send_RequestMode       : 0
Send_RequestModeAck    : 0
Send_RequestModeReject : 0

H245 received Messages:
Recv_TCSRequest        : 0
Recv_TCSAck            : 0
Recv_TCSReject         : 0
Recv_OlcRequest        : 0
Recv_OlcAck            : 0
Recv_OlcReject         : 0
Recv_MsdRequest        : 0
Recv_MsdAck            : 0
Recv_ClcRequest        : 0
Recv_ClcAck            : 0
Recv_StartH245         : 0
Recv_RequestMode       : 0
Recv_RequestModeAck    : 0
Recv_RequestModeReject : 0

Ras sent Messages:
Send_GRQ            : 0
Send_GCF            : 0
Send_GRJ            : 0
Send_RRQ            : 0
Send_RCF            : 0
Send_RRJ            : 0
Send_LRQ            : 0
Send_LCF            : 0
Send_LRJ            : 0
Send_ARQ            : 0
Send_ACF            : 0
Send_ARJ            : 0
Send_URQ            : 0
Send_UCF            : 0
Send_URJ            : 0
Send_DRQ            : 0
Send_DCF            : 0
```

```
Send_DRJ            : 0
Send_CheckADMStatus : 0
Send_ADMStatus      : 0

Ras received Messages:
Recv_GRQ            : 0
Recv_GCF            : 0
Recv_GRJ            : 0
Recv_RRQ            : 0
Recv_RCF            : 0
Recv_RRJ            : 0
Recv_LRQ            : 0
Recv_LCF            : 0
Recv_LRJ            : 0
Recv_ARQ            : 0
Recv_ACF            : 0
Recv_ARJ            : 0
Recv_URQ            : 0
Recv_UCF            : 0
Recv_URJ            : 0
Recv_DRQ            : 0
Recv_DCF            : 0
Recv_DRJ            : 0
Recv_CheckADMStatus : 0
Recv_ADMStatus      : 0
```

16.1.7.13 display voice statistics module pots

Function

The **display voice statistics module pots** command displays statistical information about the POTS module.

Format

display voice statistics module pots [**srv** | **line**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the POT0 module.	-
line	Specifies LINE statistical information about the POT0 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the POTS module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module pots
  Srv Messages:
  Recv_StartRing            : 0
  Recv_Stop_Ring            : 1
  Recv_InitRing             : 1
  Recv_StartService         : 0
  Recv_EndService           : 0
  Recv_EndServiceByCa       : 0
  Recv_EndServiceAck        : 0
  Recv_RingSendTelnum       : 0
  Recv_SendTelnum           : 0
  Recv_SendAoce             : 0
  Recv_Light                : 0
  Recv_OverLight            : 0
  Recv_RingSplash           : 0
  Recv_Lock                 : 2
  Recv_NomalLineFeed        : 0
  Recv_Reverse              : 0
  Recv_KC                   : 0
  Recv_EndOfCall            : 0
  Recv_DisconnectClear      : 0
  Recv_DisconnectClearFail : 0
  Recv_TempFlashhookTime    : 0
  Recv_NoBattery            : 0
  Recv_NormalPolarity       : 0
  Recv_Hold                 : 0
  Recv_TransmitEnable       : 0
  Recv_TransmitDisenable    : 0

  Line Messages:
  Send_DialReport           : 2
  Send_OffHook              : 2
  Send_StopDialTone         : 0
  Send_OnHook               : 1
  Send_Hooking              : 0
  Send_CalledHook           : 0
  Send_StartFSK             : 1
  Send_RingFail             : 0
  Send_PortStatReport       : 0
  Send_TSLoopAck            : 0
  Send_CancelTSLoopAck      : 0
  Send_EarthConnect         : 0
  Send_EarthCancel          : 0
  Send_RecvGain             : 0
  Send_SendGain             : 0
  Send_DisconnectClearAck : 0
  Send_PortFail             : 1
  Send_PortResume           : 2
  Send_PortLoop             : 0
  Send_LoopCancel           : 0
  Send_LineTestStart        : 0
  Send_LineTestStop         : 0
  Send_GTCTestStart         : 0
  Send_GTCTestStop          : 0
  Send_LineFail             : 0
  Send_LineResume           : 0
  Send_PowerPermissible     : 0
  Send_PowerOverloadBuff    : 0
  Send_PowerOverloadLimit : 0
```

16.1.7.14 display voice statistics module q931

Function

The **display voice statistics module q931** command displays statistical information about the Q931 module.

Format

display voice statistics module q931 { **srv** | **protocol** } [**net** | **te**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the Q931 module.	-
protocol	Specifies protocol statistical information about the Q931 module.	-
net	Specifies NET statistical information about the Q931 module.	-
te	Specifies TE statistical information about the Q931 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the Q931 module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module q931
  Srv Net Sent Messages:
  Send_Alerting          : 0
  Send_CallProceeding    : 0
  Send_Progress          : 0
  Send_Setup             : 0
  Send_Connect           : 0
  Send_SetupAck          : 0
  Send_ConnectAck        : 0
  Send_UserInformation   : 0
  Send_SuspendReject     : 0
  Send_ResumeReject      : 0
  Send_Hold              : 0
```

```
Send_Suspend           : 0
Send_Resume            : 0
Send_HoldAck           : 0
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Srv Net Received Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0

Srv User Sent Messages:
Send_Alerting          : 0
Send_CallProceeding    : 0
Send_Progress          : 0
Send_Setup             : 0
Send_Connect           : 0
Send_SetupAck          : 0
Send_ConnectAck        : 0
Send_UserInformation   : 0
Send_SuspendReject     : 0
Send_ResumeReject      : 0
Send_Hold              : 0
Send_Suspend           : 0
```

```
Send_Resume            : 0
Send_HoldAck           : 0
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Srv User Rreceived Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0

Protocol Net Sent Messages:
Send_Alerting          : 0
Send_CallProceeding    : 0
Send_Progress          : 0
Send_Setup             : 0
Send_Connect           : 0
Send_SetupAck          : 0
Send_ConnectAck        : 0
Send_UserInformation   : 0
Send_SuspendReject     : 0
Send_ResumeReject      : 0
Send_Hold              : 0
Send_Suspend           : 0
Send_Resume            : 0
```

```
Send_HoldAck           : 0
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Protocol Net Received Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0

Protocol User Sent Messages:
Send_Alerting          : 0
Send_CallProceeding    : 0
Send_Progress          : 0
Send_Setup             : 0
Send_Connect           : 0
Send_SetupAck          : 0
Send_ConnectAck        : 0
Send_UserInformation   : 0
Send_SuspendReject     : 0
Send_ResumeReject      : 0
Send_Hold              : 0
Send_Suspend           : 0
Send_Resume            : 0
Send_HoldAck           : 0
```

```
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Protocol User Received Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0
```

16.1.7.15 display voice statistics module r2

Function

The **display voice statistics module r2** command displays statistical information about the R2 module.

Format

display voice statistics module r2 [**srv** | **rs** | **line**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the R2 module.	-
rs	Specifies RS statistical information about the R2 module.	-
line	Specifies LINE statistical information about the R2 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the R2 module.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose]display voice statistics module r2
  Srv Messages:
  Send_Alerting       : 0
  Send_CallProceeding : 0
  Send_Progress       : 0
  Send_Setup          : 0
  Send_Connect        : 0
  Send_ConnectAck     : 0
  Send_SetupAck       : 0
  Send_Disconnect     : 0
  Send_Release        : 0
  Send_RestartAck     : 0
  Send_Segment        : 0
  Send_Facility       : 0
  Send_Notify         : 0

  Recv_Alerting       : 0
  Recv_CallProceeding : 0
  Recv_Progress       : 0
  Recv_Setup          : 0
  Recv_Connect        : 0
  Recv_ConnectAck     : 0
  Recv_SetupAck       : 0
  Recv_Disconnect     : 0
  Recv_Release        : 0
  Recv_RestartAck     : 0
  Recv_Segment        : 0
  Recv_Facility       : 0
  Recv_Notify         : 0

  Line Messages:
  Send_Seize        : 0
  Send_SeizeAck     : 0
  Send_Answer       : 0
  Send_ClearForward : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Send_ClearBack    : 0
Send_CASFailure   : 0
Send_Block        : 0
Send_UnBlock      : 0
Send_Idle         : 0
Send_Error        : 0
Send_InService    : 0
Send_OutService   : 0

Recv_Seize        : 0
Recv_SeizeAck     : 0
Recv_Answer       : 0
Recv_ClearForward : 0
Recv_ClearBack    : 0
Recv_CASFailure   : 0
Recv_Block        : 0
Recv_UnBlock      : 0
Recv_Idle         : 0
Recv_Error        : 0
Recv_InService    : 0
Recv_OutService   : 0

Rs Messages:
Send_PropertySrcNumLen  : 0
Send_PropertyCmpSeqTime : 0
Send_EventRequset       : 0
Send_SignalR2addr       : 0
Send_SignalCongestion   : 0
Send_SignalCPRS         : 0
Send_SignalStop         : 0
Send_DmmMatchResult     : 0

Recv_R2addr      : 0
Recv_CPRS        : 0
Recv_R2F         : 0
Recv_DI          : 0
Recv_SI          : 0
Recv_SC          : 0
Recv_ES          : 0
Recv_CC          : 0
Recv_DISC        : 0
Recv_NAC         : 0
Recv_CNG         : 0
Recv_SubPrio     : 0
Recv_CasFail     : 0
Recv_SignalCOMPL : 0
Recv_RecvNum     : 0
Recv_BGRPAck     : 0
Recv_ChargeType  : 0
```

16.1.7.16 display voice statistics module sip

Function

The **display voice statistics module sip** command displays statistical information about the SIP module.

Format

display voice statistics module sip { **srv** | **protocol** }

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the RIP module.	-
protocol	Specifies protocol statistical information about the RIP module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the SIP module.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose]display voice statistics module sip
  Protocol Sent Request Messages:
  Send_Invite    : 0
  Send_Ack       : 0
  Send_Bye       : 0
  Send_Cancel    : 0
  Send_Register  : 0
  Send_Info      : 0
  Send_Update    : 0
  Send_Subscribe : 0
  Send_Notify    : 0
  Send_Message   : 0
  Send_Refer     : 0
  Send_Options   : 2298
  Send_Prack     : 0

  Protocol Received Request Messages:
  Recv_Invite    : 0
  Recv_Ack       : 0
  Recv_Bye       : 0
  Recv_Cancel    : 0
  Recv_Register  : 24
  Recv_Info      : 0
  Recv_Update    : 0
  Recv_Subscribe : 0
  Recv_Notify    : 0
  Recv_Message   : 0
  Recv_Refer     : 0
  Recv_Options   : 1529
  Recv_Prack     : 0

  Protocol Sent Response Messages:
  Send_1XX : 0
  Send_2XX : 1529
  Send_3XX : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Send_4XX : 0
Send_5XX : 0
Send_6XX : 0

Protocol Received Response Messages:
Recv_1XX : 0
Recv_2XX : 1530
Recv_3XX : 0
Recv_4XX : 0
Recv_5XX : 0
Recv_6XX : 0

Srv Sent Messages:
Send_Alerting          : 0
......
```

16.1.7.17 pots circuit-test

Function

The **pots circuit-test** command triggers a POTS internal line test.

Format

pots circuit-test { *slot-id* | **telno** *telno-value* | **mgid** *mgid-value* | **terminalid** *terminalid-value* } [**busy** { **cancel** | **force** | **defer** [**deferred-time** *deferred-time-value* | **timeout-proc** *timeout-proc-value*] }]

Parameters

Parameter	Description	Value
slot-id	Specifies a slot ID/subcard ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters.
telno *telno-value*	Specifies a test number.	The value is a string of 1 to 16 characters.
mgid *mgid-value*	Specifies a gateway ID.	The value is an integer that ranges from 0 to 16777215.
terminalid *terminalid-value*	Specifies a terminal ID.	The value is an integer that ranges from 0 to 16777215.
deferred-time *deferred-time-value*	Specifies the delay.	The value is an integer that ranges from 1 to 1440.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
timeout-proc *timeout-proc-value*	Specifies the timeout period.	Enumerated value. ● 0: It does not POTS internal line test when timeout. ● 1: It will be tested mandatorily upon timeout.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Trigger a POTS internal line test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots circuit-test 5/0/0
  slot 5 subcard 0 port 0 ( telno 5000 mgid - terminalid - )
  under testing, Please wait......
[Huawei-voice-vdiagnose]
  Testing port:  5/0/0
  Telno       :  5000
  MGid        :  -
  Terminalid  :  -
  -------------------------------------------------------
  Test item                              Result
  -------------------------------------------------------
  Digital Voltage:                        Normal
  Low Battery:                            Normal
  High Battery:                           Normal
  Positive Battery:                       Normal
  Feeder voltage:                          Normal
  Loop current:                           Normal
  Ringing current voltage:                   Normal
  Ringing current frequency:                  Normal
  VAG:                                  Normal
  VBG:                                  Normal
  -------------------------------------------------------
  Feeder voltage(V):                       47.830
  Ringing current voltage(V):                0.000
  Loop current(mA):                        0.000
  -------------------------------------------------------
```

16.1.7.18 pots loop-line-test

Function

The **pots loop-line-test** command triggers a POTS external line test.

Format

pots loop-line-test { *slot-id* | **telno** *telno-value* | **mgid** *mgid-value* **terminalid** *terminalid-value* } [**busy** { **cancel** | **force** | **defer** [**deferred-time** *deferred-time-value* | **timeout-proc** *timeout-proc-value*] }]

Parameters

Parameter	Description	Value
slot-id	Specifies a slot ID/subcard ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. ● *slotid*: based on product specifications ● *subcardid*: based on product specifications ● *portid*: based on product specifications
telno *telno-value*	Specifies a test number.	The value is a string of 1 to 16 characters.
mgid *mgid-value*	Specifies a gateway ID.	The value is an integer that ranges from 0 to 16777215.
terminalid *terminalid-value*	Specifies a terminal ID.	The value is an integer that ranges from 0 to 16777215.
deferred-time *deferred-time-value*	Specifies the delay.	The value is an integer that ranges from 1 to 1440.
timeout-proc *timeout-proc-value*	Specifies the timeout period.	Enumerated value. ● 0: It does not POTS internal line test when timeout. ● 1: It will be tested mandatorily upon timeout.

Views

Voice Diagnostic view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Trigger a POTS external line test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots loop-line-test 5/0/0
  slot 5 subcard 0 port 0 ( telno 5000 mgid - terminalid - )
  under testing, Please wait......
[Huawei-voice-vdiagnose]
  Testing port:  5/0/0
  Telno       :  5000
  MGid        :  -
  Terminalid  :  -
  ---------------------------------------------------------------------------
  Test item                                Result
  ---------------------------------------------------------------------------
  A->ground AC voltage              (V)       0.000
  B->ground AC voltage              (V)       0.000
  A->B      AC voltage              (V)       0.000
  A->ground DC voltage              (V)      -1.474
  B->ground DC voltage              (V)      -1.438
  A->B      DC voltage              (V)      -0.036
  A->ground insulation resistance  (ohm)    >10M
  B->ground insulation resistance  (ohm)    >10M
  A->B insulation resistance       (ohm)     1.333M
  A->B loop resistance             (ohm)     0
  A->B polarity reversal resistance(ohm)     1.333M
  A->ground capacitance            (uF)      0.050
  B->ground capacitance            (uF)      0.050
  A->B capacitance                 (uF)      0.000
  Conclusion                               Phone not connected
  ---------------------------------------------------------------------------
```

16.1.7.19 pots loop-line-threshold

Function

The **pots loop-line-threshold** command configures detection thresholds for POTS external line tests.

Format

pots loop-line-threshold { **restore** | **set** *threshold-type threshold-value* }

Parameters

Parameter	Description	Value
restore	Restore thresholds for POTS external line tests.	-

Parameter	Description	Value
threshold-type	Specifies an external line test standard.	The value is an integer. The options are as follows: ● 0: A/B wire touching the power line: AC voltage ● 1: external line mixing: DC voltage ● 2: external line grounding: resistance to ground ● 3: off-hook: resistance lower limit between A and B wires ● 4: off-hook: resistance upper limit between A and B wires ● 5: off-hook: loop resistance lower limit ● 6: off-hook: loop resistance upper limit ● 7: external line mixing: resistance between A and B wires ● 8: poor insulation between A and B wires: resistance lower limit between A and B wires ● 9: poor insulation between A and B wires: resistance upper limit between A and B wires ● 10: electric leakage: grounding capacitance ● 11: normal: minimum grounding capacitance ● 12: normal: capacity between A and B wires ● 13: normal: minimum grounding capacitance

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
threshold-value	Specifies the value of an external test standard.	The value is a hexadecimal integer that ranges from 0x0 to 0x7fffffff.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Set the POTS external line test standard "external line grounding: resistance to ground" to 5.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots loop-line-threshold set 2 0x5
```

16.1.7.20 pots path-test

Function

The **pots path-test** command triggers a POTS hardware or service test.

Format

pots path-test *slotid/subcard* **port all type** { **hardware** | **business** }

pots path-test *slotid/subcard* **port** *port-id* **type** { **hardware** | **business** } [**assist-port** *port-id*]

undo pots path-test *slotid/subcard*

Parameters

Parameter	Description	Value
slotid/subcard	Specifies a slot ID/subcard ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. • *slotid*: based on product specifications • *subcardid*: based on product specifications
port-id	Specifies a port number.	The value is an integer that ranges from 0 to 63.
type	Specifies the test type.	Enumerated type. The value can be hardware or business.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

To trigger a POTS hardware or service test, run **pots path-test** command.

Example

Trigger a POTS hardware test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] diagnose
[Huawei-voice-vdiagnose] pots path-test 6/0 port all type hardware
  This operation will take several minutes, please wait...
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/0        Assist port :  6/0/2
  Test result :  Normal
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/1        Assist port :  6/0/3
  Test result :  Normal
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/2        Assist port :  6/0/0
  Test result :  Normal
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/3        Assist port :  6/0/1
  Test result :  Normal
```

 Copyright © Huawei Technologies Co., Ltd.

16.1.7.21 pots subcard-loopline-adjust get

Function

The **pots subcard-loopline-adjust get** command displays calibration values for frame analog user ports in external line disconnection and self-mixed situations.

Format

pots subcard-loopline-adjust get *frameid* { **cutline-port***slotid1/portid1* | **selfmixed-port** *slotid2/portid2* } *

Parameters

Parameter	Description	Value
frameid	Specifies a frame ID.	The value is fixed at 0.
cutline-port *slotid1/portid1*	Specifies a slot ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. • *slotid1*: based on product specifications • *portid1*: based on product specifications
selfmixed-port *slotid2/portid2*	Specifies a slot ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. • *slotid2*: based on product specifications • *portid2*: based on product specifications

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display calibration values for frame analog user ports in external line disconnection and self-mixed situations.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots subcard-loopline-adjust get 0 cutline-port 5/0 selfmixed-port 5/1
  slot 5 subcard 0 port 0
  under geting adjust, Please wait......
[Huawei-voice-vdiagnose]
  -----------------------------------------
  slot 5 subcard 0 port 0 cutline adjust:
  -----------------------------------------
  CAB(nF)                    0
  CAG(nF)                    50
  CBG(nF)                    50
  -----------------------------------------
```

16.1.7.22 pots subcard-loopline-adjust restore

Function

The **pots subcard-loopline-adjust restore** command restores the default calibration values for frame analog user ports in external line disconnection and self-mixed situations.

Format

pots subcard-loopline-adjust restore { **from** *startframeid* [**to** *endframeid*] | *frameid* }

Parameters

Parameter	Description	Value
startframeid	Specifies the start frame ID.	The value is fixed at 0.
endframeid	Specifies the end frame ID.	The value is fixed at 0.
frameid	Specifies a frame ID.	The value is fixed at 0.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Restore the default calibration values for frame analog user ports in external line disconnection and self-mixed situations.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots subcard-loopline-adjust restore 0
  Are you sure to restore the default value? (y/n)[n]:y
  Success: adjust of frame  0 restore successfully
```

16.1.7.23 pots subcard-loopline-adjust set

Function

The **pots subcard-loopline-adjust set** command sets or modifies calibration values for frame analog user ports in external line disconnection and self-mixed situations.

Format

pots subcard-loopline-adjust set { **from** *startframeid* [**to** *endframeid*] | *frameid* } { **cab** *cab-value* | **cag** *cag-value* | **cbg***cbg-value* | **rab** *rab-value* } *

Parameters

Parameter	Description	Value
startframeid	Specifies the start frame ID.	The value is fixed at 0.
endframeid	Specifies the end frame ID.	The value is fixed at 0.
frameid	Specifies a frame ID.	The value is fixed at 0.
cab-value	Specifies the capacity between A and B wires.	The value is an integer that ranges from 0 to 10000000.
cag-value	Specifies the grounding capacity of A wire.	The value is an integer that ranges from 0 to 10000000.
cbg-value	Specifies the grounding capacity of B wire.	The value is an integer that ranges from 0 to 10000000.
rab-value	Specifies the resistance between A and B wires.	The value is an integer that ranges from 0 to 10000000.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

To set or modifies calibration values for frame analog user ports in external line disconnection and self-mixed situations, run **pots subcard-loopline-adjust set** command.

Example

Modify calibration values for frame analog user ports in external line disconnection and self-mixed situations.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots subcard-loopline-adjust set 0 rab 5 cag 5
  Success: adjust of frame  0 set successfully
```

16.1.7.24 reset voice statistics module

Function

The **reset voice statistics module** command clears statistics on each module.

Format

reset voice statistics module { **at0** | **h323** | **pots** | **q931** | **r2** | **sip** }

Parameters

Parameter	Description	Value
at0	Clears statistics on AT0 messages.	-
h323	Clears statistics on H323 messages.	-
pots	Clears statistics on POTS messages.	-
q931	Clears statistics on Q931 messages.	-
r2	Clears statistics on R2 messages.	-
sip	Clears statistics on SIP messages.	-

Views

Diagnostic view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

You can run the **reset voice statistics module** command to clear statistics on each module.

Example

Clear statistics on the AT0 module.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] reset voice statistics module at0
```

16.1.7.25 ts6em

Function

The **ts6em** command triggers the voice time slot test for dsp.

Format

ts6em slot-in *slot-in-id* **slot-out** *slot-out-id*

Parameters

Parameter	Description	Value
slot-in *slot-in-id*	Input slot ID. This parameter is mandatory and specifies the input of opening channel. It is also used for time slot switch.	The value is an integer of 0 to 12 characters.
slot-out *slot-out-id*	Output slot ID. This parameter is used for time slot switch.	The value is an integer of 0 to 12 characters.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

The **ts6em** command triggers the voice time slot test for dsp.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]ts6em slot-in 1 slot-out 2
 The Test Statics:
 Time Slot:0 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:1 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:2 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:3 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:4 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:5 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
```

16.2 Voice interface Commands

16.2.1 Voice interface Configuration Commands

16.2.1.1 access-mode

Function

Using the **access-mode** command, you can set the access mode for a VE1 interface.

Using the **undo access-mode** command, you can restore the default access mode of a VE1 interface.

By default, the access mode of a VE1 interface is digital.

Format

access-mode { **digital** | **direct** }

undo access-mode

Parameters

Parameter	Description	Value
digital	Indicates the digital section access mode.	-
direct	Indicates the direct access mode.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

When the access mode is set to direct, all the SA bits of an E1 frame must be always set to 1s, and the loopback2 operation is not allowed. When the access mode is set to digital, an E1 interface must comply with ETS 300.233.

Example

Set the access mode of a VE1 interface to digital.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] access-mode digital
```

16.2.1.2 access-mode (BRA Interface View)

Function

The **access-mode** command configures the working mode of a basic rate access (BRA) interface.

The **undo access-mode** command restores the default working mode of a BRA interface.

By default, a BRA interface works in NT mode.

NOTE

Only AR169CVW-4B4S supports this command.

Format

access-mode *access-mode-value*

undo access-mode

Parameters

Parameter	Description	Value
access-mode-value	Specifies the working mode of a BRA interface.	Enumerated value. The options are as follows: ● te: The BRA interface works in Terminal Equipment (TE) mode. ● nt: The BRA interface work in Network Termination (NT) mode.

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device uses a BRA interface to connect to an ISDN phone, the BRA interface should work in NT mode. When a device uses a BRA interface to connect to an ISDN network, the BRA interface should work in TE mode.

Precautions

This command can only be used to configure the working mode of the BRA0/0/0 and BRA0/0/1 interfaces on the AR169CVW-4B4S.

Example

Configure a BRA interface to work in TE mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 0/0/0
[Huawei-voice-bra0/0/0] access-mode te
```

16.2.1.3 alarm

Function

Using the **alarm** command, you can enable or disable the UNI alarm function on a BRA interface.

Using the **undo alarm** command, you can restore the default configuration.

By default, the UNI alarm function is disabled on a BRA interface.

Format

alarm { **enable** | **disable** }

undo alarm

Parameters

Parameter	Description	Value
enable	Enables the UNI alarm function.	-
disable	Disables the UNI alarm function.	-

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the UNI alarm function on a BRA interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] alarm enable
```

16.2.1.4 crc4

Function

Using the **crc4** command, you can enable or disable cyclic redundancy check 4 (CRC4) on a VE1 interface.

Using the **undo crc4** command, you can restore the default configuration.

By default, CRC4 check is disabled on a VE1 interface.

Format

crc4 { **enable** | **disable** }

undo crc4

Parameters

Parameter	Description	Value
enable	Enables CRC4 check on a VE1 interface.	_
disable	Disables CRC4 check on a VE1 interface.	_

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable CRC4 check on a VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] crc4 enable
```

16.2.1.5 crc (VE1 interface view)

Function

The **crc** command sets the CRC mode on a VE1 interface.

The **undo crc** command restores the default setting.

By default, 16-bit CRC is used.

Format

crc { 16 | 32 | none }

undo crc

Parameters

Parameter	Description	Value
16	Configures 16-bit CRC on the interface.	-
32	Configures 32-bit CRC on the interface.	-
none	Configures no CRC on the interface.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Cyclic Redundancy Check (CRC) is often used to detect transmission errors in a communication system. CRC checks data consistency and provides high algorithm accuracy. A 32-bit field can achieve higher accuracy than a 16-bit field but uses more resources.

Precautions

If you run the **crc** command multiple times in the same VE1 interface view, only the latest configuration takes effect.

Example

Enable 32-bit CRC on the VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] crc 32
  Set crc successfully
```

16.2.1.6 crc-alarm-threshold

Function

Using the **crc-alarm-threshold** command, you can set the errored seconds threshold, consecutively severely errored seconds threshold, and degraded minute threshold.

Using the **undo crc-alarm-threshold** command, you can restore the default errored seconds threshold, consecutively severely errored seconds threshold, and degraded minute threshold.

 Copyright © Huawei Technologies Co., Ltd.

By default:

- The errored seconds threshold is 432 errored seconds per hour.
- The consecutively severely errored seconds threshold is 4 severely errored seconds per hour.
- The degraded minute threshold is 8 degraded minutes per hour.

Format

crc-alarm-threshold { **es** *es-threshold* | **cses** *cses-threshold* | **dm** *dm-threshold* }

undo crc-alarm-threshold { **es** | **cses** | **dm** }

Parameters

Parameter	Description	Value
es*es-threshold*	Specifies the errored seconds threshold.	The value is an integer that ranges from 1 to 3600. The unit is error seconds per hour. The default value is 432.
cses*cses-threshold*	Specifies the consecutively severely errored seconds threshold.	The value is an integer that ranges from 1 to 60. The unit is consecutively severely errored seconds per hour. The default value is 4.
dm*dm-threshold*	Specifies the degraded minute threshold.	The value is an integer that ranges from 1 to 60. The unit is degraded minutes per hour. The default value is 8.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the errored seconds threshold to 60, consecutively severely errored seconds threshold to 30, and degraded minute threshold to 30 on a VE1 interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] crc-alarm-threshold cses 30
[Huawei-voice-ve1-2/0/0] crc-alarm-threshold es 60
[Huawei-voice-ve1-2/0/0] crc-alarm-threshold dm 30
```

16.2.1.7 display voice port bra

Function

The **display voice port bra** command displays the configuration and status of a BRA interface.

Format

display voice port bra [**state** *slotid/subcardid/portid* | *slotid/subcardid/portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcard ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port bra** command displays existing BRA interfaces.

Example

Display the configuration of a BRA interface.

```
<Huawei> display voice port bra 1/0/0
 Port BRA(Slot/Subcard/Port) 1/0/0
 L2 monitor          : Enable
 Work mode           : P2MP
```

```
Remote power        : Disable
Alarm               : Disable
```

Table 16-17 Description of the display voice port bra command output

Item	Description
L2 monitor	Whether Layer 2 monitoring is enabled on a BRA interface: ● Enable ● Disable
Work mode	Working mode of a BRA interface: ● P2MP ● P2P
Remote power	Whether remote power supply is enabled on a BRA interface: ● Enable ● Disable
Alarm	Whether the UNI alarm function is enabled on a BRA interface: ● Enable ● Disable

16.2.1.8 display voice port fxo

Function

The **display voice port fxo** command displays the configuration and status of an FXO interface.

Format

display voice port fxo [**state** *slotid*|*subcardid*|*portid* | *slotid*|*subcardid*|*portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcardid ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port fxo** command displays existing FXO interfaces.

Example

Display the configuration of an FXO interface.

```
<Huawei> display voice port fxo 2/0/4
 Port FXO config: 2/0/4
 Send gain            : 0dB
 Recv gain            : -3.5dB
 DC impedance         : 50Ω
 AC impedance         : 600
 Ring min duration    : 200ms
 Ring max interval    : Not use
 Ring frequence       : 25Hz
 Ring AC amplitude    : 50V
 Ring offset          : 20V
 Feed max voltage     : -20V
 Feed min voltage     : -80V
 Feed max current     : 35mA
 Feed min current     : 16mA
```

Table 16-18 Description of the display voice port fxo command output

Item	Description
Send gain	Output gain of an FXO interface.
Recv gain	Input gain of an FXO interface.
DC impedance	DC impedance of an FXO interface.
AC impedance	AC impedance of an FXO interface.
Ring min duration	Shortest length of ring currents on an FXO interface.
Ring max interval	Maximum interval between ring currents on an FXO interface.
Ring frequence	Ring current frequency on an FXO interface.
Ring AC amplitude	AC amplitude of the ring current on an FXO interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ring offset	AC offset of the ring current on an FXO interface.
Feed max voltage	Maximum feed voltage of an FXO interface.
Feed min voltage	Minimum feed voltage of an FXO interface.
Feed max current	Maximum feed current of an FXO interface.
Feed min current	Minimum feed current of an FXO interface.

16.2.1.9 display voice port fxs

Function

The **display voice port fxs** command displays the configuration and status of an FXS interface.

Format

display voice port fxs [**state** *slotid/subcardid/portid* | *slotid/subcardid/portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcardid ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port fxs** command displays existing FXS interfaces.

Example

Display the configuration of an FXS interface.

```
<Huawei> display voice port fxs 0/0/0
 Port FXS config: 0/0/0
 Reverse pole pulse level(ms)  : 100
 Line lock                     : Enable
 NLP mode                      : NLP normal mode
 Current(mA)                   : 20mA steady current
 Impedance                     : 600 Ohm interface
 Send gain                     : 0dB
 Receive gain                  : -7dB
 Actual send gain              :
 Actual receive gain           :
```

Table 16-19 Description of the display voice port fxs command output

Item	Description
Reverse pole pulse level(ms)	Polarity reversal pulse level width of an FXS interface.
Line lock	Whether port locking is enabled on an FXS interface: ● Enable ● Disable
NLP mode	Non-linear processing (NLP) mode supported by an FXS interface. ● disable: indicates that NLP is enabled. ● normal: indicates that the DSP processes echoes normally. ● ec-gain-adjust: indicates that the DSP uses a special processing mechanism to perform digit collecting on intelligent public phones. ● enhance: indicates that the DSP enhances NLP. ● reduce: indicates that the DSP reduces NLP.
Current(mA)	Current on an FXS interface.
Impedance	Impedance on an FXS interface.
Send gain	Output gain configured on an FXS interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Receive gain	Input gain configured on an FXS interface.
Actual send gain	Actual output gain of an FXS interface.
Actual receive gain	Actual input gain of an FXS interface.

16.2.1.10 display voice port ve1

Function

The **display voice port ve1** command displays the configuration and status of a VE1 interface.

Format

display voice port ve1 [**state** *slotid|subcardid|portid* | *slotid|subcardid|portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcard ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port ve1** command displays existing VE1 interfaces.

Example

Display the configuration of a VE1 interface.

```
<Huawei> display voice port ve1 2/0/0
 Port VE1(Slot/Subcard/Port) 2/0/0
 Access mode              : Digital
 CRC4                     : Disable
 Impedance                :
75 Ohm
 L2 monitor               : Enable
 Signal type              : CCS
 Idle type                : 7e
 Idle number              : 4
 SA                       : 0 0 0 0 0 0 0 0 0 0
 Invert Tx                : Disable
 Invert Rx                : Disable
 CRC                      : 16
 PCM alarm
 Line fault               : Enable
 Ulf                      : Enable
 Olf                      : Enable
 Ldt                      : Disable
 Frmslip                  : Disable
 Transient event          : Disable

 CRC alarm threshold Es    : 432s
 CRC alarm threshold Cses  : 4s
 CRC alarm threshold Dm    : 8s
```

Table 16-20 Description of the display voice port ve1 command output

Item	Description
Access mode	Access mode of a VE1 interface. ● Digital: indicates the digital section access mode. ● Direct: indicates the direct access mode.
CRC4	Whether CRC4 check is enabled on a VE1 interface. ● Enable ● Disable
Impedance	Impedance on a VE1 interface.
Itf number	Specifies the number of interframe filling tags on the E1-F interface.
Itf type	Specifies the interframe filling tag type on the E1-F interface.
SA	Specifies the content of the five outgoing SA bits in the CRC4 multiframe. (The first five SA bits are incoming bits, which can be queried but cannot be configured. The latter five SA bis are outgoing bits).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Invert	Specifies whether to invert timeslot data of sent or received signaling. ● Tx: Invert timeslot data of sent signaling. ● Rx: Invert timeslot data of received signaling.
CRC	Specifies the CRC mode on the VE1 interface. ● 16: 16-bit CRC is used. ● 32: 32-bit CRC is used. ● none: No CRC is used.
L2 monitor	Whether Layer 2 monitoring is enabled on a VE1 interface: ● Enable ● Disable
Signal type	Signaling mode of a VE1 interface. ● CCS: common channel signaling ● CAS: channel associated signaling
Line fault	Whether calling line identification presentation (CLIP) polarity reversal is enabled: ● Enable ● Disable
Ulf	Whether the alarm on the unconditional line fault bit error rate is enabled: ● Enable ● Disable
Olf	Whether the alarm on the conditional line fault bit error rate is enabled: ● Enable ● Disable
Ldt	Whether the alarm on temporary line interference bit error rate is enabled: ● Enable ● Disable

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Frmslip	Whether the alarm on loss of PCM frames: ● Enable ● Disable
Transient event	Whether the alarm on transient line events is enabled: ● Enable ● Disable
CRC alarm threshold Es	Errored seconds threshold.
CRC alarm threshold Cses	Consecutively severely errored seconds threshold.
CRC alarm threshold Dm	Degraded minute threshold.

16.2.1.11 electric current

Function

Using the **electric current** command, you can set the current for an FXS interface.

Using the **undo electric current** command, you can restore the default current of an FXS interface.

By default, the current of an FXS interface is 20 mA.

Format

electric current *current-value*

undo electric current

Parameters

Parameter	Description	Value
current-value	Specifies the current of an FXS interface.	Enumerated type. The values are 16 mA, 20 mA, 25 mA, 30 mA, 35 mA.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the current of an FXS interface to 16 mA.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric current 16mA
```

16.2.1.12 electric impedance

Function

Using the **electric impedance** command, you can set the impedance for an FXS interface.

Using the **undo electric impedance** command, you can restore the default impedance of an FXS interface.

By default, the impedance of an FXS interface is 600 ohm.

Format

electric impedance *impedance-value*

undo electric impedance

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
impedance-value	Specifies the impedance of an FXS interface.	The value is an integer that ranges from 0 to 15: ● 0: CNOF (200+680|| 100 nF) ● 1: CNUSER (200+560|| 100 nF) ● 2: 600 ohm ● 3: RUSSIA (150+510|| 47 nF) ● 4: (220+820|| 115 nF) ● 5: (220+820|| 120 nF) ● 6: 900 ohm ● 7: BRAZIL (800|| 50 nF) ● 8: BT0 (Zin=87+1052|| 228nF+229||28.4nF, Zload=93+615||\ 471nF+179||495nF +244||32 nF) ● 9: HK_BT3 (Zin=370+620|| 310nf,Zload=600) ● 10: HK_BT5 (Zin=270+264|| 357nf +1434|| 265nf,Zload=600) ● 11: BT1 (BT0 without AGC) ● 12: BT2 (Zin=87+1052||228 nF + 229||28.4nF, Zload=270+264||\ 357 nF + 1434||265 nF) ● 13: BT3(Zin=87+1052|| 228 nF + 229||28.4nF, Zload=164+162||\ 363 nF + 1227||350 nF) ● 14: EUROPE GLOBAL (Zin= 270+750|| 150 nF) ● 15: NEW ZEALAND (Zin=370+620|| 310 nF)

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		NOTE The AR129CV, AR129CVW, and AR129CGVW-L do not support the 1, 8 to 13 parameter value.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the impedance of an FXS interface to 3.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric impedance 3
```

16.2.1.13 electric receive-gain

Function

The **electric receive-gain** command configures the receive gain of an FXS interface.

The **undo electric receive-gain** command restores the default receive gain of an FXS interface.

By default, the receive gain of an FXS interface is –7 dB.

Format

electric receive-gain *recvgain-value*

undo electric receive-gain

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
recvgain-value	Specifies the receive gain of an FXS interface.	The value is an integer that ranges from 0 to 40: ● 0: 0 dB ● 1: –0.5 dB ● 2: –1 dB ● 3: –1.5 dB ● 4: –2 dB ● 5: –2.5 dB ● 6: –3 dB ● 7: –3.5 dB ● 8: –4 dB ● 9: –4.5 dB ● 10: –5 dB ● 11: –5.5 dB ● 12: –6 dB ● 13: –6.5 dB ● 14: –7 dB ● 15: –7.5 dB ● 16: –8 dB ● 17: –8.5 dB ● 18: –9 dB ● 19: –9.5 dB ● 20: –10 dB ● 21: –10.5 dB ● 22: –11 dB ● 23: –11.5 dB ● 24: –12 dB ● 25: –12.5 dB ● 26: –13 dB ● 27: –13.5 dB ● 28: –14 dB ● 29: –14.5 dB ● 30: –15 dB ● 31: –15.5 dB ● 32: –16 dB ● 33: –16.5 dB ● 34: –17 dB ● 35: –17.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 36: –18 dB • 37: –18.5 dB • 38: –19 dB • 39: –19.5 dB • 40: –20 dB **NOTE** The receive gain of an FXS interface on an AR129CV, AR129CVW, AR129CGVW-L, 16-port FXS interface card, or 32-port FXS interface card ranges from –12 dB to 0 dB.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

The receive gain of an FXS interface affects the volume of the voice a local user receives. A smaller value of *recvgain-value* indicates a lower voice.

Example

Set the receive gain of an FXS interface to 0 dB (value 0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric receive-gain 0
```

16.2.1.14 electric send-gain

Function

The **electric send-gain** command configures the send gain of an FXS interface.

The **undo electric send-gain** command restores the default send gain of an FXS interface.

By default, the send gain of an FXS interface is 0 dB.

Format

electric send-gain *sendgain-value*

undo electric send-gain

Parameters

Parameter	Description	Value
sendgain-value	Specifies the send gain of an FXS interface.	The value is an integer that ranges from 0 to 50. ● 0: 5 dB ● 1: 4.5 dB ● 2: 4 dB ● 3: 3.5 dB ● 4: 3 dB ● 5: 2.5 dB ● 6: 2 dB ● 7: 1.5 dB ● 8: 1 dB ● 9: 0.5 dB ● 10: 0 dB ● 11: –0.5 dB ● 12: –1 dB ● 13: –1.5 dB ● 14: –2 dB ● 15: –2.5 dB ● 16: –3 dB ● 17: –3.5 dB ● 18: –4 dB ● 19: –4.5 dB ● 20: –5 dB ● 21: –5.5 dB ● 22: –6 dB ● 23: –6.5 dB ● 24: –7 dB ● 25: –7.5 dB ● 26: –8 dB ● 27: –8.5 dB ● 28: –9 dB ● 29: –9.5 dB ● 30: –10 dB ● 31: –10.5 dB ● 32: –11 dB ● 33: –11.5 dB ● 34: –12 dB ● 35: –12.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 36: –13 dB • 37: –13.5 dB • 38: –14 dB • 39: –14.5 dB • 40: –15 dB • 41: –15.5 dB • 42: –16 dB • 43: –16.5 dB • 44: –17 dB • 45: –17.5 dB • 46: –18 dB • 47: –18.5 dB • 48: –19 dB • 49: –19.5 dB • 50: –20 dB **NOTE** The send gain of an FXS interface on an AR129CVW, AR129CGVW-L, 16-port FXS interface card, or 32-port FXS interface card ranges from –6 dB to 5 dB.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

The send gain of an FXS interface affects the volume of the voice a remote user receives. A smaller value of *sendgain-value* indicates a lower voice.

Example

Set the send gain of an FXS interface to 0 dB (value 10).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric send-gain 10
```

16.2.1.15 feed

Function

Using the **feed** command, you can set feed parameters for an FXO interface.

Using the **undo feed** command, you can restore the default feed parameter settings of an FXO interface.

Format

feed { **maximum-voltage** *max-vol-value* | **minimum-voltage** *min-vol-value* | **minimum-current** *min-current-value* }

undo feed { **maximum-voltage** | **minimum-voltage** | **minimum-current** }

Parameters

Parameter	Description	Value
maximum-voltage *max-vol-value*	Specifies the maximum feed voltage.	The value is an integer that ranges from -100 to 0, in volt. The default value is -20.
minimum-voltage *min-vol-value*	Specifies the minimum feed voltage.	The value is an integer that ranges from -100 to 0, in volt. The default value is -80.
minimum-current *min-current-value*	Specifies the minimum feed current.	The value is an integer that ranges from 6 to 20, in mA. The default value is 10.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the minimum feed voltage of an FXO interface to -50 V.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] feed minimum-voltage -50
```

16.2.1.16 gain

Function

Using the **gain** command, you can set the send gain and receive gain for an FXO interface.

Using the **undo gain** command, you can restore the default send gain and receive gain of an FXO interface.

By default, the send gain and receive gain of an FXO interface are both 0 dB.

Format

gain { **send** *send-value* | **receive** *recvgain-value* }

undo gain { **send** | **receive** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
send *send-value*	Specifies the send gain of an FXO interface.	The value is an integer that ranges from 0 to 60: ● 0: +13.5 dB ● 1: +13.0 dB ● 2: +12.5 dB ● 3: +12.0 dB ● 4: +11.5 dB ● 5: +11.0 dB ● 6:+10.5 dB ● 7:+10.0 dB ● 8: +9.5 dB ● 9: +9.0 dB ● 10: +8.5 dB ● 11: +8.0 dB ● 12: +7.5 dB ● 13: +7.0 dB ● 14: +6.5 dB ● 15: +6.0 dB ● 16: +5.5 dB ● 17: +5.0 dB ● 18: +4.5 dB ● 19: +4.0 dB ● 20: +3.5 dB ● 21: +3.0 dB ● 22: +2.5 dB ● 23: +2.0 dB ● 24: +1.5 dB ● 25: +1.0 dB ● 26: +0.5 dB ● 27: 0 dB ● 28: -0.5 dB ● 29: -1.0 dB ● 30: -1.5 dB ● 31: -2.0 dB ● 32: -2.5 dB ● 33: -3.0 dB ● 34: -3.5 dB ● 35: -4.0 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		● 36: -4.5 dB ● 37: -5.0 dB ● 38: -5.5 dB ● 39: -6.0 dB ● 40: -6.5 dB ● 41: -7.0 dB ● 42: -7.5 dB ● 43: -8.0 dB ● 44: -8.5 dB ● 45: -9.0 dB ● 46: -9.5 dB ● 47: -10.0 dB ● 48: -10.5 dB ● 49: -11.0 dB ● 50: -11.5 dB ● 51: -12.0 dB ● 52: -12.5 dB ● 53: -13.0 dB ● 54: -13.5 dB ● 55: -14.0 dB ● 56: -14.5 dB ● 57: -15.0 dB ● 58: -15.5 dB ● 59: -16.0 dB ● 60: -16.5 dB The default value is 27.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
receive *recvgain-value*	Specifies the receive gain of an FXO interface.	The value is an integer that ranges from 0 to 60: ● 0: +13.5 dB ● 1: +13.0 dB ● 2: +12.5 dB ● 3: +12.0 dB ● 4: +11.5 dB ● 5: +11.0 dB ● 6:+10.5 dB ● 7:+10.0 dB ● 8: +9.5 dB ● 9: +9.0 dB ● 10: +8.5 dB ● 11: +8.0 dB ● 12: +7.5 dB ● 13: +7.0 dB ● 14: +6.5 dB ● 15: +6.0 dB ● 16: +5.5 dB ● 17: +5.0 dB ● 18: +4.5 dB ● 19: +4.0 dB ● 20: +3.5 dB ● 21: +3.0 dB ● 22: +2.5 dB ● 23: +2.0 dB ● 24: +1.5 dB ● 25: +1.0 dB ● 26: +0.5 dB ● 27: 0 dB ● 28: -0.5 dB ● 29: -1.0 dB ● 30: -1.5 dB ● 31: -2.0 dB ● 32: -2.5 dB ● 33: -3.0 dB ● 34: -3.5 dB ● 35: -4.0 dB ● 36: -4.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 37: -5.0 dB • 38: -5.5 dB • 39: -6.0 dB • 40: -6.5 dB • 41: -7.0 dB • 42: -7.5 dB • 43: -8.0 dB • 44: -8.5 dB • 45: -9.0 dB • 46: -9.5 dB • 47: -10.0 dB • 48: -10.5 dB • 49: -11.0 dB • 50: -11.5 dB • 51: -12.0 dB • 52: -12.5 dB • 53: -13.0 dB • 54: -13.5 dB • 55: -14.0 dB • 56: -14.5 dB • 57: -15.0 dB • 58: -15.5 dB • 59: -16.0 dB • 60: -16.5 dB The default value is 27.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the send gain and receive gain of an FXO interface to 12 dB (value 3).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] gain receive 3
[Huawei-voice-fxo1/0/4] gain send 3
```

16.2.1.17 impedance (FXO interface view)

Function

Using the **impedance** command, you can set the DC impedance and AC impedance for an FXO interface.

Using the **undo impedance** command, you can restore the default DC impedance and AC impedance of an FXO interface.

By default, the DC impedance of an FXO interface is 50 nF, and the AC impedance is 600 nF.

Format

impedance { **dc** *value* | **ac** *value* }

undo impedance { **dc** | **ac** }

Parameters

Parameter	Description	Value
dc *value*	Specifies the DC impedance.	The value is 0 or 1: ● 0: 50 nF ● 1: 800 nF The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ac *value*	Specifies the AC impedance.	The value is an integer that ranges from 0 to 15: ● 0: 600 ● 1: 900 ● 2: 270 + (750 || 150 nF) and 275 + (780 || 150 nF) ● 3: 220 + (820 || 120 nF) and 220 + (820 || 115 nF) ● 4: 370 + (620 || 310 nF) ● 5: 320 + (1050 || 230 nF) ● 6: 370 + (820 || 110 nF) ● 7: 275 + (780 || 115 nF) ● 8: 20 + (820 || 110 nF) ● 9: 350 + (1000 || 210 nF) ● 10: 200 + (680 || 100 nF) ● 11: 600 + 2.16 uF ● 12: 900 + 1 uF ● 13: 900 + 2.16 uF ● 14: 600 + 1 uF ● 15: Global impedance The default value is 0.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the DC impedance of an FXO interface to 50 nF (value 0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] impedance DC 0
```

16.2.1.18 impedance (VE1 interface view)

Function

Using the **impedance** command, you can set the impedance for a VE1 interface.

Using the **undo impedance** command, you can restore the default impedance of a VE1 interface.

By default, the impedance of a VE1 interface is 75 ohm.

Format

impedance *impedance-value*

undo impedance

Parameters

Parameter	Description	Value
impedance-value	Specifies the impedance on a VE1 interface.	The value is 75 or 120, in ohm. The default value is 75.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the impedance of a VE1 interface to 75 ohm.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] impedance 75
 Set impendance successfully
```

 Copyright © Huawei Technologies Co., Ltd.

16.2.1.19 invert

Function

The **invert** command sets whether to revert signaling timeslots that are sent and received.

The **undo invert** command restores the default setting.

By default, signaling timeslots that are sent and received are not inverted.

Format

invert { **tx** | **rx** }

undo invert { **tx** | **rx** }

Parameters

Parameter	Description	Value
tx	Configures the AR to invert signaling timeslots that are sent.	-
rx	Configures the AR to invert signaling timeslots that are received.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VE1 interface is connected in PRI mode, you need to configure whether to invert signaling timeslot data as needed, ensuring signaling timeslot interconnecting without bit error or packet loss.

Precautions

Configure whether to invert timeslot data of sent or received signaling on a VE1 interface as needed. By default, signaling timeslot data is not inverted.

Example

#Configure to invert signaling timeslots that are sent and received on the VE1 interface.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] invert tx
  Set invert successfully
[Huawei-voice-ve1-2/0/0] invert rx
  Set invert successfully
```

16.2.1.20 itf(VE1 interface view)

Function

The **itf** command sets the interframe filling tag type and the number of interframe filling tags on the VE1 interface.

Format

itf { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 7.
type	Specifies the interframe filling tag type.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag on a VE1 interface is the code that is sent when no service data is sent through the timeslot bundled to a logical channel.

A VE1 interface supports two types of interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- The same interframe filling tag type and number of interframe filling tags must set for interfaces on both ends; otherwise, communication exceptions may occur.
- Because interframe filling tags occupy bandwidth, the actual data transmission rate on a VE1 interface cannot reach the maximum bandwidth. To improve the actual data transmission rate on a VE1 interface, run the **itf number** command to set the number of interframe filling tags to 0.

Example

Set the interframe filling tag to 0x7e on the VE1 interface and set six interframe filling tags.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] itf type ff
  Set itf successfully
[Huawei-voice-ve1-2/0/0] itf number 6
  Set itf successfully
```

16.2.1.21 l2-monitor

Function

Using the **l2-monitor** command, you can enable or disable Layer 2 monitoring on a BRA interface.

Using the **undo l2-monitor** command, you can restore the default status of Layer 2 monitoring on a BRA interface.

By default, Layer 2 monitoring is enabled on a BRA interface.

Format

l2-monitor { **enable** | **disable** }

undo l2-monitor

Parameters

Parameter	Description	Value
enable	Enables Layer 2 monitoring on a BRA interface.	_
disable	Disables Layer 2 monitoring on a BRA interface.	_

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable Layer 2 monitoring on a BRA interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] l2-monitor enable
```

16.2.1.22 l2-monitor (VE1 interface view)

Function

Using the **l2-monitor** command, you can enable or disable Layer 2 monitoring on a VE1 interface.

Using the **undo l2-monitor** command, you can restore the default status of Layer 2 monitoring on a VE1 interface.

By default, Layer 2 monitoring is enabled on a VE1 interface.

Format

l2-monitor { **enable** | **disable** }

undo l2-monitor

Parameters

Parameter	Description	Value
enable	Enables Layer 2 monitoring on a VE1 interface.	_
disable	Disables Layer 2 monitoring on a VE1 interface.	_

Views

VE1 interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Enable Layer 2 monitoring on a VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] l2-monitor enable
```

16.2.1.23 line-lock

Function

Using the **line-lock** command, you can enable or disable port locking on an FXS interface.

Using the **undo line-lock** command, you can restore the default port locking status on an FXS interface.

By default, port locking is enabled on an FXS interface.

Format

line-lock { **enable** | **disable** }

undo line-lock

Parameters

Parameter	Description	Value
enable	Enables port locking.	_
disable	Disables port locking.	_

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable port locking on an FXS interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] line-lock enable
```

16.2.1.24 loop

Function

The **loop** command sets a port loopback flag.

The **undo loop** command deletes a port loopback flag.

By default, the system does not have any loopback flags.

Format

loop { **remote** | **local** }

undo loop

Parameters

Parameter	Description	Value
remote	Specifies a remote loopback flag.	-
local	Specifies a local loopback flag.	-

Views

BRA, FXS or FXO port view

Default Level

2: Configuration level

Usage Guidelines

You do not need to use this command in normal configurations. This command is mainly used in progressive debugging of call fault points.

Example

Configure remote loopback for an ISDN BRA port.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] loop remote
```

16.2.1.25 nlp-mode

Function

Using the **nlp-mode** command, you can specify the non-linear echo processing (NLP) mode supported by an FXS interface.

Using the **undo nlp-mode** command, you can restore the default NLP mode supported by an FXS interface.

By default, an FXS supports the normal NLP mode.

Format

nlp-mode { **disable** | **normal** | **ec-gain-adjust** | **enhance** | **reduce** }

undo nlp-mode

Parameters

Parameter	Description	Value
disable	Disables the NLP function on an FXS interface so that the digital signal processor (DSP) on the interface does not process non-liner echoes.	_
normal	Indicates the normal NLP mode. In this mode, the DSP processes echoes normally.	_
ec-gain-adjust	Indicates the EC gain adjustment mode. In this mode, the DSP uses a special processing mechanism to perform digit collecting on intelligent public phones.	_
enhance	Indicates the enhanced mode. In this mode, the DSP enhances non-liner echoes.	_
reduce	Indicates the reduction mode. In this mode, the DSP reduces non-liner echoes.	_

 Copyright © Huawei Technologies Co., Ltd.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the NLP mode to normal on an FXS interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] nlp-mode normal
```

16.2.1.26 pcm-alarm

Function

Using the **pcm-alarm** command, you can enable or disable the pulse code modulation (PCM) alarm function on a VE1 interface.

Using the **undo pcm-alarm** command, you can restore the default status of the PCM alarm function on a VE1 interface.

Format

pcm-alarm [**line-fault** *line-fault-value* | **ulf** *ulf-value* | **olf** *olf-value* | **ldt** *ldt-value* | **frmslip** *frmslip-value* | **transient-event** *transient-event-value*]

undo pcm-alarm [**line-fault** | **ulf** | **olf** | **ldt** | **frmslip** | **transient-event**]

Parameters

Parameter	Description	Value
line-fault *line-fault-value*	Enables or disables alarms on line faults.	Enumerated type. The values are as follows: ● disable: disables alarms on line faults. ● enable: enables alarms on line faults. The default value is **enable**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ulf *ulf-value*	Enables or disables alarms on the unconditional line fault bit error rate.	Enumerated type. The values are as follows: ● disable: disables alarms on the unconditional line fault bit error rate. ● enable: enables alarms on the unconditional line fault bit error rate. The default value is **enable**.
olf *olf-value*	Enables or disables alarms on the conditional line fault bit error rate.	Enumerated type. The values are as follows: ● disable: disables alarms on the conditional line fault bit error rate. ● enable: enables alarms on the conditional line fault bit error rate. The default value is **enable**.
ldt *ldt-value*	Enables or disables alarms on the temporary line interference bit error rate.	Enumerated type. The values are as follows: ● disable: disables alarms on the temporary line interference bit error rate. ● enable: enables alarms on the temporary line interference bit error rate. The default value is **disable**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
frmslip *frmslip-value*	Enables or disables alarms on loss of PCM frames.	Enumerated type. The values are as follows: ● disable: disables alarms on loss of PCM frames. ● enable: enables alarms on loss of PCM frames. The default value is **disable**.
transient-event *transient-event-value*	Enables or disables alarms on transient line events.	Enumerated type. The values are as follows: ● disable: disables alarms on transient line events. ● enable: enables alarms on transient line events. The default value is **disable**.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable line fault alarms on a VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] pcm-alarm line-fault enable
```

16.2.1.27 port bra

Function

Using the **port bra** command, you can enter the BRA interface view.

Format

port bra *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port bra** command to view existing BRA interfaces.

Example

Enter the view of BRA interface 2/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 2/0/0
[Huawei-voice-bra-2/0/0]
```

16.2.1.28 port fxo

Function

Using the **port fxo** command, you can enter the FXO interface view.

Format

port fxo*slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcardid ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port fxo** command to view existing FXO interfaces.

Example

Enter the view of FXO interface 2/0/4.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 2/0/4
[Huawei-voice-fxo-2/0/4]
```

16.2.1.29 port fxs

Function

Using the **port fxs** command, you can enter the FXS interface view.

By default, the region identifier is China mainland.

Format

port fxs *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcardid ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port fxs** command to view existing FXS interfaces.

Example

Enter the view of FXS interface 2/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0]
```

16.2.1.30 port ve1

Function

Using the **port ve1** command, you can enter the VE1 interface view.

Format

port ve1 *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port ve1** command to view existing VE1 interfaces.

Example

Enter the view of VE1 interface 2/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0]
```

16.2.1.31 remote-power

Function

Using the **remote-power** command, you can enable the remote power supply function.

Using the **undo remote-power** command, you can restore the default configuration.

By default, the remote power supply function is disabled.

Format

remote-power { **enable** | **disable** }

undo remote-power

Parameters

Parameter	Description	Value
enable	Enables the remote power supply function.	-
disable	Disables the remote power supply function.	-

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

A BRA phone must be powered by a dedicated transformer. If no dedicated transformer is available, run the **remote-power** command to enable the remote power supply function on the BRA interface so that the BRA interface can supply power for BRA phones.

Example

Enable the remote power supply function on a BRA interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] remote-power enable
```

16.2.1.32 reset line-fault

Function

Using the **reset line-fault** command, you can reset line fault alarms.

Format

reset line-fault

Parameters

None

Views

FXS interface view

Default Level

3: Management level

Usage Guidelines

The **reset line-fault** command resets line fault alarms on an FXS interface.

Example

Reset line fault alarms on an FXS interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] reset line-fault
```

16.2.1.33 reverse-pole-pulse level

Function

Using the **reverse-pole-pulse level** command, you can set the polarity reversal pulse level width for an FXS interface.

Using the **undo reverse-pole-pulse level** command, you can restore the default polarity reversal pulse level width of an FXS interface.

By default, the polarity reversal pulse level width of an FXS interface is 100 ms.

Format

reverse-pole-pulse level *level-value*

undo reverse-pole-pulse level

Parameters

Parameter	Description	Value
level *level-value*	Specifies the polarity reversal pulse level width.	The value is an integer that ranges from 20 to 1270, with increments of 10. The unit is ms.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

This command sets the polarity reversal pulse level width for an FXS interface.

Example

Set the polarity reversal pulse level width of an FXS interface to 30 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] reverse-pole-pulse level 30
```

16.2.1.34 ring

Function

Using the **ring** command, you can set ring current parameters on an FXS interface.

Using the **undo ring** command, you can restore the default values of ring current parameters on an FXS interface.

By default, the shortest length of a ring current is 200 ms; the maximum ring current interval is not set; the ring current frequency is 25 Hz; the AC amplitude is 50 V; the AC offset is 70.

Format

ring { **minimum-duration** *min-duration-value* | **maximum-interval** *max-interval-value* | **frequence** *frequence-value* | **ac-amplitude** *ac-amplitude-value* | **offset** *offset-value* }

undo ring { **minimum-duration** | **maximum-interval** | **frequence** | **ac-amplitude** | **offset** }

Parameters

Parameter	Description	Value
minimum-duration *min-duration-value*	Specifies the shortest length of a ring current.	The value is an integer that ranges from 0 to 7: • 0: 100 ms • 1: 150 ms • 2: 200 ms • 3: 256 ms • 4: 384 ms • 5: 512 ms • 6: 640 ms • 7: 1024 ms The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
maximum-interval *max-interval-value*	Specifies the maximum interval between ring currents.	The value is an integer that ranges from 0 to 28: ● 0: not use ● 1: 128 ms ● 2: 256 ms ● 3: 284 ms ● 4: 512 ms ● 5: 640 ms ● 6: 768 ms ● 7: 896 ms ● 8: 1024 ms ● 9: 1152 ms ● 10: 1280 ms ● 11: 1408 ms ● 12: 1536 ms ● 13: 1664 ms ● 14: 1792 ms ● 15: 1920 ms ● 16: 2000 ms ● 17: 2500 ms ● 18: 3000 ms ● 19: 3500 ms ● 20: 4000 ms ● 21: 4500 ms ● 22: 5000 ms ● 23: 6000 ms ● 24: 7000 ms ● 25: 8000 ms ● 26: 9000 ms ● 27: 10000 ms ● 28: 15000 ms The default value is 0.
frequence *frequence-value*	Specifies the ring current frequency.	The value is an integer that ranges from 0 to 2: ● 0: 16 Hz ● 1: 25 Hz ● 2: 50 Hz The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ac-amplitude *ac-amplitude-value*	Specifies the AC Amplitude of a ring current.	The value is an integer that ranges from 0 to 2: ● 0: 74 V ● 1: 65 V ● 2: 50 V The default value is 2.
offset *offset-value*	Specifies the AC offset of a ring current.	The value is an integer that ranges from 0 to 100. The default value is 70.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to set the shortest length of a ring current, maximum interval between ring currents, ring current frequency, AC Amplitude of a ring current, and AC offset of a ring current.

Example

Set the shortest length of a ring current on an FXO interface to 100 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] ring minimum-duration 0
```

16.2.1.35 sa

Function

The **sa** command sets the content of the five outgoing sa bits.

The **undo sa** command restores the default setting.

By default, the content of the five outgoing sa bits is 0.

Format

sa *sa4 sa5 sa6 sa7 sa8*

undo sa

Parameters

Parameter	Description	Value
sa4	Sets the content of the outgoing sa4 bit.	The value is a decimal integer that ranges from 0 to 255.
sa5	Sets the content of the outgoing sa5 bit.	The value is a decimal integer that ranges from 0 to 255.
sa6	Sets the content of the outgoing sa6 bit.	The value is a decimal integer that ranges from 0 to 255.
sa7	Sets the content of the outgoing sa7 bit.	The value is a decimal integer that ranges from 0 to 255.
sa8	Sets the content of the outgoing sa8 bit.	The value is a decimal integer that ranges from 0 to 255.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

When a VE1 interface is connected in PRI mode, if the E1 frame is a CRC4 multiframe, SA4 to SA8 in the E1 multiframe can be used for transmitting low-speed data. By default, the values of SA4 to SA8 are 0. In some scenarios, the remote device will check received SA fields. Therefore, SA fields must be configurable on an AR to ensure normal connection of the VE1 interface.

Precautions

By default, the SA field value is 0. Before configuring the SA field, collect configuration information on the remote device.

Example

Set the content of five outgoing sa bits to 1, 2, 3, 4, and 5 respectively.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] sa 1 2 3 4 5
  Set sa successfully
```

16.2.1.36 shutdown

Function

The **shutdown** command shuts down a BRA port.

 Copyright © Huawei Technologies Co., Ltd.

The **undo shutdown** command restores a BRA port.

Format

shutdown

undo shutdown

Parameters

None

Views

BRA port view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to disable an ISDN BRA port.

Example

Shuts down an ISDN BRA port.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] shutdown
```

16.2.1.37 signal(VE1 interface view)

Function

Using the **signal** command, you can set the signaling mode of a VE1 interface.

Using the **undo signal** command, you can restore the default signaling mode of a VE1 interface.

By default, a VE1 interface uses the common channel signaling (CCS) mode.

Format

signal { **ccs** | **cas** }

undo signal

Parameters

Parameter	Description	Value
ccs	Indicates the common channel signaling mode.	-
cas	Indicates the channel associated signaling mode.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

A VE1 interface can work in CCS or CAS mode. To change the signaling mode, run the **signal** command.

Example

Configure a VE1 interface to work in CCS mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] signal ccs
  Set signal type successfully
```

16.2.1.38 work-mode

Function

Using the **work-mode** command, you can set the working mode for a BRA interface.

Using the **undo work-mode** command, you can restore the default working mode of a BRA interface.

By default, a BRA interface works in point-to-multipoint (P2MP) mode.

Format

work-mode { **p2p** | **p2mp** }

undo work-mode

Parameters

Parameter	Description	Value
p2mp	Indicates the point-to-multipoint (P2MP) mode.	-
p2p	Indicates the point-to-point (P2P) mode.	-

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

This command sets the working mode for a BRA interface.

A BRA interface works in either of the following modes:

- P2MP: Multiple terminals can connect to the BRA interface.
- P2P: Only one terminal can connect to the BRA interface.

Example

Configure a BRA interface to work in P2P mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] work-mode p2p
```

16.3 Voice Configuration Commands

16.3.1 Basic Voice Configuration Commands

16.3.1.1 debugging voice logserver

Function

Using the **debugging voice logserver** command, you can configure the IP address and port number of the log server, and the local IP address.

Format

debugging voice logserver ip *ip-address* **port** *port* **local-ip** *local-ip*

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the IP address of the log server.	The value is a string of 1 to 64 characters.
port *port*	Specifies the port number of the log server.	The value is an integer that ranges from 0 to 65535.
local-ip *local-ip*	Specifies the local IP address.	The value is a string of 1 to 64 characters. The local IP address must be in the signaling IP address pool.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

You can use this command to configure an IP address and a port number of the log server, and a local IP address, then use the Wireshark to capture logs.

Example

Configure the IP address and port number of the log server, and the local IP address.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose]debugging voice logserver ip 192.168.1.1 port 2000 local-ip 192.168.1.2
```

16.3.1.2 debugging voice module-name cmd

Function

The **debugging voice module-name cmd** command enables software debugging of each module.

 Copyright © Huawei Technologies Co., Ltd.

Format

debugging voice module-name cmd *cmd-value* [**p1** *p1-value*] [**p2** *p2-value*] [**p3** p3-value] [**p4** p4-value] [**p5** *p5-value*] [**p6** *p6-value*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
module-name	Specifies the voice module of the debugging messages.	Enumerated type. The values are as follows: • **at0** • **bill** • **billserver** • **bin** • **ccm** • **conference** • **db** • **dss1** • **error** • **h323** • **innertrace** • **lm** • **ms** • **nm** • **pbxmp** • **pbxomshl** • **r2** • **r2rs** • **rm** • **scm** • **sdb** • **sip** • **sipdlg** • **sipem** • **sipmsg** • **sippa** • **siptk** • **ssm** • **sys** • **tam** • **tbcm** • **tkh** • **tpa** • **trace** • **transfer** • **trc**

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• **uam** • **ucbincli** • **userlocation** • **vcm** • **vpm** • **vrm** • **vsppdt** • **ioee** • **vu**
cmd *cmd-value*	Specifies the command value.	The value is an integer that ranges from 0 to 65535.
p1 *p1-value*	Specifies the value of parameter 1.	The value is an integer that ranges from 0 to 4294967295.
p2 *p2-value*	Specifies the value of parameter 2.	The value is an integer that ranges from 0 to 4294967295.
p3 *p3-value*	Specifies the value of parameter 3.	The value is an integer that ranges from 0 to 4294967295.
p4 *p4-value*	Specifies the value of parameter 4.	The value is an integer that ranges from 0 to 4294967295.
p5 *p5-value*	Specifies the value of parameter 5.	The value is a string of 1 to 64 characters.
p6 *p6-value*	Specifies the value of parameter 6.	The value is a string of 1 to 64 characters.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable software debugging for the CCM module.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] debugging voice ccm cmd 0
```

```
->CCM_DebugFunc: dwDebugCmd = 0, dwPara1 = 4294967295, dwPara2 = 4294967295, dwPara3 =
4294967295, dwPara4 = 4294967295
---------------------- CCM Debug Help ----------------------------------------
  0   : print debug help information .......................command parmeters:[-]

---------------------- CCM Block Debug Help ---------------------------------
  1   : show All CCM control block In Used..................command parameters:[-]
  2   : show content of CCM control block ..................command parameters:[p1:ccm no]

---------------------- CCM Timer Debug Help ---------------------------------
  11  : show timer switch of CCM ...........................command parameters:[-]
  12  : set timer switch of CCM ............................command parameters:[-]
  13  : show timer length of CCM ...........................command parameters:[-]
  14  : set ccm timer length to default ....................command parameters:[-]

---------------------- CCM Newservice Debug Help ----------------------------
  21   : show All ringsevice CB In Used.....................command parameters:[-]
  22   : show info of ringsevice CB ........................command parameters:[p1:ringservice no]
  23   : show PickupGroup Stack Info........................command parameters:[-]

---------------------- CCM Bill Debug Help ----------------------------------
  31   : generate bills.....................................command parameters:[P1:bills number(0-5000) P2-CCM No(0-132)]
  32   : show max number length the bill could display .....command parameters:[-]
  33   : modify max number length the bill could display ...command parameters:[p1:length]
  35   : show diameter info by ccm number...................command parameters:[p1:ccm no]
```

16.3.1.3 debugging voice module-name debug-level-value

Function

The **debugging voice module-name debug-level-value** command enables the debug log function for modules.

The **undo debugging voice module-name** command disables the debug log function for modules.

Format

debugging voice *module-name debug-level-value*

debugging voice msgtrace [**caller** *caller-telno*] *debug-level-value*

undo debugging voice *module-name*

undo debugging voice msgtrace

Parameters

Parameter	Description	Value
module-name	Specifies the voice module of the debugging messages.	Enumerated type. The values are as follows: • **at0** • **bill** • **billserver** • **bin** • **cs** • **ccm** • **conference** • **db** • **dss1** • **error** • **h248dmm** • **h248sp** • **h248pa** • **h323** • **innertrace** • **l2ua** • **lm** • **ms** • **nm** • **pbxmp** • **pbxomshl** • **r2** • **r2rs** • **rm** • **scm** • **sdb** • **sip** • **sipbcm** • **sipcc** • **sipcom** • **sipcp** • **sipdlg** • **sipdmm** • **sipem** • **sipmp** • **sipmpc**

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• **sipmsg** • **sippa** • **sipsl** • **siptk** • **snm** • **ssm** • **sys** • **ioee** • **tam** • **tbcm** • **tkh** • **tpa** • **trace** • **transfer** • **trc** • **uam** • **ucbincli** • **userlocation** • **vcm** • **volc** • **vpm** • **vrm** • **vu**
debug-level-value	Specifies the debug log level.	The value can be **error**, **event**, **trace**, or **all**. • error: error level • event: event level • trace: trace level • all: all levels

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the debug log function for the DSS1 module and set the debug log level to all.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] debugging voice dss1 all
```

16.3.1.4 display voice configuration

Function

Using the **display voice configuration** command, you can view global voice parameters.

Format

display voice configuration

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

View global voice parameters.

```
<Huawei> display voice configuration
  Country                 : China-mainland
  Stop initial ring       : Enable
  MWI mode                : FSK without ring
  Flash hook upper        : 1000 ms
  Flash hook lower        : 100 ms
  Park feed               : Disable
  PCM                     : a law
  Ring frequency          : 25HZ
  Ring ac amplitude       : 45Vrms
```

Table 16-21 Description of the **display voice configuration** command output

Item	Description
Country	Region identifier. The following identifiers are supported: ● brazil: Brazil version. ● britain-msfuk: Britain MSFUK version. ● britain-etsi: Britain ESTI version. ● bulgaria: Bulgaria version. ● china-hongkong: China Hongkong version. ● china-mainland: China mainland version. ● egypt: Egypt version. ● france: France version. ● singapore: Singapore version. ● thailand: Thailand version.
Stop initial ring	Stop initial ring
MWI mode	MWI mode
Flash hook upper	Flash hook upper
Flash hook lower	Flash hook lower
Park feed	Park feed
PCM	PCM
Ring frequency	Ring frequency
Ring ac amplitude	Specifies a ringing voltage.

16.3.1.5 display voice debugging

Function

The **display voice debugging** command displays the voice debugging status.

Format

display voice debugging *module-name*

Parameters

Parameter	Description	Value
module-name	Displays debugging messages of the specified voice module.	Enumerated type. The values are as follows: ● at0 ● bill ● billserver ● bin ● ccm ● conference ● db ● dss1 ● h323 ● innertrace ● lm ● ms ● msgtrace ● nm ● pbxmp ● pbxomshl ● r2 ● r2rs ● rm ● scm ● sdb ● sip ● sipdlg ● sipem ● sipmsg ● sippa ● siptk ● ssm ● sys ● tam ● tbcm ● tkh ● tpa ● trace ● transfer ● trc

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• uam • ucbincli • userlocation • vcm • vpm • vrm • vu • all

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

View debugging information about the DSS1 module.

```
<Huawei> display voice debugging dss1
 DSS1  current tracing is disabled.
```

16.3.1.6 display voice diagnostic-information

Function

The **display voice diagnostic-information** command displays the voice diagnostic information.

Format

display voice diagnostic-information

Parameters

None

Views

All view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the voice diagnostic information.

```
<Huawei> display voice diagnostic-information
 ================================================================
  ===============display voice service-mode===============
================================================================
 The voice service mode is PBX.
================================================================
  ===============display voice dsp statistic===============
================================================================
  Slotid/DSP-Index                11/2
  Total                         128
  Idle                          128
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                    0

  Sum of Sub-Board
  Total                         128
  Idle                          128
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                    0
================================================================
  ===============display voice dsp state 11/2===============
================================================================

  Symbol:
     0-idle $-G.711 busy A-All busy W-Wastage X-fault
     @-IP loopback *-PCM loopback #-prohibited

  Channel NO.  DSP channel state
  ---------------------------------------------------------------------
  0000-0049  00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
  0050-0099  00000 00000 00000 00000 00000 00000 00000 00000 00000 00000
  0100-0127  00000 00000 00000 00000 00000 000

  Total:
     128 DSP channel
     128 idle, 0 G.711 Busy, 0 All Busy, 0 Wastage, 0 Fault,
     0   IP loopback, 0 PCM loopback, 0 prohibited
================================================================
```

16.3.1.7 display voice error

Function

The **display voice error** command displays error logs about latest call failures (including the current call).

Format

display voice error

Parameters

None

Views

All view

Default Level

2: Configuration level

Usage Guidelines

When a call fails, run the **display voice error** command to view the error log to rapidly troubleshoot the call failures caused by incorrect configurations.

Example

Display error logs about latest call failures.

```
<Huawei> display voice error
<Huawei> 2016/03/30-14:08:23 AR[N@18][CCM:1]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@53][CCM:2]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
```

16.3.1.8 display voice media-port

Function

The **display voice media-port** command displays the media port number range.

Format

display voice media-port

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the media port number range.

```
<Huawei> display voice media-port
 media-port start 59392 end 62724
```

Table 16-22 Description of the **display voice media-port** command output

Item	Description
media-port start 59392 end 62724	• Start port number • End port number

16.3.1.9 display voice mix-info

Function

The **display voice mix-info** command displays voice mixing information.

Format

display voice mix-info { **port** *slotid*|*dspindex*|*dspchannel* | **dsp** *slotid*|*subcardid*|*portid* }

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display voice mixing information.

```
<Huawei> display voice mix-info port 2/0/0
 media-port start 59392 end 62724
```

Table 16-23 Description of the **display voice mix-info** command output

Item	Description
media-port start 59392 end 62724	• Start port number • End port number

16.3.1.10 display voice online-info

Function

The **display voice online-info** command displays current online user information on the device.

Format

display voice online-info [**callee** *callee-number* | **caller***caller-number*]

Parameters

Parameter	Description	Value
callee *callee-number*	Displays information about called parties.	The value is a string of 1 to 32 characters.
caller *caller-number*	Displays information about calling parties.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display the current online user information on the device.

```
<Huawei> display voice online-info
 Online User Number : 2
 Online Call Information:
 Call type          : INNER
 Caller Service      : NORMAL
 Caller type         : SIPUE
 Caller info         : 214
 Caller DSP          : 0/0/17
```

```
Caller RTP          : 192.168.0.3:62565
Callee Service       : NORMAL
Callee type          : PSTN
Callee info          : 1/0/0
Callee DSP           : -
Callee RTP           : -
Callee CodecType     : G711U
Start time           : 2012-07-16 14:21:58
Call duration (s)    : 0:0:16

Codec                          : G711U
Packetization duration (ms)      : 20
Local IP address: port           : 192.168.0.3:62656
Remote IP address: port          : 192.168.0.1:10002
Total number of Rx RTP bytes     : 756
Total number of Tx RTP bytes     : 120000
Total number of Rx RTP packets   : 756
Total number of Tx RTP packets   : 750
Total number of lost RTP packets : 0
Maximum network jitter (ms)      : 29
Minimum network jitter (ms)      : 17
Maximum loop delay (ms)          : 0
Minimum loop delay (ms)          : 0
Maximum Drop packets Rate (%)    : 0
Minimum Drop packets Rate (%)    : 0
```

Table 16-24 Description of the display voice online-info command output

Item	Description
Online Users Number	Number of online users.
Call type	Call type. For details, see the parameter description in **16.5.1.5 call-type**.
Caller Service	Service type. For details, see the parameter description in **16.5.1.5 call-type**.
Caller type	Caller type.
Caller info	Caller terminal identifier.
Caller DSP	DSP used by the caller terminal.
Caller RTP	IP address and port number in RTP packets received and sent by the calling party.
Callee Service	Service type. For details, see the parameter description in **16.5.1.5 call-type**.
Callee type	Callee type.
Callee info	Callee terminal identifier.
Callee DSP	DSP used by the callee terminal.

Item	Description
Callee RTP	IP address and port number in RTP packets received and sent by the called party.
Callee CodecType	Codec type: ● G711U ● G726 ● G723 ● G711A ● G722 ● G728 ● G729 ● G723Low ● g726-16k ● g726-24k ● g726-32k ● g726-40k ● R2198 ● R2833 ● v150 ● clearmode ● T.38 ● T.38+2
Start time	Start time of a call.
Call duration (s)	Duration in which a call lasts.
Codec	-
Packetization duration (ms)	-
Local IP address: port	Local IP address and port number.
Remote IP address: port	Remote IP address and port number.
Total number of Rx RTP bytes	Total number of bytes received by the local end.
Total number of Tx RTP bytes	Total number of bytes sent by the local end.
Total number of Rx RTP packets	Total number of packets received by the local end.
Total number of Tx RTP packets	Total number of packets sent by the local end.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Total number of lost RTP packets	Total number of discarded RTP packets.
Maximum network jitter (ms)	-
Minimum network jitter (ms)	-
Maximum loop delay (ms)	-
Minimum loop delay (ms)	-
Maximum Drop packets Rate (%)	Maximum packet loss ratio.
Minimum Drop packets Rate (%)	Minimum packet loss ratio.

16.3.1.11 display voice run-stat

Function

display voice run-stat command displays running state information of voice module.

Format

display voice run-stat{ **call-info** | **dsp** | **port** | **proxy-rtp** | **rtp** | **user** }

Parameters

Parameter	Description	Value
call-info	Call-relevant port info	-
dsp	State of dsp channel	-
port	State of port	-
proxy-rtp	RTP port info of media proxy	-
rtp	RTP port info	-

Views

All views

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None.

Example

displays running state information of voice module

```
<Huawei> display voice run-stat call-info
 [DSP statistics]
  Total          DSP channel : 36
  Idle           DSP channel : 33
  Occupy         DSP channel : 1
  Fault          DSP channel : 0
  Waste          DSP channel : 2
  Prohibit       DSP channel : 0
  PCM loopback   DSP channel : 0
  IP loopback    DSP channel : 0

 [RTP port statistics]
  Total  RTP  port : 250
  Idle   RTP  port : 249
  Occupy RTP  port : 1
  Fault  RTP  port : 0

 [PORT statistics]
  Total  port      : 7
  Busy   port      : 0
  Idle   port      : 7
  Fault  port      : 0
  Locked port      : 0
  Other  port      : 0

 [Proxy RTP port statistics]
  Total  RTP  port : 250
  Idle   RTP  port : 250
  Occupy RTP  port : 0
```

Table 16-25 Description of the **display voice run-stat call-info** command output

Item	Description
[DSP statistics]	DSP statistics
Total DSP channel	Total DSP channel number
Idle DSP channel	Idle DSP channel number
Occupy DSP channel	Occupy DSP channel number
Fault DSP channel	Fault DSP channel number
Waste DSP channel	Waste DSP channel number
Prohibit DSP channel	Prohibit DSP channel number
PCM loopback DSP channel	PCM loopback DSP channel number
IP loopback DSP channel	IP loopback DSP channel number
[RTP port statistics]	RTP port statistics
Total RTP port	Total RTP port number

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Idle RTP port	Idle RTP port number
Occupy RTP port	Occupy RTP port number
Fault RTP port	Fault RTP port number
[PORT statistics]	PORT statistics
Total port	Total port number
Busy port	Busy port number
Idle port	Idle port number
Fault port	Fault port number
Locked port	Locked port number
Other port	Other port number
[Proxy RTP port statistics]	Proxy RTP port statistics
Total RTP port	Total RTP port number
Idle RTP port	Idle RTP port number
Occupy RTP port	Occupy RTP port number

16.3.1.12 display voice service-mode

Function

Using the **display voice service-mode** command, you can view the voice service mode.

Format

display voice service-mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The default voice service mode is SIPAG. When configuring voice functions, you must specify the voice service mode.

Example

View the current voice service mode.

```
<Huawei> display voice service-mode
 The voice service mode is PBX.
```

Table 16-26 Description of the **display voice service-mode** command output

Item	Description
The voice service mode is PBX.	Voice service mode. The device supports the following service modes: ● H248AG ● SIP AG ● PBX

16.3.1.13 display voice sip-reg-count-per-second

Function

The **display voice sip-reg-count-per-second** command displays the number of SIP register messages sent every second.

Format

display voice sip-reg-count-per-second

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display the number of SIP register messages sent every second.

```
<Huawei> display voice sip-reg-count-per-second
 Sip register message count per second is 10!
```

16.3.1.14 display voice trace

Function

The **display voice trace** command displays the latest log information about call failures, including error and call logs.

Format

display voice trace

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When a call fails, run the **display voice trace** command to view the call log to rapidly troubleshoot call failures.

Example

Display call logs about latest call failures, including error and call logs.

```
<Huawei> display voice trace
<Huawei> 2016/03/30-14:08:23 AR[N@18][CCM:1]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@53][CCM:2]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@49]------[CCM     :    2]  <-- SETUP             --  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@50]------[CCM     :    2]  -- SETUP_ACK          -->  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@51]------[CCM     :    2]  <-- INFORMATION        --  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@52]------[CCM     :    2]  caller(2003) called(69****412)
<Huawei> 2016/03/30-14:08:30 AR[N@53][CCM:2]###### ERR: Callee number analysis failed,Please check
the configuration of callprefix ######
<Huawei> 2016/03/30-14:08:30 AR[N@54]------[CCM     :    2]  -- RELEASE            -->  [UAM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@55]------[UAM-SIP :    2]  <-- SETUP_ACK          --  [CCM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@56]------[UAM-SIP :    2]  <-- RELEASE            --  [CCM     ]
<Huawei> 2016/03/30-14:08:30 AR[N@57]------[CCM     :    2]  <-- RELEASE_COMPLETE   --  [UAM     ]
```

16.3.1.15 display voice upgrade-info

Function

The **display voice upgrade-info** command displays the configuration that fails to be upgraded after version upgrade.

Format

display voice upgrade-info

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After version upgrade, you can run the **display voice upgrade-info** command to view the configuration that fails to be upgraded.

Example

Display upgrade information.

```
<Huawei> system-view
[Huawei]display voice upgrade-info
[Upgrade-info: Upgrade unsuccessful command]
telno country-code 86 area-code 571 telno-value 6005
[Upgrade-info: End]
```

16.3.1.16 display voice voip-address

Function

Using the **display voice voip-address** command, you can view the configuration of the signaling IP address pool and media IP address pool.

Format

display voice voip-address

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice voip-address** command shows the configuration of the signaling IP address pool and media IP address pool.

Example

Display the configuration of the signaling IP address pool and media IP address pool.

```
<Huawei> display voice voip-address

  IP type          : Media IP
  Method             : Static
  Interface        : GigabitEthernet0/0/1
  IP address       : 192.168.1.1

  IP type          : Signal IP
  Method             : Static
  Interface        : GigabitEthernet0/0/1
  IP address       : 192.168.1.1
```

Table 16-27 Description of the display voice voip-address command output

Item	Description
IP type	IP address pool type: ● Media IP: media IP address pool ● Signal IP: signaling IP address pool
Method	Mode in which an IP address pool is configured: ● Static: The IP address pool is configured statically. ● dynamic: The IP address pool is allocated dynamically.
Interface	Interface where an IP address pool is configured.
IP address	IP addresses in an IP address pool.

 Copyright © Huawei Technologies Co., Ltd.

16.3.1.17 eid-para signalling (PBX user view)

Function

Using the **eid-para signalling** command, you can set the signaling type for a PBX user on a BRA port.

Using the **undo eid-para signalling** command, you can restore the default signaling type of a PBX user on a BRA port.

By default, the signaling type of a PBX user on a BRA port is Digital Subscriber Signalling System No. 1 (DSS1).

Format

eid-para signalling *sigtype*

undo eid-para signalling

Parameters

Parameter	Description	Value
sigtype	Specifies the signaling type.	The value can be: ● dss1 ● qsig

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

You need to configure the signaling type only for PBX users on a BRA port:

- When the device functions as a user-side device and uses DSS1 to connect to a network, set the signaling type to **dss1**.
- When the device functions as a user-side device and uses Q signaling (QSIG) to connect to a network, set the signaling type to **qsig**.

Example

Set the signaling type of a PBX user to QSIG.

```
<system-view> system-view
[Huawei] voice
[Huawei-voice] pbxuser jack
[Huawei-voice-pbxuser-jack] eid-para signalling qsig
```

16.3.1.18 flash-hook lower

Function

Using the **flash-hook lower** command, you can set the lower threshold for hookflash pressing.

Using the **undo flash-hook lower** command, you can restore the default lower threshold for hookflash pressing.

By default, the lower threshold for hookflash pressing is 100 ms.

Format

flash-hook lower *lower-value*

undo flash-hook lower

Parameters

Parameter	Description	Value
lower-value	Specifies the lower hookflash threshold.	The value is an integer that ranges from 50 to 1400, in milliseconds. **NOTE** The value of *lower-value* plus 50 cannot be larger than the value of *upper-value*.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The hookflash can be pressed by a calling party or a called party:

- Hookflash pressed by a called party: If the called party user A wants to transfer an incoming call to user B or another phone, user A can press the hookflash and dial the number of user C.
- Hookflash pressed by a calling party: User A calls user B. User B answers the call and talks with user A. User A can press the hookflash and dial the number of user C after hearing a special dial tone.

After user A presses the hookflash, if user C is busy or does not respond for a long period of time, user A can press the hookflash and talk with user B. If the phone of user C rings, user A hangs up and user B hears the ringback tone. User C picks

 Copyright © Huawei Technologies Co., Ltd.

up the phone and talks with user B. Whether a called party can be transferred to a toll call is restricted by the outgoing right of the called party.

The hookflash function can support the multi-party call service that users on a local network apply for, such as call waiting, call hold, three-party service, and call conference. Centrex users can call only users in the Centrex group.

Example

Set the lower threshold for hookflash pressing to 200 ms on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] flash-hook lower 200
```

16.3.1.19 flash-hook upper

Function

Using the **flash-hook upper** command, you can set the upper threshold for hookflash pressing.

Using the **undo flash-hook upper**command, you can restore the default upper threshold for hookflash pressing.

By default, the upper threshold for hookflash pressing is 350 ms.

Format

flash-hook upper *upper-value*

undo flash-hook upper

Parameters

Parameter	Description	Value
upper-value	Specifies the upper threshold for hookflash pressing.	The value is an integer ranging from 50 to 1400, in milliseconds. **NOTE** The value that ranges from 100 to 1400 is supported by AR129CGVM-L.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The hookflash can be pressed by a calling party or a called party:

- Hookflash pressed by a called party: If the called party user A wants to transfer an incoming call to user B or another phone, user A can press the hookflash and dial the number of user C.
- Hookflash pressed by a calling party: User A calls user B. User B answers the call and talks with user A. User A can press the hookflash and dial the number of user C after hearing a special dial tone.

After user A presses the hookflash, if user C is busy or does not respond for a long period of time, user A can press the hookflash and talk with user B. If the phone of user C rings, user A hangs up and user B hears the ringback tone. User C picks up the phone and talks with user B. Whether a called party can be transferred to a toll call is restricted by the outgoing right of the called party.

The hookflash function can support the multi-party call service that users on a local network apply for, such as call waiting, call hold, three-party service, and call conference. Centrex users can call only users in the Centrex group.

Example

Set the upper threshold for hookflash pressing to 1200 ms on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] flash-hook upper 1200
```

16.3.1.20 load voice-package

Function

The **load voice-package** command loads the voice prompt file.

Format

load voice-package *filename*

Parameters

Parameter	Description	Value
filename	Specifies the voice prompt file to be loaded.	The value is a string of 1 to 64 case-insensitive characters. The file name extension is .res or .cc. The recommended format is drive name:/directory name/file name, for example, flash:/voicepacket.res.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A prompt tone is the voice prompt heard by the calling and called users when the calling user initiates a call. For example, when the calling user calls the called user, the calling user hears the prompt tone indicating that the called user is busy. A voice prompt file stores all voice prompt tones.

The system software has the default voice prompt file. Voice prompt tone rules and services (including three-way conversation, three-party service, teleconference, call transfer, and call waiting) have different usage scenarios in different countries. You can customize the voice prompt file according to service requirements. To make the voice prompt voice file take effect immediately, run the **load voice-package** command to load the files. After loading the voice prompt file, run the **display startup** command to check the loaded voice prompt file according to the Startup voice-files field.

Prerequisites

Before loading the voice prompt file, perform the following operations:

1. Make the voice prompt file and generate a file with file name extension .res or .cc.

   NOTE

   For details about generating the voice prompt file with file name extension .res or .cc, contact technical support personnel.

2. Upload or download the voice prompt file to the device's memory.

Precautions

- When you use the **load voice-package** command to load the voice prompt file, the file take effect immediately after being loaded and the voice prompt file for next startup is modified.
- To restore the default English language, run the **load voice-package** command to load the system software package (.cc file) used for the current startup.

Example

Load voice prompt file **voicepacket.res**.

```
<Huawei> load voice-package voicepacket.res
 Info: Succeeded in activating the file
<Huawei> display startup
 MainBoard:
  Startup system software:                flash:/ar_v2r2c00.cc
  Next startup system software:             flash:/ar_v2r2c00.cc
```

```
Backup system software for next startup:   null
Startup saved-configuration file:          flash:/vrpcfg.zip
Next startup saved-configuration file:     flash:/vrpcfg.zip
Startup license file:                      null
Next startup license file:                 null
Startup patch package:                     null
Next startup patch package:                null
Startup voice-files:                       flash:/voicepacket.res
Next startup voice-files:                  flash:/voicepacket.res
```

16.3.1.21 media-port

Function

The **media-port** command configures a media port number range.

The **undo media-port** command restores the default values of media port number range.

By default, the system allocates a media port number range.

Format

media-port start *start-port-value* **end** *end-port-value*

undo media-port

Parameters

Parameter	Description	Value
start *start-port-value*	Specifies the start media port number.	The value is an integer that ranges from 1025 to 65535. Compatible with older versions whose range for this port value is from 1025 to 65535. **NOTE** Four media port numbers constitute a group, so the start media port number must be a multiple of 4.
end *end-port-value*	Specifies the end media port number.	The value is an integer that ranges from 1025 to 65532.Compatible with older versions whose range for this port value is from 1025 to 65535. **NOTE** Four media port numbers constitute a group, so the end media port number must be a multiple of 4.

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

M indicates the maximum number of online users and N indicates the start media port number (N + M*4 <= 65535).

Example

Set the media port number range to 54000-64000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] media-port start 54000 end 64000
```

16.3.1.22 mwi-mode

Function

Using the **mwi-mode** command, you can set the message waiting indicator (MWI) mode.

Using the **undo mwi-mode** command, you can restore the default MWI mode.

By default, the MWI mode is **fsk-without-ring**, in which the FSK is sent but no ring message is sent.

Format

mwi-mode { **fsk-with-ring** | **fsk-without-ring** }

undo mwi-mode

Parameters

Parameter	Description	Value
fsk-with-ring	Indicates that the FSK and a ring message are sent.	-
fsk-without-ring	Indicates that the FSK is sent but no ring message is sent.	-

Views

Voice view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the MWI mode to **fsk-with-ring**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] mwi-mode fsk-with-ring
```

16.3.1.23 pcm

Function

Using the **pcm** command, you can set the codec mode for voice services.

Using the **undo pcm** command, you can restore the default codec mode for voice services.

By default, the codec mode for voice services is A law.

Format

pcm { **a-law** | **u-law** }

undo pcm

Parameters

Parameter	Description	Value
a-law	Indicates the a-law algorithm.	-
u-law	Indicates the u-law algorithm.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

G.711 defines two compression algorithms: A-law algorithm and u-law algorithm. G.711, also known as Pulse Code Modulation (PCM), is a commonly used

waveform codec. G.711 uses a sampling rate of 8,000 samples per second. Non-uniform quantization (logarithmic) with 8 bits is used to represent each sample, resulting in a 64 kbit/s bit rate.

G.711 defines two main compression algorithms, the μ-law algorithm (used in North America and Japan) and A-law algorithm (used in Europe and the rest of the world). A-law encoding takes a 13-bit signed linear audio sample as input. μ-law encoding takes a 15-bit signed linear audio sample as input.

Example

Set the codec mode to u-law on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pcm u-law
```

16.3.1.24 park-feed

Function

Using the **park-feed** command, you can enable the device to reduce the feed on locked ports or disable this function.

Using the **undo park-feed** command, you can cancel the configuration.

By default, the device reduces the feed on locked ports.

Format

park-feed { **enable** | **disable** }

undo park-feed

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The **park-feed enable** command configures the system to reduce the feed on a Foreign Exchange Station (FXS) port when the port is locked.

NOTE

This function takes effect only for FXS ports.

Example

Disable the device from reducing the feed on locked FXS ports.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] park-feed disable
```

16.3.1.25 save tracelog

Function

The **save tracelog** command saves logs in the error log buffer and call log buffer to the **tracelog.zip** file in the flash memory of the device.

Format

save tracelog

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When a call fails, it is slow to generate error and call logs on the console interface. You can run the **save tracelog** command to save error and call logs in the log buffer to the **flash:/tracelog.zip** file. Technical personnel can export the logs from the device to rapidly troubleshoot the call failure.

Example

Save logs in the error log buffer and call log buffer to the **tracelog.zip** file in the flash memory of the device.

```
<Huawei> save tracelog
```

16.3.1.26 service-mode

Function

Using the **service-mode** command, you can set the voice operation mode.

By default, the voice operation mode is SIPAG mode.

Format

service-mode { **h248ag** | **sipag** | **pbx**}

Parameters

Parameter	Description	Value
h248ag	Indicates the H248AG mode.	-
sipag	Indicates the SIP AG mode.	-
pbx	Indicates the PBX mode.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Before configuring voice functions, you must specify the voice operation mode on the device.

After running the **service-mode** command to switch the voice operation mode of the device, save the configuration and run the **reboot** command in the user view to restart the device.

Example

Set the service mode to PBX.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service-mode PBX
 The modification takes effect only after you save the data and reboot the device.
[Huawei-voice] quit
[Huawei] quit
<Huawei> save
  The current configuration will be written to the device.
  Are you sure to continue? (y/n)[n]:y
  It will take several minutes to save configuration file, please wait.........
  Configuration file had been saved successfully
  Note: The configuration file will take effect after being activated
<Huawei> reboot
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.1.27 sip-reg-count-per-second

Function

The **sip-reg-count-per-second** command sets the number of SIP register messages sent every second.

The **undo sip-reg-count-per-second** command restores the default number of SIP register messages sent every second.

By default, five SIP register messages are sent every second.

Format

sip-reg-count-per-second *reg-count-value*

undo sip-reg-count-per-second

Parameters

Parameter	Description	Value
reg-count-value	Specifies the number of SIP register messages sent every second.	The value is an integer that ranges from 1 to 1024.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the number of SIP register messages sent every second to 3.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip-reg-count-per-second 3
```

16.3.1.28 startup voice-package

Function

The **startup voice-package** command specifies the voice prompt file for next startup.

 Copyright © Huawei Technologies Co., Ltd.

Format

startup voice-package *filename*

Parameters

Parameter	Description	Value
filename	Specifies the voice prompt file for next startup.	The value is a string of 1 to 64 case-insensitive characters. The file name extension is .res or .cc. The recommended format is drive name:/directory name/file name, for example, flash:/voicepacket.res.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A prompt tone is the voice prompt heard by the calling and called users when the calling user initiates a call. For example, when the calling user calls the called user, the calling user hears the prompt tone indicating that the called user is busy. A voice prompt file stores all voice prompt tones.

The system software has the default voice prompt file. Voice prompt tone rules and services (including three-way conversation, three-party service, teleconference, call transfer, and call waiting) have different usage scenarios in different countries. You can customize the voice prompt file according to service requirements. To make the current voice prompt file continue to take effect and the new voice prompt file file take effect during next startup, run the **startup voice-package** command to specify the voice prompt file for next startup. After loading the voice prompt file, run the **display startup** command to check the loaded voice prompt file according to the Next startup voice-files field.

Prerequisites

Before loading the voice prompt file, perform the following operations:

1. Make the voice prompt file and generate a file with file name extension .res or .cc.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

For details about generating the voice prompt file with file name extension .res or .cc, contact technical support personnel.

2. Upload or download the voice prompt file to the device's memory.

Follow-up Procedure

To make the configuration take effect, run the **reboot** command in the user view to restart the device.

Example

Specify the voice prompt file **voicepacket.res** for next startup.

```
<Huawei> startup voice-package flash:/voicepacket.res
 This operation will take several minutes, please wait.........................
 ..
 Info: Succeeded in setting the file for booting system
<Huawei> display startup
 MainBoard:
  Startup system software:                    flash:/ar_v2r2c00.cc
  Next startup system software:               flash:/ar_v2r2c00.cc
  Backup system software for next startup:    null
  Startup saved-configuration file:           flash:/vrpcfg.zip
  Next startup saved-configuration file:      flash:/vrpcfg.zip
  Startup license file:                       null
  Next startup license file:                  null
  Startup patch package:                      null
  Next startup patch package:                 null
  Startup voice-files:                        null
  Next startup voice-files:                   flash:/voicepacket.res
```

16.3.1.29 voice

Function

Using the **voice** command, you can enter the voice view.

Format

voice

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Voice configurations can be performed only in the voice view.

Example

Enter the voice view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]
```

16.3.1.30 voip-address media

Function

Using the **voip-address media** command, you can assign a media IP address pool to an interface.

Using the **undo voip-address media** command, you can delete the media IP address pool of an interface.

Format

voip-address media interface *interface-type interface-number* { *ip-address* | **dynamic** }

undo voip-address media interface *interface-type interface-number* { *ip-address* | **dynamic** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
dynamic	Obtains IP addresses dynamically.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When configuring a media IP address pool:

- To specify the *ip-address* parameter, ensure that an IP address has been configured for the specified interface.

- To specify the **dynamic** parameter, ensure that an IP address has been dynamically assigned to the specified interface.

Example

Assign the media IP address pool 192.168.1.1 to GigabitEthernet 0/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] voip-address media interface GigabitEthernet 0/0/0 192.168.1.1
```

Related Topics

16.3.1.31 voip-address signalling

16.3.1.31 voip-address signalling

Function

Using the **voip-address signalling** command, you can assign a signaling IP address pool to an interface.

Using the **undo voip-address signalling** command, you can delete the signaling IP address pool of an interface.

Format

voip-address signalling interface *interface-type interface-number* { *ip-address* | **dynamic** }

undo voip-address signalling interface *interface-type interface-number* { *ip-address* | **dynamic** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
ip-address	Specifies an IP address.	The value is in dotted decimal notation.
dynamic	Obtains IP addresses dynamically.	-

Views

Voice view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When configuring a signaling IP address pool:

- To specify the *ip-address* parameter, ensure that an IP address has been configured for the specified interface.
- To specify the **dynamic** parameter, ensure that an IP address has been dynamically assigned to the specified interface.

Example

Assign the signaling IP address pool 192.168.1.1 to GigabitEthernet 0/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] voip-address signalling interface GigabitEthernet 0/0/0 192.168.1.1
```

Related Topics

16.3.1.30 voip-address media

16.3.1.32 voip-vpn-instance

Function

The **voip-vpn-instance** command specifies a VPN instance used by voice services.

The **undo voip-vpn-instance** command deletes the VPN instance used by voice services.

By default, no VPN instance is specified to be used by voice services.

Format

voip-vpn-instance *vpn-instance-name*

undo voip-vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The VPN instance must already exist.

Views

Voice view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the interfaces to which specified media IP addresses and signaling IP addresses belong are bound to a VPN instance, you can run the **voip-vpn-instance** command in the voice view to specify the VPN instance to be used by voice services.

Prerequisites

- The VPN instance used by voice services can be configured only when the router works in PBX mode. By default, a router works in PBX mode. If the router does not work in PBX mode, run the **service-mode** command in the voice view to change the work mode of the router to PBX.
- Before running the **voip-vpn-instance** command, run the **ip vpn-instance** command to create a VPN instance.

Precautions

- After a VPN instance is specified to be used by voice services, reset the SIP server and SIP trunk group.
- In the voice view, you can specify only one VPN instance to be used by voice services.

Example

Specify the VPN instance vpn1 to be used by voice services.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] route-distinguisher 22:1
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] voice
[Huawei-voice] voip-vpn-instance vpn1
```

Related Topics

12.9.35 ip vpn-instance

16.3.1.30 voip-address media

16.3.1.31 voip-address signalling

16.3.1.33 undo logserver

Function

Using the **undo logserver** command, you can disable the port for communicating with the log server to stop sending logs to the log server.

Format

undo logserver

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Disable the port for communicating with the log server to stop sending logs to the log server.

```
<Huawei> system-view
[Huawei] diag
[Huawei-diagnose]undo logserver
```

16.3.2 Clip Configuration Commands

16.3.2.1 clip offhook ack-fsk-interval

Function

Using the **clip offhook ack-fsk-interval** command, you can set the interval between the time when the ACK message is received and the time when the frequency-shift keying (FSK) is transmitted in offhook state.

Using the **undo clip offhook ack-fsk-interval** command, you can restore the default interval.

By default, the interval between the time when the ACK message is received and the time when the FSK is transmitted in offhook state is 50 ms.

Format

clip offhook ack-fsk-interval *ack-fsk-interval*

undo clip offhook ack-fsk-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ack-fsk-interval	Specifies the interval between the time when the ACK message is received and the time when the FSK is transmitted in offhook state.	The value is an integer that ranges from 0 to 1000, in milliseconds. The default value is 50.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the interval between the time when the ACK message is received and the time when the FSK is transmitted in offhook state to 200 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook ack-fsk-interval 200
```

16.3.2.2 clip offhook dtas-ack-interval

Function

Using the **clip offhook dtas-ack-interval** command, you can set the maximum duration between the time when the dual tone-alerting signal (DT-AS) is transmitted and the time when the ACK message is received in offhook state.

Using the **undo clip offhook dtas-ack-interval** command, you can restore the default maximum duration.

By default, the maximum duration is 160 ms.

Format

clip offhook dtas-ack-interval *dtas-ack-interval*

undo clip offhook dtas-ack-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-ack-interval	Specifies the maximum duration between the time when the DT-AS is transmitted and the time when the ACK message is received in offhook state.	The value is an integer that ranges from 0 to 1000, in milliseconds. The default value is 160 ms.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the maximum duration between the time when the DT-AS is transmitted and the time when the ACK message is received in offhook state to 500 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook dtas-ack-interval 500
```

16.3.2.3 clip offhook dtas-duration

Function

Using the **clip offhook dtas-duration** command, you can set the duration of the dual tone-alerting signal (DT-AS) in offhook state.

Using the **undo clip offhook dtas-duration** command, you can restore the default duration of the DT-AS in offhook state.

By default, the duration of the DT-AS in offhook state is 80 ms.

Format

clip offhook dtas-duration *dtas-dur-value*

undo clip offhook dtas-duration

Parameters

Parameter	Description	Value
dtas-dur-value	Specifies the duration of the DT-AS in offhook state.	The value is an integer ranging from 0 to 1000, in milliseconds. The default value is 80.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the duration of the DT-AS in offhook state to 200 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook dtas-duration 200
```

16.3.2.4 clip offhook dtas-level

Function

Using the **clip offhook dtas-level** command, you can configure the level of the dual tone-alerting signal (DT-AS) in offhook state.

Using the **undo clip offhook dtas-level** command, you can restore the default level of the DT-AS in offhook state.

By default, the level of the DT-AS in offhook state is 10, that is, -15.5 dBm0.

Format

clip offhook dtas-level *dtas-level*

undo clip offhook dtas-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-level	Specifies the level of the DT-AS in offhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 10.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the DT-AS in offhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook dtas-level 15
```

16.3.2.5 clip offhook fsk-level

Function

Using the **clip offhook fsk-level** command, you can configure the level of the frequency-shift keying (FSK) in offhook state.

Using the **undo clip offhook fsk-level** command, you can restore the default level of the FSK in offhook state.

By default, the level of the FSK in offhook state is 3, that is, -8.5 dBm0.

Format

clip offhook fsk-level *fsk-level*

undo clip offhook fsk-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
fsk-level	Specifies the level of the FSK in offhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 3.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the FSK in offhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook fsk-level 15
```

16.3.2.6 clip offhook mark-signal-bit

Function

Using the **clip offhook mark-signal-bit** command, you can set the number of bits of the FSK synchronization mask in offhook state.

Using the **undo clip offhook mark-signal-bit** command, you can restore the default number of bits of the FSK synchronization mask in offhook state.

By default, the number of bits of the FSK synchronization mask in offhook state is 80.

Format

clip offhook mark-signal-bit *mark-signal-bit*

undo clip offhook mark-signal-bit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mark-signal-bit	Specifies the number of bits of the FSK synchronization mask in offhook state.	The value is an integer that ranges from 0 to 1000. The default value is 80.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of bits of the FSK synchronization mask in offhook state to 200 on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip offhook mark-signal-bit 200
```

16.3.2.7 clip onhook channel-seize-bit

Function

Using the **clip onhook channel-seize-bit** command, you can set the number of bits seized by a channel in onhook state.

Using the **undo clip onhook channel-seize-bit** command, you can restore the default number of bits seized by a channel in onhook state.

By default, the number of bits seized by a channel in onhook state is 300.

Format

clip onhook channel-seize-bit *channel-seize-bit*

undo clip onhook channel-seize-bit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
channel-seize-bit	Specifies the number of bits seized by a channel in onhook state.	The value is an integer that ranges from 0 to 1000. The default value is 300.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of bits seized by a channel in onhook state to 500 on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook channel-seize-bit 500
```

16.3.2.8 clip onhook dtas-duration

Function

Using the **clip onhook dtas-duration** command, you can set the duration of the DT-AS in onhook state.

Using the **undo clip onhook dtas-duration** command, you can restore the default duration of the DT-AS in onhook state.

By default, the duration of the DT-AS in onhook state is 100 ms.

Format

clip onhook dtas-duration *dtas-dur-value*

undo clip onhook dtas-duration

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-dur-value	Specifies the duration of the DT-AS in onhook state.	The value is an integer ranging from 0 to 1000, in milliseconds. The default value is 100.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the duration of the DT-AS in onhook state to 500 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook dtas-duration 500
```

16.3.2.9 clip onhook dtas-fsk-interval

Function

Using the **clip onhook dtas-fsk-interval** command, you can set the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state.

Using the **undo clip onhook dtas-fsk-interval** command, you can restore the default interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state.

By default, the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state is 250 ms.

Format

clip onhook dtas-fsk-interval *dtas-fsk-interval*

undo clip onhook dtas-fsk-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-fsk-interval	Specifies the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state.	The value is an integer ranging from 0 to 1000, in milliseconds. The default value is 250.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted in onhook state to 500 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook dtas-fsk-interval 500
```

16.3.2.10 clip onhook dtas-level

Function

Using the **clip onhook dtas-level** command, you can configure the level of the DT-AS in onhook state.

Using the **undo clip onhook dtas-level** command, you can restore the default level of the DT-AS in onhook state.

By default, the level of the DT-AS in onhook state is 3, that is, -8.5 dBm0.

Format

clip onhook dtas-level *dtas-level*

undo clip onhook dtas-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dtas-level	Specifies the level of the DT-AS in onhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 3.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the DT-AS in onhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook dtas-level 15
```

16.3.2.11 clip onhook fsk-level

Function

Using the **clip onhook fsk-level** command, you can configure the level of the FSK in onhook state.

Using the **undo clip onhook fsk-level** command, you can restore the default level of the FSK in onhook state.

By default, the level of the FSK in onhook state is 3, that is, -8.5 dBm0.

Format

clip onhook fsk-level *fsk-level*

undo clip onhook fsk-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
fsk-level	Specifies the level of the FSK in onhook state.	The value is an integer that ranges from 0 to 15. The value 0 indicates -5.5 dBm0 and the value 15 indicates -20.5 dBm0. The step is 1 dBm0. The default value is 3.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the level of the FSK in onhook state to 15 (-20.5 dBm0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook fsk-level 15
```

16.3.2.12 clip onhook mark-signal-bit

Function

Using the **clip onhook mark-signal-bit** command, you can set the number of bits of the FSK synchronization mask in onhook state.

Using the **undo clip onhook mark-signal-bit** command, you can restore the default number of bits of the FSK synchronization mask in onhook state.

By default, the number of bits of the FSK synchronization mask in onhook state is 180.

Format

clip onhook mark-signal-bit *marksignal-bit*

undo clip onhook mark-signal-bit

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
marksignal-bit	Specifies the number of bits of the FSK synchronization mask in onhook state.	The value is an integer that ranges from 0 to 1000. The default value is 180.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of bits of the FSK synchronization mask in onhook state to 600.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] clip onhook mark-signal-bit 600
```

16.3.2.13 display voice clip

Function

Using the **display voice clip** command, you can view Calling Line Identification Presentation (CLIP) parameters.

Format

display voice clip

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display CLIP parameters on the device.

```
<Huawei> display voice clip
 CLIP onhook parameters:
  DTAS level                  : -8.5dBm0
  FSK level                   : -8.5dBm0
  Channel seize bit           : 300
  Mark signal bit             : 180
  DTAS FSK interval(ms)       : 250
  DTAS duration(ms)           : 100

 CLIP offhook parameters:
  DTAS level                  : -15.5dBm0
  FSK level                   : -8.5dBm0
  Mark signal bit             : 80
  DTAS ack interval(ms)       : 160
  Ack FSK interval(ms)        : 50
  DTAS duration(ms)           : 80
```

Table 16-28 Description of the display voice clip command output

Item	Description
CLIP onhook parameters	CLIP parameters in onhook state.
DTAS level	Level of the DT-AS.
FSK level	Level of the FSK.
Channel seize bit	Number of bits seized by a channel.
Mark signal bit	Number of bits of the FSK synchronization mask.
DTAS FSK interval	Interval between the time when the DT-AS is transmitted and the time when the FSK is transmitted.
DTAS duration	Duration of the DT-AS.
CLIP offhook parameters	CLIP parameters in offhook state.
Ack FSK interval	Interval between the time when the ACK message is received and the time when the FSK is transmitted.
DTAS ack interval	Maximum duration between the time when the DT-AS is transmitted and the time when the ACK message is received.

 Copyright © Huawei Technologies Co., Ltd.

16.3.3 Ring Configuration Commands

16.3.3.1 display voice user-defined-ring

Function

Using the **display voice user-defined-ring** command, you can view the user-defined ring information.

Format

display voice user-defined-ring [*ring-index*]

Parameters

Parameter	Description	Value
ring-index	Specifies the index of a user-defined ring.	The value is an integer that ranges from 0 to 15.

Views

All views

Default Level

3: Management level

Usage Guidelines

If *ring-index* is not specified, information about all user-defined rings is displayed.

Example

Display information about user-defined ring 1.

```
<Huawei> display voice user-defined-ring 1
      First-ring(ms)  Second-ring(ms) Third-ring(ms)
 Index Ring   Interval  Ring  Interval  Ring  Interval
 1     0      0         0     0         0     0
```

Display information about user-defined rings.

```
<Huawei> display voice user-defined-ring
       First-ring(ms)  Second-ring(ms) Third-ring(ms)
 Index Ring   Interval  Ring  Interval  Ring  Interval
 0     0      0         0     0         0     0
 1     0      0         0     0         0     0
 2     0      0         0     0         0     0
 3     0      0         0     0         0     0
 4     0      0         0     0         0     0
 5     0      0         0     0         0     0
 6     0      0         0     0         0     0
 7     0      0         0     0         0     0
```

 Copyright © Huawei Technologies Co., Ltd.

```
8    0     0       0    0       0    0
9    0     0       0    0       0    0
10   0     0       0    0       0    0
11   0     0       0    0       0    0
12   0     0       0    0       0    0
13   0     0       0    0       0    0
14   0     0       0    0       0    0
15   0     0       0    0       0    0
```

Table 16-29 Description of the display voice user-defined-ring command output

Item	Description
Index	Index of the user-defined ring.
First-ring	Duration of the first ring tone.
Second-ring	Duration of the second ring tone.
Third-ring	Duration of the third ring tone.
Ring	Ringing duration.
Interval	Duration after ringing stops.

16.3.3.2 ring frequency

Function

Using the **ring frequency** command, you can set the frequency of the ringing current.

Using the **undo ring frequency** command, you can restore the default frequency of the ringing current.

By default, the frequency of the ringing current is 25 Hz.

Format

ring frequency { **16hz** | **25hz** | **50hz** }

undo ring frequency

Parameters

Parameter	Description	Value
16hz	Indicates that the frequency of the ringing current is 16 Hz.	-
25hz	Indicates that the frequency of the ringing current is 25 Hz.	-

Parameter	Description	Value
50hz	Indicates that the frequency of the ringing current is 50 Hz.	-

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

A higher frequency of the ringing current indicates a sharper ring tone.

Example

Set the frequency of the ringing current on the device to 16 Hz.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring frequency 16hz
```

16.3.3.3 ring voltage

Function

The **ring voltage** command configures the ringing voltage.

The **undo ring voltage** command restores the default ringing voltage.

By default, the ringing voltage is 45 Vrms. On the AR169FVW-8S, the default ringing voltage is 50 Vrms.

Format

ring voltage *voltage-value*

undo ring voltage

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
voltage-value	Specifies a ringing voltage.	Enumerated type. The value can be: • 65 Vrms • 53 Vrms • 50 Vrms • 45 Vrms **NOTE** Only 129CGVW-L, AR129CVW and AR129CV support 53 Vrms.

Views

Voice views

Default Level

2: Configuration level

Usage Guidelines

When the default ringing voltage cannot meet requirements, you can run the **ring voltage** command to change the ringing voltage as required. You can run the **display voice configuration** command to verify the current ringing voltage configured on a device.

Example

Set the ringing voltage to 50 Vrms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring voltage 50Vrms
```

Related Topics

16.3.1.4 display voice configuration

16.3.3.4 stop-initial-ring enable

Function

Using the **stop-initial-ring enable** command, you can disable the initial ringing function.

Using the **stop-initial-ring disable** command, you can enable the initial ringing function.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo stop-initial-ring** command, you can restore the default initial ringing function.

By default, the initial ringing function is disabled.

Format

stop-initial-ring { **enable** | **disable** }

undo stop-initial-ring

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the initial ringing function on the device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] stop-initial-ring disable
```

16.3.3.5 user-defined-ring

Function

Using the **user-defined-ring** command, you can set the cadence ratio of the specified user-defined ring type.

Using the **undo user-defined-ring** command, you can delete the cadence ratio of the specified user-defined ring type.

Format

user-defined-ring *ring-index* { **first-ring** *first-ring-period* | **first-interval** *first-interval* | **second-ring** *second-ring-period* | **second-interval** *second-interval* | **third-ring** *third-ring-period* | **third-interval** *third-interval* }*

undo user-defined-ring *ring-index* { **first-ring** | **first-interval** | **second-ring** | **second-interval** | **third-ring** | **third-interval** }*

Parameters

Parameter	Description	Value
ring-index	Specifies the index of the user-defined ring type.	The value is an integer that ranges from 0 to 15.
first-ring *first-ring-period*	Specifies the duration of the first ring tone.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds. The value 0 indicates that the first ring tone is canceled.
first-interval *first-interval*	Specifies the duration after the first ring stops.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
second-ring *second-ring-period*	Specifies the duration of the second ring tone.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
second-interval *second-interval*	Specifies the duration after the second ring stops.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
third-ring *third-ring-period*	Specifies the duration of the third ring tone.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.
third-interval *third-interval*	Specifies the duration after the third ring stops.	The value can be 0 or an integer that ranges from 200 to 12750, in milliseconds.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can set different ring types based on the ringing duration.

The **ring-mode** command can reference the cadence ratio configured by the **user-defined-ring** command. The *cadencering-value* values 128 to 143 in the **ring-mode** command correspond to *index* values 0 to 15 in the **user-defined-ring**.

The *initialring-value* values 144 to 159 in the **ring-mode** command correspond to *index* values 0 to 15 in the **user-defined-ring** command.

The device supports the following combinations:

- 1-segment ringing: **first-ring**
- 2-segment ringing: **first-ring** + **first-interval**
- 4-segment ringing: **first-ring** + **first-interval** + **second-ring** + **second-interval**
- 6-segment ringing: **first-ring** + **first-interval** + **second-ring**+**second-interval** + **third-ring** + **third-interval**

Example

Configure user-defined ring 0 as 6-segment ringing and set the cadence ratio to 200:200:200:200:200:200.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] user-defined-ring 0 first-ring 200 first-interval 200 second-ring 200 second-interval 200 third-ring 200 third-interval 200
```

16.3.4 Upward-bandwidth Configuration Commands

16.3.4.1 display voice media-bandwidth-control

Function

Using the **display voice media-bandwidth-control** command, you can view the call restriction configuration when the uplink bandwidth is insufficient.

Format

display voice media-bandwidth-control

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display voice media-bandwidth-control** command only after the **media-bandwidth-control enable** command is executed to enable the call restriction function when the uplink bandwidth is insufficient.

Example

Display the call restriction configuration when the uplink bandwidth is insufficient.

```
<Huawei> display voice media-bandwidth-control
 Upward bandwidth                          : disable
 The maximum upward bandwidth              : 100000 kbit/s
 The reserved bandwidth for emergency call : 1000 kbit/s
 The used normal bandwidth                 : 0 kbit/s
 The used bandwidth for emergency call     : 0 kbit/s
```

Table 16-30 Description of the display voice upward-bandwidth command output

Item	Description
Upward bandwidth	Whether call restriction is enabled when the uplink bandwidth is insufficient. ● enable: call restriction is enabled when the uplink bandwidth is insufficient. ● disable: call restriction is disabled when the uplink bandwidth is insufficient.
The maximum upward bandwidth	Maximum uplink bandwidth.
The reserved bandwidth for emergency call	Reserved bandwidth for emergency calls.
The used normal bandwidth	Used bandwidth.
The used bandwidth for emergency call	Used bandwidth for emergency calls.

16.3.4.2 media-bandwidth-control enable

Function

Using the **media-bandwidth-control enable** command, you can enable the call restriction function when the uplink bandwidth is insufficient or disable this function.

Using the **media-bandwidth-control disable** command, you can cancel the configuration.

By default, the call restriction function is disabled when the uplink bandwidth is insufficient.

Format

media-bandwidth-control enable

media-bandwidth-control disable

Parameters

None

Views

Trunk-group view or sipserver view

Default Level

2: Configuration level

Usage Guidelines

Before running the **16.3.4.3 media-bandwidth-control max-bandwidth** command to set the maximum uplink bandwidth, you must run the **media-bandwidth-control enable** command.

Example

Enable the call restriction function when the uplink bandwidth is insufficient.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] media-bandwidth-control enable
```

16.3.4.3 media-bandwidth-control max-bandwidth

Function

Using the **media-bandwidth-control max-bandwidth** command, you can set the maximum uplink bandwidth.

Using the **undo media-bandwidth-control max-bandwidth** command, you can restore the default maximum uplink bandwidth.

By default, the maximum uplink bandwidth is 100000 kbit/s.

Format

media-bandwidth-control max-bandwidth *max-bandwidth*

undo media-bandwidth-control max-bandwidth

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-bandwidth	Specifies the maximum uplink bandwidth.	The value is an integer that ranges from 1 to 5000, in 100 kbit/s. The default value is 1000, that is, 100000 kbit/s.

Views

trunk-group view or sipserver view

Default Level

2: Configuration level

Usage Guidelines

Before running the **media-bandwidth-control max-bandwidth** command, you must run the **media-bandwidth-control enable** command to enable the call restriction function when the uplink bandwidth is insufficient.

When the common bandwidth is overloaded, calls of common users are rejected. Emergency calls can be resumed within the range of the reserved bandwidth. (Common bandwidth = Maximum uplink bandwidth - Reserved bandwidth for emergency calls)

NOTE

Even if the remaining bandwidth is insufficient, the system allows the last call to be connected.

Example

Set the maximum uplink bandwidth to 90000 kbit/s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]sipserver
[Huawei-voice-sipserver]media-bandwidth-control enable
[Huawei-voice-sipserver]media-bandwidth-control max-bandwidth 900
```

16.3.5 Sip Stack Configuration Commands

16.3.5.1 display voice sip

Function

Using the **display voice sip** command, you can view the configuration of Session Initiation Protocol (SIP) parameters.

Format

display voice sip

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the configuration of SIP parameters on the device.

```
<Huawei> display voice sip
 SIP stack parameter & timers:
  Server header field                    :
  Organization header field              :
  User-agent header field                :
  Max-forwards header field              : 70
  Headline folding flag                  : Disable
  T1 timer(ms)                           : 500
  T2 timer(ms)                           : 4000
  T4 timer(ms)                           : 5000
  TD timer(ms)                           : 32000
  Min-SE timer(s)                        : 90
  Session progress timer(s)              : 180
  Session reliable progress timer(s)     : 60
  Entity based session timer flag        : Disable
  To header strict check flag            : Disable
```

Table 16-31 Description of the display voice sip command output

Item	Description
SIP stack parameter & timers	SIP stack parameter and values of timers.
Server header field	Value of the Server header field.
Organization header field	Value of the Organization header field.
User-agent header field	Value of the User-agent header field.
Max-forwards header field	Value of the Max-forwards header field.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Headline folding flag	Header folding flag in the authentication header field.
Entity based session timer flag	Whether the session timer defined by RFC 4028 based on the user agent (UA) is started.
T1 timer(ms)	T1 timer, which defines the estimated round-trip timer (RTT) time. For details, see RFC 3261.
T2 timer(ms)	T2 timer, which defines the maximum interval at which non-INVITE request messages and INVITE response messages are retransmitted. For details, see RFC 3261.
T4 timer(ms)	T4 timer, which defines the maximum duration a message will remain on a network. For details, see RFC 3261.
TD timer(ms)	TD timer, which defines the waiting time for retransmitting response messages. For details, see RFC 3261.
Min-SE timer(s)	Minimum value for the session interval. For details, see RFC 4028.
Session progress timer(s)	Unreliable provisional response retransmission timer, which determines the frequency for retransmitting unreliable provisional responses. For details, see RFC 3261.
Session reliable progress timer(s)	Reliable provisional response retransmission timer, which determines the frequency for retransmitting reliable provisional responses. For details, see RFC 3261.
To header strict check flag	Whether the To header field of the SIP protocol is strictly checked.

16.3.5.2 entity-based-sessions-timer

Function

Using the **entity-based-sessions-timer** command, you can enable the session timer defined by RFC4028 based on the UA or disable this function.

undo entity-based-sessions-timer command, you can disable the session timer defined by RFC4028 based on the UA.

 Copyright © Huawei Technologies Co., Ltd.

By default, the session timer defined by RFC4028 based on the UA is disabled.

Format

entity-based-sessions-timer { **enable** | **disable** }

undo entity-based-sessions-timer

Parameters

None

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the session timer defined by RFC4028 based on the UA.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] entity-based-sessions-timer enable
```

16.3.5.3 field-header max-forwards

Function

Using the **field-header max-forwards** command, you can set the value of the Max-forwards header field.

Using the **undo field-header max-forwards** command, you can restore the default value of the Max-forwards header field.

By default, the value of the Max-forwards header field is 70.

Format

field-header max-forwards *max-forwards-value*

undo field-header max-forwards

Parameters

Parameter	Description	Value
max-forwards-value	Specifies the value of the Max-forwards header field.	The value is an integer that ranges from 0 to 255.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the Max-forwards header field to 90.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header max-forwards 90
```

16.3.5.4 field-header organization

Function

Using the **field-header organization** command, you can set the value of the Organization header field.

Using the **undo field-header organization** command, you can restore the default value of the Organization header field.

By default, the value of the Organization header field is empty.

Format

field-header organization *organization-head*

undo field-header organization

Parameters

Parameter	Description	Value
organization-head	Specifies the value of the Organization header field.	The value is a string of 1 to 64 characters. **NOTE** If the hyphen (-) is entered, the value of the Organization header field is deleted.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the Organization header field in the SIP stack to OrganizationTemp.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header organization OrganizationTemp
```

16.3.5.5 field-header server

Function

Using the **field-header server** command, you can set the value of the Server header field.

Using the **undo field-header server** command, you can restore the default value of the Server header field.

By default, the value of the Server header field is empty.

Format

field-header server *server-head*

undo field-header server

Parameters

Parameter	Description	Value
server-head	Specifies the value of the Server header field.	The value is a string of 1 to 64 characters. **NOTE** If the hyphen (-) is entered, the value of the Server header field is deleted.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the Server header field in the SIP stack to HuaweiServerV2.0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header server huaweiserverv2.0
```

16.3.5.6 field-header user-agent

Function

Using the **field-header user-agent** command, you can set the value of the User-agent header field.

Using the **undo field-header user-agent** command, you can restore the default value of the User-agent header field.

By default, the value of the User-agent header field is empty.

Format

field-header user-agent *user-agent-head*

undo field-header user-agent

Parameters

Parameter	Description	Value
user-agent-head	Specifies the value of the User-agent header field.	The value is a string of 1 to 64 characters. **NOTE** If the hyphen (-) is entered, the value of the User-agent header field is deleted.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The settings of header fields must comply with RFC3261.

Example

Set the value of the User-agent header field in the SIP stack to SoftPhone V2.0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] field-header user-agent softphoneV2.0
```

16.3.5.7 header-folding

Function

Using the **header-folding** command, you can enable header folding in the authentication header field or disable this function.

Using the **undo header-folding** command, you can cancel the configuration.

By default, header folding in the authentication header field is disabled.

Format

header-folding { enable | disable }

undo header-folding

Parameters

None

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable header folding in the authentication header field.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] header-folding enable
```

16.3.5.8 min-se

Function

Using the **min-se** command, you can set the minimum value of the session timer.

Using the **undo min-se** command, you can restore the default minimum value of the session timer.

By default, the minimum value of the session timer is 90s.

Format

min-se *min-se-period*

undo min-se

Parameters

Parameter	Description	Value
min-se-period	Specifies the minimum value of the session timer.	The value is an integer that ranges from 90 to 86400, in seconds. The default value is 90.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the minimum value of the session timer to 90s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] min-se 90
```

16.3.5.9 session-progress

Function

Using the **session-progress** command, you can set the value of the unreliable provisional response retransmission timer.

Using the **undo session-progress** command, you can restore the default value of the unreliable provisional response retransmission timer.

By default, the value of the unreliable provisional response retransmission timer is 180s.

Format

session-progress *session-progress-period*

undo session-progress

Parameters

Parameter	Description	Value
session-progress-period	Specifies the value of the unreliable provisional response retransmission timer.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 180.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the value of the unreliable provisional response retransmission timer to 90s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] session-progress 90
```

16.3.5.10 session-rel-progress

Function

Using the **session-rel-progress** command, you can set the value of the reliable provisional response retransmission timer.

Using the **undo session-rel-progress** command, you can restore the default value of the reliable provisional response retransmission timer.

By default, the value of the reliable provisional response retransmission timer is 60s.

Format

session-rel-progress *session-rel-progress-period*

undo session-rel-progress

Parameters

Parameter	Description	Value
session-rel-progress-period	Specifies the value of the reliable provisional response retransmission timer.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 60.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the value of the reliable provisional response retransmission timer to 90s.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] sip
[Huawei-voice-sip] session-rel-progress 90
```

16.3.5.11 sip

Function

Using the **sip** command, you can enter the SIP view.

Format

sip

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

SIP stack parameters are set in the SIP view.

Example

Enter the SIP view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip]
```

16.3.5.12 to-header-check-flag

Function

The **to-header-check-flag** command enables or disables strict check on the To header in SIP.

Using the **undo to-header-check-flag** command, you can cancel the configuration.

By default, strict check on the To header in SIP is disabled.

Format

to-header-check-flag { **enable** | **disable** }

undo to-header-check-flag

Parameters

None

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable strict check on the To header in SIP.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] to-header-check-flag enable
```

16.3.5.13 t1

Function

Using the **t1** command, you can set the value of the T1 timer.

Using the **undo t1** command, you can restore the default value of the T1 timer.

By default, the value of the T1 timer is 500 ms.

Format

t1 *t1-period*

undo t1

Parameters

Parameter	Description	Value
t1-period	Specifies the value of the T1 timer.	The value is an integer that ranges from 200 to 10000, in milliseconds. The default value is 500 ms.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The T1 timer defines the estimated round-trip timer (RTT) time.

Example

Set the value of the T1 timer to 1000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] t1 1000
```

16.3.5.14 t2

Function

Using the **t2** command, you can set the value of the T2 timer.

Using the **undo t2** command, you can restore the default value of the T2 timer.

By default, the value of the T2 timer is 4000 ms.

Format

t2 *t2-period*

undo t2

Parameters

Parameter	Description	Value
t2-period	Specifies the value of the T2 timer.	The value is an integer that ranges from 200 to 10000, in milliseconds. The default value is 4000 ms.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The T2 timer defines the maximum interval at which non-INVITE request messages and INVITE response messages are retransmitted.

Example

Set the value of the T2 timer to 1000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] t2 1000
```

16.3.5.15 t4

Function

Using the **t4** command, you can set the value of the T4 timer.

Using the **undo t4** command, you can restore the default value of the T4 timer.

By default, the value of the T4 timer is 5000 ms.

Format

t4 *t4-period*

undo t4

Parameters

Parameter	Description	Value
t4-period	Specifies the value of the T4 timer.	The value is an integer that ranges from 200 to 10000, in milliseconds. The default value is 5000 ms.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The T4 timer defines the maximum duration a message will remain on a network.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the T4 timer to 6000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] t4 6000
```

16.3.5.16 td

Function

Using the **td** command, you can set the value of the TD timer.

Using the **undo td** command, you can restore the default value of the TD timer.

By default, the value of the TD timer is 32000 ms.

Format

td *td-period*

undo td

Parameters

Parameter	Description	Value
td-period	Specifies the value of the TD timer.	The value is an integer that ranges from 0 to 300000, in milliseconds. The default value is 32000 ms. **NOTE** If UDP is used, the value must be greater than or equal to 32000. If TCP/SCTP is used, the value is 0.

Views

SIP view

Default Level

2: Configuration level

Usage Guidelines

The TD timer defines the waiting time for retransmitting response messages.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the TD timer to 60000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip
[Huawei-voice-sip] td 60000
```

16.3.6 Dsp Configuration Commands

16.3.6.1 display voice dsp state

Function

The **display voice dsp state** command displays the status of a digital signal processor (DSP) or DSP channel.

Format

display voice dsp state { *slot/dsp-index* | **channel***slot/dsp-index/channel* }

Parameters

Parameter	Description	Value
slot/dsp-index	Specifies the slot ID and index of a DSP.	The value is a string of 1 to 15 case-insensitive characters. For example, if the slot ID is 0 and the DSP index is 0, the value is 0/0.
channel*slot/dsp-index/channel*	Specifies the slot ID, DSP index, and DSP channel index.	The value is a string of 1 to 15 case-insensitive characters. For example, if the slot ID is 0, the DSP index is 0, and the DSP index is 5, the value is 0/0/5.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the status of DSP 0/0.

```
<Huawei> display voice dsp state 0/0

 Symbol:
    0-idle $-G.711 busy A-All busy W-Wastage X-fault
    @-IP loopback *-PCM loopback #-prohibited

 Channel NO.  DSP channel state
 ---------------------------------------------------------------------
 0000-0035  00000 00000 00000 00000 00000 00000 00000 0

 Total:
    36  DSP channel
    36  idle, 0 G.711 Busy, 0 All Busy, 0 Wastage, 0 Fault,
    0   IP loopback, 0 PCM loopback, 0 prohibited
```

Table 16-32 Description of the display voice dsp state command output

Item	Description
0-idle	0 indicates that the DSP channel is in idle state.
$-G.711	$ indicates that the DSP channel works in G.711 codec state.
A-All busy	A indicates that the DSP channel works in non-G.711 codec state, such as the G.729 and G.723 codec state.
W-Wastage	W indicates that the the DSP channel is in wastage state, for example, G.729 codec may consume extra DSP channels.
X-fault	X indicates that the DSP channel is in faulty state, and a call cannot be connected through the DSP channel.
@-IP loopback	@ indicates that the DSP channel works in IP loopback state.
*-PCM loopback	* indicates that the DSP channel works in PCM loopback state.
#-prohibited	# indicates that the DSP channel is in prohibited state.
Channel NO	Number of a channel.
DSP channel state	DSP channel status displayed in graphs.

The AR150/200 series has the DSP chip. The following figure lists the maximum number of calls supported by the DSP chip in each codec state and packetization duration.

Table 16-33 Maximum number of calls supported by the AR150/200 series DSP chip in each codec state and packetization duration

Codec	5 ms	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	8	8	8	8	8	8	8
G723	-	-	-	8	-	-	8
G726	-	8	8	8	8	8	8
G729	-	8	8	8	8	8	8

The AR1200 series has the DSP chip. The following figure lists the maximum number of calls supported by the DSP chip in each codec state and packetization duration.

Table 16-34 Maximum number of calls supported by the AR1200 series DSP chip in each codec state and packetization duration

Codec	5 ms	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	32	32	32	32	32	32	32
G723	-	-	-	12	-	-	12
G726	-	12	12	12	12	12	12
G729	-	32	32	32	32	32	32

A DSP slot on the AR2200 and AR3200 series supports up to 128-channel DSP chip. The following figure lists the maximum number of calls supported by the DSP chip in each codec state and packetization duration.

Table 16-35 Maximum number of calls supported by the 128-channel DSP chip in each codec state and packetization duration

Codec	5 ms	10 ms	20 ms	30 ms	40 ms	50 ms	60 ms
G.711	32	72	128	128	128	72	128
G723	-	-	-	36	-	-	36
G726	-	36	48	48	48	48	48
G729	-	32	32	32	32	32	32

NOTE

AR2201 and AR2202 do not support the voice feature because they have no DSP slot.

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.2 display voice dsp statistic

Function

Using the **display voice dsp statistic** command, you can view the DSP statistics.

Format

display voice dsp statistic [*slotid|dsp-index*]

Parameters

Parameter	Description	Value
slotid|dsp-index	Specifies the slot ID and index of a DSP.	The value is a string of 1 to 15 case-insensitive characters. For example, if the slot ID is 0 and the DSP index is 0, the value is 0/0.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the statistics about all DSPs.

```
<Huawei> display voice dsp statistic
  Slotid/DSP-Index                0/0
  Total                         108
  Idle                          108
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                      0
  Sum of Sub-Board
  Total                         108
  Idle                          108
  G.711 busy                      0
  All busy                      0
  Wastage                         0
  Fault                         0
  Loop back                       0
  Prohibited                      0
```

16.3.6.3 display voice dsp-attribute

Function

Using the **display voice dsp-attribute** command, you can view the configuration of DSP parameters.

Format

display voice dsp-attribute

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the configuration of DSP parameters.

```
<Huawei> display voice dsp-attribute
 DSP code type                                  : G711A
 DSP RTP packet interval(ms)                    : 20
 T30 redundancy parameter value of T38 fax      : 3
 T4 redundancy parameter value of T38 fax       : 3
 Fax ECM                                        : Enable
 Fax train mode                                 : E2E train
 Fax max train rate                             : V17
 Fax V8 negotiate                               : Disable
 DSP min adapted jitter buffer(ms)              : 2
 DSP max adapted jitter buffer(ms)              : 135
 DSP init adapted jitter buffer(ms)             : 2
 DSP adapted jitter buffer threshold(ms)        : 150
 DSP min fixed jitter buffer(ms)                : 2
 DSP max fixed jitter buffer(ms)                : 135
 DSP init fixed jitter buffer(ms)               : 60
 DSP redundancy payload value                   : 96
 DSP NTE payload value                          : 97
 DSP clearmode payload value                    : 100
 DSP G.726-16k payload value                    : 103
 DSP G.726-24k payload value                    : 104
 DSP G.726-32k payload value                    : 101
 DSP G.726-40k payload value                    : 105
 DSP VBD payload value                          : 102
 VQM                                            : Disable
 RTCP package send interval time(ms)            : 5000
 RTCPXR                                         : Enable
 Severe degrade second threshold                : 400
 DSP echo check                                 : On
```

```
DSP packet lose compensate                    : Off
DSP silence reduce                          : Off
DTMF negative twist value                     : 10, unit 0.1db
DTMF positive twist value                    : 40, unit 0.1db
DSP 2833 event volume adjustment mode         : disable
DSP 2833 event volume adjustment devia        :  0  dBm
 Workmode         Threshold1   Threshold2   Threshold3
 Normal
```

Table 16-36 Description of the display voice dsp-attribute command output

Item	Description
DSP code type	Default DSP channel code type: ● G711A ● G711u ● G723_1 ● G729 ● G726-16k ● G726-24k ● G726-32k ● G726-40k
DSP Rtp Packet interval (ms)	Interval for the DSP channel to packetize RTP packets, in milliseconds. ● 5 ms ● 10 ms ● 20 ms ● 30 ms
T30 redundancy parameter value of T38 fax	T.30 redundancy parameter value of the T.38 fax. The value ranges from 0 to 7.
T4 redundancy parameter value of T38 fax	T.4 redundancy parameter value of the T.38 fax. The value ranges from 0 to 3.
Fax ECM	Fax ECM mode: ● enable: ECM ● disable: NECM
Fax train Mode	Fax training mode: ● e2e: End-to-end training ● local: Local training This parameter takes effect only when the T.38 fax is used.

Item	Description
Fax Max train Rate	Maximum fax training rate: ● V17: negotiation using V.17 fax and a maximum fax training rate of 14.4 kbit/s. ● V29: negotiation using V.29 fax and a maximum fax training rate of 9.6 kbit/s. ● V27: negotiation using V.27 fax and a maximum fax training rate of 4.8 kbit/s.
Fax V8 Negotiate	Whether V.8 negotiation of the T.38 fax is enabled or disabled.
DSP min adapted jitter buffer (ms)	Minimum value of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP max adapted jitter buffer (ms)	Maximum value of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP init adapted jitter buffer (ms)	Initial value of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP adapted jitter buffer threshold (ms)	Alarm threshold of the dynamic jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP min fixed jitter buffer (ms)	Minimum value of the static jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP max fixed jitter buffer (ms)	Maximum value of the static jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP init fixed jitter buffer (ms)	Initial value of the static jitter buffer of the DSP channel. The value ranges from 0 to 150, in milliseconds.
DSP redundancy payload value	Redundancy payload value of the DSP channel. The value ranges from 96 to 127.
DSP NTE payload value	NTE payload value of the DSP channel. The value ranges from 96 to 127.
DSP clearmode payload value	RTP payload value of the DSP channel. The value ranges from 96 to 127.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DSP G.726-16k payload value	G.726-16k payload value of the DSP channel. The value ranges from 96 to 127.
DSP G.726-24k payload value	G.726-24k payload value of the DSP channel. The value ranges from 96 to 127.
DSP G.726-32k payload value	G.726-32k payload value of the DSP channel. The value ranges from 96 to 127.
DSP G.726-40k payload value	G.726-40k payload value of the DSP channel. The value ranges from 96 to 127.
DSP VBD payload value	VBD payload value of the DSP channel. The value ranges from 96 to 127.
VQM	Whether voice quality monitor (VQM) is enabled. ● disable: VQM is disabled. ● enable: VQM is enabled.
RTCPXR	Whether RTP Control Protocol Extended Reports (RTCP XR) is enabled. ● disable: RTCP XR is disabled. ● enable: RTCP XR is enabled.
RTCP package send interval time (ms)	Interval for the DSP channel to send RTCP packets. The value can be 0 or in the range of 500 to 65535, in milliseconds.
Severe Degrade Second Threshold	Default threshold for the number of severe degrade seconds. The value ranges from 1 to 65535.
DSP echo check	Whether echo cancellation is enabled on the DSP channel. ● disable: Echo cancellation is disabled on the DSP channel. ● enable: Echo cancellation is enabled on the DSP channel.
DSP Packet Lose Compensate	Whether the Packet Loss Concealment (PLC) function is enabled on the DSP channel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DSP silence reduce	Whether silence compression is enabled on the DSP channel.
DTMF negative twist value	DTMF detection negative twist value, range 0~100, unit 0.1db
DTMF positive twist value	DTMF detection positive twist value, range 0~100, unit 0.1db
DSP 2833 event volume adjustment mode	The mode in which the DSP adjusts the volume of DTMF tones during RFC 2833 DTMF transmission. **NOTE** Only AR1200, AR2200, and AR3200 that support voice communication support this parameter.
DSP 2833 event volume adjustment devia	The value of the DSP adjusts the volume of DTMF tones in fixed mode during RFC 2833 DTMF transmission. **NOTE** Only AR1200, AR2200, and AR3200 that support voice communication support this parameter.

16.3.6.4 display voice tone

Function

The **display voice tone** command is used to verify the current configuration on a signal tone.

Format

display voice tone *tone-id*

Parameters

Parameter	Description	Value
tone-id	Display the configuration of the specified signal tone.	The value is an integer that ranges from 1 to 11.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

```
<Huawei> display voice tone 3
-----------------Parameter Tone ID: 3 ----------------
------------------------------------------------------------
 Frequency(Unit:hz)  Ampletude(Unit:dbm)
        450                  0.3
          0                  0.0
          0                  0.0
          0                  0.0
 Cadences(count:1)   On-time  Off-time Frequency-Base-Flag
 Sequence[1]          65535        0       1

---------Attributes for detect Tone--------
            Frequency_Low[hz] Frequency_High[hz] Low-Ampletude[dbm] High-Ampletude[dbm]
1st Frequency      420                480                0.0              0.0
2nd Frequency      0                  0                  0.0              0.0
             Time_Onlow[ms]   Time_OnHigh[ms]  Time_OffLow[ms]  Time_OffHigh[ms]
1st Cadence:        2000              0                0                0
2nd Cadence:          0               0                0                0
```

16.3.6.5 dsp

Function

Using the **dsp** command, you can enter the DSP resource management view.

Format

dsp *slot/dsp-index*

Parameters

Parameter	Description	Value
slot/dsp-index	Specifies the slot ID and index of a DSP.	The value is a string of 1 to 15 characters. For example, if the slot ID is 0 and the DSP index is 0, the value is 0/0.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

To manage DSP resources, run the **dsp** command to enter the DSP resource management view.

Example

Enter the view of DSP 0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp 0/0
```

16.3.6.6 dsp-attribute

Function

Using the **dsp-attribute** command, you can enter the DSP attribute view.

Format

dsp-attribute

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

DSP configurations can be performed only in the DSP attribute view.

Example

Enter the DSP attribute view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute]
```

16.3.6.7 dtmf-twist-value(dsp-attribute view)

Function

command **dtmf-twist-value** is used to configure dtmf detection twist values

command **undo dtmf-twist-value** restores the default dtmf detection twist values

Format

dtmf-twist-value negative-twist *negative-twist-value* **positive-twist** *positive-twist-value*

undo dtmf-twist-value

Parameters

parameter	description	value
negative-twist *negative-twist-value*	negative dtmf twist value	integer 0-100, unit 0.1db.
positive-twist *positive-twist-value*	positive dtmf twist value	integer 0-100, unit 0.1db.

Views

dsp-attribute view

Default Level

2: Configuration level

Usage Guidelines

To configure dtmf detection twist values, run **dtmf-twist-value** command.

Example

set the negative twist value of dtmf detection to 5 db, and positive twist value to 10db.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] dtmf-twist-value negative-twist 50 positive-twist 100
```

16.3.6.8 echo

Function

Using the **echo** command, you can enable echo cancelation on the DSP channel or disable this function.

Using the **undo echo** command, you can cancel the configuration.

By default, echo cancelation is disabled on the DSP channel.

Format

echo { **enable** | **disable** }

undo echo

Parameters

None

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **echo enable** command enables echo cancelation on an MGC.

Example

Disable echo cancelation.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] echo disable
```

16.3.6.9 fax ecm

Function

The **fax ecm** command enables T.38 Error Correction Mode (ECM) or disable this function.

The **undo fax ecm** command restores the default T.38 ECM setting.

By default, T.38 ECM is enabled.

Format

fax ecm { **enable** | **disable** }

undo fax ecm

Parameters

None

Views

DSP attribute view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

ECM takes effect only when T.38 is used. After ECM is enabled, fax quality is optimized but the rate of fax messages is reduced. To increase the rate of fax messages, disable ECM.

Example

Enable T.38 ECM.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax ecm enable
```

16.3.6.10 fax redundancy-t30

Function

Using the **fax redundancy-t30** command, you can set the T.30 redundancy parameter value of the T.38 fax.

Using the **undo fax redundancy-t30** command, you can restore the default T.30 redundancy parameter value of the T.38 fax.

By default, the T.30 redundancy parameter value of the T.38 fax is 3.

Format

fax redundancy-t30 *redundancy-t30-value*

undo fax redundancy-t30

Parameters

Parameter	Description	Value
redundancy-t30-value	Specifies the T.30 redundancy parameter value of the T.38 fax.	The value is an integer that ranges from 0 to 7. The default value is 3.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the T.30 redundancy parameter value of the T.38 fax to 5.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax redundancy-t30 5
```

16.3.6.11 fax redundancy-t4

Function

Using the **fax redundancy-t4** command, you can set the T.4 redundancy parameter value of the T.38 fax.

Using the **undo fax redundancy-t4** command, you can restore the default T.4 redundancy parameter value of the T.38 fax.

By default, the T.4 redundancy parameter value of the T.38 fax is 3.

Format

fax redundancy-t4 *redundancy-t4-value*

undo fax redundancy-t4

Parameters

Parameter	Description	Value
redundancy-t4-value	Specifies the T.4 redundancy parameter value of the T.38 fax.	The value is an integer that ranges from 0 to 3. The default value is 3.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the T.4 redundancy parameter value of the T.38 fax to 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax redundancy-t4 2
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.12 fax training-mode

Function

Using the **fax training-mode** command, you can set the fax training mode.

Using the **undo fax training-mode** command, you can restore the default fax training mode.

By default, end-to-end training is used.

Format

fax training-mode { **e2e** | **local** }

undo fax training-mode

Parameters

Parameter	Description	Value
e2e	Indicates the end-to-end training mode.	-
local	Indicates the local training mode.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The fax training mode takes effect only when the T.38 fax is used. End-to-end training and local training modes are distinguished based on rate training signals sent from the transmit gateway to the receive gateway:

- If rate training signals need to be sent to the peer end, end-to-end training is used.
- If the gateway terminates and generates training signals, local training is used.

To use the local training mode, consider the maximum rate of the gateway, which is represented by the maximum fax rate supported on the DSP channel. The training mode is invalid for high-rate fax and low-rate transparent transmission.

Example

Set the fax training mode to local training.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax training-mode local
```

16.3.6.13 fax training-rate

Function

Using the **fax training-rate** command, you can set the maximum fax training rate.

Using the **undo fax training-rate** command, you can restore the default maximum fax training rate.

By default, the maximum fax training rate is V17.

Format

fax training-rate { **v17** | **v29** | **v27** }

undo fax training-rate

Parameters

Parameter	Description	Value
v17	Indicates the negotiation using V.17 and a maximum fax training rate of 14.4 kbit/s.	-
v29	Indicates the negotiation using V.29 and a maximum fax training rate of 9.6 kbit/s.	-
v27	Indicates the negotiation using V.27 and a maximum fax training rate of 4.8 kbit/s.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The maximum fax training rate takes effect only when local training is used, and is invalid for fax in transparent transmission mode. When the rate of the fax

machine can be reduced and the network is not running properly, reduce the fax training rate.

Example

Set the maximum fax training rate to V29.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax training-rate v29
```

16.3.6.14 fax v8negotiate

Function

Using the **fax v8negotiate** command, you can enable V8 negotiation or disable this function.

Using the **undo fax v8negotiate** command, you can restore the V8 negotiation parameter setting.

By default, V8 negotiation is disabled.

Format

fax v8negotiate { **enable** | **disable** }

undo fax v8negotiate

Parameters

None

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

During communication between two fax machines, one fax machine supports the V.34 fax (high-speed fax) and the other fax machine supports only the low-speed fax. To prevent the two fax machines from performing high-speed fax negotiation, disable V8 negotiation so that the two fax machines implement low-speed fax.

Example

Enable V8 negotiation.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] fax v8negotiate enable
```

16.3.6.15 jitter-buffer adapt-jb-threshold

Function

Using the **jitter-buffer adapt-jb-threshold** command, you can set the alarm threshold of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer adapt-jb-threshold** command, you can restore the default alarm threshold of the dynamic jitter buffer of the DSP channel.

By default, the alarm threshold of the dynamic jitter buffer of the DSP channel is 150 ms.

Format

jitter-buffer adapt-jb-threshold *adapt-jb-threshold*

undo jitter-buffer adapt-jb-threshold

Parameters

Parameter	Description	Value
adapt-jb-threshold	Specifies the alarm threshold of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 150 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer

MinAdaptJitterBuffer < ThresholdJitterBuffer

Example

Set the alarm threshold of the dynamic jitter buffer of the DSP channel to 100 ms.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer adapt-jb-threshold 100
```

16.3.6.16 jitter-buffer init-adapt-jb

Function

Using the **jitter-buffer init-adapt-jb** command, you can set the initial value of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer init-adapt-jb** command, you can restore the default initial value of the dynamic jitter buffer of the DSP channel.

By default, the initial value of the dynamic jitter buffer of the DSP channel is 2 ms.

Format

jitter-buffer init-adapt-jb *init-adapt-jb-value*

undo jitter-buffer init-adapt-jb

Parameters

Parameter	Description	Value
init-adapt-jb-value	Specifies the initial value of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 2 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the

specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

Example

Set the initial value of the dynamic jitter buffer of the DSP channel to 30 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer init-adapt-jb 30
```

16.3.6.17 jitter-buffer init-fixed-jb

Function

Using the **jitter-buffer init-fixed-jb** command, you can set the initial value of the static jitter buffer of the DSP channel.

Using the **undo jitter-buffer init-fixed-jb** command, you can restore the default initial value of the static jitter buffer of the DSP channel.

By default, the initial value of the static jitter buffer of the DSP channel is 60 ms.

Format

jitter-buffer init-fixed-jb *init-fixed-jb-value*

undo jitter-buffer init-fixed-jb

Parameters

Parameter	Description	Value
init-fixed-jb-value	Specifies the initial value of the static jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 60 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately.

 Copyright © Huawei Technologies Co., Ltd.

The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= IinitFixedJitterBuffer <= MaxFixedJitterBuffer and the MinAdaptJitterBuffer

Example

Set the initial value of the static jitter buffer of the DSP channel to 90 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer init-fixed-jb 90
```

16.3.6.18 jitter-buffer max-adapt-jb

Function

Using the **jitter-buffer max-adapt-jb** command, you can set the maximum value of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer max-adapt-jb** command, you can restore the default maximum value of the dynamic jitter buffer of the DSP channel.

By default, the maximum value of the dynamic jitter buffer of the DSP channel is 135 ms.

Format

jitter-buffer max-adapt-jb *max-adapt-jb-value*

undo jitter-buffer max-adapt-jb

Parameters

Parameter	Description	Value
max-adapt-jb-value	Specifies the maximum value of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 135 ms.

Views

DSP attribute view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

Example

Set the maximum value of the dynamic jitter buffer of the DSP channel to 120 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer max-adapt-jb 120
```

16.3.6.19 jitter-buffer max-fixed-jb

Function

Using the **jitter-buffer max-fixed-jb** command, you can set the maximum value of the static jitter buffer of the DSP channel.

Using the **undo jitter-buffer max-fixed-jb** command, you can restore the default maximum value of the static jitter buffer of the DSP channel.

By default, the maximum value of the static jitter buffer of the DSP channel is 135 ms.

Format

jitter-buffer max-fixed-jb *max-fixed-jb-value*

undo jitter-buffer max-fixed-jb

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-fixed-jb-value	Specifies the maximum value of the static jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 135 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer

MinAdaptJitterBuffer < ThresholdJitterBuffer

Example

Set the maximum value of the static jitter buffer of the DSP channel to 120 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer max-fixed-jb 120
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.20 jitter-buffer min-adapt-jb

Function

Using the **jitter-buffer min-adapt-jb** command, you can set the minimum value of the dynamic jitter buffer of the DSP channel.

Using the **undo jitter-buffer min-adapt-jb** command, you can restore the default minimum value of the dynamic jitter buffer of the DSP channel.

By default, the minimum value of the dynamic jitter buffer of the DSP channel is 2 ms.

Format

jitter-buffer min-adapt-jb *min-adapt-jb-value*

undo jitter-buffer min-adapt-jb

Parameters

Parameter	Description	Value
min-adapt-jb-value	Specifies the minimum value of the dynamic jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 2 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

 Copyright © Huawei Technologies Co., Ltd.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer

MinAdaptJitterBuffer < ThresholdJitterBuffer

Example

Set the minimum value of the dynamic jitter buffer of the DSP channel to 30 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer min-adapt-jb 30
```

16.3.6.21 jitter-buffer min-fixed-jb

Function

Using the **jitter-buffer min-fixed-jb** command, you can set the minimum value of the static jitter buffer of the DSP channel.

Using the **undo jitter-buffer min-fixed-jb** command, you can restore the default minimum value of the static jitter buffer of the DSP channel.

By default, the minimum value of the static jitter buffer of the DSP channel is 2 ms.

Format

jitter-buffer min-fixed-jb *min-fixed-jb-value*

undo jitter-buffer min-fixed-jb

Parameters

Parameter	Description	Value
min-fixed-jb-value	Specifies the minimum value of the static jitter buffer of the DSP channel.	The value is an integer that ranges from 0 to 150, in milliseconds. The default value is 2 ms.

Views

DSP attribute view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The transmission delay, processing delay, and serial link delay on the VoIP network cause voice jitter and make the call quality deteriorated. The jitter buffer removes the delay and improves the voice quality using Packet Loss Concealment (PLC).

The jitter buffer is installed at the receive end of an IP phone. A received IP packet is first received by the buffer but not transmitted to the called end immediately. The jitter buffer forwards each packet at intervals only after a certain number of IP voice packets are received. By doing this, the jitter of the IP phone is removed to a certain degree.

The jitter buffer does not forward each voice packet immediately after receiving it, so the forwarding delay must be specified. If the delay is too long, the system delay is long. If the delay is too short, IP voice packets cannot arrive within the specified time range and the voice jitter still occurs. The proper delay of a jitter buffer is about 30 ms.

The constraints of jitter buffer values are as follows:

MinFixedJitterBuffer <= NormalFixedJitterBuffer <= MaxFixedJitterBuffer and the MinAdaptJitterBuffer

Example

Set the minimum value of the static jitter buffer of the DSP channel to 5 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] jitter-buffer min-fixed-jb 5
```

16.3.6.22 loop-back (DSP resource management view)

Function

Using the **loop-back** command, you can configure the loopback function on a DSP channel.

Using the **undo loop-back** command, you can disable the loopback function.

Format

loop-back *loop-back-typechannel*

undo loop-back

Parameters

Parameter	Description	Value
loop-back-type	Specifies the loopback type.	The value can be: ● pcm-side: performs a loopback test at the pulse code modulation (PCM) channel side. ● ip-side: performs a loopback test at the IP side.
channel	Specifies the index of the DSP channel where the loopback test is performed.	The value is an integer that ranges from 0 to the maximum DSP channel index.

Views

DSP resource management view

Default Level

2: Configuration level

Usage Guidelines

When using the **loop-back** command, pay attention to the following points:

- This command is invalid for DSP channels in Idle, Fault, Wastage, or Prohibited state.
- When the DSP channel between the calling party and called party cannot transmit signals or can transmit signals only in one direction, run this command to locate the fault. For example, if the calling party hears the echo in a PCM-side loopback test, the speech channel between the calling phone and the calling DSP channel is functioning properly. If the called party hears the echo in an IP-side loopback test, the speech channel between the called phone and the calling DSP channel is functioning properly.

When using the **undo loop-back** command, pay attention to the following points:

- This command is valid only on DSP channels with the loopback function configured.
- After disabling the loopback function, you can run the **display voice dsp state** command to check the status of the DSP channel.

Example

Perform a PCM-side loopback test on DSP channel 5 in DSP 0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp 0/0
[Huawei-voice-dsp0/0] loop-back pcm-side 5
```

16.3.6.23 nte2833-volume deviation

Function

The **nte2833-volume deviation** command specifies how much the DSP adjusts the volume of DTMF tones in fixed mode.

The **undo nte2833-volume deviation** command restores the default setting of how much the DSP adjusts the volume of DTMF tones in fixed mode.

The default value is 20, indicating that the DSP adjusts the volume of DTMF tones by 0 dBm.

NOTE

Only AR1200, AR2200, and AR3200 that support voice communication support this command.

Format

nte2833-volume deviation *deviation-value*

undo nte2833-volume deviation

Parameters

Parameter	Description	Value
deviation-value	Indicates how much the DSP adjusts the volume of DTMF tones.	The value is an integer ranging from 0 to 40. For example, the value 0 indicates that the DSP adjusts the volume of DTMF tones by 20 dBm, the value 1 indicates adjusting by 19 dBm, and the value 40 indicates adjusting by –20 dBm.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

When the value of *deviation-value* is 0, it indicates that the volume of DTMF tones is increased by 20 dBm. The value 0 is called configured adjustment value, and 20 dBm the actual adjustment value. The conversion between the two values is as follows: Actual adjustment value = 20 – Configured adjustment value

The original volume of DTMF tones plus the actual adjustment value is the adjusted volume of DTMF tones. If the actual adjustment value is larger than 0 dBm, the DSP increases the volume of DTMF tones. If the actual adjustment value is smaller than 0 dBm, the DSP reduces the volume of DTMF tones. The actual adjustment value 0 indicates that the DSP does not change the volume of DTMF tones.

Precautions

The **nte2833-volume deviation** command takes effect only when the mode in which the DSP adjusts the volume of DTMF tones is fixed. You can run the **nte2833-volume mode** command to configure the DSP's DTMF tone adjustment mode.

Example

Configure the DSP to adjust the volume of DTMF tones by –5 dBm.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] nte2833-volume deviation 25
```

Related Topics

16.3.6.3 display voice dsp-attribute

16.3.6.24 nte2833-volume mode

16.3.6.24 nte2833-volume mode

Function

The **nte2833-volume mode** command configures the mode in which the DSP adjusts the volume of DTMF tones.

The **undo nte2833-volume** command restores the default mode in which the DSP adjusts the volume of DTMF tones.

By default, the adjustment mode is disabled.

NOTE

Only AR1200, AR2200, and AR3200 that support voice communication support this command.

Format

nte2833-volume mode *mode-value*

undo nte2833-volume mode

Parameters

Parameter	Description	Value
mode-value	Indicates the mode in which the DSP adjusts the volume of DTMF tones.	Enumerated type. The value can be: • **auto_attenuation**: Automatic attenuation mode • **disable**: Disabled mode • **fixed_adjust**: Fixed mode

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

During RFC 2833 DTMF transmission, the volume of DTMF tones may be high or low and cannot be automatically adjusted by DSP gains. In this case, you can run the **nte2833-volume mode** command to configure the DSP's DTMF tone adjustment mode, and thereby enable the DSP to adjust the volume of DTMF tones to solve the problem.

Example

Set the mode in which the DSP adjusts the volume of DTMF tones to **auto_attenuation**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] nte2833-volume mode auto_attenuation
```

Related Topics

16.3.6.3 display voice dsp-attribute
16.3.6.23 nte2833-volume deviation

16.3.6.25 payload-type clear-mode

Function

Using the **payload-type clear-mode** command, you can set the RTP payload type value of the DSP channel.

Using the **undo payload-type clear-mode** command, you can restore the default RTP payload type value of the DSP channel.

By default, the RTP payload type value of the DSP channel is 100.

Format

payload-type clear-mode *clear-mode-value*

undo payload-type clear-mode

Parameters

Parameter	Description	Value
clear-mode-value	Specifies the RTP payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 100.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The RTP payload type values at both ends must be identical and unique.

Example

Set the RTP payload type value of the DSP channel to 120.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type clear-mode 120
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.26 payload-type g726-16k

Function

Using the **payload-type g726-16k** command, you can set the G.726-16k payload type value of the DSP channel.

Using the **undo payload-type g726-16k** command, you can restore the default G.726-16k payload type value of the DSP channel.

By default, the G.726-16k payload type value of the DSP channel is 103.

Format

payload-type g726-16k *g726-16k-value*

undo payload-type g726-16k

Parameters

Parameter	Description	Value
g726-16k-value	Specifies the G.726-16k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 103.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-16k payload type values at both ends must be identical and unique.

Example

Set the G.726-16k payload type value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-16k 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.27 payload-type g726-24k

Function

Using the **payload-type g726-24k** command, you can set the G.726-24k payload type value of the DSP channel.

Using the **undo payload-type g726-24k** command, you can restore the default G.726-24k payload type value of the DSP channel.

By default, the G.726-24k payload type value of the DSP channel is 104.

Format

payload-type g726-24k *g726-24k-value*

undo payload-type g726-24k

Parameters

Parameter	Description	Value
g726-24k-value	Specifies the G.726-24k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 104.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-24k payload type values at both ends must be identical and unique.

Example

Set the G.726-24k payload type value of the DSP channel to 101.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-24k 101
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.28 payload-type g726-32k

Function

Using the **payload-type g726-32k** command, you can set the G.726-32k payload type value of the DSP channel.

Using the **undo payload-type g726-32k** command, you can restore the default G.726-32k payload type value of the DSP channel.

By default, the G.726-32k payload type value of the DSP channel is 101.

Format

payload-type g726-32k *g726-32k-value*

undo payload-type g726-32k

Parameters

Parameter	Description	Value
g726-32k-value	Specifies the G.726-32k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 101.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-32k payload type values at both ends must be identical and unique.

Example

Set the G.726-32k payload type value of the DSP channel to 102.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-32k 102
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.29 payload-type g726-40k

Function

Using the **payload-type g726-40k** command, you can set the G.726-40k payload type value of the DSP channel.

Using the **undo payload-type g726-40k** command, you can restore the default G.726-40k payload type value of the DSP channel.

By default, the G.726-40k payload type value of the DSP channel is 105.

Format

payload-type g726-40k *g726-40k-value*

undo payload-type g726-40k

Parameters

Parameter	Description	Value
g726-40k-value	Specifies the G.726-40k payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 105.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The G.726-40k payload type values at both ends must be identical and unique.

Example

Set the G.726-40k payload type value of the DSP channel to 103.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type g726-40k 103
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.30 payload-type nte

Function

Using the **payload-type nte** command, you can set the NTE payload type value of the DSP channel.

Using the **undo payload-type nte** command, you can restore the default NTE payload type value of the DSP channel.

By default, the NTE payload type value of the DSP channel is 97.

Format

payload-type nte *nte-value*

undo payload-type nte

Parameters

Parameter	Description	Value
nte-value	Specifies the NTE payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 97.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The NTE payload type values at both ends must be identical and unique.

Example

Set the NTE payload value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type nte 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.31 payload-type redundancy

Function

Using the **payload-type redundancy** command, you can set the redundancy payload type value of the DSP channel.

Using the **undo payload-type redundancy** command, you can restore the default redundancy payload type value of the DSP channel.

By default, the redundancy payload type value of the DSP channel is 96.

Format

payload-type redundancy *redundancy-value*

undo payload-type redundancy

Parameters

Parameter	Description	Value
redundancy-value	Specifies the redundancy payload type value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 96.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The redundancy payload type values at both ends must be identical and unique.

Example

Set the redundancy payload type value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type redundancy 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.32 payload-type vbd

Function

Using the **payload-type vbd** command, you can set the VBD payload type value of the DSP channel.

Using the **undo payload-type vbd** command, you can restore the default VBD payload type value of the DSP channel.

By default, the VBD payload type value of the DSP channel is 102.

Format

payload-type vbd *vbd-value*

undo payload-type vbd

Parameters

Parameter	Description	Value
vbd-value	Specifies the VBD payload value of the DSP channel.	The value is an integer that ranges from 96 to 127. The default value is 102.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The VBD payload type values at both ends must be identical and unique.

Example

Set the VBD payload value of the DSP channel to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] payload-type vbd 100
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.33 plc

Function

Using the **plc** command, you can enable the Packet Loss Concealment (PLC) function on the DSP channel or disable this function.

Using the **undo plc** command, you can cancel the configuration.

By default, the PLC function is disabled.

Format

plc { enable | disable }

undo plc

Parameters

Parameter	Description	Value
enable	Enable the Packet Loss Concealment (PLC) function on the DSP channel.	-
disable	Disable the Packet Loss Concealment (PLC) function on the DSP channel.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Packet loss makes the voice quality deteriorated. The PLC recovers the packet loss to minimize the effect of packet loss in digital communications.

Example

Enable the PLC function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] plc enable
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.34 prohibit

Function

Using the **prohibit** command, you can prohibit DSP channels.

Using the **undo prohibit** command, you can restore the prohibited DSP channels.

Format

prohibit *channel* [*count*]

undo prohibit *channel* [*count*]

Parameters

Parameter	Description	Value
channel	Specifies the index of a DSP channel.	The value is an integer that ranges from 0 to the maximum DSP channel index.
count	Specifies the number of DSP channels to be prohibited.	The value is an integer that ranges from 1 to the maximum number of DSP channels supported.

Views

DSP resource management view

Default Level

2: Configuration level

Usage Guidelines

DSP channels in Busy or Wastage state or unregistered DSP channels cannot be prohibited.

Example

Prohibit channel 5 in DSP 0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp 0/0
[Huawei-voice-dsp0/0] prohibit 5
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.6.35 resource-threshold

Function

Using the **resource-threshold** command, you can set the resource threshold in hierarchical control mode.

Using the **undo resource-threshold mode** command, you can restore the default resource threshold in hierarchical control mode.

Format

resource-threshold { **threshold1** *threshold1* | **threshold2** *threshold2* | **threshold3** *threshold3* }

undo resource-threshold { **threshold1** | **threshold2** | **threshold3** }

Parameters

Parameter	Description	Value
threshold1 *threshold1*	Specifies the resource threshold of common users (cat1).	The value is an integer that ranges from 0 to 100. The default value is 100.
threshold2 *threshold2*	Specifies the resource threshold of category 2 users (cat2).	The value is an integer that ranges from 0 to 100. The default value is 100.
threshold3 *threshold3*	Specifies the resource threshold of category 3 users (cat3).	The value is an integer that ranges from 0 to 100. The default value is 100.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The thresholds in the **resource-threshold** command are as follows: *threshold1-val* <= *threshold2-val* <= *threshold3-val*

When the DSP resource control mode is hierarchical control, DSP resource allocation is determined based on user levels. The resources that can be used are configured by the **resource-threshold** command.

Example

Set the resource threshold for an authorized user to 60.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] resource-threshold threshold 1 60
```

16.3.6.36 resource-threshold mode

Function

Using the **resource-threshold mode** command, you can set the DSP resource control mode.

Using the **undo resource-threshold mode** command, you can restore the default DSP resource control mode.

By default, the DSP resource control mode is normal.

Format

resource-threshold mode { **priority** | **normal** }

undo resource-threshold mode

Parameters

Parameter	Description	Value
priority	Indicates that the DSP resource control mode is hierarchical control.	-
normal	Indicates that the DSP resource control mode is normal.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

When the DSP resource control mode is hierarchical control, DSP resource allocation is determined based on user levels. The resources that can be used are configured by the **resource-threshold** command.

 Copyright © Huawei Technologies Co., Ltd.

When the DSP resource control mode is normal, users at any level can occupy all DSP resources.

Example

Set the DSP resource control mode to hierarchical control.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] resource-threshold mode priority
```

16.3.6.37 rtcp rtcp-interval

Function

Using the **rtcp rtcp-interval** command, you can set the interval at which the DSP channel sends RTCP packets.

Using the **undo rtcp rtcp-interval** command, you can restore the default interval at which the DSP channel sends RTCP packets.

By default, the interval at which the DSP channel sends RTCP packets is 5000 ms.

Format

rtcp rtcp-interval *rtcp-interval*

undo rtcp rtcp-interval

Parameters

Parameter	Description	Value
rtcp-interval	Specifies the interval at which the DSP channel sends RTCP packets.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5000 ms.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **rtcp rtcp-interval** command sets the interval at which the DSP channel sends RTCP packets on an MGC.

Example

Set the interval at which the DSP channel sends RTCP packets to 8000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp rtcp-interval 8000
```

16.3.6.38 rtcp rtcpxr

Function

Using the **rtcp rtcpxr** command, you can enable the RTP Control Protocol Extended Reports (RTCP XR) function or disable this function.

Using the **undo rtcp rtcpxr** command, you can cancel the configuration.

By default, the RTCP XR function is disabled.

Format

rtcp rtcpxr { enable | disable }

undo rtcp rtcpxr

Parameters

Parameter	Description	Value
enable	Enable the RTP Control Protocol Extended Reports function.	-
disable	Disable the RTP Control Protocol Extended Reports function.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the RTCP XR function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp rtcpxr enable
```

16.3.6.39 rtcp sev-degrade-threshold

Function

Using the **rtcp sev-degrade-threshold** command, you can set the threshold for the number of severe degrade seconds.

Using the **undo rtcp sev-degrade-threshold** command, you can restore the default threshold for the number of severe degrade seconds.

By default, the threshold for the number of severe degrade seconds is 400.

Format

rtcp sev-degrade-threshold *sev-degrade-thresholdval*

undo rtcp sev-degrade-threshold

Parameters

Parameter	Description	Value
sev-degrade-thresholdval	Specifies the threshold for the number of severe degrade seconds.	The value is an integer that ranges from 1 to 65535. The default value is 400.

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the threshold for the number of severe degrade seconds to 1000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp sev-degrade-threshold 1000
```

16.3.6.40 rtcp vqm

Function

Using the **rtcp vqm** command, you can enable the Voice Quality Monitor (VQM) function or disable this function.

Using the **undo rtcp vqm** command, you can cancel the configuration.

By default, the VQM function is disabled.

Format

rtcp vqm { enable | disable }

undo rtcp vqm

Parameters

Parameter	Description	Value
enable	Enable the Voice Quality Monitor function.	-
disable	Disable the Voice Quality Monitor function.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the VQM function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] rtcp vqm enable
```

16.3.6.41 silence

Function

Using the **silence** command, you can enable silence compression on the DSP channel.

Using the **undo silence** command, you can cancel the configuration.

By default, silence compression is disabled on the DSP channel.

Format

silence { enable | disable }

undo silence

Parameters

Parameter	Description	Value
enable	Enable the silence compression on the DSP channel.	-
disable	Disable the silence compression on the DSP channel.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

The **silence enable** command enables silence compression on an MGC.

Example

Enable silence compression.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] silence enable
```

16.3.6.42 tone (Voice View)

Function

tone can be either used to enter a specific tone-id view or create a new tone-id view, and hence configure the parameters of that tone-id

undo tone deletes a tone id

 Copyright © Huawei Technologies Co., Ltd.

Format

tone *Tone-id*

undo tone *Tone-id*

Parameters

parameter	description	value
Tone-id	Tone id number	integer, ranging from 1 to 11

Views

voice view

Default Level

Configuration level

Usage Guidelines

In the past, tone parameters were customized by way of importing a particular tone file. The disadvantage of this approach is that once some parameters need to be modified, the tone file has to be remade and imported again. This tone command can alleviate the trouble of the above process by enabling users to make customizations on the commandline.

Example

#create a view for tone id 3

```
[Huawei-voice]tone 3
Welcome enter the tone configuration!
As a diagnose feature,you'd better make change with the guide of handbook and local standards! Be
careful!
[Huawei-voice-tone-3]
```

16.3.6.43 tone-frequency

Function

The **tone-frequency** command configures the frequency and amplitude of a signal tone.

The **undo tone-frequency** command cancels any configuration on a signal tone's frequency and amplitude.

Format

tone-frequency { **frequency-1** *freq1-value amplitude1-value* [**frequency-2** *freq2-value amplitude2-value* [**frequency-3** *freq3-value amplitude3-value* [**frequency-4** *freq4-value amplitude4-value*]]] }

undo tone-frequency

Parameters

Parameter	Description	Value
frequency-1 *freq1-value*	Specifies the frequency of the first frequency set.	Integer, range: 0-4000, unit: Hz
amplitude1-value	Specifies the first amplitude of the Nth frequency set.	Integer, range: 0-100, unit: 0.1 dBm
frequency-2 *freq2-value*	Specifies the frequency of the second frequency set.	Integer, range: 0-4000, unit: Hz
amplitude2-value	Specifies the amplitude of the second frequency set.	Integer, range: 0-100, unit: 0.1 dBm
frequency-3 *freq3-value*	Specifies the frequency of the third frequency set.	Integer, range: 0-4000, unit: Hz
amplitude3-value	Specifies the amplitude of third frequency set.	Integer, range: 0-100, unit: 0.1 dBm
frequency-4 *freq4-value*	Specifies the frequency of the fourth frequency set.	Integer, range: 0-4000, unit: Hz
amplitude4-value	Specifies the amplitude of the fourth frequency set.	Integer, range: 0-100, unit: 0.1 dBm

Views

Tone view

Default Level

Configuration level

Usage Guidelines

Usually users should only perform find-tune on the frequency and the amplitude. Radical changes on those parameters may have undesirable effect upon normal calls.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure tone 3, set the frequency to be 980 Hz and amplitude 0.3 dBm. After doing so, the dial-tone becomes sharper because of higher pitch and larger amplitude.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tone 3
[Huawei-voice-tone-3] tone-frequency frequency-1 980 3
```

16.3.6.44 tone-cadence

Function

tone-cadence sets the cadence.

undo tone-cadence restores the default cadence.

Format

tone-cadence continus *base-frequency-flag*

tone-cadence sequence { *ontime1-value offtime1-value base-frequency-flag1* } [{ *ontime2-value offtime2-value base-frequency-flag2* } [{ *ontime3-value offtime3-value base-frequency-flag3* } [{ *ontime4-value offtime4-value base-frequency-flag4* }]]]

undo tone-cadence

Parameters

parameter	description	value
continus *base-frequency-flag*	Frequency flag. Convert this number into a 4-bit binary number, and each of the 4 bits corresponds to a frequency set (See the **tone-frequency** command).	Integer, range: 1-6, 8-10, 12.
sequence	Sequential flag.	-
ontimeN-value	Length of playing time for the Nth cadence.	Integer, range: 0-65535, unit: ms.
offtimeN-value	Length of silence time for the Nth cadence.	Integer, range: 0-65535, unit: ms.
base-frequency-flagN	Frequency flag of the Nth cadence.	Integer, range: 1-6, 8-10, 12.

 Copyright © Huawei Technologies Co., Ltd.

Views

Tone view

Default Level

Configuration level

Usage Guidelines

Usually users should only perform find-tune on the cadence. Radical changes on those parameters may have undesirable effect upon normal calls.

Example

Scenario 1:

Configure the cadence on tone 3, making it play continuously with frequency 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tone 3
[Huawei-voice-tone-3] tone-cadence continus 1
```

Scenario 2:

```
[Huawei-voice-tone-3] tone-cadence sequence 400 200 1 500 200 2
```

Set up to 2 cadences. The first one plays 400 ms, then begins a silence period that lasts 200 ms; the second plays for 500 ms, and then begins a 200 ms' silence. The values '1' and '2' are base-frequency-flags, which should be converted to binary numbers as follows:

1 == 0001 frequency 1

2 == 0010 frequency 2

3 == 0011 frequency 1 and frequency 2

4 == 0100 frequency 3

5 == 0101 frequency 1 and frequency 3

.....

After the above configuration, the tone that comes out when one picks up the phone sounds almost the same as before, except that the cadence differs.

Restores the default cadence

```
[Huawei-voice-tone-3] undo tone-cadence
```

16.3.6.45 tone-detect-info

Function

tone-detect-info configure the detection on both the tone-id's frequency and cadence.

undo tone-detect-info cancels any tone-id detection that has been configured.

Format

tone-detect-info { **frequency-1** *freq-low-throld-value1 freq-high-throld-value1* | **amplitude-1** *amp-low-throld-value1 amp-high-throld-value1* }* [{ **frequency-2** *freq-low-throld-value2 freq-high-throld-value2* | **amplitude-2** *amp-low-throld-value2 amp-high-throld-value2* }*

tone-detect-info { **cadence-1** *cadence-ontime-low-throld-value1 cadence-ontime-high-throld-value1 cadence-offtime-low-throld-value1 cadence-offtime-high-throld-value1* | **cadence-2** *cadence-ontime-low-throld-value2 cadence-ontime-high-throld-value2 cadence-offtime-low-throld-value2 cadence-offtime-high-throld-value2* }*

Parameters

Parameter	Description	Integer
frequency-1	frequency detection on frequency set N.	-
freq-low-throld-value1	the low threshold of frequency detection on frequency set N.	Integer, range: 0-4000, unit: Hz
freq-high-throld-value1	the high threshold of frequency detection on frequency set N.	Integer, range: 0-4000, unit: Hz
cadence-1	amplitude detection on frequency set 1.	-
amplitude-1 *amp-low-throld-value1*	the low threshold of amplitude detection on frequency set 1.	Integer, range: 0-100, unit: 0.1 dBm
amp-high-throld-value1	the high threshold of amplitude detection on frequency set 1.	integer, range: 0-100, unit: 0.1 dBm
cadence-2 *cadence-ontime-low-throld-value2*	when to start detecting the play of cadence 1.	Integer, range: 0-65535, unit: ms
cadence-ontime-high-throld-value1	when to stop detecting the play of cadence 1.	Integer, range: 0-65535, unit: ms
cadence-offtime-low-throld-value1	when to start detecting the cadence 1's silence period.	Integer, range: 0-65535, unit: ms
cadence-offtime-high-throld-value1	when to stop detecting the cadence 1's silence period.	Integer, range: 0-65535, unit: ms

Views

tone-id view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

Configuration level

Usage Guidelines

Precautions

For now, tone detection only supports at most two cadences and two frequencies.

This command requires a device restart before it takes effect.

Example

Configure the detection on tone3 frequency.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tone 3
[Huawei-voice-tone-3] tone-detect-info frequency-1 440 460 amplitude-1 2 4
```

Set frequency detection on frequency 1 to be [440, 460]Hz, and detection on amplitude to be [2,4]. The detection on frequency set 2 uses its original detection values when it is not set here.

Configure the detection on tone3 cadence.

```
[Huawei-voice-tone-3] tone-detect-info cadence-1 400 500 200 300 cadence-2 480 520 320 360
```

Set the play time detection on cadence 1 to be [400, 500]ms, and silence detection at time [200, 300]ms. Set the play time detection on cadence 2 to be [480, 520]ms, and silence detection at [320,360]ms.

16.3.6.46 traffic-policy (DSP attribute view)

Function

The **traffic-policy** command applies a traffic policy to a DSP channel.

The **undo traffic-policy** command deletes a traffic policy from a DSP channel.

By default, no traffic policy is applied to a DSP channel.

Format

traffic-policy *policy-name* **inbound**

undo traffic-policy inbound

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value is a string of 1 to 31 case-sensitive characters without spaces and starts with a letter.
inbound	Applies a traffic policy to the inbound direction of a DSP channel.	-

Views

DSP attribute view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The redirection function of the MQC is used for routing voice packets.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

A traffic policy supports only filtering and redirection.

NOTE

After a traffic policy is applied, you cannot directly delete the traffic policy or traffic classifiers or traffic behaviors in the traffic policy. If the traffic policy that you want to delete has been applied to a DSP channel, run the **undo traffic-policy** command to unbind the traffic policy. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction of a DSP channel.

```
<Huawei> system-view
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] voice
```

```
[Huawei-voice] dsp-attribute
[Huawei-voice-dsp-attribute] traffic-policy p1 inbound
```

16.3.7 Voice Diagnose Commands

NOTE

- The following product models support voice functions (such as the PBX, SIP AG, and H.248 AG):
  - AR120 series: AR129CV, AR129CVW, and AR129CGVW-L
  - AR150 series: AR157VW and AR158EVW
  - AR160 series: AR161, AR169FVW, AR169FVW-8S, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR161FV-1P, and AR169FGVW-L
  - AR200 series: AR201VW-P, AR207V, AR207VW, and AR207V-P
  - AR1200 series: AR1220V, AR1220VW, AR1220EV, and AR1220EVW
  - AR2200 series: AR2204, AR2220, AR2220L, AR2220E.
  - AR2240: For the equipped with SRU40, SRU60, SRU80, and SRU100.
  - AR3200 series: For the AR3260 equipped with SRU40, SRU60, SRU80, or SRU100, the same voice mode is set for the active and standby SRUs.

  The AR129CV, AR129CVW, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, and AR169CVW-4B4S only support the PBX and SIP AG, but not the H.248 AG.
- When an AR2204, AR2220L, or AR2220E router needs to provide voice services, install a DSP module and a voice subcard in the router. When an AR2220, AR2240, or AR3200 router needs to provide voice services, install a DSP module.
- To provide voice services to POTS users on the AR1200, AR2200, or AR3200, install the 4FXS1FXO, 16FXS, or 32FXS card. The AR1200 does not support the 32FXS card.
- To provide voice services to ISDN phone users on the AR1200, AR2200, or AR3200, install the 2BST card.
- To connect an AR1200, AR2200, or AR3200 router to a TDM PBX through the E1 interface, install the E1T1-M card.
- On the AR169FGVW-L, AR1220EV, and AR1220EVW, the AT0 trunk cannot be connected to the SIP server or SIP trunk.

16.3.7.1 clip port

Function

The **clip port** command is used to test the display of the POTS calling number.

Format

clip port *slot-id* { **transwhen** *transwhen-value* | **format** *format-value* | **reversepole-beforecid** *reversepole-before-cid-value* | **input-gain** *input-gain-value* | **output-gain** *output-gain-value* | **telno** *telno-value* | **telname** *telname-value* }*

Parameters

Parameter	Description	Value
slot-id	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.
transwhen *transwhen-value*	Displays the time.	Enumerated type. The values are as follows: ● after-ring ● before-ring
format *format-value*	Displays the format.	Enumerated type. The values are as follows: ● SDMF ● MDMF ● DTMF ● ETSI ● R15
reversepole-beforecid *reversepole-before-cid-value*	Displays the polarity reversal tag before a number.	Enumerated type. The values are as follows: ● disable ● enable
input-gain *input-gain-value*	Indicates the input gain.	The value is an integer that ranges from 0 to 15.
output-gain *output-gain-value*	Indicates the output gain.	The value is an integer that ranges from 0 to 20.
telno *telno-value*	Displays the calling number.	The value is a string of 1 to 32 characters.
telname *telname-value*	Displays the calling name.	The value is a string of 1 to 32 characters.

Views

Voice Diagnostic view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Configure the tested POTS calling number to be displayed after ringing.

```
<Huawei> system-view
[Huawei] diagnose
[Huawei-diagnose] clip port 1/0/0 transwhen after-ring
```

16.3.7.2 debugging voice-adapt

Function

the **debugging voice-adapt** command is used to configure debugging print level for voice-adapt-related modules.

Format

debugging voice-adapt { **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** } *debug-level-value*

undo debugging voice-adapt { **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** }

display voice-adapt debugging { **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** }

Parameters

Parameter	Description	Value
{ **emtest** | **vproduct** | **vpm** | **vcm** | **vam** | **vom** | **volc** | **vnet** | **vrm** | **vsp** }	Module name.	-
debug-level-value	Debugging print level.	Enumerated value: ● error ● event ● trace ● all

Views

Diagnostic views

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Switch on debugging print for voice-adapt-related modules. Used for troubleshooting.

Example

Set debugging print level for vproduct module to be all.

```
[Huawei-diagnose] debugging voice-adapt vproduct all
```

undo all debugging print from vom module.

```
[Huawei-diagnose] undo debugging voice-adapt vom
```

16.3.7.3 diagnose

Function

The **diagnose** command displays the Diagnostic view.

Format

diagnose

Parameters

None

Views

Voice view

Default Level

3: Management level

Usage Guidelines

None

Example

Enter the Diagnostic view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]
```

16.3.7.4 digit-trace

Function

The **digit-trace** command is used to enable POTS number diagnosis.

The **undo digit-trace** command is used to disable POTS number diagnosis.

Format

digit-trace *slotid/subcardid/portid*

undo digit-trace *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable POTS number diagnosis

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]digit-trace 1/0/0
```

16.3.7.5 display fe slot fe-id table port-map dsp-port base-port

Function

The **display fe slot fe-id table port-map dsp-port base-port** command displays voice portmap entries.

Format

display fe slot *slot-id* **fe-id** *fe-id* **table port-map dsp-port** *dsp-port-num* **base-port** *base-port-num*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value is the slot where the LPU is installed.
fe-id *fe-id*	Specifies the multicore forwarding engine number.	The value is an integer that ranges from 0 to 256.
dsp-port *dsp-port-num*	Specifies the DSP port number.	The value is an integer that ranges from 61440 to 65535.
base-port *base-port-num*	Specifies the BASE port number.	The value is an integer that ranges from 0 to 61440.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display voice portmap entries of BASE port 0 in DSP port 61440 of engine 0 in slot 0.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] display fe slot 0 fe-id 0 table port-map dsp-port 61440 base-port 0
memory data:
0000 0000
```

16.3.7.6 display fe slot fe-id table voice-mr dest-ip port protocol

Function

The **display fe slot fe-id table voice-mr dest-ip port protocol** command displays the VoiceMr table.

Format

display fe slot *slot-id* **fe-id** *fe-id* **table voice-mr dest-ip** *ip-address* **port** *port-num* **protocol** *protocol-num*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value is the slot where the LPU is installed.
fe-id *fe-id*	Specifies the multicore forwarding engine number.	The value is an integer that ranges from 0 to 256.
dest-ip *ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.
port *port-num*	Specifies the port number.	The value is an integer that ranges from 0 to 65535.
protocol *protocol-num*	Specifies the protocol number.	The value is an integer that ranges from 0 to 255.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the VoiceMr table of engine 0 in slot 0. Engine 0 has destination IP address 192.168.0.1, port number 10, and protocol number 0.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] display fe slot 0 fe-id 0 table voice-mr dest-ip 192.168.0.1 port 10 protocol 0
memory data:
0000 0000
```

16.3.7.7 display fe slot fe-id table voice-signal

Function

The **display fe slot fe-id table voice-signal** command displays voice signaling entries.

Format

display fe slot *slot-id* **fe-id** *fe-id* **table voice-signal** *ip-address port-num protocol-num*

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID.	The value is the slot where the LPU is installed.
fe-id *fe-id*	Specifies the multicore forwarding engine number.	The value is an integer that ranges from 0 to 256.
ip-address	Specifies the destination IP address.	The value is in dotted decimal notation.
port-num	Specifies the destination port number.	The value is an integer that ranges from 5000 to 5999.
protocol-num	Specifies the protocol number.	The value is an integer that ranges from 6 to 17.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the voice signaling entry of engine 0 in slot 0. Engine 0 has destination IP address 192.168.0.1, port number 5000, and protocol number 7.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] display fe slot 0 fe-id 0 table voice-signal 192.168.0.1 5000 7
memory data:
0000 0000
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.7.8 display pots loop-line-threshold

Function

The **display pots loop-line-threshold** command is used to check the POTS loop line detection threshold.

Format

display pots loop-line-threshold

Parameters

None

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Check the POTS loop line detection threshold.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]display pots loop-line-threshold
 ---------------------------------------------------------------------------
  Loop-line test threshold item                                   Value
 ---------------------------------------------------------------------------
  Touch the power line : AC voltage threshold(volt)                  55
  Loop-line mixed with others:DC voltage threshold(volt)              40
  Loop-line grounding: ground resistance threshold(ohm)              20000
  Off-hook: A-B resistance min. threshold(ohm)                      100
  Off-hook: A-B resistance max. threshold(ohm)                     100000
  Off-hook: loop resistance min. threshold(ohm)                    2000
  Off-hook: loop resistance max. threshold(ohm)                    2000
  Loop-line mixed with others: A-B resistance threshold(ohm)          2000
  A-B poor insulation:A-B resistance min. threshold(ohm)             2000
  A-B poor insulation:A-B resistance max. threshold(ohm)             20000
  Leakage: ground capacitance threshold(nF)                         700
  Normal: ground capacitance threshold 1(nF)                        200
  Normal: ground capacitance threshold 2(nF)                        350
  Normal: ground capacitance threshold 3(nF)                         50
 ---------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.7.9 display pots subcard-loopline-adjust

Function

The **display pots subcard-loopline-adjust** command is used to check the calibration value in the scenario of POTS user port disconnection and self-mixing.

Format

display pots subcard-loopline-adjust [**from** *startframeid* [**to** *endframeid*] | *frameid*]

Parameters

Parameter	Description	Value
from *startframeid*	Specifies the start frame ID.	The value is fixed at 0.
to *endframeid*	Specifies the end frame ID.	The value is fixed at 0.
frameid	Specifies a frame ID.	The value is fixed at 0.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Check the calibration value in the scenario of POTS user port disconnection and self-mixing.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]display pots subcard-loopline-adjust
  ------------------------------------------------------------
  FrameID    Adjust flag    CAB(nF)  CAG(nF)  CBG(nF)  RAB(ohm)
  ------------------------------------------------------------
      0          Null          -        -        -        -
  ------------------------------------------------------------
  Total: All 0, Capacitance 0, Resistance 0, Null 1
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.7.10 display voice device state

Function

The **display voice device state** command displays device voice status.

Format

display voice device state

Parameters

None

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View device voice status.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice device state
  pots user number          : 0
  bra user number           : 0
  sipue user number         : 252
  Sipat0 trunk number       : 250
  At0 trunk number          : 1
  Pra trunk circuit number : 32
  R2 trunk circuit number  : 0
  Sip trunk group number   : 2
  H323 trunk group number  : 0
  Active call number        : 0
  Max call number           : 80
```

16.3.7.11 display voice statistics module at0

Function

The **display voice statistics module at0** command displays statistical information about the AT0 module.

Format

display voice statistics module at0 [**srv** | **line** | **rm**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the AT0 module.	-
line	Specifies LINE statistical information about the AT0 module.	-
rm	Specifies RM statistical information about the AT0 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the AT0 module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module at0
  Srv Messages:
  Send_Alerting       : 0
  Send_CallProceeding : 0
  Send_Progress       : 0
  Send_Setup          : 0
  Send_Connect        : 0
  Send_SetupAck       : 0
  Send_Disconnect     : 0
  Send_Release        : 0
  Send_RestartAck     : 0
  Send_Facility       : 0
  Send_Notify         : 0

  Recv_Alerting       : 0
  Recv_CallProceeding : 0
  Recv_Progress       : 0
  Recv_Setup          : 0
  Recv_Connect        : 0
  Recv_SetupAck       : 0
  Recv_Disconnect     : 0
  Recv_Release        : 0
  Recv_RestartAck     : 0
  Recv_Facility       : 0
  Recv_Notify         : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Line Messages:
Send_OccupyTrunk      : 0
Send_ReleaseTrunk     : 0
Send_SendNumber       : 0
Send_SetActive        : 0
Send_SetA/MuLaw       : 0
Send_SetGain          : 0
Send_SetNumberType    : 0
Send_SetRecvDTMF      : 0
Send_SetDTMFPara      : 0
Send_SetPulsePara     : 0
Send_ResetChannel     : 0
Send_ResetBoard       : 0
Send_InquireVersion   : 0
Send_SetRingAttribute : 0
Send_SetFeedVoltage   : 0
Send_SetFeedCurrent   : 0
Send_SetImpedance     : 0
Send_TsLoop           : 0

Recv_OccupyConfirm      : 0
Recv_CallInCome         : 0
Recv_CallRelease        : 0
Recv_PolarityReverse    : 0
Recv_SecondDialNumber   : 0
Recv_CallerIdRecvEnd    : 0
Recv_SendNumberComplete : 0
Recv_UtdDetect          : 0
Recv_ChannelResetOk     : 1
Recv_ChannelResetFault  : 1

Rm Messages:
Send_Alloc            : 2
Send_Release          : 2
Send_Add              : 0
Send_Del              : 0
Send_HandleOpen       : 1
Send_HandleClose      : 0
Send_HandleSendTone   : 0
Send_HandleStopTone   : 0
Send_HandleSendFSK    : 0
Send_HandleInsertDTMF : 0

Recv_Alloc            : 2
Recv_Release          : 2
Recv_Add              : 0
Recv_Del              : 0
Recv_HandleOpen       : 1
Recv_HandleClose      : 0
Recv_HandleSendTone   : 0
Recv_HandleStopTone   : 0
Recv_HandleSendFSK    : 0
Recv_HandleInsertDTMF : 0
```

16.3.7.12 display voice statistics module h323

Function

The **display voice statistics module h323** command displays statistical information about the H323 module.

Format

display voice statistics module h323 [**srv** | **h225** | **h245** | **ras**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the H323 module.	-
h225	Specifies H225 statistical information about the H323 module.	-
h245	Specifies H245 statistical information about the H323 module.	-
ras	Specifies RAS statistical information about the H323 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the H323 module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module h323
  Srv Sent Messages:
  Send_Setup           : 0
  Send_SetupAck        : 0
  Send_Callproceeding  : 0
  Send_Alerting        : 0
  Send_Connect         : 0
  Send_ConnectAck      : 0
  Send_ReleaseComplete : 0
  Send_Progress        : 0
  Send_ProgressRsp     : 0
  Send_ProgressAck     : 0
  Send_Information     : 0
  Send_Facility        : 0
  Send_Bearinfo        : 0
  Send_BearinfoRsp     : 0
  Send_BearinfoAck     : 0
  Send_GRQ             : 0
  Send_GCF             : 0
  Send_GRJ             : 0
  Send_RRQ             : 0
  Send_RCF             : 0
  Send_RRJ             : 0
  Send_LRQ             : 0
  Send_LCF             : 0
  Send_LRJ             : 0
  Send_ARQ             : 0
```

```
Send_ACF            : 0
Send_ARJ            : 0
Send_URQ            : 0
Send_UCF            : 0
Send_URJ            : 0
Send_DRQ            : 0
Send_DCF            : 0
Send_DRJ            : 0

Srv received Messages:
Recv_Setup          : 0
Recv_SetupAck       : 0
Recv_Callproceeding  : 0
Recv_Alerting       : 0
Recv_Connect        : 0
Recv_ConnectAck     : 0
Recv_ReleaseComplete : 0
Recv_Progress       : 0
Recv_ProgressRsp    : 0
Recv_ProgressAck    : 0
Recv_Information    : 0
Recv_Facility       : 0
Recv_Bearinfo       : 0
Recv_BearinfoRsp    : 0
Recv_BearinfoAck    : 0
Recv_GRQ            : 0
Recv_GCF            : 0
Recv_GRJ            : 0
Recv_RRQ            : 0
Recv_RCF            : 0
Recv_RRJ            : 0
Recv_LRQ            : 0
Recv_LCF            : 0
Recv_LRJ            : 0
Recv_ARQ            : 0
Recv_ACF            : 0
Recv_ARJ            : 0
Recv_URQ            : 0
Recv_UCF            : 0
Recv_URJ            : 0
Recv_DRQ            : 0
Recv_DCF            : 0
Recv_DRJ            : 0

H225 Sent Messages:
Send_Setup                    : 0
Send_SetupAck                 : 0
Send_Callproceeding           : 0
Send_Alerting                 : 0
Send_Connect                  : 0
Send_ReleaseComplete          : 0
Send_FacilityTCSQequest       : 0
Send_FacilityTCSAck           : 0
Send_FacilityTCSReject        : 0
Send_FacilityOLCRequest       : 0
Send_FacilityOLCAck           : 0
Send_FacilityOLCReject        : 0
Send_FacilityMSDRequest       : 0
Send_FacilityMSDAck           : 0
Send_FacilityCLCRequest       : 0
Send_FacilityCLCAck           : 0
Send_FacilityRequestMode      : 0
Send_FacilityRequestModeAck   : 0
Send_FacilityRequestModeReject : 0
Send_Progress                 : 0

H225 received Messages:
Recv_Setup                    : 0
Recv_SetupAck                 : 0
```

```
Recv_Callproceeding            : 0
Recv_Alerting                  : 0
Recv_Connect                   : 0
Recv_ReleaseComplete           : 0
Recv_FacilityTCSQequest        : 0
Recv_FacilityTCSAck            : 0
Recv_FacilityTCSReject         : 0
Recv_FacilityOLCRequest        : 0
Recv_FacilityOLCAck            : 0
Recv_FacilityOLCReject         : 0
Recv_FacilityMSDRequest        : 0
Recv_FacilityMSDAck            : 0
Recv_FacilityCLCRequest        : 0
Recv_FacilityCLCAck            : 0
Recv_FacilityRequestMode       : 0
Recv_FacilityRequestModeAck    : 0
Recv_FacilityRequestModeReject : 0
Recv_Progress                  : 0

H245 sent Messages:
Send_TCSRequest        : 0
Send_TCSAck            : 0
Send_TCSReject         : 0
Send_OlcRequest        : 0
Send_OlcAck            : 0
Send_OlcReject         : 0
Send_MsdRequest        : 0
Send_MsdAck            : 0
Send_ClcRequest        : 0
Send_ClcAck            : 0
Send_StartH245         : 0
Send_RequestMode       : 0
Send_RequestModeAck    : 0
Send_RequestModeReject : 0

H245 received Messages:
Recv_TCSRequest        : 0
Recv_TCSAck            : 0
Recv_TCSReject         : 0
Recv_OlcRequest        : 0
Recv_OlcAck            : 0
Recv_OlcReject         : 0
Recv_MsdRequest        : 0
Recv_MsdAck            : 0
Recv_ClcRequest        : 0
Recv_ClcAck            : 0
Recv_StartH245         : 0
Recv_RequestMode       : 0
Recv_RequestModeAck    : 0
Recv_RequestModeReject : 0

Ras sent Messages:
Send_GRQ            : 0
Send_GCF            : 0
Send_GRJ            : 0
Send_RRQ            : 0
Send_RCF            : 0
Send_RRJ            : 0
Send_LRQ            : 0
Send_LCF            : 0
Send_LRJ            : 0
Send_ARQ            : 0
Send_ACF            : 0
Send_ARJ            : 0
Send_URQ            : 0
Send_UCF            : 0
Send_URJ            : 0
Send_DRQ            : 0
Send_DCF            : 0
```

```
Send_DRJ            : 0
Send_CheckADMStatus : 0
Send_ADMStatus      : 0

Ras received Messages:
Recv_GRQ            : 0
Recv_GCF            : 0
Recv_GRJ            : 0
Recv_RRQ            : 0
Recv_RCF            : 0
Recv_RRJ            : 0
Recv_LRQ            : 0
Recv_LCF            : 0
Recv_LRJ            : 0
Recv_ARQ            : 0
Recv_ACF            : 0
Recv_ARJ            : 0
Recv_URQ            : 0
Recv_UCF            : 0
Recv_URJ            : 0
Recv_DRQ            : 0
Recv_DCF            : 0
Recv_DRJ            : 0
Recv_CheckADMStatus : 0
Recv_ADMStatus      : 0
```

16.3.7.13 display voice statistics module pots

Function

The **display voice statistics module pots** command displays statistical information about the POTS module.

Format

display voice statistics module pots [**srv** | **line**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the POT0 module.	-
line	Specifies LINE statistical information about the POT0 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the POTS module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module pots
  Srv Messages:
  Recv_StartRing            : 0
  Recv_Stop_Ring            : 1
  Recv_InitRing             : 1
  Recv_StartService         : 0
  Recv_EndService           : 0
  Recv_EndServiceByCa       : 0
  Recv_EndServiceAck        : 0
  Recv_RingSendTelnum       : 0
  Recv_SendTelnum           : 0
  Recv_SendAoce             : 0
  Recv_Light                : 0
  Recv_OverLight            : 0
  Recv_RingSplash           : 0
  Recv_Lock                 : 2
  Recv_NomalLineFeed        : 0
  Recv_Reverse              : 0
  Recv_KC                   : 0
  Recv_EndOfCall            : 0
  Recv_DisconnectClear      : 0
  Recv_DisconnectClearFail : 0
  Recv_TempFlashhookTime    : 0
  Recv_NoBattery            : 0
  Recv_NormalPolarity       : 0
  Recv_Hold                 : 0
  Recv_TransmitEnable       : 0
  Recv_TransmitDisenable    : 0

  Line Messages:
  Send_DialReport           : 2
  Send_OffHook              : 2
  Send_StopDialTone         : 0
  Send_OnHook               : 1
  Send_Hooking              : 0
  Send_CalledHook           : 0
  Send_StartFSK             : 1
  Send_RingFail             : 0
  Send_PortStatReport       : 0
  Send_TSLoopAck            : 0
  Send_CancelTSLoopAck      : 0
  Send_EarthConnect         : 0
  Send_EarthCancel          : 0
  Send_RecvGain             : 0
  Send_SendGain             : 0
  Send_DisconnectClearAck : 0
  Send_PortFail             : 1
  Send_PortResume           : 2
  Send_PortLoop             : 0
  Send_LoopCancel           : 0
  Send_LineTestStart        : 0
  Send_LineTestStop         : 0
  Send_GTCTestStart         : 0
  Send_GTCTestStop          : 0
  Send_LineFail             : 0
  Send_LineResume           : 0
  Send_PowerPermissible     : 0
  Send_PowerOverloadBuff    : 0
  Send_PowerOverloadLimit : 0
```

16.3.7.14 display voice statistics module q931

Function

The **display voice statistics module q931** command displays statistical information about the Q931 module.

Format

display voice statistics module q931 { **srv** | **protocol** } [**net** | **te**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the Q931 module.	-
protocol	Specifies protocol statistical information about the Q931 module.	-
net	Specifies NET statistical information about the Q931 module.	-
te	Specifies TE statistical information about the Q931 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the Q931 module.

```
<Huawei>system-view
[Huawei]diag
Now you enter a diagnostic command view for developer's testing, some commands
may affect operation by wrong use, please carefully use it with HUAWEI
engineer's direction.
[Huawei-diagnose]display voice statistics module q931
  Srv Net Sent Messages:
  Send_Alerting          : 0
  Send_CallProceeding    : 0
  Send_Progress          : 0
  Send_Setup             : 0
  Send_Connect           : 0
  Send_SetupAck          : 0
  Send_ConnectAck        : 0
  Send_UserInformation   : 0
  Send_SuspendReject     : 0
  Send_ResumeReject      : 0
  Send_Hold              : 0
```

```
Send_Suspend           : 0
Send_Resume            : 0
Send_HoldAck           : 0
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Srv Net Received Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0

Srv User Sent Messages:
Send_Alerting          : 0
Send_CallProceeding    : 0
Send_Progress          : 0
Send_Setup             : 0
Send_Connect           : 0
Send_SetupAck          : 0
Send_ConnectAck        : 0
Send_UserInformation   : 0
Send_SuspendReject     : 0
Send_ResumeReject      : 0
Send_Hold              : 0
Send_Suspend           : 0
```

```
Send_Resume            : 0
Send_HoldAck           : 0
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Srv User Rreceived Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0

Protocol Net Sent Messages:
Send_Alerting          : 0
Send_CallProceeding    : 0
Send_Progress          : 0
Send_Setup             : 0
Send_Connect           : 0
Send_SetupAck          : 0
Send_ConnectAck        : 0
Send_UserInformation   : 0
Send_SuspendReject     : 0
Send_ResumeReject      : 0
Send_Hold              : 0
Send_Suspend           : 0
Send_Resume            : 0
```

```
Send_HoldAck           : 0
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Protocol Net Received Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0

Protocol User Sent Messages:
Send_Alerting          : 0
Send_CallProceeding    : 0
Send_Progress          : 0
Send_Setup             : 0
Send_Connect           : 0
Send_SetupAck          : 0
Send_ConnectAck        : 0
Send_UserInformation   : 0
Send_SuspendReject     : 0
Send_ResumeReject      : 0
Send_Hold              : 0
Send_Suspend           : 0
Send_Resume            : 0
Send_HoldAck           : 0
```

```
Send_SuspendAck        : 0
Send_ResumeAcknowledge : 0
Send_HoldReject        : 0
Send_Retrieve          : 0
Send_RetrieveAck       : 0
Send_RetrieveReject    : 0
Send_Disconnect        : 0
Send_Restart           : 0
Send_Release           : 0
Send_RestartAck        : 0
Send_ReleaseComplete   : 0
Send_SegmDss1          : 0
Send_Facility          : 0
Send_Notify            : 0
Send_Statusdss1Query   : 0
Send_CongestionControl : 0
Send_Information       : 0
Send_Status            : 0

Protocol User Received Messages:
Recv_Alerting          : 0
Recv_CallProceeding    : 0
Recv_Progress          : 0
Recv_Setup             : 0
Recv_Connect           : 0
Recv_SetupAck          : 0
Recv_ConnectAck        : 0
Recv_UserInformation   : 0
Recv_SuspendReject     : 0
Recv_ResumeReject      : 0
Recv_Hold              : 0
Recv_Suspend           : 0
Recv_Resume            : 0
Recv_HoldAck           : 0
Recv_SuspendAck        : 0
Recv_ResumeAcknowledge : 0
Recv_HoldReject        : 0
Recv_Retrieve          : 0
Recv_RetrieveAck       : 0
Recv_RetrieveReject    : 0
Recv_Disconnect        : 0
Recv_Restart           : 0
Recv_Release           : 0
Recv_RestartAck        : 0
Recv_ReleaseComplete   : 0
Recv_SegmDss1          : 0
Recv_Facility          : 0
Recv_Notify            : 0
Recv_Statusdss1Query   : 0
Recv_CongestionControl : 0
Recv_Information       : 0
Recv_Status            : 0
```

16.3.7.15 display voice statistics module r2

Function

The **display voice statistics module r2** command displays statistical information about the R2 module.

Format

display voice statistics module r2 [**srv** | **rs** | **line**]

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the R2 module.	-
rs	Specifies RS statistical information about the R2 module.	-
line	Specifies LINE statistical information about the R2 module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the R2 module.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose]display voice statistics module r2
  Srv Messages:
  Send_Alerting       : 0
  Send_CallProceeding : 0
  Send_Progress       : 0
  Send_Setup          : 0
  Send_Connect        : 0
  Send_ConnectAck     : 0
  Send_SetupAck       : 0
  Send_Disconnect     : 0
  Send_Release        : 0
  Send_RestartAck     : 0
  Send_Segment        : 0
  Send_Facility       : 0
  Send_Notify         : 0

  Recv_Alerting       : 0
  Recv_CallProceeding : 0
  Recv_Progress       : 0
  Recv_Setup          : 0
  Recv_Connect        : 0
  Recv_ConnectAck     : 0
  Recv_SetupAck       : 0
  Recv_Disconnect     : 0
  Recv_Release        : 0
  Recv_RestartAck     : 0
  Recv_Segment        : 0
  Recv_Facility       : 0
  Recv_Notify         : 0

  Line Messages:
  Send_Seize        : 0
  Send_SeizeAck     : 0
  Send_Answer       : 0
  Send_ClearForward : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Send_ClearBack    : 0
Send_CASFailure   : 0
Send_Block        : 0
Send_UnBlock      : 0
Send_Idle         : 0
Send_Error        : 0
Send_InService    : 0
Send_OutService   : 0

Recv_Seize        : 0
Recv_SeizeAck     : 0
Recv_Answer       : 0
Recv_ClearForward : 0
Recv_ClearBack    : 0
Recv_CASFailure   : 0
Recv_Block        : 0
Recv_UnBlock      : 0
Recv_Idle         : 0
Recv_Error        : 0
Recv_InService    : 0
Recv_OutService   : 0

Rs Messages:
Send_PropertySrcNumLen  : 0
Send_PropertyCmpSeqTime : 0
Send_EventRequset       : 0
Send_SignalR2addr       : 0
Send_SignalCongestion   : 0
Send_SignalCPRS         : 0
Send_SignalStop         : 0
Send_DmmMatchResult     : 0

Recv_R2addr      : 0
Recv_CPRS        : 0
Recv_R2F         : 0
Recv_DI          : 0
Recv_SI          : 0
Recv_SC          : 0
Recv_ES          : 0
Recv_CC          : 0
Recv_DISC        : 0
Recv_NAC         : 0
Recv_CNG         : 0
Recv_SubPrio     : 0
Recv_CasFail     : 0
Recv_SignalCOMPL : 0
Recv_RecvNum     : 0
Recv_BGRPAck     : 0
Recv_ChargeType  : 0
```

16.3.7.16 display voice statistics module sip

Function

The **display voice statistics module sip** command displays statistical information about the SIP module.

Format

display voice statistics module sip { **srv** | **protocol** }

Parameters

Parameter	Description	Value
srv	Specifies SRV statistical information about the RIP module.	-
protocol	Specifies protocol statistical information about the RIP module.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

View statistical information about the SIP module.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose]display voice statistics module sip
  Protocol Sent Request Messages:
  Send_Invite    : 0
  Send_Ack       : 0
  Send_Bye       : 0
  Send_Cancel    : 0
  Send_Register  : 0
  Send_Info      : 0
  Send_Update    : 0
  Send_Subscribe : 0
  Send_Notify    : 0
  Send_Message   : 0
  Send_Refer     : 0
  Send_Options   : 2298
  Send_Prack     : 0

  Protocol Received Request Messages:
  Recv_Invite    : 0
  Recv_Ack       : 0
  Recv_Bye       : 0
  Recv_Cancel    : 0
  Recv_Register  : 24
  Recv_Info      : 0
  Recv_Update    : 0
  Recv_Subscribe : 0
  Recv_Notify    : 0
  Recv_Message   : 0
  Recv_Refer     : 0
  Recv_Options   : 1529
  Recv_Prack     : 0

  Protocol Sent Response Messages:
  Send_1XX : 0
  Send_2XX : 1529
  Send_3XX : 0
```

```
Send_4XX : 0
Send_5XX : 0
Send_6XX : 0

Protocol Received Response Messages:
Recv_1XX : 0
Recv_2XX : 1530
Recv_3XX : 0
Recv_4XX : 0
Recv_5XX : 0
Recv_6XX : 0

Srv Sent Messages:
Send_Alerting          : 0
......
```

16.3.7.17 pots circuit-test

Function

The **pots circuit-test** command triggers a POTS internal line test.

Format

pots circuit-test { *slot-id* | **telno** *telno-value* | **mgid** *mgid-value* | **terminalid** *terminalid-value* } [**busy** { **cancel** | **force** | **defer** [**deferred-time** *deferred-time-value* | **timeout-proc** *timeout-proc-value*] }]

Parameters

Parameter	Description	Value
slot-id	Specifies a slot ID/subcard ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters.
telno *telno-value*	Specifies a test number.	The value is a string of 1 to 16 characters.
mgid *mgid-value*	Specifies a gateway ID.	The value is an integer that ranges from 0 to 16777215.
terminalid *terminalid-value*	Specifies a terminal ID.	The value is an integer that ranges from 0 to 16777215.
deferred-time *deferred-time-value*	Specifies the delay.	The value is an integer that ranges from 1 to 1440.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
timeout-proc *timeout-proc-value*	Specifies the timeout period.	Enumerated value. ● 0: It does not POTS internal line test when timeout. ● 1: It will be tested mandatorily upon timeout.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Trigger a POTS internal line test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots circuit-test 5/0/0
  slot 5 subcard 0 port 0 ( telno 5000 mgid - terminalid - )
  under testing, Please wait......
[Huawei-voice-vdiagnose]
  Testing port:  5/0/0
  Telno       :  5000
  MGid        :  -
  Terminalid  :  -
  -------------------------------------------------------
  Test item                              Result
  -------------------------------------------------------
  Digital Voltage:                        Normal
  Low Battery:                            Normal
  High Battery:                           Normal
  Positive Battery:                       Normal
  Feeder voltage:                          Normal
  Loop current:                           Normal
  Ringing current voltage:                    Normal
  Ringing current frequency:                   Normal
  VAG:                                  Normal
  VBG:                                  Normal
  -------------------------------------------------------
  Feeder voltage(V):                       47.830
  Ringing current voltage(V):                0.000
  Loop current(mA):                         0.000
  -------------------------------------------------------
```

16.3.7.18 pots loop-line-test

Function

The **pots loop-line-test** command triggers a POTS external line test.

Format

pots loop-line-test { *slot-id* | **telno** *telno-value* | **mgid** *mgid-value* **terminalid** *terminalid-value* } [**busy** { **cancel** | **force** | **defer** [**deferred-time** *deferred-time-value* | **timeout-proc** *timeout-proc-value*] }]

Parameters

Parameter	Description	Value
slot-id	Specifies a slot ID/subcard ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. ● *slotid*: based on product specifications ● *subcardid*: based on product specifications ● *portid*: based on product specifications
telno *telno-value*	Specifies a test number.	The value is a string of 1 to 16 characters.
mgid *mgid-value*	Specifies a gateway ID.	The value is an integer that ranges from 0 to 16777215.
terminalid *terminalid-value*	Specifies a terminal ID.	The value is an integer that ranges from 0 to 16777215.
deferred-time *deferred-time-value*	Specifies the delay.	The value is an integer that ranges from 1 to 1440.
timeout-proc *timeout-proc-value*	Specifies the timeout period.	Enumerated value. ● 0: It does not POTS internal line test when timeout. ● 1: It will be tested mandatorily upon timeout.

Views

Voice Diagnostic view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Trigger a POTS external line test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots loop-line-test 5/0/0
  slot 5 subcard 0 port 0 ( telno 5000 mgid - terminalid - )
  under testing, Please wait......
[Huawei-voice-vdiagnose]
  Testing port:  5/0/0
  Telno       :  5000
  MGid        :  -
  Terminalid  :  -
  ---------------------------------------------------------------------------
  Test item                                Result
  ---------------------------------------------------------------------------
  A->ground AC voltage              (V)       0.000
  B->ground AC voltage              (V)       0.000
  A->B      AC voltage              (V)       0.000
  A->ground DC voltage              (V)      -1.474
  B->ground DC voltage              (V)      -1.438
  A->B      DC voltage              (V)      -0.036
  A->ground insulation resistance  (ohm)    >10M
  B->ground insulation resistance  (ohm)    >10M
  A->B insulation resistance       (ohm)     1.333M
  A->B loop resistance             (ohm)     0
  A->B polarity reversal resistance(ohm)     1.333M
  A->ground capacitance            (uF)      0.050
  B->ground capacitance            (uF)      0.050
  A->B capacitance                 (uF)      0.000
  Conclusion                               Phone not connected
  ---------------------------------------------------------------------------
```

16.3.7.19 pots loop-line-threshold

Function

The **pots loop-line-threshold** command configures detection thresholds for POTS external line tests.

Format

pots loop-line-threshold { **restore** | **set** *threshold-type threshold-value* }

Parameters

Parameter	Description	Value
restore	Restore thresholds for POTS external line tests.	-

Parameter	Description	Value
threshold-type	Specifies an external line test standard.	The value is an integer. The options are as follows: ● 0: A/B wire touching the power line: AC voltage ● 1: external line mixing: DC voltage ● 2: external line grounding: resistance to ground ● 3: off-hook: resistance lower limit between A and B wires ● 4: off-hook: resistance upper limit between A and B wires ● 5: off-hook: loop resistance lower limit ● 6: off-hook: loop resistance upper limit ● 7: external line mixing: resistance between A and B wires ● 8: poor insulation between A and B wires: resistance lower limit between A and B wires ● 9: poor insulation between A and B wires: resistance upper limit between A and B wires ● 10: electric leakage: grounding capacitance ● 11: normal: minimum grounding capacitance ● 12: normal: capacity between A and B wires ● 13: normal: minimum grounding capacitance

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
threshold-value	Specifies the value of an external test standard.	The value is a hexadecimal integer that ranges from 0x0 to 0x7fffffff.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Set the POTS external line test standard "external line grounding: resistance to ground" to 5.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots loop-line-threshold set 2 0x5
```

16.3.7.20 pots path-test

Function

The **pots path-test** command triggers a POTS hardware or service test.

Format

pots path-test *slotid/subcard* **port all type** { **hardware** | **business** }

pots path-test *slotid/subcard* **port** *port-id* **type** { **hardware** | **business** } [**assist-port** *port-id*]

undo pots path-test *slotid/subcard*

Parameters

Parameter	Description	Value
slotid/subcard	Specifies a slot ID/subcard ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. • *slotid*: based on product specifications • *subcardid*: based on product specifications
port-id	Specifies a port number.	The value is an integer that ranges from 0 to 63.
type	Specifies the test type.	Enumerated type. The value can be hardware or business.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

To trigger a POTS hardware or service test, run **pots path-test** command.

Example

Trigger a POTS hardware test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] diagnose
[Huawei-voice-vdiagnose] pots path-test 6/0 port all type hardware
  This operation will take several minutes, please wait...
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/0        Assist port :  6/0/2
  Test result :  Normal
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/1        Assist port :  6/0/3
  Test result :  Normal
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/2        Assist port :  6/0/0
  Test result :  Normal
[Huawei-voice-vdiagnose]
  Dest port   :  6/0/3        Assist port :  6/0/1
  Test result :  Normal
```

 Copyright © Huawei Technologies Co., Ltd.

16.3.7.21 pots subcard-loopline-adjust get

Function

The **pots subcard-loopline-adjust get** command displays calibration values for frame analog user ports in external line disconnection and self-mixed situations.

Format

pots subcard-loopline-adjust get *frameid* { **cutline-port***slotid1/portid1* | **selfmixed-port** *slotid2/portid2* } *

Parameters

Parameter	Description	Value
frameid	Specifies a frame ID.	The value is fixed at 0.
cutline-port *slotid1/portid1*	Specifies a slot ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. ● *slotid1*: based on product specifications ● *portid1*: based on product specifications
selfmixed-port *slotid2/portid2*	Specifies a slot ID/port ID. This parameter is mandatory and specifies the physical location of the user to be tested. The slash (/) must be retained.	The value is a string of 1 to 15 characters. ● *slotid2*: based on product specifications ● *portid2*: based on product specifications

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Display calibration values for frame analog user ports in external line disconnection and self-mixed situations.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots subcard-loopline-adjust get 0 cutline-port 5/0 selfmixed-port 5/1
  slot 5 subcard 0 port 0
  under geting adjust, Please wait......
[Huawei-voice-vdiagnose]
  -----------------------------------------
  slot 5 subcard 0 port 0 cutline adjust:
  -----------------------------------------
  CAB(nF)                    0
  CAG(nF)                    50
  CBG(nF)                    50
  -----------------------------------------
```

16.3.7.22 pots subcard-loopline-adjust restore

Function

The **pots subcard-loopline-adjust restore** command restores the default calibration values for frame analog user ports in external line disconnection and self-mixed situations.

Format

pots subcard-loopline-adjust restore { **from** *startframeid* [**to** *endframeid*] | *frameid* }

Parameters

Parameter	Description	Value
startframeid	Specifies the start frame ID.	The value is fixed at 0.
endframeid	Specifies the end frame ID.	The value is fixed at 0.
frameid	Specifies a frame ID.	The value is fixed at 0.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

Restore the default calibration values for frame analog user ports in external line disconnection and self-mixed situations.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots subcard-loopline-adjust restore 0
  Are you sure to restore the default value? (y/n)[n]:y
  Success: adjust of frame  0 restore successfully
```

16.3.7.23 pots subcard-loopline-adjust set

Function

The **pots subcard-loopline-adjust set** command sets or modifies calibration values for frame analog user ports in external line disconnection and self-mixed situations.

Format

pots subcard-loopline-adjust set { **from** *startframeid* [**to** *endframeid*] | *frameid* } { **cab** *cab-value* | **cag** *cag-value* | **cbg***cbg-value* | **rab** *rab-value* } *

Parameters

Parameter	Description	Value
startframeid	Specifies the start frame ID.	The value is fixed at 0.
endframeid	Specifies the end frame ID.	The value is fixed at 0.
frameid	Specifies a frame ID.	The value is fixed at 0.
cab-value	Specifies the capacity between A and B wires.	The value is an integer that ranges from 0 to 10000000.
cag-value	Specifies the grounding capacity of A wire.	The value is an integer that ranges from 0 to 10000000.
cbg-value	Specifies the grounding capacity of B wire.	The value is an integer that ranges from 0 to 10000000.
rab-value	Specifies the resistance between A and B wires.	The value is an integer that ranges from 0 to 10000000.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

To set or modifies calibration values for frame analog user ports in external line disconnection and self-mixed situations, run **pots subcard-loopline-adjust set** command.

Example

Modify calibration values for frame analog user ports in external line disconnection and self-mixed situations.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diag
[Huawei-voice-vdiagnose]pots subcard-loopline-adjust set 0 rab 5 cag 5
  Success: adjust of frame  0 set successfully
```

16.3.7.24 reset voice statistics module

Function

The **reset voice statistics module** command clears statistics on each module.

Format

reset voice statistics module { **at0** | **h323** | **pots** | **q931** | **r2** | **sip** }

Parameters

Parameter	Description	Value
at0	Clears statistics on AT0 messages.	-
h323	Clears statistics on H323 messages.	-
pots	Clears statistics on POTS messages.	-
q931	Clears statistics on Q931 messages.	-
r2	Clears statistics on R2 messages.	-
sip	Clears statistics on SIP messages.	-

Views

Diagnostic view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

You can run the **reset voice statistics module** command to clear statistics on each module.

Example

Clear statistics on the AT0 module.

```
<Huawei>system-view
[Huawei]diagnose
[Huawei-diagnose] reset voice statistics module at0
```

16.3.7.25 ts6em

Function

The **ts6em** command triggers the voice time slot test for dsp.

Format

ts6em slot-in *slot-in-id* **slot-out** *slot-out-id*

Parameters

Parameter	Description	Value
slot-in *slot-in-id*	Input slot ID. This parameter is mandatory and specifies the input of opening channel. It is also used for time slot switch.	The value is an integer of 0 to 12 characters.
slot-out *slot-out-id*	Output slot ID. This parameter is used for time slot switch.	The value is an integer of 0 to 12 characters.

Views

Voice Diagnostic view

Default Level

3: Management level

Usage Guidelines

None

Example

The **ts6em** command triggers the voice time slot test for dsp.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]diagnose
[Huawei-voice-vdiagnose]ts6em slot-in 1 slot-out 2
 The Test Statics:
 Time Slot:0 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:1 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:2 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:3 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:4 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
 Time Slot:5 --- Failed Errno: 6 Total Success Times: 0 Failed Times: 1
```

16.4 Voice interface Commands

16.4.1 Voice interface Configuration Commands

16.4.1.1 access-mode

Function

Using the **access-mode** command, you can set the access mode for a VE1 interface.

Using the **undo access-mode** command, you can restore the default access mode of a VE1 interface.

By default, the access mode of a VE1 interface is digital.

Format

access-mode { **digital** | **direct** }

undo access-mode

Parameters

Parameter	Description	Value
digital	Indicates the digital section access mode.	-
direct	Indicates the direct access mode.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

When the access mode is set to direct, all the SA bits of an E1 frame must be always set to 1s, and the loopback2 operation is not allowed. When the access mode is set to digital, an E1 interface must comply with ETS 300.233.

Example

Set the access mode of a VE1 interface to digital.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] access-mode digital
```

16.4.1.2 access-mode (BRA Interface View)

Function

The **access-mode** command configures the working mode of a basic rate access (BRA) interface.

The **undo access-mode** command restores the default working mode of a BRA interface.

By default, a BRA interface works in NT mode.

NOTE

Only AR169CVW-4B4S supports this command.

Format

access-mode *access-mode-value*

undo access-mode

Parameters

Parameter	Description	Value
access-mode-value	Specifies the working mode of a BRA interface.	Enumerated value. The options are as follows: ● te: The BRA interface works in Terminal Equipment (TE) mode. ● nt: The BRA interface work in Network Termination (NT) mode.

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device uses a BRA interface to connect to an ISDN phone, the BRA interface should work in NT mode. When a device uses a BRA interface to connect to an ISDN network, the BRA interface should work in TE mode.

Precautions

This command can only be used to configure the working mode of the BRA0/0/0 and BRA0/0/1 interfaces on the AR169CVW-4B4S.

Example

Configure a BRA interface to work in TE mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 0/0/0
[Huawei-voice-bra0/0/0] access-mode te
```

16.4.1.3 alarm

Function

Using the **alarm** command, you can enable or disable the UNI alarm function on a BRA interface.

Using the **undo alarm** command, you can restore the default configuration.

By default, the UNI alarm function is disabled on a BRA interface.

Format

alarm { **enable** | **disable** }

undo alarm

Parameters

Parameter	Description	Value
enable	Enables the UNI alarm function.	-
disable	Disables the UNI alarm function.	-

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the UNI alarm function on a BRA interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] alarm enable
```

16.4.1.4 crc4

Function

Using the **crc4** command, you can enable or disable cyclic redundancy check 4 (CRC4) on a VE1 interface.

Using the **undo crc4** command, you can restore the default configuration.

By default, CRC4 check is disabled on a VE1 interface.

Format

crc4 { **enable** | **disable** }

undo crc4

Parameters

Parameter	Description	Value
enable	Enables CRC4 check on a VE1 interface.	_
disable	Disables CRC4 check on a VE1 interface.	_

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable CRC4 check on a VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] crc4 enable
```

16.4.1.5 crc (VE1 interface view)

Function

The **crc** command sets the CRC mode on a VE1 interface.

The **undo crc** command restores the default setting.

By default, 16-bit CRC is used.

Format

crc { 16 | 32 | none }

undo crc

Parameters

Parameter	Description	Value
16	Configures 16-bit CRC on the interface.	-
32	Configures 32-bit CRC on the interface.	-
none	Configures no CRC on the interface.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Cyclic Redundancy Check (CRC) is often used to detect transmission errors in a communication system. CRC checks data consistency and provides high algorithm accuracy. A 32-bit field can achieve higher accuracy than a 16-bit field but uses more resources.

Precautions

If you run the **crc** command multiple times in the same VE1 interface view, only the latest configuration takes effect.

Example

Enable 32-bit CRC on the VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] crc 32
  Set crc successfully
```

16.4.1.6 crc-alarm-threshold

Function

Using the **crc-alarm-threshold** command, you can set the errored seconds threshold, consecutively severely errored seconds threshold, and degraded minute threshold.

Using the **undo crc-alarm-threshold** command, you can restore the default errored seconds threshold, consecutively severely errored seconds threshold, and degraded minute threshold.

 Copyright © Huawei Technologies Co., Ltd.

By default:

- The errored seconds threshold is 432 errored seconds per hour.
- The consecutively severely errored seconds threshold is 4 severely errored seconds per hour.
- The degraded minute threshold is 8 degraded minutes per hour.

Format

crc-alarm-threshold { **es** *es-threshold* | **cses** *cses-threshold* | **dm** *dm-threshold* }

undo crc-alarm-threshold { **es** | **cses** | **dm** }

Parameters

Parameter	Description	Value
es*es-threshold*	Specifies the errored seconds threshold.	The value is an integer that ranges from 1 to 3600. The unit is error seconds per hour. The default value is 432.
cses*cses-threshold*	Specifies the consecutively severely errored seconds threshold.	The value is an integer that ranges from 1 to 60. The unit is consecutively severely errored seconds per hour. The default value is 4.
dm*dm-threshold*	Specifies the degraded minute threshold.	The value is an integer that ranges from 1 to 60. The unit is degraded minutes per hour. The default value is 8.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the errored seconds threshold to 60, consecutively severely errored seconds threshold to 30, and degraded minute threshold to 30 on a VE1 interface.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] crc-alarm-threshold cses 30
[Huawei-voice-ve1-2/0/0] crc-alarm-threshold es 60
[Huawei-voice-ve1-2/0/0] crc-alarm-threshold dm 30
```

16.4.1.7 display voice port bra

Function

The **display voice port bra** command displays the configuration and status of a BRA interface.

Format

display voice port bra [**state** *slotid/subcardid/portid* | *slotid/subcardid/portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcard ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port bra** command displays existing BRA interfaces.

Example

Display the configuration of a BRA interface.

```
<Huawei> display voice port bra 1/0/0
 Port BRA(Slot/Subcard/Port) 1/0/0
 L2 monitor            : Enable
 Work mode             : P2MP
```

```
Remote power        : Disable
Alarm               : Disable
```

Table 16-37 Description of the display voice port bra command output

Item	Description
L2 monitor	Whether Layer 2 monitoring is enabled on a BRA interface: ● Enable ● Disable
Work mode	Working mode of a BRA interface: ● P2MP ● P2P
Remote power	Whether remote power supply is enabled on a BRA interface: ● Enable ● Disable
Alarm	Whether the UNI alarm function is enabled on a BRA interface: ● Enable ● Disable

16.4.1.8 display voice port fxo

Function

The **display voice port fxo** command displays the configuration and status of an FXO interface.

Format

display voice port fxo [**state** *slotid|subcardid|portid* | *slotid|subcardid|portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcardid ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port fxo** command displays existing FXO interfaces.

Example

Display the configuration of an FXO interface.

```
<Huawei> display voice port fxo 2/0/4
 Port FXO config: 2/0/4
 Send gain            : 0dB
 Recv gain            : -3.5dB
 DC impedance         : 50Ω
 AC impedance         : 600
 Ring min duration    : 200ms
 Ring max interval    : Not use
 Ring frequence       : 25Hz
 Ring AC amplitude    : 50V
 Ring offset          : 20V
 Feed max voltage     : -20V
 Feed min voltage     : -80V
 Feed max current     : 35mA
 Feed min current     : 16mA
```

Table 16-38 Description of the display voice port fxo command output

Item	Description
Send gain	Output gain of an FXO interface.
Recv gain	Input gain of an FXO interface.
DC impedance	DC impedance of an FXO interface.
AC impedance	AC impedance of an FXO interface.
Ring min duration	Shortest length of ring currents on an FXO interface.
Ring max interval	Maximum interval between ring currents on an FXO interface.
Ring frequence	Ring current frequency on an FXO interface.
Ring AC amplitude	AC amplitude of the ring current on an FXO interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ring offset	AC offset of the ring current on an FXO interface.
Feed max voltage	Maximum feed voltage of an FXO interface.
Feed min voltage	Minimum feed voltage of an FXO interface.
Feed max current	Maximum feed current of an FXO interface.
Feed min current	Minimum feed current of an FXO interface.

16.4.1.9 display voice port fxs

Function

The **display voice port fxs** command displays the configuration and status of an FXS interface.

Format

display voice port fxs [**state** *slotid/subcardid/portid* | *slotid/subcardid/portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcardid ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port fxs** command displays existing FXS interfaces.

Example

Display the configuration of an FXS interface.

```
<Huawei> display voice port fxs 0/0/0
 Port FXS config: 0/0/0
 Reverse pole pulse level(ms)  : 100
 Line lock                     : Enable
 NLP mode                      : NLP normal mode
 Current(mA)                   : 20mA steady current
 Impedance                     : 600 Ohm interface
 Send gain                     : 0dB
 Receive gain                  : -7dB
 Actual send gain              :
 Actual receive gain           :
```

Table 16-39 Description of the display voice port fxs command output

Item	Description
Reverse pole pulse level(ms)	Polarity reversal pulse level width of an FXS interface.
Line lock	Whether port locking is enabled on an FXS interface: ● Enable ● Disable
NLP mode	Non-linear processing (NLP) mode supported by an FXS interface. ● disable: indicates that NLP is enabled. ● normal: indicates that the DSP processes echoes normally. ● ec-gain-adjust: indicates that the DSP uses a special processing mechanism to perform digit collecting on intelligent public phones. ● enhance: indicates that the DSP enhances NLP. ● reduce: indicates that the DSP reduces NLP.
Current(mA)	Current on an FXS interface.
Impedance	Impedance on an FXS interface.
Send gain	Output gain configured on an FXS interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Receive gain	Input gain configured on an FXS interface.
Actual send gain	Actual output gain of an FXS interface.
Actual receive gain	Actual input gain of an FXS interface.

16.4.1.10 display voice port ve1

Function

The **display voice port ve1** command displays the configuration and status of a VE1 interface.

Format

display voice port ve1 [**state** *slotid|subcardid|portid* | *slotid|subcardid|portid*]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The values of the slot ID, subcard ID, and port number depend on the product model.
state	Indicates the interface status.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When **state** and *slotid/subcardid/portid* are not specified, the **display voice port ve1** command displays existing VE1 interfaces.

Example

Display the configuration of a VE1 interface.

```
<Huawei> display voice port ve1 2/0/0
 Port VE1(Slot/Subcard/Port) 2/0/0
 Access mode              : Digital
 CRC4                     : Disable
 Impedance                :
75 Ohm
 L2 monitor               : Enable
 Signal type              : CCS
 Idle type                : 7e
 Idle number              : 4
 SA                       : 0 0 0 0 0 0 0 0 0 0
 Invert Tx                : Disable
 Invert Rx                : Disable
 CRC                      : 16
 PCM alarm
 Line fault               : Enable
 Ulf                      : Enable
 Olf                      : Enable
 Ldt                      : Disable
 Frmslip                  : Disable
 Transient event          : Disable

 CRC alarm threshold Es    : 432s
 CRC alarm threshold Cses  : 4s
 CRC alarm threshold Dm    : 8s
```

Table 16-40 Description of the display voice port ve1 command output

Item	Description
Access mode	Access mode of a VE1 interface. ● Digital: indicates the digital section access mode. ● Direct: indicates the direct access mode.
CRC4	Whether CRC4 check is enabled on a VE1 interface. ● Enable ● Disable
Impedance	Impedance on a VE1 interface.
Itf number	Specifies the number of interframe filling tags on the E1-F interface.
Itf type	Specifies the interframe filling tag type on the E1-F interface.
SA	Specifies the content of the five outgoing SA bits in the CRC4 multiframe. (The first five SA bits are incoming bits, which can be queried but cannot be configured. The latter five SA bis are outgoing bits).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Invert	Specifies whether to invert timeslot data of sent or received signaling. ● Tx: Invert timeslot data of sent signaling. ● Rx: Invert timeslot data of received signaling.
CRC	Specifies the CRC mode on the VE1 interface. ● 16: 16-bit CRC is used. ● 32: 32-bit CRC is used. ● none: No CRC is used.
L2 monitor	Whether Layer 2 monitoring is enabled on a VE1 interface: ● Enable ● Disable
Signal type	Signaling mode of a VE1 interface. ● CCS: common channel signaling ● CAS: channel associated signaling
Line fault	Whether calling line identification presentation (CLIP) polarity reversal is enabled: ● Enable ● Disable
Ulf	Whether the alarm on the unconditional line fault bit error rate is enabled: ● Enable ● Disable
Olf	Whether the alarm on the conditional line fault bit error rate is enabled: ● Enable ● Disable
Ldt	Whether the alarm on temporary line interference bit error rate is enabled: ● Enable ● Disable

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Frmslip	Whether the alarm on loss of PCM frames: ● Enable ● Disable
Transient event	Whether the alarm on transient line events is enabled: ● Enable ● Disable
CRC alarm threshold Es	Errored seconds threshold.
CRC alarm threshold Cses	Consecutively severely errored seconds threshold.
CRC alarm threshold Dm	Degraded minute threshold.

16.4.1.11 electric current

Function

Using the **electric current** command, you can set the current for an FXS interface.

Using the **undo electric current** command, you can restore the default current of an FXS interface.

By default, the current of an FXS interface is 20 mA.

Format

electric current *current-value*

undo electric current

Parameters

Parameter	Description	Value
current-value	Specifies the current of an FXS interface.	Enumerated type. The values are 16 mA, 20 mA, 25 mA, 30 mA, 35 mA.

Views

FXS interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the current of an FXS interface to 16 mA.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric current 16mA
```

16.4.1.12 electric impedance

Function

Using the **electric impedance** command, you can set the impedance for an FXS interface.

Using the **undo electric impedance** command, you can restore the default impedance of an FXS interface.

By default, the impedance of an FXS interface is 600 ohm.

Format

electric impedance *impedance-value*

undo electric impedance

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
impedance-value	Specifies the impedance of an FXS interface.	The value is an integer that ranges from 0 to 15: ● 0: CNOF (200+680|| 100 nF) ● 1: CNUSER (200+560|| 100 nF) ● 2: 600 ohm ● 3: RUSSIA (150+510|| 47 nF) ● 4: (220+820|| 115 nF) ● 5: (220+820|| 120 nF) ● 6: 900 ohm ● 7: BRAZIL (800|| 50 nF) ● 8: BT0 (Zin=87+1052|| 228nF+229||28.4nF, Zload=93+615||\ 471nF+179||495nF +244||32 nF) ● 9: HK_BT3 (Zin=370+620|| 310nf,Zload=600) ● 10: HK_BT5 (Zin=270+264|| 357nf +1434|| 265nf,Zload=600) ● 11: BT1 (BT0 without AGC) ● 12: BT2 (Zin=87+1052||228 nF + 229||28.4nF, Zload=270+264||\ 357 nF + 1434||265 nF) ● 13: BT3(Zin=87+1052|| 228 nF + 229||28.4nF, Zload=164+162||\ 363 nF + 1227||350 nF) ● 14: EUROPE GLOBAL (Zin= 270+750|| 150 nF) ● 15: NEW ZEALAND (Zin=370+620|| 310 nF)

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		NOTE The AR129CV, AR129CVW, and AR129CGVW-L do not support the 1, 8 to 13 parameter value.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the impedance of an FXS interface to 3.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric impedance 3
```

16.4.1.13 electric receive-gain

Function

The **electric receive-gain** command configures the receive gain of an FXS interface.

The **undo electric receive-gain** command restores the default receive gain of an FXS interface.

By default, the receive gain of an FXS interface is –7 dB.

Format

electric receive-gain *recvgain-value*

undo electric receive-gain

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
recvgain-value	Specifies the receive gain of an FXS interface.	The value is an integer that ranges from 0 to 40: ● 0: 0 dB ● 1: –0.5 dB ● 2: –1 dB ● 3: –1.5 dB ● 4: –2 dB ● 5: –2.5 dB ● 6: –3 dB ● 7: –3.5 dB ● 8: –4 dB ● 9: –4.5 dB ● 10: –5 dB ● 11: –5.5 dB ● 12: –6 dB ● 13: –6.5 dB ● 14: –7 dB ● 15: –7.5 dB ● 16: –8 dB ● 17: –8.5 dB ● 18: –9 dB ● 19: –9.5 dB ● 20: –10 dB ● 21: –10.5 dB ● 22: –11 dB ● 23: –11.5 dB ● 24: –12 dB ● 25: –12.5 dB ● 26: –13 dB ● 27: –13.5 dB ● 28: –14 dB ● 29: –14.5 dB ● 30: –15 dB ● 31: –15.5 dB ● 32: –16 dB ● 33: –16.5 dB ● 34: –17 dB ● 35: –17.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 36: –18 dB • 37: –18.5 dB • 38: –19 dB • 39: –19.5 dB • 40: –20 dB **NOTE** The receive gain of an FXS interface on an AR129CV, AR129CVW, AR129CGVW-L, 16-port FXS interface card, or 32-port FXS interface card ranges from –12 dB to 0 dB.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

The receive gain of an FXS interface affects the volume of the voice a local user receives. A smaller value of *recvgain-value* indicates a lower voice.

Example

Set the receive gain of an FXS interface to 0 dB (value 0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric receive-gain 0
```

16.4.1.14 electric send-gain

Function

The **electric send-gain** command configures the send gain of an FXS interface.

The **undo electric send-gain** command restores the default send gain of an FXS interface.

By default, the send gain of an FXS interface is 0 dB.

Format

electric send-gain *sendgain-value*

undo electric send-gain

Parameters

Parameter	Description	Value
sendgain-value	Specifies the send gain of an FXS interface.	The value is an integer that ranges from 0 to 50. ● 0: 5 dB ● 1: 4.5 dB ● 2: 4 dB ● 3: 3.5 dB ● 4: 3 dB ● 5: 2.5 dB ● 6: 2 dB ● 7: 1.5 dB ● 8: 1 dB ● 9: 0.5 dB ● 10: 0 dB ● 11: –0.5 dB ● 12: –1 dB ● 13: –1.5 dB ● 14: –2 dB ● 15: –2.5 dB ● 16: –3 dB ● 17: –3.5 dB ● 18: –4 dB ● 19: –4.5 dB ● 20: –5 dB ● 21: –5.5 dB ● 22: –6 dB ● 23: –6.5 dB ● 24: –7 dB ● 25: –7.5 dB ● 26: –8 dB ● 27: –8.5 dB ● 28: –9 dB ● 29: –9.5 dB ● 30: –10 dB ● 31: –10.5 dB ● 32: –11 dB ● 33: –11.5 dB ● 34: –12 dB ● 35: –12.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 36: –13 dB • 37: –13.5 dB • 38: –14 dB • 39: –14.5 dB • 40: –15 dB • 41: –15.5 dB • 42: –16 dB • 43: –16.5 dB • 44: –17 dB • 45: –17.5 dB • 46: –18 dB • 47: –18.5 dB • 48: –19 dB • 49: –19.5 dB • 50: –20 dB **NOTE** The send gain of an FXS interface on an AR129CVW, AR129CGVW-L, 16-port FXS interface card, or 32-port FXS interface card ranges from –6 dB to 5 dB.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

The send gain of an FXS interface affects the volume of the voice a remote user receives. A smaller value of *sendgain-value* indicates a lower voice.

Example

Set the send gain of an FXS interface to 0 dB (value 10).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] electric send-gain 10
```

16.4.1.15 feed

Function

Using the **feed** command, you can set feed parameters for an FXO interface.

Using the **undo feed** command, you can restore the default feed parameter settings of an FXO interface.

Format

feed { **maximum-voltage** *max-vol-value* | **minimum-voltage** *min-vol-value* | **minimum-current** *min-current-value* }

undo feed { **maximum-voltage** | **minimum-voltage** | **minimum-current** }

Parameters

Parameter	Description	Value
maximum-voltage *max-vol-value*	Specifies the maximum feed voltage.	The value is an integer that ranges from -100 to 0, in volt. The default value is -20.
minimum-voltage *min-vol-value*	Specifies the minimum feed voltage.	The value is an integer that ranges from -100 to 0, in volt. The default value is -80.
minimum-current *min-current-value*	Specifies the minimum feed current.	The value is an integer that ranges from 6 to 20, in mA. The default value is 10.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the minimum feed voltage of an FXO interface to -50 V.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] feed minimum-voltage -50
```

16.4.1.16 gain

Function

Using the **gain** command, you can set the send gain and receive gain for an FXO interface.

Using the **undo gain** command, you can restore the default send gain and receive gain of an FXO interface.

By default, the send gain and receive gain of an FXO interface are both 0 dB.

Format

gain { **send** *send-value* | **receive** *recvgain-value* }

undo gain { **send** | **receive** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
send *send-value*	Specifies the send gain of an FXO interface.	The value is an integer that ranges from 0 to 60: ● 0: +13.5 dB ● 1: +13.0 dB ● 2: +12.5 dB ● 3: +12.0 dB ● 4: +11.5 dB ● 5: +11.0 dB ● 6:+10.5 dB ● 7:+10.0 dB ● 8: +9.5 dB ● 9: +9.0 dB ● 10: +8.5 dB ● 11: +8.0 dB ● 12: +7.5 dB ● 13: +7.0 dB ● 14: +6.5 dB ● 15: +6.0 dB ● 16: +5.5 dB ● 17: +5.0 dB ● 18: +4.5 dB ● 19: +4.0 dB ● 20: +3.5 dB ● 21: +3.0 dB ● 22: +2.5 dB ● 23: +2.0 dB ● 24: +1.5 dB ● 25: +1.0 dB ● 26: +0.5 dB ● 27: 0 dB ● 28: -0.5 dB ● 29: -1.0 dB ● 30: -1.5 dB ● 31: -2.0 dB ● 32: -2.5 dB ● 33: -3.0 dB ● 34: -3.5 dB ● 35: -4.0 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		● 36: -4.5 dB ● 37: -5.0 dB ● 38: -5.5 dB ● 39: -6.0 dB ● 40: -6.5 dB ● 41: -7.0 dB ● 42: -7.5 dB ● 43: -8.0 dB ● 44: -8.5 dB ● 45: -9.0 dB ● 46: -9.5 dB ● 47: -10.0 dB ● 48: -10.5 dB ● 49: -11.0 dB ● 50: -11.5 dB ● 51: -12.0 dB ● 52: -12.5 dB ● 53: -13.0 dB ● 54: -13.5 dB ● 55: -14.0 dB ● 56: -14.5 dB ● 57: -15.0 dB ● 58: -15.5 dB ● 59: -16.0 dB ● 60: -16.5 dB The default value is 27.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
receive *recvgain-value*	Specifies the receive gain of an FXO interface.	The value is an integer that ranges from 0 to 60: ● 0: +13.5 dB ● 1: +13.0 dB ● 2: +12.5 dB ● 3: +12.0 dB ● 4: +11.5 dB ● 5: +11.0 dB ● 6:+10.5 dB ● 7:+10.0 dB ● 8: +9.5 dB ● 9: +9.0 dB ● 10: +8.5 dB ● 11: +8.0 dB ● 12: +7.5 dB ● 13: +7.0 dB ● 14: +6.5 dB ● 15: +6.0 dB ● 16: +5.5 dB ● 17: +5.0 dB ● 18: +4.5 dB ● 19: +4.0 dB ● 20: +3.5 dB ● 21: +3.0 dB ● 22: +2.5 dB ● 23: +2.0 dB ● 24: +1.5 dB ● 25: +1.0 dB ● 26: +0.5 dB ● 27: 0 dB ● 28: -0.5 dB ● 29: -1.0 dB ● 30: -1.5 dB ● 31: -2.0 dB ● 32: -2.5 dB ● 33: -3.0 dB ● 34: -3.5 dB ● 35: -4.0 dB ● 36: -4.5 dB

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 37: -5.0 dB • 38: -5.5 dB • 39: -6.0 dB • 40: -6.5 dB • 41: -7.0 dB • 42: -7.5 dB • 43: -8.0 dB • 44: -8.5 dB • 45: -9.0 dB • 46: -9.5 dB • 47: -10.0 dB • 48: -10.5 dB • 49: -11.0 dB • 50: -11.5 dB • 51: -12.0 dB • 52: -12.5 dB • 53: -13.0 dB • 54: -13.5 dB • 55: -14.0 dB • 56: -14.5 dB • 57: -15.0 dB • 58: -15.5 dB • 59: -16.0 dB • 60: -16.5 dB The default value is 27.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the send gain and receive gain of an FXO interface to 12 dB (value 3).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] gain receive 3
[Huawei-voice-fxo1/0/4] gain send 3
```

16.4.1.17 impedance (FXO interface view)

Function

Using the **impedance** command, you can set the DC impedance and AC impedance for an FXO interface.

Using the **undo impedance** command, you can restore the default DC impedance and AC impedance of an FXO interface.

By default, the DC impedance of an FXO interface is 50 nF, and the AC impedance is 600 nF.

Format

impedance { **dc** *value* | **ac** *value* }

undo impedance { **dc** | **ac** }

Parameters

Parameter	Description	Value
dc *value*	Specifies the DC impedance.	The value is 0 or 1: ● 0: 50 nF ● 1: 800 nF The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ac *value*	Specifies the AC impedance.	The value is an integer that ranges from 0 to 15: ● 0: 600 ● 1: 900 ● 2: 270 + (750 || 150 nF) and 275 + (780 || 150 nF) ● 3: 220 + (820 || 120 nF) and 220 + (820 || 115 nF) ● 4: 370 + (620 || 310 nF) ● 5: 320 + (1050 || 230 nF) ● 6: 370 + (820 || 110 nF) ● 7: 275 + (780 || 115 nF) ● 8: 20 + (820 || 110 nF) ● 9: 350 + (1000 || 210 nF) ● 10: 200 + (680 || 100 nF) ● 11: 600 + 2.16 uF ● 12: 900 + 1 uF ● 13: 900 + 2.16 uF ● 14: 600 + 1 uF ● 15: Global impedance The default value is 0.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the DC impedance of an FXO interface to 50 nF (value 0).

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] impedance DC 0
```

16.4.1.18 impedance (VE1 interface view)

Function

Using the **impedance** command, you can set the impedance for a VE1 interface.

Using the **undo impedance** command, you can restore the default impedance of a VE1 interface.

By default, the impedance of a VE1 interface is 75 ohm.

Format

impedance *impedance-value*

undo impedance

Parameters

Parameter	Description	Value
impedance-value	Specifies the impedance on a VE1 interface.	The value is 75 or 120, in ohm. The default value is 75.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the impedance of a VE1 interface to 75 ohm.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] impedance 75
 Set impendance successfully
```

16.4.1.19 invert

Function

The **invert** command sets whether to revert signaling timeslots that are sent and received.

The **undo invert** command restores the default setting.

By default, signaling timeslots that are sent and received are not inverted.

Format

invert { **tx** | **rx** }

undo invert { **tx** | **rx** }

Parameters

Parameter	Description	Value
tx	Configures the AR to invert signaling timeslots that are sent.	-
rx	Configures the AR to invert signaling timeslots that are received.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VE1 interface is connected in PRI mode, you need to configure whether to invert signaling timeslot data as needed, ensuring signaling timeslot interconnecting without bit error or packet loss.

Precautions

Configure whether to invert timeslot data of sent or received signaling on a VE1 interface as needed. By default, signaling timeslot data is not inverted.

Example

#Configure to invert signaling timeslots that are sent and received on the VE1 interface.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] invert tx
  Set invert successfully
[Huawei-voice-ve1-2/0/0] invert rx
  Set invert successfully
```

16.4.1.20 itf(VE1 interface view)

Function

The **itf** command sets the interframe filling tag type and the number of interframe filling tags on the VE1 interface.

Format

itf { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **number** | **type** }

Parameters

Parameter	Description	Value
number *number*	Specifies the number of interframe filling tags.	The value is an integer that ranges from 0 to 7.
type	Specifies the interframe filling tag type.	-
7e	Sets the interframe filling tag to 0x7e.	-
ff	Sets the interframe filling tag to 0xff.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The interframe filling tag on a VE1 interface is the code that is sent when no service data is sent through the timeslot bundled to a logical channel.

A VE1 interface supports two types of interframe filling tags: 0x7e and 0xff. The default interframe filling tag 0x7e is recommended.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- The same interframe filling tag type and number of interframe filling tags must set for interfaces on both ends; otherwise, communication exceptions may occur.
- Because interframe filling tags occupy bandwidth, the actual data transmission rate on a VE1 interface cannot reach the maximum bandwidth. To improve the actual data transmission rate on a VE1 interface, run the **itf number** command to set the number of interframe filling tags to 0.

Example

Set the interframe filling tag to 0x7e on the VE1 interface and set six interframe filling tags.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] itf type ff
  Set itf successfully
[Huawei-voice-ve1-2/0/0] itf number 6
  Set itf successfully
```

16.4.1.21 l2-monitor

Function

Using the **l2-monitor** command, you can enable or disable Layer 2 monitoring on a BRA interface.

Using the **undo l2-monitor** command, you can restore the default status of Layer 2 monitoring on a BRA interface.

By default, Layer 2 monitoring is enabled on a BRA interface.

Format

l2-monitor { **enable** | **disable** }

undo l2-monitor

Parameters

Parameter	Description	Value
enable	Enables Layer 2 monitoring on a BRA interface.	_
disable	Disables Layer 2 monitoring on a BRA interface.	_

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable Layer 2 monitoring on a BRA interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] l2-monitor enable
```

16.4.1.22 l2-monitor (VE1 interface view)

Function

Using the **l2-monitor** command, you can enable or disable Layer 2 monitoring on a VE1 interface.

Using the **undo l2-monitor** command, you can restore the default status of Layer 2 monitoring on a VE1 interface.

By default, Layer 2 monitoring is enabled on a VE1 interface.

Format

l2-monitor { **enable** | **disable** }

undo l2-monitor

Parameters

Parameter	Description	Value
enable	Enables Layer 2 monitoring on a VE1 interface.	_
disable	Disables Layer 2 monitoring on a VE1 interface.	_

Views

VE1 interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Enable Layer 2 monitoring on a VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] l2-monitor enable
```

16.4.1.23 line-lock

Function

Using the **line-lock** command, you can enable or disable port locking on an FXS interface.

Using the **undo line-lock** command, you can restore the default port locking status on an FXS interface.

By default, port locking is enabled on an FXS interface.

Format

line-lock { **enable** | **disable** }

undo line-lock

Parameters

Parameter	Description	Value
enable	Enables port locking.	_
disable	Disables port locking.	_

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable port locking on an FXS interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] line-lock enable
```

16.4.1.24 loop

Function

The **loop** command sets a port loopback flag.

The **undo loop** command deletes a port loopback flag.

By default, the system does not have any loopback flags.

Format

loop { **remote** | **local** }

undo loop

Parameters

Parameter	Description	Value
remote	Specifies a remote loopback flag.	-
local	Specifies a local loopback flag.	-

Views

BRA, FXS or FXO port view

Default Level

2: Configuration level

Usage Guidelines

You do not need to use this command in normal configurations. This command is mainly used in progressive debugging of call fault points.

Example

Configure remote loopback for an ISDN BRA port.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] loop remote
```

16.4.1.25 nlp-mode

Function

Using the **nlp-mode** command, you can specify the non-linear echo processing (NLP) mode supported by an FXS interface.

Using the **undo nlp-mode** command, you can restore the default NLP mode supported by an FXS interface.

By default, an FXS supports the normal NLP mode.

Format

nlp-mode { **disable** | **normal** | **ec-gain-adjust** | **enhance** | **reduce** }

undo nlp-mode

Parameters

Parameter	Description	Value
disable	Disables the NLP function on an FXS interface so that the digital signal processor (DSP) on the interface does not process non-liner echoes.	_
normal	Indicates the normal NLP mode. In this mode, the DSP processes echoes normally.	_
ec-gain-adjust	Indicates the EC gain adjustment mode. In this mode, the DSP uses a special processing mechanism to perform digit collecting on intelligent public phones.	_
enhance	Indicates the enhanced mode. In this mode, the DSP enhances non-liner echoes.	_
reduce	Indicates the reduction mode. In this mode, the DSP reduces non-liner echoes.	_

 Copyright © Huawei Technologies Co., Ltd.

Views

FXS interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the NLP mode to normal on an FXS interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] nlp-mode normal
```

16.4.1.26 pcm-alarm

Function

Using the **pcm-alarm** command, you can enable or disable the pulse code modulation (PCM) alarm function on a VE1 interface.

Using the **undo pcm-alarm** command, you can restore the default status of the PCM alarm function on a VE1 interface.

Format

pcm-alarm [**line-fault** *line-fault-value* | **ulf** *ulf-value* | **olf** *olf-value* | **ldt** *ldt-value* | **frmslip** *frmslip-value* | **transient-event** *transient-event-value*]

undo pcm-alarm [**line-fault** | **ulf** | **olf** | **ldt** | **frmslip** | **transient-event**]

Parameters

Parameter	Description	Value
line-fault *line-fault-value*	Enables or disables alarms on line faults.	Enumerated type. The values are as follows: ● disable: disables alarms on line faults. ● enable: enables alarms on line faults. The default value is **enable**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ulf *ulf-value*	Enables or disables alarms on the unconditional line fault bit error rate.	Enumerated type. The values are as follows: ● disable: disables alarms on the unconditional line fault bit error rate. ● enable: enables alarms on the unconditional line fault bit error rate. The default value is **enable**.
olf *olf-value*	Enables or disables alarms on the conditional line fault bit error rate.	Enumerated type. The values are as follows: ● disable: disables alarms on the conditional line fault bit error rate. ● enable: enables alarms on the conditional line fault bit error rate. The default value is **enable**.
ldt *ldt-value*	Enables or disables alarms on the temporary line interference bit error rate.	Enumerated type. The values are as follows: ● disable: disables alarms on the temporary line interference bit error rate. ● enable: enables alarms on the temporary line interference bit error rate. The default value is **disable**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
frmslip *frmslip-value*	Enables or disables alarms on loss of PCM frames.	Enumerated type. The values are as follows: ● disable: disables alarms on loss of PCM frames. ● enable: enables alarms on loss of PCM frames. The default value is **disable**.
transient-event *transient-event-value*	Enables or disables alarms on transient line events.	Enumerated type. The values are as follows: ● disable: disables alarms on transient line events. ● enable: enables alarms on transient line events. The default value is **disable**.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable line fault alarms on a VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] pcm-alarm line-fault enable
```

16.4.1.27 port bra

Function

Using the **port bra** command, you can enter the BRA interface view.

Format

port bra *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port bra** command to view existing BRA interfaces.

Example

Enter the view of BRA interface 2/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 2/0/0
[Huawei-voice-bra-2/0/0]
```

16.4.1.28 port fxo

Function

Using the **port fxo** command, you can enter the FXO interface view.

Format

port fxo*slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcardid ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port fxo** command to view existing FXO interfaces.

Example

Enter the view of FXO interface 2/0/4.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 2/0/4
[Huawei-voice-fxo-2/0/4]
```

16.4.1.29 port fxs

Function

Using the **port fxs** command, you can enter the FXS interface view.

By default, the region identifier is China mainland.

Format

port fxs *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcardid ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcardid ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port fxs** command to view existing FXS interfaces.

Example

Enter the view of FXS interface 2/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0]
```

16.4.1.30 port ve1

Function

Using the **port ve1** command, you can enter the VE1 interface view.

Format

port ve1 *slotid/subcardid/portid*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number.	The value is a string of 1 to 15 characters. The value ranges of the slot ID, subcard ID, and port number vary according to the device configuration.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice port ve1** command to view existing VE1 interfaces.

Example

Enter the view of VE1 interface 2/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0]
```

16.4.1.31 remote-power

Function

Using the **remote-power** command, you can enable the remote power supply function.

Using the **undo remote-power** command, you can restore the default configuration.

By default, the remote power supply function is disabled.

Format

remote-power { **enable** | **disable** }

undo remote-power

Parameters

Parameter	Description	Value
enable	Enables the remote power supply function.	-
disable	Disables the remote power supply function.	-

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

A BRA phone must be powered by a dedicated transformer. If no dedicated transformer is available, run the **remote-power** command to enable the remote power supply function on the BRA interface so that the BRA interface can supply power for BRA phones.

Example

Enable the remote power supply function on a BRA interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] remote-power enable
```

16.4.1.32 reset line-fault

Function

Using the **reset line-fault** command, you can reset line fault alarms.

Format

reset line-fault

Parameters

None

Views

FXS interface view

Default Level

3: Management level

Usage Guidelines

The **reset line-fault** command resets line fault alarms on an FXS interface.

Example

Reset line fault alarms on an FXS interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] reset line-fault
```

16.4.1.33 reverse-pole-pulse level

Function

Using the **reverse-pole-pulse level** command, you can set the polarity reversal pulse level width for an FXS interface.

Using the **undo reverse-pole-pulse level** command, you can restore the default polarity reversal pulse level width of an FXS interface.

By default, the polarity reversal pulse level width of an FXS interface is 100 ms.

Format

reverse-pole-pulse level *level-value*

undo reverse-pole-pulse level

Parameters

Parameter	Description	Value
level *level-value*	Specifies the polarity reversal pulse level width.	The value is an integer that ranges from 20 to 1270, with increments of 10. The unit is ms.

Views

FXS interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command sets the polarity reversal pulse level width for an FXS interface.

Example

Set the polarity reversal pulse level width of an FXS interface to 30 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs2/0/0] reverse-pole-pulse level 30
```

16.4.1.34 ring

Function

Using the **ring** command, you can set ring current parameters on an FXS interface.

Using the **undo ring** command, you can restore the default values of ring current parameters on an FXS interface.

By default, the shortest length of a ring current is 200 ms; the maximum ring current interval is not set; the ring current frequency is 25 Hz; the AC amplitude is 50 V; the AC offset is 70.

Format

ring { **minimum-duration** *min-duration-value* | **maximum-interval** *max-interval-value* | **frequence** *frequence-value* | **ac-amplitude** *ac-amplitude-value* | **offset** *offset-value* }

undo ring { **minimum-duration** | **maximum-interval** | **frequence** | **ac-amplitude** | **offset** }

Parameters

Parameter	Description	Value
minimum-duration *min-duration-value*	Specifies the shortest length of a ring current.	The value is an integer that ranges from 0 to 7: • 0: 100 ms • 1: 150 ms • 2: 200 ms • 3: 256 ms • 4: 384 ms • 5: 512 ms • 6: 640 ms • 7: 1024 ms The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
maximum-interval *max-interval-value*	Specifies the maximum interval between ring currents.	The value is an integer that ranges from 0 to 28: ● 0: not use ● 1: 128 ms ● 2: 256 ms ● 3: 284 ms ● 4: 512 ms ● 5: 640 ms ● 6: 768 ms ● 7: 896 ms ● 8: 1024 ms ● 9: 1152 ms ● 10: 1280 ms ● 11: 1408 ms ● 12: 1536 ms ● 13: 1664 ms ● 14: 1792 ms ● 15: 1920 ms ● 16: 2000 ms ● 17: 2500 ms ● 18: 3000 ms ● 19: 3500 ms ● 20: 4000 ms ● 21: 4500 ms ● 22: 5000 ms ● 23: 6000 ms ● 24: 7000 ms ● 25: 8000 ms ● 26: 9000 ms ● 27: 10000 ms ● 28: 15000 ms The default value is 0.
frequence *frequence-value*	Specifies the ring current frequency.	The value is an integer that ranges from 0 to 2: ● 0: 16 Hz ● 1: 25 Hz ● 2: 50 Hz The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ac-amplitude *ac-amplitude-value*	Specifies the AC Amplitude of a ring current.	The value is an integer that ranges from 0 to 2: ● 0: 74 V ● 1: 65 V ● 2: 50 V The default value is 2.
offset *offset-value*	Specifies the AC offset of a ring current.	The value is an integer that ranges from 0 to 100. The default value is 70.

Views

FXO interface view

Default Level

2: Configuration level

Usage Guidelines

You can use this command to set the shortest length of a ring current, maximum interval between ring currents, ring current frequency, AC Amplitude of a ring current, and AC offset of a ring current.

Example

Set the shortest length of a ring current on an FXO interface to 100 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxo 1/0/4
[Huawei-voice-fxo1/0/4] ring minimum-duration 0
```

16.4.1.35 sa

Function

The **sa** command sets the content of the five outgoing sa bits.

The **undo sa** command restores the default setting.

By default, the content of the five outgoing sa bits is 0.

Format

sa *sa4 sa5 sa6 sa7 sa8*

undo sa

Parameters

Parameter	Description	Value
sa4	Sets the content of the outgoing sa4 bit.	The value is a decimal integer that ranges from 0 to 255.
sa5	Sets the content of the outgoing sa5 bit.	The value is a decimal integer that ranges from 0 to 255.
sa6	Sets the content of the outgoing sa6 bit.	The value is a decimal integer that ranges from 0 to 255.
sa7	Sets the content of the outgoing sa7 bit.	The value is a decimal integer that ranges from 0 to 255.
sa8	Sets the content of the outgoing sa8 bit.	The value is a decimal integer that ranges from 0 to 255.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

When a VE1 interface is connected in PRI mode, if the E1 frame is a CRC4 multiframe, SA4 to SA8 in the E1 multiframe can be used for transmitting low-speed data. By default, the values of SA4 to SA8 are 0. In some scenarios, the remote device will check received SA fields. Therefore, SA fields must be configurable on an AR to ensure normal connection of the VE1 interface.

Precautions

By default, the SA field value is 0. Before configuring the SA field, collect configuration information on the remote device.

Example

Set the content of five outgoing sa bits to 1, 2, 3, 4, and 5 respectively.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] sa 1 2 3 4 5
  Set sa successfully
```

16.4.1.36 shutdown

Function

The **shutdown** command shuts down a BRA port.

The **undo shutdown** command restores a BRA port.

Format

shutdown

undo shutdown

Parameters

None

Views

BRA port view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to disable an ISDN BRA port.

Example

Shuts down an ISDN BRA port.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] shutdown
```

16.4.1.37 signal(VE1 interface view)

Function

Using the **signal** command, you can set the signaling mode of a VE1 interface.

Using the **undo signal** command, you can restore the default signaling mode of a VE1 interface.

By default, a VE1 interface uses the common channel signaling (CCS) mode.

Format

signal { **ccs** | **cas** }

undo signal

Parameters

Parameter	Description	Value
ccs	Indicates the common channel signaling mode.	-
cas	Indicates the channel associated signaling mode.	-

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

A VE1 interface can work in CCS or CAS mode. To change the signaling mode, run the **signal** command.

Example

Configure a VE1 interface to work in CCS mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] signal ccs
  Set signal type successfully
```

16.4.1.38 work-mode

Function

Using the **work-mode** command, you can set the working mode for a BRA interface.

Using the **undo work-mode** command, you can restore the default working mode of a BRA interface.

By default, a BRA interface works in point-to-multipoint (P2MP) mode.

Format

work-mode { **p2p** | **p2mp** }

undo work-mode

Parameters

Parameter	Description	Value
p2mp	Indicates the point-to-multipoint (P2MP) mode.	-
p2p	Indicates the point-to-point (P2P) mode.	-

Views

BRA interface view

Default Level

2: Configuration level

Usage Guidelines

This command sets the working mode for a BRA interface.

A BRA interface works in either of the following modes:

- P2MP: Multiple terminals can connect to the BRA interface.
- P2P: Only one terminal can connect to the BRA interface.

Example

Configure a BRA interface to work in P2P mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 1/0/0
[Huawei-voice-bra1/0/0] work-mode p2p
```

 Copyright © Huawei Technologies Co., Ltd.

16.5 PBX Configuration Commands

NOTE

- The following product models support voice functions (such as the PBX, SIP AG, and H.248 AG):
  - AR120 series: AR129CV, AR129CVW, and AR129CGVW-L
  - AR150 series: AR157VW and AR158EVW
  - AR160 series: AR161, AR169FVW, AR169FVW-8S, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR161FV-1P, and AR169FGVW-L
  - AR200 series: AR201VW-P, AR207V, AR207VW, and AR207V-P
  - AR1200 series: AR1220V, AR1220VW, AR1220EV, and AR1220EVW
  - AR2200 series: AR2204, AR2220, AR2220L, AR2220E.
  - AR2240: For the equipped with SRU40, SRU60, SRU80, and SRU100.
  - AR3200 series: For the AR3260 equipped with SRU40, SRU60, SRU80, or SRU100, the same voice mode is set for the active and standby SRUs.

  The AR129CV, AR129CVW, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, and AR169CVW-4B4S only support the PBX and SIP AG, but not the H.248 AG.
- When an AR2204, AR2220L, or AR2220E router needs to provide voice services, install a DSP module and a voice subcard in the router. When an AR2220, AR2240, or AR3200 router needs to provide voice services, install a DSP module.
- To provide voice services to POTS users on the AR1200, AR2200, or AR3200, install the 4FXS1FXO, 16FXS, or 32FXS card. The AR1200 does not support the 32FXS card.
- To provide voice services to ISDN phone users on the AR1200, AR2200, or AR3200, install the 2BST card.
- To connect an AR1200, AR2200, or AR3200 router to a TDM PBX through the E1 interface, install the E1T1-M card.
- On the AR169FGVW-L, AR1220EV, and AR1220EVW, the AT0 trunk cannot be connected to the SIP server or SIP trunk.

16.5.1 PBX Basic Configuration Commands

16.5.1.1 access-telno (disa view)

Function

The **access-telno** command configures an accessible telno for disa.

Format

access-telno *telno*

Parameters

Parameter	Description	Value
telno	Specifies the telno.	The value is a string of 1 to 16 characters without spaces.

Views

Disa view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configures an accessible telno 83786000 for disa d1.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] disa d1
 [Huawei-voice-disa-d1] access-telno 83786000
```

16.5.1.2 account-set

Function

Using the **account-set** command, you can configure an **account-set** and enter the **account-set** profile view.

Using the **undo account-set** command, you can delete the **account-set** profile.

By default, no **account-set** profile is configured.

Format

account-set *account-set-name* [**password** | **account**]

undo account-set *account-set-name*

Parameters

Parameter	Description	Value
account-set-name	Specifies the name of account-set profile.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
[**password** | **account**]	Specifies the mode of account-set: account mode and password mode. The default value is the password mode.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create an account-set profile q.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] account-set 1
[Huawei-voice-account-1]
```

16.5.1.3 b2brouteadd

Function

The **b2brouteadd** command configures a backtoback route.

The **undo b2brouteadd** command deletes a configured backtoback route.

Format

b2brouteadd src-trunkgroup *src-trunkgroupname* **dst-trunkgroup** *dst-trunkgroupname*

undo b2brouteadd src-trunkgroup *src-trunkgroupname* **dst-trunkgroup** *dst-trunkgroupname*

Parameters

Parameter	Description	Value
src-trunkgroup *src-trunkgroupname*	Specifies the source trunk group name.	The value is a string of 1 to 32 characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dst-trunkgroup *dst-trunkgroupname*	Specifies the destination trunk group name.	The value is a string of 1 to 32 characters without spaces.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the backtoback route in the view of the call prefix **prefix-user1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix-user1
[Huawei-voice-callprefix-prefix-user1]b2brouteadd src-trunkgroup bra dst-trunkgroup sipip
```

16.5.1.4 cac

Function

The **cac** command enables call limiting over one or more SIP trunks for the same peer IP address and configures the maximum number of online calls.

The **undo cac** command cancels call limiting for a specific IP address.

By default, call limiting rules are not configured.

Format

cac destination-ip *ip-address* **max-call-number** *max-call-number-value*

undo cac destination-ip *ip-address*

Parameters

Parameter	Description	Value
destination-ip *ip-address*	Specifies the peer IP address from which calls are limited.	The value is in dotted decimal notation.

Parameter	Description	Value
max-call-number *max-call-number-value*	Specifies the maximum number of online calls.	The value is an integer that ranges from 1 to 2000.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used to limit calls if multiple SIP trunks (including SIP IP, SIP PRA, and SIP AT0 trunks) have the same remote IP address. When call limiting is enabled for a remote IP address, if the number of online incoming and outgoing calls on the trunk with the IP address from which calls are limited reaches the configured maximum number of online calls, calls can no longer be made.

Example

Set the maximum number of online calls over the SIP trunk for the IP address of 192.168.0.1 to 2000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]cac destination-ip 192.168.0.1 max-call-number 2000
```

16.5.1.5 call-type

Function

The **call-type** command configures the call category and call attribute of a call prefix.

By default, the call category and call attribute of a call prefix are not configured.

Format

call-type category { *callcategory* **attribute** *attribute* [**cdr-alais** *cdr-alais*] **|** **vu-service vu-service-name** *vuservicename* }

Parameters

Parameter	Description	Value
category *callcategory*	Specifies the call category.	Enumerated type. The value can be **basic-service**, **new-supplementary-management**, or **supplementary-service**. ● basic-service: basic service for call attributes 0 to 20 ● new-supplementary-management: supplementary service for call attributes 21 to 170 ● supplementary-service: supplementary service for call attributes 171 to 240

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
attribute *attribute*	Specifies the call attribute.	The value is an integer. ● 0: Internal dialing ● 1: Local dialing ● 2: Domestic direct dialing ● 3: International direct dialing ● 4: local call first, if fail then inter-office call ● 5: inter-office call first, if fail then local call ● 6-20: basic service prefix reservation ● 21: call forwarding unconditional (CFU) service registration ● 22: CFU service deregistration ● 23: call forwarding busy (CFB) service registration ● 24: CFB service deregistration ● 25: call forwarding no reply (CFNR) service registration ● 26: CFNR service deregistration ● 27: call forwarding offline (CFO) service registration ● 28: CFO service deregistration ● 29: reserved ● 30: reserved ● 31: call waiting (CW) service registration ● 32: CW service deregistration ● 33: reserved ● 34: reserved

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		● 35: do-not-disturb (DND) service registration ● 36: DND service deregistration ● 37: abbreviated dialing service registration ● 38: abbreviated dialing service deregistration ● 39: RAC service registration ● 40: RAC service deregistration ● 41: wake-up service registration ● 42: wakeup service deregistration ● 43: reserved ● 44: reserved ● 45: reserved ● 46: reserved ● 47: reserved ● 48: reserved ● 49: Selective Call Rejection (SCR) number registration ● 50: SCR number deregistration ● 51: SCR time registration ● 52: SCR time deregistration ● 53: SCR weekday registration ● 54: SCR weekday deregistration ● 55: SCR service activation ● 56: SCR service deactivation ● 57: SCR service verification

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 58: SCR service deletion • 59: Selective Call Acceptance (SCA) number registration • 60: SCA number deregistration • 61: SCA time registration • 62: SCA time deregistration • 63: SCA weekday registration • 64: SCA weekday deregistration • 65: SCA service activation • 66: SCA service deactivation • 67: SCA service verification • 68: SCA service deletion • 69: reserved • 70: reserved • 71: reserved • 72: SCR service registration • 73: SCR servicedergistration • 74: reserved • 75: SCC service deregistration • 76: reserved • 77: reserved • 78: reserved • 79: reserved • 80: reserved • 81: reserved • 82: reserved • 83: reserved • 84: reserved

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 85: reserved • 86: reserved • 87: password call barring service verification • 88: password call barring service registration • 89: call limiting cancellation • 90: number barring service activation • 91: number barring service deactivation • 92: number barring service deregistration • 93: reserved • 94: reserved • 95: active pwcb service • 96: deactive pwcb service • 97: reserved • 98: password barring service registration • 99: call barring service password change • 100: call barring service password verification • 101: call barring service password deactivation • 102: reserved • 103: reserved • 104: bust callback service deregistration • 105: reserved • 106: reserved • 107: no answer callback service deregistration • 108: reserved

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 109: immediate hotline service registration • 110: immediate hotline service deregistration • 111: delayed hotline service registration • 112: delayed hotline service deregistration • 113: CFU-voice mail (VM) service activation • 114: CFU-VM service deregistration • 115: CFB-VM service activation • 116: CFB-VM service deregistration • 117: CFNR-VM service activation • 118: CFNR-VM service deregistration • 119: CFO-VM service activation • 120: CFO-VM service deregistration • 121: user service password change • 122-170: reserved • 171: co-group pickup service • 172: designated pickup service • 173: self-number query • 174: abbreviated dialing • 175:Temporarily-active-CLIR • 176:Temporarily-deactive-CLIR • 177: reserved • 178: reserved

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 179: reserved • 180: reserved • 181: reserved • 182: reserved • 183: reserved • 191: reserved • 192: actual self-number query • 193: set the MWI service mode on • 194: set the MWI service mode off • 195-240: reserved
vu-service	Specifies the IVR service.	-
vu-service-name vuservicename	Specifies a VU service name.	The value is a string of 1 to 32 characters without spaces. Default: • vuvmswelcometone (record welcome tone service) • vuvmsleavemsg (leave voice mail message service) • vuvmsgetmsg (get voice mail message service) • vuconference (conference service) • vudefault (switchboard service) • vupwdcalllimit (pwd calllimit service for vu)

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

If you run the **call-type** command multiple times, only the latest configuration takes effect.

Example

Set the call type to local basic service in the view of the call prefix **prefix1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix1
[Huawei-voice-callprefix-prefix1] call-type category basic-service attribute 1
```

16.5.1.6 callprefix

Function

Using the **callprefix** command, you can configure a call prefix profile and enter the call prefix profile view.

Using the **undo callprefix** command, you can delete the call prefix profile.

By default, no call prefix profile is configured.

Format

callprefix *callprefix-name*

undo callprefix *callprefix-name*

Parameters

Parameter	Description	Value
callprefix-name	Specifies the name of a call prefix profile.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create a call prefix profile 20000.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix 20000
[Huawei-voice-callprefix-20000]
```

16.5.1.7 callroute (call prefix view)

Function

The **callroute** command configures a call route.

The **undo callroute** command deletes a configured call route.

Format

callroute *callroute-name*

undo callroute *callroute-name*

Parameters

Parameter	Description	Value
callroute-name	Specifies the call route name.	The value is a string of 1 to 32 characters without spaces.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure a call route named **router1** for call prefix 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix 2
[Huawei-voice-callprefix-2] callroute route1
```

16.5.1.8 cause-mapping

Function

Using the **cause-mapping** command, you can configure the mappings between ISDN cause values and SIP error codes.

Using the **undo cause-mapping** command, you can restore the mappings to defaults.

Format

cause-mapping { **isdn-cause** *isdn-cause-value* | **sip-response** *sip-response-value* } *

undo cause-mapping { **isdn-cause** [*isdn-cause-value*] | **sip-response** [*sip-response-value*] }

Parameters

Parameter	Description	Value
isdn-cause *isdn-cause-value*	Indicates the ISDN cause value.	The value is an integer that ranges from 1 to 127.
sip-response *sip-response-value*	Indicates the SIP error code.	The value is an integer that ranges from 100 to 699.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

You can run the **cause-mapping** command to customize the mappings between ISDN cause values and SIP error codes. The default mappings are used if you do not configure them.

Example

Map ISDN cause value 1 to SIP error code 404.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] cause-mapping isdn-cause 1 sip-response 404
```

16.5.1.9 collectcall (call prefix view)

Function

The **collectcall** command enables or disables the called party payment function.

The **undo collectcall** command disables the called party payment function.

By default, the called party payment function is disabled.

Format

collectcall *collectcall-value*

undo collectcall

Parameters

Parameter	Description	Value
collectcall-value	Indicates whether the called party payment function is enabled.	Enumerated value: • disable: The called party payment function is disabled. • enable: The called party payment function is enabled.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

When you deploy a called party payment service on a network, you need to enable the called party payment function for a prefix. During call setup, the payment flag is delivered to the remote device by signaling, and then the called party payment service is implemented in the charging system.

NOTE

The called party payment function is used only for E1R2 trunk connection and PRA trunk connection scenarios.

Example

Enable the called party payment function for a prefix.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix1
[Huawei-voice-prefix1] collectcall enable
```

16.5.1.10 country-code

Function

Using the **country-code** command, you can configure a country/region code.

Using the **undo country-code** command, you can cancel the configuration.

By default, some country/region codes are pre-configured on the device. You can run the **display voice country-code** command to view the country/region codes.

Format

country-code *country-code-value* [**country-name***country-name* | **international-prefix** *international-prefix-value* | **national-prefix** *national-prefix-value*]*

undo country-code *country-code-value* [**country-name** | **international-prefix** | **national-prefix**]

Parameters

Parameter	Description	Value
country-code-value	Specifies the country/region code.	The value is a numeral string of 1 to 4 digits.
country-name *country-name*	Specifies the country/region name.	The value is a string of 1 to 32 characters without spaces.
international-prefix *international-prefix-value*	Specifies the prefix of an international toll call.	The value is a numeral string of 1 to 5 digits.
national-prefix *national-prefix-value*	Specifies the prefix of a national toll call.	The value is a numeral string of 1 to 5 digits.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The **undo country-code** command cannot delete the pre-configured country/region codes.

NOTE

The device does not support the user-defined country code and region code. If the user-defined country code and region code are used, communication may fail.

Example

Set country/region code to 86, country name to **china**, and national toll call prefix to 025.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] country-code 86 country-name china national-prefix 0
```

16.5.1.11 crbt (enterprise view)

Function

Using the **crbt** command, you can enable the RBT function for an enterprise or disable this function.

Using the **undo crbt** command, you can cancel the configuration.

By default, the RBT function is disabled for an enterprise.

Format

crbt { enable | disable }

undo crbt

Parameters

Parameter	Description	Value
enable	Enable the RBT function for an enterprise.	-
disable	Disable the RBT function for an enterprise.	-

Views

Enterprise view

Default Level

2: Configuration level

Usage Guidelines

The **crbt disable** command disables the RBT function for an enterprise.

Example

Enable the RBT function for the enterprise **user1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] enterprise user1
[Huawei-voice-enterprise-user1] crbt enable
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.1.12 custom-right (call prefix view)

Function

The **custom-right** command binds a customized 32-level right to a call prefix.

By default, no 32-level right is bound to a call prefix.

Format

custom-right *custom-right-choice*.

undo custom-right.

Parameters

Parameter	Description	Value
custom-right-choice	Specifies a 32-level right to be bound to a call prefix.	The value can be only one of **c1** to **c32**.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

32-level rights can be bound to any prefixes. (For a VU prefix, the VU's 32-level right can be bound to the VU prefix additionally.)

Example

Bind 32-level right **c1** to **prefix1** in the call prefix view.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] callprefix prefix1
 [Huawei-voice-prefix1] custom-right c1
```

16.5.1.13 description (enterprise view)

Function

Using the **description** command, you can configure the description of an enterprise.

Using the **undo description** command, you can delete the description of an enterprise.

By default, no description is configured for an enterprise.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an enterprise.	The name is a string of 1 to 64 case-sensitive characters without spaces.

Views

Enterprise view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the description of the enterprise **user1** as **bank**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] enterprise user1
[Huawei-voice-enterprise-user1] description bank
```

16.5.1.14 digit-length

Function

The **digit-length** command sets the length of a number that can be parsed.

By default, the length of a number that can be parsed is not set.

Format

digit-length *minimum-length-value maximum-length-value*

Parameters

Parameter	Description	Value
maximum-length-value	Specifies the maximum length of a number that can be parsed.	The value is an integer that ranges from 1 to 32.
minimum-length-value	Specifies the minimum length of a number that can be parsed.	The value is an integer that ranges from 1 to 32.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

The maximum length of a number that can be parsed (*maximum-length-value*) must be greater than or equal to the minimum length of a number that can be parsed (*minimum-length-value*).

If the **digit-length** command runs for multiple times, the latest configuration overrides the previous one.

Example

Set the maximum length of a number that can be parsed to 20 and the minimum length to 5 in the view of the call prefix **prefix-user1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix-user1
[Huawei-voice-callprefix-prefix-user1] digit-length 5 20
```

16.5.1.15 disa

Function

Using the **disa** command, you can configure a **disa** profile and enter the **disa** profile view.

Using the **undo disa** command, you can delete the **disa** profile.

By default, no **disa** profile is configured.

Format

disa *disa-name* [**enterprise** *enterprise-name*]

undo disa*disa-name*

Parameters

Parameter	Description	Value
disa-name	Specifies the name of a disa profile.	The value is a string of 1 to 32 characters.
enterprise-name	Specifies the name of an enterprise profile.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create a disa profile d1.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] disa d1
 [Huawei-voice-disa-d1]
```

16.5.1.16 display voice account-set

Function

The **display voice account-set** command displays the configuration of account-set.

Format

display voice account-set [*account-set-name*]

Parameters

Parameter	Description	Value
account-set-name	Displays the configuration of a specified account-set. If the name of an account-set is not specified, the configuration of all account-sets is displayed.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice account-set** command displays the configuration of account-sets.

Example

Display the configuration of account-set.

```
[Huawei-voice]display voice account-set
  Spec:  10, Records: 1
  ------------------------
  Account-set              : 1
  Type                     : password
  Enterprise               : default
```

Table 16-41 Description of the **display voice account-set** command output

Item	Description
Account-set	Name of an account-set profile. To configure an account-set profile, run the **account-set** command.
Type	Type of account-set. There are account and password. By default, the type is password.
Enterprise	Enterprise name. To configure an enterprise name, run the **enterprise** command.

 Copyright © Huawei Technologies Co., Ltd.

16.5.1.17 display voice cac

Function

The **display voice cac** command queries the maximum number of online calls and current online calls for an IP address from which calls are limited.

Format

display voice cac destination-ip *ip-address*

Parameters

Parameter	Description	Value
ip-address	Specifies the peer IP address from which calls are limited.	The value is in dotted decimal notation.

Views

All views

Default Level

3: Management level

Usage Guidelines

Run this command to check whether call limiting has been configured for an IP address and check the number of online calls based the IP address.

Example

Query the maximum number of online calls and current online calls for the peer IP address of 192.168.0.1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice cac destination-ip 192.168.0.1
The maximum calls                  : 2000
The current calls                  : 2
```

Table 16-42 Description of the **display voice cac destination-ip** command output

Item	Description
Maximum calls	Specifies the maximum number of online calls on the trunk with the IP address from which calls are limited. Run the **16.5.1.4 cac**command to set this item.

Item	Description
Current calls	Specifies the current number of online calls on the trunk with the IP address from which calls are limited.

16.5.1.18 display voice callprefix

Function

The **display voice callprefix** command displays the configuration of call prefixes.

Format

display voice callprefix [*callprefix-name*]

Parameters

Parameter	Description	Value
callprefix-name	Displays the configuration of a specified call prefix. If the name of a call prefix is specified, the configuration of all call prefixes is displayed.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice callprefix** command displays the configuration of call prefixes.

During call prefix query, in the result, **#*****, ********, **#99***, and ***99*** are reserved prefixes, **#***** and ******** are used for the conference call service, and **#99*** and ***99*** are used for the MWI service**.**

Example

Display the configuration of call prefix.

```
<Huawei> display voice callprefix 01
  Callprefix        : 01
  Enterprise         : default
```

```
  Dn-set           : DefaultDialPlan
  Prefix           : 01
  Call category     : Basic service
  Call attribute    : 1(Local)
  Pwd Call Limit    : enable
  Minimum length    : 2
  Maximum length    : 10
  Long cli switch   : disable
  Caller map switch : disable
  Called map switch : disable
  Call route name   : sipbb
<Huawei> display voice callprefix 10089
  Callprefix        : 10089
  Enterprise        : default
  Dn-set           : DefaultDialPlan
  Prefix           : 10089
  Call category     : Vu service
  Vu Service Name   : IVR1
  VU Loop Count     : 0
  VU outgoing right : inter
  Pwd Call Limit    : enable
  Minimum length    : 5
  Maximum length    : 32
  Long cli switch   : disable
  Caller map switch : disable
  Called map switch : disable
```

Table 16-43 Description of the display voice callprefix command output

Item	Description
Callprefix	Name of a call prefix profile. To configure a call prefix profile, run the **callprefix** command.
Enterprise	Enterprise name. To configure an enterprise name, run the **16.5.1.34 enterprise (call prefix view)** command.
Dn-set	DN set name. To configure a DN set, run the **16.5.1.34 enterprise (call prefix view)** command.
Prefix	Call prefix name. To configure a call prefix, run the **16.5.1.41 prefix (call prefix view)** command.
Call category	Category of the call. To configure a call category, run the **16.5.1.5 call-type** command.
Call attribute	Attribute of a call. To configure a call attribute, run the **16.5.1.5 call-type** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VU Loop Count	Number of times the IVR voice file for the call prefix can be played. To configure a vu Loop Count, run the **vuloopcount** command.
VU outgoing right	Call out rights of the VU switchboard. To configure a vu outgoing right, run the **vuoutgoingright** command.
Minimum length	Minimum length of a number that can be parsed. To set the minimum length of a number that can be parsed, run the **digit-length** command.
Maximum length	Maximum length of a number that can be parsed. To set the maximum length of a number that can be parsed, run the **digit-length** command.
Long cli switch	Long number conversion switch. To configure a long cli switch, run the **special-deal** command.
Call route name	Call route name.
Caller map switch	Calling number mapping flag.
Called map switch	Called number mapping flag.
Pwd Call Limit	Password call barring flag.

16.5.1.19 display voice cause-mapping

Function

Using the **display voice cause-mapping** command, you can view the current mappings.

Format

display voice cause-mapping { **isdn-cause** | **sip-response** }

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the mappings of ISDN cause values.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice cause-mapping isdn-cause
  ISDN cause : 1      SIP response : 404
```

16.5.1.20 display voice country-code

Function

The **display voice country-code** command displays the configuration of country/region codes.

Format

display voice country-code [*country-code-value*]

Parameters

Parameter	Description	Value
country-code-value	Displays the configuration of a specified country/region code. If this parameter is not specified, the configuration of all country/region codes is displayed.	The value is a string of 1 to 4 digits.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice country-code** command displays the configuration of country/region codes.

Example

Display the configuration of country code 221.

```
<Huawei> display voice country-code 221
  Country code          : 221
  Country name          : Senegal
  International prefix  : 00
  National prefix       : 0
```

Table 16-44 Description of the **display voice country-code** command output

Item	Description
Country code	Country/Region code. To configure a country/region code, run the **country-code** command.
Country name	Country/Region name. To configure a country/region name, run the **country-code** command.
International prefix	Prefix of the international toll call. To configure the prefix of the international toll call, run the **country-code** command.
National prefix	Prefix of the national toll call. To configure the prefix of the national toll call, run the **country-code** command.

16.5.1.21 display voice disa

Function

The **display voice disa** command displays the configuration of disa.

Format

display voice disa [*disa-name*]

Parameters

Parameter	Description	Value
disa-name	Displays the configuration of a specified disa. If the name of a disa is not specified, the configuration of all disas is displayed.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice disa** command displays the configuration of disas.

Example

Display the configuration of disa.

```
[Huawei-voice-disa-d1]display voice disa d1
  Disa                    : d1
  Enterprise              : default
  Dn-set                  : DefaultDialPlan
  Access telno            : 89286000
  Account set             : 1
  Dst Enterprise          : hw
  Dst dn-set              : DefaultDialPlan
```

Table 16-45 Description of the **display voice disa** command output

Item	Description
Disa	Name of a disa profile. To configure a disa profile, run the **16.5.1.15 disa** command.
Enterprise	Enterprise name. To configure an enterprise name, run the **16.5.1.35 enterprise (voice view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dn-set	DN set name. To configure a DN set, run the **dn-set** command.
Access telno	access telno.
Account set	account-set name. To configure a call attribute, run the **account-set** command.
Dst Enterprise	Destination enterprise name. To configure an enterprise name, run the **16.5.1.35 enterprise (voice view)** command.
Dst dn-set	Destination dn-set name. To configure a DN set, run the **dn-set** command.

16.5.1.22 display voice dss1 timer

Function

The **display voice dss1 timer** command queries default durations and current values of all DSS1 timers.

Format

display voice dss1 timer

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Run this command to check the default duration and configured duration of a DSS1 timer.

 Copyright © Huawei Technologies Co., Ltd.

Example

Query the default durations and current values of all DSS1 timers.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice dss1 timer
Dss1-Timer     Default-Value     Current_Value
  T301          180               300
  T302          10               15
  T303          4                4
  T304          20               20
  T305          30               65535
  T306          30               30
  T307          180               0
  T308          4                6
  T309          90               65535
  T310          30               30
  T312          6                9000
  T313          4                4
  T314          4                4
  T316          120               8000
  T317          100               100
  T318          4                4
  T319          4                4
  T320          30               30
  T321          30               30
  T322          4                65535
```

Table 16-46 Description of the **display voice dss1 timer** command output

Item	Description
Dss1-Timer	Specifies the name of a DSS1 timer
Default-Value	Specifies the default duration of a DSS1 timer.
Current_Value	Specifies the configured duration of a DSS1 timer. Run the **dss1 timer** command to set this item.

16.5.1.23 display voice enterprise

Function

The **display voice enterprise** command displays the configuration of enterprises.

Format

display voice enterprise [**service crbt**] [*enterprise-name*]

Parameters

Parameter	Description	Value
enterprise-name	Displays the configuration of a specified enterprise. If this parameter is not specified, the configuration of all enterprises is displayed.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice enterprise** command displays the configuration of enterprises.

Example

Display the configuration of the enterprise **user1**.

```
<Huawei> display voice enterprise user1
  Enterprise              : hw
  Max dn-set number       : 5
  Dn-set                  : hwdnset
  Dn-set description      :
  Dn-set                  : DefaultDialPlan
  Dn-set description      : DefaultDialPlan
```

Table 16-47 Description of the display voice enterprise command output

Item	Description
Enterprise	Enterprise name. To configure an enterprise name, run the **16.5.1.34 enterprise (call prefix view)** command.
Enterprise description	Enterprise description.
Max dn-set number	Max dn-set number.
Dn-set	Dn-set name. To configure a dn-set name, run the **16.5.1.34 enterprise (call prefix view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dn-set description	Dn-set description.

16.5.1.24 display voice media-bandwidth-control (PBX)

Function

The **display voice media-bandwidth-control** command displays CAC configurations and media bandwidth occupied by voice data on a PBX.

Format

display voice media-bandwidth-control [**sipserver** | **trunk-group** *groupname*]

Parameters

Parameter	Description	Value
sipserver	Displays CAC configurations and media bandwidth occupied by voice data on the SIP server and SBC proxy.	-
trunk-group *groupname*	Displays CAC configurations and media bandwidth occupied by voice data in a specified truck group.	The group name is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display CAC configurations and media bandwidth occupied by voice data on the SIP server and SBC proxy.

```
<Huawei> display voice media-bandwidth-control sipserver
 Upward bandwidth                    : enable
```

```
The maximum upward bandwidth            : 500000 kbit/s
The used normal bandwidth               : 0 kbit/s

Media proxy upward bandwidth                        : enable
The maximum upward bandwidth of media proxy            : 500000 kbit/s
The used normal bandwidth of media proxy               : 0 kbit/s
```

Table 16-48 Description of the display voice media-bandwidth-control command output

Item	Description
Upward bandwidth	Whether CAC is enabled on the SIP server: ● Enable ● Disable To enable CAC on the SIP server, run the **16.5.6.57 media-bandwidth-control enable (trunk-group)** command.
The maximum upward bandwidth	Maximum media bandwidth on the SIP server. To set the maximum media bandwidth on the SIP server, run the **16.5.6.58 media-bandwidth-control max-bandwidth (trunk-group)** command.
The used normal bandwidth	Media bandwidth occupied by voice data on the SIP server.
Media proxy upward bandwidth	Whether CAC is enabled on the SBC proxy: ● Enable ● Disable To enable CAC on the SBC proxy, run the **16.5.5.2 media-bandwidth-control media-proxy enable** command.
The maximum upward bandwidth of media proxy	Maximum media bandwidth on the SBC proxy. To set the maximum media bandwidth on the SBC proxy, run the **16.5.5.3 media-bandwidth-control media-proxy max-bandwidth** command.
The used normal bandwidth of media proxy	Media bandwidth occupied by voice data on the SBC proxy.

 Copyright © Huawei Technologies Co., Ltd.

16.5.1.25 display voice pbx country-area-transform

Function

The **display voice pbx country-area-transform** command displays the country code, area code, and enable/disable status of PBX number normalization.

Format

display voice pbx country-area-transform

Parameters

None.

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display the country code, area code, and enable/disable status of PBX number normalization.

```
<Huawei> display voice pbx country-area-transform
    Default country code:                    86
    Default area code:                      755
    Enable Country Area Transform Flag:        enable
```

Table 16-49 Description of the **display voice pbx country-area-transform** command output

Item	Description
Default country code	Default country code.
Default area code	Default area code.
Enable Country Area Transform Flag	Enable/Disable status of number normalization.

 Copyright © Huawei Technologies Co., Ltd.

16.5.1.26 display voice pbx parameter

Function

The **display voice pbx parameter** command displays PBX control points and service priorities.

Format

display voice pbx parameter

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display PBX control points and service priorities.

```
<Huawei> display voice pbx parameter
  Number parameter No.     Value

    0                  0
    1                  1
    2                  1
    3                  30
    4                  0
    5                  5000
    6                  1
    7                  3
    8                  1
    9                  1
    10                 30000
    11                 3000
    12                 1
    13                 5000
    14                 30
    15                 0
    16                 0
    17                 8
    18                 2
    19                 0
    20                 2
    21                 18
    22                 1
    23                 4
    24                 3
    25                 8
```

 Copyright © Huawei Technologies Co., Ltd.

26	1
27	8
28	3
29	0
30	1
31	250
32	2
33	1
34	1000
35	4000
36	28000
37	0
38	0
39	5
40	0
41	30000
42	25000
43	8000
44	15000
45	30000
46	60000
47	90000
48	120000
49	60000
50	1
51	3
52	2
53	0
54	4000
55	300000
56	0
57	0
58	1
59	1
60	1
61	4
62	50
63	1
64	0
65	40000
66	60000
67	5
68	1800
69	3
70	180
71	0
72	0
73	1
74	100
75	0
76	0
77	0
78	0
79	0
80	0
81	0
82	0
83	0
84	2400
85	0
86	2
87	15
88	2
89	32
90	7
91	10
92	10
93	15
94	0

 Copyright © Huawei Technologies Co., Ltd.

95	4294967295
96	16
97	10
98	60
99	2
100	500
101	0
102	0
103	0
104	1
105	1
106	16560000
107	0
108	0
109	5
110	0
111	0
112	1
113	10
114	0
115	0
116	0
117	4294967295
118	4294967295
119	4294967295
120	4294967295
121	4294967295
122	4294967295
123	4294967295
124	4294967295
125	4294967295
126	4294967295
127	4294967295
128	4294967295
129	4294967295
130	4294967295
131	4294967295
132	4294967295
133	4294967295
134	4294967295
135	4294967295
136	4294967295
137	4294967295
138	4294967295
139	4294967295
140	4294967295
141	4294967295
142	4294967295
143	4294967295
144	4294967295
145	4294967295
146	4294967295
147	4294967295
148	4294967295
149	4294967295
150	4294967295
151	4294967295
152	4294967295
153	4294967295
154	4294967295
155	4294967295
156	4294967295
157	4294967295
158	4294967295
159	4294967295
160	4294967295
161	4294967295
162	4294967295
163	4294967295

 Copyright © Huawei Technologies Co., Ltd.

```
    164             4294967295
    165             4294967295
    166             4294967295
    167             4294967295
    168             4294967295
    169             4294967295
    170             4294967295
    171             4294967295
    172             4294967295
    173             4294967295
    174             4294967295
    175             4294967295
    176             4294967295
    177             4294967295
    178             4294967295
    179             4294967295
    180             4294967295
    181             4294967295
    182             4294967295
    183             4294967295
    184             4294967295
    185             4294967295
    186             4294967295
    187             4294967295
    188             4294967295
    189             4294967295
    190             4294967295
    191             4294967295
    192             4294967295
    193             4294967295
    194             4294967295
    195             4294967295
    196             4294967295
    197             4294967295
    198             4294967295
    199             4294967295
    200             0
    201             0
    202             1
    203             0
    204             0
    205             10
    206             0
    207             1
    208             1
    209             1
    210             1
    211             0
    212             2
    213             0
    214             1

String parameter No.     Value

    Default country code:                  86
    Default area code:                    755
    Enable Country Area Transform Flag:        enable
```

Table 16-50 Description of the display voice pbx-parameter command output

Item	Description
Number parameter No.	Number of a control point. For the meaning of each parameter number, see the Usage Guidelines of the **pbx number-parameter** command.

Item	Description
Value	Value of a control point. For the default value of each parameter, see the Usage Guidelines of the **pbx number-parameter** command.
Default country code	Default country code.
Default area code	Default area code.
Enable Country Area Transform Flag	Number normalization flag.

16.5.1.27 display voice ring-mode

Function

The **display voice ring-mode** command displays PBX ring mapping parameters.

Format

display voice ring-mode [*index*]

Parameters

Parameter	Description	Value
index	Specifies the index of a ring mapping. If no ring mapping index is specified, all ring mapping parameters are displayed.	The value is an integer that ranges from 0 to 15.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If no PBX ring mapping parameter is set by using the **ring-mode** command, the **display voice ring-mode** command does not display any information.

Example

Display information about ring mapping 1.

```
<Huawei> display voice ring-mode 1
  PBX ring type          : 1
  PSTN init ring type    : 17
  PSTN cadence ring type : 6
  SIPUE ring type name   : AlertInfo1
```

Table 16-51 Description of the display voice ring-mode command output

Item	Description
PBX ring type	Index of a ring. To set the index of a ring, run the **16.5.1.44 ring-mode** command.
PSTN init ring type	Type of the initial ringing. To set the type of the initial ringing, run the **16.5.1.44 ring-mode** command.
PSTN cadence ring type	Type of the cadence ringing. To set the type of the cadence ringing, run the **16.5.1.44 ring-mode** command.
SIPUE ring type name	Name of the differentiated ringing type of a SIP UE user. To set the name of the differentiated ringing type of a SIP UE user, run the **16.5.1.44 ring-mode** command.

16.5.1.28 display voice tone-set

Function

The **display voice tone-set** command displays the mapping between cause codes and tones.

Format

display voice tone-set

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the mapping between cause codes and tones after the mapping is configured.

Example

View the mapping between cause codes and tones.

```
<Huawei> display voice tone-set
 Type : dnerror
 Tone Id : 177
```

16.5.1.29 dn-set (disa view)

Function

Using the **dn-set** command, you can configure a dialed number (DN) set.

By default, the disa has a name for **defaultdialplan** DN set.

Format

dn-set *dn-set-name*

Parameters

Parameter	Description	Value
dn-set-name	Specifies the name of a DN set.	The value is a string of 1 to 32 characters without spaces.

Views

Disa view

Default Level

2: Configuration level

Usage Guidelines

A DN set is a collection of prefixes that all users on the PSTN can dial. The device supports a maximum of four DN sets except the default DN set.

Example

Create a DN set **dialplan1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] disa d1
[Huawei-voice-disa-d1] dn-set dialplan1
```

16.5.1.30 dn-set (enterprise view)

Function

Using the **dn-set** command, you can configure a dialed number (DN) set.

Using the **undo dn-set** command, you can delete a DN set.

By default, the enterprise have a name for **defaultdialplan** DN set.

Format

dn-set *dn-set-name* [**description** *description*]

undo dn-set *dn-set-name* [**description**]

Parameters

Parameter	Description	Value
dn-set-name	Specifies the name of a DN set.	The value is a string of 1 to 32 characters without spaces.
description	Specifies the description of a DN set.	The value is a string of 1 to 64 characters without spaces.

Views

Enterprise view

Default Level

2: Configuration level

Usage Guidelines

A DN set is a collection of prefixes that all users on the PSTN can dial. The device supports a maximum of four DN sets except the default DN set.

Example

Create a DN set **dialplan1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] enterprise user1
[Huawei-voice-enterprise-user1] dn-set dialplan1
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.1.31 dss1 timer

Function

The **dss1 timer** command sets the duration of a DSS1 timer.

The **undo dss1 timer** command restores the default settings of all DSS1 timers.

By default, each timer uses the default value.

Format

dss1 timer { **T301 | T302 | T303 | T304 | T305 | T306 | T307 | T308 | T310 | T312 | T313 | T314 | T316 | T317 | T318 | T319 | T320 | T321 | T322** } **timer-length** *timer-length-value*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
timer-length-value	Specifies the timer duration, in seconds.	• T301 timer: The value is an integer that ranges from 180 to 65535. The default value is 180. • T302 timer: The value is an integer that ranges from 5 to 65535. The default value is 10. • T303 timer: The value is an integer that ranges from 0 to 65535. The default value is 4. • T304 timer: The value is an integer that ranges from 0 to 65535. The default value is 20. • T305 timer: The value is an integer that ranges from 0 to 65535. The default value is 30. • T306 timer: The value is an integer that ranges from 0 to 65535. The default value is 30. • T307 timer: The value is an integer that ranges from 0 to 65535. The default value is 180. • T308 timer: The value is an integer that ranges from 0 to 65535. The default value is 4. • T309 timer: The value is an integer that ranges from 0 to 65535. The default value is 90. • T310 timer: The value is an integer that ranges from 0 to 40. The default value is 30. • T312 timer: The value is an integer that ranges from 0 to 65535. The default value is 6.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• T313 timer: The value is an integer that ranges from 0 to 65535. The default value is 4. • T314 timer: The value is an integer that ranges from 0 to 65535. The default value is 4. • T316 timer: The value is an integer that ranges from 0 to 65535. The default value is 120. • T317 timer: The value is an integer that ranges from 0 to 65535. The default value is 100. • T318 timer: The value is an integer that ranges from 0 to 65535. The default value is 4. • T319 timer: The value is an integer that ranges from 0 to 65535. The default value is 4. • T320 timer: The value is an integer that ranges from 0 to 65535. The default value is 30. • T321 timer: The value is an integer that ranges from 0 to 65535. The default value is 30. • T322 timer: The value is an integer that ranges from 0 to 65535. The default value is 4.

Views

Voice view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Run this command to independently configure durations of DSS1 timers on a BRA/PRA trunk and during calling of BRA users.

Precautions

This command takes effect globally. After the value of a time is set, the value is valid for all BRA/PRA trunks and the calling process of BRA users.

Example

Set the duration of the T301 timer to 200s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] dss1 timer T301 timer-length 200
```

16.5.1.32 dst-enterprise (disa view)

Function

The **dst-enterprise** command configures the destination enterprise and the destination dn-set of disa.

Format

dst-enterprise *enterprise-name* [**dst-dnset** *dn-set-name*]

Parameters

Parameter	Description	Value
enterprise-name	Specifies the destination enterprise name.	The value is a string of 1 to 32 characters without spaces.
dst-dnset *dn-set-name*	Specifies the destination dn-set name.	The value is a string of 1 to 32 characters without spaces.

Views

Disa view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure a dst-enterprise named ab for disa d1.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] disa d1
 [Huawei-voice-disa-d1]dst-enterprise ab
```

16.5.1.33 enterprise (account-set view)

Function

The **enterprise** command binds an enterprise to an account-set.

The **undo enterprise** command unbinds an enterprise from an account-set.

By default, no enterprise is bound to an account-set.

Format

enterprise *enterprise-name*

undo enterprise

Parameters

Parameter	Description	Value
enterprise-name	Specifies the name of an enterprise. An enterprise is created by using the **enterprise** command in the PBX view.	The value is a string of 1 to 32 characters without spaces.

Views

Account-set view

Default Level

2: Configuration level

Usage Guidelines

An account-set can be bound to only one enterprise, but an enterprise can be bound to multiple account-sets.

Example

Bind the account-set **1** to the enterprise **ab**.

```
<Huawei> system-view
[Huawei] voice
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-voice] account-set 1
[Huawei-voice-account-set-1] enterprise ab
```

16.5.1.34 enterprise (call prefix view)

Function

The **enterprise** command binds an enterprise, and DN set to a call prefix.

The **undo enterprise** command unbinds an enterprise, and DN set from a call prefix.

By default, no enterprise, or DN set is bound to a call prefix.

Format

enterprise *enterprise-name* [**dn-set** *dn-set-name*]

undo enterprise

Parameters

Parameter	Description	Value
enterprise-name	Specifies the name of an enterprise. An enterprise is created by using the **enterprise** command in the PBX view.	The value is a string of 1 to 32 characters without spaces.
dn-set *dn-set-name*	Specifies the name of a DN set.	The value is a string of 1 to 32 characters without spaces.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

A call prefix can be bound to only one enterprise, but an enterprise can be bound to multiple call prefixes.

Example

Bind the call prefix **prefix-user1** to the enterprise **user1**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] callprefix prefix-user1
[Huawei-voice-callprefix-prefix-user1] enterprise user1
```

16.5.1.35 enterprise (voice view)

Function

The **enterprise** command creates an enterprise and enters the enterprise view.

The **undo enterprise** command deletes an enterprise.

By default, an enterprise named **default** exists on the device.

Format

enterprise *enterprise-name*

undo enterprise *enterprise-name*

Parameters

Parameter	Description	Value
enterprise-name	Specifies the name of an enterprise.	The value is a string of 1 to 32 characters without spaces.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When the device is connected to multiple enterprises, you can create enterprises and configure these enterprises.

Example

Create an enterprise **user1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] enterprise user1
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.1.36 inter-only-call-source

Function

Using the **inter-only-call-source** command, you can configure inter only call source of a call prefix.

Using the **undo inter-only-call-source** command, you can cancel inter only call source of a call prefix.

By default, no inter only call source is configured.

Format

inter-only-call-source *callsource-name*

undo inter-only-call-source

Parameters

Parameter	Description	Value
callsource-name	The name of a call source.	The value is a string of 1 to 32 characters.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create a inter only call source 30000.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] callprefix 20000
 [Huawei-voice-callprefix-20000] inter-only-call-source 30000
```

16.5.1.37 password cipher (account-set view)

Function

The **password cipher** command configures the password of the account-set.

The **undo password** command deletes the password of the account-set.

Format

password cipher *password-value*

undo password *password-value*

Parameters

Parameter	Description	Value
password-value	Specifies the password value.	The value is a string of 6 to 8 digits without spaces.

Views

account-set view

Default Level

2: Configuration level

Usage Guidelines

None

Example

configure the password 12345678 for account-set 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]account-set 1
[Huawei-voice-account-set-1]password cipher
Please input user password(6-8 chars):********
```

16.5.1.38 pbx default-country-code default-area-code

Function

The **pbx default-country-code default-area-code** command configures the system default country code and area code.

The **undo pbx default-country-code default-area-code** command restores the default settings.

By default, the country code is 86 and area code is 755.

Format

pbx { **default-country-code** *dcc-value* | **default-area-code** *dac-value* | **default-area-code** *dac-value* }

undo pbx { **default-country-code** | **default-area-code** }

Parameters

Parameter	Description	Value
default-country-code *dcc-value*	Indicates the country code parameters.	The value is a numeral string of 1 to 4 digits.
default-area-code *dac-value*	Indicates the area code parameters.	The value is a numeral string of 1 to 8 digits.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the default region code to **25**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbx default-area-code 25
```

16.5.1.39 pbx enable-country-area-transform

Function

The **pbx enable-country-area-transform** command configures whether to enable number regulation.

By default, number regulation is disabled.

Format

pbx enable-country-area-transform *enable-country-area-transform-value*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
enable-country-area-transform-value	Indicates whether number regulation is enabled.	Enumerated type. The options are as follows: ● enable ● disable default:disable

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable number regulation.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbx enable-country-area-transform enable
```

16.5.1.40 pbx number-parameter

Function

The **pbx number-parameter** command sets control points for a PBX.

The **undo pbx number-parameter** command restores the default control point settings of a PBX.

Format

pbx number-parameter *name value*

undo pbx number-parameter *value*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name	Specifies the name of a control point.	The value is an integer that ranges from 0 to 250.
value	Specifies the value of a control point.	The value is an integer that ranges from 0 to 4294967295. The value of *value* varies according to *name*. For details, see the usage guideline.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The following table describes the meanings and values of control points.

Control Point Name	Description	Value
0	Configures whether to support SDP RTCP.	Enumerated value. The options are as follows: ● 0: SDP RTCP is not supported. ● 1: SDP RTCP is supported. The default value is 0.
1 to 3	Reserved.	-
4	Indicates whether the PBX processes CNG signals.	Enumerated value. The options are as follows: ● 0: The PBX does not process CNG signals. ● 1: The PBX processes CNG signals. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
5	Sets the delay in processing modem events.	The value is an integer that ranges from 0 to 50000, in milliseconds. The default value is 5000. The value 0 indicates that model events are processed immediately.
6	Reserved.	-
7	Configures whether to initiate re-negotiation when the H.323 was in early media condition.	Enumerated value. The options are as follows: ● 0: Re-negotiation is not initiated. ● 1: Re-negotiation is initiated. The default value is 0.
8	Configures whether to use the local or remote priority mode for SDP negotiation.	Enumerated value. The options are as follows: ● 0: The local priority mode is used for SDP negotiation. ● 1: The remote priority mode is used for SDP negotiation. The default value is 1.
9	Sets the SDP packetization time format.	Enumerated value. The options are as follows: ● 0: maxmptime ● 1: ptime The default value is 1.
10 to 14	Reserved.	-
15	Configures whether to use VBD when G.711 is used.	Enumerated value. The options are as follows: ● 0: VBD is not used when the codec is G.711. ● 1: VBD is used when the codec is G.711. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
16	Sets the service triggering mode.	Enumerated value. The options are as follows: ● 0: Loose coupling mode. ● 1: Semi-tight coupling in inband mode ● 2: Semi-tight coupling in outband mode ● 3: Full coupling mode The default value is 0.
17	Sets the codec mode when the codec priority is 0.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726-32 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 21: G726-16 ● 22: G726-24 ● 23: G726-40 ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 8.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
18	Sets the packetization time when the codec priority is 0.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 2.
19	Sets the codec mode when the codec priority is 1.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 0.
20	Sets the packetization time when the codec priority is 1.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
21	Sets the codec mode when the codec priority is 2.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 18.
22	Sets the packetization time when the codec priority is 2.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
23	Sets the codec mode when the codec priority is 3.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 4.
24	Sets the packetization time when the codec priority is 3.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 3.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
25	Sets the codec mode when the codec priority is 4.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 8.
26	Sets the packetization time when the codec priority is 4.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
27	Sets the codec mode when the codec priority is 5.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 8.
28	Sets the packetization time when the codec priority is 5.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 3.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
29	Sets the codec mode when the codec priority is 6.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 0.
30	Sets the packetization time when the codec priority is 6.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
31	Sets the codec mode when the codec priority is 7.	Enumerated value. The options are as follows: ● 0: G711U ● 2: G726 ● 4: G723 ● 8: G711A ● 9: G722 ● 15: G728 ● 18: G729 ● 20: G723Low ● 96: R2198 ● 97: R2833 ● 98: v150 ● 99: clear mode ● 250: T.38 ● 251: T.38+2 The default value is 250.
32	Sets the packetization time when the codec priority is 7.	Enumerated value. The options are as follows: ● 0: 5 ms ● 1: 10 ms ● 2: 20 ms ● 3: 30 ms ● 4: 40 ms ● 5: 50 ms ● 6: 60 ms The default value is 2.
33	Configures whether to support early media.	Enumerated value. The options are as follows: ● 0: Early media is not supported. ● 1: Early media is supported. The default value is 1.
34 to 36	Reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
37	Configures whether to use CLIP polarity reversal.	Enumerated value. The options are as follows: ● 0: CLIP polarity reversal is not required. ● 1: CLIP polarity reversal is required. The default value is 0.
38	Sets the sequence in which B channels will be selected.	Enumerated value. The options are as follows: ● 0: Preferred ● 1: Designated The default value is 0.
39	Sets the duration during which the AG0 port detects the calling number.	The value is an integer that ranges from 0 to 15, in seconds. The default value is 5.
40	Sets the interval between two digits on the AG0 port.	The value is an integer that ranges from 0 to 15, in seconds. The default value is 0.
41	Sets the period during which a user does not dial any number after picking up the phone.	The value is an integer that ranges from 10000 to 30000, in milliseconds. The default value is 10000.
42	Sets the interval between two digits for common calls.	The value is an integer that ranges from 5000 to 60000, in milliseconds. The default value is 20000.
43	Sets Trunk PRI out call Transfer Capability field filled with 3.1 kHz audio or SPEECH.	Enumerated value. The options are as follows: ● 0: 3.1 kHz audio ● 1: SPEECH The default value is 1.
44	Sets the duration of waiting for called response	The value is an integer that ranges from 1500 to 300000, in milliseconds. The default value is 1500.
45	Reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
46	Indicates the waiting time threshold, crossing which an intra-office or local call is regarded as no response.	The value is an integer that ranges from 10000 to 300000, in milliseconds. The default value is 60000.
47	Indicates the waiting time threshold, crossing which a national toll call is regarded as no response.	The value is an integer that ranges from 10000 to 300000, in milliseconds. The default value is 90000.
48	Indicates the waiting time threshold, crossing which an international toll call is regarded as no response.	The value is an integer that ranges from 10000 to 300000, in milliseconds. The default value is 120000.
49	Reserved.	-
50	Configures whether to display the default calling number of the trunk group.	Enumerated value. The options are as follows: ● 0: The default calling number is not displayed. ● 1: The default calling number is displayed. The default value is 1.
51 and 52	Reserved.	-
53	Sets the CDR format.	Enumerated value. The options are as follows: ● 0: CDR ● 1: SOFTX ● 2: MINI ● 3: UCBILL The default value is 0.
54 to 61	Reserved.	-
62	Whether use 91 as clearmode payload.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
63	Reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
64	Specifies whether to check the remote IP address when the H.323 receives an incoming call.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 1.
65	Specifies the duration of the busy tone.	The value is an integer that ranges from 1000 to 300000, in milliseconds. The default value is 40000.
66-67	Reserved.	-
68	Sets the lifecycle of the CCBS/CCNR service.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 1800. 0: The CCBS/CCNR service is always effective.
69	Sets the number of CCBS/CCNR service attempts.	The value is an integer that ranges from 0 to 20. The default value is 3. 0: The CCBS/CCNR service is always effective.
70	Sets the interval for CCBS/CCNR service attempts.	The value is an integer that ranges from 1 to 1800, in seconds. The default value is 180.
71	Whether to delete the pound sign (#) when users call external users.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
72	Configures whether the AT0 trunk that does not provide calling number detection releases calls.	Enumerated value. The options are as follows: ● 0: The AT0 trunk that does not provide calling number detection does not release calls. ● 1: The AT0 trunk that does not provide calling number detection releases calls. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
73	Sets the stream mode for playing the announcement.	Enumerated value. The options are as follows: ● 0: Sendonly ● 1: SendRecv The default value is 0.
74	Sets the delay in collecting digits.	The value is an integer that ranges from 0 to 1000, in 10 ms. The default value is 100.
75	Configures whether to allow user register at local device.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
76	Set the dsp ignore event.	The value is an integer that ranges from 0 to 62. The default value is 0.
77-83	Reserved.	-
84	Sets the FTP server size in the CDR.	The value is an integer that ranges from 1 to 30000. The default value is 2400.
85	Configures whether to store CDRs locally.	Enumerated value. The options are as follows: ● 0: CDRs cannot be stored locally. ● 1: CDRs can be stored locally. The default value is 0.
86	Sets the number of stored CDRs.	The value is an integer that ranges from 1 to 1024. The default value is 2.
87	Sets the interval at which CDRs are saved.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 15.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
88	Sets the processing policy after the hard disk or memory is full.	Enumerated value. The options are as follows: ● 0: Calls are rejected. ● 1: CDRs are not generated. ● 2: Old CDRs are overwritten. The default value is 2.
89 to 93	Reserved.	-
94	Sets the MWI mode of the ISDN port.	Enumerated value. The options are as follows: ● 0: DEFERRED ● 1: IMMEDIATE ● 2: COMBINE The default value is 0.
95 to 97	Reserved.	-
98	Sets the value of the protection timer.	The value is an integer that ranges from 1 to 0xFFFF, in seconds. The default value is 60.
99	Reserved.	-
100	Sets the duration for the MWI completes FSK transmission.	The value is an integer that ranges from 10 to 0xFFFF, in milliseconds. The default value is 500.
101	Sets the MWI format.	Enumerated value. The options are as follows: ● 0: The MWI is on or off. ● 1: Defined by the ETSI standards. The default value is 0.
102	Configures whether the trunk group sends the number of the minimum length.	Enumerated value. The options are as follows: ● 0: The trunk group does not send the number of the minimum length. ● 1: The trunk group sends the number of the minimum length. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
103	Configures whether to enable media proxy when the media proxy policy is auto and IP addresses of both communicating parties are the same.	Enumerated value. The options are as follows: ● 0: Media proxy is not enabled. ● 1: Media proxy is enabled. The default value is 0.
104	Configures whether to enable media proxy when SIP trunks are connected.	Enumerated value. The options are as follows: ● 0: Media proxy is enabled when SIP trunks are connected. ● 1: Media proxy is not enabled when SIP trunks are connected. The default value is 1.
105	Configures media proxy address selection after IP-side media proxy is enabled.	Enumerated value. The options are as follows: ● 0: The configured media IP address is used. ● 1: The IP address between the media IP address and media mapping IP address is used, which is on the same network segment as the remote end. The default value is 1.
106 and 107	Reserved.	-
108	Configures whether to use the calling number for the call forwarding service.	Enumerated value. The options are as follows: ● 0: The calling number for the call forwarding service is not used. ● 1: The calling number for the call forwarding service is used. The default value is 0.
109 and 110	Reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
111	Configures whether to initiate re-negotiation when the invite200 message sent by the peer end contains multiple codec values.	Enumerated value. The options are as follows: ● 0: Re-negotiation is not initiated. ● 1: Re-negotiation is initiated. The default value is 0.
112 and 113	Reserved.	-
114	Sets the attributes of the calling or called number over the BRA or PRA trunk.	Enumerated value. The options are as follows: ● 0: The call number attribute remains unchanged. ● 1: The international call number attributes are unknown. ● 2: The national call number attributes are unknown. ● 3: The international and national call number attributes are unknown. ● 4: The local call number attributes are unknown. ● 5: The local and international call number attributes are unknown. ● 6: The local and national call number attributes are unknown. ● 7: The local, national, and international call number attributes are unknown. The default value is 0.
115 to 119	Reserved.	-
120	Indicates the duration of the T301 timer on the DSS1 side.	The value is an integer that ranges from 180 to 65535, in seconds. The default value is 180.
121	Indicates the duration of the T302 timer on the DSS1 side.	The value is an integer that ranges from 5 to 65535, in seconds. The default value is 10.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
122	Indicates the duration of the T303 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.
123	Indicates the duration of the T304 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 20.
124	Indicates the duration of the T305 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
125	Indicates the duration of the T306 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
126	Indicates the duration of the T307 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 180.
127	Indicates the duration of the T308 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.
128	Indicates the duration of the T309 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 90.
129	Indicates the duration of the T310 timer on the DSS1 side.	The value is an integer that ranges from 0 to 40, in seconds. The default value is 30.
130	Indicates the duration of the T312 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 6.
131	Indicates the duration of the T314 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
132	Indicates the duration of the T316 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 120.
133	Indicates the duration of the T317 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 100.
134	Indicates the duration of the T320 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
135	Indicates the duration of the T321 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
136	Indicates the duration of the T322 timer on the DSS1 side.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.
137	Specifies whether to respond to the session update without reporting the service.	Enumerated value. The options are as follows: ● 0: Yes ● 1: No The default value is 0.
138	Set the IP trunk wait dial number timer length.	The value is an integer that ranges from 1 to 15, in seconds. The default value is 5.
139	Indicates whether the AR sends subsequent requests to the new address when the peer address or port number is changed in the contact field of the response that the AR receives.	Enumerated value. The options are as follows: ● 0: Yes ● 1: No The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
140	Specifies whether to delete the reason header field when calls of FXS or unknown local users are made over the SIP trunk and released.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
141	Indicates the timer duration, exceeding which an outgoing local call routed through the SIP trunk is regarded as no response.	The value is an integer that ranges from 10000 to 600000, in milliseconds. The default value is 60000.
142	Indicates the timer duration, exceeding which an outgoing national toll call routed through the SIP trunk is regarded as no response.	The value is an integer that ranges from 10000 to 600000, in milliseconds. The default value is 90000.
143	Indicates the timer duration, exceeding which an outgoing international toll call routed through the SIP trunk is regarded as no response.	The value is an integer that ranges from 10000 to 600000, in milliseconds. The default value is 120000.
144	Set the ISDN trunk wait dial number timer length.	The value is an integer that ranges from 1 to 15, in seconds. The default value is 10.
145	Reserved.	-
146	Whether to play a congestion tone by DISCONNECT message in the net-to-user direction.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
147	Configures whether print the log on the screen.	Enumerated value. The options are as follows: ● 0: Yes ● 1: No The default value is 0.
148	Specifies whether to change the Min-SE value to a valid one if it is 0.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes (Change the value to 90) The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
149	Specifies the aging time of the SIP Flood and DDoS attack prevention whitelist.	The value is an integer that ranges from 30 to 1800, in seconds. The default value is 90.
150	Specifies whether to send progress to dss1 after alerting	Enumerated value. The options are as follows: ● 0: Not send ● 1: Send The default value is 1.
151	Specifies whether to enable limiting after registration fails.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0. **NOTE** This control point determines whether to start limiting on registration packets only. This control point needs to be used with control point 152 to determine whether to enable limiting on registration packets. The status of this control point does not affect generated entries in the flow limiting table.
152	Specifies the failure count before limiting is enabled.	The value is an integer that ranges from 1 to 10. The default value is 3.
153	Specifies the aging time of entries in the flow limiting table.	The value is an integer that ranges from 60 to 1800, in seconds. The default value is 300. **NOTE** If the aging time is too short, you can run the **debugging voice nm cmd 800** and **debugging voice nm cmd 801 p1 0** command on the nm module to perform software commissioning and delete corresponding entries in the flow limiting table.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
154	Specifies whether to delete the audio line when the media and audio or t38 and audio exist in one media line.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
155	Specifies whether the AR plays the ringback tone for the downlink device.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
156	Indicates whether a call is released when no sequential ringing group member answers the call.	Enumerated value. The options are as follows: ● 0: Calls are not released. ● 1: Calls are released. The default value is 0.
157	Indicates whether the SDP-answer that is sent after a media negotiation is performed contains all common codecs shared by the system and SDP-offer.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
158	Specifies whether a device immediately sends a Cancel message to release the session with a remote device when it does not receive an Invite response from the remote device after sending an Invite message to the remote external device using a SIP AT0 trunk.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
159	Specifies a call waiting service mode.	The value is an integer. The options are as follows: ● 0: IVR prompt mode. ● 1: Simplified mode. A user can press the hookflash directly without hearing a prompt tone and switch the call. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
160	Specifies whether to convert the Progress messages of a BRA trunk to the Alerting messages.	The value is an integer. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
161	Specifies whether the IMS core can use UA profiles in SIP to set the service attributes of a PBX user through an SIP AT0 trunk.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
162	Indicates whether authentication information is carried in the registration refresh messages sent by AR routers in SIP AT0 and SIP PRA connection scenarios.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
163	Indicates whether to forcibly add SDP to 180 Ringing messages that are mapped to the SIP side after an AR receives Alerting messages sent from the PRA side in the scenario where SIP trunk incoming calls are transferred to a PRA trunk.	The value is an integer. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
164	Indicates whether an AR proactively releases a call upon the receiving of an ACK message carrying media information after media negotiation is completed using an INVITE message and a 200 OK message on a SIP trunk.	The value is an integer. The options are as follows: ● 0: Yes ● 1: No The default value is 0.
165	IVR two dial connected to the U1981 on the IP phone, U1981 to the same group after the answer whether the end sent Re-invite message.	The value is an integer. The options are as follows: ● 0: Yes ● 1: No The default value is 0.
166 to 199	Reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
200	Switch for generating failure-specific CDRs.	Enumerated value. The options are as follows: ● 0: No CDRs are generated for any failures. ● 1: CDRs for all failures are generated. ● 2: CDR for trunk failures are generated. The default value is 0.
201	Switch for changing a called number in the CDR.	Enumerated value. The options are as follows: ● 0: Before change ● 1: After change The default value is 0.
202	Indicates whether the narrowband trunk plays tones on the narrowband trunk.	Enumerated value: ● 0: No ● 1: Yes The default value is 0.
203	Switch for direct-dialing through Virtual User (VU) numbers.	Enumerated value. The options are as follows: ● 0: Disable ● 1: Enable The default value is 0.
204	Switch for displaying the original caller number.	Enumerated value. The options are as follows: ● 0: Not display the original caller number ● 1: Display the original caller number The default value is 0.
205	Specifies an interval for processing a new registration request upon a SIPUE authentication failure.	The value is an integer that ranges from 0 to 300, in seconds. The default value is 10.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
206	Switch for generating local-survival bill when deactivate.	Enumerated value. The options are as follows: ● 0: Not generate. ● 1: Generate. The default value is 0.
207	Switch for generating system bill.	Enumerated value. The options are as follows: ● 0: Not generate. ● 1: Generate. The default value is 1.
208	Switch for checking voice password.	Enumerated value. The options are as follows: ● 0: Not check ● 1: Check The default value is 1. **NOTE** To secure devices, the password complexity verification function must be enabled.
209	Specifies whether to send the number when ISDN trunk group reaches the minimum number length.	Enumerated value. The options are as follows: ● 0: Not send ● 1: Send The default value is 1.
210	Switch for enabling preempted registration.	Enumerated value. The options are as follows: ● 0: Allowed ● 1: Allowed when not busy ● 2: All forbidden The default value is 1.
211	Whether to transparently transfer the number sign (#) in the called number for a trunk-based outgoing call.	Enumerated value. The options are as follows: ● 0: The number sign (#) is not transparently transferred. ● 1: The number sign (#) is transparently transferred. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
212	Path refresh timer length.	The value is an integer that ranges from 0 to 5, in seconds. The default value is 2.
213	Change sdp port when re-invite negotiation.	Enumerated value. The options are as follows: ● 0: Yes ● 1: No The default value is 0.
214	Whether restrict outgoing right by caller.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 1.
215	Caller release call duration of not offhook under called control mode.	The value is an integer that ranges from 60 to 65535, in seconds. The default value is 180.
216	Caller detects dtmf send high frequency tone duration of offhook under called control mode.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 30.
217	Send high frequency tone length under called control mode.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 2.
218	Whether to set single Pre-dial number that can trigger outgoing dial-tone.	The value is an integer that ranges from 0 to 0xFFFF. The default value is 0xFFFF (not provided).
219	Whether UAC responds to 200OK when the refresh is initiated by UAC and UAS sends the update message.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
220	Specifies whether to add cdsc in sdp when support t38 fax.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
221	Specifies whether pra trunk play ringback tone to peer.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
222	Specifies whether to check country and area code when a trunk calls out.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 1.
223	Specifies whether to play the voice tone when abnormal call.	Enumerated value. The options are as follows: ● 0: Yes ● 1: No The default value is 0.
224	Specifies whether through payload of voice when call from IP to IP	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 1.
225	Specifies whether to send 403 or 486 message when no circuit/channel available.	Enumerated value. The options are as follows: ● 0: 403 ● 1: 486 The default value is 0.
226	Specifies whether to enable DDoS attack prevention.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
227	Indicates the threshold of DDoS attack prevention.	The value is an integer that ranges from 0 to 1000, in packets per second. The default value is 20.
228	Specifies whether to refresh timer when recv alerting again.	Enumerated value. The options are as follows: ● 0: Not refresh ● 1: Refresh The default value is 1.
229	Determines whether the called party payment service is supported.	Enumerated type. The options are as follows: ● 0: The called party payment service is not supported. ● 1: The called party payment service is supported. The default value is 1.
230	Determines whether the callingnumber field is hidden in the Setup message of Dss1.	Enumerated type. The options are as follows: ● 0: The callingnumber field is not hidden in the Setup message of Dss1. ● 1: The callingnumber field is hidden in the Setup message of Dss1. The default value is 0.
231	Determines whether the R2 trunk sends the A4 message if the interim dialing timer times out on the called party side.	Enumerated type. The options are as follows: ● 0: The R2 trunk does not send the A4 message if the interim dialing timer times out on the called party side. ● 1: The R2 trunk sends the A4 message if the interim dialing timer times out on the called party side. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
232	Determines whether the DSS1 trunk listens to the ringback tones of the remote device.	Enumerated type. The options are as follows: ● 0: The DSS1 trunk does not listen to the ringback tones of the remote device. ● 1: The DSS1 trunk listens to the ringback tones of the remote device. The default value is 0.
233	Determines whether the eri-location field is in the cause field of the SIP message.	Enumerated type. The values range from 0 to 1. ● 0: The eri-location field is not in the cause field of the SIP message. ● 1: The eri-location field is in the cause field of the SIP message. The default value is 1.
234	Determines the negotiation mode of the fax in a multi-M-line scenario.	Enumerated type. The options are as follows: ● 0: T38 is used. ● 1: The transparent transmission is used. ● 2: The order is used. The default value is 2.
235	Specifies whether to convert the G.729 to G.729B when an H323 trunk is used.	Enumerated type. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
236	Indicates whether the AR or the IMS registered with the AR controls the three-party call service.	Enumerated type. The options are as follows: ● 0: AR ● 1: IMS The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
237	Indicates whether the AR or the IMS registered with the AR controls the call forwarding service.	Enumerated type. The options are as follows: ● 0: AR ● 1: IMS The default value is 0.
238	Indicates whether the AR plays call hold tones to the remote end when a user presses the hookflash.	Enumerated type. The options are as follows: ● 0: No ● 1: Yes The default value is 1.
239	Indicates the SIP message caching timeout.	The value is an integer that ranges from 0 to 2000, in milliseconds. The default value is 1000.
240	Reserved.	-
241	Reserved.	-
242	Specifies whether to enable the simplified three-party call service and call wait flow.	The value can be 0 or 1. ● 0: Disable ● 1: Enable The default value is 0. **NOTE** By default, the AR129CV, AR129CGVW-L or AR129CVW allows a maximum of one intra-office POTS user to participate in a three-party call. After the control point 242 is enabled, multiple intra-office POTS users can participate in a three-party call.
243	Specifies whether to enable an FXO interface to work in auto-answer mode.	Enumerated value. The options are as follows: ● 0: Disable ● 1: Enable The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
244	Specifies a no answering timer for an FXO interface when the FXO interface works in non-auto answering mode.	The value is an integer that ranges from 5 to 10, in seconds. The default value is 5. **NOTE** This configuration takes effect only after **pbx number-parameter 243 0** is configured.
245 **NOTE** Only the V200R010C10 and later version supports this control point.	Reserved. Configures whether to associate the status of FXS port users with the status of the bound SIP AT0 trunk.	- The default value is 0. The value is an integer. The options are as follows: ● 0: No ● 1: Yes
246	Specifies whether to enable polarity reversal on an FXS interface.	Enumerated value. The options are as follows: ● 0: Disable ● 1: Enable reversal on seizure (ROS) ● 2: Enable reversal on answer (ROA) **NOTE** ROS and ROA cannot be enabled simultaneously. The default value is 0.
247	Indicates whether the R2 trunk supports accounting pulse in the Argentina and Brazil templates.	Enumerated value. The options are as follows: ● 0: No ● 1: Yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
248	Specifies whether to enable automatic IVR two-stage dialing.	Enumerated value. The options are as follows: ● 0: Disable ● 1: Enable The default value is 0. **NOTE** ● Automatic IVR two-stage dialing requires short codes with 0 as the dialing index. If automatic IVR two-stage dialing is enabled, the system automatically forwards a call to a number with 0 as the dialing index after playing greetings. ● When automatic IVR two-stage dialing is enabled, do not dial a number while the system is playing greetings. Otherwise, the dialing takes no effect. ● Automatic IVR two-stage dialing does not support the time section index.
249	Indicates whether to replace the display header left empty in the H323 Q.931 message on the local device with the display header in the Q.931 message sent for H323 incoming calls.	The value is an integer. The options are as follows: ● 0: No ● 1: Yes The default value is 1.
250	Indicates whether to directly send an LRQ message to the called Gatekeeper after the calling Gatekeeper receives an ARQ request from the calling Gateway in the scenario where the calling Gatekeeper queries the called gateway address across regions.	The value is an integer. The options are as follows: ● 0: No ● 1: Yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
252 **NOTE** Only the V200R010C10 and later version supports this control point.	Configures whether to associate the status of the SIP AT0 trunk bound to FXS port users with the status of the LED indicator corresponding to the FXS port.	The value is an integer. The options are as follows: ● 0: No ● 1: Yes The default value is 0.
251 **NOTE** Only the V200R010C10 and later version supports this control point.	Indicates whether to use Australian standards to implement semi-consult transfer by pressing the hookflash and then 4.	The value is an integer. The options are as follows: ● 0: No ● 1: Yes The default value is 0.

Example

Enable the PBX to save CDRs.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbx number-parameter 85 1
```

16.5.1.41 prefix (call prefix view)

Function

Using the **prefix** command, you can configure a call prefix.

By default, no call prefix is configured.

Format

prefix *prefix*

Parameters

Parameter	Description	Value
prefix	Specifies the name of a call prefix.	The value is a string of 1 to 24 characters, including digits 0 to 9, asterisk (*), and number sign (#).

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set a call prefix 20000 in the view of call prefix **prefix1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix1
[Huawei-voice-prefix1] prefix 20000
```

16.5.1.42 pwdcalllimit

Function

The **pwdcalllimit** command enables or disables password call for a prefix.

By default, password call is enabled for a prefix.

Format

pwdcalllimit pwdcalllimit-*value*

Parameters

Parameter	Description	Value
pwdcalllimit-*value*	Indicates whether to enable password call.	Enumerated value. The options are as follows: ● disable ● enable

 Copyright © Huawei Technologies Co., Ltd.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

The **pwdcalllimit**-*value* command specifies whether the password is required when a user who has the password call service enabled dials a prefix.

Example

Disable password call for prefix-user1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix-user1
[Huawei-voice-callprefix-prefix-user1] pwdcalllimit disable
```

16.5.1.43 re-route (call prefix view)

Function

Using the **re-route** command, you can configure the function of rerouting upon a call failure.

Using the **undo re-route** command, you can cancel the function of rerouting upon a call failure.

Format

re-route *re-route-value*

undo re-route

Parameters

Parameter	Description	Value
re-route-value	Indicates whether to enable rerouting upon a call failure.	Enumerated value. The options are as follows: ● disable: disables rerouting upon a call failure. ● enable: enables rerouting upon a call failure. The default value is disable.

 Copyright © Huawei Technologies Co., Ltd.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

1. By default, rerouting upon failures of calls routed through the AT0 trunk is not supported. To support such type of rerouting, you need to change the value of global control point 40 to a non-0 value, for example, 2s or another appropriate value.

2. The number of line selection attempts upon a call failure is 6 (excluding the normal line selection).

3. Rerouting upon a call failure in the prefix view conflicts with that in the voice view. If rerouting upon a call failure in the prefix view is configured, rerouting upon a call failure in the voice view, if any, does not take effect.

4. With regard to rerouting upon a call failure in the prefix view, when a call fails, the trunk group will be reselected to make the call. Therefore, the intelligent routing function is affected to some extent.

5. A call is considered as a failed one when there is no non-release message from the peer after the setup message is sent or after the setup-ack is received. However, if the peer end plays announcements, the local device will consider the call as a successful one and rerouting will not be triggered. Therefore, to trigger rerouting, the peer end cannot play announcements.

Example

Configure rerouting upon a call failure in the prefix1 view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix1
[Huawei-voice-prefix1] re-route enable
```

16.5.1.44 ring-mode

Function

Using the **ring-mode** command, you can set the ring type for a PBX user.

Using the **undo ring-mode** command, you can restore the default ring type of a PBX user.

By default, the initial ring type is 4, the cadence ring type is 0, and the distinctive ring type of a SIP UE user is empty.

Format

ring-mode *index* [**init-ring** *init-ring-value* | **cadence-ring** *cadence-ring-value* | **sipue-ring-name** *sipue-ring-name-value*] *

undo ring-mode *index*

Parameters

Parameter	Description	Value
index	Specifies the index of a ring.	The value is an integer that ranges from 0 to 15.
init-ring *init-ring-value*	Specifies the initial ring type.	The value is an integer, which can be 4, 17, 18, 22, 24-26, 29-31, 144-159, or 255. The default value is 4. The options are as follows: ● 4: normal ringing (FSK) 1:4 ● 17: special ringing (FSK) 1:2 ● 18: special ringing (FSK) 0.4:0.2:0.4:4 ● 22: special ringing (FSK) 1.2:2 ● 24: HK Ring (FSK) 1:3 ● 25: HK CNTRX (FSK) 0.4:0.2:0.4:0.2:0.4:3.0 ● 26: HK DN-A (FSK) 0.4:0.2:0.4:3.0 ● 29: HK DN-B (FSK) 1.2:3 ● 30: CNTRX_IN (FSK) 0.4:0.2:0.4:0.2:0.4:2.6 ● 31: Egypt toll ringing (FSK) 2:1 ● 144-159: user-defined ringing mode (FSK) 0-15 ● 255: NULL, indicating the default ringing mode

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cadence-ring *cadence-ring-value*	Specifies the cadence ring type.	The value is an integer, which can be 0-3, 6, 8-15, 128-143, or 255. The default value is 0. The options are as follows: ● 0: normal ringing 1:4 ● 1: special ringing 1:2 ● 2: special ringing 0.4:0.2:0.4:4 ● 3: long ringing ● 6: special ringing 1.2:2 ● 8: HK Ring 1:3 ● 9: HK CNTRX 0.4:0.2:0.4:0.2:0.4:3.0 ● 10: HK DN-A 0.4:0.2:0.4:3.0 ● 11: HK ACB 0.4:0.2 ● 12: HK reminder ringing (one tone every 0.4 second; only one tone is generated.) ● 13: HK DN-B 1.2:3 ● 14: CNTRX_IN 0.4:0.2:0.4:0.2:0.4:2.6 ● 15: Egypt toll ringing 2:1 ● 128-143: user-defined ringing mode 0-15 ● 255: NULL, indicating the default ringing mode
sipue-ring-name s*ipue-ring-name-value*	Specifies the name of the differentiated ringing type of a SIP UE user. To add the Alert-info header field in an INVITE message, use this parameter. The default parameter is empty.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the initial ring type to 17, the cadence ring type to 6, and the SIP UE name to AlertInfo1 for the ringing type with the index of 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring-mode 1 init-ring 17 cadence-ring 6 sipue-ring-name AlertInfo1
```

16.5.1.45 ssl-client-policy (SIP server view)

Function

The **ssl-client-policy** command configures an SSL policy of client type when the SIP server uses TLS.

The **undo ssl-client-policy** command cancels an SSL policy of client type when the SIP server uses TLS.

By default, no SSL policy of client type is configured when the SIP server uses TLS.

Format

ssl-client-policy *server-policy-name*

undo ssl-client-policy

Parameters

Parameter	Description	Value
server-policy-name	Specifies the name of the bound SSL policy of client type when the SIP server uses TLS.	The value is a string of 1 to 31 case-insensitive characters without question marks (?) or spaces.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the AR functions as the SIP server and the security of voice signal transmission needs to be enhanced, you can run this command to configure an SSL policy of client type on the AR and configure an SSL policy of server type on the remote device. Data encryption, identity authentication, and integrity authentication mechanisms of SSL ensure data transmission security.

Prerequisites

The **ssl policy** command has been executed to create an SSL policy and specify the type of the SSL policy as client.

The **cs-mode** command has been executed in the SIP server view to configure the transmission mode of reliable connections of a SIP trunk group as client or client_server.

The **transfer** command has been executed in the SIP server view to configure the transmission mode of a trunk group as TLS.

Precautions

When the SIP server uses TLS and is bound to an SSL policy of client type, the remote device needs to be configured with an SSL policy of server type.

If you run the **ssl-client-policy** command multiple times, only the latest configuration takes effect.

The SSL policy of client type for the voice service must be exclusive. If the SSL policy of client type is used by other services such as HTTPS, the SSL policy of client type for the voice service cannot be bound.

Example

Configure an SSL policy of client type as **user1** when the SIP server uses TLS.

```
<Huawei> system-view
[Huawei] ssl policy user1 type client
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] transfer TLS
[Huawei-voice-sipserver] cs-mode client
[Huawei-voice-sipserver] ssl-client-policy user1
```

16.5.1.46 ssl-client-policy (trunk group view)

Function

The **ssl-client-policy** command configures an SSL policy of client type when a trunk group uses TLS.

The **undo ssl-client-policy** command cancels an SSL policy of client type when a trunk group uses TLS.

 Copyright © Huawei Technologies Co., Ltd.

By default, no SSL policy of client type is configured when a trunk group uses TLS.

Format

ssl-client-policy *server-policy-name*

undo ssl-client-policy

Parameters

Parameter	Description	Value
server-policy-name	Specifies the name of the bound SSL policy of client type when a trunk group uses TLS.	The value is a string of 1 to 31 case-insensitive characters without question marks (?) or spaces.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the AR functions as the client and the security of voice signal transmission needs to be enhanced, you can run this command to configure an SSL policy of client type on the AR and configure an SSL policy of server type on the remote device. Data encryption, identity authentication, and integrity authentication mechanisms of SSL ensure data transmission security.

Prerequisites

The **ssl policy** command has been executed to create an SSL policy and specify the type of the SSL policy as client.

The **cs-mode** command has been executed in the trunk group view to configure the transmission mode of reliable connections of a SIP trunk group as client or client_server.

The **transfer** command has been executed in the trunk group view to configure the transmission mode of a trunk group as TLS.

Precautions

When a trunk group uses TLS and is bound to an SSL policy of client type, the remote device needs to be configured with an SSL policy of server type.

If you run the **ssl-client-policy** command multiple times, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

The SSL policy of client type for the voice service must be exclusive. If the SSL policy of client type is used by other services such as HTTPS, the SSL policy of client type for the voice service cannot be bound.

Example

Configure an SSL policy of client type as **user1** when a trunk group uses TLS.

```
<Huawei> system-view
[Huawei] ssl policy user1 type client
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] transfer TLS
[Huawei-voice-trunkgroup-test] cs-mode client
[Huawei-voice-trunkgroup-test] ssl-client-policy user1
```

16.5.1.47 ssl-server-policy (SIP server view)

Function

The **ssl-server-policy** command configures an SSL policy of server type when the SIP server uses TLS.

The **undo ssl-server-policy** command cancels an SSL policy of server type when the SIP server uses TLS.

By default, no SSL policy of server type is configured when the SIP server uses TLS.

Format

ssl-server-policy *server-policy-name*

undo ssl-server-policy

Parameters

Parameter	Description	Value
server-policy-name	Specifies the name of the bound SSL policy of server type when the SIP server uses TLS.	The value is a string of 1 to 31 case-insensitive characters without question marks (?) or spaces.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the AR functions as the SIP server and the security of voice signal transmission needs to be enhanced, you can run this command to configure an SSL policy of server type on the AR and configure an SSL policy of client type on the remote device. Data encryption, identity authentication, and integrity authentication mechanisms of SSL ensure data transmission security.

Prerequisites

The **ssl policy** command has been executed to create an SSL policy and specify the type of the SSL policy as server.

The **cs-mode** command has been executed in the SIP server view to configure the transmission mode of reliable connections of a SIP trunk group as server or client_server.

The **transfer** command has been executed in the SIP server view to configure the transmission mode of a trunk group as TLS.

Precautions

When the SIP server uses TLS and is bound to an SSL policy of server type, the remote device needs to be configured with an SSL policy of client type.

If you run the **ssl-server-policy** command multiple times, only the latest configuration takes effect.

The SSL policy of server type for the voice service must be exclusive. If the SSL policy of server type is used by other services such as HTTPS, the SSL policy of server type for the voice service cannot be bound.

Example

Configure an SSL policy of server type as **user1** when the SIP server uses TLS.

```
<Huawei> system-view
[Huawei] ssl policy user1 type server
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] transfer TLS
[Huawei-voice-sipserver] cs-mode server
[Huawei-voice-sipserver] ssl-server-policy user1
```

16.5.1.48 ssl-server-policy (trunk group view)

Function

The **ssl-server-policy** command configures an SSL policy of server type when a trunk group uses TLS.

The **undo ssl-server-policy** command cancels an SSL policy of server type when a trunk group uses TLS.

By default, no SSL policy of server type is configured when a trunk group uses TLS.

 Copyright © Huawei Technologies Co., Ltd.

Format

ssl-server-policy *server-policy-name*

undo ssl-server-policy

Parameters

Parameter	Description	Value
server-policy-name	Specifies the name of the bound SSL policy of server type when a trunk group uses TLS.	The value is a string of 1 to 31 case-insensitive characters without question marks (?) or spaces.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the AR functions as the server and the security of voice signal transmission needs to be enhanced, you can run this command to configure an SSL policy of server type on the AR and configure an SSL policy of client type on the remote device. Data encryption, identity authentication, and integrity authentication mechanisms of SSL ensure data transmission security.

Prerequisites

The **ssl policy** command has been executed to create an SSL policy and specify the type of the SSL policy as server.

The **cs-mode** command has been executed in the trunk group view to configure the transmission mode of reliable connections of a SIP trunk group as server or client_server.

The **transfer** command has been executed in the trunk group view to configure the transmission mode of a SIP trunk group as TLS.

Precautions

When a trunk group uses TLS and is bound to an SSL policy of server type, the remote device needs to be configured with an SSL policy of client type.

If you run the **ssl-server-policy** command multiple times, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

The SSL policy of server type for the voice service must be exclusive. If the SSL policy of server type is used by other services such as HTTPS, the SSL policy of server type for the voice service cannot be bound.

Example

Configure an SSL policy of server type as **user1** when a trunk group uses TLS.

```
<Huawei> system-view
[Huawei] ssl policy user1 type server
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] transfer TLS
[Huawei-voice-trunkgroup-test] cs-mode server
[Huawei-voice-trunkgroup-test] ssl-server-policy user1
```

16.5.1.49 special-deal

Function

The **special-deal** command configure number conversion for a prefix.

The **undo special-deal** command is used to delete number conversion for a prefix.

By default, number conversion is disabled for a prefix.

Format

special-deal { **long-caller** *long-cli-flag* | **caller-map** *cli-map-flag* | **called-map** *cld-map-flag* }*

undo special-deal { **long-caller** | **caller-map** | **called-map** }

Parameters

Parameter	Description	Value
long-cli-flag	long number conversion flag.	Enumerated type. The options are as follows: ● enable ● disable default:disable
cli-map-flag	caller map conversion flag.	Enumerated type. The options are as follows: ● enable ● disable default:disable

Parameter	Description	Value
cld-map-flag	called map conversion flag.	Enumerated type. The options are as follows: ● enable ● disable default:disable

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

If a telephone number and a long number are both configured for a user, long number conversion can be enabled for a prefix.

If you run the command several times, the latest configuration takes effect.

Example

Enable long number conversion in call prefix view **prefix-user1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix-user1
[Huawei-voice-callprefix-prefix-user1] special-deal long-caller enable
```

16.5.1.50 time

Function

The **time** command configures a time template.

The **undo time** command deletes a time template.

Format

time *time-name* { **time-period** { **from** *from-date* [*from-time*] | **to** *to-date* [*to-time*] } | **time-repeat** { { **yearly** | **monthly** } *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] } }

undo time *time-name*

Parameters

Parameter	Description	Value
time-name	Specifies the time name.	The value is a string of 1 to 32 characters.
time-period	Specifies the validity period.	-
from *from-date*	Specifies the validity date.	The value is in yyyy-mm-dd format.
from-time	Specifies the validity time.	The value is in hh:mm:ss format.
to *to-date*	Specifies the expiration date.	The value is in yyyy-mm-dd format.
to-time	Specifies the expiration time.	The value is in hh:mm:ss format.
time-repeat	Indicates the repeat mode.	-
yearly	Indicates the configuration takes effect every year.	-
monthly	Indicates the configuration takes effect every month.	-
begin-date	Specifies the start date of the validity period.	The value is in mm-dd or dd format.
begin-time	Specifies the start time of the validity period.	The value is in hh:mm:ss format.
end-date	Specifies the end date of the validity period.	The value is in mm-dd or dd format.
end-time	Specifies the end time of the validity period.	The value is in hh:mm:ss format.
weekly	Indicates the configuration takes effect every week.	-
begin-weekday	Specifies the start weekday.	Enumerated value. The value can be Mon, Tue, Wed, Thu, Fri, Sat, or Sun .

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-weekday	Specifies the end weekday.	Enumerated value. The value can be Mon, Tue, Wed, Thu, Fri, Sat, or Sun.
begin-time	Specifies the start time.	The value is in hh:mm:ss format.
end-time	Specifies the end time.	The value is in hh:mm:ss format.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure a time template that specifies a time range from 10:00:00 to 11:00:00 every day.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] time test time-repeat daily 10:00:00 11:00:00
```

16.5.1.51 tone-set

Function

The **tone-set** command configures the call block tone mapping.

The **undo tone-set** command deletes the mapping relationship.

By default, call block uses a tone based on the failure cause. After the **tone-set** command is executed, call block uses the tone specified by the command.

Format

tone-set type *type-value* **toneid** *toneid-value*

undo tone-set type [*type-value*]

Parameters

Parameter	Description	Value
type *type-value*	Specifies the status.	Enumerated type. Options: busy, no_answer, offline, dnerror, no_right, and unreachable
toneid *toneid-value*	Specifies the tone ID.	Integer type. Value range: 1-566

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When a call is unexpectedly released upon a call setup failure, the system plays a tone corresponding to the release cause according to the configured mapping relationship.

Example

Configure mapping between the busy state and tone ID 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tone-set type busy toneid 2
```

16.5.1.52 user-account(account-set view)

Function

The **user-account** command configures an **account** and password of the account-set in account mode.

The **undo user-account** command deletes the account and password of the account-set.

By default, no **account** is configured.

Format

user-account *user-account-name* **password cipher** *password-value*

Parameters

Parameter	Description	Value
user-account-name	Specifies the account name.	The value is a string of 1 to 12 digits without spaces.
password-value	Specifies the password for account.	The value is a string of 6 to 8 digits without spaces.

Views

account-set view

Default Level

2: Configuration level

Usage Guidelines

To configures an account and password of the account-set in account mode, run **user-account** command.

Example

Configure an account named 1001 and password 12345678 for account-set 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]account-set 1 account     [Huawei-voice-account-set-1]user-account 1001 password cipher
Please input user password(6-8 chars):********
```

16.5.1.53 use-account-set (disa view)

Function

The **use-account-set** command binds an account-set for disa.

Format

use-account-set *account-set-name*

Parameters

Parameter	Description	Value
account-set-name	Specifies the account-set name.	The value is a string of 1 to 32 characters without spaces.

Views

Disa view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Bind an account-set named 1 for disa d1.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] disa d1
 [Huawei-voice-disa-d1] use-account-set 1
```

16.5.1.54 vu-custom-right (call prefix view)

Function

The **vu-custom-right** command configures the customized 32 levels of call rights to be bound to call prefixes.

By default, a call prefix is not bound to any of the 32 levels of call rights.

Format

vu-custom-right { *c1* | *c2* | *c3* | ... | *c32* } *

undo vu-custom-right [*c1* | *c2* | *c3* | ... | *c32*] *

Parameters

Parameter	Description	Value
c1 | *c2* | *c3* | ... | *c32*	Specifies the customized 32 levels of call rights to be bound to VU prefixes.	The value can be one or more options in c1-c32.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

The 32 levels of call rights for VU prefixes limit the call rights for external users to perform two-stage dialing (automatic switchboard number+internal user's short number).

This command takes effect only on VU prefixes. 32 levels of call rights can be configured for the VU prefix and also for the VU service. The configurations do not conflict with each other.

Example

Bind c1 and c2 call rights to VU prefix 1 in the prefix1 view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix1
[Huawei-voice-prefix1] call-type category vu-service vu-service-name vudefault
[Huawei-voice-prefix1] vu-custom-right c1 c2
```

16.5.1.55 vuloopcount

Function

The **vuloopcount** command configures the loop count of the VU switchboard.

By default, the loop count of the VU switchboard is 0.

Format

vuloopcount *vuloopcount-value*

Parameters

Parameter	Description	Value
vuloopcount-value	Specifies the loop count of the VU switchboard.	The value is an integer that ranges from 0 to 6.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

If you run the **vuloopcount** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the attribute of the call prefix to VU and the loop count to 5 in the call prefix view **prefix-user1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callprefix prefix-user1
[Huawei-voice-callprefix-prefix-user1] vuloopcount 5
```

16.5.1.56 vuoutgoingright

Function

The **vuoutgoingright** command configures the call out rights of the VU switchboard.

By default, the call out rights of the VU switchboard is **inter**.

Format

vuoutgoingright { { **inter** *value* | **local** *value* | **idd** *value* | **ddd** *value* } * | **all** *value* }

Parameters

Parameter	Description	Value
value	Specifies the call out rights.	Enumerated type. The values are as follows: ● Enable: The call out rights are added. ● Disable: The call out rights are deleted.

Views

Call prefix view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the call out rights of the VU call prefix to **ddd**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] callprefix user1
[Huawei-voice-callprefix-prefix-user1] vuoutgoingright ddd enable
```

16.5.2 SIP Server Configuration Commands

16.5.2.1 codec-priority

Function

Using the **codec-priority** command, you can configure the codec priority, codec value, and packetization time for a SIP server.

Using the **undo codec-priority** command, you can restore the default settings of the codec priority, codec value, and packetization time of a SIP server.

The default values of the codec priority, codec value, and packetization time is shown in **Table 16-52**.

Format

codec-priority *pri-value codec-value pt-value*

undo codec-priority

Parameters

Parameter	Description	Value
pri-value	Indicates the codec priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
codec-value	Indicates the codec value.	Enumerated value. The value ranges from 0 to 255. The options are as follows: • 0: G711U • 2: G726 • 4: G723 • 8: G711A • 9: G722 • 15: G728 • 18: G729 • 20: G723Low • 21: G726-16 • 22: G726-24 • 23: G726-40 • 96: R2198 • 97: R2833 • 98: v150 • 99: clearmode • 250: T.38 • 251: T.38+2 • 252: wildcard ($) • 253: wildcard (*) • 254: H.246
pt-value	Indicates the packetization time.	The value is an integer that ranges from 0 to 255, in milliseconds. The valid values are 5,10, 20, 30, 40, 50, and 60.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

The default values are shown in **Table 16-52**.

Table 16-52 The default values

Codec Priority	Codec Value	Packetization Time
0	8	20
1	0	20
2	18	10
3	4	30
4	8	10
5	8	30
6	0	10
7	250	20

Example

Set the codec value to 1, codec priority to 0, and packetization time to 20 for a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] codec-priority 0 1 20
```

16.5.2.2 cs-mode (SIP server view)

Function

Using the **cs-mode** command, you can configure the reliable transmission mode for a SIP server.

By default, no reliable transmission mode is configured for a SIP server.

undo cs-mode restores the default sipserver transmission mode

Format

cs-mode *cs-mode-value*

undo cs-mode

Parameters

Parameter	Description	Value
cs-mode-value	Specifies the reliable transmission mode.	The values are as follows: ● server ● client_server

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

The reliable transmission mode is valid only when the transmission mode of the SIP server is **tcp**.

Example

Set the reliable transmission mode for the SIP server to client_server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] transfer tcp
[Huawei-voice-sipserver] cs-mode client_server
```

restore the default transmission mode for the SIP server

```
[Huawei-voice-sipserver]undo cs-mode
[Huawei-voice-sipserver]
```

16.5.2.3 ddns-client

Function

Using the **ddns-client** command, you can configure a dynamic domain name system (DDNS) name for a SIP server that uses a dynamic signaling IP address.

By default, no DDNS client name is configured for a SIP server using a dynamic signaling IP address.

Format

ddns-client *ddns-client-name*

Parameters

Parameter	Description	Value
ddns-client-name	Specifies the DDNS client name for a SIP server.	The value is a string of 1 to 64 case-insensitive characters.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

When a SIP server uses a dynamic signaling IP address, configure a DDNS client name for the SIP server so that the DDNS server can update the mapping between the signaling domain name and IP address.

Example

Set the DDNS client name to **myddns** for a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] ddns-client myddns
```

16.5.2.4 display voice sipserver

Function

The **display voice sipserver** command displays the configuration of a SIP server.

Format

display voice sipserver [*mode-name*]

Parameters

Parameter	Description	Value
mode-name	Indicates the configuration item name.	The options are as follows: ● number-parameter: parameter index. ● fax-modem: fax/modem configuration of a SIP server. ● redundancy-nte: whether a SIP server is enabled to transmit the RFC 2833 audio data using RFC 2198 redundancy transmission. ● codec-priority: codec priority, codec value, and packetization time. ● dtmf: DTMF transmission mode over RTP.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice sipserver** command displays the configuration of a SIP server.

NOTE

In the command output, if the SIP server configuration is inconsistent with the SIP server running information, the current configuration does not take effect.

Example

Display the configuration of a SIP server.

```
<Huawei> display voice sipserver
  Config
  Signalling IP                  : 192.168.0.1
  Signalling IP address name     :
  Signalling domain              : abcd.com
```

```
DDNS client name              :
Signalling port               : 5060
Media IP                      : 192.168.0.1
Media IP address name         :
Register URI                  : abcd.com
Home domain                   : abcd.com
Transfer mode                 : UDP
Signalling Proxy              : Disable
Media Proxy                   : Disable
Mapped Signalling IP          :
Mapped Signalling port        :
Mapped Media IP               :
Mapped Media Port Start       :
Mapped Media Proxy Port Start :
Register Count Per Second     : 20

Running
Status                        : Normal
Signalling IP                 : 192.168.0.1
Signalling IP address name    :
Signalling domain             :
DDNS client name              :
Signalling port               : 5060
Media IP                      : 192.168.0.1
Media IP address name         :
Register URI                  : abcd.com
Home domain                   : abcd.com
Transfer mode                 : UDP
Signalling Proxy              : Disable
Media Proxy                   : Disable
Mapped Signalling IP          :
Mapped Signalling port        :
Mapped Media IP               :
Mapped Media Port Start       :
Mapped Media Proxy Port Start :
Register Count Per Second     : 20
```

Table 16-53 Description of the display voice sipserver command output

Item	Description
Signalling IP	Signaling IP address of a SIP server. To configure the signaling IP address of a SIP server, run the **16.5.2.30 signalling-address** command.
Signalling IP address name	Name of the dynamic signaling IP address of a SIP server. To configure the name of the dynamic signaling IP address of the SIP server, run the **16.5.2.30 signalling-address** command.
Signalling domain	Signaling domain name of the dynamic DNS. To configure the signaling domain name of the dynamic DNS, run the **16.5.2.31 signalling-domain** command.
DDNS client name	DDNS client name.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Signalling port	Signaling port number of a SIP server. To configure the signaling port number of a SIP server, run the **16.5.2.30 signalling-address** command.
Media IP	Media IP address of a SIP server. To configure the media IP address of a SIP server, run the **16.5.2.17 media-ip** command.
Media IP address name	Name of the dynamic media IP address of a SIP server. To configure the name of the dynamic media IP address of a SIP server, run the **16.5.2.17 media-ip** command.
Register URI	Uniform resource identifier (URI) of a SIP server. To configure the URI of a SIP server, run the **16.5.2.27 register-uri** command.
Home domain	Home domain of a SIP server. To configure the home domain of a SIP server, run the **16.5.2.14 home-domain (SIP server view)** command.
Transfer mode	Transfer mode of a SIP server.
Signalling Proxy	Signaling proxy.
Media Proxy	Media proxy.
Mapped Signalling IP	Mapped signaling IP address.
Mapped Signalling port	Mapped signaling port.
Mapped Media IP	Mapped media IP address.
Mapped Media Port Start	Mapped media start port.
Mapped Media Proxy Port Start	Mapped media proxy start port.
Register Count Per Second	Number of registration times per second.
Status	Status of a SIP server.

 Copyright © Huawei Technologies Co., Ltd.

16.5.2.5 display voice sipserver dtmf

Function

The **display voice sipserver dtmf** command displays the Dual-Tone Multifrequency (DTMF) transmission mode over RTP.

Format

display voice sipserver dtmf

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the DTMF transmission mode over RTP.

```
<Huawei> display voice sipserver dtmf
    DTMF                : throughly
```

Table 16-54 Description of the display voice sipserver dtmf command output

Item	Description
DTMF	DTMF transmission mode over RTP. ● erase: erase mode ● throughly: transparent transmission mode To watch the DTMF transmission mode over RTP, run the **display voice sipserver dtmf** command.

 Copyright © Huawei Technologies Co., Ltd.

16.5.2.6 display voice sipserver fax-modem

Function

The **display voice sipserver fax-modem** command displays fax/modem parameters of a SIP server.

Format

display voice sipserver fax-modem

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display voice sipserver fax-modem** command displays fax/modem parameters of a SIP server, including:

- Fax/modem transmission mode
- Fax/modem codec negotiation mode
- Packetization interval in transparent transmission mode
- VBD attribute type
- VBD codec mode
- VBD payload type

Example

Display fax/modem parameters of a SIP server.

```
<Huawei> display voice sipserver fax-modem
    Fax modem fax          : T.38
    Fax modem modem        : throughly
    Fax modem negomode     : Negotiation
    RTP interval           : 10ms
    VBD attribute          : V152
    VBD codec              : G711a
    VBD payload type       : Static
```

Table 16-55 Description of the display voice sipserver fax-modem command output

Item	Description
Fax modem fax	Fax transmission mode. ● T.38: T.38 mode ● Throughly: transparent transmission mode ● To configure the fax transmission mode, run the **fax-modem fax transmission-mode** command.
Fax modem modem	Modem transmission mode. ● Relay: relay mode ● Throughly: transparent transmission mode To configure the modem transmission mode, run the **fax-modem modem transmission-mode** command.
Fax modem negomode	Fax/modem codec negotiation mode. ● Negotiate: negotiation mode ● Self-switch: self-switching mode To configure the fax/modem codec negotiation mode, run the **fax-modem common negotiation-mode** command.
RTP interval	Packetization interval in transparent transmission mode. To configure the packetization interval in transparent transmission mode, run the **fax-modem common rtp-interval** command.
VBD attribute	VBD attribute type. ● Chinatelecom: China Telecom mode ● Extchinatelecom: extended China Telecom mode ● Ietf: IETF mode ● V.152: V.152 mode To configure the VBD attribute type, run the **fax-modem common vbd-attribute-type** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VBD codec	VBD codec mode. ● G711a: G.711 A ● G711u: G.711 μ To configure the VBD codec mode, run the **fax-modem common vbd-codec** command.
VBD VBD payload type	VBD payload type. ● Dynamic: dynamic payload type ● Static: static payload type To configure the VBD payload type, run the **fax-modem common vbd-payload-type** command.

16.5.2.7 dtmf-transmission-mode

Function

Using the **dtmf-transmission-mode** command, you can configure the Dual-Tone Multifrequency (DTMF) transmission mode of RTP.

Using the **undo dtmf-transmission-mode** command, you can restore the default DTMF transmission mode of RTP.

By default, the DTMF transmission mode of RTP is transparent transmission.

Format

dtmf-transmission-mode { **erase** | **throughly** }

undo dtmf-transmission-mode

Parameters

Parameter	Description	Value
erase	Removes DTMF tones from RTP packets. This mode is used when DTMF signals are transmitted in accordance with RFC2833 and DTMF signals do not need to be transmitted.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
throughly	Specifies DTMF transparent transmission. This mode is used when DTMF signals are transmitted in accordance with RFC2833 and DTMF signals need to be transmitted.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the DTMF transmission mode to transparent transmission.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] dtmf-transmission-mode throughly
```

16.5.2.8 fax-modem common negotiation-mode

Function

Using the **fax-modem common negotiation-mode** command, you can set the codec negotiation mode of a fax machine or modem.

Using the **undo fax-modem common negotiation-mode** command, you can restore the default codec negotiation mode of a fax machine or modem.

By default, the codec negotiation mode of a fax machine or modem is negotiation.

Format

fax-modem common negotiation-mode { **negotiate** | **self-switch** }

undo fax-modem common negotiation-mode

Parameters

Parameter	Description	Value
negotiate	Indicates that the codec negotiation mode of a fax machine or modem is negotiation. In this mode, the MG needs to negotiate with the MGC through signaling for the codec negotiation mode.	-
self-switch	Indicates that the codec negotiation mode of a fax machine or modem is self-switch.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the codec negotiation mode of a fax machine or modem to negotiation.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] fax-modem common negotiation-mode negotiate
```

16.5.2.9 fax-modem common rtp-interval

Function

Using the **fax-modem common rtp-interval** command, you can set the packetization interval in transparent transmission mode.

Using the **undo fax-modem common rtp-interval** command, you can restore the default packetization interval in transparent transmission mode.

By default, the packetization interval in transparent transmission mode is 10 ms.

 Copyright © Huawei Technologies Co., Ltd.

Format

fax-modem common rtp-interval { **5ms** | **10ms** | **20ms** | **30ms** |**40ms** }

undo fax-modem common rtp-interval

Parameters

None

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

After the **fax-modem modem transmission-mode** command sets the modem transparent transmission mode or the **fax-modem fax transmission-mode** command sets the fax transparent transmission mode, run the **fax-modem common rtp-interval** command to change the packetization interval.

Example

Set the packetization interval in transparent transmission mode to 5 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] fax-modem common rtp-interval 5ms
```

16.5.2.10 fax-modem common vbd-attribute-type

Function

Using the **fax-modem common vbd-attribute-type** command, you can set the attribute type of the voice-band data (VBD).

Using the **undo fax-modem common vbd-attribute-type** command, you can restore the default attribute type of the VBD.

By default, the attribute type of the VBD is v152.

Format

fax-modem common vbd-attribute-type { **chinatelecom** | **extchinatelecom** | **ietf** | **v152** }

undo fax-modem common vbd-attribute-type

Parameters

Parameter	Description	Value
chinatelecom	Indicates the China Telecom mode.	-
extchinatelecom	Indicates the extended China Telecom mode.	-
ietf	Indicates the IETF mode.	-
v152	Indicates the v.152 mode.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the VBD attribute type to IETF.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] fax-modem common vbd-attribute-type ietf
```

16.5.2.11 fax-modem common vbd-codec

Function

Using the **fax-modem common vbd-codec** command, you can set the codec mode of the VBD.

Using the **undo fax-modem common vbd-codec** command, you can restore the default codec mode of the VBD.

By default, the codec mode of the VBD is A-law algorithm in G.711.

Format

fax-modem common vbd-codec {**g711a** | **g711u** | **g711a_u** | **g711u_a**}

undo fax-modem common vbd-codec

Parameters

Parameter	Description	Value
g711a	Indicates the A-law algorithm in G.711.	-
g711u	Indicates the u-law algorithm in G.711.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the codec mode of the VBD to u-law algorithm in G.711.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] fax-modem common vbd-codec g711u
```

16.5.2.12 fax-modem common vbd-payload-type

Function

Using the **fax-modem common vbd-payload-type** command, you can configure the payload type of the VBD.

Using the **undo fax-modem common vbd-payload-type** command, you can restore the default payload type of the VBD.

By default, the payload type of the VBD is static.

Format

fax-modem common vbd-payload-type { **dynamic** | **static** }

undo fax-modem common vbd-payload-type

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dynamic	Indicates dynamic payload.	-
static	Indicates static payload.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure dynamic payload.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] fax-modem common vbd-payload-type dynamic
```

16.5.2.13 fax-modem fax transmission-mode

Function

Using the **fax-modem fax transmission-mode** command, you can configure the fax transmission mode.

Using the **undo fax-modem fax transmission-mode** command, you can restore the default fax transmission mode.

By default, the fax transmission mode is transparent transmission.

Format

fax-modem fax transmission-mode { **T38** | **throughly** | **T38_throughly** | **throughly_T38** }

undo fax-modem fax transmission-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
T38	Indicates the T.38 mode. The T.38 mode is the fax-dedicated coding mode.	-
throughly	Indicates the transparent transmission mode. The transparent transmission mode uses the coding mode of G.711.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the fax transmission mode to transparent transmission.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] fax-modem fax transmission-mode throughly
```

16.5.2.14 home-domain (SIP server view)

Function

Using the **home-domain** command, you can configure a home domain that a SIP server belongs to.

By default, no home domain is configured.

Format

home-domain *domain*

Parameters

Parameter	Description	Value
domain	Specifies a home domain.	The value is a string of 1 to 64 characters that start with a letter or a numeral and consist of letters, numerals, and decimal points (.).

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure a home domain **ippbx** that a SIP server belongs to.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] home-domain ippbx
```

16.5.2.15 media-bandwidth-control (SIP server view)

Function

The **media-bandwidth-control** command enables CAC on the SIP server.

The **undo media-bandwidth-control {** max-bandwidth **|** media-proxy **}** command disables CAC on the SIP server.

By default, CAC is disabled on the SIP server.

Format

media-bandwidth-control { ***enable*** **|** ***disable*** **|** ***max-bandwidth*** **|** ***media-proxy*** **}**

undo media-bandwidth-control { ***max-bandwidth*** **|** ***media-proxy*** **}**

Parameters

None

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a SIP UE user calls a local POTS user, the media bandwidth of the SIP server is occupied. However, the media bandwidth of the SIP server is limited. To improve the voice communication quality, run the **media-bandwidth-control enable** command to enable CAC on the SIP server.

NOTE

- When a SIP UE user registered to the SIP server through the SBC proxy calls a locally-registered SIP UE user, the media bandwidth of both the SBC proxy and the SIP server is occupied.
- When two locally-registered SIP UE users communicate with each other, the media bandwidth on the SIP server is not occupied. When a locally-registered SIP UE user communicates with a POTS user, the media bandwidth on the SIP server is occupied.

Follow-up Procedure

Run the **16.5.2.15 media-bandwidth-control (SIP server view)** command to set the maximum uplink media bandwidth of voice data on the SIP server.

Example

Enable CAC on the SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] media-bandwidth-control enable
```

16.5.2.16 media-bandwidth-control max-bandwidth (SIP server view)

Function

The **media-bandwidth-control max-bandwidth** command sets the maximum uplink media bandwidth of voice data on a SIP server.

The **undo media-bandwidth-control max-bandwidth** command restores the maximum uplink media bandwidth of voice data on a SIP server to the default value.

By default, the maximum uplink media bandwidth of voice data on a SIP server is 500000 kbit/s.

Format

media-bandwidth-control max-bandwidth *max-bandwidth-value*

undo media-bandwidth-control max-bandwidth

Parameters

Parameter	Description	Value
max-bandwidth-value	Specifies the maximum media bandwidth on a SIP server.	The value is an integer that ranges from 1 to 5000, in 100 kbit/s. The default value is 5000, that is, 500000 kbit/s.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After CAC is enabled on the SIP server by running the media-bandwidth-control enable (SIP server view) command, run the **media-bandwidth-control max-bandwidth** command to specify the maximum media bandwidth of voice data on the SIP server. If the **media-bandwidth-control max-bandwidth** command is not run and CAC is enabled on the SIP server, the maximum uplink bandwidth is 500000 kbit/s. When the bandwidth is used up on the SIP server, new calls that occupy bandwidth on the SIP server are restricted.

NOTE

- When a SIP UE user registered to the SIP server through the SBC proxy calls a locally-registered SIP UE user, the media bandwidth of both the SBC proxy and the SIP server is occupied.
- When two locally-registered SIP UE users communicate with each other, the media bandwidth on the SIP server is not occupied. When a locally-registered SIP UE user communicates with a POTS user, the media bandwidth on the SIP server is occupied.

Prerequisites

CAC has been enabled on the SIP server using the media-bandwidth-control enable (SIP server view) command.

Example

Set the maximum media bandwidth on the SIP server to 400000 kbit/s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] media-bandwidth-control enable
[Huawei-voice-sipserver] media-bandwidth-control max-bandwidth 4000
```

16.5.2.17 media-ip

Function

Using the **media-ip** command, you can configure a media IP address or a dynamic media IP address name for a SIP server.

By default, no media IP address or dynamic media IP address name is configured for a SIP server.

Format

media-ip { *ip-address* | **addr-name** *addr-name-value* }

Parameters

Parameter	Description	Value
ip-address	Specifies a media IP address.	The value is in dotted decimal notation.
addr-name *addr-name-value*	Specifies a dynamic media IP address name.	The value is a string of 1 to 64 case-insensitive characters.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Before specifying the media IP address for a SIP server, create a media IP address or a dynamic media IP address name.

Example

Configure a media IP address 192.168.0.2 for a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] media-ip 192.168.0.2
```

16.5.2.18 nte-fax-modem

Function

Using the **nte-fax-modem** command, you can enable fax and modem event transmission in accordance with RFC 2833 or disable this function.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo nte-fax-modem** command, you can cancel the configuration.

By default, fax and modem event transmission in accordance with RFC 2833 is enabled.

Format

nte-fax-modem { enable | disable }

undo nte-fax-modem

Parameters

None

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable fax and modem event transmission in accordance with RFC 2833.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] nte-fax-modem enable
```

16.5.2.19 nte-negotiation-mode

Function

Using the **nte-negotiation-mode** command, you can configure the mode in which RFC 2833 redundancy transmission is started based on negotiation.

Using the **undo nte-negotiation-mode** command, you can restore the default mode in which RFC 2833 redundancy transmission is started based on negotiation.

By default, RFC 2833 redundancy transmission is started based on negotiation in **no-initiative-start** mode.

Format

nte-negotiation-mode { **fixed-start** | **negotiation** | **no-initiative-start** }

undo nte-negotiation-mode

Parameters

Parameter	Description	Value
fixed-start	Indicates the fixed startup mode. In fixed startup mode, the local end does not initiate any negotiation but accepts the initiated negotiation. If the negotiation fails, RFC 2833 redundancy transmission is started based on the local configuration.	-
negotiation	Indicates the initiative startup mode. In initiative startup mode, RFC 2833 redundancy transmission starts only after the negotiation between the local end and remote end succeeds. The negotiation may be initiated by the local end or remote end.	-
no-initiative-start	Indicates the no-initiative startup mode. In no-initiative startup mode, RFC 2833 transmission starts only after the local end receives the negotiation invitation from the remote end. If the negotiation fails, RFC 2833 redundancy transmission is not started.	-

Views

SIP server view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Set the mode in which RFC 2833 redundancy transmission is started based on negotiation to **fixedstart**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] nte-negotiation-mode fixed-start
```

16.5.2.20 number-parameter (SIP server view)

Function

The **number-parameter** command configures control points for a SIP server.

The **undo number-parameter** command restores the default control point settings of a SIP server.

Format

number-parameter *name value*

undo number-parameter *name*

Parameters

Parameter	Description	Value
name	Specifies the name of a control point.	The value is an integer that ranges from 0 to 56.
value	Specifies the value of a control point.	The value is an integer, the value of *value* varies according to *name*. For details, see the **Table 16-56**.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

You can run the **number-parameter** command to change values of control points to configure functions of a SIP server as required. For example, you can specify the

registration lifecycle, modify the minimum message waiting indicator (MWI) subscription timeout duration, and specify whether the registration subscription function is enabled. **Table 16-56** describes the control point names and values.

Table 16-56 Description of control point names and values

Control Point Name	Description	Value
0	Sets the registration lifecycle.	The value is an integer that ranges from 60 to 65534, in seconds. The default value is 600.
1	Specifies the header field from which the calling number is obtained for the SIP Server.	Integer type. The options are as follows: ● 0: The calling number is obtained from the P-asserted-Identity header field. ● 1: The calling number is obtained from the From header field. The default value is 0.
2	Sets event values added to the AllowEvent header field.	The value is an integer that ranges from 0 to 22. The default value is 18.
3	Configures whether SIP messages contain the Date header field.	Integer type. The options are as follows: ● 0: SIP messages do not contain the Data header field. ● 1: SIP messages contain the Date header field. The default value is 0.
4	Configures whether to support event values.	The value is an integer that ranges from 0 to 4294967295. The default value is 1039.
5	Sets the format of the From header field.	Integer type. The options are as follows: ● 1: SIP URI. ● 2: Phone number. ● 3: Private ID. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
6	Configures whether SDP-Answer field value in a received 18X message can be overwritten by the SDP-Answer field value in next received 18X message.	Integer type. The options are as follows: ● 0: No. ● 1: Yes. The default value is 0.
7	Configures whether SDP-Answer field value in a received 200 message can be overwritten by the SDP-Answer field value in next received 200 message.	Integer type. The options are as follows: ● 0: No. ● 1: Yes. The default value is 0.
8	Configures whether to convert the pound key (#) to %23.	Integer type. The options are as follows: ● 0: Does not convert the pound key (#) to %23 if the received SIP message contains the userphone field. ● 1: Converts the pound key (#) to %23 if the received SIP message contains the userphone field. ● 2: Does not convert the pound key (#) to %23 regardless of whether the received SIP message contains the userphone field. The default value is 0.
9	Configures whether to send a Cancel message when canceling a session.	Integer type. The options are as follows: ● 0: No. ● 1: Yes. The default value is 0.
10	Configures whether to enable the serial message sending function.	Integer type. The options are as follows: ● 0: No. ● 1: Yes. The default value is 0.
11	Reserved.	Reserved.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
12	Specifies the SIP overlap sending mode.	Integer type. The options are as follows: ● 0: A phone number is sent as a whole. ● 1: A phone number is sent digit by digit. The default value is 1.
13	Sets the format of the To header field.	Integer type. The options are as follows: ● 1: The To header field is in user name@domain name format. ● 2: The To header field is in phone number format. ● 3: The To header field is in URI format. The default value is 1.
14	Sets the session timer value.	The value is an integer that ranges from 90 to 86400, in seconds. The default value is 1800.
15	Configures whether the PBX stops playing the early media and starts to play the local ring back tone when receiving a SIP 180 message if the PBX has received a SIP 183 message with an SDP field before.	Integer type. The options are as follows: ● 0: Continues playing the early media. ● 1: Stops playing the early media and starts to play the local ring back tone. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
16	Configures a temporary response policy used when the PBX is the called party.	Integer type. The options are as follows: ● 0: The ring back tone SDP information is contained in 180 messages. ● 1: The ring back tone SDP information is contained in 183 messages. ● 2: The PBX sends a SIP 180 message after a SIP 183 message. The default value is 0.
17	Sets the SDP field value in a message that the PBX sends to trigger a flash-hooking action.	Integer type. The options are as follows: ● 0: SendOnly. ● 1: SendRecv. ● 2: Inactive. The default value is 1.
18	Sets the header field that indicates a call forwarding event of a SIPUE user.	Integer type. The options are as follows: ● 0: History-info header field. ● 1: Diversion header field. The default value is 0.
19	Configures whether to create a new socket when a PBX IP trunk (or trunk group) receives a 302 message.	Integer type. The options are as follows: ● 0: Does not create a new socket when a PBX IP trunk (or trunk group) receives a 302 message. ● 1: Creates a new socket when a PBX IP trunk (or trunk group) receives a 302 message. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
20	Sets the maximum number of dynamic TLS connections.	The value is an integer that ranges from 0 to 0xFFFFFFFE. The default value is 0xFFFFFFFF, indicating that the number of dynamic TLS connections is not limited.
21	Sets the return code for call attempts.	Integer type. The options are as follows: ● 0: Returns 486 when the called user is busy. ● 1: Returns 200 when the called user is busy. The default value is 0.
22	Configures whether to use the global codec priority or SIP server codec priority.	Integer type. The options are as follows: ● 0: Uses the global codec priority. ● 1: Uses the codec priority configured on the SIP server. The default value is 0.
23	Reserved.	Reserved.
24	Configures whether to initiate G729B negotiation.	Integer type. The options are as follows: ● 0: The local PBX does not initiate a G729B negotiation. ● 1: The local PBX can initiate a G729B negotiation. The default value is 0.
25	Configures whether to send the P-EARLY-MEDIA header field.	Integer type. The options are as follows: ● 0: Does not send the P-EARLY-MEDIA header field. ● 1: Sends the P-EARLY-MEDIA header field. The default value is 0.
26	Reserved.	Reserved.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
27	Configures whether to wait for the 200 message with SDP in unreliable 180 negotiation.	Integer type. The options are as follows: ● 0: No. ● 1: Yes. The default value is 1.
28	Sets the flag for the device to update the session.	Integer type. The options are as follows: ● 0: The flag is not included. ● 1: UAC. ● 2: UAS. The default value is 0.
29	Configures whether to initiate VBD negotiation when there a delay in processing modem events. **NOTE** To set the delay in processing modem events, run the **16.5.1.40 pbx number-parameter 5 1** command.	Integer type. The options are as follows: ● 0: VBD negotiation is not initiated. ● 1: VBD negotiation is initiated. The default value is 1.
30	Reserved.	Reserved.
31	Specifies whether clear 100rel of 18X.	Integer type. The options are as follows: ● 0: Not clear. ● 1: Clear. The default value is 0.
32	Specifies whether the From, To, and Request-Uri header fields in the INVITE message carry the registration IP address or domain name.	Integer type. The options are as follows: ● 0: Domain name. ● 1: Registration IP address. The default value is 0. **NOTE** For the 'To' field, groupreg's domain has precedence over sip server's.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
33	Specifies whether to check **home-domain** and **register-uri** values for user registration.	Integer type. The options are as follows: ● 0: No. ● 1: Yes. The default value is 1.
34	Specifies the threshold of INVITE message–based call barring.	The value is an integer that ranges from 0 to 1000, in packets per second. The default value is 30.
35 to 49	Reserved.	Reserved.
50	Specifies to listen tone or send status code.	Integer type. The options are as follows: ● 0: Listen tone. ● 1: Send status code. The default value is 0.
51	Subscriber min-expire for callinfo (In Advanced Secretary Service) and message summary (Leavemsg lights operation) events.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 60.
52	Specifies whether to enable the SIPUE overlap dialnum.	Integer type. The options are as follows: ● 0: Disable. ● 1: Enable. The default value is 0.
53	Specifies whether to perform user-agent authentication.	Integer type. The options are as follows: ● 0: Do not perform the authentication. ● 1: Perform the authentication. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Control Point Name	Description	Value
54	Specifies whether the destination port in a registration response is obtained from the Contact header field.	Integer type. The options are as follows: ● 0: The destination port in a registration response is obtained through UDP. ● 1: The destination port in a registration response is obtained from the Contact header field. The default value is 0.
55	Specifies whether the destination address in a call message is obtained from the Contact header field.	Integer type. The options are as follows: ● 0: No. ● 1: Yes. The default value is 1.
56	Specifies whether registration status subscription is supported.	Integer type. The options are as follows: ● 0: indicates that this function is not supported. ● 1: indicates that this function is supported. The default value is 0.

Example

Set the SIP registration lifecycle to 60s in the SIP server view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] number-parameter 0 60
```

16.5.2.21 qos stream (SIP server view)

Function

Using the **qos stream** command, you can set the priority of voice packets during transmission.

Using the **undo qos stream** command, you can delete the DSCP parameter in media and signaling packets.

Format

qos stream { **media** | **signaling** } **dscp** *dscp-value*

undo qos stream [**media | signaling**]

Parameters

Parameter	Description	Value
media	Specifies the priority of the media packets to be transmitted.	-
signaling	Specifies the priority of the signaling packets to be transmitted.	-
dscp-value	Specifies the priority of the voice packets to be transmitted.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

When the network quality is poor, this command can be used to specify a higher priority for voice packets to ensure the voice quality.

Example

Set the priority of media packets to 0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] qos stream media dscp 0
```

16.5.2.22 redundancy-negotiation-mode

Function

Using the **redundancy-negotiation-mode** command, you can configure the mode in which RFC 2198 redundancy transmission is started based on negotiation.

Using the **undo redundancy-negotiation-mode** command, you can restore the default mode in which RFC 2198 redundancy transmission is started based on negotiation.

By default, RFC 2198 redundancy transmission is started based on negotiation in **no-initiative-start** mode.

Format

redundancy-negotiation-mode { **fixed-start** | **negotiation** | **no-initiative-start** }

undo redundancy-negotiation-mode

Parameters

Parameter	Description	Value
fixed-start	Indicates the fixed startup mode. In fixed startup mode, the local end does not initiate any negotiation but accepts the initiated negotiation. If the negotiation fails, RFC 2198 redundancy transmission is started based on the local configuration.	-
negotiation	Indicates the initiative startup mode. In initiative startup mode, RFC 2198 redundancy transmission starts only after the negotiation between the local end and remote end succeeds. The negotiation may be initiated by the local end or remote end.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-initiative-start	Indicates the no-initiative startup mode. In no-initiative startup mode, RFC 2198 transmission starts only after the local end receives the negotiation invitation from the remote end. If the negotiation fails, RFC 2198 redundancy transmission is not started.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the mode in which RFC 2198 redundancy transmission is started based on negotiation to **fixedstart**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] redundancy-negotiation-mode fixed-start
```

16.5.2.23 redundancy-nte

Function

Using the **redundancy-nte** command, you can enable a SIP server to use RFC 2198 redundancy transmission to transmit the RFC 2833 audio data or disable this function.

Using the **undo redundancy-nte** command, you can cancel the configuration.

By default, a SIP server is disabled from using RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.

 Copyright © Huawei Technologies Co., Ltd.

Format

redundancy-nte { **enable** | **disable** }

undo redundancy-nte

Parameters

Parameter	Description	Value
enable	Enable a SIP server to use RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.	-
disable	Disable a SIP server to use RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable a SIP server to use RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] redundancy-nte enable
```

16.5.2.24 redundancy-start-mode

Function

Using the **redundancy-start-mode** command, you can configure the mode in which RFC 2198 redundancy transmission is started.

Using the **undo redundancy-start-mode** command, you can restore the default mode in which RFC 2198 redundancy transmission is started.

By default, RFC 2198 redundancy transmission is started in ordinary startup mode.

Format

redundancy-start-mode { **ordinary2198** | **smart2198** }

undo redundancy-start-mode

Parameters

Parameter	Description	Value
ordinary2198	Indicates the ordinary startup mode.	-
smart2198	Indicates the smart startup mode. In smart startup mode, RFC 2198 redundancy transmission is started automatically when packet loss occurs.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the mode in which RFC 2198 redundancy transmission is started to the smart startup mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] redundancy-start-mode smart2198
```

16.5.2.25 redundancy-vbd

Function

Using the **redundancy-vbd** command, you can enable a SIP server to use RFC 2198 redundancy transmission to transmit VBD or disable this function.

Using the **undo redundancy-vbd** command, you can cancel the configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, a SIP server is enabled to use RFC 2198 redundancy transmission to transmit VBD.

Format

redundancy-vbd enable

undo redundancy-vbd

Parameters

None

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable a SIP server to use RFC 2198 redundancy transmission to transmit VBD.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] redundancy-vbd enable
```

16.5.2.26 reg-count-per-second

Function

The **reg-count-per-second** command configures the number of registration times per second allowed by a SIP server.

The **undo reg-count-per-second** command restores the default number of registration times per second allowed by a SIP server.

By default, the number of registration times per second is 2.5 times of the CAPS.

Format

reg-count-per-second *count*

undo reg-count-per-second

Parameters

Parameter	Description	Value
count	Specifies the number of registration times per second allowed by a SIP server.	The value is an unsigned integer that ranges from 1 to 1024.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number of registration times per second allowed by a SIP server to 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] reg-count-per-second 100
```

16.5.2.27 register-uri

Function

Using the **register-uri** command, you can set the uniform resource identifier (URI) of a SIP server.

By default, no URI of the SIP server is configured.

Format

register-uri *uri*

Parameters

Parameter	Description	Value
uri	Specifies the URI of a SIP server.	The value is a string of 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the URI of the SIP server to **abcd.com**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] register-uri abcd.com
```

16.5.2.28 reset (SIP server view)

Function

Using the **reset** command, you can reset a SIP server.

Format

reset

Parameters

None

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

The SIP server will be reset after you run the **reset** command. Exercise caution when you run this command.

Example

Reset the SIP server.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] sipserver
[Huawei-voice-sipserver] reset
```

16.5.2.29 shutdown (SIP server view)

Function

Using the **shutdown** command, you can shut down a SIP server.

Format

shutdown

Parameters

None

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Shut down a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] shutdown
```

16.5.2.30 signalling-address

Function

The **signalling-address** command configures a signaling IP address and a signaling port number for a SIP server.

By default, no signaling IP address or signaling port number is configured.

Format

signalling-address { **ip** *ip-address* | **addr-name** *addr-name-value* } **port** *port-value*

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies a signaling IP address.	The value is in dotted decimal notation.
addr-name *addr-name-value*	Specifies a dynamic signaling IP address name.	The value is a string of 1 to 64 case-insensitive characters.
port *port-value*	Indicates the signaling port number of a SIP server.	The value is an integer that ranges from 5000 to 5999.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Before specifying the signaling IP address for a SIP server, create a signaling IP address or a dynamic signaling IP address name.

Example

Configure a signaling IP address 192.168.0.2 and a signaling port number 5000 for a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-address  ip 192.168.0.2 port 5000
```

16.5.2.31 signalling-domain

Function

Using the **signalling-domain** command, you can configure a signaling domain name for a SIP server that uses a dynamic signaling IP address.

By default, no signaling domain name is configured for a SIP server using a dynamic signaling IP address.

Format

signalling-domain *signalling-domain-value*

Parameters

Parameter	Description	Value
signalling-domain-value	Specifies a signaling domain name.	The value is a string of 1 to 64 characters.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

When a SIP server uses a dynamic signaling IP address, configure a signaling domain name for the SIP server.

Example

Set the signaling domain name to **abcd.com** for a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-domain abcd.com
```

16.5.2.32 sipserver

Function

Using the **sipserver** command, you can enter the SIP server view.

Using the **undo sipserver** command, you can delete the SIP server.

Format

sipserver

undo sipserver

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as a SIP server, run the **sipserver** command to enter the SIP server view and configure this SIP server.

Example

Enter the SIP server view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver]signalling-domain abcd.com
```

16.5.2.33 transfer(SIP server view)

Function

Using the **transfer** command, you can configure the transfer mode for a SIP server.

Using the **undo transfer** command, you can restore the default transfer mode of a SIP server.

The default transfer mode of a SIP server is UDP.

Format

transfer *transfer-value*

undo transfer

Parameters

Parameter	Description	Value
transfer-value	Specifies the transfer mode for a SIP server.	Enumerated type. The values are as follows: ● TCP ● UDP ● TLS

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the transfer mode of a SIP server to TCP.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] transfer TCP
```

16.5.3 CDR Server Configuration Commands

16.5.3.1 bill format

Function

The **bill format** command specifies the format of CDRs output by the AR.

The **undo bill format** command restores the default format of CDRs output by the AR.

By default, the output format is CDR.

Format

bill format *format-value*

undo bill format

Parameters

Parameter	Description	Value
format-value	Specifies the format of CDRs.	Enumerated value. The options are as follows: ● CDR: CDR binary format ● SOFTX: SOFT X3000 binary format ● MINI: MINI text format ● UCBILL: U1900 CDR

Views

CDR server view

Default Level

2: Configuration level

Usage Guidelines

The **bill format** command specifies the format of CDRs output by the AR.

Example

Set the CDR format to UCBILL.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] cdr-server
[Huawei-voice-cdr-server] bill format UCBILL
```

16.5.3.2 bill textfield

Function

The **bill textfield** command specifies the output item of MINI CDRs.

The **undo bill textfield** command restores the default output item of MINI CDRs.

By default, the output item of MINI CDRs is ALL.

Format

bill textfield *index*

undo bill textfield

Parameters

Parameter	Description	Value
index	Specifies the output item.	The value ranges from 0 to 43.

Views

CDR server view

Default Level

2: Configuration level

Usage Guidelines

The **bill textfield** command specifies the output item of MINI CDRs.

Example

Configure the device not to output the IP address.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]cdr-server
[Huawei-voice-cdr-server]bill textfield 0 disable
```

16.5.3.3 bill transfertype

Function

The **bill transfertype** command specifies CDR transfer mode.

The **undo bill transfertype** command restores the default CDR transfer mode.

The default transfer mode is SFTP.

Format

bill transfertype { FTP | SFTP }

undo bill transfertype

Parameters

Parameter	Description	Value
transfertype	Specifies the CDR transfer mode.	The value can be **FTP** or **SFTP**. ● FTP: Transfer CDRs to an FTP server using FTP. ● SFTP: Transfer CDRs to an SFTP server using SFTP.

Views

CDR server view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the CDR transfer mode.

Example

Set the CDR transfer mode to SFTP.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]cdr-server
[Huawei-voice-cdr-server]bill transfertype SFTP
```

16.5.3.4 billpoolfull

Function

The **billpoolfull** command configures a policy when the CDR pool is full.

The **undo billpoolfull** command restores the default policy when the CDR pool is full.

By default, the values of **billdiscard** and **calleelimit** are **disable**.

Format

billpoolfull { **billdiscard** *billdiscard* | **calleelimit** *calleelimit* | **callerlimit** *callerlimit* }

undo billpoolfull { **billdiscard** | **calleelimit** | **callerlimit** }

Parameters

Parameter	Description	Value
billdiscard	Specifies a policy for new CDRs when the CDR pool is full.	Enumerated value. The options are as follows: ● disable: New CDRs overwrite old CDRs. ● enable: New CDRs are discarded.
calleelimit	Specifies a called limiting policy when the CDR pool is full.	Enumerated value. The options are as follows: ● disable: Calls are not limited. ● enable: Calls are limited: – VU: IVR call limiting. – ddd: Domestic direct dialing call limiting. – idd: International direct dialing call limiting. – inter: Internal dialing call limiting. – local: Local dialing call limiting.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
callerlimit	Specifies a caller limiting policy when the CDR pool is full	Enumerated value. The options are as follows: ● disable: Calls are not limited. ● enable: Calls are limited: – ddd: Domestic direct dialing call limiting. – idd: International direct dialing call limiting. – inter: Internal dialing call limiting. – local: Local dialing call limiting.

Views

CDR server view

Default Level

2: Configuration level

Usage Guidelines

The **billpoolfull** command configures a policy when the CDR pool is full.

Example

Configure local call limiting.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] cdr-server
[Huawei-voice-cdr-server] billpoolfull calleelimit enable local enable
```

16.5.3.5 cdr-server

Function

Using the **cdr-server** command, you can enter the Call Detail Record (CDR) server view.

Using the **undo cdr-server** command, you can delete the Call Detail Record (CDR) server.

Format

cdr-server

undo cdr-server

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enter the CDR server view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] cdr-server
[Huawei-voice-cdr-server]
```

16.5.3.6 display voice cdr-server

Function

The **display voice cdr-server** command displays the configuration of a CDR server.

Format

display voice cdr-server

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

The **display voice cdr-server** command displays the configuration of a CDR server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the configuration of a CDR server.

```
<Huawei> display voice cdr-server
  Protocol type        : FTP
  Server IP address    : 192.168.0.1
  Server port          : 2020
  User name            :
  Password             :
  Connection status    : Released
  Bill Format          : CDR
  Billpoolfull discard : disable
  Bill pool state      :
      Used             : 12
      Max              : 34952
      Alarm            : 31456
      Alarm state      : NOT FULL
  Caller limit         : disable
  Callee limit         : disable
  Textfield include    : ALL
```

Table 16-57 Description of the display voice cdr-server command output

Item	Description
Protocol type	Protocol type.
Server IP address	IP address of a CDR server. To configure the IP address of a CDR server, run the **16.5.3.7 server ip port** command.
Server UDP port	Port number of a CDR server. To configure the port number of a CDR server, run the **16.5.3.7 server ip port** command.
User name	User name of a CDR server. To configure the user name of a CDR server, run the **16.5.3.8 username password** command.
Password	Password of a CDR server. To configure the password of a CDR server, run the **16.5.3.8 username password** command.
Connection status	Connection status.
Bill Format	CDR type. This parameter can be set using the **bill format** command.
Billpoolfull discard	New CDR policy when the CDR pool is full. This parameter can be set using the **billpoolfull** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Bill pool state	CDR pool status.
Caller limit	Calling party barring policy when the CDR pool is full. This parameter can be set using the **billpoolfull callerlimit** command.
Called limit	Called party barring policy when the CDR pool is full. This parameter can be set using the **billpoolfull calledlimit** command.
Textfield include	CDR text fields. This parameter can be set using the **bill textfield** command.

16.5.3.7 server ip port

Function

Using the **server ip port** command, you can specify the IP address and port number of a CDR server.

By default, no IP address or port number of the CDR server is specified.

Format

server ip *ip-address* **port** *port-number*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a CDR server.	The value is in dotted decimal notation.
port-number	Specifies the port number of a CDR server.	The value is an integer that ranges from 1 to 65535.

Views

CDR server view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the IP address and port number of a CDR server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] cdr-server
[Huawei-voice-cdr-server] server ip 192.168.0.2 port 21
```

16.5.3.8 username password

Function

The **username password** command configures user names and passwords.

The **undo username** command deletes user names.

Format

username *username* **password cipher** *cipher-password*

undo username

Parameters

Parameter	Description	Value
username	Specifies the user name.	The value is a string of 1 to 15 characters.
cipher *cipher-password*	Specifies the password sent in cipher text. **NOTE** You can configure *cipher-password* after inputting **cipher** and pressing **Enter**.	The value is a string of case-sensitive characters without spaces. A cipher password may contain 1 to 15 encrypted characters.

Views

CDR server view

Default Level

2: Configuration level

Usage Guidelines

N/A

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the user name to **user1** and the password to **admin**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] cdr-server
[Huawei-voice-cdr-server] username user1 password cipher
 Please input user password(1-15 chars):*****
```

16.5.4 PBX User Configuration Commands

16.5.4.1 bind trunk-group (PBX user view)

Function

Using the **bind trunk-group** command, you can associate a specified PBX user with a specified SIP AT0 trunk group so that registration status is kept consistent between the PBX user and SIP AT0 trunk group. By default, this function is not configured for users.

Format

bind trunk-group *trunk-group-name* **trunk-sipat0** *register-privateid*

undo bind trunk-group trunk-sipat0

Parameters

Parameter	Description	Value
trunk-group-name	Specifies the SIP AT0 trunk group name.	The value is a string of 1 to 32 characters.
register-privateid	Specifies the registration ID of the SIP AT0 trunk.	The value is a string of 1 to 32 characters.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

This command is generally used in the eSBC scenario for conversion between public and private networks. This command ensures that the registration status of the IP PBX with the AR is consistent with that of the AR with the IMS.

 Copyright © Huawei Technologies Co., Ltd.

Example

Keep registration status of SIP user 28980000 to be consistent with that of the SIP AT0 trunk (28980000) from the AR to IMS.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser 28980000 sipue
[Huawei-voice-pbxuser-28980000] sipue 28980000
[Huawei-voice-pbxuser-28980000] telno 28980000
[Huawei-voice-pbxuser-28980000] bind trunk-group sipat0 trunk-sipat0 28980000
```

16.5.4.2 call-right

Function

The **call-right** command configures incoming and outgoing call rights for trunk groups.

The **undo call-right** command restores the default settings.

By default, inter office calls are allowed.

Format

call-right { **in** | **out** } { { **inter** *inter-value* | **local** *local-value* | **ddd** *ddd-value* | **idd** *idd-value* } * | **all** }

undo call-right [**in** | **out**]

Parameters

Parameter	Description	Value
inter-value	Internal dialing call right.	Enumerated type. The values are as follows: ● disable ● enable
local-value	Local dialing call right	Enumerated type. The values are as follows: ● disable ● enable
ddd-value	Domestic direct dialing call right	Enumerated type. The values are as follows: ● disable ● enable
idd-value	International direct dialing call right	Enumerated type. The values are as follows: ● disable ● enable

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	all call right	all: All (inter&local&ddd&idd) right

Views

Pbxuser view

Default Level

2: Configuration level

Usage Guidelines

N/A

Example

Configure the incoming and outgoing call rights for national toll calls.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser huawei
[Huawei-voice-pbxuser-huawei] call-right in all
[Huawei-voice-pbxuser-huawei] call-right out idd enable
```

16.5.4.3 custom-right (PBX user view)

Function

The **custom-right** command binds customized 32-level rights to a PBX user.

By default, no 32-level right is bound to a PBX user.

Format

custom-right { *c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32* }*

undo custom-right [*c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32*] *

Parameters

Parameter	Description	Value
c1 | *c2* | *c3* | *c4* | *c5* | ...| *c32*	Specifies 32-level rights to be bound to a PBX user.	The value can be one or more of **c1** to **c32**.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

By default, no 32-level right is bound to a PBX user. You can configure 1 to 32 customized rights.

Adding or deleting a right does not affect existing 32-level rights.

To clear all 32-level rights bound to a user, run the **undo custom-right** command.

Example

Bind 32-level rights **c4** and **c8** to PBX user 28980000.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] pbxuser 28980000 pots
 [Huawei-voice-pbxuser-28980000] custom-right c4 c8
```

Unbind 32-level right **c4** from PBX user 28980000.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] pbxuser 28980000
 [Huawei-voice-pbxuser-28980000] undo custom-right c4
```

Clear all 32-level rights bound to PBX user 28980000.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] pbxuser 28980000
 [Huawei-voice-pbxuser-28980000] undo custom-right
```

16.5.4.4 display voice pbxuser

Function

The **display voice pbxuser** command displays the configuration of a PBX user.

Format

display voice pbxuser [*pbxuser-name* | *user-category*] [**enterprise** *enterprise*]

Parameters

Parameter	Description	Value
pbxuser-name	Displays the configuration of a specified PBX user.	The value is a string of 1 to 32 characters without spaces.

Parameter	Description	Value
user-category	Displays the configuration of PBX users by user types.	Enumerated type. Categories are as follows: **pots** **bra** **sipue**

Views

All views

Default Level

3: Management level

Usage Guidelines

If no PBX user name is specified, the configuration of all PBX users is displayed.

Example

Display the configuration of the PBX user 2000.

```
<Huawei> display voice pbxuser 2000
  PBX user                : 2000
  Enterprise              : default
  Port                    : 2/0/0
  Sipue Type              :
  Dn-set                  : DefaultDialPlan
  Telephone number        : 2000
  Long telno              :
  Callin right            : inter&local&ddd&idd
  Callout right           : inter&local
  User type               : Normal
  Priority of user        : Default
  PickupGroup name        :
  Newmsgs number          : 0
  Oldmsgs number          : 0
  User name               : join
  Service status          : Idle
```

Table 16-58 Description of the **display voice pbxuser** command output

Item	Description
PBX user	Name of a PBX user. To set the name of a PBX user, run the **16.5.4.33 pbxuser (voice view)** command.

Item	Description
Enterprise	Enterprise to which a PBX user belongs. To configure the enterprise to which a PBX user belongs, run the **16.5.4.33 pbxuser (voice view)** command.
Port	Physical interface to which a POTS user is bound. To configure the physical interface to which a POTS user is bound, run the **16.5.4.33 pbxuser (voice view)** command.
Sipue Type	Type of a SIP user.
Dn-set	DN set of a PBX user. To set the DN set of a PBX user, run the **16.5.4.13 dn-set (PBX user view)**command.
Telephone number	Phone number of a PBX user. To set the phone number of a PBX user, run the **telno** command.
Long telno	Long telno of a PBX user. To set the phone number of a PBX user, run the **telno** command.
Callin right	Call-in right.
Callout right	Call-out right.
User type	User type.
Priority of user	Priority of a PBX user.
PickupGroup name	Pickup group name.
Newmsgs number	Number of new voicemail messages.
Oldmsgs number	Number of old voicemail messages.
Service status	Service status.
Priority group name	Call priority group with which a PBX user is associated.

 Copyright © Huawei Technologies Co., Ltd.

16.5.4.5 display voice pbxuser brief

Function

The **display voice pbxuser brief** command displays the basic configuration of PBX users.

Format

display voice pbxuser brief [*pbxuser-name*]

Parameters

Parameter	Description	Value
pbxuser-name	Displays the configuration of a specified PBX user.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can view the basic configuration of PBX users.

Example

Display the basic configuration of all PBX users.

```
<Huawei>display voice pbxuser brief
 Spec: 250, Records: 250
 ---------------------------------------------------------------
 Pbxuser              PTP Status        CTP Status
 2000                 Normal            Idle
 2001                 Normal            Idle
 2002                 Normal            Idle
 2003                 Normal            Idle
 2010                 Out of service     Block
 2011                 Out of service     Block
 2012                 Out of service     Block
 2013                 Out of service     Block
 2014                 Out of service     Block
 2015                 Out of service     Block
 2016                 In service        Idle
 2018                 Out of service     Block
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-59 Description of the display voice pbxuser command output

Item	Description
PBX user	Name of the PBX user. You can configure the PBX user name by running the **pbxuser (voice view)** command.
PTP status	PBX user registration status.
CTP status	PBX user call status.

16.5.4.6 display voice pbxuser eid-para

Function

The **display voice pbxuser eid-para** command displays EID parameters configured for a PBX user.

Format

display voice pbxuser *name* **eid-para**

Parameters

Parameter	Description	Value
name	Specifies a PBX user name.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

View EID parameters configured for a PBX user.

```
<Huawei> display voice pbxuser pots1 eid-para
  Description                    :
  Priority                       : cat3
```

```
Pots line type                    : DEL
CLIP transmission sequence        : after-ring
CLIP format                       : SDMF(FSK)
DC time(ms)                       : 100
FSK time(ms)                      : 800
VQE auto gain active flag         : Disable
VQE auto gain target level        : -22
VQE noise suppression active flag : Disable
VQE noise suppression level       : 12
DSP input gain(db)                : 0
DSP output gain(db)               : 0
Detect ANS BRA by single tone flag: Disable
Bell ANS flag                     : Disable
FSK mode                          : BELL_202
TAS mode                          : NO-TAS
```

Table 16-60 Description of the display voice pbxuser eid-para command output

Item	Description
Description	Description. This parameter can be set using the **eid-para description** command.
Priority	User priority. This parameter can be set using the **eid-para Priority** command.
Pots line type	User type. This parameter can be set using the **eid-para line-type** command.
CLIP transmission sequence	CLIP transmission sequence
CLIP format	Calling number format. This parameter can be set using the **eid-para clip-format** command.
DC time	Power-off interval. This parameter can be set using the **eid-para dc-time** command.
FSK time	FSK delay. This parameter can be set using the **eid-para fsk-time** command.
VQE auto gain active flag	Automatic voice gain flag. This parameter can be set using the **eid-para vqe-agc** command.
VQE auto gain target level	Automatic voice gain value. This parameter can be set using the **eid-para vqe-agc** command.
VQE noise suppression active flag	Noise suppression flag. This parameter can be set using the **eid-para vqe-sns** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VQE noise suppression level	Noise suppression level. This parameter can be set using the **eid-para vqe-sns-level** command.
DSP input gain	DSP input gain. This parameter can be set using the **eid-para dsp-input-gain** command.
DSP output gain	DSP output gain. This parameter can be set using the **eid-para dsp-output-gain** command.
Detect ANS BRA by single tone flag	ANSbar signal detection using single tones flag. This parameter can be set using the **eid-para detect-ansbra-by-single-tone** command.
Bell ANS flag	Bell ANS signal flag. This parameter can be set using the **eid-para bell-ans-flag** command.
FSK mode	FSK mode. This parameter can be set using the **eid-para fsk-mode** command.
TAS mode	TAS mode. This parameter can be set using the **eid-para tas-pattern** command.

16.5.4.7 display voice pbxuser port

Function

The **display voice pbxuser port** command displays the PBX user configuration on an interface.

Format

display voice pbxuser port *port-type* [*interface-number*]

Parameters

Parameter	Description	Value
port-type	Specifies the type of the interface to be checked.	Enumerated value. The options are as follows: ● pots: Foreign exchange station (FXS) interface. ● bra: Basic rate access (BRA) interface.
interface-number	Specifies the number of the interface on which the PBX user configuration is checked.	The value is a string of 1 to 15 characters without spaces. The value of *interface-number* is based on the device specifications.

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display voice pbxuser port** command to check information about users that are bound to an interface.

Example

Display the PBX user configuration on the POTS interface 0/0/0.

```
<Huawei> display voice pbxuser port pots 0/0/0
  PBX user                : 20000
  Enterprise              : default
  Port                    : 0/0/0
  Port type               : pots
  Sipue Type              :
  Dn-set                  : DefaultDialPlan
  Telephone number        : 20000
  Long telno              :
  Service status          : Idle
```

Table 16-61 Description of the **display voice pbxuser port** command output

Item	Description
PBX user	Name of the PBX user.
Enterprise	Enterprise of the PBX user.

Item	Description
Port	Physical port bound to the PBX user.
Port type	Type of the port bound to the PBX user. **NOTE** Only AR169CVW-4B4S supports this parameter.
Sipue Type	SIP user type.
Dn-set	DN set of the PBX user.
Telephone number	Phone number of the PBX user.
Long telno	Long number of the PBX user.
Service status	Service status.

Related Topics

16.5.4.33 pbxuser (voice view)
16.5.4.36 port (PBX user view)
16.5.4.13 dn-set (PBX user view)

16.5.4.8 display voice pbxuser sipue

Function

The display voice pbxuser sipue command displays the configuration of PBX SIP users.

Format

display voice pbxuser sipue [*sipue-eid* | *enterprise*]

Parameters

Parameter	Description	Value
sipue-eid	Specifies the EID.	Character string type. The value is a string of 1-64 characters, and space is not supported.

Views

All views

Default Level

3: Management level

Usage Guidelines

If the EID is not specified, the configuration of all SIP users is displayed.

Example

Display the configuration of a PBX SIP user.

```
<Huawei> display voice pbxuser sipue
  PBX user                : 2010
  Enterprise              : default
  Eid                     : 2010
  Sipue Type              : SIPUE
  Dn-set                  : DefaultDialPlan
  Telephone number        : 2010
  Long telno              :
  Register status         : Out of service
  Service status          : Block
```

Table 16-62 Description of the **display voice pbxuser sipue** command

Item	Description
PBX user	Name of the PBX user. You can configure the PBX user name by running the **pbxuser (voice view)** command.
Enterprise	Enterprise of the PBX user. You can configure the enterprise of the PBX user by running the **pbxuser (voice view)** command.
Eid	Device identifier of the SIP user.
Sipue Type	Type of the SIP user.
Dn-set	DN set of the PBX user. You can configure the DN set by running the **dn-set (PBX user view)** command.
Telephone number	Phone number of the PBX user. You can configure the phone number by running the **telno** command.
Long telno	Long number of the PBX user. You can configure the long number by running the **telno** command.
Register status	User registration status.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Service status	User status.

16.5.4.9 display voice pbxuser sipue-register-state

Function

The **display voice pbxuser sipue-register-state** command displays registration information about a PBX user.

Format

display voice pbxuser sipue-register-state [*pbxuser-name*]

Parameters

Parameter	Description	Value
pbxuser-name	Displays the configuration of a specified PBX user.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

If the PBX user name is not specified, registration information about all PBX users is displayed.

Example

View registration information about PBX user 2016.

```
<Huawei>display voice pbxuser sipue-register-state 2016
 Pbxuser         : 2016
 SIPUE           : 192.168.0.1:5060
 Expires(s)      : 2197
 Interval(s)     : 3600
 Status          : In service
```

Table 16-63 Description of the display voice pbxuser command output

Item	Description
PBX user	Name of a PBX user. To set the name of a PBX user, run the **16.5.4.33 pbxuser (voice view)** command.
SIPUE	Registration source.
Expires	Registration timeout interval.
Intervals	Registration interval.
Status	Registration status.

16.5.4.10 display voice pbxuser start-telno

Function

The **display voice pbxuser start-telno** command displays the configuration information about PBX users.

Format

display voice pbxuser start-telno *start-telno* [**end-telno** *end-telno*]

Parameters

Parameter	Description	Value
start-telno	Specifies the start number of the PBX users to query.	The value is a string of 1 to 24 characters excluding space.
end-telno *end-telno*	Specifies the end number of the PBX users to query.	The value is a string of 1 to 24 characters excluding space.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the configuration information about PBX user those number start with **20000**.

```
<Huawei> display voice pbxuser start-telno 20000
  PBX user                : 200000
  Enterprise              : default
  Eid                     : 200000
  Sipue Type              : SIPUE
  Dn-set                  : DefaultDialPlan
  Telephone number        : 200000
  Long telno              :
  Register status         : Out of service
  Service status          : Block

  PBX user                : 200001
  Enterprise              : default
  Eid                     : 200001
  Sipue Type              : SIPUE
  Dn-set                  : DefaultDialPlan
  Telephone number        : 200001
  Long telno              :
  Register status         : Out of service
  Service status          : Block
```

Table 16-64 display voice pbxuser command output

Parameter	Description
PBX user	PBX user name. This parameter can be set using the **16.5.4.33 pbxuser (voice view)** command.
Enterprise	Enterprise to which the PBX user belongs. This parameter can be set using the **16.5.4.33 pbxuser (voice view)** command.
Port	Physical port bound to the PBX user. This parameter can be set using the **16.5.4.36 port (PBX user view)** command.
Dn-set	DN set of the PBX user. This parameter can be set using the **16.5.4.13 dn-set (PBX user view)** command.
Telephone number	Telephone number of the PBX user. This parameter can be set using the **16.5.4.42 telno (PBX user view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Long telno	Long number of the PBX user. This parameter can be set using the **16.5.4.42 telno (PBX user view)** command.
Register status	User registration status.
Service status	User status.

16.5.4.11 display voice pbxuser state

Function

The **display voice pbxuser** command displays the PBX user configuration according to the user status.

Format

display voice pbxuser *state*

Parameters

Parameter	Description	Value
state	Displays the PBX user status.	Enumerated type. The values are as follows: • **idle**: The PBX user is idle. • **busy**: The PBX user is busy. • **blocked**: The PBX user is blocked.

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display the configuration of PBX users in busy state.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] display voice pbxuser busy
 PBX user                : 1387
 Enterprise              : default
 Eid                     : 1387
 Sipue Type              : SIPUE
 Dn-set                  : DefaultDialPlan
 Telephone number        : 1387
 Long telno              :
 Register status         : In service
 Service status          : Busy
```

Table 16-65 display voice pbxuser command output

Item	Description
PBX user	Name of the PBX user. You can configure the PBX user name by running the **pbxuser (voice view)** command.
Enterprise	Enterprise of the PBX user. You can configure the enterprise of the PBX user by running the **pbxuser (voice view)** command.
Eid	Device identifier of the SIP user.
Sipue Type	Type of the SIP user.
Dn-set	DN set of the PBX user. You can configure the DN set by running the **dn-set (PBX user view)** command.
Telephone number	Phone number of the PBX user.
Long telno	Long number of the PBX user.
Register status	User registration status.
Service status	User status.

16.5.4.12 display voice priority-group

Function

The **display voice priority-group** command displays call priority group configurations.

Format

display voice priority-group [*priority-group-name*]

Parameters

Parameter	Description	Value
priority-group-name	Indicates the name of the call priority group to be checked.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run the **display voice priority-group** command to check numbers and priorities of users in a call priority group.

Example

Check configurations of all call priority groups.

```
<Huawei> display voice priority-group
  Priority group name    : Group1
  Priority telno         : 1002
  Priority level         : 2
```

Table 16-66 Description of the **display voice priority-group** command output

Item	Description
Priority group name	Name of the call priority group.
Priority telno	Phone number of a calling user.
Priority level	Priority of a calling user.

16.5.4.13 dn-set (PBX user view)

Function

Using the **dn-set** command, you can configure a DN set for PBX users.

Using the **undo dn-set** command, you can delete a DN set for PBX users.

By default, PBX uses use the default DN set **DefaultDialPlan**.

Format

dn-set *dn-set-name*

undo dn-set

Parameters

Parameter	Description	Value
dn-set-name	Specifies the name of a DN set.	The value is a string of 1 to 32 characters without spaces.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

A DN set is a collection of prefixes that all users on the PSTN can dial. Before configuring a DN set to which users belong, run the **dn-set (enterprise view)** command to create a DN set.

Example

Set the DN set to **user001** for PBX users.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser aaa pots enterprise huawei
[Huawei-voice-pbxuser-aaa] dn-set user001
```

16.5.4.14 eid-para bell-ans-flag

Function

Using the **eid-para bell-ans-flag** command, you can configure the device to support Bell ANS signals or disable this function.

The **undo eid-para bell-ans-flag** command restores the default setting of Bell ANS signals.

By default, the device does not support Bell ANS signals.

Format

eid-para bell-ans-flag { **enable** | **disable** }

undo eid-para bell-ans-flag

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the device to support Bell ANS signals.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser aaa pots
[Huawei-voice-pbxuser-aaa] port 1/0/1
[Huawei-voice-pbxuser-aaa] eid-para bell-ans-flag enable
```

16.5.4.15 eid-para clip-format

Function

Using the **eid-para clip-format** command, you can configure the calling number format.

Using the **undo eid-para clip-format** command, you can restore the default calling number format.

By default, the calling number format is frequency-shift keying (FSK) simple data format.

ps: Valid only for pots users

Format

eid-para clip-format { **sdmf-fsk** | **mdmf-fsk** | **dtmf** | **etsi** | **r1_5** }

undo eid-para clip-format

Parameters

Parameter	Description	Value
sdmf-fsk	Specifies the frequency-shift keying (FSK) simple data format.	-

Parameter	Description	Value
mdmf-fsk	Specifies the FSK compound data format.	-
dtmf	Specifies the Dual Tone Multifrequency (DTMF) format.	-
etsi	Specifies the BT calling number format.	-
r1_5	Specifies the Russia calling number format.	-

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the calling number format to SDMF.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser aaa pots
[Huawei-voice-pbxuser-aaa] port 1/0/1
[Huawei-voice-pbxuser-aaa] eid-para clip-format sdmf
```

16.5.4.16 eid-para dc-time

Function

Using the **eid-para dc-time** command, you can set the power-off interval.

Using the **undo eid-para dc-time** command, you can restore the default power-off interval.

By default, the power-off interval is 100 milliseconds.

Format

eid-para dc-time *dc-time*

undo eid-para dc-time

Parameters

Parameter	Description	Value
dc-time	Specifies the power-off interval.	The value is an integer that ranges from 10 to 100, in 10 milliseconds.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the power-off interval to 100 milliseconds.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser aaa pots
[Huawei-voice-pbxuser-aaa] port 1/0/1
[Huawei-voice-pbxuser-aaa] eid-para dc-time 10
```

16.5.4.17 eid-para default-cli

Function

The **eid-para default-cli** command configures the default calling number for a BRA user.

The **undo eid-para default-cli** command deletes the default calling number of a BRA user.

By default, no calling number is configured for a BRA user.

Format

eid-para default-cli *default-cli-value*

undo eid-para default-cli

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
default-cli *default-cli-value*	Specifies the default calling number. **NOTE** *When an ISDN user makes outgoing calls over the SIP PRA trunk without calling number information, the default calling number can be used.*	The value is a string of 1 to 64 characters without spaces.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

When an ISDN user makes an outgoing call over the SIP PRA trunk without calling number information (for example, the user enables the restriction on the calling number), run this command to configure the default calling number.

Example

Configure the default calling number of the BRA user named **user001** to 1100.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] pbxuser user001 bra
 [Huawei-voice-pbxuser-user001] eid-para default-cli 1100
```

16.5.4.18 eid-para description (PBX user view)

Function

Using the **eid-para description** command, you can configure the description of a PBX user.

Using the **undo eid-para description** command, you can delete the description of a PBX user.

By default, no description is configured for a PBX user.

Format

eid-para description *description*

undo eid-para description

Parameters

Parameter	Description	Value
description	Specifies the description of a PBX user.	The name is a string of 1 to 64 case-sensitive characters without spaces.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the description of the PBX user **user001** as **pots**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para description pots
```

16.5.4.19 eid-para detect-ansbar-by-single-tone

Function

Using the **eid-para detect-ansbar-by-single-tone** command, you can enable ANSbar signal detection using single tones or disable this function.

The **undo eid-para detect-ansbar-by-single-tone** command restores the default setting of ANSbar signal detection using single tones.

By default, ANSbar signal detection using single tones is disabled.

Format

eid-para detect-ansbar-by-single-tone { enable | disable }

undo eid-para detect-ansbar-by-single-tone disable

Parameters

None

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable ANSbar signal detection using single tones.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para detect-ansbar-by-single-tone enable
```

16.5.4.20 eid-para dsp-input-gain

Function

Using the **eid-para dsp-input-gain** command, you can configure the DSP chip input gain.

Using the **undo eid-para dsp-input-gain** command, you can restore the default DSP chip input gain.

By default, the DSP chip input gain is 10, that is, 0 dB.

Format

eid-para dsp-input-gain *dsp-input-gain*

undo eid-para dsp-input-gain

Parameters

Parameter	Description	Value
dsp-input-gain	Specifies the input gain of the DSP module. **NOTE** The input gain refers to the gain from the PCM side to the IP side.	The value is an integer that ranges from 0 to 15. The values 0 to 15 correspond to -10 dB to 5 dB. The default value is 0 dB.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

You can run the **eid-para dsp-input-gain** command to improve the voice quality.

Example

Set the input gain of the DSP module to 5 dB.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para dsp-input-gain 15
```

16.5.4.21 eid-para dsp-output-gain

Function

Using the **eid-para dsp-output-gain** command, you can configure the output gain of the DSP module.

Using the **undo eid-para dsp-output-gain** command, you can restore the default output gain of the DSP module.

By default, the output gain of the DSP module is 10, that is, 0 dB.

Format

eid-para dsp-output-gain *dsp-output-gain*

undo eid-para dsp-output-gain

Parameters

Parameter	Description	Value
dsp-output-gain	Specifies the output gain of the DSP module. **NOTE** The output gain refers to the gain from the IP side to the PCM side.	The value is an integer that ranges from 0 to 20. The values 0 to 20 correspond to -10 dB to 10 dB. The default value is 0 dB.

Views

PBX user view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **eid-para dsp-output-gain** command to adjust the voice quality.

Example

Set the output gain of the DSP module to 10 dB.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] dsp-output-gain 20
```

16.5.4.22 eid-para endservice

Function

Using the **eid-para endservice** command, you can terminate services of PSTN users.

Using the **undo eid-para endservice** command, you can restore services of PSTN users.

Format

eid-para endservice

undo eid-para endservice

Parameters

None

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The **eid-para endservice** command terminates services of PSTN users. Exercise caution when you run this command.

Example

Terminate services of PSTN users.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para endservice
 Note: Stop service successful.
```

16.5.4.23 eid-para fsk-mode

Function

Using the **eid-para fsk-mode** command, you can configure the FSK call display mode.

Using the **undo eid-para fsk-mode** command, you can restore the default FSK call display mode.

By default, the FSK call display mode is BELL_202.

Format

eid-para fsk-mode { **bell_202** | **ccitt_v23** | **ntt** }

undo eid-para fsk-mode

Parameters

Parameter	Description	Value
bell_202	Sets the FSK call display mode to BELL_202.	-
ccitt_v23	Sets the FSK call display mode to CCITT_V23.	-
ntt	Sets the FSK call display mode to NTT.	-

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the FSK call display mode to NTT.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para fsk-mode ntt
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.4.24 eid-para fsk-time

Function

Using the **eid-para fsk-time** command, you can set the FSK delay.

Using the **undo eid-para fsk-time** command, you can restore the default FSK delay.

By default, the FSK delay is 800 milliseconds.

Format

eid-para fsk-time *fsk-time*

undo eid-para fsk-time

Parameters

Parameter	Description	Value
fsk-time	Specifies the FSK delay.	The value is an integer that ranges from 0 to 100, in 10 milliseconds.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the FSK delay to 100 milliseconds.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para fsk-time 10
```

16.5.4.25 eid-para line-type

Function

Using the **eid-para line-type** command, you can configure the PSTN user type.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo eid-para line-type** command, you can restore the default PSTN user type.

By default, the PSTN user type is DEL.

Format

eid-para line-type { **del** | **ecpbx** | **lcpbx** | **payphone** }

undo eid-para line-type

Parameters

Parameter	Description	Value
del	Specifies the PSTN user type as Direct Exchange Lines (DEL). DEL users' lines are directly connected to device ports.	-
ecpbx	Specifies the PSTN user type as Earth Calling PBX (ECPBX). PBX users' lines are connected to device ports through the PBX.	-
lcpbx	Specifies the PSTN user type as Loop Calling PBX (LCPBX). LCPBX users' lines are connected to device ports through the PBX.	-
payphone	Specifies the user type as pay phone. Pay phone users' lines are connected to the accounting terminal through the device ports.	-

Views

PBX user view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Configure the type of the PBX user **user001** as payphone.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para line-type payphone
```

16.5.4.26 eid-para password (PBX user view)

Function

The **eid-para password** command configures the authentication password for a SIP UE user.

The **undo eid-para password** command deletes the authentication password of a SIP UE user.

By default, no authentication password is configured for a SIP UE user.

Format

eid-para passwordcipher *password-value*

undo eid-para password

Parameters

Parameter	Description	Value
cipher*password-value*	Specifies the string of the cipher text password. **NOTE** You can configure *password-value* after inputting **cipher** and pressing **Enter**.	The value is a string of 6 to 64 characters without space. It must contain numbers, letters, and special characters.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

N/A

Example

Configure the authentication password **abcde123@** for a SIP UE user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 sipue
[Huawei-voice-pbxuser-user001] sipue 001
[Huawei-voice-pbxuser-user001] eid-para password cipher
 Please input user password(6-64 chars):********
```

16.5.4.27 eid-para priority (PBX user view)

Function

The **eid-para priority** command configures the priority for a PBX user.

The **undo eid-para priority** command restores the default priority of a PBX user.

By default, the priority of a PBX user is **cat3** after the PBX user is created.

Format

eid-para priority { **cat1** | **cat2** | **cat3** }

undo eid-para priority

Parameters

Parameter	Description	Value
cat1	Sets the priority to category-1 user priority.	-
cat2	Sets the priority to category-2 user priority.	-
cat3	Sets the priority to normal.	-

Views

PBX user view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The eid-para priority command is supported only when the user type is pots and bra.

Example

Set the priority of PBX user **user001** to **cat1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para priority cat1
```

16.5.4.28 eid-para tas-pattern

Function

Using the **eid-para tas-pattern** command, you can configure the TAS mode of Calling Line Identification Presentation (CLIP).

Using the **undo eid-para tas-pattern** command, you can restore the default TAS mode of CLIP.

By default, the TAS mode of CLIP is NO-TAS.

Format

eid-para tas-pattern { **dt-as** | **no-tas** }

undo eid-para tas-pattern

Parameters

None

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the TAS mode of CLIP to DT-AS.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
```

```
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para tas-pattern dt-as
```

16.5.4.29 eid-para vqe-agc

Function

Using the **eid-para vqe-agc** command, you can enable voice quality enhancement (VQE) or disable this function.

The **undo eid-para vqe-agc** command restores the default VQE setting.

Format

eid-para vqe-agc { enable | disable }

undo eid-para vqe-agc

Parameters

None

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable VQE.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para vqe-agc enable
```

16.5.4.30 eid-para vqe-agc-level

Function

Using the **eid-para vqe-agc-level** command, you can configure the target voice quality enhancement (VQE) level.

Using the **undo eid-para vqe-agc-level** command, you can restore the default target VQE level.

By default, the target VQE level is 13, that is -22 dB.

 Copyright © Huawei Technologies Co., Ltd.

Format

eid-para vqe-agc-level *vqe-agc-level*

undo eid-para vqe-agc-level

Parameters

Parameter	Description	Value
vqe-agc-level	Specifies the target VQE level.	The value is an integer that ranges from 0 to 15, that is, -9 dB to -24 dB.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Before running this command, run the **eid-para vqe-agc** command to enable the VQE.

Example

Set the target VQE level to -24 dB.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para vqe-agc-level 15
```

16.5.4.31 eid-para vqe-sns

Function

Using the **eid-para vqe-sns** command, you can enable noise suppression or disable this function.

The **undo eid-para vqe-sns** command restores the default setting of noise suppression.

By default, noise suppression is disabled.

Format

eid-para vqe-sns { enable | disable }

undo eid-para vqe-sns

Parameters

None

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable noise suppression.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para vqe-sns enable
```

16.5.4.32 eid-para vqe-sns-level

Function

Using the **eid-para vqe-sns-level** command, you can set the noise suppression level.

Using the **undo eid-para vqe-sns-level** command, you can restore the default noise suppression level.

By default, the noise suppression level is 12, that is, 12 dB.

Format

eid-para vqe-sns-level *vqe-sns-level*

undo eid-para vqe-sns-level

Parameters

Parameter	Description	Value
vqe-sns-level	Specifies a noise suppression level.	The value is an integer that ranges from 6 to 20, in dB. The default value is 12.

 Copyright © Huawei Technologies Co., Ltd.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Before running this command, run the **eid-para vqe-sns enable** command to enable noise suppression.

Example

Set the noise suppression level to 20 dB.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001
[Huawei-voice-pbxuser-user001] port 1/0/1
[Huawei-voice-pbxuser-user001] eid-para vqe-sns-level 20
```

16.5.4.33 pbxuser (voice view)

Function

The **pbxuser** command adds a PBX user and enters the PBX user view.

The **undo pbxuser** command deletes a PBX user.

By default, no PBX user is configured.

Format

pbxuser *name* [{ **pots** | **bra** | **sipue**} [**enterprise** *enterprise-name*]]

undo pbxuser *name*

Parameters

Parameter	Description	Value
name	Specifies the PBX user name.	The value is a string of 1 to 32 case-insensitive characters without spaces.
pots	Indicates that the PBX user type is POTS.	-
sipue	Indicates that the PBX user type is SIP UE.	-
bra	Indicates that the PBX user type is BRA	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
enterprise *enterprise-name*	Specifies the enterprise to which a PBX user belongs.	The value is a string of 1 to 32 characters without spaces. **NOTE** By default, the PBX user belongs enterprise name for the **default**.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When creating a PBX user, specify the PBX user type. After the PBX user is created, you do not need to enter the PBX user type in the user view.

Example

Create a PBX user **user001** and enter the PBX user view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
```

16.5.4.34 pbxuser-batch

Function

The **pbxuser-batch** command creates PBX users in a batch.

The **undo pbxuser-batch** command deletes PBX users in a batch.

By default, no PBX user is created.

Format

pbxuser-batch pots pbxuser *name* **port** *slotid/subcardid/portid* **number** *num-value*

pbxuser-batch sipue pbxuser *name* **sipue** *eid-value* **number** *num-value*

undo pbxuser-batch pbxuser *name* **number** *num-value*

Parameters

Parameter	Description	Value
pots	Indicates that the PBX user type is POTS.	-
pbxuser *name*	Specifies the initial PBX user name.	The value is a string of 1 to 16 digits without spaces.
port *slotid/subcardid/portid*	Indicates the slot ID/sub-card number/port number of the physical interface bound to the POTS user.	The value is a string of 1 to 15 characters. Enter a slash (/) between the slot ID, sub-card number, and port number. ● *slotid*: depends on product specifications. ● *subcardid*: depends on product specifications. ● *portid*: depends on product specifications.
number *num-value*	Specifies the number of users that are processed in a batch.	The value is an integer that ranges from 1 to 100.
sipue	Indicates that the PBX user type is SIP.	-
sipue *eid-value*	Specifies the initial device ID of a SIP user.	The value is a string of 1 to 32 digits without spaces.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario where multiple users are created in a batch, after the first user is created, the system starts to automatically generates user names of PBX users, port numbers of the physical interfaces bound to POTS users, and device IDs of SIP users. The values of *name*, *portid*, and *eid-value* are increased by 1 each time a user is created.

Prerequisites

- The SIP server has been configured on the AR when SIP users are created in a batch.
- The physical interface bound to POTS users has been created when POTS users are created in a batch.

Precautions

- When users are created in a batch, the user name of a PBX user will be the number allocated to the PBX user. The number of a PBX user needs to be used as the PBX user name.
- When multiple users as deleted in a batch, user names must contain only digits and strings have an increment of 1.
- Creating or deleting multiple users in a batch will fail if the initial user name is valid but the end user name is invalid.

Example

Create eight SIP users in a batch. If the device ID of the initial SIP user is 9000, the user names of the eight SIP users are 9000 to 9007.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] signalling-address ip 192.168.1.3 port 5060
[Huawei-voice-sipserver] media-ip 192.168.1.3
[Huawei-voice-sipserver] register-uri abcd.com
[Huawei-voice-sipserver] home-domain abcd.com
[Huawei-voice-sipserver] quit
[Huawei-voice] pbxuser-batch sipue pbxuser 9000 sipue 9000 number 8
```

Create four POTS users in a batch. If the initial user name is 9000, the user names of the four POTS users that are bound to 1/0/0 interfaces are 9000, 9001, 9002, and 9003.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser-batch pots pbxuser 9000 port 1/0/0 number 4
```

Delete four PBX users in a batch. If the initial use name is 9000, the user names of the four PBX users are 9000, 9001, 9002, and 9003.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] undo pbxuser-batch pbxuser 9000 number 4
```

16.5.4.35 pickupgroup-name

Function

The **pickupgroup-name** command specifies the name of a pickup group that PBX users belong to.

The **undo pickupgroup-name** command cancels the configuration.

By default, PBX users do not belong to any pickup group

Format

pickupgroup-name *pickupgroupname*

undo pickupgroup-name

Parameters

Parameter	Description	Value
pickupgroupname	Specifies the name of a pickup group that PBX users belong to.	The value is a string of 1 to 32 characters.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Specify the pickup group **abc** for PBX users.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser aaa pots
[Huawei-voice-pbxuser-aaa] pickupgroup-name abcd
```

16.5.4.36 port (PBX user view)

Function

The **port** command configures the port number for a POTS/BRA user.

By default, no port number is specified for the new POTS /BRA user.

Format

port *slotid/subcard/portid*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
slotid/subcard/portid	Specifies the slot ID/subcard ID/port number. This parameter identifies the location of the POTS user to be deleted. You must enter the slash (/).	The value is a string of 1 to 15 characters. The values of *slotid*, *subcardid*, and *portid* depend on the product model.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

N/A

Example

Configure a port number for the POTS user **user001**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 pots
[Huawei-voice-pbxuser-user001] port 2/0/1
```

16.5.4.37 priority (PBX user view)

Function

The **priority** command configures a user level.

The **undo priority** command restores the default user level.

By default, the user level is **default**.

Format

priority *priority-value*

undo priority

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
priority-value	Specifies a user level, High-level users can use the reserved resources or preemption relay occupied by low-level users to make outgoing calls relay.	Enumerated value. The options are as follows: ● default: default level ● normal: normal level ● advanced: advanced level ● super: highest level The default value is **default**.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the PBX user level to **normal**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser aaa pots
[Huawei-voice-pbxuser-aaa] priority normal
```

16.5.4.38 priority-group (voice view)

Function

The **priority-group** command creates call priority groups and enters the priority-group view.

The **undo priority-group** command deletes call priority groups.

By default, no call priority group is created.

Format

priority-group *priority-group-name*

undo priority-group *priority-group-name*

Parameters

Parameter	Description	Value
priority-group-name	Specifies the name of a call priority group.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Important calls to a PBX user cannot be connected when the PBX user is engaged in a call. In this case, a call priority group can be configured for the PBX user. User numbers are added to the group and the priority of each user is specified. If a high-priority user calls the PBX user during a conversation between the PBX user and another user, the current conversation is immediately interrupted and a call with the high-priority user is established.

Follow-up Procedure

Run the **telno** command to configure user numbers and the priority of each user, and associate the call priority group with a PBX user.

Example

Create a call priority group named **group1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] priority-group group1
```

Related Topics

16.5.4.12 display voice priority-group
16.5.4.39 priority-group (PBX user view)
16.5.4.43 telno (priority-group view)

16.5.4.39 priority-group (PBX user view)

Function

The **priority-group** command associates a PBX user with a call priority group.

The **undo priority-group** command deletes the call priority group associated with a PBX user.

By default, a PBX user is not associated with a call priority group.

Format

priority-group *priority-group-name*

undo priority-group

Parameters

Parameter	Description	Value
priority-group-name	Specifies the name of a call priority group.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Important calls to a PBX user cannot be connected when the PBX user is engaged in a call. In this case, a call priority group can be configured for the PBX user. User numbers are added to the group and the priority of each user is specified. If a high-priority user calls the PBX user during a conversation between the PBX user and another user, the current conversation is immediately interrupted and a call with the high-priority user is established.

Prerequisite

- A call priority group has been created.
- A PBX user has been created, and the mandatory parameters have been completed.

Precautions

Only SIP and POTS users can be associated with call priority groups using the **priority-group** command. A PBX user can be associated with one call priority group, but one call priority group can be associated with multiple PBX users.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the name of the call priority group associated with the PBX user 7001 to **group1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] priority-group group1
[Huawei-voice-priority-group-group1] telno 56628888 priority 0
[Huawei-voice-priority-group-group1] quit
[Huawei-voice] pbxuser 7001 sipue
[Huawei-voice-pbxuser-7001] sipue 7001
[Huawei-voice-pbxuser-7001] telno 7001
[Huawei-voice-pbxuser-7001] priority-group group1
```

Related Topics

16.5.4.12 display voice priority-group

16.5.4.33 pbxuser (voice view)

16.5.4.38 priority-group (voice view)

16.5.4.43 telno (priority-group view)

16.5.4.40 proxyreg-id (PBX user view)

Function

proxyreg-id command is used to configure a proxy register id for current user.

proxyreg-password command is used to configure a password for proxy register.

Format

proxyreg-id *id-value*

proxyreg-password cipher *password-value*

undo proxyreg-id

undo proxyreg-password

Parameters

Parameter	Description	Value
id-value	proxy register-id value	a string consisting of 1-32 characters
password-value	password for proxy register	a string consisting of 1-32 characters

Views

pbxuser view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level:

Usage Guidelines

By default, user is not configured with proxy register function.

As a local gateway, you want to use ports, we suggest you configure proxyreg-id and proxyreg-password (configure following local-survival view).

undo proxyreg-id command can cancel proxy register function.

Example

configure proxy register id *90000* and proxy register password *huawei123* for pbxuser 28980000.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] pbxuser 28980000 pots
 [Huawei-voice-pbxuser-28980000] proxyreg-id 90000
 [Huawei-voice-pbxuser-28980000] proxyreg-password cipher
 Please input user password(1-32 chars): *********
```

16.5.4.41 sipue (PBX user view)

Function

The **sipue** command configures the ID for a SIP UE user.

Format

sipue *eid-value*

Parameters

Parameter	Description	Value
eid-value	Specifies the ID of a SIP UE user.	The value is a string of 1 to 32 characters.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

N/A

Example

Configure the ID for the SIP UE user named **user001**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001 sipue
[Huawei-voice-pbxuser-user001] sipue 800
```

16.5.4.42 telno (PBX user view)

Function

The **telno** command configures numbers for a PBX user.

By default, numbers are configured for PBX users.

Format

telno *telno-value* [**long-telno** *longno-value*]

Parameters

Parameter	Description	Value
telno-value	Specifies a user number.	The value is a string of 1 to 16 characters.
long-telno *longno-value*	Specifies a long number.	The value is a string of 1 to 24 characters.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the long number of PBX user 1388 to 28291388.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser 1388
[Huawei-voice-pbxuser-1388]telno 1388 long-telno 28291388
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.4.43 telno (priority-group view)

Function

The **telno** command configures numbers of calling users and the priority of each user.

The **undo telno** command deletes calling numbers and priorities.

By default, no calling number and priority are configured.

Format

telno *telno-value* **priority** *priority-level*

undo telno *telno-value*

Parameters

Parameter	Description	Value
telno-value	Specifies a calling number.	The value is a string of 1 to 32 digits and symbols (including + and *) without spaces. The symbols + and * can be used only once, and the symbol + can be used only at the start of the string.
priority *priority-level*	Specifies the priority of a calling user.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.

Views

Priority-group view

Default Level

2: Configuration level

Usage Guidelines

Important calls to a PBX user cannot be connected when the PBX user is engaged in a call. In this case, a call priority group can be configured for the PBX user. User numbers are added to the group and the priority of each user is specified. If a high-priority user calls the PBX user during a conversation between the PBX user and another user, the current conversation is immediately interrupted and a call with the high-priority user is established.

 Copyright © Huawei Technologies Co., Ltd.

Numbers in a call priority group have higher priorities than those not configured in the call priority group.

Example

Set the priority of the number 56628888 in the call priority group group1 to **0**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] priority-group group1
[Huawei-voice-priority-group-group1] telno 56628888 priority 0
```

Related Topics

16.5.4.12 display voice priority-group

16.5.4.38 priority-group (voice view)

16.5.4.44 telno service-password cipher (PBX user view)

Function

The **telno service-password cipher** command configures the service password for a user.

The **undo telno service-password** command restores the default service password for a user.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

telno service-password cipher

undo telno service-password

Parameters

Parameter	Description	Value
cipher *password-value*	Specifies cipher text of a password. **NOTE** You can set *password-value* only after entering **cipher** and pressing **Enter**.	The value is a string of 6 characters without spaces.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

To configure the service password for a user, run **telno service-password cipher** command.

Example

Set the service password of a SIP UE user to **987654**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser 1388
[Huawei-voice-pbxuser-1388] telno service-password cipher
 Please input user password(6-6 chars):******
```

16.5.4.45 user-type (PBX user view)

Function

The **user-type** command specifies the user type.

The **undo user-type** command restores the default user type.

By default, users are common users.

Format

user-type *type*

undo user-type

Parameters

Parameter	Description	Value
type	Specifies the user type.	Enumerated type. The values are as follows: ● normal: indicates common users. ● priority-user: indicates users with priority. ● operator: indicates operators. ● card: indicates card users.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

N/A

Example

Configure PBX users as operators.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser aaa pots
[Huawei-voice-pbxuser-aaa] user-type operator
```

16.5.4.46 user-name

Function

The **user-name** command configures the name of a PBX user.

The **undo user-name** command deletes the name of a PBX user.

By default, no name is configured for a PBX user.

Format

user-name *user-name-value*

undo user-name

Parameters

Parameter	Description	Value
user-name-value	Specifies the name of a PBX user.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **user-name** command to configure the name of a PBX user for the name identification presentation service. For example, set the name of User B to **Jone**. Assume that the name identification presentation service is enabled for User A. When a call connection is established between User A and User B, the name of User B **Jone** is displayed to User A.

Prerequisite

A PBX user has been created and mandatory configurations have been performed. For details, see **Configuring a PBX User**.

Example

Set the name of the PBX user 7001 to **Jone**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser 7001 sipue
[Huawei-voice-pbxuser-7001] sipue 7001
[Huawei-voice-pbxuser-7001] telno 7001
[Huawei-voice-pbxuser-7001] user-name Jone
```

16.5.4.47 web-password (PBX user view)

Function

The **web-password** command is used to set the password for the PBX user to access the web self-help service system.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

web-password cipher

undo web-password

Parameters

None

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The password is in ciphertext during password setting.

After the **undo web-password** command is executed, the password is restored to the default one.

Example

Set the password of PBX user **2001** to **12345678**.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice] pbxuser 2001 sipue
[Huawei-voice-pbxuser-2001] sipue 2001
[Huawei-voice-pbxuser-2001] telno 2001
[Huawei-voice-pbxuser-2001] web-password cipher
 please input user password(6-32 chars):********
```

16.5.5 SBC Proxy configuration commands

16.5.5.1 display voice sbc media-relay

Function

Using the **display voice sbc media-relay** command, you can view the configured media relay interface and relay type.

Format

display voice sbc media-relay

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Display the media relay interface and relay type.

```
<Huawei> display voice sbc media-relay
 sbc media-relay interface Vlanif 100 internal
```

Table 16-67 Description of the display voice sbc media-relay command output

Item	Description
sbc media-relay interface Vlanif 100 internal	The media relay interface is VLANIF 100 and the relay type is internal. Enumerated type. The values are as follows: ● external: an external network ● internal: an internal network By default, the media relay type is internal.

16.5.5.2 media-bandwidth-control media-proxy enable

Function

The **media-bandwidth-control media-proxy enable** command enables CAC on an SBC proxy.

The **undo media-bandwidth-control media-proxy enable** command disables CAC on an SBC proxy.

By default, CAC is disabled on an SBC proxy.

Format

media-bandwidth-control media-proxy enable

undo media-bandwidth-control media-proxy enable

Parameters

None

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a SIP UE user registered through the SBC proxy makes a call, the SBC proxy media bandwidth is occupied. More voice calls occupy more SBC proxy media bandwidth. To improve the voice communication quality, run the **media-bandwidth-control media-proxy enable** command to enable CAC on the SBC proxy.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **media-bandwidth-control media-proxy max-bandwidth** command to set the maximum SBC proxy media bandwidth.

Example

Enable CAC on the SBC proxy.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] media-bandwidth-control media-proxy enable
```

16.5.5.3 media-bandwidth-control media-proxy max-bandwidth

Function

The **media-bandwidth-control media-proxy max-bandwidth** command sets the maximum media bandwidth on an SBC proxy.

The **undo media-bandwidth-control media-proxy max-bandwidth** command restores the default maximum media bandwidth on an SBC proxy.

By default, the maximum media bandwidth on an SBC proxy is 500000 kbit/s.

Format

media-bandwidth-control media-proxy max-bandwidth *max-bandwidth-value*

undo media-bandwidth-control media-proxy max-bandwidth

Parameters

Parameter	Description	Value
max-bandwidth-value	Specifies the maximum media bandwidth on an SBC proxy.	The value is an integer that ranges from 1 to 5000, in 100 kbit/s. The default value is 5000, that is, 500000 kbit/s.

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **media-bandwidth-control media-proxy max-bandwidth** command sets the maximum media bandwidth on an SBC proxy after CAC is enabled on the SBC proxy by using the **media-bandwidth-control media-proxy enable** command. If the **media-bandwidth-control media-proxy max-bandwidth** command is not run, and CAC is enabled on the SBC proxy, the default maximum media bandwidth is 500000 kbit/s. When the media bandwidth on the SBC proxy is used up, the system limits new calls that occupy the media bandwidth on the SBC proxy.

Prerequisites

- CAC has been enabled on the SBC proxy using the **media-bandwidth-control media-proxy enable** command.

Example

Set the maximum bandwidth on the SBC proxy to 400000 kbit/s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] media-bandwidth-control media-proxy enable
[Huawei-voice-sipserver] media-bandwidth-control media-proxy max-bandwidth 4000
```

16.5.5.4 sbc mapped-media-ip

Function

Using the **sbc mapped-media-ip** command, you can configure a media IP address for a SIP server or a SIP trunk group.

Using the **undo sbc mapped-media-ip** command, you can delete the media IP address of a SIP server or a SIP trunk group.

By default, no media IP address is configured for a SIP server or a SIP trunk group.

Format

sbc mapped-media-ip *ip-address*

undo sbc mapped-media-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the media IP address of a SIP server or a SIP trunk group.	The value is in dotted decimal notation.

Views

SIP server view, trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the media IP address of a SIP server to 192.168.2.12.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] sbc mapped-media-ip 192.168.2.12
```

16.5.5.5 sbc mapped-media-port-start

Function

Using the **sbc mapped-media-port-start** command, you can configure a start media port number for a SIP server or a SIP trunk group.

Using the **undo sbc mapped-media-port-start** command, you can delete the start media port number of a SIP server or a SIP trunk group.

By default, no start media port number is configured for a SIP server or a SIP trunk group.

Format

sbc mapped-media-port-start *port-value*

undo sbc mapped-media-port-start

Parameters

Parameter	Description	Value
port-value	Specifies the start media port number of a SIP server or a SIP trunk group.	The value is an integer that ranges from 1 to 65535.

Views

SIP server view, trunk group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Media ports 61728 to 65535 are supported. M indicates the maximum number of online users and N indicates the start port number (N + Mx4 <= 65535). The device specifications are as follows:

- The AR150 supports a maximum of 20 concurrent users.
- The AR200 supports a maximum of 30 concurrent users.
- The AR1240 support a maximum of 64 concurrent users.
- The AR1220 supports a maximum of 125 concurrent users.
- The AR2204 support a maximum of 125 concurrent users.
- The AR2220 support a maximum of 250 concurrent users.
- The AR2240 support a maximum of 1000 concurrent users.
- The AR3260 supports a maximum of 2000 concurrent users.

Example

Set the start media port number of a SIP server to 64000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] sbc mapped-media-port-start 64000
```

16.5.5.6 sbc mapped-media-proxy-port-start

Function

Using the **sbc mapped-media-proxy-port-start** command, you can configure a start media port number for a SIP server or a SIP trunk group.

Using the **undo sbc mapped-media-proxy-port-start** command, you can delete the start media port number of a SIP server or a SIP trunk group.

By default, no start media port number is configured for a SIP server or a SIP trunk group.

Format

sbc mapped-media-proxy-port-start *port-value*

undo sbc mapped-media-proxy-port-start

Parameters

Parameter	Description	Value
port-value	Specifies the start media port number of a SIP server or a SIP trunk group.	The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP server view, trunk group view

Default Level

2: Configuration level

Usage Guidelines

The device supports media port numbers 59392 to 61439. When media proxy is used, four port numbers 61436 to 61439 are required. The start media port number and must be smaller than or equal to 61436.

Example

Set the start media port number of a SIP server to 59392.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] sbc mapped-media-proxy-port-start 59392
```

16.5.5.7 sbc mapped-signalling-address

Function

The **sbc mapped-signalling-address** command configures a public IP address and port number for the signaling mapping of the SIP server or SIP trunk group.

The **undo sbc mapped-signalling-address** command deletes the configured public IP address and port number for the signaling mapping for the SIP server or SIP trunk group.

By default, the public IP address and port number are not configured for a SIP server or a SIP trunk group.

Format

sbc mapped-signalling-address ip *ip-address* **port** *port-value*

undo sbc mapped-signalling-address

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies the signaling IP address of a SIP server or a SIP trunk group.	The value is in dotted decimal notation.
port*port-value*	Specifies the signaling port number of a SIP server or a SIP trunk group.	The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP server view, trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the public IP address to **192.168.2.12** and port number to **5062** for the signaling mapping of the SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] sbc mapped-signalling-address ip 192.168.2.12 port 5062
```

16.5.5.8 sbc media-proxy

Function

Using the **sbc media-proxy** command, you can configure a media proxy policy for a SIP server or a SIP trunk group.

Using the **undo sbc media-proxy** command, you can restore the default media proxy policy of a SIP server or a SIP trunk group.

By default, no media proxy policy is configured for a SIP server or a SIP trunk group.

Format

sbc media-proxy { **enable** | **disable** | **auto** }

undo sbc media-proxy

Parameters

Parameter	Description	Value
enable	A media proxy is enabled.	-
disable	A media proxy is disabled.	-
auto	A media proxy is enabled automatically.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP server view, trunk group view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable media proxy for a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] sbc media-proxy enable
```

16.5.5.9 sbc media-relay

Function

Using the **sbc media-relay** command, you can configure the media relay interface and relay type.

Using the **undo sbc media-relay** command, you can delete the configured media relay interface and relay type.

By default, the media relay interface and relay type are not configured.

Format

sbc media-relay interface *interface-type interface-numberrelay-type*

undo sbc media-relay interface *interface-type interface-numberrelay-type*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	-

Parameter	Description	Value
relay-type	Specifies the media relay type.	Enumerated type. The values are as follows: ● external: an external network ● internal: an internal network By default, the media relay type is internal.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the media relay type to **internal**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sbc media-relay interface GigabitEthernet 0/0/0 internal
```

16.5.5.10 sbc signalling-proxy

Function

Using the **sbc signalling-proxy** command, you can configure a signaling proxy policy for a SIP server.

Using the **undo sbc signalling-proxy** command, you can restore the default signaling proxy policy of a SIP server.

By default, signaling proxy is disabled for a SIP server.

Format

sbc signalling-proxy { **enable** | **disable** | **auto** }

undo sbc signalling-proxy

Parameters

Parameter	Description	Value
enable	A media proxy is enabled.	-
disable	A media proxy is disabled.	-
auto	A media proxy is enabled automatically.	-

Views

SIP server view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable signaling proxy for a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] sbc signalling-proxy enable
```

16.5.6 Trunk Group configuration commands

16.5.6.1 auto-connect-controlchannel

Function

The **auto-connect-controlchannel** command configures whether the H323 protocol supports automatic establishment of H245 channels.

The **undo auto-connect-controlchannel** command restores the default configuration.

By default, H245 channels cannot be automatically established.

Format

auto-connect-controlchannel { **enable** | **disable** }

undo auto-connect-controlchannel

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
enable	Enables automatic establishment of H245 channels.	-
disable	Disables automatic establishment of H245 channels.	-

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the H323 protocol to automatically set up H245 channels.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] auto-connect-controlchannel enable
```

16.5.6.2 callproc-wait-response-timeout

Function

The **callproc-wait-response-timeout** command sets the timeout interval for the Alerting or Connect message from the called party.

The **undo callproc-wait-response-timeout** command restores the default timeout.

The default timeout is 500000 ms.

Format

callproc-wait-response-timeout *callproc-wait-response-timeout-value*

undo callproc-wait-response-timeout

Parameters

Parameter	Description	Value
callproc-wait-response-timeout-value	Specifies the timeout interval for the Alerting or Connect message from the called party.	The value is an integer that ranges from 10000 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the timeout to 50000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] callproc-wait-response-timeout 50000
```

16.5.6.3 callroute (trunk group view)

Function

The **callroute** *callroute-name* command binds a call route to a trunk group.

The **undo callroute** *callroute-name* command unbinds a call route from a trunk group.

Format

callroute *callroute-name* [[[**time** *time-name* | **callertelno** *callertelno-value*] * | **charge** *charge-value* | **percent** *percent-value* | **userpriorlevel** *userpriorilevel-value*] | [**select-level** *select-level-value*]] *

undo callroute *callroute-name* [**select-level**]

Parameters

Parameter	Description	Value
callroute-name	Specifies the name of a call route.	The value is a string of 1 to 32 characters.
time-name	Specifies the name of a time index.	The value is a string of 1 to 32 characters.
charge-value	Specifies the charge rate.	The value is an integer that ranges from 0 to 65535. The default value is 65535.
percent-value	Specifies a percentage.	The value is an integer that ranges from 0 to 100. The default value is 100.
userpriorlevel-value	Specifies a user level.	Enumerated value. The value can be **default**, **normal**, **advanced**, or **super**. The default value is **default**.
callertelno-value	Specifies a calling number.	The value is a string of 1 to 32 characters.
select-level-value	Line selection level of a trunk under a route.	The value is an integer that ranges from 0 to 254. The default value is 254.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Bind the call route **test** to a trunk group and set the route selection policy to **perloadshare**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callroute test
[Huawei-voice-callroute-test] selecttype perloadshare
[Huawei-voice-callroute-test] quit
[Huawei-voice] trunk-group huawei sip trunk-circuit
[Huawei-voice-trunkgroup-huawei] callroute test percent 20
```

16.5.6.4 callsource (trunk group view)

Function

The **callsource** command configures the call source for trunk groups.

The **undo callsource** command restores the default call source for trunk groups.

Format

callsource *callsource-name*

undo callsource

Parameters

Parameter	Description	Value
callsource-name	Specifies a call source.	The value is a string of 1 to 32 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the call source for trunk groups to **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sipip
[Huawei-voice-trunkgroup-sipip] callsource test
```

16.5.6.5 channels-timeout

Function

The **channels-timeout** command sets the channel establishment timeout.

The **undo channels-timeout** command restores the default channel establishment timeout.

By default, the channel establishment timeout is 15000 ms.

 Copyright © Huawei Technologies Co., Ltd.

Format

channels-timeout *channels-timeout-value*

undo channels-timeout

Parameters

Parameter	Description	Value
channels-timeout-value	Specifies the channel establishment timeout.	The value is an integer that ranges from 0 to 4294967295, in seconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the channel establishment timeout to 50000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] channels-timeout 50000
```

16.5.6.6 circuit-state-relate (trunk group view)

Function

The **circuit-state-relate** command associates a trunk group with trunk groups.

The **undo circuit-state-relate** command configures trunk groups associated with a trunk group.

By default, a trunk group is not associated with any trunk group.

Format

circuit-state-relate *trunk-group-name*

undo circuit-state-relate *trunk-group-name*

Parameters

Parameter	Description	Value
trunk-group-name	Indicates names of trunk groups associated with a trunk group.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the trunk tandem scenario, a router accesses to an IMS network through SIP trunks, and connects to the PBX through PRA or BRA trunks. When the SIP trunks are faulty, the PBX cannot detect the fault. Inter-office calls are sent to the router through the PRA or BRA trunks, and services are affected.

In the SIP trunk group view, run the **circuit-state-relate** command to associate the SIP trunk group with the PRA or BRA trunk group. If the SIP trunk group is faulty, the status of the trunk group associated with the SIP trunk group synchronously changes to Disconnected. When detecting the fault, the PBX or IMS immediately switches services to the backup link or processes services in other ways. After the fault is rectified, the status of the trunk group associated with the SIP trunk group automatically changes to Normal.

Prerequisites

The trunk groups to be associated have been created.

Precautions

- A SIP trunk group can be associated with BRA trunk groups and PRA trunk groups.
- A PRA trunk group can be associated with SIP trunk groups.
- Trunk groups of other types cannot be associated with any trunk group.

Example

Associate a SIP trunk group named **huawei** with a BRA trunk group named **bra**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group bra bra-dss1
[Huawei-voice-trunkgroup-bra] quit
[Huawei-voice] trunk-group test sip trunk-group
[Huawei-voice-trunkgroup-test] circuit-state-relate bra
```

16.5.6.7 codec-priority(trunk group view)

Function

Using the **codec-priority** command, you can configure the codec priority, codec value, and packetization time for a SIP trunk group.

Using the **undo codec-priority** command, you can restore the default settings of the codec priority, codec value, and packetization time of a SIP trunk group.

The default values of the codec priority, codec value, and packetization time is shown in **Table 16-68**.

Format

codec-priority *pri-value codec-value pt-value*

undo codec-priority *pri-value*

Parameters

Parameter	Description	Value
pri-value	Indicates the codec priority.	The value is an integer that ranges from 0 to 7. A smaller value indicates a higher priority.
codec-value	Indicates the codec value.	Enumerated value. The value ranges from 0 to 252. The options are as follows: • 0: G711U • 2: G726 • 4: G723 • 8: G711A • 9: G722 • 15: G728 • 18: G729 • 20: G723Low • 21: G726-16 • 22: G726-24 • 23: G726-40 • 96: R2198 • 97: R2833 • 98: v150 • 99: clearmode • 250: T.38 • 251: T.38+2

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pt-value	Indicates the packetization time.	The value is an integer that ranges from 0 to 6, in milliseconds. • 0: 5 ms • 1: 10 ms • 2: 20 ms • 3: 30 ms • 4: 40 ms • 5: 50 ms • 6: 60 ms

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

The default values are shown in **Table 16-68**.

Table 16-68 The default values

Codec Priority	Codec Value	Packetization Time
0	8	20
1	0	20
2	18	10
3	4	30
4	8	10
5	8	30
6	0	10
7	250	20

Example

Set the codec priority to 2, codec value to 2, and packetization time to 80 for the SIP trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] codec-priority 2 2 80
```

16.5.6.8 cs-mode (trunk group view)

Function

Using the **cs-mode** command, you can configure the reliable transmission mode for a SIP trunk group.

By default, no reliable transmission mode is configured for a SIP trunk group.

Format

cs-mode *mode-value*

Parameters

Parameter	Description	Value
mode-value	Indicates the reliable transmission mode.	Enumerated type. The value is client, server, or client_server.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

The reliable transmission mode is valid only when the transmission mode of the SIP trunk (**16.5.6.118 transfer (trunk group view)**) group is **tcp** or **tls**.

Example

Set the reliable transmission mode for the SIP trunk group **001** to client_server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 001
[Huawei-voice-trunkgroup-001] cs-mode client_server
```

16.5.6.9 custom-right (trunk group view)

Function

The **custom-right** command binds customized 32-level rights to a trunk group.

By default, no 32-level right is bound to a trunk group.

Format

custom-right {*c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32*}

undo custom-right [*c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32*]

Parameters

Parameter	Description	Value
c1 | *c2* | *c3* | *c4* | *c5* | ...| *c32*	Specifies 32-level rights to be bound to a trunk group.	The value can be one or more of **c1** to **c32**.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Rights of a trunk group are restricted in voice call scenarios where a trunk group is the calling party, that is, scenarios of trunk-based incoming calls.

By default, no 32-level right is bound to a trunk group. You can configure 1 to 32 customized rights.

Adding or deleting a right does not affect existing 32-level rights.

To clear all 32-level rights bound to a trunk group, run the **undo custom-right** command.

Example

Bind 32-level rights **c4**, **c8**, and **c12** to trunk group **at0**.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] trunk-group at0 fxo
 [Huawei-voice-trunkgroup-at0] custom-right c4 c8 c12
```

Unbind 32-level right **c4** from trunk group **at0**.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] trunk-group at0
 [Huawei-voice-trunkgroup-at0] undo custom-right c4
```

Clear all 32-level rights bound to trunk group **at0**.

```
<Huawei> system-view
 [Huawei] voice
 [Huawei-voice] trunk-group at0
 [Huawei-voice-trunkgroup-at0] undo custom-right
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.10 default-caller-telno (trunk view)

Function

The **default-caller-telno** command configures the default number displayed for a trunk group.

The **undo default-caller-telno** command deletes the default number displayed for a trunk group.

Format

default-caller-telno *telno-value*

undo default-caller-telno

Parameters

Parameter	Description	Value
telno-value	Indicates the default number displayed.	The value is a string of 1 to 24 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

The **default-caller-telno** command will be effective when at0 trunk-group, bra trunk-group, or pra trunk-group cannot obtain the calling number.

Example

Set the default phone number of a trunk group to 123456.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group at0 fxo
[Huawei-voice-trunkgroup-at0] default-caller-telno 123456
```

16.5.6.11 del-techprefix

Function

The **del-techprefix** command configures whether to delete a technical prefix.

The **undo del-techprefix** command restores the default configuration.

By default, the technical prefix is not deleted.

 Copyright © Huawei Technologies Co., Ltd.

Format

del-techprefix *h323-send-techprefix-value*

undo del-techprefix

Parameters

Parameter	Description	Value
h323-send-techprefix-value	Indicates whether to delete the technical prefix.	The value is enable or disable: ● enable: deletes the technical prefix. ● disable: keeps the technical prefix.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

The received numbers contain technical prefixes. If call routing is based on numbers, the technical prefixes must be deleted.

Example

Retain the technical prefix.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 register-gateway
[Huawei-voice-trunkgroup-test] del-techprefix disable
```

16.5.6.12 description (trunk group view)

Function

Using the **description** command, you can configure the description of a trunk group.

Using the **undo description** command, you can cancel the description of a trunk group.

Format

description *desc-value*

undo description

Parameters

Parameter	Description	Value
desc-value	Indicates the description of a trunk group.	The value is a string of 1 to 64 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the description **huawei** for the trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] description huawei
```

16.5.6.13 digest-username

Function

The **digest-username** command configures the authentication digest user name when the SIP trunk registration mode is trunk group registration.

The **undo digest-username** command deletes the authentication digest user name when the SIP trunk registration mode is trunk group registration.

No authentication digest user name is configured when the SIP trunk registration mode is trunk group registration.

Format

digest-username *digest-username-value*

undo digest-username

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
digest-username-value	Specifies the authentication digest user name.	The value is a string of 1 to 32 case-sensitive characters without spaces and question mark (?).

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

When a SIP trunk group that has the authentication digest user name configured and uses trunk group registration registers with the peer device, the SIP trunk group encrypts the authentication digest user name and sends it to the peer device for authentication. If the authentication digest user name is not configured, the trunk group encrypts the registration ID and sends it to the peer end for authentication.

NOTE

The authentication digest user name is used only when the SIP trunk registration mode is trunk group registration.

Example

Set the authentication digest user name to abcd for the trunk group **sippra**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sippra sip trunk-group
[Huawei-voice-trunkgroup-sippra] digest-username abcd
```

16.5.6.14 display voice gatekeeper callprefix

Function

The **display voice gatekeeper callprefix** command displays information about the prefix used by the H.323 trunk registered with a gatekeeper.

Format

display voice gatekeeper callprefix

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After a gateway successfully registers with a gatekeeper through an H.323 trunk, dynamic prefix information is generated on the gatekeeper. You can run the **display voice gatekeeper callprefix** command to check the dynamic prefix information, including the call prefixes registered on the gateway and generated by the gatekeeper for planning call policies.

Example

Display information about the prefix used by the H.323 trunk registered with a gatekeeper.

```
<Huawei> display voice gatekeeper callprefix
 Spec:  500, Records: 4
 ----------------------------------------------------------------------
 Callprefix        Type        H323ID          IP              Port
 60000             register    gateway1        192.168.1.1     1720
 60001             register    gateway2        192.168.1.2     1720
 *99*             config       -               -               -
 #99*              config      -               -               -
```

Table 16-69 Description of the **display voice gatekeeper callprefix** command output

Item	Description
Spec	Total space of prefix information.
Records	Number of records.
Callprefix	Call prefix.
Type	Prefix type.
H323ID	Gateway ID.
IP	Signaling address of a call.
Port	Signaling port of a call.

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.15 display voice gatekeeper endpoints

Function

The **display voice gatekeeper endpoints** command displays the dynamic information of a gateway registered with the H.323 trunk of a gatekeeper.

Format

display voice gatekeeper endpoints

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After the H.323 trunk group is deployed on a gatekeeper and a gateway registers with the gatekeeper, the gatekeeper records the registration information of the gateway. You can run the **display voice gatekeeper endpoints** to check information about all gateways registered with the gatekeeper.

Example

Display the dynamic information of a gateway registered with the H.323 trunk of a gatekeeper.

```
<Huawei> display voice gatekeeper endpoints
 Spec: 150, Records: 1
 ------------------------
 GatekeeperID       : gatekeeper
 H323ID             : gateway
 CallSignalIP       : 192.168.1.1
 CallSignalPort     : 1720
 RASSignalIP        : 192.168.1.1
 RASSignalPort      : 1719
 State              : Idle
```

Table 16-70 Description of the **display voice gatekeeper endpoints** command output

Item	Description
Spec	Total space of the gateways that allow registrations.

Item	Description
Records	Number of records.
GatekeeperID	Gatekeeper ID.
H323ID	Gateway ID.
CallSignalIP	Signaling address of a call.
CallSignalPort	Signaling port of a call.
RASSignalIP	Address of the RAS message.
RASSignalPort	Port of the RAS message.
State	Registration status of a gateway.

16.5.6.16 display voice h323 app-time

Function

The **display voice h323 app-time** command displays the H323 trunk group timers.

Format

display voice h323 app-time

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the H323 trunk group timers.

```
<Huawei> display voice h323 app-time
    Timer index : 0        Timer value : 15000ms
    Timer index : 1        Timer value : 120000ms
    Timer index : 2        Timer value : 180000ms
    Timer index : 3        Timer value : 15000ms
```

```
Timer index : 4        Timer value : 30000ms
Timer index : 5        Timer value : 1000ms
Timer index : 6        Timer value : 5000ms
Timer index : 7        Timer value : 10000ms
Timer index : 8        Timer value : 60000ms
Timer index : 9        Timer value : 5000ms
Timer index : 10       Timer value : 60000ms
Timer index : 11       Timer value : 17000ms
Timer index : 12       Timer value : 3000ms
Timer index : 13       Timer value : 5000ms
Timer index : 14       Timer value : 5000ms
Timer index : 15       Timer value : 180000ms
Timer index : 16       Timer value : 300000ms
Timer index : 17       Timer value : 222222ms
Timer index : 18       Timer value : 12000ms
Timer index : 19       Timer value : 0ms
Timer index : 20       Timer value : 4294967295ms
Timer index : 21       Timer value : 4294967295ms
Timer index : 22       Timer value : 4294967295ms
Timer index : 23       Timer value : 4294967295ms
Timer index : 24       Timer value : 4294967295ms
Timer index : 25       Timer value : 4294967295ms
Timer index : 26       Timer value : 15000ms
Timer index : 27       Timer value : 15000ms
Timer index : 28       Timer value : 15000ms
Timer index : 29       Timer value : 60000ms
Timer index : 30       Timer value : 60000ms
Timer index : 31       Timer value : 15000ms
Timer index : 32       Timer value : 15000ms
Timer index : 33       Timer value : 15000ms
Timer index : 34       Timer value : 15000ms
Timer index : 35       Timer value : 5000ms
Timer index : 36       Timer value : 50000ms
Timer index : 37       Timer value : 60000ms
Timer index : 38       Timer value : 3000ms
Timer index : 39       Timer value : 10000ms
Timer index : 40       Timer value : 3600000ms
Timer index : 41       Timer value : 4294967295ms
Timer index : 42       Timer value : 4294967295ms
Timer index : 43       Timer value : 4294967295ms
Timer index : 44       Timer value : 4294967295ms
Timer index : 45       Timer value : 4294967295ms
Timer index : 46       Timer value : 4294967295ms
Timer index : 47       Timer value : 4294967295ms
Timer index : 48       Timer value : 4294967295ms
Timer index : 49       Timer value : 4294967295ms
Timer index : 50       Timer value : 4294967295ms
Timer index : 51       Timer value : 4294967295ms
```

Table 16-71 Description of the display voice h323 app-time command output

Item	Description
Timer index :	Indicates the timer index. Each timer has a unique index. For description about the timer indexes, see **h323-app-timer**.
Timer value :	Indicates the timer value. For the default timer values, see **h323-app-timer**.

16.5.6.17 display voice h323 config

Function

The **display voice h323 config** command displays H323 parameters.

Format

display voice h323 config

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the H323 parameters.

```
<Huawei>display voice h323 config
  System name                      : HUAWEI
  Product name                     : HUAWEI-AR
  H323 version                     : V4
  H245 version                     : V4
  Display name                     : HUAWEI
  LocalIP                          : 192.168.2.22
  RAS port                         : 1719
  Q931 listen port                 : 1720
  Workmode                         : international
  Tcp keep alive time out          : 3600ms
  Support h245 tunnel              : Enable
  Faststart flag                   : Enable
  Auto connect control channel     : Disable
  Earlyh245                        : Disable
  Tcp connection time out          : 15000ms
  Setup wait response time out     : 500000ms
  Callproc wait response time out  : 500000ms
  Recvalert wait response time out : 500000ms
  Channels time out                : 15000ms
  Roundtrip delay time out         : 15000ms
  Request channel close time out   : 15000ms
  Requestmode time out             : 15000ms
  Medialoop time out               : 15000ms
  Endsession time out              : 3000ms
<Huawei>
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-72 Description of the display voice h323 config command output

Item	Description
System name	H323 system name.
Product name	H323 product name.
H323 version	H323 protocol version, including V2, V3, V4, and V5. The default version is V4.
H245 version	H245 protocol version, including V2, V3, V4, and V5. The default version is V4.
Display name	display header field in the Q931 message.
LocalIP	Local IP address.
RAS port	UDP port number of RAS signals.
Q931 listen port	Q931 listening port.
Workmode	Operation mode of the H323 stack, including international, national, and VT. The default mode is international.
Tcp keep alive time out	TCP keepalive timer value.
Support h245 tunnel	Whether the H245 control signaling channel is supported.
Faststart flag	Whether the fast start function is enabled.
Auto connect control channel	Whether the H245 channel can be automatically established.
Earlyh245	Whether the Setup message contains the H245 address.
Tcp connection time out	TCP connection timeout interval.
Setup wait response time out	Timeout interval for the Callproceeding, Alerting, or Connect response.
Callproc wait response time out	Timeout interval for the Alerting or Connect response.
Recvalert wait response time out	Timeout interval for the Connect response.
Channels time out	Channel establishment timeout interval.
Roundtrip delay time out	Roundtrip timeout interval.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Request channel close time out	Timeout interval for the logical channel close response.
Requestmode time out	Timeout interval for mode switching request response.
Medialoop time out	Media loopback timeout interval.
Endsession time out	EndSessionCommand timeout interval.

16.5.6.18 display voice h323 running

Function

The **display voice h323 running** command displays H323 running parameters.

Format

display voice h323 running

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display H323 running parameters.

```
<Huawei> display voice h323 running
  System name                    : HUAWEI
  Product name                   : HUAWEI
  H323 version                   : V4
  H245 version                   : V4
  Display name                   : HUAWEI
  LocalIP                        : 192.168.0.1
  RAS port                       : 1720
  Q931 listen port               : 1280
  Workmode                       : international
  Tcp keep alive time out        : 3600ms
  Support h245 tunnel            : Disable
  Faststart flag                 : Enable
```

```
Auto connect control channel     : Disable
Earlyh245                        : Disable
Tcp connection time out          : 15000ms
Setup wait response time out     : 500000ms
Callproc wait response time out  : 500000ms
Recvalert wait response time out : 500000ms
Channels time out                : 15000ms
Request channel close time out   : 15000ms
Requestmode time out             : 15000ms
Endsession time out              : 3000ms
Init status                      : Initsucceed
```

Table 16-73 Description of the display voice h323 running command output

Item	Description
System name	H323 system name.
Product name	H323 product name.
H323 version	H323 protocol version, including V2, V3, V4, and V5. The default version is V4.
H245 version	H245 protocol version, including V2, V3, V4, and V5. The default version is V4.
Display name	display header field in the Q931 message.
LocalIP	Local IP address.
RAS port	UDP port number of RAS signals.
Q931 listen port	Q931 listening port.
Workmode	Operation mode of the H323 stack, including international, national, and VT. The default mode is international.
Tcp keep alive time out	TCP keepalive timer value.
Support h245 tunnel	Whether the H245 control signaling channel is supported.
Faststart flag	Whether the fast start function is enabled.
Auto connect control channel	Whether the H245 channel can be automatically established.
Earlyh245	Whether the Setup message contains the H245 address.
Tcp connection time out	TCP connection timeout interval.
Setup wait response time out	Timeout interval for the Callproceeding, Alerting, or Connect response.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Callproc wait response time out	Timeout interval for the Alerting or Connect response.
Recvalert wait response time out	Timeout interval for the Connect response.
Channels time out	Channel establishment timeout interval.
Request channel close time out	Timeout interval for the logical channel close response.
Requestmode time out	Timeout interval for mode switching request response.
Endsession time out	EndSessionCommand timeout interval.
Init status	Initialization status of the H323 stack, including: ● Initsucceed: initialization is successful. ● Initfailed: initialization is failed. ● Meminitsucceed: memory initialization is successful. ● Meminitfailed: memory initialization is failed. ● Cfgsucceed: H323 stack configuration is successful. ● Cfgfailed: H323 stack configuration is failed.

16.5.6.19 display voice r2 profile

Function

Using the **display voice r2 profile** command, you can view the E1R2 profile configuration.

Format

display voice r2 profile [*profile-name*]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an E1R2 profile.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If *profile-name* is not specified, the **display voice r2 profile** command displays the configuration of all E1R2 profiles.

Example

Display the configuration of the E1R2 profile **test**.

```
<Huawei> display voice r2 profile test
 -------------------------------------------------------
                R2 signalling profile
 -------------------------------------------------------
 name:                      test
 signalling-type-name:     standard
 -------------------------------------------------------
                R2 register signalling attribute
 -------------------------------------------------------
 InType                  : 0
 OutType                 : 0
 BackPulseTime           : 150ms
 SendVoltage             : 13dBm
 DtmfSendIntervalTime    : 68ms
 CompSeqKeepTime         : 40000ms
 DtmfSendTime            : 68ms
 NumberMaxInterval       : 50s
 RecNumMaxInterval       : 50s
 SignalStopPerTime       : 15s
 WaitCallCategoryTime    : 50s
 WaitBSigTime            : 50s
 NumberSendMode          : delay
 CallNumberSendLen       : 12
 IsSendPulseSignal       : disable
 -------------------------------------------------------
                R2 register address send
 -------------------------------------------------------
 ProfileName            : test
 CallingNumber          : enable
 CalledNumber           : enable
 CallingUserType        : enable
 EchoCancellation       : disable
 CountryCode            : disable
 DistinctiveIndication : disable
 CircuitCharacter       : disable
 CallingUserPriority    : disable
 -------------------------------------------------------
                R2 register address receive
 -------------------------------------------------------
 ProfileName            : test
 CallingNumber          : enable
 CalledNumber           : enable
 CallingUserType        : enable
 EchoCancellation       : disable
 CountryCode            : disable
 DistinctiveIndication : disable
 CircuitCharacter       : disable
 CallingUserPriority    : disable
```

```
CidPostion            : 1
CalltypePostion       : 1
-----------------------------------------------------------
                R2 line signal
-----------------------------------------------------------
Profile-name:                        test
seize ack time:                      5000ms
wait answering signal time:          300s
wait front line-releasing duration:  200ms
wait protecting duration:            200ms
line signal type:                    1
```

Table 16-74 Description of the display voice r2 profile command output

Item	Description
R2 register signalling attribute	R2 signaling attribute.
InType	Incoming signaling type.
OutType	Outgoing signaling type.
BackPulseTime	Backward pulse duration.
SendVoltage	Transmitting voltage.
DtmfSendIntervalTime	Interval at which DTMF signals are sent.
CompSeqKeepTime	Keepalive time of the register signaling compelling sequence.
DtmfSendTime	Period during which DTMF signals are sent.
NumberMaxInterval	Interval at which the calling number is sent.
RecNumMaxInterval	Interval at which digits are collected.
WaitCallCategoryTime	Period from the time to request the caller category to the time to receive the caller category.
WaitBSigTime	Period from the time to request group B signals to the time to receive group B signals.
NumberSendMode	Digit collection mode.
CallNumberSendLen	Maximum length of the calling number.
IsSendPulseSignal	Whether the end-of-pulsing signal is sent.
R2 register address send	Output register address format.
ProfileName	R2 profile name.
CallingNumber	Whether the calling number is sent.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CalledNumber	Whether the called number is sent.
CallingUserType	Whether the calling user type is sent.
EchoCancellation	Whether echo cancellation information is sent.
CountryCode	Whether the country code is sent.
DistinctiveIndication	Whether the distinctive indication is sent.
CircuitCharacter	Whether the circuit character is sent.
CallingUserPriority	Whether the calling user priority is sent.
R2 register address receive	Input register address format.
Profilename	R2 profile name.
CallingNumber	Whether the calling number is received.
CalledNumber	Whether the called number is received.
CallingUserType	Whether the calling user type is received.
EchoCancellation	Whether echo cancellation information is received.
CountryCode	Whether the country code is received.
DistinctiveIndication	Whether the distinctive indication is received.
CircuitCharacter	Whether the circuit character is received.
CallingUserPriority	Whether the calling user priority is received.
CidPostion	Calling number location.
CalltypePostion	Calling user type location.
R2 line signal	Line signaling attribute.
Profile-name	R2 profile name.
seize ack time	Waiting time for signal seizing acknowledgement.
wait answering signal time	Time at which answer signals are identified.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
wait front line-releasing duration	Time at which clear-forward (CLF) signals are identified.
wait protecting duration	Protection duration.
line signal type	R2 line signaling type.

16.5.6.20 display voice r2 signalling-type

Function

Using the **display voice r2 signalling-type** command, you can view the configuration of an E1R2 signaling type.

Format

display voice r2 signalling-type [*signalling-type-name* [**register-signal-send** | **register-signal-receive** | **line-signal-send** | **line-signal-receive**]]

Parameters

Parameter	Description	Value
signalling-type-name	Specifies the name of a signaling type.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Display the configuration of the E1R2 signaling type brazil.

```
<Huawei> display voice r2 signalling-type brazil
  R2 Signalling-type :test
  Register-signal-send[7]:0,0,10
  Register-signal-send[7]:0,1,1
  Register-signal-send[7]:0,2,2
  Register-signal-send[7]:0,3,3
  Register-signal-send[7]:0,4,4
```

```
Register-signal-send[7]:0,5,5
Register-signal-send[7]:0,6,6
Register-signal-send[7]:0,7,7
Register-signal-send[7]:0,8,8
Register-signal-send[7]:0,9,9
Register-signal-send[7]:1,0,10
Register-signal-send[7]:1,1,1
Register-signal-send[7]:1,2,2
Register-signal-send[7]:1,3,3
Register-signal-send[7]:1,4,4
Register-signal-send[7]:1,5,5
Register-signal-send[7]:1,6,6
Register-signal-send[7]:1,7,7
Register-signal-send[7]:1,8,8
Register-signal-send[7]:1,9,9
Register-signal-send[7]:2,0,11
Register-signal-send[7]:2,1,12
Register-signal-send[7]:2,2,14
Register-signal-send[7]:3,0,14
Register-signal-send[7]:3,1,13
Register-signal-send[7]:4,0,14
Register-signal-send[7]:5,0,1
Register-signal-send[7]:5,1,2
Register-signal-send[7]:5,2,3
Register-signal-send[7]:5,3,4
Register-signal-send[7]:5,4,5
Register-signal-send[7]:5,5,10
Register-signal-send[7]:8,0,12
Register-signal-send[7]:9,0,15
Register-signal-send[7]:9,1,15
Register-signal-send[7]:10,1,1
Register-signal-send[7]:10,2,2
Register-signal-send[7]:10,3,3
Register-signal-send[7]:10,4,5
Register-signal-send[7]:10,5,6
Register-signal-send[7]:10,6,7
Register-signal-send[7]:10,7,10
Register-signal-send[7]:10,8,8
Register-signal-send[7]:10,9,9
Register-signal-send[7]:11,0,9
Register-signal-send[7]:11,1,1
Register-signal-send[7]:11,2,2
Register-signal-send[7]:11,3,7
Register-signal-send[7]:11,4,8
Register-signal-send[7]:11,5,5
Register-signal-send[7]:11,6,11
Register-signal-send[7]:11,8,12
Register-signal-send[7]:11,9,13
Register-signal-send[7]:11,10,14
Register-signal-send[7]:11,11,5
Register-signal-send[7]:11,12,10
Register-signal-send[7]:12,0,3
Register-signal-send[7]:13,0,6
Register-signal-send[7]:14,0,4
Register-signal-send[7]:15,0,2
Register-signal-send[7]:16,0,3
Register-signal-send[7]:17,0,5
Register-signal-send[7]:18,0,6
Register-signal-send[7]:19,0,7
Register-signal-send[7]:20,0,8
Register-signal-send[7]:25,0,4
Register-signal-recv[7]:1,1,11,1
Register-signal-recv[7]:1,2,11,1
Register-signal-recv[7]:1,4,0,1
Register-signal-recv[7]:1,5,1,1
Register-signal-recv[7]:1,6,10,1
Register-signal-recv[7]:1,7,10,1
Register-signal-recv[7]:1,8,5,0
Register-signal-recv[7]:1,9,0,1
```

```
Register-signal-recv[7]:2,1,11,2
Register-signal-recv[7]:2,3,15,0
Register-signal-recv[7]:2,4,0,2
Register-signal-recv[7]:2,5,1,2
Register-signal-recv[7]:2,6,10,2
Register-signal-recv[7]:2,7,10,2
Register-signal-recv[7]:2,8,5,1
Register-signal-recv[7]:2,9,0,2
Register-signal-recv[7]:3,1,12,0
Register-signal-recv[7]:3,3,16,0
Register-signal-recv[7]:3,4,0,3
Register-signal-recv[7]:3,5,1,3
Register-signal-recv[7]:3,6,10,3
Register-signal-recv[7]:3,7,10,3
Register-signal-recv[7]:3,8,5,2
Register-signal-recv[7]:3,9,0,3
Register-signal-recv[7]:4,1,14,0
Register-signal-recv[7]:4,2,14,0
Register-signal-recv[7]:4,3,25,0
Register-signal-recv[7]:4,4,0,4
Register-signal-recv[7]:4,5,1,4
Register-signal-recv[7]:4,8,5,3
Register-signal-recv[7]:4,9,0,4
Register-signal-recv[7]:5,1,11,5
Register-signal-recv[7]:5,2,11,11
Register-signal-recv[7]:5,3,17,0
Register-signal-recv[7]:5,4,0,5
Register-signal-recv[7]:5,5,1,5
Register-signal-recv[7]:5,6,10,4
Register-signal-recv[7]:5,7,10,4
Register-signal-recv[7]:5,8,5,4
Register-signal-recv[7]:5,9,0,5
Register-signal-recv[7]:6,1,13,0
Register-signal-recv[7]:6,3,18,0
Register-signal-recv[7]:6,4,0,6
Register-signal-recv[7]:6,5,1,6
Register-signal-recv[7]:6,6,10,5
Register-signal-recv[7]:6,7,10,5
Register-signal-recv[7]:6,9,0,6
Register-signal-recv[7]:7,1,11,3
Register-signal-recv[7]:7,3,19,0
Register-signal-recv[7]:7,4,0,7
Register-signal-recv[7]:7,5,1,7
Register-signal-recv[7]:7,6,10,6
Register-signal-recv[7]:7,7,10,6
Register-signal-recv[7]:7,9,0,7
Register-signal-recv[7]:8,1,11,4
Register-signal-recv[7]:8,3,20,0
Register-signal-recv[7]:8,4,0,8
Register-signal-recv[7]:8,5,1,8
Register-signal-recv[7]:8,6,10,8
Register-signal-recv[7]:8,7,10,8
Register-signal-recv[7]:8,9,0,8
Register-signal-recv[7]:9,1,11,0
Register-signal-recv[7]:9,4,0,9
Register-signal-recv[7]:9,5,1,9
Register-signal-recv[7]:9,6,10,9
Register-signal-recv[7]:9,7,10,9
Register-signal-recv[7]:9,9,0,9
Register-signal-recv[7]:10,1,11,12
Register-signal-recv[7]:10,2,11,12
Register-signal-recv[7]:10,4,0,0
Register-signal-recv[7]:10,5,1,0
Register-signal-recv[7]:10,6,10,7
Register-signal-recv[7]:10,7,10,7
Register-signal-recv[7]:10,8,5,5
Register-signal-recv[7]:10,9,0,0
Register-signal-recv[7]:11,1,11,6
Register-signal-recv[7]:11,8,2,0
```

```
Register-signal-recv[7]:12,1,11,8
Register-signal-recv[7]:12,5,8,0
Register-signal-recv[7]:12,8,2,1
Register-signal-recv[7]:12,10,8,0
Register-signal-recv[7]:13,1,11,9
Register-signal-recv[7]:13,2,11,9
Register-signal-recv[7]:13,10,3,1
Register-signal-recv[7]:14,1,11,10
Register-signal-recv[7]:14,8,2,2
Register-signal-recv[7]:14,9,4,0
Register-signal-recv[7]:14,10,3,0
Register-signal-recv[7]:15,1,14,0
Register-signal-recv[7]:15,2,14,0
Register-signal-recv[7]:15,4,9,1
Register-signal-recv[7]:15,5,9,0
Line-signal-send[7]:0,0,1,0,10
Line-signal-send[7]:2,0,9,0,10
Line-signal-send[7]:3,0,9,0,10
Line-signal-send[7]:4,0,9,0,10
Line-signal-send[7]:5,0,13,0,10
Line-signal-send[7]:6,0,5,0,10
Line-signal-send[7]:7,0,5,0,10
Line-signal-send[7]:8,0,13,0,10
Line-signal-send[7]:9,0,1,0,10
Line-signal-send[7]:10,0,9,0,10
Line-signal-send[7]:11,0,13,0,10
Line-signal-send[7]:12,0,9,0,10
Line-signal-recv[7]:0,0,0,0,0
Line-signal-recv[7]:0,0,0,3,0
Line-signal-recv[7]:0,0,0,7,0
Line-signal-recv[7]:0,0,0,8,9
Line-signal-recv[7]:0,0,0,11,9
Line-signal-recv[7]:0,2,0,8,6
Line-signal-recv[7]:0,2,0,10,7
Line-signal-recv[7]:0,4,0,0,3
Line-signal-recv[7]:0,4,0,1,2
Line-signal-recv[7]:0,4,0,2,2
Line-signal-recv[7]:0,4,0,3,2
Line-signal-recv[7]:0,4,0,4,2
Line-signal-recv[7]:0,4,0,5,2
Line-signal-recv[7]:0,4,0,6,2
Line-signal-recv[7]:0,4,0,7,10
Line-signal-recv[7]:0,4,0,8,10
Line-signal-recv[7]:0,4,0,9,10
Line-signal-recv[7]:0,4,0,10,10
Line-signal-recv[7]:0,4,0,11,10
Line-signal-recv[7]:0,4,0,12,10
Line-signal-recv[7]:0,4,0,13,10
Line-signal-recv[7]:0,4,0,14,10
Line-signal-recv[7]:0,6,0,0,11
Line-signal-recv[7]:0,6,0,7,5
Line-signal-recv[7]:0,6,0,8,8
Line-signal-recv[7]:0,6,0,9,8
Line-signal-recv[7]:0,6,0,11,8
Line-signal-recv[7]:0,6,0,13,8
Line-signal-recv[7]:3,4,0,0,3
Line-signal-recv[7]:3,4,0,3,3
Line-signal-recv[7]:3,6,0,0,11
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-75 Description of the display voice r2 signalling-type command output

Item	Description
Register-signal-send[7]:0,0,10	Register signaling output parameters of the R2 signaling type. The value 7 indicates the index value, and the values 0, 0, 10 represent the logical command, parameter in the logical command, and physical command respectively.
Register-signal-recv[7]:1,1,11,1	Register signaling input parameters of the R2 signaling type. The value 7 indicates the index value, and the values 1, 1, 11, 1 represent the physical command, line call parameter, logical command, and parameter in the logical command respectively.
Line-signal-send[7]:0,0,1,0,10	Line signaling output parameters of the R2 signaling type. The value 7 indicates the index value, and the values 0, 0, 1, 0, 10 represent the parameter in a logical command, logical signaling type, physical command, call status, and signaling transmitting duration respectively.
Line-signal-recv[7]:0,0,0,0,0	Line signaling input parameters of the R2 signaling type. The value 7 indicates the index value, and the values 0, 0, 0, 0, 0 represent the logical signaling type, physical command, parameter in the physical command, call status, and logical command respectively.

16.5.6.21 display voice trunk-at0

Function

The **display voice trunk-at0** command displays the configuration of an AT0 trunk.

Format

display voice trunk-at0

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the configuration of an AT0 trunk.

```
<Huawei> display voice trunk-at0
  Spec: 16, Records: 1
  -------------------------
  Trunkgroup name          : at0
  Slot/Subcard/Port        : 1/0/4
  Cid transtype            : Bell202
  Dial delay(ms)           : 2000
  Dial mode                : DTMF
  Insert prefix delay(ms) : 2000
  Insert prefix            :
  Default called number    : 28980000
  Circuit config status    : Normal
```

Table 16-76 Description of the **display voice trunk-at0** command output

Item	Description
Spec	Total space.
Records	Number of records.
Trunkgroup name	Name of a trunk group.
Slot/Subcard/Port	Slot ID/Subcard ID/Port number.
Cid transtype	Signal transmission type for the CLIP service.
Dial delay	Dialing delay.
Dial mode	Dialing mode.
Insert prefix delay	Dial delay after a call prefix is inserted into numbers.
Insert prefix	Inserted call prefix.
Default called number	Bound IVR number.
Circuit config status	Line status.

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.22 display voice trunk-e1r2

Function

The **display voice trunk-e1r2** command displays information about trunks in an R2 trunk group.

Format

display voice trunk-e1r2

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can use the **display voice trunk-e1r2** command to verify the configuration and current status of each trunk in an R2 trunk group for real-time monitoring of the trunk status and fault location and rectification.

Example

Verify the configuration of an R2 trunk group.

```
<Huawei> display voice trunk-e1r2
  Spec: 64, Records: 32
  --------------------
  Trunkgroup name   : r201
  Slot/Subcard/Port : 2/0/0
  B-Channel config status[0]    : Reserved
  B-Channel line admin state[0] : Reserved

  B-Channel config status[1]    : Normal
  B-Channel line admin state[1] : LBlock

  B-Channel config status[2]    : Normal
  B-Channel line admin state[2] : LBlock

  B-Channel config status[3]    : Normal
  B-Channel line admin state[3] : LBlock

  B-Channel config status[4]    : Normal
  B-Channel line admin state[4] : LBlock
  ......
  B-Channel config status[15]    : Normal
  B-Channel line admin state[15] : LBlock

  B-Channel config status[16]    : Reserved
  B-Channel line admin state[16] : Reserved
  ......
```

```
B-Channel config status[31]    : Normal
B-Channel line admin state[31] : LBlock
```

Table 16-77

Parameter	Description
Spec	Total space.
Records	Actual records.
Trunkgroup name	Name of the trunk group.
Slot/Subcard/Port	E1 interface number.
B-Channel config status	Configuration status of a B channel. The values are as follows: ● Normal ● Reserved ● Block
B-Channel line admin state	Line administrator status of a B channel. The values are as follows: ● Normal ● Reserved ● LBlock ● RBlock ● LRBlock

16.5.6.23 display voice trunk-group

Function

The **display voice trunk-group** command displays the information about PBX trunk groups.

Format

display voice trunk-group [*trunk-group-name* [*para-value*]]

Parameters

Parameter	Description	Value
trunk-group-name	Specifies the name of a trunk group.	The value is a string of 1 to 32 case-sensitive characters.

Parameter	Description	Value
para-value	Specifies the parameter to display.	Options: ● callroute: call route bound to the trunk group. ● gnr-number: gnr-number bound to the trunk group. ● codec-priority: codec priority, codec value, and packetization time. ● dtmf: DTMF transmission mode of the trunk group. ● fax-modem: Fax/Modem configuration information about the SIP trunk. ● number-parameter: parameter index ● redundancy-nte: whether to enable RFC2198 redundancy transmission of RFC2833. ● statuscode-toneid-mapping: mapping relationships between error codes and tones played. ● trunk-at0: AT0 trunk. ● trunk-bra: BRA trunk. ● trunk-e1r2: E1R2 trunk. ● trunk-pra: PRA trunk. ● trunk-sipat0: SIPAT0 trunk.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If the trunk group name is not specified, the information about all trunk groups is displayed.

Example

Display the information about trunk group sipbb.

```
<Huawei> display voice trunk-group sipbb
  Config
  Trunkgroup name                 : sipbb
  Trunkgroup ID                   : 10
  Description                     :
  Sigtype                         : sip
  Dn-set                          : DefaultDialPlan
  Enterprise                      : default
  Select mode                     : Loop
  Priority of trunk group         : Default
  Reserved circuit number         : 0
  Reserved circuit priority       : Super
  Outgoing right                  : inter&local&ddd&idd
  Custom right                    :
  Relate call route name          : sipbb
  Relate call source name         : -
  Support cli change              : enable
  Country/Region code             : 86
  Area Code                       : 755
  Default caller number           :
  Register mode                   : No register
  Local signalling IP             : 192.168.0.1
  Local signalling IP address name:
  Local signalling port           : 5071
  Local media IP                  : 192.168.0.1
  Local media IP address name     :
  Primary server IP               : 3.3.1.18
  Primary server port             : 1719
  Secondary server IP             : 3.3.1.47
  Secondary server port           : 1719
  Proxy address mode              : Static IP
  Primary server IP               : 192.168.0.2
  Primary server port             : 5071
  Secondary server IP             :
  Secondary server port           : 65535
  Register server URI             :
  Home domain                     : abcd.com
  Transfer mode                   : UDP
  Transfer CS mode                :
  Register ID                     :
  Register password               :
  Maximum number of calls         : 10
  IP trunk adapter type           : MG
  Media Proxy                     : Disable
  Mapped Signalling IP            :
  Mapped Signalling port          :
  Mapped Media IP                 :
  Mapped Media Port Start         :
  Mapped Media Proxy Port Start   :
  Use rule set                    :

  Running
  Trunkgroup name                 : sipbb
  Trunkgroup ID                   : 10
  Description                     :
  Sigtype                         : sip
  Dn-set                          : DefaultDialPlan
  Enterprise                      : default
  Select mode                     : Loop
```

```
Priority of trunk group        : Default
Reserved circuit number        : 0
Reserved circuit priority      : Super
Outgoing right                 : inter&local&ddd&idd
Custom right                   :
Relate call route name         : sipbb
Relate call source name        : -
Support cli change             : enable
Country/Region code            : 86
Area Code                      : 755
Default caller number          :
Register mode                  : No register
SIP trunk group state          : Normal
Local signalling IP            : 192.168.0.1
Local signalling IP address name:
Local signalling port          : 5071
Local media IP                 : 192.168.0.1
Local media IP address name    :
Peer IP                        : 192.168.0.2
Peer port                      : 5071
Proxy address mode             : Static IP
Primary server IP              : 192.168.0.2
Primary server port            : 5071
Secondary server IP            :
Secondary server port          : 65535
Primary server state           : Up
Secondary server state         : Unknown
Current server                 : Primary server
Register server URI            :
Home domain                    : abcd.com
Transfer mode                  : UDP
Transfer CS mode               :
Register ID                    :
Register password              :
Maximum number of calls        : 10
IP trunk adapter type          : MG
Media Proxy                    : Disable
Mapped Signalling IP           :
Mapped Signalling port         :
Mapped Media IP                :
Mapped Media Port Start        :
Mapped Media Proxy Port Start  :
Use rule set                   :
```

Table 16-78 Description of the **display voice trunk-group command** output

Item	Description
Trunkgroup name	Name of the trunk group. You can configure the trunk group name by running the **trunk-group** command.
Trunkgroup ID	Trunkgroup ID.
Description	Description of the trunk group. You can configure the trunk group description by running the **description (trunk group view)** command.

Item	Description
Sigtype	Trunk signaling type. You can configure the trunk signaling type by running the **trunk-group** command.
Dn-set	DN set. You can configure the DN set by running the **enterprise dn-set (trunk group view)** command.
Enterprise	Enterprise name. You can configure the enterprise name by running the **enterprise dn-set (trunk group view)** command.
Select mode	The trunk group circuit selection mode.
Reserved circuit number	Reserved circuit number.
Reserved circuit priority	Reserved circuit priority.
Outgoing right	Outgoing right.
Custom right	Trunk group right.
Relate call route name	Relate call route name.
Relate call source name	Relate call source name.
Support cli change	Whether support calling number change.
Country/Region code	Country code.
Area Code	Area Code.
Default caller number	Default caller number.
Register mode	Registration mode.
Local signalling IP	Local signaling IP address.
Local signalling IP address name	Interface name of the local signaling IP address.
Local signalling port	Local signaling port.
Local media IP	Local media IP address.
Local media IP address name	Interface name of the local media IP address.
Peer IP	Remote IP address.
Peer port	Remote port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Proxy address mode	Peer address mode, either dynamic or static.
Primary server IP	IP address of the primary server.
Primary server port	Port of the primary server.
Secondary server IP	IP address of the Secondary server.
Secondary server port	Port of the Secondary server.
Register server URI	URI carried in the registration header field.
Home domain	Domain name carried in the registration header field.
Transfer mode	Transfer mode.
Transfer CS mode	Reliable connection mode.
Register ID	Register ID.
Register password	Register password.
Maximum number of calls	Maximum number of call connections.
IP trunk adapter type	SIP IP Relay Group adapter type.
Media Proxy	Media Proxy.
Mapped Signalling IP	Mapped signaling IP address.
Mapped Signalling port	Mapped signaling port.
Mapped Media IP	Mapped media IP address.
Mapped Media Port Start	Mapped media start port.
Mapped Media Proxy Port Start	Mapped media proxy start port.
Use rule set	Used rule set.

16.5.6.24 display voice trunk-bra

Function

The **display voice trunk-bra** command displays the configuration of a BRA trunk.

Format

display voice trunk-bra

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the configuration of a BRA trunk.

```
<Huawei> display voice trunk-bra
  Spec: 4, Records: 1
  -------------------
 Trunkgroup name              : bra
 Slot/Subcard/Port            : 2/0/0
 Default called number        :
 Caller enterprise            : default
 Caller no country code       :
 Caller no area code          :
 Caller no                    :
 B-Channel config status[0]   : Normal
 B-Channel config status[1]   : Normal
```

Table 16-79 Description of the **display voice trunk-bra** command output

Item	Description
Spec	Total space.
Records	Number of records.
Trunkgroup name	Trunk group name.
Slot/Subcard/Port	Slot ID/Subcard ID/Port ID.
Default called number	Default called number.
Caller enterprise	Caller enterprise.
Caller no country code	Caller no country code.
Caller no area code	Caller no area code.
Caller no	Caller number.
B-Channel config status	Port configuration status.

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.25 display voice trunk-pra

Function

The **display voice trunk-pra** command displays the configuration of a PRA trunk.

Format

display voice trunk-pra

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the configuration of a PRA trunk.

```
<Huawei> display voice trunk-pra
  Spec: 256, Records: 64
  -------------------
  Trunkgroup name              : NA
  Slot/Subcard/Port            : 1/0/0
  Default Cli                  : 28980808
  Time-slot config status[ 0]  : Reserved

  Trunkgroup name              : pra-net
  Slot/Subcard/Port            : 1/0/0
  Default Cli                  : 28980808
  Time-slot config status[ 1]  : Normal
```

Table 16-80 Description of the **display voice trunk-pra** command output

Item	Description
Spec	Total space.
Records	Number of records.
Time-slot config status[1]	Port configuration status.
Trunkgroup name	Trunk group name.
Slot/Subcard/Port	Slot ID/Subcard ID/Port ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default Cli	Default calling number

16.5.6.26 display voice trunk-sipat0

Function

The **display voice trunk-sipat0** command displays the configuration of the SIP AT0 trunk.

Format

display voice trunk-sipat0 [*register-id* | **brief**]

Parameters

Parameter	Description	Value
register-id	Specifies the registered ID of the SIP AT0 trunk.	The value is a string of 1 to 32 case-sensitive characters without spaces.
brief	Display brief information about all SIP AT0 trunk groups.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

The **display voice trunk-sipat0** command displays configurations and status of trunks in the SIP AT0 trunk group, helping to monitor the status of trunks in real time and troubleshoot faults.

Example

Display the configuration of a SIP AT0 trunk.

```
<Huawei> display voice trunk-sipat0
Spec: 400, Records: 1, registered count: 1, unregisterd count: 0
 ------------------------------------------------------------------------------
 Trunkgroup name       : sipat0
```

```
Register id          : 90001
Password             :
Default called number : 10086
Max calls            : 1
Caller telno         :
Register status      : In service
Refresh time         : 286
Reason               : -
Service status       : Idle
```

Table 16-81 Description of the **display voice trunk-sipat0** command output

Item	Description
Spec	Space of trunk groups.
Records	Number of records.
registered count	Number of registered trunk groups.
unregisterd count	Number of unregistered trunk groups.
Trunkgroup name	Name of the trunk group.
Register id	Registered ID for the SIP AT0 trunk.
Password	Registration password of the SIP AT0 trunk.
Default called number	Called number for incoming calls.
Max calls	Maximum number of calls.
Caller telno	Calling number for outgoing calls routed through the SIP AT0 trunk.
Register status	Registration status of the SIP AT0 trunk.
Refresh time	Remaining time for the SIP AT0 trunk to refresh the registration status in seconds.
Reason	Cause of the SIP AT0 registration failure.
Service status	SIP AT0 service status.

16.5.6.27 displayname

Function

The **displayname** command configures the display header value in Q.931 messages.

The **undo displayname** command restores the default display header value in Q.931 messages.

By default, the display header in Q.931 messages is HUAWEI.

Format

displayname *displayname-value*

undo displayname

Parameters

Parameter	Description	Value
displayname-value	Indicates the display header in the Q.931 message.	The value is a string of 1 to 32 case-sensitive characters without spaces. **NOTE** The value '-' indicates that the value of the display header in a Q.931 message is empty.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the name of a calling party or called party that is displayed on a terminal, you can run the **displayname** command and change the value of the display header in Q.931 messages.

Based on scenarios, the value of the display header in a Q.931 message is described as follows:

- When an outgoing call is made over an H.323 trunk, the value of the display header in the Q.931 message sent by the AR is the value configured by the **displayname** command.
- An incoming call is received over an H.323 trunk:
  - If the parameter is set to -, the value of the display header in the Q.931 message sent by the AR is empty.
  - If the parameter is set to another value, the value of the display header in the Q.931 message sent by the AR is the same as that in the Q.931 message received by the AR, but not the value configured by the **displayname** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After running the **displayname** command, you need to run the **reset** command to reset the H.323 system to enable the configuration to take effect.

Example

Set the display header in the Q931 message to user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] displayname user
[Huawei-voice-h323-attribute] reset
```

16.5.6.28 dtmf-transmission-mode (trunk group view)

Function

Using the **dtmf-transmission-mode** command, you can configure the Dual-Tone Multi-frequency (DTMF) transmission mode for a PBX.

Using the **undo dtmf-transmission-mode** command, you can restore the default DTMF transmission mode of a PBX.

By default, the DTMF transmission mode is transparent transmission.

Format

dtmf-transmission-mode { **throughly** | **erase** }

undo dtmf-transmission-mode

Parameters

Parameter	Description	Value
throughly	Indicates DTMF transparent transmission.	-
erase	Indicates DTMF signal removing.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

SIP or H.323 trunk group support the **dtmf-transmode** command. Before using the **dtmf-transmode** command, run the **trunk-group** command to create a SIP or H.323 trunk group.

 Copyright © Huawei Technologies Co., Ltd.

The **dtmf-transmode** command configures the DTMF transmission mode for a PBX.

- DTMF transparent transmission: the default DTMF transmission mode.
- DTMF signal removing: used when DTMF signaling is transmitted in accordance with RFC 2833 and DTMF signals do not need to be transmitted.

Example

Set the DTMF transmission mode to transparent transmission for a PBX.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group abcd sip trunk-group
[Huawei-voice-trunkgroup-abcd] dtmf-transmission-mode throughly
```

16.5.6.29 earlyh245

Function

The **earlyh245** command configures whether the Setup message contains the H245 address.

The **undo earlyh245** command restores the default configuration.

By default, the Setup message does not contain the H245 address.

Format

earlyh245 { **enable** | **disable** }

undo earlyh245

Parameters

Parameter	Description	Value
enable	Indicates that the Setup message contains the H245 address.	-
disable	Indicates that the Setup message does not contain the H245 address.	-

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

When the Setup message contains the H245 address, the H245 address is sent to the called party, and media negotiation can be performed based on this address.

Example

Specify that the Setup message contains the H245 address.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] earlyh245 enable
```

16.5.6.30 endservice trunk-sipat0(SIP AT0 trunk view)

Function

The **endservice trunk-sipat0** command stops the SIP AT0 service.

The **undo endservice trunk-sipat0** command starts the SIP AT0 service.

Format

endservice trunk-sipat0 *register-private-id*

undo endservice trunk-sipat0 *register-private-id*

Parameters

Parameter	Description	Value
register-private-id	Specifies the registration ID.	The value is a string of 1 to 32 characters.

Views

SIP AT0 trunk view

Default Level

2: Configuration level

Usage Guidelines

N/A

Example

Stop the SIP AT0 service.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] endservice trunk-sipat0 2
```

16.5.6.31 endsession-timeout

Function

The **endsession-timeout** command sets the EndSessionCommand timeout. The EndSessionCommand message is used to end the H245 channel.

The **undo endsession-timeout** command restores the default EndSessionCommand timeout.

By default, the EndSessionCommand timeout is 3000 ms.

Format

endsession-timeout *endsession-timeout-value*

undo endsession-timeout

Parameters

Parameter	Description	Value
endsession-timeout-value	Indicates the EndSessionCommand timeout.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the EndSessionCommand timeout to 50000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] endsession-timeout 50000
```

16.5.6.32 enterprise dn-set (trunk group view)

Function

The **enterprise dn-set** command binds an enterprise and a DN set to a trunk group.

The **undo enterprise** command unbinds an enterprise and a DN set from a trunk group.

Format

enterprise *enterprise-name* [**dn-set** *dn-set-name*]

undo enterprise

Parameters

Parameter	Description	Value
enterprise-name	Specifies the enterprise to which the trunk group belongs.	The value is a string of 1 to 32 characters.
dn-set *dn-set-name*	Specifies the DN set name.	The value is a string of 1 to 32 characters. The default value is defaultdialplan.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

When an enterprise has multiple DN sets, run this command to specify a DN set for a trunk group.

Example

Bind the enterprise **abcd** to the trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test
[Huawei-voice-trunkgroup-test] enterprise abcd
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.33 faststart-flag

Function

The **faststart-flag** command enables or disables the fast start function.

The **undo faststart-flag** command restores the default configuration.

By default, the fast start function is enabled.

Format

faststart-flag { **enable** | **disable** }

undo faststart-flag

Parameters

Parameter	Description	Value
enable	Enables fast start.	-
disable	Disables fast start.	-

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

After the fast start function is enabled, sessions can be set up quickly.

Example

Disable the fast start function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] faststart-flag disable
```

16.5.6.34 fax-modem common negotiation-mode

Function

Using the **fax-modem common negotiation-mode** command, you can set the fax/modem codec negotiation mode of a PBX.

Using the **undo fax-modem common negotiation-mode** command, you can restore the default fax/modem codec negotiation mode of a PBX.

By default, the fax/modem codec negotiation mode is negotiation.

Format

fax-modem common negotiation-mode { **negotiate** | **self-switch** }

undo fax-modem common negotiation-mode

Parameters

Parameter	Description	Value
negotiate	Sets the fax/modem codec negotiation mode to negotiation. In negotiation mode, the MG needs to negotiate with the MGC for the codec negotiation mode using signaling.	-
self-switch	Sets the fax/modem codec negotiation mode to self-switch.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

SIP or H.323 trunk groups support the **fax-modem common negotiation-mode** command. Before using the **fax-modem common negotiation-mode** command, run the **trunk-group** command to create a SIP or H.323 trunk group.

Example

Set the fax/modem codec negotiation mode of the PBX to self-switch.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] fax-modem common negotiation-mode self-switch
```

16.5.6.35 fax-modem common rtp-interval

Function

Using the **fax-modem common rtp-interval** command, you can set the packetization interval in transparent transmission mode.

Using the **undo fax-modem common rtp-interval** command, you can restore the default packetization interval in transparent transmission mode.

By default, the packetization interval in transparent transmission mode is 10 ms.

Format

fax-modem common rtp-interval { **5ms** | **10ms** | **20ms** | **30ms** }

undo fax-modem common rtp-interval

Parameters

None

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

SIP or H.323 trunk group support the **fax-modem common rtp-interval** command. Before using the **fax-modem common rtp-interval** command, run the **trunk-group** command to create a SIP or H.323 trunk group.

Example

Set the packetization interval in transparent transmission mode to 20 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] fax-modem common rtp-interval 20ms
```

16.5.6.36 fax-modem common vbd-attribute-type

Function

Using the **fax-modem common vbd-attribute-type** command, you can set the VBD attribute type of a PBX.

Using the **undo fax-modem common vbd-attribute-type** command, you can restore the default VBD attribute type of a PBX.

By default, the VBD attribute type is V.152.

Format

fax-modem common vbd-attribute-type { **chinatelecom** | **extchinatelecom** | **ietf** | **v152** }

undo fax-modem common vbd-attribute-type

Parameters

Parameter	Description	Value
chinatelecom	Indicates the China Telecom mode.	-
extchinatelecom	Indicates the extended China Telecom mode.	-
ietf	Indicates the IETF mode.	-
v152	Indicates the V.152 mode.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

SIP or H.323 trunk group support the **fax-modem common vbd-attribute-type** command. Before using the **fax-modem common vbd-attribute-type** command, run the **trunk-group** command to create a SIP or H.323 trunk group.

Example

Set the VBD attribute type to IETF.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] fax-modem common vbd-attribute-type ietf
```

16.5.6.37 fax-modem common vbd-codec

Function

Using the **fax-modem common vbd-codec** command, you can set the VBD codec mode of a PBX.

Using the **undo fax-modem common vbd-codec** command, you can restore the default VBD codec mode of a PBX.

By default, the VBD codec mode is A-law algorithm in G.711.

 Copyright © Huawei Technologies Co., Ltd.

Format

fax-modem common vbd-codec { **g711a** | **g711u** | **g711a_u** | **g711u_a**}

undo fax-modem common vbd-codec

Parameters

Parameter	Description	Value
g711a	Indicates the A-law algorithm in G.711.	-
g711u	Indicates the u-law algorithm in G.711.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

SIP or H.323 trunk group support the **fax-modem common vbd-codec** command. Before using the **fax-modem common vbd-codec** command, run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a SIP or H.323 trunk group.

Example

Set the VBD codec mode of the PBX to u-law algorithm in G.711.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] fax-modem common vbd-codec g711u
```

16.5.6.38 fax-modem common vbd-payload-type

Function

Using the **fax-modem common vbd-payload-type** command, you can configure the VBD payload type of a PBX.

Using the **undo fax-modem common vbd-payload-type** command, you can restore the default VBD payload type of a PBX.

By default, the VBD payload type is static.

 Copyright © Huawei Technologies Co., Ltd.

Format

fax-modem common vbd-payload-type { **dynamic** | **static** }

undo fax-modem common vbd-payload-type

Parameters

Parameter	Description	Value
dynamic	Indicates dynamic payload.	-
static	Indicates static payload.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

SIP or H.323 trunk group support the **fax-modem common vbd-payload-type** command. Before using the **fax-modem common vbd-payload-type** command, run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a SIP or H.323 trunk group.

Example

Set the VBD payload type to dynamic payload.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] fax-modem common vbd-payload-type dynamic
```

16.5.6.39 fax-modem fax transmission-mode

Function

Using the **fax-modem fax transmission-mode** command, you can configure the fax transmission mode for a PBX.

Using the **undo fax-modem fax transmission-mode** command, you can restore the default fax transmission mode of a PBX.

By default, the fax transmission mode of a PBX is transparent transmission.

 Copyright © Huawei Technologies Co., Ltd.

Format

fax-modem fax transmission-mode { **throughly** | **T38** | **T38_throughly** | **throughly_T38** }

undo fax-modem fax transmission-mode

Parameters

Parameter	Description	Value
throughly	Indicates the transparent transmission mode.	-
T38	Indicates the T.38 mode.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

The trunk group of the SIP or H.323 type supports the **fax-modem fax transmission-mode** command. Before using the **fax-modem fax transmission-mode** command, run the **trunk-group** command to create a trunk group of the SIP or H.323 type.

The **fax-modem fax parameters transmission-mode** command configures the fax transmission mode for a PBX:

- Transparent transmission mode: uses the coding mode defined in G.711.
- T.38 mode: uses the fax-dedicated coding mode.
- T38_throughly: primary T.38 mode, secondary Transparent transmission mode.
- throughly_T38: primary Transparent transmission mode, secondary T.38 mode.

Example

Set the fax transmission mode of a PBX to transparent transmission.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] fax-modem fax transmission-mode throughly
```

16.5.6.40 gatekeeper-techprefix

Function

The **gatekeeper-techprefix** command configures the gateway technical prefix.

The **undo gatekeeper-techprefix** command deletes the gateway technical prefix.

By default, no gateway technical prefix is configured in the system.

Format

gatekeeper-techprefix *gatekeeper-techprefix-value*

undo gatekeeper-techprefix *gatekeeper-techprefix-value*

Parameters

Parameter	Description	Value
gatekeeper-techprefix-value	Specifies the gateway technical prefix.	The value is a string of 1 to 16 characters. The value can only contain digits, the number sign (#), and asterisk (*).

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a gw-gk type H.323 trunk group, a gateway sends an RRQ message to the gatekeeper for registration. If the RRQ message carries a gateway technical prefix, the gatekeeper associates the gateway technical prefix with the gateway source address and records the association. The association information can be used to locate the called party during a call. If multiple gateways exist, the same gateway technical prefix can be configured for the gateways that provide the same type of services (for example, voice or video). The gatekeeper organizes gateways with the same technical prefix into one group to facilitate information search. For example, when a calling party requests a voice service, the gatekeeper searches the voice service group for the corresponding gateway information without traversing all gateways and then forwards the call to the calling party.

Precautions

This command is applicable only to gw-gk type H.323 trunk groups.

Example

Set the gateway technical prefix to **1#**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test h323 gw-gk
[Huawei-voice-trunkgroup-test] gatekeeper-techprefix 1#
```

16.5.6.41 gkid

Function

The **gkid** command configures IDs of the active and standby gatekeepers with which a gateway registers.

The **undo gkid** command deletes IDs of the active and standby gatekeepers with which a gateway registers.

By default, a gateway is not configured with IDs of the active and standby gatekeepers with which the gateway registers.

Format

gkid *id* [**secondary** *secondary-id*]

undo gkid

Parameters

Parameter	Description	Value
id	The ID of the gatekeeper with which a gateway registers.	The name is a string of 1 to 32 case-insensitive characters without spaces.
secondary *secondary-id*	The ID of the standby gatekeeper with which a gateway registers.	The name is a string of 1 to 32 case-insensitive characters without spaces.

Views

H323 trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an AR router functions as a gateway registering with gatekeepers in an H.323 trunk, IDs of the active and standby gatekeepers to be registered with must be specified on the gateway.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The configuration takes effect only after the trunk group is restarted.

Example

Set **gkid** to **Aa123** and **secondary** to **Bb123**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 gw-gk
[Huawei-voice-trunkgroup-test] gkid Aa123 secondary Bb123
```

16.5.6.42 gnr-number (trunk group view)

Function

gnr-number gnr-number-value command binds gnr-number to a trunk group.

undo gnr-number gnr-number-value command deletes gnr-number under a trunk group.

Format

gnr-number *gnr-number-value* [**num** *count* **step-lenth** *step-lenth-value*]

undo gnr-number *gnr-number-value* | *all*

Parameters

Parameter	Description	Value
gnr-numebr-value	Specifies gnr-number binds to trunk group	The value must already exist in system.
count	The gnr-number count add to trunk group in batch.	1~30
step-lenth-value	The step-lenth between gnr-numbers add to trunk group in batch,Optional.	1~99

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

To bind gnr-number to a trunk group, run **gnr-number** gnr-number-value command.

Example

Configure gnr-number 123456, and bind it to trunk-group pra.

```
[Huawei-voice]gnr-number 123456
[Huawei-voice-gnrnumber-123456]q
[Huawei-voice]trunk-group pra [Huawei-voice-trunkgroup-pra]gnr-number 123456 [Huawei-voice-
trunkgroup-pra]display this
[V200R005C20SPC212T]
#
  trunk-group pra dss1-user
  callroute 89
  trunk-pra 1/0/0
  gnr-number 123456
#
return
```

16.5.6.43 gwid

Function

The **gwid** command configures the gateway ID of the H323 trunk.

The **undo gwid** command deletes the gateway ID of the H323 trunk.

By default, no gateway ID is configured.

Format

gwid *gwid-value*

undo gwid

Parameters

Parameter	Description	Value
gwid-value	Indicates the gateway ID.	The value is a string of 1 to 32 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

In the registration mode, the gateway ID must be configured and must be the same as that configured on the peer.

Example

Set the gateway ID to client.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 register-gateway
[Huawei-voice-trunkgroup-test] gwid client
```

16.5.6.44 h245version

Function

The **h245version** command sets the H.245 protocol version.

The **undo h245version** command restores the default H.245 protocol version.

By default, the H.245 protocol version is V4.

Format

h245version *h245version-value*

undo h245version

Parameters

Parameter	Description	Value
h245version-value	Specifies the H245 protocol version.	The values are as follows: ● V2 ● V3 ● V4 ● V5 The default value is V4.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the H.245 protocol version to V2.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] h245version v2
```

16.5.6.45 h323-app-timer

Function

The **h323-app-timer** command sets H323 timers.

The **undo h323-app-timer** command restores the default H323 timer values.

Format

h323-app-timer *timerindex timerlen*

undo h323-app-timer *timerindex*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
timerindex timerlen	Specifies the H323 timer values: ● *timerindex* indicates the timer index. ● *timerlen* specifies the timer value.	The value of *timerindex* is an integer ranging from 0 to 51. The value of *timerlen* is an integer, in ms. ● When the *timerindex* value is 0, it indicates the CR SetupAck timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 1, it indicates the CR CallProceeding/Alerting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 120000. ● When the *timerindex* value is 2, it indicates the CR Connect timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 180000. ● When the *timerindex* value is 3, it indicates the RAS PS Admission Confirm timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 4, it indicates the

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		H.245 setup timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 30000. ● When the *timerindex* value is 5, it indicates the check mechanism timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 1000. ● When the *timerindex* value is 6, it indicates the OLC setup timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 5000. ● When the *timerindex* value is 7, it indicates the TCS message sending timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 10000. ● When the *timerindex* value is 8, it indicates the timeout during which the peer EP disables the logical channel. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 60000. ● When the *timerindex* value is 9, it indicates the

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		CLC setup timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 5000. ● When the *timerindex* value is 10, it indicates call self-check timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 60000. ● When the *timerindex* value is 11, it indicates the call self-check waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 17000. ● When the *timerindex* value is 12, it indicates the call self-check waiting release timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 3000. ● When the *timerindex* value is 13, it indicates the AIP notification timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 5000. ● When the *timerindex* value is 14, it indicates the SDP modification

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 5000. ● When the *timerindex* value is 15, it indicates the connect waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 180000. ● When the *timerindex* value is 16, it indicates the call setup timer. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 300000. ● When the *timerindex* value is 17, it indicates the call release waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 200. ● When the *timerindex* value is 18, it indicates the media redirection timer. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 12000. ● When the *timerindex* value ranges from 19 to 24,

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		it indicates a reserved timer. ● When the *timerindex* value is 25, it indicates the CR Admission waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 26, it indicates the EP ARQ waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 27, it indicates the EP DRQ waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 28, it indicates the CR Disengage waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 29, it indicates the EP IRR waiting timeout. The *timerlen* value ranges from 0 to

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		4294967295, in ms. The default value is 60000. ● When the *timerindex* value is 30, it indicates the IRR message sending timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 60000. ● When the *timerindex* value is 31, it indicates the EDM Disengage waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 32, it indicates the EDM Register waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 33, it indicates the EDM Unregister waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 34, it indicates the CDB Dispatch waiting timeout. The *timerlen* value

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		ranges from 0 to 4294967295, in ms. The default value is 15000. ● When the *timerindex* value is 35, it indicates the CR Location waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 5000. ● When the *timerindex* value is 36, it indicates the EP URQ waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 50000. ● When the *timerindex* value is 37, it indicates the RAS self-check timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 60000. ● When the *timerindex* value is 38, it indicates the RAS self-check IRR waiting timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 3000. ● When the *timerindex* value is 39, it indicates the EP DCF timeout. The *timerlen* value

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		ranges from 0 to 4294967295, in ms. The default value is 10000. ● When the *timerindex* value is 40, it indicates status check timeout. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 3600000. ● When the *timerindex* value is 41, it indicates the duration when the local gateway waits for a registration response from the active gatekeeper and then sends a registration request to the standby gatekeeper. The *timerlen* value ranges from 0 to 4294967295, in ms. The default value is 15000. **NOTE** If *timerlen* is set to a value ranging from 0 to 10000, only the value 10000 takes effect. ● When the *timerindex* value ranges from 42 to 51, it indicates a reserved timer.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the call release waiting timeout to 222222 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] h323-app-timer 17 222222
```

16.5.6.46 h323-attribute

Function

The **h323-attribute** command displays the H323 attribute view.

Format

h323-attribute

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enter the H323 configuration view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute]
```

16.5.6.47 h323-number-parameter

Function

The **h323-number-parameter** command sets H323 trunk group parameters.

The **undo h323-number-parameter** command restores the default parameter settings.

 Copyright © Huawei Technologies Co., Ltd.

Format

h323-number-parameter *numpara-nonumpara-value*

undo h323-number-parameter *numpara-no*

Parameters

Parameter	Description	Value
numpara-nonumpara-value	Indicates the H323 trunk group parameter. *numpara-no* indicates the parameter index and *numpara-value* indicates the parameter value.	The value of *numpara-no* is an integer that ranges from 0 to 17. The *numpara-value* value varies according to the *numpara-no* value. ● When the *numpara-no* value is 0, it indicates whether the Setup message contains the display field. The *numpara-no* value is 0 or 1: 1. 0: The Setup message does not contain the display field. 2. 1: The Setup message contains the display field. The default value is 1. ● When the *numpara-no* value is 1, it indicates which of sourceAddress and Calling Party Number IE is selected as the calling number when their values are different. The *numpara-no* value is 0 or 1: 1. 0: The sourceAddress is used as the calling number. 2. 1: The Calling Party Number IE is used as the calling number. The default value is 0. ● When the *numpara-no* value is 2, it indicates the

Parameter	Description	Value
		transport mode. The *numpara-no* value is 0 or 1: 1. 0: packet switching mode 2. 1: circuit mode The default value is 0. ● When the *numpara-no* value is 3, it indicates whether the current media is added to the media list when the TCS message is received. The *numpara-no* value is 0 or 1: 1. 0: no 2. 1: yes The default value is 0. ● When the *numpara-no* value is 4, it indicates the fax mode. The *numpara-no* value is 0 or 1: 1. 0: private mode 2. 1: Cisco mode The default value is 1. ● When the *numpara-no* value is 5, it indicates whether the slow start tone is played using the Connect message if the protocol contains the H245 address. The *numpara-no* value is 0 or 1: 1. 0: The Connect message is not used to play the slow start tone. 2. 1: The Connect message is used to

Parameter	Description	Value
		play the slow start tone. The default value is 1. ● When the *numpara-no* value is 6, Reserved. ● When the *numpara-no* value is 7, it indicates whether to stop playing early media and play the local ringback tone instead. The *numpara-no* value is 0 or 1: 1. 0: no 2. 1: yes The default value is 0. ● When the *numpara-no* value is 8, it indicates that whether the number is sent in the Information message when the H323 trunk is stable. The *numpara-no* value is 0 or 1: 1. 0: The number in the Information message is sent. 2. 1: The number in the Information message is not sent. The default value is 0. ● When the *numpara-no* value is 9, it indicates that whether the decoding priority is marked using the global setting or trunk setting. The *numpara-no* value is 0 or 1:

Parameter	Description	Value
		1. 0: Global setting is used. 2. 1: Trunk setting is used. The default value is 0. ● When the *numpara-no* value is 10, Reserved. ● When the *numpara-no* value is 11, it indicates how H245 sends the Information message. The *numpara-no* value is 0 or 1: 1. 0: signal 2. 1: Alphanumeric The default value is 0. ● When the *numpara-no* value is 12, it indicates the value of the Information transfer capability field in Bearer Capability of Q.931 messages. The *numpara-no* value is 0 to 5. The default value is 0. ● When the *numpara-no* value is 13, it indicates the value of the user information layer 1 protocol field in Bearer Capability of Q.931 messages. The *numpara-no* value is 0 to 8. The default value is 4. ● When the *numpara-no* value is 14, it indicates whether the Information message with SendComplete is sent if the called number to be sent by

Parameter	Description	Value
		the H.323 trunk group does not reach the maximum prefix length and does not end with the number sign (#). The *numpara-no* value is 0 or 1: 1. 0: The Information message with SendComplete is not sent. 2. 1: The Information message with SendComplete is sent. The default value is 0. ● When the *numpara-no* value is 15, it indicates whether to play announcements to the peer end. The *numpara-no* value is 0 or 1: 1. 0: Announcements are not played to the peer end. 2. 1: Announcements are played to the peer end. The default value is 0. ● When the *numpara-no* value is 16, it indicates media control address carried in connect olc message for reverse channel comes from peer or local. The *numpara-no* value is 0 or 1: 1. 0: peer 2. 1: local The default value is 0. ● When the *numpara-no* value is 17, it

Parameter	Description	Value
		indicates whether to send connect message with bearer capability. The *numpara-no* value is 0 or 1: 1. 0: without bearer capability 2. 1: with bearer capability The default value is 1.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

After running the **h323-number-parameter** command to configure a control point, run the **reset** command to reset the trunk group to make the configuration take effect.

Example

Set H323 trunk group parameters.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 register-gateway
[Huawei-voice-trunkgroup-test] h323-number-parameter 0 0
```

16.5.6.48 h323-systemname

Function

The **h323-systemname** command configures the H323 stack system name.

The **undo h323-systemname** command deletes the H323 stack system name.

By default, the H323 stack system name is HUAWEI.

Format

h323-systemname *h323systemname-value*

undo h323-systemname

Parameters

Parameter	Description	Value
h323systemname-value	Specifies the H323 stack system name.	The value is a string of 1 to 32 characters.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the H323 stack system name to **user**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] h323-systemname user
```

16.5.6.49 h323version

Function

The **h323version** command configures the H.323 protocol version.

The **undo h323version** command restores the default H.323 protocol version.

By default, the H.323 protocol version is V4.

Format

h323version *h323version-value*

undo h323version

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
h323version-value	Specifies the H.323 protocol version.	Enumerated type. The values are as follows: ● V2 ● V3 ● V4 ● V5 The default H.323 protocol version is V4.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the H.323 protocol version to V2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] h323version v2
```

16.5.6.50 heartbeat

Function

The **heartbeat** command configures the heartbeat detection timeout period and retry count for a gatekeeper.

The **undo heartbeat** command restores the default heartbeat detection timeout period and retry count.

By default, the timeout period is ten seconds, and the retry count is three.

Format

heartbeat { **timeout** *time* | **retrycount** *count* } *

undo heartbeat [**timeout** | **retrycount**]

Parameters

Parameter	Description	Value
timeout*time*	Specifies the heartbeat detection timeout period.	The value an integer that ranges from 5 to 3600, in seconds. The default value is 10s.
retrycount*count*	Specifies the heartbeat detection retry count.	The value is an integer that ranges from 1 to 10. The default value is 3.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

A local gatekeeper sends heartbeat messages to check whether there is a peer gatekeeper. If the peer gatekeeper responds to the heartbeat message, the status of the trunk group is in the normal state. If the heartbeat detection retry count exceeds the threshold, the status of the trunk is in the failed state.

NOTE

Heartbeat detection parameters must be configured only when the H323 trunk works in gk-gk mode.

Example

Set the heartbeat detection timeout period of the H323 trunk **test** to 30 seconds and the heartbeat detection retry count to 6.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 gk-gk
[Huawei-voice-trunkgroup-test] heartbeat timeout 30 retrycount 6
```

16.5.6.51 home-domain (trunk group view)

Function

Using the **home-domain** command, you can specify the domain to which the peer SIP trunk group belongs.

Format

home-domain *value*

Parameters

Parameter	Description	Value
value	Specifies the name of the domain to which the peer IP trunk group belongs.	The value is a string of 1 to 32 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only the trunk group of the SIP type supports the **home-domain** command. Before using the **home-domain** command, run the **trunk-group** command to create a trunk group of the SIP type.

The domain names configured at both ends must be the same.

Example

Set the name of the domain to which the peer IP trunk group belongs to abcd.com.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-group
[Huawei-voice-trunkgroup-test] home-domain abcd.com
```

16.5.6.52 line-signal-receive

Function

Using the **line-signal-receive** command, you can set line signaling input parameters for an R2 signaling type.

Using the **undo line-signal-receive** command, you can restore the default line signaling input parameters for an R2 signaling type.

Format

line-signal-receive *line-phy-signal-type line-phy-cmd line-phy-cmd-para line-call-state* { *line-logic-cmd* | **no-process** }

undo line-signal-receive *line-phy-signal-type line-phy-cmd line-phy-cmd-para line-call-state*

Parameters

Parameter	Description	Value
line-phy-signal-type	Specifies the logical signaling type on an E1 line.	The value is an integer that ranges from 0 to 3. A value corresponds to a signaling type.
line-phy-cmd	Specifies a physical command on an E1 line.	The value is an integer that ranges from 0 to 15. A value corresponds to a physical command.
line-phy-cmd-para	Specifies a parameter in a physical command on an E1 line.	The value is an integer that ranges from 0 to 7. A value corresponds to a parameter.
line-call-state	Specifies the call status on an E1 line.	The value is an integer that ranges from 0 to 31. A value corresponds to one call status.
line-logic-cmd	Specifies a logical command on an E1 line.	The value is an integer that ranges from 0 to 255. A value corresponds to a logical command.
no-process	Specifies an invalid command.	-

Views

R2 signaling type view

Default Level

2: Configuration level

Usage Guidelines

To enable the device to communicate with a non-Huawei device supporting R2 signaling, run the **line-signal-receive** command to adjust line signaling input parameters if the two devices define different line signaling input parameters.

Example

Set the logical signaling type to 1, physical command to 1, physical command parameter to 1, call status to 1, and logical command to 1 for the R2 signaling type **test**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] r2 signalling-type test
[Huawei-voice-r2-signalling-type-test] line-signal-receive 1 1 1 1 1
```

16.5.6.53 line-signal-send

Function

Using the **line-signal-send** command, you can set line signaling output parameters for an R2 signaling type.

Using the **undo line-signal-send** command, you can restore the default line signaling output parameters for an R2 signaling type.

Format

line-signal-send *line-logic-cmd* { *line-logic-signal-type line-phy-cmd-para line-call-state line-phy-send-time* | **no-process** }

undo line-signal-send *line-logic-cmd*

Parameters

Parameter	Description	Value
line-logic-cmd	Specifies a parameter in a logical command.	The value is an integer that ranges from 0 to 63. A value corresponds to a parameter.
line-logic-signal-type	Specifies a logical signaling type.	The value is an integer that ranges from 0 to 3. A value corresponds to a signaling type.
line-phy-cmd-para	Specifies a physical command on an E1 line.	The value is an integer that ranges from 0 to 255. A value corresponds to a physical command.
line-call-state	Specifies the call status on an E1 line.	The value is an integer that ranges from 0 to 255. A value corresponds to one call status.
line-phy-send-time	Specifies the period during which line signaling is sent.	The value is an integer that ranges from 0 to 255.
no-process	Specifies an invalid command.	-

Views

R2 signaling type view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

To enable the device to communicate with a non-Huawei device supporting R2 signaling, run the **line-signal-send** command to adjust line signaling output parameters if the two devices define different line signaling output parameters.

Example

Set the logical command parameter to 1, logical signaling type to 1, physical command to 1, call status to 1, and line signaling transmitting duration to 1 for the R2 signaling type **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 signalling-type test
[Huawei-voice-r2-signalling-type-test] line-signal-send 1 1 1 1 1
```

16.5.6.54 line-signalling

Function

Using the **line-signalling** command, you can configure line signaling attributes in an R2 profile.

Using the **undo line-signalling** command, you can restore the default line signaling attributes in an R2 profile.

Format

line-signalling { **line-signalling-type** *line-signalling-type-value* | **wait-answer-time** *wait-answer-time-value* | **wait-clear-forward-time** *wait-clear-forward-time-value* | **wait-protect-time** *wait-protect-time-value* | **wait-seize-ack-time** *wait-seize-ack-time-value* }

undo line-signalling { **line-signalling-type** | **wait-answer-time** | **wait-clear-forward-time** | **wait-protect-time** | **wait-seize-ack-time** }

Parameters

Parameter	Description	Value
line-signalling-type *line-signalling-type-value*	Specifies the line signaling type.	Enumerated type. The values are as follows: L1B, L2B, L3B and PULSE. The default value is L2B.
wait-answer-time *wait-answer-time-value*	Specifies the time at which answer signals are identified.	The value is an integer that ranges from 0 to 511, in seconds. The default interval is 300.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wait-clear-forward-time *wait-clear-forward-time-value*	Specifies the time at which clear-forward (CLF) signals are identified.	The value is an integer that ranges from 0 to 2000, in milliseconds. The default interval is 200.
wait-protect-time *wait-protect-time-value*	Specifies the protection duration.	The value is an integer that ranges from 0 to 2000, in milliseconds. The default interval is 200.
wait-seize-ack-time *wait-seize-ack-time-value*	Specifies the waiting time for signal seizing acknowledgement.	The value is an integer that ranges from 0 to 7000, in milliseconds. The default interval is 5000.

Views

R2 profile view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the value of **wait-seize-ack-time** to 400 ms in the R2 profile **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 profile test
[Huawei-voice-r2-profile-test] line-signalling wait-answer-time 400
```

16.5.6.55 localip

Function

The **localip** command configures the default local IP address.

The **undo localip** command restores the default local IP address.

By default, the default local IP address is 255.255.255.255.

Format

localip *ip-address*

undo localip

Parameters

Parameter	Description	Value
ip-address	Specifies the default local IP address.	The value is in dotted decimal notation.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the default local IP address of the H323 stack to 192.168.0.1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] localip 192.168.0.1
```

16.5.6.56 maxcr (trunk group view)

Function

Using the **maxcr** command, you can set the maximum number of concurrent calls in a SIP trunk group.

Using the **undo maxcr** command, you can restore the default maximum number of concurrent calls in a SIP trunk group.

By default, a maximum of 65535 concurrent calls are allowed.

Format

maxcr *maxcr-value*

undo maxcr

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
maxcr-value	Specifies the maximum number of concurrent calls in a trunk group.	The value is an integer that ranges from 1 to *N*. **NOTE** *N* indicates the maximum number of users supported by the device minus the number of configured users.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only the trunk group of the SIP or H.323 type supports the **maxcr** command. Before using the **maxcr** command, run the **trunk-group** command to create a trunk group of the SIP or H.323 type.

Example

Set the maximum number of concurrent calls in the trunk group **test** to 256.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-group
[Huawei-voice-trunkgroup-test] maxcr 256
```

16.5.6.57 media-bandwidth-control enable (trunk-group)

Function

The **media-bandwidth-control enable** command enables CAC on a trunk group.

The **undo media-bandwidth-control** command disables CAC on a trunk group.

By default, CAC is disabled on a trunk group.

Format

media-bandwidth-control enable

undo media-bandwidth-control

Parameters

None

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The bandwidth is limited on the IP bearer network. If voice data is transmitted through the IP bearer network, the voice communication may be restricted by the bandwidth of the IP bearer network. When POTS users make incoming and outgoing calls through a SIP trunk group, the media bandwidth in the trunk group is occupied. More voice calls occupy more bandwidth on the network. To improve the voice communication quality, run the **media-bandwidth-control enable** command to enable CAC on the trunk group.

NOTE

- When SIP UE users in a SIP trunk group make incoming and outgoing calls, the bandwidth of common IP packets on the IP network, instead of the media bandwidth on the trunk group, is occupied.
- The **media-bandwidth-control enable** command only applies to SIP trunk groups.

Prerequisites

A trunk group has been created using the **trunk-group** command.

Follow-up Procedure

Run the **media-bandwidth-control max-bandwidth (trunk-group)** command to set the maximum media bandwidth of a trunk group.

Example

Enable CAC on the SIP trunk group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sipip sip
[Huawei-voice-trunkgroup-sipip] media-bandwidth-control enable
```

16.5.6.58 media-bandwidth-control max-bandwidth (trunk-group)

Function

The **media-bandwidth-control max-bandwidth** command sets the maximum media bandwidth in a trunk group.

The **undo media-bandwidth-control max-bandwidth** command restores the default maximum media bandwidth in a trunk group.

By default, the maximum media bandwidth in a trunk group is 500000 kbit/s.

Format

media-bandwidth-control max-bandwidth *max-bandwidth-value*

undo media-bandwidth-control max-bandwidth

Parameters

Parameter	Description	Value
max-bandwidth-value	Specifies the maximum media bandwidth in a trunk group.	The value is an integer that ranges from 1 to 5000, in 100 kbit/s. The default value is 5000, that is, 500000 kbit/s.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **media-bandwidth-control max-bandwidth** command sets the maximum media bandwidth in a trunk group after CAC is enabled on the trunk group by using the **media-bandwidth-control enable (trunk-group)** command. If the **media-bandwidth-control max-bandwidth** command is not run, and CAC is enabled on the trunk group, the default maximum media bandwidth is 500000 kbit/s. When the media bandwidth in the trunk group is used up, the system limits incoming and outgoing calls made by POTS users through SIP trunk groups.

NOTE

- When SIP UE users in a SIP trunk group make incoming and outgoing calls, the bandwidth of common IP packets on the IP network, instead of the media bandwidth on the trunk group, is occupied.
- The **media-bandwidth-control max-bandwidth** command only applies to SIP trunk groups.

Prerequisites

CAC has been enabled on the trunk group using the **media-bandwidth-control enable (trunk-group)** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum media bandwidth in the SIPIP trunk group to 400000 kbit/s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sipip
[Huawei-voice-trunkgroup-sipip] media-bandwidth-control enable
[Huawei-voice-trunkgroup-sipip] media-bandwidth-control max-bandwidth 4000
```

16.5.6.59 media-ip (H323 Trunk group view)

Function

The **media-ip** command configures a media IP address or a dynamic media IP address name for an H323 trunk group.

By default, no media IP address or dynamic media IP address name is configured for an H323 trunk group.

Format

media-ip { *ip-address* | **addr-name** *addr-name-value* }

Parameters

Parameter	Description	Value
ip-address	Specifies a media IP address for an H323 trunk group.	The value is in dotted decimal notation.
addr-name *addr-name-value*	Specifies a dynamic media IP address name for an H323 trunk group.	The value is a string of 1 to 64 case-insensitive characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before configuring a media IP address for an H323 trunk group, create a media IP address or a dynamic media IP address name.

Example

Configure a media IP address 192.168.0.2 for an H323 trunk group.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test h323 register-gateway
[Huawei-voice-trunkgroup-test] media-ip 192.168.0.2
```

16.5.6.60 media-ip (SIP Trunk group view)

Function

Using the **media-ip** command, you can configure a media IP address or a dynamic media IP address name for a SIP trunk group.

By default, no media IP address or dynamic media IP address name is configured for a SIP trunk group.

Format

media-ip { *ip-address* | **addr-name** *addr-name-value* }

Parameters

Parameter	Description	Value
ip-address	Specifies a media IP address for a SIP trunk group.	The value is in dotted decimal notation.
addr-name *addr-name-value*	Specifies a dynamic media IP address name for a SIP trunk group.	The value is a string of 1 to 64 case-insensitive characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

The following operations must have been performed before this command is used:

- Run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a trunk group of the SIP type. This is because only the trunk group of the SIP type supports the **media-ip** command.
- Create a media IP address or dynamic media IP address name.

Example

Configure a media IP address 192.168.0.2 for a SIP trunk group.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group siptrkgrp sip trunk-group
[Huawei-voice-trunkgroup-siptrkgrp] media-ip 192.168.0.2
```

16.5.6.61 medialoop-timeout

Function

The **medialoop-timeout** command sets the timeout interval of the media loop process.

The **undo medialoop-timeout** command restores the default timeout interval of the media loop process.

By default, the timeout interval of the media loop process is 15000 ms.

Format

medialoop-timeout *medialoop-timeout-value*

undo medialoop-timeout

Parameters

Parameter	Description	Value
medialoop-timeout-value	Specifies the timeout interval of the media loop process.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the timeout interval of the media loop process to 50000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] medialoop-timeout 50000
```

16.5.6.62 nte-fax-modem

Function

Using the **nte-fax-modem** command, you can enable or disable RFC 2833 fax and modem transmission on a PBX.

Using the **undo nte-fax-modem** command, you can restore the default configuration on a PBX.

By default, RFC 2833 fax and modem transmission is enabled.

Format

nte-fax-modem { **enable** | **disable** }

undo nte-fax-modem

Parameters

Parameter	Description	Value
enable	Enables RFC 2833 fax and modem transmission.	-
disable	Disables RFC 2833 fax and modem transmission.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only SIP or H323 trunk groups support the **nte-fax-modem** command. Before using the **nte-fax-modem** command, run the **trunk-group** command to create a SIP trunk group.

Example

Enable RFC 2833 fax and modem transmission on a PBX.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] nte-fax-modem enable
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.63 nte-negotiation-mode

Function

Using the **nte-negotiation-mode** command, you can configure the mode in which RFC 2833 transmission is started.

Using the **undo nte-negotiation-mode** command, you can restore the default mode in which RFC 2833 transmission is started.

By default, the mode in which RFC 2833 transmission is started is **no-initiative-start**.

Format

nte-negotiation-mode { **negotiation** | **fixed-start** | **no-initiative-start** }

undo nte-negotiation-mode

Parameters

Parameter	Description	Value
negotiation	Indicates the initiative startup mode.	-
fixed-start	Indicates the fixed startup mode.	-
no-initiative-start	Indicates the no-initiative startup mode.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only SIP or H323 trunk group support the **nte-negotiation-mode** command. Before using the **nte-negotiation-mode** command, run the **trunk-group** command to create a SIP trunk group.

The **nte-negotiation-mode** command configures the mode in which RFC 2833 transmission is started:

- Initiative startup: RFC 2833 transmission is started after negotiation between the local end and remote end succeeds. The negotiation may be initiated by the local end or remote end.

 Copyright © Huawei Technologies Co., Ltd.

- Fixed startup: The local end does not initiate any negotiation but accepts negotiation requests. If negotiation fails, RFC 2833 transmission is started based on the local configuration.
- No-initiative startup: RFC 2833 transmission starts only after the local end receives the negotiation request from the remote end.

Example

Set the mode in which RFC 2833 transmission is started to fixed startup.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] nte-negotiation-mode fixed-start
```

16.5.6.64 num-plan-identify called

Function

The **num-plan-identify called** command configures a numbering plan for called numbers of a PRA or BRA trunk.

The **undo num-plan-identify called** command cancels the configuration.

By default, a numbering plan for called numbers of a PRA or BRA trunk is not configured.

Format

num-plan-identify called *numplanidentify-value*

undo num-plan-identify called

Parameters

Parameter	Description	Value
numplanidentify-value	Specifies a numbering plan for called numbers.	Enumerated value: • unknown: unknown. • isdn: ISDN/telephony numbering plan. • data: data numbering plan. • telex: telex numbering plan. • national: national standard numbering plan. • private: private numbering plan.

 Copyright © Huawei Technologies Co., Ltd.

Views

PRA or BRA trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a communication network, a numbering plan refers to the structure and allocation rules of numbers. You need to configure a numbering plan based on requirements of the remote device during interconnection between devices.

Precautions

Before configuring a numbering plan, run the **trunk-group** command to create a trunk group.

Example

Set the data numbering plan for called numbers of a PRA trunk.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group pra
[Huawei-voice-trunk-group-pra] num-plan-identify called data
```

16.5.6.65 num-plan-identify caller

Function

The **num-plan-identify caller** command configures a numbering plan for calling numbers of a PRA or BRA trunk.

The **undo num-plan-identify caller** command cancels the configuration.

By default, a numbering plan for calling numbers of a PRA or BRA trunk is not configured.

Format

num-plan-identify caller *numplanidentify-value*

undo num-plan-identify caller

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
numplanidentify-value	Specifies a numbering plan for calling numbers.	Enumerated value: • unknown: unknown. • isdn: ISDN/telephony numbering plan. • data: data numbering plan. • telex: telex numbering plan. • national: national standard numbering plan. • private: private numbering plan.

Views

PRA or BRA trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a communication network, a numbering plan refers to the structure and allocation rules of numbers. You need to configure a numbering plan based on requirements of the remote device during interconnection between devices.

Precautions

Before configuring a numbering plan, run the **trunk-group** command to create a trunk group.

Example

Set the data numbering plan for calling numbers of a PRA trunk.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group pra
[Huawei-voice-trunk-group-pra] num-plan-identify caller data
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.66 number-parameter (trunk group view)

Function

The **number-parameter** command configures the numeral control point and its index.

The **undo number-parameter** command deletes the configured numeral control point and its index.

Format

number-parameter *numpara-no numpara-value*

undo number-parameter *numpara-no*

Parameters

Parameter	Description	Value
numpara-no	Specifies the index of a numeral control point.	The value is an integer that ranges from 0 to 136.
numpara-value	Specifies the value of a numeral control point.	The value is an integer that ranges from 0 to 4294967295. The value of *numpara-value* varies according to *numpara-no*. For details, see the usage guideline.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Only SIP trunk groups support the **number-parameter** command. Before using the **number-parameter** command, run the **trunk-group** command to create a SIP trunk group.

The following table describes the meanings and values of control points.

Parameter	Description	Value
0	Indicates whether a SUBSCRIBE message is sent after a SIP trunk is registered successfully.	Enumerated value: ● 0: The SUBSCRIBE message is not sent. ● 1: The SUBSCRIBE message is sent. The default value is 0.
1	Specifies the registration lifecycle of a SIP trunk group.	The value is an integer that ranges from 60 to 65534, in seconds. The default value is 600.
2	Specifies the special events supported by the SIP trunk group.	Besides basic events, the SIP trunk supports the following special events: ● TAC_NULL = 0x00 ● TAC_100REL = 0x01 ● TAC_REPLACES = 0x02 ● TAC_TIMER = 0x04 ● TAC_PRIVACY = 0x08 ● TAC_PRECONDITION = 0x10 ● TAC_HISTINFO = 0x20 ● TAC_JOIN = 0x40 ● TAC_ANSWERMODE = 0x80 ● TAC_DTMFINFO = 0x100 ● TAC_FROMCHANGE = 0x200 ● TAC_INDIALOG = 0x400 ● PREF = 0x800 ● URI_LIST = 0x1000 ● NOREFERSUB = 0x2000 ● SUBSCRIPTION = 0x8000 ● DIV_INFO = 0x10000 ● DND_INFO = 0x20000 ● OVERLAP = 0x80000 The device supports the following events: REGISTER, INVITE, SUBSCRIBE, BYE, PRACK, REFER, UPDATE, ACK, OPTIONS, CANCEL, INFO. The default value is 1039.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
3	Specifies the header field from which the calling number is obtained for the SIP trunk group.	Enumerated value: ● 0: The calling number is obtained from the P-Asserted-Identity header field. ● 1: The calling number is obtained from the From header field. The default value is 0.
4	Reserved.	-
5	Specifies the content of the Invite From header field for the trunk group.	Enumerated value: ● 1: Tel+PublicID. ● 2: Tel PublicID. ● 3: User-defined format. The default value is 1.
6	Indicates whether the plus sign (+) is added to the register from header field for the trunk group.	Enumerated value: ● 0: Plus sign (+) is not added. ● 1: Plus sign (+) is added. The default value is 0.
7	Indicates user=phone is added to the register from header field in SIP mode for the trunk group.	Enumerated value: ● 0: user=phone is not added. ● 1: user=phone is added. The default value is 0.
8	Specifies the delay in sending a SUBSCRIBE message after a SIP trunk is registered successfully.	The value is an integer that ranges from 0 to 60, in seconds. The default value is 0. 0 indicates that the SUBSCRIBE message is sent immediately after a SIP trunk is registered successfully.
9	Indicates whether SDP-Answer in a received 18X message overwrites SDP-Answer in the original 18X message.	Enumerated values: ● 0: SDP-Answer in a received 18X message does not overwrite SDP-Answer in the original 18X message. ● 1: SDP-Answer in a received 18X message overwrites SDP-Answer in the original 18X message. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
10	Indicates whether SDP-Answer in a received 200 message overwrites SDP-Answer in the original 200 message.	Enumerated value: ● 0: SDP-Answer in a received 200 message does not overwrite SDP-Answer in the original 200 message. ● 1: SDP-Answer in a received 200 message overwrites SDP-Answer in the original 200 message. The default value is 0.
11	Indicates whether the trunk group carries extended Centrex group number.	Enumerated value: ● 0: Not supported. ● 1: Supported. If the relay group registers the default value is 0, the other case the default value is 1.
12	Indicates whether INVITE and REGISTER messages carry routes for the trunk group.	Enumerated value: ● 0: The INVITE and REGISTER messages do not carry routes. ● 1: The INVITE and REGISTER messages carry routes. The default value is 1.
13	Specifies the REGISTER authentication mode for the trunk group.	Enumerated value: ● 1: Users who call over the trunk group share one user name and password for authentication. ● 2: Each user has a user name and password for authentication. The default value is 2.
14	Specifies the format of the REGISTER From header field.	Enumerated value: ● 1: S/S/P format. ● 2: SIP format. ● 3: TEL format. The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
15	Specifies the format of the register contact header field.	Enumerated value: ● 1: S/S/P format. ● 2: SIP format. ● 3: TEL format. The default value is 2.
16	Specifies the format of the subscribe RequestURI, From, and To header fields.	Enumerated value: ● 1: Public ID in SIP format. ● 2: Public ID in TEL format. ● 3: Temporary public ID. The default value is 1.
17	Specifies the subscribe Contact format for the trunk group.	Enumerated value: ● 1: Reserved. ● 2: SIP format. ● 3: TEL format. The default value is 2.
18	Specifies the Invite Contact format for the trunk group.	Enumerated value: ● 1: Reserved. ● 2: SIP format. ● 3: TEL format. The default value is 2.
19	Specifies the user name format for user authentication for the trunk group.	Enumerated value: ● 0: Userinfo. ● 1: Userinfo@domain. ● 2: User-defined. The default value is 0.
20	Indicates whether authentication is enabled during the call.	Enumerated value: ● 0: Authentication is not enabled during the call. ● 1: Authentication is enabled during the call. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
21	Indicates whether the number sign (#) in the called number is converted into 23.	Enumerated value: ● 0: The number sign (#) is not converted into 23 when parameter User=Phone is contained. ● 1: All number signs (#) are converted into 23. ● 2: None of number signs (#) is converted into 23. The default value is 0.
22	Reserved.	-
23	Indicates whether a CANCEL message is sent to peer end when the trunk group receives the REINVITE message.	Enumerated value: ● 0: The CANCEL message is not sent. ● 1: The CANCEL message is sent. The default value is 0.
24	Indicates whether the serial sending function is enabled for trunk group messages.	Enumerated value: ● 0: The serial sending function is not enabled. ● 1: The serial sending function is enabled. The default value is 0.
25	Specifies the maximum retransmission count of Invite messages after the trunk group receives the 301 or 302 message.	The value is an integer that ranges from 0 to 16. The default value is 1.
26	Specifies the format of the To header field for the trunk group.	Enumerated value: ● 1: TelNum@homedomain (number @ local domain name). ● 2: TelNum@proxydomain (number @ Proxy Server domain name). ● 3: telURI (number + URI). The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
27	Indicates whether number regulation is enabled for the trunk group.	Enumerated value: ● 0: Number regulation is not enabled. ● 1: Number regulation is enabled. The default value is 1.
28	Specifies the prefix conversion type when URI is of international toll number type during number regulation of the trunk group.	Enumerated value: ● 1: The prefix is plus sign (+). ● 2: No prefix is used. ● 3: With international toll call prefix. The default value is 1.
29	Specifies the duration in which the session in Invite messages is updated for the trunk group.	The value is an integer that ranges from 90 to 86400, in seconds. The default value is 1800.
30	Indicates whether authentication information is added to a session request.	Enumerated value: ● 0: No authentication information is added. ● 1: Authentication information is added. The default value is 0.
31	Specifies the value of the realm in authentication messages for the trunk group.	Enumerated value: ● 0: The value of the realm in authentication messages from the peer end is used. ● 1: The home domain configured on the interface is used. The default value is 0.
32	Specifies the returned value of OPTION in a call when the peer end status is tested.	Enumerated value: ● 0: 486 is returned when the called user is busy. ● 1: 200 is returned when the called user is busy. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
33	Specifies the mode of checking the proxy server for the trunk group.	Enumerated value: ● 0: OPTIONS. ● 1: Heartbeat detection in probe mode. ● 2: REGISTER. The default value is 2. The probe mode takes effect only when the IMS Core dual-homing function is not supported. If the server is configured to support the IMS Core dual-homing function, the OPTIONS and REGISTER modes are used. The REGISTER is the default mode in a common process. The REGISTER mode is the default mode in the DT process.
34	Specifies the average roundtrip time **T1** for MSAN and the IMS Core messages.	The value is an integer that ranges from 50 to 5000, in milliseconds. The default value is 500.
35	Specifies the interval (unit time: T1) for sending OPTIONS message in normal state.	The value is an integer that ranges from 1 to 65535, in T1. The default value is 10.
36	Specifies the interval (unit time: T1) for sending OPTIONS message in faulty state.	The value is an integer that ranges from 1 to 100, in T1. The default value is 20.
37	Specifies the duration (unit time: T1) of the timer for detecting transactions.	The value is an integer that ranges from 1 to 30, in T1. The default value is 3.
38	Specifies the fault identification threshold. When the threshold is reached, the status of the detected object changes from **Normal** to **Failed**.	The value is an integer that ranges from 1 to 30. The default value is 3.
39	Specifies the threshold for identifying fault rectification. When the threshold is reached, the status of the detected object changes from **Failed** to **Normal**.	The value is an integer that ranges from 1 to 60. The default value is 6.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
40	Specifies the duration of the timer for detecting the proxy server status.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
41	Specifies the duration during which the standby proxy server switches to the active proxy server.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 21600. It is the duration during which the standby proxy server switches to the active proxy server when the active proxy server fails and the proxy server status is detected in register mode.
42	Indicates whether the trunk group supports the dual-homing function.	Enumerated value: ● 0: The dual-homing function is not supported. ● 1: The dual-homing function is supported. The default value is 0.
43	Indicates whether re-registration is initiated immediately when the trunk group is switched to the proxy server.	Enumerated value: ● 0: Re-registration is initiated after the refresh timer times out. ● 1: Re-registration is immediately initiated. The default value is 0.
44	Indicates whether the ongoing call is released during proxy server switching.	Enumerated value: ● 0: All calls are released. ● 1: All calls are held. ● 2: Releasing calls depends on whether the Session Timer is supported. The default value is 0.
45	Specifies the period for domain name resolution during URI registration for the trunk group.	The value is an integer ranging from 0 to 65535, in seconds. The default value is 90.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
46	Specifies the refresh mode for domain name resolution during the URI registration for the trunk group.	Enumerated value: ● 0: The refresh duration that is configured in the profile is used. The refresh duration is static. ● 1: The refresh duration that is returned from the DNS server is used. The refresh duration is dynamic. The default value is 0.
47	Reserved.	-
48	Indicates whether the trunk group switches back to the active proxy server when the active proxy server recovers.	Enumerated value: ● 0: Automatic switchback is not performed. ● 1: Automatic switchback is performed.
49	Indicates whether the trunk group stops playing the early media and starts to play the local ringback tone when the trunk group receives a 180 or 183 message right now and has received a 180 or 183 message with an SDP field.	Enumerated value: ● 0: The early media is played continuously. ● 1: The early media is stopped and the local ringback tone starts to be played when receive 180. ● 2: The early media is stopped and the local ringback tone starts to be played when receive 183. ● 3: The early media is stopped and the local ringback tone starts to be played when receive 180 or 183. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
50	Specifies the temporary response policy when the PBX is used as the called party.	Enumerated value: ● 0: The ringback tone SDP information is contained in SIP 180 messages. ● 1: The ringback tone SDP information is contained in SIP 183 messages. ● 2: The PBX sends a SIP 180 message after sending a SIP 183 message. The default value is 0.
51	Specifies the SDP stream mode when the PBX initiates a hookflash action.	Enumerated value: ● 0: SendOnly. ● 1: SendRecv. ● 2: Inactive. The default value is 1.
52	Indicates whether a new socket is created when a PBX IP trunk group receives a 302 message.	Enumerated value: ● 0: A new socket is not created when a PBX IP trunk group receives a 302 message. ● 1: A new socket is created when a PBX IP trunk group receives a 302 message. The default value is 1.
53	Indicates whether the connection can be bound to the proxy IP address of the peer end, port number of the peer end, local IP address, and local port number.	Enumerated value: ● 0: The connection cannot be bound with the proxy IP address of the peer end, the port ID of the peer end, the local IP address, and the local port ID. ● 1: The connection can be bound with the proxy IP address of the peer end, the port ID of the peer end, the local IP address, and the local port ID. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
54	Specifies a header field in the INVITE message, which is generated when a local user call is forwarded to a SIP trunk, to indicate forwarding.	Enumerated value: ● 0: History-info header field ● 1: Diversion header field The default value is 0.
55	Indicates whether INFO signaling is allowed to send digits during a call.	Enumerated value: ● 0: INFO signaling is not allowed to send digits during a call. ● 1: INFO signaling is allowed to send digits during a call. The default value is 0.
56	Specifies the maximum number of dynamic connections that TCP or TLS can request in the trunk group.	The value is an integer that ranges from 0 to 4294967295. The default value is 4294967295. When the maximum number is set to 4294967295, the number of dynamic connections is not limited.
57	Specifies the codec priority for the trunk group.	Enumerated value: ● 0: The global parameter is used. ● 1: The priority is defined on an interface. The default value is 0.
58	Reserved.	-
59	Specifies the format of **user=** for RequestURI and To URI fields in INVITE messages when the number to be parsed is not of international toll number type and no matter whether number regulation is initiated.	Enumerated value: ● 0: The parameters are not contained. ● 1: user=phone ● 2: user=dialstring ● 3: user=ip (not supported) The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
60	Specifies the switchback mode of the active proxy server when the trunk group is in **register** mode.	Enumerated value: ● 0: The switchback is performed when the timer times out. ● 1: An immediate switchback is performed. The default value is 0.
61	Reserved.	-
62	Indicates whether the ongoing call is released when 408 message is sent to respond to the request message.	Enumerated value: ● 0: The ongoing call is not released. ● 1: The ongoing call is released. The default value is 0.
63	Specifies the VAD negotiation mode for the trunk group.	Enumerated value: ● 0: The annexa or annexb parameter is not sent. Whether the G.723/G.729 VAD function is enabled depends on the local setting. ● 1: The annexa or annexb parameter is sent. Whether the G.723/G.729 VAD function is enabled depends on the SDP message from the peer. The default value is 0.
64	Indicates whether the early media is carried for the trunk group.	Enumerated value: ● 0: The early media is not carried. ● 1: The early media is carried. The default value is 0.
65	Indicates whether **HostUri** is used as the home domain name.	Enumerated value: ● 0: **HostUri** is not used as the home domain name. ● 1: **HostUri** is used as the home domain name. The default value is 0.
66	Reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
67	Indicates whether the SDP is carried in returned invite 200 message when negotiation of SIP 180 message is unreliable.	Enumerated value: ● 0: SDP is not carried in returned invite 200 message. ● 1: SDP is carried in returned invite 200 message. The default value is 1.
68	Indicates whether the trunk group receives packets from the proxy server when the trunk group receives the SIP 3xx message.	Enumerated value: ● 0: The trunk group does not receive packets from the proxy server. ● 1: The trunk group receives packets from the proxy server. The default value is 0.
69	Sets a mark for the device that updates the session.	Enumerated value: ● 0: The mark is not included. ● 1: UAC. ● 2: UAS. The default value is 0.
70	Configures whether to initiate VBD negotiation when there a delay in processing modem events. **NOTE** To set the delay in processing modem events, run the **pbx number-parameter 5** command.	Enumerated value: ● 0: VBD negotiation is not initiated. ● 1: VBD negotiation is initiated. The default value is 1.
71	Specifies the percentage value for calculating the registration refresh interval of the timer. Refresh interval = Registration timeout period – Registration timeout period*Percentage of the configured value	The value is an integer that ranges from 0 to 50, in percentage. The default value is 50.
72	Specifies the re-registration interval of the SIP trunk.	The value is an integer that ranges from 1 to 65535, in seconds. The default value is 30.
73	Specifies the re-registration count of the SIP trunk.	The value is an integer that ranges from 1 to 65535. The default value is 6.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
74	Specifies the re-registration algorithm.	Enumerated value: ● 0: re-registration count*interval. ● 1: exponential type, 2^ (re-registration count)*interval. ● 2: exponential type, 2^ (re-registration count/retry count)*interval. ● 3: NICC. ● 4: random algorithm. The default value is 0.
75	Specifies the minimum duration of the re-registration random algorithm.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 600.
76	Specifies the maximum duration of the re-registration random algorithm.	The value is an integer that ranges from 10 to 65535, in seconds. The default value is 900.
77	Specifies whether to play the call hold tone when the media stream is inactive.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
78	Configures whether the SIP trunk group converts SIP 183 messages into ISDN PROGRESS messages.	Enumerated value: ● 0: The SIP trunk group does not convert SIP 183 messages into ISDN PROGRESS messages. ● 1: The SIP trunk group converts SIP 183 messages into ISDN PROGRESS messages. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
79	Configures whether the SIP trunk group converts ISDN PROGRESS messages into SIP 183 messages.	Enumerated value: ● 0: The SIP trunk group does not convert ISDN PROGRESS messages into SIP 183 messages. ● 1: The SIP trunk group converts ISDN PROGRESS messages into SIP 183 messages. The default value is 0.
80	Reserved.	-
81	Specifies whether to encapsulate require100rel into the 18X message.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
82	Configures whether the SDP is repeated in the 200 OK message.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
83	Indicates whether to release the fork control block and send Cancel after the 200 OK response of the INVITE message is received.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 1.
84	Reserved.	-
85	Specifies whether to reply with the inactive message after the AR receives the sendonly message.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
86-113	Reserved.	-
114	Indicates whether the device plays the early media forcibly when receiving a 181 message without the SDP.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
115	Indicates whether the device encapsulates the DisplayName field in the From file and PAI or PPI header field of an Invite message.	Enumerated value: ● 0: Number. ● 1: Name. ● 2: None. The default value is 0.
116	Indicates whether to initiate re-negotiation after the RBT is played.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 1.
117	Specifies the threshold of INVITE message–based call barring.	The value is an integer that ranges from 0 to 1000, in packets per second. The default value is 30.
118-119	Reserved.	-
120	Indicates whether to play announcements to the peer end.	Enumerated value: ● 0: Announcements are not played to the peer end. ● 1: Announcements are played to the peer end. The default value is 0.
121	The delay time to send re-invite after early dialog end.	The value is an integer that ranges from 0 to 5, in seconds. The default value is 0.
122	Select the called number from which the message field	Enumerated value: ● 0: Select from P-Called-Num first, then RequestUri, last from To header field. ● 1: Select from RequestUri. ● 2: Select from To header field. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
123	Which events are allowed	Hex value. The options are as follows: ● ALO_NULL = 0x00 ● ALO_INVITE = 0x01 ● ALO_ACK = 0x02 ● ALO_OPTIONS = 0x04 ● ALO_BYE = 0x08 ● ALO_CANCEL = 0x10 ● ALO_REGISTER = 0x20 ● ALO_INFO = 0x40 ● ALO_PRACK = 0x80 ● ALO_SUBSCRIBE = 0x100 ● ALO_NOTIFY = 0x200 ● ALO_UPDATE = 0x400 ● ALO_MESSAGE = 0x800 ● ALO_REFER = 0x1000 ● ALO_PUBLISH = 0x2000 ● ALO_CONFSUB = 0X4000 The default value is 0x5FFF.
124	SIP trunk session refresh method	Enumerated value: ● 0: Negotiate. ● 1: Re-invite. The default value is 0.
125	From format for anonymous call of sip trunk	Enumerated value: ● 0: caller number@domain name ● 1: anonymous@domain name ● 2: anonymous@anonymous.invalid The default value is 1.
126	Whether a SIP AT0 trunk group's INVITE message fills caller number in from field with the registered number	Enumerated value: ● 0: No. ● 1: Yes. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
127	Indicates that SIP AT0/SIP PRA trunk group invite message contains the PPI field or PAI field.	Enumerated value: ● 0: PAI field. ● 1: PPI field. ● 2: No. ● 3: If a Downs Link user has the right of the CLIR service, the message contains the PAI field or PPI field. Otherwise, the message does not contain the PAI or PPI field. The default value is 1.
128	Whether to get request-line information from proxy.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
129	Specifies whether to enable the load balancing function when the remote device works in DNS-SRV mode.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
130	Specifies whether to play the ringback tone when the AR receives the message with the progress indicator of 1.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
131	Specifies whether SIP AT0 trunk supports the anonymous call.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
132	Specifies whether to switch the proxy server after the SIP registration trunk receives the 4xx5xx6xx message.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
133	Specifies whether to send the CNG message when T38 is used.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
134	Specifies whether SIP PRA gets PAI/PPI from register-id.	Enumerated value: ● 0: No. ● 1: Yes. The default value is 0.
135	Specifies whether start sbc transcoding	Enumerated value: ● 0: Not start. ● 1: Start. The default value is 0.
136	Specifies whether subsequent requests are sent to the address in the Contact header field when the Contact address in the received INVITE message is different from the remote address of the trunk group.	Enumerated value. The values are as follows: ● 0: No. ● 1: Yes. The default value is 0.

Precautions

After running the **number-parameter** command to configure a control point, run the **reset** command to reset the trunk group to make the configuration take effect.

Example

Configure the trunk group to initiate number regulation.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test
[Huawei-voice-trunkgroup-test] number-parameter 27 1
```

16.5.6.67 outgoing-right(trunk group view)

Function

The **outgoing-right** command configures the call-out right.

The **undo outgoing-right** command deletes the call-out right.

By default, the call-out rights are inter and local.

Format

outgoing-right { { **inter** *inter-value* | **local** *local-value* | **ddd** *ddd-value* | **idd** *idd-value* }* | **all** }

undo outgoing-right [**inter** | **local** | **ddd** | **idd**]

Parameters

Parameter	Description	Value
inter-value	Specifies the internal dialing call right.	Enumerated value. The value can be enable or disable. The default value is enable.
local-value	Specifies the local dialing call right.	Enumerated value. The value can be enable or disable. The default value is enable.
ddd-value	Specifies the domestic direct dialing call right.	Enumerated value. The value can be enable or disable. The default value is disable.
idd-value	Specifies the international direct dialing call right.	Enumerated value. The value can be enable or disable. The default value is disable.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the national toll call right.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-group
[Huawei-voice-trunkgroup-test] outgoing-right ddd enable
```

16.5.6.68 peer-address

Function

The **peer-address** command configures the remote domain name for an SIP trunk group.

Format

peer-address { **dns-a** *primary-domain-value primary-port-value* [**secondary** *secondary-domain-value secondary-port-value*] | **dns-srv** *domain-value* | **dns-naptr** *domain-value* }

Parameters

Parameter	Description	Value
dns-a	Indicates Class-A query, which is used to obtain the IP address corresponding to a specified domain name.	-
dns-srv	Indicates Service Record (SRV) query, which is used to obtain information about a server based on the protocol running on the server, including the server's domain name and port number.	-
dns-naptr	Indicates Naming Authority Pointer (NAPTR) query, which is used to obtain information about a server based on the server's domain name, including the IP address, port number, and the transmission protocol.	-
primary-domain-value	Specifies the domain name of the primary remote server for an SIP trunk group.	The value is a string of 1 to 64 characters.
primary-port-value	Specifies the port number of the primary remote server for an SIP trunk group.	The value is an integer ranging from 1 to 65535.
secondary-domain-value	Specifies the domain name of the secondary remote server for an SIP trunk group.	The value is a string of 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
secondary-port-value	Specifies the port number of the secondary remote server for an SIP trunk group.	The value is an integer ranging from 1 to 65535.
domain-value	Specifies the domain name of the remote server for an SIP trunk group.	The value is a string of 1 to 64 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

When the DNS server query mode is Class-A query, you can configure the domain names of primary remote servers for an SIP trunk group. Domain names and port numbers must be configured simultaneously.

When the DNS server query mode is SRV or NAPTR query, you only need to configure the remote domain name. The port number can be automatically obtained using the domain name. You can configure only one domain name when the DNS server query mode is SRV or NAPTR query.

Example

Configure the remote domain name as **aaa** for the SIP trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test no-register
[Huawei-voice-trunkgroup-test] peer-address dns-srv aaa
```

16.5.6.69 peer-address static (H323 trunk group view)

Function

The **peer-address static** command configures a remote IP address and port for an H.323 trunk group.

Format

peer-address static *primary-ip-value primary-port-value* [**secondary** *secondary-ip-valuese condary-port-value*]

Parameters

Parameter	Description	Value
primary-ip-value	Specifies the remote primary IP address of an H.323 trunk group.	The value is in dotted decimal notation.
primary-port-value	Specifies the remote primary port of an H.323 trunk group.	The value is an integer that ranges from 1 to 65535.
secondary	Specifies the remote secondary IP address and port of an H.323 trunk group.	-
secondary-ip-value	Specifies the remote secondary IP address of an H.323 trunk group.	The value is in dotted decimal notation.
secondary-port-value	Specifies the remote secondary port of an H.323 trunk group.	The value is an integer that ranges from 1 to 65535.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

You must set the remote IP address and port for an H.323 trunk group in peer mode.

Example

Set the remote IP address and port for an H.323 trunk group to 192.168.2.2 and 2000 respectively.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 gw-gk
[Huawei-voice-trunkgroup-test] peer-address static 192.168.2.2 2000
```

16.5.6.70 peer-address static (trunk group view)

Function

Using the **peer-address static** command, you can configure a remote IP address and port for a SIP or H323 trunk group.

Using the **undo peer-address secondary** command, you can remove second remote IP address and port for a SIP trunk group

Format

peer-address static *primary-ip-value primary-port-value* **[secondary** *secondary-ip-value secondary-port-value* **]**

undo peer-address secondary

Parameters

Parameter	Description	Value
primary-ip-value	Specifies the remote IP address of a SIP trunk group.	The value is in dotted decimal notation.
primary-port-value	Specifies the remote primary port of a SIP trunk group.	The value is an integer that ranges from 1 to 65535.
secondary	secondary remote IP and remote port of a SIP trunk group.	-
secondary-ip-value	Specifies the secondary remote IP address of a SIP trunk group.	The value is in dotted decimal notation.
secondary-port-value	Specifies the secondary remote port of a SIP trunk group.	The value is an integer that ranges from 1 to 65535.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the remote IP address and port for a SIP trunk group to 192.168.2.2 and 2000 respectively.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] peer-address static 192.168.2.2 2000
```

16.5.6.71 peer-address switchover

Function

Using the **peer-address switchover** command, you can switch services on a SIP trunk group to the primary or secondary trunk on the peer device.

Format

peer-address switchover *switchover-value*

Parameters

Parameter	Description	Value
switchover-value	Switches services on a SIP trunk group to the primary or secondary trunk on the peer device.	Enumerated type. The values are as follows: ● primary: switches services on a SIP trunk group to the primary trunk on the peer device. ● secondary: switches services on a SIP trunk group to the secondary trunk on the peer device.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Switch services on a SIP trunk group to the secondary trunk on the peer device.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test
[Huawei-voice-trunkgroup-test] peer-address switchover secondary
 Are you sure to switchover the trunkgroup?(y/n)[n]y
[Huawei-voice-trunkgroup-test]
```

16.5.6.72 pra-restart

Function

The **pra-restart** command configures the pra trunk send restart message or not.

By default, that is disable.

Format

pra-restart { **enable** | **disable**}

Parameters

None

Views

PRA trunk group view

Default Level

2: Configuration level

Usage Guidelines

After the PRA trunk send sabme, if received ua with link establish indication or confirm, if **pra-restart enable**, pra trunk will send restart message to peer-side, if **pra-restart disable**, pra trunk will not send restart message to peer-side.

Example

Configure **pra-restart enable** for the PRA trunk group pra01.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group pra01
[Huawei-voice-trunkgroup-pra01] pra-restart enable
```

16.5.6.73 priority(trunk group view)

Function

The **priority** *priority-value* command configures the priority of a trunk group.

The **undo priority** command restores the default priority of a trunk group.

Format

priority *priority-value*

undo priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of a trunk group.	Enumerated value. The value can be **default**, **normal**, **advanced**, or **super**. The default value is **default**.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the priority of a trunk group to **normal**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-group
[Huawei-voice-trunkgroup-test] priority normal
```

16.5.6.74 productname

Function

The **productname** command configures the H323 stack product name.

The **undo productname** command restores the default H323 product name.

By default, the H323 stack product name is HUAWEI-AR.

Format

productname *productname-value*

undo productname

Parameters

Parameter	Description	Value
productname-value	Specifies the H323 stack product name.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the H323 stack product name to **user**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] productname user
```

16.5.6.75 q931-listenport

Function

The **q931-listenport** command configures a Q931 signaling port.

The **undo q931-listenport** command restores the default Q931 signaling port.

By default, the Q931 signaling port is 1720.

Format

q931-listenport *q931listenport-value*

undo q931-listenport

Parameters

Parameter	Description	Value
q931listenport-value	Specifies the Q931 signaling port.	The value is an integer that ranges from 1 to 51200.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the Q931 signaling port to 1780.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] q931-listenport 1780
```

16.5.6.76 qos stream (trunk group view)

Function

Using the **qos stream** command, you can set the priority of voice packets during transmission.

Using the **undo qos stream** command, you can delete the DSCP parameter in media and signaling packets.

Format

qos stream { **media** | **signaling** } **dscp** *dscp-value*

undo qos stream [**media** | **signaling**]

Parameters

Parameter	Description	Value
dscp-value	Specifies the priority of the voice packets to be transmitted.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Trunk group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

When the network quality is poor, this command can be used to specify a higher priority for voice packets to ensure the voice quality.

Example

Set the priority of media packets to 0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sip
[Huawei-voice-trunkgroup-sip] qos stream media dscp 0
```

16.5.6.77 r2 profile

Function

Using the **r2 profile** command, you can create an R2 profile and enter the R2 profile view.

Using the **undo r2 profile** command, you can delete an R2 profile.

Format

r2 profile *profile-name*

undo r2 profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an R2 profile.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When configuring an E1R2 trunk group, bind an R2 profile to the E1R2 trunk group.

Example

Create an R2 profile named **test**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 profile test
[Huawei-voice-r2-profile-test]
```

16.5.6.78 r2 signalling-type

Function

Using the **r2 signalling-type** command, you can create an R2 signaling type and enter the R2 signaling type view or the existing R2 signaling type view.

Using the **undo r2 signalling-type** command, you can delete an R2 signaling type.

Format

r2 signalling-type *signalling-type-name*

undo r2 signalling-type *signalling-type-name*

Parameters

Parameter	Description	Value
signalling-type-name	Specifies the name of a signaling type.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Different countries define different R2 signaling standards. The **r2 signalling-type** command identifies the R2 signaling standard. By default, the R2 signaling types of argentina, brazil, mexico, and standard are defined, which cannot be deleted.

Example

Create an R2 signaling type **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 signalling-type test
[Huawei-voice-r2-signalling-type-test]
```

16.5.6.79 r2-play-ringback

Function

Using the **r2-play-ringback** command, you can enable an E1R2 trunk group to play ringback tones to the remote end.

Using the **undo r2-play-ringback** command, you can disable an E1R2 trunk group from playing ringback tones to the remote end.

By default, an E1R2 trunk group plays ringback tones to the remote end.

Format

r2-play-ringback *r2-play-ringback-value*

undo r2-play-ringback

Parameters

Parameter	Description	Value
r2-play-ringback-value	Specifies whether to play ringback tones to the remote end.	Enumerated type. The values are as follows: ● disable: indicates that the E1R2 trunk group does not play ringback tones to the remote end. ● enable: indicates that the E1R2 trunk group plays ringback tones to the remote end.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable an E1R2 trunk group to play ringback tones to the remote end.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test e1-r2
[Huawei-voice-trunkgroup-test] r2-play-ringback enable
```

16.5.6.80 r2-profile (trunk group view)

Function

Using the **r2-profile** command, you can bind an R2 profile to an E1R2 trunk group.

Format

r2-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of an R2 profile.	The value is a string of 1 to 32 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Bind the R2 profile **test** to the E1R2 trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 profile test
[Huawei-voicer-2-profile-test] quit
[Huawei-voice] trunk-group test e1-r2
[Huawei-voice-trunkgroup-test] r2-profile test
```

16.5.6.81 r2-receive-earlymedia

Function

Using the **r2-receive-earlymedia** command, you can determine whether an E1R2 trunk group uses early media.

Using the **undo r2-receive-earlymedia** command, you can disable an E1R2 trunk group from using early media.

By default, an E1R2 trunk group does not use early media.

Format

r2-receive-earlymedia *r2-receive-earlymedia-value*

undo r2-receive-earlymedia

Parameters

Parameter	Description	Value
r2-receive-earlymedia-value	Specifies whether an E1R2 trunk group uses early media.	Enumerated type. The values are as follows: ● disable: indicates that an E1R2 trunk group does not use early media. ● enable: indicates that an E1R2 trunk group uses early media.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Configure the E1R2 trunk group **test** to use early media.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test e1-r2
[Huawei-voice-trunkgroup-test] r2-receive-earlymedia enable
```

16.5.6.82 rasport

Function

The **rasport** command configures the UDP port number of RAS signals.

The **undo rasport** command restores the default UDP port number of RAS signals.

By default, the UDP port number of RAS signals is 1719.

Format

rasport *rasport-value*

undo rasport

Parameters

Parameter	Description	Value
rasport-value	Specifies the UDP port number of RAS signals.	The value is an integer that ranges from 1025 to 51200.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the UDP port number of RAS signals to 1720.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] rasport 1720
```

16.5.6.83 reanswer

Function

The **reanswer** command enables or disables the calling party control function for an E1R2 trunk group.

The **undo reanswer** command disables the calling party control function for an E1R2 trunk group.

By default, the calling party control function is disabled for an E1R2 trunk group.

Format

reanswer *reanswer-value*

undo reanswer

Parameters

Parameter	Description	Value
reanswer-value	Determines whether the calling party control function is enabled.	Enumerated value: ● disable: The calling party control function is disabled. ● enable: The calling party control function is enabled.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

In an E1R2 trunk scenario, calls on the local device (calling party side) are made through an R2 trunk. If the calling party control function is enabled, when the local device receives a **clear back** message from the remote device, the local device waits for 90s and keeps online but not immediately releases the call. During the 90s, if the local device receives an **answer** message sent by the remote device, the call continues; otherwise, the local device releases the call.

Example

Enable the calling party control function for an E1R2 trunk group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test e1-r2
[Huawei-voice-trunkgroup-test] reanswer enable
```

16.5.6.84 recvalert-wait-response-timeout

Function

The **recvalert-wait-response-timeout** command sets the timeout interval for Connect messages.

The **undo recvalert-wait-response-timeout** command restores the default timeout interval for Connect messages.

By default, the timeout interval for Connect messages is 500000 ms.

Format

recvalert-wait-response-timeout *recvalert-wait-response-timeout-value*

undo recvalert-wait-response-timeout

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
recvalert-wait-response-timeout-value	Specifies the timeout interval for Connect messages.	The value is an integer that ranges from 180000 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the timeout interval for Connect messages to 500000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] recvalert-wait-response-timeout 500000
```

16.5.6.85 redundancy-negotiation-mode

Function

Using the **redundancy-negotiation-mode** command, you can configure the mode in which RFC 2198 redundancy transmission is started based on negotiation.

Using the **undo redundancy-negotiation-mode** command, you can restore the default mode in which RFC 2198 redundancy transmission is started based on negotiation.

By default, the mode in which RFC 2198 redundancy transmission is started based on negotiation is **no-initiative-start**.

Format

redundancy-negotiation-mode { **negotiation** | **fixed-start** | **no-initiative-start** }

undo redundancy-negotiation-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
negotiation	Indicates the initiative startup mode.	-
fixed-start	Indicates the fixed startup mode.	-
no-initiative-start	Indicates the no-initiative startup mode.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only SIP trunk groups support the **redundancy-negotiation-mode** command. Before using the **redundancy-negotiation-mode** command, run the **trunk-group** command to create a SIP trunk group.

You can run the **redundancy-negotiation-mode** command to configure the mode in which RFC 2198 redundancy transmission is started based on negotiation:

- Initiative startup: RFC 2198 redundancy transmission is started only after negotiation between the local end and remote end succeeds. The negotiation may be initiated by the local end or remote end.
- Fixed startup: The local end does not initiate any negotiation but accepts initiated negotiation. If negotiation fails, RFC 2198 redundancy transmission is started based on the local configuration.
- No-initiative startup: RFC 2198 redundancy transmission starts only after the local end receives a negotiation request from the remote end. If negotiation fails, RFC 2198 redundancy transmission is not started.

Example

Configure the fixed startup mode for RFC 2198 redundancy transmission based on negotiation.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] redundancy-negotiation-mode fixed-start
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.86 redundancy-nte (trunk group view)

Function

Using the **redundancy-nte** command, you can enable a PBX trunk group to transmit RFC 2833 audio data using RFC 2198 redundancy transmission or disable this function.

Using the **undo redundancy-nte** command, you can cancel the configuration.

By default, a PBX trunk group is disabled from transmitting RFC 2833 audio data using RFC 2198 redundancy transmission.

Format

redundancy-nte { **enable** | **disable** }

undo redundancy-nte

Parameters

Parameter	Description	Value
enable	Enables a PBX trunk group to transmit RFC 2833 audio data using RFC 2198 redundancy transmission.	-
disable	Disables a PBX trunk group from transmitting RFC 2833 audio data using RFC 2198 redundancy transmission.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only the trunk group of the SIP type supports the **redundancy-nte** command. Before using the **redundancy-nte** command, run the **trunk-group** command to create a trunk group of the SIP type.

Example

Enable a PBX trunk group to transmit RFC 2833 audio data using RFC 2198 redundancy transmission.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] redundancy-nte enable
```

16.5.6.87 redundancy-start-mode (trunk group view)

Function

Using the **redundancy-start-mode** command, you can configure the mode used by a PBX trunk group to start RFC 2198 redundancy transmission.

Using the **undo redundancy-start-mode** command, you can restore the default mode used by a PBX trunk group to start RFC 2198 redundancy transmission.

By default, RFC 2198 redundancy transmission is started in ordinary mode.

Format

redundancy-start-mode { **ordinary2198** | **smart2198** }

undo redundancy-start-mode

Parameters

Parameter	Description	Value
ordinary2198	Starts RFC 2198 redundancy transmission in ordinary mode.	-
smart2198	Starts RFC 2198 redundancy transmission in smart mode.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only SIP trunk groups support the **redundancy-start-mode** command. Before using the **redundancy-start-mode** command, run the **trunk-group** command to create a SIP trunk group.

In smart startup mode, RFC 2198 redundancy transmission is started automatically when packet loss occurs.

Example

Configure the smart start mode for RFC 2198 redundancy transmission.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] redundancy-start-mode smart2198
```

16.5.6.88 redundancy-vbd (trunk group view)

Function

Using the **redundancy-vbd** command, you can enable a PBX trunk group to transmit voice-band data (VBD) using RFC 2198 redundancy transmission or disable this function.

Using the **undo redundancy-vbd** command, you can disable a PBX trunk group from transmitting VBD using RFC 2198 redundancy transmission.

By default, a PBX trunk group is enabled to transmit VBD using RFC 2198 redundancy transmission.

Format

redundancy-vbd { **enable** | **disable** }

undo redundancy-vbd

Parameters

Parameter	Description	Value
enable	Enables a PBX trunk group to transmit VBD using RFC 2198 redundancy transmission.	-
disable	Disables a PBX trunk group from transmitting VBD using RFC 2198 redundancy transmission.	-

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only SIP trunk groups support the **redundancy-vbd** command. Before using the **redundancy-vbd** command, run the **trunk-group** command to create a SIP trunk group.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable a PBX trunk group to transmit VBD using RFC 2198 redundancy transmission.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group 1
[Huawei-voice-trunkgroup-1] redundancy-vbd enable
```

16.5.6.89 register-E164-number (H323 trunk group view)

Function

The **register-E164-number** command configures a registration E.164 number on an H323 trunk group.

The **undo register-E164-number** command deletes a registration E.164 number on an H323 trunk group.

Format

register-E164-number *E164-telno-value*

undo register-E164-number *E164-telno-value*

Parameters

Parameter	Description	Value
register-E164-number *E164-telno-value*	Specifies a registration E.164 number on an H323 trunk group.	The value is a numeral string of 1 to 22 digits.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

When the trunk type is gw-gk, to register E.164 numbers with a gatekeeper, configure a registration E.164 number. After a registration E.164 number is configured, H323 registration messages sent by the device carry the registration E.164 number.

A maximum of 32 registration E.164 numbers can be configured.

Example

Set the registration E.164 number to 2000.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 gw-gk
[Huawei-voice-trunkgroup-test] register-E164-number 2000
```

16.5.6.90 register-address-receive

Function

Using the **register-address-receive** command, you can set the register address format in an R2 profile.

Using the **undo register-address-receive** command, you can restore the default format of the register address in an R2 profile.

Format

register-address-receive { **country-code** *value* | **distinctive-indication** *value* | **echo-cancellation** *value* | **circuit-character** *value* | **calling-number** *value* | **calling-user-type** *value* | **calling-user-priority** *value* | **calling-number-location** *calling-number-location-value* | **user-type-location** *user-type-location-value* }

undo register-address-receive { **country-code** | **distinctive-indication** | **echo-cancellation** | **circuit-character** | **calling-number** | **calling-user-type** | **calling-user-priority** | **calling-number-location** | **user-type-location** }

Parameters

Parameter	Description	Value
country-code *value*	Indicates whether the device receives the country code.	Enumerated type. The values are as follows: ● enable: indicates that the device receives the country code. ● disable: indicates that the device does not receive the country code. By default, the country code is not received.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
distinctive-indication *value*	Indicates whether the device receives the distinctive indication.	Enumerated type. The values are as follows: ● enable: indicates that the device receives the distinctive indication. ● disable: indicates that the device does not receive the distinctive indication. By default, the device does not receive the distinctive indication.
echo-cancellation *value*	Indicates whether the device receives echo cancellation information.	Enumerated type. The values are as follows: ● enable: indicates that the device receives echo cancellation information. ● disable: indicates that the device does not receive echo cancellation information. By default, the device does not receive echo cancellation information.
circuit-character *value*	Indicates whether the device receives the circuit character.	Enumerated type. The values are as follows: ● enable: indicates that the device receives the circuit character. ● disable: indicates that the device does not receive the circuit character. By default, the device does not receive the circuit character.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
calling-number *value*	Indicates whether the device receives the calling number.	Enumerated type. The values are as follows: ● enable: indicates that the device receives the calling number. ● disable: indicates that the device does not receive the calling number. By default, the device does not receive the calling number.
calling-user-type *value*	Indicates whether the device receives the calling user type.	Enumerated type. The values are as follows: ● enable: indicates that the device receives the calling user type. ● disable: indicates that the device does not receive the calling user type. By default, the device does not receive the calling user type.
calling-user-priority *value*	Indicates whether the device receives the calling user priority.	Enumerated type. The values are as follows: ● enable: indicates that the device receives the calling user priority. ● disable: indicates that the device does not receive the calling user priority. By default, the device does not receive the calling user priority.
calling-number-location *calling-number-location-value*	Specifies the calling number location in the register address.	The value is an integer ranging from 1 to 12. The default value is 1.
user-type-location *user-type-location-value*	Specifies the user type location in the register address.	The value is an integer ranging from 1 to 12. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Views

R2 profile view

Default Level

2: Configuration level

Usage Guidelines

R2 standards in different countries define different register address attributes. To enable different devices to interwork with each other, run the **register-address-receive** command to adjust register address attributes.

Example

Enable the device to receive the country code in the R2 profile **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 profile test
[Huawei-voice-r2-profile-test] register-address-receive country-code enable
```

16.5.6.91 register-address-send

Function

Using the **register-address-send** command, you can set the output register address format in an R2 profile.

Using the **undo register-address-send** command, you can restore the default format of the output register address in an R2 profile.

Format

register-address-send { **country-code** *value* | **distinctive-indication** *value* | **echo-cancellation** *value* | **circuit-character** *value* | **calling-number** *value* | **calling-user-priority** *value* }

undo register-address-send { **country-code** | **distinctive-indication** | **echo-cancellation** | **circuit-character** | **calling-number** | **calling-user-priority** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
country-code *value*	Indicates whether the device sends the country code.	Enumerated type. The values are as follows: ● enable: indicates that the device sends the country code. ● disable: indicates that the device does not send the country code. By default, the device does not send the country code.
distinctive-indication *value*	Indicates whether the device sends the distinctive indication.	Enumerated type. The values are as follows: ● enable: indicates that the device sends the distinctive indication. ● disable: indicates that the device does not send the distinctive indication. By default, the device does not send the distinctive indication.
echo-cancellation *value*	Indicates whether the device sends echo cancellation information.	Enumerated type. The values are as follows: ● enable: indicates that the device sends echo cancellation information. ● disable: indicates that the device does not send echo cancellation information. By default, the device does not send echo cancellation information.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
circuit-character *value*	Indicates whether the device sends the circuit character.	Enumerated type. The values are as follows: ● enable: indicates that the device sends the circuit character. ● disable: indicates that the device does not send the circuit character. By default, the device does not send the circuit character.
calling-number *value*	Indicates whether the device sends the calling number.	Enumerated type. The values are as follows: ● enable: indicates that the device sends the calling number. ● disable: indicates that the device does not send the calling number. By default, the device does not send the calling number.
calling-user-priority *value*	Indicates whether the device sends the calling user priority.	Enumerated type. The values are as follows: ● enable: indicates that the device sends the calling user priority. ● disable: indicates that the device does not send the calling user priority. By default, the device does not send the calling user priority.

Views

R2 profile view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the device to send the country code in the R2 profile **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 profile test
[Huawei-voice-r2-profile-test] register-address-send country-code enable
```

16.5.6.92 register-id (trunk group view)

Function

The **register-id** command configures the ID and authentication password for a SIP trunk group.

The **undo register-id password** command clears the authentication password.

Format

register-id *register-uri-value* [**password cipher** *password-value*]

undo register-id password

Parameters

Parameter	Description	Value
register-uri-value	Specifies the URI of a registrar.	The value is a string of 1 to 32 characters.
password cipher *password-value*	Specifies the string of the cipher text password. **NOTE** You can configure *password-value* after and inputting **cipher** and pressing **Enter**.	The value is a string of 1 to 32 characters without spaces.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only the trunk group of the SIP type supports the **register-id** command. Before using the **register-id** command, run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a trunk group of the SIP type.

If the **register-id** command runs for multiple times, the latest configuration overrides the previous one.

Example

Set the identifier of a trunk group to 123456 and the password to **abcdef**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test
[Huawei-voice-trunkgroup-test] register-id 123456 password cipher
 Please input user password(1-32 chars):******
```

16.5.6.93 register-signal-receive

Function

Using the **register-signal-receive** command, you can set register signaling input parameters for an R2 signaling type.

Using the **undo register-signal-receive** command, you can restore the default register signaling input parameters for an R2 signaling type.

Format

register-signal-receive *Register-phy-cmdRegister-call-state* { *Register-logic-cmdRegister-logic-cmd-para* | **no-process** }

undo register-signal-receive *register-phy-cmdregister-call-state*

Parameters

Parameter	Description	Value
register-phy-cmd	Specifies a physical command.	The value is an integer that ranges from 1 to 15. A value corresponds to a physical command.
register-call-state	Specifies a line call parameter.	The value is an integer that ranges from 1 to 10. A value corresponds to a line call parameter.
register-logic-cmd	Specifies a logical command.	The value is an integer that ranges from 0 to 31. A value corresponds to a logical command.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
register-logic-cmd-para	Specifies a parameter in a logical command.	The value is an integer that ranges from 0 to 15. A value corresponds to a parameter.
no-process	Specifies an invalid command.	-

Views

R2 signaling type view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set register signaling input parameters for the R2 signaling type **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 signalling-type test
[Huawei-voice-r2-signalling-type-test] register-signal-receive 1 1 1 1
```

16.5.6.94 register-signal-send

Function

The **register-signal-send** command sets register signaling output parameters for an R2 signaling type.

The **undo register-signal-send** command restores the default register signaling output parameters for an R2 signaling type.

Format

register-signal-send *register-logic-cmdregister-logic-cmd-para* { *register-phy-cmd* | **no-process** }

undo register-signal-send *register-logic-cmdregister-logic-cmd-para*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
register-logic-cmd	Specifies a logical command.	The value is an integer that ranges from 0 to 31. A value corresponds to a logical command.
register-logic-cmd-para	Specifies a parameter in a logical command.	The value is an integer that ranges from 0 to 15. A value corresponds to a parameter.
register-phy-cmd	Specifies a physical command.	The value is an integer that ranges from 1 to 15. A value corresponds to a physical command.
no-process	Specifies an invalid command.	-

Views

R2 signaling type view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the logical command to 2, logical command parameter to 1, and physical command to 1 for the R2 signaling **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 signalling-type test
[Huawei-voice-r2-signalling-type-test] register-signal-send 1 1 1
```

16.5.6.95 register-signalling

Function

Using the **register-signalling** command, you can configure register signaling attributes in an R2 profile.

Using the **undo register-signalling** command, you can restore the default register signaling attributes in an R2 profile.

Format

register-signalling { **back-pulse-time** *back-pulse-time-value* | **calling-number-max-length** *calling-number-max-length-value* | **compelling-sequence-keepalive-time** *compelling-sequence-keepalive-time-value* | **dtmf-send-interval** *dtmf-send-interval-time* | **dtmf-send-time** *dtmf-send-time-value* | **incoming-type** *incoming-type-value* | **number-max-interval** *number-max-interval-time* | **number-send-mode** *number-send-mode-value* | **outgoing-type** *outgoing-type-value* | **receive-number-max-interval** *receive-number-max-interval-time* | **send-pulse-signal** *signal-value* | **signal-send-voltage** *signal-send-voltage-value* | **signal-stop-permit-time** *signal-stop-permit-time-value* | **wait-Bsignal-time** *wait-Bsignal-time-value* | **wait-caller-category-time** *wait-caller-category-time-value* }

undo register-signalling { **back-pulse-time** | **calling-number-max-length** | **compelling-sequence-keepalive-time** | **dtmf-send-interval** | **dtmf-send-time** | **incoming-type** | **number-max-interval** | **number-send-mode** | **outgoing-type** | **receive-number-max-interval** | **send-pulse-signal** | **signal-send-voltage** | **signal-stop-permit-time** | **wait-Bsignal-time** | **wait-caller-category-time** }

Parameters

Parameter	Description	Value
back-pulse-time *back-pulse-time-value*	Specifies the backward pulse duration.	The value is an integer that ranges from 100 to 200, in milliseconds. The default interval is 150.
calling-number-max-length *calling-number-max-length-value*	Specifies the maximum length of a calling number.	The value is an integer that ranges from 0 to 24, in digits. By default, the maximum length of a calling number is 12.
compelling-sequence-keepalive-time *compelling-sequence-keepalive-time-value*	Specifies the Keepalive time of the register signaling compelling sequence.	The value is an integer that ranges from 0 to 60000, in milliseconds. The default value is 40000.
dtmf-send-interval *dtmf-send-interval-time*	Specifies the interval at which DTMF signals are sent.	The value is an integer that ranges from 50 to 500, in milliseconds. The default value is 68.
dtmf-send-time *dtmf-send-time-value*	Specifies the period during which DTMF signals are sent.	The value is an integer that ranges from 50 to 200, in milliseconds. The default value is 68.
incoming-type *incoming-type-value*	Specifies the incoming register signaling type.	Enumerated type. The values are as follows: MFC, DTMF. The default value is MFC.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
number-max-interval *number-max-interval-time*	Specifies the interval at which the calling number is sent.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 50.
number-send-mode *number-send-mode-value*	Specifies the digit collection mode.	Enumerated type. The values are as follows: immediately and delay. The default value is delay.
outgoing-type *outgoing-type-value*	Specifies the register signaling type.	Enumerated type. The values are as follows: MFC, DTMF. The default value is MFC.
receive-number-max-interval *receive-number-max-interval-time*	Specifies the interval at which digits are collected.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 50.
send-pulse-signal *signal-value*	Indicates whether the end-of-pulsing signal is sent.	The values are as follows: ● enable: indicates that the end-of-pulsing signal is sent. ● disable: indicates that the end-of-pulsing signal is not sent. By default, the end-of-pulsing signal is not sent.
signal-send-voltage *signal-send-voltage-value*	Specifies the voltage of the signal to be sent.	The value is an integer that ranges from 0 to 22. The value 0 indicates -25 dBM and the value 22 indicates -3 dBM. The step is 1 dBM. The default value is 13.
signal-stop-permit-time *signal-stop-permit-time-value*	Specifies the period during which the device is allowed to stop transmitting signals.	The value is an integer ranging from 1 to 30, in seconds. The default value is 15.
wait-Bsignal-time *wait-Bsignal-time-value*	Specifies the period from the time to request group B signals to the time to receive group B signals.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 50.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
wait-caller-category-time *wait-caller-category-time-value*	Specifies the period from the time to request the caller category to the time to receive the caller category.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 50.

Views

R2 profile view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the voltage for transmitting signals to 10 in the R2 profile **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 profile test
[Huawei-voice-r2-profile-test] register-signalling signal-send-voltage 10
```

16.5.6.96 register-uri (trunk group view)

Function

Using the **register-uri** command, you can configure a URI for a registrar.

Format

register-uri *register-uri-value*

Parameters

Parameter	Description	Value
register-uri-value	Specifies the URI of a registrar.	The value is a string of 1 to 64 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only the trunk group of the SIP type supports the **register-uri** command. Before using the **register-uri** command, run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a trunk group of the SIP type.

Example

Set the URI of a registrar to abcd.com.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-group
[Huawei-voice-trunkgroup-test] register-uri abcd.com
```

16.5.6.97 request-channelclose-timeout

Function

The **request-channelclose-timeout** command sets the timeout interval for a request for closing a logical channel.

The **undo request-channelclose-timeout** command restores the default timeout interval for a request for closing a logical channel.

By default, the timeout interval is 15000 ms.

Format

request-channelclose-timeout *request-channelclose-timeout-value*

undo request-channelclose-timeout

Parameters

Parameter	Description	Value
request-channelclose-timeout-value	Specifies the timeout interval for a request for closing a logical channel.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the timeout interval for a request for closing a logical channel to 50000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] request-channelclose-timeout 50000
```

16.5.6.98 requestmode-timeout

Function

The **requestmode-timeout** command sets the timeout interval for mode switching.

The **undo requestmode-timeout** command restores the default timeout interval for mode switching.

By default, the timeout interval is 15000 ms.

Format

requestmode-timeout *requestmode-timeout-value*

undo requestmode-timeout

Parameters

Parameter	Description	Value
requestmode-timeout-value	Specifies the timeout interval for mode switching.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the timeout interval for mode switching to 50000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] requestmode-timeout 50000
```

16.5.6.99 reserved-circuit (trunk group view)

Function

The **reserved-circuit** command configures a reserved circuit.

The **undo reserved-circuit** command cancels a reserved circuit.

Format

reserved-circuit number *number-value* [**priority** *priority-value*]

undo reserved-circuit

Parameters

Parameter	Description	Value
number-value	Specifies the number of reserved circuits.	The value is an integer that ranges from 0 to 254.
priority-value	Specifies the lowest level for using reserved circuits.	Enumerated value. The value can be **default**, **normal**, **advanced**, or **super**. The default value is **super**.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

When the number of reserved circuits is not smaller than maxcr, circuits are reserved for users with a specified level.

Example

Reserve two circuits for users with normal or higher levels.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-group
[Huawei-voice-trunkgroup-test] reserved-circuit number 2 priority normal
```

16.5.6.100 reset (H323 attribute view)

Function

The **reset** command resets the H323 system.

Format

reset

Parameters

None

Views

H323 attribute view

Default Level

3: Management level

Usage Guidelines

You must reset the H323 system to make the H323 configuration take effect.

Example

Reset the H323 system.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] reset
H323 system parameters reset successfully!
```

16.5.6.101 reset (trunk group view)

Function

Using the **reset** command, you can reset a trunk group.

Format

reset

Parameters

None

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Only SIP or H323 trunk group support the **reset** command. Before using the **reset** command, run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a SIP trunk group.

Example

Reset the trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test
[Huawei-voice-trunkgroup-test] reset
```

16.5.6.102 roundtrip-delay-timeout

Function

The **roundtrip-delay-timeout** command sets the timeout interval of the roundtrip delay process.

The **undo roundtrip-delay-timeout** command restores the default timeout interval of the roundtrip delay process.

By default, the timeout interval is 15000 ms.

Format

roundtrip-delay-timeout *roundtrip-delay-timeout-value*

undo roundtrip-delay-timeout

Parameters

Parameter	Description	Value
roundtrip-delay-timeout-value	Specifies the timeout interval of the roundtrip delay process.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.

Views

H323 attribute view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the timeout interval of the roundtrip delay process to 50000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] roundtrip-delay-timeout 50000
```

16.5.6.103 select-mode (trunk group view)

Function

Using the **select-mode** command, you can configure a circuit selection mode for a trunk group.

Using the **undo select-mode** command, you can restore the default circuit selection mode for a trunk group.

By default, the polling mode is used to select a circuit for a trunk group.

Format

select-mode *selectmode-value*

undo select-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
selectmode-value	Specifies the value of a circuit selection mode.	Enumerated type. The values are as follows: • loop: indicates the polling mode. • increase: indicates the ascending mode. • decrease: indicates the descending mode. • port-loop: indicates the ascending mode. (In the case of call failure, re-select a time slot on the same port in ascending order.) • port-increase:indicates the ascending mode. (In the case of call failure, re-select a port in ascending order.) default: loop

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before configuring a circuit selection mode, run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a trunk group.

Example

Set the circuit selection mode for a trunk group to ascending mode.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test
[Huawei-voice-trunkgroup-test] select-mode increase
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.104 send-heartbeat

Function

The **send-heartbeat** command enables a gatekeeper to send heartbeat messages.

The **undo send-heartbeat** command disables a gatekeeper from sending heartbeat messages.

By default, a gatekeeper does not send heartbeat messages.

Format

send-heartbeat { **disable** | **enable** }

undo send-heartbeat

Parameters

Parameter	Description	Value
disable	Disables a gatekeeper from sending heartbeat messages.	-
enable	Enables a gatekeeper to send heartbeat messages.	-

Views

trunk group view

Default Level

2: Configuration level

Usage Guidelines

A local gatekeeper sends heartbeat messages to check whether there is a peer gatekeeper.

NOTE

The heartbeat message sending must be configured only when the H323 trunk works in gk-gk mode.

Example

Enable the H323 trunk **test** to send heartbeat messages.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test h323 gk-gk
[Huawei-voice-trunkgroup-test] send-heartbeat enable
```

16.5.6.105 send-techprefix

Function

The **send-techprefix** command configures the device whether to send the technical prefix.

The **undo send-techprefix** command cancels the configuration.

By default, the device does not send the technical prefix.

Format

send-techprefix *h323-send-techprefix-value*

undo send-techprefix

Parameters

Parameter	Description	Value
h323-send-techprefix-value	Indicates whether the device sends the technical prefix.	Enumerated type. The values are as follows: ● enable: The technical prefix is sent. ● disable: The technical prefix is not sent.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the device not to send the technical prefix.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 register-gateway
[Huawei-voice-trunkgroup-test] send-techprefix disable
```

16.5.6.106 setup-wait-response-timeout

Function

The **setup-wait-response-timeout** command sets the timeout interval for Setup messages.

The **undo setup-wait-response-timeout** command restores the default timeout interval for Setup messages.

By default, the timeout interval for Setup messages is 500000 ms.

Format

setup-wait-response-timeout *setup-wait-response-timeout-value*

undo setup-wait-response-timeout

Parameters

Parameter	Description	Value
setup-wait-response-timeout-value	Specifies the timeout interval for Setup messages.	The value is an integer that ranges from 4000 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the timeout interval for Setup messages to 5000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] setup-wait-response-timeout 5000
```

16.5.6.107 shutdown (H323 attribute view)

Function

The **shutdown** command shuts down the H323 system.

Format

shutdown

Parameters

None

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

To disable H323 on the device, run this command.

To enable H323 on the device, run the **reset (H323 attribute view)** command.

Example

Shut down the H323 system.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] shutdown
 H323 system parameters shutdown successfully!
```

16.5.6.108 shutdown (trunk group view)

Function

Using the **shutdown** command, you can shut down a SIP or a H323 trunk group.

Format

shutdown

Parameters

None

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before shutting down a SIP or a H323 trunk group, complete mandatory configurations of the group and enable the trunk group to take effect by running the **reset (trunk group view)** command to reset the trunk group.

Example

Shut down a trunk group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] shutdown
```

16.5.6.109 signalling-address

Function

The **signalling-address** command configures a signaling IP address and a local signaling port number for a SIP trunk group.

By default, no signaling IP address or local signaling port number is configured.

Format

signalling-address { **ip** *ip-address* | **addr-name** *signal-addr-name-value* } **port** *port-value*

Parameters

Parameter	Description	Value
ip-address	Specifies a signaling IP address for a trunk group.	The value is in dotted decimal notation.
addr-name *ip-address*	Specifies a dynamic IP address name for a trunk group.	The value is a string of 1 to 64 case-insensitive characters.
port *port-value*	Specifies the local signaling port number for a SIP trunk group.	The value is an integer that ranges from 5000 to 5999.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before configuring a signaling IP address for a SIP trunk group, create a signaling IP address or a dynamic signaling IP address name by running the **voip-address signalling** command.

Example

Configure a signaling IP address 192.168.1.1 for a SIP trunk group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group siptrkgrp sip trunk-group
[Huawei-trunkgroup-siptrkgrp] signalling-address ip 192.168.1.1 port 5005
```

16.5.6.110 signalling-type

Function

Using the **signalling-type** command, you can set the adaptation signaling type in an R2 profile.

Using the **undo signalling-type** command, you can restore the default adaptation signaling type in an R2 profile.

Format

signalling-type *signalling-type-name*

undo signalling-type

Parameters

Parameter	Description	Value
signalling-type-name	Specifies the name of a signaling type.	The value is a string of 1 to 32 characters.

Views

R2 profile view

Default Level

2: Configuration level

Usage Guidelines

The system provides adaptation signaling types of standard, brazil, argentina, and mexico, and supports user-defined mexico adaptation signaling type.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the signaling type to **test** in the R2 profile **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] r2 profile test
[Huawei-voice-r2-profile-test] signalling-type test
```

16.5.6.111 stable delay-time

Function

The **stable delay-time** command configures the status synchronization delay for trunk groups associated with a trunk group.

The **undo stable delay-time** command restores the default configuration.

By default, the status synchronization delay of trunk groups associated with a trunk group is 30s.

Format

stable delay-time *time-value*

undo stable delay-time

Parameters

Parameter	Description	Value
time-value	Specifies the status synchronization delay of trunk groups associated with a trunk group.	The value is an integer that ranges from 0 to 120, in seconds.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a trunk group link is disconnected or restored, the associated trunk group synchronizes status after a period of time. This period of time is status synchronization delay. A status synchronization delay can suppress frequent switching of the status of trunk groups associated with a trunk group due to unstable trunk group links.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The **stable delay-time** command can be run only in the PRA trunk group view and in the scenario where a PRA trunk group is associated with SIP trunk groups. This command configures the status synchronization delay for a SIP trunk group associated with the PRA trunk group when a PRA trunk group link is disconnected or restored.

Example

Set the status synchronization delay of an associated trunk group to **15s**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test dss1-net
[Huawei-voice-trunkgroup-test] stable delay-time 15
```

16.5.6.112 statuscode-toneid-mapping (trunk group view)

Function

The **statuscode-toneid-mapping** command configures mapping between SIP response codes and tone IDs.

The **undo statuscode-toneid-mapping** command restore the default mapping between SIP response codes and tone IDs.

Format

statuscode-toneid-mapping *StatusCode ToneId*

undo statuscode-toneid-mapping *StatusCode*

Parameters

Parameter	Description	Value
StatusCode	Specifies the SIP response code.	The value is an integer that ranges from 400 to 699.
ToneId	Specifies a tone ID.	The value is an integer that ranges from 1 to 255.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The trunk group type is SIP IP trunk or SIP AT0 trunk.

When outgoing calls are made through the SIP IP trunk or SIP AT0 trunk, run the **statuscode-toneid-mapping** command so that the device plays the prompt tone based on the SIP response code. This command applies to the following scenarios:

- The calling party is a POTS user and the device plays the prompt tone based on the mapping.
- The calling party is a BRA user or incoming calls are made through the BRA or PRA trunk. The pbx **number-parameter 202 1** command must have been executed in the voice view.

Prerequisites

The **display voice tone type** command has been executed to view the prompt tones supported by the PBX.

Example

In the SIP IP trunk group sip, map sip-response 410 to tone 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sip sip no-register
[Huawei-voice-trunkgroup-sip] statuscode-toneid-mapping 410 2
```

16.5.6.113 support-cli-change

Function

Using the **support-cli-change** command, you can configure whether to support caller change.

By default, support caller change.

Format

support-cli-change { **enable** | **disable** }

Parameters

None

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

It is used in trunk group relay scenario to change the caller number of down-link trunk, and the **support-cli-change** command should be configured at the up-link trunk.

Example

Set the sipat0 trunk group not to support caller change.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sipat0
[huawei-voice-trunkgroup-sipat0] support-cli-change disable
```

16.5.6.114 support-h245tul

Function

The **support-h245tul** command configures the device whether to support the H245 control signaling channel.

The **undo support-h245tul** command cancels the configuration.

By default, the device does not support the H245 control signaling channel.

Format

support-h245tul { **enable** | **disable** }

undo support-h245tul

Parameters

Parameter	Description	Value
enable	Indicates that the device supports the H245 control signaling channel.	-
disable	Indicates that the device does not support the H245 control signaling channel.	-

Views

H323 attribute view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Configure the H323 stack to support the H245 control signaling channel.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] support-h245tul enable
```

16.5.6.115 tcp-connection-timeout

Function

The **tcp-connection-timeout** command sets the timeout interval for TCP connections.

The **undo tcp-connection-timeout** command restores the default timeout interval for TCP connections.

By default, the timeout interval for TCP connections is 15000 ms.

Format

tcp-connection-timeout *tcp-connection-timeout-value*

undo tcp-connection-timeout

Parameters

Parameter	Description	Value
tcp-connection-timeout-value	Specifies the timeout interval for TCP connections.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the timeout interval for TCP connections to 150000 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] tcp-connection-timeout 150000
```

16.5.6.116 tcp-keepalive-timerlen

Function

The **tcp-keepalive-timerlen** command sets the value of the TCP keepalive timer.

The **undo tcp-keepalive-timerlen** command restores the default value of the TCP keepalive timer.

By default, the value of the TCP keepalive timer is 3600 ms.

Format

tcp-keepalive-timerlen *tcp-keepalive-timerLen-value*

undo tcp-keepalive-timerlen

Parameters

Parameter	Description	Value
tcp-keepalive-timerLen-value	Specifies the value of the TCP keepalive timer.	The value is an integer that ranges from 0 to 65535, in milliseconds.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the value of the TCP keepalive timer to 1280 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] tcp-keepalive-timerlen 1280
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.117 techprefix

Function

The **techprefix** command configures the technical prefix.

The **undo techprefix** command deletes the technical prefix.

By default, no technical prefix is configured.

Format

techprefix *techprefix-value*

undo techprefix

Parameters

Parameter	Description	Value
techprefix-value	Specifies the technical prefix.	The value is a string of 1 to 16 characters.

Views

H323 Trunk group view

Default Level

2: Configuration level

Usage Guidelines

When there are trunk groups of various H323 types, run the **techprefix** command to configure the technical prefix to differentiate trunk groups.

Example

Set the technical prefix to 2222.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 register-gateway
[Huawei-voice-trunkgroup-test] techprefix 2222
```

16.5.6.118 transfer (trunk group view)

Function

Using the **transfer** command, you can configure the transfer mode for a SIP trunk group.

Using the **undo transfer** command, you can restore the default transfer mode of a SIP trunk group.

 Copyright © Huawei Technologies Co., Ltd.

The default transfer mode of a SIP trunk group is UDP.

Format

transfer *transfer-value*

undo transfer

Parameters

Parameter	Description	Value
transfer-value	Specifies the transfer mode of a SIP trunk group.	Enumerated type. The values are as follows: • TCP • UDP

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **transfer** command to configure the transfer mode for a SIP trunk group as required.

Prerequisites

Only the trunk group of the SIP type supports the **transfer** command. Before using the **transfer** command, run the **16.5.1.24 display voice media-bandwidth-control (PBX)** command to create a trunk group of the SIP type.

Precautions

When the transfer mode of a SIP trunk group is TCP, the signaling port number ranges from 5000 to 5099. When the transfer mode of a SIP trunk group is UDP, the signaling port number ranges from 5000 to 5999.

Example

Set the transfer mode of a SIP trunk group to TCP.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] transfer TCP
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.6.119 trunk-at0

Function

The **trunk-at0** command binds trunks to an AT0 trunk group.

The **undo trunk-at0** command unbinds trunks from an AT0 trunk group.

By default, no trunk is bound to an AT0 trunk group.

Format

trunk-at0 *slotid/subcardid/portid* [**default-called-telno** *default-called-telno-value* | **caller-telno** [**enterprise** *enterprise-name*] *caller-telno-value* | **cid-transmit-type** *cid-transmit-type-value* | **config-status** *config-status-value* | **dial-delay** *dial-delay-value* | **dial-mode** *dial-mode-value* | **insert-prefix** *insert-prefix-value* | **insert-prefix-delay** *insert-prefix-delay-value*] *

undo trunk-at0 *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID, subcard ID, and port number. This parameter identifies the location of the user to be configured. Enter forward slashes (/) between the slot ID, subcard ID, and port number.	The value is a string of 1 to 15 characters. The values of *slotid*, *subcardid*, and *portid* depend on the product model.
default-called-telno *default-called-telno-value*	Indicates the called number configured for incoming calls. It can be an IVR number.	The value is a string of 1 to 32 digits without spaces.
caller-telno *caller-telno-value*	Indicates the phone number of a calling user to be bound to a trunk.	The value is a string of 1 to 24 digits without spaces.
enterprise *enterprise-name*	Indicates the name of the enterprise to which a calling number belongs.	The value is a string of 1 to 32 case-insensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cid-transmit-type *cid-transmit-type-value*	Indicates the signal transmission type for the CLIP service.	Integer type. The values are as follows: ● 0: Bell 202 ● 1: V.23 ● 2: NTT ● 3: DTMF ● 4: R1.5 ● 5: Bell 202, V.23, and DTMF ● 6: None The default value is 0.
config-status *config-status-value*	Indicates the AT0 trunk status.	Enumerated type. The values are as follows: ● block ● normal The default value is normal.
dial-delay *dial-delay-value*	Indicates the dial delay.	The value is an integer that ranges from 0 to 10,000, in milliseconds. The default value is 2000 ms.
dial-mode *dial-mode-value*	Indicates the dialing mode.	Enumerated type. The values are as follows: ● dtmf: DTMF dialing ● pulse: pulse dialing The default value is dtmf.
insert-prefix *insert-prefix-value*	Indicates the inserted call prefix.	The value is a string of 1 to 4 case-insensitive characters without spaces.
insert-prefix-delay *insert-prefix-delay-value*	Indicates the dial delay after a call prefix is inserted into numbers.	The value is an integer that ranges from 0 to 10000, in milliseconds. The default value is 2000 ms.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **default-called-telno** command to specify whether the calls routed through an AT0 trunk is connected to an intra-office user (dedicated access) or to the automatic main number (switchboard access).

By configuring **caller-telno**, you can specify a number for outgoing calls through the AT0 trunk. Only the outgoing calls that are made using the number can be routed through the AT0 trunk. When the AT0 trunk is unavailable, the outgoing calls that are made using the number specified by **caller-telno** can be routed through other trunks, and incoming calls through the AT0 trunk are routed to the number specified by **default-called-telno**. To route incoming calls through the AT0 trunk to the number specified by **caller-telno**, you can set **default-called-telno** and **caller-telno** to the same value.

Precaution

When you bind a trunk to an AT0 trunk group, the **default-called-telno** parameter is mandatory.

Example

Bind a trunk to an AT0 trunk group. Set **default-called-telno** to **10086** and *slotid/subcardid/portid* to **2/0/4**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test fxo
[Huawei-voice-trunkgroup-test] trunk-at0 2/0/4 default-called-telno 10086
```

16.5.6.120 trunk-bra

Function

The **trunk-bra** command binds a trunk to a BRA trunk group.

The **undo trunk-bra** command unbinds a trunk from a BRA trunk group.

Format

trunk-bra *slotid/subcardid/portid* [**default-called-telno** *default-called-telno-value* | **caller-telno** [**enterprise** *enterprise-name*] *telno-value* | **default-cli** *default-cli-value* | [**b-channels** *b-channels-value* [**num** *num-value*]] **config-status** *config-status-value*] *

undo trunk-bra *slotid/subcardid/portid*

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number. This parameter identifies the location of the user to be deleted.	The value is a string of 1 to 15 characters. The value of *slotid*, *subcardid*, and *portid* depend on product specifications.
default-called-telno *default-called-telno-value*	Specifies the default called number.	The value is a string of 1 to 24 characters.
caller-telno	Specifies the called number.	-
enterprise *enterprise-name*	Specifies the name of an enterprise.	The value is a string of 1 to 32 characters without spaces.
country-code *country-code-value*	Specifies a country code.	The value is a string of 1 to 4 characters.
area-code *area-code-value*	Specifies an area code.	The value is a string of 1 to 8 characters.
telno-value	Specifies the calling number.	The value is a string of 1 to 24 characters.
default-cli *default-cli-value*	Specifies the default calling number. **NOTE** When BRA trunk make outgoing calls over the SIP PRA trunk without calling number information, the default calling number is used.	The value is a string of 1 to 64 characters without spaces.
b-channels *b-channels-value*	Specifies the ID of B channel.	Numeral type. The value ranges from 0 to 1.
num *num-value*	Specifies the number of B channels.	Numeral type. The value ranges from 1 to 2.
config-status *config-status-value*	Specifies the trunk status.	Enumerated type. The value is block or normal. ● block ● normal The default value is normal.

 Copyright © Huawei Technologies Co., Ltd.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before binding a trunk to a BRA trunk group, ensure that the trunk group has been created.

Example

Set the number of the physical interface bound to the trunk that is bound to the BRA trunk to 2/0/0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test bra-qsig
[Huawei-voice-trunkgroup-test] trunk-bra 2/0/0
```

16.5.6.121 trunk-bra typeofnumber

Function

The **trunk-bra typeofnumber** command configures the call type on the port bound to a BRA trunk group.

The **undo trunk-bra typeofnumber** command cancels the configuration of the call type on the port bound to a BRA trunk group.

Format

trunk-bra slotid/subcardid/portid [**typeofnumber** { **caller** | **called** } <typeofnumber-value>]

undo trunk-bra slotid/subcardid/portid [**typeofnumber** { **caller** | **called** }]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number. This parameter must be set to identify the physical location of the user to be deleted. The slash (/) must be entered.	The value is a string of 1 to 15 characters. The options are as follows: • *slotid*: depends on the product model. • *subcardid*: depends on the product model. • *portid*: depends on the product model.

Parameter	Description	Value
typeofnumber { **caller** | **called** } <typeofnumber-value>	Specifies the calling or called number type.	Enumerated value: ● Unknown: unknown type ● International: international number ● National: national number ● NewworkSpecific: network specific number ● Subscriber: user number ● Abbreviated: abbreviated number ● ReservedForExtension: reserved By default, the calling or called number type is not configured.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before binding a trunk to a trunk group, ensure that the trunk group has been created.

Example

Set the physical interface associated with a trunk bound to a BRA trunk group to 2/0/0, and the calling number type to an international number.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test bra-qsig
[Huawei-voice-trunkgroup-test] trunk-bra 2/0/0 typeofnumber caller International
```

16.5.6.122 trunk-group

Function

The **trunk-group** command creates a trunk group and displays the trunk group view, or directly displays the view of an existing trunk group.

The **undo trunk-group** command deletes the trunk group.

By default, no trunk group is created.

Format

trunk-group *trunk-group-name* [**bra-dss1** | **bra-qsig** | **dss1-net** | **dss1-user** | **e1-r2** | **fxo** | **h323** *h323-type* | **qsig-net** | **qsig-user** | **sip** *register-mode* | **cs**]

undo trunk-group *trunk-group-name*

Parameters

Parameter	Description	Value
trunk-group-name	Specifies the name of a trunk group.	The value is a string of 1 to 32 case-insensitive characters without spaces.
bra-dss1	Indicates that the trunk type is BRA and protocol is Q.931.	-
bra-qsig	Indicates that the trunk type is BRA and protocol is QSIG.	-
dss1-net	Indicates that the PRA network-side trunk and Q.931 are used.	-
dss1-user	Indicates that the PRA user-side trunk and Q.931 are used.	-
e1-r2	Indicates that the trunk type is R2.	-
fxo	Indicates that the trunk type is AT0.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
h323 *h323-type*	Specifies the trunk type of the H.323 trunk group.	Enumerated value. The values are as follows: ● symmetrical: the trunk type in peer gateway mode. ● register-gateway: the trunk type on the gatekeeper that allows registration of one gateway. ● gw-gk: the trunk type on the gateway that registers to the gatekeeper. ● gk-gk: the trunk type in peer gatekeeper mode. ● gatekeeper: the trunk type on the gatekeeper that allows registration of multiple gateways.
qsig-net	Indicates that the PRA network-side trunk and QSIG are used.	-
qsig-user	Indicates that the PRA user-side trunk and QSIG are used.	-
sip *register-mode*	Configures the registration mode for the SIP trunk group.	Enumerated type. The values are as follows: ● trunk-circuit: trunk circuit registration (SIP AT0 trunk). ● trunk-group: SIP PRA trunk. ● no-register: SIP IP trunk.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

An H.323 trunk is used in the following scenarios:

- In peer gateway mode, the H.323 trunk type of gateways on both ends is **symmetrical**.
- In peer gatekeeper mode, the H.323 trunk type of gatekeepers on both ends is **gk-gk**.
- In one-to-one registration mode, the H.323 trunk types on the gateway and gatekeeper are **gw-gk** and **register-gateway**, respectively. The H.323 trunk group on the gatekeeper allows registration of one gateway.
- In one-to-many registration mode, the H.323 trunk types on the gateway and gatekeeper are **gw-gk** and **gatekeeper**, respectively. The H.323 trunk group on the gatekeeper allows registration of multiple gateways.

Example

Create a trunk group named **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test SIP trunk-circuit
[Huawei-voice-trunkgroup-test]
```

16.5.6.123 trunk-pra

Function

The **trunk-pra** command binds a trunk to a PRA trunk group.

The **undo trunk-pra** command unbinds a trunk from a PRA trunk group.

Format

trunk-pra *Slotid/Subcardid/Portid* [[**b-channels** *b-channels-value* [**num** *num-value*]] [**config-status** *config-status-value*] [**default-cli** *default-cli-value*]]

undo trunk-pra *Slotid/Subcardid/Portid* [**b-channels** *b-channels-value* [**num** *num-value*]]

Parameters

Parameter	Description	Value
Slotid/Subcardid/Portid	Specifies the slot ID/subcard ID/port number of the port connected to the PRA trunk.	The value is a string of 1 to 15 characters. The values of *slotid*, *subcardid*, and *portid* depend on the product model.
b-channels *b-channels-value*	Specifies the ID of B channel.	Numeral type. The value ranges from 0 to 31.

Parameter	Description	Value
num *num-value*	Specifies the number of B channels.	Numeral type. The value ranges from 1 to 32.
config-status *config-status-value*	Specifies the trunk status.	Enumerated type. The value is block or normal. ● block ● normal The default value is normal.
default-cli *default-cli-value*	Specifies the default calling number. **NOTE** When PRA trunk make outgoing calls over the SIP PRA trunk without calling number information, the default calling number is used.	The value is a string of 1 to 64 characters without spaces.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Bind trunks to the PRA trunk group, and set the trunk port number to 1/0/1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test dss1-net
[Huawei-voice-trunkgroup-test] trunk-pra 1/0/1
```

16.5.6.124 trunk-pra typeofnumber

Function

The **trunk-pra typeofnumber** command configures the call type on the port bound to a PRA trunk group.

The **undo trunk-pra typeofnumber** command cancels the configuration of the call type on the port bound to a PRA trunk group.

Format

trunk-pra slotid/subcardid/portid [**typeofnumber** { **caller** | **called** } <typeofnumber-value>]

undo trunk-pra slotid/subcardid/portid [**typeofnumber** { **caller** | **called** }]

Parameters

Parameter	Description	Value
slotid/subcardid/portid	Specifies the slot ID/subcard ID/port number. This parameter must be set to identify the physical location of the user to be deleted. The slash (/) must be entered.	The value is a string of 1 to 15 characters. The options are as follows: ● *slotid*: depends on the product model. ● *subcardid*: depends on the product model. ● *portid*: depends on the product model.
typeofnumber { **caller** | **called** } <typeofnumber-value>	Specifies the calling or called number type.	Enumerated value: ● Unknown: unknown type ● International: international number ● National: national number ● NewworkSpecific: network specific number ● Subscriber: user number ● Abbreviated: abbreviated number ● ReservedForExtension: reserved By default, the calling or called number type is not configured.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before binding a trunk to a trunk group, ensure that the trunk group has been created.

Example

Set the physical interface associated with a trunk bound to a PRA trunk group to 1/0/0, and the calling number type to an international number.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test dss1-net
[Huawei-voice-trunkgroup-test] trunk-pra 1/0/0 typeofnumber caller International
```

16.5.6.125 trunk-r2

Function

The **trunk-r2** command binds trunks to an E1R2 trunk group.

The **undo trunk-r2** command unbinds trunks from an E1R2 trunk group.

Format

trunk-r2 *Slotid/Subcardid/Portid* [[**b-channels** *b-channels-value* [**num** *num-value*]] **config-status** *config-status-value*]

undo trunk-r2 *Slotid/Subcardid/Portid*

Parameters

Parameter	Description	Value
Slotid/Subcardid/Portid	Specifies the slot ID/subcard ID/port number of the FXO port connected to the E1R2 trunk.	The value is a string of 1 to 15 characters. The values of *slotid*, *subcardid*, and *portid* depend on the product model.
b-channels *b-channels-value*	Specifies the ID of B channel.	Numeral type. The value ranges from 0 to 31.
num *num-value*	Specifies the number of B channels.	Numeral type. The value ranges from 1 to 32.
config-status *config-status-value*	Specifies the trunk status.	Enumerated type. The value is block or normal. ● block ● normal The default value is normal.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

N/A

Example

Bind trunks to the E1R2 trunk group, and set the trunk port number to 1/0/1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test e1-r2
[Huawei-voice-trunkgroup-test] trunk-r2 1/0/1
```

16.5.6.126 trunk-sipat0

Function

The **trunk-sipat0** command binds a trunk to a SIP AT0 trunk group.

The **undo trunk-sipat0** command unbinds a trunk from a SIP AT0 trunk group.

Format

trunk-sipat0 *register-id* { **password cipher** *cipher-password* | **caller-telno** [**enterprise** *enterprise-name*] *telno-value* | **default-called-telno** *default-called-telno-value* | **max-calls** *max-calls-value* | **digest-username** *digest-username-value* } *

undo trunk-sipat0 *register-id*

Parameters

Parameter	Description	Value
register-id	Specifies the ID used by a SIP AT0 trunk for registration.	The value is a string of 1 to 32 characters.
password cipher *cipher-password*	Specifies a password in cipher text. **NOTE** You can configure *cipher-password* after inputting **cipher** and pressing **Enter**.	The value is a string of 1 to 32 characters without spaces.
caller-telno	Specifies the calling number special for the current circuit.	-

Parameter	Description	Value
enterprise *enterprise-name*	Specifies the enterprise that the SIP AT0 trunk belongs to.	The value is a string of 1 to 32 characters without spaces.
telno-value	Specifies the calling number for the SIP AT0 trunk.	The value is a string of 1 to 24 characters, which must be digits 0 through 9.
default-called-telno *default-called-telno-value*	Specifies the called number configured for incoming calls.	The value is a string of 1 to 24 characters, which must be digits 0 through 9.
max-calls *max-call-value*	Specifies the maximum number of calls.	The value is an integer that ranges from 1 to 150.
digest-username *digest-username-value*	Indicates an authentication digest user name.	The value is a string of 1 to 128 characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PBX supports multiple trunks of the same type to be added to the same trunk group and invoked by call routes. If there is only one trunk, a trunk group must be configured for the trunk, facilitating the trunk management.

When a trunk is bound to a SIP AT0 trunk group, the **default-called-telno** specifies whether calls routed through the trunk are connected to a specific user or to the automatic main number.

After **number-parameter 19 2** is configured on the system, you need to specify a value for **digest-username** *digest-username-value* to define an authentication digest user name.

Precautions

The **default-called-telno** parameter of SIP AT0 configuration is mandatory.

Example

Set the ID used by a SIP AT0 trunk for registration to 58981000 and the called number configured for incoming calls to 28981000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test sip trunk-circuit
[Huawei-voice-trunkgroup-test] trunk-sipat0 58981000 default-called-telno 28981000
```

16.5.6.127 ttlrrq

Function

The **ttlrrq** command configures the registration lifetime of a gateway.

The **undo ttlrrq** command restores the default registration lifetime of a gateway.

By default, the registration lifetime of a gateway is 360 seconds.

Format

ttlrrq *time*

undo ttlrrq

Parameters

Parameter	Description	Value
time	Specifies the registration lifetime of a gateway.	The value is an integer that ranges from 30 to 6000, in seconds. The default value is 360s.

Views

H323 trunk group view

Default Level

2: Configuration level

Usage Guidelines

The registration lifetime of a gateway is limited. After the gateway sends a registration request (RRQ) message including the time to live (TTL) field to a gatekeeper, the gatekeeper responds with a registration confirmation (RCF) message including a same or shorter TTL. When the registration lifetime reaches the limit, the registration is terminated. At the half of the registration lifetime, the gateway sends a new RRQ message to the gatekeeper and the gatekeeper responds with an RCF message, and the new registration lifetime starts.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This command takes effect only when the H323 trunk works in gw-gk mode.

Example

Set the registration lifetime of the H323 trunk group to 3600 seconds.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test h323 gw-gk
[Huawei-voice-trunkgroup-test] ttlrrq 3600
```

16.5.6.128 typeofnumber called

Function

The **typeofnumber called** command configures the called number type for PRA, BRA, or QSIG trunk groups.

The **undo typeofnumber called** command deletes the called number type configured for PRA, BRA, or QSIG trunk groups.

By default, the called number type is not configured for PRA, BRA, or QSIG trunk groups.

Format

typeofnumber called *calednumber-value*

undo typeofnumber called

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
callednumber-value	Specifies the called number type.	Called number type. Enumerated value. The options are as follows: ● Unknown: unknown type ● International: internal number ● National: national number ● NewworkSpecific: network specific number ● Subscriber: user number ● Smart: smart number ● Abbreviated: abbreviated number ● ReservedForExtension: reserved By default, the called number type is not configured.

Views

PRA, BRA, or QSIG trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the called number type for PRA trunk groups to international.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]trunk-group pra
[Huawei-voice-trunk-group pra]typeofnumber called International
```

16.5.6.129 typeofnumber caller

Function

The **typeofnumber caller** command configures the calling number type for PRA, BRA, or QSIG trunk groups.

The **undo typeofnumber caller** command deletes the calling number type configured for PRA, BRA, or QSIG trunk groups.

By default, the calling number type is not configured for PRA, BRA, or QSIG trunk groups.

Format

typeofnumber caller *callernumber-value*

undo typeofnumber caller

Parameters

Parameters	Parameter	Description Value
callernumber-value	Specifies the calling number type.	Calling number type. Enumerated value. The options are as follows: ● Unknown: unknown type ● International: internal number ● National: national number ● NewworkSpecific: network specific number ● Subscriber: user number ● Smart: smart number ● Abbreviated: abbreviated number ● ReservedForExtension: reserved By default, the calling number type is not configured.

 Copyright © Huawei Technologies Co., Ltd.

Views

PRA, BRA, or QSIG trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the calling number type for PRA trunk groups to international.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]trunk-group pra
[Huawei-voice-trunk-group pra]typeofnumber caller International
```

16.5.6.130 use-rule-set

Function

The use-rule-set command configures the blacklist and whitelist rule for the trunk group of the SIP or H.323 type.

The undo use-rule-set command restores the blacklist and whitelist rule configured for the trunk group.

By default, no blacklist or whitelist is configured.

Format

use-rule-set *rulename*

undo use-rule-set

Parameters

Parameter	Description	Value
rulename	Specifies the name of the blacklist and whitelist rule.	Character string type. The value is a string of 1-32 characters.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

Before configuring the blacklist and whitelist rule for trunk group, add the rule in the voice view.

Example

Configure the blacklist and whitelist named **rulenametest** for the H.323 trunk group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]rule-set rulenametest
[Huawei-voice-rule-set-rulenametest]quit
[Huawei-voice] trunk-group h323sy h323 symmetrical
[Huawei-voice-trunkgroup-h323sy]use-rule-set rulenametest
```

16.5.6.131 workmode (H323 attribute view)

Function

The **workmode** command sets the operation mode for the H323 stack.

The **undo workmode** command restores the default operation mode of the H323 stack.

By default, the H323 stack uses the international mode.

Format

workmode *workmode-value*

undo workmode

Parameters

Parameter	Description	Value
workmode-value	Specifies the operation mode of the H323 stack.	Enumerated type. The values are as follows: ● international ● national ● VT **NOTE** When the device connects to a Cisco device, the VT mode is recommended. By default, the operation mode is international.

Views

H323 attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the operation mode of the H323 stack to national.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h323-attribute
[Huawei-voice-h323-attribute] workmode national
```

16.5.7 Call Route configuration command

16.5.7.1 callroute

Function

The **callroute** command configures a call route.

The **undo callroute** command deletes a configured call route.

Format

callroute *callroute-name*

undo callroute *callroute-name*

Parameters

Parameter	Description	Value
callroute-name	Specifies the call route name.	The value is a string of 1 to 32 characters without spaces.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a call route named **router1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callroute route1
```

16.5.7.2 callroute (reroute view)

Function

The **callroute** command is used to configure the calling route for rerouting.

Format

callroute *callroute-name*

Parameters

Parameter	Description	Value
callroute-name	Specifies the call route name.	The value is a string of 1 to 32 characters without spaces.

Views

Reroute-deal view

Default Level

2: Configuration level

Usage Guidelines

The **callroute** command is used to configure the calling route for rerouting.

Example

Configure calling route for rerouting as test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] reroute-deal reroute-test
[Huawei-voice-reroute-deal-reroute-test] callroute test
```

16.5.7.3 callroute (route-analysis view)

Function

The **callroute** command configures a call route that references route-analysis.

Format

callroute *callroute-name*

Parameters

Parameter	Description	Value
callroute-name	Specifies the name of a call route.	The value is a string of 1 to 32 characters without spaces.

Views

route-analysis

Default Level

2: Configuration level

Usage Guidelines

The **callroute** command configures a call route that references route-analysis.

Example

Configure the call route **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] route-analysis test
[Huawei-voice-route-analysis-test] callroute test
```

16.5.7.4 callsource

Function

The **callsource command** configures a call source.

The **undo callsource command** deletes a configured call source.

Format

callsource *callsource-name*

undo callsource *callsource-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
callsource-name	Specifies the name of a call source.	The value is a string of 1 to 32 characters without spaces.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the call source **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callsource test
```

16.5.7.5 callsource (route-analysis view)

Function

The **callsource** command configures a call route that references route-analysis.

Format

callsource *callsource-name*

Parameters

Parameter	Description	Value
callsource-name	Specifies the name of a call source.	The value is a string of 1 to 32 characters without spaces.

Views

route-analysis

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **callsource** command configures a call source that references route-analysis.

Example

Configure the call source **a**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] route-analysis ra
[Huawei-voice-route-analysis-test] callsource a
```

16.5.7.6 display voice callroute

Function

The **display voice callroute** command displays the configuration of a call route.

The **display voice callroute** *callroute-name* **trunk-group brief** command displays the order for selecting trunk groups under a call route.

Format

display voice callroute [*callroute-name*] **detail**

display voice callroute *callroute-name* **trunk-group brief**

Parameters

Parameter	Description	Value
callroute *callroute-name*	Call route	The value is a string of 1 to 32 characters.
detail	Detail information	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command is used to display the call route.

Example

Display the configuration of a call route.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice] display voice callroute route detail
 Call route name        : route
 Reroute-deal name      : reroute-test
```

Display the order for selecting trunk groups under a call route.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice]display voice callroute sipip trunk-group brief
 Spec: 255, Records: 3
 ---------------------------------------------------------------------
 Index    Trunk group name     N/A    Select level   Trunk group id
 0        test                 ---    128            2
 1        pra                  ---    253            0
 2        sipip                ---    254            1
```

16.5.7.7 display voice callsource

Function

The **display voice callsource** command displays the configuration of a call source.

Format

display voice callsource [*callsource-name*]

Parameters

Parameter	Description	Value
callsource-name	Call source	The value is a string of 1 to 32 characters.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command is used to display the call source.

Example

Display the configuration of a call route.

```
<Huawei>system-view
[Huawei]voice
[Huawei-voice]display voice callsource
 Spec: 256, Records: 2
 ------------------------
 Call source name : default

 Call source name : test
```

16.5.7.8 display voice reroute-deal

Function

The **display voice reroute-deal** command displays reroute information.

Format

display voice reroute-deal [*reroute-deal-name*]

Parameters

Parameter	Description	Value
reroute-deal-name	Specifies the reroute name.	The value is a string of 1 to 32 characters without spaces.

Views

ALL

Default Level

2: Configuration level

Usage Guidelines

reroute-deal-name is optional. If *reroute-deal-name* is not supplied, all the reroute-deal configurations will be listed.

Example

Display the information about the reroute named **reroute-test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice reroute-deal reroute-test
Reroute-deal name : reroute-test
Recall route name : sipat0
Call route name   : route
Failed type value : route-failed
```

While no reroute-deal configuration is found, information is as follows.

```
[Huawei-voice]display voice reroute-deal
 Info: The reroute-deal record does not exist
```

Table 16-82 Description of the display voice reroute-deal command output

Item	Description
Reroute-deal name	Reroute name.
Recall route name	Name of the call route referenced by the reroute.
Call route name	Name of the call route that references the reroute.
Failed type value	Type of the reroute.

16.5.7.9 display voice route-analysis

Function

The **display voice route-analysis** command displays route analysis information.

Format

display voice route-analysis [*route-analysis-name*]

Parameters

Parameter	Description	Value
route-analysis-name	Specifies the route analysis name.	The value is a string of 1 to 32 characters without spaces.

Views

ALL

Default Level

2: Configuration level

Usage Guidelines

route-analysis-name is optional. If *route-analysis-name* is not supplied, all the route-analysis configurations will be listed.

Example

Display the information about the route analysis named **ra**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice]display voice route-analysis ra
 Route-analysis name : ra
 Call source name    : a
 Call route name     : 29
 Trunk group name    : sipip29
```

While no route-analysis configuration is found, information is as follows.

```
[Huawei-voice]display voice route-analysis
 Info: The route-analysis record does not exist
```

Table 16-83 Description of the display voice reroute-deal command output

Item	Description
Route-analysis name	Route analysis name.
Call source name	Name of the call source referenced by the route analysis.
Call route name	Name of the call route that references the route analysis.
Trunk group name	Name of the trunk group that references the route analysis.

16.5.7.10 failed-type (reroute view)

Function

The **failed-type** command configures a failure type of re-routing.

Format

failed-type *type-value*

Parameters

Parameter	Description	Value
type-value	Specifies the failure type of re-routing.	The value is <route-failed,call-failed>. route-failed: routing fails. call-failed: Calls fail. The default value is **route-failed**.

Views

reroute-deal

Default Level

2: Configuration level

Usage Guidelines

The **failed-type** command configures a failure type of re-routing.

Example

Set the failure type of re-routing to **call-failed**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] reroute-deal reroute-test
[Huawei-voice-reroute-deal-reroute-test] callroute test
[Huawei-voice-reroute-deal-reroute-test] re-callroute test2
[Huawei-voice-reroute-deal-reroute-test] failed-type call-failed
```

16.5.7.11 re-callroute (reroute view)

Function

The **re-callroute** command configures a call route referenced by a reroute.

Format

re-callroute *callroute-name*

Parameters

Parameter	Description	Value
callroute-name	Specifies the call route name.	The value is a string of 1 to 32 characters without spaces.

Views

Reroute-deal view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure a call route **test2** referenced by route **test** for rerouting.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] reroute-deal reroute-test
[Huawei-voice-reroute-deal-reroute-test] callroute test
[Huawei-voice-reroute-deal-reroute-test] re-callroute test2
```

16.5.7.12 reroute-deal

Function

The **reroute-deal** command establish a new reroute configuration or enter a configured reroute-deal view.

The **undo reroute-deal** *reroute-deal-name* command deletes a configured reroute configuration.

Format

reroute-deal *reroute-deal-name*

undo reroute-deal *reroute-deal-name*

Parameters

Parameter	Description	Value
reroute-deal-name	Specifies the reroute name.	The value is a string of 1 to 32 characters without spaces.

Views

voice

Default Level

2: Configuration level

Usage Guidelines

The **reroute-deal** command is the entrance of reroute-deal configuration. A reroute can be configured only in the reroute view.

Example

Configure a reroute named **reroute-test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] reroute-deal reroute-test
[Huawei-voice-reroute-deal-reroute-test]
```

16.5.7.13 route-analysis

Function

The **route-analysis** command establish route analysis record or enter a configured route-analysis view.

The **undo route-analysis** *route-analysis-name* command deletes a configured route-analysis configuration.

Format

route-analysis *route-analysis-name*

undo route-analysis *route-analysis-name*

Parameters

Parameter	Description	Value
route-analysis-name	Specifies the route analysis name.	The value is a string of 1 to 32 characters without spaces.

Views

voice

Default Level

2: Configuration level

Usage Guidelines

The **route-analysis** command is the entrance of route-analysis configuration.

Example

Configure a route-analysis named **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] route-analysis test
[Huawei-voice-route-analysis-test]
```

16.5.7.14 selecttype

Function

The **selecttype** command configures a call route policy.

The **undo selecttype** command restores the default call route policy.

By default, a call route policy is a non-intelligent route policy.

 Copyright © Huawei Technologies Co., Ltd.

Format

selecttype *selecttype-value*

undo selecttype

Parameters

Parameter	Description	Value
selecttype-value	Specifies a call route policy.	Enumerated value. The options are as follows: ● chargebase: charge rate-based ● loadshare: load balancing ● perloadshare: percentage-based ● userpriorlevel: user level-based ● loadbalance: based on the number of idle circuits ● callertimebase: based on the time and calling number ● none: non-intelligent-route

Views

Call route view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the call route policy to **loadshare**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] callroute route
[Huawei-voice-calloute-route]  selecttype loadshare
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.7.15 trunk-group (route-analysis view)

Function

The **trunk-group** command configures a trunk group that references route-analysis.

Format

trunk-group *trunk-group-name*

Parameters

Parameter	Description	Value
trunk-group-name	Specifies the name of a trunk group.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

A trunk group has been created.

Example

Configure the trunk-group **29** in route-analysis record.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] route-analysis ra
[Huawei-voice-route-analysis-ra] trunk-group 29
```

16.5.8 PBX Service Configuration Commands

16.5.8.1 access-telno

Function

The **access-telno** command configures an access number for group services.

Format

access-telno *telno-value*

Parameters

Parameter	Description	Value
telno-value	Indicates the access number for user group services.	The value is a number containing 1 to 16 digits.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Currently, the following access numbers are available:

PBX line selection (hunt)

Example

Set the country code to 86, the area code to 755, and the telephone number to 28980000 for the sequential ringing group test.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 28980000
```

16.5.8.2 afterroute-change

Function

Using the **afterroute-change** command, you can create a post-routing number change plan and enter its view.

Using the **undo afterroute-change** command, you can delete a post-routing number change plan.

Format

afterroute-change *name*

undo afterroute-change *name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name	Specifies the name of the post-routing number change plan.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create post-routing number change plan **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] afterroute-change test
[Huawei-voice-afterroute-change-test]
```

16.5.8.3 beforeroute-change

Function

Using the **beforeroute-change** command, you can create a pre-routing number change plan and enter its view.

Using the **undo beforeroute-change** command, you can delete a pre-routing number change plan.

Format

beforeroute-change *name*

undo beforeroute-change *name*

Parameters

Parameter	Description	Value
name	Specifies the name of the pre-routing number change plan.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

This command creates a pre-routing number change plan.

Example

Create pre-routing number change plan **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] beforeroute-change test
[Huawei-voice-beforeroute-change-test]
```

16.5.8.4 bind (service user group view)

Function

The **bind** command configures the other members except the primary number bound to the unicall service.

The **undo bind** command cancels the other members except the primary number bound to the unicall service.

Format

bind *bind-type bind-value* [**priority** *priority-value*] [**time-templet** *time-templet-name*]

undo bind *bind-type bind-value*

Parameters

Parameter	Description	Value
bind-type	Specifies the attribute of the bound terminal.	Enumerated type. The options are as follows: ● internal-telno: An intra-office user number is bound to the unicall service. ● external-telno: An inter-office user number is bound to the unicall service. ● SIPUE: A SIP UE is bound to the unicall service.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
bind-value	Specifies the number or ID of the bound terminal.	The value is a string of 1 to 32 characters.
priority *priority-value*	Specifies the priority of the bound terminal.	The value is an integer that ranges from 0 to 3.
time-templet *time-templet-name*	Valid time template name.	The value is a string of 1 to 32 characters. The time template must exist.

Views

service user group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Bind the intra-office user number **28780005** to the unicall service user group **28780004**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] unicall-group pbxuser 28980004
[Huawei-voice-unicall-group-28980004] bind internal-telno 28980005
```

16.5.8.5 bind main-eid (service view for the senior manager's secretary)

Function

The **bind main-eid** command binds the shared lines of the manager and secretary.

The **undo bind main-eid** command unbinds the shared lines of the manager and secretary.

Format

bind main-eid *main-eid-value* **shared-eid** *shared-eid-value*

undo bind main-eid *main-eid-value* **shared-eid** *shared-eid-value*

Parameters

Parameter	Description	Value
main-eid-value	Specifies the manager's shared line to be bound.	The value is a string of 1 to 32 characters.
shared-eid-value	Specifies the secretary's shared line to be bound.	The value is a string of 1 to 32 characters.

Views

Service view for the senior manager's secretary view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Bind shared lines of the manager and secretary for PBX user 1001.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ssca-group pbxuser 1001
[Huawei-ssca-group-1001] bind main-eid 1001 shared-eid 1002
```

16.5.8.6 busyselectmode (service user group view)

Function

The **busyselectmode** command configures the selection mode during busy hours for the ONLY service.

The **undo busyselectmode** command restores the default selection mode during busy hours for the ONLY service.

Format

busyselectmode *busyselect-value*

undo busyselectmode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
busyselect-value	Specifies the selection mode during busy hours for the ONLY service.	Enumerated type. The values are as follows: ● null: Do not call any terminal. ● all: Call all the terminals. ● active: Call the terminal that is in conversation. ● inactive: Call an idle terminal. ● By default, the value is all

Views

service user group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the selection mode during busy hours of the ONLY service user group **28780004** to **active**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] unicall-group pbxuser 28780004
[Huawei-voice-unicall-group-28780004] busyselectmode active
```

16.5.8.7 call dual-dial-tone-flag (pre-routing number change plan view)

Function

Using the **call dual-dial-tone-flag** command, you can configure whether to play second dial tone.

Using the **undo call dual-dial-tone-flag** command, you can restore the default setting. By default, second dial tone is not played.

Format

call dual-dial-tone-flag *dual-dial-tone-flag-value*

undo call dual-dial-tone-flag

Parameters

Parameter	Description	Value
dual-dial-tone-flag-value	Indicates whether to play second dial tone.	Enumerated type. The value is disable or enable: ● disable: Second dial tone is not played. ● enable: Second dial tone is played. ● the default value is disable

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable second dial tone playing.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] call dual-dial-tone-flag enable
```

16.5.8.8 call new-attribute (pre-routing number change plan view)

Function

The **call new-attribute** command configures the pre-routing number change plan for enterprises and DN sets.

The **undo call new-attribute** command cancels the pre-routing number change plan.

Format

call new-attribute { **enterprise** *enterprise-name* | **dn-set** *dn-set-name* } *

undo call new-attribute

Parameters

Parameter	Description	Value
enterprise *enterprise-name*	Specifies the name of an enterprise.	The value is a string of 1 to 32 characters.
dn-set *dn-set-name*	Specifies a DN set.	The value is a string of 1 to 32 characters.

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

This command configures the pre-routing number change plan.

Example

Configure enterprise named ab for the pre-routing number change plan.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] enterprise ab
[Huawei-voice-enterprise-hw] quit
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] call new-attribute enterprise ab
```

16.5.8.9 call re-analyse (pre-routing number change plan view)

Function

Using the **call re-analyse** command, you can configure whether to reanalyze the changed numbers.

Using the **undo call re-analyse** command, you can restore the default setting.

By default, the device does not reanalyze the changed numbers.

Format

call re-analyse *reanalyze-value*

undo call re-analyse

Parameters

Parameter	Description	Value
reanalyze-value	Indicates whether to reanalyze the changed numbers.	Enumerated type. The value is enable or disable: ● disable: not reanalyze the changed numbers. ● enable: reanalyze the changed numbers. The default value is disable.

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

This command configures the pre-routing number change plan.

Example

Configure the device to reanalyze the changed numbers.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] call re-analyse enable
```

16.5.8.10 call-right (user group view)

Function

The **call-right** command configures call-in and call-out rights for users in a user group.

The **undo call-right** command restores the default setting.

By default, users of a user group have all call-in rights and call-out rights of intra-office and local calls.

Format

call-right { **in** | **out** } { { **inter** *inter-value* | **local** *local-value* | **ddd** *ddd-value* | **idd** *idd-value* } * | **all** }

undo call-right [**in** | **out**]

Parameters

Parameter	Description	Value
in	Indicates call-in rights of users in a user group.	-
out	Indicates call-out rights of users in a user group.	-
inter *inter-value*	Indicates whether the intra-office call right is enabled.	Enumerated value. The options are as follows: ● disable ● enable
local *local-value*	Indicates whether the local call right is enabled.	Enumerated value. The options are as follows: ● disable ● enable
ddd *ddd-value*	Indicates whether the right of national toll calls is enabled.	Enumerated value. The options are as follows: ● disable ● enable
idd *idd-value*	Indicates the right of international toll calls is enabled.	Enumerated value. The options are as follows: ● disable ● enable
all	Indicates that all rights are enabled.	The rights include **inter** (intra-office calls), **local** (local calls), **ddd** (national toll calls), and **idd** (international toll calls).

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Calls are classified into intra-office calls, local calls, national toll calls, and international toll calls. The system determines whether an outgoing call is allowed

based on the call-out rights configured for the calling user group and requirements of the called prefix on call rights. The system determines whether an incoming call is allowed based on the call-in rights configured for the called user group and requirement of the calling prefix on call rights.

Prerequisite

A user group has been created and the access code has been configured.

Example

Disable the **idd** call-in right and enable the **ddd** call-out right for the user group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 1001
[Huawei-voice-pbxusergroup-test] call-right in idd disable
[Huawei-voice-pbxusergroup-test] call-right out ddd enable
```

16.5.8.11 called (calling number change view)

Function

The **called** command configures a called number change rule for a calling number change plan.

Format

called { **del-then-insert** *del-offset del-len insert-telnum* | **del** *del-offset del-len* | **insert** *insert-offset insert-telnum* | **no-change** }

Parameters

Parameter	Description	Value
del-then-insert	Changes some digits of the called number.	–
del-offset	Indicates the start digit to be deleted from the long called number.	The value is an integer that ranges from 1 to 32.
del-len	Indicates the number of digits to be deleted.	The value is an integer that ranges from 1 to 32.
insert-telnum	Indicates the number inserted into the called number.	The value is a string of 1 to 24 characters.
del	Deletes some digits from the called number.	–
insert	Inserts a number.	–

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
insert-offset	Indicates the location to insert a number.	The value is an integer that ranges from 1 to 24.
no-change	Indicates that the called number is not changed.	–

Views

Calling number change view

Default Level

2: Configuration level

Usage Guidelines

The **called** command configures a called number change rule for a calling number change plan.

Example

Configure the called number not to change

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change test
[Huawei-voice-caller-change-test] called no-change
```

16.5.8.12 called (post-routing number change plan view)

Function

The **called** command configures a called number change rule for a post-routing number change plan.

Format

called{ **del-then-insert** *del-offset del-len insert-telnum* | **del** *del-offset del-len* | **insert** *insert-offset insert-telnum* | **no-change** }

Parameters

Parameter	Description	Value
del-then-insert	Changes some digits of the called number.	–
del-offset	Indicates the start digit to be deleted from the long called number.	The value is an integer that ranges from 1 to 32.

Parameter	Description	Value
del-len	Indicates the number of digits to be deleted.	The value is an integer that ranges from 1 to 32.
insert-telnum	Indicates the number inserted into the called number.	The value is a string of 1 to 24 characters.
del	Deletes some digits from the called number.	–
insert	Inserts a number.	–
insert-offset	Indicates the location to insert a number.	The value is an integer that ranges from 1 to 24.
no-change	Indicates that the called number is not changed.	–

Views

Post-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

The **called** command configures a called number change rule for a post-routing number change plan.

Example

Configure the called number not to change.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] afterroute-change test
[Huawei-voice-afterroute-change-test] called no-change
```

16.5.8.13 called (pre-routing number change plan view)

Function

Using the **called** command, you can configure the called number change rule for a pre-routing number change plan.

Format

called { **del-then-insert** *del-offset del-len insert-telnum* | **del** *del-offset del-len* | **insert** *insert-offset insert-telnum* | **no-change** }

Parameters

Parameter	Description	Value
del-then-insert	Changes some digits of the called number.	-
del-offset	Indicates the start digit to be deleted from the long called number.	The value is an integer that ranges from 1 to 32.
del-len	Indicates the number of digits to be deleted.	The value is an integer that ranges from 1 to 32.
insert-telnum	Indicates the number inserted into the called number.	The value is a string of 1 to 24 characters.
del	Deletes some digits from the called number.	-
insert	Inserts a number.	-
insert-offset	Indicates the location to insert the number.	The value is an integer that ranges from 1 to 24.
no-change	Indicates that the called number is not changed.	-

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

This command configures the pre-routing number change plan.

Example

Configure the called number not to change.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] called no-change
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.14 caller (calling number change view)

Function

The **caller** command configures a calling number change rule for a calling number change plan.

Format

caller { **del-then-insert** *del-offset del-len insert-telnum* | **del** *del-offset del-len* | **insert** *insert-offset insert-telnum* | **no-change** }

Parameters

Parameter	Description	Value
del-then-insert	Changes some digits of the calling number.	–
del-offset	Indicates the start digit to be deleted from the long calling number.	The value is an integer that ranges from 1 to 32.
del-len	Indicates the number of digits to be deleted.	The value is an integer that ranges from 1 to 32.
insert-telnum	Indicates the number inserted into the calling number.	The value is a string of 1 to 24 characters.
del	Deletes some digits from the calling number.	–
insert	Inserts a number.	–
insert-offset	Indicates the location to insert a number.	The value is an integer that ranges from 1 to 24.
no-change	Indicates that the calling number is not changed.	–

Views

Calling number change view

Default Level

2: Configuration level

Usage Guidelines

The **caller** command configures a calling number change rule for a calling number change plan.

Example

Configure a rule to change the calling number: delete the first three digits, and then insert 888.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change test
[Huawei-voice-caller-change-test] caller del-then-insert 1 3 888
```

16.5.8.15 caller (post-routing number change plan view)

Function

Using the **caller** command, you can configure the calling number change rule for a post-routing number change plan.

Format

caller { **del-then-insert** *del-offset del-len insert-telnum* | **del** *del-offset del-len* | **insert** *insert-offset insert-telnum* | **no-change** }

Parameters

Parameter	Description	Value
del-then-insert	Changes some digits of the calling number.	-
del-offset	Indicates the start digit to be deleted from the long calling number.	The value is an integer that ranges from 1 to 32.
del-len	Indicates the number of digits to be deleted.	The value is an integer that ranges from 1 to 32.
insert-telnum	Indicates the number inserted into the calling number.	The value is a string of 1 to 24 characters.
del	Deletes some digits from the calling number.	-
insert	Inserts a number.	-
insert-offset	Indicates the location to insert the number.	The value is an integer that ranges from 1 to 24.
no-change	Indicates that the calling number is not changed.	-

Views

Post-routing number change plan view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command configures the post-routing number change plan.

Example

Configure a rule to change the calling number: delete the first three digits, and then insert 245.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] afterroute-change test
[Huawei-voice-afterroute-change-test] caller del-then-Insert 1 3 245
```

16.5.8.16 caller (pre-routing number change plan view)

Function

The **caller** command configures a calling number change rule for a pre-routing number change plan.

Format

caller { **del-then-insert** *del-offset del-leninsert-telnum* | **del** *del-offset del-len* | **insert** *insert-offset insert-telnum* | **no-change**}

Parameters

Parameter	Description	Value
del-then-insert	Changes some digits of the calling number.	–
del-offset	Indicates the start digit to be deleted from the long calling number.	The value is an integer that ranges from 1 to 32.
del-len	Indicates the number of digits to be deleted.	The value is an integer that ranges from 1 to 32.
insert-telnum	Indicates the number inserted into the calling number.	The value is a string of 1 to 24 characters.
del	Deletes some digits from the calling number.	–
insert	Inserts a number.	–
insert-offset	Indicates the location to insert a number.	The value is an integer that ranges from 1 to 24.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-change	Indicates that the calling number is not changed.	-

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

The **caller** command configures a calling number change rule for a pre-routing number change plan.

Example

Configure the calling number not to change.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] caller no-change
```

16.5.8.17 caller-change (voice view)

Function

The **caller-change** command configures the calling number change service.

The **undo caller-change** command deletes the calling number change service.

By default, the calling number change service is not configured.

Format

caller-change *caller-change-name*

undo caller-change *caller-change-name*

Parameters

Parameter	Description	Value
caller-change-name	Specifies the name of the calling number change view.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

To hide calling numbers or display the same calling number for all outgoing calls, configure the calling number change service. When a user initiates calls, the calling number changes to the new number.

NOTE

Calling number change is also called calling number discrimination.

Example

Configure the calling number change view **caller**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change caller
```

16.5.8.18 callerprefix (calling number change view)

Function

The **callerprefix** command configures a calling number to be changed.

Format

callerprefix [**non-match**] *callerprefix-value*

Parameters

Parameter	Description	Value
non-match	Specifies performing the NOT operation on the matching result when the calling number is matched.	-
callerprefix-value	Specifies a calling number to be changed.	The value is a numeral string of 1 to 24 digits.

Views

Calling number change view

Default Level

2: Configuration level

Usage Guidelines

The **callerprefix** command configures a calling number to be changed.

When the **non-match** field is configured, the AR performs the NOT operation on the matching result when the calling number is matched. For example, when **callerprefix non-match 800** is configured, all numbers in character strings except 800 can be matched.

Example

Specify calling number 800 to be changed

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change test
[Huawei-voice-caller-change-test] callerprefix 800
```

16.5.8.19 callprefix (post-routing number change plan view)

Function

Using the **callprefix** command, you can configure a call prefix for a post-routing number change plan.

Format

callprefix *callprefix-value*

Parameters

Parameter	Description	Value
callprefix-value	Indicates the call prefix.	The value is a string of 1 to 32 characters.

Views

Post-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

Before using the **callprefix (post-routing number change plan view)** command, run the callprefix command to create a call prefix.

Example

Set the call prefix for the post-routing number change plan to 2898.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] afterroute-change test
[Huawei-voice-afterroute-change-test] callprefix 2898
```

16.5.8.20 callprefix (pre-routing number change plan view)

Function

Using the **callprefix** command, you can configure a call prefix for a pre-routing number change plan.

Format

callprefix *callprefix-value*

Parameters

Parameter	Description	Value
callprefix-value	Indicates the call prefix.	The value is a string of 1 to 32 characters.

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

Before using the **callprefix (pre-routing number change plan view)** command, run the callprefix command to create a call prefix.

Example

Set the call prefix for the pre-routing number change plan to 2898.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] callprefix 2898
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.21 condition called-telno (pre-routing number change plan view)

Function

The **condition called-telno** command configures a called number for a pre-routing number change plan.

The **undo condition called-telno** command deletes the called number for a pre-routing number change plan.

By default, no called number is configured for a pre-routing change plan.

Format

condition called-telno *telno-value*

undo condition called-telno

Parameters

Parameter	Description	Value
telno-value	Specifies a called number that needs to be changed before route selection.	The value is a string of 1 to 16 characters, which can be digits, the lowercase character "x", and asterisk (*). The "x" represents any digit. The asterisk (*) represents 1 to 16 digits and can appear only once in a number.

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a called number received by the system is the same as the called number configured by using the **condition called-telno** command, the pre-routing number change plan takes effect.

Precautions

When running the **condition called-telno** command to configure a called number for a pre-routing number change plan, the prefix of the configured called number

 Copyright © Huawei Technologies Co., Ltd.

must be the same as the prefix bound to the pre-routing number change plan. Otherwise, the pre-routing number change plan does not take effect.

Example

Set the called number of the pre-routing number change plan to 123456.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] condition called-telno 123456
```

16.5.8.22 condition caller-telno (post-routing number change plan view)

Function

The **condition caller-telno** command configures the calling number for a post-routing number change plan.

The **undo condition caller-telno** command deletes the calling number for a post-routing number change plan.

Format

condition caller-telno *telno-value*

undo condition caller-telno

Parameters

Parameter	Description	Value
caller-telno *telno-value*	Specifies the calling number that requires post-routing change.	The value is a string of 1 to 16 characters.

Views

Post-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

This command configures the post-routing number change plan.

Example

Set the calling number of the post-routing number change plan **test** to **123456**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] afterroute-change test
[Huawei-voice-afterroute-change-test] condition caller-telno 123456
```

16.5.8.23 condition caller-telno (pre-routing number change plan view)

Function

The **condition caller-telno** command configures the calling number for a pre-routing number change plan.

The **undo condition caller-telno** command deletes the calling number of a pre-routing number change plan.

Format

condition caller-telno *telno-value*

undo condition caller-telno

Parameters

Parameter	Description	Value
caller-telno *telno-value*	Specifies the calling number that requires pre-routing change.	The value is a string of 1 to 16 characters, which can be digits, the lowercase character "x", and asterisk (*). The "x" represents any digit. The asterisk (*) represents 1 to 16 digits and can appear only once in a number.

Views

Pre-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

This command configures the pre-routing number change plan.

Example

Set the calling number of the pre-routing number change plan to **123456**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] beforeroute-change 1
[Huawei-voice-beforeroute-change-1] condition caller-telno 123456
```

16.5.8.24 config-dn (service view for the senior manager's secretary)

Function

The **config-dn** command modifies parameters for the manager or secretary.

The **undo config-dn** command cancels parameters for the manager or secretary.

Format

config-dn *user-dn-value* {**alerting-silence** *alerting-silence-value* | **auto-answer** *auto-answer-value* | **private-dn** *private-dn-value*}

undo config-dn *user-dn-value* { **alerting-silence** | **auto-answer** | **private-dn** }

Parameters

Parameter	Description	Value
user-dn-value	Specifies a user number.	The value is a string of 1 to 32 characters.
alerting-silence-value	Specifies a silent mode.	Enumerated type. The options are as follows: ● enable ● disable default:disable
auto-answer-value	Specifies an automatic answering mode.	Enumerated type. The options are as follows: ● enable ● disable default:disable
private-dn-value	Specifies a private line number.	The value is a string of 1 to 32 characters.

Views

Service view for the senior manager's secretary view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set a private line number for manager number 1001.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]ssca-group pbxuser 1001
[Huawei-ssca-group-1001]config-dn 1001 private-dn 1002
```

16.5.8.25 country-code (trunk group view)

Function

The **country-code** command configures the country code and region code for a trunk group.

The **undo country-code** command restores the configuration.

By default, the country code is the same as the system country code.

Format

country-code *country-code-value* [**area-code** *area-code-value*]

undo country-code

Parameters

Parameter	Description	Value
country-code-value	Specifies a country code.	The value is a numeric string of 1 to 4 digits.
area-code *area-code-value*	Specifies an area code.	The value is a numeric string of 1 to 8 digits.

Views

Trunk group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the country code to 86 and region code to 25 for the trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] trunk-group test fxo
[Huawei-voice-trunkgroup-test] country-code 86 area-code 25
```

16.5.8.26 cpu-flowcontrol

Function

The **cpu-flowcontrol** command sets upper and lower thresholds for CPU overload flow control.

The **undo cpu-flowcontrol** command cancels upper and lower thresholds for CPU overload flow control.

By default, the lower threshold for CPU overload flow control is 95, the upper threshold for CPU overload flow control is 99.

Format

cpu-flowcontrol low-level { *low-level-value* | **high-level** *high-level-value* }*

undo cpu-flowcontrol

Parameters

Parameter	Description	Value
low-level *low-level-value*	Specifies the lower threshold for CPU overload flow control.	The value is an integer that ranges from 1 to 99.
high-level *high-level-value*	Specifies the upper threshold for CPU overload flow control.	The value is an integer that ranges from 1 to 99.

NOTE

The lower threshold must be smaller than the upper threshold.

Views

Voice view

Default Level

3: Management level

Usage Guidelines

The user can run **cpu-flowcontrol** command sets upper and lower thresholds for CPU overload flow control.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set upper and lower thresholds for CPU overload flow control.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] cpu-flowcontrol low-level 95 high-level 99
```

16.5.8.27 crbt (user group view)

Function

The **crbt** command enables or disables the RBT service for a user group.

The **undo crbt** command restores the default setting.

By default, the RBT service is disabled for a user group.

Format

crbt *crbt-right-value*

undo crbt

Parameters

Parameter	Description	Value
crbt-right-value	Indicates whether to enable or disable the RBT function for a user group.	Enumerated value. The options are as follows: ● disable ● enable

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When there are users that take effect currently in a user group and the RBT function is enabled for the user group, a calling user can hear the configured RBT announcements when calling the user group.

Prerequisite

A user group has been created and the access code has been configured.

Example

Enable the RBT function for the user group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 1001
[Huawei-voice-pbxusergroup-test] crbt enable
```

16.5.8.28 crbt-file (user group view)

Function

The **crbt-file** command specifies an RBT file for a user group.

The **undo crbt-file** command restores the default setting.

By default, no RBT file is specified for a user group.

Format

crbt-file *crbt-file-name* **status** *status-value* [**description** *description*]

undo crbt-file *crbt-file-name* [**description**]

Parameters

Parameter	Description	Value
crbt-file-name	Indicates the name of an RBT file.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of *path:/file-name*, for example, **flash:/test.wav**.
status *status-value*	Specifies the approval status of an RBT file.	Enumerated value. The options are as follows: ● no_check: The RBT file is not approved. ● pass: The RBT file is approved. ● no_pass: The RBT file fails to be approved.
description *description*	Specifies the description of an RBT file.	The value is a string of 1 to 64 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **crbt-file** command to configure multiple RBT files for a user group in the user group view, and then run the **service crbt** command to activate one of the RBT files. When a user calls the user group, the music or sound effect but not the common ringback tone will be played to the calling user.

Prerequisite

A user group has been created and the access code has been configured.

Precautions

RBT files must be in .wav format.

Example

Specify the RBT file **sss.wav** with the approval status **pass** for the user group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 1001
[Huawei-voice-pbxusergroup-test] crbt-file flash:/sss.wav status pass
```

16.5.8.29 crbt-file (enterprise view)

Function

Using the **crbt-file** command, you can specify the RBT file for the enterprise.

Using the **undo crbt-file** command, you can restore the default setting.

Format

crbt-file *crbt-file-name* **status** *status-value* [**description** *description*]

undo crbt-file *crbt-file-name* [**description**]

Parameters

Parameter	Description	Value
crbt-file-name	Specifies the RBT file name.	The value is a string of 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
status *status-value*	Specifies the approval status of an RBT file.	The value is **no_check**, **pass** or **no_pass**. ● **no_check**: unapproved ● **pass**: approved ● **no_pass**: rejected The default value is **no_check**.
description *description*	Indicates the description of an RBT file.	The value is a string of 1 to 64 characters.

Views

Enterprise view

Default Level

2: Configuration level

Usage Guidelines

RBT files must be in the wav format.

Example

Specify the RBT file **sss.wav** with the approval status **pass** for the enterprise **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] enterprise test
[Huawei-voice-enterprise-test] crbt-file flash:/sss.wav status pass
```

16.5.8.30 custom-right (calling number change view)

Function

The **custom-right** command configures 32-level rights for calling number change.

By default, no 32-level right is bound to a calling number after change.

Format

custom-right { *c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32* } *

undo custom-right [*c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32*] *

Parameters

Parameter	Description	Value
c1 | *c2* | *c3* | *c4* | *c5* | ...| *c32*	Specifies 32-level rights to be configured for calling number change.	The value can be one or more of **c1** to **c32**.

Views

Calling number change view

Default Level

2: Configuration level

Usage Guidelines

32-level rights for calling number change refer to 32-level rights of calling numbers after change. Currently, these rights are applicable only to calling number change for a trunk group, and are not involved in other scenarios.

By default, if no 32-level right is configured for calling number change, a calling number after change loses all 32-level rights.

You can configure 1 to 32 customized rights.

Adding or deleting a right does not affect existing 32-level rights.

To clear all 32-level rights configured for calling number change, run the **undo custom-right** command.

Example

Configure 32-level rights **c2**, **c4**, and **c8** for calling number change **callerchg1**.

```
<Huawei> system-view
[Huawei-voice] caller-change callerchg1
[Huawei-voice-caller-change-callerchg1] callerprefix 2898*
[Huawei-voice-caller-change-callerchg1] caller no-change
[Huawei-voice-caller-change-callerchg1]called no-change
[Huawei-voice-caller-change-callerchg1]custom-right c2 c4 c8
```

Delete 32-level right **c4** for calling number change **callerchg1**.

```
<Huawei> system-view
[Huawei-voice] caller-change callerchg1
[Huawei-voice-caller-change-callerchg1] undo custom-right c4
```

Clear all 32-level rights configured for calling number change **callerchg1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change callerchg1
[Huawei-voice-caller-change-callerchg1] undo custom-right
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.31 display voice afterroute-change

Function

The **display voice afterroute-change** command displays the configuration of the post-routing number change service.

Format

display voice afterroute-change [*name*]

Parameters

Parameter	Description	Value
name	Specifies the name of the post-routing number change service.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When *name* is not specified, the configurations of the post-routing number change services are displayed.

Example

Display the configuration of the post-routing number change service **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice afterroute-change test
  After route change name  : test
  callprefix               : 01
  Prefix                   : 01
  Trunk group              : sipbb
  Caller telephone number  :
  Caller change type       : No change
  Called change type       : No change
```

Table 16-84 Description of the **display voice afterroute-change** command output

Item	Description
After route change name	Name of the post-routing number change service.
callprefix	Call prefix view bound to the post-routing number change service. You can set this parameter using the **16.5.8.19 callprefix (post-routing number change plan view)** command.
Prefix	Prefix bound to the post-routing number change service.
Trunk group	Trunk group bound to the post-routing number change service. You can set this parameter using the **16.5.8.120 trunk-group (post-routing number change plan view)**command.
Caller telephone number	Calling number for a post-routing number change service. You can set this parameter using the **16.5.8.22 condition caller-telno (post-routing number change plan view)** command.
Caller change type	Caller number change type. You can set this parameter using the **16.5.8.15 caller (post-routing number change plan view)** command
Called change type	Called number change type. You can set this parameter using the **16.5.8.12 called (post-routing number change plan view)** command.

16.5.8.32 display voice beforeroute-change

Function

The **display voice beforeroute-change** command displays the configuration of the pre-routing number change service.

Format

display voice beforeroute-change [*name*]

Parameters

Parameter	Description	Value
name	Specifies the name of the pre-routing number change service.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

When *name* is not specified, the configurations of the pre-routing number change services are displayed.

Example

Display the configuration of the pre-routing number change service.

```
<Huawei> display voice beforeroute-change test
  Before route change name : test
  callprefix                : abcd
  Prefix                    : 123
  Caller telephone number  : 500
  Caller change type        : Insert
  Caller change position    : 1
  Caller change new number : 0571
  Called change type        : Delete
  Called change position    : 1
  Called change length      : 2
  Re-analyze                : Disable
  Dual dialtone flag        : Disable
  New enterprise            : ab
  New dn-set                : local
```

Table 16-85 Description of the display voice beforeroute-change command output

Item	Description
Before route change name	Name of the pre-routing number change service.
Callprefix	Call prefix bound to the pre-routing number change service. You can set this parameter using the **16.5.8.20 callprefix (pre-routing number change plan view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Prefix	Prefix bound to pre-routing number change.
Caller telephone number	Calling number for a pre-routing number change service. You can set this parameter using the **16.5.8.23 condition caller-telno (pre-routing number change plan view)** command.
Caller change type	Caller number change type.
Caller change position	Calling number change position.
Caller change length	Calling number change length.
Called change type	Called number change type.
Called change position	Called number change position.
Called change length	Called number change length.
Re-analyze	Whether to reanalyze the changed numbers. You can set this parameter using the **16.5.8.9 call re-analyse (pre-routing number change plan view)** command.
Dual dialtone flag	Whether to play second dial tone. You can set this parameter using the **16.5.8.7 call dual-dial-tone-flag (pre-routing number change plan view)** command.
New enterprise	New enterprise. You can set this parameter using the **16.5.8.8 call new-attribute (pre-routing number change plan view)** command.
New dn-set	New DN set. You can set this parameter using the **16.5.8.8 call new-attribute (pre-routing number change plan view)** command.

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.33 display voice caller-change

Function

The **display voice caller-change** command displays the configuration of the number change service.

Format

display voice caller-change [*caller-change-name*]

Parameters

Parameter	Description	Value
caller-change-name	Specifies the calling number change view name.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

View information about calling number change view test.

```
<Huawei> display voice caller-change test
  Spec:  128, Records count: 2
  --------------------------
  Caller change name       : 0
  Caller Prefix Value      : 7*
  Enterprise               : default
  Dn-set                   : DefaultDialPlan
  New Callsource Name      :
  Caller change type       : Delete Then Insert
  Caller change position   : 1
  Caller change length     : 32
  Caller change new number : 28987000
  Called change type       : Delete Then Insert
  Called change position   : 1
  Called change length     : 3
  Called change new number : 888
  Outgoing right           : inter&local
  Custom right             : No custom right
```

Table 16-86 Description of the **display voice caller-change** command output

Item	Description
Spec	Total space of prefix information.
Records count	Number of records.
Caller change name	Calling number change view name.
Caller Prefix Value	Calling number to change.
Enterprise	Enterprise of the calling number to change.
Dn-set	DN set of the calling number to change.
New Callsource Name	New call source.
Caller change type	Calling number change type.
Caller change position	Calling number change position.
Caller change length	Calling number change length.
Caller change new number	The number inserted into the caller number.
Called change type	Called number change type.
Called change position	Called number change position.
Called change length	Called number change length.
Called change new number	The number inserted into the called number.
Outgoing right	Outgoing right of the calling number to change.
Custom right	32-level rights.

16.5.8.34 display voice cpu-flowcontrol

Function

The **display voice cpu-flowcontrol** command displays the upper and lower thresholds for CPU overload control.

Format

display voice cpu-flowcontrol

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

By default, the upper and lower thresholds for CPU overload control are 99 and 95 respectively.

Example

#Display the upper and lower thresholds for CPU overload control

```
<Huawei> display voice cpu-flowcontrol
 CPU-FlowControl Lowlevel-value: [95%]
 CPU-FlowControl Highlevel-value: [99%]
[Huawei-voice]
```

16.5.8.35 display voice gnr-number

Function

The **display voice gnr-number** command displays information of GNR numbers and full-numbers under the GNR number in the system.

Format

display voice gnr-number [*gnr-number-value*]

Parameters

Parameter	Description	Value
gnr-number-value	show the full-numbers of the GNR-number	The value is a string of 1 to 32 characters.

Views

All view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None.

Example

Display information of all gnr-numbers configs in the system.

```
<Huawei> display voice gnr-number
  Spec:  30, Records: 4
  -----------------------
  gnr-number    : 23374
  full-number   : 1223833
  full-number   : 122383833

  gnr-number    : 068741
  full-number   : 0687411000
  full-number   : 0687411001
  full-number   : 0687411002
  full-number   : +0687411003

  gnr-number    : 123444001
  full-number   : 23478237
  full-number   : 1182772

  gnr-number    : 123456001
  full-number   : 12334444
  full-number   : 12334338348
  full-number   : 1233433834349
  full-number   : 123343383434234
  full-number   : 12334338
```

Display information about GNR number 068741.

```
<Huawei> display voice gnr-number 068741
  gnr-number    : 068741
  Spec:  50, Records: 4
  -----------------------
  full-number   : 0687411000
  full-number   : 0687411001
  full-number   : 0687411002
  full-number   : +0687411003
```

16.5.8.36 display voice group-member

Function

The **display voice groupmember** command displays information about all hunt-group members or one hunt-group member in the system.

Format

display voice group-member [**pbxusergroup** *user-group-name* | **pbxuser** *pbxuser-name*]

Parameters

Parameter	Description	Value
pbxusergroup *user-group-name*	Displays information about members of a specified user group. *user-group-name* specifies the name of the user group.	The value is a string of 1 to 32 characters.
pbxuser *pbxuser-name*	Displays detailed information about members of a user group.	The value is a string of 1 to 32 characters.

Views

All view

Default Level

3: Management level

Usage Guidelines

None.

Example

Display information about members of user group 28980000.

```
<Huawei> display voice group-member pbxuser 28980000
  Group name              : hunt1
  Enterprise              : default
  Telno                   : 28980000
  Time period from date  : -
  Time period to date    : -
  Time period from time  : -
  Time period to time    : -
  Time repeat begin date : -
  Time repeat end date   : -
  Time repeat begin time : -
  Time repeat end time   : -
  Time repeat begin week : -
  Time repeat end week   : -
  Member index            : 0
  Admin state             : On Line
```

Display information about the hunt member of pbxuser hunt1.

```
<Huawei> display voice group-member pbxusergroup hunt1
 Group name              : hunt1
 Enterprise              : default
 Telno                   : 28980000
 Time period from date  : -
 Time period to date    : -
 Time period from time  : -
 Time period to time    : -
```

```
Time repeat begin date : -
Time repeat end date   : -
Time repeat begin time : -
Time repeat end time   : -
Time repeat begin week : -
Time repeat end week   : -
Member index           : 0
Admin state            : On Line

Group name             : hunt1
Enterprise             : default
Telno                  : 28980002
Time period from date  : -
Time period to date    : -
Time period from time  : -
Time period to time    : -
Time repeat begin date : -
Time repeat end date   : -
Time repeat begin time : -
Time repeat end time   : -
Time repeat begin week : -
Time repeat end week   : -
Member index           : 1
Admin state            : On Line
```

Table 16-87 Description of the **display voice group-member** command output

Item	Description
Group name	User group name.
Enterprise	Enterprise that members belong to.
Telno	Phone number of the user group member.
Time period from date	Start date in a period.
Time period to date	End date in a period.
Time period from time	Start time in a period.
Time period to time	End time in a period.
Time repeat begin date	Start date.
Time repeat end date	End date.
Time repeat begin time	Start time.
Time repeat end time	End time.
Time repeat begin week	Start weekday.
Time repeat end week	End weekday.
Member index	-
Admin state	Administrator status.

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.37 display voice ivr-voice-file

Function

The **display voice ivr-voice-file** command displays information about all IVR files.

Format

display voice ivr-voice-file

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display information about all IVR files

```
<Huawei> display voice ivr-voice-file
 Voice filename: sd1:/menu.wav
 Voice type: menu
 Voice filename: sd1:/welcome.wav
 Voice type: welcome
```

Table 16-88 Description of the **display voice ivr-voice-file** command output

Item	Description
Voice filename	Name of the IVR file.
Voice type	Type of the IVR file.

16.5.8.38 display voice number-map

Function

The **display voice number-map** command displays number mapping records.

Format

display voice number-map [*number-map-name*]

Parameters

Parameter	Description	Value
number-map-name	Specifies the name of a number mapping record.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display all number mapping records.

```
<Huawei> display voice number-map
 Spec: 250, Records:1
 ------------------------
 Internal-num value: 1000
 External-num value: 05711000
 Enterprise name   : default
```

16.5.8.39 display voice pbxuser callback-info

Function

The **display voice pbxuser callback-info** command displays callback info of a PBX user.

Format

display voice pbxuser *name* **callback-info**

Parameters

Parameter	Description	Value
name	Indicates the PBX user name.	The value is a string of 1 to 32 characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the callback info of the PBX user **abcd**.

```
<Huawei> display voice pbxuser abcd callback-info
  Busy callback registed called number          :
  No answer callback registed called number     :
```

Table 16-89 Description of the **display voice pbxuser callback-info** command output

Item	Description
Busy callback registed called number	Registered ccbs called number of the PBX user.
No answer callback registed called number	Registered ccnr called number of the PBX user.

16.5.8.40 display voice pbxuser service-active

Function

The **display voice pbxuser service-active** command displays service rights of a PBX user.

Format

display voice pbxuser *name* **service-active**

Parameters

Parameter	Description	Value
name	Indicates the PBX user name.	The value is a string of 1 to 32 characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the user rights of the PBX user **pots1**.

```
<Huawei> display voice pbxuser pots1 service-active
 Password call barring          : Disable
  Call waiting                  : Disable
  Digital number limit call     : Disable
```

Table 16-90 Description of the **display voice pbxuser service-right** command output

Item	Description
Password call barring	Password-based call barring.
Call waiting	Call waiting.
Digital number limit call	Call barring by number

.

16.5.8.41 display voice pbxuser service-right

Function

The **display voice pbxuser service-right** command displays service rights of a PBX user.

Format

display voice pbxuser *name* **service-right**

Parameters

Parameter	Description	Value
name	Indicates the PBX user name.	The value is a string of 1 to 32 characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the user rights of the PBX user **abcd**.

```
<Huawei> display voice pbxuser abcd service-right
  Abbreviated dialing                          : Enable
  Call barring                                 : Enable
  Call forwarding busy                         : Enable
  Call forwarding condition                    : Enable
  Call forwarding no reply                     : Enable
  Call forwarding offline                      : Enable
  Call forwarding unconditional                : Enable
  Call waiting                                 : Enable
  Calling line identification presentation     : Enable
  Calling line identification restriction override  : Disable
  Calling line identification restriction      : Disable
  Completion of calls to busy subscriber       : Disable
  Completion of calls to no reply subscriber   : Disable
  Digital number limit call                    : Disable
  Do not disturb                               : Enable
  Password call barring                        : Disable
  Pickup in group                              : Disable
  Pickup in special                            : Disable
  Query dial number                            : Enable
  Reject anonymous call                        : Disable
  Reject call selective                        : Disable
  Ring service                                 : Disable
  SCC cancel register service                  : Disable
  Secretary                                    : Disable
  Selective call acceptance                    : Disable
  Three party                                  : Disable
  Wake call                                    : Enable
  Instant conference                           : Disable
  Hotline                                      : Disable
Message waiting indication                     : Disable
  forwarding call to voice mail unconditional  : Disable
  forwarding call to voice mail on busy        : Disable
  forwarding call to voice mail on no reply    : Disable
  forwarding call to voice mail on offline     : Disable
  Call of multiple lines                       : Disable
Caller line name presentation                  : Enable
Caller line name presentation                  : Disable
```

Table 16-91 Description of the display voice pbxuser service-right command output

Item	Description
Abbreviated dialing	Abbreviated dialing.

Item	Description
Call barring	Call barring.
Call forwarding busy	Call forwarding busy.
Call forwarding condition	Call forwarding condition.
Call forwarding no reply	Call forwarding no reply.
Call forwarding offline	Call forwarding offline.
Call forwarding unconditional	Call forwarding unconditional.
Call waiting	Call waiting.
Calling line identification presentation	Calling line identification presentation.
Calling line identification restriction override	Calling line identification restriction override.
Calling line identification restriction	Calling line identification restriction.
Completion of calls to busy subscriber	Completion of calls to busy subscriber.
Completion of calls to no reply subscriber	Completion of calls to no reply subscriber.
Digital number limit call	Digital number call limit.
Do not disturb	Do not disturb.
Password call barring	Password call barring.
Pickup in group	Pickup in group.
Pickup in special	Pickup in special.
Query dial number	Query dial number.
Reject anonymous call	Reject anonymous call.
Reject call selective	Reject call selective.
Ring service	Ring service.
SCC cancel register service	SCC cancel register service.
Secretary	Secretary.
Selective call acceptance	Selective call acceptance.
Three party	Three party.
Wake call	Wake call.
Instant conference	Instant conference.
Hotline	Hotline.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
forwarding call to voice mail unconditional	Forwarding call to voice mail unconditional.
forwarding call to voice mail on busy	Forwarding call to voice mail on busy.
forwarding call to voice mail on no reply	Forwarding call to voice mail on no reply.
forwarding call to voice mail on offline	Forwarding call to voice mail on offline.
Call of multiple lines	Call of multiple lines.
Caller line name presentation	Calling Name Identification Presentation.
Called line name presentation	Connected Name Identification Presentation.

.

16.5.8.42 display voice pbxusergroup

Function

The **display voice pbxusergroup** command displays configuration information about a PBX user group.

Format

display voice pbxusergroup [*pbxusergroup-name*]

Parameters

Parameter	Description	Value
pbxusergroup-name	Specifies a PBX user group.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

If the PBX user group name is not specified, the summary of all PBX user groups is displayed. If the PBX user group name is specified, detailed configuration information about the PBX user group is displayed.

Example

View detailed configuration information about PBX user group **hunt**.

```
<Huawei> display voice pbxusergroup hunt
 PBX select group name    : hunt
 Enterprise               : default
 Dn-set                   : DefaultDialPlan
 Access telno             : 1111
 Ring mode                : Ring serial
 Ring time(s)             : 12
 Select mode              : Loop
 Master first             : Enable
 CRBT                     : Disable
 Group name               : hunt
```

Table 16-92 Description of **the display voice pbxusergroup** command output

Item	Description
PBX select group name	User group name.
Enterprise	Enterprise bound to a user group.
Dn-set	DN set bound to a user group.
Access telno	User group access code.
Ring mode	Ringing mode.
Ring time(s)	Ringing duration.
Select mode	Selective ringing mode.
Master first	Primary number preference.
CRBT	Crbt.
Group name	Group name.

View the summary of all PBX user groups.

```
<Huawei> display voice pbxusergroup
  Spec: 64, Records: 3
  --------------------------
  User group name          : hunt
  Enterprise               : default
  User group type          : hunt group

  User group name          : master
  Enterprise               : default
  User group type          : hunt group

  User group name          : selfsame
```

```
Enterprise          : default
User group type       : hunt group
```

Table 16-93 Description of the **display voice pbxusergroup** command output

Item	Description
Spec	Maximum number of users supported by the device.
Records	Current number of users on the device.
User group name	User group name.
Enterprise	Enterprise bound to a user group.
User group type	Service type of a user group. Currently, the PBX only supports the following group service: ● PBX line selection service (hunt)

16.5.8.43 display voice pickup-group

Function

The **display voice pickup-group** command displays configuration information about the current pickup group.

Format

display voice pickup-group [**pickupgroup-name** *pickupgroup-name-value*]

Parameters

Parameter	Description	Value
pickupgroup-name *pickupgroup-name-value*	Specifies a pickup group name.	The value is a string of 1 to 32 characters without spaces.

Views

Voice views

Default Level

3: Management level

Usage Guidelines

If the pickup group name is not specified, configuration information about all pickup groups is displayed.

Example

Display configuration information about the current pickup group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice pickup-group
 Pickup group name   : aaa
 Group member pbxuser: 1400
 Group member pbxuser: 1503
```

16.5.8.44 display voice ring-parallel-group

Function

The **display voice ring-parallel-group** command displays the configuration of a simultaneous ringing group of a PBX user.

Format

display voice ring-parallel-group [**pbxuser** *pbxuser-name*]

Parameters

Parameter	Description	Value
pbxuser *pbxuser-name*	Displays the configuration of a simultaneous ringing group of a specified PBX user.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

If the PBX user name is not specified, the summary of simultaneous ringing groups of all PBX users is displayed. If the PBX user name is specified, detailed information of the simultaneous ringing group of the PBX user is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the detailed configuration of a simultaneous ringing group of a PBX user.

```
<Huawei> display voice ring-parallel-group pbxuser 28980001
 Ring parallel pbxuser       : 28980001
 Ring parallel access number : 28980001
 Trigger type                : unspecified
 Group member telno          : 28980002
 Member index                : 0
```

Table 16-94 Description of the **display voice ring-parallel-group** command output

Item	Description
Ring parallel pbxuser	Name of the simultaneous ringing group.
Ring parallel access number	Number of the primary user in a user group.
Trigger type	Triggering type of a user group.
Group member pbxuser	User group member.
Member index	Index of a user group member.

16.5.8.45 display voice ring-serial-group

Function

The **display voice ring-serial-group** command displays the configuration of a sequential ringing group of a PBX user.

Format

display voice ring-serial-group [**pbxuser** *pbxuser-name*]

Parameters

Parameter	Description	Value
pbxuser *pbxuser-name*	Displays the configuration of a sequential ringing group of a specified PBX user.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

If the PBX user name is not specified, the summary of sequential ringing groups of all PBX users is displayed. If the PBX user name is specified, detailed information of the sequential ringing group of the PBX user is displayed.

Example

Display the detailed configuration of a sequential ringing group of a PBX user.

```
<Huawei> display voice ring-serial-group pbxuser 28980004
 Ring serial pbxuser          : 28980004
 Ring serial access number    : 28980004
 Trigger type                 : unspecified
 Select interval              : 20(s)
 Group member telno           : 28980003
 Member index: 0
```

Table 16-95 Description of the **display voice ring-serial-group** command output

Item	Description
Ring serial pbxuser	Name of the sequential ringing group.
Ring serial access number	Number of the primary user in a user group.
Trigger type	Triggering type of a user group.
Select interval	Ringing interval of a sequential ringing group.
Group member telno	User group member.
Member index	Index of a user group member.

16.5.8.46 display voice rule-set

Function

The **display voice rule-set** command displays the blacklist/whitelist configuration in a specified rule set or all rule sets.

Format

display voice rule-set [*rule-set-name*]

Parameters

Parameter	Description	Value
rule-set-name	Displays blacklist/whitelist configuration in a specified rule set. If this parameter is not specified, blacklist/whitelist configuration in all rule sets is displayed.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display blacklist/whitelist configuration in rule set 001.

```
<Huawei> display voice rule-set 001

 Rule-set                : 001
 Enterprise              : huawei

  Type                  : deny
  Direction               : incoming
  Call-num                : 1234
```

Table 16-96 Description of the **display voice rule-set** command output

Item	Description
Rule-set	Name of a rule set.
Enterprise	Enterprise to which the blacklist/whitelist is applied.
Type	Whether the telephone numbers are in the blacklist or whitelist. ● deny: The telephone numbers are in the blacklist. ● permit: The telephone numbers are in the whitelist.

Item	Description
Direction	Call type restricted by the blacklist/whitelist. ● incoming: The blacklist/whitelist restricts incoming calls. ● outgoing: The blacklist/whitelist restricts outgoing calls.
Call-num	Number restricted by the blacklist/whitelist.

16.5.8.47 display voice service alert-ring

Function

The **display voice service alert-ring** command displays the configuration of a specified distinctive ringing service or all distinctive ringing services.

Format

display voice service alert-ring [*alert-ring-name*]

Parameters

Parameter	Description	Value
alert-ring-name	Specifies the name of a distinctive ringing service.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the configuration of the distinctive ringing service **test**.

```
<Huawei> display voice service alert-ring test
 Service alert ring name: test
```

```
Enterprise            : huawei
Local ring ID          : 1
Domestic ring ID       : 1
International ring ID  :
```

Table 16-97 Description of the **display voice service-alert-ring** command output

Item	Description
Service alert ring name	Dialing plan of a user.
Enterprise	Enterprise that a user belongs to.
Local ring ID	Local call ring ID.
Domestic ring ID	National toll call ring ID.
International ring ID	International call ring ID.

16.5.8.48 display voice ssca-group

Function

The **display voice ssca-group** command displays information about the advanced secretary service configured on the PBX.

Format

display voice ssca-group [**pbxuser** *pbxuser-name*]

Parameters

Parameter	Description	Value
pbxuser *pbxuser-name*	Displays detailed information about members of a user group.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display information about the advanced secretary service configured on the PBX.

```
<Huawei> display voice ssca-group pbxuser 1001
boss dn: 1001
  line share mode: single
  alerting silence: disable
  auto answer mode: disable
secretary dn: 1003
  bind boss eid: 1001
  bind secretary eid: 1003
  alerting silence: disable
  auto answer mode: disable
secretary dn: 1004
  bind boss eid: 1002
  bind secretary eid: 1004
  alerting silence: disable
  auto answer mode: disable
```

16.5.8.49 display voice tone type

Function

The **display voice tone type** command displays the prompt tones on the PBX.

Format

display voice tone type

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the prompt tones on the device.

```
<Huawei> display voice tone type
-----------------------------------------------------------------
 Tone type                  Description
-----------------------------------------------------------------
  1                         Busy tone
  2                         Howl tone
  3                         Dial tone
  4                         Ring back tone
```

5	Dual dial tone
6	Special dial tone
7	Short busy tone
8	Call waiting tone
9	Mute tone
10	CAS tone
11	SAS tone
12	Voice-MWI-on tone
13	Voice-MWI-off tone
14	Confirmation tone
15	Congestion tone
16	Negative acknowledge tone
17	User-defined tone 1
18	User-defined tone 2
19	User-defined tone 3
20	User-defined tone 4
21	User-defined tone 5
22	Reserved
23	Reserved
24	Message waiting tone
25	Call waiting tone 2
26	Number unobtainable tone
27	Equipment engaged tone
28	AN: Unrecognized number
29	AN: Fault
30	AN: Number temporarily out of order
31	AN: No reply
32	AN: All lines busy
33	AN: Number unavailable
34	AN: Other party cleared
35	AN: Call cannot be connected
36	AN: Call gapping
37	AN: Incoming calls barred
38	AN: No digits
39	AN: Service termination
40	Reorder tone 1
41	Reorder tone 2
42	Call waiting tone 3
43	Call waiting tone 4
44	Call waiting tone 5
45	Stutter dial tone (PCCW)
46	Congestion tone (PCCW)
47	Number unobtainable tone (PCCW)
48	Service acceptance tone (PCCW)
49	AN: MGC overload
50	Bulgarian line lock tone
51	Argentina leave tone
52	Bulgarian SRVTN hold tone
53	Confirmation tone
54	All trunks busy tone
55	Warning tone
56	Special information tone
57	Locating tone
58	AN: Call waiting
59	Power overload tone
60	VMS: GetleaveMsg Welcome tone
61	VMS: LeaveMsg is getting
62	VMS: SPACELESS
63	VMS: You have
64	VMS: NewMsgNum
65	VMS: OldMsgNum
66	VMS: Listen old msg or new msg
67	VMS: Get msg fail
68	VMS: Listen msg type
69	VMS: Delete success
70	VMS: Delete fail
71	VMS: No welcome tone
72	VMS: Forward Msg Tone
73	VMS: Welcome Msg Operation tone

 Copyright © Huawei Technologies Co., Ltd.

74	VMS: Forward Msg fail
75	VMS: Forward Msg success
76	VMS: Record Msg coming
77	VMS: LeaveMsg full
78	VMS: LeaveMsg Operation
79	VMS: Save success
80	VMS: Save fail
81	VMS: Cancel success
82	VMS: Cancel fail
83	VMS: Record end coming
84	VMS: Di
85	VMS: Record fail tone
86	VMS: Welcome record start
87	VMS: Welcome coming
88	VMS: No vms right
89	VMS: Listen new msg
90	VMS: Listen old msg
91	VMS: Get welcome number
95	Music
101	Leave msg tone
102	Voip call restriction tone
103	Register CFU OK tone
104	Register CFB OK tone
105	Register CFNR OK tone
106	Register CFU fail tone
107	Register CFB fail tone
108	Register CFNR fail tone
110	Join conf ahead fail tone
111	Join conf as chairman fail tone
112	No response tone
113	Trunk all busy tone
114	Conf operation success tone
115	Conf operation fail tone
116	Called offline tone
117	Conf operation tone
118	CFNR redirect tone
119	CFB redirect tone
120	CFU redirect tone
121	CFO redirect tone
122	CFUMS redirect tone
133	Called billing tone
134	Callin restrict tone
135	Called not active tone
136	WakeUp tone
137	Conf calling tone
138	Call back tone
139	New service cancel tone
140	Called busy tone
141	Error Num tone
142	No disturb tone
143	Absent tone
145	New service register tone
146	New service fail tone
148	Call restriction tone
149	Malicious call success tone
151	Number changed tone
152	Leave msg notification tone
153	Leave msg cancel notification tone
154	Wrong password tone
155	Called unreachable tone
156	Called out of service tone
157	Voipmain called restriction tone
158	Call fowarding restriction tone
159	Waiting tone
160	Service not provided tone
161	Service not applied tone
162	Owned fail tone
163	Owned warning tone
165	Conf: Dial roomno tone

 Copyright © Huawei Technologies Co., Ltd.

166	Conf: Dial password tone
167	Conf: Convoke tone
168	Conf: Welcome tone
169	Conf: Chairman hooking prompt tone
170	Conf: Attendee hooking dial tone
171	Conf: Chairman hooking confirm tone
172	Conf: Attendee full tone
173	Number changed waiting tone
174	Number changed dial tone
175	3PTY hooking prompt tone
176	Callwaiting hooking prompt tone
177	NULL number tone
178	Conf: Chairman exist tone
179	Conf: Someone incoming tone
180	Conf: Someone outgoing tone
181	Busy callback egister tone
182	Input password tone
183	Input error and try again tone
184	Input error exceed and limit tone
185	Busy and No answer callback start tone
186	No answer callback register tone
187	Card service success tone
188	Card service fail tone
189	Phone binded input password tone
190	Input charge card tone
191	Input charge password tone
192	Card balance tone
193	Input new password tone
194	Card balance not enough tone
195	Card account fail tone
197	Time not enough tone
198	User suppended tone
199	System busy and dial later
200	Conf center service tone
201	No right creat instant conf
202	Conf end awoke tone
203	User is used by others tone
204	Bill full prompt tone
205	No conf resource
206	Callwaiting one release tone
208	One minute left tone
209	Transfer restrict tone
210	ThreeParty restrict tone
211	PwdLimit accout tone
212	PwdLimit password tone
213	PwdLimit callednum tone
214	PwdLimit password again tone
215	PwdLimit password set ok tone
216	Connect meeting error tone
217	Conf mute set tone
218	Conf mute cancel tone
219	Join conf welcome tone
220	Input number setted tone
221	Input forward number tone
222	Select forward type tone
223	Advsca service operate tone
224	No response callback tone
225	Chairman tone
226	Guest tone
227	Prompt annouce name tone
228	Enter conf tone
229	Leave conf tone
230	Conf record beep
231	Change CFUMS tone
232	Collect call tone
233	Joint espace busy tone
234	Invert incomming tone
235	Invert outgoing tone
236	Record start tone

 Copyright © Huawei Technologies Co., Ltd.

237	Record end tone
238	Console queue busy tone
241	128 service indicating tone
242	125 service indicating tone
250	Dial extension tone
251	Input incorrect and dial opertator tone
512	Number 0
513	Number 1
514	Number 2
515	Number 3
516	Number 4
517	Number 5
518	Number 6
519	Number 7
520	Number 8
521	Number 9
522	Number 10
523	Hour
524	Minute
525	Second
526	yuan
527	jiao
528	fen
529	Number 11
530	Number 12
531	Number 13
532	Number 14
533	Number 15
534	Number 16
535	Number 17
536	Number 18
537	Number 19
538	Number 20
539	Anonymous reject tone
541	Thanks and bye
558	New password wrong and input again
559	Password is changed success
560	Disaivr portal greeting
561	Disaivr input id
562	Disaivr input password
563	Disaivr id invalid
564	Disaivr password invalid
565	Disaivr input timeout
566	Disaivr input telephone no

Table 16-98 Description of the display voice tone type command output

Parameter	Description
1	Busy tone.
2	Howler tone.
3	Dial tone.
4	Ringback tone.
5	Two-stage dial tone.
6	Special dial tone.
7	Short busy tone.
8	Call waiting tone.
9	Mute tone.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
10	CAS tone.
11	SAS tone.
12	The MWI is on.
13	The MWI is off.
14	Confirmation tone.
15	Congestion tone.
16	Rejection tone.
17	User-defined tone 1.
18	User-defined tone 2.
19	User-defined tone 3.
20	User-defined tone 4.
21	User-defined tone 5.
22	Reserved.
23	Reserved.
24	Message leaving tone.
25	Call waiting tone 2.
26	Number unobtainable tone.
27	Equipment engaged tone.
28	The number cannot be recognized.
29	Fault.
30	The number is out of order.
31	No reply.
32	All lines are busy.
33	The number is unavailable.
34	The peer party does not exist.
35	The call cannot be connected.
36	Call gap.
37	Incoming calls are barred.
38	Non-digit.
39	The service is terminated.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
40	Part one of the RO tone.
41	Part two of the RO tone.
42	PCCW call waiting tone 3.
43	PCCW call waiting tone 4.
44	PCCW call waiting tone 5.
45	PCCW signal tone (STT).
46	PCCW signal tone (CT).
47	PCCW signal tone (NUT).
48	PCCW signal tone (SAT).
49	MGC overload tone.
50	Bulgarian line lock tone.
51	Argentina message leaving tone.
52	Call hold tone.
53	Confirmation tone.
54	All trunks are busy.
55	Warning tone.
56	Special information tone.
57	Locating tone.
58	Call waiting tone.
59	Power overload tone.
60	Greeting for retrieving messages.
61	Sorry, the messages for the user are being retrieved. Goodbye.
62	Your message space is insufficient. Please delete unnecessary messages.
63	You have.
64	Messages.
65	Old messages.
66	To listen to new messages, please press 1. To listen to old messages, please press 2.
67	Sorry, failed to retrieve the message.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
68	To listen to the next message, please press 1. To listen to the previous message, please press 2. To listen to the message again, please press 3. To forward the message, please press 4. To delete the message, please press 5. To delete all read messages, please press 6. To return, please press the star key.
69	The message is deleted.
70	Failed to delete the message.
71	Sorry, the user does not have any greetings. Goodbye.
72	Enter the user number to which you want to forward the message, and end it with the pound key.
73	To record greetings, please press 1. To delete greetings, please press 2.
74	Sorry, failed to forward the message.
75	The message is forwarded successfully.
76	Welcome to the voice message system. Leave a message when you hear the beep. To stop the recording, press any key.
77	Sorry, the message space for the user is full. Goodbye.
78	To replay the message, please press 1. To save and exit, please press 2. To leave a new message, please press 3. To cancel the message, please press 4.
79	The message is saved. Goodbye.
80	Failed to save the message. Goodbye.
81	The message is canceled. Goodbye.
82	Failed to delete or cancel the message. Goodbye.
83	Sorry, your message leaving duration is up.
84	Beep.
85	Sorry, failed to leave the message. Goodbye.
86	To set greetings for this number, please press the pound key. To set greetings for another number, please enter the number and end it with the pound key.
87	Leave a message when you hear the beep. To stop the recording, press any key.
88	Sorry, the user does not enable the message leaving right.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
89	To listen to new messages, please press 1.
90	To listen to old messages, please press 2.
91	Obtain the greeting index.
95	Music.
101	Message waiting tone.
102	VoIP call barring tone.
110	Failed to join a conference in advance.
111	Failed to join a conference as the moderator.
112	The called party does not answer the call.
113	The trunk is busy, and the call cannot be made.
114	The conference operation succeeds.
115	The conference operation fails.
116	The called party is offline.
117	Conference command operation prompt tone.
118	Sorry, the number you dialed is not answered. Your call is being transferred.
119	Sorry, the number you dialed is busy. Your call is being transferred.
120	Your call is being transferred.
121	Sorry, the number you dialed cannot be reached at this time. Your call is being transferred.
122	Your call is being transferred to the voice message system.
133	The called party pays.
134	Incoming calls are barred.
135	The called party is not activated.
136	Wake-up tone.
137	Conference calling tone.
138	Completion of calls to busy subscriber tone.
139	The new service is disabled successfully.
140	The called party is busy.
141	Wrong number tone.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
142	Do not disturb tone.
143	The called party is absent.
145	The new service is enabled successfully.
146	The new service fails.
148	The call is barred.
149	Malicious calls are identified successfully.
151	Number change tone.
152	Message leaving tone.
153	The message is canceled.
154	The password is invalid.
155	The called party is unreachable.
156	The called party encounters a fault.
157	VoIP called domain call barring tone.
158	Call forwarding is restricted.
159	Call waiting tone.
160	The service is not provided.
161	The service is not applied.
162	The called party is in arrears.
163	The calling party is in arrears.
165	Dial the conference ID.
166	Dial the conference password.
167	The conference is being set up.
168	Conference greeting.
169	Moderator hookflash prompt tone.
170	Moderator hookflash dial tone.
171	Moderator convening confirmation tone.
172	The conference is full.
173	Number change waiting tone.
174	Number change dial tone.
175	Three-party call hookflash prompt tone.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
176	Call waiting hookflash prompt tone.
177	Sorry, the number you dialed does not exist. Please dial again.
178	The moderator has joined the conference.
179	A participant joins the conference.
180	A participant leaves the conference.
181	Enter the card number.
182	Enter the card password.
183	Incorrect input. Enter a correct value.
184	Input errors exceed the maximum limit.
185	The authentication is successful. Enter the called number.
186	Prompt tone about whether authentication is required for card binding.
187	The card service operation succeeds.
188	The card service operation fails.
189	The phone is bound. Enter the card password.
190	Enter the charge card number.
191	Enter the charge card password.
192	Card balance tone.
193	Enter the new card password.
194	The card balance is insufficient.
195	The card charging fails.
197	The balance is about to be used up.
198	The user is suspended.
199	The system is busy. Please dial later.
200	Conference center service prompt tone.
201	Failed to create an instant conference.
202	The conference is about to end.
203	The phone involved in the number portability service has been used.
204	The CDR pool is full.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
205	No conference resource is available.
206	Call waiting release tone.
208	The call will be disconnected in 1 minute.
209	Call barring prompt tone in call transfer.
210	Call barring prompt tone in a three-party call.
211	The password is changed successfully.
212	Call barring password.
213	Selection prompt tone.
214	Enter the confirm password.
215	The password is changed. Press the pound key to return to the upper-level menu.
216	Failed to create a conference.
217	You are muted.
218	You are unmuted.
219	The conference is being set up. (No music, ITUC scenario)
220	Enter the number to set.
221	Enter the forwarded-to number.
222	Select the call forwarding type.
223	Select to activate or deactivate the advanced secretary service.
224	Call completion no reply.
225	Moderator.
226	Guest.
227	Participant name broadcasting tone.
228	Join a conference.
229	Leave a conference.
230	Beep tone for conference recording.
231	Forwarding call to voice mail unconditional tone.
232	The called party pays.
233	Busy connecting to eSpace.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
234	A user enters in the break-in service.
235	A user exits from the break-in service.
236	Recording starts.
237	Records ends.
238	All agents are busy.
241	128 service prompt tone.
242	125 service prompt tone.
250	Expanded dial tone.
251	Incorrect input dial tone.
512	Number 0.
513	Number 1.
514	Number 2.
515	Number 3.
516	Number 4.
517	Number 5.
518	Number 6.
519	Number 7.
520	Number 8.
521	Number 9.
522	Number 10.
523	Hour.
524	Minute.
525	Second.
526	Yuan.
527	Jiao.
528	Fen.
529	Number 11.
530	Number 12.
531	Number 13.
532	Number 14.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
533	Number 15.
534	Number 16.
535	Number 17.
536	Number 18.
537	Number 19.
538	Number 20.
539	Reject anonymous call.
541	Thank you for use. Goodbye.
558	The new password that you input is incorrect. Please input the correct one.
559	Your service password has been changed. Thank you.
560	Prompt tone when a user dials the conference access code: Welcome to the DISA system.
561	Prompt tone for entering the conference ID: Enter the account and end it with the pound key. Press the star key to reenter the conference ID.
562	Prompt tone for entering the conference password: Enter the password and end it with the pound key. Press the star key to reenter the password.
563	Prompt tone when the conference ID is incorrect: The account does not exist.
564	Prompt tone when the conference password is incorrect: The password is invalid.
565	Input timeout prompt tone: Your input times out.
566	Prompt tone for entering the telephone number: Enter the telephone number and end it with the pound key. Directly press the pound key to complete input.

16.5.8.50 display voice trunk-group trunk-circuit state brief

Function

The **display voice trunk-group trunk-circuit state brief** command displays the trunk circuit number and status in a trunk group.

Format

display voice trunk-group *trunk-group-name* **trunk-circuit state brief**

Parameters

Parameter	Description	Value
trunk-group-name	Specifies a trunk group name.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the trunk circuit information of the trunk group **sipip.**

```
<Huawei> display voice trunk-group sipip trunk-circuit status brief
 TKC under trunk group state: sipip
 -------------------------------
 TKC No  State
 2441    Fault
 2442    Fault
 2443    Fault
 2444    Fault
 2445    Fault
```

Table 16-99 Description of the display voice trunk-group sipip trunk-circuit status brief

Item	Description
TKC No	Number of TKC.
State	Status of TKC. ● Fault: Link error. ● Idle: Link Idle. ● Busy: Link busy.

16.5.8.51 display voice unicall-group

Function

The **display voice unicall-group**command displays information about the One Number Link to You (ONLY) service configured on the PBX.

Format

display voice unicall-group [**pbxuser** *pbxuser-name*]

Parameters

Parameter	Description	Value
pbxuser *pbxuser-name*	Displays detailed information about members of a user group.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display information about the ONLY service configured on the PBX.

```
<Huawei> display voice unicall-group
Unicall group name: 855001
Unicall access telno : 855001
BusySelect mode: all
Priority mode: static
Ring mode: append
Select interval: 12(s)
Bind value: 855002
Bind type: internal-no
Bind priority: 0
```

Table 16-100 Description of the display voice unicall-group command output

Item	Description
Unicall group name	Specifies the name of the ONLY service user group.
Unicall access telno	Indicates the access number for user group services.
BusySelect mode	Specifies the selection mode during busy hours for the ONLY service.
Priority mode	Priority mode.
Ring mode	Specifies the ring type for a PBX user.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Select interval	Ringing interval of a sequential ringing group.
Bind value	Specifies the number or ID of the bound terminal.
Bind type	Specifies the attribute of the bound terminal.
Bind priority	Specifies the priority of the bound terminal.

16.5.8.52 display voice vms

Function

The **display voice vms** command displays the VMS parameter configuration.

Format

display voice vms

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the VMS parameter configuration

```
<Huawei> display voice vms
 VMS parameter:
 FilePath value            :sd1:
 Max record Time           :20
 Max record Number         :10
 Space Warning number-left :1
 If entrypt                :enable
 vmsno          : 0
 callprefix value: 30
```

```
vmsno          : 1
callprefix value: 40
```

Table 16-101 Description of the **display voice vms** command output

Item	Description
FilePath value	Path of the file.
Max record Time	-
Max record Number	-
Space Warning number-left	-
If entrypt	Whether to support encryption. By default, encryption is not supported.
vmsno	VMS email number.
callprefix value	Call prefix.

16.5.8.53 dn-set (PBX user group view)

Function

Using the **dn-set** command, you can configure a DN set for PBX user group.

Using the **undo dn-set** command, you can delete a DN set for PBX user group.

By default, PBX use group use the default DN set **defaultdiaplan**.

Format

dn-set *dn-set-name*

undo dn-set

Parameters

Parameter	Description	Value
dn-set-name	Specifies the name of a DN set.	The value is a string of 1 to 32 characters without spaces.

Views

PBX user group view

Default Level

2: Configuration level

Usage Guidelines

A DN set is a collection of prefixes that all users on the PSTN can dial. Before configuring a DN set to which user group belongs, run the **dn-set (enterprise view)** command to create a DN set.

Example

Set the DN set to **user001** for PBX users.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] dn-set user001
```

16.5.8.54 enterprise (calling number change view)

Function

The **enterprise** command specifies the enterprise and DN set in a calling number change plan.

The **undo enterprise** command restores the default enterprise and DN set in a calling number change plan.

Format

enterprise *enterprise-name* [**dn-set** *dn-set-name*]

Parameters

Parameter	Description	Value
enterprise-name	Specifies the name of an enterprise.	The value is a string of 1 to 32 characters.
dn-set *dn-set-name*	Specifies the name of a DN set.	The value is a string of 1 to 32 characters.

Views

Calling number change view

Default Level

2: Configuration level

Usage Guidelines

The **enterprise** command specifies the enterprise and DN set in a calling number change plan.

Example

In the calling number change plan, set the enterprise and DN set to abcd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change test
[Huawei-voice-caller-change-test] enterprise huawei dn-set abcd
```

16.5.8.55 enterprise (distinctive ringing service view)

Function

The **enterprise** command binds an enterprise to the distinctive ringing service.

The **undo enterprise** command unbinds an enterprise from the distinctive ringing service.

Format

enterprise *enterprise-name*

undo enterprise

Parameters

Parameter	Description	Value
enterprise-name	Specifies the enterprise name.	The value is a string of 1 to 32 characters.

Views

Distinctive ringing service view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Bind the enterprise **abcd** to the distinctive ringing service **test**.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] service alert-ring test
[Huawei-voice-service-alert-ring-test] enterprise abcd
```

16.5.8.56 enterprise (number map view)

Function

The **enterprise** command configures an enterprise for number mapping.

The **undo enterprise** command restores the default enterprise for number mapping.

Format

enterprise *enterprise-name*

undo enterprise

Parameters

Parameter	Description	Value
enterprise-name	Specifies an enterprise name.	The value is a string of 1 to 32 characters without spaces.

Views

Number Map view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure enterprise **ab** for number mapping.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] number-map test
[Huawei-voice-number-map-test] internal-num 1000
[Huawei-voice-number-map-test] external-num 05711000
[Huawei-voice-number-map-test] enterprise ab
```

16.5.8.57 enterprise (rule-set view)

Function

The **enterprise** command binds an enterprise to a rule set (blacklist or whitelist).

The **undo enterprise** command restores the default enterprise bound to the rule set.

By default, enterprise **default** is bound to a rule set.

Format

enterprise *enterprise-name*

undo enterprise

Parameters

Parameter	Description	Value
enterprise-name	Specifies the name of an enterprise.	The value is a string of 1 to 32 characters.

Views

Rule-set view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Bind enterprise **abcd** to rule set 100.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] rule-set 100
[Huawei-voice-rule-set-100] enterprise abcd
```

16.5.8.58 external-num

Function

The **external-num** command configures an external number for number mapping.

Format

external-num *external-num*

Parameters

Parameter	Description	Value
external-num	Specifies an external number.	The value is a string of 1 to 32 characters without spaces.

Views

Number Map view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure an external number for number mapping.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] number-map test
[Huawei-voice-number-map-test] internal-num 1000
[Huawei-voice-number-map-test] external-num 05711000
```

16.5.8.59 forward-condition

Function

The **forward-condition** command configures the conditions for conditional forwarding.

undo forward-condition delete conditions for conditional forwarding.

Format

forward-condition id *id-value* **forwardnum** *forwardnum-value* [**umsno** *umsno-value*] **state** *state-value* [**caller-telno** *caller-telno-value*] [**call-attribute** *call-attribute-value*] [**weekly** *weekly-walue*] [*begin-time*] [*end-time*]

undo forward-condition id *id-value*

Parameters

Parameter	Description	Value
id *id-value*	Indicates the index value.	The value is an integer that ranges from 0 to 9.

Parameter	Description	Value
forwardnum *forwardnum-value*	Indicates the forward-to number	The value is a string of 1 to 24 characters.
umsno *umsno-value*	ums no	The value is an integer that ranges from 0 to 254.
state *state-value*	Indicates the user status.	Enumerated type. The values can be any, busy, noanswer, offline, or donotdisturb.
caller-telno *caller-telno-value*	Indicates the calling number.	The value is an integer that ranges from 1 to 32.
call-attribute *call-attribute-value*	Indicates the call attribute. Enumerated type.	The values can be **internal** or **external**.
weekly *weekly-walue*	Enumerated type.	The values can be **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, or **Sun**.
begin-time	Indicates the start time.	The value is a time.
end-time	Indicates the end time.	The value is a time.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

You need to run this command to configure the conditions before you run the **service cfc condition** command to configure conditional forwarding.

Example

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] forward-condition id 1 forwardnum 55001122 state any weekly Mon
11:00:00 12:00:00
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.60 full-number (GNR view)

Function

The **full-number** command configures full number under GNR number.

The **undo full-number** command deletes full number under GNR number.

Format

full-number *full-number-value* [**number** *number-value* **steplen** *steplen-value*]

undo full-number *full-number-value*

Parameters

Parameter	Description	Value
full-number-value	Indicates the full number.	The value is a string of 1 to 32 characters without spaces.
number *number-value*	Indicates the number of full numbers when multiple full numbers are configured.	The value ranges from 1 to 50.
steplen *steplen-value*	Indicates the step between two full number which is multiple configured.	The value ranges from 1 to 65535.

Views

GNR view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure full number 0687411000 under GNR 068741.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]gnr-number 068741
[Huawei-voice-gnrnumber-068741]full-number 0687411000
```

Batch config full number under GNR 068741, the full number is start with 0687411001, configure number 5, step length 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]gnr-number 068741
[Huawei-voice-gnrnumber-068741] full-number 0687411000 number 5 steplen 2
```

16.5.8.61 gnr-number (voice view)

Function

Command **gnr-number** is used to config GNR number.

Command **undo gnr-number** is used to delete GNR number.

Format

gnr-number *gnr-number-value*

undo gnr-number *gnr-number-value*

Parameters

Parameter	Description	Value
gnr-number-value	GNR number.	The value is a number string of 1 to 32 characters without spaces.

Views

voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Config GNR number 068741.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]gnr-number 068741
```

16.5.8.62 group-member

Function

The **group-member** command configures members for a group.

The **undo group-member** command deletes members from a group.

By default, no group member is configured.

Format

group-member { **pbxuser** *pbxuser-name* | **external-telno** *external-telno-value* } [**condition** { **time-period** { **from** *from-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **time-repeat** { { **yearly** | **monthly** } *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] } } *] [**admin-state** *admin-state-value*] [**member-index** *member-index-value*]

undo group-member { **pbxuser** *pbxuser-name* | **external-telno** *external-telno-value* } [**condition** { **time-period** { **from** *from-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **time-repeat** { { **yearly** | **monthly** } *begin-date* [*begin-time*] [**end-date** [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] } } *]

Parameters

Parameter	Description	Value
pbxuser *pbxuser-name*	Indicates the name of a group member specified as an intra-office user.	The value is a string of 1 to 32 case-insensitive characters without spaces.
external-telno *external-telno-value*	Indicates the name of a group member specified as an outer-office number.	The value is a string of 1 to 32 digits without spaces.
condition	Specifies the time period condition.	-
time-period	Specifies the validity period.	-
from *from-date*	Specifies the validity date.	The format is year-month-day. The default value is 1970-01-01.
from-time	Specifies the validity time.	The format is hour:minute:second. The default value is 00:00:00.

Parameter	Description	Value
to *to-date*	Specifies the expiration date.	The format is year-month-day. The default value is 2100-12-31.
to-time	Specifies the expiration time.	The format is hour:minute:second. The default value is 23:59:59.
time-repeat	Indicates the repeat mode.	-
yearly	Indicates that a group member takes effect every year.	-
monthly	Indicates that a group member takes effect every month.	-
begin-date	Specifies the start date of the validity period.	The format is year-month-day. The default value is the same as the value of *from-date*.
end-date	Specifies the end date of the validity period.	The format is year-month-day. The default value is the same as the value of *to-date*.
begin-time	Specifies the start time of the validity period.	The format is hour:minute:second. The default value is 00:00:00.
end-time	Specifies the end time of the validity period.	The format is hour:minute:second. The default value is 23:59:59.
weekly	Indicates that a group member takes effect every week.	-
begin-weekday	Specifies the start day of the validity period.	Enumerated type. The value can be **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, or **sun**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-weekday	Specifies the end day of the validity period.	Enumerated type. The value can be **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, or **sun**.
daily	Indicates that a group member takes effect every day.	-
admin-state admin-state-value	Specifies the administrative status.	Enumerated type. The value can be **off-line**, **on-line**.
member-index member-index-value	Specifies the member index.	The value is an integer, and the value range depends on the device specification.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In some services, the system connects calls to different group members at different time. For example, the system needs to connect calls to different telephone operators at different time because the telephone operators have different on-duty and off-duty time. You can configure a time period condition for each group member by configuring the **condition** parameter to meet the requirement.

The following are two time period conditions.

time-period: A group member takes effect within the time range specified by **from** and **to**.

time-repeat: A group member takes effect within a specified time period every year, month, week, or day as configured. You can configure the **time-period** parameter to specify a time range in which the repeat mode takes effect.

Precautions

Run the **external-telno** *external-telno-value* command to specify members of a group as outer-office numbers. The specified numbers must be different from intra-office numbers and access codes.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the group member **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] group-member pbxuser test
```

16.5.8.63 group-member (simultaneous ringing user group view and sequential ringing user group view)

Function

The **group-member** command configures a member number in a group.

Format

group-member telno *telno-value* [**member-index** *member-index-value*]

undo group-member telno *telno-value*

Parameters

Parameter	Description	Value
telno *telno-value*	Specifies the number of a member.	The value is a string of 1 to 32 characters.
member-index *member-index-value*	Specifies the index of a member.	The value is an integer that ranges from 0 to 9.

Views

Simultaneous ringing user group view and sequential ringing user group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the number to 28980002 and index to 1 for a member in simultaneous ringing group 28980001.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring-parallel-group telno 28980001
[Huawei-voice-ring-parallel-group-28980001] group-member telno 28980002 member-index 1
```

16.5.8.64 group-name

Function

The **group-name** command configures the name of a user group.

The **undo group-name** command deletes the name of a user group.

By default, the name of a user group name is not configured.

Format

group-name *group-name-value*

undo group-name

Parameters

Parameter	Description	Value
group-name-value	Specifies the name of a user group.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **group-name** command in the user group view to configure the name of a user group for the CNOP service. When a user calls the intra-office user group, the configured name of the user group is displayed to the calling user.

Prerequisite

A user group has been created and the access code has been configured.

Example

Set the name of a user group to **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 1001
[Huawei-voice-pbxusergroup-test] group-name test
```

16.5.8.65 If-encrypt

Function

The **If-encrypt** command configures whether to encrypt recording files.

The **undo If-encrypt** command restores the default configuration.

Format

If-encrypt *if-encrypt-value*

undo If-encrypt

Parameters

Parameter	Description	Value
if-encrypt-value	Indicates whether to encrypt recording files.	Enumerated type. The options are as follows: ● disable: Recording files are not encrypted. ● enable: Recording files are encrypted. default value: disable

Views

VMS view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the device not to encrypt recording files.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] vms
[Huawei-voice-vms] If-encrypt disable
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.66 internal-num

Function

internal-num configures an internal number for number mapping.

Format

internal-num *internal-num*

Parameters

Parameter	Description	Value
internal-num	Specifies an internal number.	The value is a string of 1 to 32 characters without spaces.

Views

Number Map view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure an internal number for number mapping.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] number-map test
[Huawei-voice-number-map-test] internal-num 1000
```

16.5.8.67 ivr-voice-file

Function

The **ivr-voice-file** command specifies an IVR file for the IVR service.

The **undo ivr-voice-file** command deletes an IVR file of the IVR service

Format

ivr-voice-file voice-type *type* **file-name** *file-name-value*

undo ivr-voice-file file-name *file-name-value*

Parameters

Parameter	Description	Value
voice-type *type*	Specifies the type of an IVR file.	Enumerated type. The value is **welcome**, **menu**.
file-name *file-name-value*	Specifies the name of an IVR file.	The value is a string of 1 to 64 characters, in the format of path:/file-name, for example, flash:/test.wav.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the IVR file **test.wav** for the IVR service.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ivr-voice-file voice-type welcome file-name flash:/test.wav
```

16.5.8.68 line-share-mode (service view for the senior manager's secretary)

Function

The **line-share-mode** command changes the line sharing mode for the service for the senior manager's secretary.

Format

line-share-mode *line-share-mode-value*

Parameters

Parameter	Description	Value
line-share-mode-value	Specifies a line sharing mode.	Enumerated type. The value is: ● all ● single By default, the value is single.

Views

Service view for the senior manager's secretary view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the line sharing mode to **all** for user 1001's secretary.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ssca-group pbxuser 1001
[Huawei-ssca-group-1001] line-share-mode all
```

16.5.8.69 master-first

Function

The **master-first** command enables or disables the primary number preference rule.

The **undo master-first** command restores the default setting of the primary number preference rule.

Format

master-first *master-first-value*

undo master-first

Parameters

Parameter	Description	Value
master-first-value	Indicates whether to enable the primary number preference rule.	The value can be **disable** or **enable**. ● enable: Enable the primary number preference rule. ● disable: Disable the primary number preference rule. The default value is enable.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

The access code must be the same as a member number.

Example

Enables the primary number preference rule.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] master-first enable
```

16.5.8.70 max-record-num

Function

The **max-record-num** command sets the maximum number of leave messages for each user.

The **undo max-record-nums** command restores the default maximum number of leave messages for each user.

Format

max-record-num *max-record-num-value*

undo max-record-num

Parameters

Parameter	Description	Value
max-record-num-value	Specifies the maximum number of leave messages for each user.	The value is an integer that ranges from 0 to 20. The default value is 20.

Views

VMS view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set a maximum number of five leave messages for each user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] vms
[Huawei-voice-vms] max-record-num 10
```

16.5.8.71 max-record-time

Function

The **max-record-time** command sets the maximum duration of each leave message.

The **undo max-record-time** command restores the default maximum duration of each leave message.

Format

max-record-time *max-record-time-value*

undo max-record-time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
max-record-time-value	Specifies the maximum duration of each leave message.	The value is an integer that ranges from 1 to 120, in seconds. The default value is 120.

Views

VMS view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the maximum duration of each leave message to 100s

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] vms
[Huawei-voice-vms] max-record-time 100
```

16.5.8.72 new-callsource (calling number change view)

Function

The **new-callsource** command configures a call source in a calling number change plan.

Format

new-callsource *new-callsource-name*

Parameters

Parameter	Description	Value
new-callsource-name	Specifies a call source.	The value is a string of 1 to 32 characters.

Views

Calling number change view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **new-callsource** command configures a call source in a calling number change plan.

Example

Set the call source to **new-test** for calling number 800

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change test
[Huawei-voice-caller-change-test] callerprefix 800
[Huawei-voice-caller-change-test] new-callsource new-test
```

16.5.8.73 number-map

Function

The **number-map** command configures a number mapping view.

The **undo number-map** command deletes a configured number mapping view.

Format

number-map *number-map-name*

undo number-map *number-map-name*

Parameters

Parameter	Description	Value
number-map-name	Specifies the name of a number mapping view.	The value is a string of 1 to 32 characters without spaces.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure a number mapping

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] number-map test
```

16.5.8.74 out-ddd-ring-id

Function

Using the **out-idd-ring-id** command, you can configure the national toll call ring tone ID for the distinctive ringing service.

Format

out-ddd-ring-id *out-ddd-ring-id-value*

Parameters

Parameter	Description	Value
out-ddd-ring-id-value	Specifies the national toll call ring ID.	The value is an integer that ranges from 0 to 15.

Views

Distinctive ringing service view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the national toll call ring tone ID to 3 for the distinctive ringing service **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service alert-ring test
[Huawei-voice-service-alert-ring-test] out-ddd-ring-id 3
```

16.5.8.75 out-idd-ring-id

Function

Using the **out-idd-ring-id** command, you can configure the international call ring tone ID for the distinctive ringing service.

 Copyright © Huawei Technologies Co., Ltd.

Format

out-idd-ring-id *out-idd-ring-id-value*

Parameters

Parameter	Description	Value
out-idd-ring-id-value	Specifies the international call ring ID.	The value is an integer that ranges from 0 to 15.

Views

Distinctive ringing service view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the international call ring tone ID to 4 for the distinctive ringing service **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service alert-ring test
[Huawei-voice-service-alert-ring-test] out-idd-ring-id 4
```

16.5.8.76 out-inter-ring-id

Function

Using the **out-inter-ring-id** command, you can configure the internal call ring tone ID for the distinctive ringing service.

Format

out-inter-ring-id *out-inter-ring-id-value*

Parameters

Parameter	Description	Value
out-inter-ring-id-value	Specifies the internal call ring ID.	The value is an integer that ranges from 0 to 15.

 Copyright © Huawei Technologies Co., Ltd.

Views

Distinctive ringing service view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the internal call ring tone ID to 4 for the distinctive ringing service **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service alert-ring test
[Huawei-voice-service-alert-ring-test] out-inter-ring-id 4
```

16.5.8.77 out-local-ring-id

Function

Using the **out-local-ring-id** command, you can configure the local call ring tone ID for the distinctive ringing service.

Format

out-local-ring-id *out-local-ring-id-value*

Parameters

Parameter	Description	Value
out-local-ring-id-value	Specifies the local call ring ID.	The value is an integer that ranges from 0 to 15.

Views

Distinctive ringing service view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the local call ring tone ID to 2 for the distinctive ringing service **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service alert-ring test
[Huawei-voice-service-alert-ring-test] out-local-ring-id 2
```

16.5.8.78 outgoing-right (calling number change view)

Function

The **outgoing-right** command configures the call-out right matching a prefix of a calling party.

The **outgoing-right** command cancels the call-out right matching a prefix of a calling party.

Format

outgoing-right { { **inter** *inter-value* | **local** *local-value* | **ddd** *ddd-value* | **idd** *idd-value*} * | **all** }

undo outgoing-right [**inter** | **local** | **ddd** | **idd**]

Parameters

Parameter	Description	Value
inter *inter-value*	Specifies the intra-office right.	Enumerated value. The value can be enable or disable. The default value is enable.
local *local-value*	Specifies the local call right.	Enumerated value. The value can be enable or disable. The default value is enable.
ddd *ddd-value*	Specifies the national toll call right.	Enumerated value. The value can be enable or disable. The default value is disable.
idd *idd-value*	Specifies the international toll call right.	Enumerated value. The value can be enable or disable. The default value is disable.

Views

Calling number change view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the international toll call right matching prefix 200*.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] caller-change test
[Huawei-voice-caller-change-test] callerprefix 200*
[Huawei-voice-caller-change-test] outgoing-right idd enable
```

16.5.8.79 pbxusergroup

Function

The **pbxusergroup** command creates a user group view, enters the user group view, and specifies a group service type.

The **undo pbxusergroup** command deletes a created user group.

Format

pbxusergroup *user-group-name* [**hunt** [**enterprise** *enterprise-name*]]

undo pbxusergroup *user-group-name*

Parameters

Parameter	Description	Value
user-group-name	Specifies the name of a user group.	The value is a string of 1 to 32 characters.
hunt	Indicates a PBX line selection group.	-
enterprise *enterprise-name*	Specifies the name of an enterprise to which the user group belongs.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You must specify a service type when creating a group service. Currently, PBX users support the following services:

PBX line selection (hunt)

Example

Create a sequential ringing group test and set its service type to ring-serial

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
```

16.5.8.80 prioritymode (service user group view)

Function

The **prioritymode** command configures the terminal priority mode for the ONLY service.

The **undo prioritymode** command restores the default terminal priority mode for the ONLY service.

Format

prioritymode prioritymode-*value*

undo prioritymode

Parameters

Parameter	Description	Value
prioritymode-*value*	Specifies the terminal priority mode of the ONLY service.	Enumerated type. The options are as follows: ● dynamic: Terminal priorities are dynamically adjusted. The priority of the user who picks up the last time becomes the highest. ● static: Terminal priorities remain unchanged. the default value is static

Views

service user group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the terminal priority mode of the ONLY service user group **28980004** to **dynamic**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]unicall-group pbxuser 28980004
[Huawei-voice-unicall-group-28980004]prioritymode dynamic
```

16.5.8.81 ring (user group view)

Function

The **ring** command configures the ringing duration, ringing mode, and line selection mode of a PBX group.

The **undo ring** command restores default values of the ringing duration, ringing mode, and line selection mode of a PBX group.

By default, the ringing duration is 12s, ringing mode is **ring-serial**, and line selection mode is **loop**.

Format

ring { **mode** *ring-mode-value* | **time** *ring-time-value* | **select** *select-mode-value* }

undo ring [**mode** | **time** | **select**]

Parameters

Parameter	Description	Value
mode *ring-mode-value*	Specifies the ringing mode of a PBX group.	The values are as follows: ● ring-parallel: indicates simultaneous ringing. ● ring-serial: indicates sequential ringing. ● ring-one: indicates that only one phone rings. ● ring-circline: indicates cyclic ringing.
time *ring-time-value*	Specifies the ringing duration of a PBX group.	The value is an integer that ranges from 1 to 255, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
select *select-mode-value*	Specifies the line selection mode of a PBX group.	Enumerated value. The options are as follows: ● loop: Lines are selected in polling mode. ● increase: Lines are selected in ascending order of line IDs. ● decrease: Lines are selected in descending order of line IDs.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Run the **ring** command to configure the ringing duration, ringing mode, and line selection mode of a PBX group.

Example

Configure the ringing mode of the PBX group named test as **ring-one**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] ring mode ring-one
```

16.5.8.82 ring-parallel-group

Function

The **ring-parallel-group** command creates a simultaneous ringing group and displays the simultaneous ringing group view.

Format

ring-parallel-group pbxuser *ring-service-pbxuser-name*

undo ring-parallel-group pbxuser *ring-service-pbxuser-name*

Parameters

Parameter	Description	Value
ring-service-pbxuser-name	Specifies the name of a simultaneous ringing group.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

To configure a simultaneous ringing group for a PBX user, the PBX user must have the ringing service right.

Example

Create simultaneous ringing group 28980001.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring-parallel-group pbxuser 28980001
[Huawei-voice-ring-parallel-group-28980001]
```

16.5.8.83 ring-serial-group

Function

The **ring-serial-group** command creates a sequential ringing group and displays the sequential ringing group view.

The **undo ring-serial-group** command deletes a sequential ringing group.

Format

ring-serial-group pbxuser *ring-service-pbxuser-name*

undo ring-serial-group pbxuser *ring-service-pbxuser-name*

Parameters

Parameter	Description	Value
ring-service-pbxuser-name	Specifies the name of a sequential ringing group.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

To configure a sequential ringing group for a PBX user, the PBX user must have the ringing service right.

Example

Create sequential ringing group 28980001.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring-serial-group pbxuser 28980001
[Huawei-voice-ring-serial-group-28980001]
```

16.5.8.84 ringmode (service user group view)

Function

The **ringmode** command configures the terminal ringing mode for the ONLY service.

The **undo ringmode** command restores the default terminal ringing mode for the ONLY service.

Format

ringmode ringmode-*value*

undo ringmode

Parameters

Parameter	Description	Value
ringmode-value	Specifies the terminal ringing mode of the ONLY service.	Enumerated type. The values are as follows: ● alter: When the terminal with a lower priority begins to ring, the terminal with a higher priority stops ringing. ● append: When the terminal with a lower priority begins to ring, the terminal with a higher priority keeps on ringing. ● the default value is append

Views

service user group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the terminal ringing mode of the ONLY service user group **28980004** to **alter**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]unicall-group pbxuser 28980004
[Huawei-voice-unicall-group-28980004]ringmode alter
```

16.5.8.85 rule caller-telno called-telno

Function

The **rule caller-telno called-telno** command adds specified phone numbers to the blacklist or whitelist and sets the type of calls restricted by the blacklist or whitelist.

The **undo rule caller-telno called-telno** command cancels the whitelist/blacklist configuration.

Format

rule { **deny** | **permit** } { **incoming** | **outgoing** } { **caller-telno** *caller-telno-value* | **called-telno** *called-telno-value* }

undo rule { **deny** | **permit** } { **incoming** | **outgoing** } { **caller-telno** *caller-telno-value* | **called-telno** *called-telno-value* }

Parameters

Parameter	Description	Value
deny	Adds specified numbers to the blacklist.	-
permit	Adds specified numbers to the whitelist.	-
incoming	Restricts incoming calls made from the specified numbers.	-
outgoing	Restricts outgoing calls made from the specified numbers.	-
caller-telno-value	Specifies the calling number to be restricted. Wildcards of asterisk (*), X, and x are supported. An asterisk (*) indicates a number segment, and x or X indicates a digit.	The value is a string of 1 to 32 characters.
called-telno-value	Specifies the called number to be restricted. Wildcards of asterisk (*), X, and x are supported. An asterisk (*) indicates a number segment, and x or X indicates a digit.	The value is a string of 1 to 32 characters.

Views

Rule-set view

Default Level

2: Configuration level

Usage Guidelines

When an enterprise allows only some users to make calls through trunks, configure a rule set on the PBX to implement the blacklist or whitelist function.

 Copyright © Huawei Technologies Co., Ltd.

Example

Add number 8888 to the blacklist to restrict incoming calls from this number.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] rule-set 001
[Huawei-voice-rule-set-001] rule deny incoming caller-telno 8888
```

16.5.8.86 rule disconnect-cause incoming

Function

The **rule disconnect-cause incoming** command is used to configure the cause code that is returned when an incoming call is blocked by the blacklist.

The **undo rule disconnect-cause incoming** command is used to restore the default cause code returned when an incoming call is blocked by the blacklist.

By default, the error **code call reject** is returned when an incoming call is blocked by the blacklist.

Format

rule disconnect-cause incoming *disconnect-cause-value*

undo disconnect-cause incoming

Parameters

Parameter	Description	Value
disconnect-cause-value	Specifies the cause code that is returned when an incoming call is blocked by the blacklist.	Enumerated type. The options are **call-reject**, **invalid-number**, **unassigned-number**, and **user-busy**.

Views

Rule-set view

Default Level

2: Configuration level

Usage Guidelines

If the enterprise wants to return a specific cause value to the peer end rather than the default call-reject, you can run the **rule disconnect-cause incoming** command to configure the cause value.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the cause code to **user-busy** when the incoming call is blocked by the blacklist.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] rule-set 001
[Huawei-voice-rule-set-001] rule disconnect-cause incoming user-busy
```

16.5.8.87 rule-set

Function

The **rule-set** command configures a rule set to implement the blacklist or whitelist function.

The **undo rule-set** command deletes a rule set.

Format

rule-set *rule-set-name*

undo rule-set *rule-set-name*

Parameters

Parameter	Description	Value
rule-set-name	Specifies the name of a rule set.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When an enterprise allows only some users to make calls through trunks, configure a rule set on the PBX to implement the blacklist or whitelist function.

Example

Create a rule set 001.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] rule-set 001
[Huawei-voice-rule-set-001]
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.88 selectinterval (ONLY group view)

Function

The **selectinterval** command configures the interval for two neighboring terminals to ring.

Format

selectinterval *selectinterval-value*

Parameters

Parameter	Description	Value
selectinterval-value	Specifies **the interval for two neighboring terminals to ring.**	The value is an integer that ranges from 5 to 30. The default value is 12.

Views

ONLY group view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the interval for two neighboring terminals to ring to 15.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]unicall-group pbxuser 28980004
[Huawei-voice-unicall-group-28980004]selectinterval 15
```

16.5.8.89 selectinterval (service group view)

Function

The **selectinterval** command configures the interval at which two terminals with continuous priorities begin to ring.

The **undo selectinterval** command restores the default interval at which two terminals with continuous priorities begin to ring.

 Copyright © Huawei Technologies Co., Ltd.

Format

selectinterval selectinterval-*value*

undo selectinterval

Parameters

Parameter	Description	Value
selectinterval-*value*	Specifies the interval at which two terminals with continuous priorities begin to ring.	• The value is an integer that ranges from 5 to 30. The default value is 12.

Views

service user group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the ringing interval of the sequential ringing group **28980004** to 15 seconds.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]unicall-group pbxuser 28980004
[Huawei-voice-unicall-group-28980004]selectinterval 15
```

16.5.8.90 service abbdial

Function

Using the **service abbdial** command, you can create an abbreviated dialing service.

Using the **undo service abbdial** command, you can delete an abbreviated dialing service.

By default, no abbreviated dialing service is configured.

Format

service abbdial *abb-telno called-telno*

undo service abbdial [*abb-telno*]

Parameters

Parameter	Description	Value
abb-telno	Specifies the abbreviated code.	The value is an integer that ranges from 00 to 99.
called-telno	Specifies the original number corresponding to the abbreviated code.	The value is a string of 1 to 24 numeral characters.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Before using the **service abbdial** command, run the **service-right abbdial enable** command in the PBX user view to enable the abbreviated dialing service.

The abbreviated dialing service allows a user to initiate a call by dialing the 2-digit abbreviated code instead of the original called number.

Example

Set the abbreviated code corresponding to 55001122 to 01.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service abbdial 01 55001122
```

16.5.8.91 service alert-ring

Function

Using the **service alert-ring** command, you can create a distinctive ringing service plan and enter the distinctive ringing service plan view.

Using the **undo service alert-ring** command, you can delete the configured distinctive ringing service plan.

By default, no distinctive ringing service plan is configured.

Format

service alert-ring *alert-ring-name*

undo service alert-ring *alert-ring-name*

Parameters

Parameter	Description	Value
alert-ring-name	Specifies the name of a distinctive ringing service plan.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create a distinctive ringing service plan named **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] service alert-ring test
[Huawei-voice-service-alert-ring-test]
```

16.5.8.92 service cba

Function

Using the **service cba** command, you can create a call-out restriction service scheme.

Using the **undo service cba** command, you can delete a call-out restriction service scheme.

By default, no call-out restriction service scheme is configured.

Format

service cba *cba-value*

undo service cba

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cba-value	Restricts type.	Enumerated type. The options are as follows: • all: Restricts the outgoing calls • IDD_DDD: Restricts outgoing international and national toll calls. • IDD: Restricts outgoing international toll calls.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

You can restrict some outgoing calls of a phone, for example, toll calls.

Before using the **service cba** command, run the **service-right cba enable** command in the PBX user view to enable the call-out restriction service.

Example

Create a call-out restriction service scheme **cba-center**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service cba IDD
```

16.5.8.93 service cfb

Function

The **service cfb** command configures a CFB forward-to number.

The **undo service cfb** command deletes the configured CFB forward-to number.

By default, the CFB forward-to number is not configured.

Format

service cfb *fwd-telno*

undo service cfb

Parameters

Parameter	Description	Value
fwd-telno	Specifies a forwarded-to number.	The value is an integer that ranges from 1 to 24.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Incoming calls of a CFB user are forwarded to a preset number when the user line is busy.

Before using the **service cfb** command, run the **service-right cfb enable** command in the PBX user view to enable the CFB service.

Example

Set the forward-to number to 55001133 when the user line is busy.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service cfb 55001133
```

16.5.8.94 service cfc

Function

The **service cfc condition** command configures call forwarding conditional (CFC) conditions.

The **undo service cfc condition** command cancels CFC conditions.

By default, CFC conditions are not configured.

Format

service cfc condition *id1/id2*

undo service cfc condition

Parameters

Parameter	Description	Value
id1/id2..	Specifies CFC conditions, which must be preconfigured.	The value is a string of 1 to 19 characters.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The CFC service allows the AR to forward all incoming calls to another phone number according to CFC conditions.

Before using the **service cfc condition** command, run the **service-right cfcf enable** command in the PBX user view to enable the CFC service.

Example

Configure the CFC conditions.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] forward-condition id 1 forwardnum 55001122 state any
[Huawei-voice-pbxuser-test] forward-condition id 2 forwardnum 55001123 state any
[Huawei-voice-pbxuser-test] service cfc condition 1/2
```

16.5.8.95 service cfnr

Function

The **service cfnr** command configures a CFNR forward-to number.

The **undo service cfnr** command deletes the configured CFNR forward-to number.

By default, the CFNR forward-to number is not configured.

Format

service cfnr { **telno** *fwd-telno* | *time* **telno** *fwd-telno* }

undo service cfnr

Parameters

Parameter	Description	Value
fwd-telno	Specifies a forward-to number.	The value is an integer that ranges from 1 to 24.
time	Specifies the CFNR delay.	The value is an integer that ranges from 5 to 55, in seconds. The default value is 30.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Incoming calls of a CFNR user are forwarded to a preset number when the user does not answer the call.

Before using the **service cfnr** command, run the **service-right cfnr enable** command in the PBX user view to enable the CFNR service.

Example

Set the forward-to number to 55001155 and the CFNR delay to 30s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service cfnr 30 55001155
```

16.5.8.96 service cfnr (user group view)

Function

The **service cfnr** command specifies a CFNR forwarded-to number for all users in a user group.

The **undo service cfnr** command cancels the CFNR forwarded-to number for all users in a user group.

By default, no CFNR forwarded-to number is specified.

Format

service cfnr [*time*] **telno** *fwd-telno*

undo service cfnr

Parameters

Parameter	Description	Value
time	Specifies the waiting time when no response is receive.	The value is an integer that ranges from 5 to 55, in seconds. By default, the value is 30s.
telno *fwd-telno*	Specifies a CFNR forwarded-to number.	The value is a string of 1 to 24 digits without spaces.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Call Forwarding No Reply(CFNR) service: indicates that incoming calls of a CFNR user are forwarded to a preset number when all users of the user group do not answer the call.

Prerequisite

A user group has been created and the access code has been configured.

Precautions

The configuration takes effect only when simultaneous ringing is configured for a user group. You can run the **ring mode** *ring-mode-value* command to configure the ringing mode, and set the *ring-mode-value* parameter to **ring-parallel**.

Example

Set the forwarded-to number to 55001155 and the waiting time to 40s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 1001
[Huawei-voice-pbxusergroup-test] service cfnr 40 telno 55001155
```

16.5.8.97 service cfo

Function

The **service cfo** command configures a CFO forward-to number.

The **undo service cfo** command deletes the CFO forward-to number.

By default, the CFO forward-to number is not configured.

Format

service cfo *fwd-telno*

undo service cfo

Parameters

Parameter	Description	Value
fwd-telno	Specifies a forward-to number.	The value is an integer that ranges from 1 to 24.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Incoming calls of a CFO user are forwarded to a preset number when the user is offline.

NOTE

If a user does not initiate registration update after registration expires, the device sets the user status to offline.

Before using the **service cfo** command, run the **service-right cfo enable** command in the PBX user view to enable the CFO service.

Example

Set the forward-to number to 55001144 when the user line is offline.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service cfo 55001144
```

16.5.8.98 service cfo (user group view)

Function

The **service cfo** command specifies a CFO forwarded-to number for users in a user group.

The **undo service cfo** command cancels the CFO forwarded-to number for users in a user group.

By default, no CFO forwarded-to number is specified.

Format

service cfo *fwd-telno*

undo service cfo

Parameters

Parameter	Description	Value
fwd-telno	Specifies a CFO forwarded-to number.	The value is a string of 1 to 24 digits without spaces.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Call Forwarding Offline (CFO) service: indicates that incoming calls of a CFO user are forwarded to a preset number when all members of the user group are invalid.

All user group members are invalid in the following situations:

- All the group members are offline or busy.
- No group member takes effect currently.
- There is no member configured for the user group.

Prerequisite

A user group has been created and the access code has been configured.

Example

Set the CFO forwarded-to number to 55001144.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 1001
[Huawei-voice-pbxusergroup-test] service cfo 55001144
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.99 service cfu

Function

The **service cfu** command configures a CFU forward-to number.

The **undo service cfu** command deletes the CFU forward-to number.

By default, the CFU forward-to number is not configured.

Format

service cfu *fwd-telno*

undo service cfu

Parameters

Parameter	Description	Value
fwd-telno	Specifies a forwarded-to number.	The value is an integer of 1 to 24 digits.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

All incoming calls of a service cfu user are forwarded to a preset number.

Before using the **service cfu** command, run the **service-right service cfu enable** command in the PBX user view to enable the CFU service.

Example

Set the forward-to number to 55001122.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service cfu 55001122
```

16.5.8.100 service crbt (enterprise view)

Function

The **service crbt** command configures the ring back tone (RBT) service for an enterprise.

 Copyright © Huawei Technologies Co., Ltd.

The **undo service crbt** command deletes the RBT service of an enterprise.

By default, no RBT service is configured.

Format

service crbt [**condition**{ **caller-telno***caller-telno-value* | **caller-trunkgroup** *trunkgroup-name* | **time-period** { **from***from-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **time-repeat** { **yearly** *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **monthly** *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] } } *] **file-name** *file-name-value*

undo service crbt [**condition** { **caller-telno** *caller-telno-value* | **caller-trunkgroup** *trunkgroup-name* | **time-period** { **from** *from-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **time-repeat** { **yearly** *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **monthly** *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] } } *]

Parameters

Parameter	Description	Value
condition	Indicates the RBT service.	N/A
caller-telno *caller-telno-value*	Specifies the calling number. **NOTE** Ensure that the specified phone number exists.	The value is a string of 1 to 44 characters.
caller-trunkgroup *trunkgroup-name*	Specifies the name of a calling trunk group. **NOTE** Ensure that the specified trunk group exists.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-period { **from***from-date* [*from-time*] | **to***to-date* [*to-time*] }	Specifies the validity period of the RBT service.	*from-date* and *to-date* specify the start date and end date. The date format is yyyy-mm-dd. yyyy (year) is an integer that ranges from 2000 to 2099. mm (month) is an integer that ranges form 1 to 12. dd (date) is an integer that ranges from 1 to 31. The end date must be later than the start date. *from-time* and *to-time* specify the start time and end time. The time format is hh:mm:ss. hh (hour) is an integer that ranges from 0 to 23. mm (minute) is an integer that ranges from 0 to 59. ss (second) is an integer that ranges from 0 to 59.
time-repeat { **yearly** *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **monthly** *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] }	Specifies the validity period of the RBT service.	**yearly** indicates that the RBT service takes effect every year. **monthly** indicates that the RBT service takes effect every month. **weekly** indicates that the RBT service takes effect every week. **daily** indicates that the RBT service takes effect every day.
file-name *file-name-value*	Specifies the RBT file name.	The value is a string of 1 to 64 characters. The format is path/:file-name, for example, flash:/qqqg.wav.

Views

Enterprise view

Default Level

2: Configuration level

Usage Guidelines

Enterprise ring-back-tone (RBT) is a piece of music or sound customized by an enterprise. After an enterprise registers the RBT service, the user can set different RBTs for a calling party or a group of calling parties in different periods.

Example

Configure the RBT service for the enterprise **abcd**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] enterprise abcd
[Huawei-voice-enterprise-abcd] service crbt condition caller-telno 12345678 time-period from
2012-12-30 08:00:00 to 2050-12-30 12:00:00 caller-trunkgroup abcd time-repeat daily 08:00:00 file-
name flash:/qqqg.wav
```

16.5.8.101 service crbt (user group view)

Function

The **service crbt** command configures an attribute of the user group RBT service.

The **undo service crbt** command deletes an attribute of the user group RBT service.

By default, an attribute of the user group RBT service is not configured.

Format

service crbt file-name *file-name-value*

undo service crbt

Parameters

Parameter	Description	Value
file-name *file-name-value*	Specifies the name of an RBT file.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of *path*:/*file-name*, for example, **flash:/test.wav**.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **service crbt** command to configure attributes for the user group RBT service and then activate an RBT file. When a user calls the user group, the music or sound effect but not the common ringback tone will be played to the calling user.

Prerequisite

A user group has been created and the access code has been configured.

Precautions

RBT files must be in .wav format.

Example

Configure service attributes for the RBT of the user group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxusergroup test hunt
[Huawei-voice-pbxusergroup-test] access-telno 1001
[Huawei-voice-pbxusergroup-test] service crbt file-name flash:/test.wav
```

16.5.8.102 service dlc

Function

Using the **service dlc** command, you can configure a number to be rejected.

Using the **undo service dlc** command, you can delete a number to be rejected.

By default, no number is rejected.

Format

service dlc *dlc-telno*

undo service dlc [*dlc-telno*]

Parameters

Parameter	Description	Value
dlc-telno	Specifies a number to be rejected.	The value is a string of 1 to 24 characters, which can be digits, the lowercase character "x", and asterisk (*). The "x" represents any digit. The asterisk (*) represents 1 to 16 digits and can appear only once in a number.

 Copyright © Huawei Technologies Co., Ltd.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Reject calling numbers 55661122.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service dlc 55661122
```

16.5.8.103 service dnd

Function

Using the **service dnd** command, you can configure a DND service.

Using the **undo service dnd** command, you can delete a DND service.

By default, no DND service is configured.

Format

service dnd [**tone-id** *tone-id*]

undo service dnd [**tone-id**]

Parameters

Parameter	Description	Value
tone-id *tone-id*	Specifies the ID of a DND tone.	The value is an integer that ranges from 1 to 566. By default, the value is 155. **NOTE** For details about voice tones, see the **display voice tone type** command.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The DND service allows a user to reject all incoming calls during a certain period. When a user calls the DND user, the user will hear the DND tone or busy tone.

NOTE

The DND service does not affect outgoing calls.

Before using the **service dnd** command, run the **service-right dnd enable** command in the user identifier view to enable the DND service.

Example

configure a DND service.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service dnd
```

16.5.8.104 service hotline

Function

The **service hotline** command configures a hotline number.

The **undo service hotline** command deletes the hotline number.

By default, no hotline number is configured.

Format

service hotline { **immediate** | **delay** } **hotline-telno** *hotline-telno-value*

undo service hotline { **immediate** | **delay** }

Parameters

Parameter	Description	Value
immediate	Indicates that a call is initiated immediately after a user picks up the phone.	-

Parameter	Description	Value
delay	Indicates that a call is initiates 5 minutes after a user picks up the phone and does not dial any number. **NOTE** This parameter is not supported.	-
hotline-telno *hotline-telno-value*	Specifies a hotline number. **NOTE** The hotline number cannot be an IVR number.	The value is an integer that ranges from 1 to 24.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Hotline service: After a user picks up the phone and does not dial any number, the device dials the hotline number for the user.

The PBX user type is POTS.

Prerequisites

The hotline number can be dialed and the call is reachable.

The hotline service has been enabled using the **service-right hotline enable** command in the PBX user view.

Example

Configure hotline number 55001155.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service-right hotline enable
[Huawei-voice-pbxuser-test] service hotline immediate hotline-telno 55001155
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.105 service rac

Function

Using the **service rac** command, you can configure a RAC service.

Using the **undo service rac** command, you can delete a RAC service.

By default, no RAC service is configured.

Format

service rac [**tone-id** *tone-id*]

undo service rac [**tone-id**]

Parameters

Parameter	Description	Value
tone-id *tone-id*	Specifies the ID of a RAC tone.	The value is an integer that ranges from 1 to 566. **NOTE** For details about voice tones, see the **display voice tone type** command.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The RAC service allows a user to reject anonymous calls during a certain period. When a user calls the RAC user, the user will hear the RAC tone or busy tone.

NOTE

The RAC service does not affect outgoing calls.

Before using the **service rac** command, run the **service-right rac enable** command in the user identifier view to enable the RAC service.

Example

configure a RAC service.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service rac
```

16.5.8.106 service rcs

Function

The **service rcs** command configures the selective call rejection (SCR) service.

The **undo service rcs** command deletes the configured SCR service.

By default, no SCR service is configured.

Format

service rcs judgegrp *judgegrp-value* [**condition** { **caller-telno** *caller-telno-value* | **time-period** { **from** *from-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **time-repeat** { { **yearly** | **monthly** } *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] } }*] [**active** *active-value*]

undo service rcs judgegrp *judgegrp-value*

Parameters

Parameter	Description	Value
judgegrp *judgegrp-value*	Specifies a judge group.	The value is an integer that ranges from 0 to 99.
caller-telno *caller-telno-value*	Specifies an SCR number.	The value is a string of 1 to 44 characters.
time-period	Indicates the lifecycle.	None
from	Indicates the start date.	None
from-date	Specifies the start date.	The format is year-month-day. The default value is 1970-01-01.
from-time	Specifies the start time.	The format is hour:minute:second. The default value is 00:00:00.
to	Indicates the end time.	None
to-date	Specifies the end time.	The format is year-month-day. The default value is 2100-12-31.
to-time	Specifies the end time.	The format is hour:minute:second. The default value is 23:59:59.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-repeat	Indicates the repeat mode.	None
yearly	Indicates that the SCR service takes effect every year.	None
monthly	Indicates that the SCR service takes effect every month.	None
begin-date	Specifies the start date of the validity period.	The format is year-month-day.The default value is 1970-01-01.
end-date	Specifies the end date of the validity period.	The format is year-month-day. The default value is the same as the end date.
begin-time	Specifies the start time of the validity period.	The format is hour:minute:second. The default value is 00:00:00.
end-time	Specifies the end time of the validity period.	The format is hour:minute:second. The default value is 23:59:59.
weekly	Indicates that the SCR service takes effect every week.	None
begin-weekday	Specifies the start day of the validity period.	Enumerated type. The value can be **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, or **sun**.
end-weekday	Specifies the end day of the validity period.	Enumerated type. The value can be **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, or **sun**.
daily	Indicates that the SCR service takes effect every day.	None
begin-time	Specifies the start time of the validity period.	The format is hour:minute:second. The default value is 00:00:00.
end-time	Specifies the end time of the validity period.	The format is hour:minute:second. The default value is 00:00:00.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
active *active-value*	Activates the configuration.	Enumerated type. The value can be **disable** or **enable**. ● disable: The configuration is disabled. ● enable: The configuration is enabled.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the SCR judge group number to 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service rcs judgegrp 2
```

16.5.8.107 service sca

Function

The **service sca** command configures the SCA service.

The **undo service sca** command deletes the SCA service.

By default, no SCA service is configured.

Format

service sca judgegrp *judgegrp-value* [**condition** { **caller-telno** *caller-telno-value* | **time-period** { **from** *from-date* [*from-time*] | **to** *to-date* [*to-time*] } * | **time-repeat** { { **yearly** | **monthly** } *begin-date* [*begin-time*] [*end-date* [*end-time*]] | **weekly** *begin-weekday* [*begin-time*] [*end-weekday* [*end-time*]] | **daily** *begin-time* [*end-time*] } }*] [**active** *active-value*]

undo service sca judgegrp *judgegrp-value*

Parameters

Parameter	Description	Value
judgegrp *judgegrp-value*	Specifies a judge group.	The value is an integer that ranges from 0 to 99.
caller-telno *caller-telno-value*	Specifies an SCA number.	The value is a string of 1 to 44 characters.
time-period	Indicates the lifecycle.	None
from	Indicates the start date.	None
from-date	Specifies the start date.	The format is year-month-day. The default value is 1970-01-01.
from-time	Specifies the start time.	The format is hour:minute:second. The default value is 00:00:00.
to	Specifies the end date.	None
to-date	Specifies the end date.	The format is year-month-day. The default value is 2100-12-31.
to-time	Specifies the end time.	The format is hour:minute:second. The default value is 23:59:59.
time-repeat	Indicates the repeat mode.	None
yearly	Indicates that the SCA service takes effect every year.	None
monthly	Indicates that the SCA service takes effect every month.	None
begin-date	Specifies the start date of the validity period.	The format is year-month-day.The default value is 1970-01-01.
end-date	Specifies the end date of the validity period.	The format is year-month-day. The default value is 2100-12-31.
begin-time	Specifies the start time of the validity period.	The format is hour:minute:second. The default value is 00:00:00.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-time	Specifies the end time of the validity period.	The format is hour:minute:second. The default value is 23:59:59.
weekly	Indicates that the SCA service takes effect every week.	None
begin-weekday	Specifies the start day of the validity period.	Enumerated type. The value can be **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, or **sun**.
end-weekday	Specifies the end day of the validity period.	Enumerated type. The value can be **mon**, **tue**, **wed**, **thu**, **fri**, **sat**, or **sun**.
daily	Indicates that the SCA service takes effect every day.	None
begin-time	Specifies the start time of the validity period.	The format is hour:minute:second. The default value is 00:00:00.
end-time	Specifies the end time of the validity period.	The format is hour:minute:second. The default value is 00:00:00.
active *active-value*	Activates the configuration.	Enumerated type. The value can be **disable** or **enable**. ● disable: The configuration is disabled. ● enable: The configuration is enabled.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the SCA judge group number to 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service sca judgegrp 2
```

16.5.8.108 service scr

Function

The **service scr** command configures a secretary number.

The **undo service scr** command deletes a secretary number.

By default, no secretary number is configured.

Format

service scr telno *scr-telno*

undo service scr

Parameters

Parameter	Description	Value
telno *scr-telno*	Specifies a secretary number.	The value is a string of 1 to 24 digits without spaces.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the secretary number to 55661122 for user **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service scr telno 55661122
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.109 service voicemailcfb

Function

The **service voicemailcfb** command configures the call forwarding busy (CFB)-voice mail (VM) service.

The **undo service voicemailcfb** command cancels the CFB-VM service.

By default, the CFB-VM service is not configured.

Format

service voicemailcfb { **vmsno** *vmsno-value* | **active** *active-value* } *

undo service voicemailcfb

Parameters

Parameter	Description	Value
vmsno-value	Specifies the voice mail number.	The value is an integer that ranges from 0 to 254.
active-value	Indicates whether the CFB-VM service is activated.	Enumerated type. The values are as follows: ● disable: The CFB-VM service is deactivated. ● enable: The CFB-VM service is activated.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The CFB-VM service allows the device to forward all incoming calls to a voice mail when the PBX user is busy.

Before using this command, run the **service-right voicemailcfb enable** command in the PBX user view to enable the CFB-VM service.

Example

Configure the CFB-VM service

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service voicemailcfb vmsno 0 active enable
```

16.5.8.110 service voicemailcfnr

Function

The **service voicemailcfnr** command configures the call forwarding no reply (CFNR)-voice mail (VM) service.

The **undo service voicemailcfnr** command cancels the CFNR-VM service.

By default, the CFNR-VM service is not configured.

Format

service voicemailcfnr [*time*] { **vmsno** *vmsno-value* | **active** *active-value* } *

undo service voicemailcfnr

Parameters

Parameter	Description	Value
vmsno-value	Specifies the voice mail number.	The value is an integer that ranges from 0 to 254.
active-value	Indicates whether the CFNR-VM service is activated.	Enumerated type. The options are as follows: ● disable: The CFNR-VM service is deactivated. ● enable: The CFNR-VM service is activated.
time	the time length of no answer	The value is an integer that ranges from 5 to 55. The default value is 20.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The CFNR-VM service allows the device to forward all incoming calls to a voice mail when the PBX user does not respond.

Before using this command, run the **service-right voicemailcfnr enable** command in the PBX user view to enable the CFNR-VM service.

Example

Configure the CFNR-VM service.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service voicemailcfnr 30 vmsno 0 active enable
```

16.5.8.111 service voicemailcfo

Function

The **service voicemailcfo** command configures the call forwarding offline (CFO)-voice mail (VM) service.

The **undo service voicemailcfo** command cancels the CFO-VM service.

By default, the CFO-VM service is not configured.

Format

service voicemailcfo { **vmsno** *vmsno-value* | **active** *active-value* } *

undo service voicemailcfo

Parameters

Parameter	Description	Value
vmsno-value	Specifies the voice mail number.	The value is an integer that ranges from 0 to 254.
active-value	Indicates whether the CFO-VM service is activated.	Enumerated type. The values are as follows: ● disable: The CFO-VM service is deactivated. ● enable: The CFO-VM service is activated.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The CFO-VM service allows the device to forward all incoming calls to a voice mail when the PBX user is offline.

Before using this command, run the **service-right voicemailcfo enable** command in the PBX user view to enable the CFO-VM service

Example

Configure the CFO-VM service

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service voicemailcfo vmsno 0 active enable
```

16.5.8.112 service voicemailcfu

Function

The **service voicemailcfu** command configures the call forwarding unconditional (CFU)-voice mail (VM) service.

The **undo service voicemailcfu** command cancels the CFU-VM service.

By default, the CFU-VM service is not configured.

Format

service voicemailcfu { **vmsno** *vmsno-value* | **active** *active-value* } *

undo service voicemailcfu

Parameters

Parameter	Description	Value
vmsno-value	Specifies the voice mail number.	The value is an integer that ranges from 0 to 254.
active-value	Indicates whether the CFU-VM service is activated.	Enumerated type. The values are as follows: ● disable: The CFU-VM service is deactivated. ● enable: The CFU-VM service is activated.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The CFU-VM service allows the device to forward all incoming calls to a voice mail unconditionally.

Before using this command, run the **service-right voicemailcfu enable** command in the PBX user view to enable the CFU-VM service.

Example

Configure the CFU-VM service.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test
[Huawei-voice-pbxuser-test] service voicemailcfu vmsno 0 active enable
```

16.5.8.113 service wake-call

Function

The **service wake-call** command creates a wake-up service.

The **undo service wake-call** command deletes a wake-up service.

By default, no wake-up service is configured.

Format

service wake-call wake-time *wake-time-value* [**begin-date** *begin-date-value* | **wake-days** *wake-days-value* | **tone-id** *tone-id-value*] *

undo service wake-call

Parameters

Parameter	Description	Value
wake-time *wake-time-value*	Specifies the start time of the wake-up service.	hh (hour) ranges from 0 to 23. mm (minute) ranges from 0 to 59. ss (second) ranges from 0 to 59.
begin-date *begin-date-value*	Specifies the start date of the wake-up service.	N/A
wake-days *wake-days-value*	Specifies the number of days during which the wake-up service takes effect.	The value is an integer that ranges from 0 to 99, in days.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tone-id *tone-id-value*	Specifies the ID of a wake-up tone.	The value is an integer that ranges from 1 to 566. **NOTE** For details about voice tones, see the **display voice tone type** command.

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

The wake-up service allows a phone to ring automatically at the preset time.

Before using the **service wake-call** command, run the **service-right wake-call enable** command in the PBX user view to enable the wake-up service.

Example

Set the start time of the wake-up service to 22:00:00.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser test pots
[Huawei-voice-pbxuser-test] service wake-call wake-time 22:00:00
```

16.5.8.114 service-active

Function

The **service-active** command activates the call waiting, digital number limit call, or password call service.

The **undo service-active** command deactivates the call waiting, number barring, or password call service.

By default, the call waiting, digital number limit call, and password call services are disabled.

Format

service-active *service-name*

undo service-active *service-name*

Parameters

service-name could be one of the parameters as follows

Parameter	Description	Value
cw	Specifies the call waiting service.	-
dlc	Specifies the digit number limit call service.	-
pwcb	Specifies the password call service.	-

Views

PBX User view

Default Level

2: Configuration level

Usage Guidelines

After the call waiting, number barring, or password call service is enabled, run the **service-active** command to activate the service to make it take effect.

Example

Activate the call waiting service.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser user001
[Huawei-voice-pbxuser-user001] service-active cw enable
[Huawei-voice-pbxuser-user001] service-active cw
```

16.5.8.115 service-right

Function

The **service-right** command enables or disables a specified service right.

The **undo service-right** command restores the default setting.

By default, the following service rights are granted to users: **abbdial**, **cba**, **cfb**, **cfc**, **cfnr**, **cfo**, **cfu**, **clip**, **cnip**, **cw**, **dnd**, **query-dialno**, and **wake-call**.

Format

service-right *service-name right-value*

undo service-right *service-name*

Parameters

Parameter	Description	Value
service-name	Specifies a service name.	The services include: • **abbdial**: Abbreviated dialing • **called-control**: Called control • **cba**: Call barring • **ccbs**: busy callback • **ccnr**: no answer callback • **cfb**: Call forwarding on busy • **cfc**: Call forwarding conditionally • **cfnr**: Call forwarding on no reply • **cfo**: Call forwarding on offline • **cfu**: Call forwarding unconditionally • **clip**: Calling line identification presentation • **clir**: Calling line identification restriction • **cnip**: Calling name identification presentation • **conp**: Connected name identification presentation • **cw**: Call waiting • **dlc**: Digital number limit call • **dnd**: Do not disturb • **hotline**: Hotline service • **instant-conference**: Instant conference • **multiplecallright**: Call of multiple lines • **overstepclir**: Calling line identification restriction override • **pickup-in-group**: Pickup in group • **pickupspecial**: Pickup in special • **pwcb**: Password call • **query-dialno**: Query telephone number • **rac**: Rejecting anonymous call • **rcs**: Selective call rejection • **ring-service**: Ring service • **sca**: Selective call acceptance • **scc-cancel**: Deregistering all services • **scr**: Secretary service • **three-party**: Three-party service

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• **voicemailcfb**: Forwarding call to voice mail on busy • **voicemailcfnr**: Forwarding call to voice mail on no reply • **voicemailcfo**: Forwarding call to voice mail on offline • **voicemailcfu**: Forwarding call to voice mail unconditional • **wake-call**: Wake-up call
right-value	Specifies whether a service right is enabled or disabled.	Enumerated value. The options are as follows: • disable • enable

Views

PBX user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure different service rights for users of different types.

- BRA users have only the **clip** and **query-dialno** service rights.
- The **hotline** service is only for POTS users.
- The **cnip** and **conp** services are only for SIP users.

Prerequisite

A PBX user has been created and mandatory configurations have been performed. For details, see **Configuring a PBX User**.

Example

Enable the call waiting service for the user abcd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] pbxuser abcd sipue
[Huawei-voice-pbxuser-abcd] sipue 1002
[Huawei-voice-pbxuser-abcd] telno 1002
[Huawei-voice-pbxuser-abcd] service-right cw enable
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.8.116 space-waring-num-left

Function

The **space-waring-num-left** command specifies the number of remaining leave messages in an alarm notification.

The **undo space-waring-num-left** command restores the default number of remaining leave messages in an alarm notification.

Format

space-waring-num-left *space-waring-num-left-value*

undo space-waring-num-left

Parameters

Parameter	Description	Value
space-waring-num-left-value	Specifies the number of remaining leave messages in an alarm notification.	The value is an integer that ranges from 0 to 20. The default value is 5.

Views

VMS view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the number of remaining leave messages in an alarm notification to 3

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] vms
[Huawei-voice-vms] space-waring-num-left 3
```

16.5.8.117 ssca-group

Function

The **ssca-group** command creates and enters the service view for the senior manager's secretary and specifies the PBX user with the right of the service for the senior manager's secretary.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ssca-group** group deletes the created service view for the senior manager's secretary.

Format

ssca-group pbxuser *pbxusername*

undo ssca-group pbxuser *pbxusername*

Parameters

Parameter	Description	Value
pbxuser *pbxusername*	Specifies a PBX user with the right of the service for the senior manager's secretary.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create and enter the service view for the senior manager's secretary and specify PBX user 1001 with the right of the service for the senior manager's secretary.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]ssca-group pbxuser 1001
[Huawei-voice-ssca-group-1001]
```

16.5.8.118 track vrrp

Function

The **track vrrp interface** command associates a VRRP group with SIP server.

The **undo track vrrp interface** command cancels the configuration.

By default, no VRRP group is associated with a trunk group or SIP server.

Format

track vrrp interface *interface-type interface-number* **vrid** *virtual-router-id*

undo track vrrp

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface associated with a VRRP group.	-
vrid *virtual-router-id*	Specifies the ID of a VRRP group.	The value is an integer that ranges from 0 to 255.

Views

SIP server view, trunk group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **track vrrp interface** command implements SIP AG backup in the following scenarios:

- Two ARSRGUSR routers function as SIP AGs at the egress of an enterprise network. Their downlink interfaces connect to an IP PBX that does not register with the session border controller (SBC), and their uplink interfaces connect to an IP multimedia subsystem (IMS) network. Downlink interfaces of the routers form a VRRP group to implement SIP AG backup. When an active/standby switchover occurs in the VRRP group, the IP PBX and IMS network cannot detect the switchover. You can associate the VRRP group with a trunk group or SIP server on the IP PBX. When a switchover occurs in the VRRP group, traffic of the trunk group or SIP server is switched to the new master device. Only the VRRP master registers with the SBC and forwards signaling streams and media streams of voice services.
- Two ARSRGUSR routers function as SIP AGs at the egress of an enterprise network. Their downlink interfaces connect to an IP PBX that has registered with the SBC, and their uplink interfaces connect to an IMS network. Downlink interfaces of the routers form a VRRP group to implement SIP AG backup. When an active/standby switchover occurs in the VRRP group, the IMS network cannot detect the switchover. The IP PBX needs to register with the SBC again to restore services.

Prerequisites

- VRRP has been configured on downlink interfaces of the routers.

 Copyright © Huawei Technologies Co., Ltd.

- (Optional) VRRP association has been configured so that an uplink or downlink failure can trigger a VRRP switchover.
- A PBX trunk group has been configured.

Example

Associate a VRRP group with a trunk group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group sipip
[Huawei-voice-trunkgroup-sipip] track vrrp interface GigabitEthernet 0/0/0 vrid 2
```

Associate a VRRP group with a SIP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipserver
[Huawei-voice-sipserver] track vrrp interface GigabitEthernet 0/0/0 vrid 2
```

16.5.8.119 triggertype (simultaneous or sequential ringing group view)

Function

The **triggertype** command configures the triggering type of a simultaneous or sequential ringing group.

Format

triggertype *triggertype-value*

undo triggertype

Parameters

Parameter	Description	Value
triggertype-value	Specifies the triggering type of a simultaneous or sequential ringing group.	Enumerated type. The options are as follows: ● internal: intra-office ● external: intra-office ● unspecified ● The default value is **unspecified**.

Views

Simultaneous or sequential ringing group view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the triggering type of sequential ringing group 28980004 to **internal**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] ring-serial-group pbxuser 28980004
[Huawei-voice-ring-serial-group-28980004]triggertype internal
```

16.5.8.120 trunk-group (post-routing number change plan view)

Function

Using the **trunk-group** command, you can configure the system to change numbers from which calls pass through a specified trunk group.

Format

trunk-group *trunk-group-name*

Parameters

Parameter	Description	Value
trunk-group-name	Specifies the name of a trunk group.	The value is a string of 1 to 32 characters.

Views

Post-routing number change plan view

Default Level

2: Configuration level

Usage Guidelines

The **trunk-group** command configures the system to change numbers from which calls pass through a specified trunk group.

Example

Configure the system to change numbers from which calls pass through a SIP trunk group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] afterroute-change test
[Huawei-voice-afterroute-change-test] trunk-kgroup SIP
```

16.5.8.121 unicall-group

Function

The **unicall-group** command creates an ONLY service user group and enters the ONLY service user group view.

The **undo unicall-group** command deletes the ONLY service user group.

.

Format

unicall-group pbxuser *pbxuser-name*

undo unicall-group pbxuser *pbxuser-name*

Parameters

Parameter	Description	Value
pbxuser *pbxuser-name*	Specifies the name of a user group.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

After you create an ONLY service user group and specify a PBX user in the group, the specified PBX user becomes the primary user in the group.

Example

Create an ONLY service user group **28980001**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] unicall-group pbxuser 28980001
```

16.5.8.122 use-rule-set

Function

The **use-rule-set** command applies a rule set (blacklist or whitelist) to a trunk group.

 Copyright © Huawei Technologies Co., Ltd.

The **undo use-rule-set** command deletes a rule set (blacklist or whitelist) from a trunk group.

Format

use-rule-set *rule-set-name*

undo use-rule-set

Parameters

Parameter	Description	Value
rule-set-name	Specifies the name of a rule set.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

Trunk group view

Default Level

2: Configuration level

Example

Apply the rule set **rule** to the trunk group **test**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] trunk-group test
[Huawei-voice-trunkgroup-test] use-rule-set rule
```

16.5.8.123 vms

Function

The **vms** command enters the voice mail service (VMS) view.

Format

vms

Parameters

None

Views

Voice view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enter the VMS view

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]vms
```

16.5.8.124 vmsdata-storage-path

Function

The **vmsdata-storage-path** command specifies the path for storing leave messages.

The **undo vmsdata-storage-path** command deletes the path for storing leave messages.

Format

vmsdata-storage-path *vmsdata-storage-filepath-value*

undo vmsdata-storage-path

Parameters

Parameter	Description	Value
vmsdata-storage-filepath-value	Specifies the path for storing leave messages.	The value is a string of 1 to 15 characters.

Views

VMS view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the path for storing leave messages.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] vms
[Huawei-voice-vms] vmsdata-storage-path sd1:
```

16.5.8.125 vmsno

Function

The **vmsno** command configures VMS mailbox information.

The **undo vmsno** command deletes a VMS mailbox information.

Format

vmsno *vmsno* **callprefix** *callprefix-value*

undo vmsno *vmsno*

Parameters

Parameter	Description	Value
vmsno	Specifies the voice mail number.	The value is an integer that ranges from 0 to 254.
callprefix *callprefix-value*	Specifies the name of the call prefix view.	The value is a string of 1 to 32 characters without spaces.

Views

VMS view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure VMS mail information

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] vms
[Huawei-voice-vms] vmsno 0 callprefix 10000
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.9 Local Survival Configuration Commands

16.5.9.1 dataserver

Function

The **dataserver** command configures an IP address and port number for the data server.

Format

dataserver ip *ip-address* [**port** *port-number*]

undo dataserver

Parameters

Parameter	Description	Value
ip-address	Specifies the data server's IP address.	The value is in dotted decimal notation.
port-number	Specifies the data server's port number.	The value is an integer that ranges from 1 to 65535.

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Configure the IP address and port number for the data server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival]dataserver ip 192.168.0.2 port 21
```

16.5.9.2 dataservertype

Function

The **dataservertype** command configures the data server type.

 Copyright © Huawei Technologies Co., Ltd.

Format

dataservertype *type-value*

Parameters

Parameter	Description	Value
type-value	Specifies the data server type.	Enumerated type. The value is <BMP, U1900>. The default value is BMP.

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Configure the data server type.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival]dataservertype u1900
```

16.5.9.3 display voice local-survival lefttime

Function

The **display voice local-survival lefttime** command displays the remaining available time of the license for the **best** item.

Format

display voice local-survival lefttime

Parameters

None

Views

All view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

The **best** resource item in the license is for local survival. When the local node properly connects to the central node, the license controls the call resources. When the local node disconnects from the central node or when the **best** resource item is used but local survival is not configured, a 720-hour period is provided for the call services on the local node. When the time expires, call services are unavailable until the local node reconnects to the central node. When the local node reconnects to the central node, the remaining time restores to 720 hours and the time does not elapse. If the best source item is available but is not used, calls are not restricted.

Example

Display the remaining available time of the license for the **best** item for local survival.

```
<Huawei>display voice local-survival lefttime
 Best License Time Left:   708(Hours)
```

16.5.9.4 display voice local-survival status

Function

The **display voice local-survival status** command displays the local survival configuration.

Format

display voice local-survival status

Parameters

None

Views

All view

Default Level

3: Management level

Usage Guidelines

After local survival data is configured, you can run this command to verify the configuration.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

In the command output, if the local survival configuration is inconsistent with the running information, the current configuration does not take effect.

Example

Display the local survival configuration.

```
<Huawei> display voice local-survival status
Local Survival Config Infomation:
Station Type:           localgw
Bmp Server IP:          192.168.10.29
Bmp Server Port:        8889
Primaryserver IP:
Transfer mode:          TCP
SSL server policy:
Primary Trunk Group:    primary
Secondary Trunk Group:
ProxyReg Trunk Group:
Bill Switch:            OFF

Local Survival Running Infomation:   WorkStatus:          ACTIVATE
Station Type:           localgw
Bmp Server IP:          192.168.10.29
Bmp Server Port:        8889
Primaryserver IP:
Transfer mode:          TCP
SSL server policy:
Primary Trunk Group:    primary
Secondary Trunk Group:
ProxyReg Trunk Group:
Bill Switch:            OFF
```

Table 16-102 Description of the **display voice sipserver** command output

Item	Description
WorkStatus	Working status. In local survival mode, the value is Active. In non-local-survival mode, the value is DEACTIVE.
Station Type	Type of the station.
Bmp Server IP	BMP server's IP address.
Bmp Server Port	BMP server's port number.
Primaryserver IP	Data server's IP address.
Transfer mode	Transfer mode of the BIN channel.
SSL server policy	Serer SSL policy bound to the BIN channel.
Primary Trunk Group	Name of the trunk group associated with the primary central node.
Secondary Trunk Group	Name of the trunk group associated with the secondary central node.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ProxyReg Trunk Group	Name of trunk group is used for AR proxy register
Bill Switch	The bill switch when status is deactive

16.5.9.5 local-address

Function

The **local-address ip** command configures the IP address and port for the BIN channel.

The **undo local-address ip** command deletes the IP address and port of the BIN channel.

Format

local-address ip *ip-value* [**port** *port-value*]

undo local-address

Parameters

Parameter	Description	Value
ip-value	Specifies an IP address for the BIN channel.	The value is in dotted decimal notation.
port-value	Specifies a port for the BIN channel.	The value is an integer that ranges from 8000 to 65534. The default value is 8000.

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Specify IP address 192.168.1.1 and port 8001 for the BIN channel.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival] local-address 192.168.1.1 port 8001
```

16.5.9.6 local-bill

Function

The **local-bill** command configures the local bill.

The **undo local-bill** command restores the default local bill.

Format

local-bill *bill-switch-value*

undo local-bill

Parameters

Parameter	Description	Value
bill-switch-value	Indicates whether the CDR is enabled when the local node is in deactive state.	Enumerated value. The value is OFF, ON. The default value is OFF.

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure the data server type.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival] local-bill ON
```

16.5.9.7 local-survival

Function

The **local-survival** command enters the local survival view.

The **undo local-survival** command deletes the local survival configuration.

Format

local-survival

undo local-survival

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When the device functions as the local node in UC scenarios, run this command to enter the local survival view.

Example

Enter the local survival view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]local-survival
[Huawei-voice-local-survival]
```

16.5.9.8 password cipher

Function

The **password cipher** command configures an authentication password for the BIN channel.

Format

password cipher *password-value*

Parameters

Parameter	Description	Value
password-value	Specifies a cipher text password. **NOTE** You can set this parameter only after entering **cipher** and pressing **Enter**.	The value is a string of 16 to 32 characters without spaces.

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the authentication password to **abcdefgh12345678** for the BIN channel.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival]password cipher  Please input user password(16-32 chars):****************
```

16.5.9.9 primary-trunk-group

Function

The **primary-trunk-group** command binds a trunk group to the primary central node. The heartbeat of the trunk group represents the connection status between the local node and central node.

The **secondary-trunk-group** command binds a trunk group to the secondary central node. The heartbeat of the trunk group represents the connection status between the local node and central node.

The **proxyreg-trunk-group** command binds a trunk group to the central node for proxy-register. The heartbeat of the trunk group represents the connection status between the local node and central node.

The **undo primary-trunk-group** command unbinds the trunk group from the central node.

 Copyright © Huawei Technologies Co., Ltd.

Format

primary-trunk-group *trunk-group-name* [**secondary-trunk-group** *trunk-group-name*] [**proxyreg-trunk-group** *trunk-group-name*]

undo primary-trunk-group

Parameters

Parameter	Description	Value
trunk-group-name	Specifies the name of a trunk group.	The value is a string of 1 to 32 characters.

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

#Configure primary and secondary trunk groups.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival]primary-trunk-group tkg1 secondary-trunk-group tkg2 proxyreg-trunk-group tkg3
```

16.5.9.10 reset

Function

The **reset** command resets local survival data.

Format

reset

Parameters

None

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

After this command is used, local survival data is reset. Exercise caution when you run this command.

Example

Reset local survival data.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival]reset
```

16.5.9.11 ssl-server-policy

Function

The **ssl-server-policy** command binds a server SSL policy to the BIN channel.

The **undo ssl-server-policy** command unbinds a server SSL policy from the BIN channel.

By default, no server SSL policy is bound to the BIN channel.

Format

ssl-server-policy*server-policy-name*

undo ssl-server-policy

Parameters

Parameter	Description	Value
server-policy-name	Specifies the name of a server SSL policy.	The value is a string of 1 to 31 case-insensitive characters without question marks (?) or spaces.

Views

Local survival view, SIP server view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance data transmission security on the BIN channel, run the **ssl-server-policy** command to bind a server SSL policy to the BIN channel. Data encryption, identity authentication, and message integrity check mechanisms of the SSL protocol protect security of data transmitted on the BIN channel.

Prerequisites

A server **SSL policy** has been configured.

The transfer mode on the BIN channel has been set to TLS.

Configuration Impact

If you run the **ssl-server-policy** command multiple times, only the latest configuration takes effect.

The server SSL policy bound to the BIN channel cannot be used by other services such as HTTPS; otherwise, the BIN channel cannot transmit data.

Example

Bind the server SSL policy **server** to the BIN channel.

```
Huawei> system-view
[Huawei] voice
[Huawei-voice]local-survival
[Huawei-voice-local-survival] transfer TLS
[Huawei-voice-local-survival] ssl-server-policy server
```

16.5.9.12 sync-interval

Function

The **sync-interval** command enables timing synchronization and sets the synchronization interval for the BIN channel.

The **undo sync-interval** command disables timing synchronization and deletes the synchronization interval for the BIN channel.

Format

sync-interval *sync-interval-value*

undo sync-interval

Parameters

Parameter	Description	Value
sync-interval-value	Specifies the synchronization interval for the BIN channel.	The value is an integer that ranges from 2 to 240, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Local survival view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the synchronization interval to 5s for the BIN channel.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival]sync-interval 5
```

16.5.9.13 transfer

Function

The **transfer** command configures a transfer mode for the BIN channel.

The **undo transfer** command restores the default transfer mode for the BIN channel.

By default, the transfer mode for the BIN channel is TLS.

Format

transfer *transfer-value*

undo transfer

Parameters

Parameter	Description	Value
transfer-value	Specifies a transfer mode for the BIN channel.	Enumerated type. The options are as follows: ● TLS ● TCP The default value is TLS.

Views

Local survival view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the transfer mode to TCP for the BIN channel.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-survival
[Huawei-voice-local-survival] transfer TCP
```

16.5.10 Conference Configuration Commands

16.5.10.1 attendee-password

Function

The **attendee-password** command configures an attendee password.

Format

attendee-password cipher

Parameters

Parameter	Description	Value
cipher	After user confirmed by ENTER button, can input the password with masked character of '*' printed on screen	The value is a string of 6 to 16 digits.

Views

Conference view

Default Level

2: Configuration level

Usage Guidelines

- This command is optional. If no attendee password is configured when you create a new user, the system automatically assigns a random password to the user.

- The password must be a string of 6-16 digits.
- The password for the participants cannot be the same as or the reverse of the password for the moderator.
- The conference password cannot be the same as or the reverse of the account of the user who schedules the conference.
- When the conference subject is a string of digits only, the conference password cannot be the same as the conference subject.

Example

Create a conference named **myconference** and set the attendee password to **132456**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]conference myconference
[Huawei-voice-conference-myconference]attendee-password cipher
 Please input user password(6-16 chars):******
[Huawei-voice-conference-myconference]
```

16.5.10.2 attendee-telno

Function

The **attendee-telno** command connects an attendee to a specific conference or controls attendees of a conference.

Format

attendee-telno *attendeedn-string* [**mode** *mode-type*]

undo attendee-telno *attendeedn-string*

Parameters

Parameter	Description	Value
attendeedn-string	Specifies the telephone number of the user to be connected to a conference.	The value is a string of 1 to 32 characters.
mode *mode-type*	Specifies the mode in which the user is connected to the conference.	Enumerated type. The values are as follows: ● listenspeak ● listenonly ● chairman ● isolate the default value is listenspeak.

Views

Conference view

Default Level

2: Configuration level

Usage Guidelines

- This is the core configuration. If a telephone number is not registered on the device, the device connects the telephone number to the conference in default mode. You can run this command to change the connection mode of registered users.
- If *mode-type* is not specified, the **listenspeak** mode is used by default.
- Do not specify *isolate* before a scheduled conference begins. After a conference begins, you can specify *isolate* to isolate specified users attending the conference.

Example

Create a conference named **myconference** and connect telephone numbers 3001, 3002, and 3003 to the conference. 3001 is the chairman; 3002 is a common attendee; and 3003 is an attendee with listenonly rights.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference myconference
[Huawei-voice-conference-myconference] attendee-telno 3001 mode chairman
[Huawei-voice-conference-myconference] attendee-telno 3002
[Huawei-voice-conference-myconference] attendee-telno 3003 mode listenonly
```

Delete the attendee 3002.

```
[Huawei-voice-conference-myconference] undo attendee-telno 3002
```

16.5.10.3 chairman-password

Function

The **chairman-password** command configures a chairman password.

Format

chairman-password cipher

Parameters

Parameter	Description	Value
cipher	After user confirmed by ENTER button, he can input the password with masked character of '*' printed on screen.	The value is a string of 6 to 16 digits.

Views

Conference view

Default Level

2: Configuration level

Usage Guidelines

- This command is optional. If no chairman password is configured when you create a new user, the system automatically assigns a random password to the user.
- The password must be a string of 6-16 digits.
- The password for the participants cannot be the same as or the reverse of the password for the moderator.
- The conference password cannot be the same as or the reverse of the account of the user who schedules the conference.
- When the conference subject is a string of digits only, the conference password cannot be the same as the conference subject.

Example

Create a conference named **myconference** and set the chairman password to **142356**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference myconference
[Huawei-voice-conference-myconference] chairman-password cipher
 Please input user password(6-16 chars):******
[Huawei-voice-conference-myconference]
```

16.5.10.4 conference

Function

The **conference** command initializes a scheduled conference or enter a specific conference view, and generate a random attendee password and chairman password. Both chairman and attendees can see their password through self-services http web page.

Format

conference *conference-name* [**enterprise** *enterprise-name*]

undo conference *conference-name*

Parameters

Parameter	Description	Value
conference-name	Specifies a conference name.	The value is a string of 1 to 32 characters.
enterprise *enterprise-name*	Specifies an enterprise name.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

- After you run this command to initialize a conference, you cannot modify the enterprise.
- If the *enterprise* parameter is not specified when you create a conference, the conference belongs to the default enterprise.

Example

Create a conference named **myconference**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]conference myconference
[Huawei-voice-conference-myconference]
```

Delete the conference **myconference**.

```
[Huawei-voice] undo conference myconference
```

16.5.10.5 conference-attribute

Function

The **conference-attribute** command configures conference attributes and enters the global conference attribute view.

Format

conference-attribute

undo conference-attribute

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enter the conference attribute view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]conference-attribute
[Huawei-voice-conference-attribute]conference-id-length two
```

Display all the global conference parameters.

```
[Huawei-voice]display voice conference-attribute
 The length of conference ID is 2
 Conference convoker telnumber: 10010
 The reconvoke attempts for conference is 4
 Conference callright out (ddd)  :  Enable
 Conference callright out (idd)  :  Enable
 Conference callright out (inter):  Enable
 Conference callright out (local):  Enable
```

Restore all the global conference parameters to the default values.

```
[Huawei-voice]undo conference-attribute
```

Display all the global conference parameters after parameters restored.

```
[Huawei-voice]display voice conference-attribute
 The length of conference ID is 8
 Conference convoker is not set!
 The reconvoke attempts for conference is 0
 Conference callright out (ddd)  :  Disable
 Conference callright out (idd)  :  Disable
 Conference callright out (inter):  Enable
 Conference callright out (local):  Enable
[Huawei-voice]
```

16.5.10.6 conference-convoker

Function

The **conference-convoker** command configures the default convener number globally when the conference has no chairman.

Format

conference-convoker *convoker-telno*

undo conference-convoker

Parameters

Parameter	Description	Value
convoker-telno	Specifies the telephone number of the convener.	The value is a string of 1 to 32 digits without spaces.

Views

Conference attribute view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the telephone number of the convener to 10010.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference-attribute
[Huawei-voice-conference-attribute] conference-convoker 10010
```

Delete the telephone number of the convener globally.

```
[Huawei-voice-conference-attribute] undo conference-convoker
```

16.5.10.7 conference-id-length

Function

The **conference-id-length** command configures the length of a conference ID globally.

Format

conference-id-length *length-choice*

undo conference-id-length

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
length-choice	Specifies the length of a conference ID.	Enumerated type. The values are as follows: ● two: The length of the conference ID is 2. ● eight: The length of the conference ID is 8. The default value is eight.

Views

Conference attribute view

Default Level

2: Configuration level

Usage Guidelines

Delete all the conferences on the current device before you can change the length of a conference ID.

Example

Set the length of a conference ID to 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference-attribute
[Huawei-voice-conference-attribute] conference-id-length two
```

Restore the length of a conference ID to 8.

```
[Huawei-voice-conference-attribute] undo conference-id-length
```

16.5.10.8 conference-reconvoke-attempts

Function

The conference-reconvoke-attempts command configures the re-convoke attempts of a scheduled conference globally.

Format

conference-reconvoke-attempts *reconvoke-times*

undo conference-reconvoke-attempts

Parameters

Parameter	Description	Value
reconvoke-times	Specifies the re-convoke attempts.	The value is an integer that ranges from 0 to 16. value 0 is set as default.

Views

Conference attribute view

Default Level

2: Configuration level

Usage Guidelines

This command is optional. The device does not re-convoke a scheduled conference, that is, *reconvoke-times* is set to 0.

This command takes effect in only a few scenarios listed as follows:

- Do-not-disturb
- Called user is busy
- Called user is absent
- Called user is restricted
- Called user didn't respond
- Called user rejected

Example

Set the re-convoke attempts of a scheduled conference to 4.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference-attribute
[Huawei-voice-conference-attribute] conference-reconvoke-attempts 4
```

Restore the re-convoke attempts of a scheduled conference to 0.

```
[Huawei-voice-conference-attribute] undo conference-reconvoke-attempts
```

16.5.10.9 custom-right (conference-attribute view)

Function

The **custom-right** command configures default 32-level rights for conferences globally.

Format

custom-right {*c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32*}.

undo custom-right [*c1* | *c2* | *c3* | *c4* | *c5* | ...| *c32*].

Parameters

Parameter	Description	Value
c1 | *c2* | *c3* | *c4* | *c5* | ...| *c32*	Specifies 32-level rights to be configured for conferences globally.	The value can be one or more of **c1** to **c32**.

Views

conference-attribute view

Default Level

2: Configuration level

Usage Guidelines

(1) This configuration is mainly used to perform call barring based on the 32-level rights for conferences through system convening where no moderator exists, and further enhances **out-right** for global conferences.

(2) This configuration is optional. By default, a conference does not have any 32-level rights.

(3) This configuration is mainly used to control 32-level rights of conference calls and prevent users from making fraud calls beyond their rights through conferences.

Example

Configure 32-level rights **c4**, **c8**, and **c12** for conferences globally.

```
<Huawei> system-view
[Huawei]voice
[Huawei]conference-attribute
[Huawei-voice-conference-attribute]custom-right c4 c8 c12
```

Delete 32-level right **c8** for conferences.

```
[Huawei-voice-conference-attribute]undo custom-right c8
```

Clear all 32-level rights configured for conferences.

```
[Huawei-voice-conference-attribute]undo custom-right
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.10.10 description

Function

The **description** command configures brief description about a conference.

Format

description *conference-description;*

undo description

Parameters

Parameter	Description	Value
conference-description	Indicates conference description.	The value is a string of 1 to 64 characters.

Views

Conference view

Default Level

2: Configuration level

Usage Guidelines

This command is optional.

Example

Create a conference named **myconference** and configure the conference description as **workmeeting**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]conference myconference
[Huawei-voice-conference-myconference]description workmeeting
```

Delete description of a conference.

```
[Huawei-voice-conference-myconference]undo description
```

16.5.10.11 display voice conference

Function

The **display voice conference** command displays specified or call conferences.

Format

display voice conference [*conference-name*]

Parameters

Parameter	Description	Value
conference-name	Specifies the conference name.	The value is a string of 1–32 characters.

Views

All views

Default Level

3: Management level

Usage Guidelines

To display specified or call conferences, run **display voice conference** command.

Example

Display the conference named **myconference**.

```
<Huawei> display voice conference myconference
 ********Conference name: myconference*********
 Conference ID: 00082794
 Start Type: reserved
 Is Started: no
 Enterprise: default
 Dnset     : DefaultDialPlan
 Register Number: 6
 Status: idle

 Attendee list of the conference:


 Total attendee number listed  : 0
 Total attendee number present : 0
```

16.5.10.12 display voice conference-attribute

Function

The **display voice conference-attribute** command displays the global conference attributes configured in the current system.

Format

display voice conference-attribute

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To display the global conference attributes configured in the current system, run the **display voice conference-attribute** command.

Example

Display the global conference attributes.

```
<Huawei> display voice conference-attribute
 The length of conference ID is 2
 Conference convoker telnumber: 10010
 The reconvoke attempts for conference is 4
 Conference callright out (ddd)  :  Enable
 Conference callright out (idd)  :  Enable
 Conference callright out (inter):  Enable
 Conference callright out (local):  Enable
```

16.5.10.13 display voice conference-convoker

Function

The **display voice conference-convoker** command displays the default number for convening a conference without a moderator.

Format

display voice conference-convoker

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the number of the conference convener.

```
<Huawei> display voice conference-convoker
 Conference convoker telnumber: 10010
```

16.5.10.14 display voice conference-custom-right

Function

The **display voice conference-custom-right** command displays default 32-level rights configured for conferences globally.

Format

display voice conference-custom-right

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display default 32-level rights configured for conferences.

```
<Huawei> display voice conference-custom-right
 Conference callright out (custom):  c2&c4
```

16.5.10.15 display voice conference-id-length

Function

The **display voice conference-id-length** command displays the conference ID length that is set globally.

Format

display voice conference-id-length

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the conference ID length.

```
<Huawei> display voice conference-id-length
 The length of conference ID is 2
```

16.5.10.16 display voice conference-out-right

Function

The **display voice conference-out-right** command displays the default conference call-out rights that is set globally.

Format

display voice conference-out-right

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To display the default conference call-out rights that is set globally, run the **display voice conference-out-right** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the conference call-out rights.

```
<Huawei> display voice conference-out-right
 Conference callright out (ddd)  :  Enable
 Conference callright out (idd)  :  Disable
 Conference callright out (inter):  Enable
 Conference callright out (local):  Enable
```

16.5.10.17 display voice conference-reconvoke-attempts

Function

The **display voice conference-reconvoke-attempts** command displays the number of attempts to reconvene a scheduled conference upon a convening failure.

Format

display voice conference-reconvoke-attempts

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the attempts to reconvene a scheduled conference.

```
<Huawei>display voice conference-reconvoke-attempts
 The reconvoke attempts for conference is 6
```

16.5.10.18 dn-set

Function

The **dn-set** command configures the dialing plan set information about a conference.

Format

dn-set *dn-set-name*

undo dn-set

Parameters

Parameter	Description	Value
dn-set-name	Specifies the dialing plan name.	The value is a string of 1 to 32 characters.

Views

Conference view

Default Level

2: Configuration level

Usage Guidelines

This command is optional.

When you configure this command, ensure that a DN set is configured for the enterprise to which the conference belongs.

Example

#Create a conference named **myconference** and set the conference DN set to **abcd-dnset**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference myconference
[Huawei-voice-conference-myconference] dn-set abcd-dnset
```

Restore the default DN set of a conference.

```
[Huawei-voice-conference-myconference] undo dn-set
```

16.5.10.19 out-right

Function

The **out-right** command configures the outgoing right of conference globally.

The **undo out-right** command restores the outgoing right of conference globally to the default value.

By default, the outgoing right is inter and local.

Format

out-right { { **inter** *inter-value* | **local** *local-value* | **ddd** *ddd-value* | **idd** *idd-value* } * | **all** *all-value* }

undo out-right { **inter** | **local** | **ddd** | **idd** | **all** }

Parameters

Parameter	Description	Value
inter *inter-value*	Specifies the internal dialing outgoing right.	Enumerated type. The options are as follows: ● disable ● enable
local *local-value*	Specifies the local dialing outgoing right.	Enumerated type. The options are as follows: ● disable ● enable
ddd *ddd-value*	Specifies the domestic direct dialing outgoing right.	Enumerated type. The options are as follows: ● disable ● enable
idd *idd-value*	Specifies the international direct dialing outgoing right.	Enumerated type. The options are as follows: ● disable ● enable
all *all-value*	Specifies all (inter&local&ddd&idd) outgoing rights.	Enumerated type. The options are as follows: ● disable ● enable

Views

Conference attribute view

Default Level

2: Configuration level

Usage Guidelines

The conference outgoing rights are controlled to avoid toll fraud using conference calls.

Example

Enable all the conference outgoing rights, and then disable idd outgoing right.

```
<Huawei> system-view
[Huawei] voice
[Huawei] conference-attribute
[Huawei-voice-conference-attribute] out-right all enable
```

 Copyright © Huawei Technologies Co., Ltd.

16.5.10.20 regnum

Function

The **regnum** command configures the maximum number of registered users of a conference.

The **undo regnum** command restores the maximum number of registered users of a conference to the default value.

By default, the maximum number of registered users of a conference is 3.

Format

regnum *regnum-value*

undo regnum

Parameters

Parameter	Description	Value
regnum-value	Specifies the maximum number of registered users of a conference.	The value is a string of 3 to x characters. x depends on the product model. AR150: 3 AR200: 6 AR1200: 12 AR2204: 6 AR2220, AR2220L: 12 AR2240: 30 AR3260: 30

Views

Conference view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create a conference named **myconference** and set the maximum number of registered users of the conference to 10.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference myconference
[Huawei-voice-conference-myconference] regnum 10
```

Restore the maximum number of registered users of the conference to its default value.

```
[Huawei-voice-conference-myconference] undo regnum
```

16.5.10.21 schedule

Function

The **schedule** command configures the start time and end time of a conference.

Format

schedule from [*from-date*] *from-time* **to** [*to-date*] *to-time*

Parameters

Parameter	Description	Value
from	Configures the start time.	-
from-date	Specifies the start date.	Date type, in the format of YYYY-MM-DD.
from-time	Specifies the start time.	Time type, in the format of HH:MM:SS.
to	Configures the end time.	-
to-date	Specifies the end date.	Date type, in the format of YYYY-MM-DD.
to-time	Specifies the end time.	Time type, in the format of HH:MM:SS.

Views

Conference view

Default Level

2: Configuration level

Usage Guidelines

This is the core configuration.

- The start time and end time are mandatory. If the start date and end date are not specified, the conference starts and ends in the current day.

- You can schedule a conference only seven days in advance.
- The conference cannot last for more than 24 hours.
- If the start time is earlier than the current system time, the system time is used as the start time by default.

Example

Create a conference named **myconference** and set the conference duration to 10 a.m. to 12 p.m. on 2013-10-14.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] conference myconference
[Huawei-voice-conference-myconference] schedule from 2013-10-14 10:00:00 to 2013-10-14 12:00:00
```

16.5.11 Self Service Http Server Commands

16.5.11.1 display voice self-service-http-server

Function

The **display voice self-service-http-server** command displays the self-service HTTP server configuration.

Format

display voice self-service-http-server

Parameters

None

Views

Self-service HTTP server configuration view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the self-service HTTP server configuration.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]self-service-http-server
[Huawei-voice-self-service-http-server]display voice self-service-http-server
  Self service HTTP server status    : Disable        (default: disable)
  Self service HTTP server port      : 1080           (default: 1080)
```

```
Self service HTTPS server status   : Disable        (default: disable)
Self service HTTPS server port     : 1443           (default: 1443)
```

16.5.11.2 self-service-http-server

Function

The **self-service-http-server** command displays the self-service HTTP server configuration view.

The **undo self-service-http-server** command deletes the self-service HTTP server configuration view.

Format

self-service-http-server

undo self-service-http-server

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Run this command when using the voice self-service to enter the self-service HTTP server configuration view.

Example

Enter the voice HTTP server configuration view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]self-service-http-server
[Huawei-voice-self-service-http-server]
```

16.5.11.3 self-service http server enable

Function

The **self-service http server enable** command starts the self-service HTTP server.

The **undo self-service http server enable** command stops the self-service HTTP server.

By default, the self-service HTTP server is disabled.

Format

self-service http server enable

undo self-service http server enable

Parameters

None

Views

Self-service HTTP server configuration view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Start the self-service HTTP server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]self-service-http-server
[Huawei-voice-self-service-http-server]self-service http server enable
 This operation will take several minutes, please wait...
 Info: Succeeded in starting the self service HTTP server
```

16.5.11.4 self-service http server port

Function

The **self-service http server port** command configures the self-service HTTP server port.

The **undo self-service http server port** command deletes the self-service HTTP server port.

Format

self-service http server port *port-value*

undo self-service http server port

Parameters

Parameter	Description	Value
port-value	Specifies the self-service HTTP server port.	The value is an integer that ranges from 1025 to 51200. The default value is 1080.

Views

Self-service HTTP server configuration view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Change the self-service HTTP server port to 1500.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]self-service-http-server
[Huawei-voice-self-service-http-server]self-service http server port 1500
```

16.5.11.5 self-service http secure-server enable

Function

The **self-service http secure-server enable** command enables the self-service HTTPS server.

The **undo self-service http secure-server enable** command disables the self-service HTTPS server.

By default, the self-service HTTPS server is disabled.

Format

self-service http secure-server enable

undo self-service http secure-server enable

Parameters

None

Views

Self-service HTTP server configuration view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the self-service HTTPS server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]self-service-http-server
[Huawei-voice-self-service-http-server]self-service http secure-server enable
 This operation will take several minutes, please wait...
 Info: Succeeded in starting the self service HTTPS server
```

16.5.11.6 self-service http secure-server port

Function

The **self-service http secure-server port** command configures the self-service HTTPS server port.

The **undo self-service http secure-server port** command deletes the self-service HTTPS server port.

Format

self-service http secure-server port *port-value*

undo self-service http secure-server port

Parameters

Parameter	Description	Value
port-value	Specifies the self-service HTTPS server port.	The value is an integer that ranges from 1025 to 51200. The default value is 1443.

Views

Self-service HTTP server configuration view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Change the self-service HTTPS server port to 1600.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] self-service-http-server
[Huawei-voice-self-service-http-server] self-service http secure-server port 1600
```

16.5.12 Group Registrar Configuration Commands

16.5.12.1 bind trunk-group (group resistrar view)

Function

Using the **bind trunk-group** command, you can associate a group registrar with a specified SIP PRA trunk group so that registration status is kept consistent between users under the group registrar and the SIP PRA trunk group. By default, this function is not configured for users.

Using the **undo bind trunk-group** command, you can remove the association between a group registrar and a SIP PRA trunk group.

Format

bind trunk-group *trunk-group-name*

undo bind trunk-group

Parameters

Parameter	Description	Value
trunk-group-name	Specifies the SIP PRA trunk group name.	The value is a string of 1 to 32 characters.

Views

Group registrar view

Default Level

2: Configuration level

Usage Guidelines

This command is generally used in the eSBC scenario for conversion between public and private networks. This command ensures that the registration status of the IP PBX with the AR is consistent with that of the AR with the IMS.

Example

Keep registration status of users under group registrar **example** to be consistent with that of a SIP PRA trunk.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] groupreg example
[Huawei-voice-groupreg-example] bind trunk-group sippra
```

16.5.12.2 display voice groupreg

Function

Using the **display voice groupreg** command, you can view configurations of a group registrar.

Format

display voice groupreg [*groupreg-name*]

Parameters

Parameter	Description	Value
groupreg-name	Specifies the group registrar name.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

If no group registrar name is specified, configurations of all group registrars are displayed.

Example

View configurations of group registrar **example**.

```
<Huawei> display voice groupreg example
 Group reg name          : example
```

```
IMPI                    : 28988000
IMPU                    : 2898800!.*!
Register password       : ******
Pbx user                : 28988000
Pbx user                : 28988001
Pbx user                : 28988002
Pbx user                : 28988003
Pbx user                : 28988004
Pbx user                : 28988005
Pbx user                : 28988006
Pbx user                : 28988007
Pbx user                : 28988008
Pbx user                : 28988009
Trunk group             : sippra
```

Table 16-103 Description of the display voice groupreg command output

Item	Description
Group reg name	Group registrar name.
IMPI	IMPI of the group registrar.
IMPU	IMPU of the group registrar.
Register password	Authentication password of the group registrar.
Pbx user	User under the group registrar.
Trunk group	Trunk group associated with the group registrar.

16.5.12.3 display voice groupreg pbxuser brief

Function

Using the **display voice groupreg pbxuser brief** command, you can view registration information about users under a group registrar.

Format

display voice groupreg *groupreg-name* **pbxuser brief**

Parameters

Parameter	Description	Value
groupreg-name	Specifies the group registrar name.	The value is a string of 1 to 32 characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays registration information about users under a group registrar.

Example

View registration information about users under group registrar **example**.

```
<Huawei> display voice groupreg example pbxuser brief
 Spec: 256, Records: 10
 --------------------------------------------------------------------------------
 Index Telno    Service-status SIPUE          Expires(s) Interval(s) Reg-status
 0     28988000 Idle           192.168.0.1:5080 428       600         In service
 1     28988001 Idle           192.168.0.1:5080 428       600         In service
 2     28988002 Idle           192.168.0.1:5080 428       600         In service
 3     28988003 Idle           192.168.0.1:5080 428       600         In service
 4     28988004 Idle           192.168.0.1:5080 428       600         In service
 5     28988005 Idle           192.168.0.1:5080 428       600         In service
 6     28988006 Idle           192.168.0.1:5080 428       600         In service
 7     28988007 Idle           192.168.0.1:5080 428       600         In service
 8     28988008 Idle           192.168.0.1:5080 428       600         In service
 9     28988009 Idle           192.168.0.1:5080 428       600         In service
```

Table 16-104 Description of the display voice groupreg pbxuser brief command output

Item	Description
Index	Index number.
Telno	User number.
Service-status	Service status.
SIPUE	Registration source.
Expires(s)	Remaining time before registration times out, in seconds.
Interval(s)	Registration interval, in seconds.
Reg-status	Registration status.

16.5.12.4 groupreg

Function

Using the **groupreg** command, you can configure a group registrar and enter the group registrar view.

Using the **undo groupreg** command, you can delete group registrar configurations.

By default, no group registrar data is configured.

Format

groupreg *groupreg-name*

undo groupreg *groupreg-name*

Parameters

Parameter	Description	Value
groupreg-name	Specifies the group registrar name.	The value is a string of 1 to 32 characters without spaces.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

A group registrar is used for connecting to the SIP PRA trunk in a simple way, that is, allocating numbers to the downlink SIP PRA trunk.

Example

Configure a group registrar named **example** and enter the group registrar view.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] groupreg example
[Huawei-voice-groupreg-example]
```

16.5.12.5 home-domain (group resistrar view)

Function

Using the **home-domain** command, you can configure the domain name in group registration.

Using the **undo home-domain** command, you can delete the domain name configured in group registration.

Format

home-domain *home-domain-value*

undo home-domain

Parameters

Parameter	Description	Value
home-domain-value	Indicates the domain name.	The value is a string of 1 to 32 characters.

Views

Group registrar view

Default Level

2: Configuration level

Usage Guidelines

The **home-domain** command is generally used in the scenario of SIP PRA registration under eSBC. When multiple IP PBXs register with the AR in SIP PRA mode, you can run this command to specify the domain name of the IP PBX to which calls are sent.

Example

Set the domain name for group registration **example** to **example.com**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] groupreg example
[Huawei-voice-groupreg-example] home-domain example.com
```

16.5.12.6 impi

Function

Using the **impi** command, you can configure the IMPI of a group registrar.

Using the **undo impi** command, you can delete the IMPI of a group registrar.

Format

impi *impi-value* **impu** *impu-value* [**password cipher** *cipher-password-value*]

undo impi [**password**]

Parameters

Parameter	Description	Value
impi-value	Specifies the IMPI of the group registrar.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
impu-value	Specifies the IMPU of the group registrar.	The value is a string of 1 to 32 characters.
cipher-password-value	Specifies the authentication password of the group registrar. **NOTE** You can configure *password-value* after and inputting **cipher** and pressing **Enter**.	The value is a string of 6 to 32 characters.

Views

Group registrar view

Default Level

2: Configuration level

Usage Guidelines

You must configure the IMPU for a group registrar with the IMPI configured. A group registrar with the IMPU configured is considered as a wildcard registrar. A group registrar with no IMPU configured is considered as an implicit registrar.

The maximum number of users supported by an implicit registrar is less than that supported by a wildcard registrar. If the number of configured users under a group registrar exceeds that supported by an implicit registrar, you cannot directly delete the IMPI. To delete the IMPI, you must first delete excess users under the group registrar.

NOTE

- If the **password** parameter is not specified, the **undo impi** [**password**] command deletes the IMPI of the group registrar; if the **password** parameter is specified, the command deletes only the authentication password configured for the group registrar.

Example

Set the IMPI of group registrar **example** to **28988000** and the corresponding IMPU to **2898800!.*!**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] groupreg example
[Huawei-voice-groupreg-example] impi 28988000 impu 2898800!.*!
```

16.5.12.7 pbxuser

Function

Using the **pbxuser** command, you can configure users under a group registrar.

Using the **undo pbxuser** command, you can delete users from a group registrar.

Format

pbxuser *user-name* [**step** *step-value*] [**number** *number-value*]

undo pbxuser *user-name* [**step** *step-value*] [**number** *number-value*]

Parameters

Parameter	Description	Value
user-name	Specifies the user name.	The value is a string of 1 to 32 characters. **NOTE** If the user has not been configured, the user name must be set to a value consisting of only digits or a value starting with the plus sign (+) followed by all digits. (Only the 1220EV, 1220EVW, and 161FGV-L support the user who has not been configured.)
step-value	Specifies the step for adding users in a batch.	The value is an integer that ranges from 1 to 1000.
number-value	Specifies the number of users added in a batch.	The value is an integer that ranges from 1 to *N*. **NOTE** *N* indicates the maximum number of users supported by the device minus the number of configured users.

Views

Group registrar view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Add users 28988000 to 28988009 to a group registrar.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] groupreg example
[Huawei-voice-groupreg-example] pbxuser 28988000 number 10
```

16.6 SIP AG Commands

Function Description

SIP AG commands are used to configure SIP AG parameters and SIP AG users.

NOTE

- The following product models support voice functions (such as the PBX, SIP AG, and H.248 AG):
  - AR120 series: AR129CV, AR129CVW, and AR129CGVW-L
  - AR150 series: AR157VW and AR158EVW
  - AR160 series: AR161, AR169FVW, AR169FVW-8S, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR161FV-1P, and AR169FGVW-L
  - AR200 series: AR201VW-P, AR207V, AR207VW, and AR207V-P
  - AR1200 series: AR1220V, AR1220VW, AR1220EV, and AR1220EVW
  - AR2200 series: AR2204, AR2220, AR2220L, AR2220E.
  - AR2240: For the equipped with SRU40, SRU60, SRU80, and SRU100.
  - AR3200 series: For the AR3260 equipped with SRU40, SRU60, SRU80, or SRU100, the same voice mode is set for the active and standby SRUs.

  The AR129CV, AR129CVW, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, and AR169CVW-4B4S only support the PBX and SIP AG, but not the H.248 AG.
- When an AR2204, AR2220L, or AR2220E router needs to provide voice services, install a DSP module and a voice subcard in the router. When an AR2220, AR2240, or AR3200 router needs to provide voice services, install a DSP module.
- To provide voice services to POTS users on the AR1200, AR2200, or AR3200, install the 4FXS1FXO, 16FXS, or 32FXS card. The AR1200 does not support the 32FXS card.
- To provide voice services to ISDN phone users on the AR1200, AR2200, or AR3200, install the 2BST card.
- To connect an AR1200, AR2200, or AR3200 router to a TDM PBX through the E1 interface, install the E1T1-M card.
- On the AR169FGVW-L, AR1220EV, and AR1220EVW, the AT0 trunk cannot be connected to the SIP server or SIP trunk.

16.6.1 SIP AG Parameter Configuration Commands

Function Description

This section describes the commands used to configure SIP AG parameters.

16.6.1.1 ag number-parameter

Function

Using the **ag number-parameter** command, you can set control points for a SIP AG.

Using the **undo ag number-parameter** command, you can restore the default control points of a SIP AG.

Format

ag number-parameter *name value*

undo ag number-parameter *name*

Parameters

Parameter	Description	Value
name	Specifies the name of a control point.	The value is an integer that ranges from 0 to 27.
value	Specifies the value of a control point.	The value is an integer. Values vary according to control points.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The following table describes the meanings and values of control points.

Parameter	Description	Value
0	Tone type for local blocking.	The value is an integer that ranges from 0 to 4: ● 0: busy tone ● 1: device congestion tone ● 2: silence ● 3: user-defined tone 1 ● 4: user-defined tone 2 The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
1	Tone type for remote blocking.	The value is an integer that ranges from 0 to 4: ● 0: busy tone ● 1: device congestion tone ● 2: silence ● 3: user-defined tone 1 ● 4: user-defined tone 2 The default value is 0.
2	Whether auto-switching is supported.	The value can be 0 or 1: ● 0: indicates that auto-sensing is not supported. ● 1: indicates that auto-sensing is supported. The default value is 0.
3	Ordinary call control mode.	The value is an integer that ranges from 0 to 2: ● 0: indicates that calls are not controlled. ● 1: indicates that outgoing calls are controlled. ● 2: indicates that incoming calls are controlled. The default value is 0.
4	Emergency call control mode.	The value is an integer that ranges from 0 to 2: ● 0: indicates that calls are not controlled. ● 1: indicates that outgoing calls are controlled. ● 2: indicates that incoming calls are controlled. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
5	Emergency call silence compression.	The value can be 0 or 1: ● 0: indicates that emergency call silence compression is disabled forcibly. ● 1: indicates that emergency call silence compression is not controlled. The default value is 0.
6	It is reserved.	-
7	It is reserved.	-
8	It is reserved.	-
9	It is reserved.	-
10	It is reserved.	-
11	It is reserved.	-
12	It is reserved.	-
13	Digitmap matching mode.	The value can be 0 or 1: ● 0: indicates minimum matching. ● 1: indicates maximum matching. The default value is 0.
14	It is reserved.	-
15	Whether RTP filtering is supported. Specify this parameter when RTP filtering needs to be configured on a SIP AG. After RTP filtering is used, only the media streams from a specified interface are accepted.	The value can be 0 or 1: ● 0: indicates that RTP filtering is not supported. ● 1: indicates that RTP filtering is supported. The default value is 0.
16	It is reserved.	-
17	It is reserved.	-
18	It is reserved.	-
19	It is reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
20	It is reserved.	-
21	It is reserved.	-
22	It is reserved.	-
23	Registration lifecycle.	The value is an integer ranging from 1 to 65534, in seconds. The default value is 600.
24	Mode in which QoS statistics are reported.	The value can be 0 or 1: ● 0: indicates the T1 mode. ● 1: indicates that QoS statistics are not reported. The default value is 1.
25	Whether to convert pulse signals into DTMF signals.	The value can be 0 or 1: ● 0: disable ● 1: enable The default value is 0.
26	Register retry interval.	The value is an integer ranging from 1 to 65535, in seconds. The default value is 30.
27	Hotline time length.	The value is an integer ranging from 1 to 255, in seconds. The default value is 5.

Example

Enable a SIP AG to convert pulse signals into DTMF signals.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] ag number-parameter 25 1
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.2 ag string-parameter

Function

Using the **ag string-parameter** command, you can set string parameters for a SIP AG.

Using the **undo ag string-parameter** command, you can restore the default string parameters of a SIP AG.

Format

ag string-parameter *strpara-name strpara-value*

undo ag string-parameter *strpara-name*

Parameters

Parameter	Description	Value
strpara-name	Specifies the sequence number of a string parameter.	The value is an integer ranging from 1 to 38.
strpara-value	Specifies the value of a string parameter.	The value is a string of 1 to 64 characters.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The following table describes the meanings and values of string parameters.

Parameter	Description	Value
1	Visited network ID.	The value is a string of 1 to 64 characters. The default value is an empty string.
2	Prefix of the national toll call.	The value is a string of 1 to 64 characters. The default value is an empty string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
3	Prefix of the international toll call.	The value is a string of 1 to 64 characters. The default value is an empty string.
4	CC number string.	The value is a string of 1 to 64 characters. The default value is an empty string.
5	NDC number string.	The value is a string of 1 to 64 characters. The default value is an empty string.
6	SCC domain name.	The value is a string of 1 to 64 characters. The default value is an empty string.
7	It is reserved.	-
8	It is reserved.	-
9	It is reserved.	-
10	It is reserved.	-
11	String indicating that the Calling Line Identification Presentation (CLIP) function is unavailable.	The value is a string of 1 to 64 characters. The default value is an empty string.
12	It is reserved.	-
13	String indicating that the CLIP function is restricted.	The value is a string of 1 to 64 characters. The default value is an empty string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
14	SCC number of the MCID service. When the MCID service is triggered in SCC mode, check this parameter to determine whether the MCID service is triggered: ● If this parameter is set and the SCC number is the same as the parameter value, the MCID service is triggered. If the SCC number is different from the parameter value, the MCID service is not triggered. ● If this parameter is not set, the MCID service cannot be triggered.	The value is a string of 1 to 64 characters. The default value is an empty string.
15	SCC number indicating that Call Forwarding Unconditional (CFU) is activated. According to the SCC number, a SIP AG analyzes the CFU operation and records its status to determine whether to play the special dial tone.	The value is a string of 1 to 64 characters. The default value is an empty string.
16	SCC number indicating that CFU is deactivated. According to the SCC number, a SIP AG analyzes the CFU operation and records its status to determine whether to play the special dial tone.	The value is a string of 1 to 64 characters. The default value is an empty string.
17	SDP owner name.	The value is a string of 1 to 64 characters. The default value is an empty string.
18	SDP session name string.	The value is a string of 1 to 64 characters. The default value is an empty string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
19	It is reserved.	-
20	Contents of a hookflash pressing event.	The value is a string of 1 to 64 characters. The default value is an empty string.
21	CAT1 ordinary call Resource-Priority header field.	The value is a string of 1 to 64 characters. The default value is an empty string.
22	CAT2 ordinary call Resource-Priority header field.	The value is a string of 1 to 64 characters. The default value is an empty string.
23	CAT3 ordinary call Resource-Priority header field.	The value is a string of 1 to 64 characters. The default value is an empty string.
24	CAT1 emergency call Resource-Priority header field.	The value is a string of 1 to 64 characters. The default value is an empty string.
25	CAT2 emergency call Resource-Priority header field.	The value is a string of 1 to 64 characters. The default value is an empty string.
26	CAT3 emergency call Resource-Priority header field.	The value is a string of 1 to 64 characters. The default value is an empty string.
27	Service domain in the URI of the Route header field.	The value is a string of 1 to 64 characters. The default value is an empty string.
28	Service activation SCC code 1. If multiple services need to be activated, they are separated by a semicolon. The first service is CW.	The value is a string of 1 to 64 characters. The default value is an empty string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
29	Service deactivation SCC code 2. If multiple services need to be activated, they are separated by a semicolon. The first service is CW.	The value is a string of 1 to 64 characters. The default value is an empty string.
30	It is reserved.	-
31	Activation code of user-defined event SCC1 code. If this parameter is matched, SIP_SEVENT_CUSTOM_SCC1 occurs. This string can contain parameters. For example, the value *12*(*.)# indicates that SIP_SEVENT_CUSTOM_SCC1 occurs and parameters matching *. are contained.	The value is a string of 1 to 64 characters. The default value is an empty string.
32	Activation code of user-defined event SCC2 code. If this parameter is matched, SIP_SEVENT_CUSTOM_SCC2 occurs. This string can contain parameters. For example, the value *12*(*.)# indicates that SIP_SEVENT_CUSTOM_SCC2 occurs and parameters matching *. are contained.	The value is a string of 1 to 64 characters. The default value is an empty string.
33	Activation code of user-defined event SCC3 code. This parameter is reserved.	The value is a string of 1 to 64 characters. The default value is an empty string.
34	P-Access-Network-Info header field of POTS.	The value is a string of 1 to 64 characters. The default value is an empty string.
35	P-Access-Network-Info header field of BRI.	The value is a string of 1 to 64 characters. The default value is an empty string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
36	P-Access-Network-Info header field of PRI.	The value is a string of 1 to 64 characters. The default value is an empty string.
37	Default hotline address.	The value is a string of 1 to 64 characters. The default value is an empty string.
38	It is reserved.	-

Precautions

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the CAT2 Resource-Priority header field to **huawei.em2** for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] ag string-parameter 25 huawei.em2
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.3 ag-domain

Function

Using the **ag-domain** command, you can configure a domain name for a SIP AG.

Using the **undo ag-domain** command, you can delete a domain name of a SIP AG.

By default, no domain name is configured for a SIP AG.

Format

ag-domain *ag-domain-name*

undo ag-domain

Parameters

Parameter	Description	Value
ag-domain-name	Specifies the domain name of a SIP AG.	The value is a string of 1 to 64 case-sensitive characters.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure a domain name **abcd.com** for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] ag-domain abcd.com
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.4 auth mode

Function

The **auth mode** command configures the authentication mode for a SIP AG.

The **undo auth mode** command restores the default authentication mode of a SIP AG.

By default, the authentication mode of a SIP AG is **user**.

Format

auth mode *mode-value*

undo auth mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mode-value	Specifies the authentication mode for a SIP AG.	Enumerated type. The values are as follows: • interface: configures all the users connected to a SIP AG to share the same authentication user name. • user: specifies an IP Multimedia Subsystem Private Identity (IMPI) for a user.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Configure all the users connected to a SIP AG to share the same authentication user name.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] auth mode interface
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.5 auth (SIP AG view)

Function

The **auth** command configures the authentication user name and password for a SIP AG.

The **undo auth** command deletes the authentication user name and password of a SIP AG.

By default, no authentication user name or password is configured for a SIP AG.

Format

auth username *auth-username* **password** { **cipher** *cipher-password* | **ha1 cipher** *cipher-password* }

undo auth

Parameters

Parameter	Description	Value
auth-username	Specifies the authentication user name.	The value is a string of 1 to 64 characters without question mark and spaces.
password	Specifies the authentication password.	-
cipher *cipher-password*	Indicates the password in cipher text. **NOTE** You can configure *cipher-password* after inputting **cipher** and pressing **Enter**.	The *cipher-password* value is a string of case-sensitive characters without spaces. A cipher password may contain 1 to 64 encrypted characters. The input character string - indicates that the password is empty.
ha1 cipher *cipher-password*	Indicates the password in HA1 mode.	The *cipher-password* value is a string of case-sensitive characters without spaces. A cipher password may contain 1 to 32 encrypted characters. The input character string - indicates that the password is empty.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

To authenticate a SIP AG user, configure the user name and password for the SIP AG.

If you run the **auth** command multiple times in the same SIP AG view, only the latest configuration takes effect.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the authentication user name **huawei**, and password to 1234 for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] auth username huawei password cipher
Please input user password(1-64 chars):****
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.4 auth mode

16.6.1.6 conference-factory-uri

Function

Using the **conference-factory-uri** command, you can configure the conference factory URI for a SIP AG.

Using the **undo conference-factory-uri** command, you can delete the conference factory URI of a SIP AG.

By default, no conference factory URI is configured for a SIP AG.

Format

conference-factory-uri *uri*

undo conference-factory-uri

Parameters

Parameter	Description	Value
uri	Specifies the conference factory URI for a SIP AG.	The value is a string of 1 to 64 case-sensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

When a SIP AG subscribes to the conference service, you must configure a conference factory URI for the SIP AG; otherwise, the SIP AG cannot use the conference service.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the conference factory URI **confac** for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] conference-factory-uri confac
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.7 description (SIP AG view)

Function

Using the **description** command, you can configure the description for a SIP AG.

Using the **undo description** command, you can delete the description of a SIP AG.

By default, a SIP AG has no description.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description for a SIP AG.	The name is a string of 1 to 32 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **description** command configures the description for a SIP AG and helps to manage the SIP AG.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the description **hotel105** for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] description hotel105
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.8 digitmap-timer

Function

Using the **digitmap-timer** command, you can set the timers for a SIP AG.

Using the **undo digitmap-timer** command, you can restore the default timer values of a SIP AG.

For the default timer values, see the parameter description.

Format

digitmap-timer { **long** *long-timer-value* | **short** *short-timer-value* | **start** *start-timer-value* }

undo digitmap { **long** | **short** | **start** }

Parameters

Parameter	Description	Value
long *long-timer-value*	Specifies the value for a digitmap long timer.	The value is an integer that ranges from 1 to 99, in seconds. The default value is 20.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
short *short-timer-value*	Specifies the value for a digitmap short timer.	The value is an integer that ranges from 1 to 99, in seconds. The default value is 4.
start *start-timer-value*	Specifies the value for a digitmap start timer.	The value is an integer that ranges from 0 to 99, in seconds. The default value is 20.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

Timers configured using the **digitmap** command are used in the following situations:

- The digitmap start timer is used when a user has picked up the phone but has not dialed any number.
- The digitmap short timer is used when the collected number has matched at least one dialing scheme but more numbers may be received and match other dialing schemes.
- The digitmap long timer is used when the dialed number does not match any dialing scheme.

Example

Set the value for a digitmap short timer of a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] digitmap-timer short 5
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.9 display voice media-bandwidth-control (SIP AG)

Function

The **display voice media-bandwidth-control** command displays CAC configurations and uplink bandwidth occupied by voice data on a SIP AG.

Format

display voice media-bandwidth-control

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display CAC configurations and uplink bandwidth occupied by voice data on the SIP AG.

```
<Huawei> display voice media-bandwidth-control
 Upward bandwidth                        : enable
 The maximum upward bandwidth            : 500000 kbit/s
 The used normal bandwidth               : 0 kbit/s
```

Table 16-105 Description of the display voice media-bandwidth-control command output

Item	Description
Upward bandwidth	Whether CAC is enabled on the SIP AG: ● Enable ● Disable To enable CAC on the SIP AG, run the **16.6.1.44 media-bandwidth-control enable (SIPAG)** command.
The maximum upward bandwidth	Maximum uplink media bandwidth occupied by voice data. To set the maximum uplink media bandwidth, run the **16.6.1.45 media-bandwidth-control max-bandwidth (SIPAG)** command.
The used normal bandwidth	Uplink media bandwidth occupied by voice data.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.44 media-bandwidth-control enable (SIPAG)

16.6.1.45 media-bandwidth-control max-bandwidth (SIPAG)

16.6.1.10 display voice local-digitmap

Function

Using the **display voice local-digitmap** command, you can view information about a local digitmap configured on a SIP AG.

Format

display voice local-digitmap [*local-digitmap-name*]

Parameters

Parameter	Description	Value
local-digitmap-name	Specifies the name of a digitmap.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

3: Management level

Usage Guidelines

When a calling user fails to be connected to the called user or waits for a long period of time after dialing the called number, run the **display voice local-digitmap** command to view the configurations of local digitmaps on the SIP AG. You can rectify the fault according to the command output.

If *local-digitmap-name* is not specified, all local digitmaps are displayed.

Example

Display information about a local digitmap on a SIP AG.

```
<Huawei> display voice local-digitmap huawei
  Name : huawei
  Type : Normal
  Body : 8888xxxx
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-106 Description of the display voice local-digitmap command output

Item	Description
Name	Indicates the name of a SIP AG digitmap.
Type	Indicates the digitmap type.
Body	Indicates the body of a SIP AG digitmap.

Related Topics

16.6.1.15 display voice sipag

16.6.1.11 display voice sctp-global-statistics

Function

The **display voice sctp-global-statistics** command displays global Stream Control Transport Protocol (SCTP) statistics.

Format

display voice sctp-global-statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

To view global SCTP statistics, run the **display voice sctp-global-statistics** command.

Example

Display global SCTP statistics.

```
<Huawei> display voice sctp-global-statistics
 Current established associations      : 0
 Active established associations       : 0
 Passive established associations      : 0
 Active associations fails             : 0
 Passive associations fails            : 0
 Associations aborted                  : 0
 Associations shut down                : 0
```

```
Received out of blue chunks          : 0
Sent control chunks                  : 0
Sent ordered data chunks             : 0
Sent unordered data chunks           : 0
Received control chunks              : 0
Received ordered data chunks         : 0
Received unordered data chunks       : 0
Retrains data chunks                 : 0
Fragmented user messages             : 0
Reassembled user messages            : 0
Received checksum error packets      : 0
Sent SCTP packets                    : 0
Received SCTP packets                : 0
```

Table 16-107 Description of the display voice sctp-global-statistics command output

Item	Description
Current established associations	Number of current connections.
Active established associations	Number of connections initiated by the local end.
Passive established associations	Number of connections initiated by the remote end.
Active associations fails	Number of failed connections initiated by the local end.
Passive associations fails	Number of failed connections initiated by the remote end.
Associations aborted	Number of aborted connections.
Associations shut down	Number of connections normally shut down.
Received out of blue chunks	Number of abnormal data blocks received by the local end.
Sent control chunks	Number of sent control data blocks.
Sent ordered data chunks	Number of sent ordered data blocks.
Sent unordered data chunks	Number of sent out-of-order data blocks.
Received control chunks	Number of received control data blocks.
Received ordered data chunks	Number of received ordered data blocks.
Received unordered data chunks	Number of received unordered data blocks.
Retrains data chunks	Number of retransmitted data blocks.
Fragmented user messages	Number of fragmented user messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reassembled user messages	Number of reassembled user messages.
Received checksum error packets	Number of received checksum error packets.
Sent SCTP packets	Number of sent SCTP packets.
Received SCTP packets	Number of received SCTP packets.

Related Topics

16.6.1.81 sipag

16.6.1.12 display voice sip-profile

Function

The **display voice sip-profile** command displays the configuration of a SIP profile.

Format

display voice sip-profile [*index* [**sip-profile-detail**]]

Parameters

Parameter	Description	Value
index	Specifies the index of a SIP profile.	The value is an integer that ranges from 0 to 9.
sip-profile-detail	Displays detailed information about a SIP profile.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To view parameter settings of configured and predefined SIP profiles in the system, run the **display voice sip-profile** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the configurations of SIP profiles.

```
<Huawei> display voice sip-profile 0 sip-profile-detail

  Profile name : Customizing ProfileTemplet
  Profile index: 0

  SysPara:
  SP2  : 1

  Codec Pri:
  Pri: 0    Codec: 8    Pt: 20

  Srv Pri:
  Pri: 0    Srvid: 4

  Reason tone:
  Sameness

  Status tone:
  Sameness
```

Table 16-108 Description of the display voice sip-profile command output

Item	Description
Profile name	Profile name.
Profile index	Profile index.
SysPara	System parameter. System parameters, including system parameter indexes and corresponding values. For example, the index and value of number 2 system parameter are respectively SP2 and 1.
Codec Pri	Codec priority.
Pri	Codec/service priority. The value is an integer that ranges from 0 to 255. A smaller value indicates a higher priority.
Codec	Codec value. The value is an integer that ranges from 0 to 255. Common codecs are G711U (0), G723 (4), G711A (8), and G729 (18).
Pt	Packetization duration. The value is an integer that ranges from 0 to 4294967295. Generally, the value is a multiple of 5. Common packetization durations are 10, 20, and 30 milliseconds.
Srv Pri	Service priority.
Srvid	Service type. The value is an integer that ranges from 0 to 4294967295.
Reason tone	Mapping between status codes carried in the Reason header field and local tones.
Status tone	Mapping between the status code and the local tone.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.1.13 display voice sip-reg-count-per-second

Function

The **display voice sip-reg-count-per-second** command displays the number of SIP register messages sent every second.

Format

display voice sip-reg-count-per-second

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None.

Example

Display the number of SIP register messages sent every second.

```
<Huawei> display voice sip-reg-count-per-second
 Sip register message count per second is 10!
```

16.6.1.14 display voice sip-service-logic

Function

The **display voice sip-service-logic** command displays information about a SIP service logic.

Format

display voice sip-service-logic [*service-logic-index* [*srvid*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
service-logic-index	Specifies the index of a SIP service logic.	The value is an integer that ranges from 0 to 9.
srvid	Specifies the ID of a service type.	The value is an integer that ranges from 0 to 255.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view information about configured and predefined SIP service logics, run the **display voice sip-service-logic** command.

Example

Display information about SIP service logics.

```
<Huawei> display voice sip-service-logic 0
 Srv SrvLogic-Description(SS,LS,EVT,OSS,OEVT:...OEVT,ACT:...ACT)
 SN=0,SS=0,LS=1,EVT=16,OSS=8,OEVT=18:21:22:26,ACT=9,TIMERLEN=0;
 SN=0,SS=1,LS=3,EVT=16,OSS=8,OEVT=18:21:22:26:25,ACT=9,TIMERLEN=0;
 SN=0,SS=1,LS=3,EVT=18,OSS=11,OEVT=19:26:28,ACT=4:45:37:20,TIMERLEN=0;
 SN=0,SS=1,LS=3,EVT=25,OSS=9,OEVT=18:16:23:26,ACT=4:45:37:22,TIMERLEN=0;
 SN=0,SS=1,LS=3,EVT=26,OSS=0,OEVT=16:17,ACT=5,TIMERLEN=0;
 SN=0,SS=1,LS=8,EVT=16,OSS=8,OEVT=18:21:22:24,ACT=57,TIMERLEN=0;
 SN=0,SS=1,LS=8,EVT=18,OSS=0,OEVT=16:17,ACT=19,TIMERLEN=0;
 SN=0,SS=1,LS=8,EVT=24,OSS=0,OEVT=16:17,ACT=25:19,TIMERLEN=0;
 SN=0,SS=2,LS=2,EVT=15,OSS=10,OEVT=18:16:29:27:26,ACT=13:41:46:38,TIMERLEN=0;
 SN=0,SS=2,LS=2,EVT=16,OSS=0,OEVT=16:17,ACT=23:28:11,TIMERLEN=0;
 SN=0,SS=2,LS=2,EVT=18,OSS=11,OEVT=19:26:28,ACT=23:28:20,TIMERLEN=0;
 SN=0,SS=2,LS=2,EVT=20,OSS=9,OEVT=18:16:23:26,ACT=22,TIMERLEN=0;
 SN=0,SS=2,LS=2,EVT=26,OSS=0,OEVT=16:17,ACT=23:28:5,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=0,OSS=0,OEVT=16:17,ACT=12:5,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=1,OSS=0,OEVT=16:17,ACT=4:45:37:11,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=2,OSS=1,OEVT=18:16:25:26,ACT=40:37:45:12,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=3,OSS=13,OEVT=18:29:25:26:24,ACT=40:17:35,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=16,OSS=1,OEVT=18:16:25:26,ACT=23:28:12,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=18,OSS=11,OEVT=19:26:28,ACT=23:28:4:45:37:20,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=20,OSS=9,OEVT=18:16:23:26:25,ACT=22,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=25,OSS=9,OEVT=18:16:23:26,ACT=23:28:4:45:37:22,TIMERLEN=0;
 SN=0,SS=3,LS=3,EVT=26,OSS=0,OEVT=16:17,ACT=23:28:12:5,TIMERLEN=0;
 SN=0,SS=4,LS=8,EVT=6,OSS=7,OEVT=18:16:15:20:24,ACT=3,TIMERLEN=0;
 SN=0,SS=4,LS=8,EVT=14,OSS=1,OEVT=18:24,ACT=58:13,TIMERLEN=0;
 SN=0,SS=4,LS=8,EVT=16,OSS=1,OEVT=18:16:24,ACT=23:28:58,TIMERLEN=0;
 SN=0,SS=4,LS=8,EVT=18,OSS=0,OEVT=16:17,ACT=19,TIMERLEN=0;
 SN=0,SS=4,LS=8,EVT=20,OSS=1,OEVT=18:16:24,ACT=58,TIMERLEN=0;
 SN=0,SS=4,LS=8,EVT=24,OSS=0,OEVT=16:17,ACT=25:19,TIMERLEN=0;
 SN=0,SS=7,LS=8,EVT=15,OSS=14,OEVT=18:24:30:31,ACT=58:18,TIMERLEN=0;
 SN=0,SS=7,LS=8,EVT=16,OSS=1,OEVT=18:16:24,ACT=23:28:58,TIMERLEN=0;
```

 Copyright © Huawei Technologies Co., Ltd.

```
SN=0,SS=7,LS=8,EVT=18,OSS=0,OEVT=16:17,ACT=19,TIMERLEN=0;
SN=0,SS=7,LS=8,EVT=20,OSS=9,OEVT=18:16:24:23,ACT=22,TIMERLEN=0;
SN=0,SS=7,LS=8,EVT=24,OSS=0,OEVT=16:17,ACT=25:19,TIMERLEN=0;
SN=0,SS=8,LS=2,EVT=18,OSS=0,OEVT=16:17,ACT=19,TIMERLEN=0;
SN=0,SS=8,LS=2,EVT=21,OSS=2,OEVT=18:16:15:20:26,ACT=3,TIMERLEN=0;
SN=0,SS=8,LS=2,EVT=22,OSS=0,OEVT=16:17,ACT=11,TIMERLEN=0;
SN=0,SS=8,LS=2,EVT=26,OSS=0,OEVT=16:17,ACT=5,TIMERLEN=0;
SN=0,SS=8,LS=3,EVT=18,OSS=11,OEVT=19:26:28,ACT=4:45:37:20,TIMERLEN=0;
SN=0,SS=8,LS=3,EVT=21,OSS=3,OEVT=18:16:0:1:2:3:4:20:25:26,ACT=0,TIMERLEN=0;
SN=0,SS=8,LS=3,EVT=22,OSS=1,OEVT=18:16:26:25,ACT=12,TIMERLEN=0;
SN=0,SS=8,LS=3,EVT=25,OSS=9,OEVT=18:16:23:26,ACT=4:45:37:22,TIMERLEN=0;
SN=0,SS=8,LS=3,EVT=26,OSS=0,OEVT=16:17,ACT=12:5,TIMERLEN=0;
SN=0,SS=8,LS=8,EVT=18,OSS=0,OEVT=16:17,ACT=19,TIMERLEN=0;
SN=0,SS=8,LS=8,EVT=21,OSS=4,OEVT=18:14:6:16:20:24,ACT=2,TIMERLEN=0;
SN=0,SS=8,LS=8,EVT=22,OSS=1,OEVT=18:16:24,ACT=58,TIMERLEN=0;
SN=0,SS=8,LS=8,EVT=24,OSS=0,OEVT=16:17,ACT=25:19,TIMERLEN=0;
```

Table 16-109 Description of the display voice sip-service-logic command output

Item	Description
Srv	Service type.
SrvLogic-Description	Service logic description in the format of SS,LS,EVT,OSS,OEVT:...OEVT,ACT:...ACT. ● SS indicates the service status. ● LS indicates the comprehensive status. ● EVT indicates the input event. ● OSS indicates the status of service switching. ● OEVT:...OEVT indicates the observation event list. Each **OEVT** indicates an observation event, and two observation events are separates separated by a colon (:). ● ACT:...ACT indicates the action list. Each **ACT** indicates an action, and two actions are separated by a colon (:).

Related Topics

16.6.1.15 display voice sipag

16.6.1.15 display voice sipag

Function

The **display voice sipag** command displays control points of a SIP AG.

Format

display voice sipag [*sipag-interface-id* { **running** | **config** }]

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.
running	Displays running control points of a SIP AG.	-
config	Displays configured control points of a SIP AG.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To view control points of a specified SIP AG, run the **display voice sipag** command.

Example

Display the configured control points of SIP AG 1.

```
<Huawei> display voice sipag 1 config
  AGID                                : 1
  Dynamic signalling IP address name   :
  Signalling IP                       : 192.168.1.1
  Signalling port                     : 5060
  Dynamic media IP address name        :
  Media IP                            : 192.168.1.1
  Transfer mode                       : TCP
  Primary proxy IP 1                  : 192.168.1.1
  Primary proxy IP 2                  :
  Secondary proxy IP 1                :
  Secondary proxy IP 2                :
  Primary proxy port                  : 5060
  Secondary proxy port                : 65535
  Primary proxy domain name           :
  Secondary proxy domain name         :
  Proxy address mode                  : IP
  Home domain name                    : abcd.com
  SIP profile index                   : 1: Default
  Service logic index                 : 0: Default
  Server Address DHCP option          : 0: None
  Description                         :
  AG domain name                      :
  Phone context                       :
  Register URI                        :
  Conference factory URI              :
  Subscribe to UA profile             : Enable
```

 Copyright © Huawei Technologies Co., Ltd.

```
Subscribe to reg state              : Disable
Subscribe to MWI                    : Disable
SDP negotiation mode                  : Remote
Mode of supporting proxy dual-homing : Manual switch over
Proxy detection mode                  : Probe
Proxy refresh mode                  :
```

Table 16-110 Description of the display voice sipag command output

Item	Description
AGID	SIP AG ID.
Dynamic signalling IP address name	Dynamic signaling IP address.
Signalling IP	Signaling IP address.
Signalling port	Signaling port number.
Dynamic media IP address name	Dynamic media IP address.
Media IP	Media IP address.
Transfer mode	Transmission protocol.
Primary proxy IP 1	IP address 1 of the primary proxy server.
Primary proxy IP 2	IP address 2 of the primary proxy server.
Secondary proxy IP 1	IP address 1 of the secondary proxy server.
Secondary proxy IP 2	IP address 2 of the secondary proxy server.
Primary proxy port	Port number of the primary proxy server.
Secondary proxy port	Port number of the secondary proxy server.
Primary proxy domain name	Domain name of the primary proxy server.
Secondary proxy domain name	Domain name of the secondary proxy server.
Proxy address mode	Mode in which the IP address of a proxy server is obtained.
Home domain name	Home domain name.
SIP profile index	Profile index of the SIP AG.
Service logic Index	Service logic index used by the SIP AG.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Server Address DHCP option	Mode in which DHCP Request packets are sent.
Description	Description of the SIP AG.
AG domain name	Domain name of the SIP AG.
Phone context	Phone context of the SIP AG.
Register URI	URI of a registrar.
Conference factory URI	Conference factory URI of the SIP AG.
Subscribe to UA profile	UA profile subscription function.
Subscribe to reg state	Register status subscription function.
Subscribe to MWI	MWI subscription function.
SDP negotiation mode	Whether the local or remote priority mode is used for SDP negotiation.
Mode of supporting proxy dual-homing	The proxy dual-homing mode is supported.
Proxy detection mode	Proxy detection mode.
Proxy refresh mode	Mode in which the proxy server is switched when the address of the running proxy server is changed.

Related Topics

16.6.1.81 sipag

16.6.1.7 description (SIP AG view)

16.6.1.16 display voice sipag auth

Function

Using the **display voice sipag auth** command, you can view authentication information about a SIP AG.

Format

display voice sipag *sipag-interface-id* **auth** { **config** | **running** }

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.
config	Displays the configured SIP AG attributes.	-
running	Displays the used SIP AG attributes.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To view authentication information about a SIP AG, run the **display voice sipag auth** command.

Example

Display the configured authentication attributes of SIP AG 1.

```
<Huawei> display voice sipag 1 auth config
  SIP auth para
  AGID                    : 1
  Auth mode                 : Single-user
  Auth username               : 1
  Auth mode                 : password
  Auth password               : ******
```

Table 16-111 Description of the **display voice sipag auth** command output

Item	Description
SIP auth para	Authentication parameters of the SIP AG.
AGID	SIP AG ID.
Auth mode	Authentication mode: ● Password: original password authentication ● Ha1: Message Digest 5 (MD5) authentication
Auth username	Authentication user name.
Auth password	Authentication password.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.5 auth (SIP AG view)

16.6.1.17 display voice sipag dtmf

Function

Using the **display voice sipag dtmf** command, you can view the Dual-Tone Multifrequency (DTMF) parameters of a SIP AG.

Format

display voice sipag *sipag-interface-id* **dtmf**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the DTMF parameters of a specified SIP AG, run the **display voice sipag dtmf** command.

Example

Display the DTMF parameters of SIP AG 1.

```
<Huawei> display voice sipag 1 dtmf
 AGID                    : 1
 DTMF/MF transfer mode   : throughly
```

Table 16-112 Description of the **display voice sipag dtmf** command output

Item	Description
AGID	SIP AG ID.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DTMF/MF transfer mode	DMF transmission mode: ● throughly: DMF transparent transmission ● erase: DTMF signal removing

Related Topics

16.6.1.30 dtmf-transmission-mode

16.6.1.18 display voice sipag fax-modem

Function

Using the **display voice sipag fax-modem** command, you can view the fax and modem parameters of a SIP AG.

Format

display voice sipag *sipag-interface-id* **fax-modem**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the fax and modem parameters of a specified SIP AG, run the **display voice sipag fax-modem** command.

Example

Display the fax and modem parameters of SIP AG 1.

```
<Huawei> display voice sipag 1 fax-modem
  AGID                : 1
  Nego mode             : Negotiate
  RTP interval          : 10ms
```

```
VBD codec            : G.711A
VBD pt type          : Static
VBD attribute type     : V.152
Fax transmode          : throughly
Modem transmode          : throughly
```

Table 16-113 Description of the display voice sipag fax-modem command output

Item	Description
AGID	SIP AG ID.
Nego mode	Fax/modem codec negotiation mode: ● negotiate: negotiation mode ● self-switch: self-switching mode
RTP interval	Packetization interval in transparent transmission mode.
VBD codec	VBD codec mode: ● G.711a: A-law algorithm in G.711 ● G.711u: μ-law algorithm in G.711
VBD pt type	VBD payload type: ● dynamic ● static
VBD attribute type	VBD attribute type: ● chinatelecom: China Telecom mode ● extchinatelecom: extended China Telecom mode ● ietf: IETF mode ● V.152: V.152 mode
Fax transmode	Fax transmission mode: ● throughly: transparent transmission ● T.38: T.38 mode
Modem transmode	Modem transmission mode: ● relay: relay mode ● throughly: transparent transmission mode

Related Topics

16.6.1.37 fax-modem modem transmission-mode
16.6.1.32 fax-modem common rtp-interval
16.6.1.31 fax-modem common negotiation-mode
16.6.1.36 fax-modem fax transmission-mode
16.6.1.34 fax-modem common vbd-codec
16.6.1.35 fax-modem common vbd-pt-type

 Copyright © Huawei Technologies Co., Ltd.

16.6.1.19 display voice sipag nte

Function

Using the **display voice sipag nte** command, you can view RFC 2833 redundancy transmission information about a SIP AG.

Format

display voice sipag *sipag-interface-id* **nte**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view RFC 2833 redundancy transmission information about a specified SIP AG, run the **display voice sipag nte** command.

Example

Display RFC 2833 redundancy transmission information about SIP AG 1.

```
<Huawei> display voice sipag 1 nte
 AGID                    : 1
 NTE negomode            : No initiative start
 NTE fax modem           : Enable
 NTE flashhook           : Disable
 NTE DTMF                : Enable
```

Table 16-114 Description of the **display voice sipag nte** command output

Item	Description
AGID	SIP AG ID.

Item	Description
NTE negomode	Mode in which RFC 2833 transmission is started based on negotiation: ● Fixed start: fixed startup mode ● Nego start: initiative startup mode ● No initiative start: no-initiative startup mode
NTE fax modem	Status of RFC 2833 fax and modem transmission: ● Enable: RFC 2833 fax and modem transmission is enabled. ● Disable: RFC 2833 fax and modem transmission is disabled.
NTE DTMF	Status of RFC 2833 DTMF transmission: ● Enable: RFC 2833 DTMF transmission is enabled. ● Disable: RFC 2833 DTMF transmission is disabled.

Related Topics

16.6.1.46 nte-dtmf

16.6.1.47 nte-fax-modem

16.6.1.49 nte-negotiation-mode

16.6.1.20 display voice sipag number-parameter

Function

The **display voice sipag number-parameter** command displays the parameter indexes and values of a SIP AG.

Format

display voice sipag *sipag-interface-id* **number-parameter**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the parameter indexes and values of a specified SIP AG, run the **display voice sipag number-parameter** command.

Example

Display the parameter indexes and values of SIP AG 1.

```
<Huawei> display voice sipag 1 number-parameter
 Para index: 0              Value: 0
 Para index: 1              Value: 0
 Para index: 2              Value: 0
 Para index: 3              Value: 0
 Para index: 4              Value: 0
 Para index: 5              Value: 1
 Para index: 6              Value: 0
 Para index: 8              Value: 0
 Para index: 13              Value: 0
 Para index: 15              Value: 0
 Para index: 23              Value: 600
 Para index: 24              Value: 1
 Para index: 25              Value: 0
 Para index: 26              Value: 30
 Para index: 27              Value: 5
```

Table 16-115 Description of the display voice sipag number-parameter command output

Item	Description
Para index	SIP interface parameter index.
Value	SIP interface parameter value.

Related Topics

16.6.1.81 sipag

16.6.1.21 display voice sipag ring-mode

Function

The **display voice sipag ring-mode** command displays the SIP AG ring mode.

Format

display voice sipag *sipag-interface-id* **ring-mode**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the ring mode of a SIP AG, run the **display voice sipag ring-mode** command.

Example

Display the ring mode of SIP AG 1.

```
<Huawei> display voice sipag 1 ring-mode
  AGID            : 1
  Index           : 1
  Ring mode name  : huawei
  Cadence ring    : 0: Normal ring 1:4
  Initial ring    : 4: Normal ring (FSK) 1:4
```

Table 16-116 Description of the display voice sipag ring-mode command output

Item	Description
AGID	Interface ID of a SIP AG.
Index	Index of a ring mapping.
Ring mode name	Name of a ringing mapping.
Cadence ring	Type of the cadence ringing.
Initial ring	Type of the initial ringing.

Related Topics

16.6.1.70 ring-mode

16.6.1.81 sipag

16.6.1.22 display voice sipag string-parameter

Function

Using the **display voice sipag string-parameter** command, you can view the string parameter indexes and values of a SIP AG.

Format

display voice sipag *sipag-interface-id* **string-parameter** { **config** | **running** }

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.
config	Displays the configured parameters.	-
running	Displays the used parameters.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the string parameter indexes and values of a specified SIP AG, run the **display voice sipag string-parameter** command.

Example

Display the configured string parameter indexes and values of SIP AG 1.

```
<Huawei> display voice sipag 1 string-parameter config
 String index: 1
 String:
 String index: 2
 String:
 String index: 3
 String:
 String index: 4
 String:
 String index: 5
 String:
 String index: 6
 String:
```

```
String index: 11
String:
String index: 13
String:
String index: 14
String:
String index: 15
String:
String index: 16
String:
String index: 17
String:
String index: 18
String:
String index: 19
String:
String index: 20
String:
String index: 21
String:
String index: 22
String:
String index: 23
String:
String index: 24
String:
String index: 25
String:
String index: 26
String:
String index: 27
String:
String index: 28
String:
String index: 29
String:
String index: 30
String:
String index: 31
String:
String index: 32
String:
String index: 33
String:
String index: 34
String:
String index: 35
String:
String index: 36
String:
String index: 37
String:
String index: 38
String:
```

Table 16-117 Description of the display voice sipag string-parameter command output

Item	Description
String Index	Index of a string parameter.
String	Value of a string parameter.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.2 ag string-parameter

16.6.1.23 display voice sipag redundancy

Function

Using the **display voice sipag redundancy** command, you can view the redundancy parameters of a SIP AG.

Format

display voice sipag *sipag-interface-id* **redundancy**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the redundancy parameters of a specified SIP AG, run the **display voice sipag redundancy** command.

Example

Display the redundancy parameters of SIP AG 1.

```
<Huawei> display voice sipag 1 redundancy
 AGID                    : 1
 Redundancy negomode     : Fixed start
 Redundancy start mode   : Ordinary redundancy
 Redundancy red NTE      : Disable
 Redundancy red VBD      : Enable
 Redundancy red voice    : Disable
```

Table 16-118 Description of the display voice sipag redundancy command output

Item	Description
AGID	SIP AG ID.

Item	Description
Redundancy negomode	Mode in which RFC 2198 redundancy transmission is started based on negotiation: ● Fixed start: fixed startup mode ● Nego start: initiative startup mode ● No initiative start: no-initiative startup mode
Redundancy start mode	Mode in which RFC 2198 transmission is started: ● Ordinary redundancy: ordinary mode ● Smart redundancy: smart mode
Redundancy red NTE	Function that uses RFC 2198 redundancy transmission to transmit RFC 2833 audio data: ● Enable: This function is enabled. ● Disable: This function is disabled.
Redundancy red VBD	Function that uses RFC 2198 redundancy transmission to transmit VBD: ● enable: This function is enabled. ● disable: This function is disabled.
Redundancy red voice	Function that uses RFC 2198 redundancy transmission to transmit voice services: ● Enable: This function is enabled. ● Disable: This function is disabled.

Related Topics

16.6.1.63 redundancy-start-mode
16.6.1.62 redundancy-nte
16.6.1.61 redundancy-negotiation-mode
16.6.1.64 redundancy-vbd
16.6.1.65 redundancy-voice

16.6.1.24 display voice sipag sctp-association-info

Function

The **display voice sipag sctp-association-info** command displays Stream Control Transport Protocol (SCTP) association information about a SIP AG.

Format

display voice sipag *sipag-interface-id* **sctp-association-info**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

An association is a logical channel for data transmission, which is established by two SCTP endpoints through the 4-way handshake mechanism of SCTP. To view SCTP association information about a specified SIP AG, run the **display voice sipag sctp-association-info** command.

This command takes effect only when the transport protocol of the SIP AG is SCTP and an association is available.

Example

Display SCTP association information about SIP AG 1.

```
<Huawei> display voice sipag 1 sctp-association-info
  Association ID                  : 12
  Association state               : established
  Association type                : client
  Application ID                  : 1
  Local port                      : 5012
  Remote port                     : 5068
  Local IP address                : 192.168.1.213
  Remote active IP address        : 192.168.1.43
  Whether allow HB                : yes
  Local Received window           : 14000
  Remote Received window          : 206348
  Total unconfirmed data chunks   : 0
  Remote IP address 1             : 192.168.1.43
  Remote IP 1 state               : active
  Waiting ack data chunks         : 0
  Congestion window               : 4380
  Outstanding data chunks         : 0
  Retransmission time-out         : 1000
  Smoothed round-trip time        : 139ms
  Round-trip time variation       : 83ms
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-119 Description of the display voice sipag sctp-association-info command output

Item	Description
Association ID	SCTP association ID.
Association state	SCTP association status.
Association type	SCTP association type. The value can be client or server.
Application ID	Upper-layer user ID.
Local port	ID of the local port in an SCTP association.
Remote port	ID of the remote port in an SCTP association.
Local IP address	IP address of the local port in an SCTP association.
Remote active IP address	Primary IP address of the remote port in an SCTP association.
Whether allow HB	Whether the local end in an SCTP association is allowed to send heartbeat packets.
Local Received window	Receiving window size of the local end in an SCTP association.
Remote Received window	Receiving window size of the remote end in an SCTP association.
Total unconfirmed data chunks	Number of unconfirmed sent data blocks.
Remote IP address 1	IP address 1 of the remote port in an SCTP association.
Remote IP 1 state	Status of IP address 1 of the remote port in an SCTP association.
Waiting ack data chunks	Number of data blocks to be confirmed by the remote end.
Congestion window	Congestion window size.
Outstanding data chunks	Number of unconfirmed data blocks sent through the SCTP association path.
Retransmission time-out	Retransmission timeout.
Smoothed round-trip time	Average round trip time of the SCTP association path.
Round-trip time variation	Average round trip time variables of the SCTP association path.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.81 sipag

16.6.1.25 display voice sipag sctp-association-statistics

Function

The **display voice sipag sctp-association-statistics** command displays SCTP association statistics about a SIP AG.

Format

display voice sipag *sipag-interface-id* **sctp-association-statistics**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

This command takes effect only when the transport protocol of the SIP AG is SCTP and an association is available.

Example

Display SCTP association statistics about SIP AG 1.

```
<Huawei> display voice sipag 1 sctp-association-statistics
  Association ID                  : 12
  Times of T1 timer expires       : 0
  Times of T2 timer expires       : 0
  Retrans data chunks             : 0
  Sent data chunks                : 1241
  Received data chunks            : 42
  Sent sctp packets               : 0
  Received sctp packets           : 1804
  Received error sctp packets     : 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-120 Description of the display voice sipag sctp-association-statistics command output

Item	Description
Association ID	SCTP association ID.
Times of T1 timer expires	Number of T1 timer timeouts.
Times of T2 timer expires	Number of T2 timer timeouts.
Retrans data chunks	Number of association data block retransmissions.
Sent data chunks	Number of sent data blocks.
Received data chunks	Number of received data blocks.
Sent sctp packets	Number of sent SCTP packets.
Received sctp packets	Number of received SCTP packets.
Received error sctp packets	Number of received error SCTP packets.

Related Topics

16.6.1.81 sipag

16.6.1.26 display voice sipag sctp-protocol

Function

The **display voice sipag sctp-protocol** command displays SCTP stack parameters of a SIP AG.

Format

display voice sipag *sipag-interface-id* **sctp-protocol** { **config** | **running** }

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.
config	Displays the configured SCTP stack parameters.	-
running	Displays the running SCTP stack parameters.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view SCTP stack parameters of a specified SIP AG, run the **display voice sipag sctp-protocol** command.

Example

Display the configured SCTP stack parameters of SIP AG 1.

```
<Huawei> display voice sipag 1 sctp-protocol config
  In streams                : 33
  Out streams               : 33
  Maximum RTO value(ms)     : 3000
  Initial RTO value(ms)     : 1000
  RTO alpha parameter(%)    : 12
  RTO beta parameter(%)     : 25
  Heartbeat interval(ms)    : 10000
  Valid cookie lifetime(ms) : 60000
  Maximum init retrans      : 8
  Association maxretrans    : 10
  Path maximum retrans      : 5
  No congestion level(%)    : 40
  Low congestion level(%)   : 60
  High congestion level(%)  : 80
  Checksum arithmetic       : crc32
```

Table 16-121 Description of the display voice sipag sctp-protocol command output

Item	Description
In streams	Number of input SCTP streams.
Out streams	Number of output SCTP streams.
Maximum RTO value(ms)	Maximum timeout period of retransmissions.
Initial RTO value(ms)	Initial timeout period of retransmissions.
RTO alpha parameter(%)	Alpha factor in the timeout period of retransmissions.
RTO beta parameter(%)	Beta factor in the timeout period of retransmissions.
Heartbeat interval(ms)	Heartbeat interval.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Valid cookie lifetime(ms)	Life cycle of a valid cookie.
Maximum init retrans	Maximum number of times an init message is retransmitted.
Association maxretrans	Maximum number of times an association request is retransmitted.
Path maximum retrans	Maximum number of times a path is retransmitted.
No congestion level(%)	Level of no traffic congestion.
Low congestion level(%)	Level of low traffic congestion.
High congestion level(%)	Level of high traffic congestion.
Checksum arithmetic	Checksum algorithm.

Related Topics

16.6.1.81 sipag

16.6.1.27 display voice sipag signal

Function

The **display voice sipag signal** command displays the signal mapping lists of a SIP AG.

Format

display voice sipag signal *sipag-interface-id*

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the signal mapping lists of a SIP AG, run the **display voice sipag signal** command.

Example

Display the signal mapping lists of a SIP AG.

```
<Huawei> display voice sipag signal 1
  Signal name                    : test
  AGID                           : 1
  Signal unit                    : 8

  Seq                            : 0
  Type                           : -
  Duration(ms)                   : 4294967295
  Repeat                         : 1
  Start-cond(delay-time)(ms)     : ss
  End-cond(delay-time)(ms)       : -

  Seq                            : 1
  Type                           : -
  Duration(ms)                   : 4294967295
  Repeat                         : 1
  Start-cond(delay-time)(ms)     : 0e
  End-cond(delay-time)(ms)       : -

  Seq                            : 2
  Type                           : -
  Duration(ms)                   : 4294967295
  Repeat                         : 1
  Start-cond(delay-time)(ms)     : 1e
  End-cond(delay-time)(ms)       : -

  Seq                            : 3
  Type                           : -
  Duration(ms)                   : 4294967295
  Repeat                         : 1
  Start-cond(delay-time)(ms)     : 2e
  End-cond(delay-time)(ms)       : -

  Seq                            : 4
  Type                           : -
  Duration(ms)                   : 4294967295
  Repeat                         : 1
  Start-cond(delay-time)(ms)     : 3e
  End-cond(delay-time)(ms)       : -

  Seq                            : 5
  Type                           : -
  Duration(ms)                   : 4294967295
  Repeat                         : 1
  Start-cond(delay-time)(ms)     : 4e
  End-cond(delay-time)(ms)       : -

  Seq                            : 6
  Type                           : -
  Duration(ms)                   : 4294967295
  Repeat                         : 1
  Start-cond(delay-time)(ms)     : 5e
  End-cond(delay-time)(ms)       : -
```

 Copyright © Huawei Technologies Co., Ltd.

```
Seq                          : 7
Type                         : -
Duration(ms)                 : 4294967295
Repeat                       : 1
Start-cond(delay-time)(ms)   : 6e
End-cond(delay-time)(ms)     : -

Mapping scene name           : local:dial
```

Table 16-122 Description of the display voice sipag signal command output

Item	Description
Signal name	Signal name.
AGID	ID of the SIP AG interface that the user belongs to.
Signal unit	Signal unit.
Seq	Sequence number of a signal unit.
Type	Signal unit type.
Duration(ms)	Duration of a signal unit.
Repeat	Number of times a signal unit can be repeated.
Start-cond(delay-time)(ms)	Condition that will trigger end of a signal unit.
End-cond(delay-time)(ms)	Condition that will trigger start of a signal unit.
Mapping scene name	Scenario name.

Related Topics

16.6.1.15 display voice sipag

16.6.1.28 display voice sipag status-code-mapping

Function

The **display voice sipag status-code-mapping** command displays the mapping between scenarios and status codes of a SIP AG.

Format

display voice sipag *sipag-interface-id* **status-code-mapping**

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view mapping between scenarios and status codes of a SIP AG, run the **display voice sipag status-code-mapping** command. The status code of a scenario is contained in the response message when this scenario occurs during a call.

Example

Display the mapping between scenarios and status codes of SIP AG 1.

```
<Huawei> display voice sipag 1 status-code-mapping

 Running:  Scene        Status-code

           0            503
           1            503
           2            404
           3            486
           4            480
           5            480
           6            480
           7            486
           8            486
           9            480
           10            488
           11            500
           12            606
           13            486
           14            486
           15            487
           16            486
           17            486
           18            410
           19            481

 Config:   Scene        Status-code
```

Table 16-123 Description of the display voice sipag status-code-mapping command output

Parameter	Description	Value
0	The CPU is overloaded.	The value is an integer that ranges from 400 to 699. The default value is 503.
1	The power consumption exceeds the threshold.	The value is an integer that ranges from 400 to 699. The default value is 503.
2	The called party does not exist.	The value is an integer that ranges from 400 to 699. The default value is 404.
3	The specified port is occupied by another user account.	The value is an integer that ranges from 400 to 699. The default value is 486.
4	A port does not have a license.	The value is an integer that ranges from 400 to 699. The default value is 480.
5	A port is quitting the service after a delay.	The value is an integer that ranges from 400 to 699. The default value is 480.
6	A port is blocked.	The value is an integer that ranges from 400 to 699. The default value is 480.
7	The port is being locked.	The value is an integer that ranges from 400 to 699. The default value is 486.
8	A port is being tested.	The value is an integer that ranges from 400 to 699. The default value is 486.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
9	A user has not quit the service.	The value is an integer that ranges from 400 to 699. The default value is 480.
10	Digital signal processing (DSP) resources are insufficient.	The value is an integer that ranges from 400 to 699. The default value is 488.
11	System resources are insufficient.	The value is an integer that ranges from 400 to 699. The default value is 500.
12	The call is controlled by the calling party or called party.	The value is an integer that ranges from 400 to 699. The default value is 606.
13	The call is being connected to the called user.	The value is an integer that ranges from 400 to 699. The default value is 486.
14	The called user is talking.	The value is an integer that ranges from 400 to 699. The default value is 486.
15	The ringing time exceeds the timeout period.	The value is an integer that ranges from 400 to 699. The default value is 487.
16	The call is rejected in call waiting mode.	The value is an integer that ranges from 400 to 699. The default value is 486.
17	The call times out in call waiting mode.	The value is an integer that ranges from 400 to 699. The default value is 486.
18	The user hangs up to release the waiting call in semi-tight coupling mode.	The value is an integer that ranges from 400 to 699. The default value is 410.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
19	A conversation or an event does not exist.	The value is an integer that ranges from 400 to 699. The default value is 481.

Related Topics

16.6.1.81 sipag

16.6.1.29 display voice sipag user-defined-profile

Function

The **display voice sipag user-defined-profile** command displays the user-defined parameters of a SIP AG.

Format

display voice sipag *sipag-interface-id* **user-defined-profile** { **running** | **config** }

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the SIP AG ID.	The value is an integer that ranges from 0 to 16777215.
running	Displays the running user-defined parameters.	-
config	Displays the configured user-defined parameters.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the user-defined parameters of a specified SIP AG, run the **display voice sipag user-defined-profile** command.

Example

Display the user-defined parameters of SIP AG 1.

```
<Huawei> display voice sipag 1 user-defined-profile config
  SIPAG AGID : 1

  Codec-Pri:

  Pri : 0          Codec : 8          Pt : 20
  Pri : 1          Codec : 0          Pt : 20
  Pri : 2          Codec : 18          Pt : 10
  Pri : 3          Codec : 4          Pt : 30

  Srv-Pri:

  Pri : 0          Srvid : 4
  Pri : 1          Srvid : 5
  Pri : 2          Srvid : 3
  Pri : 3          Srvid : 2
  Pri : 4          Srvid : 0
  Pri : 5          Srvid : 1
  Pri : 6          Srvid : 6
  Pri : 7          Srvid : 7
  Pri : 8          Srvid : 8
  Pri : 9          Srvid : 9
  Pri : 10          Srvid : 10
  Pri : 11          Srvid : 11
  Pri : 12          Srvid : 12
  Pri : 13          Srvid : 13
  Pri : 14          Srvid : 14
  Pri : 15          Srvid : 15
  Pri : 16          Srvid : 16
  Pri : 17          Srvid : 17
  Pri : 18          Srvid : 18
  Pri : 19          Srvid : 19
  Pri : 20          Srvid : 20
  Pri : 21          Srvid : 21
  Pri : 22          Srvid : 22

  SysPara:

  SP2  : 1
  SP3  : 1
  SP7  : 1
  SP9  : 1
  SP11 : 0
  SP12 : 0
  SP13 : 1
  SP14 : 1
  SP15 : 0
  SP16 : 0
  SP17 : 0
  SP18 : 0
  SP19 : 0
  SP20 : 1
  SP21 : 1
  SP22 : 0
  SP23 : 64
  SP24 : 15
  SP25 : 180
  SP26 : 32
  SP27 : 120
  SP28 : 120
  SP29 : 30
  SP30 : 60
  SP31 : 20
  SP32 : 20
  SP33 : 500
```

 Copyright © Huawei Technologies Co., Ltd.

```
SP34 : 45
SP35 : 0
SP36 : 33007
SP37 : 24575
SP38 : 532615
SP39 : 1039
SP40 : 33007
SP41 : 1
SP42 : 1
SP43 : 2
SP47 : 0
SP50 : 1
SP51 : 1
SP52 : 2
SP53 : 0
SP55 : 0
SP56 : 0
SP58 : 0
SP59 : 0
SP62 : 500
SP63 : 10
SP64 : 20
SP65 : 3
SP66 : 3
SP67 : 6
SP69 : 0
SP70 : 0
SP72 : 0
SP80 : 0
SP82 : 0
SP85 : 1
SP86 : 3
SP87 : 1
SP88 : 180
SP89 : 10
SP90 : 4
SP91 : 20
SP92 : 30
SP93 : 30
SP94 : 180
SP95 : 4
SP96 : 90
SP97 : 30
SP98 : 6
SP99 : 4
SP100: 120
SP101: 100
SP102: 30
SP103: 30
SP104: 4
SP105: 10
SP106: 10
SP107: 16
SP108: 8
SP109: 2
SP110: 0
SP111: 1
SP112: 2
SP113: 2
SP114: 1
SP115: 2
SP116: 1
SP117: 0
SP118: 0
SP119: 1
SP120: 0
SP121: 1
SP122: 2
SP123: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
SP124: 0
SP125: 0
SP126: 0
SP127: 0
SP128: 0
SP129: 0
SP130: 0
SP131: 0
SP132: 0
SP133: 1
SP134: 0
SP135: 0
SP136: 0
SP137: 1
SP138: 0
SP139: 0
SP140: 0
SP141: 1
SP142: 0
SP143: 0
SP144: 0
SP145: 1
SP146: 1
SP148: 1
SP150: 36000
SP151: 500
SP152: 0
SP154: 8194
SP155: 0
SP156: 0
SP157: 50
SP158: 0
SP159: 0
SP160: 0
SP161: 1
SP162: 1
SP163: 0
SP164: 0
SP165: 0
SP166: 1
SP167: 0
SP168: 0
SP169: 0
SP170: 0
SP171: 0
SP172: 180
SP173: 90
SP174: 0
SP175: 0
SP176: 0
SP177: 30
SP179: 0
SP180: 0
SP181: 1
SP182: 0
SP183: 0
SP184: 1
SP185: 1
SP186: 2
SP187: 70000
SP188: 1
SP189: 0
SP190: 0
SP191: 0
SP192: 0
SP193: 30
SP194: 21600
SP195: 0
SP196: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
SP197: 0
SP198: 0
SP199: 0
SP200: 0
SP201: 0
SP202: 0
SP203: 0
SP204: 480
SP205: 486
SP206: 486
SP207: 0
SP208: 30
SP210: 0
SP211: 0
SP212: 1
SP213: 0
SP214: 0
SP215: 0
SP216: 0
SP217: 0
SP218: 0
SP219: 0
SP220: 0
SP221: 15
SP222: 0
SP223: 1
SP224: 0
SP225: 20
SP226: 20
SP227: 4
SP228: 0
SP229: 0
SP230: 0
SP231: 0
SP232: 0
SP233: 1
SP234: 0
SP235: 0
SP236: 0
SP237: 0
SP238: 1800
SP239: 0
SP240: 0
SP241: 0
SP242: 1200
SP243: 1
SP244: 0
SP245: 0
SP246: 6
SP247: 0
SP248: 0
SP249: 1
SP251: 1000
SP252: 0
SP253: 1
SP254: 0
SP255: 0
SP256: 1
SP257: 1
SP258: 0
SP259: 0
SP261: 0
SP262: 0
SP263: 1
SP264: 0
SP265: 1
SP266: 100
SP267: 1
SP268: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
SP269: 0
SP270: 1
SP271: 0
SP272: 0
SP273: 0
SP274: 0
SP275: 0
SP276: 0
SP277: 1
SP278: 1
SP279: 0
SP280: 2147434495
SP281: 0
SP282: 1
SP283: 0
SP284: 0
SP285: 0
SP286: 0
SP287: 0
SP301: 0
SP302: 0
SP303: 0
SP304: 1
SP305: 1
SP306: 0
SP307: 0
SP308: 2147483639
SP309: 2147483647
SP310: 0
SP311: 2
SP312: 2147483647
SP313: 2147483647
SP314: 2147483647
SP315: 2147483647
SP316: 2147483647
SP317: 2147483647
SP318: 2147483647
SP319: 2147483647
SP320: 2147483647
SP321: 2147483647
SP322: 2147483647
SP323: 2147483647
SP324: 0
SP325: 0
SP326: 0
SP327: 8
SP328: 1
```

Table 16-124 Description of the display voice sipag user-defined-profile command output

Item	Description
SIPAG AGID	ID of the SIP AG interface that the user belongs to.
Codec-Pri	Codec priority.
Pri	Codec/service priority. The value is an integer that ranges from 0 to 255. A smaller value indicates a higher priority.
Codec	Codec value. The value is an integer that ranges from 0 to 255. Common codecs are G711U (0), G723 (4), G711A (8), and G729 (18).

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pt	Packetization duration. The value is an integer that ranges from 0 to 4294967295. Generally, the value is a multiple of 5. Common packetization durations are 10, 20, and 30 milliseconds.
Srv-Pri	Service priority.
Srvid	Service type. The value is an integer that ranges from 0 to 4294967295.
SysPara	System parameters, including system parameter indexes and corresponding values. For example, the index and value of number 7 system parameter are respectively SP7 and 1.

Related Topics

16.6.1.81 sipag

16.6.1.30 dtmf-transmission-mode

Function

Using the **dtmf-transmission-mode** command, you can configure the Dual-Tone Multifrequency (DTMF) transmission mode for a SIP AG.

Using the **undo dtmf-transmission-mode** command, you can restore the default DTMF transmission mode of a SIP AG.

By default, the DTMF transmission mode is transparent transmission.

Format

dtmf-transmission-mode { **throughly** | **erase** }

undo dtmf-transmission-mode

Parameters

Parameter	Description	Value
throughly	Indicates DTMF transparent transmission.	-
erase	Indicates DTMF signal removing.	-

Views

SIP AG view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **dtmf-transmission-mode** command configures the DTMF transmission mode for a SIP AG:

- DTMF transparent transmission: is the default DTMF transmission mode.
- DTMF signal removing: is used when DTMF signaling is transmitted in accordance with RFC 2833 and DTMF signals do not need to be transmitted.

Example

Set the DTMF transmission mode to transparent transmission for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] dtmf-transmission-mode throughly
```

Related Topics

16.6.1.17 display voice sipag dtmf

16.6.1.31 fax-modem common negotiation-mode

Function

Using the **fax-modem common negotiation-mode** command, you can set the fax/modem codec negotiation mode of a SIP AG.

Using the **undo fax-modem common negotiation-mode** command, you can restore the default fax/modem codec negotiation mode of a SIP AG.

By default, the fax/modem codec negotiation mode is negotiation.

Format

fax-modem common negotiation-mode { **negotiate** | **self-switch** }

undo fax-modem common negotiation-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
negotiate	Sets the fax/modem codec negotiation mode to negotiation. In negotiation mode, the MG needs to negotiate with the MGC for the codec negotiation mode using signaling.	-
self-switch	Sets the fax/modem codec negotiation mode to self-switch.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

To set the fax/modem codec negotiation mode of a SIP AG, run the **fax-modem common negotiation-mode** command.

Example

Set the fax/modem codec negotiation mode of SIP AG 1 to self-switch.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] fax-modem common negotiation-mode self-switch
```

Related Topics

16.6.1.18 display voice sipag fax-modem

16.6.1.32 fax-modem common rtp-interval

Function

Using the **fax-modem common rtp-interval** command, you can set the packetization interval in transparent transmission mode.

Using the **undo fax-modem common rtp-interval** command, you can restore the default packetization interval in transparent transmission mode.

By default, the packetization interval in transparent transmission mode is 10 ms.

 Copyright © Huawei Technologies Co., Ltd.

Format

fax-modem common rtp-interval { **5ms** | **10ms** | **20ms** | **30ms** }

undo fax-modem common rtp-interval

Parameters

None

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

Before setting the packetization interval, perform either of the following operations:

- Run the **fax-modem modem transmission-mode** command to set the modem transmission mode to transparent transmission.
- Run the **fax-modem fax transmission-mode** command to set the fax transmission mode to transparent transmission.

Example

Set the packetization interval in transparent transmission mode to 20 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] fax-modem common rtp-interval 20ms
```

Related Topics

16.6.1.36 fax-modem fax transmission-mode

16.6.1.37 fax-modem modem transmission-mode

16.6.1.18 display voice sipag fax-modem

16.6.1.33 fax-modem common vbd-attribute-type

Function

Using the **fax-modem common vbd-attribute-type** command, you can set the VBD attribute type of a SIP AG.

Using the **undo fax-modem common vbd-attribute-type** command, you can restore the default VBD attribute type of a SIP AG.

By default, the VBD attribute type is V.152.

 Copyright © Huawei Technologies Co., Ltd.

Format

fax-modem common vbd-attribute-type { **chinatelecom** | **chinatelecomext** | **ietf** | **v152** }

undo fax-modem common vbd-attribute-type

Parameters

Parameter	Description	Value
chinatelecom	Indicates the China Telecom mode.	-
chinatelecomext	Indicates the extended China Telecom mode.	-
ietf	Indicates the IETF mode.	-
v152	Indicates the V.152 mode.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

To set the VBD attribute type of a SIP AG, run the **fax-modem common vbd-attribute-type** command.

Example

Set the VBD attribute type to IETF.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] fax-modem common vbd-attribute-type ietf
```

Related Topics

16.6.1.18 display voice sipag fax-modem

16.6.1.34 fax-modem common vbd-codec

Function

Using the **fax-modem common vbd-codec** command, you can set the VBD codec mode of a SIP AG.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo fax-modem common vbd-codec** command, you can restore the default VBD codec mode of a SIP AG.

By default, the VBD codec mode is A-law algorithm in G.711.

Format

fax-modem common vbd-codec { **g711a** | **g711u** }

undo fax-modem common vbd-codec

Parameters

Parameter	Description	Value
g711a	Indicates the A-law algorithm in G.711.	-
g711u	Indicates the μ-law algorithm in G.711.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

To set the VBD codec mode of a SIP AG, run the **fax-modem common vbd-codec** command.

Example

Set the VBD codec mode of SIP AG 1 to μ-law algorithm in G.711.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] fax-modem common vbd-codec g711u
```

Related Topics

16.6.1.18 display voice sipag fax-modem

16.6.1.35 fax-modem common vbd-pt-type

Function

Using the **fax-modem common vbd-pt-type** command, you can configure the VBD payload type of a SIP AG.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo fax-modem common vbd-pt-type** command, you can restore the default VBD payload type of a SIP AG.

By default, the VBD payload type is static.

Format

fax-modem common vbd-pt-type { **dynamic** | **static** }

undo fax-modem common vbd-pt-type

Parameters

Parameter	Description	Value
dynamic	Indicates dynamic payload.	-
static	Indicates static payload.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

To configure the VBD payload type of a SIP AG, run the **fax-modem common vbd-pt-type** command.

Example

Set the VBD payload type to dynamic payload.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] fax-modem common vbd-pt-type dynamic
```

Related Topics

16.6.1.18 display voice sipag fax-modem

16.6.1.36 fax-modem fax transmission-mode

Function

Using the **fax-modem fax transmission-mode** command, you can configure the fax transmission mode for a SIP AG.

Using the **undo fax-modem fax transmission-mode** command, you can restore the default fax transmission mode of a SIP AG.

By default, the fax transmission mode of a SIP AG is transparent transmission.

Format

fax-modem fax transmission-mode { **throughly** | **t38** }

undo fax-modem fax transmission-mode

Parameters

Parameter	Description	Value
throughly	Indicates the transparent transmission mode.	-
t38	Indicates the T.38 mode.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **fax-modem fax transmission-mode** command configures the fax transmission mode for a SIP AG:

- Transparent transmission mode: uses the coding mode defined in G.711.
- T.38 mode: uses the fax-dedicated coding mode.

Example

Set the fax transmission mode to transparent transmission for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] fax-modem fax transmission-mode throughly
```

Related Topics

16.6.1.18 display voice sipag fax-modem

16.6.1.37 fax-modem modem transmission-mode

Function

Using the **fax-modem modem transmission-mode** command, you can configure the modem transmission mode for a SIP AG.

Using the **undo fax-modem modem transmission-mode** command, you can restore the default modem transmission mode of a SIP AG.

By default, the modem transmission mode of a SIP AG is transparent transmission.

Format

fax-modem modem transmission-mode { **throughly** | **relay** }

undo fax-modem modem transmission-mode

Parameters

Parameter	Description	Value
throughly	Indicates the transparent transmission mode.	-
relay	Indicates the relay mode.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **fax-modem modem transmission-mode** command configures the modem transmission mode for a SIP AG:

- Transparent transmission mode: The G.711 codec is used, and modem signals are processed as ordinary RTP data. This mode depends on the bearer network. If users are disconnected from the network, the access rate is low, or the network is unstable, check the packet loss ratio and jitter on the bearer network.
- Relay mode: is also called the redundancy mode. The gateway modulates modem signals. Generally, the gateway also performs local error check and transmits the modulated data to the peer gateway by using a reliable protocol.

Example

Set the modem transmission mode to the relay mode.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] fax-modem modem transmission-mode relay
```

Related Topics

16.6.1.18 display voice sipag fax-modem

16.6.1.38 home-domain

Function

Using the **home-domain** command, you can configure a home domain name for a SIP AG.

Using the **undo home-domain** command, you can delete the home domain name of a SIP AG.

By default, no home domain name is configured for a SIP AG.

Format

home-domain *home-domain-value*

undo home-domain

Parameters

Parameter	Description	Value
home-domain-value	Specifies a home domain name.	The name is a string of 1 to 64 case-sensitive characters without spaces and underscores.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The home domain name is a mandatory parameter.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure a home domain name **abcd.com** for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] home-domain abcd.com
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.39 local-digitmap

Function

Using the **local-digitmap** command, you can configure a SIP AG digitmap.

Using the **undo local-digitmap** command, you can delete a SIP AG digitmap.

By default, no SIP AG digitmap is configured.

Format

local-digitmap *name-value* { **append** | **type** { **normal** | **emergency** | **scc** | **direct-centrex** | **second-centrex** } } *body-value*

undo local-digitmap *name-value* [*body-value*]

Parameters

Parameter	Description	Value
name-value	Specifies the name of a SIP AG digitmap.	The value is a string of 1 to 32 characters.
append	Adds a body to a SIP AG digitmap.	-
type { **normal** | **emergency** | **scc** | **direct-centrex** | **second-centrex** }	Specifies the digitmap type.	Enumerated type. The values are as follows: • **normal**: configures a normal digitmap. • **emergency**: configures an emergency digitmap. • **scc**: configures a service digitmap. • **direct-centrex**: configures a direct dialing Centrex digitmap. • **second-centrex**: configures a two-stage dialing Centrex digitmap.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
body-value	Specifies the body of a SIP AG digitmap.	The value is a string of 1 to 180 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

A SIP AG digitmap contains one or more bodies. Each body contains no more than 256 bytes.

A digitmap defines dialup rules. Calls can be initiated only when numbers match the rules. By default, all calling numbers are allowed.

A body can contain the following characters: digits 0 to 9, dot (.), vertical bar (|), square brackets [ ], hyphen (-), parentheses ( ), letters A to K and X, and letters T, S, L, Z (case-sensitive). A body complies with the following rules:

- Parentheses ( ) and square brackets [ ] must be used in pairs, and ( ) cannot be placed in the middle of the body.
- X, |, or . cannot be included in square brackets.
- A hyphen (-) is placed between two numbers, indicating a value range. The number behind the hyphen must be greater than the number before the hyphen. The value range must be included in square brackets.
- L, S, T, or Z cannot be followed by a dot.
- A body cannot start with L, S, T, Z, or a dot.

Default digitmap are as follows, when new digitmap is being configured, default digitmap will be cleared.

- Default service digitmap: (ExxFx.E|ExxFx.L|ExFx.E|ExFx.L|Exx.F|EFxx.F|Fxx.F)
- Default emergency hotline digitmap: (11X|91X|0E)
- Default dial digitmap: ([2-8]xxxxxxx|[2-8]xxSxxxxxxx|13xxxxxxxxx|0xxxxxxxxx|9xxxx|1[0124-9]x|F|x.F|[0-9].S)

Example

Configure a digitmap for a SIP AG, which allows only 8-digit numbers starting with 8888.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-digitmap huawei type normal 8888xxxx
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.40 loop (VE1 interface view)

Function

The **loop** command enables the loopback attribute on a VE1 interface.

The **undo loop** command disables the loopback attribute on a VE1 interface.

By default, the loopback attribute is disabled on a VE1 interface.

Format

loop *loop-value*

undo loop

Parameters

Parameter	Description	Value
loop *loop-value*	Indicates the loopback attribute on the interface.	Enumerated type. The values are as follows: • remote: indicates remote loopback. • local: indicates local loopback.

Views

VE1 interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the local loopback attribute on the VE1 interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port ve1 2/0/0
[Huawei-voice-ve1-2/0/0] loop local
```

 Copyright © Huawei Technologies Co., Ltd.

16.6.1.41 loop (bra interface view)

Function

The **loop** command enables the loopback attribute on a bra interface.

The **undo loop** command disables the loopback attribute on a bra interface.

By default, the loopback attribute is disabled on a bra interface.

Format

loop *loop-value*

undo loop

Parameters

Parameter	Description	Value
loop *loop-value*	Indicates the loopback attribute on the interface.	Enumerated type. The values are as follows: ● remote: indicates remote loopback. ● local: indicates local loopback.

Views

bra interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the local loopback attribute on the bra interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port bra 2/0/0
[Huawei-voice-bra-2/0/0] loop local
```

16.6.1.42 loop (fxs interface view)

Function

The **loop** command enables the loopback attribute on a fxs interface.

 Copyright © Huawei Technologies Co., Ltd.

The **undo loop** command disables the loopback attribute on a fxs interface.

By default, the loopback attribute is disabled on a fxs interface.

NOTE

The AR129CV, AR129CVW, and AR129CGVW-L do not support this command.

Format

loop *loop-value*

undo loop

Parameters

Parameter	Description	Value
loop *loop-value*	Indicates the loopback attribute on the interface.	Enumerated type. The values are as follows: ● remote: indicates remote loopback. ● local: indicates local loopback.

Views

fxs interface view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the local loopback attribute on the fxs interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] port fxs 2/0/0
[Huawei-voice-fxs-2/0/0] loop local
```

16.6.1.43 media-addr

Function

Using the **media-addr** command, you can configure a media IP address for a SIP AG and configure a name for the media IP address.

Using the **undo media-addr** command, you can delete the media IP address and media IP address name of a SIP AG.

By default, no media IP address or media IP address name is configured for a SIP AG.

Format

media-addr { *media-ip* | **addr-name** *media-addr-name* }

undo media-ip

undo media-addr-name

Parameters

Parameter	Description	Value
media-ip	Specifies the media IP address of a SIP AG.	The value is in dotted decimal notation.
media-addr-name	Specifies the media IP address name of a SIP AG.	The value is a string of 1 to 64 characters.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

To provide the media exchange function, a SIP AG must have a media IP address or a media IP address name. To view the mode in which the IP address of a proxy server is obtained, run the **display voice sipag** command:

- If the static mode is set, the configured IP address takes effect.
- If another mode is set, the configured IP address name takes effect.

Precautions

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure an existing media IP address 192.168.1.1 for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] media-addr 192.168.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.1.44 media-bandwidth-control enable (SIPAG)

Function

The **media-bandwidth-control enable** command enables CAC on a SIP AG.

The **undo media-bandwidth-control enable** command disables CAC on a SIP AG.

By default, CAC is disabled on a SIP AG.

Format

media-bandwidth-control enable

undo media-bandwidth-control enable

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The uplink bandwidth is limited on the IP bearer network. For example, some users may access the IP bearer network using ADSL. If voice data is transmitted through the IP bearer network, the voice communication may be restricted by the bandwidth. More voice calls occupy more bandwidth on the network. To improve the voice communication quality, run the **media-bandwidth-control enable** command to enable CAC on the SIP AG.

Follow-up Procedure

Run the **media-bandwidth-control_max-bandwidth_sipag** command to set the maximum uplink media bandwidth of voice data.

Example

Enable CAC on the SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] media-bandwidth-control enable
```

16.6.1.45 media-bandwidth-control max-bandwidth (SIPAG)

Function

The **media-bandwidth-control max-bandwidth** command sets the maximum uplink media bandwidth of voice data.

The **undo media-bandwidth-control max-bandwidth** command restores the default maximum uplink media bandwidth of voice data.

By default, the maximum uplink media bandwidth of voice data is 500000 kbit/s.

Format

media-bandwidth-control max-bandwidth *max-bandwidth-value*

undo media-bandwidth-control max-bandwidth

Parameters

Parameter	Description	Value
max-bandwidth-value	Specifies the maximum uplink media bandwidth occupied by voice data.	The value is an integer that ranges from 1 to 5000, in 100 kbit/s. The default value is 5000, that is, 500000 kbit/s.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After CAC is enabled on the SIP AG by running the **16.6.1.44 media-bandwidth-control enable (SIPAG)** command, run the **media-bandwidth-control max-bandwidth** command to specify the maximum uplink media bandwidth of voice data. If call restriction is enabled when the uplink bandwidth is insufficient and the **media-bandwidth-control max-bandwidth** command is not run, the default maximum uplink media bandwidth is 500000 kbit/s. When the bandwidth occupied by voice calls reaches the maximum value, new voice calls are restricted.

CAC calculates the bandwidth occupied by voice communication based on the number of voice calls. Each voice call occupies 95 kbit/s in G.711. When the uplink media bandwidth of voice data is 0, new voice calls are rejected. When the uplink media bandwidth of voice data is lower than 95 kbit/s, only one call is allowed. Then the uplink bandwidth is used up.

 Copyright © Huawei Technologies Co., Ltd.

CAC can only detect the uplink media bandwidth of voice data, but not that of non-voice data packets. If the reserved maximum uplink media bandwidth of voice data is improper, the voice communication quality may be affected.

For example, the reserved uplink media bandwidth supports a maximum of 100 calls. When the 80th call is connected, the uplink bandwidth of the IP network has been used up by voice data packets and other IP data packets. However, CAC cannot detect that the uplink bandwidth is used up. The 81st call is not rejected because the uplink media bandwidth supports 100 calls. When the 81st call is connected, packets may be lost and the network may be blocked, affecting the voice communication quality.

Prerequisites

CAC has been enabled on the SIP AG using the **16.6.1.44 media-bandwidth-control enable (SIPAG)** command.

Example

Set the maximum uplink bandwidth to 400000 kbit/s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] media-bandwidth-control enable
[Huawei-voice] media-bandwidth-control max-bandwidth 4000
```

16.6.1.46 nte-dtmf

Function

Using the **nte-dtmf** command, you can enable or disable RFC 2833 DTMF transmission.

Using the **undo nte-dtmf** command, you can restore the default configuration.

By default, RFC 2833 DTMF transmission is enabled.

Format

nte-dtmf { **enable** | **disable** }

undo nte-dtmf

Parameters

Parameter	Description	Value
enable	Enables RFC 2833 DTMF transmission.	-
disable	Disables RFC 2833 DTMF transmission.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run the **nte-dtmf** command to enable or disable RFC 2833 DTMF transmission.

Example

Enable RFC 2833 DTMF transmission on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] nte-dtmf enable
```

Related Topics

16.6.1.19 display voice sipag nte

16.6.1.47 nte-fax-modem

Function

Using the **nte-fax-modem** command, you can enable or disable RFC 2833 fax and modem transmission.

Using the **undo nte-fax-modem** command, you can restore the default configuration.

By default, RFC 2833 fax and modem transmission is enabled.

Format

nte-fax-modem { **enable** | **disable** }

undo nte-fax-modem

Parameters

Parameter	Description	Value
enable	Enables RFC 2833 fax and modem transmission.	-
disable	Disables RFC 2833 fax and modem transmission.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run the **nte-fax-modem** command to enable or disable RFC 2833 fax and modem transmission.

Example

Enable RFC 2833 fax and modem transmission on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] nte-fax-modem enable
```

Related Topics

16.6.1.19 display voice sipag nte

16.6.1.48 nte-flash-hook

Function

Using the **nte-flash-hook** command, you can enable or disable RFC 2833 hookflash transmission.

Using the **undo nte-flash-hook** command, you can restore the default configuration.

By default, RFC 2833 hookflash transmission is disabled.

Format

nte-flash-hook { **enable** | **disable** }

undo nte-flash-hook

Parameters

Parameter	Description	Value
enable	Enables RFC 2833 hookflash transmission.	-

Parameter	Description	Value
disable	Disables RFC 2833 hookflash transmission.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run the **nte-flash-hook** command to enable or disable RFC 2833 hookflash transmission.

Example

Enable RFC 2833 hookflash transmission on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] nte-flash-hook enable
```

Related Topics

16.6.1.19 display voice sipag nte

16.6.1.49 nte-negotiation-mode

Function

The **nte-negotiation-mode** command configures the mode in which RFC 2833 transmission is started based on negotiation.

The **undo nte-negotiation-mode** command restores the default mode in which RFC 2833 transmission is started based on negotiation.

By default, the mode in which RFC 2833 transmission is started based on negotiation is **no-initiative-start**.

Format

nte-negotiation-mode *mode-value*

undo nte-negotiation-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mode-value	Specifies the mode in which RFC 2833 transmission is started based on negotiation.	Enumerated type. The values are as follows: • **negotiation**: configures the initiative startup mode. • **fixed-start**: configures the fixed startup mode. • **no-initiative-start**: configures the no-initiative startup mode.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **nte-negotiation-mode** command configures the mode in which RFC 2833 transmission is started based on negotiation:

- Initiative startup: RFC 2833 transmission is started only after the negotiation between the local end and remote end succeeds. The negotiation may be initiated by the local end or remote end.
- Fixed startup: The local end does not initiate any negotiation but accepts the initiated negotiation. In fixed startup mode, RFC 2833 transmission is started based on the local configuration regardless of the negotiation result.
- No-initiative startup: RFC 2833 transmission starts only after the local end receives the negotiation invitation from the remote end.

Example

Set the mode in which RFC 2833 transmission is started based on negotiation to **fixed-start**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] nte-negotiation-mode fixed-start
```

Related Topics

16.6.1.19 display voice sipag nte

16.6.1.50 phone-context

Function

Using the **phone-context** command, you can configure the phone context for a SIP AG.

Using the **phone-context** command, you can delete the phone context of a SIP AG.

By default, no phone context is configured for a SIP AG.

Format

phone-context *phone-context-value*

undo phone-context

Parameters

Parameter	Description	Value
phone-context-value	Specifies the phone context for a SIP AG.	The value is a string of 1 to 32 case-sensitive characters.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **phone-context** command configures the phone context for a SIP AG. The phone context identifies the context of a local number, that is, the number range. The phone context and local number identify a unique resource.

The phone context can be expressed using a global number or domain name.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the phone context of a SIP AG to **+8625**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] phone-context +8625
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.1.51 primary-proxy-addr dns-a

Function

The **primary-proxy-addr dns-a** command configures the DNS-A domain name and port number for the primary proxy server.

The **undo primary-proxy-addr** command deletes the DNS-A domain name and port number of the primary proxy server.

By default, no DNS-A domain name or port number is configured for the primary proxy server.

Format

primary-proxy-addr dns-a *dns-a-domain-name dns-a-port-number*

undo primary-proxy-addr

Parameters

Parameter	Description	Value
dns-a-domain-name	Specifies the DNS-A domain name of the primary proxy server.	The value is a string of 1 to 64 characters.
dns-a-port-number	Specifies the port number of the DNS-A domain name.	The value is an integer that ranges from 1 to 65535.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the DNS-A domain name and port number of the primary proxy server on a SIP AG to www.abcd.com and 5060.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] primary-proxy-addr dns-a www.abcd.com 5060
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.52 primary-proxy-addr dns-naptr

Function

The **primary-proxy-addr dns-naptr** command configures the DNS-NAPTR domain name of the primary proxy server.

The **undo primary-proxy-addr** command deletes the DNS-NAPTR domain name of the primary proxy server.

By default, no DNS-NAPTR domain name is configured for the primary proxy server.

Format

primary-proxy-addr dns-naptr *dns-naptr-domain-name*

undo primary-proxy-addr

Parameters

Parameter	Description	Value
dns-naptr-domain-name	Specifies the DNS-NAPTR domain name of the primary proxy server.	The value is a string of 1 to 64 characters.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the DNS-NAPTR domain name of the primary proxy server on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] primary-proxy-addr dns-naptr www.abcd.com
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.53 primary-proxy-addr dns-srv

Function

The **primary-proxy-addr dns-srv** command configures the DNS-SRV domain name of the primary proxy server.

The **undo primary-proxy-addr** command deletes the DNS-SRV domain name of the primary proxy server.

By default, no DNS-SRV domain name is configured for the primary proxy server.

Format

primary-proxy-addr dns-srv *dns-srv-domain-name*

undo primary-proxy-addr

Parameters

Parameter	Description	Value
dns-srv-domain-name	Specifies the DNS-SRV domain name of the primary proxy server.	The value is a string of 1 to 64 characters.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the DNS-SRV domain name of the primary proxy server on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] primary-proxy-addr dns-srv www.abcd.com
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.54 primary-proxy-addr static

Function

The **primary-proxy-addr static** command configures a static IP address for the primary proxy server.

The **undo primary-proxy-addr** command deletes the static IP address of the primary proxy server.

By default, no static IP address is configured for the primary proxy server.

Format

primary-proxy-addr static *static-ip-address static-ip-address-port* [**secondary** *static-ip-address2*]

undo primary-proxy-addr

Parameters

Parameter	Description	Value
static-ip-address	Specifies a static IP address for the primary proxy server.	The value is in dotted decimal notation.
static-ip-address-port	Specifies a port number of the static IP address.	The value is an integer that ranges from 1 to 65534.
secondary *static-ip-address2*	Specifies a static IP address 2 for the primary proxy server.	The value is in dotted decimal notation.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the IP address of the primary proxy server for a SIP AG to 192.168.1.1 and port number to 5061.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] primary-proxy-addr 192.168.1.1 5061
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.55 profile

Function

The **profile** command configures the profile index of a SIP AG.

The **undo profile** command restores the default profile index of a SIP AG.

By default, the profile index of a SIP AG is 1.

Format

profile *profile-index*

undo profile

Parameters

Parameter	Description	Value
profile-index	Specifies the profile index.	The value is an integer that ranges from 0 to 3: • 0: user-defined profile • 1: default profile • 2: pre-configured profile

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the profile index of a SIP AG to 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] profile 1
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.56 proxy-detect-mode

Function

Using the **proxy-detect-mode** command, you can configure the mode used by a SIP AG to detect a proxy server.

Using the **undo proxy-detect-mode** command, you can restore the default mode used by a SIP AG to detect a proxy server.

By default, a SIP AG uses the probe mode to detect a proxy server.

Format

proxy-detect-mode { **option** | **probe** | **register** }

undo proxy-detect-mode

Parameters

Parameter	Description	Value
option	Specifies the option message mode.	-
probe	Specifies the probe mode.	-
register	Specifies the register mode.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the mode used by a SIP AG to detect a proxy server, including the option message mode, probe mode, and register mode.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the mode used for detecting a proxy server to **register**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] proxy-detect-mode register
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.57 proxy-dhcp-option

Function

The **proxy-dhcp-option** command configures the mode used for sending DHCP requests.

The **undo proxy-dhcp-option** command restores the default mode used for sending DHCP requests.

By default, the mode used for sending DHCP request is none.

Format

proxy-dhcp-option *option-value*

undo proxy-dhcp-option

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
option-value	Sets the mode used for sending DHCP requests.	Enumerated type. The values are as follows: • None: sets the mode used for sending DHCP requests to none. • Option120: sets the mode used for sending DHCP requests to Option120. • Option21: sets the mode used for sending DHCP requests to Option21.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the mode used for sending DHCP requests to **Option120**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] proxy-dhcp-option Option120
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.58 proxy-dual-home

Function

Using the **proxy-dual-home** command, you can configure the mode in which a SIP AG is dual homed to proxy servers.

Using the **undo proxy-dual-home** command, you can restore the default mode in which a SIP AG is dual homed to proxy servers.

By default, a SIP AG supports dual homing but does not support automatic switchover.

Format

proxy-dual-home { **disable** | **manual-switchover** | **auto-switchover** }

undo proxy-dual-home

Parameters

Parameter	Description	Value
disable	Disables dual-homing.	-
manual-switchover	Enables dual-homing and disables automatic switchover.	-
auto-switchover	Enables dual-homing and automatic switchover.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the mode in which a SIP AG is dual homed to proxy servers. The mode can be disabled dual-homing, enabled dual-homing and disabled automatic switchover, or enabled dual-homing and automatic switchover.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the mode in which a SIP AG is dual homed to proxy servers to **auto-switchover**

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] proxy-dual-home auto-switchover
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.1.59 proxy-refresh-mode

Function

Using the **proxy-refresh-mode** command, you can configure the mode used by a SIP AG to update the proxy server address.

Using the **undo proxy-refresh-mode** command, you can restore the default mode used by a SIP AG to update the proxy server address.

By default, a SIP AG updates the proxy server IP address after a delay (defer mode).

Format

proxy-refresh-mode { **no-switch** | **defer** | **immediate** }

undo proxy-refresh-mode

Parameters

Parameter	Description	Value
no-switch	Indicates that the proxy server address is not updated.	-
defer	Indicates that the proxy server address is updated after a delay.	-
immediate	Indicates that the proxy server address is updated immediately.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the mode used by a SIP AG to update the proxy server address, including no update, deferred update, and immediate update.

 Copyright © Huawei Technologies Co., Ltd.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure a SIP AG to update the proxy server address immediately.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] proxy-refresh-mode immediate
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.60 proxy-switchover

Function

Using the **proxy-switchover** command, you can register a SIP AG with the specified proxy server.

Format

proxy-switchover { **primary** | **secondary** }

Parameters

Parameter	Description	Value
primary	Indicates the primary proxy server.	-
secondary	Indicates the secondary proxy server.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

When you need to maintain or troubleshoot the current proxy server, run this command. After this command is executed successfully, the SIP AG registers with the specified proxy server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Register a SIP AG with the specified secondary server.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] proxy-switchover secondary
  Are you sure to switch proxy?(y/n)[n]:
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.61 redundancy-negotiation-mode

Function

The **redundancy-negotiation-mode** command configures the mode used to start the RFC 2198 redundancy transmission based on the negotiation.

The **undo redundancy-negotiation-mode** command restores the default mode used to start the RFC 2198 redundancy transmission based on the negotiation.

The default mode is **no-initiative-start**.

Format

redundancy-negotiation-mode *negotiation-mode*

undo redundancy-negotiation-mode

Parameters

Parameter	Description	Value
negotiation-mode	Sets the mode used to start the RFC 2198 redundancy transmission based on the negotiation.	Enumerated type. The values are as follows: • **negotiation**: configures the initiative startup mode. • **fixed-start**: configures the fixed startup mode. • **no-initiative-start**: configures the no-initiative startup mode.

Views

SIP AG view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the mode used to start the RFC 2198 redundancy transmission based on the negotiation. You can use the following modes:

- Initiative startup: You can start the RFC 2198 redundancy transmission only after the negotiation between the local end and the remote end succeeds. The negotiation may be initiated by the local end or remote end.
- Fixed startup: The local end does not initiate negotiations but receives initiated negotiations. In fixed startup mode, RFC 2198 redundancy transmission is started based on the local configuration regardless of the negotiation result.
- No-initiative startup: You can start the RFC 2198 redundancy transmission based on the negotiation only after the local end receives negotiation invitations from the remote end. If the negotiation fails, the RFC 2198 redundancy transmission is not started.

Example

Set the mode used for starting the RFC 2198 redundancy transmission to **fixed-start**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] redundancy-negotiation-mode fixed-start
```

Related Topics

16.6.1.23 display voice sipag redundancy

16.6.1.62 redundancy-nte

Function

Using the **redundancy-nte** command, you can enable a SIP AG to use RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.

Using the **undo redundancy-nte** command, you can disable a SIP AG from using RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.

By default, a SIP AG is disabled from using RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.

Format

redundancy-nte { **enable** | **disable** }

undo redundancy-nte

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
enable	Enables a SIP AG to use RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.	-
disable	Disables a SIP AG from using RFC 2198 redundancy transmission to transmit the RFC 2833 audio data.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enable a SIP AG to use RFC 2198 redundancy transmission to transmit the RFC 2833 audio data or disable this function.

Example

Enable a SIP AG to use RFC 2198 to transmit the RFC 2833 audio data.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] redundancy-nte enable
```

Related Topics

16.6.1.23 display voice sipag redundancy

16.6.1.63 redundancy-start-mode

Function

The **redundancy-start-mode** command configures the mode used by a SIP AG to start RFC 2198 redundancy transmission.

The **undo redundancy-start-mode** command restores the default mode used by a SIP AG to start RFC 2198 redundancy transmission.

By default, **ordinary** is used to start RFC 2198 redundancy transmission.

 Copyright © Huawei Technologies Co., Ltd.

Format

redundancy-start-mode *mode-value*

undo redundancy-start-mode

Parameters

Parameter	Description	Value
mode-value	Specifies the mode used by a SIP AG to start RFC 2198 redundancy transmission.	Enumerated type. The values are as follows: • **ordinary**: indicates the ordinary mode used to start RFC 2198 redundancy transmission. • **smart**: indicates the smart mode used to start RFC 2198 redundancy transmission.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

In smart mode, RFC 2198 redundancy transmission is started automatically when packet loss occurs.

Example

Set the mode used for starting RFC 2198 redundancy transmission to **smart**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] redundancy-start-mode smart
```

Related Topics

16.6.1.23 display voice sipag redundancy

16.6.1.64 redundancy-vbd

Function

Using the **redundancy-vbd** command, you can enable a SIP AG to use RFC 2198 redundancy transmission to transmit voice-band data (VBD).

Using the **undo redundancy-vbd** command, you can disable a SIP AG from using RFC 2198 redundancy transmission to transmit VBD.

By default, a SIP AG is enabled to use RFC 2198 redundancy transmission to transmit VBD.

Format

redundancy-vbd { **enable** | **disable** }

undo redundancy-vbd

Parameters

Parameter	Description	Value
enable	Enables a SIP AG to use RFC 2198 redundancy transmission to transmit VBD.	-
disable	Disables a SIP AG from using RFC 2198 redundancy transmission to transmit VBD.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enable a SIP AG to use RFC 2198 redundancy transmission to transmit VBD or disable this function.

Example

Enable a SIP AG to use RFC 2198 redundancy transmission to transmit VBD.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] redundancy-vbd enable
```

Related Topics

16.6.1.23 display voice sipag redundancy

16.6.1.65 redundancy-voice

Function

Using the **redundancy-voice** command, you can enable a SIP AG to use RFC 2198 redundancy transmission to transmit voice.

Using the **undo redundancy-voice** command, you can disable a SIP AG from using RFC 2198 redundancy transmission to transmit voice.

By default, a SIP AG does not use RFC 2198 redundancy transmission to transmit voice.

Format

redundancy-voice { **enable** | **disable** }

undo redundancy-voice

Parameters

Parameter	Description	Value
enable	enable a SIP AG to use RFC 2198 redundancy transmission to transmit voice.	-
disable	disable a SIP AG to use RFC 2198 redundancy transmission to transmit voice.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to enable a SIP AG to use RFC 2198 redundancy transmission to transmit voice or disable this function.

Example

Enable a SIP AG to use RFC 2198 redundancy transmission to transmit voice.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] redundancy-voice enable
```

Related Topics

16.6.1.23 display voice sipag redundancy

16.6.1.66 register-server-uri (SIP AG view)

Function

The **register-server-uri** command configures a registrar uniform resource identifier (URI) for a SIP AG.

The **undo register-server-uri** command deletes the registrar URI of a SIP AG.

By default, no registrar URI is configured for a SIP AG.

Format

register-server-uri *uri*

undo register-server-uri

Parameters

Parameter	Description	Value
uri	Specifies the registrar URI of a SIP AG.	The value is a string of 1 to 64 case-sensitive characters.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

If no registrar URI is configured, the domain name, as a mandatory attribute, is used for registration.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the registrar URI of a SIP AG to **register**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] register-server-uri register
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.67 reset sctp-association-statistics

Function

Using the **reset sctp-association-statistics** command, you can delete the statistics about the SCTP associations on a SIP AG.

Format

reset sctp-association-statistics

Parameters

None.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

An association is a logical relation (channel) used for data transmission, which is established by two SCTP endpoints using the 4-way handshake mechanism of SCTP. You can run this command to delete the statistics about the SCTP associations on a SIP AG. If the operation succeeds, the statistics about the association between SCTP ends are initialized.

Example

Delete the statistics about SCTP associations on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] reset sctp-association-statistics
```

Related Topics

16.6.1.15 display voice sipag

 Copyright © Huawei Technologies Co., Ltd.

16.6.1.68 reset sctp-global-statistics

Function

Using the **reset sctp-global-statistics** command, you can delete global Stream Control Transmission Protocol (SCTP) statistics.

Format

reset sctp-global-statistics

Parameters

None

Views

Voice view

Default Level

3: Management level

Usage Guidelines

The **reset sctp-global-statistics** command deletes all the global SCTP statistics. After this command is executed, global SCTP statistics are initialized.

Example

Delete global SCTP statistics.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] reset sctp-global-statistics
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.69 reset (SIP AG view)

Function

The **reset** command resets a SIP AG.

Format

reset

Parameters

None.

Views

SIP AG view

Default Level

3: Management level

Usage Guidelines

You can run this command to enable the modified attributes of a SIP AG and start the new SIP AG. If the operation succeeds, the SIP AG is reset. After the reset is complete, the SIP AG can work properly and configured attributes take effect immediately.

NOTE

Use this command with caution because resetting a SIP AG affects current services.

Example

Reset a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] reset
Are you sure to reset MG interface?(y/n)[n]:y
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.70 ring-mode

Function

Using the **ring-mode** command, you can configure the ringing parameters of a SIP AG.

Using the **undo ring-mode** command, you can restore the default ringing parameters of a SIP AG.

By default, no ringing parameter is configured.

Format

ring-mode *index ringmode-name* [**cadence-ring** *cadencering-value* | **initial-ring** *initialring-value*] *

undo ring-mode [*index*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
index	Specifies the index of a ring mapping.	The value is an integer that ranges from 0 to 15.
ringmode-name	Specifies the name of a ringing mapping.	The value is a string of 1 to 32 characters.
cadence-ring *cadencering-value*	Specifies the type of the cadence ringing.	The value range is 0 to 3, 6, 8 to 15, 128 to 143, and 255. The value is an integer.
initial-ring *initialring-value*	Specifies the type of the initial ringing.	The value range is 4, 17, 18, 22, 24 to 26, 29 to 31, 144 to 159, and 255. The value is an integer.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The meanings of *ringmode-name* value is that the sipaguser will ring as the ringing mode specified by ringmode-name, when the *ringmode-name* string matches the Alert-Info header field in the INVITE message.

The meanings of **cadence-ring** values are as follows:

- 0: normal ring 1:4 (1:4 is the cadence ratio, in the sequence of ring, stop, ring...)
- 1: special ringing 1:2
- 2: special ringing 0.4:0.2:0.4:4
- 3: long ringing
- 6: special ringing 1.2:2
- 8: HK ringing 1:3
- 9: HK CNTRX 0.4:0.2:0.4:0.2:0.4:3.0
- 10: HK DN-A 0.4:0.2:0.4:3.0
- 11: HK ACB 0.4:0.2
- 12: HK reminder ringing (one tone every 0.4 second; only one tone is generated at a time.)
- 13: HK DN-B 1.2:3

 Copyright © Huawei Technologies Co., Ltd.

- 14: CNTRX_IN 0.4:0.2:0.4:0.2:0.4:2.6
- 15: Egypt long-distance ringing 2:1
- 128-143: user-defined ringing mode 0-15
- 255: NULL, indicating the default ringing mode.

The meanings of **initial-ring** values are as follows:

- 4: normal ringing (FSK) 1:4
- 17: special ringing (FSK) 1:2
- 18: special ringing (FSK) 0.4:0.2:0.4:4
- 22: special ringing (FSK) 1.2:2
- 24: HK Ring (FSK) 1:3
- 25: HK CNTRX (FSK) 0.4:0.2:0.4:0.2:0.4:3.0
- 26: HK DN-A (FSK) 0.4:0.2:0.4:3.0
- 29: HK DN-B (FSK) 1.2:3
- 30: CNTRX_IN (FSK) 0.4:0.2:0.4:0.2:0.4:2.6
- 31: Egypt long-distance ringing (FSK) 2:1
- 144-159: user-defined ringing mode (FSK) 0-15
- 255: NULL, indicating the default ringing mode.

Example

Configure the ringing parameters on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] ring-mode 1 huawei cadence-ring 2
[Huawei-voice-sipag-1] ring-mode 1 huawei initial-ring 4
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.71 scene

Function

Using the **scene** command, you can configure the mapping between a call scenarios and a signal.

Using the **undo scene** command, you can delete the mapping between a scenario and a signal.

Format

scene *scene-value*

undo scene *scene-value*

Parameters

Parameter	Description	Value
scene-value	Specifies the name of a scenario that maps a signal.	The value is a string of 1 to 25 characters.

Views

Signal view

Default Level

2: Configuration level

Usage Guidelines

The scenario name must comply with the following rules:

- The local scenario name beginning with local can only be system-defined.
- **status:xxx** indicates the SIP response code scenario, and **xxx** indicates the response code. The value ranges from 300 to 703. The values ranging from 700 to 703 indicate the universal status code, among which 700 indicates 3xx, 701 indicates 4xx, 702 indicates 5xx, and 703 indicates 6xx.
- **reason:xxx** indicates the Q850 scenario, and **xxx** indicates the Q850 value. The value ranges from 0 to 127.
- **map:xxx** indicates the name mapping scenario, and **xxx** indicates the sub-scenario name. The value is a string of 1 to 21 characters. The sub-scenario name and **map:** form a scenario name.

Example

Configure the mapping between the scenario and signal.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] signal 1 test
[Huawei-voice-signal-test] scene status:500
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.72 sctp

Function

Using the **sctp** command, you can configure Stream Control Transport Protocol (SCTP) stack parameters for a SIP AG.

Using the **undo sctp** command, you can restore the default SCTP stack parameters of a SIP AG.

Format

sctp { **assoc-maximum-retransmission** *assoc-max-retrans* | **checksum-arithmetic** *checksum-arith* | **heartbeat-interval** *hb-interval* | **high-congestion-level** *high-congestion-level-value* | **in-stream-number** *in-stream-num* | **low-congestion-level** *low-congestion-level-value* | **maximum-init-retransmission** *max-init-retrans* | **no-congestion-level** *no-congestion-level-value* | **out-stream-number** *out-stream-num* | **path-maximum-retransmission** *path-max-retrans* | **rto-alpha** *rto-alpha-value* | **rto-beta** *rto-beta-value* | **rto-init** *rto-init-value* | **rto-maximum** *rto-max* | **valid-cookie-life** *valid-cookie-life-value* }

undo sctp { **assoc-maximum-retransmission** | **checksum-arithmetic** | **heartbeat-interval** | **high-congestion-level** | **in-stream-number** | **low-congestion-level** | **maximum-init-retransmission** | **no-congestion-level** | **out-stream-number** | **path-maximum-retransmission** | **rto-alpha** | **rto-beta** | **rto-init** | **rto-maximum** | **valid-cookie-life** }

Parameters

Parameter	Description	Value
assoc-maximum-retransmission *assoc-max-retrans*	Specifies the maximum number of times an association request is retransmitted. This parameter is optional.	The value is an integer that ranges from 8 to 16. The default value is 10.
checksum-arithmetic *checksum-arith*	Specifies the checksum algorithm. This parameter is optional.	The value can be adler 32 or crc 32, in enumerated type. The default value is crc32.
heartbeat-interval *hb-interval*	Specifies the heartbeat interval. This parameter is optional.	The value is an integer that ranges from 10000 to 120000, in milliseconds. The default value is 10000 ms.
high-congestion-level *high-congestion-level-value*	Specifies the level of high traffic congestion. This parameter is optional. *high-congestion-level-value* must be larger than *low-congestion-level-value*.	The value is an integer that ranges from 70 to 100. The default value is 80.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
in-stream-number *in-stream-num*	Specifies the number of input SCTP streams. This parameter is optional. You can use this parameter to configure the number of input SCTP streams added to the link on the ISDN Q.921-User Adaptation (IUA) layer. You can set a value for this parameter or use the default value.	The value is an integer and varies according to models. ● AR150&160&200, AR1200, and AR2204: 2 - 33 ● AR2220: 2 - 56 ● AR2240: 2 - 86 ● AR3200: 2 - 152 The default value is 33
low-congestion-level *low-congestion-level-value*	Specifies the level of low traffic congestion. This parameter is optional. This parameter is used to configure the level of low traffic congestion. *low-congestion-level-value* must be smaller than *high-congestion-level-value*.	The value is an integer that ranges from 50 to 80. The default value is 60.
maximum-init-retransmission *max-init-retrans*	Specifies the maximum number of times an init message is retransmitted. An init message is transmitted when a 4-way handshake is performed to establish an SCTP association. This parameter is optional.	The value is an integer that ranges from 3 to 10. The default value is 8.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-congestion-level *no-congestion-level-value*	Specifies the level of no traffic congestion. This parameter is optional. This parameter is used to configure the level of no traffic congestion. *no-congestion-level-value* must be smaller than *low-congestion-level-value* and *high-congestion-level-value*.	The value is an integer that ranges from 1 to 60. The default value is 40.
out-stream-number *out-stream-num*	Specifies the number of output SCTP streams. This parameter is optional. You can set a value for this parameter or use the default value.	The value is an integer and varies according to models. ● AR150&160&200, AR1200, and AR2204: 2 - 33 ● AR2220: 2 - 56 ● AR2240: 2 - 86 ● AR3200: 2 - 152 The default value is 33
path-maximum-retransmission *path-max-retrans*	Specifies the maximum number of times a path is retransmitted. This parameter is optional.	The value is an integer that ranges from 3 to 8. The default value is 5.
rto-alpha *rto-alpha-value*	Specifies the alpha factor in the timeout period of retransmissions. This parameter is optional. *rto-alpha-value* cannot be greater than *rto-beta-value*.	The value is an integer that ranges from 1 to 100. The default value is 12.
rto-beta *rto-beta-value*	Specifies the beta factor in the timeout period of retransmissions. This parameter is optional. *rto-beta-value* is not smaller than *rto-alpha-value*.	The value is an integer that ranges from 1 to 100. The default value is 25.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rto-init *rto-init-value*	Specifies the initial timeout period of retransmissions. This parameter is optional.	The value is an integer that ranges from 1000 to 90000, in milliseconds. The default value is 1000 ms.
rto-maximum *rto-max*	Specifies the maximum timeout period of retransmissions. This parameter is optional. *rto-max* must be larger than *rto-init-value* so that the configuration takes effect.	The value is an integer that ranges from 3000 to 90000, in milliseconds. The default value is 3000 ms.
valid-cookie-life *valid-cookie-life-value*	Specifies the life cycle of a valid cookie. This parameter is optional.	The value is an integer that ranges from 3000 to 120000, in milliseconds. The default value is 60000 ms.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to modify the SCTP stack parameters of a SIP AG.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the SCTP stack parameters of a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] sctp rto-maximum 30000
[Huawei-voice-sipag-1] sctp rto-init 4000
[Huawei-voice-sipag-1] sctp valid-cookie-life 40000
[Huawei-voice-sipag-1] sctp heartbeat-interval 50000
[Huawei-voice-sipag-1] sctp rto-alpha 4
[Huawei-voice-sipag-1] sctp rto-beta 60
[Huawei-voice-sipag-1] sctp assoc-maximum-retransmission 12
[Huawei-voice-sipag-1] sctp path-maximum-retransmission 5
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-voice-sipag-1] sctp no-congestion-level 40
[Huawei-voice-sipag-1] sctp low-congestion-level 50
[Huawei-voice-sipag-1] sctp high-congestion-level 88
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.73 sdp-negotiation-mode

Function

Using the **sdp-negotiation-mode** command, you can configure the mode used for Session Description Protocol (SDP) negotiation.

Using the **undo sdp-negotiation-mode** command, you can restore the default SDP negotiation mode of a SIP AG.

By default, the remote priority mode is used for SDP negotiation.

Format

sdp-negotiation-mode { **local** | **remote** }

undo sdp-negotiation-mode

Parameters

Parameter	Description	Value
local	Indicates the local priority mode.	-
remote	Indicates the remote priority mode.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the SDP negotiation mode for a SIP AG, including the local priority mode and remote priority mode.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the SDP negotiation mode of a SIP AG to **local**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] sdp-negotiation-mode local
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.74 secondary-proxy-addr dns-a

Function

The **secondary-proxy-addr dns-a** command configures the DNS-A domain name and port number of the secondary proxy server.

The **undo secondary-proxy-addr** command deletes the DNS-A domain name and port number of the secondary proxy server.

By default, no DNS-A domain name or port number is configured for the secondary proxy server.

Format

secondary-proxy-addr dns-a *dns-a-domain-name dns-a-port-number*

undo secondary-proxy-addr

Parameters

Parameter	Description	Value
dns-a-domain-name	Specifies the DNS-A domain name of the secondary proxy server.	The value is a string of 1 to 64 characters.
dns-a-port-number	Specifies the port number of the DNS-A domain name.	The value is an integer that ranges from 1 to 65535.

Views

SIP AG view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the DNS-A domain name and port number of the secondary proxy server on a SIP AG to www.abcd.com and 5060.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] secondary-proxy-addr dns-a www.abcd.com 5060
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.75 secondary-proxy-addr dns-naptr

Function

The **secondary-proxy-addr dns-naptr** command configures the DNS-NAPTR domain name of the secondary proxy server.

The **undo secondary-proxy-addr** command deletes the DNS-NAPTR domain name of the secondary proxy server.

By default, no DNS-NAPTR domain name is configured for the secondary proxy server.

Format

secondary-proxy-addr dns-naptr *dns-naptr-domain-name*

undo secondary-proxy-addr

Parameters

Parameter	Description	Value
dns-naptr-domain-name	Specifies the DNS-NAPTR domain name of the secondary proxy server.	The value is a string of 1 to 64 characters.

Views

SIP AG view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the DNS-NAPTR domain name of the secondary proxy server on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] secondary-proxy-addr dns-naptr www.abcd.com
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.76 secondary-proxy-addr dns-srv

Function

The **secondary-proxy-addr dns-srv** command configures the DNS-SRV domain name of the secondary proxy server.

The **undo secondary-proxy-addr** command deletes the DNS-SRV domain name of the secondary proxy server.

By default, no DNS-SRV domain name is configured for the secondary proxy server.

Format

secondary-proxy-addr dns-srv *dns-srv-domain-name*

undo secondary-proxy-addr

Parameters

Parameter	Description	Value
dns-srv-domain-name	Specifies the DNS-SRV domain name of the secondary proxy server.	The value is a string of 1 to 64 characters.

Views

SIP AG view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the DNS-SRV domain name of the secondary proxy server on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] secondary-proxy-addr dns-srv www.abcd.com
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.77 secondary-proxy-addr static

Function

The **secondary-proxy-addr static** command configures the static IP address and port number of the secondary proxy server.

The **undo secondary-proxy-addr** command deletes the static IP address and port number of the secondary proxy server.

By default, no static IP address or port number is configured for the secondary proxy server.

Format

secondary-proxy-addr static *static-ip-address static-ip-address-port* [**secondary** *static-ip-address2*]

undo secondary-proxy-addr

Parameters

Parameter	Description	Value
static-ip-address	Specifies a static IP address for the secondary proxy server.	The value is in dotted decimal notation.
static-ip-address-port	Specifies the port number of the static IP address.	The value is an integer that ranges from 1 to 65535.
secondary *static-ip-address2*	Specifies a static IP address 2 for the secondary proxy server.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

Before configuring the secondary proxy server, configure the primary proxy server.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the static IP address and port number of the secondary proxy server on a SIP AG to 192.168.1.1 and 5060.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] secondary-proxy-addr static 192.168.1.1 5060
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.78 service-logic

Function

The **service-logic** command configures the index of the service logic used by a SIP AG.

The **undo service-logic** command restores the default index of the service logic used by a SIP AG.

By default, the service logic index of a SIP AG is 0.

Format

service-logic *service-logic-index*

undo service-logic

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
service-logic-index	Specifies the index of the service logic used by a SIP AG.	The value is an integer that ranges from 0 to 9: • 0: default service logic • 1: pre-configured service logic with the index DT-AGW/1 • 2: pre-configured service logic with the index CHINA-MOBILE/1 • 3: pre-configured service logic with the index NWT-WTT/1 • 4: pre-configured service logic with the index BT/1

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the index of the service logic used by a SIP AG to 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] service-logic 1
```

Related Topics

16.6.1.15 display voice sipag

 Copyright © Huawei Technologies Co., Ltd.

16.6.1.79 signal

Function

The **signal** command configures a signal name for a SIP AG.

The **undo signal** command deletes a signal name.

Format

signal *sipag-interface-id signal-name*

undo signal *sipag-interface-id signal-name*

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the interface ID of a SIP AG.	The value is an integer that ranges from 0 to 16777215.
signal-name	Specifies a signal name for a SIP AG.	The value is a string of 1 to 20 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

This command configures a signal name for a SIP AG and displays the signal view.

Example

Set the interface ID to 1 and signal name to **test** on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] signal 1 test
[Huawei-voice-signal-test]
```

Related Topics

16.6.1.15 display voice sipag

 Copyright © Huawei Technologies Co., Ltd.

16.6.1.80 signalling-addr

Function

The **signalling-addr** command configures a signaling IP address for a SIP AG or specifies the name of a signaling IP address and port number.

The **undo signalling-addr** command deletes the signaling IP address, its name and port number.

By default, no signaling IP address or port number is configured for a SIP AG.

Format

signalling-addr { *signal-ip* | **addr-name** *signal-addr-name* } *signal-port*

undo signalling-addr

Parameters

Parameter	Description	Value
signal-ip	Specifies the signaling IP address of a SIP AG.	The value is in dotted decimal notation.
addr-name *signal-addr-name*	Specifies the name of the signaling IP address.	The value is a string of 1 to 64 characters.
signal-port	Specifies the port number used in signaling exchange.	The value is an integer that ranges from 5000 to 5999.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

To exchange signaling messages with other devices, a SIP AG must have a signaling IP address and port number configured. When configuring the signaling IP address or IP address name, ensure that:

- The specified IP address must be in the signaling IP address pool.
- The specified IP address name must exist.

Precautions

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure an existing signaling IP address 192.168.1.1 for a SIP AG and set the port number to 5060.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] signalling-addr 192.168.1.1 5060
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.81 sipag

Function

The **sipag** command creates a SIP AG interface and displays the SIP AG interface view.

The **undo sipag** command deletes a SIP AG interface.

By default, no SIP AG interface is created.

Format

sipag *sipag-interface-id*

undo sipag *sipag-interface-id*

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the interface ID of a SIP AG.	The value is an integer that ranges from 0 to 16777215.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When a SIP AG is required to communicate with the remote device, use the **sipag** command to create a SIP AG interface. If the specified SIP AG interface exists, the SIP AG interface view is displayed. After creating a SIP AG interface, you can configure attributes, control points, and protocol stack parameters for the SIP AG interface. When deleting a SIP AG interface, pay attention to the following points:

 Copyright © Huawei Technologies Co., Ltd.

- Before deleting a SIP AG interface, delete all the user number configured on the SIP AG interface.
- Before deleting a SIP AG interface, disable SIP AG interface.
- When a SIP AG interface is deleted, configurations of the SIP AG interface including ring mappings and control points are deleted.

Example

Create SIP AG 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1]
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.82 sip-reg-count-per-second

Function

The **sip-reg-count-per-second** command sets the number of SIP register messages sent every second.

The **undo sip-reg-count-per-second** command restores the default number of SIP register messages sent every second.

By default, five SIP register messages are sent every second.

Format

sip-reg-count-per-second *reg-count-value*

undo sip-reg-count-per-second

Parameters

Parameter	Description	Value
reg-count-value	Specifies the number of SIP register messages sent every second.	The value is an integer that ranges from 1 to 1024.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Set the number of SIP register messages sent every second to 3.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sip-reg-count-per-second 3
```

16.6.1.83 status-code-mapping

Function

Using the **status-code-mapping** command, you can configure the mapping between a call scenario and a status code on a SIP AG.

Using the **undo status-code-mapping** command, you can delete a mapping between a call scenario and a status code.

Format

status-code-mapping *scene status-code*

undo status-code-mapping *scene*

Parameters

Parameter	Description	Value
scene	Specifies a call scenario.	The value is an integer that ranges from 0 to 18.
status-code	Specifies a status code.	The value is an integer that ranges from 400 to 699.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

When using the **status-code-mapping** command, note the following:

- If default status codes defined in the system cannot meet requirements, you can define status codes for different call scenarios.

 Copyright © Huawei Technologies Co., Ltd.

- After configuring the status code of a call scenario, reset the SIP AG so that the configuration can take effect.
- The status code of a scenario is contained in the response message when this scenario occurs during a call.

The following table lists mappings between scenarios and status codes on a SIP AG.

Scenario	Description	Status Code
0	The CPU is overloaded.	The value is an integer that ranges from 400 to 699. The default value is 503.
1	The power consumption exceeds the threshold.	The value is an integer that ranges from 400 to 699. The default value is 503.
2	The called party does not exist.	The value is an integer that ranges from 400 to 699. The default value is 404.
3	The specified port is occupied by another user account.	The value is an integer that ranges from 400 to 699. The default value is 486.
4	A port does not have a license.	The value is an integer that ranges from 400 to 699. The default value is 480.
5	A port is quitting the service after a delay.	The value is an integer that ranges from 400 to 699. The default value is 480.
6	A port is blocked.	The value is an integer that ranges from 400 to 699. The default value is 480.
7	The port is being blocked.	The value is an integer that ranges from 400 to 699. The default value is 486.

 Copyright © Huawei Technologies Co., Ltd.

Scenario	Description	Status Code
8	A port is being tested.	The value is an integer that ranges from 400 to 699. The default value is 486.
9	A user has not quit the service.	The value is an integer that ranges from 400 to 699. The default value is 480.
10	Digital signal processing (DSP) resources are insufficient.	The value is an integer that ranges from 400 to 699. The default value is 488.
11	System resources are insufficient.	The value is an integer that ranges from 400 to 699. The default value is 500.
12	The call is controlled by the calling party or called party.	The value is an integer that ranges from 400 to 699. The default value is 606.
13	The call is being connected to the called user.	The value is an integer that ranges from 400 to 699. The default value is 486.
14	The called user is talking.	The value is an integer that ranges from 400 to 699. The default value is 486.
15	The ringing time exceeds the timeout period.	The value is an integer that ranges from 400 to 699. The default value is 487.
16	The call is rejected in call waiting mode.	The value is an integer that ranges from 400 to 699. The default value is 486.
17	The call times out in call waiting mode.	The value is an integer that ranges from 400 to 699. The default value is 486.

 Copyright © Huawei Technologies Co., Ltd.

Scenario	Description	Status Code
18	The user hangs up to release the waiting call in semi-tight coupling mode.	The value is an integer that ranges from 400 to 699. The default value is 410.

Precautions

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure the mapping between a call scenario and a status code.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] status-code-mapping 8 405
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.84 subscribe mwi

Function

Using the **subscribe mwi** command, you can enable or disable the message waiting indicator (MWI) subscription function on a SIP AG.

Using the **undo subscribe mwi** command, you can restore the default status of the MWI subscription function.

By default, the MWI subscription function is disabled on a SIP AG.

Format

subscribe mwi { **enable** | **disable** }

undo subscribe mwi

Parameters

Parameter	Description	Value
enable	Enables the MWI subscription function.	-
disable	Disables the MWI subscription function.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **subscribe mwi** command enables or disables the MWI subscription function.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Enable the MWI subscription function on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] subscribe mwi enable
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.85 subscribe reg

Function

Using the **subscribe reg** command, you can enable or disable the register status subscription function on a SIP AG.

Using the **undo subscribe reg** command, you can restore the default status of the register status subscription function.

By default, the status subscription function is disabled on a SIP AG.

Format

subscribe reg { **enable** | **disable** }

undo subscribe reg

Parameters

Parameter	Description	Value
enable	Enables the register status subscription function.	-

Parameter	Description	Value
disable	Disables the register status subscription function.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **subscribe reg** command enables or disables the register status subscription function.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Enable the register status subscription function on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] subscribe reg enable
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.86 subscribe ua-profile

Function

Using the **subscribe ua-profile** command, you can enable or disable the user authority (UA) profile subscription function on a SIP AG.

Using the **undo subscribe ua-profile** command, you can restore the default status of the UA profile subscription function.

By default, the UA profile subscription function is enabled on a SIP AG.

Format

subscribe ua-profile { **enable** | **disable** }

undo subscribe ua-profile

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
enable	Enables the UA profile subscription function.	-
disable	Disables the UA profile subscription function.	-

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **subscribe ua-profile** command enables or disables the UA profile subscription function.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Enable the UA profile subscription function on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] subscribe ua-profile enable
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.87 transfer (SIP AG view)

Function

The **transfer** command specifies the transmission protocol used by a SIP AG.

The **undo transfer** command restores the default transmission protocol used by a SIP AG.

By default, a SIP uses the User Datagram Protocol (UDP) protocol as the transmission protocol.

Format

transfer *transfer-protocol*

 Copyright © Huawei Technologies Co., Ltd.

undo transfer

Parameters

Parameter	Description	Value
transfer-protocol	Specifies the transmission protocol type.	Enumerated type. The values are as follows: • TCP: specifies the Transmission Control Protocol (TCP) as the transmission protocol. • UDP: specifies UDP as the transmission protocol. • SCTP: specifies SCTP as the transmission protocol.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Configure a SIP AG to use UDP as the transmission protocol.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] transfer udp
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.88 unit

Function

Using the **unit** command, you can configure attributes of a signal unit.

Using the **undo unit** command, you can delete the configured attribute values of a signal unit.

Format

unit *unit-seq* { **duration** *duration-value* | **end-condition** *end-condition-value* | **repeat** *repeat-value* | **start-condition** *start-condition-value* | **type** *type-value* }

undo unit *unit-seq* [**repeat** | **duration**]

Parameters

Parameter	Description	Value
unit-seq	Specifies the sequence number of a signal unit.	The value is an integer that ranges from 0 to 7.
duration *duration-value*	Specifies the duration of a signal unit.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.
end-condition *end-condition-value*	Specifies the condition that will trigger start of a signal unit.	The value is a string of 1 to 35 characters.
repeat *repeat-value*	Specifies the number of times a signal unit can be repeated.	The value is an integer that ranges from 0 to 255.
start-condition *start-condition-value*	Specifies the condition that will trigger end of a signal unit.	The value is a string of 1 to 35 characters.
type *type-value*	Specifies a signal unit type.	The value is a string of 1 to 15 characters.

Views

Signal view

Default Level

2: Configuration level

Usage Guidelines

The signal unit type string complies with the following rules:

- The signal unit type string must be in *main type*:*sub-type* format.
- The values of the main type and sub-type are:
  - If the main type is tone, the sub-type is the tone ID, for example, tone:1.

- If the main type is data, the sub-type is fixed at 0. The signal unit type string is data:0.
- If the main type is init (indicating initial ring), the sub-type is a ring mapping ID. You can view the configured ring mapping IDs by using the **display ringmode** command. If the ring mapping ID is 100, the default ringing mode is used. For example, the signal unit type string can be init:100.
- If the main type is cade (indicating cadence ring), the sub-type is a ring mapping ID. You can view the configured ring mapping IDs by using the **display ringmode** command. If the ring mapping ID is 100, the default ringing mode is used. For example, the signal unit type string can be cade:100.
- If the main type is pole (indicating polarity reversal), the sub-type 0 or 1, for example, pole:1. The value 0 indicates non-polarity reversal, the value indicates polarity reversal.
- If the main type is trans (indicating transmission enabled), the sub-type is fixed at 0. The signal unit type string is trans:0.
- If the main type is pulse, the sub-type is fixed at 0. The signal unit type string is pulse:0.
- If the main type is mwi, the sub-type is fixed at 0. The signal unit type string is mwi:0.

The condition that will trigger start of a signal unit contains a maximum of two sub-conditions. Each sub-condition defines an event or an event with a delay. The event and delay are separated by a colon (:). If a condition contains two sub-conditions, the sub-conditions are separated by the & or | sign. The & sign indicates that both sub-conditions must be met, and the | sign indicates that one of the sub-conditions must be met. The condition string complies with the following rules:

- An event must be one of the following: ss (signal starts), 0s (the first signal unit starts), 1s (the second signal unit starts), 2s (the third signal unit starts), 3s (the fourth signal unit starts), 0e (the first signal unit ends), 1e (the second signal unit ends), 2e (the third signal unit ends), 3e (the fourth signal unit ends), fs (fsk_start is reported), fe (fsk_end is reported), or te (tone_end is reported).
- If a sub-condition defines a delay, the sub-condition is met only when the delay expires after the specified event happens.
- If a sub-condition defines no delay, the sub-condition is met immediately when the specified event happens.

The condition that will trigger end of a signal unit contains a maximum of two sub-conditions. Each sub-condition defines an event or an event with a delay. The event and delay are separated by a colon (:). If a condition contains two sub-conditions, the sub-conditions are separated by the & or | sign. The & sign indicates that both sub-conditions must be met, and the | sign indicates that one of the sub-conditions must be met. The condition string complies with the following rules:

- An event must be one of the following: ss (signal starts), 0s (the first signal unit starts), 1s (the second signal unit starts), 2s (the third signal unit starts), 3s (the fourth signal unit starts), 0e (the first signal unit ends), 1e (the second signal unit ends), 2e (the third signal unit ends), 3e (the fourth signal unit

ends), fs (fsk_start is reported), fe (fsk_end is reported), or te (tone_end is reported).

- If a sub-condition defines a delay, the sub-condition is met only when the delay expires after the specified event happens.
- If a sub-condition defines no delay, the sub-condition is met immediately when the specified event happens.

Example

Configure signal unit attributes on a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] signal 1 test
[Huawei-voice-signal-test] unit 2 duration 1
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.89 user-defined-profile codec-priority

Function

Using the **user-defined-profile codec-priority** command, you can configure the codec priority, codec value, and packetization interval for a SIP AG.

Using the **undo user-defined-profile codec-priority** command, you can delete the codec priority, codec value, and packetization interval.

Format

user-defined-profile codec-priority *pri-value codec-value pt-value*

undo user-defined-profile codec-priority [*pri-value*]

Parameters

Parameter	Description	Value
pri-value	Specifies a codec priority.	The value is an integer that ranges from 0 to 255.
codec-value	Specifies a codec value.	The value is an integer that ranges from 0 to 255.
pt-value	Specifies the packetization interval.	The value is an integer that ranges from 0 to 4294967295, in milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **user-defined-profile codec-priority** command configures the codec priority, codec value, and packetization interval for a SIP AG.

If you change the priority of a codec value, priorities of other codec values are also changed. For example, if you change the priority of a codec value from 4 to 2, the priorities of codec values with priorities of 2 and 3 are changed to 3 and 4. If you change the priority of a codec value from 4 to 6, the priorities of codec values with priorities of 5 and 6 are changed to 4 and 5.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the codec priority to 4, codec value to 8, and packetization interval to 20 milliseconds.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] user-defined-profile codec-priority 4 8 20
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.90 user-defined-profile number-parameter

Function

The **user-defined-profile number-parameter** command sets the control point with a specified sequence number for a SIP AG.

The **undo user-defined-profile number-parameter** command restores the default settings of all control points for a SIP AG.

Format

user-defined-profile number-parameter *strpara-no strpara-value*

undo user-defined-profile number-parameter *strpara-no*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
strpara-no	Specifies the sequence number of a control point.	The value is an integer that ranges from 1 to 331.
strpara-value	Specifies the value of a control point.	The value is an integer that ranges from 0 to 4294967295. The value of *strpara-value* varies according to *strpara-no*. For details, see the usage guideline.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The following table describes the meanings and values of control points.

Parameter	Description	Value
1	- **NOTE** This control object is discarded.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
2	Sets the call priority for SIP AG users.	Enumerated type. The options are as follows: ● 1: The calling party is preferred. When a user receives an INVITE message from the network side after picking up the phone, a 486 message is returned to reject the invitation. ● 2: The called party is preferred. When a user receives an INVITE message from the network side after picking up the phone, a 200 message is returned and the call is established. The default value is 1.
3	Sets the uniform resource identifier (URI) format for SIP AG users.	Enumerated type. The options are as follows: ● 1: TelNum@homedomain ● 2: TelNum@proxydomain ● 3: telURI The default value is 1.
4 to 6	- **NOTE** These objects are discarded.	-
7	Sets the maximum number of subscription attempts for SIP AG users.	The value is an integer that ranges from 1 to 10. The default value is 1.
8	- **NOTE** This control object is discarded.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
9	Sets the AOCE notification to ringing for SIP AG users. **NOTE** This control object is read-only.	The value is 1.
10	- **NOTE** This control object is discarded.	-
11	Indicates whether offhook of SIP AG users is immediately reported.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
12	Sets the reporting mode of the initial number for SIP AG users.	Enumerated type. The options are as follows: ● 0: digital map ● 1: Ta4+maximum number mode The default value is 0.
13	Sets whether to continue to make a call when distributed message manager (DMM) match fails for SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
14	Sets whether digits are reported one by one when a SIP AG user in In-Dialog state dials a number.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
15	Indicates whether to set the Prefer header field in SIP messages sent by SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
16	Indicates whether to set the Priority header field in SIP messages sent by SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
17	Indicates whether to set the VisitedNet header field in SIP messages sent by SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
18	Indicates whether to set the AccessNet header field in SIP messages sent by SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
19	Sets whether to send normal polarity when SIP AG users hang up.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
20	Sets whether to send normal polarity when SIP AG users pick up the phone.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
21	Sets whether to support the initial route setting for SIP AG users. When the initial route setting is supported, the ROUTE field is added to the INVITE and REGISTER messages.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
22	Sets the remote ringback tone mode for SIP AG users.	Enumerated type. The options are as follows: ● 0: No remote ringback tone is sent. ● 1: IETF mode (not supported) ● 2: TISPAN mode ● 3: common mode The default value is 0.
23	Sets the T303 timer for SIP AG users in OVERLAP state.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 64.
24	Sets the Ta2 timer of overlap sending for SIP AG users.	The value is an integer that ranges from 0 to 4294967294, in seconds. The default value is 15. The value 0 indicates that the Ta2 timer of overlap sending is disabled.
25	Sets the T301 timer for SIP AG users in ALERTING state.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 180.
26	Sets the T313 timer for SIP AG users in CONNECTREQ state.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 32.
27	Sets the timer for SIP AG users in ACTIVE state.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 120.
28	Sets the call waiting (CW) timer in the service logic process for SIP AG users.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 120.
29	Sets the short busy tone timer in the service logic process for SIP AG users.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 30.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
30	Sets the offhook timer in the service logic process for SIP AG users.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 60.
31	Sets the waiting time before the busy tone stops in the WAITHOOK subprocess to 20 seconds for SIP AG users. **NOTE** This control object is read-only.	The value is read-only, in seconds. The default value is 20.
32	Sets the waiting time before the howler tone stops in the WAITHOOK subprocess to 20 seconds for SIP AG users. **NOTE** This control object is read-only.	The value is read-only, in seconds. The default value is 20.
33	Sets the ringing tone delay to 500 ms for SIP AG users. **NOTE** This control object is read-only.	The value is read-only, in milliseconds. The default value is 500.
34	Sets the CID2 number sending timer for SIP AG users.	The value is an integer that ranges from 1 to 4294967294, in milliseconds. The default value is 45.
35	Sets whether to add the Date header field for SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
36	Sets the type of SIP messages sent by SIP AG users where the Allow header field is inserted.	The value is an integer ranging from 0 to 4294967295. ● 0: The Allow header field is inserted to no SIP messages. ● 1: REGISTER message ● 2: INVITE message ● 4: SUBSCRIBE message ● 8: BYE message ● 16: OPTIONS message ● 32: PRACK message ● 64: REFER message ● 128: UPDATE message ● 256: NOTIFY message ● 512: INFO message ● 1024: MESSAGE message ● 2048: REGISTER-2XX message ● 4096: SUBSCRIBE-2XX message ● 8192: INVITE-2XX message ● 16384: BYE-2XX message ● 32768: OPTIONS-2XX-AND-486 message ● 65536: PRACK-2XX message ● 131072: REFER-2XX message ● 262144: UPDATE-2XX message ● 524288: NOTIFY-2XX message ● 1048576: INFO-2XX message ● 2097152: MESSAGE-2XX message

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 4194304: INVITE-18X message The default value is 33007, indicating that the Allow header field is inserted to the REGISTER, INVITE, SUBSCRIBE, BYE, PRACK, REFER, UPDATE, and OPTIONS-2XX-AND-486 messages. **NOTE** When the Allow header field is inserted to multiple types of messages, set the value to the sum value of these types of messages. For example, when the Allow header field is inserted to the OPTIONS and PRACK messages, set the value to 48 (16+32).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
37	Sets the methods supported by the Allow header field in SIP messages.	The value is an integer ranging from 0 to 4294967295. ● 0: No method is supported. ● 1: INVITE method ● 2: ACK method ● 4: OPTIONS method ● 8: BYE method ● 16: CANCEL method ● 32: REGISTER method ● 64: INFO method ● 128: PRACK method ● 256: SUBSCRIBE method ● 512: NOTIFY method ● 1024: UPDATE method ● 2048: MESSAGE method ● 4096: REFER method ● 8192: PUBLISH method ● 16384: CONFSUB method The default value is 24575, indicating that INVITE, ACK, OPTIONS, BYE, CANCEL, REGISTER, INFO, PRACK, SUBSCRIBE, NOTIFY, UPDATE, MESSAGE, REFER, and CONFSUB methods are supported. **NOTE** When the Allow header field supports multiple methods, set the value to the sum value of these methods. For example, when the Allow header field supports the OPTIONS and PRACK methods, set the value to 132 (4+128).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
38	Sets the type of SIP messages sent by SIP AG users where the Support header field is inserted.	The value is an integer ranging from 0 to 4294967295. ● 0: The Support header field is inserted to no SIP messages. ● 1: REGISTER message ● 2: INVITE message ● 4: SUBSCRIBE message ● 8: BYE message ● 16: OPTIONS message ● 32: PRACK message ● 64: REFER message ● 128: UPDATE message ● 256: NOTIFY message ● 512: INFO message ● 1024: MESSAGE message ● 2048: CANCEL message ● 4096: REGISTER-2XX message ● 8192: INVITE-2XX message ● 16384: SUBSCRIBE-2XX message ● 32768: BYE-2XX message ● 65536: OPTIONS-2XX message ● 131072: PRACK-2XX message ● 262144: REFER-2XX message ● 524288: UPDATE-2XX message ● 1048576: NOTIFY-2XX message ● 2097152: INFO-2XX message

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 4194304: MESSAGE-2XX message • 8388608: CANCEL-2XX message The default value is 532615, indicating that the Support header field is inserted to the REGISTER, INVITE, SUBSCRIBE, UPDATE, INVITE-2XX, and UPDATE-2XX messages. **NOTE** When the Support header field is inserted to multiple types of messages, set the value to the sum value of these types of messages. For example, when the Support header field is inserted to the OPTIONS and PRACK messages, set the value to 48 (16+32).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
39	Sets the methods supported by the Support header field in SIP messages.	The value is an integer ranging from 0 to 4294967295. ● 0: No method is supported. ● 1: TAC_100REL method ● 2: TAC_REPLACES method ● 4: TAC_TIMER method ● 8: TAC_PRIVACY method ● 16: TAC_PRECONDITION method ● 32: TAC_HISTINFO method ● 64: TAC_JOIN method ● 128: TAC_ANSWERMODE method ● 256: TAC_DTMFINFO method ● 512: TAC_FROMCHANGE method ● 1024: TAC_INDIALOG method ● 2048: PREF method ● 4096: URI_LIST method ● 8192: TAC_NOREFERSUB method ● 16384: TAS_SUBSCRIPTION method ● 65536: DIV_INFO method ● 131072: DND_INFO method ● 262144: TAC_PATH method

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 524288: OVERLAP method The default value is 1039, indicating that TAC_100REL, TAC_REPLACES, TAC_TIMER, TAC_PRIVACY, and TAC_INDIALOG methods are supported. **NOTE** When the Support header field supports multiple methods, set the value to the sum value of these methods. For example, when the Support header field supports the TAC_HISTINFO and TAC_JOIN methods, set the value to 96 (32+64).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
40	Sets the type of SIP messages sent by SIP AG users where the Accept header field is inserted.	The value is an integer ranging from 0 to 4294967295. ● 0: The Accept header field is inserted to no SIP messages. ● 1: REGISTER message ● 2: INVITE message ● 4: SUBSCRIBE message ● 8: BYE message ● 16: OPTIONS message ● 32: PRACK message ● 64: REFER message ● 128: UPDATE message ● 256: NOTIFY message ● 512: INFO message ● 1024: MESSAGE message ● 2048: REGISTER-2XX message ● 4096: SUBSCRIBE-2XX message ● 8192: INVITE-2XX message ● 16384: BYE-2XX message ● 32768: OPTIONS-2XX message ● 65536: PRACK-2XX message ● 131072: REFER-2XX message ● 262144: UPDATE-2XX message ● 524288: NOTIFY-2XX message ● 1048576: INFO-2XX message ● 2097152: MESSAGE-2XX message

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		The default value is 33007, indicating that the Accept header field is inserted to the REGISTER, INVITE, SUBSCRIBE, BYE, PRACK, REFER, UPDATE, and OPTIONS-2XX messages. **NOTE** When the Accept header field is inserted to multiple types of messages, set the value to the sum value of these types of messages. For example, when the Accept header field is inserted to the OPTIONS and PRACK messages, set the value to 48 (16+32).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
41	Sets the message body supported by the Accept header field in SIP messages.	The value is an integer ranging from 0 to 4294967295. ● 0: No message body is supported. ● 1: SDP message body ● 2: IMAGE message body ● 4: AUDIO message body ● 8: VIDEO message body ● 16: MESSAGE message body ● 32: MULTMIXED message body ● 64: MWI message body ● 128: REGINFO message body ● 256: DIALOG message body ● 512: CONF message body ● 1024: UAPROFILE message body ● 2048: PULSECHARGE message body ● 4096: CHARGEINFO message body ● 8192: PIDF message body ● 16384: WATCH message body ● 8388608: MCIDREQ message body ● 33554432: VNDETSIAOC message body ● 67108864: CUG message body ● 134217728: BODY_MIX message body

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		● 268435456: DTMFINFO message body ● 536870912: BROADSOFT message body ● 1073741824: TCSINFO message body ● 2147483648: TEXT message body The default value is 1, indicating that the SDP message body is supported. **NOTE** When the Accept header field supports multiple types of message bodies, set the value to the sum value of these types of message bodies. For example, the Accept header field supports the MULTMIXED and MWI message bodies, set the value to 96 (32+64).
42	Sets the encoding/decoding mode supported by the Accept header field in SIP messages.	The value ranges from 0 to 255. ● 0: No encoding/decoding mode is supported. ● 1: ACCENC_IDENTITY encoding/decoding ● 2: ACCENC_GZIP encoding/decoding ● 4: ACCENC_COMPRESS encoding/decoding ● 8: ACCENC_TAR encoding/decoding ● 16: ACCENC_DEFLATE encoding/decoding The default value is 1, indicating the ACCENC_IDENTITY encoding/decoding mode.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
43	Sets the language supported by the Accept header field in SIP messages.	The value ranges from 0 to 255. ● 0: No language is supported. ● 1: default language ● 2: English ● 4: Chinese The default value is 2, indicating English.
44-46	- **NOTE** These objects are discarded.	-
47	Sets the content of the C line in the SDP message body.	Enumerated type. The options are as follows: ● 0: session description ● 1: media description ● 2: session description and media description The default value is 0.
48	- **NOTE** This control object is discarded.	-
49	- **NOTE** This control object is discarded.	-
50	Sets the type of CW tones. **NOTE** This control object is read-only.	Enumerated type. The options are as follows: ● 0: DT ● 1: China ● 2: Ihug ● 3: Hungary ● 4: Hungary eliminating GAP The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
51	Sets whether the SIP AG reports the digital map match error to the upper-level device.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
52	Sets whether to report hookflash events to upper-level devices.	Enumerated type. The options are as follows: ● 0: The original and new calls are not reported. ● 1: The new call is reported, but the original call is not reported after being switched to an agent. ● 2: reports the new call and the original call that is switched to an agent. ● 3: reports the new call and end the original call that is switched to an agent by sending BYE messages. The default value is 2.
53	Sets the special process control.	Enumerated type. The options are as follows: ● 0: standard process ● 1: special Ihug process ● 2: special Polish process ● 3: special Hungarian process The default value is 0.
54	- **NOTE** This control object is discarded.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
55	Sets whether to save leave messages to the buffer when the SIP AG has services to process or the SIP AG power consumption is low.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
56	Plays the howler tone after the busy tone times out for SIP AG users. **NOTE** This control object is read-only.	The value is 0.
57	- **NOTE** This control object is discarded.	-
58	Sets whether to initiate registration again when proxy switchover is performed.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
59	Sets whether the SIP AG releases the ongoing call when services are switched between the active and standby proxy servers.	Enumerated type. The options are as follows: ● 0: releases all calls immediately. ● 1: holds all calls. ● 2: If both the two parties support the Session Timer, the call is held; otherwise, the call is released. The default value is 0.
60 and 61	- **NOTE** These control objects are discarded.	-
62	Sets the average round trip time (RTT) T1 of messages between the MSAN and IMS Core.	The value is an integer that ranges from 50 to 5000, in milliseconds. The default value is 500.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
63	Sets the interval for sending OPTIONS messages when the SIP AG is working properly.	The value is an integer that ranges from 1 to 65535. The unit of time is T1. The default value is 10.
64	Sets the interval for sending OPTIONS messages when the SIP AG is faulty.	The value is an integer that ranges from 1 to 100. The unit of time is T1. The default value is 20.
65	Sets the timer for the SIP AG to detect events.	The value is an integer that ranges from 1 to 30. The unit of time is T1. The default value is 3.
66	Sets the fault threshold for the object detected by the SIP AG. When the threshold is reached, the object status changes from Normal to Failed.	The value is an integer that ranges from 1 to 30. The default value is 3.
67	Sets the fault recovery threshold for the object detected by the SIP AG. When the threshold is reached, the object status changes from Failed to Normal.	The value is an integer that ranges from 1 to 60. The default value is 6.
68	- **NOTE** This control object is discarded.	-
69	Sets the priority of the header field from which the calling number is obtained.	Enumerated type. The options are as follows: ● 0: obtains the calling number from the P-Asserted-Identity header field. ● 1: obtains the calling number from the From header field. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
70	Sets whether the SIP AG plays the local ringback tone when an early media negotiation result exists and the SIP AG receives a 180 message that does not contain the P-Early-Media or Alert-Info header field.	Enumerated type. The options are as follows: ● 0: The SIP AG does not play the local ringback tone. ● 1: The SIP AG plays the local ringback tone. The default value is 0.
71	- **NOTE** This control object is discarded.	-
72	Sets whether the SIP AG converts the number sign (#) to %23.	Enumerated type. The options are as follows: ● 0: The number sign (#) is not converted to %23 when User=Phone exists in the SIP message. ● 1: All number signs (#) are converted to %23. ● 2: No number sign (#) is converted to "%23". The default value is 0.
73 to 79	- **NOTE** These control objects are discarded.	-
80	Sets the number regulation mode in which SIP AG calling number or called number is displayed.	Enumerated type. The options are as follows: ● 0: non-number-regulation ● 1: global format ● 2: national format ● 3: local format The default value is 0.
81	- **NOTE** This control object is discarded.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
82	Sets the priority of the green call service and the hookflash service.	Enumerated type. The options are as follows: ● 0: The hookflash service is preferred. ● 1: The green call service is preferred. The default value is 0.
83 and 84	- **NOTE** This control object is discarded.	-
85	Indicates whether the 3.1 KHz voice bearing capability can be converted into speech.	Enumerated type. The options are as follows: ● 0: No ● 1: Yes The default value is 1.
86	Sets the maximum CW counts of BRA users.	The value is an integer that ranges from 1 to 16. The default value is 3.
87	Sets the occupation mode of the B channel for ISDN users.	Enumerated type. The options are as follows: ● 0: PREFER ● 1: EXCLUSIVE The default value is 1.
88	Sets the DSS1-side T301 timer of the ISDN users.	The value is an integer that ranges from 180 to 65535, in seconds. The default value is 180.
89	Sets the DSS1-side T302 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 10.
90	Sets the DSS1-side T303 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.
91	Sets the DSS1-side T304 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 20.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
92	Sets the DSS1-side T305 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
93	Sets the DSS1-side T306 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
94	Sets the DSS1-side T307 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 180.
95	Sets the DSS1-side T308 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.
96	Sets the DSS1-side T309 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 90.
97	Sets the DSS1-side T310 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
98	Sets the DSS1-side T312 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 6.
99	Sets the DSS1-side T314 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.
100	Sets the DSS1-side T316 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 120.
101	Sets the DSS1-side T317 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 100.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
102	Sets the DSS1-side T320 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
103	Sets the DSS1-side T321 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
104	Sets the DSS1-side T322 timer of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 4.
105	Sets the DSS1-side UUS3 timer 1 of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 10.
106	Sets the DSS1-side UUS3 timer 2 of the ISDN users.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 10.
107	Sets the UUS3 flow control X parameter of DSS1-side for ISDN users.	The value is an integer that ranges from 0 to 65535. The default value is 16.
108	Sets the UUS3 flow control Y parameter of DSS1-side for ISDN users.	The value is an integer that ranges from 0 to 65535. The default value is 8.
109	Sets the number of information fields in the UUS2 service message of DSS1-side for ISDN users.	The value is an integer that ranges from 0 to 65535. The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
110	Sets the 18X messages returned by PSTN users in the CW service.	Enumerated type. The options are as follows: ● 0: returns a 182 message and then a 180 message. ● 1: returns a 183 message and then a 180 message. ● 2: returns only a 180 message. ● 3: returns only a 182 message. ● 4: returns only a 183 message. The default value is 0.
111	Specifies the header field in the 18X messages sent by the SIP AG in the CW service.	Enumerated type. The options are as follows: ● 0: P-Service-Notification ● 1: P-Notification ● 2: P-Alert-Info The default value is 1.
112	Sets the format of the register from header field in the SIP messages sent by the SIP AG.	Enumerated type. The options are as follows: ● 1: S/S/P format ● 2: SIP format of the phone number ● 3: TEL format of the phone number The default value is 2.
113	Sets the format of the register contact header field in the SIP messages sent by the SIP AG.	Enumerated type. The options are as follows: ● 1: S/S/P ● 2: SIP format of the phone number ● 3: plus sign (+) followed by the phone number The default value is 2.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
114	Sets the format of the RequestURI/From/To fields in the subscribe message sent by the SIP AG.	Enumerated type. The options are as follows: ● 1: public ID in the SIP format ● 2: public ID in the TEL format ● 3: temporary public ID The default value is 1.
115	Sets the format of Contact in the subscribe messages sent by the SIP AG.	Enumerated type. The options are as follows: ● 1: S/S/P format ● 2: SIP format of the phone number ● 3: plus sign (+) followed by the phone number The default value is 2.
116	Sets the format of P-Preferred in the SIP messages sent by the SIP AG.	Enumerated type. The options are as follows: ● 1: public ID in the SIP format ● 2: public ID in the TEL format ● 3: temporary public ID The default value is 1.
117	Sets the mode in which the SIP AG plays announcements.	Enumerated type. The options are as follows: ● 0: Q850 reason code ● 1: status code The default value is 0.
118	Sets whether the SIP AG plays announcement based on the status code and Q850 reason code in the WAITHOOK subprocess.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
119	Sets whether PSTN users support the IBMTEST call scenario (in which NDUB is not used and users determine the busy state).	Enumerated type. The options are as follows: ● 0: not supported ● 1: supported The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
120	Sets the SIP AG service triggering mode.	Enumerated type. The options are as follows: ● 0: loosely coupled mode ● 1: semi-tight coupling in inband mode ● 2: semi-tight coupling in outband mode ● 3: all-tight coupling mode (Info reporting) The default value is 0.
121	Sets whether to release the fork control block and send a Bye message after the SIP AG user sends an INVITE message and receives a 200 OK message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
122	Sets the receiving policy of the SIP AG fork early media.	Enumerated type. The options are as follows: ● 0: receives the first. ● 1: receives the latest. ● 2: process the latest 18X messages. The default value is 2.
123	Sets whether the SDP-Answer field value in a received 18X message can be overwritten by the SDP-Answer field value in next received 18X message.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.
124	Sets whether the SDP-Answer field value in a received 200 message can be overwritten by the SDP-Answer field value in next received 200 message.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
125	Sets whether to release the call of a SIP AG user after the user receives a 408 message.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.
126	Sets the 18X message (local early media is not used and ringback tone is played) processing policy for SIP AG users when the implicit early media indication is used (that is, the P-Early and CompositionType header fields are not used).	Enumerated type. The options are as follows: ● 0: does not stop the local ringback tone. ● 1: stops the local ringback tone. The default value is 0.
127	Sets whether the 200 message contains the SDP-Answer field when the early media is applied and the SIP AG user is the called party.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
128	Sets whether the subsequent 18X message contains the SDP-Answer field when the early media is applied and the SIP AG user is the called party.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
129	Sets whether SIP AG users actively send the P-EARLY-MEDIA:SUPPORT application.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.
130	Sets whether SIP AG users enable in-conversation authentication.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
131	Sets whether to add the authentication information unit to the first in-dialog and out-dialog requests (including only the OPTIONS and REGISTER requests) sent by SIP AG users.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.
132	Sets whether SIP AG processes CNG signals.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.
133	Sets the format of the Invite From header field in the SIP messages sent by the SIP AG.	Enumerated type. The options are as follows: ● 1: SIP: SIP PublicID ● 2: Tel: Tel PublicID ● 3: Private The default value is 1.
134	Sets the **user=** parameter in the RequestURI and To URI fields in INVITE messages sent by the SIP AG users when the number regulation is disabled or the number regulation is enabled but not the global format.	Enumerated type. The options are as follows: ● 0: The RequestURI and To URI fields do not contain the **user=** parameter. ● 1: The parameter format is user=phone. ● 2: The parameter format is user=dialstring. ● 3: The parameter format is user=IP. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
135	Sets the **user=** parameter in the RequestURI and To URI fields in INVITE messages sent by the SIP AG users when the number regulation is enabled and the global format is used.	Enumerated type. The options are as follows: ● 0: The RequestURI and To URI fields do not contain the **user=** parameter. ● 1: The parameter format is user=phone. ● 2: The parameter format is user=dialstring. ● 3: The parameter format is user=IP. The default value is 0.
136	Sets the **user=** parameter in the To URI field in INFO messages when the SIP AG user dials a number during overlap sending, phone ringing, or call connection.	Enumerated type. The options are as follows: ● 0: The parameter format is user=phone. ● 1: The To URI field does not contain the **user=** parameter. ● 2: The parameter format is user=dialstring. ● 3: The parameter format is user=IP. The default value is 0.
137	Sets whether to convert the international prefix to the plus sign (+) for the international URI during SIP AG number regulation.	Enumerated type. The options are as follows: ● 1: yes ● 2: no The default value is 1.
138	Sets whether to enable SIP AG number regulation.	Enumerated type. The options are as follows: ● 0: yes ● 1: no The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
139	Sets the preference mode of multiple M lines when SIP AG users update the INVITE messages.	Enumerated type. The options are as follows: ● 0: The audio service is preferred. ● 1: The image service is preferred. ● 2: First comes, first served. The default value is 0.
140	Sets the **user=** parameter in the From and Prefer URI fields in INVITE messages sent by the SIP AG users when the number regulation is enabled and the global format is used.	Enumerated type. The options are as follows: ● 0: The parameter is not contained. ● 1: The parameter format is user = phone. ● 2: The parameter format is user=dialstring. ● 3: The parameter format is user=IP. (Currently, user=IP is not supported.) The default value is 0.
141	Sets the calling number mapping mode during SIP AG number regulation.	Enumerated type. The options are as follows: ● 1: a string of characters ● 2: CC+NDC mode The default value is 1.
142	Sets whether the SIP AG deletes the end "#" during common or emergent digital map matching.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
143	Sets whether to enable messages to be sent in serial mode for SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
144	Sets all-tight coupling hookflash reporting mode	Enumerated type. The options are as follows: ● 0: APP/Broadsoft ● 1: XML/TCS-info ● 2: SSCC The default value is 0.
145	Sets the A line of packing duration in the SDP message body of SIP messages sent by the SIP AG.	Enumerated type. The options are as follows: ● 0: maxmptime ● 1: ptime The default value is 1.
146	Sets whether the protocol stack sends a CANCEL message when SIP AG users release the call while ringing. By default, the protocol stack sends a BYE message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
147	- **NOTE** This control object is discarded.	-
148	Sets whether SIP AG users need to send the outgoing prefix.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
149	- **NOTE** This control object is discarded.	-
150	Sets the CC status machine timer for the SIP AG to release a call.	The value is an integer that ranges from 1000 to 50000, in milliseconds. The default value is 36000.
151	Sets the CC status machine timer for RTP statistics reporting to the SIP AG.	The value is an integer that ranges from 50 to 5000, in milliseconds. The default value is 500.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
152	Sets the authentication user name format of a single SIP AG user.	Enumerated type. The options are as follows: ● 0: Userinfo ● 1: Userinfo@domain ● 2: user-defined format The default value is 0.
153	- **NOTE** This control object is discarded.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
154	Sets the type of messages sent by SIP AG users where the Allow_Event header field is inserted.	The value is an integer ranging from 0 to 4294967295. ● 0: The Allow_Event header field is inserted to no SIP messages. ● 1: REGISTER message ● 2: INVITE message ● 4: SUBSCRIBE message ● 8: BYE message ● 16: OPTIONS message ● 32: PRACK message ● 64: REFER message ● 128: UPDATE message ● 256: NOTIFY message ● 512: INFO message ● 1024: MESSAGE message ● 2048: CANCEL message ● 4096: REGISTER-2XX message ● 8192: INVITE-2XX message ● 16384: SUBSCRIBE-2XX message ● 32768: BYE-2XX message ● 65536: OPTIONS-2XX message ● 131072: PRACK-2XX message ● 262144: REFER-2XX message ● 524288: UPDATE-2XX message ● 1048576: NOTIFY-2XX message

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• 2097152: INFO-2XX message • 4194304: MESSAGE-2XX message • 8388608: CANCEL-2XX message The default value is 8194, indicating that the Allow_Event header field is inserted to the INVITE and INVITE-2XX messages. **NOTE** When the Allow_Event header field is inserted to multiple types of messages, set the value to the sum value of these types of messages. For example, when the Allow_Event header field is inserted to the OPTIONS and PRACK messages, set the value to 48 (16+32).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
155	Sets the events inserted to the Allow_Event header field in messages sent by the SIP AG users.	The value is an integer ranging from 0 to 4294967295. ● 0: No event is inserted to the Allow_Event header field. ● 2: REFER event ● 4: PRESENCE event ● 8: WINFO event ● 16: MESSAGE_SUMMARY event ● 32: REG event ● 32768: PROFILE event ● 65536: CONFERENCESTATE event ● 131072: DIALOGSTATE event ● 262144: DIVINFO event ● 524288: DNDINFO event The default value is 0, indicating that no event is inserted to the Allow_Event header field. **NOTE** When multiple events are inserted to the Allow_Event header field, set the value to the sum value of these event values. For example, when the REFER and WINFO events are inserted to the Allow_Event header field, set the value to 10 (2+8).
156	Sets whether SIP AG users start the TI-CLIR special process.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
157	Sets the percentage for calculating the SIP AG user update timer. The calculation formula is as follows: Refresh = Expires - Expires x (Configured value)%	The value is an integer that ranges from 0 to 50. The default value is 50.
158	Sets whether to delete the last # when the SCC digital map matching succeeds.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
159	Sets whether to add a plus sign (+) in front of the register from header field (not in S/S/P format) in SIP messages sent by the SIP AG users.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
160	Specifies whether to add user = phone to the register from header field in the SIP message sent from the SIP AG when the register from header field is not in the slotid/subcard/portid format.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
161	Sets the maximum retransmission count of Invite messages after the SIP AG user receives a 301 or 302 message.	The value is an integer that ranges from 0 to 16. The default value is 1.
162	Sets the URL format in the contact header field in 302 messages of the CFX service.	Enumerated type. The options are as follows: ● 0: TEL format ● 1: SIP+proxy format ● 2: SIP+home format The default value is 1.
163	Sets the delay in initiating subscription by SIP AG users.	The value is an integer that ranges from 0 to 60, in seconds. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
164	Sets the delay in processing modem events for SIP AG users.	The value is an integer that ranges from 0 to 10000, in milliseconds. The default value is 0.
165	Sets the playing mode of the remote ringback tone for SIP AG users in the CW service.	Enumerated type. The options are as follows: ● 0: No remote ringback tone is sent. ● 1: IETF mode (not supported) ● 2: TISPAN mode ● 3: common mode The default value is 0.
166	Sets the channel switching mode when the SIP AG ends the CW early media.	Enumerated type. The options are as follows: ● 0: A 200 response message replaces the negotiation parameters. ● 1: A Re-INVITE message is sent for renegotiation. The default value is 1.
167	Sets the encoding/decoding policy when the SIP AG users automatically switch data services.	Enumerated type. The options are as follows: ● 0: The audio encoding/decoding is preferred. ● 1: The locally configured VBD encoding/decoding is used. The default value is 0.
168	Sets the signal tone mapping mode for SIP AG users when the response message contains the Reason header field.	Enumerated type. The options are as follows: ● 0: The status code is preferred. ● 1: The Reason header field is preferred. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
169	Indicates whether the SDP protocol stack supports the extended RFC3605 for RTCP information transmission.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
170	Sets the NAT binding entry update mode for media IP addresses when the SIP AG supports the Simple Traversal of UDP through NAT (STUN) function.	Enumerated type. The options are as follows: ● 0: using RTP flows ● 1: using STUN packets The default value is 0.
171	Sets the NAT binding entry update mode for signaling IP addresses when the SIP AG supports the STUN function.	Enumerated type. The options are as follows: ● 0: using OPTIONS messages ● 1: using STUN packets The default value is 0.
172	Sets the protection timer for calling party and called party control.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 180.
173	Sets the DNS update interval for SIP AG users.	The value is an integer that ranges from 0 to 65535, in seconds. If interval is set to 0, the DNS update is not performed. The default value is 90.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
174	Sets the **user=** parameter in the RequestURI and To URI fields in INVITE messages when the SIP AG users use the SCC service.	Enumerated type. The options are as follows: ● 0: The RequestURI and To URI fields do not contain the **user=** parameter. ● 1: The parameter format is user=phone. ● 2: The parameter format is user=dialstring. ● 3: The parameter format is user=IP. The default value is 0.
175	Sets the **phone-context** parameter when user=dialstring is set and number regulation is disabled.	Enumerated type. The options are as follows: ● 0: The **phone-context** parameter is not set. ● 1: The **phone-context** parameter is set to a domain. The default value is 0.
176	Sets whether to allow the SIP AG to send the private XML of the SIP ISDN.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
177	Sets the T310 timer for SIP AG users in OVERLAP state.	The value is an integer that ranges from 1 to 4294967294, in seconds. The default value is 30.
178	- **NOTE** This control object is discarded.	-
179	Sets whether the matched ongoing prefix needs to be matched during digital map matching.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
180	Selects the format of the calling number and called number from multiple URIs in the P-Asserted-Identity header field.	Enumerated type. The options are as follows: ● 0: SIP or SIPS format ● 1: TEL format The default value is 0.
181	Sets the format of host information in the CONTACT and VIA header fields for SIP AG users.	Enumerated type. The options are as follows: ● 0: IP ● 1: IP+port ● 2: domain ● 3: domain+port The default value is 1.
182	Sets whether to send a Cancel message after the SIP AG user sends a REINVITE message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
183	Sets whether the SIP AG plays the local ringback tone when the 180 message contains the SDP message body but not the early media indication.	Enumerated type. The options are as follows: ● 0: The SIP AG does not play the local ringback tone. ● 1: The SIP AG plays the local ringback tone. The default value is 0.
184	Sets whether the Route header field contains port information. Whether the Router header field contains the IP address and domain is determined by the command line.	Enumerated type. The options are as follows: ● 0: The Route header field does not contain port information. ● 1: The Route header field contains port information. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
185	Sets the returned error code when the SIP AG that does not support Refer messages receives Refer messages.	Enumerated type. The options are as follows: ● 0: returns the 403 error code. ● 1: returns the 405 error code. ● 2: returns the 501 error code. The default value is 1.
186	Sets the format of Contact in the Invite SIP messages sent by the SIP AG.	Enumerated type. The options are as follows: ● 1: S/S/P format ● 2: SIP format of the phone number ● 3: plus sign (+) followed by the phone number The default value is 2.
187	Sets the maximum value of the timer for preventing a large of concurrent registration counts.	The value is an integer that ranges from 1000 to 4294967294, in milliseconds. The default value is 70000.
188	Sets the conference service establishment mode for SIP AG users.	Enumerated type. The options are as follows: ● 0: URI List mode ● 1: Refer mode The default value is 1 in common process and 0 in DT process.
189	Sets whether to support IMS playing error tones.	Enumerated type. The options are as follows: ● 0: not supported ● 1: supported The default value is 0.
190	Sets the response code when the SIP AG user in CW state rejects a third-party call.	Enumerated type. The options are as follows: ● 0: response code 486 ● 1: response code 603 The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
191	Sets the response code when the call of the SIP AG user in CW state is released.	Enumerated type. The options are as follows: ● 0: response code 486 ● 1: response code 480 The default value is 0.
192	Sets the port base value for SIP AG users.	The value is an integer that ranges from 0 to 255. The default value is 30.
193	Sets the timer for the SIP AG detects the proxy server status.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 30.
194	Sets the timer for the standby proxy server to switch back to the active proxy server.	The value is an integer that ranges from 0 to 65535, in seconds. The default value is 21600.
195	Sets the URI format of chassis, slot, and port numbers.	Enumerated type. The options are as follows: ● 0: channel/port/slot/shelf/rack/AN_ID@<Domain> ● 1: port/slot/shelf/rack/AN_ID@<Domain>. When the length of AN_ID is 0, the format is port/slot/shelf/rack@<Domain>. ● 2: port/slot/shelf/rack/AN_ID@<Domain>. When the length of AN_ID is 0, the format is port/slot/shelf/rack/@<Domain>. The default value is 0.
196	Sets the slot base value for SIP AG users.	The value is an integer that ranges from 0 to 255. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
197	Sets the subcard base value for SIP AG users.	The value is an integer that ranges from 0 to 255. The default value is 0.
198	Sets where the phone number that the SIP AG user dials during overlap sending or call connection to the To header field.	Enumerated type. The options are as follows: ● 0: The To header field contains the phone number. ● 1: The x-session-info message body contains the phone number. The default value is 0.
199	Sets whether the SIP AG users support the voice band data (VBD) multi-mode.	Enumerated type. The options are as follows: ● 0: not supported ● 1: supported The default value is 0.
200	Plays the common dialing tone when the SIP AG user presses the hookflash. **NOTE** This control object is read-only.	The value is 1.
201	Plays the busy tone when the SIP AG receives a Bye message from the IMS. **NOTE** This control object is read-only.	The value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
202	Sets whether pressing 1 means hookflash when the phone is in pulse dialing mode and in non-digit-collecting mode.	Enumerated type. The options are as follows: ● 0: Pressing 1 does not mean hookflash. ● 1: advanced mode. The old-fashioned phones are not supported. ● 2: basic mode. The old-fashioned phones are supported. The default value is 0.
203	Sets whether the SIP AG supports the init parameter in the initial registration messages and registration message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
204	Sets the response error code when user registration fails.	The value is an integer that ranges from 0 to 65535. The default value is 480.
205	Sets the response error code when the SIP AG port is locked.	The value is an integer that ranges from 0 to 65535. The default value is 486.
206	Sets the response error code when the SIP AG port is being tested.	The value is an integer that ranges from 0 to 65535. The default value is 486.
207	Sets whether the SIP AG switches to the proxy when 4xx (excluding the 401 Unauthorized, 407, and 423 Interval Too Brief messages), 5xx, and 6xx messages are received during registration.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
208	Sets the duration that the SIP AG initiates resubscription requests for users. For example, the SIP AG resubscribes the voice message service for users.	The value is an integer that ranges from 0 to 600, in seconds. The default value is 30. **NOTE** The value 0 indicates that the SIP AG initiates resubscription requests for users immediately.
209	- **NOTE** This control object is discarded.	-
210	Sets whether the userinfo value is processed as the phone number (filtering out the visible separators) when the PublicID field contains SIP URI but not user=phone and userinfo is in TEL format This function applies to the scenarios that the SIP AG locates the called party for the incoming call, matches the calling number for outgoing calls of ISDN/R2 users, and reads the user account in the HASH table.	Enumerated type. The options are as follows: ● 0: The original userinfo is extracted and not processed as the phone number. ● 1: Visible separators such as + - ( ) , and . in the original userinfo are filtered out. Only the digits are extracted. The default value is 0.
211	Sets the method in which the SIP AG obtains the alert ID of the AlertInfo field.	Enumerated type. The options are as follows: ● 0: obtains the alert ID from GenericPara. ● 1: obtains the alert ID from the URI. The default value is 0.
212	Sets whether the connection can be bound to the proxy remote IP address, remote port number, local IP address, and local port number.	Enumerated type. The options are as follows: ● 0: not supported ● 1: supported The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
213	Sets whether to control the format defined by the time division multiplexing (TDM) private branch exchange (PBX) when the Calling Line Identification Presentation (CLIP) is configured.	Enumerated type. The options are as follows: ● 0: not controlled ● 1: controlled The default value is 0.
214	Sets whether to clear the calling number, called number, and name when the messages of incoming and outgoing calls do not contain the calling number and called number.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
215	Sets whether to display the name when the CLIP is configured.	Enumerated type. The options are as follows: ● 0: displays the name. ● 1: does not display the name. The default value is 0.
216	Enables the SIP AG to select the SIP format or TEL format of a configured hotline phone number.	Enumerated type. The options are as follows: ● 0: SIP format ● 1: TEL format The default value is 0.
217	Sets whether the SIP AG supports the CPC parameter.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
218	Sets whether the SIP AG supports single digital map.	Enumerated type. The options are as follows: ● 0: not supported ● 1: supported The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
219	Sets whether the SIP AG sends EOC signals to the SIP AG user's phone when the other party hangs up.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
220	Sets whether the SIP AG sends DisconnectClear signals to terminals when the SIP AG receives the event that the SIP AG user or remote user releases the call.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
221	Sets the Ta3 timer for SIP AG overlap sending.	The value is an integer that ranges from 0 to 4294967294, in seconds. The default value is 15. **NOTE** The value 0 indicates that the timer is not started.
222	Sets the update duration that the SIP AG uses.	Enumerated type. The options are as follows: ● 0: The (static) update duration configured in a control object is used. ● 1: The (dynamic) update duration returned by the DNS server is used. The default value is 0.
223	Sets whether the P-Preferred-Identity header field contains the CentrexNo field for SIP AG outgoing calls.	Enumerated type. The options are as follows: ● 0: The P-Preferred-Identity header field does not contain the CentrexNo field. ● 1: The P-Preferred-Identity header field contains the CentrexNo field. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
224	Sets whether pressing the hookflash and then dialing 5 trigger the CCBS process when users in successive state.	Enumerated type. The options are as follows: ● 0: Pressing the hookflash and then dialing 5 do not trigger the CCBS process. ● 1: Pressing the hookflash and then dialing 5 trigger the CCBS process. The default value is 0.
225	Sets the timer for dialing the initial number during SIP AG overlap sending.	The value is an integer that ranges from 0 to 4294967294, in seconds. The default value is 20. **NOTE** The value 0 indicates that the timer is not started.
226	Sets the timer for dialing the next number during SIP AG overlap sending.	The value is an integer that ranges from 0 to 4294967294, in seconds. The default value is 20. **NOTE** The value 0 indicates that the timer is not started.
227	Sets the Ta1 timer for SIP AG overlap sending.	The value is an integer that ranges from 0 to 4294967294, in seconds. The default value is 4. **NOTE** The value 0 indicates that the timer is not started.
228	Sets the QOP authentication mode.	Enumerated type. The options are as follows: ● 0: Auth ● 1: Auth-int The default value is 0.
229	Sets whether to trigger the Refer success event when a 2xx message is returned for a Refer message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
230	Sets the SIP AG to use the proxy sub-domain name or main domain name.	Enumerated type. The options are as follows: ● 0: uses the proxy main domain name. ● 1: uses the proxy sub-domain name. The default value is 0.
231	Sets the information carried in the Accept header field.	The mappings between the values and information carried in the Accept header field are as follows: ● 0: No information is carried in the Accept header field. ● 1: SSCC ● 2: DIV ● 4: DND ● 8: MCID ● 16: ETSI_SIMSERVS ● 32: SIMSERV ● 64: PSTN The default value is 0, indicating that the Accept header field contains no information. **NOTE** When the Accept header field contains multiple types of information, set the value to the sum value of these types of information. For example, when the Accept header field contains SSCC and MCID, set the value to 9 (1+8).
232	Sets the realm parameter in the authentication message.	Enumerated type. The options are as follows: ● 0: uses the realm value in the IMS response message. ● 1: uses the home domain configured on the interface. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
233	Sets whether the SIP AG supports multiple enterprises.	Enumerated type. The options are as follows: ● 0: not supported ● 1: supported The default value is 1.
234	Sets the Reinvite media direction for the user who is holding a call. Sets the stream mode for the user who is holding a call. In ONT mode, the stream mode is inactive when the user is holding a call and becomes sendrecv when the call is resumed.	Enumerated type. The options are as follows: ● 0: sendonly ● 1: ONT mode The default value is 0.
235	Sets the sending mode of the annexa/annexb parameter when the SIP AG uses G.723/G.729.	Enumerated type. The options are as follows: ● 0: The annexa or annexb parameter is not sent. Whether the G.723/G.729 voice activity detection (VAD) function is enabled depends on the local setting. ● 1: The annexa or annexb parameter is sent. Whether the G.723/G.729 VAD function is enabled depends on the SDP message from the peer. ● 2: The annexa or annexb parameter is sent. Whether the G.723/G.729 VAD function is enabled depends on the local setting. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
236	Sets the mode in which the SIP AG adds a type of media stream.	Enumerated type. The options are as follows: ● 0: modifies the parameter of the original media stream. ● 1: adds parameters to the M line in the SDP message. The default value is 0.
237	Sets whether to activate the connection when the SIP AG is sending data. **NOTE** This control object is read-only.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
238	Sets the SIP AG session timer.	The value is an integer that ranges from 90 to 65535, in seconds. The default value is 1800.
239	Sets the method to identify the called party.	Enumerated type. The options are as follows: ● 0: uses userinfo (only user domain information is identified). ● 1: uses URI (the entire URI is matched to identify the user). The default value is 0.
240	Sets whether to release the ongoing call when the SIP AG receives a new call during a SIP call for the emergency standalone service.	Enumerated type. The options are as follows: ● 0: The ongoing call is not released. ● 1: The ongoing call is released. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
241	Sets the special dialing tone as the dial tone type when the message waiting indicator (MWI) service is configured. **NOTE** This control object is read-only.	The value is 0.
242	Sets the heartbeat interval of the active DSS1 on a SIP AG.	The value is an integer that ranges from 0 to 65534, in seconds. The default value is 1200. **NOTE** The value 0 indicates that the heartbeat detection is not performed.
243	Specifies the rule for filling in the Contact header field.	Enumerated type. The options are as follows: ● 0: The Contact header field of each user is generated independently. ● 1: The format of the Contact header field is the same as that of the major user. ● 2: The Contact header field is in SIP URI format without userinfo. The default value is 1.
244	Specifies the mode used by a SIP AG to update sessions.	Enumerated type. The options are as follows: ● 0: not defined ● 1: UAC ● 2: UAS The default value is 0.
245	Specifies the default mode to control tunes during call waiting. **NOTE** This control object is read-only.	The value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
246	Sets the maximum SIP AG re-registration counts.	The value is an integer that ranges from 1 to 65535. The default value is 6.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
247	Specifies the algorithm for SIP AG re-registrations.	Enumerated type. The options are as follows: ● 0: indicates that the algorithm is the re-registration counts multiply the interval. If the re-registration counts exceed the maximum counts, re-registration is initiated at the maximum interval. ● 1: indicates that the algorithm is $2^{(\text{number of re-registrations} - 1) * \text{interval}}$. If the re-registration counts exceed the maximum number, re-registration is initiated at the maximum interval. ● 2: indicates that the algorithm $2^{((\text{number of re-registrations} - 1) \% (\text{maximum number of re-registrations}))* \text{interval}}$. If the re-registration counts exceed the maximum number, re-registration is initiated at the maximum interval. ● 3: indicates the NICC algorithm. If the SIP AG consecutively receives error codes in the first registration, the interval is 5 minutes. If the SIP AG consecutively receives error codes in updating registration, the interval is 30 minutes. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
248	Indicates that a busy tone is played if the user does not dial numbers after offhook. **NOTE** This control object is read-only.	The value is 0.
249	Specifies the delivery mode for the SIP AG MWI.	Enumerated type. The options are as follows: ● 0: Only information about MWI is delivered. ● 1: Information is delivered based on ETSI. The default value is 1.
250	-	- **NOTE** This control object is reserved.
251	Specifies the value of the protection timer when services are switched due to the changes in the payload of the media stream to prevent repeated switching between data services and voice services.	The value is an integer that ranges from 0 to 65534, in milliseconds. The default value is 1000.
252	Indicates whether to switch back to voice services after the SIP AG finishes transparent data transmission.	Enumerated type. The options are as follows: ● 0: actively switches back to voice services. ● 1: inactively switches back to voice services. The default value is 0.
253	Specifies the matching number of symbols in the digital map.	Enumerated type. The options are as follows: ● 0: 0 to multiple times ● 1: 1 to multiple times The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
254	Sets whether the SIP AG stops playing the early media and starts to play the local ringback tone when receiving a SIP 180 message if the SIP AG has received a SIP 183 message with an SDP field before.	Enumerated type. The options are as follows: ● 0: The SIP AG continues playing the early media. ● 1: The SIP AG stops playing the early media and starts to play the local ring back tone. The default value is 0.
255	Specifies temporary response policy used when the PBX is the called party.	Enumerated type. The options are as follows: ● 0: The ring back tone SDP information is contained in SIP 180 messages. ● 1: The ring back tone SDP information is contained in SIP 183 messages. ● 2: The PBX sends a SIP 180 message after a SIP 183 message. The default value is 0.
256	Specifies the SDP field value in a message that the PBX sends to trigger a hookflash action.	Enumerated type. The options are as follows: ● 0: SendOnly ● 1: SendRecv ● 2: Inactive The default value is 1.
257	Indicates whether to re-establish a connection if the destination address or port and the remote address or port are different when the SIP interface receives an INVITE message in TCP mode.	Enumerated type. The options are as follows: ● 0: No socket is re-established. ● 1: A socket is re-established. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
258	Specifies the header field in the signal behavior when the SIP UE or SIP trunk connected to an IP PBX sends an INVITE request and call forwarding occurs.	Enumerated type. The options are as follows: ● 0: History-Info ● 1: Diversion The default value is 0.
259	Indicates whether to use INFO signals to send numbers during a call connection.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
260	- **NOTE** This control object is discarded.	-
261	Specifies users who can switch the proxy server.	Enumerated type. The options are as follows: ● 0: all the users belonging to the proxy server. ● 1: an individual user. The default value is 0.
262	Specifies the recovery mode after the primary proxy server fails when dual-homing and automatic switchover are enabled in Register mode.	Enumerated type. The options are as follows: ● 0: Services are recovered after the revertive switching timer times out. ● 1: Register message detection. The default value is 0.
263	Specifies the number of incorrect responses received by the register that is considered as a proxy fault.	The value is an integer that ranges from 1 to 5. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
264	Specifies how to use the call hold and dual-communications.	Enumerated type. The options are as follows: ● 0: The call hold and dual-communications are used together. ● 1: The call hold and dual-communications are used independently. The default value is 0.
265	- **NOTE** This control object is discarded.	-
266	- **NOTE** This control object is discarded.	-
267	- **NOTE** This control object is discarded.	-
268	- **NOTE** This control object is discarded.	-
269	Reserved	-
270	Indicates whether the SIP AG detects the registration timeout period returned from the network side.	Enumerated type. The options are as follows: ● 0: Always use the Expire message returned from the network side as the registration timeout period. ● 1: Check the registration timeout period returned from the network side. If the value is larger than the default value, the locally configured value takes effect. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
271	Indicates whether to carry the authentication header field in the Register message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
272	Indicates whether to authenticate the 200 response message.	Enumerated type. The options are as follows: ● 0: The 200 response message is not authenticated regardless the authentication header field is contained. ● 1: The 200 response message is authenticated no matter whether the authentication header field is contained. ● 2: The 200 response message is authenticated when the authentication header field is contained and is not authenticated when the authentication header field is contained. The default value is 0.
273	Indicates how to display **name** when **userinfo** of the called and calling numbers is invalid.	Enumerated type. The options are as follows: ● 0: **name** is displayed as "O". ● 1: **name** is displayed if **display name** exists and is not displayed if **display name** does not exist. ● 2: **name** is not displayed regardless **display name** exists. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
274	Indicates how to display **name** when **userinfo** of the called and calling numbers is displayed with restrictions.	Enumerated type. The options are as follows: ● 0: **name** is displayed as "P". ● 1: **name** is displayed if **display name** exists and is not displayed if **display name** does not exist. ● 2: **name** is not displayed regardless **display name** exists. The default value is 0.
275	Indicates whether the IP address on the C line in the SDP message can be changed to 0.0.0.0 by the Re-Invite message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
276	Indicates whether the Contact header field contains **expires** when the user logs out.	Enumerated type. The options are as follows: ● 0: The Contact header field does not contain **expires**. ● 1: The Contact header field contains **expires**. The default value is 0.
277	Indicates whether the reliable provisional response is needed.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.
278	Indicates whether to release calls if Prack messages do not contain SDP in 18x/Prack negotiation.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
279	Indicates the default value of service authority.	The options are as follows: ● 1: CONF ● 2: 3PTY ● 4: ECT ● 8: MCID ● 16: DC ● 32: CW ● 64: HOTLINE ● 128: MWI ● 256: HOLD ● 512: TP ● 1024: CD ● 2048: UUS1 ● 4096: UUS2 ● 8192: UUS3 ● 16384: AUTOREVERSEPOLARITY ● 32768: ANONYMOUS_CALL ● 65536: PERMANENT_HOLD ● 131072: CUTOFF_DISSCONNECT ● 262144: SCC_CLASS ● 524288: FAST_DISCONNECT The default value is 0, indicating that no authority is specified on any services. **NOTE** If you need to configure service authorities, the value must be accumulated. For example, if you need to configure authorities of CONF, DC, and CW services, the value is 49 (1+16+32).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
280	Specifies the sending mode of the SIP AG number.	Enumerated type. The options are as follows: ● 0: sends all the numbers. ● 1: In-Dialog mode. ● 2: Multiple INVITE mode. The default value is 1.
281	Indicates whether to release calls and cancel services after the user fails to log in to all the proxy servers.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
282	Specifies the range of service authorities.	The options are as follows: ● 1: CONF ● 2: 3PTY ● 4: ECT ● 8: MCID ● 16: DC ● 32: CW ● 64: HOTLINE ● 128: MWI ● 256: HOLD ● 512: TP ● 1024: CD ● 2048: UUS1 ● 4096: UUS2 ● 8192: UUS3 ● 16384: AUTOREVERSEPOLARITY ● 32768: ANONYMOUS_CALL ● 65536: PERMANENT_HOLD ● 131072: CUTOFF_DISSCONNECT ● 262144: SCC_CLASS ● 524288: FAST_DISCONNECT The default value is 2147434495, indicating authorities on all the services. **NOTE** If you need to configure service authorities, the value must be accumulated. For example, if you need to configure authorities of CONF, DC, and CW services, the value is 49 (1+16+32).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
283	Indicates whether to change the call ID in the Register message when the proxy server is switched.	Enumerated type. The options are as follows: ● 0: change. ● 1: not change. The default value is 0.
284	Indicates whether to change the call ID in the Register message when the life cycle expires.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
285	Indicates whether to change the call ID in the Register message when a 403 message is returned after a non-Register message is sent.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
286	Indicates whether to change the call ID in re-registration when the user logs out due to registration failure on all the proxy servers.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
287	Indicates whether the SIP AG sends the received data of media protocols not supported by the SIP AG.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
288 - 300	Indicates reserved control objects.	-
301	Indicates whether the user deregisters after the user receives a 403 Invite message.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.
302	Indicates whether the Invite event timer is out of service.	Enumerated type. The options are as follows: ● 0: no ● 1: yes The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
303	Sets the value of the Ta4 timers in overlap sending mode.	The value is an integer that ranges from 0 to 4294967294, in milliseconds. The default value is 0.
304	Sets the length of the minimum number in overlap sending mode.	The value is an integer that ranges from 0 to 64. The default value is 1. The value 0 indicates that no limit is set on the length of the minimum number.
305	Sets the value of ptime when ptime is not contained in the SDP Answer message.	Enumerated type. The options are as follows: ● 0: Obtains the negotiated ptime. If no ptime is negotiated, set the value based on the DSP attributes. ● 1: Sets the value based on the DSP attributes. ● 2: Obtains the value corresponding to the codec in the Offer message based on the codec in the Answer message. The default value is 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
306	Sets the value of **ptime** when **ptime** is not contained in the SDP Offer message.	Enumerated type. The options are as follows: ● 0: Obtains the negotiated ptime. If no ptime is negotiated, set the value based on the DSP attributes. ● 1: Sets the value based on the DSP attributes. ● 2: Obtains the value corresponding to the codec based on the codec in the priority list configured on the interface or single user. The default value is 0.
307	Sets the value of **ptime** when **ptime** corresponding to the first code in the Offer message is not empty but the **ptime** is invalid.	Enumerated type. The options are as follows: ● 0: The negotiation fails if the system does not support the DSP codec in the Offer message. ● 1: Sets the value based on the DSP attributes. ● 2: Obtains the value corresponding to the codec based on the codec in the priority list configured on the interface or single user. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
308	Specifies new services supported by the calling service.	The value is an integer that ranges from 0 to 2147483647. The options are as follows: ● 1: SIP_PROFILE_RIGHT_CONF ● 2: SIP_PROFILE_RIGHT_3PTY ● 4: SIP_PROFILE_RIGHT_ECT ● 8: SIP_PROFILE_RIGHT_MCID ● 16: SIP_PROFILE_RIGHT_DC ● 32: SIP_PROFILE_RIGHT_CW ● 64: SIP_PROFILE_RIGHT_HOTLINE ● 128: SIP_PROFILE_RIGHT_MWI ● 256: SIP_PROFILE_RIGHT_HOLD ● 512: SIP_PROFILE_RIGHT_TP ● 1024: SIP_PROFILE_RIGHT_CD ● 2048: SIP_PROFILE_RIGHT_UUS1 ● 4096: SIP_PROFILE_RIGHT_UUS2 ● 8192: SIP_PROFILE_RIGHT_UUS3

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		● 16384: SIP_PROFILE_RIGHT_AUTOREVERSEPOLARITY ● 32768: SIP_PROFILE_ANONYMOUS_CALL ● 65536: SIP_PROFILE_PERMANENT_HOLD ● 131072: SIP_PROFILE_CUTOFF_DISSCONNECT ● 262144: SIP_PROFILE_SCC_CLASS ● 524288: SIP_PROFILE_FAST_DISCONNECT ● 1048576: SIP_PROFILE_CCW The default value is 2147483639, indicating that all the services except the SIP_PROFILE_RIGHT_MCID are supported. **NOTE** If you need to configure the calling service to support multiple services, the value must be accumulated. For example, if you configure the called service to support SIP_PROFILE_RIGHT_CW and SIP_PROFILE_RIGHT_HOTLINE, the value is 96 (32+64).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
309	Specifies new services supported by the called service.	The value is an integer that ranges from 0 to 2147483647. The options are as follows: ● 1: SIP_PROFILE_RIGHT_CONF ● 2: SIP_PROFILE_RIGHT_3PTY ● 4: SIP_PROFILE_RIGHT_ECT ● 8: SIP_PROFILE_RIGHT_MCID ● 16: SIP_PROFILE_RIGHT_DC ● 32: SIP_PROFILE_RIGHT_CW ● 64: SIP_PROFILE_RIGHT_HOTLINE ● 128: SIP_PROFILE_RIGHT_MWI ● 256: SIP_PROFILE_RIGHT_HOLD ● 512: SIP_PROFILE_RIGHT_TP ● 1024: SIP_PROFILE_RIGHT_CD ● 2048: SIP_PROFILE_RIGHT_UUS1 ● 4096: SIP_PROFILE_RIGHT_UUS2 ● 8192: SIP_PROFILE_RIGHT_UUS3

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		● 16384: SIP_PROFILE_RIGHT_AUTOREVERSEPOLARITY ● 32768: SIP_PROFILE_ANONYMOUS_CALL ● 65536: SIP_PROFILE_PERMANENT_HOLD ● 131072: SIP_PROFILE_CUTOFF_DISSCONNECT ● 262144: SIP_PROFILE_SCC_CLASS ● 524288: SIP_PROFILE_FAST_DISCONNECT ● 1073741824: SIP_PROFILE_CCW The default value is 2147483647, indicating that all the services are supported. **NOTE** If you need to configure the called service to support multiple services, the value must be accumulated. For example, if you configure the called service to support SIP_PROFILE_RIGHT_CW and SIP_PROFILE_RIGHT_HOTLINE, the value is 96 (32+64).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
310	Sets the value of **ptime** when **ptime** corresponding to the first code in the Answer message is not empty but the **ptime** is invalid.	Enumerated type. The options are as follows: ● 0: Sets the value based on the DSP attributes. ● 1: Obtains the value corresponding to the codec in the Offer message based on the codec in the Answer message. The default value is 0.
311	Specifies how to release forking on the user side before receiving the INVITE-200 message.	Enumerated type. The options are as follows: ● 1: The SIP AG sends a CANCEL message. ● 2: Each forking sends a BYE message. ● 3: Each forking sends a BYE message. ● 4: Each forking sends a BYE message. **NOTE** The values 3 and 4 are reserved and have the same processing as the value 2. The default value is 2.
312 - 328	Reserved	-
329	Indicates whether to receive packets from the proxy server when the SIP AG sends SIP 3xx messages.	Enumerated value. The options are as follows: ● 0: Packets from the proxy server are not received. ● 1: Packets from the proxy server are received. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
330	Sets a mark for the device that updates the session.	Enumerated value. The options are as follows: ● 0: The mark is not included. ● 1: UAC ● 2: UAS The default value is 0.
331	Configures whether to initiate VBD negotiation when there a delay in processing modem events. **NOTE** This control point takes effect after parameter 164 is used to set the delay in processing modem events for SIP AG users. It is recommended that the delay in processing modem events for SIP AG users be set to 5s.	Enumerated value. The options are as follows: ● 0: VBD negotiation is not initiated. ● 1: VBD negotiation is initiated. The default value is 1.

Example

Set the parameter with the sequence number 18 to 1 for a SIP AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] user-defined-profile number-parameter 18 1
```

Related Topics

16.6.1.15 display voice sipag

16.6.1.91 user-defined-profile service-priority

Function

Using the **user-defined-profile service-priority** command, you can configure the priority of a service type on a SIP AG.

Using the **undo user-defined-profile service-priority** command, you can delete the configured priority of a service type on a SIP AG.

Format

user-defined-profile service-priority *pri-value srvid-value*

undo user-defined-profile service-priority *pri-value*

Parameters

Parameter	Description	Value
pri-value	Specifies a service priority.	The value is an integer that ranges from 1 to 255.
srvid-value	Specifies a service type.	The value is an integer that ranges from 0 to 4294967295.

Views

SIP AG view

Default Level

2: Configuration level

Usage Guidelines

The **user-defined-profile service-priority** command configures the priority of a specified service type.

If you change the priority of a service type, priorities of other service types are also changed. For example, if you change the priority of a service type from 4 to 2, priorities of the service types with priorities 2 and 3 are changed to 3 and 4. If you change the priority of a service type from 4 to 6, priorities of the service types with priorities 5 and 6 are changed to 4 and 5.

This configuration takes effect after the SIP AG interface is reset using the **16.6.1.69 reset (SIP AG view)** command.

Example

Set the priority of service type 12 to 4.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipag 1
[Huawei-voice-sipag-1] user-defined-profile service-priority 4 12
```

Related Topics

16.6.1.15 display voice sipag

16.6.2 SIP AG User Configuration Commands

Function Description

This section describes the commands used to configure SIP AG users.

 Copyright © Huawei Technologies Co., Ltd.

16.6.2.1 active-mask time-slot config-status

Function

The **active-mask time-slot config-status** command specifies the timeslot status.

Format

active-mask time-slot *time-slot-value* **config-status** *config-status-value*

Parameters

Parameter	Description	Value
time-slot-value	Specifies the timeslot number.	The value is an integer that ranges from 0 to 31.
config-status *config-status-value*	Specifies the timeslot status.	Enumerated type. The values are as follows: • **block**: Timeslots are disabled. • **normal**: Timeslots are enabled.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

When the 1E1T1-M/2E1T1-M card is installed on the device and works in e1-voice/t1-voice mode, run the **active-mask time-slot config-status** command to specify the timeslot status.

Example

Set the status of timeslot 1 to **normal**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] active-mask time-slot 1 config-status normal
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.2 agid (SIP AG user view)

Function

Using the **agid** command, you can configure the SIP AG interface ID for a SIP AG user.

By default, no SIP AG interface ID is configured for a SIP AG user.

Format

agid *sipag-interface-id*

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the ID of a SIP AG interface.	The value is an integer that ranges from 0 to 16777215.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **agid** command configures the SIP AG interface ID for a SIP AG user. Only one SIP AG interface ID can be configured for a SIP AG user.

Example

Configure the SIP AG interface ID for a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] agid 1
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.3 auth (SIP service data profile view)

Function

The **auth** command configures an authentication user name and a password in a SIP service data profile.

 Copyright © Huawei Technologies Co., Ltd.

The **undo auth** command deletes the authentication user name and the password from a SIP service data profile.

Format

auth username *auth-username* **password** { **cipher** *cipher-password* | **ha1 cipher** *cipher-password* }

undo auth

Parameters

Parameter	Description	Value
username *auth-username*	Specifies the authentication user name.	The value is a string of 1 to 64 characters without spaces or question marks (?).
password	Specifies the authentication password.	-
cipher *cipher-password*	Indicates the password in cipher text. **NOTE** You can configure *cipher-password* after inputting **cipher** and pressing **Enter**.	The *cipher-password* value is a string of case-sensitive characters without spaces. A cipher password may contain 1 to 64 encrypted characters. The input character string - indicates that the password is empty.
ha1 cipher *cipher-password*	Sets the password format to HA1.	The *cipher-password* value is a string of case-sensitive characters without spaces. A cipher password may contain 1 to 32 encrypted characters. The input character string - indicates that the password is empty.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

To ensure security, configure a user name and a password for authentication.

Before using the **auth** command, run the **16.6.2.39 sipaguser (Voice View)** command to create a SIP AG user.

Example

Set the authentication user name to **huawei**, password format to cipher, and password to 1234567 in SIP service data profile.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] auth username huawei password cipher
 Please input user password(1-64 chars):*******
```

16.6.2.4 auth (user group view)

Function

The **auth** command configures the authentication user name and password for a user group.

The **undo auth** command deletes the authentication user name and password of a user group.

By default, no authentication user name or password is configured for a user group.

Format

auth username *auth-username* **password** { **cipher** *cipher-password* | **ha1 cipher** *cipher-password* }

undo auth

Parameters

Parameter	Description	Value
username *auth-username*	Specifies the authentication user name for a user group.	The value is a string of 1 to 64 characters without question mark and spaces.
password	Specifies the authentication password for a user group.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-password*	Indicates the password in cipher text. **NOTE** You can configure *cipher-password* after inputting **cipher** and pressing **Enter**.	The *cipher-password* value is a string of case-sensitive characters without spaces. A cipher password may contain 1 to 64 encrypted characters. The input character string - indicates that the password is empty.
ha1 cipher *cipher-password*	Sets the password format to HA1.	The *cipher-password* value is a string of case-sensitive characters without spaces. A cipher password may contain 1 to 32 encrypted characters. The input character string - indicates that the password is empty.

Views

SIP AG user group view

Default Level

2: Configuration level

Usage Guidelines

To perform authentication on a user group, configure the user name and password for the user group.

Example

Set the authentication user name to **h12345**, password format to cipher, and password to 12345678 for a user group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 1 1
[Huawei-voice-sipagusergroup-1-1] auth username h12345 password cipher
 Please input user password(1-64 chars):********
```

16.6.2.5 auto-resume-limit

Function

Using the **auto-resume-limit** command, you can set the maximum number of automatic recoveries from deterioration.

Using the **undo auto-resume-limit** command, you can restore the default maximum number of automatic recoveries from deterioration.

By default, the maximum number of automatic recoveries from deterioration is 20.

Format

auto-resume-limit *auto-resume-limit*

undo auto-resume-limit

Parameters

Parameter	Description	Value
auto-resume-limit	Specifies the maximum number of automatic recoveries from deterioration.	The value is an integer that ranges from 0 to 255.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the maximum number of automatic recoveries from deterioration to 50.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] auto-resume-limit 50
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.6 base-telno

Function

The **base-telno** command configures a basic telephone number for a SIP AG user.

The **undo base-telno** command deletes the basic telephone number of a SIP AG user.

By default, no basic telephone number is configured for a SIP AG user.

Format

base-telno *telno-value* [**sipagusergroup** *usergroup-id*]

undo base-telno [**sipagusergroup**]

Parameters

Parameter	Description	Value
telno-value	Specifies a basic telephone number for a SIP AG user.	The value is a string of 1 to 32 characters.
sipagusergroup *usergroup-id*	Specifies the user group of the basic telephone number.	The value is an integer that ranges from 0 to 65535.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **base-telno** command configures a basic telephone number for a SIP AG user. Only one basic telephone number can be configured for a SIP AG user.

Example

Configure a basic telephone number for a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] base-telno 12345678
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.7 bell-ans-flag

Function

Using the **bell-ans-flag** command, you can enable or disable the SIP AG's capability to support the BELL ANS flag.

Using the **undo bell-ans-flag** command, you can restore the default configuration.

By default, the BELL ANS flag is not supported.

Format

bell-ans-flag { **enable** | **disable** }

undo bell-ans-flag

Parameters

Parameter	Description	Value
enable	Indicates that the BELL ANS flag is supported.	-
disable	Indicates that the BELL ANS flag is not supported.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **bell-ans-flag** command enables or disables the SIP AG's capability to support the BELL ANS flag. This command is valid only on FXS interfaces.

Precautions

Before using the **bell-ans-flag** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Configure the SIP AG to support the BELL ANS flag.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] bell-ans-flag enable
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.8 centrex-dial

Function

Using the **centrex-dial** command, you can configure the dial-out mode for Centrex users in a SIP service data profile. The dial-out mode determines how users in a Centrex group call users out of the Centrex group.

Using the **undo centrex-dial** command, you can restore the default call-out mode in a SIP service data profile.

By default, the dial-out mode for Centrex users is direct dialing.

Format

centrex-dial { **directly** | **secondary** }

undo centrex-dial

Parameters

Parameter	Description	Value
directly	Indicates the direct dialing mode.	-
secondary	Indicates the two-stage dialing mode.	-

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

The **centrex-dial** determines how users in a Centrex group call users out of the Centrex group. The direct dialing mode is recommended.

Example

Configure the dial-out mode for Centrex users in SIP service data profile 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata 1 12345678
[Huawei-voice-sipservicedata-1-12345678] centrex-dial directly
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.9 centrex-number

Function

Using the **centrex-number** command, you can configure a Centrex number in a SIP service data profile.

Using the **undo centrex-number** command, you can delete the Centrex number in a SIP service data profile.

Format

centrex-number *centrex-number*

undo centrex-number

Parameters

Parameter	Description	Value
centrex-number	Specifies a Centrex number.	The value is an integer that ranges from 0 to 4294967295.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

Users in a Centrex group can enjoy preferential services. For example, users in the Centrex group can call each other free of charge.

Example

Configure a Centrex number in SIP service data profile 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata 1 12345678
[Huawei-voice-sipservicedata-1-12345678] centrex-number 1
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.2.10 centrex-prefix

Function

Using the **centrex-prefix** command, you can configure a Centrex prefix in a SIP service data profile.

Using the **undo centrex-prefix** command, you can delete the Centrex prefix from a SIP service data profile.

Format

centrex-prefix *centrex-prefix*

undo centrex-prefix

Parameters

Parameter	Description	Value
centrex-prefix	Specifies a Centrex prefix.	The value is an integer that ranges from 1 to 7.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

When a user in a Centrex group needs to call a user out of the Centrex group, the user must dial the Centrex prefix before dialing the number of the called user.

Example

Configure a Centrex prefix in SIP service data profile 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata 1 12345678
[Huawei-voice-sipservicedata-1-12345678] centrex-prefix 6
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.11 clip-format

Function

The **clip-format** command configures the calling number format for a SIP AG user.

The **undo clip-format** command restores the default calling number format of a SIP AG user.

By default, the calling number format of a SIP AG user is **SDMF-FSK**.

Format

clip-format *format-value*

undo clip-format

Parameters

Parameter	Description	Value
format-value	Specifies the calling number format for a SIP AG user.	Enumerated type. The values are as follows: • **SDMF-FSK**: specifies the frequency-shift keying (FSK) simple data format. • **MDMF-FSK**: specifies the FSK compound data format. • **DTMF**: specifies the Dual Tone Multifrequency (DTMF) format. • **r15**: specifies the Russia calling number format. • **ETSI**: specifies the BT calling number format.

Views

SIP AG user view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Before using the **clip-format** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Configure the FSK simple data format as the calling number format.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] clip-format sdmf-fsk
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.12 clip-transmission-sequence

Function

Using the **clip-transmission-sequence** command, you can configure the sequence in which the calling number of a SIP AG user is displayed.

Using the **undo clip-transmission-sequence** command, you can restore the default sequence in which the calling number of a SIP AG user is displayed.

By default, the calling number of a SIP AG user is displayed after ringing.

Format

clip-transmission-sequence { **after-ring** | **before-ring** }

undo clip-transmission-sequence

Parameters

Parameter	Description	Value
after-ring	Configures the calling number to be displayed after ringing.	-
before-ring	Configures the calling number to be displayed before ringing.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **clip-transmission-sequence** command configures the sequence in which the calling number of a SIP AG user is displayed. You can set the sequence to **after-ring** or **before-ring**.

Before using the **clip-transmission-sequence** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the sequence in which the calling number of a SIP AG user is displayed to **before-ring**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] clip-transmission-sequence before-ring
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.13 dc-time

Function

Using the **dc-time** command, you can set the power-off interval for a SIP AG user.

Using the **undo dc-time** command, you can restore the default power-off interval of a SIP AG user.

By default, the power-off interval of a SIP AG user is 100 ms.

Format

dc-time *dc-time*

undo dc-time

Parameters

Parameter	Description	Value
dc-time	Specifies the power-off interval.	The value is an integer that ranges from 0 to 100, in 10 milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **dc-time** command sets the power-off interval for a SIP AG user. The *dc-time* parameter is optional.

Before using the **dc-time** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the power-off interval of a SIP AG user to 50 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] dc-time 5
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.14 detect-ansbar-by-single-tone

Function

Using the **detect-ansbar-by-single-tone** command, you can enable or disable ANSbar signal detection using single tones.

Using the **undo detect-ansbar-by-single-tone** command, you can restore the default configuration.

By default, ANSbar signal detection using single tones is disabled.

Format

detect-ansbar-by-single-tone { **enable** | **disable** }

undo detect-ansbar-by-single-tone

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
enable	Enables ANSbar signal detection using single tones.	-
disable	Disables ANSbar signal detection using single tones.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **detect-ansbar-by-single-tone** command enables or disables ANSbar signal detection using single tones.

Before using the **detect-ansbar-by-single-tone** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Enable ANSbar signal detection using single tones.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] detect-ansbar-by-single-tone enable
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.15 dial-tone

Function

Using the **dial-tone** command, you can configure the dial tone type in a SIP service data profile.

Using the **undo dial-tone** command, you can restore the default dial tone type in a SIP service data profile.

By default, the normal dial tone type is used in a SIP service data profile.

 Copyright © Huawei Technologies Co., Ltd.

Format

dial-tone { **normal** | **special** | **mwi** }

undo dial-tone

Parameters

Parameter	Description	Value
normal	Indicates the normal dial tone type.	-
special	Indicates the special dial tone type.	-
mwi	Indicates the message waiting tone.	-

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

The **dial-tone** command configures the dial tone type, including the normal dial tone, special dial tone, and message waiting tone.

Example

Set the dial tone type to **mwi** in SIP service data profile.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] dial-tone mwi
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.16 display voice sipagusergroup

Function

The **display voice sipagusergroup** command displays information about the configured user group.

Format

display voice sipagusergroup [*sipag-interface-id* [*usergroup-id*]]

Parameters

Parameter	Description	Value
sipag-interface-id	Displays user group information on a specified SIP AG interface.	The value is an integer that ranges from 0 to 16777215.
usergroup-id	Displays information about a specified user group.	The value is an integer that ranges from 0 to 65535.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view information about the configured user group, run the **display voice sipag usergroup** command.

Example

Display user group information on SIP AG interface 1.

```
<Huawei> display voice sipagusergroup 1
  Spec: 16, Records: 1
  -------------------------
  AGID                    : 1
  Groupid                 : 1
```

Display information about user group 1 on SIP AG interface 1.

```
<Huawei> display voice sipagusergroup 1 1
  Running state           : RBlock
  AGID                    : 1
  Groupid                 : 1
  Register URI mode       : inneruser
  Precinct mode           : local
  Subscribe               : enable
  Group name              : huawei
  Uri                     : 28780!*!
  Auth username           :
  Auth password mode      : password
  Auth password           :
```

Table 16-125 Description of the display voice sipagusergroup command output

Item	Description
Running state	Registration status of a user group, including: ● RBlock: The remote interface is blocked. ● LBlock: The local interface is blocked. ● StartSvc: The service starts.
AGID	ID of the SIP AG interface that the user group belongs to.
Groupid	User group ID.
Register URI mode	Registration URI mode. The values are as follows: ● inneruser: indicates that the user group uses the registrar URI of a member user. ● alone: indicates that the user group uses an independent registrar URI.
Precinct mode	Mode in which a user group manages users. The values are as follows: ● local ● remote
Subscribe	User authority (UA) profile subscription request. The values are as follows: ● enable: indicates that a UA profile subscription request is initiated by a user group. ● disable: indicates that a UA profile subscription request is initiated by a single user.
Group name	User group name.
Uri	User group URI.
Auth username	Authentication user name for a user group.
Auth password mode	Authentication password mode for a user group, including password and HA1. The values are as follows: ● password ● ha1
Auth password	Authentication password for a user group.

Related Topics

16.6.1.15 display voice sipag

16.6.2.17 display voice sipaguser

Function

The **display voice sipaguser** command displays the configuration of a SIP AG user.

Format

display voice sipaguser [*sipaguser-name*]

Parameters

Parameter	Description	Value
sipaguser-name	Specifies a SIP AG user name.	The value is a string of 1 to 32 characters.

Views

All view

Default Level

3: Management level

Usage Guidelines

To view the configuration of a SIP AG user, run the **display voice sipaguser** command.

Example

Display configurations of all SIP AG users.

```
<Huawei> display voice sipaguser
  Spec: 96, Records: 2
  -------------------------
  Sipaguser name            : 1100
  Slotid/Subcard/Portid     : 1/0/0
  AGID                      : 1
  Base telno                : 1100

  Sipaguser name            : 1101
  Slotid/Subcard/Portid     : 1/0/1
  AGID                      : 1
  Base telno                : 1101
```

Table 16-126 Description of the display voice sipagusergroup command output

Item	Description
Sipaguser name	User name.

Item	Description
Slotid/Subcard/Portid	Slot number/subcard number/interface number of the user.
AGID	ID of the SIP AG interface that the user belongs to.
Base telno	Phone number of the SIP AG user.

Display the configuration of SIP AG user 1100.

```
<Huawei> display voice sipaguser 1100
  Slotid/Subcard/Portid      : 1/0/0
  AGID                       : 1
  Base telno                 : 1100
  GroupID                    :
  Priority                   : cat3
  Line type                  : DEL
  CLIP transmission sequence : After ring
  CLIP format                : SDMF FSK
  DC time(ms)                : 100
  FSK time(ms)               : 800
  VQE agc                    : Off
  VQE agc level(dbm0)        : -22
  VQE sns                    : Off
  VQE sns level(dB)          : 12
  DSP input gain(dB)         : 0
  DSP output gain(dB)        : 0
  DSP template               :
  Ans bar by single tone     : Off
  Bell ans flag              : Off
  FSK mode                   : BELL202
  Fsk tas pattern            : NO TAS
```

Table 16-127 Description of the display voice sipagusergroup command output

Item	Description
Slotid/Subcard/Portid	Slot number/subcard number/interface number of the user.
AGID	ID of the SIP AG interface that the user belongs to.
Base telno	Phone number of the SIP AG user.
GroupID	Group ID that a user belongs to.
Priority	User terminal priority.
Line type	User type.
CLIP transmission sequence	Calling number delivery sequence.
CLIP format	Calling number format.
DC time(ms)	Duration for releasing call signals.
FSK time(ms)	FSK delay.

Item	Description
VQE agc	VQE function flag.
VQE agc level(dbm0)	Target VQE level.
VQE sns	VQE noise suppression flag.
VQE sns level(dB)	VQE noise suppression level, in dB.
DSP input gain(dB)	DSP chip input gain.
DSP output gain(dB)	DSP chip output gain.
DSP template	DSP template name.
Ans bar by single tone	Whether single-tone ANSbar signal detection is supported.
Bell ans flag	Whether the BELL ANS flag is supported.
FSK mode	FSK mode of CLIP.
Fsk tas pattern	TAS mode of CLIP.

Related Topics

16.6.1.15 display voice sipag

16.6.2.18 display voice sipservicedata

Function

The **display voice sipservicedata** command displays the user service data of a SIP AG.

Format

display voice sipservicedata *sipag-user-name telephone-number*

Parameters

Parameter	Description	Value
sipag-user-name	Specifies the user name of a SIP AG.	The value is a string of 1 to 32 characters.
telephone-number	Specifies the telephone number of a SIP AG.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

To view the user service data of a SIP AG, run the **display voice sipservicedata** command.

Example

Display the service data of a service data profile **user**.

```
<Huawei> display voice sipservicedata user 12345678
  Auth name                    : huawei
  Auth password mode           : Password
  Auth password                : ****
  Call hold                    : Enable
  Three party                  : Enable
  Conference                   : Enable
  Call transfer                : Enable
  Call waiting                 : Disable
  Malicious call identification : Disable
  Mwi                          : Disable
  Terminal portability         : Disable
  Call diversion               : Disable
  Anonymous call               : Disable
  Hotline                      : Disable
  Uus1                         : Disable
  Uus2                         : Disable
  Uus3                         : Disable
  Centrex number               :
  Centrex prefix               :
  Centrex dial                 : Dial directly
  Dial tone                    : Mw
  Mwi mode                     : Deferred
  Hotline number               :
  CFB number                   :
  CFU number                   :
  CFNR number                  :
```

Table 16-128 Description of the display voice sipservicedata command output

Item	Description
Auth name	Authentication user name for a user group.
Auth password mode	Authentication password mode for a user group, including password and HA1. The values are as follows: ● password ● ha1
Auth password	Authentication password for a user group.
Call hold	Whether the call holding service is supported.

Item	Description
Three party	Whether the three-party service is supported.
Conference	Whether the conference call service is supported.
Call transfer	Whether the call transfer service is supported.
Call waiting	Whether the call waiting service is supported.
Malicious call identification	Whether the malicious call identification service is supported.
Mwi	Whether the message waiting indicator (MWI) service is supported.
Terminal portability	Whether the terminal mobility service is supported.
Call diversion	Whether the call forwarding service is supported.
Anonymous call	Whether the anonymous call service is supported.
Hotline	Whether the hotline service is supported.
Uus1	Whether the user-to-user signalling1 service is supported.
Uus2	Whether the user-to-user signalling2 service is supported.
Uus3	Whether the user-to-user signalling3 service is supported.
Centrex number	Centrex group number.
Centrex prefix	Outgoing prefix.
Centrex dial	Centrex group attribute. ● directly: indicates direct dialing ● secondary: indicates two-stage dialing
Dial tone	Dial tone type. ● normal: indicates normal tone ● special: indicates special tone ● mwi: indicates message waiting tone
Mwi mode	MWI service mode. ● deferred: indicates deferred MWI mode ● immediate: indicates immediate MWI mode ● combine: indicates combined MWI mode
Hotline number	Hotline number.
CFB number	Call forwarding busy (CFB) number.
CFU number	Call forwarding unconditional (CFU) number.
CFNR number	Call forwarding on no reply (CFNR) number.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.2.41 sipservicedata

16.6.2.19 dsp-input-gain

Function

Using the **dsp-input-gain** command, you can configure the DSP chip input gain for a SIP AG user.

Using the **undo dsp-input-gain** command, you can restore the default DSP chip input gain of a SIP AG user.

By default, the DSP chip input gain of a SIP AG user is 0 dB.

Format

dsp-input-gain *dsp-input-gain*

undo dsp-input-gain

Parameters

Parameter	Description	Value
dsp-input-gain	Specifies the DSP chip input gain.	The value is an integer that ranges from 0 to 15, in dB.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **dsp-input-gain** command configures the DSP chip input gain for a SIP AG user. You can improve the voice quality by configuring the DSP chip input gain.

Before using the **dsp-input-gain** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the DSP chip input gain to 5 for a SIP AG user.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] dsp-input-gain 5
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.20 dsp-output-gain

Function

Using the **dsp-output-gain** command, you can configure the DSP chip output gain for a SIP AG user.

Using the **undo dsp-output-gain** command, you can restore the default DSP chip output gain of a SIP AG user.

By default, the DSP chip output gain of a SIP AG user is 0 dB.

Format

dsp-output-gain *dsp-output-gain*

undo dsp-output-gain

Parameters

Parameter	Description	Value
dsp-output-gain	Specifies the DSP chip output gain.	The value is an integer that ranges from 0 to 20, in dB.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **dsp-output-gain** command configures the DSP chip output gain for a SIP AG user. You can improve the voice quality by configuring the DSP chip output gain.

Before using the **dsp-output-gain** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the DSP chip output gain to 5 for a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] dsp-output-gain 5
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.21 dsp-template

Function

Using the **dsp-template** command, you can configure a DSP template name for a SIP AG user.

Using the **undo dsp-template** command, you can delete a DSP template name of a SIP AG user.

By default, no DSP template name is configured for a SIP AG user.

Format

dsp-template *dsp-template*

undo dsp-template

Parameters

Parameter	Description	Value
dsp-template	Specifies the name of a DSP template.	The value is a string of 1 to 31 characters.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

Before using the **dsp-template** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a DSP template name **highspeed-modem** for a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] dsp-template highspeed-modem
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.22 endservice (SIP AG user view)

Function

Using the **endservice** command, you can terminate services of a specified SIP AG user.

Using the **undo endservice** command, you can restart services of a SIP AG user.

By default, services of a SIP AG user are not terminated.

Format

endservice { **defer** [**maxcobtime** *maxcobtime-value*] | **immediate** }

undo endservice

Parameters

Parameter	Description	Value
defer	Indicates the delay mode used for terminating services of a SIP AG user.	-
maxcobtime *maxcobtime-value*	Specifies the maximum delay duration for terminating services of a SIP AG user.	It is an integer that ranges from 1 to 1440, in minutes. The default value is 240.
immediate	Indicates the mode used for immediately terminating services of a SIP AG user.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

This command can terminate services of a SIP AG user. When using this command, pay attention to the following:

- When **defer** is specified, services on a port are terminated properly within the delay range; if services are not terminated within the delay range, the system handles services according to the mode when the delay expires.
- **maxcobtime** *maxcobtime-value* specifies the maximum duration for which the system allows services on a port to be terminated. If services on the port are not terminated within the maximum duration, the system handles services according to the mode when the delay expires.

NOTE

Services of users are terminated after this command is executed. Confirm the action before you run this command.

Example

Terminate services of the SIP AG user **huawei** immediately.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] endservice immediate
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.23 endservice (User group view)

Function

Using the **endservice** command, you can terminate services of a user group.

Using the **undo endservice** command, you can restart services of a user group.

Format

endservice

undo endservice

Parameters

None

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

To terminate services of a user group, run the **endservice** command. Services of users are terminated after this command is used; therefore, exercise caution when you run this command.

Example

Terminate services of a specified user group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 1 1
[Huawei-voice-sipagusergroup-1-1] endservice
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.24 extend-telno

Function

The **extend-telno** command configures an extended telephone number for a SIP AG user.

The **undo extend-telno** command deletes the extended telephone number of a SIP AG user.

By default, no extended telephone number is configured for a SIP AG user.

Format

extend-telno *telno-value* [**sipagusergroup** *usergroup-id*]

undo extend-telno *telno-value* [**sipagusergroup**]

Parameters

Parameter	Description	Value
telno-value	Specifies an extended telephone number for a SIP AG user.	The value is a string of 1 to 32 characters.
sipagusergroup *usergroup-id*	Specifies the user group of the extended telephone number.	The value is an integer that ranges from 0 to 65535.

Views

SIP AG user view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The **extend-telno** command configures an extended telephone number for a SIP AG user so that the SIP has multiple telephone numbers.

Example

Configure an extended telephone number for a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] extend-telno 12341234
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.25 fsk-mode

Function

Using the **fsk-mode** command, you can configure the FSK call display mode.

Using the **undo fsk-mode** command, you can restore the default FSK call display mode.

By default, the FSK call display mode is BELL_202.

Format

fsk-mode { **BELL_202** | **CCITT_V23** | **NTT** }

undo fsk-mode

Parameters

Parameter	Description	Value
BELL_202	Sets the FSK call display mode to BELL_202.	-
CCITT_V23	Sets the FSK call display mode to CCITT_V23.	-
NTT	Sets the FSK call display mode to NTT.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **fsk-mode** command configures the FSK call display mode. The **fsk-mode** parameter is optional.

Before using the **fsk-mode** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the FSK call display mode to CCITT_V23.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] fsk-mode CCITT_V23
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.26 fsk-time

Function

Using the **fsk-time** command, you can set the FSK delay for a SIP AG user.

Using the **undo fsk-time** command, you can restore the default FSK delay of a SIP AG user.

By default, the FSK delay of a SIP AG user is 800 ms.

Format

fsk-time *fsk-time*

undo fsk-time

Parameters

Parameter	Description	Value
fsk-time	Specifies the FSK delay.	The value is an integer that ranges from 0 to 100 The unit is 10 milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **fsk-time** command sets the FSK delay for a SIP AG user. The *fsk-time* parameter is optional.

Before using the **fsk-time** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the FSK delay of a SIP AG user to 50 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] fsk-time 5
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.27 group-name

Function

The **group-name** command configures a name for a user group.

The **undo group-name** command deletes the name for the user group.

Format

group-name *usergroup-name*

undo group-name

Parameters

Parameter	Description	Value
usergroup-name	Specifies the user group name.	The value is a string of 1 to 64 characters.

Views

SIP AG user group view

Default Level

2: Configuration level

Usage Guidelines

To facilitate user group management and maintenance, run the **group-name** command to configure a name for a user group.

Example

Configure a user group name **ip123**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 1 1
[Huawei-voice-sipagusergroup-1-1] group-name ip123
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.28 line-type

Function

Using the **line-type** command, you can set the user type for a SIP AG user.

Using the **undo line-type** command, you can restore the default user type of a SIP AG user.

By default, the user type of a SIG AG user is **DEL**.

Format

line-type { **DEL** | **ECPBX** | **LCPBX** | **PayPhone** }

undo line-type

Parameters

Parameter	Description	Value
DEL	Specifies the user type as Direct Exchange Lines (DEL).	-
ECPBX	Specifies the user type as Earth Calling PBX (ECPBX).	-
LCPBX	Specifies the user type as Loop Calling PBX (LCPBX).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
PayPhone	Specifies the user type as pay phone.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **line-type** command sets the user type for a SIP AG user.

Before using the **line-type** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the user type to **PayPhone** for the SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] line-type PayPhone
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.29 mwi-mode

Function

Using the **mwi-mode** command, you can configure the message waiting indicator (MWI) service mode in a SIP service data profile.

Using the **undo mwi-mode** command, you can restore the default MWI service mode in a SIP service data profile.

By default, the deferred MWI service mode is used.

Format

mwi-mode { **deferred** | **immediate** | **combine** }

undo mwi-mode

Parameters

Parameter	Description	Value
deferred	Indicates that the MWI is sent after a delay.	-
immediate	Indicates that the MWI is sent immediately.	-
combine	Indicates the combined WMI mode.	-

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

The **mwi-mode** command configures the MWI service mode in a SIP service data profile. The deferred mode is recommended.

Example

Set the MWI service mode in SIP service data profile 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata 1 12345678
[Huawei-voice-sipservicedata-1-12345678] mwi-mode deferred
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.30 precinct-mode

Function

The **precinct-mode** command configures the mode in which a user group manages users.

The **undo precinct-mode** command restores the default mode in which a user group manages users.

By default, the mode in which a user group manages users is **local**.

Format

precinct-mode { **local** | **remote** }

undo precinct-mode

Parameters

Parameter	Description	Value
local	Indicates that users are managed locally.	-
remote	Indicates that users are managed by the remote IMS.	-

Views

SIP AG user group view

Default Level

2: Configuration level

Usage Guidelines

The **precinct-mode** command configures the mode in which a user group manages users.

Example

Set the mode in which a user group manages users to **local**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 1 1
[Huawei-voice-sipagusergroup-1-1] precinct-mode local
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.31 priority

Function

Using the **priority** command, you can configure the priority for a SIP AG user.

Using the **undo priority** command, you can restore the default priority of a SIP AG user.

By default, the priority of a SIG AG user is **cat3**.

Format

priority { **cat1** | **cat2** | **cat3** }

undo priority

Parameters

Parameter	Description	Value
cat1	Specifies the category-1 user priority.	-
cat2	Specifies the category-2 user priority.	-
cat3	Specifies the category-3 user priority.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the SIP AG user priority. Priorities are **cat1**, **cat2**, **cat3** in a descending order.

Example

Set the SIP AG user priority to **cat1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] priority cat1
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.32 register-uri-mode

Function

The **register-uri-mode** command configures the registrar URI mode for a user group.

Format

register-uri-mode { **inneruser** | **alone** }

undo register-uri-mode

Parameters

Parameter	Description	Value
inneruser	Indicates that the user group uses the registrar URI of a member user.	-
alone	Indicates that the user group uses an independent registrar URI. Different users are configured with different URIs.	-

Views

SIP AG user group view

Default Level

2: Configuration level

Usage Guidelines

This command is mandatory and used to configure the registrar URI mode for a user group.

If you run the **register-uri-mode** command multiple times in the same user group view, only the latest configuration takes effect.

Example

Set the registrar URI mode of a user group to **alone**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 1 1
[Huawei-voice-sipagusergroup-1-1] register-uri-mode alone
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.33 service cfb

Function

Using the **service cfb** command, you can configure a forward-to number for the call forwarding busy (CFB) service in a SIP service data profile.

Using the **undo service cfb** command, you can delete the CFB forward-to number from a SIP service data profile.

 Copyright © Huawei Technologies Co., Ltd.

By default, no CFB forward-to number is configured in a SIP service data profile.

Format

service cfb *cfbnum-value*

undo service cfb

Parameters

Parameter	Description	Value
cfbnum-value	Specifies a CFB forward-to number.	The value is a string of 1 to 32 characters.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

When the called user is busy, the call is forwarded to the specified number.

Example

Set the CFB forward-to number to 12345678.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] service cfb 12345678
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.34 service cfnr

Function

The **service cfnr** command configures a forward-to number for the call forwarding no reply (CFNR) service in a SIP service data profile.

The **undo service cfnr** command deletes a CFNR forward-to number from a SIP service data profile.

By default, no CFNR forward-to number is configured in a SIP service data profile.

Format

service cfnr *cfnrnumtime-value cfnrnum-value*

undo service cfnr

Parameters

Parameter	Description	Value
cfnrnumtime-value	Specifies the CFNR timeout period.	The value is an integer that ranges from 0 to 65535, in seconds.
cfnrnum-value	Specifies a CFNR forward-to number.	The value is a string of 1 to 32 characters.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

The **service cfnr** command sets a CFNR forward-to number and CFNR timeout period. When a called party does not answer a call after the CFNR timeout period expires, CFNR is activated.

Example

Set the CFNR forward-to number to 12345679 and timeout period to 30 seconds.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] service cfnr 30 12345679
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.35 service cfo

Function

The **service cfo** command configures a forward-to number for the call forwarding offline (CFO) service in a SIP service data profile.

The **undo service cfo** command deletes the CFO forward-to number from a SIP service data profile.

 Copyright © Huawei Technologies Co., Ltd.

By default, no CFO forward-to number is configured.

Format

service cfo *cfonum-value*

undo service cfo

Parameters

Parameter	Description	Value
cfonum-value	Specifies a CFO forward-to number.	The value is a string of 1 to 32 characters.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

The **service cfo** command configures a CFO forward-to number. When a user is offline, incoming calls of the user are forwarded to the CFO forward-to number.

Example

Set the CFO forward-to number to 12345679.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] service cfo 12345679
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.36 service cfu

Function

Using the **service cfu** command, you can configure a forward-to number for the call forwarding unconditional (CFU) service in a SIP service data profile.

Using the **undo service cfu** command, you can delete CFU forward-to number from a SIP service data profile.

By default, no CFU forward-to number is configured in a SIP service data profile.

 Copyright © Huawei Technologies Co., Ltd.

Format

service cfu *cfunum-value*

undo service cfu

Parameters

Parameter	Description	Value
cfunum-value	Specifies a CFU forward-to number.	The value is a string of 1 to 32 characters.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

When the CFU service is configured for a user, calls to this user are always forwarded to the specified number.

Example

Set the CFU forward-to number to 12345679.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] service cfu 12345679
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.37 service hotline

Function

The **service hotline** command configures a hotline number in a SIP service data profile.

The **undo service hotline** command deletes the hotline number from a SIP service data profile.

By default, no hotline number is configured.

Format

service hotline *hotline-time hotline-number*

 Copyright © Huawei Technologies Co., Ltd.

undo service hotline

Parameters

Parameter	Description	Value
hotline-time	Specifies the time to wait before dialing a hotline number.	The value is an integer that ranges from 0 to 255, in seconds.
hotline-number	Specifies a hotline number.	The value is a string of 1 to 24 characters.

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

If a user that has subscribed to the hotline service does not dial any number within the specified period after picking up the phone, the system dials the hotline number for the user. The default time (100 seconds) is recommended.

Example

Set the hotline number to 123456 and the time to wait before dialing the hotline number to 80 seconds in a SIP service data profile.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] service hotline 80 123456
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.38 service-right (SIP service data profile view)

Function

The **service-right enable** command enables the service right.

The **service-right dsable** command disables the service right.

Format

service-right *service-name* **enable**

service-right *service-name* **disable**

Parameters

Parameter	Description	Value
service-name	Specifies a service name.	The services include: ● anonymous-call: anonymous call ● call-diversion: call forwarding ● call-hold: call hold ● call-transfer: call transfer ● conf: conference ● cw: call waiting ● hotline: hotline ● malicious-call-identification: malicious call identification ● mwi: message waiting indicator ● terminal-portability: terminal portability ● three-party: three-party service ● uus1: UUS1 ● uus2: UUS2 ● uus3: UUS3
enable	Specifies enabling the service right.	-
disable	Specifies disabling the service right.	-

Views

SIP service data profile view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable the RBT service.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata user 12345678
[Huawei-voice-sipservicedata-user-12345678] service-right anonymous-call enable
```

16.6.2.39 sipaguser (Voice View)

Function

The **sipaguser** command creates a SIP AG user and displays the SIP AG user view.

The **undo sipaguser** command deletes a SIP AG user.

By default, no SIP AG user is created.

Format

sipaguser *sipaguser-name* [**port** [**pots** | **bra**] *interface-number*]

undo sipaguser *sipaguser-name*

Parameters

Parameter	Description	Value
sipaguser-name	Specifies a SIP AG user name.	The value is a string of 1 to 32 case-insensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
port	Indicates the interface of a SIP AG user.	-
pots	Indicates an FXS interface.	-
bra	Indicates a BRA interface.	-
interface-number	Specifies an interface number for a SIP AG user.	The value is a string of 1 to 15 characters without spaces. The value of *interface-number* is based on the device specifications.

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a terminal user connects to the IMS through the SIP AG. You need to create a SIP AG user for the terminal user and run the **agid** command to add the SIP AG user to a specified SIP AG interface. When creating a SIP AG user, you must specify the interface number by specifying the **port** [**pots** | **bra**] *interface-number* parameter. After entering the view of an existing SIP AG user, you do not need to input the interface number.

Precautions

If the router does not work in SIP AG mode, you need to run the **service-mode** command to configure the router to work in SIP AG mode.

Example

Create a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei port 1/0/0
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.40 sipagusergroup

Function

The **sipagusergroup** command creates a SIP AG user group.

The **undo sipagusergroup** command deletes a SIP AG user group.

Format

sipagusergroup *sipag-interface-id usergroup-id*

undo sipagusergroup *sipag-interface-id usergroup-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
sipag-interface-id	Specifies the interface ID of a SIP AG.	The value is an integer that ranges from 0 to 16777215.
usergroup-id	Specifies the user group ID of a SIP AG.	The value is an integer that ranges from 0 to 65535.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When you need to configure a user group for a SIP AG, use the **usergroup** command. After creating a SIP AG user group, add it to the specified SIP AG. The user group must also be added to the IP Multimedia Subsystem (IMS), and the parameters of the user group must be the same on the SIP AG and IMS.

Example

Create a SIP AG user group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 2 1
[Huawei-voice-sipagusergroup-2-1]
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.41 sipservicedata

Function

Using the **sipservicedata** command, you can create a SIP service data profile and enter its view.

Using the **undo sipservicedata** command, you can delete a SIP service data profile.

By default, no SIP service data profile is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

sipservicedata *sipaguser-name telephone-number*

undo sipservicedata *sipaguser-name telephone-number*

Parameters

Parameter	Description	Value
sipaguser-name	Specifies a SIP AG user.	The value is a string of 1 to 32 characters.
telephone-number	Specifies the phone number of the SIP AG user.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

A SIP service data profile controls services of a SIP AG user. The **sipservicedata** command creates a SIP service data profile.

The configured phone number must be the same as the phone number configured for the SIP AG user.

Example

Create a SIP service data profile.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipservicedata huawei 12345678
[Huawei-voice-sipservicedata-huawei-12345678]
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.42 subscribe ua-profile

Function

Using the **subscribe ua-profile** command, you can determine whether the request to subscribe to a user authority (UA) profile is initiated by a user group or a single user.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo subscribe ua-profile** command, you can restore the default configuration.

By default, a UA profile subscription request is initiated by a user group.

Format

subscribe ua-profile { **enable** | **disable** }

undo subscribe ua-profile

Parameters

Parameter	Description	Value
enable	Initiates a UA profile subscription request by a user group.	-
disable	Initiates a UA profile subscription request by a single user.	-

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

The **subscribe ua-profile** command determines whether a UA profile subscription request is initiated by a user group for a single user.

Example

Specify that a UA profile subscription request is initiated by a user group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 1 1
[Huawei-voice-sipagusergroup-1-1] subscribe ua-profile enable
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.43 tas-pattern

Function

Using the **tas-pattern** command, you can configure the TAS mode of Calling Line Identification Presentation (CLIP).

Using the **undo tas-pattern** command, you can restore the default TAS mode of CLIP.

By default, the TAS mode of CLIP is NO-TAS.

Format

tas-pattern { **NO-TAS** | **DT-AS** }

undo tas-pattern

Parameters

Parameter	Description	Value
NO-TAS	Sets the TAS mode of CLIP to NO-TAS.	-
DT-AS	Sets the TAS mode of CLIP to DT-AS.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **tas-pattern** command sets the TAS mode of CLIP for a SIP AG user.

Before using the **tas-pattern** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the TAS mode of CLIP to NO-TAS.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] tas-pattern NO-TAS
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.2.44 uni-report

Function

Using the **uni-report** command, you can enable or disable the function that reports user network interface (UNI) faults.

Using the **undo uni-report** command, you can restore the default status of the UNI fault reporting function.

By default, the UNI fault reporting function is disabled.

Format

uni-report { **enable** | **disable** }

undo uni-report

Parameters

Parameter	Description	Value
enable	Enables the UNI fault reporting function.	-
disable	Disables the UNI fault reporting function.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **uni-report** command enables or disables the UNI fault reporting function. If this function is enabled, users on a UNI are deregistered when the UNI fails. This command is optional.

Example

Enable the UNI fault reporting function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] uni-report enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.2.45 uri

Function

The **uri** command configures a uniform resource identifier (URI) for a user group.

Format

uri *uri*

Parameters

Parameter	Description	Value
uri	Specifies a URI for a user group.	The value is a string of 1 to 64 characters.

Views

SIP AG user group view

Default Level

2: Configuration level

Usage Guidelines

This command configures a URI for a user group. User groups must use different URIs.

If you run the **uri** command multiple times in the same user group view, only the latest configuration takes effect.

Example

Set the URI of a user group to **28780!*!**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipagusergroup 1 1
[Huawei-voice-sipagusergroup-1-1] uri 28780!*!
```

Related Topics

16.6.1.15 display voice sipag

 Copyright © Huawei Technologies Co., Ltd.

16.6.2.46 vqe-agc

Function

Using the **vqe-agc** command, you can enable or disable the voice quality enhancement (VQE) function for a SIP AG user.

Using the **undo vqe-agc** command, you can restore the default VQE status for a SIP AG user.

By default, VQE is disabled for a SIP AG user.

Format

vqe-agc { **enable** | **disable** }

undo vqe-agc

Parameters

Parameter	Description	Value
enable	Enables the VQE function.	-
disable	Disables the VQE function.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **vqe-agc** command enables or disables the VQE function for a SIP AG user. This command is optional.

Before using the **vqe-agc** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Enable the VQE function for a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] vqe-agc enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

16.6.1.15 display voice sipag

16.6.2.47 vqe-agc-level

Function

Using the **vqe-agc-level** command, you can set the target voice quality enhancement (VQE) level for a SIP AG user.

Using the **undo vqe-agc-level** command, you can restore the default target VQE level for a SIP AG user.

By default, the target VQE level of a SIP AG user is 13.

Format

vqe-agc-level *vqe-agc-level*

undo vqe-agc-level

Parameters

Parameter	Description	Value
vqe-agc-level	Specifies the target VQE level.	The value is an integer that ranges from 0 to 15.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **vqe-agc-level** command sets the target VQE level for a SIP AG user. This command is optional.

Before using the **vqe-agc-level** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the target VQE level of a SIP AG user to 10

```
<Huawei> system-view
[Huawei] voice
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] vqe-agc-level 10
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.48 vqe-sns

Function

Using the **vqe-sns** command, you can enable or disable voice quality enhancement (VQE) noise suppression for a SIP AG user.

Using the **undo vqe-sns** command, you can restore the default status of VQE noise suppression.

By default, VQE noise suppression is disabled for a SIP AG user.

Format

vqe-sns { **enable** | **disable** }

undo vqe-sns

Parameters

Parameter	Description	Value
enable	Enables VQE noise suppression.	-
disable	Disables VQE noise suppression.	-

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **vqe-sns** command enables or disables VQE noise suppression for a SIP AG user. This command is optional.

Before using the **vqe-sns** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable VQE noise suppression for a SIP AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] vqe-sns enable
```

Related Topics

16.6.1.15 display voice sipag

16.6.2.49 vqe-sns-level

Function

Using the **vqe-sns-level** command, you can set the VQE noise suppression value for a SIP AG user.

Using the **undo vqe-sns-level** command, you can restore the default VQE noise suppression value for a SIP AG user.

By default, the VQE noise suppression value of a SIP AG user is 12 dB.

Format

vqe-sns-level *vqe-sns-level*

undo vqe-sns-level

Parameters

Parameter	Description	Value
vqe-sns-level	Specifies a VQE noise suppression value.	The value is an integer that ranges from 6 to 20, in dB.

Views

SIP AG user view

Default Level

2: Configuration level

Usage Guidelines

The **vqe-sns-level** command sets the VQE noise suppression value for a SIP AG user. This command is optional.

Before using the **vqe-sns-level** command, run the **16.6.2.39 sipaguser (Voice View)** command to configure the interface number for the SIP AG user and run

 Copyright © Huawei Technologies Co., Ltd.

the **16.6.2.2 agid (SIP AG user view)** command to configure the SIP AG ID for the SIP AG user.

Example

Set the VQE noise suppression value of a SIP AG user to 10.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sipaguser huawei
[Huawei-voice-sipaguser-huawei] vqe-sns-level 10
```

Related Topics

16.6.1.15 display voice sipag

16.7 H.248 AG Commands

Description

This topic describes H.248 AG parameter setting and user configuration commands.

NOTE

- The following product models support voice functions (such as the PBX, SIP AG, and H.248 AG):
  - AR120 series: AR129CV, AR129CVW, and AR129CGVW-L
  - AR150 series: AR157VW and AR158EVW
  - AR160 series: AR161, AR169FVW, AR169FVW-8S, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR161FV-1P, and AR169FGVW-L
  - AR200 series: AR201VW-P, AR207V, AR207VW, and AR207V-P
  - AR1200 series: AR1220V, AR1220VW, AR1220EV, and AR1220EVW
  - AR2200 series: AR2204, AR2220, AR2220L, AR2220E.
  - AR2240: For the equipped with SRU40, SRU60, SRU80, and SRU100.
  - AR3200 series: For the AR3260 equipped with SRU40, SRU60, SRU80, or SRU100, the same voice mode is set for the active and standby SRUs.

  The AR129CV, AR129CVW, AR169CVW, AR169JFVW-4B4S, AR169JFVW-2S, and AR169CVW-4B4S only support the PBX and SIP AG, but not the H.248 AG.
- When an AR2204, AR2220L, or AR2220E router needs to provide voice services, install a DSP module and a voice subcard in the router. When an AR2220, AR2240, or AR3200 router needs to provide voice services, install a DSP module.
- To provide voice services to POTS users on the AR1200, AR2200, or AR3200, install the 4FXS1FXO, 16FXS, or 32FXS card. The AR1200 does not support the 32FXS card.
- To provide voice services to ISDN phone users on the AR1200, AR2200, or AR3200, install the 2BST card.
- To connect an AR1200, AR2200, or AR3200 router to a TDM PBX through the E1 interface, install the E1T1-M card.
- On the AR169FGVW-L, AR1220EV, and AR1220EVW, the AT0 trunk cannot be connected to the SIP server or SIP trunk.

16.7.1 H.248 AG Parameter Setting Commands

Description

This topic describes H.248 AG parameter setting commands.

16.7.1.1 2833encrypt

Function

The **2833encrypt** command configures the 2833 key supported by an MG interface.

Format

2833encrypt cipher *password-value*

undo 2833encrypt

Parameters

Parameter	Description	Value
cipher *password-value*	Specifies cipher text of a password. **NOTE** You can set password-value only after entering **cipher** and pressing **Enter**.	The value is a string of 1 to 16 characters.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

Set this parameter when you need to configure the 2833 key for the specified MG interface. The 2833 key is used to encrypt signals transmitted using RTP packages that comply with RFC 2833. The same key must be configured on the MG and MGC or on the two MGs that communicate with each other.

Example

Set the 2833 key for an MG interface to **abc123**. Keys are sensitive data. Keep them secure.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] 2833encrypt cipher
please input 2833encrypt (1-16 chars,and "-" indicates the deletion):******
```

16.7.1.2 auth

Function

The **auth** command sets authentication parameters on an MG interface that supports H.248 protocol.

Format

auth { **initial_key** *initial_key* | **auth_mgid** *auth_mgid* }

undo auth { **initial_key** | **auth_mgid** }

Parameters

Parameter	Description	Value
initial_key	Specifies the initial key. A hyphen (-) indicates that the initial key is deleted. Set this parameter when the MG interface supports authentication. Used with the authentication identification, the initial key is used to calculate the digital signature of the MG interface.	The value is a string of 1 to 16 characters. The initial key starting with AH must contain 16 characters.
auth_mgid	Specifies the authentication identification of an MG interface. A hyphen (-) indicates that the identification is deleted. Set this parameter when the MG interface supports authentication. The MG interface calculates the digital signature based on the authentication parameters **initial_key** and **auth_mgid**.	The value is a string of 1 to 16 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- This command can be executed only in H.248 AG view.
- The parameter settings must be the same as those on the MGC.

Example

Set the authentication identification for H.248 AG to **myh248ag** and password to **12345678**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1]auth  auth_mgid myh248ag
[Huawei-voice-h248ag-1]auth initial_key cipher
 please input initialkey (1-16 chars):********
```

16.7.1.3 desc

Function

The **desc** command configures the MG interface description.

Format

desc *description*

undo desc

Parameters

Parameter	Description	Value
description	Specifies the MG interface description. Set this parameter when you need to describe MG interfaces to facilitate the maintenance of different interfaces.	The value is a string of 1 to 32 characters.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

Run this command when you need to describe MG interfaces to facilitate the maintenance of different interfaces. After this command is executed, run the **reset** command to reset the MG interface for the configuration to take effect.

Example

The **desc** command configures the description for a H.248 AG and helps to manage the H.248 AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] desc h248ag
```

16.7.1.4 deviceName

Function

The **deviceName** command configures the device name on an MG interface.

Format

deviceName *device-name*

undo deviceName

Parameters

Parameter	Description	Value
device-name	Specifies the device name of an MG interface. Use this parameter when you need to specify the device name of an MG interface after **MIDType** is set to **deviceName**.	The value is a string of 1 to 64 characters.

Views

H.248 AG view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Use this parameter when you need to specify the device name of an MG interface after **MIDType** is set to **deviceName**

Example

Set the device name of an MG interface to **myag**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] deviceName myag
```

16.7.1.5 digitmap

Function

The **digitmap** command configures user-defined internal call digit map, survival channel digit map, auto redialing digit map, and overload emergency call digit map on an MG interface that supports H.248.

Format

digitmap { **inner** *innerldigitmap* | **emergency** *emergencydigitmap* | **dualdial** *dualdialdigitmap* | **urgent** *urgent-digitmap* }*

undo digitmap {**inner** | **emergency** | **dualdial** | **urgent** }*

Parameters

Parameter	Description	Value
innerldigitmap	Specifies the user-defined internal call digit map (also called local switch digit map). Set this parameter when you need to configure the internal call digit map. The internal call digit map is used to match phone numbers for calls made between internal users on an MG.	The value is a string of 1 to 127 characters. The following characters are allowed: (0123456789.|ABCDEFXx[]TSL)
emergencydigitmap	Specifies the user-defined survival channel digit map. Set this parameter when you need to configure the survival channel digit map.	The value is a string of 1 to 127 characters. The following characters are allowed: (0123456789.|ABCDEFXx[]TSL)

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dualdialdigitmap	Specifies the user-defined auto redialing digit map. Set this parameter when you need to configure the auto redialing digit map. Only one dialing scheme is supported, such as 2xxx. Multiple dialing schemes such as 2xxx|4xxx|6xxx are not supported.	The value is a string of 1 to 14 characters. The following characters are allowed: (0123456789.ABCDEFXx[]TSL)
urgent-digitmap	Specifies the user-defined emergency call digit map used in overload or insufficient bandwidth scenario. Set this parameter when you need to configure the emergency call digit map used in overload or insufficient bandwidth scenario.	The value is a string of 1 to 127 characters. The following characters are allowed: (0123456789.|ABCDEFXx[]TSL)

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- A digitmap is a dialing scheme of the MG interface, used for detecting and reporting dialing events received on a termination.
- When configuring a digit map, ensure that the input characters must be within the related ranges, and comply with the following rules:
  - The inside of the character [] cannot be empty.
  - Character "." cannot follow character "S" or "L".
- You can configure one or more types of digit maps. When configuring a digit map, enter the type of the digit map. If you select dualdial and urgent, it indicates that you configure the auto redialing digit map, emergency call digit map used in overload or insufficient bandwidth scenario at the same time. When you set the digit map, the input characters are case insensitive.
- When you set the digit map, the input characters are case insensitive.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the user-defined survival channel digit map **1xx**, internal call digit map **2xx**, auto redialing digit map **3xx**, and emergency call digit map used in overload or insufficient bandwidth scenario **4xx**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1]digitmap emergency 1xx inner 2xx dualdial 3xx urgent 4xx
```

16.7.1.6 digitmap-timer

Function

The **digitmap-timer** command configures digit map timers.

Format

digitmap-timer { **start** *startvalue* | **short** *shortvalue* | **long** *longvalue* | **duration** *durationvalue* }

undo digitmap-timer { **start** | **short** | **long** | **duration** }

Parameters

Parameter	Description	Value
start *startvalue*	Specifies the duration of the digit map start timer. Set this parameter when you need to configure the duration of the digit map start timer. The digit map start timer applies after a user picks up and before the user dials the first digit. If the duration of the digit map start timer is set to 0, the MG indefinitely waits for the user to dial.	The value is an integer that ranges from 0 to 99. Unit: s Default value: 20

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
short *shortvalue*	Specifies the duration of the digit map short timer. Set this parameter when you need to configure the duration of the digit map short timer. The digit map short timer applies when the digits collected match at least one dialing scheme but may match another dialing scheme when more digits are collected. If the user does not dial any number within the duration of the digit map short timer, the digit map short timer times out and the collected digits that match a dialing scheme are reported. If the user continues to dial within the duration, the MG continues to match the digits collected with dialing schemes. You are advised to use the default value 4s.	The value is an integer that ranges from 1 to 99. Unit: s Default value: 4

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
long *longvalue*	Specifies the duration of the digit map long timer. Set this parameter when you need to configure the duration of the digit map long timer. The digit map long timer applies when the digits collected do not match any dialing scheme. If the user does not dial any number within the duration of the digit map long timer, the digit map long timer times out and the no-match failure is reported. If the user continues to dial within the duration, the MG continues to match the digits collected with dialing schemes. You are advised to use the default value 20s.	The value is an integer that ranges from 1 to 99. Unit: s Default value: 20
duration *durationvalue*	Specifies the duration of the digit map persistence timer. Set this parameter when you need to configure the duration of the digit map persistence timer. The digit map persistence timer protects the digits collected based on the digit map.	The value is an integer that ranges from 100 to 9900. Unit: ms Default value: 3000

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- This command is used to configure the time length of the digitmap duration timer, long timer, short timer, and start timer of an MG interface that supports the H.248 protocol.
- The time length set by using this command for four timers must be shorter than that set on the MGC. Otherwise, the timer time length set on the MGC is adopted.

Example

Set the duration of the digit map start timer to 22, duration of the digit map short timer to 33, duration of the digit map long timer to 55, and duration of the digit map persistence timer to 666.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] digitmap-timer  start 22 short 33 long 55 duration 666
```

16.7.1.7 display voice h248ag

Function

The **display voice h248ag** [*agid* { **running** | **config** }] command displays attribute configurations of an MG interface.

Format

display voice h248ag [*agid* { **running** | **config** }]

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. This parameter is available only in the privilege mode and is mandatory. It specifies the MG interface to be queried.	The value is an integer that ranges from 0 to 16777215.
running	Displays running software parameters of a H248 AG.	-
config	Displays configured software parameters of a H248 AG.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

- When you run this command to query attribute configurations of an MG interface, detailed attribute configurations of the MG interface are displayed. For details about each parameter, see parameter description.
- If an interface attribute is not configured, a hyphen (-) is displayed.

Example

Display attribute configurations of MG interface 0.

```
[huawei-voice]display voice h248ag 0 config

 ---------------------------------------------------
 MGID                            0
 MG Description                     mg0
 MG DomainName                        abcd.com
 Protocol                        H248
 Start Negotiate Version            3
 Profile Negotiation Parameter      Disable
 Profile index                    1:NoProfile("")
 2833Encrypt                        -
 Codetype                         Text
 Transfer Mode                      SCTP
 HeartBeatGenTimer(s)               60
 HeartBeatRetransTimes              3
 HeartBeatRetransTimer(s)           60
 MG signaling IP                  10.71.46.69
 MG signaling Port                 2944
 MG media IP 1                      10.10.1.12
 MG media IP 2                      -
 MIDType                          IP4_ADDR
 DeviceName                         -
 Retrans                         Enable

 Active MGC       MGC Port       :2944          MGC IP1:10.71.46.23
 Active MGC       MGC Port       :2944          MGC IP2:10.71.46.24
 Active MGC       MGC Domain Name:-
 Standby MGC      MGC Port       :2944          MGC IP1:10.71.44.23
 Standby MGC      MGC Port       :2944          MGC IP2:10.71.44.24
 Standby MGC      MGC Domain Name:-
 Stand-Alone-MGC  MGC Port       :2945          MGC IP1:192.168.0.91
 Stand-Alone-MGC  MGC Port       :2945          MGC IP2:-
 ---------------------------------------------------
```

Table 16-129 Description of the display voice h248ag agid config command output

Item	Description
MGID	ID of an MG interface.
MG Description	Description of an MG interface.

Item	Description
MG DomainName	Domain name of an MG interface.
Protocol	Protocol used by an MG interface. The value is **H248** for MG interfaces.
Start Negotiate Version	H.248 protocol version for starting negotiation between the MG and MGC.
Profile Negotiation Parameter	Profile negotiation parameter of an MG interface.
Profile index	Index of the profile used by an MG interface.
2833Encrypt	2833 key configured for an MG interface. The 2833 key used by the MG interface must be the same as that configured on the MGC.
Codetype	Code type supported by an MG interface. The code type used by the MG interface must be the same as that configured on the MGC.
Transfer Mode	Transfer mode supported by an MG interface. The transfer mode used by the MG interface must be the same as that configured on the MGC.
HeartBeatGenTimer(s)	Heartbeat initiation duration on an MG interface, in seconds.
HeartBeatRetransTimes	Heartbeat message retransmission times on an MG interface.
HeartBeatRetransTimer(s)	Heartbeat retransmission interval on an MG interface, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MG signaling IP	Signaling IP address of an MG interface. ● If the signaling IP address is a fixed IP address, the parameter value is the specific IP address. ● If the signaling IP address is obtained using DHCP, the parameter value is **DHCP(vlan x)**, where *x* is the DHCP VLAN ID. ● If the signaling IP address is obtained in dynamic IP address name mode, this parameter is replaced with **MG dynamic signaling IP address name**. The parameter value is the dynamic signaling IP address name. The signaling IP address must exist in the signaling IP address pool.
MG signaling Port	Transport layer protocol port number of an MG interface. The port number configured for an MG interface must be the same as that configured on the MGC.
MG MID IP	MID IP address of an MG interface. If this IP address is configured and the MID type is IP address, this IP address is used as the MID header.
MG media IP1	Media IP address 1 of an MG interface. ● If media IP address 1 is a fixed IP address, the parameter value is the specific IP address. ● If media IP address 1 is obtained using DHCP, the parameter value is **DHCP(vlan x)**, where *x* is the DHCP VLAN ID. ● If media IP address 1 is obtained in dynamic IP address name mode, this parameter is replaced with **Dynamic media IP address 1 name**. The parameter value is the dynamic signaling IP address name. The media IP address must exist in the media IP address pool.
MG media IP2	Media IP address 2 of an MG interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MIDType	H.248 MID type of an MG interface.
DeviceName	Device name of an MG interface.
Active MGC MGC Port	Transport layer protocol port number of the primary MGC. When the transport protocol is SCTP, two transport layer protocol port numbers exist.
Active MGC MGC IP1	IP address 1 of the primary MGC.
Active MGC MGC IP2	IP address 2 of the primary MGC. When the transport protocol is UDP, this IP address is invalid and this parameter is optional. If the IAS_VSP_OVERSCTP feature is discarded, this parameter is unavailable.
Active MGC MGC Domain Name	Domain name of the primary MGC.
Standby MGC MGC Port	Transport layer protocol port number of the standby MGC. When the transport protocol is SCTP, two transport layer protocol port numbers exist.
Standby MGC MGC IP1	IP address 1 of the standby MGC.
Standby MGC MGC IP2	IP address 2 of the standby MGC. When the transport protocol is UDP, this IP address is invalid and this parameter is optional. If the IAS_VSP_OVERSCTP feature is discarded, this parameter is unavailable.
Standby MGC MGC Domain Name	Domain name of the standby MGC.
Retrans	Transaction reliability flag of an MG interface.
Stand-Alone-MGC MGC Port	Transport layer protocol port number of the standalone MGC. When the transport protocol is SCTP, two transport layer protocol port numbers exist.
Stand-Alone-MGC MGC IP1	IP address 1 of the standalone MGC.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Stand-Alone-MGC MGC IP2	IP address 2 of the standalone MGC. When the transport protocol is UDP, this IP address is invalid and this parameter is optional. If the IAS_VSP_OVERSCTP feature is discarded, this parameter is unavailable.

16.7.1.8 display voice h248ag h248stack

Function

The **display voice h248ag** *agid* **h248stack** command displays H.248 protocol stack parameter settings on an MG interface. When you need to display H.248 protocol stack parameter settings on the specified MG interface, run this command.

Format

display voice h248ag *agid* **h248stack** { **MTU** | **format** | **messagesegmentation** | **sdpencodetype** | **securitytype** | **tr** }

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. This parameter is available only in the privilege mode and is mandatory. It specifies the MG interface to be queried. If you do not set this parameter in the H.248 mode, H.248 protocol stack parameter settings on the current MG interface are displayed. In the privilege mode, the specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
MTU	Displays the MTU. Set this parameter when you need to display the MTU on an MG interface.	-
format	Displays the H.248 message format. The formats include long and short. Set this parameter when you need to display the H.248 message format on an MG interface.	-
messagesegmentation	Indicates whether H.248 message packet fragmentation is supported. Set this parameter when you need to check whether packet fragmentation is supported.	-
sdpencodetype	Displays the H.248 protocol stack SDP codec type. The types include text and hex. Set this parameter when you need to display the H.248 protocol stack SDP codec type.	-
securitytype	Displays the H.248 message authentication type. The types include noah, sha1, and md5. Set this parameter when you need to display the H.248 message authentication type.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tr	Displays H.248 protocol stack transaction reliability parameters. For details about each parameter, see parameter description. Set this parameter when you need to display the H.248 protocol stack transaction reliability parameters.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display H.248 protocol stack transaction reliability parameter settings on MG interface 0.

```
<Huawei> system-view
[Huawei] voice
[huawei-voice]display voice h248ag 0 h248stack tr
  -----------------------------------------------
  three way handshake                      : false
  longtimer(units: ms)                     : 30000
  MG provisional response timer(units: ms) : 8000
  MGC provisional response timer(units: ms): 8000
  MG originated pending limit              : 5
  MGC originated pending limit             : 5
  retransfailoption                        : max retransfer times
  maxretranstimes                          : 7
  retransmode                              : auto
  maxretranstimerval(units: ms)            : 4000
  minretranstimerval(units: ms)            : 500
  -----------------------------------------------
```

Table 16-130 Description of the display voice h248ag h248stack tr command output

Item	Description
three way handshake	Whether to proactively send the RESPONSE ACK message in the common three-way handshake scenario.
longtimer(units: ms)	Duration of the long timer, in milliseconds.
MG provisional response timer(units: ms)	Duration of the temporary response timer on the MG, in milliseconds.
MGC provisional response timer(units: ms)	Duration of the temporary response timer on the MGC, in milliseconds.
MG originated pending limit	Limit of times that the transaction reliability MG sends the temporary response.
MGC originated pending limit	Limit of times that the transaction reliability MGC sends the temporary response.
retransfailoption	Retransmission failure option, indicating whether the retransmission failure is determined by the maximum retransmission times or retransmission duration.
maxretranstimes	Maximum retransmission times.
retransmode	Retransmission mode. The options include **auto** and **fixed**.
maxretranstimerval(units: ms)	Maximum duration of the retransmission timer.
minretranstimerval(units: ms)	Minimum duration of the retransmission timer.

16.7.1.9 display voice h248ag auth

Function

The **display voice h248ag auth** command displays the authentication configuration of an MG interface that supports H.248. When you need to display the authentication configuration of the specified MG interface, run this command.

Format

display voice h248ag *agid* **auth**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. It specifies the MG interface to be queried.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the authentication configuration of MG interface 0 that supports H.248.

```
[Huawei-voice]display voice h248ag 0 auth
 [AUTH_PARA config]
  Initial Key    : ******
  Auth MGid      : AG
  Algorithm      : MD5
```

Table 16-131 Description of the display voice h248ag auth command output

Item	Description
Initial Key	Initial key configured for an MG interface.
Auth MGid	Authentication MG interface ID configured for an MG interface.
Algorithm	Encryption algorithm used by an MG interface.

16.7.1.10 display voice h248ag digitmap

Function

The **display voice h248ag** *agid* **digitmap** command displays the digit map configuration of an MG interface that supports H.248. When you need to display the digit map configuration of the specified MG interface, run this command.

Format

display voice h248ag *agid* **digitmap**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the digit map configuration of MG interface 0 that supports H.248.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]display voice h248ag 0 digitmap
  ------------------------------------------------------------------------------
  Inner digitmap                                  : 1xx
  Emergency digitmap                                : 119x
  Urgent digitmap (for overload or bandwidth restrict)   : 4xxx
  Dualdial digitmap for card service                : 00xxx
  ------------------------------------------------------------------------------
```

Table 16-132 Description of the display voice h248ag digitmap command output

Item	Description
Inner digitmap	Internal call digit map.
Emergency digitmap	Survival channel digit map.
Urgent digitmap (for overload or bandwidth restrict)	Emergency call digit map used in overload or insufficient bandwidth scenario.
Dualdial digitmap for card service	Auto redialing digit map for card services.

 Copyright © Huawei Technologies Co., Ltd.

16.7.1.11 display voice h248ag digitmap-timer

Function

The **display voice h248ag** *agid* **digitmap-timer** command displays the digit map persistence timer, long timer, short timer, and start timer durations configured on an MG interface that supports H.248. When you need to display the durations of the preceding timers configured on the specified MG interface, run this command.

Format

display voice h248ag *agid* **digitmap-timer**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display timer durations of MG interface 0 that supports H.248.

```
<Huawei>display voice h248ag 0 digitmap-timer
  ----------------------------------------------------
  Start     Timer length(s)  : 20
  Short     Timer length(s)  : 4
  Long      Timer length(s)  : 20
  Duration  Timer length(ms) : 3000
  ----------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-133 Description of the display voice h248ag agid digitmap-timer command output

Item	Description
Start Timer length(s)	Duration of the digit map start timer, in seconds.
Short Timer length(s)	Duration of the digit map short timer, in seconds.
Long Timer length(s)	Duration of the digit map long timer, in seconds.
Duration Timer length(ms)	Duration of the digit map persistence timer, in milliseconds.

16.7.1.12 display voice h248ag h248profile

Function

The **display voice h248ag** *agid* **h248profile** command displays profile information.

Format

display voice h248ag *agid* **h248profile** [**list** | **detail** | **profile-index** *indexvalue* | **para** *paravalue*]

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.
list	Displays all profile names instead of profile parameters.	-
detail	Displays detailed information about all profile parameters. If the **detail** parameter is not set, only information about the parameters different from the default profile is displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
profile-index *indexvalue*	Specifies the index of an MG interface profile. This parameter is optional. Set this parameter when you need to specify the profile used by the specified MG interface. The value 0 indicates that the profile custom template is used. The values 1 to 7 indicates that system built-in profiles are used, where the value 1 indicates that the default profile is used.	The value is an integer that ranges from 0 to 7. Default value: 0
para *paravalue*	Displays the profile parameter with the specified ID.	The value is an integer that ranges from 0 to 4294967295.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If the **detail** parameter is not set, only information about the parameters different from the default profile is displayed.

Example

Display the profile list on H.248 interface 0.

```
<Huawei>display voice h248ag 0 h248profile list
 ---------------------------------------------
 Profile-Index Profile-Name("Negotiation-Name")
 ---------------------------------------------
 0             CustomizingProfileTemplet("")
 1             NoProfile("")
 2             BT_AGW/3("BT_AGW/3")
 3             FT_AGW/2("FT_AGW/2")
 4             KPN_AGW/1("KPN_AGW/1")
 5             PCCW_AGW/1("PCCW_AGW/1")
 6             ZTE_AGW/1("ZTE_AGW/1")
 7             BELL_AGW/1("BELL_AGW/1")
 ---------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-134 Description of the display voice h248ag agid h248profile command output

Item	Description
Profile-Name	Name of an H.248 template.
Profile-Name("Negotiation-Name")	Name of an H.248 template.
Profile-Negotiation-Name	ID of an MG interface.
Profile-Index	Terminal ID.

16.7.1.13 display voice h248ag h248statistics

Function

The **display voice h248ag** *agid* **h248statistics** command displays statistical information about an MG interface that supports H.248. When you need to display statistical information about the specified MG interface, such as the numbers of transactions received and sent, number of H.248 messages received, and number of voice playing signals, run this command.

Format

display voice h248ag *agid* **h248statistics**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command on an MG interface that is not reset. You must first run the **reset** command to reset the MG interface.

Example

Display statistical information about MG interface 0 that supports H.248.

```
<Huawei>display voice h248ag 0 h248statistics
  -------------------------------------------------------
  H248 Messages Sent                          2
  H248 Messages Re-Sent                       0
  Transaction Requests sent                   2
  Transaction Replies sent                    0
  Transactions Re-Sent                        0
  H248 Messages Received                      1
  Transaction Requests Received               0
  Transaction Replies Received                1
  Dial Tone Signals Received                  0
  Busy Tone Signals Received                  0
  Ringback Tone Signals Received              0
  Howler Tone Signals Received                0
  -------------------------------------------------------
```

Table 16-135 Description of the display voice h248ag h248statistics command output

Item	Description
H248 Messages Sent	Number of H.248 messages sent by an MG interface. If the value is 0, the MG interface is abnormal.
H248 Messages Re-Sent	Number of H.248 messages resent by an MG interface. If the value is not 0, the MG interface has resent messages because it does not receive any response message from the peer device in a period of time and considers that the message sending failure occurs. You must determine whether the number of resent messages meets network quality requirements.
Transaction Requests sent	Number of transaction requests sent by an MG interface.
Transaction Replies sent	Number of transaction responses sent by an MG interface. The number of transaction responses sent by the MG interface must be the same as that of transaction requests sent by the MG interface; otherwise, the communication between the MG and MGC is abnormal, and packet loss occurs. You must determine whether the number of lost packets meets network quality requirements.
Transactions Re-Sent	Number of transactions resent by an MG interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
H248 Messages Received	Number of H.248 messages received by an MG interface. The number of H.248 messages received by an MG interface must be the same as that of H.248 messages sent by the MG interface; otherwise, the communication between the MG and MGC is abnormal, and packet loss occurs. You must determine whether the number of lost packets meets network quality requirements.
Transaction Requests Received	Number of transaction requests received by an MG interface.
Transaction Replies Received	Number of transaction responses received by an MG interface. The number of transaction responses received by the MG interface must be the same as that of transaction requests received by the MG interface; otherwise, the communication between the MG and MGC is abnormal, and packet loss occurs. You must determine whether the number of lost packets meets network quality requirements.
Dial Tone Signals Received	Total number of dial tone signals received by an MG interface in a period of time.
Busy Tone Signals Received	Total number of busy tone signals received by an MG interface in a period of time.
Ringback Tone Signals Received	Total number of ring back tone signals received by an MG interface in a period of time.
Howler Tone Signals Received	Total number of howler tone signals received by an MG interface in a period of time.

16.7.1.14 display voice h248ag mg-software

Function

The **display voice h248ag** *agid* **mg-software parameter** command displays control point settings on an MG interface that supports H.248.

Format

display voice h248ag *agid* **mg-software** [*name*]

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.
name	Specifies the control point name. Set this parameter when you need to display the setting of the specified control point. If this parameter is not set, settings of all control points are displayed.	The value is an integer that ranges from 0 to 37.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If you do not enter the control point name index, settings of all control points are displayed.

The following table lists MG interface control points.

Parameter	Description	Value
0	System reserved.	-
1	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
2	Indicates whether an MG interface supports multihoming. Set this parameter when you need to determine whether an MG interface supports multihoming. This parameter can be set only when the MG interface is in Local Closed state. If multihoming is not supported and the MG interface fails to register with the primary MGC, the MG interface will not register with the standby or standalone MGC no matter whether the standby or standalone MGC is configured. If multihoming is supported and a primary MGC fault occurs when the current MG interface is registered with the primary MGC, the MG interface registers with the standby MGC and standalone MGC cyclically. ● If the standby MGC runs properly, the MG interface switches to the standby MGC. ● If the standby MGC is faulty or not configured and the standalone MGC runs properly, the MG interface switches to the standalone MGC. Note: When the MG interface switches to the standalone MGC, the interface restarts	The value can be 0, 1, or 2. ● 0: Multihoming is not supported. ● 1: Multihoming is supported while automatic switchover is not. ● 2: Both multihoming and automatic switchover are supported. Default value: 0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	and services will be interrupted. If the MG interface supports both multihoming and automatic switchover, the MG interface functions as follows: ● If the MG interface is registered with the standby MGC and the primary MGC recovers, the MG interface automatically switches to the primary MGC. ● If the MG interface is registered with the standalone MGC and the primary or standby MGC recovers, the MG interface automatically switches to the primary or standby MGC. Note: When the MG interface switches to the primary or standby MGC from the standalone MGC, the interface restarts and services will be interrupted. If the MG interface supports multihoming but does not support automatic switchover, the MGC will not automatically switch to the primary MGC from the standby or standalone MGC when the primary MGC recovers. You can run the **mgc switch** command to	

Parameter	Description	Value
	forcibly switch the MG interface to the primary MGC. If the MG interface supports multihoming, you can run the **mgc switch** command to forcibly switch the MG interface: ● Between the primary and standby MGCs. ● From the standalone MGC to the primary or standby MGC if the MG interface registers with the standalone MGC.	
3	System reserved.	-
4	Indicates whether wildcard characters are used during MG interface registration. Set this parameter when you need to determine whether wildcard characters are used during MG interface registration. If wildcard characters are used, all terminals on the MG interface are registered with the MGC using one message, which reduces the number of messages sent between the MG interface and MGC. If wildcard characters are not used, all terminals on the MG interface register with the MGC one by one. The registration mode where wildcard characters are not used is also called single-endpoint registration.	The value can be 0 or 1. ● 0: used. ● 1: not used. Default value: 0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
5	System reserved.	-
6	Indicates whether an MG interface supports device authentication. Set this parameter when you need to determine whether an MG interface supports device authentication. After enabling device authentication support, you can run the **auth** command to set authentication parameters and run the **reset** command to reset the MG interface. After the configuration, the MGC manages the MG device security to prevent unauthorized devices from registering with the MGC. Note: When the MG interface is reset, services may be interrupted.	The value is an integer that ranges from 0 to 1. ● 0: supported. ● 1: not supported. Default value: 1
7	Indicates whether an MG interface supports the security header. Set this parameter when you need to determine whether an MG interface supports the security header. After enabling security header support, you can run the **auth** command to set authentication parameters and run the **reset** command to reset the MG interface. After the configuration, the MGC manages the MG device security to ensure data integrity.	The value is an integer that ranges from 0 to 1. ● 0: supported. ● 1: not supported. Default value: 1

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
8	System reserved.	-
9	System reserved.	-
10	System reserved.	-
11	Indicates whether an MG interface supports local switch. Set this parameter when you need to determine whether an MG interface supports local switch. If the MG interface supports local switch and the MG is disconnected from the MGC, users on the MG can still make calls.	The value is an integer that ranges from 0 to 3. ● 0: No call is allowed. ● 1: Only internal calls are allowed. ● 2: Only survival calls are allowed. ● 3: All calls are allowed. Default value: 0
12	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
13	Digit map match scheme used by an MG interface. Set this parameter when you need to configure the digit map match scheme used by an MG interface. In the shortest match scheme, the MG interface reports collected digits immediately when they match a dialing scheme. In the longest match scheme, the MG interface does not report collected digits immediately when they match a dialing scheme. Instead, the MG interface continues to collect digits and match collected digits with dialing schemes if the user dials any numbers within the short timer duration (4s by default), and reports collected digits only when the short timer times out. In the self-adaptive match scheme, the MG interface checks digit map sub-schemes to automatically determine whether to use the shortest or longest match scheme. You can run the **digitmap-timer** command to configure digit map timer durations.	The value is an integer that ranges from 0 to 3. ● 0: based on protocol requirements. ● 1: longest match. ● 2: shortest match. ● 3: self-adaptive match. Default value: 2
14	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
15	Indicates whether an MG interface filters media stream source ports. Set this parameter when you need to determine whether an MG interface filters media stream source ports. When the media stream source port filtering function is used, the MG interface receives media stream only from specified ports.	The value is an integer that ranges from 0 to 1. ● 0: not filtered. ● 1: filtered. Default value: 0
16	Duration of the media stream source port filtering timer. If the media stream source port filtering function is disabled, the MG port starts the timer when media streams are received. If the command for enabling the media stream source port filtering function is not received within the timer duration, the timer times out and the media stream source port filtering function is automatically enabled.	The value is an integer that ranges from 1 to 30, in seconds. Default value: 5
17	System reserved.	-
18	System reserved.	-
19	System reserved.	-
20	System reserved.	-
21	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
22	Type of the tone that the MG plays to users when the MG is disconnected from the MGC.	The value is an integer that ranges from 0 to 2. ● 0: busy tone. ● 1: congestion tone. ● 2: voice announcement. Default value: 0
23	Duration of the port status synchronization timer. When a remotely blocked port receives signaling from the MGC, the device determines whether to directly update the port status or initiate port registration to the MGC. If the device initiates port registration, the device initiates port registration again after the port status synchronization timer duration. This parameter is invalid for RTP terminals.	The value is an integer that ranges from 0 to 120, in seconds. Default value: 35

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
24	Maximum RTP terminal index. An RTP terminal is a temporary terminal, which is a unique terminal type for an MG interface that supports H.248. A temporary terminal represents temporary information streams and exists only when the MG uses these information streams. For example, when establishing media streams, the MG interface uses remote MGC information and a temporary terminal exists. The maximum number of RTP terminals on the MGC must be the same as that on the MG.	The value is an integer. The value range depends on product specifications.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
25	Maximum random number for the avalanche prevention mechanism. When the system is reset, all H.248 interfaces on the device register with the MGC again. When all interfaces initiate registration simultaneously, packet conflicts will occur and the MGC may break down. The avalanche prevention mechanism can help avoid this situation. After the maximum random number for the avalanche prevention mechanism is configured, the system uses an internal algorithm to generate the duration after which an H.248 interface can initiate registration. The duration after which an H.248 interface can initiate registration is greater than the sum of the system internal base number and the maximum random number for the avalanche prevention mechanism.	The value is an integer that ranges from 30000 to 300000, in milliseconds. Default value: 60000
26	Local blocking tone type. When the MG interface is faulty or you run the **endservice** command, the MG interface enters the local blocking state. This parameter specifies the type of the tone played in local blocking state.	The value is an integer that ranges from 0 to 4. ● 0: busy tone. ● 1: congestion tone. ● 2: muted. ● 3: custom tone 1. ● 4: custom tone 2. Default value: 0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
27	Remote blocking tone type. When the MGC does not respond and a response error occurs, the MG interface enters the remote blocking state. This parameter specifies the type of the tone played in remote blocking state.	The value is an integer that ranges from 0 to 4. ● 0: busy tone. ● 1: congestion tone. ● 2: muted. ● 3: custom tone 1. ● 4: custom tone 2. Default value: 0
28	Duration of the howler tone. If a user does not hang up the phone after a call ends or picks up but forgets to hang up, the howler tone is played when the busy tone timer times out. After the duration of the howler tone, the port is locked. In this case, the phone cannot be called. The port is automatically unlocked when the user hangs up the phone.	The value is an integer that ranges from 1 to 65535, in seconds. Default value: 60
29	Duration of message prompt tone. When a user who has enabled the message prompt tone service picks up the phone, the MGC delivers the message prompt tone (similar in delivering the dial tone).	The value is an integer that ranges from 1 to 60000, in seconds. Default value: 3
30	Duration for generating the long call alarm. If the long call alarm is enabled and the duration of a call exceeds that for generating the long call alarm, the system generates the H.248 user long call event.	The value is an integer that ranges from 1 to 65535, in minutes. Default value: 60

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
31	Indicates whether the long call alarm is enabled.	The value is an integer that ranges from 0 to 1. ● 0: enabled. ● 1: disabled. Default value: 1
32	Minimum automatic registration interval for a remotely blocked port. When the interface that a port belongs to functions properly but the port is blocked remotely because the MGC does not respond and a response error occurs, the port automatically initiates registration requests to the MGC based on the interval specified by this parameter.	The value is an integer that ranges from 0 to 60000. The value 0 indicates that the port does not automatically register with the MGC. Unit: s Default value: 1800
33	Indicates whether the heartbeat function is disabled on an MG interface. Generally, the heartbeat function is enabled for the MG to keep the connection with the MGC. In a few cases, some MGCs cannot recognize the heartbeat message sent by the MG interface, and the heartbeat function is disabled. The MGC periodically send the Notify message to keep the connection.	The value is an integer that ranges from 0 to 1. ● 0: disabled. ● 1: enabled. Default value: 1
34	Indicates whether the MG needs to proactively establish or tear links for BRA users when ISDN ports are in service or out of service due to the MGC.	The value is an integer that ranges from 0 to 1. ● 0: yes. ● 1: no. Default value: 0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
35	Mode in which an ISDN port enters the in-service or out-of-service state. ● If the wildcard mode is supported, the ISDN report only one in-service or out-of-service message. This reduces the number of messages sent between the MG interface and MGC. ● If the single-channel mode is supported, each channel reports an in-service or out-of-service message. ● If both the wildcard and single-channel modes are supported, the ISDN port selects a mode as required.	The value is an integer that ranges from 0 to 2. ● 0: Both the wildcard and single-channel modes are supported. ● 1: Only the single-channel mode is supported. ● 2: Only the wildcard mode is supported. Default value: 1
36	Interval for sending the registration message when an MG interface switches between multiple MGCs. Set this parameter when you need to configure the interval for sending the registration message when an MG interface switches among the primary, standby, and standalone MGCs.	The value is an integer that ranges from 1 to 1800, in seconds. Default value: 40
37	Indicates whether to enable the function of converting pulse signals to DTMF signals. Set this parameter when you need to convert pulse signals to DTMF signals for transmission.	The value is an integer that ranges from 0 to 1. ● 0: enabled. ● 1: disabled. Default value: 1

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the parameter for determining whether wildcard characters are used during the registration of MG interface 0.

```
<Huawei>display voice h248ag 0 mg-software 4
  -----------------------------------------------
  Interface Id:0          para index:4   value:0
  -----------------------------------------------
 APPENDIX:
  -----------------------------------------------
   Interface software parameter name:
   4: Whether MG uses wildcard in registration
      0: Yes
      1: No
```

Table 16-136 Description of the display voice h248ag mg-software command output

Item	Description
Interface Id	ID of interface.
para index	Index of parameter.
value	Value.
APPENDIX	Appendix information.
Interface software parameter name	The name if interface software parameter.
4: Whether MG uses wildcard in registration	Indicates whether wildcard characters are used during MG interface registration. ● 0: used ● 1: not used

16.7.1.15 display voice h248ag standalone

Function

The **display voice h248ag** *agid* **standalone** command displays local switch parameter settings. When you need to display dial tone, ringing, and busy tone durations, run this command.

Format

display voice h248ag *agid* **standalone**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display local switch parameter settings on MG interface 0.

```
<Huawei>display voice h248ag 0 standalone
  ------------------------------------------------------------------------------
  System stand alone para of timer for dial tone :10 (s)
  System stand alone para of timer for busy tone :40 (s)
  System stand alone para of timer for ring      :50 (s)
  ------------------------------------------------------------------------------
```

Table 16-137 Description of the display voice h248ag standalone command output

Item	Description
System stand alone para of timer for dial tone	Duration of the local switch dial tone timer.
System stand alone para of timer for busy tone	Duration of the local switch busy tone timer.
System stand alone para of timer for ring	Duration of the local switch ringing timer.

16.7.1.16 display voice h248ag tid-format

Function

The **display voice h248ag** *agid* **tid-format** command displays the prefix and TID template used by each terminal on one or all MG interfaces. When you need to

display the prefix and TID template used by each terminal on one or all MG interfaces, run this command.

Format

display voice h248ag *agid* **tid-format**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

The TID template configured for an MG interface takes effect only when the MG interface is reset. Therefore, the TID template currently used by an MG interface may be different from that configured for the MG interface.

Example

Display the prefix and TID template used by each terminal on MG interface 0.

```
<Huawei>display voice h248ag 0 tid-format
  ----------------------------------------------------------
  MGID      term-type     template-index  prefix
  ----------------------------------------------------------
  0         RTP           1               A
  0         PSTN           2               A
  0         BRA            2               A
  0         PRA            2               A
  0         R2            2               r2/
  ----------------------------------------------------------
```

Table 16-138 Description of the display voice h248ag tid-format command output

Item	Description
MGID	ID of an MG interface.
term-type	Terminal type.
template-index	TID template index.

Item	Description
prefix	Terminal prefix.

16.7.1.17 display voice h248ag mg-ringmode attribute

Function

The **display voice h248ag** *agid* **mg-ringmode attribute** command displays ringing mode mapping records on an MG interface.

Format

display voice h248ag *agid* **mg-ringmode attribute** [*mgcpara*]

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.
mgcpara	Specifies the peer parameter identification delivered by the MGC. This parameter is optional. Set this parameter when you need to display the ringing mapping based on the specified peer parameter.	The value is an integer that ranges from 0 to 15.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

To display the ringing mode based on the specified peer parameter, you must set *mgcpara*. To display all ringing modes on an MG interface, you do not need to set *mgcpara*.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display ringing mode mapping records on all MG interfaces.

```
[huawei-voice]display voice h248ag 0 mg-ringmode attribute
-------------------------------------------------------
  MGID   PeerPara   CadenceRing   InitialRing
-------------------------------------------------------
  0      0          0             4
-------------------------------------------------------
```

Table 16-139 Description of the display voice h248ag mg-ringmode attribute command output

Item	Description
MGID	ID of an MG interface.
PeerPara	Peer parameter identification delivered by the MGC. If no peer parameter identifier is delivered by the MGC, the **MgcPara** parameter delivered is 1.
CadenceRing	Cadence ringing type.
InitialRing	Initial ringing type.

16.7.1.18 display voice h248ag mg-ringmode default-mgcpara

Function

The **display voice h248ag** *agid* **mg-ringmode default-mgcpara** command displays the default ringing mode of an MG interface.

Format

display voice h248ag *agid* **mg-ringmode default-mgcpara**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. It specifies the MG interface to be queried.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display the default ringing mode of MG interface 0.

```
<huawei>display voice h248ag 0 mg-ringmode default-mgcpara
  -------------------------------------------------------
  MGID       Ring-Default-Mgcpara   Mwi-Default-Mgcpara
  -------------------------------------------------------
  0          1                      2
  -------------------------------------------------------
```

Table 16-140 Description of the display voice h248ag mg-ringmode default-mgcpara command output

Item	Description
MGID	ID of an MG interface.
Ring-Default-Mgcpara	Peer parameter identification of default ringing.
Mwi-Default-Mgcpara	Peer parameter identification of MWI ringing.

16.7.1.19 display voice h248ag sctp protocol

Function

The **display voice h248ag** *agid* **sctp protocol** command displays SCTP protocol stack parameter settings on an MG interface. When you need to display SCTP protocol stack parameter settings that are currently used or have been configured on an MG interface, run this command.

Format

display voice h248ag *agid* **sctp protocol** { **running** | **config** }

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

Parameter	Description	Value
running	Displays SCTP protocol stack parameter settings that are currently used by an MG interface.	-
config	Displays SCTP protocol stack parameter settings that have been configured for an MG interface in the database. (These parameter settings may not take effect.)	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display SCTP protocol stack parameter settings on MG interface 0.

```
<Huawei>display voice h248ag agid sctp protocol config
  ----------------------------------------
  In streams              : 33
  Out streams             : 33
  Minimum rto value       : 1000ms
  Maximum rto value       : 60000ms
  Initial rto value       : 1000ms
  Rto alpha parameter     : 12%
  Rto beta parameter      : 25%
  Heartbeat interval      : 30000ms
  Valid cookie lifetime   : 60000ms
  Maximum init retrans    : 8
  Association maxretrans : 10
  Path maximum retrans    : 5
  No congestion level     : 40%
  Low congestion level    : 60%
  High congestion level   : 80%
  Send checksum           : yes
  Receive checksum        : yes
  Checksum arithmetic     : CRC32
  ----------------------------------------
```

Table 16-141 Description of the display voice h248ag sctp-protocol command output

Item	Description
In streams	Number of input SCTP streams.
Out streams	Number of output SCTP streams.
Minimum rto value	Minimum retransmission timeout duration.
Maximum rto value	Maximum retransmission timeout duration.
Initial rto value	Initial value of the retransmission timeout duration.
Valid cookie lifetime	Life cycle of the valid cookie.
Heartbeat interval	Heartbeat interval.
Maximum init retrans	Maximum init message retransmission times.
Rto alpha parameter	Retransmission timeout duration α factor.
Rto beta parameter	Retransmission timeout duration β factor.
Association maxretrans	Maximum association retransmission times.
Path maximum retrans	Maximum route retransmission times.
No congestion level	Non-congestion level.
Low congestion level	Low-congestion level.
High congestion level	High-congestion level.
Send checksum	Whether to send the checksum in a message. The options are as follows: ● yes ● no
Receive checksum	Whether to receive the checksum in a message. The options are as follows: ● yes ● no
Checksum arithmetic	Checksum algorithm.

 Copyright © Huawei Technologies Co., Ltd.

16.7.1.20 display voice h248ag sctp association statistics

Function

The **display voice h248ag** *agid* **sctp association statistics** command displays SCTP association statistics on an MG interface. An association refers to a logical channel for transmitting data between two SCTP endpoints. The channel is established using the four-way handshake mechanism specified in SCTP. When you need to display SCTP association statistics on an MG interface, run this command.

Format

display voice h248ag *agid* **sctp association statistics**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command can be executed successfully only when the transport protocol used by the MG interface is SCTP and an association exists.

Example

Display SCTP association statistics on MG interface 0.

```
<Huawei> display voice h248ag 0 sctp association statistics
 ---------------------------------------------
 Association ID                  : 4
 Times of T1 timer expires       : 0
 Times of T2 timer expires       : 0
 Retrans data chunks             : 0
 Retrans chunks                  : 4
 Sent data chunks                : 426
 Received data chunks            : 874
 Received sctp packets           : 876
 Received error sctp packets     : 0
 ---------------------------------------------
```

Table 16-142 Description of the display voice h248ag agid sctp-association-statistics command output

Item	Description
Association ID	SCTP association ID.
Times of T1 timer expires	Times that the T1 timer times out.
Times of T2 timer expires	Times that the T2 timer times out.
Retrans data chunks	Association data chunk retransmission times.
Retrans chunks	Number of sent association data chunks.
Sent data chunks	Number of sent data chunks.
Received data chunks	Number of received data chunks.
Received sctp packets	Number of received SCTP packets.
Received error sctp packets	Number of received error SCTP packets.

16.7.1.21 display voice h248ag sctp association info

Function

The **display voice h248ag** *agid* **sctp association info** command displays SCTP association information about an MG interface. An association refers to a logical channel for transmitting data between two SCTP endpoints. The channel is established using the four-way handshake mechanism specified in SCTP. When you need to display SCTP association information about an MG interface, run this command.

Format

display voice h248ag *agid* **sctp association info**

Parameters

Parameter	Description	Value
agid	Specifies the MG interface ID. The specified MG interface must exist in the system.	The value is an integer that ranges from 0 to 16777215.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command can be executed successfully only when the transport protocol used by the MG interface is SCTP and an association exists.

Example

Display the SCTP association information about MG interface 0 that supports H.248.

```
<Huawei>display voice h248ag 0 sctp association info
  ---------------------------------------------
  Association ID                  : 10
  Association state               : established
  Association type                : client
  Application ID                  : 1
  Local port                      : 9901
  Remote port                     : 9900
  Local IP address                : 10.144.70.50
  Remote active IP address        : 10.144.82.114
  Local Received window           : 251500
  Remote Received window          : 65536
  Total unfirm data chunks        : 0
  Remote IP address 1             : 10.144.82.114
  Remote IP 1 state               : active
  Waiting ack data chunks         : 0
  Congestion window               : 6000
  Outstanding data chunks         : 0
  Retransmission time-out         : 1000
  Smoothed round-trip time        : 24ms
  Round-trip time variation       : 34ms
  Whether allow HB                : yes
  ---------------------------------------------
```

Table 16-143 Description of the display voice h248ag agid association info command output

Item	Description
Association ID	SCTP association ID.
Association state	SCTP association status.
Association type	SCTP association type, including the client and server.
Application ID	Upper-level user ID.
Local port	Local port corresponding to the SCTP association.

Item	Description
Remote port	Remote port corresponding to the SCTP association.
Local IP address	Local IP address corresponding to the SCTP association.
Remote active IP address	Remote primary IP address corresponding to the SCTP association.
Local Received window	Local receive window size.
Remote Received window	Remote receive window size.
Total unfirm data chunks	Number of unconfirmed data chunks.
Remote IP address 1	Remote IP address 1.
Remote IP 1 state	Current status of remote IP address 1.
Waiting ack data chunks	Number of data chunks waiting for the peer end to acknowledge.
Congestion window	Congestion window size.
Outstanding data chunks	Number of unconfirmed data chunks on the path.
Retransmission time-out	Retransmission timeout duration.
Smoothed round-trip time	Average round-trip time of the path.
Round-trip time variation	Average round-trip time variation of the path.
Whether allow HB	Whether the address can send heartbeat messages.

16.7.1.22 display voice h248ag mg-ringmode default-ringpara

Function

The **display voice h248ag** *agid* **mg-ringmode default-ringpara** command displays the default short ringing and advice of charge at the end of conversation (AOCE) ringing type configuration on the specified MG interface.

Format

display voice h248ag *agid* **mg-ringmode default-ringpara**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
agid	Specifies the MG interface to be queried. This parameter is available only in the privilege mode and is mandatory.	The value is an integer that ranges from 0 to 16777215.

Views

H.248 AG interface view

Default Level

2: Configuration level

Usage Guidelines

This command displays the default short ringing and AOCE ringing type configuration on the specified MG interface.

Example

Display the default short ringing and AOCE ringing type configuration on MG interface 0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]h248ag 0
[Huawei-voice-h248ag-0]display voice h248ag 0 mg-ringmode default-ringpara
  -------------------------------------------------------
  MGID       Short-Ring   AOCE-Ring
  -------------------------------------------------------
  0          12           4
  -------------------------------------------------------
```

Table 16-144 Description of the display voice h248ag mg-ringmode default-ringpara command output

Item	Description
MGID	ID of an MG interface.
Short-Ring	Short ringing type.
AOCE-Ring	AOCE ringing type.

16.7.1.23 display voice sctp version

Function

The **display voice sctp version** command displays the SCTP version information.

Format

display voice sctp version

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the SCTP version information.

```
<Huawei> display voice sctp version
  ------------------------------------------------------------------------
 Sctp protocol version : VPP V300R003C18T034 (SCTP) Suse10Sp01 Gcc_Suse10 ASAU
 Feb 24 2013 07:44:20

 ------------------------------------------------------------------------
 Service status          : Idle
```

16.7.1.24 domainName

Function

The **domainname** command configures the domain name of the device where an MG interface is located.

Format

domainname *domainname*

Parameters

Parameter	Description	Value
domainname	Specifies the domain name of the device where an MG interface is located when **MIDType** is set to **domainName**.	The value is a string of 1 to 64 characters. A hyphen (-) indicates that the domain name is deleted.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command sets the **domaninName** attribute of an MG interface that supports H.248. You must run this command when you need to configure the **domaninName** attribute after adding an interface or modify the **domaninName** attribute of an existing MG interface. After this command is executed successfully, you must run the **reset** command to reset the MG interface for the attribute to take effect.

Example

Configure the domain name to abc.com.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 0
[Huawei-voice-h248ag-0] domainName abc.com
```

16.7.1.25 h248profile

Function

The **h248profile** command configures a user-defined profile for the MG interface on an H.248 interface.

The **undo h248profile** command deletes a user-defined profile for the MG interface on an H.248 interface.

Format

h248profile { **profile-name** *profile-name* | **profile-negotiation-name** *profile-negotiation-name* | **para** *para-no para-value* }

undo h248profile { **profile-name** | **profile-negotiation-name** | **para** *para-no para-value* }

Parameters

Parameter	Description	Value
profile-name	Specified the name of a user-defined profile. This parameter is optional. Use this parameter when you need to modify the name of the user-defined profile on an H.248 interface.	The value is a string of 1-67 characters.
profile-negotiation-name	Specifies the negotiation name of a user-defined profile. This parameter is optional. Use this parameter when you need to modify the negotiation name of the user-defined profile on an H.248 interface.	The value is a string of 1-67 characters.
para-no para-value	Specifies the value of a parameter for a user-defined profile. This parameter is optional. Use this parameter when you need to change the value of a parameter for the user-defined profile on an H.248 interface.	para-no: numeral type. Value range: 0-255 para-value: numeral type. Value range: 0-4294967295

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

Before running the **h248profile modify** command, run the **profile-index 0** to set a profile to the user-defined profile.

After the configuration is complete, run the **reset** command for the configuration to take effect.

Example

Change the value of the second parameter in the user-defined profile on an H.248 interface to 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[huawei-voice-h248ag-1] h248profile modify para 2 2
```

16.7.1.26 h248stack format

Function

The **h248stack format** command configures the protocol stack message format.

Format

h248stack format *format*

undo h248stack format

Parameters

Parameter	Description	Value
format	Specifies the H.248 message format. Set this parameter when you need to configure the H.248 message format. The value **short** indicates the short message format, where commands and descriptors are in abbreviated form, such as **A** for the **ADD** command. The value **long** indicates the long message format, where commands are in complete form.	The value can be **short** or **long**. Default value: short

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the protocol stack message format.

Example

Configure the H.248 message format to **short**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] h248stack format short
```

16.7.1.27 h248stack messagesegmentation

Function

The **h248stack messagesegmentation** command configures the protocol stack packet fragmentation flag.

Format

h248stack messagesegmentation *messagesegmentation*

Undo h248stack messagesegmentation

Parameters

Parameter	Description	Value
messagesegmentation *messagesegmentation*	Specifies the packet fragmentation flag. Set this parameter when you need to enable or disable packet fragmentation.	The value can be **support** or **notsupport**. Default value: support

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the protocol stack packet fragmentation flag.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the packet fragmentation flag to **support**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] h248stack messagesegmentation support
```

16.7.1.28 h248stack MTU

Function

The **h248stack MTU** command configures the protocol stack maximum transmission unit (MTU).

Format

h248stack MTU *mtu*

undo h248stack MTU

Parameters

Parameter	Description	Value
mtu	Specifies the MTU. Set this parameter when you need to configure the MTU.	The value is an integer that ranges from 1 to 5000. Unit: byte Default value: 1500

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the protocol stack maximum transmission unit (MTU).

Example

Set the protocol stack MTU on an H.248 interface to 2000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] h248stack MTU 2000
```

 Copyright © Huawei Technologies Co., Ltd.

16.7.1.29 h248stack sdpencodetype

Function

The **h248stack sdpencodetype** command configures the SDP codec type on an MG interface.

Format

h248stack sdpencodetype *sdpencodetypeval*

undo h248stack sdpencodetype

Parameters

Parameter	Description	Value
sdpencodetypeval	Specifies the H.248 protocol stack SDP codec type. Set this parameter when you need to configure the H.248 protocol stack SDP codec type.	The value can be **text** or **hex**. Default value: text

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the SDP codec type on an MG interface.

Example

Set the H.248 protocol stack SDP codec type to **text**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] h248stack sdpencodetype hex
```

16.7.1.30 h248stack securitytype

Function

The **h248stack securitytype** command configures the protocol stack message authentication type.

Format

h248stack securitytype *securitytypeval*

undo h248stack securitytype

Parameters

Parameter	Description	Value
securitytypeval	Specifies the H.248 protocol stack message authentication type. Set this parameter when you need to configure the H.248 protocol stack message authentication type.	The value can be **noah**, **sha1**, and **md5**. Currently, the system does not support the MD5 and SHA1 authentication types. Default value: noah

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the protocol stack message authentication type.

Example

Set the H.248 protocol stack message authentication type to **noah**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] h248stack securitytype noah
```

16.7.1.31 h248stack tr

Function

The **h248stack tr** command sets protocol stack transaction reliability parameters on an MG interface.

Format

h248stack tr { **responseackctrl** *response-ack* | **mgcprovtimer** *provtimerval* | **longtimer** *longtimerval* | **retransfailoption** { **t-max** *t-max* | **times** *maxretranstimes* } | **retransmode** { **auto** { **max-retrans-timer** *maxretranstimerval* | **min-retrans-timer** *minretranstimerval* } | **fixed** *retranstimerval* }

Undo h248stack tr { **response-ack** | **prov-timer** | **long-timer** | **retrans-failoption** | **retrans-mode** }

Parameters

Parameter	Description	Value
responseackctrl *response-ack*	Specifies whether to proactively send the RESPONSE ACK message in the common three-way handshake scenario (without the PENDING message). Set this parameter when you need to determine whether to proactively send the RESPONSE ACK message in the common three-way handshake scenario.	The value can be **false** or **true**. Default value: false
mgcprovtimer *provtimerval*	Specifies the duration of the temporary response timer. Within the timer duration, the receiver does not process repeated messages and only returns response messages. Set this parameter when you need to configure the duration of the temporary response timer.	The value is an integer that ranges from 6000 to 10000. Unit: ms Default value: 8000
longtimer *longtimerval*	Specifies the duration of the long timer. If no response is received within the timer duration, the MG interface considers that the transaction transmission fails and starts retransmission. Set this parameter when you need to configure the duration of the long timer.	The value is an integer that ranges from 10000 to 40000. Unit: ms Default value: 30000
retransfailoption	Specifies the retransmission failure option.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
t-max *t-max*	Specifies the maximum retransmission duration. After the transaction fails, the MG interface retransmits the message within the duration specified by **t-max**. If no response is received within the maximum retransmission duration, the MG interface considers that the retransmission fails and stops retransmission. Set this parameter when you need to configure the maximum retransmission duration.	The value is an integer that ranges from 10000 to 30000. Unit: ms Default value: 25000
times *maxretranstimes*	Specifies the maximum retransmission times. After the transaction fails, the MG interface retransmits the message for times specified by **maxretranstimes**. If no response is received after the retransmission times reaches the maximum, the MG interface considers that the retransmission fails and stops retransmission. Set this parameter when you need to configure the maximum retransmission times.	The value is an integer that ranges from 1 to 9. Default value: 7
retransmode	Specifies the retransmission mode.	-
auto	Specifies the automatic mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
max-retrans-timer *maxretranstimerval*	Specifies the maximum duration of the retransmission timer. This parameter is valid only when **Transaction Reliability** is set to **Yes** and **Retransmission Mode** is set to **Automatic**. Set this parameter when you need to configure a maximum duration for the retransmission timer.	The value is an integer that ranges from 500 to 16000. Unit: ms Default value: 4000
min-retrans-timer *minretranstimerval*	Specifies the minimum duration of the retransmission timer. This parameter is valid only when **Transaction Reliability** is set to **Yes** and **Retransmission Mode** is set to **Automatic**. Set this parameter when you need to configure a minimum duration for the retransmission timer.	The value is an integer that ranges from 100 to 4000. Unit: ms Default value: 500
fixed *retranstimerval*	Specifies the fixed duration of the retransmission timer. This parameter is valid only when **Transaction Reliability** is set to **Yes** and **Retransmission Mode** is set to **Fixed**. Set this parameter when you need to configure a fixed duration for the retransmission timer.	The value is an integer that ranges from 100 to 4000. Unit: ms Default value: 2000

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- This command sets transaction reliability parameters of the H.248 protocol stack.
- When you need to use the maximum retransmission times, the duration of the long timer must be greater than the value of the maximum retransmission times multiplied by the maximum duration of the retransmission timer.
- When you need to use the maximum retransmission duration, the duration of the long timer must be greater than the maximum retransmission duration of the transaction reliability timer.

Example

Configure automatic retransmission. Set the minimum duration of the retransmission timer to 500 and maximum duration to 5000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] h248stack tr retransmode auto minretranstimer 500 maxretranstimer 5000
```

16.7.1.32 heartBeat

Function

The **heartBeat** command sets heartbeat parameters on an MG interface.

Format

heartBeat { **genTimer** *gentimer* | **retransTimer** *interval* | **retransTimes** *retrans* }*

undo heartBeat { **genTimer** | **retransTimer** | **retransTimes** }*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
gentimer	Specifies the heartbeat initiation duration on an MG interface. Set this parameter when you need to configure the heartbeat initiation duration on an MG interface. If the MG interface does not receive any messages from the MGC or the MGC fails to respond to a request initiated by the MG interface within the duration specified by **heartBeatGenTimer**, the MG interface starts to send the heartbeat message to the MGC.	The value is an integer that ranges from 0 to 655. Unit: s Default value: 60
interval	Specifies the heartbeat retransmission interval on an MG interface. Set this parameter when you need to configure the heartbeat retransmission interval on an MG interface. If the MGC fails to respond to the heartbeat message sent by the MG interface within the interval specified by **heartBeatRetransTimer**, the MG interface resends the heartbeat message. If this parameter is set to 0, interface interruption cannot be detected using heartbeat messages.	The value is an integer that ranges from 0 to 655. Unit: s Default value: 60

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
retrans	Specifies the heartbeat message retransmission times on an MG interface. Set this parameter when you need to configure the heartbeat message retransmission times on an MG interface. If the MG interface resends the heartbeat message to the MGC for the times specified by **Times** but still no response is received, the MG interface considers that the connection with the MGC is interrupted.	The value is an integer that ranges from 0 to 20. Default value: 3

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command sets heartbeat parameters on an MG interface.

Example

Set the heartbeat parameters on an MG interface. Specifically, set the heartbeat initiation duration to 500, heartbeat retransmission interval to 50, and heartbeat message retransmission times to 6.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] heartBeat genTimer 500 retransTimer 50 retransTimes 6
```

16.7.1.33 mgc switch

Function

The **mgc-switch** command forcibly registers an MG interface with the other MGC.

Format

Mgc switch mgcno *mgcno*

Parameters

Parameter	Description	Value
mgcno *mgcno*	Specifies the MGC ID. This parameter is mandatory. 1 means the primary MGC. 2 means the secondary MGC.	The value is an integer that ranges from 1 to 2.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

When the current MGC is under maintenance or overhaul, run this command. After the command is executed successfully, the MG interface registers with the new MGC.

Example

Forcibly switch the registration of an MG interface to the MGC with **mgcno** being 2.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mgc switch mgcno 2
```

16.7.1.34 mg-media-ip1

Function

The **mg-media-ip1** command configures the media IP address 1 of an MG interface.

Format

mg-media-ip1 {*mg-media-ip* | **addr-name** *addr-name* }

undo mg-media-ip1

Parameters

Parameter	Description	Value
mg-media-ip	Specifies the media IP address 1 of an MG interface. Set this parameter when you need to use a static media IP address. The media IP address must exist in the media IP address pool.	The value is an IP address in dotted decimal notation.
addr-name	Specifies the dynamic address name. The dynamic address name must exist in the system.	The value is a string of 1 to 64 characters.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the media IP address 1 of an MG interface. The IP address can be a dynamic or static IP address.

The media IP address to specify must exist in the media IP address pool.

Example

Configure the media IP address 1 of an MG interface, and set the dynamic address name to **GigabitEthernet0/0/0**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mg-media-ip1 media-addr-name GigabitEthernet0/0/0
```

16.7.1.35 mg-media-ip2

Function

The **mg-media-ip2** command configures the media IP address 2 of an MG interface.

Format

mg-media-ip2 *mg-media-ip*

undo mg-media-ip2

Parameters

Parameter	Description	Value
mg-media-ip	Specifies the media IP address 2 of an MG interface. Set this parameter when you need to classify media packets based on the priority. The IP adders cannot be obtained using DHCP. The media IP address must exist in the media IP address pool.	The value is an IP address in dotted decimal notation.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the media IP address 2 of an MG interface. The IP address must be a static IP address.

The media IP address to specify must exist in the media IP address pool.

Example

Set the media IP address 2 of an MG interface to 192.168.1.126.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mg-media-ip2 192.168.1.126
```

16.7.1.36 mg-ringmode

Function

The **mg-ringmode** command configures ringing mode mapping.

Format

mg-ringmode *index* [**cadence-ring** *cadencering-value* | **initial-ring** *initialring-value*]*

undo mg-ringmode [*index*]

Parameters

Parameter	Description	Value
index	Specifies the peer parameter ID issued by the MGC. If the MGC does not specify this ID, the value of **MgcPara** is 1.	Numeral type. Value range: 0-15
cadence-ring *cadencering-value*	Specifies the cadence-ringing type corresponding to the peer parameter.	Numeral type. Value range: 0-3, 5–15, 128-143, and 255
initial-ring *initialring-value*	Specifies the initial ringing type. This parameter is optional. Use this parameter when you need to configure initial ringing type corresponding to the peer parameter.	Numeral type. Value range: 4, 17, 18, 21, 22, 24-26, 29-31, 144-159, and 255

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- This command adds a ringing mode mapping on an MG interface.
- On an MG interface, if multiple ringing mode mappings have the same value of cadence, only one record is saved.
- A maximum of ringing mode mappings can be configured.

Example

Set the index of the ringing mode mapping to 6, cadence-ringing type to 2, and initial ringing type to 17.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mg-ringmode 6 cadencering 2 initialring 17
```

16.7.1.37 mg-ringmode default-mgcpara

Function

The **mg-ringmode default-mgcpara** command sets default MGC ringing parameters.

Format

mg-ringmode default-mgcpara { **ring** *ring-default-mgcpara* | **mwi** *mwi-default-mgcpara* } *

undo mg-ringmode default-mgcpara { **ring** | **mwi** } *

Parameters

Parameter	Description	Value
ring *ring-default-mgcpara*	Specifies the peer parameter identification delivered by the MGC. If no ringing type is delivered by the MGC, this setting is used by default. This parameter is optional.	The value is an integer within the range of 0–15 and 255. The value 255 indicates that the system default setting is used. Default value: 255
mwi *mwi-default-mgcpara*	Specifies the peer parameter identification delivered by the MGC. If no MWI ringing type is delivered by the MGC, this setting is used by default. This parameter is optional.	The value is an integer within the range of 0–15 and 255. The value 255 indicates that the system default setting is used. Default value: 255

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the default ring parameter of media gateway controller (MGC) on a specified gateway (MG) interface. When the MGC issues a ring or a message waiting indicator (MWI) ring, the ring type and MWI ring

pattern value configured using this command are used if the pattern value is not specified.

Example

Set the MWI type of the default ring on an MGC to 0 and ring type to 0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mg-ringmode default-mgcpara mwi 0 ring 0
```

16.7.1.38 mg-ringmode default-ringpara

Function

The **mg-ringmode default-ringpara** command configures the default common ringing type.

Format

mg-ringmode default-ringpara { **short-ring** *short-ring* | **aoce-ring** *aoce-ring* } *

undo mg-ringmode default-ringpara { **short-ring** | **aoce-ring** }

Parameters

Parameter	Description	Value
short-ring *short-ring*	Specifies the short ringing type. Set this parameter when you need to configure the short ringing type corresponding to the peer parameter.	The value is an integer within the range of 0–4, 5, 6, 8–15, 17, 18, 21, 22, 24–26, 29–31, 128–159, and 255.
aoce-ring *aoce-ring*	Specifies the AOCE ringing type. This parameter is optional. Set this parameter when you need to configure the AOCE ringing type.	The value is an integer within the range of 4, 17, 18, 21, 22, 24–26, 29–31, 144–159, and 255.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the default common ring type on a specified media gateway (MG) interface. When the media gateway controller (MGC) issues a short-ring or an advice of charge (AoC) ring, the ring type configured using this command is used if no value is specified for the ring type.

Example

Configure the short ringing type of a common ring to 4 and AOCE ringing type to 17.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mg-ringmode default-ringpara short-ring 4 aoce-ring 17
```

16.7.1.39 mg-signal-ip

Function

The **mg-signal-ip** command sets the signaling IP address and port number on the current H.248 interface. These parameters take effect only after the H.248 interface is reset.

Format

mg-signal-ip { *ip_addr* | **signal-addr-name** *name* } **mgport** *port*

Parameters

Parameter	Description	Value
ip_addr	Specifies the signaling IP address of an MG interface. Set this parameter when you need to use a static signaling IP address. The signaling IP address must exist in the signaling IP address pool. You can run the **ip address** command to configure the signaling IP address pool.	The value is an IP address in dotted decimal notation.
signal-addr-name	Specifies the dynamic address name. The dynamic address name must exist in the system.	The value is a string of 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port	Specifies the transport layer protocol port number of an MG interface. The value must be the same as the MG port number configured on the MGC.	The value is an integer that ranges from 2900 to 2999.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command sets the signaling IP address and port number on the current H.248 interface. The signaling IP address must exist in the signaling IP address pool.

These parameters take effect only after the H.248 interface is reset.

Example

Set the dynamic address name of the signaling IP address on an H.248 interface to **GigabitEthernet0/0/0** and port number to **2949**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mg-signal-ip signal-addr-name GigabitEthernet0/0/0 mgport 2949
```

16.7.1.40 mg-software parameter

Function

The **mg-software parameter** command sets control points.

The **undo mg-software parameter** command restores the default value of control points.

Format

mg-software parameter *name value*

undo mg-software parameter *name*

Parameters

Parameter	Description	Value
name	Specifies the control point name.	The value is an integer that ranges from 0 to 37.
value	Specifies the control point value.	The value is an integer. Different control points may use different value ranges.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- You can configure control point 2 of the MG interface (whether or not to support multi-homing) only when the MG interface is in the locally closed state. Currently, the multi-homing function and the single-endpoint registration function in the system conflict with each other. If control point 2 is set to 1 or 2, control point 4 must be set to 0 (using the wildcard for registration).
- You can configure control point 4 of the MG interface (whether or not to use the wildcard for registration) only when the MG interface is in the locally closed state. The dual-homing function and the single-endpoint registration function in the system conflict with each other. If control point 4 is set to 1 (not using the wildcard for registration), control point 2 must be set to 0 (not supporting dual-homing). The single-endpoint registration function and the authentication function conflict with each other. If control point 4 is set to 1 (not using the wildcard for registration), control point 6 must be set to 1 (not supporting authentication).

The following table lists MG interface control points.

Parameter	Description	Value
0	System reserved.	-
1	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
2	Indicates whether an MG interface supports multihoming. Set this parameter when you need to determine whether an MG interface supports multihoming. This parameter can be set only when the MG interface is in Local Closed state. If multihoming is not supported and the MG interface fails to register with the primary MGC, the MG interface will not register with the standby or standalone MGC no matter whether the standby or standalone MGC is configured. If multihoming is supported and a primary MGC fault occurs when the current MG interface is registered with the primary MGC, the MG interface registers with the standby MGC and standalone MGC cyclically. ● If the standby MGC runs properly, the MG interface switches to the standby MGC. ● If the standby MGC is faulty or not configured and the standalone MGC runs properly, the MG interface switches to the standalone MGC. Note: When the MG interface switches to the standalone MGC, the interface restarts	The value can be 0, 1, or 2. ● 0: Multihoming is not supported. ● 1: Multihoming is supported while automatic switchover is not. ● 2: Both multihoming and automatic switchover are supported. Default value: 0

Parameter	Description	Value
	and services will be interrupted. If the MG interface supports both multihoming and automatic switchover, the MG interface functions as follows: ● If the MG interface is registered with the standby MGC and the primary MGC recovers, the MG interface automatically switches to the primary MGC. ● If the MG interface is registered with the standalone MGC and the primary or standby MGC recovers, the MG interface automatically switches to the primary or standby MGC. Note: When the MG interface switches to the primary or standby MGC from the standalone MGC, the interface restarts and services will be interrupted. If the MG interface supports multihoming but does not support automatic switchover, the MGC will not automatically switch to the primary MGC from the standby or standalone MGC when the primary MGC recovers. You can run the **mgc switch** command to	

Parameter	Description	Value
	forcibly switch the MG interface to the primary MGC. If the MG interface supports multihoming, you can run the **mgc switch** command to forcibly switch the MG interface: ● Between the primary and standby MGCs. ● From the standalone MGC to the primary or standby MGC if the MG interface registers with the standalone MGC.	
3	System reserved.	-
4	Indicates whether wildcard characters are used during MG interface registration. Set this parameter when you need to determine whether wildcard characters are used during MG interface registration. If wildcard characters are used, all terminals on the MG interface are registered with the MGC using one message, which reduces the number of messages sent between the MG interface and MGC. If wildcard characters are not used, all terminals on the MG interface register with the MGC one by one. The registration mode where wildcard characters are not used is also called single-endpoint registration.	The value can be 0 or 1. ● 0: used. ● 1: not used. Default value: 0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
5	System reserved.	-
6	Indicates whether an MG interface supports device authentication. Set this parameter when you need to determine whether an MG interface supports device authentication. After enabling device authentication support, you can run the **auth** command to set authentication parameters and run the **reset** command to reset the MG interface. After the configuration, the MGC manages the MG device security to prevent unauthorized devices from registering with the MGC. Note: When the MG interface is reset, services may be interrupted.	The value is an integer that ranges from 0 to 1. ● 0: supported. ● 1: not supported. Default value: 1
7	Indicates whether an MG interface supports the security header. Set this parameter when you need to determine whether an MG interface supports the security header. After enabling security header support, you can run the **auth** command to set authentication parameters and run the **reset** command to reset the MG interface. After the configuration, the MGC manages the MG device security to ensure data integrity.	The value is an integer that ranges from 0 to 1. ● 0: supported. ● 1: not supported. Default value: 1

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
8	System reserved.	-
9	System reserved.	-
10	System reserved.	-
11	Indicates whether an MG interface supports local switch. Set this parameter when you need to determine whether an MG interface supports local switch. If the MG interface supports local switch and the MG is disconnected from the MGC, users on the MG can still make calls.	The value is an integer that ranges from 0 to 3. ● 0: No call is allowed. ● 1: Only internal calls are allowed. ● 2: Only survival calls are allowed. ● 3: All calls are allowed. Default value: 0
12	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
13	Digit map match scheme used by an MG interface. Set this parameter when you need to configure the digit map match scheme used by an MG interface. In the shortest match scheme, the MG interface reports collected digits immediately when they match a dialing scheme. In the longest match scheme, the MG interface does not report collected digits immediately when they match a dialing scheme. Instead, the MG interface continues to collect digits and match collected digits with dialing schemes if the user dials any numbers within the short timer duration (4s by default), and reports collected digits only when the short timer times out. In the self-adaptive match scheme, the MG interface checks digit map sub-schemes to automatically determine whether to use the shortest or longest match scheme. You can run the **digitmap-timer** command to configure digit map timer durations.	The value is an integer that ranges from 0 to 3. ● 0: based on protocol requirements. ● 1: longest match. ● 2: shortest match. ● 3: self-adaptive match. Default value: 2
14	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
15	Indicates whether an MG interface filters media stream source ports. Set this parameter when you need to determine whether an MG interface filters media stream source ports. When the media stream source port filtering function is used, the MG interface receives media stream only from specified ports.	The value is an integer that ranges from 0 to 1. ● 0: not filtered. ● 1: filtered. Default value: 0
16	Duration of the media stream source port filtering timer. If the media stream source port filtering function is disabled, the MG port starts the timer when media streams are received. If the command for enabling the media stream source port filtering function is not received within the timer duration, the timer times out and the media stream source port filtering function is automatically enabled.	The value is an integer that ranges from 1 to 30, in seconds. Default value: 5
17	System reserved.	-
18	System reserved.	-
19	System reserved.	-
20	System reserved.	-
21	System reserved.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
22	Type of the tone that the MG plays to users when the MG is disconnected from the MGC.	The value is an integer that ranges from 0 to 2. ● 0: busy tone. ● 1: congestion tone. ● 2: voice announcement. Default value: 0
23	Duration of the port status synchronization timer. When a remotely blocked port receives signaling from the MGC, the device determines whether to directly update the port status or initiate port registration to the MGC. If the device initiates port registration, the device initiates port registration again after the port status synchronization timer duration. This parameter is invalid for RTP terminals.	The value is an integer that ranges from 0 to 120, in seconds. Default value: 35

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
24	Maximum RTP terminal index. An RTP terminal is a temporary terminal, which is a unique terminal type for an MG interface that supports H.248. A temporary terminal represents temporary information streams and exists only when the MG uses these information streams. For example, when establishing media streams, the MG interface uses remote MGC information and a temporary terminal exists. The maximum number of RTP terminals on the MGC must be the same as that on the MG.	The value is an integer. The value range depends on product specifications.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
25	Maximum random number for the avalanche prevention mechanism. When the system is reset, all H.248 interfaces on the device register with the MGC again. When all interfaces initiate registration simultaneously, packet conflicts will occur and the MGC may break down. The avalanche prevention mechanism can help avoid this situation. After the maximum random number for the avalanche prevention mechanism is configured, the system uses an internal algorithm to generate the duration after which an H.248 interface can initiate registration. The duration after which an H.248 interface can initiate registration is greater than the sum of the system internal base number and the maximum random number for the avalanche prevention mechanism.	The value is an integer that ranges from 30000 to 300000, in milliseconds. Default value: 60000
26	Local blocking tone type. When the MG interface is faulty or you run the **endservice** command, the MG interface enters the local blocking state. This parameter specifies the type of the tone played in local blocking state.	The value is an integer that ranges from 0 to 4. ● 0: busy tone. ● 1: congestion tone. ● 2: muted. ● 3: custom tone 1. ● 4: custom tone 2. Default value: 0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
27	Remote blocking tone type. When the MGC does not respond and a response error occurs, the MG interface enters the remote blocking state. This parameter specifies the type of the tone played in remote blocking state.	The value is an integer that ranges from 0 to 4. ● 0: busy tone. ● 1: congestion tone. ● 2: muted. ● 3: custom tone 1. ● 4: custom tone 2. Default value: 0
28	Duration of the howler tone. If a user does not hang up the phone after a call ends or picks up but forgets to hang up, the howler tone is played when the busy tone timer times out. After the duration of the howler tone, the port is locked. In this case, the phone cannot be called. The port is automatically unlocked when the user hangs up the phone.	The value is an integer that ranges from 1 to 65535, in seconds. Default value: 60
29	Duration of message prompt tone. When a user who has enabled the message prompt tone service picks up the phone, the MGC delivers the message prompt tone (similar in delivering the dial tone).	The value is an integer that ranges from 1 to 60000, in seconds. Default value: 3
30	Duration for generating the long call alarm. If the long call alarm is enabled and the duration of a call exceeds that for generating the long call alarm, the system generates the H.248 user long call event.	The value is an integer that ranges from 1 to 65535, in minutes. Default value: 60

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
31	Indicates whether the long call alarm is enabled.	The value is an integer that ranges from 0 to 1. ● 0: enabled. ● 1: disabled. Default value: 1
32	Minimum automatic registration interval for a remotely blocked port. When the interface that a port belongs to functions properly but the port is blocked remotely because the MGC does not respond and a response error occurs, the port automatically initiates registration requests to the MGC based on the interval specified by this parameter.	The value is an integer that ranges from 0 to 60000. The value 0 indicates that the port does not automatically register with the MGC. Unit: s Default value: 1800
33	Indicates whether the heartbeat function is disabled on an MG interface. Generally, the heartbeat function is enabled for the MG to keep the connection with the MGC. In a few cases, some MGCs cannot recognize the heartbeat message sent by the MG interface, and the heartbeat function is disabled. The MGC periodically sends the Notify message to keep the connection.	The value is an integer that ranges from 0 to 1. ● 0: disabled. ● 1: enabled. Default value: 1
34	Indicates whether the MG needs to proactively establish or tear links for BRA users when ISDN ports are in service or out of service due to the MGC.	The value is an integer that ranges from 0 to 1. ● 0: yes. ● 1: no. Default value: 0

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
35	Mode in which an ISDN port enters the in-service or out-of-service state. ● If the wildcard mode is supported, the ISDN report only one in-service or out-of-service message. This reduces the number of messages sent between the MG interface and MGC. ● If the single-channel mode is supported, each channel reports an in-service or out-of-service message. ● If both the wildcard and single-channel modes are supported, the ISDN port selects a mode as required.	The value is an integer that ranges from 0 to 2. ● 0: Both the wildcard and single-channel modes are supported. ● 1: Only the single-channel mode is supported. ● 2: Only the wildcard mode is supported. Default value: 1
36	Interval for sending the registration message when an MG interface switches between multiple MGCs. Set this parameter when you need to configure the interval for sending the registration message when an MG interface switches among the primary, standby, and standalone MGCs.	The value is an integer that ranges from 1 to 1800, in seconds. Default value: 40
37	Indicates whether to enable the function of converting pulse signals to DTMF signals. Set this parameter when you need to convert pulse signals to DTMF signals for transmission.	The value is an integer that ranges from 0 to 1. ● 0: enabled. ● 1: disabled. Default value: 1

Example

Set the value of control point 25 on an MG interface to 40000.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] mg-software parameter 25 40000
```

16.7.1.41 MIDType

Function

The **midtype** command configures the H.248 message identification (MID) type.

Format

MIDType *midtypeval*

undo MIDType

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
midtypeval	Specifies the H.248 MID type. The MID is contained in a message header and is used to identify the user sending the message. Set this parameter when you need to configure the H.248 MID type for the specified MG interface. When the MG interface IP address is used to identify the user sending the message, select **ip4Address**. When the name of the domain that the device deployed on the MG interface belongs to is used to identify the user sending the message, select **domainName**. When the name of the device deployed on the MG interface is used to identify the user sending the message, select **deviceName**. This parameter is generally set to **ip4Address**. You can select a value based on functions supported by the MGC.	The value can be **ip4Address**, **domainName**, or **deviceName**. Default value: ip4Address

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the H.248 message identification (MID) type.

- When the MG interface IP address is used to identify the user sending the message, select **ip4Address**.

 Copyright © Huawei Technologies Co., Ltd.

- When the name of the domain that the device deployed on the MG interface belongs to is used to identify the user sending the message, select **domainName**.
- When the name of the device deployed on the MG interface is used to identify the user sending the message, select **deviceName**.

Example

Set the H.248 MID type to **deviceName**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] MIDType deviceName
```

16.7.1.42 profile-negotiation

Function

The **profile-negotiation** command sets the profile negotiation parameter on an MG interface.

The **undo profile-negotiation** command restores the default setting.

Format

profile-negotiation *profile-negotiation*

undo profile-negotiation

Parameters

Parameter	Description	Value
profile-negotiation	Specifies whether to enable profile negotiation. Set this parameter to **enable** when the MG and the MGC negotiate the profile negotiation name. When the MG and MGC have different profile negotiation names, the negotiation process is as follows: if the MG and MGC have the same profile, the MG and MGC negotiate based on the profile; if the MG and MGC have different profiles, the negotiation fails. When this parameter is set to **disable** and the MG and the MGC have different profile negotiation names, the negotiation fails.	The value can be **enable** or **disable**. Default value: disable

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

When the profile-negotiation is set to enable,

- the MG negotiates the profile-negotiation-name with the MGC.
- When the profile-negotiation-name is inconsistent, if the MG uses the same profile as the MGC, the profile used on the MGC is used for negotiation.
- Otherwise, the negotiation fails.

When the profile-negotiation is set to disable, the profile-negotiation-name of the MG is inconsistent with that of the MGC, the negotiation fails.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable profile negotiation between the MG and MGC.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] profile-negotiation enable
```

16.7.1.43 profile-index

Function

The **profile-index** command configures a profile index of an MG interface.

The **undo profile-index** command deletes a profile index of an MG interface.

Format

profile-index *index*

undo profile-index

Parameters

Parameter	Description	Value
index	Profile index of an MG interface.	Numeral type. Value range: 0–7. Default value: 1 Values: ● 0: CustomizingProfile-Templet("") ● 1: NoProfile("") ● 2: BT_AGW/3("BT_AGW/3") ● 3: FT_AGW/2("FT_AGW/2") ● 4: KPN_AGW/1("KPN_AGW/1") ● 5: PCCW_AGW/1("PCCW_AGW/1") ● 6: ZTE_AGW/1("ZTE_AGW/1") ● 7: BELL_AGW/1("BELL_AGW/1")

Views

H248AG view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

When signaling processing on the MG is different from that on the MGC, configure the profile for adaptation.

The profile used by the MG interface must be the same as that on the MGC.

Index 0 specifies a user-defined profile, index 1 specifies the default profile, and the other indexes specify preset profiles in the system.

Example

Set the profile index of an MG interface to 0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] profile-index 0
```

16.7.1.44 primary-mgc-address1

Function

The **primary-mgc-address1** command configures the primary MGC domain name and port number on an H.248 interface.

Format

primary-mgc-address1 primary-mgc-domain-name *domainname port*

Parameters

Parameter	Description	Value
primary-mgc-domain-name *domainname*	Specifies the name of the primary MGC domain that an MG interface belongs to. The MGC that an MG interface belongs to can be identified using the MGC IP address or domain name.	The value is a string of 1 to 64 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port	Specifies the transmission protocol port number of the primary MGC that an MG interface belongs to. The MGC protocol port number configured on an MG interface must be the same as that configured on the MGC.	The value is an integer that ranges from 1 to 65534.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the primary MGC domain name and port number on an H.248 interface.

Example

Set the primary MGC domain name to **abcd.com** and port number to **2949**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1]primary-mgc-address1 primary-mgc-domain-name abcd.com 2949
```

16.7.1.45 primary-mgc-address1 static

Function

The **primary-mgc-address1 static** command configures the primary MGC IP address and port number.

Format

primary-mgc-address1 static *ip_addr port* [**primary-mgc-address2** *ip_addr2*]

Parameters

Parameter	Description	Value
ip_addr	Specifies IP address 1 of the primary MGC that an MG interface belongs to. The MGC that an MG interface belongs to can be identified using the MGC IP address or domain name. Set this parameter when the IP address is used to identify the primary MGC that an MG interface belongs to.	The value is an IP address in dotted decimal notation.
port	Specifies the transmission protocol port number of the primary MGC that an MG interface belongs to. The MGC protocol port number configured on an MG interface must be the same as that configured on the MGC.	The value is an integer that ranges from 1 to 65534.
ip_addr2	Specifies IP address 2 of the primary MGC that an MG interface belongs to. This parameter is optional and takes effect only when the transmission protocol is SCTP.	The value is an IP address in dotted decimal notation.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command configures the primary MGC IP address and port number.

When the IP address of the primary MGC exists, you can delete the domain name of the primary MGC. When the domain name of the primary MGC exists, you can

delete the IP address of the primary MGC. However, the domain name and IP address of the primary MGC cannot be deleted at the same time.

When the data of the primary MGC is not configured completely, the data of other secondary MGCs cannot be configured.

Upon the configuration, you must run the **reset** command to reset the MG interface for validating the configuration data. Otherwise, the configuration data is just stored in the database.

Example

Set the primary MGC IP address to 192.168.1.110 and port number to 2944.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 0
[Huawei-voice-h248ag-0] primary-mgc-address1 static 192.168.1.110 2944
```

16.7.1.46 reset

Function

The **reset** command resets an interface.

Format

reset *resettype*

Parameters

Parameter	Description	Value
resettype	Specifies the MG interface reset mode. Set this parameter to specify the reset mode. An MG interface performs different reset operations and sends different registration requests to the MGC based on the reset mode. The options are as follows: ● servicerestored: service restoration. When this reset mode is used, the status of terminals on the MG interface does not change. ● coldstart: cold startup. When this reset mode is used, the status of terminals on the MG interface will be initialized to the default value. ● warmstart: warm startup. When this reset mode is used, the status of terminals on the MG interface does not change. During warm startup, data in all ongoing processes will be lost; however, the status of terminals on the MG interface does not change. ● capabilitieschange: MG performance change. When this reset mode is used, the status of terminals on the MG interface does not change. MG	The value can be **servicerestored**, **coldstart**, **warmstart**, or **capabilitieschange**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	performance change occurs when the data package does not change while the performance parameters change. The MGC monitors the MG performance to determine which performance parameters can change.	

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- Only when the MG interface is in the normal or graceful shutdown state, it can be reset in servicerestored mode. The coldstart mode is not restricted.
- You can run this command to reset the interface only after the attributes of the MG interface are configured, such as the signaling IP address, media IP address, port number of the transport layering protocol, MGC IP address, port number of the MGC transport layering protocol, and the transport protocol type.

Example

Cold start the H.248 AG.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] reset coldstart
```

16.7.1.47 retrans

Function

The **retrans** command configures transaction reliability.

The **undo retrans** command disables configuring transaction reliability.

Format

retrans *retransval*

undo retrans

Parameters

Parameter	Description	Value
retransval	When retransval is set to enable, the system considers a message sending failure if the MG port does not receive a response message from the peer end within a period of time. In this case, the system sends the message again. When xxx is set to disable, the system does not send the message again even if the MG port does not receive a response message from the peer end.	The value can be **enable** or **disable**.

Views

H.248 view

Default Level

2: Configuration level

Usage Guidelines

When retransval is set to enable, the system considers a message sending failure if the MG port does not receive a response message from the peer end within a period of time. In this case, the system sends the message again. When xxx is set to disable, the system does not send the message again even if the MG port does not receive a response message from the peer end.

Example

Enable transaction reliability.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 0
[Huawei-voice-h248ag-0] retrans enable
```

 Copyright © Huawei Technologies Co., Ltd.

16.7.1.48 secondary-mgc-address1

Function

The **secondary-mgc-address1** command sets the secondary MGC domain name and port number.

The **undo secondary-mgc-address1** command restores default setting.

Format

secondary-mgc-address1 secondary-mgc-domain-name *domainname port*

undo secondary-mgc-address1

Parameters

Parameter	Description	Value
secondary-mgc-domain-name *domainname*	Specifies the name of the secondary MGC domain that an MG interface belongs to. The MGC that an MG interface belongs to can be identified using the MGC IP address or domain name.	The value is a string of 1 to 64 characters.
port	Specifies the transmission protocol port number of the secondary MGC that an MG interface belongs to. The MGC protocol port number configured on an MG interface must be the same as that configured on the MGC.	The value is an integer that ranges from 1 to 65534.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

This command sets the secondary MGC domain name and port number.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the secondary MGC domain name to **abcd.com** and port number to **2949**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] secondmary-mgc-address1  secondary-mgc-domain-name abcd.com 2949
```

16.7.1.49 secondary-mgc-address1 static

Function

The **secondary-mgc-address1 static** command configures the secondary MGC IP address and port number.

Format

secondary-mgc-address1 static *ip_addr port* [**primary-mgc-address2** *ip_addr2*]

undo secondary-mgc-address1

Parameters

Parameter	Description	Value
ip_addr	Specifies IP address 1 of the secondary MGC that an MG interface belongs to. The MGC that an MG interface belongs to can be identified using the MGC IP address or domain name. Set this parameter when multihoming is configured and the IP address is used to identify the secondary MGC that an MG interface belongs to.	The value is an IP address in dotted decimal notation. The value **255.255.255.255** indicates that the secondary MGC IP address 1 is deleted. However, you cannot enter **255.255.255.255** to delete a primary MGC IP address in use.
port	Specifies the transmission protocol port number of the secondary MGC that an MG interface belongs to. Set this parameter when multihoming is configured.	The value is an integer that ranges from 1 to 65534.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip_addr2	Specifies IP address 2 of the secondary MGC that an MG interface belongs to. This parameter is optional and takes effect only when the transmission protocol is SCTP.	The value is an IP address in dotted decimal notation. The value **255.255.255.255** indicates that the secondary MGC IP address 2 is deleted.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

The command sets the secondary MGC IP address and port number.

Example

Set the secondary MGC IP address to 192.168.1.110 and port number to 2944.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-0] primary-mgc-address1 static 192.168.1.110 2944
```

16.7.1.50 shutdown

Function

The **shutdown** command disables an MG interface.

Format

shutdown { **force** | **graceful** *gracetime* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
force	Forcibly disables an MG interface. Set this parameter when you need to forcibly disable an MG interface. When an MG interface is forcibly disabled, all calls routed though this interface are immediately disconnected.	-
graceful *gracetime*	Gracefully disables an MG interface. In the preceding command, *gracetime* indicates the duration when an MG interface is gracefully disabled, and the *gracetime* value varies based on the service running in the system. Set this parameter when you need to gracefully disable an MG interface. Before an MG interface is gracefully disabled, only existing calls routed though this interface can be handled during the duration specified in *gracetime*. When *gracetime* is set to 0s, the MG interface can be disabled only after all existing calls end.	The value is an integer that ranges from 0 to 86400. Unit: s

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

- If you set the MG interface to support single-endpoint registration (that is, control point 4 is configured to 1) by running the **mg-software parameter** command, you cannot shut down the interface in graceful mode.
- To reset the MG interface, run the **reset** command in H.248 mode.
- After the duration of the graceful shutdown completes or all calls on the MG interface complete, the MG interface can shut down automatically.
- The MG interface can be shut down in graceful mode only when it is in service or the remote end interface is shut down. In addition, if the user already performs graceful shutdown on an interface, the interface cannot be shut down in graceful mode again before the previous shutdown operation is complete.

Example

Forcibly disables an MG interface.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] shutdown force
```

16.7.1.51 standalone parameters

Function

The **standalone parameters** command sets local switch parameters.

Format

standalone parameters { **dialtone** *dialtoneval* | **ring** *ringval* | **busytone** *busytoneval* } *

undo standalone parameters { **dialtone** | **ring** | **busytone** }

Parameters

Parameter	Description	Value
dialtone *dialtoneval*	Specifies the dialing timer duration. This parameter is optional. Set this parameter when you need to configure the dialing timer duration. If a calling party does not dial a number after the duration specified on the dialing timer, the busy tone is played to the calling party.	The value is an integer that ranges from 1 to 120. Unit: s Default value: 10

Parameter	Description	Value
ring *ringval*	Specifies the ringing timer duration. This parameter is optional. Set this parameter when you need to configure the ringing timer duration. If a called party does not answer an incoming call after the duration specified on the ringing timer, the ring tone is stopped.	The value is an integer that ranges from 1 to 120. Unit: s Default value: 50
busytone *busytoneval*	Specifies the busy tone timer duration. This parameter is optional. Set this parameter when you need to configure the busy tone timer duration. When the duration specified on the ringing timer expires, the howler tone is played.	The value is an integer that ranges from 1 to 120. Unit: s Default value: 40

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

When you need to set the time length of the busy tone timer, the dial tone timer, or the ringing timer, run this command.

The timer time length that is configured by this command takes effect only to emergency standalone.

When you make a call in the case of emergency standalone, if the time length of the busy tone, dial tone or ringing is the same as the time length that is set, the operation is successful.

Example

Set the dialing timer duration to 33, ringing timer duration to 44, and busy tone timer duration to 55.

```
<Huawei> system-view
[Huawei] voice
```

```
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] standalone parameters dialtone 33 ring 44 busytone 55
```

16.7.1.52 stand-alone-mgc-ip1

Function

The **stand-alone-mgc-ip1** command sets the standalone MGC IP address and port number.

Format

stand-alone-mgc-ip1 *ip_addr* [**stand-alone-mgc-ip2** *ip_addr2*] **stand-alone-mgc-port** *port*

Undo stand-alone-mgc-ip1

Parameters

Parameter	Description	Value
ip_addr	Specifies IP address 1 of the standalone MGC that an MG interface belongs to. The MGC that an MG interface belongs to can be identified using the MGC IP address or domain name. Set this parameter when multihoming is configured and the IP address is used to identify the standalone MGC that an MG interface belongs to. After multihoming is configured using this parameter, if the primary and secondary MGCs are faulty and the network gateway disconnects from the softswitch, services can be automatically switched to the standalone MGC, inter-office calls can be connected, and users can use the PSTN network to make emergency calls.	The value is an IP address in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
stand-alone-mgc-ip2 *ip_addr2*	Specifies IP address 2 of the standalone MGC that an MG interface belongs to. Set this parameter when multihoming is configured.	The value is an IP address in dotted decimal notation.
stand-alone-mgc-port *port*	Specifies the transmission protocol port number of the standalone MGC that an MG interface belongs to. Set this parameter when multihoming is configured.	The value is an integer that ranges from 1 to 65535.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

To configure multihoming and use the IP address to identify the standalone MGC to which the MG interface belongs, use this parameter.

Example

Set IP address 1 of the standalone MGC that an MG interface belongs to **192.168.1.1**, IP address 2 to **10.10.10.2**, and transmission protocol port number to **2988**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] stand-alone-mgc-ip1 192.168.1.1 stand-alone-mgc-ip2 10.10.10.2 stand-alone-mgc-port 2988
```

16.7.1.53 start-negotiate-version

Function

The **start-negotiate-version** command configures the H.248 protocol version for starting negotiation between the MG and MGC.

Format

start-negotiate-version *verno*

undo start-negotiate-version

Parameters

Parameter	Description	Value
verno	Specifies the H.248 protocol version for starting negotiation between the MG and MGC. If the MG and MGC have the same signal handling process, the H.248 protocol version for starting negotiation can be configured as required; if the MG and MGC have different signal handling processes, the H.248 protocol version for starting negotiation is set to 0 so that MG negotiates with the MGC based on the profile.	The value is an integer that ranges from 0 to 3. Default value: 3 0: negotiates based on the profile. 1: starts negotiation from V1. 2: starts negotiation from V2. 3: starts negotiation from V3. The negotiation starts based on the H.248 protocol version in ascending order. The recommended value is 1.

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

During the negotiation between the MG and MGC,

- if the signaling processing procedures are the same, configure the negotiation version according to the actual requirement;
- if the signaling processing procedures are different, the negotiation version is configured to 0, that is, negotiating according to the profile.

Example

Set the H.248 protocol version for starting negotiation between the MG and MGC to 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1]start-negotiate-version 1
```

16.7.1.54 transfer

Function

The **transfer** command configures the signaling transmission mode.

Format

transfer *protocol*

undo transfer

Parameters

Parameter	Description	Value
protocol	Specifies the protocol signaling transmission mode used by an MG interface. The signaling transmission mode used by the MG interface must be the same as that configured on the MGC.	The value can be **tcp**, **udp**, **sctp**. The TCP protocol is not supported currently. Default value: udp

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

The transmission mode used by the MG interface must be the same as that configured on the MGC.

Example

Set the signaling transmission mode on an H.248 interface to **sctp**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] transfer sctp
```

 Copyright © Huawei Technologies Co., Ltd.

16.7.1.55 tid-format

Function

The **tid-format** command sets the terminal ID (TID) format for an MG interface.

Format

tid-format { { **rtp** | **pstn** | **bra** | **pra** } { **prefix** *prefix-string* | **template** *index* } * } *

undo tid-format

Parameters

Parameter	Description	Value
rtp	Specifies the RTP terminal.	-
pstn	Specifies the PSTN terminal.	-
bra	Specifies the BRA terminal.	-
pra	Specifies the PRA terminal.	-
prefix *prefix-string*	Specifies the terminal prefix. The terminal flag is generated based on the terminal prefix and the TID template.	The value is a string of 1 to 64 characters.
template *index*	Specifies the TID template index used by the terminal. The terminal flag is generated based on the terminal prefix and the TID template. This parameter is optional. Set this parameter when you need to configure the TID template index used by the terminal.	The value is an integer that ranges from 0 to 63.

Views

H.248 AG view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

When setting prefixes, you must ensure that the PSTN, PRA, and BRA terminal prefixes are the same or different each other.

Example

Set the PSTN terminal prefix to **pstn12** and the TID template index used by the terminal to **4**. Set the BRA terminal prefix to **bra12** and TID template index used by the terminal to **14**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1] tid-format pstn prefix pstn12 template 4 bra prefix bra12 template 14
```

16.7.2 H.248 AG User Configuration Commands

Description

This topic describes H.248 AG user configuration commands.

16.7.2.1 active-mask

Function

The **active-mask** command configures the mask for enabling an ISDN PRA user sub-channel.

The **undo active-mask** command restores the mask for enabling an ISDN PRA user sub-channel to the initial value.

Format

active-mask *mask-value*

undo active-mask

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mask-value	Specifies the mask for enabling an ISDN PRA user sub-channel. A mask enables a channel from channel 31 to channel 0. The options are as follows: ● 0: unavailable. ● 1: available. The masks for channels 0 and 16 must be set to 1.	Dotted decimal notation. Format: mask0:mask1:mask2:mask3. Mask0 to mask3 are the active masks of sub-channel 31 to sub-channel 0. For each mask, the identification of sub-channel B is from right to left. That is, mask3=1 indicates that sub-channel 0 is available and mask3=3 indicates that sub-channels 0 and 1 are available. Default value: 255.255.255.255. The default value indicates that all sub-channels are available.

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

Run this command when you need to enable or disable an ISDN PRA user sub-channel.

Example

Set the mask for enabling an ISDN PRA user sub-channel to 192.168.1.1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser-1/0/0
[Huawei-voice-h248aguser-1/0/0] active-mask 192.168.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

16.7.2.2 auto-resume-limit

Function

Using the **auto-resume-limit** command, you can set the maximum number of automatic recoveries from deterioration.

Using the **undo auto-resume-limit** command, you can restore the default maximum number of automatic recoveries from deterioration.

By default, the maximum number of automatic recoveries from deterioration is 20.

Format

auto-resume-limit *limit*

undo auto-resume-limit

Parameters

Parameter	Description	Value
limit	Specifies the upper limit of times that a degradation fault (especially, a port fault) is automatically rectified.	The value is an integer that ranges from 0 to 255. The default value is 20. The value 0 indicates that the fault is not automatically rectified. The value 255 indicates unlimited times.

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command sets the upper limit of times that a degradation fault (especially, a port fault) is automatically rectified of PSTN users.

Example

Set the maximum number of automatic recoveries from deterioration to 50.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser-1/0/0
[Huawei-voice-h248aguser-1/0/0] auto-resume-limit 10
```

16.7.2.3 bell-ans-flag

Function

The **bell-ans-flag** command configures the flag for enabling BELL ANS signal support.

The **undo bell-ans-flag** command deletes the flag for enabling BELL ANS signal support.

Format

bell-ans-flag [*bell-ans-flag-value*]

undo bell-ans-flag

Parameters

Parameter	Description	Value
bell-ans-flag-value	Specifies the flag for enabling BELL ANS signal support.	The value can be **enable** or **disable**. Default value: disable

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command sets the flag for enabling BELL ANS signal support of PSTN users.

Example

#Enable BELL ANS signal support.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] bell-ans-flag enable
```

16.7.2.4 clip-format

Function

The **clip-format** command configures the calling number format.

The **undo clip-format** command deletes the calling number format.

Format

clip-format [*clipformat-value*]

undo clip-format

Parameters

Parameter	Description	Value
clipformat-value	Specifies the calling number format. This parameter is optional. Set this parameter when you need to configure the calling number format for PSTN users. The options are as follows: ● sdmffsk: FSK Single Data Message Format (SDMF) format. ● mdmffsk: FSK Multiple Data Message Format (MDMF) format. ● dtmf: DTMF format. ● r1.5: Russia calling number display format. ● etsi: BT calling number display format.	The value can be **sdmffsk**, **mdmffsk**, **dtmf**, **r1.5**, or **etsi**. Default value: sdmffsk

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

- This command sets the calling number format of PSTN users.
- This command can be executed only in H.248 AG user view.

 Copyright © Huawei Technologies Co., Ltd.

Example

#Specify the calling number format to **mdmffsk**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] clip-format mdmffsk
```

16.7.2.5 clip-transmission-sequence

Function

The **clip-transmission-sequence** command configures the mode for delivering calling numbers for PSTN users.

The **undo clip-transmission-sequence** command restores the mode for delivering calling numbers for PSTN users to the default value.

Format

clip-transmission-sequence [*clip-transmission-sequence*]

undo clip-transmission-sequence

Parameters

Parameter	Description	Value
clip-transmission-sequence	Specifies the mode for delivering calling numbers. This parameter is optional. Set this parameter when you need to configure the mode for delivering calling numbers for PSTN users. The options are as follows: ● after-ring: delivers calling numbers after ringing. ● before-ring: delivers calling numbers before ringing.	The value can be **after-ring** or **before-ring**. Default value: after-ring

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

- This command sets the mode for delivering calling numbers of PSTN users.
- This command can be executed only in H.248 AG user view.

Example

#Configure the mode for delivering calling numbers to **before-ring**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] clip-transmission-sequence before-ring
```

16.7.2.6 dc-time

Function

The **dc-time** command configures the power-off interval for PSTN users.

The **undo dc-time** command deletes the power-off interval for PSTN users.

Format

dc-time [*dc-time-value*]

undo dc-time

Parameters

Parameter	Description	Value
dc-time-value	Specifies the power-off interval. This parameter is optional. Set this parameter when you need to configure the power-off interval for PSTN users.	The value is an integer that ranges from 10 to 100 (100 ms to 1000 ms). Unit: 10 ms Default value: 10 (100 ms)

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

- This command sets the power-off interval of PSTN users.
- This command can be executed only in H.248 AG user view.

Example

#Set the power-off interval to 200 ms.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] dc-time 20
```

16.7.2.7 detect-ansbar-by-single-tone

Function

The **detect-ansbar-by-single-tone** command configures the flag for enabling ANSbar signal detection based on the single tone (special modem process in Bahrain).

The **undo detect-ansbar-by-single-tone** command deletes the flag for enabling ANSbar signal detection based on the single tone (special modem process in Bahrain).

Format

detect-ansbar-by-single-tone [*detect-ansbar-by-single-tone-value*]

undo detect-ansbar-by-single-tone

Parameters

Parameter	Description	Value
detect-ansbar-by-single-tone-value	Specifies the flag for enabling ANSbar signal detection based on the single tone (special modem process in Bahrain).	The value can be **enable** or **disable**. Default value: disable

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

- This command enables or disables ANSbar signal detection based on the single tone for an existing PSTN user.
- This command can be executed only in H.248 AG user view.

Example

#Enable ANSbar signal detection based on the single tone.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] detect-ansbar-by-single-tone enable
```

16.7.2.8 display voice h248aguser

Function

The **display voice h248aguser** command displays the information about all H.248 AG users.

Format

display voice h248aguser

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

#Display the information about all H.248 AG users.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice h248aguser
S /SC/P MGID TerminalID
1 /0 /0 0 A0
1 /0 /1 0 A1
3 /0 /0 0 A300
4 /0 /0 0 A400
```

 Copyright © Huawei Technologies Co., Ltd.

Table 16-145 Parameters in the display voice h248aguser command output

Parameter	Description
S	Slot ID of an H.248 user
SC	Subcard ID of an H.248 user.
P	Port ID of an H.248 user.
MGID	H.248 interface ID of an H.248 user.
TerminalID	Terminal ID.

16.7.2.9 display voice h248aguser bra

Function

The **display voice h248aguser bra** command displays basic rate access (BRA) user information.

Format

display voice h248aguser bra { *mgid terminalID* [*spanarea*] | **attribute** *username* | *username* }

Parameters

Parameter	Description	Value
mgid	Specifies the ID of the interface that a user belongs to.	The value is an integer that ranges from 0 to 16777215.
username	Specifies the user name.	The value is a string. Value format: *slot/subcard/port*
terminalID	Specifies the terminal ID.	The value is an integer that ranges from 0 to 9999.
spanarea	Specifies the terminal range.	The value is an integer that ranges from 1 to 10000. Default value: 1

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display BRA user information.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice h248aguser bra 0 0 500
-------------------------------------------------------------------------------
S /SC/P /B MGID LinkSetNo UserIFID TelNo Priority TerminalID
-------------------------------------------------------------------------------
 4 /0 /0 /0 0 0 400 - Cat3 A400
```

Table 16-146 Parameters in the display voice h248aguser bra command output

Parameter	Description
S	Slot ID of a BRA user.
SC	Subcard ID of a BRA user.
P	Port ID of a BRA user.
B	B channel ID.
Linkset	IUA link set of a BRA user.
UserIFID	Interface ID of a BRA user.
TelNo	Phone number of a BRA user.
Priority	Priority of a BRA user.
TerminalID	Terminal ID.

16.7.2.10 display voice h248aguser pots

Function

The **display voice h248aguser pots** command displays PSTN user information.

Format

display voice h248aguser pots { *mgid terminalID* [*spanarea*] | **attribute** { *mgid terminalID* [*spanarea*] | *username* } | *username* }

Parameters

Parameter	Description	Value
mgid	Specifies the ID of the interface that a user belongs to.	The value is an integer that ranges from 0 to 16777215.
username	Specifies the user name.	The value is a string. Value format: *slot/subcard/port*
terminalID	Specifies the terminal ID.	The value is an integer that ranges from 0 to 9999.
spanarea	Specifies the terminal range.	The value is an integer that ranges from 1 to 10000. Default value: 1

Views

All views

Default Level

2: Configuration level

Usage Guidelines

None

Example

Display POTS user information.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice h248aguser pots 0 0 100
-------------------------------------------------------------------------------
 S /SC/P MGID TelNo Priority PotsLineType TerminalID
-------------------------------------------------------------------------------
 1 /0 /0 0 - Cat3 DEL A0
 1 /0 /1 0 - Cat3 DEL A1
```

Table 16-147 Parameters in the display voice h248aguser pots command output

Parameter	Description
S	Slot ID of a POTS user.
SC	Subcard ID of a POTS user.

Parameter	Description
P	Port ID of a POTS user.
MGID	H.248 interface ID.
TelNo	Phone number of a POTS user.
Priority	Priority of a POTS user.
PotsLineType	Line type of a POTS user.
TerminalID	Terminal ID.

16.7.2.11 display voice h248aguser pra

Function

The **display voice h248aguser pra** command displays PRA user information.

Format

display voice h248aguser pra { **all** | **attribute** *username* | *username* }

Parameters

Parameter	Description	Value
all	Specifies all the users.	-
attribute	Specifies the designated user.	-
username	Specifies the user name.	The value is a string. Value format: *slot/subcard/port.*

Views

All views

Default Level

2: Configuration level

Usage Guidelines

To display PRA user information, run **display voice h248aguser pra** command.

Example

Display PRA user information.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice h248aguser pra attribute 3/0/0
-----------------------------------------------------------------
 F /S /P : 3 /0 /0
 UNIreport : disable
 Prior : Cat3
 Mask of sub channel : 255.255.255.255
 Auto reservice times/limit : 0/20
 Powerdialer : enable
```

Table 16-148 Parameters in the **display voice h248aguser pots** command output

Parameter	Description
F /S /P	Subrack ID/Slot ID/Port ID of a port.
UNIreport	Flag for reporting UNI faults. Options: enable and disable
Prior	Terminal priority. Options: cat1, cat2, and cat3
Mask of sub channel	Sub-channel mask.
Auto reservice times/limit	Automatic in-service count/Automatic in-service limit.
Powerdialer	Malicious call detection.

16.7.2.12 display voice iua-link

Function

The **display voice iua-link** command displays configurations on an IUA link.

Format

display voice iua-link sctp { **protocol** { **running** | **config** } | **association** { **info** | **statistics** } } *linkno*

Parameters

Parameter	Description	Value
linkno	Specifies the ID of an IUA link.	The value is an integer that ranges from 0 to 15.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to query the configuration of an IUA link.

Example

Display the configuration of an IUA link.

```
<Huawei> display voice iua-link sctp protocol config 0
  In streams              : 33
  Out streams             : 33
  Minimum rto value       : 1000ms
  Maximum rto value       : 60000ms
  Initial rto value       : 1000ms
  Rto alpha parameter     : 12%
  Rto beta parameter      : 25%
  Heartbeat interval      : 30000ms
  Valid cookie lifetime   : 60000ms
  Maximum init retrans    : 8
  Association maxretrans  : 10
  Path maximum retrans    : 5
  No congestion level     : 40%
  Low congestion level    : 60%
  High congestion level   : 80%
  Send checksum           : yes
  Receive checksum        : yes
  Checksum arithmetic     : CRC32
```

Table 16-149 Description of the **display voice iua-link sctp** command output

Parameter	Description
In streams	Indicates the number of incoming SCTP streams.
Out streams	Indicates the number of outgoing SCTP streams.
Minimum rto value	Indicates the minimum retransmission time-out duration.
Maximum rto value	Indicates the maximum retransmission time-out duration.
Initial rto value	Indicates the initial value of the retransmission time-out duration.
Valid cookie lifetime	Indicates the life cycle of the valid cookie.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
Heartbeat interval	Indicates the heartbeat interval.
Maximum init retrans	Indicates the maximum init retransmission count.
Rto alpha parameter	Indicates the retransmission time-out duration factor α.
Rto beta parameter	Indicates the retransmission time-out duration factor β.
No congestion level	Indicates the no congestion level.
Low congestion level	Indicates the low congestion level.
High congestion level	Indicates the high congestion level.
Send checksum	Indicates whether to send the checksum when sending messages. The query result can be: ● yes: send ● no: Not send
Receive checksum	Indicates whether to receive the checksum when receiving messages. The query result can be: ● yes: receive ● no: not receive
Checksum arithmetic	Indicates the checksum algorithm.

Related Topics

16.7.3.9 iua-link

16.7.2.13 display voice iua-linkset

Function

The **display voice iua-linkset** command displays configurations on an IUA link set.

Format

display voice iua-linkset { **state** | **attribute** | **statistics** } *linksetno*

Parameters

Parameter	Description	Value
state	Displays status information about an IUA link set.	-
attribute	Displays basic information about an IUA link set.	-
statistics	Displays statistical information about an IUA link set.	-
linksetno	Specifies the ID of an IUA link set. This parameter is mandatory.	The value is an integer that ranges from 0 to 15.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to query the configuration of an IUA link set.

Example

Display the configuration of an IUA link set.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sigtran
[Huawei-voice-sigtran] display voice iua-linkset attribute 0
  LinksetNo            :0
  MGID                 :-
  PendingTime          :50
  TrafficMode          :override
  C/S-Mode             :server
  IID-Type             :integer
  IID-Map              :1
  BRA IID-Prefix       :-
  BRA IID-Suffix       :-
  PRA IID-Prefix       :-
  PRA IID-Suffix       :-
  Jointly-Work         :disable
```

Table 16-150 Description of the **display voice iua-linkset** command output

Parameter	Description
LinksetNo	Linkset ID.
MGID	Indicates the corresponding MG interface ID of the IUA link set. In the case of a SIP protocol, this parameter is not displayed. If MGID is not specified in adding the link set, this parameter is displayed as "-".
PendingTime	Indicates the pending duration of the IUA link set.
TrafficMode	Indicates the working mode of an IUA link set. The query result can be: ● override: active/standby mode ● loadshare: load sharing mode
C/S-Mode	Indicates the corresponding service environment of the IUA link set. The query result can be: ● server: The link set is configured at the server side. ● client: The link set is configured at the client side.
IID-Type	Indicates the corresponding interface ID type of the IUA link set.
IID-Map	Indicates the mode of generating the identifier corresponding to the IUA link set.
Jointly-Work	Indicates whether the IUA link supports the interlocking. If the system supports only one protocol, the parameter is visible only when the system protocol is H.248. The parameter is displayed as disable if the link does not switch over in the H.248 protocol or SIP protocol.
BRA IID-Prefix	Indicates the bra prefix of the interface ID of the IUA link set.
BRA IID-Suffix	Indicates the bra suffix of the interface ID of the IUA link set.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description
PRA IID-Prefix	Indicates the pra prefix of the interface ID of the IUA link set.
PRA IID-Suffix	Indicates the pra suffix of the interface ID of the IUA link set.

Related Topics

16.7.3.14 iua-linkset

16.7.2.14 dsp-input-gain

Function

The **dsp-input-gain** command configures the input gain of a DSP chip.

The **undo dsp-input-gain** command deletes the input gain configured for a DSP chip.

Format

dsp-input-gain *dsp-input-gain-value*

undo dsp-input-gain

Parameters

Parameter	Description	Value
dsp-input-gain-value	Specifies the input gain of a DSP chip. This parameter is optional. Set this parameter when you need to configure the input gain of a DSP chip. The input gain refers to the gain from the PCM side to IP side. By configuring the gain, you can adjust the voice quality.	The value is an integer that ranges from 0 to 15 (–10 dB to +5 dB). Default value: 10 (0 dB)

Views

H.248 AG user view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command configures the input gain of a DSP chip.

Example

#Specify the input gain of a DSP chip to +5 dB.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] dsp-input-gain 15
```

16.7.2.15 dsp-output-gain

Function

The **dsp-input-gain** command configures the output gain of a DSP chip.

The **undo dsp-output-gain** command deletes the output gain configured for a DSP chip.

Format

dsp-output-gain *dsp-output-gain-value*

undo dsp-output-gain

Parameters

Parameter	Description	Value
dsp-output-gain-value	Specifies the output gain of a DSP chip. This parameter is optional. Set this parameter when you need to configure the output gain of a DSP chip. The output gain refers to the gain from the IP side to PCM side. By configuring the gain, you can adjust the voice quality.	The value is an integer that ranges from 0 to 20 (–10 dB to +10 dB). Default value: 10 (0 dB)

Views

H.248 AG user view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command configures the output gain of a DSP chip.

Example

#Specify the output gain of a DSP chip to +10 dB.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] dsp-output-gain 20
```

16.7.2.16 dsp-template

Function

The **dsp-template** command configures the DSP parameter template name.

The **undo dsp-template** command deletes the DSP parameter template name.

Format

dsp-template *dsp-template-name*

undo dsp-template

Parameters

Parameter	Description	Value
dsp-template-name	Specifies the DSP parameter template name. You can set the work mode parameter to **FAX** or **MODEM** for a DSP parameter template only when the fax or modem negotiation mode is local switch. If you use the template in the IMS negotiation mode, the function may be unavailable.	The value is a string of 1 to 31 characters. Default value: a hyphen (-), indicating that no DSP parameter template is set.

Views

H.248 AG user view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command specifies an existing DSP parameter template to users.

Example

#Name the DSP parameter template **1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] dsp-template 1
```

16.7.2.17 endservice

Function

The **endservice** command terminates user services.

The **undo endservice** command restores user services.

Format

endservice { **immediate** | **defer** [**maxcobtime** maxcobtime [**onexpire** [forced | cancel]]] }

undo endservice

Parameters

Parameter	Description	Value
immediate	Indicates the mode that the port immediately quits the services.	-
defer	Indicates the mode that the port delays quitting the services. When this mode is used, the port quits the services normally if the services on the port are terminated within the delay duration; otherwise, the services are processed in the corresponding way after the delay duration.	-

Parameter	Description	Value
maxcobtime *maxcobtime*	Indicates the maximum delay duration within which the port delays quitting the services. When the mode that the port delays quitting the services is used, this parameter is used to specify the maximum duration for the system to wait for the services on the port. If the port does not quit services after this duration, the system processes the services in the corresponding way specified for the case where the delay duration times out.	Numeral type. Range: 1-1440. Unit: minute. Default value: 240.
onexpire	Indicates processing way specified for the case where the delay duration times out. ● forced: The port is forced to quit the services. When the mode in which the port delays quitting the services is used, the port is forced to quit the services after the delay duration. ● cancel: The operation that the port quits the services is canceled. When the mode in which the port delays quitting the services is used, the port does not quit the services after the delay duration.	Enumerated type. Options: forced and cancel. Default value: forced.

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command terminates user services.

Example

Terminate services of a specified user group.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] endservice
```

16.7.2.18 force-sendfsk

Function

The **force-sendfsk** command configures the forcibly sent FSK flag.

The **undo force-sendfsk** command deletes the forcibly sent FSK flag.

Format

force-sendfsk *force-sendfsk-value*

undo force-sendfsk

Parameters

Parameter	Description	Value
force-sendfsk-value	Specifies the forcibly sent FSK flag. This parameter is optional. Set this parameter when you need to modify the forcibly sent FSK flag.	The value can be **enable** or **disable**. Default value: disable

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the forcibly sent FSK flag of an existing PSTN user.

Example

#Enable the forcibly sent FSK flag.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] force-sendfsk enable
```

16.7.2.19 fsk-mode

Function

The **fsk-mode** command configures the FSK CLIP mode.

The **undo fsk-mode** command deletes the FSK CLIP mode.

Format

fsk-mode *fsk-mode*

undo fsk-mode

Parameters

Parameter	Description	Value
fsk-mode	Specifies the FSK CLIP mode. This parameter is optional. CCITT_V23 is a special mode for Telecom Austria.	The value can be **BELL_202**, **CCITT_V23**, or **NTT**. Default value: BELL_202

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the FSK CLIP mode of an existing PSTN user.

Example

#Set the FSK CLIP mode to **ntt**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] fsk-mode ntt
```

16.7.2.20 fsk-time

Function

The **fsk-time** command configures the FSK delay.

The **undo fsk-time** command deletes the FSK delay.

Format

fsk-time *fsk-time-value*

undo fsk-time

Parameters

Parameter	Description	Value
fsk-time-value	Specifies the FSK delay. This parameter is optional. Set this parameter when you need to configure the FSK delay for PSTN users.	The value is an integer that ranges from 0 to 100 (0 ms to 1000 ms). Unit: 10 ms Default value: 80 (800 ms)

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the FSK delay of an existing PSTN user.

Example

#Set the FSK delay to 200 ms.

```
<Huawei> system-view
[Huawei] voice
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] fsk-time 20
```

16.7.2.21 h248aguser

Function

The **h248aguser** command adds a H248 AG user or displays the H248 AG user view (if the user exists).

The **undo h248aguser** command deletes a H248 AG user.

By default, no H248 AG user is created.

Format

h248aguser *slotid|subcard|portid* [**agid** *agid* [**terminalid** *terminalid* **linksetno** *linksetno* **interfaceid** *interfaceid*] *]

Parameters

Parameter	Description	Value
slotid|subcard|portid	Specifies the user name in the *slot/subcard/port* format.	The value is a string of 1 to 15 characters.
agid *agid*	Specifies the ID of the interface that a user belongs to.	The value is an integer that ranges from 1 to 16777215.
terminalid *terminalid*	Specifies the terminal ID.	The value is an integer that ranges from 0 to 9999.
linksetno *linksetno*	Specifies the link set that a user belongs to. This parameter is required only for ISDN users.	The value is an integer that ranges from 0 to 15.
interfaceid *interfaceid*	Specifies the interface that a user belongs to. This parameter is required only for ISDN users.	The value is an integer that ranges from 0 to 65535.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

This command adds a H248 AG user or displays the H248 AG user view (if the user exists).

Example

Create a H248 AG user.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0 ag 0
```

16.7.2.22 line-type

Function

The **line-type** command sets the line type of PSTN users.

The **undo line-type** command deletes the line type of PSTN users.

Format

line-type *line-type*

undo line-type

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
line-type	Specifies the line type of PSTN users. Set this parameter based on the actual PSTN line type. Currently, the following line types are available: ● Direct Exchange Line (DEL) ● Earth Calling PBX (ECPBX) ● Loop Calling PBX (LCPBX) ● Pay Phone (PayPhone) Device ports of DEL users are directly connected to user lines. Device ports of PBX users are connected to user lines through the PBX. Device ports of PayPhone users are connected to charging terminals.	The value can be **DEL**, **ECPBX**, **LCPBX**, or **PayPhone**. Default value: DEL

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command sets the line type of PSTN users.

Example

#Set the user line type to **ECPBX**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] line-type ecpbx
```

 Copyright © Huawei Technologies Co., Ltd.

16.7.2.23 priority

Function

Using the **priority** command, you can configure the priority for a H248 AG user.

Using the **undo priority** command, you can restore the default priority of a H248 AG user.

By default, the priority of a H248 AG user is **cat3**.

Format

priority *priority*

undo priority

Parameters

Parameter	Description	Value
priority	Specifies the user priority. This parameter is optional. Set this parameter when you need to specify the priority for a new user. The options are as follows: ● cat1: category-1 user priority ● cat2: category-2 user priority ● cat3: normal (common user)	The value can be **cat1**, **cat2**, or **cat3**. Default value: cat3

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to configure the H248 AG user priority. Priorities are **cat1**, **cat2**, **cat3** in a descending order.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the SIP AG user priority to **cat1**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser-1/0/0
[Huawei-voice-h248aguser-1/0/0] priority cat1
```

16.7.2.24 power-dialer

Function

The **power-dialer** command configures malicious calling user detection for ISDN users.

Format

power-dialer *flag*

undo power-dialer

Parameters

Parameter	Description	Value
flag	Specifies malicious calling user detection. This parameter indicates whether malicious calling user detection is supported. The options are as follows: ● enable: enables malicious calling user detection. ● disable: disables malicious calling user detection.	The value can be **enable** or **disable**. Default value: enable

Views

ISDN user view

Default Level

2: Configuration level

Usage Guidelines

This command configures malicious calling user detection for ISDN users.

Example

Enable malicious calling user detection.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] power-dialer enable
```

16.7.2.25 tas-pattern

Function

The **tas-pattern** command configures the TAS CLIP mode.

The **undo tas-pattern** command disables the TAS CLIP mode.

Format

tas-pattern [*tas-pattern-value*]

undo tas-pattern

Parameters

Parameter	Description	Value
tas-pattern-value	Specifies the TAS CLIP mode. This parameter is optional.	The value can be **NO-TAS** or **DT-AS**. Default value: NO-TAS

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the TAS CLIP mode of an existing PSTN user.

Example

#Set the TAS CLIP mode to **NO-TAS**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] tas-pattern NO-TAS
```

 Copyright © Huawei Technologies Co., Ltd.

16.7.2.26 telno

Function

The **telno** command configures a user's emergency standalone number.

Format

telno *telno*

undo telno

Parameters

Parameter	Description	Value
telno	Specifies the phone number.	The value is a string of 1 to 15 digits.

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command configures the emergency standalone number for an existing user.

Example

Set the emergency standalone number for an existing user to 123456.

```
<Huawei>system-view
[Huawei] voice
[Huawei-voice] h248aguser-1/0/0
[Huawei-voice-h248aguser-1/0/0]telno 123456
```

16.7.2.27 uni-report

Function

Using the **uni-report** command, you can enable or disable the function that reports user network interface (UNI) faults.

Using the **undo uni-report** command, you can restore the default status of the UNI fault reporting function.

By default, the UNI fault reporting function is **disabled**.

 Copyright © Huawei Technologies Co., Ltd.

Format

uni-report *flag*

undo uni-report

Parameters

Parameter	Description	Value
flag	Specifies the flag for reporting UNI faults to ISDN PRA users. Set this parameter to enable or disable the function of reporting UNI faults to ISDN PRA users.	The value can be **enable** or **disable**. Default value: disable

Views

H.248 AG view

Default Level

2: Configuration level

Usage Guidelines

Set this parameter to enable or disable the function of reporting UNI faults to ISDN PRA users.

Example

Enable the UNI fault reporting function.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser-1/0/0
[Huawei-voice-h248aguser-1/0/0]uni-report enable
```

16.7.2.28 vqe-agc

Function

The **vqe-agc** command configures the VQE automatic gain flag.

The **undo vqe-agc** command deletes the VQE automatic gain flag.

Format

vqe-agc [*vqe-agc*]

undo vqe-agc

Parameters

Parameter	Description	Value
vqe-agc	Specifies the VQE automatic gain flag. This parameter is optional. Set this parameter when you need to modify the VQE automatic gain flag.	The value can be **enable** or **disable**. Default value: disable

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the VQE automatic gain flag of an existing PSTN user.

Example

#Enable the VQE automatic gain flag.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] vqe-agc enable
```

16.7.2.29 vqe-agc-level

Function

The **vqe-agc-level** command configures the target value for VQE automatic gain.

The **undo vqe-agc-level** command deletes the target value for VQE automatic gain.

Format

vqe-agc-level [*levelvalue*]

undo vqe-agc-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
levelvalue	Specifies the target value for VQE automatic gain. This parameter is optional. Set this parameter when you need to modify the target value for VQE automatic gain.	The value is an integer that ranges from 0 to 15 (-9 dBm0 to -24 dBm0). Default value: 13 (-22 dBm0)

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the target value for VQE automatic gain of an existing PSTN user.

Example

#Set the target value for VQE automatic gain to -19 dBm0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] vqe-agc-level 10
```

16.7.2.30 vqe-sns

Function

The **vqe-sns** command configures the VQE noise suppression flag.

The **undo vqe-sns** command deletes the VQE noise suppression flag.

Format

vqe-sns [*vqe-sns*]

undo vqe-sns

Parameters

Parameter	Description	Value
vqe-sns	Specifies the VQE noise suppression flag. This parameter is optional. Set this parameter when you need to modify the VQE noise suppression flag.	The value can be **enable** or **disable**. Default value: disable

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the VQE noise suppression flag of an existing PSTN user.

Example

#Enable the VQE noise suppression flag.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] vuq-sns enable
```

16.7.2.31 vqe-sns-level

Function

The **vqe-sns-level** command configures the VQE noise suppression value.

The **undo vqe-sns-level** command deletes the VQE noise suppression value.

Format

vqe-sns-level [*levelvalue*]

undo vqe-sns-level

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
levelvalue	Specifies the VQE noise suppression value. This parameter is optional. Set this parameter when you need to modify the VQE noise suppression value.	The value is an integer that ranges from 6 to 20. Unit: dB Default value: 12

Views

H.248 AG user view

Default Level

2: Configuration level

Usage Guidelines

This command is used to configure the VQE noise suppression value of an existing PSTN user.

Example

#Set the VQE noise suppression value to 10 dB.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248aguser 1/0/0
[Huawei-voice-h248aguser-1/0/0] vqe-sns-level 10
```

16.7.3 H.248 AG Common Commands

Description

This topic describes H.248 AG common configuration commands.

16.7.3.1 display voice fax-modem

Function

The **display voice fax-modem** command displays settings of fax, modem, and public parameters.

Format

display voice fax-modem

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command displays settings of fax, modem, and public parameters.

Example

Display the settings of fax, modem, and public parameters.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice fax-modem
  ------------------------------------------------------------------------------
  FAX transfers mode                    : throughly
  T38 Fax Port                        : RTP port
  FAX flow                           : V5 Flow
  ------------------------------------------------------------------------------
  MODEM transfers mode                   : -
  MODEM event mode                      : Direct
  ------------------------------------------------------------------------------
  Negomode                            : Negotiation
  Packet-interval-10ms                  : Disable
  Rfc2198-start-mode                    : Disable Rfc2198SmartStartup
  TransEvent                         : ControlledByMGC
  Vbd-codec                          : G.711A
  Vbd-payload-type                      : Static
  ------------------------------------------------------------------------------
```

Table 16-151 Description of the **display voice fax-modem** command output

Item	Description
FAX transfers mode	Fax codec mode. The options are as follows: ● throughly: transparent mode. ● T.38: T.38 mode.
T38 Fax Port	T.38 fax port. The options are as follows: ● RTP port: voice port number. ● RTP port+2: voice port number + 2.
FAX flow	Fax negotiation process. The options are as follows: ● V2 Flow: V2 process (self negotiation process). ● V3 Flow: V3 process. ● V5 Flow: V5 process.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MODEM transfers mode	Modem transfer mode. The options are as follows: ● throughly: transparent mode. ● Relay: relay mode.
MODEM event mode	Mode for reporting modem events. The options are as follows: ● Delay: buffer reporting mode. ● Direct: direct reporting mode. ● Direct for high-speed signals: high-speed signal immediate reporting mode.
Negomode	Codec negotiation mode. Codec negotiation modes include local switch and negotiation modes. In the negotiation mode, the MG uses signaling to negotiate the codec with the MGC. The local switch does not have this process. The value can be **selfswitch** or **negotiation**. ● selfswitch: local switch mode. ● negotiation: negotiation mode. Default value: negotiation
Packet-interval-10ms	Flag for enabling the 10 ms packing function. The 10 ms packing function improves the stability of the fax and modem services but occupies more bandwidth resources. The value can be **enable** or **disable**. ● enable: The 10 ms packing function is enabled. ● disable: The 10 ms packing function is disabled. Default value: disable

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rfc2198-start-mode	Flag for enabling the RFC 2198 smart start function. The RFC 2198 smart start function ensures that RFC 2198 redundant transmission automatically starts when packet loss occurs. RFC 2198 improves message reliability by sending redundant packets and ensures the service quality when the network quality is poor. To use this function, both the sending and receiving parties must enable this function; otherwise, faxes cannot be sent or received properly. When connecting the device to devices from other vendors, you must ensure that the RFC 2198 parameters are consistent on both ends. The value can be **DisableRfc2198SmartStartup**, **EnableRfc2198SmartStartup**, or **ImmediatelyStartupRFC2198**. ● DisableRfc2198SmartStartup: The RFC 2198 smart start function is disabled. ● EnableRfc2198SmartStartup: The RFC 2198 smart start function is enabled. When packet loss occurs, the system automatically starts RFC 2198 redundant transmission. ● ImmediatelyStartupRFC2198: The system immediately starts RFC 2198 redundant transmission. Default value: DisableRfc2198SmartStartup
TransEvent	Mode for sending fax or modem events. This parameter is optional. Set this parameter when you need to set the mode for sending fax or modem events. The value can be **ControlledByMGC** or **RFC2833**. ● ControlledByMGC: softswitch control mode. By default, transparent transmission is used. ● RFC2833: RFC 2833 transmission mode (self control). Default value: ControlledByMGC
Vbd-codec	VBD codec mode. This parameter is optional. Set this parameter when you need to set the VBD codec mode. The value can be **G.711A** or **G.711U**. Default value: G.711A

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Vbd-payload-type	VBD payload type. This parameter is optional. Set this parameter when you need to set the VBD payload type. The value can be **static** or **dynamic**. ● static: static payload. ● dynamic: dynamic payload. Default value: static

Related Topics

16.7.3.6 fax-modem common
16.7.3.7 fax-modem fax
16.7.3.8 fax-modem modem

16.7.3.2 display voice media-bandwidth-control

Function

Using the **display voice media-bandwidth-control** command, you can view the call restriction configuration when the uplink bandwidth is insufficient.

Format

display voice media-bandwidth-control

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display voice media-bandwidth-control** command only after the **media-bandwidth-control enable** command is executed to enable the call restriction function when the uplink bandwidth is insufficient.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the call restriction configuration when the uplink bandwidth is insufficient.

```
<Huawei> display voice media-bandwidth-control
 Upward bandwidth                          : disable
 The maximum upward bandwidth              : 100000 kbit/s
 The reserved bandwidth for emergency call : 1000 kbit/s
 The used normal bandwidth                 : 0 kbit/s
 The used bandwidth for emergency call     : 0 kbit/s
```

Table 16-152 Description of the display voice upward-bandwidth command output

Item	Description
Upward bandwidth	Whether call restriction is enabled when the uplink bandwidth is insufficient. ● enable: call restriction is enabled when the uplink bandwidth is insufficient. ● disable: call restriction is disabled when the uplink bandwidth is insufficient.
The maximum upward bandwidth	Maximum uplink bandwidth.
The reserved bandwidth for emergency call	Reserved bandwidth for emergency calls.
The used normal bandwidth	Used bandwidth.
The used bandwidth for emergency call	Used bandwidth for emergency calls.

16.7.3.3 display voice rfc2198

Function

The **display voice rfc2198** command displays the upper limit of the packet loss rate and the number of RFC 2198 redundant packets at each of the four stages.

Format

display voice rfc2198 smart-parameters

Parameters

Parameter	Description	Value
smart-parameters	Displays the upper limit of the packet loss rate and the number of RFC 2198 redundant packets at each of the four stages.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command displays the upper limit of the packet loss rate and the number of RFC 2198 redundant packets at each of the four stages.

Example

Display the upper limit of the packet loss rate and the number of RFC 2198 redundant packets at each stage.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice rfc2198 smart-parameters
  ------------------------------------------------------------------------------
  Section                        : first
  Up-threshold                       : 20
  Redundant-num                          : 3
  ------------------------------------------------------------------------------
  Section                        : second
  Up-threshold                       : 30
  Redundant-num                          : 1
  ------------------------------------------------------------------------------
  Section                        : third
  Up-threshold                       : 50
  Redundant-num                          : 2
  ------------------------------------------------------------------------------
  Section                        : fourth
  Up-threshold                       : 1000
  Redundant-num                          : 3
  ------------------------------------------------------------------------------
```

Table 16-153 Description of the **display voice rfc2198 smart-parameters** command output

Parameter	Description
Section	Stage.

Parameter	Description
Up-threshold	Upper limit of the packet loss rate.
Redundant-num	Number of redundant packets.

16.7.3.4 display voice tid-template

Function

The **display voice tid-template** command displays basic information about one or all TID templates.

Format

display voice tid-template [*index*]

Parameters

Parameter	Description	Value
index	Specifies the index of a TID template. If this parameter is not set, basic information about all TID templates is displayed.	The value is an integer that ranges from 0 to 63.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command displays basic information about one or all TID templates.

Example

Display basic information about TID template 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] display voice tid-template 1
  Index      : 1
  Format     : %u
  Para-list  : R+100000001
  Name       : Rtp_No_Delamination
```

Parameter	Description
Index	TID template index.
Format	TID template format.
Para-list	Parameter list.
Name	TID template name.

Related Topics

16.7.3.19 tid-template
16.7.3.20 tid-template-modify

16.7.3.5 h248ag

Function

The **h248ag** command creates a H248 AG interface and displays the H248 AG interface view.

The **undo h248ag** command deletes a H248 AG interface.

By default, no H248 AG interface is created.

Format

h248ag *mg-id*

undo h248ag *mg-id*

Parameters

Parameter	Description	Value
mg-id	Specifies the interface ID of a H248 AG.	The value is an integer that ranges from 0 to 16777215.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

When a H248 AG is required to communicate with the remote device, use the **h248ag** command to create a H248 AG interface. If the specified H248 AG

 Copyright © Huawei Technologies Co., Ltd.

interface exists, the H248 AG interface view is displayed. After creating a H248 AG interface, you can configure attributes, control points, and protocol stack parameters for the H248 AG interface. When deleting a H248 AG interface, pay attention to the following points:

- Before deleting a H248 AG interface, delete all the user number configured on the H248 AG interface.
- Before deleting a H248 AG interface, disable H248 AG interface.
- When a H248 AG interface is deleted, configurations of the H248 AG interface including ring mappings and control points are deleted.

Example

Create H248 AG 1.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] h248ag 1
[Huawei-voice-h248ag-1]
```

Related Topics

16.7.1.7 display voice h248ag

16.7.3.6 fax-modem common

Function

The **fax-modem common** command sets public parameters for an MG. If the MG supports fax and modem services, you must run this command to the set public fax and modem parameters. After the parameters are set, the fax machine and modem work in the specified mode.

Format

fax-modem common { **negomode** *negomode-value* | **packet-interval-10ms** *packet-interval-10ms-value* | **transevent** *transevent-value* | **vbd-codec** *vbd-codec-value* | **vbd-pt-type** *vbd-pt-type-value* | rfc2198-start-mode rfc2198-start-mode }

undo fax-modem common { **negomode** | **packet-interval-10ms** | **transevent** | **vbd-codec** | **vbd-pt-type** | rfc2198-start-mode }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
negomode-value	Specifies the codec negotiation mode. Codec negotiation modes include local switch and negotiation modes. In the negotiation mode, the MG uses signaling to negotiate the codec with the MGC. The local switch mode does not have this process.	The value can be **selfswitch** or **negotiation**. ● selfswitch: local switch mode. ● negotiation: negotiation mode. Default value: negotiation
packet-interval-10ms-value	Specifies the flag for enabling the 10 ms packing function. The 10 ms packing function improves the stability of the fax and modem services but occupies more bandwidth resources.	The value can be **enable** or **disable**. ● enable: enables the 10 ms packing function. ● disable: disables the 10 ms packing function. Default value: disable
transevent-value	Specifies the mode for sending fax or modem events. This parameter is optional. Set this parameter when you need to set the mode for sending fax or modem events.	The value can be **ControlledByMGC** or **RFC2833**. ● ControlledByMGC: softswitch control mode. By default, transparent transmission. ● RFC2833: the RFC 2833 transmission mode (self control). Default value: ControlledByMGC
vbd-codec-value	Specifies the VBD codec mode. This parameter is optional. Set this parameter when you need to set the VBD codec mode.	The value can be **G.711A** or **G.711U**. Default value: G.711A
vbd-pt-type-value	Specifies the VBD payload type. This parameter is optional. Set this parameter when you need to set the VBD payload type.	The value can be **static** or **dynamic**. ● static: static payload. ● dynamic: dynamic payload. Default value: static

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rfc2198-start-mode	Indicates the flag of enabling the RFC2198 intelligent enabling function. The RFC2198 intelligent enabling function ensures that the RFC2198 redundancy transmission is enabled automatically when the packet loss occurs in the network. RFC2198 defines redundant transmission, which is used to improve the reliability of data transmission and to ensure service quality in the case of poor network conditions. Redundant transmission must be enabled on both the receiver and transmitter. Otherwise, the fax service is abnormal. Ensure that RFC2198 parameters are consistent when the modem is interconnected with devices from another manufacturer.	Enumerated type. Options: DisableRfc2198SmartStartup, EnableRfc2198SmartStartup, and ImmediatelyStartupRFC2198. ● DisableRfc2198SmartStartup: The RFC2198 intelligent enabling function is disabled. ● EnableRfc2198SmartStartup: The RFC2198 intelligent enabling function is enabled (When the packet loss occurs in the network, the RFC2198 redundancy transmission is enabled automatically.) ● ImmediatelyStartupRFC2198: The RFC2198 intelligent enabling function is immediately enabled. Default value: DisableRfc2198SmartStartup.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Run this command when you need to configure the fax and modem functions for the MG.

Example

Configure the fax codec negotiation mode to **selfswitch**.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]fax-modem common negomode selfswitch
```

Related Topics

16.7.3.8 fax-modem modem

16.7.3.7 fax-modem fax

16.7.3.7 fax-modem fax

Function

The **fax-modem common** command sets fax parameters. If the MG supports the fax service, you must run this command to the set fax parameters. After the parameters are set, the fax machine works in the specified mode.

Format

fax-modem fax { **is-port+2** *portvalue* | **transmission-mode** *mode* | **flow** *flowvalue* }

undo fax-modem fax { **is-port+2** | **transmission-mode** | **flow** }

Parameters

Parameter	Description	Value
portvalue	Specifies the T.38 fax port. Set this parameter when the fax transmission mode is set to self negotiation T.38. The value must be the same as the T.38 fax port configured on the peer MG.	The value is an integer that ranges from 0 to 1. ● 0: voice port number. ● 1: voice port number + 2. Default value: 0
mode	Specifies the fax codec mode. Fax codec modes include transparent and T.38 mode. The fax transmission mode is based on two aspects: codec mode (transparent or T.38) and MGC involvement. This parameter determines the codec mode. If the codec is G.711, the transparent mode is used. T.38 is a dedicated fax codec mode. The **flowvalue** parameter determines the MGC involvement.	The value can be **throughly** or **T.38**. ● throughly: transparent mode. ● T.38: T.38 mode. Default value: throughly

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
flowvalue	Specifies the fax negotiation process. The fax transmission mode is based on two aspects: codec mode (transparent or T.38) and MGC involvement. This parameter determines the MGC involvement. The **mode** parameter determines the codec mode.	The value can be **v2**, **v3**, or **v5**. ● v2: V2 process (self negotiation process). ● v3: V3 process. ● v5: V5 process. Default value: v3

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

If the MG supports the fax service, you must run this command to the set fax parameters.

Example

Configure the fax negotiation process to V5.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] fax-modem fax flow v5
```

Related Topics

16.7.3.6 fax-modem common

16.7.3.8 fax-modem modem

Function

The **fax-modem modem** command sets modem parameters for an MG. If the MG supports high-speed fax machines or modems, you must run this command to set modem parameters.

Format

fax-modem modem { **eventmode** *eventmode* | **tranmode** *tranmode* }

undo fax-modem modem { **eventmode** | **tranmode** }

Parameters

Parameter	Description	Value
eventmode	Specifies the mode for reporting modem events. Modes for reporting modem events include buffer reporting, direct reporting, and high-speed signal immediate reporting modes. ● Buffer reporting mode: When a modem event is received from the driver, the host does not report the modem event immediately. Instead, the host waits for the timeout duration and reports the modem event only when no fax event V21flag is reported within the duration. In this way, when high-speed transmission negotiation (modem mode to the host) fails on the high-speed fax machine, the low-speed transmission (fax mode to the host) can be used. ● Direct reporting mode: When a modem event is received from the driver, the host immediately reports the modem event to the MGC. ● High-speed signal immediate reporting mode: The host waits for 5.5s before reporting low-speed modem signals but immediately reports high-speed modem signals.	The value is an integer that ranges from 0 to 2. ● 0: buffer reporting mode. ● 1: direct reporting mode. ● 2: high-speed signal immediate reporting mode. Default value: 1

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tranmode	Specifies the modem transmission mode. Modem transmission modes include transparent transmission and relay modes. ● Transparent transmission mode: The G.711 codec is used, and modem signals are processed as common RTP data. The transparent transmission mode depends on the bearer network. If disconnection, low access rate, or instability occurs, you are advised to check the packet loss rate, delay, and jitter counters of the bearer network. ● Relay mode: also called redundancy mode. The gateway modulates modem signals, performs local error correction in most cases, and sends the modulated data to the peer gateway using a reliable transmission protocol. Currently, only the transparent transmission mode is supported.	The value is an integer that ranges from 0 to 1. ● 0: transparent transmission mode. ● 1: relay mode. Default value: 0

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Run this command when the MG needs to support devices such as high-speed fax machines and modems.

Example

Configure the mode for the MG to report modem events to buffer reporting.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]fax-modem modem eventmode 0
```

16.7.3.9 iua-link

Function

The **iua-link** command adds an IUA link or displays the IUA link view.

The **undo iualink** *linkno* command deletes an IUA link.

Format

iua-link *linkno linksetno localport* { *localipaddr* | **local-addr-name** *local-addr-name-value* } *remoteport remoteipaddr*1 [**remoteipaddr2** *remoteipaddr2* | **priority** *priority* | **jointly-work-with** *jointly-work-with*] *

undo iua-link *linkno*

Parameters

Parameter	Description	Value
linkno	Specifies the ID of an IUA link. This parameter is mandatory and uniquely identifies a link in an IUA link set. An IUA link set can have a maximum of two IUA links configured. The IDs of the two links must be two different values within the value range of **linkno**.	The value is an integer that ranges from 0 to 15.
linksetno	Specifies the ID of an IUA link set. This parameter is mandatory and identifies the IUA link to which you want to add an IUA link.	The value is an integer that ranges from 0 to 15.

Parameter	Description	Value
localipaddr	Specifies the local IP address. This parameter is optional. Set this parameter when you need to use a permanent local IP address. The value must be the same as the remote IP address configured on the MGC. In the same link set, the local IP addresses of links must be the same. Local port numbers, local IP addresses, remote port numbers, and remote IP addresses for different links cannot be all the same; otherwise, the link cannot be configured.	The value is an IP address in dotted decimal notation.
local-addr-name-value	Specifies the dynamic address name corresponding to the local IP address. This parameter is optional. Set this parameter when you need to obtain the local IP address using the dynamic address name. The dynamic address name must exist in the system.	The value is a string of 1 to 64 characters.
localport	Specifies the local port number. This parameter is mandatory and must be the same as the remote port number configured on the MGC so that the link can be activated properly. Local port numbers, local IP addresses, remote port numbers, and remote IP addresses for different links cannot be all the same; otherwise, the link cannot be configured.	The value is an integer that ranges from 1 to 65534.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remoteipaddr	Specifies the primary remote IP address. This parameter is mandatory and must be the same as the local IP address configured on the MGC. Local port numbers, local IP addresses, remote port numbers, and remote IP addresses for different links cannot be all the same; otherwise, the link cannot be configured. SCTP supports multihoming and can use multiple IP address to transmit data. This parameter configures the primary IP address.	The value is an IP address in dotted decimal notation.
remoteport	Specifies the remote port number. This parameter is mandatory and must be the same as the local port number configured on the MGC so that the link can be activated properly. Local port numbers, local IP addresses, remote port numbers, and remote IP addresses for different links cannot be all the same; otherwise, the link cannot be configured.	The value is an integer that ranges from 1 to 65534.
remoteipaddr2	Specifies the secondary remote IP address. This parameter is optional. Set this parameters when you need to configure the secondary remote IP address for the new IUA link. During the establishment of a connection, the primary path (primary IP address) is used first, and the secondary IP address is used only when the primary path is unreachable or retransmission is required.	The value is an IP address in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
priority	Specifies the priority of an IUA link. This parameter is optional and is valid when the IUA link set works in load balancing mode. In load balancing mode, the system selects current link based on the link priority and balances load among links with the same priority. The system select links with a lower priority only when all links with a higher priority are faulty. When links with a higher priority recover, the system switches services back to these links.	The value is an integer that ranges from 0 to 15. (A smaller value means a higher priority.) Default value: 0
jointly-work-with	Specifies the MGC bound to an IUA link, that is, specifies the MGC that the link jointly works with. This parameter is available only when the system protocol is H.248.	The value can be **primary-mgc** or **secondary-mgc**. ● primary-mgc: jointly works with the primary MGC. ● secondary-mgc: jointly works with the secondary MGC.

Views

SIGTRAN view

Default Level

2: Configuration level

Usage Guidelines

When you need to configure the system to support the communication between ISDN users and configure the link for ISDN users, run this command. After the link is configured, you can add the matched IUA link on the MGC, and then the link can be activated.

When you add links in an IUA link set, pay attention to the following points:

- Before adding a link, run the **iua-linkset add** command to add the matched link set. Otherwise, the link set to which the link belongs might not be used.
- For the local port number, local IP address, remote port number and remote IP address, ensure that at least one of them has different numbers among different links.

 Copyright © Huawei Technologies Co., Ltd.

- Only 2 links can be configured in the same link set.
- The local IP addresses of two links that belong to the same link set must be the same.

Example

Add an IUA link. Set the link ID to 0, link set ID to 9, local port number to 6666, local IP address to 192.168.1.209, remote port number to 6666, and remote IP address 1 to 10.10.10.1, and use default values for the other parameters.

```
<huawei> system
[huawei] voice
[huawei-voice] sigtran
[huawei-voice-sigtran] iua-link 0 0 6666 192.168.1.209 6666 10.10.10.1 priority 0
```

Related Topics

16.7.2.12 display voice iua-link

16.7.3.10 iua-link clear sctp association statistics

Function

The **iua-link clear sctp association statistics** command clears SCTP association statistics on an IUA link.

Format

iua-link clear sctp association statistics *linkno*

Parameters

Parameter	Description	Value
linkno	Specifies the ID of an IUA link. This parameter is mandatory and identifies the IUA link on which you want to clear SCTP association statistics.	The value is an integer that ranges from 1 to 15.

Views

SIGTRAN view

Default Level

2: Configuration level

Usage Guidelines

This command is used to clear the statistics of the Stream Control Transport Protocol (SCTP) association on an IUA link. An association refers to the logical relation (channel) for data transmission that is set up by two SCTP endpoints through the 4-way handshake mechanism of SCTP. When you need to clear the statistics of the SCTP association on an IUA link, run this command.

Example

Clear SCTP association statistics on IUA link 0.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sigtran
[huawei-voice-sigtran]iua-link clear sctp association statistics  0
```

16.7.3.11 iua-link clear statistics

Function

The **iua-link clear statistics** command clears statistical information about an IUA link.

Format

iua-link clear statistics *linkno*

Parameters

Parameter	Description	Value
linkno	Specifies the ID of an IUA link. This parameter is mandatory and uniquely identifies a link in an IUA link set.	The value is an integer that ranges from 1 to 15.

Views

SIGTRAN view

Default Level

2: Configuration level

Usage Guidelines

This command clears statistical information about an IUA link.

Example

Clear statistical information about IUA link 0.

```
<huawei> system
[huawei] voice
[huawei-voice] sigtran
[huawei-voice-sigtran] iua-link clear statistics 0
```

Related Topics

16.7.3.9 iua-link

16.7.3.12 iua-link lock

Function

The **iua-link lock** command locks an IUA link. If the link is a server link, the link is released when it is locked and the status is also locked so that the link cannot be reactivated. If the link is a client link, the link is directly released when it is locked.

The **undo iua-link lock** command unlocks an IUA link.

Format

iua-link lock *linkno*

undo iua-link lock *linkno*

Parameters

Parameter	Description	Value
linkno	Specifies the ID of an IUA link. This parameter is mandatory and identifies the IUA link that you want to lock or unlock.	The value is an integer that ranges from 1 to 15.

Views

SIGTRAN view

Default Level

2: Configuration level

Usage Guidelines

- After an IUA link is locked successfully, the link is released and link status is locked and cannot be activated again in the case of a server link, and the link is directly released in the case of a client link.

 Copyright © Huawei Technologies Co., Ltd.

- After an IUA link is unlocked, the locking status of the link is canceled and can be activated again in the case of a server link, and a link setup is initiated to activate the link.

Example

Lock IUA link 0.

```
<huawei> system
[huawei] voice
[huawei-voice] sigtran
[huawei-voice-sigtran] iua-link lock 0
[huawei-voice-sigtran] undo iua-link lock 0
```

Related Topics

16.7.3.9 iua-link

16.7.3.13 iua-link reset

Function

The **iua-link reset** command resets an IUA link. After SCTP protocol stack parameters for an IUA link are modified, you must run this command to reset the IUA link for the modifications to take effect. When an IUA link is reset, the link is reactivated.

Format

iua-link reset *linkno*

Parameters

Parameter	Description	Value
linkno	Specifies the ID of an IUA link. This parameter is mandatory and identifies the IUA link that you want to reset.	The value is an integer that ranges from 1 to 15.

Views

SIGTRAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After SCTP protocol stack parameters for an IUA link are modified, you must run this command to reset the IUA link for the modifications to take effect. When an IUA link is reset, the link is reactivated.

Example

Reset IUA link 0.

```
<huawei> system
[huawei] voice
[huawei-voice] sigtran
[huawei-voice-sigtran] iua-link reset 0
  This operation may interrupt the service of the IUA link, Are you sure? (y/n)[n]:y
```

Related Topics

16.7.3.9 iua-link

16.7.3.14 iua-linkset

Function

The **iua-linkset** command adds an IUA link set.

The **undo iua-linkset linksetno** command deletes an IUA link set.

Format

iua-linkset *linksetno* [**mgid** *mgid* [**jointly-work** *jointly-work*] | **trafficmode** *trafficmode* | **pendingtime** *pendingtime* | **iid-map** *iid-map* [**braprefix** *braprefix* | **brasuffix** *brasuffix* | **praprefix** *praprefix* | **prasuffix** *prasuffix*] | **cs-mode** *cs-mode*] *

undo iua-linkset linksetno

Parameters

Parameter	Description	Value
linksetno	Specifies the ID of an IUA link set. This parameter is mandatory and uniquely identifies an IUA link set.	The value is an integer that ranges from 0 to 15.
mgid *mgid*	Specifies the MG interface ID.	The value is an integer that ranges from 0 to 16777215.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
jointly-work *jointly-work*	Specifies whether links in a link set support switchover.	The value can be **enable** or **disable**. ● enable: support. ● disable: not support. Default value: disable
trafficmode *trafficmode*	Specifies the work mode of a link set. This parameter is optional. Set this parameter when you need to configure the work mode for the new link set. A link set can work in the primary/secondary mode (**override**) or load balancing mode (**loadshare**). A link set may contain multiple links. In the primary/standby mode, one link is the primary link and other links are secondary links. In the load balancing mode, all links bear load.	The value can be **override** or **loadshare**. Default value: override
pendingtime *pendingtime*	Specifies the pending duration. This parameter is optional. Set this parameter when you need to configure the pending duration for the new link set. When the status of a link set changes, the system first changes the link state to Pending to prevent jitter, starts timing, and changes the link set to the final state when the pending duration ends.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
iid-map *iid-map*	Specifies the interface ID (IID) generation mode. This parameter is optional. Set this parameter when the default IID generation mode cannot meet the requirements.	The value is an integer that ranges from 1 to 5. ● 1: The IID is configured by a user. ● 2: The system uses an automatically generated decimal value in the *ffsspp* format as the IID. In the preceding format, *ff* indicates the subrack ID, *ss* indicates the slot ID, and *pp* indicates the port number. ● 3: The system uses an automatically generated binary value in the *rrrrrfffffsssssppppppxxxxxxxxxx* format as the IID. In the preceding format, *rrrrr* indicates the shelf ID (automatically recognized by the system), *fffff* indicates the subrack ID, *sssss* indicates the slot ID, *pppppppp* indicates the port number, and *xxxxxxxxxx* is not used (system fixed value). ● 4: The system uses an automatically generated string in the *prefix* + *ff/ss/pp* format as the IID. In the preceding format, *ff* indicates the subrack ID, *ss* indicates the slot ID, and *pp* indicates the port number. ● 5: The system uses an automatically generated string in the *prefix* + *interfaceID* + *suffix* format as the IID. In the preceding format, *prefix* indicates the prefix, *interfaceID* indicates the IID entered by a user, and *suffix* indicates the suffix. Default value: 1
braprefix *braprefix*	Specifies the BRA IID prefix. This parameter is optional. When **iid-map** is set to 4, the IID is in the *prefix* + *ff/ss/pp* format. When **iid-map** is set to 5, the IID is in the *prefix* + *interfaceID* + *suffix* format.	The value is a string of 1 to 20 characters. Default value: a hyphen (-)

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
brasuffix *brasuffix*	Specifies the BRA IID suffix. This parameter is optional. When **iid-map** is set to 5, the IID is in the *prefix* + *interfaceID* + *suffix* format.	The value is a string of 1 to 20 characters. Default value: a hyphen (-)
praprefix *praprefix*	Specifies the PRA IID prefix. This parameter is optional. When **iid-map** is set to 4, the IID is in the *prefix* + *ff/ss/pp* format. When **iid-map** is set to 5, the IID is in the *prefix* + *interfaceID* + *suffix* format.	The value is a string of 1 to 20 characters. Default value: a hyphen (-)
prasuffix *prasuffix*	Specifies the PRA IID suffix. This parameter is optional. When **iid-map** is set to 5, the IID is in the *prefix* + *interfaceID* + *suffix* format.	The value is a string of 1 to 20 characters. Default value: a hyphen (-)
cs-mode *cs-mode*	Specifies the server environment for an IUA link set. This parameter is optional. Set this parameter when the default configuration cannot meet the requirements.	The value can be **server** or **client**. ● server: The link set is configured on the server. ● client: The link set is configured on the client. Default value: server

Views

SIGTRAN view

Default Level

2: Configuration level

Usage Guidelines

When you need to add an ISDN user and configure link set for the user, run this command. After the link set is successfully added, the user can be added.

Example

Add an IUA link set. Set the link set ID to 0 and MG interface ID to 0, enable link switchover, and set the working mode to primary/secondary mode, pending duration to 100s, and IID generation mode to user input.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sigtran
[Huawei-voice-sigtran] iua-linkset 0 mgid 0 jointly-work enable trafficmode override pendingtime 100
iid-map 1
```

Related Topics

16.7.2.13 display voice iua-linkset

16.7.3.15 iua-linkset-pendingtime

Function

The **iua-linkset-pendingtime** command changes the pending duration of an IUA link set.

Format

iua-linkset-pendingtime *linksetno* **pendingtime** *timevalue*

undo iua-linkset-pendingtime *linksetno*

Parameters

Parameter	Description	Value
linksetno	Specifies the ID of an IUA link set. This parameter is mandatory.	The value is an integer that ranges from 0 to 15.
timevalue	This parameter is mandatory. When the status of a link set changes, the system first changes the link state to Pending to prevent jitter, starts timing, and changes the link set to the final state when the pending duration ends.	The value is an integer that ranges from 1 to 100. Unit: s

Views

SIGTRAN view

Default Level

2: Configuration level

Usage Guidelines

The configuration of the pending duration for a link set helps prevent jitter caused by link set status change.

Example

Set the pending duration of IUA link set 0 to 50s.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] sigtran
[huawei-voice-sigtran] iua-linkset-pendingtime 0 pendingtime 50
```

Related Topics

16.7.3.14 iua-linkset

16.7.3.16 local-digitmap

Function

The **local-digitmap** command adds a local preset digit map or adds the local preset digit map body for a local preset digit map. When you need to add a local preset digit map for matching phone numbers based on the digit map, run this command.

Format

local-digitmap *name* {*bodyvalue* | **append** *bodyvalue* }

undo local-digitmap *name* [*bodyvalue*]

Parameters

Parameter	Description	Value
name	Specifies the name of a digit map. This parameter is mandatory.	The value is a string of 1 to 32 characters. The first character must be a letter, and subsequent characters must be digits, letters, or underscores.

Parameter	Description	Value
Bodyvalue	Specifies the digit map body, that is, the digit map match scheme. This parameter is optional.	The value is a string of 1 to 256 characters. The digit map body can contain one or more sub-schemes. Each sub-scheme cannot exceed 180 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

A H248 AG digitmap contains one or more bodies. Each body contains no more than 256 bytes.

A digitmap defines dialup rules. Calls can be initiated only when numbers match the rules. By default, all calling numbers are allowed.

A body can contain the following characters: digits 0 to 9, dot (.), vertical bar (|), square brackets [ ], hyphen (-), parentheses ( ), letters A to K and X, and letters T, S, L, Z (case-sensitive). A body complies with the following rules:

- Parentheses ( ) and square brackets [ ] must be used in pairs, and ( ) cannot be placed in the middle of the body.
- X, |, or . cannot be included in square brackets.
- A hyphen (-) is placed between two numbers, indicating a value range. The number behind the hyphen must be greater than the number before the hyphen. The value range must be included in square brackets.
- L, S, T, or Z cannot be followed by a dot.
- A body cannot start with L, S, T, Z, or a dot.

Example

Configure a digitmap for a H248 AG, which allows only 8-digit numbers starting with 8888.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] local-digitmap huawei type normal 8888xxxx
```

Related Topics

16.6.1.10 display voice local-digitmap

16.7.3.17 rfc2198 smart-parameters

Function

The **rfc2198 smart-parameters** command configures the upper limit of the packet loss rate and the number of RFC 2198 redundant packets at each of the four stages.

The **undo rfc2198 smart-parameters** command disables the RFC 2198 packet loss settings.

Format

rfc2198 smart-parameters *section-value* { **up-threshold** *up-threshold-value* | **redundant-num** *redundant-num-value* }*

undo rfc2198 smart-parameters *section-value* { **up-threshold** | **redundant-num** }*

Parameters

Parameter	Description	Value
section-value	Specifies the redundant packet stage based on the packet loss rate.	The value can be **first**, **second**, **third**, or **fourth**. ● first: stage 1. ● second: stage 2. ● third: stage 3. ● fourth: stage 4.
up-threshold-value	Specifies the upper limit of the packet loss rate at each stage. Set this parameter to specify the upper limit of the packet loss rate during RFC 2198 intelligent startup. The parameter value is expressed in permillage and must be greater than the upper limit of the packet loss rate specified in the previous stage.	The value is an integer that ranges from 0 to 1000. Default value: first-5; second-30; third-50; fourth-1000
redundant-num-value	Specifies the number of RFC 2198 redundant packets at each stage.	The value is an integer that ranges from 0 to 3. Default value: first-0; second-1; third-2; fourth-3

 Copyright © Huawei Technologies Co., Ltd.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

The upper threshold of the packet loss rate in one section must be greater than that in the previous section and smaller than that in the next section. The packet loss rate in section four must be configured to 1000.

Example

Set the number of RFC 2198 redundant packets to 3 at the first stage and upper limit of the packet loss rate to 20.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice]rfc2198 smart-parameters first redundant-num 3 up-threshold 20
```

16.7.3.18 sigtran

Function

The **sigtran** command switches from the voice view to the SIGTRAN view.

Format

sigtran

Parameters

None

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

Switch from the voice view to the SIGTRAN view.

Example

Switch from the voice view to the SIGTRAN view.

```
<huawei> system-view
[huawei] voice
```

```
[huawei-voice] sigtran
[huawei-voice-sigtran]
```

16.7.3.19 tid-template

Function

The **tid-template** command adds a user-defined TID template.

The **undo tid-template** command deletes a TID template.

Format

tid-template *templateid* **format** *formatstring* **parameter-list** *string* **name** *namestring*

undo tid-template

Parameters

Parameter	Description	Value
templateid	Specifies the template index that uniquely identifies a TID template.	The value is an integer that ranges from 32 to 63.
format *formatstring*	Specifies the format string that defines the format of strings generated from the parameter list.	The value is a string of 2 to 64 characters.
parameter-list *string*	Specifies the parameter list that defines parameters to be converted to strings. The number of parameters must be the same as that defined in the format string.	The value is a string of 1 to 64 characters.
name *namestring*	Specifies the unique template name.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

- The index and name of an added profile must be different from that of any profile existing in the system.

 Copyright © Huawei Technologies Co., Ltd.

- There are 19 default TID profiles (profiles 0-18) in the system. The default TID profiles can be referenced but cannot be added, modified or deleted.
- The format character string and the parameter list must comply with the following format rules:
  - A security character string is a character string used for separating data formats, and can consist of letters, "/" and "_".
  - A format character string contains one or more data formats, and the security character string between data formats. (A format character string can contain no security character string.).
  - The data format is divided into fixed length data format and non-fixed length data format. The fixed length data format is %u and the non-fixed length data format is %0Xu. The X is an integer between 1 and 10 and indicates the length of a figure. If a figure is shorter than x, 0s are added in front of the figure.
  - There must be a security character between two non-fixed length data formats or when a non-fixed length data format is in front of a fixed length data format. For example, %02u%u is valid while %u%02u is invalid, because a security character string must be added between %u and %02.
  - A parameter list consists of one or more parameters, which are separated by ",".
  - The format of a parameter: parameter = "keyword" or "keyword + offset".
  - Only F, S, P, B, G and R are valid keywords and the meaning that each of them indicates is shown as follows:
    - F: Frame, indicates the shelf number.
    - S: Slot, indicates the slot number.
    - P: Port, indicates the port number.
    - B: B Channel, indicates the B channel number.
    - G: indicates the general permanent termination index.
    - R: indicates the RTP ephemeral termination index.
  - In a parameter list, the keyword cannot occur repeatedly, and the offset is an integer between 1 and 0X40000000.
  - The format character string and the parameter list must match each other, that is, the number of the data formats in the format character string must be the same as that of the parameters in the parameter list. If a parameter maps a format character string in a fixed length, the offset of the parameter cannot exceed the length defined by the format character string. For example, data format %02u that parameter G+100 maps is invalid because parameter G+100 contains at least three figures.
  - The mapping between the terminal type and the keyword is shown as follows:

Terminal Type	Keyword of the Matched Parameter List
RTP	Contains and contains only R.

Terminal Type	Keyword of the Matched Parameter List
PSTN	Contains only G when the terminal identifier is not layered.
PSTN	Contains and contains only F, S and P when the terminal identifier is layered.
BRA	Contains only G or G, B when the terminal identifier is not layered.
BRA	Contains and contains only F, S, P and B when the terminal identifier is layered.
PRA	Contains only G or G, B when the terminal identifier is not layered.
PRA	Contains and contains only F, S, P and B when the terminal identifier is layered.
R2	Contains only G or G, B when the terminal identifier is not layered.
R2	Contains and contains only F, S, P and B when the terminal identifier is layered.

Example

Add TID template 36.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tid-template 36 format %u/%u/%u parameter-list F+1,S+1,P+1 name SelfDesign
```

16.7.3.20 tid-template-modify

Function

The **tid-template-modify** command modifies a user-defined TID template.

Format

tid-template-modify *templateid* { **format** *formatstring* **parameter-list** *string* **name** *namestring* } *

Parameters

Parameter	Description	Value
templateid	Specifies the template index that uniquely identifies a TID template.	The value is an integer that ranges from 32 to 63.

Parameter	Description	Value
formatstring	Specifies the format string that defines the format of strings generated from the parameter list.	The value is a string of 2 to 64 characters.
string	Specifies the parameter list that defines parameters to be converted to strings. The number of parameters must be the same as that defined in the format string.	The value is a string of 1 to 64 characters.
namestring	Specifies the unique template name.	The value is a string of 1 to 32 characters.

Views

Voice view

Default Level

2: Configuration level

Usage Guidelines

This command modifies a user-defined TID template.

Example

Modify TID template 36.

```
<Huawei> system-view
[Huawei] voice
[Huawei-voice] tid-template-modify 36 format %u/%u/%u parameter-list F+1,S+1,P+1 name
SelfDesign
```

 Copyright © Huawei Technologies Co., Ltd.

17 Virtualization Commands

About This Chapter

NOTE

Only the AR3670, AR169-P-M9, AR169W-P-M9 and AR169RW-P-M9 support virtualization.

17.1 attach disk
17.2 blank-disk name
17.3 cpu
17.4 delete package
17.5 display blank-disk name
17.6 display download-ratio package
17.7 display ovs bridge information
17.8 display ovs mac-address bridge
17.9 display ovs traffic-statistics bridge
17.10 display package information
17.11 display resource-usage
17.12 display veth information
17.13 display virtual-environment link
17.14 display virtual-environment reserve cpu-thread statistic
17.15 display virtual-environment resource
17.16 display vm
17.17 display vnc-server information
17.18 download package
17.19 exception-action

 Copyright © Huawei Technologies Co., Ltd.

17.20 install vm
17.21 link
17.22 memory size
17.23 ova file
17.24 ovs bridge
17.25 port (vSwitch view)
17.26 port default vlan (vSwitch view)
17.27 port trunk allow-pass vlan (vSwitch view)
17.28 reset cdrom file
17.29 reset ovs traffic-statistics bridge
17.30 set cdrom file
17.31 uninstall vm
17.32 veth
17.33 virtual-environment
17.34 virtual-environment reserve cpu-thread number
17.35 virtual-network-card number
17.36 vm
17.37 vm activate
17.38 vm deactivate
17.39 vm start
17.40 vm stop
17.41 vnc-server port

17.1 attach disk

Function

The **attach disk** command adds a disk to a VM.

The **undo attach disk** command removes a disk from a VM.

Format

attach disk *disk-name*

undo attach disk *disk-name*

Parameters

Parameter	Description	Value
disk-name	Specifies the disk name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a VM, you can run this command to add disks to the VM to expand the capacity.

Prerequisites

A blank disk has been created using the **blank-disk name** command.

Example

Add the disk **disk1** to a VM.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] blank-disk name disk1 size 15
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] attach disk disk1
```

Related Topics

17.2 blank-disk name

17.2 blank-disk name

Function

The **blank-disk name** command creates a blank disk.

The **undo blank-disk name** command deletes a disk.

Format

blank-disk name *name* **size** *size*

undo blank-disk name *name*

Parameters

Parameter	Description	Value
name	Specifies the disk name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.
size *size*	Specifies the disk size.	The value is an integer that ranges from 5 to 500, in GB.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command in the following scenarios:

- If you need to make a VM installation package online, run this command to create a blank disk.
- If you need to expand the capacity of a created VM, run this command to create a blank disk.

Follow-up Procedure

If you need to make a VM installation package online, run the **ova file** command to make a VM installation package.

If you need to expand the capacity of a VM, run the **attach disk** command to add a disk to the VM.

Example

Create the blank disk **disk1** with the size 15 GB.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] blank-disk name disk1 size 15
```

Related Topics

17.23 ova file

17.1 attach disk

17.3 cpu

Function

The **cpu** command configures CPU cores and mode of using CPU cores for a VM.

By default, all VMs share all CPU cores in the virtual environment.

Format

cpu { *cpu-id* **mono** | *cpu-id* **share** }*

Parameters

Parameter	Description	Value
cpu-id	Specifies the CPU core ID.	The value is an integer that ranges from 2 to 11 on the AR3670 and from 0 to 3 on the AR169-P-M9&AR169W-P-M9&AR169RW-P-M9.
mono	Indicates that a CPU core is exclusively used by a VM.	-
share	Indicates that a CPU core is shared by VMs.	-

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a VM, you can run this command to allocate CPU cores to the VM and configure the CPU core usage mode.

Precautions

If you run this command to configure a VM to exclusively use a CPU core, other VMs cannot use the CPU core.

Example

Configure the VM **vm1** to use CPU core 7 in sharing mode.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] cpu 7 share
```

17.4 delete package

Function

The **delete package** command deletes a file in the storage path of the virtual environment.

Format

delete package *package-name*

Parameters

Parameter	Description	Value
package-name	Specifies the file name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

You can run this command to delete a file in the specified storage path of the virtual environment. To view files in the path, run the **display package information** command.

Example

Delete the VM installation package **ova1.ova** in the storage path of the virtual environment.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] delete package ova1.ova
```

Related Topics

17.10 display package information

17.5 display blank-disk name

Function

The **display blank-disk name** command displays blank disk information.

Format

display blank-disk name *name*

Parameters

Parameter	Description	Value
name	Specifies the blank disk name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

You can run this command to view information about a blank disk.

Example

Display information about the blank disk **disk1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display blank-disk name disk1
Filename        disk1
  File format:  qcow2
  Virtual size: 5G
  Disk size:    192K
```

Table 17-1 Description of the **display blank-disk name** command output

Item	Description
Filename	Blank disk name.
File format	Blank disk type. Only the qcow2 type is supported.
Virtual size	Blank disk size specified when the disk is created.
Disk size	Actual size of the blank disk.

 Copyright © Huawei Technologies Co., Ltd.

17.6 display download-ratio package

Function

The **display download-ratio package** command displays the download progress of a file.

Format

display download-ratio package *package-name*

Parameters

Parameter	Description	Value
package-name	Specifies the file name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

If you run the **download package** command to download a file to the specified path in the virtual environment, you can run the **display download-ratio package** command to view the file download progress.

Example

Display the download progress of the VM installation package **ova1.ova**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display download-ratio package ova1.ova
The download ratio is 34%
```

Table 17-2 Description of the **display download-ratio package** command output

Item	Description
The download ratio	File download progress.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

17.18 download package

17.7 display ovs bridge information

Function

The **display ovs bridge information** command displays the vSwitch configuration.

Format

display ovs bridge information

Parameters

None

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

You can run this command to view the vSwitch configuration on the device.

Example

Display the vSwitch configuration.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display ovs bridge information
Bridge: bridge2015
  Port: p9
    Type: access
    VLAN: 1
  Port: p8
    Type: access
    VLAN: 1
```

Table 17-3 Description of the **display ovs bridge information** command output

Item	Description
Bridge	Name of a vSwitch. This parameter is configured using the **ovs bridge** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Port	Name of an interface. This parameter is configured using the **port (vSwitch view)** command.
Type	Type of an interface. This parameter is configured using the **port (vSwitch view)** command.
VLAN	VLAN to which an interface belongs. This parameter is configured using the **port default vlan (vSwitch view)** command.

Related Topics

17.24 ovs bridge
17.25 port (vSwitch view)
17.26 port default vlan (vSwitch view)

17.8 display ovs mac-address bridge

Function

The **display ovs mac-address bridge** command displays the MAC address of a vSwitch.

Format

display ovs mac-address bridge *bridge-name*

Parameters

Parameter	Description	Value
bridge-name	Specifies the vSwitch name.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run this command to view the MAC address of a vSwitch.

Example

Display the MAC address of the vSwitch **bridge2015**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display ovs mac-address bridge bridge2015
-----------------------------------------------------------------
  MAC Address   VLAN  PORT    Age
-----------------------------------------------------------------
ceac-97d0-55ba    10     port1     408
-----------------------------------------------------------------
```

Table 17-4 Description of the **display ovs mac-address bridge** command output

Item	Description
MAC Address	MAC address.
VLAN	VLAN to which a vSwitch belongs.
PORT	Interface that learns the MAC address.
Age	Aging time of the MAC address.

17.9 display ovs traffic-statistics bridge

Function

The **display ovs traffic-statistics bridge** command displays traffic statistics on a vSwitch.

Format

display ovs traffic-statistics bridge *bridge-name* [**port** *port-name*]

Parameters

Parameter	Description	Value
bridge-name	Specifies the vSwitch name.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.
port *port-name*	Specifies the name of an interface on the vSwitch.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.

 Copyright © Huawei Technologies Co., Ltd.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

You can run this command to view traffic statistics on a vSwitch.

Example

Display traffic statistics on the vSwitch **bridge2015**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display ovs traffic-statistics bridge bridge2015
veth5:  rx pkts=0, bytes=0, drop=0, errs=0
        tx pkts=0, bytes=0, drop=0, errs=0
veth7: rx pkts=0, bytes=0, drop=0, errs=0
        tx pkts=0, bytes=0, drop=0, errs=0
veth11: rx pkts=0, bytes=0, drop=0, errs=0
        tx pkts=0, bytes=0, drop=0, errs=0
```

Table 17-5 Description of the **display ovs traffic-statistics bridge** command output

Item	Description
rx pkts	Number of received packets.
tx pkts	Number of sent packets.
bytes	Number of bytes in packets.
drop	Number of discarded packets.
errs	Number of error packets.

17.10 display package information

Function

The **display package information** command displays files in the specified path of the virtual environment.

Format

display package information

Parameters

None

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

If you run the **download package** command to download a file to the specified path in the virtual environment, you can run the **display package information** command to view files in the path.

Example

Display files in the specified path of the virtual environment.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display package information
File list:
  vyatta.iso
  ova1.ova
```

Table 17-6 Description of the **display package information** command output

Item	Description
File list	Files in the specified path of the virtual environment. ● File with the file name extension **.iso**: OS image ● File with the file name extension **.ova**: VM installation package

Related Topics

17.18 download package

17.11 display resource-usage

Function

The **display resource-usage** command displays resource usage of a process to which a VM belongs.

Format

display resource-usage

Parameters

None

Views

VM view

Default Level

3: Management level

Usage Guidelines

After creating a VM. You can run this command to view resource usage of a process to which the VM belongs.

Example

Display resource usage of the process to which **vm1** belongs.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] display resource-usage
Cpu:    30%
Memory: 15M
Storage:  65M
```

Table 17-7 Description of the **display resource-usage** command output

Item	Description
Cpu	CPU usage.
Memory	Memory usage.
Storage	Storage space usage.

17.12 display veth information

Function

The **display veth information** command displays virtual interfaces on the HostOS.

Format

display veth information

Parameters

None

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to view virtual interfaces on the HostOS.

Precautions

This command does not display a HostOS virtual interface that uses the same name as a vSwitch.

Example

Display virtual interfaces on the HostOS.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display veth information
Name:
  veth3
```

Table 17-8 Description of the **display veth information** command output

Item	Description
Name	Name of a virtual interface on the HostOS.

17.13 display virtual-environment link

Function

The **display virtual-environment link** command displays virtual link information.

Format

display virtual-environment link

Parameters

None

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

You can run this command to view virtual link information.

Example

Display virtual link information.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display virtual-environment link
Dst vport                    Src vport

GigabitEthernet0/0/0             veth1
GigabitEthernet0/0/1             veth3
```

Table 17-9 Description of the **display virtual-environment link** command output

Item	Description
Dst vport	Destination virtual interface.
Src vport	Source virtual interface.

17.14 display virtual-environment reserve cpu-thread statistic

Function

The **display virtual-environment reserve cpu-thread statistic** command displays CPU resources allocated to VMs.

NOTE

Only the AR3670 support this command.

Format

display virtual-environment reserve cpu-thread statistic

Parameters

None

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

After completing the VM configuration, you can run this command to view CPU resources allocated to VMs.

Example

Display CPU resources allocated to VMs.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display virtual-environment reserve cpu-thread statistic
Cpu thread assign statistic:
  Current:  6  7  8  9  10  11
  Next:
```

Table 17-10 Description of the **display virtual-environment reserve cpu-thread statistic** command output

Item	Description
Cpu thread assign statistic	Statistics on allocated CPU cores.
Current	CPU cores occupied in the virtual environment.
Next	CPU cores that will be occupied in the virtual environment at the next startup. If the CPU cores are the same as the currently occupied CPU cores, this field is null.

17.15 display virtual-environment resource

Function

The **display virtual-environment resource** command displays resources in the virtual environment.

Format

display virtual-environment resource { **all** | **type** *type* }

Parameters

Parameter	Description	Value
all	Specifies all resources in the virtual environment.	-
type *type*	Specifies a certain type of resources in the virtual environment.	Currently, the following values are supported: • **cpu** • **memory** • **storage**

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

You can run this command to view resources allocated to the virtual environment.

Example

Display all resources in the virtual environment.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display virtual-environment resource all
CPU:

  Total:  12
  Share:  0
  Mono :  0 1 2 3 4 5 6
7
Storage:
  Total:  938770M
  Free:
927889M

Memory:
  Total:  16384M
  Free:   16384M
```

Table 17-11 Description of the **display virtual-environment resource** command output

Item	Description
CPU	CPU cores allocated to the virtual environment.

Item	Description
Storage	Storage space allocated to the virtual environment.
Memory	Memory allocated to the virtual environment.
Total	All available resources.
Share	CPU core shared by all VMs.
Mono	CPU core exclusively used by a VM.
Free	Unused resource.

17.16 display vm

Function

The **display vm** command displays information about VMs.

Format

display vm { **all** | *vm-name* }

Parameters

Parameter	Description	Value
all	Specifies all VMs.	-
vm-name	Specifies the VM name.	The value is a string of 1 to 32 case-insensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a VM, you can run this command to view information about the VM.

Prerequisites

A VM has been created.

Example

Display information about the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display vm vm1
Name:               vm1
Status:             running
Package:            ova1.ova
Auto-boot:          disable
Exception-action:reboot
Cpu-shared:
  Current:          7  8  9  10  11
  Next:
Cpu-mono:
  Current:
  Next:
Storage-claimed:
  Current:
    Disk:           1222
    Target:         hda
    Size:           5120M
  Next:
    Disk:           att1222
    Target:         hdc
    Size:           5120M
    Disk:           1222
    Target:         hda
    Size:           5120M
Cdrom:
  Current:
    Name:           iso1.iso
    Type:           public
  Next:
Memory:
  Current:          512M
  Next:
Veth:
  Current:
    Name:           vm1_eth2
    Mac:            00:e0:d7:34:af:33
    Name:           vm1_eth1
    Mac:            00:e0:12:4c:fb:13

Next:
```

Table 17-12 Description of the **display vm** command output

Item	Description
Name	VM name.
Status	VM running status. ● config: The VM is not activated. ● activated: The VM is activated. ● running: The VM is running properly. ● exception: The VM fails.

Item	Description
Package	VM installation package name.
Auto-boot	Automatic VM restart function. ● enable: The function is enabled. ● disable: The function is disabled.
Exception-action	Default processing mode upon a VM exception. ● reboot: The system restarts the VM. ● alarm: The system generates an alarm.
Cpu-shared	CPU core shared by VMs.
Cpu-mono	CPU core exclusively used by a VM.
Storage-claimed	Available storage space for a VM.
Cdrom	Image file in a VM's CD-ROM. ● Name: indicates the name of the image file. ● Type: The value **public** indicates that the OVA package does not contain an image file. The value **private** indicates that the OVA package contains an image file.
Memory	Available memory for a VM, in GB.
Veth	Virtual interface on a VM.
Current	Current VM status.
Next	VM status at the next startup. If the VM status is the same as the current VM status, this field is null.
Disk	Disk name.
Target	Disk location.
Size	Disk size, in GB.
Name	Name of a virtual interface on a VM.
Mac	MAC address of an interface.

Related Topics

17.20 install vm

17.17 display vnc-server information

Function

The **display vnc-server information** command displays the VNC service port number and authentication type.

Format

display vnc-server information

Parameters

None

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

You can run this command to check the VNC service port number and authentication type.

Example

Display the VNC service port number and authentication type.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] display vnc-server information
Virtual machine          Port          Authentication-type

vm111                     1            none
vmwin                     2            tls
vmwin1                    3            none
```

Table 17-13 Description of the **display vnc-server information** command output

Item	Description
Virtual machine	VM name.
Port	VNC service port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication-type	VNC authentication type. • none: No VNC authentication type is configured. • tls: The VNC authentication type is set to TLS. To configure the VNC authentication type, run the **vnc-server port** command.

Related Topics

17.41 vnc-server port

17.18 download package

Function

The **download package** command downloads a file.

The **undo download package** command cancels file download.

Format

download package *package-name* **ftp** *ftp-file* **user** *user-name* **password cipher**

undo download package *package-name*

Parameters

Parameter	Description	Value
package-name	Specifies the name of the file to be downloaded.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ftp *ftp-file*	Specifies a file on the FTP server. The file is in the format of ftp://*ip*:*port*/*file-name*, where: ● *ip*: indicates the IP address of the FTP server. ● *port*: indicates the port number used by the FTP server. If the value is 21, the file format does not include the port number, that is, the file is in the format of ftp://*ip*/*file-name*. ● *file-name*: indicates the name of the downloaded file. The value includes the file name extension.	The value is a string of 1 to 128 case-insensitive characters.
user *user-name*	Specifies the user name used to log in to the FTP server.	The value is a string of 1 to 32 case-insensitive characters.
password cipher	Specifies the password used to log in to the FTP server. The password entered in interactive mode is not displayed on the screen.	-

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command in the following scenarios:

- If you make a VM installation package offline, run this command to download the VM installation package to the device.
- If you make a VM installation package online, run this command to download the OS image to the device.

Follow-up Procedure

Run the **display download-ratio package** command to view the file download progress.

Example

Download the VM installation package **ova1.ova**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] download package ova1.ova ftp ftp://192.168.1.220//ova1.ova user 1
password cipher
Enter Password(<1-16>):
```

Related Topics

17.6 display download-ratio package

17.19 exception-action

Function

The **exception-action** command configures the default processing mode upon a VM exception.

By default, the system generates an alarm upon a VM exception.

Format

exception-action { **reboot** | **alarm** }

Parameters

Parameter	Description	Value
reboot	Configures the system to restart the VM upon a VM exception.	-
alarm	Configures the system to generate an alarm upon a VM exception.	-

Views

VM view

Default Level

3: Management level

Usage Guidelines

You can run this command to configure the default processing mode upon a VM exception.

Example

Configure the system to restart the VM upon a VM exception.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] exception-action reboot
```

 Copyright © Huawei Technologies Co., Ltd.

17.20 install vm

Function

The **install vm** command creates a VM.

Format

install vm *vm-name* **package** *package-name*

Parameters

Parameter	Description	Value
vm-name	Specifies the VM name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.
package *package-name*	Specifies the name of a VM installation package.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To use VM services, you can run this command to create a VM.

Prerequisites

A VM installation package exists on the device.

Follow-up Procedure

Run the **vm active** command to activate and allocate resources to the VM.

Example

Create the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] install vm vm1 package ova.ova
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

17.37 vm activate

17.21 link

Function

The **link** command configures a virtual link.

The **undo link** command deletes a virtual link.

By default, the system on the AR3670 creates a virtual link between the routing system virtual interface GE0/0/0 and the HostOS virtual interface veth1 and a virtual link between the routing system virtual interface GE0/0/1 and the HostOS virtual interface veth2. By default, the system on the AR169-P-M9 creates a virtual link between the routing system virtual interface GE0/0/6 and the HostOS virtual interface veth1.

Format

link interface *interface-type interface-number* **to veth** *vport-name*

link veth *vport-name* **to** { **interface** *interface-type interface-number* | **veth** *vport-name* }

undo link interface *interface-type interface-number*

undo link veth *vport-name*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of a virtual interface in the routing system.	-
veth *vport-name*	Specifies the name of a virtual interface on the HostOS or a VM.	The name of a HostOS virtual interface is a string of 1 to 64 case-sensitive characters and consists of letters and digits. A VM virtual interface is created by the system by default and its name is in the format of VM name_ + eth + interface number.

Views

Virtual-environment view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To access a VM, ensure that the VM can communicate with the external network. Virtual links connect virtual systems (including the routing system, VM, and HostOS) on the device. VMs communicate with the external network through the routing system. You need to run the **link** command to create virtual links between the VM, HostOS, and routing system.

Precautions

Any two interfaces can communicate with each other after being connected using a virtual link. The virtual link is not unidirectional.

Example

Create a virtual link between the virtual interface **GE0/0/2** in the routing system and the virtual interface **vm1_eth1** on a VM.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] link interface gigabitethernet 0/0/2 to veth vm1_eth1
```

17.22 memory size

Function

The **memory size** command configures the memory size for a VM.

Format

memory size *size*

Parameters

Parameter	Description	Value
size	Specifies the memory size for a VM.	The value is an integer that ranges from 256 to 8192, in MB.

Views

VM view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After creating a VM, you can run this command to reconfigure the memory size for the VM.

Prerequisites

A VM has been created using the **install vm** command.

Example

Set the memory size of the VM **vm1** to 512 MB.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] memory size 512
```

Related Topics

17.20 install vm

17.23 ova file

Function

The **ova file** command makes a VM installation package.

The **undo ova file** command deletes a VM installation package.

Format

ova file *ova-name* **iso** [**package**] *iso-file* **disk** *disk-name* [**cpu** *cpu-num*] **memory** *size* **network-card** *network-card-num* **network-card-type** *network-card-type* [**extend-description** *extend-description* | **external-unit** { **usb** | **media** | **disk** | **serial** }*]

undo ova file *ova-name*

NOTE

Only the AR169-P-M9&AR169W-P-M9&AR169RW-P-M9 support the **extend-description** *extend-description* and **external-unit** { **usb** | **media** | **disk** | **serial** } parameter.

If the **extend-description** *extend-description* parameter is specified, the value of **memory** *size* cannot be greater than 2848 MB.

If the **extend-description** *extend-description* parameter is specified, the configured VM installation package cannot be used by two VMs at the same time.

After the **extend-description** *extend-description* parameter is specified, ensure that the Windows OS does not enter hibernate mode when installing the Windows OS on a VM.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ova-name	Specifies the name of a VM installation package.	The value is a string of 1 to 28 case-sensitive characters and consists of letters and digits.
package	Indicates that the OS image is copied to the OVA file.	-
iso *iso-file*	Specifies the OS image name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.
disk *disk-name*	Specifies the disk name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.
cpu *cpu-num*	Specifies the number of CPUs.	The value is an integer that ranges from 1 to 8. The default value is 1.
memory *size*	Specifies the memory size.	The value is an integer that ranges from 256 to 8192, in MB.
network-card *network-card-num*	Specifies the number of network adapters.	The value is an integer that ranges from 1 to 8.
network-card-type *network-card-type*	Specifies the network adapter type.	The following type is supported: ● e1000 ● rpl8139 ● virtio A network adapter of the virtio type is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
extend-description *extend-description*	Specifies the extended description for customized parameters. The customized parameters include the removable hardware mounted to VM. **NOTE** The command length supported by the device is limited. If multiple user-defined parameters are used, the command length may exceed the limit. In this scenario, you are advised to make a VM installation package offline.	The value is a string of 1 to 256 characters. It is enclosed within double quotation marks (" "). The character string inside the double quotation marks does not support double quotation marks (" "), single quotation marks (' '), and escape characters (\). For example, the value can be **"-hdb /dev/external_disk"**. The recommended values for user-defined parameters are as follows: ● Audio and video: "-device pci-assign,host=0000:00:02.0,id=inteligd -gfx_passthru -device pci-assign,host=0000:00:1b.0" ● Hard disk: "-hdb /dev/external_disk" ● Serial interface: "-device /dev/ttyS1" ● USB/Hub: " -device ehci,driver=ich9-usb-ehci1,addr=1c.0,multifunction=on,id=ehci -device uhci-1,driver=ich9-usb-uhci1,addr=1c.1,multifunction=on,masterbus=ehci.0,firstport=0 -device uhci-2,driver=ich9-usb-uhci2,addr=1c.2,multifunction=on,masterbus=ehci.0,firstport=2 -device uhci-3,driver=ich9-usb-uhci3,addr=1c.3,multifunction=on,masterbus=ehci.0,firstport=4 -device usb-host,hostbus=1,hostport=2,bus=ehci.0 -device usb-host,hostbus=1,hostport=2.1,bus=ehci.0 -device usb-host,hostbus=1,hostport=2.2,bus=ehci.0 -device usb-host,hostbus=1,hostport=2.3,bus=ehci.0 -device usb-host,hostbus=1,hostport=2.4,bus=ehci.0 -device ehci,driver=ich9-usb-ehci1,addr=1d.0,multifunction=on,id=ehci1 -device uhci-1,driver=ich9-usb-uhci1,addr=1d.1,multifunction=on,masterbus=ehci1.0,firstport=0 -device uhci-2,driver=ich9-usb-uhci2,addr=1d.2,multifunction=on,masterbus=ehci1.0,firstport=2 -device uhci-3,driver=ich9-usb-uhci3,addr=1d.3,multifunction=on,masterbus=ehci1.0,firstport=4 -device usb-host,hostbus=1,hostport=3,bus=ehci1.0 -device usb-host,hostbus=1,hostport=3.1,bus=ehci1.0 -device usb-host,hostbus=1,hostport=3.2,bus=ehci1.0 -device usb-host,hostbus=1,hostport=3.3,bus=ehci1.0 -device usb-host,hostbus=1,hostport=3.4,bus=ehci1.0 -device ehci,driver=ich9-usb-ehci1,addr=1e.0,multifunction=on,id=ehci2 -device uhci-1,driver=ich9-usb-

Parameter	Description	Value
		uhci1,addr=1e.1,multifunction=on,masterbus=ehci2.0,firstport=0 -device uhci-2,driver=ich9-usb-uhci2,addr=1e.2,multifunction=on,masterbus=ehci2.0,firstport=2 -device uhci-3,driver=ich9-usb-uhci3,addr=1e.3,multifunction=on,masterbus=ehci2.0,firstport=4 -device usb-host,hostbus=1,hostport=1,bus=ehci2.0 -device usb-host,hostbus=1,hostport=1.1,bus=ehci2.0 -device usb-host,hostbus=1,hostport=1.2,bus=ehci2.0 -device usb-host,hostbus=1,hostport=1.3,bus=ehci2.0 -device usb-host,hostbus=1,hostport=1.4,bus=ehci2.0"

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
external-unit { **usb** | **media** | **disk** | **serial** }	Configures an external device supported by the AR router and saves the configuration to the VM installation package. External device types include: ● usb: Universal Serial Bus (USB) ● media: audio terminal and video terminal **NOTE** The AR router supports only audio and video terminals connected to the router using the HDMI video cable and VGA video cable. ● disk: hard disk ● serial: serial interface	-

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to make a VM installation package online. The VM installation package is an .ova file.

Prerequisites

An OS image with the file name extension .iso has been prepared.

Example

Make the VM installation package **ova1.ova**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] ova file ova1 iso iso1.iso disk disk1 cpu 2 memory 512 network-card 4
network-card-type virtio
```

17.24 ovs bridge

Function

The **ovs bridge** command creates a vSwitch and displays the vSwitch view, or displays an existing vSwitch view.

The **undo ovs bridge** command deletes a vSwitch.

By default, the system creates the vSwitch br0.

Format

ovs bridge *bridge-name*

undo ovs bridge *bridge-name*

Parameters

Parameter	Description	Value
bridge-name	Specifies the vSwitch name.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A virtual switch (vSwitch) is created using virtualization technology and provides functions of a traditional switch. A vSwitch transmits traffic between VMs and connects VMs to the external network. To enable VMs to communicate through a vSwitch, you can run this command to create a vSwitch and enter the vSwitch view, or enter an existing vSwitch view.

Follow-up Procedure

Run the **port (vSwitch view)** command to add virtual interfaces to the vSwitch.

Precautions

The AR3670 supports a maximum of four vSwitches and has a default vSwitch br0. The AR169-P-M9&AR169W-P-M9&AR169RW-P-M9 has only one vSwitch br0, which is created by the system by default.

Example

Create the vSwitch **bridge2015**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] ovs bridge bridge2015
```

Related Topics

6.3.27 port

17.25 port (vSwitch view)

Function

The **port** command adds a virtual interface to a vSwitch.

The **undo port** command removes a virtual interface from a vSwitch.

Format

port *port-name* **link-type** { **access** | **trunk** }

undo port *port-name*

Parameters

Parameter	Description	Value
port-name	Specifies the name of a virtual interface.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
link-type	Specifies the link type of a virtual interface.	-
access	Sets the link type of a virtual interface to access.	-
trunk	Sets the link type of a virtual interface to trunk.	-

Views

vSwitch view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If virtual systems (including the routing system, VM, and HostOS) on the device communicate through a vSwitch, you need to add HostOS virtual interfaces that connect the routing system and VM to the vSwitch. To configure a VLAN, set the link type of virtual interfaces to trunk.

Prerequisites

A vSwitch has been created on the device.

Example

Add the HostOS virtual interface **veth4** to a vSwitch and set its link type to access.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] ovs bridge bridge2015
[Huawei-virtual-environment-ovs-bridge2015] port veth4 link-type access
```

17.26 port default vlan (vSwitch view)

Function

The **port default vlan** command configures the default VLAN for a virtual interface and adds the interface to the VLAN.

The **undo port default vlan** command deletes the default VLAN of a virtual interface and removes the interface from the VLAN.

By default, VLAN 1 is the default VLAN of all virtual interfaces.

Format

port *port-name* **default vlan** *vlan-id*

undo port *port-name* **default vlan**

Parameters

Parameter	Description	Value
port-name	Specifies the name of a virtual interface.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.
vlan-id	Specifies the ID of the default VLAN.	The value is an integer that ranges from 1 to 4094.

Views

vSwitch view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A virtual interface may receive both untagged and tagged frames, but the device processes only tagged frames. Therefore, the device adds a tag to each untagged frame received by a virtual interface. To achieve this purpose, you must configure a default VLAN for the virtual interface. When the virtual interface receives an untagged frame, the device adds the VLAN tag of the default VLAN to the untagged frame.

Precautions

If you delete the default VLAN in the system view, this command configuration is automatically deleted from the configuration file.

If you run the **port default vlan** command multiple times, only the latest configuration takes effect.

The default VLAN of Eth0/0/0 is VLAN 1. After the VM starts, the VM cannot obtain the IP address of sub-interface 1. If the VM needs to obtain the IP address of a sub-interface, another VLAN ID needs to be configured for a virtual interface of HostOS connected to the VM.

Example

Configure VLAN 10 as the default VLAN of the virtual interface **veth4**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] ovs bridge bridge2015
[Huawei-virtual-environment-ovs-bridge2015]  port veth4 default vlan 10
```

17.27 port trunk allow-pass vlan (vSwitch view)

Function

The **port trunk allow-pass vlan** command adds a virtual trunk interface to a VLAN.

The **undo port trunk allow-pass vlan** command deletes a virtual trunk interface from a VLAN.

Format

port *port-name* **trunk allow-pass vlan** { **all** | *vlan-id* &<1-10> | *vlan-id1* **to** *vlan-id2* }

undo port *port-name* **trunk allow-pass vlan**

Parameters

Parameter	Description	Value
port-name	Specifies the name of a virtual interface.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.
all	Adds a virtual trunk interface to all VLANs.	-
vlan-id	Specifies the ID of a VLAN to which a virtual trunk interface is added.	The value is an integer that ranges from 1 to 4094.
vlan-id1 **to** *vlan-id2*	Specifies the IDs of VLANs to which a virtual trunk interface is added. ● *vlan-id1* specifies the first VLAN ID. ● *vlan-id2* specifies the last VLAN ID. The value of *vlan-id2* must be greater than or equal to the value of *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

vSwitch view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to add a virtual trunk interface to a VLAN.

Prerequisites

The virtual interface has been added to a vSwitch and its link type has been set to trunk using the **port (vSwitch view)** command.

Precautions

If you run the **port trunk allow-pass vlan (vSwitch view)** command multiple times on the same virtual interface, the virtual interface is added to all the specified VLANs.

Example

Add the virtual interface **veth4** to VLANs 10 to 20.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] ovs bridge bridge2015
[Huawei-virtual-environment-ovs-bridge2015] port veth4 trunk allow-pass vlan 10 to 20
```

Related Topics

6.3.27 port

17.28 reset cdrom file

Function

The **reset cdrom file** command restores the image file in a VM's CD-ROM to the image file used during VM installation.

Format

reset cdrom file

Parameters

None

Views

VM view

Default Level

3: Management level

Usage Guidelines

If you have replaced the image file in a VM's CD-ROM, you can run this command to restore the image file used during VM installation.

Example

Restore the image file in a VM's CD-ROM to the image file used during VM installation.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] reset cdrom file
```

Related Topics

17.30 set cdrom file

17.29 reset ovs traffic-statistics bridge

Function

The **reset ovs traffic-statistics bridge** command deletes traffic statistics on a vSwitch.

Format

reset ovs traffic-statistics bridge *bridge-name* [**port** *port-name*]

Parameters

Parameter	Description	Value
bridge-name	Specifies the vSwitch name.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.
port *port-name*	Specifies the name of an interface on the vSwitch.	The value is a string of 1 to 15 case-insensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To ensure that traffic statistics on a vSwitch is accurate, you can run this command to delete traffic statistics on the vSwitch before executing a service, and view traffic statistics on the vSwitch after the service is executed.

Example

Delete traffic statistics on the vSwitch **bridge2015**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] reset ovs traffic-statistics bridge bridge2015
```

Related Topics

17.9 display ovs traffic-statistics bridge

17.30 set cdrom file

Function

The **set cdrom file** command replaces the image file in a VM's CD-ROM.

Format

set cdrom file *filename*

Parameters

Parameter	Description	Value
filename	Specifies the name of the new image file that is an .iso file.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To replace the image file in a VM's CD-ROM when performing operations such as installing a driver, you can run this command to replace the image file with the required image file.

 Copyright © Huawei Technologies Co., Ltd.

To restore the image file used during VM installation, run the **reset cdrom file** command.

Prerequisites

The new image file has been downloaded using the **download package** command.

Example

Replace the image file in a VM's CD-ROM with **virtio.iso**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] set cdrom file virtio.iso
```

Related Topics

17.18 download package
17.28 reset cdrom file

17.31 uninstall vm

Function

The **uninstall vm** command deletes a VM.

Format

uninstall vm *vm-name*

Parameters

Parameter	Description	Value
vm-name	Specifies the VM name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to delete an unused VM.

Prerequisites

The VM has been stopped using the **vm stop** command.

Precautions

After a VM is deleted, all services on the VM are interrupted and cannot be restored. Therefore, exercise caution when deciding to perform this operation.

Example

Delete the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] uninstall vm vm1
```

Related Topics

17.40 vm stop

17.32 veth

Function

The **veth** command creates a virtual interface for the HostOS.

The **undo veth** command deletes a virtual interface of the HostOS.

By default, the system on the AR3670 creates HostOS virtual interfaces veth1, veth2, and br0, and the system on the AR169-P-M9 &AR169W-P-M9&AR169RW-P-M9creates HostOS virtual interfaces veth1 and br0.

Format

veth *vport-name*

undo veth *vport-name*

Parameters

Parameter	Description	Value
vport-name	Specifies the name of a virtual interface on the HostOS.	The value is a string of 1 to 15 case-sensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After creating a VM, you need to connect the HostOS to the VM and routing system. Therefore, you need to run this command to create a virtual interface for the HostOS.

Follow-up Procedure

Run the **link** command to configure virtual links to connect the VM, routing system, and HostOS.

Example

Create the virtual interface **veth3** for the HostOS.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] veth veth3
```

Related Topics

17.21 link

17.33 virtual-environment

Function

The **virtual-environment** command displays the virtual-environment view.

Format

virtual-environment

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You need to enter the virtual-environment view to configure a VM. You can run this command in the system view to enter the virtual-environment view.

Precautions

On the AR169-P-M9&AR169W-P-M9&AR169RW-P-M9, add the parameter *ip-address* when running this command to enter the virtual-environment view. The parameter *ip-address* indicates the IP address of the virtual interface br0.

Example

Display the virtual-environment view.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment]
```

17.34 virtual-environment reserve cpu-thread number

Function

The **virtual-environment reserve cpu-thread number** command configures the number of available CPU cores for VMs.

NOTE

Only the AR3670 support this command.

By default, VMs can use four CPU cores.

Format

virtual-environment reserve cpu-thread number *number*

Parameters

Parameter	Description	Value
number	Specifies the number of CPU cores.	The value is an integer that ranges from 0 to 10 on the AR3670 and from 0 to 4 on the AR169-P-M9.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

When configuring VMs, you can run this command to allocate available CPU cores to the VMs. You can run the **display virtual-environment reserve cpu-thread statistic** command to view the number of CPU cores allocated to VMs.

Example

Set the number of available CPU cores to 2 for VMs.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] virtual-environment reserve cpu-thread number 2
```

Related Topics

17.14 display virtual-environment reserve cpu-thread statistic

17.35 virtual-network-card number

Function

The **virtual-network-card number** command configures the number of network adapters for a VM.

Format

virtual-network-card number *number*

Parameters

Parameter	Description	Value
number	Specifies the number of network adapters for a VM.	The value is an integer that ranges from 1 to 8.

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a VM, you can run this command to configure the number of network adapters for the VM. Each network adapter on a VM corresponds to a virtual interface.

Prerequisites

A VM has been created using the **install vm** command.

Example

Set the number of network adapters to 3 for the VM **vm1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] virtual-network-card number 3
```

Related Topics

17.20 install vm

17.36 vm

Function

The **vm** command displays the view of a specified VM.

Format

vm *vm-name*

Parameters

Parameter	Description	Value
vm-name	Specifies the VM name.	The value is a string of 1 to 32 case-sensitive characters and consists of letters and digits.

Views

Virtual-environment view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to enter the view of a specified VM.

To configure a VM, you need to enter the corresponding VM view. You can run this command in the virtual-environment view to enter the view of a specified VM.

Prerequisites

A VM has been created using the **install vm** command.

Example

Display the view of the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

17.20 install vm

17.37 vm activate

Function

The **vm activate** command activates a VM.

Format

vm activate

Parameters

None

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If you need to allocate resources to a created VM, run this command to activate the VM. To reclaim resources from the VM, run the **vm deactivate** command to deactivate the VM.

Prerequisites

A VM has been created using the **install vm** command.

Example

Activate the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] vm activate
```

Related Topics

17.20 install vm

17.38 vm deactivate

 Copyright © Huawei Technologies Co., Ltd.

17.38 vm deactivate

Function

The **vm deactivate** command deactivates a VM.

Format

vm deactivate

Parameters

None

Views

VM view

Default Level

3: Management level

Usage Guidelines

You can run this command to deactivate a VM in the VM view to release resources occupied by the VM. To reallocate resources to the VM, run the **vm activate** command to activate the VM.

Example

Deactivate the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] vm deactivate
```

Related Topics

17.37 vm activate

17.39 vm start

Function

The **vm start** command starts a VM.

Format

vm start

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating and activating a VM, you can run this command to start the VM and use VM services. To temporarily stop services on a VM, you can run the **vm stop** command to stop the VM.

Prerequisites

A VM has been created using the **install vm** command.

Example

Start the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] vm start
```

Related Topics

17.20 install vm

17.40 vm stop

Function

The **vm stop** command stops a VM.

Format

vm stop

Parameters

None

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to stop a VM for fault diagnosis or to terminate services on the VM. If you want to use services on a VM after stopping the VM, run the **vm start** command to start the VM.

Prerequisites

The VM has been started using the **vm start** command.

Example

Stop the VM **vm1**.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] vm stop
```

Related Topics

17.39 vm start

17.41 vnc-server port

Function

The **vnc-server port** command configures the VNC service port number and authentication password.

Format

vnc-server port *port-num* [**authentication-type** *authentication-type*] **password cipher**

Parameters

Parameter	Description	Value
port-num	Specifies the VNC service port number.	The value is an integer that ranges from 1 to 8.
authentication-type *authentication-type*	Specifies the VNC authentication type.	Currently, the VNC authentication type can only be set to TLS.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password cipher	Specifies the password for VNC authentication. The password is displayed in ciphertext.	The value is a string of 6 to 8 case-sensitive characters with spaces supported.

Views

VM view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure VNC for VM login, you need to run this command to configure the VNC service port number and authentication password.

Precautions

Before running this command, ensure that the VM is deactivated.

Example

Set the VNC service port number to 7 and authentication password to admin123.

```
<Huawei> system-view
[Huawei] virtual-environment
[Huawei-virtual-environment] vm vm1
[Huawei-virtual-environment-vm-vm1] vnc-server port 7 password cipher
Enter Password(<6-8>):
[Huawei-virtual-environment-vm-vm1]
```

Related Topics

17.17 display vnc-server information

18 Reliability Commands

About This Chapter

18.1 Interface Backup Configuration Commands
18.2 Interface Monitoring Group Configuration Commands
18.3 NSR Configuration Commands
18.4 HSB Configuration Commands
18.5 BFD Configuration Commands
18.6 VRRP Configuration Commands
18.7 EFM Configuration Commands
18.8 CFM Configuration Commands
18.9 Y.1731 Configuration Commands

18.1 Interface Backup Configuration Commands

18.1.1 display standby state

Function

The **display standby state** command displays the configuration and status of the primary and backup interfaces.

Format

display standby state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After interface backup is configured, you can run the **display standby state** command to view the status of the primary and backup interfaces. The **display standby state** command displays the status of the primary and backup interfaces, backup status, backup status flag, backup interface's priority, load balancing status, and association status.

Example

Display the configuration and status of the primary interface and backup interfaces.

```
<Huawei>display standby state
Interface              Interfacestate   Backupstate   Backupflag    Pri   Loadstate
GigabitEthernet1/0/0                UP           MUP           MU
GigabitEthernet2/0/0              DOWN          DOWN           BU     30
Backup-flag meaning:
M---MAIN  B---BACKUP     V---MOVED    U---USED
D---LOAD  P---PULLED
--------------------------------------------------------------------------------
Below is track BFD information:
Bfd-Name              Bfd-State  BackupInterface              State

--------------------------------------------------------------------------------
Below is track IP route information:
Destination/Mask    Route-State  BackupInterface              State

--------------------------------------------------------------------------------
Below is track NQA Information:
Instance Name                    BackupInterface              State
user
test                                                    OK
                              GigabitEthernet2/0/0         STANDBY
```

Table 18-1 Description of the display standby state command output

Item	Description
Interface	Type and number of the primary interface and backup interface. The first column is the primary interface and the other columns are backup interfaces.
Interfacestate	Interface status: ● The primary interface status can be Up or Down. ● The backup interface status can be Up, Down, or standby.

Item	Description
Backupstate	Backup status: • The backup status of the primary interface can be MUP, MUPDELAY, MDOWN, or MDOWNDELAY. • The backup status of the backup interface can be UP, UPDELAY, DOWN, DOWNDELAY, or STANDBY. **NOTE** • M in the primary interface status identifier: indicates that the interface is the primary interface. For example, MUP indicates that the primary interface is in Up state. • UPDELAY: indicates the delay status before the interface changes from Down to Up. • DOWNDELAY: indicates the delay status before the interface changes from Up to Down. • STANDBY: indicates that the interface is in standby state.
Backupflag	Backup status flag, which is represented by characters: • M: MAIN. The interface is the primary interface. • B: BACKUP. The interface is the backup interface. • V: MOVED. The interface is moved; primary interface of the interface is moved; all the backup interfaces of the interface are moved. • U: USED. The interface functions as the primary or backup interface and is in use. • D: LOAD. The primary interface participates in load balancing. • P: PULLED. The LPU where the interface is located is removed.
Pri	Priority of a backup interface. To set the priority of a backup interface, run the **standby interface** *interface-type interface-number priority* command.
Loadstate	Load balancing status: • The load balancing status of the backup interface can be WAKE, TO-HYPNOTIZE, TO-WAKE, or idle. • The load balancing status of the backup interface can be WAKE or idle. **NOTE** The load balancing status is as follows: • WAKE: The interface is in load balancing state. • TO-HYPNOTIZE: The interface will be shut down because traffic reduces. • TO-WAKE: The interface will be started because traffic increases. • Idle: The interface does not work in load balancing mode.
Bfd-Name	Name of the BFD session associated with the backup interface. To configure the name for a BFD session, run the **bfd** *session-name* **bind peer-ip** *ip-address* command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Bfd-State	Status of the BFD session bound to the backup interface.
Destination/Mask	Destination IP address and mask of the route associated with the backup interface.
Route-State	Status of the route associated with the backup interface.
Instance Name	Name of the NQA test instance associated with the backup interface. The administrator of the NQA test instance and instance name are displayed in this field. To configure the administrator of the NQA test instance and instance name, run the **nqa test-instance** *admin-name test-name* command.
BackupInterface	Backup interface.
State	Status of the NQA test instance and backup interface. ● The NQA test instance status includes OK and ERR. ● The backup interface status includes UP and STANDBY. **NOTE** ● OK: The link is in a good condition. ● ERR: The link is unreachable. ● UP: The interface is in Up state and is transmitting services. ● STANDBY: The interface is in backup state and does not transmit services.

Related Topics

18.1.3 standby interface

18.1.2 standby bandwidth

Function

The **standby bandwidth** command sets the maximum bandwidth of the primary interface in load balancing mode.

The **undo standby bandwidth** command restores the default maximum bandwidth of the primary interface in load balancing mode.

By default, the primary interface uses the actual physical bandwidth provided by the system as the maximum bandwidth.

Format

standby bandwidth *size*

undo standby bandwidth

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
size	Specifies the maximum bandwidth of the primary interface in load balancing mode.	The value is an integer that ranges from 0 to 4000000, in kbit/s.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Prerequisites

Interface backup has been configured by using the **standby interface** command.

Precautions

When the primary interface participates in load balancing, run the **standby bandwidth** command to set the maximum bandwidth of the primary interface. If *size* is not specified, the primary interface uses the actual physical bandwidth provided by the system.

NOTE

The configured maximum bandwidth of the primary interface must be smaller than the actual physical bandwidth.

Example

In load balancing mode, configure GE1/0/0 as the backup interface of GE2/0/0, and set the priority of GE1/0/0 to 30 and the maximum bandwidth of GE2/0/0 to 10000 kbit/s.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] standby interface gigabitethernet 1/0/0 30
[Huawei-GigabitEthernet2/0/0] standby bandwidth 10000
```

Related Topics

18.1.3 standby interface

 Copyright © Huawei Technologies Co., Ltd.

18.1.3 standby interface

Function

The **standby interface** command specifies a backup interface and sets the priority for the backup interface.

The **undo standby interface** command deletes the specified backup interface.

By default, no backup interface is specified.

Format

standby interface *interface-type interface-number* [*priority*]

undo standby interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of a backup interface.	-
priority	Specifies the priority of a backup interface.	The value is an integer that ranges from 0 to 255. A larger value indicates a higher priority of a backup interface. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A router plays an important role on a network. When an interface on the router is faulty, the interface backup function allows the router to quickly switch services from the faulty interface to a working interfaces. This ensures non-stop transmission and network security. Interface backup provides two working modes:

1. Active/Standby mode: Only one interface transmits services at any time. When the primary interface is faulty, a backup interface is used.

 Copyright © Huawei Technologies Co., Ltd.

2. Load balancing mode: Traffic is load balanced among multiple interfaces by setting the upper and lower thresholds of traffic of the primary interface.

Precautions

The **standby interface** command specifies a backup interface and sets the priority for the backup interface. When the primary interface becomes Down, backup interfaces are selected in ascending order of priority. The interface with the highest priority is selected as the primary interface. If backup interfaces have the same priority, the backup interface that were configured first is selected as the primary interface.

NOTE

- A maximum of 10 primary interfaces can be configured on a device simultaneously.
- A primary interface has a maximum of three backup interfaces. An interface can be used as the backup interface of only one primary interface.
- The primary interface cannot be configured as the backup interface of another interface, and the backup interface cannot be configured as the primary interface of another interface.
- The thresholds determine whether to use the active/standby mode or load balancing mode. If the thresholds are set, the load balancing mode is used. Otherwise, the active/standby mode is used.
- Primary interfaces: Ethernet Layer 3 interface and subinterface, dialer interface, ATM interface, ISDN BRI interface, Async interface, cellular interface, PON interface, MP-group interface, MFR interface, FR subinterface, and serial interface and subinterface.
- Backup interfaces: Ethernet Layer 3 interface and subinterface, dialer interface, ATM interface, BRI interface, Async interface, cellular interface, MP-group interface, MFR interface and subinterface, and serial interface and subinterface.
- On the AR100&AR120&AR150&AR160&AR200 device, primary and backup interfaces cannot be ISDN BRI interfaces, PON interfaces, or Async interfaces.

Example

Configure GE1/0/0 and GE2/0/0 as backup interfaces of GE3/0/0, and set the priority of GE1/0/0 to 30 and the priority of GE2/0/0 to 20.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 3/0/0
[Huawei-GigabitEthernet3/0/0] standby interface gigabitethernet 1/0/0 30
[Huawei-GigabitEthernet3/0/0] standby interface gigabitethernet 2/0/0 20
```

Related Topics

18.1.1 display standby state

18.1.4 standby threshold

Function

The **standby threshold** command sets the upper and lower thresholds of the traffic volume in load balancing mode.

The **undo standby threshold** command deletes the upper and lower thresholds of the traffic volume in load balancing mode.

By default, load balancing thresholds are not configured.

Format

standby threshold *enable-threshold disable-threshold*

undo standby threshold

Parameters

Parameter	Description	Value
enable-threshold	Specifies the upper threshold of traffic in load balancing mode.	The value is an integer ranging from 1 to 99.
disable-threshold	Specifies the lower threshold of traffic in load balancing mode.	The value is an integer ranging from 1 to 99.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When only one interface transmits services and the interface bandwidth is insufficient, traffic may be lost. You can run the **standby threshold** command to set the upper and lower thresholds of traffic on the primary interface so that traffic is load balanced among multiple interfaces. This improves reliability of data transmission.

Prerequisites

Interface backup has been configured by using the **standby interface** command.

Precautions

By default, the load balancing function of interface backup is disabled. If the thresholds are set by using the **standby threshold** command, the load balancing mode is used. Otherwise, the active/standby mode is used.

If the primary interface is faulty in load balancing mode, the system switches to the active/standby mode:

- If no backup interface is started, the system uses the backup interface with the highest priority to transmit services. If backup interfaces have the same priority, the system uses the backup interface that was configured first to transmit services.
- If a backup interface has been started, the system uses the backup interface with the highest priority to transmit services. If backup interfaces have the

 Copyright © Huawei Technologies Co., Ltd.

same priority, the system uses the backup interface that was configured first to transmit services.

NOTE

- The upper and lower thresholds refer to percentage of the maximum bandwidth. The maximum bandwidth can be set by using the **standby bandwidth** command.
- *enable-threshold* must be greater than *disable-threshold*.
- When you run the **undo standby threshold** command, if backup interfaces have been started, all the backup interfaces are shut down and only the primary interface is available.

Example

In load balancing mode, configure GE1/0/0 as the backup interface of GE2/0/0, and set the priority of GE1/0/0 to 30, the maximum bandwidth of GE2/0/0 to 10000 kbit/s, and the upper and lower thresholds to 80% and 20%.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] standby interface gigabitethernet 1/0/0 30
[Huawei-GigabitEthernet2/0/0] standby bandwidth 10000
[Huawei-GigabitEthernet2/0/0] standby threshold 80 20
```

Related Topics

18.1.3 standby interface

18.1.2 standby bandwidth

18.1.5 standby timer delay

Function

The **standby timer delay** command sets the delay in switching services between the primary interface and the backup interface.

The **undo standby timer delay** command restores the default delay.

By default, the delay is 5s.

Format

standby timer delay *enable-delay disable-delay*

undo standby timer delay

Parameters

Parameter	Description	Value
enable-delay	Specifies the delay in switching services from the primary interface to the backup interface.	The value ranges from 0 to 65535, in seconds. By default, the delay is 5s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
disable-delay	Specifies the delay in switching services from the backup interface to the primary interface.	The value ranges from 0 to 65535, in seconds. By default, the delay is 5s.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent frequent switchovers between the primary interface and the backup interface because of the unstable interface status, run the **standby timer delay** command to set the delay. After the primary interface changes from Up to Down, the system processes services in the following situations:

- If the primary interface is still Down after the delay, the system switches services to the backup interface.
- If the primary interface is restored during the delay, the system does not switch services.

Prerequisites

Interface backup has been configured by using the **standby interface** command.

Precautions

A small delay may cause route flapping and a large delay may cause traffic loss. Set the delay based on networking requirements:

- On a network that does not require high reliability for data transmission, set a long delay to prevent route flapping.
- On a network that requires high reliability for data transmission, set a short delay to prevent data loss.

Example

Specify GE1/0/0 as the backup interface of GE2/0/0 and set the delay to 10s.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] standby interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet2/0/0] standby timer delay 10 10
```

Related Topics

18.1.3 standby interface

18.1.6 standby track bfd-session

Function

The **standby track bfd-session** command associates interface backup with BFD.

The **undo standby track bfd-session** command disassociates interface backup from BFD.

By default, interface backup is not associated with BFD.

Format

standby track bfd-session session-name *session-name*

undo standby track bfd-session session-name *session-name*

Parameters

Parameter	Description	Value
session-name *session-name*	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the upstream indirectly connected link of the primary interface is faulty, the interface backup module cannot detect the fault, causing service interruption. BFD provides fast fault detection independent of media and routing protocols. It can rapidly detect faults on the forwarding path between two adjacent routers. Association between interface backup and BFD enables the system to detect connectivity of the primary link and implement rapid switching when the primary link is faulty. This ensures reliability of service transmission.

Association between interface backup and BFD is applicable to the networks demanding high reliability and short delay.

Prerequisites

A BFD session has been created.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure association between interface backup and BFD on GE1/0/0, and configure the BFD session **test** to detect the link status of the primary interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] standby track bfd-session session-name test
```

18.1.7 standby track nqa

Function

The **standby track nqa** command associates interface backup with NQA.

The **undo standby track nqa** command disassociates interface backup from NQA.

By default, interface backup is not associated with NQA.

Format

standby track nqa *admin-name test-name*

undo standby track nqa *admin-name test-name*

Parameters

Parameter	Description	Value
admin-name	Specifies the name of the administrator for an NQA test instance.	The value is a string of 1 to 32 case-insensitive characters without spaces.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-insensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the upstream indirectly connected link of the primary interface is faulty, the interface backup module cannot detect the fault, causing service interruption. The NQA technology measures network performance and collects statistics on the

delay, jitter, and packet loss ratio. Association between interface backup and NQA enables the system to detect connectivity of the primary link and implement rapid switching when the primary link is faulty.

You only need to configure association between interface backup and NQA on the backup interface. It is easy to configure and the NQA test instance detects packet statistics in addition to interface status detection. However, it takes a long time for the NQA test instance to detect faults.

Prerequisites

A specified NQA test instance with the specified administrator name has been created.

Example

Configure association between interface backup and NQA on GE1/0/0, configure the administrator of the NQA test instance as **user** and the test instance name as **test**.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] standby track nqa user test
```

18.1.8 standby track ip route

Function

The **standby track ip route** command associates interface backup and routing.

The **undo standby track ip route** command disassociates interface backup from routing.

By default, interface backup is not associated with routing.

Format

standby track ip route *ip-address* { *mask* | *mask-length* } [**vpn-instance** *vpn-instance-name*]

undo standby track ip route

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address of the route associated with interface backup.	The value is in dotted decimal notation.
mask	Specifies the mask of the IP address.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mask-length	Specifies the mask length. The 32-bit mask is represented by consecutive 1s, and the mask in dotted decimal notation can be replaced by the mask length.	The value is an integer ranging from 0 to 32.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The name is a string of 1 to 31 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the upstream indirectly connected link of the primary interface is faulty, the interface backup module cannot detect the fault, causing service interruption. When a link is faulty, the routing entry of the link is deleted or becomes inactive. Association between interface backup and routing enables the system to detect connectivity of the primary link and implement rapid switching when the primary link is faulty. This ensures reliability of service transmission.

Precautions

Only dynamic routes can be used.

Example

Configure GE1/0/0 as a backup interface and associate it with a route on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] standby track ip route 10.1.1.2 24
```

18.1.9 standby timer flow-check

Function

The **standby timer flow-check** command sets the interval for detecting traffic on the primary interface.

The **undo standby timer flow-check** command restores the default interval.

By default, the interval is 10s.

Format

standby timer flow-check *time*

undo standby timer flow-check

Parameters

Parameter	Description	Value
time	Specifies the interval for detecting traffic on the primary interface.	The value ranges from 10 to 600, in seconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

A small interval for detecting traffic on the primary interface may cause a waste of bandwidth resources, and a larger interval for detecting traffic on the primary interface may cause packet loss. Set the interval based on actual networking.

NOTE

To ensure traffic detection correctness, do not change the configured standby interface and traffic detection interval. If the configuration is changed, the traffic detection result may be incorrect, causing an incorrect interface status switchover.

Example

Configure GE1/0/0 as the backup interface of GE2/0/0, and set the maximum bandwidth of GE2/0/0 to 10000 kbit/s, upper and lower thresholds to 80% and 50%, and interval for detecting traffic to 60s.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] standby interface gigabitethernet1/0/0 50
[Huawei-GigabitEthernet2/0/0] standby bandwidth 10000
[Huawei-GigabitEthernet2/0/0] standby threshold 80 50
[Huawei-GigabitEthernet2/0/0] standby timer flow-check 60
```

Related Topics

18.1.3 standby interface

18.2 Interface Monitoring Group Configuration Commands

18.2.1 binding interface

Function

The **binding interface** command adds an interface to an interface monitoring group.

The **undo binding interface** command removes an interface from an interface monitoring group.

By default, an interface monitoring group has no binding interface.

Format

binding interface *interface-type interface-number* [**down-weight** *down-weight-value*]

undo binding interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of a binding interface.	The binding interfaces can be physical Ethernet interfaces, POS interfaces, ATM interfaces, Eth-Trunk interfaces, or IP-Trunk interfaces.
down-weight *down-weight-value*	Specifies the down-weight of a binding interface. If the sum of binding interface down-weights in an interface monitoring group is greater than that of the track interface, the track interface goes Down.	The value is an integer ranging from 1 to 1000. The default value is 10.

Views

Interface monitoring group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Generally, binding interfaces are network-side interfaces. Any network-side interface can be added to an interface monitoring group. An interface monitoring group changes the status of track interfaces based on the status of binding interfaces.

In a dual-system backup scenario, after an interface monitoring group is created using the **monitor-group** command, the **binding interface** command needs to be run to add network-side interfaces to the interface monitoring group.

Prerequisites

The **monitor-group** command has been run to create an interface monitoring group before running the **binding interface** command.

Precautions

An interface monitoring group has a maximum of 32 binding interfaces.

NOTE

An interface can be either a binding interface or a track interface.

An Eth-Trunk and its member interfaces cannot be added to the same interface monitoring group.

Example

Add GE 1/0/0 to an interface monitoring group, and set the down-weight to 20 for GE 1/0/0.

```
<Huawei> system-view
[Huawei] monitor-group group1
[Huawei-monitor-group-group1] binding interface GigabitEthernet 1/0/0 down-weight 20
```

Related Topics

18.2.5 monitor-group

18.2.2 clear monitor-group

Function

The **clear monitor-group** command deletes invalid interfaces from an interface monitoring group.

Format

clear monitor-group *monitor-group-name* **invalid-interface** { **binding** | **track** }

Parameters

Parameter	Description	Value
monitor-group-name	Specifies the name of an interface monitoring group.	The value is a string of 1 to 31 case-sensitive characters without spaces.
invalid-interface	Deletes invalid interfaces from an interface monitoring group.	-
binding	Deletes invalid binding interfaces from an interface monitoring group.	-
track	Deletes invalid track interfaces associated with an interface monitoring group.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a board is removed from a device, the interfaces that reside on the board and are added to be an interface monitoring interface become invalid. These interfaces cannot be removed from the interface monitoring group because they do not exist. To address the problem, run the **clear monitor-group** command to delete the invalid interfaces from the interface monitoring group.

Prerequisites

The **monitor-group** command has been run to create an interface monitoring group before running the **clear monitor-group** command.

Precautions

After the **clear monitor-group** command is run, invalid interfaces are removed from a specified interface monitoring group.

Before deleting invalid interfaces, check whether the deletion operation does not cause the trigger-down-weight value of a track interface to be greater than the sum of the down-weight values of all binding interfaces. If the deletion operation causes the trigger-down-weight value of a track interface to be greater than the sum of the down-weight values of all binding interfaces, the interface monitoring group becomes invalid.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete invalid binding interfaces from an interface monitoring group named **group1**.

```
<Huawei> clear monitor-group group1 invalid-interface binding
```

Related Topics

18.2.5 monitor-group

18.2.1 binding interface

18.2.6 track monitor-group

18.2.3 display monitor-group

Function

The **display monitor-group** command displays information about interface monitoring groups.

Format

display monitor-group [*monitor-group-name*]

Parameters

Parameter	Description	Value
monitor-group-name	Specifies the name of an interface monitoring group. If *monitor-group-name* is specified in the command, the detailed information about the specified interface monitoring group is displayed. If *monitor-group-name* is not specified in the command, the brief information about all interface monitoring groups is displayed.	The value is a string of 1 to 31 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The status of a binding interface consists of the physical status (Up/Down) and BFD status (Up/Down).

After the **display monitor-group** command is run to display the brief information about all interface monitoring groups, the interface monitoring groups are displayed and arranged alphabetically by name.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the brief information about all interface monitoring groups.

```
<Huawei> display monitor-group
Monitor-group number : 6
monitor-group                down weight        status    index
a1                           50                 Active    3
b1                           120                Active    1
c1                           70                 Active    4
d1                           40                 Active    5
e1                           90                 Active    6
f1                           100                Active    2
```

Table 18-2 Description of the **display monitor-group** command output

Item	Description
monitor-group	Indicates the name of an interface monitoring group.
down weight	Indicates the down weight of a binding interface group
status	Indicates the status of an interface monitoring group. ● Active: indicates that an interface monitoring group is in the Active state. ● Inactive: indicates that an interface monitoring group is in the Inactive state.
index	Index of an interface monitoring group.

Display the detailed information about an interface monitoring group named **f1**.

```
<Huawei> display monitor-group f1
 monitor-group f1
   Index            : 1
   Down weight      : 20
   Weight sum       : 40
   Max track weight : 100
   Trigger-up delay : 20 (s)
   Status           : Inactive
-------------------------------------------------------
  monitor-group binding interface number : 2
-------------------------------------------------------
   Interface name  :  GigabitEthernet7/0/1
   Interface index :  11
   Config down weight     :  20
   Phystatus       :  UP
   Bfdstatus       :  -
   LastPhyuptime   :  -
   LastPhydowntime :  -
   LastBFDuptime   :  -
   LastBFDdowntime :  -
   ValidFlag       :  valid

   Interface name  :  GigabitEthernet7/0/2
   Interface index :  12
   Down-weight     :  20
```

```
  Phystatus       :  DOWN
  Bfdstatus       :  -
  LastPhyuptime   :  -
  LastPhydowntime :  -
  LastBFDuptime   :  -
  LastBFDdowntime :  -
  ValidFlag       :  valid

-------------------------------------------------------
 monitor-group track interface number : 1
-------------------------------------------------------
  Interface name      :  Ethernet3/0/1
  Interface index     :  51
  Trigger-down-weight :  100
  TriggerStatus       :  NORMAL
  LastTriggerUpTime   :  -
  LastTriggerDownTime :  -
  ValidFlag           :  valid
```

Table 18-3 Description of the **display monitor-group** command output

Item	Description
index	Index of an interface monitoring group.
Down weight	Indicates the down-weight of an interface monitoring group.
Weight sum	Indicates the sum of down-weights of all binding interfaces.
Max track weight	Indicates that the maximum trigger-down-weight among the trigger-down-weights of track interfaces associated with an interface monitoring group.
Trigger-up delay	The delay for a track interface to go Up.
Status	Indicates the status of an interface monitoring group. ● Active: indicates that an interface monitoring group is in the Active state. ● Inactive: indicates that an interface monitoring group is in the Inactive state.
monitor-group binding interface number	Indicates the number of binding interfaces in an interface monitoring group.
Interface name	Indicates the interface name.
Interface index	Indicates the interface index.
Config down weight	Indicates the down weight of a binding interface.
LastPhyuptime	Indicates the time at which the physical status of a binding interface becomes Up last time. "-" indicates that the physical status of a binding interface remains unchanged.

Item	Description
LastPhydowntime	Indicates the time at which the physical status of a binding interface becomes Down last time. "-" indicates that the physical status of a binding interface remains unchanged.
LastBFDuptime	Indicates the time at which the BFD status of a binding interface becomes Up last time. "-" indicates that the BFD status of a binding interface remains unchanged.
LastBFDdowntime	Indicates the time at which the BFD status of a binding interface becomes Down last time. "-" indicates that the BFD status of a binding interface remains unchanged.
ValidFlag	Indicates a flap identifying whether an interface is valid.
monitor-group track interface number	Indicates the total number of track interfaces associated with an interface monitoring group.
Trigger-down-weight	Indicates the trigger-down-weight of a track interface.
TriggerStatus	Indicates the triggered status of a track interface. • NORMAL: The track interface status is not triggered by the monitoring group. • TRIGGER UP: Triggered by the monitoring group, the track interface becomes Up. • TRIGGER DOWN: Triggered by the monitoring group, the track interface becomes Down.
LastTriggerUpTime	Indicates the time at which a track interface is triggered by an interface monitoring group to go Up. "-" indicates that the status of a track interface remains unchanged.
LastTriggerDown-Time	Indicates the time at which a track interface is triggered by an interface monitoring group to go Down. "-" indicates that the status of a track interface remains unchanged.

Related Topics

18.2.5 monitor-group

18.2.4 monitor enable

Function

The **monitor enable** command creates an interface monitoring group.

The **undo monitor enable** command deletes an interface monitoring group.

By default, interface monitoring group is disabled.

Format

monitor enable

undo monitor enable

Parameters

None

Views

Interface monitoring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of network-side interfaces need to be added to or removed from an interface monitoring group, the corresponding trace interface may alternate between Up and Down due to frequent weight changes. To address the problem, run the **undo monitor enable** command to shut down the interface monitoring group. After having added interfaces to or removed interfaces from the interface monitoring group, run the **monitor enable** command.

Prerequisites

The **monitor-group** command has been run to create an interface monitoring group before running the **monitor enable** command.

Precautions

After the **undo monitor enable** command is run, an interface monitoring group is shut down. Network-side interfaces, however, can still be added to or removed from the interface monitoring group, and the interface monitoring group can detect the physical status and BFD status changes of the binding interfaces.

Example

Shut down an interface monitoring group named **group1**.

```
<Huawei> system-view
[Huawei] monitor-group group1
[Huawei-monitor-group-group1] undo monitor enable
```

18.2.5 monitor-group

Function

The **monitor-group** command creates an interface monitoring group and displays the view of the interface monitoring group.

The **undo monitor-group** command deletes an interface monitoring group.

 Copyright © Huawei Technologies Co., Ltd.

By default, no interface monitoring group is created.

Format

monitor-group *monitor-group-name*

undo monitor-group *monitor-group-name*

Parameters

Parameter	Description	Value
monitor-group-name	Specifies the name of an interface monitoring group.	The value is a string of 1 to 31 case-sensitive characters, with spaces not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All monitored network-side interfaces of the same type can be added to a group, called an interface monitoring group. Each interface monitoring group is identified by a unique name. The monitored network-side interfaces are binding interfaces. The access-side interfaces associated with an interface monitoring group are called track interfaces. The status of the track interfaces is associated with the status of the monitoring interface group. An interface monitoring group monitors the status of the binding interfaces. If the number of binding interfaces that go Down reaches a certain value, the status of corresponding track interfaces becomes Down, and services are switched to the backup link. When the number of binding interfaces in the Down state falls below a certain value, the status of the corresponding track interface goes Up again, and the services are switched back to the master link.

In a dual-system backup scenario, if a network-side link fails, the **monitor-group** command can be used to create an interface monitoring group to monitor the status of access-side interfaces. This enables services to be switched to the backup link in time, preventing traffic overload and forwarding failures.

Precautions

After the **monitor-group** *monitor-group-name* command is run, if there is no interface monitoring group with the name specified *monitor-group-name*, a new interface monitoring group will be created. If there is an interface monitoring group with the name specified by *monitor-group-name*, the view of the interface monitoring group is displayed.

A maximum of 32 interface monitoring groups can be configured on a device.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The **undo monitor-group** command deletes all configurations of an interface monitoring group. If an interface monitoring group is still associated with track interfaces, the interface monitoring group cannot be deleted.

Example

Create an interface monitoring group named **group1**.

```
<Huawei> system-view
[Huawei] monitor-group group1
[Huawei-monitor-group-group1]
```

Related Topics

18.2.3 display monitor-group

18.2.6 track monitor-group

Function

The **track monitor-group** command configures an interface to track an interface monitoring group.

The **undo track monitor-group** command cancels the configuration.

By default, an interface does not track any interface monitoring group.

Format

track monitor-group *monitor-group-name* [**trigger-down-weight** *trigger-down-weight-value*]

undo track monitor-group

Parameters

Parameter	Description	Value
monitor-group-name	Specifies the name of an interface monitoring group to be tracked by an interface.	The value is a string of 1 to 31 case-sensitive characters, with spaces not supported.
trigger-down-weight *trigger-down-weight-value*	Specifies the trigger-down-weight of a track interface.	The value is an integer ranging from 1 to 1000. The default value is the sum of down-weights of all binding interfaces in an interface monitoring group.

Views

Interface monitoring group view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a dual-system backup scenario, after an interface monitoring group is created using the **monitor-group** command and network-side interfaces are added to the interface monitoring group using the **binding interface** command, the **track monitor-group** command needs to be run to configure access-side interfaces to track the interface monitoring group. If the number of binding interfaces that go Down reaches a certain value, the status of corresponding track interfaces becomes Down, and services are switched to the backup link. When the number of binding interfaces in the Down state is smaller than a certain value, the status of the corresponding track interface goes Up again, and the services are switched back to the master link.

Prerequisites

The **monitor-group** command has been run to create an interface monitoring group before running the **track monitor-group** command.

Precautions

After the **track monitor-group** command is run, an interface tracks a specified interface monitoring group, and changes its own status based on the status of the binding interfaces in the interface monitoring group.

An interface monitoring group can be tracked by a maximum of 256 track interfaces, and a track interface, however, can track only one interface monitoring group.

The track interface must be a VE interface, an Ethernet interface, an Ethernet sub-interface, an ATM interface, an ATM sub-interface, an Eth-Trunk interface, an Eth-Trunk sub-interface, or a Tunnel interface. An Eth-Trunk and its member interfaces cannot be associated with the same interface group.

NOTE

The trigger-down-weight of a track interface must be smaller than the sum of the down-weights of all binding interfaces in an interface monitoring group.

Example

Configure GE 2/0/0 to track an interface monitoring group named **group1**, and set the trigger-down-weight to 100 for GE 2/0/0.

```
<Huawei> system-view
[Huawei] monitor-group group1
[Huawei-monitor-group-group1] binding interface GigabitEthernet 1/0/0 down-weight 20
[Huawei-monitor-group-group1] binding interface GigabitEthernet 1/0/1 down-weight 40
[Huawei-monitor-group-group1] binding interface GigabitEthernet 1/0/2 down-weight 60
[Huawei-monitor-group-group1] quit
[Huawei] interface GigabitEthernet 2/0/0
[Huawei-GigabitEthernet2/0/0] track monitor-group group1 trigger-down-weight 100
[Huawei-GigabitEthernet2/0/0] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

18.2.5 monitor-group

18.2.7 trigger-up-delay

Function

The **trigger-up-delay** command sets the delay for a track interface to go Up.

The **undo trigger-up-delay** command restores the default setting.

By default, a track interface becomes Up immediately after corresponding binding interface go Up.

Format

trigger-up-delay *trigger-up-delay-value*

undo trigger-up-delay

Parameters

Parameter	Description	Value
trigger-up-delay-value	Specifies the delay for a track interface to go Up.	The value is an integer ranging from 1 to 4294967295, in seconds.

Views

Interface monitoring group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a network fault is rectified and corresponding binding interfaces of an interface monitoring group become Up, it takes a certain period of time to establish routes and entries. If a track interface immediately becomes Up, packet loss will occur because the corresponding binding interface cannot forward packets. The **trigger-up-delay** command can be used to set the delay for the track interface to go Up. This prevents packet loss caused by the status inconsistency between the binding interface and track interface.

Precaution

After the **trigger-up-delay** *trigger-up-delay-value* command is run, a track interface goes Up *trigger-up-delay-value* seconds after the corresponding binding interface recovers from a fault.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the delay for a track interface to go Up to 20s.

```
<Huawei> system-view
[Huawei] monitor-group group1
[Huawei-monitor-group-group1] trigger-up-delay 20
```

18.3 NSR Configuration Commands

NOTE

Only the AR3200 series support NSR.

18.3.1 display switchover mode

Function

The **display switchover mode** command displays the HA working mode of the current system.

Format

display switchover mode

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

HA has two working modes: Nonstop Forwarding (NSF) and Nonstop Routing (NSR). The system allows only one working mode to run at a time. You can run the **display switchover mode** command to view the running mode.

Example

Display the HA working mode of the current system.

```
<Huawei> display switchover mode
Switchover mode: nonstop-routing.
```

Table 18-4 Description of the display switchover mode command output

Item	Description
Switchover mode	HA working mode of the system.

18.3.2 switchover mode

Function

The **switchover mode** command sets the HA working mode for the system.

By default, the HA working mode is NSF.

Format

switchover mode { **nonstop-routing** | **nonstop-forwarding** }

Parameters

Parameter	Description	Value
nonstop-routing	Sets the HA working mode to NSR (Non-Stopping Routing) for the system. In NSR mode, the system can process routes and forward services without interruption.	-
nonstop-forwarding	Sets the HA working mode to nonstop forwarding (NSF) for the system. In NSF mode, service interruption duration is greatly reduced.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A system failure, software upgrade, or system maintenance may trigger a master/slave switchover on the device. In this case, you can set the HA working mode to NSF or NSR for the system to ensure nonstop service forwarding and high device reliability after the master/slave MPU switchover is performed. You can set the NSF or NSR mode based on the following situations:

 Copyright © Huawei Technologies Co., Ltd.

- When a network has low requirements for packet loss ratio and route convergence, you can run the **switchover mode nonstop-forwarding** command to enable the NSF function.
- When a network has high requirements for packet loss ratio and route convergence, you can run the **switchover mode nonstop-routing** command to enable the NSR function.

Prerequisites

Before using the **switchover mode** command, ensure that the device has a master MPU and a slave MPU and the system is in the real-time backup state.

Precautions

After the NSF mode is switched to the NSR mode, the system restarts the slave MPU and the master MPU backs up data to the slave MPU. During the process, other configuration operations cannot be performed.

Ensure that the network topology and interface status are unchanged during the master/slave MPU switchover. Otherwise, service forwarding may fail.

Example

Set the HA working mode to NSR for the system.

```
<Huawei> system-view
[Huawei] switchover mode nonstop-routing
```

18.4 HSB Configuration Commands

NOTE

- HSB allows only two devices to back up each other. In addition, the model and software version of the two devices must be the same.
- Only firewall HSB is supported.
- In a hot standby system, the master and slave systems exchange TCP plain-text data, which brings security risk. It is recommended to configure IPSec between the master and slave systems to protect data.

18.4.1 bind-service

Function

The **bind-service** command binds an HSB service to an HSB group.

The **undo bind-service** command unbinds the HSB service from the HSB group.

By default, no HSB service is bound to an HSB group.

Format

bind-service *service-index*

undo bind-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The value is fixed as 0.

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB group synchronizes backup information and responds to link status changes through the HSB channel established by the HSB service. To make the HSB group work properly, bind an HSB service to the HSB group.

Prerequisites

An HSB group has been configured.

Example

Bind HSB service 0 to an HSB group.

```
<Huawei> system-view
[Huawei] hsb-group 0
[Huawei-hsb-group-0] bind-service 0
```

Related Topics

18.4.11 hsb-group

18.4.2 display firewall hsb statistics event

Function

The **display firewall hsb statistics event** command displays statistics on firewall HSB events.

Format

display firewall hsb statistics event

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view statistics on firewall HSB events, run this command.

Example

Display statistics on firewall HSB events.

```
<Huawei> display firewall hsb statistics event
Firewall HSB Statistic Event:
-----------------------------------------------------------
  Firewall Notify Fecd Enable Error  : 0
  Firewall Notify Fecd Working Error : 0
  Firewall Notify Fecd Tunnel  Error : 0
  Firewall Notify Fecd Status  Error : 0
  Firewall Notify Fecd Purge   Error : 0
  Firewall Notify Fecd Backup  Error : 0

  Firewall Receive Purge Entry        : 1
  Firewall Receive Purge Event        : 0
  Firewall Purge Write Error          : 0

  Firewall Receive Backup Entry:      : 0
  Firewall Receive Backup Event       : 0
  Firewall Backup Write Error         : 0

  Firewall Receive Event Error        : 0
  Firewall Deal Event Event           : 0
  Firewall Deal Event Independent     : 0
  Firewall Deal Event Del             : 1
  Firewall Deal Event Add             : 0
  Firewall Deal Event Switch          : 0

  Firewall Receive Pkt Error          : 0
  Firewall Deal Pkt Event             : 0
  Firewall Deal Pkt Switch End        : 0
  Firewall Deal Pkt Backup End        : 1
  Firewall Write Event End Error      : 0

  Firewall Receive Tunnel Cfg Error   : 0
  Firewall Send Fecd Cfg Error        : 0
  Firewall Deal Tunnel Add            : 1
  Firewall Deal Tunnel Del            : 0

  Firewall Write Event Que Failed     : 0
  Firewall Write Pkt Que Failed       : 0
  Firewall Write Srv-cfg Que Failed   : 0
-----------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 18-5 Description of the display firewall hsb statistics event command output

Item	Description
Firewall Notify Fecd Enable Error	The control plane notifies the forwarding plane of the failure in enabling the firewall HSB function.
Firewall Notify Fecd Working Error	The control plane notifies the forwarding plane of the failure in enabling the firewall function.
Firewall Notify Fecd Tunnel Error	The control plane notifies the forwarding plane of the failure in setting HSB service channel parameters.
Firewall Notify Fecd Status Error	The control plane notifies the forwarding plane of the failure in backup.
Firewall Notify Fecd Purge Error	The control plane notifies the forwarding plane of the batch deletion failure.
Firewall Notify Fecd Backup Error	The control plane notifies the forwarding plane of the batch backup failure.
Firewall Receive Purge Entry	Entrance for receiving the batch deletion end event from the forwarding plane on the control plane.
Firewall Receive Purge Event	Failure in receiving the batch deletion end event from the forwarding plane on the control plane.
Firewall Purge Write Error	Errors occur when the control plane completes writing HSB mechanism batch deletion events.
Firewall Receive Backup Entry	Entrance for receiving the batch backup end event from the forwarding plane on the control plane.
Firewall Receive Backup Event	Failure in receiving the batch backup end event from the forwarding plane on the control plane.
Firewall Backup Write Error	Errors occur when the control plane completes writing HSB mechanism batch backup events.
Firewall Receive Event Error	Errors occur when firewall HSB receives HSB group events.
Firewall Deal Event Event	Firewall HSB fails to process HSB group events.
Firewall Deal Event Independent	Firewall HSB processes HSB group independent events.
Firewall Deal Event Del	Firewall HSB processes HSB group batch deletion events.
Firewall Deal Event Add	Firewall HSB processes HSB group batch backup events.
Firewall Deal Event Switch	Firewall HSB processes HSB group switch events.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Firewall Receive Pkt Error	Errors occur when firewall HSB receives HSB mechanism packets.
Firewall Deal Pkt Event	Firewall HSB fails to process HSB mechanism packets.
Firewall Deal Pkt Switch End	Firewall HSB receives the peer firewall master/backup switch end packets.
Firewall Deal Pkt Backup End	Firewall HSB receives the peer firewall batch backup end packets.
Firewall Write Event End Error	Errors occur when the control plane completes writing HSB mechanism batch backup or switch events.
Firewall Receive Tunnel Cfg Error	Errors occur when firewall HSB receives HSB channel configurations.
Firewall Send Fecd Cfg Error	Firewall HSB fails to deliver channel configurations to the forwarding plane.
Firewall Deal Tunnel Add	Firewall HSB receives channel adding events.
Firewall Deal Tunnel Del	Firewall HSB receives channel deletion events.
Firewall Write Event Que Failed	Number of failures to write HSB notification events received by firewall HSB into the queue.
Firewall Write Pkt Que Failed	Number of failures to write HSB packets received by firewall HSB into the queue.
Firewall Write Srv-cfg Que Failed	Number of failures to write HSB channel configuration notifications received by firewall HSB into the queue.

18.4.3 display hsb statistics hsb-group

Function

The **display hsb statistics hsb-group** command displays statistics on processes of an HSB group.

Format

display hsb statistics hsb-group *group-index* **event**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The value is 0 and only one HSB group is supported.
event	Indicates process statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hsb statistics hsb-group** command displays statistics on processes. Two main processes are involved: negotiation process and switching process.

Example

Display statistics on processes of the HSB public mechanism.

```
<Huawei> display hsb statistics hsb-group 0 event
Hot Standby Statistic Event:
-----------------------------------------------------------
Hot Standby Group Dealed Vrrp Group Record:
  Local_Vrrp Peer_Vrrp  Batch_Status  Systime
  BACKUP     BACKUP     Ind            No   2013-4-23 11:55:2
  MASTER     BACKUP     Ind            No   2013-4-23 11:55:8

Hot Standby Group Event Record:
  Run Independent Event   : 0
  Realtime Sync Event     : 0
  Delete Event(Snd, Recv) : 0, 0
  Add Event(Snd, Recv)    : 1, 0
  Switch Event(Snd, Recv) : 0, 0

Hot Standby Group Process Record:
  Negotiate Start Entry                : 1
  Negotiate Has Started                : 0
  Negotiate Start Send Pkt Failed      : 0

  Negotiate Req Entry                  : 0
  Negotiate Req Failed                 : 0
  Negotiate Req Batch Status Error     : 0
  Negotiate Req Vrrp Status Error      : 0
  Negotiate Req Check Para Failed      : 0
  Negotiate Req Notify Event Failed    : 0

  Negotiate Del Entry                  : 0
  Negotiate Del Batch Status Error     : 0
  Negotiate Del Vrrp Status Error      : 0
  Negotiate Del Send Pkt Failed        : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Negotiate Ack Entry                  : 1
Negotiate Ack Failed                 : 0
Negotiate Ack Batch Status Error      : 0
Negotiate Ack Vrrp Status Error       : 0
Negotiate Ack Notify Event Failed     : 0

Negotiate Add Entry                  : 0
Negotiate Add Batch Status Error      : 0
Negotiate Add Vrrp Status Error       : 0
Negotiate Add Send Pkt Failed         : 0

Negotiate End Entry                  : 1
Negotiate End Failed                 : 0
Negotiate End Batch Status Error      : 0
Negotiate End Vrrp Status Error       : 0

Switch Start Entry                   : 0
Switch Has Started                   : 0
Switch Start Send Pkt Failed         : 0

Switch Req Entry                     : 0
Switch Req Failed                    : 0
Switch Req Batch Status Error        : 0
Switch Req Notify Event Failed       : 0

Switch Switching Entry               : 0
Switch Switching Batch Status Error   : 0
Switch Switching Send Pkt Failed      : 0
Switch Switching Vrrp Changed         : 0
Switch Switching Notify Vrrp Failed   : 0

Switch End Entry                     : 0
Switch End Failed                    : 0
Switch End Batch Status Error        : 0
Switch End Vrrp Changed              : 0
Switch End Notify Vrrp Failed        : 0

HSB Group Vrrp All Master            : 0
HSB Group Vrrp All Backup            : 0

HSB Group Notify All Group Event Error : 0
HSB Group Notify One Group Event Error : 0
HSB Group Receive Group Event Error    : 0
HSB Group Vrrp State Event             : 2
HSB Group Vrrp State Dealed Event      : 0
HSB Group Packet To Task Error         : 0
HSB Group Packet To Task Failed        : 0
-----------------------------------------------------------
```

Table 18-6 Description of the display hsb statistics hsb-group command output

Item	Description
Hot Standby Group Dealed Vrrp Group Record	Record of the VRRP group of which services are received and processed by the HSB group.
Local_Vrrp	Local VRRP group.
Peer_Vrrp	Remote VRRP group.
Batch_Status	Backup process status.
Switch_Flag	Whether there are two master devices.
Systime	System time.

Item	Description
Hot Standby Group Event Record	Record of events notified by the backup service module and received events.
Run Independent Event	Number of events running independently.
Realtime Sync Event	Number of events synchronized in real time.
Delete Event(Snd, Recv)	Number of deleted events that are received or sent.
Add Event(Snd, Recv)	Number of added events that are received or sent.
Switch Event(Snd, Recv)	Number of switched events that are received or sent.
Hot Standby Group Process Record	Statistics on backup processes of the HSB public mechanism.
Negotiate Start Entry	The master device starts to be negotiated.
Negotiate Has Started	Negotiating master and backup devices has started.
Negotiate Start Send Pkt Failed	Sending negotiation packets fails.
Negotiate Req Entry	Batch deletion of backup devices starts.
Negotiate Req Failed	The master device fails to send negotiation-start packets to the backup device.
Negotiate Req Batch Status Error	The backup process status is incorrect. The backup process status of the current backup group is not Independent.
Negotiate Req Vrrp Status Error	The VRRP group status is incorrect and is not Backup.
Negotiate Req Check Para Failed	The backup device checks that some backup parameters from the master device are invalid.
Negotiate Req Notify Event Failed	The backup device notifies that batch deleting backup services fails.
Negotiate Del Entry	Batch deleting firewall services on the backup device is complete.
Negotiate Del Batch Status Error	The backup device fails to check the negotiation process and is not none.
Negotiate Del Vrrp Status Error	The backup device fails to check the VRRP group status.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Negotiate Del Send Pkt Failed	The backup device fails to send batch deletion complete messages to the master device.
Negotiate Ack Entry	Batch backup on the master device starts.
Negotiate Ack Failed	The backup device notifies the master device that the negotiation end message fails to be sent.
Negotiate Ack Batch Status Error	The master device fails to check the negotiation process and is not Batch-Started.
Negotiate Ack Vrrp Status Error	The VRRP group status of the master device is incorrect.
Negotiate Ack Notify Event Failed	The master device fails to notify batch backup events on the firewall forwarding plane.
Negotiate Add Entry	The master device receives a message indicating that batch backup on the firewall forwarding plane is complete.
Negotiate Add Batch Status Error	The master device fails to check the negotiation process and is not Batch-Adding.
Negotiate Add Vrrp Status Error	The master device fails to check the VRRP group status and is not Backup.
Negotiate Add Send Pkt Failed	The master device fails to send batch deletion complete messages to the backup device.
Negotiate End Entry	Negotiation ends.
Negotiate End Failed	The master device notifies the backup device that the negotiation end message fails to be sent.
Negotiate End Batch Status Error	The master device fails to check the negotiation process and is not Batch-Adding.
Negotiate End Vrrp Status Error	The VRRP group status is incorrect and is not Master.
Switch Start Entry	Switching starts.
Switch Has Started	Switch Has Started.
Switch Start Send Pkt Failed	Sending switching-start messages fails.
Switch Req Entry	The original master device responds to switching messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Switch Req Failed	The original backup device fails to initiate switching.
Switch Req Batch Status Error	The original master device fails to check the switching process status and is not Realtime.
Switch Req Notify Event Failed	The original master device fails to notify switching of backup services.
Switch Switching Entry	Switching is complete.
Switch Switching Batch Status Error	The original slave device fails to check the switching process status.
Switch Switching Send Pkt Failed	The original backup service fails to send a message indicating that the switching is complete.
Switch Switching Vrrp Changed	During switching, the VRRP status of the original backup device changes.
Switch Switching Notify Vrrp Failed	During switching, the VRRP status of the backup device changes and is not master. The change is notified to the remote device.
Switch End Entry	Switching ends.
Switch End Failed	The original backup device receives a message indicating the switching failure.
Switch End Batch Status Error	The original master device fails to check the switching process status.
Switch End Vrrp Changed	During switching, the VRRP status of the original backup device changes.
Switch End Notify Vrrp Failed	During switching, the VRRP status of the backup device changes and is not backup. The change is notified to the remote device.
HSB Group Vrrp All Master	There are two master devices.
HSB Group Vrrp All Backup	There are two backup devices.
HSB Group Notify All Group Event Error	The HSB group fails to notify backup events of all VRRP groups.
HSB Group Notify One Group Event Error	The HSB group fails to notify backup events of a single VRRP group.
HSB Group Receive Group Event Error	The HSB group fails to receive a notification indicating that the backup service is complete.
HSB Group Vrrp State Event	VRRP group status change event.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
HSB Group Packet To Task Error	An error occurs when the HSB group delivers HSB service packets.
HSB Group Packet To Task Failed	The HSB group fails to deliver HSB service packets.

Related Topics

18.4.17 reset hsb statistics hsb-group

18.4.4 display hsb statistics hsb-service

Function

The **display hsb statistics hsb-service** command displays statistics on packets or processes of the HSB public mechanism.

Format

display hsb statistics hsb-service *service-index* { **event** | **packet** }

Parameters

Parameter	Description	Value
service-index	Specifies the index of an HSB service.	The value is 0 and only one HSB service is supported.
packet	Indicates packet statistics.	-
event	Indicates process statistics.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hsb statistics hsb-service** command displays statistics on received, sent, and discarded packets or processes of the HSB public mechanism.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics on processes of the HSB public mechanism.

```
<Huawei> display hsb statistics hsb-service 0 event
Hot Standby Service Process Record:
-----------------------------------------------------------
  HSB Service Packet To Group Failed    : 0
  HSB Service Packet To Group Error     : 0
  HSB Service Packet To Task Error      : 0
  HSB Service Packet To Outer Error     : 0
  HSB Service Tunnel State Event        : 1
-----------------------------------------------------------
```

Table 18-7 Description of the **display hsb statistics hsb-service** command output

Item	Description
HSB Service Packet To Group Failed	An error occurs when the HSB service delivers HSB service packets to the HSB group.
HSB Service Packet To Group Error	Failure to deliver HSB service packets to the HSB group.
HSB Service Packet To Task Error	Failure to deliver HSB service packets to the backup service.
HSB Service Packet To Outer Error	Failure to deliver HSB service packets to the external module (HSB group or HSB service).
HSB Service Tunnel State Event	HSB service tunnel status event.

Related Topics

18.4.18 reset hsb statistics hsb-service

18.4.5 display hsb-group

Function

The **display hsb-group** command displays information about an HSB group.

Format

display hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the ID of an HSB group.	The value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about an HSB group.

Example

Display information about HSB group 0.

```
<Huawei> display hsb-group 0
Hot Standby Group Information:
-----------------------------------------------------------
  HSB-group ID                : 0
  Vrrp Group ID               : 2
  Vrrp Interface              : Vlanif100
  Service Index               : 0
  Group Vrrp Status           : Master
  Group Status                : Active
  Group Backup Process        : Realtime
  Peer Group Device Name      : AR1220
  Peer Group Software Version : V200R010
  Group Backup Modules        : Firewall
```

Table 18-8 Description of the display hsb-group command output

Item	Description
HSB-group ID	ID of an HSB group.
Vrrp Group ID	VRID of the Virtual Router Redundancy Protocol (VRRP) group.
Vrrp Interface	Interface configured with the VRRP group.
Service Index	HSB service ID.
Group Vrrp Status	Status of the VRRP group: ● Master ● Backup ● Initialize
Group Status	HSB group status: ● Active ● Inactive ● Independent ● Switching

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Group Backup Process	Backup process status: ● Independent: independent backup state ● Batch-Started: batch backup negotiation state ● Batch-Deleting: batch deletion state ● Batch-Delete-End: batch deletion end state ● Batch-Adding: batch backup state ● Realtime: real-time backup state ● Switching: switching state
Peer Group Device Name	Device name corresponding to the peer HSB group.
Peer Group Software Version	Software version corresponding to the peer HSB group.
Group Backup Modules	Service module bound to the HSB group.

Related Topics

18.4.11 hsb-group
18.4.12 hsb-service
18.6.37 vrrp vrid virtual-ip

18.4.6 display hsb-service

Function

The **display hsb-service** command displays information about an HSB service.

Format

display hsb-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The value is fixed as 0.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about an HSB service.

Example

Display the HSB service configuration.

```
<Huawei> display hsb-service 0
Hot Standby Service Information:
-----------------------------------------------------------
  Local IP Address       : 192.168.4.1
  Peer IP Address        : 192.168.4.2
  Source Port            : 10245
  Destination Port       : 10245
  Keep Alive Times       : 5
  Keep Alive Interval    : 3
  Service State          : Not Valid
  Service Batch Modules  :
  Shared-key             : -
-----------------------------------------------------------
```

Table 18-9 Description of the **display hsb-service** command output

Item	Description
Local IP Address	IP address of the local device. To set this parameter, run the **18.4.19 service-ip-port** command.
Peer IP Address	IP address of the peer device. To set this parameter, run the **18.4.19 service-ip-port** command.
Source Port	Local port number. To set this parameter, run the **18.4.19 service-ip-port** command.
Destination Port	Destination port number. To set this parameter, run the **18.4.19 service-ip-port** command.
Keep Alive Times	Number of times that heartbeat packets are sent. To set this parameter, run the **18.4.20 service-keep-alive detect** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Keep Alive Interval	Interval for sending heartbeat packets. To set this parameter, run the **18.4.20 service-keep-alive detect** command.
Service State	Status of the HSB service: • Connected • Disconnected • Not Valid
Service Batch Modules	Service modules bound to an HSB service.
Shared-key	Key used by the HSB devices. To set this parameter, run the **18.4.15 key** command.

18.4.7 display hsb-service-type firewall hsb-group

Function

The **display hsb-service-type firewall hsb-group** command displays firewall HSB group information.

Format

display hsb-service-type firewall hsb-group

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the firewall service works in HSB mode, you can run this command to view firewall HSB group information.

Example

Display firewall HSB group information.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display hsb-service-type firewall hsb-group
Firewall HSB Group Information:
-------------------------------------------------------
  Firewall HSB Group : 0
-------------------------------------------------------
```

Table 18-10 Description of the **display hsb-service-type firewall hsb-group** command output

Item	Description
Firewall HSB Group	ID of the HSB group.

18.4.8 display hsb-service-type vpn-instance

Function

The **display hsb-service-type vpn-instance** command displays information about the HSB service bound to a VPN instance.

Format

display hsb-service-type vpn-instance hsb-service

Parameters

Parameter	Description	Value
hsb-service	Information about the HSB service.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display hsb-service-type vpn-instance** command displays information about the HSB service bound to a VPN instance.

Example

Display information about the HSB service bound to a VPN instance.

```
<Huawei> display hsb-service-type vpn-instance hsb-service
Vpn-instance HSB Service Information:
```

```
-----------------------------------------------------------
 Vpn-instance HSB Service : 0
-----------------------------------------------------------
```

Related Topics

18.4.14 hsb-service-type vpn-instance

18.4.9 display hsb-service-type vpn-instance information

Function

The **display hsb-service-type vpn-instance information** command displays HSB information about VPN instances.

Format

display hsb-service-type vpn-instance information

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view the mapping between the VPN instance name, VPN instance ID on the local device, and VPN instance ID on the remote device.

Example

Display HSB information about VPN instances.

```
<Huawei> display hsb-service-type vpn-instance information
Vpn-instance HSB information:
-------------------------------------------------------------------
 Vpn-Name                    Local Vpn-ID     Remote Vpn-ID
 aaa                       1            1
 abcd                       2            -
 bbb                       3            3
 ddd                       4            4
 eee                       5            5
 asdf                      -            2
-------------------------------------------------------------------
```

Table 18-11 Description of the display hsb-service-type vpn-instance information command output

Item	Description
Vpn-Name	VPN instance name.
Local Vpn-ID	VPN instance ID on the local device.
Remote Vpn-ID	VPN instance ID on the remote device.

18.4.10 hsb enable

Function

The **hsb enable** command enables HSB for an HSB group.

The **undo hsb enable** command disables HSB for an HSB group.

By default, HSB is disabled.

Format

hsb enable

undo hsb enable

Parameters

None

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After HSB is enabled for an HSB group, the HSB group configuration takes effect and the HSB group can notify service modules of link status changes. You can run the **hsb enable** command to enable HSB for an HSB group after the HSB group configuration is complete.

Precautions

Do not run the **undo hsb enable** command when the master and backup devices perform batch backup.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable HSB for HSB group 0.

```
<Huawei> system-view
[Huawei] hsb-group 0
[Huawei-hsb-group-0] hsb enable
```

Related Topics

18.4.11 hsb-group

18.4.11 hsb-group

Function

The **hsb-group** command creates an HSB group.

The **undo hsb-group** command deletes an HSB group.

By default, no HSB group is created.

Format

hsb-group *group-index*

undo hsb-group *group-index*

Parameters

Parameter	Description	Value
group-index	Specifies the ID of an HSB group.	The value is fixed as 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure HSB functions, create an HSB group first. An HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization. An HSB group supports status negotiation and event notification functions, implementing service synchronization on master and backup devices.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After HSB is enabled for an HSB group, an HSB service cannot be bound to the HSB group.

Example

Create HSB group 0.

```
<Huawei> system-view
[Huawei] hsb-group 0
[Huawei-hsb-group-0]
```

Related Topics

18.4.1 bind-service

18.4.5 display hsb-group

18.4.10 hsb enable

18.4.12 hsb-service

18.4.21 track vrrp

18.4.12 hsb-service

Function

The **hsb-service** commands creates an HSB service and displays the HSB service view.

The **undo hsb-service** command deletes an HSB service.

By default, no HSB service is created.

Format

hsb-service *service-index*

undo hsb-service *service-index*

Parameters

Parameter	Description	Value
service-index	Specifies the ID of an HSB service.	The fixed value is 0.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

An HSB service establishes an HSB channel for transmitting packets of other services and maintains the link status by notifying the HSB group of the faulty link. Only after an HSB group is bound to an HSB service, the HSB function can be implemented.

Example

Create HSB service 0.

```
<Huawei> system-view
[Huawei] hsb-service 0
```

Related Topics

18.4.6 display hsb-service

18.4.11 hsb-group

18.4.13 hsb-service-type firewall

Function

The **hsb-service-type firewall** command enables the firewall HSB function and binds the firewall to an HSB group.

The **undo hsb-service-type firewall** command disables the firewall HSB function.

By default, the firewall HSB function is disabled.

Format

hsb-service-type firewall hsb-group *group-index*

undo hsb-service-type firewall hsb-group *group-index*

Parameters

Parameter	Description	Value
hsb-group *group-index*	Specifies the ID of an HSB group.	The value is fixed as 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

All traffic must pass through the firewall. If the firewall fails, all traffic is interrupted. To prevent traffic from being interrupted, solve single-point failures on the firewall by configuring two firewalls to work in backup mode.

Prerequisites

An HSB group has been created using the **hsb-group** command.

Precautions

When enabling the firewall HSB function, ensure that flows in one interzone need to be backed up.

Example

Enable the firewall HSB function and bind the firewall to the created HSB group.

```
<Huawei> system-view
[Huawei] hsb-service-type firewall hsb-group 0
```

Related Topics

18.4.11 hsb-group

18.4.14 hsb-service-type vpn-instance

Function

The **hsb-service-type vpn-instance** command enables backup of VPN information.

The **undo hsb-service-type vpn-instance** command disables backup of VPN information.

By default, backup of VPN information is disabled.

Format

hsb-service-type vpn-instance hsb-service *service-index*

undo hsb-service-type vpn-instance hsb-service *service-index*

Parameters

Parameter	Description	Value
hsb-service *service-index*	Specifies the index of the HSB service.	The value is 0.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To back up VPN information on the HSB channel, run the **hsb-service-type vpn-instance** command.

Prerequisites

The HSB service has been created using the **hsb-service** command.

Example

Enables backup of VPN information.

```
<Huawei> system-view
[Huawei] hsb-service-type vpn-instance hsb-service 0
```

Related Topics

18.4.8 display hsb-service-type vpn-instance

18.4.15 key

Function

The **key** command configures the key used by the HSB devices.

The **undo key** command deletes the key used by the HSB devices.

By default, the key used by HSB devices is not configured.

Format

key cipher *key-string*

undo key

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cipher *key-string*	Indicates the key used by the HSB devices.	The value can be a string of 48 characters in cipher text or a string of 8 to 16 characters in plain text. **NOTE** A secure password should be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters. The password must consist of at least six characters.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure security of HSB information negotiation and service backup and prevent the attacks initiated by using bogus packets or modifying packets, run the **key** command to configure the key used by HSB devices. The key provides authentication and verification mechanisms.

Precautions

- Configuring a shared key for HSB devices is not recommended in a secure network environment, as this configuration will degrade the HSB performance.
- The **key** command must be configured before the **18.4.19 service-ip-port** command. Otherwise, the **key** configuration will fail.
- The two HSB devices must be configured with the same shared key. Inconsistent keys on two ends will cause frequent interruption of the HSB channel.

Example

Set the key used by HSB devices to **Huawei@123**.

```
<Huawei> system-view
[Huawei] hsb-service 0
[Huawei-hsb-service-0] key cipher Huawei@123
```

18.4.16 reset firewall hsb statistics event

Function

The **reset firewall hsb statistics event** command clears statistics on firewall HSB events.

Format

reset firewall hsb statistics event

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

During routine maintenance, to view firewall HSB statistics within a period, clear historical statistics so that the device recollects firewall HSB statistics. You can run this command to clear statistics on firewall HSB events.

Example

Clear statistics on firewall HSB events.

```
<Huawei> reset firewall hsb statistics event
```

18.4.17 reset hsb statistics hsb-group

Function

The **reset hsb statistics hsb-group** command clears statistics on HSB processes.

Format

reset hsb statistics hsb-group *group-index* **event**

Parameters

Parameter	Description	Value
group-index	Specifies the index of an HSB group.	The value is 0 and only one HSB group is supported.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
event	Indicates process statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting HSB statistics within a certain period, run this command to clear the existing HSB statistics. You can run this command to clear statistics about HSB processes. Two main processes are involved: HSB negotiation process and HSB switching process.

Example

Clear statistics about HSB processes.

```
<Huawei> reset hsb statistics hsb-group 0 event
```

Related Topics

18.4.3 display hsb statistics hsb-group

18.4.18 reset hsb statistics hsb-service

Function

The **reset hsb statistics hsb-service** command clears statistics on packets or processes of the HSB public mechanism.

Format

reset hsb statistics hsb-service *service-index* { **packet** | **event** }

Parameters

Parameter	Description	Value
service-index	Specifies the index of an HSB service.	The value is 0 and only one HSB service is supported.
packet	Indicates packet statistics.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
event	Indicates process statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Before collecting HSB statistics within a certain period, run this command to clear the existing HSB statistics. You can run this command to clear statistics on packets or processes of the HSB public mechanism.

Example

Clear statistics on packets of the HSB public mechanism.

```
<Huawei> reset hsb statistics hsb-service 0 packet
```

Clear statistics on processes of the HSB public mechanism.

```
<Huawei> reset hsb statistics hsb-service 0 event
```

Related Topics

18.4.4 display hsb statistics hsb-service

18.4.19 service-ip-port

Function

The **service-ip-port** command configures the IP address and port number of an HSB channel.

The **undo service-ip-port** command deletes the IP address and port number of an HSB channel.

By default, the IP address and port number of an HSB channel are not configured.

Format

service-ip-port local-ip *local-ip-address* **peer-ip** *peer-ip-address* **local-data-port** *local-port* **peer-data-port** *peer-port*

undo service-ip-port [**local-ip** *local-ip-address* **peer-ip** *peer-ip-address* **local-data-port** *local-port* **peer-data-port** *peer-port*]

Parameters

Parameter	Description	Value
local-ip *local-ip-address*	Specifies the local IP address of the HSB service.	The value is in dotted decimal notation.
peer-ip *peer-ip-address*	Specifies the peer IP address of the HSB service.	The value is in dotted decimal notation.
local-data-port *local-port*	Specifies the local port number of the HSB service.	The value is an integer that ranges from 10240 to 49152.
peer-data-port *peer-port*	Specifies the peer port number of the HSB service.	The value is an integer that ranges from 10240 to 49152.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you create an HSB service using the **hsb-service** command, run the **service-ip-port** command to configure IP addresses and port numbers for the local and peer devices. When the configuration is complete, the HSB service establishes a Transmission Control Protocol (TCP) channel to transmit packets of other services and notifies service modules of link status changes.

Prerequisites

An HSB service has been created.

Precautions

It is recommended that the HSB channel be configured on an independent and highly reliable physical link.

Example

Configure IPv4 addresses and port numbers for the local and peer devices for the HSB service 0.

```
<Huawei> system-view
[Huawei] hsb-service 0
[Huawei-hsb-service-0] service-ip-port local-ip 192.168.1.1 peer-ip 192.168.1.2 local-data-port 10240
peer-data-port 10240
```

 Copyright © Huawei Technologies Co., Ltd.

18.4.20 service-keep-alive detect

Function

The **service-keep-alive detect** command sets the number of retransmission times and interval of HSB packets.

The **undo service-keep-alive** command restores the default number of retransmission times and interval of HSB packets.

The default number of retransmission times is 5, and the default retransmission interval is 3 seconds.

Format

service-keep-alive detect retransmit *retransmit-times* **interval** *interval-value*

undo service-keep-alive [**detect retransmit** *retransmit-times* **interval** *interval-value*]

Parameters

Parameter	Description	Value
retransmit *retransmit-times*	Specifies the number of times HSB packets are retransmitted.	The value is an integer that ranges from 1 to 20.
interval *interval-value*	Specifies the retransmission interval of HSB packets.	The value is an integer that ranges from 1 to 10, in seconds.

Views

HSB service view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An HSB service sends and retransmits HSB packets to prevent long TCP interruption that is not detected by the protocol stack. If a device does not receive an HSB packet from the peer device within the period (value of *retransmit-times* x value of *interval-value*), the local device receives a message indicating the exception and then re-establishes a channel to the peer.

Prerequisites

An HSB service has been configured.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the number of retransmission times for HSB service 0 to 5, and the retransmission interval to 1 second.

```
<Huawei> system-view
[Huawei] hsb-service 0
[Huawei-hsb-service-0] service-keep-alive detect retransmit 5 interval 1
```

Related Topics

18.4.12 hsb-service

18.4.21 track vrrp

Function

The **track vrrp** command binds a VRRP group to an HSB group.

The **undo track vrrp** command unbinds a VRRP group from an HSB group.

By default, no HSB group is bound to a VRRP group.

Format

track vrrp vrid *virtual-router-id* **interface** *interface-type interface-number*

undo track vrrp [**vrid** *virtual-router-id* **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the ID of a VRRP group bound to an HSB group.	The value is an integer that ranges from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of the interface in a VRRP group. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

HSB group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **track vrrp** command to bind a VRRP group to an HSB group. The HSB group negotiates the service status based on the VRRP status. By monitoring the changes in the bound HSB channel status and VRRP status, the HSB group instructs service modules to perform batch backup, real-time backup, and status synchronization.

Prerequisites

An HSB group has been configured.

Example

Bind GE1/0/0 in VRRP group 4 to HSB group 0.

```
<Huawei> system-view
[Huawei] hsb-group 0
[Huawei-hsb-group-0] track vrrp vrid 4 interface gigabitethernet 1/0/0
```

Related Topics

18.4.11 hsb-group

18.6.37 vrrp vrid virtual-ip

18.5 BFD Configuration Commands

18.5.1 authentication-mode (BFD)

Function

The **authentication-mode** command configures BFD session authentication information.

The **undo authentication-mode** command deletes the configured BFD session authentication information.

By default, BFD session authentication information is not configured.

Format

authentication-mode met-sha1 key-id *key-id-value* **cipher** *cipher-text* **nego-packet** [**timeout-interval** *interval-value*]

undo authentication-mode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
met-sha1 key-id *key-id-value*	Specifies the authentication key ID of a BFD session.	The value is an integer ranging from 1 to 255.
cipher *ciphertext*	Specifies a ciphertext BFD authentication password. You can enter either a simple or ciphertext password, but the password is displayed in ciphertext in the configuration file.	The value is a string of characters. ● The value is a string of 1 to 20 characters for simple authentication passwords. ● The value is a string of 20 to 148 characters for ciphertext authentication passwords. **NOTE** The characters exclude question marks (?) and spaces. However, if a password string is between a pair of quotation marks, the string can contain spaces.
nego-packet	Authenticates BFD negotiation packets.	-
timeout-interval *interval-value*	Specifies the negotiation timeout period of a BFD session.	The value is an integer ranging from 1 to 10000, in seconds. This parameter has no default value. **NOTE** After a BFD negotiation timeout period is configured, the BFD negotiation timeout timer is started when the BFD session goes Down (the event is not triggered by a link fault detected). If the timer has expired but the BFD session is still Down, the link protocol of the associated interface goes Down.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network demanding higher security, run the **authentication-mode** command to configure BFD session authentication information to improve network security. In a specific access scenario, for example, when a multicast BFD

session is associated with the protocol status of an interface, you need to configure authentication information for the BFD session on the interface. BFD negotiation can succeed, the BFD-associated protocol status of the interface can be activated, and users can access the device through this interface only when the BFD session authentication information on both ends is consistent.

Prerequisites

BFD has been globally enabled using the **bfd** command in the system view.

A BFD session used to detect the physical link status has been created using the **bfd** *session-name* **bind peer-ip default-ip interface** *interface-type interface-number* [**source-ip** *source-ip*] command in the system view.

Precautions

If you run the **authentication-mode** command to configure BFD session authentication information, BFD renegotiation will be performed. BFD renegotiation can succeed only when the BFD session authentication information on both ends is consistent.

Adding, modifying, or deleting BFD session authentication information may interrupt the service associated with the BFD session.

Example

Configure multicast BFD session authentication information.

```
<Huawei> system-view
[Huawei] bfd test bind peer-ip default-ip interface GigabitEthernet0/0/1
[Huawei-bfd-session-test] authentication-mode met-sha1 key-id 5 cipher Huawei-123 nego-packet
timeout-interval 5
```

Related Topics

18.5.4 bfd bind peer-ip default-ip

18.5.2 bfd

Function

The **bfd** command enables the global Bidirectional Forwarding Detection (BFD) function and displays the BFD view.

The **undo bfd** command disables global BFD.

By default, global BFD is disabled.

Format

bfd

undo bfd

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect link faults, run the **bfd** command in the system view to enable global BFD.

Precautions

After the **undo bfd** command is executed, all the BFD functions are disabled. If a BFD session is configured, all the BFD sessions configuration will be deleted.

Example

Enable the global BFD function.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd]
```

18.5.3 bfd bind peer-ip

Function

The **bfd bind peer-ip** command creates a BFD session, specifies the peer IP address, and displays the BFD session view.

The **undo bfd** *session-name* command deletes a specified BFD session and cancels the peer IP address.

By default, BFD binding is not created.

Format

bfd *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] [**source-ip** *ip-address*]

undo bfd *session-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	-
vpn-instance *vpn-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. If no VPN instance is specified, the peer IP address is considered as the public network address. If this parameter is specified, the VPN instance must have been created by using the **ip vpn-instance** command.
interface *interface-type interface-number*	Specifies the type and number of the interface bound to the BFD session. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. ● During BFD session negotiation, if the source IP address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address is reachable. The IP address of this outbound interface is used as the source IP address of the BFD packets sent by the local end. ● When a BFD session is detecting links, if this parameter is not specified, the system uses a fixed source IP address in BFD packets. Generally, you do not need to set this parameter. When BFD is used with the Unicast Reverse Path Forwarding (URPF) function, you must manually configure the source IP address in BFD packets because the URPF function checks the source IP address in received packets. **NOTE** For details about URPF, see URPF Configuration in the *Huawei AR Series Access Routers Configuration Guide - Security Configuration*.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect and monitor links, create BFD sessions.

To create a BFD binding, pay attention to the following points:

- If only the peer IP address is specified, BFD is configured to detect the multi-hop link.
- If the peer IP address and local interface are specified, BFD is configured to detect the single-hop link, that is, a specific route with this interface as the outbound interface and with the peer IP address as the next-hop address.
- If both the peer IP address and the VPN instance are specified, BFD is configured to detect the multi-hop link in the VPN instance.
- The single-hop link in the VPN instance is detected if both the peer IP address, VPN instance, and local interface are specified.

Prerequisites

Global BFD has been enabled by using the **bfd** command in the system view.

Follow-up Procedure

- Run the **discriminator** command to set the local and remote discriminators for the current BFD session.

Precautions

- When creating a single-hop BFD session, bind the single-hop BFD session to the peer IP address and the local address. You only need to bind a multi-hop BFD session to the peer IP address.
- When the BFD configuration items are created, the system checks only the format of the IP address. The BFD session cannot be established if an incorrect peer IP address or source IP address is bound.

NOTE

After configuring a BFD session, run the **commit** command to commit the configuration. Otherwise, the configuration cannot take effect.

Example

Create a BFD session named **atoc** to detect the multi-hop link to the peer IP address 10.10.20.2.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd atoc bind peer-ip 10.10.20.2
```

18.5.4 bfd bind peer-ip default-ip

 Copyright © Huawei Technologies Co., Ltd.

Function

The **bfd bind peer-ip default-ip** command creates a BFD binding for detecting the physical status of a link.

The **undo bfd** *session-name* command deletes a specified BFD session and the created BFD binding.

By default, no BFD binding for monitoring physical status of a link is configured.

Format

bfd *session-name* **bind peer-ip default-ip interface** *interface-type interface-number* [**source-ip** *ip-address*]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the session name of BFD.	The value is a string of 1 to 15 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip default-ip	Indicates the default multicast IP address that is bound to a BFD session.	By default, BFD uses the multicast IP address 224.0.0.184. You can set the multicast IP address by running the **default-ip-address** command.
interface *interface-type interface-number*	Specifies the type and number of the interface bound to a BFD session. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. If the source IP address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address can be reached. The IP address of this outbound interface is used as the source IP address of BFD packets sent by the local end. Generally, this parameter is not required. When BFD is used with the Unicast Reverse Path Forwarding (URPF) function, you must manually configure the source IP address in BFD packets because the URPF function checks the source IP address in received packets. **NOTE** For details about URPF, see URPF Configuration in the *Huawei AR Series Access Routers Configuration Guide - Security Configuration*.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If **source-ip** is specified, the URPF-enabled device does not incorrectly discard BFD packets. Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

If the IP address of an outbound interface is changed after a BFD session is configured, the source IP address of BFD packets is not updated.

NOTE

After the **bfd bind peer-ip default-ip** command is executed, run the **commit** command to commit the configuration to make the configuration take effect.

Example

Configure a BFD session named **test** on GE 1/0/0.1 to which a default multicast address is bound, to detect the one-hop link on GE1/0/0.1.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ip default-ip interface gigabitethernet 1/0/0.1
[Huawei-bfd-session-test]
```

Related Topics

18.5.2 bfd

18.5.14 default-ip-address

18.5.5 bfd bind peer-ip source-ip auto

Function

The **bfd bind peer-ip source-ip auto** command creates a static BFD session with automatically negotiated discriminators.

The **undo bfd** *session-name* command deletes a specified BFD session.

By default, no static BFD session with automatically negotiated discriminators is established.

Format

bfd *session-name* **bind peer-ip** *ip-address* [**vpn-instance** *vpn-name*] [**interface** *interface-type interface-number*] **source-ip** *ip-address* **auto**

undo bfd *session-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
peer-ip *ip-address*	Specifies the peer IP address bound to the BFD session.	-
vpn-instance *vpn-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. If no VPN instance is specified, the peer IP address is considered as the public network address. If this parameter is specified, the VPN instance must have been created by using the **ip vpn-instance** command.
interface *interface-type interface-number*	Specifies the type and number of the interface bound to the BFD session. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-
source-ip *ip-address*	Indicates the source IP address carried in BFD packets, that is, IP address of the outbound interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
auto	Enables automatic negotiation of local and remote discriminators.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To fast detect and monitor links, when the peer device uses dynamic BFD and the local device wants to communicate with the peer device and detect static routes, run the **bfd bind peer-ip source-ip auto** command to create a BFD session with automatically negotiated discriminators.

When creating a static BFD session with automatically negotiated discriminators, pay attention to the following points:

- If only the peer IP address is specified, BFD is configured to detect the multi-hop link.
- If the peer IP address and local interface are specified, BFD is configured to detect the single-hop link, that is, a specific route with this interface as the outbound interface and with the peer IP address as the next-hop address.
- The source IP address prevents BFD packets from being discarded incorrectly when the URPF function is enabled. Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness.
- If both the peer IP address and the VPN instance are specified, BFD is configured to detect the multi-hop link in the VPN instance.
- If the peer IP address, VPN instance, and local interface are specified, BFD is configured to detect the single-hop link in the VPN instance.

Prerequisites

Global BFD has been enabled by using the **bfd** command in the system view.

Precautions

- When creating a BFD session, bind the BFD session to the peer IP address and the local address.
- When the BFD configuration items are created, the system checks only the format of the IP address. The BFD session cannot be established if an incorrect peer IP address or source IP address is bound.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a static BFD session with automatically negotiated discriminators.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd atob bind peer-ip 10.1.1.2 interface gigabitethernet 1/0/0 source-ip 10.1.1.1 auto
```

Related Topics

18.5.2 bfd

18.5.6 bfd bind peer-ipv6

Function

The **bfd bind peer-ipv6** command creates a BFD for IPv6 session to monitor an IPv6 link.

The **undo bfd** *session-name* command deletes the specified BFD for IPv6 session.

By default, no BFD for IPv6 session to monitor an IPv6 link is created.

Format

bfd *session-name* **bind peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] [**source-ipv6** *ipv6-address*]

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD for IPv6 session.	A string of 1 to 15 case-insensitive characters, spaces not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ipv6	Specifies the peer IPv6 address bound to the BFD for IPv6 session.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPNv6 instance bound to the BFD for IPv6 session. If no VPNv6 instance is specified, the peer IPv6 address is considered as a public network address.	The value must be an existing VPNv6 instance.
interface *interface-type interface-number*	Specifies the type and number of a local Layer 3 interface bound to the BFD for IPv6 session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD packets. This parameter usually does not need to be set, with the exception in the following situations: ● During negotiation on parameters of a BFD session for IPv6, the device searches for the IPv6 address of an outbound interface connected to the remote end in the local routing table as the source IPv6 address before the device sends BFD packets. ● During BFD for IPv6 detection, the device sets the source IPv6 address to a fixed value. **NOTE** BFD works with unicast reverse path forwarding (URPF). URPF checks the source IPv6 address in received packets, and therefore the source IPv6 address needs to be set manually for the BFD packets.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BFD session for IPv6 can be established to rapidly detect faults in IPv6 links.

When creating a BFD session for IPv6, configuring optional parameters to implement different functions:

- The BFD for IPv6 session monitors a multi-hop link if only the peer IPv6 address is specified.
- The BFD for IPv6 session monitors a single-hop link if both a peer IPv6 address and a local interface are specified. This means that the BFD for IPv6 session monitors a specific route in which the outbound interface is the local interface and the next-hop address is the peer IPv6 address.
- The BFD for IPv6 session monitors a multi-hop link of the VPN route if the peer IPv6 address and the VPN instance are specified.
- The BFD for IPv6 session monitors a single-hop link with the specific VPN route if both the IP addresses of the peer IPv6, the VPN instance, and the local interface are specified.

NOTE

If the source addresses of BFD packets are specified, and URPF is enabled, use the **source-ipv6** command parameter to prevent BFD packets from being incorrectly discarded. The source IPv6 address must be configured correctly because the system only checks the validity of the source IPv6 address format but not the correctness. The source IPv6 address cannot be a multicast or broadcast address.

Prerequisites

Before running the **bfd bind peer-ipv6** command, you must enable BFD globally. Run the **bfd** command in the system view.

- Run the **description** command to configure the description of a BFD for IPv6 session.
- Run the **min-tx-interval** command to set the desired interval at which BFD for IPv6 packets are sent.
- Run the **min-rx-interval** command to set the desired interval at which BFD for IPv6 packets are received.
- Run the **detect-multiplier** command to configure the local detection multiple of BFD for IPv6 packets.
- Run the **wtr** command to set the WTR time for the BFD for IPv6 session.

Precautions

- BFD for IPv6 sessions monitor bidirectional links. Therefore, the **bfd bind peer-ipv6** command must be configured on the two ends of the links.
- If the IPv6 address of the outbound interface is changed after a BFD for IPv6 session has been created, the following situations occur:
  - During negotiation, the source IPv6 address to be carried in BFD for IPv6 packets is updated.
  - During detection, the source IPv6 address carried in BFD for IPv6 packets is not updated.

Example

Create a BFD for IPv6 session named **test** to monitor a single-hop link.

```
<Huawei> system-view
[Huawei] bfd
```

```
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ipv6 2001:db8:1::1 interface gigabitethernet 1/0/0
[Huawei-bfd-session-test] discriminator local 1
[Huawei-bfd-session-test] discriminator remote 2
[Huawei-bfd-session-test] commit
```

Create a BFD for IPv6 session named **pos0** for detecting the multi-hop link with the peer IPv6 address **2001:db8:1::2**.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd pos0 bind peer-ipv6 2001:db8:1::2
[Huawei-bfd-session-pos0] discriminator local 3
[Huawei-bfd-session-pos0] discriminator remote 4
[Huawei-bfd-session-pos0] commit
```

18.5.7 bfd bind peer-ipv6 source-ipv6 auto

Function

The **bfd bind peer-ipv6 source-ipv6 auto** command creates a static BFD for IPv6 session with automatically negotiated discriminators.

The **undo bfd** *session-name* command deletes the specified BFD for IPv6 session.

By default, static BFD for IPv6 session with automatically negotiated discriminators is not created.

Format

bfd *session-name* **bind peer-ipv6** *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**interface** *interface-type interface-number*] **source-ipv6** *ipv6-address* **auto**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD for IPv6 session.	A string of 1 to 15 case-insensitive characters, spaces not supported. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.
peer-ipv6 *peer-ipv6*	Specifies the peer IPv6 address bound to the BFD for IPv6 session.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance bound to the BFD for IPv6 session. If no VPN instance is specified, the peer IPv6 address is considered as a public network address, which means that VrfIndex is 0.	The value must be an existing VPNv6 instance.
interface *interface-type interface-number*	Specifies the type and number of an outbound interface bound to the BFD for IPv6 session. ● *interface-type* specifies the type of the interface. ● *interface-number* specifies the number of the interface.	-
source-ipv6 *ipv6-address*	Specifies the source IPv6 address carried in BFD for IPv6 packets.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A BFD for IPv6 session can be established to rapidly detect faults in IPv6 links. A device needs to establish a BFD session with a remote device on which a dynamic BFD session is established to detect faults in static routes. In this case, the **bfd bind peer-ipv6 source-ipv6 auto** command is used to create a BFD for IPv6 session with automatically negotiated discriminators.

The parameters are optional in the **bfd bind peer-ipv6 source-ipv6 auto** command to provide various functions:

- The BFD for IPv6 session monitors a multi-hop link if only the peer IPv6 address is specified.
- The BFD for IPv6 session monitors a single-hop link if both the peer IPv6 address and the local interface are specified. This means that the BFD for IPv6 session monitors a specific route in which the outbound interface is the local interface and the next-hop address is the peer IPv6 address.
- The BFD for IPv6 session monitors a multi-hop link for VPN routes if both the peer IPv6 address and VPN instance name are specified.

 Copyright © Huawei Technologies Co., Ltd.

- The BFD for IPv6 session monitors a single-hop link for VPN routes if the peer IPv6 address, VPN instance name, and local interface are specified.

NOTE

If the source IPv6 address is configured, BFD packets will not be discarded incorrectly after URPF is enabled. The source IP address must be configured correctly because the system only checks the validity of the source IPv6 address format but not correctness. The source IPv6 address cannot be a multicast or broadcast address.

Prerequisites

BFD must be enabled globally using the **bfd** command in the system view before the **bfd bind peer-ipv6 source-ip auto** command is run.

Follow-up Procedure

After a static BFD session for IPv6 with automatically negotiated discriminators is created, perform the following optional operations in the BFD for IPv6 view:

- Run the **description** command to configure the description of a BFD for IPv6 session.
- Run the **min-tx-interval** command to set the desired minimum interval at which BFD for IPv6 packets are sent.
- Run the **min-rx-interval** command to set the desired minimum interval at which BFD for IPv6 packets are received.
- Run the **detect-multiplier** command to set the local detection multiplier of the BFD for IPv6 session.
- Run the **process-pst** command to enable the BFD for IPv6 session to modify the PST if the BFD session detects a fault.
- Run the **wtr** command to set the WTR time for the BFD for IPv6 session.

Precautions

The difference between a static BFD session and a static BFD for IPv6 session with automatically negotiated discriminators is as follows:

- The static BFD for IPv6 session requires the configuration of local and remote discriminators.
- The static BFD for IPv6 session with automatically-negotiated discriminators does require the local or remote discriminator.

If the IPv6 address of the outbound interface is changed after the BFD for IPv6 session has been configured, the IPv6 address carried in the BFD for IPv6 packets will not be changed.

The source address must be configured if BFD for IPv6 with automatic negotiation on a local discriminator configured.

Example

Create a BFD for IPv6 session named **test** with automatically negotiated discriminators to monitor a single-hop link.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd test bind peer-ipv6 2001:db8:1::1 interface gigabitethernet 1/0/0 source-ipv6
```

```
2001:db8:1::2 auto
[Huawei-bfd-session-test] commit
```

Create a BFD for IPv6 session named **pos0** with automatically negotiated discriminators to monitor a multi-hop link with the peer IPv6 address **2001:db8:1::2**.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd pos0 bind peer-ipv6 2001:db8:1::1 source-ipv6 2001:db8:1::2 auto
[Huawei-bfd-session-pos0] commit
```

Related Topics

18.5.2 bfd

18.5.17 detect-multiplier

18.5.27 min-rx-interval

18.5.28 min-tx-interval

18.5.8 bfd one-arm-echo

Function

The **bfd one-arm-echo** command configures the BFD echo function.

The **undo bfd** command deletes a specified BFD session and cancels the binding.

By default, the BFD echo function is not configured.

Format

bfd *session-name* **bind peer-ip** *peer-ip* [**vpn-instance** *vpn-instance-name*] **interface** *interface-type interface-number* [**source-ip** *ip-address*] **one-arm-echo**

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session supporting the BFD echo function.	The value is a string of 1 to 15 case-insensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
bind peer-ip *peer-ip*	Specifies the peer IP address bound to the BFD session.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a Virtual Private Network (VPN) instance that is bound to a BFD session.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. If no VPN instance is specified, the peer IP address is considered as the public network address. If this parameter is specified, the VPN instance must have been created by using the **ip vpn-instance** command.
interface *interface-type interface-number*	Specifies the type and number of the interface bound to a BFD session. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
source-ip *ip-address*	Indicates the source IP address carried in BFD packets. If the source IP address is not specified, the system searches the local routing table for an outbound interface from which the peer IP address can be reached. The IP address of this outbound interface is used as the source IP address of BFD packets sent by the local end. Generally, this parameter is not required.	-
one-arm-echo	Indicates a BFD session supporting the BFD echo function.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Among two directly connected devices, one device supports BFD, whereas the other device does not support BFD. To rapidly detect forwarding failures between the two devices, configure a BFD session supporting the BFD echo function on the BFD-supporting device. The BFD-supporting device sends an Echo Request packet to the remote device. The remote device sends the Echo Request packet back along the same path to detect the forwarding link connectivity.

When you configure a BFD session supporting the BFD echo function:

- If **source-ip** is specified, the URPF-enabled device does not incorrectly discard BFD packets. Ensure that the source IP address is correct. The system only checks whether the source IP address is valid (for example, it cannot be a multicast or broadcast address) without checking correctness.
- If a VPN instance is specified, BFD is configured to detect the one-hop link in the VPN instance.

Prerequisites

Global BFD has been enabled using the **bfd** command in the system view.

Precautions

The difference between a BFD session supporting the BFD echo function and a common BFD session is as follows:

- When configuring a BFD session supporting the BFD echo function, you can only specify **local** *discr-value* in the **discriminator** command.
- You can only run the **min-echo-rx-interval** command to change the interval for receiving BFD packets.

NOTE

- If the IP address of an outbound interface is changed after a BFD session is configured, the source IP address of BFD packets is not updated.
- The BFD echo function is only applicable to single-hop BFD sessions.
- After the **bfd one-arm-echo** command is executed, run the **commit** command to commit the configuration to make the configuration take effect.

Example

Configure a BFD session **test** supporting the BFD echo function.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
```

```
[Huawei] bfd test bind peer-ip 10.10.10.1 interface gigabitethernet 1/0/0 one-arm-echo
[Huawei-bfd-session-test] discriminator local 100
[Huawei-bfd-session-test] commit
```

Related Topics

18.5.2 bfd

18.5.9 bfd session-name

18.5.26 min-echo-rx-interval

18.5.9 bfd session-name

Function

The **bfd** command displays the view of a specified BFD session.

The **undo bfd** command deletes a specified BFD session.

Format

bfd *session-name*

undo bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the created BFD session, run the **bfd** *session-name* command to enter the specified BFD session view.

Prerequisites

A BFD session has been created by using either of the following commands:

- **bfd bind peer-ip**
- **bfd bind peer-ip default-ip**
- **bfd bind peer-ip source-ip auto**
- **bfd one-arm-echo**

Precautions

The **bfd** *session-name* command displays the BFD session view regardless of whether the BFD session status is Up.

Example

Enter the view of the BFD session **session**.

```
<Huawei> system-view
[Huawei] bfd session
[Huawei-bfd-session-session]
```

18.5.10 bfd session nonexistent-config-check

Function

The **bfd session nonexistent-config-check enable** command enables the device to check whether the associated BFD session is deleted.

The **undo bfd session nonexistent-config-check disable** command enables the device to check whether the associated BFD session is deleted.

The **bfd session nonexistent-config-check disable** command disables the device from checking whether the associated BFD session is deleted.

By default, the device is enabled to check whether the associated BFD session is deleted.

Format

bfd session nonexistent-config-check enable

undo bfd session nonexistent-config-check disable

bfd session nonexistent-config-check disable

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

After static BFD for IPv4 static routes and association between VRRP and BFD are configured, deleting the BFD session may cause the association function to become ineffective. You can run the **bfd session nonexistent-config-check enable** command to enable the device to check whether the associated BFD session is deleted. When the associated BFD session is being deleted, the system displays a message indicating that the BFD session cannot be deleted. This function prevents the associated BFD session from being deleted incorrectly.

Example

Disable the device from checking whether the associated BFD session is deleted.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] bfd session nonexistent-config-check disable
```

18.5.11 bfd-group

Function

The **bfd-group** command creates a BFD group and displays the BFD group view.

The **undo bfd-group** command deletes a BFD group.

By default, no BFD group is created.

Format

bfd-group *group-name*

undo bfd-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a BFD group.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If multiple BFD sessions need to be monitored, you can create a BFD group. Then the device only need to monitor the BFD group.

Example

Create a BFD group.

```
<Huawei> system-view
[Huawei] bfd-group group
[Huawei-bfd-group-group]
```

18.5.12 commit

Function

The **commit** command commits the BFD session configuration.

Format

commit

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To make the modification on a BFD session take effect, you must run the **commit** command.

Precautions

- To establish a BFD session, the interface bound to the BFD session must be Up and there is a reachable route to the peer IP address.
- If conditions for BFD session setup are not met, the system keeps the configuration entries of the BFD session. The BFD session, however, cannot be established when you use the **commit** command.
- The system periodically scans BFD configuration entries that are committed but not used to establish sessions. If conditions are met, a session is established.
- The number of BFD sessions that can be established in the system is limited. When the number of established BFD sessions reaches the upper limit and

you use the **commit** command to commit the configurations of a new BFD session, the system generates a log indicating that the BFD session cannot be established and sends traps.

- After running the **bfd bind peer-ip source-ip auto** command to create configurations for a static BFD session with automatically negotiated discriminators, you do not need to run the **commit** command to commit the configurations. BFD sessions can be automatically established, and relevant configurations are labeled with the commit tags. To modify session parameters such as **process-interface-status**, **min-rx-interval**, **min-tx-interval**, **detect-multiplier**, **tos-exp**, **wtr**, **description**, and **authentication-mode(BFD)**, you can directly run the corresponding commands without running the **commit** command, and the modification takes effect immediately. The **commit** command can still be used but does not take effect.

Example

Commit the BFD session configuration.

```
<Huawei> system-view
[Huawei] bfd test bind peer-ip 10.1.1.1 interface gigabitethernet 1/0/0
[Huawei-bfd-session-test] discriminator local 22
[Huawei-bfd-session-test] discriminator remote 33
[Huawei-bfd-session-test] commit
```

Related Topics

18.5.9 bfd session-name

18.5.13 dampening timer-interval

Function

The **dampening timer-interval** command configures BFD session flapping suppression timers.

The **undo dampening timer-interval** command restores the default configuration.

BFD session flapping suppression timers start by default.

The default initial, secondary, and maximum BFD session flapping suppression timer values are 2000 ms, 5000 ms, and 12000 ms, respectively.

Format

dampening timer-interval maximum *maximum-milliseconds* **initial** *initial-milliseconds* **secondary** *secondary-milliseconds*

undo dampening timer-interval [**maximum** *maximum-milliseconds* **initial** *initial-milliseconds* **secondary** *secondary-milliseconds*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
maximum *maximum-milliseconds*	Specifies a maximum BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 12000.
initial *initial-milliseconds*	Specifies an initial BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 2000.
secondary *secondary-milliseconds*	Specifies a secondary BFD session flapping suppression timer value.	The value is an integer ranging from 1 to 3600000, in milliseconds. The default value is 5000.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If BFD detects link Down, services are switched. A penalty mechanism is provided to delay BFD session negotiation and prevent frequent service switchovers, protecting link resources and reducing link resource consumption.

To configure BFD session flapping suppression timers, run the **dampening timer-interval** command.

Prerequisites

BFD has been globally enabled using the **bfd** command in the system view.

Configuration Impact

After the **dampening timer-interval** command is run:

1. When a BFD session flaps for the first time, the initial BFD session flapping suppression timer starts. If the BFD session flaps again before the initial BFD session flapping suppression timer expires, BFD session renegotiation is triggered after the initial BFD session flapping suppression timer expires.
2. After the initial BFD session flapping suppression timer ends, the secondary BFD session flapping suppression timer starts. If the BFD session flaps before the secondary BFD session flapping suppression timer expires, BFD session renegotiation is triggered after the secondary BFD session flapping suppression timer expires. After that, the timer value is *secondary-milliseconds* x $2^{(n-1)}$, where *n* is the number of times that the secondary BFD session flapping suppression timer starts.
3. After the timer value of *secondary-milliseconds* x $2^{(n-1)}$ is greater than or equal to the value specified by *maximum-milliseconds*, the BFD session uses

the value specified by *maximum-milliseconds* as a flapping delay three consecutive times. After that, the BFD session flapping delay is recalculated based on Step 1.

Precautions

The configured maximum BFD session flapping suppression timer value must be greater than the configured initial or secondary BFD session flapping suppression timer value. Otherwise, the configuration fails.

Do not configure both the **dampening timer-interval** and **wtr** commands. Otherwise, the BFD session recovery period becomes long.

Example

Set a maximum, initial, and secondary BFD session flapping suppression timer values to 20000 ms, 1000 ms, and 3000 ms, respectively.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] dampening timer-interval maximum 20000 initial 1000 secondary 3000
```

18.5.14 default-ip-address

Function

The **default-ip-address** command configures the default multicast IP address used by all BFD sessions.

The **undo default-ip-address** command restores the default multicast IP address.

By default, BFD uses the multicast IP address 224.0.0.184.

Format

default-ip-address *ip-address*

undo default-ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default multicast IP address.	The value ranges from 224.0.0.107 to 224.0.0.250.

Views

BFD view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When using BFD to detect the physical status of a link, you may not specify the peer IP address. In certain situations, the peer such as the member link of the Eth-Trunk is not assigned an IP address. In this case, you need to bind a BFD session to a multicast IP address and send BFD control packets to the multicast IP address.

You must change the default multicast IP address in the following situations:

- On the network, other protocols use the multicast IP address.
- If multiple BFD sessions exist on a path, for example, Layer 3 interfaces are connected through Layer 2 switching devices that support BFD, configure different default multicast IP addresses for the devices where different BFD sessions are established. In this manner, BFD packets can be correctly forwarded.

Prerequisites

BFD has been enabled globally using the **bfd** command in the system view.

Precautions

If a BFD session that is bound to the default multicast IP address is configured, you cannot change the default multicast IP address.

Example

Set the default multicast IP address to 224.0.0.150.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] default-ip-address 224.0.0.150
```

Related Topics

18.5.4 bfd bind peer-ip default-ip

18.5.15 delay-up

Function

The **delay-up** command sets a delay before a BFD session becomes Up.

The **undo delay-up** command cancels a delay before a BFD session becomes Up.

By default, a delay is not set before a BFD session becomes Up.

Format

delay-up *time*

undo delay-up

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time	Specifies the delay before a BFD session becomes Up.	The value is an integer ranging from 1 to 600, in seconds. The default value is 0, indicating that a BFD session immediately becomes Up.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Router restarts, services on the active link need to be switched to the standby link. After the Router restarts, services need to be switched back to the active link. In practice, some devices determine whether to switch traffic based on the BFD session status. Because the routing protocol becomes Up after the interface becomes Up, routes may be not found when services are switched back, causing traffic loss. Therefore, the interval between the time when the routing protocol becomes Up and the time when the interface becomes Up must be eliminated. To solve this problem, run the **delay-up** command.

Prerequisites

Global BFD has been enabled by using the **bfd** command in the system view.

Precautions

The **delay-up** command affects BFD sessions whose configurations are not committed. When a created BFD session becomes Down, the session becomes Up after the delay.

Example

Set the delay before a BFD session becomes Up to 120s.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] delay-up 120
```

Related Topics

18.5.2 bfd

 Copyright © Huawei Technologies Co., Ltd.

18.5.16 description (BFD session view)

Function

The **description** command configures the description of a BFD session.

The **undo description** command deletes the description of a BFD session.

By default, the description of a BFD session is empty.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a BFD session.	The value is a string of 1 to 51 case-sensitive characters with spaces.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, multiple BFD sessions need to be configured. To differentiate BFD sessions, run the **description** command to configure a description for a BFD session. A meaningful description is recommended.

Configuration Impact

It is difficult to identify a BFD session that is not configured or whose description is deleted.

Precautions

If you run the **description** command in the same BFD session view multiple times, only the latest configuration takes effect.

The **description** command takes effect only for statically configured BFD sessions but does not take effect for dynamic BFD sessions or BFD sessions with automatically negotiated discriminators.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the description of the BFD session named **atoc**.

```
<Huawei> system-view
[Huawei] bfd atoc
[Huawei-bfd-session-atoc] description RouterA_to_RouterC
```

18.5.17 detect-multiplier

Function

The **detect-multiplier** command sets the local detection multiplier.

The **undo detect-multiplier** command restores the default local detection multiplier.

By default, the local detection multiplier is 3.

Format

detect-multiplier *multiplier*

undo detect-multiplier

Parameters

Parameter	Description	Value
multiplier	Specifies the local detection multiplier of a BFD session.	The value is an integer that ranges from 3 to 50.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command

 Copyright © Huawei Technologies Co., Ltd.

- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

You can increase or reduce the local detection multiplier based on actual networking. On a stable link, there is no need to frequently detect the link status, so you can increase the local detection multiplier.

If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

Configuration Impact

- On an unstable link, if the local detection multiplier is small, the BFD session may flap. It is recommended that a larger local detection multiplier be used.
- When other protocols are associated with BFD, if a larger local detection multiplier is used, the BFD session takes a long period of time to detect faults on the link and traffic is switched to the backup link after the specified period. Packets may be lost during this period.

Precautions

Both ends of a BFD session can use different local detection multipliers.

Example

Set the local detection multiplier of the BFD session **atoc** to 10.

```
<Huawei> system-view
[Huawei] bfd atoc
[Huawei-bfd-session-atoc] detect-multiplier 10
```

Related Topics

18.5.27 min-rx-interval

18.5.28 min-tx-interval

18.5.18 discriminator

Function

The **discriminator** command sets local and remote discriminators for a static BFD session.

Format

discriminator { **local** *discr-value* | **remote** *discr-value* }

Parameters

Parameter	Description	Value
local *discr-value*	Specifies the local discriminator of a BFD session	The value is an integer that ranges from 1 to 8191.
remote *discr-value*	Specifies the remote discriminator of a BFD session	The value is an integer that ranges from 1 to 8191.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When creating a static BFD session, run the **discriminator** command to set local and remote discriminators. Otherwise, the static BFD session cannot be set up. The local and remote discriminators differentiate BFD sessions between two systems.

Precautions

- Only static BFD sessions require settings of local and remote discriminators.
- The local discriminator of the local system and the remote discriminator of the remote system must be the same. If the local discriminator of the local system and the remote discriminator of the remote system are different, a static BFD session cannot be set up.
- After the local and remote discriminators of a static BFD session are configured, the local and remote discriminators cannot be modified. To modify the local and remote discriminators of a static BFD session, delete the BFD session and reconfigure the local and remote discriminators.

Example

Set the local discriminator of a BFD session to 80 and the remote discriminator to 800.

```
<Huawei> system-view
[Huawei] bfd atoc
[Huawei-bfd-session-atoc] discriminator local 80
[Huawei-bfd-session-atoc] discriminator remote 800
```

Related Topics

18.5.9 bfd session-name

18.5.19 display bfd configuration

Function

The **display bfd configuration** command displays the BFD session configuration.

Format

display bfd configuration { { **all** | **static** } [**for-ip** | **for-lsp** | **for-pw** | **for-te**] | **passive-dynamic** [**peer-ip** *peer-ip* **remote-discriminator** *discriminator*] } [**verbose**]

display bfd configuration { **static** [**name** *session-name*] | **discriminator** *local-discr-value* | **dynamic** | **peer-ip** { *peer-ip* [**vpn-instance** *vpn-name*] | **default-ip** } | **static-auto** } [**verbose**]

display bfd configuration { **ldp-lsp peer-ip** *peer-ip* **nexthop** *nexthop* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* | **mpls-te interface tunnel** *interface-number* [**te-lsp**] | **pw interface** *interface-type interface-number* [**secondary**] } [**verbose**]

display bfd configuration peer-ipv6 *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**verbose**]

display bfd configuration { **all** | **static** } **for-ipv6** [**verbose**]

NOTE

On AR150&160&200, the following parameters cannot be specified: **for-lsp**, **for-pw**, **for-te**, **ldp-lsp**, **static-lsp**, **mpls-te**, **pw interface**.

Parameters

Parameter	Description	Value
all	Displays the configuration of all BFD sessions.	-
static	Displays the configuration of static BFD sessions.	-
for-ip	Displays the configuration of BFD sessions for detecting an IP link.	-
for-ipv6	Displays the configuration of a BFD6 session that monitors an IPv6 link.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
for-lsp	Displays the configuration of BFD sessions for detecting an LSP.	-
for-pw	Displays the configuration of BFD sessions for detecting a PW.	-
for-te	Displays the configuration of BFD sessions for detecting a TE tunnel.	-
peer-ip *peer-ip*	Specifies the peer IP address bound to the BFD session.	-
passive-dynamic	Displays the configuration of passive-dynamic BFD sessions.	-
remote-discriminator *discriminator*	Specifies the BFD local discriminator of the source that initiates a BFD session.	The value is an integer that ranges from 1 to 4294967295.
verbose	Displays detailed configuration of BFD sessions.	-
name *session-name*	Displays the configuration of a specified static BFD session. *session-name* specifies the name of the BFD session.	The value is a string of 1 to 15 characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
dynamic	Displays the configuration of dynamic BFD sessions.	-
discriminator *local-discr-value*	Displays the configuration of BFD sessions with a specified local discriminator.	The value is an integer that ranges from 1 to 16383.
default-ip	Display statistics about BFD sessions with the default multicast address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
peer-ipv6 *peer-ipv6*	Displays the configuration of a BFD6 session bound to a specified peer IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-name*	Displays the configuration of BFD sessions bound to a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
static-auto	Displays the configuration of static BFD sessions with automatically negotiated discriminators.	-
ldp-lsp	Displays the configuration of BFD sessions for detecting an LDP LSP.	-
nexthop *nexthop*	Specifies the next hop address.	Expressed in dotted decimal notation.
interface *interface-type interface-number*	Displays the configuration of BFD sessions on a specified interface.	-
static-lsp	Displays the configuration of BFD sessions for detecting a static LSP.	-
lsp-name	Specifies the name of a static LSP.	The value is a string of 1 to 19 case-sensitive characters.
mpls-te	Displays the configuration of BFD sessions for detecting an MPLS TE tunnel.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface tunnel *interface-number*	Displays the configuration of BFD sessions on a specified tunnel interface.	-
te-lsp	Displays the configuration of BFD sessions for detecting the primary LSP bound to a TE tunnel.	-
pw	Displays the configuration of BFD sessions for detecting a PW.	-
secondary	Displays the configuration of BFD sessions for detecting the secondary PW.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

When multiple BFD sessions exist, you can view information about certain BFD sessions by specifying the parameters such as the type, name, and peer IP address.

Precautions

If a static BFD session with automatically negotiated discriminators and a dynamic BFD session share the same configurations, you can view that the shared session configurations by BFD session type (static and dynamic).

Example

Display the configuration of all BFD sessions.

```
<Huawei> display bfd configuration all
--------------------------------------------------------------------------------
CFG Name        CFG Type       LocalDiscr MIndex    SessNum  Commit   AdminDown
--------------------------------------------------------------------------------
3               S_IP_IF        10         16384     0        True     False
4               S_IP_IF        61         16385     1        True     False
eth63           S_IP_IF        106        16386     1        True     False
```

```
eth63forip      S_IP_IF        1511        16387     1        True     False
g1/0/6          S_IP_IF        101         16388     1        True     False
g7/0/22         S_IP_IF        103         16389     1        True     False
dyn_8200        Dynamic        8200        16398     1        True     False
dyn_8201        Dynamic        8201        16399     1        True     False
--------------------------------------------------------------------------------
    Total Commit/Uncommit CFG Number : 8/0
```

Display configurations of the BFD6 session bound to the peer IPv6 address 2001:1001:1002:1003:1004:1005:1006:1007.

```
<Huawei> display bfd configuration peer-ipv6 2001:1001:1002:1003:1004:1005:1006:1007
--------------------------------------------------------------------------------
CFG Name        CFG Type       LocalDiscr MIndex    SessNum  Commit   AdminDown
--------------------------------------------------------------------------------
pp              S_IP_IF        14         4099      1        True     False
--------------------------------------------------------------------------------
    Total Commit/Uncommit CFG Number : 1/0
```

Table 18-12 Description of the **display bfd configuration** command output

Item	Specification
CFG Name	BFD session name.
CFG Type	BFD session setup type: ● S_IP_IF: indicates a single-hop BFD session that is established statically and bound to an interface. ● S_IP_PEER: indicates a multi-hop BFD session that is established statically. ● S_STA_LSP: indicates a BFD session that is established statically and used for detecting an LSP. ● S_LDP_LSP: indicates a BFD session that is established statically and used for detecting an LDP LSP. ● S_TE_LSP: indicates a BFD session that is statically established and used for detecting a TE LSP. ● S_TE_TNL: indicates a BFD session that is statically established and used for detecting a TE tunnel. ● S_PW: indicates a BFD session that is statically established and used for detecting a PW. ● Dynamic: indicates a BFD session that is dynamically established. ● Entire_Dynamic: indicates a BFD session that is entirely and dynamically established. ● S_AUTO_IF: indicates a static single-hop BFD session with automatically negotiated discriminators. ● S_AUTO_PEER: indicates a static multi-hop BFD session with automatically negotiated discriminators.
LocalDiscr	Local discriminator of the BFD session.
MIndex	Configuration entry index of a BFD session.

Item	Specification
SessNum	Number of BFD sessions in a configuration entry.
Commit	Flag of enabling a BFD session. After you run the **commit** command to commit configurations in the BFD session view, the flag is displayed as **True**. Otherwise, it is displayed as **False**.
AdminDown	Flag of the management status of a BFD session. After you run the **shutdown (BFD session view)** command to disable the local session in the BFD session view, the flag is displayed as **True**. Otherwise, it is displayed as **False**.
Total Commit/ Uncommit CFG Number	Total number of BFD sessions that are committed through the **commit** command in the BFD session view and total number of BFD sessions that are not committed.

Display detailed configuration of all BFD sessions.

```
<Huawei> display bfd configuration all verbose
-------------------------------------------------------------------------------
 BFD Session Configuration Name : 1
-------------------------------------------------------------------------------
 Local Discriminator    : -              Remote Discriminator   : -
 BFD Bind Type          : Peer IP Address
 Bind Session Type      : Static
 Bind Peer IP Address   : 10.10.10.1
 Bind Interface         : -
 Select Board           : -
 Track Interface        : -
 TOS-EXP                : 7              Local Detect Multi     : 3
 Min Tx Interval (ms)   : 1000           Min Rx Interval (ms)   : 1000
 WTR Interval (ms)      : -              Process PST            : Disable
 Proc Interface Status  : Disable
 Bind Application       : No Application Bind
 Session Description    : -
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
 BFD Session Configuration Name : atob
-------------------------------------------------------------------------------
 Local Discriminator    : 1              Remote Discriminator   : 2
 BFD Bind Type          : Interface(GigabitEthernet0/0/1)
 Bind Session Type      : Static
 Bind Peer IP Address   : 10.10.10.2
 Bind Interface         : GigabitEthernet0/0/1
 TOS-EXP                : 7              Local Detect Multi     : 3
 Min Tx Interval (ms)   : 50             Min Rx Interval (ms)   : 50
 WTR Interval (ms)      : -              Process PST            : Disable
 Proc Interface Status  : Disable
 Bind Application       : No Application Bind
 Session Description    : -
-------------------------------------------------------------------------------

   Total Commit/Uncommit CFG Number : 1/1
```

Display detailed configurations of the BFD6 session bound to the peer IPv6 address 2001:1001:1002:1003:1004:1005:1006:1007.

```
<Huawei> display bfd configuration peer-ipv6 2001:1001:1002:1003:1004:1005:1006:1007 verbose
--------------------------------------------------------------------------------
BFD Session Configuration Name : pp
--------------------------------------------------------------------------------
Local Discriminator    : 14              Remote Discriminator : 41
BFD Bind Type          : Interface(GigabitEthernet1/0/0)
Bind Session Type      : Static
Bind Peer IP Address   : 2001:1001:1002:1003:1004:1005:1006:1007
Bind Interface         : GigabitEthernet1/0/0
TOS-EXP                : 7               Local Detect Multi : 3
Min Tx Interval (ms)   : 100             Min Rx Interval (ms) : 100
WTR Interval (ms)      : -               Process PST : Disable
Proc Interface Status  : Disable
Bind Application       : No Application Bind
Session Description    : -
Session Create Status  :Success
--------------------------------------------------------------------------------
    Total Commit/Uncommit CFG Number : 1/0
```

Table 18-13 Description of the **display bfd configuration all verbose** command output

Item	Specification
BFD Session Configuration Name	BFD session name.
Local Discriminator	Local discriminator of a BFD session.
Remote Discriminator	Remote discriminator of a BFD session.
BFD Bind Type	BFD session binding type: ● Peer IP Address: indicates multi-hop BFD for an IP link. ● Interface: indicates single-hop BFD for an IP link. ● STATIC_LSP: indicates that a static LSP is detected. ● LDP_LSP: indicates that an LDP LSP is detected. ● TE_LSP: indicates that an LSP bound to a TE tunnel is detected. ● TE_TUNNEL: indicates that a TE tunnel is detected. ● PW: indicates that a PW is detected. ● Static_Auto: indicates the statically established BFD sessions with automatically negotiated discriminators.

 Copyright © Huawei Technologies Co., Ltd.

Item	Specification
Bind Session Type	Mode in which a BFD session is established: ● Static: indicates the BFD sessions that are established through the static configurations. ● Dynamic: indicates the BFD sessions that are triggered dynamically. ● Static_Auto: indicates the statically established BFD sessions with automatically negotiated discriminators.
Bind Peer IP Address	Peer IP address of a BFD session or multicast IP address bound to a BFD session.
Bind Interface	Local interface bound to a BFD session.
Select-board	Indicates the board for processing the BFD state machine, which can be a main control board or an interface board
Track Interface	Interface tracked by the BFD session
TOS-EXP	Priority of a BFD packet.
Local Detect Multi	Local detection multiplier.
Min Tx Interval (ms)	Minimum interval for sending BFD packets.
Min Rx Interval (ms)	Minimum interval for receiving BFD packets.
WTR Interval (ms)	WTR time.
Process PST	Flag for processing the Port Status Table (PST). If the **process-pst** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Proc interface status	Flag of association between the BFD session status and the interface status. If the **process-interface-status** command is configured, this field is displayed as Enable. If the **process-interface-status sub-if** command is configured, this field is displayed as **Enable(Sub-If)**. Otherwise, it is displayed as **Disable**.
Bind Application	Application bound to the BFD session.
Session Description	Description of the BFD session.
Total Commit/Uncommit CFG Number	Total number of BFD sessions that are committed through the **commit** command in the BFD session view and total number of BFD sessions that are not committed.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

18.5.2 bfd
18.5.3 bfd bind peer-ip
18.5.5 bfd bind peer-ip source-ip auto
18.5.16 description (BFD session view)
18.5.17 detect-multiplier
18.5.18 discriminator
18.5.27 min-rx-interval
18.5.28 min-tx-interval
18.5.34 shutdown (BFD session view)
18.5.37 tos-exp
18.5.40 wtr

18.5.20 display bfd interface

Function

The **display bfd interface** command displays information about a BFD-enabled interface.

Format

display bfd interface [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to the BFD session. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **display bfd interface** command displays information about a BFD-enabled interface, including the BFD session bound to the interface and the BFD session status.

Example

Display information about a BFD-enabled interface.

```
<Huawei> display bfd interface
-------------------------------------------------------------------------------
Interface Name                        MIndex    Sess-Count   BFD-State
-------------------------------------------------------------------------------
GigabitEthernet0/0/1                    64        1            up
-------------------------------------------------------------------------------
    Total Interface Number : 1
```

Table 18-14 Description of the display bfd interface command output

Item	Description
Interface Name	Name of the BFD-enabled interface.
MIndex	Index of the interface entry.
Sess-Count	Number of BFD sessions bound to the interface.
BFD-State	BFD status of an interface. The value can be up or down.

Related Topics

18.5.2 bfd

18.5.21 display bfd session

Function

The **display bfd session** command displays information about BFD sessions.

Format

display bfd session { { **all** | **static** } [**for-ip** | **for-lsp** | **for-pw** | **for-te**] | **passive-dynamic** [**peer-ip** *peer-ip* **remote-discriminator** *remote-discr-value*] }
[**verbose**]

display bfd session { **dynamic** | **discriminator** *discr-value* | **peer-ip** { **default-ip** | *peer-ip* [**vpn-instance** *vpn-instance-name*] } | **static-auto** } [**verbose**]

display bfd session { **ldp-lsp peer-ip** *peer-ip* **nexthop** *ip-address* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* | **mpls-te interface**

interface-type interface-number [**te-lsp**] | **pw interface** *interface-type interface-number* [**secondary**] } [**verbose**]

display bfd session peer-ipv6 *peer-ipv6* [**vpn-instance** *vpn-instance-name*] [**verbose**]

display bfd session { **all** | **static** } **for-ipv6** [**verbose**]

NOTE

On AR100&AR120&AR150&AR160&AR200, the following parameters cannot be specified: **for-lsp**, **for-pw**, **for-te**, **ldp-lsp**, **static-lsp**, **mpls-te**, **pw interface**.

Parameters

Parameter	Description	Value
all	Displays all configurations of BFD sessions.	-
static	Displays the configuration of a static BFD session.	-
for-ip	Displays the configuration of a BFD session that monitors an IP link.	-
for-ipv6	Displays the configuration of the BFD6 session that monitors an IPv6 link.	-
for-lsp	Displays the configuration of a BFD session that monitors an LSP.	-
for-pw	Displays the configuration of a BFD session that monitors a PW link.	-
for-te	Displays the configuration of a BFD session that monitors a TE tunnel.	-
nexthop *ip-address*	Specifies the next hop address.	Expressed in dotted decimal notation.
interface *interface-type interface-number*	Specifies the type and number of an outbound interface bound to a BFD session.	-
verbose	Displays detailed information about the BFD configuration.	-
dynamic	Displays information about all dynamic BFD sessions and the static BFD sessions with auto-negotiated discriminators.	-
passive-dynamic	Displays information about all passive-dynamic BFD sessions.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
discriminator *discr-value*	Displays information about a BFD session with a specified discriminator. You can specify a local discriminator only.	A decimal integer ranging from 1 to 16383.
remote-discriminator *remote-discr-value*	Displays information about a BFD session with a specified discriminator. You can specify a remote discriminator only.	A decimal integer ranging from 1 to 4294967295.
peer-ip *peer-ip*	Displays information about a BFD session bound to the peer with a specified IP address.	Expressed in dotted decimal notation.
default-ip	Display statistics about a BFD session with a default multicast address.	-
peer-ipv6 *peer-ipv6*	Displays the configuration of a BFD6 session bound to a specified peer IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
vpn-instance *vpn-instance-name*	Displays information about a BFD session bound to a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
static-auto	Displays information about a static BFD session with automatically negotiated discriminators.	-
ldp-lsp	Displays information about a BFD session that monitors an LDP LSP.	-
static-lsp	Displays information about a BFD session that monitors a static LSP.	-
lsp-name	Specifies the name of a static LSP.	The value is a string of 1 to 19 case-sensitive characters without spaces.
mpls-te	Displays information about a BFD session for detecting the MPLS TE.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
te-lsp	Displays information about a BFD session that monitors a primary TE LSP.	-
pw	Displays information about a BFD session that monitors a PW.	-
secondary	Displays information about a BFD session that monitors a secondary PW.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd session** command displays information about BFD sessions.

Prerequisites

BFD has been enabled globally.

Precautions

- When a BFD session changes from Down to Up, if the WTR time of the session is not 0, BFD sends a notification that the session becomes Up only after the WTR time expires.
- If a static BFD session with automatically negotiated discriminators and a dynamic BFD session are bound to the same peer IP address, the **display bfd session** command displays the same entry for the static BFD session or dynamic BFD session.

Example

Display the summary of all BFD sessions.

```
<Huawei> display bfd session all
-------------------------------------------------------------------------------
Local  Remote PeerIpAddr         State       Type             InterfaceName
-------------------------------------------------------------------------------
111    222    224.0.0.184        Up          S_IP_IF          GigabitEthernet1/0/0
-------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 1/0
```

Display brief information about a BFD6 session with the peer IPv6 address 2001:1001:1002:1003:1004:1005:1006:1007.

```
<Huawei> display bfd session peer-ipv6 2001:1001:1002:1003:1004:1005:1006:1007
-------------------------------------------------------------------------------
```

```
Local  Remote PeerIpAddr      State     Type      InterfaceName
--------------------------------------------------------------------------------
11     22     2001:1001:1002:1003:1004:1005:1006:1007
                                Up      S_IP_IF     GigabitEthernet1/0/0
--------------------------------------------------------------------------------
    Total UP/DOWN Session Number : 1/0
```

Table 18-15 Description of the **display bfd session all** command output

Item	Description
Local	Local discriminator of the BFD session. To set the local discriminator, run the **discriminator** command.
Remote	Remote discriminator of the BFD session. To set the remote discriminator, run the **discriminator** command.
PeerIpAddr	Peer IP address bound to the BFD session.
State	BFD session status: ● Up: indicates that the BFD session is in Up state. ● Down: indicates that the BFD session is in Down state. ● AdmDown: indicates that a BFD session is AdminDown when the **shutdown (BFD session view)** command is run. If **slot** is not specified, the BFD session status on the main control board is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Type	BFD session type: ● S_TE_LSP: indicates a BFD session that is established statically and bound to a TE LSP. ● S_TE_TNL: indicates a BFD session that is established statically and bound to a TE tunnel. ● S_IP_PEER: indicates a BFD session that is established statically and bound to an IP link. ● S_IP_IF: indicates a BFD session that is established statically and bound to an interface. ● S_LDP_LSP: indicates a BFD session that is established statically and bound to a dynamic LSP. ● S_PW(M): indicates a BFD session that is established statically and bound to the primary PW. ● S_PW(S): indicates a BFD session that is established statically and bound to the secondary PW. ● S_STA_LSP: indicates a BFD session that is established statically and bound to a static LSP. ● D_IP_PEER: indicates a BFD session that is created dynamically and bound to an IP link. ● D_IP_IF: indicates a BFD session that is established dynamically and bound to an interface. ● D_LDP_LSP: indicates a BFD session that is established dynamically and bound to a dynamic LSP. ● D_TE_LSP: indicates a BFD session that is established dynamically and bound to a TE LSP. ● D_PW(S): indicates a BFD session that is established dynamically and bound to the secondary PW. ● D_PW(M): indicates a BFD session that is established dynamically and bound to the primary PW. ● E_Dynamic: indicates a BFD session that is established entirely and dynamically. After you enable the function of dynamically establishing a BFD session on the destination of an LSP, this session type is created. ● S_AUTO_IF: indicates a static single-hop BFD session with automatically negotiated discriminators. ● S_AUTO_PEER: indicates a static multi-hop BFD session with automatically negotiated discriminators.
InterfaceName	Outbound interface bound to the BFD session. In multi-hop BFD, this field is displayed as - - because no interface is bound to a BFD session.
Total UP/ DOWN Session Number :	Number of BFD sessions in Up or Down state.

 Copyright © Huawei Technologies Co., Ltd.

Display detailed information about all BFD sessions.

```
<Huawei> display bfd session all verbose
-------------------------------------------------------------------------------
Session MIndex : 64        (One Hop) State : Up        Name : atob
-------------------------------------------------------------------------------
  Local Discriminator    : 1                Remote Discriminator   : 2
  Session Detect Mode    : Asynchronous Mode Without Echo Function
  BFD Bind Type          : Interface(GigabitEthernet1/0/0)
  Bind Session Type      : Static
  Bind Peer IP Address   : 10.1.1.2
  NextHop Ip Address     : 10.1.1.2
  Bind Interface         : GigabitEthernet1/0/0
  FSM Board Id           : 0                TOS-EXP               : 7
  Min Tx Interval (ms)   : 1000             Min Rx Interval (ms)   : 1000
  Actual Tx Interval (ms): 1000             Actual Rx Interval (ms): 1000
  Local Detect Multi     : 3                Detect Interval (ms)   : 3000
  Echo Passive           : Disable          Acl Number             : -
  Destination Port       : 3784             TTL                    : 255
  Proc Interface Status  : Disable          Process PST            : Disable
  WTR Interval (ms)      : -
  Active Multi           : 3                DSCP                   : -
  Last Local Diagnostic  : No Diagnostic
  Bind Application       : No Application Bind
  Session TX TmrID       : -                Session Detect TmrID   : -
  Session Init TmrID     : -                Session WTR TmrID      : -
  Session Echo Tx TmrID  : -
  PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
  Session Description    : -
-------------------------------------------------------------------------------

    Total UP/DOWN Session Number : 1/0
```

Display detailed configurations of the BFD6 session bound with the peer IPv6 address 2001:1001:1002:1003:1004:1005:1006:1007.

```
<Huawei> display bfd session peer-ipv6 2001:1001:1002:1003:1004:1005:1006:1007 verbose
-------------------------------------------------------------------------------
Session MIndex : 4103      (One Hop) State : Down      Name : kk
-------------------------------------------------------------------------------
Local Discriminator    : 11               Remote Discriminator : 22
Session Detect Mode    : Asynchronous Mode Without Echo Function
BFD Bind Type          : Interface(Vlanif110)
Bind Session Type      : Static
Bind Peer IP Address   : 2001:1001:1002:1003:1004:1005:1006:1007
NextHop Ip Address     : 2001:1001:1002:1003:1004:1005:1006:1007
Bind Interface         : Vlanif110
FSM Board Id           : 1                TOS-EXP               : 7
Min Tx Interval (ms)   : 100              Min Rx Interval (ms)   : 100
Actual Tx Interval (ms): -                Actual Rx Interval (ms): -
Local Detect Multi     : 3                Detect Interval (ms)   : -
Echo Passive           : Disable          Acl Number             : -
Destination Port       : 3784             TTL                    : 255
Proc Interface Status  : Disable          Process PST            : Disable
WTR Interval (ms)      : -
Last Local Diagnostic  : No Diagnostic
Bind Application       : No Application Bind
Session TX TmrID       : -                Session Detect TmrID   : -
Session Init TmrID     : -                Session WTR TmrID      : -
Session Echo Tx TmrID  : -
PDT Index              : FSM-0 | RCV-0 | IF-0 | TOKEN-0
Session Description    : -
-------------------------------------------------------------------------------

    Total UP/DOWN Session Number : 0/1
```

Table 18-16 Description of the **display bfd session all verbose** command output

Item	Specification
Session MIndex	Index of session entries.
State	BFD session status: ● Up: indicates that the BFD session is in Up state. ● Down: indicates that the BFD session is in Down state. ● AdminDown: indicates that a BFD session is AdminDown when the **shutdown(BFD session view)** command is run.
Name	Name of a BFD session.
Local Discriminator	Local discriminator of the BFD session.
Remote Discriminator	Remote discriminator of the BFD session.
Session Detect Mode	BFD detection modes: ● Asynchronous Mode Without Echo Function: indicates the asynchronous mode without the echo function. ● Demand Mode Without Echo Function: indicates the demand mode without the echo function.
BFD Bind Type	BFD session binding type: ● Peer IP Address: indicates that a multi-hop IP link is detected. ● When one-hop BFD is used to detect an IP link, this field is displayed as Interface and the name of the bound local interface. ● Static_Auto: indicates the BFD session with automatically negotiated discriminators.
Bind Session Type	Mode in which a BFD session is established: ● Static: indicates that a BFD session is established manually. ● Dynamic: indicates that a BFD session is established dynamically. ● Static_Auto: indicates that a BFD session is established with automatically negotiated discriminators.
Bind Peer IP Address	Peer IP address bound to the BFD session.
NextHop Ip Address	Nexthop IP address bound to the BFD session.
Bind Interface	Outbound interface bound to the BFD session.

 Copyright © Huawei Technologies Co., Ltd.

Item	Specification
FSM Board Id	Number of the processing board where the state machine works.
TOS-EXP	Priority of a BFD packet.
Min Tx Interval(ms)	Configured minimum interval for sending BFD packets.
Min Rx Interval(ms)	Configured minimum interval for receiving BFD packets.
Actual Tx Interval(ms)	Actual minimum interval for sending BFD packets.
Actual Rx Interval(ms)	Actual minimum interval for receiving BFD packets.
Local Detect Multi	Local detection multiplier.
Detect Interval(ms)	BFD detection time.
Echo Passive	Echo function: ● Disable ● Enable
Acl Number	ACL rule.
Destination Port	Number of the destination port of a BFD control packet. The single-hop BFD control packet uses destination port 3784 and the multi-hop BFD control packet uses destination port 3784 or 4784.
TTL	TTL value of BFD packets.
Proc Interface Status	Flag of association between the BFD session status and the interface status. This field is displayed as **Disable**. Flag of association between the BFD session status and the interface status. If the **process-interface-status** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
WTR Interval (ms)	WTR time of the BFD session.
Process PST	Flag for processing the Port Status Table (PST). If the **process-pst** command is configured, this field is displayed as **Enable**. Otherwise, it is displayed as **Disable**.
Active Multi	Detection multiplier that is effective.
DSCP	DSCP value in the BFD session. The value ranges from 1 to 63. The value - indicates that the DSCP value does not take effect in the BFD session.

 Copyright © Huawei Technologies Co., Ltd.

Item	Specification
Last Local Diagnostic	Cause for the last BFD session in Down state: ● Control Detection Time Expired ● No Diagnostic ● Neighbor Signaled Session Down
Bind Application	Application bound to the BFD session. ● If a BFD session is not bound to an application, this field is displayed as "No Application Bind." ● If a BFD session is bound to an application, this field is displayed as the detailed application. For example, if a BFD session is associated with OSPF, this field is displayed as OSPF.
Session TX TmrID	Timer used for a BFD session to send packets.
Session Detect TmrID	BFD session detection timer.
Session Init TmrID	Timer for state machine initialization of a BFD session.
Session WTR TmrID	WTR timer of a BFD session.
Session Echo Tx TmrID	Timer used for a BFD session to send Echo packets.
PDT Index	Product information.
Session Description	Description of the BFD session.
Total UP/DOWN Session Number	Number of BFD sessions in Up or Down state.

Related Topics

18.5.2 bfd
18.5.3 bfd bind peer-ip
18.5.5 bfd bind peer-ip source-ip auto
18.5.16 description (BFD session view)
18.5.17 detect-multiplier
18.5.18 discriminator
18.5.27 min-rx-interval
18.5.28 min-tx-interval
18.5.34 shutdown (BFD session view)
18.5.37 tos-exp
18.5.40 wtr

 Copyright © Huawei Technologies Co., Ltd.

18.5.22 display bfd statistics

Function

The **display bfd statistics** command displays global BFD statistics.

Format

display bfd statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd statistics** command displays global BFD statistics.

Precautions

Before using the **display bfd statistics** command to view BFD statistics within a specified period, run the **reset bfd statistics** command to clear existing statistics.

Example

Display global BFD statistics.

```
<Huawei> display bfd statistics
Current Display Board Number : Main ; Current Product Register Type:AR
IP Multihop Destination Port : 3784
Total Up/Down Session Number : 1/0
Current Session Number :
    Static session     : 1              Dynamic session        : 0
    E_Dynamic session  : 0              STATIC_AUTO session    : 0
    LDP_LSP session    : 0              STATIC_LSP session     : 0
    TE_TUNNEL session  : 0              TE_LSP session         : 0
    PW session         : 0              IP session             : 1
    LDP_TUNNEL session : 0              BGP_TUNNEL session     : 0
-------------------------------------------------------------------------------
PAF/LCS Name                    Maxnum        Minnum        Create
-------------------------------------------------------------------------------
BFD_CFG_NUM                      32            1             2
BFD_IF_NUM                       32            1             1
BFD_SESSION_NUM                  32            1             1
BFD_IO_SESSION_NUM               32            1             0
BFD_PER_TUNNEL_CFG_NUM           16            1             0
-------------------------------------------------------------------------------
IO Board Current Created Session Statistics Information :(slot/number)
-------------------------------------------------------------------------------
```

```
          0/1          1/0          2/0          3/0
          4/0          5/0          6/0          7/0
          8/0          9/0         10/0         11/0
         12/0         13/0          14/0          15/0
         16/0
-------------------------------------------------------------------------------
Current Total Used Discriminator Num              : 1
-------------------------------------------------------------------------------
IO Board Reserved Sessions Number Information :(slot/number)
-------------------------------------------------------------------------------
          0/0          1/0          2/0          3/0
          4/0          5/0          6/0          7/0
          8/0          9/0         10/0         11/0
         12/0         13/0          14/0          15/0
         16/0
-------------------------------------------------------------------------------
BFD HA Information :
-------------------------------------------------------------------------------
Core Current HA Status                        : Slave Not Ready
Shell Current HA Status                       : Slave Not Ready
-------------------------------------------------------------------------------
BFD for LSP Information :
-------------------------------------------------------------------------------
Ability of auto creating BFD session on egress     : Disable
Period of LSP Ping                            : 60
System Session Delay Up Timer                 : OFF
-------------------------------------------------------------------------------
```

Table 18-17 Description of the display bfd statistics command output

Item	Description
Current Display Board Number	Number of the board where information is displayed. "Main" indicates the MPU.
Current Product Register Type	Type of the current product.
IP Multihop Destination Port	UDP port number.
Total Up/Down Session Number	Total number of BFD sessions in Up or Down state.
Current Session Number	Number of current BFD sessions.
Static session	Number of static BFD sessions.
Dynamic session	Number of dynamic BFD sessions.
E_Dynamic session	Number of entirely dynamic sessions.
STATIC_AUTO session	Number of BFD sessions with automatically negotiated discriminators.
LDP_LSP session	Number of BFD sessions for detecting an LDP LSP.
STATIC_LSP session	Number of BFD sessions for detecting a static LSP.
TE_TUNNEL session	Number of BFD sessions for detecting a TE tunnel.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TE_LSP session	Number of BFD sessions for detecting a TE LSP.
PW session	Number of BFD sessions for detecting a PW.
IP session	Number of BFD sessions for detecting an IP address.
LDP_TUNNEL session	Number of current BFD sessions for LDP tunnel
BGP_TUNNEL session	Number of current BFD sessions for BGP tunnel
PAF/LCS Name	Project name of the license file.
BFD_CFG_NUM	Maximum number of BFD sessions that can be globally configured.
BFD_IF_NUM	Maximum number of BFD sessions that can be bound to an interface.
BFD_SESSION_NUM	Maximum number of BFD sessions that can be globally established.
BFD_IO_SESSION_NUM	Maximum number of BFD sessions that can be established globally.
BFD_PER_TUNNEL_CFG_NUM	Maximum number of BFD sessions that can be configured on a tunnel.
IO Board Current Created Session Statistics Information :	Number of BFD sessions that are established on a board.
Current Total Used Discriminator Num	Total number of currently configured discriminators.
IO Board Reserved Sessions Number Information : (slot/number)	Number of reserved boards that are bound to a BFD session.
BFD HA Information	-
Core Current HA Status	HA status in the core: ● Normal: indicates that the HA status is normal. ● Batch Backup Going: indicates that backup is being performed. ● Slave Not Ready: indicates that the slave board is not ready. ● Smooth Going: indicates that smooth processing is being performed.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Shell Current HA Status	HA status in the shell: • Normal: indicates that the HA status is normal. • Batch Backup Going: indicates that backup is being performed. • Slave Not Ready: indicates that the slave board is not ready. • Smooth Going: indicates that smooth processing is being performed.
Ability of auto creating BFD session on egress	Whether the capability to establish an entirely dynamic BFD session is enabled.
Period of LSP Ping	Interval for sending LSP ping packets of dynamic BFD sessions for detecting an LSP/PW.
System Session Delay Up Timer	Status of the delay Up timer: • OFF: indicates that the system works properly. • Xs: indicates that the system recovers after X seconds and a BFD session can be Up.

Related Topics

18.5.2 bfd
18.5.3 bfd bind peer-ip
18.5.5 bfd bind peer-ip source-ip auto
18.5.15 delay-up
18.5.18 discriminator

18.5.23 display bfd statistics session

Function

The **display bfd statistics session** command displays BFD session statistics.

Format

display bfd statistics session { **all** | **static** } [**for-ip** | **for-lsp** | **for-pw** | **for-te**]

display bfd statistics session { **dynamic** | **discriminator** *discr-value* | **peer-ip default-ip** | **peer-ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **static-auto** }

display bfd statistics session { **ldp-lsp peer-ip** *ip-address* **nexthop** *nexthop-address* [**interface** *interface-type interface-number*] | **static-lsp** *lsp-name* | **mpls-te interface** *interface-type interface-number* [**te-lsp**]] | **pw interface** *interface-type interface-number* [**secondary**] }

 Copyright © Huawei Technologies Co., Ltd.

display bfd statistics session peer-ipv6 *peer-ipv6* [**vpn-instance** *vpn-instance-name*]

display bfd statistics session { **all** | **static** } **for-ipv6**

NOTE

On AR150&AR160&AR200, the following parameters cannot be specified: **for-lsp**, **for-pw**, **for-te**, **ldp-lsp**, **static-lsp**, **mpls-te**, **pw interface**.

Parameters

Parameter	Description	Value
all	Displays statistics on all BFD sessions.	-
static	Displays statistics on all static BFD sessions.	-
dynamic	Displays statistics on all dynamic BFD sessions.	-
discriminator *discr-value*	Displays statistics on a BFD session with a specified local discriminator.	The value is an integer that ranges from 1 to 16383.
peer-ip *default-ip*	Display statistics about BFD sessions with the default multicast address.	-
peer-ip *ip-address*	Displays statistics on BFD sessions bound to a specified IP address.	-
peer-ipv6 *peer-ipv6*	Displays statistics about a BFD6 session bound to a specified peer IPv6 address.	-
static-auto	Displays the configuration of static BFD sessions with automatically negotiated discriminators.	-
vpn-instance *vpn-instance-name*	Displays statistics on BFD sessions bound to a specified VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
for-ip	Displays statistics on BFD sessions for detecting IP links.	-
for-ipv6	Displays statistics about a BFD6 session that monitors an IPv6 link.	-
for-pw	Displays statistics on BFD sessions for detecting a PW.	-
for-lsp	Displays statistics on BFD sessions for detecting an LSP.	-
for-te	Displays statistics on BFD sessions for detecting a TE tunnel.	-
ldp-lsp	Displays statistics on BFD sessions for detecting an LDP LSP.	-
nexthop *nexthop-address*	Specifies the next hop address.	Expressed in dotted decimal notation
interface-type interface-number	Specifies the type and number of the interface bound to a BFD session. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
static-lsp	Displays statistics on BFD sessions for detecting a static LSP.	-
lsp-name	Specifies the name of a static LSP.	The value is a string of 1 to 19 case-sensitive characters without spaces.
mpls-te	Displays statistics on BFD sessions for detecting an MPLS TE tunnel.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
te-lsp	Displays statistics on BFD sessions for detecting the primary LSP bound to a TE tunnel.	-
pw	Displays statistics on BFD sessions for detecting a PW.	-
secondary	Displays statistics on BFD sessions for detecting the secondary PW.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd statistics session** command displays BFD session statistics.

Precautions

- If static BFD with automatically negotiated discriminators and dynamic BFD share a session, you can specify **all**, **static-auto**, or **dynamic** for query.
- Before using the **display bfd statistics session** command to view BFD session statistics, run the **reset bfd statistics** command to clear existing statistics.

Example

Display statistics on all BFD sessions.

```
<Huawei> display bfd statistics session all
-------------------------------------------------------------------------------
Session MIndex : 64        (One Hop) State : Up       Name : atob
-------------------------------------------------------------------------------
  Session Type                        : Static
  Bind Type                           : IP
  Local/Remote Discriminator          : 10/20
  Received Packets                    : 0
  Send Packets                        : 7
  Received Bad Packets                : 0
  Send Bad Packets                    : 2217
  Down Count                          : 1
  ShortBreak Count                    : 0
  Send Lsp Ping Count                 : 0
```

```
Dynamic Session Delete Count        : 0
Create Time                         : 2011/12/08 10:34:08
Last Down Time                      : 2011/12/08 10:38:16
Total Time From Last DOWN           : ---D:--H:--M:--S
Last Up Time                        : 2011/12/08 10:35:01
Last Up Lasting Time                : 000D:00H:03M:15S
Total Time From Create              : 000D:07H:28M:51S
-------------------------------------------------------------------------------
    Total Session Number : 1
```

Table 18-18 Description of the **display bfd statistics session all** command output

Item	Description
Session MIndex	Index of session entries.
State	Status of a session.
Name	Name of a BFD session
Session Type	Mode in which a BFD session is established: ● Static: indicates that a BFD session is established statically. ● Dynamic: indicates that a BFD session is established dynamically. ● Static_Auto: indicates that a BFD session is established with automatically negotiated discriminators. ● Entire_Dynamic: indicates the BFD sessions that are triggered entirely dynamically. After dynamic BFD session setup is enabled on the sink point of an LSP, a BFD session of this type is created.
Bind Type	BFD session binding type.
Local/Remote Discriminator	Local or remote discriminator of a BFD session.
Received Packets	Number of BFD packets received at the local end. This field can be deleted using the **reset bfd statistics** command.
Send Packets	Number of BFD packets sent by the local end. This field can be deleted using the **reset bfd statistics** command.
Received Bad Packets	Number of received error packets.
Send Bad Packets	Number of sent error packets.
Down Count	Number of times that a BFD session became Down.
ShortBreak Count	Number of times that a BFD session was transiently disconnected.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Send Lsp Ping Count	Number of LSP ping packets sent by the local end.
Dynamic Session Delete Count	Number of dynamic BFD sessions deleted.
Create Time	Time when a BFD session was created.
Last Down Time	Last time when a BFD session became Down.
Total Time From Last DOWN	Period from last time when a BFD session became Down to the current time.
Last Up Time	Last time the BFD session becomes Up.
Last Up Lasting Time	Period from the last time when a BFD session is Up to the current time.
Total Session Number	Number of BFD sessions.

Related Topics

18.5.2 bfd
18.5.3 bfd bind peer-ip
18.5.5 bfd bind peer-ip source-ip auto
18.5.9 bfd session-name
18.5.33 reset bfd statistics

18.5.24 display bfd ttl

Function

The **display bfd ttl** command displays the globally configured TTL.

Format

display bfd ttl

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display bfd ttl** command displays the globally configured TTL.

Example

Display information about all globally configured TTLs.

```
<Huawei> display bfd ttl
-------------------------------------------------------------------------------
Peer IP                          Mask       Type         Value
-------------------------------------------------------------------------------
10.10.10.0                        24        single-hop   255
```

Table 18-19 Description of the display bfd ttl command output

Item	Specification
Peer IP	IP segment address.
Mask	Mask length.
Type	Type of the BFD session. The value can be single-hop or multi-hop.
Value	Initial value of the global TTL value.

Related Topics

18.5.2 bfd

18.5.30 peer-ip ttl

18.5.25 display snmp-agent trap feature-name bfd all

Function

The **display snmp-agent trap feature-name bfd all** command displays the status of all traps on the BFD module.

Format

display snmp-agent trap feature-name bfd all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The Simple Network Management Protocol (SNMP) is a network management standard widely used on the TCP/IP network. It uses a central computer (a network management station) that runs network management software to manage network elements. The SNMP agent reports trap messages to the network management station so that the network management station can obtain the network status in a timely manner, and the network administrator can take measures accordingly.

The **display snmp-agent trap feature-name bfd all** command displays the following information:

- Trap names supported by the BFD module. The trap names are the same as the trap names specified by the **snmp-agent trap enable feature-name bfd trap-name** { **hwbfdsessdown** | **hwbfdsessreachlimit** | **hwbfdsessreachlimitbindif** | **hwbfdsessup** } command. Each trap name corresponds to a network element abnormality.
- Trap status of the BFD module. You can check whether the trap is reported based on the trap name.

Prerequisites

SNMP has been enabled. See **snmp-agent**.

Example

Display all the traps of the BFD module.

```
<Huawei>display snmp-agent trap feature-name bfd all
-----------------------------------------------------------------------------
Feature name: BFD
Trap number : 4
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwBfdSessUp                    off                     off
hwBfdSessDown                    off                     off
hwBfdSessReachLimit              off                     off
hwBfdSessReachLimitBindIf        off                     off
```

Table 18-20 Description of the display snmp-agent trap feature-name bfd all command output

Item	Specification
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.

Item	Specification
Trap name	Trap name. Traps of the BFD module include: ● hwBfdSessUp: A Huawei proprietary trap is sent when the BFD session becomes Up. ● hwBfdSessDown: A Huawei proprietary trap is sent when the BFD session becomes Down. ● hwBfdSessReachLimit: A Huawei proprietary trap is sent when the number of established BFD sessions on the device reaches the upper limit. ● hwBfdSessReachLimitBindIf: A Huawei proprietary trap is sent when the number of established BFD sessions on the board reaches the upper limit.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled by default. ● off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Related Topics

18.5.36 snmp-agent trap enable feature-name bfd

18.5.26 min-echo-rx-interval

Function

The **min-echo-rx-interval** command configures the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.

The **undo min-echo-rx-interval** command restores the default minimum interval.

By default, the minimum interval is 1000 ms.

Format

min-echo-rx-interval *interval*

undo min-echo-rx-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.	The value is an integer that ranges from 10 to 2000, in milliseconds.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a BFD session supporting the BFD echo function, you can set the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function.

Prerequisites

A BFD session supporting the echo function has been configured using the **bfd one-arm-echo** command.

Example

Set the minimum interval for receiving BFD packets of a BFD session supporting the BFD echo function to 100 ms.

```
<Huawei> system-view
[Huawei] bfd test
[Huawei-bfd-session-test] min-echo-rx-interval 100
```

Related Topics

18.5.2 bfd

18.5.9 bfd session-name

18.5.8 bfd one-arm-echo

18.5.27 min-rx-interval

Function

The **min-rx-interval** command sets the minimum interval for receiving BFD packets.

 Copyright © Huawei Technologies Co., Ltd.

The **undo min-rx-interval** command restores the default minimum interval for receiving BFD packets.

By default, the minimum interval for receiving BFD packets is 1000 ms.

Format

min-rx-interval *interval*

undo min-rx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for receiving BFD packets.	The value is an integer that ranges from 10 to 2000, in milliseconds.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

Precaution

- You can increase or reduce the minimum interval for receiving BFD packets based on actual networking. The minimum interval for receiving BFD packets determines the detection time of a BFD session. On an unstable link, if the minimum interval for receiving BFD packets is small, the BFD session may flap. You can increase the minimum interval for receiving BFD packets. The default value is recommended. Do not randomly change the minimum interval for receiving BFD packets.

 Copyright © Huawei Technologies Co., Ltd.

- If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

Example

Set the minimum interval for receiving BFD packets to 500 ms.

```
<Huawei> system-view
[Huawei] bfd session
[Huawei-bfd-session-session] min-rx-interval 500
```

Related Topics

18.5.17 detect-multiplier

18.5.28 min-tx-interval

18.5.28 min-tx-interval

Function

The **min-tx-interval** command sets the minimum interval for sending BFD packets.

The **undo min-tx-interval** command restores the default minimum interval for sending BFD packets.

By default, the minimum interval for sending BFD packets is 1000 ms.

Format

min-tx-interval *interval*

undo min-tx-interval

Parameters

Parameter	Description	Value
interval	Specifies the minimum interval for sending BFD packets.	The value is an integer that ranges from 10 to 2000, in milliseconds.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The local detection multiplier determines the detection time of a BFD session.

Detection time = Received Detect Multi of the remote system x Max (Local RMRI/ Received DMTI)

where

- Detect Multi: local detection multiplier, which is set by using the **detect-multiplier** command
- Required Min Rx Interval (RMRI): minimum interval for receiving BFD packets, which is set by using the **min-rx-interval** command
- Desired Min Tx Interval (DMTI): minimum interval for sending BFD packets, which is set by using the **min-tx-interval** command

Precaution

- You can increase or reduce the minimum interval for sending BFD packets based on actual networking. The minimum interval for sending BFD packets determines the detection time of a BFD session. On an unstable link, if the minimum interval for sending BFD packets is small, the BFD session may flap. You can increase the minimum interval for sending BFD packets. The default value is recommended. Do not randomly change the minimum interval for sending BFD packets.
- If no BFD packet is received from the peer device within the detection time, the link is considered as faulty and the BFD session enters the Down state. To reduce the usage of system resources, when the BFD session is detected in Down state, the system adjusts the sending interval to a random value greater than 1000 ms. When the BFD session becomes Up, the configured interval is restored.

Example

Set the minimum interval for sending BFD packets to 500 ms.

```
<Huawei> system-view
[Huawei] bfd session
[Huawei-bfd-session-session] min-tx-interval 500
```

Related Topics

18.5.17 detect-multiplier

18.5.27 min-rx-interval

18.5.29 multi-hop destination-port

Function

The **multi-hop destination-port** command configures the destination port number for a multi-hop BFD session.

The **undo multi-hop destination-port** command restores the default destination port number for a multi-hop BFD session.

 Copyright © Huawei Technologies Co., Ltd.

By default, destination port 3784 is used in multi-hop BFD control packets.

Format

multi-hop destination-port { **3784** | **4784** }

undo multi-hop destination-port

Parameters

Parameter	Description	Value
3784	Indicates that destination port 3784 is used in multi-hop BFD control packets.	-
4784	Indicates that destination port 4784 is used in multi-hop BFD control packets.	-

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As defined in the BFD draft, destination port 4784 is used by multi-hop BFD control packets. When the device running the latest version interworks with devices running earlier versions, destination port 3784 is used by multi-hop BFD control packets. When the device interworks with non-Huawei devices, destination port 4784 is used by multi-hop BFD control packets.

Precautions

- If destination port 4784 is used by multi-hop BFD control packets, the device fails to negotiate with the remote device on which destination port 3784 is used by multi-hop BFD control packets.
- If destination port 3784 is used by multi-hop BFD control packets, the device can successfully negotiate with the remote device on which destination port 4784 is used by multi-hop BFD control packets. On the device that is configured with destination port 3784, destination port 3784 is automatically updated to destination port 4784.
- If destination port 3784 is used by both multi-hop and single-hop BFD control packets, the single-hop and multi-hop BFD control packets are processed according to their TTLs.

 Copyright © Huawei Technologies Co., Ltd.

- When a large number of multi-hop BFD sessions are set up, updating the destination ports may take a long time. Therefore, when a smaller interval for configuring multi-hop BFD sessions is used, the system displays a message indicating that the BFD session is being updated and you may try later.
- When the number of the destination port used in a multi-hop BFD control packet is updated, the BFD session in Up state may change to Down and then the BFD session is renegotiated.

NOTE

Determine to use port 3784 or 4784 before configuring a multi-hop BFD session between a Huawei device and a non-Huawei device. If the port number is not specified, you must change the port number after the BFD session becomes Up. Before changing the port number, shut down the BFD session. This is because changing the port number may cause all multi-hop BFD session to flap and affect services.

Example

Set the default destination port number to 4784 for multi-hop BFD control packets.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] multi-hop destination-port 4784
```

Related Topics

18.5.21 display bfd session
18.5.22 display bfd statistics
18.5.30 peer-ip ttl

18.5.30 peer-ip ttl

Function

The **peer-ip ttl** command configures the TTL value in BFD packets.

The **undo peer-ip ttl** command restores the default TTL value in BFD packets.

By default, the TTL value in BFD packets varies with the BFD session type. By default, for a static BFD session, the TTL value of a single-hop BFD packet is 255 and the TTL value of a multi-hop BFD packet is 254. For a dynamic BFD session, the TTL value of a single-hop BFD packet is 255 and the TTL value of a multi-hop BFD packet is 253.

Format

peer-ip *peer-ip mask-length* **ttl** { **single-hop** | **multi-hop** } *ttl-value*

undo peer-ip *peer-ip mask-length* **ttl** { **single-hop** | **multi-hop** }

Parameters

Parameter	Description	Value
peer-ip	Specifies the peer IP address bound to the BFD session.	-
mask-length	Specifies the mask length of the IP address.	The value is an integer that ranges from 8 to 32.
single-hop	Indicates the single-hop BFD session.	-
multi-hop	Indicates the multi-hop BFD session.	-
ttl-value	Specifies the TTL value in BFD packets.	The value is an integer that ranges from 1 to 255.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the TTL value in BFD packets to enable the Huawei device to interwork with each other in different versions, with upgraded devices, and with non-Huawei devices.

Precautions

- The length of the IP segment address must match the mask. A long mask takes precedence over a short mask.
- The same IP segment addresses, masks, and TTL values of specified BFD session types cannot be configured simultaneously.
- When the IP network segment addresses and mask lengths are the same, the TTL value of a single-hop BFD session must be greater than the TTL value of a multi-hop BFD session.
- When a large number of BFD sessions are set up, updating the TTL value may take a long time. Therefore, when a smaller interval for configuring BFD sessions is used, the system displays a message indicating that the BFD session is being updated and you may try later.
- After the TTL value in multi-hop BFD packets is configured, you must configure the same peer IP address, mask length longer than the mask length for the TTL value in multi-hop BFD packets, and TTL value in single-hop BFD

 Copyright © Huawei Technologies Co., Ltd.

packets. This is because the TTL value in multi-hop BFD packets affects dynamic single-hop BFD sessions.

Example

Set the TTL value of single-hop BFD sessions to 254, the IP segment address to 10.10.10.0, and the mask length to 24.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] peer-ip 10.10.10.0 24 ttl single-hop 254
```

Related Topics

18.5.29 multi-hop destination-port

18.5.21 display bfd session

18.5.24 display bfd ttl

18.5.31 process-interface-status

Function

The **process-interface-status** command associates the BFD session status with the bound interface status.

The **undo process-interface-status** command restores the default setting.

By default, the BFD session status is not associated with the interface status. That is, the change of the BFD session status does not affect the interface status.

Format

process-interface-status [**sub-if**][**reboot-no-impact**]

undo process-interface-status [**sub-if**] [**reboot-no-impact**]

Parameters

Parameter	Description	Value
sub-if	Associates the BFD session status with the bound sub-interface status. The status change of a BFD session that is bound to a primary interface affects the status of the primary interface and sub-interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
reboot-no-impact	Disables the association between a multicast BFD session and interface during device startup.	-

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a transmission device exists on a direct link, BFD detects a link fault faster than a link protocol on an interface. The link protocol status of a trunk or VLANIF interface depends on the link protocol status of member interfaces.

To help BFD rapidly report the detection result to the application, a BFD status attribute is added to the interface management module of each interface. This attribute indicates the status of the BFD session that is bound to the interface. The system obtains the interface status based on the link status, protocol status, and BFD status on the interface, and then reports the interface status to the application.

Precautions

When configuring the **process-interface-status** command, pay attention to the following points:

- The **process-interface-status** command takes effect for only the single-hop BFD session that uses the default multicast address. The BFD session can be associated to the primary interface or sub-interface status.
- If multiple BFD sessions are bound to an interface, you can use the **process-interface-status** command for only one BFD session. The change of only one BFD session changes the status of the bound interface.
- The BFD session does not report the BFD status to the bound interface immediately after the **commit** command is executed because the BFD session may not be set up or not Up before the **commit** command is executed. This prevents the BFD session from reporting an incorrect state to the interface. When the **commit** command is executed and the BFD status changes, the BFD session reports the BFD status to the interface to trigger the interface status change.
- If the **process-interface-status** command is saved in the configuration file, the BFD session for which the **process-interface-status** command is run notifies an interface that the BFD session becomes Down when the device is restarted. This is because the initial status of the interface is Down.

 Copyright © Huawei Technologies Co., Ltd.

- Before the BFD session status is associated with the interface status, the BFD configurations on two ends must be correct and matched. If the BFD session status on the local interface is Down, check whether the BFD configuration on the peer end is correct or whether the BFD session is shut down.
- If the BFD session must be synchronized to an interface immediately, ensure that the BFD configurations on the two ends are the same and run the **shutdown (BFD session view)** and **undo shutdown (BFD session view)** commands on the BFD session. When the **undo shutdown (BFD session view)** command is executed for a BFD session, a BFD session detection timer is started. If the BFD session becomes Up through negotiation before the timer times out, the BFD session notifies an interface of the Up state. Otherwise, the BFD session considers the link faulty and notifies the interface of the Down state. The status of a BFD session and the status of an interface can be synchronized in real time.

Example

Associate the BFD session with an interface to which the BFD session is bound.

```
<Huawei> system-view
[Huawei] bfd test
[Huawei-bfd-session-test] process-interface-status
```

Related Topics

18.5.4 bfd bind peer-ip default-ip

18.5.9 bfd session-name

18.5.21 display bfd session

18.5.32 process-pst

Function

The **process-pst** command enables the system to modify the port status table (PST) when the BFD session status changes.

The **undo process-pst** command restores the default configuration.

By default, the device is disabled from modifying the PST.

Format

process-pst

undo process-pst

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a BFD session that is enabled to modify the PST detects a BFD session Down event, the system modifies the corresponding entry in the PST.

In a static BFD for CR-LSP scenario, this command triggers a fast switchover between a primary CR-LSP and a backup CR-LSP when the BFD session status changes.

In a static BFD for TE scenario, this command triggers a fast switchover between TE tunnels when the BFD session status changes.

In both scenarios, when an LSP or a TE tunnel functions as a backward tunnel, this command triggers a primary/secondary switchover if the current BFD session becomes Down.

Precautions

- You can only run the **process-pst** command in the BFD session view that is bound to an interface (single-hop BFD) or the BFD session view that is bound to LDP LSP, Static LSP, or MPLS TE.
- When configuring static BFD-based LDP FRR, you must configure the **process-pst** command.
- When configuring static BFD for CR-LSP and static BFD for TE, you must configure the **process-pst** command.
- For applications in which a fault detected by BFD is not sensed through the PST, you do not need to configure the **process-pst** command.

Example

Enable the system to modify the PST when the BFD session status changes.

```
<Huawei> system-view
[Huawei] bfd 4ldplsp bind ldp-lsp peer-ip 10.10.9.9 nexthop 10.10.10.10
[Huawei-bfd-lsp-session-4ldplsp] process-pst
<Huawei> system-view
[Huawei] bfd 4staticlsp bind static-lsp 39
[Huawei-bfd-lsp-session-4staticlsp] process-pst
<Huawei> system-view
[Huawei] bfd 4mplste bind mpls-te interface Tunnel 0/0/0
[Huawei-bfd-lsp-session-4mplste] process-pst
<Huawei> system-view
[Huawei] bfd 4mplstelsp bind mpls-te interface Tunnel 0/0/0 te-lsp
[Huawei-bfd-lsp-session-4mplstelsp] process-pst
```

Related Topics

18.5.9 bfd session-name
18.5.21 display bfd session

18.5.33 reset bfd statistics

Function

The **reset bfd statistics** command clears statistics on received and sent packets of a BFD session.

Format

reset bfd statistics { **all** | **discriminator** *discr-value* }

Parameters

Parameter	Description	Value
all	Clears statistics on received and sent packets of all the BFD sessions.	-
discriminator *discr-value*	Clears statistics on received and sent packets of a BFD session with a specified discriminator.	The value is an integer that ranges from 1 to 16383.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **reset bfd statistics** command clears statistics on received and sent packets of a BFD session.

Precautions

The deleted statistics on received and sent packets of a BFD session cannot be restored. Exercise caution when you use this command.

Example

Clear statistics on packets of all BFD sessions.

```
<Huawei> reset bfd statistics all
```

Related Topics

18.5.22 display bfd statistics
18.5.23 display bfd statistics session

18.5.34 shutdown (BFD session view)

Function

The **shutdown** command enables the BFD session to enter the AdminDown state.

The **undo shutdown** command enables a BFD session.

By default, a BFD session is enabled.

Format

shutdown

undo shutdown

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **shutdown** command enables the BFD session to enter the AdminDown state.

Prerequisites

A BFD session has been created.

Precautions

- To modify the configuration of a BFD session, run the **shutdown** command to disable the BFD session. After the configuration is modified successfully, run the **undo shutdown** command to enable the BFD session again.
- To disable a BFD session without affecting the upper-layer application, run the **shutdown** command to enable the BFD session to enter the AdminDown state.

Example

Stop the BFD session **atoc**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] bfd atoc
[Huawei-bfd-session-atoc] shutdown
```

Related Topics

18.5.9 bfd session-name

18.5.35 snmp-agent bfd trap-interval

Function

The **snmp-agent bfd trap-interval** command sets the interval at which traps are sent.

The **undo snmp-agent bfd trap-interval** command restores the default interval at which traps are sent.

By default, the interval at which traps are sent is 120s.

Format

snmp-agent bfd trap-interval *interval*

undo snmp-agent bfd trap-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which traps are sent.	The value is an integer that ranges from 1 to 600, in seconds.

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the BFD module is enabled with the SNMP alarm function, the NMS will receive BFD Up or Down messages. If the BFD session flaps, the NMS receives a large number of traps. In this case, BFD traps need to be suppressed. Run the **snmp-agent bfd trap-interval** command to set the interval at which traps are sent to prevent overflow of traps.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

Global BFD has been enabled using the **bfd** command.

Example

Set the interval at which traps are sent to 100s.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] snmp-agent bfd trap-interval 100
```

18.5.36 snmp-agent trap enable feature-name bfd

Function

The **snmp-agent trap enable feature-name bfd** command enables the trap function for the BFD module.

The **undo snmp-agent trap enable feature-name bfd** command disables the trap function for the BFD module.

By default, the trap function is disabled for the BFD module.

Format

snmp-agent trap enable feature-name bfd [**trap-name** { **hwbfdsessdown** | **hwbfdsessreachlimit** | **hwbfdsessreachlimitbindif** | **hwbfdsessup** }]

undo snmp-agent trap enable feature-name bfd [**trap-name** { **hwbfdsessdown** | **hwbfdsessreachlimit** | **hwbfdsessreachlimitbindif** | **hwbfdsessup** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwbfdsessdown	Sends a Huawei proprietary trap when the BFD session goes Down.	-
hwbfdsessreachlimit	Sends a Huawei proprietary trap when the number of established BFD sessions on the device reaches the upper limit.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwbfdsessreachlimit-bindif	Sends a Huawei proprietary trap when the number of established BFD sessions reaches the upper limit.	-
hwbfdsessup	Sends a Huawei proprietary trap when the BFD session becomes Up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can specify **trap-name** to enable the trap function for one or more events of the BFD module.

Example

Enable the device to send a Huawei proprietary trap when the number of established BFD sessions on the board reaches the upper limit.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name bfd trap-name hwbfdsessreachlimit
```

Related Topics

18.5.25 display snmp-agent trap feature-name bfd all

18.5.37 tos-exp

Function

The **tos-exp** command sets the priority of BFD packets.

The **undo tos-exp** command restores the default priority of BFD packets.

By default, the priority of BFD packets is 7.

Format

tos-exp *tos-value*

undo tos-exp

Parameters

Parameter	Description	Value
tos-value	Specifies the priority of BFD packets. A greater value indicates a higher priority of BFD packets.	The value is an integer that ranges from 0 to 7. The default value is 7.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can change the priority of BFD packets in the following scenarios:

- Detect whether packets with different priorities on a link can be forwarded.
- Ensure that BFD packets with a higher priority are forwarded first.

Precautions

When congestion occurs, the system first sends BFD packets with a higher priority.

The **tos-exp** command takes effect for only static BFD sessions.

Example

Set the priority of BFD packets for the BFD session **atob** to 5.

```
<Huawei> system-view
[Huawei] bfd atob
[Huawei-bfd-session-atob] tos-exp 5
```

Related Topics

18.5.9 bfd session-name

18.5.38 track bfd

Function

The **track bfd** command adds a BFD session to a BFD group.

The **undo track bfd** command deletes a BFD session from a BFD group.

Format

track bfd *session-name*

undo track bfd *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a BFD session.	The value is a string of 1 to 15 case-sensitive characters without spaces. **NOTE** If the character string is quoted by quotation marks, the character string can contain spaces.

Views

BFD group view

Default Level

2: Configuration level

Usage Guidelines

On a live network, to improve network reliability, a branch gateway connects to the headquarters using multiple links. The branch gateway needs to determine on which link an IPSec tunnel is established. You can associate IPSec with BFD so that the branch gateway controls IPSec tunnel setup or teardown according to the BFD session or BFD group status. The association ensures that only one link is available at any time, and implements redundancy control of the IPSec tunnel.

Example

Add a BFD session to a BFD group.

```
<Huawei> system-view
[Huawei] bfd-group group
[Huawei-bfd-group-group] track bfd bfd
```

18.5.39 unlimited-negotiate

Function

The **unlimited-negotiate** command enables unlimited negotiation for a multicast BFD session.

The **undo unlimited-negotiate** command disables unlimited negotiation for a multicast BFD session.

By default, unlimited negotiation is disabled for a multicast BFD session.

Format

unlimited-negotiate

undo unlimited-negotiate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

If a multicast BFD session is bound to a Layer 3 interface to which no IP address is assigned, the status of the session is set to Down. You can run the **unlimited-negotiate** command to restart session negotiation. If the link is normal, the session can go Up through negotiation.

Example

Enable unlimited negotiation for a multicast BFD session.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd atob bind peer-ip default-ip interface gigabitethernet 1/0/0
[Huawei-bfd-session-atob] unlimited-negotiate
```

18.5.40 wtr

Function

The **wtr** command sets the WTR time of a BFD session.

The **undo wtr** command restores the default WTR time of a BFD session.

By default, the WTR time is 0, indicating that the status change of a BFD session is reported immediately.

Format

wtr *wtr-value*

undo wtr

Parameters

Parameter	Description	Value
wtr-value	Specifies the WTR time of a BFD session.	The value is an integer that ranges from 0 to 60, in minutes. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Views

BFD session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a BFD session flaps, the WTR time prevents frequent active/standby switchovers of the application associated with the BFD session.

Precautions

- If the WTR time is set, the system reports the BFD session Up event to the upper-layer application only after the WTR timer expires. Other status change events are reported immediately, which are not affected by the WTR time.
- Both ends must use the same WTR time. Otherwise, when the session status changes at one end, applications at both ends detect different BFD session status.

Example

Set the WTR time of a BFD session to 10 minutes.

```
<Huawei> system-view
[Huawei] bfd atoc
[Huawei-bfd-session-atoc] wtr 10
```

Related Topics

18.5.9 bfd session-name

18.5.41 lsp-path-check disable

Function

The **lsp-path-check disable** command disables consistency check for the forward and reverse primary and backup paths in a static BFD for CR-LSP scenario.

The **undo lsp-path-check disable** command enables consistency check for the forward and reverse primary and backup paths in a static BFD for CR-LSP scenario.

By default, when BFD is enabled globally, consistency check is enabled for the forward and reverse primary and backup paths.

Format

lsp-path-check disable

undo lsp-path-check disable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

BFD view

Default Level

2: Configuration level

Usage Guidelines

In a BFD for CR-LSP scenario, if the forward primary path is the same as the reverse backup path and the reverse primary path is the same as the forward backup path, path inconsistency occurs. If consistency check has been enabled for the forward and reverse primary and backup paths, the device reports an alarm, prompting you to reconfigure primary and backup paths. If the forward and reverse primary paths are the same and the forward and reverse backup paths are also the same, run the **lsp-path-check disable** command to disable consistency check for the forward and reverse primary and backup paths.

Example

Disable consistency check for the forward and reverse primary and backup paths.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] lsp-path-check disable
```

18.6 VRRP Configuration Commands

18.6.1 direct-route track vrrp

Function

The **direct-route track vrrp** command associates a direct route with a VRRP group.

The **undo direct-route track vrrp** command disassociates a direct route from a VRRP group.

By default, a direct route is not associated with a VRRP group.

Format

direct-route track vrrp vrid *virtual-router-id* **degrade-cost** *cost*

undo direct-route track vrrp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
degrade-cost *cost*	Specifies the link cost of an interface.	The value is an integer that ranges from 1 to 4294967295.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the IP RAN scenario, when the faulty UPE recovers, the interface becomes Up and a direct route is generated immediately. However, the interface does not learn the MAC address. As a result, the forwarding performance is low and the traffic that is switched back is lost. This problem can be prevented if the direct route is generated after the VRRP group status becomes Master. After the **direct-route track vrrp** command is executed to associate a direct route with a VRRP group, the cost of the direct route on the network segment where the address of the master's interface belongs is adjusted based on the VRRP group status.

Configuration Impact

After this command is executed, the cost of the direct route on the network segment where the address of the master's interface belongs is adjusted based on the VRRP group status:

- When the VRRP group is in Backup state, the cost of the direct route increases by *cost*. The priority of the direct route is reduced so that the direct route is not selected preferentially.
- When the VRRP group is in Master state, the cost of the direct route is reset. That is, the direct route is preferred.

Precautions

- Before running the **direct-route track vrrp** command, ensure that a VRRP group has been created.
- The **direct-route track vrrp** command can be only executed at one time on an interface. Before associating a direct route with a VRRP group specified by **vrid** *virtual-router-id*, delete the original command.

Example

Associate the direct route of the network segment where GE1/0/0 belongs to with a VRRP group.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 2 virtual-ip 10.1.1.10
[Huawei-GigabitEthernet1/0/0] direct-route track vrrp vrid 2 degrade-cost 230
```

18.6.2 display snmp-agent trap feature-name vrrp all

Function

The **display snmp-agent trap feature-name vrrp all** command displays all trap messages of the VRRP module.

Format

display snmp-agent trap feature-name vrrp all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The Simple Network Management Protocol (SNMP) is a network management protocol widely used on TCP/IP networks. SNMP uses a central computer (a network management station) that runs network management software to manage network elements. The SNMP agent reports trap messages to the network management station so that the network management station can quickly determine the network status, and the network administrator can take measures accordingly.

The **display snmp-agent trap feature-name vrrp all** command displays the following information:

- Trap names supported by the VRRP module: The trap names are the same as the trap names specified by the **snmp-agent trap enable feature-name vrrp** [**trap-name** { **vrrptrapauthfailure** | **vrrptrapmasterdown** | **vrrptrapnewmaster** }] command. Each trap name corresponds to a network element abnormality.
- Trap status of the VRRP module: You can check whether a trap is reported based on the trap name.

Prerequisites

SNMP agent has been enabled using the **snmp-agent** command.

Example

Display all trap messages of the VRRP module.

```
<Huawei> display snmp-agent trap feature-name vrrp all
-------------------------------------------------------------------------------
Feature name: VRRP
Trap number : 6
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
vrrpTrapNewMaster              on                      on
vrrpTrapAuthFailure            on                      on
vrrpTrapMasterDown             on                      on
hwVrrpExtTrapNonMaster         on                      on
vrrpv3NewMaster                on                      on
vrrpv3ProtoError               on                      on
```

Table 18-21 Description of the **display snmp-agent trap feature-name vrrp all** command output

Item	Description
Feature name	Name of the module that a trap message belongs to.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the VRRP module: ● vrrpTrapAuthFailure: This trap message is generated when the authentication mode and key in the received packet conflicts with those on the device. ● vrrpTrapMasterDown: This trap message is generated when the VRRP group status changes from Master to another status. ● vrrpTrapNewMaster: This trap message is generated when the VRRP group status changes to Master. ● hwVrrpExtTrapNonMaster: This trap is generated when the VRRP backup group status changes from Backup to Initialize or from Initialize to Backup. ● vrrpv3NewMaster: This trap is generated when VRRPv3 changes from another state to the Master state. ● vrrpv3ProtoError: This trap is generated when a device in a VRRPv3 backup group receives an incorrect VRRP packet.
Default switch status	Whether the trap function is enabled by default: ● on: The trap function is enabled. ● off: The trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Status of the trap function: • on: The trap function is enabled. • off: That the trap function is disabled.

Related Topics

18.6.14 snmp-agent trap enable feature-name vrrp

18.6.3 display vrrp

Function

The **display vrrp** command displays the status and configuration parameters of VRRP groups.

Format

display vrrp [**interface** *interface-type interface-number*] [*virtual-router-id*] [**brief**]

display vrrp { **interface** *interface-type interface-number* [*virtual-router-id*] | *virtual-router-id* } **verbose**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the status of all VRRP groups on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
virtual-router-id	Displays the status of a VRRP group with the specified VRID.	The VRID of the VRRP group must have been created.
brief	Displays brief information about a specified VRRP group. If this parameter is not specified, detailed information about a VRRP group is displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
verbose	Displays detailed information about a VRRP group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp** command displays information about VRRP groups.

Example

Display information about all VRRP groups on the router.

```
<Huawei> display vrrp
GigabitEthernet1/0/0 | Virtual Router 1
    State : Master
    Virtual IP : 10.1.1.100
    Master IP : 10.1.1.2
    PriorityRun : 120
    PriorityConfig : 120
    MasterPriority : 120
    Preempt : YES   Delay Time : 20 s
    TimerRun : 2 s
    TimerConfig : 2 s
    Auth type : SIMPLE   Auth key : ******
    Virtual MAC : 0000-5e00-0101
    Check TTL : YES
    Config type : normal-vrrp
    Backup-forward : disabled
    Track BFD : 69                    Priority reduced : 10
    BFD-session state : UP
    Create time : 2011-10-07 15:43:42
    Last change time : 2011-10-07 15:44:03
```

Table 18-22 Description of the **display vrrp** command output

Item	Description
GigabitEthernet1/0/0 | Virtual Router 1	Interface where the VRRP group is configured and VRID of the VRRP group.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
State	VRRP status of the device: ● Master: The device functions as the master in the VRRP group. ● Backup: The device functions as the backup in the VRRP group. ● Initialize: All VRRP groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP group status is switched to Initialize.
Virtual IP	Virtual IP address of a VRRP group. To configure a virtual IP address for a VRRP group, run the **vrrp vrid virtual-ip** command.
Master IP	Primary IP address of the interface configured with the VRRP group on the master.
PriorityRun	Priority of the router when the VRRP group runs. If the router is the IP address owner in a VRRP group, the running priority of the router in the group is displayed as **255**.
PriorityConfig	Priority configured for the router using the **vrrp vrid priority** command. If the router is the IP address owner and this value is not configured, the default priority 100 but not 255 is displayed.
MasterPriority	Priority of the master in the VRRP group. If the router is the IP address owner in a VRRP group, the priority of the router in the group is displayed as **255**.
Preempt	Preemption mode: ● YES: preemption ● NO: no preemption To disable the preemption mode, run the **vrrp vrid preempt-mode disable** command.
Delay Time	Preemption delay, in seconds. To set the preemption delay, run the **vrrp vrid preempt-mode timer delay** command.
TimerRun	Interval at which the master in the VRRP group sends VRRP Advertisement packets, in seconds.
TimerConfig	Configured interval at which the master in the VRRP group sends VRRP Advertisement packets, in seconds. To set the interval at which the master in the VRRP group sends VRRP Advertisement packets, run the **vrrp vrid timer advertise** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Auth type	VRRP Advertisement packet authentication mode: ● NONE: non-authentication ● SIMPLE: simple authentication ● MD5: MD5 authentication To set an authentication mode, run the **vrrp vrid authentication-mode** command. VRRPv3 does not support authentication.
Auth key	Authentication key. If authentication is configured, ****** is displayed. If no authentication is configured, this field is not displayed.
Virtual MAC	Virtual MAC address of the VRRP group.
Check TTL	Whether the TTL value of a VRRP Advertisement packet is checked: ● YES: The TTL value of a VRRP Advertisement packet is checked. ● NO: The TTL value of a VRRP Advertisement packet is not checked. To configure the router to check the TTL value in a VRRP Advertisement packet, run the **vrrp un-check ttl** command.
Config type	VRRP group type. This field has a fixed value of **normal-vrrp**.
Backup-forward	Whether the backup is enabled to forward traffic: ● enabled ● disabled
Track BFD	Local discriminator or name of the BFD session associated with the VRRP group. This field is displayed when only the BFD session is associated with the VRRP group.
Priority reduced	Value by which the VRRP priority reduces if the interface or BFD session associated with the VRRP group becomes Down. If the Increase mode is configured, **Priority increased** is displayed. **Priority increased** indicates the value by which the VRRP priority increases if the interface or BFD session associated with the VRRP group becomes Down.
BFD-session state	Status of the BFD session associated with the VRRP group: ● UP: A BFD session is in Up state. ● DOWN: A BFD session is in Down state. ● AdminDown: A BFD session is in AdminDown state.
Create time	Time when the VRRP group was created.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Last change time	Last time the VRRP group status changed.

Display brief information about all VRRP groups on the router.

```
<Huawei> display vrrp brief
Total:1     Master:0     Backup:0     Non-active:1
VRID  State        Interface                Type     Virtual IP
------------------------------------------------------------------
1     Initialize   Vlanif23                 Normal   10.1.1.100
```

Table 18-23 Description of the **display vrrp brief** command output

Item	Description
VRID	VRID of the VRRP group.
State	VRRP status of the router: ● Master: The router functions as the master in the VRRP group. ● Backup: The router functions as the backup in the VRRP group. ● Initialize: All VRRP groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP group status changes to Initialize.
Interface	Interface configured with the VRRP group.
Type	VRRP group type. This field has a fixed value of **normal-vrrp**.
Virtual IP	Virtual IP address of the VRRP group.
Total	Number of VRRP groups.
Master	Number of VRRP groups in Master state.
Backup	Number of VRRP groups in Backup state.
Non-active	Number of VRRP groups in Non-active state.

Related Topics

18.6.37 vrrp vrid virtual-ip
18.6.30 vrrp vrid priority
18.6.28 vrrp vrid preempt-mode disable
18.6.29 vrrp vrid preempt-mode timer delay
18.6.31 vrrp vrid timer advertise
18.6.27 vrrp vrid authentication-mode

 Copyright © Huawei Technologies Co., Ltd.

18.6.22 vrrp un-check ttl

18.6.4 display vrrp protocol-information

Function

The **display vrrp protocol-information** command displays VRRP information.

Format

display vrrp protocol-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display vrrp protocol-information** command to view VRRP information.

Example

Display VRRP information.

```
<Huawei> display vrrp protocol-information
 VRRP protocol information is shown as below:
   VRRP protocol version : V2
   Send advertisement packet mode : send v2 only
```

Table 18-24 Description of the **display vrrp protocol-information** command output

Item	Description
VRRP protocol version	VRRP version number: ● V2 ● V3 To configure a VRRP version number, run the **vrrp version** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Send advertisement packet mode	Mode in which VRRP Advertisement packets are sent: • send v2 only: Only VRRPv2 Advertisement packets are sent. • send v3 only: Only VRRPv3 Advertisement packets are sent. It is displayed only when VRRPv3 is used. • send v2v3 both: VRRPv2 and VRRPv3 Advertisement packets are sent. It is displayed only when VRRPv3 is used. To configure the mode in which VRRP Advertisement packets are sent, run the **vrrp vrid version-3 send-packet-mode** command in the interface view or run the **vrrp version-3 send-packet-mode** command in the system view.

Related Topics

18.6.23 vrrp version

18.6.36 vrrp vrid version-3 send-packet-mode

18.6.24 vrrp version-3 send-packet-mode

18.6.5 display vrrp state-change interface vrid

Function

The **display vrrp state-change interface vrid** command displays status changes of a specified VRRP group. This command can display a maximum of 10 of the latest status changes of a VRRP group.

Format

display vrrp state-change interface *interface-type interface-number* **vrid** *virtual-router-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface where status changes of a VRRP group are displayed. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vrid *virtual-router-id*	Specifies the VRID of a VRRP group.	The VRID of the VRRP group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the VRRP status becomes abnormal, run the **display vrrp state-change interface vrid** command to view the last 10 status changes of the VRRP group, including the time at which the VRRP group status changed, the VRRP group status before and after the change, and the cause of the VRRP group status change. The command output helps you locate faults.

Example

Display status changes of VRRP group 1 on VLANIF 100.

```
<Huawei> display vrrp state-change interface vlanif 100 vrid 1
  Time                    SourceState   DestState     Reason
  ---------------------------------------------------------------
  2012-01-27 15:29:45       Backup        Master        Protocol timer expired
  2012-01-27 15:29:42       Initialize    Backup        Interface UP
```

 Copyright © Huawei Technologies Co., Ltd.

Table 18-25 Description of the **display vrrp state-change interface vrid** command output

Item	Description
Time	Time when the VRRP group status changed.
SourceState	VRRP group status before the change: ● Master ● Backup ● Initialize
DestState	VRRP group status after the change: ● Master ● Backup ● Initialize
Reason	Cause of the VRRP status change: ● Admin-vrrp drove ● BFD configure deleted ● CFM session down ● CFM session up ● EFM configure deleted ● EFM session down ● EFM session up ● Interface UP ● Interface down ● Ignore interface down ● Link BFD session down ● Link BFD session up ● Link BFD session deleted ● Link BFD down-number changed ● Peer BFD session down ● Priority calculation ● Protocol timer expired ● Track interface ● Track BFD session

18.6.6 display vrrp statistics

Function

The **display vrrp statistics** command displays statistics about sent and received packets of VRRP groups.

Format

display vrrp [**interface** *interface-type interface-number*] [*virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about sent and received packets of all VRRP groups on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are displayed.	-
virtual-router-id	Displays statistics about sent and received packets of a specified VRRP group. If this parameter is not specified, statistics about sent and received packets of all VRRP groups on the device or a specified interface are displayed.	The VRID of the VRRP group must have been created.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display vrrp statistics** command displays information about sent and received packets of VRRP groups.

Example

Display statistics about sent and received packets of VRRP group 1 on GE1/0/0.

```
<Huawei> display vrrp interface gigabitethernet 1/0/0 1 statistics
 GigabitEthernet 1/0/0 | Virtual Router 1
                        Transited to master : 1
                        Transited to backup : 1
                   Transited to initialize : 0
                   Received advertisements : 0
                       Sent advertisements : 1000
             Advertisement interval errors : 0
            Failed to authentication check : 0
                    Received ip ttl errors : 0
        Received packets with priority zero : 0
           Sent packets with priority zero : 0
            Received invalid type packets : 0
     Received unmatched address list packets : 0
        Unknown authentication type packets : 0
            Mismatched authentication type : 0
                     Packet length errors : 0
     Discarded packets since track admin-vrrp : 0
                Received attacking packets : 0
                 Received selfsend packets : 0
```

Display statistics about all VRRP Advertisement packets on the device.

```
<Huawei> display vrrp statistics
 Checksum errors : 0
  Version errors : 0
     Vrid errors : 0
    Other errors : 0

 GigabitEthernet1/0/0 | Virtual Router 1
                        Transited to master : 1
                        Transited to backup : 1
                   Transited to initialize : 0
                   Received advertisements : 0
                       Sent advertisements : 1000
             Advertisement interval errors : 0
            Failed to authentication check : 0
                    Received ip ttl errors : 0
        Received packets with priority zero : 0
           Sent packets with priority zero : 0
            Received invalid type packets : 0
     Received unmatched address list packets : 0
        Unknown authentication type packets : 0
            Mismatched authentication type : 0
                     Packet length errors : 0
     Discarded packets since track admin-vrrp : 0
                Received attacking packets : 0
                 Received selfsend packets : 0
```

Table 18-26 Description of the display vrrp statistics command output

Item	Description
Checksum errors	CRC error count.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Version errors	Version error count.
Vrid errors	Number of VRID errors.
Other errors	Number of other errors.
GigabitEthernet 1/0/0 | Virtual Router 1	Interface where the VRRP group is configured and VRID of the VRRP group.
Transited to master	Number of times the router transitions to the Master state.
Transited to backup	Number of times the router transitions to the Backup state.
Transited to initialize	Number of times the router transitions to the Initialize state.
Received advertisements	Number of received VRRP Advertisement packets.
Sent advertisements	Number of sent VRRP Advertisement packets.
Advertisement interval errors	Number of times VRRP Advertisement packets are sent at an incorrect interval.
Failed to authentication check	Number of authentication failures.
Received ip ttl errors	Number of packets with TTL errors.
Received packets with priority zero	Number of received VRRP Advertisement packets with the priority of 0.
Sent packets with priority zero	Number of sent VRRP Advertisement packets with the priority of 0.
Received invalid type packets	Number of received VRRP Advertisement packets of invalid type.
Received unmatched address list packets	Number of packets with incorrect virtual IP address lists.
Unknown authentication type packets	Number of packets with an unknown authentication mode.
Mismatched authentication type	Number of packets with a non-matched authentication mode.
Packet length errors	Number of packets with incorrect length.
Discarded packets since track admin-vrrp	Number of received packets that are discarded after a VRRP group is bound to a management VRRP (mVRRP) group. The router does not support mVRRP.
Received attacking packets	Number of received attack packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Received selfsend packets	Number of received packets sent by the router.

Related Topics

18.6.37 vrrp vrid virtual-ip
18.6.30 vrrp vrid priority
18.6.28 vrrp vrid preempt-mode disable
18.6.29 vrrp vrid preempt-mode timer delay
18.6.31 vrrp vrid timer advertise
18.6.27 vrrp vrid authentication-mode
18.6.22 vrrp un-check ttl

18.6.7 display vrrp6

Function

The **display vrrp6** command displays the status and configuration parameters of VRRP6 groups.

Format

display vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] [**brief**]

display vrrp6 { **interface** *interface-type interface-number* [**vrid** *virtual-router-id*] | **vrid** *virtual-router-id* } **verbose**

Parameters

Parameter	Description	Description
interface *interface-type interface-number*	Displays the status of all VRRP6 groups on the specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, information about all VRRP6 groups is displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Description
vrid *virtual-router-id*	Displays the status of a VRRP6 group with the specified VRID.	The VRID of the VRRP6 group must have been created.
brief	Displays brief information about a specified VRRP6 group.	-
verbose	Displays detailed information about a specified VRRP6 group.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can view the status and configuration of all VRRP6 groups based on networking, including interfaces where mVRRP6 groups are configured, and VRIDs and statuses of VRRP6 groups.

Example

Display information about all VRRP6 groups on the router with VRID 4.

```
<Huawei> display vrrp6 vrid 4
GigabitEthernet1/0/0 | Virtual Router 4
    State            : Master
    Virtual IP       : FE80::1:2
    Master IP : FE80::218:82FF:FED3:2AF1
    PriorityRun      : 200
    PriorityConfig   : 200
    MasterPriority   : 200
    Preempt          : YES                    Delay Time : 0 s
    TimerRun         : 100 cs
    TimerConfig      : 100 cs
    Virtual Mac      : 0000-5e00-0204
    Check hop limit  : YES
    Config type      : normal-vrrp
    Backup-forward   : disabled
    Track BFD : 69                    Priority reduced : 10
    BFD-session state : UP
    Create time      : 2012-05-22 17:40:56
    Last change time : 2012-05-22 17:41:03
```

Table 18-27 Description of the display vrrp6 command output

Item	Description
GigabitEthernet1/0/0 | Virtual Router 4	Interface where the VRRP6 group is configured and VRID of the VRRP6 group.
State	VRRP6 status of the device: ● Master: The device functions as the master in the VRRP6 group. ● Backup: The device functions as the backup in the VRRP6 group. ● Initialize: All VRRP6 groups begin in Initialize state. When the status of an interface is Down or administratively Down, the VRRP6 group status changes to Initialize.
Virtual IP	Virtual IP address of the VRRP6 group. To configure a virtual IP address for a VRRP6 group, run the **vrrp6 vrid virtual-ip** command.
Master IP	Primary IP address of the interface configured with the VRRP6 group on the master.
PriorityRun	Priority of the router when the VRRP6 group runs. If the router is the IP address owner in a VRRP6 group, the running priority of the router in the group is displayed as **255**.
PriorityConfig	Priority configured for the router using the **vrrp6 vrid priority** command. If the router is the IP address owner, the default priority 100 but not 255 is displayed.
MasterPriority	Priority of the master in the VRRP6 group. If the router is the IP address owner in a VRRP6 group, the priority of the router in the group is displayed as **255**.
Preempt	Preemption mode: ● YES: preemption ● NO: no preemption To disable the preemption mode, run the **vrrp6 vrid preempt-mode disable** command.
Delay Time	Preemption delay, in seconds. To set the preemption delay, run the **vrrp6 vrid preempt-mode timer delay** command.
TimerRun	Interval at which the master in the VRRP6 group sends VRRP Advertisement packets, in centiseconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TimerConfig	Configured interval at which the master in the VRRP6 group sends VRRP6 Advertisement packets, in centiseconds. To set the interval at which the master in the VRRP6 group sends VRRP6 Advertisement packets, run the **vrrp6 vrid timer advertise** command.
Virtual Mac	Virtual MAC address of the VRRP6 group.
Check hop limit	Whether the TTL value of a VRRP6 Advertisement packet is checked: ● YES: The TTL value of a VRRP6 Advertisement packet is checked. ● NO: The TTL value of a VRRP6 Advertisement packet is not checked. To configure the device to check the TTL value in a VRRP6 Advertisement packet, run the **vrrp6 un-check hop-limit** command.
Config type	VRRP6 group type. This field has a fixed value of **normal-vrrp**.
Backup-forward	Whether the backup is enabled to forward traffic: ● enabled ● disabled
Track BFD	Local discriminator or name of the BFD session associated with the VRRP6 group. This field is displayed when only the BFD session is associated with the VRRP6 group.
Priority reduced	Value by which the VRRP6 priority reduces if the interface or BFD session associated with the VRRP6 group becomes Down. If the Increase mode is configured, **Priority increased** is displayed. **Priority increased** indicates the value by which the VRRP6 priority increases if the interface or BFD session associated with the VRRP6 group becomes Down.
BFD-Session State	Status of the BFD session associated with the VRRP6 group: ● UP: A BFD session is in Up state. ● DOWN: A BFD session is in Down state. ● AdminDown: A BFD session is in AdminDown state.
Last Change Time	Last time the VRRP6 group status changed.
Create time	Time when the VRRP6 group was created.

Display brief information about all VRRP6 groups on the device.

```
<Huawei> display vrrp6 brief
Total:2     Master:2     Backup:0     Non-active:0
VRID  State        Interface                Type     Virtual IP
```

```
-----------------------------------------------------------------
1    Master     GE0/0/1              Normal   FE80::1
2    Master     GE0/0/1              Normal   FE80::1:3
```

Table 18-28 Description of the display vrrp6 brief command output

Item	Description
VRID	VRID of the VRRP6 group.
State	VRRP6 status of the router: ● Master: The device functions as the master in the VRRP6 group. ● Backup: The device functions as the backup in the VRRP6 group. ● Initialize: All VRRP6 groups begin in Initialize state. When the interface where a VRRP group is configured becomes Down or is Administratively Down, the VRRP6 group status is switched to Initialize.
Interface	Interface configured with the VRRP6 group.
Type	VRRP6 group type. This field has a fixed value of **normal-vrrp**.
Virtual IP	Virtual IP address of the VRRP6 group.
Total	Number of VRRP6 groups.
Master	Number of VRRP6 groups in Master state.
Backup	Number of VRRP6 groups in Backup state.
Non-active	Number of VRRP6 groups in Non-active state.

Related Topics

18.6.48 vrrp6 vrid virtual-ip
18.6.42 vrrp6 vrid priority
18.6.43 vrrp6 vrid timer advertise

18.6.8 display vrrp6 state-change interface vrid

Function

The **display vrrp6 state-change interface vrid** command displays status changes of a specified VRRP6 group. This command can display a maximum of the latest 10 status changes of a VRRP6 group.

Format

display vrrp6 state-change interface *interface-type interface-number* **vrid** *virtual-router-id*

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface where status changes of a VRRP6 group are displayed.	-
virtual-router-id	Specifies the VRID of a VRRP6 group.	The VRID of the VRRP6 group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When the VRRP6 status becomes abnormal, run the **display vrrp6 state-change interface vrid** command to view the latest 10 status changes of the VRRP6 group. The command output includes the time when the VRRP6 group status changed, VRRP6 group status before and after each change, and causes of the status changes. The command output helps you locate faults.

Example

Display status changes of VRRP6 group 1 on VLANIF 100.

```
<Huawei> display vrrp6 state-change interface vlanif 100 vrid 1
Time                        SourceState  DestState   Reason
--------------------------------------------------------------------------------
2012-05-19 20:36:44         Initialize   Backup      interface up
2012-05-19 20:37:07         Backup       Master      protocol timer expired
```

Table 18-29 Description of the **display vrrp6 state-change interface vrid** command output

Item	Description
Time	Time when the VRRP6 status changed.
SourceState	Status before the change: ● Master ● Backup ● Initialize

Item	Description
DestState	Status after the change: ● Master ● Backup ● Initialize
Reason	Reason of the change in the status of the VRRP6 backup group: ● Admin-vrrp drove ● BFD configure deleted ● Interface up ● Interface down ● Link BFD session down ● Link BFD session up ● Link BFD session deleted ● Peer BFD session down ● Priority calculation ● Protocol timer expired ● Track interface ● Track BFD session

18.6.9 display vrrp6 statistics

Function

The **display vrrp6 statistics** command displays statistics about sent and received packets of VRRP6 groups.

Format

display vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about sent and received packets of all VRRP6 groups on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the router are displayed.	-
vrid *virtual-router-id*	Displays statistics about sent and received packets of a specified VRRP6 group. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups on the router or a specified interface are displayed.	The VRID of the VRRP6 group must have been created.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display vrrp6 statistics** command displays information about sent and received packets of VRRP6 groups.

Example

Display statistics about all VRRP6 Advertisement packets on the router.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display vrrp6 statistics
  Checksum errors : 0
   Version errors : 0
      Vrid errors : 0
     Other errors : 0

  GigabitEthernet1/0/0 | Virtual Router 1
                          Transited to master : 1
                          Transited to backup : 1
                     Transited to initialize : 0
                     Received advertisements : 0
                        Sent advertisements : 1000
               Advertisement interval errors : 0
               Failed to authentication check : 0
                     Received ip ttl errors : 0
          Received packets with priority zero : 0
             Sent packets with priority zero : 0
              Received invalid type packets : 0
       Received unmatched address list packets : 0
          Unknown authentication type packets : 0
             Mismatched authentication type : 0
                     Packet length errors : 0
       Discarded packets since track admin-vrrp : 0
                 Received attacking packets : 0
                  Received selfSend packets : 0
```

Table 18-30 Description of the **display vrrp6 statistics** command output

Item	Description
Checksum errors	CRC error count.
Version errors	Version error count.
Vrid errors	The Number of VRID errors of the VRRP6 group.
Other errors	Number of other errors.
GigabitEthernet1/0/0 | Virtual Router 1	Interface where the VRRP6 group is configured and VRID of the VRRP6 group.
Transited to master	Number of times the router transitions to the Master state.
Transited to backup	Number of times the router transitions to the Backup state.
Transited to initialize	Number of times the router transitions to the Initialize state.
Received advertisements	Number of received VRRP Advertisement packets.
Sent advertisements	Number of sent VRRP Advertisement packets.
Advertisement interval errors	Number of times VRRP Advertisement packets are sent at an incorrect interval.
Failed to authentication check	Number of authentication failures.
Received ip ttl errors	Number of packets with TTL errors.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Received packets with priority zero	Number of received VRRP Advertisement packets with the priority of 0.
Sent packets with priority zero	Number of sent VRRP Advertisement packets with the priority of 0.
Received invalid type packets	Number of received VRRP6 Advertisement packets of invalid type.
Received unmatched address list packets	Number of packets with incorrect virtual IPv6 address lists.
Unknown authentication type packets	Number of invalid authentication packets.
Mismatched authentication type	Number of packets with mismatching authentication types.
Packet length errors	Number of packets with incorrect length.
Discarded packets since track admin-vrrp	Number of received packets that are discarded after a VRRP6 group is bound to a management VRRP6 (mVRRP6) group. The router does not support mVRRP6.
Received attacking packets	Number of received attack packets.
Received selfsend packets	Number of received packets sent by the router.

18.6.10 dot1q vrrp

Function

The **dot1q vrrp** command enables a Dot1q termination sub-interface on a VRRP device to send VRRP Advertisement packets to a specified VLAN.

The **undo dot1q vrrp** command restores the default setting.

By default, a VRRP-enabled device sends VRRP Advertisement packets to only the VLAN with the minimum ID specified on a Dot1q termination sub-interface.

Format

dot1q vrrp vid *vid*

undo dot1q vrrp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vid *vid*	Specifies the ID of a VLAN.	The value is a decimal integer that ranges from 1 to 4094.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view, Eth-Trunk sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When VRRP is enabled on a Dot1q termination sub-interface, VRRP Advertisement packets need to be encapsulated with a VLAN tag so that VRRP Advertisement packets can be transmitted in the VLAN and negotiation can be performed between VRRP-enabled devices. The **dot1q vrrp** command enables a Dot1q termination sub-interface to add a specified VLAN tag to VRRP Advertisement packets or remove a specified tag from VRRP Advertisement packets.

Prerequisites

The **dot1q termination vid** command has been executed on an Ethernet sub-interface.

Precautions

When configuring VRRP and static ARP on a Dot1q termination sub-interface, QinQ termination sub-interface, or VLANIF interface, pay attention to the following points:

- An IP address mapped to a static ARP entry cannot be used as a virtual IP address.
- The virtual IP address of a VRRP group cannot map to a static ARP entry.

If a VRRP virtual IP address is mapped to a static ARP entry on a device, the device generates incorrect host routes, affecting traffic forwarding.

Example

Configure VRRP-enabled gigabitethernet1/0/0.1 to send VRRP Advertisement packets with VLAN ID 100.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0.1
[Huawei-GigabitEthernet1/0/0.1] dot1q termination vid 100
[Huawei-GigabitEthernet1/0/0.1] dot1q vrrp vid 100
[Huawei-GigabitEthernet1/0/0.1] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

6.3.19 dot1q termination vid

18.6.11 qinq vrrp

Function

The **qinq vrrp** command enables a QinQ terminal sub-interface on a VRRP-enabled device to send VRRP Advertisement packets to a specified VLAN.

The **undo qinq vrrp** command restores the default setting.

By default, a QinQ terminal sub-interface sends VRRP Advertisement packets to only the VLAN with the minimum ID specified on a QinQ termination sub-interface.

Format

qinq vrrp pe-vid *pe-vid* **ce-vid** *ce-vid*

undo qinq vrrp

Parameters

Parameter	Description	Value
pe-vid *pe-vid*	Specifies the VLAN ID of a PE (outer VLAN tag).	The value is a decimal integer that ranges from 1 to 4094.
ce-vid *ce-vid*	Specifies the VLAN ID of a CE (inner VLAN tag).	The value is a decimal integer that ranges from 1 to 4094.

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If VRRP is enabled on a QinQ termination sub-interface, VRRP Advertisement packets need to be encapsulated with inner and outer VLAN tags so that VRRP Advertisement packets can be transmitted in VLANs and negotiation can be performed between VRRP-enabled devices. The **qinq vrrp** command enables a QinQ termination sub-interface to add specified VLAN tags to VRRP Advertisement packets or remove specified tags from VRRP Advertisement packets.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **qinq termination pe-vid ce-vid** command has been executed on an Ethernet sub-interface.

Precautions

When configuring VRRP and static ARP on a Dot1q termination sub-interface, QinQ termination sub-interface, or VLANIF interface, pay attention to the following points:

- An IP address mapped to a static ARP entry cannot be used as a virtual IP address.
- The virtual IP address of a VRRP group cannot map to a static ARP entry.

If a VRRP virtual IP address is mapped to a static ARP entry on a device, the device generates incorrect host routes, affecting traffic forwarding.

NOTE

pe-vid and *ce-vid* in the **qinq vrrp** command must match *pe-vid* and *ce-vid* in the **qinq termination pe-vid ce-vid** command.

Example

Configure gigabitethernet1/0/0.1 to send packets with inner VLAN 100 and outer VLAN 200 to maintain the VRRP status.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0.1
[Huawei-GigabitEthernet1/0/0.1] qinq termination pe-vid 100 ce-vid 200
[Huawei-GigabitEthernet1/0/0.1] qinq vrrp pe-vid 100 ce-vid 200
[Huawei-GigabitEthernet1/0/0.1] quit
```

Related Topics

6.3.36 qinq termination pe-vid ce-vid

18.6.12 reset vrrp statistics

Function

The **reset vrrp statistics** command clears statistics about received and sent packets of VRRP groups.

Format

reset vrrp [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics about sent and received packets of all VRRP groups on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are cleared.	-
vrid *virtual-router-id*	Clears statistics about sent and received packets of a specified VRRP group. If this parameter is not specified, statistics about sent and received packets of all VRRP groups or a specified VRRP group on the device are cleared.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about VRRP Advertisement packets, run the **reset vrrp statistics** command to clear existing statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when executing the **reset vrrp statistics** command.

Example

Clear statistics about sent and received packets of VRRP group 1 on GE1/0/0.

```
<Huawei> reset vrrp interface gigabitethernet 1/0/0 vrid 1 statistics
```

Clear statistics about all the packets of VRRP group 1.

```
<Huawei> reset vrrp vrid 1 statistics
```

Clear statistics about packets of all VRRP groups on the router.

```
<Huawei> reset vrrp statistics
```

18.6.13 reset vrrp6 statistics

Function

The **reset vrrp6 statistics** command clears statistics about received and sent packets of VRRP6 groups.

Format

reset vrrp6 [**interface** *interface-type interface-number*] [**vrid** *virtual-router-id*] **statistics**

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics about sent and received packets of all VRRP6 groups on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the device are cleared.	-

Parameter	Description	Value
vrid *virtual-router-id*	Clears statistics about sent and received packets of a specified VRRP6 group. If this parameter is not specified, statistics about sent and received packets of all VRRP6 groups or a specified VRRP6 group on the device are cleared.	The value is an integer that ranges from 1 to 255.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before recollecting statistics about VRRP6 Advertisement packets, run the **reset vrrp6 statistics** command to clear existing statistics.

Precautions

The cleared statistics cannot be restored. Exercise caution when executing the **reset vrrp6 statistics** command.

Example

Clear statistics about sent and received packets of VRRP6 group 1 on GE1/0/0.

```
<Huawei> reset vrrp6 interface gigabitethernet 1/0/0 vrid 1 statistics
```

Clear statistics about all the packets of VRRP6 group 1.

```
<Huawei> reset vrrp6 vrid 1 statistics
```

Clear statistics about packets of all VRRP6 groups on the router.

```
<Huawei> reset vrrp6 statistics
```

18.6.14 snmp-agent trap enable feature-name vrrp

Function

The **snmp-agent trap enable feature-name vrrp** command enables the trap function for the VRRP module.

The **undo snmp-agent trap enable feature-name vrrp** command disables the trap function for the VRRP module.

By default, the trap function is enabled for the VRRP module.

Format

snmp-agent trap enable feature-name vrrp [**trap-name** { **hwvrrpexttrapnonmaster** | **vrrptrapauthfailure** | **vrrptrapmasterdown** | **vrrptrapnewmaster** | **vrrpv3newmaster** | **vrrpv3protoerror** }]

undo snmp-agent trap enable feature-name vrrp [**trap-name** { **hwvrrpexttrapnonmaster** | **vrrptrapauthfailure** | **vrrptrapmasterdown** | **vrrptrapnewmaster** | **vrrpv3newmaster** | **vrrpv3protoerror** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for the specified event. If no event type is specified using the **trap-name** parameter, the trap function is enabled for all events.	-
hwvrrpexttrapnonmaster	This trap is generated when the VRRP group status changes from Backup to Initialize or from Initialize to Backup.	-
vrrptrapauthfailure	Enables the vrrptrapauthfailure trap. When the authentication mode and key in the received packet conflicts with those on the router, the router sends this trap message to the NMS.	-
vrrptrapmasterdown	Enables the vrrptrapmasterdown trap. When the VRRP status changes from the Master state to the Backup or Initialize state, the router sends this trap message to the NMS.	-
vrrptrapnewmaster	Enables the vrrptrapnewmaster trap. When the VRRP status change from Backup or Initialize to Master, the router sends this trap message to the NMS.	-
vrrpv3newmaster	Enables the trap function when VRRPv3 changes from another state to the Master state.	-
vrrpv3protoerror	Enables the trap function when a device in a VRRPv3 backup group receives an incorrect VRRP packet.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

You can specify **trap-name** to enable the trap function for one or more events of the VRRP module.

Example

Enable the vrrptrapauthfailure trap.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name vrrp trap-name vrrptrapauthfailure
```

Related Topics

18.6.2 display snmp-agent trap feature-name vrrp all

18.6.15 vrrp advertise send-mode

Function

The **vrrp advertise send-mode** command configures a mode in which the master sends VRRP Advertisement packets in a super-VLAN.

The **undo vrrp advertise send-mode** command restores the default mode in which the master sends VRRP Advertisement packets in a super-VLAN.

By default, the master sends VRRP Advertisement packets to a sub-VLAN that is Up and has the smallest VLAN ID in a super-VLAN.

Format

vrrp advertise send-mode { *sub-vlan-id* | **all** }

undo vrrp advertise send-mode

Parameters

Parameter	Description	Value
sub-vlan-id	Specifies the ID of a sub-VLAN where the master sends VRRP Advertisement packets.	The value is an integer that ranges from 1 to 4094.
all	Indicates that the master sends VRRP Advertisement packets to all sub-VLANs in a super-VLAN.	-

Views

VLANIF interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VRRP group is configured in a super-VLAN, run the **vrrp advertise send-mode** command to configure the master to send VRRP Advertisement packets to a specified sub-VLAN or all sub-VLANs in the super-VLAN. If there are a large number of sub-VLANs in a super-VLAN, to save bandwidth, configure the master to send VRRP Advertisement packets to a specified sub-VLAN.

Prerequisites

A VRRP group has been configured on the VLANIF interface corresponding to the super-VLAN.

Precautions

If **all** is specified, the master broadcasts VRRP Advertisement packets to all sub-VLANs of a super-VLAN, increasing the CPU usage.

Example

Configure the master to broadcast VRRP Advertisement packets to all sub-VLANs in super-VLAN 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] aggregate-vlan
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] vrrp vrid 1 virtual-ip 10.10.10.10
[Huawei-Vlanif100] vrrp advertise send-mode all
```

18.6.16 vrrp arp send-mode simple

Function

The **vrrp arp send-mode simple** command configures the master on a QinQ termination sub-interface to send gratuitous ARP packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag.

The **undo vrrp arp send-mode simple** command restores the default setting.

By default, the master on a QinQ termination sub-interface sends gratuitous ARP packets to the VLAN specified by the outer VLAN tag and all VLANs in the VLAN range specified by the inner VLAN tag.

Format

vrrp arp send-mode simple

undo vrrp arp send-mode simple

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When VRRP is deployed on a QinQ termination sub-interface, the system sends double-tagged ARP packets. If the inner VLAN tag specifies a VLAN range, the system sends ARP packets to all the VLANs in the VLAN range specified by the inner VLAN tag. This ensures that MAC address entries on the downstream device are updated immediately, but causes a heavy burden. The **vrrp arp send-mode simple** command configures the master on a QinQ termination sub-interface to send gratuitous ARP packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag. This prevents excess gratuitous ARP packets from affecting the system.

NOTE

The **vrrp arp send-mode simple** command takes effect in VLANs specified only by the inner VLAN tag but not VLANs specified by the outer VLAN tag. For example, the VLAN ID in the outer tag ranges from 1 to 10 and the VLAN ID in the inner tag ranges from 1 to 10. After the **vrrp arp send-mode simple** command is run, gratuitous ARP packets are transmitted in only VLAN 1 (specified by the inner VLAn tag). A total of 10 gratuitous ARP packets (10 outer VLAN IDs x 1 inner VLAN ID) are sent.

Precautions

The **vrrp arp send-mode simple** command must be executed on a QinQ termination sub-interface.

Example

Configure gigabitethernet0/0/1.1 to send gratuitous ARP packets in VLAN 1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1.1
[Huawei-GigabitEthernet0/0/1.1] qinq termination pe-vid 2 ce-vid 1
[Huawei-GigabitEthernet0/0/1.1] qinq vrrp pe-vid 2 ce-vid 1
[Huawei-GigabitEthernet0/0/1.1] vrrp vrid 1 virtual-ip 10.1.1.1
[Huawei-GigabitEthernet0/0/1.1] vrrp arp send-mode simple
```

18.6.17 vrrp gratuitous-arp timeout

Function

The **vrrp gratuitous-arp timeout** command sets the interval at which the master sends gratuitous ARP packets.

The **undo vrrp gratuitous-arp timeout** command restores the default interval at which the master sends gratuitous ARP packets.

By default, the master sends gratuitous ARP packets every 120s.

Format

vrrp gratuitous-arp timeout *time*

undo vrrp gratuitous-arp timeout

Parameters

Parameter	Description	Value
time	Specifies the interval at which the master sends gratuitous ARP packets.	The value is an integer that ranges from 30 to 1200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an active/standby switchover is performed, the master in a VRRP group periodically sends gratuitous ARP packets to update MAC address entries on the downstream switch.

Precautions

- If a short interval is used, bandwidth resources will be consumed. If a long interval is used, MAC address entries on the downstream switch cannot be updated immediately.
- The interval at which the master sends gratuitous ARP packets must be shorter than the aging time of MAC address entries on user devices.

Set the interval based on actual networking:

- To restore the default interval at which the master sends gratuitous ARP packets, run the **undo vrrp gratuitous-arp timeout** command in the system view.
- If gratuitous ARP packet do not need to be sent, run the **vrrp gratuitous-arp timeout disable** command in the system view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval at which the master sends gratuitous ARP packets to 100 seconds.

```
<Huawei> system-view
[Huawei] vrrp gratuitous-arp timeout 100
```

Related Topics

18.6.18 vrrp gratuitous-arp timeout disable

18.6.18 vrrp gratuitous-arp timeout disable

Function

The **vrrp gratuitous-arp timeout disable** command disables the master from sending gratuitous ARP packets.

By default, the master sends gratuitous ARP packets every 120s.

Format

vrrp gratuitous-arp timeout disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a VRRP group is running properly, the master periodically sends gratuitous ARP packets so that MAC address entries on the downstream switch can be updated immediately. Sending gratuitous ARP packets may cause ARP attacks. If the system requires high security, run the **vrrp gratuitous-arp timeout disable** command to disable the master from sending gratuitous ARP packets.

Precautions

After the **vrrp gratuitous-arp timeout disable** command is executed, the master does not send gratuitous ARP packets. If a VRRP active/standby switchover occurs, MAC address entries on the downstream switch may be not updated immediately, causing data loss on the downstream switch.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the master from sending gratuitous ARP packets.

```
<Huawei> system-view
[Huawei] vrrp gratuitous-arp timeout disable
```

Related Topics

18.6.17 vrrp gratuitous-arp timeout

18.6.19 vrrp recover-delay

Function

The **vrrp recover-delay** command sets the delay before a VRRP group recovers.

The **undo vrrp recover-delay** command restores the default delay before a VRRP group recovers.

By default, the delay before a VRRP group recovers is 0.

Format

vrrp recover-delay *delay-value*

undo vrrp recover-delay

Parameters

Parameter	Description	Value
delay-value	Specifies the delay before a VRRP group recovers.	The value is an integer that ranges from 0 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an interface or a BFD session associated with a VRRP group alternates between Up and Down states, the VRRP group status may flap, causing user traffic loss. To solve this problem, run the **vrrp recover-delay** command to set the delay before a VRRP group recovers. A VRRP group then only responds to the interface or BFD session Up event after the delay expires.

Precautions

- When the device in a VRRP group restarts, the VRRP group status may flap. It is recommended that the delay be set based on actual networking.

 Copyright © Huawei Technologies Co., Ltd.

- After an interface or a BFD session associated with a VRRP group alternates between Up and Down states, the system only records logs and alarms at one time during each delay. This prevents the same alarms from being displayed repeatedly.

Example

Set the delay before a VRRP group recovers to 5 seconds.

```
<Huawei> system-view
[Huawei] vrrp recover-delay 5
```

18.6.20 vrrp smooth-switching timer

Function

The **vrrp smooth-switching timer** command enables VRRP smooth switching and sets the interval contained in VRRP Advertisement packets during VRRP smooth switching.

The **undo vrrp smooth-switching timer** command disables VRRP smooth switching.

By default, VRRP smooth switching is enabled and the interval contained in VRRP Advertisement packets is 100s.

Format

vrrp smooth-switching timer *timer-value*

undo vrrp smooth-switching timer

Parameters

Parameter	Description	Value
timer-value	Specifies the interval contained in VRRP Advertisement packets during VRRP smooth switching. After VRRP smooth switching is enabled on the master, the master sends VRRP Advertisement packets at this interval during an active/standby switchover.	The value is an integer that ranges from 1 to 255, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an active/standby switchover occurs on the master equipped with dual MPUs in a VRRP group, the master and backup may fail to communicate with each other during the switchover. During the switchover, the backup with the highest priority becomes the new master if backups receive no VRRP Advertisement packet after the VRRP Advertisement packet sending interval expires. In this situation, two masters coexist. After the active/standby switchover is complete on the original master, the original master switches to the master because its priority is higher than the new master. During this process, services are switched twice, causing unstable service transmission.

After VRRP smooth switching is enabled on the device equipped with dual MPUs, backups learn the smooth switching time. This implementation extends the timeout interval for receiving VRRP Advertisement packets during VRRP smooth switching, ensuring stability of the VRRP group status.

Prerequisites

The device has been enabled to learn the interval for sending VRRP Advertisement packets using the **vrrp timer-advertise learning enable** command.

Precautions

After receiving VRRP Advertisement packets from the master, the non-master device checks the interval in VRRP Advertisement packets. If the interval in VRRP Advertisement packets is different from the interval of the non-master device, the non-master device learns the interval and adjusts its own interval to be the same as the learned interval.

- *timer-value* must be greater than the interval at which VRRP Advertisement packets are sent. Otherwise, the master may be busy during the switchover and unable to send VRRP Advertisement packets in a timely manner. As a result, a backup switches to the master.
- After the **undo vrrp timer-advertise learning enable** command is executed, VRRP smooth switching is also disabled.

Example

Enable VRRP smooth switching and set the interval contained in VRRP Advertisement packets during VRRP smooth switching to 20 seconds.

```
<Huawei> system-view
[Huawei] vrrp smooth-switching timer 20
```

Related Topics

18.6.21 vrrp timer-advertise learning enable

18.6.21 vrrp timer-advertise learning enable

Function

The **vrrp timer-advertise learning enable** command enables the device to learn the interval for sending VRRP Advertisement packets.

The **vrrp timer-advertise learning disable** command disables the device from learning the interval for sending VRRP Advertisement packets.

 Copyright © Huawei Technologies Co., Ltd.

The **undo vrrp timer-advertise learning enable** command disables the device from learning the interval for sending VRRP Advertisement packets.

By default, the device is enabled to learn the interval for sending VRRP Advertisement packets.

Format

vrrp timer-advertise learning enable

vrrp timer-advertise learning disable

undo vrrp timer-advertise learning enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a link fault triggers an active/standby switchover, VRRP smooth switching is enabled to prevent traffic loss. Before enabling VRRP smooth switching, run the **vrrp timer advertise learning enable** command to enable the device to learn the interval for sending VRRP Advertisement packets. Then non-master devices in the VRRP group will learn the interval at which VRRP Advertisement packets are sent and update their interval to be the same as the learned interval.

Prerequisites

A VRRP group has been created.

Precautions

If VRRP smooth switching has been enabled, running the **undo vrrp timer-advertise learning enable** command disables VRRP smooth switching.

The **undo vrrp timer-advertise learning enable** command is valid only for VRRPv2.

Example

Enable the device to learn the interval for sending VRRP Advertisement packets.

```
<Huawei> system-view
[Huawei] vrrp timer-advertise learning enable
```

18.6.22 vrrp un-check ttl

Function

The **vrrp un-check ttl** command disables the device from checking the TTL value in VRRP Advertisement packets.

The **undo vrrp un-check ttl** command enables the device to check the TTL value in VRRP Advertisement packets.

By default, the system checks the TTL value in VRRP Advertisement packets.

Format

vrrp un-check ttl

undo vrrp un-check ttl

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

The device checks the TTL value in received VRRP Advertisement packets. If the TTL value in a VRRP Advertisement packet is not 255, the device discards the VRRP Advertisement packet and generates a log about the VRRP Advertisement packet error.

On certain networks, especially on a network where the device interworks with non-Huawei devices, valid packets may be discarded if TTL check is enabled. You can configure the device not to check the TTL value in VRRP Advertisement packets.

Example

Disable the router from checking the TTL value in VRRP Advertisement packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp un-check ttl
```

Related Topics

18.6.3 display vrrp

 Copyright © Huawei Technologies Co., Ltd.

18.6.23 vrrp version

Function

The **vrrp version** command configures a VRRP version number.

The **undo vrrp version** command restores the default VRRP version number.

By default, VRRPv2 is used.

Format

vrrp version { **v2** | **v3** }

undo vrrp version

Parameters

Parameter	Description	Value
v2	Indicates that VRRPv2 is used.	-
v3	Indicates that VRRPv3 is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If VRRPv2 and VRRPv3 are used on a network and devices running VRRPv2 need to communicate with devices running VRRPv3, run the **vrrp version** command to specify a VRRP version number.

Precautions

A VRRPv2 group can only send and receive VRRPv2 Advertisement packets. It discards the received VRRPv3 Advertisement packets.

A VRRPv3 group can send and receive both VRRPv2 and VRRPv3 Advertisement packets. You can configure a mode in which VRRPv3 Advertisement packets are sent so that devices running VRRPv2 and VRRPv3 can communicate.

Follow-up Procedure

After VRRPv3 is used, run the **vrrp version-3 send-packet-mode** command in the system view or the **vrrp vrid version-3 send-packet-mode** command in the interface view to configure a mode in which VRRP Advertisement packets are sent.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the VRRP version of the device to VRRPv3.

```
<Huawei> system-view
[Huawei] vrrp version v3
```

Related Topics

18.6.24 vrrp version-3 send-packet-mode

18.6.36 vrrp vrid version-3 send-packet-mode

18.6.24 vrrp version-3 send-packet-mode

Function

The **vrrp version-3 send-packet-mode** command configures a mode in which VRRPv3 Advertisement packets are sent.

The **undo vrrp version-3 send-packet-mode** command restores the default mode in which VRRPv3 Advertisement packets are sent.

By default, the mode is **v3-only**.

Format

vrrp version-3 send-packet-mode { **v2-only** | **v3-only** | **v2v3-both** }

undo vrrp version-3 send-packet-mode

Parameters

Parameter	Description	Value
v2-only	Indicates that the device sends only VRRPv2 Advertisement packets.	-
v3-only	Indicates that the device sends only VRRPv3 Advertisement packets.	-
v2v3-both	Indicates that the device sends both VRRPv2 and VRRPv3 Advertisement packets.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

If devices in a VRRP group use different VRRP version numbers, the VRRP group may fail to negotiate the status. This is because a VRRPv2-enabled device can only receive VRRPv2 Advertisement packets and discards the received VRRPv3 Advertisement packets. You can configure a mode in which VRRP Advertisement packets are sent so that devices running VRRPv2 and VRRPv3 in the VRRP group can negotiate the status.

Precautions

- Only VRRPv3 supports this command.
- If both the **vrrp version-3 send-packet-mode** and **vrrp vrid version-3 send-packet-mode** commands are run, the **vrrp vrid version-3 send-packet-mode** command takes precedence over the **vrrp version-3 send-packet-mode** command.

NOTE

If a large number of VRRP groups are configured, **v2v3-both** is not recommended.

Example

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only**.

```
<Huawei> system-view
[Huawei] vrrp version-3 send-packet-mode v2-only
```

Related Topics

18.6.23 vrrp version

18.6.25 vrrp virtual-ip ping enable

Function

The **vrrp virtual-ip ping enable** command enables the master to respond to ping packets sent to a virtual IP address.

The **vrrp virtual-ip ping disable** command disables the master from responding to ping packets sent to a virtual IP address.

The **undo vrrp virtual-ip ping enable** command disables the master from responding to ping packets sent to a virtual IP address.

By default, the master is enabled to respond to ping packets sent to a virtual IP address.

Format

vrrp virtual-ip ping enable

vrrp virtual-ip ping disable

undo vrrp virtual-ip ping enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The router allows user devices to ping a virtual IP address to serve the following purposes:

- Monitors the operating status of the master in a VRRP group.
- Monitors communication between a user device and a network connected by a default gateway using the virtual IP address.

Precautions

If the ping to a virtual IP address is enabled, a device on an external network can ping a virtual IP address. This imposes the router to ICMP-based attacks.

After the **undo vrrp virtual-ip ping enable** command is run to disable the master from responding to ping packets sent to a virtual IP address, the host route for the virtual IP address is deleted. As a result, services transmitted using the host route are interrupted. For example, after the **undo vrrp virtual-ip ping enable** command is run, the GRE tunnel with the source IP address of a virtual IP address goes Down.

Example

Disable the master from responding to ping packets.

```
<Huawei> system-view
[Huawei] undo vrrp virtual-ip ping enable
```

18.6.26 vrrp virtual-ip route-advertise disable

Function

The **vrrp virtual-ip route-advertise disable** command disables a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

The **undo vrrp virtual-ip route-advertise disable** command enables a dynamic routing protocol to advertise routes generated by the virtual IP address of a VRRP group.

By default, a dynamic routing protocol is enabled to advertise routes generated by the virtual IP address of a VRRP group.

Format

vrrp virtual-ip route-advertise disable [**isis** | **ospf** | **rip**] *

undo vrrp virtual-ip route-advertise disable

Parameters

None

Parameter	Description	Value
isis	Disables IS-IS from advertising the routes generated by the virtual IP address of a VRRP group.	-
ospf	Disables OSPF from advertising the routes generated by the virtual IP address of a VRRP group.	-
rip	Disables RIP from advertising the routes generated by the virtual IP address of a VRRP group.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Direct routes generated by the virtual IP address of a VRRP group can be imported to a dynamic routing protocol. By default, these routes are advertised by a dynamic routing protocol to neighbors. In practice, a large number of routes may be generated by the virtual IP address of a VRRP group. If a dynamic routing protocol imports theses routes and advertises them to neighbors, there is a heavy burden on network devices and network performance deteriorates. You can run the **vrrp virtual-ip route-advertise disable** command to disable a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

Prerequisites

- A virtual IP address has been configured for a VRRP group.
- A dynamic routing protocol has imported routes generated by the virtual IP address of the VRRP group.

Precautions

After the **vrrp virtual-ip route-advertise disable** command is executed, routes generated by virtual IP addresses of all VRRP groups cannot be advertised by a dynamic routing protocol.

On a network that has MPLS LDP configured, the peer device cannot receive routes generated by the virtual IP address of a VRRP group, so the peer device cannot generate the LSP to the virtual IP address of the VRRP group.

The **vrrp virtual-ip route-advertise disable** command is only valid for OSPF and IS-IS.

 Copyright © Huawei Technologies Co., Ltd.

If routes generated by the virtual IP address of a VRRP group must be advertised by a dynamic routing protocol, do not run the **vrrp virtual-ip route-advertise disable** command.

Example

Disable a dynamic routing protocol from advertising routes generated by the virtual IP address of a VRRP group.

```
<Huawei> system-view
[Huawei] vrrp virtual-ip route-advertise disable
```

18.6.27 vrrp vrid authentication-mode

Function

The **vrrp vrid authentication-mode** command configures an authentication mode and an authentication key for a VRRP group.

The **undo vrrp vrid authentication-mode** command cancels the authentication mode and authentication key for a VRRP group.

By default, a VRRP group uses non-authentication.

Format

vrrp vrid *virtual-router-id* **authentication-mode** { **simple** { *key* | **plain** *key* | **cipher** *cipher-key* } | **md5** *md5-key* }

undo vrrp vrid *virtual-router-id* **authentication-mode**

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
simple	Indicates simple authentication.	-
key	Specifies the authentication key in simple authentication mode.	The value is a string of 1 to 8 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
plain *key*	Specifies the authentication key in plain text authentication mode. **NOTE** If **plain** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	The value is a string of 1 to 8 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
cipher *cipher-key*	Specifies the authentication key in cipher text authentication mode.	The value is a string of 1 to 8 case-sensitive characters in plain text or a string of 32 or 48 case-sensitive characters in cipher text, without spaces. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** Ciphertext password with various lengths configured in an earlier version are also supported in the existing version.
md5 *md5-key*	Specifies the authentication key in MD5 authentication mode.	The value is a string of 1 to 8 case-sensitive characters in plain text or a string of 24 or 32 or 48 case-sensitive characters in cipher text, without spaces. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** Ciphertext password with various lengths configured in an earlier version are also supported in the existing version.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To ensure security, you are advised to use MD5 as the authentication algorithm of VRRP.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To be compatible with VRRP and interwork with other devices, VRRP provides simple authentication and MD5 authentication. The **vrrp vrid authentication-mode** command configures an authentication mode and an authentication key for a VRRP group.

Prerequisites

A VRRP group has been configured on a specified interface.

Precautions

Devices in a VRRP group must be configured with the same authentication mode and authentication key; otherwise, the VRRP group cannot negotiate the Master and Backup states.

Example

Set the authentication mode of the VRRP group with VRID 2 on GE2/0/0 to MD5 authentication and set the authentication key to **Huawei-1**.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] vrrp vrid 2 virtual-ip 10.1.1.1
[Huawei-GigabitEthernet2/0/0] vrrp vrid 2 authentication-mode md5 Huawei-1
```

Related Topics

18.6.37 vrrp vrid virtual-ip

18.6.28 vrrp vrid preempt-mode disable

Function

The **vrrp vrid preempt-mode disable** command configures the device in a VRRP group in non-preemption mode.

The **undo vrrp vrid preempt-mode** command restores the default preemption mode.

By default, the device uses the immediate preemption mode.

Format

vrrp vrid *virtual-router-id* **preempt-mode disable**

undo vrrp vrid *virtual-router-id* **preempt-mode**

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device with higher priority in a VRRP group to be the master, set the preemption mode on the device. In non-preemption mode, as long as the master is working properly, the backup with higher priority cannot be the master.

NOTE

When non-preemption is disabled, the preemption delay is restored to be 0 seconds immediately.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Example

Configure VRRP group 1 in non-preemption mode.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.2
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 preempt-mode disable
```

Related Topics

18.6.29 vrrp vrid preempt-mode timer delay

18.6.37 vrrp vrid virtual-ip

 Copyright © Huawei Technologies Co., Ltd.

18.6.29 vrrp vrid preempt-mode timer delay

Function

The **vrrp vrid preempt-mode timer delay** command sets the preemption delay for the device in a VRRP group.

The **undo vrrp vrid preempt-mode timer delay** command restores the default preemption delay for the device in a VRRP group.

By default, the preemption delay is 0 seconds.

Format

vrrp vrid *virtual-router-id* **preempt-mode timer delay** *delay-value*

undo vrrp vrid *virtual-router-id* **preempt-mode timer delay**

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
delay *delay-value*	Specifies the preemption delay.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the backup in a VRRP group does not receive VRRP Advertisement packets from the master within a specified period of time, the backup becomes the master. On an unstable network, even if the master is working properly, the backup may not receive packets from the master because of network congestion. In this case, the VRRP group status may flap and traffic is lost. To prevent frequent switching of the VRRP group status, run the **vrrp vrid preempt-mode timer delay** command to set the preemption delay so that the backup becomes the master only after the delay expires.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- This command takes effect only when the device can receive VRRP heartbeat packets and the priority in these packets is lower than the priority of the device in a VRRP group.
- You are advised to set the preemption delay of the backup in a VRRP group to 0, configure the master in preemption mode, and set the preemption delay to be longer than 15s. These settings allow a period of time for status synchronization between the uplink and downlink on devices in a VRRP group on an unstable network. If the preceding settings are not used, two masters coexist and user devices may learn an incorrect master address. As a result, traffic is interrupted.
  - The preemption delay refers to the delay before the backup switches to the master. Therefore, the IP address owner is irrelevant to the preemption delay. After the IP address owner recovers, it becomes the master immediately, without any delay.
  - On a stable network, a short preemption delay is recommended. When the master is faulty, the backup with the highest priority can rapidly switch to the master. This prevents traffic loss. On an unstable network, a long preemption delay is recommended. This prevents traffic loss caused by frequent switching of the VRRP group status.

Example

Set the preemption delay of VRRP group 1 to 5 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] vrrp vrid 1 preempt-mode timer delay 5
```

Related Topics

18.6.28 vrrp vrid preempt-mode disable

18.6.30 vrrp vrid priority

Function

The **vrrp vrid priority** command sets the priority of the device in a VRRP group.

The **undo vrrp vrid priority** command restores the default priority of the device in a VRRP group.

By default, the priority of the device in a VRRP group is 100.

Format

vrrp vrid *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
priority *priority-value*	Specifies the priority of the device in a VRRP group.	The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the device in a VRRP group as the default gateway, run the **vrrp vrid priority** command to specify the highest priority for the device so that the device can become the master.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed to create a VRRP group.

Precautions

- Priority 0 is reserved in the system. Priority 255 is reserved for the IP address owner.
- When devices in a VRRP group have the same priority, the device that first changes to master state becomes the master. If devices attempt to be the master simultaneously, the device where the interface with the largest IP address is located becomes the master.

Example

Set the priority of the router in VRRP group 1 to 150.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.2
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 priority 150
```

Related Topics

18.6.37 vrrp vrid virtual-ip

18.6.31 vrrp vrid timer advertise

Function

The **vrrp vrid timer advertise** command sets the interval at which the master sends VRRP Advertisement packets.

The **undo vrrp vrid timer advertise** command restores the default interval at which the master sends VRRP Advertisement packets.

By default, the master sends VRRP Advertisement packets every 1 second.

Format

vrrp vrid *virtual-router-id* **timer advertise** *advertise-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
advertise *advertise-interval*	Specifies the interval at which the master sends VRRP Advertisement packets.	The value is an integer, in seconds. In VRRPv2, the value ranges from 1 to 255. In VRRPv3, the value ranges from 1 to 40.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP group sends VRRP Advertisement packets to backups at intervals to notify that it is working properly. If the backup with the highest priority does not receive any VRRP Advertisement packets from the master at the specified interval, it considers the master faulty and becomes the master. The **vrrp vrid timer advertise** command sets the interval at which the master sends VRRP Advertisement packets.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Precautions

If a longer interval is used, backups in the same VRRP group cannot detect the fault on the master in a timely manner, causing packet loss. If a shorter interval is used, system resources are occupied. In addition, when network traffic is heavy or the network is unstable, backups may not receive packets after the Master_Down_Interval timer expires. As a result, the VRRP group status is incorrectly switched. Set the interval based on actual networking.

Example

Set the interval at which the master in VRRP group 1 sends VRRP Advertisement packets to 5 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.2
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 timer advertise 5
```

Related Topics

18.6.37 vrrp vrid virtual-ip

18.6.32 vrrp vrid track bfd-session

Function

The **vrrp vrid track bfd-session** command associates a VRRP group with a BFD session.

The **undo vrrp vrid track bfd-session** command disassociates a VRRP group from a BFD session.

By default, a VRRP group is not associated with a BFD session.

Format

vrrp vrid *virtual-router-id* **track bfd-session** { *bfd-session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track bfd-session** [*bfd-session-id* | **session-name** *bfd-configure-name*]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
bfd-session-id	Specifies the local discriminator of the monitored BFD session.	The value is an integer that ranges from 1 to 8191.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
session-name *bfd-configure-name*	Specifies the name of the monitored BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
increased *value-increased*	Specifies the value by which the priority increases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored BFD session becomes Down, the VRRP priority decreases by 10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between a VRRP group and a BFD session implements the following functions:

1. Rapid active/standby switchover: When the link of a VRRP group or the master is faulty, the backup becomes the master after a certain period of time (second level), causing packet loss. You can associate the VRRP group with a BFD session on the backup so that the BFD session can rapidly detect communication faults of the VRRP group. When the BFD session detects a fault, it notifies the VRRP group that the priority of the backup needs to be increased. Then an active/standby switchover is triggered immediately. This millisecond-level switchover reduces traffic loss. When the monitored BFD session recovers, the original priority of the device in the VRRP group is restored.
2. Monitoring the uplink: Because VRRP cannot detect faults on the uplink of a VRRP group, services are interrupted. You can associate the VRRP group with

a BFD session on the master so that the BFD session monitors the uplink status of the master. When the BFD session detects a fault on the uplink, it notifies the VRRP group that the priority of the master needs to be decreased. Then an active/standby switchover is triggered immediately. This reduces the impact of the uplink fault on service forwarding. When the monitored BFD session recovers, the original priority of the device in the VRRP group is restored.

Prerequisites

A VRRP group has been created and a static BFD session or a static BFD session with automatically negotiated discriminators has been created.

Precautions

After a VRRP group is associated with a BFD session, the BFD session type cannot be modified. Before deleting the BFD session type, you must delete all original configurations.

After a VRRP group is associated with a BFD session, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored BFD session becomes Down.

Multiple VRRP groups can monitor a BFD session, and a VRRP group can monitor a maximum of eight BFD sessions simultaneously.

NOTE

When associating a VRRP group with a BFD session, note the following points:

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If an IP address owner exists in the VRRP group, the VRRP group cannot monitor the BFD session.
- If **session-name** *bfd-configure-name* is specified, the VRRP group can be bound to only the static BFD session with automatically negotiated discriminators.
- If *bfd-session-id* is specified, the VRRP group can be bound to only the static BFD session.

Example

Configure VRRP group 1 to monitor the BFD session with local discriminator 1 on GE1/0/0.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd abc bind peer-ip 10.1.1.1 interface gigabitethernet 1/0/0
[Huawei-bfd-session-abc] discriminator local 1
[Huawei-bfd-session-abc] discriminator remote 2
[Huawei-bfd-session-abc] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.12
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session 1 reduced 40
```

Configure VRRP group 1 to monitor the BFD session **hello** on GE1/0/0.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
```

```
[Huawei] bfd hello bind peer-ip 10.2.1.1 interface gigabitethernet 1/0/0 source-ip 10.2.1.2 auto
[Huawei-bfd-session-hello] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.2.1.12
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 track bfd-session session-name hello reduced 40
```

18.6.33 vrrp vrid track interface

Function

The **vrrp vrid track interface** command associates a VRRP group with an interface.

The **undo vrrp vrid track interface** command disassociates a VRRP group from an interface.

By default, a VRRP group is not associated with an interface.

Format

vrrp vrid *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface monitored by a VRRP group. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. **NOTE** A VRRP backup group can track Layer 2 and Layer 3 interfaces. ● If the tracked interface is a Layer 2 interface, the VRRP backup group tracks the physical status of the Layer 2 interface and changes its own priority based on the tracked physical status. ● If the tracked interface is a Layer 3 interface, the VRRP backup group tracks the protocol status of the Layer 3 interface and changes its own priority based on the tracked protocol status.	-
increased *value-increased*	Specifies the value by which the priority increases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored interface goes Down, the VRRP priority of the device decreases by 10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VRRP can only detect the status change of the interface on which a VRRP group is configured. VRRP cannot detect faults on the uplink interface, causing service interruption. You can run the **vrrp vrid track interface** command to associate a VRRP group with a device interface not in the VRRP group. When the monitored interface becomes Down, the priority of the device is adjusted and an active/standby switchover is triggered. Therefore, services can be forwarded correctly. When the status of the monitored interface recovers, the original priority of the device in the VRRP group is restored.

Prerequisites

The **vrrp vrid virtual-ip** command has been executed on an interface to create a VRRP group.

Precautions

After a VRRP group is associated with an interface, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored interface becomes Down.

NOTE

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If the device is the IP address owner (the virtual router IP address is used as the actual interface address), you cannot associate a VRRP group with an interface.
- Multiple VRRP groups can monitor an interface, and a VRRP group can monitor a maximum of 8 interfaces simultaneously.

Example

Associate VRRP group 1 with GE2/0/0 and set **reduced** *value-reduced* to 50 when GE2/0/0 becomes Down.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] vrrp vrid 1 virtual-ip 10.1.1.1
[Huawei-GigabitEthernet2/0/0] vrrp vrid 1 track interface gigabitethernet 1/0/0 reduced 50
```

Related Topics

18.6.37 vrrp vrid virtual-ip

18.6.34 vrrp vrid track ip route

Function

The **vrrp vrid track ip route** command associates a VRRP group with a route.

The **undo vrrp vrid track ip route** command disassociates a VRRP group from a route.

By default, a VRRP group is not associated with a route.

Format

vrrp vrid *virtual-router-id* **track ip route** *ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*] [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track ip route** [*ip-address* { *mask-address* | *mask-length* } [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
ip-address	Specifies the destination address of the monitored route.	The value is in dotted decimal notation.
mask-address	Specifies the mask of the destination address of the monitored route.	The value is in dotted decimal notation.
mask-length	Specifies the mask length of the destination address of the monitored route.	The value is an integer that ranges from 0 to 32.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
reduced *value-reduced*	Specifies the value by which the master' priority decreases if the monitored route is withdrawn or becomes inactive.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, the master' priority decreases by 10 if the associated route is withdrawn or becomes inactive.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve device reliability, two user gateways are configured to work in master/backup mode, and VRRP is enabled on these gateways to determine their Master and Backup states. Although a VRRP group has been configured, access devices may not detect route changes caused by the faulty uplink or network topology change. Consequently, data traffic is lost.

You can associate a VRRP group with a route for forwarding uplink traffic. When the route is withdrawn or becomes inactive, the master' priority is adjusted and an active/standby switchover is performed. When the status of the monitored route recovers, the original priority of the master in the VRRP group is restored.

Pre-configuration Tasks

A VRRP group and a routing protocol such as OSPF, BGP, or IS-IS have been configured.

Precautions

The VRRP group to be associated with a route cannot contain an IP address owner.

The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and non-0 on the master.

When associating a VRRP group with a route in a VPN instance, note the following points:

- If the VPN instance does not exist, association between the VRRP group and the VPN route cannot work.
- If the VPN instance is deleted after the VRRP group is associated with the VPN route, association between the VRRP group and the VPN route is also deleted.

Example

Configure VRRP group 1 to monitor the route on 10.2.1.0, and set the value by which the master' priority decreases if the monitored route is withdrawn or becomes inactive to 20.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.1.1.12
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 track ip route 10.2.1.0 24 reduced 20
```

 Copyright © Huawei Technologies Co., Ltd.

18.6.35 vrrp vrid track nqa

Function

The **vrrp vrid track nqa** command associates a VRRP group with an NQA test instance to implement a rapid active/standby switchover.

The **undo vrrp vrid track nqa** command disassociates a VRRP group from an NQA test instance.

By default, a VRRP group is not associated with an NQA test instance.

Format

vrrp vrid *virtual-router-id* **track nqa** *admin-name test-name* [**reduced** *value-reduced*]

undo vrrp vrid *virtual-router-id* **track nqa** [*admin-name test-name*]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
admin-name	Specifies the administrator name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
reduced *value-reduced*	Specifies the value by which the master's priority reduces if the NQA test instance detects that the uplink is unavailable.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, the master's priority value decreases by 10 if the associated NQA test instance detects that the uplink is unavailable.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve device reliability, two user gateways are configured to work in master/backup mode, and VRRP is enabled on these gateways to determine their Master and Backup states. Although a VRRP group has been configured, the uplink may be unreachable and access devices may not detect the faulty uplink. Consequently, data traffic is lost.

You can associate a VRRP group with an NQA test instance to solve this problem. The NQA test instance periodically sends ICMP packets to detect whether the destination IP address of the uplink is reachable. When the destination IP address is unreachable, the NQA test instance reports the fault to the associated VRRP group and instructs the VRRP group to adjust the priority, implementing an active/standby switchover. When the status of the monitored NQA test instance recovers, the original priority of the master in the VRRP group is restored.

Prerequisites

An NQA test instance of ICMP has been configured.

Precautions

- The master and backup in the VRRP group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and non-0 on the master.
- The VRRP group to be associated with a route cannot contain an IP address owner.
- The VRRP group can only be associated with an NQA test instance of ICMP.
- A VRRP group can monitor a maximum of eight NQA test instances.

Example

Associate a VRRP group with NQA test instance **user user1** on GE0/0/1 and set **reduced** *value-reduced* to 20 when the destination IP address is unreachable.

```
<Huawei> system-view
[Huawei] nqa test-instance user user1
[Huawei-nqa-user-user1] test-type icmp
[Huawei-nqa-user-user1] destination-address ipv4 10.1.1.1
[Huawei-nqa-user-user1] frequency 10
[Huawei-nqa-user-user1] probe-count 2
[Huawei-nqa-user-user1] start now
[Huawei-nqa-user-user1] quit
[Huawei] interface gigabitethernet 0/0/1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-GigabitEthernet0/0/1] vrrp vrid 1 virtual-ip 10.2.1.12
[Huawei-GigabitEthernet0/0/1] vrrp vrid 1 track nqa user user1 reduced 20
```

18.6.36 vrrp vrid version-3 send-packet-mode

Function

The **vrrp vrid version-3 send-packet-mode** command configures a mode in which VRRPv3 Advertisement packets are sent on an interface.

The **undo vrrp vrid version-3 send-packet-mode** command restores the default mode.

By default, VRRPv3 Advertisement packets are sent in **v3-only** mode.

Format

vrrp vrid *virtual-router-id* **version-3 send-packet-mode** { **v2-only** | **v3-only** | **v2v3-both** }

undo vrrp vrid *virtual-router-id* **version-3 send-packet-mode**

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.
v2-only	Indicates that only VRRPv2 Advertisement packets are sent.	-
v3-only	Indicates that only VRRPv3 Advertisement packets are sent.	-
v2v3-both	Indicates that both VRRPv2 and VRRPv3 Advertisement packets are sent.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If devices in a VRRP group use different VRRP version numbers, the VRRP group may fail to negotiate the status. This is because a VRRPv2-enabled device can only receive VRRPv2 Advertisement packets and discards the received VRRPv3 Advertisement packets. You can set the mode in which VRRP Advertisement

packets are sent on the VRRPv3-enabled device so that the VRRPv2-enabled and VRRPv3-enabled devices can negotiate the status.

Precautions

- Only VRRPv3 supports this command.
- If the **vrrp version-3 send-packet-mode** command is used in the system view and interface view simultaneously, the configuration in the interface view takes effect.

NOTE

If a large number of VRRP groups are configured, **v2v3-both** is not recommended.

Example

Set the mode in which VRRPv3 Advertisement packets are sent to **v2-only** on GE1/0/0.

```
<Huawei> system-view
[Huawei] vrrp version v3
[Huawei] vrrp version-3 send-packet-mode v2-only
Warning: The globally configured packet sending mode will take effect for every VRRP backup
group.Continue?[Y/N]:y
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 24 version-3 send-packet-mode v2-only
```

Related Topics

18.6.23 vrrp version

18.6.37 vrrp vrid virtual-ip

Function

The **vrrp vrid virtual-ip** command creates a VRRP group and assigns a virtual IP address to the group.

The **undo vrrp vrid virtual-ip** command deletes the virtual IP address of a VRRP group.

By default, no VRRP group is created.

Format

vrrp vrid *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** *virtual-address*]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP group.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
virtual-ip *virtual-address*	Specifies the virtual IP address of a VRRP group.	The value is in dotted decimal notation.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, hosts use the default gateway to communicate with external networks. As value-added services such as IPTV or video conferencing services are widely deployed, hosts may fail to communicate with external networks if the default gateway fails. Configuring dynamic routing protocols such as RIP, OSPF, or ICMP can improve system reliability. However, it is difficult to configure dynamic routing protocols and some hosts may not support dynamic routing protocols. VRRP virtualizes multiple routing devices into a virtual router without changing the networking. The virtual router IP address is configured as the default gateway address.

If users on a network have the same reliability requirements, configure multiple virtual IP addresses for a VRRP group. By doing this, one virtual IP address serves one separate user group, and the default gateway address remains consistent regardless of changes in VRRP device locations. A VRRP group can be assigned a maximum of 16 virtual IP addresses.

Precautions

If all the virtual IP addresses in a VRRP group are deleted, the VRRP group is deleted automatically.

After the **vrrp vrid virtual-ip** command is run on an interface, when the ARP entries learned by the interface are aged, the device sends ARP aging probe packets with the source IP address being the interface's IP address. The virtual IP address of the interface is not used as the source IP address.

When VRRP and static ARP are configured simultaneously, note the following points:

- When VRRP is configured on a dot1q termination sub-interface, QinQ termination sub-interface, or VLANIF interface, the IP address corresponding to the dot1q termination sub-interface, QinQ termination sub-interface, or VLANIF interface in a static ARP entry cannot be set to the virtual IP address of a VRRP group. Otherwise, services cannot be forwarded between devices. For example, if a static ARP entry contains IP address 10.1.1.1, the IP address 10.1.1.1 cannot be used as the virtual IP address.

 Copyright © Huawei Technologies Co., Ltd.

- When VRRP is configured on a dot1q termination sub-interface, QinQ termination sub-interface, or VLANIF interface, the virtual IP address of a VRRP group cannot be used as the IP address corresponding to the dot1q termination sub-interface, QinQ termination sub-interface, or VLANIF interface in a static ARP entry. Otherwise, services cannot be forwarded between devices. For example, if the VRRP group uses virtual IP address 10.1.1.1, the IP address 10.1.1.1 cannot be used in a static ARP entry.

NOTE

- VRRP groups must use different virtual IP addresses.
- Two devices in a VRRP group must be configured with the same VRID.
- VRRP groups on different interfaces of a device can be configured with the same VRID.
- A virtual IP address must be different from the IP address of a user host. If the user host IP address is the same as the virtual IP address, all packets on the local network segment are sent to the user host. As a result, data of this network segment cannot be forwarded correctly.

Example

Create a VRRP group on GE 1/0/0 with ID 1 and virtual IP address 10.10.10.10.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp vrid 1 virtual-ip 10.10.10.10
```

18.6.38 vrrp6 nd send-mode simple

Function

The **vrrp6 nd send-mode simple** command configures the master on a QinQ termination sub-interface to send ND packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag.

The **undo vrrp6 nd send-mode simple** command cancels the configuration.

By default, the master on a QinQ termination sub-interface sends ND packets to the VLAN specified by the outer VLAN tag and all VLANs in the VLAN range specified by the inner VLAN tag.

Format

vrrp6 nd send-mode simple

undo vrrp6 nd send-mode simple

Parameters

None

Views

Ethernet sub-interface view, GE sub-interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When VRRP6 is deployed on a QinQ termination sub-interface, the system sends double-tagged ND packets. If the inner VLAN tag specifies a VLAN range, the system sends ND packets to all the VLANs in the VLAN range specified by the inner VLAN tag. This ensures that MAC address entries on the downstream device are updated immediately, but causes a heavy burden. The **vrrp6 nd send-mode simple** command configures the master on a QinQ termination sub-interface to send ND packets to the VLAN specified by the outer VLAN tag and the first VLAN in the VLAN range specified by the inner VLAN tag. This prevents excess ND packets from affecting the system.

NOTE

The **vrrp6 nd send-mode simple** command affects only the inner VLAN tag. For example, both the inner and outer VLAN tags specify the VLAN range 1 to 10. After the **vrrp6 nd send-mode simple** command is executed, ND packets are sent in VLAN 1.

Precautions

The **vrrp6 nd send-mode simple** command must be executed on a QinQ termination sub-interface.

Example

Configure the master to send gratuitous ND packets in VLAN 1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0.1
[Huawei-GigabitEthernet1/0/0.1] qinq termination pe-vid 2 ce-vid 1
[Huawei-GigabitEthernet1/0/0.1] qinq vrrp pe-vid 2 ce-vid 1
[Huawei-GigabitEthernet1/0/0.1] ipv6 enable
[Huawei-GigabitEthernet1/0/0.1] ipv6 address auto link-local
[Huawei-GigabitEthernet1/0/0.1] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet1/0/0.1] vrrp6 nd send-mode simple
```

18.6.39 vrrp6 un-check hop-limit

Function

The **vrrp6 un-check hop-limit** command disables the device from checking the TTL value in VRRP6 Advertisement packets.

The **undo vrrp6 un-check hop-limit** command enables the device to check the TTL value in VRRP6 Advertisement packets.

By default, the system checks the TTL value in VRRP6 Advertisement packets.

Format

vrrp6 un-check hop-limit

undo vrrp6 un-check hop-limit

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

As defined by RFC, the device checks the TTL value in received VRRP6 Advertisement packets. If the TTL value of a VRRP6 Advertisement packet is not 255, the device discards the packet.

On certain networks, especially on a network where the device interworks with non-Huawei devices, valid packets may be discarded if TTL check is enabled. You can configure the device not to check the TTL value in VRRP6 Advertisement packets.

Example

Disable the device from checking the TTL value in VRRP6 Advertisement packets.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 un-check hop-limit
```

Related Topics

18.6.48 vrrp6 vrid virtual-ip

18.6.40 vrrp6 vrid preempt-mode disable

Function

The **vrrp6 vrid preempt-mode disable** command configures the device in a VRRP6 group in non-preemption mode.

The **undo vrrp6 vrid preempt-mode** command restores the default preemption mode.

By default, the device uses the immediate preemption mode.

Format

vrrp6 vrid *virtual-router-id* **preempt-mode disable**

undo vrrp6 vrid *virtual-router-id* **preempt-mode**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device with higher priority in a VRRP6 group to be the master, set the preemption mode on the device. In non-preemption mode, as long as the master is working properly, the backup with higher priority cannot be the master.

NOTE

When non-preemption is disabled, the preemption delay is restored to be 0 seconds immediately.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Example

Configure VRRP6 group 1 in non-preemption mode.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 preempt-mode disable
```

Related Topics

18.6.41 vrrp6 vrid preempt-mode timer delay

18.6.48 vrrp6 vrid virtual-ip

18.6.41 vrrp6 vrid preempt-mode timer delay

Function

The **vrrp6 vrid preempt-mode timer delay** command sets the preemption delay for the device in a VRRP6 group.

The **undo vrrp6 vrid preempt-mode timer delay** command restores the default preemption delay for the device in a VRRP6 group.

By default, the preemption delay is 0 seconds, indicating immediate preemption.

Format

vrrp6 vrid *virtual-router-id* **preempt-mode timer delay** *delay-value*

undo vrrp6 vrid *virtual-router-id* **preempt-mode timer delay**

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
delay *delay-value*	Specifies the preemption delay.	The value is an integer that ranges from 0 to 3600, in seconds. The default value is 0.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the backup in a VRRP6 group does not receive VRRP6 Advertisement packets from the master within a specified period of time, the backup becomes the master. On an unstable network, even if the master is working properly, the backup may not receive packets from the master because of network congestion. In this case, the VRRP6 group status may flap and traffic is lost. To prevent frequent switching of the VRRP6 group status, run the **vrrp6 vrid preempt-mode timer delay** command to set the preemption delay so that the backup becomes the master only after the delay expires.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed to create a VRRP6 group.

Precautions

You are advised to set the preemption delay of the backup in a VRRP6 group to 0, configure the master in preemption mode, and set the preemption delay to be longer than 15s. These settings allow a period of time for status synchronization between the uplink and downlink on devices on an unstable network. If the

 Copyright © Huawei Technologies Co., Ltd.

preceding settings are not used, two masters coexist and user devices may learn an incorrect master address. As a result, traffic is interrupted.

- The preemption delay refers to the delay before the backup switches to the master. Therefore, the IP address owner is irrelevant to the preemption delay. After the IP address owner recovers, it becomes the master immediately without a delay.
- On a stable network, a short preemption delay is recommended. When the master is faulty, the backup can rapidly switch to the master. This prevents traffic loss. On an unstable network, a long preemption delay is recommended. This prevents traffic loss caused by frequent switching of the VRRP6 group status.

Example

Set the preemption delay of VRRP6 group 1 to 10 seconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 preempt-mode timer delay 10
```

18.6.42 vrrp6 vrid priority

Function

The **vrrp6 vrid priority** command sets the priority of the device in a VRRP6 group.

The **undo vrrp6 vrid priority** command restores the default priority of the device in a VRRP6 group.

By default, the priority of the device in a VRRP6 group is 100.

Format

vrrp6 vrid *virtual-router-id* **priority** *priority-value*

undo vrrp6 vrid *virtual-router-id* **priority**

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
priority *priority-value*	Specifies the priority of the device in a VRRP6 group.	The value is an integer that ranges from 1 to 254. A larger value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the device in a VRRP6 group as the default gateway, run the **vrrp6 vrid priority** command to specify the highest priority for the device so that the device can become the master.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed to create a VRRP6 group.

Precautions

- Priority 0 is reserved in the system. Priority 255 is reserved for the IP address owner.
- When devices in a VRRP6 group have the same priority, the device that first changes to master state becomes the master. If devices attempt to be the master simultaneously, the device where the interface with the largest IP address is located becomes the master.

Example

Set the priority of the router in VRRP6 group 2 to 120.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 2 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 2 priority 120
```

18.6.43 vrrp6 vrid timer advertise

Function

The **vrrp6 vrid timer advertise** command sets the interval at which the master sends VRRP6 Advertisement packets.

The **undo vrrp6 vrid timer advertise** command restores the default interval at which the master sends VRRP6 Advertisement packets.

By default, the master sends VRRP6 Advertisement packets every 1 second.

Format

vrrp6 vrid *virtual-router-id* **timer advertise** *advertise-interval*

undo vrrp6 vrid *virtual-router-id* **timer advertise**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
advertise *advertise-interval*	Specifies the interval at which the master sends VRRP6 Advertisement packets.	The value is an integer that ranges from 100 to 4095, in centiseconds.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The master in a VRRP6 group sends VRRP6 Advertisement packets to backups at intervals to notify that it is working properly. If the backup with the highest priority does not receive any VRRP6 Advertisement packets from the master at the specified interval (usually, three times the interval for sending VRRP6 Advertisement packets), it considers the master faulty and becomes the master. The **vrrp6 vrid timer advertise** command sets the interval at which the master sends VRRP6 Advertisement packets.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Precautions

If a longer interval is used, backups in the same VRRP6 group cannot detect the fault on the master in a timely manner, causing packet loss. If a shorter interval is used, system resources are occupied. In addition, when network traffic is heavy or the network is unstable, backups may not receive packets after the Master_Down_Interval timer expires. As a result, the VRRP6 group status is incorrectly switched. Set the interval based on actual networking.

NOTE

- For VRRP for IPv4, set the same interval for sending VRRP Advertisement packets for members in a VRRP group to prevent multiple masters in the VRRP group.
- For VRRP for IPv6, even if you set different intervals for sending VRRP Advertisement packets for members in a VRRP6 group, there is only one master in a VRRP6 group.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval at which the master in VRRP6 group 1 sends VRRP6 Advertisement packets to 200 centiseconds.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 timer advertise 200
```

Related Topics

18.6.48 vrrp6 vrid virtual-ip

18.6.44 vrrp6 vrid track bfd-session

Function

The **vrrp6 vrid track bfd-session** command associates a VRRP6 group with a BFD session.

The **undo vrrp6 vrid track bfd-session** command disassociates a VRRP6 group from a BFD session.

By default, a VRRP6 group is not associated with a BFD session.

Format

vrrp6 vrid *virtual-router-id* **track bfd-session** { *session-id* | **session-name** *bfd-configure-name* } [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track bfd-session** [*session-id* | **session-name** *bfd-configure-name*]

Parameters

Parameter	Description	Value
vrid *virtual-router-id*	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
session-id	Specifies the local discriminator of the monitored BFD session.	The value is an integer that ranges from 1 to 8191.
session-name *bfd-configure-name*	Specifies the name of the monitored BFD session.	The value is a string of 1 to 15 case-insensitive characters without spaces. **NOTE** When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
increased *value-increased*	Specifies the value by which the priority increases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored BFD session becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored BFD session becomes Down, the VRRP6 priority decreases by 10.

Views

Ethernet interface view, Ethernet sub-interface view, GE interface view, GE sub-interface view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between a VRRP6 group and a BFD session implements the following functions:

1. Rapid active/standby switchover: When the link of a VRRP6 group or the master is faulty, the backup becomes the master after a certain time (second level), causing packet loss. You can associate the VRRP6 group with a BFD session on the backup so that the BFD session can rapidly detect communication faults of the VRRP6 group. When the BFD session detects a fault, it notifies the VRRP6 group that the priority of the backup needs to be increased. Then an active/standby switchover is triggered immediately. This millisecond-level switchover reduces traffic loss. When the monitored BFD session recovers, the original priority of the device in the VRRP6 group is restored.
2. Monitoring the uplink: Because VRRP6 cannot detect faults on the uplink of a VRRP6 group, services are interrupted. You can associate the VRRP6 group with a BFD session on the master so that the BFD session monitors the uplink status of the master. When the BFD session detects a fault on the uplink, it notifies the VRRP6 group that the priority of the master needs to be decreased. Then an active/standby switchover is triggered immediately. This reduces the impact of the uplink fault on service forwarding. When the monitored BFD session recovers, the original priority of the device in the VRRP6 group is restored.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A VRRP6 group has been created and a static BFD session or a static BFD session with automatically negotiated discriminators has been created.

Precautions

After a VRRP6 group is associated with a BFD session, the BFD session type cannot be modified. Before deleting the BFD session type, you must delete all original configurations.

After a VRRP6 group is associated with a BFD session, set an appropriate value of **increased** *value-increased* or **reduced** *value-reduced*. This setting ensures that an active/standby switchover is performed immediately when the monitored BFD session becomes Down.

Multiple VRRP6 groups can monitor a BFD session, and a VRRP6 group can monitor a maximum of eight BFD sessions simultaneously.

NOTE

When associating a VRRP6 group with a BFD session, note the following points:

- If an IPv6 address owner exists in the VRRP6 group, the VRRP6 group cannot monitor the BFD session.
- If **session-name** *bfd-configure-name* is specified, the VRRP6 group can be bound to only the static BFD session with automatically negotiated discriminators.
- If *session-id* is specified, the VRRP6 group can bind to only a static BFD session.

Example

Associate VRRP6 group 1 with the BFD session **hello** on GE1/0/0.

```
<Huawei> system-view
[Huawei] bfd
[Huawei-bfd] quit
[Huawei] bfd hello bind peer-ipv6 FC00::1 interface gigabitethernet 1/0/0 source-ip FC00::2 auto
[Huawei-bfd-session-hello] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FC00::100
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 track bfd session-name hello reduced 40
```

18.6.45 vrrp6 vrid track interface

Function

The **vrrp6 vrid track interface** command associates a VRRP6 group with an interface.

The **undo vrrp6 vrid track interface** command disassociates a VRRP6 group from an interface.

By default, a VRRP6 group is not associated with an interface.

Format

vrrp6 vrid *virtual-router-id* **track interface** *interface-type interface-number* [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.
interface-type interface-number	Specifies the type and number of an interface monitored by a VRRP6 group. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
increased *value-increased*	Specifies the value by which the priority increases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The maximum priority value is 254.
reduced *value-reduced*	Specifies the value by which the priority decreases when the monitored interface becomes Down.	The value is an integer that ranges from 1 to 255. The priority can decrease to 1. By default, when the monitored interface goes Down, the VRRP6 priority of the device decreases by 10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

VRRP6 can only detect the status change of the interface on which a VRRP6 group is configured. VRRP6 cannot detect faults on the uplink interface of the master, causing service interruption. You can associate a VRRP6 group with a device

interface that is not in the VRRP6 group. When the monitored interface is faulty, the priority of the master is reduced. This triggers an active/standby switchover and reduces the impact of services on the uplink interface. When the fault is rectified, the original master restores its priority and switches to the master to forward traffic.

Prerequisites

The **vrrp6 vrid virtual-ip** command has been executed on an interface to create a VRRP6 group.

Precautions

After a VRRP6 group is associated with an interface, set **increased** *value-increased* or **reduced** *value-reduced* to an appropriate value. This setting ensures that an active/standby switchover is performed immediately when the monitored interface becomes Down.

NOTE

- The master and backup in the VRRP6 group must work in preemption mode. It is recommended that the preemption delay be 0 on the backup and larger than 0 on the master.
- If the device is the IPv6 address owner (the virtual router IPv6 address is used as the actual interface address), you cannot associate a VRRP6 group with an interface.
- If the IPv4 protocol status on the monitored interface configured with an IPv4 address changes, a new master in the VRRP6 group is selected. If the IPv6 protocol status on the monitored interface configured with an IPv6 address changes, the VRRP6 group remains unchanged.

Example

Associate VRRP6 group 1 with GE2/0/0 and set **reduced** *value-reduced* to 50 when GE2/0/0 becomes Down.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 2/0/0
[Huawei-GigabitEthernet2/0/0] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet2/0/0] vrrp6 vrid 1 virtual-ip FC00::2
[Huawei-GigabitEthernet2/0/0] vrrp6 vrid 1 track interface gigabitethernet 1/0/0 reduced 50
```

Related Topics

18.6.48 vrrp6 vrid virtual-ip

18.6.46 vrrp6 vrid track interface ipv6-state

Function

The **vrrp6 vrid track interface ipv6-state** command configures a Virtual Router Redundancy Protocol for IPv6 (VRRP6) backup group to track the IPv6 state of a VRRP6-disabled interface, implementing a rapid master/backup VRRP6 switchover.

The **undo vrrp6 vrid track interface ipv6-state** command restores the default configuration.

By default, a VRRP6 backup group does not track the IPv6 state of a VRRP6-disabled interface.

Format

vrrp6 vrid *virtual-router-id* **track interface** *interface-type interface-number* **ipv6-state** [**increased** *value-increased* | **reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track interface** [*interface-type interface-number*]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the ID of a VRRP6 backup group.	The value is an integer ranging from 1 to 255.
interface *interface-type interface-number*	Specifies the type and number of a VRRP6-disabled interface to be tracked.	Currently, the following interfaces cannot be tracked: loopback, NULL, E1-Group (serial interfaces formed by using the channel-set command), Virtual-Template, BRI, DIALER, and AUX, and so on.
increased *value-increased*	Specifies a value by which the VRRP6 priority increases when a tracked VRRP6-disabled interface goes Down.	The value is an integer ranging from 1 to 255. The value 255 is reserved for an IP address owner, and therefore the largest value can be set to 254.
reduced *value-reduced*	Specifies a value by which the VRRP6 priority reduces when a tracked VRRP6-disabled interface goes Down.	The value is an integer ranging from 1 to 255. The smallest value can be set to 1. By default, the VRRP6 priority reduces by 10 if a VRRP6-disabled interface tracked by a VRRP6 backup group goes Down.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

A VRRP6 backup group can track the IPv6 state of a VRRP6-disabled interface. If a device or tracked interface fails, the VRRP6 backup group provides the backup function. To configure a VRRP6 backup group to track the IPv6 state of a VRRP6-disabled interface, run the **vrrp6 vrid track interface ipv6-state** command. After the configuration is complete, if the tracked interface goes Down, the priority of the device in the VRRP6 backup group reduces or increases according to the configuration. In this manner, a new master device is elected to implement the backup function.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The IPv6 state of an interface is described as follows:

- If the tracked interface is a Layer 3 interface, the IPv6 protocol status of the interface is tracked.
- If the tracked interface is a Layer 2 interface or an Eth-Trunk member interface, the physical status of the interface is tracked.

If a tracked VRRP6-disabled interface goes Up, the device on which the interface resides restores its priority.

Before running the **vrrp6 vrid track interface ipv6-state** command, you must run the **vrrp6 vrid virtual-ip** command to configure a VRRP6 backup group.

NOTE

- If an interface on which a VRRP6 backup group is configured is an IP address owner, the VRRP6 backup group cannot be configured to track the status of the interface.
- If a VRRP6 backup group is configured to track the IPv6 state of a VRRP6-disabled interface and an IPv6 address is configured for the interface, any IPv6 protocol status change triggers the VRRP6 backup group to re-elect a master device. If an IPv4 address is configured for the interface, any IPv4 protocol status change does not affect the status of the VRRP6 backup group.

Example

Configure VRRP6 backup group 1 to track the IPv6 state of GE 2/0/0.1, and set *value-reduced* to 20.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 enable
[Huawei-GigabitEthernet1/0/0] ipv6 address 2001:db8::1 64
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::7 link-local
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 track interface gigabitethernet GE2/0/0.1 ipv6-state
reduced 20
```

18.6.47 vrrp6 vrid track ipv6 route

Function

The **vrrp6 vrid track ipv6 route** command configures a Virtual Router Redundancy Protocol (VRRP6) backup group to track a specified route.

The **undo vrrp6 vrid track ipv6 route** command disables a VRRP6 backup group from tracking a specified route.

By default, a VRRP6 backup group tracks no route.

Format

vrrp6 vrid *virtual-router-id* **track ipv6 route** *ipv6-address prefix-length* [**vpn-instance** *vpn-instance-name*] [**reduced** *value-reduced*]

undo vrrp6 vrid *virtual-router-id* **track ipv6 route** [*ipv6-address prefix-length* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the ID of a VRRP6 backup group.	The value is an integer ranging from 1 to 255.
ipv6-address	Specifies the destination IPV6 address of the route to be tracked.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
prefix-length	Specifies the prefix length of an IPv6 address.	The value is an integer ranging from 1 to 128.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
reduced *value-reduced*	Specifies the value by which the master device' priority value decreases if the tracked route is withdrawn or becomes inactive.	The value is an integer ranging from 1 to 255. The default value is 10.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve device reliability, two user gateways are configured to work in master/backup mode, and VRRP6 is enabled on these gateways to determine their master and backup states. Although a VRRP6 backup group has been configured, if an uplink route to a network becomes unreachable, access-side users still use the VRRP6 backup group to forwards service data along the uplink route, causing service data loss.

Association between the VRRP6 backup group and route can prevent service data loss. The VRRP6 backup group can be configured to track the uplink route to the network. If the route is withdrawn or becomes inactive, the route management (RM) module notifies the VRRP6 backup group of the change. After receiving the notification, the VRRP6 backup group changes its master device's VRRP6 priority, and performs a master/backup switchover.

Prerequisites

A routing protocol such as OSPF, IS-IS, or BGP has been configured on the device with a VRRP6 backup group.

Configuration Impact

If the tracked route is withdrawn or becomes inactive, the RM module notifies the VRRP6 module of the unreachable route. After receiving the notification, the VRRP6 backup group changes its master device's VRRP6 priority value and triggers a master/backup VRRP6 switchover.

Precautions

A VRRP6-enabled device configured as the IP address owner cannot track routes.

If a VRRP6 backup group tracks a route of a specified VPN instance, either of the following situations occurs:

- If the VPN instance does not exist, the configuration does not take effect.
- If the VPN instance is deleted after the configuration is complete, the configuration is automatically deleted.

Example

Configure a VRRP6 backup group with VRID of 1 to track a network segment route to 10::1 and allows the master device's VRRP6 priority value to decrease by 20 if the tracked route is withdrawn or becomes inactive.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 track ipv6 route 10::1 64 reduced 20
```

18.6.48 vrrp6 vrid virtual-ip

Function

The **vrrp6 vrid virtual-ip** command creates a VRRP6 group and assigns a virtual IPv6 address to the group.

The **undo vrrp6 vrid virtual-ip** command deletes the virtual IPv6 address of a VRRP6 group.

By default, no VRRP6 group is created.

Format

vrrp6 vrid *virtual-router-id* **virtual-ip** *virtual-ipv6-address* [**link-local**]

undo vrrp6 vrid *virtual-router-id* [**virtual-ip** *virtual-ipv6-address* [**link-local**]]

Parameters

Parameter	Description	Value
virtual-router-id	Specifies the VRID of a VRRP6 group.	The value is an integer that ranges from 1 to 255.

Parameter	Description	Value
virtual-ip *virtual-ipv6-address*	Specifies the virtual IPv6 address of a VRRP6 group.	The address is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
link-local	Indicates that a link-local address is used as the virtual IPv6 address of a VRRP6 group. The first virtual IPv6 address of a VRRP6 group must be a link-local address.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, hosts use the default gateway to communicate with external networks. As value-added services such as IPTV or video conferencing services are widely deployed, hosts may fail to communicate with external networks if the default gateway fails. Configuring dynamic routing protocols such as RIPng, OSPFv3, or ICMPv6 can improve system reliability. However, it is difficult to configure dynamic routing protocols and some hosts may not support dynamic routing protocols. VRRP6 virtualizes multiple routing devices into a virtual router without changing the networking. The virtual router IPv6 address is configured as the default gateway address.

If users on a network have the same reliability requirements, configure multiple virtual IPv6 addresses for a VRRP6 group. By doing this, one virtual IPv6 address serves one separate user group, and the default gateway address remains consistent regardless of changes in VRRP6 device locations. A VRRP6 group can be assigned a maximum of 16 virtual IPv6 addresses.

Precautions

If all the virtual IPv6 addresses in a VRRP6 group are deleted, the VRRP6 group is deleted automatically.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The first virtual IPv6 address of a VRRP6 group must be a link-local address. That is, you must run the **vrrp6 vrid** *virtual-router-id* **virtual-ip** *virtual-ipv6-address* **link-local** command before assigning other virtual IPv6 addresses to the VRRP6 group.
- VRRP6 groups must use different virtual IP addresses.
- Two devices in a VRRP6 group must be configured with the same VRID.
- VRRP6 groups on different interfaces of a device can be configured with the same VRID.

Example

Configure a VRRP6 group on GE1/0/0 and configure the virtual IPv6 address FE80::7.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] vrrp6 vrid 1 virtual-ip FE80::7 link-local
```

18.7 EFM Configuration Commands

18.7.1 clear mgr inactive-configuration slot

Function

The **clear mgr inactive-configuration slot** command deletes the inactive Ethernet OAM configurations from the board that does not register.

Format

clear mgr inactive-configuration slot *slot-id* [**card** *card-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Specifies the slot ID of a board that does not register.	The value is an integer and the value range depends on device model.
card *card-id*	Specifies the offline card ID.	The value is an integer and the value range depends on device model.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a board or a subcard has been replaced, using the **clear mgr inactive-configuration slot** command deletes the configurations of the board or subcard that does not register if these configurations do not need to be saved.

Running the **clear mgr inactive-configuration slot** command can delete the inactivate configurations and the sub-interfaces from the board that does not register.

Before using this command, note the following issues:

- Ensure that the specified board on which configurations are to be deleted does not register.
- Ensure that the specified subcard on which configurations are to be deleted does not register.

Example

Delete the configurations from the board that does not register in slot 1.

```
<Huawei> system-view
[Huawei] clear mgr inactive-configuration slot 1
Warning: The inactive oam-mgr configuration related to the interfaces of the slot or card will be deleted
and cannot be restored, continue? [Y/N]:y
Info: Operation succeeded.
```

18.7.2 display efm

Function

The **display efm** command displays the EFM configuration on an interface.

Format

display efm { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays the EFM configuration on all the interfaces enabled with EFM.	-

Parameter	Description	Value
interface *interface-type interface-number*	Displays the EFM configuration of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view the EFM configuration on the device, run the **display efm** command.

- If **all** is specified, all EFM configuration is displayed.
- If **interface** *interface-type interface-number* is specified, the EFM configuration of a specified interface is displayed.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Display the EFM configuration on Ethernet2/0/0.

```
<Huawei> display efm interface ethernet 2/0/0
 Item                          Value
 -----------------------------------------------------
 Interface:                    Ethernet2/0/0
 EFM Enable Flag:              enable
 Mode:                         active
 Loopback IgnoreRequest:       no
 OAMPDU MaxSize:               128
 OAMPDU Timeout:               5000
 OAMPDU Interval:              1000
 Parser:                       forward
 Multiplexer:                  forward
 ErrCodeNotification:          disable
 ErrCodePeriod:                1
 ErrCodeThreshold:             1
 ErrFrameNotification:         disable
 ErrFramePeriod:               1
 ErrFrameThreshold:            1
 ErrFrameSecondNotification:   disable
 ErrFrameSecondPeriod:         60
 ErrFrameSecondThreshold:      1
 Hold Up Time:                 10
 ThresholdEvtTriggerErrDown:   enable
 TriggerIfDown:                disable
 TriggerMacRenew:              disable
```

 Copyright © Huawei Technologies Co., Ltd.

```
Remote MAC:                    --
Remote EFM Enable Flag:        --
Remote Mode:                   --
Remote MaxSize:                --
Remote Loopback IgnoreRequest: --
Remote State:                  --
Remote Parser:                 --
Remote Multiplexer:            --
ErrFramePeriodNotification:    disable
ErrFramePeriodPeriod:          200000
ErrFramePeriodThreshold:       1
Loopback Remain Time:          1189
```

Table 18-31 Description of the display efm command output

Item	Description
EFM Enable Flag	Whether EFM is enabled on an interface: ● disable: indicates that EFM is disabled on an interface. ● enable: indicates that EFM is enabled on an interface.
Mode	Operation mode of EFM on an interface: ● active: indicates that EFM works in active mode. ● passive: indicates that EFM works in passive mode.
Loopback IgnoreRequest	Whether loopback requests from the remote end are ignored: ● yes: Loopback requests from the remote end are ignored. ● no: Loopback requests from the remote end are processed.
OAMPDU MaxSize	Maximum size of an EFM OAMPDU on an interface. The value ranges from 64 to 1518, in bytes. The default value is 128 bytes.
OAMPDU Timeout	Timeout interval at which an interface receives EFM OAMPDUs. The value is an integer that ranges from 3000 to 30000, in milliseconds. It must be an integer multiple of 1000. The default value is 5000 ms.
OAMPDU Interval	Timeout interval at which an interface sends EFM OAMPDUs. The value is an integer that ranges from 100 to 1000, in milliseconds. The step is 100, for example, the value can be 100, 200, or 300. The default value is 1000 milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Parser	Parser ● forward: device is forwarding non-OAMPDUS to the lower sublayer. ● loopback: device is looping back non-OAMPDUs to lower sublayer. ● discard: device is discarding non-OAMPDUS.
Multiplexer	Multiplexer ● forward: device is forwarding non-OAMPDUs to higher sublayer. ● discard: device is discarding non-OAMPDUS.
ErrCodeNotification	Whether detection of EFM errored codes is enabled: ● disable: indicates that detection of EFM errored codes is disabled. ● enable: indicates that detection of EFM errored codes is enabled.
ErrCodePeriod	Period for detecting EFM errored codes on an interface. The value ranges from 1 to 60, in seconds. The default value is 1s.
ErrCodeThreshold	Threshold for detecting EFM errored codes on an interface. The value ranges from 0 to 65535. The default value is 1.
ErrFrameNotification	Whether detection of EFM errored frames is enabled: ● disable: indicates that detection of EFM errored frames is disabled. ● enable: indicates that detection of EFM errored frames is enabled.
ErrFramePeriod	Period for detecting EFM errored frames on an interface. The value ranges from 1 to 60, in seconds. The default value is 1s.
ErrFrameThreshold	Threshold for detecting EFM errored frames on an interface. The value ranges from 0 to 65535. The default value is 1.
ErrFrameSecondNotification	Whether detection of EFM errored frame seconds is enabled: ● disable: indicates that detection of EFM errored frame seconds is disabled. ● enable: indicates that detection of EFM errored frame seconds is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ErrFrameSecondPeriod	Period for detecting EFM errored frame seconds on an interface. The value ranges from 10 to 900, in seconds. The default value is 60s.
ErrFrameSecondThres-hold	Threshold for detecting EFM errored frame seconds on an interface. The value ranges from 0 to 900. The default value is 1.
Hold Up Time	Value of the EFM faulty-state holdup timer. The value ranges from 0 to 50, in seconds. The default value is 0.
ThresholdEvtTriggerErr-Down	Whether a threshold crossing event is associated with an interface: ● disable: A threshold crossing event is not associated with an interface. ● enable: A threshold crossing event is associated with an interface.
TriggerIfDown	Whether an interface is blocked when the interface detects a fault on the link between the local and peer interfaces: ● disable: The system does not block an interface when detecting a fault on the link between the local and peer interfaces. ● enable: The system blocks an interface when detecting a fault on the link between the local and peer interfaces.
TriggerMacRenew	Whether the MAC address entry on an interface is updated when the interface detects a fault on the link between the local and peer interfaces: ● disable: The system does not update the MAC address entry when detecting a fault on the link between the local and peer interfaces. ● enable: The system updates the MAC address entry when detecting a fault on the link between the local and peer interfaces.
Remote MAC	MAC address of the remote interface. The value -- indicates that the system cannot obtain the MAC address of the remote interface.
Remote EFM Enable Flag	Whether EFM is enabled on the remote interface: ● disable: indicates that EFM is disabled on the remote interface. ● enable: indicates that EFM is enabled on the remote interface. ● --: indicates that the system cannot obtain the EFM status on the remote device.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote Mode	Operation mode of EFM on the remote interface: ● active: indicates that EFM works in active mode. ● passive: indicates that EFM works in passive mode. ● --: indicates that the system cannot obtain the operation mode of EFM on the remote device.
Remote MaxSize	Maximum size of an OAMPDU on the remote interface, in bytes. The value -- indicates that the system cannot obtain the maximum size of an OAMPDU on the remote interface.
Remote Loopback IgnoreRequest	Whether the remote interface ignores loopback requests from the local end: ● --: The system cannot obtain the mode in which the remote interface processes loopback requests from the local end. ● yes: The remote interface ignores loopback requests from the local end. ● no: The remote interface processes loopback requests from the local end.
Remote State	Active/Standby information of the peer device. The value -- indicates that the system cannot obtain the active/standby information of the peer device.
Remote Parser	Remote parser ● forward: device is forwarding non-OAMPDUS to the lower sublayer. ● loopback: device is looping back non-OAMPDUs to lower sublayer. ● discard: device is discarding non-OAMPDUS.
Remote Multiplexer	Remote Multiplexer ● forward: device is forwarding non-OAMPDUs to higher sublayer. ● discard: device is discarding non-OAMPDUS.
ErrFramePeriodNotification	Whether detection of EFM errored frame periods is enabled: ● disable: indicates that detection of EFM errored frame periods is disabled. ● enable: indicates that detection of EFM errored frame periods is enabled.
ErrFramePeriodPeriod	Period for detecting errored frame periods on the interface. The value is an integer that ranges from 20000 to 4294967295. The default value is 200000.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ErrFramePeriodThreshold	Threshold for detecting errored frame periods on the interface. The value is an integer that ranges from 0 to 900. The default value is 1.
Loopback Remain Time	Remaining time of remote loopback: ● --: The interface does not send a remote loopback request. ● Never Timeout: The interface sends a remote loopback request. The value of **timeout** is 0, indicating that the interface is always in remote loopback state. ● Loopback Remain Time: The interface sends a remote loopback request, and the timeout interval of remote loopback is specified.

Related Topics

18.7.7 efm enable
18.7.8 efm error-code notification enable
18.7.9 efm error-code period
18.7.10 efm error-code threshold
18.7.11 efm error-frame notification enable
18.7.12 efm error-frame period
18.7.13 efm error-frame threshold
18.7.14 efm error-frame-second notification enable
18.7.15 efm error-frame-second period
18.7.16 efm error-frame-second threshold
18.7.20 efm mode
18.7.21 efm packet max-size
18.7.27 efm trigger if-down

18.7.3 display efm link-event local

Function

The **display efm link-event local** command displays statistics about local link events.

Format

display efm link-event local { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays statistics about local link events of all interfaces.	-
interface *interface-type interface-number*	Displays statistics about local link events of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After error code detection, error frame detection, or error frame second detection is configured, you can run the **display efm link-event local** command to view statistics about local link events.

Precautions

After the **display efm link-event local** command is run, a hyphen (-) is displayed if error code detection, error frame detection, or error frame second detection is not configured in the interface view.

Example

Displays statistics about local link events on Ethernet2/0/0.

```
<Huawei> display efm link-event local interface ethernet 2/0/0
Item                    Value
-------------------------------------------------------
Interface:              Ethernet2/0/0
-------------------------
Errored-code
Errors:                 0
Error Running Total :   0
Event Running Total :   0
-------------------------
Errored-frame
Errors:                 0
Error Running Total :   0
Event Running Total :   0
-------------------------
Errored-frame-period
Errors:                 0
Error Running Total :   0
```

```
Event Running Total :     0
-------------------------
Errored-frame-seconds
Errors:                   0
Error Running Total :     0
Event Running Total :     0
```

Table 18-32 Description of the display efm link-event local command output

Item	Description
Interface	Interface enabled with EFM.
Errors	Number of currently detected error codes, error frames, or error frame seconds.
Error Running Total	Total number of detected error codes, error frames, or error frame seconds.
Event Running Total	Count of detected error codes, error frames, or error frame seconds.

Related Topics

18.7.8 efm error-code notification enable
18.7.9 efm error-code period
18.7.10 efm error-code threshold
18.7.11 efm error-frame notification enable
18.7.12 efm error-frame period
18.7.13 efm error-frame threshold
18.7.14 efm error-frame-second notification enable
18.7.15 efm error-frame-second period
18.7.16 efm error-frame-second threshold

18.7.4 display efm session

Function

The **display efm session** command displays information about an EFM session between the specified interface and the peer.

Format

display efm session { **all** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
all	Displays information about EFM sessions between all interfaces configured with EFM and the peers.	-
interface *interface-type interface-number*	Displays information about the EFM session between the specified interface and the peer. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether an EFM session configured on a device is negotiated successfully, run the **display efm session** command. The command output includes the EFM status and timeout interval of a loopback test.

- If **all** is specified, information about all EFM sessions configured on the device is displayed.
- If **interface** *interface-type interface-number* is specified, information about EFM sessions configured on a specified interface is displayed.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Display information about EFM sessions between all interfaces and the peers.

```
<Huawei> display efm session all
Interface              EFM State              Loopback Timeout
-----------------------------------------------------------------
Ethernet2/0/0      discovery                  --
```

Table 18-33 Description of the display efm session command output

Item	Description
Interface	Interface name.

Item	Description
EFM State	EFM protocol status on the interface: • disabled: The EFM protocol is disabled on the interface. • discovery: The interface is in OAM discovery state. • detect: The interface is in Detect state. • loopback (control): The interface initiates remote loopback and discards the packets looped back. • loopback (be controlled): The interface responds to remote loopback.
Loopback Timeout	Timeout interval of a loopback test.

Related Topics

18.7.7 efm enable

18.7.18 efm loopback

18.7.5 display snmp-agent trap feature-name efm all

Function

The **display snmp-agent trap feature-name efm all** command displays the status of all traps of the EFM module.

Format

display snmp-agent trap feature-name efm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The Simple Network Management Protocol (SNMP) is a network management standard widely used on the TCP/IP network. It uses a central computer (a

network management station) that runs network management software to manage network elements. The SNMP agent reports trap messages to the network management station so that the network management station can obtain the network status in a timely manner, and the network administrator can take measures accordingly.

The **display snmp-agent trap feature-name efm all** command displays the following information:

- Trap names supported by the EFM module. The trap names are the same as the trap names specified by the **snmp-agent trap enable feature-name efm trap-name** *trap-name* command. Each trap name corresponds to a network element abnormality.
- Trap status of the EFM module. You can check whether the trap is reported based on the trap name.

Prerequisites

SNMP has been enabled. See **snmp-agent**.

Example

Display the status of all traps of the EFM module.

```
<Huawei> display snmp-agent trap feature-name efm all
-----------------------------------------------------------------------------
Feature name: EFM
Trap number : 5
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
threshold                    off                     off
nonthreshold                 off                     off
dyinggasp                    off                     off
nonthredholdrecovery         off                     off
loopbackfailed               off                     off
```

Table 18-34 Description of the display snmp-agent trap feature-name efm all command output

Item	Description
Feature name	Name of the module that the trap belongs to.
Trap number	Number of traps.
Trap name	Trap name. Traps of the EFM module include: • nonthreshold: trap sent when a non-threshold crossing event occurs. • threshold: trap sent when a threshold crossing event occurs. • dyinggasp: trap of dying gasp. • nonthredholdrecovery: trap sent when a non-threshold fault is rectified. • loopbackfailed: trap sent when the loopback failed.

Item	Description
Default switch status	Default status of the trap function: • on: indicates that the trap function is enabled by default. • off: indicates that the trap function is disabled by default.
Current switch status	Status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

18.7.37 snmp-agent trap enable feature-name efm

18.7.6 display test-packet result

Function

The **display test-packet result** command displays information about sent test packets.

Format

display test-packet result

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After remote loopback is enabled and the **test-packet start** command is used to configure a device to send test packets, the **display test-packet result** command can be used to view information about sent test packets. You can determine link performance based on the information about test packets.

Example

Display information about sent test packets.

```
<Huawei> display test-packet result
  TestResult                Value
-----------------------------------------------------------
  PacketsSend :               5
  PacketsReceive :            5
  PacketsLost :               0
  BytesSend :                 320
  BytesReceive :              320
  BytesLost :                 0
  StartTime :                 06-13-2012 14:44:13 UTC+03:00
  EndTime :                   06-13-2012 14:44:14 UTC+03:00
```

Table 18-35 Description of the display test-packet result command output

Item	Description
PacketsSend	Number of sent test packets.
PacketsReceive	Number of received test packets.
PacketsLost	Number of discarded test packets.
BytesSend	Total length of sent test packets, in bytes.
BytesReceive	Total length of received test packets, in bytes.
BytesLost	Total length of discarded test packets, in bytes.
StartTime	Start time test packets are sent.
EndTime	End time test packets are sent.

Related Topics

18.7.38 test-packet start

18.7.7 efm enable

Function

The **efm enable** command enables EFM globally or on an interface.

The **undo efm enable** command disables EFM globally or on an interface.

By default, EFM is disabled globally. That is, EFM is disabled on all interfaces.

Format

efm enable

undo efm enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using EFM functions, you must enable EFM globally.

After EFM is enabled on an interface, the interface starts to send OAM PDUs to perform point-to-point EFM link detection. EFM link detection can be implemented between two interfaces only after EFM is enabled on the peer interface.

Precautions

When you use the **undo efm enable** command to disable EFM globally, the device deletes all EFM configurations. When the device is implementing remote loopback and sending a great deal of test packets, running the **undo efm enable** command will cause packets to be forwarded.

Example

Enable EFM globally.

```
<Huawei> system-view
[Huawei] efm enable
Info: Operation succeeded.
```

Enable EFM on interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] efm enable
Info: Operation succeeded.
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm
18.7.20 efm mode

18.7.8 efm error-code notification enable

Function

The **efm error-code notification enable** command enables an interface to detect EFM errored codes.

The **undo efm error-code notification enable** command disables an interface from detecting EFM errored codes.

 Copyright © Huawei Technologies Co., Ltd.

By default, an interface is not enabled to detect EFM errored codes.

Format

efm error-code notification enable

undo efm error-code notification enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-code notification enable** command enables an interface to detect EFM errored codes. The local device considers a link faulty if the number of detected errored codes within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAM PDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable interface Ethernet2/0/0 to detect errored codes.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
```

```
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm error-code notification enable
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.9 efm error-code period

18.7.10 efm error-code threshold

18.7.9 efm error-code period

Function

The **efm error-code period** command sets the period for detecting EFM errored codes on an interface.

The **undo efm error-code period** command restores the default period for detecting EFM errored codes on an interface.

By default, the period for detecting EFM errored codes on an interface is 1s.

Format

efm error-code period *period*

undo efm error-code period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored codes.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 1s.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-code period** *period* command is run to set the period for detecting EFM errored codes, run the **efm error-code notification enable** command to enable an interface to detect EFM errored codes. When the number

 Copyright © Huawei Technologies Co., Ltd.

of detected errored codes during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored codes on interface Ethernet2/0/0 to 20s.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm error-code period 20
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.8 efm error-code notification enable

18.7.10 efm error-code threshold

18.7.10 efm error-code threshold

Function

The **efm error-code threshold** command sets the threshold for detecting EFM errored codes on an interface.

The **undo efm error-code threshold** command restores the default threshold for detecting EFM errored codes on an interface.

By default, the threshold for threshold for detecting EFM errored codes on an interface is 1.

Format

efm error-code threshold *threshold*

undo efm error-code threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored codes.	The value is an integer that ranges from 0 to 65535. The default value is 1. The value 0 is not recommended.

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-code period** *period* commands is executed to set the period for detecting EFM errored codes, run the **efm error-code threshold** *threshold* command to set the threshold for detecting errored codes. Run the **efm error-code notification enable** command to enable an interface to detect EFM errored codes. When the number of detected errored codes during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored codes on interfaceEthernet2/0/0 to 100.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm error-code threshold 100
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.8 efm error-code notification enable

18.7.9 efm error-code period

18.7.11 efm error-frame notification enable

Function

The **efm error-frame notification enable** command enables an interface to detect EFM errored frames.

The **undo efm error-frame notification enable** command disables an interface from detecting EFM errored frames.

By default, an interface is not enabled to detect EFM errored frames.

 Copyright © Huawei Technologies Co., Ltd.

Format

efm error-frame notification enable

undo efm error-frame notification enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-frame notification enable** command enables an interface to detect EFM errored frames. The local device considers a link faulty if the number of detected errored frames within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAM PDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable interfaceEthernet2/0/0 to detect errored frames.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm error-frame notification enable
Info: Operation succeeded.
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

18.7.2 display efm
18.7.7 efm enable
18.7.12 efm error-frame period
18.7.13 efm error-frame threshold

18.7.12 efm error-frame period

Function

The **efm error-frame period** command sets the period for detecting EFM errored frames on an interface.

The **undo efm error-frame period** command restores the default period for detecting EFM errored frames on an interface.

By default, the period for detecting EFM errored frames on an interface is 1s.

Format

efm error-frame period *period*

undo efm error-frame period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored frames.	The value is an integer that ranges from 1 to 60, in seconds. The default value is 1s.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-frame period** *period* command is run to set the period for detecting EFM errored frames on an interface, run the **efm error-frame notification enable** command to enable an interface to detect EFM errored frames. When the number of detected errored frames during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

EFM has been enabled globally using the **efm enable** command.

Example

Set the period for detecting EFM errored frames on interface Ethernet2/0/0 to 20 seconds.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm error-frame period 20
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.11 efm error-frame notification enable

18.7.13 efm error-frame threshold

18.7.13 efm error-frame threshold

Function

The **efm error-frame threshold** command sets the threshold for detecting EFM errored frames on an interface.

The **undo efm error-frame threshold** command restores the default threshold for detecting EFM errored frames on an interface.

By default, the threshold for detecting EFM errored frames on an interface is 1.

Format

efm error-frame threshold *threshold*

undo efm error-frame threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored frames.	The value is an integer that ranges from 0 to 65535. The default value is 1. The value 0 is not recommended.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After the **efm error-frame period** *period* commands is executed to set the period for detecting EFM errored frames on an interface, run the **efm error-frame threshold** *threshold* command to set the threshold for detecting errored frames. Run the **efm error-frame notification enable** command to enable an interface to detect EFM errored frames. When the number of detected errored frames during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored frames on interface Ethernet2/0/0 to 100.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm error-frame threshold 100
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.11 efm error-frame notification enable

18.7.12 efm error-frame period

18.7.14 efm error-frame-second notification enable

Function

The **efm error-frame-second notification enable** command enables an interface to detect EFM errored frame seconds.

The **undo efm error-frame-second notification enable** command disables an interface from detecting EFM errored frame seconds.

By default, an interface is not enabled to detect EFM errored frame seconds.

Format

efm error-frame-second notification enable

undo efm error-frame-second notification enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Monitoring Ethernet links is difficult if network performance deteriorates while traffic is being transmitted over physical links. Link monitoring is used to detect link layer faults in various environments. After EFM link monitoring is configured, the device queries statistics about the physical layer data of the interface management module to monitor the quality of the link connected to an interface. EFM link monitoring implements the following functions:

- Reports an alarm when the number of errored codes detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frames detected during a specified detection interval exceeds the preset threshold.
- Reports an alarm when the number of errored frame seconds detected during a specified interval exceeds the preset threshold.

The **efm error-frame-second notification enable** command enables an interface to to detect EFM errored frame seconds. The local device considers a link faulty if the number of detected errored frame seconds within the detection interval reaches or exceeds the preset threshold. Then the local device generates an alarm, reports the alarm to the NMS, and sends an OAM PDU to notify the peer device of the link failure.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable interface Ethernet2/0/0 to detect errored frame seconds.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm error-frame-second notification enable
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm
18.7.7 efm enable
18.7.15 efm error-frame-second period
18.7.16 efm error-frame-second threshold

18.7.15 efm error-frame-second period

Function

The **efm error-frame-second period** command sets the period for detecting EFM errored frame seconds on an interface.

The **undo efm error-frame-second period** command restores the default period for detecting EFM errored frame seconds on an interface.

By default, the period for detecting EFM errored frame seconds on an interface is 60s.

Format

efm error-frame-second period *period*

undo efm error-frame-second period

Parameters

Parameter	Description	Value
period	Specifies the period for detecting EFM errored frame seconds.	The value is an integer that ranges from 10 to 900, in seconds. The default value is 60s.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm error-frame-second period** *period* command is run to set the period for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second notification enable** command to enable an interface to detect EFM errored frame seconds. When the number of detected errored frame seconds during the period reaches or exceeds a preset threshold, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the period for detecting EFM errored frame seconds on interface Ethernet2/0/0 to 20s.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm error-frame-second period 20
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.14 efm error-frame-second notification enable

18.7.16 efm error-frame-second threshold

18.7.16 efm error-frame-second threshold

Function

The **efm error-frame-second threshold** command sets the threshold for detecting EFM errored frame seconds on an interface.

The **undo efm error-frame-second threshold** command restores the default threshold for detecting EFM errored frame seconds on an interface.

By default, the threshold for detecting EFM errored frame seconds on an interface is 1.

Format

efm error-frame-second threshold *threshold*

undo efm error-frame-second threshold

Parameters

Parameter	Description	Value
threshold	Specifies the threshold for detecting EFM errored frame seconds.	The value is an integer that ranges from 0 to 900. The default value is 1. The value 0 is not recommended.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After the **efm error-frame-second period** *period* commands is executed to set the threshold for detecting EFM errored frame seconds on an interface, run the **efm error-frame-second threshold** *threshold* command to set the threshold for detecting errored frame seconds. Run the **efm error-frame-second notification enable** command to enable an interface to detect EFM errored frame seconds. When the number of detected errored frame seconds during the period reaches or exceeds the threshold specified by *threshold*, the local device generates an alarm and notifies the peer device of the alarm event.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Example

Set the threshold for detecting EFM errored frame seconds on interface Ethernet2/0/0 to 10.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm error-frame-second threshold 10
Info: Operation succeeded.
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.14 efm error-frame-second notification enable

18.7.15 efm error-frame-second period

18.7.17 efm holdup-timer

Function

The **efm holdup-timer** command sets the value of the EFM faulty-state holdup timer on an interface.

The **undo efm holdup-timer** command restores the default value interval of the EFM faulty-state holdup timer on an interface.

By default, the value of the EFM faulty-state holdup timer is 0s.

Format

efm holdup-timer *time*

undo efm holdup-timer

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time	Specifies the value of the EFM faulty-state holdup timer on an interface.	The value is an integer that ranges from 0 to 50, in seconds. The default value is 0.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **efm trigger if-down** command is used to associate EFM with an interface, run the **efm holdup-timer** command to set the value of the EFM faulty-state holdup timer for connectivity faults detected by EFM. The faulty state remains unchanged within the value of the holdup timer. EFM does not detect whether the connectivity fault is cleared until the faulty-state holdup timer expires.

After the failed link recovers, EFM works as follows:

- If *time* is not specified, EFM immediately changes the link status to Up.
- If *time* is specified, EFM changes the link status to Up only after the time specified by *time* expires. This prevents the link from frequently alternating between Up and Down.

Prerequisites

EFM has been enabled globally and on interfaces using the **efm enable** command.

It is recommended that you run the **efm trigger if-down** command to associate EFM with an interface before running the **efm holdup-timer** command to set the value of EFM faulty-state holdup timer on the interface. Otherwise, the holdup timer does not take effect.

Example

Set the value of EFM faulty-state holdup timer on Ethernet2/0/0 to 10s.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm trigger if-down
[Huawei-Ethernet2/0/0] efm holdup-timer 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

18.7.7 efm enable
18.7.27 efm trigger if-down

18.7.18 efm loopback

Function

The **efm loopback** command configures an interface to initiate or end an EFM remote loopback.

Format

efm loopback { **start** [**timeout** *timeout*] | **stop** }

Parameters

Parameter	Description	Value
start	Initiate an EFM remote loopback.	-
timeout *timeout*	Specifies the timeout interval of an EFM remote loopback.	The value is an integer that ranges from 0 to 1000, in minutes. The default value is 20. The value 0 indicates that no timeout interval is set. That is, the interface remains in remote loopback state.
stop	Ends an EFM remote loopback.	-

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

EFM remote loopback is used to locate link failures and test the link quality. After remote loopback is enabled, configure the local device to send test packets to the peer device. Based on the statistics about sent and received test packets, you can check connectivity and performance of a specified link.

- If **start** is specified, an interface on the local device sends a remote loopback message to the peer device. After receiving the message, the peer device

enters the loopback state. In loopback state, the peer sends back all received packets, except EFM OAMPDUs, to the local device through the interface that has received these packets.

- If **stop** is specified, an interface on the local device sends a remote loopback stop message to the peer device. After receiving the message, the peer device exits from the loopback state.
- If remote loopback is left enabled, the remote device keeps looping back service data, causing a service interruption. To prevent this problem, a capability can be configured to disable remote loopback automatically after a specified timeout interval. By default, the timeout interval for remote loopback is 20 minutes. The remote loopback test stops after 20 minutes. You can set the timeout interval to 0 to keep a link in remote loopback state.

  NOTE

  The link in remote loopback state will not forward service data. Therefore, execute caution when you set the timeout interval to 0.

Prerequisites

- EFM has been enabled and is in detect state.
- The device has been configured to work in active mode using the **efm mode active** command.

Precautions

After remote loopback is enabled, all packets except EFM OAMPDUs are looped back on the remote device. EFM OAM remote loopback must be implemented on the link that does not need to forward service data. Otherwise, service data forwarding is affected.

Remote loopback is implemented successfully only when EFM protocols at the local end and the peer are in handshake state and EFM at the local end works in active mode. You can use the **display efm session** command to check whether EFM OAM protocols on the local interface and the peer are in handshake state.

Example

Configure interface Ethernet2/0/0 to initiate an EFM OAM remote loopback.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm loopback start
```

Set the timeout interval for an EFM OAM remote loopback on interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm loopback start timeout 10
```

Configure interface Ethernet2/0/0 to stop an EFM OAM remote loopback.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
```

```
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm loopback stop
```

Related Topics

18.7.4 display efm session

18.7.20 efm mode

18.7.7 efm enable

18.7.19 efm loopback ignore-request

Function

The **efm loopback ignore-request** command enables an interface to ignore loopback requests sent by the remote end.

The **undo efm loopback ignore-request** command restores the default setting for the loopback function on an interface.

By default, an interface supports remote loopback. After receiving a loopback request from a remote end, the interface enters the loopback state.

Format

efm loopback ignore-request

undo efm loopback ignore-request

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Remote loopback is used to monitor link quality and locate link faults. Periodic loopback detection helps detect network faults in a timely manner.

If an interface is in loopback state, the interface loops back all received traffic, causing service interruption and imposing attacks. To solve this problem, run the **efm loopback ignore-request** command to enable the interface to reject the remote Ethernet OAM loopback request carried in a Loopback Control OAMPDU sent by a remote interface.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command and the interface is not in loopback state.

Precautions

After the **efm loopback ignore-request** command is run, the interface will discard an OAMPDU carrying a remote loopback request.

Example

Enable interface Ethernet2/0/0 to ignore loopback requests sent by a specified remote interface.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm loopback ignore-request
```

Related Topics

18.7.4 display efm session

18.7.20 efm mode

18.7.7 efm enable

18.7.18 efm loopback

18.7.20 efm mode

Function

The **efm mode** command configures the working mode of EFM on an interface.

The **undo efm mode** command restores the default working mode of EFM on an interface.

By default, EFM on an interface works in active mode.

Format

efm mode { **active** | **passive** }

undo efm mode

Parameters

Parameter	Description	Value
active	Indicates that EFM on an interface works in active mode.	-
passive	Indicates that EFM on an interface works in passive mode.	-

Views

Ethernet interface view, GE interface view, XGE interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

EFM supports two connection modes: active and passive. By setting the working mode of EFM OAM, you can configure whether a device can send or receive a specified type of EFM OAMPDU. **Table 18-36** describes the differences between the active and passive modes.

Table 18-36 Capabilities for processing OAMPDUs in active and passive modes

Event	Active Mode	Passive Mode
Initiate a connection request by sending an Information OAMPDU during the discovery process	Supported	Not supported
Respond to a connection request during the discovery process	Supported	Supported
Send Information OAMPDUs	Supported	Supported
Send Event Notification OAMPDUs	Supported	Supported
Send Loopback Control OAMPDUs	Supported	Not supported
Respond to Loopback Control OAMPDUs	Supported (The remote EFM entity must work in active mode.)	Supported

Precautions

- The working mode of EFM can be set on an interface only after EFM is enabled globally and before EFM is enabled on the interface. The working mode of EFM on an interface cannot be changed after EFM is enabled on the interface. Before changing the working mode of EFM on an interface, run the **undo efm enable** command to disable EFM on the interface.
- An EFM connection can only be initiated by an OAM entity working in active mode. An OAM entity working in passive mode waits to receive a connection request from its peer entity.
- Two OAM entities both working in passive mode cannot establish an EFM connection between them.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure EFM OAM on interface Ethernet2/0/0 to work in passive mode.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm mode passive
```

Related Topics

18.7.4 display efm session

18.7.7 efm enable

18.7.18 efm loopback

18.7.21 efm packet max-size

Function

The **efm packet max-size** command sets the maximum size of an EFM OAMPDU on an interface. All EFM OAMPDUs that exceed the maximum size on an interface are discarded as invalid packets.

The **undo efm packet max-size** command restores the default maximum size of an EFM OAMPDU on an interface.

By default, the maximum size of an EFM OAMPDU on an interface is 128 bytes.

Format

efm packet max-size *size*

undo efm packet max-size

Parameters

Parameter	Description	Value
size	Specifies the maximum size of an EFM OAMPDU. The size contains the length of Layer 2 frame header and the length of the cyclic redundancy check (CRC) field.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 128 bytes.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can run the **efm packet max-size** command to adjust the maximum size of an EFM OAMPDU so that non-Huawei devices can communicate.

Prerequisites

EFM has been enabled globally using the **efm enable** command.

Precautions

The local device and the peer determine the actual value of the maximum size of an EFM OAMPDU through negotiation. The smaller maximum size of an EFM OAMPDU set on the local interface or the peer is used.

Example

Set the maximum size of an EFM OAMPDU on interface Ethernet2/0/0 to 120 bytes.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm packet max-size 120
```

Related Topics

18.7.2 display efm

18.7.7 efm enable

18.7.22 efm timeout

Function

The **efm timeout** command sets the timeout interval at which EFM OAMPDUs are received.

The **undo efm timeout** command restores the default timeout interval.

By default, the timeout interval at which EFM OAMPDUs are received is 5000 milliseconds.

Format

efm timeout *timeout-value*

undo efm timeout

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
timeout-value	Specifies the timeout interval at which an interface receives EFM OAMPDUs.	The value is an integer that ranges from 3000 to 30000, in milliseconds. The step is 1000 milliseconds. The default value is 5000 milliseconds.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By setting the timeout interval at which OAMPDUs are received, you can change the time required for connectivity fault detection.

Prerequisites

EFM OAM has been enabled globally but is not enabled on an interface.

Precautions

After the timeout interval expires, the EFM OAM protocol switches back to the discovery state. Ensure that interfaces on both ends of a link use the same timeout interval. Otherwise, EFM session negotiation may fail, or the EFM session may flap.

After EFM OAM is enabled on an interface, the timeout interval cannot be changed.

- A shorter timeout interval indicates a shorter time required for connectivity fault detection.
- A longer timeout interval indicates a longer time required for connectivity fault detection.

Example

Set the timeout interval at which EFM OAMPDUs are received on interface Ethernet2/0/0 to 3000 ms.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm timeout 3000
```

 Copyright © Huawei Technologies Co., Ltd.

18.7.23 efm src-mac

Function

The **efm src-mac** command configures an interface or bridge MAC address as the source MAC address in an OAMPDU.

The **undo efm src-mac** command restores the default configuration.

By default, a bridge MAC address is used as the source MAC address in an OAMPDU.

Format

efm src-mac { **port** | **bridge** }

undo efm src-mac

Parameters

Parameter	Description	Value
port	Configures an interface MAC address as the source MAC address in an OAMPDU.	-
bridge	Configures a bridge MAC address as the source MAC address in an OAMPDU.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

OAMPDUs support interface or bridge MAC addresses as source MAC addresses. You can run the **efm src-mac** command to configure an interface or bridge MAC address as the source MAC address in an OAMPDU before enabling EFM globally.

Example

Configure an interface MAC address as the source MAC address in an OAMPDU.

```
<Huawei> system-view
[Huawei] efm src-mac port
```

18.7.24 efm threshold-event trigger error-down

 Copyright © Huawei Technologies Co., Ltd.

Function

The **efm threshold-event trigger error-down** command associates an EFM threshold crossing event with an interface.

The **undo efm threshold-event trigger error-down** command disassociates an EFM threshold crossing event from an interface.

By default, a threshold crossing event is not associated with an interface.

Format

efm threshold-event trigger error-down

undo efm threshold-event trigger error-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When link monitoring is configured for an interface on a link, the link is considered unavailable, if the number of errored frames, errored codes, or errored frame seconds detected by the interface reaches or exceeds the threshold within a period. In this case, you can run the **efm threshold-event trigger error-down** command to associate a threshold crossing event with an interface so that the system sets the administrative state of the interface to Down. As a result, all services on the interface are interrupted.

Prerequisites

EFM has been enabled on an interface using the **efm enable** command.

Follow-up Procedure

Configure the interface to go administratively Up by using either of the following methods:

- Run the **error-down auto-recovery** command to set the auto-recovery delay before an interface goes administratively Up.
- Run the **shutdown** command and then the **undo shutdown** command to restore the administrative state of the interface to Up.

Example

Associate a threshold crossing event with interface Ethernet2/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm threshold-event trigger error-down
```

18.7.25 efm trigger clear-arp vlan

Function

The **efm trigger clear-arp vlan** command clears an ARP entry corresponding to a VLANIF interface.

The **undo efm trigger clear-arp vlan** command cancels the configuration.

By default, an interface does not clear an ARP entry.

Format

efm trigger clear-arp vlan *vlan-id*

undo efm trigger clear-arp vlan *vlan-id*

Parameters

Parameter	Description	Value
vlan-id	Specifies the VLAN ID in an ARP entry.	The value is an integer that ranges from 1 to 4094.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a fault, the EFM module notifies the OAM management module of the fault. The OAM management module searches the EFM fault relationship table based on the interface number and VLAN ID, and then clears the ARP entry that corresponds to the VLANIF interface.

Prerequisites

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Enable Ethernet2/0/0 in VLAN 10 to clear ARP entries.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm trigger clear-arp vlan 10
```

Related Topics

18.7.7 efm enable

18.7.26 efm trigger error-down

Function

The **efm trigger error-down** command associates an error event with an interface.

The **undo efm trigger error-down** command disassociates an error event from an interface.

By default, an error event is not associated with an interface.

Format

efm { **critical-event** | **dying-gasp** | **link-fault** | **timeout** } **trigger error-down**

undo efm { **critical-event** | **dying-gasp** | **link-fault** | **timeout** } **trigger error-down**

NOTE

Only the AR161F-DGP and devices that support the Dying Gasp capacity card support dying-gasp.

Parameters

Parameter	Description	Value
critical-event	Indicates an unspecified critical event. It usually refers to a fault on the interface associated with MGR.	-
dying-gasp	Indicates an unrecoverable failure. It usually refers to board reset or system restart.	-
link-fault	Indicates a physical link fault. It usually refers to a fault on an interface.	-
timeout	Indicates the timeout interval at which EFM OAMPDUs are received.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When EFM OAM associated with an interface detects a connectivity fault on a link, the protocol status of the interface goes Down. The interface goes Up after the faulty link recovers.

After the **efm trigger error-down** command is used, the administrative status of the interface goes Down when EFM OAM detects remote **critical-event**, **dying-gasp**, or **link-fault** events, or local **timeout** event. Traffic will not be switched back after the faulty link recovers. Check link quality before switching traffic back to the original link.

Prerequisites

EFM OAM has been enabled globally and on an interface using the **efm enable** command.

Follow-up Procedure

When an associated error event occurs, the interface goes Down. The protocol status of the interface will not go Up even if the faulty link recovers. In this case, perform either of the following operations:

- Disassociates an error event from the interface.
- Run the **shutdown (interface view)** command, and then run the **undo shutdown (interface view)** command in the interface view.

Precautions

An interface can be associated with various types of error events. For example, if both **efm critical-event trigger error-down** and **efm dying-gasp trigger error-down** are used, the protocol status of the interface becomes Down when the device receives EFM OAM packets indicating **critical-event** or **dying-gasp** faults.

- The **efm critical-event trigger error-down** command is used and the remote interface associated with MGR goes Down. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **critical-event** fault.
- The **efm dying-gasp trigger error-down** command is used and the board where the remote interface resides is reset or the system restarts. The local device will set the protocol status of the corresponding interface to Down after receiving an EFM OAM packet indicating a **dying-gasp** fault.
- The **efm link-fault trigger error-down** command is used and the physical link of the remote device is faulty. The local device will set the protocol status

 Copyright © Huawei Technologies Co., Ltd.

of the corresponding interface to Down after receiving an EFM OAM packet indicating a **link-fault** fault.

- The **efm timeout trigger error-down** command is used on the local device. The local device will set the protocol status of the corresponding interface to Down if it does not receive packets from the remote device in a specified period of time (5s by default).

NOTE

The **efm trigger if-down** and **efm trigger error-down** commands cannot be used simultaneously, and the **efm trigger mac-renew** and **efm trigger error-down** commands cannot be used simultaneously.

Example

Associate **dying-gasp** faults with interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm dying-gasp trigger error-down
```

Related Topics

18.7.27 efm trigger if-down

18.7.27 efm trigger if-down

Function

The **efm trigger if-down** command associates EFM with an interface.

The **undo efm trigger if-down** command disassociates EFM from an interface.

By default, EFM OAM is not associated with any interface.

Format

efm trigger if-down

undo efm trigger if-down

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

EFM can be associated with interfaces. On a scenario with primary and backup links, if EFM detects a fault on the primary link, it will set the protocol status of the associated interface to ETHOAM Down, speeding up routing convergence. Traffic can be fast switched to the backup link.

Prerequisites

EFM has been enabled globally and on an interface, and is in detect state.

Precautions

If EFM is associated with an interface and detects a link fault, the protocol status of the interface becomes ETHOAM Down, and no packet except EFM OAMPDUs can be forwarded by the interface, and all Layer 2 and Layer 3 services are blocked. Therefore, associating EFM with an interface may greatly affect services. When the interface detects link recovery using EFM, the interface can forward all packets and unblocks Layer 2 and Layer 3 services.

If Layer 2 and Layer 3 services are blocked due to a misoperation, run the **undo efm trigger if-down** command in the interface view to restore services.

Example

Associate EFM with interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm trigger if-down
```

18.7.28 efm trigger mac-renew

Function

The **efm trigger mac-renew** command configures the device to clear the MAC address table on a physical interface.

The **undo efm trigger mac-renew** command cancels the configuration.

By default, an interface is not enabled to clear the MAC address table.

Format

efm trigger mac-renew

undo efm trigger mac-renew

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To detect a fault on a VLL configured on the PE device connected to a CE device and to perform PW switching by clearing the MAC address table, run the **efm trigger mac-renew** command on the corresponding interface of the CE device.

Precautions

EFM has been enabled globally and on an interface using the **efm enable** command.

Example

Configure Ethernet2/0/0 to delete the corresponding MAC entry after a fault notification is received.

```
<Huawei> system-view
[Huawei] efm enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] efm enable
[Huawei-Ethernet2/0/0] efm trigger mac-renew
```

Related Topics

18.7.7 efm enable

18.7.29 oam-bind efm interface bfd-session

Function

The **oam-bind efm interface bfd-session** command enables bidirectional fault notification between EFM OAM and BFD.

The **undo oam-bind efm interface bfd-session** command cancels the configuration.

By default, bidirectional transmission of fault messages between EFM OAM and BFD is not configured.

Format

oam-bind efm interface *interface-type interface-number* **bfd-session** *bfd-session-id*

undo oam-bind efm interface *interface-type interface-number* **bfd-session** *bfd-session-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bfd-session-id	Specifies the ID of a BFD session.	The value is an integer that ranges from 1 to 8191.
interface-type interface-number	Specifies the type and number of the interface enabled with EFM. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and BFD is deployed at another side of a device, associate EFM with BFD on the device. This allows EFM and BFD to notify each other of faults and ensures reliable service transmission.

Association between EFM and BFD is bidirectional:

- If EFM detects a link fault, it will notify BFD of the fault.
- If BFD detects a link fault, it will notify EFM of the fault.

The following commands are used to associate BFD with EFM:

- **oam-bind efm interface bfd-session**
- **oam-bind ingress bfd-session egress efm interface**
- **oam-bind ingress efm interface egress bfd-session**

Choose the preceding commands in different scenarios according to **Table 18-37**.

 Copyright © Huawei Technologies Co., Ltd.

Table 18-37 Association between EFM and BFD

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and BFD	Use the **oam-bind efm interface bfd-session** command to configure EFM and BFD to notify each other of faults.	Run the following commands at a random order: • Run the **oam-bind ingress efm interface egress bfd-session** command to configure EFM to notify BFD of faults. • Run the **oam-bind ingress bfd-session egress efm interface** command to configure BFD to notify EFM of faults.
Unidirectional fault notification between EFM and BFD	Choose either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress bfd-session** command to configure EFM to notify BFD of faults. • Run the **oam-bind ingress bfd-session egress efm interface** command to configure BFD to notify EFM of faults.	None

Prerequisites

A BFD session has been created and EFM OAM has been enabled globally and on an interface.

Precautions

The following types of BFD sessions can be used:

- Static BFD for LSP (LDP, TE, TE LSP, static LSP, and vll pw) sessions (a PST is required)
- BFD for IP sessions (no PST is required)

Example

Configure bidirectional fault notification between EFM OAM and BFD through Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind efm interface ethernet 2/0/0 bfd-session 50
```

Related Topics

18.7.7 efm enable

18.7.30 oam-bind efm interface trigger if-down interface

Function

The **oam-bind efm interface trigger if-down interface** command enables bidirectional fault notification between EFM and an interface.

The **undo oam-bind efm interface trigger if-down interface** command cancels the configuration.

By default, bidirectional transmission of information about a fault between EFM OAM and an interface is not configured.

Format

oam-bind efm interface *interface-type1 interface-number1* **trigger if-down interface** *interface-type2 interface-number2*

undo oam-bind efm interface *interface-type1 interface-number1* **trigger if-down interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 18-38 describes the implementation of association between EFM and an interface.

Table 18-38 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The **display current-configuration** command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**

 Copyright © Huawei Technologies Co., Ltd.

Scenario	Configuration Solution 1	Configuration Solution 2
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Precautions

When configuring bidirectional fault notification between EFM and an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type1 interface-number1*.
- EFM and an interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

Example

Configure bidirectional fault notification between an EFM session and Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind efm interface ethernet 2/0/0 trigger if-down interface ethernet 2/0/1
```

Related Topics

18.7.7 efm enable

18.7.36 oam-mgr

18.7.33 oam-bind ingress efm interface trigger if-down egress interface

18.7.34 oam-bind ingress interface egress efm interface trigger if-down

18.7.31 oam-bind ingress bfd-session egress efm interface

Function

The **oam-bind ingress bfd-session egress efm interface** command configures BFD to report faults to EFM OAM.

The **undo oam-bind ingress bfd-session egress efm interface** command cancels the configuration.

By default, BFD module does not send fault messages to EFM OAM.

Format

oam-bind ingress bfd-session *bfd-session-id* **egress efm interface** *interface-type interface-number*

undo oam-bind ingress bfd-session *bfd-session-id* **egress efm interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
bfd-session-id	Specifies the ID of a BFD session.	The value is an integer that ranges from 1 to 8191.
interface-type interface-number	Specifies the type and number of an Ethernet interface. The interface must have been enabled with EFM OAM. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and BFD is deployed at another side of a device, associate EFM with BFD on the device. This allows EFM and BFD to notify each other of faults and ensures reliable service transmission.

Association between EFM and BFD is bidirectional:

- If EFM detects a link fault, it will notify BFD of the fault.
- If BFD detects a link fault, it will notify EFM of the fault.

The following commands are used to associate BFD with EFM:

 Copyright © Huawei Technologies Co., Ltd.

- **oam-bind efm interface bfd-session**
- **oam-bind ingress bfd-session egress efm interface**
- **oam-bind ingress efm interface egress bfd-session**

Choose the preceding commands in different scenarios according to **Table 18-39**.

Table 18-39 Association between EFM and BFD

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and BFD	Use the **oam-bind efm interface bfd-session** command to configure EFM and BFD to notify each other of faults.	Run the following commands at a random order: • Run the **oam-bind ingress efm interface egress bfd-session** command to configure EFM to notify BFD of faults. • Run the **oam-bind ingress bfd-session egress efm interface** command to configure BFD to notify EFM of faults.
Unidirectional fault notification between EFM and BFD	Choose either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress bfd-session** command to configure EFM to notify BFD of faults. • Run the **oam-bind ingress bfd-session egress efm interface** command to configure BFD to notify EFM of faults.	None

Prerequisites

A BFD session has been created and EFM OAM has been enabled on an interface.

Precautions

The following types of BFD sessions can be used:

- Static BFD for LSP (LDP, TE, TE LSP, static LSP, and vll pw) sessions (a PST is required)
- BFD for IP sessions (no PST is required)

Example

Configure BFD to report faults to EFM OAM through Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress bfd-session 50 egress efm interface ethernet 2/0/0
```

Related Topics

18.7.7 efm enable

18.7.32 oam-bind ingress efm interface egress bfd-session

Function

The **oam-bind ingress efm interface egress bfd-session** command configures EFM OAM to report faults to BFD.

The **undo oam-bind ingress efm interface egress bfd-session** command cancels the configuration.

By default, EFM OAM from sending fault messages to BFD is not configured.

Format

oam-bind ingress efm interface *interface-type interface-number* **egress bfd-session** *bfd-session-id*

undo oam-bind ingress efm interface *interface-type interface-number* **egress bfd-session** *bfd-session-id*

Parameters

Parameter	Description	Value
bfd-session-id	Specifies the ID of a BFD session.	The value is an integer that ranges from 1 to 8191.
interface-type interface-number	Specifies the type and number of an Ethernet interface. The interface must have been enabled with EFM OAM. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If EFM is deployed at one side and BFD is deployed at another side of a device, associate EFM with BFD on the device. This allows EFM and BFD to notify each other of faults and ensures reliable service transmission.

Association between EFM and BFD is bidirectional:

- If EFM detects a link fault, it will notify BFD of the fault.
- If BFD detects a link fault, it will notify EFM of the fault.

The following commands are used to associate BFD with EFM:

- **oam-bind efm interface bfd-session**
- **oam-bind ingress bfd-session egress efm interface**
- **oam-bind ingress efm interface egress bfd-session**

Choose the preceding commands in different scenarios according to **Table 18-40**.

Table 18-40 Association between EFM and BFD

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and BFD	Use the **oam-bind efm interface bfd-session** command to configure EFM and BFD to notify each other of faults.	Run the following commands at a random order: • Run the **oam-bind ingress efm interface egress bfd-session** command to configure EFM to notify BFD of faults. • Run the **oam-bind ingress bfd-session egress efm interface** command to configure BFD to notify EFM of faults.
Unidirectional fault notification between EFM and BFD	Choose either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress bfd-session** command to configure EFM to notify BFD of faults. • Run the **oam-bind ingress bfd-session egress efm interface** command to configure BFD to notify EFM of faults.	None

Prerequisites

A BFD session has been created and EFM OAM has been enabled globally and on an interface.

Precautions

The following types of BFD sessions can be used:

- Static BFD for LSP (LDP, TE, TE LSP, static LSP, and VLL PW) sessions (a PST is required)
- BFD for IP sessions (no PST is required)

Example

Configure EFM OAM to report faults to BFD through Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress efm interface ethernet 2/0/0 egress bfd-session 50
```

Related Topics

18.7.7 efm enable

18.7.33 oam-bind ingress efm interface trigger if-down egress interface

Function

The **oam-bind ingress efm interface trigger if-down egress interface** command enables EFM to report faults to an interface.

The **undo oam-bind ingress efm interface trigger if-down egress interface** command cancels the configuration.

By default, unidirectional transmission of information about a fault from EFM OAM to an interface is not configured.

Format

oam-bind ingress efm interface *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2*

undo oam-bind ingress efm interface *interface-type1 interface-number1* **trigger if-down egress interface** *interface-type2 interface-number2*

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. • *interface-type1* specifies the interface type. • *interface-number1* specifies the interface number.	-

Parameter	Description	Value
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 18-41 describes the implementation of association between EFM and an interface.

 Copyright © Huawei Technologies Co., Ltd.

Table 18-41 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The command displays **oam-bind ingress interface egress efm interface trigger if-down** and**oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Precautions

Before enabling EFM to report faults to an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.

- EFM and the interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

Ingress EFM reports faults to the specified interface.

Example

Configure EFM to report a fault to Ethernet2/0/1.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress efm interface ethernet 2/0/0 trigger if-down egress interface
ethernet 2/0/1
```

Related Topics

18.7.7 efm enable

18.7.36 oam-mgr

18.7.34 oam-bind ingress interface egress efm interface trigger if-down

18.7.30 oam-bind efm interface trigger if-down interface

18.7.34 oam-bind ingress interface egress efm interface trigger if-down

Function

The **oam-bind ingress interface egress efm interface trigger if-down** command enables an interface to report faults to EFM OAM.

The **undo oam-bind ingress interface egress efm interface trigger if-down** command cancels the configuration.

By default, unidirectional transmission of information about a fault from an interface to EFM OAM is disabled.

Format

oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down**

undo oam-bind ingress interface *interface-type1 interface-number1* **egress efm interface** *interface-type2 interface-number2* **trigger if-down**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM OAM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 18-42 describes the implementation of association between EFM and an interface.

Table 18-42 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Configuration Impact

After an interface goes Down, the status of the associated EFM OAM session does not change. However, the device configured with association sends a message to inform the peer of the fault and triggers the peer to generate an alarm.

Precautions

Before enabling an interface to report faults to EFM OAM, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and an interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.

The ingress interface reports faults to egress EFM.

Example

Configure Ethernet2/0/0 to report a fault to EFM.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress interface ethernet 2/0/0 egress efm interface ethernet 2/0/1
trigger if-down
```

18.7.35 oam-bind interface efm interface trigger if-down

Function

The **oam-bind interface efm interface trigger if-down** command enables bidirectional transmission of fault messages between an interface and EFM OAM.

The **undo oam-bind interface efm interface trigger if-down** command cancels the configuration.

By default, bidirectional transmission of information about a fault between an interface and EFM OAM is not configured.

Format

oam-bind interface *interface-type1 interface-number1* **efm interface** *interface-type2 interface-number2* **trigger if-down**

undo oam-bind interface *interface-type1 interface-number1* **efm interface** *interface-type2 interface-number2* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type1 interface-number1	Specifies the type and number of the interface enabled with EFM. ● *interface-type1* specifies the interface type. ● *interface-number1* specifies the interface number.	-

Parameter	Description	Value
interface-type2 interface-number2	Specifies the type and number of the interface bound to an EFM session. ● *interface-type2* specifies the interface type. ● *interface-number2* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Association between EFM and an interface in the OAM management view is bidirectional:

- After EFM OAM detects a fault, the OAM module notifies the interface associated with EFM OAM of the fault. Then the interface goes Down. After EFM detects that the fault is rectified, the OAM module notifies the interface associated with EFM OAM. Then the interface goes Up.
- After the interface goes Down, the OAM module notifies EFM OAM of the interface Down event.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

The following commands are used to configure association between EFM and an interface in the OAM management view:

- **oam-bind efm interface trigger if-down interface**
- **oam-bind interface efm interface trigger if-down**
- **oam-bind ingress efm interface trigger if-down egress interface**
- **oam-bind ingress interface egress efm interface trigger if-down**

Table 18-43 describes the implementation of association between EFM and an interface.

 Copyright © Huawei Technologies Co., Ltd.

Table 18-43 Association between EFM and an EFM-incapable interface

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and an interface	Choose either of the following commands (the two commands have the same function): • To specify an EFM OAM session first, run the **oam-bind efm interface trigger if-down interface** command. • To specify an interface first, run the **oam-bind interface efm interface trigger if-down** command. **NOTE** After configuring bidirectional fault notification between EFM and an interface, run the **display current-configuration** command to view the current configuration. The command displays **oam-bind ingress interface egress efm interface trigger if-down** and **oam-bind ingress efm interface trigger if-down egress interface** commands, but does not display the **oam-bind efm interface trigger if-down interface** or **oam-bind interface efm interface trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands at a random order: • **oam-bind ingress efm interface trigger if-down egress interface** • **oam-bind ingress interface egress efm interface trigger if-down**
Unidirectional fault notification between EFM and an interface	Choose either of the following commands based on the transmission direction: • To configure EFM OAM to report faults to an interface, run the **oam-bind ingress efm interface trigger if-down egress interface** command. • To configure an interface to report faults to EFM OAM, run the **oam-bind ingress interface egress efm interface trigger if-down** command.	None

Prerequisites

Basic EFM OAM functions have been configured.

Precautions

When configuring bidirectional transmission of fault messages between EFM and an interface, pay attention to the following points:

- EFM has been enabled on the interface specified by **efm interface** *interface-type2 interface-number2*.
- EFM and the interface are associated with each other. After an interface is associated with an EFM session, the interface cannot be associated with other EFM sessions. Similarly, when EFM is bound to an interface, EFM cannot be bound to other interfaces.
- Association between EFM and an EFM-capable interface and association between EFM and an EFM-incapable interface cannot be configured together.
- A physical interface associated with EFM cannot be the one that EFM monitors. If EFM is associated with a physical interface that it monitors, the link is locked.

Example

Configure bidirectional transmission of fault messages between EFM and Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind interface ethernet 2/0/0 efm interface ethernet 1/0/2 trigger if-down
```

Related Topics

18.7.7 efm enable

18.7.36 oam-mgr

18.7.33 oam-bind ingress efm interface trigger if-down egress interface

18.7.34 oam-bind ingress interface egress efm interface trigger if-down

18.7.36 oam-mgr

Function

The **oam-mgr** command displays the OAM management view.

The **undo oam-mgr** command exits from the OAM management view.

Format

oam-mgr

undo oam-mgr

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

CFM can advertise fault information to interfaces or protocol modules. Ethernet OAM fault advertisement is implemented by an OAM manager, application modules, and detection modules. An OAMMGR module associates one module with another. A detection module monitors link status and network performance. If a detection module detects a fault, it instructs the OAMMGR module to notify an application module or another detection module of the fault. After receiving the notification, the application or detection module takes measures to prevent a communication interruption or service quality deterioration. Run the **oam-mgr** command to display the MGR view before associating the CFM module and other modules.

Example

Enter the OAM management view.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr]
```

18.7.37 snmp-agent trap enable feature-name efm

Function

The **snmp-agent trap enable feature-name efm** command enables the trap function for the EFM module.

The **undo snmp-agent trap enable feature-name efm** command disables the trap function for the EFM module.

By default, the trap function is disabled for the EFM module.

Format

snmp-agent trap enable feature-name efm [**trap-name** { **nonthreshold** | **threshold** | **nonthredholdrecovery** | **dyinggasp** | **loopbackfailed** }]

undo snmp-agent trap enable feature-name efm [**trap-name** { **nonthreshold** | **threshold** | **nonthredholdrecovery** | **dyinggasp** | **loopbackfailed** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
nonthreshold	Enables the device to send a trap when a non-threshold crossing event occurs.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
threshold	Enables the device to send a trap when a threshold crossing event occurs.	-
nonthredholdrecovery	Enables the device to send a trap when a non-threshold fault is rectified.	-
loopbackfailed	Enables the device to send a trap when loopback fails.	-
dyinggasp	Enables the device to send a trap when a remote Dying Gasp event occurs.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

You can specify **trap-name** to enable the trap function for one or more events.

Example

Enable the device to send a trap when a non-threshold crossing event occurs.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name efm trap-name nonthreshold
```

18.7.38 test-packet start

Function

The **test-packet start** command configures the device to send test packets.

Format

test-packet start interface *interface-type interface-number* [**-c** *count* | **-s** *size*] *

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the outbound interface of test packets. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
-c *count*	Specifies the number of test packets to be sent.	The value is an integer that ranges from 1 to 65535. The default value is 5.
-s *size*	Specifies the length of a test packet.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 64 bytes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After remote loopback is enabled on the device, run the **test-packet start** command on an interface in active mode to configure the device to send test packets. Then check link connectivity and performance based on returned test packets.

Press **Ctrl+C** to stop sending test packets. After using this command to send test packets, use the **display test-packet result** command to view the test result.

Precautions

During test packet transmission, parameters of sent test packets cannot be changed.

Example

Send test packets from outbound interface Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] test-packet start interface ethernet 2/0/0
```

Related Topics

18.7.6 display test-packet result

18.8 CFM Configuration Commands

18.8.1 cfm enable (system view)

Function

The **cfm enable** command enables Connectivity Fault Management (CFM) globally.

The **undo cfm enable** command disables CFM globally.

By default, CFM is disabled globally.

Format

cfm enable

undo cfm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on links, enable CFM globally.

Precautions

If you use the **undo cfm enable** command to disable CFM globally, the device automatically deletes all the CFM configurations, including the configurations of MDs, MAs, MEPs and RMEPs.

All the configuration commands related to the CFM function are valid only after CFM is enabled globally.

Example

Enable CFM globally.

```
<Huawei> system-view
[Huawei] cfm enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

18.8.16 display oam global configuration

18.8.2 active time

Function

The **active time** command sets the RMEP activation time.

The **undo active time** command deletes the RMEP activation time.

By default, the RMEP activation time is 0 seconds.

Format

active time *time*

undo active time

Parameters

Parameter	Description	Value
time *time*	Specifies the RMEP activation time.	The value ranges from 0 to 600, in seconds.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **remote-mep ccm-receive enable** command to enable the local device to receive CCMs from an RMEP in the same MA, the local device generates an alarm about the RMEP connectivity fault in the following situations:

- A connectivity fault is detected between the local MEP and the RMEP using CC.
- The physical link works normally between the local MEP and the RMEP. The remote device is not configured with a MEP when the connectivity check is performed, or the MEP is configured after the connectivity check. In this case, if the local MEP does not receive the CCM from the RMEP within three consecutive intervals for sending CCMs, the local device considers a connectivity fault to have occurred between the local MEP and the RMEP.

  The RMEP connectivity fault alarm is generated incorrectly. To solve the problem, set the RMEP activation time.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If the RMEP activation time is set on the local device that is enabled to receive CCMs from a certain RMEP, the local device can receive CCMs at the configured RMEP activation time. That is, the activation time is the time reserved for configuring the RMEP.

At the RMEP activation time, if the local MEP does not receive any CCMs during three consecutive CCM sending intervals, a connectivity fault occurs between the local MEP and the RMEP. Then the local device generates an alarm about the RMEP connectivity fault.

If the local device uses the default RMEP activation time, the local MEP receives CCMs from the RMEP immediately after the local device is enabled to receive CCMs from the RMEP.

NOTE

The RMEP activation time takes effect only for subsequent RMEPs in an MA, but is invalid for existing RMEPs in the MA.

Example

Set the RMEP activation time to 30s.

```
<Huawei> system-view
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] active time 30
```

Related Topics

18.8.7 cfm md

18.8.17 ma

18.8.30 remote-mep ccm-receive enable

18.8.6 ccm-interval

18.8.3 alarm finish time

Function

The **alarm finish time** command sets the clear alarm anti-jitter time.

The **undo alarm finish time** command restores the default clear alarm anti-jitter time.

By default, the clear alarm anti-jitter time is 10000 ms.

Format

alarm finish time *time*

undo alarm finish time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time *time*	Specifies the clear alarm anti-jitter time.	The value ranges from 0 to 30000, in milliseconds. The step is 500, for example, the anti-jitter time can be 500, 1000, or 1500.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a link fault or link recovery, CFM sends an alarm to the NMS. If CFM detects link faults or recoveries frequently, alarm flapping occurs.

Precautions

To suppress alarm flapping, run this command to set the clear alarm anti-jitter time. This prevents the NMS or system from being affected by frequently reported alarms. When detecting link recovery, CFM compares the current link recovery time with the last time the fault was generated. CFM sends an alarm to the NMS only when the time difference is at least as large as the clear alarm anti-jitter time.

Example

Set the clear alarm anti-jitter time to 2000 ms.

```
<Huawei> system-view
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] alarm finish time 2000
```

Related Topics

18.8.7 cfm md

18.8.17 ma

18.8.4 alarm occur time

Function

The **alarm occur time** command sets the alarm anti-jitter time.

The **undo alarm occur time** command restores the default alarm anti-jitter time.

 Copyright © Huawei Technologies Co., Ltd.

By default, the alarm anti-jitter time is 2500 ms.

Format

alarm occur time *time*

undo alarm occur time

Parameters

Parameter	Description	Value
time *time*	Specifies the alarm anti-jitter time.	The value ranges from 0 to 30000, in milliseconds. The step is 500, for example, the anti-jitter time can be 500, 1000, or 1500.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When detecting a link fault or link recovery, CFM sends an alarm to the NMS. If CFM detects link faults or recoveries frequently, alarm flapping occurs.

Precautions

To suppress alarm flapping, run this command to set the alarm anti-jitter time. This prevents the NMS or system from being affected by frequently reported alarms. When detecting link recovery, CFM compares the current link recovery time with the last time the fault was generated. CFM sends an alarm to the NMS only when the time difference is at least as large as the alarm anti-jitter time.

Example

Set the alarm anti-jitter time to 2000 ms.

```
<Huawei> system-view
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] alarm occur time 2000
```

Related Topics

18.8.7 cfm md

18.8.17 ma

 Copyright © Huawei Technologies Co., Ltd.

18.8.5 alarm rdi track-action disable

Function

The **alarm rdi track-action disable** command disables CFM from being triggered when a Remote Defect Indication (RDI) alarm is generated.

The **undo alarm rdi track-action disable** command enables CFM to be triggered when an RDI alarm is generated.

By default, CFM is triggered when an RDI alarm is generated.

Format

alarm rdi track-action oam-mgr disable

undo alarm rdi track-action oam-mgr disable

Parameters

Parameter	Description	Value
oam-mgr	Indicates that CFM is associated with another feature in the OAM management view.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When CFM is associated with another feature and the device receives an RDI alarm, run this command to disable CFM from being triggered.

Prerequisites

An MD has been created using the **cfm md** *md-name* command, and an MA has been created using the **ma** *ma-name* command.

Example

Disable CFM from being triggered when an RDI alarm is generated.

```
<Huawei> system-view
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] alarm rdi track-action oam-mgr disable
```

18.8.6 ccm-interval

 Copyright © Huawei Technologies Co., Ltd.

Function

The **ccm-interval** command sets the interval at which a Maintenance Association End Point (MEP) sends or detects Continuity Check Messages (CCMs) in an MA.

The **undo ccm-interval** command restores the default interval.

By default, a MEP in an MA sends or detects CCMs every 1000 ms.

Format

ccm-interval *interval*

undo ccm-interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a MEP sends or detects CCMs.	The value is an integer, in milliseconds. The value is 10, 1000, or 10000.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command sets the interval at which a MEP in an MA sends or detects CCMs.

Precautions

All the MEPs in an MA must send or detect CCMs at the same interval.

Multiple MAs can be configured on a device. The interval at which CCMs are sent or detected cannot be changed on the device in an MA if any of the following operations has been performed:

- The device is enabled to send CCMs using the **mep ccm-send enable** command.
- The device is enabled to receive CCMs using the **remote-mep ccm-receive enable** command.

The **undo mep ccm-send enable** or **undo mep ccm-receive enable** command must be run before the interval is changed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval for sending or detecting CCMs to 1000 ms within the MA **ma1** where the device is not enabled to send or receive CCMs.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] ccm-interval 1000
```

Set the interval for sending or detecting CCMs to 1000 ms within the MA **ma1** where the device is enabled to send and receive CCMs.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] undo mep ccm-send enable
[Huawei-md-md1-ma-ma1] undo remote-mep ccm-receive enable
[Huawei-md-md1-ma-ma1] ccm-interval 1000
```

Related Topics

18.8.33 mep ccm-send enable

18.8.30 remote-mep ccm-receive enable

18.8.7 cfm md

Function

The **cfm md** command creates an MD and displays the MD view, or displays the view of an existing MD.

The **undo cfm md** command deletes an MD.

Format

cfm md *md-name* [**format** { **no-md-name** | **dns** *dns-md-format-name* | **mac-address** *mac-md-format-name* | **string** *string-md-format-name* }] [**level** *level*]

undo cfm md [*md-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The name of an MD on a device must be unique. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
no-md-name	Indicates that the MA ID field of a sent packet does not contain an MD name.	-
dns *dns-md-format-name*	Specifies the DNS name used as the MD name carried in packets.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
mac-address *mac-md-format-name*	Specifies an MD name carried in packets. The value is composed of the MAC address plus a two-digit integer, and is in the format of H-H-H:U<0-65535>. An H is a hexadecimal number of 4 digits and the U is an integer. For example, the value is 0001-0001-0001:1.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
string *string-md-format-name*	Specifies an MD name as a character string.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
level *level*	Specifies the level of an MD.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher MD priority. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure CFM to identify and locate faults on links, use this command to create an MD.

Precautions

- All the CFM-enabled devices of an ISP can be added to the same MD.

  NOTE

  When 802.1ag packets in a low-level MD enter a high-level MD, the 802.1ag packets are discarded. 802.1ag packets in a high-level MD can traverse a low-level MD. 802.1ag packets in an MD cannot traverse the MD of the same level.

  Only IEEE Standard 802.1ag-2007 supports **format**, **no-md-name**, **dns** *dns-md-format-name*, **mac-address** *mac-md-format-name*, and **string** *string-md-format-name*.

- The MD name format can be specified during MD configuration. Each MD can be configured with only one name format and one level. You can use this command to enter the view of the existing MD but cannot change the name format and level of the existing MD. To change the name format and level of the existing MD, delete the MD and then use the cfm md command to create an MD.
- When an MD is deleted, a device automatically deletes all the configurations of MAs, MEPs and RMEPs within the MD.
- The MA, MEP, and RMEP must be created within an MD, so you must create an MD before creating the MA, MEP, and RMEP.
- The level of the MD with **format** specified cannot be changed.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Create an MD named **mdcustomer** at level 4.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md mdcustomer level 4
```

Change the level of **mdcustomer** from 4 to 6.

```
<Huawei> system-view
[Huawei] undo cfm md mdcustomer
Warning: Deleting the MD(s) will delete all information about the MA(s). Continue?[Y/N]:y
[Huawei] cfm md mdcustomer level 6
```

 Copyright © Huawei Technologies Co., Ltd.

Create an MD named **mdcustomer** at level 4, with the MD name in no-md-name format.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md mdcustomer format no-md-name level 4
```

Related Topics

18.8.1 cfm enable (system view)
18.8.11 display cfm md

18.8.8 cfm default md

Function

The **cfm default md** command creates the default MD.

The **undo cfm default md** command deletes the default MD.

By default, the default MD is not created.

Format

cfm default md [**level** *level*]

undo cfm default md

Parameters

Parameter	Description	Value
level *level*	Specifies the level of the default MD.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher MD priority. By default, the level of the default MD is 7 (highest level).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To identify and locate faults on an MP or a link in an MD, create the default MD.

Precautions

The level of the default MD must be higher than that of all MDs to which MEPs configured on the local device belong. In addition, the default MD must be of the

same level as the higher-level MD. The default MD transmits higher-level CCMs and creates MIPs to send LTR messages.

On the device configured with the default MD, a MIP can be created based on the default MD in the MA that is not associated with a VLAN. The interface where the default MD is configured generates a MIP based on the MIP creation rule.

To modify the MD level, delete the default MD and reconfigure it.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Create the default MD at level 6.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm default md level 6
```

Related Topics

18.8.1 cfm enable (system view)

18.8.12 display cfm default md

18.8.9 cfm portid-tlv type

Function

The **cfm portid-tlv type** command sets the portid-tlv type for trace packets.

The **undo cfm portid-tlv type** command restores the default portid-tlv type for trace packets.

By default, the portid-tlv type in trace packets is in character string format.

Format

cfm portid-tlv type { **interface-name** | **local** }

undo cfm portid-tlv type

Parameters

Parameter	Description	Value
interface-name	Indicates that the type of the port ID TLV is in character string format.	-
local	Indicates that the portid-tlv type is in Huawei proprietary format.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When using the trace function, you need to specify the name format of inbound and outbound interfaces of a device. You can use the **cfm portid-tlv type** command to set the name type of the specified interface.

Precautions

Vendors may use different TLV types. To implement interworking between Huawei devices and non-Huawei devices, configure **interface-name** to specify the interface name type in character string format.

If all the devices running on the entire network are Huawei data communications devices, to interwork with devices running different versions, configure **local** to specify the interface name type in Huawei proprietary format.

Example

Set the type of the port ID TLV in character string format.

```
<Huawei> system-view
[Huawei] cfm portid-tlv type interface-name
```

18.8.10 display cfm ma

Function

The **display cfm ma** command displays detailed information about MAs.

Format

display cfm ma [**md** *md-name* [**ma** *ma-name*]]

Parameters

Parameter	Description	Value
md *md-name*	Displays detailed MA information in a specified MD. If the parameter is not specified, detailed information about all MAs in all MDs is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ma *ma-name*	Displays detailed information about the specified MA. If *md-name* is specified but this parameter is not specified, detailed information about all the MAs in the MD specified by *md-name* is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an MA is configured or if CFM cannot work properly, use this command to check the MA configuration and the numbers of MEPs and RMEPs in the MA.

Example

Display detailed information about the MA named **ma1** in the MD named **md1**.

```
<Huawei> display cfm ma md md1 ma ma1
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA Name            : ma1
 MA Name Format     : string
 Interval           : 1000
 Priority           : 7
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MEP Number         : 0
 RMEP Number        : 0
 Suppressing Alarms : No
 Sending AIS Packet : No
 Interface TLV      : disabled
 RDI Track-action   : all-enabled
```

Display detailed information about all the MAs in the specified MD.

```
<Huawei> display cfm ma md md1
The total number of MAs is : 1
--------------------------------------------------
 MD Name            : md1
```

```
MD Name Format     : string
Level              : 0
MIP Create-type    : none
SenderID TLV-type  : defer
MA Name            : ma1
MA Name Format     : string
Interval           : 1000
Priority           : 7
VLAN ID            : --
VSI Name           : --
L2VC ID            : --
MEP Number         : 0
RMEP Number        : 0
Suppressing Alarms : No
Sending AIS Packet : No
Interface TLV      : disabled
RDI Track-action   : all-enabled
```

Table 18-44 Description of the **display cfm ma** command output

Item	Description
MD Name	Name of the MD.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string
Level	Level of an MD. The value ranges from 0 to 7.
MIP Create-type	MIP creation rule: ● default ● explicit ● none
SenderID TLV-type	Type of the Sender ID TLV filled in the CCM: ● none ● chassis ● manage ● chassisManage ● defer
MA Name	Name of the MA.
Interval	Interval at which CCMs are sent in an MA.
Priority	802.1p priority of CFM packets in an MA. The value ranges from 0 to 7. A larger value indicates a higher priority. The default value is 7.
VLAN ID	ID of the VLAN associated with an MA.
VSI Name	Name of the VSI associated with an MA.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MEP Number	Number of MEPs in an MA.
RMEP Number	Number of RMEPs in an MA.
Suppressing Alarms	Whether the current device is suppressing alarms
Sending AIS Packet	Whether the current device is sending AIS packets
Interface TLV	Whether the CCM TLV is enabled: ● disabled ● enabled
RDI Track-action	Whether CFM is triggered when an RDI alarm is generated.

Related Topics

18.8.6 ccm-interval
18.8.17 ma
18.8.18 map
18.8.19 mep mep-id
18.8.27 packet-priority

18.8.11 display cfm md

Function

The **display cfm md** command displays MD information, including the MD name and level.

Format

display cfm md [*md-name*]

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD. If this parameter is not specified, information about all the MDs created on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display cfm md** command displays MD information, including the MD level, MD name format, MIP creation rule in the MD, and Sender ID TLV type. In addition, you can view brief information about MAs in the MD, including the MA name, interval at which CCMs are sent, ID of the VLAN associated with the MA, and name of the VSI associated with the MA. If *md-name* is not specified, information about all the created MDs is displayed.

Example

Display information about the MD named **mdcustomer**.

```
<Huawei> display cfm md mdcustomer
 MD Name            : mdcustomer
 MD Name Format     : string
 Level              : 0
 MIP Create-type    : none
 SenderID TLV-type  : defer
 MA list            :
 MA Name            : ma
 MA Name Format     : string
 Interval           : 1000
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
```

Table 18-45 Description of the **display cfm md** command output

Item	Description
MD Name	Name of the MD.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MIP Create-type	MIP creation rule: ● default ● explicit ● none
SenderID TLV-type	Type of the Sender ID TLV filled in the CCM: ● none ● chassis ● manage ● chassisManage ● defer
MA list	Information about MAs in the MD.
MA Name	Name of the MA.
Interval	Interval at which CCMs are sent.
VLAN ID	ID of the VLAN associated with an MA.
VSI Name	Name of the VSI associated with an MA.

Related Topics

18.8.7 cfm md

18.8.12 display cfm default md

Function

The **display cfm default md** command displays information about the default MD.

Format

display cfm default md

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display cfm default md** command displays information about the level of the default MD, MIP creation rule, sender ID TLV type, and the VLAN list associated with the default MD.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Example

Display information about the default MD.

```
<Huawei> display cfm default md
Level   MIP-Create-type   SenderID TLV-type   VLAN-List
-----------------------------------------------------------------------------------------
7       default          defer               100 to 200 2049
```

Table 18-46 Description of the **display cfm md** command output

Item	Description
Level	Level of the default MD. The value ranges from 0 to 7. A higher level represents a higher priority of the default MD.
MIP-Create-type	MIP creation rule: ● default ● explicit ● none
SenderID TLV-type	Type of the Sender ID TLV filled in the CCM: ● none ● chassis ● manage ● chassisManage ● defer
VLAN-List	IDs of VLANs associated with the default MD.

Related Topics

18.8.1 cfm enable (system view)
18.8.8 cfm default md

18.8.13 display cfm mep

Function

The **display cfm mep** command displays MEP information in a specified MD and MA.

Format

display cfm mep [**md** *md-name* [**ma** *ma-name* [**mep-id** *mep-id*]]]

Parameters

Parameter	Description	Value
md *md-name*	Displays MEP information in a specified MD. If this parameter is not specified, information about MEPs in all MDs and MAs on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma *ma-name*	Displays MEP information in a specified MA. If this parameter is not specified and *ma-name* is specified, information about MEPs in all the MAs of a specified MD on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
mep-id *mep-id*	Displays information about a specified MEP. *mep-id* specifies the ID of the MEP.	The value is an integer that ranges from 1 to 8191.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After a MEP is configured or if CFM cannot work properly, use this command to check the MEP configuration.

Example

Display information about the MEP with an ID of 10 in in the MA named **ma1** of the MD named **md1**.

```
<Huawei> display cfm mep md md1 ma ma1 mep-id 10
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma1
 MEP ID             : 2
```

```
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : Ethernet2/0/0
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 0002-0003-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
```

Display information about all MEPs in the MA named **ma1** of the MD named **md1**.

```
<Huawei> display cfm mep md md1 ma ma1
The total number of MEPs is : 1
--------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma1
 MEP ID             : 2
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : Ethernet2/0/0
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 0002-0003-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
```

Display information about all MEPs in the MD named **md1**.

```
<Huawei> display cfm mep md md1
The total number of MEPs is : 2
--------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma1
 MEP ID             : 2
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : Ethernet2/0/0
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 0002-0003-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma2
 MEP ID             : 4
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
```

```
Interface Name     : Ethernet0/0/2
CCM Send           : enabled
Direction          : outward
MAC Address        : 0002-0003-0161
MEP Pe-vid         : --
MEP Ce-vid         : --
MEP Vid            : --
Alarm Status       : LOC
Alarm AIS          : enabled
Alarm RDI          : enabled
```

Table 18-47 Description of the **display cfm mep** command output

Item	Description
MD Name	Name of the MD.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority of the MD. **NOTE** If the level of a MEP on an intermediate node is higher than or equal to that on the source node, run the **cfm md** command to change the level of the MEP on the intermediate node to be lower than that on the source node.
MA Name	Name of an MA.
MEP ID	ID of the MEP.
VLAN ID	ID of the VLAN associated with an MA.
VSI Name	Name of the VSI associated with an MA.
Interface Name	Interface where a MEP is configured. If a MEP is based on VLANIF interfaces, this field is displayed as --.
CCM Send	Whether the MEP is enabled to send CCMs: ● enabled: The MEP is enabled to send CCMs. ● disabled: The MEP is disabled from sending CCMs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Direction	Type of the MEP: ● inward: indicates an inward-facing MEP. An inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA, but does not send 802.1ag packets to the interface where the MEP is configured. ● outward: indicates an outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured. **NOTE** If the MEP direction is incorrect, run the **mep mep-id** command to configure a correct direction.
MAC Address	MAC address of the MEP.
MEP Pe-vid	Outer VLAN ID of the QinQ interface where the MEP is configured.
MEP Ce-vid	Inner VLAN ID of the QinQ interface where the MEP is configured.
MEP Vid	VLAN ID of the Dot1q interface where the MEP is configured.
Alarm Status	Alarm type: ● unexpectedMEP: The MEP receives CCMs with an unexpected flag. ● MEP ID mismerge: The MEP ID in received CCMs is different from the configured MEP ID. ● unexpectedPeriod: The interval in the received CCMs is different from the configured interval. ● unexpectedMAC: The MEP's MAC address in the received CCM is different from the MAC address of the RMEP. ● LOC: At least one session between the MEP and an RMEP is terminated. ● RDI: The MEP receives CCMs with the RDI.
Alarm AIS	Whether the device is enabled to report AIS alarms: ● enable ● disable
Alarm RDI	Whether the device is enabled to report RDI alarms: ● enable ● disable

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

18.8.19 mep mep-id

18.8.33 mep ccm-send enable

18.8.14 display cfm mp-info

Function

The **display cfm mp-info** command displays information about CFM objects on a specified interface or in a VLAN.

Format

display cfm mp-info [**interface** *interface-type interface-number*] [**level** *md-level*] [**inward** | **outward**] [**vlan** *vlanid* | **no-associated-vlan**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays CFM information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
level *md-level*	Specifies the level of an MD.	The value is an integer that ranges from 0 to 7. The default value is 0.
inward	Indicates the inward-facing MEP. An inward-facing MEP sends 802.1ag packets through all interfaces in a VLAN associated with an MA, except the interface on which the MEP is configured. That is, the inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA.	-
outward	Indicates the outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured.	-
vlan *vlanid*	Displays CFM information in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-associated-vlan	Indicates the MP that is not associated with a VLAN.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display cfm mp-info** command displays information about CFM objects and the relationship between MPs on the interface so that you can configure MEPs correctly.

Prerequisites

CFM has been enabled globally using the **cfm enable (system view)** command.

Precautions

Multiple MEPs can be configured and multiple MIPs can be generated on an interface; however, the levels of MEPs or MIPs must be the same. Incorrect configurations can cause CCM leaks to occur, or LBR or LTR messages to be sent incorrectly.

Example

Display information about the specified interface, MD level, MEP type, and VLAN.

```
<Huawei> display cfm mp-info interface ethernet 2/0/0
The total number of MPs is : 1
The number of MEPs is : 1. The number of MIPs is : 0.
--------------------------------------------------
 MD Name            : md1
 MD Name Format     : string
 Level              : 0
 MA Name            : ma2
 MEP ID             : 4
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 Interface Name     : Ethernet2/0/0
 CCM Send           : enabled
 Direction          : outward
 MAC Address        : 0002-0003-0161
 MEP Pe-vid         : --
 MEP Ce-vid         : --
 MEP Vid            : --
 Alarm Status       : LOC
 Alarm AIS          : enabled
 Alarm RDI          : enabled
```

Table 18-48 Description of the **display cfm mp-info** command output

Item	Description
Interface Name	Name of the interface.
MD Name	Name of the MD.
MD Name Format	Format of the MD name: ● no-md-name ● dns ● mac-address ● string
Level	Level of the MD, MA, or MP. The value ranges from 0 to 7. A higher level indicates a higher priority.
MA Name	Name of the MA.
MEP ID	ID of the MEP.
CCM Send	Whether the MEP is enabled to send CCMs: ● enabled ● disabled
L2VC ID	ID of the L2VC associated with an MA.
Direction	Type of the MEP: ● inward ● outward
VLAN ID	ID of the VLAN associated with an MA.
VSI Name	Name of the VSI associated with the MA.
MAC Address	MAC address of the MEP or MIP. **NOTE** An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.

Related Topics

18.8.33 mep ccm-send enable
18.8.19 mep mep-id

18.8.15 display cfm remote-mep

Function

The **display cfm remote-mep** command displays information about RMEPs in a specified MD and MA, including:

- Name and level of the MD
- Name of the MA and VLAN associated with the MA
- ID of the RMEP
- MAC address of the RMEP
- Whether the MEP is enabled to receive CCMs from the RMEP
- Alarm status

Format

display cfm remote-mep md *md-name* **ma** *ma-name* **mep-id** *mep-id*

display cfm remote-mep [**md** *md-name* [**ma** *ma-name*]] [**cfm-state** { **up** | **down** | **disable** }]

Parameters

Parameter	Description	Value
md *md-name*	Displays information about RMEPs in a specified MD. If this parameter is not specified, information about RMEPs in all MDs and MAs on the device is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma *ma-name*	Displays information about RMEPs in a specified MA. If this parameter is not specified, information about RMEPs in all MAs in a specified MD is displayed.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
mep-id *mep-id*	Displays information about a specified RMEP. *mep-id* specifies the ID of the RMEP.	The value is an integer that ranges from 1 to 8191.
cfm-state	Displays RMEP information based on the CFM status.	-
up	Displays information about RMEPs in Up state.	-
down	Displays information about RMEPs in Down state.	-
disable	Displays information about RMEPs in disabled state.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After an RMEP is configured or if CFM cannot work properly, use this command to check the RMEP configuration.

You can specify **cfm-state** to view RMEP information in the specified CFM state.

Example

Display information about the RMEP with an ID of 50 in the MA named **ma1** of the MD named **md1**.

```
<Huawei> display cfm remote-mep md md1 ma ma1 mep-id 50
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 5
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : enabled
 CFM Status         : down
 Alarm Status       : LOC
 Interface TLV      : --
 Connect Status     : up
```

Display information about all RMEPs in the MA named **ma1** of the MD named **md1**.

```
<Huawei> display cfm remote-mep md md1 ma ma1
The total number of RMEPs is : 1
The status of RMEPs : 0 up, 1 down, 0 disable
--------------------------------------------------
 MD Name            : md1
 Level              : 0
 MA Name            : ma1
 RMEP ID            : 5
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : enabled
 CFM Status         : down
 Alarm Status       : LOC
 Interface TLV      : --
 Connect Status     : up
```

Display information about all the RMEPs configured on the local device.

```
<Huawei> display cfm remote-mep
The total number of RMEPs is : 1
```

```
The status of RMEPs : 0 up, 0 down, 1 disable
--------------------------------------------------
 MD Name            : md
 Level            : 0
 MA Name            : ma
 RMEP ID            : 1
 VLAN ID            : --
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : disabled
 Trigger-If-Down    : disabled
 CFM Status         : disabled
 Alarm Status       : none
 Interface TLV      : --
 Connect Status     : up
```

Display information about all RMEPs in Down state.

```
<Huawei> display cfm remote-mep cfm-state down
The total number of RMEPs is : 2
The status of RMEPs : 0 up, 2 down, 0 disable
--------------------------------------------------
 MD Name            : md
 Level            : 0
 MA Name            : ma
 RMEP ID            : 1111
 VLAN ID            : 1111
 VSI Name           : --
 L2VC ID            : --
 MAC                : --
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : down
 Alarm Status       : none
 Interface TLV      : --
 Connect Status     : up
 MD Name            : md1
 Level            : 0
 MA Name            : ma1
 RMEP ID            : 2
 VLAN ID            : 100
 VSI Name           : --
 L2VC ID            : --
 MAC                : 0044-0141-5410
 CCM Receive        : enabled
 Trigger-If-Down    : disabled
 CFM Status         : down
 Alarm Status       : LOC
 Interface TLV      : --
 Connect Status     : up
```

Table 18-49 Description of the **display cfm remote-mep** command output

Item	Description
The total number of RMEPs is	Number of RMEPs.
MD Name	Name of the MD.
Level	Level of the MD. The value ranges from 0 to 7. A higher level indicates a higher priority of the MD.
MA Name	Name of the MA.

Item	Description
RMEP ID	ID of the RMEP.
VLAN ID	ID of the VLAN associated with an MA.
VSI Name	Name of the VSI associated with an MA.
MAC	MAC address of the RMEP. **NOTE** An RMEP's MAC address can be a bridge MAC address or the MAC address of the interface where the RMEP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an RMEP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an RMEP uses the MAC address of the interface where the RMEP is configured.
CCM Receive	Whether the MEP is enabled to receive CCMs from the RMEP: ● disabled: The MEP is disabled from receiving CCMs from the RMEP. ● enabled: The MEP is enabled to receive CCMs from the RMEP.
Trigger-If-Down	Whether the interface where the RMEP is configured is shut down and enabled when a fault is detected: ● disabled: The interface where the RMEP is configured is not shut down or enabled when a fault is detected. ● enabled: The interface where the RMEP is configured is shut down and enabled when a fault is detected. That is, when a MEP detects a connectivity fault between the MEP and the RMEP in the same MA, the system shuts down the interface on which the MEP is configured and then enables it.
CFM Status	CFM status: ● up: CC works properly. ● down: No MEP is configured on the device or the interface where the MEP is configured is unavailable (the interface card or subcard is not installed or has been restarted, or the Eth-Trunk has no member interface or all member interfaces are Down). ● disable: CFM is not configured, that is, the MEP is not enabled to send CCMs and the RMEP is not enabled to receive CCMs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm Status	CFM alarm status: ● unexpectedPeriod: The interval carried in a CCM sent by the RMEP is different from that configured on the MEP. ● unexpectedMAC: The source MAC address carried in a CCM sent by the RMEP is different from the RMEP's MAC address configured on the MEP. ● LOC: The session is terminated. ● exceptionalMACstatus: The RMEP reports that the interface is not Up. ● RDI: The MEP receives CCMs with the RDI. ● none: No alarm is generated. **NOTE** If the device is configured with no MEP but an RMEP, the CFM status is Down. However, no alarm is generated. That is, the field is none.
Interface TLV	Status of an interface type-length-value (TLV): ● - -: The default value is 0. No TLV status is available on the interface. ● up: The interface status is Up, and the interface can transmit packets. ● down: The interface status is Down, and the interface cannot transmit packets. ● testing: The TLV status of the interface is testing. ● unknown: The interface status is unknown. ● dormant: The interface is blocked and is waiting for an external event. ● notPresent: Information about the interface components is lost. ● lowerLayerDown: The lower layer status of the interface is Down. **NOTE** ● The packets carrying the interface TLV field with the value of Up or Down can be sent. ● The received packets carrying the interface TLV field with any value can be parsed.

Related Topics

18.8.30 remote-mep ccm-receive enable

18.8.16 display oam global configuration

Function

The **display oam global configuration** command displays the global configuration of Ethernet OAM, including:

- Whether Ethernet CFM is enabled globally
- Whether MAC ping is enabled
- Whether MAC trace is enabled
- Whether EFM OAM is enabled globally
- Ethernet CFM version information on the device running IEEE Standard 802.1ag-2007
- MP address model

Format

display oam global configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display oam global configuration** command displays whether Ethernet OAM is enabled globally.

Example

Display the global configuration of Ethernet OAM on the local device.

```
<Huawei> display oam global configuration
Global Configuration                          Value
-----------------------------------------------------------
CFM Status                                  enabled
Ping MAC Status                               disabled
Trace MAC Status                              disabled
CFM MAC-tunnel MIP Trace Status                     disabled
EFM Status                                 disabled
CFM Protocol                                standard
CFM MP-address-model                              bridge
```

Table 18-50 Description of the **display oam global configuration** command output

Item	Description
CFM Status	Whether Ethernet CFM is enabled globally: ● disabled: Ethernet CFM is disabled globally. ● enabled: Ethernet CFM is enabled globally.
Ping MAC Status	Whether GMAC ping is enabled: ● disabled: GMAC ping is disabled. ● enabled: GMAC ping is enabled.
Trace MAC Status	Whether GMAC trace is enabled: ● disabled: GMAC trace is disabled. ● enabled: GMAC trace is enabled.
CFM MAC-tunnel MIP Trace Status	Whether the intermediate node in the MAC tunnel is enabled to respond to MAC trace messages: ● disabled: The intermediate node in the MAC tunnel is disabled from responding to MAC trace messages. ● enabled: The intermediate node in the MAC tunnel is enabled to respond to MAC trace messages.
EFM Status	Whether EFM OAM is enabled globally: ● disabled: EFM OAM is disabled globally. ● enabled: EFM OAM is enabled globally.
CFM Protocol	Ethernet CFM protocol number.

Related Topics

18.8.1 cfm enable (system view)

18.7.7 efm enable

18.8.17 ma

Function

The **ma** command creates an MA in an MD and displays the MA view, or directly displays view of an existing MA.

The **undo ma** command deletes an MA.

Format

MD view and MA view:

ma *ma-name* [**format** { **icc-based** *iccbased-ma-format-name* | **string** *ma-format-name* }]

MD view:

undo ma [*ma-name*]

Parameters

Parameter	Description	Value
ma-name	Specifies the name of an MA. The name of an MA in an MD is unique.	The value is a string of case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
icc-based *iccbased-ma-format-name*	Specifies an ICC-based MA name carried in CCMs to be sent. ITU carrier codes (ICCs) are assigned to network operators or service providers and maintained by ITU-T Telecommunication Standardization Bureau (TSB) in compliance with ITU-T M.1400 Recommendation.	The value is a string of 1 to 13 case-sensitive characters without spaces, hyphens (-), and question marks (?).
string *ma-format-name*	Specifies a string-based MA name carried in CCMs to be sent.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).

Views

MD view, MA view

Default Level

2: Configuration level

Usage Guidelines

Up to 256 MAs can be created in an MD on the device. Up to 256 MAs can be created on the device.

NOTE

- The AR3260 and AR2240 support up to 16 MDs, 256 MAs, and 256 MEPs.
- The AR1200 supports up to 8 MDs, 128 MAs, and 128 MEPs.

Usage Scenario

Generally, services are deployed based on VLANs or VSIs on a network. If CFM is required to monitor link connectivity, run the **ma** *ma-name* command to create an MA. Then CFM can be implemented in the MA.

Prerequisites

An MD has been created using the **cfm md** *md-name* command.

Precautions

- When an MA is deleted, the device automatically deletes all MEPs and RMEPs in the MA, stops CC, and clears MA-related alarms.
- An ICC-based MA can be only configured in the MD with the MD name in **no-md-name** format.

Example

Create an MA named **ma1**.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1]
```

Related Topics

18.8.10 display cfm ma

18.8.18 map

18.8.27 packet-priority

18.8.18 map

Function

The **map** command associates a VLAN with an MA.

The **undo map** command disassociates a VLAN from an MA.

By default, an MA is not associated with any VLAN.

Format

map vlan *vlan-id*

undo map vlan

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Ethernet CFM detects connectivity faults in each MA. After an MA is associated with a VLAN, Ethernet CFM can detect connectivity faults in the VLAN.

Precautions

If you use CFM to detect connectivity faults between two directly connected devices, the MA does not need to be associated with a VLAN.

An MA can be associated with only one VLAN.

NOTICE

You cannot create or delete the association between an MA and a VLAN if an MEP or RMEP is configured in the MA.

Before changing the VLAN associated with an MA, use the **undo map** command to disassociate the MA from the VLAN.

Example

Associate an MA with VLAN 10. Ensure that the MA is not associated with any VLAN.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 10
```

Related Topics

18.8.17 ma

 Copyright © Huawei Technologies Co., Ltd.

18.8.19 mep mep-id

Function

The **mep mep-id** command creates a MEP.

Using the **undo mep mep-id** command deletes a MEP.

Format

mep mep-id *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** }

undo mep mep-id *mep-id*

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. A MEP ID identifies a MEP. Each MEP must have a unique ID in an MA or a VLAN.	The value is an integer that ranges from 1 to 8191.
interface-type interface-number	Specifies the type and number of the interface where a MEP is configured. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Specifies the ID of a VLAN.	The value is an integer that ranges from 1 to 4094.
pe-vid *pe-vid*	Specifies the outer VLAN ID of a PE.	The value is a decimal integer that ranges from 1 to 4094.
ce-vid *ce-vid*	Specifies the inner VLAN ID of a CE.	The value is a decimal integer that ranges from 1 to 4094.
inward	Indicates an inward-facing MEP. An inward-facing MEP sends 802.1ag packets through all interfaces in a VLAN associated with an MA, except the interface on which the MEP is configured. That is, the inward-facing MEP broadcasts 802.1ag packets in the VLAN associated with the MA.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
outward	Indicates an outward-facing MEP. An outward-facing MEP sends 802.1ag packets through an interface on which the MEP is configured.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To create a MEP, run the **mep mep-id** command.

Precautions

MEPs fall into inward-facing and outward-facing MEPs based on the scope where 802.1ag packets are sent.

The following restrictions apply to MEPs in an MA:

- Inward-facing and outward-facing MEPs cannot coexist.
- You can create multiple inward-facing interface-based MEPs but only one outward-facing interface-based MEP. Only one inward-facing interface-based MEP can be created on an interface.

Example

Create an inward-facing MEP on Ethernet2/0/0 in the MA **ma1** of the MD **md1** and set the MEP ID to 15.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] port ethernet 2/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 15 interface ethernet 2/0/0 inward
```

Related Topics

18.8.18 map
18.8.13 display cfm mep

18.8.20 mep alarm disable

Function

The **mep alarm disable** command disables a MEP from reporting alarms.

The **undo mep alarm disable** command enables a MEP to report alarms.

By default, a MEP is enabled to report alarms.

Format

mep mep-id *mep-id* **alarm rdi disable**

undo mep mep-id *mep-id* **alarm rdi disable**

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. A MEP ID identifies a MEP. Each MEP must have a unique ID in an MA or a VLAN.	The value is an integer that ranges from 1 to 8191.
alarm rdi	Disables a MEP from reporting remote defect indication (RDI) alarms.	-

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an NMS manages many MEPs on a network, it may receive a large number of RDI and AIS alarms. To reduce such alarms, you can disable the MEPs from reporting alarms to the NMS. This reduces the load of the NMS and local device.

Prerequisites

The following operations must have been performed:

1. Run the **cfm md** command to create an MD.
2. Run the **ma** command to create an MA.
3. Run the **mep mep-id** command to create a MEP.

Example

Disable MEP 1 in the MA **ma1** of the MD **md1** from reporting RDI alarms.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 alarm rdi disable
```

Related Topics

18.8.18 map

18.8.13 display cfm mep

18.8.21 oam-bind cfm md ma efm interface

Function

The **oam-bind cfm md ma efm interface** command configures EFM and Ethernet CFM to report faults to each other.

The **undo oam-bind cfm md ma efm interface** command cancels the configuration.

By default, EFM OAM and Ethernet CFM are not configured to report faults to each other.

Format

oam-bind cfm md *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*

undo oam-bind cfm md *md-name* **ma** *ma-name* **efm interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
interface-type interface-number	Specifies the type and number of an Ethernet interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side of a device and CFM is deployed at the other, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- If EFM detects a link fault, it notifies CFM.
- If CFM detects a link fault, it notifies EFM.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands according to your scenario as described in **Table 18-51**.

Table 18-51 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands in any order (each command configures fault transmission in a single direction): • The **oam-bind ingress efm interface egress cfm md ma** command configures EFM to report faults to CFM. • The **oam-bind ingress cfm md ma egress efm interface** command configures CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. • Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Precautions

The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.

Example

Configure EFM and CFM to report faults to each other through Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind cfm md mdcustomer ma customer efm interface ethernet 2/0/0
```

Related Topics

18.8.1 cfm enable (system view)

18.8.7 cfm md
18.8.17 ma
18.7.7 efm enable

18.8.22 oam-bind interface cfm md ma trigger if-down

Function

The **oam-bind interface cfm md ma trigger if-down** command configures an interface and Ethernet CFM to report faults to each other.

The **undo oam-bind interface cfm md ma trigger if-down** command cancels the configuration.

By default, an interface and Ethernet CFM are not configured to report faults to each other.

Format

oam-bind interface *interface-type interface-number* **cfm md** *md-name* **ma** *ma-name* **trigger if-down**

undo oam-bind interface *interface-type interface-number* **cfm md** *md-name* **ma** *ma-name* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate an interface with CFM, run the **oam-bind interface cfm md ma trigger if-down** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional transmission of fault information between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands according to your scenario as described in **Table 18-52**.

Table 18-52 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands in any order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: • To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. • To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Enable Ethernet2/0/0 to report faults to Ethernet CFM.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind interface ethernet 2/0/0 cfm md md1 ma ma1 trigger if-down
```

Related Topics

18.7.7 efm enable

18.7.36 oam-mgr

18.8.23 oam-bind ingress cfm md ma trigger egress interface

18.8.26 oam-bind ingress interface egress cfm md ma trigger if-down

 Copyright © Huawei Technologies Co., Ltd.

18.8.23 oam-bind ingress cfm md ma trigger egress interface

Function

The **oam-bind ingress cfm md ma trigger egress interface** command configures Ethernet CFM to report faults to an interface.

The **undo oam-bind ingress cfm md ma trigger egress interface** command cancels the configuration.

By default, Ethernet CFM is not configured to report faults to an interface.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **trigger if-down egress interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **trigger if-down egress interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
if-down	Indicates that the physical status of an interface is triggered to go Down when the Ethernet CFM module bound to the interface is faulty.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface bound to CFM. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate CFM with an interface, run the **oam-bind ingress cfm md ma egress interface** command.

Precautions

Before configuring CFM and an interface to report faults to each other, pay attention to the following points:

- Fault messages are transmitted from the ingress to the egress.
- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional transmission of fault information between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

Select the preceding commands according to your scenario as described in **Table 18-53**.

Table 18-53 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands in any order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: • To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. • To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure Ethernet CFM to report faults to Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress cfm md md1 ma ma1 trigger if-down egress interface ethernet 2/0/0
```

Related Topics

18.7.7 efm enable
18.7.36 oam-mgr
18.8.22 oam-bind interface cfm md ma trigger if-down
18.8.26 oam-bind ingress interface egress cfm md ma trigger if-down

 Copyright © Huawei Technologies Co., Ltd.

18.8.24 oam-bind ingress cfm md ma egress efm interface

Function

The **oam-bind ingress cfm md ma egress efm interface** command configures Ethernet CFM to report faults to EFM OAM.

The **undo oam-bind ingress cfm md ma egress efm interface** command cancels the configuration.

By default, Ethernet CFM is not configured to report faults to EFM OAM.

Format

oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number*

undo oam-bind ingress cfm md *md-name* **ma** *ma-name* **egress efm interface** *interface-type interface-number*

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters.
interface-type interface-number	Specifies the type and number of an Ethernet interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side of a device and CFM is deployed at the other, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- If EFM detects a link fault, it notifies CFM.
- If CFM detects a link fault, it notifies EFM.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands according to your scenario as described in **Table 18-54**.

Table 18-54 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands in any order (each command configures fault transmission in a single direction): • The **oam-bind ingress efm interface egress cfm md ma** command configures EFM to report faults to CFM. • The **oam-bind ingress cfm md ma egress efm interface** command configures CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. • Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Example

Configure Ethernet CFM to report faults to EFM through Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress cfm md mdcustomer ma customer egress efm interface ethernet 2/0/0
```

Related Topics

18.8.1 cfm enable (system view)

18.8.7 cfm md

18.8.17 ma

18.7.7 efm enable

18.8.25 oam-bind ingress efm interface egress cfm md ma

Function

The **oam-bind ingress efm interface egress cfm md ma** command configures EFM OAM to report faults to Ethernet CFM.

The **undo oam-bind ingress efm interface egress cfm md ma** command cancels the configuration.

By default, EFM OAM is not configured to report faults to Ethernet CFM.

Format

oam-bind ingress efm interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

undo oam-bind ingress efm interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name*

Parameters

Parameter	Description	Value
md-name	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ma-name	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
interface-type interface-number	Specifies the type and number of an Ethernet interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. The interface must have been enabled with EFM OAM.	-

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If EFM is deployed at one side of a device and CFM is deployed at the other, associate EFM with CFM on the device so that EFM and CFM can report faults to each other.

Association between EFM and CFM is bidirectional:

- If EFM detects a link fault, it notifies CFM.
- If CFM detects a link fault, it notifies EFM.

The following commands are used to associate EFM with CFM:

- **oam-bind cfm md ma efm interface**
- **oam-bind ingress cfm md ma egress efm interface**
- **oam-bind ingress efm interface egress cfm md ma**

Select the preceding commands according to your scenario as described in **Table 18-55**.

Table 18-55 Association between EFM and CFM

Scenario	Configuration Solution 1	Configuration Solution 2
Bidirectional fault notification between EFM and CFM	The **oam-bind cfm md ma efm interface** command is used to configure EFM and CFM to report faults to each other.	Run the following commands in any order (each command configures fault transmission in a single direction): • The **oam-bind ingress efm interface egress cfm md ma** command configures EFM to report faults to CFM. • The **oam-bind ingress cfm md ma egress efm interface** command configures CFM to report faults to EFM.
Unidirectional fault notification between EFM and CFM	Select either of the following commands based on the transmission direction: • Run the **oam-bind ingress efm interface egress cfm md ma** command to configure EFM to report faults to CFM. • Run the **oam-bind ingress cfm md ma egress efm interface** command to configure CFM to report faults to EFM.	None

Prerequisites

The MD and MA have been created and EFM has been enabled on the specified interface.

Example

Configure EFM to report faults to CFM through Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress efm interface ethernet 2/0/0 egress cfm md mdcustomer ma customer
```

Related Topics

18.8.1 cfm enable (system view)

18.8.7 cfm md

18.8.17 ma

18.7.7 efm enable

18.8.26 oam-bind ingress interface egress cfm md ma trigger if-down

Function

The **oam-bind ingress interface egress cfm md ma trigger if-down** command configures an interface to report faults to Ethernet CFM.

The **undo oam-bind ingress interface egress cfm md ma trigger if-down** command cancels the configuration.

By default, an interface is disabled from reporting faults to Ethernet CFM.

Format

oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down**

undo oam-bind ingress interface *interface-type interface-number* **egress cfm md** *md-name* **ma** *ma-name* **trigger if-down**

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ma *ma-name*	Specifies the name of an MA.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

OAM management view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To associate an interface with CFM, run the **oam-bind ingress interface egress cfm md ma trigger if-down** command.

Precautions

If CFM is associated with an interface on a device and the device interface goes Down, the OAM management module notifies Ethernet CFM of the fault and Ethernet CFM notifies the remote end.

Prerequisites

The following requirements must be met before configuring unidirectional fault transmission from an interface to Ethernet CFM:

- The MD and MA related to the Ethernet CFM module must have been created.
- The binding between an Ethernet CFM module and an interface is one-to-one. That is, when an Ethernet CFM module is bound to an interface, the Ethernet CFM module cannot be bound to other interfaces.
- A physical interface associated with CFM cannot be monitored by CFM. If CFM is associated with a physical interface monitored by itself, the link is locked.

Configure unidirectional or bidirectional transmission of fault information between Ethernet CFM and an interface. You may use the following commands when associating Ethernet CFM with an interface:

- **oam-bind interface cfm md ma trigger if-down**
- **oam-bind ingress cfm md ma egress interface**
- **oam-bind ingress interface egress cfm md ma trigger if-down**

 Copyright © Huawei Technologies Co., Ltd.

Select the preceding commands according to your scenario as described in **Table 18-56**.

Table 18-56 Association between Ethernet CFM and an interface

Scenario	Configuration Solution 1	Configuration Solution 2
Faults need to be transmitted bidirectionally between Ethernet CFM and an interface.	Use the **oam-bind interface cfm md ma trigger if-down** command. **NOTE** After configuring Ethernet CFM and an interface to report faults to each other, run the **display current-configuration** command to check the configuration. The command output displays the **oam-bind ingress cfm md ma egress interface** and **oam-bind ingress interface egress cfm md ma trigger if-down** commands, but does not display the **oam-bind interface cfm md ma trigger if-down** command. The displayed commands configure reverse transmission directions of fault information.	Run the following commands in any order (each command configures fault transmission in a single direction): • **oam-bind ingress cfm md ma egress interface** • **oam-bind ingress interface egress cfm md ma trigger if-down**
Faults need to be transmitted unidirectionally between Ethernet CFM and an interface.	Select either of the following commands based on the transmission direction: • To configure Ethernet CFM to report faults to an interface, use the **oam-bind ingress cfm md ma egress interface** command. • To configure an interface to report faults to Ethernet CFM, use the **oam-bind ingress interface egress cfm md ma trigger if-down** command.	None

Example

Configure Ethernet CFM to report faults to Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] oam-mgr
[Huawei-oam-mgr] oam-bind ingress interface ethernet 2/0/0 egress cfm md md1 ma ma1 trigger if-down
```

Related Topics

18.7.7 efm enable

18.7.36 oam-mgr
18.8.22 oam-bind interface cfm md ma trigger if-down
18.8.23 oam-bind ingress cfm md ma trigger egress interface

18.8.27 packet-priority

Function

The **packet-priority** command sets the 802.1p priority of 802.1ag packets in an MA.

The **undo packet-priority** command restores the default 802.1p priority of 802.1ag packets in an MA.

By default, the 802.1p priority of 802.1ag packets in an MA is 7.

Format

packet-priority *priority*

undo packet-priority

Parameters

Parameter	Description	Value
priority	Specifies the 802.1p priority of 802.1ag packets.	The value is an integer that ranges from 0 to 7. The default value is 7. A larger value indicates a higher priority.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.1ag packets with different 802.1p priorities are processed with different transmission quality. You can use this command to change the transmission quality of 802.1ag packets on a network.

Example

Set the 802.1p priority of 802.1ag packets in an MA to 3.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
```

```
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] packet-priority 3
```

Related Topics

18.8.10 display cfm ma

18.8.28 ping mac-8021ag

Function

The **ping mac-8021ag** command enables 802.1ag MAC ping to detect connectivity faults between a MEP and an RMEP or a MIP in an MA.

Format

All views except the MA view:

ping mac-8021ag mep mep-id *mep-id* **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

MA view:

ping mac-8021ag mep mep-id *mep-id* { **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } | **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**-c** *count* | **interface** *interface-type interface-number* | **-s** *packetsize* | **-t** *timeout* | **-p** *priority-value*] *

Parameters

Parameter	Description	Value
mep mep-id *mep-id*	Specifies the ID of a MEP. The MEP must have been created using the **mep mep-id** command.	The value is an integer that ranges from 1 to 8191.
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?).
ma *ma-name*	Specifies the name of an MA.	The value is a string of case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac *mac-address*	Specifies the MAC address of the destination node. The destination node can be a MEP or a MIP. *mac-address* specifies the MP's MAC address. **NOTE** An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address.
remote-mep mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
-c *count*	Specifies the number of ping attempts.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
interface *interface-type interface-number*	Specifies the outbound interface for sending ping packets on the local device. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
-s *packetsize*	Specifies the size of a ping packet.	The value is an integer that ranges from 95 to 1500, in bytes. The default value is 95.
-t *timeout*	Specifies the timeout interval for waiting for a response packet.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
-p *priority-value*	Specifies the priority of ping packets.	The value is an integer that ranges from 0 to 7. The default value is the same as the 802.1p priority of 802.1ag packets specified in the MA view.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Similar to ping, 802.1ag MAC ping enables the local device to send test packets and wait for a response to check whether the destination device is reachable. It also calculates the period for waiting for the response of ping packets at the transmit end for network performance analysis.

A device is usually configured with multiple MDs and MAs. To accurately detect connectivity of a link between two or more devices, perform either of the following operations:

- Run the **ping mac-8021ag** command in the MA view.
  - Run the **ping mac-8021ag** command without **md** *md-name* **ma** *ma-name* specified to check connectivity of links in a specified MA.
  - Run the **ping mac-8021ag** command with **md** *md-name* **ma** *ma-name* specified to check connectivity of links based on the configured MA and MD.
- Run the **ping mac-8021ag md** *md-name* **ma** *ma-name* command in all views except the MA view to check connectivity of links based on the configured MA and MD.

Prerequisites

- The MA has been associated with a VLAN.
- The MEP has been configured in the MA.

Precautions

802.1ag MAC ping is initiated by the local MEP in the MA and destined for a MEP or a MIP of the same level on another device. The source node and the destination node can be located in the same MA or different MAs.

Example

Ping the MIP with a bridge MAC address of 0001-0300-0204 twice on the MEP in **ma1** and set the size of ping packets to 112 bytes.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] ping mac-8021ag mep mep-id 1 mac 0001-0300-0204 -c 2 -s 112
Pinging 0001-0300-0204 with 112 bytes of data:
Reply from 0001-0300-0204: bytes = 112 time = 9ms
Reply from 0001-0300-0204: bytes = 112 time = 11ms
Packets: Sent = 2, Received = 2, Lost = 0  <0% Lost >
Minimum = 9ms, Maximum = 11ms, Average = 10ms
```

Table 18-57 Description of the **ping mac-8021ag** command output

Item	Description
Reply from 0001-0300-0204: bytes = 112 time = 9ms	Size and response time of ping packets sent by the destination device. When the response time is less than 1 ms, "time < 1ms" is displayed.
Packets: Sent = 2, Received = 2, Lost = 0 <0% Lost >	Number of sent ping packets, number of received response packets, and number and percentage of discarded packets.
Minimum	Minimum round-trip time (RTT).
Maximum	Maximum RTT.
Average	Average RTT.

Related Topics

18.8.19 mep mep-id

18.8.32 trace mac-8021ag

18.8.29 remote-mep

Function

The **remote-mep** command configures an RMEP in an MA.

The **undo remote-mep** command deletes an RMEP from an MA.

Format

remote-mep mep-id *mep-id* [**mac** *mac-address*]

undo remote-mep mep-id *mep-id*

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
mac *mac-address*	Specifies the MAC address of an RMEP.	The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits.

Views

MA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command configures an RMEP.

Precautions

To detect CFM connectivity faults between a device and an RMEP in an MA, complete the following tasks:

- Run the **remote-mep** command to configure an RMEP in an MA.
- Run the **remote-mep ccm-receive enable** command to enable the MEP to receive CCMs from the RMEP.

To modify the bridge MAC address of the RMEP, you must delete the RMEP from an MA and then reconfigure the RMEP.

NOTICE

- If multiple MEPs exist in an MA, the configured RMEP corresponds to multiple MEPs.
- If one MEP exists in an MA, one or more configured RMEPs correspond to one MEP.

Example

Configure RMEP 10 in **ma1** on the device with the bridge MAC address of 0001-0300-0204.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] remote-mep mep-id 10 mac 0001-0300-0204
```

Related Topics

18.8.15 display cfm remote-mep

18.8.30 remote-mep ccm-receive enable

18.8.30 remote-mep ccm-receive enable

Function

The **remote-mep ccm-receive enable** command enables a MEP on the device to receive CCMs from an RMEP in the same MA or MAC tunnel.

The **undo remote-mep ccm-receive enable** command cancels the configuration.

 Copyright © Huawei Technologies Co., Ltd.

By default, a MEP does not receive CCMs from an RMEP.

Format

remote-mep ccm-receive [**mep-id** *mep-id*] **enable**

undo remote-mep ccm-receive [**mep-id** *mep-id*] **enable**

Parameters

Parameter	Description	Value
mep-id *mep-id*	Enables a MEP to receive CCMs from the specified RMEP. If this parameter is not specified, a MEP can receive CCMs from all RMEPs in the same MA.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **remote-mep ccm-receive enable** command enables a MEP on the device to receive CCMs from the RMEP in the same MA or MAC tunnel.

Precautions

Multiple MAs can be configured on a device. The interval at which CCMs are sent or detected cannot be changed on the device in an MA if any of the following operations has been performed:

- The device is enabled to send CCMs using the **mep ccm-send enable** command.
- The device is enabled to receive CCMs using the **remote-mep ccm-receive enable** command.

The **undo mep ccm-send** or **undo mep ccm-receive** command must be run before the interval is changed.

Prerequisites

A MEP and an RMEP have been created in the MA.

Example

Enable the device to receive CCMs from RMEP 10 in **ma1**.

```
<Huawei> system-view
[Huawei] cfm enable
```

```
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] remote-mep mep-id 10 mac 0001-0300-0204
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 10 enable
```

Related Topics

18.8.6 ccm-interval

18.8.15 display cfm remote-mep

18.8.33 mep ccm-send enable

18.8.31 senderid-tlv-type

Function

The **senderid-tlv-type** command sets the type of the Sender ID TLV in CFM packets.

The **undo senderid-tlv-type** command restores the default type of the Sender ID TLV in CFM packets.

By default, the type of the Sender ID TLV is **defer**.

Format

senderid-tlv-type { **none** | **chassis** | **manage** | **chassis-manage** | **defer** }

undo senderid-tlv-type

Parameters

Parameter	Description	Value
none	Indicates that a sent CFM packet does not contain the Sender ID TLV.	-
chassis	Indicates that a sent CFM packet contains the chassis ID.	-
manage	Indicates that a sent CFM packet contains the management address.	-
chassis-manage	Indicates that a sent CFM packet contains the chassis ID and management address.	-
defer	Indicates that the content of the Sender ID TLV is determined by the MD object.	-

Views

MD view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can use the **undo senderid-tlv-type** command to configure the type of the Sender ID TLV in CFM packets in the MD view or default MD view.

Example

Set the type of the Sender ID TLV to **manage**.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm default md
[Huawei-default-md] senderid-tlv-type manage
```

Related Topics

18.8.1 cfm enable (system view)

18.8.8 cfm default md

18.8.32 trace mac-8021ag

Function

The **trace mac-8021ag** command enables 802.1ag MAC trace to detect connectivity faults between a MEP and an RMEP or a MIP in an MA.

Format

All views except the MA view:

trace mac-8021ag mep mep-id *mep-id* **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *

MA view:

trace mac-8021ag mep mep-id *mep-id* { **md** *md-name* **ma** *ma-name* { **mac** *mac-address* | **remote-mep mep-id** *mep-id* } | **mac** *mac-address* | **remote-mep mep-id** *mep-id* } [**interface** *interface-type interface-number* | **-t** *timeout* | **ttl** *ttl*] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
md *md-name*	Specifies the name of an MD.	The value is a string of 1 to 43 case-sensitive characters without spaces, hyphens (-), and question marks (?). **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ma *ma-name*	Specifies the name of an MA.	The value is a string of case-sensitive characters without spaces, hyphens (-), and question marks (?). The total length of the names of the MA and MD cannot exceed 44 characters. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.
mac *mac-address*	Specifies the MAC address of the destination node. The destination node can be a MEP or a MIP. *mac-address* specifies the MP's MAC address. The value is in H-H-H format. An H is a hexadecimal number of 1 to 4 digits. The value cannot be a broadcast or multicast MAC address. **NOTE** An MP's MAC address can be a bridge MAC address or the MAC address of the interface where the MP is configured. The MAC address depends on the configured MP address model: ● If the shared MP address model is configured, an MP uses a bridge MAC address as its own MAC address. ● If the independent MP address model is configured, an MP uses the MAC address of the interface where the MP is configured.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remote-mep mep-id *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
interface-type interface-number	Specifies the outbound interface for sending LTMs on the local device. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. This parameter must be specified if the forwarding entry of the destination node does not exist in the MAC address table or there is more than one interface in a VLAN.	-
-t *timeout*	Specifies the timeout interval for waiting for LTR messages.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 2000 ms.
ttl *ttl*	Specifies the maximum hop of LTMs.	The value is an integer that ranges from 1 to 255. The default value is 64.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

Similar to traceroute (or tracert in some systems), 802.1ag MAC trace tests the path between the local device and the destination device or locates failure points by sending test packets and receiving reply packets.

A device is usually configured with multiple MDs and MAs. To locate failure points or detect connectivity of a link between one MEP to another MEP or a MIP in the same MA, perform either of the following operations:

- Run the **trace mac-8021ag** command in the MA view.
  - Run the **trace mac-8021ag** command without **md** *md-name* **ma** *ma-name* specified to test the actual forwarding path and locate failure points in a specified MA.

  - Run the **trace mac-8021ag** command with **md** *md-name* **ma** *ma-name* specified to test the actual forwarding path and locate failure points in a specified MA based on the configured MA and MD.
- Run the **trace mac-8021ag md** *md-name* **ma** *ma-name* command in all views except the MA view to test the actual forwarding path and locate failure points based on the configured MA and MD.

Prerequisites

- The MA has been associated with a VLAN.
- The MEP has been configured in the MA.

Precautions

A MEP initiates an 802.1ag MAC trace test to monitor reachability of the MEP's or MIP's destination address. These nodes have the same level and can be located in the same MA or different MAs.

Example

Trace the MEP with the MAC address of aa99-6600-5600 from the MEP in the MA **macustomer**, with the TTL of 64.

```
<Huawei> system-view
[Huawei] cfm enable
[Huawei] cfm md mdcustomer
[Huawei-md-mdcustomer] ma macustomer
[Huawei-md-mdcustomer-ma-macustomer] trace mac-8021ag mep mep-id 1 mac aa99-6600-5600 ttl 64
Tracing the route to aa99-6600-5600 over a maximum of 64 hops:
-------------------------------------------------------------------------------
 Hops  Ingress Mac        Ingress Port              Ingress Action      Relay Action
       Egress Mac         Egress Port               Egress Action       Ismep
-------------------------------------------------------------------------------
1       2155-2201-3302     GigabitEthernet2/0/0      IngOK               RlyFDB
        0018-82e2-36db     GigabitEthernet2/0/0      EgrOK               NoMep
```

Table 18-58 Description of the **trace mac-8021ag** command output

Item	Description
Hops	Number of hops.
Ingress Mac	MAC address of the inbound interface for receiving LTMs on the intermediate node or destination node.
Ingress Port	Inbound interface for receiving LTMs on the intermediate node or destination node.
Ingress Action	Action taken by the inbound interface to process LTMs: ● If the value is IngOK, the inbound interface forwards LTMs successfully. ● If this field is empty, the inbound interface fails to forward LTMs.

Item	Description
Reply Action	Action taken by the device to process LTMs: ● RlyFDB: The device forwards LTMs to the next-hop device. ● RlyHit: The device forwards LTMs to the destination device.
Egress Port	Outbound interface for forwarding LTMs on the intermediate node.
Egress Action	Action taken by the outbound interface to process LTMs: ● If the value is EgrOK, the outbound interface forwards LTMs successfully. ● If this field is empty, the outbound interface does not forward LTMs or fails to forward LTMs.
Ismep	Whether the mode of the outbound interface is a MEP: ● NoMep: indicates that the node is not a MEP. ● IsMep: indicates that the node is a MEP.

Related Topics

18.8.1 cfm enable (system view)

18.8.28 ping mac-8021ag

18.8.33 mep ccm-send enable

Function

The **mep ccm-send enable** command enables a MEP in an MA to send CCMs.

The **undo mep ccm-send enable** command disables a MEP in an MA from sending CCMs.

By default, a MEP is disabled from sending CCMs.

Format

mep ccm-send [**mep-id** *mep-id*] **enable**

undo mep ccm-send [**mep-id** *mep-id*] **enable**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mep-id *mep-id*	Specifies the ID of a MEP. If this parameter is not specified, all the MEPs in the MA are enabled to send CCMs or disabled from sending CCMs.	The value is an integer that ranges from 1 to 8191.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you use the **mep mep-id** command to configure a MEP, use this command to enable the MEP to send CCMs.

Precautions

Multiple MAs can be configured on a device. The interval at which CCMs are sent or received cannot be changed on the device in an MA if any of the following operations has been performed:

- The **mep ccm-send enable** command is run to enable a MEP in an MA to send CCMs.
- The **remote mep ccm-receive enable** command is run to enable a MEP in an MA to receive CCMs.

The **undo mep ccm-send enable** or **undo mep ccm-receive enable** command must be run before the interval is changed.

Example

Enable MEP 10 in the MA named **ma1** to send CCMs.

```
<Huawei> system-view
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 10 enable
```

Related Topics

18.8.6 ccm-interval

18.8.13 display cfm mep

18.8.30 remote-mep ccm-receive enable

18.8.34 vlan (default MD view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **vlan** command creates a VLAN in the default MD.

The **undo vlan** command deletes a VLAN from the default MD.

Format

vlan { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

undo vlan { *vlan-id1* [**to** *vlan-id2*] }&<1-10>

Parameters

Parameter	Description	Value
vlan-id1	Specifies the start VLAN ID.	The value is an integer that ranges from 1 to 4094.
vlan-id2	Specifies the end VLAN ID.	The value is an integer that ranges from 1 to 4094. The value of *vlan-id2* must be greater than the value of *vlan-id1*.

Views

Default MD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run the **vlan** command in the default MD view, all the interfaces in the specified VLAN can generate MIPs according to the configured MIP creation rule in the default MD.

Precautions

If the **vlan** command is run more than once, all configurations take effect.

NOTE

The specified VLAN cannot be associated with any MA.

Example

Associate VLAN 100 to VLAN 200 with the default MD.

```
<Huawei> system-view
[Huawei] cfm default md
[Huawei-default-md] vlan 100 to 200
```

Related Topics

18.8.8 cfm default md

18.9 Y.1731 Configuration Commands

18.9.1 delay-measure two-way continual send test-id

Function

The **delay-measure two-way continual send test-id** command configures proactive two-way frame delay measurement.

The **undo delay-measure two-way continual send test-id** command cancels the configuration.

By default, proactive two-way frame delay measurement is not configured in an MA.

Format

delay-measure two-way continual send test-id *test-id* **interval** { **1000** | **10000** | **15000** | **30000** } [**packet-size** *packet-size*]

undo delay-measure two-way continual send test-id *test-id*

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
interval	Specifies the interval at which DMMs are sent.	The value is an integer, in milliseconds. The value can be 1000, 10000, 15000, or 30000.
packet-size *packet-size*	Specify the number of bytes of packets to be sent.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

To configure proactive two-way frame delay measurement in a point-to-multipoint scenario, run the **delay-measure two-way continual send test-id** command.

Prerequisites

The **delay-measure two-way continual send test-id** command takes effect only when the following basic CFM configurations have been performed:

- Run the **vlan** *vlan-id* command in the system view to create a VLAN and enter the VLAN view.

  By default, all interfaces belong to the default VLAN, that is, VLAN 1.
- Run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view to configure the default VLAN of an interface and add the interface to the default VLAN.

  By default, VLAN 1 is the default VLAN of all interfaces.
- Run the **cfm enable (system view)** command in the system view to enable CFM globally.

  By default, CFM is disabled globally.
- Run the **cfm md** *md-name* command in the system view to create a maintenance domain (MD).
- Run the **ma** *ma-name* command in the MD view to create a maintenance association (MA).
- Run the **map vlan** *vlan-id* command in the MA view to associate a VLAN with an MA.

  By default, an MA is not associated with any VLAN.
- Run the **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** } command in the MA view to create a maintenance association end point (MEP).
- Run the **mep ccm-send** [**mep-id** *mep-id*] **enable** command in the MA view to enable a MEP in an MA to send continuity check messages (CCMs).

  By default, a MEP is disabled from sending CCMs.
- Run the **remote-mep mep-id** *mep-id* [**mac** *mac-address*] command in the MA view to create a remote maintenance association end point (RMEP) in an MA.

  NOTE

  When this command is configured on the transmit device, the **mac** *mac-address* command must be configured. Otherwise, on-demand two-way frame delay measurement cannot be configured, and proactive two-way frame delay measurement can be configured but does not take effect.
- Run the **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable** command to enable a MEP on the device to receive CCMs from an RMEP in the same MA.

  By default, a MEP is disabled from receiving CCMs from an RMEP.
- Run the **test-id** *test-id* **mep** *mep-id* **remote-mep** *mep-id* [**8021p** *8021p-value*] [**description** *description*] command in the MA view to configure a test instance.

  By default, no test instance is configured in an MA.

Precautions

When two-way delay measurement is configured and the MEP and RMEP are the same in the same MA, if multiple test IDs are configured, only the test instance with the highest priority is detected.

Example

Configure two-way frame delay measurement with the test instance ID of 1, 100-byte DMMs, and the DMM sending interval of 30s.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] port GigabitEthernet 9/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet 9/0/0 inward
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[Huawei-md-md1-ma-ma1] remote-mep mep-id 2 mac 0001-0300-0204
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[Huawei-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[Huawei-md-md1-ma-ma1] delay-measure two-way continual send test-id 1 interval 30000 packet-
size 100
```

Related Topics

18.9.2 delay-measure two-way receive test-id

18.9.2 delay-measure two-way receive test-id

Function

The **delay-measure two-way receive test-id** command configures the RMEP to receive delay measurement messages (DMMs) for two-way frame delay measurement.

The **undo delay-measure two-way receive test-id** command cancels the configuration.

By default, the RMEP in an MA is not configured to receive DMMs.

Format

delay-measure two-way receive test-id *test-id*

undo delay-measure two-way receive test-id *test-id*

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **delay-measure two-way continual send test-id** or **delay-measure two-way send test-id** command is used to configure proactive or on-demand two-way frame delay measurement, run the **delay-measure two-way receive test-id** command to configure the RMEP to receive DMMs.

Prerequisites

The **delay-measure two-way receive test-id** command takes effect only when the following basic CFM configurations have been performed:

- Run the **vlan** *vlan-id* command in the system view to create a VLAN and enter the VLAN view.

  By default, all interfaces belong to the default VLAN, that is, VLAN 1.
- Run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view to configure the default VLAN of an interface and add the interface to the default VLAN.

  By default, VLAN 1 is the default VLAN of all interfaces.
- Run the **cfm enable (system view)** command in the system view to enable CFM globally.

  By default, CFM is disabled globally.
- Run the **cfm md** *md-name* command in the system view to create a maintenance domain (MD).
- Run the **ma** *ma-name* command in the MD view to create a maintenance association (MA).
- Run the **map vlan** *vlan-id* command in the MA view to associate a VLAN with an MA.

  By default, an MA is not associated with any VLAN.
- Run the **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** } command in the MA view to create a maintenance association end point (MEP).
- Run the **mep ccm-send** [**mep-id** *mep-id*] **enable** command in the MA view to enable a MEP in an MA to send continuity check messages (CCMs).

  By default, a MEP is disabled from sending CCMs.
- Run the **remote-mep mep-id** *mep-id* [**mac** *mac-address*] command in the MA view to create a remote maintenance association end point (RMEP) in an MA.
- Run the **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable** command to enable a MEP on the device to receive CCMs from an RMEP in the same MA.

  By default, a MEP is disabled from receiving CCMs from an RMEP.
- Run the **test-id** *test-id* **mep** *mep-id* **remote-mep** *mep-id* [**8021p** *8021p-value*] [**description** *description*] command in the MA view to configure a test instance.

By default, no test instance is configured in an MA.

If the configuration of the receive end is deleted or modified multiple times, the statistics may be incorrect or minus. After the configuration is completed, you are advised not to delete or modify the statistics collection task.

To modify the configuration, disable the RMEP from receiving DMMs and reconfigure it.

Precautions

When two-way delay measurement is configured and the MEP and RMEP are the same in the same MA, if multiple test IDs are configured, only the test instance with the highest priority is detected.

Example

Configure the RMEP to receive DMMs with the test instance ID of 1.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] port GigabitEthernet 9/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet 9/0/0 inward
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[Huawei-md-md1-ma-ma1] remote-mep mep-id 2
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[Huawei-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[Huawei-md-md1-ma-ma1] delay-measure two-way receive test-id 1
```

Related Topics

18.9.1 delay-measure two-way continual send test-id

18.9.3 delay-measure two-way send test-id

18.9.3 delay-measure two-way send test-id

Function

The **delay-measure two-way send test-id** command configures on-demand two-way frame delay measurement.

By default, proactive two-way frame delay measurement is not configured in an MA.

Format

delay-measure two-way send test-id *test-id* **interval** { **1000** | **10000** } **count** *count* [**packet-size** *packet-size*]

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
interval	Specifies the interval at which DMMs are sent.	The value is 1000 or 10000, in milliseconds.
count *count*	Specifies the DMM sending count.	The value is an integer that ranges from 1 to 60.
packet-size *packet-size*	Specify the number of bytes of packets to be sent.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure on-demand two-way frame delay measurement in a point-to-multipoint scenario, run the **delay-measure two-way send test-id** command.

Prerequisites

The **delay-measure two-way continual send test-id** command takes effect only when the following basic CFM configurations have been performed:

- Run the **vlan** *vlan-id* command in the system view to create a VLAN and enter the VLAN view.

  By default, all interfaces belong to the default VLAN, that is, VLAN 1.
- Run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view to configure the default VLAN of an interface and add the interface to the default VLAN.

  By default, VLAN 1 is the default VLAN of all interfaces.
- Run the **cfm enable (system view)** command in the system view to enable CFM globally.

  By default, CFM is disabled globally.
- Run the **cfm md** *md-name* command in the system view to create a maintenance domain (MD).
- Run the **ma** *ma-name* command in the MD view to create a maintenance association (MA).
- Run the **map vlan** *vlan-id* command in the MA view to associate a VLAN with an MA.

 Copyright © Huawei Technologies Co., Ltd.

By default, an MA is not associated with any VLAN.

- Run the **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** } command in the MA view to create a maintenance association end point (MEP).
- Run the **mep ccm-send** [**mep-id** *mep-id*] **enable** command in the MA view to enable a MEP in an MA to send continuity check messages (CCMs).

  By default, a MEP is disabled from sending CCMs.
- Run the **remote-mep** **mep-id** *mep-id* [**mac** *mac-address*] command in the MA view to create a remote maintenance association end point (RMEP) in an MA.

  NOTE

  When this command is configured on the transmit device, the **mac** *mac-address* command must be configured. Otherwise, on-demand two-way frame delay measurement cannot be configured, and proactive two-way frame delay measurement can be configured but does not take effect.
- Run the **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable** command to enable a MEP on the device to receive CCMs from an RMEP in the same MA.

  By default, a MEP is disabled from receiving CCMs from an RMEP.
- Run the **test-id** *test-id* **mep** *mep-id* **remote-mep** *mep-id* [**8021p** *8021p-value*] [**description** *description*] command in the MA view to configure a test instance.

  By default, no test instance is configured in an MA.

Precautions

When two-way delay measurement is configured and the MEP and RMEP are the same in the same MA, if multiple test IDs are configured, only the test instance with the highest priority is detected.

Example

Configure on-demand frame delay measurement with the test instance ID of 1, DMM sending interval of 10s, and DMM sending count of 60.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] port GigabitEthernet 9/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet 9/0/0 inward
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[Huawei-md-md1-ma-ma1] remote-mep mep-id 2 mac 0001-0300-0204
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[Huawei-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[Huawei-md-md1-ma-ma1] delay-measure two-way send test-id 1 interval 10000 count 60
```

Related Topics

18.9.2 delay-measure two-way receive test-id

18.9.4 display y1731 statistic-type

Function

The **display y1731 statistic-type** command displays Y.1731 performance data.

Format

display y1731 statistic-type { **single-synthetic-loss** | **twoway-delay** } **test-id** *test-id* [**count** *count-value*]

Parameters

Parameter	Description	Value
single-synthetic-loss	Displays single-ended SLM statistics.	-
twoway-delay	Displays statistics about two-way frame delay measurement.	-
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
count *count-value*	Displays the number of statistical entries. If the parameter is not specified, all statistical entries are displayed.	The value is an integer that ranges from 1 to 60.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When single-ended SLM or two-way frame delay measurement is configured, you can run this command to check statistics about single-ended SLM or two-way frame delay measurement in the specified test instance.

Example

Display single-ended SLM statistics in test instance 1.

```
<Huawei> display y1731 statistic-type single-synthetic-loss test-id 1
--------------------------------------------------------------------------------
Index       L-send R-send L-recv Unack  L-loss R-loss L-loss-ratio R-loss-ratio
--------------------------------------------------------------------------------
193         10     0      0      10     0      10     0.0000%     100.0000%
194         10     0      0      10     0      10     0.0000%     100.0000%
195         10     0      0      10     0      10     0.0000%     100.0000%
```

```
196        10    0    0    10        0    10    0.0000%    100.0000%
197        10    0    0    10        0    10    0.0000%    100.0000%
198        10    0    0    10        0    10    0.0000%    100.0000%
199        10    0    0    10        0    10    0.0000%    100.0000%
200        10    0    0    10        0    10    0.0000%    100.0000%
201        10    0    0    10        0    10    0.0000%    100.0000%
202        10    0    0    10        0    10    0.0000%    100.0000%
203        10    0    0    10        0    10    0.0000%    100.0000%
204        10    0    0    10        0    10    0.0000%    100.0000%
205        10    0    0    10        0    10    0.0000%    100.0000%
206        10    0    0    10        0    10    0.0000%    100.0000%
207        10    0    0    10        0    10    0.0000%    100.0000%
208        10    0    0    10        0    10    0.0000%    100.0000%
209        10    0    0    10        0    10    0.0000%    100.0000%
210        10    0    0    10        0    10    0.0000%    100.0000%
211        10    0    0    10        0    10    0.0000%    100.0000%
212        10    0    0    10        0    10    0.0000%    100.0000%
213        10    0    0    10        0    10    0.0000%    100.0000%
214        10    0    0    10        0    10    0.0000%    100.0000%
215        10    0    0    10        0    10    0.0000%    100.0000%
216        10    0    0    10        0    10    0.0000%    100.0000%
217        10    0    0    10        0    10    0.0000%    100.0000%
218        10    0    0    10        0    10    0.0000%    100.0000%
219        10    0    0    10        0    10    0.0000%    100.0000%
220        10    0    0    10        0    10    0.0000%    100.0000%
221        10    0    0    10        0    10    0.0000%    100.0000%
222        10    0    0    10        0    10    0.0000%    100.0000%
223        10    0    0    10        0    10    0.0000%    100.0000%
224        10    0    0    10        0    10    0.0000%    100.0000%
225        10    0    0    10        0    10    0.0000%    100.0000%
226        10    0    0    10        0    10    0.0000%    100.0000%
227        10    0    0    10        0    10    0.0000%    100.0000%
228        10    0    0    10        0    10    0.0000%    100.0000%
229        10    0    0    10        0    10    0.0000%    100.0000%
230        10    0    0    10        0    10    0.0000%    100.0000%
231        10    0    0    10        0    10    0.0000%    100.0000%
232        10    0    0    10        0    10    0.0000%    100.0000%
233        10    0    0    10        0    10    0.0000%    100.0000%
234        10    0    0    10        0    10    0.0000%    100.0000%
235        10    0    0    10        0    10    0.0000%    100.0000%
236        10    0    0    10        0    10    0.0000%    100.0000%
237        10    0    0    10        0    10    0.0000%    100.0000%
238        10    0    0    10        0    10    0.0000%    100.0000%
239        10    0    0    10        0    10    0.0000%    100.0000%
240        10    0    0    10        0    10    0.0000%    100.0000%
241        10    0    0    10        0    10    0.0000%    100.0000%
242        10    0    0    10        0    10    0.0000%    100.0000%
243        10    0    0    10        0    10    0.0000%    100.0000%
244        10    0    0    10        0    10    0.0000%    100.0000%
245        10    0    0    10        0    10    0.0000%    100.0000%
246        10    0    0    10        0    10    0.0000%    100.0000%
247        10    0    0    10        0    10    0.0000%    100.0000%
248        10    0    0    10        0    10    0.0000%    100.0000%
249        10    0    0    10        0    10    0.0000%    100.0000%
250        10    0    0    10        0    10    0.0000%    100.0000%
251        10    0    0    10        0    10    0.0000%    100.0000%
252        10    0    0    10        0    10    0.0000%    100.0000%
--------------------------------------------------------------------------------
Average Local-loss  :          0    Average Local-loss Ratio  :         0.0000%
Maximum Local-loss  :          0    Maximum Local-loss Ratio  :         0.0000%
Minimum Local-loss  :          0    Minimum Local-loss Ratio  :         0.0000%
Average Remote-loss :         10    Average Remote-loss Ratio :       100.0000%
Maximum Remote-loss :         10    Maximum Remote-loss Ratio :       100.0000%
Minimum Remote-loss :         10    Minimum Remote-loss Ratio :       100.0000%
```

Table 18-59 Description of the **display y1731 statistic-type single-synthetic-loss test-id 1** command output

Item	Description
Index	-
L-send	Number of packets to be sent from the local end in each round.
R-send	Number of packets to be sent from the remote end in each round.
L-recv	Number of packets received by the local end in each round.
Unack	Number of unacknowledged packets.
L-loss	Number of lost packets on the local end in each round.
R-loss	Number of lost packets on the remote end in each round.
L-loss-ratio	Packet loss ratio on the local end in each round.
R-loss-ratio	Packet loss ratio on the remote end in each round.
Average Local-loss	Average number of lost packets on the local end.
Average Local-loss Ratio	Average packet loss ratio on the local end.
Maximum Local-loss	Maximum number of lost packets on the local end.
Maximum Local-loss Ratio	Maximum packet loss ratio on the local end.
Minimum Local-loss	Minimum number of lost packets on the local end.
Minimum Local-loss Ratio	Minimum packet loss ratio on the local end.
Average Remote-loss	Average number of lost packets on the remote end.
Average Remote-loss Ratio	Average packet loss ratio on the remote end.
Maximum Remote-loss	Maximum number of lost packets on the remote end.
Maximum Remote-loss Ratio	Maximum packet loss ratio on the remote end.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Minimum Remote-loss	Minimum number of lost packets on the remote end.
Minimum Remote-loss Ratio	Minimum packet loss ratio on the remote end.

Display statistics about two-way frame delay measurement in test instance 1.

```
<Huawei> display y1731 statistic-type twoway-delay test-id 1
Measurement Start Time : 2017-10-18 16:16:31+01:00
Latest two-way delay statistics:
--------------------------------------------------------------------------------
Index    Delay(usec)    Delay variation(usec)
--------------------------------------------------------------------------------
  1          75                  11
  2          74                   1
  3          74                   0
  4          84                  10
  5          88                   4
  6          87                   1
  7          77                  10
  8          86                   9
  9          82                   4
 10          88                   6
 11          76                  12
 12          82                   6
 13          78                   4
 14          81                   3
 15          85                   4
 16          72                  13
 17          80                   8
 18          79                   1
 19          87                   8
 20          81                   6
 21          81                   0
 22          85                   4
 23          90                   5
 24          83                   7
 25          77                   6
 26          80                   3
 27          83                   3
 28          79                   4
 29          90                  11
 30          86                   4
--------------------------------------------------------------------------------
Average delay(usec) :        81    Average delay variation(usec) :        5
Maximum delay(usec) :        90    Maximum delay variation(usec) :        13
Minimum delay(usec) :        72    Minimum delay variation(usec) :        0
```

Table 18-60 Description of the **display y1731 statistic-type twoway-delay test-id 1** command output

Item	Description
Measurement Start Time	Start time of measurement.
Index	-
Delay(usec)	Two-way frame delay.

Item	Description
Delay variation(usec)	Two-way frame delay variation.
Average delay(usec)	Average two-way frame delay.
Maximum delay(usec)	Maximum two-way frame delay.
Minimum delay(usec)	Minimum two-way frame delay.
Average delay variation(usec)	Average two-way frame delay variation.
Maximum delay variation(usec)	Maximum two-way frame delay variation.
Minimum delay variation(usec)	Minimum two-way frame delay variation.

18.9.5 display y1731 test-info

Function

The **display y1731 test-info** command displays information about the Y.1731 test instance.

Format

display y1731 test-info [**test-id** *test-id*]

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a test instance is configured, you can run this command to check information about the test instance.

Example

Display information about all test instances.

```
<Huawei> display y1731 test-info
-------------------------------------------------------------
```

```
TestId 1 information:
-----------------------------------------------------------
MD Name                    : md1
MA Name                    : ma1
MEP ID                     : 1
Local Mac                  : 04f9-38e5-3996
Remote MEP ID              : 2
Bind Mac                   : --
Send Mac                   : 0001-0300-0204
8021p                      : --
Uplink 8021p               : --
Downlink 8021p             : --
Single LM                  : disabled
Single LM Interval         : --
Single LM Count            : --
Single LM Receive          : disabled
OneWay DM                  : disabled
OneWay DM Interval         : --
OneWay DM Count            : --
OneWay DM Packet Size      : --
OneWay DM Receive          : disabled
TwoWay DM                  : continual
TwoWay DM Interval         : 30000ms
TwoWay DM Count            : --
TwoWay DM Packet Size      : 100
TwoWay DM Receive          : enabled
Single SLM                 : continual
Single SLM Interval        : 10ms
Single SLM SendingCount    : 10
Single SLM SendTimeout     : 5s
Single SLM Receive         : enabled
Single SLM RecvTimeout     : 300s
```

Table 18-61 Description of the **display y1731 test-info** command output

Item	Description
MD Name	Name of the MD.
MA Name	Name of the MA.
MEP ID	ID of the MEP.
Local Mac	MAC address of the MEP.
Remote MEP ID	ID of the RMEP.
Bind Mac	MAC address of the RMEP.
Send Mac	MAC address in CCMs.
8021p	802.1p priority configured by the **test-id** command.
Uplink 8021p	Uplink 802.1p priority.
Downlink 8021p	Downlink 802.1p priority.
Single LM	Whether to send single-ended LM frames.
Single LM Interval	Frequency for sending single-ended LM frames.
Single LM Count	Number of sent single-ended LM frames.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Single LM Receive	Whether to receive single-ended LM frames.
OneWay DM	Whether to send one-way DMMs.
OneWay DM Interval	Frequency for sending one-way DMMs.
OneWay DM Count	Number of sent one-way DMMs.
OneWay DM Packet Size	Size of one-way DMMs.
OneWay DM Receive	Whether to receive one-way DMMs.
TwoWay DM	Whether to send two-way DMMs.
TwoWay DM Interval	Frequency for sending two-way DMMs.
TwoWay DM Count	Number of sent two-way DMMs.
TwoWay DM Packet Size	Size of two-way DMMs.
TwoWay DM Receive	Whether to receive two-way DMMs.
Single SLM	Whether to send single-ended SLM frames.
Single SLM Interval	Frequency for sending single-ended SLM frames.
Single SLM SendingCount	Number of sent single-ended SLM frames in each round.
Single SLM SendTimeout	Timeout interval for the transmit end to receive SLM frames.
Single SLM Receive	Whether to receive single-ended SLM frames.
Single SLM RecvTimeout	Timeout interval for the receive end to receive single-ended SLM frames.

18.9.6 loss-measure single-ended-synthetic continual send

Function

The **loss-measure single-ended-synthetic continual send** command configures proactive single-ended SLM.

The **undo loss-measure single-ended-synthetic continual send** command cancels the configuration.

By default, proactive single-ended SLM is not configured in an MA.

 Copyright © Huawei Technologies Co., Ltd.

Format

loss-measure single-ended-synthetic continual send test-id *test-id* **interval** { **10** | **100** | **1000** | **10000** } [**sending-count** *count-value*] [**time-out** *timeout*] [**packet-size** *packet-size*]

undo loss-measure single-ended-synthetic continual send test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
interval	Specifies the interval at which SLM frames are sent.	The value is an integer, which can be 10, 100, 1000, or 10000, in milliseconds.
sending-count *count-value*	Specifies the SLM frame sending count in each round.	The value is an integer that ranges from 1 to 1000. The default value is 10.
timeout *timeout*	Specifies the timeout interval for waiting for SLRs.	The value is an integer that ranges from 1 to 10, in seconds. The default value is 5.
packet-size *packet-size*	Specify the number of bytes of packets to be sent.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 64.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the point-to-multipoint scenario, when packet loss performance of the link needs to be counted accurately, you can configure proactive single-ended SLM.

Prerequisites

The **loss-measure single-ended-synthetic continual send** command takes effect only when the following basic CFM configurations have been performed:

- Run the **vlan** *vlan-id* command in the system view to create a VLAN and enter the VLAN view.

  By default, all interfaces belong to the default VLAN, that is, VLAN 1.
- Run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view to configure the default VLAN of an interface and add the interface to the default VLAN.

By default, VLAN 1 is the default VLAN of all interfaces.

- Run the **cfm enable (system view)** command in the system view to enable CFM globally.

  By default, CFM is disabled globally.
- Run the **cfm md** *md-name* command in the system view to create a maintenance domain (MD).
- Run the **ma** *ma-name* command in the MD view to create a maintenance association (MA).
- Run the **map vlan** *vlan-id* command in the MA view to associate a VLAN with an MA.

  By default, an MA is not associated with any VLAN.
- Run the **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** } command in the MA view to create a maintenance association end point (MEP).
- Run the **mep ccm-send** [**mep-id** *mep-id*] **enable** command in the MA view to enable a MEP in an MA to send continuity check messages (CCMs).

  By default, a MEP is disabled from sending CCMs.
- Run the **remote-mep mep-id** *mep-id* [**mac** *mac-address*] command in the MA view to create a remote maintenance association end point (RMEP) in an MA.

  NOTE

  When this command is configured on the transmit device, the **mac** *mac-address* command must be configured. Otherwise, on-demand single-ended SLM cannot be configured, and proactive single-ended SLM can be configured but does not take effect.
- Run the **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable** command to enable a MEP on the device to receive CCMs from an RMEP in the same MA.

  By default, a MEP is disabled from receiving CCMs from an RMEP.
- Run the **test-id** *test-id* **mep** *mep-id* **remote-mep** *mep-id* [**8021p** *8021p-value*] [**description** *description*] command in the MA view to configure a test instance.

  By default, no test instance is configured in an MA.

Example

Configure single-ended SLM with the test instance ID of 1 and sending interval of 10s.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] port GigabitEthernet 9/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet 9/0/0 inward
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[Huawei-md-md1-ma-ma1] remote-mep mep-id 2 mac 0001-0300-0204
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[Huawei-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[Huawei-md-md1-ma-ma1] loss-measure single-ended-synthetic continual send test-id 1 interval 10
sending-count 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

18.9.7 loss-measure single-ended-synthetic receive

18.9.7 loss-measure single-ended-synthetic receive

Function

The **loss-measure single-ended-synthetic receive** command enables the RMEP to receive SLM frames.

The **undo loss-measure single-ended-synthetic receive** command cancels the configuration.

By default, the RMEP in an MA is not configured to receive SLM frames.

Format

loss-measure single-ended-synthetic receive test-id *test-id* [**time-out** *timeout-value*]

undo loss-measure single-ended-synthetic receive test-id *test-id*

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
time-out *timeout-value*	Specifies the timeout interval for the receive end to receive SLM frames.	The value is an integer that ranges from 10 to 300, in seconds. The default value is 300.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **loss-measure single-ended-synthetic send** or **loss-measure single-ended-synthetic continual send** command is used to configure on-demand or proactive single-ended SLM, run the **loss-measure single-ended-synthetic receive** command to enable the RMEP to receive SLM frames.

Prerequisites

The **loss-measure single-ended-synthetic receive** command takes effect only when the following basic CFM configurations have been performed:

 Copyright © Huawei Technologies Co., Ltd.

- Run the **vlan** *vlan-id* command in the system view to create a VLAN and enter the VLAN view.

  By default, all interfaces belong to the default VLAN, that is, VLAN 1.
- Run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view to configure the default VLAN of an interface and add the interface to the default VLAN.

  By default, VLAN 1 is the default VLAN of all interfaces.
- Run the **cfm enable (system view)** command in the system view to enable CFM globally.

  By default, CFM is disabled globally.
- Run the **cfm md** *md-name* command in the system view to create a maintenance domain (MD).
- Run the **ma** *ma-name* command in the MD view to create a maintenance association (MA).
- Run the **map vlan** *vlan-id* command in the MA view to associate a VLAN with an MA.

  By default, an MA is not associated with any VLAN.
- Run the **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** } command in the MA view to create a maintenance association end point (MEP).
- Run the **mep ccm-send** [**mep-id** *mep-id*] **enable** command in the MA view to enable a MEP in an MA to send continuity check messages (CCMs).

  By default, a MEP is disabled from sending CCMs.
- Run the **remote-mep mep-id** *mep-id* [**mac** *mac-address*] command in the MA view to create a remote maintenance association end point (RMEP) in an MA.
- Run the **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable** command to enable a MEP on the device to receive CCMs from an RMEP in the same MA.

  By default, a MEP is disabled from receiving CCMs from an RMEP.
- Run the **test-id** *test-id* **mep** *mep-id* **remote-mep** *mep-id* [**8021p** *8021p-value*] [**description** *description*] command in the MA view to configure a test instance.

  By default, no test instance is configured in an MA.

If the configuration of the receive end is deleted or modified multiple times, the statistics may be incorrect or minus. After the configuration is completed, you are advised not to delete or modify the statistics collection task.

To modify the configuration, disable the RMEP from receiving SLM frames and reconfigure it.

For proactive single-ended SLM, you are advised to set the value of **time-out** on the receive end to be larger than the value of **interval** on the transmit end.

Example

Configure the RMEP to receive SLM frames.

```
<Huawei> system-view
[Huawei] vlan 100
```

```
[Huawei-vlan100] port GigabitEthernet 9/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet 9/0/0 inward
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[Huawei-md-md1-ma-ma1] remote-mep mep-id 2
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[Huawei-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[Huawei-md-md1-ma-ma1] loss-measure single-ended-synthetic receive test-id 1 time-out 300
```

Related Topics

18.9.6 loss-measure single-ended-synthetic continual send
18.9.8 loss-measure single-ended-synthetic send

18.9.8 loss-measure single-ended-synthetic send

Function

The **loss-measure single-ended-synthetic send** command configures on-demand single-ended SLM.

By default, on-demand single-ended SLM is not configured in an MA.

Format

loss-measure single-ended-synthetic send test-id *test-id* **interval** { **10** |**100** | **1000** | **10000** } [**sending-count** *count-value*] [**time-out** *time-out-value*] [**packet-size** *packet-size*] [**measurement-count** *measurement-count*]

Parameters

Parameter	Description	Value
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
interval	Specifies the interval at which SLM frames are sent.	The value is an integer, which can be 10, 100, 1000, or 10000, in milliseconds.
sending-count *count-value*	Specifies the SLM frame sending count in each round.	The value is an integer that ranges from 1 to 1000. The default value is 10.
time-out *time-out-value*	Specifies the timeout interval for waiting for SLRs.	The value is an integer that ranges from 1 to 10, in seconds. The default value is 5.
packet-size *packet-size*	Specify the number of bytes of packets to be sent.	The value is an integer that ranges from 64 to 1518, in bytes. The default value is 64.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
measurement-count *measurement-count*	Specifies the measurement count.	The value is an integer that ranges from 1 to 60. The default value is 1.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MEP sends a frame carrying the ETH-LM request to its RMEP and receives a frame carrying the ETH-LM response from its RMEP. You can run this command to configure on-demand SLM.

Prerequisites

The **loss-measure single-ended-synthetic continual send** command takes effect only when the following basic CFM configurations have been performed:

- Run the **vlan** *vlan-id* command in the system view to create a VLAN and enter the VLAN view.

  By default, all interfaces belong to the default VLAN, that is, VLAN 1.
- Run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view to configure the default VLAN of an interface and add the interface to the default VLAN.

  By default, VLAN 1 is the default VLAN of all interfaces.
- Run the **cfm enable (system view)** command in the system view to enable CFM globally.

  By default, CFM is disabled globally.
- Run the **cfm md** *md-name* command in the system view to create a maintenance domain (MD).
- Run the **ma** *ma-name* command in the MD view to create a maintenance association (MA).
- Run the **map vlan** *vlan-id* command in the MA view to associate a VLAN with an MA.

  By default, an MA is not associated with any VLAN.
- Run the **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** } command in the MA view to create a maintenance association end point (MEP).
- Run the **mep ccm-send** [**mep-id** *mep-id*] **enable** command in the MA view to enable a MEP in an MA to send continuity check messages (CCMs).

  By default, a MEP is disabled from sending CCMs.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **remote-mep mep-id** *mep-id* [**mac** *mac-address*] command in the MA view to create a remote maintenance association end point (RMEP) in an MA.

  NOTE

  When this command is configured on the transmit device, the **mac** *mac-address* command must be configured. Otherwise, on-demand single-ended SLM cannot be configured, and proactive single-ended SLM can be configured but does not take effect.

- Run the **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable** command to enable a MEP on the device to receive CCMs from an RMEP in the same MA.

  By default, a MEP is disabled from receiving CCMs from an RMEP.

- Run the **test-id** *test-id* **mep** *mep-id* **remote-mep** *mep-id* [**8021p** *8021p-value*] [**description** *description*] command in the MA view to configure a test instance.

  By default, no test instance is configured in an MA.

Example

Configure single-ended SLM with the test instance ID of 1, SLM frame sending interval of 1s, SLM frame sending count of 10, and timeout interval of 5s in a VLAN.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] port GigabitEthernet 9/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet 9/0/0 inward
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[Huawei-md-md1-ma-ma1] remote-mep mep-id 2 mac 0001-0300-0204
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[Huawei-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
[Huawei-md-md1-ma-ma1] loss-measure single-ended-synthetic send test-id 1 interval 1000 sending-count 10 time-out 5
```

Related Topics

18.9.7 loss-measure single-ended-synthetic receive

18.9.9 reset y1731 statistic-type

Function

The **reset y1731 statistic-type** command clears statistics about two-way frame delay measurement or single-ended SLM.

Format

reset y1731 statistic-type { **single-synthetic-loss** | **twoway-delay** } **test-id** *test-id*

Parameters

Parameter	Description	Value
twoway-delay	Clears statistics about two-way frame delay measurement.	-
single-synthetic-loss	Clears statistics about single-ended SLM.	-
test-id *test-id*	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain Y.1731 statistics within a specified period of time, run the **reset y1731 statistic-type** command to delete existing Y.1731 statistics. Then you can run the **display y1731 statistic-type** command to check packet statistics.

Prerequisites

The specified MA has been created.

Configuration Impact

After the **reset y1731 statistic-type** command is executed, statistics are cleared and cannot be restored. Exercise caution when you run this command.

Example

Clear single-ended SLM statistics in test instance 2.

```
<Huawei> reset y1731 statistic-type single-synthetic-loss test-id 2
```

18.9.10 test-id

Function

The **test-id** command configures a test instance.

The **undo test-id** command cancels the configuration.

By default, no test instance is configured in an MA.

Format

test-id *test-id* **mep** *mep-id* **remote-mep** *mep-id* [**8021p** *8021p-value*] [**description** *description*]

undo test-id *test-id*

Parameters

Parameter	Description	Value
test-id	Specifies the ID of a test instance.	The value is an integer that ranges from 1 to 4294967295.
mep *mep-id*	Specifies the ID of a MEP.	The value is an integer that ranges from 1 to 8191.
remote-mep *mep-id*	Specifies the ID of an RMEP.	The value is an integer that ranges from 1 to 8191.
8021p *8021p-value*	Specifies the 802.1p priority of packets.	The value is an integer that ranges from 0 to 7.
description *description*	Specifies the description of a test instance.	The value is a string of 1 to 63 characters.

Views

MA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure single-ended SLM or two-way frame delay measurement, run the **test-id** command to configure a test instance.

Prerequisites

The **test-id** command takes effect only when the following basic CFM configurations have been performed:

- Run the **vlan** *vlan-id* command in the system view to create a VLAN and enter the VLAN view.

  By default, all interfaces belong to the default VLAN, that is, VLAN 1.
- Run the **port** *interface-type* { *interface-number1* [**to** *interface-number2*] } &<1-10> command in the VLAN view to configure the default VLAN of an interface and add the interface to the default VLAN.

  By default, VLAN 1 is the default VLAN of all interfaces.
- Run the **cfm enable (system view)** command in the system view to enable CFM globally.

 Copyright © Huawei Technologies Co., Ltd.

By default, CFM is disabled globally.

- Run the **cfm md** *md-name* command in the system view to create a maintenance domain (MD).
- Run the **ma** *ma-name* command in the MD view to create a maintenance association (MA).
- Run the **map vlan** *vlan-id* command in the MA view to associate a VLAN with an MA.

  By default, an MA is not associated with any VLAN.
- Run the **mep mep-id** *mep-id* **interface** *interface-type interface-number* [**vlan** *vlan-id* | **pe-vid** *pe-vid* **ce-vid** *ce-vid*] { **inward** | **outward** } command in the MA view to create a maintenance association end point (MEP).
- Run the **mep ccm-send** [**mep-id** *mep-id*] **enable** command in the MA view to enable a MEP in an MA to send continuity check messages (CCMs).

  By default, a MEP is disabled from sending CCMs.
- Run the **remote-mep mep-id** *mep-id* [**mac** *mac-address*] command in the MA view to create a remote maintenance association end point (RMEP) in an MA.

  NOTE

  When this command is configured on the transmit device, the **mac** *mac-address* command must be configured. Otherwise, on-demand single-ended SLM or two-way frame delay measurement cannot be configured, and proactive single-ended SLM or two-way frame delay measurement can be configured but does not take effect.
- Run the **remote-mep ccm-receive** [**mep-id** *mep-id*] **enable** command to enable a MEP on the device to receive CCMs from an RMEP in the same MA.

  By default, a MEP is disabled from receiving CCMs from an RMEP.

Example

Configure test instance 1.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] port GigabitEthernet 9/0/0
[Huawei-vlan100] quit
[Huawei] cfm enable
[Huawei] cfm md md1
[Huawei-md-md1] ma ma1
[Huawei-md-md1-ma-ma1] map vlan 100
[Huawei-md-md1-ma-ma1] mep mep-id 1 interface GigabitEthernet 9/0/0 inward
[Huawei-md-md1-ma-ma1] mep ccm-send mep-id 1 enable
[Huawei-md-md1-ma-ma1] remote-mep mep-id 2 mac 0001-0300-0204
[Huawei-md-md1-ma-ma1] remote-mep ccm-receive mep-id 2 enable
[Huawei-md-md1-ma-ma1] test-id 1 mep 1 remote-mep 2
```

Related Topics

18.8.33 mep ccm-send enable

18.8.30 remote-mep ccm-receive enable

19 Security Commands

About This Chapter

19.1 AAA Configuration Commands
19.2 RADIUS Configuration Commands
19.3 HWTACACS Configuration Commands
19.4 HACA Configuration Commands
19.5 DAA Configuration Commands
19.6 NAC Configuration Commands
19.7 ACL Configuration Commands
19.8 Firewall Configuration Commands
19.9 Deep Security Configuration Commands
19.10 Local Attack Defense Configuration Commands
19.11 Attack Defense Configuration Commands
19.12 Traffic Suppression Configuration Commands
19.13 ARP Security Configuration Commands
19.14 DHCP Snooping Configuration Commands
19.15 IP Source Guard Configuration Commands
19.16 URPF Configuration Commands
19.17 PKI Configuration Commands
19.18 SSL Configuration Commands
19.19 HTTPS Configuration Commands
19.20 Keychain Configuration Commands

 Copyright © Huawei Technologies Co., Ltd.

19.1 AAA Configuration Commands

19.1.1 aaa

Function

The **aaa** command displays the AAA view.

The **undo aaa** command disables the AAA services.

Format

aaa

undo aaa

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Using the **aaa** command in the system view, you can enter the AAA view and perform the following security configurations for access users:

- Creating users
- Configuring user levels
- Creating an authentication scheme
- Creating an authorization scheme
- Creating a domain

After you run the **undo aaa** command, the AAA services are disabled. If the domain or service scheme configured for AAA is referenced by other modules, this domain or service scheme is not deleted, but the domain state turns to initialized. A domain in initialized state only binds to the default authentication scheme and accounting scheme, but does not bind to the authorization scheme, RADIUS server, and HWTACACS server. This command does not force online users to log out. You can run the **cut access-user** command to force users to log out.

Example

Access the AAA view.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa]
```

19.1.2 aaa abnormal-offline-record

Function

The **aaa abnormal-offline-record** command enables the device to record users' abnormal logout information.

The **undo aaa abnormal-offline-record** command disables the device from recording users' abnormal logout information.

By default, the device records users' abnormal logout information.

Format

aaa abnormal-offline-record

undo aaa abnormal-offline-record

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If users abnormally log out, run **aaa abnormal-offline-record** command to enable the record function for fault locating.

After the **undo aaa abnormal-offline-record** command is run, no abnormal logout information is recorded unless the **aaa abnormal-offline-record** command is run.

Example

Enable the device to record users' abnormal logout information.

```
<Huawei> system-view
[Huawei] aaa abnormal-offline-record
```

Disable the device from recording users' abnormal logout information.

```
<Huawei> system-view
[Huawei] undo aaa abnormal-offline-record
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.3 aaa offline-record

Function

The **aaa offline-record** command enables the device to record users' normal logout information.

The **undo aaa offline-record** command disables the device from recording users' normal logout information.

By default, the device is enabled to record user normal logout information.

Format

aaa offline-record

undo aaa offline-record

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If users fail to get online, run **aaa offline-record** command to enable the record function for fault locating.

After the **undo aaa offline-record** command is run, no logout information is recorded unless the **aaa offline-record** command is run.

Example

Enable the device to record users' normal logout information.

```
<Huawei> system-view
[Huawei] aaa offline-record
```

Disable the device from recording users' normal logout information.

```
<Huawei> system-view
[Huawei] undo aaa offline-record
```

19.1.4 aaa online-fail-record

Function

The **aaa online-fail-record** command enables the device to record users' online failures.

 Copyright © Huawei Technologies Co., Ltd.

The **undo aaa online-fail-record** command disables the device from recording users' online failures.

By default, the device records users' online failures.

Format

aaa online-fail-record

undo aaa online-fail-record

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you want to query the login failure records to find out unauthorized users, run the **aaa online-fail-record** command to enable the device to record users' online failures.

After the **undo aaa online-fail-record** command is run, no online failure is recorded unless the **aaa online-fail-record** command is run.

Example

Enable the device to record users' online failures.

```
<Huawei> system-view
[Huawei] aaa online-fail-record
```

Disable the device from recording users' online failures.

```
<Huawei> system-view
[Huawei] undo aaa online-fail-record
```

19.1.5 aaa-authen-bypass

Function

The **aaa-authen-bypass** command sets the bypass authentication timeout interval.

The **undo aaa-authen-bypass** command cancels the bypass authentication timeout interval.

By default, no bypass authentication timeout interval is set.

 Copyright © Huawei Technologies Co., Ltd.

Format

aaa-authen-bypass enable time *time-value*

undo aaa-authen-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote bypass authentication.	-
time *time-value*	Specifies the bypass authentication timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast authentication response. When a user in a user domain where multiple authentication modes (for example, RADIUS authentication and local authentication) are configured, bypass authentication is enabled, and the bypass authentication timeout interval is configured, the user will be authenticated using the local authentication mode and the bypass authentication timer is enabled simultaneously if the RADIUS server does not respond to the authentication request. When other users in the same domain are authenticated during the configured bypass authentication timeout interval, the users are directly authenticated using the local authentication mode, so that the users can be authenticated without waiting until the RADIUS server responds to their authentication requests, accelerating the authentication response.

Precautions

When only one authentication mode is configured in a user domain and the bypass authentication timer is enabled, other users in the same domain are directly considered to fail the authentication during the bypass authentication timeout interval.

Example

Set the bypass authentication timeout interval to 3 minutes.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] aaa-authen-bypass enable time 3
```

Related Topics

19.1.6 aaa-author-bypass

19.1.7 aaa-author-cmd-bypass

19.1.6 aaa-author-bypass

Function

The **aaa-author-bypass** command sets the bypass authorization timeout interval.

The **undo aaa-author-bypass** command cancels the bypass authorization timeout interval.

By default, no bypass authorization timeout interval is set.

Format

aaa-author-bypass enable time *time-value*

undo aaa-author-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote bypass authorization.	-
time *time-value*	Specifies the bypass authorization timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast authorization response. When a user in a user domain where multiple authorization modes (for example, HWTACACS authorization and local authorization) are configured, bypass authorization is enabled, and the bypass authorization timeout interval is configured, the user will be authorized using the local authorization mode and the

bypass authorization timer is enabled simultaneously if the HWTACACS server does not respond to the authorization request. When other users in the same domain are authorized during the configured bypass authorization timeout interval, the users are directly authorized using the local authorization mode, so that the users can be authorized without waiting until the HWTACACS server responds to their authorization requests, accelerating the authorization response.

Precautions

When only one authorization mode is configured in a user domain and the bypass authorization timer is enabled, other users in the same domain are directly considered to fail the authorization during the bypass authorization timeout interval.

Example

Set the bypass authorization timeout interval to 3 minutes.

```
<Huawei> system-view
[Huawei] aaa-author-bypass enable time 3
```

Related Topics

19.1.5 aaa-authen-bypass
19.1.7 aaa-author-cmd-bypass

19.1.7 aaa-author-cmd-bypass

Function

The **aaa-author-cmd-bypass** command sets the command-line bypass authorization timeout interval.

The **undo aaa-author-cmd-bypass** command cancels the command-line bypass authorization timeout interval.

By default, no command-line bypass authorization timeout interval is set.

Format

aaa-author-cmd-bypass enable time *time-value*

undo aaa-author-cmd-bypass enable

Parameters

Parameter	Description	Value
enable	Enables remote command-line bypass authorization.	-
time *time-value*	Specifies the command-line bypass authorization timeout interval.	The value is an integer that ranges from 1 to 1440, in minutes.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the scenarios that require fast command-line authorization response. When a user in a user domain where multiple command-line authorization modes (for example, HWTACACS authorization and local authorization) are configured, command-line bypass authorization is enabled, and the command-line bypass authorization timeout interval is configured, the user will be authorized using the local authorization mode and the command-line bypass authorization timer is enabled simultaneously if the HWTACACS server does not respond to the command-line authorization request. When other users in the same domain are authorized during the configured command-line bypass authorization timeout interval, the users are directly authorized using the local authorization mode, so that the users can be authorized without waiting until the HWTACACS server responds to their authorization requests, accelerating the authorization response.

Precautions

When only one command-line authorization mode is configured in a user domain and the command-line bypass authorization timer is enabled, other users in the same domain are directly considered to fail the command-line authorization during the command-line bypass authorization timeout interval.

Example

Set the command-line bypass authorization timeout interval to 3 minutes.

```
<Huawei> system-view
[Huawei] aaa-author-cmd-bypass enable time 3
```

Related Topics

19.1.5 aaa-authen-bypass

19.1.6 aaa-author-bypass

19.1.8 aaa-quiet administrator except-list

Function

The **aaa-quiet administrator except-list** command configures a user to access the network using a specified IP address when the user account is locked.

 Copyright © Huawei Technologies Co., Ltd.

The **undo aaa-quiet administrator except-list** command restores the default setting.

By default, a user cannot access the network when the account is locked.

Format

aaa-quiet administrator except-list { *ipv4-address* | *ipv6-address* } &<1-32>

undo aaa-quiet administrator except-list

Parameters

Parameter	Description	Value
ipv4-address	Specifies an IPv4 address. A user can access the network using this IPv4 address when the user account is locked.	The value must be a valid unicast address in dotted decimal notation.
ipv6-address	Specifies an IPv6 address. A user can access the network using this IPv6 address when the user account is locked.	The total length of the value is 128 bits, which are divided into eight groups. Each group contains four hexadecimal digits. The value is in the format of X:X:X:X:X:X:X:X.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In AAA view, after the function of locking the account of an AAA local authentication user or AAA remote authentication user is configured using the **19.1.57 local-aaa-user wrong-password** or **19.1.78 remote-aaa-user authen-fail** command, if a user consecutively enters an incorrect password and the number of times that the user enters an incorrect password reaches the allowed maximum number of times, the user account is locked and the user cannot access the network when the account is locked. To facilitate maintenance and management, you can run the **aaa-quiet administrator except-list** command to configure the user to access the network using a specified IP address when the user account is locked.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- This function takes effect only for the administrators.
- A maximum of 64 IPv4 and IPv6 addresses can be configured.

Example

Configure a user to access the network using the specified IP address 10.1.1.1 when the user account is locked.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] aaa-quiet administrator except-list 10.1.1.1
```

Related Topics

19.1.34 display aaa-quiet administrator except-list

19.1.9 accounting interim-fail

Function

The **accounting interim-fail** command sets the maximum number of real-time accounting failures and configures a policy used after the number of real-time accounting failures exceeds the maximum.

The **undo accounting interim-fail** command restores the default maximum number of real-time accounting failures and the default policy.

By default, the maximum number of real-time accounting failures is 3 and the device keeps users online after the number of real-time accounting failures exceeds the maximum.

Format

accounting interim-fail [**max-times** *times*] { **offline** | **online** }

undo accounting interim-fail

Parameters

Parameter	Description	Value
max-times *times*	Specifies the maximum number of real-time accounting failures. If the maximum number of real-time accounting failures is reached and the next accounting request still has no response, the device considers that accounting fails and takes a policy for users.	The value is an integer that ranges from 1 to 255. The default value is 3.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
offline	Disconnects users if real-time accounting fails.	-
online	Keeps users online if real-time accounting fails.	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the real-time accounting function takes effect, the device sends real-time accounting requests to an accounting server, and the accounting server responds to the accounting requests. If the network is unstable, for example, a jitter occurs, the device may not receive response packets. As a result, accounting is interrupted for a short period of time. To reduce or prevent accounting interruption, run the **accounting interim-fail** command to set the maximum number of real-time accounting failures. The device considers that real-time accounting fails only after the number of consecutive real-time accounting failures exceeds the maximum.

Choose one of the following policies to be applied after the maximum number of real-time accounting failures is reached:

- **online**: To prevent users from being affected by network faults, use the **online** policy to allow paid users to go online.
- **offline**: To stop providing services when accounting fails, use the **offline** policy to force paid users to go offline.

Prerequisites

The real-time accounting function has been enabled by using the **accounting realtime** command.

Precautions

The **accounting interim-fail** command does not take effect for online users, but takes effect for the users who go online after the command is executed.

Example

In the accounting scheme **scheme1**, set the maximum number of real-time accounting failures to 5 and use the **offline** policy.

```
<Huawei> system-view
[Huawei] aaa
```

```
[Huawei-aaa] accounting-scheme scheme1
[Huawei-aaa-accounting-scheme1] accounting realtime 3
[Huawei-aaa-accounting-scheme1] accounting interim-fail max-times 5 offline
```

Related Topics

19.1.10 accounting realtime

19.1.10 accounting realtime

Function

The **accounting realtime** command enables the real-time accounting function and sets the interval for real-time accounting in an accounting scheme.

The **undo accounting realtime** command disables the real-time accounting function.

By default, the device performs accounting based on user online duration, the real-time accounting function is disabled.

Format

accounting realtime *interval*

undo accounting realtime

Parameters

Parameter	Description	Value
interval	Specifies the interval for real-time accounting.	The value is an integer that ranges from 0 to 65535, in minutes. When the value is set to 0, real-time accounting is disabled. The default value is 0.

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the users who are charged based on online duration. If a user goes offline unexpectedly, the accounting server cannot receive the

 Copyright © Huawei Technologies Co., Ltd.

accounting-stop packet, so it keeps charging the user while they are not receiving a service. To solve the problem, configure the real-time accounting function on the device. After the real-time accounting function is configured, the device periodically sends real-time accounting packets to the accounting server. After receiving the real-time accounting packets, the accounting server charges the user. If the device detects that the user goes offline, it stops sending real-time accounting packets and the accounting server stops accounting. The result of real-time accounting is precise.

Precautions

- When the accounting interval is set using both the **accounting realtime** command and the Acct-Interim-Interval attribute, if the Acct-Interim-Interval value range is 60-3932100, the interval set by Acct-Interim-Interval has a higher priority. Otherwise, the interval set by the **accounting realtime** command takes effect.
- If an accounting scheme is applied to a domain, the **accounting realtime** command does not affect online users, but only takes effect for the users who go online after the command is executed.
- If *interval* is set to 0 and the IP address of the client is changed, the device still sends a real-time accounting packet carrying the changed IP address information to the RADIUS server.
- A short interval for real-time accounting requires high performance of the device and accounting server. If there are more than 1000 users, setting a long interval for real-time accounting is recommended. The following table lists the suggested real-time accounting intervals for different user quantities.

Table 19-1 Real-time accounting interval for different user quantities

User Quantity	Interval for Real-Time Accounting (Minutes)
1-99	3
100-499	6
500-999	12
≥ 1000	≥ 15

Example

In the accounting scheme **scheme1**, enable the real-time accounting function and set the interval for real-time accounting to 6 minutes.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] accounting-scheme scheme1
[Huawei-aaa-accounting-scheme1] accounting realtime 6
```

Related Topics

19.1.9 accounting interim-fail

19.1.11 accounting start-fail

Function

The **accounting start-fail** command configures a policy for accounting-start failures.

The **undo accounting start-fail** command restores the default policy for accounting-start failures.

By default, users cannot go online if accounting-start fails. That is, the **offline** policy is used.

Format

accounting start-fail { **offline** | **online** }

undo accounting start-fail

Parameters

Parameter	Description	Value
offline	Rejects users' online requests if accounting-start fails.	-
online	Allows users to go online if accounting-start fails.	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user goes online after an accounting scheme is applied, the device sends an accounting-start packet to an accounting server. When the network is working properly, the accounting server responds to the accounting-start packet. If a fault occurs on the network, the device may not receive the response packet from the accounting server. As a result, accounting fails. The device provides the following policies for accounting failures:

- **online**: To prevent users from being affected by network faults, use the **online** policy to allow paid users to go online.
- **offline**: To stop providing services when accounting fails, use the **offline** policy to force paid users to go offline.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The command takes effect only when the accounting mode configured using the **19.1.13 accounting-mode** command is HWTACACS or RADIUS.

Example

In the accounting scheme **scheme1**, use the **online** policy for accounting-start failures.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] accounting-scheme scheme1
[Huawei-aaa-accounting-scheme1] accounting start-fail online
```

19.1.12 accounting-copy radius-server

Function

The **accounting-copy radius-server** command enables the RADIUS accounting packet copy function and configures a RADIUS server template for level-2 accounting.

The **undo accounting-copy radius-server** command disables the RADIUS accounting packet copy function.

By default, the RADIUS accounting packet copy function is disabled.

Format

accounting-copy radius-server *template-name*

undo accounting-copy radius-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The value must be an existing RADIUS server template name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The existing RADIUS server on the network performs authentication, authorization, and accounting for users. User login and logout information is sent to the server through accounting packets. Users want to deploy an independent RADIUS accounting server (called the level-2 RADIUS accounting server) to obtain user login and logout information for analyzing user behavior and managing users' access to the network. However, the device currently does not send accounting packets to the level-2 RADIUS accounting server. In this case, you can configure the RADIUS accounting packet copy function on the device. After this function is configured, the device sends user login and logout information to the level-2 RADIUS accounting server through accounting packets for third-party user behavior analysis.

Prerequisites

The RADIUS server template has been created using the **radius-server template** command.

Precautions

- Ensure that the IP address of the configured level-2 RADIUS accounting server must be different from that of the level-1 RADIUS accounting server (including the active/standby RADIUS accounting server).
- Ensure that the level-2 RADIUS accounting server template configured in the domain is different from the RADIUS server template for authentication and accounting in the domain. If they are the same, the **accounting-copy radius-server** command cannot be configured and the system displays an error message during the command configuration.

Example

In the **huawei** domain, set the IP addresses of the RADIUS authentication and accounting servers to 10.1.1.1, port IDs of the servers to 1813 and 1814, name of the RADIUS server template to which the RADIUS authentication and accounting servers belong to **t1**, IP address of the level-2 RADIUS accounting server to 10.1.1.2, port ID of the server to 1814, and name of the RADIUS server template to which the level-2 RADIUS accounting server belongs to **t2**.

```
<Huawei> system-view
[Huawei] radius-server template t1
[Huawei-radius-t1] radius-server authentication 10.1.1.1 1813
[Huawei-radius-t1] radius-server accounting 10.1.1.1 1814
[Huawei-radius-t1] quit
[Huawei] radius-server template t2
[Huawei-radius-t2] radius-server accounting 10.1.1.2 1814
[Huawei-radius-t2] quit
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] radius-server t1
[Huawei-aaa-domain-huawei] accounting-copy radius-server t2
```

19.1.13 accounting-mode

Function

The **accounting-mode** command configures an accounting mode in an accounting scheme.

The **undo accounting-mode** command restores the default accounting mode in an accounting scheme.

By default, the accounting mode is **none**.

Format

accounting-mode { **hwtacacs** | **none** | **radius** | **haca** }

undo accounting-mode

Parameters

Parameter	Description	Value
hwtacacs	Indicates that accounting is performed by an HWTACACS server.	-
none	Indicates non-accounting.	-
radius	Indicates that accounting is performed by a RADIUS server.	-
haca	Indicates that accounting is performed by an HACA server.	-

Views

Accounting scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Enterprises or carriers need to generate revenue by charging users who are accessing the Internet.

When a user goes online, accounting starts after the user is authenticated and authorized. When the user goes offline, accounting stops. The client sends the account packet containing the user's online duration to the accounting server.

To charge users, set the accounting mode to RADIUS or HWTACACS or HACA. Generally, the accounting mode is consistent with the authentication mode. If you do not need to charge users, set the accounting mode to none.

Precautions

The device does not support local accounting. When the authentication scheme configured using the **19.1.19 authentication-mode (authentication scheme view)** command defines local authentication, you need to run the **accounting-mode none** command to configure non-accounting or run the **19.1.11 accounting start-fail** command to configure a policy for accounting-start failures.

Follow-up Procedure

Apply the accounting scheme to a domain to enable the device to charge the users in the domain using the **19.1.50 domain (AAA view)** command.

Example

Set the accounting mode to RADIUS in the accounting scheme **scheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] accounting-scheme scheme1
[Huawei-aaa-accounting-scheme1] accounting-mode radius
```

19.1.14 accounting-scheme (AAA domain view)

Function

The **accounting-scheme** command applies an accounting scheme to a domain.

The **undo accounting-scheme** command restores the default accounting scheme of a domain.

By default, the accounting scheme named **default** is applied to a domain. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Format

accounting-scheme *accounting-scheme-name*

undo accounting-scheme

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The accounting scheme must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To charge users in a domain, create an accounting scheme and perform configurations in the accounting scheme, for example, set the accounting mode and policy for accounting-start failures. Run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to the domain.

Prerequisites

An accounting scheme has been created and configured using the **19.1.15 accounting-scheme (AAA view)** command. For example, the accounting mode and policy for accounting-start failures have been configured.

Example

Apply the accounting scheme **account1** to the domain **isp1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] accounting-scheme account1
[Huawei-aaa-accounting-account1] quit
[Huawei-aaa] domain isp1
[Huawei-aaa-domain-isp1] accounting-scheme account1
```

Restore the default accounting scheme of the domain **isp2**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain isp2
[Huawei-aaa-domain-isp2] undo accounting-scheme
```

Related Topics

19.1.15 accounting-scheme (AAA view)

19.1.38 display accounting-scheme

19.1.15 accounting-scheme (AAA view)

Function

The **accounting-scheme** command creates an accounting scheme and displays the accounting scheme view.

The **undo accounting-scheme** command deletes an accounting scheme.

By default, there is an accounting scheme named **default** in the system. This default accounting scheme can be modified but cannot be deleted. In this default accounting scheme, non-accounting is used and the real-time accounting function is disabled.

Format

accounting-scheme *accounting-scheme-name*

undo accounting-scheme *accounting-scheme-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To charge users in a domain, create and configure an accounting scheme, for example, the accounting mode and policy for accounting-start failures. Run the **accounting-scheme** command in the AAA domain view to apply the accounting scheme to the domain.

Follow-up Procedure

After an accounting scheme is created:

- Run the **accounting interim-fail** command to set the maximum number of real-time accounting failures and configure a policy used after a real-time accounting failure.
- Run the **accounting realtime** command to enable the real-time accounting function and set the interval for real-time accounting in an accounting scheme.
- Run the **accounting start-fail** command to configure a policy for accounting-start failures.
- Run the **accounting-mode** command to configure an accounting mode in an accounting scheme.

After an accounting scheme is configured, run the **19.1.14 accounting-scheme (AAA domain view)** command in the AAA domain view to apply the accounting scheme to a domain.

Precautions

If the configured accounting scheme does not exist, the **accounting-scheme** command in the AAA view creates an accounting scheme and displays the accounting scheme view. If the configured accounting scheme already exists, the

 Copyright © Huawei Technologies Co., Ltd.

accounting-scheme command in the AAA view displays the accounting scheme view directly.

The system supports a maximum of 32 accounting schemes, including the default accounting scheme.

To delete an accounting scheme applied to a domain, run the **undo accounting-scheme (AAA domain view)** command.

Example

Create an accounting scheme named **scheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] accounting-scheme scheme1
[Huawei-aaa-accounting-scheme1]
```

Enter the default accounting scheme view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] accounting-scheme default
[Huawei-aaa-accounting-default]
```

Related Topics

19.1.14 accounting-scheme (AAA domain view)

19.1.16 admin-user privilege level

Function

The **admin-user privilege level** command configures a user as an administrator to log in to the device and sets the user level.

The **undo admin-user privilege level** command cancels the default user level.

By default, the user level is not configured.

Format

admin-user privilege level *level*

undo admin-user privilege level

Parameters

Parameter	Description	Value
level	Specifies the level of a user. A larger value indicates a higher user level. After logging in to the device, a user can run only the commands of the same level or lower levels.	The value is an integer that ranges from 0 to 15.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device provides hierarchical management of commands. A command has a level, and a user can run only the commands of the same level or lower levels. By using the **admin-user privilege level** command to set the user level, the device controls commands used by users.

By default, commands are classified into the following levels:

- Level 0 (visit level): Commands at level 0 include diagnosis commands such as ping and tracert commands and commands that are used to access a remote device such as the Telnet client. Commands at level 0 cannot be used to save configuration files.
- Level 1 (monitoring level): Commands at level 1 are used for system maintenance, including display commands. Commands at level 1 cannot be used to save configuration files.
- Level 2 (configuration level): Commands at level 2 are used for service configuration, including routing commands and commands at each network layer to provide network services for users.
- Level 3 (management level): Commands at level 3 are used for basic operations of the system to support services, including file system, FTP, Trivial File Transfer Protocol (TFTP), configuration file switching commands, slave board control commands, user management commands, command level configuration commands, and debugging commands.

To manage users refinedly, upgrade command levels to levels 0 to 15. You can run the **command-privilege level** command to upgrade command levels in a batch.

- If non-authentication is used, the administrator level is specified using the **user privilege** command in the VTY interface view.

 Copyright © Huawei Technologies Co., Ltd.

- If local authentication is used, the administrator level is specified using the **local-user privilege level** command.
- If remote authentication is used, the administrator level can be set in the following ways, in descending order of priority:
  a. Using the user level sent by an authentication server to the device after authentication has succeeded
  b. Running the **admin-user privilege level** command to set the administrator level in a service scheme
  c. Running the **user privilege** command to set the user level in the VTY interface view
- If remote authentication and local authentication are configured, remote authentication is first used. If remote authentication fails, local authentication is used. The administrator level can be set in the following ways, in descending order of priority:
  a. Using the user level sent by an authentication server to the device after authentication has succeeded
  b. Running the **local-user privilege level** command to set the local user level

  NOTE

  The local user level is used only when the remote authentication server is faulty. If the remote authentication server responds to authentication requests but does not deliver user levels, the configured local user level does not take effect.

The device can update the configuration in a domain dynamically. After a service scheme is applied to a domain, you can directly modify the user level in the service scheme but cannot unbind the service scheme from the domain. To delete the service scheme, run the **undo service-scheme (AAA domain view)** command.

Follow-up Procedure

Run the **display service-scheme** command to view the user level in a service scheme.

Example

Configure a user as an administrator to log in to the device and set the administrator level to 15.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] admin-user privilege level 15
```

Related Topics

19.1.47 display service-scheme

19.1.60 local-user

19.1.90 service-scheme (AAA view)

3.8.24 user privilege

19.1.17 authentication { roam-accounting | update-ip-accounting } * enable

Function

The **authentication** { **roam-accounting** | **update-ip-accounting** } * **enable** command enables a device to send accounting packets for roaming and address updating.

The **undo authentication** { **roam-accounting** | **update-ip-accounting** } * **enable** command disables a device from sending accounting packets for roaming and address updating.

By default, the device is enabled to send accounting packets for roaming and address updating.

Format

authentication { **roam-accounting** | **update-ip-accounting** } * **enable**

undo authentication { **roam-accounting** | **update-ip-accounting** } * **enable**

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the device sends accounting packets for roaming and address updating to the accounting server. Some accounting servers may not require the accounting packets. In this case, resources on the device are occupied. You can run the **undo authentication** { **roam-accounting** | **update-ip-accounting** } * **enable** command to disable the device from sending accounting packets for roaming and address updating, saving resources on the device. After roaming and address updating are complete, the device sends accounting packets again and the accounting function is not affected.

- **roam-accounting** indicates that accounting packets are immediately sent during roaming.
- Only wireless user devices support the **roam-accounting** parameter.
- **update-info-accounting** indicates that accounting packets are immediately sent during address updating.
- If the terminal information (including the DHCP Option, UA, or LLDP information) is updated for the first time, the device immediately triggers

 Copyright © Huawei Technologies Co., Ltd.

real-time accounting. If the terminal information is not updated for the first time, the device only updates the user entry and reports the new terminal information through subsequent accounting messages.

- After the **undo authentication** { **roam-accounting** | **update-ip-accounting** } * **enable** command is configured, the device does not send the accounting packet immediately after obtaining the packet, and waits until the real-time accounting timer expires.

Example

Disable a device from sending accounting packets for address updating.

```
<Huawei> system-view
[Huawei] authentication-profile name test
[Huawei-authen-profile-test] undo authentication update-ip-accounting enable
```

19.1.18 authentication roam-accounting update-session-mode

Function

The **authentication roam-accounting update-session-mode** command enables the accounting session update mode during roaming accounting.

The **undo authentication roam-accounting update-session-mode** command disables the accounting session update mode during roaming accounting.

By default, the accounting session update mode is not used during roaming accounting.

Format

authentication roam-accounting update-session-mode

undo authentication roam-accounting update-session-mode

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

For multi-link accounting users, each link corresponds to different values of the RADIUS attribute Acct-Session-Id, but all links correspond to the same value of the RADIUS attribute Acct-Multi-Session-Id. After the roaming accounting function is enabled for users using the **authentication roam-accounting enable** command,

users' accounting session IDs are carried in the RADIUS attribute Acct-Session-Id. However, if the Acct-Session-Id changes, the server performs accounting again. To resolve this problem, you can run the **authentication roam-accounting update-session-mode** command to configure the accounting session update mode during roaming accounting. After this command is configured, user accounting packets carry the RADIUS attribute Acct-Multi-Session-Id. During roaming accounting, the RADIUS attribute Acct-Multi-Session-Id is used to identify users.

Precautions

This function takes effect only after the roaming accounting function is enabled for users using the **authentication roam-accounting enable** command.

Example

Enables the accounting session update mode during roaming accounting.

```
<Huawei> system-view
[Huawei] authentication-profile name test
[Huawei-authentication-profile-test] authentication roam-accounting update-session-mode
```

19.1.19 authentication-mode (authentication scheme view)

Function

The **authentication-mode** command configures an authentication mode for an authentication scheme.

The **undo authentication-mode** command restores the default authentication mode in an authentication scheme.

By default, local authentication is used.

Format

authentication-mode { **hwtacacs** | **local** | **radius** | **haca** } * [**none**]

authentication-mode none

undo authentication-mode

Parameters

Parameter	Description	Value
hwtacacs	Authenticates users using an HWTACACS server. To perform HWTACACS authentication, configure an HWTACACS authentication server in an HWTACACS server template.	-
local	Authenticates users locally.	-
radius	Authenticates users using a RADIUS server. To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
haca	Authenticates users using a Huawei Agile Cloud Authentication (HACA) server.	-
none	Indicates non-authentication. That is, users access the network without being authenticated.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users, configure an authentication mode in an authentication scheme.

If multiple authentication modes are configured in an authentication scheme, the authentication modes are used according to the sequence in which they were configured.

- In the sequence of local authentication followed by remote authentication:

  If a login account is not created locally but exists on the remote server, the authentication mode is changed from local authentication to remote authentication.

  If a login account is created locally and on the remote server, and local authentication fails because the password is incorrect, remote authentication will not be performed.
- In the sequence of remote authentication followed by local authentication:

  If a login account is created locally but not on the remote server, remote authentication fails and local authentication will not be performed.

  A user is authenticated using the local authentication mode only when the remote server is Down or does not respond to the user's authentication request.

  NOTE

  Normally, if the remote server is Down or does not respond, local authentication is used. If a large number of users need to go online through the device, the device may be unable to process responses from the server in a timely manner. As a result, the AAA module of the device cannot receive responses from the server until the protection timer expires. These users then cannot go online and cannot be authenticated using local authentication. In this case, reconnect these offline users to the device.

You can configure multiple authentication modes in an authentication scheme to reduce authentication failure possibilities.

- After the **authentication-mode radius local** command is used, the device cannot complete RADIUS authentication if it fails to connect to the RADIUS authentication server. In this case, the device starts local authentication.
- After the **authentication-mode local radius** command is used, if the entered user name exists on the device but the entered password is incorrect, the user fails the authentication; if the entered user name does not exist on the device, the user is redirected to the RADIUS authentication mode and is authenticated based on user information on the RADIUS server.

NOTE

- When both RADIUS authentication and non-authentication are configured, if the user fails the RADIUS authentication, non-authentication cannot be used. As a result, a user fails to log in.
- If you run the **authentication-mode** command to configure non-authentication and run the **authentication-mode (user interface view)** command to configure AAA authentication, the device does not allow administrators to log in from the user interface view.

Precautions

If non-authentication is configured using the **authentication-mode** command, users can pass the authentication using any user name or password. Therefore, to protect the device and improve network security, you are advised to enable authentication, allowing only authenticated users to access the device or network.

Example

Configure the authentication scheme named **scheme1** to use RADIUS authentication.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authentication-scheme scheme1
[Huawei-aaa-authen-scheme1] authentication-mode radius
```

19.1.20 authentication-scheme (AAA domain view)

Function

The **authentication-scheme** command applies an authentication scheme to a domain.

The **undo authentication-scheme** command restores the default configuration of the authentication scheme in a domain.

By default, the authentication scheme named **radius** is applied to the **default** domain, the authentication scheme named **default** is applied to the **default_admin** domain, and the authentication scheme named **radius** is applied to other domains.

Format

authentication-scheme *scheme-name*

undo authentication-scheme

Parameters

Parameter	Description	Value
scheme-name	Specifies the name of an authentication scheme.	The value must be an existing authentication scheme name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users in a domain, run the **authentication-scheme (AAA domain view)** command to apply an authentication scheme to a domain.

Prerequisites

An authentication scheme has been created and configured with required parameters, for example, the authentication mode and authentication mode for upgrading user levels.

Example

Apply the authentication scheme named **scheme1** to a domain named **domain1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain domain1
[Huawei-aaa-domain-domain1] authentication-scheme scheme1
```

Related Topics

19.1.21 authentication-scheme (AAA view)
19.1.39 display authentication-scheme

19.1.21 authentication-scheme (AAA view)

Function

The **authentication-scheme** command creates an authentication scheme and displays its view.

The **undo authentication-scheme** command deletes an authentication scheme.

By default, the default authentication scheme is used. This default authentication scheme can be modified but cannot be deleted. In the default authentication scheme:

- Local authentication is used.
- The **offline** policy is used for authentication failures.

By default, the system also provides the authentication scheme **radius**. The **radius** authentication scheme can be modified, but cannot be deleted. In the **radius** authentication scheme:

- RADIUS authentication is used.
- The **offline** policy is used for authentication failures.

Format

authentication-scheme *scheme-name*

undo authentication-scheme *scheme-name*

Parameters

Parameter	Description	Value
scheme-name	Specifies the name of an authentication scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users, run the **authentication-scheme** command to create an authentication scheme. Creating an authentication scheme is necessary before performing authentication-relevant configurations.

Follow-up Procedure

After an authentication scheme is created, run the **authentication-mode (authentication scheme view)** command to configure an authentication mode in an authentication scheme.

After an authentication scheme is configured, run the **authentication-scheme (AAA domain view)** command to apply the authentication scheme to a domain.

Precautions

If the configured authentication scheme does not exist, the **authentication-scheme** command creates an authentication scheme and displays the authentication scheme view. If the configured authentication scheme already

 Copyright © Huawei Technologies Co., Ltd.

exists, the **authentication-scheme** command directly displays the authentication scheme view.

To delete an authentication scheme applied to a domain, run the **undo authentication-scheme (AAA domain view)** command.

Example

Create an authentication scheme named **newscheme**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authentication-scheme newscheme
[Huawei-aaa-authen-newscheme]
```

Access the default authentication scheme view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authentication-scheme default
[Huawei-aaa-authen-default]
```

Related Topics

19.1.20 authentication-scheme (AAA domain view)

19.1.39 display authentication-scheme

19.1.22 authentication-super

Function

The **authentication-super** command configures an authentication mode for upgrading user levels in an authentication scheme.

The **undo authentication-super** command restores the default authentication mode for upgrading user levels in an authentication scheme.

By default, the **super** mode is used. That is, local authentication is used.

Format

authentication-super { **hwtacacs** | **super** } * [**none**]

authentication-super none

undo authentication-super

Parameters

Parameter	Description	Value
hwtacacs	Uses HWTACACS authentication to upgrade user levels.	-
super	Uses local authentication to upgrade user levels.	-

Parameter	Description	Value
none	Indicates that user levels can be upgraded without authentication.	-

Views

Authentication scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If users in a domain need to upgrade their levels, the device requests the users to enter the password to authenticate the users. If AAA authentication has been configured using the **authentication-mode (user interface view)** command, run the **authentication-super** command to configure an authentication mode for upgrading user levels.

When you use the **super** command to switch a user level to a lower level or the same level, no authentication is required. When you use the **super** command to switch a user level to a higher level, authentication is required. The user can be granted rights only after being authenticated.

- If **super** is used and the local authentication is specified, run the **local-user** command in the AAA view to create a local user and set parameters for the local user.
- If **hwtacacs** is used and the HWTACACS authentication is specified, perform configurations relevant to HWTACACS authentication.
- If **none** is used, no authentication is required.

Precautions

If multiple authentication modes are configured in an authentication scheme, these authentication modes are used in the sequence in which they were configured. The device uses another authentication mode only when it does not receive any response in the current authentication. The device does not switch to another authentication mode if the user fails to pass one authentication mode.

Example

Set the authentication mode to HWTACACS authentication in the authentication scheme **scheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authentication-scheme scheme1
[Huawei-aaa-authen-scheme1] authentication-super hwtacacs
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

3.8.3 authentication-mode (user interface view)
19.1.20 authentication-scheme (AAA domain view)
19.1.21 authentication-scheme (AAA view)
19.1.39 display authentication-scheme

19.1.23 authorization-cmd

Function

The **authorization-cmd** command configures command-specific authorization for an administrator of a specific level. After command-specific authorization is enabled and an administrator of a specific level logs in to the device, the commands that the administrator enters can be executed only after being authorized by the HWTACACS server.

The **undo authorization-cmd** command disables command-specific authorization for an administrator of a specific level.

By default, the command-specific authorization is disabled. That is, an administrator of any level can execute only commands of or below its level after logging in to the device.

Format

authorization-cmd *privilege-level* **hwtacacs** [**local**] [**none**]

undo authorization-cmd *privilege-level*

Parameters

Parameter	Description	Value
privilege-level	Specified the administrator level.	The value is an integer that ranges from 0 to 15.
hwtacacs	Indicates HWTACACS authorization.	-
local	Indicates local authorization.	-
none	Indicates that command line authorization is directly performed for a user if the HWTACACS server does not respond to the authorization request of the user.	-

Views

Authorization scheme view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After being authorized, the users at a certain level can run the commands of the same or lower levels. Command line authorization can be configured to implement minimum user rights control. When command line authorization is enabled, each command entered by users can be executed only after being authorized. After command line authorization is enabled for users at a certain level, the commands run by the users at that level must be authorized by an HWTACACS server.

Precautions

You are advised to configure local authorization as a backup of command line authorization. If command line authorization cannot be performed because of a failure on an HWTACACS server, the device starts local authorization.

After the **authorization-cmd** command is executed, command line authorization does not take effect immediately. Command line authorization takes effect only when an authorization scheme containing command line authorization is applied to administrator view correctly.

NOTICE

After an authorization scheme containing command line authorization is applied to administrator view, if you run the **undo authorization-cmd** command, an online administrator at a certain level cannot run any commands except for the **quit** command. The administrator needs to log in again.

Example

Configure command line authorization administrators at level 2.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authorization-scheme scheme1
[Huawei-aaa-author-scheme1] authorization-cmd 2 hwtacacs
```

19.1.24 authorization-mode

Function

The **authorization-mode** command configures an authorization mode for an authorization scheme.

The **undo authorization-mode** command restores the default authorization mode in an authorization scheme.

By default, local authorization is used.

Format

authorization-mode { **hwtacacs** | **if-authenticated** | **local** } * [**none**]

authorization-mode none

undo authorization-mode

Parameters

Parameter	Description	Value
hwtacacs	Indicates that the user is authorized by an HWTACACS server.	-
if-authenticated	Indicates that only the user who succeeds in authentication (authentication exemption excluded) is authorized. The configuration of if-authenticated authorization does not take effect in RADIUS authentication.	-
local	Authenticates users locally	-
none	Indicates non-authorization.	-

Views

Authorization scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authorize users, configure an authorization mode in an authorization scheme.

You can configure multiple authorization modes in an authorization scheme to reduce the chance of authorization failures.

After the **authorization-mode hwtacacs local** command is used, if it fails to connect to the HWTACACS authentication server and HWTACACS authorization cannot be performed, the device starts local authorization.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- If multiple authorization modes are used in an authorization scheme, the **if-authenticated** mode or **none** mode must be used as the last authorization mode.
- When the authorization mode is **if-authenticated** or **none**, the user privilege level is inherited from the user domain or is the same as that set in the VTY user view.
- If multiple authorization modes are configured in an authorization scheme, the authorization modes are used according to the sequence in which they were configured. The device uses another authorization mode only when it does not receive any response in the current authorization.

Example

Configure the authorization scheme named **scheme1** to apply HWTACACS authorization.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authorization-scheme scheme1
[Huawei-aaa-author-scheme1] authorization-mode hwtacacs
```

19.1.25 authorization-modify mode

Function

The **authorization-modify mode** command configures the update mode for user authorization information delivered by the authorization server.

The **undo authorization-modify mode** command restores the default update mode for user authorization information delivered by the authorization server.

By default, the update mode of user authorization information delivered by the authorization server is **overlay**. That is, the new user authorization information overwrites all existing user authorization information.

Format

authorization-modify mode { **modify** | **overlay** }

undo authorization-modify mode

NOTE

The modify mode is valid for only the user authorization information, such as ACL rule and dynamic VLAN.

Parameters

Parameter	Description	Value
modify	Indicates the **modify** mode.	-
overlay	Indicates the **overlay** mode.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

The authorization server can deliver all or part of user authorization information, such as the ACL rule and dynamic VLAN.

You can run the **authorization-modify mode** command to configure one of the following update modes for user authorization information delivered by the authorization server:

- **modify**: modification mode indicating that new user authorization information overwrites only existing user authorization information of the same type.
- **overlay**: overwriting mode indicating that new user authorization information overwrites all existing user authorization information.

If the authorization server has delivered ACL 3001 to a user, and the administrator needs to deliver new authorization information:

- In the **modify** mode, if the new authorization information is ACL 3002, the authorization information of the user is ACL 3002. If the new authorization information is VLAN 100, the authorization information of the user is ACL 3001 and VLAN 100.
- In the **overlay** mode, no matter whether the new authorization information is ACL 3002 or VLAN 100, the authorization information of the user is the new ACL or VLAN.

This command takes effect for only the authorization information delivered by the RADIUS server.

After a user group or service scheme is authorized to a user on the device and a certain attribute configured in the user group or service scheme is modified on the server, if other configured attributes need to be modified, the authorization information on the server must contain the previously modified attribute. Otherwise, the original attribute value in the service group or service scheme will be restored. For example, to modify an attribute in a user group:

1. The device authorizes the user group configured with the VLAN and ACL attributes to a user.
2. To modify the VLAN attribute, authorize the new VLAN attribute to the user through the RADIUS server.
3. To modify the ACL attribute after the VLAN attribute is modified, you must authorize the modified VLAN attribute and new ACL attribute through the RADIUS server. Otherwise, the original VLAN attribute in the user group will be restored.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the update mode of user authorization information delivered by the authorization server to **modify**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authorization-modify mode modify
```

19.1.26 authorization-scheme (AAA domain view)

Function

The **authorization-scheme** command applies an authorization scheme to a domain.

The **undo authorization-scheme** command unbinds an authorization scheme from a domain.

By default, no authorization scheme is applied to a domain.

Format

authorization-scheme *authorization-scheme-name*

undo authorization-scheme

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The authorization scheme must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RADIUS integrates authentication and authorization; therefore, RADIUS authorization and authentication must be used together. HWTACACS separates authentication from authorization; therefore, you can configure another authorization type even if HWTACACS authentication, local authentication, or non-authentication is used.

 Copyright © Huawei Technologies Co., Ltd.

To authorize users in a domain, run the **authorization-scheme (AAA domain view)** command.

Prerequisites

An authorization scheme has been created and configured with required parameters, for example, the authorization mode and command line authorization.

Example

Apply the authorization scheme **author1** to the domain **isp1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authorization-scheme author1
[Huawei-aaa-author-author1] quit
[Huawei-aaa] domain isp1
[Huawei-aaa-domain-isp1] authorization-scheme author1
```

Related Topics

19.1.27 authorization-scheme (AAA view)
19.1.40 display authorization-scheme

19.1.27 authorization-scheme (AAA view)

Function

The **authorization-scheme** command creates an authorization scheme and enters the authorization scheme view, or directly enters an existing authorization scheme view.

The **undo authorization-scheme** command deletes an authorization scheme.

By default, the default authorization scheme is used. This default authorization scheme can be modified but cannot be deleted. In the default authorization scheme, local authorization is used and command line authorization is disabled.

Format

authorization-scheme *authorization-scheme-name*

undo authorization-scheme *authorization-scheme-name*

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

 Copyright © Huawei Technologies Co., Ltd.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

RADIUS integrates authentication and authorization; therefore, RADIUS authorization and authentication must be used together. HWTACACS separates authentication from authorization; therefore, you can configure another authorization type even if HWTACACS authentication, local authentication, or non-authentication is used. You must run the **authorization-scheme** command to create an authorization scheme before performing authorization-relevant configurations, for example, setting the authorization mode and command line authorization function.

Follow-up Procedure

After an authorization scheme is created:

- Run the **authorization-mode** command to configure an authorization mode in an authorization scheme.
- Run the **authorization-cmd** command to configure command line authorization for users at a certain level.

After an authorization scheme is configured, run the **authorization-scheme (AAA domain view)** command to apply the authorization scheme to a domain.

Precautions

- If the configured authorization scheme does not exist, the **authorization-scheme (AAA view)** command creates an authorization scheme and displays the authorization scheme view.
- If the configured authorization scheme already exists, the **authorization-scheme (AAA view)** command directly displays the authorization scheme view.

The system supports a maximum of 32 authorization schemes, including the default authorization scheme.

To delete the authorization scheme applied to a domain, run the **undo authorization-scheme (AAA domain view)** command.

Example

Create an authorization scheme named **scheme0**.

```
<Huawei> system-view
[Huawei] aaa
```

```
[Huawei-aaa] authorization-scheme scheme0
[Huawei-aaa-author-scheme0]
```

Enter the default authorization scheme view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] authorization-scheme default
[Huawei-aaa-author-default]
```

Related Topics

19.1.26 authorization-scheme (AAA domain view)

19.1.28 auto-update url (service scheme view)

Function

The **auto-update url** command configures the URL and version number of a service scheme.

The **undo auto-update url** command deletes the URL and version number of a service scheme.

By default, the URL and version number of a service scheme are not configured.

Format

auto-update url *url-string* **version** *version-number*

undo auto-update url

Parameters

Parameter	Description	Value
url-string	Indicates the URL.	The value is a string of 1 to 208 case-sensitive characters.
version-number	Indicates the version number.	The value is an integer that ranges from 1 to 4294967294.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

The AAA service scheme allows the URL and version number to be bound. IPSec binds the AAA service scheme to the IPSec policy template and sends the URL and version number to users.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the URL **ftp://huawei:huawei2012@10.10.10.1/test** and version number **1** for the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] auto-update url ftp://huawei:huawei2012@10.10.10.1/test version 1
```

Related Topics

19.1.47 display service-scheme

19.1.29 cmd recording-scheme

Function

The **cmd recording-scheme** command applies a policy in a recording scheme to record the commands executed on the device.

The **undo cmd recording-scheme** command deletes a policy from a recording scheme.

By default, the commands that are used on the device are not recorded.

Format

cmd recording-scheme *recording-scheme-name*

undo cmd recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During the device configuration, incorrect operations may result in network faults. After the **cmd recording-scheme** command is executed, you can view records of the commands executed on the device to locate the network faults.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A recording scheme has been created by using the **recording-scheme** command and a recording mode has been configured by using the **recording-mode hwtacacs** command.

Example

Configure a policy in the recording scheme **scheme0** to record the commands executed on the device.

```
<Huawei> system-view
[Huawei] hwtacacs-server template hw1
[Huawei-hwtacacs-hw1] quit
[Huawei] aaa
[Huawei-aaa] recording-scheme scheme0
[Huawei-aaa-recording-scheme0] recording-mode hwtacacs hw1
[Huawei-aaa-recording-scheme0] quit
[Huawei-aaa] cmd recording-scheme scheme0
```

Related Topics

19.1.45 display recording-scheme

19.1.76 recording-mode hwtacacs

19.1.77 recording-scheme

19.1.30 cut access-user

Function

The **cut access-user** command terminates one or multiple access user connections, also forcibly disconnecting online users.

Format

cut access-user { **domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **access-slot** *slot-id* | **ssid** *ssid-name* | **user-group** *group-number* | **user-id** *begin-number* [*end-number*] | **username** *user-name* }

cut access-user access-type { **admin** [**ftp** | **ssh** | **telnet** | **terminal** | **web**] | **ppp** | **l2tp** } [**username** *user-name*]

Parameters

Parameter	Description	Value
domain *domain-name*	Disconnects sessions in a specified domain.	The value must be the name of an existing domain.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Disconnects sessions on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id* [**qinq** *qinq-vlan-id*]	Disconnects sessions in a specified VLAN. ● *vlan-id* specifies the ID of a VLAN. In QinQ applications, this parameter specifies the inner VLAN ID. ● *qinq-vlan-id* specifies the outer VLAN ID.	The values of *vlan-id* and *qinq-vlan-id* are integers that range from 1 to 4094.
ip-address *ip-address*	Disconnects sessions initiated by a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value is a string of 1 to 31 case-sensitive characters without spaces.
mac-address *mac-address*	Disconnects sessions initiated by a specified MAC address.	The value is in H-H-H format. An H contains 4 hexadecimal digits.
service-scheme *service-scheme-name*	Terminates connections based on the service scheme.	The value must be the name of an existing service scheme.
access-slot *slot-id*	Disconnects sessions on a specified LPU.	The value range depends on the model of the device.
ssid *ssid-name*	Disconnects sessions initiated by a service set identifier (SSID).	The SSID must already exist.
user-group *group-number*	Disconnects sessions of a user-group.	The value is a string of 1 to 64 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.
user-id *begin-number* [*end-number*]	Disconnects sessions of a specified user.	The user-id must exist on the device.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
username *user-name*	Disconnects sessions of a user with a specified user name.	The value must be the name of an existing user.
access-type	Displays information about the users using the specified authentication mode.	-
admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**]	Displays information about the administrators using the specified authentication mode. ● **ftp**: FTP user ● **ssh**: SSH user ● **telnet**: Telnet user ● **terminal**: Terminal user ● **web**: Web user	-
ppp	Displays information about online users using PPP authentication.	-
l2tp	Displays information about online users using L2TP authentication.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Performing some configurations, such as AAA, on the device, requires that no users be online. You can run the **cut access-user** command to disconnect sessions.

Precautions

The **cut access-user** command interrupts all services of the user whose session is torn down.

If the character string of the user name contains spaces (for example, a b), you can run the **display access-user username "a b"** command to view online users.

If the character string of the user name contains spaces and quotation marks ("") simultaneously, you cannot use the user name to view online users. In this case, you can run the **display access-user | include** *username* command to view the user ID of the online user, and then run the **display access-user user-id** *user-id* command to view the user. Alternatively, you can run the **cut access-user user-id** *user-id* command to force the user to go offline.

Example

Tear down the session initiated by the IP address 10.1.1.1.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] cut access-user ip-address 10.1.1.1
```

Related Topics

19.1.37 display access-user (All views)

19.1.31 dhcp-server group (service scheme view)

Function

The **dhcp-server group** command specifies an existing DHCP server group in a service scheme.

The **undo dhcp-server group** command deletes the DHCP server group in a service scheme.

By default, no DHCP server group is specified in a service scheme.

Format

dhcp-server group *group-name*

undo dhcp-server group

Parameters

Parameter	Description	Value
group-name	Specifies the name of a DHCP server group.	The value is a string of 1 to 32 case-sensitive characters without spaces. The DHCP server group must have been configured using the **dhcp server group** command.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

If a service scheme is bound to a domain, the service scheme configurations are valid for the users in the domain.

Example

Specify the DHCP server group **group1** for the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] dhcp-server group group1
```

Related Topics

8.3.40 dhcp server group

19.1.47 display service-scheme

19.1.32 display aaa

Function

The **display aaa** command displays information about normal logout, abnormal logout, and login failures.

Format

display aaa { **offline-record** | **abnormal-offline-record** | **online-fail-record** } { **all** | **reverse-order** | **domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **mac-address** *mac-address* | **access-slot** *slot-number* | **time** *start-time end-time* [**date** *start-date end-date*] | **username** *user-name* [**time** *start-time end-time* [**date** *start-date end-date*]] } [**brief**]

Parameters

Parameter	Description	Value
offline-record	Displays normal logout records.	-
abnormal-offline-record	Displays abnormal logout records.	-
online-fail-record	Displays login failure records.	-
all	Displays all login and logout records.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
reverse-order	Displays the records in a sequence reverse to the sequence in which they were generated. That is, the latest records are displayed first.	-
domain *domain-name*	Specifies the name of a domain.	The value is a string of 1 to 64 case-insensitive characters, excluding spaces, *, ?, and ".
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
vlan *vlan-id*	Specifies the inner VLAN ID.	The value is an integer that ranges from 1 to 4094.
qinq *qinq-vlan-id*	Specifies the outer VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies an IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 characters without spaces. It is case sensitive.
mac-address *mac-address*	Specifies a MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
access-slot *slot-number*	Specifies the slot ID.	The value is an integer. It must be the slot ID of an operating LPU.
username *user-name*	Specifies a user.	The value must be an existing user.
time *start-time end-time*	Specifies a time range.	The format is HH:MM:SS, indicating hour:minute:second.
date *start-date end-date*	Specifies a date.	The format is YYYY/MM/DD. YYYY is the year, MM is the month, and DD is the day.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
brief	Displays brief login and logout information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command allows you to view information about user normal logouts, abnormal logouts, and login failures based on the domain name, interface, IP address, VPN instance, MAC address, or slot ID.

Precautions

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following 19; that is, only 22 characters are displayed.

Example

View information about user normal logouts in domain **rds**.

```
<Huawei> display aaa offline-record domain rds
 ----------------------------------------------------------------------
  User name              : test@rds
  Domain name            : rds
  User MAC               : 0021-9746-b67c
  User access type       : 802.1x
  User access interface : GigabitEthernet1/0/2
  Qinq vlan/User vlan    : 0/1
  User IP address        : 192.168.2.2
  User IPV6 address      : -
  User ID                : 19
  User login time        : 2008/10/01 04:49:39
  User offline time      : 2008/10/01 04:59:43
  User offline reason    : EAPOL user request
  User name to server    : test@rds
  AP ID                  : 1
  Radio ID               : 0
  AP MAC                 : b001-0000-ac01
  SSID                   : ssid1
```

```
-----------------------------------------------------------------
Are you sure to display some information?(y/n)[y]:
```

Table 19-2 Description of the **display aaa offline-record domain** command output

Item	Description
User name	User name.
Domain name	Domain of a user.
User MAC	MAC address of a user.
User access type	Access type of a user. ● 802.1x indicates that the user accesses the network through 802.1X. ● PPPoE indicates that the user accesses the network through PPPoE. ● FTP indicates that the user accesses the network through FTP. ● Telnet indicates that the user accesses the network through Telnet. ● Terminal indicates that the user accesses the network through terminal. ● SSH indicates that the user accesses the network through SSH. ● x25-pad indicates that the user accesses the network through x25-pad. ● HTTP indicates that the user accesses the network through HTTP. ● Web indicates that the user accesses the network through web. ● Bind indicates that the user accesses the network through IP session. ● SSLVPN indicates that the user accesses the network through SSL VPN. For the related command, see **19.1.67 local-user service-type**.
User access interface	Access interface of a user.

Item	Description
Qinq vlan/User vlan	VLAN that a user belongs to. ● In QinQ application, QinQvlan indicates the outer VLAN ID and Uservlan indicates the inner VLAN ID. ● For a common VLAN, Uservlan indicates the VLAN ID, and QinQvlan is 0.
User IP address	IP address of a user.
User IPV6 address	IPv6 address of a user.
User ID	Index of a user.
User login time	Time when a user goes online.
User offline time	Time when a user goes offline.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
User offline reason	Reason why a user fails to go online or offline. The common reasons are as follows: ● The value "EAPOL user request" indicates that an 802.1X user requests to go offline. ● The value "PPP user request" indicates that a PPP user requests to go offline. ● The value "Web user request" indicates that a web user requests to go offline. ● The value "AAA cut command" indicates that a user is deleted using command line. ● The value "Session time out" indicates that a session times out. ● The value "Idle cut" indicates that a user is disconnected because the user does not perform any operation within a specified period. ● The value "PPP authentication fail" indicates a PPP authentication failure. ● The value "STA disassociation" indicates that an STA is disassociated. ● The value "console reset or disable port" indicates that the management interface is down. ● The value "Interface net down" indicates that an interface is down. ● The value "No authentication server configured" indicates that no authentication server is configured. ● The value "No radius-server template bound" indicates that no RADIUS server template is bound. ● The value "No tacacs-server template bound" indicates that no TACACS server template is bound. ● The value "No accounting server configured" indicates that no accounting server is configured.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• The value "Accounting server no response" indicates that the accounting server does not respond. • The value "Local Authentication user block" indicates that the local user is locked. • The value "Authorize vlan error" indicates that VLAN authorization fails.
User name to server	User name sent by the device to the server.
AP ID	ID of the AP that a wireless user associates with.
Radio ID	ID of the radio that a wireless user associates with.
AP MAC	MAC address of the AP that a wireless user associates with.
SSID	SSID that a wireless user associates with.

19.1.33 display aaa configuration

Function

The **display aaa configuration** command displays the AAA configurations, for example, the domain, authentication scheme, authorization scheme, and accounting scheme.

Format

display aaa configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

AAA configurations are limited by system specifications. Before performing AAA configurations, run the **display aaa configuration** command to check whether there are sufficient resources.

Example

Display the AAA summary.

```
<Huawei> display aaa configuration

  Domain Name Delimiter            : @
  Domainname parse direction       : Left to right
  Domainname location              : After-delimiter
  Administrator user default domain: default_admin
  Normal user default domain       : default
  Domain                           : total: 256     used: 3
  Authentication-scheme            : total: 33      used: 1
  Accounting-scheme                : total: 32      used: 2
  Authorization-scheme             : total: 32      used: 1
  Service-scheme                   : total: 256     used: 1
  Recording-scheme                 : total: 32      used: 0
  Local-user                       : total: 512     used: 10
  Local-user block retry-interval  : 30 Min(s)
  Local-user block retry-time      : 5
  Local-user block time            : 30 Min(s)
  Remote-user block retry-interval : 5 Min(s)
  Remote-user block retry-time     : 3
  Remote-user block time           : 5 Min(s)
  Session timeout invalid enable   : Yes
```

Table 19-3 Description of the **display aaa configuration** command output

Item	Description
Domain Name Delimiter	Domain name delimiter, which can be any of the following characters: \ / : < > | @ ' %. The default domain name delimiter is @.
Domain	Number of domains. ● total: indicates the total number of domains that can be created. ● used: indicates the number of domains that have been created.
Domainname parse direction	Parsing direction of the user name and domain name. ● Left to right ● Right to left
Domainname location	Domain name location. ● After-delimiter: The domain name is placed behind the domain name delimiter. ● Before-delimiter: The domain name is placed before the domain name delimiter.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Administrator user default domain	Domain name of administrator users.
Normal user default domain	Domain name of normal users.
Authentication-scheme	Number of authentication schemes. ● total: indicates the total number of authentication schemes that can be created. ● used: indicates the number of authentication schemes that have been created.
Accounting-scheme	Number of accounting schemes. ● total: indicates the total number of accounting schemes that can be created. ● used: indicates the number of accounting schemes that have been created.
Authorization-scheme	Number of authorization schemes. ● total: indicates the total number of authorization schemes that can be created. ● used: indicates the number of authorization schemes that have been created.
Service-scheme	Number of service schemes. ● total: indicates the total number of service schemes that can be created. ● used: indicates the number of service schemes that have been created.
Recording-scheme	Number of recording schemes. ● total: indicates the total number of recording schemes that can be created. ● used: indicates the number of recording schemes that have been created.
Local-user	Number of local users. ● total: indicates the total number of local users that can be created. ● used: indicates the number of local users that have been created.
Local-user block retry-interval	Authentication retry interval of a local account.
Local-user block retry-time	Maximum number of consecutive authentication failures.
Local-user block time	Locking time of a local account.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Remote-user block retry-interval	Authentication retry interval of a remote AAA authentication user.
Remote-user block retry-time	Maximum number of consecutive authentication failures.
Remote-user block time	Locking time of a remote AAA authentication user.
Session timeout invalid enable	• Yes: The device will not disconnect or reauthenticate users when the RADIUS server delivers session-timeout with value 0. • No: The device will disconnect or reauthenticate users when the RADIUS server delivers session-timeout with value 0.

Related Topics

19.1.1 aaa
19.1.50 domain (AAA view)

19.1.34 display aaa-quiet administrator except-list

Function

The **display aaa-quiet administrator except-list** command displays IP addresses that a user can use to access the network when the user account is locked.

Format

display aaa-quiet administrator except-list

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

After a user is configured to access the network using a specified IP address when the user account is locked using the **19.1.8 aaa-quiet administrator except-list** command, you can run the **display aaa-quiet administrator except-list** command to check information about the specified IP addresses.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display IP addresses that a user can use to access the network when the user account is locked.

```
<Huawei> display aaa-quiet administrator except-list
 ------------------------------------------------------------------------------
 Admin silent whitelist
 ------------------------------------------------------------------------------
 10.2.2.1
 10.2.2.2
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
```

Table 19-4 Description of the **display aaa-quiet administrator except-list** command output

Item	Description
Admin silent whitelist	IP addresses configured in a whitelist.

19.1.35 display aaa statistics access-type-authenreq

Function

The **display aaa statistics access-type-authenreq** command displays the number of requests for MAC, Portal, or 802.1X authentication.

Format

display aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, or 802.1X authentications.

To view the number of requests for MAC, Portal, or 802.1X authentication, run the **display aaa statistics access-type-authenreq** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the number of requests for MAC, Portal, or 802.1X authentication.

```
<Huawei> display aaa statistics access-type-authenreq
mac     authentication request     :2
portal  authentication request     :0
dot1x   authentication request     :0
```

Table 19-5 Description of the **display aaa statistics access-type-authenreq** command output

Item	Description
mac authentication request	Number of MAC authentication requests.
portal authentication request	Number of Portal authentication requests.
dot1x authentication request	Number of 802.1X authentication requests.

19.1.36 display aaa statistics offline-reason

Function

The **display aaa statistics offline-reason** command displays the reasons why users go offline.

Format

display aaa statistics offline-reason

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display aaa statistics offline-reason** command helps you know the reason why a user goes offline. You can locate network faults according to the command output.

Example

Display reasons why users go offline.

```
<Huawei> display aaa statistics offline-reason
19  User request to offline      :2
87  AAA cut command              :1
```

Table 19-6 Description of the display aaa statistics offline-reason command output

Item	Description
19/87	Reason code.
User request to offline	A user requested to go offline.
2/1	Number of times users go offline.
AAA cut command	A user is disconnected by the **19.1.30 cut access-user** command.

19.1.37 display access-user (All views)

Function

The **display access-user** command displays information about online users (including access users and administrators).

Format

display access-user [**domain** *domain-name* | **interface** *interface-type interface-number* [**vlan** *vlan-id* [**qinq** *qinq-vlan-id*]] | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **ipv6-address** *ipv6-address* | **access-slot** *slot-id* | **user-group** *user-group-name* | **username** *user-name*] [**detail**]

display access-user [**mac-address** *mac-address* | **service-scheme** *service-scheme-name* | **user-id** *user-id* | **ssid** *ssid-name*]

display access-user statistics

display access-user access-type { **admin** [**ftp** | **ssh** | **telnet** | **terminal** | **web**] | **ppp** | **l2tp** } [**username** *user-name*]

Parameters

Parameter	Description	Value
domain *domain-name*	Displays information about users in a specified domain.	The domain name must already exist.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about users on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id* [**qinq** *qinq-vlan-id*]	Displays information about users in a VLAN. ● *vlan-id* specifies the ID of a VLAN. In QinQ applications, this parameter specifies the inner VLAN ID. ● *qinq-vlan-id* specifies the outer VLAN ID.	The values of *vlan-id* and *qinq-vlan-id* are integers that range from 1 to 4094.
ip-address *ip-address*	Displays information about the user with a specified IP address. **NOTE** When the user type is NAC, details about the user are displayed. When the user is in another type, brief information about the user is displayed.	The value of *ip-address* is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The VPN instance must already exist.
ipv6-address *ipv6-address*	Displays information about the user with a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.
mac-address *mac-address*	Displays information about the user with a specified MAC address.	The value is in H-H-H format. An H contains four hexadecimal digits.
service-scheme *service-scheme-name*	Displays information about the user with a specified service scheme.	The service scheme must already exist.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
access-slot *slot-id*	Displays information about users connecting to a specified LPU.	The value range depends on the model of the device.
ssid *ssid-name*	Specifies the SSID.	The SSID must already exist.
statistics	Displays user statistics on the device. ● Historical user statistics: displays historical WLAN user statistics on the device. ● Current online user statistics: displays current user statistics on the device.	-
user-group *user-group-name*	Displays information about users in a specified user group.	The value is a string of 1 to 64 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.
user-id *user-id*	Displays information about sessions of a specified user. If this parameter is specified, detailed information about the user is displayed.	The user-id must exist on the device.
username *user-name*	Displays information about the user with a user name.	The user name must already exist.
detail	Displays detailed information about users.	-
access-type	Displays information about the users using the specified authentication mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
admin [**ftp** | **ssh** | **telnet** | **terminal** | **web**]	Displays information about the administrators using the specified authentication mode. ● **ftp**: FTP user ● **ssh**: SSH user ● **telnet**: Telnet user ● **terminal**: Terminal user ● **web**: Web user	-
ppp	Displays information about online users using PPP authentication.	-
l2tp	Displays information about online users using L2TP authentication.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

This command displays information about user sessions on the device.

Precautions

If the character string of the user name contains spaces (for example, a b), you can run the **display access-user username "a b"** command to view online users.

If the character string of the user name contains spaces and quotation marks ("") simultaneously, you cannot use the user name to view online users. In this case, you can run the **display access-user | include** *username* command to view the user ID of the online user, and then run the **display access-user user-id** *user-id* command to view the user. Alternatively, you can run the **cut access-user user-id** *user-id* command to force the user to go offline.

When displaying VPN user entries based on user IP address, you must set the **vpn-instance** *vpn-instance-name* parameter to specify the VPN instance to which the IP address belongs.

 Copyright © Huawei Technologies Co., Ltd.

If **user-id** is specified, detailed information about the specified user is displayed. If **user-id** is not specified, brief information about all online users is displayed, including the user ID, user name, IP address, and MAC address of each user.

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following 19; that is, only 22 characters are displayed.

When querying user information based on MAC addresses, or VLANs, the device only displays information about 802.1X, MAC address, or Portal authentication users.

Example

Display the users connected to the interface Eth2/0/0.

```
<Huawei> display access-user interface ethernet 2/0/0
 ----------------------------------------------------------------------------------------------
 UserID Username                    IP address              MAC            Status
 ----------------------------------------------------------------------------------------------
 36     test@rds                    -                       0021-9746-b67c  Success
 17     c0a80642@none               192.168.6.66            4487-fc40-f05b  Success
 ----------------------------------------------------------------------------------------------
 Total 2,2 printed
```

NOTE

If you specify the **include** or **exclude** parameter in the command, the values of **Total** and **printed** are still the total number of users.

Display the user with the user ID being 36.

```
<Huawei> display access-user user-id 36

Basic:
  User ID                        : 36
  User name                      : test@rds
  Domain-name                    : rds
  User MAC                       : 0021-9746-b67c
  User IP address                : -
  User IPv6 address              : -
  User access Interface          : Ethernet2/0/0
  QinQVlan/UserVlan              : 0/10
  User access time               : 2010/11/28 23:37:27
  User accounting session ID     : Huawei04007000000010d****3000036
  User access type               : 802.1x
  User Privilege                 : 15
  Terminal Device Type           : Data Terminal
  Dynamic ACL ID(Effective)      : 3100
  Dynamic group index(Effective) : 10
  Dynamic group name(Effective)  : nac
  Upstream CAR CIR               : 300
  Upstream CAR PIR               : 200
  Upstream CAR CBS               : 56400
  Upstream CAR PBS               : 37600
  Up packets number(Packet)      : 239
```

```
  Up bytes number(Byte)          : 19,171
  Downstream CAR CIR             : 500
  Downstream CAR PIR             : 400
  Downstream CAR CBS             : 94000
  Downstream CAR PBS             : 75200
  Down packets number(Packet)     : 4
  Down bytes number(Byte)         : 256

AAA:
  User authentication type        : 802.1x authentication
  Current authentication method   : RADIUS
  Current authorization method    : -
  Current accounting method       : RADIUS
```

Display the user with the user ID being 17.

```
<Huawei> display access-user user-id 17

Basic:
  User ID                         : 17
  User name                       : c0a80642
  Domain-name                     : none
  User MAC                        : 4487-fc40-f05b
  User IP address                 : 192.168.6.66
  User IPv6 address               : -
  User access Interface           : Ethernet2/0/0
  QinQVlan/UserVlan               : 0/6
  User access time                : 2014/09/10 13:15:39
  User accounting session ID      : Huawei04007000000010d****3000036
  User access type                : WEB
  User Privilege                  : 15
  AP ID                           : 0
  AP name                         : ap-0
  Radio ID                        : 0
  AP MAC                          : 0a0b-0c00-0500
  SSID                            : 222222
  Online time                     : 417(s)
  Web-server IP address           : 10.9.9.1
  User session timeout            : 4(h)

AAA:
  User authentication type        : WEB authentication
  Current authentication method   : None
  Current authorization method    : -
  Current accounting method       : None
```

Display user statistics on the device.

```
<Huawei> display access-user statistics
Historical wireless user statistics:
 Access total number          : 358
 Access failed number         : 0
 Access success number        : 358
 Abnormal offline number      : 0
Current online user statistics:
  Total access number             : 0
  MAC access number               : 0
  802.1x access number            : 0
  Web access number               : 0
  Static access number            : 0
  PPPoE access number             : 0
  Unauthenticated access number   : 0
```

Table 19-7 Description of the **display access-user** command output

Item	Description
Basic	Basic information about a user.

Item	Description
User ID	ID of a user.
User name	Name of a user.
Domain-name	Name of the domain that a user belongs to.
User MAC	MAC address of a user.
User IP address	IP address of a user.
User IPv6 address	IPv6 address of a user.
User access Interface	Access interface connected to a user.
Status	Whether a user joins a VLAN. ● Open: no authentication ● Success: authentication is successful ● Pre-authen: pre-authentication ● Client-no-resp: the client does not respond ● Fail-authorized: authorization upon authentication failure ● Web-server-down: web server is Down
QinQVlan/UserVlan	VLAN that a user belongs to. ● In QinQ applications, QinQVlan indicates the outer VLAN ID and UserVlan indicates the inner VLAN ID. ● For a common VLAN, UserVlan indicates the VLAN ID, and QinQVlan is 0.
User access time	Time when a user goes online.
User accounting session ID	ID of the accounting session for a user.
User access type	Access type of a user.
User Privilege	Level of a user.
Terminal Device Type	Terminal device type of a user.
Dynamic ACL ID(Effective)	ACL ID. ● Effective: The dynamic ACL has taken effect. ● Effective: The dynamic ACL has taken effect.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dynamic group index(Effective)	ID of a UCL group.This option is available only in NAC unified mode.
Dynamic group name(Effective)	Name of a UCL group. This option is available only in NAC unified mode.
Upstream CAR CIR	Upstream CIR dynamically delivered by the RADIUS server to online user.
Upstream CAR PIR	Upstream PIR dynamically delivered by the RADIUS server to online user.
Upstream CAR CBS	Upstream CBS dynamically delivered by the RADIUS server to online user.
Upstream CAR PBS	Upstream PBS dynamically delivered by the RADIUS server to online user.
Up packets number(Packet)	Number of incoming packets of a user.
Up bytes number(Byte)	Number of bytes in incoming packets of a user.
Downstream CAR CIR	Downstream CIR dynamically delivered by the RADIUS server to online user.
Downstream CAR PIR	Downstream PIR dynamically delivered by the RADIUS server to online user.
Downstream CAR CBS	Downstream CBS dynamically delivered by the RADIUS server to online user.
Downstream CAR PBS	Downstream PBS dynamically delivered by the RADIUS server to online user.
Down packets number(Packet)	Number of outgoing packets of a user.
Down bytes number(Byte)	Number of bytes in outgoing packets of a user.
Web-server IP address	IP address of the WEB server.
User session timeout	Timeout interval of user sessions.
AP ID	ID of the AP connected to users.
AP name	Name of the AP connected to users.
Radio ID	ID of the radio.
AP MAC	MAC address of the AP connected to users.
SSID	SSID of a STA.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Online time	STA online time.
AAA	AAA information about a user.
User authentication type	Authentication type of a user, which depends on the access type of the user.
Current authentication method	Authentication mode.
Current authorization method	Authorization mode.
Current accounting method	Accounting mode.
Historical user statistics	Number of history users.
Access total number	Total access times users.
Access failed number	Number of times users fail to access.
Access success number	Number of times users successfully access.
Abnormal offline number	Number of times users go offline unexpectedly.
Current online user statistics	Number of online users.
Total access number	Total number of access users.
MAC access number	Number of online users passing MAC address authentication.
802.1x access number	Number of online users passing 802.1X authentication.
Web access number	Number of online users passing web authentication.
Static access number	Number of online static users.
PPPoE access number	Number of online PPPoE users.
Unauthenticated access number	Number of users failing authentication.

19.1.38 display accounting-scheme

Function

The **display accounting-scheme** command displays the configuration of accounting schemes, including accounting scheme names and accounting modes.

 Copyright © Huawei Technologies Co., Ltd.

Format

display accounting-scheme [*accounting-scheme-name*]

Parameters

Parameter	Description	Value
accounting-scheme-name	Specifies the name of an accounting scheme.	The accounting scheme must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the accounting scheme configuration is complete, run the **display accounting-scheme** command to view the configuration of accounting schemes.

Before applying an accounting scheme to a domain, run the **display accounting-scheme** command to check whether configuration of the accounting scheme is correct.

Precautions

The **display accounting-scheme** command displays the detailed configuration if the name of an accounting scheme is specified. Otherwise, this command displays only the summary of accounting schemes.

Example

Display the summary of all accounting schemes.

```
<Huawei> display accounting-scheme
  ------------------------------------------------------------------
  Accounting-scheme-name              Accounting-method
  ------------------------------------------------------------------
  default                             None
  radius-1                            RADIUS
  tacas-1                             HWTACACS
  haca-1                              HACA

  ------------------------------------------------------------------
  Total of accounting-scheme: 4
```

Display the detailed configuration of the default accounting scheme.

```
<Huawei> display accounting-scheme default

  Accounting-scheme-name              : default
```

```
Accounting-method                    : None
Realtime-accounting-switch           : Disabled
Realtime-accounting-interval(min)    : -
Start-accounting-fail-policy         : Offline
Realtime-accounting-fail-policy      : Online
Realtime-accounting-failure-retries  : 3
```

Table 19-8 Description of the **display accounting-scheme** command output

Item	Description
Accounting-scheme-name	Name of an accounting scheme. To create an accounting scheme, run the **accounting-scheme (AAA view)** command.
Accounting-method	Accounting mode in the accounting scheme. The accounting modes are as follows: ● HWTACACS: indicates that an HWTACACS server performs accounting. ● None: indicates non-accounting. ● RADIUS: indicates that a RADIUS server performs accounting. ● HACA: indicates that an HACA server performs accounting. To configure an accounting mode, run the **accounting-mode** command.
Realtime-accounting-switch	Whether the real-time accounting function is enabled: ● Disabled: indicates that the real-time accounting function is disabled. ● Enabled: indicates that the real-time accounting function is enabled. To set the interval for real-time accounting, run the **accounting realtime** command.
Realtime-accounting-interval(min)	Interval for real-time accounting. To set the interval for real-time accounting, run the **accounting realtime** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Start-accounting-fail-policy	Policy used for accounting-start failures. ● Offline: disconnects users. ● Online: keeps users online. To configure a policy for accounting-start failures, run the **accounting start-fail** command.
Realtime-accounting-fail-policy	Policy used for real-time accounting failures. ● Offline: disconnects users. ● Online: keeps users online. To configure the policy used for real-time accounting failures, run the **accounting interim-fail** command.
Realtime-accounting-failure-retries	Number of retries before a real-time accounting failure is confirmed. To set the number of real-time retries before a real-time accounting failure is confirmed, run the **accounting interim-fail** command.

19.1.39 display authentication-scheme

Function

The **display authentication-scheme** command displays the configuration of authentication schemes.

Format

display authentication-scheme [*authentication-scheme-name*]

Parameters

Parameter	Description	Value
authentication-scheme-name	Specifies the name of an authentication scheme.	The authentication scheme must already exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the authentication scheme configuration is complete, run the **display authentication-scheme** command to view the configuration of authentication schemes.

Precautions

The **display authentication-scheme** command displays the detailed configuration if the command is executed in the authentication scheme view or the name of an authentication scheme is specified. Otherwise, this command displays only the summary of authentication schemes.

Example

Display the summary of all authentication schemes.

```
<Huawei> display authentication-scheme
  -----------------------------------------------------------------
  Authentication-scheme-name          Authentication-method
  -----------------------------------------------------------------
  default                              Local
  radius                              RADIUS
  -----------------------------------------------------------------
  Total of authentication scheme: 2
```

Display the detailed configuration of the default authentication scheme.

```
<Huawei> display authentication-scheme default

  Authentication-scheme-name          : default
  Authentication-method               : Local
```

Table 19-9 Description of the **display authentication-scheme** command output

Item	Description
Authentication-scheme-name	Name of an authentication scheme. To create an authentication scheme, run the **19.1.21 authentication-scheme (AAA view)** command.
Authentication-method	Authentication mode in an authentication scheme. To configure an authentication mode in an authentication scheme, run the **19.1.19 authentication-mode (authentication scheme view)** command.

 Copyright © Huawei Technologies Co., Ltd.

19.1.40 display authorization-scheme

Function

The **display authorization-scheme** command displays the configuration of authorization schemes.

Format

display authorization-scheme [*authorization-scheme-name*]

Parameters

Parameter	Description	Value
authorization-scheme-name	Specifies the name of an authorization scheme.	The authorization scheme must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the authorization scheme configuration is complete, run the **display authorization-scheme** command to view the configuration of authorization schemes.

Before applying an authorization scheme to a domain, run the **display authorization-scheme** command to check whether configuration of the authorization scheme is correct.

Precautions

The **display authorization-scheme** command displays the detailed configuration if the name of an authorization scheme is specified. Otherwise, this command displays only the summary of authorization schemes.

Example

Display the summary of all authorization schemes.

```
<Huawei> display authorization-scheme
  ------------------------------------------------------------------
  Authorization-scheme-name          Authorization-method
  ------------------------------------------------------------------
  default                            Local
```

```
 scheme0                        Local
 ------------------------------------------------------------------
  Total of authorization-scheme: 2
```

Display the detailed configuration of the authorization scheme **scheme0**.

```
<Huawei> display authorization-scheme scheme0
--------------------------------------------------------------------------
 Authorization-scheme-name   : scheme0
 Authorization-method        : Local
 Authorization-cmd level  0   : Disabled
 Authorization-cmd level  1   : Disabled
 Authorization-cmd level  2   : Disabled
 Authorization-cmd level  3   : Disabled
 Authorization-cmd level  4   : Disabled
 Authorization-cmd level  5   : Disabled
 Authorization-cmd level  6   : Disabled
 Authorization-cmd level  7   : Disabled
 Authorization-cmd level  8   : Disabled
 Authorization-cmd level  9   : Disabled
 Authorization-cmd level 10   : Disabled
 Authorization-cmd level 11   : Disabled
 Authorization-cmd level 12   : Disabled
 Authorization-cmd level 13   : Disabled
 Authorization-cmd level 14   : Disabled
 Authorization-cmd level 15   : Disabled
 Authorization-cmd no-response-policy    : Online
--------------------------------------------------------------------------
```

Table 19-10 Description of the **display authorization-scheme** command output

Item	Description
Authorization-scheme-name	Name of the authorization scheme. To create an authorization scheme, run the **authorization-scheme (AAA view)** command.
Authorization-method	Authorization mode set for the authorization scheme. To configure an authorization mode, run the **authorization-mode** command.
Authorization-cmd level	Whether the command line authorization function is enabled for a user with a specified level: ● Disabled: indicates that the command line authorization function is disabled. ● Enabled: indicates that the command line authorization function is enabled. To set the command line authorization function, run the **authorization-cmd** command.
Authorization-cmd no-response-policy	Policy for command line authorization failures, in which users are allowed to go online.

19.1.41 display domain

Function

The **display domain** command displays the domain configuration.

Format

display domain [**name** *domain-name*]

Parameters

Parameter	Description	Value
name *domain-name*	Specifies the name of a domain. If this parameter is not specified, brief information about all domains is displayed.	The domain name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a domain is created by the **domain** command with required parameters specified, you can run the **display domain** command to view the domain configuration.

Example

Display brief information about all domains.

```
<Huawei> display domain
  ------------------------------------------------------------------------------
  index    DomainName
  ------------------------------------------------------------------------------
  0        default
  1        default_admin
  ------------------------------------------------------------------------------
  Total: 2
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-11 Description of the **display domain** command output

Item	Description
index	Index of a domain. To configure this parameter, run the **19.1.50 domain (AAA view)** command.
DomainName	Name of a domain. To configure this parameter, run the **19.1.50 domain (AAA view)** command.

Display the configuration of the domain **default**.

```
<Huawei> display domain name default

 Domain-name                      : default
 Domain-index                     : 0
 Domain-state                     : Active
 Authentication-scheme-name       : default
 Accounting-scheme-name           : default
 Authorization-scheme-name        : -
 Service-scheme-name              : -
 RADIUS-server-template           : -
 HWTACACS-server-template         : -
 User-group                       : -
 Push-url-address                 : -
 Domain auto block Time-range     : asd
 Flow-statistic                   : enable
 Tariff-level
  Qos-profile                     : huawei
  Accounting-flag                 : enable
```

Table 19-12 Description of the **display domain name** command output

Item	Description
Domain-name	Name of a domain. To configure this item, run the **19.1.50 domain (AAA view)** command.
Domain-index	Index of a domain. To configure this item, run the **19.1.50 domain (AAA view)** command.
Domain-state	Status of a domain. ● Active: indicates that the domain is activated. ● Block: indicates that the domain is blocked. To configure this item, run the **19.1.91 state (AAA domain view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication-scheme-name	Name of the authentication scheme used in a domain. To configure this item, run the **19.1.20 authentication-scheme (AAA domain view)** command.
Accounting-scheme-name	Name of the accounting scheme used in a domain. To configure this item, run the **19.1.14 accounting-scheme (AAA domain view)** command.
Authorization-scheme-name	Name of the authorization scheme used in a domain. To configure this item, run the **19.1.26 authorization-scheme (AAA domain view)** command.
Service-scheme-name	Name of the service scheme used in a domain. To configure this item, run the **19.1.89 service-scheme (aaa domain view)** command.
RADIUS-server-template	Name of the RADIUS server template used in a domain. To configure this item, run the **19.2.21 radius-server (aaa domain view)** command.
HWTACACS-server-template	Name of the HWTACACS server template used in a domain. To configure this item, run the **19.3.5 hwtacacs-server** command.
User-group	Name of the user group authorized to users in a domain. To configure this item, run the **19.1.94 user-group (AAA domain view)** command.
Push-url-address	Pushed URL used in a domain. To configure this item, run the **19.6.80 force-push** command.
Domain auto block Time-range	Automatic block time range of a domain.
Flow-statistic	Whether traffic statistics collection is enabled for users in a domain. ● enable: The function is enabled. ● -: The function is disabled. To configure this item, run the **19.1.92 statistic enable (AAA domain view)** command.
Tariff-level	Tariff level.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Qos-profile	QoS profile corresponding to the tariff level.
Accounting-flag	Whether accounting is enabled for the tariff level. ● enable: The function is enabled. ● disable: The function is disabled.

19.1.42 display local-user

Function

The **display local-user** command displays information about local users.

Format

display local-user [**domain** *domain-name* | **state** { **active** | **block** } | **username** *user-name*] *

Parameters

Parameter	Description	Value
domain *domain-name*	Displays information about local users in a specified domain.	The domain name must already exist.
state { **active** | **block** }	Displays the attributes of local users in the specified state. ● **active**: indicates the active state. ● **block**: indicates the blocking state.	-
username *user-name*	Displays information about a specified local user name.	The user name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display local-user** command output helps you check the configuration of local users and isolate faults related to the local users.

Precautions

If no parameter is specified, brief information about all local users is displayed. If a parameter is specified, detailed information about the specified local user is displayed.

Low-level users cannot view information about high-level users.

Example

Display brief information about local users.

```
<Huawei> display local-user
  ------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
  ------------------------------------------------------------------------------
  user-a                          A      A         0
  user-c                          A      A         0
  ------------------------------------------------------------------------------
  Total 2 user(s)
```

Display detailed information about the local user **user-a**.

```
<Huawei> display local-user username user-a
  The contents of local user(s):
  Password              : ****************
  State                 : active
  Service-type-mask     : A
  Privilege level       : -
  Ftp-directory         : -
  Access-limit          : Yes
  Access-limit-max      : 4294967295
  Accessed-num          : 0
  Idle-timeout          : -
  User-group            : -
  Account-type          : cmcc-tr069
  Original-password     : No
  Password-set-time     : 2019-12-01 18:42:57+01:00 DST
  Password-expired      : No
  Password-expire-time : -
  Account-expire-time  : -
  Bind IP               : 10.1.1.1
```

NOTE

For a local user who fails to log in to the device but is not locked, **Retry-time-left** is displayed. For a local user whose initial password is changed, **Change password retry-count-left** is displayed. When the number of continuous login failures or the number of initial password change failures reaches the limit specified using the **19.1.57 local-aaa-user wrong-password** command, the user is locked.

Display information about local user **user1** who fails to log in to the device.

```
<Huawei> display local-user username
user1
  The contents of local user(s):
  Password              : ****************
  State                 : active
  Service-type-mask     : T
  Privilege level       : 0
```

```
  Ftp-directory        : -
  HTTP-directory       : -
  Access-limit         : -
  Accessed-num         : 0
  Idle-timeout         : -
  Retry-interval       : 4 Min(s)
  Retry-time-left      : 1
  Original-password    : Yes
  Password-set-time    : 2019-01-27 13:26:55+08:00
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
```

Display information about local user **user1** whose initial password fails to be changed.

```
<Huawei> display local-user username user1
  The contents of local user(s):
  Password             : ****************
  State                : active
  Service-type-mask    : T
  Privilege level      : 0
  Ftp-directory        : -
  HTTP-directory       : -
  Access-limit         : -
  Accessed-num         : 1
  Idle-timeout         : -
  Change password retry-interval  : 4 Min(s)
  Change password retry-count-left: 3
  Original-password    : Yes
  Password-set-time    : 2019-01-27 13:26:55+08:00
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
```

Display information about local users in blocking state.

```
<Huawei> display local-user state block
  ------------------------------------------------------------------------------
  User-name                      State  AuthMask  AdminLevel
BlockTime
  ------------------------------------------------------------------------------
  test2                          B      T         0          2018-04-10 01:55:11-00:00
  ------------------------------------------------------------------------------
  Total 1 user(s)
```

Display information about local user **test2** in blocking state.

```
<Huawei> display local-user state block username test2
  The contents of local user(s):
  Password             : ****************
  State                : block
  Service-type-mask    : T
  Privilege level      : 0
  Ftp-directory        : -
  HTTP-directory       : -
  Access-limit         : -
  Accessed-num         : 0
  Idle-timeout         : -
  Block-time-left      : 8 Min(s)
  Original-password    : Yes
  Password-set-time    : 2019-01-27 13:26:55+08:00
  Password-expired     : No
  Password-expire-time : -
  Account-expire-time  : -
```

Table 19-13 Description of the **display local-user** command output

Item	Description
User-name	Name of the local user. To configure this parameter, run the **19.1.60 local-user** command.
State	State of the local user: • A: Active • B: Block To configure this parameter, run the **19.1.60 local-user** command.
AuthMask	Access type of the local user. • T: indicates the Telnet users. • M: indicates the terminal users, which usually refer to the console users. • S: indicates the SSH users. • F: indicates the FTP users. • W: indicates the web users. • B: indicates the IP session users. • X: indicates the 802.1X users. • A: indicates all access types. • H: indicates the HTTP users. • D: indicates the X25-PAD users. • P: indicates the PPP users. • Combination: For example, MH indicates either a terminal user or an HTTP user. To configure this parameter, run the **19.1.67 local-user service-type** command.
AdminLevel	Local user level. To configure this parameter, run the **19.1.60 local-user** command.
Password	Password of the local user. To configure this parameter, run the **19.1.60 local-user** command.
Service-type-mask	Service type of the local user. Same as the AuthMask type. To configure this parameter, run the **19.1.67 local-user service-type** command.
Privilege level	Local user level. To configure this parameter, run the **19.1.60 local-user** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ftp-directory	FTP directory of the local user. To configure this parameter, run the **19.1.60 local-user** command.
Access-limit	Whether the maximum number of sessions of the local user is configured. To configure this parameter, run the **19.1.60 local-user** command.
Access-limit-max	Maximum number of sessions of the local user. To configure this parameter, run the **19.1.60 local-user** command.
Accessed-num	Number of established sessions.
Idle-timeout	Idle timeout interval. To configure this parameter, run the **19.1.60 local-user** command.
User-group	Authorization information of the user group to which the local user is bound. To configure this parameter, run the **19.1.60 local-user** command.
Account-type	Account type of the local user. To set the account type of the local user to CMCC-TR069, run the **local-user account-type** command.
Original-password	Whether the password of a local user is the initial password: ● Yes ● No To configure this parameter, run the **19.1.71 password alert original** command.
Password-set-time	Time when the local user's password is created. The value is in format local time + DST offset.
Password-expired	Whether a local user's password has expired: ● Yes ● No
Password-expire-time	Time when the local user's password expires. The value is in format local time + DST offset. To configure this parameter, run the **19.1.72 password expire** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Account-expire-time	Expiry time of a local user account. The value is in format local time + DST offset. To configure this parameter, run the **19.1.64 local-user expire-date** command.
Bind IP	IP address bound to a local user. To configure this parameter, run the **19.1.62 local-user bind-ip** command.
BlockTime/Block-time-left	Remaining time of locked local users. (Local users are locked because the entered password is incorrect consecutively.)
Retry-interval	Login retry interval before a local user is locked. To configure this parameter, run the **19.1.57 local-aaa-user wrong-password** command.
Retry-time-left	Remaining number of login retries before a local user is locked. To configure this parameter, run the **19.1.57 local-aaa-user wrong-password** command.
Change password retry-interval	Retry interval for changing the initial password of a local user before the user is locked. To configure this parameter, run the **19.1.57 local-aaa-user wrong-password** command.
Change password retry-count-left	Remaining number of initial password change retries before a local user is locked. To configure this parameter, run the **19.1.57 local-aaa-user wrong-password** command.

Related Topics

19.1.60 local-user

19.1.43 display local-user expire-time

Function

The **display local-user expire-time** command displays the time when local accounts expire.

Format

display local-user expire-time

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The command output helps you diagnose and rectify the faults related to local user passwords.

Example

Display the time when local accounts expire.

```
<Huawei> display local-user expire-time
 ------------------------------------------------------------------------------
 Username              Password-expire       Account-expire           Expired
 ------------------------------------------------------------------------------
 zsh                   2014-12-01 21:25:44    -                       NO
 mm001                 2014-12-01 21:29:58    -                       NO
 ------------------------------------------------------------------------------
 Total: 2, printed: 2
```

Table 19-14 Description of the **display local-user expire-time** command output

Item	Description
Username	Local account name. To configure this parameter, run the **19.1.60 local-user** command.
Password-expire	Number of days after which the password expires. To configure this parameter, run the **19.1.72 password expire** command.
Account-expire	Account expiration time. To configure this parameter, run the **19.1.64 local-user expire-date** command.
Expired	Whether the local account has expired: ● YES ● NO **NOTE** The displayed value and actual value may have a difference within one minute; there is a possibility that the password has expired, but the displayed value is **NO**. When the local user account or password has expired, the local user becomes invalid.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.64 local-user expire-date

19.1.72 password expire

19.1.44 display local-aaa-user password policy

Function

The **display local-aaa-user password policy** command displays the password policy of local user.

Format

display local-aaa-user password policy { **access-user** | **administrator** }

Parameters

Parameter	Description	Value
access-user	Indicates the password policy of local access users.	-
administrator	Indicates the password policy of local administrator.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

After configuring the password policy for local users, you can run the **display local-aaa-user password policy** command to check whether the configuration is correct.

Example

Display the password policy of local access users.

```
<Huawei> display local-aaa-user password policy access-user
  Password control              : Enable
  Password history              : Enable (history records:5)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-15 Description of the **display local-aaa-user password policy access-user** command output

Item	Description
Password control	Whether the password control function is enabled: ● Enable ● Disable To configure this function, run the **19.1.58 local-aaa-user password policy access-user** command.
Password history	Whether the historical password recording function is enabled and the maximum number of historical passwords of each user. To configure this function, run the **19.1.73 password history record number** command.

Display the password policy of local administrator.

```
<Huawei> display local-aaa-user password policy administrator
  Password control                : Enable
  Password expiration             : Enable (180 days)
  Password history                : Enable (history records:5)
  Password alert before expiration : 30 days
  Password alert original         : Enable
```

Table 19-16 Description of the **display local-aaa-user password policy administrator** command output

Item	Description
Password control	Whether the password control function is enabled: ● Enable ● Disable To configure this function, run the **19.1.59 local-aaa-user password policy administrator** command.
Password expiration	Whether the password expiration function is enabled and password expiration time. To configure this function, run the **19.1.72 password expire** command.
Password history	Whether the historical password recording function is enabled and the maximum number of historical passwords of each user. To configure this function, run the **19.1.73 password history record number** command.
Password alert before expiration	Password expiration prompt days. To configure this function, run the **19.1.70 password alert before-expire** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Password alert original	Whether the device prompt users to change the initial passwords: ● Enable ● Disable To configure this function, run the **19.1.71 password alert original** command.

Related Topics

19.1.58 local-aaa-user password policy access-user
19.1.59 local-aaa-user password policy administrator
19.1.72 password expire
19.1.70 password alert before-expire
19.1.71 password alert original
19.1.73 password history record number

19.1.45 display recording-scheme

Function

The **display recording-scheme** command displays the configuration of recording schemes.

Format

display recording-scheme [*recording-scheme-name*]

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display recording-scheme** command displays the configuration of recording schemes.

Example

Display the configuration of the recording scheme **scheme0**.

```
<Huawei> display recording-scheme scheme0
-----------------------------------------------------------------
 Recording-scheme-name          : scheme0
 HWTACACS-template-name          : tacas-1
-----------------------------------------------------------------
```

Table 19-17 Description of the **display recording-scheme** command output

Item	Description
Recording-scheme-name	Name of the recording scheme. To create a recording scheme, run the **recording-scheme** command.
HWTACACS-template-name	Name of the HWTACACS server template associated with the recording scheme. To associate an HWTACACS server template with a recording scheme, run the **recording-mode hwtacacs** command.

Related Topics

19.1.76 recording-mode hwtacacs

19.1.77 recording-scheme

19.1.46 display remote-user authen-fail

Function

The **display remote-user authen-fail** command displays the accounts that fail in remote AAA authentication.

Format

display remote-user authen-fail [**blocked** | **username** *username*]

Parameters

Parameter	Description	Value
blocked	Displays all the remote AAA authentication accounts that have been locked.	-
username *username*	Displays details about the accounts that fail in remote AAA authentication. If the *username* parameter is not specified, basic information about all accounts that fail in remote AAA authentication is displayed.	It is a string of 1 to 253 case-insensitive characters without spaces.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the account locking function is enabled for the users who fail in AAA remote authentication, the device records all failed accounts, including:

- The accounts that failed in authentication and are locked, for example, when the user entered the wrong account name or password too many times.
- The accounts that failed in authentication, but are not locked, for example, when the number of times the account name or password was entered incorrectly did not exceed the limit.

Prerequisites

Precautions

The device cannot back up a recorded account that fails the AAA authentication. If an active/standby switchover policy has been configured on the device, all user entries are cleared when the device completes an active/standby switchover.

Example

Display all accounts that have failed in remote AAA authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display remote-user authen-fail
  Interval: Retry Interval(Mins)
  TimeLeft: Retry Time Left
  BlockDuration: Block Duration(Mins)
  ---------------------------------------------------------------------------------------------
  Username                Interval  TimeLeft  BlockDuration
  ---------------------------------------------------------------------------------------------
  www@test                 0         0         65414
  ---------------------------------------------------------------------------------------------
  Total 1, 1 printed
```

Display all locked accounts.

```
<Huawei> display remote-user authen-fail blocked
  Interval: Retry Interval(Mins)
  TimeLeft: Retry Time Left
  BlockDuration: Block Duration(Mins)
  ---------------------------------------------------------------------------------------------
  Username                Interval  TimeLeft  BlockDuration
BlockTime
  ---------------------------------------------------------------------------------------------
  www@test                 0         0         65414          2018-04-23
17:22:09+08:00
  ---------------------------------------------------------------------------------------------
  Total 1, 1 printed
```

Display details about the account **test** that failed in remote AAA authentication.

```
<Huawei> display remote-user authen-fail username test
  The contents of the user:
  Retry-interval     : 0 Min(s)
  Retry-time-left    : 0
  Block-time-left    : 4 Min(s)
  User-state         : Block
```

Table 19-18 Description of the **display remote-user authen-fail** command output

Item	Description
Username	User name.
Interval: RetryInterval(Mins)	Authentication retry interval, in minutes. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
Retry-interval	Authentication retry interval. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
TimeLeft: Retry Time Left	Remaining number of consecutive authentication failures. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
Retry-time-left	Remaining number of consecutive authentication failures. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
BlockDuration: Block Duration(Mins)	User account locking duration, in minutes. To configure this parameter, run the **19.1.78 remote-aaa-user authen-fail** command.
BlockTime	User account locking time.
Block-time-left	Remaining locking time of an account.
User-state	User status: • Block • Active

Related Topics

19.1.78 remote-aaa-user authen-fail

19.1.47 display service-scheme

Function

The **display service-scheme** command displays the configuration of service schemes.

Format

display service-scheme [**name** *name*]

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a service scheme.	The service scheme must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display service-scheme** command displays the configuration of service schemes.

 Copyright © Huawei Technologies Co., Ltd.

Before applying a service scheme to a domain, run the **display service-scheme** command to check whether the service scheme is correct.

Precautions

The **display service-scheme** command displays the detailed configuration if the command is executed in the service scheme view or the name of a service scheme is specified. Otherwise, this command displays only the summary of service schemes.

Example

Display information about all service schemes.

```
<Huawei> display service-scheme
  ------------------------------------------------------------------
  service-scheme-name                    scheme-index
  ------------------------------------------------------------------
  svcscheme1                             0
  svcscheme2                             1
  ------------------------------------------------------------------
  Total of service scheme: 2
```

Display the configuration of the service scheme **svcscheme1**.

```
<Huawei> display service-scheme name svcscheme1

  service-scheme-name           : svcscheme1
  service-scheme-dns-name       : -
  service-scheme-primary-dns    : -
  service-scheme-secondary-dns  : -
  service-scheme-adminlevel     : 15
  service-scheme-dhcpgroup      : -
  service-scheme-ippool         : -
  service-scheme-primary-wins   : -
  service-scheme-secondary-wins : -
  service-scheme-update-config  : -
  service-scheme-update-version : -
  service-scheme-acl-number     : -
  service-scheme-interface-flag : -
  service-scheme-qosprofile     : -
  service-scheme-idlecut-time   : 10
  service-scheme-idlecut-flow   : 20
  service-scheme-idlecut-direct : Inbound and Outbound
  Tariff-level                  : 1
   Qos-profile                  : svcscheme1000
   Accounting-flag              : enable
```

Table 19-19 Description of the **display service-scheme** command output

Item	Description
service-scheme-name	Name of a service scheme. To create a service scheme, run the **service-scheme (AAA view)** command.
scheme-index	Index of the service scheme.
service-scheme-dns-name	Default DNS domain name in the service scheme.
service-scheme-primary-dns	Address of the primary DNS server.

Item	Description
service-scheme-secondary-dns	Address of the secondary DNS server.
service-scheme-adminlevel	Level of an administrator. The value is an integer that ranges from 0 to 15. The value 15 indicates that this parameter is invalid. To configure a level of an administrator, run the **admin-user privilege level** command.
service-scheme-dhcpgroup	DHCP server group.
service-scheme-ippool	IP address pool in the service scheme.
service-scheme-primary-wins	Address of the primary wins server.
service-scheme-secondary-wins	Address of the secondary wins server.
service-scheme-update-config	The URL of the update packet.
service-scheme-update-version	Version number of the update packet.
service-scheme-acl-number	The local subnet information to be sent to the remote end.
service-scheme-interface-flag	The address of the interface bound to the IPSec tunnel to be sent to the remote end.
service-scheme-qosprofile	Name of the bound QoS profile. To configure this item, run the **19.1.75 qos-profile (service scheme view)** command.
service-scheme-idlecut-time	Idle-cut timeout interval, in minutes. To configure this item, run the **19.1.55 idle-cut (service scheme view)** command.
service-scheme-idlecut-flow	Traffic threshold for idle-cut, in kbytes. To configure this item, run the **19.1.55 idle-cut (service scheme view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
service-scheme-idlecut-direct	Direction in which idle-cut takes effect for traffic. The value can be: ● Inbound: Idle-cut takes effect for uplink traffic. ● Outbound: Idle-cut takes effect for downlink traffic. ● Inbound and Outbound: Idle-cut takes effect for uplink and downlink traffic. To configure this item, run the **19.1.55 idle-cut (service scheme view)** command.
Tariff-level	Tariff level of traffic.
Qos-profile	QoS profile corresponding to the tariff level. To set the tariff level, run the **tariff-level** command.
Accounting-flag	Whether accounting is enabled for the tariff level: ● enable ● disable To enable accounting for the tariff level, run the **tariff-level** command.

Related Topics

19.1.90 service-scheme (AAA view)

19.1.48 dns (service scheme view)

Function

The **dns** command configures the primary or secondary DNS server in a service scheme.

The **undo dns** command cancels the configuration of the primary or secondary DNS server in a service scheme.

By default, no primary or secondary DNS server is configured in a service scheme.

Format

dns *ip-address* [**secondary**]

undo dns [*ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a DNS server.	The value is in dotted decimal notation.
secondary	Specifies the secondary DNS server.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

If no DNS server is specified when a local address pool, DHCP server, or RADIUS server assigns IP addresses to users, the DNS server configured in the service scheme view is used.

Example

Set the IP address of the primary DNS server in the service scheme **svcscheme1** to 10.10.10.1.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] dns 10.10.10.1
```

Set the IP address of the secondary DNS server in the service scheme **svcscheme1** to 10.10.20.1.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] dns 10.10.20.1 secondary
```

Related Topics

19.1.47 display service-scheme

19.1.49 dns-name (service scheme view)

Function

The **dns-name** command configures the default DNS domain name in a service scheme.

The **undo dns-name** command deletes the default DNS domain name in a service scheme.

By default, no default DNS domain name is configured in a service scheme.

 Copyright © Huawei Technologies Co., Ltd.

Format

dns-name *domain-name*

undo dns-name

Parameters

Parameter	Description	Value
domain-name	Specifies the default DNS domain name.	The value is a string of 1 to 255 case-sensitive characters. For example, the value can be **huawei.com**.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

The AAA service scheme allows the default DNS domain name to be bound and sends the default DNS domain name to users.

Example

Configure the default DNS domain name in the service scheme **svcscheme1** to **huawei.com**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] dns-name huawei.com
```

Related Topics

19.1.47 display service-scheme

19.1.50 domain (AAA view)

Function

The **domain** command creates a domain and displays its view.

The **undo domain** command deletes a domain.

By default, the device has two domains: **default** and **default_admin**. The two domains can be modified but cannot be deleted.

Format

domain *domain-name* [**domain-index** *domain-index*]

undo domain *domain-name*

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a domain.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces or the following symbols: * ? ". The value cannot be - or --.
domain-index *domain-index*	Specifies the index of a domain.	The value is an integer that ranges from 0 to 255.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device can manage users through domains. A domain is the minimum user management unit. A domain name can be an ISP name or the name of a service provided by an ISP. A domain can use the default authorization attribute, and be configured with a RADIUS template and authentication and accounting schemes.

If the domain to be configured already exists, the **domain** command displays the domain view.

If a user that belongs to this domain is online, you cannot run the **undo domain** command to delete the domain.

Prerequisites

To perform AAA for access users, you need to apply the authentication schemes, authorization schemes, and accounting schemes in the domain view. Therefore, authentication, authorization, and accounting schemes must be configured in the AAA view in advance.

Precautions

- The domain **default** is a global default common domain for user access, for example, NAC. By default, the domain is activated, and is bound to the authentication scheme **radius** and accounting scheme **default**, but is not bound to any authorization scheme.
- The domain **default_admin** is a global default management domain for users who log in to the device through HTTPS, SSH, Telnet, and the Web system, namely, administrators. By default, the domain is activated, and is bound to the authentication scheme **default** and accounting scheme **default**, but is not bound to any authorization scheme.

 Copyright © Huawei Technologies Co., Ltd.

The device supports a maximum of 256 domains, including the **default** and **default_admin** domains.

Example

Specify the domain named **domain1** and access the domain view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain domain1
[Huawei-aaa-domain-domain1]
```

Related Topics

19.1.41 display domain

19.1.51 domain (system view)

Function

The **domain** command configures a global default domain.

The **undo domain** command restores the default setting.

By default, there are two global default domains: common domain **default** and administrative domain **default_admin**. The former is used as the global default domain of access users, while the latter as the global default domain of administrators.

Format

Common domain **default**:

domain *domain-name*

undo domain

Administrative domain **default_admin**:

domain *domain-name* **admin**

undo domain admin

Parameters

Parameter	Description	Value
domain-name	Specifies the name of a global default domain.	The domain must already exist.
admin	Configures a domain for administrators. If this parameter is not specified, the domain for common access users is configured.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the global default domain is configured, a user must be managed by the global default domain if their domain cannot be identified.

Precautions

You must create a domain before configuring the domain as the global default domain.

Example

Create domain **abc** and configure it as the global default common domain.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain abc
[Huawei-aaa-domain-abc] quit
[Huawei-aaa] quit
[Huawei] domain abc
```

Related Topics

19.1.50 domain (AAA view)

19.1.41 display domain

19.1.52 domain-location

Function

The **domain-location** command configures the position of a domain name.

The **undo domain-location** command restores the default position of a domain name.

By default, the domain name in the AAA view is placed behind the domain name delimiter, and no position is configured in the authentication profile view.

Format

domain-location { **after-delimiter** | **before-delimiter** }

undo domain-location

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
after-delimiter	Indicates that the domain name is placed behind the domain name delimiter.	-
before-delimiter	Indicates that the domain name is placed before the domain name delimiter.	-

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

The format of a user name is **user name@domain name**. If **before-delimiter** is specified, the format **domain name@user name** is used.

You can use the **domain-location** command only when there is no online user.

Precautions

If you run the **domain-location** command in the AAA view, the position of a domain is configured globally and the configuration takes effect for all users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the interface view, the configuration takes effect for only the users connected to this interface. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the domain name before the domain name delimiter.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain-location before-delimiter
```

Related Topics

19.1.33 display aaa configuration

19.1.53 domain-name-delimiter

Function

The **domain-name-delimiter** command configures a domain name delimiter.

The **undo domain-name-delimiter** command restores the default domain name delimiter.

By default, the domain name delimiter in the AAA view is @, and no delimiter is available in the authentication profile view.

Format

domain-name-delimiter *delimiter*

undo domain-name-delimiter

Parameters

Parameter	Description	Value
delimiter	Specifies a domain name delimiter of only one bit.	The value can only be one of the following characters: \ / : < > | @ ' %.

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

Different AAA servers may use different domain name delimiters. To ensure that an AAA server obtains the correct user name and domain name, configure the same domain name delimiter on the device and the AAA server.

For example, if the domain name delimiter is %, the user name of **user1** in the domain **dom1** is **user1%dom1** or **dom1%user1**.

Precautions

Before using the **domain-name-delimiter** command, ensure that no local user exists.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **domain-name-delimiter** command in the AAA view, the domain name delimiter is configured globally and the configuration takes effect for all users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the domain name delimiter as / in the AAA view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain-name-delimiter /
```

Related Topics

19.1.33 display aaa configuration
19.1.60 local-user

19.1.54 domainname-parse-direction

Function

The **domainname-parse-direction** command configures the direction in which a domain name is parsed.

The **undo domainname-parse-direction** command restores the default direction in which a domain name is parsed.

By default, the domain name is parsed in the AAA view from left to right, and no direction is configured in which a domain name is parsed.

Format

domainname-parse-direction { **left-to-right** | **right-to-left** }

undo domainname-parse-direction

Parameters

Parameter	Description	Value
left-to-right	Parses a domain name form left to right.	-
right-to-left	Parses a domain name form right to left.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

In AAA implementations, users belong to different domains. A network access server (NAS) centrally manages users in a domain. During a user's login, the NAS parses the entered user name. A user is authenticated only when the user has the correct user name and domain name. When configuring an AAA scheme, run the **domainname-parse-direction** { **left-to-right** | **right-to-left** } command to configure the direction in which a domain name is parsed.

Assume that the user name is **username@dom1@dom2**.

- If the **domain-location** command configures the domain name behind the domain name delimiter:
  - When **left-to-right** is specified, the user name is **username** and the domain name is **dom1@dom2**.
  - When **right-to-left** is specified, the user name is **username@dom1** and the domain name is **dom2**.
- If the **domain-location** command configures the domain name before the domain name delimiter:
  - When **left-to-right** is specified, the user name is **dom1@dom2** and the domain name is **username**.
  - When **right-to-left** is specified, the user name is **dom2** and the domain name is **username@dom1**.

Precautions

If you run the **domainname-parse-direction** command in the AAA view, the direction in which a domain name is parsed is configured globally and the configuration takes effect for all users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the interface view, the configuration takes effect for only the users connected to this interface. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

Example

Configure the device to parse a domain name from right to left in the AAA view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domainname-parse-direction right-to-left
```

Related Topics

19.1.33 display aaa configuration

19.1.55 idle-cut (service scheme view)

Function

The **idle-cut** command enables the idle-cut function for domain users and sets the idle-cut parameters.

The **undo idle-cut** command disables the idle-cut function.

By default, the idle-cut function is disabled for domain users.

Format

idle-cut *idle-time flow-value* [**inbound** | **outbound**]

undo idle-cut

Parameters

Parameter	Description	Value
idle-time	Specifies the period in which an idle user can stay online.	The value is an integer that ranges from 1 to 1440, in minutes.
flow-value	Specifies the traffic threshold for idle-cut function. When the traffic of a user stays below this threshold for a certain period, the device considers that the user is in idle state.	The value is an integer that ranges from 0 to 4294967295, in kbytes.
inbound	Indicates that the idle-cut function takes effect for only upstream traffic of users.	-
outbound	Indicates that the idle-cut function takes effect for only downstream traffic of users. **NOTE** If neither **inbound** nor **outbound** is specified, the idle-cut function takes effect for both upstream and downstream traffic.	-

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user uses no or a little network traffic for a long time, the user still occupies certain bandwidth, which reduces access rate of other users. The idle-cut function disconnects the users whose traffic volume stays below the traffic threshold within the idle time, to save resources and improve service experience of other users.

Precautions

- The **idle-cut** command configured in the service scheme view takes effect for administrators. For common users, the function takes effect only for PPPoE and Portal users.
- When idle-cut in the service scheme view and RADIUS attribute 28 (Idle-Timeout) delivered by the remote RADIUS server exist simultaneously, RADIUS attribute 28 has a higher priority. RADIUS attribute 28 can be used together with the traffic and direction configured using this command.
- The idle-cut function takes effect only after the idle time and traffic threshold are configured. To configure the traffic threshold, run the **idle-cut** *idle-time flow-value* command. To configure the idle time, use the value of *idle-time* configured on the device or the value (carried in RADIUS attribute 28 Idle-Timeout) authorized by the RADIUS server. If both values exist, the value authorized by the RADIUS server has a higher priority.

Example

Enable the idle-cut function for the domain, and set the idle time to 1 minute and the traffic threshold to 10 kbytes.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme huawei
[Huawei-aaa-service-huawei] idle-cut 1 10
```

Related Topics

19.1.47 display service-scheme

19.1.56 ip-pool (service scheme view)

Function

The **ip-pool** command sets the IP address pool bound to a service scheme or moves the location of a configured IP address pool bound to a service scheme.

The **undo ip-pool** command deletes the IP address pool bound to a service scheme. If no parameter is specified, all the IP address pools bound to a service scheme are deleted.

By default, no IP address pool is bounded in a service scheme.

 Copyright © Huawei Technologies Co., Ltd.

Format

ip-pool *pool-name* [**move-to** *new-position*]

undo ip-pool [*pool-name*]

Parameters

Parameter	Description	Value
pool-name	Specifies the IP address pool name.	The name is a string of 1 to 64 characters and can contain letters, digits (0-9), dots (.), hyphens (-), and underscores (_).
move-to *new-position*	Moves the location of a configured IP address pool bound to a service scheme.	The value range varies according to the number of configured address pools bound to a domain. For example, if there are ten IP address pools in a domain, the value ranges from 1 to 10. The number of IP address pools ranges from 1 to 16.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command limits the range of IP addresses of users in a service scheme. The **ip-pool** command is used to reference the configured address pool to a service scheme. An IP address pool is configured using the **ip pool (system view)** command.

Prerequisites

A global IP address pool has been created using the **8.3.83 ip pool (system view)** command and the address range has been specified using the **8.3.92 network (IP address pool view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the IP address pool **pool1** for the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] ip pool pool1
[Huawei-ip-pool-pool1] network 192.168.100.0 mask 24
[Huawei-ip-pool-pool1] quit
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] ip-pool pool1
```

Change the position of the IP address **ippool1** in the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] ip pool ippool1
[Huawei-ip-pool-ippool1] network 192.168.100.0 mask 24
[Huawei-ip-pool-ippool1] quit
[Huawei] ip pool ippool2
[Huawei-ip-pool-ippool2] network 192.168.200.0 mask 24
[Huawei-ip-pool-ippool2] quit
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] ip-pool ippool1
[Huawei-aaa-service-svcscheme1] ip-pool ippool2
[Huawei-aaa-service-svcscheme1] ip-pool ippool1 move-to 2
```

Related Topics

19.1.47 display service-scheme

8.3.83 ip pool (system view)

19.1.57 local-aaa-user wrong-password

Function

The **local-aaa-user wrong-password** command enables local account locking function and sets the retry interval, consecutive incorrect password attempts, and locking duration.

The **undo local-aaa-user wrong-password** command disables local account locking function.

By default, the local account locking function is enabled, retry interval is 5 minutes, maximum number of consecutive incorrect password attempts is 3, and account locking period is 5 minutes.

Format

local-aaa-user wrong-password retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo local-aaa-user wrong-password

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the retry interval of a local account.	The value is an integer that ranges from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the consecutive incorrect password attempts.	The value is an integer that ranges from 3 to 65535.
block-time *block-time*	Specifies the local account locking duration. In actual application, there is a one minute difference in locking time.	The value is an integer that ranges from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies to the following scenarios:

- The command locks a local account to improve password security of the local user. If the password is entered incorrectly more than a certain number of times within the given retry period, the account is locked. The device does not authenticate the user when the account is locked.
- The command locks a local account to ensure that the password will not be cracked by a brute force from a malicious user. When attempting to change the password, if the original password is entered incorrectly more than a certain number of times within the given retry period, the account is locked. The user cannot modify the password when the account is locked.

Follow-up Procedure

After a local account is locked, you can run the **local-user** *user-name* **state active** command to unlock the local account.

Precautions

Only entering the incorrect password can lock the account. Other local authentication failures will not lock the account.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable local account locking, and set the authentication retry interval to 5 minutes, maximum number of consecutive incorrect password attempts to 3, and account locking period to 5 minutes.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user wrong-password retry-interval 5 retry-time 3 block-time 5
```

19.1.58 local-aaa-user password policy access-user

Function

The **local-aaa-user password policy access-user** command enables the password policy for local access users and enters the local access user password policy view.

The **undo local-aaa-user password policy access-user** command disables the password policy of local access users.

By default, the password policy of local access users is enabled.

Format

local-aaa-user password policy access-user

undo local-aaa-user password policy access-user

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

After a local user is created using the **local-user** command, the minimum length and complexity of the password are limited. If you want to improve password security, run this command to configure password policy. The new password cannot be the same as any previously used password stored on the device.

Example

Enable the local access user password policy and enter the local access user password policy view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy access-user
[Huawei-aaa-lupp-acc]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.73 password history record number

19.1.59 local-aaa-user password policy administrator

Function

The **local-aaa-user password policy administrator** command enables the password policy for local administrators and enters the local administrator password policy view.

The **undo local-aaa-user password policy administrator** command disables the password policy of local administrators.

By default, the password policy for local administrators is enabled.

Format

local-aaa-user password policy administrator

undo local-aaa-user password policy administrator

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local user is created using the **local-user** command, the minimum length and complexity of the password are limited. If you want to improve password security, you can run the following commands to configure the password policy for the local administrators:

- Run the **password expire** command to set the password validity period.
- Run the **password alert before-expire** command to set the password expiration prompt days.
- Run the **password alert original** command to enable the device to prompt users to change initial passwords.
- Run the **password history record number** command to set the maximum number of previously used passwords recorded for each user.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After the **undo local-aaa-user password policy administrator** command is executed, the administrator password policy will be disabled, causing a security risk.

Example

Enable the local administrator password policy and enter the local administrator password policy view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy administrator
[Huawei-aaa-lupp-admin]
```

Related Topics

19.1.60 local-user

19.1.72 password expire

19.1.70 password alert before-expire

19.1.71 password alert original

19.1.73 password history record number

19.1.60 local-user

Function

The **local-user** command creates a local user and sets parameters of the local user.

The **undo local-user** command deletes a local user.

By default, the local user **admin** exists in the system. The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it. The irreversible encryption algorithm is used, the level is 15, and service type is http.

Format

local-user *user-name* { **access-limit** *max-number* | **ftp-directory** *directory* | **idle-cut** | **idle-timeout** *minutes* [*seconds*] | **password** { **cipher** | **irreversible-cipher** } *password* [**opt**] | **privilege level** *level* | **state** { **active** | **block** } | **user-group** *group-name* } *

undo local-user *user-name* [**access-limit** | **ftp-directory** | **idle-timeout** | **privilege level** | **user-group**]

Parameters

Parameter	Description	Value
user-name	Specifies a user name. If the user name contains a domain name delimiter such as @, the character before @ is the user name and the character behind @ is the domain name. If the value does not contain @, the entire character string is the user name and the domain name is the default one.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
access-limit *max-number*	Specifies the maximum number of connections established by a specified user. If this parameter is not specified, a user can establish a maximum of 4294967295 connections by default.	The value is an integer that ranges from 1 to 4294967295. The actual number of connections is the smaller value between *max-number* and the maximum number of users of a type on different models.
ftp-directory *directory*	Specifies the directory that an FTP user can access. If this parameter is not specified, the FTP directory of the local user is empty. The device will check whether the default FTP directory has been set using the **3.11.59 set default ftp-directory** command. If no FTP directory exists, FTP users cannot log in to the device. **NOTE** Ensure that the configured FTP directory is an absolute path; otherwise, the configuration does not take effect.	The value is a string of 1 to 64 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
opt	Indicates that the challenge in the MD5 algorithm takes precedence. By default, the password takes precedence.	-
idle-cut	Indicates the idle-cut function for local user. If a user uses no or a little network traffic for a long time, the user still occupies certain bandwidth, which reduces access rate of other users. After the **local-user idle-cut** command is run, the device periodically detects the specified users. If the traffic volume of a user within the idle-cut period is lower than the threshold, the user is disconnected. By default, the idle-cut period is 10 minutes and threshold is 600K bytes. If the service scheme bound to an AAA domain contains the idle-cut parameters configured by the **19.1.55 idle-cut (service scheme view)** command, these idle-cut parameters take effect.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
idle-timeout *minutes* [*seconds*]	Specifies the idle timeout interval. • *minutes* indicates the idle timeout interval, in minutes. • *seconds* indicates the idle timeout interval, in seconds. If this parameter is not specified, the device uses the idle timeout interval configured by the **3.8.15 idle-timeout** command in the user interface view. If *minutes* [*seconds*] is set to **0 0**, the idle disconnection function is disabled. **NOTICE** If the idle timeout interval is set to 0 or a large value, the terminal will remain in the login state, resulting in security risks. You are advised to run the **lock** command to lock the current connection.	The value of *minutes* is an integer that ranges from 0 to 35791, in minutes. The value of *seconds* is an integer that ranges from 0 to 59, in seconds.
privilege level *level*	Specifies the level of a local user. After logging in to the device, a user can run only the commands of the same level or lower levels. **NOTE** If this parameter is not specified, the user level is 0.	The value is an integer that ranges from 0 to 15. A larger value indicates a higher level of a user.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password { **cipher** | **irreversible-cipher** } *password*	Specifies the password of a local user. ● The **cipher** parameter indicates that the user password is encrypted using the reversible encryption algorithm. Unauthorized users can obtain the plain text by using the corresponding decryption algorithm, so security is low. ● The **irreversible-cipher** parameter indicates that the user password is encrypted using the irreversible encryption algorithm. Unauthorized users cannot obtain the plain text by using the special encryption algorithm. User security is ensured. If this parameter is not specified, the device automatically allocates the default password to the user. For security purposes, change the password immediately and update the password periodically. If a user is allowed to encrypt the local user password using the irreversible encryption algorithm, the device does not support CHAP authentication for the user.	The value is a case-sensitive string without question marks (?) or spaces. ● If the **cipher** parameter is specified, the value of *password* can be a plain text of 8 to 128 characters or a cipher-text password of 48 to 188 characters. ● If the **irreversible-cipher** parameter is specified, the value of *password* can be a plain text of 8 to 128 characters or a cipher-text password of 68 characters. A simple local user password may bring security risks. The user password must consist of two types of characters, including uppercase letters, lowercase letters, numerals, and special characters. In addition, the password cannot be the same as the user name or user name in an inverse order.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	NOTICE It is recommended that you set the user password when creating a user. The interaction method using the **19.1.66 local-user password** command is recommended.	
state { **active** | **block** }	Indicates the state of a local user. • **active**: indicates the active state. The device accepts and processes the authentication request from the user, and allows the user to change the password. • **block**: indicates the blocking state. The device rejects the authentication request from the user and does not allow the user to change the password. If a user has established a connection with the device, when the user is set in blocking state, the connection still takes effect but the device rejects subsequent authentication requests from the user. If this parameter is not specified, the status of a local user is active.	-
user-group *group-name*	Specifies the name of a user group.	The value is a string of 1 to 64 case-sensitive characters without spaces. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

 Copyright © Huawei Technologies Co., Ltd.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To facilitate device maintenance, run the **local-user** command on the device to create a local user and set parameters such as the password, user level, and FTP directory.

Prerequisites

Before adding a local user to a user group, ensure that the user group has been created using the **19.6.150 user-group** command.

Precautions

- For device security purposes, change the password periodically.
- Security risks exist if the user login mode is set to Telnet or FTP. You are advised set the user login mode to STelnet or SFTP and set the user access type to SSH.

  When a device starts without any configuration, HTTP uses the randomly generated self-signed certificate to support HTTPs. The self-signed certificate may bring risks. Therefore, you are advised to replace it with the officially authorized digital certificate.
- After a local administrator logs in to the device, the administrator can create, modify, or delete attributes of other local users of the same or a lower level. The attributes include password, user level, maximum number of access users, and account validity period.

  After you change the rights (for example, the password, level, FTP directory, idle timeout interval, or status) of a local account, the rights of users already online do not change. The change takes effect when the user next goes online.
- The user name function may be invalid due to improper configuration of the domain name delimiter.
- A maximum of 512 local accounts can be configured.
- V200R005C00 and later versions use new encryption mechanism. After the AR is upgraded to V200R005C00 and later versions, you are advised to change the password to a more secure password.

  V200R005C00 and later versions use new encryption mechanism. If the version is rolled back, the original version cannot identify the password configured in V200R005C00 and later versions. As a result, the configuration becomes invalid. To ensure that the password takes effect after rollback, during rollback, restore the password-relevant configuration in the configuration file to the configuration before the upgrade or change the password-relevant configuration in the configuration file to the configuration that can be identified by the original version.

 Copyright © Huawei Technologies Co., Ltd.

- One user group can be used by multiple local users. However, a local user belongs to only one user group.

  If the user groups have been configured for the local user and in the service template, only the user group configured for the local user takes effect.

  The user groups that are used by a local user or an online user cannot be deleted.
- The **idle-cut** command configured in the service scheme view takes effect for administrators. For common users, the function takes effect only for PPPoE and Portal users.

Example

Create a local user **user1**, and set the domain name to **vipdomain**, the password to **admin@12345** in cipher text, the maximum number of connections to 100, and the idle timeout interval to 10 minutes.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user user1@vipdomain password irreversible-cipher admin@12345 access-limit 100
idle-timeout 10
```

Related Topics

19.1.42 display local-user

19.1.61 local-user account-type

Function

The **local-user account-type** command sets the account type for a local user.

The **undo local-user account-type** command restores the default account type for a local user.

By default, the account type of local users is not specified.

Format

local-user *user-name* **account-type cmcc-tr069**

undo local-user *user-name* **account-type**

Parameters

Parameter	Description	Value
user-name	Specifies the local user of which the account type needs to be set.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

Parameter	Description	Value
cmcc-tr069	Sets the account type of the local user to CMCC-TR069.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

TR-069, also called CPE WAN Management Protocol (CWMP), defines the communication mechanism between the Customer Premises Equipment (CPE) and Auto-Configuration Server (ACS) and allows the ACS to centrally manage CPEs.

This command is applicable to the following scenarios:

- After a user is created by the **local-user** command, set the account type of the user to CMCC-TR069, which indicates a TR069 administrator of China Mobile.
- When a device functions as a CPE, if the ACS of China Mobile creates an administrator on the CPE through TR-069, the CPE automatically executes this command to set the account type of the administrator to CMCC-TR069.

After the CMCC-TR069 administrator is created, the administrator can manage the device through ACS. When the device restores configurations after a reboot, the ACS quickly obtains information about the CMCC-TR069 administrator.

Precautions

If the TR-069 function is not enabled by the **4.2.16 set operator-code cmcc** command, this command cannot be executed.

Only one CMCC-TR069 user is supported on a device.

Example

Set the account type of the local user user1@vipdomain to CMCC-TR069.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user user1@vipdomain account-type cmcc-tr069
```

Related Topics

19.1.60 local-user

19.1.42 display local-user

19.1.62 local-user bind-ip

Function

The **local-user bind-ip** command allocates a fixed IP address to a local user.

The **undo local-user bind-ip** command restores the default setting.

By default, no fixed IP address is allocated to the local user.

Format

local-user *user-name* **bind-ip** *ip-address*

undo local-user *user-name* **bind-ip**

Parameters

Parameter	Description	Value
user-name	Specifies the name of a local user.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
ip-address	A fixed IP address is allocated to the local user.	The value is in dotted decimal notation.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local user passes authentication, run the **local-user bind-ip** command to allocate a fixed IP address to the user. Then the user has the network access right corresponding to the allocated IP address. For example, if a public network address is allocated, the user can access the public network; if a private network address is allocated, the user can access the private network. When the user goes offline and online again, the IP address is still bound to the user.

Precautions

After you run this command to allocate a fixed IP address to a local user, you need to exclude this IP address from the DHCP address pool, preventing this IP address from being allocated to another user to cause an IP address conflict.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind IP address 192.168.1.1 to the local user **hello@163.net**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net bind-ip 192.168.1.1
```

19.1.63 local-user change-password

Function

The **local-user change-password** command enables local users to change their passwords.

Format

local-user change-password

Parameters

None

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

If you are a low-level administrator, to ensure security of the password, you can run the **local-user change-password** command in the user view to change your password after passing the authentication.

Precautions

- To modify the password, a local user must enter the old password.
- After the user that passes local authentication changes the password, the user must type the new password to pass local authentication.
- The **local-user change-password** command is used to change the password of a local user. It does not save the configuration, but the result of changing the password is saved through the **local-user password** command. If the server does not receive old password, new password, or confirmed password from the user within 30 seconds, it terminates the password change process. When the user presses **Ctrl+C** to cancel password change, the password change process is terminated.
- A simple password of a local user may bring security risks. When a local user changes the password, the new password must be a string of 8 to 128 characters and must contain at least two types of the following: uppercase

letters, lowercase letters, digits, and special characters. In addition, the new password cannot be the same as the user name or the user name in a reverse order.

- For device security purposes, change the password periodically.

Example

The local user changes the password.

```
<Huawei> local-user change-password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, including lowercase letters, uppercase letters, numer
als and special characters.
Please enter old password:
Please enter new password:
Please confirm new password:
Info: The password is changed successfully.
```

19.1.64 local-user expire-date

Function

The **local-user expire-date** command sets the expiration date of a local account.

The **undo local-user expire-date** command restores the default expiration date of a local account.

By default, a local account is permanently valid.

Format

local-user *user-name* **expire-date** *expire-date*

undo local-user *user-name* **expire-date**

Parameters

Parameter	Description	Value
user-name	Specifies a local account.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
expire-date	Specifies the expiration date of the local account.	The value is in YYYY/MM/DD format. YYYY specifies the year, MM specifies the month, and DD specifies the day. The value ranges from 2000/1/1 to 2099/12/31.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a local account is created, the account has no expiration date by default. You can run the **local-user expire-date** command to set the expiration date of a local account. When the expiration date is reached, the account expires. This configuration enhances network security.

Precautions

- For example, if the expiration date of the local account is set to 2013-10-1, the account becomes invalid at 00:00 on 2013-10-1.
- This function takes effect only for users who go online after this function is successfully configured.

Example

Set the expiration date of local account **hello@163.net** to 2013/10/1.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net expire-date 2013/10/1
```

Related Topics

19.1.60 local-user

19.1.65 local-user idle-cut

Function

The **local-user idle-cut** command enables the idle-cut function for local users.

The **undo local-user idle-cut** command restores the default setting.

By default, the idle-cut function is disabled for local users.

Format

local-user *user-name* **idle-cut**

undo local-user *user-name* **idle-cut**

Parameters

Parameter	Description	Value
user-name	Specifies a user name.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

 Copyright © Huawei Technologies Co., Ltd.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a user uses no or a little network traffic for a long time, the user still occupies certain bandwidth, which reduces access rate of other users. After this command is executed, the device periodically detects the specified users. If the traffic volume of a user within the idle-cut period is lower than the threshold, the user is disconnected. By default, the idle-cut period is 10 minutes and threshold is 600K bytes. If the service scheme bound to an AAA domain contains the idle-cut parameters configured by the **19.1.55 idle-cut (service scheme view)** command, these idle-cut parameters take effect.

Precautions

When local authentication is used, this command is valid to only common users (for example, NAC and PPP users). To configure idle-cut for administrators, run the **local-user idle-timeout** command.

Example

Enable the idle-cut function for local user **hello@163.net**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net idle-cut
```

19.1.66 local-user password

Function

The **local-user password** command configures a password for a local account.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

local-user *user-name* **password**

NOTE

This command is an interactive command. After you enter **local-user** *user-name* **password** and press **Enter**, you can set the password as prompted. The local user password is a string of 8~128 case-sensitive characters.

Parameters

Parameter	Description	Value
user-name	Specifies the local user name.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

If no password is configured when a local user is created, the password is empty, and the local user cannot log in to the device.

NOTICE

A simple local user password may bring security risks. The user password must consist of two types of characters, including uppercase letters, lowercase letters, numerals, and special characters. In addition, the password cannot be the same as the user name or user name in a reverse order.

V200R005C00 and later versions use new encryption mechanism. After the AR is upgraded to V200R005C00 and later versions, you are advised to change the password to a more secure password.

V200R005C00 and later versions use new encryption mechanism. If the version is rolled back, the original version cannot identify the password configured in V200R005C00 and later versions. As a result, the configuration becomes invalid. To ensure that the password takes effect after rollback, during rollback, restore the password-relevant configuration in the configuration file to the configuration before the upgrade or change the password-relevant configuration in the configuration file to the configuration that can be identified by the original version.

Example

Set the password to abc@#123456 for the local account hello@163.net.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net password
Please configure the login password (8-128)
It is recommended that the password consist of at least 2 types of characters, i
ncluding lowercase letters, uppercase letters, numerals and special characters.
Please enter password:          //Enter the password abc@#123456
```

```
Please confirm password:          //Confirm the password abc@#123456
Info: Add a new user.
```

Related Topics

19.1.42 display local-user

19.1.67 local-user service-type

Function

The **local-user service-type** command sets the access type for a local user.

The **undo local-user service-type** command restores the default access type for a local user.

By default, a local user cannot use any access type.

Format

local-user *user-name* **service-type** { **8021x** | **bind** | **ftp** | **http** | **ppp** | **ssh** | **sslvpn** | **telnet** | **terminal** | **web** | **x25-pad** } *

undo local-user *user-name* **service-type**

Parameters

Parameter	Description	Value
user-name	Specifies a user name. If the user name contains a domain name delimiter such as @, the character before @ is the user name and the character behind @ is the domain name. If the value does not contain @, the entire character string is the user name and the domain name is the default one.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.
8021x	Indicates an 802.1X user.	-
bind	Indicates an IP session user.	-
ftp	Indicates an FTP user.	-
http	Indicates an HTTP user, which is usually used for web system login.	-
ppp	Indicates a PPP user.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ssh	Indicates an SSH user.	-
sslvpn	Indicates an SSLVPN user.	-
telnet	Indicates a Telnet user, which is usually a network administrator.	-
terminal	Indicates a terminal user, which is usually a user connected using a console port.	-
web	Indicates a Portal authentication user.	-
x25-pad	Indicates an X25-PAD user.	-

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device can manage access types of local users. After you specify the access type of a user, the user can successfully log in only when the configured access type is the same as the actual access type of the user.

Local users have the following access types:

- Administrative: FTP, HTTP, SSH, Telnet, x25-pad, and Terminal
- Common: 802.1X, bind, ppp, sslvpn, and web

Precautions

- When MAC authentication users use AAA local authentication, the device does not match or check the access type of local users. However, the access type must be configured; otherwise, local authentication for MAC address authentication users fails.
- Security risks exist if the user login mode is set to Telnet or FTP. You are advised set the user login mode to STelnet or SFTP and set the user access type to SSH.

  When a device starts without any configuration, HTTP uses the randomly generated self-signed certificate to support HTTPs. The self-signed certificate

may bring risks. Therefore, you are advised to replace it with the officially authorized digital certificate.

- Common access types cannot be configured together with administrative access types.

  If a user has been created and the password uses an irreversible encryption algorithm, the access type can only be set to an administrative one.

  If a user has been created and the password uses a reversible encryption algorithm, the access type can be set to an administrative or common one. When the access type is set to an administrative one, the encryption algorithm of the password is automatically converted into an irreversible encryption algorithm.

Example

Set the access type of the local user **user1@vipdomain** to SSH.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-user user1@vipdomain service-type ssh
```

Related Topics

19.1.60 local-user

19.1.42 display local-user

19.1.68 local-user time-range

Function

The **local-user time-range** command sets the access permission time range for a local user.

The **undo local-user time-range** command deletes the access permission time range for a local user.

By default, a local account can access the network anytime.

Format

local-user *user-name* **time-range** *time-name*

undo local-user *user-name* **time-range**

Parameters

Parameter	Description	Value
user-name	Indicates the local account.	The value is a string of 1 to 64 case-insensitive characters. It cannot contain spaces, asterisk, double quotation mark and question mark.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-name	Indicates the access permission time range of the local account. *time-name* specifies the name of the access permission time range.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word **all** cannot be specified as a time range name.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Use Scenario

After a local account is created, the account has no expiration date by default. To restrict the network access time of a local account, run the **local-user time-range** command. After the command is executed, the account can access network resources only in the specified time range.

Prerequisite

The time range has been created using the **19.7.24 time-range** command.

Precautions

If you run the **local-user time-range** and **19.1.64 local-user expire-date** commands in the AAA view multiple times, only the latest configuration takes effect.

After the access permission time range of an online local user is changed, the access permission time range of the user will take effect only when the user goes online next time.

Example

Set the access permission time segment of local account hello@163.net to 9:00-18:00 from Monday to Friday.

```
<Huawei> system-view
[Huawei] time-range huawei 9:00 to 18:00 working-day
[Huawei] aaa
[Huawei-aaa] local-user hello@163.net time-range huawei
```

Related Topics

19.1.42 display local-user

19.1.69 outbound recording-scheme

Function

The **outbound recording-scheme** command applies a policy to a recording scheme to record the connection information.

The **undo outbound recording-scheme** command deletes a policy from a recording scheme. Connection information is not recorded then.

By default, connection information is not recorded.

Format

outbound recording-scheme *recording-scheme-name*

undo outbound recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Incorrect connections may result in network faults, for example, loops. The connection information recorded on a server helps you monitor devices. When network faults occur, you can locate faults based on the connection information recorded on the server.

Prerequisites

A recording scheme has been created using the **recording-scheme** command in the AAA view and an HWTACACS server template has been associated with a recording scheme using the **recording-mode hwtacacs** command in the recording scheme view.

Example

Apply a policy to the recording scheme **scheme** to record the connection information.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server template hw1
[Huawei-hwtacacs-hw1] quit
[Huawei] aaa
[Huawei-aaa] recording-scheme scheme
[Huawei-aaa-recording-scheme] recording-mode hwtacacs hw1
[Huawei-aaa-recording-scheme] quit
[Huawei-aaa] outbound recording-scheme scheme
```

Related Topics

19.1.45 display recording-scheme
19.1.77 recording-scheme

19.1.70 password alert before-expire

Function

The **password alert before-expire** command to set the password expiration prompt days.

The **undo password alert before-expire** command restores the default password expiration prompt days.

By default, the number of password expiration prompt days is 30 days.

Format

password alert before-expire *day*

undo password alert before-expire

Parameters

Parameter	Description	Value
day	Indicates how long the system displays a prompt before the password expires. If the value is set to 0, the device does not prompt users that the passwords will expire.	The value is an integer that ranges from 0 to 999, in days. The default value is 30.

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

When a user logs in to the device, the device checks how many more days the password is valid for. If the number of days is less than the prompt days set in this

command, the device notifies the user in how many days the password will expire and asks the user whether they want to change the password.

- If the user changes the password, the device records the new password and modification time.
- If the user does not change the password or fails to change the password, the user can still log in as long as the password has not expired.

Example

Set the number of password expiration prompt days to 90.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy administrator
[Huawei-aaa-lupp-admin] password alert before-expire 90
```

19.1.71 password alert original

Function

The **password alert original** command enables the device to prompt users to change initial passwords.

The **undo password alert original** command disables the device from prompting users to change initial passwords.

By default, the device prompts users to change initial passwords.

Format

password alert original

undo password alert original

Parameters

None

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve device security, use this command to enable the initial password change prompt function. When a user logs in to the device:

- If the user enters the initial password, the device displays a message to ask whether to change the initial password. The user can select **Y** or **N**:

  - If the user selects **Y** to change the password, the user needs to enter the old password, new password, and confirm password. The password can be successfully changed only when the old password is correct and the new password and confirm password are the same and meet requirements (password length and complexity). After the password is changed, the user can log in to the device successfully.
  - If the user selects **N** or fails to change the password, and the initial password is the default password, the device does not allow the user to log in. If the initial password is not the default password, the device allows the user to log in.
- If the entered password is not the initial password, the device does not display any message and the user can successfully log in.

After the **undo password alert original** command is executed, the initial password alert will be disabled, causing a security risk.

NOTE

The initial password may be the default password, the password created by a local user in the first login, or the password changed by another user (for example, user B changes user A's password, and user A uses the changed password to log in. The device displays a prompt message in this situation).

Precautions

This function is only valid for Telnet users, SSH users, and terminal users.

Example

Enable the device to prompt users to change initial passwords.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy administrator
[Huawei-aaa-lupp-admin] password alert original
```

19.1.72 password expire

Function

The **password expire** command sets the password validity period.

The **undo password expire** command restores the default password validity period.

By default, the password validity period is 90 days.

Format

password expire *day*

undo password expire

Parameters

Parameter	Description	Value
day	Indicates the password validity period. If the value is 0, the password is permanently valid.	The value is an integer that ranges from 0 to 999, in days. The default value is 90.

Views

Local administrator password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, the administrator can use this command to set the validity period for local user's password. When the validity period expires, the password becomes invalid.

If the local user still uses this password to log in to the device, the device allows the user to log in, prompts the user that the password has expired, and asks the user whether to change the password:

- If the user selects **Y**, the user needs to enter the old password, new password, and confirm password. The password can be successfully changed only when the old password is correct and the new password and confirm password are the same and meet requirements (password length and complexity). After the password is changed, the user can log in to the device successfully.
- If the user selects **N** or fails to change the password, the user cannot log in.

Precautions

Changing the system time will affect the password validity status.

After this command is executed, the device checks whether the password expires every minute; therefore, there may be a time difference within 1 minute.

Example

Set the password validity period to 120 days.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy administrator
[Huawei-aaa-lupp-admin] password expire 120
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.73 password history record number

Function

The **password history record number** command sets the maximum number of historical passwords recorded for each user.

The **undo password history record number** command restores the default maximum number of historical passwords recorded for each user.

By default, five historical passwords are recorded for each user.

Format

password history record number *number*

undo password history record number

Parameters

Parameter	Description	Value
number	Indicates the maximum number of historical passwords recorded for each user. If the value is set to 0, the device will not check whether a changed password is the same as any historical password.	The value is an integer that ranges from 0 to 12. The default value is 5.

Views

Local administrator password policy view, local access user password policy view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve password security, it is not recommended that you use a previously used password. You can set the maximum number of historical passwords recorded for each user. When a user changes the password, the device compares the new password against the historical passwords stored on the device. If the new password is the same as a stored password, the device displays an error message to prompt the user that password change fails.

Precautions

When the number of recorded historical passwords reaches the maximum value, the later password will overwrite the earliest password on the device.

 Copyright © Huawei Technologies Co., Ltd.

After the historical password recording function is disabled, the device does not record historical passwords; however, the passwords that have been stored are not deleted.

Example

Set the maximum number of historical passwords recorded for each administrator to 10.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy administrator
[Huawei-aaa-lupp-admin] password history record number 10
```

Set the maximum number of historical passwords recorded for each local access user to 10.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] local-aaa-user password policy access-user
[Huawei-aaa-lupp-acc] password history record number 10
```

19.1.74 permit-domain

Function

The **permit-domain** command specifies permitted domains for WLAN users.

The **undo permit-domain** command deletes the permitted domains of WLAN users.

By default, no permitted domain is specified for WLAN users.

Format

permit-domain name *domain-name* &<1-4>

undo permit-domain { **name** *domain-name* | **all** }

Parameters

Item	Description	Value
name *domain-name*	Specifies the name of a permitted domain for WLAN users.	The domain must already exist.
all	Deletes the permitted domain for all WLAN users.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a permitted domain is specified on an authentication profile or an interface, only the WLAN users in the permitted domain can be authenticated, authorized, or charged.

Prerequisites

Permitted domains have been created using the **domain** command.

Precautions

This command applies only to wireless users.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

If the service set mapping the interface has been bound to the radio, you cannot run this command. The command can be configured only after the service set is unbound from the radio.

Example

Specify permitted domain **dom** for WLAN users to the authentication profile **john**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain dom
[Huawei-aaa-domain-dom] quit
[Huawei-aaa] quit
[Huawei] authentication-profile name john
[Huawei-authen-profile-john] permit-domain name dom
```

Related Topics

19.1.50 domain (AAA view)

19.1.75 qos-profile (service scheme view)

Function

The **qos-profile** command binds a QoS profile to a service scheme.

The **undo qos-profile** command unbinds the QoS profile from the service scheme.

By default, no QoS profile is bound to a service scheme.

Format

qos-profile *profile-name*

undo qos-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of the QoS profile bound to the service scheme.	The value is the name of an existing QoS profile.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After creating a service scheme using the **19.1.90 service-scheme (AAA view)** command, you can run the **qos-profile** command to bind a QoS profile to the service scheme. The user assigned with the service scheme will have the attributes in the QoS profile.

Prerequisites

A QoS profile has been created using the **20.3.18 qos-profile** command.

Precautions

The RADIUS server can also deliver a QoS profile and the CAR to the device. (The CAR can also be set in a QoS profile.)

When the server delivers the CAR and a QoS profile using Huawei extended RADIUS attributes:

- If the server delivers the CAR, the device uses the CAR.
- If the server delivers a QoS profile, the device uses the QoS profile.
- If the server delivers the CAR and a QoS profile, the device preferentially uses the CAR.
- If the server does not deliver the CAR and QoS profile, the device uses the QoS profile bound to the service scheme.

Example

Bind the QoS profile **abc** to the service scheme **huawei**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme huawei
[Huawei-aaa-service-huawei] qos-profile abc
```

Related Topics

19.1.90 service-scheme (AAA view)

 Copyright © Huawei Technologies Co., Ltd.

19.1.76 recording-mode hwtacacs

Function

The **recording-mode hwtacacs** command associates an HWTACACS server template with a recording scheme.

The **undo recording-mode** command unbinds an HWTACACS server template from a recording scheme.

By default, no HWTACACS server template is associated with a recording scheme.

Format

recording-mode hwtacacs *template-name*

undo recording-mode

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

Recording scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device needs to send the records such as the executed commands, connection information, and system events to the specified HWTACACS accounting server; therefore, an HWTACACS server template needs to be associated with a recording scheme.

Prerequisites

The HWTACACS server template has been created by using the **19.3.14 hwtacacs-server template** command.

Example

Associate the recording scheme **scheme0** with the HWTACACS server template **tacacs1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server template tacacs1
[Huawei-hwtacacs-tacacs1] quit
[Huawei] aaa
[Huawei-aaa] recording-scheme scheme0
[Huawei-aaa-recording-scheme0] recording-mode hwtacacs tacacs1
```

Related Topics

19.3.2 display hwtacacs-server template

19.1.45 display recording-scheme

19.3.14 hwtacacs-server template

19.1.77 recording-scheme

19.1.77 recording-scheme

Function

The **recording-scheme** command creates a recording scheme and displays the recording scheme view.

The **undo recording-scheme** command deletes a recording scheme.

By default, no recording scheme is configured on the device.

Format

recording-scheme *recording-scheme-name*

undo recording-scheme *recording-scheme-name*

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a recording scheme takes effect, you can view the records such as the executed commands, connection information, and system-level events on the recording server. The records help you locate network faults. Because a recording scheme needs to be associated with an HWTACACS server template, the recording scheme is configured only when HWTACACS authentication or authorization is performed.

Creating a recording template using the **recording-scheme** command is mandatory for configuration.

Follow-up Procedure

Run the **recording-mode hwtacacs** command to associate an HWTACACS server template with the recording scheme.

After a recording scheme is created and associated with an HWTACACS server template, perform the following configurations in the AAA view:

- Run the **cmd recording-scheme** command to apply a policy in a recording scheme to record the commands executed on the device.
- Run the **outbound recording-scheme** command to apply a policy in a recording scheme to record the connection information.
- Run the **system recording-scheme** command to apply a policy in a recording scheme to record the system events.

Precautions

If the recording scheme to be configured does not exist, the **recording-scheme** command creates a recording scheme and displays the recording scheme view. If the recording scheme to be configured already exists, the **recording-scheme** command displays the recording scheme view.

Before deleting a recording scheme, ensure that the scheme has not been referenced by the **cmd recording-scheme** or **outbound recording-scheme** or **system recording-scheme** command.

Example

Create a recording scheme **scheme0**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] recording-scheme scheme0
[Huawei-aaa-recording-scheme0]
```

Related Topics

19.1.29 cmd recording-scheme
19.1.45 display recording-scheme
19.1.69 outbound recording-scheme
19.1.76 recording-mode hwtacacs
19.1.93 system recording-scheme

19.1.78 remote-aaa-user authen-fail

Function

The **remote-aaa-user authen-fail** command enables the remote AAA authentication account locking function, and sets the authentication retry interval, maximum number of consecutive authentication failures, and account locking period.

The **undo remote-aaa-user authen-fail** command disables the remote AAA authentication account locking function.

By default, the remote AAA account locking function is enabled, authentication retry interval is 30 minutes, maximum number of consecutive authentication failures is 30, and account locking period is 30 minutes.

Format

remote-aaa-user authen-fail retry-interval *retry-interval* **retry-time** *retry-time* **block-time** *block-time*

undo remote-aaa-user authen-fail

Parameters

Parameter	Description	Value
retry-interval *retry-interval*	Specifies the authentication retry interval.	The value is an integer that ranges from 5 to 65535, in minutes.
retry-time *retry-time*	Specifies the maximum number of consecutive authentication failures.	The value is an integer that ranges from 3 to 65535.
block-time *block-time*	Specifies the account locking period.	The value is an integer that ranges from 5 to 65535, in minutes.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To ensure account security, you can enable the device to lock the accounts that fail in remote AAA authentication. If a user enters incorrect account and password

 Copyright © Huawei Technologies Co., Ltd.

more than the maximum number of consecutive authentication failures within the given period, the account is locked. After a certain period, the account is unlocked.

Precautions

- This command is valid only for remote AAA authentication and is invalid for local authentication.
- In scenarios where an active/standby switchover is performed, the originally locked account is automatically unlocked.
- After the remote AAA authentication account locking function is disabled using the **undo remote-aaa-user authen-fail** command, the originally locked account is automatically unlocked.

Example

Enable the remote AAA account locking function, and set the authentication retry interval to 5 minutes, maximum number of consecutive authentication failures to 3, and account locking period to 5 minutes.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] remote-aaa-user authen-fail retry-interval 5 retry-time 3 block-time 5
```

Disable the remote AAA account locking function.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] undo remote-aaa-user authen-fail
Info: All blocked users will unblock. Continue?[Y/N] y
```

Related Topics

19.1.46 display remote-user authen-fail

19.1.79 remote-user authen-fail unblock

19.1.79 remote-user authen-fail unblock

Function

The **remote-user authen-fail unblock** command unlocks remote AAA authentication accounts.

Format

remote-user authen-fail unblock { **all** | **username** *username* }

Parameters

Parameter	Description	Value
all	Unlocks all accounts that fail the remote AAA authentication.	-

Parameter	Description	Value
username *username*	Unlocks a specified account that fails the remote AAA authentication.	The value is a string of 1 to 253 case-insensitive characters without spaces.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

You may need to unlock remote AAA authentication accounts in the following situations:

- When a user enters an incorrect user name or password fewer times than the maximum permitted, run the **remote-user authen-fail unblock** command to unlock the user and delete the incorrect record of the user from the device.
- When a user is incorrectly locked or needs to be unlocked due to special reasons, run the **remote-user authen-fail unblock** command to unlock the user.

Example

Unlock the remote AAA authentication account **test**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] remote-user authen-fail unblock username test
```

Related Topics

19.1.46 display remote-user authen-fail

19.1.80 reset aaa

Function

Using the **reset aaa** command, you can clear records of abnormal offline, user offline and failure to get online.

Format

reset aaa { **abnormal-offline-record** | **offline-record** | **online-fail-record** }

Parameters

Parameter	Description	Value
abnormal-offline-record	Clears records of user abnormal offline.	-
offline-record	Clears records of user offline.	-
online-fail-record	Clears records of user failure to get online.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

This command allows you to clear records of user offline, abnormal offline, and failure to get online. After the records are cleared, the function of recording information is enabled.

Example

Clear user offline records.

```
<Huawei> system-view
[Huawei] reset aaa offline-record
```

19.1.81 reset aaa statistics access-type-authenreq

Function

The **reset aaa statistics access-type-authenreq** command clears the number of requesting for MAC, Portal, or 802.1X authentication.

Format

reset aaa statistics access-type-authenreq

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When users send authentication requests, the device collects statistics on the number of initiating MAC, Portal, and 802.1X authentications.

To clear the number of requesting for MAC, Portal, or 802.1X authentication, run the **reset aaa statistics access-type-authenreq** command.

Example

Clear the number of requesting for MAC, Portal, or 802.1X authentication.

```
<Huawei> reset aaa statistics access-type-authenreq
```

19.1.82 reset aaa statistics offline-reason

Function

Using the **reset aaa statistics offline-reason** command, you can clear the statistics about reasons why users go offline.

Format

reset aaa statistics offline-reason

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **reset aaa statistics offline-reason** command to delete the statistics about reasons why users go offline, and then collect new statistics.

Example

Clear the statistics about reasons why users go offline.

```
<Huawei> reset aaa statistics offline-reason
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.83 reset access-user statistics

Function

The **reset access-user statistics** command deletes the statistics on access user authentication.

Format

reset access-user statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

When diagnosing and locating faults related to access user authentication, you need to collect statistics on user login and logout information within a period of time. Before the statistics collection, you can run the **reset access-user statistics** command to clear the historical statistics, and then run the **display access-user statistics** command to view the current statistics.

Example

Delete the statistics on access user authentication.

```
<Huawei> reset access-user statistics
```

19.1.84 reset local-user password history record

Function

The **reset local-user password history record** command clears historical passwords stored for the local user.

Format

reset local-user [*user-name*] **password history record**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
user-name	Clears the historical passwords of the specified user. If this parameter is not specified, the historical passwords of all local users are cleared.	The local user must exist on the device.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the administrator wants to record historical passwords of local users again, this command can be used to clear existing historical passwords.

Precautions

After this command is used, all historical passwords on the device are deleted and cannot be restored. This operation has security risks, so exercise caution when using it.

Example

Clear historical passwords of all local users.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] reset local-user password history record
```

Related Topics

19.1.73 password history record number

19.1.85 route set acl

Function

The **route set acl** command configures the local subnet information to be sent to the remote end.

The **undo route set acl** command restores the default setting.

By default, no local subnet information is sent to the remote end.

Format

route set acl *acl-number*

undo route set acl

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL to be sent to the remote end.	The value is an integer that ranges from 3000 to 3999.

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The headquarters and a branch use virtual tunnel interfaces to set up an IPSec tunnel. When you apply an IPSec profile to the Tunnel-template interface on the headquarters gateway and apply an IPSec profile to the tunnel interface on the branch gateway, you can run this command to send the source IP address configured in an ACL to the remote end. The source IP address can be used to generate subnet route information.

Precautions

This command can send subnet route information only when it is used together with the **19.1.86 route set interface** command.

Before running this command, you are advised to run the **19.7.4 acl (system view)** command to create an ACL.

Example

Send information about ACL 3000 to the remote end.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit ip source 192.168.1.0 0.0.0.255 destination 192.168.3.0 0.0.0.255
[Huawei-acl-adv-3000] quit
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] route set acl 3000
```

Related Topics

19.7.4 acl (system view)

 Copyright © Huawei Technologies Co., Ltd.

19.1.47 display service-scheme

19.1.86 route set interface

Function

The **route set interface** command configures the address of the interface bound to the IPSec tunnel to be sent to the remote end.

The **undo route set interface** command restores the default setting.

By default, no address of the interface bound to the IPSec tunnel is sent to the remote end.

Format

route set interface

undo route set interface

Parameters

None

Views

Service scheme view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The headquarters and a branch use virtual tunnel interfaces to set up an IPSec tunnel. You can run this command to send the address of the interface bound to the IPSec tunnel to the remote end. This address can be used to generate subnet route information.

Precautions

If you do not configure this command, packets cannot be sent through the IPSec tunnel even if the IPSec tunnel is successfully established and route information is sent to the remote end.

Example

Configure the address of the interface bound to the IPSec tunnel to be sent to the remote end.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] route set interface
```

Related Topics

19.1.47 display service-scheme

19.1.87 security-name enable

Function

The **security-name enable** command enables the security string function.

The **undo security-name enable** command disables the security string function.

By default, the security string function is enabled.

Format

security-name enable

undo security-name enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Some special clients use user names in the format of **username@domain*securitystring** in which a security string and a security string delimiter (*) are added to the user name. To ensure that the AAA server can identify such user names, run the **security-name enable** command to enable the security string function on the device. When sending a user name to the AAA server, the device deletes ***securitystring** and only uses **username@domain** for authentication.

You can run the **19.1.88 security-name-delimiter** command to modify the security string delimiter.

Example

Enable the security string function.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] security-name enable
```

 Copyright © Huawei Technologies Co., Ltd.

19.1.88 security-name-delimiter

Function

The **security-name-delimiter** command configures a delimiter for a security string.

The **undo security-name-delimiter** command restores the default delimiter for a security string.

By default, the delimiter for a security string in the AAA view is *, and no delimiter is available in the authentication profile view.

NOTE

This command only applies to 802.1X users. If the CHAP or PAP authentication is configured for 802.1X users, the device removes the security string, but does not encapsulate it into the HW-SecurityStr attribute. If the EAP authentication is configured for 802.1X users, the device removes the security string and encapsulates it into the HW-SecurityStr attribute.

Format

security-name-delimiter *delimiter*

undo security-name-delimiter

Parameters

Parameter	Description	Value
delimiter	Specifies a delimiter for a security string.	The value is \ / : < > | @ ' % or *.

Views

AAA view, authentication profile view

Default Level

In the AAA view, the default level is management level.

In the authentication profile view, the default level is configuration level.

Usage Guidelines

Usage Scenario

Some STAs may use the user name in the format of **username@domain*securitystring**. * is the security string delimiter. To enable the AAA server to identify this type of user name, you need to configure a delimiter for a security string on the device. In this way, when sending the user name to the AAA server, the device deletes the ***securitystring** and only uses **username@domain** for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When the command is executed in the AAA view, the configuration takes effect for all users. When the command is executed in the interface view, the configuration takes effect for only the users connected to this interface. When the command is executed in the authentication profile, the configuration takes effect for only the users connected to this authentication profile.

The delimiter for a security string cannot be the same as the domain name delimiter.

If you run the **security-name-delimiter** command in the AAA view, the delimiter for a security string is configured globally.

When this command is executed in the authentication profile, the configuration takes effect only after the authentication profile is bound to a VAP profile.

Example

Configure the delimiter for a security string as / in the AAA view.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] security-name-delimiter /
```

19.1.89 service-scheme (aaa domain view)

Function

The **service-scheme** command applies a service scheme to a domain.

The **undo service-scheme** command unbinds a service scheme from a domain.

By default, no service scheme is bound to a domain.

Format

service-scheme *service-scheme-name*

undo service-scheme

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme.	The value must be an existing service scheme name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The authorization configuration in a service scheme takes effect only when the service scheme is applied to a domain.

Prerequisites

A service scheme has been created and configured with required parameters.

Example

Apply the service scheme **srvscheme1** to the domain **huawei**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme srvscheme1
[Huawei-aaa-service-srvscheme1] quit
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] service-scheme srvscheme1
```

Related Topics

19.1.47 display service-scheme

19.1.90 service-scheme (AAA view)

19.1.90 service-scheme (AAA view)

Function

The **service-scheme** command creates a service scheme and displays the service scheme view.

The **undo service-scheme** command deletes a service scheme.

By default, no service scheme is configured.

Format

service-scheme *service-scheme-name*

undo service-scheme *service-scheme-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
service-scheme-name	Specifies the name of a service scheme.	The value is a string of 1 to 32 case-sensitive characters. It cannot contain spaces or the following symbols: /, \, :, *, ?, ", <, >, |, @, ', and %. The value cannot be - or --.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The service scheme is used to assign IP address pool and DNS server parameters to users.

Follow-up Procedure

Run the **service-scheme (AAA domain view)** command to apply the service scheme to a domain.

Precautions

If the service scheme to be configured does not exist, the **service-scheme (AAA view)** command creates a service scheme and displays the service scheme view. If the service scheme to be configured already exists, the **service-scheme (AAA view)** command displays the service scheme view.

A maximum of 256 service schemes can be configured on the device.

To delete or modify the service scheme applied to a domain, run the **undo service-scheme (AAA domain view)** command to unbind the service scheme from the domain.

Example

Create a service scheme **srvscheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme srvscheme1
[Huawei-aaa-service-srvscheme1]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.1.47 display service-scheme
19.1.89 service-scheme (aaa domain view)

19.1.91 state (AAA domain view)

Function

The **state** command configures the state of a domain.

The **undo state** command restores the state of a domain.

By default, a domain is in active state after being created.

Format

state { **active** | **block** [**time-range** *time-name* &<1-4>] }

undo state [**block time-range** [*time-name* &<1-4>]]

Parameters

Parameter	Description	Value
active	Sets the domain state to active.	-
block	Sets the domain state to blocking.	-
time-range *time-name*	Indicates the block time range of the domain. *time-name* specifies the name of the block time range. If this parameter is not specified, the domain is always blocked.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. In addition, the word **all** cannot be specified as a time range name.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If exceptions occur during service configuration, set the domain in blocking state to block access of new users. After the service configuration is complete, set the domain in active state.

Prerequisite

Before specifying the *time-name* parameter, ensure that the time range has been created using the **19.7.24 time-range** command.

Precautions

After the **state block** command is run to set the domain state to block, online users in the domain are not affected.

After the **state block time-range** command is run to set the state of a domain including online users to block, the domain state turns from active to block within the specified time range, and online users are forced to go offline.

Example

Set the state of the domain **vipdomain** to blocking.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain vipdomain
[Huawei-aaa-domain-vipdomain] state block
```

Set the name of the time range in which the **vipdomain** domain state turns to block to **tim**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain vipdomain
[Huawei-aaa-domain-vipdomain] state block time-range tim
Warning: This operation may cause online users to go offline. Continue? [Y/N]Y
```

Related Topics

19.1.50 domain (AAA view)

19.1.92 statistic enable (AAA domain view)

Function

The **statistic enable** command enables traffic statistics collection for domain users.

The **undo statistic enable** command disables traffic statistics collection for domain users.

By default, traffic statistics collection is disabled for domain users.

Format

statistic enable

undo statistic enable

Parameters

None

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To implement traffic-based accounting, you can use this command to enable traffic statistics collection for a domain. Then the device collects traffic statistics for the users in the domain. If an accounting server is configured, the device sends traffic statistics to the accounting server through accounting packets so that the server performs accounting for the users based on traffic statistics.

Follow-up Procedure

Run the **19.1.37 display access-user (All views)** command to view traffic statistics of users.

Precautions

The **20.6.2 statistics enable (QoS profile view)** command executed in the QoS profile view collects DAA service statistics for domain users. The statistics include the number of bytes matching each tariff level. This command collects non-DAA service statistics. The device sends the two types of statistics to the accounting server for flexible accounting.

Only Portal authentication users on the WAN-side interface and PPP authentication users support this command.

Example

Enable traffic statistics collection for domain users.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] statistic enable
```

Related Topics

19.1.41 display domain

19.1.93 system recording-scheme

Function

The **system recording-scheme** command applies a policy in a recording scheme to record the system events.

The **undo system recording-scheme** command deletes a policy from a recording scheme. System events are not recorded then.

By default, system events are not recorded.

Format

system recording-scheme *recording-scheme-name*

undo system recording-scheme

Parameters

Parameter	Description	Value
recording-scheme-name	Specifies the name of a recording scheme.	The recording scheme must already exist.

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system events recorded on an HWTACACS server helps you monitor devices. When network faults occur, you can isolate faults based on the system events recorded on the HWTACACS server.

Prerequisites

A recording scheme has been created using the **recording-scheme** command in the AAA view and an HWTACACS server template has been associated with a recording scheme using the **recording-mode hwtacacs** command in the recording scheme view.

Precautions

Currently, the device can record only the events caused by the **reboot** command.

Example

Apply a policy in the recording scheme **scheme** to record the system events.

```
<Huawei> system-view
[Huawei] hwtacacs-server template hw1
[Huawei-hwtacacs-hw1] quit
[Huawei] aaa
[Huawei-aaa] recording-scheme scheme
[Huawei-aaa-recording-scheme] recording-mode hwtacacs hw1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-aaa-recording-scheme] quit
[Huawei-aaa] system recording-scheme scheme
```

Related Topics

19.1.45 display recording-scheme

19.1.77 recording-scheme

19.1.94 user-group (AAA domain view)

Function

The **user-group** command binds the users in a domain to the authorization information of a user group.

The **undo user-group** command unbinds the users in a domain from the authorization information of a user group.

By default, no authorization information of a user group is bound to the users in a domain.

Format

user-group *group-name*

undo user-group

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The user group name must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **user-group** command in the AAA domain to bind the users in a domain to the authorization information of a user group.

Precautions

- The user group to be specified using the **local-user user-group** command must have been created using the **user-group** command.

 Copyright © Huawei Technologies Co., Ltd.

- A user group cannot be deleted after being referenced to a domain using this command.
- Huawei proprietary attribute 82 delivered by RADIUS cannot be used together with the function of binding authentication information of a user group to a domain.

Example

Bind the user group **group1** to the domain **test**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain test
[Huawei-aaa-domain-test] user-group group1
```

Related Topics

19.6.150 user-group

19.1.95 user-password complexity-check

Function

The **user-password complexity-check** command enables password complexity check.

The **undo user-password complexity-check** command disables password complexity check.

By default, a device checks password complexity.

Format

user-password complexity-check

undo user-password complexity-check

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can choose whether to enable password complexity check.

Precautions

To ensure device security, do not disable password complexity check, and change the password periodically.

Example

Disable password complexity check.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] undo user-password complexity-check
```

Related Topics

19.1.60 local-user

19.1.96 wins (service scheme view)

Function

The **wins** command configures the primary or secondary WINS server address in the service scheme view.

The **undo wins** command deletes a primary or secondary WINS server address.

By default, no primary or secondary WINS server address is configured in a service scheme.

Format

wins *ip-address* [**secondary**]

undo wins [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Indicates the WINS server address configured in a service scheme.	The value is in dotted decimal notation.
secondary	Indicates that the IP address of the secondary WINS server is configured.	-

Views

service scheme view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The AAA service scheme allows the WINS server address to be bound. IPSec binds the AAA service scheme to the IPSec policy template and sends the WINS server address to users.

Example

Configure the WINS server address in the service scheme **svcscheme1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] service-scheme svcscheme1
[Huawei-aaa-service-svcscheme1] wins 10.1.1.1
```

Related Topics

19.1.47 display service-scheme

19.1.97 aaa-author session-timeout invalid-value enable

Function

The **aaa-author session-timeout invalid-value enable** command prevents a device from disconnecting or reauthenticating users when the RADIUS server delivers session-timeout with value 0.

The **undo aaa-author session-timeout invalid-value enable** command restores the default setting.

By default, when the RADIUS server delivers session-timeout with value 0, this attribute does not take effect.

Format

aaa-author session-timeout invalid-value enable

undo aaa-author session-timeout invalid-value enable

Parameters

None

Views

AAA view

Default Level

3: Management level

Usage Guidelines

When the RADIUS server delivers session-timeout with value 0:

- If the **aaa-author session-timeout invalid-value enable** command is not configured, the session-timeout attribute delivered by the server does not take

 Copyright © Huawei Technologies Co., Ltd.

effect and the period for disconnecting or reauthenticating users depends on the device configuration.

- If the **aaa-author session-timeout invalid-value enable** command is configured, the session-timeout attribute delivered by the server takes effect and the device does not disconnect or reauthenticate users.

You can run the **dot1x timer reauthenticate-period** *reauthenticate-period-value* or **mac-authen timer reauthenticate-period** *reauthenticate-period-value* command to configure the period for disconnecting or reauthenticating users on the device.

Example

Prevent the device from disconnecting or reauthenticating users when the RADIUS server delivers session-timeout with value 0.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] aaa-author session-timeout invalid-value enable
```

19.2 RADIUS Configuration Commands

19.2.1 called-station-id mac-format

Function

The **called-station-id mac-format** command sets the encapsulation format of the MAC address in the called-station-id (Type 30) attribute of RADIUS packets.

The **undo called-station-id mac-format** command restores the default encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets.

By default, the encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets is XX-XX-XX-XX-XX-XX, in uppercase.

Format

called-station-id mac-format { **dot-split** | **hyphen-split** } [**mode1** | **mode2**] [**lowercase** | **uppercase**]

called-station-id mac-format unformatted [**lowercase** | **uppercase**]

undo called-station-id mac-format

Parameters

Parameter	Description	Value
dot-split	Indicates that the dot (.) is used as the separator in a MAC address.	-

Parameter	Description	Value
hyphen-split	Indicates that the hyphen (-) is used as the separator in a MAC address.	-
unformatted	Indicates that no separator is used in a MAC address.	-
mode1	Indicates that the MAC address in the called-station-id attribute uses the XXXX-XXXX-XXXX or XXXX.XXXX.XXXX format.	-
mode2	Indicates that the MAC address in the called-station-id attribute uses the XX-XX-XX-XX-XX-XX or XX.XX.XX.XX.XX.XX format.	-
lowercase	Indicates that the MAC address in the called-station-id attribute uses the lowercase.	-
uppercase	Indicates that the MAC address in the called-station-id attribute uses the uppercase.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Called-station-id (Type 30) attribute indicates the MAC address and SSID of an AP. The default format of the MAC address in the called-station-id attribute of RADIUS packets from the device is XX-XX-XX-XX-XX-XX. If the RADIUS server does not support the default format, run the **called-station-id mac-format** command to change the format.

Example

Set the dot as the separator in a MAC address and the encapsulation format of the MAC address in the called-station-id attribute to XX.XX.XX.XX.XX.XX in uppercase.

```
<Huawei> system-view
[Huawei] radius-server template huawei
[Huawei-radius-huawei] called-station-id mac-format dot-split mode2 uppercase
```

Related Topics

19.2.9 display radius-server configuration

19.2.2 calling-station-id mac-format

Function

The **calling-station-id mac-format** command sets the encapsulation format of the MAC address in the calling-station-id (Type 31) attribute of RADIUS packets.

The **undo calling-station-id mac-format** command restores the default encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets.

By default, the encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets is xxxx-xxxx-xxxx, in lowercase.

Format

calling-station-id mac-format { **dot-split** | **hyphen-split** | **colon-split** } [**mode1** | **mode2**] [**lowercase** | **uppercase**]

calling-station-id mac-format unformatted [**lowercase** | **uppercase**]

calling-station-id mac-format bin

undo calling-station-id mac-format

Parameters

Parameter	Description	Value
dot-split	Indicates that the dot (.) is used as the separator in a MAC address.	-
hyphen-split	Indicates that the hyphen (-) is used as the separator in a MAC address.	-
colon-split	Indicates that the colon (:) is used as the separator in a MAC address.	-
unformatted	Indicates that no separator is used in a MAC address.	-
mode1	Indicates that the MAC address in the calling-station-id attribute uses the "xxxx**separator**xxxx**separator**xxxx" format.	-
mode2	Indicates that the MAC address in the calling-station-id attribute uses the "xx**separator**xx**separator**xx**separator**xx**separator**xx**separator**xx" format.	-
lowercase	Indicates that the MAC address in the calling-station-id attribute uses the lowercase.	-
uppercase	Indicates that the MAC address in the calling-station-id attribute uses the uppercase.	-
bin	Indicates that the MAC address in the calling-station-id attribute uses the binary form.	-

Views

RADIUS server template view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

The default format of the MAC address in the calling-station-id (Type 31) attribute of RADIUS packets from the device is xxxx-xxxx-xxxx. If the RADIUS server does not support the default format, run the **calling-station-id mac-format** command to change the format.

Example

Set the dot as the separator in a MAC address and the encapsulation format of the MAC address in the calling-station-id attribute to XX.XX.XX.XX.XX.XX in uppercase.

```
<Huawei> system-view
[Huawei] radius-server template huawei
[Huawei-radius-huawei] calling-station-id mac-format dot-split mode2 uppercase
```

Related Topics

19.2.9 display radius-server configuration

19.2.3 display radius-attribute

Function

The **display radius-attribute** command displays the RADIUS attributes supported by the device.

Format

display radius-attribute [**name** *attribute-name* | **type** { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* }]

Parameters

Parameter	Description	Value
name *attribute-name*	Displays a specified RADIUS attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
type { *attribute-number1* | **huawei** *attribute-number2* | **microsoft** *attribute-number3* | **dslforum** *attribute-number4* }	Displays the RADIUS attribute of a specified type: • *attribute-number1* specifies the standard attribute. • **huawei** *attribute-number2* specifies a Huawei attribute. • **microsoft** *attribute-number3* specifies a Microsoft attribute. • **dslforum** *attribute-number4* specifies a Digital Subscriber Line Forum attribute.	The value of *attribute-number1*, *attribute-number2*, *attribute-number3*, or *attribute-number4* is an integer that ranges from 1 to 2048.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before connecting the device to a RADIUS server, run the **display radius-attribute** command to view the RADIUS attributes supported by the device. If the device and RADIUS server support different RADIUS attributes according to the command output, run the **19.2.15 radius-attribute disable** command on the device to disable RADIUS attributes that are not supported by the RADIUS server or run the **19.2.20 radius-attribute translate** command to translate RADIUS attributes.

Example

Display the RADIUS attributes supported by the device.

```
<Huawei> display radius-attribute
  Codes: Auth(Authentication), Acct(Accounting)
         Req(Request), Accp(Accept), Rej(Reject)
         Resp(Response), COA(Change-of-Authorization)
         0(Can not exist in this packet)
         1(Can exist in this packet)
-------------------------------------------------------------------------------
Attribute                    Service    Auth Auth Auth Acct Acct COA COA
Name(Type)                      Type     Req  Accp Rej  Req  Resp Req Ack
-------------------------------------------------------------------------------
User-Name(1)                   All       1    0    0    1    0    1    1
User-Password(2)               All       1    0    0    0    0    0    0
CHAP-Password(3)               All       1    0    0    0    0    0    0
```

```
NAS-IP-Address(4)          All      1    0    0    1    0    1    1
NAS-Port(5)                All      1    0    0    1    0    1    1
Service-Type(6)            All      1    1    0    0    0    0    0
......
```

NOTE

The preceding information is an example. The displayed attribute type depends on the actual situation.

Table 19-20 Description of the **display radius-attribute** command output

Item	Description
0(Can not exist in this packet)	Attribute not supported in packets.
1(Can exist in this packet)	Attribute supported in packets.
Attribute Name(Type)	Attribute name and type.
Service Type	Protocol type of the attribute.
Auth Req	Authentication request packet.
Auth Accp	Authentication accept packet.
Auth Rej	Authentication reject packet.
Acct Req	Accounting request packet.
Acct Resp	Accounting response packet.
COA Req	Change of Authorization (COA) request packet.
COA Ack	COA acknowledgement packet.

Display the RADIUS attribute numbered 2.

```
<Huawei> display radius-attribute type 2
 Radius Attribute Type        : 2
 Radius Attribute Name        : User-Password
 Radius Attribute Description : This Attribute indicates the password of the user to be authenticated. Only
valid for the PAP authentication.
 Supported Packets            : Auth Request
```

Table 19-21 Description of the **display radius-attribute type** command output

Item	Description
Radius Attribute Type	Type of the RADIUS attribute.
Radius Attribute Name	Name of the RADIUS attribute.
Radius Attribute Description	Description of the RADIUS attribute.
Supported Packets	Packets that support the RADIUS attribute.

Related Topics

19.2.15 radius-attribute disable

19.2.20 radius-attribute translate

19.2.4 display radius-attribute check

Function

The **display radius-attribute check** command displays the attributes to be checked in RADIUS Access-Accept packets.

Format

display radius-attribute [**template** *template-name*] **check**

Parameters

Parameter	Description	Value
template *template-name*	Displays the RADIUS attribute check configuration of a specified RADIUS server template.	The RADIUS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the **radius-attribute check** command is executed to configure the attributes to be checked in RADIUS Access-Accept packets, you can use the **display radius-attribute check** command to view these attributes.

Example

Check the attributes to be checked in RADIUS Access-Accept packets.

```
<Huawei> display radius-attribute check
Server-template-name: test1
-----------------------------------------------
check-attr
-----------------------------------------------
Framed-Protocol
-----------------------------------------------
```

Table 19-22 Description of the **display radius-attribute check** command output

Item	Description
Server-template-name	Name of the RADIUS server template.
check-attr	Attributes to be checked in RADIUS Access-Accept packets.
Framed-Protocol	Encapsulation protocol for services of the Frame type.

Related Topics

19.2.14 radius-attribute check

19.2.5 display radius-attribute disable

Function

The **display radius-attribute disable** command displays the disabled RADIUS attributes.

Format

display radius-attribute [**template** *template-name*] **disable**

Parameters

Parameter	Description	Value
template *template-name*	Displays the disabled RADIUS attributes in a specified RADIUS server template. If this parameter is not specified, the disabled RADIUS attributes in all the RADIUS server templates are displayed.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can use the **display radius-attribute disable** command to view the RADIUS attributes disabled by using the **radius-attribute disable** command.

To enable a RADIUS attribute, run the **undo radius-attribute disable** command in the RADIUS server template view.

Example

Display the disabled RADIUS attributes on the device.

```
<Huawei> display radius-attribute disable
Packet-Type: Type of the RADIUS packets to be modified. 1 indicates valid; 0 ind
icates invalid. Bit 1 to bit 4 indicate the authentication request, authenticati
on accept, accounting request, and accounting response packets.

Server-template-name: d
--------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
--------------------------------------------------------------------------------
0                7             0             0            send      0 0 0 0
--------------------------------------------------------------------------------
```

Table 19-23 Description of the display radius-attribute disable command output

Item	Description
Server-template-name	RADIUS server template name.
Source-Vendor-ID	Vendor ID of the source attribute.
Source-Sub-ID	ID of the source attribute's sub-attribute.
Dest-Vendor-ID	Vendor ID of the destination attribute.
Dest-Sub-ID	ID of the destination attribute's sub-attribute.
Direct	Direction in which the attribute is translated. • receive: Translates RADIUS attributes for received packets. • send: Translates RADIUS attributes for sent packets.
Packet-Type	Type of RADIUS packets. • 0: The RADIUS attributes of this type of packets are not translated. • 1: The RADIUS attributes of this type of packets are translated.

Related Topics

19.2.15 radius-attribute disable

19.2.6 display radius-attribute translate

Function

The **display radius-attribute translate** command displays the RADIUS attribute translation configuration.

Format

display radius-attribute [**template** *template-name*] **translate**

Parameters

Parameter	Description	Value
template *template-name*	Displays the RADIUS attribute translation configuration of a specified RADIUS server template. *template-name* specifies the name of the RADIUS server template that is created using the **radius-server template** command. If this parameter is not specified, the disabled RADIUS attributes translation configuration in all the RADIUS server templates are displayed.	The value must be an existing RADIUS server template name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **radius-attribute translate** command to configure the device to translate RADIUS attributes, run the **display radius-attribute translate** command to check the configuration.

Example

Display the RADIUS attribute translation configuration.

```
<Huawei> display radius-attribute translate
Packet-Type: Type of the RADIUS packets to be modified. 1 indicates valid; 0 indicates invalid. Bit 1 to bit 4
```

```
indicate the authentication request, authentication accept, accounting request, and accounting response
packets.

Server-template-name: rds
--------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
--------------------------------------------------------------------------------
0              6            0             40          receive    0 0 0 0
--------------------------------------------------------------------------------
Server-template-name: eee
--------------------------------------------------------------------------------
Source-Vendor-ID Source-Sub-ID Dest-Vendor-ID Dest-Sub-ID  Direct    Packet-Type
--------------------------------------------------------------------------------
234567         123          2011          20          --         0 1 0 1
--------------------------------------------------------------------------------
```

Table 19-24 Description of the **display radius-attribute translate** command output

Item	Description
Server-template-name	Server template name.
Source-Vendor-ID	Vendor ID of the source attribute.
Source-Sub-ID	ID of the source attribute's sub-attribute.
Dest-Vendor-ID	Vendor ID of the destination attribute.
Dest-Sub-ID	ID of the destination attribute's sub-attribute.
Direct	Direction in which the attribute is translated. ● receive: Translates RADIUS attributes for received packets. ● send: Translates RADIUS attributes for sent packets.
Packet-Type	Type of RADIUS packets. ● 0: The RADIUS attributes of this type of packets are not translated. ● 1: The RADIUS attributes of this type of packets are translated.

Related Topics

19.2.20 radius-attribute translate

19.2.7 display radius-server accounting-stop-packet

Function

The **display radius-server accounting-stop-packet** command displays information about accounting-stop packets on the RADIUS server.

Format

display radius-server accounting-stop-packet { **all** | **ip** { *ip-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Displays all the accounting-stop packets.	-
ip *ip-address*	Displays the accounting-stop packets with the specified IP address.	The value of *ip-address* is in dotted decimal notation.
ip *ipv6-address*	Displays the accounting-stop packets with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display radius-server accounting-stop-packet** command output helps you check configurations or isolate faults.

Example

Display the accounting-stop packets with the IP address being 10.138.104.32.

```
<Huawei> display radius-server accounting-stop-packet ip 10.138.104.32
 ---------------------------------------------------------------------------
 Time Stamp  Resend Times  Session Time  Username
 ---------------------------------------------------------------------------
 1980409     6             22            g@rds
 ---------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 19-25 Description of the display radius-server accounting-stop-packet command output

Item	Description
Time Stamp	Timestamp of an accounting-stop packet.

Item	Description
Resend Times	Number of times that accounting-stop packets have been retransmitted.
Session Time	Session time, in seconds.
Username	User name.

Related Topics

19.2.23 radius-server accounting-stop-packet resend
19.2.48 reset radius-server accounting-stop-packet

19.2.8 display radius-server authorization configuration

Function

The **display radius-server authorization configuration** command displays the configuration of RADIUS authorization servers.

Format

display radius-server authorization configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After running the **radius-server authorization** command to configure an authorization server, run the **display radius-server authorization configuration** command to check whether the authorization server configuration is correct.

Example

Display the configuration of RADIUS authorization servers.

```
<Huawei> display radius-server authorization configuration
 ---------------------------------------------------------------------------
 Attribute decode same as template    :  N
 Attribute encode same as template    :  Y
 User information match type          :  all
 Calling-station-id decode MAC-format :  xx-xx-xx-xx-xx-xx
```

```
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
IP-Address      Shared-key              Group                   Protect         Ack-reserved-interval
--------------------------------------------------------------------------------
10.10.1.114     ****************        -                       Y               20
vpn-instance : -
--------------------------------------------------------------------------------
1 RADIUS authorization server(s) in total
```

Table 19-26 Description of the **display radius-server authorization configuration** command output

Item	Description
Attribute decode same as template	Whether the device parses attributes in the RADIUS dynamic authorization packet based on the configurations in the RADIUS server template. To configure this field, run the **19.2.29 radius-server authorization attribute-decode-sameastemplate** command.
Attribute encode same as template	Whether the device encapsulates attributes in the CoA or DM Response packet based on the configurations in the RADIUS server template. To configure this field, run the **19.2.30 radius-server authorization attribute-encode-sameastemplate** command.
User information match type	Method used by a device to perform a match check between the RADIUS attribute in the received CoA or DM Request packet and user information on the device. The values are as follows: ● all: The device performs a match check between all attributes in the received CoA or DM Request packet and user information on the device. ● any: The device performs a match check between an attribute in the received CoA or DM Request packet and user information on the device. To configure this field, run the **19.2.32 radius-server authorization match-type** command.
IP-Address	IP address of a RADIUS authorization server. To configure this field, run the **radius-server authorization** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Shared-key	Shared key of the RADIUS authorization server. To configure this field, run the **radius-server authorization** command.
Group	RADIUS server group matching the RADIUS authorization server. To configure this field, run the **radius-server authorization** command.
Ack-reserved-interval	Holdtime of RADIUS authorization response packets. To configure this field, run the **radius-server authorization** command.
Protect	Whether the security hardening function is enabled. To configure this field, run the **radius-server authorization** command.
vpn-instance	Name of the VPN instance that the RADIUS authorization server is bound to. To configure this field, run the **radius-server authorization** command.

Related Topics

19.2.28 radius-server authorization

19.2.9 display radius-server configuration

Function

The **display radius-server configuration** command displays configuration information about a RADIUS server template.

Format

display radius-server configuration [**template** *template-name*]

Parameters

Parameter	Description	Value
template *template-name*	Specifies the name of a RADIUS server template. If this parameter is not specified, configuration information of all RADIUS server templates is displayed.	The RADIUS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the configuration of a RADIUS server template is completed or a RADIUS fault needs to be rectified, you can run this command to check whether the configuration of the RADIUS server template is correct.

Example

Display configuration information about the RADIUS server template named **shiva**.

```
<Huawei> display radius-server configuration template shiva
  ------------------------------------------------------------------------------
  Server-template-name          :  shiva
  Protocol-version              :  standard
  Traffic-unit                  :  B
  Shared-secret-key             :  %^%#O09i(W[^YT4g#Z37Nct9$IK#TH(-B6-1|<;q|D)"%^%#
  Group-filter                  :  class
  Timeout-interval(in second)   :  5
  Retransmission                :  2
  EndPacketSendTime             :  0
  Dead time(in minute)          :  5
  Domain-included               :  YES
  NAS-IP-Address                :  -
  Calling-station-id MAC-format :  xxxx-xxxx-xxxx
  Called-station-id MAC-format  :  XX.XX.XX.XX.XX.XX
  NAS-Port-ID format            :  New
  Service-type                  :  -
  NAS-IPv6-Address              :  ::
  Server algorithm              :  master-backup
  Detect-interval(in second)    :  60
  Testuser-username             :  huawei
  Testuser-ciperpwd             :  %^%#.5*EDl^j_WXg[#Z>plj8;k|8.s*ju<_F~g9k`0*9%^%#
  Authentication Server 1       :  10.7.66.66     Port:1812  Weight:80  [UP]
                                Vrf:- LoopBack:NULL Vlanif:NULL
                                Source IP: ::
  Authentication Server 2       :  10.7.66.67     Port:1812  Weight:80  [UP]
                                Vrf:- LoopBack:NULL Vlanif:NULL
```

```
                          Source IP: ::
Accounting Server    1      :  10.7.66.66     Port:1813  Weight:80  [UP]
                          Vrf:- LoopBack:NULL Vlanif:NULL
                          Source IP: ::
Accounting Server    2      :  10.7.66.67     Port:1813  Weight:80  [UP]
                          Vrf:- LoopBack:NULL Vlanif:NULL
                          Source IP: ::
-------------------------------------------------------------------------------
```

Table 19-27 Description of the **display radius-server configuration template** *template-name* command output

Item	Description
Server-template-name	Name of a RADIUS server template. To configure this item, run the **radius-server template** command.
Protocol-version	RADIUS protocol version: ● standard ● huawei ● iphotel ● portal
Traffic-unit	Traffic unit in the RADIUS server template: ● B: Byte ● KB: Kilobyte ● MB: Megabyte ● GB: Gigabyte To configure this item, run the **radius-server traffic-unit** command.
Shared-secret-key	Shared key in the RADIUS server template. To configure this item, run the **radius-server shared-key** command.
Group-filter	Filtering field of a user group. Currently, only the class field can be used as the filtering field of a user group.
Timeout-interval(in second)	Response timeout period of a RADIUS server. To configure this item, run the **19.2.40 radius-server retransmit timeout dead-time** command.
Retransmission	Number of times RADIUS packets are retransmitted. To configure this item, run the **19.2.40 radius-server retransmit timeout dead-time** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EndPacketSendTime	Number of times RADIUS accounting-stop packets are retransmitted. To configure this item, run the **radius-server accounting-stop-packet resend** command.
Dead time(in minute)	Interval for the primary RADIUS server to revert to the active status. To configure this item, run the **19.2.40 radius-server retransmit timeout dead-time** command.
Domain-included	Whether the RADIUS user name contains the domain name. ● YES: The user name contains the domain name. ● NO: The user name does not contain the domain name. ● Original: The device does not modify the user name entered by the user. To configure this item, run the **19.2.47 radius-server user-name domain-included** command.
NAS-IP-Address	NAS IP address in RADIUS packets.
Calling-station-id MAC-format	Encapsulation format of the MAC address in the calling-station-id attribute of RADIUS packets.
Called-station-id MAC-format	Encapsulation format of the MAC address in the called-station-id attribute of RADIUS packets. To configure this item, run the **19.2.1 called-station-id mac-format** command.
NAS-Port-ID format	Format of the NAS-Port-ID attribute on the RADIUS server. ● New: Uses the new format of the NAS-Port-ID attribute. ● Old: Uses the old format of the NAS-Port-ID attribute. To configure this item, run the **19.2.39 radius-server nas-port-id-format** command.
Service-type	Service type.
NAS-IPv6-Address	NAS IPv6 address in RADIUS packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Server algorithm	Algorithm for selecting RADIUS servers. • master-backup: Specifies the algorithm for selecting RADIUS servers as packet-based primary/secondary. • master-backup based-user: Specifies the algorithm for selecting RADIUS servers as single user-based primary/secondary. • loading-share: Specifies the algorithm for selecting RADIUS servers as packet-based load balancing. • loading-share based-user: Specifies the algorithm for selecting RADIUS servers as single user-based load balancing. To configure this item, run the **19.2.24 radius-server algorithm** command.
Detect-interval(in second)	Automatic detection interval for RADIUS servers. To configure this item, run the **radius-server detect-server** command.
Testuser-username	User name for automatic RADIUS server detection. To configure this item, run the **radius-server testuser** command.
Testuser-ciperpwd	User password for automatic RADIUS server detection. To configure this item, run the **radius-server testuser** command.
Authentication Server 1	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the primary RADIUS authentication server. To configure this item, run the **radius-server authentication** command.
Authentication Server 2	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the secondary RADIUS authentication server. To configure this item, run the **radius-server authentication** command.
Accounting Server 1	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the primary RADIUS accounting server. To configure this item, run the **radius-server accounting** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Accounting Server 2	IP address, interface number, weight, status, VPN instance, source interface, and source IP address of the secondary RADIUS accounting server. To configure this item, run the **radius-server accounting** command.

19.2.10 display radius-server dead-interval dead-count

Function

The **display radius-server dead-interval dead-count** command displays configuration information about the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval.

Format

display radius-server { **dead-interval** | **dead-count** }

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval are configured using the **19.2.33 radius-server dead-interval dead-count** command, you can run the **display radius-server** { **dead-interval** | **dead-count** } command to check configuration information about the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval.

Example

Display configuration information about the RADIUS server detection interval.

```
<Huawei> display radius-server dead-interval
Radius server state detected internal is 5.
```

Display configuration information about the maximum number of consecutive packets that are not acknowledged by the RADIUS server in each detection interval.

```
<Huawei> display radius-server dead-count
Radius server state detected count is 2.
```

Table 19-28 Description of the **display radius-server** { **dead-interval** | **dead-count** } command output

Item	Description
Radius server state detected internal is	Detection interval of the current RADIUS server.
Radius server state detected count is	Maximum number of consecutive packets that are not acknowledged by the RADIUS server.

19.2.11 display radius-server session-manage configuration

Function

The **display radius-server session-manage configuration** command displays session management configuration on the RADIUS server.

Format

display radius-server session-manage configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After session management is enabled using the **radius-server session-manage** command on the RADIUS server, you can run this command to view session management configuration.

Example

Display session management configuration on the RADIUS server.

```
<Huawei> display radius-server session-manage configuration
--------------------------------------------------------------------------------
Session Manage Enable : True    Session Manage AnyServer : False
--------------------------------------------------------------------------------
IP Address      VPN Instance                    Shared-key
--------------------------------------------------------------------------------
10.1.1.1        -                               ****************
--------------------------------------------------------------------------------
1 Radius session manage server(s) in total
```

Table 19-29 Description of the **display radius-server session-manage configuration** command output

Item	Description
Session Manage Enable	Whether session management is enabled: ● True: enabled ● False: disabled To set this parameter, run the **radius-server session-manage** command.
Session Manage AnyServer	Whether any RADIUS session management server is configured: ● True: configured ● False: not configured
IP Address	IP address of the RADIUS session management server.
VPN Instance	Name of the VPN instance bound to the RADIUS session management server.
Shared-key	Shared key of the RADIUS session management server.
Radius session manage server(s) in total	Number of the RADIUS session management servers.

19.2.12 display radius-server item

Function

The **display radius-server item** command shows the RADIUS server configuration.

Format

display radius-server item { **ip-address** { *ipv4-address* | *ipv6-address* } { **accounting** | **authentication** } | **template** *template-name* }

Parameters

Parameter	Description	Value
ip-address { *ipv4-address* | *ipv6-address* }	Specifies the IP address of the RADIUS server.	*ipv4-address*: The value is in dotted decimal notation. *ipv6-address*: The value is a 32-digit hexadecimal number.
accounting	Indicates the RADIUS accounting server.	-
authentication	Indicates the RADIUS authentication server.	-
template *template-name*	Specifies the RADIUS server template name.	The value must be an existing RADIUS server template name.

Views

ALL views

Default Level

3: Management level

Usage Guidelines

The **display radius-server item** command shows the RADIUS server configuration.

Example

Display the configuration of RADIUS server template **rds**.

```
<Huawei> display radius-server item template rds
 ---------------------------------------------------------------------------
  STState    = STState-up
  STChgTime  = -
  Type       = auth-server
  State      = state-up
  AlarmFlag  = false
  STUseNum   = 1
  IPAddress  = 192.168.30.1
  AlarmTimer = 0xffffffff
  Head       = 1057
  Tail       = 1311
  ProbeID    = 255
  Type       = acct-server
  State      = state-up
  AlarmFlag  = false
  STUseNum   = 1
  IPAddress  = 192.168.30.1
  AlarmTimer = 0xffffffff
  Head       = 1057
```

```
Tail       = 1311
ProbeID    = 255
-----------------------------------------------------------------------------
```

Table 19-30 Description of the **display radius-server item** template command output

Item	Description
STState	Status of the RADIUS server template. ● STState-up: indicates that the RADIUS server template is UP status. ● STState-down: indicates that the RADIUS server template is DOWN status.
STChgTime	Time when the RADIUS server template status changes.
Type	RADIUS server type: authentication or accounting server. ● auth-server: indicates authentication server. ● acct-server: indicates accounting server.
State	RADIUS server status. ● state-up: indicates that the RADIUS server is in UP status. ● state-down: indicates that the RADIUS server is in DOWN status. ● state-probe: indicates that the RADIUS server is in detection status.
AlarmFlag	Alarm flag. ● true: indicates that an alarm about status change has been sent. ● false: indicates that an alarm about status change is not sent.
STUseNum	RADIUS server template ID.
IPAddress	RADIUS server IP address.
AlarmTimer	ID of the alarm timer.
Head	Head pointer used to allocate the ID to RADIUS packets.
Tail	Tail pointer used to allocate the ID to RADIUS packets.
ProbeID	ID of probe packets.

 Copyright © Huawei Technologies Co., Ltd.

19.2.13 display snmp-agent trap feature-name radius all

Function

The **display snmp-agent trap feature-name radius all** command displays the status of all traps on the RDS module.

Format

display snmp-agent trap feature-name radius all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the RDS module, you can run this command to check the status of all traps on the RDS module. To enable the trap function for the RDS module, run the **snmp-agent trap enable feature-name radius** command.

Prerequisites

The SNMP function has been enabled on the device.

Example

Display the status of all traps on the RDS module.

```
<Huawei>display snmp-agent trap feature-name radius all
-----------------------------------------------------------------------------
Feature name: radius
Trap number : 4
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwRadiusAuthServerUp           off                     off
hwRadiusAuthServerDown          off                     off
hwRadiusAcctServerUp           off                     off
hwRadiusAcctServerDown          off                     off
```

Table 19-31 Description of the **display snmp-agent trap feature-name radius all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Name of a trap. Traps on the RDS module include: ● hwRadiusAuthServerUp: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is restored. ● hwRadiusAuthServerDown: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is interrupted. ● hwRadiusAcctServerUp: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is restored. ● hwRadiusAcctServerDown: The device sends a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is interrupted.
Default switch status	Default status of the trap function: ● on: The trap function is enabled by default. ● off: The trap function is disabled by default.
Current switch status	Trap status: ● on: The trap is enabled. ● off: The trap is disabled.

Related Topics

19.2.49 snmp-agent trap enable feature-name radius

19.2.14 radius-attribute check

Function

The **radius-attribute check** command enables the device to check the specified attributes in the received RADIUS Access-Accept packets.

The **undo radius-attribute check** command disables the device from checking the specified attributes in the received RADIUS Access-Accept packets.

By default, the device does not check whether a RADIUS Access-Accept packet contains the specified attributes.

 Copyright © Huawei Technologies Co., Ltd.

Format

radius-attribute check *attribute-name*

undo radius-attribute check [*attribute-name*]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of the RADIUS attribute. If this parameter is specified, the RADIUS Access-Accept packets are checked based on attribute names.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the **radius-attribute check** command is executed, the device checks whether the received RADIUS Access-Accept packets contain the specified attributes. If yes, the device considers that authentication was successful; if not, the device considers that authentication failed and discards the packet. For example, after the **radius-attribute check filter-id** command is executed, the device checks the filter-id attribute in the received RADIUS Access-Accept packets. If a RADIUS packet does not contain this attribute, authentication fails.

Precautions

- When you use the **undo radius-attribute check** command with parameters, the device checks the specified attributes in the RADIUS Access-Accept packets. When you use the **undo radius-attribute check** command without any parameter, the device does not check RADIUS Access-Accept packets.
- The **display radius-attribute** can display RADIUS attribute names.

Example

Check whether the RADIUS Access-Accept packets contain the framed-protocol attribute.

```
<Huawei> system-view
[Huawei] radius-server template test1
[Huawei-radius-test1] radius-attribute check framed-protocol
```

Related Topics

19.2.3 display radius-attribute

19.2.15 radius-attribute disable

Function

The **radius-attribute disable** command disables a RADIUS attribute.

The **undo radius-attribute disable** command enables a disabled RADIUS attribute.

By default, no RADIUS attribute is disabled.

Format

radius-attribute disable *attribute-name* { **receive** | **send** } *

undo radius-attribute disable [*attribute-name*]

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of a RADIUS attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
receive	Disables a RADIUS attribute for received packets.	-
send	Disables a RADIUS attribute for sent packets.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Generally, a RADIUS server connects to multiple network devices, which can be one vendor's devices or different vendors' devices. If some vendors' devices require

the RADIUS server to deliver an attribute to support a specified feature but other vendors' device do not support the delivered attribute, the RADIUS attribute may fail to be parsed.

The device may communicate with RADIUS servers of different vendors. Some RADIUS servers require the device to send some attributes but other RADIUS servers cannot process the attributes. Errors may occur.

The **radius-attribute disable** command disables RADIUS attributes on the device. You can configure the device to ignore incompatible attributes when receiving RADIUS packets to prevent parsing failures. You can also configure the device to disable RADIUS attributes when sending RADIUS packets. When the device sends RADIUS packets, it does not encapsulate the disabled RADIUS attributes in the RADIUS packets.

Prerequisites

The RADIUS attribute translation function has been enabled using the **19.2.26 radius-server attribute translate** command.

Precautions

Before disabling RADIUS attributes, run the **19.2.3 display radius-attribute** command to view the RADIUS attributes supported by the device.

Example

Disable the Frame-Route attribute in sent packets.

```
<Huawei> system-view
[Huawei] radius-server template test1
[Huawei-radius-test1] radius-server attribute translate
[Huawei-radius-test1] radius-attribute disable framed-route send
```

Related Topics

19.2.3 display radius-attribute

19.2.44 radius-server template

19.2.16 radius-attribute nas-ip

Function

The **radius-attribute nas-ip** command sets the NAS-IP-Address attribute in a RADIUS packet sent from an NAS.

The **undo radius-attribute nas-ip** command deletes the configured NAS-IP-Address attribute.

By default, the source IP address of the NAS is the NAS-IP-Address attribute value.

Format

radius-attribute nas-ip { *ip-address* | **ap-info** }

undo radius-attribute nas-ip [**ap-info**]

Parameters

Parameter	Description	Value
ip-address	Specifies the NAS-IP-Address attribute value in RADIUS packets sent by the device. In wireless scenarios, when a device functions as an AC, the IP address of the AC is specified as the NAS-IP-Address attribute value in RADIUS packets sent by the device.	The value is a valid unicast address in dotted decimal notation.
ap-info	The IP address of the AP is specified as the NAS-IP-Address attribute value in RADIUS packets sent by the device when the device functions as an AC in a wireless scenario.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A RADIUS server uses the NAS-IP-Address attributes in RADIUS packets sent by NASs to identify NASs. You can run the **radius-attribute nas-ip** command in the RADIUS server template view to set the NAS-IP-Address attribute.

When the RADIUS server interconnected with the device requires that the NAS-IP-Address attribute value is the IP address of the AP when the device functions as an AC in a wireless scenario, you need to run the **radius-attribute nas-ip ap-info** command.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If the RADIUS NAS-IP-Address attribute is set to an invalid IP address, the configuration fails and an error message is displayed.

Example

Set the RADIUS NAS-IP-Address attribute.

```
<Huawei> system-view
[Huawei] radius-server template temp1
[Huawei-radius-temp1] radius-attribute nas-ip 10.3.3.3
```

Related Topics

19.2.9 display radius-server configuration

19.2.17 radius-attribute nas-ipv6

Function

The **radius-attribute nas-ipv6** command sets the NAS-IPv6-Address attribute in a RADIUS packet sent from a network access server (NAS).

The **undo radius-attribute nas-ipv6** command deletes the configured NAS-IPv6-Address attribute.

By default, no NAS-IPv6-Address attribute is configured.

Format

radius-attribute nas-ipv6 *ipv6-address*

undo radius-attribute nas-ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies the NAS-IPv6-Address attribute in a RADIUS packet.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The RADIUS server uses IP addresses to identify different NASs. The NAS-IPv6-Address attribute in a RADIUS packet can be configured using the **radius-attribute nas-ipv6** command in the RADIUS template.

Prerequisites

A RADIUS server template has been created using the **radius-server template** command.

Precautions

If the RADIUS NAS-IP-Address attribute is set to an invalid IP address, the configuration fails and an error message is displayed.

Example

Set the RADIUS NAS-IPv6-Address attribute.

```
<Huawei> system-view
[Huawei] radius-server template temp1
[Huawei-radius-temp1] radius-attribute nas-ipv6 FC00::7
```

Related Topics

19.2.9 display radius-server configuration

19.2.18 radius-attribute set

Function

The **radius-attribute set** command modifies the RADIUS attributes.

The **undo radius-attribute set** command restores the default RADIUS attributes.

By default, values of the RADIUS attributes are not modified.

Format

radius-attribute set *attribute-name attribute-value* [**auth-type mac** | **user-type ipsession**]

undo radius-attribute set *attribute-name*

Parameters

Parameter	Description	Value
attribute-name	Specifies the name of the attribute to be modified.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
attribute-value	Indicates the value of the attribute to be modified.	The value of *attribute-value* is automatically displayed.
auth-type mac	Sets the user authentication mode to MAC address authentication. Only the Service-Type attribute supports this parameter.	-
user-type ipsession	Specifies the users with user type being IP session. Only the Service-Type attribute supports this parameter.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The RADIUS attribute values of different vendors are different. To ensure that Huawei device can successfully communicate with the devices of other vendors, run the **radius-attribute set** command to modify the RADIUS attribute values.

For example, the Huawei device uses Service-Type value 2 to indicate an authentication request from a common user by default, while a non-Huawei RADIUS server uses Service-Type value 1 to indicate an authentication request from a common user; you can run the **radius-attribute set service-type 1** command to change the Service-Type value on the device so that the device can communicate with the RADIUS server.

Precautions

- The **radius-attribute set** command can modify only the RADIUS attributes in the authentication or accounting request packets sent from a device to the RADIUS server, and cannot modify the RADIUS attributes in the packets sent from the RADIUS server to a device.

  If you run the **display radius-attribute** command to check the RADIUS attributes supported by a device and the **Auth Req** or **Acct Req** field in the command output displays 1, the RADIUS attributes supported by the device can be carried in the authentication or accounting request packets sent from the device to the RADIUS server.

 Copyright © Huawei Technologies Co., Ltd.

Among the RADIUS attributes that can be carried in the authentication or accounting packets sent from the device to the RADIUS server, you cannot run the **radius-attribute set** command to modify the following attributes: User-Password, NAS-IP-Address, NAS-IPv6-Address, CHAP-Password, CHAP-Challenge, EAP-Message, Framed-Interface-Id, Framed-IPv6-Prefix, and Message-Authenticator.

- The type of the attribute modified by the **radius-attribute set** command cannot be changed.
- The **radius-attribute set service-type** *attribute-value* { **auth-type mac** | **user-type ipsession** } command has a higher priority than the **radius-attribute set service-type** *attribute-value* command.
- A maximum of 8 attributes can be set in a RADIUS server template.
- If the value of the HW-Output-Committed-Information-Rate attribute is changed to 0, sent packets do not carry this attribute.

Example

Create the template **temp1** and set the Service-Type attribute value to 1.

```
<Huawei> system-view
[Huawei] radius-server template temp1
[Huawei-radius-temp1] radius-attribute set service-type 1
```

Related Topics

19.2.44 radius-server template

19.2.19 radius-attribute service-type with-authenonly-reauthen

Function

The **radius-attribute service-type with-authenonly-reauthen** command set the reauthentication mode to reauthentication only.

The **undo radius-attribute service-type with-authenonly-reauthen** command restores the reauthentication mode to reauthentication and reauthorization.

By default, this command is not configured and the reauthentication mode is reauthentication and reauthorization.

Format

radius-attribute service-type with-authenonly-reauthen

undo radius-attribute service-type with-authenonly-reauthen

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A large number of users are online at the same time and each user has a lot of authorization information. If the users need to be reauthenticated, the device delivers authorization information to each user after the authentication is successful. It is difficult for the device to process a lot of authorization information. As a result, users go offline due to authorization failures. After the **radius-attribute service-type with-authenonly-reauthen** command is run in the RADIUS server template view, the device only reauthenticates users during reauthentication, and does not redeliver authorization information, preventing users from going offline due to authorization failures.

Precautions

After this command is configured, users still use the original authorization information after being successfully reauthenticated even if the user authorization information changes.

This function takes effect after the Service-Type attribute on the RADIUS server is set to Authenticate Only.

Example

Set the reauthentication mode to reauthentication only.

```
<Huawei> system-view
[Huawei] radius-server template test
[Huawei-radius-test] radius-attribute service-type with-authenonly-reauthen
```

Related Topics

19.2.9 display radius-server configuration

19.2.20 radius-attribute translate

Function

The **radius-attribute translate** command configures a RADIUS attribute to be translated.

The **undo radius-attribute translate** command cancels the configuration.

By default, no RADIUS attribute is translated.

Format

radius-attribute translate *src-attribute-name dest-attribute-name* { **receive** | **send** | **access-accept** | **access-request** | **account-request** | **account-response** } *

radius-attribute translate extend vendor-specific *src-vendor-id src-sub-id dest-attribute-name* { **access-accept** | **account-response** } *

radius-attribute translate extend *src-attribute-name* **vendor-specific** *dest-vendor-id dest-sub-id* { **access-request** | **account-request** } *

undo radius-attribute translate [*src-attribute-name*]

undo radius-attribute translate extend *src-attribute-name*

undo radius-attribute translate extend vendor-specific *src-vendor-id src-sub-id*

Parameters

Parameter	Description	Value
src-attribute-name	Specifies the name of the source attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
dest-attribute-name	Specifies the name of the destination attribute.	The value is a string of 1 to 64 characters. After the name is entered, the system automatically associates the RADIUS attribute with the name.
receive	Translates RADIUS attributes for received packets.	-
send	Translates RADIUS attributes for sent packets.	-
access-request	Translates RADIUS attributes for Authentication Request packets.	-
account-request	Translates RADIUS attributes for Accounting Request packets.	-
access-accept	Translates RADIUS attributes for Authentication Accept packets.	-
account-response	Translates RADIUS attributes for Accounting Response packets.	-
extend	Translates extended RADIUS attributes.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vendor-specific *src-vendor-id src-sub-id*	Specifies the source extended attribute to be translated. ● *src-vendor-id*: The vendor ID in the extended RADIUS attributes needs to be translated. ● *src-sub-id*: The sub ID in the RADIUS attributes needs to be translated.	● The value of *src-vendor-id* is an integer ranging from 1 to 4294967295. ● The value of *src-sub-id* is an integer ranging from 1 to 255.
vendor-specific *dest-vendor-id dest-sub-id*	Specifies the destination extended attribute to be translated. ● *dest-vendor-id*: The vendor ID in the extended RADIUS attributes needs to be translated. ● *dest-sub-id*: The sub ID in the extended RADIUS attributes needs to be translated.	● The value of *dest-vendor-id* is an integer ranging from 1 to 4294967295. ● The value of *dest-sub-id* is an integer ranging from 1 to 255.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Currently, RADIUS servers of different vendors may support different RADIUS attributes and have vendor-specific RADIUS attributes. To communicate with different RADIUS servers, the device provides the RADIUS attribute translation function. After RADIUS attribute translation is enabled, the device can translate RADIUS attributes when sending or receiving packets.

RADIUS attribute translation is used in the following modes:

- Format translation for the same attribute

 Copyright © Huawei Technologies Co., Ltd.

This mode is widely applied. It solves the problem of compatibility because different users have different requirements for the format of a RADIUS attribute.

- Translation between different attributes

  This mode is used because different vendors have different implementations of RADIUS attributes.

  For example, the device delivers the priority of the administrator by using the Huawei proprietary attribute HW-Exec-Privilege (26-29), whereas another vendor's device delivers it by using the Login-service (15) attribute. When the device and the vendor's device use the same RADIUS server on a network, the user hopes that the device can deliver the priority of the administrator by using the Login-service (15) attribute. After the **radius-attribute translate** command is configured, the device automatically processes the Login-service attribute in the received RADIUS authentication response packet as the HW-Exec-Privilege attribute.

Prerequisites

RADIUS attribute translation has been enabled by using the **radius-server attribute translate** command.

Before configuring RADIUS attribute translation, run the **display radius-attribute** command to view the RADIUS attributes supported by the device.

Precautions

- When the device sends packets, if attribute A is to be translated to attribute B, the type of the encapsulated attribute is the same as that of attribute B but the attribute content and format are the same as those of attribute A.
- When the device receives packets, if attribute A is to be translated to attribute B, the device parses the received attribute A as attribute B.
- Three commands are available to translate RADIUS attributes:
  - To translate the attributes supported by the device to other attributes also supported by the device, run the **radius-attribute translate** command.
  - To translate the non-Huawei attributes not supported by the device to the attributes supported by the device, run the **radius-attribute translate extend vendor-specific** command.
  - To translate the attributes supported by the device to the non-Huawei attributes not supported by the device, run the **radius-attribute translate extend** command.
- The RADIUS attribute consists of Type, Length, and Value fields. A device can translate a non-Huawei RADIUS attribute (specified using the *src-sub-id* and *dest-sub-id* parameters) only when the length of the Type field in the RADIUS attribute is 1 byte.
- The device can translate the RADIUS attribute only when the type of the source RADIUS attribute is the same as that of the destination RADIUS attribute. For example, the types of NAS-Identifier and NAS-Port-Id attributes are string, and they can be translated into each other. The types of NAS-Identifier and NAS-Port attributes are string and integer respectively, they cannot be translated into each other.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the device to translate NAS-Identifier into NAS-Port-Id when sending RADIUS packets.

```
<Huawei> system-view
[Huawei] radius-server template temp1
[Huawei-radius-temp1] radius-server attribute translate
[Huawei-radius-temp1] radius-attribute translate nas-identifier nas-port-id send
```

Translate the Cisco No. 2 attribute (vendor ID 9) in Authentication Accept and Accounting Response packets to Huawei No. 155 extended attribute HW-URL-Flag.

```
<Huawei> system-view
[Huawei] radius-server template temp1
[Huawei-radius-temp1] radius-server attribute translate
[Huawei-radius-temp1] radius-attribute translate extend Vendor-Specific 9 2 HW-URL-Flag access-accept account-response
```

Translate the Huawei No. 153 extended attribute HW-Access-Type in Authentication Request and Accounting Request packets to Cisco No. 11 attribute.

```
<Huawei> system-view
[Huawei] radius-server template temp1
[Huawei-radius-temp1] radius-server attribute translate
[Huawei-radius-temp1] radius-attribute translate extend HW-Access-Type vendor-specific 9 11 access-request account-request
```

Related Topics

19.2.3 display radius-attribute

19.2.6 display radius-attribute translate

19.2.26 radius-server attribute translate

19.2.44 radius-server template

19.2.21 radius-server (aaa domain view)

Function

The **radius-server** command applies a RADIUS server template to a domain.

The **undo radius-server** command unbinds an RADIUS server template from a domain.

By default, the RADIUS server template **default** is bound to a configured domain and the domain **default**, and no RADIUS server template is bound to the domain **default_admin**.

Format

radius-server *template-name*

undo radius-server

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform RADIUS authentication and accounting for users in a domain, apply a RADIUS server template to the domain. A RADIUS server template takes effect only after the RADIUS server template is applied to a domain.

Prerequisites

A RADIUS server template has been created using the **19.2.44 radius-server template** command.

Example

Apply the RADIUS server template **template1** to the domain **radius1**.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] quit
[Huawei] aaa
[Huawei-aaa] domain radius1
[Huawei-aaa-domain-radius1] radius-server template1
```

Related Topics

19.2.9 display radius-server configuration

19.2.44 radius-server template

19.2.22 radius-server accounting

Function

The **radius-server accounting** command configures the RADIUS accounting server.

The **undo radius-server accounting** command deletes the configuration.

By default, no RADIUS accounting server is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

radius-server accounting *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server accounting *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

undo radius-server accounting [*ipv4-address* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

undo radius-server accounting [*ipv6-address* [*port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight**]]]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of a RADIUS accounting server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS accounting server is bound to.	The vpn-instance must already exist.
source loopback *interface-number*	Specifies the number of a loopback interface.	The loopback interface must already exist.
source ip-address *ipv4-address*	Specifies the source IPv4 address of a RADIUS accounting server.	The value is a valid unicast address in dotted decimal notation.
source ip-address *ipv6-address*	Specifies the source IPv6 address of a RADIUS accounting server. This address cannot be a VRRP6 virtual address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source vlanif *interface-number*	Specifies the IP address of a VLANIF interface as the source IP address. *interface-number* specifies the number of a VLANIF interface.	The VLANIF interface must exist.
weight *weight-value*	Specifies the weight of a RADIUS accounting server. When multiple servers are available, the device uses the server with the highest weight to perform accounting. If the servers have the same weights, the device uses the server configured first to perform accounting.	The value is an integer that ranges from 0 to 100.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform accounting for users, configure a RADIUS accounting server. The device communicates with a RADIUS accounting server to obtain accounting information, and performs accounting for users based on the accounting information. The device sends accounting packets to the RADIUS accounting server only after the IP address and port number of the RADIUS accounting server are specified in the RADIUS server template.

Precautions

The IP address of the primary accounting server must be different from the IP address of the secondary accounting server; otherwise, the configuration fails.

Example

Configure the primary RADIUS accounting server.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] radius-server template group1
[Huawei-radius-group1] radius-server accounting 10.163.155.12 1813
```

Configure the secondary RADIUS accounting server.

```
<Huawei> system-view
[Huawei] radius-server template group1
[Huawei-radius-group1] radius-server accounting 10.163.155.15 1813 weight 50
```

Related Topics

19.2.9 display radius-server configuration

19.2.23 radius-server accounting-stop-packet resend

Function

The **radius-server accounting-stop-packet resend** command enables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted each time.

The **undo radius-server accounting-stop-packet resend** command disables retransmission of accounting-stop packets.

By default, retransmission of accounting-stop packets is enabled, and the retransmission times is 3.

NOTE

The default settings are recommended. If accounting-stop packets need to be retransmitted many times, the RADIUS authentication performance of the switch will be affected and even cause a failure to send accounting-stop packets.

Format

radius-server accounting-stop-packet resend [*resend-times*]

undo radius-server accounting-stop-packet resend

Parameters

Parameter	Description	Value
resend-times	Specifies the number of accounting-stop packets that can be retransmitted each time.	The value is an integer that ranges from 0 to 300.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

When accounting-stop packets cannot be sent to the RADIUS server that is unreachable, you can run the **radius-server accounting-stop-packet resend** command to save the accounting-stop packets in the buffer and send them at the preset intervals until the number of allowed retransmission times is reached or the packets are sent successfully.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted each time to 50.

```
<Huawei> system-view
[Huawei] radius-server template test1
[Huawei-radius-test1] radius-server accounting-stop-packet resend 50
```

Related Topics

19.2.9 display radius-server configuration

19.2.24 radius-server algorithm

Function

The **radius-server algorithm** command configures the algorithm for selecting RADIUS servers.

The **undo radius-server algorithm** command restores the default algorithm for selecting RADIUS servers.

By default, the algorithm for selecting RADIUS servers is primary/secondary.

Format

radius-server algorithm { **loading-share** | **master-backup** } [**based-user**]

undo radius-server algorithm

Parameters

Parameter	Description	Value
loading-share	Sets the algorithm for selecting RADIUS servers to load balancing.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
based-user	Sets the algorithm for selecting RADIUS servers to the single user-based algorithm. If this parameter is not specified, the algorithm for selecting RADIUS servers is the packet-based algorithm.	-
master-backup	Sets the algorithm for selecting RADIUS servers to primary/secondary.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When two or more than two RADIUS servers are available, you can use the **radius-server algorithm** command to set the algorithm for selecting RADIUS servers.

- When **master-backup** is specified, the weight is used to determine the primary and secondary RADIUS authentication or accounting servers. The server with a larger weight value is the primary server. If devices have the same weight, the server that was first configured is the primary server.
- When **loading-share** is specified, the device sends a packet to a server according to the weights configured on servers. For example, if the weights of RADIUS server A, RADIUS server B, and RADIUS server C are 80, 80, and 40 respectively, the probabilities of sending packets to RADIUS server A, RADIUS server B, and RADIUS server C are as follows:
  - RADIUS server A: 80/(80 + 80 + 40) = 40%
  - RADIUS server B: 80/(80 + 80 + 40) = 40%
  - RADIUS server C: 40/(80 + 80 + 40) = 20%

If the algorithm for selecting RADIUS servers is set to the single user-based algorithm, authentication server information is saved in the authentication phase, and the device preferentially sends an accounting request to the accounting server in the accounting phase when the accounting server is the same as the authentication server. If the algorithm for selecting RADIUS servers is set to the packet-based algorithm, authentication server information is not saved in the

 Copyright © Huawei Technologies Co., Ltd.

authentication phase, and the accounting server is reselected in the accounting phase, which may result in that authentication and accounting for a user is not performed on the same server.

Precautions

If you run the **radius-server algorithm** command multiple times in the same RADIUS server template view, only the latest configuration takes effect.

Example

Set the algorithm for selecting RADIUS servers to load balancing.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server algorithm loading-share
```

Related Topics

19.2.9 display radius-server configuration

19.2.25 radius-server attribute message-authenticator access-request

Function

The **radius-server attribute message-authenticator access-request** command carries the Message-Authenticator attribute in RADIUS authentication packets sent by the device.

The **undo radius-server attribute message-authenticator access-request** command cancels the Message-Authenticator attribute from RADIUS authentication packets sent by the device.

By default, RADIUS authentication packets do not carry the Message-Authenticator attribute.

Format

radius-server attribute message-authenticator access-request

undo radius-server attribute message-authenticator access-request

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The Message-Authenticator attribute is used to identify and verify authentication packets to prevent invalid packets.

NOTE

- This command is used when the PAP or CHAP authentication is enabled.
- When EAP authentication is enabled, RADIUS packets contain the Message-Authenticator attribute by default. You do not need to run this command.

Example

Configure the Message-Authenticator attribute to RADIUS authentication packets.

```
<Huawei> system-view
[Huawei] radius-server template test1
[Huawei-radius-test1] radius-server attribute message-authenticator access-request
```

19.2.26 radius-server attribute translate

Function

The **radius-server attribute translate** command enables RADIUS attribute translation.

The **undo radius-server attribute translate** command disables RADIUS attribute translation.

By default, RADIUS attribute translation is disabled.

Format

radius-server attribute translate

undo radius-server attribute translate

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Currently, RADIUS servers of different vendors may support different RADIUS attributes and have vendor-specific RADIUS attributes. To communicate with

different RADIUS servers, the device provides the RADIUS attribute translation function. After RADIUS attribute translation is enabled, the device can translate RADIUS attributes when sending or receiving packets.

Follow-up Procedure

After RADIUS attribute translation is enabled, perform either of the following operations to make the function to take effect:

- Run the **19.2.20 radius-attribute translate** command to specify the RADIUS attributes that you want to translate.
- Run the **19.2.15 radius-attribute disable** command to specify the RADIUS attributes that you do not want to translate.

Example

Enable RADIUS attribute translation.

```
<Huawei> system-view
[Huawei] radius-server template test1
[Huawei-radius-test1] radius-server attribute translate
```

Related Topics

19.2.20 radius-attribute translate

19.2.44 radius-server template

19.2.27 radius-server authentication

Function

The **radius-server authentication** command configures a RADIUS authentication server.

The **undo radius-server authentication** command deletes the configured RADIUS authentication server.

By default, no RADIUS authentication server is specified.

Format

radius-server authentication *ipv4-address port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

radius-server authentication *ipv6-address port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight** *weight-value*] *

undo radius-server authentication [*ipv4-address* [*port* [**vpn-instance** *vpn-instance-name* | **source** { **loopback** *interface-number* | **ip-address** *ipv4-address* | **vlanif** *interface-number* } | **weight**] *]]

undo radius-server authentication [*ipv6-address* [*port* [**source** { **loopback** *interface-number* | **ip-address** *ipv6-address* | **vlanif** *interface-number* } | **weight**]]]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of a RADIUS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of a RADIUS authentication server.	The value is an integer that ranges from 1 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authentication server is bound to.	The VPN instance must already exist.
source loopback *interface-number*	Specifies the IP address of the loopback interface taken as the source IP address. *interface-number* specifies the number of a loopback interface.	The loopback interface must already exist.
source ip-address *ipv4-address*	Specifies the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv4 address of the outbound interface is used as the source IPv4 address in RADIUS packets sent from the device to a RADIUS authentication server.	The value is a valid unicast address in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source ip-address *ipv6-address*	Specifies the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. If this parameter is not specified, the IPv6 address of the outbound interface is used as the source IPv6 address in RADIUS packets sent from the device to a RADIUS authentication server. This address cannot be a VRRP6 virtual address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source vlanif *interface-number*	Specifies the IP address of a VLANIF interface as the source IP address. *interface-number* specifies the number of a VLANIF interface.	The VLANIF interface must exist.
weight *weight-value*	Specifies the weight of a RADIUS authentication server. When multiple servers are available, the device uses the server with the highest weight to perform authentication. If the servers have the same weights, the device uses the server configured first to perform authentication.	The value is an integer that ranges from 0 to 100. The default value is 80.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

To perform RADIUS authentication, configure a RADIUS authentication server in a RADIUS server template. The device uses the RADIUS protocol to communicate

with a RADIUS authentication server to obtain authentication information, and authenticates users based on the authentication information. The device sends authentication packets to the RADIUS authentication server only after the IP address and port number of the RADIUS authentication server are specified in the RADIUS server template.

When the **radius-server algorithm master-backup** command has been executed to specify the master/backup algorithm on the RADIUS server and both the primary and secondary authentication servers are configured, the device sends an authentication request packet to the secondary authentication server in either of the following situations:

- The primary authentication server does not send an authentication response packet.
- The authentication request packet retransmission count reaches the maximum.

Example

Configure the IP address of the primary RADIUS authentication server to 10.163.155.13 and the port number to 1812.

```
<Huawei> system-view
[Huawei] radius-server template group1
[Huawei-radius-group1] radius-server authentication 10.163.155.13 1812
```

Configure the IP address of the secondary RADIUS authentication server to 10.163.155.15, the port number to 1812 and the weigh to 50.

```
<Huawei> system-view
[Huawei] radius-server template group1
[Huawei-radius-group1] radius-server authentication 10.163.155.15 1812 weight 50
```

Related Topics

19.2.9 display radius-server configuration

19.2.28 radius-server authorization

Function

The **radius-server authorization** command configures the RADIUS authorization server.

The **undo radius-server authorization** command deletes the configured RADIUS authorization server.

By default, no RADIUS authorization server is configured.

Format

radius-server authorization *ip-address* [**vpn-instance** *vpn-instance-name*] { **server-group** *group-name* **shared-key cipher** *key-string* | **shared-key cipher** *key-string* [**server-group** *group-name*] } [**ack-reserved-interval** *interval*] [**protect enable**]

undo radius-server authorization { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] }

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of a RADIUS authorization server.	The value is a unicast address in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the RADIUS authorization server is bound to.	The value is a string of 1 to 31 case-sensitive characters.
server-group *group-name*	Specifies the name of a RADIUS group corresponding to a RADIUS server template.	The value is a string of 1 to 32 characters, including letters (case-sensitive), numerals (0 to 9), punctuation mark (.), dash (-), and underline (_). The value cannot be - or --.
shared-key cipher *key-string*	Specifies the shared key of a RADIUS server.	The value is a case-sensitive character string without spaces or question marks (?). The *key-string* may be a plain text consisting of 1 to 128 characters or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.
ack-reserved-interval *interval*	Specifies the duration for retaining a RADIUS authorization response packet.	The value is an integer that ranges from 0 to 300, in seconds. By default, the value is 0s.
protect enable	Enables the security hardening function.	-
all	Deletes all RADIUS authorization servers.	-

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

An independent RADIUS authorization server can be used to authorize online users. RADIUS provides two authorization methods: Change of Authorization (CoA) and Disconnect Message (DM).

- CoA: After a user is successfully authenticated, you can modify the rights of the online user through the RADIUS authorization server. For example, a VLAN ID can be delivered to access users of a certain department through CoA packets, so that they belong to the same VLAN no matter which interfaces they connect to.
- DM: The administrator can forcibly disconnect a user through the RADIUS authorization server.

After the parameters such as IP address and shared key are configured for the RADIUS authorization server, the device can receive authorization requests from the server and grant rights to users according to the authorization information. After authorization is complete, the device returns authorization response packets carrying the results to the server.

After the security hardening function is enabled by specifying the **protect enable** parameter, the following occurs:

- When a CoA or DM request packet carries the Message-Authenticator attribute, the device checks the Message-Authenticator attribute. If the check fails, the device discards the request packet and does not respond the packet. If the check succeeds, the device sends a CoA or DM response packet (ACK or NAK) that carries the Message-Authenticator attribute.
- When a CoA or DM request packet does not carry the Message-Authenticator attribute, the device does not check the attribute and sends a CoA or DM response packet (ACK or NAK) that does not carry the Message-Authenticator attribute.

NOTE

When a CoA or DM request packet carries the Message-Authenticator attribute, if the **radius-attribute disable message-authenticator receive** command is configured, the device does not check the attribute and sends a response packet that does not carry the Message-Authenticator attribute; if the **radius-attribute disable message-authenticator send** command is configured, the device sends a response packet that does not carry the Message-Authenticator attribute even if the attribute check succeeds.

Precautions

To improve security, it is recommended that the password contains at least three types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 16 characters.

Example

Specify a RADIUS authorization server.

```
<Huawei> system-view
[Huawei] radius-server authorization 10.1.1.116 shared-key cipher Huawei@2012
```

Related Topics

19.2.8 display radius-server authorization configuration
19.2.44 radius-server template

19.2.29 radius-server authorization attribute-decode-sameastemplate

Function

The **radius-server authorization attribute-decode-sameastemplate** command configures the device to parse RADIUS dynamic authorization packet attributes based on the configuration in RADIUS server template.

The **undo radius-server authorization attribute-decode-sameastemplate** command restores the default method of parsing RADIUS authorization packet attributes.

By default, the device parses RADIUS dynamic authorization packet attributes based on global configuration.

Format

radius-server authorization attribute-decode-sameastemplate

undo radius-server authorization attribute-decode-sameastemplate

Parameters

None.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device parses the MAC address in the Calling-Station-Id attribute in RADIUS dynamic authorization packets. By default, the MAC address format that can be parsed is configured using the **radius-server authorization calling-station-id decode-mac-format** command in the system view. When the device is connected to multiple RADIUS servers, the MAC address formats are different in the Calling-Station-Id attribute in dynamic authorization packets sent by different RADIUS servers. In this case, the MAC address may fail to be parsed if the same parse mode is used, resulting in that the device fails to be connected to some RADIUS servers. You can run the **radius-server authorization attribute-decode-sameastemplate** command to configure the device to parse RADIUS dynamic authorization packet attributes based on the Calling-Station-Id attribute

 Copyright © Huawei Technologies Co., Ltd.

encapsulation mode configured in each RADIUS server template, making the device be successfully connected to multiple RADIUS servers.

Prerequisites

This function is used to make the Calling-Station-Id attribute parse mode the same as the Calling-Station-Id attribute encapsulation mode configured in RADIUS server template. Therefore, make sure that the following steps have been performed before using this function.

1. The **calling-station-id mac-format** command has been run in the RADIUS server template view to configure the encapsulation mode of the MAC address in the Calling-Station-Id attribute.
2. The **radius-server authorization** command has been run in the system view to configure the authorization server to use the RADIUS server template **server-group**.

NOTE

If the RADIUS server template used by the authorization server is not specified, this function cannot be implemented on a device. You can run the **radius-server authorization calling-station-id decode-mac-format** command in the system view to configure the Calling-Station-Id attribute parse mode.

Precautions

The configuration in a RADIUS server template has a higher priority than the global configuration.

Example

Configure the RADIUS authorization server to parse attributes depending on the configuration in a RADIUS template.

```
<Huawei> system-view
[Huawei] radius-server authorization attribute-decode-sameastemplate
```

19.2.30 radius-server authorization attribute-encode-sameastemplate

Function

The **radius-server authorization attribute-encode-sameastemplate** command configures a device to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template.

The **undo radius-server authorization attribute-encode-sameastemplate** command restores the default setting.

By default, a device is not configured to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template.

Format

radius-server authorization attribute-encode-sameastemplate

undo radius-server authorization attribute-encode-sameastemplate

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The attribute match check function is configured on the RADIUS servers of some vendors. The attribute match check succeeds and the RADIUS server successfully interconnects with a device to implement dynamic authorization or offline operations only when the attribute encapsulation formats in the COA or DM Response packet received by the RADIUS server are the same as those parsed from the RADIUS authentication Response packets. The RADIUS server encapsulates the attributes parsed from the RADIUS Response packet based on the configurations in the RADIUS server template. To ensure that the attribute formats in the COA or DM Response packet are the same as those parsed by the RADIUS server from the RADIUS packet, you can run the **radius-server authorization attribute-encode-sameastemplate** command to configure the device to encapsulate attributes in the COA or DM Response packet based on the configurations in the RADIUS server template, so that the device is successfully interconnected with the RADIUS server.

Attributes whose encapsulation formats need to be configured in the COA or DM Response packet include Calling-Station-Id (31), NAS-IP-Address (4), and User-Name (1).

Precautions

- This function is used to configure the encapsulation modes of the Calling-Station-Id (31), NAS-IP-Address (4), and User-Name (1) attributes in the COA or DM Response packet to be the same as those configured in the RADIUS server template. Therefore, perform the following steps before using this function.
  a. Configure the encapsulation modes of attributes in the RADIUS server template view.
     - Run the **calling-station-id mac-format** command to configure the encapsulation mode of the MAC address in the Calling-Station-Id attribute.
     - Run the **19.2.16 radius-attribute nas-ip** command to configure the NAS-IP-Address attribute in a RADIUS packet sent from an NAS.
     - Run the **19.2.47 radius-server user-name domain-included** command to configure whether the user name carried in the RADIUS packet contains a domain name.

 Copyright © Huawei Technologies Co., Ltd.

b. Run the **radius-server authorization** command in the system view to configure the authorization server to use the RADIUS server template **server-group**.

- After this function is configured, the priority of the NAS IP address in the NAS-IP-Address (4) attribute is as follows: NAS IP address configured in the RADIUS server template>source IP address configured on the accounting server>source IP address configured on the authentication server>destination IP address of the Request packet
- If the **radius-server authorization attribute-encode-sameastemplate** command is not configured, no RADIUS server template is bound to the authorization server, or no attribute format configuration exists in the RADIUS server template, the formats of COA or DM response packets are as follows:
  - MAC address in the Calling-Station-Id (31) attribute: The MAC address is encapsulated in the default format XXXXXXXXXXXX.
  - NAS IP address in the NAS-IP-Address (4) attribute: destination IP address in the Request packet
  - User name in the User-Name (1) attribute: The user name in the Request packet is used.

Example

Configure the RADIUS authorization server to parse attributes based on the configurations in the RADIUS server template.

```
<Huawei> system-view
[Huawei] radius-server authorization attribute-encode-sameastemplate
```

19.2.31 radius-server authorization calling-station-id decode-mac-format

Function

The **radius-server authorization calling-station-id decode-mac-format** command sets the format of MAC address that can be parsed by a device in the calling-station-id (Type 31) attribute carried in RADIUS authorization packets.

The **undo radius-server authorization calling-station-id decode-mac-format** command restores the default format of the MAC address in the calling-station-id (Type 31) attribute.

By default, the MAC address format in the calling-station-id attribute carried in RADIUS dynamic authorization packets is xxxxxxxxxxxx, in lowercase.

Format

radius-server authorization calling-station-id decode-mac-format { **bin** | **ascii** { **unformatted** | { **dot-split** | **hyphen-split** } [**common** | **compress**] } }

undo radius-server authorization calling-station-id decode-mac-format

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
bin	Indicates that the MAC address in the calling-station-id attribute uses the binary format.	-
ascii	Indicates that the MAC address in the calling-station-id attribute uses the ASCII format.	-
unformatted	Indicates that no separator is used in the MAC address in the calling-station-id field.	-
dot-split	Indicates that dots are used as the separators in MAC address.	-
hyphen-split	Indicates that the hyphens are used as the separators in MAC address.	-
common	Indicates that the MAC address in the calling-station-id attribute uses the "xx**separator**xx**separator**xx**separator**xx**separator**xx**separator**xx" format.	-
compress	Indicates that the MAC address in the calling-station-id attribute uses the "xxxx**separator**xxxx**separator**xxxx" format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the MAC address format in the calling-station-id attribute carried in RADIUS dynamic authorization packets is xxxxxxxxxxxx. If the MAC address format in the calling-station-id attribute sent by the RADIUS server is not the default format used on the device, run the **radius-server authorization calling-station-id decode-mac-format** command to change the MAC address format on the device.

When a device connects to multiple RADIUS servers, the RADIUS servers may send MAC addresses in different formats in the calling-station-id attribute to the device. You need to run the **radius-server authorization attribute-decode-sameastemplate** command to configure the device to parse the RADIUS authorization packet attributes based on the configuration in RADIUS server template, so that the device can work with these RADIUS servers.

Precautions

The configuration in a RADIUS server template has a higher priority than the global configuration.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the format of MAC address that can be parsed by the device in the calling-station-id attribute to binary.

```
<Huawei> system-view
[Huawei] radius-server authorization calling-station-id decode-mac-format bin
```

19.2.32 radius-server authorization match-type

Function

The **radius-server authorization match-type** command configures the method used by a device to perform a match check between the RADIUS attribute in the received COA or DM Request packet and user information on the device.

The **undo radius-server authorization match-type** command restores the default setting.

By default, a device performs a match check between the RADIUS attribute in the received COA or DM Request packet and user information on the device using the **any** method, namely, the device performs a match check between a selected attribute in the Request packet and user information on the device.

Format

radius-server authorization match-type { **any** | **all** }

undo radius-server authorization match-type

Parameters

Parameter	Description	Value
any	Indicates that the device performs a match check between a specified attribute and user information on the device.	-
all	Indicates that the device performs a match check between all attributes and user information on the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A device performs a match check between the RADIUS attribute in the COA or DM Request packet and user information on the device to identify users in the following two methods:

- **any** method: The device performs a match check between an attribute and user information on the device. The priority of identifying the RADIUS attributes used by the users is as follows: Acct-Session-ID (4)>Calling-Station-Id (31)>Framed-IP-Address (8) The device searches for the attributes in the Request packet based on the priority, and performs a match check between the first found attribute and user information on the device. If the attribute is successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.
- **all** method: The device performs a match check between all attributes and user information on the device. The device identifies the following RADIUS attributes used by the users: Acct-Session-ID (4), Calling-Station-Id (31), Framed-IP-Address (8), and User-Name (1) The device performs a match check between all the preceding attributes in the Request packet and user information on the device. If all the preceding attributes are successfully matched, the device responds with an ACK packet; otherwise, the device responds with a NAK packet.

Precautions

When the RADIUS attribute translation function is configured in the RADIUS template using the **19.2.20 radius-attribute translate** command, the match will fail.

Example

Configure a device to perform a match check between all RADIUS attributes in the received COA or DM Request packet and user information on the device.

```
<Huawei> system-view
[Huawei] radius-server authorization match-type all
```

19.2.33 radius-server dead-interval dead-count

Function

The **radius-server dead-interval dead-count** command configures the RADIUS server detection interval and maximum number of consecutive unacknowledged packets in each detection interval.

The **undo radius-server dead-interval dead-count** command restores the default settings.

Format

radius-server { **dead-interval** *dead-interval* | **dead-count** *dead-count* }

undo radius-server { **dead-interval** | **dead-count** }

Parameters

Parameter	Description	Value
dead-interval	Specifies the RADIUS server detection interval.	The value is an integer that ranges from 1 to 300, in seconds.
dead-count	Specifies the maximum number of consecutive unacknowledged packets in each detection interval.	The value is an integer that ranges from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the system starts, the RADIUS server status detection timer runs. The device sets the RADIUS server status to Up. When the device sends a RADIUS request packet to the RADIUS server, if the conditions for setting the RADIUS server status to Down are met, the device sets the RADIUS server status to Down; if the conditions are not met, the RADIUS server status remains to be Up.

If multiple RADIUS servers are configured, some servers are Up and the other servers are Down, and the device receives an authentication request packet from a user, the device retransmits the packet to a RADIUS server in Up status based on the server priority and detects the actual status of the server. The following describes the process in which a device detects the status of a RADIUS server.

1. If the device receives no response packet from the RADIUS server and the number of times that the device receives no response packet after sending an authentication request packet is greater than or equal to the maximum number of consecutive unacknowledged packets within the detection interval, the device records a communication interruption.
2. If the device records two consecutive communication interruptions with one RADIUS server, the device considers that the RADIUS server is unavailable and the condition for the device to set the status of the RADIUS server to Down is met.

   NOTE

   If the first connection attempt fails but the second one succeeds, the device deletes the recorded communication interruption with the RADIUS server.
3. When sending an authentication request packet to the RADIUS server again, the device sets the server status to Down. If a response packet is received

from the server, the device restores the server status to Up. If no response packet is received from the server and the number of retransmission times is not reached, the device sends an authentication request packet to the server again. If the server still does not respond, the device no longer sends any authentication request packet to the server.

If the device sets the status of all servers that are originally set to Up to Down after the device completes the server status detection based on the preceding detection process or these servers do not respond to the authentication request packets sent from the device, the device sends an authentication request packet to a RADIUS server that is originally set to be Down based on the server priority to detect the server status. (In the original mechanism, the device does not send authentication request packets to the RADIUS servers that are originally set to be Down.)

Precautions

- If the device has reported a RADIUS server Up alarm and needs to report a RADIUS server Down alarm, the device will send the Down alarm 10 seconds after the Up alarm is sent, even if the RADIUS server Down detection interval is shorter than 10 seconds (for example, the value of *dead-interval* is set to 4 seconds, and the RADIUS server Down detection interval is 8 seconds). This function prevents frequent alarm sending.
- To rapidly detect whether the RADIUS server goes Down, when there are a small number of users, smaller values are recommended for the detection interval and maximum number.

Example

Set the RADIUS server detection interval to 10 seconds and maximum number of consecutive unacknowledged packets in each detection interval to 2.

```
<Huawei> system-view
[Huawei] radius-server dead-interval 10
[Huawei] radius-server dead-count 2
```

19.2.34 radius-server detect-server interval

Function

The **radius-server detect-server interval** command configures an automatic detection interval for RADIUS servers.

The **undo radius-server detect-server interval** command restores the default settings.

The default automatic detection interval is 60 seconds.

Format

radius-server detect-server interval *interval*

undo radius-server detect-server interval

Parameters

Parameter	Description	Value
interval	Specifies the automatic detection interval for RADIUS servers.	The value is an integer that ranges from 5 to 3600, in seconds.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After the automatic detection function is enabled using the **radius-server testuser** command, you can run the **radius-server detect-server interval** command to adjust the automatic detection interval for RADIUS servers.

Example

Set the automatic detection interval for RADIUS servers to 100 seconds in the RADIUS server template **acs**.

```
<Huawei> system-view
[Huawei] radius-server template acs
[Huawei-radius-acs] radius-server detect-server interval 100
```

19.2.35 radius-server format-attribute

Function

The **radius-server format-attribute** command configures the format of the NAS-Port attribute.

The **undo radius-server format-attribute** command deletes the configured attribute format.

By default, the format of the NAS-Port attribute is **new**.

Format

radius-server format-attribute nas-port *nas-port-sting*

undo radius-server format-attribute nas-port

Parameters

Parameter	Description	Value
nas-port *nas-port-sting*	Specifies the format of the NAS-Port attribute. ● The keywords **s**, **t**, **p**, **o**, and **i** stand for slot, subslot, port, out-vlan (qinqvlan)/vpi, and vlan (user-vlan)/vci respectively. The keywords **n** and **z** are used as paddings. The keyword **n** indicates 1 and the keyword **z** indicates 0. ● The keywords **s**, **t**, **p**, **o**, and **i** must be followed by numbers, and the numbers must range from 1 to 32. The keywords **s**, **t**, **p**, **o**, and **i** can be present in the format string only once. ● The keywords **s**, **t**, **p**, **o**, **i**, **n**, and **z** must range from 1 to 9. ● **n** and **z** can be present multiple times at any position. They are followed by numbers. For example, **n12** indicates that this position is filled by twelve 1s, and **z12** indicates that this position is filled by twelve 0s. ● The character string must contain 32 bits. ● The format string must start with **s**, **t**, **p**, **o**, **i**, **n**, or **z** and end with a number. ● If no VLAN exists, you can add **n** or **z** before **o** or **i** to indicate whether this position	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	is filled by 0s or 1s. That is, **n** and **z** can be followed by numbers or **o/i** in this case, and the numbers must range from 1 to 32. ● To specify the format string, determine the interface type, and then determine the encapsulation type of the interface. If the format string does not contain **o** or **i**, the NAS-Port attribute does not contain the QinQ VLAN or user VLAN field. If the format string contains **o** or **i** but no outer VLAN exists, the outer VLAN field is filled by 0s. If **n** is added before **o** or **i**, this field is filled by 1s when no outer VLAN or inner VLAN exists.	

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The NAS port format affects the information about the physical port. The NAS port format can be used by the RADIUS server to process services, such as binding the user name and port. This attribute is developed by Huawei, which is used to ensure connectivity and service cooperation among Huawei devices.

If the **radius-server nas-port-format** command sets the format of the NAS-Port attribute to **new** (the default format is **new**), the device will check whether the **radius-server format-attribute nas-port** command configuration exists. If yes, the device will assemble the NAS-Port attribute in the format configured by the **radius-server format-attribute nas-port** command. If no, the device will

assemble the NAS-Port attribute in the **new** format. If the **radius-server nas-port-format** command sets the format of the NAS-Port attribute to **old**, the device will assemble the NAS-Port attribute in the **old** format, regardless of whether the **radius-server format-attribute nas-port** command configuration exists.

Example

Configure the format of the NAS-Port attribute to s2t2p6no10ni12. That is, the NAS-Port attribute consists of a 2-bit slot field, a 2-bit subslot field, a 6-bit port field, a 10-bit outer VLAN field, and a 12-bit inner VLAN field. If the outer VLAN does not exist, this field is filled by ten 1s. If the inner VLAN does not exist, this field is filled by twelve 1s. Therefore, the NAS-port attribute contains 32 bits.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server format-attribute nas-port s2t2p6no10ni12
```

Related Topics

19.2.38 radius-server nas-port-format

19.2.36 radius-server hw-ap-info-format include-ap-ip

Function

The **radius-server hw-ap-info-format include-ap-ip** command configures the AP's IP address carried in Huawei extended attribute HW-AP-Information.

The **undo radius-server hw-ap-info-format** command restores the default setting.

By default, Huawei extended attribute HW-AP-Information does not carry AP's IP address.

Format

radius-server hw-ap-info-format include-ap-ip

undo radius-server hw-ap-info-format

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

RADIUS is a fully extensible protocol. Device vendors can expand the No. 26 attribute defined in the protocol to implement functions not supported by

 Copyright © Huawei Technologies Co., Ltd.

standard RADIUS attributes. Huawei defines the No. 141 sub-attribute (HW-AP-Information) in the No. 26 attribute to indicate AP information, including the MAC and IP addresses of an AP. The HW-AP-Information attribute is carried in the authentication or accounting request packet send by a device, so that the RADIUS server can use the AP's MAC and IP addresses as the filter criterion to select a policy template to be delivered.

When an AP's IP address is carried in the HW-AP-Information attribute, the encapsulation format of the attribute is AP-MAC AP-IP.

Example

#Configure the AP's IP address in Huawei extended attribute HW-AP-Information.

```
<Huawei> system-view
[Huawei] radius-server template huawei
[Huawei-radius-huawei] radius-server hw-ap-info-format include-ap-ip
```

19.2.37 radius-server nas-identifier-format

Function

The **radius-server nas-identifier-format** command sets the encapsulation format of the NAS-Identifier attribute.

The **undo radius-server nas-identifier-format** command restores the default encapsulation format of the NAS-Identifier attribute.

By default, the NAS-Identifier attribute encapsulation format is the device's hostname.

Format

radius-server nas-identifier-format { **hostname** | **vlan-id** | **ap-info** }

undo radius-server nas-identifier-format

Parameters

Parameter	Description	Value
hostname	Sets the encapsulation format of NAS-Identifier to a device's host name.	-
vlan-id	Sets the encapsulation format of NAS-Identifier to a user's VLAN ID.	-
ap-info	Sets the encapsulation format of NAS-Identifier to the AP's MAC address.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

A RADIUS server uses the NAS-Identifier attributes to identify NASs. The NASs also use the NAS-Identifier attributes carried in the sent RADIUS packets to identify themselves.

When the RADIUS server interconnected with the device requires that the NAS-Identifier attribute value is the MAC address of the AP when the device functions as an AC in a wireless scenario, you need to run the **radius-server nas-identifier-format ap-info** command.

Example

Set the NAS-Identifier encapsulation format to VLAN ID.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server nas-identifier-format vlan-id
```

19.2.38 radius-server nas-port-format

Function

The **radius-server nas-port-format** command sets the format of the NAS port attribute.

The **undo radius-server nas-port-format** command restores the default format of the NAS port attribute.

By default, the new NAS port format is used.

Format

radius-server nas-port-format { **new** | **old** }

undo radius-server nas-port-format

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
new	Uses the new format of an NAS port. The new format of the NAS port attribute is slot number (8 bits) + subslot number (4 bits) + port number (8 bits) + VLAN ID (12 bits).	-
old	Uses the old format of an NAS port. The old format of the NAS port attribute is slot number (12 bits) + port number (8 bits) + VLAN ID (12 bits).	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NAS port format affects the information about the physical port. The NAS port format can be used by the RADIUS server to process services, such as binding the user name and port. This attribute is developed by Huawei, which is used to ensure connectivity and service cooperation among Huawei devices.

Precautions

The difference between the two NAS port formats lies in the physical ports connected to Ethernet access users.

- The new format of the NAS port attribute is slot number (8 bits) + subslot number (4 bits) + port number (8 bits) + VLAN ID (12 bits).
- The old format of the NAS port attribute is slot number (12 bits) + port number (8 bits) + VLAN ID (12 bits).

The format of the NAS port attribute for Asymmetric Digital Subscriber Line (ADSL) access users is slot number (4 bits) + subslot number (2 bits) + port number (2 bits) + VPI (8 bits) + VCI (16 bits). This format is not affected by the command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the format of the NAS port attribute to **new**.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server nas-port-format new
```

19.2.39 radius-server nas-port-id-format

Function

The **radius-server nas-port-id-format** command sets the format of the NAS port ID attribute.

The **undo radius-server nas-port-id-format** command restores the default format of the NAS port ID attribute.

By default, the new format of the NAS port ID attribute is used.

Format

radius-server nas-port-id-format { **new** | **old** | **vendor** *vendor-id* }

undo radius-server nas-port-id-format

Parameters

Parameter	Description	Value
new	Uses the new format of the NAS port ID.	-
client-option82	Uses the content of the Option82 field as the format of the NAS-Port-Id attribute.	-
old	Uses the old format of the NAS port ID.	-

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NAS port format and the NAS port ID format are developed by Huawei, which are used to ensure connectivity and service cooperation among Huawei devices.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When **new** is specified:

- For Ethernet access users, the NAS port ID format is slot=xx; subslot=xx; port=xxx; VLAN ID=xxxx, in which *slot* ranges from 0 to 15, *subslot* from 0 to 15, *port* from 0 to 255, and *VLAN ID* from 1 to 4094.
- For ADSL access users, the NAS port ID format is slot=xx; subslot=x; port=x;VPI=xxx; VCI=xxxxx, in which *slot* ranges from 0 to 15, *subslot* from 0 to 9, *port* from 0 to 9, *VPI* from 0 to 255, and *VCI* from 0 to 65535.

When **old** is specified:

- For Ethernet access users, the NAS port ID format is slot number (2 characters) + subslot number (2 bytes) + card number (3 bytes) + VLAN ID (9 characters).
- For ADSL access users, the NAS port ID format is slot number (2 characters) + subslot number (2 bytes) + card number (3 bytes) + VPI (8 characters) + VCI (16 characters). A field is prefixed with 0s if its actual value contains fewer characters.

Example

Set the format of the NAS port ID attribute to **new**.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server nas-port-id-format new
```

Related Topics

19.2.9 display radius-server configuration

19.2.40 radius-server retransmit timeout dead-time

Function

The **radius-server retransmit timeout dead-time** command sets the number of times that RADIUS request packets are retransmitted, timeout period, and interval for the server to revert to the active status.

The **undo radius-server retransmit timeout dead-time** command restores the default number of retransmission times, the default timeout period, and the default interval for the server to revert to the active status.

By default, the number of retransmission times is 3, timeout period is 5 seconds, and the interval for the server to revert to the active status is 5 minutes.

Format

radius-server { **retransmit** *retry-times* | **timeout** *time-value* | **dead-time** *dead-time* } *

undo radius-server { **retransmit** [*retry-times*] | **timeout** [*time-value*] | **dead-time** [*dead-time*] } *

Parameters

Parameter	Description	Value
retransmit *retry-times*	Specifies the number of retransmission times. The value is the total number of times a packet is transmitted.	The value is an integer that ranges from 1 to 5.
timeout *time-value*	Specifies the timeout period.	The value is an integer that ranges from 1 to 10, in seconds.
dead-time *dead-time*	Specifies the interval for the server to revert to the active status.	The value is an integer that ranges from 1 to 65535, in minutes.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The retransmission upon timeout mechanism is configured for a device to forward RADIUS Access-Request packets sourced from users to the server. The overall retransmission time depends on the retransmission interval, retransmission times, RADIUS server status, and number of servers configured in the RADIUS server template.

You can configure the number of times that RADIUS request packets are retransmitted and the timeout period using the **radius-server retransmit** *retry-times* and **radius-server timeout** *time-value* commands, respectively. If a device sends an authentication request packet to the RADIUS server and does not receive any response packet from the server during the timeout period, the device sends an authentication request packet again.

You can run the **radius-server dead-time** *dead-time* command to configure the duration for which the RADIUS server status remains Down. After the device sets the RADIUS server status to Down and the interval specified by *dead-time* expires, the device resets the server status to Force-up. If a new user needs to be authenticated in RADIUS mode and no RADIUS server is available, the device attempts to re-establish a connection with a RADIUS server in Force-up status. The Force-up status is defined to prevent servers in Down status from remaining idle.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If automatic detection for RADIUS servers is configured using the **radius-server testuser** command, the server status is maintained using the automatic detection function. The interval for the RADIUS server to revert to the active status configured using the **radius-server retransmit timeout dead-time** command does not take effect.

This command can improve the reliability of RADIUS authentication.

Precautions

- The request packet retransmission time (number of retransmission times x timeout period) of the RADIUS server must be shorter than the request packet retransmission time of the Portal server.
- If more than 8 authentication server IP addresses are configured in the RADIUS server template, reduce the number of retransmission times and timeout period.
- To rapidly detect whether the RADIUS server goes Down, smaller values are recommended for the timeout period and number of retransmission times when there are a small number of users.

Example

Set the number of retransmission times to 3, the timeout period to 2s, and the interval for the server to revert to the active status to 10 minutes.

```
<Huawei> system-view
[Huawei] radius-server template test1
[Huawei-radius-test1] radius-server retransmit 3 timeout 2 dead-time 10
```

Related Topics

19.2.9 display radius-server configuration

19.2.44 radius-server template

19.2.41 radius-server session-manage

Function

The **radius-server session-manage** command enables session management on the RADIUS server.

The **undo radius-server session-manage** command disables session management on the RADIUS server.

By default, session management is disabled on the RADIUS server.

Format

radius-server session-manage { *ip-address* [**vpn-instance** *vpn-instance-name*] **shared-key cipher** *share-key* | **any** }

undo radius-server session-manage [*ip-address* [**vpn-instance** *vpn-instance-name*] | **all**]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of the RADIUS session management server.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance bound to the RADIUS session management server.	The value must be the name of an existing VPN instance.
shared-key cipher *share-key*	Specifies the shared key of the RADIUS session management server.	The value is a string of case-sensitive characters without spaces, and question marks. *share-key* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.
any	Indicates that no RADIUS session management server is specified.	-
all	Deletes all RADIUS session management servers.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To improve device security, run this command to enable session management on the RADIUS server. After this function is enabled, the device checks the source IP addresses and shared keys for the received session management packets. When the source IP addresses and shared keys match the configured values, the packets are processed; otherwise, the packets are discarded.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- When the **any** parameter is specified, there is a security risk. You are advised to configure the IP address and shared key for a specified RADIUS session management server.

Example

Enable session management on the RADIUS server, and set the IP address and shared key of the RADIUS session management server to 10.1.1.1 and **Huawei@2012** respectively.

```
<Huawei> system-view
[Huawei] radius-server session-manage 10.1.1.1 shared-key cipher Huawei@2012
```

Related Topics

19.2.11 display radius-server session-manage configuration

19.2.42 radius-server shared-key (RADIUS server template view)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

The **undo radius-server shared-key** command restores the default shared key of a RADIUS server.

The default username and password are available in *AR Router Default Usernames and Passwords* (**Enterprise Network** or **Carrier**). If you have not obtained the access permission of the document, see **Help** on the website to find out how to obtain it.

Format

radius-server shared-key cipher *key-string*

undo radius-server shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the shared key in cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-string	Specifies the shared key of a RADIUS server.	The value is a case-sensitive character string without spaces, single quotation marks ('), or question marks (?). *key-string* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with a RADIUS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. To ensure validity of both communication parties, the device and RADIUS server must be configured with the same shared key.

NOTE

To improve security, change the default shared key immediately. It is recommended that the new shared key contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.

Example

Set the shared key of a RADIUS server to **Huawei@2012** in cipher text.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server shared-key cipher Huawei@2012
```

Related Topics

19.2.9 display radius-server configuration

19.2.44 radius-server template

19.2.43 radius-server shared-key (system view)

Function

The **radius-server shared-key** command configures the shared key of a RADIUS server.

The **undo radius-server shared-key** command deletes the shared key of a RADIUS server.

By default, no global shared key is configured for the RADIUS server.

Format

radius-server ip-address { *ipv4-address* | *ipv6-address* } **shared-key cipher** *key-string*

undo radius-server ip-address { *ipv4-address* | *ipv6-address* } **shared-key**

Parameters

Parameter	Description	Value
ip-address { *ipv4-address* | *ipv6-address* }	Specifies the IPv4 or IPv6 address of the RADIUS server.	• *ipv4-address*: The value is in dotted decimal notation. • *ipv6-address*: The value is a 32-bit hexadecimal string in format X:X:X:X:X:X:X:X.
cipher *key-string*	Specifies the shared key in cipher text.	The value is a case-sensitive character string without spaces, single quotation marks ('), or question marks (?). *key-string* can be a string of 1-128 characters in plain text or a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters in cipher text.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with a RADIUS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. To ensure validity of both communication parties, the device and RADIUS server must be configured with the same shared key.

You can run the **19.2.42 radius-server shared-key (RADIUS server template view)** command in the RADIUS server template view to configure the shared keys. However, after this command is run, all RADIUS servers in the template use the same shared key. To configure different shared keys for RADIUS servers, run the **radius-server shared-key** command in the system view.

Precautions

To improve security, it is recommended that the shared key contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.

When the shared keys are configured in both the RADIUS server template and system view, the configuration in the system view takes effect.

Example

Set the shared key for RADIUS server to **Huawei@2012**.

```
<Huawei> system-view
[Huawei] radius-server ip-address 10.1.1.1 shared-key cipher Huawei@2012
```

Related Topics

19.2.42 radius-server shared-key (RADIUS server template view)

19.2.44 radius-server template

Function

The **radius-server template** command creates a RADIUS server template and displays the RADIUS server template view.

The **undo radius-server template** command deletes a RADIUS server template.

By default, the device contains the RADIUS server template **default**. The template can be modified, but cannot be deleted.

Format

radius-server template *template-name*

undo radius-server template *template-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
template-name	Specifies the name of a RADIUS server template.	The value is a string of 1 to 32 case-sensitive characters, including letters (case-sensitive), numerals (0 to 9), punctuation mark (.), underline (_), and hyphens (-).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Creating a RADIUS server template is the prerequisite for configuring RADIUS authentication and accounting. You can perform RADIUS configurations, such as the configuration of authentication servers, accounting servers, and shared key only after a RADIUS server template is created.

Follow-up Procedure

Configure an authentication server, an accounting server, and shared key in the RADIUS server template view, and then run the **19.2.21 radius-server (aaa domain view)** command to apply the RADIUS server template.

Example

Create a RADIUS server template **template1** and enter the RADIUS server template view.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1]
```

Related Topics

19.2.9 display radius-server configuration

19.2.21 radius-server (aaa domain view)

 Copyright © Huawei Technologies Co., Ltd.

19.2.45 radius-server testuser

Function

The **radius-server testuser** command enables the automatic detection function and configures an automatic detection account.

The **undo radius-server testuser** command restores the default settings.

By default, the automatic detection function is disabled.

Format

radius-server testuser username *user-name* **password cipher** *password*

undo radius-server testuser

Parameters

Parameter	Description	Value
username *user-name*	Specifies a user name used for automatic detection.	The value is a string of 1 to 253 case-sensitive characters. If the user name contains spaces, you must enclose the name with double quotation marks ("), for example, "user for test".
password cipher *password*	Specifies the user password for automatic detection.	The value is a character string of 1 to 128 characters without spaces and question marks. It is case sensitive. If it is in cipher text, the password is a string of 48, 68, 88, 108, 128, 148, 168, or 188 characters.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

After the RADIUS server status is set to Down, you can configure the automatic detection function to test the RADIUS server reachability.

 Copyright © Huawei Technologies Co., Ltd.

After automatic detection is configured for users, if the device does not receive authentication packets from the users within the detection interval (configured using the **radius-server detect-server** command), the device performs a RADIUS server detection.

For the automatic status detection function, only the automatic detection user name and password need to be configured in the RADIUS server template on the device, and the automatic detection account does not need to be configured on the RADIUS server. Authentication success is not mandatory. If the device can receive the authentication failure response packet, the RADIUS server is properly working and the device sets the RADIUS server status to Up. If the device cannot receive the response packet, the RADIUS server is unavailable and the device sets the RADIUS server status to Down.

Example

Create a user account with the user name **test** and password **Huawei@2012** in RADIUS server template **acs**.

```
<Huawei> system-view
[Huawei] radius-server template acs
[Huawei-radius-acs] radius-server testuser username test password cipher Huawei@2012
```

19.2.46 radius-server traffic-unit

Function

The **radius-server traffic-unit** command sets the traffic unit used by a RADIUS server.

The **undo radius-server traffic-unit** command restores the default traffic unit used by a RADIUS server.

The default RADIUS traffic unit is byte on the device.

Format

radius-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

undo radius-server traffic-unit

Parameters

Parameter	Description	Value
byte	Indicates that the traffic unit is byte.	-
kbyte	Indicates that the traffic unit is kilobyte.	-
mbyte	Indicates that the traffic unit is megabyte.	-
gbyte	Indicates that the traffic unit is gigabyte.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Different RADIUS servers may use different traffic units; therefore, you need to set the traffic unit for each RADIUS server group on the router and the traffic unit must be the same as that on the RADIUS server.

Example

Set the traffic unit used by a RADIUS server to kilobyte.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] radius-server traffic-unit kbyte
```

Related Topics

19.2.9 display radius-server configuration

19.2.47 radius-server user-name domain-included

Function

The **radius-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in RADIUS packets to be sent to a RADIUS server.

The **radius-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to the RADIUS server.

The **undo radius-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending RADIUS packets to a RADIUS server.

The **undo radius-server user-name domain-included except-eap** command configures the device not to encapsulate the domain name in the user name when sending packets to a RADIUS server (applicable to other authentication modes except EAP authentication).

By default, the device does not modify the user name entered by the user in the packets sent to the RADIUS server.

Format

radius-server user-name domain-included

 Copyright © Huawei Technologies Co., Ltd.

radius-server user-name original

undo radius-server user-name domain-included

undo radius-server user-name domain-included except-eap

Parameters

None

Views

RADIUS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter. The domain name delimiter can also be any of the following symbols: \ / : < > | ' %.

If the RADIUS server does not accept the user name with the domain name, run the **undo radius-server user-name domain-included** command to delete the domain name from the user name.

Precautions

If the user names in the RADIUS packets sent from the device to RADIUS server contain domain names, ensure that the total length of a user name (user name + domain name delimiter + domain name) is not longer than 253 characters; otherwise, the user name cannot be contained in RADIUS packets. As a result, authentication will fail.

Example

Configure the device not to encapsulate the domain name in the user name when sending RADIUS packets to a RADIUS server.

```
<Huawei> system-view
[Huawei] radius-server template template1
[Huawei-radius-template1] undo radius-server user-name domain-included
```

Related Topics

19.2.9 display radius-server configuration

19.2.48 reset radius-server accounting-stop-packet

Function

The **reset radius-server accounting-stop-packet** command clears statistics on the remaining buffer information of RADIUS accounting-stop packets.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset radius-server accounting-stop-packet { **all** | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets.	-
ip *ipv4-address*	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets with the specified IPv4 address.	The value of *ipv4-address* is in dotted decimal notation.
ip *ipv6-address*	Clears statistics on the remaining buffer information of RADIUS accounting-stop packets with the specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command can clear statistics on the remaining buffer information of RADIUS accounting-stop packets. The deleted statistics cannot be restored.

Example

Clear statistics on the remaining buffer information of all RADIUS accounting-stop packets.

```
<Huawei> reset radius-server accounting-stop-packet all
```

Related Topics

19.2.7 display radius-server accounting-stop-packet

 Copyright © Huawei Technologies Co., Ltd.

19.2.49 snmp-agent trap enable feature-name radius

Function

The **snmp-agent trap enable feature-name radius** command enables the trap function for the RDS module.

The **undo snmp-agent trap enable feature-name radius** command disables the trap function for the RDS module.

By default, the trap function is disabled for the RDS module.

Format

snmp-agent trap enable feature-name radius [**trap-name** { **hwradiusacctserverdown** | **hwradiusacctserverup** | **hwradiusauthserverdown** | **hwradiusauthserverup** }]

undo snmp-agent trap enable feature-name radius [**trap-name** { **hwradiusacctserverdown** | **hwradiusacctserverup** | **hwradiusauthserverdown** | **hwradiusauthserverup** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the RDS module.	-
hwradiusacctserver-down	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is interrupted.	-
hwradiusacctserverup	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS accounting server is restored.	-
hwradiusauthserver-down	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is interrupted.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwradiusauthserverup	Enables the device to send a Huawei proprietary trap when it detects that communication with the RADIUS authentication server is restored.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

Example

Enable the trap function for hwradiusacctserverdown of the RDS module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name radius trap-name hwradiusacctserverdown
```

Related Topics

19.2.13 display snmp-agent trap feature-name radius all

19.2.50 test-aaa

Function

The **test-aaa** command tests the connectivity between the device and the authentication server or accounting server, and tests whether a user can be authenticated using authentication server and whether the accounting server can charge a user.

Format

test-aaa *user-name user-password* **radius-template** *template-name* [**chap** | **pap** | **accounting** [**start** | **realtime** | **stop**]]

 Copyright © Huawei Technologies Co., Ltd.

test-aaa *user-name user-password* **hwtacacs-template** *template-name* [**accounting** [**start** | **realtime** | **stop**]]

Parameters

Parameter	Description	Value
user-name	Specifies a user name.	The value is a string of 1 to 253 case-insensitive characters. **NOTE** When the HWTACACS, or RADIUS server is detected, the user name cannot contain spaces.
user-password	Specifies a user password.	The value is a string of 1 to 128 case-sensitive characters.
radius-template *template-name*	Specifies the name of a RADIUS server template.	The RADIUS server template must already exist.
chap	Indicates Challenge Handshake Authentication Protocol (CHAP) authentication. The NAS device sends the user name, password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pap	Indicates Password Authentication Protocol (PAP) authentication. The NAS device adds the user name and encrypted password to the corresponding fields of authentication request packets, and then sends the packets to the RADIUS server. The NAS device determines whether to allow the user go online based on the result returned by the RADIUS server.	-
accounting	Indicates accounting. By default, an accounting-start packet is sent.	-
start	Indicates that the sent packet is an accounting-start packet.	-
realtime	Indicates that the sent packet is a real-time accounting packet.	-
stop	Indicates that the sent packet is an accounting-stop packet.	-
hwtacacs-template *template-name*	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The test-aaa command tests service reachability of the server. The device sends an authentication or accounting request packet to the server. If the server returns an authentication or accounting success packet, the device and server can communicate with each other. If the server's response times out, the device and server cannot communicate with each other.

Prerequisites

An authentication server template or accounting server template has been created, an authentication server or accounting server has been specified in the

authentication server template or accounting server template, and the authentication server or accounting server has been configured.

Follow-up Procedure

If the test result indicates that the user fails to be authenticated by using authentication server or the accounting server fails to charge the user, check whether the configuration of the authentication server template and the authentication server is correct, and check the connectivity between the device and the authentication server.

Precautions

chap and **pap** are two authentication modes.

- PAP: The NAS device adds the user name and encrypted password to the corresponding fields of authentication request packets, and then sends the packets to the RADIUS server. The NAS device determines whether to allow the user go online based on the result returned by the RADIUS server.
- CHAP: The NAS device sends the user name, password, and 16-byte random code to the RADIUS server. The RADIUS server searches for the database according to the user name and obtains the password that is the same as the encrypted password at the user side. The RADIUS server then encrypts the received 16-byte random code and compares the result with the password. If they are the same, the user is authenticated. If they are different, the user fails to be authenticated. In addition, if the user is authenticated, the RADIUS server generates a 16-byte random code to challenge the user.

Before running the **test-aaa** command, you only need to create a RADIUS server template and specify an authentication server or accounting server in the RADIUS server template.

Example

Test whether the user **user1** can be authenticated using CHAP authentication in the RADIUS server template **huawei**.

```
<Huawei> test-aaa user1 userkey radius-template huawei chap
Info: The server template does not exist.
```

19.2.51 radius-server dead-detect-condition by-server-ip

Function

The **radius-server dead-detect-condition by-server-ip** command configures keepalive detection for RADIUS server based on the RADIUS server IP address.

The **undo radius-server dead-detect-condition by-server-ip** command restores the default setting.

By default, keepalive detection is performed for only RADIUS authentication server.

Format

radius-server dead-detect-condition by-server-ip

undo radius-server dead-detect-condition by-server-ip

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device periodically sends authentication request packets to the RADIUS server in Down state. If the RADIUS server responds, the device sets the RADIUS authentication server status to Up. The device does not perform keepalive detection for RADIUS accounting servers in Down state. Instead, the device sets the RADIUS accounting server status to Up only when the server recovery time expires.

To allow the device to promptly detect the status of RADIUS accounting servers that are in Down state, run the **radius-server dead-detect-condition by-server-ip** command. After the command is executed, the device performs keepalive detection on RADIUS servers based on the RADIUS server IP address, so that the status of RADIUS accounting server is associated with the status of authentication server.

Precautions

After the **radius-server dead-detect-condition by-server-ip** command is executed, run the **radius-server testuser** command to configure automatic user detection.

When detecting the Down states of RADIUS authentication and accounting servers, the device counts the numbers of authentication and accounting request packets separately. After the **radius-server dead-detect-condition by-server-ip** command is executed, if the authentication and accounting servers sharing the same IP address are in the same VPN instance, the device accumulates the number of authentication and accounting packets sent by the servers. In addition, the status of RADIUS authentication server with the same IP address in the same VPN instance is updated.

Example

Configure keepalive detection for RADIUS server based on RADIUS server IP address.

```
<Huawei> system-view
[Huawei] radius-server dead-detect-condition by-server-ip
```

19.3 HWTACACS Configuration Commands

19.3.1 display hwtacacs-server accounting-stop-packet

Function

The **display hwtacacs-server accounting-stop-packet** command displays information about Accounting-Stop packets sent by an HWTACACS server.

Format

display hwtacacs-server accounting-stop-packet { **all** | *number* | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Displays information about all Accounting-Stop packets.	-
number	Displays information about Accounting-Stop packets starting from a specified number.	The value is an integer that ranges from 1 to 65535.
ip *ipv4-address*	Displays information about Accounting-Stop packets sent by the HWTACACS server with a specified IPv4 address.	The value is in dotted decimal notation.
ip *ipv6-address*	Displays information about Accounting-Stop packets sent by the HWTACACS server with a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

During HWTACACS troubleshooting, you can run this command to check information about Accounting-Stop packets sent by the HWTACACS server.

Example

Display information about all Accounting-Stop packets.

```
<Huawei> display hwtacacs-server accounting-stop-packet all
-------------------------------------------------------------
NO. SendTime      IP Address                    Template
1   10            192.168.1.110                 tac
-------------------------------------------------------------
Whole accounting stop packet to resend:1
```

Table 19-32 Description of the **display hwtacacs-server accounting-stop-packet** command output

Item	Description
NO.	Number of the Accounting-Stop packet.
SendTime	Number of times that Accounting-Stop packets are sent.
IP Address	IP address of the HWTACACS server.
Template	Name of the HWTACACS server template.
Whole accounting stop packet to resend	Total number of Accounting-Stop packets sent by a device.

Related Topics

19.3.7 hwtacacs-server accounting-stop-packet resend

19.3.20 reset hwtacacs-server accounting-stop-packet

19.3.2 display hwtacacs-server template

Function

The **display hwtacacs-server template** command displays the configurations of an HWTACACS server template.

Format

display hwtacacs-server template [*template-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display hwtacacs-server template** command output helps you check the configuration of HWTACACS server templates and isolate faults.

NOTE

The device determines whether its communication with the HWTACACS server is proper based on the response timeout mechanism of HWTACACS request packets, and always marks the status of the last HWTACACS server as Up.

Example

Display the configuration of all HWTACACS server templates.

```
<Huawei> display hwtacacs-server template
  ------------------------------------------------------------------------------
  Global:
  Shared-key                      : ****************
  ------------------------------------------------------------------------------
  HWTACACS-server template name   : template0
  Primary-authentication-server   : 192.168.18.102:49 Vrf:- Shared-key:- Status:UP
  Primary-authorization-server    : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
  Primary-accounting-server       : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
  Secondary-authentication-server : -:0 Vrf:- Shared-key:- Status:-
  Secondary-authorization-server  : -:0 Vrf:- Shared-key:- Status:-
  Secondary-accounting-server     : -:0 Vrf:- Shared-key:- Status:-
  Third-authentication-server     : -:0 Vrf:- Shared-key:- Status:-
  Third-authorization-server      : -:0 Vrf:- Shared-key:- Status:-
  Third-accounting-server         : -:0 Vrf:- Shared-key:- Status:-
  Current-authentication-server   : 192.168.18.102:49 Vrf:- Shared-key:- Status:UP
  Current-authorization-server    : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
  Current-accounting-server       : 192.168.18.102:49 Vrf:- Shared-key:* Status:UP
  Source-IP-address               : -
  Source-LoopBack                 : -
  Source-IPv6-address             : -
  IPv6 Source-LoopBack            : -
  Shared-key                      : -
  Quiet-interval(min)             : 5
  Response-timeout-Interval(sec)  : 5
  Domain-included                 : NO
  Traffic-unit                    : B
  ------------------------------------------------------------------------------
  Total 2,2 printed
```

Display the configuration of the HWTACACS server template **template0**.

```
<Huawei> display hwtacacs-server template template0
 ----------------------------------------------------------------------------
 HWTACACS-server template name   : template0
 Primary-authentication-server   : FC00::2:1:20 Vrf:- Shared-key:- Status:UP
 Primary-authorization-server    : -:0 Vrf:- Shared-key:- Status:-
 Primary-accounting-server       : -:0 Vrf:- Shared-key:- Status:-
 Secondary-authentication-server : 10.1.1.1:20 Vrf:- Shared-key:* Status:UP
 Secondary-authorization-server  : -:0 Vrf:- Shared-key:- Status:-
 Secondary-accounting-server     : 10.1.1.1:10 Vrf:- Shared-key:* Status:UP
 Third-authentication-server     : -:0 Vrf:- Shared-key:- Status:-
 Third-authorization-server      : -:0 Vrf:- Shared-key:- Status:-
 Third-accounting-server         : -:0 Vrf:- Shared-key:- Status:-
 Current-authentication-server   : FC00::2:1:20 Vrf:- Shared-key:- Status:UP
 Current-authorization-server    : -:0 Vrf:- Shared-key:- Status:-
 Current-accounting-server       : 10.1.1.1:10 Vrf:- Shared-key:* Status:UP
 Source-IP-address               : -
 Source-LoopBack                 : -
 Source-IPv6-address             : -
 IPv6 Source-LoopBack            : -
 Shared-key                      : -
 Quiet-interval(min)             : 5
 Response-timeout-Interval(sec)  : 5
 Domain-included                 : Original
 Traffic-unit                    : B
 ----------------------------------------------------------------------------
```

Table 19-33 Description of the **display hwtacacs-server template** command output

Item	Description
Global	Global configuration information.
HWTACACS-server template name	Name of the HWTACACS server template.
Primary-authentication-server	IP address, port number, VPN instance, shared key, and status of the primary authentication server.
Primary-authorization-server	IP address, port number, VPN instance, shared key, and status of the primary authorization server.
Primary-accounting-server	IP address, port number, VPN instance, shared key, and status of the primary accounting server.
Secondary-authentication-server	IP address, port number, VPN instance, shared key, and status of the second authentication server.
Secondary-authorization-server	IP address, port number, VPN instance, shared key, and status of the second authorization server.
Secondary-accounting-server	IP address, port number, VPN instance, shared key, and status of the second accounting server.
Third-authentication-server	IP address, port number, VPN instance, shared key, and status of the third authentication server.
Third-authorization-server	IP address, port number, VPN instance, shared key, and status of the third authorization server.
Third-accounting-server	IP address, port number, VPN instance, shared key, and status of the third accounting server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current-authentication-server	IP address, port number, VPN instance, shared key, and status of the authentication server in use.
Current-authorization-server	IP address, port number, VPN instance, shared key, and status of the authorization server in use.
Current-accounting-server	IP address, port number, VPN instance, shared key, and status of the accounting server in use.
Source-IP-address	Source IP address for communication between the device and the HWTACACS server.
Source-IPv6-address	Source IPv6 address for communication between the device and the HWTACACS server.
IPv6 Source-LoopBack	Number of the loopback interface. The IPv6 address of the loopback interface is used as the source IPv6 address for communication between the device and the HWTACACS server.
Shared-key	The first Shared-key indicates the shared key of the HWTACACS server configured in the system view. The second Shared-key indicates the shared key of the HWTACACS server configured in the HWTACACS server template view.
Quiet-interval(min)	Interval for the primary server to return to the active state, in minutes.
Response-timeout-Interval(sec)	Response timeout interval of the HWTACACS server, in seconds.
Domain-included	Whether the user name contains an authentication domain name. ● Yes: The user name contains the domain name. ● No: The user name does not contain the domain name. ● Original: The device does not modify the user name entered by the user.
Traffic-unit	Traffic unit used by the HWTACACS server, in bytes.
Total 1,1 printed	Total number of HWTACACS server templates and number of printed HWTACACS server templates.

19.3.3 display hwtacacs-server template verbose

Function

The **display hwtacacs-server template verbose** command displays statistics on HWTACACS authentication, accounting, and authorization.

Format

display hwtacacs-server template *template-name* **verbose**

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

By viewing statistics on HWTACACS authentication, accounting, and authorization, administrators can better understand the interaction between modules, facilitating fault locating and troubleshooting.

You can run the **reset hwtacacs-server statistics** { **all** | **accounting** | **authentication** | **authorization** } command to delete statistics on HWTACACS authentication, accounting, and authorization.

Precautions

In the HWTACACS server template, you can query the relevant statistics only after the IP address of the authentication server, the IP address of the authorization server, or the IP address of the accounting server is configured.

Example

Display statistics on HWTACACS authentication, accounting, and authorization in the HWTACACS server template *test1*.

```
<Huawei> display hwtacacs-server template test1 verbose
---[HWTACACS template test1 primary
authentication]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS authen client access request packet number:
0
HWTACACS authen client access response packet number:
0
HWTACACS authen client unknown type number:
0
HWTACACS authen client timeout number: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
HWTACACS authen client packet dropped number:
0
HWTACACS authen client access request change password number:
0
HWTACACS authen client access request login number:
0
HWTACACS authen client access request send authentication number:
0
HWTACACS authen client access request send password number:
0
HWTACACS authen client access connect abort number:
0
HWTACACS authen client access connect packet number:
0
HWTACACS authen client access response error number:
0
HWTACACS authen client access response failure number:
0
HWTACACS authen client access response follow number:
0
HWTACACS authen client access response getdata number:
0
HWTACACS authen client access response getpassword number:
0
HWTACACS authen client access response getuser number:
0
HWTACACS authen client access response pass number:
0
HWTACACS authen client access response restart number:
0
HWTACACS authen client malformed access response number:
0
HWTACACS authen client round trip time(s): 0
---[HWTACACS template test1 primary
authorization]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS author client request packet number:
0
HWTACACS author client response packet number:
0
HWTACACS author client timeout number: 0
HWTACACS author client packet dropped number:
0
HWTACACS author client unknown type number:
0
HWTACACS author client request EXEC number:
0
HWTACACS author client request PPP number: 0
HWTACACS author client request VPDN number:
0
HWTACACS author client response error number:
0
HWTACACS author client response EXEC number:
0
HWTACACS author client response PPP number:
0
HWTACACS author client response VPDN number:
0
HWTACACS author client round trip time(s): 0
---[HWTACACS template test1 primary
accounting]---
HWTACACS server open number:
1670281960
HWTACACS server close number: 508333868
HWTACACS account client request packet number:
0
HWTACACS account client response packet number:
```

```
0
HWTACACS account client unknown type number:
0
HWTACACS account client timeout number: 0
HWTACACS account client packet dropped number:
0
HWTACACS account client request command level number:
0
HWTACACS account client request connection number:
0
HWTACACS account client request EXEC number:
0
HWTACACS account client request network number:
0
HWTACACS account client request system event number:
0
HWTACACS account client request update number:
0
HWTACACS account client response error number:
0
HWTACACS account client round trip time(s): 0
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-34 Description of the **display hwtacacs-server template verbose** command output

Item	Description
HWTACACS template test1 primary authentication	Statistics on the primary authentication server in the HWTACACS server template *test1*. If the secondary and third authentication servers are configured, the relevant statistics are also displayed, including: ● HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up ● HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected ● HWTACACS authen client access request packet number: Number of HWTACACS client authentication request packets ● HWTACACS authen client access response packet number: Number of HWTACACS client authentication response packets ● HWTACACS authen client unknown type number: Number of unknown HWTACACS client authentication messages ● HWTACACS authen client timeout number: Number of HWTACACS client authentication timeouts ● HWTACACS authen client packet dropped number: Number of times that HWTACACS client authentication packets are dropped ● HWTACACS authen client access request change password number: Number of password change requests from an HWTACACS client ● HWTACACS authen client access request login number: Number of HWTACACS client login requests ● HWTACACS authen client access request send authentication number: Number of authentication requests sent by an HWTACACS client ● HWTACACS authen client access request send password number: Number of times that an HWTACACS client sends passwords ● HWTACACS authen client access connect abort number: Number of connection-stop packets sent by an HWTACACS client ● HWTACACS authen client access connect packet number: Number of continuous packets sent by an HWTACACS client ● HWTACACS authen client access response error number: Number of error packets received by an HWTACACS client

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• HWTACACS authen client access response failure number: Number of authentication failure packets received by an HWTACACS client • HWTACACS authen client access response follow number: Number of packets that an HWTACACS client receives from the server for re-authentication • HWTACACS authen client access response getdata number: Number of packets that an HWTACACS client receives from the server for user information • HWTACACS authen client access response getpassword number: Number of packets that an HWTACACS client receives from the server for user password • HWTACACS authen client access response getuser number: Number of packets that an HWTACACS client receives from the server for user name • HWTACACS authen client access response pass number: Number of authentication success packets received by an HWTACACS client • HWTACACS authen client access response restart number: Number of authentication restart packets that an HWTACACS client receives from the server • HWTACACS authen client malformed access response number: Number of invalid response packets received by an HWTACACS client • HWTACACS authen client round trip time(s): Last authentication response time of the HWTACACS server

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
HWTACACS template test1 primary authorization	Statistics on the primary authorization server in the HWTACACS server template *test1*. If the secondary and third authorization servers are configured, the relevant statistics are also displayed, including: ● HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up ● HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected ● HWTACACS author client request packet number: Number of HWTACACS client authorization request packets ● HWTACACS author client response packet number: Number of HWTACACS client authorization response packets ● HWTACACS author client timeout number: Number of HWTACACS client authorization timeouts ● HWTACACS author client packet dropped number: Number of times that HWTACACS client authorization packets are dropped ● HWTACACS author client unknown type number: Number of unknown authorization packets on an HWTACACS client ● HWTACACS author client request EXEC number: Number of EXEC user request packets authorized by an HWTACACS client ● HWTACACS author client request PPP number: Number of PPP user request packets authorized by an HWTACACS client ● HWTACACS author client request VPDN number: Number of VPDN user request packets authorized by an HWTACACS client ● HWTACACS author client response error number: Number of error authorization response packets received by an HWTACACS client ● HWTACACS author client response EXEC number: Number of authorized EXEC user response packets received by an HWTACACS client ● HWTACACS author client response PPP number: Number of authorized PPP user response packets received by an HWTACACS client ● HWTACACS author client response VPDN number: Number of authorized VPDN user response packets received by an HWTACACS client ● HWTACACS author client round trip time(s): Last authorization response time of the HWTACACS server

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
HWTACACS template test1 primary accounting	Statistics on the primary accounting server in the HWTACACS server template *test1*. If the secondary and third accounting servers are configured, the relevant statistics are also displayed, including: ● HWTACACS server open number: Number of times that the socket connection of the HWTACACS server is set up ● HWTACACS server close number: Number of times that the socket connection of the HWTACACS server is disconnected ● HWTACACS account client request packet number: Number of HWTACACS client accounting request packets ● HWTACACS account client response packet number: Number of HWTACACS client accounting response packets ● HWTACACS account client unknown type number: Number of unknown HWTACACS client accounting packets ● HWTACACS account client timeout number: Number of HWTACACS client accounting timeouts ● HWTACACS account client packet dropped number: Number of times that HWTACACS client accounting packets are dropped ● HWTACACS account client request command level number: Number of HWTACACS client accounting requests for command line packets ● HWTACACS account client request connection number: Number of HWTACACS client accounting requests for connection ● HWTACACS account client request EXEC number: Number of HWTACACS client accounting requests for EXEC packets ● HWTACACS account client request network number: Number of HWTACACS client accounting requests for Network packets ● HWTACACS account client request system event number: Number of HWTACACS client accounting requests for system event packets ● HWTACACS account client request update number: Number of HWTACACS client accounting requests for update packets ● HWTACACS account client response error number: Number of HWTACACS client accounting requests for error packets

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• HWTACACS account client round trip time(s): Response time of the last accounting packet of the HWTACACS server

19.3.4 hwtacacs enable

Function

The **hwtacacs enable** command enables Huawei Terminal Access Controller Access Control System (HWTACACS).

The **undo hwtacacs enable** command disables HWTACACS.

By default, HWTACACS is enabled.

Format

hwtacacs enable

undo hwtacacs enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To use HWTACACS authentication, authorization, or accounting, run the **hwtacacs enable** command to enable the HWTACACS function.

Precautions

If the **undo hwtacacs enable** command is run when a user is performing HWTACACS authentication, authorization, or accounting, the command does not take effect.

Example

Disable HWTACACS.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] undo hwtacacs enable
```

19.3.5 hwtacacs-server

Function

The **hwtacacs-server** command applies an HWTACACS server template to a domain.

The **undo hwtacacs-server** command deletes an HWTACACS server template from a domain.

By default, no HWTACACS server template is applied to a domain.

Format

hwtacacs-server *template-name*

undo hwtacacs-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform HWTACACS authentication, authorization, and accounting for users in a domain, configure an HWTACACS server template in the domain. After the HWTACACS server template is configured in the domain, the configuration in the HWTACACS server template takes effect.

Prerequisites

An HWTACACS server template has been created by using the **19.3.14 hwtacacs-server template** command.

Example

Apply the HWTACACS server template **tacacs1** to the domain **tacacs1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server template tacacs1
[Huawei-hwtacacs-tacacs1] quit
[Huawei] aaa
[Huawei-aaa] domain tacacs1
[Huawei-aaa-domain-tacacs1] hwtacacs-server tacacs1
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.6 hwtacacs-server accounting

Function

The **hwtacacs-server accounting** command configures an HWTACACS accounting server.

The **undo hwtacacs-server accounting** command cancels the configuration.

By default, no HWTACACS accounting server is configured.

Format

hwtacacs-server accounting *ipv4-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third**] [**shared-key cipher** *key-string*]

hwtacacs-server accounting *ipv6-address* [*port*] [**public-net**] [**secondary** | **third**] [**shared-key cipher** *key-string*]

undo hwtacacs-server accounting [**secondary** | **third**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS accounting server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the HWTACACS accounting server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS accounting server.	The value is an integer that ranges from 1 to 65535. The default value is 49.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
public-net	Indicates that the HWTACACS accounting server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS accounting server is bound to.	The VPN instance must already exist.
secondary	Configures the second HWTACACS accounting server as the standby server. If no standby server is configured, the primary HWTACACS accounting server is specified.	-
third	Specifies the third HWTACACS accounting server as the secondary server. If no secondary server is configured, the primary HWTACACS accounting server is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
shared-key cipher *key-string*	Indicates the shared key of the specified HWTACACS accounting server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: ● Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. ● Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device does not support local accounting; therefore, you need to configure an HWTACACS accounting server to perform accounting. The device sends accounting

packets to an HWTACACS accounting server only after the accounting server is specified in an HWTACACS server template.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.
- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same type (for example, the servers are all primary servers), only the latest configuration takes effect.

Example

Configure the shared key of the primary HWTACACS accounting server to **Admin@123**.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server accounting 10.163.155.12 52 shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.7 hwtacacs-server accounting-stop-packet resend

Function

The **hwtacacs-server accounting-stop-packet resend** command enables or disables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted each time.

By default, 100 accounting-stop packets can be retransmitted each time.

Format

hwtacacs-server accounting-stop-packet resend { **disable** | **enable** *number* }

Parameters

Parameter	Description	Value
disable	Disables the retransmission of accounting-stop packets.	-
enable *number*	Enables the retransmission of accounting-stop packets, and specifies the number of packets that can be retransmitted each time.	The value is an integer that ranges from 1 to 300.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a user goes offline, the device sends an accounting-stop packet to an accounting server. After the accounting server receives the accounting-stop packet, it stops accounting for the user. If the accounting server does not receive the accounting-stop packet because of network faults, it continues to perform accounting for the user. As a result, the user is charged incorrectly. To solve this problem, configure the device to send accounting-stop packets multiple times.

Precautions

- If **disable** is configured, an accounting-stop packet is transmitted only once even when packet transmission fails.
- If **enable** *number* is configured, *number* specifies the number of accounting-stop packets that can be retransmitted each time when the device does not receive any response packet from the HWTACACS server or fails to receive the response packet.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted each time to 50.

```
<Huawei> system-view
[Huawei] hwtacacs-server accounting-stop-packet resend enable 50
```

Related Topics

19.3.1 display hwtacacs-server accounting-stop-packet

19.3.8 hwtacacs-server authentication

Function

The **hwtacacs-server authentication** command configures the HWTACACS authentication server.

The **undo hwtacacs-server authentication** command deletes configurations of the HWTACACS authentication server.

By default, no HWTACACS authentication server is configured.

Format

hwtacacs-server authentication *ipv4-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third**] [**shared-key cipher** *key-string*]

hwtacacs-server authentication *ipv6-address* [*port*] [**public-net**] [**secondary** | **third**] [**shared-key cipher** *key-string*]

undo hwtacacs-server authentication [**secondary** | **third**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authentication server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of an HWTACACS authentication server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS authentication server.	The value is an integer that ranges from 1 to 65535. The default value is 49.
public-net	Indicates that the HWTACACS authentication server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS accounting server is bound to.	The VPN instance must already exist.
secondary	Configures the second HWTACACS authentication server as the standby server. If no standby server is configured, the primary HWTACACS authentication server is specified.	-
third	Configures the third HWTACACS authentication server as the standby server. If no secondary server is configured, the primary HWTACACS authentication server is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
shared-key cipher *key-string*	Indicates the shared key of the specified HWTACACS authentication server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: ● Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. ● Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authenticate users in HWTACACS mode, you must configure the HWTACACS authentication server. When both the primary and secondary authentication

servers are configured, the device sends an authentication request packet to the secondary authentication server in any of the following situations:

- The device fails to send a request packet to the primary authentication server.
- If the device does not receive any authentication response packet from the primary server:
- The primary authentication server requires re-authentication.
- The primary authentication server considers that the received authentication request packet is incorrect.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.
- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same type (for example, the servers are all primary servers), only the latest configuration takes effect.

Example

Configure the shared key of the primary HWTACACS authentication server to **Admin@123**.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server authentication 10.163.155.12 49 shared-key cipher
Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.9 hwtacacs-server authorization

Function

The **hwtacacs-server authorization** command configures the HWTACACS authorization server.

The **undo hwtacacs-server authorization** command deletes configurations of the HWTACACS authorization server.

By default, no HWTACACS authorization server is configured.

Format

hwtacacs-server authorization *ipv4-address* [*port*] [**public-net** | **vpn-instance** *vpn-instance-name*] [**secondary** | **third**] [**shared-key cipher** *key-string*]

hwtacacs-server authorization *ipv6-address* [*port*] [**public-net**] [**secondary** | **third**] [**shared-key cipher** *key-string*]

undo hwtacacs-server authorization [**secondary** | **third**]

Parameters

Parameter	Description	Value
ipv4-address	Specifies the IPv4 address of an HWTACACS authorization server.	The value is a valid unicast address in dotted decimal notation.
ipv6-address	Specifies the IPv6 address of the HWTACACS authorization server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
port	Specifies the port number of an HWTACACS authorization server.	The value is an integer that ranges from 1 to 65535. The default value is 49.
public-net	Indicates that the HWTACACS authorization server is connected to the public network.	-
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance that the HWTACACS authorization server is bound to.	The VPN instance must already exist.
secondary	Configures the second HWTACACS authorization server as the standby server. If no standby server is configured, the primary HWTACACS authorization server is specified.	-
third	Configures the third HWTACACS authorization server as the standby server. If no secondary server is configured, the primary HWTACACS authorization server is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
shared-key cipher *key-string*	Indicates the shared key of the specified HWTACACS authorization server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: ● Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. ● Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To authorize users in HWTACACS mode, you must configure the HWTACACS authorization server.

Precautions

- You can modify this configuration only when device does not set up TCP connection with the specified accounting server.
- The IP addresses of the primary and secondary servers must be different. Otherwise, the server configuration fails.
- If the command is run for multiple times in the same HWTACACS server template to configure the servers with the same type (for example, the servers are all primary servers), only the latest configuration takes effect.

Example

Configure the shared key of the primary HWTACACS authorization server to **Admin@123**.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server authorization 10.163.155.12 49 shared-key cipher
Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.10 hwtacacs-server shared-key

Function

The **hwtacacs-server shared-key** command sets a shared key for an HWTACACS server.

The **undo hwtacacs-server shared-key** command cancels the configuration.

By default, the HWTACACS server is not configured with any shared key.

Format

hwtacacs-server shared-key cipher *key-string*

undo hwtacacs-server shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the shared key in cipher text.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
key-string	Specifies a shared key.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: ● Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. ● Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with an HWTACACS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. The device and HWTACACS server must use the same key to ensure their validity in the authentication.

Precautions

To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.

You can modify this configuration only when the HWTACACS server template is not in use.

To be compatible with the earlier versions, the device supports the shared key of 20 characters in cipher text. The length of the shared key cannot be configured.

Example

Set the shared key of the HWTACACS server to **Admin@123**.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.11 hwtacacs-server shared-key (system view)

Function

The **hwtacacs-server shared-key** command sets a shared key for an HWTACACS server.

The **undo hwtacacs-server shared-key** command cancels the configuration.

By default, the HWTACACS server is not configured with any shared key.

Format

hwtacacs-server shared-key cipher *key-string*

undo hwtacacs-server shared-key

Parameters

Parameter	Description	Value
cipher	Indicates the shared key in cipher text.	-
key-string	Indicates the shared key of the HWTACACS server.	The value is a string of case-sensitive characters in plaintext or ciphertext, spaces and question marks not supported. If the string is quoted by double quotation marks, spaces and question marks can be included. Length range: ● Simple text: 1 to 128. The system encrypts the entered character string and saves it in the configuration file. ● Ciphertext: The length value can be only 48, 68, 88, 108, 128, 148, 168, or 188. If a user enters a shared key with 32, 56, 80, 104, or 128 characters and the system can decrypt the shared key, the system determines that the shared key is ciphertext. If the system cannot decrypt the shared key, the system determines that the shared key is simple text.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The shared key is used to encrypt the password and generate the response authenticator.

When exchanging authentication packets with an HWTACACS server, the device uses MD5 to encrypt important data such as the password to ensure security of data transmission over the network. The device and HWTACACS server must use the same key to ensure their validity in the authentication.

You can run the **19.3.10 hwtacacs-server shared-key** command in the HWTACACS server template view to configure the shared keys. However, after this command is run, all HWTACACS servers in the template use the same shared key. To configure shared keys for different HWTACACS servers, run the **19.3.8 hwtacacs-server authentication**, **19.3.9 hwtacacs-server authorization**, and **19.3.6 hwtacacs-server accounting** commands.

If no shared key is configured in the HWTACACS server template, run the **hwtacacs-server shared-key** command in the system view to configure it. The shared key configured in the system view is valid for all HWTACACS server templates.

Precautions

To improve security, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.

To be compatible with the earlier versions, the device supports the shared key of 20 characters in cipher text. The length of the shared key cannot be configured.

The HWTACACS shared keys are used in the following order:

1. Shared key of the HWTACACS authentication, authorization, and accounting server with the specified IP address configured in the HWTACACS server template view
2. Shared key of the HWTACACS server configured in the HWTACACS server template view
3. Shared key of the HWTACACS server configured in the system view
4. If there is no available shared key of HWTACACS server, the system considers that the operation failed.

Example

Set the shared key of the HWTACACS server to **Admin@123**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server shared-key cipher Admin@123
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.12 hwtacacs-server source-ip

Function

The **hwtacacs-server source-ip** command specifies the source IPv4 address used by a device to communicate with an HWTACACS server.

The **undo hwtacacs-server source-ip** command cancels the configuration.

By default, the device uses the IPv4 address of the actual outbound interface as the source IPv4 address encapsulated in HWTACACS packets.

Format

hwtacacs-server source-ip *ip-address*

hwtacacs-server source-ip source-loopback *interface-number*

undo hwtacacs-server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address for communication between the device and HWTACACS server.	The value is a valid unicast address in dotted decimal notation.
source-loopback *interface-number*	Specifies the IPv4 address of the LoopBack interface as the source IPv4 address for communication between the device and HWTACACS server.	The loopback interface must already exist.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

You can configure all HWTACACS packets sent by the device to use the same source IPv4 address. In this way, an HWTACACS server uses only one IPv4 address to communicate with the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify the source IPv4 address 10.1.1.1 for communication between the device and HWTACACS server.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server source-ip 10.1.1.1
```

Related Topics

19.3.2 display hwtacacs-server template
19.3.14 hwtacacs-server template

19.3.13 hwtacacs-server source-ipv6

Function

The **hwtacacs-server source-ipv6** command specifies the source IPv6 address used by a device to communicate with an HWTACACS server.

The **undo hwtacacs-server source-ipv6** command cancels the configuration.

By default, the device uses the IPv6 address of the actual outbound interface as the source IPv6 address encapsulated in HWTACACS packets.

Format

hwtacacs-server source-ipv6 *ipv6-address*

hwtacacs-server source-ipv6 source-loopback *interface-number*

undo hwtacacs-server source-ipv6

Parameters

Parameter	Description	Value
ipv6-address	Specifies the source IPv6 address for communicating with the HWTACACS server.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
source-loopback *interface-number*	Configures a loopback interface as the source IPv6 address for communicating with the HWTACACS server.	The loopback interface must already exist.

Views

HWTACACS server template view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

After you specify the source IPv6 address in HWTACACS packets, the device uses this IPv6 address to communicate with the HWTACACS server.

Example

Specify the source IPv6 address fc00::1 in HWTACACS packets.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server source-ipv6 fc00::1
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

Function

The **hwtacacs-server template** command creates an HWTACACS server template and enters the HWTACACS server template view.

The **undo hwtacacs-server template** command deletes an HWTACACS server template.

By default, no HWTACACS server template is configured.

Format

hwtacacs-server template *template-name*

undo hwtacacs-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The value is a string of 1 to 32 case-sensitive characters. The name contains only letters, digits (0-9), dots (.), underscores (_) and hyphens (-), and a combination of the above characters. The value cannot be - or --.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can perform HWTACACS configurations, such as the configuration of authentication servers, authorization servers, accounting servers, and shared key, only after an HWTACACS server template is created.

Follow-up Procedure

Configure an authentication server, accounting server, and shared key in the HWTACACS server template view, and run the **19.3.5 hwtacacs-server** command in the domain view to apply the HWTACACS server template.

Precautions

You can modify the content of a template or delete a template only when the template is not in use.

Example

Create an HWTACACS server template **template1** and enter the HWTACACS server template view.

```
<Huawei> system-view
[Huawei] hwtacacs-server template template1
[Huawei-hwtacacs-template1]
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.5 hwtacacs-server

19.3.15 hwtacacs-server timer quiet

Function

The **hwtacacs-server timer quiet** command sets the quiet interval before the primary server reverts to the active state.

The **undo hwtacacs-server timer quiet** command restores the default quiet interval before the primary server reverts to the active state.

By default, the quiet interval before the primary HWTACACS server reverts to the active state is 5 minutes.

Format

hwtacacs-server timer quiet *interval*

 Copyright © Huawei Technologies Co., Ltd.

undo hwtacacs-server timer quiet

Parameters

Parameter	Description	Value
interval	Specifies the quiet interval before the primary server reverts to the active state.	The value is an integer ranging from 0 to 255, in minutes.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the primary server is unavailable, the device automatically switches services to the standby server and sends packets to the standby server. After the quiet interval before the primary server reverts to the active state expires, the device attempts to establish a connection with the primary server.

- If the primary server is still unavailable, the device continues to send packets to the standby server until the next interval expires. Such a process repeats.
- If the primary server is available, the device switches services to the primary server and sends packets to the primary server.

The quiet interval before the primary server reverts to the active state ensures that the primary server can be restored immediately and reduces the number of detection times during the switchover.

The default value is recommended.

Precautions

When the quiet interval of the active server is set to 0, if the active server fails, the device sends packets to the standby server. When the active server is recovered, the device does not connect to the active server, but still sends packets to the standby server until the standby server fails.

When you run the **hwtacacs-server timer quiet** command to change the quiet interval before the primary server reverts to the active state, the device does not check whether the HWTACACS server template is in use.

Example

Set the quiet interval before the primary server reverts to the active state to 3 minutes.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] hwtacacs-server template template1
[Huawei-hwtacacs-template1] hwtacacs-server timer quiet 3
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.16 hwtacacs-server timer response-timeout

Function

The **hwtacacs-server timer response-timeout** command sets the response timeout interval of an HWTACACS server.

The **undo hwtacacs-server timer response-timeout** command restores the default response timeout interval of an HWTACACS server.

By default, the response timeout interval for an HWTACACS server is 5 seconds.

Format

hwtacacs-server timer response-timeout *interval*

undo hwtacacs-server timer response-timeout

Parameters

Parameter	Description	Value
interval	Specifies the response timeout interval of an HWTACACS server.	The value is an integer ranging from 1 to 300, in seconds.

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the device sends a request packet to the HWTACACS server, if the device does not receive any response packet from the server within the specified response timeout interval:

- If only one HWTACACS server is configured, the device does not retransmit the request to this server.
- If both active/standby HWTACACS servers are available and the TCP link between them works normally, the device retransmits the request to the

standby server after timeout. If the TCP link is broken during the timeout interval, the device immediately retransmits the request to the standby server.

This improves reliability of HWTACACS authentication, authorization, and accounting.

The default value is recommended.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

Example

Set the response timeout interval of an HWTACACS server to 30s.

```
<Huawei> system-view
[Huawei] hwtacacs-server template test1
[Huawei-hwtacacs-test1] hwtacacs-server timer response-timeout 30
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.17 hwtacacs-server traffic-unit

Function

The **hwtacacs-server traffic-unit** command sets the traffic unit used by an HWTACACS server.

The **undo hwtacacs-server traffic-unit** command restores the default traffic unit used by the HWTACACS server.

By default, the traffic unit is byte on the device.

Format

hwtacacs-server traffic-unit { **byte** | **kbyte** | **mbyte** | **gbyte** }

undo hwtacacs-server traffic-unit

Parameters

Parameter	Description	Value
byte	Indicates that the traffic unit is byte.	-
kbyte	Indicates that the traffic unit is KByte.	-
mbyte	Indicates that the traffic unit is MByte.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
gbyte	Indicates that the traffic unit is GByte.	-

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Different HWTACACS servers may use different traffic units; therefore, you need to set the traffic unit for each HWTACACS server group on the device and the traffic unit must be the same as that on the HWTACACS server.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

Example

Set the traffic unit used by an HWTACACS server to KByte.

```
<Huawei> system-view
[Huawei] hwtacacs-server template template1
[Huawei-hwtacacs-template1] hwtacacs-server traffic-unit kbyte
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.14 hwtacacs-server template

19.3.18 hwtacacs-server user-name domain-included

Function

The **hwtacacs-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in HWTACACS packets to be sent to an HWTACACS server.

The **hwtacacs-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to the HWTACACS server.

The **undo hwtacacs-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

 Copyright © Huawei Technologies Co., Ltd.

By default, the device does not modify the user name entered by the user in the packets sent to the HWTACACS server.

Format

hwtacacs-server user-name domain-included

hwtacacs-server user-name original

undo hwtacacs-server user-name domain-included

Parameters

None

Views

HWTACACS server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter.

If the HWTACACS server does not accept the user name with the domain name, run the **undo hwtacacs-server user-name domain-included** command to delete the domain name from the user name.

Precautions

You can modify this configuration only when the HWTACACS server template is not in use.

If the user names in the HWTACACS packets sent from the device to HWTACACS server contain domain names, ensure that the total length of a user name (user name + domain name delimiter + domain name) is not longer than 64 characters; otherwise, the user name cannot be contained in HWTACACS packets. As a result, authentication will fail.

Example

Configure the device to encapsulate the domain name in the user name when sending HWTACACS packets to an HWTACACS server.

```
<Huawei> system-view
[Huawei] hwtacacs-server template template1
[Huawei-hwtacacs-template1] hwtacacs-server user-name domain-included
```

Related Topics

19.3.2 display hwtacacs-server template

19.3.19 hwtacacs-user change-password hwtacacs-server

Function

The **hwtacacs-user change-password hwtacacs-server** command enables the device to change the passwords saved on the HWTACACS server.

Format

hwtacacs-user change-password hwtacacs-server *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HWTACACS server template.	The HWTACACS server template must already exist.

Views

User view

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

To change the password saved on the HWTACACS server, users can run the **hwtacacs-user change-password hwtacacs-server** command on the device. You do not need to change the configuration on the HWTACACS server.

Precautions

- Users are HWTACACS authenticated and the HWTACACS server template is configured.
- Users can run this command to change the passwords only when the user names and passwords saved on the HWTACACS do not expire. When a user whose password has expired logs in to the device, the HWTACACS server does not allow the user to change the password and displays a message indicating that the authentication fails.
- The system wait period is 30 seconds. If the TACACS server does not receive the user name, new password, or confirmed password from the user within such a period, it terminates the password change process.
- Users can also press **Ctrl+C** to cancel password change.
- HWTACACS users who pass AAA authentication can use the **hwtacacs-user change-password hwtacacs-server** command to change the passwords

 Copyright © Huawei Technologies Co., Ltd.

before the passwords expire. If a user needs to run this command to change the passwords of other users, the user must have the system rights.

Example

Enable the user that passes HWTACACS authentication to change the password.

```
<Huawei> hwtacacs-user change-password hwtacacs-server huawei
Username:cj@huawei
Old Password:
New Password:
Re-enter New password:
Info: The password has been changed successfully.
```

19.3.20 reset hwtacacs-server accounting-stop-packet

Function

The **reset hwtacacs-server accounting-stop-packet** command clears statistics on the remaining buffer information of HWTACACS accounting-stop packets.

Format

reset hwtacacs-server accounting-stop-packet { **all** | **ip** { *ipv4-address* | *ipv6-address* } }

Parameters

Parameter	Description	Value
all	Clears statistics on the remaining buffer information of HWTACACS accounting-stop packets.	-
ip *ipv4-address*	Clears the statistics about the Accounting-Stop packets sent by the HWTACACS server with a specified IPv4 address.	The value is in dotted decimal notation.
ip *ipv6-address*	Clears the remaining buffer information about Accounting-Stop packets sent by the HWTACACS server with a specified IPv6 address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

This command can clear statistics on the remaining buffer information of HWTACACS accounting-stop packets. The deleted statistics cannot be restored.

Example

Clear statistics on the remaining buffer information of all HWTACACS accounting-stop packets.

```
<Huawei> reset hwtacacs-server accounting-stop-packet all
```

Related Topics

19.3.1 display hwtacacs-server accounting-stop-packet

19.3.21 reset hwtacacs-server statistics

Function

The **reset hwtacacs-server statistics** command clears the statistics on HWTACACS authentication, accounting, and authorization.

Format

reset hwtacacs-server statistics { **all** | **accounting** | **authentication** | **authorization** }

Parameters

Parameter	Description	Value
all	Clears all the statistics.	-
accounting	Clears the statistics on HWTACACS accounting.	-
authentication	Clears the statistics on HWTACACS authentication.	-
authorization	Clears the statistics on HWTACACS authorization.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If statistics about HWTACACS authentication, accounting, and authorization need to be collected in a specified period of time, you must clear the original statistics first.

Precautions

- After the **reset hwtacacs-server statistics** command is run, all the statistics about HWTACACS authentication, accounting, and authorization is cleared. In addition, the statistics cannot be restored once being cleared. Therefore, exercise caution when you decide to run this command.
- You can run the **display hwtacacs-server template** *template-name* **verbose** command to check statistics about HWTACACS authentication, accounting, and authorization in the specified server template.

Example

Clear all the statistics.

```
<Huawei> reset hwtacacs-server statistics all
```

Related Topics

19.3.2 display hwtacacs-server template

19.4 HACA Configuration Commands

19.4.1 display haca-server accounting-stop-packet all

Function

The **display haca-server accounting-stop-packet all** command displays information about all accounting-stop packets on the HACA server.

Format

display haca-server accounting-stop-packet all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display haca-server accounting-stop-packet all** command output helps you check configurations or locate HACA server faults.

Example

View information about all accounting-stop packets on the HACA server.

```
<Huawei> display haca-server accounting-stop-packet all
-----------------------------------------------------------------------------
 Time Stamp  Resend Times  Session Time
Username
 -----------------------------------------------------------------------------
 3245884970  32           49           123
 -----------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 19-35 Description of the **display haca-server accounting-stop-packet all** command output

Item	Description
Time Stamp	Timestamp of an accounting-stop packet.
Resend Times	Number of times that accounting-stop packets have been retransmitted.
Session Time	Session time, in seconds.
Username	User name.

Related Topics

19.4.6 haca-server accounting-stop-packet resend

19.4.17 reset haca-server accounting-stop-packet all

19.4.2 display haca-server configuration

Function

The **display haca-server configuration** command displays the configurations of HACA server templates.

Format

display haca-server configuration [**template** *template-name*]

Parameters

Parameter	Description	Value
template *template-name*	Specifies the name of an HACA server template. If this parameter is not specified, the configuration of all the HACA server templates is displayed.	The HACA server template must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display haca-server configuration** command output helps you check the configuration of HACA server templates or troubleshoot HACA.

Example

Display the configurations of HACA server templates.

```
<Huawei> display haca-server configuration
  ------------------------------------------------------------------------------
  HACA-server template name                  : haca
  HACA-server server-ip-address(port)        : 10.22.85.246(50300)
  HACA-server pki-realm-name                 : default
  HACA-server Status                         : REGISTE
  HACA-server source-ip-address              : -
  HACA-server down-delay-interval(sec)       : 30
  HACA-server response-timeout-interval(sec) : 5
  HACA-server domain-included                : ORIGINAL
  HACA-server heart-beat-interval(min)       : 20
  HACA-server reconnection-interval(min)     : 1
  HACA-server user-syn-interval(min)         : 9
  HACA-server server-escape-state            : 0
  HACA-server accounting-stop-packet resend  : 3
  ------------------------------------------------------------------------------
  Total 1,1 printed
```

Table 19-36 Description of the **display haca-server configuration** command output

Item	Description
HACA-server template name	Name of the HACA server template. To create an HACA server template, run the **haca-server template** command.

Item	Description
HACA-server server-ip-address(port)	IP address and port number of the HACA server. To set the IP address and port number for the HACA server, run the **19.4.7 haca-server server-address** command.
HACA-server pki-realm-name	Name of a PKI domain of the HACA server. To set the name of a PKI domain of the HACA server, run the **19.4.7 haca-server server-address** command.
HACA-server Status	Status of the HACA server. The values are as follows: ● IDLE: indicates the idle state. ● INIT: indicates the initial state. ● UP: indicates the UP state. ● REGISTE: indicates the registration state. ● DOWN: indicates the DOWN state.
HACA-server source-ip-address	Source IP address of HACA packets. To set the source IP address of HACA packets, run the **19.4.8 haca-server source-ip** command.
HACA-server down-delay-interval(sec)	Delay interval for HACA server to restart from the DOWN state, in seconds. To set the delay interval, run the **19.4.10 haca-server timer down-delay** command.
HACA-server response-timeout-interval(sec)	Timeout period for the HACA server to send reply packets, in seconds. To set the timeout period, run the **19.4.13 haca-server timer response-timeout** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
HACA-server domain-included	Format of HACA user name. It specifies whether the user name sent to the HACA server contains a domain name. ● YES: indicates that the user name contains the domain name. ● NO: indicates that the user name does not contain the domain name. ● ORIGINAL: indicates that the device does not modify the user name entered by the user. To set the user name format, run the **19.4.15 haca-server user-name** command.
HACA-server heart-beat-interval(min)	Interval for the HACA server to send heartbeat packets, in minutes. To set the heartbeat interval, run the **19.4.11 haca-server timer heart-beat** command.
HACA-server reconnection-interval(min)	Interval for the HACA server to be reconnected, in minutes. To set the reconnection interval, run the **19.4.12 haca-server timer reconnection** command.
HACA-server user-syn-interval(min)	Interval for synchronizing HACA user information, in minutes. To set the synchronization interval, run the **19.4.14 haca-server timer user-syn** command.
HACA-server server-escape-state	Escape state of HACA. ● 0: indicates that the server is in the UP state, and the best-effort path will not be used. ● 1: indicates that the server is in the DOWN state, and the best-effort path is being prepared. ● 2: indicates that the server is in the initial state, and the best-effort path will not be used.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
HACA-server accounting-stop-packet resend	Number of times HACA accounting-stop packets are retransmitted. To set the number of times HACA accounting-stop packets can be retransmitted, run the **19.4.6 haca-server accounting-stop-packet resend** command.

19.4.3 display haca-server statistics

Function

The **display haca-server statistics** command displays HACA packet statistics.

Format

display haca-server statistics { **all** | **message** | **packet** [**authentication** | **authorization** | **accounting** | **cut-notify** | **cut-request** | **register** | **user-syn**] } [**template** *template-name*]

Parameters

Parameter	Description	Value
all	Displays statistics about all packets.	-
message	Displays statistics about messages.	-
packet	Displays statistics about the specified type of packets.	-
authentication	Displays statistics about authentication packets.	-
authorization	Displays statistics about authorization packets.	-
accounting	Displays statistics about accounting packet.	-
cut-notify	Displays statistics about logout notification packets.	-
cut-request	Displays statistics about logout request packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
register	Displays statistics about registration packets.	-
user-syn	Displays statistics about user synchronization packets.	-
template *template-name*	Displays packet statistics about the specified HACA server template.	The HACA server template must exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

During fault location, you can run this command to view statistics about HACA packets.

Example

Display HACA packet statistics.

```
<Huawei> display haca-server statistics all
  ------------------------------------------------------------
  Haca-server Template haca Statistics:
  ------------------------------------------------------------
  Authen_Request_Messages                    = 0
  Authen_Accept_Messages                     = 0
  Authen_Reject_Messages                     = 0
  Author_Request_Messages                    = 0
  Author_Accept_Messages                     = 0
  Author_Reject_Messages                     = 0
  Coa_Request_Messages                       = 0
  Coa_Accept_Messages                        = 0
  Coa_Reject_Messages                        = 0
  Account_Start_Messages                     = 0
  Account_RT_Messages                        = 0
  Account_Stop_Messages                      = 0
  Account_StartAck_Messages                  = 0
  Account_RTAck_Messages                     = 0
  Account_StopAck_Messages                   = 0
  Account_StartAckFail_Messages              = 0
  Account_RTAckFail_Messages                 = 0
  Account_StopAckFail_Messages               = 0
  UserSyn_Request_To_Server_Messages         = 0
  UserSyn_Response_From_Server_Messages      = 0
  UserSyn_Request_From_Server_Messages       = 0
  UserSyn_Response_To_Server_Messages        = 0
  Cut_Request_Messages                       = 0
  Cut_Response_Messages                      = 0
  Cut_Notify_Messages                        = 0
  Send_to_HacaServer_RegRequest_Packets      = 0
```

```
Received_from_HacaServer_RegResponse_Packets          = 0
Error_Send_to_HacaServer_RegRequest_Packets           = 0
Error_Received_from_HacaServer_RegResponse_Packets    = 0
Send_to_HacaServer_AuthenRequest_Packets              = 0
Received_from_HacaServer_AuthenAccept_Packets         = 0
Received_from_HacaServer_AuthenReject_Packets         = 0
Error_Send_to_HacaServer_AuthenRequest_Packets        = 0
Error_Received_from_HacaServer_AuthenAccept_Packets   = 0
Error_Received_from_HacaServer_AuthenReject_Packets   = 0
Received_from_HacaServer_AuthorRequest_Packets        = 0
Send_to_HacaServer_AuthorAccept_Packets               = 0
Send_to_HacaServer_AuthorReject_Packets               = 0
Error_Received_from_HacaServer_AuthorRequest_Packets  = 0
Error_Send_to_HacaServer_AuthorAccept_Packets         = 0
Error_Send_to_HacaServer_AuthorReject_Packets         = 0
Received_from_HacaServer_CoaRequest_Packets           = 0
Send_to_HacaServer_CoaAccept_Packets                  = 0
Send_to_HacaServer_CoaReject_Packets                  = 0
Error_Received_from_HacaServer_CoaRequest_Packets     = 0
Error_Send_to_HacaServer_CoaAccept_Packets            = 0
Error_Send_to_HacaServer_CoaReject_Packets            = 0
Received_from_HacaServer_AcctSucc_Packets             = 0
Send_to_HacaServer_AcctSend_Packets                   = 0
Error_Received_from_HacaServer_AcctFail_Packets       = 0
Error_Send_to_HacaServer_AcctSendFail_Packets         = 0
Send_to_HacaServer_UserSynRequest_Packets             = 0
Received_from_HacaServer_UserSynResponse_Packets      = 0
Send_to_HacaServer_UserSynRespons_Packets             = 0
Received_from_HacaServer_UserSynRequest_Packets       = 0
Error_Send_to_HacaServer_UserSynRequest_Packets       = 0
Error_Received_from_HacaServer_UserSynResponse_Packets = 0
Error_Send_to_HacaServer_UserSynRespons_Packets       = 0
Error_Received_from_HacaServer_UserSynRequest_Packets = 0
Send_to_HacaServer_CutNotify_Packets                  = 0
Error_Send_to_HacaServer_CutNotify_Packets            = 0
Received_from_HacaServer_CutRequest_Packets           = 0
Send_to_HacaServer_CutResponse_Packets                = 0
Error_Received_from_HacaServer_CutRequest_Packets     = 0
Error_Send_to_HacaServer_CutResponse_Packets          = 0
-------------------------------------------------------------
```

Table 19-37 Description of the **display haca-server statistics** command output

Item	Description
Haca-server Template haca Statistics	Statistics about the HACA server template haca.
Authen_Request_Messages	Statistics about authentication request messages.
Authen_Accept_Messages	Statistics about access-accept messages.
Authen_Reject_Messages	Statistics about access-reject messages.
Author_Request_Messages	Statistics about authorization request messages.
Author_Accept_Messages	Statistics about authorization-accept messages.

Item	Description
Author_Reject_Messages	Statistics about authorization-reject messages.
Coa_Request_Messages	Statistics about CoA request messages.
Coa_Accept_Messages	Statistics about CoA-accept messages.
Coa_Reject_Messages	Statistics about CoA-reject messages.
Account_Start_Messages	Statistics about accounting-start request messages.
Account_RT_Messages	Statistics about real-time accounting request messages.
Account_Stop_Messages	Statistics about accounting-stop request messages.
Account_StartAck_Messages	Statistics about accounting-start response success messages.
Account_RTAck_Messages	Statistics about real-time accounting response success messages.
Account_StopAck_Messages	Statistics about accounting-stop response success messages.
Account_StartAckFail_Messages	Statistics about accounting-start response failure messages.
Account_RTAckFail_Messages	Statistics about real-time accounting response failure messages.
Account_StopAckFail_Messages	Statistics about accounting-stop response failure messages.
UserSyn_Request_To_Server_Messages	Statistics about user synchronization request messages sent to the HACA server.
UserSyn_Response_From_Server_Messages	Statistics about user synchronization response messages received from the HACA server.
UserSyn_Request_From_Server_Messages	Statistics about user synchronization request messages received from the HACA server.
UserSyn_Response_To_Server_Messages	Statistics about user synchronization response messages sent to the HACA server.
Cut_Request_Messages	Statistics about logout request messages.
Cut_Response_Messages	Statistics about logout response messages.
Cut_Notify_Messages	Statistics about logout notification messages.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Send_to_HacaServer_RegRequest_Packets	Statistics about registration request messages sent to the HACA server.
Received_from_HacaServer_RegResponse_Packets	Statistics about registration response messages received from the HACA server.
Error_Send_to_HacaServer_RegRequest_Packets	Statistics about error registration request messages sent to the HACA server.
Error_Received_from_HacaServer_RegResponse_Packets	Statistics about error registration response messages received from the HACA server.
Send_to_HacaServer_AuthenRequest_Packets	Statistics about authentication request messages sent to the HACA server.
Received_from_HacaServer_AuthenAccept_Packets	Statistics about authentication response messages received from the HACA server.
Received_from_HacaServer_AuthenReject_Packets	Statistics about access-reject messages received from the HACA server.
Error_Send_to_HacaServer_AuthenRequest_Packets	Statistics about error authentication request messages sent to the HACA server.
Error_Received_from_HacaServer_AuthenAccept_Packets	Statistics about error authentication response messages received from the HACA server.
Error_Received_from_HacaServer_AuthenReject_Packets	Statistics about error access-reject messages received from the HACA server.
Received_from_HacaServer_AuthorRequest_Packets	Statistics about authorization request messages received from the HACA server.
Send_to_HacaServer_AuthorAccept_Packets	Statistics about authorization response messages sent to the HACA server.
Send_to_HacaServer_AuthorReject_Packets	Statistics about authorization-reject messages sent to the HACA server.
Error_Received_from_HacaServer_AuthorRequest_Packets	Statistics about error authorization request messages received from the HACA server.
Error_Send_to_HacaServer_AuthorAccept_Packets	Statistics about error authorization response messages sent to the HACA server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Error_Send_to_HacaServer_AuthorReject_Packets	Statistics about error authorization-reject messages sent to the HACA server.
Received_from_HacaServer_CoaRequest_Packets	Statistics about CoA request messages received from the HACA server.
Send_to_HacaServer_CoaAccept_Packets	Statistics about CoA response messages sent to the HACA server.
Send_to_HacaServer_CoaReject_Packets	Statistics about CoA-reject messages sent to the HACA server.
Error_Received_from_HacaServer_CoaRequest_Packets	Statistics about error CoA request messages received from the HACA server.
Error_Send_to_HacaServer_CoaAccept_Packets	Statistics about error CoA response messages sent to the HACA server.
Error_Send_to_HacaServer_CoaReject_Packets	Statistics about error CoA-reject messages sent to the HACA server.
Received_from_HacaServer_AcctSucc_Packets	Statistics about the received accounting response success messages.
Send_to_HacaServer_AcctSend_Packets	Statistics about the sent accounting request success messages.
Error_Received_from_HacaServer_AcctFail_Packets	Statistics about the received accounting request failure messages.
Error_Send_to_HacaServer_AcctSendFail_Packets	Statistics about the sent accounting request failure messages.
Send_to_HacaServer_UserSynRequest_Packets	Statistics about user synchronization request messages sent to the HACA server.
Received_from_HacaServer_UserSynResponse_Packets	Statistics about user synchronization response messages received from the HACA server.
Send_to_HacaServer_UserSynRespons_Packets	Statistics about user synchronization response messages sent to the HACA server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Received_from_HacaServer_UserSynRequest_Packets	Statistics about user synchronization request messages received from the HACA server.
Error_Send_to_HacaServer_UserSynRequest_Packets	Statistics about error user synchronization request messages sent to the HACA server.
Error_Received_from_HacaServer_UserSynResponse_Packets	Statistics about error user synchronization response messages received from the HACA server.
Error_Send_to_HacaServer_UserSynRespons_Packets	Statistics about error user synchronization response messages sent to the HACA server.
Error_Received_from_HacaServer_UserSynRequest_Packets	Statistics about error user synchronization request messages received from the HACA server.
Send_to_HacaServer_CutNotify_Packets	Statistics about user logout notification messages sent to the HACA server.
Error_Send_to_HacaServer_CutNotify_Packets	Statistics about error user logout notification messages sent to the HACA server.
Received_from_HacaServer_CutRequest_Packets	Statistics about error user logout request messages received from the HACA server.
Send_to_HacaServer_CutResponse_Packets	Statistics about user logout request messages sent to the HACA server.
Error_Received_from_HacaServer_CutRequest_Packets	Statistics about error user logout request messages received from the HACA server.
Error_Send_to_HacaServer_CutResponse_Packets	Statistics about error user logout response messages sent to the HACA server.

19.4.4 haca enable

Function

The **haca enable** command enables the HACA function.

The **undo haca enable** command disables the HACA function.

By default, HACA is disabled.

Format

haca enable

undo haca enable

Parameters

None

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

In the cloud management scenario, users are authenticated through Portal. The authentication server is located on the cloud, so packets between the device and server must traverse the NAT device. However, Portal protocol packets cannot traverse the NAT device. HACA implements communication between the device and server, and then Portal authentication can be performed.

If you require HACA authentication, run the **haca enable** command to enable HACA.

Prerequisites

The IP address and port number of the HACA server have been configured using the **19.4.7 haca-server server-address** command.

Example

Enable HACA.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei] haca-server server-address 10.1.1.1 default
[Huawei-haca-haca] haca enable
```

19.4.5 haca-server (AAA domain view)

Function

The **haca-server** command applies an HACA server template to a domain.

The **undo haca-server** command unbinds an HACA server template from a domain.

By default, no HACA server template is configured in a domain.

 Copyright © Huawei Technologies Co., Ltd.

Format

haca-server *template-name*

undo haca-server

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HACA server template.	The HACA server template must exist.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To perform HACA authentication for users in a domain, apply an HACA server template to the domain. An HACA server template takes effect only after the HACA server template is applied to the domain.

Precautions

An HACA server template has been created by using the **haca-server template** command.

Example

Apply the HACA server template **haca** to the domain **huawei**.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] quit
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] haca-server haca
```

19.4.6 haca-server accounting-stop-packet resend

Function

The **haca-server accounting-stop-packet resend** command enables retransmission of accounting-stop packets and sets the number of accounting-stop packets that can be retransmitted.

The **undo haca-server accounting-stop-packet resend** command disables retransmission of accounting-stop packets.

 Copyright © Huawei Technologies Co., Ltd.

By default, three accounting-stop packets can be retransmitted.

Format

haca-server accounting-stop-packet resend [*resend-times*]

undo haca-server accounting-stop-packet resend

Parameters

Parameter	Description	Value
resend-times	Specifies the number of retransmitted accounting-stop packets.	The value is an integer that ranges from 0 to 300.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

Accounting-stop packets cannot be forwarded to an HACA server that is unreachable. You can run the **haca-server accounting-stop-packet resend** command to save the accounting-stop packets in the buffer and send them at the preset intervals until the number of allowed retransmission times is reached or the packets are sent successfully.

You can modify the configuration only when the HACA server template is not in use.

Example

Enable the retransmission of accounting-stop packets and set the number of accounting-stop packets that can be retransmitted to 50.

```
<Huawei> system-view
[Huawei] haca-server template test1
[Huawei-haca-test1] haca-server accounting-stop-packet resend 50
```

19.4.7 haca-server server-address

Function

The **haca-server server-address** command configures the IP address and port number for the HACA server.

The **undo haca-server server-address** command deletes the IP address and port number configured for the HACA server.

By default, the IP address and port number of the HACA server are not configured on the device.

Format

haca-server server-address *ip-address* [*port*] *pki-realm-name*

undo haca-server server-address [*ip-address* [*port*]]

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an HACA server.	The value is in dotted decimal notation. It must be a valid unicast address.
port	Specifies the port number of an HACA server. If the parameter is not specified, the default value is used.	The value is an integer that ranges from 1 to 65535. The default value is 50300.
pki-realm-name	Specifies the name of a PKI domain.	The value must be an existing PKI domain name.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

The device needs to be connected to an HACA server for authentication. The HACA server is located on the Internet. Therefore, the device sends authentication packets to the HACA server only after the IP address and port number of the HACA server are specified.

Example

Configure the IP address of the HACA server to 10.1.1.1.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server server-address 10.1.1.1 default
```

19.4.8 haca-server source-ip

Function

The **haca-server source-ip** command configures a source IP address for the device to communicate with an HACA server.

The **undo haca-server source-ip** restores the default setting.

By default, no source IP address is configured for HACA packets. The device uses the IP address of the actual outbound interface as the source IP address of HACA packets.

Format

haca-server source-ip *ip-address*

undo haca-server source-ip

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with an HACA server.	The value is in dotted decimal notation. It must be a valid unicast address.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

To communicate with an HACA server, the device sends packets encapsulated with source IP addresses. By default, the device uses the IP addresses of the actual outbound interfaces as the source IP address. This leads to a waste of IP addresses, and complicates the configuration. To simplify the configuration, run the **haca-server source-ip** command to set a same source IP address for all HACA packets. In this way, the HACA server can use only one IP address to communicate with the device.

Example

Set the source IP address for communication between the device and an HACA server to 10.1.1.1.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server source-ip 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

19.4.9 haca-server template

Function

The **haca-server template** command creates an HACA server template and displays the HACA server template view.

The **undo haca-server template** command deletes an HACA server template.

By default, no HACA server template is created.

Format

haca-server template *template-name*

undo haca-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an HACA server template.	The value is a string of 1 to 32 case-sensitive characters. The name contains only letters, digits (0-9), dots (.), underscores (_) and hyphens (-). It cannot be - or --.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To configure HACA authentication, you must create an HACA server template. You can perform HACA configurations, such as setting the IP address and interval of HACA heartbeat packets, only after an HACA server template is created.

Follow-up Procedure

After creating an HACA template, set the HACA server IP address and interval of the HACA heartbeat packets in the HACA server template view, and perform other configurations. Then, run the **19.4.5 haca-server (AAA domain view)** in the domain view to apply the HACA server template.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an HACA server template **haca** and display the HACA server template view.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca]
```

19.4.10 haca-server timer down-delay

Function

The **haca-server timer down-delay** command sets the delay after which an HACA server is disconnected.

The **undo haca-server timer down-delay** command restores the default delay in which an HACA server is disconnected.

By default, the delay after which an HACA server is disconnected is 30s.

Format

haca-server timer down-delay *interval*

undo haca-server timer down-delay

Parameters

Parameter	Description	Value
interval	Specifies the delay after which an HACA server is disconnected.	The value is an integer that ranges from 0 to 600, in seconds. Value 0 indicates that no delay is set for HACA server disconnection.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

If the communication between an HACA server and an access device is interrupted, authenticated users enter best-effort paths. That is, the users are allowed to access the network and will be reauthenticated after the communication re-establishes. If the HACA server is disconnected and connected

frequently in a short period, a large number of users will be reauthenticated, which consumes device resources.

Therefore, set the delay after which an HACA server is disconnected to enable best-effort paths during the interval. When communication between the access devices and server is interrupted, the previously authenticated users will not be reauthenticated until the delay ends. This setting prevents resource exhaustion caused by frequent disconnection and reconnection.

Example

Set the delay after which an HACA server is disconnected to 60s.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server timer down-delay 60
```

19.4.11 haca-server timer heart-beat

Function

The **haca-server timer heart-beat** command sets the interval for sending HACA heartbeat packets.

The **undo haca-server timer heart-beat** command restores the default value of the interval for sending HACA heartbeat packets.

By default, the interval for sending HACA heartbeat packets is 5 minutes.

Format

haca-server timer heart-beat *interval*

undo haca-server timer heart-beat

Parameters

Parameter	Description	Value
interval	Specifies the interval at which HACA heartbeat packets are sent.	The value is an integer that ranges from 1 to 1440, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

A firewall may exist between the access device and HACA server. If the firewall does not detect packets for a long time, it may interrupt the connection. Run the

haca-server timer heart-beat command to set the interval at which the client sends HACA heartbeat packets to ensure a proper connection.

Example

Set the interval for sending HACA heartbeat packets to 6 minutes.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server timer heart-beat 6
```

19.4.12 haca-server timer reconnection

Function

The **haca-server timer reconnection** command sets the reconnection interval for an HACA server.

The **undo haca-server timer down-detection** command restores the default value of the reconnection interval for an HACA server.

By default, the interval for reconnecting to an HACA server is one minute.

Format

haca-server timer reconnection *interval*

undo haca-server timer reconnection

Parameters

Parameter	Description	Value
interval	Specifies the interval for reconnecting to an HACA server.	The value is an integer that ranges from 1 to 255, in minutes.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

If the communication between an access device and an HACA server is interrupted, the device reconnects to the server immediately. If that reconnection fails, the device reconnects to HACA at the HACA reconnection interval until the connection succeeds.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the reconnection interval for the HACA server to 2 minutes.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server timer reconnection 2
```

19.4.13 haca-server timer response-timeout

Function

The **haca-server timer response-timeout** command sets the response timeout interval for an HACA server.

The **undo haca-server timer response-timeout** command restores the default value of the response timeout interval for an HACA server.

By default, the response timeout interval for an HACA server is 5 seconds.

Format

haca-server timer response-timeout *interval*

undo haca-server timer response-timeout

Parameters

Parameter	Description	Value
interval	Specifies the response timeout interval of an HACA server.	It is an integer that ranges from 1 to 300, in seconds.

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

A device may not receive the response packets from HACA after sending request packets to the server. After a response timeout interval is set, if a device does not receive response packets from the HACA server in that specified time after sending request packets, the device will send request packets again. This improves the reliability of HACA authentication.

Example

Set the response timeout interval for an HACA server to 30s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server timer response-timeout 30
```

19.4.14 haca-server timer user-syn

Function

The **haca-server timer user-syn** command sets the interval for synchronizing user information for an HACA server.

The **undo haca-server timer user-syn** command restores the default value of the interval for synchronizing user information for an HACA server.

By default, the user information synchronization interval for an HACA server is 10 minutes.

Format

haca-server timer user-syn *interval*

undo haca-server timer user-syn

Parameters

Parameter	Description	Value
interval	Specifies the user information synchronization interval for an HACA server.	The value can be 0 or range from 3 to 65535, in minutes. The value **0** indicates that user information synchronization is disabled.

Views

System view

Default Level

3: Management level

Usage Guidelines

In HACA authentication application, if communication between the device and HACA server is interrupted due to a network failure or HACA server failure, online HACA users cannot go offline normally. As a result, user information on the device may be different from that on the HACA server, causing inaccurate accounting. Run the **haca-server timer user-syn** *interval* command to enable user information synchronization. Then user information will be synchronized between the device and HACA server at the interval, which ensures user information consistency.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the user information synchronization interval for the HACA server to 30 minutes.

```
<Huawei> system-view
[Huawei] haca-server timer user-syn 30
```

19.4.15 haca-server user-name

Function

The **haca-server user-name domain-included** command configures the device to encapsulate the domain name in the user name in HACA packets to be sent to an HACA server.

The **haca-server user-name original** command configures the device not to modify the user name entered by the user in the packets sent to the HACA server.

The **undo haca-server user-name domain-included** command configures the device not to encapsulate the domain name in the user name when sending HACA packets to an HACA server.

By default, the device does not modify the user name entered by the user in the packets sent to the HACA server.

Format

haca-server user-name domain-included

haca-server user-name original

undo haca-server user-name domain-included

Parameters

None

Views

HACA server template view

Default Level

3: Management level

Usage Guidelines

The device manages access users based on domains. Each access user belongs to a domain. The users are authenticated in the specified domain when the entered user names contain domain names, or in the default domain when entered user names do not contain domain names. If a user name contains a domain name, the user belongs to that domain; otherwise, the user belongs to the default domain. When access users are authenticated in different domains, run the **haca-server user-name domain-included** command to configure the domain name

encapsulated by the device in the user name in HACA packets to be sent to an HACA server.

The format of a user name is user name@domain name. In the user name, @ is the domain name delimiter. The domain name delimiter can also be any of the following symbols: \ / : < > | ' %.

If the HACA server does not accept the user name with the domain name, run the **undo haca-server user-name domain-included** command to delete the domain name from the user name.

Example

Configure the device not to encapsulate the domain name in the user name when sending HACA packets to an HACA server.

```
<Huawei> system-view
[Huawei] haca-server template haca
[Huawei-haca-haca] haca-server user-name domain-included
```

19.4.16 reset haca-server statistics

Function

The **reset haca-server statistics** command clears HACA packet statistics.

Format

reset haca-server statistics { **all** | **message** | **packet** [**register** | **accounting** | **authentication** | **authorization** | **user-syn** | **cut-notify** | **cut-request**] }
[**template** *template-name*]

Parameters

Parameter	Description	Value
all	Clears all the statistics.	-
message	Clears all HACA message debugging information.	-
packet	Clears information about the specified type of packets.	-
register	Clears information about the registration packets.	-
accounting	Clears all statistics about HACA accounting.	-
authentication	Clears all statistics about HACA authentication.	-
authorization	Clears all statistics about HACA authorization.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-syn	Clears all HACA user synchronization information.	-
cut-notify	Clears all HACA logout notifications.	-
cut-request	Clears all HACA logout requests.	-
template *template-name*	Clears statistics about the specified HACA server template.	The HACA server template must already exist.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

During fault location, you may need to collect statistics about the HACA packets in a certain period. Before collecting new statistics, clear the existing statistics. Then run the **19.4.3 display haca-server statistics** command to view HACA statistics.

Precautions

The **reset haca-server statistics** command clears statistics about HACA packets, and the cleared statistics cannot be restored. Therefore, exercise caution when running this command.

Example

Clear all HACA statistics.

```
<Huawei> reset haca-server statistics all
```

Related Topics

19.4.3 display haca-server statistics

19.4.17 reset haca-server accounting-stop-packet all

Function

The **reset haca-server accounting-stop-packet all** command clears the remaining buffer information of all HACA accounting-stop packets.

Format

reset haca-server accounting-stop-packet all

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

You can run the **reset haca-server accounting-stop-packet all** command to clear the remaining buffer information of all HACA accounting-stop packets. Exercise caution when running this command because the information cannot be restored after being cleared.

Example

Clear the remaining buffer information of HACA accounting-stop packets.

```
<Huawei> reset haca-server accounting-stop-packet all
```

Related Topics

19.4.1 display haca-server accounting-stop-packet all

19.5 DAA Configuration Commands

19.5.1 acl tariff-level

Function

The **acl tariff-level** command configures a tariff level for traffic.

The **undo acl tariff-level** command deletes the tariff level.

By default, no tariff level is configured.

Format

acl *acl-number* **tariff-level** *tariff-level*

undo acl *acl-number* **tariff-level**

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 3000 to 3999.
tariff-level	Specifies the tariff level.	The value is an integer that ranges from 1 to 2.

Views

Traffic group view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On a network where users need to pay for the network access service, such as a campus network, users are not charged when they access internal network resources, and are charged when they access the Internet resources. Therefore, the device must be able to know whether the user traffic goes to the internal network or Internet according to the destination IP addresses of the traffic.

After distinguishing the traffic, the device uses the tariff level specified for the traffic and the corresponding accounting policy to offer differentiated services. This command is used to specify the tariff levels for different traffic.

Prerequisites

An IPv4 ACL must have been created using the **19.7.4 acl (system view)** or **19.7.3 acl name** command.

Precautions

- In the ACL rule, the destination address (the **destination** parameter) is mandatory, and the source address (the **source** parameter) is optional. Configuring both the source and destination addresses can precisely specify the traffic on which accounting will be performed.
- If there is an ACL rule with both the source and destination addresses configured and the destination address is the same as that in another ACL rule, you are advised to match this ACL rule with a tariff level (*tariff-level*) with a small value during configuration. For example, most users accessing destination address A on the network use the same tariff corresponding to ACL 3000, and a small number of users with source address B and accessing destination address A use another tariff corresponding to ACL 3001. In this case, the tariff level corresponding to ACL 3001 should have a smaller value than the tariff level corresponding to ACL 3000.

 Copyright © Huawei Technologies Co., Ltd.

- If the **any** parameter is specified, the device does not check the source and destination addresses of packets, and considers that all packets match the ACL rule. The device then executes the corresponding action.

Example

Configure tariff level 1 for the traffic matching ACL 3000.

```
<Huawei> system-view
[Huawei] acl number 3000
[Huawei-acl-adv-3000] rule 5 permit ip source any destination 10.0.0.1 0.0.0.255
[Huawei-acl-adv-3000] quit
[Huawei] traffic-group p1
[Huawei-traffic-group-p1] acl 3000 tariff-level 1
```

Related Topics

19.5.2 display traffic-group

19.5.2 display traffic-group

Function

The **display traffic-group** command displays information about traffic groups.

Format

display traffic-group { **all** | **name** *group-name* }

Parameters

Parameter	Description	Value
all	Displays information about all traffic groups.	-
name *group-name*	Displays detailed information about a specified traffic group.	The traffic group name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display traffic-group** command displays information about traffic groups.

Example

Display information about all traffic groups.

```
<Huawei> display traffic-group all
  ------------------------------------------------------------------------------
  ID   Traffic-group-name              Rule-num   Tariff-level-num  Status
  ------------------------------------------------------------------------------
  1    huawei                        1          1                 disable
  ------------------------------------------------------------------------------
  Total: 1
```

Table 19-38 Description of the display traffic-group all command output

Item	Description
ID	Traffic group ID.
Traffic-group-name	Name of the traffic group. To configure a traffic group, run the **19.5.4 traffic-group** command.
Rule-num	Number of ACL rules in a traffic group.
Tariff-level-num	Number of tariff levels in a traffic group.
Status	Status of a traffic group: ● enable: Traffic group is enabled. ● disable: Traffic group is disabled. To apply a traffic group, run the **19.5.5 traffic-group enable** command.
Total	Number of traffic groups.

Display details about the traffic group **huawei**.

```
<Huawei> display traffic-group name huawei
  ------------------------------------------------------------------------------
  Acl-id               Tariff-level
  ------------------------------------------------------------------------------
  3000                   1
  ------------------------------------------------------------------------------
  Total: 1
```

Table 19-39 Description of the display traffic-group name command output

Item	Description
Acl-id	ACL rule that identifies traffic. To specify an ACL rule, run the **19.5.1 acl tariff-level** command.
Tariff-level	Tariff level of traffic. To configure a tariff level, run the **19.5.1 acl tariff-level** command.

Item	Description
Total	Number of ACL rules in a traffic group.

Related Topics

19.5.4 traffic-group

19.5.1 acl tariff-level

19.5.5 traffic-group enable

19.5.3 tariff-level

Function

The **tariff-level** command configures the QoS profile and accounting function for a tariff level.

The **undo tariff-level** command restores the default configuration.

By default, the QoS profile and accounting function are not configured for tariff levels.

Format

tariff-level *tariff-level* { **qos-profile** *profile-name* | **accounting-on** } *

undo tariff-level *tariff-level* [**qos-profile** | **accounting-on**]

Parameters

Parameter	Description	Value
tariff-level	Specifies the tariff level.	The value is an integer that ranges from 1 to 2.
qos-profile *profile-name*	Specifies the name of the QoS profile corresponding to the tariff level.	The QoS profile name must already exist.
accounting-on	Enables accounting for the tariff level.	-

Views

AAA domain view, service scheme view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After the tariff level is configured for classified traffic, you need to configure the QoS profile and accounting function for the tariff level to implement destination-based accounting. The QoS profile is used to collect traffic statistics based on destination addresses. After the accounting function is enabled, the device can send statistics to the RADIUS accounting server.

The DAA policy priorities on the device are as follows: DAA policy in a service scheme delivered by the RADIUS server > DAA policy in a service scheme bound to a domain > DAA policy configured in a domain.

To delete a DAA policy, it is recommended that you make users go offline first and make them go online after deleting the DAA policy.

Prerequisites

The QoS profile has been created using the **20.3.18 qos-profile** command.

Example

Configure the QoS profile huawei for tariff level 1 and enable the accounting function.

```
<Huawei> system-view
[Huawei] qos-profile huawei
[Huawei-qos-profile-huawei] statistics enable
[Huawei-qos-profile-huawei] quit
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] tariff-level 1 qos-profile huawei accounting-on
```

Related Topics

19.1.41 display domain

20.3.18 qos-profile

19.5.4 traffic-group

Function

The **traffic-group** command creates a traffic group and displays the traffic group view, or displays the view of an existing traffic group.

The **undo traffic-group** command deletes a traffic group.

By default, no traffic group exists on the device.

Format

traffic-group *group-name*

undo traffic-group *group-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
group-name	Indicates the name of a traffic group.	The value is a string of 1 to 31 case-sensitive characters. It cannot be - or -- and cannot contain spaces or the following symbols: / \ : < > | @ ' % * " ?.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By using the traffic group, the device can identify the traffic going to different destination addresses, apply different tariff levels for the traffic, and enforce different accounting policies.

Follow-up Procedure

- After a traffic group is created, the traffic group view is displayed. Run the **19.5.1 acl tariff-level** command in the traffic group view to configure a tariff level.
- Run the **19.5.5 traffic-group enable** command in the system view to make the traffic group effective.

Precautions

The device supports a maximum of 8 traffic groups.

Example

Create the traffic group p1.

```
<Huawei> system-view
[Huawei] traffic-group p1
```

Related Topics

19.5.2 display traffic-group

 Copyright © Huawei Technologies Co., Ltd.

19.5.5 traffic-group enable

Function

The **traffic-group enable** command applies a traffic group to the device globally.

The **undo traffic-group enable** command restores the default configuration.

By default, no traffic group is applied to the device.

Format

traffic-group *group-name* **enable**

undo traffic-group *group-name* **enable**

Parameters

Parameter	Description	Value
group-name	Specifies the name of a traffic group that you want to apply to the device.	The traffic group name must already exist.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The traffic group takes effect for users only after it is globally applied to the device.

Prerequisites

The traffic group has been created using the **19.5.4 traffic-group** command.

Precautions

- Only one traffic group can be applied to the device globally.
- If you run this command multiple times, only the latest configuration takes effect.
- If you modify a traffic group that has been applied, the modification takes effect only after the traffic group is applied to the device again by using this command.

 Copyright © Huawei Technologies Co., Ltd.

- The **19.5.1 acl tariff-level** command changes the tariff level of traffic.
- The **19.7.16 rule (advanced ACL view)** command changes the source or destination address in the traffic classification rule.

Example

Apply the traffic group p1 to the device globally.

```
<Huawei> system-view
[Huawei] traffic-group p1
[Huawei-traffic-group-p1] quit
[Huawei] traffic-group p1 enable
```

Related Topics

19.5.2 display traffic-group

19.6 NAC Configuration Commands

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support NAC.

19.6.1 access-domain

Function

The **access-domain** command configures a default or forcible domain in an authentication profile for users.

The **undo access-domain** command deletes a configured default or forcible domain in an authentication profile.

By default, no default or forcible domain is configured in an authentication profile.

Format

access-domain *domain-name* [**dot1x** | **mac-authen** | **portal**] * [**force**]

undo access-domain [**dot1x** | **mac-authen** | **portal**] * [**force**]

Parameters

Parameter	Description	Value
domain-name	Specifies the domain name.	The value must be the name of an existing domain.
dot1x	Specifies a default or forcible domain for 802.1X authentication users.	-

Parameter	Description	Value
mac-authen	Specifies a default or forcible domain for MAC address authentication users.	-
portal	Specifies a default or forcible domain for Portal authentication users.	-
force	Specifies the configured domain as a forcible domain. If this parameter is not specified, the configured domain is a default domain.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device manages users in domains. For example, AAA schemes and authorization information are bound to domains. During user authentication, the device assigns users to specified domains based on the domain names contained in user names. However, user names entered by many users on actual networks do not contain domain names. In this case, you can configure a default domain in an authentication profile. If users using this profile enter user names that do not contain domain names, the device manages the users in the default domain.

On actual networks, user names entered by some users contain domain names and those entered by other users do not. The device uses different domains to manage the users. Because authentication, authorization and accounting (AAA) information in the domains are different, users use different AAA information. To ensure that users using the same authentication profile use the same AAA information, you can configure a forcible domain in the authentication profile for the users. The device then manages the users in the forcible domain regardless of whether entered user names contain domain names or not.

Prerequisites

A domain has been configured using the **19.1.50 domain (AAA view)** command in the AAA view.

Precautions

When you configure a default or forcible domain in an authentication profile, the domain takes effect as follows:

- If you do not specify the user authentication mode (**dot1x**, **mac-authen**, or **portal**), the domain takes effect for all access authentication users using the authentication profile.
- If both a default domain and a forcible domain are configured, the device authenticates users in the forcible domain.
- This function takes effect only for users who go online after this function is successfully configured.
- In a wireless scenario, RADIUS accounting is performed only for AAA users who do not need to pass authentication in a forcible domain, and cannot be performed for such users in the default domain.

Example

Configure the forcible domain **huawei** in the authentication profile **p1**.

```
<Huawei> system-view
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] quit
[Huawei-aaa] quit
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] access-domain huawei force
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.2 access-user arp-detect

Function

The **access-user arp-detect** command sets the source IP address and source MAC address of offline detection packets in a VLAN.

The **undo access-user arp-detect** command deletes the source IP address and source MAC address of offline detection packets in a VLAN.

By default, the source IP address and source MAC address are not specified for offline detection packets in a VLAN.

Format

access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

undo access-user arp-detect vlan *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address*

Parameters

Parameter	Description	Value
vlan *vlan-id*	Specifies a VLAN ID.	The value is an integer that ranges from 1 to 4094.
ip-address *ip-address*	Specifies the source IP address of offline detection packets.	The value is in dotted decimal notation.
mac-address *mac-address*	Specifies the source MAC address of offline detection packets.	The value is a unicast MAC address in H-H-H format, where H can be one to four hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

If the VLAN to which the user belongs does not have a VLANIF interface or the VLANIF interface does not have an IP address, the device sends an offline detection packet using 0.0.0.0 as the source IP address. If a user cannot respond to an ARP probe packet with the source IP address 0.0.0.0, you can specify a source IP address for the offline detection packet.

You are advised to specify the user gateway IP address and its corresponding MAC address as the source IP address and source MAC address of offline detection packets.

Precautions

This function does not take effect for users who use Layer 3 Portal authentication.

You can set source addresses of offline detection packets for users in a maximum of 1024 VLANs.

If a user on a physical interface is online, this command takes effect only after the user goes online again or the device re-authenticates the user.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the source IP address and MAC address of offline detection packets for users in VLAN 10 to 192.168.1.1 and 2222-1111-1234 respectively.

```
<Huawei> system-view
[Huawei] access-user arp-detect vlan 10 ip-address 192.168.1.1 mac-address 2222-1111-1234
```

19.6.3 access-user arp-detect default ip-address

Function

The **access-user arp-detect default ip-address** command sets the default source IP address of offline detection packets.

The **undo access-user arp-detect default ip-address** command restores the default setting.

By default, the default source IP address of offline detection packets is 0.0.0.0.

Format

access-user arp-detect default ip-address *ip-address*

undo access-user arp-detect default ip-address

Parameters

Parameter	Description	Value
ip-address	Specifies the default source IP address of offline detection packets.	The value is in dotted decimal notation and can be 0.0.0.0 or 255.255.255.255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends an ARP probe packet to check the user online status. If the user does not respond within a detection period, the device considers that the user is offline.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- This function does not take effect for users who use Layer 3 Portal authentication.
- In normal situations, after a device sends an ARP probe packet with a default source IP address, online clients will immediately respond with ARP reply packets. If online clients do not respond with ARP reply packets, the device logs them out unexpectedly. To resolve this problem, use either of the following methods:
  - Run the **access-user arp-detect vlan** *vlan-id* **ip-address** *ip-address* **mac-address** *mac-address* command to specify a VLAN ID, source IP address, and source MAC address for ARP probe packets.
  - Run the **authentication timer handshake-period** *handshake-period* command to increase the handshake period so that the device can detect gratuitous ARP packets that these clients send at an irregular period. Once the device detects such packets, it does not log them out.

Example

Set the default source IP address of offline detection packets to 0.0.0.0.

```
<Huawei> system-view
[Huawei] access-user arp-detect default ip-address 0.0.0.0
```

19.6.4 access-user acl-priviledge-revert

Function

The **access-user acl-priviledge-revert** command configures the device to match packets with ACL rules in ascending order by rule IDs. That is, a smaller rule ID indicates a higher priority of the rule.

The **undo access-user acl-priviledge-revert** command restores the default matching sequence for ACL rules.

By default, the device matches packets with ACL rules in descending order by rule IDs. That is, a larger rule ID indicates a higher priority of the rule.

Format

access-user acl-priviledge-revert

undo access-user acl-priviledge-revert

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device matches packets with ACL rules in descending order by rule IDs. You can use the **access-user acl-priviledge-revert** command to configure the device to match packets with ACL rules in ascending order by rule IDs.

Precautions

The configuration takes effect only after the device is restarted.

Example

Configure the device to match packets with ACL rules in ascending order by rule IDs.

```
<Huawei> system-view
[Huawei] access-user acl-priviledge-revert
```

19.6.5 acl-id (user group view)

Function

The **acl-id** command binds an ACL to a user group.

The **undo acl-id** command unbinds an ACL from a user group.

By default, no ACL is bound to a user group.

Format

acl-id *acl-number*

undo acl-id { *acl-number* | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL bound to a user group.	The value is an integer that ranges from 3000 to 3999.
all	Deletes all ACLs bound to a user group.	-

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a user group using the **19.6.150 user-group** command, you can run the **acl-id** command to bind an ACL to the user group. The device will deliver ACL rules based on the user group and the ACL rules apply to all users in the user group.

Prerequisites

The ACL to be bound to a user group must have been created using the **19.7.4 acl (system view)** command.

Precautions

- If a user group contains online users, the ACL bound to the user group cannot be modified or deleted in the system view.
- If no ACL rule is configured for a user group, the device does not restrict the network access rights of users in the user group.
- When configuring ACL rules in a user group, add an ACL rule that denies all network access and ensure that the ACL rule takes effect.
- To grant the same network access rights to all users in a user group, do not configure the source IP address in an ACL rule bound to the user group. If an ACL rule defines the source IP address, only users whose IP address is the source IP address match the ACL rule.

Example

Bind ACL 3001 to the user group **abc**.

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule 5 deny ip destination 192.168.5.0 0.0.0.255
[Huawei-acl-adv-3001] quit
[Huawei] user-group abc
[Huawei-user-group-abc] acl-id 3001
```

Related Topics

19.6.51 display user-group

19.6.6 authentication handshake

Function

The **authentication handshake** command enables the handshake with pre-connection users and authorized users.

The **undo authentication handshake** command disables the handshake with pre-connection users and authorized users.

By default, the handshake with pre-connection users and authorized users is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

authentication handshake

undo authentication handshake

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates entries for pre-connection users, users who fail to be authenticated and are assigned network access rights, and users who are authenticated. After users go offline in normal situations, the system immediately deletes the corresponding user entries. However, if some users go offline due to exceptions such as network disconnections, the system cannot immediately delete the corresponding user entries. If there are too many such invalid user entries, other users may fail to access the network.

To solve this problem, run the **authentication handshake** command to enable the handshake with pre-connection users and authorized users. If a user does not respond to the handshake request from the device within the handshake interval (set using the **19.6.16 authentication timer handshake-period** command), the device deletes the user entry.

Precautions

- All pre-connection users support this function. Among users who fail to be authenticated or pass authentication, only MAC address authentication users, and 802.1X authentication users support this function. The offline detection function for Portal authentication users is configured using the **portal timer offline-detect** command.
- This function takes effect only for the wired users who obtain IP addresses.
- When the configuration changes, the configuration takes effect only for new online wired users.
- The handshake function is implemented using ARP probe packets or neighbor discovery (ND) probe packets.

Example

In the authentication profile **p1**, enable the handshake with pre-connection users and authorized users.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] authentication handshake
```

19.6.7 authentication authen-fail fail-times

Function

The **authentication authen-fail fail-times** command configures the maximum number of consecutive authentication failures.

The **undo authentication authen-fail** command restores the default maximum number of consecutive authentication failures.

By default, the maximum number of consecutive authentication failures is 1.

Format

authentication authen-fail fail-times *fail-times*

undo authentication authen-fail

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of consecutive authentication failures.	The value is an integer that ranges from 1 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users may fail to pass authentication due to reasons such as temporary unreachability of the server. To improve authentication reliability, you can configure the maximum number of consecutive authentication failures so that users can be re-authenticated after an authentication failure within the allowed range. If the number of consecutive authentication failures exceeds the maximum value, the authentication fails.

Example

Set the maximum number of consecutive authentication failures to 2.

```
<Huawei> system-view
[Huawei] authentication authen-fail fail-times 2
```

19.6.8 authentication dot1x-mac-bypass

Function

The **authentication dot1x-mac-bypass** command enables MAC address bypass authentication.

The **undo authentication dot1x-mac-bypass** command disables MAC address bypass authentication.

By default, MAC address bypass authentication is disabled.

Format

authentication dot1x-mac-bypass

undo authentication dot1x-mac-bypass

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure MAC address bypass authentication to authenticate terminals such as printers that cannot have the 802.1X client installed.

After MAC address bypass authentication is enabled in an authentication profile, the device performs 802.1X authentication for users using the authentication profile. If the user name request times out, the device starts the MAC address authentication process for the users.

Precautions

MAC address bypass authentication involves 802.1X authentication and MAC address authentication. Before enabling this function in an authentication profile, ensure that an 802.1X access profile and a MAC access profile have been bound to the authentication profile.

Example

In the authentication profile **p1**, enable MAC address bypass authentication.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] authentication dot1x-mac-bypass
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.9 authentication event action authorize

Function

The **authentication event action authorize** command configures authentication event authorization information.

The **undo authentication event action authorize** command restores the default setting.

By default, authentication event authorization information is not configured.

Format

User authorization in the case of pre-connections:

authentication event pre-authen action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* }

undo authentication event pre-authen action authorize

User authorization when authentication fails:

authentication event authen-fail action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* } [**response-fail**]

undo authentication event authen-fail action authorize

User authorization when the authentication server is Down:

authentication event authen-server-down action authorize { **vlan** *vlan-id* | **service-scheme** *service-scheme-name* } [**response-fail**]

undo authentication event authen-server-down action authorize

Parameters

Parameter	Description	Value
pre-authen	Configures the device to assign network access rights to users when the users establish pre-connections with the device.	-
authen-fail	Configures the device to assign network access rights to users when the authentication server sends authentication failure packets to the device.	-
authen-server-down	Configures the device to assign network access rights to users when the authentication server is Down or the server is in the forcible Up state.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
response-fail	Configures the device to send authentication failure packets to users after assigning network access rights to the users. If this parameter is not specified, the device by default sends authentication success packets to users and therefore the users cannot know the fact that they fail to be authenticated. To solve this problem, specify this parameter so that the device will send authentication failure packets for the users to know their authentication results.	-
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, users can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094. The VLAN must exist on the device. Otherwise, the configuration does not take effect.
service-scheme *service-scheme-name*	Specifies the name of the service scheme based on which network access rights are assigned to users.	The value must be an existing service scheme name on the device.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If users establish pre-connections with the device or fail to be authenticated, they have no network access rights.

To meet these users' basic network access requirements such as updating the antivirus database and downloading the client, configure authentication event

authorization information. The device will assign network access rights to these users based on the authentication phase.

Precautions

Wireless 802.1X authentication does not support this function.

If no network access right is configured for users who fail authentication or when the authentication server is Down, the users establish pre-connections with the device after the authentication fails and then have the network access rights mapping pre-connection users.

Only the 8FE1GE, 24GE, and 24ES2GP cards, and the AR2201-48FE and AR2202-48FE support the delivery of authorized VLANs to users.

VLAN-based authorization does not apply to the authentication users who access through VLANIF interfaces.

An authorized VLAN cannot be delivered to online Portal users.

This function takes effect only for users who go online after this function is successfully configured.

When the authentication server is in Down state, user authentication fails, or the user is in pre-connection state, the redirection ACL function is not supported.

In 802.1X authentication for wired users, when the RADIUS server is Down, some new clients do not have escape rights. For example, when a new Windows client receives a Success packet from the device but does not receive the authentication packets exchanged with the RADIUS server, the client will fail the authentication and cannot go online. Currently, the following clients have escape rights when they go online for the first time: H3C iNode clients using EAP-MD5 or PEAP and Cisco AnyConnect clients using EAP-FAST or PEAP. For Windows clients, for example, Windows 7, choose "Local Area Connection> Properties> Authentication> Fallback to unauthorized network access".

Authentication event authorization information cannot be configured for static users identified by IP addresses.

Example

In the authentication profile **authen1**, configure the device to assign network access rights specified in VLAN 10 to pre-connection users.

```
<Huawei> system-view
[Huawei] vlan batch 10
[Huawei] authentication-profile name authen1
[Huawei-authen-profile-authen1] authentication event pre-authen action authorize vlan 10
```

19.6.10 authentication event authen-server-up action re-authen

Function

The **authentication event authen-server-up action re-authen** command enables the device to re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to Up.

The **undo authentication event authen-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users in the survival state when the authentication server changes from Down or forcible Up to UP.

Format

authentication event authen-server-up action re-authen

undo authentication event authen-server-up action re-authen

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The users in the survival state can only access limited network resources after the device assigns specified network access rights to users who fail authentication because the authentication server is Down. To meet the users' normal network access requirements, the device needs to re-authenticate users in the survival state in real time when the authentication server turns Up.

After the status of the RADIUS server is set to Down, you can run the **radius-server dead-time** *dead-time* command to set the interval for the RADIUS server to return to the active state. When the value of *dead-time* expires, the status of the RADIUS server is set to forcible Up. When the server successfully transmits and receives packets, the status is set to Up. The device can re-authenticate users in the survival state when the server changes from Down or forcible Up to Up. Re-authentication cannot be triggered when the server turns from Down to forcible Up.

Prerequisites

The **19.2.45 radius-server testuser** command has been configured in the RADIUS server template so that the device can detect that the authentication server changes from Down to Up.

Example

In the authentication profile **authen1**, enable the device to re-authenticate users when the authentication server turns Up from Down or forcible Up.

```
<Huawei> system-view
[Huawei] authentication-profile name authen1
[Huawei-authen-profile-authen1] authentication event authen-server-up action re-authen
```

19.6.11 authentication event client-no-response action authorize

Function

The **authentication event client-no-response action authorize** command configures network access rights for users when the 802.1X client does not respond.

The **undo authentication event client-no-response action authorize** command restores the default setting.

By default, no network access right is configured for users when the 802.1X client does not respond.

Format

authentication event client-no-response action authorize { **service-scheme** *service-scheme-name* | **user-group** *user-group-name* | **vlan** *vlan-id* }

undo authentication event client-no-response action authorize

Parameters

Parameter	Description	Value
service-scheme *service-scheme-name*	Specifies the name of a service scheme based on which network access rights are assigned.	The value must be an existing service scheme name on the device.
user-group *user-group-name*	Specifies the name of a user group based on which network access rights are assigned.	The value must be an existing user group name on the device.
vlan *vlan-id*	Specifies a VLAN ID. When this parameter is specified, users can access only the resources in the VLAN.	The value is an integer that ranges from 1 to 4094.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the 802.1X client does not respond, users cannot pass authentication and thereby have no network access right. Before being successfully authenticated, some users may need certain basic network access rights to download client software and update the antivirus database. The network access rights can be configured for the users when the 802.1X client does not respond, so that the users can access specified network resources.

Precautions

Only the 8FE1GE, 24GE, and 24ES2GP cards, and the AR2201-48FE and AR2202-48FE support the delivery of authorized VLANs to users.

Wireless 802.1X authentication does not support this function.

This function takes effect only for users who go online after this function is successfully configured.

When an 802.1X client does not respond, the redirection ACL function is not supported.

Example

In the 802.1X access profile **d1**, configure the device to assign the network access rights specified in VLAN 10 for users when the 802.1X client does not respond.

```
<Huawei> system-view
[Huawei] vlan batch 10
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] authentication event client-no-response action authorize vlan 10
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.12 authentication event portal-server-down action authorize

Function

The **authentication event portal-server-down action authorize** command configures network access rights for users when the Portal server is Down.

The **undo authentication event portal-server-down action authorize** command deletes the network access rights configured for users when the Portal server is Down.

By default, no network access right is configured for users when the Portal server is Down.

 Copyright © Huawei Technologies Co., Ltd.

Format

authentication event portal-server-down action authorize user-group *user-group-name*

undo authentication event portal-server-down action authorize

Parameters

Parameter	Description	Value
user-group *user-group-name*	Specifies the name of the user group based on which network access rights are assigned to users.	The value must be an existing user group name.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the Portal server is Down, users cannot pass the authentication and thereby have no network access right. Before being successfully authenticated, some users may need certain basic network access rights to download client software and update the antivirus database. The network access rights can be configured for the users when the Portal server is Down, so that the users can access specified network resources.

Prerequisites

A user group has been created using the **user-group** command in the system view.

Precautions

- This function takes effect only for users who go online after this function is successfully configured.
- Only HTTP messages-triggered Portal authentication users support this function.
- Before enabling the access device to assign network access rights to users when the Portal server is Down, enable the heartbeat detection function on the Portal server and run the **server-detect** command on the access device to enable the Portal server detection function.
- When the Portal server is in Down state, the redirection ACL function is not supported.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the Portal access profile **p1**, configure the device to assign network access rights based on the user group **g1** to users when the Portal server is Down.

```
<Huawei> system-view
[Huawei] user-group g1
[Huawei-user-group-g1] quit
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] authentication event portal-server-down action authorize user-group
g1
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.13 authentication event portal-server-up action re-authen

Function

The **authentication event portal-server-up action re-authen** command enables the device to re-authenticate users when the Portal server turns Up from Down.

The **undo authentication event portal-server-up action re-authen** command restores the default setting.

By default, the device does not re-authenticate users when the Portal server turns Up from Down.

Format

authentication event portal-server-up action re-authen

undo authentication event portal-server-up action re-authen

Parameters

None

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is configured to assign network access rights to users when the Portal server is Down, users can access limited network resources after the device detects that the Portal server is Down. To ensure that users can obtain normal network access rights after the Portal server goes Up, you can enable the device to re-

authenticate users when the Portal server changes from Down to Up. After the Portal server goes Up, the device sets the status of users who display **web-server-down** to pre-connection. The re-authentication process starts when the users visit any web page. If the authentication succeeds, the device assigns normal network access rights to the users.

Precautions

- This command does not apply to users connected to the route main interface.
- This function takes effect only for users who go online after this function is successfully configured.
- Before enabling the access device to assign network access rights to users when the Portal server is Down, enable the heartbeat detection function on the Portal server and run the **server-detect** command on the access device to enable the Portal server detection function.

Example

In the Portal access profile **p1**, enable the device to re-authenticate users when the Portal server turns Up from Down.

```
<Huawei> system-view
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] authentication event portal-server-up action re-authen
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.14 authentication ip-address in-accounting-start

Function

The **authentication ip-address in-accounting-start** command enables the function of carrying users' IP addresses in Accounting-Start packets.

The **undo authentication ip-address in-accounting-start** command disables the function of carrying users' IP addresses in Accounting-Start packets.

By default, the function of carrying users' IP addresses in Accounting-Start packets is disabled.

Format

authentication ip-address in-accounting-start

undo authentication ip-address in-accounting-start

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device reports access information and basic network information (IP address) of users through Accounting-Start packets. Therefore, the device needs to support carrying users' IP addresses in Accounting-Start packets.

Precautions

If the device cannot learn IP addresses of users, the device does not send Accounting-Start packets.

This command takes effect only for 802.1X authentication and MAC address authentication users. By default, Accounting-Start packets for Portal authentication carry users' IP addresses.

This command takes effect on both IPv4 and IPv6 users.

Example

Enable the function of carrying users' IP addresses in Accounting-Start packets.

```
<Huawei> system-view
[Huawei] authentication-profile name test
[Huawei-authen-profile-test] authentication ip-address in-accounting-start
```

19.6.15 authentication single-access

Function

The **authentication single-access** command configures the device to allow users to access in only one authentication mode.

The **undo authentication single-access** command restores the default setting.

By default, the device allows users to access in different authentication modes.

Format

authentication single-access

undo authentication single-access

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

After hybrid authentication is configured, the device by default allows users to access in different authentication modes. You can run the **authentication single-access** command to disable this default function. The device then allows users to access in only one authentication mode and does not process the packets of other authentication modes.

Example

In the authentication profile **authen1**, configure the device to allow users to access in only one authentication mode.

```
<Huawei> system-view
[Huawei] authentication-profile name authen1
[Huawei-authen-profile-authen1] authentication single-access
```

19.6.16 authentication timer handshake-period

Function

The **authentication timer handshake-period** command sets the handshake interval of the device with pre-connection users and authorized users.

The **undo authentication timer handshake-period** command restores the default setting.

The default handshake interval of the device with pre-connection users and authorized users is 300 seconds.

Format

authentication timer handshake-period *handshake-period*

undo authentication timer handshake-period

Parameters

Parameter	Description	Value
handshake-period	Specifies the handshake interval.	The value is an integer that ranges from 5 to 7200, in seconds.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling the handshake with pre-connection users and authorized users using the **19.6.6 authentication handshake** command, you can run the this command to set the handshake interval. After that, if a user does not respond to the handshake request from the device within the handshake interval, the device deletes the user entry.

Precautions

- All pre-connection users support this function. Among users who fail to be authenticated or pass authentication, only MAC address authentication users, and 802.1X authentication users support this function. The offline detection function for Portal authentication users is configured using the **portal timer offline-detect** command.
- This function takes effect only for the wired users who obtain IP addresses. By default, wired users without IP addresses go offline after 30 minutes.
- This function takes effect only for users who go online after this function is successfully configured.
- The handshake function is implemented using ARP probe packets or neighbor discovery (ND) probe packets.
- If the configured handshake interval is less than the default value, an IP address conflict may occur between terminal detection and device ARP probe. For example, a Windows client sends a detection packet with the source address 0.0.0.0 at an interval of 10 seconds after obtaining an IP address. If the device also initiates ARP probe with the source address 0.0.0.0, a conflict occurs.
- If the number of ARP probe packets exceeds the default CAR value, the probe fails and the users are logged out (The **display cpu-defend statistics** command can be run to check whether ARP request and response packets are lost.). To resolve the problem, the following methods are recommended:
  - Increase the handshake interval based on the number of users. The default handshake interval is recommended when there are less than 8000 users; the handshake interval should be no less than 600 seconds when there are more than 8000 users.
  - Deploy the port attack defense function on the access device and limit the rate of packets sent to the CPU.

Example

In the authentication profile **p1**, set the handshake interval of the device with pre-connection users and authorized users to 200 seconds.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] authentication timer handshake-period 200
```

19.6.17 authentication timer authen-fail-aging

Function

The **authentication timer authen-fail-aging** command configures the aging time for entries of the users who fail to be authenticated.

The **undo authentication timer authen-fail-aging** command restores the default aging time for entries of the users who fail to be authenticated.

By default, the aging time for entries of the users who fail to be authenticated is 23 hours.

Format

authentication timer authen-fail-aging *aging-time*

undo authentication timer authen-fail-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After network access policies are configured for users who fail to be authenticated, the device creates entries for these users. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.

The entries of the users who fail to be authenticated share device resources with the entries of the users who are authenticated. If there are excess entries of the users who fail to be authenticated, other users fail to be authenticated. To solve this problem, run the **authentication timer authen-fail-aging** command to reduce the aging time for entries of the users who fail to be authenticated. In addition, if the time that the users who fail to be authenticated have network access policies should be shortened, you can run this command to decrease the aging time for the user entries.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only wired users support this function.

Example

In the authentication profile **p1**, configure the aging time for entries of the users who fail to be authenticated to 3600 seconds.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] authentication timer authen-fail-aging 3600
```

19.6.18 authentication timer pre-authen-aging

Function

The **authentication timer pre-authen-aging** command configures the aging time for pre-connection user entries.

The **undo authentication timer pre-authen-aging** command restores the default aging time for pre-connection user entries.

By default, the aging time for pre-connection user entries is 23 hours.

Format

authentication timer pre-authen-aging *aging-time*

undo authentication timer pre-authen-aging

Parameters

Parameter	Description	Value
aging-time	Specifies the aging time.	The value is an integer that ranges from 0 or 60 to 4294860, in seconds. The value **0** indicates that the entry does not age.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a pre-connection is established between the device and a user, the device creates the pre-connection user entry. If the user still fails to be authenticated when the user aging time expires, the user entry is deleted.

The pre-connection user entries share device resources with the entries of the users who are authenticated. If there are excess pre-connection user entries, other users fail to be authenticated. To solve this problem, run the **authentication timer pre-authen-aging** command to reduce the aging time for the pre-connection user entries. In addition, if the time that the pre-connection users have network access policies should be extended, you can run this command to increase the aging time for the pre-connection user entries.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

Only wired users support this function.

Example

In the authentication profile **p1**, configure the aging time for the pre-connection user entries to 3600 seconds.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] authentication timer pre-authen-aging 3600
```

19.6.19 authentication timer re-authen

Function

The **authentication timer re-authen** command configures the interval for re-authenticating pre-connection users or users who fail to be authenticated.

The **undo authentication timer re-authen** command restores the default setting.

By default, pre-connection users and users who fail to be authenticated are re-authenticated at an interval of 60 seconds.

Format

authentication timer re-authen { **pre-authen** *re-authen-time* | **authen-fail** *re-authen-time* }

undo authentication timer re-authen { **pre-authen** | **authen-fail** }

Parameters

Parameter	Description	Value
pre-authen *re-authen-time*	Specifies the interval for re-authenticating pre-connection users.	The value is an integer that ranges from 0 or 30 to 7200, in seconds. The value **0** indicates that the re-authentication function is disabled for pre-connection users.
authen-fail *re-authen-time*	Specifies the interval for re-authenticating users who fail to be authenticated.	The value is an integer that ranges from 0 or 30 to 7200, in seconds. The value **0** indicates that the re-authentication function is disabled for users who fail to be authenticated.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device creates the mapping user entries when network access policies are assigned to users who are in the pre-connection phase or fail authentication. To enable users to pass authentication in real time, the device periodically re-authenticates the users who are in the pre-connection phase or fail authentication according to the user entries. The administrator can adjust the re-authentication interval based on the actual network requirements.

Precautions

This command only applies to 802.1X authentication and MAC address authentication.

This function takes effect only for users who go online after this function is successfully configured.

The device cannot re-authenticate wireless users who are in the pre-connection phase or fail authentication. Therefore, the **authentication timer re-authen** command does not apply to wireless users.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the authentication profile **authen1**, set the interval for re-authenticating users who fail to be authenticated to 300 seconds.

```
<Huawei> system-view
[Huawei] authentication-profile name authen1
[Huawei-authen-profile-authen1] authentication timer re-authen authen-fail 300
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.20 authentication roam pre-authen mac-authen enable

Function

The **authentication roam pre-authen mac-authen enable** command enables MAC address authentication for roaming STAs.

The **undo authentication roam pre-authen mac-authen enable** command disables MAC address authentication for roaming STAs.

By default, MAC address authentication is disabled for roaming STAs.

NOTE

This command applies only to wireless users.

Format

authentication roam pre-authen mac-authen enable

undo authentication roam pre-authen mac-authen enable

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In versions earlier than V200R010C00, MAC address authentication is enabled for roaming STAs. A STA connects to the network through MAC address authentication or MAC address-prioritized Portal authentication. If the STA roams, MAC address authentication is triggered after successful roaming. However, MAC address authentication may fail, and the STA enters the pre-connection state and

 Copyright © Huawei Technologies Co., Ltd.

no longer has the original access permission. To prevent this problem, the MAC address authentication is disabled for roaming STAs by default in V200R010C00 and later versions. You are not advised to retain the default configuration.

Precautions

MAC address authentication for roaming STAs takes effect only when the following authentication event authorization information is configured:

- Authorization for STAs in pre-connection users
- Authorization for STAs that fail the authentication
- Authorization for STAs if the authorization server goes Down
- Authorization for STAs if the Portal server goes Down

Example

Enable MAC address authentication for roaming STAs.

```
<Huawei> system-view
[Huawei] authentication-profile name test
[Huawei-authen-profile-test] authentication roam pre-authen mac-authen enable
```

19.6.21 authentication mode

Function

The **authentication mode** command configures the user access mode.

The **undo authentication mode** command restores the default user access mode.

By default, the user access mode is **multi-authen**.

Format

authentication mode { **single-terminal** | **single-voice-with-data** | **multi-share** | **multi-authen** [**max-user** *max-user-number* [**dot1x** | **mac-authen** | **portal** | **none**] *] }

undo authentication mode [**multi-authen max-user** [**dot1x** | **mac-authen** | **portal** | **none**] *]

Parameters

Parameter	Description	Value
single-terminal	Specifies the interface to allow only one user to go online.	-
single-voice-with-data	Specifies the interface to allow only one data user and one voice user to go online. This mode applies to the scenario in which a data user connects to a network through a voice terminal.	-

Parameter	Description	Value
multi-share	Specifies the interface to allow multiple users to go online. In this mode, the device only authenticates the first user. If the first user can be authenticated, the subsequent users share the same network access rights with the first user. If the first user goes offline, other users are also offline.	-
multi-authen	Specifies the interface to allow multiple users to go online. In this mode, the device authenticates each access user. If users can be authenticated, the users have their individual network access rights. If a user goes offline, other users are not affected. **NOTE** AR100&AR120&AR150&AR160&AR200&AR1200 series do not support to bind a VLAN in MAC-based mode.	-
max-user *max-user-number*	Specifies the maximum number of access users on the interface in **multi-authen** mode.	The value ranges from 1 to 2048 and the default value is 2048.
dot1x	Specifies the maximum number of 802.1X authentication users allowed to connect to the interface in **multi-authen** mode.	-
mac-authen	Specifies the maximum number of MAC address authentication users allowed to connect to the interface in **multi-authen** mode.	-
portal	Specifies the maximum number of Portal authentication users allowed to connect to the interface in **multi-authen** mode.	-
none	Specifies the maximum number of pre-connection users allowed to connect to the interface in **multi-authen** mode.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling NAC authentication, you can configure a user access mode based on the user access on the interface. The user access modes include:

- **single-terminal**: applies to the scenario in which only one data terminal is connected to the network through the interface.
- **single-voice-with-data**: applies to the scenario in which only one data terminal is connected to the network on the device interface through a voice terminal.
- **multi-share**: applies to the scenario that does not require high security and in which multiple data terminals are connected to the network on the device interface.
- **multi-authen**: applies to the scenario that requires high security and in which multiple data terminals are connected to the network on the device interface. In this access mode, you can configure the maximum number of access users based on the actual user quantity on the interface. This prevents malicious users from occupying a large amount of device resources and ensures that the users on other device interfaces can normally go online.

Precautions

- VLANIF interfaces do not support this function.
- Only wired users support this function.
- If the first access user fails to be authenticated on a physical interface and sets up a pre-connection after the **multi-share** mode is configured on the physical interface, new access users will also fail to be authenticated on the interface. Therefore, the following operations are recommended if the first access user may fail to be authenticated after the **multi-share** mode is configured on a physical interface.
  - Do not use the **multi-share** mode with Portal authentication.

Example

In the authentication profile **p1**, set the user access mode to **multi-authen**.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] authentication mode multi-authen
```

19.6.22 authentication speed-limit auto

Function

The **authentication speed-limit auto** command enables the device to dynamically adjust the rate of packets from NAC users.

The **undo authentication speed-limit auto** command disables the device from dynamically adjusting the rate of packets from NAC users.

By default, the device does not dynamically adjust the rate of packets from NAC users.

Format

authentication speed-limit auto

undo authentication speed-limit auto

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When a lot of NAC users send authentication or log off requests to the device, the CPU usage may be overloaded especially when the CPU or memory usage is already high (for example, above 80%). After the device is enabled to dynamically adjust the rate of packets from NAC users, the device limits the number of NAC packets received per second if the CPU or memory usage is high. This function reduces loads on the device CPU.

Example

Enable the device to dynamically adjust the rate of packets from NAC users.

```
<Huawei> system-view
[Huawei] authentication speed-limit auto
```

19.6.23 authentication termination-action reauthenticate

Function

The **authentication termination-action reauthenticate** command configures the device to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

The **undo authentication termination-action** command restores the default setting.

By default, the device is not configured to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

Format

authentication termination-action reauthenticate

undo authentication termination-action

Parameters

None

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The RADIUS server uses the **Session-Timeout** attribute to control the remaining online time of a user, and uses the **Termination-Action** attribute to determine whether to re-authenticate the user when the timeout interval expires. By default, if the RADIUS server delivers **Session-Timeout** but no **Termination-Action**, the device disconnects users when the time exceeds the value of **Session-Timeout**. To re-authenticate users without modifying the server configuration, you can run this command to configure the device to re-authenticate users when the timeout interval expires.

Precautions

Only 802.1X authentication and MAC address authentication on Layer 2 interfaces support this function.

Example

In authentication profile **authen1**, configure the device to re-authenticate users when the time exceeds the value of **Session-Timeout** delivered by the RADIUS server.

```
<Huawei> system-view
[Huawei] authentication-profile name authen1
[Huawei-authen-profile-authen1] authentication termination-action reauthenticate
```

19.6.24 authentication trigger-condition (802.1X authentication)

Function

The **authentication trigger-condition** command configures the packet types that can trigger 802.1X authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP packets can trigger 802.1X authentication.

Format

authentication trigger-condition { **dhcp** | **arp** } *

undo authentication trigger-condition [**dhcp** | **arp**] *

Parameters

Parameter	Description	Value
dhcp	Triggers 802.1X authentication through DHCP packets.	-
arp	Triggers 802.1X authentication through ARP packets.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After 802.1X authentication is enabled, the device can trigger 802.1X authentication on users by default when receiving DHCP or ARP packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger 802.1X authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger 802.1X authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger 802.1X authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

Precautions

This function takes effect only for users who go online after this function is successfully configured.

When MAC address authentication and 802.1X authentication are both enabled on an interface, packets that can trigger authentication include all the packet types that can trigger authentication in the MAC access profile and 802.1X access profile. For example, assume that ARP packets in the MAC access profile are unable to trigger authentication and ARP packets in the 802.1X access profile can trigger authentication. If MAC address authentication and 802.1X authentication are both enabled on an interface, ARP packets can trigger MAC address authentication.

Example

In the 802.1X access profile **d1**, configure the device to use DHCP packets to trigger 802.1X authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] authentication trigger-condition dhcp
```

19.6.25 authentication trigger-condition (MAC address authentication)

Function

The **authentication trigger-condition** command configures the packet types that can trigger MAC address authentication.

The **undo authentication trigger-condition** command restores the default configuration.

By default, DHCP/ARP packets can trigger MAC address authentication.

Format

authentication trigger-condition { **dhcp** | **arp** } *

undo authentication trigger-condition [**dhcp** | **arp**] *

Parameters

Parameter	Description	Value
dhcp	Triggers MAC address authentication through DHCP packets.	-
arp	Triggers MAC address authentication through ARP packets.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After MAC address authentication is enabled, the device can trigger MAC address authentication on users by default when receiving DHCP/ARP packets. Based on user information on the actual network, the administrator can adjust the packet types that can trigger MAC address authentication. For example, if all users on a network dynamically obtain IPv4 addresses, the device can be configured to trigger MAC address authentication only through DHCP packets. This prevents the device from continuously sending ARP packets to trigger MAC address authentication when static IPv4 addresses are configured for unauthorized users on the network, and reduces device CPU occupation.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- After the VLANIF interface is enabled with the MAC address authentication function, MAC address authentication cannot be triggered for users when the interface receives DHCP packets.
- This function takes effect only for users who go online after this function is successfully configured.
- Only wired users support MAC address authentication triggered by DHCP/ARP packets. For wireless users, MAC address authentication is triggered by association packets.
- When MAC address authentication and 802.1X authentication are both enabled on an interface, packets that can trigger authentication include all the packet types that can trigger authentication in the MAC access profile and 802.1X access profile. For example, assume that ARP packets in the MAC access profile are unable to trigger authentication and ARP packets in the 802.1X access profile can trigger authentication. If MAC address authentication and 802.1X authentication are both enabled on an interface, ARP packets can trigger MAC address authentication.

Example

In the MAC access profile **m1**, configure the device to trigger MAC address authentication only through ARP packets.

```
<Huawei> system-view
[Huawei] mac-access-profile name m1
[Huawei-mac-access-profile-m1] authentication trigger-condition arp
```

19.6.26 authentication-profile (Interface view or VAP profile view)

Function

The **authentication-profile** command applies an authentication profile to the interface or VAP profile.

The **undo authentication-profile** command restores the default setting.

By default, no authentication profile is applied to the interface or VAP profile.

Format

authentication-profile *authentication-profile-name*

undo authentication-profile

Parameters

Parameter	Description	Value
authentication-profile-name	Specifies the name of an authentication profile.	The value must be an existing authentication profile name.

Views

interface or VAP profile

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An authentication profile uniformly manages NAC configuration. The authentication profile is bound to the interface or VAP profile view to enable NAC, implementing access control on the users in the interface or VAP profile. The authentication type of the users in the interface or VAP profile is determined by the access profile bound to the authentication profile.

Prerequisites

An authentication profile has been created using the **19.6.27 authentication-profile (system view)** command in the system view.

When configuring NAC, pay attention to the following points:

- Layer 2 physical interfaces, Layer 3 physical interfaces, routed main interfaces, VLANIF interfaces, WAN-side interfaces, port groups, and VAP profiles support NAC. The support for authentication types on different interfaces is as follows:
  - Layer 2 physical interfaces: 802.1X authentication, MAC address authentication, and Layer 2 Portal authentication

    NOTE

    The Layer 2 physical interfaces of AR100&AR120&AR150&AR160&AR200 do not support Layer 2 Portal authentication, and support only 802.1X authentication in multicast mode.
  - Layer 3 physical interfaces and routed main interface: Layer 3 Portal authentication

    NOTE

    In wireless scenarios, it does not support Layer 3 Portal authentication.
  - VLANIF interfaces: Layer 2 Portal authentication, MAC address-prioritized Portal authentication in Fat AP Wi-Fi scenarios, and Layer 3 Portal authentication.
  - WAN-side interfaces: Layer 3 Portal authentication
- Physical interfaces do not support multi-mode authentication modes containing Portal authentication.
- For the access of wireless users through APs, ensure that the APs can be authenticated (for example, adding the APs to static users) when NAC authentication is deployed for users. Otherwise, the wireless users cannot be authenticated.
- NAC authentication cannot be enabled both on a Layer 2 Ethernet interface and the VLANIF interface mapping the VLAN of the Ethernet interface. Otherwise, the users have no network access rights after connecting to the

network. In addition, NAC authentication cannot be enabled both on VAP profiles and VLANIF interfaces in wireless scenarios.

- After enabling NAC on an interface, you cannot run the following commands on the interface. Similarly, after running the following commands on an interface, you cannot enable NAC on the interface.

Command	Function
mac-limit	Sets the maximum number of MAC addresses that can be learned by an interface.
mac-address learning disable	Disables MAC address learning on an interface.
port-security enable	Enables port security.

Example

Apply the authentication profile **m1** to VLANIF10.

```
<Huawei> system-view
[Huawei] authentication-profile name m1
[Huawei-authen-profile-m1] quit
[Huawei] interface vlanif 10
[Huawei-Vlanif10] authentication-profile m1
```

19.6.27 authentication-profile (system view)

Function

The **authentication-profile** command creates an authentication profile and displays the authentication profile view.

The **undo authentication-profile** command deletes the authentication profile.

By default, the device has six built-in authentication profiles: default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile.

Format

authentication-profile name *authentication-profile-name*

undo authentication-profile name *authentication-profile-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
name *authentication-profile-name*	Specifies the name of an authentication profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NAC can implement access control on users. The device uses authentication profiles to uniformly manage NAC configuration so that users can easily configure NAC functions. The parameters (for example, the bound access profile and authentication type) in the authentication profile can be configured to provide various access control modes for different users. After the configuration is complete, the authentication profile is applied to the interface or VAP profile to enable NAC.

Follow-up Procedure

1. Configuring authentication profiles: Configure the access profile, and authorization information in the authentication profiles.
2. Applying authentication profiles: Run the **19.6.26 authentication-profile (Interface view or VAP profile view)** command to apply the authentication profiles to the interface or VAP profile.

Precautions

- The device supports a maximum of 8 authentication profiles. The built-in authentication profile **default_authen_profile** and the compatibility profile converted after an upgrade are not counted in the configuration specification. The six built-in authentication profiles (default_authen_profile, dot1x_authen_profile, mac_authen_profile, portal_authen_profile, dot1xmac_authen_profile, and multi_authen_profile) can be modified and applied, but cannot be deleted.
- Before deleting an authentication profile, ensure that this profile is not bound to any interface or VAP profile. You can run the **19.6.31 display**

authentication-profile configuration command to check whether the authentication profile is bound to interface or VAP profile

Example

Create the authentication profile named **mac_authen_profile1**.

```
<Huawei> system-view
[Huawei] authentication-profile name mac_authen_profile1
```

Related Topics

19.6.72 dot1x-access-profile (authentication profile view)

19.6.82 mac-access-profile (authentication profile view)

19.6.129 portal-access-profile (authentication profile view)

19.6.31 display authentication-profile configuration

19.6.28 cut web-authentication-user

Function

The **cut web-authentication-user** command configures the device to force Portal authentication users offline when a 3G/LTE link is disconnected.

The **undo cut web-authentication-user** command configures the device not to force Portal authentication users offline when a 3G/LTE link is disconnected.

By default, the Portal authentication users are still online when the 3G/LTE link is disconnected.

Format

cut web-authentication-user [**domain** *domain-name* | **ssid** *ssid*]

undo cut web-authentication-user

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name used in Portal authentication. After this parameter is specified, the device forcibly disconnects the users who use this domain name to go online when the 3G/LTE link is disconnected.	The value must be an existing domain name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ssid *ssid*	Specifies the service set identifier (SSID) of the wireless network. After this parameter is specified, the device forcibly disconnects the users who connect to this wireless network when the 3G/LTE link is disconnected.	The value must be an existing SSID.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

When the router functioning as a mobile Internet gateway is deployed on a bus or metro, only the users who pass Portal authentication can connect to the vehicle-mounted Wi-Fi network and access external networks using the 3G/LTE interface. After the 3G/LTE link is disconnected, the users are not disconnected in real time while they cannot access any web page immediately. This had a negative effect on user experience.

After you run the **cut web-authentication-user** command on the 3G/LTE interface, the device forces Portal authentication users offline when the 3G/LTE link is disconnected. The disconnected users can still access internal network resources of the router, so they can have good user experience.

Example

Configure the device to forcibly disconnect the users who connect to the wireless network **bus-wlan** when the 3G/LTE link is disconnected.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] cut web-authentication-user ssid bus-wlan
```

19.6.29 display access-user

Function

The **display access-user** command displays information about NAC access users.

Format

display access-user service-scheme *service-scheme*

display access-user user-group *user-group-name*

Parameters

Parameter	Description	Value
service-scheme *service-scheme*	Displays information about users assigned with a specified service scheme.	The value must be the name of an existing service scheme.
user-group *user-group-name*	Displays information about users in a specified user group.	The value must be the name of an existing user group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about online NAC users.

Example

Display information about users who are assigned the service scheme **huawei**.

```
<Huawei> display access-user service-scheme huawei
 ------------------------------------------------------------------------------
 UserID Username              IP address      MAC           Status
 ------------------------------------------------------------------------------
 16018  zqm                   10.12.12.254    78ac-c0c2-0175 Pre-authen
 ------------------------------------------------------------------------------
 Total: 1, printed: 1
```

NOTE

Only letters, digits, and special characters can be displayed for **username**.

When the value of **username** contains special characters or characters in other languages except English, the device displays dots (.) for these characters. If there are more than three such consecutive characters, three dots (.) are displayed. Here, the special characters are the ASCII codes smaller than 32 (space) or larger than 126 (~).

When the value of **username** is longer than 20 characters, the device displays up to three dots (.) for the characters following 19; that is, only 22 characters are displayed.

Table 19-40 Description of the **display access-user** command output

Item	Description
UserID	ID automatically allocated to an online user by the device.
Username	User name.
IP address	User IP address. When both IPv4 and IPv6 addresses exist, only the IPv4 address is recorded. When only IPv6 addresses exist, only the latest updated IPv6 address is recorded.
MAC	User MAC address.
Status	User status.

19.6.30 display authentication interface

Function

The **display authentication interface** command displays the configuration of the NAC authentication mode on an interface.

Format

display authentication interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface-type interface-number	Displays the configuration of the NAC authentication mode on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the NAC authentication mode, you can run this command to check the configuration.

Example

Display the configuration of the NAC authentication mode on Eth2/0/0.

```
<Huawei> display authentication interface ethernet 2/0/0
Authentication profile: p1
Port authentication order:
                    MAC
                    DOT1X
                    WEB
```

Table 19-41 Description of the **display authentication interface** command output

Item	Description
Authentication profile	Name of the authentication profile applied to the interface.
Port authentication order	Authentication mode configured in the authentication profile applied to the interface. Authentication modes include: ● MAC: indicates the MAC address authentication mode. ● DOT1X: indicates the 802.1X authentication mode. ● WEB: indicates the Portal authentication mode.

19.6.31 display authentication-profile configuration

Function

The **display authentication-profile configuration** command displays the configuration of an authentication profile.

Format

display authentication-profile configuration [**name** *authentication-profile-name*]

Parameters

Parameter	Description	Value
name *authentication-profile-name*	Displays the configuration of a specified authentication profile. If **name** *authentication-profile-name* is not specified, the device displays all the authentication profiles configured on the device.	The value must be the name of an existing authentication profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an authentication profile, you can run this command to check whether the configuration is correct.

NOTE

The built-in authentication profile **default_authen_profile** is not counted in the configuration specification. The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is also not counted in the configuration specification.

Example

Display all the authentication profiles configured on the device.

```
<Huawei> display authentication-profile configuration
-------------------------------------------------------------------------------
  ID       Auth-profile name
-------------------------------------------------------------------------------
   0       default_authen_profile
   1       dot1x_authen_profile
   2       mac_authen_profile
   3       portal_authen_profile
   4       dot1xmac_authen_profile
-------------------------------------------------------------------------------
  Total 5, printed 5
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-42 Description of the **display authentication-profile configuration** command output

Item	Description
ID	Authentication profile ID.
Auth-profile name	Authentication profile name.

Display the configuration of the authentication profile **p1**.

```
<Huawei> display authentication-profile configuration name p1
  Profile name                              : p1
  Dot1x access profile name                 : -
  Mac access profile name                   : -
  Portal access profile name                : testdel
  Free rule template                        : -
  Force domain                              : -
  Dot1x force domain                        : -
  Mac-authen force domain                   : -
  Portal force domain                       : -
  Default domain                            : 110
  Dot1x default domain                      : -
  Mac-authen default domain                 : -
  Portal default domain                     : -
  Permit domain                             : -
  Authentication handshake                  : Enable
  Authentication handshake period           : 300s
  Auth-fail re-auth period                  : 60s
  Pre-auth re-auth period                   : 60s
  Auth-fail aging time                      : 82800s
  Pre-auth aging time                       : 82800s
  Dot1x-mac-bypass                          : Disable
  Single-access                             : Disable
  Device-type authorize service-scheme      : -
  Authentication mode                       : multi-authen
  Authen-fail authorize service-scheme      : -
  Authen-server-down authorize service-scheme : -
  Pre-authen authorize service-scheme       : -
  Security-name-delimiter                   : -
  Domain-name-delimiter                     : -
  Domain-location                           : -
  Domainname-parse-direction                : -
  Bound vap profile                         : -
  SVF flag                                  : Disable
  Ip-static-user                            : Disable
  Roam-realtime-accounting                  : Enable
  Update-IP-realtime-accounting             : Enable
  IP-address in-accounting-start            : Enable
  IP-address arp-delay                      : Disable
  Update-session-mode                       : Disable
  Linkdown offline delay time               : 50
  LDAP-server template                      : -
  AD-server template                        : -
  Termination action                        : reauthenticate
  Authentication roam pre-authen mac-authen : Enable
```

Table 19-43 Description of the **display authentication-profile configuration name** command output

Item	Description
Profile name	Authentication profile name.

Item	Description
Dot1x access profile name	802.1X access profile bound to the authentication profile. To configure an 802.1X access profile, run the **19.6.72 dot1x-access-profile (authentication profile view)** command.
Mac access profile name	MAC access profile bound to the authentication profile. To configure a MAC access profile, run the **19.6.82 mac-access-profile (authentication profile view)** command.
Portal access profile name	Portal access profile bound to the authentication profile. To configure a Portal access profile, run the **19.6.129 portal-access-profile (authentication profile view)** command.
Free rule template	Authentication-free rule profile bound to the authentication profile. To configure an authentication-free rule profile, run the **19.6.76 free-rule-template (authentication profile view)** command.
Force domain	Forcible domain for users. To configure a forcible domain, run the **19.6.1 access-domain** command.
Dot1x force domain	Forcible domain for 802.1X authentication users. To configure a forcible domain for 802.1X authentication users, run the **19.6.1 access-domain** command.
Mac-authen force domain	Forcible domain for MAC address authentication users. To configure a forcible domain for MAC address authentication users, run the **19.6.1 access-domain** command.
Portal force domain	Forcible domain for Portal authentication users. To configure a forcible domain for Portal authentication users, run the **19.6.1 access-domain** command.
Default domain	Default domain for users. To configure a default domain for users, run the **19.6.1 access-domain** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dot1x default domain	Default domain for 802.1X authentication users. To configure a default domain for 802.1X authentication users, run the **19.6.1 access-domain** command.
Mac-authen default domain	Default domain for MAC address authentication users. To configure a default domain for MAC address authentication users, run the **19.6.1 access-domain** command.
Portal default domain	Default domain for Portal authentication users. To configure a default domain for Portal authentication users, run the **19.6.1 access-domain** command.
Permit domain	Permitted domain for users. To configure a permitted domain, run the **19.1.74 permit-domain** command.
Authentication handshake	Whether the handshake function is enabled. ● Enable ● Disable To enable the handshake function, run the **19.6.6 authentication handshake** command.
Authentication handshake period	Handshake interval. To configure the handshake interval, run the **19.6.16 authentication timer handshake-period** command.
Auth-fail re-auth period	Interval for re-authenticating users who fail to be authenticated. To configure the interval, run the **19.6.19 authentication timer re-authen** command.
Pre-auth re-auth period	Interval for re-authenticating pre-connection users. To configure the interval, run the **19.6.19 authentication timer re-authen** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Auth-fail aging Time	Aging time for entries of the users who fail to be authenticated. To configure the aging time, run the **19.6.17 authentication timer authen-fail-aging** command.
Pre-auth aging Time	Aging time for pre-connection user entries. To configure the aging time, run the **19.6.18 authentication timer pre-authen-aging** command.
Dot1x-mac-bypass	Whether MAC address bypass authentication is enabled. ● Enable ● Disable To configure the function, run the **19.6.8 authentication dot1x-mac-bypass** command.
Single-access	Whether the device allows users to access in only one authentication mode. To configure the function, run the **19.6.15 authentication single-access** command.
Authentication mode	User access mode. To configure the mode, run the **19.6.21 authentication mode** command.
Authen-fail authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users who fail to be authenticated. To configure the name, run the **19.6.9 authentication event action authorize** command.
Authen-server-down authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users when the authentication server is Down. To configure the name, run the **19.6.9 authentication event action authorize** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Pre-authen authorize service-scheme	Name of the service scheme based on which the device assigns network access rights to users who are in the pre-connection state. To configure the name, run the **19.6.9 authentication event action authorize** command.
Security-name-delimiter	Security string delimiter. To configure the delimiter, run the **19.1.88 security-name-delimiter** command.
Domain-name-delimiter	Domain name delimiter. To configure the delimiter, run the **19.1.53 domain-name-delimiter** command.
Domain-location	Domain name location. To configure the location, run the **19.1.52 domain-location** command.
Domainname-parse-direction	Domain name resolution direction. To configure the direction, run the **19.1.54 domainname-parse-direction** command.
Bound vap profile	VAP profile to which the authentication profile is bound. To configure the VAP profile, run the **19.6.26 authentication-profile (Interface view or VAP profile view)** command.
SVF flag	The flag of SVF status. • Enable • Disable
Ip-static-user	Whether the function of identifying static users through IP addresses is enabled. • Enable • Disable
Roam-realtime-accounting	Whether a device is enabled to send accounting packets for roaming. • Enable • Disable To configure the function, run the **19.1.17 authentication { roam-accounting | update-ip-accounting } * enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Update-IP-realtime-accounting	Whether a device is enabled to send accounting packets for address updating. ● Enable ● Disable To configure the function, run the **19.1.17 authentication { roam-accounting | update-ip-accounting } * enable** command.
Linkdown offline delay time	User logout delay when an interface link is faulty. To configure the delay, run the **19.6.81 link-down offline delay** command.
IP-address in-accounting-start	Whether the function of carrying users' IP addresses in Accounting-Start packets is enabled. ● Enable ● Disable To configure the function, run the **19.6.14 authentication ip-address in-accounting-start** command.
Update-session-mode	Whether to use the accounting session update mode during roaming accounting. ● Enable ● Disable To configure the function, run the **19.1.18 authentication roam-accounting update-session-mode**.
LDAP-server template	LDAP server template bound to the authentication profile.
AD-server template	AD server template bound to the authentication profile.
Termination action	Action that the device takes when the timeout period specified by the Session-Timeout attribute delivered by the RADIUS server expires. ● reauthenticate To configure the function, run the **19.6.23 authentication termination-action reauthenticate** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication roam pre-authen mac-authen	Whether to enable MAC address authentication for roaming STAs. ● Enable ● Disable To configure this function, run the **19.6.20 authentication roam pre-authen mac-authen enable** command.

19.6.32 display dot1x

Function

The **display dot1x** command displays 802.1X authentication information.

Format

display dot1x [**statistics**] [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-5>]

Parameters

Parameter	Description	Value
statistics	Displays statistics on 802.1X authentication. The statistics about 802.1X authentication is displayed only when this parameter is specified.	-
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays 802.1X authentication information of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, 802.1X authentication information of all interfaces is displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display dot1x** command to view configuration results of all configuration commands in 802.1X authentication and statistics about 802.1X packets.

The command output helps you to check whether the current 802.1X authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

The **display dot1x** command displays the statistics on 802.1X packets. You can locate the fault according to the packet statistics. When the fault is rectified, run the **reset dot1x statistics** command to clear the packet statistics. After a period of time, run the **display dot1x** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display 802.1X authentication information.

Display 802.1X statistics.

```
<Huawei> display dot1x statistics
  Max users: 2048
  Current users: 0
  Global default domain is default
  Quiet function is Disabled
  Mc-trigger port-up-send is Enabled
  Parameter set:Quiet Period                60s   Quiet-times          3
                Tx Period                   30s   Mac-By-Pass Delay   30s
  Dot1x URL: Not configed.

 GigabitEthernet7/0/0 status: DOWN  802.1x protocol is
Enabled
  Controlled User(s) amount to  0

  Authentication Success: 0          Failure: 0
  Enter Enquence        : 0
  EAPOL Packets: TX     : 1          RX     : 0
  Sent      EAPOL Request/Identity Packets       : 0
            EAPOL Request/Challenge Packets      : 0
            Multicast Trigger Packets            : 1
            EAPOL Success Packets                : 0
            EAPOL Failure Packets                : 0
  Received  EAPOL Start Packets                  : 0
            EAPOL Logoff Packets                 : 0
            EAPOL Response/Identity Packets      : 0
            EAPOL Response/Challenge Packets     : 0
```

Table 19-44 Description of the **display dot1x** command output

Item	Description
Max users	Maximum number of global online users.
Current users	Number of current online users.
Global default domain is	Global default authentication domain. To configure the global default authentication domain, run the **19.1.51 domain (system view)** command.
Quiet function is	Whether the quiet function is enabled. ● Enabled. ● Disabled. To configure the quiet function, run the **dot1x quiet-period** command.
Mc-trigger port-up-send is	Whether the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is enabled. ● Enabled. ● Disabled. To configure the function, run the **dot1x mc-trigger port-up-send enable** command.
Parameter set	Settings of 802.1X parameters: ● Quiet Period: specifies the quiet period set by the quiet timer. To configure the quiet period, run the **dot1x timer quiet-period** command. ● Quiet-times: specifies the maximum number of authentication failures before the device quiets a user. To configure the maximum value, run the **dot1x quiet-times** command. ● Tx Period: specifies the interval for sending authentication requests. To configure the interval, run the **dot1x timer tx-period** command. ● Mac-By-Pass Delay: specifies the value of the delay timer for MAC address bypass authentication.
Dot1x URL	Redirect-to URL for HTTP access of 802.1X users. To configure the redirect-to URL, run the **dot1x url** command.
Dot1x access profile is	802.1X access profile name. To configure the 802.1X access profile name, run the **19.6.73 dot1x-access-profile (system view)** command.
Authentication mode is	User access mode. To configure the user access mode, run the **19.6.21 authentication mode** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Authentication method is	Authentication mode of 802.1X users. To configure the authentication mode of 802.1X users, run the **19.6.55 dot1x authentication-method** command.
Reauthentication is	Whether re-authentication is enabled for online 802.1X users. To configure the function, run the **19.6.63 dot1x reauthenticate** command.
Dot1x retry times	Maximum number of attempts to send authentication requests to 802.1X users. To configure maximum number of attempts to send authentication requests to 802.1X users, run the **19.6.64 dot1x retry** command.
Authenticating users	Number of users who are being authenticated.
Maximum users	Maximum number of online users on the interface.
Current users	Number of online users on the interface.
Authentication Success Failure	Number of successful and failed authentications. The statistics include statistics on online 802.1X users but not on the users using MAC address bypass authentication.
Enter Enquence	Number of packets entering the queue.
EAPOL Packets: TX RX	Number of globally received and sent EAPOL packets.
EAPOL Request/ Identity Packets	Number of globally received and sent EAPOL Request/ Identity packets.
EAPOL Request/ Challenge Packets	Number of globally received and sent EAPOL Request/ Challenge packets.
Multicast Trigger Packets	Number of globally received and sent multicast packets that trigger authentication.
EAPOL Success Packets	Number of globally received and sent EAPOL Success packets.
EAPOL Failure Packets	Number of globally received and sent EAPOL Failure packets.
EAPOL Start Packets	Number of globally received and sent EAPOL Start packets.
EAPOL Logoff Packets	Number of globally received and sent EAPOL LogOff packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
EAPOL Response/ Identity Packets	Number of globally received and sent EAPOL Response/ Identity packets.
EAPOL Response/ Challenge Packets	Number of globally received and sent EAPOL Response/ Challenge packets.
Controlled User(s) amount to	Number of users who pass authentication successfully.

19.6.33 display dot1x-access-profile configuration

Function

The **display dot1x-access-profile configuration** command displays the configuration of an 802.1X access profile.

Format

display dot1x-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of an 802.1X access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the 802.1X access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified 802.1X access profile.	The value must be the name of an existing 802.1X access profile.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After configuring an 802.1X access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the 802.1X access profiles configured on the device.

```
<Huawei> display dot1x-access-profile configuration
-------------------------------------------------------------------------------
 ID            Dot1x-Access-Profile Name
-------------------------------------------------------------------------------
 0             dot1x_access_profile
 1             d1
 2             d2
 3             d3
 4             d4
-------------------------------------------------------------------------------
 Total: 5 printed: 5.
```

Table 19-45 Description of the **display dot1x-access-profile configuration** command output

Item	Description
ID	802.1X access profile ID.
Dot1x-Access-Profile Name	802.1X access profile name.

Display the configuration of the 802.1X access profile **d1**.

```
<Huawei> display dot1x-access-profile configuration name d1
  Profile Name                  : d1
  Authentication method         : EAP
  Port control                  : authorized-force
  Re-authen                     : Disable
  Client-no-response authorize : -
  Trigger condition             :
  Unicast trigger               : Disable
  Trigger dhcp-bind             : Disable
  Handshake                     : Disable
  Max retry value               : 2
  Reauthen Period               : 3600s
  Client Timeout                : 5s
  Handshake Period              : 15s
  Bound authentication profile : p2
```

Table 19-46 Description of the **display dot1x-access-profile configuration name** command output

Item	Description
Profile Name	802.1X access profile name.
Authentication method	Authentication mode of 802.1X users: ● CHAP ● PAP ● EAP To configure the authentication mode, run the **19.6.55 dot1x authentication-method** command.
Port control	802.1X authentication interface's authorization status: ● auto ● authorized-force ● unauthorized-force To set an authorization state for an interface, run the **19.6.74 dot1x port-control** command.
Re-authen	Whether re-authentication for online 802.1X users is enabled: ● Enable ● Disable To configure the re-authentication function, run the **19.6.63 dot1x reauthenticate** command.
Client-no-response authorize	Network access rights granted to users when the 802.1X client does not respond. To configure the network access rights, run the **19.6.11 authentication event client-no-response action authorize** command.
Trigger condition	Packet type that can trigger 802.1X authentication: ● dhcp ● arp To configure the packet type, run the **19.6.24 authentication trigger-condition (802.1X authentication)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Unicast trigger	Whether 802.1X authentication triggered by unicast packets is enabled: ● Enable ● Disable To configure the function, run the **19.6.70 dot1x unicast-trigger** command.
Trigger dhcp-bind	Whether the device is enabled to automatically generate DHCP snooping binding entries for users with static IP addresses: ● Enable ● Disable To configure the function, run the **19.6.67 dot1x trigger dhcp-binding** command.
Handshake	Whether handshake with online 802.1X authentication users is enabled: ● Enable ● Disable To configure the function, run the **19.6.57 dot1x handshake** command.
Max retry value	Maximum number of attempts to send authentication requests to 802.1X users. To configure the maximum value, run the **19.6.64 dot1x retry** command.
Reauthen Period	Re-authentication interval for online 802.1X users. To configure the re-authentication interval, run the **19.6.65 dot1x timer** command.
Client Timeout	Authentication timeout period for 802.1X clients. To configure the authentication timeout period, run the **19.6.65 dot1x timer** command.
Handshake Period	Interval at which the device handshakes with an 802.1X client on a non-Eth-Trunk interface. To configure the interval, run the **19.6.65 dot1x timer** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Bound authentication profile	Authentication profile to which the 802.1X access profile is bound. To configure the authentication profile, run the **19.6.72 dot1x-access-profile (authentication profile view)** command.

19.6.34 display dot1x quiet-user

Function

The **display dot1x quiet-user** command displays information about 802.1X authentication users who are quieted.

Format

display dot1x quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all 802.1X authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a quiet 802.1X authentication user with a specified MAC address.	The value is in H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about 802.1X authentication users who are quieted.

Example

Display information about all 802.1X authentication users who are quieted.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display dot1x quiet-user all
--------------------------------------------------------------------------------
MacAddress                                  Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
0001-0002-0003                                50
--------------------------------------------------------------------------------
1 silent mac address(es) found, 1 printed.
```

Table 19-47 Description of the **display dot1x quiet-user all** command output

Item	Description
MacAddress	MAC address of an 802.1X authentication user who is quieted.
Quiet Remain Time(Sec)	Remaining quiet time of an 802.1X authentication user who is quieted, in seconds.

19.6.35 display free-rule-template configuration

Function

The **display free-rule-template configuration** command displays the configuration of an authentication-free rule profile.

Format

display free-rule-template configuration [**name** *free-rule-name*]

Parameters

Parameter	Description	Value
name *free-rule-name*	Displays the configuration of an authentication-free rule profile with a specified name. If **name** *free-rule-name* is not specified, the device displays all the authentication-free rule profiles configured on the device. If **name** *free-rule-name* is specified, the device displays the configuration of a specified authentication-free rule profile.	The value must be the name of an existing authentication-free rule profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring an authentication-free rule profile, you can run this command to check whether the configuration is correct.

Example

Display all the authentication-free rule profiles configured on the device.

```
<Huawei> display free-rule-template configuration
-------------------------------------------------------------------------------
 ID            Free-rule-template Name
-------------------------------------------------------------------------------
 0             default_free_rule
-------------------------------------------------------------------------------
 Total: 1 printed: 1.
```

Table 19-48 Description of the **display free-rule-template configuration** command output

Item	Description
ID	ID of an authentication-free rule profile.
Free-rule-template Name	Name of an authentication-free rule profile.

19.6.36 display mac-address authen

Function

The **display mac-address authen** command displays the current authen MAC address entries in the system.

Format

display mac-address authen [*interface-type interface-number* | **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After MAC address authentication or 802.1X authentication is configured successfully, the administrator can run this command to check the existing authen MAC address entries on the device. The administrator can check information about user access based on these MAC address entries to locate user access faults. The **authen** entry is generated after a user passes MAC address authentication or 802.1X authentication.

Precautions

If there are a lot of **authen** MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all authen MAC address entries in the system.

```
<Huawei> display mac-address authen
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge/VSI        Learned-From            Type
--------------------------------------------------------------------------------
```

```
0000-0000-0100   3000                    GE2/0/0        authen
0000-0000-0400   3000                    GE2/0/0        authen
0000-0000-0200   3000                    GE2/0/0        authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 19-49 Description of the **display mac-address authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/Bridge/VSI	VLAN/Bridge/VSI that the outbound interface belongs to.
Learned-From	Interface on which a MAC address is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

19.6.37 display mac-address pre-authen

Function

The **display mac-address pre-authen** command displays the current pre-authen MAC address entries in the system.

Format

display mac-address pre-authen [*interface-type interface-number* | **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays MAC address entries in a specified VLAN. If no VLAN is specified, MAC address entries in all VLANs of the device are displayed.	The value is an integer that ranges from 1 to 4094.
interface-type interface-number	Displays MAC address entries on a specified interface. If no interface is specified, MAC address entries on all interfaces of the device are displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to check the existing MAC address entries of the pre-connection type to obtain access information about pre-connection users and locate faults.

Precautions

If there are a lot of pre-authen MAC address entries, you can specify a VLAN or use a pipe operator (|) to filter the output information. Otherwise, the following problems may occur due to excessive output information:

- The displayed information is refreshed repeatedly on the terminal screen and the administrator cannot obtain the required information.
- The device traverses and retrieves information for a long time, and does not respond to any request.

Example

Display all pre-authen MAC address entries in the system.

```
<Huawei> display mac-address pre-authen
--------------------------------------------------------------------------------
MAC Address       VLAN/Bridge/VSI        Learned-From              Type
--------------------------------------------------------------------------------
0000-0000-0100    3000                       GE2/0/0           pre-authen
0000-0000-0400    3000                       GE2/0/0           pre-authen
0000-0000-0200    3000                       GE2/0/0           pre-authen
--------------------------------------------------------------------------------
Total items displayed = 3
```

Table 19-50 Description of the **display mac-address pre-authen** command output

Item	Description
MAC Address	MAC address of a user to be authenticated.
VLAN/Bridge/VSI	VLAN/Bridge/VSI that the interface belongs to.
Learned-From	Interface on which a MAC address of a user to be authenticated is learned.
Type	Type of a MAC address entry.
Total items displayed	Total number of MAC address entries that match the filter condition.

 Copyright © Huawei Technologies Co., Ltd.

19.6.38 display mac-access-profile configuration

Function

The **display mac-access-profile configuration** command displays the configuration of a MAC access profile.

Format

display mac-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of a MAC access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the MAC access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified MAC access profile.	The value must be the name of an existing MAC access profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a MAC access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display all the MAC access profiles configured on the device.

```
<Huawei> display mac-access-profile configuration
--------------------------------------------------------------------------------
 ID          Mac-Access-Profile Name
--------------------------------------------------------------------------------
 0           mac_access_profile
 1           m1
 2           m2
 3           m3
 4           m4
--------------------------------------------------------------------------------
 Total: 5 printed: 5.
```

Table 19-51 Description of the **display mac-access-profile configuration** command output

Item	Description
ID	MAC access profile ID.
Mac-Access-Profile Name	MAC access profile name.

Display the configuration of the MAC access profile **m1** (the MAC address authentication user configures a password).

```
<Huawei> display mac-access-profile configuration name m1
  Profile Name                 : m1
  Authentication method        : CHAP
  Username format              : fixed username: a1
  Password type                : cipher
  Re-authen                    : Disable
  Trigger condition            : arp dhcp
  Trigger dhcp-bind            : Enable
  Reauthen Period              : 1800s
  Bound authentication profile : -
```

Display the configuration of the MAC access profile **m2** (the MAC address authentication user does not configure a password).

```
<Huawei> display mac-access-profile configuration name m2
  Profile Name                 : m2
  Authentication method        : CHAP
  Username format              : fixed username: a1
  Password                     : not configured
  Re-authen                    : Disable
  Trigger condition            : arp dhcp
  Trigger dhcp-bind            : Enable
  Reauthen Period              : 1800s
  Bound authentication profile : -
```

Table 19-52 Description of the **display mac-access-profile configuration name** command output

Item	Description
Profile Name	MAC access profile name.

Item	Description
Authentication method	Authentication mode for MAC address authentication. ● CHAP ● PAP To configure the authentication mode, run the **19.6.84 mac-authen authentication-method** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Username format	User name format for MAC address authentication. ● use MAC address without-hyphen as username: A user name is a MAC address that does not contain hyphens (-), for example, 0005e01c02e3. ● use MAC address with-hyphen as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-e01c-02e3. ● use MAC address with-hyphen normal as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-e0-1c-02-e3. ● use MAC address without-hyphen upper as username: A user name is a MAC address in the uppercase format that does not contain hyphens (-), for example, 0005E01C02E3. ● use MAC address with-hyphen upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-E01C-02E3. ● use MAC address with-hyphen normal upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-E0-1C-02-E3. ● use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every four digits, for example, 0005:e01c:02e3. ● use MAC address with-hyphen normal colon as username A user name is a MAC address that contains colons (:) and the colons are inserted between every two digits, for example, 00:05:e0:1c:02:e3.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
	• use MAC address with-hyphen colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every four digits, for example, 0005:E01C:02E3. • use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every two digits, for example, 00:05:E0:1C:02:E3. • fixed username: The user name is fixed. • use option82 as username: The content of the Option 82 field is used as the user name. • not configured: The user name format is not configured. To configure the user name format, run the **19.6.93 mac-authen username** command.
Password type	Password display mode for MAC address authentication. • cipher To configure the password display mode, run the **19.6.93 mac-authen username** command.
password	Password of the MAC address authentication user. This field has the following fixed value: • not configured: indicates that the MAC address authentication user does not configure a password.
Re-authen	Whether re-authentication for online MAC address authentication users is enabled: • Enable: indicates that re-authentication is enabled. • Disable: indicates that re-authentication is disabled. To configure the re-authentication function, run the **19.6.89 mac-authen reauthenticate** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trigger condition	Packet type that can trigger MAC address authentication. To configure the packet type, run the **19.6.25 authentication trigger-condition (MAC address authentication)** command.
Trigger dhcp-bind	Whether the device is enabled to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-connection phase: ● Enable ● Disable To configure the function, run the **19.6.92 mac-authen trigger dhcp-binding** command.
Reauthen Period	Re-authentication interval for online MAC address authentication users. To configure the re-authentication interval, run the **19.6.91 mac-authen timer reauthenticate-period** command.
Bound authentication profile	Authentication profile to which the MAC access profile is bound. To configure the authentication profile, run the **19.6.82 mac-access-profile (authentication profile view)** command.

19.6.39 display mac-authen

Function

The **display mac-authen** command displays information about MAC address authentication.

Format

display mac-authen [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-5> | **configuration**]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Displays MAC authentication information of a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, MAC authentication information of all interfaces is displayed.	-
configuration	Displays the global information about MAC address authentication.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display mac-authen** command to view configuration results of all configuration commands in MAC address authentication. The command output helps you to check whether the MAC address authentication configuration is correct and isolate faults accordingly.

Follow-up Procedure

You can locate the fault according to the packet statistics that is displayed using the **display mac-authen** command. When the fault is rectified, run the **reset mac-authen statistics** command to clear the packet statistics. After a period of time, run the **display mac-authen** command again to check the packet statistics. If no error packet is found, the fault is rectified.

Example

Display the configuration of MAC address authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display mac-authen
  Quiet period is 60s
  Authentication fail times before quiet is 1
  Maximum users: 2048
  Current users: 1
  Global default domain is default

 GigabitEthernet2/0/0 state: UP.  MAC address authentication is enabled
  MAC access profile is mac_access_profile
  Reauthentication is disabled
  Maximum users: 2048
  Current users: 1
  Username format: fixed username: gcs
  Password type: cipher
  Fixed password: %^%#2}*{%bMY.D*Kw3HxDgU3CW7g'|54H&<]S,Zfu;%^%#
  Authentication Success: 22, Failure: 85

 Online user(s) info:
 UserId   MAC/VLAN          AccessTime            UserName
 ---------------------------------------------------------------------------
 37223    a088-b44d-573c/2003 2014/09/28 15:45:45     gcs
 ---------------------------------------------------------------------------
 Total: 1, printed: 1
```

Table 19-53 Description of the **display mac-authen** command output

Item	Description
Quiet period	Quiet period during which the device quiets a user who fails to be authenticated. The default value of the quiet timer is 60 seconds. To configure the quiet period, run the **19.6.90 mac-authen timer quiet-period** command.
Authentication fail times before quiet	Maximum number of authentication failures before the device quiets a user. To configure the maximum value, run the **19.6.87 mac-authen quiet-times** command.
Maximum users	Maximum number of users allowed on the device.
Current users	Number of online users.
Global default domain	Global default authentication domain. To configure the global default authentication domain, run the **19.1.51 domain (system view)** command.
interface state	Interface status: ● UP: The interface is enabled. ● DOWN: The interface is shut down.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
MAC address authentication	Whether MAC address authentication is enabled on the interface. ● enabled ● disabled
MAC access profile	MAC access profile name. To configure the MAC access profile name, run the **19.6.83 mac-access-profile (system view)** command.
Reauthentication	Whether re-authentication for MAC address authentication users is enabled. ● enabled ● disabled To configure whether re-authentication for MAC address authentication users is enabled, run the **19.6.89 mac-authen reauthenticate** command.
Current users	Number of current online users on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Username format	User name format for MAC address authentication. ● use MAC address without-hyphen as username: A user name is a MAC address that does not contain hyphens (-), for example, 0005e01c02e3. ● use MAC address with-hyphen as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-e01c-02e3. ● use MAC address with-hyphen normal as username: A user name is a MAC address that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-e0-1c-02-e3. ● use MAC address without-hyphen upper as username: A user name is a MAC address in the uppercase format that does not contain hyphens (-), for example, 0005E01C02E3. ● use MAC address with-hyphen upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every four digits, for example, 0005-E01C-02E3. ● use MAC address with-hyphen normal upper as username: A user name is a MAC address in the uppercase format that contains hyphens (-) and the hyphens are inserted between every two digits, for example, 00-05-E0-1C-02-E3. ● use MAC address with-hyphen colon as username: A user name is a MAC address that contains colons (:) and the colons are inserted between every four digits, for example, 0005:e01c:02e3. ● use MAC address with-hyphen normal colon as username: A user name is a MAC address that

Item	Description
	contains colons (:) and the colons are inserted between every two digits, for example, 00:05:e0:1c:02:e3. ● use MAC address with-hyphen colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every four digits, for example, 0005:E01C:02E3. ● use MAC address with-hyphen normal colon upper as username: A user name is a MAC address in the uppercase format that contains colons (:) and the colons are inserted between every two digits, for example, 00:05:E0:1C:02:E3. ● fixed username: The user name is fixed. ● use option82 as username: The content of the Option 82 field is used as the user name. ● not configured: The user name format is not configured. To configure the user name format for MAC address authentication, run the **19.6.93 mac-authen username** command.
Password type	Password display mode for MAC address authentication. ● cipher To configure the password display mode for MAC address authentication, run the **19.6.93 mac-authen username** command.
Fixed password	Password for MAC address authentication. To configure the password for MAC address authentication, run the **19.6.93 mac-authen username** command.
Authentication Success: *m*, Failure: *n*	Numbers of successful authentications (*m*) and failed authentications (*n*) on the interface.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Online user(s) info	Online user information. ● UserId: ID of an online user. ● MAC/VLAN: MAC address and VLAN of an online user. ● AccessTime: access time of an online user. ● UserName: name of an online user. ● Total: total number of online users. ● printed: number of displayed online users.

19.6.40 display mac-authen quiet-user

Function

The **display mac-authen quiet-user** command displays information about MAC address authentication users who are quieted.

Format

display mac-authen quiet-user { **all** | **mac-address** *mac-address* }

Parameters

Parameter	Description	Value
all	Displays information about all MAC address authentication users who are quieted.	-
mac-address *mac-address*	Displays information about a specified MAC address authentication user who is quieted.	The value is in the H-H-H format. Each H is a hexadecimal number of 1 to 4 digits.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view information about MAC address authentication users who are quieted.

Example

Display information about all MAC address authentication users who are quieted.

```
<Huawei> display mac-authen quiet-user all
--------------------------------------------------------------------------------
MacAddress                                    Quiet Remain Time(Sec)
--------------------------------------------------------------------------------
0001-0002-0003                                 50
--------------------------------------------------------------------------------
1 silent mac address(es) found, 1 printed.
```

Table 19-54 Description of the **display mac-authen quiet-user all** command output

Item	Description
MacAddress	MAC address of a MAC address authentication user who is quieted.
Quiet Remain Time(Sec)	Remaining quiet time of a MAC address authentication user who is quieted, in seconds.

19.6.41 display portal

Function

The **display portal** command displays the Portal authentication configuration.

Format

display portal [**interface** *interface-type interface-number* | **configuration**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays Portal authentication information of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, Portal authentication information of all interfaces is displayed.	-
configuration	Displays the global Portal authentication information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal** command to view the Portal authentication configuration and check whether the configuration is correct.

Example

Display the Portal authentication configuration.

```
<Huawei> display portal
  Portal max-user number:2048
  Quiet function is Enabled
  Different-server is Enabled
  Parameter set:Quiet Period        60s   Quiet-times          3
  Logout packets resend: Resend-times 3  Timeout 5s
  Portal Https Redirect: Enable

  Vlanif10 protocol status: down, web-auth-server layer2(direct)
```

Table 19-55 Description of the **display portal** command output

Item	Description
Portal max-user number	Maximum number of concurrent Portal authentication users allowed to access the device. To set the maximum number of concurrent Portal authentication users allowed to access the device, run the **19.6.120 portal max-user** command.
Quiet function is Enabled or Quiet function is Disabled	Whether the quiet function in Portal authentication is enabled: ● Enabled ● Disabled To enable the quiet function, run the **19.6.121 portal quiet-period** command.
Different-server is Enabled or Different-server is Disabled	Whether a device is enabled to process user logout requests sent by a Portal server other than the one from which users log in: ● Enabled ● Disabled To configure a device to process user logout requests sent by a Portal server other than the one from which users log in, run the **19.6.118 portal logout different-server enable** command.
Parameter set	Parameter settings of the quiet function in Portal authentication. ● Quiet Period: indicates the quiet period in Portal authentication. To set the quiet period in Portal authentication, run the **19.6.123 portal timer quiet-period** command. ● Quiet-times: indicates the maximum number of authentication failures within 60 seconds before a Portal authentication user enters the quiet state. To set the maximum number of authentication failures, run the **19.6.122 portal quiet-times** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Logout packets resend	Configuration of the logout packet re-transmission function for Portal authentication users. ● Resend-times: indicates the number of re-transmission times for Portal authentication user logout packets. ● Timeout: indicates the re-transmission interval of Portal authentication user logout packets. To set the re-transmission interval, run the **19.6.119 portal logout resend timeout** command.
Portal Https Redirect	Whether HTTPS redirection of Portal authentication is enabled: ● Enable ● Disable To enable this function, run the **19.6.102 portal https-redirect enable** command.
interface protocol status	Link layer protocol state of the interface. ● up: indicates that the interface is running properly. ● down: indicates that the interface is disabled. ● web-auth-server layer3: indicates that the authentication mode is set to Layer 3 Portal authentication on a specified interface. ● web-auth-server layer2(direct): indicates that the authentication mode is set to Layer 2 Portal authentication on a specified interface.

19.6.42 display portal local-server connect

Function

The **display portal local-server connect** command displays the connection status of users to be authenticated on a built-in Portal server.

Format

display portal local-server connect [**user-ip** *ip-address*]

Parameters

Parameter	Description	Value
user-ip *ip-address*	Displays the connection entry of a user with a specified IP address on a built-in Portal server. The connection entries of all users on the built-in Portal server are displayed if this parameter is not specified.	The value of *ip-address* is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal local-server connect** command to check the authentication mode and status of users to be authenticated on a built-in Portal server.

Example

Display the connection status of the user with the IP address 10.1.1.10 on a built-in Portal server.

```
<Huawei> display portal local-server connect user-ip 10.1.1.10
-----------------------------------------------------------------------------------------
 CID  IP Address   AuthMode  State    Session-timeout(hours)
-----------------------------------------------------------------------------------------
 1    10.1.1.10    CHAP      ONLINE   8
-----------------------------------------------------------------------------------------
```

Table 19-56 Description of the **display portal local-server connect** command output

Item	Description
CID	User table index.
IP Address	IP address of a user.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AuthMode	Authentication mode: • CHAP: The built-in Portal server uses CHAP to authenticate the user. • PAP: The built-in Portal server uses PAP to authenticate the user. To set the authentication method, run the **19.6.104 portal local-server authentication-method** command.
State	User status: • WAIT_CHALLENGE: waiting for the challenge • WAIT_AUTHACK: waiting for the authentication response • ONLINE: online • WAIT_LOGOUTACK: waiting for logout
Session-timeout(hours)	The session timeout interval. To set the session timeout interval, run the **19.6.117 portal local-server timer session-timeout**.

19.6.43 display portal local-server

Function

The **display portal local-server** command displays the configurations of a built-in Portal server.

Format

display portal local-server

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the built-in Portal authentication, run this command to view the configurations of a built-in Portal server.

Example

Display the configurations of a built-in Portal server.

```
<Huawei> display portal local-server
 Portal local-server config:
  server status                 : disable
  Heartbeat-check status        : auto
  Heartbeat-timeout value       : 60(s)
  server ip                     : 10.1.1.1
  authentication method         : chap
  protocol                      : -
  https ssl-policy              : -
  server port                   : 0
  session-timeout               : 8(h)
  syslog-limit                  : enable
  syslog-limit period           : 300(s)
  server pagename               : -
  server page-text              : -
  server policy-text            : -
  server background-image       : default-image0
  server background-color       : -
  server logo                   : -
  server ad-image               : -
```

Table 19-57 Description of the **display portal local-server** command output

Item	Description
server status	Status of a built-in Portal server. To enable the built-in Portal server function, run the **portal local-server** command. ● disable: Portal authentication is disabled. ● enable: Portal authentication is enabled.
Heartbeat-check status	Heartbeat detection status of the built-in Portal server. To set the heartbeat detection status, run the **19.6.109 portal local-server keep-alive** command. ● disable: indicates that the heartbeat detection function is disabled. ● enable: indicates the forcible detection mode. ● auto: indicates the automatic detection mode.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Heartbeat-timeout value	Heartbeat detection interval of the built-in Portal server. To set the heartbeat detection interval, run the **19.6.109 portal local-server keep-alive** command. This parameter is unavailable when the value of **Heartbeat-check status** is **disable**.
server ip	IP address of a built-in Portal server. To set the server IP address, run the **portal local-server ip** command.
authentication method	Authentication method used by a built-in Portal server for web users. To set the authentication method, run the **portal local-server authentication-method** command. ● chap: CHAP-based authentication (CHAP stands for Challenge Handshake Authentication Protocol.) ● pap: PAP-based authentication (PAP stands for Password Authentication Protocol.)
protocol	Protocol used for authentication information exchange between a built-in Portal server and users. To enable the built-in Portal server function, run the **portal local-server** command.
https ssl-policy	SSL policy used for authentication information exchange between a built-in Portal server and users. To enable the built-in Portal server function, run the **portal local-server** command.
server port	TCP port number used by HTTPS. To specify a TCP port number used by HTTPS, run the **portal local-server** command.
session-timeout	User session timeout interval configured on the built-in Portal server. To set the session timeout interval, run the **portal local-server timer session-timeout** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
syslog-limit	Status of the log suppression function for built-in Portal authentication users. To enable or disable the log suppression function, run the **19.6.115 portal local-server syslog-limit enable** command. • disable: indicates that the log suppression function is disabled for built-in Portal authentication users. • enable: indicates that the log suppression function is enabled for built-in Portal authentication users.
syslog-limit period	Log suppression duration for built-in Portal authentication users. To set the log suppression duration, run the **19.6.116 portal local-server syslog-limit period** command.
server pagename	Name of the page file package loaded to the built-in Portal server. To set the package name, run the **19.6.110 portal local-server load** command.
server page-text	Loaded use instruction page file of the built-in Portal server. To load a use instruction page file, run the **19.6.113 portal local-server page-text load** command.
server policy-text	Disclaimer page loaded to the built-in Portal server. To load a disclaimer page, run the **19.6.114 portal local-server policy-text load** command.
server background-image	Background image of the built-in Portal server login page. To set the background image, run the **19.6.106 portal local-server background-image load** command.
server background-color	Background color of the built-in Portal server login page. To set the background color, run the **19.6.105 portal local-server background-color** command.
server logo	Logo file of the built-in Portal server login page. To load a logo file, run the **19.6.111 portal local-server logo load** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
server ad-image	Advertisement image file of the built-in Portal server login page. To load an advertisement image file, run the **19.6.103 portal local-server ad-image load** command.

19.6.44 display portal local-server page-information

Function

The **display portal local-server page-information** command displays the page files loaded to the memory of a built-in Portal server.

Format

display portal local-server page-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display portal local-server page-information** command to check the page files loaded to the memory of a built-in Portal server.

Example

Display the page files loaded to the memory of a built-in Portal server.

```
<Huawei> display portal local-server page-information
-----------------------------------------------------------------------------
    Number of backup pages:35
    Size of backup pages:94438 byte
-----------------------------------------------------------------------------
    Name:/logout_success.html
    Size:4042 byte
    Last-Modified-Time:2011-12-16 20:24:46
-----------------------------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-58 Description of the **display portal local-server page-information** command output

Item	Description
Number of backup pages	Number of page files loaded.
Size of backup pages	Total size of the loaded page files.
Name	Name of a page file.
Size	Size of a page file.
Last-Modified-Time	Last modification time.

Related Topics

19.6.110 portal local-server load

19.6.45 display portal-access-profile configuration

Function

The **display portal-access-profile configuration** command displays the configuration of a Portal access profile.

Format

display portal-access-profile configuration [**name** *access-profile-name*]

Parameters

Parameter	Description	Value
name *access-profile-name*	Displays the configuration of a Portal access profile with a specified name. If **name** *access-profile-name* is not specified, the device displays all the Portal access profiles configured on the device. If **name** *access-profile-name* is specified, the device displays the configuration of a specified Portal access profile.	The value must be the name of an existing Portal access profile.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a Portal access profile, you can run this command to check whether the configuration is correct.

NOTE

The name of the compatibility profile converted after an upgrade begins with the at sign (@) and the profile is not counted in the configuration specification.

Example

Display all the Portal access profiles configured on the device.

```
<Huawei> display portal-access-profile configuration
-------------------------------------------------------------------------------
 ID            Portal-access-profile Name
-------------------------------------------------------------------------------
 0             portal_access_profile
 1             p1
 2             p2
-------------------------------------------------------------------------------
 Total: 3 printed: 3.
```

Table 19-59 Description of the **display portal-access-profile configuration** command output

Item	Description
ID	Portal access profile ID.
Portal-access-profile Name	Portal access profile name.

Display the configuration of the Portal access profile **p1**.

```
<Huawei> display portal-access-profile configuration name p1
  Profile name                      : p1
  Portal timer offline-detect length: 300
  User-group name                   : -
  Re-auth                           : Disable
  Network IP Num                    : 3
  Network IP List                   : 10.1.1.0 255.255.255.0
                                      10.10.1.0 255.255.255.0
                                      10.1.2.0 255.255.255.0
  Web-auth-server Name              : s1
  Layer                             : Layer two portal
  Local-server                      : Disable
  Bound authentication profile      : -
```

Table 19-60 Description of the **display portal-access-profile configuration name** command output

Item	Description
Profile name	Portal access profile name.
Portal timer offline-detect length	Offline detection interval for Portal authentication users. To configure the interval, run the **19.6.124 portal timer offline-detect** command.
User-group name	Name of the user group based on which the device assigns network access rights to users when the Portal server is Down. To configure the user group name, run the **19.6.12 authentication event portal-server-down action authorize** command.
Re-auth	Whether the device is enabled to re-authenticate users when the Portal server changes from Down to Up. To configure the function, run the **19.6.13 authentication event portal-server-up action re-authen** command.
Network IP Num	Number of source IP address segments for Portal authentication. To configure the number, run the **19.6.99 portal auth-network** command.
Network IP List	Source IP address segment for Portal authentication. To configure the source IP address segment, run the **19.6.99 portal auth-network** command.
Web-auth-server Name	Portal server profile bound to the Portal access profile. To configure the Portal server profile, run the **19.6.155 web-auth-server (Portal access profile view)** command.
Layer	Portal authentication mode. To configure the Portal authentication mode, run the **19.6.155 web-auth-server (Portal access profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Local-server	Whether the built-in Portal server function is enabled. To configure the built-in Portal server function, run the **19.6.107 portal local-server enable** command.
Bound authentication profile	Authentication profile to which the portal access profile is bound. To configure the authentication profile, run the **19.6.129 portal-access-profile (authentication profile view)** command.

19.6.46 display portal quiet-user

Function

The **display portal quiet-user** command displays information about Portal authentication users in quiet state.

Format

display portal quiet-user { **all** | **user-ip** *ip-address* | **server-ip** *ip-address* }

Parameters

Parameter	Description	Value
all	Displays information about all Portal authentication users in quiet state.	-
user-ip *ip-address*	Displays information about the quiet user with the specified IP address.	The value is in dotted decimal notation.
server-ip *ip-address*	Displays information about all the users in quiet state authenticated by the Portal authentication server with a specified IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After the quiet timer is enabled, you can run the **display portal quiet-user** command to view information about Portal authentication users in quiet state.

Example

Display information about all Portal authentication users in quiet state.

```
<Huawei> display portal quiet-user all
Quiet IP information
-----------------------------------------------------------------------------------
Quiet ip                                        Quiet Remain Time(Sec)
-----------------------------------------------------------------------------------
192.168.1.1                                        10
192.168.1.2                                        20
-----------------------------------------------------------------------------------
2 quiet IP found, 2 printed.
```

Display information about all the users in quiet state authenticated by the Portal authentication server with IP address 192.168.2.1.

```
<Huawei> display portal quiet-user server-ip 192.168.2.1
Quiet IP information
-----------------------------------------------------------------------------------
Quiet ip                                        Quiet Remain Time(Sec)
-----------------------------------------------------------------------------------
192.168.1.3                                        10
192.168.1.4                                        20
-----------------------------------------------------------------------------------
2 quiet IP found, 2 printed.
```

Display information about the user in quiet state at 192.168.1.1.

```
<Huawei> display portal quiet-user user-ip 192.168.1.1
 Quiet remain second     100
```

Table 19-61 Description of the **display portal quiet-user** command output

Item	Description
Quiet IP information	Information about the user in quiet state.
Quiet ip	IP address of the user in quiet state.
Quiet Remain Time(Sec)	Remaining quiet time of the user in quiet state, in seconds.
Quiet remain second	Remaining quiet period of the user in quiet state.

19.6.47 display portal url-encode configuration

Function

The **display portal url-encode configuration** command displays the configuration of URL encoding and decoding.

Format

display portal url-encode configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring URL encoding and decoding, you can run the **display portal url-encode configuration** command to check the configuration.

Example

Display the configuration of URL encoding and decoding.

```
<Huawei> display portal url-encode configuration
  Portal URL Encode : Disable
```

Table 19-62 Description of the **display portal url-encode configuration** command output

Item	Description
Portal URL Encode	Whether URL encoding and decoding are enabled: ● Disable ● Enable To configure the function, run the **19.6.128 portal url-encode enable** command.

Related Topics

19.6.128 portal url-encode enable

19.6.48 display portal user-logout

Function

The **display portal user-logout** command displays temporary logout entries of Portal authentication users.

Format

display portal user-logout [**ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*]]

Parameters

Parameter	Description	Value
ip-address *ip-address*	Displays temporary logout entries of the Portal authentication user with a specified IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Displays temporary logout entries of the Portal authentication user with a specified VPN instance.	The value must be an existing VPN instance name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a Portal authentication user goes offline, the device sends an offline request packet to the Portal server. If the device does not receive an ACK packet from the Portal server, it records a temporary logout entry of the user. You can run the **display portal user-logout** command to check temporary logout entries of Portal authentication users.

If the parameter **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] is not specified, the temporary logout entries of all Portal authentication users are displayed.

Example

Display the temporary logout entries of all Portal authentication users.

```
<Huawei> display portal user-logout
-----------------------------------------------------------------
UserIP          Vrf     Resend Times TableID
-----------------------------------------------------------------
192.168.111.100  1        3            0
-----------------------------------------------------------------
Total: 1, printed: 1
```

Table 19-63 Description of the **display portal user-logout** command output

Item	Description
UserIP	IP address of the Portal authentication user.
Vrf	VPN instance that the Portal authentication user belongs to.
Resend Times	Number of logout packet re-transmission times. To set the number of logout packet re-transmission times, run the **19.6.119 portal logout resend timeout** command.
TableID	Index of the temporary logout entry.
Total: *m*, printed: *n*	Total number of temporary logout entries and number of displayed entries.

19.6.49 display server-detect state

Function

The **display server-detect state** command displays the status of a Portal server.

Format

display server-detect state [**web-auth-server** *server-name*]

Parameters

Parameter	Description	Value
web-auth-server *server-name*	Displays information about the Portal server status configured in the specified Portal server profile. If this parameter is not specified, status of all Portal servers is displayed.	The Portal server profile name must exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When an external Portal server is used for Portal authentication, you can run the **display server-detect state** command to check information about the Portal server status.

Example

Display information about the Portal server status configured in the Portal server profile **abc**.

```
<Huawei> display server-detect state web-auth-server abc
  Web-auth-server     :    abc
  Total-servers       :    4
  Live-servers        :    1
  Critical-num        :    0
  Status              :    Normal
  Ip-address               Status
  192.168.2.1               UP
  192.168.2.2               DOWN
  192.168.2.3               DOWN
  192.168.2.4               DOWN
```

Table 19-64 Description of the **display server-detect state** command output

Item	Description
Web-auth-server	Name of the Portal server profile.
Total-servers	Number of Portal servers configured.
Live-servers	Number of Portal servers in Up state.
Critical-num	Minimum number of Portal servers in Up state. If the number of Portal servers is less than this value, enable the survival function in the corresponding Portal server profile view.
Status	Status of the Portal server. The values are as follows: ● Normal: indicates that the Portal server is in normal state. When *Total-servers* in the command output is larger than *Critical-num*, *Status* is displayed as **Normal**. If the **server-ip** *server-ip-address* &<1-10> command is not run in the Portal server template view to configure an IP address for the Portal server, *Status* is displayed as **Normal**. ● Abnormal: indicates that the Portal server is in abnormal state. When *Total-servers* in the command output is less than or equal to *Critical-num*, *Status* is displayed as **Abnormal**.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ip-address	IP address of the Portal server.
Status	Whether the Portal server with the specified IP address is reachable. The values are as follows: • UP: reachable • DOWN: unreachable

Related Topics

19.6.136 server-ip (Portal server profile view)
19.6.135 server-detect

19.6.50 display url-template

Function

The **display url-template** command displays information about URL templates.

Format

display url-template { **all** | **name** *template-name* }

Parameters

Parameter	Description	Value
all	Displays information about all configured URL templates.	-
name *template-name*	Displays information about the URL template with a specified name.	The value must be the name of an existing URL template.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After a URL template is configured, run the **display url-template** command to view information about the URL template.

Example

Display information about all configured URL templates.

```
<Huawei> display url-template all

--------------------------------------------------------------------------------
 Name                        URL     Start  Assignment  Isolate
                           Number  Mark   Mark        Mark
--------------------------------------------------------------------------------
 huawei                       0      ?      =           &
 huawei2                      0      ?      =           &
 huawei3                      0      ?      =           &
--------------------------------------------------------------------------------
 Total 3
```

Display information about the URL template **huawei**.

```
<Huawei> display url-template name huawei
 Name : huawei
 URL  :
 Start mark      : ?
 Assignment mark : =
 Isolate mark    : &
 AC IP           :
 AC MAC          :
 AP IP           :
 AP MAC          :
 SSID            :
 User MAC        :
 Redirect URL    :
 User IP address :
 Sysname         :
 User VLAN       :
 Delimiter       :
 Format          :
 Ac-ip Value     : 10.1.1.1
 Ap-ip Value     : Vlanif10
 ESN             :
```

Table 19-65 Description of the **display url-template** command output

Item	Description
Name	Name of a URL template.
URL Number	Number of URLs.
URL	URL of the Portal server. To configure this parameter, run the **19.6.142 url (URL template view)** command.
Start mark/Start Mark	Start character in the URL. To configure this parameter, run the **19.6.97 parameter** command.
Assignment mark/Assignment Mark	Assignment character in the URL. To configure this parameter, run the **19.6.97 parameter** command.
Isolate mark/Isolate Mark	Delimiter between URLs. To configure this parameter, run the **19.6.97 parameter** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
AC IP	Name of **ac-ip** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
AC MAC	Name of **ac-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
AP IP	Name of **ap-ip** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
AP MAC	Name of **ap-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
SSID	Name of **ssid** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
User MAC	Name of **user-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
Redirect URL	Name of **redirect-url** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
User IP address	Name of **user-mac** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
Sysname	Name of **sysname** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
User VLAN	Name of **user-vlan** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.
Delimiter	Delimiter between MAC addresses in the URL. To configure this parameter, run the **19.6.144 url-parameter mac-address format** command.
Format	Format of MAC addresses in the URL. To configure this parameter, run the **19.6.144 url-parameter mac-address format** command.
ESN	Name of **esn** in the URL. To configure this parameter, run the **19.6.145 url-parameter** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ac-ip Value	Value of the redirection parameter **ac-ip**. To configure this parameter, run the **19.6.146 url-parameter set** command.
Ap-ip Value	Value of the redirection parameter **ap-ip**. To configure this parameter, run the **19.6.146 url-parameter set** command.

19.6.51 display user-group

Function

The **display user-group** command displays the configuration of a user group.

Format

display user-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the configuration of a user group with a specified name. If this parameter is not specified, the configurations of all user groups are displayed.	The value must be the name of an existing user group.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring a user group, you can run this command to check whether the configuration is correct.

Example

Display the configurations of all user groups.

```
<Huawei> display user-group
 ------------------------------------------------------------------------------
 ID    Group name                    User-num
```

```
--------------------------------------------------------------------------------
0     g1                                0
--------------------------------------------------------------------------------
Total 1
```

NOTE

When the length of **Group name** exceeds 14 characters, the name is displayed in abridged mode.

Display the configuration of the user group **g1**.

```
<Huawei> display user-group g1
  User group ID           : 0
  Group name              : g1
  ACL ID                  :
  ACL rule number         : 0
  User-num                : 0
  VLAN                    :
  Remark dscp             :
  Remark 8021p            :
  Remark exp              :
  Remark lp               :
  IsolateInter            : No
  IsolateInner            : No
```

Table 19-66 Description of the **display user-group** command output

Item	Description
ID/User group ID	User group ID.
Group name	User group name.
ACL ID	ID of the IPv4 ACL bound to the user group. To configure the ACL ID, run the **19.6.5 acl-id (user group view)** command.
ACL rule number	Number of ACL rules.
User-num	Number of online users bound to the user group.
VLAN	VLAN bound to the user group. To configure the VLAN, run the **19.6.152 user-vlan** command.
Remark dscp	Priorities for processing IP packets. To set the priorities, run the **19.6.132 remark** command.
Remark 8021p	Priorities for processing Ethernet Layer 2 packets. To set the priorities, run the **19.6.132 remark** command.

Item	Description
Remark exp	Processing priority of MPLS packets. To set the priorities, run the **19.6.132 remark** command.
Remark lp	Processing priority of internal packets. To set the priorities, run the **19.6.132 remark** command.
IsolateInter	Inter-group user isolation.
IsolateInner	Intra-group user isolation.

19.6.52 display web-auth-server configuration

Function

The **display web-auth-server configuration** command displays the Portal server configuration.

Format

display web-auth-server configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the Portal server template is configured, the **display web-auth-server configuration** displays the Portal server configuration.

Example

Display the Portal server configuration.

```
<Huawei> display web-auth-server configuration
  Listening port        : 2000
  Portal                : version 1, version 2
  Include reply message : enabled

-----------------------------------------------------------------------------
```

```
Web-auth-server Name : huawei
IP-address           :
Shared-key           :
Source-IP            : -
Port / PortFlag      : 50100 / NO
URL                  : https://192.168.2.10:8443/webauth
URL Template         :
Redirection          : Enable
Sync                 : Disable
Sync Seconds         : 300
Sync Max-times       : 3
Detect               : Disable
Detect Seconds       : 60
Detect Max-times     : 3
Detect Critical-num  : 0
Detect Action        :
VPN Instance         :
Bound Portal profile :

Protocol             : portal


------------------------------------------------------------------------------
1 Web authentication server(s) in total
```

Table 19-67 Description of the **display web-auth-server configuration** command output

Item	Description
Listening port	Listening port for Portal protocol packets. To configure a listening port, run the **19.6.154 web-auth-server listening-port** command.
Portal	Portal protocol version. ● version 1, version 2: The device supports both the versions V1.0 and V2.0. ● version 2: The device supports the versions V2.0. To configure the Portal protocol version, run the **19.6.158 web-auth-server version** command.
Include reply message	Whether the packets sent from the device to the Portal server contain authentication responses. ● enabled ● disabled To enable the device to transparently transmit authentication responses of users sent by the authentication server to the Portal server, run the **19.6.156 web-auth-server reply-message** command.

Item	Description
Web-auth-server Name	Name of the Portal server template. To configure the Portal server template name, run the **19.6.157 web-auth-server (system view)** command.
IP-address	IP address of the Portal server. To configure the IP address of the Portal server, run the **19.6.136 server-ip (Portal server profile view)** command.
Shared-key	Shared key of the Portal server. To configure the shared key of the Portal server, run the **19.6.137 shared-key (Portal server profile view)** command.
Source-IP	IP address used for communication with the Portal server. To configure the IP address used for communication with the Portal server, run the **19.6.139 source-ip (Portal server profile view)** command.
Port / PortFlag	• Port: indicates the port number of the Portal server. • PortFlag: indicates whether packets are always sent through this port. To configure the port number of the Portal server, run the **19.6.98 port (Portal server profile view)** command.
URL	URL of the Portal server. To configure the URL of the Portal server, run the **19.6.143 url (Portal server profile view)** command.
URL Template	URL template bound to the Portal server template. To configure the URL template, run the **19.6.148 url-template (Portal server profile view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Redirection	Redirection status of Portal authentication. ● Disable: Redirection of Portal authentication is disabled. ● Enable: Redirection of Portal authentication is enabled. To configure redirection of Portal authentication, run the **19.6.159 web-redirection disable (Portal server profile view)** command.
Sync	User information synchronization. To enable user information synchronization, run the **19.6.149 user-sync** command.
Sync Seconds	User information synchronization interval. To set the user information synchronization interval, run the **19.6.149 user-sync** command.
Sync Max-times	Maximum number of times that user information synchronization fails. To set the maximum number of times that user information synchronization fails, run the **19.6.149 user-sync** command.
Detect	Portal server detection function. To configure Portal server detection function, run the **19.6.135 server-detect** command.
Detect Seconds	Detection interval of the Portal server. To set the detection interval of the Portal server, run the **19.6.135 server-detect** command.
Detect Max-times	Maximum number of detection failures. To set the maximum number of detection failures, run the **19.6.135 server-detect** command.
Detect Critical-num	Minimum number of Portal servers in Up state. To configure this function, run the **19.6.135 server-detect** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Detect Action	Action taken after the number of detection failures exceeds the maximum. ● log: The device sends logs after the number of detection failures exceeds the maximum. ● trap: The device sends traps after the number of detection failures exceeds the maximum. To configure an action taken after the number of detection failures exceeds the maximum, run the **19.6.135 server-detect** command.
VPN Instance	VPN instance used in Portal authentication. To configure the VPN instance, run the **19.6.153 vpn-instance (Portal server template view)** command.
Bound Portal profile	Portal access profile to which the Portal server template is bound. To configure the Portal access profile, run the **19.6.155 web-auth-server (Portal access profile view)** command.
Protocol	Protocol used in Portal authentication. ● Portal ● haca To configure the protocol, run the **19.6.127 protocol** command.

19.6.53 display snmp-agent trap feature-name mid_eapol all

Function

The **display snmp-agent trap feature-name mid_eapol all** command displays the status of all traps on the DOT1X module.

Format

display snmp-agent trap feature-name mid_eapol all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the DOT1X module, you can run this command to check the status of all traps on the DOT1X module. To enable the trap function for the DOT1X module, run the **snmp-agent trap enable feature-name mid_eapol** command.

Prerequisites

The SNMP function has been enabled on the device. For details, see **snmp-agent**.

Example

Display the status of all traps on the DOT1X module.

```
<Huawei> display snmp-agent trap feature-name mid_eapol all
-----------------------------------------------------------------------------
Feature name: MID_EAPOL
Trap number : 2
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwSrvcfgEapMaxUserAlarm        on                        on
hwMacAuthenMaxUserAlarm        on                        on
```

Table 19-68 Description of the **display snmp-agent trap feature-name mid_eapol all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Name of a trap. Traps on the DOT1X module include: • hwSrvcfgEapMaxUserAlarm: The device sends a Huawei proprietary trap when the number of 802.1X authentication users reaches the maximum number allowed on an interface. • hwMacAuthenMaxUserAlarm: The device sends a Huawei proprietary trap when the number of MAC address authentication users reaches the maximum number allowed on an interface.
Default switch status	Default status of the trap function: • on: The trap function is enabled by default. • off: The trap function is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Trap status: • on: The trap is enabled. • off: The trap is disabled.

Related Topics

19.6.140 snmp-agent trap enable feature-name mid_eapol

19.6.54 display snmp-agent trap feature-name mid_web all

Function

The **display snmp-agent trap feature-name mid_web all** command displays the status of all traps on the web authentication module.

Format

display snmp-agent trap feature-name mid_web all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After enabling the trap function for the web authentication module, you can run this command to check the status of all traps on the web authentication module. To enable the trap function for the web authentication module, run the **snmp-agent trap enable feature-name mid_web** command.

Prerequisites

The SNMP function has been enabled on the device. For details, see **snmp-agent**.

Example

Display the status of all traps on the web authentication module.

```
<Huawei> display snmp-agent trap feature-name mid_web all
-----------------------------------------------------------------------------
Feature name: MID_WEB
```

```
Trap number : 4
--------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwPortalServerUp               on                      on
hwPortalServerDown             on                      on
hwPortalMaxUserAlarm           on                      on
hwPortalUserClearAlarm         on                      on
```

Table 19-69 Description of the **display snmp-agent trap feature-name mid_web all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Name of a trap. Traps on the web authentication module include: ● hwPortalServerUp: The device sends a Huawei proprietary trap when it detects that the Portal server changes from Down to Up. ● hwPortalServerDown: The device sends a Huawei proprietary trap when it detects that the Portal server changes from Up to Down. ● hwPortalMaxUserAlarm: The device sends a Huawei proprietary trap when the number of online Portal authentication users exceeds the upper threshold. ● hwPortalUserClearAlarm: The device sends a Huawei proprietary trap when the number of online Portal authentication users falls below the lower threshold.
Default switch status	Default status of the trap function: ● on: The trap function is enabled by default. ● off: The trap function is disabled by default.
Current switch status	Trap status: ● on: The trap is enabled. ● off: The trap is disabled.

Related Topics

19.6.141 snmp-agent trap enable feature-name mid_web

19.6.55 dot1x authentication-method

Function

The **dot1x authentication-method** command configures an 802.1X authentication mode.

The **undo dot1x authentication-method** command restores the default configuration.

The default 802.1X authentication mode is **eap**, which indicates Extensible Authentication Protocol (EAP) relay authentication.

Format

dot1x authentication-method { **chap** | **pap** | **eap** }

undo dot1x authentication-method

Parameters

Parameter	Description	Value
chap	Specifies EAP termination authentication using the Challenge Handshake Authentication Protocol (CHAP).	-
pap	Specifies EAP termination authentication using the Password Authentication Protocol (PAP).	-
eap	Specifies Extensible Authentication Protocol (EAP) relay authentication.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, users exchange authentication information with the device using EAP packets. The device uses two modes to exchange authentication information with the RADIUS server.

- EAP termination: The device directly parses EAP packets, encapsulates user authentication information into a RADIUS packet, and sends the packet to the RADIUS server for authentication. EAP termination is classified into PAP or CHAP authentication.

  - PAP: The device arranges the MAC address, shared key, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the User-Password attribute.
  - CHAP: The device arranges the CHAP ID, MAC address, and random value in sequence, performs hash processing on them using the MD5 algorithm, and encapsulates the hash result into the CHAP-Password and CHAP-Challenge attributes.
- EAP relay (specified by **eap**): The device encapsulates EAP packets into RADIUS packets and sends the RADIUS packets to the RADIUS server. The device does not parse the received EAP packets but encapsulates them into RADIUS packets. This mechanism is called EAP over Radius (EAPoR).

The processing capability of the RADIUS server determines whether EAP termination or EAP relay is used. If the RADIUS server has a higher processing capability and can parse a large number of EAP packets before authentication, the EAP relay mode is recommended. If the RADIUS server has a processing capability not good enough to parse a large number of EAP packets and complete authentication, the EAP termination mode is recommended and the device parses EAP packets for the RADIUS server. When the authentication packet processing method is configured, ensure that the client and server both support this method; otherwise, the users cannot pass authentication.

NOTE

- The EAP relay can be configured for 802.1X users only when RADIUS authentication is used.
- If AAA local authentication is used, the authentication mode for 802.1X users can only be set to EAP termination.
- Because mobile phones do not support EAP termination mode (PAP and CHAP), the 802.1X authentication + local authentication mode cannot be configured for mobile phones. Terminals such as laptop computers support EAP termination mode only after having third-party clients installed.
- If the 802.1X client uses the MD5 encryption mode, the user authentication mode on the device can be set to EAP or CHAP; if the 802.1X client uses the PEAP authentication mode, the authentication mode on the device can be set to EAP.
- In a wireless access scenario, if WPA or WPA2 authentication mode is configured in the security policy profile, 802.1X authentication does not support pre-authentication domain-based authorization.
- If an interface has online 802.1X users and the authentication mode is changed between EAP termination and EAP relay in the 802.1X access profile bound to the interface, the online 802.1X users will be logged out. If the authentication mode is changed between CHAP and PAP in EAP termination mode, the online 802.1X users will not be logged out.

Example

In the 802.1X access profile **d1**, configure the device to use PAP authentication for 802.1X users.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x authentication-method pap
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.56 dot1x eap-notify-packet

Function

The **dot1x eap-notify-packet** command configures the device to send EAP packets with a code number to 802.1X users.

The **undo dot1x eap-notify-packet** command restores the default configuration.

By default, the device does not send EAP packets with a code number to users.

Format

dot1x eap-notify-packet eap-code *code-number* **data-type** *type-number*

undo dot1x eap-notify-packet [**eap-code** *code-number* **data-type** *type-number*]

Parameters

Parameter	Description	Value
eap-code *code-number*	Specifies the code number in EAP packets sent by the device.	The value is an integer that ranges from 5 to 255, the default value is 255.
data-type *type-number*	Specifies the data type in EAP packets sent by the device.	The value is an integer that ranges from 1 to 255, the default value is 255.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a non-Huawei device used as the RADIUS server sends RADIUS packets with attribute 61, EAP packet code number 0xa (hexadecimal notation, 10 in decimal notation), and data type being 0x19 (hexadecimal notation, 25 in decimal notation) to the device, run the **dot1x eap-notify-packet** command on the device so that the device can send EAP packets with code number 0xa and data type 0x19 to users. If the **dot1x eap-notify-packet** command is not executed, the device does not process EAP packets of this type and users are disconnected.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The device can only send EAP packets with code number 10 and data type 25.

Example

In the 802.1X access profile **d1**, configure the device to send EAP packets with code number 10 and data type 25 to users.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x eap-notify-packet eap-code 10 data-type 25
```

19.6.57 dot1x handshake

Function

The **dot1x handshake** command enables the device to send handshake packets to online 802.1X users.

The **undo dot1x handshake** command disables the device from sending handshake packets to online 802.1X users.

By default, the device handshake function is disabled for online 802.1X users.

Format

dot1x handshake

undo dot1x handshake

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To check whether an 802.1X user is online in real time, run the **19.6.6 authentication handshake** command to enable the device to send handshake packets to the 802.1X user. If some clients support handshake with online 802.1X users, run the **dot1x handshake** command to enable handshake with online 802.1X users. Then the device sends EAP handshake request packets to the user. If the user sends a response packet within the handshake interval (configured using the **19.6.65 dot1x timer** command), the device considers that the user is online. If the user does not send any response packet within the interval, the device considers that the user is offline.

Precautions

Currently, most clients do not support this function, for example, the Windows built-in client, AnyConnect client, and iOS built-in client. If a client does not support the handshake function, the device will not receive handshake response packets within the handshake interval and considers that the user is offline. Therefore, you need to disable the device from sending handshake packets to an online 802.1X user when the user's client does not support the handshake function.

After the **dot1x handshake** command is run, the **19.6.6 authentication handshake** command does not take effect.

This function takes effect only for the wired users.

Example

In the 802.1X access profile **d1**, enable the device to send handshake packets to online 802.1X users.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x handshake
```

19.6.58 dot1x mc-trigger

Function

The **dot1x mc-trigger** command enables multicast-triggered 802.1X authentication.

The **undo dot1x mc-trigger** command disables multicast-triggered 802.1X authentication.

By default, multicast-triggered 802.1X authentication is enabled.

Format

dot1x mc-trigger

undo dot1x mc-trigger

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a client (for example, the built-in 802.1X client of the Windows operating system) cannot send an EAPOL-Start packet to perform 802.1X authentication, you

can enable multicast-triggered 802.1X authentication. After that, the device multicasts an EAP-Request/Identity packet to the client to trigger authentication.

Example

Enable multicast-triggered 802.1X authentication.

```
<Huawei> system-view
[Huawei] dot1x mc-trigger
```

19.6.59 dot1x mc-trigger port-up-send enable

Function

The **dot1x mc-trigger port-up-send enable** command enables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

The **undo dot1x mc-trigger port-up-send enable** command disables the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

By default, the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up is disabled.

Format

dot1x mc-trigger port-up-send enable

undo dot1x mc-trigger port-up-send enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an 802.1X authentication scenario, if the device interface connecting to a client changes from Down to Up, the client needs to send EAPOL-Start packets again for 802.1X authentication, which takes a long time. You can run the **dot1x mc-trigger port-up-send enable** command on the device to enable the device interface to multicast EAP-Request/Identity packets to the client to trigger 802.1X authentication through EAPOL-Start packets sent by the client immediately after the interface goes Up. This configuration shortens the re-authentication time.

Prerequisites

The function of triggering 802.1X authentication through multicast packets has been enabled using the **dot1x mc-trigger** command.

Example

Enable the function of triggering 802.1X authentication through multicast packets immediately after an interface goes Up.

```
<Huawei> system-view
[Huawei] dot1x mc-trigger
[Huawei] dot1x mc-trigger port-up-send enable
```

19.6.60 dot1x quiet-period

Function

The **dot1x quiet-period** command enables the quiet function for 802.1X authentication users.

The **undo dot1x quiet-period** command disables the quiet function for 802.1X authentication users.

By default, the quiet function is enabled for 802.1X authentication users.

Format

dot1x quiet-period

undo dot1x quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function is enabled, if the number of authentication failures of an 802.1X user exceeds a specified value (set using the **19.6.61 dot1x quiet-times** command) within 60 seconds, the user enters a quiet period. During the quiet period, the device discards the 802.1X authentication request packets from the user. This prevents the impact on the system due to frequent user authentication.

The value of the quiet timer is set using the **19.6.66 dot1x timer quiet-period** command. When the quiet timer expires, the device re-authenticates the user.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the quiet timer.

```
<Huawei> system-view
[Huawei] dot1x quiet-period
```

19.6.61 dot1x quiet-times

Function

The **dot1x quiet-times** command sets the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state.

The **undo dot1x quiet-times** command restores the default setting.

By default, an 802.1X user enters the quiet state after 10 authentication failures within 60 seconds.

Format

dot1x quiet-times *fail-times*

undo dot1x quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before the 802.1X user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the quiet timer function of the device is enabled using the **19.6.60 dot1x quiet-period** command, if the number of authentication failures of an 802.1X user exceeds the value that is set using the **dot1x quiet-times** command within 60 seconds, the user enters the quiet state. This prevents the impact on the system due to frequent user authentication.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the maximum number of authentication failures within 60 seconds before an 802.1X user enters the quiet state to 4.

```
<Huawei> system-view
[Huawei] dot1x quiet-times 4
```

19.6.62 dot1x reauthenticate mac-address

Function

The **dot1x reauthenticate mac-address** command enables re-authentication for an online 802.1X user with the specified MAC address.

By default, re-authentication is disabled for an online 802.1X user with the specified MAC address.

Format

dot1x reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies the MAC address of an 802.1X user to be re-authenticated.	The value is a unicast MAC address in H-H-H format, where H can be one to four hexadecimal digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **dot1x reauthenticate**.

The **dot1x reauthenticate mac-address** and **dot1x reauthenticate** commands re-authenticate online 802.1X users and their difference is as follows:

- The **dot1x reauthenticate mac-address** command configures the device to re-authenticate a specified user for once.
- The **dot1x reauthenticate** command configures the device to re-authenticate all users at intervals.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable re-authentication for an 802.1X user with the MAC address of 00e0-fc01-0005.

```
<Huawei> system-view
[Huawei] dot1x reauthenticate mac-address 00e0-fc01-0005
```

19.6.63 dot1x reauthenticate

Function

The **dot1x reauthenticate** command configures re-authentication for online 802.1X authentication users.

The **undo dot1x reauthenticate** command restores the default configuration.

By default, re-authentication is not configured for online 802.1X authentication users.

Format

dot1x reauthenticate

undo dot1x reauthenticate

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After modifying the authentication parameters of a user on the authentication server, the administrator must re-authenticate the user in real time to ensure user validity if the user has been online.

After the user goes online, the device saves authentication parameters of the user. After re-authentication is configured for online 802.1X authentication users using the **dot1x reauthenticate** command in the 802.1X access profile, the device automatically sends the user authentication parameters in the 802.1X access profile to the authentication server at an interval (specified using the **19.6.65 dot1x timer reauthenticate-period** *reauthenticate-period-value* command) for re-authentication. If the user authentication information on the authentication server remains unchanged, the users are kept online. If the information has been changed, the users are disconnected and need to be re-authenticated based on the changed authentication parameters.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After re-authentication is configured for online 802.1X authentication users, a large number of 802.1X authentication logs are generated.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

In the 802.1X access profile **d1**, configure re-authentication for online 802.1X authentication users.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x reauthenticate
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.64 dot1x retry

Function

The **dot1x retry** command configures the number of times an authentication request or handshake packet is retransmitted to an 802.1X user.

The **undo dot1x retry** command restores the default configuration.

By default, the device can retransmit an authentication request or handshake packet to an 802.1X user twice.

Format

dot1x retry *max-retry-value*

undo dot1x retry

Parameters

Parameter	Description	Value
max-retry-value	Specifies the number of times an authentication request or handshake packet is retransmitted to an 802.1X user.	The value is an integer that ranges from 1 to 10.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device does not receive any response from a user within a specified time after sending an authentication request or handshake packet to the user, the device sends the authentication request or handshake packet again. If the authentication request or handshake packet has been sent for the maximum retransmission times and no response is received, the user authentication or handshake fails. In this process, the total number of authentication requests or handshake packets sent by the device is *max-retry-value* plus 1.

Precautions

Repeated authentication requests occupy a lot of system resources. When using the **dot1x retry** command, you can set the maximum number of times according to user requirements and device resources. The default value is recommended.

The following table lists the intervals at which the device retransmits different types of packets and related commands.

Packet Type	Interval for Retransmitting Packets	Command
EAP-Request/Identity packet (MAC address bypass authentication is disabled)	*tx-period-value*	**19.6.69 dot1x timer tx-period** *tx-period-value*
EAP-Request/Identity packet (MAC address bypass authentication is enabled)	Integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)	**19.6.68 dot1x timer mac-bypass-delay** *delay-time-value*
EAP-Request/MD5 Challenge packet	*client-timeout-value*	**19.6.65 dot1x timer client-timeout** *client-timeout-value*
Handshake packet	*handshake-period-value*	**19.6.65 dot1x timer handshake-period** *handshake-period-value*

Example

In the 802.1X access profile **d1**, configure the number of times an authentication request or handshake packet can be retransmitted to 802.1X users to 4.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x retry 4
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.65 dot1x timer

Function

The **dot1x timer** command configures the parameters of each 802.1X timer.

The **undo dot1x timer** command restores the default settings.

For the default parameter settings of each 802.1X timer, see the parameter description.

Format

dot1x timer { **client-timeout** *client-timeout-value* | **reauthenticate-period** *reauthenticate-period-value* | **handshake-period** *handshake-period-value* }

undo dot1x timer { **client-timeout** | **reauthenticate-period** | **handshake-period** }

Parameters

Parameter	Description	Value
client-timeout *client-timeout-value*	Specifies the client authentication timeout interval. **NOTE** On the network, some terminals may delay in responding to EAP-Request/MD5 Challenge packets sent from the device. If the delay is long, you can increase client-timeout client-timeout-value so that these terminals can go online. The adjustment rule is as follows:3 x client-timeout client-timeout-value > Terminal response delay.	The value is an integer that ranges from 1 to 120, in seconds. By default, the client authentication timeout interval is 5 seconds.
reauthenticate-period *reauthenticate-period-value*	Specifies the periodic re-authentication period for online 802.1X users.	The value is an integer that ranges from 60 to 7200, in seconds. By default, the periodic re-authentication period is 3600 seconds for online 802.1X users.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
handshake-period *handshake-period-value*	Specifies the interval at which the device handshakes with an 802.1X client on a non-Eth-Trunk interface. For details, see **19.6.57 dot1x handshake**.	The value is an integer that ranges from 5 to 7200, in seconds. By default, the interval for sending handshake packets is 15s.

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

During 802.1X authentication, multiple timers are started to implement proper and orderly interactions between access users, access devices, and the authentication server. You can change the values of timers by running the **dot1x timer** command to adjust the interaction process. (The values of some timers cannot be changed.) This command is necessary in special network environments. It is recommended that you retain the default settings of the timers.

This command only sets the values of the timers. To enable the timers, perform corresponding configurations or use default settings.

- The client authentication timeout timer and the interval for sending authentication requests are enabled by default. You can run the **19.6.64 dot1x retry** command to configure the number of retransmissions of authentication request packets when the client authentication times out.
- The re-authentication timer for online 802.1X users is disabled by default. To enable this timer, run the **19.6.63 dot1x reauthenticate** command.
- The online 802.1X user handshake function is disabled by default. You can run the **19.6.57 dot1x handshake** command to enable the online 802.1X user handshake function. The handshake function takes effect only for the wired users.

NOTE

It is recommended that the re-authentication interval be set to the default value. If multiple ACLs need to be delivered during user authorization, you are advised to disable the re-authentication function or set a longer re-authentication interval to improve the device's processing performance.

In remote authentication and authorization, if the re-authentication interval is set to a shorter time, the CPU usage may be higher.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the 802.1X access profile **d1**, set the client authentication timeout interval to 90 seconds.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x timer client-timeout 90
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.66 dot1x timer quiet-period

Function

The **dot1x timer quiet-period** command configures the quiet period for 802.1X users who fail to be authenticated.

The **undo dot1x timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for 802.1X users who fail to be authenticated.

Format

dot1x timer quiet-period *quiet-period-times*

undo dot1x timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-times	Sets the quiet period for 802.1X users who fail to be authenticated.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If an 802.1X authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled using the **19.6.60 dot1x quiet-period** command, if the number of times that an 802.1X user fails to be authenticated

within 60s exceeds the upper limit (configured using the **19.6.61 dot1x quiet-times** command), the device discards the user's 802.1X authentication request packets for a period to avoid frequent authentication failures.

Example

Set the quiet period to 100 seconds for 802.1X users who fail to be authenticated.

```
<Huawei> system-view
[Huawei] dot1x timer quiet-period 100
```

19.6.67 dot1x trigger dhcp-binding

Function

The **dot1x trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-connection phase.

The **undo dot1x trigger dhcp-binding** command restores the default setting.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

Format

dot1x trigger dhcp-binding

undo dot1x trigger dhcp-binding

Parameters

None

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through 802.1X authentication, the unauthorized users can obtain the same identities as the authorized users and connect to the network without authentication. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting

 Copyright © Huawei Technologies Co., Ltd.

normal communication between authorized users. To prevent the previous attacks, configure IPSG and DAI. These two functions are implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After the static IP users who pass 802.1X authentication or are at the pre-authentication phase send EAP packets to trigger generation of the user information table, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface recorded in the table.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass 802.1X authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.
- In the interface view, run the **arp anti-attack check user-bind enable** command to enable DAI.

For detailed configurations of IPSG and DAI, see **IPSG Configuration** and **ARP Security Configuration** in the *Huawei AR Series V200R010 Configuration Guide - Security*.

Precautions

- To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the 802.1X access profile is bound to enable the DHCP snooping function on the interface and globally.
- The EAP protocol does not specify a standard attribute to carry IP address information. Therefore, if the EAP request packet sent by a static IP user does not contain an IP address, the IP address information in the DHCP snooping binding table is obtained from the user' first ARP request packet with the same MAC address as the user information table after the user passes authentication. On a network, unauthorized users may forge authorized users' MAC addresses to initiate ARP snooping attacks to devices, and the DHCP snooping binding table generated accordingly may be unreliable. Therefore, the **dot1x trigger dhcp-binding** command is not recommended and you are advised to run the **user-bind static** command to configure the static binding table.
- For users who are assigned IP addresses using DHCP, you do not need to run the **dot1x trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.
- The IP address in the DHCP snooping binding table is extracted from the ARP request packet (the first ARP request packet sent by the user after the user is authenticated or in the pre-connection state that has the same MAC address

in the user information table). If the static IP address of a user is changed, the user needs to be authenticated again.

Example

In the 802.1X access profile **d1**, enable the device to automatically generate the DHCP snooping binding table after static IP users pass 802.1X authentication or when the users are at the pre-authentication phase.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x trigger dhcp-binding
```

19.6.68 dot1x timer mac-bypass-delay

Function

The **dot1x timer mac-bypass-delay** command configures the 802.1X authentication timeout timer after which MAC address authentication is performed.

The **undo dot1x timer mac-bypass-delay** command restores the default configuration.

By default, the device performs MAC address authentication if 802.1X authentication is not successful within 30 seconds.

Format

dot1x timer mac-bypass-delay *delay-time-value*

undo dot1x timer mac-bypass-delay

Parameters

Parameter	Description	Value
delay-time-value	Specifies the value of the 802.1X authentication timeout timer after which MAC address authentication is performed.	The value is an integer in the range 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After MAC address bypass authentication is configured, the device performs 802.1X authentication first and starts the timer configured using the **dot1x timer mac-bypass-delay** *delay-time-value* command. If 802.1X authentication is not successful before the timer expires, the device performs MAC address authentication on users. You can run the **19.6.64 dot1x retry** *max-retry-value* command to set the number of times an authentication request is retransmitted to an 802.1X user. The retransmission interval is the integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)

Example

Configure the device to perform MAC address authentication if 802.1X authentication is not successful within 60 seconds.

```
<Huawei> system-view
[Huawei] dot1x timer mac-bypass-delay 60
```

19.6.69 dot1x timer tx-period

Function

The **dot1x timer tx-period** command sets the interval at which the device sends authentication requests.

The **undo dot1x timer tx-period** command restores the default configuration.

By default, the device sends authentication requests at an interval of 30 seconds.

Format

dot1x timer tx-period *tx-period-value*

undo dot1x timer tx-period

Parameters

Parameter	Description	Value
tx-period-value	Specifies the interval for sending authentication requests.	The value is an integer that ranges from 1 to 120, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device starts the **tx-period** timer in either of the following situations:

- When the client initiates authentication and MAC address bypass authentication is not configured, the device sends a unicast Request/Identity packet to the client and starts the **tx-period** timer. If the client does not respond within the period set by the timer, the device retransmits the authentication request.
- To authenticate the 802.1X clients that cannot initiate authentication, the device periodically sends multicast Request/Identity packets through the 802.1X-enabled interface to the clients at the interval set by the **tx-period** timer.

After MAC address bypass authentication is enabled on a device, the interval at which the device sends unicast Request/Identity packets to clients is determined by *delay-time-value* configured in the **19.6.68 dot1x timer mac-bypass-delay** command and *max-retry-value* configured in the **19.6.64 dot1x retry** command. The retransmission interval is the integer part of the value calculated using the following formula: *delay-time-value*/(*max-retry-value* + 1)

Normally, it is recommended that you retain the default setting of the timer.

Example

Set the interval at which the device sends authentication requests to 90 seconds.

```
<Huawei> system-view
[Huawei] dot1x timer tx-period 90
```

19.6.70 dot1x unicast-trigger

Function

The **dot1x unicast-trigger** command enables 802.1X authentication triggered by unicast packets.

The **undo dot1x unicast-trigger** command disables 802.1X authentication triggered by unicast packets.

By default, 802.1X authentication triggered by unicast packets is disabled.

Format

dot1x unicast-trigger

undo dot1x unicast-trigger

Parameters

None

Views

802.1X access profile view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

After the **dot1x unicast-trigger** command is used on the device, the device sends a unicast packet to respond to the received ARP or DHCP Request packet from a client. If the client does not respond within the timeout interval (set by the **19.6.65 dot1x timer client-timeout** *client-timeout-value* command), the device retransmits the unicast packet (the maximum of retransmission times is set by the **19.6.64 dot1x retry** *max-retry-value* command). This function allows users to use the 802.1X client provided by the operating system for authentication, helping quickly deploy an 802.1X network.

After receiving a packet that triggers 802.1X authentication from a client, the device sends a unicast packet to the client. For clients that cannot send packets to trigger 802.1X authentication, configure multicast packets to trigger 802.1X authentication.

Example

In the 802.1X access profile **d1**, enable 802.1X authentication triggered by unicast packets.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x unicast-trigger
```

19.6.71 dot1x url

Function

The **dot1x url** command configures the redirect-to URL in 802.1X authentication.

The **undo dot1x url** command cancels the redirect-to URL configuration in 802.1X authentication.

By default, no redirect-to URL is configured in 802.1X authentication.

Format

dot1x url *url-string*

undo dot1x url

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url-string	Specifies the redirect-to URL.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?). When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the early stage of network deployment, 802.1X client deployment is difficult with heavy workload. You can run the **dot1x url** command to set the redirect-to URL to the 802.1X client download web page address. When a user attempts to access a non-free IP subnet, the device redirects the user to the redirect-to URL where the user can download and install the 802.1X client software.

Follow-up Procedure

Run the **19.6.75 free-rule** command to configure a free IP subnet where the redirect URL used in 802.1X authentication belongs.

Precautions

Wireless users do not support the redirect URL configuration in 802.1X authentication.

The device does not support the triggering of a redirect URL through HTTPS packets.

Example

Set the redirect-to URL in 802.1X authentication to http://www.***.com.cn.

```
<Huawei> system-view
[Huawei] dot1x url http://www.***.com.cn
```

19.6.72 dot1x-access-profile (authentication profile view)

Function

The **dot1x-access-profile** command binds an authentication profile to an 802.1X access profile.

The **undo dot1x-access-profile** command unbinds an authentication profile from an 802.1X access profile.

By default, an authentication profile is not bound to an 802.1X access profile.

Format

dot1x-access-profile *access-profile-name*

undo dot1x-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of an 802.1X access profile.	The value must be the name of an existing 802.1X access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to an 802.1X access profile, the authentication profile is enabled with 802.1X authentication. After the authentication profile is applied to the interface or VAP profile, 802.1X authentication can be performed on online users.

Prerequisites

An 802.1X access profile has been created using the **19.6.73 dot1x-access-profile (system view)** command.

Follow-up Procedure

Run the **19.6.26 authentication-profile (Interface view or VAP profile view)** command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one 802.1X access profile.

Example

Bind the authentication profile **dot1x_authen_profile1** to the 802.1X access profile **dot1x_access_profile1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name dot1x_access_profile1
[Huawei-dot1x-access-profile-dot1x_access_profile1] quit
[Huawei] authentication-profile name dot1x_authen_profile1
[Huawei-authen-profile-dot1x_authen_profile1] dot1x-access-profile dot1x_access_profile1
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.73 dot1x-access-profile (system view)

Function

The **dot1x-access-profile** command creates an 802.1X access profile and displays the 802.1X access profile view.

The **undo dot1x-access-profile** command deletes an 802.1X access profile.

By default, the device has a built-in 802.1X access profile named dot1x_access_profile.

Format

dot1x-access-profile name *access-profile-name*

undo dot1x-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of an 802.1X access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses 802.1X access profiles to uniformly manage all 802.1X users access configurations. To perform 802.1X authentication for the users in the interface or

VAP profile, bind the authentication profile applied to the interface or VAP profile to an 802.1X access profile.

Follow-up Procedure

Run the **19.6.72 dot1x-access-profile (authentication profile view)** command in the authentication profile view to bind the authentication profile to an 802.1X access profile.

Precautions

- The device supports a maximum of 8 configurable 802.1X access profiles. The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in 802.1X access profile dot1x_access_profile can be modified and applied, but cannot be deleted.
- Before deleting an 802.1X access profile, ensure that this profile is not bound to any authentication profile.

Example

Create the 802.1X access profile named **dot1x_access_profile1**.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name dot1x_access_profile1
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.74 dot1x port-control

Function

The **dot1x port-control** command sets the authorization state of an interface.

The **undo dot1x port-control** command restores the default authorization state of an interface.

By default, the authorization state of an interface is **auto**.

Format

dot1x port-control { **auto** | **authorized-force** | **unauthorized-force** }

undo dot1x port-control

Parameters

Parameter	Description	Value
auto	Indicates the auto identification mode. In this mode, an interface is initially in Unauthorized state and only allows users to send and receive EAPOL packets. Users cannot access network resources. After the users are authenticated, the interface becomes authorized and allows the users to access network resources.	-
authorized-force	Indicates the forcible authorization mode. In this mode, the interface is always in Authorized state, does not handle EAPOL packets, and allows users to access network resources without authentication or authorization. Indicates the forcible unauthorized mode. In this mode, the interface is always in Unauthorized state, does not handle EAPOL packets, and prohibits users from accessing network resources.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
unauthorized-force	Indicates the forcible authorization mode. In this mode, the interface is always in Authorized state, does not handle EAPOL packets, and allows users to access network resources without authentication or authorization. Indicates the forcible unauthorized mode. In this mode, the interface is always in Unauthorized state, does not handle EAPOL packets, and prohibits users from accessing network resources.	-

Views

802.1X access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **auto** mode is recommended. Only authenticated users can access network resources. To trust all users on an interface without authentication, configure the **authorized-force** mode. To disable access rights of all users on an interface to ensure security, configure the **unauthorized-force** mode.

Precautions

If 802.1X users on an interface have gone online, changing the authorization state in the 802.1X access profile bound to the interface will make the online 802.1X users go offline.

It is recommended that you set the authorization state of an interface in the early stage of network deployment. When the network is running properly, run the **cut access-user** command to disconnect all users from the interface before changing the authorization state.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the authorization state of an interface as **unauthorized-force** in 802.1X access profile **d1**.

```
<Huawei> system-view
[Huawei] dot1x-access-profile name d1
[Huawei-dot1x-access-profile-d1] dot1x port-control unauthorized-force
```

Related Topics

19.6.33 display dot1x-access-profile configuration

19.6.75 free-rule

Function

The **free-rule** command configures authentication-free rules for NAC authentication users.

The **undo free-rule** command restores the default settings.

By default, no authentication-free rule is configured for NAC authentication users.

Format

Common authentication-free rule:

free-rule *rule-id* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } } | **source** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *ip-mask* } | **any** } } } *

undo free-rule { *rule-id* | **all** }

Authentication-free rule defined by ACL:

free-rule acl *acl-id*

undo free-rule acl

Parameters

Parameter	Description	Value
rule-id	Specifies the number of an authentication-free rule for NAC authentication users.	The value is an integer that ranges from 0 to 39.
destination	Specifies the destination network resource that NAC authentication users can access without authentication.	-
source	Specifies source information for NAC authentication users without authentication.	-

Parameter	Description	Value
any	Indicates any condition. When **any** is used together with different keywords, the effect of the command is different.	-
ip *ip-address*	Specifies the source or destination IP address depending on the keyword.	The value is in dotted decimal notation.
mask *mask-length*	Specifies the mask length of the source or destination IP address depending on the keyword.	The value is an integer that ranges from 1 to 32.
mask *ip-mask*	Specifies the mask of the source or destination IP address depending on the keyword.	The value is in dotted decimal notation.
acl	Specifies an authentication-free rule defined by ACL.	-
acl-id	Specifies the number of an IPv4 ACL.	The value is an integer that ranges from 6000 to 6031.
all	Specifies all rules.	-

Views

Authentication-free rule profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To meet basic network access requirements of users who have not passed authentication, the users need to obtain some network access rights without authentication, for example, download 802.1X client software and update the antivirus database. After running the **19.6.77 free-rule-template (system view)** command to create an authentication-free rule profile, run the **free-rule** command to configure authentication-free rules in the profile. The users then can obtain some network access rights without authentication.

Precautions

Wireless 802.1X authentication does not support this function.

A common authentication-free rule cannot be configured together with an authentication-free rule defined by ACL.

 Copyright © Huawei Technologies Co., Ltd.

The priority of the ACL rule delivered by the RADIUS server is higher than that of the authentication-free rule configured on the device.

Example

In the authentication-free rule profile **default_free_rule**, allow all NAC authentication users to access the network with the IP address 10.1.1.1/24 without authentication.

```
<Huawei> system-view
[Huawei] free-rule-template name default_free_rule
[Huawei-free-rule-default_free_rule] free-rule 1 destination ip 10.1.1.1 mask 24 source ip any
```

19.6.76 free-rule-template (authentication profile view)

Function

The **free-rule-template** command binds an authentication-free rule profile to an authentication profile.

The **undo free-rule-template** command unbinds an authentication-free rule profile from an authentication profile.

By default, no authentication-free rule profile is bound to an authentication profile.

Format

free-rule-template *free-rule-template-name*

undo free-rule-template

Parameters

Parameter	Description	Value
free-rule-template-name	Specifies the name of an authentication-free rule profile.	The value must be the name of an existing authentication-free rule profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before being authenticated, users need to obtain some network access rights to meet basic network access requirements such as downloading the 802.1X client

and updating antivirus database. The device uses an authentication-free rule profile to uniformly manage authorization information for authentication-free users. You can define some network access rules in the profile to determine network access rights that can be obtained by authentication-free users. You need to bind a configured authentication-free rule profile to an authentication profile. Users using the authentication profile then can obtain authentication-free authorization information.

Prerequisites

An authentication-free rule profile has been created using the **19.6.77 free-rule-template (system view)** command.

Example

Bind the authentication-free rule profile **default_free_rule** to the authentication profile **p1**.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] free-rule-template default_free_rule
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.35 display free-rule-template configuration

19.6.77 free-rule-template (system view)

Function

The **free-rule-template** command creates an authentication-free rule profile and displays the authentication-free rule profile view.

By default, the device has a built-in authentication-free rule profile named default_free_rule.

Format

free-rule-template name *free-rule-template-name*

Parameters

Parameter	Description	Value
name *free-rule-template-name*	Specifies the name of an authentication-free rule profile.	Currently, the device supports only one authentication-free rule profile, that is, the built-in profile **default_free_rule**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To meet basic network access requirements of users who have not passed authentication, the users need to obtain some network access rights without authentication, for example, download 802.1X client software and update the antivirus database. After creating an authentication-free rule profile using the **free-rule-template** command, you can configure authentication-free rules in the profile to allow the users to access the specified network resources without authentication.

Follow-up Procedure

Run the **19.6.75 free-rule** command in the authentication-free rule profile view to configure authentication-free rules for users.

Precautions

Currently, the device supports only one authentication-free rule profile, that is, the built-in profile **default_free_rule**.

Example

Display the view of the authentication-free rule profile **default_free_rule**.

```
<Huawei> system-view
[Huawei] free-rule-template name default_free_rule
[Huawei-free-rule-default_free_rule]
```

Related Topics

19.6.35 display free-rule-template configuration

19.6.78 http get-method enable

Function

The **http get-method enable** command configures the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

The **undo http get-method enable** command restores the default setting.

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication.

Format

http get-method enable

undo http get-method enable

Parameters

None

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device does not allow users to submit user name and password information to the device in GET mode during Portal authentication. You can run the **http get-method enable** command to configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

Precautions

The GET mode has the risk of password disclosure. Therefore, the POST mode is recommended.

This command only applies to scenarios in which HTTP or HTTPS is used for Portal connection establishment.

Example

Configure the device to allow users to submit user name and password information to the device in GET mode during Portal authentication.

```
<Huawei> system-view
[Huawei] web-auth-server abc
[Huawei-web-auth-server-abc] http get-method enable
```

19.6.79 http-method post

Function

The **http-method post** command configures parameters for parsing and replying to POST or GET request packets of the HTTP or HTTPS protocol.

The **undo http-method post** command restores the default configuration.

By default, the system has configured parameters for parsing and replying to POST or GET request packets of the HTTP or HTTPS protocol. For details, see the "Parameters" table.

Format

http-method post { **cmd-key** *cmd-key* [**login** *login-key* | **logout** *logout-key*] * | **init-url-key** *init-url-key* | **login-fail response** { **err-msg** { **authenserve-reply-**

message | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] } | **login-success response** { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* } | **logout-fail response** { **msg** *msg* | **redirect-url** *redirect-url* } | **logout-success response** { **msg** *msg* | **redirect-url** *redirect-url* } | **password-key** *password-key* | **user-mac-key** *user-mac-key* | **userip-key** *userip-key* | **username-key** *username-key* } *

undo http-method post { **all** | { **cmd-key** | **init-url-key** | **login-fail** | **login-success** | **logout-fail** | **logout-success** | **password-key** | **user-mac-key** | **userip-key** | **username-key** } * }

Parameters

Parameter	Description	Value
cmd-key *cmd-key*	Specifies the command identification keyword. The default value is **cmd**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
login *login-key*	Specifies the user login identification keyword. The default value is **login**.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
logout *logout-key*	Specifies the user logout identification keyword. The default value is **logout**.	The value is a string of 1 to 15 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
init-url-key *init-url-key*	Specifies the identification keyword for the user initial login URL. The default value is **initurl**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
login-fail response { **err-msg** { **authenserve-reply-message** | **msg** *msg* } | **redirect-login-url** | **redirect-url** *redirect-url* [**append-reply-message** *msgkey*] }	Specifies the response message upon a user login failure. • **err-msg authenserve-reply-message**: The authentication server response message is displayed after a user login failure. • **err-msg msg** *msg*: A specified message is displayed after a user login failure. • **redirect-login-url**: A user is redirected to the login URL after a login failure. This mode is the default mode. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after a login failure. • **append-reply-message** *msgkey*: specifies the identification keyword for the authentication server response message carried in the redirection URL.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 200 case-sensitive characters without spaces. • *msgkey*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
login-success response { **msg** *msg* | **redirect-init-url** | **redirect-url** *redirect-url* }	Specifies the response message upon successful user login. • **msg** *msg*: A specified message is displayed after successful user login. • **redirect-init-url**: A user is redirected to the initial login URL after successful login. This mode is the default mode. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after successful login.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 200 case-sensitive characters without spaces.
logout-fail response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon a user logout failure. • **msg** *msg*: A specified message is displayed after a user logout failure. The default value is **LogoutFail!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after a logout failure.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 200 case-sensitive characters without spaces.
logout-success response { **msg** *msg* | **redirect-url** *redirect-url* }	Specifies the response message upon successful user logout. • **msg** *msg*: A specified message is displayed after successful user logout. The default value is **LogoutSuccess!**. • **redirect-url** *redirect-url*: A user is redirected to a specified URL after successful logout.	• *msg*: The value is a string of 1 to 200 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). • *redirect-url*: The value is a string of 1 to 200 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password-key *password-key*	Specifies the password identification keyword. The default value is **password**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
user-mac-key *user-mac-key*	Specifies the identification keyword for the user MAC address. The default value is **macaddress**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
userip-key *userip-key*	Specifies the identification keyword for the user IP address. The default value is **ipaddress**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
username-key *username-key*	Specifies the user name identification keyword. The default value is **username**.	The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=).
all	Indicates all parameters.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

When the device uses the HTTP or HTTPS protocol to communicate with the Portal server, a user sends POST or GET request packets (carrying parameters such as the user name and MAC address) to the device as required by the Portal server. After receiving the POST or GET request packets, the device parses parameters in the packets. If identification keywords of the parameters differ from those configured on the device, the user authentication fails. Therefore, you need to run the **http-method post** command to configure the identification keywords based on the Portal server configuration.

After successful user login or logout, or a user login or logout failure, the device sends the login or logout result to the user based on the **http-method post**

command configuration. For example, the device sends the **LogoutSuccess!** message to a user who logs out successfully by default.

Example

Set the command identification keyword to **cmd1** for parsing POST or GET request packets of the HTTP or HTTPS protocol.

```
<Huawei> system-view
[Huawei] web-auth-server abc
[Huawei-web-auth-server-abc] http-method post cmd-key cmd1
```

19.6.80 force-push

Function

The **force-push** command enables the forcible URL template or URL push function.

The **undo force-push** command disables the forcible URL template or URL push function.

By default, the forcible URL template or URL push function is disabled.

Format

force-push { **url-template** *template-name* | **url** *url-address* }

undo force-push

Parameters

Parameter	Description	Value
url-template *template-name*	Specifies the name of a pushed URL template.	The value must be the name of an existing URL template.
url *url-address*	Specifies a pushed URL.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?). When double quotation marks are used around the string, spaces are allowed in the string.

Views

AAA domain view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a user is successfully authenticated, the device forcibly redirect the user to a web page when receiving the HTTP or HTTPS packet from the user who accesses web pages for the first time. In addition to pushing advertisement pages, the device can obtain user terminal information through the HTTP or HTTPS packets sent by the users, and apply the information to other services. There are two ways to push web pages:

1. URL: pushes the URL corresponding to the web page.
2. URL template: pushes the URL template. A URL template must be created. The URL template contains the URL of the pushed web page and URL parameters.

Prerequisites

The URL configured using the **19.6.142 url (URL template view)** command in the URL template view cannot be a redirection URL; otherwise, the command does not take effect.

Precautions

If an application program that actively sends HTTP or HTTPS packets is installed on the user terminal, the terminal has sent the HTTP or HTTPS packet before the user accesses a web page. Therefore, the user is unaware of the web page push process.

For HTTP and HTTPS packets, the forcible push function takes effect only when a redirection ACL is used. If the user table always contains redirection ACLs, a web page is forcibly pushed when HTTPS packets from users match redirection ACL rules. Usually, you can configure the RADIUS server to authorize the Huawei extended RADIUS attribute **HW-Redirect-ACL** to users for redirection ACL implementation.

A pushed URL configured in a domain need to be used together with a redirect ACL or push flag attribute. The redirect ACL has a higher priority than the push flag attribute. By default, a pushed URL configured in a domain carries the push flag attribute. Users will be redirected to the pushed URL when they are successfully authenticated.

When an IPv4 redirect ACL is configured for an IPv6 user or an IPv6 redirect ACL is configured for an IPv4 user, the **Push URL content** field in the **19.6.29 display access-user** command output displays the pushed URL, but the browser of the user cannot redirect to the pushed URL .

Example

Push the URL template **abc** in the domain **huawei**.

```
<Huawei> system-view
[Huawei] url-template name abc
[Huawei-url-template-abc] quit
[Huawei] aaa
[Huawei-aaa] domain huawei
[Huawei-aaa-domain-huawei] force-push url-template abc
```

19.6.81 link-down offline delay

Function

The **link-down offline delay** command configures the user logout delay when an interface link is faulty.

The **undo link-down offline delay** command restores the default configuration.

By default, the user logout delay is 10 seconds when an interface link is faulty.

Format

link-down offline delay { *delay-value* | **unlimited** }

undo link-down offline delay

Parameters

Parameter	Description	Value
delay-value	Specifies the user logout delay when an interface link is faulty.	The value is an integer that ranges from 0 to 60, in seconds. If the value is 0, users are logged out immediately when an interface link is faulty.
unlimited	Indicates that users are not logged out when an interface link is faulty.	-

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a link is faulty, the interface is interrupted and users are directly logged out. To solve this problem, you can configure the user logout delay function. When the interface link is faulty, the users remain online within the delay. In this case, if the link is restored, the users do not need to be re-authenticated. If the users are disconnected after the delay and the link is restored, the users need to be re-authenticated.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- This function takes effect only for wired users who go online on Layer 2 physical interfaces that have been configured with NAC authentication.
- To make the function take effect, it is recommended that the configured interval be greater than the time during which the interface is in Up state.

Example

In the authentication profile **p1**, set the user logout delay to 5 seconds when the link is faulty.

```
<Huawei> system-view
[Huawei] authentication-profile name p1
[Huawei-authen-profile-p1] link-down offline delay 5
```

19.6.82 mac-access-profile (authentication profile view)

Function

The **mac-access-profile** command binds an authentication profile to a MAC access profile.

The **undo mac-access-profile** command unbinds an authentication profile from a MAC access profile.

By default, an authentication profile is not bound to a MAC access profile.

Format

mac-access-profile *access-profile-name*

undo mac-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of a MAC access profile.	The value must be the name of an existing MAC access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to a MAC

access profile, the authentication profile is enabled with MAC address authentication. After the authentication profile is applied to the interface or VAP profile, MAC address authentication can be performed on online users.

Prerequisites

A MAC access profile has been created using the **19.6.83 mac-access-profile (system view)** command.

Follow-up Procedure

Run the **19.6.26 authentication-profile (Interface view or VAP profile view)** command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one MAC access profile.

Example

Bind the authentication profile **mac_authen_profile1** to the MAC access profile **mac_access_profile**.

```
<Huawei> system-view
[Huawei] mac-access-profile name mac_access_profile
[Huawei-mac-access-profile-mac_access_profile] quit
[Huawei] authentication-profile name mac_authen_profile1
[Huawei-authen-profile-mac_authen_profile1] mac-access-profile mac_access_profile
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.83 mac-access-profile (system view)

Function

The **mac-access-profile** command creates a MAC access profile and displays the MAC access profile view.

The **undo mac-access-profile** command deletes the MAC access profile.

By default, the device has a built-in MAC access profile named **mac_access_profile**.

Format

mac-access-profile name *access-profile-name*

undo mac-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of a MAC access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses MAC access profiles to uniformly manage all MAC users access configurations. To perform MAC address authentication for the users in the interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to a MAC access profile.

Follow-up Procedure

Run the **19.6.82 mac-access-profile (authentication profile view)** command in the authentication profile view to bind the authentication profile to a MAC access profile.

Precautions

- The device supports a maximum of 8 configurable MAC access profiles. The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in MAC access profile **mac_access_profile** can be modified and applied, but cannot be deleted.
- Before deleting a MAC access profile, ensure that this profile is not bound to any authentication profile.

Example

Create the MAC access profile named **mac_access_profile**.

```
<Huawei> system-view
[Huawei] mac-access-profile name mac_access_profile
```

Related Topics

19.6.38 display mac-access-profile configuration

 Copyright © Huawei Technologies Co., Ltd.

19.6.84 mac-authen authentication-method

Function

The **mac-authen authentication-method** command configures the authentication mode for MAC address authentication.

The **undo mac-authen authentication-method** command restores the default configuration.

By default, the authentication mode for MAC address authentication is set to PAP.

Format

mac-authen authentication-method { **chap** | **pap** }

undo mac-authen authentication-method

Parameters

Parameter	Description	Value
chap	Indicates the Challenge Handshake Authentication Protocol (CHAP) authentication mode.	-
pap	Indicates the Password Authentication Protocol (PAP) authentication mode.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In MAC address authentication, the access device exchanges RADIUS packets with the authentication server. Differences between authentication modes PAP and CHAP are as follows:

- PAP is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.

 Copyright © Huawei Technologies Co., Ltd.

- CHAP is a three-way handshake authentication protocol. It transmits only user names but not passwords in RADIUS packets. CHAP is more secure and reliable than PAP. If high security is required, CHAP is recommended.

By default, the authentication mode for MAC address authentication is set to PAP. The authentication mode can be changed to CHAP for higher security.

Precautions

The authentication server must support CHAP when the authentication mode is set to CHAP.

Example

In the MAC access profile **mac_access_profile**, set the authentication mode for MAC address authentication to CHAP.

```
<Huawei> system-view
[Huawei] mac-access-profile name mac_access_profile
[Huawei-mac-access-profile-mac_access_profile] mac-authen authentication-method chap
```

19.6.85 mac-authen domain

Function

The **mac-authen domain** command configures an authentication domain for MAC address authentication users.

The **undo mac-authen domain** command restores the global default authentication domain for MAC address authentication users.

The default authentication domain for MAC address authentication users is the global default domain.

Format

mac-authen domain *isp-name* **mac-address** *mac-address* **mask** *mask*

undo mac-authen domain [*isp-name*] **mac-address** *mac-address*

undo mac-authen domain mac-address all

Parameters

Parameter	Description	Value
isp-name	Specifies the ISP domain name.	The value is a string of 1 to 64 case-insensitive characters without any space, asterisk (*), question mark (?), quotation mark ("), hyphen (-) or consecutive hyphens (--).

Parameter	Description	Value
mac-address *mac-address*	Specifies an authentication domain for the MAC address authentication user with a specified MAC address.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the mask of a MAC address.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
all	Restores the global default domain for all MAC address authentication users.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When user names for MAC address authentication do not contain domain names, the device authenticates users using the **default** domain if no authentication domain is configured on the device.

Precautions

You must specify a unicast MAC address in the **mac-authen domain** command. A user with an all-0 MAC address is not authenticated.

The configured authentication domain is applied to the MAC addresses calculated with the mask. Therefore, the **undo mac-authen domain** command will delete the authentication domain of the calculated MAC addresses. Before running the **undo mac-authen domain** command, run the **display this** command to view the calculated MAC addresses.

On a network configured with both 802.1X authentication and MAC address bypass authentication, an 802.1X user failing the 802.1X authentication will be authenticated in the manner of MAC address bypass authentication. If the authentication scheme of MAC address bypass authentication is none authentication, the user can go online successfully without being authenticated. To prevent such unauthorized authentication, use the **mac-authen domain** command to specify different domains for the two authentication methods.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the **huawei** domain as the authentication domain for the MAC address authentication user with the MAC address 00e0-fc09-bcf9 and MAC address mask ffff-ffff-ffff in the system view.

```
<Huawei> system-view
[Huawei] mac-authen domain huawei mac-address 00e0-fc09-bcf9 mask ffff-ffff-ffff
```

19.6.86 mac-authen permit mac-address

Function

The **mac-authen permit mac-address** command specifies the MAC address range allowed for MAC address authentication.

The **undo mac-authen permit mac-address** command deletes the MAC address range allowed for MAC address authentication.

By default, no MAC address range is specified for MAC address authentication.

Format

mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

undo mac-authen permit mac-address *mac-address* **mask** { *mask* | *mask-length* }

Parameters

Parameter	Description	Value
mac-address	Specifies a MAC address for MAC address authentication.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask*	Specifies the MAC address mask.	The value is in H-H-H format. H contains 1 to 4 hexadecimal digits.
mask *mask-length*	Specifies the MAC address mask length.	The value is an integer that ranges from 1 to 48.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a new MAC address entry is generated on the device after MAC address authentication is enabled on a VLANIF interface, MAC address authentication will be performed for the corresponding user. To actually control the users who can be authenticated using MAC addresses on the VLANIF interface, use this command to specify a MAC address range for MAC address authentication.

Precautions

Only MAC address authentication users who go online through VLANIF interfaces support this function.

Example

In the MAC access profile **m1**, set the MAC address to 0002-0002-0002 and the MAC address mask length to 24 for MAC address authentication.

```
<Huawei> system-view
[Huawei] mac-access-profile name m1
[Huawei-mac-access-profile-m1] mac-authen permit mac-address 0002-0002-0002 mask 24
```

19.6.87 mac-authen quiet-times

Function

The **mac-authen quiet-times** command configures the maximum number of authentication failures within 60 seconds before a MAC address authentication user enters the quiet state.

The **undo mac-authen quiet-times** command restores the maximum number of authentication failures to the default value.

By default, the maximum number of authentication failures is 10.

Format

mac-authen quiet-times *fail-times*

undo mac-authen quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a MAC address authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The quiet function for MAC address authentication is enabled on a device by default. When the maximum number of authentication failures exceeds 10 within 60 seconds, the device quiets a MAC address authentication user and does not process authentication requests from the user, reducing impact on the system caused by attackers.

Precautions

After the maximum number of authentication failures is set to a value larger than the configured value, the user in quiet state can initiate reauthentication only after the quiet period expires. If the user enters an incorrect user name or password again, the user authentication fails. The device does not quiet the user but allows the user to initiate reauthentication immediately.

Example

Set the maximum number of authentication failures within 60 seconds to 4.

```
<Huawei> system-view
[Huawei] mac-authen quiet-times 4
```

19.6.88 mac-authen reauthenticate mac-address

Function

The **mac-authen reauthenticate mac-address** command enables re-authentication for an online MAC address authentication user with a specified MAC address.

By default, re-authentication for an online MAC address authentication user with a specified MAC address is disabled.

Format

mac-authen reauthenticate mac-address *mac-address*

Parameters

Parameter	Description	Value
mac-address	Specifies all valid unicast MAC addresses.	The value is a unicast MAC address in H-H-H format, where H can be one to four hexadecimal digits.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

For details, see **19.6.89 mac-authen reauthenticate**.

The **mac-authen reauthenticate mac-address** and **19.6.89 mac-authen reauthenticate** commands re-authenticate online MAC address authentication users and their difference is as follows:

- The **mac-authen reauthenticate mac-address** command configures the device to immediately re-authenticate a user with a specified MAC address for once.
- The **19.6.89 mac-authen reauthenticate** command configures the device to re-authenticate all online MAC address authentication users at intervals.

Example

Enable re-authentication for an online MAC address authentication user with the MAC address 0001-0002-0003.

```
<Huawei> system-view
[Huawei] mac-authen reauthenticate mac-address 0001-0002-0003
```

19.6.89 mac-authen reauthenticate

Function

The **mac-authen reauthenticate** command enables re-authentication for online MAC address authentication users.

The **undo mac-authen reauthenticate** command restores the default configuration.

By default, re-authentication for online MAC address authentication users is disabled.

Format

mac-authen reauthenticate

undo mac-authen reauthenticate

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the administrator modifies the authentication parameters of an online user on the authentication server, the user must be re-authenticated to ensure user validity.

After the user goes online, the device saves authentication parameters of the user. After re-authentication is configured for online MAC address authentication users, the device automatically sends the user authentication parameters in the MAC access profile to the authentication server at an interval (specified using the **19.6.91 mac-authen timer reauthenticate-period** command) for re-authentication. If the user authentication information on the authentication server remains unchanged, the users are kept online. If the information has been changed, the users are disconnected and need to be re-authenticated based on the changed authentication parameters.

Precautions

After periodic re-authentication is configured for online MAC address authentication users, a large number of MAC address authentication logs are generated.

If the device is connected to a server for re-authentication and the server replies with a re-authentication deny message that makes an online user go offline, it is recommended that you locate the cause of the re-authentication failure on the server or disable the re-authentication function on the device.

Example

In the MAC access profile **mac_access_profile**, configure re-authentication for online MAC address authentication users.

```
<Huawei> system-view
[Huawei] mac-access-profile name mac_access_profile
[Huawei-mac-access-profile-mac_access_profile] mac-authen reauthenticate
```

Related Topics

19.6.38 display mac-access-profile configuration

19.6.90 mac-authen timer quiet-period

Function

The **mac-authen timer quiet-period** command configures the quiet period for MAC address authentication users who fail to be authenticated.

The **undo mac-authen timer quiet-period** command restores the default quiet period.

 Copyright © Huawei Technologies Co., Ltd.

By default, the quiet period is 60 seconds for MAC address authentication users who fail to be authenticated.

Format

mac-authen timer quiet-period *quiet-period-value*

undo mac-authen timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Sets the quiet period for MAC address authentication users who fail to be authenticated.	The value is an integer that ranges from 0 to 3600, in seconds. **NOTE** If the value of *quiet-period-value* is 0, the quiet function is disabled for MAC address authentication users.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a MAC address authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled, if the number of times that a MAC address authentication user fails to be authenticated within 60s exceeds the upper limit (configured using the **19.6.87 mac-authen quiet-times** command), the device discards the user's MAC address authentication request packets for a period to avoid frequent authentication failures.

Example

Set the quiet period to 100 seconds for MAC address authentication users who fail to be authenticated.

```
<Huawei> system-view
[Huawei] mac-authen timer quiet-period 100
```

19.6.91 mac-authen timer reauthenticate-period

Function

The **mac-authen timer reauthenticate-period** command configures the re-authentication interval for online MAC address authentication users.

The **undo mac-authen timer reauthenticate-period** command restores the default setting.

By default, the re-authentication period is 1800 seconds for online MAC address authentication users.

Format

mac-authen timer reauthenticate-period *reauthenticate-period-value*

undo mac-authen timer reauthenticate-period

Parameters

Parameter	Description	Value
reauthenticate-period-value	Specifies the interval for re-authenticating online MAC address authentication users.	The value is an integer that ranges from 60 to 7200, in seconds.

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring the re-authentication function for online MAC address authentication users using the **19.6.89 mac-authen reauthenticate** command, run the **mac-authen timer reauthenticate-period** command to configure the re-authentication interval. The device then re-authenticates online users at the specified interval, ensuring that only authorized users can keep online.

Precautions

Generally, the default re-authentication interval is recommended. If many ACL rules need to be delivered during user authorization, to improve the device processing performance, you are advised to disable re-authentication or increase the re-authentication internal. When remote authentication and authorization are

 Copyright © Huawei Technologies Co., Ltd.

used and a short re-authentication interval is used, the CPU usage may become high.

To reduce the impact on the device performance when many users exist, the user re-authentication interval may be longer than the configured re-authentication interval.

Example

In the MAC access profile **mac_access_profile**, configure the re-authentication interval for online MAC address authentication users to 2000 seconds.

```
<Huawei> system-view
[Huawei] mac-access-profile name mac_access_profile
[Huawei-mac-access-profile-mac_access_profile] mac-authen timer reauthenticate-period 2000
```

Related Topics

19.6.89 mac-authen reauthenticate

19.6.38 display mac-access-profile configuration

19.6.92 mac-authen trigger dhcp-binding

Function

The **mac-authen trigger dhcp-binding** command enables the device to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-connection phase.

The **undo mac-authen trigger dhcp-binding** command restores the default configuration.

By default, the device does not automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

Format

mac-authen trigger dhcp-binding

undo mac-authen trigger dhcp-binding

Parameters

None

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There are unauthorized users who modify their MAC addresses to those of authorized users. After authorized users are connected through MAC address authentication, the unauthorized users can obtain the same identities as the authorized users. This results in security risks of authentication and accounting. After accessing the network, unauthorized users can also initiate ARP spoofing attacks by sending bogus ARP packets. In this case, the device records incorrect ARP entries, greatly affecting normal communication between authorized users. To prevent the previous attacks, configure IPSG. This function is implemented based on binding tables. For static IP users, you can run the **user-bind static** command to configure the static binding table. However, if there are many static IP users, it takes more time to configure static binding entries one by one.

To reduce the workload, you can configure the device to automatically generate the DHCP snooping binding table for static IP users. After this function is enabled, the device automatically generates the DHCP snooping binding table based on the MAC address, IP address, and interface information of static IP users who pass MAC address authentication or are at the pre-authentication phase.

You can run the **display dhcp snooping user-bind** command to check the DHCP snooping binding table that is generated by the device for static IP users who pass MAC address authentication or are at the pre-authentication phase. The DHCP snooping binding table generated using this function will be deleted after the users are disconnected.

Follow-up Procedure

Configure IPSG and DAI after the DHCP snooping binding table is generated, prevent attacks from unauthorized users.

- In the interface view, run the **ip source check user-bind enable** command to enable IPSG.

For detailed configuration of IPSG, see **IPSG Configuration** in the *Huawei AR Series V200R010 Configuration Guide - Security*.

Precautions

- To make this function take effect, you must run the **dhcp snooping enable** command on the interface to which the mac access profile is bound to enable the DHCP snooping function on the interface and globally.
- The authentication profile bound to the MAC access profile in which the command is configured must be applied to a Layer 2 interface. If the authentication profile is applied to a Layer 3 interface, the command does not take effect.
- For users who are assigned IP addresses using DHCP, you do not need to run the **mac-authen trigger dhcp-binding** command on the device. The DHCP snooping binding table is generated through the DHCP snooping function.
- The IP address in the DHCP snooping binding table is extracted from the ARP request packet (the first ARP request packet sent by the user after the user is authenticated or in the pre-connection state that has the same MAC address in the user information table).
- This function trusts only the first ARP packet in the authentication process. If a client sends an ARP packet with a non-static IP address during

 Copyright © Huawei Technologies Co., Ltd.

authentication and then sends an ARP packet with the real IP address, the DHCP snooping binding table is not updated. After this function is enabled, online users cannot change their static IP addresses. If the static IP address of a user is changed, the user needs to be authenticated again.

Example

In the MAC access profile **m1**, enable the device to automatically generate the DHCP snooping binding table after static IP users pass MAC address authentication or when the users are at the pre-authentication phase.

```
<Huawei> system-view
[Huawei] mac-access-profile name m1
[Huawei-mac-access-profile-m1] mac-authen trigger dhcp-binding
```

19.6.93 mac-authen username

Function

The **mac-authen username** command configures the user name for MAC address authentication.

The **undo mac-authen username** command restores the default setting.

By default, the MAC address without hyphens (-) or colons (:) is used as the user name and password for MAC address authentication.

Format

mac-authen username { **fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]] }

undo mac-authen username [**fixed** *username* [**password cipher** *password*] | **macaddress** [**format** { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** } [**uppercase**] [**password cipher** *password*]]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
fixed *username*	Specifies a fixed user name for MAC address authentication.	The value is a string of 1 to 64 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password cipher *password*	Specifies the password in cipher text for MAC address authentication. ● If no password is set when a fixed user name is used, the user can log in without a password. This brings a security risk and is not recommended. ● If no password is set when the MAC address is used as the user name, the user can log in using the MAC address as the password. A password must be configured when local authentication is used in the AAA scheme.	The value is a string of case-sensitive characters without spaces. The password is either a plain-text string of 1 to 128 characters or a cipher-text string of 48 to 188 characters. When double quotation marks are used around the string, spaces are allowed in the string. **NOTE** For security purposes, change the default password in real time. The new password must be a combination of at least two of the following: digits, lowercase letters, uppercase letters, and special characters. In addition, the password must consist of six or more than six characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
macaddress	Specifies the MAC address as the user name for MAC address authentication.	-
format { **with-hyphen** [**normal**] [**colon**] | **without-hyphen** }	Specifies the MAC address format. ● **with-hyphen**: indicates that the MAC address contains hyphens (-), for example, 0005-e01c-02e3. ● **with-hyphen normal**: indicates that the MAC address contains hyphens (-), for example, 00-05-e0-1c-02-e3. ● **with-hyphen colon**: indicates that the MAC address contains colons (:), for example, 0005:e01c:02e3. ● **with-hyphen normal colon**: indicates that the MAC address contains colons (:), for example, 00:05:e0:1c:02:e3. ● **without-hyphen**: indicates that the MAC address does not contain hyphens (-) or colons (:), for example, 0005e01c02e3.	-
uppercase	Indicates that the name of a MAC address authentication user is in uppercase.	-

Views

MAC access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The following user name formats are available for MAC address authentication:

- Fixed user name: A user uses the fixed user name and password configured by the administrator for authentication.
- MAC address: A user uses the MAC address as the user name for authentication. In addition, the MAC address or user-defined character string can be used as the password.

By default, the device sends the user MAC address as the user name and password to the authentication server for authentication. However, the users cannot be

easily identified and managed in this case. To flexibly identify and manage users, run the **mac-authen username** command to configure fixed user names and passwords for MAC address authentication users.

Precautions

- When configuring the user name format for MAC address authentication, ensure that the authentication server supports the user name format.
- If MAC address authentication is enabled on a WLAN-ESS interface, passwords must be configured.

Example

In the MAC access profile **mac_access_profile**, configure the device to use the MAC address containing hyphens (-) as the user name.

```
<Huawei> system-view
[Huawei] mac-access-profile name mac_access_profile
[Huawei-mac-access-profile-mac_access_profile] mac-authen username macaddress format with-hyphen
```

Related Topics

19.6.38 display mac-access-profile configuration

19.6.94 nginx proxy port

Function

The **nginx proxy port** command configures the port number of the Nginx proxy server.

The **undo nginx proxy port** command deletes the port number of the Nginx proxy server.

By default, the port number is 81 configured for the Nginx proxy server.

NOTE

Only the AR161EW, AR161EW-M1, AR169EGW-L, and AR169EW support the Nginx server.

Format

nginx proxy port { **default** | *port-number* }

undo nginx proxy port

Parameters

Parameter	Description	Value
default	Specifies the default port for the Nginx proxy server. **NOTE** The default port number is 81.	-

Parameter	Description	Value
port-number	Specifies the port number for the Nginx proxy server. **NOTE** The configured port number must be the same as the Nginx port number included in the Nginx configuration file.	The value is an integer that ranges from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The AR router has a built-in Nginx server, which functions as a web server. The server supports independent portal authentication of the router as well as provides web service to the mobile terminals of passengers. To configure the port number for the Nginx proxy server, run the **nginx proxy port** command. When an AR receives an HTTP request packet from a user to the Internet, traffic is forwarded to the interface where Nginx server is enabled. Then the Nginx server provides services such as web service to users.

Precautions

- Before using this command, run the **ngnix enable** command to enable the Nginx server.
- The configured port number must be the same as the Nginx port number included in the Nginx configuration file.

Example

Set the port number of Ngnix proxy server to 100.

```
<Huawei> system-view
[Huawei] nginx proxy port 100
```

19.6.95 nginx enable

Function

The **nginx enable** command enables the Nginx server.

The **undo nginx enable** command disables the Nginx server.

By default, the Nginx server is disabled.

NOTE

Only the AR161EW, AR161EW-M1, AR169EGW-L, and AR169EW support the Nginx server.

Format

nginx enable

undo nginx enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The routers have an embedded Nginx server. The Nginx server functions as a web server to provide web services for passengers through mobile terminals and a running environment for the Portal authentication function.

By default, the Nginx server is disabled on a started device. You can run the **nginx enable** command to enable the Nginx server.

Precautions

The Nginx configuration file must be in correct format and successfully loaded; otherwise, the Nginx server cannot be enabled.

Example

Enable the Nginx server.

```
<Huawei> system-view
[Huawei] nginx enable
Info: Nginx has been started.
```

19.6.96 nginx load

Function

The **nginx load** command configures the device to load the Nginx configuration file to the Nginx server when the server is enabled.

NOTE

The Nginx configuration file has a name extension **.conf**.

Format

nginx load { **default** | *file-name* }

Parameters

Parameter	Description	Value
default	Loads the default Nginx configuration file.	-
file-name	Loads the Nginx configuration file stored in the specified directory of a storage medium, such as the flash memory and SD card. **NOTE** If you specify only the file name but not the directory, the device loads the Nginx configuration file in the current storage directory (root directory of the flash memory).	The value is a character string of 6 to 64 case-insensitive characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Nginx configuration file defines web services provided by the Nginx server. Usually, a default Nginx configuration file is placed in the configuration directory of the routers before delivery and defines basic web services. When the Nginx server is enabled for the first time, the device loads the default Nginx configuration file to the Nginx server.

If you expect to extend web services provided by the Nginx server, place a new Nginx configuration file in the flash memory or SD card and then run the **nginx load** *file-name* command to load the configuration file to the Nginx server.

Precautions

- After the **nginx load** *file-name* command is run, the loaded Nginx configuration file is protected in the flash memory or SD card and cannot be modified or deleted.
- If you repeatedly load Nginx configuration files of different names in the system view, only the latest configuration file takes effect.
- After the Nginx configuration file is successfully loaded, run the **undo nginx enable** and **nginx enable** command in sequence to enable the Nginx server and make the configuration file take effect.

 Copyright © Huawei Technologies Co., Ltd.

- If you restart the device without saving configurations, the Nginx server still uses the last loaded configuration file on restart.

NOTE

Only the AR161EW, AR161EW-M1, AR169EGW-L, and AR169EW support the Nginx server.

Example

Load the default Nginx configuration file.

```
<Huawei> system-view
[Huawei] nginx load default
Info: Load nginx config file successful.
[Huawei] nginx enable
Info: Nginx has been started.
```

Load the Nginx configuration file in the root directory of the flash memory.

```
<Huawei> cd flash:
<Huawei> system-view
[Huawei] nginx load test.conf
Info: Load nginx config file successful.
[Huawei] undo nginx enable
[Huawei] nginx enable
Info: Nginx has been started.
```

19.6.97 parameter

Function

The **parameter** command sets the characters used in URL.

The **undo parameter** command restores the default settings.

By default, the start character is ?, assignment character is =, and delimiter is &.

Format

parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

undo parameter { **start-mark** *parameter-value* | **assignment-mark** *parameter-value* | **isolate-mark** *parameter-value* } *

Parameters

Parameter	Description	Value
start-mark *parameter-value*	Changes the specified start character to ?.	The value is one case-sensitive character without spaces.
assignment-mark *parameter-value*	Specifies the assignment character of the URL parameters.	The value is one case-sensitive character without spaces.

Parameter	Description	Value
isolate-mark *parameter-value*	Specifies the delimiter between URL parameters.	The value is one case-sensitive character without spaces.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

The **parameter** command allows you to customize the characters in URL.

For example, if the URL configured using the **19.6.142 url (URL template view)** command in the URL template bound to a Portal server profile is http://10.1.1.1, you can run the **19.6.145 url-parameter** command to add the user MAC address, user IP address, and device system name to the URL by specifying the **user_mac**, **user_ip**, and **device** parameters.

When a user with IP address 10.1.1.11 and MAC address 0002-0002-0002 connects to an access device **huawei**, the access device redirects the user to http://10.1.1.1?user_mac=0002-0002-0002&user_ip=10.1.1.11&device=huawei for Portal authentication. In the redirection URL, ? is the default start character, = is the default assignment character, & is the delimiter between parameters.

NOTE

If *parameter-value* is set to a question mark (?) in the URL, the command cannot be executed.

Example

Change the start character in a URL from # to ?.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] parameter start-mark #
```

19.6.98 port (Portal server profile view)

Function

The **port** command sets the port number that a Portal server uses to receive notification packets from the device.

The **undo port** command restores the default port number.

By default, a Portal server uses port number 50100 to receive packets from the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

port *port-number* [**all**]

undo port [**all**]

Parameters

Parameter	Description	Value
port-number	Specifies the port number that the Portal server uses to receive and encapsulate UDP packets from the device.	The value is an integer that ranges from 1 to 65535. By default, the value is 50100.
all	Indicates that the device always uses the destination port number specified by *port-number* to encapsulate UDP packets. **NOTE** After this keyword is specified, when receiving UDP packets from a Portal server, the device does not obtain the source port number in the UDP packets as the destination port number of UDP packets to be sent to the Portal server. If the value of *port-number* is different from the source port number of the Portal server, the Portal server cannot receive the UDP packets sent by the device. Therefore, this keyword is not recommended.	-

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server profile on the device using the **19.6.157 web-auth-server (system view)** command, configure parameters for the template.

Run the **port** command to set the port number that a Portal server uses to receive notification packets from the device. After receiving a Portal authentication request packet from a user, the device sends the packet to the Portal server using the specified destination port number.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Ensure that the port number configured on the device is the same as that used by the Portal server.

Example

Set the port number that a Portal server uses to receive packets from the device to 10000 in the Portal server profile **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] port 10000
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.157 web-auth-server (system view)

19.6.99 portal auth-network

Function

The **portal auth-network** command configures the source subnet for Portal authentication.

The **undo portal auth-network** command restores the default setting.

By default, the source subnet for Portal authentication is 0.0.0.0/0, indicating that users in all subnets must pass Portal authentication.

Format

portal auth-network *network-address* { *mask-length* | *mask-address* }

undo portal auth-network { *network-address* { *mask-length* | *mask-address* } | **all** }

Parameters

Parameter	Description	Value
network-address	Specifies a Portal authentication subnet.	The value is in dotted decimal notation.
mask-length | *mask-address*	Specifies the mask length or mask of the Portal authentication subnet. • *mask-length*: specifies the mask length. • *mask-address*: specifies the mask.	• The value of *mask-length* is an integer that ranges from 1 to 32. • The value of *mask-address* is in dotted decimal notation.
all	Deletes all Portal authentication subnets.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the source subnet for Portal authentication is configured, only user packets from the subnet can trigger Portal authentication. If an unauthenticated user is not on a Portal authentication subnet and packets from the user do not match any Portal authentication-free rule, the device discards the user's packets.

Precautions

The command takes effect only for Layer 3 Portal authentication. In Layer 2 Portal authentication, users on all subnets must be authenticated.

Example

In the Portal access profile **p1**, set the source authentication subnet to 10.1.1.0/24.

```
<Huawei> system-view
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] portal auth-network 10.1.1.0 24
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.100 portal captive-adaptive enable

Function

The **portal captive-adaptive enable** command enables the Captive Network Assistant (CNA) adaptive function for iOS terminals.

The **undo portal captive-adaptive enable** command disables the CNA adaptive function for iOS terminals.

By default, the CNA adaptive function is disabled for iOS terminals.

Format

portal captive-adaptive enable

undo portal captive-adaptive enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Since WLANs are widely provided, users have a demand for quick and convenient authentication by using applications on mobile terminals, without entering user names and passwords. In such authentication mode, mobile terminals need to automatically display the application-based Portal authentication page and the applications need to communicate with the background server. Therefore, the mobile terminals must be connected to the WLANs during authentication.

iOS terminals such as iPhones, iPads, and iMac computers provide the CNA function. This function automatically detects the network connection status after iOS terminals connect to WLANs. If the network is disconnected, the iOS terminals display a page prompting users to enter user names and passwords. If users do not enter the user names and passwords, the iOS terminals automatically disconnect from the WLANs. As a result, users cannot use applications on iOS terminals for authentication.

To solve the problem, enable the CNA adaptive function so that iOS terminals are redirected to the application-based Portal authentication page when they connect to WLANs. Users can click the link on the page to start specified applications to perform Portal authentication. If users do not start applications to perform authentication, they can still access authentication-free resources on the WLANs.

Precautions

When applications on iOS mobile terminals are used to perform Portal authentication, you can run only the **portal captive-bypass enable** command to enable the CNA bypass function. After this function is enabled, users who have logged in to the applications can be automatically authenticated and connect to networks, without entering their user names and passwords.

If you run both the **portal captive-adaptive enable** and **portal captive-bypass enable** commands, the command executed later takes effect.

Due to restrictions of iOS 9.3.1, mobile terminals using iOS 9.3.1 cannot connect to WLANs after the CNA adaptive function is enabled. To solve this problem, run the **portal captive-bypass enable** command to enable the CNA bypass function. Terminal users then can be redirected to the application-based Portal authentication page after they open the browser and access a web page.

Authentication-free resources accessed by users cannot contain the URL captive.apple.com; otherwise, terminals cannot automatically display the Portal authentication page.

If the Portal authentication page is of the HTTPS type, terminals can automatically display the Portal authentication page only when an HTTPS URL is used and the domain name certificate is valid.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the CNA adaptive function for iOS terminals.

```
<Huawei> system-view
[Huawei] portal captive-adaptive enable
```

19.6.101 portal captive-bypass enable

Function

The **portal captive-bypass enable** command enables the CNA bypass function for iOS terminals.

The **undo portal captive-bypass enable** command disables the CNA bypass function.

By default, the CNA bypass function is disabled for iOS terminals.

Format

portal captive-bypass enable

undo portal captive-bypass enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The iOS operating system provides the Captive Network Assistant (CNA) function. With the CNA function, the iOS terminals (including iPhone, iPad, and iMAC) automatically detects wireless network connectivity after associating with a wireless network. If the network connection cannot be set up, the iOS terminals ask users to enter user names and passwords. If users do not enter the user names and passwords, the iOS terminals automatically disconnect from the wireless network.

However, Portal authentication allows users to access certain resources before authentication is successful. If the iOS terminals are disconnected, users cannot access the specified resources. The CNA bypass function addresses this problem. If the users do not enter user names and passwords immediately, the CNA bypass function keeps the iOS terminals online before the Portal authentication is successful. Therefore, the iOS users are allowed to access authentication-free resources.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

After the CNA bypass function is enabled for iOS terminals, the Portal authentication page will not be automatically displayed for iOS terminals.

Example

Enable the CNA bypass function for iOS terminals.

```
<Huawei> system-view
[Huawei] portal captive-bypass enable
```

19.6.102 portal https-redirect enable

Function

The **portal https-redirect enable** command enables HTTPS redirection of Portal authentication.

The **undo portal https-redirect enable** command disables HTTPS redirection of Portal authentication.

By default, HTTPS redirection of Portal authentication is disabled.

Format

portal https-redirect enable

undo portal https-redirect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Many well-known websites such as Google and Baidu use Hypertext Transfer Protocol Secure (HTTPS). When users visit these websites, it is required that users should be redirected to the Portal authentication page so that Portal authentication can be performed and the users can normally access the network. If unauthenticated Portal users visit websites using HTTPS after HTTPS redirection of Portal authentication is enabled, the device can redirect the users to the Portal authentication page.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- If Portal authentication is triggered when a user visits a website using HTTPS, the browser displays a security prompt. The user needs to click **Continue** to complete Portal authentication.
- Redirection cannot be performed for browsers or websites using HTTP Strict Transport Security (HSTS).
- If the destination port in HTTPS request packets sent by users is an unknown port (443), redirection cannot be performed.
- This function takes effect only for new Portal authentication users.
- This function takes effect only after the Portal server template is created or the IP address of the built-in Portal server is configured.

Example

Enable HTTPS redirection of Portal authentication.

```
<Huawei> system-view
[Huawei] portal https-redirect enable
```

19.6.103 portal local-server ad-image load

Function

The **portal local-server ad-image load** command loads an advertisement image file to the built-in Portal server login page.

The **undo portal local-server ad-image load** command deletes the advertisement image file loaded to the built-in Portal server login page.

By default, no advertisement image file is loaded to the built-in Portal server login page.

Format

portal local-server ad-image load *ad-image-file*

undo portal local-server ad-image load

Parameters

Parameter	Description	Value
ad-image-file	Specifies the name of an advertisement image file to be loaded to the built-in Portal server login page. The size of the advertisement image file must be equal to or less than 256 KB. A file of 670 x 405 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". ● *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a blank area on the login page of the default page package used by the built-in Portal server. Users can customize this area by loading an advertisement image file. When the login page needs to be customized based on special requirements, the administrator can upload the user-defined advertisement image file to the device and run the **portal local-server ad-image load** command. After the advertisement image file is loaded, the user-defined advertisement images are displayed on the built-in Portal server login page for authentication.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The user-defined advertisement image file has been uploaded to the device.

Example

Load the advertisement image file **ad.png** to the built-in Portal server login page.

```
<Huawei> system-view
[Huawei] portal local-server ad-image load flash:/ad.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.104 portal local-server authentication-method

Function

The **portal local-server authentication-method** command configures the authentication mode for Portal users on the built-in Portal server.

The **undo portal local-server authentication-method** command restores the default authentication mode for Portal users on the built-in Portal server.

By default, the built-in Portal server uses CHAP to authenticate Portal users.

Format

portal local-server authentication-method { **chap** | **pap** }

undo portal local-server authentication-method

Parameters

Parameter	Description	Value
chap	Indicates that the built-in Portal server uses CHAP to authenticate Portal users.	-
pap	Indicates that the built-in Portal server uses PAP to authenticate Portal users.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Password Authentication Protocol (PAP) is a two-way handshake authentication protocol. It transmits passwords in plain text format in RADIUS packets.

Challenge Handshake Authentication Protocol (CHAP) is a three-way handshake authentication protocol. It transmits only user names using RADIUS packets, but does not transmit passwords. CHAP is more secure and reliable than PAP. If high security is required, CHAP is recommended.

Prerequisites

The built-in Portal server function has been enabled globally using the **portal local-server** command.

Example

Configure the built-in Portal server to use PAP to authenticate Portal users.

```
<Huawei> system-view
[Huawei] portal local-server authentication-method pap
```

19.6.105 portal local-server background-color

Function

The **portal local-server background-color** command configures the background color of the built-in Portal server login page.

The **undo portal local-server background-color** command cancels the background color configured for the built-in Portal server login page.

By default, no background color of the built-in Portal server login page is configured.

Format

portal local-server background-color *background-color-value*

undo portal local-server background-color

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
background-color-value	Specifies the background color of the built-in Portal server login page.	The value is a string that ranges from #000000 to #FFFFFF in the RGB format. The hexadecimal code is used to indicate the page color, and the format is always #DEFABC (A-F and 0-9).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users can customize the login page of the default page package used by the built-in Portal server. The administrator can configure the background color of the login page.

Example

Configure the user-defined background color of the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server background-color #AABBCC
```

19.6.106 portal local-server background-image load

Function

The **portal local-server background-image load** command loads a background image file to the built-in Portal server login page.

The **undo portal local-server background-image load** command deletes the background image file loaded to the built-in Portal server login page.

By default, the device has two background images **default-image0** and **default-image1**. The built-in Portal server uses **default-image0** as the background image by default.

Format

portal local-server background-image load { *background-image-file* | **default-image1** }

undo portal local-server background-image load

Parameters

Parameter	Description	Value
background-image-file	Specifies the name of the background image file to be loaded to the built-in Portal server login page. The size of the background image file must be equal to or less than 512 KB. A file of 1366 x 768 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". ● *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.
default-image1	Loads the background image **default-image1** to the built-in Portal server login page.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users can customize the login page of the default page package used by the built-in Portal server. Users can customize background images or select the default ones. When the background image of the login page needs to be customized based on special requirements, the administrator can upload the user-defined background image file to the device and run the **portal local-server background-image load** command. After the image is loaded, the user-defined background image file is displayed on the built-in Portal server login page for authentication.

Prerequisites

The user-defined background image has been uploaded to the device.

Example

Load the background image file **bg.png** to the built-in Portal server login page.

```
<Huawei> system-view
[Huawei] portal local-server background-image load flash:/bg.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

19.6.107 portal local-server enable

Function

The **portal local-server enable** command enables the built-in Portal server function in a Portal access profile.

The **undo portal local-server enable** command restores the default setting.

By default, the built-in Portal server function is disabled in a Portal access profile.

Format

portal local-server enable [**layer3**]

undo portal local-server enable

Parameters

Parameter	Description	Value
layer3	Indicates Layer 3 built-in Portal authentication. If this parameter is not specified, Layer 2 built-in Portal authentication is used.	-

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In Portal authentication, the device needs to provide the IP address of the Portal server. The device supports external and built-in Portal servers. When the built-in Portal server is required to authenticate users, enable the built-in Portal server function globally and then run the **portal local-server enable** command in the Portal access profile. Then the built-in Portal server can be used to authenticate the users who use the Portal access profile.

Portal authentication can work either in Layer 2 or Layer 3 mode.

- In Layer 2 mode, there is no Layer 3 forwarding device between a device and a user. The device can learn the user's MAC address and identify the user using both the user's IP and MAC addresses.
- In Layer 3 mode, there is a Layer 3 forwarding device between a device and a user. The device cannot learn the user's MAC address and has to identify the user using the user's IP address.

Prerequisites

The built-in Portal server function has been enabled globally using the **19.6.112 portal local-server** command.

Example

In the Portal access profile **p1**, enable the built-in Portal server function.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] ip address 10.1.1.1 24
[Huawei-LoopBack1] quit
[Huawei] portal local-server ip 10.1.1.1
[Huawei] ssl policy s1 type server
[Huawei-ssl-policy-s1] pki-realm default
[Huawei-ssl-policy-s1] quit
[Huawei] http secure-server ssl-policy s1
[Huawei] portal local-server https ssl-policy s1
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] portal local-server enable
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.108 portal local-server ip

Function

The **portal local-server ip** command configures an IP address for the built-in Portal server.

The **undo portal local-server ip** command deletes an IP address of the built-in Portal server.

 Copyright © Huawei Technologies Co., Ltd.

By default, no IP address is configured for the built-in Portal server.

Format

portal local-server ip *ip-address*

undo portal local-server ip

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the built-in Portal server.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device is used as a built-in Portal server, you can run the **portal local-server ip** command to configure an IP address for the built-in Portal server. Users are then redirected to the Portal server if they enter URLs that are not located in the free IP subnet.

NOTE

- The IP address assigned to the built-in Portal server must have a reachable route to the user.
- It is recommended that a loopback interface address be assigned to the built-in Portal server because the loopback interface is stable. Additionally, packets destined for loopback interfaces are not sent to other interfaces on the network; therefore, system performance is not deteriorated even if many users request to go online.
- After users go online through the built-in Portal server, if the interface address or interface (non-physical interface) matching the built-in Portal server's IP address is deleted, online users cannot go offline and offline users cannot go online. Therefore, exercise caution when you delete the interface address or interface.

Example

Assign the IP address 10.1.1.1 to the built-in Portal server.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] ip address 10.1.1.1 24
[Huawei-LoopBack1] quit
[Huawei] portal local-server ip 10.1.1.1
```

19.6.109 portal local-server keep-alive

Function

The **portal local-server keep-alive** command configures the heartbeat detection interval and mode of the built-in Portal server.

The **undo portal local-server keep-alive** command cancels the configured heartbeat detection interval and mode of the built-in Portal server.

By default, the heartbeat detection function of the built-in Portal server is not configured.

Format

portal local-server keep-alive interval *interval-value* [**auto**]

undo portal local-server keep-alive

Parameters

Parameter	Description	Value
interval *interval-value*	Specifies the heartbeat detection interval of the built-in Portal server.	The value is an integer that ranges from 30 to 7200, in seconds.
auto	Specifies the automatic detection mode. If this parameter is not configured, the forcible detection mode is specified.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a user closes the browser or an exception occurs, the device can detect the user's online state to determine whether to make the user go offline. The administrator can configure the heartbeat detection function of the built-in Portal server. If the device does not receive a heartbeat packet from the client within a specified period, the user is specified to go offline. The heartbeat detection mode of the built-in Portal server can be either of the following modes:

 Copyright © Huawei Technologies Co., Ltd.

- Forcible detection mode: This mode is valid for all users. If the device does not receive a heartbeat packet from a user within a specified period, the device specifies the user to go offline.
- Automatic detection mode: The device checks whether the client browser supports the heartbeat program. If yes, the forcible detection mode is used for the user; if no, the device does not detect the user. You are advised to configure this mode to prevent users from going offline because the browser does not support the heartbeat program.

  NOTE

  Currently, the heartbeat program is supported by Internet Explorer 8, FireFox 3.5.2, Chrome 28.0.1500.72, and Opera 12.00 on Windows 7. A Java program must be installed and configured on the operating system.

  Browsers using Java1.7 and later versions do not support the heartbeat program.

Precautions

When the forcible detection mode is configured, the device specifies users to go offline to prevent from failing to receive heartbeat packets for a long time during network congestion. In this scenario, the heartbeat detection interval must be increased.

If you run this command multiple times in the same view, only the latest configuration takes effect.

Example

Configure the automatic detection function of the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server keep-alive interval 60 auto
```

19.6.110 portal local-server load

Function

The **portal local-server load** command loads a page file package to the built-in Portal server.

The **undo portal local-server load** command restores the default configuration.

By default, the built-in Portal server loads the default page file package **portalpage.zip**.

Format

portal local-server load *string*

undo portal local-server load

Parameters

Parameter	Description	Value
string	Specifies the name of the page file package to be loaded to the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". ● *filename*: indicates the file name. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Customized page file packages can be loaded to the built-in Portal server.

Prerequisites

The page file (.zip) has been uploaded from the PC to the device storage media.

Precautions

The default page file package can be modified but cannot be deleted. If it is deleted, the built-in Portal server fails to load the pages after startup.

This function is used by technical support personnel to develop limited page customization based on customer requirements and does not apply to customization by customers themselves.

 Copyright © Huawei Technologies Co., Ltd.

Example

Load the page file **portalpage_01.zip** on the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server load portalpage_01.zip
Warning: Portal local server has been enabled, and this operation will affect online user, continue?[Y/N]:y
```

Related Topics

19.6.44 display portal local-server page-information

19.6.43 display portal local-server

19.6.111 portal local-server logo load

Function

The **portal local-server logo load** command loads a logo file to the built-in Portal server login page.

The **undo portal local-server logo load** command deletes the logo file loaded to the built-in Portal server login page.

By default, no logo file is loaded to the built-in Portal server login page.

Format

portal local-server logo load *logo-file*

undo portal local-server logo load

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
logo-file	Specifies the name of the logo file to be loaded to the built-in Portal server login page. The size of the logo file must be equal to or less than 128 KB. A file of 591 x 80 pixels is recommended.	The value is a string of 5 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". ● *filename*: indicates the file name. The jpg and png formats are supported, and the file name extension must be .jpg, .jpeg, or .png. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a blank area on the login page of the default page package used by the built-in Portal server. Users can customize this area by loading a logo file. When the login page needs to be customized based on special requirements, the administrator can upload the user-defined logo file to the device and run the **portal local-server logo load** command. After the logo file is loaded, the user-defined logo is displayed on the built-in Portal server login page for authentication.

Prerequisites

The user-defined logo file has been uploaded to the device.

Example

Load the logo file **logo.png** to the built-in Portal server login page.

```
<Huawei> system-view
[Huawei] portal local-server logo load flash:/logo.png
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.112 portal local-server

Function

The **portal local-server** command enables the built-in Portal server function.

The **undo portal local-server** command disables the built-in Portal server function.

By default, the built-in Portal server function is disabled.

Format

portal local-server https ssl-policy *policy-name* [**port** *port-num*]

undo portal local-server https

Parameters

Parameter	Description	Value
https	Configures the built-in Portal server to exchange authentication messages with users using the Hypertext Transfer Protocol Secure (HTTPS) protocol.	-
ssl-policy *policy-name*	Specifies the Secure Sockets Layer (SSL) policy used by the built-in Portal server.	The value must be the name of an existing SSL policy.
port *port-num*	Specifies the TCP port number used. If you do not specify a port number, the default port number is used.	The value can be 443 or any integer in the range of 1025 to 55535. By default, the port number is 443.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Compared with an external Portal server, a built-in Portal server is easy to use, cost-effective, and easy to maintain. After a built-in Portal server is configured, Portal authentication can be implemented for users without an external Portal server. When using the **portal local-server** command to enable the built-in Portal server function, configure the built-in Portal server to exchange authentication messages with users using the HTTPS protocol. HTTPS is a secure extension of HTTP and uses the SSL protocol to guarantee secure communication. To enable the built-in Portal server to exchange authentication messages using HTTPS, you need to configure an SSL policy and load a digital certificate to the server.

Prerequisites

- The IP address of the built-in Portal server has been configured using the **19.6.108 portal local-server ip** command.
- An SSL policy has been configured using the **ssl policy** *policy-name* command in the system view
- A server SSL policy has been configured and associated with the HTTPS server using the **19.19.4 http secure-server ssl-policy** command.
- You have obtained a digital certificate for the SSL policy from an authorized certificate authority.

Precautions

When there are Portal authentication users online, you cannot disable the built-in Portal server function or change the SSL policy for the built-in Portal server.

Example

Enable the built-in Portal server function and configure the server to use the SSL policy **s1**.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] ip address 10.1.1.1 24
[Huawei-LoopBack1] quit
[Huawei] portal local-server ip 10.1.1.1
[Huawei] ssl policy s1 type server
[Huawei-ssl-policy-s1] pki-realm default
[Huawei-ssl-policy-s1] quit
[Huawei] http secure-server ssl-policy s1
[Huawei] portal local-server https ssl-policy s1
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.113 portal local-server page-text load

Function

The **portal local-server page-text load** command loads the use instruction page file of the built-in Portal server.

The **undo portal local-server page-text load** command deletes the loaded use instruction page file of the built-in Portal server.

By default, no use instruction page file of the built-in Portal server is loaded.

Format

portal local-server page-text load *string*

undo portal local-server page-text load

Parameters

Parameter	Description	Value
string	Specifies the use instruction page file of the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [drive] [path] filename. ● **drive** indicates the storage device name. ● **path** indicates the directory or sub-directory. The directory name cannot contain the following characters: ~ * / \ : ' " ● **filename** indicates the file name. The file name extension must be .txt or .html. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you need to customize the use instruction page, you can upload the customized use instruction page file to the device, and run this command to load the file. After the file is loaded, the hyperlink **Instruction for Use** is generated on the login page of the built-in Portal server, and users can click the hyperlink to access the use instruction page.

Prerequisite

The page file to be loaded has been uploaded to the device.

Precautions

When the to-be-loaded page is customized, the page length and width are fixed. After adjusting the page, the administrator must upload and load the modified page again.

Currently, only Chinese or English page files can be loaded on the device.

Example

Load the use instruction page file **page.html** to the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server page-text load flash:/page.html
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.114 portal local-server policy-text load

Function

The **portal local-server policy-text load** command loads a disclaimer page file to the built-in Portal server.

The **undo portal local-server policy-text load** command deletes the loaded disclaimer page file.

By default, no disclaimer page file is loaded to the built-in Portal server.

Format

portal local-server policy-text load *string*

undo portal local-server policy-text load

Parameters

Parameter	Description	Value
string	Specifies the name of the disclaimer page file to be loaded to the built-in Portal server.	The value is a string of 1 to 64 case-insensitive characters without spaces, in the format of [*drive*] [*path*] *filename*. ● *drive*: indicates the storage device name. ● *path*: indicates the directory and its subdirectory. The directory name cannot contain the following characters: ~, *, /, \, :, ', and ". ● *filename*: indicates the file name. The file name extension must be .txt or .html. If you enter only the file name, the system considers that the file is stored in the default directory.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To customize a disclaimer page, upload the disclaimer page file to the device and run this command to load the file. After the file is loaded, the hyperlink **Disclaimer** will be displayed on the login page. You can click the link to visit the disclaimer page.

Prerequisite

The disclaimer page file to be loaded has been uploaded to the device.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Currently, only Chinese and English disclaimer page files can be loaded on the device.

Example

Load the disclaimer page file **policy.html** to the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server policy-text load policy.html
Info: The loading process may take a few seconds.Please wait for a moment.
Info: Load web file successfully.
```

Related Topics

19.6.43 display portal local-server

19.6.115 portal local-server syslog-limit enable

Function

The **portal local-server syslog-limit enable** command enables the log suppression function for users authenticated through the built-in Portal server.

The **undo portal local-server syslog-limit enable** command disables the log suppression function for users authenticated through the built-in Portal server.

By default, the log suppression function is enabled for users authenticated through the built-in Portal server.

Format

portal local-server syslog-limit enable

undo portal local-server syslog-limit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device generates logs when users authenticated through the built-in Portal server fail to go online or offline. If a user fails to go online or offline, the user attempts to go online or offline repeatedly, and the device generates a large number of logs within a short time. This results in a high failure rate in the statistics and degrades the system performance. You can run the **portal local-server syslog-limit enable** command to enable the log suppression function for

users authenticated through the built-in Portal server. The device then only generates one log if a user fails to go online or offline within a suppression period (configured using the **19.6.116 portal local-server syslog-limit period** command).

Example

Enable the log suppression function for users authenticated through the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server syslog-limit enable
```

19.6.116 portal local-server syslog-limit period

Function

The **portal local-server syslog-limit period** command configures the log suppression period for users authenticated through the built-in Portal server.

The **undo portal local-server syslog-limit period** command restores the default log suppression period.

By default, the log suppression period is 300 seconds for users authenticated through the built-in Portal server.

Format

portal local-server syslog-limit period *value*

undo portal local-server syslog-limit period

Parameters

Parameter	Description	Value
value	Specifies the log suppression period for users authenticated through the built-in Portal server.	The value is an integer that ranges from 60 to 604800, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The device generates logs when users authenticated through the built-in Portal server fail to go online or offline. If a user fails to go online or offline, the user

attempts to go online or offline repeatedly, and the device generates a large number of logs within a short time. This results in a high failure rate in the statistics and degrades the system performance. You can enable the log suppression function (configured using the **19.6.115 portal local-server syslog-limit enable** command) for users authenticated through the built-in Portal server. The device then only generates one log if a user fails to go online or offline within a suppression period.

Example

Set the log suppression period to 1000 seconds for users authenticated through the built-in Portal server.

```
<Huawei> system-view
[Huawei] portal local-server syslog-limit period 1000
```

19.6.117 portal local-server timer session-timeout

Function

The **portal local-server timer session-timeout** command configures the session timeout interval for built-in Portal authentication users.

The **undo portal local-server timer session-timeout** command restores the default session timeout interval for built-in Portal authentication users.

By default, the session timeout interval is 8 hours for built-in Portal authentication users.

Format

portal local-server timer session-timeout *interval*

undo portal local-server timer session-timeout

Parameters

Parameter	Description	Value
interval	Specifies the session timeout interval for built-in Portal authentication users.	The value is an integer that ranges from 1 to 720, in hours.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Scenario

When built-in Portal authentication is used for users and the device functions as a built-in Portal server, you can configure the session timeout interval for the users. The users are disconnected after the specified session timeout interval. To connect to the network again, the users need to be re-authenticated.

Precautions

The session timeout interval for built-in Portal authentication users is calculated based on the device time. For example, if the session timeout interval is 6 hours and the device time is 2014-09-01 02:00:00 when a user was connected, the user should be disconnected at 2014-09-01 08:00:00. Therefore, ensure that the device time and time zone are correct after the session timeout interval is configured for users. If the device time is incorrect, users may fail to be connected or disconnected properly. You can run the **display clock** command to check the device time and the time zone.

Example

Set the session timeout interval to 10 hours for built-in Portal authentication users.

```
<Huawei> system-view
[Huawei] portal local-server timer session-timeout 10
```

Related Topics

19.6.43 display portal local-server

19.6.118 portal logout different-server enable

Function

The **portal logout different-server enable** command configures a device to process user logout requests sent by a Portal server other than the one from which users log in.

The **undo portal logout different-server enable** command restores the default configuration.

By default, a device does not process user logout requests sent by Portal servers other than the one from which users log in.

Format

portal logout different-server enable

undo portal logout different-server enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In a scenario where Portal server load balancing is configured, by default, a device does not process user logout requests sent by Portal servers other than the one from which users log in and responds ACK messages only to the Portal server from which users log in. Users in arrears then can still stay online. To prevent this problem, run **portal logout different-server enable** command to configure the device to process user logout requests sent by a Portal server other than the one from which users log in. Upon receipt of a user logout request from such a Portal server, the device starts a user logout process. After completing the logout event, the device responds an ACK message to the Portal server, thereby ensuring that the user logs out properly.

Precautions

The user logout requests that a device can process must be sent by Portal servers bound to an access interface. These servers include all the Portal servers configured in the master and backup Portal server templates bound to the interface.

Example

Enable a device to process user logout requests a Portal server other than the one from which users log in.

```
<Huawei> system-view
[Huawei] portal logout different-server enable
```

Related Topics

19.6.41 display portal

19.6.119 portal logout resend timeout

Function

The **portal logout resend timeout** command configures the re-transmission times and interval for the Portal authentication user logout packet.

The **undo portal logout resend timeout** command restores the default setting.

By default, the Portal authentication user logout packet can be re-transmitted three times within five seconds.

Format

portal logout resend *times* **timeout** *period*

undo portal logout { **resend** | **timeout** } *

Parameters

Parameter	Description	Value
times	Specifies the number of re-transmission times for the Portal authentication user logout packet.	The value is an integer that ranges from 0 to 15. The value 0 indicates that the re-transmission function is disabled.
period	Specifies the re-transmission interval of the Portal authentication user logout packet.	The value is an integer that ranges from 1 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After disconnecting a Portal authentication user, the device sends a user logout packet (NTF-LOGOUT) to instruct the Portal server to delete the user information. If the network between the device and Portal server is not stable or packets are lost, the Portal server may fail to receive the user logout packet from the device after the Portal authentication user is disconnected. In this case, the user is displayed as disconnected on the device but still as online on the Portal server. To enable the Portal server to receive the user logout packet and ensure that the online user information on the Portal server is correct, the administrator can enable the user logout packet re-transmission function on the device and configure the re-transmission times and interval.

Example

Configure the re-transmission times to 5 and interval to 10 seconds for the Portal authentication user logout packet.

```
<Huawei> system-view
[Huawei] portal logout resend 5 timeout 10
```

Related Topics

19.6.41 display portal
19.6.48 display portal user-logout

19.6.120 portal max-user

Function

The **portal max-user** command sets the maximum number of concurrent Portal authentication users allowed to access the device.

The **undo portal max-user** command restores the default maximum number of concurrent Portal authentication users.

By default, the number of Portal authentication users is the maximum number of Portal authentication users supported by the device.

Format

portal max-user *user-number*

undo portal max-user

Parameters

Parameter	Description	Value
user-number	Specifies the maximum number of concurrent Portal users.	The value is an integer that varies depending on product models.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can run the **portal max-user** command to set the maximum number of concurrent Portal authentication users.

Example

Set the maximum number of concurrent Portal authentication users to 25.

```
<Huawei> system-view
[Huawei] portal max-user 25
```

19.6.121 portal quiet-period

Function

The **portal quiet-period** command enables the quiet timer for Portal authentication.

The **undo portal quiet-period** command disables the quiet timer of Portal authentication.

By default, the quiet timer for Portal authentication is enabled.

Format

portal quiet-period

undo portal quiet-period

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **portal quiet-period** command is used to enable the quiet timer for Portal authentication. If the number of Portal authentication failures exceeds the value specified by the **19.6.122 portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. During the quiet period, the device discards Portal authentication requests from the user. This prevents the impact of frequent authentications on the system.

The quiet period for Portal authentication can be set using the **19.6.123 portal timer quiet-period** command. After the quiet period is reached, the device re-authenticates the user.

Example

Enable the quiet timer for Portal authentication.

```
<Huawei> system-view
[Huawei] portal quiet-period
```

19.6.122 portal quiet-times

Function

The **portal quiet-times** command sets the maximum number of authentication failures within 60s before a Portal authentication user is kept in quiet state.

The **undo portal quiet-times** command restores the default maximum number of authentication failures within 60s before a Portal authentication user enters the quiet state.

By default, the device allows a maximum of ten authentication failures within 60s before a Portal authentication user enters the quiet state.

 Copyright © Huawei Technologies Co., Ltd.

Format

portal quiet-times *fail-times*

undo portal quiet-times

Parameters

Parameter	Description	Value
fail-times	Specifies the maximum number of authentication failures before a Portal authentication user enters the quiet state.	The value is an integer that ranges from 1 to 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **19.6.121 portal quiet-period** command is used to enable the quiet timer, if the number of Portal authentication failures exceeds the value specified by the **portal quiet-times** command, the device keeps the Portal authentication user in quiet state for a period of time. This prevents the impact of frequent authentications on the system.

Example

Set the maximum number of Portal authentication failures within 60 seconds to 4.

```
<Huawei> system-view
[Huawei] portal quiet-times 4
```

19.6.123 portal timer quiet-period

Function

The **portal timer quiet-period** command configures the quiet period for Portal authentication users who fail to be authenticated.

The **undo portal timer quiet-period** command restores the default quiet period.

By default, the quiet period is 60 seconds for Portal authentication users who fail to be authenticated.

 Copyright © Huawei Technologies Co., Ltd.

Format

portal timer quiet-period *quiet-period-value*

undo portal timer quiet-period

Parameters

Parameter	Description	Value
quiet-period-value	Sets the quiet period for Portal authentication users who fail to be authenticated.	The value is an integer that ranges from 10 to 3600, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If a Portal authentication user fails to be authenticated consecutively within a short period, the system is affected and a large number of duplicated authentication failure logs are generated.

After the quiet function is enabled using the **19.6.121 portal quiet-period** command, if the number of times that a Portal authentication user fails to be authenticated within 60s exceeds the upper limit (configured using the **19.6.122 portal quiet-times** command), the device discards the user's Portal authentication request packets for a period to avoid frequent authentication failures.

Example

Set the quiet period to 100 seconds for Portal authentication users who fail to be authenticated.

```
<Huawei> system-view
[Huawei] portal timer quiet-period 100
```

19.6.124 portal timer offline-detect

Function

The **portal timer offline-detect** command sets the Portal user offline detection interval.

The **undo portal timer offline-detect** command restores the default Portal user offline detection interval.

By default, the Portal user offline detection interval is 300 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

portal timer offline-detect *time-length*

undo portal timer offline-detect

Parameters

Parameter	Description	Value
time-length	Specifies the Portal user offline detection interval.	The value is 0 or an integer that ranges from 30 to 7200, in seconds. The default value is 300. The value 0 indicates that offline detection is not performed.

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a Portal user goes offline due to power failure or network interruption, the device and Portal server may still store the user information, which causes incorrect accounting. Additionally, a limit number of users can access the device. If a user goes offline improperly but the device still stores user information, other users cannot access the network.

After the Portal user offline detection interval is set, if the user does not respond within the interval, the device considers the Portal user offline. The device and Portal server then delete the user information and release resources to ensure an efficient resource use.

Precautions

This command only applies to Layer 2 Portal authentication.

The heartbeat detection function of the authentication server can be used to ensure the normal online status of PC users for whom Layer 3 Portal authentication is used. If the authentication server detects that a user goes offline, it instructs the device to disconnect the user.

Example

In the Portal access profile **p1**, set the offline detection interval of Portal authentication users to 400s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] portal timer offline-detect 400
```

19.6.125 portal user-alarm percentage

Function

The **portal user-alarm percentage** command sets alarm thresholds for the Portal authentication user count percentage.

The **undo portal user-alarm percentage** command restores the default alarm thresholds for the Portal authentication user count percentage.

By default, the lower alarm threshold for the Portal authentication user count percentage is 50, and the upper alarm threshold for the Portal authentication user count percentage is 100.

Format

portal user-alarm percentage *percent-lower-value percent-upper-value*

undo portal user-alarm percentage

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the Portal authentication user count percentage.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After running the **19.6.120 portal max-user** command to set the maximum number of online Portal authentication users allowed on a device, you can run the **portal user-alarm percentage** command to set alarm thresholds for the Portal authentication user count percentage.

 Copyright © Huawei Technologies Co., Ltd.

When the percentage of online Portal authentication users against the maximum number of users allowed by the device exceeds the upper alarm threshold, the device generates an alarm. When the percentage of online Portal authentication users against the maximum number of users allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

If the configured upper alarm threshold for the Portal authentication user count percentage is 100, the device generates an alarm when the number of online users reaches the maximum number of users allowed by the device.

Example

Set the lower alarm threshold for the Portal authentication user count percentage to 30, and the upper alarm threshold for the Portal authentication user count percentage to 80.

```
<Huawei> system-view
[Huawei] portal user-alarm percentage 30 80
```

Related Topics

19.6.120 portal max-user

19.6.126 portal web-authen-server

Function

The **portal web-authen-server** command enables the Portal interconnection function of the HTTP or HTTPS protocol.

The **undo portal web-authen-server** command disables the Portal interconnection function of the HTTP or HTTPS protocol.

By default, the Portal interconnection function of the HTTP or HTTPS protocol is disabled.

Format

portal web-authen-server { **http** | **https ssl-policy** *policy-name* } [**port** *port-number*]

undo portal web-authen-server

Parameters

Parameter	Description	Value
http	Sets the HTTP protocol for Portal authentication. **NOTE** The HTTP protocol poses security risks. The HTTPS protocol is recommended.	-

Parameter	Description	Value
https	Sets the HTTPS protocol for Portal authentication.	-
ssl-policy *policy-name*	Specifies the name of an SSL policy.	The value must be the name of an existing SSL policy.
port *port-number*	Specifies a port number.	The default HTTP port number is 8000 and the default HTTPS port number is 8443.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the device is connected to the Portal server that only supports the HTTP or HTTPS protocol, you need to run the **portal web-authen-server** command on the device to enable the Portal interconnection function of the HTTP or HTTPS protocol.

Follow-up Procedure

Run the **19.6.127 protocol** command to set the protocol used in Portal authentication to HTTP or HTTPS.

Precautions

Modifying the **port** parameter causes the pre-connected user to go offline.

Example

Enable the Portal interconnection function of the HTTPS protocol.

```
<Huawei> system-view
[Huawei] ssl policy huawei type server
[Huawei-ssl-policy-huawei] quit
[Huawei] http secure-server ssl-policy huawei
[Huawei] portal web-authen-server https ssl-policy huawei port 8443
```

Related Topics

19.6.52 display web-auth-server configuration

 Copyright © Huawei Technologies Co., Ltd.

19.6.127 protocol

Function

The **protocol** command configures the protocol used in Portal authentication.

The **undo protocol** command restores the default configuration.

By default, the Portal protocol is used in Portal authentication.

Format

protocol { **http** [**password-encrypt** { **none** | **uam** }] | **portal** | **haca** }

undo protocol

Parameters

Parameter	Description	Value
http	Sets the protocol used in Portal authentication to HTTP or HTTPS.	-
password-encrypt { **none** | **uam** }	Specifies the password encoding mode. ● **none**: The password is not encoded. ● **uam**: The password is encoded using ASCII characters.	-
portal	Sets the protocol used in Portal authentication to Portal.	-
haca	Sets the protocol used in Portal authentication to HACA.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

In Portal authentication, the device can use the following protocols to communicate with the Portal server. You can set the protocol according to the protocol supported by the Portal server.

 Copyright © Huawei Technologies Co., Ltd.

- HACA protocol
- Portal protocol
- HTTP or HTTPS protocol

The HACA protocol used in Portal authentication has impacts on other command configurations.

- After the HACA protocol is configured, the following command configurations will not be supported:
  - Run the **19.6.98 port (Portal server profile view)** command to configure a destination port number for the device to send packets to the Portal server.
  - Run the **19.6.135 server-detect** command to enable the Portal server detection function.
  - Run the **19.6.137 shared-key (Portal server profile view)** command to configure a shared key used by the device and Portal server to exchange information.
  - Run the **19.6.139 source-ip (Portal server profile view)** command to configure a source IP address for the device to communicate with the Portal server.
  - Run the **19.6.149 user-sync** command to enable Portal user information synchronization.
  - Run the **19.6.153 vpn-instance (Portal server template view)** command to configure a VPN instance for the device to communicate with the Portal server.

  If any one of the preceding configurations is performed beforehand, the HACA protocol configuration will not take effect.
- After the HACA protocol is configured, you can run the **19.6.136 server-ip (Portal server profile view)** command to configure an IP address for the Portal server. However, if multiple Portal server IP addresses are configured, the HACA protocol configuration will not take effect.

Example

Set the protocol used in Portal authentication to HACA.

```
<Huawei> system-view
[Huawei] web-auth-server abc
[Huawei-web-auth-server-abc] protocol haca
```

19.6.128 portal url-encode enable

Function

The **portal url-encode enable** command enables URL encoding and decoding.

The **undo portal url-encode enable** command disables URL encoding and decoding.

By default, URL encoding and decoding are enabled.

Format

portal url-encode enable

undo portal url-encode enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To improve web application security, data from untrustworthy sources must be encoded before being sent to clients. URL encoding is most commonly used in web applications. To enable URL encoding and decoding, run the **portal url-encode enable** command. Some special characters in redirected URLs are then converted to secure formats, preventing clients from mistaking them for syntax signs or instructions and unexpectedly modifying the original syntax. In this way, cross-site scripting attacks and injection attacks are prevented.

Precautions

After the URL encoding and decoding function is enabled, some servers may not support the escape characters converted from special characters in redirect URLs. Therefore, check whether servers support the escape characters before configuring special characters in redirect URLs.

Example

Enable URL encoding and decoding.

```
<Huawei> system-view
[Huawei] portal url-encode enable
```

Related Topics

19.6.47 display portal url-encode configuration

19.6.129 portal-access-profile (authentication profile view)

Function

The **portal-access-profile** command binds a Portal access profile to an authentication profile.

The **undo portal-access-profile** command unbinds a Portal access profile from an authentication profile.

By default, an authentication profile is not bound to a Portal access profile.

Format

portal-access-profile *access-profile-name*

undo portal-access-profile

Parameters

Parameter	Description	Value
access-profile-name	Specifies the name of a Portal access profile.	The value must be the name of an existing Portal access profile.

Views

Authentication profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The authentication type used by an authentication profile is determined by the access profile bound to the authentication profile. After being bound to a Portal access profile, the authentication profile is enabled with Portal authentication. After the authentication profile is applied to the interface or VAP profile, Portal authentication can be performed on online users.

Prerequisites

The Portal server has been configured for the Portal access profile:

- If the external Portal server is used, the Portal server profile used by the Portal access profile has been configured using the **19.6.155 web-auth-server (Portal access profile view)** command.
- If the built-in Portal server is used, the built-in Portal server function of the Portal access profile has been enabled using the **19.6.107 portal local-server enable** command.

Follow-up Procedure

Run the **19.6.26 authentication-profile (Interface view or VAP profile view)** command to apply the authentication profile to the interface or VAP profile.

Precautions

An authentication profile can be bound to only one Portal access profile.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind the authentication profile **portal_authen_profile1** to the Portal access profile **portal_access_profile1**. The IP address of the Portal server is 192.168.10.1, and Layer 2 Portal authentication is used.

```
<Huawei> system-view
[Huawei] web-auth-server server1
[Huawei-web-auth-server-server1] server-ip 192.168.10.1
[Huawei-web-auth-server-server1] quit
[Huawei] portal-access-profile name portal_access_profile1
[Huawei-portal-acces-profile-portal_access_profile1] web-auth-server server1 direct
[Huawei-portal-acces-profile-portal_access_profile1] quit
[Huawei] authentication-profile name portal_authen_profile1
[Huawei-authen-profile-portal_authen_profile1] portal-access-profile portal_access_profile1
```

Related Topics

19.6.31 display authentication-profile configuration

19.6.130 portal-access-profile (system view)

Function

The **portal-access-profile** command creates a portal access profile and displays the portal access profile view.

The **undo portal-access-profile** command deletes the portal access profile.

By default, the device has a built-in portal access profile named **portal_access_profile**.

Format

portal-access-profile name *access-profile-name*

undo portal-access-profile name *access-profile-name*

Parameters

Parameter	Description	Value
name *access-profile-name*	Specifies the name of a portal access profile.	The value is a string of 1-31 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses portal access profiles to uniformly manage all portal users access configurations. To perform portal authentication for the users in an interface or VAP profile, bind the authentication profile applied to the interface or VAP profile to a portal access profile.

Follow-up Procedure

Configure the portal server used by the portal access profile:

- If the external portal server is used, run the **19.6.155 web-auth-server (Portal access profile view)** command to configure the portal server profile for the portal access profile.
- If the built-in portal server is used, run the **19.6.107 portal local-server enable** command to configure the built-in portal server function for the portal access profile.

Precautions

- The device supports a maximum of 8 configurable portal access profiles. The compatibility profile converted after an upgrade is not counted in the configuration specification. The built-in portal access profile **portal_access_profile** can be modified and applied, but cannot be deleted.
- Before deleting a portal access profile, ensure that this profile is not bound to any authentication profile.

Example

Create portal access profile named **portal_access_profile1**.

```
<Huawei> system-view
[Huawei] portal-access-profile name portal_access_profile1
```

Related Topics

19.6.45 display portal-access-profile configuration

19.6.131 redirect web-authentication-user

Function

The **redirect web-authentication-user** command enables the device to redirect Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected.

The **undo redirect web-authentication-user** command disables the device from redirecting Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected.

By default, the device does not redirect Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected.

Format

redirect web-authentication-user url *url-string*

undo redirect web-authentication-user

Parameters

Parameter	Description	Value
url *url-string*	Specifies the URL address of a built-in Portal server. A URL identifies the Portal server's website that Portal authentication users can access. A URL is easier to remember than an IP address.	The value is a string of 1 to 200 case-sensitive characters without spaces and question marks (?). If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

Cellular interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When routers are deployed as mobile Internet gateways on buses and subways, users can connect to the vehicle-mounted Wi-Fi network and access the Internet through the 3G/LTE interfaces after they pass Portal authentication. If 3G/LTE links are disconnected, users cannot access any page, degrading user experiences.

You can run the **redirect web-authentication-user** command on 3G/LTE interfaces to enable the device to redirect Portal authentication users to the built-in Portal server after 3G/LTE links are disconnected. In this way, users can access server resources, improving user experience.

Precautions

- The **redirect web-authentication-user** and **cut web-authentication-user** commands cannot be configured simultaneously on the same interface. It is recommended that either **redirect web-authentication-user** or **cut web-authentication-user** be configured on different interfaces of the same device.

 Copyright © Huawei Technologies Co., Ltd.

- If the **redirect web-authentication-user** command is configured on multiple cellular interfaces, ensure that the URLs configured on these interfaces are the same.
- After all 3G/LTE uplinks are disconnected, the device redirects Portal authentication users to the built-in Portal server.

Example

Redirect Portal authentication users to the built-in Portal server with the URL http://192.168.10.1 after 3G/LTE links are disconnected.

```
<Huawei> system-view
[Huawei] interface cellular 0/0/0
[Huawei-Cellular0/0/0] redirect web-authentication-user url http://192.168.10.1
```

Related Topics

19.6.28 cut web-authentication-user

19.6.132 remark

Function

The **remark** command configures the user group priority.

The **undo remark** command cancels the user group priority configuration.

By default, no user group priority is configured.

Format

remark { **8021p** *8021p-value* | **dscp** *dscp-value* | **exp** *exp-value* | **lp** *lp-value* } *

undo remark { **8021p** *8021p-value* | **dscp** *dscp-value* | **exp** *exp-value* | **lp** *lp-value* } *

Parameters

Parameter	Description	Value
8021p *8021p-value*	Specifies the priority for processing Layer 2 Ethernet packets.	The value is an integer that ranges from 0 to 7.
dscp *dscp-value*	Specifies the priority for processing IP packets.	The value is an integer that ranges from 0 to 63.
exp *exp-value*	Specifies the priority for processing MPLS packets.	The value is an integer that ranges from 0 to 7.
lp *lp-value*	Specifies the priority for processing internal packets in the device.	The value is an integer that ranges from 0 to 7.

 Copyright © Huawei Technologies Co., Ltd.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

After the user group priority is configured, users in the user group inherit the priority. That is, different user packets have different priorities. In this way, the administrator can manage different types of users more flexibly.

NOTE

When an AR router is connected to Fit APs, the user group priority configuration does not take effect for users who go online from the Fit APs.

Example

Set the priority for processing IP packets to 3 in the user group **abc**.

```
<Huawei> system-view
[Huawei] user-group abc
[Huawei-user-group-abc] remark dscp 3
```

Related Topics

19.6.150 user-group

19.6.133 reset dot1x statistics

Function

The **reset dot1x statistics** command clears 802.1X authentication statistics.

Format

reset dot1x statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-5>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears 802.1X authentication statistics on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If this parameter is not specified, 802.1X authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The 802.1X authentication statistics contain the number of times that the authentication succeeded and failed and the number of sent and received packets.

The **reset dot1x statistics** command is used in the following scenarios:

- Redeploy services. After the statistics are cleared, collect the 802.1X authentication statistics again, and run the **19.6.32 display dot1x** command to check whether the authentication function works properly and whether packets are correctly sent and received.
- Rectify a fault. After the fault is rectified, run the **reset dot1x statistics** command to clear the statistics, collect the statistics on 802.1X authentication again, and then run the **19.6.32 display dot1x** command to verify the authentication result and check whether packets are correctly sent and received. If the authentication is successful and packets are correctly sent and received, the fault is rectified.

Example

Clear 802.1X authentication statistics.

```
<Huawei> reset dot1x statistics
```

Related Topics

19.6.32 display dot1x

19.6.134 reset mac-authen statistics

Function

The **reset mac-authen statistics** command clears MAC address authentication statistics.

Format

reset mac-authen statistics [**interface** { *interface-type interface-number1* [**to** *interface-number2*] } &<1-10>]

Parameters

Parameter	Description	Value
interface { *interface-type interface-number1* [**to** *interface-number2*] }	Clears MAC address authentication statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If this parameter is not specified, MAC address authentication statistics on the device are cleared.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

The **reset mac-authen statistics** command is used in the following scenarios:

- Re-deploy services. After the statistics are cleared, collect the MAC address authentication statistics again, and run the **19.6.39 display mac-authen** command to check whether the authentication function is normal.

 Copyright © Huawei Technologies Co., Ltd.

- Rectify a fault. After the fault is rectified, run the **reset mac-authen statistics** command to clear statistics, collect MAC address authentication statistics again, and run the **19.6.39 display mac-authen** command to check the authentication result. If the authentication is successful, the fault is rectified.

Example

Clear MAC address authentication statistics.

```
<Huawei> reset mac-authen statistics
```

Related Topics

19.6.39 display mac-authen

19.6.135 server-detect

Function

The **server-detect** command enables the Portal server detection function.

The **undo server-detect** command disables the Portal server detection function.

By default, the Portal server detection function is disabled.

Format

server-detect [**interval** *interval-period* | **max-times** *times* | **critical-num** *critical-num* | **action** { **log** | **trap** } *] *

undo server-detect [**interval** | **max-times** | **critical-num** | **action** { **log** | **trap** } *]

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the detection interval of the Portal server.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 60.
max-times *times*	Specifies the maximum number of times that the detection fails.	The value is an integer that ranges from 1 to 255. The default value is 3.
critical-num *critical-num*	Specifies the minimum number of Portal servers in Up state.	The value is an integer that ranges from 0 to 16. The default value is 0. The default value is recommended.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
action	Specifies the action to be taken after the number of detection failures exceeds the maximum.	-
log	Indicates that the device sends a log after the number of detection failures exceeds the maximum.	-
trap	Indicates that the device sends a trap after the number of detection failures exceeds the maximum.	-

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

If the communication is interrupted because the network between the device and Portal server is faulty or the Portal server is faulty, new Portal authentication users cannot go online. This brings great inconvenience to users.

After the Portal server detection function is enabled in the Portal server profile, the device detects all Portal servers configured in the Portal server profile. If the number of times that the device fails to detect a Portal server exceeds the upper limit, the status of the Portal server is changed from Up to Down. If the number of Portal servers in Up state is less than or equal to the minimum number (specified by the **critical-num** parameter), the device performs the corresponding operation to allow the administrator to obtain the real-time Portal server status or ensure that the users have certain network access rights.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The detection interval of the Portal server multiplied by the maximum number of detection failures cannot be less than the keepalive heartbeat interval of the Portal server. It is recommended that the configured detection interval of the Portal server be greater than the keepalive heartbeat interval of the Portal server.

You are advised to use the default value of the **critical-num** parameter for the following reasons:

- If the number of Portal servers in Up state is less than or equal to the value of **critical-num**, the value of Status in the **display server-detect state** command output is Abnormal. If the authentication escape function is configured, users are granted limited network access rights.
- If the number of Portal servers in Up state is greater than the value of **critical-num**, the value of Status in the **display server-detect state** command output is Normal.
- If there is only one Portal server and **critical-num** is set to 1, the number of Portal servers in Up state is equal to the value of **critical-num** when the Portal server goes Up. In this case, the value of Status in the **display server-detect state** command output is Abnormal. In such scenarios, you need to set **critical-num** to the default value 0 so that the value of Status is Normal.

Example

Enable the Portal server detection and keepalive function in the Portal server profile **abc**, set the detection interval to 100s, set the maximum number of failures to 5, and specify the log sent after the number of failures exceeds the limit.

```
<Huawei> system-view
[Huawei] web-auth-server abc
[Huawei-web-auth-server-abc] server-detect interval 100 max-times 5 action log
```

Related Topics

19.6.149 user-sync

19.6.136 server-ip (Portal server profile view)

Function

The **server-ip** command configures an IP address for a Portal server.

The **undo server-ip** command deletes an IP address for a Portal server.

By default, no IP address is configured for a Portal server.

Format

server-ip *server-ip-address* &<1-10>

undo server-ip { *server-ip-address* | **all** }

Parameters

Parameter	Description	Value
server-ip-address	Specifies an IP address of a Portal server.	The value is in dotted decimal notation.

Parameter	Description	Value
all	Deletes all IP addresses of a Portal server.	-

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a Portal server profile on the device using the **19.6.157 web-auth-server (system view)** command, configure parameters for the template.

Run the **server-ip** command to configure an IP address for the Portal server in the Portal server profile view. When receiving a Portal authentication request packet from a user, the device sends a response packet to the Portal server with the configured IP address. Multiple IP addresses can be configured in a Portal server profile. This configuration allows Portal authentication users to access the same Portal authentication page using multiple IP addresses, making the authentication process more flexible.

Precautions

- After the IP address corresponding to a Portal server is configured in the Portal server profile, users are allowed to access the IP address.
- If multiple IP addresses are configured for a Portal server in the Portal server profile, you are advised to run the **19.6.143 url (Portal server profile view)** command to configure a URL for the Portal server. If no URL is configured, the device uses the first IP address as the URL by default, and the other IP addresses do not take effect.

Example

Set the Portal server IP address in the Portal server profile **huawei** to 10.10.10.1.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] server-ip 10.10.10.1
```

Related Topics

19.6.52 display web-auth-server configuration

 Copyright © Huawei Technologies Co., Ltd.

19.6.137 shared-key (Portal server profile view)

Function

The **shared-key** command configures the shared key that the device uses to exchange information with a Portal server.

The **undo shared-key** command restores the default setting.

By default, no shared key that the device uses to exchange information with a Portal server is configured.

Format

shared-key cipher *key-string*

undo shared-key

Parameters

Parameter	Description	Value
cipher	Displays a shared key in cipher text.	-
key-string	Specifies the shared key.	The value is a string of case-sensitive characters without spaces. It can be a string of 1 to 16 characters in plain text, or a string of 48 characters in cipher text. When double quotation marks are used around the string, spaces are allowed in the string.

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a shared key is configured using the **shared-key** command, the Portal packet exchanged between the device and Portal server carries an authenticator generated according to the shared key, and the authenticator is used to check whether the Portal packet at the receiver is correct. This effectively improves the information exchange security.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

For security purposes, it is recommended that the password contains at least two types of lower-case letters, upper-case letters, numerals, and special characters, and contains at least 6 characters.

Example

Configure the shared key in the Portal server profile **huawei** to **huawei@123**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] shared-key cipher huawei@123
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.138 source-interface (Portal server template view)

Function

The **source-interface** command configures an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server.

The **undo source interface** command restores the default configuration.

By default, no source IP address is configured for the device.

Format

source-interface *interface-type interface-number*

undo source-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Configures an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server: ● *interface-type* specifies the interface type. **NOTE** The interface must be a loopback interface. ● *interface-number* specifies the interface number.	-

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to communicate with the Portal server normally, ensure that the source IP address in the packets sent by the device to the Portal server is consistent with the device IP address configured on the Portal server. By default, the device uses the IP address of an outbound interface as the source IP address to communicate with the Portal server. When there are multiple outbound interfaces and the outbound interface sending packets changes, the source IP address in the packets sent by the device to the Portal server becomes inconsistent with the device IP address configured on the Portal server. In this situation, communication between the device and Portal server is interrupted. To address this problem, run the **source-interface** command on the device to specify the IP address of a loopback interface as the source IP address used by the device to communicate with the Portal server.

Precautions

The specified interface must be a Layer 3 interface with an IP address configured.

Example

Configure an IP address of a specified interface as the source IP address used by the device to communicate with the Portal server.

```
<Huawei> system-view
[Huawei] interface loopback 1
[Huawei-LoopBack1] ip address 10.1.2.25 24
[Huawei-LoopBack1] quit
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] source-interface loopback 1
```

19.6.139 source-ip (Portal server profile view)

Function

The **source-ip** command configures the source IP address for the device to communicate with a Portal server.

The **undo source-ip** command restores the default setting.

By default, no source IP address is configured for the device to communicate with a Portal server.

Format

source-ip *ip-address*

undo source-ip

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address for communication with a Portal server.	The value is in dotted decimal notation.

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure normal communication between the device and Portal server, run the **source-ip** command to configure a source IP address on the device.

If the device is configured with a loopback IP address and a common IP address, the device can communicate with the Portal server only when the loopback IP address and common IP address are the same. The **source-ip** command configures a source IP address on the device in the Portal server profile view to allow communication between the device and a Portal server.

Precautions

Ensure that the configured source IP address is the device IP address. The source IP address cannot be all 0s, all 1s, class D address, class E address, or loopback address.

Example

Set the source IP address for communication between the device and a Portal server to 192.168.1.100 in the Portal server profile **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] source-ip 192.168.1.100
```

19.6.140 snmp-agent trap enable feature-name mid_eapol

Function

The **snmp-agent trap enable feature-name mid_eapol** command enables the trap function for the DOT1X module.

The **undo snmp-agent trap enable feature-name mid_eapol** command disables the trap function for the DOT1X module.

By default, the trap function is enabled for the DOT1X module.

Format

snmp-agent trap enable feature-name mid_eapol [**trap-name** { **hwmacauthenmaxuseralarm** | **hwsrvcfgeapmaxuseralarm** }]

undo snmp-agent trap enable feature-name mid_eapol [**trap-name** { **hwmacauthenmaxuseralarm** | **hwsrvcfgeapmaxuseralarm** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the DOT1X module.	-
hwmacauthenmaxuser-alarm	Enables the device to send a Huawei proprietary trap when the number of MAC address authentication users reaches the maximum number allowed on an interface.	-
hwsrvcfgeapmaxusera-larm	Enables the device to send a Huawei proprietary trap when the number of 802.1X authentication users reaches the maximum number allowed on an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the trap function for hwmacauthenmaxuseralarm of the DOT1X module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mid_eapol trap-name hwmacauthenmaxuseralarm
```

Related Topics

19.6.53 display snmp-agent trap feature-name mid_eapol all

19.6.141 snmp-agent trap enable feature-name mid_web

Function

The **snmp-agent trap enable feature-name mid_web** command enables the trap function for the web authentication module.

The **undo snmp-agent trap enable feature-name mid_web** command disables the trap function for the web authentication module.

By default, the trap function is enabled for the web authentication module.

Format

snmp-agent trap enable feature-name mid_web [**trap-name** { **hwportalmaxuseralarm** | **hwportaluserclearalarm** | **hwportalserverdown** | **hwportalserverup** }]

undo snmp-agent trap enable feature-name mid_web [**trap-name** { **hwportalmaxuseralarm** | **hwportaluserclearalarm** | **hwportalserverdown** | **hwportalserverup** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for a specified event of the web authentication module.	-
hwportalmaxuseralarm	Enables the device to send a Huawei proprietary trap when the number of online Portal authentication users exceeds the upper threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwportaluserclearalarm	Enables the device to send a Huawei proprietary trap when the number of online Portal authentication users falls below the lower threshold.	-
hwportalserverdown	Enables the device to send a Huawei proprietary trap when it detects that the Portal server changes from Up to Down.	-
hwportalserverup	Enables the device to send a Huawei proprietary trap when it detects that the Portal server changes from Down to Up.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

After the trap function is enabled, the device generates traps during operation and sends the traps to the NMS through the SNMP module. If the trap function is disabled, the device does not generate traps and the SNMP module does not send traps to the NMS.

You can specify **trap-name** to enable the trap function for one or more events.

Example

Enable the trap function for hwportalmaxuseralarm of the web authentication module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name mid_web trap-name hwportalmaxuseralarm
```

Related Topics

19.6.54 display snmp-agent trap feature-name mid_web all

19.6.142 url (URL template view)

Function

The **url** command configures the redirection URL or pushed URL.

The **undo url** command cancels the redirection URL or pushed URL.

By default, no redirection URL or pushed URL is configured.

Format

url [**push-only** | **redirect-only**] *url-string* [**ssid** *ssid*]

undo url [**push-only** | **redirect-only**] [**ssid** *ssid*]

Parameters

Parameter	Description	Value
url-string	Specifies the redirection URL or pushed URL.	It is a string of 1 to 200 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
push-only	Specifies the URL as a pushed URL.	-
redirect-only	Specifies the URL as a redirection URL.	-
ssid *ssid*	Specifies the SSID that users associate with. This parameter is only valid for wireless access users. The SSID that users associate with must be the same as that configured on the device; otherwise, the device cannot push URLs to users.	The SSID must already exist.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **19.6.147 url-template name** command, you can run this command to configure the redirection URL or pushed URL. The difference between redirection URL and pushed URL is as follows.

- Redirection URL: When a user without network access right connects to the network, the Portal authentication device redirects the user to the redirection URL for authentication.
- Pushed URL: After an authenticated user accesses the network through web for the first time, the access device pushes the web page corresponding to the URL to the user. The web access request from the user is redirected to the specified URL, and then the user is allowed to access network resources.

Precautions

If the **push-only** and **redirect-only** parameters are not specified, the configured URL is used as both redirection URL and pushed URL. You can configure pushed URL using the **19.6.80 force-push** command, or use the **19.6.148 url-template (Portal server profile view)** command to bind a URL template to the Portal server profile to configure redirection URL.

Example

Set the redirection URL to http://10.1.1.1.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] url http://10.1.1.1
```

19.6.143 url (Portal server profile view)

Function

The **url** command configures the URL for a Portal server.

The **undo url** command restores the default setting.

By default, no URL is configured for a Portal server.

Format

url *url-string*

undo url

Parameters

Parameter	Description	Value
url-string	Specifies the URL of a portal server.	It is a string of 1 to 200 case-sensitive characters that do not contain spaces and question marks (?). When double quotation marks are used around the string, spaces are allowed in the string.

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the Portal server IP address is configured using the **19.6.136 server-ip (Portal server profile view)** command, the Portal server URL is generated by default on the device. If the existing Portal server URL is inconsistent with the default one or the domain name needs to be used, you need to run the **url** command to specify the Portal server URL.

Precautions

A Portal server only has one URL.

Example

Set the URL of a Portal server to http://www.***.com in the Portal server profile **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] url http://www.***.com
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.144 url-parameter mac-address format

Function

The **url-parameter mac-address format** command configures the MAC address format in URL.

The **undo url-parameter mac-address format** command restores the default MAC address format in URL.

By default, the MAC address format in URL is XXXXXXXXXXXX.

Format

url-parameter mac-address format delimiter *delimiter* { **normal** | **compact** }

undo url-parameter mac-address format

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delimiter *delimiter*	Specifies the delimiter in MAC address.	The value is one case-sensitive character without spaces.
normal	Sets the MAC address format to XX-XX-XX-XX-XX-XX.	-
compact	Sets the MAC address format to XXXX-XXXX-XXXX.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Portal servers or websites may require different MAC address formats. You can run the **url-parameter mac-address format** command to set MAC address formats in URL to meet the requirements of Portal servers or website.

Example

Set the delimiter to - and format to XXXX-XXXX-XXXX.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] url-parameter mac-address format delimiter - compact
```

19.6.145 url-parameter

Function

The **url-parameter** command sets parameters in a URL.

The **undo url-parameter** command deletes parameters in a URL.

By default, a URL does not carry parameters.

Format

url-parameter { **ac-ip** *ac-ip-value* | **ac-mac** *ac-mac-value* | **ap-ip** *ap-ip-value* | **ap-mac** *ap-mac-value* | **login-url** *url-key url* | **redirect-url** *redirect-url-value* | **ssid** *ssid-value* | **sysname** *sysname-value* | **user-ipaddress** *user-ipaddress-value* | **user-mac** *user-mac-value* | **user-vlan** *user-vlan-value* | **esn** *esn-value* } *

undo url-parameter

Parameters

Parameter	Description	Value
ac-ip *ac-ip-value*	Specifies the IP address of the AC carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ac-mac *ac-mac-value*	Specifies the MAC address of the AC carried in the URL and sets the parameter name displayed in the URL.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ap-ip *ap-ip-value*	Specifies the AP IP address carried in the URL and sets the parameter name. This parameter is only valid for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ap-mac *ap-mac-value*	Specifies the AP MAC address carried in the URL and sets the parameter name. This parameter is only valid for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
login-url *url-key url*	Specifies the login URL of the access device. ● *url-key*: specifies the identification keyword for the login URL sent to the Portal server during redirection. ● *url*: is a specified URL on the access device.	● *url-key*: The value is a string of 1 to 16 case-sensitive characters without spaces, question marks (?), ampersands (&), and equal signs (=). ● *url*: The value is a string of 1 to 200 case-sensitive characters without spaces.
redirect-url *redirect-url-value*	Specifies the original URL that a user accesses carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
ssid *ssid-value*	Specifies the SSID associated that users associate with carried in the URL and sets the parameter name. This parameter is only valid for wireless access users.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
sysname *sysname-value*	Specifies the device system name carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-ipaddress *user-ipaddress-value*	Specifies the user IP address carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user-mac *user-mac-value*	Specifies the user MAC address carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
user-vlan *user-vlan-value*	Specifies the user VLAN carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
esn *esn-value*	Specifies the ESN carried in the URL and sets the parameter name.	The value is a string of 1 to 16 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a URL template is created using the **19.6.147 url-template name** command and URL is configured using the **19.6.142 url (URL template view)** command, you can use the **url-parameter** command to set the parameters in the URL. When a user accesses the Portal server according to the URL, the Portal server obtains user terminal information through the parameters in the URL. The Portal server then provides the corresponding web authentication page for the user according to user terminal information.

In addition, when users are pushed to a website rather than the Portal server according to the URL, the website provides the different web pages for the users according to user terminal information carried in the URL.

Precautions

URL parameter names configured on the device must be the same as those supported by the server. In this example, the device is connected to the Agile Controller-Campus.

URL Parameter	URL Parameter Name Supported by the Agile Controller-Campus
ac-ip	ac-ip
ap-mac	apmac
ssid	ssid
redirect-url	url
user-ipaddress	userip
user-mac	usermac

Example

Set the user MAC address and access device system name in the URL.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] url-parameter user-mac usermac sysname huawei
```

19.6.146 url-parameter set

Function

The **url-parameter set** command sets redirection parameter values.

The **undo url-parameter set** command restores the default setting.

By default, the device automatically obtains redirection parameter values.

 Copyright © Huawei Technologies Co., Ltd.

Format

url-parameter set { **ac-ip** { *ip-address* | **interface** *interface-type interface-number* } | **ap-ip** { *ip-address* | **interface** *interface-type interface-number* } } *

undo url-parameter set { **ac-ip** | **ap-ip** }

Parameters

Parameter	Description	Value
ac-ip	Sets the value of the redirection parameter **ac-ip**.	-
ap-ip	Sets the value of the redirection parameter **ap-ip**.	-
ip-address	Sets the value of a redirection parameter to a specified IP address.	The value is in dotted decimal notation.
interface *interface-type interface-number*	Sets the value of a redirection parameter to the IP address of an interface.	-

Views

URL template view

Default Level

2: Configuration level

Usage Guidelines

Assume that a URL template is created using the **19.6.147 url-template name** command, and a URL is configured in the URL template using the **19.6.142 url (URL template view)** command. When the device functions as an AC and user terminals communicate with the Portal server, the default value of **ac-ip** is the CAPWAP gateway address and the default value of **ap-ip** is the AP's IP address. When the device functions as a FAT AP and user terminals communicate with the Portal server, the default values of **ac-ip** and **ap-ip** are the user-side gateway address. If clients cannot communicate with the Portal server using the default values, you can run the **url-parameter set** { **ac-ip** { *ip-address* | **interface** *interface-type interface-number* } | **ap-ip** { *ip-address* | **interface** *interface-type interface-number* } } * command to set the value of the redirection parameter **ac-ip** or **ap-ip** (to the IP address of the device's WAN interface generally). When user terminals use the URL to access the Portal server, the Portal server then can obtain user terminal information according to parameters in the URL.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the value of the redirection parameter **ap-ip** to 10.1.1.1.

```
<Huawei> system-view
[Huawei] url-template name huawei
[Huawei-url-template-huawei] url-parameter set ap-ip 10.1.1.1
```

19.6.147 url-template name

Function

The **url-template name** command creates a URL template or displays an existing URL template view.

The **undo url-template name** command deletes a URL template.

By default, no URL template exists on the device.

Format

url-template name *template-name*

undo url-template name *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of a URL template.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a Portal authentication server template is created using the **19.6.157 web-auth-server (system view)** command, you can bind a URL template to the Portal authentication server template. The URL template contains the redirection URL and redirection URL parameters.

The **url-template name** command creates a URL template or displays an existing URL template view.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a URL template named **huawei** and enter the template view.

```
<Huawei> system-view
[Huawei] url-template name huawei
```

19.6.148 url-template (Portal server profile view)

Function

The **url-template** command binds a URL template to a Portal server profile.

The **undo url-template** command unbinds a URL template from a Portal server profile.

By default, no URL template is bound to a Portal server profile.

Format

url-template *url-template*

undo url-template

Parameters

Parameter	Description	Value
url-template	Specifies the name of a URL template.	The value must be an existing URL template name.

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the parameters of a URL template are configured, the URL template must be bound to a Portal authentication server template so that users can be authenticated on the Portal authentication server corresponding to the redirection URL.

Prerequisites

A URL template has been created using the **19.6.147 url-template name** command.

Precautions

If a URL template is bound to the Portal authentication server template and the **19.6.143 url (Portal server profile view)** command is executed to configure the redirection URL corresponding to the Portal authentication server, only the parameters in the URL template take effect.

The URL configured using the **19.6.142 url (URL template view)** command in the URL template view cannot be a pushed URL; otherwise, the command does not take effect.

Example

Bind the URL template **abc** to the Portal authentication server template.

```
<Huawei> system-view
[Huawei] url-template name abc
[Huawei-url-template-abc] quit
[Huawei] web-auth-server huawei
[Huawei-web-auth-server-huawei] url-template abc
```

19.6.149 user-sync

Function

The **user-sync** command enables Portal authentication user information synchronization.

The **undo user-sync** command disables Portal authentication user information synchronization.

By default, Portal authentication user information synchronization is disabled.

Format

user-sync [**interval** *interval-period* | **max-times** *times*] *

undo user-sync

Parameters

Parameter	Description	Value
interval *interval-period*	Specifies the user information synchronization interval.	The value is an integer that ranges from 30 to 65535, in seconds. The default value is 300.
max-times *times*	Specifies the maximum number of user information synchronization failures.	The value is an integer that ranges from 2 to 255. The default value is 3.

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If communication is interrupted because the network between the device and Portal server is disconnected or the Portal server is faulty, online Portal authentication users cannot go offline. Therefore, user information on the device and on the Portal server may be inconsistent and accounting may be inaccurate.

The **user-sync** command enables user information synchronization so that user information on the device and Portal server is synchronized at intervals to ensure user information consistency.

During information synchronization, the device does not disconnect the user immediately after detecting that the device has certain user information while the server does not have such information. Instead, the device disconnects the user when the maximum number of user information synchronization failures is reached.

Precautions

If users go online during the keepalive interval of the Portal server, the Portal server does not have their entries. After the Portal server goes Up and starts synchronizing user information, the device does not disconnect these users even if synchronization fails. The device retails these users until next time these users go online and performs Portal authentication, ensuring good user experience.

The value of *interval-period***times* configured on the device must be greater than the interval for the Portal server to send synchronization packets. Otherwise, the device may force users offline when it cannot receive any synchronization packet from the Portal server after the maximum failure number is reached.

When you run the **user-sync** command, make sure that the Portal server supports this function. Otherwise, the users will go offline.

Example

Enable user information synchronization in the Portal server profile **abc**, set the interval for user information synchronization to 100s, and set the maximum number of synchronization failures to 5.

```
<Huawei> system-view
[Huawei] web-auth-server abc
[Huawei-web-auth-server-abc] user-sync interval 100 max-times 5
```

19.6.150 user-group

Function

The **user-group** command creates a user group or displays the user group view.

The **undo user-group** command deletes a user group.

By default, no user group is configured.

Format

user-group *group-name* [**group-index** *group-index*]

undo user-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of a user group.	The value is a string of 1-64 case-sensitive characters, which cannot be configured to - and --. It cannot contain spaces and the following symbols: / \ : * ? " < > | @ ' %.
group-index *group-index*	Specifies the index of a user group.	The value is an integer and varies according to device model: ● AR100 series, AR120 series, AR150 series, AR160 series, AR200 series, AR1200 series, AR2200 (except AR2204XE, AR2204XE-DC, AR2240C): 0 to 15 ● AR2204XE, AR2204XE-DC, AR2240C, AR3600 series: 0 to 31 ● AR3200 series: 0 to 7

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practical NAC applications, there are many access users and a large number of ACL rules need to be configured for each user. However, the number of user types is limited.

You can run the **user-group** command to create user groups on the device and associate each user group to a group of ACL rules (for details, see **19.6.5 acl-id (user group view)**). In this way, users in the same group share a group of ACL rules. The limited ACL resources can support a large number of access users.

Precautions

- The device supports a maximum of 32 user groups.
- When you create a user group, ensure that the user group name is different from the number of an existing ACL. You can run the **display acl all** command to view the configuration of all ACL rules on the device.

- If you want to delete the user group when the ACL bound to the user takes effect, run the **cut access-user user-group** command to disconnect all users bound to the user group.
- The priority of the user group authorization information delivered by the authentication server is higher than that of the user group authorization information applied in the AAA domain. If the user group authorization information delivered by the authentication server cannot take effect, the user group authorization information applied in the AAA domain also cannot be used. For example, if only user group B is configured on the device and the group authorization information is applied in the AAA domain when the authentication server delivers authorization information about user group A, the authorization information about user groups A and B both cannot take effect. To make the user group authorization information delivered by the authentication server take effect, ensure that this user group is configured on the device. To make the user group authorization information applied in the AAA domain take effect, ensure that the authentication server does not deliver any user group attribute.

Example

Create a user group **test1**.

```
<Huawei> system-view
[Huawei] user-group test1
```

19.6.151 user-isolated

Function

The **user-isolated** command configures inter-group or intra-group isolation in a user group.

The **undo user-isolated** command disables inter-group or intra-group isolation in a user group.

By default, inter-group or intra-group isolation is not configured in a user group.

Format

user-isolated { **inter-group** | **inner-group** } *

undo user-isolated { **inter-group** | **inner-group** } *

Parameters

Item	Description	Value
inter-group	Configures inter-group isolation.	-
inner-group	Configures intra-group isolation.	-

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After inter-group isolation is configured in a user group, users in the user group cannot communicate with users in other user groups.

After intra-group isolation is configured in a user group, users in the user group cannot exchange Layer 2 or Layer 3 packets with each other.

Precautions

After authorized users go online, the RADIUS server dynamically delivers user group information. In this situation, the inter-group or intra-group isolation configuration cannot be modified or deleted.

Example

Configure intra-group isolation in user group **general-group**.

```
<Huawei> system-view
[Huawei] user-group general-group
[Huawei-user-group-general-group] user-isolated inter-group inner-group
```

19.6.152 user-vlan

Function

The **user-vlan** command binds a VLAN to a user group.

The **undo user-vlan** command unbinds a VLAN from a user group.

By default, no VLAN is bound to a user group.

Format

user-vlan *vlan-id*

undo user-vlan

Parameters

Parameter	Description	Value
vlan-id	Specifies the ID of a VLAN bound to a user group.	The value is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

User group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After creating a user group using the **user-group** command, you can run the **user-vlan** command to bind a VLAN to the user group. The device will deliver the authorization VLAN based on the user group. When a user in the user group goes online, the user will be added to the VLAN and obtain network access rights of the user group.

Prerequisites

- The VLAN to be bound to a user group has been created using the **6.3.43 vlan** command.

Precautions

- An authorized VLAN cannot be delivered to online Portal users.
- This command does not take effect for users who are already online.

Example

Configure VLAN 10 as the authorization VLAN for the user group **abc**.

```
<Huawei> system-view
[Huawei] vlan batch 10
[Huawei] user-group abc
[Huawei-user-group-abc] user-vlan 10
```

Related Topics

19.6.51 display user-group

19.6.153 vpn-instance (Portal server template view)

Function

The **vpn-instance** command configures a VPN instance used for communication between the device and Portal server.

The **undo vpn-instance** command restores the default setting.

By default, no VPN instance is configured for communication between the device and Portal server.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be an existing VPN instance name on the device.

Views

Portal server template view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A VPN implements interconnection within the same department and between different departments in an enterprise. To enable the Portal authentication service in the VPN, run the **vpn-instance** command to bind a Portal server template to a VPN instance.

Prerequisites

A VPN instance has been created using the **ip vpn-instance** command.

Precautions

The VPN instance bound to the Portal server template must be the same as that bound to the Portal server.

The users in VPN instances bound to different Portal server templates cannot use the same IP addresses because users with the same IP addresses cannot go online or offline.

Example

Bind the Portal server template **abc** to the VPN instance **vpn1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vpn1
[Huawei-vpn-instance-vpn1] ipv4-family
[Huawei-vpn-instance-vpn1-af-ipv4] quit
[Huawei-vpn-instance-vpn1] quit
[Huawei] web-auth-server abc
[Huawei-web-auth-server-abc] vpn-instance vpn1
```

 Copyright © Huawei Technologies Co., Ltd.

19.6.154 web-auth-server listening-port

Function

The **web-auth-server listening-port** command sets the number of the port through which a device listens on Portal protocol packets.

The **undo web-auth-server listening-port** command restores the default listening port.

By default, the device uses UDP port 2000 to listen on Portal protocol packets.

Format

web-auth-server listening-port *port-number*

undo web-auth-server listening-port

Parameters

Parameter	Description	Value
port-number	Specifies the number of the listening port.	The value is an integer that ranges from 1024 to 55535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device exchanges user authentication information with the Portal server using the Portal protocol, you must configure the listening port on the device to receive Portal packets.

You can run the **web-auth-server listening-port** command to set the number of the port through which the device listens on Portal packets. The port number must be the same as the destination port number in Portal packets sent by the Portal server and must be unique.

NOTE

If a specified port is occupied by another service or is a reserved port, the configuration fails. Ensure that the specified port is available when running this command.

Example

Set the number of the port through which a device listens on Portal protocol packets to 3000.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] web-auth-server listening-port 3000
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.155 web-auth-server (Portal access profile view)

Function

The **web-auth-server** command configures the Portal server profile used by a Portal access profile.

The **undo web-auth-server** command restores the default setting.

By default, a Portal access profile does not use any Portal server profile.

Format

web-auth-server *server-name* [*bak-server-name*] { **direct** | **layer3** }

undo web-auth-server

Parameters

Parameter	Description	Value
server-name	Specifies the name of a Portal server profile.	The value must be an existing Portal server profile name.
bak-server-name	Specifies the name of a backup Portal server profile. **NOTE** The name of the backup Portal server profile cannot be configured to the command-line keywords **direct** and **layer3**.	The value must be an existing Portal server profile name.
direct	Sets the Portal authentication mode to Layer 2 authentication.	-
layer3	Sets the Portal authentication mode to Layer 3 authentication.	-

Views

Portal access profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a Portal server profile is configured on the device, this profile must be bound to a Portal access profile. When users who use the Portal access profile attempt to access charged network resources, the HTTP requests are forcibly redirected to the authentication page of the Portal server to implement Portal authentication.

To improve Portal authentication reliability, the backup Portal server profile can also be bound to the Portal access profile. When the primary Portal server is disconnected, the users are redirected to the backup Portal server for authentication. This function can take effect only when the Portal server detection function is enabled using the **19.6.135 server-detect** command and heartbeat detection is enabled on the Portal server.

The following Portal authentication modes are available:

- **direct**: When there is no Layer 3 forwarding device between the device and a user, the device can learn the user's MAC address. You can configure the Layer 2 authentication mode so that the device can identify the user using the IP address and MAC address.
- **layer3**: When there is a Layer 3 forwarding device between the device and a user, the device cannot learn the user's MAC address and can only identify the user using the IP address. You need to configure the Layer 3 authentication mode.

Prerequisites

A Portal server profile has been created using **19.6.157 web-auth-server (system view)** and the IP address of the Portal server has been configured using **19.6.136 server-ip (Portal server profile view)**.

Precautions

- After a Portal access profile is bound to an authentication profile, the Portal server profile used in the Portal access profile cannot be deleted, but can be modified.
- This command does not take effect on the VLANIF interface corresponding to the super VLAN.

Example

Bind the Portal access profile **p1** to the Portal server profiles **server1** and **server2** (backup Portal server profile), and configure the Layer 2 authentication mode.

```
<Huawei> system-view
[Huawei] web-auth-server server1
[Huawei-web-auth-server-server1] server-ip 10.10.1.1
[Huawei-web-auth-server-server1] quit
[Huawei] web-auth-server server2
[Huawei-web-auth-server-server2] server-ip 10.10.2.1
[Huawei-web-auth-server-server2] quit
[Huawei] portal-access-profile name p1
[Huawei-portal-acces-profile-p1] web-auth-server server1 server2 direct
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.6.157 web-auth-server (system view)

19.6.136 server-ip (Portal server profile view)

19.6.52 display web-auth-server configuration

19.6.31 display authentication-profile configuration

19.6.156 web-auth-server reply-message

Function

The **web-auth-server reply-message** command enables the device to transparently transmit users' authentication responses sent by the authentication server to the Portal server.

The **undo web-auth-server reply-message** command disables the device from transparently transmitting users' authentication responses sent by the authentication server to the Portal server.

By default, the device transparently transmits users' authentication responses sent by the authentication server to the Portal server.

Format

web-auth-server reply-message

undo web-auth-server reply-message

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The AAA server requires that the authentication messages sent to the Portal server contain the authentication reply; therefore, the **web-auth-server reply-message** command is required. In certain situations, the authentication messages are not required to carry the reply. In this case, run the **undo web-auth-server reply-message** command.

By default, the device directly forwards the authentication result message from the RADIUS server to the Portal server without processing. This is called transparent transmission.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the device from transparently transmitting users' authentication responses to the Portal server.

```
<Huawei> system-view
[Huawei] undo web-auth-server reply-message
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.157 web-auth-server (system view)

Function

The **web-auth-server** command creates a portal server profile or displays the portal server profile view.

The **undo web-auth-server** command deletes a portal server profile.

By default, no portal server template exists.

Format

web-auth-server *server-name*

undo web-auth-server *server-name*

Parameters

Parameter	Description	Value
server-name	Specifies the name of a portal server.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain spaces or the following symbols: / \ : * ? " < > | @ ' %. The value cannot be - or --. **NOTE** *server-name* cannot be set to listening-port, reply-message, version, or the first character or several leftmost characters of these character strings.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When an unauthenticated portal user goes online, the device forces the user to log in to a specified website (also called the portal website). The user can access resources in the portal website for free. When the user attempts to access charged network resources, the user must pass authentication on the portal website. The specific process is as follows:

1. The unauthorized user opens Internet Explorer and enters a URL in the address box. When receiving the HTTP request sent by the user, the device redirects it to the portal authentication page of the portal server.
2. The user enters user information on the authentication page or in the authentication dialog box, and the portal server forwards the user information to the device.
3. After receiving the user information from the portal server, the device sends the information to the authentication server for authentication and accounting.
4. After the user is authenticated, the device allows the user to access the Internet if no security policy is enforced.

After a portal server profile is created on the device by using the **web-auth-server** command, run other commands to create a route from the device to the portal server.

Follow-up Procedure

Run the following commands to configure related attributes of the portal server profile:

- Run the **19.6.136 server-ip (Portal server profile view)** command to configure an IP address for the portal server.
- Run the **19.6.143 url (Portal server profile view)** command to configure a URL of the portal server.
- Run the **19.6.98 port (Portal server profile view)** command to set the port number that a portal server uses to receive notification packets from the device.
- Run the **19.6.137 shared-key (Portal server profile view)** command configures the shared key that the device uses to exchange information with the portal server.

Precautions

You are advised to back up the portal server data to prevent authentication failure caused by the portal server fault.

A maximum of eight portal server profiles can be configured on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create portal server profile named **huawei**.

```
<Huawei> system-view
[Huawei] web-auth-server huawei
```

Related Topics

19.6.52 display web-auth-server configuration
19.6.143 url (Portal server profile view)
19.6.136 server-ip (Portal server profile view)
19.6.98 port (Portal server profile view)
19.6.137 shared-key (Portal server profile view)

19.6.158 web-auth-server version

Function

The **web-auth-server version** command sets the Portal protocol version supported by the device.

The **undo web-auth-server version** command restores the default setting.

By default, the device supports both the versions V1.0 and V2.0.

Format

web-auth-server version v2 [**v1**]

undo web-auth-server version

Parameters

Parameter	Description	Value
v2	Indicates that the device supports the Portal protocol version V2.0. The major version currently used is V2.0.	-
v1	Indicates that the device supports the Portal protocol version V1.0.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Currently, the Portal protocol has two versions: V1.0 and V2.0. The device and Portal server must use the Portal protocol of the same version to ensure normal

 Copyright © Huawei Technologies Co., Ltd.

communication. You can run the **web-auth-server version** command to set the Portal protocol version supported by the device.

NOTE

The version V2.0 is widely used currently.

To ensure smooth communication, the device supports both versions by default.

Example

Configure the device to use only the Portal protocol V2.0.

```
<Huawei> system-view
[Huawei] web-auth-server version v2
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.159 web-redirection disable (Portal server profile view)

Function

The **web-redirection disable** command disables the Portal authentication redirection function.

The **undo web-redirection disable** command enables the Portal authentication redirection function.

By default, the Portal authentication redirection function is enabled.

Format

web-redirection disable

undo web-redirection disable

Parameters

None

Views

Portal server profile view

Default Level

2: Configuration level

Usage Guidelines

The device redirects all unauthenticated users to the Portal authentication page when the users send access requests to external networks. For example, when the user needs to enter the URL of the authentication page manually, the **web-redirection disable** command can be executed so that unauthorized users are not forcibly redirected to the Portal authentication page.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable the Portal authentication redirection function.

```
<Huawei> system-view
[Huawei] web-auth-server nac
[Huawei-web-auth-server-nac] web-redirection disable
```

Related Topics

19.6.52 display web-auth-server configuration

19.6.160 web-service aaa server

Function

The **web-service aaa server** command configures a URL for the authentication and accounting server and enables the function of receiving user authorization information.

The **undo web-service aaa server** command deletes the URL configured for the authentication and accounting server and disables the function of receiving user authorization information.

By default, no URL is configured for the authentication and accounting server, and the function of receiving user authorization information is disabled.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service aaa server *url* **authorize-enable**

undo web-service aaa server

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url	Specifies the URL of the authentication and accounting server.	The value is a string of 1 to 128 characters in the format of **[http://]host[:port]**. ● host: indicates an IP address or a domain name. ● port: indicates a port number. The default value is 80. You need to add the port number to the IP address or domain name only when the default port number is changed. **NOTE** If the value of **host** is in the domain name format, configure a DNS table before using this command; otherwise, the IP address matching the domain name cannot be obtained. If the DNS table is modified after this command is executed, run this command again.
authorize-enable	The function of receiving user authorization information is enabled.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users connecting to the device through Wi-Fi can access the Internet only after being authenticated by the authentication and accounting server. You can run this command to configure a URL for the authentication and accounting server, and enable the function of receiving user authorization information. User authorization information includes online duration, traffic usage, and user bandwidth. When a user accesses the Internet, the device periodically sends accounting packets to the

 Copyright © Huawei Technologies Co., Ltd.

authentication and accounting server. The server performs accounting for the users based on user traffic statistics. When the online duration or traffic usage exceeds authorization, the device forcibly disconnects the user and sends the disconnection message of the user to the authentication and accounting server.

Example

Configure a URL for the authentication and accounting server and enable the function of receiving user authorization information.

```
<Huawei> system-view
[Huawei] web-service aaa server http://10.1.1.1:81 authorize-enable
```

19.6.161 web-service access enable

Function

The **web-service access enable** command enables authentication and accounting functions on a WLAN-BSS interface.

The **undo web-service access enable** command disables authentication and accounting functions on a WLAN-BSS interface.

By default, authentication and accounting functions are disabled on a WLAN-BSS interface.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service access enable

undo web-service access enable

Parameters

None

Views

WLAN-BSS interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Users connecting to the device through Wi-Fi can access the Internet only after being authenticated. After authentication and accounting functions are enabled on a WLAN-BSS interface using this command, the device provides authentication and accounting functions to users.

Example

Enable authentication and accounting functions on a WLAN-BSS interface.

```
<Huawei> system-view
[Huawei] interface wlan-bss 0

[Huawei-Wlan-Bss0] web-service access enable
```

19.6.162 web-service accounting enable

Function

The **web-service accounting enable** command enables the device to send accounting packets to the authentication and accounting server.

The **undo web-service accounting enable** command disables the device from sending accounting packets to the authentication and accounting server.

By default, the device does not send accounting packets to the authentication and accounting server.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service accounting enable

undo web-service accounting enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After a user connects to the device through Wi-Fi, is authenticated by the authentication and accounting server, and obtains rights, the user can access the websites outside the whitelist. This command enables the device to send accounting request packets to the authentication and accounting server. When the authorized online traffic volume and duration of an online user are not exceeded, the device periodically sends accounting packets to the authentication and accounting server. The server performs accounting on the user based on the traffic usage when the user stays online.

Example

Enable the device to send accounting packets to the authentication and accounting server.

```
<Huawei> system-view
[Huawei] web-service accounting enable
```

Related Topics

19.6.163 web-service accounting interval

19.6.163 web-service accounting interval

Function

The **web-service accounting interval** command configures the interval at which the device sends accounting packets to the authentication and accounting server.

The **undo web-service accounting interval** command restores the default interval at which the device sends accounting packets to the authentication and accounting server.

By default, the device sends accounting packets to the authentication and accounting server at an interval of 30 seconds.

NOTE

Only the AR121W, AR129W, AR129CVW, AR121GW-L, AR129GW-L, AR129CGVW-L, AR109W, AR109GW-L, AR151W-P, AR156W, AR157W, AR157VW, AR158EVW, AR161W, AR161EW, AR161EW-M1, AR161FGW-L, AR161FGW-Lc, AR169W, AR161FW, AR161FW-P-M5, AR161FGW-La, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169CVW-4B4S, AR169EGW-L, AR169EW, AR169CVW, AR169FGVW-L, AR169FGW-L, AR169W-P-M9, AR169RW-P-M9, AR201VW-P, AR207VW, AR1220W, AR1220EVW, and AR1220VW that can work as a WLAN Fat AP support this command.

Format

web-service accounting interval *interval*

undo web-service accounting interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the device sends accounting packets to the authentication and accounting server.	The value is an integer that ranges from 5 to 60, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Users connecting to the device through Wi-Fi can access the Internet only after being authenticated by the authentication and accounting server. You can run this command to configure the interval at which the device sends accounting packets to the authentication and accounting server.

Example

Set the interval at which the device sends accounting packets to the authentication and accounting server to 10 seconds.

```
<Huawei> system-view
[Huawei] web-service accounting interval 10
```

19.7 ACL Configuration Commands

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support the ACL configured for Layer 2 forwarding traffic.

19.7.1 acl ipv6 name

Function

The **acl ipv6 name** command creates a named ACL6 and enters the ACL6 view.

The **undo acl ipv6 name** command deletes a named ACL6.

By default, no named ACL6 is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

acl ipv6 name *acl6-name* [**advance** | **basic** | *acl6-number*] [**match-order** { **auto** | **config** }]

undo acl ipv6 name *acl6-name*

Parameters

Parameter	Description	Value
acl6-name	Specifies the name of an ACL6.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
advance	Indicates an advanced ACL6.	-
basic	Indicates a basic ACL6.	-
acl6-number	Specifies the number of an ACL6.	The value is an integer that ranges from 2000 to 3999. ● The value of a basic ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL6 ranges from 3000 to 3999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. ● **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL6 rules are matched based on the configuration order. The ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6s are mainly used in QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services which packets need to be filtered.

Precautions

If the number of a named ACL6 is not specified, the Router allocates a number to the named ACL6. The following situations are involved:

- If only the type of a named ACL6 is specified, the number of the named ACL6 allocated by the Router is the maximum value of the named ACL6 of the type.
- If the number and the type of a named ACL6 are not specified, the Router considers the named ACL6 as the advanced ACL6 and allocates the maximum value to the named ACL6.

After you create a named ACL6 by using the **acl ipv6 name** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6 name** *acl6-name* or **undo acl ipv6** *acl6-number* command to delete the ACL6.

When you delete an ACL6 that has been referenced by other services, the services may be interrupted. Therefore, before deleting an ACL6, ensure that the ACL6 is not in use.

Example

Create basic ACL6 2001 named **test2**.

```
<Huawei> system-view
[Huawei] acl ipv6 name test2 2001
```

Related Topics

19.7.8 display acl ipv6

19.7.2 acl ipv6 (system view)

Function

The **acl ipv6** command creates a numbered ACL6 and enters the ACL6 view.

The **undo acl ipv6** command deletes a numbered ACL6.

By default, no numbered ACL6 is created.

Format

acl ipv6 [**number**] *acl6-number* [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | [**number**] *acl6-number* }

Parameters

Parameter	Description	Value
number	Indicates the number that identifies an ACL.	-
acl6-number	Specifies an ACL6 number.	The value is an integer that ranges from 2000 to 3999. ● The value of a basic ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL6 ranges from 3000 to 3999.
match-order { **auto** | **config** }	Indicates the matching order of ACL6 rules. ● **auto**: indicates that ACL6 rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL6 rules are matched based on the configuration order. The ACL6 rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL6 rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL6, the default match order **config** is used.	-
all	Indicates that all the configured ACL6s are deleted.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

An ACL6 is a set of rules composed of **permit** or **deny** clauses. ACL6 rules can be referenced by modules. ACL6s are applicable to QoS. ACL6s can limit data flows to improve network performance. For example, ACL6s are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.

Follow-up Procedure

Run the **rule** command to configure ACL6 rules and apply the ACL6 to services which packets need to be filtered.

Precautions

After you create a named ACL6 by using the **acl ipv6** command, the ACL6 still exists even if you exit from the ACL6 view. You must run the **undo acl ipv6** *acl6-number* command to delete the ACL6.

When you delete an ACL6 that has been referenced by other services, the services may be interrupted. Before deleting an ACL6, ensure that the ACL6 is unused.

All ACL6s can be deleted on the device at one time, whereas this method is not recommended.

Example

Create an ACL6 with the number of 3000.

```
<Huawei> system-view
[Huawei] acl ipv6 number 3000
```

Related Topics

19.7.8 display acl ipv6
19.7.19 rule (basic ACL6 view)
19.7.17 rule (advanced ACL6 view)

19.7.3 acl name

Function

The **acl name** command creates a named ACL and enters the ACL view.

The **undo acl** command deletes a named ACL.

By default, no ACL is created.

Format

acl name *acl-name* [**advance** | **basic** | **link** | *acl-number*] [**match-order** { **auto** | **config** }]

undo acl name *acl-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
acl-name	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
advance	Indicates an advanced ACL.	-
basic	Indicates a basic ACL.	-
link	Indicates a Layer 2 ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. ● **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services which packets need to be filtered.

Precautions

After you create a named ACL by using the **acl name** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl name** *acl-name* or **undo acl** *acl-number* command to delete the ACL.

When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.

If the number of a named ACL is not specified, the device automatically allocates a number to the named ACL. The following situations are involved:

- If the type of a named ACL is specified, the number of the named ACL allocated by the device is the maximum value of the named ACL of the type.
- If the number and the type of a named ACL are not specified, the device considers the named ACL as the advanced ACL and allocates the maximum value to the named ACL.

The Router does not allocate the number to a named ACL repeatedly.

Example

Create basic ACL 2001 named **test1**.

```
<Huawei> system-view
[Huawei] acl name test1 2001
```

Related Topics

19.7.7 display acl

19.7.4 acl (system view)

Function

The **acl** command creates an ACL with the specified number and enters the ACL view.

The **undo acl** command deletes a specified ACL.

By default, no ACL is created.

Format

acl [**number**] *acl-number* [**match-order** { **auto** | **config** }]

undo acl { [**number**] *acl-number* | **all** }

Parameters

Parameter	Description	Value
number	Specifies the number that identifies an ACL.	-
acl-number	Specifies the number of an ACL.	The value is an integer. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999. ● The number of a Layer 2 ACL ranges from 4000 to 4999. ● The number of a user ACL ranges from 6000 to 6031.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
match-order { **auto** | **config** }	Indicates the matching order of ACL rules. ● **auto**: indicates that ACL rules are matched based on the depth first principle. If the ACL rules are of the same depth first order, they are matched in ascending order of rule IDs. ● **config**: indicates that ACL rules are matched based on the configuration order. The ACL rules are matched based on the configuration order only when the rule ID is not specified. If rule IDs are specified, the ACL rules are matched in ascending order of rule IDs. If the **match-order** parameter is not specified when you create an ACL, the default match order **config** is used.	-
all	Indicates that all ACLs are deleted.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An ACL consists of a series of rules defined by multiple **permit** or **deny** clauses. ACLs are mainly applied to QoS, route filtering, and user access. The major functions of ACLs are as follows:

- Limit data flows to improve network performance. For example, ACLs are configured on an enterprise network to limit video data flows, which lowers the network load and improves network performance.
- Provide flow control. For example, ACLs are used to limit transmission of routing updates so that the bandwidth is saved.
- Provide network access security. For example, ACLs are configured to allow specified users to access the human resource network.

Follow-up Procedure

Run the **rule** command to configure ACL rules and apply the ACL to services which packets need to be filtered.

Precautions

After you create an ACL by using the **acl** command, the ACL still exists even if you exit from the ACL view. You must run the **undo acl** *acl-number* command to delete the ACL.

When you delete an ACL that has been referenced by other services, the services may be interrupted. Before deleting an ACL, ensure that the ACL is not in use.

You are advised not to delete all ACLs because this operation may cause a service interruption.

Example

Create an ACL numbered 2000.

```
<Huawei> system-view
[Huawei] acl number 2000
```

Related Topics

19.7.7 display acl
19.7.18 rule (basic ACL view)
19.7.16 rule (advanced ACL view)
19.7.20 rule (layer 2 ACL view)
19.7.21 rule (user ACL view)

19.7.5 acl logging

Function

The **acl logging** command sets the update interval and aging timeout for the simplified ACL log.

By default, the update interval and aging timeout of the simplified ACL log are 900 seconds.

Format

acl logging { **timeout** | **update** } { *interval* | **default** }

Parameters

Parameter	Description	Value
timeout	Indicates the aging timeout of the simplified ACL log.	-
update	Indicates the update interval of the simplified ACL log.	-
interval	Specifies the value of update interval or aging timeout.	The value is an integer that ranges from 30 to 65535, in seconds.
default	Restores the default update interval or aging timeout.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After simplified ACL is configured, the device periodically (300 seconds earlier or later than the update interval) prints the simplified ACL log entries that have not been aged out. You can check information about the packets matching the simplified ACL. You can use this command to set the update interval and aging timeout of the simplified ACL log.

The display mode of ACL logs is recorded in the **QOS/4/SACL_LOG** log.

Example

Set the update interval of the simplified ACL log to 300 seconds.

```
<Huawei> system-view
[Huawei] acl logging update 300
```

19.7.6 description

Function

The **description** command configures the description of an ACL.

The **undo description** command deletes the description of an ACL.

By default, no description is configured for an ACL.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Describes an ACL.	The value is a string of 1 to 127 case-sensitive characters with spaces supported.

Views

ACL view, ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an ACL, for example, the usage or application scenario of the ACL. It is used to differentiate ACLs.

Prerequisites

The ACL to be described has been created.

Configuration Impact

If you run the **description** command multiple times in the same ACL view, only the latest configuration takes effect.

Example

Configure the description of ACL 2100.

```
<Huawei> system-view
[Huawei] acl 2100
[Huawei-acl-basic-2100] description This acl is used in QoS policy
[Huawei-acl-basic-2100] display acl 2100
Basic ACL 2100, 0 rule
This acl is used in QoS policy
ACL's step is 5
```

Configure the description of ACL6 2100.

```
<Huawei> system-view
[Huawei] acl ipv6 2100
[Huawei-acl6-basic-2000] description This acl6 is used in QoS policy
[Huawei-acl6-basic-2100] display acl ipv6 2100
```

 Copyright © Huawei Technologies Co., Ltd.

```
Basic IPv6 ACL 2100, 0 rule
This acl6 is used in QoS policy
Acl's step is 5
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

19.7.2 acl ipv6 (system view)

19.7.7 display acl

Function

The **display acl** command displays the configuration of an ACL.

Format

display acl { *acl-number* | **name** *acl-name* | **all** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer. • The number of a basic ACL ranges from 2000 to 2999. • The number of a numbered advanced ACL ranges from 3000 to 3999. • The number of a Layer 2 ACL ranges from 4000 to 4999. • The number of a user ACL ranges from 6000 to 6031.
name *acl-name*	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
all	Indicates all ACLs.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **display acl** command displays the ACL configuration.

Configuration Impact

The **display acl** command takes effect only for the MQC service.

Example

Display configuration about the ACL named **test**.

```
<Huawei> display acl name test
Advanced ACL test 3999, 1 rule, match-order is auto
Acl's step is 5
 rule 5 permit ip destination 10.10.10.1 0 (2 matches)
```

Display the ACL configuration.

```
<Huawei> display acl all
 Total quantity of nonempty ACL number is 1

Advanced ACL 3000, 1 rule
Acl's step is 5
 rule 5 permit ip dscp cs1 (2 matches)
```

Table 19-70 Description of the **display acl** command output

Item	Description
Advanced ACL test 3999, 1 rule, match-order is auto	Advanced ACL 3999 named **test** that matches in the automatic order and contains one rule.
Acl's step is 5	The ACL's step is 5. To set the step between ACL rule IDs, run the **step** command.
rule 5 permit ip destination 10.10.10.1 0 (2 matches)	Rule 5 that matches packets whose source IP address is 10.10.10.1. The number of packets that match Rule 5 is 2. If no packet is matched, the **matches** field is not displayed. To modify an advanced ACL rule, run the **rule (advanced ACL view)** command.
Total quantity of nonempty ACL number is 1	One ACL contains rules.
Advanced ACL 3000, 1 rule	Advanced ACL 3000 contains one rule.
rule 5 permit ip dscp cs1 (2 matches)	Rule 5 that matches packets with DSCP priorities. The number of packets that match Rule 5 is 2. To modify an advanced ACL rule, run the **rule (advanced ACL view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.7.4 acl (system view)
19.7.6 description
19.7.18 rule (basic ACL view)
19.7.16 rule (advanced ACL view)
19.7.20 rule (layer 2 ACL view)
19.7.21 rule (user ACL view)
19.7.23 step

19.7.8 display acl ipv6

Function

The **display acl ipv6** command displays the configuration of a specific ACL6 or all ACL6s.

Format

display acl ipv6 { *acl6-number* | **name** *acl6-name* | **all** }

Parameters

Parameter	Description	Value
acl6-number	Specifies an ACL6 number.	The value is an integer that ranges from 2000 to 3999. The ACL6 with a number ranging from 2000 to 2999 is a basic ACL6 and the ACL6 with a number ranging from 3000 to 3999 is an advanced ACL6.
name *acl6-name*	Displays the ACL6 with a specified name.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
all	Displays the configurations of all ACL6s.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display acl ipv6** command displays the ACL6 configuration.

Example

Display the configuration about the ACL6 with the number of 2000.

```
<Huawei> display acl ipv6 2000

Basic IPv6 ACL 2000, 2 rules
Acl's step is 5
 rule 5 deny source 3::/64
 rule 10 permit source 4::/64
```

Display the ACL6 configuration.

```
<Huawei> display acl ipv6 all
 Total nonempty acl6 number is 1

Basic IPv6 ACL 2000, 2 rules
Acl's step is 5
 rule 5 deny source 3::/64
 rule 10 permit source 4::/64 (2 matches)
```

Table 19-71 Description of the display acl ipv6 command output

Item	Description
Total nonempty acl6 number is 1	One ACL6 contains rules.
Basic IPv6 ACL 2000, 2 rules	ACL6 2000, which is a basic ACL6 and has two rules.
Acl's step is 5	ACL's step is 5. To set the step between ACL rule IDs, run the **step** command.
rule 5 deny source 3::/64	ACL6 rule 5, which denies packets with the source IPv6 address 3::/64. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
rule 10 permit source 4::/64 (2 matches)	ACL6 rule 10, which permits packets with the source IPv6 address 4::/64. The number of packets that match Rule 10 is 2. If no packet is matched, the **matches** field is not displayed. To modify a basic ACL6 rule, run the **rule (rule basic acl6 view)** command.

Related Topics

19.7.2 acl ipv6 (system view)
19.7.19 rule (basic ACL6 view)
19.7.17 rule (advanced ACL6 view)
19.7.23 step

19.7.9 display acl resource

Function

The **display acl resource** command displays information about ACL resources.

Format

display acl resource [**slot** *slot-id*]

Parameters

Parameter	Description	Value
slot *slot-id*	Displays ACL rules on the specified LPU. *slot-id* specifies the slot ID of the LPU. ● If the **slot** parameter is not specified, the ACL resources on the SRU are displayed. ● If the **slot** parameter is specified: – When the LAN-side interface card 8FE1GE or 24GE is in the slot specified by *slot-id*, the ACL rules on the Ethernet LAN interface card are displayed. – When a WAN-side card or a LAN-side card of another type is in the slot specified by *slot-id*, the ACL resources on the main control board are displayed.	Set the value according to the device configuration. **NOTE** AR100&AR120&AR150&AR160&AR200 do not support this parameter.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If ACL configuration fails, all the ACL resources on the device may have been used up. You can run the **display acl resource** command to check whether there are available ACL resources (including ACL4 and ACL6).

Example

View ACL rules on the SRU.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display acl resource
 Slot: 0
-----------------------------------------------------------------------
 Type            Total    Reserved    Remaining  Configured
-----------------------------------------------------------------------
 ACL              8192     N/A         6904       1288
 Meter            8192     N/A         8189       3
 Counter          8192     N/A         8188       4
-----------------------------------------------------------------------
```

Table 19-72 Description of the display acl resource command output

Item	Description
Slot: 0	The slot ID of the board is 0.
Type	Resource type. • ACL: all ACL rules. • Meter: ACL rules applied to the traffic classifier that is bound to the traffic policing action. • Counter: ACL rules applied to the traffic classifier.
Total	Total number of ACL rules of the specified type.
Reserved	Number of reserved ACL rules of the specified type.
Remaining	Number of remaining ACL rules of the specified type.
Configured	Number of configured ACL rules of the specified type.

Related Topics

19.7.4 acl (system view)

19.7.10 display time-range

Function

The **display time-range** command displays the configuration and status of the current time range.

Format

display time-range { **all** | *time-name* }

Parameters

Parameter	Description	Value
all	Indicates all the configured time ranges.	-
time-name	Specifies the name of a time range during which ACL rules take effect.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To specify a time range during which ACL rules take effect, run the **time-range** command to configure the time range and reference the time range name when you configure an ACL.

Before using a time range to filter data packets, run the **display time-range** command to view the time range configuration to avoid duplicate time ranges.

NOTE

The device updates the status of ACLs with a delay of about 10 seconds. The **display time-range** command adopts the current time range to determine the status of ACLs; therefore, you may find that the ACL using an active time range is inactive. This is normal.

Example

Display the configuration and status of all time ranges.

```
<Huawei> display time-range all
Current time is 14:48:13 10-17-2012 Wednesday

Time-range : abc (Active)
from 23:23 2012/9/9 to 23:59 2012/12/31
```

Table 19-73 Description of the display time-range command output

Item	Description
Current time is 14:48:13 10-17-2012 Wednesday	The current time is Wednesday 14:48:13 10-17-2012.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Time-range:abc (Active)	The time range is named **abc** and is active. The time range can be: ● Active. ● Inactive.
from 23:23 2012/9/9 to 23:59 2012/12/31	Time range abc is from 23:23 2012/9/9 to 23:59 2012/12/31.

Related Topics

19.7.24 time-range

19.7.11 ip port-set

Function

The **ip port-set** command creates a port set and displays the port set view.

The **undo ip port-set** command deletes a port set.

By default, no port set is created.

Format

ip port-set *port-set-name* **protocol** { **tcp** | **udp** }

undo ip port-set *port-set-name*

Parameters

Parameter	Description	Value
port-set-name	Specifies the port set name.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter, spaces not supported.
protocol { **tcp** | **udp** }	Specifies the protocol type, TCP or UDP.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If an advanced ACL rule matching source or destination port numbers is complex or the same port rules need to be defined for multiple ACL rules, you can configure a port set and bind the port set to the advanced ACL.

Follow-up Procedure

Run the **19.7.12 port (port set view)** command to create port rules for the port set and bind the port set to the advanced ACL.

Precautions

- A port set without port rules cannot be bound to an advanced ACL.
- The protocol type specified in the port set must be the same as the protocol type specified in the advanced ACL.

Example

Create the port set **fromCenter** with the protocol type TCP, configure rules for ACL 3000, and bind the port set **fromCenter** to ACL 3000.

```
<Huawei> system-view
[Huawei] ip port-set fromCenter protocol tcp
[Huawei-port-set-fromCenter] port range 1000 2000
[Huawei-port-set-fromCenter] quit
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit tcp destination-port port-set fromCenter
```

Related Topics

19.7.12 port (port set view)

19.7.16 rule (advanced ACL view)

19.7.12 port (port set view)

Function

The **port** command configures port rules for a port set.

The **undo port** command deletes port rules of a port set.

By default, no port rule is configured.

Format

port [*port-rule-id*] { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }

undo port *port-rule-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
port-rule-id	Specifies the port rule ID. ● If the rule matching the specified ID already exists, the new rule will overwrite the old rule. If no rule matches the specified ID, a rule is created, and inserted into the rule list based on the ID order. ● If a rule is created without specifying its ID, an ID following the existing IDs is automatically allocated to the rule.	The value is an integer that ranges from 0 to 63.
eq *port*	Indicates the port number equivalent to the specified value.	The port number may be a name or numeral. If the port number is a numeral, the value ranges from 0 to 65535.
gt *port*	Indicates the port numbers greater than the specified value.	
lt *port*	Indicates the port numbers smaller than the specified value.	
range *port-start port-end*	Indicates a port number range. *port-start* indicates the start port number, and *port-end* indicates the end port number.	

Views

Port set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When configuring an advanced ACL, you can bind a port set with port rules configured to the advanced ACL, specifying the source or destination port number for the ACL rules.

Prerequisites

The **ip port-set** command has been run to create a port set.

Example

Set the port range to 1000-2000.

```
<Huawei> system-view
[Huawei] ip port-set fromCenter protocol tcp
[Huawei-port-set-fromCenter] port 0 range 1000 2000
```

Related Topics

19.7.11 ip port-set

19.7.13 reset acl counter

Function

The **reset acl counter** command clears statistics about ACLs.

Format

reset acl counter { **name** *acl-name* | *acl-number* | **all** }

Parameters

Parameter	Description	Value
name *acl-name*	Specifies the name of an ACL whose statistics need to be cleared.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
acl-number	Specifies the number of an ACL whose statistics need to be cleared.	The value is an integer. • The number of a basic ACL ranges from 2000 to 2999. • The number of a numbered advanced ACL ranges from 3000 to 3999. • The number of a Layer 2 ACL ranges from 4000 to 4999.
all	Clears all the ACL statistics.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL statistics generated in a certain period, run the **reset acl counter** command to clear existing statistics and start statistics collection.

NOTICE

After the **reset acl counter** command is executed, the system does not prompt you the statistics deletion.

Before using the **reset acl counter** command, determine whether you intend to clear ACL statistics.

Follow-up Procedure

After running the **reset acl counter** command to clear the previous ACL statistics, you can use the **display acl** command to view ACL rules and statistics on the packets matching the ACL rules in the current period.

Example

Clear statistics about ACL 2000.

```
<Huawei> reset acl counter 2000
```

Related Topics

19.7.7 display acl

19.7.14 reset acl ipv6 counter

Function

The **reset acl ipv6 counter** command clears the ACL6 statistics.

Format

reset acl ipv6 counter { **name** *acl6-name* | *acl6-number* | **all** }

Parameters

Parameter	Description	Value
name *acl6-name*	Specifies the name of an ACL6 whose statistics need to be cleared.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).
acl6-number	Specifies the number of an ACL6 whose statistics need to be cleared.	The value is an integer that ranges from 2000 to 3999. ● ACL6s numbered 2000 to 2999 are basic ACL6s. ● ACL6s numbered 3000 to 3999 are advanced ACL6s.
all	Clears all the ACL6 statistics.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain the accurate ACL6 statistics in a certain period, run the **reset acl ipv6 counter** command to clear existing statistics and start statistics collection.

NOTICE

Before using the **reset acl ipv6 counter** command, determine whether you intend to clear ACL6 statistics.

After the **reset acl ipv6 counter** command is executed, the system does not prompt you the statistics deletion.

Follow-up Procedure

After running the **reset acl ipv6 counter** command to clear the previous ACL statistics, you can use the **display acl ipv6** command to view ACL rules and statistics on the packets matching the ACL rules in the current period.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear the statistics about basic ACL6 2000.

```
<Huawei> reset acl ipv6 counter 2000
```

Related Topics

19.7.8 display acl ipv6

19.7.15 reset acl logging

Function

The **reset acl logging** command deletes all simplified ACL logs.

Format

reset acl logging

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

When there are simplified ACL logs that have not been aged out on the device, the device prints these logs at the specified interval. This command can clear all simplified ACL logs on the device, except the printed ones.

Example

Delete all simplified ACL logs on the device.

```
<Huawei> reset acl logging
```

19.7.16 rule (advanced ACL view)

Function

The **rule** command adds or modifies an advanced ACL rule.

The **undo rule** command deletes an advanced ACL rule.

By default, no advanced ACL rule is configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

- When the Internet Control Management Protocol (ICMP) is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When the Transmission Control Protocol (TCP) is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When the User Datagram Protocol (UDP) is used, run:

  rule [*rule-id*] { **deny** | **permit** }{ *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When GRE, IGMP, IPinIP, or OSPF is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- When the IP protocol version is IPv4, run:

  rule [*rule-id*] { **deny** | **permit** } **ip** [**destination** { *destination-address destination-wildcard* | **any** } | **source** { *source-address source-wildcard* | **any** } | **logging** | **time-range** *time-name* | **vpn-instance** *vpn-instance-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | [**fragment** | **none-first-fragment**] | **vni** *vni-id*] *

- To delete an advanced ACL rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | **icmp-type** | **source** | **source-port** | **tcp-flag** | **logging** | **time-range** | **vpn-instance** | [**dscp** | [**tos** | **precedence**] *] | [**fragment** | **none-first-fragment**]] *

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
protocol-number	Indicates the protocol type expressed by name or number. **NOTE** Parameters in an ACL vary with the protocol type. The combination of **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } and **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } is applicable to TCP and UDP only.	The value expressed by number is an integer that ranges from 1 to 255. The value expressed by name can be **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **ospf**, **tcp**, or **udp**. **icmp**, **tcp**, **udp**, **gre**, **igmp**, **ipinip**, and **ospf** correspond to 1, 6, 17, 47, 2, 4, and 89.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination { *destination-address destination-wildcard* | **any** }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. • *destination-address*: specifies the destination IP address of data packets. • *destination-wildcard*: specifies the wildcard mask of the destination IP address. • **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 or the value of *destination-wildcard* is 255.255.255.255.	*destination-address*: The value is in dotted decimal notation. *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
icmp-type { *icmp-name* | *icmp-type icmp-code* }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. • *icmp-name*: specifies the name of ICMP packets. • *icmp-type*: specifies the type of ICMP packets. • *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. **Table 19-75** lists the mapping between ICMP names and ICMP types and codes.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source { *source-address source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. ● *source-address*: specifies the source IP address of packets. ● *source-wildcard*: specifies the wildcard mask of the source IP address. ● **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address* : The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value is a string of 1 to 32 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: ● **eq** *port*: equivalent to the destination port number. ● **gt** *port*: greater than the destination port number. ● **1t** *port*: smaller than the destination port number. ● **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number. ● **port-set** *port-set-name*: binds a port set to specify destination ports.	● The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. ● The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. ● *port-set-name* is the name of an existing port set.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* | **port-set** *port-set-name* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: • **eq** *port*: equivalent to the source port number. • **gt** *port*: greater than the source port number. • **1t** *port*: smaller than the source port number. • **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number. • **port-set** *port-set-name*: binds a port set to specify source ports.	• The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. • The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535. • *port-set-name* is the name of an existing port set.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to firewall and IPSec features.	The value is a string of 1 to 31 characters without spaces. Letters, digits, underscores (_), and dots (.) are allowed.

Parameter	Description	Value
dscp *dscp*	Specifies the value of a Differentiated Services Code Point (DSCP). **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value is an integer or a name. • The value ranges from 0 to 63 when it is an integer. • When it is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. • The value ranges from 0 to 15 when it is an integer. • When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 19-74** describes the mapping between ToS names and values.
precedence *precedence*	Indicates that packets are filtered based on the precedence field. *precedence* specifies the precedence value.	The value ranges from 0 to 7. The values 0 to 7 correspond to *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network*.
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain fragment or none-first-fragment parameters are valid for all packets.	-
vni *vni-id*	Specifies the VNI ID of the packets that match the rule. **NOTE** This parameter is valid only in the VXLAN scenario.	The value is an integer that ranges from 0 to 16777215.
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-

Table 19-74 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 19-75 Mapping between ICMP names and ICMP types and codes

icmp-name	icmp-type	icmp-code
Echo	8	0
Echo-reply	0	0

 Copyright © Huawei Technologies Co., Ltd.

icmp-name	icmp-type	icmp-code
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0
Information-request	15	0
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0

Views

Advanced ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An advanced ACL matches packets based on information such as source and destination IP addresses, source and destination port numbers, and protocol types.

The **rule** command defines the time range and flexibly configures the time ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

- If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.
- To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.
- The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to firewall and IPSec features.
- To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.
- When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.
- The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.
- When an advanced ACL rule whose ToS value is 1 is configured on the device, fast forwarding is disabled on the interface.
- A port set without port rules cannot be bound to an advanced ACL.
- The protocol type specified in the port set must be the same as the protocol type specified in the advanced ACL.

Example

Add a rule to ACL 3000 to filter ICMP packets.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 1 permit icmp
```

Delete a rule from ACL 3000.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] undo rule 1
```

Add a rule to ACL 3000 to filter IGMP packets.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 2 permit igmp
```

Add a rule to ACL 3000 to filter packets with DSCP priorities.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 3 permit ip dscp cs1
```

Add a rule to ACL 3001 to filter all the IP packets sent from hosts at 10.9.0.0 to hosts at 10.38.160.0.

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit ip source 10.9.0.0 0.0.255.255 destination 10.38.160.0 0.0.0.255
```

Add a rule to ACL 3001 to filter the packets with source UDP port number 128 from 10.9.8.0 to 10.38.160.0.

```
<Huawei> system-view
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit udp source 10.9.8.0 0.0.0.255 destination 10.38.160.0 0.0.0.255
destination-port eq 128
```

Add a rule to ACL 3000 to filter tcp-flag packets.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit tcp tcp-flag established
```

Related Topics

19.7.4 acl (system view)
19.7.3 acl name
19.7.7 display acl
19.7.23 step

19.7.17 rule (advanced ACL6 view)

Function

The **rule** command adds or modifies an advanced ACL6 rule.

The **undo rule** command deletes an ACL6 rule.

By default, no advanced ACL6 rule is created.

Format

- When **protocol** is set to TCP, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** | **established** } * | **logging** | **time-range** *time-name* | **tos** *tos*] *

- When **protocol** is set to UDP, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **dscp** *dscp* | **precedence** *precedence* | **source** { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- When **protocol** is set to ICMPv6, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmpv6** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-*

length | **any** } | **dscp** *dscp* | **icmp6-type** { *icmp6-type-name* | *icmp6-type icmp6-code* } | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- When **protocol** is set to IPv6, the command format of an advanced ACL6 rule is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **ipv6** } [**destination** { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* } | **dscp** *dscp* | [**fragment** | **none-first-fragment**] | **precedence** *precedence* | **source** { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- When GRE or OSPF is used, run:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **ospf** } [**destination** { *destination-ipv6-address prefix-length* | *destination-ipv6-address/prefix-length* | **any** } | **dscp** *dscp* | **precedence** *precedence* | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name* | **tos** *tos*] *

- Rule for deleting an advanced ACL6:

  undo rule *rule-id* [**destination** | **destination-port** | [**fragment** | **none-first-fragment**] | **icmp6-type** | **precedence** | **source** | **source-port** | **logging** | **time-range** | **tos**] *

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL6 rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step value, the device creates ACL6 rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL6 rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Indicates to drop packets conforming to certain conditions.	-
permit	Indicates to forward packets conforming to certain conditions.	-
tcp	Specifies the protocol type is TCP.	-
udp	Specifies the protocol type is UDP.	-
icmpv6	Specifies the protocol type is ICMPv6.	-
protocol-number	Specifies the protocol type that is expressed as a name or a number.	The value ranges from 1 to 255. The protocol type expressed as a name can be GRE, ICMPv6, IPv6, OSPF, TCP, and UDP.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination { [**pd** *prefix*] *destination-ipv6-address prefix-length* | [**pd** *prefix*] *destination-ipv6-address/prefix-length* | **any** | **pd** *destination-dhcpv6-prefix* }	Indicates the destination address and prefix of a packet. • The **pd** *prefix destination-ipv6-address prefix-length* specifies an IPv6 prefix and a destination IPv6 address, based on which a new IPv6 destination address is calculated through OR operation. An ACL6 rule matches the destination IPv6 addresses of packets against this new IPv6 address. • The **pd** *destination-dhcpv6-prefix* parameter specifies an IPv6 address prefix obtained by a DHCPv6 PD client. An ACL6 rule matches the IPv6 address assigned based on this IPv6 address prefix as the destination IP address of packets.	• The value of *prefix* is a string of 1 to 63 characters. • *destination-ipv6-address* is expressed in hexadecimal notation. The value of *prefix-length* is an integer that ranges from 1 to 128. • **any** represents any source address. • The value of *destination-dhcpv6-prefix* is a string of 1 to 63 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
dscp *dscp*	Specifies the Differentiated Services Code Point (DSCP) value. **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value of *dscp* can be an integer or a name. When the value is an integer, the value ranges from 0 to 63. When the value is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain **fragment** and **none-first-fragment** parameters are valid for all packets.	-
precedence *precedence*	Indicates that the packets are filtered according to the precedence field.	**precedence** can be expressed as a name or a number. The number ranges from 0 to 7.
source { [**pd** *prefix*] *source-ipv6-address prefix-length* | [**pd** *prefix*] *source-ipv6-address/prefix-length* | **any** | **pd** *source-dhcpv6-prefix* }	Indicates the source address and prefix of a packet. • The **pd** *prefix source-ipv6-address prefix-length* specifies an IPv6 prefix and a source IPv6 address, based on which a new IPv6 source address is calculated through OR operation. An ACL6 rule matches the source IPv6 addresses of packets against this new IPv6 address. • The **pd** *source-dhcpv6-prefix* parameter specifies an IPv6 address prefix obtained by a DHCPv6 PD client. An ACL6 rule matches the IPv6 address assigned based on this IPv6 address prefix as the source IP address of packets.	• The value of *prefix* is a string of 1 to 63 characters. • *source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128. • **any** represents any source address. • The value of *source-dhcpv6-prefix* is a string of 1 to 63 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: ● **eq** *port*: equivalent to the destination port number. ● **gt** *port*: greater than the destination port number. ● **1t** *port*: smaller than the destination port number. ● **range** *port-start port-end*: destination port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: ● **eq** *port*: equivalent to the source port number. ● **gt** *port*: greater than the source port number. ● **1t** *port*: smaller than the source port number. ● **range** *port-start port-end*: source port number range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or a number. When the value is expressed as a number, it ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp6-type { *icmp6-type-name* | *icmp6-type icmp6-code* }	Indicates that the type and code of ICMPv6 packets, which is effective only when the packet protocol is ICMP. If this parameter is not specified, all ICMP packets are matched.	*icmp6-type*: indicates the type of ICMP messages. The value ranges from 0 to 255. *icmp6-code*: indicates the type of ICMP messages. The value ranges from 0 to 255. The value of *icmp6-type-name* and the corresponding ICMP-Type and ICMP-Code are as **Table 19-76**.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Specifies the type of the SYN Flag in the TCP packet header is ack(010000).	-
fin	Specifies the type of the SYN Flag in the TCP packet header is fin(000001).	-
psh	Specifies the type of the SYN Flag in the TCP packet header is psh(001000).	-
rst	Specifies the type of the SYN Flag in the TCP packet header is rst(000100).	-
syn	Specifies the type of the SYN Flag in the TCP packet header is syn(000010).	-
urg	Specifies the type of the SYN Flag in the TCP packet header is urg(100000).	-
established	Indicates that the SYN Flag type in the TCP packet header is ack(010000) or rst(000100).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. ● The value ranges from 0 to 15 when it is an integer. ● When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 19-74** describes the mapping between ToS names and values.

Table 19-76 Values of *icmp6-type-name* and the corresponding ICMP-Type and ICMP-Code

icmp6-type-name	icmp-type	icmp-code
Redirect	137	0
Echo	128	0
Echo-reply	129	0
Err-Header-field	4	0
Frag-time-exceeded	3	1
Hop-limit-exceeded	3	0
Host-admin-prohib	1	1
Host-unreachable	1	3
Neighbor-advertisement	136	0
Neighbor-solicitation	135	0

 Copyright © Huawei Technologies Co., Ltd.

icmp6-type-name	icmp-type	icmp-code
Network-unreachable	1	0
Packet-too-big	2	0
Port-unreachable	1	4
Router-advertisement	134	0
Router-solicitation	133	0
Unknown-ipv6-opt	4	2
Unknown-next-hdr	4	1

Views

Advanced ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Advanced ACL6s classify data packets based on the source IP address, destination IP address, source port number, destination port number, and protocol type.

The **rule** command defines the time range and flexibly configures the time ACL6 rules take effect.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

- If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.
- To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.
- To configure both the **precedence** *precedence* and **tos** *tos* parameters, set the two parameters consecutively in the command.
- Only the packet filtering firewall service supports the **rule (advanced ACL6 view)** command to configure ACL6 rules to match the IPv6 address, which is assigned based on the IPv6 address prefix obtained by a DHCPv6 client, as the source or destination IP address of packets. In the same ACL6 rule, **destination pd** *destination-dhcpv6-prefix* and **source pd** *source-dhcpv6-prefix* parameters cannot be configured simultaneously.

 Copyright © Huawei Technologies Co., Ltd.

- When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.
- The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Exercise caution when you run the **undo rule** command.
- A DHCPv6 PD client does not support the depth first principle.

Example

Add a rule to ACL6 3000 to deny the packets with the source UDP port number that is greater than 128 from fc00:1::1 to fc00:3::1.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule deny udp source fc00:1::1 64 destination fc00:3::1 64 destination-port gt 128
```

Add a rule to ACL6 3000 to filter tcp-flag packets.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule permit tcp tcp-flag established
```

Related Topics

19.7.2 acl ipv6 (system view)

19.7.1 acl ipv6 name

19.7.8 display acl ipv6

19.7.18 rule (basic ACL view)

Function

The **rule** command adds or modifies a basic ACL rule.

The **undo rule** command deletes a basic ACL rule.

By default, no rule is configured for a basic ACL.

Format

rule [*rule-id*] { **deny** | **permit** } [**source** { *source-address source-wildcard* | **any** } | **vpn-instance** *vpn-instance-name* | [**fragment** | **none-first-fragment**] | **logging** | **time-range** *time-name*] *

undo rule *rule-id* [**source** | **logging** | **time-range** | **vpn-instance** | [**fragment** | **none-first-fragment**]] *

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match a rule.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source { *source-address source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. ● *source-address*: specifies the source IP address of packets. ● *source-wildcard*: specifies the wildcard mask of the source IP address. ● **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 or the value of *source-wildcard* is 255.255.255.255.	*source-address* : The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance. **NOTE** The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to the firewall feature.	The value is a string of 1 to 31 characters without spaces. Letters, digits, underscores (_), and dots (.) are allowed.
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain **fragment** and **none-first-fragment** parameters are valid for all packets.	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value is a string of 1 to 32 characters.

Views

Basic ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL matches packets based on information such as source IP addresses, fragment flags, and time ranges.

The **rule** command defines the time range and flexibly configures the time ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.

The ACL with the **vpn-instance** *vpn-instance-name* parameter specified is only applied to the firewall feature.

When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.

Example

Add a rule in ACL 2001 to permit the packets from 192.168.32.1.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule permit source 192.168.32.1 0
```

Delete rule 5 from ACL 2001.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] undo rule 5
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

19.7.7 display acl

19.7.23 step

19.7.19 rule (basic ACL6 view)

Function

The **rule** command adds or modifies basic ACL6 rules.

The **undo rule** command deletes an ACL6 rule.

By default, there is no basic ACL6 rule.

Format

rule [*rule-id*] { **deny** | **permit** } [[**fragment** | **none-first-fragment**] | **source** { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* | **any** } | **logging** | **time-range** *time-name*] *

undo rule *rule-id* [[**fragment** | **none-first-fragment**] | **source** | **logging** | **time-range**] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of a rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL6 rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step value, the device creates ACL6 rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL6 rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Indicates to drop packets conforming to certain conditions.	-
permit	Indicates to forward packets conforming to certain conditions.	-
logging	Specifies the log recording the IP information, port number, and protocol type of the packets that match the rule. **NOTE** The **logging** only takes effect when the **traffic-filter** command references ACLs.	-
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-
none-first-fragment	Indicates that the rule is valid for only non-initial fragments. If this parameter is specified, the rule is valid for only non-initial fragments. **NOTE** The rules that do not contain fragment and none-first-fragment parameters are valid for all packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source { *source-ipv6-address prefix-length* | *source-ipv6-address/prefix-length* }	Indicates the source address and prefix of a packet.	*source-ipv6-address* indicates the source address and is expressed in hexadecimal notation. *prefix-length* is an integer that ranges from 1 to 128.
any	Indicates any source address.	-
time-range *time-name*	Indicates that the configured ACL6 rule is effective only in the specified time range. *time-name* indicates the name of the time range during which the ACL6 rule takes effect. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL6, if the specified *time-name* does not exit, the ACL6 does not take effect.	The value of *time-name* is a string of 1 to 32 characters.

Views

Basic ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A basic ACL6 matches packets based on information such as source IP addresses, fragment flags, and time ranges.

Prerequisites

An ACL6 has been created before the rule is configured.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.

When you use the **undo rule** command to delete an ACL6 rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl ipv6** command to view the rule ID.

The **undo rule** command deletes an ACL6 rule even if the ACL6 rule is referenced. Exercise caution when you run the **undo rule** command.

Example

Add a rule for the ACL6 with a number of 2000 to prohibit the passing of packets from the source fc00:1::1/64.

```
<Huawei> system-view
[Huawei] acl ipv6 2000
[Huawei-acl6-basic-2000] rule deny source fc00:1::1/64
```

Related Topics

19.7.2 acl ipv6 (system view)

19.7.1 acl ipv6 name

19.7.8 display acl ipv6

19.7.20 rule (layer 2 ACL view)

Function

The **rule** command adds or modifies a Layer 2 ACL rule.

The **undo rule** command deletes a Layer 2 ACL rule.

By default, there is no rule in the related Layer 2 ACL view.

Format

rule [*rule-id*] { **permit** | **deny** } [**l2-protocol** *type-value* [*type-mask*] | **destination-mac** *dest-mac-address* [*dest-mac-mask*] | **source-mac** *source-mac-address* [*source-mac-mask*] | **vlan-id** *vlan-id* [*vlan-id-mask*] | **8021p** *802.1p-value* | **time-range** *time-name*] *

undo rule *rule-id*

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule overwrites the old rule. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically by the device starts from the step value. The default step value is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on. The specified *rule-id* is valid only when the **config** mode is used. When the **auto** mode is used, the specified *rule-id* is invalid, and the device automatically assigns rule IDs to the ACL rules using the depth first algorithm.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match a rule.	-
permit	Permits the packets that match a rule.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
l2-protocol *type-value* [*type-mask*]	Indicates the type of a Layer 2 protocol. This parameter corresponds to the Ethernet type of Ethernet_II frames and the type-code domain of Ethernet_SNAP frames. ● *type-value*: specifies the type value of a Layer 2 protocol. ● *type-mask*: specifies the type mask of a Layer 2 protocol.	*type-value* can be a hexadecimal number of 3 to 6 bits that ranges from 0x600 to 0xFFFF or the following protocol name: ● ARP, corresponding to 0x0806 ● IP, corresponding to 0x0800 ● MPLS, corresponding to 0x8847 ● RARP, corresponding to 0x8035 The default value of *type-mask* is 0xffff.
destination-mac *dest-mac-address* [*dest-mac-mask*]	Specifies the destination MAC address of packets that matches ACL rules. If the parameter is not specified, packets with any destination address are matched. ● *dest-mac-address* specifies the destination MAC address of packets. ● *dest-mac-mask* specifies the mask of the destination MAC address of packets.	*dest-mac-address* and *dest-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *dest-mac-mask* is ffff-ffff-ffff. You can obtain the required destination MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-mac *source-mac-address* [*source-mac-mask*]	Specifies the source MAC address of packets that matches ACL rules. If this parameter is not specified, the packets with any source MAC address are matched. ● *source-mac-address* specifies the source MAC address of packets. ● *source-mac-mask* specifies the mask of the source MAC address of packets. If this parameter is not specified, the mask is ffff-ffff-ffff.	*source-mac-address* and *source-mac-mask* are both in the format of H-H-H. Each H stands for one to four hexadecimal digits. The default value of the *source-mac-mask* is ffff-ffff-ffff. You can obtain the required source MAC address range by specifying *source-mac-address* and *source-mac-mask*. For example, 00e0-fc01-0101 ffff-ffff-ffff specifies a MAC address 00e0-fc01-0101, whereas 00e0-fc01-0101 ffff-ffff-0000 specifies a MAC address range from 00e0-fc01-0000 to 00e0-fc01-ffff.
vlan-id *vlan-id* [*vlan-id-mask*]	Indicates the outer VLAN ID contained in a packet that matches the rule. ● *vlan-id*: specifies the number of the VLAN ID. ● *vlan-id-mask*: specifies the mask of the VLAN ID. If this parameter is not specified, the mask is 0xFFF.	The value of *vlan-id* is an integer ranging from 1 to 4094. The value of the *vlan-id-mask* is a hexadecimal number ranging from 0x0 to 0xFFF. The default value is 0xFFF.
8021p *802.1p-value*	Indicates the 802.1p priority in the outer VLAN tag of a packet that matches the rule.	The value is an integer ranging from 0 to 7.
time-range *time-name*	Defines the time range during which an ACL rule is valid. *time-name* specifies the name of a time range. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value of *time-name* is a string of 1 to 32 characters.

Views

layer 2 ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Layer 2 ACL matches packets based on Layer 2 information of the packets, such as source MAC addresses, destination MAC addresses, and Layer 2 protocol types.

The **rule** command defines the time range and flexibly configures the time when the ACL rules take effect.

Prerequisites

An ACL has been created before the rule is configured.

Precautions

If the specified rule ID already exists, the new rule overwrites the old rule no matter whether the rules conflict.

To modify an existing rule, delete the old rule, and then create a new rule. Otherwise, the configuration result may be incorrect.

When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.

Example

Add a rule to ACL 4001 to match packets with the destination MAC address being 0000-0000-0001, source MAC address being 0000-0000-0002, and the value of the Layer 2 protocol type being 0x0800.

```
<Huawei> system-view
[Huawei] acl 4001
[Huawei-acl-L2-4001] rule permit destination-mac 0000-0000-0001 source-mac 0000-0000-0002 l2-protocol 0x0800
```

Related Topics

19.7.4 acl (system view)

19.7.3 acl name

19.7.7 display acl

19.7.23 step

 Copyright © Huawei Technologies Co., Ltd.

19.7.21 rule (user ACL view)

Function

The **rule** command configures a user ACL rule.

The **undo rule** command deletes a user ACL rule.

By default, no user ACL rule is configured.

Format

- When the parameter *protocol* is specified as the ICMP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **icmp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **icmp-type** { *icmp-name* | *icmp-type icmp-code* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the parameter *protocol* is specified as the TCP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **tcp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **tcp-flag** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** } * | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the parameter *protocol* is specified as the UDP, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **udp** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **source** { *source-address source-wildcard* | **any** } | **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- When the parameter *protocol* is specified as the GRE, IGMP, IP, IPINIP, or OSPF, the command format is as follows:

  rule [*rule-id*] { **deny** | **permit** } { *protocol-number* | **gre** | **igmp** | **ip** | **ipinip** | **ospf** } [**destination** { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* } | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-name* | [**dscp** *dscp* | [**tos** *tos* | **precedence** *precedence*] *] | **fragment**] *

- To delete an ACL rule, run:

  undo rule *rule-id* [**destination** | **destination-port** | **icmp-type** | **source** | **source-port** | **tcp-flag** | **time-range** | **dscp** | **tos** | **precedence** | **fragment**] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule. ● If the specified rule ID has been created, the new rule is added to the rule with this ID, that is, the old rule is modified. If the specified rule ID does not exist, the device creates a rule and determines the position of the rule according to the ID. ● If the rule ID is not specified, the device allocates an ID to the new rule. The rule IDs are sorted in ascending order. The device automatically allocates IDs according to the step. The step value is set by using the **step** command. **NOTE** ACL rule IDs assigned automatically start from the step value. The default step is 5. With this step, the device creates ACL rules with IDs being 5, 10, 15, and so on.	The value is an integer that ranges from 0 to 4294967294.
deny	Denies the packets that match the rule.	-
permit	Permits the packets that match the rule.	-
icmp	Indicates that the protocol type is ICMP. The value 1 indicates that ICMP is specified.	-
tcp	Indicates that the protocol type is TCP. The value 6 indicates that TCP is specified.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
udp	Indicates that the protocol type is UDP. The value 17 indicates that UDP is specified.	-
protocol-number	Indicates the protocol type expressed by name or number. **NOTE** Parameters in an ACL vary with the protocol type. The combination of **source-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } and **destination-port** { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* } is applicable to TCP and UDP only.	The value expressed by number is an integer that ranges from 1 to 255. The value expressed by name can be **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **ospf**, **tcp**, or **udp**. **icmp**, **tcp**, **udp**, **gre**, **igmp**, **ipinip**, and **ospf** correspond to 1, 6, 17, 47, 2, 4, and 89.
source { *source-address source-wildcard* | **any** }	Indicates the source IP address of packets that match an ACL rule. If this parameter is not specified, packets with any source IP address are matched. ● *source-address*: specifies the source IP address of packets. ● *source-wildcard*: specifies the wildcard mask of the source IP address. ● **any**: indicates any source IP address of packets. That is, the value of *source-address* is 0.0.0.0 and the value of *source-wildcard* is 255.255.255.255.	*source-address*: The value is in dotted decimal notation. *source-wildcard*: The value is in dotted decimal notation. The wildcard mask of the source IP address can be 0, equivalent to 0.0.0.0, indicating that the source IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination { *destination-address destination-wildcard* | **any** | **passthrough-domain** *domain-string* }	Indicates the destination IP address of packets that match ACL rules. If this parameter is not specified, packets with any destination IP address are matched. ● *destination-address*: specifies the destination IP address of data packets. ● *destination-wildcard*: specifies the wildcard mask of the destination IP address. ● **any**: indicates any destination IP address of packets. That is, the value of *destination-address* is 0.0.0.0 and the value of *destination-wildcard* is 255.255.255.255. ● **passthrough-domain** *domain-string*: indicates the destination domain name of permitted packets. **NOTE** The **passthrough-domain** *domain-string* parameter is valid only when the **permit** parameter is specified.	*destination-address*: The value is in dotted decimal notation. *destination-wildcard*: The value is in dotted decimal notation. The wildcard mask of the destination IP address can be 0, equivalent to 0.0.0.0, indicating that the destination IP address is the host address. **NOTE** The wildcard is in dotted decimal format. After the value is converted to a binary number, the value 0 indicates that the IP address needs to be matched and the value 1 indicates that the IP address does not need to be matched. The values 1 and 0 can be discontinuous. For example, the IP address 192.168.1.169 and the wildcard 0.0.0.172 represent the website 192.168.1.x0x0xx01. The value x can be 0 or 1. *domain-string*: The value is a string of 3 to 137 characters. The value of *domain-string* must meet the following requirements: ● The value cannot contain two consecutive dots (..). ● If you use the fuzzy match function, the first character can be set to *, and * can only be used as the first character of the domain name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
icmp-type { *icmp-name* | *icmp-type icmp-code* }	Indicates the type and code of ICMP packets, which are valid only when the protocol of packets is ICMP. If this parameter is not specified, all types of ICMP packets are matched. • *icmp-name*: specifies the name of ICMP packets. • *icmp-type*: specifies the type of ICMP packets. • *icmp-code*: specifies the code of ICMP packets.	*icmp-type* is an integer that ranges from 0 to 255. *icmp-code* is an integer that ranges from 0 to 255. **NOTE** Table 19-78 lists the mapping between ICMP names and ICMP types and codes.
source-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the source port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any source port are matched. The operators are as follows: • **eq** *port*: equal operator. • **gt** *port*: greater than operator. • **1t** *port*: smaller than operator. • **range** *port-start port-end*: within the range. *port-start* specifies the start port number, and *port-end* specifies the end port number.	The value of *port* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-port { **eq** *port* | **gt** *port* | **lt** *port* | **range** *port-start port-end* }	Specifies the destination port of UDP or TCP packets. The value is valid only when the protocol of packets is TCP or UDP. If this parameter is not specified, TCP or UDP packets with any destination port are matched. The operators are as follows: ● **eq** *port*: equal operator. ● **gt** *port*: greater than operator. ● **1t** *port*: smaller than operator. ● **range** *port-start port-end*: within the range. *port-start* specifies the start port number. *port-end* specifies the end port number.	The value of *port* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535 in **eq** *port*, from 0 to 65535 in **gt** *port*, and from 0 to 65535 in **lt** *port*. The value of *port-start* and *port-end* can be a name or an integer. When the value is expressed as an integer, it ranges from 0 to 65535.
tcp-flag	Indicates the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ack (010000).	-
fin	Indicates that the SYN Flag type in the TCP packet header is fin (000001).	-
psh	Indicates that the SYN Flag type in the TCP packet header is psh (001000).	-
rst	Indicates that the SYN Flag type in the TCP packet header is rst (000100).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
syn	Indicates that the SYN Flag type in the TCP packet header is syn (000010).	-
urg	Indicates that the SYN Flag type in the TCP packet header is urg (100000).	-
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules take effect at any time. **NOTE** When you specify the **time-range** parameter to reference a time range to the ACL, if the specified *time-name* does not exit, the ACL does not take effect.	The value is a string of 1 to 32 characters.
dscp *dscp*	Specifies the value of a Differentiated Services Code Point (DSCP). **NOTE** The **dscp** *dscp* and **precedence** *precedence* parameters cannot be set for the same rule. The **dscp** *dscp* and **tos** *tos* parameters cannot be set for the same rule.	The value is an integer or a name. ● The value ranges from 0 to 63 when it is an integer. ● When it is a name, the value can be af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, or ef.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tos *tos*	Indicates that packets are filtered according to the Type of Service (ToS).	The value is an integer or a name. • The value ranges from 0 to 15 when it is an integer. • When the value is a name, the value can be normal, min-monetary-cost, max-reliability, max-throughput, or min-delay. **Table 19-77** describes the mapping between ToS names and values.
precedence *precedence*	Indicates that packets are filtered based on the precedence field. *precedence* specifies the precedence value.	The value ranges from 0 to 7. The values 0 to 7 correspond to *routine*, *priority*, *immediate*, *flash*, *flash-override*, *critical*, *internet*, and *network*.
fragment	Indicates that the rule is valid for all fragments. If this parameter is specified, the rule is valid for all fragments.	-

Table 19-77 Mapping between ToS names and values

ToS Name	Value	ToS Name	Value
normal	0	max-reliability	2
min-monetary-cost	1	max-throughput	4
min-delay	8	-	-

Table 19-78 Mapping between ICMP names and ICMP types and codes

icmp-name	icmp-type	icmp-code
Echo	8	0
Echo-reply	0	0

 Copyright © Huawei Technologies Co., Ltd.

icmp-name	icmp-type	icmp-code
Fragmentneed-DFset	3	4
Host-redirect	5	1
Host-tos-redirect	5	3
Host-unreachable	3	1
Information-reply	16	0
Information-request	15	0
Net-redirect	5	0
Net-tos-redirect	5	2
Net-unreachable	3	0
Parameter-problem	12	0
Port-unreachable	3	3
Protocol-unreachable	3	2
Reassembly-timeout	11	1
Source-quench	4	0
Source-route-failed	3	5
Timestamp-reply	14	0
Timestamp-request	13	0
Ttl-exceeded	11	0

Views

User ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A user ACL matches packets based on information such as source IP addresses, destination IP addresses, source port numbers, destination port numbers, and protocol types.

Currently, the user ACL can only be applied to the NAC feature.

Precautions

If the specified rule ID already exists and the new rule conflicts with the original rule, the new rule replaces the original rule.

When you use the **undo rule** command to delete an ACL rule, the rule ID must exist. If the rule ID is unknown, you can use the **display acl** command to view the rule ID.

The **undo rule** command deletes an ACL rule even if the ACL rule is referenced. Exercise caution when you run the **undo rule** command.

The **passthrough-domain** *domain-string* parameter can specify the name of the domain in which packets can pass. When you attempt to use a UC browser to visit the domain addresses (website addresses) in the whitelist, you may fail to access the websites or response is slow.

Example

Add a rule to ACL 6000 to match all IP packets with destination domain name **www.huawei.com**.

```
<Huawei> system-view
[Huawei] acl 6000
[Huawei-acl-ucl-6000] rule permit ip destination passthrough-domain www.huawei.com
```

Add a rule to ACL 6000 to match all IP packets with destination domain name ***.huawei.com**.

```
<Huawei> system-view
[Huawei] acl 6000
[Huawei-acl-ucl-6000] rule permit ip destination passthrough-domain *.huawei.com
```

Related Topics

19.7.4 acl (system view)
19.7.7 display acl

19.7.22 rule description

Function

The **rule description** command configures the description of an ACL rule.

The **undo rule description** command deletes the description of an ACL rule.

By default, no description is configured for an ACL rule.

Format

rule *rule-id* **description** *description*

undo rule *rule-id* **description**

Parameters

Parameter	Description	Value
rule-id	Specifies the ID of an ACL rule.	The value is an integer that ranges from 0 to 4294967294.
description *description*	Specifies the description of an ACL rule. You can configure the description to record an ACL rule in detail.	The value is a character string and contains a maximum of 127 characters.

Views

ACL view, ACL6 view

Default Level

2: Configuration level

Usage Guidelines

Application Scenarios

The *rule-id* parameter identifies a rule, but cannot describe the meaning and usage of the rule. The description with a character string can be used to solve the problem.

Prerequisites

The ACL rule has been created. If the ACL rule does not exist, the system displays an error message when you run this command.

Precautions

If the **rule description** command is run repeatedly, the latest configuration takes effect.

After you run the **undo rule** *rule-id* command, the rule and rule description are deleted.

Example

Configure the description for rule 5 in acl 2001, which permits the packets from 192.168.32.1.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule 5 permit source 192.168.32.1 0
[Huawei-acl-basic-2001] rule 5 description permit 192.168.32.1
[Huawei-acl-basic-2001] display acl 2001
Basic ACL 2001, 1 rule
Acl's step is 5
```

```
rule 5 permit source 192.168.32.1 0
rule 5 description permit 192.168.32.1
```

Related Topics

19.7.18 rule (basic ACL view)
19.7.16 rule (advanced ACL view)
19.7.20 rule (layer 2 ACL view)
19.7.17 rule (advanced ACL6 view)
19.7.19 rule (basic ACL6 view)
19.7.7 display acl
19.7.8 display acl ipv6

19.7.23 step

Function

The **step** command sets the step between ACL rule IDs.

The **undo step** command restores the default step between ACL rule IDs.

By default, the step between ACL rule IDs is 5.

Format

step *step*

undo step

Parameters

Parameter	Description	Value
step	Specifies the step between ACL rule IDs.	The value is an integer that ranges from 1 to 20.

Views

ACL view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The step is the difference between rule IDs when the system automatically assigns rule IDs. For example, if the ACL step value is set to 5, rules are numbered 5, 10, 15, and so on.

 Copyright © Huawei Technologies Co., Ltd.

To add a rule between existing rules, you need to reset the step. For example, an ACL in **config** mode contains three rules with IDs being 5, 10, and 15. To insert a new rule after rule 5 (the first rule), run the **rule 7** *xxxx* command to insert rule 7.

If the step value is changed, ACL rule IDs are arranged automatically. For example, if the original rule IDs are 5, 10, and 15, the rule IDs become 2, 4, and 6 after you change the step value to 2.

NOTE

The **undo step** command can be used to realign ACL rule IDs immediately based on the default step. For example, ACL rule group 3001 contains four rules with IDs being 1, 3, 5, and 7, and the step is 2. After the **undo step** command is executed, the rule IDs become 5, 10, 15, and 20 and the step value is restored to 5.

Prerequisites

An ACL has been created by running the **acl** command.

Example

Set the step between rules in ACL 3101 to 2.

```
<Huawei> system-view
[Huawei] acl 3101
[Huawei-acl-adv-3101] step 2
```

Set the step between rules in ACL6 3101 to 2.

```
<Huawei> system-view
[Huawei] acl ipv6 3101
[Huawei-acl6-adv-3101] step 2
```

Related Topics

19.7.4 acl (system view)
19.7.3 acl name

19.7.24 time-range

Function

The **time-range** command sets a time range.

The **undo time-range** command deletes a time range.

By default, no time range is set.

Format

time-range *time-name* { *start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*] }

undo time-range *time-name* [*start-time* **to** *end-time* { *days* } &<1-7> | **from** *time1 date1* [**to** *time2 date2*]]

Parameters

Parameter	Description	Value
time-name	Specifies the name of a time range.	The value is a string of case-sensitive characters without spaces and must begin with a letter. The value ranges from 1 to 32. To avoid confusion, do not use "all" as the name of a time range.
start-time	Specify the start time of a time range.	The format is hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59.
end-time	Specify the end time of a time range.	The format is hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
days	Specifies the date on which the time range takes effect.	The value can be one of the following: ● The numbers 0 to 6 indicate that the time range takes effect from Sunday to Saturday. The number 0 refers to Sunday. ● A weekday includes Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. ● The value "Daily" indicates that the time range takes effect during the seven days in a week. ● The value "off-day" indicates that the time range takes effect on weekends including Saturday and Sunday. ● The value "Working-day" indicates that the time range takes effect in five days from Monday to Friday.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
from *time1 date1*	Specifies the time for the time range to take effect.	*time1* is in the format of hh:mm. ● *hh* specifies the hour. The value is an integer that ranges from 0 to 23. ● *mm* specifies the minute. The value is an integer that ranges from 0 to 59. *date1* is in the format of yyyy/mm/dd. ● *yyyy* specifies the year. The value is an integer that ranges from 1970 to 2099. ● *mm* specifies the month. The value is an integer that ranges from 1 to 12. ● *dd* specifies the day. The value is an integer that ranges from 1 to 31.
to *time2 date2*	Specifies the end of a time range.	The formats *time2* and *date2* are the same as those of the start time. The end time must be later than the start time. If the end time is not set, the device takes the maximum value allowed by the system.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If some services or functions need to be started at intervals or periodically, you can run the **time-range** command to set the time range. When configuring ACL or ACL6 rules, you can reference the names of time ranges.

The time range is classified into the following types:

- Relative time range (periodic time range): It is specified by *start-time* and *end-time*. The weekday when the time range takes effect is determined by *days*.
- Absolute time range: It is specified by **from** and **to**. The absolute time range can be used to limit the periodic time range.

You can set the same name for multiple time ranges to describe a special period. If multiple time ranges have the same name, the periodic time ranges are ORed, and a periodic time range and a definite time range are ANDed. For example, three time ranges are set with the same name **test**:

- Time range 1: 01.01.2010 00:00 to 31.12.2010 23:59 (absolute time range)
- Time range 2: 8:00 to 18:00 from Monday to Friday (periodic time range)
- Time range 3: 14:00 to 18:00 on Saturday and Sunday (periodic time range)

The time range **test** takes effect at 8:00-18:00 on Monday to Friday and 14:00-18:00 on Saturday and Sunday in the year 2010.

Precautions

Deleting the time range in use may affect the ACL rule referenced by the time range. Therefore, use this command with caution.

If a router (AR100, AR120, AR161, AR161W, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169W, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR169G-L) restarts unexpectedly, the system time is restored to factory setting. After the router restarts, set the system time correctly; otherwise, the command cannot be run.

Example

Set a time range named **test** that takes effect from 2010-01-01 00:00 to 2010-12-31 23:59.

```
<Huawei> system-view
[Huawei] time-range test from 0:0 2010/1/1 to 23:59 2010/12/31
```

Set a time range named **test** that takes effect at 8:00-18:00 from Monday to Friday.

```
<Huawei> system-view
[Huawei] time-range test 8:00 to 18:00 working-day
```

Set a time range named **test** that takes effect from 14:00 to 18:00 on every Saturday and Sunday.

```
<Huawei> system-view
[Huawei] time-range test 14:00 to 18:00 off-day
```

Related Topics

19.7.10 display time-range

19.8 Firewall Configuration Commands

19.8.1 bypass

Function

The **bypass** command enables the packet filtering firewall bypass function in an interzone.

The **undo bypass** command disables the packet filtering firewall bypass function in an interzone.

By default, the packet filtering firewall bypass function is disabled in an interzone.

Format

bypass [**session-overrun**]

undo bypass

Parameters

Parameter	Description	Value
session-overrun	Configures the device to create a flow table and forward traffic based on the flow table before the number of flow tables reaches the upper limit, and to create no flow table and forward traffic based on the interzone ACL policy after the number of flow tables reaches the upper limit. If this parameter is not specified, the device does not create a flow table and forwards traffic based on the interzone ACL policy.	-

Views

Interzone view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

A packet filtering firewall builds a flow table based on source IP addresses, source ports, destination IP addresses, destination ports, and transport-layer protocol. There is a limit on the flow table size since it occupies memory resources. If the flow table size reaches the limit, traffic of new services will fail to be forwarded because they cannot obtain flow table resources. To address this issue, configure the packet filtering firewall bypass function in an interzone. This configuration allows traffic to be forwarded based on inter-zone ACL rules, without the need of building flow table entries.

NOTE

After the packet filtering firewall bypass function is configured, the firewall supports only the packet filtering and packet filtering log functions.

Example

Enable the packet filtering firewall bypass function in the interzone between zone1 and zone2.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] bypass
```

19.8.2 clear firewall statistics system

Function

The **clear firewall statistics system** command clears the statistics about normal packets in the system.

Format

clear firewall statistics system normal

Parameters

Parameter	Description	Value
normal	Indicates the statistics about normal packets.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

To view the communication packets of a device within a specified period, run the **clear firewall statistics system normal** command to clear the previous packet statistics on the device first.

Example

Clear the statistics about normal packets in the system.

```
<Huawei> system-view
[Huawei] clear firewall statistics system normal
```

19.8.3 clear firewall statistics zone

Function

The **clear firewall statistics zone** command clears the statistics about normal packets in a zone.

Format

clear firewall statistics zone *zone-name*

Parameters

Parameter	Description	Value
zone-name	Specifies the name of a zone.	The value must be the name of an existing zone.

Views

System view

Default Level

3: Management level

Usage Guidelines

To view the packets in a zone within a specified period, run the **clear firewall statistics zone** command to clear the previous packet statistics in the zone first.

Example

Clear the statistics about normal packets in the zone **zone1**.

```
<Huawei> system-view
[Huawei] clear firewall statistics zone zone1
```

19.8.4 detect aspf

Function

The **detect aspf** command enables application specific packet filter (ASPF) in an interzone.

The **undo detect aspf** command disables ASPF in an interzone.

By default, ASPF is disabled in an interzone.

Format

detect aspf { **ftp** | **rtsp** | **sip** }

undo detect aspf { **ftp** | **rtsp** | **sip** }

Parameters

Parameter	Description	Value
ftp	Applies ASPF to the FTP protocol packets.	-
rtsp	Applies ASPF to the RTSP protocol packets.	-
sip	Applies ASPF to the SIP protocol packets.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ASPF filters application-layer protocol packets. It is a status-based packet filtering method. ASPF can detect the sessions that attempt to traverse the application layer and deny the undesired packets.

Prerequisites

An interzone has been created using the **firewall interzone** command.

Example

Enable ASPF in the interzone between **zone1** and **zone2**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone2-zone1] detect aspf ftp
```

Related Topics

19.8.10 display firewall interzone

19.8.5 display firewall app session table

Function

The **display firewall app session table** command displays the application session table.

Format

display firewall app session table [**application-protocol** { **dns** | **ftp** | **http** | **pptp** | **rtsp** | **sip** }] [**source-ip** *ip-address* [*port-number*]] [**destination-ip** *ip-address* [*port-number*]]

Parameters

Parameter	Description	Value
application-protocol	Indicates the type of the application-layer protocol.	-
dns	Displays the application session table information of DNS packets.	-
ftp	Displays the application session table information of FTP packets.	-
http	Displays the application session table information of HTTP packets.	-
pptp	Displays the application session table information of PPTP packets.	-
rtsp	Displays the application session table information of RTSP packets.	-
sip	Displays the application session table information of SIP packets.	-
source-ip *ip-address*	Indicates the source IP address of flows.	The value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
destination-ip *ip-address*	Indicates the destination IP address of flows.	The value is in dotted decimal notation.
port-number	Indicates the port number.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display firewall app session table** command displays information about a specified application session table or all application session tables. The application session table information is displayed only when some traffic is sent to the application layer.

Example

Display information about all application session tables.

```
<Huawei> display firewall app session table
 The total number of session tables is 1.
  NO.1.
    APP-Protocol : RTSP
    Initiator-VPN: ----
    Responder-VPN: ----
    Connection Info:
      Initiator(IP:Port)         Responder(IP:Port)    Protocol
      10.7.11.2       :33713 ---> 10.5.11.2       :554   TCP(6)
      10.7.11.2       :33713 <--- 10.5.11.2       :554   TCP(6)
```

Table 19-79 Description of the display firewall app session table command output

Item	Description
NO.1.	The first entry in the session table.
APP-Protocol : RTSP	The application protocol is RTSP.
Initiator-VPN: ----	Source VPN name.
Responder-VPN: ----	Destination VPN name.
Connection Info:	Connection between source address and destination address.
Initiator(IP:Port)	Source IP address and port number.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Responder(IP:Port)	Destination IP address and port number.
Protocol	Transport protocol type (TCP/UDP).

19.8.6 display firewall app table statistics

Function

The **display firewall app table statistics** command displays statistics on firewall application entries.

Format

display firewall app { **servermap** | **session** } **table statistics**

Parameters

Parameter	Description	Value
servermap	Displays statistics on servermap entries at the application layer.	-
session	Displays statistics on session entries at the application layer.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view statistics on firewall Session entries and Servermap entries to facilitate firewall related fault diagnosis and troubleshooting.

Session entry: includes quintuple information (the protocol number, source IP address, source port number, destination IP address, and destination port number). When each session passes through the firewall, a session entry is created on the firewall.

Servermap entry: includes triplet information (the protocol number, source IP address, and destination IP address). When the firewall uses a multi-channel protocol for communication, Servermap entries are created.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display statistics on all session entries at the application layer.

```
<Huawei> display firewall app session table statistics
 App-inspect Session History Maximum Info:
 Maximum Number :115
 Record Time    :2013-09-22 12:19:05
```

Table 19-80 Description of the display firewall app session table statistics command output

Item	Description
App-inspect Session History Maximum Info	Information about maximum number of session entries in the history.
Maximum Number	Maximum number of session entries.
Record Time	Time when maximum number of session entries is recorded.

Display statistics on all Servermap entries at the application layer.

```
<Huawei> display firewall app servermap table statistics
 App-inspect Servermap History Maximum Info:
 Maximum Number :115
 Record Time    :2013-09-22 12:19:31
```

Table 19-81 Description of the display firewall app servermap table statistics command output

Item	Description
App-inspect Servermap History Maximum Info	Information about maximum number of Servermap entries in the history.
Maximum Number	Maximum number of Servermap entries.
Record Time	Time when maximum number of Servermap entries is recorded.

Related Topics

19.8.66 reset firewall app table statistics

19.8.7 display firewall blacklist

Function

The **display firewall blacklist** command displays the blacklist entries.

Format

display firewall blacklist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **dynamic** | **static** | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
all	Displays all the blacklist entries.	-
ip-address	Displays the blacklist entry matching a specified IP address.	The value is a valid IPv4 IP address.
dynamic	Displays the dynamic blacklist entries.	-
static	Displays the static blacklist entries.	-
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all the blacklist entries.

```
<Huawei> display firewall blacklist all
Firewall blacklist items :
-----------------------------------------------------------------------
IP-Address      Reason       Expire-Time(m)    VPN-Instance
-----------------------------------------------------------------------
10.1.1.1        Manual       100
-----------------------------------------------------------------------
 Total number is : 1
```

Table 19-82 Description of the display firewall blacklist command output

Item	Description
IP-Address	IP address in a blacklist entry.
Reason	Reason why a blacklist entry is generated, including: ● IPSweep: The entry is generated because of an IP address sweeping attack. ● Manual: The entry is added to the blacklist manually. ● PortScan: The entry is generated because of a port scanning attack.
Expire-Time(m)	Aging time of a blacklist entry. m indicates minute. If the *Permanent* keyword is used, the entry will be valid permanently. To configure a blacklist entry, run the **firewall blacklist** command.
VPN-Instance	Name of the VPN instance that the IP address in a blacklist entry belongs to.
Total number is : 1	There is a total of one entry in the blacklist.

Related Topics

19.8.22 firewall blacklist

19.8.8 display firewall blacklist configuration

Function

The **display firewall blacklist configuration** command displays the status of the blacklist function.

Format

display firewall blacklist configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Check whether the blacklist function is enabled on the device.

```
<Huawei> display firewall blacklist configuration
Info:Blacklist is disabled.
```

Table 19-83 Description of the display firewall blacklist configuration command output

Item	Description
Info:Blacklist is disabled	The blacklist function is disabled. To enable the blacklist function, run the **firewall blacklist enable** command.

Related Topics

19.8.23 firewall blacklist enable

19.8.9 display firewall defend

Function

The **display firewall defend** command displays the status and configurations of the attack defense functions. For the Flood attack defense function, you can also view the attack defense configuration of the specified zone or IP address.

Format

display firewall defend { **flag** | { **icmp-flood** | **syn-flood** | **udp-flood** } [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]] | *other-attack-type* }

Parameters

Parameter	Description	Value
flag	Displays the status of all the attack defense functions.	-
icmp-flood	Displays the configuration of the ICMP Flood attack defense.	-

Parameter	Description	Value
syn-flood	Displays the configuration of the SYN Flood attack defense.	-
udp-flood	Displays the configuration of the UDP Flood attack defense.	-
ip [*ip-address*]	Displays the Flood attack defense function configured for the specified IP address.	The value is a valid IPv4 IP address.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.
zone [*zone-name*]	Displays the Flood attack defense function configured for the specified zone.	The value of *zone-name* is a string of 1 to 32 case-sensitive characters. It must be an existing zone name.
other-attack-type	Displays the configurations of other attack defense except for the Flood attack defense.	The other types of attacks include: ● fraggle ● icmp-redirect ● icmp-unreachable ● ip-fragment ● ip-sweep ● land ● large-icmp ● ping-of-death ● port-scan ● smurf ● tcp-flag ● teardrop ● tracert ● winnuke

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status of each attack defense function.

```
<Huawei> display firewall defend flag
--------------------------------
  Type                  Flag
--------------------------------
  land                 : disable
  smurf                : disable
  fraggle              : disable
  winnuke              : disable
  syn-flood            : disable
  udp-flood            : disable
  icmp-flood           : disable
  icmp-redirect        : disable
  icmp-unreachable     : disable
  ip-sweep             : disable
  port-scan            : disable
  tracert              : disable
  ping-of-death        : disable
  teardrop             : disable
  tcp-flag             : disable
  ip-fragment          : disable
  large-icmp           : disable
--------------------------------
```

Display the configuration of IP address sweeping attack defense.

```
<Huawei> display firewall defend ip-sweep

  defend-flag          : disable
  max-rate             : 4000  (pps)
  blacklist-expire-time : 20    (m)
```

Table 19-84 Description of the display firewall defend command output

Item	Description
Type	Type of attacks to defend against.
Flag	Flag indicating whether attack defense is enabled. ● disable: Attack defense is disabled. ● enable: Attack defense is enabled.
defend-flag	Flag indicating whether attack defense is enabled. ● disable: Attack defense is disabled. ● enable: Attack defense is enabled.

Item	Description
max-rate	Maximum session rate of address scanning attack defense, in pps. To set the maximum session rate of address scanning attack defense, run the **firewall defend ip-sweep** command.
blacklist-expire-time	Timeout interval of the blacklist. To set the timeout interval of the blacklist, run the **firewall defend ip-sweep** command.

19.8.10 display firewall interzone

Function

The **display firewall interzone** command displays information about an interzone.

Format

display firewall interzone [*zone-name1 zone-name2*]

Parameters

Parameter	Description	Value
zone-name1	Specifies the name of a zone included in the interzone.	The name is a string of 1 to 32 case-sensitive characters. *zone-name1* must be a zone name created by the **19.8.59 firewall zone** command.
zone-name2	Specifies the name of a zone included in the interzone.	The name is a string of 1 to 32 case-sensitive characters. *zone-name2* must be a zone name created by the **19.8.59 firewall zone** command.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can use the **display firewall interzone** command to obtain information about an interzone.

Example

Display information about the interzone between **zone1** and **zone2**.

```
<Huawei> display firewall interzone zone1 zone2
interzone zone2 zone1
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 session-log 3000 inbound
 detect aspf ftp
 bypass
<Huawei> display firewall interzone zone1 zone2
interzone zone2 zone1
 firewall enable
 packet-filter default deny inbound
 packet-filter default permit outbound
 packet-filter 3000 inbound
 packet-filter logging inbound permit
 bypass session-overrun
```

Table 19-85 Description of the display firewall interzone command output

Item	Description
interzone zone2 zone1	Interzone between two zones. To configure an interzone, run the **firewall interzone** command.
firewall enable	Firewall function is enabled in the interzone. To enable the firewall function, run the **firewall enable** command.
session-log 2006 inbound	Firewall logs are recorded based on filtering rules in ACL 2006. To reference an ACL, run the **session-log** command.
packet-filter default permit inbound	Default inbound packet filtering rule in an interzone: permit. To configure a packet filtering rule, run the **packet-filter** command.
packet-filter default deny outbound	Default outbound packet filtering rule in an interzone: deny. To configure a packet filtering rule, run the **packet-filter** command.
detect aspf ftp	ASPF is enabled for FTP packets. To enable ASPF, run the **detect aspf** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
packet-filter logging inbound permit	Packet filtering log function. To configure the packet filtering log function, run the **packet-filter logging** command.
bypass/bypass session-overrun	The packet filtering firewall bypass function is enabled in an interzone. To enable this function, run the **bypass** command.

Related Topics

19.8.51 firewall interzone
19.8.50 firewall enable
19.8.61 packet-filter
19.8.4 detect aspf

19.8.11 display firewall ipv6 session

Function

The **display firewall ipv6 session** command displays the IPv6 session table of the firewall.

Format

display firewall ipv6 session { **all** [**verbose**] | **number** }

display firewall ipv6 session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display firewall ipv6 session destination *destination-address* [*destination-port*] [**verbose**]

display firewall ipv6 session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all session table information.	-
verbose	Displays detailed information about the session table.	-

Parameter	Description	Value
number	Displays the number of entries in the session table.	-
protocol { *protocol-number* | *protocol-name* }	Displays the entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMPv6, TCP, or UDP.
source *source-address* [*source-port*]	Displays the entries with a specified source IPv6 address or both a source IPv6 address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• The total length of *source-address* is 128 bits. The string is divided into 8 groups, each of which consists of 4 hexadecimal digits. The value is in format X:X:X:X:X:X:X:X. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address*[*destination-port*]	Displays the entry with a specified destination IPv6 address or both a destination IPv6 address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• The total length of *destination-address* is 128 bits. The string is divided into 8 groups, each of which consists of 4 hexadecimal digits. The value is in format X:X:X:X:X:X:X:X. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about a firewall session table.

Example

Display the number of IPv6 entries in the session table.

```
<Huawei> display firewall ipv6 session number
 The total number of firewall ipv6 session tables is: 1
```

Display details about all IPv6 entries in the session table.

```
<Huawei> display firewall ipv6 session all verbose
  Firewall Ipv6 Session Table Information:
     Protocol          : TCP(6)
     SrcAddr  Port Vpn : fe80::1          1
     DestAddr Port Vpn : fc00::1          1
     Time To Live      : 120 s
     Firewall-Info
       InZone          : untrust
       OutZone         : trust
  Total : 1
```

Table 19-86 Description of the **display firewall session all verbose** command output

Item	Description
Firewall Ipv6 Session Table Information	IPv6 session table information.
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name.
Time To Live	Lifetime of the session table entries.
Firewall-Info	Firewall information.
InZone	Inzone name.
OutZone	Outzone name.
Total	Number of entries in the session table.

19.8.12 display firewall log configuration

Function

The **display firewall log configuration** command displays the global configuration of the firewall logging functions.

Format

display firewall log configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global configuration of the firewall logging functions.

```
<Huawei> display firewall log configuration
defend log :
  status : enabled
  log-interval : 30 s
statistics log :
  status : enabled
  log-interval : 30 s
blacklist log :
  status : enabled
  log-interval : 30 s
session log :
  status : enabled
  log-interval : 30 s
  nat-session : disabled
binary-log host :
  host                  source                VPN instance-name
  ----:--               ----:--               ---
packet filter log :
  status : disabled
  log-interval : 30 s
```

Table 19-87 Description of the display firewall log configuration command output

Item	Description
status	Status of a firewall logging function. **enable** indicates that the logging function is enabled; **disable** indicates that the logging function is disabled.
log-interval	Interval for exporting logs.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
nat-session	Status of NAT session logs. **enable** indicates that the logging function is enabled; **disable** indicates that the logging function is disabled.
host	IP address and port number of the log server.
source	IP address and port number used by the device to communicate with the log server.
VPN instance-name	Name of a VPN instance.

Related Topics

19.8.53 firewall log enable
19.8.54 firewall log log-interval
19.8.52 firewall log binary-log host
19.8.55 firewall log session nat enable

19.8.13 display firewall session

Function

The **display firewall session** command displays the firewall session table.

Format

display firewall session { **all** [**verbose**] | **number** }

display firewall session destination *destination-address* [*destination-port*] [**verbose**]

display firewall session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display firewall session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all entries in the firewall session table.	-
verbose	Displays details about the firewall session table.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
number	Displays the number of entries in the firewall session table.	-
protocol { *protocol-number* | *protocol-name* }	Displays entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.
source *source-address* [*source-port*]	Displays entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address*[*destination-port*]	Displays entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about a firewall session table.

Example

Display the number of entries in the session table.

```
<Huawei> display firewall session number
 The total number of firewall session tables is: 1
```

Display details about all entries in the session table.

```
<Huawei> display firewall session all verbose
  Firewall Session Table Information:
     Protocol           : TCP(6)
     SrcAddr  Port Vpn : 10.6.34.204    114   vpn1
     DestAddr Port Vpn : 10.1.1.1         21
     Time To Live       : 120 s
     Firewall-Info
       InZone          : a
       OutZone          : b

  Total : 1
```

Table 19-88 Description of the display firewall session all verbose command output

Item	Description
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name.
Time To Live	Lifetime of the session table entries.
Firewall-Info	Firewall information.
InZone	Inbound zone name.
OutZone	Outbound zone name.
Total	Number of entries in the firewall session table.

19.8.14 display firewall statistics system

Function

The **display firewall statistics system** command displays traffic statistics on the firewall.

Format

display firewall statistics system [**normal all** | **defend**]

Parameters

Parameter	Description	Value
normal all	Displays the statistics about packets passing the firewall.	-
defend	Displays the statistics about attack packets passing the firewall.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When you run the **display firewall statistics system** command without specifying any parameters, the upper and lower thresholds for controlling the TCP, UDP, ICMP, TCP proxy, and IP fragment packets (session number) are displayed.

Example

Display the global traffic thresholds set on the firewall.

```
<Huawei> display firewall statistics system
 ----------------------------------------------------------------------
            Global system statistics config information
 ----------------------------------------------------------------------
  Is enable          0                  <enable : 1  disable : 0 >
 ---------------------------------High---------------------Low-------
 Tcp connect-number                 16384                  12288

 Udp connect-number                 16384                  12288

 Icmp connect-number                16384                  12288

 Tcp-proxy connect-number           16384                  12288

 Frag connect-number                16384                  12288

 ----------------------------------------------------------------------
```

Display the statistics of packets passing the firewall.

```
<Huawei> display firewall statistics system normal all
IPv4 statistics:
HistoryTcpTotal-------------0
CurTcpTearTotal-------------0
HistoryUdpTotal-------------0
CurUdpTearTotal-------------0
HistoryIcmpTotal------------0
CurIcmpTearTotal------------0
HisTcpProxyTotal------------0
CurTcpProxyTearTotal--------0
```

```
HistoryFragTotal------------0
CurFragTearTotal------------0
IPv6 statistics:
HistoryIPv6Total------------0
CurTcpIPv6TearTotal---------0
HistoryUdpIPv6Total---------0
CurUdpIPv6TearTotal---------0
HistoryIcmpV6Total----------0
CurIcmpV6TearTotal----------0
HistoryIPv6FragTotal--------0
CurIPv6FragTearTotal--------0
```

Table 19-89 Description of the display firewall statistics system normal all command output

Item	Description
IPv4 statistics:	IPv4 traffic statistics on the firewall.
HistoryTcpTotal	Number of historical TCP connections.
CurTcpTearTotal	Number of TCP current connections.
HistoryUdpTotal	Number of history UDP connections.
CurUdpTearTotal	Number of UDP current connections.
HistoryIcmpTotal	Number of history ICMP connections.
CurIcmpTearTotal	Number of ICMP current connections.
HisTcpProxyTotal	Number of historical TCP proxy connections.
CurTcpProxyTearTotal	Number of TCP current proxy connections.
HistoryFragTotal	Number of historical fragment flow entries.
CurFragTearTotal	Number of current fragment flow entries.
IPv6 statistics:	IPv6 traffic statistics on the firewall.
HistoryIPv6Total	Number of historical TCP IPv6 connections.
CurTcpIPv6TearTotal	Number of TCP IPv6 connections that are torn down.
HistoryUdpIPv6Total	Number of historical UDP IPv6 connections.
CurUdpIPv6TearTotal	Number of UDP IPv6 connections that are torn down.
HistoryIcmpV6Total	Number of historical ICMPv6 connections
CurIcmpV6TearTotal	Number of ICMPv6 connections that are torn down.
HistoryIPv6FragTotal	Number of historical IPv6 fragment flow entries.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CurIPv6FragTearTotal	Number of current IPv6 fragment flow entries.

Display the statistics on attack packets passing the firewall.

```
<Huawei> display firewall statistics system defend
 --------------------FW GLOBAL DEFEND TABLE--------------------
DropID[710]            0 FW_INTERZONE_DENY_DROP
DropID[715]            0 FW_ACL_FILTER_DENY_DROP
DropID[736]            0 FW_GLOBAL_UDP_CONNECT_DROP
DropID[737]            0 FW_GLOBAL_TCP_CONNECT_DROP
DropID[738]            0 FW_GLOBAL_ICMP_CONNECT_DROP
DropID[739]            0 FW_GLOBAL_TCP_PROXY_CONNECT_DROP
DropID[740]            0 FW_ZONE_IN_UDP_CONNECT_DROP
DropID[741]            0 FW_ZONE_OUT_UDP_CONNECT_DROP
DropID[742]            0 FW_ZONE_IN_TCP_CONNECT_DROP
DropID[743]            0 FW_ZONE_OUT_TCP_CONNECT_DROP
DropID[744]            0 FW_ZONE_IN_ICMP_CONNECT_DROP
DropID[745]            0 FW_ZONE_OUT_ICMP_CONNECT_DROP
DropID[746]            0 FW_ZONE_IP_IN_UDP_CONNECT_DROP
DropID[747]            0 FW_ZONE_IP_OUT_UDP_CONNECT_DROP
DropID[748]            0 FW_ZONE_IP_IN_TCP_CONNECT_DROP
DropID[749]            0 FW_ZONE_IP_OUT_TCP_CONNECT_DROP
DropID[750]            0 FW_ZONE_IP_IN_ICMP_CONNECT_DROP
DropID[751]            0 FW_ZONE_IP_OUT_ICMP_CONNECT_DROP
DropID[752]            0 FW_GLOBAL_FRAG_CONNECT_DROP
DropID[764]            0 FW_LAND_DEFEND_DROP
DropID[765]            0 FW_SMURF_DEFEND_DROP
DropID[766]            0 FW_FRAGGLE_DEFEND_DROP
DropID[767]            0 FW_WINNUKE_DEFEND_DROP
DropID[768]            0 FW_CONNECT_SYNFLOOD_DEFEND_DROP
DropID[769]            0 FW_CONNECT_ICMPFLOOD_DEFEND_DROP
DropID[770]            0 FW_CONNECT_UDPFLOOD_DEFEND_DROP
DropID[771]            0 FW_ICMPREDIRECT_DEFEND_DROP
DropID[772]            0 FW_ICMPUNREACHABLE_DEFEND_DROP
DropID[773]            0 FW_IPSWEEP_DEFEND_DROP
DropID[774]            0 FW_PORTSCAN_DEFEND_DROP
DropID[775]            0 FW_TRACERT_DEFEND_DROP
DropID[776]            0 FW_PINGOFDEATH_DEFEND_DROP
DropID[777]            0 FW_TEARDROP_DEFEND_DROP
DropID[778]            0 FW_TCPFLAG_DEFEND_DROP
DropID[779]            0 FW_IPFRAGMENT_DEFEND_DROP
DropID[780]            0 FW_LARGEICMP_DEFEND_DROP
DropID[781]            0 FW_BLACKIPLIST_DEFEND_DROP
DropID[782]            0 FW_FLOW_SYNFLOOD_DEFEND_DROP
DropID[783]            0 FW_FLOW_ICMPFLOOD_DEFEND_DROP
DropID[784]            0 FW_FLOW_UDPFLOOD_DEFEND_DROP
DropID[785]            0 FW_FRAG_SESSION_NUM_OVER_DROP
DropID[786]            0 FW_TEARDROP_BAD_IPLEN_DROP
```

Table 19-90 Description of the display firewall statistics system defend command output

Item	Description
FW_INTERZONE_DENY_DROP	Number of packets rejected by the firewall.
FW_ACL_FILTER_DENY_DROP	Number of packets rejected by the ACL.
FW_GLOBAL_UDP_CONNECT_DROP	Number of discarded packets of excess global UDP connections.

Item	Description
FW_GLOBAL_TCP_CONNECT_DROP	Number of discarded packets of excess global TCP connections.
FW_GLOBAL_ICMP_CONNECT_DROP	Number of discarded packets of excess global ICMP connections.
FW_GLOBAL_TCP_PROXY_CONNECT_DROP	Number of discarded packets of excess global split TCP proxy connections initiated globally.
FW_ZONE_IN_UDP_CONNECT_DROP	Number of discarded incoming packets of excess UDP connections in a zone.
FW_ZONE_OUT_UDP_CONNECT_DROP	Number of discarded outgoing packets of excess UDP connections.
FW_ZONE_IN_TCP_CONNECT_DROP	Number of discarded incoming packets of excess TCP connections in a zone.
FW_ZONE_OUT_TCP_CONNECT_DROP	Number of discarded outgoing packets of excess TCP connections in a zone.
FW_ZONE_IN_ICMP_CONNECT_DROP	Number of discarded incoming packets of excess ICMP connections.
FW_ZONE_OUT_ICMP_CONNECT_DROP	Number of discarded outgoing packets of excess ICMP connections in a zone.
FW_ZONE_IP_IN_UDP_CONNECT_DROP	Number of discarded incoming packets of excess UDP connections.
FW_ZONE_IP_OUT_UDP_CONNECT_DROP	Number of discarded outgoing packets of excess UDP connections.
FW_ZONE_IP_IN_TCP_CONNECT_DROP	Number of discarded incoming packets of excess TCP connections.
FW_ZONE_IP_OUT_TCP_CONNECT_DROP	Number of discarded outgoing packets of excess TCP connections.
FW_ZONE_IP_IN_ICMP_CONNECT_DROP	Number of discarded incoming packets of excess ICMP connections.
FW_ZONE_IP_OUT_ICMP_CONNECT_DROP	Number of discarded outgoing packets of excess ICMP connections.
FW_GLOBAL_FRAG_CONNECT_DROP	Number of discarded packets of excess fragment connections initiated globally.
FW_LAND_DEFEND_DROP	Number of discarded Land attack packets.
FW_SMURF_DEFEND_DROP	Number of discarded Smurf attack packets.
FW_FRAGGLE_DEFEND_DROP	Number of discarded Fraggle attack packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FW_WINNUKE_DEFEND_DROP	Number of discarded Winnuke attack packets.
FW_CONNECT_SYNFLOOD_DEFEND_DROP	Number of discarded initial packets of SYN flood attacks.
FW_CONNECT_ICMPFLOOD_DEFEND_DROP	Number of discarded initial packets of ICMP flood attacks.
FW_CONNECT_UDPFLOOD_DEFEND_DROP	Number of discarded initial packets of UDP flood attacks.
FW_ICMPREDIRECT_DEFEND_DROP	Number of discarded ICMP redirection attack packets.
FW_ICMPUNREACHABLE_DEFEND_DROP	Number of discarded ICMP unreachable attack packets.
FW_IPSWEEP_DEFEND_DROP	Number of discarded IP scanning attack packets.
FW_PORTSCAN_DEFEND_DROP	Number of discarded port scanning attack packets.
FW_TRACERT_DEFEND_DROP	Number of discarded Tracert attack packets.
FW_PINGOFDEATH_DEFEND_DROP	Number of discarded ping of death attack packets.
FW_TEARDROP_DEFEND_DROP	Number of discarded Teardrop attack packets.
FW_TCPFLAG_DEFEND_DROP	Number of discarded malformed TCP attack packets.
FW_IPFRAGMENT_DEFEND_DROP	Number of discarded IP fragment attack packets.
FW_LARGEICMP_DEFEND_DROP	Number of discarded large-sized ICMP attack packets.
FW_BLACKIPLIST_DEFEND_DROP	Number of discarded blacklisted attack packets.
FW_FLOW_SYNFLOOD_DEFEND_DROP	Number of discarded non-initial SYN flood attack packets.
FW_FLOW_ICMPFLOOD_DEFEND_DROP	Number of discarded non-initial ICMP flood attack packets.
FW_FLOW_UDPFLOOD_DEFEND_DROP	Number of discarded non-initial UDP flood attack packets.
FW_FRAG_SESSION_NUM_OVER_DROP	Number of discarded excess fragments.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FW_TEARDROP_BAD_IPLEN_DROP	Number of discarded invalid packets.

Related Topics

19.8.56 firewall statistics system connect-number

19.8.15 display firewall statistics zone

Function

The **display firewall statistics zone** command displays traffic statistics and monitoring information in a zone.

Format

display firewall statistics zone *zone-name* { **inzone** | **outzone** } **all**

Parameters

Parameter	Description	Value
zone-name	Indicates the name of a zone.	The value must be the name of an existing zone.
inzone	Displays the statistics about the traffic entering the zone.	-
outzone	Displays the statistics about the traffic leaving the zone.	-
all	Displays the statistics about the traffic entering and leaving the zone.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The **display firewall statistics zone** command displays the number of current sessions and historical sessions in the inbound or outbound direction of a zone and the number of HTTP, FTP, or DNS packets in a certain direction.

Example

Display the inbound packet statistics of zone1.

```
<Huawei> display firewall statistics zone zone1 inzone all
ZoneID:0  Direction:IN
InTcpSetupTotal-----------------0
InTcpTearTotal------------------0
InUdpSetupTotal-----------------0
InUdpTearTotal------------------0
InIcmpSetupTotal----------------0
InIcmpTearTotal-----------------0
```

Display the outbound packet statistics of zone1.

```
<Huawei> display firewall statistics zone zone1 outzone all
ZoneID:0  Direction:OUT
OutTcpSetupTotal----------------0
OutTcpTearTotal-----------------0
OutUdpSetupTotal----------------0
OutUdpTearTotal-----------------0
OutIcmpSetupTotal---------------0
OutIcmpTearTotal----------------0
```

Table 19-91 Description of the display firewall statistics zone command output

Item	Description
InTcpSetupTotal / OutTcpSetupTotal	Number of TCP connections in inbound and outbound directions.
InTcpTearTotal / OutTcpTearTotal	Number of deleted TCP connections in inbound and outbound directions.
InUdpSetupTotal / OutUdpSetupTotal	Number of UDP connections in inbound and outbound directions.
InUdpTearTotal / OutUdpTearTotal	Number of deleted UDP connections in inbound and outbound directions.
InIcmpSetupTotal / OutIcmpSetupTotal	Number of ICMP connections in inbound and outbound directions.
InIcmpTearTotal / OutIcmpTearTotal	Number of deleted ICMP connections in inbound and outbound directions.

Related Topics

19.8.73 statistics connect-number zone
19.8.75 statistics zone enable

19.8.16 display firewall statistics zone-ip

Function

The **display firewall statistics zone-ip** command displays the status of traffic monitoring function and session thresholds for each protocol.

Format

display firewall statistics zone-ip *zone-name*

Parameters

Parameter	Description	Value
zone-name	Indicates the name of a zone.	The value must be the name of an existing zone.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the traffic monitoring function is enabled and the session thresholds of each protocol are set, you can run the **display firewall statistics zone-ip** command to view the traffic monitoring information of the zone.

Example

Display the configuration of traffic monitoring in zone2.

```
<Huawei> display firewall statistics zone-ip zone2
 ---------------------------------------------------------------------
                 Zone statistics config information
 ---------------------------------------------------------------------
 Zone in enable          0              <enable : 1  disable : 0>
 ---------------------------------High---------------------Low-------
 Tcp connect-number              16384                  12288

 Udp connect-number              16384                  12288

 Icmp connect-number             16384                  12288

 ---------------------------------------------------------------------
 Zone out enable         0              <enable : 1  disable : 0>
 ---------------------------------------------------------------------
 Tcp connect-number              16384                  12288

 Udp connect-number              16384                  12288
```

```
Icmp connect-number            16384                12288

-----------------------------------------------------------------
Ip in enable          0            <enable : 1  disable : 0>
-----------------------------------------------------------------
Tcp connect-number             16384                12288

Udp connect-number             16384                12288

Icmp connect-number            16384                12288

-----------------------------------------------------------------
Ip out enable         0            <enable : 1  disable : 0>
-----------------------------------------------------------------
Tcp connect-number             16384                12288

Udp connect-number             16384                12288

Icmp connect-number            16384                12288

-----------------------------------------------------------------
```

Related Topics

19.8.72 statistics connect-number ip

19.8.74 statistics ip enable

19.8.17 display firewall whitelist

Function

The **display firewall whitelist** command displays entries in the whitelist.

Format

display firewall whitelist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
all	Displays all the entries in the whitelist.	-
ip-address	Displays the whitelist entry matching the specified IP address.	The value is a valid IPv4 IP address in dotted decimal notation.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display all the whitelist entries on the device.

```
<Huawei> display firewall whitelist all
Firewall whitelist items  :
-----------------------------------------------------------------------
IP-Address     Expire-Time(m)  VPN-Instance
-----------------------------------------------------------------------
10.1.1.1       3               vpn1
10.1.1.2       Permanent       vpn2
10.1.1.3       6
 -----------------------------------------------------------------------
 Total number is : 3
```

Table 19-92 Description of the display firewall whitelist command output

Item	Description
IP-Address	IP address in a whitelist entry.
VPN-Instance	Name of the VPN instance that the IP address in a whitelist entry belongs to.
Expire-Time(m)	Aging time of a whitelist entry, in minutes.
Total number is : 3	There are a total of three entries in the whitelist.

Related Topics

19.8.58 firewall whitelist

19.8.18 display firewall zone

Function

The **display firewall zone** command displays the configuration of a specified zone or all zones.

Format

display firewall zone [*zone-name*] [**interface** | **priority**]

Parameters

Parameter	Description	Value
zone-name	Displays the configuration of a specified zone.	The value is a string of 1 to 32 case-sensitive characters. The character string cannot contain name or -.
interface	Displays the interfaces added to the zone.	-
priority	Displays the priorities of all zones.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display information about all zones configured on the device.

```
<Huawei> display firewall zone
zone zone1
 priority is 5
 interface of the zone is (total number 1):
 Vlanif77

 total number is : 1
```

Table 19-93 Description of the display firewall interzone command output

Item	Description
zone zone1	Security zone named **zone1**. To configure a security zone, run the **firewall zone** command.
priority is 5	Priority of a security zone: 5. To configure the priority for a security zone, run the **priority** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
interface of the zone is (total number 1): Vlanif77	One interface, VLANIF 77, has been added to the zone. To add interfaces a zone, run the **zone** command.
total number is : 1	There is a total of one zone on the device.

Related Topics

19.8.59 firewall zone
19.8.65 priority (security zone view)
19.8.76 zone

19.8.19 display firewall-nat session aging-time

Function

The **display firewall-nat session aging-time** command displays the timeout interval of entries in the firewall session table or NAT session table.

Format

display firewall-nat session aging-time

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the timeout interval of sessions on the firewall session table or NAT session table.

Example

Display the timeout time of all entries in the session table.

```
<Huawei> display firewall-nat session aging-time
-----------------------------------------------
Protocol timeout:
  tcp protocol timeout         : 600   (s)
  tcp-proxy timeout            : 10    (s)
```

```
  http protocol timeout        : 120   (s)
  udp protocol timeout         : 120   (s)
  icmp protocol timeout        : 20    (s)
  dns protocol timeout         : 120   (s)
  ftp protocol timeout         : 120   (s)
  ftp-data protocol timeout    : 120   (s)
  rtsp protocol timeout        : 60    (s)
  rtsp-media protocol timeout  : 120   (s)
  sip protocol timeout         : 1800  (s)
  sip-media protocol timeout   : 120   (s)
User-define port timeout:
  tcp protocol port 10001      : 65535 (s)
  tcp protocol port 1          : 111   (s)
  tcp protocol port 4443       : 65535 (s)
  tcp protocol port 181        : 180   (s)
  udp protocol port 180        : 180   (s)
  udp protocol port 182        : 208   (s)
---------------------------------------------
```

Table 19-94 Description of the **display firewall-nat session aging-time** command output

Item	Description
Protocol timeout	Session timeout interval of each protocol.
tcp protocol timeout	Timeout interval of TCP connections. The default value is 600, in seconds.
tcp-proxy timeout	Timeout interval of the TCP proxy. The default value is 10, in seconds.
udp protocol timeout	Timeout interval of UDP connections. The default value is 120, in seconds.
icmp protocol timeout	Timeout interval of ICMP connections. The default value is 20, in seconds.
dns protocol timeout	Timeout interval of the DNS protocol. The default value is 120, in seconds.
http protocol timeout	Timeout interval of the HTTP connections. The default value is 120, in seconds.
ftp protocol timeout	Timeout interval of the FTP control connection. The default value is 120, in seconds.
ftp-data protocol timeout	Timeout interval of the FTP connections. The default value is 120, in seconds.
sip protocol timeout	Timeout interval of the SIP protocol. The default value is 1800, in seconds.
sip-media protocol timeout	Timeout interval of the SIP media protocol. The default value is 120, in seconds.
rtsp protocol timeout	Timeout interval of the RTSP protocol. The default value is 60, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
rtsp-media protocol timeout	Timeout interval of the RTSP media protocol. The default value is 120, in seconds.
User-define port timeout	Timeout interval of a connection with a user-defined port as the destination port.
tcp protocol port *port-number*	Timeout interval of a data connection with a user-defined TCP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.
udp protocol port *port-number*	Timeout interval of a data connection with a user-defined UDP port as the destination port. The default value is the default data connection timeout interval of the corresponding protocol, in seconds.

Related Topics

19.8.60 firewall-nat session aging-time

19.8.20 display port-mapping

Function

The **display port-mapping** command displays mappings between the specified application-layer protocols and ports.

Format

display port-mapping [**dns** | **ftp** | **http** | **rtsp** | **sip** | **port** *port-number* | **pptp**]

Parameters

Parameter	Description	Value
dns	Displays the mapping between the DNS protocol and port.	-
ftp	Displays the mapping between the FTP protocol and port.	-
http	Displays the mapping between the HTTP protocol and port.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rtsp	Displays the mapping between the RTSP protocol and port.	-
sip	Displays the mapping between the SIP protocol and port.	-
port *port-number*	Displays the mapping between the specified port and the application-layer protocol.	The value is an integer that ranges from 1 to 65535.
pptp	Displays the mapping between the PPTP protocol and port.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display port-mapping** command displays the port mappings, including the mappings between application-layer protocols and ports, condition (ACL) in which each mapping takes effect, and the type of each mapping (defined by the system or user).

Example

Display the mapping between the DNS protocol and port.

```
<Huawei> display port-mapping dns
 -------------------------------------------------
 Service    Port       Acl        Type
 -------------------------------------------------
 dns          53                  system defined
 -------------------------------------------------
Total number is : 1
```

Table 19-95 Description of the display port-mapping command output

Item	Description
Service	Type of the application-layer protocol.
Port	Port number.

Item	Description
Acl	Number of the ACL for mappings.
Type	Mapping type. ● system defined: default mapping. ● user defined: mapping defined by the user.
Total number is : 1	The total number of mappings is 1.

Related Topics

19.8.64 port-mapping

19.8.21 display session

Function

The **display session** command displays the session table information.

Format

display session { **all** [**verbose**] | **number** }

display session destination *destination-address* [*destination-port*] [**verbose**]

display session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]] [**verbose**]

display session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]] [**verbose**]

Parameters

Parameter	Description	Value
all	Displays all session table information.	-
verbose	Displays detailed information about the session table.	-
number	Displays the number of entries in the session table.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol { *protocol-number* | *protocol-name* }	Displays entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.
source *source-address* [*source-port*]	Displays entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Displays entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to check information about a firewall session table, NAT session table, or a common session table.

Example

Display the number of entries in the session table.

```
<Huawei> display session number
  The total number of session tables is: 1
```

Display details about all entries in the session table.

```
<Huawei> display session all verbose
  Session Table Information:
    Protocol          : TCP(6)
    SrcAddr  Port Vpn : 10.200.200.200 65532 vpn1
    DestAddr Port Vpn : 10.100.100.100 1024
    Time To Live      : 60 s
    NAT-Info
      New SrcAddr     : 10.10.10.10
      New SrcPort     : 10240
      New DestAddr    : 10.30.30.30
      New DestPort    : 21
    Firewall-Info
      InZone          : a
      OutZone         : b

  Total : 1
```

Table 19-96 Description of the display session all verbose command output

Item	Description
Protocol	Protocol type.
SrcAddr Port Vpn	Source address, service port number, and VPN instance name.
DestAddr Port Vpn	Destination address, service port number, and VPN instance name.
Time To Live	Lifetime of the session table entries.
NAT-Info	NAT information.
New SrcAddr	Translated source IP address.
New SrcPort	Translated source port.
New DestAddr	Translated destination IP address.
New DestPort	Translated destination port.
Firewall-Info	Firewall information.
InZone	Inbound zone name.
OutZone	Outbound zone name.
Total	Number of entries in the session table.

 Copyright © Huawei Technologies Co., Ltd.

19.8.22 firewall blacklist

Function

The **firewall blacklist** command adds an entry to the blacklist.

The **undo firewall blacklist** command deletes an entry from the blacklist.

Format

firewall blacklist *ip-address* [**vpn-instance** *vpn-instance-name*] [**expire-time** *minutes*]

undo firewall blacklist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
ip-address	Indicates the IP address that you want to add to the blacklist.	The value is a valid IPv4 IP address.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.
expire-time *minutes*	Specifies the aging time of a blacklist entry.	The value is an integer that ranges from 1 to 1000, in minutes. **NOTE** If this parameter is not set, the entry is always valid.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After an IP address is added to the blacklist by the **firewall blacklist** command, the firewall denies the packets from this IP address until this entry ages.

An IP address cannot exist in both the whitelist and blacklist.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The blacklist entry with an aging time is not written into the configuration file. You can view it using the **19.8.7 display firewall blacklist** command.

Example

Add IP address 192.168.10.10 to the blacklist entry and set its aging time to 100 minutes.

```
<Huawei> system-view
[Huawei] firewall blacklist 192.168.10.10 expire-time 100
```

Related Topics

19.8.7 display firewall blacklist

19.8.23 firewall blacklist enable

Function

The **firewall blacklist enable** command enables the blacklist function.

The **undo firewall blacklist enable** command disables the blacklist function.

By default, the blacklist function is disabled.

Format

firewall blacklist enable

undo firewall blacklist enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Configurations of the blacklist take effect only after you run the **firewall blacklist enable** command to enable the blacklist function.

Precautions

A blacklist entry can be manually configured or automatically generated.

After you run the **firewall defend ip-sweep enable** command to enable defense against address scanning attacks, the device adds attacking IP addresses to the blacklist.

After you run the **firewall defend port-scan enable** command to enable defense against port scanning attacks, the device adds attacking ports to the blacklist.

Example

Enable the blacklist function.

```
<Huawei> system-view
[Huawei] firewall blacklist enable
```

19.8.24 firewall black-white-list load configuration-file

Function

The **firewall black-white-list load configuration-file** command loads the configuration file of blacklist and whitelist.

Format

firewall black-white-list load configuration-file *configuration-file-name*

Parameters

Parameter	Description	Value
configuration-file-name	Indicates the name of the configuration file.	The value is a string of 1 to 127 characters in the format [drive][file-name] (the default drive is flash:/). The configuration file is in txt format.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can batch configure entries in the blacklist and whitelist by loading a configuration file.

A configuration file can contain multiple entries, but the entries must be edited one by one. Blank lines are allowed between lines. A configuration file contains up to 50000 lines. The following is an example of the configuration file:

 Copyright © Huawei Technologies Co., Ltd.

```
[FirewallBlacklist]
IPAddress = 10.10.10.1
VPNName = vpna
[FirewallBlacklist]
IPAddress = 10.10.10.2
VPNName =

[FirewallWhitelist]
IPAddress = 10.10.10.3
VPNName = vpnb
[FirewallWhitelist]
IPAddress = 10.20.20.1
VPNName =
```

NOTE

An invalid configuration file cannot be loaded. For example, if a configuration file contains an invalid IP address or excess entries, the invalid IP address cannot be added and the excess entries do not take effect; however, the valid IP addresses and the entries in the range can still take effect.

Example

Load the configuration file named **bwls.txt**.

```
<Huawei> system-view
[Huawei] firewall black-white-list load configuration-file bwls.txt
```

Related Topics

19.8.25 firewall black-white-list save configuration-file

19.8.25 firewall black-white-list save configuration-file

Function

The **firewall black-white-list save configuration-file** command saves the blacklist and whitelist to a configuration file.

Format

firewall black-white-list save configuration-file *configuration-file-name*

Parameters

Parameter	Description	Value
configuration-file-name	Indicates the name of the configuration file.	The value is a string of 1 to 127 characters in the format [drive][file-name] (the default drive is flash:/). The configuration file is in txt format.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By using this command, you can save the blacklist and whitelist to the configuration file *configuration-file-name*. Only the entries with the aging time being 0 can be saved.

NOTE

The configuration file *configuration-file-name* must be available before this command is executed.

Example

Save the blacklist and whitelist to the configuration file **bls_wls.txt**.

```
<Huawei> system-view
[Huawei] firewall black-white-list save configuration-file bwls.txt
```

Related Topics

19.8.24 firewall black-white-list load configuration-file

19.8.26 firewall defend all enable

Function

The **firewall defend all enable** command enables all the attack defense functions.

The **undo firewall defend all enable** command disables all the attack defense functions.

By default, no attack defense function is enabled.

Format

firewall defend all enable

undo firewall defend all enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable all attack defense functions.

```
<Huawei> system-view
[Huawei] firewall defend all enable
```

Related Topics

19.8.9 display firewall defend

19.8.27 firewall defend fraggle enable

Function

The **firewall defend fraggle enable** command enables the Fraggle attack defense function.

The **undo firewall defend fraggle enable** command disables the Fraggle attack defense function.

By default, the Fraggle attack defense function is disabled.

Format

firewall defend fraggle enable

undo firewall defend fraggle enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A Fraggle attack is similar to a Smurf attack, except that the Fraggle attack sends UDP packets, rather than ICMP packets. Therefore, the Fraggle attack packets can traverse some firewalls that prevent ICMP packets.

 Copyright © Huawei Technologies Co., Ltd.

A Fraggle attack can be successful because both UDP port 7 (ECHO) and port 19 (Chargen) return responses after receiving UDP packets. The details are as follows:

- UDP port 7 returns a response (similar to the ICMP ECHO-Reply packet) after receiving a packet.
- UDP port 19 generates a character stream after receiving the packet.

The two UDP ports send a lot of response packets, which occupy high network bandwidth.

An attacker can send a UDP packet to the target network. The source address of the UDP packet is the IP address of the attacked host and its destination address is the broadcast address or network address of the host's subnet. The destination port number of the packet is 7 or 19. All the hosts on the subnet then send response packets to the attacked host. This generates heavy traffic and hence congests the network or makes the host break down.

Example

Enable the Fraggle attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend fraggle enable
```

Related Topics

19.8.9 display firewall defend

19.8.28 firewall defend icmp-flood

Function

The **firewall defend icmp-flood** command sets the parameters of ICMP Flood attack defense, including the protected zone or IP address and maximum connection rate.

The **undo firewall defend icmp-flood** command restores the default values of ICMP Flood attack defense parameters.

By default, the maximum connection rate of ICMP Flood attack defense is 1000 pps.

Format

firewall defend icmp-flood { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*]

undo firewall defend icmp-flood [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies a protected IP address.	The value is a valid IPv4 IP address.
zone *zone-name*	Specifies a protected zone.	The value of *zone-name* is a string of 1 to 32 characters. It must be an existing zone name.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.
max-rate *rate-value*	Specifies the maximum connection rate of a new flow.	The value of *rate-value* is an integer that ranges from 1 to 65535, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ICMP Flood attack sends a large number of ICMP packets (such as ping packets) to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

ICMP Flood attack defense parameters configured for an IP address take precedence over those configured for a zone. If ICMP Flood attack defense is configured for both an IP address and the zone where the IP address resides, the configuration for the IP address takes effect. If you cancel the configuration for the IP address, the configuration for the zone takes effect.

Precautions

Parameters of ICMP Flood attack defense take effect only after ICMP Flood defense is enabled using the **firewall defend icmp-flood enable** command.

Example

Enable ICMP Flood attack defense for IP address 10.1.64.200 and set the maximum connection rate of ICMP packets to 500 pps.

```
<Huawei> system-view
[Huawei] firewall defend icmp-flood enable
```

```
[Huawei] firewall defend icmp-flood ip 10.1.64.200 max-rate 500
```

Related Topics

19.8.9 display firewall defend

19.8.27 firewall defend fraggle enable

19.8.29 firewall defend icmp-flood enable

Function

The **firewall defend icmp-flood enable** command enables the ICMP Flood attack defense function.

The **undo firewall defend icmp-flood enable** command disables the ICMP Flood attack defense function.

By default, the ICMP Flood attack defense function is disabled.

Format

firewall defend icmp-flood enable

undo firewall defend icmp-flood enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ICMP Flood attack sends a large number of ICMP packets (such as ping packets) to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

Precaution

You can run **firewall defend icmp-flood** command to set parameters for ICMP Flood attack defense.

Example

Enable the ICMP Flood attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend icmp-flood enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend

19.8.28 firewall defend icmp-flood

19.8.30 firewall defend icmp-redirect enable

Function

The **firewall defend icmp-redirect enable** command enables the ICMP-Redirect attack defense function.

The **undo firewall defend icmp-redirect enable** command disables the ICMP-Redirect attack defense function.

By default, the ICMP-Redirect attack defense function is disabled.

Format

firewall defend icmp-redirect enable

undo firewall defend icmp-redirect enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the ICMP-Redirect attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend icmp-redirect enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.31 firewall defend icmp-unreachable enable

Function

The **firewall defend icmp-unreachable enable** command enables the ICMP-Unreachable attack defense function.

The **undo firewall defend icmp-unreachable enable** command disables the ICMP-Unreachable attack defense function.

By default, the ICMP-Unreachable attack defense function is disabled.

Format

firewall defend icmp-unreachable enable

undo firewall defend icmp-unreachable enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the ICMP-Unreachable attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend icmp-unreachable enable
```

Related Topics

19.8.9 display firewall defend

19.8.32 firewall defend ip-fragment enable

Function

The **firewall defend ip-fragment enable** command enables the IP fragment attack defense function.

The **undo firewall defend ip-fragment enable** command disables the IP fragment attack defense function.

 Copyright © Huawei Technologies Co., Ltd.

By default, the IP fragment attack defense function is disabled.

Format

firewall defend ip-fragment enable

undo firewall defend ip-fragment enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable the IP fragment attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend ip-fragment enable
```

Related Topics

19.8.9 display firewall defend

19.8.33 firewall defend ip-sweep

Function

The **firewall defend ip-sweep** command sets the parameters of address sweeping attack defense, including the maximum session rate and blacklist timeout interval.

The **undo firewall defend ip-sweep** command restores the default values of address sweeping attack defense parameters.

By default, the maximum session rate for address scanning and port scanning attack defense is 4000 pps, and the blacklist timeout interval is 20 minutes.

Format

firewall defend ip-sweep { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

undo firewall defend ip-sweep { **blacklist-expire-time** | **max-rate** }

Parameters

Parameter	Description	Value
blacklist-expire-time *interval*	Specifies the timeout interval of blacklist entries. After an IP address stays in the blacklist for the specified period, the firewall deletes the IP address from the blacklist. Then the IP address can initiate connections.	The value of *interval* is an integer that from 1 to 1000, in minutes. The default value is 20.
max-rate *rate-value*	Specifies the maximum session rate. When the session rate of an IP address exceeds the limit, the firewall considers that an IP address sweeping attack occurs. Then the firewall adds the IP address to the blacklist and denies the new sessions from the IP address or port.	The value of *rate-value* is an integer that ranges from 1 to 10000, in pps. The default value is 4000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Parameters of address sweeping attack defense take effect only after address sweeping attack defense is enabled using the **firewall defend ip-sweep enable** command.

Example

Enable the address sweeping attack defense function, set the maximum session rate to 1000 pps, and set the blacklist timeout interval to 5 minutes.

```
<Huawei> system-view
[Huawei] firewall defend ip-sweep enable
[Huawei] firewall defend ip-sweep max-rate 1000
[Huawei] firewall defend ip-sweep blacklist-expire-time 5
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend

19.8.34 firewall defend ip-sweep enable

19.8.34 firewall defend ip-sweep enable

Function

The **firewall defend ip-sweep enable** command enables the IP sweeping attack defense function.

The **undo firewall defend ip-sweep enable** command disables the IP sweeping attack defense function.

By default, the IP sweeping attack defense function is disabled.

Format

firewall defend ip-sweep enable

undo firewall defend ip-sweep enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP sweeping attack detects the IP addresses of the target hosts by using scanning tools. The attacker then determines the hosts that exist on the target network according to the responses received.

Precaution

You can run **firewall defend ip-sweep** command to set parameters for IP address sweep attack defense.

Example

Enable the IP sweeping defense function.

```
<Huawei> system-view
[Huawei] firewall defend ip-sweep enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend

19.8.33 firewall defend ip-sweep

19.8.35 firewall defend land enable

Function

The **firewall defend land enable** command enables the defense against Land attacks.

The **undo firewall defend land enable** command disables the defense against Land attacks.

By default, the Land attack defense function is disabled.

Format

firewall defend land enable

undo firewall defend land enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable the defense against Land attacks.

```
<Huawei> system-view
[Huawei] firewall defend land enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.36 firewall defend large-icmp

Function

The **firewall defend large-icmp** command sets the maximum length of ICMP packets allowed to pass.

The **undo firewall defend large-icmp** command restores the default maximum length of ICMP packets allowed to pass.

By default, the maximum length of ICMP packet allowed to pass is 4000 bytes.

Format

firewall defend large-icmp max-length *length*

undo firewall defend large-icmp max-length

Parameters

Parameter	Description	Value
max-length *length*	Specifies the maximum length of ICMP packets allowed to pass.	The value of *length* is an integer that ranges from 28 to 65535, in bytes. The default value is 4000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Similar to a "Ping of Death" attack, a Large-ICMP attack sends the oversized ICMP packets to attack a system. The difference is that the length of Large-ICMP packet does not exceed the maximum length of an IP packet (65535 bytes). Large-ICMP packets also have great impact on some operating systems. To prevent Large-ICMP attack, set the maximum length of ICMP packets on the firewall.

Precautions

The maximum length of ICMP packets allowed to pass takes effect only after large-ICMP attack defense is enabled using the **firewall defend large-icmp enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable Large-ICMP attack defense and set the maximum length of ICMP packet allowed to pass to 4000 bytes.

```
<Huawei> system-view
[Huawei] firewall defend large-icmp enable
[Huawei] firewall defend large-icmp max-length 4000
```

Related Topics

19.8.9 display firewall defend

19.8.37 firewall defend large-icmp enable

Function

The **firewall defend large-icmp enable** command enables the Large-ICMP attack defense function.

The **undo firewall defend large-icmp enable** command disables the Large-ICMP attack defense function.

By default, the Large-ICMP attack defense function is disabled.

Format

firewall defend large-icmp enable

undo firewall defend large-icmp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Similar to a "Ping of Death" attack, a large-ICMP attack sends the oversize ICMP packets to attack a system. The difference is that the length of Large-ICMP packet does not exceed the maximum length of an IP packet (65535 bytes). Large-ICMP packets also have great impact on some operating systems.

Precaution

You can run **firewall defend large-icmp** command to set Large-ICMP attack defense.

Example

Enable the Large-ICMP attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend large-icmp enable
```

Related Topics

19.8.9 display firewall defend

19.8.36 firewall defend large-icmp

19.8.38 firewall defend ping-of-death enable

Function

The **firewall defend ping-of-death enable** command enables the defense against Ping of Death attack.

The **undo firewall defend ping-of-death enable** command disables the defense against Ping of Death attack.

By default, the defense against Ping of Death attack is disabled.

Format

firewall defend ping-of-death enable

undo firewall defend ping-of-death enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the defense against Ping of Death attack.

```
<Huawei> system-view
[Huawei] firewall defend ping-of-death enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.39 firewall defend port-scan

Function

The **firewall defend port-scan** command sets the parameters of port scanning attack defense, including the maximum session rate and blacklist timeout interval.

The **undo firewall defend port-scan** command restores the default values of port scanning attack defense parameters.

By default, the maximum session rate for port scanning attack defense is 4000 pps, and the blacklist timeout interval is 20 minutes.

Format

firewall defend port-scan { **blacklist-expire-time** *interval* | **max-rate** *rate-value* }

undo firewall defend port-scan { **blacklist-expire-time** | **max-rate** }

Parameters

Parameter	Description	Value
blacklist-expire-time *interval*	Specifies the timeout interval of blacklist entries. After a port stays in the blacklist for the specified period, the firewall deletes the port from the blacklist. Then the port can initiate connections.	The value of *interval* is an integer that from 1 to 1000, in minutes. The default value is 20.
max-rate *rate-value*	Specifies the maximum session rate. When the session rate of a port exceeds the limit, the firewall considers that a scanning attack occurs. Then the firewall adds the port to the blacklist and denies the new sessions from the port.	The value of *rate-value* is an integer that ranges from 1 to 10000, in pps. The default value is 4000.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Parameters of port scanning attack defense take effect only after port scanning attack defense is enabled using the **firewall defend port-scan enable** command.

Example

Enable the port scanning attack defense function, set the maximum session rate to 1000 pps, and set the blacklist timeout interval to 5 minutes.

```
<Huawei> system-view
[Huawei] firewall defend port-scan enable
[Huawei] firewall defend port-scan max-rate 1000
[Huawei] firewall defend port-scan blacklist-expire-time 5
```

Related Topics

19.8.9 display firewall defend

19.8.40 firewall defend port-scan enable

19.8.40 firewall defend port-scan enable

Function

The **firewall defend port-scan enable** command enables the port scanning attack defense function.

The **undo firewall defend port-scan enable** command disables the port scanning attack defense function.

By default, the port scanning attack defense function is disabled.

Format

firewall defend port-scan enable

undo firewall defend port-scan enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Port scanning attack detects the ports of the target hosts by using scanning tools. The attacker then finds out the hosts that exist on the target network according to the responses and the ports that are used to provide services.

Precaution

You can run the **firewall defend port-scan** command to set parameters for port scanning attack defense.

Example

Enable the port scanning attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend port-scan enable
```

Related Topics

19.8.9 display firewall defend

19.8.39 firewall defend port-scan

19.8.41 firewall defend smurf enable

Function

The **firewall defend smurf enable** command enables the Smurf attack defense function.

The **undo firewall defend smurf enable** command disables the Smurf attack defense function.

By default, the Smurf attack defense function is disabled.

Format

firewall defend smurf enable

undo firewall defend smurf enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enables the Smurf attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend smurf enable
```

Related Topics

19.8.9 display firewall defend

19.8.42 firewall defend syn-flood

Function

The **firewall defend syn-flood** command sets the parameters of SYN Flood attack defense, including the protected zone or IP address and maximum connection rate.

The **undo firewall defend syn-flood** command restores the default configuration of SYN Flood attack defense.

By default, the maximum connection rate of SYN Flood attack defense is 1000 pps.

Format

firewall defend syn-flood { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*] [**tcp-proxy** { **auto** | **off** | **on** }]

undo firewall defend syn-flood [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]]

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies a protected IP address.	The value is a valid IPv4 IP address.
zone *zone-name*	Specifies a protected zone.	The value of *zone-name* is a string of 1 to 32 characters. It must be an existing zone name.
max-rate *rate-value*	Specifies the maximum connection rate of a new flow.	The value of *rate-value* is an integer that ranges from 1 to 65535. The default value is 1000, in pps.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tcp-proxy { **auto** | **off** | **on** }	Indicates whether to use the TCP proxy. The status of TCP proxy includes: • **auto**: The TCP proxy is enabled automatically when the actual connection rate exceeds the upper limit. • **off**: The TCP proxy is always disabled. • **on**: The TCP proxy is always enabled.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flood attack defense parameters configured for an IP address take precedence over those configured for a zone. If Flood attack defense is configured for both an IP address and the zone where the IP address resides, the configuration for the IP address takes effect. If you cancel the configuration for the IP address, the configuration for the zone takes effect.

Precautions

Parameters of SYN Flood attack defense take effect only after SYN Flood attack defense is enabled using the **firewall defend syn-flood enable** command.

Example

Enable SYN Flood attack defense for IP address 10.1.64.200 and set the maximum connection rate of TCP packets to 500 pps.

```
<Huawei> system-view
[Huawei] firewall defend syn-flood enable
[Huawei] firewall defend syn-flood ip 10.1.64.200 max-rate 500
```

Related Topics

19.8.9 display firewall defend
19.8.43 firewall defend syn-flood enable

19.8.43 firewall defend syn-flood enable

Function

The **firewall defend syn-flood enable** command enables the SYN Flood attack defense function.

The **undo firewall defend syn-flood enable** command disables the SYN Flood attack defense function.

By default, the SYN Flood attack defense function is disabled.

Format

firewall defend syn-flood enable

undo firewall defend syn-flood enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The TCP/IP protocol stack permits only a certain number of TCP connections due to resource restriction. SYN Flood attacks utilize this feature. The attacker forges a SYN packet with a forged or nonexistent source address to initiate a connection to the server. When receiving this packet, the server replies with a SYN-ACK message. The receiver of the SYN-ACK packet does not exist, so a half-connection is caused. If the attacker sends a large number of such packets, a lot of half-connections will be produced on the attacked host and the resources of the attacked host will be exhausted. Therefore, authorized users cannot access the host till the half-connections expire. If the number of connections is not limited, SYN Flood will consume the system resources such as memory.

Precaution

You can run **firewall defend syn-flood** command to set parameters for SYN Flood attack defense.

Example

Enable the SYN Flood attack defense function.

```
<Huawei> system-view
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] firewall defend syn-flood enable
```

Related Topics

19.8.9 display firewall defend

19.8.28 firewall defend icmp-flood

19.8.44 firewall defend tcp-flag enable

Function

The **firewall defend tcp-flag enable** command enables the defense against TCP flag attack.

The **undo firewall defend tcp-flag enable** command disables the defense against TCP flag attack.

By default, the TCP flag attack defense function is disabled.

Format

firewall defend tcp-flag enable

undo firewall defend tcp-flag enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Enable the TCP flag attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend tcp-flag enable
```

Related Topics

19.8.9 display firewall defend

 Copyright © Huawei Technologies Co., Ltd.

19.8.45 firewall defend teardrop enable

Function

The **firewall defend teardrop enable** command enables the defense against Teardrop attack.

The **undo firewall defend teardrop enable** command disables the defense against Teardrop attack.

By default, the Teardrop attack defense function is disabled.

Format

firewall defend teardrop enable

undo firewall defend teardrop enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None.

Example

Enable the defense against Teardrop attack.

```
<Huawei> system-view
[Huawei] firewall defend teardrop enable
```

Related Topics

19.8.9 display firewall defend

19.8.46 firewall defend tracert enable

Function

The **firewall defend tracert enable** command enables the Tracert attack defense function.

The **undo firewall defend tracert enable** command disables the Tracert attack defense function.

By default, the Tracert attack defense function is disabled.

Format

firewall defend tracert enable

undo firewall defend tracert enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Tracert attack traces the path of an ICMP timeout packet returned when the value of time to live (TTL) is 0 or an ICMP port-unreachable packet. In this way, the attacker obtains the network structure.

Example

Enable the Tracert attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend tracert enable
```

Related Topics

19.8.9 display firewall defend

19.8.47 firewall defend udp-flood

Function

The **firewall defend udp-flood** command sets the parameters of UDP Flood attack defense, including the protected zone or IP address and maximum connection rate.

The **undo firewall defend udp-flood** command restores the default configuration of UDP Flood attack defense.

By default, the maximum connection rate of UDP Flood attack defense is 1000 pps.

Format

firewall defend udp-flood { **ip** *ip-address* [**vpn-instance** *vpn-instance-name*] | **zone** *zone-name* } [**max-rate** *rate-value*]

undo firewall defend udp-flood [**ip** [*ip-address* [**vpn-instance** *vpn-instance-name*]] | **zone** [*zone-name*]]

Parameters

Parameter	Description	Value
ip *ip-address*	Specifies a protected IP address.	The value is a valid IPv4 IP address.
zone *zone-name*	Specifies a protected zone.	The value of *zone-name* is a string of 1 to 32 characters. It must be an existing zone name.
max-rate *rate-value*	Specifies the maximum connection rate of a new flow.	The value of *rate-value* is an integer that ranges from 1 to 65535. The default value is 1000, in pps.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

UDP Flood attack sends a large number of UDP packets to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

Flood attack defense parameters configured for an IP address take precedence over those configured for a zone. If Flood attack defense is configured for both an IP address and the zone where the IP address resides, the configuration for the IP address takes effect. If you cancel the configuration for the IP address, the configuration for the zone takes effect.

Precautions

Parameters of UDP Flood attack defense take effect only after UDP Flood attack defense is enabled using the **firewall defend udp-flood enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable UDP Flood attack defense for IP address 10.1.64.200 and set the maximum connection rate of UDP packets to 500 pps.

```
<Huawei> system-view
[Huawei] firewall defend udp-flood enable
[Huawei] firewall defend udp-flood ip 10.1.64.200 max-rate 500
```

Related Topics

19.8.9 display firewall defend

19.8.48 firewall defend udp-flood enable

Function

The **firewall defend udp-flood enable** command enables the UDP Flood attack defense function.

The **undo firewall defend udp-flood enable** command disables the UDP Flood attack defense function.

By default, the UDP Flood attack defense function is disabled.

Format

firewall defend udp-flood enable

undo firewall defend udp-flood enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

UDP Flood attack sends a large number of UDP packets to the attacked host in a short time and requests for responses. The host is then overloaded and cannot process normal tasks.

Precaution

You can run **firewall defend udp-flood** command to set parameters for ICMP Flood attack defense.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable UDP Flood attack defense.

```
<Huawei> system-view
[Huawei] firewall defend udp-flood enable
```

Related Topics

19.8.9 display firewall defend

19.8.49 firewall defend winnuke enable

Function

The **firewall defend winnuke enable** command enables the WinNuke attack defense function.

The **undo firewall defend winnuke enable** command disables the WinNuke attack defense function.

By default, the WinNuke attack defense function is disabled.

Format

firewall defend winnuke enable

undo firewall defend winnuke enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

WinNuke attack sends an out-of-band (OOB) data packet to the NetBIOS port (139) of the target host running a Windows operating system. The NetBIOS fragment then overlaps and the host stops responding. An Internet Group Management Protocol (IGMP) fragment packet can also damage the target host because the IGMP packet should not be fragmented. If a host receives an IGMP fragment packet, the host may be attacked.

Example

Enables the WinNuke attack defense function.

```
<Huawei> system-view
[Huawei] firewall defend winnuke enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.8.9 display firewall defend

19.8.50 firewall enable

Function

The **firewall enable** command enables the firewall function in an interzone.

The **undo firewall enable** command disables the firewall function in an interzone.

By default, the firewall function is disabled in an interzone.

Format

firewall enable

undo firewall enable

Parameters

None

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

The packet filtering, ASPF, and attack defense functions take effect only after this command is executed. This command does not needs to be executed for other advanced security features, such as IPS and URL filtering.

Example

Enable the firewall function in the interzone between zone1 and zone2.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] firewall enable
```

Related Topics

19.8.10 display firewall interzone

19.8.51 firewall interzone

Function

The **firewall interzone** command creates an interzone.

 Copyright © Huawei Technologies Co., Ltd.

The **undo firewall interzone** command deletes an interzone.

Format

firewall interzone *zone-name1 zone-name2*

undo firewall interzone *zone-name1 zone-name2*

Parameters

Parameter	Description	Value
zone-name1	Specifies the name of a zone included in the interzone.	The name is a string of 1 to 32 characters. *zone-name1* must be a zone name created by the **19.8.59 firewall zone** command.
zone-name2	Specifies the name of the other zone included in the interzone.	The name is a string of 1 to 32 characters. *zone-name2* must be a zone name created by the **19.8.59 firewall zone** command.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To configure the firewall in an interzone to filter packets or application-layer services, run the **firewall interzone** command to enter the interzone view.

Precautions

At least two valid zones must exist on the device; otherwise, the device does not execute the **firewall interzone** command.

The interzone is determined by two zones, which is irrelevant to the sequence of the two zones in the command.

Example

Create an interzone between zone1 and zone2.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] firewall interzone zone1 zone2
```

Related Topics

19.8.10 display firewall interzone

19.8.52 firewall log binary-log host

Function

The **firewall log binary-log host** command sets parameters of a binary log server, including the IP address and port number of the binary log server, and the IP address and port number that the local device uses to communicate with the log server.

The **undo firewall log binary-log host** command deletes a binary log server.

Format

firewall log binary-log host *host-ip-address host-port* **source** *source-ip-address source-port* [**vpn-instance** *vpn-instance-name*]

undo firewall log binary-log host

Parameters

Parameter	Description	Value
host-ip-address	Specifies the IP address of the log server.	The value is a valid IPv4 IP address.
host-port	Specifies the port number of the log server.	The value is an integer that ranges from 1 to 65535.
source-ip-address	Specifies the source IP address that the local device uses to send logs to the log server.	The value is a valid IPv4 IP address.
source-port	Specifies the source port number that the local device uses to send logs to the log server.	The value is an integer that ranges from 10240 to 55534.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the source IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Only one binary log server can be configured in the system view. Any time a new binary log server is configured, the new one replaces the previous one.

Example

Configure a binary log server whose IP address is 10.10.10.1 and port number is 3456. Set the source IP address and source port number used to communicate with the log server to 10.10.10.2 and 20000 respectively.

```
<Huawei> system-view
[Huawei] firewall log binary-log host 10.10.10.1 3456 source 10.10.10.2 20000
```

Related Topics

19.8.12 display firewall log configuration

19.8.53 firewall log enable

Function

The **firewall log enable** command enables the firewall logging function.

The **undo firewall log enable** command disables the firewall logging function.

By default, firewall logging function is disabled.

Format

firewall log { **all** | **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **enable**

undo firewall log { **all** | **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **enable**

Parameters

Parameter	Description	Value
all	Enables all the logging functions on the firewall. **NOTE** Firewall logs are classified into blacklist logs, attack defense logs, session logs, and traffic statistics logs.	-
blacklist	Enables blacklist logs.	-
defend	Enables attack defense logs.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
session	Enables session logs.	-
statistics	Enables traffic statistics logs.	-
packet-filter	Enables packet-filter logs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Firewall logs record the operating status of the firewall in real time. By analyzing the logs, the network administrator can find potential security threats to the network and take preventive measures to protect the network.

You can configure the following types of logs on the firewall:

- Blacklist log: records the IP addresses that are added to or deleted from the blacklist.
- Attack defense log: records different types of attacks detected by the firewall.
- Session log: records the sessions that match the specified ACL rules and sessions processed by the NAT server.
- Traffic statistics log: records the events that the traffic rate exceeds the threshold or falls below the threshold.
- Packet filtering log: records information about packet filtering.

Example

Enable blacklist logs.

```
<Huawei> system-view
[Huawei] firewall log blacklist enable
```

Related Topics

19.8.54 firewall log log-interval
19.8.12 display firewall log configuration

19.8.54 firewall log log-interval

Function

The **firewall log log-interval** command sets the interval for exporting firewall logs.

The **undo firewall log log-interval** command restores the default interval for exporting firewall logs.

By default, firewall logs are exported every 30 seconds.

Format

firewall log { **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **log-interval** *time*

undo firewall log { **blacklist** | **defend** | **session** | **statistics** | **packet-filter** } **log-interval**

Parameters

Parameter	Description	Value
blacklist	Sets the interval for sending blacklist logs to the log server.	-
defend	Sets the interval for sending attack defense logs to the log server.	-
session	Sets the interval for sending session logs to the log server.	-
statistics	Sets the interval for sending traffic statistics logs to the log server.	-
packet-filter	Sets the interval for sending packet filtering logs to the log server.	-
log-interval *time*	Specifies the value of the interval.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Firewall logs are classified into binary logs and text logs depending on the format. Binary logs are sent to the binary log server in real time, and text logs are sent to the text log server at intervals. The **firewall log log-interval** command sets the interval for sending text logs to the text log server.

Example

Set the interval for sending attack defense logs to the log server to 200 seconds.

```
<Huawei> system-view
[Huawei] firewall log defend log-interval 200
```

Related Topics

19.8.53 firewall log enable

19.8.12 display firewall log configuration

19.8.55 firewall log session nat enable

Function

The **firewall log session nat enable** command enables NAT session logs.

The **undo firewall log session nat enable** command disables NAT session logs.

By default, NAT session logs are disabled.

Format

firewall log session nat enable

undo firewall log session nat enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Session logs record the sessions that match the specified ACL rules and sessions processed by the NAT server.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable NAT session logs.

```
<Huawei> system-view
[Huawei] firewall log session nat enable
```

Related Topics

19.8.53 firewall log enable

19.8.54 firewall log log-interval

19.8.12 display firewall log configuration

19.8.56 firewall statistics system connect-number

Function

The **firewall statistics system connect-number** command sets the session thresholds on the firewall.

The **undo firewall statistics system connect-number** command restores the default session thresholds on the firewall.

Format

firewall statistics system connect-number { **frag** | **icmp** | **tcp** | **tcp-proxy** | **udp** } **high** *high-threshold* **low** *low-threshold*

undo firewall statistics system connect-number { **frag** | **icmp** | **tcp** | **tcp-proxy** | **udp** }

Parameters

Parameter	Description	Value
frag	Sets the session thresholds of IP fragment packets.	-
icmp	Sets the session thresholds of ICMP packets.	-
tcp	Sets the session thresholds of TCP packets.	-
tcp-proxy	Sets the session thresholds of TCP proxy packets.	-
udp	Sets the session thresholds of UDP packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high *high-threshold*	Specifies the upper threshold of a specified type of protocol packets.	The value is an integer and the value range varies according to product model: ● AR120&AR150&AR160&AR200: 1-16384. The default value is 16384. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 16384. ● AR2220, AR2220E: 1-65536. The default value is 65536. ● AR2240C: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU40: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU60: 1-160000. The default value is 160000. ● AR2204XE, and AR2204XE-DC: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU80 and SRU100E: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU200 and SRU200E: 1-400000. The default value is 400000. ● AR2240 and AR3260, SRU400: 1-800000. The default value is 800000. ● AR3600 series: 1-400000. The default value is 400000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
low *low-threshold*	Specifies the lower threshold of a specified type of protocol packets.	The value is an integer and the value range varies according to product model: ● AR120&AR150&AR160&AR200: 1-16384. The default value is 12288. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 12288. ● AR2220, AR2220E: 1-65536. The default value is 52224. ● AR2240C: 1-65536. The default value is 52224. ● AR2240, AR3260, and SRU40: 1-65536. The default value is 52224. ● AR2240, AR3260, and SRU60: 1-160000. The default value is 52224. ● AR2204XE, and AR2204XE-DC: 1-204800. The default value is 163840. ● AR2240, AR3260, SRU80 and SRU100E: 1-204800. The default value is 163840. ● AR2240, AR3260, SRU200 and SRU200E: 1-400000. The default value is 163840. ● AR2240, AR3260,SRU400: 1-800000. The default value is 163840. ● AR3600 series: 1-400000. The default value is 163840.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before setting the session thresholds on the firewall, run the **19.8.57 firewall statistics system enable** command to enable traffic statistics collection on the firewall.

Example

Set the session thresholds of TCP packets on the firewall. Set the upper threshold to 15000 and lower threshold to 10000.

```
<Huawei> system-view
[Huawei] firewall statistics system enable
[Huawei] firewall statistics system connect-number tcp high 15000 low 10000
```

Related Topics

19.8.57 firewall statistics system enable

19.8.14 display firewall statistics system

19.8.57 firewall statistics system enable

Function

The **firewall statistics system enable** command enables traffic statistics collection on the firewall.

The **undo firewall statistics system enable** command disables traffic statistics collection on the firewall.

By default, traffic statistics collection is disabled on the firewall.

Format

firewall statistics system enable

undo firewall statistics system enable

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **19.8.14 display firewall statistics system** command to check whether traffic statistics collection is enabled.

Example

Enable traffic statistics collection on the firewall.

```
<Huawei> system-view
[Huawei] firewall statistics system enable
```

Related Topics

19.8.14 display firewall statistics system

19.8.58 firewall whitelist

Function

The **firewall whitelist** command adds an entry to the whitelist.

The **undo firewall whitelist** command deletes an entry from the whitelist.

Format

firewall whitelist *ip-address* [**vpn-instance** *vpn-instance-name*] [**expire-time** *minutes*]

undo firewall whitelist { **all** | *ip-address* [**vpn-instance** *vpn-instance-name*] | **vpn-instance** *vpn-instance-name* }

Parameters

Parameter	Description	Value
all	Deletes all whitelist entries.	-
ip-address	Specifies the IP address to be added to the whitelist.	The value is a valid IPv4 IP address in dotted decimal notation.
expire-time *minutes*	Specifies the aging time of a whitelist entry.	The value is an integer that ranges from 1 to 1000, in minutes. **NOTE** If this parameter is not set, the entry is always valid.
vpn-instance *vpn-instance-name*	Indicates the name of the VPN instance that the specified IP address belongs to.	The value of *vpn-instance-name* is a string of 1 to 31 case-sensitive characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

An IP address cannot exist in both the whitelist and blacklist. To move an IP address from one list to the other list, delete the corresponding entry first.

The entries in the whitelist take effect directly and you do not need to enable the whitelist function.

Example

Add IP address 10.1.1.1 to the whitelist and set the aging time of this entry to 3 minutes.

```
<Huawei> system-view
[Huawei] firewall whitelist 10.1.1.1 expire-time 3
```

Related Topics

19.8.17 display firewall whitelist

19.8.59 firewall zone

Function

The **firewall zone** command creates an interzone.

The **undo firewall zone** command deletes an interzone.

Format

firewall zone *zone-name*

undo firewall zone *zone-name*

Parameters

Parameter	Description	Value
zone-name	Specifies the name of a zone.	The value is a string of 1 to 32 case-sensitive characters without hyphens (-), and must start with a letter.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before configuring a firewall, create zones. Then you can deploy security services according to the security priorities of the zones.

The device considers that the data transmission within a zone is reliable; therefore, it does not enforce any security policy on the intra-zone data transmission.

NOTE

If an interface is added to a zone, the zone cannot be deleted in the system view. To delete the zone, delete the interface from the zone first.

Example

Create the zone **zone1**.

```
<Huawei> system-view
[Huawei] firewall zone zone1
```

Related Topics

19.8.18 display firewall zone

19.8.60 firewall-nat session aging-time

Function

The **firewall-nat session aging-time** command sets the timeout interval of each entry in the session table.

The **undo firewall-nat session aging-time** command restores the default timeout interval of each entry in the session table.

Format

firewall-nat session { { **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time** *time-value*

undo firewall-nat session { { **all** | **dns** | **ftp** | **ftp-data** | **http** | **icmp** | **tcp** | **tcp-proxy** | **udp** | **sip** | **sip-media** | **rtsp** | **rtsp-media** | **pptp** | **pptp-data** } | { **tcp** | **udp** } **user-define** *port-number* } **aging-time**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dns	Sets the timeout interval of the DNS protocol.	-
ftp	Sets the timeout interval of the FTP control connection.	-
ftp-data	Sets the timeout interval of the FTP connection.	-
http	Sets the timeout interval of the HTTP connection.	-
icmp	Sets the timeout interval of the ICMP connection.	-
tcp	Sets the timeout interval of the TCP connection.	-
tcp-proxy	Sets the timeout interval of the TCP proxy.	-
udp	Sets the timeout interval of the UDP connection.	-
sip	Sets the timeout interval of the SIP connection.	-
sip-media	Sets the timeout interval of the SIP media protocol.	-
rtsp	Sets the timeout interval of the RTSP protocol.	-
rtsp-media	Sets the timeout interval of the RTSP media protocol.	-
pptp	Sets the timeout interval of the PPTP control connection.	-
pptp-data	Sets the timeout interval of the PPTP connection.	-
all	Restores the default timeout interval of all the preceding connections.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-define *port-number*	Specifies the user-defined TCP or UDP port number and configures the timeout interval for all data connections with this port as the destination port. **NOTE** This parameter only supports NAT and does not support firewall.	The value is an integer that ranges from 1 to 65535.
aging-time *time-value*	Specifies the timeout interval value.	The value is an integer that ranges from 1 to 65535, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **firewall-nat session aging-time** command sets the timeout interval for sessions of each protocol or port. If an entry in a session table is not used within the specified period, the entry expires. For example, the user with IP address 10.110.10.10 initiates a TCP connection through port 2000. If the TCP connection is not used within the timeout interval, the system deletes the TCP connection.

The default session timeout interval of a port is the same as that of the corresponding protocol. The following table lists the default session timeout interval of each protocol.

Protocol	Default Session Timeout Interval
tcp	600 seconds
tcp-proxy	10 seconds
udp	120 seconds
icmp	20 seconds
dns	120 seconds
http	120 seconds

 Copyright © Huawei Technologies Co., Ltd.

Protocol	Default Session Timeout Interval
ftp	120 seconds
ftp-data	120 seconds
sip	1800 seconds
sip-media	120 seconds
rtsp	60 seconds
rtsp-media	120 seconds
pptp	600 seconds
pptp-data	600 seconds

NOTE

When configuring the timeout interval for all sessions with a user-defined port as the destination port, you cannot set the port number to a default port number of the preceding protocols.

Precautions

For some services such as voice service, increase the TCP/UDP timeout interval to prevent service interruption.

You can set the session timeout interval for a maximum of 24 ports on the device.

Example

Set the timeout interval of the DNS connection to 60 seconds.

```
<Huawei> system-view
[Huawei] firewall-nat session dns aging-time 60
```

Related Topics

19.8.19 display firewall-nat session aging-time

19.8.61 packet-filter

Function

The **packet-filter** command configures packet filtering in an interzone.

The **undo packet-filter** command cancels packet filtering in an interzone.

By default, all outgoing packets are permitted and all incoming packets are denied.

Format

packet-filter { *acl-number* | **default** { **deny** | **permit** } } { **inbound** | **outbound** }

undo packet-filter *acl-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
acl-number	Indicates the number of the ACL for packet filtering. The ACLs include basic ACL and advanced ACL.	The value is an integer that ranges from 2000 to 3999: ● 2000-2999: basic ACLs ● 3000-3999: advanced ACLs
default	Indicates the default packet filtering method.	-
deny	Rejects all packets. **NOTE** This parameter sets the default packet filtering method of the interzone. The default packet filtering method takes effect on all the packets not matching the ACLs.	-
permit	Allows all packets to pass. **NOTE** This parameter sets the default packet filtering method of the interzone. The default packet filtering method takes effect on all the packets not matching the ACLs.	-
inbound	Filters inbound packets. An inbound packet refers to a packet sent from a low-priority zone to a high-priority zone.	-
outbound	Filters outbound packets. An outbound packet refers to a packet sent from a high-priority zone to a low-priority zone.	-

Views

Interzone view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The number of times the command is run cannot exceed the number of configured packet filtering interzones.

Example

Filter the inbound packets in the interzone between zone1 and zone2 by using ACL 3000.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule permit ip
[Huawei-acl-adv-3000] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] packet-filter 3000 inbound
```

Related Topics

19.8.10 display firewall interzone

19.8.62 packet-filter ipv6

Function

The **packet-filter ipv6** command configures IPv6 packet filtering in an interzone.

The **undo packet-filter ipv6** command cancels IPv6 packet filtering in an interzone.

By default, the outbound packets are allowed, and the inbound packets are denied.

Format

packet-filter ipv6 *acl6-number* { **inbound** | **outbound** }

undo packet-filter ipv6 *acl6-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
acl6-number	Indicates the ACL used for packet filtering, including basic ACL6 and advanced ACL6.	The value is an integer that ranges from 2000 to 3999: • 2000-2999: Basic ACL6 • 3000-3999: Advanced ACL6

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
inbound	Filters inbound packets. An inbound packet refers to a packet from a low-priority zone to a high-priority zone.	-
outbound	Filters outbound packets. An outbound packet refers to a packet from a high-priority zone to a low-priority zone.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

The number of times the command is run cannot exceed the number of configured packet filtering interzones.

Example

Filter the inbound IPv6 packets in the interzone between zone1 and zone2 by using ACL6 3000.

```
<Huawei> system-view
[Huawei] acl ipv6 3000
[Huawei-acl6-adv-3000] rule permit ipv6
[Huawei-acl6-adv-3000] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone2-zone1] packet-filter ipv6 3000 inbound
```

Related Topics

19.8.10 display firewall interzone

19.8.63 packet-filter logging

Function

The **packet-filter logging** command enables the packet filtering log in the interzone.

The **undo packet-filter logging** command disables the packet filtering log in the interzone.

By default, the packet filtering log is disabled in the interzone.

Format

packet-filter logging [{ **inbound** | **outbound** } [**permit** | **deny**]]

undo packet-filter logging [{ **inbound** | **outbound** } [**permit** | **deny**]]

Parameters

Parameter	Description	Value
inbound	Records logs for incoming packets. An incoming packet refers to a packet from a low-priority zone to a high-priority zone.	-
outbound	Records logs for outgoing packets. An outgoing packet refers to a packet from a high-priority zone to a low-priority zone.	-
permit	Records logs for packets that are allowed to pass through.	-
deny	Records logs for packets that are denied.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the firewall filters packets, a log is recorded if this function is enabled. By analyzing the logs, the network administrator can find potential security threats to the network and take preventive measures to protect the network.

When [{ **inbound** | **outbound** } [**permit** | **deny**]] is not configured, the device records logs for all packets. When { **inbound** | **outbound** } is configured and [**permit** | **deny**] is not configured, the device records logs for incoming or outgoing packets.

Precautions

This function takes effect only after the **packet-filter logging** and **firewall log packet-filter enable** commands are executed.

Example

Enable the packet filtering log in the interzone.

```
<Huawei> system-view
[Huawei] firewall zone trust
[Huawei-zone-trust] priority 14
[Huawei-zone-trust] quit
[Huawei] firewall zone untrust
[Huawei-zone-untrust] priority 12
[Huawei-zone-untrust] quit
[Huawei] firewall log packet-filter enable
[Huawei] firewall interzone trust untrust
[Huawei-interzone-trust-untrust] packet-filter logging
```

Related Topics

19.8.53 firewall log enable

19.8.64 port-mapping

Function

The **port-mapping** command configures the mappings between ports and application-layer protocols.

The **undo port-mapping** command deletes the mappings between ports and application-layer protocols.

Format

port-mapping { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number*

undo port-mapping { **all** | { **dns** | **ftp** | **http** | **sip** | **rtsp** | **pptp** } **port** *port-number* **acl** *acl-number* }

Parameters

Parameter	Description	Value
all	Deletes the mappings from all ports.	-
dns	Specifies the mapping between the DNS protocol and a port.	-
ftp	Specifies the mapping between the FTP protocol and a port.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
http	Specifies the mapping between the HTTP protocol and a port.	-
sip	Specifies the mapping between the SIP protocol and a port.	-
rtsp	Specifies the mapping between the RTSP protocol and a port.	-
pptp	Specifies the mapping between the PPTP protocol and a port.	-
port *port-number*	Specifies the port mapping to a protocol.	The value of *port-number* is an integer that ranges from 1 to 65535.
acl *acl-number*	Specifies the ACL that controls the packets to which port mapping is applied.	The value of *acl-number* is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Port mapping enables a server to provide various application-layer services for external systems through non-well-known ports. For example, the well-known port of the HTTP service is port 80. After port mapping is configured on the firewall, the firewall can use a non-well-known port to provide the HTTP service.

Port mapping reduces attacks to a certain service on the server.

Example

Map the HTTP service to port 10 and apply ACL 2000 to control the packets to which the mapping takes effect.

```
<Huawei> system-view
[Huawei] acl 2000
[Huawei-acl-basic-2000] rule  permit
[Huawei-acl-basic-2000] quit
[Huawei] port-mapping http port 10 acl 2000
```

Related Topics

19.8.20 display port-mapping

19.8.65 priority (security zone view)

Function

The **priority** command sets the priority for a zone.

Format

priority *security-priority*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
security-priority	Indicates the priority of a zone.	The value is an integer and the value range varies according to product models: ● AR100&AR120&AR150&AR160&AR200 series: 0 to 15 ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-48GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, and AR2204: 0 to 15 ● AR2220, AR2220E: 0 to 63 ● AR2240C: 0 to 63 ● AR2240 and AR3260, SRU40 and SRU60: 0 to 63 ● AR2204XE, AR2204XE-DC, AR2240 and AR3260, SRU80 and SRU100E: 0 to 127 ● AR2240 and AR3260, SRU200, SRU200E and SRU400: 0 to 127 ● AR3600 series: 0 to 127 . **NOTE** If *security-priority* is set to a large value, the priority of the zone is high.

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

After creating a zone, set a priority for the zone; otherwise, the zone is invalid.

The priority of a zone cannot be changed. If you want to change the priority, delete and re-create the zone and reconfigure the priority.

The local zone priority cannot be manually set. The priority of the local zone is the highest priority allowed by the local device plus 1.

Example

Set the priority of zone1 to 5.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] priority 5
```

Related Topics

19.8.18 display firewall zone

19.8.66 reset firewall app table statistics

Function

The **reset firewall app table statistics** command clears statistics on firewall application entries.

Format

reset firewall app { **servermap** | **session** } **table statistics**

Parameters

Parameter	Description	Value
servermap	Clears statistics on Servermap entries at the application layer.	-
session	Clears statistics on session entries at the application layer.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command when you need to collect new firewall application entry statistics. After you run this command, all statistics on firewall application entries are cleared.

Precautions

Statistics on firewall application entries cannot be restored after they are cleared. Exercise caution when you use the command.

Example

Clear statistics on firewall session entries at the application layer.

```
<Huawei> system-view
[Huawei] reset firewall app session table statistics
```

Related Topics

19.8.6 display firewall app table statistics

19.8.67 reset firewall ipv6 session all

Function

The **reset firewall ipv6 session all** command deletes all IPv6 entries from the firewall session table.

Format

reset firewall ipv6 session all

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command can delete all entries in a firewall session table.

Precautions

This command deletes entries from the firewall session table and modifies the firewall configurations immediately.

After this command is executed, you must wait at least 10 seconds if you need to run the command again; otherwise, a warning message is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete all IPv6 entries from a firewall session table.

```
<Huawei> system-view
[Huawei] reset firewall ipv6 session all
Warning:The current all firewall ipv6 sessions will be deleted.
Are you sure to continue?[Y/N]y
```

19.8.68 reset firewall session

Function

The **reset firewall session** command deletes entries from the firewall session table.

Format

reset firewall session all

reset firewall session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]]

reset firewall session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]]

reset firewall session destination *destination-address* [*destination-port*]

NOTE

V200R010C10 and later versions support the **protocol**, **source**, and **destination** parameters.

Parameters

Parameter	Description	Value
all	Deletes all entries from the firewall session table.	-
protocol { *protocol-number* | *protocol-name* }	Deletes entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source *source-address* [*source-port*]	Deletes entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Deletes entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command will delete entries from a firewall session table.

Precautions

After this command is executed, entries are deleted from the firewall session table and the firewall configurations are modified immediately.

After this command is executed, you must wait at least 10 seconds before running the command again; otherwise, an error message is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete all entries from a firewall session table.

```
<Huawei> system-view
[Huawei] reset firewall session all
Warning:The current all firewall sessions will be deleted.
Are you sure to continue?[Y/N]y
```

19.8.69 reset session

Function

The **reset session** command deletes entries from the session table.

Format

reset session all

reset session protocol { *protocol-number* | *protocol-name* } [**source** *source-address* [*source-port*]] [**destination** *destination-address* [*destination-port*]]

reset session source *source-address* [*source-port*] [**destination** *destination-address* [*destination-port*]]

reset session destination *destination-address* [*destination-port*]

NOTE

V200R010C10 and later versions support the **protocol**, **source**, and **destination** parameters.

Parameters

Parameter	Description	Value
all	Deletes all entries from the session table.	-
protocol { *protocol-number* | *protocol-name* }	Deletes entries with a specified protocol number or protocol type.	• The value of *protocol-number* is an integer that ranges from 1 to 255. • The value of *protocol-name* can be ICMP, TCP, or UDP.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source *source-address* [*source-port*]	Deletes entries with a specified source IP address or both a source IP address and a source port number. • *source-address* specifies the source IP address of packets. • *source-port* specifies the source port number of packets.	• *source-address* is in dotted decimal notation. • The value of *source-port* is an integer that ranges from 1 to 65535.
destination *destination-address* [*destination-port*]	Deletes entries with a specified destination IP address or both a destination IP address and a destination port number. • *destination-address* specifies the destination IP addresses of packets. • *destination-port* specifies the destination port number of packets.	• *destination-address* is in dotted decimal notation. • The value of *destination-port* is an integer that ranges from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command will delete entries from a firewall or NAT session table.

Precautions

After this command is executed, entries are deleted from session tables and the session table configurations are modified immediately.

After this command is executed, you must wait at least 10 seconds before running the command again; otherwise, an error message is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Delete all entries from a session table.

```
<Huawei> system-view
[Huawei] reset session all
Warning:The current all sessions will be deleted.
Are you sure to continue?[Y/N]y
```

19.8.70 reset firewall statistics system defend

Function

The **reset firewall statistics system defend** command deletes attack defense statistics on firewall.

Format

reset firewall statistics system defend

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

Before you run the **display firewall statistics system defend** command to collect attack defense statistics on a firewall, you can run this command to delete the old statistics.

Precautions

Statistics cannot be restored after they are cleared. Exercise caution when you delete them.

Example

Delete attack defense statistics on the firewall.

```
<Huawei> reset firewall statistics system defend
```

Related Topics

19.8.14 display firewall statistics system

19.8.71 session-log

Function

The **session-log** command configures a condition for recording logs about sessions in the firewall interzone.

The **undo session-log** command deletes a condition for recording logs about sessions in the firewall interzone.

By default, no condition is configured for recording logs about sessions in the firewall interzone.

Format

session-log *acl-number* { **inbound** | **outbound** }

undo session-log *acl-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
acl-number	Specifies the number of the ACL used to match sessions.	The value is an integer that ranges from 2000 to 3999.
inbound	Applies the ACL to the inbound sessions. **NOTE** An inbound session refers to a session from a low-priority zone to a high-priority zone.	-
outbound	Applies the ACL to the outbound sessions. **NOTE** An outbound session refers to a high-priority session sent from a zone to a low-priority zone.	-

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Create zone1 and zone2, and set their priorities to 10 and 5 respectively. Then configure an interzone between zone1 and zone2, and record logs about the inbound sessions (from zone 1 to zone 2) that match ACL 2001.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] priority 10
[Huawei-zone-zone1] quit
[Huawei] firewall zone zone2
[Huawei-zone-zone2] priority 5
[Huawei-zone-zone2] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] session-log 2001 inbound
[Huawei-interzone-zone1-zone2] quit
[Huawei] firewall log session enable
```

Related Topics

19.8.53 firewall log enable

19.8.10 display firewall interzone

19.8.72 statistics connect-number ip

Function

The **statistics connect-number ip** command sets the thresholds for the number of sessions on an IP address.

The **undo statistics connect-number ip** command restores the default thresholds.

Format

statistics connect-number ip [**range** *beginip endip*] { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*

undo statistics connect-number ip { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** }

Parameters

Parameter	Description	Value
range	Specified an IP address segment **NOTE** If the **range** parameter is not specified, this command takes effect on a single IP address.	-
beginip	Specifies the start IP address.	The value is in dotted decimal notation.

Parameter	Description	Value
endip	Specified the end IP address, which cannot be smaller than the start IP address. The start and end IP addresses must be in the same IP address segment.	The value is in dotted decimal notation.
inzone	Specifies the thresholds for the number of packets entering the zone.	-
outzone	Specifies the thresholds for the number of packets leaving the zone.	-
icmp	Specifies the thresholds for the number of ICMP packets.	-
tcp	Specifies the thresholds for the number of TCP packets.	-
udp	Specifies the thresholds for the number of UDP packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high *high-threshold*	Specifies the upper threshold value.	The value is an integer and the value range depends on the product type: ● AR120&AR150&AR160&AR200: 1-16384. The default value is 16384. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 16384. ● AR2220, AR2220E: 1-65536. The default value is 65536. ● AR2240C: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU40: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU60: 1-160000. The default value is 160000. ● AR2204XE, and AR2204XE-DC: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU80 and SRU100E: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU200 and SRU200E: 1-400000. The default value is 400000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• AR2240 and AR3260, SRU400: 1-800000. The default value is 800000. • AR3600 series: 1-400000. The default value is 400000.

Parameter	Description	Value
low *low-threshold*	Sets the lower thresholds value.	The value is an integer and the value range depends on the product type: ● AR120&AR150&AR160&AR200: 1-16384. The default value is 12288. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 12288. ● AR2220, AR2220E: 1-65536. The default value is 52224. ● AR2240C: 1-65536. The default value is 52224. ● AR2240, AR3260, and SRU40: 1-65536. The default value is 52224. ● AR2240, AR3260, and SRU60: 1-160000. The default value is 52224. ● AR2204XE, and AR2204XE-DC: 1-204800. The default value is 163840. ● AR2240, AR3260, SRU80 and SRU100E: 1-204800. The default value is 163840. ● AR2240, AR3260, SRU200 and SRU200E: 1-400000. The default value is 163840.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		• AR2240, AR3260,SRU400: 1-800000. The default value is 163840. • AR3600 series: 1-400000. The default value is 163840.

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

Before setting the thresholds for the number of packets sent to a certain IP address, run the **19.8.74 statistics ip enable** command to enable the IP address-level traffic statistics function in the zone.

Example

Configure the thresholds for the number of inbound TCP packets sent to a certain IP address. Set the upper threshold to 15000 and lower threshold to 10000.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics ip enable inzone
[Huawei-zone-zone1] statistics connect-number ip inzone tcp high 15000 low 10000
```

Related Topics

19.8.74 statistics ip enable

19.8.16 display firewall statistics zone-ip

19.8.73 statistics connect-number zone

Function

The **statistics connect-number zone** command sets the thresholds for the number of packets in a zone.

The **undo statistics connect-number zone** command restores the default thresholds for the number of packets in a zone.

 Copyright © Huawei Technologies Co., Ltd.

Format

statistics connect-number zone { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** } **high** *high-threshold* **low** *low-threshold*

undo statistics connect-number zone { **inzone** | **outzone** } { **icmp** | **tcp** | **udp** }

Parameters

Parameter	Description	Value
inzone	Specifies the thresholds for the number of packets entering the zone.	-
outzone	Specifies the thresholds for the number of packets leaving the zone.	-
icmp	Specifies the thresholds for the number of ICMP packets.	-
tcp	Specifies the thresholds for the number of TCP packets.	-
udp	Specifies the thresholds for the number of UDP packets.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high *high-threshold*	Specifies the upper threshold value.	The value is an integer and the value range varies according to product models: ● AR120&AR150&AR160&AR200: 1-16384. The default value is 16384. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 16384. ● AR2220, AR2220E: 1-65536. The default value is 65536. ● AR2240C: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU40: 1-65536. The default value is 65536. ● AR2240 and AR3260, SRU60: 1-160000. The default value is 160000. ● AR2204XE, and AR2204XE-DC: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU80 and SRU100E: 1-204800. The default value is 204800. ● AR2240 and AR3260, SRU200 and SRU200E: 1-400000. The default value is 400000. ● AR2240 and AR3260, SRU400: 1-800000. The default value is 800000. ● AR3600 series: 1-400000. The default value is 400000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
low *low-threshold*	Specifies the lower threshold value.	The value is an integer and the value range varies according to product models: ● AR120&AR150&AR160&AR200: 1-16384. The default value is 12288. ● AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-48GE-P, AR2204-27GE, AR2204E-D-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, AR2204: 1-16384. The default value is 12288. ● AR2220, AR2220E: 1-65536. The default value is 52224. ● AR2240C: 1-65536. The default value is 52224. ● AR2240, AR3260, and SRU40: 1-65536. The default value is 52224. ● AR2240, AR3260, and SRU60: 1-160000. The default value is 52224. ● AR2204XE, and AR2204XE-DC: 1-204800. The default value is 163840. ● AR2240, AR3260, SRU80 and SRU100E: 1-204800. The default value is 163840. ● AR2240, AR3260, SRU200 and SRU200E: 1-400000. The default value is 163840. ● AR2240, AR3260,SRU400: 1-800000. The default value is 163840. ● AR3600 series: 1-400000. The default value is 163840.

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

Before setting the thresholds for the number of packets in a zone, run the **19.8.75 statistics zone enable** command to enable the zone-level traffic statistics function.

Example

Configure the thresholds for the number of inbound TCP packets in a zone. Set the upper threshold to 15000 and lower threshold to 10000.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics zone enable inzone
[Huawei-zone-zone1] statistics connect-number zone inzone tcp high 15000 low 10000
```

Related Topics

19.8.75 statistics zone enable

19.8.15 display firewall statistics zone

19.8.74 statistics ip enable

Function

The **statistics ip enable** command enables the IP address-level traffic statistics collection in a zone.

The **undo statistics ip enable** command disables the IP address-level traffic statistics collection in a zone.

By default, IP address-level traffic statistics collection is disabled.

Format

statistics ip enable { **inzone** | **outzone** }

undo statistics ip enable { **inzone** | **outzone** }

Parameters

Parameter	Description	Value
inzone	Enables the IP address-level traffic statistics collection for the inbound packets of the zone.	-
outzone	Enables the IP address-level traffic statistics collection for the outbound packets of the zone.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

The IP address-based traffic statistics collection counts and monitors the TCP and UDP sessions set up by an IP address in a zone. When the number of TCP and UDP sessions set up by the IP address exceeds the threshold, the device reduces the number of sessions to the specified range.

You can enable IP address-level traffic statistics collection for inbound or outbound packets of a zone.

Inbound packets are sent from other zones to the local zone. Outbound packets are sent from the local zone to other zones.

NOTE

When both IP traffic statistics collection and fast ICMP reply are enabled on an AR160 or AR200, outbound IP traffic statistics are not collected.

Example

Enable IP address-level traffic statistics collection for inbound packets and outbound packets in zone1.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics ip enable inzone
[Huawei-zone-zone1] statistics ip enable outzone
```

Related Topics

19.8.72 statistics connect-number ip

19.8.16 display firewall statistics zone-ip

19.8.75 statistics zone enable

Function

The **statistics zone enable** command enables zone-level traffic statistics collection for the packets in a zone.

The **undo statistics zone enable** command disables zone-level traffic statistics collection for the packets in a zone.

By default, zone-level traffic statistics collection is disabled.

Format

statistics zone enable { **inzone** | **outzone** }

undo statistics zone enable { **inzone** | **outzone** }

Parameters

Parameter	Description	Value
inzone	Enables zone-level traffic statistics collection for the inbound packets of the zone.	-
outzone	Enables zone-level traffic statistics collection for the outbound packets of the zone.	-

Views

Security zone view

Default Level

2: Configuration level

Usage Guidelines

You can enable zone-level traffic statistics collection for inbound or outbound packets in a zone.

Example

Enable zone-level traffic statistics collection for inbound packets and outbound packets of zone1.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] statistics zone enable inzone
[Huawei-zone-zone1] statistics zone enable outzone
```

Related Topics

19.8.15 display firewall statistics zone

19.8.76 zone

Function

The **zone** command adds an interface to a zone.

The **undo zone** command deletes an interface from a zone.

Format

zone *zone-name*

undo zone

Parameters

Parameter	Description	Value
zone-name	Specifies the name of a zone.	The value is a string of 1 to 32 characters without hyphens (-), and must start with a letter.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

When you add an interface to a zone, ensure that the zone has been created using the **19.8.59 firewall zone** command.

NOTE

This command can only be used on Layer 3 interfaces, except the Loopback, NULL, Bridge-if, and Tunnel-Template interfaces.

Example

Add GE1/0/0 to zone1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] zone zone1
```

Related Topics

19.8.59 firewall zone

19.8.18 display firewall zone

19.9 Deep Security Configuration Commands

19.9.1 Security Policy Configuration Commands

NOTE

AR161, AR161F, AR161F-DGP, AR161FG-L, AR161FGW-L, AR161FGW-La, AR161FGW-Lc, AR161FW-P-M5, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR162F, AR168F, AR169, AR169-P-M9, AR169CVW, AR169CVW-4B4S, AR169F, AR169G-L, AR169W-P-M9, AR169RW-P-M9, and AR3670 do not support the security policy.

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.1 display engine information

Function

The **display engine information** command displays the status of IAE (Intelligent Awareness Engine) and the version of all signature databases.

Format

display engine information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the status of IAE and the version of all signature databases.

```
<Huawei> display engine information
==============================================================================

Engine on CPU 0 in slot 0:
==============================================================================

  Engine Status                    : Ready
  Compile Status                   : Idle
  IPS Engine Version               : V200R003C00SPC008
  IPS Signature Database Version   : 2017011104
  SA Signature Database Version    : 2017041201
  C&C Domain Name Database Version :
------------------------------------------------------------------------------
```

Table 19-97 Description of the **display engine information** command output

Item	Description
Engine on CPU *X* in slot *Y*	Engine information on CPU *X* in slot *Y*
Engine Status	Engine status, which can be: ● Not Run: The engine is not running. ● Initializing: The engine is initializing. ● Ready: The engine is ready.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Compile Status	Compilation status, which can be: ● Idle: The engine status is idle. ● Committing: The configuration is being committed. ● Commit Succeeded: Succeeded in committing the configuration. ● Commit Failed: Failed to commit the configuration. ● Commit Time Out: Committing the configuration timed out. ● Updating: The signature database is being updated. ● Update Succeeded: Succeeded in updating the signature database. ● Update Failed: Failed to update the signature database. ● Update Time Out: Updating the signature database timed out.
IPS Engine Version	Version of the IPS engine
IPS Signature Database Version	Version of the IPS signature database
SA Signature Database Version	Version of the application identification signature database used by the Router
C&C Domain Name Database Version	Version of the malicious domain name signature database

19.9.1.2 display security-policy

Function

The **display security-policy** command displays the security policy configuration.

Format

display security-policy { **all** | **name** *policy-name* }

Parameters

Parameter	Description	Value
all	Displays the configuration of all security policies.	-
name *policy-name*	Displays the configuration of a specified security policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view the configuration of a specified security policy or all security policies.

Example

Display the configuration of all security policies.

```
<Huawei> display security-policy all
  Policy-name: huawei
  Policy-ID: 0
   IPS: -
   URLF: -
   ACL: 0
  Reference-Num: 0
```

Display the configuration of the security policy **huawei**.

```
<Huawei> display security-policy name huawei
  Policy-name: huawei
  Policy-ID: 0
   IPS: -
   URLF: -
   ACL: 0
  Reference-Num: 0
```

Table 19-98 Description of the display security-policy command output

Item	Description
Policy-name	Name of the security policy. To configure a security policy, run the **19.9.1.15 security-policy** command.

Item	Description
Policy-ID	ID of the security policy.
IPS	IPS profile bound to the security policy. To bind an IPS profile to a security policy, run the **19.9.1.14 profile (security policy view)** command.
URLF	URL filtering profile bound to the security policy. To bind a URL filtering profile to a security policy, run the **19.9.1.14 profile (security policy view)** command.
ACL	ACL bound to the security policy. To bind an ACL to a security policy, run the **19.9.1.14 profile (security policy view)** command.
Reference-Num	Total number of profiles in the security policy.

Related Topics

19.9.1.15 security-policy
19.9.1.14 profile (security policy view)

19.9.1.3 display update configuration

Function

The **display update configuration** command displays the update configuration.

Format

display update configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the update configuration.

```
<Huawei> display update configuration
Update Configuration Information:
-------------------------------------------------------------
  Update Server              : sec.huawei.com
  Update Port                : 443
  Proxy State                : Disable
  Proxy Server               : -
  Proxy Port                 : -
  Proxy User                 : -
  Proxy Password             : -
  IPS-SDB:
    Application Confirmation  : Disable
    Schedule Update           : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time      : 03:35
  SA-SDB:
    Application Confirmation  : Disable
    Schedule Update           : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time      : 03:35
  CNC:
    Application Confirmation  : Disable
    Schedule Update           : Enable
    Schedule Update Frequency : Daily
    Schedule Update Time      : 03:35
-------------------------------------------------------------
```

Table 19-99 Description of the **display update configuration** command output

Item	Description
Update Server	IP address or domain name of the update server. The default domain name is sec.huawei.com.
Update Port	Port number of the update server.
Proxy State	Whether the proxy server is enabled. The value can be: ● Enable: The proxy server is enabled. ● Disable: The proxy server is disable.
Proxy Server	IP address or domain name of the proxy server.
Proxy Port	Port number of the proxy server.
Proxy User	User name of the proxy server.
Proxy Password	Password of the proxy server.
IPS-SDB	Update configuration of the IPS-SDB.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Application Confirmation	Whether manual installation confirmation is enabled. The value can be: ● Enable: Confirmation is required before the installation of the update file. ● Disable: The update file is automatically installed.
Schedule Update	Whether the scheduled update function is enabled. The value can be: ● Enable ● Disable
Schedule Update Frequency	Scheduled update frequency. The value can be: ● Weekly ● Daily ● Hourly
Schedule Update Time	Scheduled update time
SA-SDB	Update configuration of the application signature database
CNC	Update configuration of the malicious domain name database

19.9.1.4 display update information all-sdb

Function

The **display update information all-sdb** command displays the last record on signature database updates.

Format

display update information all-sdb

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To display the last record on signature database updates, run the **display update information all-sdb** command.

Example

Display the last record on signature database updates.

```
<Huawei> display update information all-sdb

Current Update Status:  Idle.
-----------------------------------------------------------------------------------------------------------------
  IPS-SDB latest update finish time       : 05:17:05 2017/01/24
  IPS-SDB latest update result            : Info: The IPS-SDB update succeeded.
-----------------------------------------------------------------------------------------------------------------
  SA-SDB latest update finish time        : 05:17:24 2017/01/24
  SA-SDB latest update result             : Info: The SA-SDB update succeeded.
-----------------------------------------------------------------------------------------------------------------
  CNC latest update finish time           : 05:17:37 2017/01/24
  CNC latest update result                : Info: No version for loading CNC.
-----------------------------------------------------------------------------------------------------------------
```

Table 19-100 Description of the **display update information all-sdb** command output

Item	Description
Current Update Status	Status of the update server: ● Idle: indicates that no signature database is being updated. ● Version Loading: indicates that the version is being loaded. ● Live Updating: indicates live update. ● Local Updating: indicates the local update. ● Version Rollbacking: indicates that version rollback is being performed. ● Stop Updating: indicates that the update is being stopped. ● Version Applying: indicates that the version is being downloaded. ● Version Restoring: indicates that the default version is being restored. ● Version Uninstalling: indicates that the version is being uninstalled. ● Update check: indicates that the update is being checked. ● Engine start loading: indicates that the engine start is being loaded.
latest update finish time	Last update time of the signature database

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
latest update result	Last update result of the signature database
IPS-SDB	IPS signature database
SA-SDB	Service awareness signature database
CNC	Malicious domain name database

19.9.1.5 display update host source

Function

The **display update host source** command displays the interface and source address configurations used in online update.

Format

display update host source

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays the configurations of the **update host source** command.

Example

Display the interface and source address configurations used in online update.

```
<Huawei> display update host source
-------------------------------------------------------------
Source IP Information:
    IP address              : 10.1.1.1
Source Interface Information:
    interface name          : GigabitEthernet1/0/0
-------------------------------------------------------------
```

Table 19-101 Description of the **display update host source** command output

Item	Description
Source IP Information	Source IP address information
IP address	IP address
Source Interface Information	Source interface information
interface name	Interface name

19.9.1.6 display update status

Function

The **display update status** command displays the update status.

Format

display update status

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

View the current update status.

```
<Huawei> display update status
  Current Update Status: Idle.
```

The update status of a database. The update status includes the update type and update status. The details are as follows:

Update type:

- Idle: indicates that no signature database is being updated.

- Version Load: indicates that the version is being loaded.
- Online Update: indicates online update.
- Local Update: indicates the local update.
- Version Rollback: indicates the version rollback.
- Stop Update: indicates that the update is stopped.
- Version Apply: indicates that the version is applied.
- Version Restore: indicates that the default version is restored.
- Version Uninstall: indicates that the version is being uninstalled.
- Update check: indicates that the update is checked.
- Engine start loading: indicates that the engine start is being loaded.

Update status:

- Ready to load The Update Package: indicates that the update package will be loaded soon.
- Verify The Authority: indicates that permission is being verified.
- Obtain The Update Package: indicates that the update package is being obtained.
- Load The Update Package: indicates that the update package is being loaded.
- Merge The Incremental Package: indicates that the incremental package is being merged.
- Retry The Update: indicates that the update is being retried.

For example:

- Online Update, Obtain The Update Package.: indicates online update and an update package is being downloaded.
- Version Rollback, Load The Update Package: indicates version rollback and a rollback package is being loaded.
- Version Apply, Verify The Authority.: indicates that the version is being applied and the permission is being verified.
- Local Update, Load The Update Package.: indicates local update and a update package is being loaded.

19.9.1.7 display version (security policy)

Function

The **display version** command displays version information of the IAE and signature database.

Format

display version { **engine** | **ips-sdb** | **sa-sdb** } *

Parameters

Parameter	Description	Value
engine	Displays version information of the intelligent awareness engine.	-
ips-sdb	Displays version information of the IPS signature database.	-
sa-sdb	Displays version information of the service awareness (SA) signature database.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display version information of the IPS signature database.

```
<Huawei> display version ips-sdb
IPS SDB Update Information List:
-----------------------------------------------------------------
  Current Version  :
    Signature Database Version    : 2012090600
    Signature Database Size(byte) : 28032
    Update Time                   : 08:34:03 2012/09/06
    Issue Time of the Update File : 00:00:33 2012/09/06

  Backup Version   :
    Signature Database Version    : 2012090600
    Signature Database Size(byte) : 26752
    Update Time                   : 07:18:56 2002/09/06
    Issue Time of the Update File : 20:11:40 2009/09/06

  Download Version:
    Signature Database Version    :
    Signature Database Size(byte) : 0
-----------------------------------------------------------------
```

Table 19-102 Description of the **display version** command output

Item	Description
Current Version	The following parameters indicate information about the current signature database.
Signature Database Version	Signature database version.

Item	Description
Signature Database size	Signature database size.
Update Time	The update time of the signature database, that is, the installation time of the update package.
Issue Time of the Update File	Release time of the update file. You can use the time to determine whether the update package is the latest.
Backup Version	The following parameters indicate information about. The signature database is rolled back to the version if you run the **update rollback** command.
Download Version	The following parameters indicate version information about the newly downloaded the intelligent awareness engine or signature database. The version installation is waiting for your confirmation. If the signature database size and time are 0, no version is downloaded. If you run the **undo update confirm** command to disable the automatic installation confirmation function, this information is not displayed.

19.9.1.8 engine configuration commit

Function

The **engine configuration commit** command commits the configuration of security policies.

Format

engine configuration commit

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Newly configured security policies or the modified security policies do not take effect until you run the **engine configuration commit** command to commit the

configuration. To save time, commit the configurations in batches after you have completed all security policy configurations.

Before committing configurations, ensure that the IAE is available. Otherwise the configurations committed using the **engine configuration commit** command do not take effect.

Example

Commit the security policy configurations.

```
<Huawei> system-view
[Huawei] engine configuration commit
```

19.9.1.9 engine enable

Function

The **engine enable** command enables the deep security function.

The **undo engine enable** command disables the deep security function.

By default, the system disables the deep security function.

Format

engine enable

undo engine enable

Parameters

none

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the IPS or URL filtering function, you need to purchase a license and run the **engine enable** command to enable the deep security function.

Precautions

To disable deep security, run the **undo engine enable** command, and restart the device. After the device restarts, the deep security configurations are deleted.

Example

Enable the deep security function.

```
<Huawei> system-view
[Huawei] engine enable
```

Related Topics

19.9.1.1 display engine information

19.9.1.10 engine enhanced-detection

Function

The **engine enhanced-detection** command configures the engine to work in enhanced detection mode.

The **undo engine enhanced-detection** command configures the engine to work in common detection mode.

Format

engine enhanced-detection

undo engine enhanced-detection

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the engine works in common detection mode.

After you configure the engine to work in enhanced detection mode, the detection capability of the device will be enhanced, and the detection speed will be decreased.

Example

Configure the engine to work in enhanced detection mode.

```
<Huawei> system-view
[Huawei] engine enhanced-detection
```

19.9.1.11 engine log enable

Function

The **engine log enable** command enables the log generation function for a specific module.

The **undo engine log enable** command disables the log generation function for a specified module.

Format

engine log { **ips** | **url-filter** } **enable**

undo engine log { **ips** | **url-filter** } **enable**

Parameters

Parameter	Description	Value
ips	Indicates intrusion prevention.	-
url-filter	Indicates URL filtering.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the log generation function is enabled for all modules.

Example

Enable the log generation function for IPS module.

```
<Huawei> system-view
[Huawei] engine log ips enable
```

19.9.1.12 engine log timeout

Function

The **engine log timeout** command sets the period for caching IPS and URL filtering logs.

The **undo engine log timeout** command restores the default period for caching IPS and URL filtering logs.

By default, the period for caching IPS and URL filtering logs is 1 minute.

 Copyright © Huawei Technologies Co., Ltd.

Format

engine log timeout *interval*

undo engine log timeout

Parameters

Parameter	Description	Value
interval	Specifies the period for caching IPS and URL filtering logs.	The value is an integer that ranges from 0 to 30, in minutes.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can set the period for caching logs to control the frequency for sending IPS and URL filtering logs.

For example, if many intrusions occur on the IPS-enabled device in a given period of time, the IPS module reports many logs to the device in a short time. If the device outputs logs in real time, the administrator has to flood the screen. After the period for caching logs is set, the device outputs logs only when the period is reached. This prevents the impact of log output.

Precautions

The log buffer records a maximum of 1024 logs, and outputs 16 logs each time. The output logs are deleted from the buffer.

Example

Set the period for caching IPS and URL filtering logs to 5 minutes.

```
<Huawei> system-view
[Huawei] engine log timeout 5
```

19.9.1.13 engine pass-through enable

Function

The **engine pass-through enable** command enables the pass-through mode of the engine.

The **undo engine pass-through enable** command disables the pass-through mode of the engine.

Format

engine pass-through enable

undo engine pass-through enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

The pass-through mode of the engine is disabled by default.

After the pass-through mode of the engine is enabled, the system generates events, such as debugging information or log during service processing, but does not perform actual actions. Even a block action is configured for a service, the system does not block traffic but records the service event state.

Example

Enable the pass-through mode of the engine.

```
<Huawei> system-view
[Huawei] engine pass-through enable
```

19.9.1.14 profile (security policy view)

Function

The **profile** command binds an IPS or URL filtering profile to a security policy.

The **undo profile** command unbinds an IPS or URL filtering profile from a security policy.

By default, no IPS or URL filtering profile is bound to a security policy.

Format

profile { **ips** *ips-name* | **urlf** *urlf-name* } * [**acl** *acl-id*]

undo profile

Parameters

Parameter	Description	Value
ips *ips-name*	Specifies the name of an IPS profile bound to a security policy.	The value is a string of case-sensitive characters. The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-). ● If the value of *ips-name* does not contain any space, the value contains 1 to 32 characters. ● If the value of *ips-name* contains spaces, you must enclose the value with double quotation marks (""), for example, "user for test", and the value contains 3 to 34 characters.
urlf *urlf-name*	Specifies the name of a URL filtering profile bound to a security policy.	The value is a string of case-sensitive characters. The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-). ● If the value of *urlf-name* does not contain any space, the value contains 1 to 32 characters. ● If the value of *urlf-name* contains spaces, you must enclose the value with double quotation marks (""), for example, "user for test", and the value contains 3 to 34 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl *acl-id*	Specifies the number of an ACL. If no ACL is specified, the device detects all traffic passing through interzones.	The value is an integer. • 2000 to 2999: basic ACLs • 3000 to 3999: advanced ACLs

Views

Security policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device uses a security policy to implement integrated detection of content security.

Integrated detection of content security indicates that the device uses the Intelligent Awareness Engine to detect and process the content of one flow at one time, implementing content security functions including intrusion defense IPS or URL filtering.

After this command binds an IPS or URL filtering profile to a security policy and the security policy is applied to an interzone, the device performs IPS or URL filtering for traffic passing through the interzone.

Prerequisites

- A URL filtering profile has been created using the **19.9.3.19 profile type url-filter name** command if the URL filtering profile needs to be bound to a security policy.
- An IPS profile has been created using the **profile type ips name** command if the IPS profile needs to be bound to a security policy.
- An ACL has been created using the **19.7.4 acl (system view)** command if the ACL needs to be bound to a security policy.

Precautions

To configure various content security protection functions (for example, URL filtering and IPS need to be configured simultaneously), configure a URL filtering profile and IPS profile, and run the **profile** command to bind the URL filtering profile and IPS profile to a security policy.

If a security policy has been applied to the interzone using the **19.9.1.16 security-policy (interzone view)** command, run the **undo security-policy** command to unbind the security policy from the interzone, and then bind the IPS or URL filtering profile to the security policy.

 Copyright © Huawei Technologies Co., Ltd.

Currently, only ACL4 is supported for IPS or URL filtering. When an ACL is bound to a security policy, pay attention to the following points:

- If the ACL rule defines a permit clause, the device detects traffic matching the ACL rule.
- If the ACL rule defines a deny clause, the device does not detect traffic matching the ACL rule.
- If traffic does not match the ACL, the device does not detect the traffic.

Example

Bind a URL filtering profile **huawei** to a security policy **huawei**.

```
<Huawei> system-view
[Huawei] profile type url-filter name huawei
[Huawei-profile-url-filter-huawei] quit
[Huawei] security-policy huawei
[Huawei-security-policy-huawei] profile urlf huawei
```

Bind a IPS profile **huawei** to a security policy **huawei**.

```
<Huawei> system-view
[Huawei] profile type ips name huawei
[Huawei-profile-ips-huawei] quit
[Huawei] security-policy huawei
[Huawei-security-policy-huawei] profile ips huawei
```

Related Topics

19.9.1.16 security-policy (interzone view)

19.9.2.53 profile type ips name

19.9.3.19 profile type url-filter name

19.9.1.15 security-policy

Function

The **security-policy** command creates a security policy and displays its view, or directly displays the view of an existing security policy.

The **undo security-policy** command deletes a security policy.

By default, no security policy is created.

Format

security-policy *policy-name*

undo security-policy *policy-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a security policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

As the network develops continuously, there are various types of potential risks such as Trojan horses, worms, and viruses in packets. Packet filtering rules based on the 5-tuple (source address, destination address, source port, destination port, protocol type) used to control traffic forwarding cannot meet requirements. Enterprises require more secure methods to protect network security.

To monitor network traffic, the device uses a security policy to implement integrated detection of content security. Integrated detection of content security indicates that the device uses the Intelligent Awareness Engine to detect and process the content of one flow at one time, implementing content security functions including intrusion defense and URL filtering. By configuring a security policy, the device controls traffic forwarding based on users and applications, provides traffic content security detection, and implements content security functions of intrusion defense, and URL filtering to ensure network security.

Follow-up Procedure

Run the **19.9.1.16 security-policy (interzone view)** command to create an interzone and enter the interzone view.

Example

Create a security policy **security**.

```
<Huawei> system-view
[Huawei] security-policy security
[Huawei-security-policy-security]
```

Related Topics

19.9.1.16 security-policy (interzone view)

19.9.1.2 display security-policy

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.16 security-policy (interzone view)

Function

The **security-policy** command binds a security policy to an interzone.

The **undo security-policy** command unbinds a security policy from an interzone.

By default, no security policy is bound to an interzone.

Format

security-policy *policy-name*

undo security-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a security policy to be bound to an interzone.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A security policy must be bound to an interzone so that IPS or URL filtering in the security policy can be used to defend against application layer attacks (for example, buffer overflow attacks, Trojan horses, and worms attacks) or control HTTP access rights.

Prerequisites

The **19.8.51 firewall interzone** command has been executed to create an interzone and enter the interzone view.

The **19.9.1.15 security-policy** command has been executed to create a security policy.

Example

Bind the security policy **security** to an interzone.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] priority 10
[Huawei-zone-zone1] quit
[Huawei] firewall zone zone2
[Huawei-zone-zone2] priority 13
[Huawei-zone-zone2] quit
[Huawei] security-policy security
[Huawei-security-policy-security] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone1-zone2] security-policy security
```

Related Topics

19.8.10 display firewall interzone

19.9.1.17 update abort

Function

The **update abort** command aborts the update process.

Format

update abort

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

The **update abort** command can only be used for online/immediate updates or update retries. In online/immediate updates, the device needs to connect to the update center. If the network rate is too low and impacts the services and device performance, you can run the **update abort** command to abort the update and then retry updating when appropriate. In update retires, you cannot perform other update operations. If you need to use another update method, run the **update abort** command to abort the update process first.

Example

Abort the update process.

```
<Huawei> system-view
[Huawei] update online cnc
[Huawei] update abort
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.18 update apply

Function

The **update apply** command installs the downloaded update files.

Format

update apply { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Installs the malicious domain name database update files.	-
ips-sdb	Installs the IPS signature database update files.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If manual installation confirmation has been enabled by the **update confirm** command, run the **update apply** command to install the update files. If update files have been uploaded to the device memory using FTP, run the **update local** command to install them.

Example

Install the malicious domain name database update files.

```
<Huawei> system-view
[Huawei] update apply cnc
```

19.9.1.19 update confirm

Function

The **update confirm** command enables manual confirmation of database installation.

The **undo update confirm** command disables manual confirmation of database installation.

Format

update confirm { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

undo update confirm { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The manual confirmation of database installation is disabled by default. That is, the device automatically installs the upgrade files after downloading them.

If you enable manual confirmation of database installation, the device will not automatically install the upgrade files after downloading them. You need to run the **update apply** command to install the upgrade files.

Example

Disable manual confirmation for the malicious domain name database installation.

```
<Huawei> system-view
[Huawei] undo update confirm cnc enable
```

19.9.1.20 update force apply

Function

The **update force apply** command forcibly installs the downloaded update files.

Format

update force apply { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Forcibly installs the malicious domain name database update files.	-
ips-sdb	Forcibly installs the IPS signature database update files.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force apply** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update apply** command to download update files, the update fails in case of insufficient system memory. In this case, you can run the **update force apply** command to forcibly install downloaded update files.

Example

Forcibly install the malicious domain name database update files.

```
<Huawei> system-view
[Huawei] update force apply cnc
```

19.9.1.21 update force local

Function

The **update force local** command configures forcible manual update of local signature database. The signature database is uploaded to the device memory using FTP or SFTP.

Format

update force local { **cnc** | **ips-sdb** | **sa-sdb** } **file** *filename*

Parameters

Parameter	Description	Value
cnc	Indicates forcible manual update of the malicious domain name database.	-
ips-sdb	Indicates forcible manual update of the IPS signature database.	-
sa-sdb	Indicates forcible manual update of the SA signature database.	-
file *filename*	Indicates the file used for the update. You must upload the update files to the device memory before the update.	The absolute path of a file is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force local** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update local** command to update signature databases locally, the update fails in case of insufficient system memory. In this case, you can run the **update force local** command to forcibly update local signature databases.

Example

Forcibly update the local malicious domain name database using file flash:/cnc_h10010000_2017111500.zip.

```
<Huawei> system-view
[Huawei] update force local cnc file flash:/cnc_h10010000_2017111500.zip
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.1.22 update force online

Function

The **update force online** command forcibly configures the immediate updates of the databases.

Format

update force online { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Forcibly indicates immediate update of the malicious domain name database.	-
ips-sdb	Forcibly indicates immediate update of the IPS signature database.	-
sa-sdb	Forcibly indicates immediate update of the SA signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force online** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update online** command to immediately update signature databases, the update fails in case of insufficient system memory. In this case, you can run the **update force online** command to immediately update signature databases.

Example

Forcibly update the malicious domain name database immediately.

```
<Huawei> system-view
[Huawei] update force online cnc
```

19.9.1.23 update force restore sdb-default

Function

The **update force restore sdb-default** command forcibly restores the signature database to the factory default version.

Format

update force restore sdb-default { **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
ips-sdb	Forcibly restores the IPS signature database to the factory default version.	-
sa-sdb	Forcibly restores the SA signature database to the factory default version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

- After you run the **update force restore sdb-default** command, the signature database files corresponding to the rollback version and download version of the signature database will be deleted.
- Running the **update force restore sdb-default** command causes the IAE not to take effect within a short period, resets all IAE-related session tables, and interrupts some services. Therefore, exercise caution when running this command.

When you run the **update restore sdb-default** command to restore the signature database to the default version, the update fails if the system memory is insufficient. In this case, you can attempt to run the **update force restore sdb-default** command to forcibly restore the signature database to the default version.

 Copyright © Huawei Technologies Co., Ltd.

Example

Forcibly restore the IPS signature database to the factory default version.

```
<Huawei> system-view
[Huawei] update force restore sdb-default ips-sdb
```

19.9.1.24 update force rollback

Function

The **update force rollback** command forcibly rolls back the version of a specified database.

Format

update force rollback { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Forcibly rolls back the malicious domain name database version.	-
ips-sdb	Forcibly rolls back the IPS signature database version.	-
sa-sdb	Forcibly rolls back the SA signature database version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

Running the **update force rollback** command causes the IAE not to take effect in a short time and resets all IAE-related session tables. Therefore, exercise cautions when using this command.

When you run the **update rollback** command to roll back signature database versions, the update fails in case of insufficient system memory. In this case, you can run the **update force rollback** command to forcibly roll back signature database versions.

 Copyright © Huawei Technologies Co., Ltd.

Example

Forcibly roll back the version of the malicious domain name database.

```
<Huawei> system-view
[Huawei] update force rollback cnc
```

19.9.1.25 update host source

Function

The **update host source** command specifies an interface IP address and VPN instance as the source IP address and VPN instance for online update request packets.

The **update host source ip** command specifies the source IP address of online update request packets.

The **undo update host source** command deletes the specified source IP address and VPN instance and interface of online update request packets.

The **undo update host source ip** command deletes the specified source IP address of online update request packets.

Format

update host source *interface-type interface-number*

update host source ip *ip-address* [**vpn-instance** *vpn-instance*]

undo update host source

undo update host source ip

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the interface type and interface number.	-
ip *ip-address*	Specifies the source IP address of online update request packets.	The value is in dotted decimal notation.
vpn-instance *vpn-instance*	Specifies the name of a VPN instance.	The name is a string of 1 to 31 characters.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

In normal cases, these commands are optional. If the administrator does not configure these commands, the system searches a route based on the IP address of the update server and uses the IP address of the outgoing interface as the source IP address of update request packets.

When the Router connects to the Internet through a VPN instance, these commands are mandatory. If the commands are not configured, the update will fail.

- When **update host source** *interface-type interface-number* is configured, the interface must be bound to the corresponding VPN instance name.
- When the **update host source ip** *ip-address* command is configured, **vpn-instance** *vpn-instance* must be specified.

Instructions on these commands are as follows:

- The interface specified in the **update host source** *interface-type interface-number* command is not necessarily the outgoing interface of update request packets. This command actually specifies the IP address of a specific interface as the source IP address. To send update request packets, the system checks the route information to determine the outgoing interface.
- If the interface has multiple IP addresses, run the **update host source ip** *ip-address* command to set the source IP address of update request packets and ensure that the Router can receive the reply packets. Otherwise, the online update may fail.

  The source IP address of the upgrade request packet cannot be the loopback address.
- When both **update host source** *interface-type interface-number* and **update host source ip** *ip-address* [**vpn-instance** *vpn-instance*] are configured, the system preferentially uses the specified IP address as the source IP address of update request packets. That is, the **update host source** *interface-type interface-number* command does not take effect.

Example

Set the interface used for online update to GigabitEthernet1/0/0.

```
<Huawei> system-view
[Huawei] interface GigabitEthernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip address 10.1.1.1 24
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] update host source GigabitEthernet 1/0/0
```

Set the source IP address of online update request packets to 10.1.1.1.

```
<Huawei> system-view
[Huawei] update host source ip 10.1.1.1
```

19.9.1.26 update local

Function

The **update local** command configures manual update of local signature database.

Format

update local { **cnc** | **ips-sdb** | **sa-sdb** } **file** *filename*

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-
file *filename*	Specifies the update file. You must upload the update files to the device memory using FTP or SFTP before the update.	The absolute path of a file is a string of 1 to 64 characters without spaces.

Views

System view

Default Level

3: Management level

Usage Guidelines

If the device cannot connect to the network, download the update files from the security center (isecurity.huawei.com) to a PC and upload the files to the device memory using FTP or SFTP. Then run the **update local** command to update the databases.

Example

Manually update the local malicious domain name database using file flash:/cnc_h10010000_2017111500.zip.

```
<Huawei> system-view
[Huawei] update local cnc file flash:/cnc_h10010000_2017111500.zip
```

19.9.1.27 update online

Function

The **update online** command configures the immediate updates of the databases.

Format

update online { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

The online update modes of signature databases include scheduled update and immediate update. Generally, scheduled update is used. In some case, a signature database needs to be updated to the latest version immediately. If the scheduled update period does not expire, you can run the **update online** command to start immediate update. Before the update, you need to check whether the domain name or IP address of the update center is accessible.

Example

Update the malicious domain name database immediately.

```
<Huawei> system-view
[Huawei] update online cnc
```

19.9.1.28 update online-mode

Function

The **update online-mode** command sets the online update mode of the signature database.

The **undo update online-mode** command restores the default setting.

Format

update online-mode { **http** | **https** }

undo update online-mode

Parameters

Parameter	Description	Value
https	Indicates the HTTPS update mode, in which the device uses HTTPS to send update requests and download signature databases.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the online update is in HTTPS mode.

NOTE

Update in HTTP mode is risky, and update in HTTPS mode is recommended. To perform update in HTTP mode, you must strictly restrict security policy matching conditions.

This setting applies only to online update in direct update scenarios (including scheduled update and immediate update) but not online update through a proxy server.

Example

Set the online signature database update mode to HTTP.

```
<Huawei> system-view
[Huawei] update online-mode http
```

19.9.1.29 update proxy

Function

The **update proxy** command sets the IP address or domain name of the proxy server.

The **undo update proxy** command deletes the proxy server setting.

Format

update proxy { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*] [**user** *user-name* [**password** *password*]]

undo update proxy

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name of the proxy server.	The value is a string of 1 to 64 characters, spaces not supported.
ip *ip-address*	Specifies the IP address of the proxy server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the proxy server.	The value is an integer ranging from 1 to 65535. The default value is 80.
user *user-name*	Specifies the user name for logging in to the proxy server.	The user name is a string and must have been set on the proxy server. The length of a user name without spaces ranges from 1 to 32 characters. The length of a user name with spaces ranges from 3 to 34 characters. If a user name contains spaces, it must be enclosed with quotation marks (such as "user for test").
password *password*	Specifies the password for logging in to the proxy server.	The password is a string and must be the same as the password corresponding to the user name of the proxy server. ● The length of a password without spaces ranges from 1 to 32 characters. The length of a password with spaces ranges from 3 to 34 characters. If a password contains spaces, it must be enclosed with quotation marks. ● The password cannot be composed only by asterisks (*).

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None.

Example

Configure a proxy server.

```
<Huawei> system-view
[Huawei] update proxy ip 192.168.2.33 port 8080 user test password Hello!123
```

19.9.1.30 update proxy enable

Function

The **update proxy enable** command enables the signature database proxy update function.

The **undo update proxy enable** command disables the signature database proxy update function.

Format

update proxy enable

undo update proxy enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the signature database proxy update function is disabled.

After this function is enabled, you must run the **update proxy** command to set the proxy server. Otherwise, the firewall cannot connect to the update server through the proxy server.

NOTE

During signature database update through a proxy server, HTTP will be used, causing security risks. You are advised to update the signature database in local or direct update mode.

Example

Enable the signature database proxy update function.

```
<Huawei> system-view
[Huawei] update proxy enable
Info: The proxy function uses the HTTP protocol, which is an unsecured protocol, user name and password plaintext transmission.
```

19.9.1.31 update restore sdb-default

Function

The **update restore sdb-default** command restores the signature database to the factory default version.

Format

update restore sdb-default { **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
ips-sdb	Restores the IPS signature database to the factory default version.	-
sa-sdb	Restores the application identification signature database to the factory default version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

NOTICE

After you run the **update restore sdb-default** command, the signature database files corresponding to the rollback version and download version of the signature database will be deleted. Therefore, exercise caution when running this command.

Example

Restore the IPS signature database to the factory default version.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] update restore sdb-default ips-sdb
```

19.9.1.32 update rollback

Function

The **update rollback** command rolls back the version of a specified database.

Format

update rollback { **cnc** | **ips-sdb** | **sa-sdb** }

Parameters

Parameter	Description	Value
cnc	Rolls back the malicious domain name database version.	-
ips-sdb	Rolls back the IPS signature database version.	-
sa-sdb	Rolls back the application identification signature database version.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Run the **update rollback** command to roll back the current version of a specified database to an earlier version. Only one earlier version is available for version rollback. If you run the **update rollback** command a second time, the version of the database is rolled back to the current version again.

NOTE

The version rollback function is unavailable before the second update is complete.

Example

Roll back the version of the malicious domain name database.

```
<Huawei> system-view
[Huawei] update rollback cnc
```

19.9.1.33 update schedule

Function

The **update schedule** command sets scheduled update time for the signature database.

Format

update schedule [{ **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*]

update schedule { **cnc** | **ips-sdb** } { **hourly** *minute* | { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time* }

update schedule sa-sdb { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*

Parameters

Parameter	Description	Value
daily	Indicates daily update of a signature database.	-
weekly { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** }	Indicates weekly update of a signature database.	-
cnc	Indicates scheduled update time of malicious domain name database.	-
ips-sdb	Indicates scheduled update time of IPS-SDB.	-
sa-sdb	Indicates scheduled update time of SA-SDB.	-
hourly	Indicates hourly update of IP reputation database. **NOTE** The AR3260 does not support this parameter.	-
minute	Specifies the minute.	The value ranges from 0 to 59.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time	Specifies the time in a day for the scheduled update of the signature database.	The format is **hh:mm**. The hour and minute are separated by a colon (:). The **hh** value is an integer ranging from 0 to 23 and the **mm** value is an integer ranging from 0 to 59.

Views

System view

Default Level

3: Management level

Usage Guidelines

- Using the **update schedule** command, you can update all signature databases daily at any point during the time range 22:00 to 08:00.
- Using the **update schedule** [{ **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time*] command, you can configure scheduled update time for all signature databases.
- Using the **update schedule** { **cnc** | **ips-sdb** } { **hourly** *minute* | { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time* } command, you can configure scheduled update time for a signature database.
- Using the **update schedule sa-sdb** { **daily** | **weekly** { **Mon** | **Tue** | **Wed** | **Thu** | **Fri** | **Sat** | **Sun** } } *time* command, you can configure scheduled update time for the application identification signature database.

Example

Configure a scheduled update of signature databases at 02:00 every Wednesday.

```
<Huawei> system-view
[Huawei] update schedule weekly wed 02:00
```

Configure a scheduled update of signature database at 03:00 every day.

```
<Huawei> system-view
[Huawei] update schedule daily 03:00
```

19.9.1.34 update schedule enable

Function

The **update schedule enable** command enables scheduled update time for the signature database.

The **undo update schedule enable** command disables scheduled update time for the signature database.

Format

update schedule { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

undo update schedule { **cnc** | **ips-sdb** | **sa-sdb** } **enable**

Parameters

Parameter	Description	Value
cnc	Indicates the malicious domain name database.	-
ips-sdb	Indicates the IPS signature database.	-
sa-sdb	Indicates the application identification signature database.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, scheduled update time for the signature database is enabled.

Example

Enable the scheduled update time function for the malicious domain name database.

```
<Huawei> system-view
[Huawei] update schedule cnc enable
```

19.9.1.35 update schedule retry-download interval

Function

The **update schedule retry-download interval** command sets the retry interval for downloading the signature database for scheduled update.

The **undo update schedule retry-download interval** command restores the default interval.

Format

update schedule retry-download interval *interval-value*

undo update schedule retry-download interval

Parameters

Parameter	Description	Value
interval-value	Specifies the retry interval for downloading the signature database for scheduled update.	The value is an integer ranging from 300 to 3600, in second. The default value is 3600 seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

In case of scheduled update, if the update server is busy, the signature database fails to be download, causing an update failure. Then, the device will retry downloading the signature database. The **update schedule retry-download interval** command is used to set the retry interval for downloading the signature database.

Example

Set the retry interval for downloading the signature database for scheduled update to 1800s.

```
<Huawei> system-view
[Huawei] update schedule retry-download interval 1800
```

19.9.1.36 update schedule retry-load interval

Function

The **update schedule retry-load interval** command sets the retry interval for loading the signature database for scheduled update.

The **undo update schedule retry-load interval** command restores the default interval.

Format

update schedule retry-load interval *interval-value*

undo update schedule retry-load interval

Parameters

Parameter	Description	Value
interval-value	Specifies the retry interval for loading the signature database for scheduled update.	The value is an integer ranging from 300 to 3600, in second. The default value is 3600 seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

In case of scheduled update, if the memory of the device is insufficient, the device fails to load the downloaded signature database. Then, the device will retry loading the signature database. The **update schedule retry-load interval** command is used to set the retry interval for loading the signature database.

Example

Set the retry interval for loading the signature database for scheduled update to 1800s.

```
<Huawei> system-view
[Huawei] update schedule retry-load interval 1800
```

19.9.1.37 update server

Function

The **update server** command sets the IP address or domain name of the update server.

The **undo update server** command deletes the IP address or domain name of the update server.

Format

update server { **domain** *domain-name* | **ip** *ip-address* } [**port** *port-number*]

undo update server

Parameters

Parameter	Description	Value
domain *domain-name*	Specifies the domain name of the update server.	The value is a string of 1 to 64 characters, spaces not supported.
ip *ip-address*	Specifies the IP address of the update server.	The value is in dotted decimal notation.
port *port-number*	Specifies the port number of the update server.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the domain name of the update server is sec.huawei.com, the HTTP port number is 80 and the HTTPS port number is 443.

Example

Set the IP address of the update server to 10.1.1.1 and port number to 86.

```
<Huawei> system-view
[Huawei] update server ip 10.1.1.1 port 86
```

19.9.2 Intrusion Prevention Configuration Commands

NOTE

- The following product models support IPS function:
  - AR160 series: AR169BF, AR169FGW-L, AR169FGVW-L, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR168F-4P, AR161EW, AR161EW-M1, AR161FW, AR161FV-1P, and AR169FVW.
  - AR1200 series: AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: AR2204, AR2204XE, AR2204XE-DC, AR2220, AR2220E, AR2240, and AR2240C.
  - AR3200 series: All models.

19.9.2.1 action (IPS signature filter view)

Function

The **action** command configures the action for an IPS signature filter.

The **undo action** command restores the default configuration.

Format

action { **alert** | **block** | **default** }

undo action

Parameters

Parameter	Description	Value
alert	Sets the action to **alert**. The device permits packets and generates a log when the packets match a signature in the signature filter.	-
block	Sets the action to **block**. The device discards packets and generates a log when the packets match a signature in the signature filter.	-
default	Uses the default action.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

The default action for the signature filter is **default**. That is, when a packet matches a signature in the signature filter, the device performs the action for the signature.

After you set the action for the signature filter to **alert** or **block**, the actions for the signatures in the signature filter no longer take effect. When packets match a signature in the signature filter, the device performs the action for the signature filter.

Example

Set the action for IPS signature filter **hello** to **alert**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] action alert
```

19.9.2.2 action (user-defined IPS signature view)

Function

The **action** command configures the action for a user-defined signature.

The **undo action** command restores the default configuration.

Format

action { **alert** | **block** | **allow** }

undo action

Parameters

Parameter	Description	Value
alert	Sets the action to **alert**. The device permits packets and generates a log when the packets match the signature.	-
block	Sets the action to **block**. The device discards packets and generates a log when the packets match the signature.	-
allow	Sets the action to **allow**. The device permits packets when the packets match the signature.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

If a signature is referenced in a signature filter, the action for the signature filter applies if packets match the signature.

The default action for the signature is **alert**.

Example

Configure a user-defined signature. Set the ID to **1**, name to **mysignature**, and action to **block**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] action block
```

19.9.2.3 application (IPS signature filter view)

Function

The **application** command configures an application name in an IPS signature filter.

The **undo application** command removes the configured application name.

Format

application { *application-name* &<1-10> | **all** }

undo application { *application-name* &<1-10> | **all** }

Parameters

Parameter	Description	Value
application-name &<1-10>	Specifies the name of the application. A maximum of 10 application names can be specified.	-
all	Indicates all applications.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

The application name specified in this command is a filtering condition in the IPS signature filter and helps filter packets of the specified application.

&<1-10> indicates that a maximum of 10 applications can be specified at a time. To specify more applications, repeat this command. A packet matches the filtering condition if the application type of this packet matches any of the specified applications.

If no application is specified, the IPS does not filter packets based on application names.

Example

In IPS profile **profile1**, configure **example_application** as the filtering condition in IPS signature filter **hello**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] application example_application
```

19.9.2.4 assoc-check enable

Function

The **assoc-check enable** command enables the correlation detection function.

The **undo assoc-check enable** command disables the correlation detection function.

Format

assoc-check enable

undo assoc-check enable

Parameters

None

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the function is enabled.

Intrusion prevention detects traffic by signatures that can be either basic signatures or correlation signatures. A basic signature describes a simple network attack. A correlation signature is composed of one or more basic signatures and describes a complex network attack. Correlation detection is implemented on the basis of correlation signatures.

If traffic matches a correlation signature, the system displays only the matched correlation signature, but not the matched basic signature of the correlation signature. After the correlation detection function is disabled, when traffic matches a basic signature included in a correlation signature, the system displays the basic signature.

Disabling correlation detection decreases the security detection capability of the system and therefore is not recommended. In addition, it is easy for traffic to match a basic signature included in a correlation signature. Therefore, correlation detection deteriorates the device performance.

Example

Enable correlation detection in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] assoc-check enable
```

19.9.2.5 category (IPS signature filter view)

Function

The **category** command adds the Intrusion Prevention System (IPS) signature of the specified category to an IPS signature filter.

The **undo category** command deletes the IPS signature of the specified category from an IPS signature filter.

Format

category { *category-name* &<1-10> | **all** }

undo category { *category-name* &<1-10> | **all** }

Parameters

Parameter	Description	Value
category-name &<1-10>	Specifies the category name. **&<1-10>** indicates that a command can have 1 to 10 such parameter values.	-
all	Indicates all categories.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

You can add signatures of a maximum of 10 categories to the signature filter at a time. To add signatures of more categories, repeat this command.

Signature categories may vary with IPS signature files. After you update the IPS signature database, view the changes of signature categories and modify configurations accordingly.

NOTE

When the IPS signature database is not loaded, only parameter **all** is available.

Example

Configure category **Remote-File-Inclusion** for IPS signature filter **hello** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] category Remote-File-Inclusion
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.6 check (user-defined signature rule view)

Function

The **check** command configures the matching order of user-defined signature rules.

The **undo check** command restores the default configuration.

Format

check { **sequential** | **random-order** }

undo check

Parameters

Parameter	Description	Value
sequential	Indicates that user-defined signature rules are matched sequentially.	-
random-order	Indicates that user-defined signature rules are matched in random order.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

User-defined signature rules are matched in random order by default.

If you select **sequential**, conditions are matched in ascending order by ID. An intrusion matches a rule only when the intrusion matches all conditions of the rule in configuration order.

If you select **random-order**, conditions are matched in random order. An intrusion matches a rule when the intrusion matches all conditions of the rule in either configuration order or random order.

NOTE

Selecting **sequential** is not recommended. If you select it, the matching order becomes stricter, which may cause false positives during intrusion detection. Sequential check does not apply to value match (including:equal, gthan, lthan, and noequal).

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the matching order to **sequential**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] check sequential
```

19.9.2.7 cnc domain-filter enable

Function

The **cnc domain-filter enable** command enables the domain name-based filtering function.

The **undo cnc domain-filter enable** command disables the domain name-based filtering function.

Format

cnc domain-filter enable [**action** { **alert** | **block** }]

undo cnc domain-filter enable

Parameters

Parameter	Description	Value
action	Indicates the action.	-
alert	Indicates that the device permits packets matching a malicious domain name, but generates an alarm and logs the event.	-
block	Indicates that the device discards packets matching a malicious domain name and logs the event.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, domain name-based filtering is disabled.

After domain name-based filtering is enabled, the default action is **alert** for packets matching the specified condition. After running **cnc domain-filter enable** to enable the function or **undo cnc domain-filter enable** to disable the function, run **engine configuration commit** to commit the configuration change to apply it.

The domain name-based filtering function enables the device to filter out packets using the malicious domain name signature database. Upon receiving a packet matching a malicious domain name, the device implements the specified action and logs the threats for auditing and troubleshooting.

Example

In IPS profile **profile1**, enable domain name-based filtering and set **action** to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] cnc domain-filter enable action block
[Huawei-profile-ips-profile1] quit
[Huawei] engine configuration commit
```

19.9.2.8 cnc domain-filter exception domain-name

Function

The **cnc domain-filter exception domain-name** command adds an exception domain name.

The **undo cnc domain-filter exception domain-name** command deletes an exception domain name.

Format

cnc domain-filter exception domain-name *domain-name*

undo cnc domain-filter exception { **domain-name** *domain-name* | **all** }

Parameters

Parameter	Description	Value
domain-name	Specifies a malicious domain name.	The value is a string of 4 to 255 characters.
all	Indicates all malicious domain names.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

These commands are used to add or delete exception domain names. To view all specified exception domain names, run **display cnc domain-filter exception**.

The exception domain name must be a domain name in the malicious domain name signature database. Adding any domain name that is not in the malicious domain name signature database is pointless. You can determine whether to add a malicious domain name as an exception domain name based on the threat logs. After a malicious domain name is added as an exception domain name, the device does not filter out the packets matching the exception domain name.

Example

Add **www.example.com** as an exception domain name.

```
<Huawei> system-view
[Huawei] cnc domain-filter exception domain-name www.example.com
```

Delete all exception domain names.

```
[Huawei] undo cnc domain-filter exception all
```

19.9.2.9 collect-attack-evidence enable (intrusion prevention profile view)

Function

The **collect-attack-evidence enable** command enables attack evidence collection of intrusion prevention.

The **undo collect-attack-evidence enable** command disables attack evidence collection of intrusion prevention.

Format

collect-attack-evidence enable

undo collect-attack-evidence enable

Parameters

None

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The attack evidence collection function of intrusion prevention is disabled by default.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Attack evidence collection does not apply to HTTPS traffic.
- Attack evidence collection is for troubleshooting only. Because attack evidence collection compromises system performance, you must enable it only when necessary and disable it immediately after you finish attack evidence collection.

After you enable the attack evidence collection function, the device starts to collect the packets that match the intrusion prevention profile. If the action in the intrusion prevention profile is block, the device collects only the identified threat packets and previous packets. Subsequent packets of the same session are blocked and discarded by the device, and therefore are not collected. If the action in the intrusion prevention profile is not block, the device collects all threat packets of the session.

One of the extreme conditions is that: The action in the intrusion prevention profile is not block and the device collects the packets that match the intrusion prevention profile. However, the storage space is insufficient after the device collects some threat packets. As a result, the device stops attack evidence collection.

Example

Enable attack evidence collection in intrusion prevention profile **hello**.

```
<Huawei> system-view
[Huawei] profile type ips name hello
[Huawei-profile-ips-hello] collect-attack-evidence enable
```

19.9.2.10 condition (user-defined signature rule view)

Function

The **condition** command configures a matching condition of a user-defined signature rule.

The **undo condition** command deletes a matching condition from a user-defined signature rule.

Format

condition [*condition-id*] **field** *field-name* **operate** { **equal** | **gthan** | **lthan** | **noequal** } **value** *value-content* [**direction** *direction* | **qualifier http-method** *http-method*] *

condition [*condition-id*] **field** *field-name* **operate pmatch value** *value-content* [**offset** { *offset-value* | **begin** }] [**depth** *depth-value*] [**direction** *direction* | **qualifier http-method** *http-method*] *

undo condition { *condition-id* | **all** }

Parameters

Parameter	Description	Value
condition-id	Specifies the ID of a condition.	The value is an integer ranging from 1 to 4.
field *field-name*	Specify a protocol field to be checked.	After you run the **protocol** command in the user-defined IPS signature view, you can check the field of the specified protocol. The default protocol of a user-defined signature is HTTP. Therefore, the *field-name* is the HTTP protocol field.
operate { **equal** | **gthan** | **lthan** | **noequal** }	Indicates the comparison action.	• **equal** indicates that the value of *field-name* equals to the value of *value-content*. • **gthan** indicates that the value of *field-name* is greater than the value of *value-content*. • **lthan** indicates that the value of *field-name* is less than the value of *value-content*. • **noequal** indicates that the value of *field-name* does not equal to the value of *value-content*.
value *value-content*	Specifies the field value.	• If you set *field-name* to **DNS.RR.A.Address**, the value is an IPv4 address in dotted decimal notation. • If you set *field-name* to **MSRPC.Interface**, the value is a hexadecimal string of 32 characters. • If you set *field-name* to other value: – If you set **operate** to **pmatch**, the value is a string of 7 to 127 characters. If the keyword contains any space and question mark (?), the value is a string of 9 to 129 characters and must be enclosed with double quotation marks (""), for example, "abcd wd?". If the keyword contains quotation marks, replace the quotation marks with \x22, for example, to set keyword **abc"ddd**, enter **abc \x22ddd**. – If you set **operate** to another value, the value is an integer ranging from 0 to 4294967295.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
operate pmatch	Sets the comparison action to pattern matching.	If the *field-name* field contains the *value-content* string, the condition is matched.
offset *offset-value*	Specifies the offset of pattern matching.	The value is an integer ranging from 0 to 65535. The default value is 0, indicating that a match is searched for from the start location of the *field-name* field. As long as a match of the *value-content* value is found in the *depth-value* range, the user-defined signature rule is matched. When the *offset-value* is 1, a match is searched for from the second byte of the *field-name* field. As long as a match of the *value-content* value is found in the *depth-value* range, the user-defined signature rule is matched. ● If *field-name* is set to **MSRPC.Interface**, the **offset** *offset-value* parameter cannot be specified. ● If *field-name* is not set to **MSRPC.Interface** and **operate** is not **pmatch**, the **offset** *offset-value* parameter cannot be specified. ● If *field-name* is not set to **MSRPC.Interface** but **operate** is **pmatch**, the **offset** *offset-value* parameter can be specified.
begin	Implements pattern match from the start location of the *field-name* field. The user-defined signature rule is matched only when a match of the *value-content* value is found.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
depth *depth-value*	Specifies the depth of pattern matching.	The value is an integer ranging from 7 to 65535. The value of *depth-value* must be greater than the number of characters in *value-content*. If *offset-value* is 1 and *depth-value* is 10, the matching starts from the second byte of the *field-name* field and 10 bytes will be matched. The matching succeeds as long as the *value-content* is within the specified range. ● If *field-name* is set to **MSRPC.Interface**, the **depth** *depth-value* parameter cannot be specified. ● If *field-name* is not set to **MSRPC.Interface** and **operate** is not **pmatch**, the **depth** *depth-value* parameter cannot be specified. ● If *field-name* is not set to **MSRPC.Interface** but **operate** is **pmatch**, the **depth** *depth-value* parameter can be specified.
direction *direction*	Specifies the packet check direction.	The direction can be: ● **both** Packets from the client and server are checked. ● **from-client** Packets from the client are checked. ● **from-server** Packets from the server are checked. **both** is the default configuration, and packets from the client and server are checked.
qualifier	Indicates the qualifier information.	-
http-method *http-method*	Checks the **Method** field of HTTP.	Supported HTTP methods include **GET**, **POST**, **PUT**, **HEAD**, **DELETE**, **OPTIONS**, **CONNECT**, **TRACE**, **LINK**, **UNLINK**, **PATCH**, **MOVE**, **COPY**, **WRAPPED**, **PROFIND**, and **PROPPATCH**. As for user-defined signature rule check items, you can configure only one HTTP Method check item and only one method.
all	Indicates all conditions.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

If *condition-id* is not specified, the system automatically sets the IDs to the missing numbers in ascending order. For example, conditions **1**, **3**, and **4** already exist in the system, and another condition is created but the *condition-id* is not specified. In this case, the system automatically sets the ID of the new condition to **2**.

Example

Create user-defined signature rule **hello** in user-defined signature **1**. Configure condition **1** to check field **HTTP.Authorization** whose value matches **threat_string**, and condition **2** to check field **HTTP.Content-Length** whose value is equal to **111**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol HTTP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] condition 1 field HTTP.Authorization operate pmatch value
threat_string
[Huawei-ips-signature-1-rule-hello] condition 2 field HTTP.Content-Length operate equal value 111
```

Create user-defined signature rule **hello** in user-defined signature **2**. Configure condition **1** to check the **HTTP.Authorization** field that matches **threat_string** and set the offset to **1** and depth to **10**.

```
<Huawei> system-view
[Huawei] ips signature-id 2
[Huawei-ips-signature-2] protocol HTTP
[Huawei-ips-signature-2] rule name hello
[Huawei-ips-signature-2-rule-hello] condition 1 field HTTP.Authorization operate pmatch value
threat_string offset 1 depth 10
```

19.9.2.11 condition associated (user-defined signature rule view)

Function

The **condition associated** command sets a check item for a user-defined associated signature.

The **undo condition associated** command cancels the settings of the check item for a user-defined associated signature.

Format

condition associated signature-id *signature-id* [**threshold** *threshold-value* | **interval** *interval-value* | **correlateby** { **source** | **destination** | **source-destination** }] *

undo condition associated

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies an associated signature ID. The value can be the ID of a user-defined or predefined signature, but cannot be the ID of a user-defined or predefined associated signature. The associated signature and user-defined associated signature must use the same protocol and object information.	The value is an integer ranging from 1 to 16777215.
threshold *threshold-value*	Specifies the threshold for signature association times.	The value is an integer ranging from 1 to 500. The default value is 30.
interval *interval-value*	Specifies the measurement period. If the number of times the associated signature is detected exceeds *threshold-value* within this period, the user-defined associated signature is matched.	The value is an integer ranging from 1 to 7200. The default value is 60.
correlateby	Indicates the association mode.	The default mode is **source-destination**.
source	Counts the times the associated signature is matched based on source IP addresses.	-
destination	Counts the times the associated signature is matched based on destination IP addresses.	-
source-destination	Counts the times the associated signature is matched based on a pair of source and destination IP addresses.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

Only one rule can be configured for a user-defined associated signature. Only one check item can be configured in the rule.

 Copyright © Huawei Technologies Co., Ltd.

If a user-defined signature is configured as an associated signature, you must remove the association relationship of the signature before deleting the user-defined signature. Only enabled predefined signatures can be configured as associated signatures.

During the IPS signature database update, if the associated signature configured for correlation detection does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Configure a check item for a user-defined associated signature.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] rule name rule1
[Huawei-ips-signature-1-rule-rule1] condition associated signature-id 1000 threshold 20 interval 23
correlateby source-destination
```

19.9.2.12 condition move (user-defined signature rule view)

Function

The **condition move** command moves a condition of the specified user-defined signature rule.

Format

condition move *condition-id* **to** *new-condition-id*

Parameters

Parameter	Description	Value
condition-id	Specifies the ID of the condition to be moved in the specified user-defined signature rule.	The value is an integer ranging from 1 to 4.
new-condition-id	Specifies the destination position (new ID of the condition) of the moved condition in the user-defined signature rule.	The value is an integer ranging from 1 to 4.

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

After you run the **check** command to configure the matching order of conditions in a user-defined signature rule to **sequential**, you can move the condition to change its priority.

If the destination *new-condition-id* is used by a condition, the moved condition and the owner of the destination ID switch IDs. For example, conditions **1** to **4** exist in a user-defined signature rule. When you run the **condition move 4 to 1** command to move condition **4** to the position of condition **1**, condition **4** becomes condition **1**, and the original condition **1** becomes condition **4**.

Example

View the existing conditions in user-defined signature rule **hello**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol HTTP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] display this
#
  condition 1 field HTTP.HeadContent operate pmatch value abcdabcd
  #
  condition 2 field HTTP.Content-Type operate pmatch value efghefgh
  #
  condition 3 field HTTP.Transfer-Encoding operate pmatch value ijklijkl
#
return
```

Move condition **2** in the user-defined signature rule to the position of condition **4**, and view the result of the move.

```
[Huawei-ips-signature-1-rule-hello] condition move 2 to 4
[Huawei-ips-signature-1-rule-hello] display this
#
  condition 1 field HTTP.HeadContent operate pmatch value abcdabcd
  #
  condition 3 field HTTP.Transfer-Encoding operate pmatch value ijklijkl
  #
  condition 4 field HTTP.Content-Type operate pmatch value efghefgh
#
return
```

Move condition **4** in the user-defined signature rule to the position of condition **1**, and view the result of the move.

```
[Huawei-ips-signature-1-rule-hello] condition move 4 to 1
[Huawei-ips-signature-1-rule-hello] display this
#
  condition 1 field HTTP.Content-Type operate pmatch value efghefgh
  #
  condition 3 field HTTP.Transfer-Encoding operate pmatch value ijklijkl
  #
  condition 4 field HTTP.HeadContent operate pmatch value abcdabcd
#
return
```

19.9.2.13 context-awareness enable

Function

The **context-awareness enable** command enables context awareness.

The **undo context-awareness enable** command disables context awareness.

Format

context-awareness { **all** | **http** | **os** } **enable**

undo context-awareness { **all** | **http** | **os** } **enable**

Parameters

Parameter	Description	Value
all	Indicates all awareness functions.	-
http	Indicates the HTTP application awareness function.	-
os	Indicates the operating system awareness function.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To enable the device to detect HTTP applications or operating systems on the network, enable context awareness.

By default, context awareness is disabled.

Example

Enable the operating system awareness function.

```
<Huawei> system-view
[Huawei] context-awareness os enable
```

19.9.2.14 description (intrusion prevention profile view)

Function

The **description** command configures the description of an intrusion prevention profile.

The **undo description** command deletes the description of an intrusion prevention profile.

 Copyright © Huawei Technologies Co., Ltd.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of an intrusion prevention profile.	The value is a case-sensitive string of 1 to 128 characters. Spaces are supported.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

You are advised to describe the features of each intrusion prevention profile.

Example

Configure description **HTTP protocol and windows system** for intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] description HTTP protocol and windows system
```

19.9.2.15 description (user-defined IPS signature view)

Function

The **description** command configures the description of a user-defined signature.

The **undo description** command deletes the description of a user-defined signature.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined signature.	The value is a case-sensitive string of 1 to 128 characters. Spaces are supported.

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

You are advised to describe the features of each user-defined signature.

Example

Configure a user-defined signature. Set the ID to **1**, name to **mysignature**, and description to **HTTP protocol and targeting client**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] description HTTP protocol and targeting client
```

19.9.2.16 destination-ip (user-defined signature rule view)

Function

The **destination-ip** command specifies the destination IP address to be checked by a user-defined signature rule.

The **undo destination-ip** command deletes the destination IP address to be checked by a user-defined signature rule.

Format

destination-ip { [**ipv4**] *start-ipv4-address* [*end-ipv4-address* | *ipv4-mask-length*] | **any** }

undo destination-ip

Parameters

Parameter	Description	Value
start-ipv4-address	Specifies the start IPv4 address.	The value is in dotted decimal notation.

Parameter	Description	Value
end-ipv4-address	Specifies the end IPv4 address.	The value is in dotted decimal notation.
ipv4-mask-length	Specifies the mask length of the IPv4 address.	The value is an integer ranging from 1 to 32.
any	Indicates any IP address.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All destination IP addresses are checked by the user-defined signature rule by default.

The user-defined signature rule can be used to check a single IP address or all address in an IP address range. To use a user-defined signature rule to check an IP address range, you can specify the start and end IP addresses or the mask-length to define the IP address range.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the destination IPv4 address to be checked to **10.2.2.1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] destination-ip 10.2.2.1
```

In user-defined signature with the ID of 1, specify user-defined signature rule **hello** and set the destination IP address range from **10.2.2.1** to **10.2.2.100** to be checked.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] destination-ip 10.2.2.1 10.2.2.100
```

19.9.2.17 destination-port (user-defined signature rule view)

Function

The **destination-port** command specifies the destination port to be checked by a user-defined signature rule.

 Copyright © Huawei Technologies Co., Ltd.

The **undo destination-port** command deletes the destination port to be checked by a user-defined signature rule.

Format

destination-port { *start-port end-port* | **any** }

undo destination-port

Parameters

Parameter	Description	Value
start-port	Specifies the start port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535.
end-port	Specifies the end port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535. The value of *end-port* must be no smaller than that of *start-port*.
any	Indicates that all destination ports are checked by the user-defined signature rule.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All destination ports are checked by the user-defined signature rule by default.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the destination port range to a range from **80** to **8080**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] destination-port 80 8080
```

19.9.2.18 display cnc domain-filter domain statistics

Function

The **display cnc domain-filter domain statistics** command displays the top N matched malicious domain names.

Format

display cnc domain-filter domain statistics [*topn-number*]

Parameters

Parameter	Description	Value
topn-number	Specifies how many most matched malicious domain names are displayed.	The value is an integer ranging from 1 to 50.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays the top N matched malicious domain names.

Example

Display the top 10 matched malicious domain names.

```
<Huawei> display cnc domain-filter domain statistics 10
 Domain statistics topN on slot 0 cpu 0:
 ---------------------------------------------------------------------------
 *                        TOP-N Statistics                        *
 *                        (Counts:   10)                         *
 ---------------------------------------------------------------------------
 TOP-N Domain Name                                        Event Counts
 ---------------------------------------------------------------------------
 1     www.example1.com                                        20
 2     www.example2.com                                        19
 3     www.example3.com                                        18
 4     www.example4.com                                        17
 5     www.example5.com                                        16
 6     www.example6.com                                        15
 7     www.example7.com                                        14
 8     www.example8.com                                        13
 9     www.example9.com                                        12
 10     www.example10.com                                       11
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-103 Description of the **display cnc domain-filter domain statistics** command output

Item	Description
TOP-N Statistics	Statistics on top N malicious domain names
Counts	Value of N
TOP-N Domain Name	Top N malicious domain names
Event Counts	Number of events

19.9.2.19 display cnc domain-filter exception

Function

The **display cnc domain-filter exception** command displays all exception domain names.

Format

display cnc domain-filter exception

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After using the **cnc domain-filter exception domain-name** command to add or delete exception domain names, you can run the command to view all configured exception domain names.

Example

Display all exception domain names.

```
<Huawei> display cnc domain-filter exception
 domain-filter exception-domain:
 Counts: 1
 ------------------------------------------------------------
 domain-name
 ------------------------------------------------------------
 www.example.com
```

Table 19-104 Description of the **display cnc domain-filter exception** command output

Item	Description
domain-filter exception-domain	Exception domain name in domain name-based filtering
Counts	Number of exception domain names
domain-name	Exception domain name

19.9.2.20 display cnc domain-filter statistics

Function

The **display cnc domain-filter statistics** command displays domain name filtering statistics.

Format

display cnc domain-filter { **exception** | **domain-name** *domain-name* } **statistics**

Parameters

Parameter	Description	Value
exception	Indicates the exception domain name.	-
domain-name	Specifies a malicious or exception domain name.	The value is a string of 4 to 255 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays filtering statistics of a domain name (**domain-name** *domain-name*) or a set of domain names (**exception**). To clear domain name-based filtering statistics, run **19.9.2.59 reset cnc domain-filter statistics**.

Example

Display filtering statistics on malicious domain name **www.example.com**.

```
<Huawei> display cnc domain-filter domain-name www.example.com statistics

--------------------------------------------------------------------------
Domain Name                                          Event Counts
--------------------------------------------------------------------------
www.example1.com                                                   1
```

Table 19-105 Description of the **display cnc domain-filter domain-name** *domain-name* **statistics** command output

Item	Description
Domain Name	Malicious domain name
Event Counts	Number of events

19.9.2.21 display context-awareness information statistics

Function

The **display context-awareness information statistics** command displays the identification results of the context awareness function.

Format

display context-awareness information [**host** *ip-address*] [**http-client** | **http-server** | **os**] **statistics**

Parameters

Parameter	Description	Value
host *ip-address*	Displays identification results by an IPv4 address.	The value is in dotted decimal notation.
http-client	Displays identification results by the HTTP client application.	-
http-server	Displays identification results by the HTTP server application.	-
os	Displays the identification results by the OS.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

The context awareness function records the identification results of only IPv4 traffic.

Example

Display the identification results of content awareness.

```
<Huawei> display context-awareness information statistics
-----------------------------------------------------------------------------------------
context-awareness information on slot 11 cpu 0:
-----------------------------------------------------------------------------------------
Address         Dir     OS                          HTTP-Application
10.1.1.1        client  Linux 2.2.x-3.x               Chrome
10.2.1.1        server  Linux 2.2.x-3.x               Apache 1.x
10.3.1.1        server  Other
10.4.1.1        client  Linux 2.2.x-3.x               Safari 5.1 or newer
-----------------------------------------------------------------------------------------
```

Table 19-106 Description of the **display context-awareness information statistics** command output

Item	Description
context-awareness information on slot *X* cpu *Y*	Statistics on CPU *Y* in slot *X*
Address	IPv4 address of the client or server
Dir	Detection direction: ● client: traffic from the client ● server: traffic from the server
OS	OS of the client or server
HTTP-Application	HTTP application used by the client or server

19.9.2.22 display context-awareness statistics

Function

The **display context-awareness statistics** command displays traffic statistics of different categories by context awareness.

Format

display context-awareness [**http-client** | **http-server** | **os**] **statistics**

Parameters

Parameter	Description	Value
http-client	Indicates an HTTP client application.	-
http-server	Indicates an HTTP server application.	-
os	Indicates the OS.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display traffic statistics by OS by context awareness.

```
<Huawei> system-view
[Huawei] display context-awareness os statistics
-------------------------------------------------------------------------------
OS statistic on slot 11 cpu 0:
-------------------------------------------------------------------------------
OS                                  Count
Android                               68205
Linux 3.x                            114939
Linux 2.6.x                           337404
Linux 2.4.x-2.6.x                       125654
Linux 2.2.x-3.x                        1993419
Windows_XP                               6524058
Windows_7,Windows_8                          960383
Windows_7                                 0
Mac_OS_X 10.x                            31457
iPhone,iPad                           174576
Mac_OS_X                               936
Other                                1647545
-------------------------------------------------------------------------------
```

Table 19-107 Description of the **display context-awareness os statistics** command output

Item	Description
OS statistic on slot *X* cpu *Y*	Statistics on CPU *Y* in slot *X*
OS	OS
Count	Matching count

19.9.2.23 display decoding statistics

Function

The **display decoding statistics** command displays decoding statistics.

NOTE

Only the AR160 (except AR169RW-P-M9) support this command.

Format

display decoding statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays decoding statistics.

Example

Display decoding statistics.

```
<Huawei> display decoding statistics
Decoding Statistic Table
-------------------------------------------------------------------------------
 Traffic statistic:
-------------------------------------------------------------------------------
   Total Traffic  :                              0
  -----------------------------------------------------------------------------
   Application                     Traffic
  -----------------------------------------------------------------------------
   HTTP                             0
   FTP                             0
   SMTP                              0
   POP3                              0
   NFS                             0
   SMB                              0
   IMAP                             0
   OTHER                              0
-------------------------------------------------------------------------------

 File statistic:
-------------------------------------------------------------------------------
   Total File  :                                 0
  -----------------------------------------------------------------------------
   Application                     File
  -----------------------------------------------------------------------------
```

```
  HTTP                          0
  FTP                          0
  SMTP                          0
  POP3                          0
  NFS                          0
  SMB                          0
  IMAP                          0
  OTHER                          0
-----------------------------------------------------------------------------
```

19.9.2.24 display ips signature-id rule

Function

The **display ips signature-id rule** command displays the user-defined signature rule with the specified name.

Format

display ips signature-id *signature-id* **rule** { **name** *rule-name* | **all** }

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of a user-defined signature.	The value is a string of 1 to 1024 characters. The value must be the ID of an existing user-defined signature.
name *rule-name*	Specifies the name of a user-defined signature rule.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-). The value must be the name of an existing user-defined signature rule.
all	Indicates IDs of all user-defined signatures.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display rules of user-defined signature **11**.

```
<Huawei> system-view
[Huawei] display ips signature-id 11 rule name rule1
 IPS Signature Rule Configurations:
 SignatureID      : 11
 -------------------------------------------------------
   Name            : rule1
   Scope           : flow
   Check           : sequential
   SourceIP        : 10.1.1.1/24
   SourcePort      : 2003-2004
   DestinationIP   :
   DestinationPort : any

   Condition:
     ID   Operator   Field                          Value
   -------------------------------------------------------
      1   noequal    HTTP.Content-Length              24
   -------------------------------------------------------
 ----------------------------------------------------------------------
```

Display the user-defined associated signature whose user-defined signature ID is 1.

Table 19-108 Description of the **display ips signature-id rule name** command output

Item	Description
SignatureID	ID of the user-defined signature where the rule reside
Name	Name of a user-defined signature rule
Scope	Detection scope of a user-defined signature rule
Check	Matching order of a user-defined signature rule
SourceIP	Source IP address checked by a user-defined signature rule
SourcePort	Source port checked by a user-defined signature rule
DestinationIP	Destination IP address checked by a user-defined signature rule
DestinationPort	Destination port checked by a user-defined signature rule
Condition	Condition of a user-defined signature rule

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ID	Condition ID
Operator	Field operation of a condition
Field	Field to be checked by a condition
Value	Value of the field to be checked by a condition
Signature-id	ID of the associated signature
ThresholdValue	Threshold for signature association times
IntervalTime	Measurement period
Correlateby	Association mode

19.9.2.25 display ips signature-state

Function

The **display ips signature-state** command displays the state of predefined signatures.

Format

display ips signature-state

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Enable all predefined signatures, disable predefined signature 12345, and then commit the changes. After that, disable predefined signature 54330 without committing the change. Then, view the state of all predefined signatures.

```
<Huawei> system-view
[Huawei] ips signature-state enabled
```

```
[Huawei] ips signature-state signature-id 12345 disabled
[Huawei] engine configuration commit
[Huawei] ips signature-state signature-id 54330 disabled
[Huawei] display ips signature-state
 -----------------------------------------------------------------
 Global    : enabled
 Count     : 2
 Committed : not committed
 -----------------------------------------------------------------
 Signature-ID    Configured-State    Default-State    Committed
 -----------------------------------------------------------------
 54330           disabled            enabled          not committed
 12345           disabled            enabled          committed
```

Table 19-109 Description of the **display ips signature-state** command output

Item	Description
Global	Default state for all predefined signatures can be either of the following: ● **enabled**: Predefined signatures are enabled by default. ● **disabled**: Predefined signatures are disabled by default. ● **non-configured**: The default state of predefined signatures is not configured. To set the default state for all predefined signatures, run **ips signature-state** { **enabled** | **disabled** }. If the default state is not specified, the state will be **non-configured**.
Count	Number of predefined signatures with changed state
Committed	Whether all state changes are committed: ● **committed**: All state changes are committed. ● **not committed**: Not all state changes are committed.
Signature-ID	ID of a predefined signature.
Configured-State	New state of a predefined signature: ● **enabled**: A predefined signature is enabled. ● **disabled**: A predefined signature is disabled. To change the state of a predefined signature, run **ips signature-state signature-id** *signature-id* { **enabled** | **disabled** }.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default-State	State of predefined signatures in the IPS signature database: ● **enabled**: A predefined signature is enabled. ● **disabled**: A predefined signature is disabled. ● **retired**: A predefined signature is deprecated. A predefined signature marked with retired is deprecated and retained only for checking the history of signatures.
Committed	Whether the state change of a predefined signature is committed: ● **committed**: The state change is committed. ● **not committed**: The state change is not committed.

19.9.2.26 display ips statistics

Function

The **display ips statistics** command displays IPS statistics.

Format

display ips statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display IPS statistics.

```
<Huawei> display ips statistics
IPS Statistic Table
-----------------------------------------------------------------------------
```

```
 Event statistic:
-------------------------------------------------------------------------------
   Total Alert Events  :                    0
   Total Block Events  :                    0
  -----------------------------------------------------------------------------
   Application             Alert Events              Block Events
  -----------------------------------------------------------------------------
   HTTP                          0                         0
   FTP                          0                         0
   SMTP                          0                         0
   POP3                          0                         0
   NFS                          0                         0
   SMB                          0                         0
   IMAP                          0                         0
   OTHER                          0                         0
-------------------------------------------------------------------------------

 Traffic statistic:
-------------------------------------------------------------------------------
   Total Traffic  :                         0
  -----------------------------------------------------------------------------
   Application                  Traffic
  -----------------------------------------------------------------------------
   HTTP                          0
   FTP                          0
   SMTP                          0
   POP3                          0
   NFS                          0
   SMB                          0
   IMAP                          0
   OTHER                          0
-------------------------------------------------------------------------------

 File statistic:
-------------------------------------------------------------------------------
   Total File  :                            0
  -----------------------------------------------------------------------------
   Application                  File
  -----------------------------------------------------------------------------
   HTTP                          0
   FTP                          0
   SMTP                          0
   POP3                          0
   NFS                          0
   SMB                          0
   IMAP                          0
   OTHER                          0
-------------------------------------------------------------------------------
```

19.9.2.27 display ips-signature

Function

The **display ips-signature** command displays information about an IPS signature.

Format

display ips-signature *ips-signature-id*

display ips-signature [{ **pre-defined** | **user-defined** } [**associated**]] [**application** { *application-name* | **all** } | **category** { *category-name* | **all** } | **os** { **all** | **android** | **ios** | **unix-like** | **windows** | **other** } * | **protocol** { *protocol-name* | **all** } | **severity** { **information** | **low** | **medium** | **high** } * | **state** { **disabled** | **enabled** | **retired** } | **target** { **server** | **client** | **both** }] *

Parameters

Parameter	Description	Value
ips-signature-id	Specifies the ID of an IPS signature.	The value is an integer ranging from 1 to 16777215. The value must be the ID of an existing IPS signature.
pre-defined	Displays information about a predefined signature.	-
user-defined	Displays information about a user-defined signature.	-
associated	Displays information about a associated signature.	-
application { *application-name* | **all** }	Specifies an application name.	• *application-name*: displays information about signatures in application *application-name*. • **all**: displays information about signatures in all applications.
category { *category-name* | **all** }	Displays signatures by category.	• *category-name*: displays information about signatures in category *category-name*. • **all**: displays information about signatures in all categories.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
os { **all** | **android** | **ios** | **unix-like** | **windows** | **other** } *	Displays signatures by operating system.	• **all**: displays information about all signatures. • **android**: displays information about signatures for the Android operating system. • **ios**: displays information about signatures for the iOS operating system. • **unix**: displays information about signatures for the UNIX operating system. • **windows**: displays information about signatures for the Windows operating system. • **other**: displays information about signatures for other operating systems.
protocol { *protocol-name* | **all** }	Displays signatures by protocol.	• *protocol-name*: displays information about signatures of protocol *protocol-name*. • **all**: displays information about signatures of all protocols.
severity { **information** | **low** | **medium** | **high** }*	Displays signatures by severity.	• **information**: displays information about signatures with informational severity. • **low**: displays information about signatures with low severity. • **medium**: displays information about signatures with medium severity. • **high**: displays information about signatures with high severity.
state { **disabled** | **enabled** | **retired** }	Indicates the state of a predefined signature.	• **disabled**: The predefined signature is disabled. • **enabled**: The predefined signature is enabled. • **retired**: The predefined signature is deprecated.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
target { **server** | **client** | **both** }	Displays signatures by target.	• **server**: displays information about signatures for detecting intrusions into a server. • **client**: displays information about signatures for detecting intrusions into a client. • **both**: displays information about signatures for detecting intrusions into both a client and a server.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ips-signature pre-defined associated** command displays information about predefined associated signatures and user-defined associated signature.

NOTE

If the IPS signature file is not loaded, predefined signatures are not displayed, the protocol cannot be specified, and the category must be set to **all**. You can upgrade services to load the IPS signature file.

Example

Display all predefined signatures.

```
<Huawei> display ips-signature pre-defined
 ---------------------------------------------------------------------------
 *                    Pre-defined Signature                          *
 *                       (Counts: 5538)                            *
 ---------------------------------------------------------------------------
 Sig-ID   Protocol   Target  Severity OS        Category        Event Counts
 ---------------------------------------------------------------------------
 1030     HTTP       server  high     windows   Overflow                 0
 1040     HTTP       client  high     windows   Overflow                 0
 1050     TCP        server  high     all       Dos                      0
 1060     HTTP       server  high     windows   Overflow                 0
 1080     TCP        server  high     windows   Overflow                 0
 1090     UDP        server  high     all       Code-execution           0
 1100     MSRPC      server  high     windows   Overflow                 0
 1102     MSRPC      server  high     windows   Overflow                 0
 1110     TCP        both    high     all       Code-execution           0
 1120     TCP        server  high     all       Overflow                 0
 1140     IMAP4      server  high     unix-like Code-execution           0
 1150     MSRPC      server  high     windows   Overflow                 0
 1160     MSRPC      server  medium   windows   Dos                      0
 1170     MSRPC      server  medium   windows   Dos                      0
 1189     TCP        server  medium   windows   Dos                      0
 1200     SUNRPC     server  high     unix-like Overflow                 0
 1220     HTTP       client  high     windows   Overflow                 0
```

```
1230     SUNRPC     server  high     all      Overflow                0
 ---- More ----
```

Display all user-defined signatures.

```
<Huawei> display ips-signature user-defined
 ---------------------------------------------------------------------------
*                    User-defined Signature                          *
*                         (Counts:   1)                          *
 ---------------------------------------------------------------------------
Sig-ID   Protocol   Target  Severity OS       Category        Event Counts
 ---------------------------------------------------------------------------
1        TCP        both    high     N/A      User-defined              0
```

Table 19-110 Description of the **display ips-signature pre-defined** and **display ips-signature user-defined** command output

Item	Description
Counts	Number of signatures
Sig-ID	Signature ID
Protocol	Protocol of packets matching the signature
Target	Detection target of the signature
Severity	Severity of intrusions matching the signature
OS	Operating system attacked by intrusions matching the signature
Category	Signature category
Event Counts	Match count of a signature **NOTE** The Router does not clear the match count of a modified or a deleted user-defined signature. When you create a user-defined signature with an ID the same as that of a deleted signature, the match count increases on the basis of the match count of the deleted signature. For example, the match count of user-defined signature 12 is 10, and the signature is deleted using the **undo ips signature-id** 12 command. If you use the **ips signature-id** 12 command to create a user-defined signature with the same name 12. The match count of the new user-defined signature 12 is 10. To clear the match count of a user-defined or predefined signature, run the **19.9.2.64 reset ips-signature statistics** command.

Display the signature with ID **16042**.

```
<Huawei> display ips-signature 16042
 ---------------------------------------------------------------------------
  SignatureID                    : 16042
  Name                           : VideoLAN VLC ActiveX Control Crafted Parameter Memory
Corruption
  Protocol                       : TCP
  Target                         : client
  Severity                       : medium
  OS                             : all
```

```
  Category                        : Overflow
  Action                          : alert
  EventCounts                     : 0
  AttackEvidenceCollectionCounts      : 0(slot 0 cpu 0)
  Reference                       : CVE:CVE-2007-6262
  State                           : enabled
  Description                     : CVE-2007-6262 : A certain ActiveX control in axvlc.dll in VideoLAN VLC 0.8.6
before 0.8.6d
allows remote attackers to execute arbitrary code via crafted arguments to the (1) addTarget, (2)
getVariable, or (3) setVariable fu
nction, resulting from a "bad initialized pointer," aka a "recursive plugin release
vulnerability."
 ------------------------------------------------------------------------------
```

Table 19-111 Description of the **display ips-signature** *ips-signature-id* command output

Item	Description
SignatureID	Signature ID
Name	Signature name
Protocol	Protocol of packets matching the signature
Target	Detection target of the signature
Severity	Severity of intrusions matching the signature
OS	Operating system attacked by the intrusions matching the signature
Category	Signature category
Action	Signature action
Threshold	Threshold for signature association times
Interval	Measurement period
Correlateby	Association mode
EventCounts	Match count of a signature **NOTE** To clear the match count of a signature, run the **19.9.2.64 reset ips-signature statistics** command.
AttackEvidenceCollectionCounts	Number of attack evidence collection sessions

Item	Description
Reference	Reference information of a signature ● CVE: indicates the Common Vulnerabilities and Exposures (CVE) ID of a signature. You can query the CVE ID on the **http://cve.mitre.org/** website and obtain detailed information based on the CVE ID. ● BID: indicates the Bugtraq ID (BID) of a signature. You can query the BID on the **http://www.securityfocus.com/bid** website and obtain detailed information based on the BID. ● CNNVD: indicates the China National Vulnerability Database of Information Security (CNNVD) ID of a signature. You can query the CNNVD ID on the **http://www.cnnvd.org.cn/** website and obtain detailed information based on the CNNVD ID.
State	Signature state
Application	Application to which a signature applies
Description	Description of a signature

19.9.2.28 display ips-signature cve-id

Function

The **display ips-signature cve-id** command displays IPS signatures of a specified CVE ID.

Format

display ips-signature cve-id { *cve-id* | **year** *year* }

Parameters

Parameter	Description	Value
cve-id	Specifies a CVE ID.	The value is a string of 13 to 16 characters.
year *year*	Specifies the release year of the CVE.	The value is an integer ranging from 1999 to 2099.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After *cve-id* is specified, this command displays predefined IPS signatures of the specified CVE ID. After *year* is specified, this command displays predefined IPS signatures of the specified release year of CVEs.

Example

Display IPS predefined signatures of the CVE with the ID being CVE-2014-0498.

```
<Huawei> display ips-signature cve-id CVE-2014-0498
 ------------------------------------------------------------------------------
 *                      Pre-defined Signature                                 *
 *                         (Counts:    1)                                 *
 ------------------------------------------------------------------------------
 Sig-ID   Protocol     Severity    OS          CVE-ID             VENDOR-ID
 ------------------------------------------------------------------------------
 281920   FILE          high       all         CVE-2014-0498       N/A
```

Display IPS predefined signatures of the CVEs released in 2014.

```
<Huawei> display ips-signature cve-id year 2014
 ------------------------------------------------------------------------------
 *                      Pre-defined Signature                                 *
 *                         (Counts:   11)                                 *
 ------------------------------------------------------------------------------
 Sig-ID   Protocol     Severity    OS          CVE-ID             VENDOR-ID
 ------------------------------------------------------------------------------
 173880   SSL          high       all         CVE-2014-0160       N/A
 269361   SSL          medium     all         CVE-2014-3566       N/A
 167250   FILE         high       windows     CVE-2014-0301
MS14-013
 174331   HTTP         high       windows     CVE-2014-0315
MS14-019
 257330   HTTP         medium     windows     CVE-2014-2880
N/A
 281920   FILE         high       all         CVE-2014-0498       N/A
 284550   HTTP         medium     all         CVE-2014-6039
N/A
 287990   TCP          high       unix-like   CVE-2014-0659       N/A
 291190   FILE         high       all         CVE-2014-0518       N/A
 291910   HTTP         high       windows     CVE-2014-6344
N/A
 269360   SSL          medium     all         CVE-2014-3566       N/A
```

Table 19-112 Description of the **display ips-signature cve-id** command output

Item	Description
Counts	Number of predefined signatures
Sig-ID	ID of a predefined signature
Protocol	Protocol of a predefined signature

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Severity	Severity of a predefined signature, which can be: ● high ● medium ● low ● info
OS	Applicable OS of a predefined signature
CVE-ID	CVE ID
VENDOR-ID	Vendor ID

19.9.2.29 display ips-signature statistics

Function

The **display ips-signature statistics** command displays the top-N IPS signatures that are most frequently matched by protocols.

Format

display ips-signature statistics *top-number*

Parameters

Parameter	Description	Value
top-number	Displays the top-N signatures that are most frequently matched.	The value is an integer ranging from 1 to 100.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run this command to view top-N IPS signatures that are most frequently matched by protocols, including the protocol, severity, category, and matching count of each signature.

Example

Display the top 6 signatures that are most frequently matched.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display ips-signature statistics 6
 IPS statistic topN on slot 0 cpu 0:
 -----------------------------------------------------------------------------
 *                    TOP-N Searched Signature                          *
 *                          (Counts:   6)                          *
 -----------------------------------------------------------------------------
 TOP-N    Sig-ID   Protocol   Severity       Category              Event Counts
 -----------------------------------------------------------------------------
 1        3        TCP        high           User-defined          25
 2        2        TCP        high           User-defined          7
 3        4        TCP        high           User-defined          3
 4        5        TCP        high           User-defined          3
 5        6        TCP        high           User-defined          3
 6        7        TCP        high           User-defined          3
```

Table 19-113 Description of the **display ips-signature statistics** command output

Item	Description
Counts	Number of signatures
TOP-N	Ranking of signatures in descending order of match count
Sig-ID	Signature ID
Protocol	Protocol of packets matching the signature
Severity	Severity of intrusions matching the signature
Category	Signature category
Event Counts	Match count of a signature **NOTE** To clear the match count of a signature, run the **19.9.2.64 reset ips-signature statistics** command.

19.9.2.30 display ips-signature vendor-id

Function

The **display ips-signature vendor-id** command displays IPS signatures of a specified vendor ID.

Format

display ips-signature vendor-id *vendor-id*

Parameters

Parameter	Description	Value
vendor-id	Specifies a vendor ID.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ips-signature vendor-id** command displays IPS signatures of a specified vendor ID.

Example

Display all IPS signatures of the vendor ID MS14-013.

```
<Huawei> display ips-signature vendor-id MS14-013
 ---------------------------------------------------------------------------
 *                        Pre-defined Signature                            *
 *                           (Counts:    1)                              *
 ---------------------------------------------------------------------------
 Sig-ID   Protocol     Severity    OS          CVE-ID             VENDOR-ID
 ---------------------------------------------------------------------------
 167250   FILE          high       windows      CVE-2014-0301       MS14-013
```

Table 19-114 Description of the **display ips-signature vendor-id** command output

Item	Description
Counts	Number of predefined signatures
Sig-ID	ID of a predefined signature
Protocol	Protocol of a predefined signature (protocol used by a network threat)
Severity	Severity of a predefined signature, which can be: ● high ● medium ● low ● info
OS	OS targeted by a network threat
CVE-ID	CVE ID
VENDOR-ID	Vendor ID

19.9.2.31 display profile type ips

Function

The **display profile type ips** command displays the configuration of an intrusion prevention profile.

Format

display profile type ips [**name** *name* [**signature-set-name** *signature-set-name* | **exception-signature-id** *exception-signature-id*]]

Parameters

Parameter	Description	Value
name *name*	Displays the information about the specified intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks ("), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks (''), or hyphens (-). The value must be an existing intrusion prevention profile.
signature-set-name *signature-set-name*	Specifies the name of a signature filter.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks ("), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks (''), or hyphens (-). The value must be the name of an existing signature filter.
exception-signature-id *exception-signature-id*	Specifies the ID of an exception signature.	The value is an integer ranging from 1 to 16777215. The value must be the ID of an existing exception signature.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The device has multiple default security profiles for different application scenarios as follows. The default security profiles can be displayed, cloned, or referenced in security policies, but cannot be modified or deleted.

Table 19-115 Default intrusion prevention profiles

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
strict	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	All	Block	The intrusion prevention profile applies to the scenarios in which the device is required to block all matched packets.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
web_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS, HTTP, FTP	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a web server.
file_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS, SMB, NETBIOS, NFS, SUNRPC, MSRPC, FILE, TELNET	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a file server.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
dns_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DNS server.
mail_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	DNS, IMAP4, SMTP, POP3	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a mail server.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
inside_firewall	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	Except **TELNET** and **TFTP**	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall.
dmz	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	Except **NETBIOS**, **NFS**, **SMB**, **TELNET** and **TFTP**	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a .

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
outside_firewall	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	Except **Scanner**	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a firewall.
ids	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	All	Alert	The intrusion prevention profile applies to the scenarios in which the device is deployed off-line as an IDS.

 Copyright © Huawei Technologies Co., Ltd.

Name	Target	Severity	Operating System	Application Program	Protocol	Category	Action	Application Scenario
default	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in-line as an IPS.

Example

Display the information about profile template **default**.

```
<Huawei> display profile type ips name default
 IPS Profile Configurations:
 --------------------------------------------------------------------------
 Name                          : default
 Description                   : This profile applies to the general scenario when the device is deployed in IPS
(inline) mode.
 Referenced                    : 1
 State                         : committed
 AttackEvidenceCollection      : disable
 AssocCheck:                   : enable

 SignatureSet                  : default
   Target                      : both
   Severity                    : low medium high
   OS                          : unix-like windows android ios other
   Protocol                    : all
   Category                    : all
   Action                      : default
   Application                 : all

 Exception:
 ID      Action                                  Name
 --------------------------------------------------------------------------

 DNS Protocol Check:

 HTTP Protocol Check:
 --------------------------------------------------------------------------
```

Display the information about intrusion prevention profile **profile_ips_1**.

Display information about signature filter **sig_set1** in intrusion prevention profile **profile_ips_1**.

```
<Huawei> display profile type ips name profile_ips_1 signature-set-name sig_set1
 IPS Profile Signature Set Configurations:
 ----------------------------------------------------------------


 SignatureSet    : sig_set1
   Target        : both
   Severity      : low medium high information
   OS            : unix-like windows android ios other
   Protocol      : all
   Category      : all
   Action        : alert
   Application   : all
 ----------------------------------------------------------------
```

Display information about exception signature **12380** in intrusion prevention profile **profile_ips_1**.

```
<Huawei> display profile type ips name profile_ips_1 exception-signature-id 12380
 IPS Profile Exception Configurations:
 ---------------------------------------------------------------------------
 ID       Action                                  Name
 ---------------------------------------------------------------------------
 12380    allow                                     HP Intelligent Management Center TFTP Server MODE Remote
Code Execution
 ---------------------------------------------------------------------------
```

19.9.2.32 dns domain check

Function

The **dns domain check** command enables the DNS domain name check function.

The **undo dns domain check** command disables the DNS domain name check function.

Format

dns domain check action { **alert** | **block** }

undo dns domain check

Parameters

Parameter	Description	Value
alert	Permits the packet and generates a log if the DNS domain name contains unexpected characters.	-
block	Blocks the packet and generates a log if the DNS domain name contains unexpected characters.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The DNS domain name check function is disabled by default.

After the DNS domain name check function is enabled, the Router permits or blocks traffic and generates a log if any domain name contains unexpected characters.

Example

In the intrusion prevention profile **profile1**, enable the DNS domain name check function and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns domain check action block
```

19.9.2.33 dns domain length check

Function

The **dns domain length check** command enables the DNS domain name length check function.

The **undo dns domain length check** command disables the DNS domain name length check function.

Format

dns domain length check [**max-length** *max-length*] **action** { **alert** | **block** }

undo dns domain length check

Parameters

Parameter	Description	Value
max-length *max-length*	Specifies the maximum DNS domain name length to be checked.	The value is an integer ranging from 1 to 255. The default value is 64.
alert	Permits the packet and generates a log if the DNS domain name is longer than the maximum length.	-
block	Blocks the packet and generates a log if the DNS domain name is longer than the maximum length.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The DNS domain name length check function is disabled by default.

After the DNS domain name length check function is enabled, the Router permits or blocks traffic and generates a log if the length of any domain name exceeds the specified maximum length. If no maximum length is specified, the default value 64 is used.

Example

In the intrusion prevention profile **profile1**, enable the DNS domain name length check function, specify the maximum length to 255, and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns domain length check max-length 255 action block
```

19.9.2.34 dns malformed-packet check

Function

The **dns malformed-packet check** command enables malformed DNS packet detection.

The **undo dns malformed-packet check** command disables malformed DNS packet detection.

Format

dns malformed-packet check action { **alert** | **block** }

undo dns malformed-packet check

Parameters

Parameter	Description	Value
alert	When the protocol format of a DNS packet is abnormal, the packet is permitted, and a log is recorded.	-
block	When the protocol format of a DNS packet is abnormal, the packet is blocked, and a log is recorded.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

Example

In IPS profile **profile1**, enable malformed DNS packet detection and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns malformed-packet check action block
```

19.9.2.35 dns request-type check

Function

The **dns request-type check** command enables DNS request packet type detection.

The **undo dns request-type check** command disables DNS request packet type detection.

Format

dns request-type check { *start-type* [**to** *end-type*] **action** | **default-action** } { **alert** | **allow** | **block** }

undo dns request-type check { **all** | *start-type* [**to** *end-type*] }

Parameters

Parameter	Description	Value
start-type end-type	Indicates the query type of a DNS packet.	The value is an integer ranging from 0 to 65535. The value of *end-type* must be no smaller than that of *start-type*.
action	Indicates the action.	-
default-action	Indicates the default action.	-
allow	The packet is permitted.	-

Parameter	Description	Value
alert	The packet is permitted, and a log is recorded.	-
block	The packet is blocked, and a log is recorded.	-
all	Indicates all query types.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

To detect all query types, set a default action (**default-action**).

You can also detect a specified query type. When the DNS packet query type is as specified, the corresponding processing action is implemented. The default processing action applies to other query types.

By default, this function is disabled.

Example

In IPS profile **profile1**, enable DNS packet query type detection and set the default action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns request-type check default-action block
```

19.9.2.36 dns session request-times check

Function

The **dns session request-times check** command enables the function of checking the number of DNS session request times.

The **undo dns session request-times check** command disables the function of checking the number of DNS session request times.

Format

dns session request-times check [**max-times** *max-time*] **action** { **alert** | **block** }

undo dns session request-times check

Parameters

Parameter	Description	Value
max-times *max-time*	Specifies the maximum number of DNS session request times.	The value is an integer ranging from 1 to 65535. The default value is 20.
alert	Permits the packet and generates a log if the number of DNS session request times is greater than the specified maximum value.	-
block	Blocks the packet and generates a log if the number of DNS session request times is greater than the specified maximum value.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The function of checking the number of DNS session request times is disabled by default.

After this function is enabled, the Router permits or blocks traffic if the number of DNS session request times is greater than the specified maximum value. If no maximum number of request times is specified, the default value 20 is used.

Example

In the intrusion prevention profile **profile1**, enable the function of checking the number of DNS session request times, specify the maximum number of request times to 50, and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] dns session request-times check max-times 50 action block
```

19.9.2.37 exception ips-signature-id

Function

The **exception ips-signature-id** command adds an IPS signature as an exception.

The **undo exception** command deletes an IPS signature from signature exception.

Format

exception ips-signature-id *ips-signature-id* [**action** { **alert** | **allow** | **block** }]

undo exception { **ips-signature-id** *ips-signature-id* | **all** }

Parameters

Parameter	Description	Value
ips-signature-id	Specifies the ID of an IPS signature.	The value is an integer ranging from 1 to 16777215.
action	Specifies the action.	-
alert	Indicates that the device generates an alarm when a packet matches an exception IPS signature.	-
allow	Indicates that the device permits a packet when a packet matches an exception IPS signature.	The default action for the exception signature is **allow**.
block	Indicates that the device denies a packet when a packet matches an exception IPS signature.	-
all	Indicates all signatures.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

This command configures different actions for certain signatures. The security policy preferentially implements the action for the exception signature.

During the IPS signature database update, if the configured exception signature does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

 Copyright © Huawei Technologies Co., Ltd.

Example

In intrusion prevention profile **profile1**, add the IPS signature with ID 2012 to the exception signature, set the action to **alert**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] exception ips-signature-id 2012 action alert
```

19.9.2.38 http multi-host check

Function

The **http multi-host check** command enables detection of HTTP packets with multiple **Host** fields.

The **undo http multi-host check** command disables detection of HTTP packets with multiple **Host** fields.

Format

http multi-host check action { **alert** | **block** }

undo http multi-host check

Parameters

Parameter	Description	Value
action	Specifies the action.	-
alert	When an HTTP packet contains multiple **Host** fields, the packet is permitted, and a log is recorded.	-
block	When an HTTP packet contains multiple **Host** fields, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

Example

In IPS profile **profile1**, enable detection of HTTP packets with multiple **Host** fields and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http multi-host check action block
```

19.9.2.39 http ssh-over-http check

Function

The **http ssh-over-http check** command enables detection of HTTP traffic involving SSH traffic.

The **undo http ssh-over-http check** command disables detection of HTTP traffic involving SSH traffic.

Format

http ssh-over-http check action { **alert** | **block** }

undo http ssh-over-http check

Parameters

Parameter	Description	Value
action	Specifies the action.	-
alert	When an HTTP traffic contains the SSH traffic, the packet is permitted, and a log is recorded.	-
block	When an HTTP traffic contains the SSH traffic, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

Example

In IPS profile **profile1**, enable detection of HTTP traffic involving SSH traffic and set the action to **block**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http ssh-over-http check action block
```

19.9.2.40 http x-forwarded-for check

Function

The **http x-forwarded-for check** command enables detection of the **X-Forwarded-For** field in HTTP packets.

The **undo http x-forwarded-for check** command disables detection of the **X-Forwarded-For** field in HTTP packets.

Format

http x-forwarded-for check { **any** | **whitelist** } **action** { **alert** | **block** }

undo http x-forwarded-for check

Parameters

Parameter	Description	Value
any	When an HTTP packet contains the **X-Forwarded-For** field, an anomaly is detected.	-
whitelist	Detects whether all proxy IP addresses in the **X-Forwarded-For** field match the whitelist. If no, an anomaly is detected.	-
action	Specifies the action.	-
alert	When the **X-Forwarded-For** field in an HTTP packet is abnormal, the packet is permitted, and a log is recorded.	-
block	When the **X-Forwarded-For** field in an HTTP packet is abnormal, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

If you have configured the detection of whether all proxy IP addresses in the **X-Forwarded-For** field match a whitelist (**whitelist**), you need also to run the **http x-forwarded-for whitelist** command to configure such a whitelist.

By default, this function is disabled.

Example

In IPS profile **profile1**, enable detection of the **X-Forwarded-For** field in HTTP packets and set the action to **block** if the packets contain such a field.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-forwarded-for check any action block
```

19.9.2.41 http x-forwarded-for whitelist

Function

The **http x-forwarded-for whitelist** command configures a whitelist used to detect the **X-Forwarded-For** field.

The **undo http x-forwarded-for whitelist** command deletes an existing whitelist.

Format

http x-forwarded-for whitelist ipv4 *ip-address*

undo http x-forwarded-for whitelist { **all** | **ipv4** *ip-address* }

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Indicates an IP address.	The IP address is in dotted decimal format.
all	Deletes all whitelists.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

To use the **http x-forwarded-for check** command to enable the detection of whether all proxy IP addresses in the **X-Forwarded-For** field match a whitelist, you need also to use the **http x-forwarded-for whitelist** command to configure such a whitelist. If not all proxy IP addresses in the **X-Forwarded-For** field match the whitelist, an anomaly is detected.

You can configure a maximum of 32 IP addresses in a whitelist.

Example

In IPS profile **profile1**, configure a whitelist used to detect the **X-Forwarded-For** field and set the IP address to **10.1.1.1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-forwarded-for check whitelist action block
[Huawei-profile-ips-profile1] http x-forwarded-for whitelist ipv4 10.1.1.1
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.42 ips associated pre-defined

Function

The **ips associated pre-defined** command sets a check item for a predefined associated signature.

The **undo ips associated pre-defined** command cancels the settings of the check item for a predefined associated signature.

Format

ips associated pre-defined signature-id *signature-id* { **threshold** *threshold-value* | **interval** *interval-value* | **correlateby** { **source** | **destination** | **source-destination** } } *

undo ips associated pre-defined { **signature-id** *signature-id* | **all** }

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of a predefined associated signature.	The value is an integer ranging from 1025 to 16777215.
threshold *threshold-value*	Specifies the threshold for signature association times.	The value is an integer ranging from 1 to 2000. The default value is 30.
interval *interval-value*	Specifies the measurement period. If the number of times the associated signature is detected exceeds *threshold-value* within this period, the predefined associated signature is matched.	The value is an integer ranging from 1 to 7200. The default value is 60.
correlateby	Indicates the association mode.	The default mode is **source-destination**.
source	Collects statistics on the number of times that the associated signature is matched for the same source IP address.	-
destination	Collects statistics on the number of times that the associated signature is matched for the same destination IP address.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
source-destination	Collects statistics on the number of times that the associated signature is matched for the same source and destination IP addresses.	-
all	Restores the check items of all predefined associated signatures to the default values.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the check items of a predefined associated signature cannot meet requirements, you can run the **ips associated pre-defined** command to modify the check items.

During the IPS signature database update, if the configured predefined associated signature does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Configure check items for a predefined associated signature.

```
<Huawei> system-view
[Huawei] ips associated pre-defined signature-id 16042 threshold 20 interval 30 correlateby source-destination
```

19.9.2.43 ips collect-attack-evidence max-session-number

Function

The **ips collect-attack-evidence max-session-number** command sets the maximum number of attack evidence collection sessions for each IPS signature on each CPU.

The **undo ips collect-attack-evidence max-session-number** command restores the default maximum number of attack evidence collection sessions for each IPS signature on each CPU.

Format

ips collect-attack-evidence max-session-number *session-number* [**signature-id** *signature-id*]

undo ips collect-attack-evidence max-session-number [**signature-id** *signature-id*]

Parameters

Parameter	Description	Value
session-number	Specifies the maximum number of attack evidence collection sessions.	The value is an integer ranging from 0 to 50. The default value is 5.
signature-id *signature-id*	Specifies the ID of an IPS signature.	The value is an integer ranging from 1025 to 16777215.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After the **collect-attack-evidence enable** command is executed, the device starts to collect the attack evidence that match the intrusion prevention profile. You can set the maximum number of sessions in which the device collects attack evidence that match the intrusion prevention profile for each IPS signature on each CPU to collect necessary information for packet tracing, with the impact on system performance controlled to the minimum extent. When the device provides multiple CPUs, the maximum number of attack evidence collection sessions for each IPS signature is the value of *session-number* multiplying the number of CPUs.

The device collects all packets in a matched session. This command specifies the maximum number of matched sessions, not the number of matched packets.

During the IPS signature database update, if the predefined signature for which the maximum number of attack evidence collection sessions is set does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Set the maximum number of attack evidence collection sessions for the signature **54330** to 10.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ips collect-attack-evidence max-session-number 10 signature-id 54330
```

19.9.2.44 http x-online-host blacklist

Function

The **http x-online-host blacklist** command configures a blacklist used to detect the **X-Online-Host** field.

The **undo http x-online-host blacklist** command deletes an existing blacklist.

Format

http x-online-host blacklist *blacklist*

undo http x-online-host blacklist { **all** | *blacklist* }

Parameters

Parameter	Description	Value
blacklist	Specifies a domain name or IP address.	The value is a string of 4 to 127 characters.
all	Deletes all blacklists.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

To use the **http x-online-host check** command to enable the detection of whether the domain name or IP address in the **X-Online-Host** field matches a blacklist, you need also to use the **http x-online-host blacklist** command to configure such a blacklist. If a domain name or IP address in the **X-Online-Host** field matches the blacklist, an anomaly is detected.

You can configure a maximum of 32 domain names or IP addresses in a blacklist.

Example

In IPS profile **profile1**, configure a blacklist used to detect the **X-Online-Host** field and set the domain name to **www.example.com**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-online-host check blacklist action block
[Huawei-profile-ips-profile1] http x-online-host blacklist www.example.com
```

19.9.2.45 http x-online-host check

Function

The **http x-online-host check** command enables detection of the **X-Online-Host** field in HTTP packets.

The **undo http x-online-host check** command disables detection of the **X-Online-Host** field in HTTP packets.

Format

http x-online-host check { **any** | **blacklist** | **multiple** } **action** { **alert** | **block** }

undo http x-online-host check

Parameters

Parameter	Description	Value
any	When an HTTP packet contains the **X-Online-Host** field, an anomaly is detected.	-
blacklist	Detects whether the domain name or IP address in an **X-Online-Host** field matches the blacklist. If yes, an anomaly is detected.	-
multiple	When an HTTP packet contains two or more **X-Online-Host** fields, an anomaly is detected.	-
action	Specifies the action.	-
alert	When the **X-Online-Host** field in an HTTP packet is abnormal, the packet is permitted, and a log is recorded.	-
block	When the **X-Online-Host** field in an HTTP packet is abnormal, the packet is blocked, and a log is recorded.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

If you have configured the detection of whether the domain name or IP address in the **X-Online-Host** field matches a blacklist (**blacklist**), you need also to run the **http x-online-host blacklist** command to configure such a blacklist.

By default, this function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Example

In IPS profile **profile1**, enable detection of the **X-Online-Host** field in HTTP packets and set the action to **block** if the packets contain such a field.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] http x-online-host check any action block
```

19.9.2.46 ips log based-on-session

Function

The **ips log based-on-session** command configures IPS threat logs to record source and destination IP addresses by session.

The **undo ips log based-on-session** command configures IPS threat logs to record source and destination IP addresses by packet.

Format

ips log based-on-session

undo ips log based-on-session

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, IPS threat logs record source and destination IP addresses by packets. The source and destination IP addresses in IPS threat logs are the source and destination IP addresses of packets.

After you run the **ips log based-on-session** command to configure IPS threat logs to record source and destination IP addresses by session, the source and destination IP addresses in IPS threat logs are the source and destination IP addresses of the sessions with threat packets.

Example

Configure IPS threat logs to record source and destination IP addresses by session.

```
<Huawei> system-view
[Huawei] ips log based-on-session
```

19.9.2.47 ips log merge enable

Function

The **ips log merge enable** command enables the IPS log aggregation function.

The **undo ips log merge enable** command disables the IPS log aggregation function.

Format

ips log merge enable

undo ips log merge enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the system enables the IPS log aggregation function.

After the log aggregation function is enabled, the IPS aggregates multiple identical IPS logs into one log.

Example

Disable the IPS log aggregation function.

```
<Huawei> system-view
[Huawei] undo ips log merge enable
```

19.9.2.48 ips signature-id

Function

The **ips signature-id** command creates a user-defined signature with the specified ID.

The **undo ips signature-id** command deletes all user-defined signatures or the user-defined signature with the specified ID.

Format

ips signature-id *signature-id*

undo ips signature-id { *signature-id* | **all** }

Parameters

Parameter	Description	Value
signature-id	Specifies the ID of a user-defined signature.	The value is an integer ranging from 1 to 1024.
all	Deletes all IPS signatures.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A view is created when you create a user-defined signature. All fields in the signature use the default values.

Example

Create user-defined signature **1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1]
```

19.9.2.49 ips signature-state

Function

The **ips signature-state** command configures the state of predefined signatures.

The **undo ips signature-state** command restores the state of all predefined signatures to their state in the IPS signature database.

Format

ips signature-state [**signature-id** *signature-id*] { **enabled** | **disabled** }

undo ips signature-state

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of a predefined signature.	The value is an integer ranging from 1025 to 16777215.
enabled	Enables the specified predefined signature.	-
disabled	Disables the specified predefined signature.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can increase threat detection ratio by enabling certain signatures or increase threat detection performance and decrease resource consumption by disabling certain signatures.

After the state of a predefined signature is changed, run **engine configuration commit** to commit the change to apply it.

The **ips signature-state** [**signature-id** *signature-id*] { **enabled** | **disabled** } command is used to enable or disable the specified signature.

If no signature ID is specified, the **ips signature-state** { **enabled** | **disabled** } command is used to enable or disable all predefined signatures.

After the state of a predefined signature is changed and committed, run **display ips signature-state** to check whether the state change takes effect.

During the IPS signature database update, if the predefined signature that has a configured state does not exist in the IPS signature database, the corresponding configurations are reserved but do not take effect. When the current configurations are queried, the following message is displayed: **Invalid configuration. The specified signature (*signature-id*) does not exist in the current library. Please check and delete it.**

Example

Enable all predefined signatures, disable predefined signature 12345, and then commit the changes. After that, disable predefined signature 54330 without committing the change. Then, view the state of all predefined signatures.

```
<Huawei> system-view
[Huawei] ips signature-state enabled
```

```
[Huawei] ips signature-state signature-id 12345 disabled
[Huawei] engine configuration commit
[Huawei] ips signature-state signature-id 54330 disabled
[Huawei] display ips signature-state
 -----------------------------------------------------------------
 Global    : enabled
 Count     : 2
 Committed : not committed
 -----------------------------------------------------------------
 Signature-ID    Configured-State    Default-State    Committed
 -----------------------------------------------------------------
 54330           disabled            enabled          not committed
 12345           disabled            enabled          committed
```

Table 19-116 Description of the **display ips signature-state** command output

Item	Description
Global	Default state for all predefined signatures can be either of the following: ● **enabled**: Predefined signatures are enabled by default. ● **disabled**: Predefined signatures are disabled by default. ● **non-configured**: The default state of predefined signatures is not configured. To set the default state for all predefined signatures, run **ips signature-state** { **enabled** | **disabled** }. If the default state is not specified, the state will be **non-configured**.
Count	Number of predefined signatures with changed state
Committed	Whether all state changes are committed: ● **committed**: All state changes are committed. ● **not committed**: Not all state changes are committed.
Signature-ID	ID of a predefined signature.
Configured-State	New state of a predefined signature: ● **enabled**: A predefined signature is enabled. ● **disabled**: A predefined signature is disabled. To change the state of a predefined signature, run **ips signature-state signature-id** *signature-id* { **enabled** | **disabled** }.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default-State	State of predefined signatures in the IPS signature database: ● **enabled**: A predefined signature is enabled. ● **disabled**: A predefined signature is disabled. ● **retired**: A predefined signature is deprecated. A predefined signature marked with retired is deprecated and retained only for checking the history of signatures.
Committed	Whether the state change of a predefined signature is committed: ● **committed**: The state change is committed. ● **not committed**: The state change is not committed.

19.9.2.50 name (user-defined IPS signature view)

Function

The **name** command sets the name of a user-defined signature.

The **undo name** command deletes the name of a user-defined signature.

Format

name *name*

undo name

Parameters

Parameter	Description	Value
name	Specifies the name of a user-defined signature.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 96 characters. If the name contains spaces, the length is 3 to 98 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks (''), or hyphens (-).

Views

User-defined IPS signature view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

None

Example

Configure user-defined signature **1** and name it **mysignature**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
```

19.9.2.51 os (IPS signature filter view)

Function

The **os** command adds the IPS signature of the specified operating system to an IPS signature filter.

The **undo os** command deletes the specified operating system from the condition.

Format

os { **android** | **ios** | **unix-like** | **windows** | **other** } *

undo os [**android** | **ios** | **unix-like** | **windows** | **other**]

Parameters

Parameter	Description	Value
android	Indicates the Android operating system.	-
ios	Indicates the iOS operating system.	-
unix-like	Indicates the UNIX operating system, including Linux, HP_unix, AIX, and Sun operating systems.	-
windows	Indicates the Windows operating system.	-
other	Indicates other operating system.	-

Views

IPS signature filter view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

No default operating system is specified in the IPS signature filter.

You can configure this command if the detected attack targets at an operating system.

other indicates the operating systems other than **android**, **ios**, **unix-like**, and **windows**. Therefore, running the **os** command with parameters **android**, **ios**, **unix-like**, **windows**, and **other** being specified is the same as the default setting.

A user-defined signature applies to all operating systems by default. The applicable operating systems cannot be manually configured.

Example

Configure operating system **unix** in IPS signature filter **hello** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] os unix-like
```

19.9.2.52 profile type ips copy

Function

The **profile type ips copy** command clones an existing intrusion prevention profile and displays the view of the new profile.

Format

profile type ips copy *old-name* [*new-name*]

Parameters

Parameter	Description	Value
old-name	Specifies the name of an intrusion prevention profile to be cloned.	The value must be the name of an existing intrusion prevention profile.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
new-name	Specifies the name of the new intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks (''), or hyphens (-).

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you need to create an intrusion prevention profile that is similar to an existing one, clone the existing one or use an intrusion prevention profile template.

If *new-name* is not specified, the default name of the new intrusion prevention profile is *old-name*_n. **n** indicates the number of times the profile has been cloned. It is an integer starting from 1.

Example

Create two intrusion prevention profiles by using profile template **default**.

```
<Huawei> system-view
[Huawei] profile type ips copy default
[Huawei-profile-ips-default_1] quit
[Huawei] profile type ips copy default p_ips_1
[Huawei-profile-ips-p_ips_1]
```

19.9.2.53 profile type ips name

Function

The **profile type ips name** command creates an intrusion prevention profile and displays the profile view.

The **undo profile type ips** command deletes all or the specified intrusion prevention profiles.

Format

profile type ips name *name*

undo profile type ips { **all** | **name** *name* }

Parameters

Parameter	Description	Value
name	Specifies the name of an intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).
all	Deletes all intrusion prevention profiles.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

As a security mechanism, intrusion prevention detects intrusions by analyzing network traffic and responds to intrusions accordingly to terminate the intrusion behaviors.

After you create an intrusion prevention profile, run the **19.9.2.70 signature-set name** command in the intrusion prevention profile view to configure a signature filter and run the **19.9.2.37 exception ips-signature-id** command to configure exception signatures.

Example

Create intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1]
```

19.9.2.54 protocol (IPS signature filter view)

Function

The **protocol** command adds the IPS signature of the specified protocol to an IPS signature filter.

The **undo protocol** command deletes the specified protocol from the filtering condition.

 Copyright © Huawei Technologies Co., Ltd.

Format

protocol { *protocol-name* &<1-10> | **all** }

undo protocol { *protocol-name* &<1-10> | **all** }

Parameters

Parameter	Description	Value
protocol-name &<1-10>	Specifies the protocol name. **&<1-10>** indicates that a command can have 1 to 10 such parameter values.	-
all	Indicates all protocols.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

No default protocol is specified in the IPS signature filter.

You can add signatures of a maximum of 10 protocols to the signature filter at a time. To add signatures of more than 10 protocols, repeat this command.

Example

Configure protocols **HTTP** and **SMTP** in IPS signature filter **hello** as the filtering conditions in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] protocol HTTP SMTP
```

19.9.2.55 protocol (user-defined IPS signature view)

Function

The **protocol** command configures the protocol in a user-defined signature.

The **undo protocol** command deletes the protocol from a user-defined signature.

Format

protocol *protocol-name*

undo protocol

Parameters

Parameter	Description	Value
protocol-name	Specifies the name of a protocol in the user-defined signature.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

A user-defined signature contains only one protocol.

The protocol of a predefined signature describes the type of the protocol used by an attack packet.

Example

Configure a user-defined signature. Set the ID to **1**, name to **mysignature**, and protocol to **UDP**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] protocol UDP
```

19.9.2.56 rename (IPS signature filter view)

Function

The **rename** command renames an existing IPS signature filter and displays the new signature filter view.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the new name of an existing IPS signature filter.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks (''), or hyphens (-).

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Change the name of signature filter **hello** to **hello_1** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] rename hello_1
[Huawei-profile-ips-profile1-sigset-hello_1]
```

19.9.2.57 rename (user-defined signature rule view)

Function

The **rename** command renames an existing user-defined signature rule and displays the new rule view.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the new name of an existing user-defined signature rule.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks (''), or hyphens (-).

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

None

Example

In the user-defined signature rule view, change the name of rule **hello** to **hello_1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] rename hello_1
[Huawei-ips-signature-1-rule-hello_1]
```

19.9.2.58 rename (intrusion prevention profile view)

Function

The **rename** command renames an intrusion prevention profile and displays the new profile view.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the new name of the intrusion prevention profile.	The value is a case-sensitive string. If the name does not contain any spaces, the length is 1 to 32 characters. If the name contains spaces, the length is 3 to 34 characters and the name must be enclosed with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Change the name of intrusion prevention profile **profile1** to **profile_ips_1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] rename profile_ips_1
[Huawei-profile-ips-profile_ips_1]
```

19.9.2.59 reset cnc domain-filter statistics

Function

The **reset cnc domain-filter statistics** command clears domain name-based filtering statistics.

Format

reset cnc domain-filter { **domain** | **exception** | **domain-name** *domain-name* } **statistics**

Parameters

Parameter	Description	Value
domain	Indicates the malicious domain name.	-
exception	Indicates the exception domain name.	-
domain-name *domain-name*	Specifies a malicious or exception domain name.	The value is a string of 4 to 255 characters.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

This command is used to clear filtering statistics of a domain name (**domain-name** *domain-name*) or a set of domain names (**domain** or **exception**). Run the **19.9.2.20 display cnc domain-filter statistics** command to display the domain name-based filtering statistics to check whether previous statistics are cleared.

Example

Clear filtering statistics on malicious domain names.

```
<Huawei> reset cnc domain-filter domain statistics
```

Clear filtering statistics on malicious domain name **www.example.com**.

```
<Huawei> reset cnc domain-filter domain-name www.example.com statistics
```

19.9.2.60 reset context-awareness information statistics

Function

The **reset context-awareness information statistics** command clears the identification results of the context awareness function.

Format

reset context-awareness information statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After checking the identification results of context awareness by using the **display context-awareness information statistics** command, you can clear the identification results by using the **reset context-awareness information statistics** command. The identification results cannot be restored after being cleared. Therefore, exercise caution when using the command.

Example

Clear the identification results of content awareness.

```
<Huawei> reset context-awareness information statistics
```

19.9.2.61 reset context-awareness statistics

Function

The **reset context-awareness statistics** command resets traffic statistics of different categories by context awareness.

Format

reset context-awareness statistics

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After checking traffic statistics of different categories by context awareness by using the **display context-awareness statistics** command, you can clear the statistics by using the **reset context-awareness statistics** command. The traffic statistics cannot be restored after being cleared. Therefore, exercise caution when using the command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Clear traffic statistics of different categories by context awareness.

```
<Huawei> reset context-awareness statistics
```

19.9.2.62 reset decoding statistics

Function

The **reset decoding statistics** command clears decoding statistics.

NOTE

Only the AR160 (except AR169RW-P-M9) supports this command.

Format

reset decoding statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

none

Example

Clear decoding statistics.

```
<Huawei> reset decoding statistics
```

19.9.2.63 reset ips statistic

Function

The **reset ips statistic** command clears IPS statistics.

Format

reset ips statistic

Parameters

None

Views

User view

Level

3: Management level

Usage Guidelines

IPS statistics cannot be restored after being cleared. Confirm your operation before clearing them.

Example

Clear IPS statistics.

```
<Huawei> reset ips statistic
```

19.9.2.64 reset ips-signature statistics

Function

The **reset ips-signature statistics** command clears IPS signature statistics.

Format

reset ips-signature statistics { **signature-id** *signature-id* | **all** } { **event** | **collect-attack-evidence** | **all** }

Parameters

Parameter	Description	Value
signature-id *signature-id*	Specifies the ID of an IPS signature.	The value is an integer ranging from 1 to 16777215. The value must be the ID of an existing IPS signature.
all	Indicates all IPS signatures.	-
event	Indicates the match count of an IPS signature.	-

Parameter	Description	Value
collect-attack-evidence	Indicates the number of attack evidence collection sessions.	-
all	Indicate all statistics.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

IPS signature statistics cannot be restored after being cleared. Exercise caution when running the reset command.

For those IPS signatures with the maximum number of matched attack evidence collection sessions, you can clear the attack evidence collection session statistics to restart the statistics collection.

Example

Clear all statistics of all signatures.

```
<Huawei> reset ips-signature statistics all all
```

Clear the match count of IPS signature No. **54330**.

```
<Huawei> reset ips-signature statistics signature-id 54330 event
```

Clear the statistics on the matched attack evidence collection sessions of IPS signature No. **54330**.

```
<Huawei> reset ips-signature statistics signature-id 54330 collect-attack-evidence
```

19.9.2.65 rule name (user-defined IPS signature view)

Function

The **rule name** command creates a user-defined signature rule with the specified name.

The **undo rule** command deletes all user-defined signature rules or the specified user-defined signature rule.

Format

rule name *name*

undo rule { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name	Specifies the name of a user-defined signature rule.	The value is a case-sensitive string. If the name does not contain any spaces, the value contains 1 to 32 characters. If the name contains spaces, the value contains 3 to 34 characters, and you must enclose the name with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks (''), or hyphens (-).
all	Indicates all user-defined signature rules.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

You can configure a maximum of four rules for one user-defined signature.

You must configure the protocol before you create a user-defined signature rule.

Example

Create user-defined signature rule **hello** in user-defined signature **1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello]
```

19.9.2.66 scope (user-defined signature rule view)

Function

The **scope** command configures the matching scope of a user-defined signature rule.

The **undo scope** command restores the default configuration.

Format

scope { **flow** | **message** | **packet** }

undo scope

Parameters

Parameter	Description	Value
flow	Indicates that the user-defined signature rule matches flows.	-
message	Indicates that the user-defined signature rule matches messages.	-
packet	Indicates that the user-defined signature rule matches packets.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

By default, the matching scope of a user-defined signature rule is **packet**.

If you select **flow**, the device detects data flows. The configuration applies only to sessions of application-layer protocols over TCP.

If you select **message**, the device detects each message.

If you select **packet**, the device detects packets, such as TCP request or reply packets.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the matching scope to **packet**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] scope packet
```

19.9.2.67 severity (IPS signature filter view)

Function

The **severity** command adds the IPS signature of the specified severity to an IPS signature filter.

The **undo severity** command deletes the specified severity from the filtering condition.

Format

severity { **high** | **medium** | **low** | **information** } *

undo severity [**high** | **medium** | **low** | **information**]

Parameters

Parameter	Description	Value
high	Configure the IPS signature filter so that only signatures of "high" level are matched.	-
medium	Configure the IPS signature filter so that only signatures of "medium" level are matched.	-
low	Configure the IPS signature filter so that only signatures of "low" level are matched.	-
information	Configure the IPS signature filter so that only signatures of "information" level are matched.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

No default severity is specified in the IPS signature filter.

Example

Configure severities **low** and **high** in IPS signature filter **hello** as the filtering conditions in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] severity low high
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.68 severity (user-defined IPS signature view)

Function

The **severity** command configures the severity of a user-defined signature.

The **undo severity** command cancels the severity of a user-defined signature.

Format

severity { **high** | **medium** | **low** | **information** }

undo severity

Parameters

Parameter	Description	Value
high	Indicates the high severity.	-
medium	Indicates the medium severity.	-
low	Indicates the low severity.	-
information	Indicates the information severity.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

The default severity of a user-defined signature is **high**.

Threat severity describes the severity of consequences caused by attacks. Higher severity indicates severer consequences caused by attacks against the signature.

Example

Configure user-defined signature **1**, name it **mysignature** and set the severity to **high**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] name mysignature
[Huawei-ips-signature-1] severity high
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.2.69 signature-set move

Function

The **signature-set move** command configures the priority of an IPS signature filter.

Format

signature-set move *signature-set-name1* { **before** | **after** } *signature-set-name2*

Parameters

Parameter	Description	Value
signature-set-name1	Specifies the signature filter to be moved.	The value must be the name of an existing signature filter.
before	Moves the signature filter to before the specified signature filter.	-
after	Moves the signature filter to after the specified signature filter.	-
signature-set-name2	Specifies the target signature filter. The signature filter to be moved is moved to before or after the target signature filter.	The value must be the name of an existing signature filter.

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

The IPS signature filter displayed in the front has a higher priority than that in the back. You can run the **display this** command in the intrusion prevention profile view to display the priority of an IPS signature filter.

Example

Move signature filter **hello** to after signature filter **world** in intrusion prevention profile **profile1**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set move hello after world
```

19.9.2.70 signature-set name

Function

The **signature-set name** command creates an IPS signature filter and displays its view.

The **undo signature-set** command deletes an IPS signature filter.

Format

signature-set name *name*

undo signature-set { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name	Specifies the name of a signature filter.	The value is a case-sensitive string. If the name does not contain any spaces, the value contains 1 to 32 characters. If the name contains spaces, the value contains 3 to 34 characters, and you must enclose the name with double quotation marks (""), for example, "user for test". The name cannot contain any question marks (?), commas (,), quotation marks ("), or hyphens (-).
all	Deletes all IPS signature filters.	-

Views

Intrusion prevention profile view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create IPS signature filter **hello** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello]
```

19.9.2.71 source-ip (user-defined signature rule view)

Function

The **source-ip** command specifies the source IP address to be checked by a user-defined signature rule.

The **undo source-ip** command deletes the source IP address to be checked by a user-defined signature rule.

Format

source-ip { [**ipv4**] *start-ipv4-address* [*end-ipv4-address* | *ipv4-mask-length*] | **any** }

undo source-ip

Parameters

Parameter	Description	Value
start-ipv4-address	Specifies the start IPv4 address.	The value is in dotted decimal notation.
end-ipv4-address	Specifies the end IPv4 address.	The value is in dotted decimal notation.
ipv4-mask-length	Specifies the mask length of the IPv4 address.	The value is an integer ranging from 1 to 32.
any	Indicates any IP address.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All source IP addresses are checked by the user-defined signature rule by default.

The user-defined signature rule can be used to check a single IP address or all address in an IP address range. To use a user-defined signature rule to check an IP

address range, you can specify the start and end IP addresses or the mask-length to define the IP address range.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the source IP address to be checked to **10.1.1.1**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] source-ip ipv4 10.1.1.1
```

In user-defined signature with the ID of 1, specify user-defined signature rule **hello** and set the source IP address range from **10.2.2.1** to **10.2.2.100** to be checked.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] source-ip ipv4 10.1.1.1 10.1.1.100
```

19.9.2.72 source-port (user-defined signature rule view)

Function

The **source-port** command specifies the source port to be checked by a user-defined signature rule.

The **undo source-port** command deletes the source port to be checked by a user-defined signature rule.

Format

source-port { *start-port end-port* | **any** }

undo source-port

Parameters

Parameter	Description	Value
start-port	Specifies the start port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535.
end-port	Specifies the end port of a port range to be checked by the user-defined signature rule.	The value is an integer ranging from 1 to 65535. The value of *end-port* must be no smaller than that of *start-port*.

Parameter	Description	Value
any	Indicates that all source ports are checked by the user-defined signature rule.	-

Views

User-defined signature rule view

Default Level

2: Configuration level

Usage Guidelines

All source ports are checked by the user-defined signature rule by default.

Example

Create user-defined signature rule **hello** in user-defined signature **1** and set the source port range to a range from **80** to **8080**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] protocol TCP
[Huawei-ips-signature-1] rule name hello
[Huawei-ips-signature-1-rule-hello] source-port 80 8080
```

19.9.2.73 target (IPS signature filter view)

Function

The **target** command adds the IPS signature of the specified target to an IPS signature filter.

The **undo target** command deletes the specified target from the filtering condition.

Format

target { **both** | **client** | **server** }

undo target

Parameters

Parameter	Description	Value
both	Adds signatures that detect packets to both clients and servers to a signature filter.	-

Parameter	Description	Value
client	Adds signatures that detect packets to clients to a signature filter.	-
server	Adds signatures detecting packets to servers to a signature filter.	-

Views

IPS signature filter view

Default Level

2: Configuration level

Usage Guidelines

No default target is specified in the IPS signature filter.

Example

Configure target **server** in IPS signature filter **hello** in intrusion prevention profile **profile1**.

```
<Huawei> system-view
[Huawei] profile type ips name profile1
[Huawei-profile-ips-profile1] signature-set name hello
[Huawei-profile-ips-profile1-sigset-hello] target server
```

19.9.2.74 target (user-defined IPS signature view)

Function

The **target** command configures the target of a user-defined signature.

The **undo target** command deletes the target of a user-defined signature.

Format

target { **both** | **client** | **server** }

undo target

Parameters

Parameter	Description	Value
both	Detects attack packets to both clients and servers.	-
client	Detects attack packets to clients.	-

Parameter	Description	Value
server	Detects attack packets to servers.	-

Views

User-defined IPS signature view

Default Level

2: Configuration level

Usage Guidelines

A user-defined signature detects attack packets to both clients and servers by default.

For example, For TCP/UDP packets, the initiator is the client, whereas the destination of the TCP/UDP packets is the server.

Example

Configure user-defined signature **1** and set the detection target to **server**.

```
<Huawei> system-view
[Huawei] ips signature-id 1
[Huawei-ips-signature-1] target server
```

19.9.3 URL Filtering Configuration Commands

NOTE

- The following product models support URL filtering function:
  - AR100&AR120&AR150&AR160&AR200&AR3200 series: All models.
  - AR1200 series: AR1220C, AR1220-8GE, AR1220E, AR1220EV, and AR1220EVW.
  - AR2200 series: all models except AR2201-48FE, AR2202-48FE, and AR2204.

19.9.3.1 add { blacklist | whitelist } (URL filtering profile view)

Function

The **add { blacklist | whitelist }** command adds blacklist and whitelist rules to the URL filtering profile.

The **undo add { blacklist | whitelist }** command removes blacklist and whitelist rules from the URL filtering profile.

Format

add { **blacklist** | **whitelist** } { **url** *url-text* | **host** *host-text* }

undo add { **blacklist** | **whitelist** } { **url** { *url-text* | **all** } | **host** { *host-text* | **all** } | **all** }

Parameters

Parameter	Description	Value
blacklist	Indicates a blacklist rule.	-
whitelist	Indicates a whitelist rule.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
url *url-text*	Specifies a URL rule.	• The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. Pre-processing removes **http://** from the entered character string. • If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is **www.example.com/abc/def?"gh**, you need to enter **www.example.com/abc/def?%22gh**. • * indicates wildcard, which appears at the beginning, middle, or end of an URL and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When the URL is configured as ***abc**, all URLs ending with **abc** are matched. – When the URL is configured as ***a*bcd***, all URLs containing **a** and **bcd** in sequence are matched. – When the URL is configured as **bcd***, all URLs starting with **bcd** are matched. • If a URL does not contain any wildcard, the URL must contain at least four consecutive characters, such as **abcd**. If the URL contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered URL ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered URL is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **.**.

Parameter	Description	Value
url all	Indicates all URL rules.	-
host *host-text*	Specifies a domain name rule.	● The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space. ● * indicates wildcard, which appears at the beginning, middle, or end of a domain name and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When a domain name is configured as ***abc**, all domain names ending with **abc** are matched. – When a domain name is configured as ***a*bcd***, all domain names containing **a** and **bcd** in sequence are matched. – When a domain name is configured as **bcd***, all domain names starting with **bcd** are matched. ● If a domain name does not contain any wildcard, the domain name must contain at least four consecutive characters, such as **abcd**. If the domain name contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. ● If the entered domain name ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. ● If the total length of the entered domain name is 4, only one ***** exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *****, and the length of the remaining common characters is 3. However, its last character is **.**.
host all	Indicates all domain name rules.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all URL and domain name rules.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

- Blacklist

  Enterprises can define a blacklist to block the access to specified websites, improve work efficiency, and optimize network resource usage.

  If a requested URL matches the blacklist, the Router blocks the access to the requested website.

- Whitelist

  Enterprises can define a whitelist to allow uncontrolled access to URLs on the whitelist.

  If a requested URL matches the whitelist, the Router grants access to the requested website.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Create a URL filtering profile **profile_development**, and add **www.example.com** to the blacklist.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] add blacklist url www.example.com
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.2 add { url | host } (predefined URL category view)

Function

The **add** { **url** | **host** } command adds a URL or domain name rule to a predefined category.

The **undo add** { **url** | **host** } command removes a URL or domain name rule from a predefined category.

Format

add { **url** *url-text* &<1-2> | **host** *host-text* &<1-2> }

undo add { **url** { *url-text* &<1-2> | **all** } | **host** { *host-text* &<1-2> | **all** } }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url-text &<1-2>	Specifies a URL rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the URL contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete URL for matching. For example, if you configure **add url www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. Pre-processing removes **http://** from the entered character string. • When you enter two strings, the URL obtained by combining the two strings contains a maximum of 480 characters. • If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is **www.example.com/abc/def?"gh**, you need to enter **www.example.com/abc/def?%22gh**. • * indicates wildcard, which appears at the beginning, middle, or end of an URL and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When the URL is configured as ***abc**, all URLs ending with **abc** are matched. – When the URL is configured as ***a*bcd***, all URLs containing **a** and **bcd** in sequence are matched.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		– When the URL is configured as **bcd***, all URLs starting with **bcd** are matched. ● If a URL does not contain any wildcard, the URL must contain at least four consecutive characters, such as **abcd**. If the URL contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. ● If the entered URL ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. ● If the total length of the entered URL is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **.**.
url all	Indicates all URL rules.	-

Parameter	Description	Value
host-text &<1-2>	Specifies a domain name rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the domain name contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete domain name for matching. For example, if you configure **add host www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space. • When you enter two strings, the domain name obtained by combining the two strings contains a maximum of 480 characters. • * indicates wildcard, which appears at the beginning, middle, or end of a domain name and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When a domain name is configured as ***abc**, all domain names ending with **abc** are matched. – When a domain name is configured as ***a*bcd***, all domain names containing **a** and **bcd** in sequence are matched. – When a domain name is configured as **bcd***, all domain names starting with **bcd** are matched. • If a domain name does not contain any wildcard, the domain name must contain at least four consecutive characters, such as **abcd**. If the domain name contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered domain name ends with **.***, there must be at least three common

Parameter	Description	Value
		characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. • If the total length of the entered domain name is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **..** Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **..**
host all	Indicates all domain name rules.	-

Views

Predefined URL category view

Default Level

2: Configuration level

Usage Guidelines

Before you add a URL rule to a predefined URL category, run the **display url-filter category pre-defined** command to view the *subcategory-id* of the predefined URL category. Then run the **url-filter category pre-defined subcategory-id** *subcategory-id* command to access the predefined URL category view and add the desired URL rule.

Run the **display url-filter category pre-defined subcategory-id** *subcategory-id* command to view existing user-defined URL and domain name rules in the predefined URL category view.

Example

Add a URL rule **www.example.com/news** to the predefined category **General Fashion**, and set the matching mode to **Exact**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 200
[Huawei-cate-pre-defined-200] add url www.example.com/news
```

Add a domain name rule **www.example.com** to the predefined category **General Fashion**, and set the matching mode to **Exact**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 200
[Huawei-cate-pre-defined-200] add host www.example.com
```

Add a URL rule **fashion** to the predefined category **General Fashion**, and set the matching mode to **Keyword**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 200
[Huawei-cate-pre-defined-200] add url *fashion*
```

19.9.3.3 add { url | host } (user-defined URL category view)

Function

The **add** { **url** | **host** } command adds a URL or domain name rule to a user-defined category.

The **undo add** { **url** | **host** } command removes a URL or domain name rule from a user-defined category.

Format

add { **url** *url-text* &<1-2> | **host** *host-text* &<1-2> }

undo add { **url** { *url-text* &<1-2> | **all** } | **host** { *host-text* &<1-2> | **all** } }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url-text &<1-2>	Specifies a URL rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the URL contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete URL for matching. For example, if you configure **add url www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. Pre-processing removes **http://** from the entered character string. • When you enter two strings, the URL obtained by combining the two strings contains a maximum of 480 characters. • If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is **www.example.com/abc/def?"gh**, you need to enter **www.example.com/abc/def?%22gh**. • * indicates wildcard, which appears at the beginning, middle, or end of an URL and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When the URL is configured as ***abc**, all URLs ending with **abc** are matched. – When the URL is configured as ***a*bcd***, all URLs containing **a** and **bcd** in sequence are matched.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		– When the URL is configured as **bcd***, all URLs starting with **bcd** are matched. ● If a URL does not contain any wildcard, the URL must contain at least four consecutive characters, such as **abcd**. If the URL contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. ● If the entered URL ends with **.***, there must be at least three common characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. ● If the total length of the entered URL is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **.**.
url all	Indicates all URL rules.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host-text &<1-2>	Specifies a domain name rule. **&<1-2>** indicates that each command can configure a maximum of two strings at a time. When the domain name contains over 255 characters, you need to enter two strings. The system automatically places the second string behind the first one to form a complete domain name for matching. For example, if you configure **add host www.example.com 123**, the system stores it as **www.example.com123** after processing.	• The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space. • When you enter two strings, the domain name obtained by combining the two strings contains a maximum of 480 characters. • * indicates wildcard, which appears at the beginning, middle, or end of a domain name and indicates suffix matching, keyword matching, and prefix matching, respectively. For example: – When a domain name is configured as ***abc**, all domain names ending with **abc** are matched. – When a domain name is configured as ***a*bcd***, all domain names containing **a** and **bcd** in sequence are matched. – When a domain name is configured as **bcd***, all domain names starting with **bcd** are matched. • If a domain name does not contain any wildcard, the domain name must contain at least four consecutive characters, such as **abcd**. If the domain name contains wildcard, it must contain at least three consecutive characters except the wildcard, such as ***abc**, ***abc***, **abc****, and ***a*bcd**. • If the entered domain name ends with **.***, there must be at least three common

Parameter	Description	Value
		characters before **.***. Take ***.*.*** as an example. It ends with **.***. However, it does not contain three common characters before **.***. ● If the total length of the entered domain name is 4, only one * exists at the beginning, and the length of the remaining common characters is 3, the last character cannot be **.**. Take ***ab.** as an example. Its total length is 4 and begins with *, and the length of the remaining common characters is 3. However, its last character is **.**.
host all	Indicates all domain name rules.	-

Views

User-defined URL category view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Add a URL rule **www.example.com** in the view of user-defined URL category **abc** and set the matching mode to **Exact**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
[Huawei-cate-user-defined-abc] add url www.example.com
```

Add a URL rule **bbs** in the view of user-defined **abc** and set the matching mode to **Keyword**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
[Huawei-cate-user-defined-abc] add url *bbs*
```

Add domain name rule **www.example.com** in the view of user-defined category **abc** and set the matching mode to **Exact**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
[Huawei-cate-user-defined-abc] add host www.example.com
```

19.9.3.4 add referer-host

Function

The **add referer-host** command adds referer-host rules to a URL filtering profile.

The **undo add referer-host** command deletes referer-host rules from a URL filtering profile.

Format

add referer-host *host-text*

undo add referer-host { *host-text* | **all** }

Parameters

Parameter	Description	Value
host-text	Specify a host rule.	The value is a string of 4 to 255 characters, without **/**, ****, **#**, **"**, **?**, or spaces.
all	Indicates all host rules.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

If only the whitelist is configured during the access to a specific web page, other links on the specified web page may fail to be accessed. For example: If only the whitelist rule www.example.com is configured during the access to the www.example.com web page, other links that do not use www.example.com as the domain name are inaccessible. To solve the preceding problem, you can run this command to add the referer-host rule to the URL filtering profile. The referer field in an HTTP request will be matched with the referer-host rule. If a match is found, the URL request is allowed. If the referer field in the HTTP request does not match the configured referer-host rule, the user can determine whether to match the referer field with all whitelist rules.

- When the function of matching the referer field in a URL request with whitelist rules is enabled, the referer field will be matched with all whitelist rules. If a match is found, the URL request is allowed.

- When the function of matching the referer field with whitelist rules is disabled, the referer field will not be matched with all whitelist rules.

By default, the function of matching the referer field in a URL request with whitelist rules is enabled. If the function is disabled, you can run the **undo referer-filter whitelist-all enable** command to disable it.

The referer field is a part of an HTTP header. A browser adds the referer field to an HTTP request before sending it to a web server, so that the web server can understand the link of the web.

Example

Create URL filtering profile **profile_development**, and add www.example.com to the referer-host rule.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] add referer-host www.example.com
```

19.9.3.5 category action (URL filtering profile view)

Function

The **category action** command specifies the action for a URL category.

The **undo category action** command specifies the default action for a URL category to **allow**.

Format

category { **pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **action** { **allow** | **alert** | **block** }

undo category { **pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **action**

Parameters

Parameter	Description	Value
category-id	Specifies the ID of a predefined URL category.	The value is an integer ranging from 1 to 100.
subcategory-id	Specifies the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.
category-name	Specifies the name of a user-defined URL category.	The URL category has been configured.
allow	Sets the category action to **allow**.	-
block	Sets the category action to **block**.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
alert	Sets the category action to **alert** and records URL filtering logs.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

Run the **display url-filter category pre-defined** command to display the *subcategory-id* of the specified predefined URL category.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the action for the predefined category **P2P** to **block** in the URL filtering profile view.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] category pre-defined subcategory-id 101 action block
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.6 category action mode (URL filtering profile view)

Function

The **category action mode** command configures the action mode of URL filtering.

The **undo category action mode** command restores the default setting.

Format

category action mode { **strict** | **loose** }

undo category action mode

Parameters

Parameter	Description	Value
strict	Indicates the strict mode.	-

Parameter	Description	Value
loose	Indicates the loose mode.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

The default action mode for URL categories is the strict mode.

If a URL belongs to multiple categories, the Router takes an action based on the action mode.

- Strict: The Router takes the strictest action among all matched categories. For example, a URL belongs to two categories, and the actions are **Alert** and **Block**. In this case, the Router takes the **Block** action.
- Loose: The Router takes the loosest action among all matched categories. For example, a URL belongs to two categories, and the actions are **Alert** and **Block**. In this case, the Router takes the **Alert** action.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the action mode of URL filtering to the loose mode.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] category action mode loose
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.7 category pre-defined control-level (URL filtering profile view)

Function

The **category pre-defined control-level** command sets the control level for predefined URL categories.

The **undo category pre-defined control-level** command sets the default control level for predefined URL categories to user-defined.

Format

category pre-defined control-level { **high** | **low** | **medium** }

undo category pre-defined control-level

Parameters

Parameter	Description	Value
high	Sets the control level to **high**.	None
low	Sets the control level to **low**.	It is the default control level.
medium	Sets the control level to **medium**.	None

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

The device performs different actions on different types of websites at different control levels. To view the category control information at a specified level, run the **display url-filter category pre-defined control-level** [**high** | **low** | **medium**] command.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the control level for predefined URL categories to **medium**.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] category pre-defined control-level medium
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.8 default action (URL filtering profile view)

Function

The **default action** command sets the default action for a URL filtering profile.

The **undo default action** command sets the default action for a URL filtering profile to **allow**.

Format

default action { **allow** | **block** | **alert** }

undo default action

Parameters

Parameter	Description	Value
allow	Sets the default action to **allow**.	-
block	Sets the default action to **block**.	-
alert	Sets the default action to **alert**.	-

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

The default action for a URL filtering profile is **allow**.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the default action for the URL filtering profile **profile_development** to **block** in the URL filtering profile view.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] default action block
[Huawei-profile-url-filter-profile_development] quit
[Huawei] engine configuration commit
```

19.9.3.9 description (URL filtering profile view)

Function

The **description** command configures the description of a URL filtering profile.

The **undo description** command deletes the description of a URL filtering profile.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of the URL filtering configuration file.	It is a case-sensitive character string of 1 to 128 characters.

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

Descriptive information about a URL filtering profile helps you remember and recognize a URL filtering profile. Run the **display profile type url-filter** command to view the description of the specified URL filtering profile.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Set the description of the URL filtering profile **abc**.

```
<Huawei> system-view
[Huawei] profile type url-filter name abc
[Huawei-profile-url-filter-abc] description for marketing
[Huawei-profile-url-filter-abc] quit
[Huawei] engine configuration commit
```

19.9.3.10 description (user-defined URL category view)

Function

The **description** command configures the description of a user-defined URL category.

The **undo description** command deletes the description of a user-defined URL category.

Format

description *description*

undo description

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined URL category.	It is a case-sensitive character string of 1 to 128 characters.

Views

User-defined URL category view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the description of the user-defined URL category **ud_abc**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name ud_abc
[Huawei-cate-user-defined-ud_abc] description for research
```

19.9.3.11 display profile type url-filter

Function

The **display profile type url-filter** command displays information about URL filtering profiles.

Format

display profile type url-filter

display profile type url-filter name *name* [**blacklist** [**url** *url-text* | **host** *host-text*] | **whitelist** [**url** *url-text* | **host** *host-text*] | **pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*]]

Parameters

Parameter	Description	Value
name *name*	Indicates the name of a URL filtering profile.	The value must be the name of an existing URL filtering profile.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
blacklist	Indicates the URL blacklist of the URL filtering profile.	-
whitelist	Indicates the URL whitelist of the URL filtering profile.	-
url *url-text*	Specifies a URL rule.	-
host *host-text*	Specifies a domain name rule.	-
pre-defined	Indicate the predefined category.	-
category-id *category-id*	Indicates the ID of a predefined URL category.	The value is an integer ranging from 1 to 100.
subcategory-id *subcategory-id*	Indicates the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.
user-defined	Specifies a user-defined category.	-
name *category-name*	Indicates the name of a user-defined URL category.	The URL category must have been configured.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display configuration information about all URL filtering profiles.

```
<Huawei> display profile type url-filter
-------------------------------------------------------------------------------
  URL Filtering Profile Configurations:
  Total Profiles: 2
-------------------------------------------------------------------------------
  Name        : abc
  Description : -
```

```
 Referenced  : 0
-------------------------------------------------------------------------------
 Default Action : Block
-------------------------------------------------------------------------------
 Action Mode    : Strict
-------------------------------------------------------------------------------
 Https-Filter   : Disable
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 All Whitelist Rule Support Refer: Enable
-------------------------------------------------------------------------------
 Blacklist Configurations:
-------------------------------------------------------------------------------
 Type              Blacklist
-------------------------------------------------------------------------------
 url               www.example.com
 host              www.example.com
-------------------------------------------------------------------------------
 Whitelist Configurations:
-------------------------------------------------------------------------------
 Type              Whitelist
-------------------------------------------------------------------------------
 url               www.example.org
 host              www.example.org
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 RefererList  Configurations:
-------------------------------------------------------------------------------
 Type              RefererList
-------------------------------------------------------------------------------
 host              www.example.com
-------------------------------------------------------------------------------
 URL Pre-defined Category Configurations:
 Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID),
        SN(Subcategory Name)
-------------------------------------------------------------------------------
 CID CN              SID   SN                              Action
-------------------------------------------------------------------------------
 1   P2P
                     101   P2P                             Allow
 2   Download
                     102   e-Books                         Allow
                     162   Software Download               Allow
                     163   Picture Download                Block
                     164   Music/Film Download             Allow
                     165   General Download                Allow
-------------------------------------------------------------------------------
 URL User-defined Category Configurations:
-------------------------------------------------------------------------------
 CID CN              SID   SN                              Action
-------------------------------------------------------------------------------
 100 User-defined
                     6001  abc                             Allow
                     6002  def                             Block
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 Name        : default
 Description : -
 Referenced  : 0
-------------------------------------------------------------------------------
 Default Action : Allow
-------------------------------------------------------------------------------
 Action Mode    : Strict
-------------------------------------------------------------------------------
 Https-Filter   : Disable
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
 All Whitelist Rule Support Refer: Enable
-------------------------------------------------------------------------------
```

```
Blacklist Configurations:
--------------------------------------------------------------------------------
Type              Blacklist
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Whitelist Configurations:
--------------------------------------------------------------------------------
Type              Whitelist
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
RefererList  Configurations:
--------------------------------------------------------------------------------
Type              RefererList
--------------------------------------------------------------------------------
URL Pre-defined Category Configurations:
Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID),
       SN(Subcategory Name)
--------------------------------------------------------------------------------
CID CN              SID   SN                                Action
--------------------------------------------------------------------------------
1   P2P
                    101   P2P                             Allow
2   Download
                    102   e-Books                         Allow
                    162   Software Download                Allow
                    163   Picture Download                Allow
                    164   Music/Film Download              Allow
                    165   General Download                 Allow
--------------------------------------------------------------------------------
URL User-defined Category Configurations:
--------------------------------------------------------------------------------
CID CN              SID   SN                                Action
--------------------------------------------------------------------------------
100 User-defined
                    6001  abc                             Block
                    6002  def                             Block
--------------------------------------------------------------------------------
```

Table 19-117 Description of the **display profile type url-filter** command output

Item	Description
URL Filtering Profile Configurations	Configuration of URL filtering profiles
Total Profiles	Total number of profiles
Name	Name of the URL filtering profile
Description	Description of the URL filtering configuration file
Referenced	Referenced count
Default Action	Default action for the URL filtering profile
Https-Filter	Encrypted-traffic filtering
Blacklist Configurations	Blacklist configuration
Whitelist Configurations	Whitelist configuration
RefererList Configurations	Referer-host configuration
Type	Match type

Item	Description
Blacklist	URL blacklist
Whitelist	URL whitelist
RefererList	Referer-host
url	URL
host	Domain name

19.9.3.12 display url-filter category

Function

The **display url-filter category** command displays the URL category list.

Format

display url-filter category [**pre-defined** [**category-id** *category-id* | **subcategory-id** *subcategory-id* | **url** *url-text* | **host** *host-text*] | **user-defined** [**name** *category-name* | **url** *url-text* | **host** *host-text*]]

Parameters

Parameter	Description	Value
pre-defined	Displays information on predefined URL categories.	-
category-id	Indicates the ID of a predefined URL category.	The value is an integer ranging from 1 to 100.
subcategory-id	Indicates the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pre-defined url *url-text*	Indicates the URL rule added to a predefined URL category.	The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is www.example.com/abc/def?"gh, you need to enter www.example.com/abc/def?%22gh.
pre-defined host *host-text*	Indicates the domain name rule added to a predefined URL category.	The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space.
user-defined	Displays information on user-defined URL categories.	-
category-name	Indicates the name of a user-defined URL category.	The category must have been configured.
user-defined url *url-text*	Indicates the URL rule added to a user-defined URL category.	The value is a character string. If the URL does not contain any space or question mark (?), the length is 4 to 255 characters. If the URL contains spaces or question marks (?) (not at the end), the URL must be enclosed by double quotation marks ("") and the length is 6 to 255 characters. If the URL contains double quotation marks (""), you need to replace them with escape characters "%22". For example, if the URL is www.example.com/abc/def?"gh, you need to enter www.example.com/abc/def?%22gh.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-defined host *host-text*	Indicates the domain name rule added to a user-defined URL category.	The value is a character string and the length is 4 to 255 characters, without special character slash (/), back slash (\), number sign (#), double quotation mark ("), question mark (?), or space.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display url-filter category pre-defined** [**url** *url-text* | **host** *host-text*] command displays only rules added to predefined URL categories but not rules in the predefined URL category database. You can view rules in the predefined URL category database on the web UI. Log in the web UI of the Router, and choose **Object** > **URL Category**. Enter a URL in the search text box and click **Search** to view URL category information.

Example

Display the URL category list.

```
<Huawei> display url-filter category
-------------------------------------------------------------------------------
 URL Pre-defined Category Count: 138
 URL Pre-defined Category List:
 Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID),
        SN(Subcategory Name)
-------------------------------------------------------------------------------
 CID   CN                    SID   SN
-------------------------------------------------------------------------------
 1     P2P
                           101   P2P
 2     Download
                           102   e-Books
                           162   Software Download
                           163   Picture Download
                           164   Music/Film Download
-------------------------------------------------------------------------------
 URL User-defined Category Count: 1
 URL User-defined Category List:
-------------------------------------------------------------------------------
 CID    CN                  SID      SN
-------------------------------------------------------------------------------
 100    User-defined
                          60001 abc
                          60001 def
-------------------------------------------------------------------------------
```

Table 19-118 Description of the **display url-filter category** command output

Item	Description
URL Pre-defined Category Count	Number of predefined URL categories
URL Pre-defined Category List	List of predefined URL categories
CID	Category ID
CN	Category name
SID	Subcategory ID
SN	Subcategory name
URL User-defined Category Count	Number of user-defined URL categories
URL User-defined Category List	List of user-defined URL categories

Display the predefined category with category ID 2.

```
<Huawei> display url-filter category pre-defined category-id 2
-------------------------------------------------------------------------------
  Category Name        : Download
  Category ID          : 2
  Category Description : Web sites related to download
-------------------------------------------------------------------------------
  Category Configuration Information:
  Codes: SID(Subcategory ID), SN(Subcategory Name)
-------------------------------------------------------------------------------
  SID   SN                                    Type      User-defined URLs/HOSTs
-------------------------------------------------------------------------------

  102   e-Books                                 url       www.example.com.com
                                            host      www.example.com
  162   Software Download                         url       www.example.com.cn
  163   Picture Download
  164   Music/Film Download                       url       www.example.com
  165   General Download
-------------------------------------------------------------------------------
```

Table 19-119 Description of the **display url-filter category pre-defined category-id 2** command output

Item	Description
Category Name	Category name
Category ID	Category ID
Category Description	Category description
Category Configuration Information	Category configuration
SID	Subcategory ID
SN	Subcategory name

Item	Description
Type	Match type
User-defined URLs/HOSTs	User-defined URL or host

Display the information about predefined subcategory 101.

```
<Huawei> display url-filter category pre-defined subcategory-id 101
-------------------------------------------------------------------------------
  Subcategory Name        : P2P
  Subcategory ID          : 101
  Subcategory Description : Web sites that provide the introduction to and download of P2P
resources, these Web sites are always bound to contain P2P tools such as Thunder and VeryCD,
providing seed download, search, and release
  Category Name           : P2P
  Category ID             : 1
-------------------------------------------------------------------------------
  Subcategory Configuration Information:
-------------------------------------------------------------------------------
                          User-defined URLs/HOSTs
                            (Count: 2)
-------------------------------------------------------------------------------
  Type                  URLs/HOSTs
-------------------------------------------------------------------------------
  url                  www.example.com.com
  host                  www.example.com
-------------------------------------------------------------------------------
```

Table 19-120 Description of the **display url-filter category pre-defined subcategory-id 101** command output

Item	Description
Subcategory Name	Name of a predefined URL subcategory
Subcategory ID	ID of a predefined URL subcategory
Subcategory Description	Description of a user-defined subcategory
Category Name	Name of a predefined URL category
Category ID	ID of a predefined URL category
Subcategory Configuration Information	Subcategory configuration
User-defined URLs/HOSTs	User-defined URL or domain name
Count	Total number user-defined URLs or domain names
Type	Match type

Display the information about the user-defined category **abc**.

```
<Huawei> display url-filter category user-defined name abc
-------------------------------------------------------------------------------
```

```
 Category Name          : abc
 Category ID            : 60001
 Category Description : -
-------------------------------------------------------------------------------
                                User-defined URLs/HOSTs
                                      (Count : 2)
-------------------------------------------------------------------------------
 Type                 URLs/HOSTs
-------------------------------------------------------------------------------
 url                 www.example.com.com
 host                 www.example.com
-------------------------------------------------------------------------------
```

Table 19-121 Description of the **display url-filter category user-defined name abc** command output

Item	Description
Category Name	Name of a user-defined URL category.
Category ID	ID of a user-defined URL category
Category Description	Description of a user-defined URL category
User-defined URLs/HOSTs	User-defined URL or domain name
Count	Total number user-defined URLs or domain names
Type	Match type

Display the rules containing **example.com** in the user-defined category.

```
<Huawei> display url-filter category user-defined host example.com
-------------------------------------------------------------------------------
 Matched Count : 2
 Matched Result Information:
 Codes: SID(Subcategory ID), SN(Subcategory Name)
-------------------------------------------------------------------------------
 SID    SN                          Matched URLs/HOSTs
-------------------------------------------------------------------------------
 60001  abc                          www.example.com
 60002  def                          www.example.com/abc
-------------------------------------------------------------------------------
```

Table 19-122 Description of the **display url-filter category user-defined host example.com** command output

Item	Description
Matched Count	Match count
Matched Result Information	Match result
SID	Subcategory ID
SN	Subcategory name
Matched URLs/HOSTs	Matched URL or domain name

19.9.3.13 display url-filter category pre-defined control-level

Function

The **display url-filter category pre-defined control-level** command displays information about all the predefined categories of a specific control level.

Format

display url-filter category pre-defined control-level [**high** | **low** | **medium**]

Parameters

Parameter	Description	Value
high	Displays information about all the predefined categories whose control level is **high**.	-
low	Displays the control level for a predefined category to **low**.	-
medium	Displays the control level for a predefined category to **medium**.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the information about all the predefined categories whose control level is **low**.

```
<Huawei> display url-filter category pre-defined control-level low
-------------------------------------------------------------------------------
 Control Level: Low
 URL Pre-defined Category Configurations:
 Codes: CID(Category ID), CN(CategoryName), SID(Subcategory ID)
        SN(Subcategory Name)
-------------------------------------------------------------------------------
 CID CN                  SID   SN                                Action
-------------------------------------------------------------------------------
 1   P2P
                     101   P2P                               Allow
 2   Download
                     102   e-Books                           Allow
                     162   Software Download                     Allow
```

```
                    163   Picture Download                    Allow
                    164   Music/Film Download                   Allow
                    165   General Download                    Allow
3   Humanity
                    103   History/Culture                   Allow
                    166   Literature                      Allow
                    167   Arts                          Allow
                    168   Music                           Allow
4   Sports
                    104   Competitive Sports                  Allow
                    169   Leisure Sports                    Allow
                    170   Sports Equipment                    Allow
.........
```

Table 19-123 Description of the **display url-filter category pre-defined control-level** command output

Item	Description
Control Level	Control level of a predefined category
CID	ID of a predefined URL category.
CN	Name of a predefined URL category
SID	ID of a predefined URL subcategory
SN	Name of a predefined URL subcategory
Action	Available actions: ● Allow ● Block ● Alert

19.9.3.14 display url-filter category statistics

Function

The **display url-filter category statistics** command displays URL category statistics.

Format

display url-filter category { **pre-defined** [**subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **statistics**

Parameters

Parameter	Description	Value
pre-defined	Displays statistics on predefined URL categories.	-

Parameter	Description	Value
subcategory-id *subcategory-id*	Specifies the subcategory ID of a predefined URL category.	The value is an integer ranging from 101 to 60000.
user-defined	Displays statistics on user-defined URL categories.	-
name *category-name*	Specifies the name of a user-defined URL category.	The specified category must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display url-filter category statistics** command to view the URL category statistics, you can run the **reset url-filter category statistics** command to clear the original statistics and collect statistics again. Cleared statistics cannot be restored. Exercise caution when you run this command.

Example

Display statistics on predefined URL categories.

```
<Huawei> display url-filter category pre-defined statistics
  Statistics Information on slot 11 cpu 0:
-------------------------------------------------------------------------------
  Category Statistics Information:
  Codes: SID(Subcategory ID), SN(Subcategory Name), SMN(Subcategory Matched
Num)
-------------------------------------------------------------------------------
  SID   SN                                   SMN
-------------------------------------------------------------------------------
  101   P2P                                  0
  102   e-Books                                0
  103   History/Culture                          0
  104   Competitive Sports                         0
  105   Charity/Public Welfare                     0
  106   Military                             0
  108   Blogs/Community                            0
  109   Lottery                              0
  110   Dating/Personals                         0
  111   Cartoon/Animation                          0
  112   Adult Recreational Places                  0
  114   Recreation                             0
  115   Video Games                              0
  117   Toys                                 0
  118   Religion                              0
  119   Divining/Supernatural                      0
  122   Adult Suppliers                          0
  123   Gardens/Yards                            0
  ---- More ----
```

Table 19-124 Description of the **display url-filter category pre-defined statistics** command output

Item	Description
Statistics Information on slot *X* cpu *Y*	Statistics of CPU *Y* in slot *X*
SID	URL subcategory ID
SN	URL subcategory name
SMN	URL subcategory match count

19.9.3.15 display url-filter statistics

Function

The **display url-filter statistics** command displays statistics on URL filtering.

Format

display url-filter statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display URL filtering statistics.

```
<Huawei> display url-filter statistics
-----------------------------------------------------------------------------
 Statistics Information:
-----------------------------------------------------------------------------
 Total HTTP Requests            : 448460
 Total Permitted HTTP Requests  : 448460
 Total Denied HTTP Requests     : 0
 Matched Blacklist              : 0
 Matched Whitelist              : 0
 Matched User-defined Category  : 0
 Matched Timeout Action         : 0
```

```
Matched Default Action        : 448460
-------------------------------------------------------------------------------
```

Table 19-125 Description of the **display url-filter statistics** command output

Item	Description
Statistics Information	Statistics on URL filtering
Total HTTP Requests	Total number of HTTP requests
Total Permitted HTTP Requests	Total number of permitted HTTP requests
Total Denied HTTP Requests	Total number of blocked HTTP requests
Matched Blacklist	Number of times the blacklist is matched
Matched Whitelist	Number of times the whitelist is matched
Matched User-defined Category	Number of times the user-defined category is matched
Matched Timeout Action	Number of times the timeout action is matched
Matched Default Action	Number of times the default action is matched

19.9.3.16 https-filter enable

Function

The **https-filter enable** command enables the encrypted traffic filtering function.

The **undo https-filter enable** command disables the function.

Format

https-filter enable

undo https-filter enable

Parameters

None

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the function is disabled.

The URL requests sent by users to access desired websites are transmitted using HTTP or HTTPS. For HTTP traffic, the Router can properly implement URL filtering. For HTTPS traffic, the Router can implement URL filtering only after encrypted traffic filtering is configured.

Encrypted traffic filtering takes effect only when it is enabled in the URL filtering profile. If encrypted traffic filtering is disabled in the URL filtering profile, the URL filtering profile does not take effect for HTTPS traffic.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Enable the encrypted traffic filtering function.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_url
[Huawei-profile-url-filter-profile_url] https-filter enable
[Huawei-profile-url-filter-profile_url] quit
[Huawei] engine configuration commit
```

19.9.3.17 import url-sdb file

Function

The **import url-sdb file** command loads the initial URL category database.

Format

import url-sdb file *filename*

Parameters

Parameter	Description	Value
filename	Specifies an initial database file name that contains the absolute path.	The value is a string of 1 to 63 characters without spaces, for example, **hda1:/url.sdb**.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If no initial URL category database is loaded on the device or the initial URL category database needs to be updated, you can manually load the initial URL category database.

If the CF card of the device is damaged, the initial URL category database cannot be loaded. In this case, contact technical support personnel.

Example

Load an initial URL category database.

```
<Huawei> system-view
[Huawei] import url-sdb file hda1:/url.sdb
```

19.9.3.18 profile type url-filter copy

Function

The **profile type url-filter copy** command creates a URL filtering profile (by cloning an existing one) and displays the view of the new URL filtering profile.

Format

profile type url-filter copy *old-name* [*new-name*]

Parameters

Parameter	Description	Value
old-name	Specifies the name of the URL filtering profile to be cloned.	The URL filtering profile must have been configured.
new-name	Specifies the name of the new URL filtering profile.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) are not supported.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can clone an existing URL filtering profile and modify it to create a similar URL filtering profile.

If *new-name* is not specified, the name of the new URL filtering profile is set to "*old-name*_num". **num** indicates the number of times the URL filtering profile is cloned. The value is an integer starting from 1.

Example

Create two URL filtering profiles by cloning the URL filtering profile **abc**.

```
<Huawei> system-view
[Huawei] profile type url-filter copy abc
[Huawei-profile-url-filter-abc_1] quit
[Huawei] profile type url-filter copy abc
[Huawei-profile-url-filter-abc_2] quit
[Huawei]
```

19.9.3.19 profile type url-filter name

Function

The **profile type url-filter name** command creates a URL filtering profile and enters the URL filtering profile view.

The **undo profile type url-filter** command deletes all or specified URL filtering profiles.

Format

profile type url-filter name *name*

undo profile type url-filter { **all** | **name** *name* }

Parameters

Parameter	Description	Value
name	Specifies the name of a URL filtering profile.	The value is a case-sensitive string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.
all	Deletes all URL filtering profiles.	None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you create a URL filtering profile, configure the blacklist, whitelist, user-defined category, and predefined category to specify the URLs that need to be filtered.

Example

Create a URL filtering profile with the name **abc**.

```
<Huawei> system-view
[Huawei] profile type url-filter name abc
[Huawei-profile-url-filter-abc]
```

19.9.3.20 referer-filter whitelist-all enable

Function

The **referer-filter whitelist-all enable** command enables the function for matching the referer field in an HTTP request with all configured whitelist rules.

The **undo referer-filter whitelist-all enable** command disables the function.

Format

referer-filter whitelist-all enable

undo referer-filter whitelist-all enable

Parameters

None

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

By default, the function is enabled. The function can be used to access other links on a specific web page.

During URL filtering, if the referer field in an HTTP request sent by a user does not match the referer-host rule configured using the **add referer-host** command, the user can determine whether to match the referer field with all whitelist rules.

- When the function of matching the referer field with whitelist rules is enabled, the referer field will be matched with all whitelist rules. If a match is found, the user can access the website.
- When the function of matching the referer field with whitelist rules is disabled, the referer field will not be matched with all whitelist rules.

Example

Disable the function for matching the referer field in an HTTP request with all configured whitelist rules.

```
<Huawei> system-view
[Huawei] profile type url-filter name profile_development
[Huawei-profile-url-filter-profile_development] undo referer-filter whitelist-all enable
```

19.9.3.21 rename (URL filtering profile view)

Function

The **rename** command renames an existing URL filtering profile and displays the new profile view.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the new name of the URL filtering profile.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.

Views

URL filtering profile view

Default Level

2: Configuration level

Usage Guidelines

Run the rename command renames an existing URL filtering profile and displays the new profile view.

The configuration do not take effect until you run the **engine configuration commit** command to commit the configuration.

Example

Rename the URL filtering profile **abc** to **hello**.

```
<Huawei> system-view
[Huawei] profile type url-filter name abc
[Huawei-profile-url-filter-abc] rename hello
[Huawei-profile-url-filter-hello] quit
[Huawei] engine configuration commit
```

19.9.3.22 rename (user-defined URL category view)

Function

The **rename** command renames an existing user-defined URL category and displays the view of the new user-defined URL category.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the name of a user-defined URL category.	The value is a string of case-insensitive characters. The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-). ● If the value does not contain any space, the value contains 1 to 32 characters. ● If the value contains spaces, you must enclose the value with double quotation marks (""), for example, "user for test", and the value contains 3 to 34 characters.

Views

User-defined URL category view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **rename** command to rename a user-defined URL category to facilitate management.

Example

Rename the user-defined URL category **company** to **development**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name company
[Huawei-category-user-defined-company] rename development
[Huawei-category-user-defined-development]
```

19.9.3.23 reset url-filter category statistics

Function

The **reset url-filter category statistics** command clears URL category statistics.

Format

reset url-filter category { **pre-defined** [**subcategory-id** *subcategory-id*] | **user-defined** [**name** *category-name*] } **statistics**

Parameters

Parameter	Description	Value
pre-defined	Clears statistics on predefined URL categories.	-
subcategory-id *subcategory-id*	Specifies the subcategory ID of a predefined URL category.	The value is an integer ranging from 101 to 60000.
user-defined	Clears statistics on user-defined URL categories.	-
name *category-name*	Specifies the name of a user-defined URL category.	The specified category must already exist.

Views

User view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you run the **display url-filter category statistics** command to view the URL category statistics, you can run the **reset url-filter category statistics** command to clear the original statistics and collect statistics again. Cleared statistics cannot be restored. Exercise caution when you run this command.

Example

Clear statistics on predefined URL categories.

```
<Huawei> reset url-filter category pre-defined statistics
```

19.9.3.24 reset url-filter statistics

Function

The **reset url-filter statistics** command clears statistics on URL filtering.

Format

reset url-filter statistics { **blacklist** | **whitelist** | **category** [**user-defined** | **pre-defined**] | **all** }

Parameters

Parameter	Description	Value
blacklist	Indicates the number of times that blacklisted URLs are matched.	-
whitelist	Indicates the number of times whitelisted URLs are matched.	-
user-defined	Indicates the number of times user-defined categories are matched.	-
pre-defined	Indicates the number of times predefined categories are matched.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
all	Indicates all URL filtering statistics, including: ● Total number of user-initiated visits, the total number of Router allowed visits, and the total number of Router blocked visits. ● Number of times when whitelisted and blacklisted URLs, and user-defined and pre-defined categories are matched. ● Number of times when the Router performs the timeout action because of query category timeout, and number of times when the Router performs the default action. ● Number of times when abnormal HTTP packets are matched. ● Matching count of a predefined cache entry.	-

Views

User view

Default Level

3: Management level

Usage Guidelines

Use caution before you decide to run this command. Once statistics on URL filtering are cleared, they cannot be restored.

Example

Clears all URL filtering statistics.

```
<Huawei> reset url-filter statistics all
```

19.9.3.25 url-filter anti-bypass enable

Function

The **url-filter anti-bypass enable** command enables the abnormal HTTP packet detection function.

The **undo url-filter anti-bypass enable** command disables the abnormal HTTP packet detection function.

Format

url-filter anti-bypass enable

undo url-filter anti-bypass enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the abnormal HTTP packet detection function is disabled.

When the web server has the fault tolerance mechanism or the web server is not designed based on the RFC standard of HTTP, attackers may evade URL filtering. When an attacker tampers with an HTTP packet to make the URL information extracted by the Router different from URL filtering rules, the Router will permit the abnormal HTTP packet. After the abnormal HTTP packet reaches the web server, the server can identify the requested URL. Therefore, the attacker can access the URL.

After you enable the abnormal HTTP packet detection function, the Router can detect abnormal HTTP packets, preventing attackers from evading URL filtering.

Example

Enable abnormal HTTP packet detection.

```
<Huawei> system-view
[Huawei] url-filter anti-bypass enable
```

19.9.3.26 url-filter category pre-defined copy

Function

The **url-filter category pre-defined copy** command clones a predefined URL category.

Format

url-filter category pre-defined copy *subcategory-id new-name*

Parameters

Parameter	Description	Value
subcategory-id	Specifies the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
new-name	Specifies the name of the predefined URL category to be created.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

You can create a user-defined URL category by cloning an existing predefined URL category and modifying it.

Example

Clone the predefined subcategory 101 and rename the new category as **company**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined copy 101 company
[Huawei-cate-user-defined-company]
```

19.9.3.27 url-filter category pre-defined subcategory-id

Function

The **url-filter category pre-defined subcategory-id** command displays the predefined subcategory view.

Format

url-filter category pre-defined subcategory-id *subcategory-id*

Parameters

Parameter	Description	Value
subcategory-id	Indicates the ID of a predefined URL subcategory.	The value is an integer ranging from 101 to 60000.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Run the **display url-filter category pre-defined** command to display the *subcategory-id* of the specified predefined URL category.

Example

Display the view of the predefined subcategory **P2P**.

```
<Huawei> system-view
[Huawei] url-filter category pre-defined subcategory-id 101
[Huawei-cate-pre-defined-101]
```

19.9.3.28 url-filter category user-defined copy

Function

The **url-filter category user-defined copy** command clones a user-defined URL category.

Format

url-filter category user-defined copy *old-name* [*new-name*]

Parameters

Parameter	Description	Value
old-name	Indicates the name of a user-defined URL category.	The category must have been configured.
new-name	Indicates the name of the URL category.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If *new-name* is not specified in the command, the name of the new URL category is the original category name suffixed by **_num**. **_num** indicates the number of times the URL category is cloned.

Example

Clone the user-defined category **company**.

```
<Huawei> system-view
[Huawei] url-filter category user-defined copy company
[Huawei-cate-user-defined-company_1]
```

19.9.3.29 url-filter category user-defined name

Function

The **url-filter category user-defined name** command creates a user-defined URL category and displays the user-defined URL category view.

The **undo url-filter category user-defined** command deletes one or all user-defined URL categories.

Format

url-filter category user-defined name *category-name*

undo url-filter category user-defined { **name** *category-name* | **all** }

Parameters

Parameter	Description	Value
category-name	Specifies the name of a user-defined URL category.	The value is a case-sensitive character string. The length of a name without spaces ranges from 1 to 32 characters. The length of a name with spaces ranges from 3 to 34 characters. If a name contains spaces, the name must be enclosed with quotation marks (for example, "user for test"). Question marks (?), commas (,), quotations marks ("), and hyphens (-) cannot be used.
all	Indicates all user-defined URL categories.	None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Create a user-defined URL category and display the user-defined URL category view.

```
<Huawei> system-view
[Huawei] url-filter category user-defined name abc
```

19.9.3.30 url-filter https-filter consistency-check enable

Function

The **url-filter https-filter consistency-check enable** command enables the encrypted traffic consistency check function.

The **undo url-filter https-filter consistency-check enable** command disables the encrypted traffic consistency check function.

Format

url-filter https-filter consistency-check enable

undo url-filter https-filter consistency-check enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, this function is disabled.

Usually, URL requests are transmitted through HTTP or HTTPS. The Router can filter HTTP traffic without any additional configuration. To filter HTTPS traffic, the Router must have the encrypted traffic filtering function enabled.

Encrypted traffic filtering of URL filtering does not decrypt HTTPS. Instead, it obtains the domain name (HOST) of the website that a user wants to access by parsing packets.

After the **url-filter https-filter consistency-check enable** command is used to enable encrypted traffic consistency check, the Router extracts the target website domain name (HOST) from the **Server Name Indication** field in the Client Hello packet of the client and the **Common Name** and **Subject Alternative Name** fields in the Certificate packet of the server and verifies the three values during TLS negotiation. In addition, the Router verifies the values of the three fields. The Router implements URL filtering only when the verification succeeds.

The website information contained in the three fields may be tampered with by malicious users. Therefore, some traffic evades URL filtering due to a field verification failure, which affects the detection accuracy of the device.

In whitelist mode (whitelist-only enable), the encrypted traffic consistency check function does not take effect. In whitelist mode, the device allows URL requests only when the ServerName, Common Name, and Subject Alternative Name fields are in the configured whitelist. If the three fields are different, that is, 1.abc.com, 2.abc.com, and 3.abc.com, set the whitelist to *.abc.com.

Example

Enable encrypted traffic consistency check.

```
<Huawei> system-view
[Huawei] url-filter https-filter consistency-check enable
```

19.9.3.31 web-url-filter user-set

Function

The **web-url-filter user-set** command enables user group-based URL filtering.

The **undo web-url-filter user-set** command disables user group-based URL filtering.

By default, user group-based URL filtering is disabled.

Format

web-url-filter user-set *user-set-name* **profile** *profile-name* [**time-range** *time-range-name*] [**description** *description-text*]

undo web-url-filter user-set *user-set-name*

Parameters

Parameter	Description	Value
user-set-name	Specifies the name of a user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.
profile *profile-name*	Specifies the name of a URL filtering profile. **NOTE** A URL filtering profile must be created using the **profile type url-filter name** command and the related parameters must be set.	The value is a string of case-insensitive characters. When the name does not contain spaces, the value is a string of 1 to 32 characters. When the name contains spaces, the value is a string of 3 to 34 characters, and you need to put the string in double quotation marks (""), for example, "user for test". The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-).
time-range *time-range-name*	Indicates the name of the created effective period. **NOTE** The effective period can take effect only after the **time-range** command is executed.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. It cannot contain question marks (?) or spaces. In addition, the word **all** cannot be specified as a time range name.
description *description-text*	Indicates the URL filtering description in the user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The web management system supports user group management. You can run the **web-url-filter user-set** command to enable user group-based URL filtering to control the URL addresses the users in the user group can access.

Prerequisites

The **user-set** command has been executed to create a user group.

Example

Enable URL filtering for the user group **huawei**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set huawei
[Huawei-web-user-set-huawei] quit
[Huawei-web] web-url-filter user-set huawei profile abc
```

19.9.3.32 enable web-url-filter user-set

Function

The **enable web-url-filter user-set** command enables user group-based URL filtering.

The **disable web-url-filter user-set** command disables user group-based URL filtering.

By default, user group-based URL filtering is disabled.

Format

enable web-url-filter user-set *user-set-name*

disable web-url-filter user-set *user-set-name* [**profile** *profile-name* [**time-range** *time-range-name*] [**description** *description-text*]]

Parameters

Parameter	Description	Value
user-set-name	Specifies the name of a user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks ("""), the string can contain spaces.

Parameter	Description	Value
profile *profile-name*	Specifies the name of a URL filtering profile. **NOTE** A URL filtering profile must be created using the **profile type url-filter name** command and the related parameters must be set.	The value is a string of case-insensitive characters. When the name does not contain spaces, the value is a string of 1 to 32 characters. When the name contains spaces, the value is a string of 3 to 34 characters, and you need to put the string in double quotation marks (""), for example, "user for test". The value cannot contain question marks (?), commas (,), double question marks ("), and hyphens (-).
time-range *time-range-name*	Indicates the name of the created effective period. **NOTE** The effective period can take effect only after the **time-range** command is executed.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. It cannot contain question marks (?) or spaces. In addition, the word **all** cannot be specified as a time range name.
description *description-text*	Indicates the URL filtering description in the user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (""), the string can contain spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The web management system supports user group management. You can run the **enable web-url-filter user-set** command to enable user group-based URL filtering to control the URL addresses the users in the user group can access.

Prerequisites

The **user-set** command has been executed to create a user group.

Example

Enable URL filtering for the user group **huawei**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set huawei
[Huawei-web-user-set-huawei] quit
[Huawei-web] enable web-url-filter user-set huawei
```

19.9.4 Deep Security Maintenance Commands

19.9.4.1 display engine session statistic

Function

The **display engine session statistic** command displays session statistics for the engine.

Format

display engine session statistic

Parameters

None

Views

All views

Level

1: Monitoring level

Usage Guidelines

None

Example

Displays session statistics for the engine.

```
<Huawei> display engine session statistic
 Engine Session Statistic Information of All Threads:
---------------------------------------------------------------------------
    Total Current Sessions                    :          0
    Total Current UDP Sessions                :          0
    Total Current TCP Sessions                :          0
    Total Blocked Sessions                    :          0
    Total Current Free Sessions               :      61440
    Total Current Buffered TCP Segments       :          0
    Total Out-of-sequence TCP Segments        :          0
    Total Overlapping TCP Segments            :          0
    Total Current Free TCP Segments           :       3000
---------------------------------------------------------------------------
Engine Session Statistic Information of Each Thread:
    T00: NgeSess        0, sent:        0 rcv:        0 lost:        0
    T01: NgeSess        0, sent:        0 rcv:        0 lost:        0
    T02: NgeSess        0, sent:        0 rcv:        0 lost:        0
    T03: NgeSess        0, sent:        0 rcv:        0 lost:        0
```

```
T04: NgeSess      0, sent:      0 rcv:      0 lost:      0
T05: NgeSess      0, sent:      0 rcv:      0 lost:      0
T06: NgeSess      0, sent:      0 rcv:      0 lost:      0
T07: NgeSess      0, sent:      0 rcv:      0 lost:      0
T08: NgeSess      0, sent:      0 rcv:      0 lost:      0
T09: NgeSess      0, sent:      0 rcv:      0 lost:      0
```

Table 19-126 Description of the **display engine session statistic** command output

Item	Description
Engine Session Statistic Information of All Threads	Session statistics for the engines used by all threads
Total Current Sessions	Total number of all sessions
Total Current UDP Sessions	Total number of UDP sessions
Total Current TCP Sessions	Total number of TCP sessions
Total Blocked Sessions	Total number of blocked sessions
Total Current Free Sessions	Total number of idle session nodes
Total Current Buffered TCP Segments	Total number of cached TCP segments
Total Out-of-sequence TCP Segments	Total number of out-of-sequence TCP segments
Total Overlapping TCP Segments	Total number of overlapped TCP segments
Total Current Free TCP Segments	Total number of TCP segments that can be cached
Engine Session Statistic Information of Each Thread	Session statistics for the engine used by each thread
NgeSess	Number of sessions
sent	Number of sent packets
rcv	Number of received packets
lost	Number of discarded packets

Related Topics

19.9.4.13 reset engine session statistic

19.9.4.2 display engine session table

Function

The **display engine session table** command displays the details about the IPv4 session table of an engine.

Format

display engine session table [**source-ip** *source-ip-address* | **source-port** *source-port-number* | **destination-ip** *destination-ip-address* | **destination-port** *destination-port-number* | **protocol** { **tcp** | **udp** }] * [**verbose**]

Parameters

Parameter	Description	Value
source-ip *source-ip-address*	Indicates a source IP address.	-
source-port *source-port-number*	Indicates a source port.	-
destination-ip *destination-ip-address*	Indicates a destination IP address.	-
destination-port *destination-port-number*	Indicates a destination port.	-
protocol	Indicates the protocol field in a session table.	-
tcp	Indicates a TCP session.	-
udp	Indicates a UDP session.	-
verbose	Indicates the details.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display details about the session table of an engine.

```
<Huawei> display engine session table
  VSys:0 Vpn:0 TCP 10.1.1.246:61487-->10.8.1.198:135 ttl:600 left-time:580

  VSys:0 Vpn:0 TCP 10.1.1.197:15141-->10.8.1.227:135 ttl:600 left-time:55

  VSys:0 Vpn:0 UDP 10.6.1.35:35141-->10.8.1.28:111 ttl:120 left-time:19

  VSys:0 Vpn:0 TCP 10.6.1.11:60833-->10.8.1.64:25 ttl:600 left-time:557

  VSys:0 Vpn:0 UDP 10.6.1.192:52189-->10.8.1.245:53 ttl:120 left-time:22

  VSys:0 Vpn:0 TCP 10.6.1.215:47705-->10.8.1.195:135 ttl:600 left-time:290

  ---- More ----
```

19.9.4.3 display engine statistic

Function

The **display engine statistic** command displays engine statistics.

Format

display engine statistic

Parameters

None

Views

All views

Level

1: Monitoring level

Usage Guidelines

None

Example

Display engine statistics.

```
<Huawei> display engine statistic
Engine Statistic Table
-------------------------------------------------------------------------------
 Total Alert Events  :        0
 Total Block Events  :        0
 -----------------------------------------------------------------------------
  Application              Alert Events              Block Events
 -----------------------------------------------------------------------------
  IPS                            0                         0
  URL-FILTER                        0                         0
-------------------------------------------------------------------------------
```

Table 19-127 Description of the **display engine statistic** command output

Item	Description
Engine Statistic Table	The engine statistics table.
Total Alert Events	Total number of all alert sessions.
Total Block Events	Total number of all block sessions.
Application	The application module ● IPS ● URL-FILTER

Item	Description
Alert Events	Number of alert sessions
Block Events	Number of block sessions

19.9.4.4 display file-frame information

Function

The **display file-frame information** command displays the resources of file frame.

Format

display file-frame information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the resources of file frame.

Table 19-128 Description of the **display file-frame information** command output

Item	Description
Max decompression size	Maximum decompressable file size

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Oversize Acion	Action for the situation that the maximum size of files that can be decompressed is exceeded: ● Allow: Allows the file transfer. ● Alert: Allows the file transfer and generates a log. ● Block: Blocks the file transfer and generates a log.
Max decompression depth	Maximum decompressable layers
Overdepth Acion	Action for the situation that the file decompression depth is exceeded: ● Allow: Allows the file transfer. ● Alert: Allows the file transfer and generates a log. ● Block: Blocks the file transfer and generates a log.
Max compression ratio	Maximum decompression ratio
Breakpoint Resume Protocol	Protocols for which resumable file transfer is disabled: ● ALL: HTTP and FTP ● HTTP ● FTP ● None: Resumable file transfer is not enabled.
File frame resources	File frame resource
Decompression handler	Number of handlers used in file decompression, with Total indicating the total number of handlers available in file decompression
File handler cachepool: file handler cache pool	
Thread name	Thread name, which can be: ● Work thread: working thread ● Total: total number of file handlers
Used	Number of used handlers
Total	Total number of available handlers
Data buffer cachepool: data block cache pool	

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Thread name	Thread name, which can be: ● Work thread: working thread ● Total: total number of data blocks
Used	Number of used data blocks
Total	Total number of available data blocks

19.9.4.5 display fragment-reassemble configuration

Function

The **display fragment-reassemble configuration** command displays the global fragment reassembly configuration.

Format

display fragment-reassemble configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global fragment reassembly configuration.

```
<Huawei> display fragment-reassemble configuration
Fragment Reassembly Configuration:
-----------------------------------------------------------
enable                : on
overflow-mode         : discard
overlap-mode          : consistency
time-out(s)           : 5
packet-cache(packets) : 255
total-cache(packets)  : 60000
-----------------------------------------------------------
```

Table 19-129 Description of the display fragment-reassemble configuration

Item	Description
enable	State of the fragment reassembly function. ● on: The function is enabled. ● off: The function is disabled.
overflow-mode	Indicates the method for handling packets arriving at a full buffer in fragment reassembly. ● discard: Packets arriving at a full buffer are discarded. ● forward: Packets arriving at a full buffer are forwarded straight through.
overlap-mode	Indicates the policy to handle overlapping fragments: ● consistency: Indicates that overlapping fragments are processed based whether the overlapping parts have the same content.
time-out(s)	Indicates the fragment reassembly timeout in seconds.
packet-cache(packets)	Indicates the fragment buffer size (in number of packets) for each packet.
total-cache(packets)	Indicates the total buffer size in number of packets.

19.9.4.6 display fragment-reassemble session table

Function

The **display fragment-reassemble session table** command displays packet fragment reassembly information in the IAE session table.

Format

display fragment-reassemble session table [**source-ip** *source-ip-address* | **destination-ip** *destination-ip-address*]*

Parameters

Parameter	Description	Value
source-ip *source-ip-address*	Specifies the source IP address.	The value is in dotted decimal notation.
destination-ip *destination-ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If the content security service is configured in the security policy for fragmented packets, the fragmented packets are sent to the IAE for processing. The IAE establishes a session and reassembles the fragmented packets. Using the **display fragment-reassemble session table** command, you can view the packet fragment reassembly information in the IAE session table.

Example

Display IPv4 packet fragment reassembly information in the IAE session table.

```
<Huawei> display fragment-reassemble session table
  VSys:0 Vpn:0 10.1.1.1-->10.2.1.1(363) ttl:5 left-time:4 frag-num:32 flags:(first 1,last 0,overflow 0,result
0)

  VSys:0 Vpn:0 10.1.1.3-->10.2.1.3(363) ttl:5 left-time:3 frag-num:32 flags:(first 1,last 0,overflow 0,result 0)
```

Table 19-130 Description of the **display fragment-reassemble session table** command output

Item	Description
VSys	Name of a virtual system
Vpn	Name of a VPN instance
ttl	Aging time of a fragment session
left-time	Remaining aging time of a fragment session
frag-num	Number of fragments

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
flags:(first 1,last 0,overflow 0,result 0)	Fragment flag, which can be: ● first: first fragment ● last: last fragment ● overflow: fragment cache overflow ● result: reassembly result

19.9.4.7 display profile

Function

The **display profile** command displays profile information about all modules.

Format

display profile

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display profile information about all modules.

```
<Huawei> display profile
 Profile Configurations:
 Total Profiles:
 ---------------------------------------------------------------------------
 ProfileName                    ProfileType  Referenced  State
 ---------------------------------------------------------------------------
 strict                         ips          0           committed
 web_server                     ips          0           committed
 file_server                    ips          0           committed
 dns_server                     ips          0           committed
 mail_server                    ips          0           committed
 inside_firewall                ips          0           committed
 dmz                            ips          0           committed
 outside_firewall               ips          0           committed
 ids                            ips          0           committed
```

```
default                    ips         1          committed
default                    url-filter  0           committed
```

Table 19-131 Description of the **display profile** command output

Item	Description
Total profiles	Total number of profiles
ProfileName	Name of the profile
ProfileType	Module where the profile belongs to
Referenced	Number of references by a security policy
State	Status of a profile: ● committed ● not committed

19.9.4.8 display stream-reassemble configuration

Function

The **display stream-reassemble configuration** command displays the global TCP stream reassembly configuration.

Format

display stream-reassemble configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the global TCP stream reassembly configuration.

```
<Huawei> display stream-reassemble configuration
Stream Reassembly Configuration:
```

```
-------------------------------------------------------------
enable                : on
overflow-mode         : forward
overlap-mode          : preserve
session-cache(KB)     : 128
total-cache(packets)  : 1024
timestamp-check       : false
tcp-option check      : false
defense-check         : on
session-timeout(s)    : 10
enhanced-mode         : off
-------------------------------------------------------------
```

Table 19-132 Description of the **display stream-reassemble configuration** command output

Item	Description
enable	Indicates the state of the TCP stream reassembly function. ● on: The function is enabled. ● off: The function is disabled.
overflow-mode	Indicates the method for handling packets arriving at a full buffer in stream reassembly. ● discard: Packets arriving at a full buffer are discarded. ● forward: Packets arriving at a full buffer are forwarded straight through.
overlap-mode	Indicates the policy to handle overlapping packets: ● overwrite: Indicate overwrite the original overlapped part. ● preserve: Indicate preserve the original overlapped part.
session-cache(KB)	Indicates the buffer size in KB for each session in TCP stream reassembly.
total-cache(packets)	Global buffer size in number of packets in stream reassembly.
timestamp-check	Indicates the state of the timestamp check function. ● true: The function is enabled. ● false: The function is disabled.
tcp-option check	Indicates the state of the TCP option check function. ● true: The function is enabled. ● false: The function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
defense-check	Indicates the status of the TCP attack defense function: ● on: The function is enabled. ● off: The function is disabled.
session-timeout(s)	Indicates the timeout of out-of-sequence TCP packet inspection, in seconds.
enhanced-mode	Status of enhanced traffic reassembly: ● on: The function is enabled. ● off: The function is disabled.

19.9.4.9 fragment-reassemble enable

Function

The **fragment-reassemble enable** command enables fragment reassembly.

The **undo fragment-reassemble enable** command disables fragment reassembly.

Format

fragment-reassemble enable

undo fragment-reassemble enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, fragment reassembly is enabled.

If fragment reassembly is disabled, fragments will not be reassembled and will not be inspected. Meanwhile, TCP stream reassembly may also fail.

Example

Enable fragment reassembly.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] fragment-reassemble enable
```

19.9.4.10 fragment-reassemble overflow-mode

Function

The **fragment-reassemble overflow-mode** command configures the action to take on fragments that overflow the cache.

The **undo fragment-reassemble overflow-mode** command restores the default action to take on fragments that overflow the cache.

By default, the device discards the fragments that overflow the cache.

Format

fragment-reassemble overflow-mode { **discard** | **forward** }

undo fragment-reassemble overflow-mode

Parameters

Parameter	Description	Value
discard	Discards the fragments that overflow the cache.	-
forward	Forwards the fragments that overflow the cache.	-

Views

System view

Level

2: Configuration level

Usage Guidelines

None.

Example

Configure the action to take on fragments that overflow the cache.

```
<Huawei> system-view
[Huawei] fragment-reassemble overflow-mode forward
```

19.9.4.11 fragment-reassemble user-configure

Function

The **fragment-reassemble user-configure** command configures user-defined items for the fragment reassembly function.

The **undo fragment-reassemble user-configure** command cancels the configuration of user-defined items for the fragment reassembly function.

Format

fragment-reassemble user-configure { **defense-check** | **pass-through** }

undo fragment-reassemble user-configure { **defense-check** | **pass-through** }

Parameters

Parameter	Description	Value
defense-check	Indicates fragment attack defense.	-
pass-through	Indicates the pass through mode.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, all user-defined items of the fragment reassembly function are disabled.

After the pass through mode is enabled (using the **fragment-reassemble user-configure pass-through** command), in some special fragment traffic scenarios (for example, the fragments completely overlap, and the overlapped part has the same content), the system will regard the traffic as abnormal traffic and will not reassemble the fragments. If the fragment attack defense function has been enabled (using the **fragment-reassemble user-configure defense-check** command), the abnormal fragments will be discarded. If the fragment attack defense function has not been enabled, the system will forward the fragments. After the pass through mode is disabled, the system assembles the fragments based on the normal processing flow.

Example

Enable the fragment attack defense function.

```
<Huawei> system-view
[Huawei] fragment-reassemble user-configure defense-check
```

19.9.4.12 fragment-reassemble user-configure defense-check

Function

The **fragment-reassemble user-configure defense-check** command enables the fragment attack defense function.

The **undo fragment-reassemble user-configure defense-check** command disables the fragment attack defense function.

Format

fragment-reassemble user-configure defense-check

undo fragment-reassemble user-configure defense-check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the fragment attack defense function is disabled.

After this function is enabled, the Router directly discards abnormal fragments.

Example

Enable the fragment attack defense function.

```
<Huawei> system-view
[Huawei] fragment-reassemble user-configure defense-check
```

19.9.4.13 reset engine session statistic

Function

The **reset engine session statistic** command clears the session statistics of the engine.

Format

reset engine session statistic

Parameters

None

Views

User view

Level

3: Management level

Usage Guidelines

NOTE

Use caution before you decide to run this command. Once the session statistics of the engine are cleared, they cannot be restored.

Example

Clear the session statistics of the engine.

```
<Huawei> reset engine session statistic
```

Related Topics

19.9.4.1 display engine session statistic

19.9.4.14 reset engine session table

Function

The **reset engine session table** command clears the session information of the engine.

Format

reset engine session table [**source** *source-ip-address* | **destination** *destination-ip-address* | **destination-port** *destination-port-number* | **protocol** { **tcp** | **udp** }] *

Parameters

Parameter	Description	Value
source *source-ip-address*	Specifies the source IP address.	The value is in dotted decimal notation.
destination *destination-ip-address*	Specifies the destination IP address.	The value is in dotted decimal notation.
destination-port *destination-port-number*	Specifies the destination port number.	The value is an integer ranging from 0 to 65535.
protocol	Indicates a protocol.	-
tcp	Indicates Transmission Control Protocol (TCP).	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
udp	Indicates User Datagram Protocol (UDP).	-

Views

User view

Default Level

3: Management level

Usage Guidelines

If no parameter is specified, all session information of the engine is cleared after you run the **reset engine session table** command.

Use caution before you decide to run this command. Clearing the session information of the engine adversely affects the service operating.

Example

Clear all session information of the engine.

```
<Huawei> reset engine session table
Warning: Reseting session table will affect the engine's normal service. Continue? [Y/N]: Y
<Huawei>
```

19.9.4.15 reset engine statistic

Function

The **reset engine statistic** command clears engine statistics.

Format

reset engine statistic

Parameters

None

Views

User view

Level

3: Management level

Usage Guidelines

None

Example

Clear engine statistics.

```
<Huawei> reset engine statistic
```

19.9.4.16 reset fragment-reassemble statistic

Function

The **reset fragment-reassemble statistic** command clears statistics on fragment reassembly.

Format

reset fragment-reassemble statistic

Parameters

None

Views

User view

Level

3: Management level

Usage Guidelines

None

Example

Clear statistics on fragment reassembly.

```
<Huawei> reset fragment-reassemble statistic
```

19.9.4.17 stream-reassemble enable

Function

The **stream-reassemble enable** command enables TCP stream reassembly.

The **undo stream-reassemble enable** command disables TCP stream reassembly.

 Copyright © Huawei Technologies Co., Ltd.

Format

stream-reassemble enable

undo stream-reassemble enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, TCP stream reassembly is enabled.

If TCP stream reassembly is disabled, TCP packets will not be reassembled and will not be inspected. In addition, security inspections based on TCP streams may also fail.

Example

Enable TCP stream reassembly.

```
<Huawei> system-view
[Huawei] stream-reassemble enable
```

19.9.4.18 stream-reassemble enhanced-mode

Function

The **stream-reassemble enhanced-mode** command enables the enhanced traffic reassembly mode.

The **undo stream-reassemble enhanced-mode** command disables the enhanced traffic reassembly mode.

Format

stream-reassemble enhanced-mode

undo stream-reassemble enhanced-mode

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the enhanced traffic reassembly mode is disabled.

The command is used to enable the enhanced traffic reassembly mode in the bypass deployment scenario. After this mode is enabled, sequence number reassembly is supported when TCP data packets and three-way handshake packets are out of order.

Example

Enable the enhanced traffic reassembly mode.

```
<Huawei> system-view
[Huawei] stream-reassemble enhanced-mode
```

19.9.4.19 stream-reassemble overflow-mode

Function

The **stream-reassemble overflow-mode** command configures the action for cache overflow during TCP stream reassembly.

The **undo stream-reassemble overflow-mode** command restores the default action for cache overflow during TCP stream reassembly.

The default action for cache overflow during TCP stream reassembly is **discard**.

Format

stream-reassemble overflow-mode { **discard** | **forward** }

undo stream-reassemble overflow-mode

Parameters

Parameter	Description	Value
discard	Discards the packets that overflow the cache.	-
forward	Forwards the fragments that overflow the cache.	-

Views

System view

Level

2: Configuration level

Usage Guidelines

None

Example

Set the action for cache overflow during TCP stream reassembly to **forward**.

```
<Huawei> system-view
[Huawei] stream-reassemble overflow-mode forward
```

19.9.4.20 stream-reassemble overlap-mode

Function

The **stream-reassemble overlap-mode** command configures the action for overlapping packets during TCP stream reassembly.

The **undo stream-reassemble overlap-mode** command restores the default action for overlapping packets during TCP stream reassembly.

The default action for the overlapping packets during TCP stream reassembly is **preserve**.

Format

stream-reassemble overlap-mode { **preserve** | **overwrite** }

undo stream-reassemble overlap-mode

Parameters

Parameter	Description	Value
preserve	Preserves overlapping packets.	-
overwrite	Overwrites overlapping packets.	-

Views

System view

Level

2: Configuration level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the action for the overlapping packets during TCP stream reassembly to **overwrite**.

```
<Huawei> system-view
[Huawei] stream-reassemble overlap-mode overwrite
```

19.9.4.21 stream-reassemble session-cache

Function

The **stream-reassemble session-cache** command configures the maximum cache for a session during TCP stream reassembly.

The **undo stream-reassemble session-cache** command restores the maximum cache for a session to the default value during TCP stream reassembly.

By default, the maximum cache for a session during TCP stream reassembly is 32 KB.

Format

stream-reassemble session-cache *session-cache-value*

undo stream-reassemble session-cache

Parameters

Parameter	Description	Value
session-cache-value	Specifies the maximum cache for a session.	The value is an integer ranging from 1 to 32, in KB.

Views

System view

Level

2: Configuration level

Usage Guidelines

None

Example

Set the maximum cache for a session to 16 KB during TCP stream reassembly.

```
<Huawei> system-view
[Huawei] stream-reassemble session-cache 16
```

 Copyright © Huawei Technologies Co., Ltd.

19.9.4.22 stream-reassemble session-timeout

Function

The **stream-reassemble session-timeout** command set the timeout time for out-of-sequence TCP packet inspection.

The **undo stream-reassemble session-timeout** command restores the default setting.

Format

stream-reassemble session-timeout *session-timeout-value*

undo stream-reassemble session-timeout

Parameters

Parameter	Description	Value
session-timeout-value	Specifies the timeout time.	The value is an integer ranging from 0 to 1200, in seconds. The default value is 10.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, out-of-sequence TCP packet inspection is enabled on the Router.

When *session-timeout-value* is 0, out-of-sequence TCP packet inspection is disabled.

When *session-timeout-value* is greater than 0 and the time when TCP packets are out of order is smaller than or equal to *session-timeout-value*, the Router will attempt to reassemble traffic. If the time when TCP packets are out of order is greater than *session-timeout-value*, the IAE does not detect the content of traffic and ensures traffic transmission preferentially.

Example

Set the timeout time for out-of-sequence TCP packet inspection to 20s.

```
<Huawei> system-view
[Huawei] stream-reassemble session-timeout 20
```

19.9.4.23 stream-reassemble tcp-option check

Function

The **stream-reassemble tcp-option check** command enables the TCP option check function.

The **undo stream-reassemble tcp-option check** command disables the TCP option check function.

Format

stream-reassemble tcp-option check

undo stream-reassemble tcp-option check

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

By default, the TCP option check function is disabled.

After this function is enabled, the engine directly discards packets with abnormal TCP options.

Example

Enable the TCP option check function.

```
<Huawei> system-view
[Huawei] stream-reassemble tcp-option check
```

19.9.4.24 stream-reassemble timestamp check

Function

The **stream-reassemble timestamp check** command enables timestamp check of TCP flow reassembly.

The **undo stream-reassemble timestamp check** command disables timestamp check of TCP flow reassembly.

Format

stream-reassemble timestamp check

undo stream-reassemble timestamp check

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you enable timestamp check of TCP flow reassembly, the device verifies the timestamp option of TCP packets. If the option is incorrect, the device discards the packets.

The timestamp check function is disabled by default.

Example

Enable timestamp check of TCP flow reassembly.

```
<Huawei> system-view
[Huawei] stream-reassemble timestamp check
```

19.9.4.25 stream-reassemble user-configure defense-check

Function

The **stream-reassemble user-configure defense-check** command enables the TCP attack defense function.

The **undo stream-reassemble user-configure defense-check** command disables the TCP attack defense function.

Format

stream-reassemble user-configure defense-check

undo stream-reassemble user-configure defense-check

Parameters

None

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

By default, the TCP attack defense function is disabled.

After this function is enabled, the Router directly discards abnormal TCP packets.

Example

Enable the TCP attack defense function.

```
<Huawei> system-view
[Huawei] stream-reassemble user-configure defense-check
```

19.10 Local Attack Defense Configuration Commands

19.10.1 application-apperceive

Function

The **application-apperceive** command sets the rate limit for Secure Shell (SSH), Telecommunication Network Protocol (Telnet), Secure Shell Version 6 (SSHv6), Telecommunication Network Protocol Version 6 (Telnetv6), Hypertext Transfer Protocol (HTTP), Border Gateway Protocol (BGP), Internet Key Exchange (IKE), or File Transfer Protocol (FTP) packets after active link protection (ALP) is enabled.

The **undo application-apperceive** command restores the default rate limit for SSH, Telnet, SSHv6, Telnetv6, HTTP, BGP, IKE, or FTP packets.

By default, the rate limit for SSH packets, Telnet packets, SSHv6 packets, Telnetv6 packets, HTTP packets, BGP packets is 512 pps, the rate limit for IKE packets is 128 pps, and the rate limit for FTP packets is 1024 pps.

Format

application-apperceive packet-type { **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** } **rate-limit** *rate-value*

undo application-apperceive packet-type { **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** }

NOTE

V200R010C10 and later versions support the **ike** parameter.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-type { **ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike** }	Specifies a packet type. ● **ssh**: Indicates that the protocol type is SSH. ● **telnet**: Indicates that the protocol type is Telnet. ● **sshv6**: Indicates that the protocol type is SSHv6. ● **telnetv6**: Indicates that the protocol type is Telnetv6. ● **bgp**: Indicates that the protocol type is BGP. ● **ftp**: Indicates that the protocol type is FTP. **NOTE** If **ftp** is specified, the rate limit for FTP packets also takes effect for TFTP packets. ● **http**: Indicates that the protocol type is HTTP. ● **ike**: Indicates that the protocol type is IKE.	-
rate-limit *rate-value*	Specifies the rate limit of protocol packets.	The value is an integer that ranges from 64 to 32768, in pps. When applying the value in pps, the device converts it to a value in kbit/s. The conversion formula is *rate-value* pps = *rate-value* x 1500 x 8/1024 kbit/s.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The default rate limit for application protocol packets such as FTP packets is low. To transmit these packets at a higher rate, run the **application-apperceive** command.

Precautions

If you run the **application-apperceive** command with the same protocol type specified in the same attack defense policy view multiple times, only the latest configuration takes effect.

This command takes effect only when active link protection is enabled by the **19.10.10 cpu-defend application-apperceive enable** command.

Example

Set the rate limit for FTP packets in the attack defense policy **mypolicy** to 1260 pps after ALP is enabled.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] application-apperceive packet-type ftp rate-limit 1260
```

Related Topics

19.10.11 cpu-defend policy

19.10.10 cpu-defend application-apperceive enable

19.10.17 display cpu-defend configuration

19.10.2 auto-defend enable

Function

The **auto-defend enable** command enables automatic attack source tracing.

The **undo auto-defend enable** command disables automatic attack source tracing.

By default, attack source tracing is disabled.

Format

auto-defend enable

undo auto-defend enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of attack packets may attack the device CPU. Attack source tracing enables the device to trace attack sources and send logs or alarms to notify the administrator so that the administrator can take measures to defend against the attacks. By default, logs are sent to notify the administrator if attack source tracing is enabled.

After automatic attack source tracing is enabled, the device traces the source of the specified packets sent to the CPU. The packet type can be set using the **19.10.6 auto-defend protocol** command.

Precautions

Attack source tracing configured in an attack defense policy takes effect only when the attack defense policy is applied in the system view.

Example

Enable attack source tracing in the attack defense policy named **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
```

Related Topics

19.10.11 cpu-defend policy

19.10.3 auto-defend action

Function

The **auto-defend action** command configures the device to discard packets sent from attack sources.

The **undo auto-defend action** command configures the device not to discard packets sent from attack sources.

By default, the device does not discard packets sent from attack sources.

Format

auto-defend action deny [**timer** *time-length*]

undo auto-defend action

Parameters

Parameter	Description	Value
deny	Configures the device to discard packets sent from an attack source.	-
timer *time-length*	Specifies the duration in which the device discards packets sent from an attack source.	The value is an integer that ranges from 5 to 86400, in seconds.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The **auto-defend action** command is applied to taking attack source **punish** actions. The device discards the packets sent from the identified source.

The **auto-defend action** command configures the device to punish attack sources. When the device detects an attacker, it discards packets sent from the attack source. This protects the device against attacks.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

The device takes **punish** actions on an attack source during the duration specified by **timer** *time-length*. When the duration expires, the device stops discarding packets sent from this attack source. If the attack source continues attacking the device, the device starts to discard packets sent from this attack source again.

Example

Configure the device to discard packets sent from an attack source, and set the duration to 20000 seconds.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] auto-defend enable
[Huawei-cpu-defend-policy-mypolicy] auto-defend action deny timer 20000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.10.11 cpu-defend policy
19.10.2 auto-defend enable

19.10.4 auto-defend alarm enable

Function

The **auto-defend alarm enable** command enables the event reporting function for attack source tracing.

The **undo auto-defend alarm enable** command disables the event reporting function for attack source tracing.

By default, the event reporting function for attack source tracing is disabled.

Format

auto-defend alarm enable

undo auto-defend alarm enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of packets of a specified protocol from an attack source exceeds the threshold in a specified period, the device reports an event to the administrator so that the administrator can take measures to protect the device.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Follow-up Procedure

Run the **auto-defend alarm threshold** command to set the event reporting threshold for attack source tracing.

Example

Enable the event reporting function in the attack defense policy **test**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] auto-defend alarm enable
```

Related Topics

19.10.11 cpu-defend policy

19.10.2 auto-defend enable

19.10.5 auto-defend alarm threshold

19.10.5 auto-defend alarm threshold

Function

The **auto-defend alarm threshold** command sets the event reporting threshold for attack source tracing.

The **undo auto-defend alarm threshold** command restores the default event reporting threshold for attack source tracing.

By default, the event reporting threshold for attack source tracing is 128 pps.

Format

auto-defend alarm threshold *threshold*

undo auto-defend alarm threshold

Parameters

Parameter	Description	Value
threshold	Specifies the event reporting threshold for attack source tracing.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the number of packets of a specified protocol from an attack source exceeds the threshold in a specified period, the device reports an event to the administrator so that the administrator can take measures to protect the device.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command, and the alarm source tracing function has been enabled using the **auto-defend alarm enable** command.

Precautions

If you run the **auto-defend alarm threshold** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

Example

Set the event reporting threshold for attack source tracing in the attack defense policy named **test** to 300 pps.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] auto-defend alarm enable
[Huawei-cpu-defend-policy-test] auto-defend alarm threshold 300
```

Related Topics

19.10.11 cpu-defend policy

19.10.2 auto-defend enable

19.10.4 auto-defend alarm enable

19.10.6 auto-defend protocol

Function

The **auto-defend protocol** command specifies the types of protocol packets that the device monitors in attack source tracing.

The **undo auto-defend protocol** command deletes specified types of protocol packets that the device monitors in attack source tracing.

By default, the device traces sources of ARP, DHCP, ICMP, IGMP, OSPF, Telnet, TCP, and TTL-expired packets in attack source tracing.

Format

auto-defend protocol { **all** | { **arp** | **dhcp** | **icmp** | **igmp** | **ospf** | **tcp** | **telnet** | **ttl-expired** } * }

undo auto-defend protocol { **arp** | **dhcp** | **icmp** | **igmp** | **ospf** | **tcp** | **telnet** | **ttl-expired** } *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
all	Configures the device to trace sources of ARP, DHCP, ICMP, IGMP, OSPF, Telnet, TCP, and TTL-expired packets in attack source tracing.	-
arp	Adds Address Resolution Protocol (ARP) packets to the list of traced packets or deletes ARP packets from the list.	-
dhcp	Adds Dynamic Host Configuration Protocol (DHCP) packets to the list of traced packets or deletes DHCP packets from the list.	-
icmp	Adds Internet Control Message Protocol (ICMP) packets to the list of traced packets or deletes ICMP packets from the list.	-
igmp	Adds Internet Group Management Protocol (IGMP) packets to the list of traced packets or deletes IGMP packets from the list.	-
ospf	Adds Open Shortest Path First (OSPF) packets to the list of traced packets or deletes OSPF packets from the list.	-
tcp	Adds Transmission Control Protocol (TCP) packets to the list of traced packets or deletes TCP packets from the list.	-
telnet	Adds Telnet packets to the list of traced packets or deletes Telnet packets from the list.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ttl-expired	Adds packets with the TTL value of 1 to the list of traced packets or deletes these packets from the list.	-

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The attack source tracing process consists of four phases: packet parsing, traffic analysis, attack source identification, and taking attack source **punish** actions. The **auto-defend protocol** command is applied to the packet parsing phase. When an attack occurs, you cannot identify the type of attack packets. The **auto-defend protocol** command allows you to flexibly specify the types of traced packets.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend protocol** command multiple times, multiple packet types are specified.

If a packet type is specified, when the device is attacked and the attack source is traced, you can run the **display auto-defend attack-source** command to view attack source information.

Example

Delete IGMP and TTL-expired packets from the list of traced packets.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] undo auto-defend protocol igmp ttl-expired
```

Related Topics

19.10.2 auto-defend enable
19.10.11 cpu-defend policy
19.10.15 display auto-defend attack-source

19.10.7 auto-defend threshold

Function

The **auto-defend threshold** command sets the checking threshold for attack source tracing.

The **undo auto-defend threshold** command restores the default checking threshold for attack source tracing.

By default, the checking threshold for attack source tracing is 128 pps.

Format

auto-defend threshold *threshold*

undo auto-defend threshold

Parameters

Parameter	Description	Value
threshold	Specifies the checking threshold for attack source tracing.	The value is an integer that ranges from 1 to 65535, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After attack source tracing is enabled, you can set the checking threshold for attack source tracing. When the number of sent protocol packets from an attack source in a specified period exceeds the checking threshold, the device traces and logs the attack source.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend threshold** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

After the **auto-defend enable** command is executed, the device traces the attack source based on the default threshold and logs the attack source even if the **auto-defend threshold** command is not used.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the checking threshold for attack source tracing in the attack defense policy named **test** to 200 pps.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] auto-defend threshold 200
```

Related Topics

19.10.11 cpu-defend policy
19.10.2 auto-defend enable

19.10.8 auto-defend trace-type

Function

The **auto-defend trace-type** command configures an attack source tracing mode.

The **undo auto-defend trace-type** command deletes an attack source tracing mode.

By default, attack source tracing is based on source MAC addresses, source IP addresses, and source ports+VLANs.

Format

auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

undo auto-defend trace-type { **source-mac** | **source-ip** | **source-portvlan** } *

Parameters

Parameter	Description	Value
source-mac	Configures attack source tracing based on source MAC addresses so that the device classifies and collects statistics based on the source MAC address and identifies the attack source.	-
source-ip	Configures attack source tracing based on source IP addresses so that the device classifies and collects statistics based on the source IP address and identifies the attack source.	-
source-portvlan	Configures attack source tracing based on source ports +VLANs so that the device classifies and collects statistics based on the source port and VLAN and identifies the attack source.	-

Views

Attack defense policy view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After enabling attack source tracing, you can specify one or more attack source tracing modes. The device then uses the specified modes to trace attack sources.

The device supports the following attack source tracing modes:

- Source IP address-based tracing: defends against Layer 3 attack packets.
- Source MAC address-based tracing: defends against Layer 2 attack packets with a fixed source MAC address.
- Source port+VLAN based tracing: defends against Layer 2 attack packets with different source MAC addresses.

Prerequisites

Attack source tracing has been enabled using the **auto-defend enable** command.

Precautions

If you run the **auto-defend trace-type** command multiple times, multiple attack source tracing modes are specified.

After the attack source tracing function is enabled on the device, you can run the **display auto-defend attack-source** command to view attack source tracing information if an attack occurs.

By default, the device traces attack sources based on source MAC addresses, source IP addresses, and source ports+VLANs. To cancel an attack source tracing mode, run the **undo auto-defend trace-type** command.

Example

Configure attack source tracing based on source MAC addresses.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] auto-defend enable
[Huawei-cpu-defend-policy-test] undo auto-defend trace-type source-ip source-portvlan
```

Related Topics

19.10.11 cpu-defend policy
19.10.15 display auto-defend attack-source

19.10.9 blacklist

Function

The **blacklist** command configures a blacklist.

The **undo blacklist** command deletes a blacklist.

By default, no blacklist is configured.

Format

blacklist *blacklist-id* **acl** *acl-number*

undo blacklist *blacklist-id*

Parameters

Parameter	Description	Value
blacklist-id	Specifies the ID of a blacklist.	The value is an integer that ranges from 1 to 8.
acl *acl-number*	Specifies the number of an Access Control List (ACL) referenced by a blacklist.	The value is an integer that ranges from 2000 to 4999. ● 2000 to 2999: basic ACLs ● 3000 to 3999: advanced ACLs ● 4000 to 4999: Layer 2 ACLs

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To defend against malicious packet attacks, the device uses ACLs to add users with the specific characteristic into a blacklist and discards the packets from the users in the blacklist.

A maximum of 8 blacklists can be configured in an attack defense policy on the device.

Precautions

If multiple blacklists need to be configured in an attack defense policy: Layer 2 ACLs and basic ACLs cannot be used together in these blacklists. Layer 2 ACLs and advanced ACLs cannot be used together in these blacklists. Basic ACLs, advanced ACLs, and Layer 2 ACLs cannot be used together in these blacklists. For example:

- For example, three blacklists are configured in the attack defense policy **mypolicyA**: blacklist1, blacklist2, and blacklist3. If blacklist1 uses a basic ACL,

blacklist2 and blacklist3 can use only basic ACLs or advanced ACLs but not Layer 2 ACLs.

- For example, three blacklists are configured in the attack defense policy **mypolicyB**: blacklist1, blacklist2, and blacklist3. If blacklist1 uses a Layer 2 ACL, blacklist2 and blacklist3 can use only Layer 2 ACLs.

Example

Specify ACL 2001 as the rule of blacklist 2.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] blacklist 2 acl 2001
```

Related Topics

19.7.4 acl (system view)

19.10.11 cpu-defend policy

19.10.10 cpu-defend application-apperceive enable

Function

The **cpu-defend application-apperceive enable** command enables active link protection (ALP).

The **undo cpu-defend application-apperceive enable** command disables ALP.

By default, ALP is enabled for SSH, Telnet, SSHv6, Telnetv6, FTP, BGP, IKE, and HTTP.

Format

cpu-defend application-apperceive [**ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike**] **enable**

undo cpu-defend application-apperceive [**ssh** | **telnet** | **sshv6** | **telnetv6** | **bgp** | **ftp** | **http** | **ike**] **enable**

NOTE

V200R010C10 and later versions support the **ike** parameter.

Parameters

Parameter	Description	Value
ssh	Indicates that the protocol type is SSH.	-
telnet	Indicates that the protocol type is Telnet.	-
sshv6	Indicates that the protocol type is SSHv6.	-

Parameter	Description	Value
telnetv6	Indicates that the protocol type is Telnetv6.	-
bgp	Indicates that the protocol type is BGP.	-
ftp	Indicates that the protocol type is FTP. **NOTE** If **ftp** is specified, ALP for FTP packets also takes effect for TFTP packets.	-
http	Indicates that the protocol type is HTTP.	-
ike	Indicates that the protocol type is IKE.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

ALP protects session-based application layer data, including data of SSH sessions, Telnet sessions, SSHv6 sessions, Telnetv6 sessions, HTTP sessions, FTP sessions, IKE sessions, and BGP sessions to ensure uninterrupted services when attacks occur.

- When the device communicates with another host or device using FTP, burst traffic of FTP packets occurs. As a result, burst traffic is discarded because it exceeds the rate limit after ALP is enabled on the device or services are interrupted because other FTP packets attack the device.
- When the device attempts to establish a BGP, an HTTP, a SSH, a Telnet, a SSHv6, or a Telnetv6 connection with another host or device, burst traffic of BGP, HTTP, SSH, Telnet, SSHv6, or Telnetv6 packets occurs. As a result, burst traffic is discarded because it exceeds the rate limit after ALP is enabled on the device or a BGP, an HTTP, a SSH, a Telnet, a SSHv6, or a Telnetv6 connection fails to be established because other BGP, HTTP, SSH, Telnet, SSHv6, or Telnetv6 packets attack the device.

When the device detects setup of SSH sessions, Telnet sessions, SSHv6 Session, Telnetv6 Session, HTTP sessions, FTP sessions, IKE sessions, and BGP sessions, ALP is enabled to protect the session. The packets matching characteristics of the session are sent at a high rate; therefore, reliability and stability of session-related services are ensured.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Run the **cpu-defend-policy** command on an LPU to apply the attack defense policy. Then the device protects data flows using the rate limit specified in the active link protection function.

Example

Enable ALP so that the rate limit after ALP is enabled in the attack defense policy **mypolicy** on the main control board takes effect.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] application-apperceive packet-type ftp rate-limit 12600
[Huawei-cpu-defend-policy-mypolicy] quit
[Huawei] cpu-defend application-apperceive enable
[Huawei] cpu-defend-policy mypolicy
```

Related Topics

19.10.11 cpu-defend policy

19.10.17 display cpu-defend configuration

19.10.1 application-apperceive

19.10.11 cpu-defend policy

Function

The **cpu-defend policy** command creates an attack defense policy and displays the attack defense policy view.

The **undo cpu-defend policy** command deletes an attack defense policy.

By default, the **default** attack defense policy exists on the device and is applied to all boards. The **default** attack defense policy cannot be deleted or modified.

Format

cpu-defend policy *policy-name*

undo cpu-defend policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A large number of packets including malicious attack packets are sent to the CPU on a network. If excess packets are sent to the CPU, the CPU usage becomes high and CPU performance deteriorates. The attack packets affect services and may even cause system breakdown. To solve the problem, create an attack defense policy and configure CPU attack defense and attack source tracing in the attack defense policy.

Precautions

The device supports a maximum of 19 attack defense policies, including the **default** attack defense policy. The **default** attack defense policy is generated in the system by default and is applied to all boards. The **default** attack defense policy cannot be deleted or modified. The other 18 policies can be created, modified, and deleted.

The configuration in a user-defined attack defense policy overrides the configuration in the **default** attack defense policy. If no parameter is set in the user-defined attack defense policy, the configuration in the **default** attack defense policy is used.

Example

Create an attack defense policy named **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test]
```

Related Topics

19.10.18 display cpu-defend policy

19.10.12 cpu-defend-policy

Function

The **cpu-defend-policy** command applies an attack defense policy.

The **undo cpu-defend-policy** command cancels the application of an attack defense policy.

By default, the **default** attack defense policy is applied to all cards.

Format

cpu-defend-policy *policy-name* [**global** | **slot** *slot-id*]

undo cpu-defend-policy [**global** | **slot** *slot-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an attack defense policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.
global	Indicates that the attack defense policy is applied globally. If **global** is specified, the attack defense policy is applied to all interface cards.	-
slot *slot-id*	Indicates that the attack defense policy is applied locally. *slot-id* specifies the slot ID of the LPU. If **slot** is specified, the attack defense policy is applied to specified interface cards. **NOTE** If either **global** or **slot** is specified, the attack defense policy is applied on the main control board.	Set *slot-id* according to the device configuration.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An attack defense policy takes effect only when it is applied to a board and only one attack defense policy can be applied to a board.

Prerequisites

An attack defense policy has been created by using the **19.10.11 cpu-defend policy** command.

Precautions

If an attack defense policy has been applied to an LPU in a specified slot, you must run the **undo cpu-defend-policy slot** *slot-id* command to unbind the attack

defense policy from the LPU so that you can run the **cpu-defend-policy** *policy-name* **global** command to apply the attack defense policy to all LPUs.

Example

Apply the attack defense policy named **test** to the main control board.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] quit
[Huawei] cpu-defend-policy test
```

Apply the attack defense policy named **test** to all cards.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] quit
[Huawei] cpu-defend-policy test global
```

Related Topics

19.10.11 cpu-defend policy

19.10.13 deny

Function

The **deny** command configures the device to discard packets sent to the CPU.

The **undo deny** command restores the default action taken for the packets sent to the CPU.

By default, the device does not discard packets sent to the CPU. Instead, the device limits the rate of packets sent to the CPU using the default rate. You can check the rate limit of each type of packets using the **display cpu-defend configuration** command.

Format

deny packet-type *packet-type*

undo deny packet-type *packet-type*

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the type of the packet to be discarded.	The supported packet type depends on the device.

Views

Attack defense policy view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After an attack defense policy is created, if the device receives attack packets of a specified type or a large number of packets sent to the CPU, run the **deny** command to configure the device to discard packets of the specified type sent to the CPU.

Precautions

After the **deny** command is executed, the **packet-type** command cannot take effect. After the **undo deny** command is executed, you can run the **packet-type** command to set the rate limit for the packets sent to the CPU.

Example

Configure the drop action taken for ARP Reply packets to be sent to the CPU in the attack defense policy **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] deny packet-type arp-reply
```

Related Topics

19.10.11 cpu-defend policy

19.10.18 display cpu-defend policy

19.10.21 packet-type

19.10.14 description (attack defense policy view)

Function

The **description** command configures the description of an attack defense policy.

The **undo description** command deletes the description of an attack defense policy.

By default, no description is configured for an attack defense policy.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the content of a description.	It is a string of 1 to 63 case-sensitive characters with spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **description** command configures the description of an attack defense policy, for example, the usage or application scenario of the attack defense policy. The description is used to differentiate attack defense policies.

Precautions

If you run the **description** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

Example

Configure the description **defend_arp_attack** for the attack defense policy named **test**.

```
<Huawei> system-view
[Huawei] cpu-defend policy test
[Huawei-cpu-defend-policy-test] description defend_arp_attack
```

Related Topics

19.10.11 cpu-defend policy

19.10.15 display auto-defend attack-source

Function

The **display auto-defend attack-source** command displays the attack sources on the SRU.

Format

display auto-defend attack-source [**detail**]

Parameters

Parameter	Description	Value
detail	Displays detailed information about the attack sources on the SRU, including the type of attack packets. If **detail** is not specified, brief information about the attack sources on the SRU is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display auto-defend attack-source** command displays the attack source list.

Example

Display the attack source list on the SRU.

```
<Huawei> display auto-defend attack-source
  Attack Source User Table:
  ---------------------------------------------------------------------------
     MacAddress       InterfaceName       Vlan:Outer/Inner       TOTAL
  ---------------------------------------------------------------------------
  0000-0000-0023       Ethernet2/0/0          199/299             1264
  ---------------------------------------------------------------------------
  Total: 1

  Attack Source Port Table:
  -------------------------------------------------------
    InterfaceName        Vlan:Outer/Inner        TOTAL
  -------------------------------------------------------
  Ethernet2/0/0               199/299             1264
  -------------------------------------------------------
  Total: 1

  Attack Source IP Table:
  --------------------------------------
  IPAddress         TOTAL Packets
  --------------------------------------
  10.105.105.2     256
  --------------------------------------
  Total: 1
```

Display detailed information about the attack source list.

```
<Huawei> display auto-defend attack-source detail
 Attack Source User Table:
```

```
-----------------------------------------------------
MAC Address                 0000-0000-0023
Interface                 Ethernet2/0/0
VLAN: Outer/Inner           199/299
    ARP:                  256
Total                     256
-----------------------------------------------------
Total: 1

Attack Source Port Table:
-----------------------------------------------------
  InterfaceName       Vlan:Outer/Inner       TOTAL
-----------------------------------------------------
Ethernet2/0/0           199/299            256
-----------------------------------------------------
Total: 1

Attack Source IP Table:
-----------------------------------------------------
IP address                  10.105.105.2
    ARP:                  256
Total                     256
-----------------------------------------------------
Total: 1
```

Table 19-133 Description of the **display auto-defend attack-source** command output

Item	Description
Attack Source User Table	Information about attack sources on the SRU, which is distinguished according to the attack user.
Attack Source Port Table	Information about attack sources on the SRU. The attack source information is distinguished according to the attacked interface.
Attack Source IP Table	Information about attack sources on the SRU. The attack source information is distinguished according to the attacked interface.
MacAddress	MAC address of the user.
InterfaceName	Interface name.
Vlan:Outer/Inner	ID of the VLAN that an interface belongs to. **Outer** indicates the outer VLAN ID and **Inner** indicates the inner VLAN ID.
TOTAL	Total number of packets.
IPAddress	IP address of a user.
TOTAL Packets	Total number of packets.

Related Topics

19.10.11 cpu-defend policy
19.10.2 auto-defend enable

19.10.16 display auto-defend configuration

Function

The **display auto-defend configuration** command displays the attack source tracing configuration.

Format

display auto-defend configuration [**cpu-defend policy** *policy-name*]

Parameters

Parameter	Description	Value
cpu-defend policy *policy-name*	Displays the attack source tracing configuration of a specified attack defense policy. ● If this parameter is specified, the configuration of the specified attack defense policy is displayed. ● If this parameter is not specified, the configurations of all attack defense policies are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After attack source tracing is configured in an attack defense policy, you can run the **display auto-defend configuration** command to view the attack source tracing configuration.

Example

Display the configurations of all attack defense policies.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display auto-defend configuration
-----------------------------------------------------------------------
Name  : mypolicy
Related slot : <0>
auto-defend                : enable
auto-defend threshold      : 200 (pps)
auto-defend alarm          : enable
auto-defend alarm threshold : 2000 (pps)
-----------------------------------------------------------------------
Name  : mypolicy1
Related slot : <>
auto-defend                : enable
auto-defend threshold      : 128 (pps)
-----------------------------------------------------------------------
```

Table 19-134 Description of the display auto-defend configuration command output

Item	Description
Name	Name of an attack defense policy.
Related slot	ID of the slot to which the attack defense policy is applied.
auto-defend	Whether attack source tracing is enabled. To enable attack source tracing, run the **19.10.2 auto-defend enable** command.
auto-defend threshold	Checking threshold for attack source tracing. To set the checking threshold for attack source tracing, run the **19.10.7 auto-defend threshold** command.
auto-defend alarm	Whether the alarm function for attack source tracing is enabled. To enable the alarm function for attack source tracing, run the **19.10.4 auto-defend alarm enable** command.
auto-defend alarm threshold	Alarm threshold for attack source tracing. To set the alarm threshold for attack source tracing, run the **19.10.5 auto-defend alarm threshold** command.

Related Topics

19.10.11 cpu-defend policy
19.10.3 auto-defend action
19.10.4 auto-defend alarm enable
19.10.5 auto-defend alarm threshold
19.10.2 auto-defend enable
19.10.6 auto-defend protocol
19.10.8 auto-defend trace-type
19.10.7 auto-defend threshold

 Copyright © Huawei Technologies Co., Ltd.

19.10.17 display cpu-defend configuration

Function

The **display cpu-defend configuration** command displays rate limits for protocol packets.

Format

display cpu-defend configuration [**packet-type** *packet-type*] { **all** | **slot** *slot-id* | **sru** }

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies a packet type.	The supported packet type depends on the device.
all	Indicates all boards, including main control boards and LPUs.	-
slot *slot-id*	Specifies a slot ID.	The value must be set according to the device configuration.
sru	Indicates the main control board. If **sru** is specified, the rate limit configuration on the SRU is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display cpu-defend configuration** command to view the rate limit of protocol packets sent to the CPU. By default, the rate limit of protocol packets in the **default** policy is displayed.

Example

Display rate limit configuration about protocol packets sent to the SRU.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display cpu-defend configuration sru
Rate configurations on main board.
-----------------------------------------------------------------
Packet-type          Status       Rate-limit(PPS)  Priority
-----------------------------------------------------------------
8021X                Disabled       160              2
arp-miss             Enabled         64              2
arp-reply            Enabled        128              2
arp-request            Enabled        128              2
bfd                  Disabled       512              4
bgp                  Enabled        256              3
......
-----------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 19-135 Description of the **display cpu-defend configuration** command output

Item	Description
Packet-type	Packet type.
Status	Protocol packet status.
Rate-limit(PPS)	Rate limit for packets, in pps. To set the rate limit for packets, run the **19.10.21 packet-type** command.
Priority	Priority of the protocol type. To set the priority of the protocol type, run the **19.10.22 packet-type priority** command.

19.10.18 display cpu-defend policy

Function

The **display cpu-defend policy** command displays the attack defense policy configuration.

Format

display cpu-defend policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Displays the configuration of a specified attack defense policy. ● If *policy-name* is specified, information about the specified attack defense policy is displayed. ● If *policy-name* is not specified, information about all attack defense policies is displayed.	The attack defense policy must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After an attack defense policy is created, you can run the **display cpu-defend policy** command to view the board that the attack defense policy is applied to and configurations of the attack defense policy.

Example

Display information about the attack defense policy named **mypolicy**.

```
<Huawei> display cpu-defend policy mypolicy
 Related slot : <0>
 BlackList Status :
   Slot<0> : Success
 Configuration :
   Blacklist 1 ACL number : 2001
   Packet-type arp-reply rate-limit : 1260(pps)
   Packet-type arp-reply priority : 3
   Rate-limit all-packets : 12600(pps)
   Dynamic Rate-limit all-packets : 0(pps)
   Application-apperceive packet-type ftp : 1260(pps)
   Application-apperceive packet-type tftp : 1260(pps)
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-136 Description of the display cpu-defend policy command output

Item	Description
Related slot	Board to which the attack defense policy is applied.
BlackList Status	Status of a blacklist.
Slot<0> : Success	A blacklist is successfully configured on the LPU in slot 0.
Blacklist 1 ACL number	Number of an ACL defined in blacklist 1. To configure a blacklist, run the **blacklist** command.
Packet-type arp-reply rate-limit	Rate limit for ARP Reply packets. To set the rate limit for ARP Reply packets, run the **packet-type** command.
Packet-type arp-reply priority	Priority of ARP Reply packets. To set the priority of ARP Reply packets, run the **packet-type priority** command.
Rate-limit all-packets	Rate limit for all packets sent to the CPU. To set the rate limit for all packets sent to the CPU, run the **rate-limit all-packets** command.
Dynamic Rate-limit all-packets	Dynamic rate limit for all packets sent to the CPU.
Application-apperceive packet-type ftp	Rate limit for FTP packets after ALP is enabled. To set the rate limit for FTP packets after ALP is enabled, run the **application-apperceive** command.
Application-apperceive packet-type tftp	Rate limit for TFTP packets after ALP is enabled.

Related Topics

19.10.9 blacklist
19.10.10 cpu-defend application-apperceive enable
19.10.11 cpu-defend policy
19.10.13 deny
19.10.14 description (attack defense policy view)

19.10.19 display cpu-defend rate-adaption statistics

Function

The **display cpu-defend rate-adaption statistics** command displays packet statistics after CPCAR values are dynamically adjusted.

Format

display cpu-defend rate-adaption statistics [**packet-type** *packet-type*]

Parameters

Parameter	Description	Value
packet-type *packet-type*	Displays statistics on the specified type of protocol packets. ● If *packet-type* is specified, statistics on the specified type of protocol packets are displayed. ● If *packet-type* is not specified, statistics on all protocol packets are displayed.	The supported packet types depend on the device model.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view packet statistics after CPCAR values are dynamically adjusted, run this command. The displayed packet statistics, including protocol types, rate of passed packets, rate of discarded packets, and packet rate limit, help you configure attack defense policies.

Example

Display packet statistics after CPCAR values are dynamically adjusted.

```
<Huawei> display cpu-defend rate-adaption statistics
-------------------------------------------------------------------------------
Packet Type                Pass          Loss       Rate-limit
                         (pps)         (pps)        (pps)
-------------------------------------------------------------------------------
8021X                        0             0          128
arp-miss                     0             0           64
arp-reply                    0             0          128
arp-request                  0             0          128
bfd                          0             0          512
bgp                          0             0          256
......
```

```
-----------------------------------------------------------------------------------------------
```

Table 19-137 Description of the **display cpu-defend rate-adaption statistics** command output

Item	Description
Packet Type	Packet type.
Pass	Rate of passed packets, in pps.
Loss	Rate of discarded packets, in pps.
Rate-limit(PPS)	Packet rate limit, in pps.

19.10.20 display cpu-defend statistics

Function

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU.

Format

display cpu-defend statistics [**packet-type** *packet-type*]

Parameters

Parameter	Description	Value
packet-type *packet-type*	Displays statistics on the specified type of protocol packets. *packet-type* specifies the packet type. ● If *packet-type* is specified, statistics on the specified type of protocol packets are displayed. ● If *packet-type* is not specified, statistics on all protocol packets are displayed.	The supported packet type depends on the device.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display cpu-defend statistics** command displays statistics on packets sent to the CPU, including the number of forwarded and discarded packets. This helps the network administrator configure attack defense policies.

Example

Display the statistics on packets sent to the main control board.

```
<Huawei> display cpu-defend statistics
-----------------------------------------------------------------------
Packet Type              Pass Packets        Drop Packets
-----------------------------------------------------------------------
8021X                          0                  0
arp-miss                       5                  0
arp-reply                   8090                  0
arp-request               1446576             127773
bfd                            0                  0
bgp                            0                  0
bgp4plus                       0                  0
dhcp-client                  879                  0
dhcp-server                    0                  0
dhcpv6-reply                   0                  0
dhcpv6-request                 0                  0
dlsw                           0                  0
dns                            4                  0
fib-hit                        0                  0
fr                             0                  0
ftp-client                     0                  0
ftp-server                     0                  0
fw-dns                         0                  0
fw-ftp                         0                  0
fw-http                        0                  0
fw-rtsp                        0                  0
fw-sip                         0                  0
gre-keepalive                  0                  0
gvrp                           0                  0
hdlc                           0                  0
http-client                    0                  0
http-server                    0                  0
hw-tacacs                      0                  0
icmp                          59                  0
icmpv6                       224                  0
igmp                         539                  0
ip-option                      0                  0
ipsec-ike                      0                  0
ipsec-isa                      0                  0
ipsec-osa                      0                  0
isis                       70252                  0
l2tp                           0                  0
lacp                           0                  0
lldp                           0                  0
ldp                            0                  0
nd                           358                  0
nd-miss                        0                  0
nhrp                           0                  0
ntp                            0                  0
ospf                           0                  0
ospfv3                         0                  0
pim                            0                  0
ppp                            0                  0
pppoe                          0                  0
```

```
radius                    0              0
rip                   11306              0
ripng                  7385              0
snmp                      0              0
ssh-client                0              0
ssh-server                0              0
sslvpn                    0              0
stp                       0              0
tcp                      15              0
telnet-client         81476              0
telnet-server             0              0
ttl-expired               0              0
udp-helper                0              0
unknown-multicast         0              0
unknown-packet        66146              0
voice                     0              0
vrrp                      0              0
-----------------------------------------------------------------
```

NOTE

The preceding information is an example. The displayed packet type depends on the actual situation.

Table 19-138 Description of the **display cpu-defend statistics** command output

Item	Description
Packet Type	Packet type.
Pass Packets	Number of forwarded packets.
Drop Packets	Number of discarded packets.

Related Topics

19.10.30 reset cpu-defend statistics

19.10.21 packet-type

Function

The **packet-type** command sets the rate limit for packets sent to the CPU.

The **undo packet-type** command restores the default rate limit for packets sent to the CPU.

By default, the default rate limit in the **default** attack defense policy is used to limit the packets sent to the CPU.

Format

packet-type *packet-type* **rate-limit** *rate-value*

undo packet-type *packet-type* **rate-limit**

Parameters

Parameter	Description	Value
packet-type	Specifies the protocol type.	The supported packet type depends on the device.
rate-limit *rate-value*	Specifies the rate limit of protocol packets.	The value is an integer that ranges from 1 to 32768, in pps.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, if the device receives attack packets of a specified protocol or a large number of packets sent to the CPU, configure rate limit for the protocol packets in the attack defense policy. The device then limits the rate of these packets to protect the CPU.

By default, the device applies the rate limit defined in the **default** attack defense policy to protocol packets. You can also create an attack defense policy and run the **packet-type** command to set the rate limit of protocol packets. The configured rate limit overrides the default rate limit defined in the **default** attack defense policy.

Prerequisites

An attack defense policy has been created using the **cpu-defend policy** command.

Precautions

If you run the **packet-type** command with the same value of *packet-type* in the same attack defense policy view multiple times, only the latest configuration takes effect.

If the **packet-type** and **deny** commands are executed on the same type of protocol packets, the **deny** command takes effect.

Example

Set the rate limit for ARP Reply packets to 1260 pps in the attack defense policy named **mypolicy**.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] packet-type arp-reply rate-limit 1260
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.10.11 cpu-defend policy
19.10.13 deny
19.10.18 display cpu-defend policy
19.10.17 display cpu-defend configuration

19.10.22 packet-type priority

Function

The **packet-type priority** command sets a priority of protocol packets sent to the CPU.

The **undo packet-type** command restores the default priority for protocol packets sent to the CPU. The default priority is defined in the **default** attack defense policy.

By default, the priority defined in the **default** attack defense policy is used.

Format

packet-type *packet-type* **priority** *priority-level*

undo packet-type *packet-type* **priority**

Parameters

Parameter	Description	Value
packet-type	Sets a priority for packets of a specified protocol.	The supported packet type depends on the device.
priority *priority-level*	Specifies the priority.	The value is an integer that ranges from 1 to 4. A larger value indicates a higher priority.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

After an attack defense policy is created, set priorities of protocol packets in the attack defense policy so that packets with higher priorities are processed first.

By default, the priority of packets of a specified protocol type is set based on the **default** policy.

Precautions

If you run the **packet-type priority** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

You can create an attack defense policy and set the priority of packets of the specified protocol type using the **packet-type priority** command. The configured priority overrides the priority in the **default** policy.

The priority of protocol packets sent to the CPU configured in an attack defense policy takes effect only when the attack defense policy is applied to the main control board.

Example

Set the priority of ARP Reply packets to 3 in the attack defense policy named **mypolicy**.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] packet-type arp-reply priority 3
```

Related Topics

19.10.11 cpu-defend policy
19.10.18 display cpu-defend policy
19.10.17 display cpu-defend configuration

19.10.23 rate-adaption adjust-period

Function

The **rate-adaption adjust-period** command sets the interval for checking the CPU usage.

The **undo rate-adaption adjust-period** command restores the default interval for checking the CPU usage.

By default, the interval for checking CPU usage is 30 seconds.

Format

rate-adaption adjust-period *period-value*

undo rate-adaption adjust-period

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
period-value	Specifies the interval for checking CPU usage.	The value is an integer that ranges from 30 to 180, in seconds.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

If the CPU usage changes frequently, the device frequently adjusts CPCAR values, causing unstable traffic. To avoid this problem, run the **rate-adaption adjust-period** command to adjust the interval for checking CPU usage. Generally, use the default interval.

Example

Set the interval for checking CPU usage to 50 seconds.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption adjust-period 50
```

Related Topics

19.10.11 cpu-defend policy

19.10.24 rate-adaption adjust-step

Function

The **rate-adaption adjust-step** command sets the dynamic CPCAR adjustment step.

The **undo rate-adaption adjust-step** command restores the default dynamic CPCAR adjustment step.

By default, the dynamic CPCAR adjustment step is 20%.

Format

rate-adaption adjust-step *step-value*

undo rate-adaption adjust-step

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
step-value	Specifies the percentage value of dynamic CPCAR adjustment step. For example, if the adjustment step is 30% and the current CPCAR value is 1000 pps, the device reduces the CPCAR value to 700 pps when CPU usage reaches the upper threshold.	The value is an integer that ranges from 1 to 100.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

After dynamic CPCAR adjustment is enabled, the device checks the CPU usage at intervals. When the device detects that the CPU usage exceeds the upper threshold (set by the **rate-adaption cpu-usage threshold** command), and reduces the CPCAR value based on the step set by the **rate-adaption adjust-step** command to reduce CPU usage. Generally, the default step value can be used.

Example

Set the dynamic CPCAR adjustment step to 40%.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption adjust-step 40
```

Related Topics

19.10.11 cpu-defend policy
19.10.25 rate-adaption cpu-usage threshold

19.10.25 rate-adaption cpu-usage threshold

Function

The **rate-adaption cpu-usage threshold** command sets the CPU usage thresholds. When the CPU usage of a device exceeds the upper threshold or falls below the lower threshold, the device adjusts the CPCAR values.

The **undo rate-adaption cpu-usage threshold** command restores the default CPU usage thresholds.

By default, the lower threshold is 65% and the upper threshold is 85%.

 Copyright © Huawei Technologies Co., Ltd.

Format

rate-adaption cpu-usage threshold low *low-value* **high** *high-value*

undo rate-adaption cpu-usage threshold

Parameters

Parameter	Description	Value
low *low-value*	Specifies the lower CPU usage threshold. When the CPU usage of a device falls below the lower threshold, the device sets the CPCAR value to the default value or a manually set value.	The value is an integer that ranges from 1 to 99.
high *high-value*	Specifies the higher CPU usage threshold. When the CPU usage of a device exceeds the upper threshold, the device reduces the CPCAR value based on the step set by the **rate-adaption adjust-step** command.	The value is an integer that ranges from *low-value* +1 to 100. The value of *high-value* must be larger than the value of *low-value*.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

After dynamic CPCAR adjustment is configured, the device checks CPU usage to determine whether an attack occurs. When the CPU usage exceeds the upper threshold, the device reduces the CPCAR value based on the step set by the **rate-adaption adjust-step** command to reduce CPU load. When the CPU usage of a device falls below the lower threshold, the device sets the CPCAR value to the default value or a manually set value.

Example

Set the CPU usage thresholds for dynamic CPCAR adjustment.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption cpu-usage threshold low 40 high 90
```

Related Topics

19.10.11 cpu-defend policy
19.10.24 rate-adaption adjust-step

19.10.26 rate-adaption enable

Function

The **rate-adaption enable** command enables dynamic CPCAR adjustment.

The **undo rate-adaption enable** command disables dynamic CPCAR adjustment.

By default, dynamic CPCAR adjustment is disabled.

Format

rate-adaption enable

undo rate-adaption enable

Parameters

None

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When CPCAR values are manually set, a device cannot immediately control the rate of packets sent to the CPU when undergoing an attack. As a result, the CPU usage exceeds the acceptable range and CPU performance degrades.

After dynamic CPCAR adjustment is configured, the device periodically checks CPU usage, and automatically adjusts CPCAR values of protocol packets when the CPU usage exceeds the specified upper threshold, reducing impact on the CPU.

Precautions

After dynamic CPCAR adjustment is enabled, the CPCAR values set using the **packet-type** command become invalid.

Example

Enable dynamic CPCAR adjustment.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption enable
```

Related Topics

19.10.11 cpu-defend policy
19.10.21 packet-type

19.10.27 rate-adaption exception packet-type

Function

The **rate-adaption exception packet-type** command specifies the types of protocol packets for which the CPCAR values cannot be dynamically adjusted.

The **undo rate-adaption exception packet-type** command cancels the types of protocol packets for which the CPCAR values cannot be dynamically adjusted.

By default, the CPCAR values for all protocol packets are dynamically adjusted.

Format

rate-adaption exception packet-type *packet-type*

undo rate-adaption exception packet-type *packet-type*

Parameters

Parameter	Description	Value
packet-type	Specifies the protocol type.	The supported packet type depends on the device.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent certain protocol packets from being affected by dynamic CPCAR adjustment, for example, Telnet packets, you can run the **rate-adaption exception packet-type** command to specify the protected protocol packets. After this command is executed, dynamic CPCAR adjustment does not take effect for the protected protocol packets and you can specify rate limits for these packets by using the **packet-type** command.

Precautions

A maximum of eight types of protected protocol packets can be specified.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the types of protocol packets for which the CPCAR values cannot be dynamically adjusted.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-adaption exception packet-type icmp
```

Related Topics

19.10.11 cpu-defend policy

19.10.21 packet-type

19.10.28 rate-limit all-packets

Function

The **rate-limit all-packets** command sets the rate limit for all packets sent to the CPU.

The **undo rate-limit all-packets** command restores the default rate limit for all packets sent to the CPU.

By default, the rate limit for all packets sent to the CPU is as follows:

- AR100&AR120&AR150&AR160&AR200 series: 1000pps
- AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, and AR2204: 1000pps
- AR2220, AR2240C: 1500pps
- AR2204XE, and AR2204XE-DC: 2000pps
- For the AR2240 and AR3260, the rate limit for all packets sent to the CPU depending on different SRUs.
  - SRU40: 1500pps
  - SRU80 and SRU100E: 2000pps
  - SRU200, SRU200E, and SRU400: 2500pps
- AR3600: 2500pps

Format

rate-limit all-packets pps *pps-value*

undo rate-limit all-packets pps

Parameters

Parameter	Description	Value
pps *pps-value*	Specifies the rate limit for all packets sent to the CPU.	The value is an integer that ranges from 500 to 65535, in pps.

 Copyright © Huawei Technologies Co., Ltd.

Views

Attack defense policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After an attack defense policy is created, you can limit the rate of all packet sent to the CPU in the attack defense policy. The device randomly discards packets that exceed the rate limit to ensure CPU security.

Precautions

If you run the **rate-limit all-packets** command in the same attack defense policy view multiple times, only the latest configuration takes effect.

The priority of protocol packets sent to the CPU configured in an attack defense policy takes effect only when the attack defense policy is applied to the main control board.

Example

Set the rate limit for all packets sent to the CPU to 12600 pps in the attack defense policy named **mypolicy**.

```
<Huawei> system-view
[Huawei] cpu-defend policy mypolicy
[Huawei-cpu-defend-policy-mypolicy] rate-limit all-packets pps 12600
```

Related Topics

19.10.11 cpu-defend policy

19.10.18 display cpu-defend policy

19.10.17 display cpu-defend configuration

19.10.29 reset auto-defend attack-source

Function

The **reset auto-defend attack-source** command clears information about attack sources.

Format

reset auto-defend attack-source

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the latest attack source information on the device, run the **reset auto-defend attack-source** command to delete the existing attack source information, wait for a period, and run the **display auto-defend attack-source** command.

Precautions

After the **reset auto-defend attack-source** command is run, information about attack sources is cleared and cannot be restored.

Example

Delete existing attack source information on the device.

```
<Huawei> reset auto-defend attack-source
```

Related Topics

19.10.15 display auto-defend attack-source

19.10.30 reset cpu-defend statistics

Function

The **reset cpu-defend statistics** command clears statistics on packets sent to the CPU.

Format

reset cpu-defend statistics [**packet-type** *packet-type*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
packet-type *packet-type*	Specifies the protocol type of packets. *packet-type* specifies the packet type. • If **packet-type** *packet-type* is specified, the statistics on the specified type of protocol packets are cleared. • If **packet-type** *packet-type* is not specified, the statistics on all protocol packets are cleared.	The supported packet type depends on the device.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view statistics on the packets sent to the CPU in a specified period, run the **reset cpu-defend statistics** command to clear existing statistics and run the **display cpu-defend statistics** command.

Precautions

The deleted packet statistics cannot be restored.

Example

Clear statistics on BGP packets on the main control board.

```
<Huawei> reset cpu-defend statistics packet-type bgp
```

Related Topics

19.10.20 display cpu-defend statistics

19.11 Attack Defense Configuration Commands

19.11.1 anti-attack abnormal enable

Function

The **anti-attack abnormal enable** command enables defense against malformed packet attacks.

The **undo anti-attack abnormal enable** command disables defense against malformed packet attacks.

The **anti-attack abnormal disable** command disables defense against malformed packet attacks.

By default, defense against malformed packet attacks is enabled.

Format

anti-attack abnormal enable

undo anti-attack abnormal enable

anti-attack abnormal disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The malformed packet attack is to send malformed IP packets to the system. If such an attack occurs, the system may break down when processing the malformed IP packets. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack abnormal enable** command to enable defense against malformed packets.

The device detects malformed packets after defense against malformed packets is enabled.

The device directly discards packets of the following types:

- Flood attacks from IP null payload packets
- Attacks from IGMP null payload packets
- LAND attacks
- Smurf attacks
- Attacks from packets with invalid TCP flag bits

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including malformed packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable defense against malformed packet attacks.

```
<Huawei> system-view
[Huawei] anti-attack abnormal enable
```

Related Topics

19.11.2 anti-attack enable

19.11.2 anti-attack enable

Function

The **anti-attack enable** command enables defense against all attack packets.

The **undo anti-attack enable** command disables defense against all attack packets.

The **anti-attack disable** command disables defense against all attack packets.

By default, defense against all attack packets is enabled.

Format

anti-attack enable

undo anti-attack enable

anti-attack disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different types of attacks on a network cause high device usage or system breakdown, affecting network services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack enable** command to enable defense against all attack packets.

Precautions

Running the **anti-attack enable** command is equivalent to running all of the following commands:

- **anti-attack abnormal enable**
- **anti-attack fragment enable**
- **anti-attack tcp-syn enable**
- **anti-attack udp-flood enable**
- **anti-attack icmp-flood enable**

Example

Enable defense against all attack packets.

```
<Huawei> system-view
[Huawei] anti-attack enable
```

Related Topics

19.11.1 anti-attack abnormal enable
19.11.3 anti-attack fragment enable
19.11.7 anti-attack tcp-syn enable
19.11.9 anti-attack udp-flood enable
19.11.5 anti-attack icmp-flood enable

19.11.3 anti-attack fragment enable

Function

The **anti-attack fragment enable** command enables defense against packet fragment attacks.

The **undo anti-attack fragment enable** command disables defense against packet fragment attacks.

The **anti-attack fragment disable** command disables defense against packet fragment attacks.

By default, defense against packet fragment attacks is enabled.

Format

anti-attack fragment enable

undo anti-attack fragment enable

anti-attack fragment disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends error packet fragments to a device, the device consumes a large number of resources to process the error packet fragments, affecting normal services. To prevent the system from breaking down and to ensure normal network services, run the **anti-attack fragment enable** command to enable defense against packet fragment attacks.

The device detects error packet fragments after defense against error packet fragments is enabled. If the device detects error packet fragments, the device limits the rate of these fragments to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including packet fragments.

Example

Enable defense against packet fragment attacks.

```
<Huawei> system-view
[Huawei] anti-attack fragment enable
```

Related Topics

19.11.2 anti-attack enable

19.11.4 anti-attack fragment car

Function

The **anti-attack fragment car** command sets the rate limit of packet fragments.

The **undo anti-attack fragment car** command restores the rate limit of packet fragments.

By default, the rate limit of packet fragments is 155000000 bit/s.

Format

anti-attack fragment car cir *cir*

undo anti-attack fragment car

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of packet fragments.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against packet fragment attacks is enabled, run the **anti-attack fragment car** command to set the rate limit of packet fragments. If the rate of received packet fragments exceeds the rate limit, the device discards excess packet fragments to ensure that the device CPU works properly.

Prerequisites

Defense against packet fragment attacks has been enabled using the **anti-attack fragment enable** command.

Example

Set the rate limit of packet fragments to 8000 bit/s.

```
<Huawei> system-view
[Huawei] anti-attack fragment enable
[Huawei] anti-attack fragment car cir 8000
```

Related Topics

19.11.5 anti-attack icmp-flood enable

19.11.5 anti-attack icmp-flood enable

Function

The **anti-attack icmp-flood enable** command enables defense against ICMP flood attacks.

The **undo anti-attack icmp-flood enable** command disables defense against ICMP flood attacks.

The **anti-attack icmp-flood disable** command disables defense against ICMP flood attacks.

 Copyright © Huawei Technologies Co., Ltd.

By default, defense against ICMP flood attacks is enabled.

Format

anti-attack icmp-flood enable

undo anti-attack icmp-flood enable

anti-attack icmp-flood disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of ICMP request packets to the target host in a short time, the target host is busy with these ICMP request packets. As a result, the target host is overloaded and cannot process normal services. To prevent ICMP flood attacks, run the **anti-attack icmp-flood enable** command to enable defense against ICMP flood attacks.

The device detects ICMP flood attack packets after defense against ICMP flood attacks is enabled. If the device detects ICMP flood attack packets, the device limits the rate of these ICMP flood attack packets to ensure that the device CPU works properly.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including ICMP flood attack packets.

Example

Enable defense against ICMP flood attacks.

```
<Huawei> system-view
[Huawei] anti-attack icmp-flood enable
```

Related Topics

19.11.6 anti-attack icmp-flood car

19.11.2 anti-attack enable

19.11.6 anti-attack icmp-flood car

Function

The **anti-attack icmp-flood car** command sets the rate limit of ICMP flood attack packets.

The **undo anti-attack icmp-flood car** command restores the default rate limit of ICMP flood attack packets.

By default, the rate limit of ICMP flood attack packets is 155000000 bit/s.

Format

anti-attack icmp-flood car cir *cir*

undo anti-attack icmp-flood car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) of ICMP flood attack packets.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After defense against ICMP flood attacks is enabled, run the **anti-attack icmp-flood car** command to set the rate limit of ICMP flood attack packets. If the rate of received ICMP flood attack packets exceeds the rate limit, the device discards excess ICMP flood attack packets to ensure that its CPU works properly.

Prerequisites

Defense against ICMP flood attacks has been enabled using the **anti-attack icmp-flood enable** command.

Example

Set the rate limit of ICMP flood attack packets to 8000 bit/s.

```
<Huawei> system-view
[Huawei] anti-attack icmp-flood enable
[Huawei] anti-attack icmp-flood car cir 8000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.11.5 anti-attack icmp-flood enable

19.11.7 anti-attack tcp-syn enable

Function

The **anti-attack tcp-syn enable** command enables defense against TCP SYN flood attacks.

The **undo anti-attack tcp-syn enable** command disables defense against TCP SYN flood attacks.

The **anti-attack tcp-syn disable** command disables defense against TCP SYN flood attacks.

By default, defense against TCP SYN flood attacks is enabled.

Format

anti-attack tcp-syn enable

undo anti-attack tcp-syn enable

anti-attack tcp-syn disable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An attacker sends a SYN packet to a target host to initiate a TCP connection but does not respond to the SYN-ACK sent from the target host. If the target host receives no ACK packet from the attacker, it keeps waiting for the ACK packet. A half-open connection is formed. The attacker keeps sending SYN packets, so many half-open connections are set up on the target host. This wastes a large number of resources. To prevent TCP SYN flood attacks, run the **anti-attack tcp-syn enable** command to enable defense against TCP SYN flood attacks.

The device detects TCP SYN flood attack packets after defense against TCP SYN flood attacks is enabled. If the device detects TCP SYN flood attack packets, the device limits the rate of these TCP SYN flood attack packets to ensure that the device CPU works properly.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including TCP SYN flood attack packets.

Example

Enable defense against TCP SYN flood attacks.

```
<Huawei> system-view
[Huawei] anti-attack tcp-syn enable
```

Related Topics

19.11.8 anti-attack tcp-syn car

19.11.2 anti-attack enable

19.11.8 anti-attack tcp-syn car

Function

The **anti-attack tcp-syn car** command sets the rate limit at which TCP SYN packets are received.

The **undo anti-attack tcp-syn car** command restores the default rate limit at which TCP SYN packets are received.

By default, the rate limit at which TCP SYN packets are received is 155000000 bit/s.

Format

anti-attack tcp-syn car cir *cir*

undo anti-attack tcp-syn car

Parameters

Parameter	Description	Value
cir *cir*	Specifies the committed information rate (CIR) at which TCP SYN packets are received.	The value is an integer that ranges from 8000 to 155000000, in bit/s.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After defense against TCP SYN flood attacks is enabled, run the **anti-attack tcp-syn car** command to set the rate limit at which TCP SYN packets are received. If the rate of received TCP SYN attack packets exceeds the rate limit, the device discards excess TCP SYN flood attack packets to ensure that the device CPU works properly.

Prerequisites

Defense against TCP SYN flood attacks has been enabled using the **anti-attack tcp-syn enable** command.

Example

Set the rate limit at which TCP SYN packets are received to 8000 bit/s.

```
<Huawei> system-view
[Huawei] anti-attack tcp-syn enable
[Huawei] anti-attack tcp-syn car cir 8000
```

Related Topics

19.11.7 anti-attack tcp-syn enable

19.11.9 anti-attack udp-flood enable

Function

The **anti-attack udp-flood enable** command enables defense against UDP flood attacks.

The **undo anti-attack udp-flood enable** command disables defense against UDP flood attacks.

The **anti-attack udp-flood disable** command disables defense against UDP flood attacks.

By default, defense against UDP flood attacks is enabled.

Format

anti-attack udp-flood enable

undo anti-attack udp-flood enable

anti-attack udp-flood disable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker sends a large number of UDP packets to the target host in a short time, the target host is busy with these UDP packets. As a result, the target host is overloaded and cannot process normal services. To prevent UDP flood attacks, run the **anti-attack udp-flood enable** command to enable defense against UDP flood attacks.

The device detects UDP flood attack packets after defense against UDP flood attacks is enabled. The device directly discards UDP flood attack packets.

Precautions

You can also run the **anti-attack enable** command in the system view to enable attack defense against all attack packets including UDP flood attack packets.

Example

Enable defense against UDP flood attacks.

```
<Huawei> system-view
[Huawei] anti-attack udp-flood enable
```

Related Topics

19.11.2 anti-attack enable

19.11.10 anti-attack urpf

Function

The **anti-attack urpf** command enables URPF.

The **undo anti-attack urpf** command disables URPF.

By default, URPF is disabled.

Format

anti-attack urpf { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo anti-attack urpf

Parameters

Parameter	Description	Value
loose	Indicates URPF loose check.	-

Parameter	Description	Value
strict	Indicates URPF strict check.	-
allow-default-route	Allows special processing of default routes.	-
acl *acl-number*	Specifies the ACL number.	The number is an integer ranging from 2000 to 3999. For the basic ACL, the number ranges from 2000 to 2999; for the advanced ACL, the number ranges from 3000 to 3999.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To ensure that the packets pass the URPF check when the forwarding table contains the related entries even if the interface that actually receives the packets does not match the outbound interface in the forwarding table, set the URPF check mode to **loose**. To ensure that the packets pass the URPF check only when the forwarding table contains related entries and the interface actually receives the packets matches the outbound interface in the forwarding table, set the URPF check mode to **strict**.

Example

Create ACL 2999, enable strict URPF check, and configure the device to allow special processing of default routes.

```
<Huawei> system-view
[Huawei] anti-attack urpf strict allow-default-route acl 2999
```

Related Topics

19.11.11 display anti-attack statistics

19.11.11 display anti-attack statistics

Function

The **display anti-attack statistics** command displays statistics about attack packets of a specified type.

If no parameter is specified, the **display anti-attack statistics** command displays statistics about attack packets of all types.

Format

display anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood** | **urpf**]

Parameters

Parameter	Description	Value
abnormal	Displays statistics about malformed packets.	-
fragment	Displays statistics about defense against packet fragments.	-
tcp-syn	Displays statistics about defense against TCP SYN flood attacks.	-
udp-flood	Displays statistics about defense against UDP flood attacks.	-
icmp-flood	Displays statistics about defense against ICMP flood attacks.	-
urpf	Displays the statistics about URPF check.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display anti-attack statistics** command displays statistics on attack packets of the following types: malformed packet attack, packet fragment attack, TCP SYN flood attack, UDP flood attack, ICMP flood attack.

Example

Display attack defense statistics.

```
<Huawei> display anti-attack statistics
Packets Statistic Information:
-------------------------------------------------------------------------------
AntiAtkType  TotalPacketNum        DropPacketNum         PassPacketNum
            (H)        (L)        (H)        (L)        (H)        (L)
-------------------------------------------------------------------------------
```

```
URPF        0        1088     0        0        0        1088
Abnormal     0        0        0        0        0        0
Fragment     0        0        0        0        0        0
Tcp-syn     0        58       0        0        0        58
Udp-flood    0        0        0        0        0        0
Icmp-flood   0        0        0        0        0        0
-------------------------------------------------------------------------------
```

Table 19-139 Description of the display anti-attack statistics command output

Item	Description
AntiAtkType	Attack defense type: • URPF: URPF check • Abnormal: defense against malformed packets • Fragment: defense against packet fragments • Tcp-syn: defense against TCP SYN flood attacks • Udp-flood: defense against UDP flood attacks • Icmp-flood: defense against ICMP flood attacks
TotalPacketNum	Total number of packets.
DropPacketNum	Number of discarded packets.
PassPacketNum	Number of forwarded packets.
(H)	Highest-order bit display.
(L)	Lowest-order bit display.

Related Topics

19.11.12 reset anti-attack statistics

19.11.12 reset anti-attack statistics

Function

The **reset anti-attack statistics** command clears attack defense statistics.

Format

reset anti-attack statistics [**abnormal** | **fragment** | **tcp-syn** | **udp-flood** | **icmp-flood** | **urpf**]

Parameters

Parameter	Description	Value
abnormal	Clears statistics about defense against malformed packets.	-
fragment	Clears statistics about defense against packet fragments.	-
tcp-syn	Clears statistics about defense against TCP SYN flood attacks.	-
udp-flood	Clears statistics about defense against UDP flood attacks.	-
icmp-flood	Clears statistics about defense against ICMP flood attacks.	-
urpf	Clears statistics about URPF check.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

If no attack defense is specified, statistics about all types of attack defense are cleared.

NOTICE

The cleared statistics cannot be restored. Exercise caution when you use the command.

Example

Clear statistics about defense against malformed packets.

```
<Huawei> reset anti-attack statistics abnormal
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.11.11 display anti-attack statistics

19.12 Traffic Suppression Configuration Commands

19.12.1 broadcast-suppression (interface view)

Function

The **broadcast-suppression** command sets the maximum traffic rate of broadcast packets that can pass through an interface.

The **undo broadcast-suppression** command cancels the rate limit for broadcast traffic on an interface.

By default, broadcast traffic is not suppressed on an interface.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, 9ES2 board do not support traffic suppression on interfaces.

This command is not supported by the AR100 series, AR120 series, AR161, AR161W, AR161G-L, AR169, AR169W, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161G-U, AR161G-Lc, AR161EW, AR161EW-M1, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR161FW-P-M5.

Format

broadcast-suppression { **cir** *cir-value* | **packets** *packets-per-second* }

undo broadcast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range is as follows: • Fast Ethernet interface: 64 to 100000. • GE interface: 64 to 1000000. • XGE interface: 64 to 10000000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
packets *packets-per-second*	Specifies the rate limit in number of packets per second (pps).	The value is an integer, in pps. The value range is as follows: ● Fast Ethernet interface: 0 to 148810. ● GE interface: 0 to 1488100. ● XGE interface: 0 to 14881000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **broadcast-suppression** command to set the threshold of broadcast traffic that an interface allows to pass through. When the broadcast traffic rate reaches the rate limit, the system discards excess broadcast packets to control the traffic rate in a proper range.

Precautions

AR1220E, AR1220EV and AR1220EVW only supports the broadcast-suppression command, but does not support the multicast-suppression or unicast-suppression command.

Different types of interfaces support different modes for traffic suppression:

- The CIR value for traffic suppression can be set on the LAN-side Ethernet interfaces of the main control board.
- The rate limit in pps can be set on the LAN-side Ethernet interfaces of the LPU.

Different models support different types of interfaces and therefore different traffic suppression modes. Set the traffic suppression mode depending on the actual device configuration.

Example

Set the rate limit for broadcast traffic to 21600 pps on Ethernet 2/0/0

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] broadcast-suppression packets 21600
```

Related Topics

19.12.7 multicast-suppression (interface view)

19.12.9 unicast-suppression (interface view)

19.12.2 broadcast-suppression (system view)

Function

The **broadcast-suppression** command sets the maximum traffic rate of broadcast packets that can pass through an interface of a device.

The **undo broadcast-suppression** command cancels the rate limiting on the broadcast packets that can pass through an interface of a device.

By default, an interface of a device does not suppress broadcast packets.

NOTE

Only the AR161EW, AR161EW-M1, AR169EW, or AR169EGW-L support this command.

Format

broadcast-suppression cir *cir-value*

undo broadcast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The accumulating broadcast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

 Copyright © Huawei Technologies Co., Ltd.

To prevent broadcast storms, you can use the **broadcast-suppression** command to set the threshold of broadcast traffic that an interface of a device allows to pass through. When the broadcast traffic rate reaches the maximum value, the system discards excess broadcast packets to control the traffic volume in a proper range.

Storm control is a simple traffic suppression approach. Although the token bucket technology is used, the bucket depth is a fixed multiple of the traffic rate and cannot be changed. As a result, the size of broadcast traffic affects the time when storm control takes effect. After the **broadcast-suppression** command is run to set the maximum rate of broadcast packets that can pass through an interface of a device, storm control takes effect at a certain interval if the traffic entering the device is small. If the traffic is heavy, storm control takes effect immediately.

Example

Set the maximum rate of broadcast packets that can pass through an interface of a device to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] broadcast-suppression cir 50000
```

Related Topics

19.12.8 multicast-suppression (system view)
19.12.10 unicast-suppression (system view)

19.12.3 display flow-suppression interface

Function

The **display flow-suppression interface** command displays the traffic suppression configuration on an interface.

Format

display flow-suppression interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the interface number.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the traffic suppression configuration on Ethernet 2/0/0.

```
<Huawei> display flow-suppression interface ethernet 2/0/0
 storm type          rate mode   set rate value
--------------------------------------------------------------------------------
 unknown-unicast    pps          pps: 1260(packet/s)
 multicast          pps          pps: 2520(packet/s)
 broadcast          pps          pps: 1260(packet/s)
--------------------------------------------------------------------------------
```

Display the traffic suppression configuration on Ethernet 0/0/0.

```
<Huawei> display flow-suppression interface ethernet 0/0/0
 storm type          rate mode   set rate value
--------------------------------------------------------------------------------
 unknown-unicast    bps          cir: 100(kbit/s)
 multicast          bps          cir: 200(kbit/s)
 broadcast          bps          cir: 100(kbit/s)
--------------------------------------------------------------------------------
```

Table 19-140 Description of the display flow-suppression interface command output

Item	Description
storm type	Traffic type. Broadcast traffic, multicast traffic, and unknown unicast traffic can be suppressed.
rate mode	Type of the rate limit. • bps: cir mode • pps: packet mode
set rate value	Configured rate limit.

Related Topics

19.12.1 broadcast-suppression (interface view)
19.12.7 multicast-suppression (interface view)
19.12.9 unicast-suppression (interface view)

19.12.4 flood-suppression (interface view)

Function

The **flood-suppression** command sets the maximum rate of broadcast, multicast, and unknown unicast packets that can pass through an interface.

The **undo flood-suppression** command cancels the rate limiting for broadcast, multicast, and unknown unicast packets on interfaces.

By default, the rate of broadcast, multicast, and unknown unicast packets on interfaces is not limited.

NOTE

Only the AR1220E, AR1220EV, and AR1220EVW support this command.

Format

flood-suppression cir *cir-value*

undo flood-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer and the unit is kbit/s. ● For an Fast Ethernet interface, the value ranges from 64 to 100000. ● For a GE interface, the value ranges from 64 to 1000000. ● For an XGE interface, the value ranges from 64 to 10000000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

The accumulating broadcast, multicast, and unknown unicast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

 Copyright © Huawei Technologies Co., Ltd.

To prevent broadcast storms, you can use the **flood-suppression** command to set the threshold of broadcast, multicast, and unknown unicast traffic that an interface allows to pass through. When the total traffic rate of broadcast, multicast, and unknown unicast traffic on an interface reaches the rate limit, the system discards excess packets to control the traffic rate in a proper range.

Example

Set the maximum rate of broadcast, multicast, and unknown unicast packets that can pass an interface to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/3
[Huawei-GigabitEthernet0/0/3] flood-suppression cir 50000
```

19.12.5 icmp rate-limit

Function

Using the **icmp rate-limit** command, you can configure the rate limit for ICMP packets globally or on an interface.

Using the **undo icmp rate-limit** command, you can restore the default rate limit for ICMP packets.

By default, the global rate limit and rate limit on an interface are both 100 pps.

Format

icmp rate-limit threshold *threshold-value*

undo icmp rate-limit threshold

Parameters

Parameter	Description	Value
threshold *threshold-value*	Indicates the rate limit for ICMP packets.	The value is an integer ranging from 1 to 32768, in pps.

Views

System view, interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

Before configuring the rate limit for ICMP packets, enable the Router to limit the rate of incoming ICMP packets by using the **icmp rate-limit enable** command.

The Router can be configured to limit the rate of incoming ICMP packets globally or on an interface, and discard excess ICMP packets when the rate of incoming ICMP packets exceeds the limit.

You can run the **icmp rate-limit** command to set a global rate limit for ICMP packets and run this command in multiple interface views to limit the rate of ICMP packets on these interfaces. The total rate of ICMP packets on all the interfaces cannot exceed the global rate limit.

Precautions

To make suppression of ICMP packets take effect, disable the fast ICMP reply function.

The **undo icmp rate-limit** command cannot be configured in the system view.

Example

Set the rate limit for ICMP packets on Eth 2/0/0 to 20 pps.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] icmp rate-limit threshold 20
```

Related Topics

19.12.6 icmp rate-limit enable

19.12.6 icmp rate-limit enable

Function

The **icmp rate-limit enable** command enables the traffic suppression function for ICMP packets.

The **undo icmp rate-limit enable** command disables the traffic suppression function for ICMP packets.

By default, the traffic suppression function for ICMP packets is disabled.

Format

icmp rate-limit enable

undo icmp rate-limit enable

Parameters

None

Views

System view, GE interface view, XGE interface view, Ethernet interface view, Eth-Trunk interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Attackers may send a large number of ICMP packets to attack a network. If the device sends all the received ICMP packets to the CPU for processing, a lot of CPU usage resources are occupied and other services may be abnormal. To prevent ICMP packet attacks, you can configure the device to suppress ICMP packets.

After you run the **icmp rate-limit enable** command in the system view or interface view, the device limits the rate of ICMP packets by the default traffic suppression.

You can then run the **icmp rate-limit** command in the system view or interface view to configure a traffic suppression for ICMP packets.

Example

Enable the traffic suppression function for ICMP packets.

```
<Huawei> system-view
[Huawei] icmp rate-limit enable
```

Related Topics

19.12.5 icmp rate-limit

19.12.7 multicast-suppression (interface view)

Function

The **multicast-suppression** command sets the maximum traffic volume of multicast packets that can pass through an interface.

Using the **undo multicast-suppression** command, you can cancel the rate limit for multicast traffic on an interface.

By default, multicast traffic is not suppressed on an interface.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, 9ES2 board do not support traffic suppression on interfaces.

This command is not supported by the AR100 series, AR120 series, AR161, AR161W, AR161G-L, AR169, AR169W, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161G-U, AR161G-Lc, AR161EW, AR161EW-M1, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR161FW-P-M5.

Format

multicast-suppression { **cir** *cir-value* | **packets** *packets-per-second* }

undo multicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range is as follows: ● Fast Ethernet interface: 64 to 100000. ● GE interface: 64 to 1000000. ● XGE interface: 64 to 10000000.
packets *packets-per-second*	Specifies the rate limit in number of packets per second (pps).	The value is an integer, in pps. The value range is as follows: ● Fast Ethernet interface: 0 to 148810. ● GE interface: 0 to 1488100. ● XGE interface: 0 to 14881000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

When an increasing number of multicast packets are transmitted on a network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **multicast-suppression** command to set the threshold of multicast traffic that an interface allows to pass through. When the multicast traffic volume exceeds the threshold, the system discards the excess multicast packets to control the traffic volume of multicast packets to a proper range.

Precautions

Different types of interfaces support different modes for traffic suppression:

- The CIR value for traffic suppression can be set on the LAN-side Ethernet interfaces of the main control board.

 Copyright © Huawei Technologies Co., Ltd.

- The rate limit in pps can be set on the LAN-side Ethernet interfaces of the LPU.

Different models support different types of interfaces and therefore different traffic suppression modes. Set the traffic suppression mode depending on the actual device configuration.

Example

Set the rate limit for multicast traffic to 21600 pps on Ethernet 2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] multicast-suppression cir 21600
```

Related Topics

19.12.1 broadcast-suppression (interface view)
19.12.9 unicast-suppression (interface view)

19.12.8 multicast-suppression (system view)

Function

The **multicast-suppression** command sets the maximum traffic rate of multicast packets that can pass through an interface of a device.

The **undo multicast-suppression** command cancels the rate limiting on the multicast packets that can pass through an interface of a device.

By default, an interface of a device does not suppress multicast packets.

NOTE

Only the AR161EW, AR161EW-M1, AR169EW, or AR169EGW-L support this command.

Format

multicast-suppression cir *cir-value*

undo multicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The accumulating multicast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **multicast-suppression** command to set the threshold of multicast traffic that an interface of a device allows to pass through. When the multicast traffic volume reaches the threshold, the system discards the excessive multicast packets to control the traffic volume of multicast packets in to a proper range.

Storm control is a simple traffic suppression approach. Although the token bucket technology is used, the bucket depth is a fixed multiple of the traffic rate and cannot be changed. As a result, the size of multicast traffic affects the time when storm control takes effect. After the **multicast-suppression** command is run to set the maximum rate of multicast packets that can pass through an interface of a device, storm control takes effect at a certain interval if the traffic entering the device is small. If the traffic is heavy, storm control takes effect immediately.

Example

Set the maximum rate of multicast packets that can pass through an interface of a device to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] multicast-suppression cir 50000
```

Related Topics

19.12.2 broadcast-suppression (system view)

19.12.10 unicast-suppression (system view)

19.12.9 unicast-suppression (interface view)

Function

The **unicast-suppression** command sets the maximum traffic volume of unknown unicast packets that can pass through an interface.

Using the **undo unicast-suppression** command, you can cancel the rate limit for unicast traffic on an interface.

By default, unicast traffic is not suppressed on an interface.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, 9ES2 board do not support traffic suppression on interfaces.

This command is not supported by the AR100 series, AR120 series, AR161, AR161W, AR161G-L, AR169, AR169W, AR169G-L, AR169-P-M9, AR169W-P-M9, AR169RW-P-M9, AR161G-U, AR161G-Lc, AR161EW, AR161EW-M1, AR169EW, AR169CVW, AR169EGW-L, AR169CVW-4B4S, AR161FW-P-M5.

Format

unicast-suppression { **cir** *cir-value* | **packets** *packets-per-second* }

undo unicast-suppression

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR).	The value is an integer, in kbit/s. The value range is as follows: ● Fast Ethernet interface: 64 to 100000. ● GE interface: 64 to 1000000. ● XGE interface: 64 to 10000000.
packets *packets-per-second*	Specifies the rate limit in number of packets per second (pps).	The value is an integer, in pps. The value range is as follows: ● Fast Ethernet interface: 0 to 148810. ● GE interface: 0 to 1488100. ● XGE interface: 0 to 14881000.

Views

Ethernet interface view, GE interface view, XGE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Guidelines

When an increasing number of unknown multicast packets are transmitted on the network, more network resources are occupied and services are affected.

To prevent broadcast storms, you can use the **unicast-suppression** command to set the threshold of unicast traffic that an interface allows to pass through. When the unknown unicast traffic rate exceeds the rate limit, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Precautions

Different types of interfaces support different modes for traffic suppression:

- The CIR value for traffic suppression can be set on the LAN-side Ethernet interfaces of the main control board.
- The rate limit in pps can be set on the LAN-side Ethernet interfaces of the LPU.

Different models support different types of interfaces and therefore different traffic suppression modes. Set the traffic suppression mode depending on the actual device configuration.

Example

Set the rate limit for unknown unicast traffic to 21600 pps on Ethernet 2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] unicast-suppression packets 21600
```

Related Topics

19.12.1 broadcast-suppression (interface view)
19.12.7 multicast-suppression (interface view)

19.12.10 unicast-suppression (system view)

Function

The **unicast-suppression** command sets the maximum traffic rate of unknown unicast packets that can pass through an interface of a device.

The **undo unicast-suppression** command cancels the rate limiting on the unknown unicast packets that can pass through an interface of a device.

By default, an interface of a device does not suppress unknown unicast packets.

NOTE

Only the AR161EW, AR161EW-M1, AR169EW, or AR169EGW-L support this command.

Format

unicast-suppression cir *cir-value*

undo unicast-suppression

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 64 to 10000000, in kbit/s.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The accumulating unknown unicast packets on the network occupy more and more network resources. This affects normal operation of services on the network.

To prevent broadcast storms, you can use the **unicast-suppression** command to set the threshold of unknown unicast traffic that an interface of a device allows to pass through. When the unknown unicast traffic rate reaches the rate limit, the system discards excess unknown unicast packets to control the traffic volume in a proper range.

Storm control is a simple traffic suppression approach. Although the token bucket technology is used, the bucket depth is a fixed multiple of the traffic rate and cannot be changed. As a result, the size of unicast traffic affects the time when storm control takes effect. After the **unicast-suppression** command is run to set the maximum rate of unicast packets that can pass through an interface of a device, storm control takes effect at a certain interval if the traffic entering the device is small. If the traffic is heavy, storm control takes effect immediately.

Example

Set the maximum rate of unknown unicast packets that can pass through an interface of a device to 50000 kbit/s.

```
<Huawei> system-view
[Huawei] unicast-suppression cir 50000
```

Related Topics

19.12.2 broadcast-suppression (system view)
19.12.8 multicast-suppression (system view)

19.13 ARP Security Configuration Commands

19.13.1 arp anti-attack check user-bind alarm enable

Function

The **arp anti-attack check user-bind alarm enable** command enables the alarm function for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm enable** command disables the alarm function for ARP packets discarded by DAI.

By default, the alarm function for ARP packets discarded by DAI is disabled.

Format

arp anti-attack check user-bind alarm enable

undo arp anti-attack check user-bind alarm enable

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After DAI is enabled, if you want to receive an alarm when a large number of ARP packets are discarded by DAI, you can run the **arp anti-attack check user-bind alarm enable** command. After the alarm function is enabled, the device sends an alarm when the number of discarded ARP packets exceeds the threshold.

The alarm threshold is set by the **19.13.2 arp anti-attack check user-bind alarm threshold** command.

Prerequisites

DAI has been enabled on the interface using the **arp anti-attack check user-bind enable** command.

Precautions

Since the default interval for sending ARP alarms is 0 (that is, no ARP alarm is sent), you must run the **arp anti-attack log-trap-timer** *time* command to increase the alarm sending interval after enabling the alarm for packets discarded by DAI.

This command can be used only on Layer 2 interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the alarm function for ARP packets discarded by DAI on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind alarm enable
```

Related Topics

19.13.5 arp anti-attack check user-bind enable
19.13.2 arp anti-attack check user-bind alarm threshold

19.13.2 arp anti-attack check user-bind alarm threshold

Function

The **arp anti-attack check user-bind alarm threshold** command sets the alarm threshold for ARP packets discarded by DAI.

The **undo arp anti-attack check user-bind alarm threshold** command restores the default alarm threshold for ARP packets discarded by DAI.

The threshold on interfaces is consistent with the threshold set by the **arp anti-attack check user-bind alarm threshold** command in the system view. If the alarm threshold is not set in the system view, the default threshold on the interface is 100.

Format

System view:

arp anti-attack check user-bind alarm threshold *threshold*

undo arp anti-attack check user-bind alarm threshold

Interface view:

arp anti-attack check user-bind alarm threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the ARP packets discarded by DAI.	The value is an integer that ranges from 1 to 1000.

Views

System view, Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can use this command to set the alarm threshold for ARP packets discarded by DAI. After the alarm threshold is set, the device sends an alarm when the number of ARP packets discarded by DAI exceeds this threshold.

Prerequisites

DAI has been enabled using the **arp anti-attack check user-bind enable** command in the interface view, and the alarm function for ARP packets discarded by DAI has been enabled using the **arp anti-attack check user-bind alarm enable** command.

Precautions

The **arp anti-attack check user-bind alarm threshold** command takes effect in the system view only when DAI and the alarm function for ARP packets discarded by DAI are enabled on the interface. The global alarm threshold takes effect on all interfaces enabled with the two functions.

If the alarm thresholds are set in the interface view and system view, the alarm threshold configured in the interface view takes effect. If the alarm threshold on an interface is not configured, the global alarm threshold is used.

The **arp anti-attack check user-bind alarm threshold** command can be used only on Layer 2 interfaces.

Example

Set the alarm threshold for ARP packets discarded by DAI on Eth2/0/0 to 200.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind alarm enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind alarm threshold 200
```

Related Topics

19.13.5 arp anti-attack check user-bind enable
19.13.1 arp anti-attack check user-bind alarm enable

19.13.3 arp anti-attack check user-bind check-item (interface view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries on an interface.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and VLAN ID.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
vlan	Indicates that the device checks VLAN IDs in ARP packets.	-

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and VLAN ID of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, use the **arp anti-attack check user-bind check-item** command to configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled on the interface using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

This command can be used only on Layer 2 interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure Eth2/0/0 to check IP addresses in ARP packets.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind check-item ip-address
```

Related Topics

19.13.5 arp anti-attack check user-bind enable
19.13.4 arp anti-attack check user-bind check-item (VLAN view)

19.13.4 arp anti-attack check user-bind check-item (VLAN view)

Function

The **arp anti-attack check user-bind check-item** command configures check items for ARP packet check based on binding entries in a VLAN.

The **undo arp anti-attack check user-bind check-item** command restores the default check items.

By default, the check items consist of IP address, MAC address, and interface number.

Format

arp anti-attack check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo arp anti-attack check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Indicates that the device checks IP addresses in ARP packets.	-
mac-address	Indicates that the device checks MAC addresses in ARP packets.	-
interface	Indicates that the device checks interface numbers in ARP packets.	-

Views

VLAN view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a device receives an ARP packet, it compares the source IP address, source MAC address, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

To allow some special ARP packets that match only one or two items in binding entries to pass through, configure the device to check ARP packets according to one or two specified items in binding entries.

Prerequisites

DAI has been enabled in the VLAN using the **arp anti-attack check user-bind enable** command.

Precautions

Check items configured for ARP packet check based on binding entries do not take effect on hosts that are configured with static binding entries. These hosts check ARP packets based on all items in static binding entries.

Example

Configure the device to check IP addresses in ARP packets from VLAN 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] arp anti-attack check user-bind enable
[Huawei-vlan100] arp anti-attack check user-bind check-item ip-address
```

Related Topics

19.13.5 arp anti-attack check user-bind enable
19.13.3 arp anti-attack check user-bind check-item (interface view)

19.13.5 arp anti-attack check user-bind enable

Function

The **arp anti-attack check user-bind enable** command enables DAI on an interface or in a VLAN. DAI enables the device to check ARP packets based on binding entries.

The **undo arp anti-attack check user-bind enable** command disables DAI on an interface or in a VLAN.

By default, DAI is disabled on an interface or in a VLAN.

Format

arp anti-attack check user-bind enable

undo arp anti-attack check user-bind enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent MITM attacks and theft on authorized user information, run the **arp anti-attack check user-bind enable** command to enable DAI. When a device receives an ARP packet, it compares the source IP address, source MAC address, VLAN ID, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows the packet to pass through. If the ARP packet matches no binding entry, the device considers the ARP packet invalid and discards the packet.

You can enable DAI in the interface view or the VLAN view. When DAI is enabled in an interface view, the device checks all ARP packets received on the interface against binding entries. When DAI is enabled in the VLAN view, the device checks ARP packets received on interfaces belong to the VLAN based on binding entries.

This command can be used only on Layer 2 interfaces.

Follow-up Procedure

Run the **arp anti-attack check user-bind check-item (interface view)** or **arp anti-attack check user-bind check-item (VLAN view)** command to configure check items for ARP packet check based on binding entries.

Example

Enable DAI on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack check user-bind enable
```

Enable DAI in VLAN 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] arp anti-attack check user-bind enable
```

Related Topics

19.13.3 arp anti-attack check user-bind check-item (interface view)
19.13.4 arp anti-attack check user-bind check-item (VLAN view)

19.13.6 arp anti-attack entry-check enable

Function

The **arp anti-attack entry-check enable** command enables ARP entry fixing.

The **undo arp anti-attack entry-check enable** command disables ARP entry fixing.

By default, ARP entry fixing is disabled.

Format

arp anti-attack entry-check { **fixed-mac** | **fixed-all** | **send-ack** } **enable**

undo arp anti-attack entry-check enable

Parameters

Parameter	Description	Value
fixed-mac	Indicates ARP entry fixing in **fixed-mac** mode. When receiving an ARP packet, the device discards the packet if the MAC address does not match the MAC address in the corresponding ARP entry. If the MAC address in the ARP packet matches that in the corresponding ARP entry while the interface number or VLAN ID does not match that in the ARP entry, the device updates the interface number or VLAN ID in the ARP entry.	-
fixed-all	Indicates ARP entry fixing in **fixed-all** mode. When the MAC address, interface number, and VLAN ID of an ARP packet match those in the corresponding ARP entry, the device updates other information about the ARP entry.	-
send-ack	Indicates ARP entry fixing in **send-ack** mode. When the device receives an ARP packet with a changed MAC address, interface number, or VLAN ID, it does not immediately update the corresponding ARP entry. Instead, the device sends a unicast ARP Request packet to the user with the IP address mapped to the original MAC address in the ARP entry, and then determines whether to change the MAC address, VLAN ID, or interface number in the ARP entry depending on the response from the user.	-

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To defend against ARP address spoofing attacks, enable ARP entry fixing. The **fixed-mac**, **fixed-all**, and **send-ack** modes are applicable to different scenarios and are mutually exclusive:

- The **fixed-mac** mode applies to networks where user MAC addresses are unchanged but user access locations often change. When a user connects to a different interface on the device, the device updates interface information in the ARP entry of the user timely.
- The **fixed-all** mode applies to networks where user MAC addresses and user access locations are fixed.
- The **send-ack** mode applies to networks where user MAC addresses and user access locations often change.

Example

Enable ARP entry fixing and specify the **fixed-mac** mode.

```
<Huawei> system-view
[Huawei] arp anti-attack entry-check fixed-mac enable
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.7 arp anti-attack gateway-duplicate enable

Function

The **arp anti-attack gateway-duplicate enable** command enables ARP gateway anti-collision.

The **undo arp anti-attack gateway-duplicate enable** command disables ARP gateway anti-collision.

By default, ARP gateway anti-collision is disabled.

Format

arp anti-attack gateway-duplicate enable

undo arp anti-attack gateway-duplicate enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges the gateway address to send ARP packets with the source IP address being the IP address of the gateway on the LAN, ARP entries on hosts in the LAN record the incorrect gateway address. As a result, all traffic from user hosts to the gateway is sent to the attacker and the attacker intercepts user information. Communication of users is interrupted.

To prevent bogus gateway attacks, enable ARP gateway anti-collision on the gateway using the **arp anti-attack gateway-duplicate enable** command. The gateway considers that a gateway collision occurs when a received ARP packet meets either of the following conditions:

- The source IP address in the ARP packet is the same as the IP address of the VLANIF interface matching the physical inbound interface of the packet.
- The source IP address in the ARP packet is the virtual IP address of the inbound interface but the source MAC address in the ARP packet is not the virtual MAC address of the VRRP group.

The device generates an ARP anti-collision entry and discards the received packets with the same source MAC address and VLAN ID in a specified period. This function prevents ARP packets with the bogus gateway address from being broadcast in a VLAN.

Precautions

A maximum of 100 ARP anti-attack entries exist on the device at the same time. When the maximum number is exceeded, the device cannot prevent new ARP gateway collision attacks.

Example

Enable ARP gateway anti-collision.

```
<Huawei> system-view
[Huawei] arp anti-attack gateway-duplicate enable
```

Related Topics

19.13.31 display arp anti-attack configuration
19.13.32 display arp anti-attack gateway-duplicate item

19.13.8 arp anti-attack log-trap-timer

Function

The **arp anti-attack log-trap-timer** command sets the interval for sending ARP alarms.

The **undo arp anti-attack log-trap-timer** command restores the default setting.

The default interval for sending alarms is 0, indicating that the device does not send ARP alarms.

Format

arp anti-attack log-trap-timer *time*

undo arp anti-attack log-trap-timer

Parameters

Parameter	Description	Value
time	Specifies the interval for sending ARP alarms.	The value is an integer that ranges from 0 to 1200, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow the administrator to learn the ARP running status in real time, define potential attacks, and take measures, the device provides the alarm function for potential ARP attacks. This function records exceptions of ARP running in real time. To avoid excessive alarms when ARP attacks occur, reduce the alarm quantity by setting a proper interval for sending alarms.

NOTE

The **arp anti-attack log-trap-timer** command takes effect only on the following alarms:

- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.4 hwARPSDaiDropALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.5 hwARPGlobleSpeedLimitALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.8 hwARPMissGlobleSpeedLimitALarm
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.3 hwARPSPacketCheck
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.1 hwARPSGatewayConflict
- SECE_1.3.6.1.4.1.2011.5.25.165.2.2.2.2 hwARPSEntryCheck

Precautions

In the insecure environment, you are advised to extend the interval for sending ARP alarms. This prevents excessive ARP alarms. In the secure environment, you are advised to shorten the interval for sending ARP alarms. This facilitates fault rectification in real time.

After the interval is set, the device discards alarms generates in this interval; therefore, some faults cannot be rectified in real time.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the interval for sending ARP alarms to 20 seconds.

```
<Huawei> system-view
[Huawei] arp anti-attack log-trap-timer 20
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.9 arp anti-attack packet-check sender-mac

Function

The **arp anti-attack packet-check sender-mac** command checks whether the source MAC address in an ARP packet is the same as that in the Ethernet frame header.

The **undo arp anti-attack packet-check sender-mac** command disables ARP packet validity check.

By default, ARP packet validity check is disabled.

Format

arp anti-attack packet-check sender-mac

undo arp anti-attack packet-check sender-mac

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After receiving an ARP packet, the device checks validity of the ARP packet, including:

- Packet length
- Validity of the source and destination MAC addresses in the ARP packet
- ARP Request type and ARP Reply type
- MAC address length
- IP address length

 Copyright © Huawei Technologies Co., Ltd.

- Whether the ARP packet is an Ethernet frame

The preceding check items are used to determine whether an ARP packet is valid. The packet with different source MAC addresses in the ARP packet and Ethernet frame header is possibly an attack packet although it is allowed by the ARP protocol. After the **arp anti-attack packet-check sender-mac** command is used, the device checks the source MAC addresses in the ARP packet and Ethernet frame header, and discards the packets with inconsistent source MAC addresses.

Precautions

The **arp validate** command can be used to configure the device to check whether the source MAC address in an ARP packet is the same as that in the Ethernet frame header. This command is different from the **arp anti-attack packet-check sender-mac** command.

- The **arp validate** command configures ARP packet validity check only on a physical interface. The **arp anti-attack packet-check sender-mac** command configures ARP packet validity check globally.
- The **arp validate** command checks whether the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header. The **arp anti-attack packet-check sender-mac** command checks whether the source MAC address in an ARP packet is the same as that in the Ethernet frame header.

Example

Enable ARP packet validity check to allow the device to check the source MAC address in an ARP packet.

```
<Huawei> system-view
[Huawei] arp anti-attack packet-check sender-mac
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.10 arp anti-attack rate-limit

Function

The **arp anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP packets globally or on an interface.

The **undo arp anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP packets globally or on an interface.

By default, a maximum of 100 ARP packets are allowed to pass per second.

Format

arp anti-attack rate-limit *packet-number* [*interval-value*]

undo arp anti-attack rate-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum rate of sending ARP packets, that is, the number of ARP packets allowed to pass through in the rate limiting duration.	The value is an integer that ranges from 1 to 32768. The default value is 100.
interval-value	Specifies the rate limiting duration of ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, run the **arp anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP packets globally or on an interface. In the rate limiting duration, if the number of received ARP packets exceeds the limit, the device discards the excess ARP packets.

Prerequisites

Rate limit on ARP packets has been enabled globally or on an interface using the **arp anti-attack rate-limit enable** command.

Precautions

If the maximum rate and rate limiting duration are configured in the system view and interface view at the same time, the device uses the configurations in the interface view and system view in order.

Example

Configure Eth2/0/0 to allow 200 ARP packets to pass through in 10 seconds.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp anti-attack rate-limit enable
[Huawei-Ethernet2/0/0] arp anti-attack rate-limit 200 10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.11 arp anti-attack rate-limit alarm enable

Function

The **arp anti-attack rate-limit alarm enable** command enables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

The **undo arp anti-attack rate-limit alarm enable** command disables the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit.

By default, the alarm function for ARP packets discarded when the rate of ARP packets exceeds the limit is disabled.

Format

arp anti-attack rate-limit alarm enable

undo arp anti-attack rate-limit alarm enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP packets is enabled, if you want the device to generate alarms for excessive discarded ARP packets, run the **arp anti-attack rate-limit alarm enable** command. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After the **arp anti-attack rate-limit alarm enable** command is run, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

Example

Enable rate limit on ARP packets globally and enable the alarm function.

```
<Huawei> system-view
[Huawei] arp anti-attack rate-limit enable
[Huawei] arp anti-attack rate-limit alarm enable
```

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.12 arp anti-attack rate-limit alarm threshold

19.13.12 arp anti-attack rate-limit alarm threshold

Function

The **arp anti-attack rate-limit alarm threshold** command sets the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.

By default, the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit is 100.

Format

arp anti-attack rate-limit alarm threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold of ARP packets discarded when the rate of ARP packets exceeds the limit.	The value is an integer that ranges from 1 to 32768.

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can use the **arp anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP packets has been enabled using the **arp anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp anti-attack rate-limit alarm enable** command.

Example

Enable rate limit on ARP packets globally, enable the alarm function, and set the alarm threshold to 50.

```
<Huawei> system-view
[Huawei] arp anti-attack rate-limit enable
[Huawei] arp anti-attack rate-limit alarm enable
[Huawei] arp anti-attack rate-limit alarm threshold 50
```

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.11 arp anti-attack rate-limit alarm enable

19.13.13 arp anti-attack rate-limit enable

Function

The **arp anti-attack rate-limit enable** command enables rate limit on ARP packets.

The **undo arp anti-attack rate-limit enable** command disables rate limit on ARP packets.

By default, rate limiting on ARP packet is disabled.

Format

arp anti-attack rate-limit enable

undo arp anti-attack rate-limit enable

Parameters

None

Views

System view, Ethernet interface view, GE interface view, XGE interface view, port group view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

The device has no sufficient CPU resource to process other services when processing a large number of ARP packets. To protect CPU resources of the device, limit the rate of ARP packets.

You can run the **arp anti-attack rate-limit enable** command to enable rate limit on ARP packets. When the rate of ARP packets exceeds the limit, excess ARP packets are discarded. To set the rate limit and rate limiting duration of ARP packets, run the **arp anti-attack rate-limit** command.

Example

Enable rate limit on ARP packets globally.

```
<Huawei> system-view
[Huawei] arp anti-attack rate-limit enable
```

Related Topics

19.13.10 arp anti-attack rate-limit

19.13.14 arp gratuitous-arp send enable

Function

The **arp gratuitous-arp send enable** command enables gratuitous ARP packet sending.

The **undo arp gratuitous-arp send enable** command disables gratuitous ARP packet sending.

By default, gratuitous ARP packet sending is disabled.

Format

arp gratuitous-arp send enable

undo arp gratuitous-arp send enable

Parameters

None

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If an attacker forges the gateway address to send ARP packets to other user hosts, ARP entries on the hosts record the incorrect gateway address. As a result, the gateway cannot receive data sent from the hosts. You can enable gratuitous ARP packet sending on the gateway. Then the gateway sends gratuitous ARP packets at intervals to update the ARP entries of authorized users so that the ARP entries contain the correct MAC address of the gateway.

By default, the device sends a gratuitous ARP packet every 90 seconds after this function is enabled. You can also set the interval using the **arp gratuitous-arp send interval** command.

Precautions

After you run the **arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is enabled on all VLANIF interfaces. In addition, gratuitous ARP packet sending is enabled on all interfaces for the NAT address pool, NAT server, and public address for static NAT.

After you run the **undo arp gratuitous-arp send enable** command in the system view, gratuitous ARP packet sending is disabled on all VLANIF interfaces.

Example

Enable gratuitous ARP packet sending on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp gratuitous-arp send enable
```

Related Topics

19.13.15 arp gratuitous-arp send interval

19.13.15 arp gratuitous-arp send interval

Function

The **arp gratuitous-arp send interval** command sets the interval for sending gratuitous ARP packets.

The **undo arp gratuitous-arp send interval** command restores the default interval for sending gratuitous ARP packets.

By default, the interval for sending gratuitous ARP packets is 90 seconds.

Format

arp gratuitous-arp send interval *interval-time*

undo arp gratuitous-arp send interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval-time	Specifies the interval for sending gratuitous ARP packets.	The value is an integer that ranges from 1 to 86400, in seconds.

Views

System view, VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device sends a gratuitous ARP packet every 90 seconds after gratuitous ARP sending is enabled. You can set the interval for sending gratuitous ARP packets using the **arp gratuitous-arp send interval** command.

If you set the interval in the system view, the configuration takes effect on all VLANIF interfaces. If you set the interval in both the system view and VLANIF interface view, the configuration on the VLANIF interface takes precedence over the global configuration.

Prerequisites

Gratuitous ARP packet sending has been enabled using the **arp gratuitous-arp send enable** command.

Example

Set the interval for sending gratuitous ARP packets to 100 seconds on VLANIF 10.

```
<Huawei> system-view
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp gratuitous-arp send enable
[Huawei-Vlanif10] arp gratuitous-arp send interval 100
```

Related Topics

19.13.14 arp gratuitous-arp send enable

19.13.16 arp learning dhcp-trigger

Function

The **arp learning dhcp-trigger** command enables ARP learning triggered by DHCP.

 Copyright © Huawei Technologies Co., Ltd.

The **undo arp learning dhcp-trigger** command disables ARP learning triggered by DHCP.

By default, ARP learning triggered by DHCP is disabled.

Format

arp learning dhcp-trigger

undo arp learning dhcp-trigger

Parameters

None

Views

VLANIF interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When many DHCP users connect to a network device, the device needs to learn and maintain many ARP entries. This affects device performance.

To address this issue, configure ARP learning triggered by DHCP on the gateway. When the DHCP server allocates an IP address for a user, the gateway generates an ARP entry for the user based on the DHCP ACK packet received on the VLANIF interface.

Precautions

Before using this command, ensure that DHCP snooping is enabled using the **dhcp snooping enable** command.

When both VRRP and DHCP relay are configured on the network, neither the **dhcp snooping enable** command nor the **arp learning dhcp-trigger** command can be configured on the VRRP master and backup devices.

Example

Enable ARP learning triggered by DHCP on VLANIF 100.

```
<Huawei> system-view
[Huawei] vlan batch 100
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface vlanif 100
[Huawei-Vlanif100] arp learning dhcp-trigger
```

Related Topics

19.14.11 dhcp snooping enable

19.13.17 arp learning strict (interface view)

Function

The **arp learning strict** command enables strict ARP learning on the interface.

The **undo arp learning strict** command restores the global configuration on the interface.

By default, the configuration of strict ARP learning is the same as the global configuration.

Format

arp learning strict { **force-enable** | **force-disable** | **trust** }

undo arp learning strict

Parameters

Parameter	Description	Value
force-enable	Indicates that strict ARP learning is enabled.	-
force-disable	Indicates that strict ARP learning is disabled.	-
trust	Indicates that the configuration of strict ARP learning is the same as the global configuration. **NOTE** The effect of the **trust** parameter is the same as the effect of the **undo arp learning strict** command.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

 Copyright © Huawei Technologies Co., Ltd.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself, but does not allow the device to learn the ARP entries for the ARP packets received from other devices. In this way, the device can defend against most ARP attacks.

Precautions

The configuration on an interface takes precedence over the global configuration.

When ARP attacks occur on many interfaces of the device, you can run the **19.13.18 arp learning strict (system view)** command to enable strict ARP learning globally.

This command can be used only on Layer 3 interfaces.

Example

Enable strict ARP learning on VLANIF 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif 100
[Huawei-Vlanif100] arp learning strict force-enable
```

Related Topics

19.13.18 arp learning strict (system view)

19.13.34 display arp learning strict

19.13.18 arp learning strict (system view)

Function

The **arp learning strict** command enables strict ARP learning.

The **undo arp learning strict** command restores the default setting.

By default, strict ARP learning is disabled.

Format

arp learning strict

undo arp learning strict

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If many user hosts send a large number of ARP packets to a device simultaneously, or attackers send bogus ARP packets to the device, the following problems occur:

- Processing ARP packets consumes many CPU resources. The device learns many invalid ARP entries, which exhaust ARP entry resources and prevent the device from learning ARP entries for ARP packets from authorized users. Consequently, communication of authorized users is interrupted.
- After receiving bogus ARP packets, the device incorrectly modifies the ARP entries. As a result, authorized users cannot communicate with each other.

To avoid the preceding problems, enable strict ARP learning on the gateway. This function indicates that the device learns only ARP entries for ARP Reply packets in response to ARP Request packets sent by itself. In this way, the device can defend against most ARP attacks.

Precautions

The configuration on an interface takes precedence over the global configuration.

Example

Enable strict ARP learning.

```
<Huawei> system-view
[Huawei] arp learning strict
```

Related Topics

19.13.17 arp learning strict (interface view)

19.13.34 display arp learning strict

19.13.19 arp speed-limit flood-rate

Function

The **arp speed-limit flood-rate** command sets the maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs.

The **undo arp speed-limit flood-rate** command restores the default maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs.

By default, the maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs is 1000 pps.

Format

arp speed-limit flood-rate *rate*

 Copyright © Huawei Technologies Co., Ltd.

undo arp speed-limit flood-rate

Parameters

Parameter	Description	Value
rate	Specifies the maximum rate of broadcasting ARP Request packets.	The value is an integer that ranges from 0 to 32768, in pps. The value 0 indicates that the rate of broadcasting ARP packets is not limited.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A VLANIF interface in a super-VLAN is triggered to learn ARP entries in the following scenarios:

- The VLANIF interface receives IP packets triggering ARP Miss messages.
- The VLANIF interface is enabled with ARP proxy and receives ARP packets whose destination IP addresses meet the proxy requirements and match no ARP entry.

The VLANIF interface replicates ARP Request packets in each sub-VLAN when learning ARP entries. If a large number of sub-VLANs are configured for the super-VLAN, the device generates a large number of ARP Request packets. As a result, the CPU is busy processing ARP Request packets, and other services are affected. To prevent this problem, limit the rate of ARP packets on the VLANIF interface of a super-VLAN.

When the CPU is busy processing packets, set the maximum rate of broadcasting ARP Request packets to a small value. When the CPU is idle, set the maximum rate of broadcasting ARP Request packets to a large value to broadcast packets efficiently. You can set the maximum rate of broadcasting ARP Request packets based on the actual network environment.

Example

Set the maximum rate of broadcasting ARP Request packets on VLANIF interfaces in all super-VLANs to 500 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit flood-rate 500
```

Related Topics

19.13.33 display arp flood statistics

19.13.20 arp speed-limit source-mac

Function

The **arp speed-limit source-mac** command sets the maximum rate of ARP packets based on source MAC addresses.

The **undo arp speed-limit source-mac** command restores the default setting.

By default, the maximum rate of ARP packets from each source MAC address is set to 0, that is, the rate of ARP packets is not limited based on source MAC addresses.

Format

arp speed-limit source-mac [*mac-address*] **maximum** *maximum*

undo arp speed-limit source-mac [*mac-address*]

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address. If this parameter is specified, the rate of ARP packets from the MAC address is limited. If this parameter is not specified, the rate of ARP packets from each MAC address is limited.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified MAC address.	The value is an integer that ranges from 0 to 32768, in pps.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed source MAC addresses but variable source IP addresses, the CPU is overloaded and ARP entries are exhausted. To prevent this problem, limit the rate of ARP packets based on source MAC addresses.

 Copyright © Huawei Technologies Co., Ltd.

After the **arp speed-limit source-mac** command is run, the device collects statistics on ARP packets from a specified source MAC address. If the number of ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source MAC address.

Example

Set the maximum rate of ARP packets from any source MAC address to 100 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit source-mac maximum 100
```

Set the maximum rate of ARP packets from a specified MAC address 0000-0000-0001 to 50 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit source-mac 0000-0000-0001 maximum 50
```

Related Topics

19.13.21 arp speed-limit source-ip
19.13.31 display arp anti-attack configuration

19.13.21 arp speed-limit source-ip

Function

The **arp speed-limit source-ip** command sets the maximum rate of ARP packets based on the source IP address.

The **undo arp speed-limit source-ip** command restores the default setting.

By default, the device allows a maximum of 5 ARP packets from the same source IP address to pass through per second.

Format

arp speed-limit source-ip [*ip-address*] **maximum** *maximum*

undo arp speed-limit source-ip [*ip-address*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the rate of ARP packets from the IP address is limited. If this parameter is not specified, the rate of ARP packets from each IP address is limited.	The value is in dotted decimal notation.
maximum *maximum*	Specifies the maximum rate of ARP packets from a specified source IP address. **NOTE** If the rate of all ARP packets is limited, a large value is recommended because valid packets may be discarded if the value is small. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The value is an integer that ranges from 0 to 32768, in pps. If the value is 0, the rate of ARP packets is not limited based on the source IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When processing a large number of ARP packets with fixed IP addresses (for example, the ARP packets with the same source IP addresses but frequently changing MAC addresses or outbound interfaces), the CPU is overloaded and cannot process other services. To prevent this problem, limit the rate of ARP packets based on the source IP address.

After the **arp speed-limit source-ip** command is run, the device collects statistics on ARP packets based on the source IP address. If the number of ARP packets from a specified source IP address per second exceeds the threshold, the device discards the excess ARP packets.

Precautions

Limiting the rate of all ARP packets is not recommended. You are advised to find out the attack source according to packet statistics, and then limit the rate of ARP packets from the specified source IP address.

Example

Set the maximum rate of ARP packets from a source IP address to 100 pps.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] arp speed-limit source-ip maximum 100
```

Set the maximum rate of ARP packets from a specified IP address 10.0.0.1 to 50 pps.

```
<Huawei> system-view
[Huawei] arp speed-limit source-ip 10.0.0.1 maximum 50
```

Related Topics

19.13.20 arp speed-limit source-mac
19.13.31 display arp anti-attack configuration

19.13.22 arp validate (interface view)

Function

The **arp validate** command enables MAC address consistency check in an ARP packet on an interface. This function compares the source and destination MAC addresses in ARP packets with those in the Ethernet frame header.

The **undo arp validate** command disables MAC address consistency check in an ARP packet on an interface.

By default, MAC address consistency check in an ARP packet is disabled.

Format

arp validate { **source-mac** | **destination-mac** } *

undo arp validate { **source-mac** | **destination-mac** } *

Parameters

Parameter	Description	Value
source-mac	Indicates that the device compares the source MAC address in a received ARP packet with that in the Ethernet frame header.	-
destination-mac	Indicates that the device compares the destination MAC address in a received ARP packet with that in the Ethernet frame header.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The MAC address consistency check function for ARP packets prevents attacks from bogus ARP packets in which the source and destination MAC addresses are different from those in the Ethernet frame header. This function is usually configured on gateways.

After the **arp validate** command is run, the gateway checks the MAC address consistency in an ARP packet before ARP learning. If the source and destination MAC addresses in an ARP packet are different from those in the Ethernet frame header, the device discards the packet as an attack. If the source and destination MAC addresses in an ARP packet are the same as those in the Ethernet frame header, the device performs ARP learning.

When using this command, note the following points:

- If **source-mac** is specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks only the source MAC address consistency.
- If **destination-mac** is specified:
  - When receiving an ARP Request packet, the device does not check the destination MAC address consistency because the ARP Request packet is broadcast.
  - When receiving an ARP Reply packet, the device checks the destination MAC address consistency.
- If **source-mac** and **destination-mac** are specified:
  - When receiving an ARP Request packet, the device checks only the source MAC address consistency.
  - When receiving an ARP Reply packet, the device checks the source and destination MAC address consistency.

Precautions

Sub-interfaces do not support the **arp validate** command. When receiving ARP packets, a sub-interface checks MAC address consistency based on the rule configured on the primary interface.

Example

Enable MAC address consistency check in an ARP packet on Layer 2 interface Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp validate source-mac destination-mac
```

19.13.23 arp-fake expire-time

Function

The **arp-fake expire-time** command sets the aging time of temporary ARP entries.

The **undo arp-fake expire-time** command restores the default aging time of temporary ARP entries.

By default, the aging time of temporary ARP entries is 1 second.

Format

arp-fake expire-time *expire-time*

undo arp-fake expire-time

Parameters

Parameter	Description	Value
expire-time	Specifies the aging time of temporary ARP entries.	The value is an integer that ranges from 1 to 36000, in seconds.

Views

Ethernet interface view, GE interface view, XGE interface view, Eth-Trunk interface view, VLANIF interface view, port group view, virtual ethernet interface view

Default Level

2: Configuration level

Usage Guidelines

When IP packets trigger ARP Miss messages, the device generates temporary ARP entries and sends ARP Request packets to the destination network.

- In the aging time of temporary ARP entries:
  - Before receiving an ARP reply packet, the device discards the IP packets matching the temporary ARP entry and does not generate ARP Miss messages.
  - After receiving an ARP Reply packet, the device generates a correct ARP entry to replace the temporary entry.
- When temporary ARP entries age out, the device clears them. If no ARP entry matches the IP packets forwarded by the device, ARP Miss messages and temporary ARP entries are repeatedly generated

When a device undergoes an ARP Miss attack, you can run the **arp-fake expire-time** command to extend the aging time of temporary ARP entries to reduce the frequency of triggering ARP Miss messages and minimize the impact on the device.

Example

Set the aging time of temporary ARP entries to 10 seconds on VLANIF10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-fake expire-time 10
```

19.13.24 arp-limit

Function

The **arp-limit** command sets the maximum number of ARP entries that an interface can dynamically learn.

The **undo arp-limit** command deletes the maximum number of ARP entries that an interface can dynamically learn.

By default, the maximum number of ARP entries that an interface can dynamically learn is the maximum value that can be configured on the interface.

Format

VLANIF interface view

arp-limit maximum *maximum*

undo arp-limit

Other interface views

arp-limit vlan *vlan-id1* [**to** *vlan-id2*] **maximum** *maximum*

undo arp-limit vlan *vlan-id1* [**to** *vlan-id2*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan *vlan-id1* [**to** *vlan-id2*]	Specifies the ID of a VLAN from which the maximum number of ARP entries an interface can dynamically learn is limited. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*. *vlan-id1* and *vlan-id2* specify a range of VLANs. If **to** *vlan-id2* is not specified, the device limits the maximum number of ARP entries an interface dynamically learns from the VLAN *vlan-id1*. If **to** *vlan-id2* is specified, the device limits the maximum number of ARP entries an interface dynamically learns from	The values of *vlan-id1* and *vlan-id2* are integers that range from 1 to 4094.

Parameter	Description	Value
	each VLAN from *vlan-id1* to *vlan-id2*.	
maximum *maximum*	Specifies the maximum number of ARP entries that an interface can dynamically learn.	The value is an integer and the value range varies according to product models: ● AR100&AR120&AR150&AR160&AR200&AR1200 series: 1 to 2000 ● AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204E, AR2204-51GE, AR2204-51GE-R, AR2204E-D and AR2204: 1 to 2000 ● AR2204XE, AR2204XE-DC, AR2220, AR2220E: 1 to 4000 ● AR2240 and AR2240C: 1 to 4000 ● AR3200 and AR3600 series: 1 to 4000 .

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent ARP entries from being exhausted by ARP attacks from a host connecting to an interface on the device, set the maximum number of ARP entries that the interface can dynamically learn. When the number of the ARP entries learned by a specified interface reaches the maximum number, no dynamic ARP entry can be added.

Precautions

If the number of ARP entries learned by an interface exceeds the maximum number, the device neither learns new ARP entries nor clears the learned ARP entries. Instead, the device asks users to delete the excess ARP entries.

 Copyright © Huawei Technologies Co., Ltd.

Ethernet, GE, VE, Eth-Trunk interfaces can work at Layer 3 or Layer 2. When they work at Layer 3, you cannot configure the VLAN ID. When they work at Layer 2, you must configure the VLAN ID.

If the **arp-limit vlan** *vlan-id1* **to** *vlan-id2* **maximum** *maximum* command is run more than once, the following situations are available:

- If **maximum** *maximum* is the same in multiple command instances, all configurations take effect. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 35 to 40 maximum 200** command are run, both configurations take effect. If the VLAN ranges specified in multiple command instances are overlapping, the system automatically merges the VLAN ranges. For example, if the **arp-limit vlan 50 to 80 maximum 200** command and then the **arp-limit vlan 70 to 100 maximum 200** command are run, both configurations take effect, and the system merges the configurations into **arp-limit vlan 50 to 100 maximum 200**.
- If **maximum** *maximum* is different in multiple command instances, the latest configuration overrides the previous one for the same VLAN range. For example, if the **arp-limit vlan 10 to 30 maximum 200** command and then the **arp-limit vlan 15 to 25 maximum 300** command are run, the system automatically divides the configurations into **arp-limit vlan 10 to 14 maximum 200**, **arp-limit vlan 15 to 25 maximum 300**, and **arp-limit vlan 26 to 30 maximum 200**.

Example

Configure that VLANIF 10 can dynamically learn a maximum of 20 ARP entries.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] quit
[Huawei] interface vlanif 10
[Huawei-Vlanif10] arp-limit maximum 20
```

Configure that Eth2/0/0 can dynamically learn a maximum of 20 ARP entries corresponding to VLAN 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] arp-limit vlan 10 maximum 20
```

Related Topics

19.13.36 display arp-limit

19.13.25 arp-miss anti-attack rate-limit

Function

The **arp-miss anti-attack rate-limit** command sets the maximum rate and rate limiting duration of ARP Miss messages.

The **undo arp-miss anti-attack rate-limit** command restores the default maximum rate and rate limiting duration of ARP Miss messages.

By default, the device can process a maximum of 100 ARP Miss messages per second.

Format

arp-miss anti-attack rate-limit *packet-number* [*interval-value*]

undo arp-miss anti-attack rate-limit

Parameters

Parameter	Description	Value
packet-number	Specifies the maximum rate of ARP Miss messages, that is, the number of ARP Miss messages the device processes in the rate limiting duration.	The value is an integer that ranges from 1 to 32768. The default value is 100.
interval-value	Specifies the rate limiting duration of ARP Miss messages.	The value is an integer that ranges from 1 to 86400, in seconds. The default value is 1 second.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, you can set maximum rate and rate limiting duration of ARP Miss messages. If the number of ARP Miss messages triggered by IP packets in the rate limiting duration exceeds the limit, the device does not process the excess ARP Miss packets and discards the IP packets triggering the excess ARP Miss messages.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command.

Example

Configure the device to process a maximum of 200 ARP Miss messages in 10 seconds.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
[Huawei] arp-miss anti-attack rate-limit 200 10
```

Related Topics

19.13.28 arp-miss anti-attack rate-limit enable

19.13.26 arp-miss anti-attack rate-limit alarm enable

Function

The **arp-miss anti-attack rate-limit alarm enable** command enables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

The **undo arp-miss anti-attack rate-limit alarm enable** command disables the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

By default, the alarm function is disabled.

Format

arp-miss anti-attack rate-limit alarm enable

undo arp-miss anti-attack rate-limit alarm enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After rate limit on ARP Miss messages is enabled, if you want that the device can generate alarms to notify the network administrator of a large number of discarded excess ARP Miss messages, run the **arp-miss anti-attack rate-limit alarm enable** command. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

You can set the alarm threshold using the **arp-miss anti-attack rate-limit alarm threshold** command.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

After the **arp-miss anti-attack rate-limit alarm enable** command is run, you need to run the **arp anti-attack log-trap-timer** *time* command to set the interval for sending alarms.

Example

Enable the alarm function for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
[Huawei] arp-miss anti-attack rate-limit alarm enable
```

Related Topics

19.13.25 arp-miss anti-attack rate-limit

19.13.27 arp-miss anti-attack rate-limit alarm threshold

19.13.28 arp-miss anti-attack rate-limit enable

19.13.27 arp-miss anti-attack rate-limit alarm threshold

Function

The **arp-miss anti-attack rate-limit alarm threshold** command sets the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss packets exceeds the limit.

By default, the alarm threshold for ARP Miss packets discarded is 100.

Format

arp-miss anti-attack rate-limit alarm threshold *threshold*

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for ARP Miss messages discarded when the rate of ARP Miss messages exceeds the limit.	The value is an integer that ranges from 1 to 32768.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can use the **arp-miss anti-attack rate-limit alarm threshold** command to set the alarm threshold. When the number of discarded ARP Miss packets exceeds the alarm threshold, the device generates an alarm.

Prerequisites

Rate limit on ARP Miss messages has been enabled using the **arp-miss anti-attack rate-limit enable** command, and the alarm function has been enabled using the **arp-miss anti-attack rate-limit alarm enable** command.

Example

Enable rate limit on ARP Miss messages, enable the alarm function, and set the alarm threshold to 200.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
[Huawei] arp-miss anti-attack rate-limit alarm enable
[Huawei] arp-miss anti-attack rate-limit alarm threshold 200
```

Related Topics

19.13.25 arp-miss anti-attack rate-limit

19.13.26 arp-miss anti-attack rate-limit alarm enable

19.13.28 arp-miss anti-attack rate-limit enable

19.13.28 arp-miss anti-attack rate-limit enable

Function

The **arp-miss anti-attack rate-limit enable** command enables rate limit on ARP Miss messages.

The **undo arp-miss anti-attack rate-limit enable** command disables rate limit on ARP Miss messages.

By default, rate limit on ARP Miss messages is disabled.

Format

arp-miss anti-attack rate-limit enable

undo arp-miss anti-attack rate-limit enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a host sends a large number of IP packets with unresolvable destination IP addresses to attack a device, that is, if the device has a route to the destination IP address of a packet but has no ARP entry matching the next hop of the route, the device triggers a large number of ARP Miss messages. IP packets triggering ARP Miss messages are sent to the control board for processing. The device generates a large number of temporary ARP entries and sends many ARP Request packets to the network, consuming a large number of CPU and bandwidth resources.

To avoid the preceding problems, configure rate limit on ARP Miss messages. The device collects statistics on ARP Miss messages. If the number of ARP Miss messages generated within the rate limiting duration exceeds the threshold (the maximum number of ARP Miss messages), the gateway discards the IP packets triggering the excess ARP Miss messages.

Follow-up Procedure

Run the **arp-miss anti-attack rate-limit** command to set the maximum rate and rate limiting duration of ARP Miss messages.

Example

Enable rate limit on ARP Miss messages.

```
<Huawei> system-view
[Huawei] arp-miss anti-attack rate-limit enable
```

Related Topics

19.13.25 arp-miss anti-attack rate-limit

19.13.29 arp-miss speed-limit source-ip

Function

The **arp-miss speed-limit source-ip** command sets the maximum number of ARP Miss messages based on source IP addresses.

The **undo arp-miss speed-limit source-ip** command restores the default setting.

By default, the device processes a maximum of 5 ARP Miss messages triggered by IP packets from the same source IP address per second.

Format

arp-miss speed-limit source-ip [*ip-address*] **maximum** *maximum*

undo arp-miss speed-limit source-ip [*ip-address*]

Parameters

Parameter	Description	Value
ip-address	Specifies the source IP address. If this parameter is specified, the maximum number of ARP Miss messages triggered by packets from this IP address is limited. If this parameter is not specified, the maximum number of ARP Miss messages triggered by packets from each IP address is limited.	The value is in dotted decimal notation.
maximum *maximum*	Specifies the maximum number of ARP Miss messages based on the source IP address. **NOTE** If the maximum number of ARP Miss messages triggered by packets from each IP address is limited, a large value is recommended for this parameter because a small value may cause discarding of valid packets. However, a too large value will deteriorate the system performance. If an IP address initiates attacks, you can set the maximum number of ARP Miss messages triggered by packets from this IP address to a small value.	The value is an integer that ranges from 0 to 32768. If the value is 0, the maximum number of ARP Miss messages is not limited based on the source IP address.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If the number of ARP Miss messages triggered by IP packets from a source IP address per second exceeds the limit, the device considers that an attack is initiated from the source IP address. The administrator can use the **arp-miss speed-limit source-ip** command to set the maximum number of ARP Miss messages that the device can process within a specified duration, protecting the system resources and ensuring proper running of other services.

Example

Set the maximum number of ARP Miss messages triggered by each source IP address per second to 60.

```
<Huawei> system-view
[Huawei] arp-miss speed-limit source-ip maximum 60
```

Set the maximum number of ARP Miss messages triggered by the IP address 10.0.0.1 per second to 100, and set the maximum number of ARP Miss messages triggered by other source IP addresses per second to 60.

```
<Huawei> system-view
[Huawei] arp-miss speed-limit source-ip maximum 60
[Huawei] arp-miss speed-limit source-ip 10.0.0.1 maximum 100
```

Related Topics

19.13.31 display arp anti-attack configuration

19.13.30 display arp anti-attack check user-bind interface

Function

The **display arp anti-attack check user-bind interface** command displays the configuration of ARP packet check on an interface.

Format

display arp anti-attack check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface where ARP packets are checked. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display arp anti-attack check user-bind interface** command to view the configuration of ARP packet check on an interface, including whether the

function is enabled, check items, whether the alarm function is enabled for discarded ARP packets, alarm threshold, and number of discarded ARP packets.

Only after DAI and the alarm function are enabled, output of this command is displayed.

Example

Display ARP check configuration on Eth2/0/0.

```
<Huawei> display arp anti-attack check user-bind interface ethernet 2/0/0
 arp anti-attack check user-bind enable
 arp anti-attack check user-bind alarm enable
 arp anti-attack check user-bind alarm threshold 50
 ARP packet drop count = 0
```

Table 19-141 Description of the **display arp anti-attack check user-bind interface** command output

Item	Description
arp anti-attack check user-bind enable	DAI has been enabled on an interface. You can run the **19.13.5 arp anti-attack check user-bind enable** command to enable DAI.
arp anti-attack check user-bind alarm enable	The alarm function for ARP packets discarded by DAI has been enabled. You can run the **19.13.1 arp anti-attack check user-bind alarm enable** command to enable the alarm function.
arp anti-attack check user-bind alarm threshold 50	Alarm threshold of discarded ARP packets matching no DHCP snooping binding entry. You can run the **19.13.2 arp anti-attack check user-bind alarm threshold** command to set the alarm threshold.
ARP packet drop count	Number of discarded ARP packets matching no DHCP snooping binding entry.

Related Topics

19.13.5 arp anti-attack check user-bind enable

19.13.1 arp anti-attack check user-bind alarm enable

19.13.2 arp anti-attack check user-bind alarm threshold

19.13.31 display arp anti-attack configuration

Function

The **display arp anti-attack configuration** command displays the ARP anti-attack configuration.

Format

display arp anti-attack configuration { **arp-rate-limit** | **arpmiss-rate-limit** | **arp-speed-limit** | **arpmiss-speed-limit** | **entry-check** | **gateway-duplicate** | **packet-check** | **all** }

Parameters

Parameter	Description	Value
arp-rate-limit	Displays the configuration of rate limit on ARP packets globally or on an interface.	-
arpmiss-rate-limit	Displays the configuration of rate limit on ARP Miss messages.	-
arp-speed-limit	Displays the configuration of rate limit on ARP packets based on the source IP address or source MAC address.	-
arpmiss-speed-limit	Displays the configuration of rate limit on ARP Miss messages based on the source IP address.	-
entry-check	Displays the ARP entry fixing mode.	-
gateway-duplicate	Displays whether gateway anti-collision is enabled.	-
packet-check	Displays whether ARP packet validity check is enabled.	-
all	Displays all ARP anti-attack configurations.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After all ARP anti-attack functions are configured, you can run this command to check all configurations.

Example

Display the maximum rate and rate limiting duration of ARP packets based on the source IP address or source MAC address.

```
<Huawei> display arp anti-attack configuration arp-speed-limit
 ARP speed-limit for source-MAC configuration:
 MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 0000-0000-0001      150
 Others              200
-------------------------------------------------------------------------------
 1 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 10.0.0.20           50
 Others              100
-------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 512 items.
```

Display the maximum rate and rate limiting duration of ARP Miss messages based on the source IP address.

```
<Huawei> display arp anti-attack configuration arpmiss-speed-limit
 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 10.0.0.20           300
 Others              100
-------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.
```

Display the ARP entry fixing mode.

```
<Huawei> display arp anti-attack configuration entry-check
 ARP anti-attack entry-check mode: fixed-mac
```

Display all ARP anti-attack configurations.

```
<Huawei> display arp anti-attack configuration all
 ARP anti-attack packet-check function: enable

 ARP anti-attack entry-check mode: disabled

 ARP gateway-duplicate anti-attack function: disabled

 ARP rate-limit configuration:
-------------------------------------------------------------------------------
 Global configuration:
    arp anti-attack rate-limit enable
 Interface configuration:
-------------------------------------------------------------------------------

 ARP miss rate-limit configuration:
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------
 Global configuration:
   arp-miss anti-attack rate-limit enable
-------------------------------------------------------------------------------

 ARP speed-limit for source-MAC configuration:
 MAC-address         suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 0000-0000-0001      200
 Others              100
-------------------------------------------------------------------------------
 1 specified MAC addresses are configured, spec is 256 items.

 ARP speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 10.0.0.1            512
 Others              126
-------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.

 ARP miss speed-limit for source-IP configuration:
 IP-address          suppress-rate(pps)(rate=0 means function disabled)
-------------------------------------------------------------------------------
 10.134.23.6         400
 Others              500
-------------------------------------------------------------------------------
 1 specified IP addresses are configured, spec is 128 items.
```

Table 19-142 Description of the display arp anti-attack configuration command output

Item	Description
ARP speed-limit for source-MAC configuration	Rate limit on ARP packets based on the source MAC address. You can run the **19.13.20 arp speed-limit source-mac** command to configure rate limit on ARP packets based on the source MAC address.
ARP speed-limit for source-IP configuration	Rate limit on ARP packets based on the source IP address. You can run the **19.13.21 arp speed-limit source-ip** command to configure rate limit on ARP packets based on the source IP address.
ARP anti-attack packet-check function	Whether MAC address consistency check in an ARP packet is enabled. You can run the **19.13.9 arp anti-attack packet-check sender-mac** command to enable MAC address consistency check in an ARP packet.
ARP miss speed-limit for source-IP configuration	Rate limit on ARP Miss messages based on source IP addresses. You can run the **19.13.29 arp-miss speed-limit source-ip** command to configure rate limit on ARP Miss messages based on the source IP address.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ARP anti-attack entry-check mode	ARP entry fixing mode. You can run the **19.13.6 arp anti-attack entry-check enable** command to set the ARP entry fixing mode.
ARP gateway-duplicate anti-attack function:	Whether ARP gateway anti-collision is enabled. You can run the **19.13.7 arp anti-attack gateway-duplicate enable** command to enable ARP gateway anti-collision.
ARP rate-limit configuration	Configuration of rate limit on ARP packets. • **Global configuration** indicates the global configuration of rate limit on ARP packets. • **Interface configuration** indicates the configuration of rate limit on ARP packets on an interface. You can run the **19.13.10 arp anti-attack rate-limit** command to configure rate limit on ARP packets.
ARP miss rate-limit configuration	Configuration of rate limit on ARP Miss messages. **Global configuration** indicates the global configuration of rate limit on ARP Miss messages. You can run the **19.13.25 arp-miss anti-attack rate-limit** command to configure rate limit on ARP Miss messages.
MAC-address	Rate limit on ARP packets based on a specified MAC address. • **ALL** indicates all MAC addresses. • **Others** indicates other MAC addresses except for the specified MAC address.
IP-address	Rate limit on ARP packets and ARP Miss messages based on a specified IP address. • **ALL** indicates all IP addresses. • **Others** indicates other IP addresses except for the specified IP address.
suppress-rate	Rate limit on ARP packets and ARP Miss messages.

Related Topics

19.13.6 arp anti-attack entry-check enable
19.13.7 arp anti-attack gateway-duplicate enable
19.13.21 arp speed-limit source-ip
19.13.29 arp-miss speed-limit source-ip
19.13.9 arp anti-attack packet-check sender-mac
19.13.25 arp-miss anti-attack rate-limit

 Copyright © Huawei Technologies Co., Ltd.

19.13.10 arp anti-attack rate-limit

19.13.32 display arp anti-attack gateway-duplicate item

Function

The **display arp anti-attack gateway-duplicate item** command displays ARP gateway anti-collision entries.

Format

display arp anti-attack gateway-duplicate item

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After ARP gateway anti-collision is enabled, you can run this command to view ARP anti-collision entries.

Example

Display ARP gateway anti-collision entries.

```
<Huawei> display arp anti-attack gateway-duplicate item
 interface            IP address      MAC address     VLANID   aging time
--------------------------------------------------------------------------------
 Ethernet2/0/0        10.1.1.1        0000-0000-0002  2        150
 Ethernet2/0/1        10.1.1.2        0000-0000-0004  2        170
--------------------------------------------------------------------------------
The number of record(s) in gateway conflict table is 2
```

Table 19-143 Description of the display arp anti-attack gateway-duplicate item command output

Item	Description
interface	Inbound interface of ARP packets.
IP address	IP address of the gateway.
MAC address	Source MAC address of ARP packets.
VLANID	VLAN ID of ARP packets.

Item	Description
aging time	Aging time of entries.

Related Topics

19.13.7 arp anti-attack gateway-duplicate enable

19.13.33 display arp flood statistics

Function

The **display arp flood statistics** command displays the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs.

Format

display arp flood statistics

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

You can run this command to view the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs.

Example

Display the statistics on ARP Request packets of all the VLANIF interfaces in a super-VLAN.

```
<Huawei> display arp flood statistics
ARP request packets statistics on supervlan:
Total ARP request packets number :  5100
Sent ARP request packets number :  4000
Dropped ARP request packets number:  1100
```

 Copyright © Huawei Technologies Co., Ltd.

Table 19-144 Description of the display arp flood statistics command output

Item	Description
ARP request packets statistics on supervlan	Statistics on ARP Request packets in all super-VLANs.
Total ARP request packets number	Total number of ARP Request packets.
Sent ARP request packets number	Number of sent ARP Request packets.
Dropped ARP request packets number	Number of discarded ARP Request packets when the rate limit on broadcasting ARP Request packets is exceeded on VLANIF interface in all super-VLANs.

Related Topics

19.13.19 arp speed-limit flood-rate

19.13.34 display arp learning strict

Function

The **display arp learning strict** command displays strict ARP learning globally and on all interfaces.

Format

display arp learning strict

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After strict ARP learning is configured, you can run this command to check the configuration.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display strict ARP learning globally and on all interfaces.

```
<Huawei> display arp learning strict
The global configuration:arp learning strict
 Interface                    LearningStrictState
-------------------------------------------------------------
 Vlanif100                     force-disable
 Vlanif200                     force-enable
-------------------------------------------------------------
 Total:2
 Force-enable:1
 Force-disable:1
```

Table 19-145 Description of the display arp learning strict command output

Item	Description
The global configuration	Global strict ARP learning. The value **arp learning strict** indicates that strict ARP learning has been enabled. If the parameter is left blank, strict ARP learning is disabled. You can run the **19.13.18 arp learning strict (system view)** command to enable strict ARP learning.
Interface	Interface name.
LearningStrictState	Strict ARP learning. • The value **force-enable** indicates that strict ARP learning is enabled. • The value **force-disable** indicates that strict ARP learning is disabled. You can run the **19.13.17 arp learning strict (interface view)** command to enable strict ARP learning.
Total	Total number of interfaces to which strict ARP learning is applied.
Force-enable	Number of the interfaces on which strict ARP learning is enabled.
Force-disable	Number of the interfaces on which strict ARP learning is disabled.

Related Topics

19.13.18 arp learning strict (system view)

19.13.17 arp learning strict (interface view)

19.13.35 display arp packet statistics

Function

The **display arp packet statistics** command displays the statistics on ARP packets.

Format

display arp packet statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To locate and rectify ARP faults, you can run this command to the statistics on ARP packets.

Example

Display the statistics on ARP packets.

```
<Huawei> display arp packet statistics
ARP Pkt Received:   sum  10088
ARP Learnt Count:   sum     52
ARP Pkt Discard For Limit:   sum      0
ARP Pkt Discard For SpeedLimit:   sum     31
ARP Pkt Discard For Proxy Suppress:   sum    307
ARP Pkt Discard For Other:   sum   9274
```

Table 19-146 Description of the display arp packet statistics command output

Item	Description
ARP Pkt Received	Number of the received ARP packets.
ARP Learnt Count	Times of ARP learning.
ARP Pkt Discard For Limit	Number of ARP packets discarded due to the ARP entry limit.
ARP Pkt Discard For SpeedLimit	Number of ARP packets discarded when the number of ARP packets from a specified source IP address exceeds the limit.
ARP Pkt Discard For Proxy Suppress	Number of packets discarded for the speed limit.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
ARP Pkt Discard For Other	Number of the packets discarded due to other causes.

19.13.36 display arp-limit

Function

The **display arp-limit** command displays the maximum number of ARP entries that an interface can dynamically learn.

Format

display arp-limit [**interface** *interface-type interface-number*] [**vlan** *vlan-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Specifies a VLAN ID. This parameter is available only for Layer 2 interfaces.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the maximum number of ARP entries that an interface can dynamically learn is set, you can run this command to check the configuration.

If **interface** *interface-type interface-number* and **vlan** *vlan-id* are specified, you can view the maximum number of ARP entries that the specified interface can

dynamically learn in the specified VLAN. If the two parameters are not specified, the maximum number of ARP entries that each interface can dynamically learn is displayed.

Example

Display the number of ARP entries that each interface can dynamically learn.

```
<Huawei> display arp-limit
 Interface             LimitNum       VlanID         LearnedNum(Mainboard)
-------------------------------------------------------------------------------
 Vlanif100             1000           0              0
 Ethernet2/0/0         16384          10             0
-------------------------------------------------------------------------------
 Total:2
```

Table 19-147 Description of the display arp-limit command output

Item	Description
Interface	Interface name.
LimitNum	Maximum number of ARP entries that an interface can dynamically learn.
VlanID	ID of the VLAN that the interface belongs to.
LearnedNum(Mainboard)	Number of ARP entries that an interface has learned.

Related Topics

19.13.24 arp-limit

19.13.37 reset arp anti-attack statistics check user-bind

Function

The **reset arp anti-attack statistics check user-bind** command clears the statistics on discarded ARP packets matching no binding entry.

Format

reset arp anti-attack statistics check user-bind interface *interface-type interface-number*

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After DAI is enabled and some ARP packets matching no binding entry are discarded, you can run this command to clear the statistics on the discarded ARP packets.

Example

Clear the statistics on discarded ARP packets on Eth2/0/0.

```
<Huawei> reset arp anti-attack statistics check user-bind interface ethernet 2/0/0
```

Related Topics

19.13.5 arp anti-attack check user-bind enable

19.13.38 reset arp anti-attack statistics rate-limit

Function

The **reset arp anti-attack statistics rate-limit** command clears the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit.

Format

reset arp anti-attack statistics rate-limit { **global** | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
global	Indicates that statistics on discarded ARP packets are cleared globally.	-
interface *interface-type interface-number*	Specifies the interface type and number. Where, • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

After rate limit on ARP packets is enabled, the device discards the excess packets when the rate of ARP packets exceeds the limit. You can run this command to clear the statistics on the discarded ARP packets.

Example

Clear the statistics on ARP packets discarded when the rate of ARP packets exceeds the limit globally.

```
<Huawei> reset arp anti-attack statistics rate-limit global
```

Related Topics

19.13.13 arp anti-attack rate-limit enable

19.13.39 reset arp flood statistics

Function

The **reset arp flood statistics** command clears the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs.

Format

reset arp flood statistics

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

After this command is run, the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs are cleared and cannot be restored.

Example

Clear the statistics on ARP Request packets of VLANIF interfaces in all super-VLANs is cleared.

```
<Huawei> reset arp flood statistics
```

Related Topics

19.13.19 arp speed-limit flood-rate

19.13.40 reset arp packet statistics

Function

The **reset arp packet statistics** command clears the statistics on ARP packets.

Format

reset arp packet statistics

Parameters

None

Views

User view

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display arp packet statistics** command to display the statistics on ARP packets. To obtain correct statistics, run the **reset arp packet statistics** command to clear existing statistics first.

The **reset arp packet statistics** command clears the ARP packet statistics only on the main control board.

Example

Clear the statistics on all ARP packets.

```
<Huawei> reset arp packet statistics
```

19.14 DHCP Snooping Configuration Commands

NOTE

- The 4GE-2S, 4ES2GP-S, 4ES2G-S, and 9ES2 cards do not support DHCP snooping.
- AR100&AR120&AR150&AR160&AR200&AR1200 series do not support DHCPv6 snooping.
- The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the following commands:
  - **19.14.14 dhcp snooping trusted**
  - **19.14.16 dhcp snooping user-bind autosave**
  - **8.9.9 dhcpv6 interface-id format**
  - **19.14.19 dhcpv6 option18 format**
  - **19.14.20 dhcpv6 option37 format**
  - **19.14.21 dhcpv6 { option18 | option37 } enable**
  - **19.14.22 dhcpv6 snooping relay-information enable**
  - **19.14.28 display dhcpv6 snooping user-bind**

19.14.1 arp dhcp-snooping-detect enable

Function

The **arp dhcp-snooping-detect enable** command enables association between the Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) snooping.

The **undo arp dhcp-snooping-detect enable** command disables association between ARP and DHCP snooping.

By default, association between ARP and DHCP snooping is disabled.

Format

arp dhcp-snooping-detect enable

undo arp dhcp-snooping-detect enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP client sends a DHCP Release message to release its IP address, the DHCP snooping-enabled device immediately deletes the binding entry of the DHCP client. If a DHCP client is abnormally disconnected and cannot send a DHCP Release message, the DHCP snooping-enabled device cannot immediately delete the binding entry of the DHCP client.

If association between ARP and DHCP snooping is enabled using this command and no ARP entry corresponding to the IP address in the DHCP snooping binding entry is found, the DHCP snooping-enabled device performs an ARP probe on the IP address. If no user is detected for consecutive four times, the DHCP snooping-enabled device deletes the DHCP snooping binding entry corresponding to the IP address. (The probe interval is 20 seconds, and the probe times and probe interval are fixed values and cannot be modified.) If the DHCP snooping-enabled device supports the DHCP relay function, this device then sends a DHCP Release message in place of the DHCP client to notify the DHCP server to release the IP address.

Prerequisites

Before association between the ARP and DHCP snooping is enabled, ensure that an IP address configured on the device is on the same network segment as the IP address of the client for ARP probe.

Example

Enable association between ARP and DHCP snooping on the device.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] arp dhcp-snooping-detect enable
```

Related Topics

19.14.11 dhcp snooping enable

8.2.2 arp detect-times

19.14.2 dhcp option82 enable

 Copyright © Huawei Technologies Co., Ltd.

Function

The **dhcp option82 enable** command enables a device to insert the Option 82 field to a DHCP message.

The **undo dhcp option82 enable** command disables a device from inserting the Option 82 field to a DHCP message.

By default, a device does not insert the Option 82 field to a DHCP message.

Format

dhcp option82 { **insert** | **rebuild** } **enable**

undo dhcp option82 { **insert** | **rebuild** } **enable**

Parameters

Parameter	Description	Value
insert	Enables a device to insert the Option 82 field to a DHCP message.	-
rebuild	Enables a device to forcibly insert the Option 82 field to a DHCP message.	-

Views

VLAN view, Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

The device inserts the Option 82 field to a DHCP message in two modes:

- Insert mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device checks whether the Option 82 field contains the remote ID. If so, the device retains the Option 82 field; if not, the device inserts the remote ID.
- Rebuild mode: Upon receiving a DHCP Request message without the Option 82 field, the device inserts the Option 82 field. If the DHCP Request message contains the Option 82 field, the device deletes the original Option 82 field and inserts the Option 82 field set by the administrator.

 Copyright © Huawei Technologies Co., Ltd.

The device handles the reply packets from the DHCP server in the same way regardless of whether the Insert or Rebuild method is used.

- The DHCP reply packets contain Option 82:
  - If the DHCP request packets received by the device do not contain Option 82, the device deletes Option 82 from the DHCP reply packets, and forwards the packets to the DHCP client.
  - If the DHCP request packets contain Option 82, the device changes the Option 82 format in the DHCP reply packets into the Option 82 format in the DHCP request packets, and forwards the packets to the DHCP client.
- If the DHCP reply packets do not contain Option 82, the device directly forwards the packets.

NOTE

The physical interface can insert Option82 to the DHCP packets directly forwarded, but does not insert Option82 to the DHCP packets forwarded through a tunnel.

Prerequisites

DHCP snooping has been enabled on the device, or the device has been configured as a DHCP relay agent.

Precautions

- When receiving a DHCP Request message, the device checks whether the field GIADDR in the packet is 0. If so, the **dhcp option82 enable** command takes effect; if not, this command does not take effect.
- DHCP Option 82 must be configured on the user-side of a device; otherwise, the DHCP messages sent to the DHCP server will not carry Option 82.

Example

Enable the device to insert the Option 82 field to DHCP messages on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 insert enable
```

Enable the device to forcibly insert the Option 82 field to DHCP messages in VLAN 100.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] dhcp option82 rebuild enable
```

Related Topics

8.3.28 dhcp select relay
19.14.11 dhcp snooping enable
19.14.23 display dhcp option82 configuration

19.14.3 dhcp option82 format

Function

The **dhcp option82 format** command configures the format of the Option 82 field in a DHCP message.

The **undo dhcp option82 format** command restores the default format of the Option 82 field in a DHCP message.

By default, the Option 82 field in a DHCP message is in the format of **default**.

Format

dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format** { **default** | **common** | **extend** | **user-defined** *text* }

undo dhcp option82 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] [**circuit-id** | **remote-id**] **format**

Parameters

Parameter	Description	Value
circuit-id	Indicates the circuit ID (CID) in the Option 82 field. If the CID is not specified, the format of the Option 82 field is **default**.	-
remote-id	Indicates the remote ID (RID) in the Option 82 field. If the RID is not specified, the format of the Option 82 field is **default**.	-
default	Indicates the default format of the Option 82 field. ● CID format: interface name:svlan.cvlan host name/0/0/0/0/0, in ASCII format ● RID format: device MAC address, in hexadecimal notation	-
common	Indicates the common format of the Option 82 field. ● CID format: {eth|trunk}slot ID/subcard ID/port ID:svlan.cvlan host name0/0/0/0/0, in ASCII format ● RID format: device MAC address (6 bytes), in ASCII format	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
extend	Indicates the extended format of the Option 82 field. ● CID format: circuit-id type (0) + length (4) + S-VLAN ID (2 bytes) + slot ID (5 bits) + subslot ID (3 bits) + port (1 byte), in hexadecimal notation ● RID format: remote-id type (0) + length (6) + device MAC address (6 bytes), in hexadecimal notation In the CID and RID formats, the values without a unit are fixed values of the fields; the values with a unit indicate the field lengths.	-
user-defined *text*	Indicates the user-defined format of the Option 82 field.	The value is a string of 1 to 255 characters. For details, see the description in "Usage Guideline."
vlan *vlan-id*	Indicates an outer VLAN ID. If a VLAN ID is specified, only the format of the Option 82 field in the DHCP messages sent from the specified VLAN is configured. If no VLAN is specified, the format of the Option 82 field in all the DHCP messages received by the interface is configured.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Indicates an inner VLAN ID.	The value is an integer that ranges from 1 to 4094.

Views

System view, Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the function of inserting the Option 82 field to DHCP messages is enabled, you can use the **dhcp option82 format** command to configure the format of the Option 82 field.

If you run the **dhcp option82 format** command in the system view, the command takes effect for all the DHCP messages on all the interfaces of the device.

You can use the following keywords to define the Option 82 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, Eth2/0/0. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.

 Copyright © Huawei Technologies Co., Ltd.

- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 82 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in a character string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, spaces, and % + keywords.
  - In a hexadecimal notation string, numbers are encapsulated in the Option 82 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
  - All the spaces in a hexadecimal character string are ignored.
  - By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
  - A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Precautions

- All Option82 fields configured in the system view or in the same interface view share a length of 1-255 bytes. If their total length exceeds 255 bytes, some Option82 information will be lost.
- There is no limit on the number of Option 82 fields configured on the device. However, a large number of Option 82 fields will occupy a lot of memory and prolong the device processing time. To ensure device performance, you are advised to configure Option 82 fields based on the service requirements and device memory size.

Example

Configure the default format for the CID in the Option 82 field.

```
<Huawei> system-view
[Huawei] dhcp option82 circuit-id format default
```

Configure the extended format for the CID and RID in the Option 82 field.

```
<Huawei> system-view
[Huawei] dhcp option82 format extend
```

Configure the user-defined string for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<Huawei> system-view
[Huawei] dhcp option82 circuit-id format user-defined "%portname:%svlan.%cvlan %sysname"
```

Configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<Huawei> system-view
[Huawei] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot %3subslot %8port
```

Configure the user-defined string for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<Huawei> system-view
[Huawei] dhcp option82 remote-id format user-defined %mac
```

On Eth2/0/0, configure the default format for the CID in the Option 82 field.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 circuit-id format default
```

On Eth2/0/0, configure the extended format for the CID and RID in the Option 82 field of DHCP messages from VLAN 10.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 vlan 10 format extend
```

On Eth2/0/0, configure a user-defined format for the CID in the Option 82 field and encapsulate the port name, outer VLAN ID, inner VLAN ID, and host name in ASCII format.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 circuit-id format user-defined "%portname:%svlan.%cvlan
%sysname"
```

On Eth2/0/0, configure a hexadecimal notation string for the CID of the Option 82 field and encapsulate the CID type (fixed as 0, indicating the hexadecimal notation), length (excluding the lengths of the CID type and the keyword length itself), outer VLAN ID, slot ID (5 bits), subcard ID (3 bits), and port ID (8 bits).

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 circuit-id format user-defined 0 %length %svlan %5slot
%3subslot %8port
```

On Eth2/0/0, configure the user-defined format for the RID in the Option 82 field and encapsulate the device MAC address in hexadecimal notation.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp option82 remote-id format user-defined %mac
```

Related Topics

19.14.2 dhcp option82 enable

19.14.4 dhcp server detect

Function

The **dhcp server detect** command enables detection of DHCP servers.

The **undo dhcp server detect** command disables detection of DHCP servers.

By default, detection of DHCP servers is disabled.

Format

dhcp server detect

undo dhcp server detect

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If bogus DHCP servers exist on the network, they send incorrect information to DHCP clients, such as the incorrect gateway address, incorrect DNS server, and incorrect IP address. As a result, DHCP clients cannot access the network or access incorrect networks.

After detection of DHCP servers is enabled, a DHCP snooping device checks and stores all information about DHCP servers in the DHCP Reply messages, such as DHCP server address and DHCP client port number, in the log. Based on logs, the network administrator checks for bogus DHCP servers on the network to maintain the network.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Enable detection of DHCP servers.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] dhcp server detect
```

Related Topics

19.14.11 dhcp snooping enable

19.14.5 dhcp snooping alarm enable

Function

The **dhcp snooping alarm enable** command enables alarm for discarded DHCP messages.

The **undo dhcp snooping alarm enable** command disables alarm for discarded DHCP messages.

By default, the alarm function for discarded DHCP messages is disabled.

Format

dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **enable** [**threshold** *threshold*]

undo dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **enable** [**threshold**]

Parameters

Parameter	Description	Value
user-bind	Generates an alarm when the number of DHCPv4 Request messages discarded because they do not match DHCP snooping binding entries reaches the threshold.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-address	Generates an alarm when the number of DHCPv4 request messages discarded because the CHADDR field in the DHCP messages does not match the source MAC address in the data frame header reaches the threshold.	-
untrust-reply	Generates an alarm when the number of DHCPv4 Response messages discarded by untrusted interfaces reaches the threshold.	-
threshold *threshold*	Specifies the alarm threshold. When the number of discarded DHCPv4 messages reaches the threshold, an alarm is generated.	The value is an integer that ranges from 1 to 1000.

Views

Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the alarm function is enabled, alarm messages are displayed if DHCP attacks occur and the number of discarded attack messages reaches the threshold. The minimum interval for sending alarm messages is 1 minute. You can run the **19.14.6 dhcp snooping alarm threshold** command to set the alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

By default, a device does not check messages received by the clients. Therefore, to make the command take effect, ensure the following is ready:

- The device has been enabled to check DHCP messages against the binding entries using the **19.14.9 dhcp snooping check user-bind enable** command before the **dhcp snooping alarm user-bind enable** command is run.
- The device has been enabled to check whether the CHADDR field is the same as the source MAC address in the header of a DHCPv4 Request message using the **19.14.8 dhcp snooping check mac-address enable** command before the **dhcp snooping alarm mac-address enable** command is run.

To ensure that alarms can be properly reported, you need to run the **8.3.106 snmp-agent trap enable feature-name dhcp** command to enable the DHCP module to report the corresponding alarm. You can check whether the DHCP

module is enabled to report the corresponding alarm using the **8.3.73 display snmp-agent trap feature-name dhcp all** command.

Example

On Eth2/0/0, enable DHCP snooping, enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address in the Ethernet frame header, and enable alarm for the DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check mac-address enable
[Huawei-Ethernet2/0/0] dhcp snooping alarm mac-address enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.6 dhcp snooping alarm threshold

19.14.6 dhcp snooping alarm threshold

Function

The **dhcp snooping alarm threshold** command sets the alarm threshold for the number of DHCP messages discarded by DHCP snooping.

The **undo dhcp snooping alarm threshold** command restores the default alarm threshold.

By default, an alarm is generated in the system when at least 100 DHCP snooping messages are discarded, and the alarm threshold on an interface is set using the **dhcp snooping alarm threshold** command in the system view.

Format

In the system view:

dhcp snooping alarm threshold *threshold*

undo dhcp snooping alarm threshold

In the interface view:

dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **threshold** *threshold*

undo dhcp snooping alarm { **user-bind** | **mac-address** | **untrust-reply** } **threshold**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
threshold	Specifies the alarm threshold for the number of DHCP snooping-discarded messages.	The value is an integer that ranges from 1 to 1000.
user-bind	Specifies the alarm threshold for the number of DHCPv4 Request messages discarded because they do not match the DHCP snooping binding entries.	-
mac-address	Specifies the alarm threshold for the number of DHCP messages discarded because the CHADDR field in the DHCPv4 request messages does not match the source MAC address in the data frame header.	-
untrust-reply	Specifies the alarm threshold for the number of DHCPv4 Response messages discarded by untrusted interfaces.	-

Views

System view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After trap for discarded DHCP messages is enabled, run the **dhcp snooping alarm threshold** command to specify the alarm threshold for the number of DHCP messages discarded by DHCP snooping. If the alarm threshold is not set on an interface, the interface uses the global alarm threshold.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

The DHCP snooping alarm function has been enabled using the **dhcp snooping alarm** { **user-bind** | **mac-address** | **untrust-reply** } **enable** command.

Precautions

If you run the **dhcp snooping alarm threshold** command in the system view, the command takes effect on all the interfaces of the device.

 Copyright © Huawei Technologies Co., Ltd.

If you specify an alarm threshold for the number of DHCP messages discarded by DHCP snooping in the system view, an alarm is generated when the number of all the discarded DHCP messages reaches the threshold.

Example

Set the global alarm threshold for the number of discarded DHCP messages to 200.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] dhcp snooping alarm threshold 200
```

On Eth2/0/0, enable DHCP snooping, enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address in the Ethernet frame header, and enable alarm for the DHCP messages discarded because the CHADDR field in the DHCP message does not match the source MAC address. Set the alarm threshold to 1000.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check mac-address enable
[Huawei-Ethernet2/0/0] dhcp snooping alarm mac-address enable
[Huawei-Ethernet2/0/0] dhcp snooping alarm mac-address threshold 1000
```

19.14.7 dhcp snooping check dhcp-giaddr enable

Function

The **dhcp snooping check dhcp-giaddr enable** command enables the device to check whether the GIADDR field in DHCP messages is 0.

The **undo dhcp snooping check dhcp-giaddr enable** command disables the device from checking whether the GIADDR field in DHCP messages is 0.

By default, the device does not check whether the GIADDR field in DHCP messages is 0.

Format

dhcp snooping check dhcp-giaddr enable

undo dhcp snooping check dhcp-giaddr enable

Parameters

None

Views

VLAN view, Interface view, Port group view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To ensure that the device obtains parameters such as MAC addresses for generating a binding table, DHCP snooping needs to be applied to Layer 2 access devices or the first DHCP relay agent from the device. Therefore, the GIADDR field in the DHCP messages received by the DHCP snooping-enabled device is 0. If the GIADDR field is not 0, the message is unauthorized and then discarded.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check dhcp-giaddr enable** command in the VLAN view, the command takes effect on all the DHCP messages from the specified VLAN. If you run the **dhcp snooping check dhcp-giaddr enable** command in the interface view, the command takes effect on all the DHCP messages received by the specified interface.

Example

Enable the device to check whether the GIADDR field in DHCP messages from VLAN1 10 is 0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping check dhcp-giaddr enable
```

Enable the device to check whether the GIADDR field in DHCP messages received on Eth2/0/0 is 0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check dhcp-giaddr enable
```

Related Topics

8.3.18 dhcp enable

19.14.11 dhcp snooping enable

19.14.8 dhcp snooping check mac-address enable

Function

The **dhcp snooping check mac-address enable** command enables the device to check whether the CHADDR field matches the source MAC address in the header of a DHCP Request message.

The **undo dhcp snooping check mac-address enable** command disables the device from checking whether the CHADDR field matches the source MAC address in the header of a DHCP Request message.

By default, the device does not check whether the CHADDR field is the same as the source MAC address in the header of a DHCP Request message.

Format

dhcp snooping check mac-address enable

undo dhcp snooping check mac-address enable

Parameters

None

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In normal situations, the CHADDR field in a DHCP Request message matches the MAC address of the DHCP client that sends the message. The DHCP server identifies the client MAC address based on the CHADDR field in the DHCP Request message. If attackers continuously apply for IP addresses by changing the CHADDR field in the DHCP Request message, addresses in the address pool on the DHCP server may be exhausted. As a result, authorized users cannot obtain IP addresses.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check mac-address enable** command in the VLAN view, the command takes effect on all the DHCP messages in the specified VLAN received by all the interfaces on the device. If you run the **dhcp snooping check**

 Copyright © Huawei Technologies Co., Ltd.

mac-address enable command in the interface view, the command takes effect for all the DHCP messages received on the interface.

Example

Enable the device to check whether the CHADDR field in the DHCP message matches the source MAC address on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping check mac-address enable
```

Related Topics

19.14.11 dhcp snooping enable
19.14.9 dhcp snooping check user-bind enable

19.14.9 dhcp snooping check user-bind enable

Function

The **dhcp snooping check user-bind enable** enables the device to check DHCP messages against the DHCP snooping binding table.

The **undo dhcp snooping check user-bind enable** disables the device from checking DHCP messages against the DHCP snooping binding table.

By default, the device does not check DHCP messages against the DHCP snooping binding table.

Format

dhcp snooping check user-bind enable

undo dhcp snooping check user-bind enable

Parameters

None

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a DHCP snooping binding table is generated, the device checks DHCP Request and Release messages against the binding table. The device forwards only

DHCP messages that match binding entries. This prevents unauthorized users from sending bogus DHCP Request or Release messages to extend or release IP addresses.

The matching rules are as follows:

- When the device receives a DHCP Request message, it performs the following operations:
  a. Checks whether the destination MAC address is all Fs. If so, the device considers the user to have gone online for the first time and directly forwards the message. If not, the device considers the user to have sent the DHCP Request message to renew the IP address lease and checks the DHCP Request message against the DHCP snooping binding table.
  b. Checks whether the CHADDR field in the DHCP Request message matches a DHCP snooping binding entry. If not, the device considers the user to have gone online for the first time and directly forwards the message. If so, the device checks whether the VLAN ID, IP address, and interface number of the message match DHCP snooping binding entries. If all these fields match a DHCP snooping binding entry, the device forwards the message; otherwise, the device discards the message.
- When receiving a DHCP Release message, the device checks whether the VLAN ID, IP address, MAC address, and interface number of the message match a dynamic DHCP snooping binding entry. If so, the device forwards the message; otherwise, the device discards the message.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

If you run the **dhcp snooping check user-bind enable** command in the VLAN view, the command takes effect for all the DHCP messages received from the specified VLAN. If you run the **dhcp snooping check user-bind enable** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

Example

Enable the device to check DHCP messages against the DHCP snooping binding table in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping enable
[Huawei-vlan10] dhcp snooping check user-bind enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.8 dhcp snooping check mac-address enable

19.14.10 dhcp snooping disable

Function

The **dhcp snooping disable** command disables DHCP snooping on an interface.

The **undo dhcp snooping disable** command cancels the configuration.

By default, if the **19.14.11 dhcp snooping enable** command is used on an interface or in a VLAN that an interface belongs to, DHCP snooping is enabled on this interface.

Format

dhcp snooping disable

undo dhcp snooping disable

Parameters

None

Views

Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If you run the **dhcp snooping enable** command to enable DHCP snooping in a VLAN, DHCP snooping is enabled on all the interfaces in the VLAN. If you do not run the **dhcp snooping enable** command to enable DHCP snooping on an interface, you cannot run the **undo dhcp snooping enable** command to disable DHCP snooping on the interface. To address this problem, run the **dhcp snooping disable** command to disable DHCP snooping on the interface. Users can properly go online from this interface, but no dynamic binding entry is generated.

Precautions

- The **dhcp snooping disable** command does not only disable DHCP snooping on an interface, but also clears the DHCP snooping configuration and the dynamic binding table. The **undo dhcp snooping enable** command, however, only disables DHCP snooping on the interface and does not clear the configuration or the dynamic binding table.
- The **undo dhcp snooping disable** command enables DHCP snooping on an interface. To enable DHCP snooping, run the **dhcp snooping enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Disable DHCP snooping on Eth2/0/0 in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping enable
[Huawei-vlan10] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping disable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.11 dhcp snooping enable

Function

The **dhcp snooping enable** command enables DHCP snooping.

The **undo dhcp snooping enable** command disables DHCP snooping.

By default, DHCP snooping is disabled on the device.

Format

In the system view:

dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

undo dhcp snooping enable [**ipv4** | **ipv6** | **vlan** { *vlan-id1* [**to** *vlan-id2*] } &<1-10>]

In the VLAN view and interface view:

dhcp snooping enable

undo dhcp snooping enable

Parameters

Parameter	Description	Value
ipv4	Indicates that the device processes only DHCPv4 messages. **NOTE** The AR169RW-P-M9 does not support this parameter.	-
ipv6	Indicates that the device processes only DHCPv6 messages. **NOTE** The AR169RW-P-M9 does not support this parameter.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Enables DHCP snooping in a specified VLAN. • *vlan-id1* specifies the first VLAN ID. • **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The specified VLAN ID must exist.

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

DHCP snooping is a security function to protect DHCP. When you run the **dhcp snooping enable** command to enable DHCP snooping on a device, the device can process both DHCPv4 and DHCPv6 messages. In practice, however, if the DHCP snooping device needs to process only DHCPv4 or DHCPv6 messages, you can run the **dhcp snooping enable ipv4** or **dhcp snooping enable ipv6** command, which improves CPU efficiency.

You must enable DHCP snooping in the system view before enabling DHCP snooping on an interface or in a VLAN.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Follow-up Procedure

Run the **dhcp snooping trusted** command to configure the interface connected to the DHCP server as a trusted interface. A binding table is generated.

Precautions

The **dhcp snooping enable** command in the system view is the prerequisite for DHCP snooping-related functions. After the **undo dhcp snooping enable** command is run, all DHCP snooping-related configurations of the device are deleted. After DHCP snooping is enabled again using the **dhcp snooping enable** command, all DHCP snooping-related configurations of the device are restored to the default configurations.

If you run the **dhcp snooping enable** command in the VLAN view, the command takes effect for all the DHCP messages from the specified VLAN. If you run the **dhcp snooping enable** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable DHCP snooping globally and configure the device to process only ipv4 messages.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable ipv4
```

Enable DHCP snooping on Eth 2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
```

Enable DHCP snooping in VLAN 100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp snooping enable
```

Enable DHCP snooping in VLANs ranging from VLAN 20 to VLAN 25 in a batch.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan batch 20 to 25
[Huawei] dhcp snooping enable vlan 20 to 25
```

19.14.12 dhcp snooping enable no-user-binding

Function

The **dhcp snooping enable no-user-binding** command disables the interfaces from generating DHCP snooping binding entries after DHCP snooping is enabled.

The **undo dhcp snooping enable no-user-binding** command restores the default setting.

By default, an interface generates DHCP snooping binding entries after DHCP snooping is enabled.

Format

System view:

dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

undo dhcp snooping enable no-user-binding vlan { *vlan-id1* [**to** *vlan-id2*] } &<1-10>

VLAN view, interface view:

dhcp snooping enable no-user-binding

undo dhcp snooping enable no-user-binding

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan { *vlan-id1* [**to** *vlan-id2*] }	Disables the interfaces in the specified VLANs from generating DHCP snooping binding entries. ● *vlan-id1* specifies the first VLAN ID. ● **to** *vlan-id2* specifies the last VLAN ID. *vlan-id2* must be larger than *vlan-id1*.	The value is an integer that ranges from 1 to 4094.

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

After DHCP snooping is enabled on a device, the device generates DHCP snooping binding entries for users by default. If the number of binding entries on the device reaches the upper limit, new users cannot go online. In certain scenarios, for example, on a trusted DHCP network, if you do not want to limit the number of online users but want to record user location information, run the **dhcp snooping enable no-user-binding** command to disable the device from generating DHCP snooping binding entries.

When the command is executed in an interface view, the command takes effect for all DHCP users connecting to the interface. When the command is executed in the VLAN view, the command takes effect for all the DHCP users belonging to this VLAN on all interfaces. When the command is executed in the system view, the command takes effect in the same way as it is executed in the VLAN view, except that multiple VLANs can be specified.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

After this command is executed, the device deletes the binding entries from the corresponding VLAN or interface.

If the DHCP snooping binding entry-dependent function such as IPSG or DAI is configured on the device, the corresponding function does not take effect after this command is run.

This command cannot be used together with **19.14.9 dhcp snooping check user-bind enable**; otherwise, online users cannot go offline.

 Copyright © Huawei Technologies Co., Ltd.

Example

In the system view, disable the interfaces in VLAN 10 and VLAN 20 from generating DHCP snooping binding entries.

```
<Huawei> system-view
[Huawei] dhcp snooping enable no-user-binding vlan 10 20
```

In the VLAN view, disable the interfaces in VLAN 10 from generating DHCP snooping binding entries.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] dhcp snooping enable no-user-binding
```

In the interface view, disable Eth2/0/0 from generating DHCP snooping binding entries.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable no-user-binding
```

Related Topics

19.14.11 dhcp snooping enable
19.14.22 dhcpv6 snooping relay-information enable

19.14.13 dhcp snooping max-user-number

Function

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface.

The **undo dhcp snooping max-user-number** command restores the default maximum number of DHCP snooping binding entries to be learned on an interface.

By default, the number of learned DHCP snooping binding entries is the maximum number of DHCP snooping binding entries that can be learned by the entire device.

Format

dhcp snooping max-user-number *max-user-number*

undo dhcp snooping max-user-number

Parameters

Parameter	Description	Value
max-user-number	Specifies the maximum number of DHCP snooping binding entries that can be learned on an interface.	The value is an integer that varies depending on product models.

 Copyright © Huawei Technologies Co., Ltd.

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping max-user-number** command sets the maximum number of DHCP snooping binding entries to be learned on an interface. If the number of DHCP snooping binding entries reaches the maximum value, subsequent users cannot access.

If you run the **dhcp snooping max-user-number** command in the VLAN view, the command takes effect on all the interfaces in the VLAN. If you run the **dhcp snooping max-user-number** command in the VLAN view, and the interface view, the smallest value takes effect.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Example

Set the maximum number of DHCP users to 100 on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcp snooping max-user-number 100
```

Set the maximum number of DHCP users in VLAN 100 to 100.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp snooping enable
[Huawei-vlan100] dhcp snooping max-user-number 100
```

Related Topics

19.14.11 dhcp snooping enable
19.14.24 display dhcp snooping

19.14.14 dhcp snooping trusted

Function

The **dhcp snooping trusted** command configures an interface as a trusted interface.

The **undo dhcp snooping trusted** command configures an interface as an untrusted interface.

By default, an interface is an untrusted interface.

NOTE

AR1200 series routers do not support this command.

Format

In the VLAN view:

dhcp snooping trusted interface *interface-type interface-number*

undo dhcp snooping trusted interface *interface-type interface-number*

In the interface view:

dhcp snooping trusted

undo dhcp snooping trusted

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface in a VLAN. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable DHCP clients to obtain IP addresses from authorized DHCP servers, DHCP snooping supports the trusted interface and untrusted interfaces. The trusted interface forwards DHCP messages while untrusted interfaces discard received DHCP ACK messages and DHCP Offer messages.

An interface directly or indirectly connected to the DHCP server trusted by the administrator needs to be configured as the trusted interface, and other interfaces are configured as untrusted interfaces. This ensures that DHCP clients obtain IP addresses from authorized DHCP servers.

Prerequisites

In the system view, run the **dhcp snooping enable** command to enable DHCP snooping.

Precautions

If you run the **dhcp snooping trusted** command in the VLAN view, the command takes effect for all the DHCP messages received from the specified VLAN. If you run the **dhcp snooping trusted** command in the interface view, the command takes effect for all the DHCP messages received on the specified interface.

Example

Configure Eth2/0/0 in VLAN 100 as the trusted interface.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] vlan 100
[Huawei-vlan100] dhcp snooping trusted interface ethernet 2/0/0
```

Configure Eth2/0/0 as the trusted interface.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping trusted
```

Related Topics

19.14.11 dhcp snooping enable

19.14.15 dhcp snooping user-alarm percentage

Function

The **dhcp snooping user-alarm percentage** command configures the alarm thresholds for the percentage of DHCP snooping binding entries.

The **undo dhcp snooping user-alarm percentage** command restores the default alarm thresholds for the percentage of DHCP snooping binding entries.

By default, the lower alarm threshold for the percentage of DHCP snooping binding entries is 50, and the upper alarm threshold for the percentage of DHCP snooping binding entries is 100.

Format

dhcp snooping user-alarm percentage *percent-lower-value percent-upper-value*

undo dhcp snooping user-alarm percentage

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
percent-lower-value	Specifies the lower alarm threshold for the percentage of DHCP snooping binding entries.	The value is an integer that ranges from 1 to 100.
percent-upper-value	Specifies the upper alarm threshold for the percentage of DHCP snooping binding entries.	The value is an integer that ranges from 1 to 100, but must be greater than or equal to the lower alarm threshold.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

After you run the **19.14.13 dhcp snooping max-user-number** command to set the maximum number of DHCP snooping binding entries on an interface, you can run the **dhcp snooping user-alarm percentage** command to set the alarm thresholds for the percentage of DHCP snooping binding entries.

When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or exceeds the upper alarm threshold, the device generates an alarm. When the percentage of learned DHCP snooping binding entries against the maximum number of DHCP snooping entries allowed by the device reaches or falls below the lower alarm threshold later, the device generates a clear alarm.

Example

Set the lower alarm threshold for the DHCP user count percentage to 30 and the upper alarm threshold to 80.

```
<Huawei> system-view
[Huawei] dhcp snooping user-alarm percentage 30 80
```

Related Topics

19.14.13 dhcp snooping max-user-number

19.14.16 dhcp snooping user-bind autosave

 Copyright © Huawei Technologies Co., Ltd.

Function

The **dhcp snooping user-bind autosave** command enables automatic backup of the DHCP snooping binding table.

The **undo dhcp snooping user-bind autosave** command disables automatic backup of the DHCP snooping binding table.

By default, automatic backup of the DHCP snooping binding table is disabled.

Format

dhcp snooping user-bind autosave *file-name* [**write-delay** *delay-time*]

undo dhcp snooping user-bind autosave

Parameters

Parameter	Description	Value
file-name	Specifies the path for storing the file that backs up the binding table and the file name. The file path and name supported by the device must be both entered.	The value is a string of 1 to 51 case-insensitive characters without spaces.
write-delay *delay-time*	Specifies the interval for local automatic backup of the DHCP snooping binding table. If this parameter is not specified, the backup interval is the default value.	The value is an integer that ranges from 60 to 4294967295, in seconds. By default, the interval for local automatic backup of the DHCP snooping binding table is 86400 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **dhcp snooping user-bind autosave** command can retain the configured DHCP snooping binding entries after the device restarts. After a DHCP snooping binding table is generated, you can run the **dhcp snooping user-bind autosave** command to enable automatic backup of the DHCP snooping binding table.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

Precautions

This prevents data loss in the DHCP snooping binding table. The suffix of the file must be .tbl.

Currently, the DHCP snooping binding table can be backed up to only the SD card.

If the system restarts within one day after the system time is changed, immediately run the **dhcp snooping user-bind autosave** command again to back up the latest dynamic binding entries because it is not the time to update the binding table. If you do not run this command, the lease will be inconsistent with the current system time after the dynamic binding table is restored.

Example

Configure the device to back up the DHCP snooping binding table to the file **backup.tbl** in the SD card every 5000 seconds.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] dhcp snooping user-bind autosave sd1:/backup.tbl write-delay 5000
```

Related Topics

19.14.11 dhcp snooping enable

19.14.17 dhcp snooping user-transfer enable

Function

The **dhcp snooping user-transfer enable** command enables location transition for DHCP snooping users.

The **undo dhcp snooping user-transfer enable** command disables location transition for DHCP snooping users.

By default, location transition is enabled for DHCP snooping users.

Format

dhcp snooping user-transfer enable

undo dhcp snooping user-transfer enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In mobile applications, if a user goes online from interfaceA and then switches to interfaceB, you need to enable location transition for DHCP snooping users.

Prerequisites

DHCP snooping has been enabled on the device using the **19.14.11 dhcp snooping enable** command.

Example

Disable location transition for DHCP snooping users.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcp snooping enable
[Huawei] undo dhcp snooping user-transfer enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.18 dhcpv6 interface-id format

Function

The **dhcpv6 interface-id format** command configures the Interface-ID format in DHCPv6 packets.

The **undo dhcpv6 interface-id format** command restores the default Interface-ID format in DHCPv6 packets.

By default, the Interface-ID format in DHCPv6 packets is **default**.

Format

dhcpv6 interface-id format { **default** | **user-defined** *text* }

undo dhcpv6 interface-id format

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
default	Specifies the default Interface-ID format. The default Interface-ID format is %04svlan.%04cvlan.%mac:%portname. The values of the S-VLAN and C-VLAN are integers containing four characters. If the length is fewer than four characters, the value is prefixed with 0s. For example, if the outer VLAN value in the DHCPv6 packets received by the device is 11, the inner VLAN value is 22, the inbound interface is VLANIF100, and the device MAC address is 6afe-870b-0000, the Interface-ID generated during the system parsing process is 0011.0022.6afe870b0000:vlanif100.	-
user-defined *text*	Specifies a user-defined format as the Interface-ID format. A user-defined format can be: ● Format defined by keywords: The Interface-ID is defined based on the keywords supported by the user-defined format. For example, if the name of the device to which the users are connected and the outer VLAN to which the users belong need to be recorded, the user-defined format can be %sysname %svlan. If the device name is HUAWEI and the S-VLAN is 100, the user location information recorded by the Interface-ID is HUAWEI 100. For description of the keywords supported by the user-defined format, see **Table 19-148**. ● Format defined by common character strings: The Interface-ID is directly defined as a character string. For example, if all users on an interface are located in the office building named N8, the Interface-ID can be directly defined as N8. ● Mixed format: The Interface-ID is defined by both the keywords and common character strings. For example, the Interface-ID can be defined as %sysname N8.	The value is a string of case-sensitive characters without spaces. The character string contains 1 to 251 characters, excluding the quotation marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Interface-ID records user access information such as the inbound interfaces of the DHCPv6 packets sent from the clients to the device. The device functions as a DHCPv6 relay or lightweight DHCPv6 relay agent (LDRA). When receiving the request packets sent from the DHCPv6 clients and forwarding the packets to the DHCPv6 server, the device can insert the Interface-ID to the packets to identify the DHCPv6 client location information. The location information can be used by the DHCPv6 server to assign IPv6 addresses and network parameters. You can run the **dhcpv6 interface-id format** command to configure the format of the Interface-ID inserted into DHCPv6 packets.

Table 19-148 Description of the keywords supported by the user-defined format

Keyword	Description
duid	Specifies the client ID, including information such as the client MAC address.
sysname	Specifies the device name of the client.
portname	Specifies the name of the inbound interface that receives the DHCPv6 packets sent from the client to the device.
porttype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is specified when the NAS interface is configured in certain scenarios.
iftype	Specifies the type of the inbound interface that receives the DHCPv6 packets sent from the client to the device. The interface type is usually GE.
mac	Specifies the device MAC address.
slot	Specifies the slot number of the DHCPv6 packet sent from the client to the device.
subslot	Specifies the sub-slot number of the DHCPv6 packet sent from the client to the device.
port	Specifies the port number of the DHCPv6 packet sent from the client to the device.
svlan	Specifies the outer VLAN of the DHCPv6 packet sent by the client.
cvlan	Specifies the inner VLAN of the DHCPv6 packet sent by the client.

 Copyright © Huawei Technologies Co., Ltd.

Keyword	Description
length	Specifies the total length of the keywords following the length keyword. The length of the length keyword is excluded.

Prerequisites

DHCP has been enabled globally using the **dhcp enable** command.

Precautions

- The user-defined format content must be specified between the double quotation marks ("""). For example, to configure the user-defined format content as **mac**, run the **dhcpv6 interface-id format user-defined "%mac"** command.
- Separators that cannot be digits must be added between the keywords in the user-defined format. Otherwise, the keywords cannot be parsed.
- The symbol % must be prefixed to the keywords in the user-defined format to differentiate them from common character strings. If a digit exists before the symbol % and keyword, the digit refers to the number of characters in the keyword.
- The self-defined content is encapsulated in ASCII format. In addition to the preceding precautions, note the following rules:
  - The symbol \ is an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents the character \.
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.

Example

Configure a user-defined format as the format of the Interface-ID in DHCPv6 packets and the device MAC address as the encapsulated content.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] dhcpv6 interface-id format user-defined "%mac"
```

19.14.19 dhcpv6 option18 format

Function

The **dhcpv6 option18 format** command configures the format of the Option 18 field in a DHCPv6 message.

The **undo dhcpv6 option18 format** command restores the default format of the Option 18 field in a DHCPv6 message.

By default, the format of the Option 18 field is not configured in a DHCPv6 message.

Format

dhcpv6 option18 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option18 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 18 field.	The value is a string of 1 to 251 characters. The details about the user-defined format string are provided in the Usage Guidelines.
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** • If a VLAN is specified, only the format of the Option 18 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 18 field in all DHCPv6 messages received by the interface is configured. • If the format of the Option 18 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. • This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
all	Deletes all formats of the Option 18 field.	-

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dhcpv6 option18** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 18 field to a DHCPv6 message, you can run the **dhcpv6 option18 format** command to configure the format of the Option 18 field in a DHCPv6 message.

You can use the following keywords to define the Option 18 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, Eth2/0/0. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.
- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.

- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 18 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in an ASCII string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.
  - By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
  - A hexadecimal notation string can contain numerals, spaces, and % + keywords.
  - In a hexadecimal notation string, numbers are encapsulated in the Option 18 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
  - All the spaces in a hexadecimal character string are ignored.
  - By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
  - If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
  - A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
  - If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.

 Copyright © Huawei Technologies Co., Ltd.

- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

Configure the format of the Option 18 field in a DHCPv6 message in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcpv6 option18 format user-defined "%length %svlan %5slot %3subslot %8port"
```

Configure the format of the Option 18 field in a DHCPv6 message on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcpv6 option18 format user-defined "%length %svlan %5slot %3subslot
%8port"
```

Related Topics

19.14.21 dhcpv6 { option18 | option37 } enable

19.14.20 dhcpv6 option37 format

Function

The **dhcpv6 option37 format** command configures the format of the Option 37 field in a DHCPv6 message.

The **undo dhcpv6 option37 format** command restores the default format of the Option 37 field in a DHCPv6 message.

By default, the format of the Option 37 field is not configured in a DHCPv6 message.

Format

dhcpv6 option37 [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format user-defined** *text*

undo dhcpv6 option37 { [**vlan** *vlan-id*] [**ce-vlan** *ce-vlan-id*] **format** | **format all** }

Parameters

Parameter	Description	Value
user-defined *text*	Indicates the user-defined format of the Option 37 field.	The value is a string of 1 to 247 characters. The details about the user-defined format string are provided in the Usage Guidelines.

Parameter	Description	Value
vlan *vlan-id*	Specifies the outer VLAN ID. **NOTE** • If a VLAN is specified, only the format of the Option 37 field in DHCPv6 messages that belong to this VLAN is configured. If no VLAN is specified, the format of the Option 37 field in all DHCPv6 messages received by the interface is configured. • If the format of the Option 37 field is configured on an interface and the VLAN to which it belongs, the configuration on the interface takes effect. • This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN ID. **NOTE** This parameter is not supported in the VLAN view.	The value is an integer that ranges from 1 to 4094.
all	Deletes all formats of the Option 37 field.	-

Views

System view, VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

After the **dhcpv6 option37** { **insert** | **rebuild** } **enable** command is executed to enable the device to insert the Option 37 field to a DHCPv6 message, you can run the **dhcpv6 option37 format** command to configure the format of the Option 37 field in a DHCPv6 message.

You can use the following keywords to define the Option 37 field. The format string can use the hexadecimal notation, ASCII format, or combination of the two formats.

- sysname: indicates the ID of the access point. This keyword is valid only in ASCII format.
- portname: indicates the name of a port, for example, Eth2/0/0. This keyword is valid only in ASCII format.
- porttype: indicates the type of a port. This keyword is a character string or in hexadecimal notation. For example, if the value is Ethernet in ASCII format, it is 15 in hexadecimal notation.
- iftype: indicates the type of an interface, which can be eth or trunk. This keyword is valid only in ASCII format.

 Copyright © Huawei Technologies Co., Ltd.

- mac: indicates the MAC address of a port. In ASCII format, the value is in the format of H-H-H; in hexadecimal notation, the value is a number of six bytes.
- slot: indicates the slot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- subslot: indicates the subslot ID. This keyword is valid in ASCII format or in hexadecimal notation.
- port: indicates the port number. This keyword is valid in ASCII format or in hexadecimal notation.
- svlan: indicates the outer VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- cvlan: specifies the inner VLAN ID. The value ranges from 1 to 4094. If this field is not required, this field is 0. This keyword is valid in ASCII format or in hexadecimal notation.
- length: indicates the total length of the keywords following the keyword length.
- n: indicates the value of the keyword **svlan** or **cvlan** if the SVLAN or CVLAN does not exist. The keyword **n** is on the left of the keyword **svlan** or **cvlan**. If the corresponding VLAN does not exist, the default value of the keyword **svlan** or **cvlan** is 4096 in ASCII format and is all Fs in hexadecimal notation. If the **n** keyword is added to the left of the keyword **svlan** or **cvlan**, the keyword **svlan** or **cvlan** is 0. This keyword is valid in ASCII format or in hexadecimal notation.

NOTE

Delimiters must be added between keywords; otherwise, the device cannot parse the keywords. The delimiters cannot be numbers.

The symbols used in the format string are as follows:

- The symbol % followed by a keyword indicates the format of the keyword.
- A number to the left of the symbol % indicates the length of the keyword following the symbol %. In an ASCII character string, %05 has the same meaning as %05d in the C language. In a hexadecimal character string, the number indicates the keyword length in bits.
- The symbol [] indicates an optional keyword. Each pair of brackets can contain only one keyword, svlan or cvlan. The keyword in the symbol [] is added to the Option 37 field only if the corresponding VLAN ID exists. To facilitate syntax check, the system does not support nesting of symbols [].
- The symbol \ indicates an escape character. The symbols %, \, and [] following the escape character indicate themselves. For example, \\ represents \.
- The contents in quotation marks (" ") are encapsulated in an ASCII string, and the contents outside the quotation marks are encapsulated in hexadecimal notation.
- Other symbols are processed as common characters. The rules for setting the format string in ASCII format or hexadecimal notation are as follows:
  - An ASCII character string can contain Arabic numerals, uppercase letters, lowercase letters, and the following symbols: ! @ # $ % ^ & * ( ) _ + | - = \ [ ] { } ; : ' " / ? . , < > `.

- By default, the length of each keyword in an ASCII character string is the actual length of the keyword.
- A hexadecimal notation string can contain numerals, spaces, and % + keywords.
- In a hexadecimal notation string, numbers are encapsulated in the Option 37 field in hexadecimal notation. A number from 0 to 255 occupies 1 byte; a number from 256 to 65535 occupies 2 bytes; a number from 65536 to 4294967295 occupies 4 bytes. Numbers larger than 4294967295 are not supported. Multiple numbers must be separated by spaces; otherwise, they are considered as one number.
- All the spaces in a hexadecimal character string are ignored.
- By default, the slot ID, subslot ID, port number, and VLAN ID in a hexadecimal character string occupy 2 bytes; the field length occupies 1 byte.
- If the length of each keyword in a hexadecimal character string is specified, the total length of the hexadecimal character string must be a multiple of 8. If the length of a specified keyword is longer than 32 bits, the first 32 bits of the keyword are the actual keyword value, and other bits are set to 0.
- A hexadecimal notation string can contain only the keywords whose values are numbers. Other keywords, such as port name, cannot be added to the hexadecimal notation string.
- If a string is not contained in quotation marks, it is encapsulated in hexadecimal notation. To encapsulate the string in the ASCII format, use a pair of quotation marks to contain the string. For example, the slot ID is 3, and the port number is 4. If the string is in the %slot %port format, the value of the encapsulated string is a hexadecimal number 00030004. If the string is in the "%slot %port" format, the value of the encapsulated string is 3 4.
- A format string can contain both hexadecimal strings and ASCII strings, for example, %slot %port "%sysname %portname:%svlan.%cvlan."

Example

Configure the format of the Option 37 field in a DHCPv6 message in VLAN 10.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] vlan 10
[Huawei-vlan10] dhcpv6 option37 format user-defined "%length %svlan %5slot %3subslot %8port"
```

Configure the format of the Option 37 field in a DHCPv6 message on Eth2/0/0.

```
<Huawei> system-view
[Huawei] dhcp snooping enable
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcpv6 option37 format user-defined "%length %svlan %5slot %3subslot
%8port"
```

Related Topics

19.14.21 dhcpv6 { option18 | option37 } enable

19.14.21 dhcpv6 { option18 | option37 } enable

Function

The **dhcpv6 { option18 | option37 } enable** command enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.

The **undo dhcpv6 { option18 | option37 } enable** command disables the device from inserting the Option 18 or Option 37 field to a DHCPv6 message.

By default, the device does not insert the Option 18 or Option 37 field to a DHCPv6 message.

Format

dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

undo dhcpv6 { **option18** | **option37** } { **insert** | **rebuild** } **enable**

Parameters

Parameter	Description	Value
insert	Enables the device to insert the Option 18 or Option 37 field to a DHCPv6 message.	-
rebuild	Enables the device to forcibly insert the Option 18 or Option 37 field to a DHCPv6 message.	-

Views

VLAN view, Interface view, Port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The function of the Option 18 and Option 37 field is similar to the function of the Option 82 field (see the **dhcp option82 enable** command). The Option 18 field contains the port number of a client and the Option 37 field contains the MAC address of the client. A device inserts the Option 18 or Option 37 field to a DHCPv6 Request message to notify the DHCP server of the DHCPv6 client location. The DHCP server can properly assign an IP address and other configurations to the DHCPv6 client, ensuring DHCP client security.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

If you run the **dhcpv6 { option18 | option37 } enable** command in the VLAN view, the command takes effect for all the DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 { option18 | option37 } enable** command in the interface view, the command takes effect for all the DHCPv6 messages received on the specified interface.

Prerequisites

DHCP snooping has been enabled on the device using the **dhcp snooping enable** command.

If you run the **dhcpv6 { option18 | option37 } enable** command in the VLAN view, the command takes effect for all the DHCPv6 messages received from the specified VLAN. If you run the **dhcpv6 { option18 | option37 } enable** command in the interface view, the command takes effect for all the DHCPv6 messages received on the specified interface.

Example

Insert the Option 37 field to DHCPv6 Request messages sent by Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] dhcp snooping enable
[Huawei-Ethernet2/0/0] dhcpv6 option37 insert enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.22 dhcpv6 snooping relay-information enable

Function

The **dhcpv6 snooping relay-information enable** command enables Lightweight DHCPv6 Relay Agent (LDRA) for DHCPv6 snooping.

The **undo dhcpv6 snooping relay-information enable** command disables LDRA.

By default, LDRA is disabled for DHCPv6 snooping.

Format

dhcpv6 snooping relay-information enable [**trust**]

undo dhcpv6 snooping relay-information enable [**trust**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
trust	Configures the device to trust the received Relay-Forward messages. If this parameter is not specified, the device does not trust the received Relay-Forward messages.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Use Scenario

In some scenarios, for example, interfaces in the same VLAN have different network access rights and QoS requirements, the DHCPv6 server must be able to detect user access locations, and assign corresponding access control and QoS policies. The DHCPv6 relay agent is usually configured on the gateway. The relay agent can record user access locations; however, if access devices are located between the relay agent and users, the relay agent cannot detect the access locations of users.

LDRA can meet the requirements of these scenarios. LDRA is configured on the user-side access device. The LDRA-enabled device can forward user access locations (such as the network-side interfaces on clients) to the DHCPv6 server. The DHCPv6 server delivers policies to users accordingly.

This command enables LDRA for DHCPv6 snooping and configures the handling methods for received Relay-Forward messages:

- Trust: The device forwards the received Relay-Forward messages to the DHCPv6 server. This method is usually used when multiple LDRA-enabled devices are directly connected. If the downstream LDRA-enabled device trusts the Relay-Forward messages from the upstream LDRA-enabled device, this method can be used.
- Untrust: The device discards the received Relay-Forward messages. This method is usually used when an LDRA-enabled device directly connects to users, and the users may send invalid Relay-Forward messages.

Prerequisites

DHCP snooping has been enabled using the **dhcp snooping enable** command.

Precautions

The LDRA function only records the client location information and forwards the information to the DHCPv6 server. The differentiated policies for IP address

 Copyright © Huawei Technologies Co., Ltd.

allocation, accounting, access control, and QoS are configured on the DHCPv6 server.

Example

Enable LDRA for DHCPv6 snooping in VLAN10.

```
<Huawei> system-view
[Huawei] vlan 10
[Huawei-vlan10] dhcpv6 snooping relay-information enable
```

Related Topics

19.14.11 dhcp snooping enable

19.14.12 dhcp snooping enable no-user-binding

8.9.9 dhcpv6 interface-id format

19.14.23 display dhcp option82 configuration

Function

The **display dhcp option82 configuration** command displays the DHCP Option 82 configuration.

Format

display dhcp option82 configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP Option 82 configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP Option 82 configuration on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can properly assign an IP address and other configurations to the DHCP client, ensuring DHCP client security.

After the Option 82 field is inserted to a DHCP message, run the **display dhcp option82 configuration** command to display the DHCP Option 82 configuration.

Example

Display all the DHCP Option82 configurations.

```
<Huawei> display dhcp option82 configuration
#
interface Ethernet2/0/0
 dhcp option82 subscriber-id format ascii 222
 dhcp option82 insert enable
 dhcp option82 encapsulation circuit-id
 dhcp option82 circuit-id format common
#
```

Table 19-149 Description of the **display dhcp option82 configuration** command output

Item	Description
interface *ifn*	Option 82 configuration on interface *ifn*.
dhcp option82 subscriber-id format ascii *text2*	The Sub6 suboption is inserted into the Option 82 field of DHCP messages. To specify the parameter, run the **19.14.32 dhcp option82 subscriber-id format** command.
dhcp option82 insert enable	The function of inserting Option 82 to DHCP messages is enabled and the insertion method is configured: • dhcp option82 rebuild enable: Rebuild mode • dhcp option82 insert enable: Insert mode To specify the parameter, run the **19.14.2 dhcp option82 enable** command.
dhcp option82 encapsulation circuit-id	The suboption inserted into the Option 82 field of DHCP messages is configured. To specify the parameter, run the **19.14.31 dhcp option82 encapsulation** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
dhcp option82 circuit-id format common	Format of the circuit-id suboption. To specify the parameter, run the **19.14.3 dhcp option82 format** command.

19.14.24 display dhcp snooping

Function

The **display dhcp snooping** command displays DHCP snooping running information.

Format

display dhcp snooping [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays DHCP snooping running information on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
vlan *vlan-id*	Displays DHCP snooping running information in a specified VLAN.	The value is an integer that ranges from 1 to 4094.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display dhcp snooping** command displays DHCP snooping running information. If no interface or VLAN is specified, global DHCP snooping running information is displayed. If an interface or a VLAN ID is specified, DHCP snooping running information about the interface or VLAN is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display global DHCP snooping running information.

```
<Huawei> display dhcp snooping
 DHCP snooping global running information   :
 DHCPv4 snooping                          : Enable
 DHCPv6 snooping                          : Enable
 Static user max number                    : 512
 Current static user number                : 0
 Dhcp user(dhcpv4/dhcpv6) max number       : 512
 Current dhcpv4 user number                : 0
 Current dhcpv6 user number                : 0
 Arp dhcp-snooping detect                  : Disable  (default)
 Alarm threshold                          : 100      (default)
 Bind-table autosave                       : Disable  (default)
 Offline remove mac-address                : Disable  (default)
 Client position transfer allowed          : Enable   (default)
 DHCPv6 confirm-client online detection     : Enable   (default)
 DHCPv6 client online detection times       : 3        (default)
 DHCPv6 client online detection interval    : 180      (default)

 DHCP snooping running information for VLAN 500   :
 DHCP snooping                            : Enable
 Dhcp user(dhcpv4/dhcpv6) max number       : 512
 Current dhcpv4 user number                : 0
 Current dhcpv6 user number                : 0
 Check dhcp-giaddr                         : Disable  (default)
 Check dhcp-chaddr                         : Disable  (default)
 Check dhcp-request                        : Disable  (default)

 DHCP snooping running information for interface Ethernet2/0/0   :
 DHCP snooping                            : Enable
 Trusted interface                        : No
 Dhcp user(dhcpv4/dhcpv6) max number       : 512
 Current dhcpv4 user number                : 0
 Current dhcpv6 user number                : 0
 Check dhcp-giaddr                         : Disable  (default)
 Check dhcp-chaddr                         : Disable  (default)
 Alarm dhcp-chaddr                         : Disable  (default)
 Discarded dhcp packets for check chaddr    : 0
 Check dhcp-request                        : Disable  (default)
 Alarm dhcp-request                        : Disable  (default)
 Alarm dhcp-reply                          : Disable  (default)
```

Table 19-150 Description of the **display dhcp snooping** command output

Item	Description
DHCPv4 snooping	Whether DHCPv4 snooping is enabled globally. To enable DHCP snooping, run the **19.14.11 dhcp snooping enable** command.
DHCPv6 snooping	Whether DHCPv6 snooping is enabled globally. To enable DHCP snooping, run the **19.14.11 dhcp snooping enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCP snooping	Whether DHCP snooping is enabled on the interface or in the VLAN. To enable DHCP snooping, run the **19.14.11 dhcp snooping enable** command.
Static user max number	Maximum number of static users.
Current static user number	Number of current static users.
Dhcp (dhcpv4/dhcpv6) max number	Shared specifications of the DHCPv4 snooping and DHCPv6 snooping binding tables.
Current dhcpv4 user number	Number of currently online DHCPv4 users.
Current dhcpv6 user number	Number of currently online DHCPv6 users.
Arp dhcp-snooping detect	Whether association between ARP and DHCP snooping is enabled. To enable association between ARP and DHCP snooping, run the **19.14.1 arp dhcp-snooping-detect enable** command.
Alarm threshold	Global alarm threshold for the number of discarded DHCP snooping messages. To set the global alarm threshold for the number of discarded DHCP snooping messages, run the **19.14.6 dhcp snooping alarm threshold** command.
Bind-table autosave	Whether a device is enabled to save the DHCP Snooping binding table. To enable the device to save the binding table, run the **19.14.16 dhcp snooping user-bind autosave** command.
Offline remove mac-address	Whether a device is enabled to delete MAC addresses of offline users.
Client position transfer allowed	Whether location transition is enabled for DHCP snooping users. To enable location transition for DHCP snooping users, run the **19.14.17 dhcp snooping user-transfer enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DHCPv6 confirm-client online detection	Whether the confirm-client probing function of DHCPv6 snooping is enabled.
DHCPv6 client online detection times	Number of times that the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online.
DHCPv6 client online detection interval	Interval at which the DAD NS messages are sent for DHCPv6 snooping to detect whether the user is online.
Trusted interface	Whether an interface is a trusted interface. To configure an interface as a trusted interface, run the **19.14.14 dhcp snooping trusted** command.
Check dhcp-giaddr	Whether a device is enabled to check the GIADDR field in a DHCP Request message. To enable the device to check the GIADDR field in a DHCP Request message, run the **19.14.7 dhcp snooping check dhcp-giaddr enable** command.
Check dhcp-chaddr	Whether a device is enabled to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header. To enable the device to check whether the CHADDR field in a DHCP Request message matches the source MAC address in the Ethernet frame header, run the **19.14.8 dhcp snooping check mac-address enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm dhcp-chaddr	Whether a device is enabled to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold. To enable the device to generate an alarm when the number of discarded DHCP Request messages with the CHADDR field different from the source MAC address in the Ethernet frame header exceeds the alarm threshold, run the **19.14.5 dhcp snooping alarm enable** command.
Discarded dhcp packets for check chaddr	Number of messages discarded because the CHADDR field in the messages does not match the source MAC address in the Ethernet frame header.
Check dhcp-request	Whether an interface is enabled to check DHCP Request messages. To enable the interface to check DHCP Request messages, run the **19.14.9 dhcp snooping check user-bind enable** command.
Alarm dhcp-request	Whether a device is enabled to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold. To enable the device to generate an alarm when the number of DHCP Request messages discarded within a specified period reaches the alarm threshold, run the **19.14.5 dhcp snooping alarm enable** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Alarm dhcp-reply	Whether a device is enabled to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface. To enable the device to generate an alarm when an interface discards a DHCP Reply message from an untrusted interface, run the **19.14.5 dhcp snooping alarm enable** command.

19.14.25 display dhcp snooping configuration

Function

The **display dhcp snooping configuration** command displays the DHCP snooping configuration.

Format

display dhcp snooping configuration [**vlan** *vlan-id* | **interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the DHCP snooping configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the DHCP snooping configuration on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping configuration is complete, run the **display dhcp snooping configuration** command to view the DHCP snooping configuration. If no VLAN or interface is specified, all the DHCP snooping configurations are displayed. If a VLAN or an interface is specified, only the DHCP snooping configuration in the VLAN or on the interface is displayed.

Example

Display all the DHCP snooping configurations.

```
<Huawei> display dhcp snooping configuration
#
dhcp snooping enable
#
vlan 3
 dhcp snooping enable
 dhcp snooping check dhcp-giaddr enable
#
interface Ethernet2/0/0
 dhcp snooping enable
#
```

Related Topics

19.14.11 dhcp snooping enable

19.14.9 dhcp snooping check user-bind enable

19.14.26 display dhcp snooping statistics

Function

The **display dhcp snooping statistics** command displays statistics on the received DHCP messages.

Format

display dhcp snooping statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use the **display dhcp snooping statistics** command to view statistics on the received DHCP messages of all types.

Example

Display statistics on the received DHCP messages.

```
<Huawei> display dhcp snooping statistics
 DHCP Snooping Statistics:

 Client Request:
  Dhcp Discover:                0
  Dhcp Request:                 0
  Dhcp Decline:                 0
  Dhcp Release:                 0
  Dhcp Inform:                  0
 Server Reply:
  Dhcp Offer:                   0
  Dhcp Ack:                     0
  Dhcp Nak:                     0
 Drop Packet:
  Dropped by mac-address check:   0
  Dropped by untrust reply:       0
  Dropped by request conflict:    0
  Dropped by untrust relay-forw:  0
 Delete DHCP snooping table:
  Receive release packet:         0
  Receive decline packet:         0
  Lease expired:                  0
  User command:                   0
  Client transferes:              0
  Interface down:                 0
  Arp detect:                     0
  Ucm notify:                     0
```

Table 19-151 Description of the display dhcp snooping statistics command output

Item	Description
Client Request	Number of packets sent by DHCP clients, including: ● Number of DHCP Discover packets ● Number of DHCP Request packets ● Number of DHCP Decline packets ● Number of DHCP Release packets ● Number of DHCP Inform packets
Server Reply	Number of packets sent by the DHCP server, including: ● Number of DHCP Offer packets ● Number of DHCP ACK packets ● Number of DHCP NAK packets
Drop Packet	Number of discarded packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dropped by mac-address check	Number of discarded DHCP messages whose MAC address is different from the CHADDR value.
Dropped by untrust reply	Number of untrusted reply packets that are discarded.
Dropped by request conflict	Number of packets that are discarded because the client and server MAC addresses conflict.
Dropped by untrust relay-forw	Number of untrusted Relay-Forward packets that are discarded.
Delete DHCP snooping table	Number of DHCP snooping binding entries deleted by the device.
Receive release packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP release packets.
Receive decline packet	Number of DHCP snooping binding entries deleted by the device after the device receives DHCP decline packets.
Lease expired	Number of DHCP snooping entries deleted by the device because of lease expiry.
User command	Number of DHCP snooping binding entries deleted by using commands.
Client transferes	Number of DHCP snooping binding entries deleted because the client connects to another interface on the device.
Interface down	Number of DHCP snooping binding entries deleted because the port is shut down.
Arp detect	Number of DHCP snooping binding entries deleted due to ARP detection.
Ucm notify	Number of times the Ucm module requests DHCP snooping to delete user binding entries.

Related Topics

19.14.11 dhcp snooping enable

19.14.27 display dhcp snooping user-bind

Function

The **display dhcp snooping user-bind** command displays the DHCP snooping binding table.

Format

display dhcp snooping user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays the binding entry mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 4 digits.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table. A binding entry contains the MAC address, IP address, number of the interface connected to the DHCP client, and VLAN ID on the interface. You can run the **display dhcp snooping user-bind** command to view the DHCP snooping binding table.

Example

Display information about the DHCP snooping binding table.

- Display all binding entries.

```
<Huawei> display dhcp snooping user-bind all
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address       MAC Address     VSI/VLAN(O/I/P) Interface      Lease
--------------------------------------------------------------------------------
10.1.28.141      78ac-d4b5-b858  10  /--  /--    Eth2/0/0       2008.10.17-07:31
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

- Display detailed information about binding entries.

```
<Huawei> display dhcp snooping user-bind all verbose
DHCP Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : 10.10.21.254
 MAC Address : 0200-0000-00e8
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : Eth2/0/0
 Lease       : 2008.01.20-19:54
 Gateway     : 10.10.21.1
 Server-ip   : 10.10.21.1
 IPSG Status : ineffective
--------------------------------------------------------------------------------
Print count:           1          Total count:           1
```

Table 19-152 Description of the **display dhcp snooping user-bind** command output

Item	Description
DHCP Dynamic Bind-table	DHCP snooping binding entries.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: Vlan-mapping
IP Address	User IP address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.

Item	Description
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.
Lease	Time when the lease of the IP address used by the user expires.
Gateway	Gateway address.
Server-ip	IP addresses of the DHCP server.
IPSG Status	Whether the binding table is effective for IP packet checking after IP packet checking is enabled. The value can be: ● effective ● ineffective This field is invalid if IP packet checking is not enabled.

Related Topics

19.14.30 reset dhcp snooping user-bind

19.14.28 display dhcpv6 snooping user-bind

Function

The **display dhcpv6 snooping user-bind** command displays the DHCPv6 snooping binding table.

Format

display dhcpv6 snooping user-bind { { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the binding entry mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table. If the parameter is not specified, brief information about the binding table is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After DHCP snooping is enabled, the device generates a DHCP snooping binding table by listening to DHCP Request messages and Reply messages. A binding entry contains the MAC address, IP address, number of the interface connected to the

 Copyright © Huawei Technologies Co., Ltd.

DHCP client, and VLAN ID. You can run the **display dhcpv6 snooping user-bind** command to view the DHCPv6 snooping binding table.

Example

Display the DHCPv6 binding table.

- Display all the dynamic binding entries.

```
<Huawei> display dhcpv6 snooping user-bind all
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address                    MAC Address     VSI/VLAN(O/I/P) Lease
--------------------------------------------------------------------------------
FC00:1::1                     00d5-0191-02de  500 /--  /--    2008.10.01-00:26
--------------------------------------------------------------------------------
print count:          1          total count:          1
```

- Display detailed information about the DHCPv6 binding table.

```
<Huawei> display dhcpv6 snooping user-bind all verbose
DHCPV6 Dynamic Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : FC00:1::1
 MAC Address : 00d5-0191-02de
 VSI         : --
 VLAN(O/I/P) : 101 /--  /--
 Interface   : Eth2/0/0
 Renew time  : 2016.12.12-15:00
 Expire time : 2016.12.12-15:00
 DadTimerId  : --
 DadPktNum   : --
 User State  : LIVE
--------------------------------------------------------------------------------
Print count:          1          Total count:          1
```

Table 19-153 Description of the display dhcpv6 snooping user-bind command output

Item	Description
DHCPV6 Dynamic Bind-table	DHCPv6 Snooping dynamic binding table.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: VLAN mapping
IP Address	User IPv6 address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.

Item	Description
Renew time	Entry update time.
Expire time	Entry expiration time.
DadTimerId	Client probing timer ID.
DadPktNum	Remaining number of times a DAD NS packet can be transmitted.
User State	Status of a DHCPv6 snooping binding entry is as follows: ● START ● DETECTION ● BOUND ● LIVE

19.14.29 reset dhcp snooping statistics

Function

The **reset dhcp snooping statistics** command clears DHCP snooping statistic.

Format

reset dhcp snooping statistics { **global** | **interface** *interface-type interface-number* [**vlan** *vlan-id*] | **vlan** *vlan-id* [**interface** *interface-type interface-number*] }

Parameters

Parameter	Description	Value
global	Clears DHCP Snooping statistics on the globally.	-
interface *interface-type interface-number*	Clears DHCP Snooping statistics on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
vlan *vlan-id*	Clears DHCP Snooping statistics in a specified VLAN. *vlan-id* specifies the ID of the VLAN.	*vlan-id* is an integer that ranges from 1 to 4094.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, if statistics are collected, you can run the **reset dhcp snooping statistics** command to clear the statistics.

Precautions

If both **interface** and **vlan** are specified, the specified interface must belong to the specified VLAN. The **reset dhcp snooping statistics** command clears DHCP Snooping statistics in the specified VLAN that the interface belongs to.

Example

Clear DHCP Snooping statistics on Eth2/0/0.

```
<Huawei> reset dhcp snooping statistics interface ethernet 2/0/0
```

Related Topics

19.14.24 display dhcp snooping

19.14.11 dhcp snooping enable

19.14.30 reset dhcp snooping user-bind

Function

The **reset dhcp snooping user-bind** command clears DHCP snooping binding entries.

Format

reset dhcp snooping user-bind [[**vlan** *vlan-id* | **interface** *interface-type interface-number*] * | **ip-address** [*ip-address*] | **ipv6-address** [*ipv6-address*]]

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the keyword **ipv6-address**.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Clears DHCP snooping binding entries mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Clears DHCP snooping binding entries mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address	Clears DHCP snooping binding entries mapping IPv4 addresses.	-
ipv6-address	Clears DHCP snooping binding entries mapping IPv6 addresses.	-
ip-address	Clears DHCP snooping binding entries mapping a specified IPv4 address.	The value is in dotted decimal notation.
ipv6-address	Clears DHCP snooping binding entries mapping a specified IPv6 address.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After DHCP snooping is enabled, the mapping DHCP snooping binding entries are generated after DHCP users log in. The **reset dhcp snooping user-bind** command clears binding entries mapping a specified parameter. If no parameter is specified, all the binding entries are cleared.

Precautions

If both **interface** *interface-type interface-number* and **vlan** *vlan-id* are configured, the interface specified by **interface** *interface-type interface-number* must have been added to the VLAN specified by **vlan** *vlan-id*. In this case, the command clears the DHCP snooping binding entries on a specified interface belonging to a certain VLAN.

Example

Clear DHCP snooping binding entries in VLAN 100.

```
<Huawei> reset dhcp snooping user-bind vlan 100
```

Related Topics

19.14.11 dhcp snooping enable

19.14.27 display dhcp snooping user-bind

19.14.31 dhcp option82 encapsulation

Function

The **dhcp option82 encapsulation** command configures suboptions inserted into the DHCP Option 82 field.

The **undo dhcp option82 encapsulation** command restores the default suboptions inserted into the DHCP Option 82 field.

By default, the circuit-id (CID), remote-id (RID), subscriber-id, and Sub9suboptions are inserted into the DHCP Option 82 field.

Format

dhcp option82 encapsulation { **circuit-id** | **remote-id** | **subscriber-id** } *

undo dhcp option82 encapsulation

Parameters

Parameter	Description	Value
circuit-id	Inserts the circuit-id suboption.	-
remote-id	Inserts the remote-id suboption.	-
subscriber-id	Inserts the subscriber-id (SID) suboption.	-

Views

System view, VLAN view, interface view, port group view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

This function applies to a DHCP relay agent or a DHCP snooping-enabled device. The Option 82 field records the location of a DHCP client. A device inserts the Option 82 field to a DHCP Request message to notify the DHCP server of the DHCP client location. The DHCP server can assign an IP address and other configurations to the DHCP client, ensuring DHCP client security. The administrator can run this command to configure the device to insert one or more of the circuit-id suboption, remote-id suboption, subscriber-id suboption, and vendor-specific suboption in the Sub9 field into the DHCP Option 82 field. After the command is run, suboptions that are not configured to be inserted are not inserted into the DHCP Option 82 field by default.

Prerequisites

The DHCP function has been enabled in the system view using the **dhcp enable** command.

Example

Insert the circuit-id suboption into the DHCP Option 82 field.

```
<Huawei> system-view
[Huawei] dhcp option82 encapsulation circuit-id
```

19.14.32 dhcp option82 subscriber-id format

Function

The **dhcp option82 subscriber-id format** command inserts the Sub6 suboption into the DHCP Option 82 field of DHCP messages and configures the format of the Sub6 suboption.

The **undo dhcp option82 subscriber-id format** command cancels the configuration of the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages.

By default, the Sub6 suboption is not inserted into the DHCP Option 82 field of DHCP messages.

Format

dhcp option82 subscriber-id format { **ascii** *ascii-text* | **hex** *hex-text* }

undo dhcp option82 subscriber-id format

Parameters

Parameter	Description	Value
ascii *ascii-text*	Specifies the ASCII character string in the Sub6 field.	The value is an ASCII character string and contains fewer than 129 characters.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hex *hex-text*	Specifies the HEX character string in the Sub6 field.	The value is in hexadecimal notation. The value can contain only digits 0 to 9, uppercase letters A to F, and lowercase letters a to f. If no space is included, the value length must be an even number smaller than 257.

Views

System view, Interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an authentication system for wired Ethernet access based on DHCP, DHCP snooping, and Option82, a device can insert suboptions (suboption 1, suboption 2, suboption 6) into the Option 82 field in DHCP Request messages. These suboptions in DHCP Request messages help locate user devices. Unauthorized users cannot access the network by using static IP addresses or stealing accounts of authorized users. You can run the **dhcp option82 subscriber-id format** command to configure the Sub6 suboption.

Prerequisites

DHCP has been enabled using the **dhcp enable** command.

Example

Configure the Sub6 suboption inserted into the DHCP Option 82 field of DHCP messages on GE0/0/1 and specify the ASCII character string in the Sub6 suboption.

```
<Huawei> system-view
[Huawei] dhcp enable
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] dhcp option82 subscriber-id format ascii hw
```

19.15 IP Source Guard Configuration Commands

NOTE

4GE-2S, 4ES2G-S,4ES2GP-S and 9ES2 cards do not support IPSG.

19.15.1 display dhcp static user-bind

Function

The **display dhcp static user-bind** command displays information about a static binding table.

Format

display dhcp static user-bind { { **interface** *interface-type interface-number* | **ip-address** *ip-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries mapping a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address *ip-address*	Displays binding entries mapping a specified IP address.	The value is in dotted decimal notation.
mac-address *mac-address*	Displays binding entries mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays binding entries mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command is used to view information about a configured static binding table. The information includes the IP address, MAC address, VLAN information, and interface information.

Example

Display information about the static binding table.

```
<Huawei> display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address          MAC Address   VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.1.1.1            0001-0002-0003 10 /-- /--      Eth2/0/0
--------------------------------------------------------------------------------
Print count:      1     Total count:      1
```

Display detailed information about the static binding table.

```
<Huawei> display dhcp static user-bind all verbose
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
--------------------------------------------------------------------------------
 IP Address  : 10.21.21.254
 MAC Address : --
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : Eth2/0/0
--------------------------------------------------------------------------------
Print count:          1          Total count:          1
```

Table 19-154 Description of the display dhcp static user-bind command output

Item	Description
DHCP static Bind-table	Static DHCP binding entries. To configure a static DHCP binding table, run the **19.15.7 user-bind static** command.
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: Vlan-mapping
IP Address	User IP address.
MAC Address	User MAC address.
VSI	Name of the VSI that the online user belongs to.
VLAN(O/I/P)	Inner VLAN ID, outer VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.

 Copyright © Huawei Technologies Co., Ltd.

19.15.2 display dhcpv6 static user-bind

Function

The **display dhcpv6 static user-bind** command displays the IPv6 binding table.

Format

display dhcpv6 static user-bind { { **interface** *interface-type interface-number* | **ipv6-address** *ipv6-address* | **mac-address** *mac-address* | **vlan** *vlan-id* } * | **all** } [**verbose**]

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the command.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays binding entries on the specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ipv6-address *ipv6-address*	Displays the binding entry mapping a specified IPv6 address.	The address is a 128-digit hexadecimal number, in the format of X:X::X:X.
mac-address *mac-address*	Displays the binding entry mapping a specified MAC address.	The value is in hexadecimal notation.
vlan *vlan-id*	Displays the binding entry mapping a specified VLAN ID.	The value is an integer that ranges from 1 to 4094.
all	Displays all entries in the binding table.	-
verbose	Displays detailed information about the binding table.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

This command is used to view information about a configured DHCPv6 static binding table. The information includes the IPv6 address, MAC address, VLAN information, and interface information. If prefix delegation (PD) users exist on the network, the device generates an IPv6 prefix binding entry. The **display dhcpv6 static user-bind ipv6-prefix** command displays the static IPv6 prefix binding entries.

Example

Display the DHCPv6 static binding table.

```
<Huawei> display dhcpv6 static user-bind all
DHCPV6 static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - map vlan
IP Address                    MAC Address     VSI/VLAN(O/I/P) Interface
-------------------------------------------------------------------------------
fc00:1::1                     0001-0002-0003  10  /--  /--    --
-------------------------------------------------------------------------------
print count:          1          total count:          1
```

Display detailed information about the DHCPv6 static binding table.

```
<Huawei> display dhcpv6 static user-bind all verbose
DHCPV6 static Bind-table:
-------------------------------------------------------------------------------
 IP Address  : fc00:1::1
 MAC Address : 0001-0002-0003
 VSI         : --
 VLAN(O/I/P) : 10  /--  /--
 Interface   : --
-------------------------------------------------------------------------------
print count:          1          total count:          1
```

Table 19-155 Description of the display dhcpv6 static user-bind command output

Item	Description
DHCPV6 static Bind-table	Static DHCPv6 binding entries. To configure a static DHCPv6 binding table, run the **19.15.7 user-bind static** command.
Flags:O - outer vlan ,I - inner vlan ,P - map vlan	VLAN ID. ● O: Outer VLAN ● I: Inner VLAN ● P: Map VLAN
IP Address	User IPv6 address.
MAC Address	User MAC address.
VSI	Name of the VPN instance that the online user belongs to.

Item	Description
VLAN(O/I/P)	Outer VLAN ID, inner VLAN ID, or VLAN mapping information of the online user.
Interface	User access interface.

Related Topics

19.15.6 ip source check user-bind enable

19.15.3 display ip source check user-bind

Function

The **display ip source check user-bind** command displays the IPSG configurations.

Format

display ip source check user-bind { **vlan** *vlan-id* | **interface** *interface-type interface-number* }

Parameters

Parameter	Description	Value
vlan *vlan-id*	Displays the IP packet check configuration in a specified VLAN.	The value is an integer that ranges from 1 to 4094.
interface *interface-type interface-number*	Displays the IP packet check configuration on a specified interface. The interface is specified by the interface type and number. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display ip source check user-bind** command displays the IP packet check configuration on an interface or in a VLAN.

Example

Display the IP packet check configuration on Ethernet2/0/0.

```
<Huawei>  display ip source check user-bind interface ethernet 2/0/0
 ip source check user-bind enable
 ip source check user-bind check-item ip-address
```

Table 19-156 Description of the display ip source check user-bind command output

Item	Description
ip source check user-bind enable	IP packet check is enabled. To enable IP packet check, run the **ip source check user-bind enable** command.
ip source check user-bind check-item ip-address	IP packet check items. To specify check items, run the **ip source check user-bind check-item** command.

Related Topics

19.15.4 ip source check user-bind check-item (interface view)

19.15.5 ip source check user-bind check-item (VLAN view)

19.15.6 ip source check user-bind enable

19.15.4 ip source check user-bind check-item (interface view)

Function

The **ip source check user-bind check-item** command configures IP packet check items on an interface.

The **undo ip source check user-bind check-item** command restores the default IP packet check items.

By default, the check items contain the IP address, MAC address, VLAN and interface information.

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **vlan** } *

undo ip source check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
vlan	Checks whether VLAN information of an IP packet matches a binding entry.	-

Views

Ethernet interface view, GE interface view, Eth-Trunk interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (interface view)** command to specify items in the IP packet to be checked on a specified interface. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP packet contain the source IP address, source MAC address, and VLAN information. Interface information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the interface view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

The **ip source check user-bind check-item (interface view)** command can only be used on Layer 2 interfaces, including Layer 2 Ethernet interfaces, Layer 2 GE interfaces, and Layer 2 Eth-Trunk interfaces.

Example

Enable IP packet check on Eth2/0/0 to check whether the IP address in the IP packet matches the binding entry.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip source check user-bind enable
```

```
[Huawei-Ethernet2/0/0] ip source check user-bind check-item ip-address
```

Related Topics

19.15.6 ip source check user-bind enable

19.15.5 ip source check user-bind check-item (VLAN view)

Function

The **ip source check user-bind check-item** command configures IP packet check items in a VLAN.

The **undo ip source check user-bind check-item** command restores the default IP packet check items in a VLAN.

By default, the check items contain the IP address, MAC address, VLAN and interface information.

Format

ip source check user-bind check-item { **ip-address** | **mac-address** | **interface** } *

undo ip source check user-bind check-item

Parameters

Parameter	Description	Value
ip-address	Checks whether the IP address of an IP packet matches a binding entry.	-
mac-address	Checks whether the MAC address of an IP packet matches a binding entry.	-
interface	Checks whether interface information of an IP packet matches a binding entry.	-

Views

VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you check an IP packet against the binding table, run the **ip source check user-bind check-item (VLAN view)** command to configure IP packet check items in a specified VLAN. When the device receives an IP packet, it checks the items against the binding table. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded. The optional check items of an IP

 Copyright © Huawei Technologies Co., Ltd.

packet contain the source IP address, source MAC address, and interface information. VLAN information is a mandatory check item.

Prerequisites

IP packet check has been enabled using the **ip source check user-bind enable** command in the VLAN view.

Precautions

When a large number of binding entries exist, it may take a long time to check IP packets, reducing forwarding efficiency.

This command is valid only for dynamic binding entries. The device checks the received packets against entries in the static binding table.

Example

Enable IP packet check in VLAN 100 and check whether the IP address in the IP packet matches the binding entry.

```
<Huawei> system-view
[Huawei] vlan 100
[Huawei-vlan100] ip source check user-bind enable
[Huawei-vlan100] ip source check user-bind check-item ip-address
```

Related Topics

19.15.6 ip source check user-bind enable

19.15.6 ip source check user-bind enable

Function

The **ip source check user-bind enable** command enables IP packet check.

The **undo ip source check user-bind enable** command disables IP packet check.

By default, IP packet check is disabled.

Format

ip source check user-bind enable

undo ip source check user-bind enable

Parameters

None

Views

Ethernet interface view, GE interface view, port group view, Eth-Trunk interface view, VLAN view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Unauthorized users often send bogus packets with the source IP address and MAC address of authorized users to access or attack the network. Then authorized users cannot access stable and secure networks. To address this problem, you can configure IP packet check.

When IP packet check is enabled, the device checks the IP address, MAC address, VLAN information, and interface information against the binding table. You can run the **19.15.4 ip source check user-bind check-item (interface view)** or **19.15.5 ip source check user-bind check-item (VLAN view)** command to specify IP packet check items. Only packets that match the binding entries can be forwarded; otherwise, packets are discarded.

Prerequisites

The IP packet check is based by binding table. So,

- The dynamic DHCP snooping binding table has been generated for DHCP users.
- The static binding table has been configured manually for users using static IP addresses.

Precautions

The **ip source check user-bind enable** command can only be used on Layer 2 interfaces, including Layer 2 Ethernet interfaces, Layer 2 GE interfaces, and Layer 2 Eth-Trunk interfaces.

Example

Enable IP packet check on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip source check user-bind enable
```

19.15.7 user-bind static

Function

The **user-bind static** command configures a static binding table.

The **undo user-bind static** command deletes a static binding table.

By default, no static binding table is configured.

Format

user-bind static { { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **mac-address** *mac-address* } * [**interface** *interface-type interface-number*] [**vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]]

undo user-bind static [**interface** *interface-type interface-number* | { **ip-address** | **ipv6-address** } { *start-ip* [**to** *end-ip*] } &<1-10> | **mac-address** *mac-address* | **vlan** *vlan-id* [**ce-vlan** *ce-vlan-id*]] *

NOTE

The AR100&AR120&AR150&AR160&AR200&AR1200 series do not support the keywords **ipv6-address** and **ce-vlan**.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the interface connected to a user in a static binding entry. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
ip-address	Indicates the static IPv4 address.	-
ipv6-address	Indicates the static IPv6 address.	-
start-ip [**to** *end-ip*]	Specifies the user IP address in a static binding entry. ● *start-ip* specifies the first IP address. ● **to** *end-ip* specifies the last IP address. The value of *end-ip* must be larger than the value of *start-ip*. *start-ip* and *end-ip* identify a VLAN range. If **to** *end-ip* is not specified, only the start IP address is added to the static binding entry. You can specify a maximum of 10 VLAN ranges at a time. The entered VLAN ranges cannot overlap.	The IPv4 address is in dotted decimal notation in the format of X.X.X.X. The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
mac-address *mac-address*	Specifies the user MAC address in a static binding entry.	The value is in hexadecimal notation. The value is in the format of H-H-H.
vlan *vlan-id*	Specifies the user VLAN ID in a static binding entry.	The value is an integer that ranges from 1 to 4094.
ce-vlan *ce-vlan-id*	Specifies the inner VLAN tag of a QinQ packet in a static binding entry.	The value is an integer that ranges from 1 to 4094.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When DHCP snooping is enabled, a dynamic binding table is automatically generated for dynamic users. However, a static binding table cannot be generated for static users. If IP source guard is enabled but no static binding table is available, the device discards all static users' forwarding packets. To enable the device to forward static users' packets, run the **user-bind static** command to configure a static binding table.

Precautions

After a static binding table is configured and IP source guard is enabled, the device performs a match check on IP packets based on the configured binding entries. If the match check fails, the device discards the IP packets.

Example

Configure a static binding entry for a user in VLAN 2 with the IP address 10.1.1.1.

```
<Huawei> system-view
[Huawei] user-bind static ip-address 10.1.1.1 vlan 2
```

Related Topics

19.15.1 display dhcp static user-bind

19.16 URPF Configuration Commands

19.16.1 ipv6 urpf

Function

The **ipv6 urpf** command enables URPF check for IPv6 packets on an interface.

The **undo ipv6 urpf** command disables URPF check for IPv6 packets on an interface.

By default, URPF check for IPv6 packets is disabled on an interface.

Format

ipv6 urpf { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo ipv6 urpf

Parameters

Parameter	Description	Value
loose	Indicates URPF loose check. When the source address of a packet exists in the FIB table, the packet is forwarded according to URPF regardless of whether the outbound interface of the matching entry is the same as the inbound interface of the packet.	-
strict	Indicates URPF strict check. A packet can be forwarded only when the source IP address of the packet exists in the FIB table and the inbound interface of the packet matches the outbound interface in the table.	-
allow-default-route	Allows special processing for the default route.	-
acl *acl-number*	Indicates URPF check for packets matching a specified ACL. URPF matches only source and destination IP addresses in ACL rules.	The value is an integer that ranges from 2000 to 3999. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

allow-default-route determines the processing mode for the default route:

- If **allow-default-route** is not specified, a packet is discarded when the source IP address is not in the FIB table in either strict mode or loose mode.
- If **allow-default-route** is specified and the source IP address is not in the FIB enable, note the following points:
  - In strict mode, if the outbound interface of the default route is the same as the inbound interface of the packet, the packet passes the check and is forwarded. Otherwise, the packet is discarded.
  - In loose mode, the packet passes the check and is forwarded no matter whether the outbound interface of the default route is the same as the inbound interface of the packet.

Prerequisites

Run the **ipv6** command in the system view, and run the **ipv6 enable** command in the interface view.

Precautions

The **ipv6 urpf** command cannot be used on Layer 2 interfaces.

Example

Enable URPF strict check for IPv6 packets on GE1/0/0 and allow special processing for the default route.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ipv6 urpf strict allow-default-route
```

19.16.2 urpf (interface view)

Function

The **urpf** command enables URPF check on the interface and configures the URPF check mode.

The **undo urpf** command disables URPF check on the interface.

By default, URPF check is not enabled on the interface.

Format

urpf { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo urpf

Parameters

Parameter	Description	Value
loose	Indicates URPF check in loose mode. A packet can be forwarded as long as the source IP address of the packet exists in the routing table or ARP entry, regardless of whether the inbound interface of the packet matches the outbound interface in the table.	-
strict	Indicates URPF strict check in strict mode. A packet can be forwarded only when the source IP address of the packet exists in the routing table or ARP entry, and the inbound interface of the packet matches the outbound interface in the table.	-
allow-default-route	Allows special processing for the default route.	-
acl *acl-number*	Indicates URPF check for packets matching a specified ACL. URPF matches only source and destination IP addresses in ACL rules.	The value is an integer that ranges from 2000 to 3999. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A Denial of Service (DoS) attack disables users from connecting to the server. DoS attacks aim to occupy many resources by sending a large number of connection requests to servers. The attacked servers cannot respond to authorized users.

URPF check enables the device to check the source IP address in the FIB table against the inbound interface of the packet. If the source IP address does not match the inbound interface of the packet, the packet is discarded. This prevents IP spoofing attacks, especially DoS attacks with bogus source IP address.

 Copyright © Huawei Technologies Co., Ltd.

You can configure **allow-default-route** in URPF check to determine processing mode for the default route.

- If **allow-default-route** is not specified, a packet is discarded when the source IP address is not in the FIB table in either strict mode or loose mode.
- If **allow-default-route** is specified and the source IP address is not in the FIB enable, note the following points:
  - In strict mode, if the outbound interface of the default route is the same as the inbound interface of the packet, the packet passes the check and is forwarded. Otherwise, the packet is discarded.
  - In loose mode, the packet passes the check and is forwarded no matter whether the outbound interface of the default route is the same as the inbound interface of the packet.

Example

Enable URPF strict check on GE1/0/0 and allow special processing for the default route.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] urpf strict allow-default-route
```

19.17 PKI Configuration Commands

19.17.1 auto-enroll

Function

The **auto-enroll** command enables automatic certificate enrollment and update.

The **undo auto-enroll** command disables automatic certificate enrollment and update.

By default, the automatic certificate enrollment and update are disabled.

Format

auto-enroll [*percent*] [**regenerate** [*key-bit*]] [**updated-effective**]

undo auto-enroll [**updated-effective**]

Parameters

Parameter	Description	Value
percent	Specifies the percentage of the certificate's validity period after which a new certificate is requested automatically.	The value is an integer that ranges from 10 to 100. The default value is 100. When the old certificate expires, the system requests a new certificate.
regenerate	Indicates the RSA key pair will be generated during certificate updates.	-
key-bit	Specifies the number of bits in the RSA key pair generated during certificate updates.	The value is an integer that ranges from 2048 to 4096. The default value is 2048.
updated-effective	Indicates that the certificate takes effect immediately after being updated. By default, an updated certificate takes effect only after the old one expires.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Automatic certificate enrollment: When the certificates are unavailable, will expire, or have expired, an entity automatically requests a new certificate or renews the certificate using the Simple Certification Enrollment Protocol (SCEP).

By default, the automatic certificate enrollment and update function is disabled. When a certificate has expired, you must request a certificate for an entity manually. You can still request a certificate for an entity manually when the automatic certificate enrollment and update function is enabled.

Precautions

- If you do not specify **regenerate**, the system uses the original RSA key pairs during automatic updates.

 Copyright © Huawei Technologies Co., Ltd.

- If you specify **regenerate**, the system generates new RSA key pairs during certificate updates for certificate requests and overwrites the original certificates and RSA key pairs with the new ones.
- After this command is run, the device checks whether the certificate has expired every 60 minutes. If the certificate has expired, the device updates the certificate.

Example

Enable automatic certificate enrollment and update for the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] auto-enroll 50 regenerate
```

19.17.2 ca-name

Function

The **ca-name** command configures the name of the CA in the PKI realm.

The **undo ca-name** command removes the name of the CA in the PKI realm.

By default, a PKI realm does not have a CA name.

Format

ca-name { *name-string* | **from-certificate filename** *file-name* }

undo ca-name

Parameters

Parameter	Description	Value
name-string	Specifies the name of the CA.	It is a string of 1 to 255 characters (including the quotation marks) and case sensitive. The value must start with and end with quotation marks ('').
from-certificate filename *file-name*	Specifies the name of the CA certificate file through which the CA name is obtained.	It is a string of 1 to 64 characters and case insensitive.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After the CA name is specified in the PKI realm, associate the PKI realm with the specified CA. By using the CA name, you can determine the corresponding PKI realm and the check mode for the certificate revocation status.

You can directly specify the CA name by running the **ca-name** *name-string* command. Ensure that the CN, O, and OU in the CA name are in the same sequence as those in the subject name. Alternatively, you can obtain the CA name from the CA certificate by running the **ca-name from-certificate filename** *file-name* command. This avoids errors caused by manual operation.

Example

For the PKI realm **test**, specify the name of the CA.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ca-name "CN=CA"
```

19.17.3 ca id

Function

The **ca id** command specifies a certificate authority (CA) trusted by a PKI realm.

The **undo ca id** command deletes the CA trusted by a PKI realm.

By default, no trusted CA is configured in a PKI realm.

Format

ca id *ca-name*

undo ca id

Parameters

Parameter	Description	Value
ca-name	Specifies the name of a CA trusted by a PKI realm.	The value is a string of 1 to 64 case-insensitive characters.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After the **ca id** command is executed to specify the CA trusted by the device, the CA then requests, obtains, revokes, or queries the device's certificate.

Example

Specify the CA **root_ca** trusted by the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] ca id root_ca
```

Related Topics

19.17.40 display pki realm

19.17.103 pki realm (system view)

19.17.4 cdp-url

Function

The **cdp-url** command configures the CRL distribution point (CDP) URL.

The **undo cdp-url** command deletes the configured CDP URL.

By default, no CDP URL is configured.

Format

cdp-url [**esc**] *url-addr*

cdp-url from-ca

undo cdp-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-addr	Specifies the CDP URL.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.
from-ca	Specifies that the CDP URL address is obtained from the CA certificate.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity needs to use HTTP to update CRL, it must set up a connection with the HTTP server based on CDP URL, and obtain the CRL from the HTTP server. By default, a PKI entity locates and downloads CRL based on the method (HTTP or LDAP) in the CDP information of the local certificate. If you do not want to download CRL based on the CDP URL in the local certificate, run this command to configure the PKI entity to obtain CDP URL from the CA certificate or manually configure the CDP URL.

When CRL is automatically updated by SCEP, you can also manually configure a CDP URL address.

Configuration Impact

Manually configuring a CDP URL address overwrites the CDP carried in the certificate. If the certificate does not contain CDP information and no CDP URL address is manually configured, the device requests the CRL from the CA server using SCEP.

Keyword **esc** only supports the URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Set the CDP URL to http://10.1.1.1/certenroll/ca_root.crl.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl scep
[Huawei-pki-realm-d1] cdp-url http://10.1.1.1/certenroll/ca_root.crl
```

Set the CDP URL to http://www.***.com/certenroll/ca_root.crl.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl scep
[Huawei-pki-realm-d1] cdp-url http://www.***.com/certenroll/ca_root.crl
```

19.17.5 certificate-check

Function

The **certificate-check** command sets the method of checking whether a certificate in the PKI realm is revoked.

The **undo certificate-check** command cancels the method of checking whether a certificate in the PKI realm is revoked.

By default, the system checks using CRLs whether a certificate in the PKI realm is revoked.

Format

certificate-check { { **crl** | **ocsp** } * [**none**] | **none** }

undo certificate-check

Parameters

Parameter	Description	Value
crl	Sets the check method to Certificate Revocation List (CRL).	-
ocsp	Sets the check method to Online Certificate Status Protocol (OCSP).	-
none	Indicates that the system does not check whether a certificate is revoked.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

After this command is executed, the PKI entity validates the peer certificate, for example, whether the peer certificate has expired and whether it is added to CRL.

The system supports the following methods to check whether a certificate in the PKI realm is revoked:

- CRL
  - If the CA server can function as a CDP, the certificate issued by CA contains the CDP information about obtaining the certificate CRL. The PKI entity then uses the specified method (HTTP or LDAP) to find the CRL from the specified location and download the CRL. If the CDP URL is configured in the PKI realm, the PKI entity obtains the CRL from the specified URL.

 Copyright © Huawei Technologies Co., Ltd.

  - If the CA does not support CDPs and no CDP URL is configured on the PKI entity, the PKI entity uses the SCEP protocol to obtain the CRL.

- OCSP

  The PKI entity can use OCSP to check certificate status online, and you do not need to frequently download CRLs.

  When two PKI entities use certificates to perform IPSec negotiation, they check the peer certificate status through OCSP in real time.

- None

  This mode is used when no CRL or OCSP server is available to the PKI entity or the PKI entity does not need to check the peer certificate status. In this mode, the PKI entity does not check whether a certificate has been revoked.

Select the following configurations:

- If the **certificate-check crl** command is configured for a certificate, the CRL mode is used.
- If the **certificate-check ocsp** command is configured for a certificate, the OCSP mode is used.
- If the **certificate-check crl none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check crl ocsp** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check ocsp crl** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as invalid.
- If the **certificate-check crl ocsp none** command is configured for a certificate, the CRL mode is used first. If the CRL mode is unavailable, the OCSP mode is used. If the OCSP mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check ocsp crl none** command is configured for a certificate, the OCSP mode is used first. If the OCSP mode is unavailable, the CRL mode is used. If the CRL mode is unavailable, the certificate is regarded as valid.
- If the **certificate-check none** command is configured for a certificate, the certificate is regarded as valid.

Precautions

After the **certificate-check crl** command is configured, if the device does not have the CRL file, the device fails the certificate verification, and the certificate becomes invalid.

It is not recommended that the none parameter be specified in the**certificate-check** command, because such a configuration poses security risks.

Example

Set the certificate check method to **crl none** in PKI realm **test**. If the CRL mode is unavailable, the certificate is regarded as valid.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] certificate-check crl none
```

19.17.6 certificate auto-update enable

Function

The **certificate auto-update enable** command enables CMPv2-based automatic certificate update.

The **undo certificate auto-update enable** command disables CMPv2-based automatic certificate update.

By default, the CMPv2-based automatic certificate update is disabled.

Format

certificate auto-update enable

undo certificate auto-update enable

Parameters

None

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

If a certificate obtained through CMPv2 is about to expire, run this command to enable CMPv2-based automatic certificate update to ensure certificate validity. After the command is executed, the system performs checks (for example, referenced PKI entity, URL for the CMPv2 server, RSA key pair for CMPv2-based certificate application). The configuration is successful only when the conditions are met.

When the system detects that the remaining validity period of the local certificate has reached the value specified in **19.17.7 certificate update expire-time**, the system automatically initiates the certificate update request and decides whether to create an RSA key pair based on the **19.17.14 cmp-request rsa local-key-pair** configuration. After the new certificate is obtained, the system replaces the previous certificate and RSA key pair with the new ones. The replacement files

 Copyright © Huawei Technologies Co., Ltd.

include the files in device storage, certificate in memory, and configuration used in IKE negotiation.

Example

Enable CMPv2-based automatic certificate update.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] certificate auto-update enable
```

19.17.7 certificate update expire-time

Function

The **certificate update expire-time** command specifies when the certificate starts to update. The time is represented by a percentage of the total validity period.

The **undo certificate update expire-time** command restores the default certificate update time.

By default, the certificate is automatically updated when the validity period is only 50% left.

Format

certificate update expire-time *valid-percent*

undo certificate update expire-time

Parameters

Parameter	Description	Value
valid-percent	Specifies the remaining percentage of the validity period.	The value is an integer that ranges from 10 to 100. The default value is 50.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

If the automatic certificate update through CMPv2 is enabled, the system sends an update request to the CMPv2 server when the specified updated time is reached. This command sets the time (percentage of the total validity period) to update the certificate.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the automatic certificate update when the used time is 60% of the validity period of the certificate.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] certificate update expire-time 60
```

19.17.8 cmp-request authentication-cert

Function

The **cmp-request authentication-cert** command configures the certificate for identity authentication in the request through CMPv2.

The **undo cmp-request authentication-cert** command deletes the certificate for identity authentication in the request through CMPv2.

By default, no certificate for identity authentication in the request through CMPv2 is configured.

Format

cmp-request authentication-cert *cert-name*

undo cmp-request authentication-cert

Parameters

Parameter	Description	Value
cert-name	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Run this command to configure the certificate for identity authentication if you need to apply for a certificate through CMPv2. For different requests through CMPv2, the required certificates are as follows:

- For Initialization Requests (IR), the required certificate is an external identity certificate.
- For certification requests (CR), the required certificate is the one that the CA has already issued to the device.

 Copyright © Huawei Technologies Co., Ltd.

- For the key update requests (KUR), the required certificate is the one that the CA has already issued to the device and is also the one to be updated.

Prerequisites

An identity authentication in the request through CMPv2 exists.

Example

Configure the certificate for identity authentication in the request through CMPv2.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request authentication-cert bb.cer
```

Related Topics

19.17.12 cmp-request origin-authentication-method

19.17.9 cmp-request ca-name

Function

The **cmp-request ca-name** command sets a CA name for the CMP session.

The **undo cmp-request ca-name** command deletes the CA name of the CMP session.

By default, no CA name is configured for a CMP session.

Format

cmp-request ca-name *ca-name*

undo cmp-request ca-name

Parameters

Parameter	Description	Value
ca-name	Indicates the name of the CA and is the field of subject in the CA certificate.	The value starts and ends with the quotation mark (") and is a string of 1 to 128 characters (including the quotation marks). A comma (,) is used to separate adjacent fields in the string.

Views

CMP session view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

A trusted authority enrolls and issues certificates to entities. Therefore, a trusted CA name must be configured.

The field order in the CA name must be the same as that in the actual CA certificate. Otherwise, the server regards the name as incorrect.

Example

Set the CA name for CMP session **test**.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request ca-name "C=cn,ST=beijing,L=shangdi,O=BB,OU=BB,CN=BB"
```

19.17.10 cmp-request entity

Function

The **cmp-request entity** command sets the entity name used to apply for certificate through CMPv2.

The **undo cmp-request entity** command deletes the entity name used to apply for certificate through CMPv2.

By default, the entity name used to apply for certificate through CMPv2 is not configured.

Format

cmp-request entity *entity-name*

undo cmp-request entity

Parameters

Parameter	Description	Value
entity-name	Specifies the entity name for certificate application.	The value must be an existing PKI entity name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To apply for a certificate through CMPv2, create a CMP session and specify the entity name in the CMP session.

Prerequisites

1. A PKI entity has been created using the **pki entity** command.
2. A PKI entity common name has been created using the **common-name** command.

Precautions

The specified entity can be referenced only by one CMP session or PKI realm.

Example

Set the entity name the device uses when applying for a certificate through CMPv2 to **entity1**.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] common-name huawei
[Huawei-pki-entity-entity1] quit
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request entity entity1
```

Related Topics

19.17.79 pki entity

19.17.17 common-name

19.17.73 pki cmp session

19.17.11 cmp-request message-authentication-code

Function

The **cmp-request message-authentication-code** command configures the reference value and secret value of the message authentication code (MAC).

The **undo cmp-request message-authentication-code** command deletes the reference value and secret value of the MAC.

By default, the reference value and secret value of the MAC are not configured.

Format

cmp-request message-authentication-code *reference-value secret-value*

undo cmp-request message-authentication-code

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
reference-value	Specifies the reference value of the MAC.	The value is a string of 1 to 128 case-sensitive characters without spaces and question marks. If the character string is quoted by double quotation marks, it can contain spaces.
secret-value	Specifies the secret value of the MAC.	The length of the plaintext ranges from 1 to 128. The length of the encrypted ciphertext ranges from 48 to 188. The value is a case-sensitive character string without question marks.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

When a device is configured to use MAC for initial request (IR), you need to check the reference value and secret value of the MAC from the CMPv2 server in out-of-band mode, and then run this command to set the values on the device.

Example

Configure the reference value and secret value of the MAC.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request message-authentication-code 1234 123456
```

Related Topics

19.17.12 cmp-request origin-authentication-method

19.17.12 cmp-request origin-authentication-method

Function

The **cmp-request origin-authentication-method** command configures the authentication method used for initial request (IR) through CMPv2.

The **undo cmp-request origin-authentication-method** command restores the default authentication method used for IR through CMPv2.

By default, the authentication method used for IR through CMPv2 is MAC.

Format

cmp-request origin-authentication-method { **message-authentication-code** | **signature** }

undo cmp-request origin-authentication-method

Parameters

Parameter	Description	Value
message-authentication-code	Indicates the MAC method for the IR.	-
signature	Indicates the signature method for the IR.	-

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

During the IR using CMPv2, a security protection measure needs to be taken:

- After you select the MAC method, run the **cmp-request message-authentication-code** command to configure the reference value and secret value. The device uses the reference value and secret value to protect messages during the IR.
- After you select the signature method, run the **cmp-request authentication-cert** command to configure the external certificate. The device uses the external certificate to protect signatures during the IR.

Example

Configure the authentication method used for IR through CMPv2.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request origin-authentication-method signature
```

19.17.13 cmp-request realm

Function

The **cmp-request realm** command specifies a PKI realm to which the CMPv2 server certificate belongs.

The **undo cmp-request realm** command deletes the specified PKI realm.

By default, no PKI realm is specified.

 Copyright © Huawei Technologies Co., Ltd.

Format

cmp-request realm *realm-name*

undo cmp-request realm

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The value must be an existing PKI realm name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the CMPv2 mode is used, run the **cmp-request realm** command to specify a PKI realm to which the CMPv2 server certificate belongs.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

Example

Set a PKI realm name of the CMPv2 server certificate to **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request realm abc
```

19.17.14 cmp-request rsa local-key-pair

Function

The **cmp-request rsa local-key-pair** command configures the RSA key pair used for certificate application through CMPv2.

The **undo cmp-request rsa local-key-pair** command deletes the RSA key pair used for certificate application through CMPv2.

 Copyright © Huawei Technologies Co., Ltd.

By default, the RSA key pair used to apply for certificate through CMPv2 is not configured.

Format

cmp-request rsa local-key-pair *key-name* [**regenerate** [*key-bit*]]

undo cmp-request rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair.	The value must be an existing RSA key pair name.
regenerate	Indicates that the RSA key pair is updated together with certificate update.	-
key-bit	Specifies the bits of the RSA key pair generated during the certificate update.	The value is an integer that ranges from 2048 to 4096. The default value is 2048.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the CMPv2 is used to apply for certificate, the certificate request message sent by the PKI entity to CA must contain public key information. Therefore, you need to configure an RSA key pair for certificate application through CMPv2.

Note the following during configurations:

- If **regenerate** is unspecified, the system uses the original RSA key pairs during automatic updates.
- If **regenerate** is specified, the system generates new RSA key pairs during certificate updates for the application for certificates and overwrites the original certificates and RSA key pairs with the new ones.

Prerequisites

The RSA key pair for certificate application has been created using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

One RSA key pair can be referenced only by one CMP session.

Example

Configure the RSA key pair to be referenced by CMP session **test** and update the RSA key pair during the certificate update.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.......................+++
.......................................................................
........+++
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request rsa local-key-pair test regenerate 2048
```

Related Topics

19.17.106 pki rsa local-key-pair create

19.17.95 pki import rsa-key-pair

19.17.15 cmp-request server url

Function

The **cmp-request server url** command specifies the URL address of a CMPv2 server.

The **undo cmp-request server url** command deletes the URL address of a CMPv2 server.

By default, the URL of a CMPv2 server is not configured.

Format

cmp-request server url [**esc**] *url-addr*

undo cmp-request server url

Parameters

Parameter	Description	Value
esc	Specifies the entering of URLs in the ASCII code.	-
url-addr	Specifies the URL of the CMPv2 server.	The value is a string starting with **http://** and consisting of 1 to 128 case-insensitive characters without spaces.

Views

CMP session view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Configure an URL for the CMPv2 server before certificate application. Then the PKI entity sends a request message to the server's URL.

A user cannot enter command lines that include a question mark (?). Therefore, keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Set the URL of the CMPv2 server for CMP session **test** to http://10.1.1.1:8080.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request server url http://10.1.1.1:8080
```

Set the URL of the CMPv2 server for CMP session **test** to http://www.***.com?page1\x3f.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request server url esc http://www.***.com\x3fpage1\\x3f
```

19.17.16 cmp-request verification-cert

Function

The **cmp-request verification-cert** command configures the certificate file for verifying the CA response signature.

The **undo cmp-request verification-cert** command deletes the certificate file for verifying the CA response signature.

By default, no certificate file for verifying the CA response signature is configured.

Format

cmp-request verification-cert *cert-file-name*

undo cmp-request verification-cert

Parameters

Parameter	Description	Value
cert-file-name	Specifies the certificate file name.	The value must be an existing certificate file name.

Views

CMP session view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After this command is executed, the device uses the configured certificate to verify the CA response signature. This command configures the CA certificate.

If this command is not executed and the CA response mode is signature, the device constructs a certificate chain based on the certificates in the response messages sent by the device itself and CA to verify the CA response signature. If the MAC mode is set, the device uses the MAC to verify the CA response signature. That is, this command does not take effect.

Prerequisites

The certificate file for verifying the CA response signature exists.

Example

Configure the certificate file for verifying the CA response signature.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] cmp-request verification-cert aa.der
```

19.17.17 common-name

Function

The **common-name** command configures a common name for an entity.

The **undo common-name** command cancels the configuration.

By default, a PKI entity does not have a common name.

Format

common-name *common-name*

undo common-name

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
common-name	Specifies the common name of an entity.	The value is a string of 1 to 64 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

After a PKI entity is created, a common name must be configured to uniquely identify the PKI entity.

After the common name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the common name of the PKI entity.

Example

Set the common name to **test** for an entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] common-name test
```

Related Topics

19.17.35 display pki entity

19.17.18 country (PKI entity view)

Function

The **country** command configures a country code for an entity.

The **undo country** command deletes the country code of a PKI entity.

By default, no country code is configured for a PKI entity.

Format

country *country-code*

 Copyright © Huawei Technologies Co., Ltd.

undo country

Parameters

Parameter	Description	Value
country-code	Specifies the country code of a PKI entity.	A country code must be two-character long. If the entered country code contains lower case letters, the system automatically changes the lower case letters into upper case letters when you create a certificate request file. You can query country codes in ISO3166. For example, CN is the legitimate country code of China, and US is the legitimate country code of the USA.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure the country code for the PKI entity, which is used as an alias of the entity.

After the country code is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this country code. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the country code of the PKI entity.

Example

Configure the country code to CN for a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] country CN
```

Related Topics

19.17.35 display pki entity

19.17.19 crl auto-update enable

Function

The **crl auto-update enable** command enables the automatic CRL update function.

The **undo crl auto-update enable** command disables the automatic CRL update function.

By default, automatic CRL update is enabled.

Format

crl auto-update enable

undo crl auto-update enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

To configure the automatic CRL update function, enable the function first.

Example

Enable the automatic certificate update function.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl auto-update enable
```

19.17.20 crl cache

Function

The **crl cache** command configures the device to use the cached CRL.

The **undo crl cache** command configures the device to retrieve the latest CRL each time.

 Copyright © Huawei Technologies Co., Ltd.

By default, the PKI realm is allowed to use cached CRLs.

Format

crl cache

undo crl cache

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The system overwrites the CRL in memory with the cached URL for certificate verification. If the PKI realm is not allowed to use cached CRL, the system must download the latest CRL every time to overwrite the CRL in memory.

Example

Allow the device to use the cached CRL in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] crl cache
```

19.17.21 crl http

Function

The **crl http** command enables automatic CRL update using HTTP.

By default, the CRL is updated automatically using HTTP.

Format

crl http

Parameters

None

Views

PKI realm view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using HTTP.

When the device automatically updates the CRL using HTTP, ensure that there is sufficient space in the device storage for the CRL file.

Example

Configure the automatic CRL update using HTTP.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl http
```

19.17.22 crl ldap

Function

The **crl ldap** command configures the device to automatically update CRL using LDAP and specifies the attribute and identifier used to obtain CRL from the LDAP server.

The **undo crl ldap** command deletes the attribute and identifier used to obtain CRL from the LDAP server.

By default, the system automatically updates CRL using HTTP.

Format

crl ldap

crl ldap [**attribute** *attr-value*] **dn** *dn-value*

undo crl ldap dn

Parameters

Parameter	Description	Value
attribute *attr-value*	Specifies the attribute value that a device uses to obtain a CRL from an LDAP server.	The value is a string of 1 to 64 case-sensitive characters. By default, the value is **certificateRevocationList**.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dn *dn-value*	Specifies the ID that a device uses to obtain a CRL from an LDAP server. The ID is generally composed of information, such as the user common name, organization name, country, or name of a certificate holder.	The value is a string of 1 to 128 case-sensitive characters, with spaces supported.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before you use LDAP to automatically update a CRL, run the **crl ldap** command.

When a PKI entity automatically updates CRL using LDAP, it queries the attribute and identifier of LDAP server in the CRL query packet and obtains CRL from the LDAP server. In this situation, run the **crl ldap** [**attribute** *attr-value*] **dn** *dn-value* command to specify the attribute and identifier used to obtain CRL from the LADP server.

Precautions

The attribute and identifier used to obtain CRL from the LDAP server can be configured only after the **crl ldap** command is executed.

Before selecting the LDAP mode, ensure that the CF card or Hda1 has sufficient space for the CRL file. This effectively avoids upgrade failures.

Example

Configure automatic CRL update using LADP.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl ldap
[Huawei-pki-realm-d1] crl ldap attribute abcde dn test
```

19.17.23 crl scep

Function

The **crl scep** command configures a device to use SCEP to automatically update a CRL.

By default, a device uses HTTP to automatically update a CRL.

Format

crl scep

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

This command is required when CRL is updated using SCEP.

Before the device automatically updates the CRL using SCEP, ensure that the device storage has sufficient space for the CRL file.

Example

Use SCEP to automatically update a CRL.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl scep
```

19.17.24 crl update-period

Function

The **crl update-period** command sets the interval for automatic CRL update.

The **undo crl update-period** command restores the default interval for automatic CRL update.

By default, the automatic CRL update interval is 8 hours.

Format

crl update-period *interval*

undo crl update-period

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the interval at which a CRL is automatically updated.	The value is an integer that ranges from 1 to 720, in hours.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The CRL update interval is the interval at which a PKI entity using a certificate downloads a CRL from the CRL storage server. The CA/RA does not issue the CRL to an entity. Instead, the entity initiates CRL query to obtain a CRL.

Example

Set the interval at which a CRL is automatically updated to 21 hours.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl update-period 21
```

19.17.25 display ldap-server template

Function

The **display ldap-server template** command displays the configurations of an LDAP server template.

Format

display ldap-server template [*template-name*]

Parameters

Parameter	Description	Value
template-name	Specifies the name of an LDAP server template.	The value must be an existing LDAP server template name.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

If no template is specified, the configurations of all LDAP servers are displayed.

Example

Display the configurations of an LDAP server.

```
<Huawei> display ldap-server template
  ----------------------------------------------------------------------
  Server-template-name              :  huawei
  Manager DN                      :
  Manager password                  :
  authentication-server             :  -:0
  ----------------------------------------------------------------------
  Total of LDAP template :1
```

Table 19-157 Description of the **display ldap-server template** command output

Item	Description
Server-template-name	Name of an LDAP server template. To configure the name, run the **ldap-server template** command.
Manager DN	Administrator Base DN for accessing an LDAP server. To configure the administrator Base DN, run the **ldap-server authentication manager** command.
Manager password	Administrator password for accessing an LDAP server. To configure the administrator password, run the **ldap-server authentication manager** command.
authentication-server	IP address and port of the LDAP server. To configure the IP address and port, run the **ldap-server authentication** command.
Total of LDAP template	Total number of LDAP server templates.

19.17.26 display pki ca-capability

Function

The **display pki ca-capability** displays the CA capabilities of a PKI realm.

Format

display pki ca-capability realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Indicates the name of a PKI realm.	The PKI realm name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display pki ca-capability** command displays the CA capabilities of a PKI realm.

If no command output is displayed, run the **pki get ca-capability realm** command in the diagnostic view to obtain the CA capabilities configured for the PKI realm.

Example

Display the CA capabilities of the PKI realm **asdf**.

```
<Huawei> display pki ca-capability realm asdf
 PKI CA Capabilities :
  GetNextCACert      :  ----
  POSTPKIOperation   :  ----
  Renewal            :  ----
  SHA-512            :  ----
  SHA-256            :  ----
  SHA-1              :  ----
  DES3               :  ----
```

Table 19-158 Description of the **display pki ca-capability** command output

Item	Description
PKI CA Capabilities	PKI CA capabilities.
GetNextCACert	Get next CA certificate.
POSTPKIOperation	Post PKI operation messages.
Renewal	Certificate renewal.
SHA-512	SHA-512 algorithm.
SHA-256	SHA-256 algorithm.
SHA-1	SHA-1 algorithm.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
DES3	DES3 algorithm.

19.17.27 display pki cert-req

Function

The **display pki cert-req** command displays the content of a certificate request file.

Format

display pki cert-req filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate request file.	The certificate request file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command displays content of a certificate request file, including the subject, public key algorithm, key modulus, attributes, and signature algorithm.

Example

Display the content of a certificate request file named **test.req**.

```
<Huawei> display pki cert-req filename test.req
Certificate Request:
    Data:
        Version: 0 (0x0)
        Subject: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:c4:01:cf:95:bb:fb:35:f0:3e:cd:1d:10:9e:11:
                    08:2e:77:48:ba:1b:e6:00:1b:43:30:56:f9:9a:6b:
                    ed:8b:fe:3e:03:57:38:02:48:88:e3:9b:39:d0:1c:
                    2b:8f:6a:9b:91:17:9b:ce:cb:fc:87:40:78:39:08:
                    1c:53:c3:71:cc:db:64:6f:ec:5a:cd:33:a5:68:5e:
```

```
                e6:52:61:ad:a1:58:55:f0:a0:0f:db:ab:05:eb:a4:
                fe:e1:68:61:8c:af:2c:3a:34:95:d2:41:ee:09:e7:
                b0:fc:59:d9:f4:12:00:de:ab:14:b6:a3:fe:29:75:
                f7:dd:7b:aa:03:81:fc:ae:41:8c:e4:ad:e3:d9:65:
                d4:be:a0:c1:e0:43:8a:91:ad:20:7b:6f:12:25:6e:
                0d:67:7d:4c:fe:8d:1b:6d:f3:96:07:31:ed:73:d3:
                71:6b:51:18:64:bd:41:d6:18:2d:2d:86:b7:fa:26:
                eb:cc:cb:a3:0f:0b:61:22:fd:dd:5f:b4:4d:9b:7d:
                bc:fa:af:e6:95:d7:27:f1:60:31:56:83:58:2c:40:
                1a:5e:6a:94:63:aa:70:2f:9b:00:e0:a3:9e:fb:73:
                62:5e:1c:3c:5f:48:42:7c:26:8f:5f:cf:39:b9:5d:
                25:90:8e:6c:e0:04:ec:e2:1b:1f:a8:0d:d2:ef:20:
                41:79
            Exponent: 65537 (0x10001)
        Attributes:
            challengePassword        :******
        Requested Extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.1.1.1, DNS:example.com, email:test@example.com
    Signature Algorithm: sha256WithRSAEncryption
        71:e7:c0:5f:36:c9:16:eb:fc:0c:8e:d1:4f:3d:ee:25:6b:47:
        65:86:4b:89:ec:22:01:42:a5:0e:5c:aa:01:0a:57:a9:25:ba:
        1b:59:6d:77:5f:74:80:3b:af:f9:37:75:97:9a:ca:80:73:8b:
        36:14:2c:4b:9a:2f:53:5c:5b:4a:93:31:88:94:0f:4d:58:84:
        36:41:e8:a8:6c:cd:f0:bb:9f:51:50:b2:a4:40:f4:ec:37:c5:
        42:08:69:b5:c5:fd:af:3d:8a:aa:47:53:d3:ce:bc:76:ec:47:
        ca:36:90:0b:49:2b:2f:04:c4:1f:f1:12:b6:99:d0:f8:33:d8:
        08:d0:32:ac:ee:34:0f:07:ef:72:9f:6b:71:80:3e:8d:37:cc:
        ca:b5:c1:56:3d:65:c7:e6:99:1b:2b:53:01:69:f5:8a:18:05:
        d1:b1:48:3e:50:e0:4c:7f:db:dc:b7:cd:a2:37:f9:96:cd:0d:
        ee:61:c2:80:61:6b:99:c0:76:0d:ab:2c:46:ce:b7:aa:6a:12:
        72:b7:6f:64:cc:78:b7:16:bd:c5:32:45:79:42:cf:4c:28:91:
        ce:cd:7d:da:eb:2b:3a:cf:90:1f:61:5e:02:25:fe:3c:82:66:
        d4:e8:c7:f8:5e:84:2c:f6:b2:f0:ba:ee:7a:c1:9b:d4:68:02:
        a4:e3:27:89
```

Table 19-159 Description of the **display pki cert-req** command output

Item	Description
Certificate Request	Information about a certificate request file.
Data	Data of a certificate request file.
Version	Version of a certificate request file.

Item	Description
Subject	Subject of a certificate request file. The subject includes the following attributes: ● C: country code of a PKI entity. It is configured using the **19.17.18 country (PKI entity view)** command. ● ST: name of the state or province to which a PKI entity belongs. It is configured using the **19.17.120 state (PKI entity view)** command. ● L: geographic area where a PKI entity is located. It is configured using the **19.17.61 locality** command. ● O: organization to which a PKI entity belongs. It is configured using the **19.17.67 organization** command. ● OU: department to which a PKI entity belongs. It is configured using the **19.17.66 organization-unit** command. ● CN: common name of a PKI entity. It is configured using the **19.17.17 common-name** command.
Subject Public Key Info	Information about the subject public key of a certificate request file.
Public Key Algorithm	Public key algorithm.
Public-Key	RSA public key. It is configured using the **19.17.116 rsa local-key-pair** command.
Modulus	Key modulus.
Exponent	Key exponent.
Attributes	Attributes of a certificate request file.
challengePassword	The challenge password used in certificate application. It is configured using the **19.17.78 pki enroll-certificate** command.
Requested Extensions	Certificate request extension.
X509v3 Subject Alternative Name	Alternative name of the X.509v3 subject.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
IP Address	IP address of a PKI entity. It is configured using the **19.17.53 ip-address** command.
DNS	DNS name of a PKI entity. It is configured using the **19.17.52 fqdn** command.
email	Email address of a PKI entity. It is configured using the **19.17.44 email** command.
Signature Algorithm	Signature algorithm. It is configured using the **19.17.47 enrollment-request signature message-digest-method** command.

19.17.28 display pki certificate

Function

The **display pki certificate** command displays the content about the CA or local certificate loaded to the device and OCSP server certificate.

Format

display pki certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

display pki certificate default { **ca** | **local** }

Parameters

Parameter	Description	Value
ca	Displays content about the CA certificate.	-
local	Displays content about the local certificate.	-
ocsp	Displays content about the Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.
default	Specifies the content of the default built-in certificate.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about the CA certificate, local certificate, and OCSP server's certificate, including signature algorithm, issuer, validity period, subject, and subject public key.

Example

Display information about the CA certificate.

```
<Huawei> display pki certificate ca realm abc
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f0:1a:f3:67:21:44:9a:4a:eb:ec:63:75:5d:d7:5f
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=ca_root
        Validity
            Not Before: Jun  4 14:58:17 2015 GMT
            Not After : Jun  4 15:07:10 2020 GMT
        Subject: CN=ca_root
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d9:5f:2a:93:cb:66:18:59:8c:26:80:db:cd:73:
                    d5:68:92:1b:04:9d:cf:33:a2:73:64:3e:5f:fe:1a:
                    53:78:0e:3d:e1:99:14:aa:86:9b:c3:b8:33:ab:bb:
                    76:e9:82:f6:8f:05:cf:f6:83:8e:76:ca:ff:7d:f1:
                    bc:22:74:5e:8f:4c:22:05:78:d5:d6:48:8d:82:a7:
                    5d:e1:4c:a4:a9:98:ec:26:a1:21:07:42:e4:32:43:
                    ff:b6:a4:bd:5e:4d:df:8d:02:49:5d:aa:cc:62:6c:
                    34:ab:14:b0:f1:58:4a:40:20:ce:be:a5:7b:77:ce:
                    a4:1d:52:14:11:fe:2a:d0:ac:ac:16:95:78:34:34:
                    21:36:f2:c7:66:2a:14:31:28:dc:7f:7e:10:12:e5:
                    6b:29:9a:e8:fb:73:b1:62:aa:7e:bd:05:e5:c6:78:
                    6d:3c:08:4c:9c:3f:3b:e0:e9:f2:fd:cb:9a:d1:b7:
                    de:1e:84:f4:4a:7d:e2:ac:08:15:09:cb:ee:82:4b:
                    6b:bd:c6:68:da:7e:c8:29:78:13:26:e0:3c:6c:72:
                    39:c5:f8:ad:99:e4:c3:dd:16:b5:2d:7f:17:e4:fd:
                    e4:51:7a:e6:86:f0:e7:82:2f:55:d1:6f:08:cb:de:
                    84:da:ce:ef:b3:b1:d6:b3:c0:56:50:d5:76:4d:c7:
                    fb:75
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C5
            X509v3 CRL Distribution Points:
```

```
                Full Name:
                  URI:http://vasp-e6000-127.china.huawei.com/CertEnroll/ca_root.
crl
                  URI:file://\\vasp-e6000-127.china.huawei.com\CertEnroll\ca_roo
t.crl

            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
         52:21:46:b8:67:c8:c3:4a:e7:f8:cd:e1:02:d4:24:a7:ce:50:
         be:33:af:8a:49:47:67:43:f9:7f:79:88:9c:99:f5:87:c9:ff:
         08:0f:f3:3b:de:f9:19:48:e5:43:0e:73:c7:0f:ef:96:ef:5a:
         5f:44:76:02:43:83:95:c4:4e:06:5e:11:27:69:65:97:90:4f:
         04:4a:1e:12:37:30:95:24:75:c6:a4:73:ee:9d:c2:de:ea:e9:
         05:c0:a4:fb:39:ec:5c:13:29:69:78:33:ed:d0:18:37:6e:99:
         bc:45:0e:a3:95:e9:2c:d8:50:fd:ca:c2:b3:5a:d8:45:82:6e:
         ec:cc:12:a2:35:f2:43:a5:ca:48:61:93:b9:6e:fe:7c:ac:41:
         bf:88:70:57:fc:bb:66:29:ae:73:9c:95:b9:bb:1d:16:f7:b4:
         6a:da:03:df:56:cf:c7:c7:8c:a9:19:23:61:5b:66:22:6f:7e:
         1d:26:92:69:53:c8:c6:0e:b3:00:ff:54:77:5e:8a:b5:07:54:
         fd:18:39:0a:03:ac:1d:9f:1f:a1:eb:b9:f8:0d:21:25:36:d5:
         06:de:33:fa:7b:c8:e9:60:f3:76:83:bf:63:c6:dc:c1:2c:e4:
         58:b9:cb:48:15:d2:a8:fa:42:72:15:43:ef:55:63:39:58:77:
         e8:ae:0f:34

Pki realm name: abc
Certificate file name: abc_ca.cer
Certificate peer name: -
```

Table 19-160 Description of the **display pki certificate** command output

Item	Description
The x509 object type is certificate.	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subject	Subject of a certificate. The subject includes the following attributes: ● C: country code of a PKI entity. ● ST: name of the state or province to which a PKI entity belongs. ● L: geographic area where a PKI entity is located. ● O: organization to which a PKI entity belongs. ● OU: department to which a PKI entity belongs. ● CN: common name of a PKI entity.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Key Usage	X509v3 key usage.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trusted.
X509v3 Subject Key Identifier	Identifier of a subject key.
X509v3 CRL Distribution Points	CRL distribution points.
Full Name	Full name of CDP.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

19.17.29 display pki certificate built-in-ca

Function

The **display pki certificate built-in-ca** command displays the content of the SSL decryption certificate uploaded on the device.

Format

display pki certificate built-in-ca

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

This command shows information about the SSL decryption certificate, including signature algorithm, issuer, validity period, subject, subject public key, PKI realm name, and certificate file name.

Example

Display information about the **built-in-ca** certificate.

```
<Huawei> display pki certificate built-in-ca
 The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f2:1c:74:f0:df:e0:2f:c6
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Validity
            Not Before: Oct 23 23:44:55 2015 GMT
            Not After : Oct 13 23:44:55 2055 GMT
        Subject: C=CN, ST=Jiangsu, L=Beijing, O=org1, OU=Group1,Sale, CN=huawei
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b1:63:50:17:73:de:cc:9e:2b:41:fe:0e:58:28:
                    47:b7:ce:6b:77:5c:29:b1:3e:cf:d3:e0:53:63:1e:
                    21:cc:f6:11:34:7c:eb:8a:d7:08:b5:96:c4:0b:4a:
                    4d:33:6c:77:23:21:51:bb:10:d6:7d:d3:82:a0:6a:
                    f5:f6:8d:17:e0:f2:73:99:7b:c7:89:c8:fc:61:42:
                    0b:a5:d7:1a:11:47:ed:e1:5f:60:a6:c5:93:f0:07:
                    3f:73:fe:80:16:98:02:23:df:ab:04:85:13:25:32:
                    61:69:e8:f3:ab:a0:d8:e9:41:f8:c2:5f:14:9e:b7:
                    3b:49:1d:48:b4:b2:8d:bf:b9:00:ee:25:5d:7a:11:
                    a6:d3:23:61:99:ad:0f:54:be:00:a1:58:dd:d2:91:
                    ad:5c:6f:9d:d0:8c:e0:6f:a3:4e:df:ba:fd:b1:e3:
                    6f:1b:b3:1f:e6:42:91:1c:1a:4f:a3:a7:0e:3c:2c:
                    4c:f9:18:1f:9d:22:f8:09:da:ff:a7:7c:b8:77:20:
                    19:8a:90:d0:00:21:e4:1f:41:cc:f0:0c:ba:8f:23:
                    c3:9f:f9:ae:d8:49:95:be:75:49:7d:d7:d0:ce:3c:
                    28:27:e9:11:02:4d:c0:1a:d0:f7:38:7f:94:f8:9c:
                    9d:78:71:43:50:d3:05:01:07:18:f4:2f:c5:ec:96:
                    5d:d5
                Exponent: 65537 (0x10001)
```

```
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                IP Address:10.1.1.1, DNS:example.com, email:test@example.com
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                3F:D2:BC:62:6B:F5:10:29:C4:59:9D:B9:71:A7:EB:B1:C4:16:91:9F
            Netscape Cert Type:
                SSL CA
            Netscape Comment:
                example comment extension
    Signature Algorithm: sha1WithRSAEncryption
        89:d5:47:31:23:c3:f9:df:fd:96:c5:38:fb:1e:b5:52:00:bd:
        21:fd:f0:18:af:8e:e8:01:b7:e6:b3:a1:0e:51:4b:61:4d:d5:
        52:1e:60:60:6a:67:9f:82:90:e3:1d:97:36:8f:c4:30:20:f4:
        14:58:4c:78:61:3c:4a:d4:0f:98:a9:05:e0:b5:cb:6a:78:eb:
        c6:40:9d:00:7b:31:8d:0e:21:72:db:31:34:83:5d:e5:42:98:
        85:09:6d:1e:c5:23:ce:e3:72:46:67:79:4b:1b:18:ba:cb:5e:
        ba:08:ee:0e:24:e5:58:07:0c:2e:b8:cf:e6:6b:09:67:76:80:
        e5:0e:66:a2:cb:3a:a1:bc:56:27:1c:1b:fd:5a:b5:ad:9f:a4:
        32:2b:32:3e:9a:9d:f5:04:ee:e5:e1:1c:76:8a:c2:45:f1:3e:
        8c:da:ab:f6:cf:82:d0:b3:4c:91:7a:c8:ad:b5:2c:28:54:e0:
        79:40:b6:b5:f1:6f:92:23:4d:94:8b:20:0d:92:86:43:98:17:
        d5:9b:b0:7f:99:f2:f1:df:0f:d3:f2:5c:9d:35:bc:64:25:13:
        39:62:ba:98:cb:cc:6a:08:fc:2c:86:2e:2e:91:80:8b:3e:27:
        14:f7:45:fe:9f:f8:1a:87:05:c9:21:c3:61:d1:69:82:e3:05:
        5c:44:c5:82

Pki realm name: -
Certificate file name: buzzcer
Certificate peer name: -
```

Table 19-161 Description of the **display pki certificate built-in-ca** command output

Item	Description
The x509 object type is certificate	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subject	Certificate subject. The subject includes the following attributes: ● C: country code of a PKI entity. It is configured using the **19.17.18 country (PKI entity view)** command. ● ST: name of the state or province to which a PKI entity belongs. It is configured using the **19.17.120 state (PKI entity view)** command. ● L: geographic area where a PKI entity is located. It is configured using the **19.17.61 locality** command. ● O: organization to which a PKI entity belongs. It is configured using the **19.17.67 organization** command. ● OU: department to which a PKI entity belongs. It is configured using the **19.17.66 organization-unit** command. ● CN: common name of a PKI entity. It is configured using the **19.17.53 ip-address** command.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm. It is configured using the **19.17.106 pki rsa local-key-pair create** command.
Public-Key	RSA public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Subject Alternative Name	Alternative name of the X.509v3 subject.
IP Address	IP address of the PKI entity. It is configured using the **19.17.53 ip-address** command.
DNS	DNS name of a PKI entity. It is configured using the **19.17.52 fqdn** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
email	Email address of a PKI entity. It is configured using the **19.17.44 email** command.
X509v3 Basic Constraints	Basic constraints.
CA	Whether the CA can be trust.
X509v3 Key Usage	X.509v3 key use.
X509v3 Subject Key Identifier	Identifier of a X.509v3 subject key.
Netscape Cert Type	Netscape Certificate Type.
Netscape Comment	Netscape Comment.
Signature Algorithm	Signature algorithm.
Pki realm name	PKI realm name. It is configured using the **19.17.103 pki realm (system view)** command.
Certificate file name	Name of a certificate file. It is configured using the **19.17.86 pki generate built-in-ca certificate** command.
Certificate peer name	Name of a certificate peer. It is configured using the **19.17.92 pki import-certificate peer** command.

19.17.30 display pki certificate enroll-status

Function

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Format

display pki certificate enroll-status [**realm** *realm-name*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The PKI realm name must already exist.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki certificate enroll-status** command displays the certificate enrollment status.

Example

Display the certificate enrollment status.

```
<Huawei> display pki certificate enroll-status realm abc
 Certificate Request Transaction 1
    Status: Pending
    Key Usage: ENC&SIG
    Entity name: test
    Remain polling count: 1
    Next polling after : 35 seconds
<Huawei> display pki certificate enroll-status realm abc
 info: No certificate request transaction in realm abc.
```

Table 19-162 Description of the **display pki certificate enroll-status** command output

Item	Description
Certificate Request Transaction	Certificate enrollment request process.
Status	Certificate enrollment status. Pending: A certificate is being enrolled.
Key Usage	Functions of a certificate public key: ● ENC: The public key is used for encryption. ● SIG: The public key is used for signature.
Entity name	Entity name.
Remain polling count	Number of times a certificate enrollment request can be initiated again.
Next polling after	Next time a certificate enrollment request is initiated.
No certificate request transaction	There is no certificate enrollment request process.

 Copyright © Huawei Technologies Co., Ltd.

19.17.31 display pki certificate filename

Function

The **display pki certificate** command displays the content about the CA or local certificate loaded to the device and OCSP server certificate.

Format

display pki certificate filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about the certificate including signature algorithm, issuer, validity period, subject, and subject public key.

Example

Display information about the certificate ca.cer.

```
<Huawei> display pki certificate filename ca.cer
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            f3:a3:3a:46:f6:09:8d:18
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
        Validity
            Not Before: May 16 11:48:04 2017 GMT
            Not After : May 14 11:48:04 2027 GMT
        Subject: C=CN, ST=JS, L=NJ, O=HW, OU=VPN, CN=CA-210235G7G410FB000060
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:ba:cc:ef:2f:55:9c:d0:09:c5:1b:d2:52:63:92:
                    c8:f0:88:ed:1b:88:f1:e4:3c:90:07:85:01:8c:d5:
                    80:d9:91:ef:64:e9:79:0c:7d:0e:b9:6c:00:a2:72:
                    e2:1b:aa:9b:2d:11:6b:6f:2d:de:5d:58:22:cf:9e:
                    2f:7d:f1:ad:71:e9:25:0e:bc:26:f1:77:57:02:3d:
                    7f:09:8f:49:63:ae:11:75:57:65:a0:bd:9c:94:c6:
```

```
                df:21:f7:c8:5a:4d:5e:f8:5e:84:b0:b0:fd:a6:c7:
                e0:78:d1:1c:8a:55:d9:e9:66:1c:e5:4e:ce:88:dd:
                fa:0f:60:d0:7e:86:a1:ec:b1:34:aa:f7:dd:72:c6:
                0a:90:c7:4a:6b:a0:86:01:30:b6:6f:23:ff:ce:ae:
                39:fb:de:18:ce:2f:b9:d7:17:09:8c:29:19:34:7a:
                69:75:dc:ee:bf:2e:d4:93:fb:f6:a6:5b:f8:2a:6d:
                fe:bd:f4:8b:30:49:5c:a8:94:76:12:9d:64:78:4a:
                48:d3:2d:63:da:0a:79:b2:ee:8e:2d:5a:a0:71:99:
                cf:b9:68:77:d3:d9:cf:12:64:80:bb:42:8c:28:1f:
                d9:bf:7c:4b:8f:39:1e:dc:92:a4:ff:8e:b3:02:58:
                c5:79:96:f2:a1:f9:17:cb:ea:49:57:b0:b0:3c:af:
                db:19
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                83:08:A4:F4:BC:EC:1B:B6:7D:B0:27:F6:10:47:77:AA:2A:66:59:D5
            Netscape Cert Type:
                SSL CA
    Signature Algorithm: sha256WithRSAEncryption
        1e:6b:2a:76:7e:8e:b0:0e:72:4e:02:53:b0:77:0d:13:28:4e:
        c3:e5:f8:0b:76:fd:56:2c:e6:5b:d1:f8:48:19:17:95:1a:79:
        5e:d9:50:b9:68:bd:36:c4:ce:7b:ce:0c:98:55:b1:44:9f:20:
        66:66:33:3c:b5:40:ad:50:c8:64:1c:07:0e:08:42:72:88:35:
        d4:af:f0:8d:5d:64:90:5d:ec:f0:5c:07:76:10:ed:9b:22:18:
        ef:44:4e:c2:29:32:40:68:fe:04:dc:0e:f6:2b:25:c2:73:f5:
        9b:64:df:25:56:c6:bb:6e:a4:2f:07:b3:9d:c0:18:60:72:cb:
        51:62:94:ee:f7:21:0a:a0:92:58:a1:bf:c8:30:0e:0c:0a:91:
        cb:f4:8f:07:52:ba:df:25:88:8a:b3:3f:f0:68:fa:4c:b7:31:
        c8:97:e0:49:08:8a:74:fc:c2:90:d7:3c:0b:00:38:90:3b:19:
        ab:66:96:24:1f:86:b9:62:49:6d:9c:2d:02:99:38:bb:96:b6:
        dd:0f:3c:6e:24:7b:3d:1e:77:58:e7:46:2b:42:cc:14:6a:a4:
        16:45:ed:3c:b1:d6:30:94:c0:30:d0:46:fa:bc:da:9a:2b:f1:
        fa:f3:df:1b:84
```

Table 19-163 Description of the **display pki certificate filename** command output

Item	Description
The x509 object type is certificate.	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Subject	Subject of a certificate. The subject includes the following attributes: ● C: country code of a PKI entity. ● ST: name of the state or province to which a PKI entity belongs. ● L: geographic area where a PKI entity is located. ● O: organization to which a PKI entity belongs. ● OU: department to which a PKI entity belongs. ● CN: common name of a PKI entity.
Subject Public Key Info	Information about the public key of a certificate.
Public Key Algorithm	Public key algorithm.
Public-Key	Public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X.509v3 certificate extensions.
X509v3 Basic Constraints	X.509v3 basic constraints.
CA	Whether the CA can be trusted.
X509v3 Subject Key Identifier	Identifier of a X.509v3 subject key.
X509v3 Key Usage	X509v3 key usage.
Netscape Cert Type	Netscape certificate type.

19.17.32 display pki cmp statistics

Function

The **display pki cmp statistics** command displays the statistics on CMP sessions.

Format

display pki cmp statistics [**session** *session-name*]

Parameters

Parameter	Description	Value
session *session-name*	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays statistics on CMP sessions, including the number of sent IR packets, sent CR packets, sent KUR packets, and received IP packets.

If a CMP session is specified, the statistics of the session is displayed. If no CMP session is specified, the statistics of all sessions is displayed.

Example

Display statistics on CMP session test.

```
<Huawei> display pki cmp statistics session test
 CMP Context Name: test
 Ir Send Counts        : 0
 Cr Send Counts        : 0
 Kur Send Counts       : 0
 PollReq Send Counts   : 0
 Ip Receive Counts     : 0
 Cp Receive Counts     : 0
 Kup Receive Counts    : 0
 PollRep Receive Counts: 0
```

Table 19-164 Description of the **display pki cmp statistics** command output

Item	Description
CMP Context Name	Name of the CMP session.
Ir Send Counts	Total number of IR packets sent during the session.
Cr Send Counts	Total number of CR packets sent during the session.
Kur Send Counts	Total number of KUR packets sent during the session.
PollReq Send Counts	Total number of requests sent in polling mode during the session.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Ip Receive Counts	Number of IP packets received during the session.
Cp Receive Counts	Number of CP packets received during the session.
Kup Receive Counts	Number of KUP packets received during the session.
PollRep Receive Counts	Number of responses received in polling mode during the session.

19.17.33 display pki credential-storage-path

Function

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

By default, the certificate file is stored in sd1:/.

Format

display pki credential-storage-path

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display pki credential-storage-path** command displays the default path where a PKI certificate is stored.

Example

Display the default path where a PKI certificate is stored.

```
<Huawei> display pki credential-storage-path
 The pki credential-storage-path is sd1:/ .
```

19.17.34 display pki crl

Function

The **display pki crl** command displays the content of the CRL in the device.

Format

display pki crl { **realm** *realm-name* | **filename** *filename* }

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm associated with the CRL.	The PKI realm name must already exist.
filename *filename*	Specifies the file name of the certificate to be imported.	The certificate file name must already exist.

Views

All views

Default Level

3: Management level

Usage Guidelines

This command shows information about local CRL, including signature algorithm, issuer, update time, revoked certificate, CRL sequence number, and revocation time.

Example

Display information about the CRL associated with the PKI realm **abc**.

```
<Huawei> display pki crl realm abc
 The x509 object type is CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: /CN=ca_root
        Last Update: Dec 15 08:24:28 2015 GMT
        Next Update: Dec 22 20:44:28 2015 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:B8:63:72:A4:5E:19:F3:B1:1D:71:E1:37:26:E1:46:39:01:B6:82:C
5
            1.3.6.1.4.1.311.21.1:
                ...
            X509v3 CRL Number:
                365
            1.3.6.1.4.1.311.21.4:
151222083428Z    .
```

```
Revoked Certificates:
    Serial Number: 28C63371000000003E04
        Revocation Date: Dec 15 08:34:27 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 28C2AB44000000003E01
        Revocation Date: Dec 15 08:30:35 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2364247C000000003D48
        Revocation Date: Dec 14 07:29:05 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 23627E0F000000003D47
        Revocation Date: Dec 14 07:27:29 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Serial Number: 2360F397000000003D46
        Revocation Date: Dec 14 07:25:48 2015 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
                Key Compromise
    Signature Algorithm: sha1WithRSAEncryption
         7a:71:54:d1:66:13:6f:9f:62:03:ac:9a:5f:42:10:15:87:46:
         e2:a1:49:0f:44:19:ce:ed:6f:c3:0e:9f:31:fe:62:d5:08:0b:
         a4:a7:7e:80:4d:9a:5b:a9:55:5c:1a:73:30:62:48:e1:28:0e:
         5b:bd:ae:04:7e:83:36:43:62:fc:f7:12:0d:f9:f6:ac:2b:be:
         9c:50:6c:67:19:43:12:31:67:c2:06:31:97:e1:34:75:1c:87:
         53:5f:e6:15:a1:33:ad:00:e7:14:68:59:05:67:28:78:a0:91:
         49:7b:ab:87:9f:9e:53:18:4b:54:53:1c:b7:1c:2d:3e:b3:57:
         63:95:1d:01:29:9e:6c:41:07:40:2d:28:d8:82:7b:d6:22:e6:
         0d:0c:4c:af:84:96:8e:f1:29:28:d4:9e:1c:37:3b:1b:2e:34:
         a7:15:e3:29:d1:c0:69:0a:7f:24:b1:ce:00:f1:b3:da:ef:8a:
         1b:14:36:f9:14:6c:b0:66:86:a8:92:95:fc:e3:78:aa:d6:d0:
         cb:4d:26:b4:bc:41:c4:47:19:d0:2a:0c:ac:c6:aa:95:c2:03:
         33:8a:39:45:3e:c3:ad:46:7d:8a:03:4d:08:e2:d0:9a:ae:39:
         fa:8d:61:d0:1c:6c:03:d4:48:2e:4d:37:60:a1:06:a4:ea:c8:
         0d:20:59:c2

Pki realm name: abc
CRL file name: abc.crl
```

Table 19-165 Description of the **display pki crl** command output

Item	Description
The x509 object type is CRL	x509 object type is CRL.
Certificate Revocation List (CRL)	Information about the CRL.
Signature Algorithm	Algorithm of signature.
Issuer	Information of issuer.
Last Update	Last time the CRL has been updated.
Next Update	Next time the CRL will be updated.
CRL extensions	CRL extended attribute.
X509v3 Authority Key Identifier	X509v3 authority key identifier.

Item	Description
X509v3 CRL Number	X509v3 CRL number.
Revoked Certificates	Certificate that is revoked.
Serial Number	Serial number of the CRL.
Revocation Date	Date when the certificate was revoked.
CRL entry extensions	CRL entry extensions.
X509v3 CRL Reason Code	Reason why CRL is revoked.
Signature Algorithm	Signature algorithm. It is configured using the **19.17.47 enrollment-request signature message-digest-method** command.
Pki realm name	PKI realm name. It is configured using the **19.17.103 pki realm (system view)** command.
CRL file name	CRL file name. It is configured using the **19.17.93 pki import-crl** command.

19.17.35 display pki entity

Function

The **display pki entity** command displays information about PKI entities.

Format

display pki entity [*entity-name*]

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity. If the *entity-name* parameter is not specified, information about all entities is displayed.	The value must be an existing PKI entity name.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command displays information about PKI entities, including names, common names, countries, province, and location where the entities reside, and organizations to which entities belong.

Example

Display information about all PKI entities.

```
<Huawei> display pki entity
PKI Entity Information:

  Entity Name      : a
  Common name      : chi
  Country          : -
  State            : A
  Locality         : -
  Organization     : A
  Organization unit: -
  FQDN             : www. e
  IP address       : -
  Email            : -
  Serial-number    : -
 Total Number: 1
```

Table 19-166 Description of the **display pki entity** command output

Item	Description
PKI Entity Information	Information of the PKI entity.
Entity Name	Entity name. It is configured using the **19.17.79 pki entity** command.
Common name	Common name of the entity. It is configured using the **19.17.17 common-name** command.
Country	Country where a PKI entity resides. It is configured using the **19.17.18 country (PKI entity view)** command.
State	Province where a PKI entity resides. It is configured using the **19.17.120 state (PKI entity view)** command.
Locality	Location of a PKI entity. It is configured using the **19.17.61 locality** command.
Organization	Organization to which a PKI entity belongs. It is configured using the **19.17.67 organization** command.
Organization unit	Organization unit to which a PKI entity belongs. It is configured using the **19.17.66 organization-unit** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
FQDN	FQDN name of a PKI entity. It is configured using the **19.17.52 fqdn** command.
IP address	IP address of a PKI entity. It is configured using the **19.17.53 ip-address** command.
Email	Email address. It is configured using the **19.17.44 email** command.
Serial-number	Serial number of the entity. It is configured using the **19.17.117 serial-number** command.

Related Topics

19.17.79 pki entity
19.17.18 country (PKI entity view)
19.17.120 state (PKI entity view)
19.17.61 locality
19.17.67 organization
19.17.66 organization-unit
19.17.17 common-name
19.17.53 ip-address
19.17.52 fqdn
19.17.44 email
19.17.117 serial-number

19.17.36 display pki ocsp cache detail

Function

The **display pki ocsp cache detail** displays the detail information of the OCSP cache.

Format

display pki ocsp cache detail

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run this command to view detail information of the OCSP cache.

Example

Display the detail information of the OCSP cache.

```
<Huawei> display pki ocsp cache detail
====================================================
Cache Hash Status Info:
num_items             = 0
num_nodes             = 8
num_alloc_nodes       = 16
num_expands           = 0
num_expand_reallocs   = 0
num_contracts         = 0
num_contract_reallocs = 0
num_hash_calls        = 0
num_comp_calls        = 0
num_insert            = 0
num_replace           = 0
num_delete            = 0
num_no_delete         = 0
num_retrieve          = 0
num_retrieve_miss     = 0
num_hash_comps        = 0

Cache Hash Node Status Info:
node      0 ->   0
node      1 ->   0
node      2 ->   0
node      3 ->   0
node      4 ->   0
node      5 ->   0
node      6 ->   0
node      7 ->   0

Cache Hash Node Usage Status Info:
0 nodes used out of 8
0 items
====================================================
```

Table 19-167 Description of the **display pki ocsp cache detail** command output

Item	Description
Cache Hash Status Info	Hash status of the OCSP cache.
num_items	Number of available hash elements.
num_nodes	Number of requested hash nodes.
num_alloc_nodes	Maximum number of hash nodes that can be expanded.
num_expands	Number of hash node expansion application times.

Item	Description
num_expand_reallocs	Number of expanded hash nodes.
num_contracts	Number of hash node reduction times.
num_contract_reallocs	Number of reduced hash nodes.
num_hash_calls	Number of times the hash function is invoked.
num_comp_calls	Number of times the hash comparison function is invoked.
num_insert	Number of inserted hash nodes.
num_replace	Number of replaced hash nodes.
num_delete	Number of deleted hash nodes.
num_no_delete	Number of undeleted hash nodes.
num_retrieve	Number of times the hash nodes in the OCSP cache are matched.
num_retrieve_miss	Number of times the hash nodes in the OCSP cache are not matched.
num_hash_comps	Number of times the hash nodes in the OCSP cache are compared.
Cache Hash Node Status Info	Hash node status in the OCSP cache. For example, **node 0 -> 0** indicates that the number 0 node is unused; **node 0 -> 1** indicates that the number 0 node is in use.
Cache Hash Node Usage Status Info	Hash node use status in the OCSP cache.
n nodes used out of 8	There are 8 hash nodes, and n nodes are in use.
n items	The nth hash element.

19.17.37 display pki ocsp cache statistics

Function

The **display pki ocsp cache statistics** command displays statistics about cached OCSP responses.

Format

display pki ocsp cache statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command shows statistics about cached OCSP responses, including the maximum number of OCSP responses that can be cached, cache update interval, and number of cached responses.

Example

Display statistics about cached OCSP responses.

```
<Huawei> display pki ocsp cache statistics

=====================================================
   OCSP Cache Function: Enable
   OCSP Cache Max Number: 2
   OCSP Cache Refresh Interval: 5 minutes
   OCSP Cache Current Number: 0
=====================================================
```

Table 19-168 Description of the **display pki ocsp cache statistics** command output

Item	Description
OCSP Cache Function	Whether OCSP caching is enabled. ● Enable ● Disable It is configured using the **19.17.100 pki ocsp response cache enable** command.
OCSP Cache Max Number	Maximum size of OCSP cache. It is configured using the **19.17.101 pki ocsp response cache number** command.
OCSP Cache Refresh Interval	OCSP cache update interval. It is configured using the **19.17.102 pki ocsp response cache refresh interval** command.
OCSP Cache Current Number	Number of cached OCSP responses.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.17.100 pki ocsp response cache enable
19.17.101 pki ocsp response cache number
19.17.102 pki ocsp response cache refresh interval

19.17.38 display pki ocsp server down-information

Function

The **display pki ocsp server down-information** command displays the DOWN state information of the OCSP server recorded on the device.

Format

display pki ocsp server down-information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to DOWN. In this case, the device will not send OCSP requests to the URL for 10 minutes.

Example

Display the DOWN state information of the OCSP server.

```
<Huawei> display pki ocsp server down-information

=====================================================

  Server URL: http://10.1.1.1/ocsp
  Timeout Times: 1
  Last timeout until now: 5 seconds
=====================================================
```

Table 19-169 Description of the **display pki ocsp server down-information** command output

Item	Description
Server URL	URL of an unreachable OCSP server. It is configured using the **19.17.64 ocsp url** command.
Timeout Times	Connection timeouts.
Last timeout until now	Time elapsed since the last connection timeout and now.

19.17.39 display pki peer-certificate

Function

The **display pki peer-certificate** command displays the imported certificates of the remote device.

Format

display pki peer-certificate { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate.	The value must be an existing peer certificate file name.
all	Displays brief information about all certificates of the remote device.	-

Views

All views

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command shows information about imported certificates of the remote device, including signature algorithm, issuer, validity period, subject, public key, and PKI realm.

Example

Display brief information about all certificates of the remote device.

```
<Huawei> display pki peer-certificate all
  Peer certificate name :abcd
  Serial Number:
    12 19 3c d3 00 00 00 00 04 9a
  Subject:
    CN=a

Total Number: 1
```

Display detailed information about the certificate **abcd** of the remote device.

```
<Huawei> display pki peer-certificate name abcd
The x509 object type is certificate:
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            12:19:3c:d3:00:00:00:00:04:9a
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: CN=CA_ROOT
        Validity
            Not Before: Feb 19 13:00:22 2013 GMT
            Not After : Feb 19 13:10:22 2014 GMT
        Subject: CN=a
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (512 bit)
                Modulus:
                    00:b9:8b:47:65:a9:99:ed:58:b2:63:74:65:56:d1:
                    08:bb:1d:8f:4e:ed:72:a2:4a:ef:d8:45:3d:53:db:
                    c8:eb:df:53:9e:5f:c7:96:46:65:14:1a:ab:72:e9:
                    a2:71:c8:7a:f0:51:0c:cc:39:bb:14:75:7d:f1:bc:
                    88:2c:a7:2e:e9
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                E2:5B:8A:03:58:01:C8:E3:14:BC:18:5B:F9:BD:00:68:5B:D1:90:4E
            X509v3 Authority Key Identifier:
                keyid:CE:BA:CA:39:C7:AD:6A:CB:85:17:D0:8A:8E:28:02:0B:52:D4:D9:2
B

            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://10.1.1.1:8080/CertEnroll/CA_ROOT.crl

            Authority Information Access:
                CA Issuers - URI:ldap:///CN=CA_ROOT,CN=AIA,CN=Public%20Key%20Ser
vices,CN=Services,CN=Configuration,DC=esap,DC=com?cACertificate?base?objectClass
=certificationAuthority
                CA Issuers - URI:http://www.example.com/CertEnroll/www.example.c
om_CA_ROOT.crt

            1.3.6.1.4.1.311.20.2:
                .0.I.P.S.E.C.I.n.t.e.r.m.e.d.i.a.t.e.O.f.f.l.i.n.e
    Signature Algorithm: sha1WithRSAEncryption
         bb:8b:77:af:ae:df:2e:0c:bd:7a:29:6e:76:23:ad:7d:69:6d:
```

```
        0d:16:d9:18:82:ad:4f:52:b3:cd:1c:1a:fc:34:00:33:36:8d:
        47:2a:20:24:52:b7:02:75:cc:ab:3b:4c:f8:2a:a9:a9:4f:46:
        fb:c2:21:00:c1:b5:c2:67:0c:b1:99:2a:62:7b:71:4d:e7:c2:
        93:29:bb:ec:b1:e9:28:82:2f:77:61:ec:28:66:35:cb:5f:15:
        04:73:77:d8:26:91:7b:a2:56:74:51:33:0b:f1:04:28:24:b2:
        71:58:ad:5c:f8:96:17:0d:f7:b7:5f:4b:b9:ed:09:79:bc:54:
        21:c5:9b:90:f7:7b:21:aa:5a:aa:6f:51:e4:79:ce:b8:35:8b:
        19:90:51:94:e6:c2:61:f8:24:46:85:4c:a9:69:bd:8a:ef:c2:
        64:b8:19:ab:0b:6b:ec:34:41:8d:43:43:44:d1:1b:4c:4a:23:
        cd:40:52:7a:2e:8c:5d:b6:62:55:93:45:c8:3e:de:b1:51:82:
        d0:bb:7c:b8:09:7b:97:08:7b:93:17:40:a8:6f:2d:ed:f4:3e:
        36:10:2a:20:e3:47:e1:fb:ad:fe:97:73:a7:53:d0:f8:52:ca:
        b6:0e:e8:f1:df:6c:7a:37:39:bb:82:f9:03:c9:4a:71:65:df:
        6f:37:e6:b7

Pki realm name: -
Certificate file name: -
Certificate peer name: abcd
```

Table 19-170 Description of the **display pki peer-certificate** command output

Item	Description
Peer certificate name	Peer certificate name.
The x509 object type is certificate	x509 object type is certificate.
Certificate	Information about a certificate.
Data	Data of a certificate.
Version	Version of a certificate.
Serial Number	Serial number of a certificate.
Signature Algorithm	Signature algorithm of a certificate.
Issuer	Issuer of a certificate.
Validity	Validity period of a certificate.
Subject	Subject of the certificate.
Subject Public Key Info	Public key of the certificate.
Public Key Algorithm	Algorithm of the Public key.
Public-Key	Information about the RSA public key.
Modulus	Key modulus.
Exponent	Key exponent.
X509v3 extensions	X509v3 certificate extensions.
X509v3 Subject Key Identifier	Identifier of a subject key.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
X509v3 CRL Distribution Points	CRL distribution points.
Full Name	Full name of CDP.
Authority Information Access	Authority information access.
Pki realm name	PKI realm name.
Certificate file name	Certificate file name.
Certificate peer name	Certificate peer name.

19.17.40 display pki realm

Function

The **display pki realm** command displays PKI realm information.

Format

display pki realm [*realm-name*]

Parameters

Parameter	Description	Value
realm-name	Displays the detailed information about a PKI realm. If the parameter is left blank, information about all PKI realms is displayed.	The PKI realm name must already exist.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

This command displays details about a PKI realm, including PKI realm name, associated CA, CA certificate subject name, URL of the certificate enrolled through SCEP, PKI entity name, digital fingerprint algorithm of CA certificate, and digital fingerprint of CA certificate.

Example

Display information about all PKI realms.

```
<Huawei> display pki realm abc
 Realm Name : abc
 CA ID: CA_ROOT
 CA Name: "/CN=ca_root"
 Enrollment URL: http://10.136.7.196:8080/certsrv/mscep/mscep.dll
 Certificate Request Interval(Minutes): 1
 Certificate Request Times: 5
 Enrollment Mode: RA
 Enrollment Method: SCEP
 Entity Name: abc
 CA Certificate Fingerprint Arithmetic: sha256
 CA Certificate Fingerprint: e71add0744360e91186b828412d279e06dcc15a4ab4bb3d1384
2820396b526a0
 OCSP Nonce: Enable
 OCSP URL: -
 Method for Getting CRL: HTTP
 CDP URL: -
 Certificate Revocation Check Method: -
 RSA Key Name: abc
 SM2 Key Name:
 Auto-enroll: Enable
 Auto-enroll Percent: 100%
 Auto-enroll Regenerate: Enable
 Auto-enroll Regenerate Key-size: 2048
 Auto-enroll Updated-effective: Disable
 Password Cipher: Enable
 Password: %^%#:,3/YY@~[@(`1DBbZ&o$s`B\@S+3:UT0tF9EzSM:%^%#
 Crl Update-period(Hours): 8
 Crl Cache: Enable
 Key-usage: -
 Vpn-instance: -
 Source Interface: -
 Enrollment-request Signature Message-digest-method: SHA256

 Total Number: 1
```

Table 19-171 Description of the **display pki realm** command output

Item	Description
Realm Name	PKI realm name. It is configured using the **19.17.103 pki realm (system view)** command.
CA ID	ID of the CA associated with the PKI realm.
CA Name	Subject name of a CA certificate.
Enrollment URL	URL of the certificate enrolled on the SCEP server. It is configured using the **19.17.48 enrollment-url** command.
Certificate Request Interval(Minutes)	Interval between two certificate enrollment status queries.

Item	Description
Certificate Request Times	Maximum number of certificate enrollment status queries.
Enrollment Mode	Certificate enrollment mode (whether enrolled through RA). It is configured using the **19.17.48 enrollment-url** command.
Enrollment Method	Certificate enrollment method, including: • SCEP: obtains certificate from CA using the SCEP protocol. • Self-Signed: obtains certificate using self-signature.
Entity Name	PKI entity name. It is configured using the **19.17.49 entity** command.
CA Certificate Fingerprint Arithmetic	Fingerprint algorithm of the CA certificate. It is configured using the **19.17.51 fingerprint** command.
CA Certificate Fingerprint	Digital fingerprint of the CA certificate. It is configured using the **19.17.51 fingerprint** command.
OCSP Nonce	Whether a nonce extension is added to the OCSP request sent by a PKI entity. • Enable: A nonce extension is added to the OCSP request sent by a PKI entity. • Disable: A nonce extension is not added to the OCSP request sent by a PKI entity. It is configured using the **19.17.62 ocsp nonce enable** command.
OCSP URL	OCSP server's URL. It is configured using the **19.17.64 ocsp url** command.
Method for Getting CRL	Method of obtaining CRL. • SCEP: updates the CRL automatically using SCEP. It is configured using the **19.17.23 crl scep** command. • HTTP: updates the CRL automatically using HTTP. It is configured using the **19.17.21 crl http** command. • LDAP: updates the CRL automatically using LDAP. It is configured using the **19.17.22 crl ldap** command.
CDP URL	URL of the CDP. It is configured using the **19.17.4 cdp-url** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Crl Cache	Whether the PKI realm is allowed to use the CRL in cache. ● Enable: The PKI realm is allowed to use the CRL in cache. ● Disable: The PKI realm is not allowed to use the CRL in cache. To configure whether to allow the PKI realm to use the CRL in cache, run the **19.17.20 crl cache** command.
Certificate Revocation Check Method	Certificate status check method. It is configured using the **19.17.5 certificate-check** command.
RSA Key Name	RSA key. It is configured using the **19.17.116 rsa local-key-pair** command.
SM2 Key Name	SM2 key.
Auto-enroll	Whether automatic certificate enrollment is enabled. ● Enable: Automatic certificate enrollment is enabled. ● Disable: Automatic certificate enrollment is disabled. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Percent	The percentage of the certificate's validity period. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Regenerate	Whether the RSA key pair will be generated during certificate updates. ● Enable: The RSA key pair will be generated during certificate updates. ● Disable: The RSA key pair will not be generated during certificate updates. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Regenerate Key-size	RSA key length. It is configured using the **19.17.1 auto-enroll** command.
Auto-enroll Updated-effective	Whether the certificate takes effect immediately after being updated. ● Enable: The certificate takes effect immediately after being updated. ● Disable: The certificate does not take effect immediately after being updated. It is configured using the **19.17.1 auto-enroll** command.
Password Cipher	Whether the challenge password can be used. ● Enable: The challenge password can be used. ● Disable: The challenge password cannot be used.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Password	Password used to apply for or revoke a certificate. It is configured using the **19.17.68 password (PKI realm view)** command.
Crl Update-period(Hours)	CRL update interval. It is configured using the **19.17.24 crl update-period** command.
Key-usage	Purpose information carried in a certificate request packet. It is configured using the **19.17.54 key-usage** command.
Vpn-instance	VPN to which the PKI realm is added. It is configured using the **19.17.123 vpn-instance** command.
Source Interface	Source interface used by the device to communicate with the PKI server. It is configured using the **19.17.119 source interface** command.
Enrollment-request Signature Message-digest-method	Digest method used for the enrollment request packet of signed certificate. It is configured using the **19.17.47 enrollment-request signature message-digest-method** command.

19.17.41 display pki rsa built-in-ca public

Function

The **display pki rsa built-in-ca public** command displays RSA key pairs and public keys of the SSL decryption certificates.

Format

display pki rsa built-in-ca [**name** *key-name*] **public**

Parameters

Parameter	Description	Value
name *key-name*	Specifies the name of the RSA key pair that you want to view. If the *key-name* parameter is not specified, information about all RSA key pairs and public keys of SSL encryption certificate is displayed.	The value must be an existing RSA key pair name.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command shows information about the RSA key pairs and public keys of the SSL decryption certificates, including the creation time, key pair name, whether the key can be exported, and public key information.

Example

Display all RSA key pairs of the SSL decryption certificates.

```
<Huawei> display pki rsa built-in-ca public

=====================================================
Time of Key pair created: 11:29:55  2015/10/21
Key Name: rsakey
Key Index: 0
Key Modules: 2048 bit
Key Exportable: Yes
=====================================================
Key code:
30820109
  02820100
    EC4E155D 90CBE9A0 E9CBB6CD 42797C2D 6B4EC67C
    BCC48F5E CB04127B 1D11D113 EA38D620 4F7E1ABE
    D35A23CF E737A04B 6D2850B7 9388353B 5CBE0206
    B731048C CEC2B347 DA123971 169086B1 85AC3BD3
    21F5125B 4207EBF6 6A578ED5 B964C9BC E0C9B8DF
    083F2689 083966CF 3E577C36 41585C30 AD2A8AC0
    54773A1F 81B893D1 A2F846C9 609434F0 DE0F9412
    B9E803DB 4D7EFE4D C1564AEF 033ACE5A 15B7EF8A
    40401769 ACF3BB72 9D39AFFA 2ACC25E1 F020998F
    43B6FF3B 96126EA5 0FA978BD 4E8ECD5C B7CA1D34
    3D783C77 73AF8FC2 277911D0 DBA7A478 30441972
    8F247DF2 D5AB6085 A6661FEA A978100C 9B0D96E5
    482420D0 D7E83F54 FD4D735F 1B4A359B
  0203
    010001
```

Table 19-172 Description of the **display pki rsa built-in-ca public** command output

Item	Description
Time of Key pair created	Time when an RSA key pair is created.
Key Name	Name of an RSA key pair. It can be configured using the **19.17.105 pki rsa built-in-ca** command.
Key Index	Index of an RSA key pair.
Key Modules	Number of bits in an RSA key pair. It can be configured using the **19.17.105 pki rsa built-in-ca** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Key Exportable	Whether an RSA key pair can be exported. It can be configured using the **19.17.105 pki rsa built-in-ca** command.
Key code	Public key in an RSA key pair.

Related Topics

19.17.105 pki rsa built-in-ca

19.17.42 display pki rsa local-key-pair

Function

The **display pki rsa local-key-pair** command displays the public key in the RSA key pair.

Format

display pki rsa local-key-pair { **pem** | **pkcs12** } *filename* [**password** *password*]

display pki rsa local-key-pair [**name** *key-name*] **public** [**temporary**]

Parameters

Parameter	Description	Value
pem	Indicates that the file format is PEM.	-
pkcs12	Indicates that the file format is PKCS12.	-
filename	Specifies the name of the file that contains the RSA key pair.	The file name must already exist.
password *password*	Specifies the decryption password of RSA key pair. The value must be the same as the password set by **19.17.83 pki export rsa-key-pair**.	The value must be the name of an existing decryption password of the RSA key pair.
name *key-name*	Specifies the RSA key pair name.	The RSA key pair name must already exist.
temporary	Displays information about the RSA key pair saved in the temporary zone.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command shows information about the RSA key pair and public key, including key pair creation time, key pair name, whether the key can be exported, and public key information.

If *key-name* is not specified, all RSA key pairs and public keys are displayed. If *key-name* is specified, the specified RSA key pair and public key are displayed.

Example

Display information about all RSA key pairs.

```
<Huawei> display pki rsa local-key-pair public

=====================================================
Time of Key pair created: 17:43:42  2016/4/18
Key Name: abc
Key Index: 0
Key Modules: 2048 bit
Key Exportable: Yes
Key Type: RSA signature key
=====================================================
Key code:
30820109
  02820100
    C23344E1 B2C2D653 EB134011 9266C6CC 7C18C45F
    440AF31F 98B29D4C D436757B F6785BB5 09EFA2A1
    09FDBB24 62F1914D 4F10678F 3BE8E3C0 E6F02FC9
    AFE2ADDE 98E07D2C A5732288 A5280D2B 6A785F59
    A8D19D37 9B80F7EF 1B15FB77 BD9C54D0 01AF270F
    90258F65 1A631282 50002C4F 23EF0482 1F62E356
    AC700041 B31AB3B4 5C7EB4C0 AFF2E5AF 3DDA4F4E
    F5B86502 08BA7AFE 37204C67 7149AE52 1462F25E
    16B777E8 E71BCFBE 0E9E02A7 C5FE6120 304BE6C3
    CEB2575A EA24EBB6 BA420994 C50F3662 D8F24F25
    0D833865 5A127754 2E954F7F 16292DAA AF9D2371
    E669ADFF 4EA9FFF8 CE8488D7 344EBCEB AAA74116
    B30EF506 C64A726E B1013CB4 E8FA6707
  0203
    010001
```

Table 19-173 Description of the **display pki rsa local-key-pair** command output

Item	Description
Time of Key pair created	Time when the RSA key pair is created.
Key Name	Name of a key pair. It is configured using the **19.17.106 pki rsa local-key-pair create** command.
Key Index	Index of the key.
Key Modules	Number of bits of the key.
Key Exportable	Whether the key can be exported.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Key Type	Type of the key.
Key code	Public key in the RSA key pair.

19.17.43 display pki sm2 local-key-pair public (System view)

Function

The **display pki sm2 local-key-pair public** command displays information about the SM2 key pair and public key.

Format

display pki sm2 local-key-pair [**name** *key-name*] **public**

Parameters

Parameter	Description	Value
name *key-name*	Specifies the name of the SM2 key pair that you want to view.	The value must be an existing SM2 key pair name.

Views

System view

Default Level

3: Management level

Usage Guidelines

This command shows information about the SM2 key pairs and public keys, including the creation time, key pair name, whether the key can be exported, and public key information.

If the *key-name* parameter is not specified, information about all SM2 keys and public keys is displayed. If the *key-name* parameter is specified, information about only the specified SM2 key and public key is displayed.

Example

Display information about all SM2 key pairs.

```
<Huawei> display pki sm2 local-key-pair public

=====================================================
Time of Key pair created: 16:59:08  2016/4/15
```

```
Key Name: 123
Key Index: 0
Key Modules: -
Key Exportable: No
=====================================================
Public-Key: (256 bit)
pub:
    04:d8:bc:77:f6:cd:6d:65:5f:c2:08:29:a4:ad:de:
    bf:d6:ee:59:5e:ba:a1:e2:38:6f:d5:e4:ff:4c:a3:
    97:b2:3b:1a:1d:12:02:5a:5d:a2:57:21:6a:8e:e5:
    29:3d:5f:84:b6:5a:5f:b9:5f:f4:76:f8:26:34:fb:
    ea:f0:66:b9:eb
Field Type: prime-field
Prime:
    00:ff:ff:ff:fe:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:
    ff:ff:ff
A:
    00:ff:ff:ff:fe:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:ff:ff:ff:ff:00:00:00:00:ff:ff:ff:ff:ff:
    ff:ff:fc
B:
    28:e9:fa:9e:9d:9f:5e:34:4d:5a:9e:4b:cf:65:09:
    a7:f3:97:89:f5:15:ab:8f:92:dd:bc:bd:41:4d:94:
    0e:93
Generator (uncompressed):
    04:32:c4:ae:2c:1f:19:81:19:5f:99:04:46:6a:39:
    c9:94:8f:e3:0b:bf:f2:66:0b:e1:71:5a:45:89:33:
    4c:74:c7:bc:37:36:a2:f4:f6:77:9c:59:bd:ce:e3:
    6b:69:21:53:d0:a9:87:7c:c6:2a:47:40:02:df:32:
    e5:21:39:f0:a0
Order:
    00:ff:ff:ff:fe:ff:ff:ff:ff:ff:ff:ff:ff:ff:ff:
    ff:ff:72:03:df:6b:21:c6:05:2b:53:bb:f4:09:39:
    d5:41:23
Cofactor:  1 (0x1)
```

Table 19-174 Description of the **display pki sm2 local-key-pair public** command output

Item	Description
Time of Key pair created	SM2 Key pair creation time.
Key Name	Name of the SM2 key pair.
Key Index	SM2 Key index.
Key Modules	SM2 Key modules.
Key Exportable	Whether the SM2 key can be exported.
Public-Key	SM2 Public key information.
pub	Public key in the SM2 key pair.
A	Prime number a in the SM2 elliptic curve cryptography (ECC).
B	Prime number b in the SM2 ECC.
Generator (uncompressed)	Generator of the SM2 ECC and whether the generator is compressed if it is converted into a large value.

Item	Description
Order	Order of the SM2 ECC generator.
Cofactor	Cofactor of the SM2 ECC, which is the Number of ECC points/Order of generator.

19.17.44 email

Function

The **email** command configures an email address for a PKI entity.

The **undo email** command cancels the configuration.

By default, no email address for an entity is configured.

Format

email *email-address*

undo email

Parameters

Parameter	Description	Value
email-address	Specifies the email address of an entity.	The value is a string of 1 to 128 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an email address for the PKI entity, which is used as an alias of the entity.

After the email address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this email address. The CA server

 Copyright © Huawei Technologies Co., Ltd.

verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the email address of the PKI entity.

Example

Set the email address to test@example.com for an entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] email test@example.com
```

Related Topics

19.17.35 display pki entity

19.17.45 enrollment self-signed

Function

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm.

The **undo enrollment self-signed** command restores the default certificate obtaining method.

By default, self-signed certificate obtaining in the PKI realm is not configured.

Format

enrollment self-signed

undo enrollment self-signed

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **enrollment self-signed** command configures self-signed certificate obtaining in the PKI realm. The device can use the self-signed certificate obtained from the PKI realm to support default HTTPS functions.

Prerequisites

The RSA key pair has been configured by using the **19.17.116 rsa local-key-pair** command.

Precautions

The device generates a self-signed certificate only when the PKI domain is applied to the service.

The device does not support lifecycle management for self-signed certificates. For example, self-signed certificates cannot be registered, updated, or revoked on the device. To ensure security of the device and certificates, it is recommended the user's certificate be used.

To configure self-signed certificate obtaining, delete the certificate in the PKI realm.

After the **enrollment self-signed** command is run, the device will not generate certificate expiration logs when its self-signed certificate expires.

Example

Configure self-signed certificate obtaining in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] enrollment self-signed
```

Related Topics

19.17.103 pki realm (system view)

19.17.40 display pki realm

19.17.46 enrollment-request specific

Function

The **enrollment-request specific** command configures the device to use a certificate request packet of the specific format to apply for a local certificate from the CA.

The **undo enrollment-request specific** command restores the default setting.

By default, the device uses a certificate request packet of the standard format to apply for a local certificate from the CA.

Format

enrollment-request specific

undo enrollment-request specific

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You need to configure this command to implement communication between the PKI entity and the CA server when the CA server has the following requirements:

- The unstructured address and unstructured name of the certificate request packet do not carry the SET identifier.
- The device uses the private key of the applied certificate to sign the certificate request packet.

Precautions

To implement communication between the device and CA server, the certificate key length cannot be longer than 2048 bits. If the RSA key length of certificates is longer than 2048 bits, the device will use the private key of a self-signed certificate to sign the certificate request packet regardless of whether the **enrollment-request specific** command is configured.

Example

Configure the device to use a certificate request packet of the specific format to apply for a local certificate from the CA.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] enrollment-request specific
```

19.17.47 enrollment-request signature message-digest-method

Function

The **enrollment-request signature message-digest-method** command sets the message digest method of signature for the enrollment request.

The **undo enrollment-request signature message-digest-method** command restores the default message digest method.

By default, the message digest method of signature for the enrollment request is **sha-256**.

Format

enrollment-request signature message-digest-method { **md5** | **sha1** | **sha-256** | **sha-384** | **sha-512** }

undo enrollment-request signature message-digest-method

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
md5	Sets the digest method used for the enrollment request packet of signed certificate to MD5.	-
sha1	Sets the digest method used for the enrollment request packet of signed certificate to SHA1.	-
sha-256	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-256.	-
sha-384	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-384.	-
sha-512	Sets the digest method used for the enrollment request packet of signed certificate to SHA2-512.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

In SCEP local certificate application mode, after a CA server receives a certificate enrollment request from a PKI entity, the CA server requests a signature for authentication, and generates a local certificate only after the authentication is successful.

Other algorithms are more secure than MD5 and SHA1 algorithms and so are recommended.

Example

Set the message-digest method of signature for enrollment request to be **sha-384**.

```
<Huawei> system-view
[Huawei] pki realm e
[Huawei-pki-realm-e] enrollment-request signature message-digest-method sha-384
```

19.17.48 enrollment-url

Function

The **enrollment-url** command configures the URL of the CA server.

The **undo enrollment-url** command deletes the URL of the CA server.

By default, the URL of the CA server is not configured.

 Copyright © Huawei Technologies Co., Ltd.

Format

enrollment-url [**esc**] *url* [**interval** *minutes*] [**times** *count*] [**ra**]

undo enrollment-url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url	Specifies the URL of the CA server. The URL is in the format of *http://server_location/ca_script_location*. *server_location* can use only the IP address format and domain name resolution. *ca_script_location* is the path where CA's application script is located. For example, **http://10.1.1.1:8080/certsrv/mscep/mscep.dll**.	The value is a string that starts with **http://** and consists of 1 to 128 case-sensitive characters without spaces.
interval *minutes*	Specifies the interval between two certificate enrollment status queries.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 1.
times *count*	Specifies the maximum number of certificate enrollment status queries.	The value is an integer that ranges from 1 to 100. The default value is 5.
ra	Configures an RA to authenticate a PKI entity's identity information during local certificate application. By default, a CA authenticates a PKI entity's identity information during local certificate application.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

The URL refers to the address provided by a CA server for certificate application. For example, a CA server running Windows Server 2008 uses a URL address in the format http://host:port/certsrv/mscep/mscep.dll, in which *host* indicates the IP address of the CA server and *port* indicates the port number.

The keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Create a PKI realm **test** and configure the URL of the CA server.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] enrollment-url http://10.1.1.1:8080/certsrv/mscep/mscep.dll ra
```

19.17.49 entity

Function

The **entity** command specifies a PKI entity that applies for a certificate.

The **undo entity** command cancels a PKI entity.

By default, no PKI entity is specified.

Format

entity *entity-name*

undo entity

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value must be an existing PKI entity name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a PKI entity requests the local certificate in the PKI realm, the device encapsulates the configuration of the specified PKI entity into the certificate request.

Prerequisites

1. The specified PKI entity has been configured by using the **19.17.79 pki entity** command.
2. The common name of the PKI entity has been configured using the **19.17.17 common-name** command.

Precautions

A PKI realm can be bound to only one PKI entity.

Example

Bind the PKI entity **a** to the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki entity a
[Huawei-pki-entity-a] common-name test
[Huawei-pki-entity-a] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] entity a
```

Related Topics

19.17.79 pki entity

19.17.17 common-name

19.17.40 display pki realm

19.17.50 extension-request enterprise

Function

The **extension-request enterprise** command configures the extended attribute in the certificate enrollment request to carry the object ID defined by Verisign.

The **undo extension-request enterprise** command restores the default extended attribute in the certificate enrollment request.

By default, the extended attribute in the certificate enrollment request carries the object ID defined by PKCS#9.

 Copyright © Huawei Technologies Co., Ltd.

Format

extension-request enterprise verisign

undo extension-request enterprise verisign

Parameters

Parameter	Description	Value
verisign	Inserts the object ID defined by Verisign into the extended attribute of the certificate enrollment request.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

When a PKI entity applies for a local certificate from the CA, the certificate applicant requires that the extended attribute in the local certificate carry the object ID defined by Verisign. You can run this command.

Example

Configure the extended request attribute in the certificate enrollment request to carry the object ID defined by Verisign.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] extension-request enterprise verisign
```

19.17.51 fingerprint

Function

The **fingerprint** command configures the CA certificate fingerprint used in CA certificate authentication.

The **undo fingerprint** command deletes the CA certificate fingerprint used in CA certificate authentication.

By default, no CA certificate fingerprint is configured for CA certificate authentication.

Format

fingerprint { **md5** | **sha1** | **sha256** } *fingerprint*

undo fingerprint

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
md5	Sets the digital fingerprint algorithm to MD5.	-
sha1	Sets the digital fingerprint algorithm to SHA1.	-
sha256	Sets the digital fingerprint algorithm to SHA256.	-
fingerprint	Specifies the digital fingerprint value. This value needs to be obtained from the CA server offline. For example, from a CA server running Windows Server 2008, you can obtain the digital fingerprint at http://*host*:*port*/certsrv/mscep_admin/, in which *host* indicates the server's IP address and *port* indicates the port number.	The digital fingerprint value is a hexadecimal string of case-insensitive characters. ● An MD5 fingerprint consists of 32 characters (16 bytes). ● An SHA1 fingerprint consists of 40 characters (20 bytes). ● An SHA256 fingerprint consists of 64 characters (32 bytes).

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When obtaining a CA certificate, the device uses an algorithm to calculate the CA certificate fingerprint and compares the CA certificate fingerprint with the configured fingerprint. If the two values are the same, the device receives the CA certificate. When verifying a certificate, the device uses the public key of the CA certificate to authenticate the digital signature. If the digital signature can be decrypted, the certificate is verified.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

You can configure an algorithm to calculate the CA certificate fingerprint. If you run the **fingerprint** command multiple times in the same PKI realm view, only the latest configuration takes effect.

The MD5 and SHA1 algorithms have a low security level. SHA256 is recommended.

Example

Configure the CA certificate fingerprint used in CA certificate authentication.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] fingerprint sha256
e71add0744360e91186b828412d279e06dcc15a4ab4bb3d13842820396b526a0
```

19.17.52 fqdn

Function

The **fqdn** command configures a fully qualified domain name (FQDN) for an entity.

The **undo fqdn** command cancels the configuration.

By default, no FQDN is configured for a PKI entity.

Format

fqdn [**unstructed-name**] *fqdn-name*

undo fqdn [**unstructed-name**]

Parameters

Parameter	Description	Value
unstructed-name	Indicates that FQDN is used as the PKCS#9 unstructed name for the PKI entity. If this parameter is not specified, FQDN is used as the alias of the PKI entity.	-
fqdn-name	Specifies the FQDN of an entity.	The value is a string of 1 to 255 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), minus signs (-), periods (.), slashes (/), colons (:), at signs (@), underscores (_), and spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an FQDN for the PKI entity, which is used as an alias of the entity.

An FQDN is the unique identifier of a PKI entity. It consists of a host name and a domain name, and can be translated into an IP address. A sample of an FQDN is www.example.com.

After the FQDN is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this FQDN. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the FQDN of the PKI entity.

If the **enrollment-request specific** command has been executed to configure the PKI entity to apply for a local certificate from the CA using the specified enrollment request format, the **unstructed-name** parameter can be specified to configure FQDN as the PKCS#9 unstructed name for the PKI entity.

Example

Set the FQDN to **example.com** for an entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] fqdn example.com
```

Related Topics

19.17.35 display pki entity

19.17.53 ip-address

Function

The **ip-address** configures an IP address for an entity.

The **undo ip-address** deletes the configuration.

By default, a PKI entity does not have an IP address.

Format

ip-address [**unstructed-address**] { *ipv4-address* | *interface-type interface-number* }

undo ip-address [**unstructed-address**]

Parameters

Parameter	Description	Value
unstructed-address	Indicates that an IP address is used as the PKCS#9 unstructed address for the PKI entity. If this parameter is not specified, an IP address is used as the alias of the PKI entity.	-
ipv4-address	Specifies the IPv4 address of a PKI entity.	The value is in dotted decimal notation.
interface-type interface-number	Specifies an interface IP address of a PKI entity. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To facilitate applicant identification, configure an IP address for the PKI entity, which is used as an alias of the PKI entity.

After an IP address is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this IP address. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device IP address.

If the **enrollment-request specific** command has been executed to configure the PKI entity to apply for a local certificate from the CA using the specified enrollment request format, the **unstructed-name** parameter can be specified to configure IP address as the PKCS#9 unstructed address for the PKI entity.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the IP address for a PKI entity to 10.1.1.1.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] ip-address 10.1.1.1
```

Related Topics

19.17.35 display pki entity

19.17.54 key-usage

Function

The **key-usage** command configures the purpose description for a certificate public key.

The **undo key-usage** command deletes the purpose description of a certificate public key.

By default, a certificate public key does not have a purpose description.

Format

key-usage { **ike** | **ssl-client** | **ssl-server** } *

undo key-usage { **ike** | **ssl-client** | **ssl-server** } *

Parameters

Parameter	Description	Value
ike	Specifies the usage of a key as ike. That is, the key is used to set up an IPSec tunnel.	-
ssl-client	Specifies the usage of a key as ssl-client. That is, the key is used by the SSL client to set up an SSL session.	-
ssl-server	Specifies the usage of a key as ssl-server. That is, the key is used by the SSL server to set up an SSL session.	-

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To improve certificate security, you can add the usage information of a key to the certificate request packet sent from the device to the CA server.

After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the usage information of the key.

For example, when setting up an SSL session, the SSL client adds a digital signature and encrypts the key by using the certificate. After you specify the usage of a key as ssl-client by using the **key-usage ssl-client** command, the certificate generated by the CA server carries the usage information, including a digital signature and encrypted key. If you use this key to encrypt data, the key will be invalid.

Example

Specify the usage of a key as ssl-client.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] key-usage ssl-client
```

19.17.55 ldap-server authentication

Function

The **ldap-server authentication** command configures an LDAP authentication server.

The **undo ldap-server authentication** command deletes an LDAP authentication server.

By default, no LDAP authentication server is configured.

Format

ldap-server authentication *ip-address* [*port-number*]

undo ldap-server authentication

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an LDAP authentication server.	The value is in dotted decimal notation.
port-number	Specifies the port number of an LDAP authentication server.	The value is an integer that ranges from 1 to 65535. The default value is 389. The port number must be the same as that on the LDAP server.

 Copyright © Huawei Technologies Co., Ltd.

Views

LDAP server template view

Default Level

3: Management level

Usage Guidelines

During LDAP authentication, LDAP is used in interaction between the device and LDAP server. The LDAP data transmission is not encrypted. For security, you can use LDAP based on SSL for encrypted transmission. LDAP server certificates need to be imported into the device to authenticate the LDAP server.

Example

Configure the primary LDAP authentication server.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1] ldap-server authentication 10.1.1.1 389
```

19.17.56 ldap-server authentication manager

Function

The **ldap-server authentication manager** command configures the administrator DN and password of an LDAP authentication server.

The **undo ldap-server authentication manager** command deletes the values of the administrator DN and password of an LDAP authentication server.

By default, no administrator DN and password of an LDAP authentication server is configured.

Format

ldap-server authentication manager *manager-dn* [*password* [*repassword*]]

undo ldap-server authentication manager

Parameters

Parameter	Description	Value
manager-dn	Specifies the administrator DN of an LDAP authentication server.	If the *manager-dn* value does not contain any space, its length ranges from 1 to 256.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password	Specifies the administrator password of an LDAP authentication server.	The value is a string that contains 1 to 63 characters in simple text or 48 to 108 characters in cipher text. The simple characters are saved in cipher text. If the string has 1 to 16 characters, the cipher text is 48-byte long; if the string has 17 to 32 characters, the cipher text is 68-byte long; if the string has 33 to 48 characters, the cipher text is 88-byte long; if the string has 49 to 63 characters, the cipher text is 108-byte long. **NOTICE** To enhance security, the password of an LDAP administrator is recommended to meet the minimum strength requirements, that is, it needs to contain at least three types of the following characters: upper-case letters, lower-case letters, digits (0 to 9), and special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%), and contains at least six characters.
repassword	Re-enters the password of an LDAP administrator.	The value must be the same as that of *password*.

Views

LDAP server template view

Default Level

3: Management level

Usage Guidelines

None

Example

Set the administrator DN and password of an LDAP authentication server to **dn** and **Admin@123**, respectively.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1] ldap-server authentication manager dn Admin@123
```

19.17.57 ldap-server authentication manager-password

Function

The **ldap-server authentication manager-password** command modifies the administrator password of an LDAP authentication server.

Format

ldap-server authentication manager-password *password* [*repassword*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
password	Specifies the administrator password of an LDAP authentication server.	The value is a string that contains 1 to 63 characters in simple text or 48 to 108 characters in cipher text. The simple characters are saved in cipher text. If the string has 1 to 16 characters, the cipher text is 48-byte long; if the string has 17 to 32 characters, the cipher text is 68-byte long; if the string has 33 to 48 characters, the cipher text is 88-byte long; if the string has 49 to 63 characters, the cipher text is 108-byte long. **NOTICE** To enhance security, the password of an LDAP administrator is recommended to meet the minimum strength requirements, that is, it needs to contain at least three types of the following characters: upper-case letters, lower-case letters, digits (0 to 9), and special characters such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%), and contains at least six characters.
repassword	Re-enters the password of an LDAP administrator.	The value must be the same as that of *password*.

Views

LDAP server template view

Default Level

3: Management level

Usage Guidelines

None

Example

Set the administrator password of an LDAP authentication server to **Admin@123** respectively.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1] ldap-server authentication manager-password Admin@123
```

19.17.58 ldap-server template

Function

The **ldap-server template** command creates an LDAP server template and displays the LDAP server template view.

The **undo ldap-server template** command deletes an LDAP server template.

By default, no LDAP server template is configured.

Format

ldap-server template *template-name*

undo ldap-server template *template-name*

Parameters

Parameter	Description	Value
template-name	Specifies the name of an LDAP server template.	The value is a case-sensitive string of 1 to 32 characters. The name contains only uppercase letters, lowercase letters, digits, dots (.), underscores (_), hyphens (-) and their combinations.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If an LDAP server template is referenced by an authentication domain, you can modify the LDAP server template, but cannot delete it.

If you attempt to delete an LDAP template in use, the system prompts the deletion failure.

Example

Create an LDAP server template named **temp1** and access the corresponding view.

```
<Huawei> system-view
[Huawei] ldap-server template temp1
[Huawei-ldap-temp1]
```

19.17.59 ldap-server-template

Function

The **ldap-server-template** command specifies a LDAP server template for a PKI realm.

The **undo ldap-server-template** command deletes the LDAP server template from the PKI realm.

By default, no LDAP server template is configured in the PKI realm.

Format

ldap-server-template *template-name*

undo ldap-server-template

Parameters

Parameter	Description	Value
template-name	Specifies the name of an LDAP server template.	The LDAP server template name must already exist.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is required when LDAP is selected for certificate download or automatic CRL update.

Prerequisites

1. An LDAP server template has been created using the **19.17.58 ldap-server template** command.
2. Automatic CRL update mode is set to LDAP using the **19.17.22 crl ldap** command.

Example

Specify an LDAP server template for a PKI realm.

```
<Huawei> system-view
[Huawei] ldap-server template user1
[Huawei-ldap-user1] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] crl ldap
[Huawei-pki-realm-abc] ldap-server-template user1
```

Related Topics

19.17.58 ldap-server template

19.17.22 crl ldap

19.17.60 ldap-server (PKI realm view)

Function

The **ldap-server** command configures an LDAP server.

The **undo ldap-server** command cancels the configuration.

By default, no LDAP server is configured.

Format

ldap-server { **authentication** *ldap-dn ldap-password* | **ip** *ip-address* [**port** *port* | **version** *version*] * }

undo ldap-server [**authentication**]

Parameters

Parameter	Description	Value
authentication *ldap-dn ldap-password*	Indicates the user name and password of an LDAP server.	• *ldap-dn*: The value is a string of 1 to 32 case-sensitive characters. • *ldap-password*: The value is a string of 1 to 32 case-sensitive characters without spaces or question marks. If the character string is quoted by double quotation marks, it can contain spaces and question marks. The system saves this string to the configuration file in ciphertext. A string of 1-16 characters is converted into a 48-byte cipher-text string; a string of 17-32 characters is converted into a 68-byte cipher-text string.
ip *ip-address*	Specifies the IP address of an LDAP server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of an LDAP server.	The value is an integer that ranges from 1 to 65535. The default value is 389.
version *version*	Specifies the version number of LDAP.	The value is an integer that ranges from 2 to 3. The default value is 3.

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a PKI entity uses LDAP to update CRL for certificate verification, the PKI entity obtains CRL from the LDAP server. In this situation, you need to specify an LDAP server.

Prerequisites

The automatic CRL update mode is set to LDAP using the **crl ldap** command.

Example

Configure the IP address to 10.1.1.1, port number to 3389, and LDAP version number to 2 for an LDAP server.

```
<Huawei> system-view
[Huawei] pki realm d1
[Huawei-pki-realm-d1] crl ldap
[Huawei-pki-realm-d1] ldap-server ip 10.1.1.1 port 3389 version 2
```

19.17.61 locality

Function

The **locality** command configures a locality name for a PKI entity.

The **undo locality** command cancels the configuration.

By default, a PKI entity does not have a locality name.

Format

locality *locality-name*

undo locality

Parameters

Parameter	Description	Value
locality-name	Specifies the locality name of an entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a locality name for the PKI entity, which is used as an alias of the entity.

After the locality name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this locality name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the locality name of the PKI entity.

Example

Set the locality name to **Beijing** for a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] locality Beijing
```

Related Topics

19.17.35 display pki entity

19.17.62 ocsp nonce enable

Function

The **ocsp nonce enable** command adds a nonce extension to the OCSP request sent by a PKI entity.

The **undo ocsp nonce enable** command cancels the configuration.

By default, the OCSP request sent by a PKI entity contains a nonce extension.

Format

ocsp nonce enable

undo ocsp nonce enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To improve security and reliability of communication between PKI entity and OCSP server, this command adds a nonce extension (a random value) to the OSCP request sent by the PKI entity. If the nonce extension values on the PKI entity and OCSP server are different, communication fails.

Example

Add a nonce extension to the OCSP request sent by a PKI entity

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ocsp nonce enable
```

19.17.63 ocsp signature enable

Function

The **ocsp signature enable** command enables the function of signing OCSP request packets.

The **undo ocsp signature enable** command disables the function of signing OCSP request packets.

By default, the function of signing OCSP request packets is disabled.

Format

ocsp signature enable

undo ocsp signature enable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

When the certificate check mode is set to OCSP, the device sends OCSP request packets to the OCSP server. To improve access security, run this command to enable signing on OCSP request packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] ocsp signature enable
```

19.17.64 ocsp url

Function

The **ocsp url** command configures the Uniform Resource Locator (URL) address for the Online Certificate Status Protocol (OCSP) server.

The **undo ocsp url** command deletes the URL address of the OCSP server.

By default, an OCSP server does not have a URL address.

Format

ocsp url [**esc**] *url-address*

undo ocsp url

Parameters

Parameter	Description	Value
esc	Indicates that the URL address is in ASCII mode.	-
url-address	Indicates the OCSP server's URL address.	The value is a string starting with **http://** and consisting of 1 to 128 case-sensitive characters without spaces.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP does not contain the AIA option, run this command to configure the OCSP server's URL. If the certificate contains the AIA option, run the **ocsp-url from-ca** command to configure the PKI entity to obtain OSCP server's URL from the AIA option.

Keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?).

 Copyright © Huawei Technologies Co., Ltd.

Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\) to \x3f and enter **http://www.***.com\x3fpage1\\x3f.**

Example

Set the OCSP server's URL address to http://10.1.1.1.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ocsp url http://10.1.1.1
```

19.17.65 ocsp-url from-ca

Function

The **ocsp-url from-ca** command configures the PKI entity to obtain the OCSP server's URL from the Authority Info Access (AIA) option in the CA certificate.

The **undo ocsp-url from-ca** command disables the PKI entity from obtaining the OCSP server's URL from the Authority Info Access (AIA) option in the CA certificate.

By default, a PKI entity does not obtain OCSP server's URL from the CA certificate's AIA option.

Format

ocsp-url from-ca

undo ocsp-url from-ca

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

If a certificate to be checked through OCSP contains the AIA option, run this command to configure the PKI entity to obtain OSCP server's URL from the AIA option. If the certificate does not contain the AIA option, run the **ocsp url** command to configure the OCSP server's URL.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the PKI entity to obtain OCSP server's URL from the CA certificate's AIA option.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] ocsp-url from-ca
```

19.17.66 organization-unit

Function

The **organization-unit** command configures the department name for a PKI entity.

The **undo organization-unit** command restores the default setting.

By default, no department name is configured for a PKI entity.

Format

organization-unit *organization-unit-name*

undo organization-unit

Parameters

Parameter	Description	Value
organization-unit-name	Specifies the department name for a PKI entity.	The department name is a string of 1 to 31 case-sensitive characters. Names of departments are separated by commas (,). The total length of all department names ranges from 1 to 191. The characters can be letters, integers, apostrophe ('), equal sign (=), brackets (), plus sign (+), comma (,), minus sign (-), dot (.), slash (/), colon (:), and spaces.

Views

PKI entity view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a department name for the PKI entity, which is used as an alias of the entity.

After the department name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this department name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the department name of the PKI entity.

Example

Configure the department name of a PKI entity to **Group1, Sale**.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] organization-unit Group1,Sale
```

Related Topics

19.17.35 display pki entity

19.17.67 organization

Function

The **organization** command configures a PKI entity's organization name.

The **undo organization** command deletes a PKI entity's organization name.

By default, a PKI entity does not have an organization name.

Format

organization *organization-name*

undo organization

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
organization-name	Specifies the organization name of the PKI entity.	It is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure an organization name for the PKI entity, which is used as an alias of the entity.

After the organization name is configured for a PKI entity, the certificate request packet sent by the device to the CA server carries this organization name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the organization name of the PKI entity.

Example

Set the organization name of the PKI entity to **org1**.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] organization org1
```

Related Topics

19.17.35 display pki entity

19.17.68 password (PKI realm view)

Function

The **password** command sets the challenge password used for certificate application through SCEP, which is also used to revoke a certificate.

The **undo password** command deletes the challenge password used for certificate application through SCEP.

 Copyright © Huawei Technologies Co., Ltd.

By default, no challenge password is configured.

Format

password cipher *password*

undo password

Parameters

Parameter	Description	Value
cipher *password*	Specifies the challenge password used for certificate application through SCEP. The password is displayed in ciphertext.	The value is a string of case-sensitive characters. It cannot contain question marks (?). The *password* is in plaintext that contains 1 to 64 characters or in ciphertext that contains 48 to 108 characters. **NOTE** To improve communication security, it is recommended that the certificate revocation password contains at least three types of lowercase letters, uppercase letters, numerals, and special characters, and contains at least six characters.

Views

PKI realm view

Default Level

3: Management level

Usage Guidelines

When a PKI entity uses SCEP to apply for a certificate from CA, CA needs to verify the challenge password of the entity. CA accepts the certificate application request only when the challenge password is correct. You need to run this command to set a challenge password for the PKI entity.

The challenge password is also used to revoke a certificate. It avoids misoperations in certificate revocation.

Example

Set the challenge password used to apply for certificate through SCEP.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] password cipher 6AE73F21E6D3571D
```

19.17.69 pki built-in-ca match-rsa-key

Function

The **pki built-in-ca match-rsa-key** command configures a device to search for the RSA key pair associated with a specific SSL decryption certificate.

Format

pki built-in-ca match-rsa-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
file-name	Specifies the name of an SSL decryption certificate.	It must be the name of an existing SSL decryption certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to view the RSA key pair associated with an SSL decryption certificate. Then the system searches all local RSA key pairs for the desired one, and displays the key pair name.

Prerequisites

An SSL decryption certificate has been generated using the **19.17.86 pki generate built-in-ca certificate** command or an SSL decryption certificate has been imported.

Example

Configure a device to search for the RSA key pair that matches certificate file **rsakey_builtinca.cer**.

```
<Huawei> system-view
[Huawei] pki generate built-in-ca certificate rsa-key-pair rsakey entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : rsakey_builtinca.cer
 Info: Generate built in CA certificate successfully.
[Huawei] pki built-in-ca match-rsa-key certificate-filename rsakey_builtinca.cer
 Info: The file rsakey_builtinca.cer contains certificates 1.
 Info: Certificate 1 from file rsakey_builtinca.cer matches RSA key rsakey.
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.17.86 pki generate built-in-ca certificate

19.17.70 pki cmp certificate-request session

Function

The **pki cmp certificate-request session** command sends a certificate request (CR) to the CMPv2 server based on the CMP session information.

Format

pki cmp certificate-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of the CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a device has a certificate issued by CA, the device can perform a CR to apply for a certificate for another device.

After this command is executed, the system checks whether the configurations in the CMP session is sufficient for certificate application. If no, the system displays an error message. If yes, the system performs the CR according to the configuration. The obtained certificate is saved in a file on the CF card or Hda1, but not imported to the memory.

NOTE

The device does not support the message authentication code mode. If the CMP session mode is set to message authentication code, the system displays an error message.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

Example

Send a CR to the CMPv2 server.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] pki cmp certificate-request session test
 Info: Initializing configuration.
 Info: Creatting certification request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending certification request packet.
 Info: Waitting for certification response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

Related Topics

19.17.73 pki cmp session

19.17.71 pki cmp initial-request session

Function

The **pki cmp initial-request session** command performs an initial request (IR) to the CMPv2 server based on the CMP session information.

Format

pki cmp initial-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the command is executed, the system checks whether the configurations in the CMP session are sufficient for certificate application. If no, the system displays an error message. If yes, the system performs an IR according to the configuration.

 Copyright © Huawei Technologies Co., Ltd.

The obtained certificate is saved in a file on the CF card or Hda1, but not imported to the memory. If the server issues the CA certificate during the response period, the CA certificate is also saved in a file.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

Example

Send an IR to the CMPv2 server.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] pki cmp initial-request session test
 Info: Initializing configuration.
 Info: Creatting initial request packet.
 Info: Connectting to CMPv2 server.
 Info: Sending initial request packet.
 Info: Waitting for initial response packet.
 Info: Creatting confirm packet.
 Info: Connectting to CMPv2 server.
 Info: Sending confirm packet.
 Info: Waitting for confirm packet from server.
 Info: CMPv2 operation finish.
```

Related Topics

19.17.73 pki cmp session

19.17.72 pki cmp keyupdate-request session

Function

The **pki cmp keyupdate-request session** command performs a key update request (KUR) to the CMPv2 server based on the CMP session information.

Format

pki cmp keyupdate-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A device performs a KUR when it has a certificate issued by the CA and requires to update the certificate.

After the command is executed, the system checks whether the configurations in the CMP session are sufficient for certificate update application. If no, the system displays an error message. If yes, the system performs a KUR according to the configuration. The updated certificate is saved in a file on the device storage, but not imported to the memory.

NOTE

The device does not support the message authentication code mode. If the CMP session mode is set to message authentication code, the system displays an error message.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

Example

Send a KUR to the CMPv2 server.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] pki cmp keyupdate-request session test
 Info: Initializing configuration.
 Info: Creatting key update request packet.
 Info: Connectting to CMPv2 server.
 Error: CMPv2 server connect failed.
 Info: CMPv2 operation finish.
```

Related Topics

19.17.73 pki cmp session

19.17.73 pki cmp session

Function

The **pki cmp session** command creates a CMP session and displays the CMP session view, or displays the view of an existing CMP session.

The **undo pki cmp session** command deletes a CMP session.

By default, no CMP session exists.

Format

pki cmp session *session-name*

undo pki cmp session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of a CMP session.	It is a string of 1 to 63 case-insensitive characters without spaces or question marks.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Before choosing CMPv2 for certificate application, run the **pki cmp session** command to create a CMP session. CMPv2 configurations are performed in the CMP session view.

Example

Create the CMP session **test** and display the CMP session view.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test]
```

19.17.74 pki create-certificate

Function

The **pki create-certificate** command creates a self-signed certificate or local certificate.

Format

pki create-certificate [**self-signed**] **filename** *file-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
self-signed	Creates a self-signed certificate. If this parameter is not specified, a local certificate is created. ● A self-signed certificate is issued by a PKI device itself. In a self-signed certificate, the certificate issuer and subject are the same. ● A local certificate is issued by a PKI entity itself based on the certificate issued by CA. The issuer in a local certificate is CA.	-
filename *filename*	Specifies the name of a certificate file.	The value is a string of 1 to 64 case-insensitive characters without spaces or question marks.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a self-signed certificate or local certificate is generated by the device, the certificate file is saved in the storage device as a PEM file. You can export the certificate for other devices to use. This simplifies certificate issue process.

When you run the **pki create-certificate** command, the system asks you to enter certificate information, for example, PKI entity parameters, certificate file name, the validity time of certificate and RSA key length.

Precautions

The device does not provide lifecycle management for self-signed certificates. For example, self-signed certificates cannot be updated or revoked on the device. To ensure security of the device and certificates, a local certificate is recommended.

Example

Create a self-signed certificate **huawei**.

```
<Huawei> system-view
[Huawei] pki create-certificate self-signed filename huawei
```

19.17.75 pki delete-certificate

Function

The **pki delete-certificate** command deletes a certificate from the memory.

Format

pki delete-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Deletes a CA certificate.	-
local	Deletes a local certificate.	-
ocsp	Deletes an Online Certificate Status Protocol (OCSP) server's certificate.	-
realm *realm-name*	Specifies the name of the PKI realm to which a certificate belongs.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the certificate expires or you want to apply for a new certificate, run this command to delete the CA, local, or OCSP server certificate from the memory.

Prerequisites

Example

Delete the local certificate from the memory.

```
<Huawei> system-view
[Huawei] pki delete-certificate local realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.76 pki delete-certificate built-in-ca

Function

The **pki delete-certificate built-in-ca** command deletes an SSL decryption certificate from the memory.

Format

pki delete-certificate built-in-ca filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the name of the SSL decryption certificate file.	The SSL decryption certificate file name must already exist in the memory.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an SSL decryption certificate expires or you want to apply for a new certificate, run the **pki delete-certificate built-in-ca** command to delete the current SSL decryption certificate from the memory. This command will not delete the certificate files in the device storage.

Prerequisites

The SSL decryption certificate has been imported to the memory using the **19.17.91 pki import-certificate built-in-ca** command.

Example

Delete an SSL decryption certificate from the memory.

```
<Huawei> system-view [Huawei] pki import-certificate built-in-ca filename test_builtinca.cer  Info: Succeeded in importing the built-in CA certificate.  [Huawei] pki delete-certificate built-in-ca filename test_builtinca.cer
```

Related Topics

19.17.91 pki import-certificate built-in-ca

19.17.77 pki delete-crl

Function

The **pki delete-crl** command deletes a CRL from the memory.

Format

pki delete-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of the PKI realm that the certificate belongs to.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a CRL expires, run this command to delete a CRL file from the memory. This command will not delete the CRL files in storage card.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Example

Delete the CRL of PKI realm **abc** from the memory.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki delete-crl realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.34 display pki crl

19.17.78 pki enroll-certificate

Function

The **pki enroll-certificate** command configures manual certificate enrollment.

Format

pki enroll-certificate realm *realm-name* [**pkcs10** [**filename** *filename*]] [**password** *password*]

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the name of a PKI realm.	The PKI realm name must already exist.
pkcs10	Uses the PKCS#10 format to display the local certificate request information. It can be used to request certificates in offline mode.	-
filename *filename*	Saves the certificate request information in a specified file. The certificate request information is saved in the file in PKCS#10 format and is sent to the CA in outband mode.	The value is a string of 1 to 64.
password *password*	Indicates a challenge password, which is used to request certificates in online mode. When the CA server processes the certificate request using the challenge password, you must set a challenge password on the entity, and the challenge password must be the same as the password configured on the CA server.	The value is a string of case-sensitive characters without question marks (?) or spaces. It can be a plain-text string of 1 to 64 characters or a cipher-text string of 48 to 108 characters. **NOTE** To improve certificate security, it is recommended that a password consist of at least two of the following: lowercase letters, uppercase letters, numerals and special characters. In addition, the password must contain at least 6 characters.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Manual certificate application is online or offline.

- Online mode (in-band mode)

  In online requests, entities request certificates from CAs using the SCEP protocol. Then the entities store the obtained certificates on the sd1 of devices.
- Offline mode (out-of-band mode)

  The device generates a certificate request file. The administrator sends the file to the CA server using methods such as disks and emails.

Prerequisites

A PKI realm has been created using the **pki realm (system view)** command.

Precautions

- If **pkcs10** is specified, an entity applies to a CA for a certificate in offline mode. The entity saves the certificate request information in a file in PKCS#10 format and sends the file to the CA in outband mode.
- If **pkcs10** is not specified, an entity applies to a CA for a certificate in online mode.
- In online mode, a PKI entity obtains a CA certificate and imports it to memory, and then obtains a local certificate and imports it to memory.
- After the **enrollment self-signed** command is used in the PKI realm, it is not allowed to use the **pki enroll-certificate** command to configure manual certificate enrollment.

Example

Enroll a certificate for the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki enroll-certificate realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.79 pki entity

Function

The **pki entity** command creates a PKI entity and displays the PKI entity view, or displays the view of an existing PKI entity.

The **undo pki entity** command deletes a PKI entity.

By default, no PKI entity is configured.

Format

pki entity *entity-name*

undo pki entity *entity-name*

Parameters

Parameter	Description	Value
entity-name	Specifies the name of a PKI entity.	The value is a string of 1 to 64 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

A PKI entity refers to the applicant or user of a certificate. A PKI entity is required when you use PKI features. After a PKI entity is created, you can configure attributes for it, for example, common name, country code, email address, FQDN, IP address, geographic area, organization, department, state, and province. These attributes include identity information of the PKI entity. The identity information will be added to the subject of a PKI entity.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Example

Configure a PKI entity **entity1** and enter the PKI entity view.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1]
```

19.17.80 pki export-certificate

Function

The **pki export-certificate** command exports a certificate to the device storage.

Format

pki export-certificate { **ca** | **local** | **ocsp** } **realm** *realm-name* { **der** | **pem** | **pkcs12** }

Parameters

Parameter	Description	Value
ca	Exports a CA certificate.	-
local	Exports a local certificate.	-
ocsp	Exports the Online Certificate Status Protocol (OCSP) certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate.	The PKI realm name must already exist.
der	Exports a certificate in DER format.	-
pem	Exports a certificate in PEM format.	-
pkcs12	Exports a certificate in P12 format.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To copy a certificate to another device, run the **pki export-certificate** command to export a certificate to the sd1 of the local device first, and then transfer the certificate to another device using a file transfer protocol.

Before using this command, run the **19.17.28 display pki certificate** command to view information about certificates on the device.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When the exported certificate file does not contain a private key, the device does not encrypt this file.

When you export the private key, the system asks you to enter the private key file name. If the private key file name and the certificate file name are the same, the private key and certificate are stored in the same file. If they are different, they are stored in different files.

When you export the private key, the system asks you to enter the private key file format and set the password. The password will be used when you run the **19.17.90 pki import-certificate** command to import this private key.

After the **enrollment self-signed** command is used in the PKI realm, you cannot use the **pki export-certificate** command to export certificates to files.

Example

Export the local certificate in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki export-certificate local realm abc pem
 Please enter the name of certificate file <length 1-127>: aa
 If you only export the certificate, do not export the private key.
 You can directly enter empty of private key file.
 Please enter the name of private key file <length 1-127>:
 Info: Succeeded in exporting the certificate.
```

Related Topics

19.17.103 pki realm (system view)

19.17.90 pki import-certificate

19.17.28 display pki certificate

19.17.81 pki export-certificate default

Function

The **pki export-certificate default** command exports a default built-in certificate to the sd1.

Format

pki export-certificate default { **ca** | **local** } **filename** *filename*

Parameters

Parameter	Description	Value
ca	Specifies the CA certificate to be exported.	-

Parameter	Description	Value
local	Specifies the local certificate to be exported.	-
filename *filename*	Specifies the name of an exported certificate file.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.

Views

System view

Default Level

3: Management level

Usage Guidelines

To copy a certificate to another device, run this command to export the certificate to the sd1 on the local device first, and transfer the certificate file to the other device using a protocol transfer protocol.

Before using this command, run the **19.17.28 display pki certificate** command to view information about default built-in certificates on the device.

Example

Export the default built-in CA certificate.

```
<Huawei> system-view
[Huawei] pki export-certificate default ca filename ca.der
 Info: Succeeded in exporting the certificate.
```

Related Topics

19.17.28 display pki certificate

19.17.82 pki export built-in-ca rsa-key-pair

Function

The **pki export built-in-ca rsa-key-pair** command exports the RSA key pair to the sd1.

Format

pki export built-in-ca rsa-key-pair *key-name* [**and-certificate** *certname*] { **pem** *file-name* [**3des** | **aes** | **des**] | **pkcs12** *file-name* } **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the RSA key pair name.	The value must be an existing RSA key pair name.
and-certificate *certname*	Indicates that the SSL decryption certificate is exported together with the associated RSA key pair.	The value must be an existing SSL decryption certificate name.
pem *file-name*	Indicates that the RSA key pair to be exported is in the PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pkcs12 *file-name*	Indicates that the RSA key pair to be exported is in the PKCS12 format and specifies the file name to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
3des | **aes** | **des**	Sets the encryption algorithm to AES, DES or 3DES if a file is exported in the PEM format. By default, AES is used. **NOTE** For security, DES and 3DES algorithms are not recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
password *password*	Specifies the password for the RSA key pair file. This password is used when you import an RSA key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). To enhance security, a password must meet the minimum strength requirements, that is, the password needs to contain at least three types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to transfer or back up the RSA key pair. After the configuration is complete, you can generate a PEM or PKCS12 file containing the RSA key pair (or also the SSL decryption certificate) in the flash.

Before using this command, run the **19.17.41 display pki rsa built-in-ca public** command to view information about the RSA key pair of the SSL decryption certificate.

Prerequisites

The RSA key pair has been created for the SSL decryption certificate using the **19.17.105 pki rsa built-in-ca** command with the **exportable** parameter specified, or the RSA key pair of the SSL decryption certificate has been imported to the memory using the **19.17.94 pki import built-in-ca rsa-key-pair** command with the **exportable** parameter specified.

Precautions

An RSA key pair is sensitive information. Delete or destroy the exported RSA key pair from your device or storage device immediately after you do not use it.

Example

Export RSA key pair **key2** to file **aaa.pem** and set the encryption method to AES.

```
<Huawei> system-view [Huawei] pki rsa built-in-ca key2 create exportable  Info: The name of the new
key-pair will be: key2  The size of the public key ranges from 512 to 4096.  Input the bits in the
modules:2048  Generating key-pairs... .......+++  ............................+++   [Huawei] pki export built-in-ca rsa-
key-pair key2 pem aaa.pem aes password Hello@123  Warning: Exporting the key pair impose security
risks, are you sure you want to  export it? [y/n]:y                                    Info: Succeeded
in exporting the RSA key pair in PEM format.
```

Related Topics

19.17.94 pki import built-in-ca rsa-key-pair

19.17.91 pki import-certificate built-in-ca

19.17.41 display pki rsa built-in-ca public

19.17.83 pki export rsa-key-pair

Function

The **pki export rsa-key-pair** command exports the RSA key pair to the sd1 and allows the export of the associated certificate.

Format

pki export rsa-key-pair *key-name* [**and-certificate** *certificate-name*] { **pem** *file-name* [**3des** | **aes** | **des**] | **pkcs12** *file-name* } **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value must be an existing RSA key pair name.
and-certificate *certificate-name*	Indicates that the certificate related to the RSA key pair are exported.	The value must be an existing certificate file name.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pem *file-name*	Indicates that the RSA key pair to be exported is in the PEM format and specifies the name of the file to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pkcs12 *file-name*	Indicates that the RSA key pair to be exported is in the PKCS12 format and specifies the file name to be exported.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
3des | **aes** | **des**	Sets the encryption algorithm to DES, 3DES or AES if a file is exported in the PEM format. The default value is AES. **NOTE** DES and 3DES are less secure than AES and are not recommended.	-
password *password*	Specifies the encryption password for the RSA key pair file. This password is used when you import an RSA key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). To enhance security, a password must contain at least two types of the following characters: uppercase letters, lowercase letters, numerals, and special characters, such as exclamation points (!), at signs (@), number signs (#), dollar signs ($), and percent (%).

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To transfer or back up an RSA key pair, run this command to generate the PEM or PKCS12 file carrying this RSA key pair (which may include the certificate) in the sd1.

Before using this command, run the **19.17.42 display pki rsa local-key-pair** command to view information about the RSA key pairs on the device.

Prerequisites

The RSA key pair has been created and configured to be exportable using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

The RSA key pair is sensitive information. Delete and destroy the exported RSA key pair on the device or storage device immediately after you do not need it.

Example

Export the RSA key pair **key1** to the file **aaa.pem** and set the encryption method to AES.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create key1 exportable
 Info: The name of the new key-pair will be: key1
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
......+++
....................+++
[Huawei] pki export rsa-key-pair key1 pem aaa.pem aes password Admin@1234
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting the RSA key pair in PEM format.
```

Related Topics

19.17.106 pki rsa local-key-pair create

19.17.95 pki import rsa-key-pair

19.17.42 display pki rsa local-key-pair

19.17.84 pki export sm2-key-pair

Function

The **pki export sm2-key-pair** command exports the SM2 key pair to the device storage.

Format

pki export sm2-key-pair *key-name* **der** *file-name*

pki export sm2-key-pair *key-name* **pem** *file-name* [**password** *password*]

Parameters

Parameter	Description	Value
key-name	Specifies the SM2 key pair name.	The value must be an existing SM2 key pair name.
der *file-name*	Exports the SM2 key pair as a DER file and specifies the file name.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
pem *file-name*	Exports the SM2 key pair as a PEM file and specifies the file name.	The value is a string of 1 to 64 case-insensitive characters without spaces and question marks (?). When the value contains a directory, it is a string of 1 to 127 characters, for example, flash:/8ab3/ab3.pem.
password *password*	Specifies the password for the SM2 key pair file. This password is used when you import an SM2 key pair file.	The value is a string of 6 to 32 case-sensitive characters without question marks (?). For security purposes, the password must contain at least three types of the following: uppercase letters, lowercase letters, numerals, and special characters (such as ! @ # $ %).

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To transfer or back up an SM2 key pair, run this command to generate a file carrying this SM2 key pair in the device storage.

Before using this command, run the **19.17.43 display pki sm2 local-key-pair public (System view)** command to view information about the SM2 key pairs on the device.

Prerequisites

The RSA key pair has been created using the **19.17.109 pki sm2 local-key-pair create** command with the **exportable** parameter specified or the RSA key pair has been imported to the memory using the **19.17.96 pki import sm2-key-pair** command with the **exportable** parameter specified.

Precautions

An SM2 key pair is sensitive information. Delete or destroy the exported SM2 key pair from your device or storage device immediately after you do not use it.

Example

Export the SM2 key pair **key-1** to the file **aaa.pem**.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create key-1 exportable
 Info: The name of the new key-pair will be: key-1
 Generating key-pairs...
[Huawei] pki export sm2-key-pair key-1 pem aaa.pem password Admin@1234
 Warning: Exporting the key pair impose security risks, are you sure you want to
 export it? [y/n]:y
 Info: Succeeded in exporting SM2 key pair in PEM format.
```

Related Topics

19.17.109 pki sm2 local-key-pair create

19.17.96 pki import sm2-key-pair

19.17.43 display pki sm2 local-key-pair public (System view)

19.17.85 pki file-format

Function

The **pki file-format** command sets the format for the saved certificate request, certificate, and CRL.

By default, the device stores certificate request, certificate, and CRL in PEM format.

Format

pki file-format { **der** | **pem** }

Parameters

Parameter	Description	Value
der	Indicates that the format of a certificate request file is DER.	-
pem	Indicates that the format of a certificate request file is PEM.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To change the format for the saved certificate request, certificate, and CRL, for example, to use the certificate and CRL obtained through CMPv2, SCEP, or LDAP, run the **pki file-format** command.

However, the certificate and CRL obtained through HTTP are downloaded directly and are not saved in the format configured using this command. The created self-signed certificate or local certificate can only be saved in PEM format.

Example

Set the format of saved certificate request, certificate, and CRL to DER.

```
<Huawei> system-view
[Huawei] pki file-format der
```

19.17.86 pki generate built-in-ca certificate

Function

The **pki generate built-in-ca certificate** command generates an SSL decryption certificate.

Format

pki generate built-in-ca certificate rsa-key-pair *rsa-key-pair-name* **entity** *entity-name*

Parameters

Parameter	Description	Value
rsa-key-pair *rsa-key-pair-name*	Specifies the name of the RSA key pair in an SSL decryption certificate.	The RSA key pair must exist in the memory.
entity *entity-name*	Specifies the PKI entity name.	The PKI entity must have been configured and have a common name. If the PKI entity does not have a common name, an SSL decryption certificate cannot be generated.

Views

System view:

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable a proxy for SSL connection, the device complies with the certificate information on the real server and issues another certificate to the client using the SSL decryption certificate.

The generated SSL decryption certificate files are saved to the "sd1:/" directory.

Prerequisites

1. An RSA key pair of the SSL decryption certificate has been created using the **19.17.105 pki rsa built-in-ca** command or the RSA key pair has been imported to the memory of the device using the **19.17.94 pki import built-in-ca rsa-key-pair** command.
2. A PKI entity has been created using the **19.17.79 pki entity** command.
3. The common name of the PKI entity has been configured using the **19.17.17 common-name** command.

Example

Generate an SSL decryption certificate.

```
<Huawei> system-view
[Huawei] pki rsa built-in-ca rsakey create
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
........++++++
........++++++
[Huawei] pki entity entity1
```

```
[Huawei-pki-entity-entity1] common-name huawei
[Huawei-pki-entity-entity1] quit
[Huawei] pki generate built-in-ca certificate rsa-key-pair rsakey entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : key1
Info: Generate built in CA certificate successfully.
```

Related Topics

19.17.105 pki rsa built-in-ca

19.17.94 pki import built-in-ca rsa-key-pair

19.17.79 pki entity

19.17.17 common-name

19.17.29 display pki certificate built-in-ca

19.17.87 pki get-certificate

Function

The **pki get-certificate** command downloads a certificate to the device storage.

Format

pki get-certificate { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Specifies a CA or RA certificate to be obtained.	-
local	Specifies a local certificate to be obtained.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be obtained.	The value must be an existing PKI realm name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the SCEP method is used, the PKI entity queries and obtains issued certificates on the CA server and stores the certificates to the local storage. The

 Copyright © Huawei Technologies Co., Ltd.

PKI entity can download their own certificates, CA certificates, or local certificates of other entities.

The purposes of obtaining a certificate are as follows:

- Stores certificates to the device storage to improve certificate query efficiency and reduce the times of querying the PKI certificate repository.
- Prepares for certificate authentication.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

Precautions

After obtaining a CA certificate, the device automatically imports the certificate to the device memory. After the device obtains a local certificate, you need to import it to the memory manually.

If the same certificate exists on the device, delete the existing one; otherwise, the certificate cannot be obtained.

Example

Obtain the CA certificate in the PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki get-certificate ca realm abc
```

Related Topics

19.17.103 pki realm (system view)

19.17.88 pki get-crl

Function

The **pki get-crl** command updates CRL immediately.

Format

pki get-crl realm *realm-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name of the CRL.	The value must be an existing PKI realm name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The CRL status is checked periodically when it is updated automatically. If the CRL on the device is likely to expire, configure this command to update CRL immediately.

After this command is executed, the new CRL replaces the old CRL in the storage, and is automatically imported to the memory to replace the old one.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command.

Example

Configure the CRL immediate update.

```
<Huawei> system-view
[Huawei] pki realm test
[Huawei-pki-realm-test] quit
[Huawei] pki get-crl realm test
```

Related Topics

19.17.103 pki realm (system view)

19.17.89 pki http

Function

The **pki http** command configures a device to use HTTP to download a CA certificate, local certificate, or CRL.

Format

pki http [**esc**] *url-address save-name*

Parameters

Parameter	Description	Value
esc	Specifies the entering of URLs in the ASCII code.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
url-address	Specifies the URL of a CA certificate, local certificate, or CRL.	The value is a string of 1 to 128 case-sensitive characters.
save-name	Specifies the name of a CA certificate, local certificate, or CRL saved on the sd1 of the device.	The value is a string of 1 to 64 case-insensitive characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Before you configure a device to use HTTP to download a CA certificate, local certificate, or CRL, ensure that the sd1 of the device has enough space to accommodate the CA certificate, local certificate, or CRL.

Keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code, and **3f** is the hexadecimal ASCII code for the question mark (?). Therefore, the entered URL must be in **\x3f** format. For example, the URL that an administrator needs to enter is **http://www.***.com\x3fpage1**, instead of **http://www.***.com?page1**. If the administrator wants to configure **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the administrator should add an escape character (\) to \x3f and enter **http://www.***.com\x3fpage1\\x3f.**

Example

Configure a device to use HTTP to download a local certificate.

```
<Huawei> system-view
[Huawei] pki http http://10.1.1.1/test.cer local.cer
```

Configure a device to use HTTP to download a local certificate.

```
<Huawei> system-view
[Huawei] pki http esc http://www.***.com\x3fpage1\\x3f local.cer
```

19.17.90 pki import-certificate

Function

The **pki import-certificate** command imports a certificate to the device memory.

Format

pki import-certificate { **ca** | **local** } **realm** *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*] [**replace**] [**no-check-validate**] [**no-check-hash-alg**]

pki import-certificate { **ca** | **local** } **realm** *realm-name* **pkcs12 filename** *filename* [**replace**] [**no-check-validate**] [**no-check-hash-alg**] **password** *password*

pki import-certificate ocsp realm *realm-name* { **der** | **pkcs12** | **pem** } [**filename** *filename*]

pki import-certificate ocsp realm *realm-name* **pkcs12 filename** *filename* **password** *password*

pki import-certificate realm *realm-name* **pem terminal password** *password*

Parameters

Parameter	Description	Value
ca	Imports a CA certificate. For example, when the device works as an SSL proxy, import the SSL proxy CA certificate and use the private key in the certificate to sign the SSL client certificate again.	-
local	Imports a local certificate.	-
realm *realm-name*	Specifies the PKI realm name of the imported certificate.	The PKI realm name must already exist. **NOTE** The domain name cannot contain spaces. Otherwise, the certificate cannot be imported.
der	Imports a certificate in DER format.	-
pkcs12	Imports a certificate in PKCS12 format.	-
pem	Imports a certificate in PEM format.	-
filename *filename*	Specifies the name of the imported certificate.	The file name must already exist.
replace	Deletes the original certificate and RSA key pair and imports the new certificate when there are repeated certificates in the domain. **NOTE** If the RSA key pair of the original certificate is not referenced by other domains, the certificate and key pair are deleted. If the RSA key pair of the original certificate is referenced by other domains or a CMP session, only the original certificate is deleted but the key pair is not deleted.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
no-check-validate	Specifies whether the validity check is performed on the imported certificate.	-
no-check-hash-alg	Specifies whether a check is performed on the hash algorithm used for the signature of the imported certificate.	-
ocsp	Imports the Online Certificate Status Protocol (OCSP) server's certificate.	-
terminal	Specifies the terminal import mode.	-
password *password*	Specifies the decryption password of the certificate, and the password is the same as the password set by the **19.17.80 pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a certificate is saved to the storage, run this command to import the certificate to the memory for it to take effect.

The device supports the following certificate import modes:

- terminal: Import or copy the certificate file of the peer to the local device. That is, you can open the PEM certificate file using a text tool and copy the certificate content to the local device.
- file: The **filename** parameter is specified to import the certificate file of the peer.

Multiple certificates can be imported on the device, including the CA certificate, local certificate, and private key.

NOTE

If you do not know the format of the certificate you want to import, configure each format in turn and check whether the certificate is successfully imported.

Prerequisites

The PKI realm has been created using the **19.17.103 pki realm (system view)** command, and the certificate file already exists on the storage device.

Precautions

If a certificate file contains a key pair file, the **pki import-certificate** command imports only the certificate file, but not the key pair file. To import the key pair file, run the **pki import rsa-key-pair** command after the **pki import-certificate** command, or run the **pki import rsa-key-pair** command to import the certificate and key pair files simultaneously.

It is not recommended that multiple local certificates be imported into the same PKI realm. Otherwise, certificate-related services may use the certificates that do not match the services, causing services to become unavailable.

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_localx.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported should be less than 50 characters, so the total certificate file name does not exceed 64 characters, and the certificate file cannot be imported to the storage component.

When you import a certificate through a terminal, the key pair name is case-sensitive and contains 1 to 64 characters without spaces or question marks (?).

The device supports importing digital certificates generated through RSA encryption algorithms.

Example

Import a local certificate to PKI realm **abc** in file transfer mode.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki import-certificate local realm abc pem filename local.cer
 Info: Succeeded in importing the certificate.
```

Import a local certificate to the PKI realm **abc** in the terminal mode.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki import-certificate realm abc pem terminal password abc123
Enter encrypted private General Purpose key name:a
Please choise the key exportable: 1 (exportable):1
Enter PEM-formatted CA certificate.
End with a blank line or "end" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIQPLn9V3dmGr1LguLTIYI8RTANBgkqhkiG9w0BAQUFADBY
MRMwEQYKCZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGaHVhd2VpMRUw
EwYKCZImiZPyLGQBGRYFY2hpbmExEjAQBgNVBAMTCUNBIHNlcnZlcjAeFw0xMzEw
MTgwMjE4MzNaFw0xODEwMTgwMjI3NTlaMFgxEzARBgoJkiaJk/IsZAEZFgNjb20x
FjAUBgoJkiaJk/IsZAEZFgZodWF3ZWkxFTATBgoJkiaJk/IsZAEZFgVjaGluYTES
MBAGA1UEAxMJQ0Egc2VydmVyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEArdox+Z5U5T8D2W+dTihLydJ7+bMRF5Z1QDZvX8M9OmL01pTGKSq2LETqRDhT
u3N9L/yuYywylDeFXLsNL5KSYJVyV/VSUpawARiJ1EzWGke4Gdpqm+zQUpI5pxT
5SCwJKNcpQVPmPRpE1rmU/3czR/YzYHYkjO6sTqLDskOUBerjpMVx0J/y35EXSC/
7oiuXd/iU0W+unv97C4T7rZwpMtrn9RPpQtL95GacP8WlDCJjIopOQd//Q5POeAX
xLzfR87z8ri66UbrU8lU6/ZWlWma6hgIiBBfMLhgUdasDZ+neiNPEFdCZEdVEbm9
Of0X3GZU5XcoD7oNSa2s4diZFQIDAQABo4IBADCB/TATBgkrBgEEAYI3FAIEBh4E
AEMAQTALBgNVHQ8EBAMCAUYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUcLyj
kl6b2uhKC8Cq87bclb768yMwgZYGA1UdHwSBjjCBizCBiKCBhaCBgoY/aHR0cDov
L3owMDEzOTkwMWFiYy5jaGluYS5odWF3ZWkuY29tL0NlcnRFbnJvbGwvQ0ElMjBz
ZXJ2ZXIuY3Jshj9maWxlOi8vXFx6MDAxMzk5MDFhYmMuY2hpbmEuaHVhd2VpLmNv
```

```
bVxDZXJ0RW5yb2xsXENBIHNlcnZlci5jcmwwEAYJKwYBBAGCNxUBBAMCAQAwDQYJ
KoZIhvcNAQEFBQADggEBAA2ROwrZ+0fQPs2FqdaoJp3QYA2pgJR8hGQ8n9vskVel
9UG3o7bsgmCPpfNb0k826Iuqur9PL7mQZvYmY+OH9tCC3zbwuJXrrZlfimFd9aH7
0V5MGRNuEkO5xPK2jNwHeg//Rnt7hCOnKiQP0/LBKRiEnXPrOoqtLgHaQsbu7gSs
HFHDoV+V1Hpo+n9Jtl0Eosi9g1gxCIueUOMT8eZC5coFHEIz661tXHcgwePK8lnh
Yfwc0YtJmbSr3gUVTztkrPODMf0msscVq8sZ3ewLfYqUlb85pt0c/GQwxSHYBfIe
JJopiEXZce1aMnwyScKjpyh8fbDOX3n6Uh/VeDCBnoU=
-----END CERTIFICATE-----
end
Enter PEM-formatted encrypted private General Purpose key.
End with "end" on a line by itself
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,F18D190B5CA99826

SFvJFyZUJbWlXOQh2cg4hh8yWW5fLeWw21rj9xn5P5ylsEtwxr+hZtgM+tGTW3BL
GzCgUkmnL+03EOaZXS4jW7v7lsNqciyvCPbeKGtSpPpGJ8MgVoqDdjAX1uKzPxsN
PcEbkMJd8Ak5o1PGv6fCtFmeFJVvTHGm/lyHtvn6aUy+riEywE4bgYNHc+C7NMHw
dIjICj31h4BAbTfBK4pyqxAL+nn3G5ayyAWlK/KYls3sEHHzScbyKQjuzIffkgNQ
ku/FcEvUvC69yBlp+75HEQG0WbpURfcCOBpLZrllxMpfrLVtMmE9HsrDeV6xG7XW
RbHeciBMjBN9zP0Pm0F0JdJp4I+Xv9CKWJ82KgigSHQTOKRVhgXp2Kryh7j4IVUh
tWOusOQC3/cKEDrhpx1sCHeRtXPA5/y3RZb6jGxx4iwkkK5qv/RN0W+4iNqZf6PO
KRKh6seR7h9F0eHQoTbT1uL5ow2SOSqfZOPnB9+t0qQBUSE4E8ZjsgohQBcTgQ8q
w21iiQZeyMHSrx6kiYsQxc1egxr8I/QV4OCEP9vH7tpu6vdnlc/WHBI7JhOV0u9Z
5sRm1ktOgfiqnpYVg+iB3wJtIVCtJiwvjSkLW0m+KdrrUiT9scPti7y0PReHacs/
fkjsey72T/mxPR24NJOpYYznF+whpwrCd3Io4lfxZDOzvUNtGD3ySbEcTe/PQBKj
TYcUlAn06VvCurYJV9jXqi9qt4tHKtQD0j7ToLTXpvTBYW0BaRULo1OZl9c+49B/
zlJfe3cU0VZpXOVowL5xPL6lvESDKjzQYRzKOBfJGwJs4OcBKGJ8XQ==
-----END RSA PRIVATE KEY-----
end
Enter PEM-formatted General Purpose certificate.
End with a blank line or "end" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIFITCCBAmgAwIBAgIKGmoeqQAAAACZVDANBgkqhkiG9w0BAQUFADBYMRMwEQYK
CZImiZPyLGQBGRYDY29tMRYwFAYKCZImiZPyLGQBGRYGaHVhd2VpMRUwEwYKCZIm
iZPyLGQBGRYFY2hpbmExEjAQBgNVBAMTCUNBIHNlcnZlcjAeFw0xNDAyMTAwNTU0
NTlaFw0xNTAyMTAwNjA0NTlaMAwxCjAIBgNVBAMTAWEwgZ8wDQYJKoZIhvcNAQEB
BQADgY0AMIGJAoGBAN5vT5A2Dy7iwTwNeisaWBecRi7SAzHyEer7U5ZzSsA/6xt9
LulqBoV8rMIsNe54flnxQww74QE8CBVkj1UJ5Fsq+S0UtU2fphSJkZMOVM0zmnPb
S6YyWoDOjR6JAKlxAgwYdAoO3iD/7xaIIgtXrKQqj+dt7eieTSy5Z8dEWkJxAgMB
AAGjggK7MIICtzAdBgNVHQ4EFgQUOOMbU4dquenYHLpyaSP5cS3vNBgwHwYDVR0j
BBgwFoAUcLyjkl6b2uhKC8Cq87bclb768yMwggFJBgNVHR8EggFAMIIBPDCCATig
ggE0oIIBMIaBq2xkYXA6Ly8vQ049Q0ElMjBzZXJ2ZXIsQ049ejAwMTM5OTAxYWJj
LENOPUNEUCxDTj1QdWJsaWMlMjBLZXklMjBTZXJ2aWNlcyxDTj1TZXJ2aWNlcyxE
Qz1VbmF2YWlsYWJsZUNvbmZpZ0ROP2NlcnRpZmljYXRlUmV2b2NhdGlvbkxpc3Q/
YmFzZT9vYmplY3RDbGFzcz1jUkxEaXN0cmlidXRpb25Qb2ludIY/aHR0cDovL3ow
MDEzOTkwMWFiYy5jaGluYS5odWF3ZWkuY29tL0NlcnRFbnJvbGwvQ0ElMjBzZXJ2
ZXIuY3Jshj9maWxlOi8vXFx6MDAxMzk5MDFhYmMuY2hpbmEuaHVhd2VpLmNvbVxD
ZXJ0RW5yb2xsXENBIHNlcnZlci5jcmwwgeYGCCsGAQUFBwEBBIHZMIHWMGkGCCsG
AQUFBzAChl1odHRwOi8vejAwMTM5OTAxYWJjLmNoaW5hLmh1YXdlaS5jb20vQ2Vy
dEVucm9sbC96MDAxMzk5MDFhYmMuY2hpbmEuaHVhd2VpLmNvbV9DQSUyMHNlcnZl
ci5jcnQwaQYIKwYBBQUHMAKGXWZpbGU6Ly9cXHowMDEzOTkwMWFiYy5jaGluYS5o
dWF3ZWkuY29tXENlcnRFbnJvbGxcejAwMTM5OTAxYWJjLmNoaW5hLmh1YXdlaS5j
b21fQ0Egc2VydmVyLmNydDA/BgkrBgEEAYI3FAIEMh4wAEkAUABTAEUAQwBJAG4A
dABlAHIAbQBlAGQAaQBhAHQAZQBPAGYAZgBsAGkAbgBlMA0GCSqGSIb3DQEBBQUA
A4IBAQAQgqIzSVgOi1MOXIMNUREK35g/8zgPZwFw19jZeM5Jc0X7aJoV3PDFeCnA
pvzvKn/H/oB6UCSCX4RVdYhJI17ymSeBZUrq4XKsWOCPykwK34xc4cPpthQ9fcjc
pwHOq+JGWSfNsS9PBdzhxn+BrH4BlndMu3H/95bluf0kFNbIyaZeuqwEmFkrJVxt
6u6PLVqhQyu0LhKUBMDavfi6e5/HEGaGoj18d2uUEYNWQOBcUoEhnnZ/7sCoTyRP
AsrXoUoS94lnX8z/GGK5nV+X6bvxbo6l0qyBtU/9Iax5MwLIXUBhzXUi0q5C5A2C
8KbFCoMv33ecr0ma94LRnn7qnVsr
-----END CERTIFICATE-----
end
 Successfully to import the certificate chain.
```

Related Topics

19.17.33 display pki credential-storage-path
19.17.103 pki realm (system view)

19.17.80 pki export-certificate
19.17.89 pki http
19.17.97 pki ldap

19.17.91 pki import-certificate built-in-ca

Function

The **pki import-certificate built-in-ca** command imports the SSL decryption certificate to the memory.

Format

pki import-certificate built-in-ca filename *file-name*

Parameters

Parameter	Description	Value
filename *file-name*	Specifies the file name of the SSL decryption certificate.	The value must be the name of an existing SSL decryption certificate.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Import the SSL decryption certificate to the memory to use it; otherwise, the certificate will not take effect.

When importing the SSL decryption certificate, make sure that the matching RSA key pair in the SSL decryption certificate exists on the device. The mapping relationship is created when the SSL decryption certificate is created. Search for the RSA key pair that corresponds to the SSL decryption certificate using the **19.17.69 pki built-in-ca match-rsa-key** command.

Prerequisites

The SSL decryption certificate file already exists on the storage device, and is generated using the **19.17.86 pki generate built-in-ca certificate** command.

Example

Import the SSL decryption certificate **key1_builtinca.cer** to the memory.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pki generate built-in-ca certificate rsa-key-pair key1 entity entity1
 Please enter the file name for built in CA certificate <length 1-64> : key1_builtinca.cer
 Info: Generate built in CA certificate successfully.
[Huawei] pki import-certificate built-in-ca filename key1_builtinca.cer
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.86 pki generate built-in-ca certificate

19.17.69 pki built-in-ca match-rsa-key

19.17.92 pki import-certificate peer

Function

The **pki import-certificate peer** command imports a certificate of the remote device to the device memory.

Format

pki import-certificate peer *peer-name* { **der** | **pem** | **pkcs12** } **filename** [*filename*]

pki import-certificate peer *peer-name* **pkcs12 filename** *filename* **password** *password*

pki import-certificate peer *peer-name* **pem terminal**

Parameters

Parameter	Description	Value
peer-name	Specifies the name of peer certificate. A certificate cannot be imported to multiple peers.	The value is a string of 1 to 32 case-insensitive characters without spaces. If the character string is quoted by double quotation marks, it can contain spaces.
der	Imports a certificate of the remote device in DER format.	-
pem	Imports a certificate of the remote device in PEM format.	-
pkcs12	Imports a certificate of the remote device in P12 format.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
filename *filename*	Imports a certificate of the remote device in file mode.	The value is an existing name of certificate of the remote device.
password *password*	Specifies the decryption password of the certificate, and the password is the same as the password set by the **19.17.80 pki export-certificate** command.	The value must be the name of an existing decryption password of the certificate.
terminal	Imports a certificate of the remote device in terminal mode.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Where digital envelop authentication is used, configure the public key of the remote device. The public key can be obtained from the public and private key management module or certificate of the remote device.

The device supports the following certificate import modes:

- terminal: Import or copy the certificate file of the peer to the local device. That is, you can open the PEM certificate file using a text tool and copy the certificate content to the local device.
- file: The **filename** parameter is specified to import the certificate file of the peer.

Prerequisites

The certificate file of the remote device must already exist on the storage device.

Precautions

When a certificate in **pkcs12** format is imported, the PKI system deletes the file name extension of the original certificate file, adds **_localx.cer** to generate a new file name, and saves it to the storage component. Therefore, the name of the certificate file to be imported cannot exceed 50 characters. Otherwise, the total certificate file name will exceed 64 characters, and the certificate file cannot be imported to the storage component.

 Copyright © Huawei Technologies Co., Ltd.

You can import a peer certificate generated using the RSA encryption algorithm to the device.

Example

Import the certificate **aa.pem** of the remote device in the file mode.

```
<Huawei> system-view
[Huawei] pki import-certificate peer abcd pem file aa.pem
 Info: Succeeded in importing the peer certificate.
```

Import the certificate **aa.pem** of the remote device in the terminal mode.

```
<Huawei> system-view
[Huawei] pki import-certificate peer abcd pem terminal
Enter PEM-formatted peer certificate.
End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIDvDCCAqSgAwIBAgIKEhk80wAAAAAEmjANBgkqhkiG9w0BAQUFADASMRAwDgYD
VQQDDAdDQV9ST09UMB4XDTEzMDIxOTEzMDAyMloXDTE0MDIxOTEzMTAyMlowDDEK
MAgGA1UEAxMBYTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC5i0dlqZntWLJjdGVW
0Qi7HY9O7XKiSu/YRT1T28jr31OeX8eWRmUUGqty6aJxyHrwUQzMObsUdX3xvIgs
py7pAgMBAAGjggHgMIIB3DAdBgNVHQ4EFgQU4luKA1gByOMUvBhb+b0AaFvRkE4w
HwYDVR0jBBgwFoAUzrrKOcetasuFF9CKjigCC1LU2SswQAYDVR0fBDkwNzA1oDOg
MYYvaHR0cDovLzEwLjEzNi41NS43Njo4MDgwL0NlcnRFbnJvbGwvQ0FfUk9PVC5j
cmwwggEVBggrBgEFBQcBAQSCAQcwggEDMIGjBggrBgEFBQcwAoaBlmxkYXA6Ly8v
Q049Q0FfUk9PVCxDTj1BSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049
U2VydmljZXMsQ049Q29uZmlndXJhdGlvbixEQz1lc2FwLERDPWNvbT9jQUNlcnRp
ZmljYXRlP2Jhc2U/b2JqZWN0Q2xhc3M9Y2VydGlmaWNhdGlvbkF1dGhvcml0eTBb
BggrBgEFBQcwAoZPaHR0cDovL2h1YXdlaS1uem01Z3cyZy5lc2FwLmNvbS9DZXJ0
RW5yb2xsL2h1YXdlaS1uem01Z3cyZy5lc2FwLmNvbV9DQV9ST09ULmNydDA/Bgkr
BgEEAYI3FAIEMh4wAEkAUABTAEUAQwBJAG4AdABlAHIAbQBlAGQAaQBhAHQAZQBP
AGYAZgBsAGkAbgBlMA0GCSqGSIb3DQEBBQUAA4IBAQC7i3evrt8uDL16KW52I619
aW0NFtkYgq1PUrPNHBr8NAAzNo1HKiAkUrcCdcyrO0z4KqmpT0b7wiEAwbXCZwyx
mSpie3FN58KTKbvssekogi93YewoZjXLXxUEc3fYJpF7olZ0UTML8QQoJLJxWK1c
+JYXDfe3X0u57Ql5vFQhxZuQ93shqlqqb1Hkec64NYsZkFGU5sJh+CRGhUypab2K
78JkuBmrC2vsNEGNQ0NE0RtMSiPNQFJ6LoxdtmJVk0XIPt6xUYLQu3y4CXuXCHuT
F0Coby3t9D42ECog40fh+63+l3OnU9D4Usq2Dujx32x6Nzm7gvkDyUpxZd9vN+a3
-----END CERTIFICATE-----

 Info: Succeeded in importing the peer certificate.
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.39 display pki peer-certificate

19.17.93 pki import-crl

Function

The **pki import-crl** command imports the CRL to the memory.

Format

pki import-crl realm *realm-name* **filename** *file-name*

Parameters

Parameter	Description	Value
realm *realm-name*	Specifies the PKI realm name.	The value must be an existing PKI realm name.
filename *file-name*	Specifies the name of an imported certificate or CRL file. The certificates only support the PEM and DER formats.	The value must be an existing certificate or CRL file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable the CRL that is obtained in out-of-band mode or is updated manually, run this command to import the CRL to the memory.

Prerequisites

A PKI realm has been created using the **19.17.103 pki realm (system view)** command and the CRL file has been downloaded using HTTP or LDAP.

Example

Import the CRL in the PKI realm to the memory.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] quit
[Huawei] pki http esc http://www.***.com\x3fpage1\\x3f abc.crl
[Huawei] pki import-crl realm abc filename abc.crl
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.103 pki realm (system view)

19.17.89 pki http

19.17.97 pki ldap

19.17.34 display pki crl

 Copyright © Huawei Technologies Co., Ltd.

19.17.94 pki import built-in-ca rsa-key-pair

Function

The **pki import built-in-ca rsa-key-pair** command imports an RSA key pair in the SSL decryption certificate to the device memory.

Format

pki import built-in-ca rsa-key-pair *key-name* { **pem** | **pkcs12** } *file-name* [**exportable**] **password** *password*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
pem *file-name*	Specifies the format of the imported RSA key pair as PEM, and specifies the name of the RSA key pair file.	The value must be an existing certificate file name.
pkcs12 *file-name*	Specifies the format of the imported RSA key pair as PKCS12, and specifies the name of the RSA key pair file.	The value must be an existing certificate file name.
exportable	Specifies the imported RSA key pair as exportable.	-
password *password*	Specifies the decryption password of the RSA key pair, and the password is the same as the password set by the **19.17.82 pki export built-in-ca rsa-key-pair** command.	The value must be the name of an existing decryption password of the RSA key pair.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When using the DSA key pair generated by other entities, store the RSA key pair on the sd1 of the local device. To make the RSA key pair take effect, run this command to import it to the memory.

Prerequisites

The RSA key pair must already exist on the storage device.

Example

Import RSA key pair **aaa.pem**. In the system, the RSA key pair name is **key-1** and password **Test!123**, and can be marked **exportable**.

```
<Huawei> system-view
[Huawei] pki import built-in-ca rsa-key-pair key-1 pem aaa.pem exportable password Test!123
 Info: Succeeded in importing the RSA key pair in PEM format.
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.82 pki export built-in-ca rsa-key-pair

19.17.95 pki import rsa-key-pair

Function

The **pki import rsa-key-pair** command imports the RSA key pair to the device memory.

Format

pki import rsa-key-pair *key-name* { **pem** | **pkcs12** } *file-name* [**exportable**] [**password** *password*]

pki import rsa-key-pair *key-name* **der** *file-name* [**exportable**]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
pem *file-name*	Indicates that the RSA key pair to be imported is in the PEM format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
pkcs12 *file-name*	Indicates that the RSA key pair to be imported is in the PKCS12 format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
der *file-name*	Indicates that the RSA key pair to be imported is in the DER format and specifies the file name to store the RSA key pair.	The value must be an existing certificate file name that stores the RSA key pair and the certificate.
exportable	Indicates that the imported RSA key pair can be exported.	-
password *password*	Specifies the decryption password of the RSA key pair. , and the password is the same as the password set by the **19.17.83 pki export rsa-key-pair** command	The value must be the name of an existing decryption password of the RSA key pair. **NOTE** If the RSA key pair file does not have a decryption password, you need to enter any character. Otherwise, the import will fail.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to use the RSA key pair generated by other entities. After the configuration, the imported RSA key pair can be referenced by the PKI module for operations such as signing.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

If you do not know the format of the key pair you want to import, configure each format in turn and check whether the key pair is successfully imported.

Prerequisites

The RSA key pair must already exist on the storage device.

Example

Import RSA key pair **aaa.pem**. In the system, the RSA key pair name is **key-1**, and the password is **Test!123456**. The RSA key pair name can be marked **exportable**.

```
<Huawei> system-view
[Huawei] pki import rsa-key-pair key-1 pem aaa.pem exportable password Test!123456
 Info: Succeeded in importing the RSA key pair in PEM format.
```

Related Topics

19.17.33 display pki credential-storage-path
19.17.83 pki export rsa-key-pair

19.17.96 pki import sm2-key-pair

Function

The **pki import sm2-key-pair** command imports the SM2 key pair to the device memory.

Format

pki import sm2-key-pair *key-name* **der** *file-name* [**exportable**]

pki import sm2-key-pair *key-name* **pem** *file-name* [**exportable**] [**password** *password*]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the SM2 key pair to be imported on the device.	The value is a string of 1 to 64 characters and case-sensitive without spaces or question marks (?). If the character string is quoted by double quotation marks (" "), the character string can contain spaces.
der *file-name*	Specifies the format of the imported SM2 key pair as DER, and specifies the name of the file that stores the SM2 key pair.	The value must be an existing SM2 key pair name.
pem *file-name*	Specifies the format of the SM2 key pair to be imported as PEM, and specifies the name of the file that stores the SM2 key pair.	The value must be an existing SM2 key pair name.
exportable	Specifies the imported SM2 key pair as exportable.	-
password *password*	Specifies the decryption password of the SM2 key pair. The decryption password is the same as the password set by the **19.17.84 pki export sm2-key-pair** command.	The value must be the existing decryption password of the SM2 key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run this command to use the SM2 key pairs generated by other entities.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The SM2 key pair must already exist on the storage device.

Example

Import the SM2 key pair "**aaa.pem**" in the PEM format. The SM2 key pair is named **key-1** in the system with the decryption password **Admin@1234**, and is marked exportable.

```
<Huawei> system-view
[Huawei] pki import sm2-key-pair key-1 pem aaa.pem exportable password Admin@1234
 Info: Succeeded in importing SM2 key pair in PEM format.
```

Related Topics

19.17.33 display pki credential-storage-path

19.17.97 pki ldap

Function

The **pki ldap** command configures a device to use LDAP to download a CA certificate, local certificate, or CRL.

Format

pki ldap ip *ip-address* **port** *port* **version** *version* [**attribute** *attr-value*] [**authentication** *ldap-dn ldap-password*] *save-name* **dn** *dn-value*

Parameters

Parameter	Description	Value
ip-address	Specifies the IP address of an LDAP server.	The value is in dotted decimal notation.
port *port*	Specifies the port number of an LDAP server.	The value is an integer that ranges from 1 to 65535. The default value is 389.
version *version*	Specifies the version number of LDAP.	The value is an integer that ranges from 2 to 3. The default value is 3.
attribute *attr-value*	Specifies the attribute used by a device to request a certificate from an LDAP server.	The value is a string of 1 to 64 case-sensitive characters without question marks and spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
authentication *ldap-dn ldap-password*	Specifies the user name and password authenticated by the LDAP server.	*ldap-dn*: The value is a string of 1 to 64 case-sensitive characters without question marks and spaces. *ldap-password*: The value is a string of 1 to 32 case-sensitive characters without question marks and spaces.
save-name	Specifies the name of a CA certificate, local certificate, or CRL saved on the CF card or Hda1 of the device.	The value is a string of 1 to 64 case-insensitive characters without question marks and spaces.
dn *dn-value*	Specifies the DN used by a device to request a certificate from an LDAP server.	The value is a string of 1 to 128 case-sensitive characters, with spaces supported.

Views

System view

Default Level

3: Management level

Usage Guidelines

Note the following points when configuring a device to download a CA certificate, local certificate, or CRL through LDAP, the sd1 of the device has enough space for accommodating the CA certificate, local certificate, or CRL file to avoid downloading failed.

Example

Configure a device to download local certificate **local.cer** from the LDAP server with the IP address 10.1.1.1, port number 3389, and LDAP version number 2 and set the DN of the certificate to **admin**.

```
<Huawei> system-view
[Huawei] pki ldap ip 10.1.1.1 port 3389 version 2 local.cer dn admin
```

19.17.98 pki match-rsa-key

Function

The **pki match-rsa-key** command configures a device to search for the RSA key pair associated with a specific certificate.

Format

pki match-rsa-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
certificate-filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to check the RSA key pair corresponding to a certificate. After configuration, the system searches for all the local RSA key pairs, compares them with the specified certificate and outputs the matched RSA key pair name once it is searched out.

Example

Configure a device to search for the RSA key pair that matches certificate file **local.cer**.

```
<Huawei> system-view
[Huawei] pki match-rsa-key certificate-filename local.cer
 Info: The file local.cer contains certificates 1.
 Info: Certificate 1 from file local.cer matches RSA key rsa2.key.
```

19.17.99 pki match-sm2-key

Function

The **pki match-sm2-key** command configures a device to search for the SM2 key pair associated with a specific certificate.

Format

pki match-sm2-key certificate-filename *file-name*

Parameters

Parameter	Description	Value
certificate-filename *file-name*	Specifies the name of a certificate file.	The value must be an existing certificate file name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command to check the SM2 key pair corresponding to a certificate. After configuration, the system searches for all the local SM2 key pairs, compares them with the specified certificate and outputs the matched SM2 key pair name once it is searched out.

Example

Configure a device to search for the SM2 key pair that matches certificate file **sm2.cer**.

```
<Huawei> system-view
[Huawei] pki match-sm2-key certificate-filename sm2.cer
 Info: The file sm2.cer contains certificates 1.
 Info: Certificate 1 from file sm2.cer matches SM2 key sm2.key.
```

19.17.100 pki ocsp response cache enable

Function

The **pki ocsp response cache enable** command enables a device to cache OCSP responses.

The **undo pki ocsp response cache enable** command disables a device from caching OCSP responses.

By default, the PKI OCSP response cache function is disabled.

Format

pki ocsp response cache enable

undo pki ocsp response cache enable

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

After you enable a PKI entity to cache OCSP responses, the PKI entity first searches its cache for the certificate revocation status. If the search fails, the PKI entity sends a request to the OCSP server. In addition, the device caches valid OCSP responses for subsequent query. The OCSP responses have a validity period. With OCSP response cache enabled, a PKI entity refreshes the cached OCSP responses every minute to clear expired OCSP responses.

Example

Enable the PKI OCSP response cache function.

```
<Huawei> system-view
[Huawei] pki ocsp response cache enable
```

19.17.101 pki ocsp response cache number

Function

The **pki ocsp response cache number** command sets the maximum number of OCSP responses that can be cached on a PKI entity.

The **undo pki ocsp response cache number** command restores the maximum number of OCSP responses that can be cached on a PKI entity to the default value.

By default, the maximum number of OCSP responses that can be cached on a PKI entity is 2.

Format

pki ocsp response cache number *number*

undo pki ocsp response cache number

Parameters

Parameter	Description	Value
number	Specifies the maximum number of OCSP responses that can be cached on a PKI entity.	The value is an integer that ranges from 1 to 9.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

A PKI entity caches valid OCSP responses for subsequent query. If the number of cached OCSP responses reaches the value specified by *number*, the PKI entity stops caching OCSP responses.

Example

Set the maximum number of OCSP responses that can be cached on a PKI entity to 3.

```
<Huawei> system-view
[Huawei] pki ocsp response cache number 3
```

19.17.102 pki ocsp response cache refresh interval

Function

The **pki ocsp response cache refresh interval** command sets the interval at which the OCSP response cache is refreshed.

The **undo pki ocsp response cache refresh interval** command restores the interval at which a PKI entity refreshes the OCSP response cache to the default value.

By default, the interval at which a PKI entity refreshes the OCSP response cache is 5 minutes.

Format

pki ocsp response cache refresh interval *interval*

undo pki ocsp response cache refresh interval

Parameters

Parameter	Description	Value
interval	Specifies the interval at which the OCSP response cache is refreshed.	The value is an integer that ranges from 1 to 1440, in minutes. The default value is 5.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

A PKI entity refreshes the OCSP response cache periodically and deletes the OCSP responses that have expired based on the *interval* value.

Example

Set the interval at which the OCSP response cache is refreshed to 30 minutes.

```
<Huawei> system-view
[Huawei] pki ocsp response cache refresh interval 30
```

19.17.103 pki realm (system view)

Function

The **pki realm** command creates a PKI realm and displays the PKI realm view, or displays the view of an existing PKI realm.

The **undo pki realm** command deletes a PKI realm.

By default, the device has a PKI realm named **default**. This realm can only be modified but cannot be deleted.

Format

pki realm *realm-name*

undo pki realm *realm-name*

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI realm.	The value is a string of 1 to 63 case-insensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

A PKI realm is a set of identity information required when a PKI entity enrolls a certificate.

Precautions

A PKI realm configured on a device is unavailable to certificate authorities (CAs) or other devices.

When a certificate is requested using a PKI realm, the system names the certificate file *PKI realm name*_**local.cer**. Therefore, if you will use a created PKI realm to request certificates, ensure that the PKI realm name length is shorter than 50 characters, because a certificate file with a name longer than 64 characters cannot be saved on a storage device.

Example

Create a PKI realm **abc**.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc]
```

Related Topics

19.17.40 display pki realm

19.17.104 pki release-certificate peer

Function

The **pki release-certificate peer** command releases a certificate of the remote device.

Format

pki release-certificate peer { **name** *peer-name* | **all** }

Parameters

Parameter	Description	Value
name *peer-name*	Specifies the name of peer certificate to be released.	The value must be an existing peer certificate file name.
all	Releases all certificates of the remote device.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the specified certificate of the remote device is not required, run the **pki release-certificate peer** command to release the certificate of the remote device.

Before using this command, run the **19.17.39 display pki peer-certificate** command to view the certificate information of the remote device.

Prerequisites

The **19.17.92 pki import-certificate peer** command has been used to import the certificate of the remote device.

Example

Release the certificate **huawei** of the remote device.

```
<Huawei> system-view
[Huawei] pki release-certificate peer name huawei
 Info: Succeeded in releasing the peer certificate.
```

Related Topics

19.17.92 pki import-certificate peer

19.17.39 display pki peer-certificate

19.17.105 pki rsa built-in-ca

Function

The **pki rsa built-in-ca** command creates, overwrites, or destroys the RSA key pair in an SSL decryption certificate.

Format

pki rsa built-in-ca *key-name* { **create** [**exportable**] | **destroy** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair in an SSL decryption certificate.	The value is a string of 1 to 64 case-sensitive characters without question marks and spaces. If the character string is quoted by double quotation marks, it can contain spaces and question marks.
create	Specifies the created RSA key pair of the SSL decryption certificate.	-
exportable	Specifies the created RSA key pair as exportable.	-
destroy	Specifies the destroyed RSA key pair of the SSL decryption certificate.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When the device uses the SSL decryption certificate to perform the proxy function for the SSL connection, the certificate must contain a public key. Run this command to create the RSA key pair of the SSL decryption certificate.

If the RSA key pair is referenced by the certificate and has been imported to the memory, you cannot overwrite or destroy the pair directly. To overwrite or destroy the RSA key pair, you can run the **19.17.76 pki delete-certificate built-in-ca** command to delete the SSL decryption certificate from the memory first.

When creating or overwriting the RSA key pair, you must enter the number of bits of the RSA key pair. The default value is 2048.

Precautions

The name of an RSA key pair cannot exceed 50 characters. Because when an RSA key pair is imported, if the certificate is imported at the same time, the PKI system adds **_builtinca.cer** after the name of the RSA key pair to generate a new certificate file name, and saves it to the storage component. If the name exceeds 50 characters, the total number of characters exceeds 64, and the certificate file cannot be saved to the storage component.

When creating the key pair, the system prompts the user to enter the number of bits of the RSA key pair. The longer the key pair, the harder it is to crack, and the

 Copyright © Huawei Technologies Co., Ltd.

more secure but slow the encryption algorithm. It is recommended that the number of bits of the RSA key pair exceed 2048; otherwise, it has security risks.

Example

Create an RSA key pair **rsakey**.

```
<Huawei> system-view
[Huawei] pki rsa built-in-ca rsakey create
 Info: The name of the new key-pair will be: rsakey
 The size of the public key ranges from 2048 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
........++++++
........++++++
```

Related Topics

19.17.76 pki delete-certificate built-in-ca

19.17.41 display pki rsa built-in-ca public

19.17.106 pki rsa local-key-pair create

Function

The **pki rsa local-key-pair create** command creates the specified RSA key pair.

Format

pki rsa local-key-pair create *key-name* [**modulus** *modulus-size*] [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be created.	The value is a string of 1 to 64 case-sensitive characters without question marks (?) and spaces. If the string is enclosed in double quotation marks (" "), the string can contain question marks (?) and spaces; however, if the string contains spaces, it cannot contain double quotation marks (").
modulus *modulus-size*	Specifies the size of the RSK key pair.	The value is an integer that ranges from: • AR100&AR120&AR150&AR160&AR200 series: 2048 to 2048. The default value is 2048. • AR1200&AR2200&AR3200&AR3600 series: 2048 to 4096. The default value is 2048.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
exportable	Indicates that the new RSA key pair can be exported from the device.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When a PKI entity requests a certificate from the CA, the certificate enrollment request that it sends contains information such as the public key. Run this command to create the RSA key pair for the certificate request.

NOTE

Windows Server 2003 has a low processing performance. For the device to connect to a Windows Server 2003, the device cannot have too many entities configured or use a large-sized key pair.

Precautions

When creating the key pair, the system prompts the user to enter the number of bits of the RSA key pair. The longer the key pair, the harder it is to crack, and the more secure but slow the encryption algorithm. It is recommended that the number of bits of the RSA key pair exceed 2048; otherwise, it has security risks.

The name of an RSA key pair cannot exceed 50 characters. Because when an RSA key pair is imported, if the certificate is imported at the same time, the PKI system adds **_localx.cer** after the name of the RSA key pair to generate a new certificate file name, and saves it to the storage component. If the name exceeds 50 characters, the total number of characters exceeds 64, and the certificate file cannot be saved to the storage component.

The RSA key pair referenced by PKI realms cannot be overwritten. They can be overwritten only after the reference relationship is removed.

If the name of the new RSA key pair is the same as that of a pair on the device, the system prompts the user to decide whether to overwrite the existing pair.

Example

Create 2048-bit RSA key pair **test**.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
```

```
Info: The name of the new key-pair will be: test
The size of the public key ranges from 2048 to 4096.
Input the bits in the modules:2048
Generating key-pairs...
......+++
.......+++
```

Related Topics

19.17.42 display pki rsa local-key-pair

19.17.107 pki rsa local-key-pair destroy

Function

The **pki rsa local-key-pair destroy** command deletes the specified RSA key pair.

Format

pki rsa local-key-pair destroy *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair to be deleted.	The value must be the name of an existing key pair.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It is recommended that you run this command to destroy the specified RSA key pair if it is leaked, damaged, unused, or lost.

After this command is executed, the specified RSA key pair is deleted from the active device and the standby device.

Prerequisites

The RSA key pair has been created using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

The RSA key pair in the creation process cannot be deleted.

 Copyright © Huawei Technologies Co., Ltd.

The RSA key pair referenced by a PKI realm or CMP session cannot be deleted. They can be deleted only after the reference relationship is removed.

Example

Delete the RSA key pair **test**.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.....+++
.........................+++
[Huawei] pki rsa local-key-pair destroy test
 Warning: The name of the key pair to be deleted is test.
 Are you sure you want to delete the key pair? [y/n]:y
 Info: Delete RSA key pair success.
```

Related Topics

19.17.95 pki import rsa-key-pair

19.17.106 pki rsa local-key-pair create

19.17.108 pki set-certificate expire-prewarning

Function

The **pki set-certificate expire-prewarning** command sets the expiration warning date for the local certificate and the CA certificate in the memory.

The **undo pki set-certificate expire-prewarning** command restores the expiration warning date for the local certificate and the CA certificate in the memory to the default value.

By default, the expiration warning date for the local certificate and the CA certificate in the memory is seven days.

Format

pki set-certificate expire-prewarning *day*

undo pki set-certificate expire-prewarning

Parameters

Parameter	Description	Value
day	Specifies the expiration warning date.	The value is an integer that ranges from 7 to 180. By default, the value is 7.

Views

System view

Default Level

3: Management level

Usage Guidelines

After this command is executed, you will be prompted the expiration of a certificate in advance. If the system detects that a certificate in the memory is to expire in less than *day*, the device sends an expiration warning to the user.

Example

Set the expiration warning date for the local certificate and the CA certificate in the memory as 30 days.

```
<Huawei> system-view
[Huawei] pki set-certificate expire-prewarning 30
```

19.17.109 pki sm2 local-key-pair create

Function

The **pki sm2 local-key-pair create** command creates an SM2 key pair.

Format

pki sm2 local-key-pair create *key-name* [**exportable**]

Parameters

Parameter	Description	Value
key-name	Specifies the name of the created SM2 key pair.	The value is a string of 1 to 64 case-sensitive characters without question marks (?) and spaces. If the string is enclosed in double quotation marks (" "), the string can contain question marks (?) and spaces; however, if the string contains spaces, it cannot contain double quotation marks (").
exportable	Specifies the created SM2 key pair as exportable.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Run this command when the certificate needs to use the SM2 key pair.

Example

Create the SM2 key pair named abc.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create abc
 Info: The name of the new key-pair will be: abc
 Generating key-pairs...
```

Related Topics

19.17.43 display pki sm2 local-key-pair public (System view)

19.17.110 pki sm2 local-key-pair destroy

Function

The **pki sm2 local-key-pair destroy** command destroys an SM2 key pair.

Format

pki sm2 local-key-pair destroy *key-name*

Parameters

Parameter	Description	Value
key-name	Specifies the name of an SM2 key pair that you want to destroy.	The value must be an existing SM2 key pair name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

It is recommended that you run this command to destroy the specified SM2 key pair if it is leaked, damaged, unused or lost.

Prerequisites

The SM2 key pair has been created using the **19.17.109 pki sm2 local-key-pair create** command or the SM2 key pair has been imported to the memory using the **19.17.96 pki import sm2-key-pair** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Destroy the SM2 key pair named abc.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create abc
 Info: The name of the new key-pair will be: abc
 Generating key-pairs...
[Huawei] pki sm2 local-key-pair destroy abc
 Warning: The name of the key pair to be deleted is abc.
 Are you sure you want to delete the key pair? [y/n]:y
 Info: Succeeded in destroying SM2 key pair.
```

Related Topics

19.17.109 pki sm2 local-key-pair create

19.17.96 pki import sm2-key-pair

19.17.111 pki validate ocsp-server-certificate enable

Function

The **pki validate ocsp-server-certificate enable** command enables the function that uses the OCSP server certificate to verify OCSP server packets.

The **undo pki validate ocsp-server-certificate enable** command disables the function that uses the OCSP server certificate to verify OCSP server packets.

By default, the function that uses the OCSP server certificate to verify OCSP server packets is disabled.

Format

pki validate ocsp-server-certificate enable

undo pki validate ocsp-server-certificate enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

For security purposes, you are advised to enable the function that uses the OCSP server certificate to verify OCSP server packets. If OCSP server packets fail the verification, the device discards these packets.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If the imported OCSP server certificate is not the correct one, OCSP server packets fail the verification, causing the local certificate to become unavailable. To prevent this problem, import the correct OCSP server certificate. If no OCSP server certificate can be obtained, run the **undo pki validate ocsp-server-certificate enable** command to disable the function that uses the OCSP server certificate to verify OCSP server packets.

Example

Enable the function that uses the OCSP server certificate to verify OCSP server packets.

```
<Huawei> system-view
[Huawei] pki validate ocsp-server-certificate enable
```

19.17.112 pki validate-certificate

Function

The **pki validate-certificate** command allows you to verify the validity of a CA certificate or a local certificate.

Format

pki validate-certificate { **ca** | **local** } **realm** *realm-name*

Parameters

Parameter	Description	Value
ca	Checks validity of the CA certificate.	-
local	Checks validity of the local certificate.	-
realm *realm-name*	Specifies the PKI realm name of a certificate to be checked.	The value must be an existing PKI realm name.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an end entity verifies a peer certificate, it checks the status of the peer certificate. For example, the end entity checks whether the peer certificate has expired and whether the certificate is in a CRL.

To verify the validity of a CA certificate or a local certificate, run the **pki validate-certificate** command.

Prerequisites

A PKI realm has been configured using the **pki realm (system view)** command.

Precautions

The **pki validate-certificate ca** command allows you to verify only the root CA certificate, but not subordinate CA certificates. When multiple CA certificates are imported on a device, you can use only the **pki validate-certificate local** command to verify the validity of subordinate certificates.

Example

Configure the device to check validity of the local certificate using CRL.

```
<Huawei> system-view
[Huawei] pki realm abc
[Huawei-pki-realm-abc] certificate-check crl
[Huawei-pki-realm-abc] quit
[Huawei] pki validate-certificate local realm abc
```

19.17.113 reset pki cmp statistics

Function

The **reset pki cmp statistics** command clears the statistics on CMP sessions.

Format

reset pki cmp statistics [**session** *session-name*]

Parameters

Parameter	Description	Value
session *session-name*	Specifies the name of a CMP session.	The value must be an existing CMP session name.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

If a CMP session is specified, the statistics of the session is cleared. If no CMP session is specified, the statistics of all sessions is cleared.

Example

Clear statistics on CMP session **test**.

```
<Huawei> reset pki cmp statistics session test
```

19.17.114 reset pki ocsp response cache

Function

The **reset pki ocsp response cache** command resets an OCSP response cache.

Format

reset pki ocsp response cache

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

The PKI entity caches valid OCSP responses for future searches. If the number of cached OCSP responses reaches the maximum value, no more OCSP responses can be cached. To ensure that the latest OCSP responses can be cached, you can run this command to clear the OCSP response cache first.

Example

Reset an OCSP response cache.

```
<Huawei> reset pki ocsp response cache
```

19.17.115 reset pki ocsp server down-information

Function

The **reset pki ocsp server down-information** command clears the DOWN status information of the OCSP server recorded on the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

reset pki ocsp server down-information [**url** [**esc**] *url-addr*]

Parameters

Parameter	Description	Value
url [**esc**] *url-addr*	Specifies the OCSP server's URL address. If no URL address is specified, clear the DOWN status information on all OCSP servers. If the **esc** parameter is specified, the URL address in ASCII format is supported.	The value is a string starting with http:// and consisting of 1 to 128 case-sensitive characters without spaces.

Views

User view

Default Level

3: Management level

Usage Guidelines

There is a mechanism to determine whether the OCSP server is down. When the OCSP server corresponding to a URL cannot be accessed, the server status is set to DOWN. In this case, the device will not send OCSP requests to the URL for 10 minutes.

However, this mechanism may falsely set the state of a transiently disconnected server to DOWN. Using this command, the user can manually clear the falsely reported DOWN state of the OCSP server so that the device can send OCSP requests to the server.

The keyword **esc** supports the entering of URLs that include the question mark (?) in the ASCII code. The URL must be in **\x3f** format, and **3f** is the hexadecimal ASCII code for the question mark (?). For example, if a user wants to enter **http://***.com?page1**, the URL is **http://***.com\x3fpage1**. If a user wants to enter **http://www.***.com?page1\x3f** that includes both a question mark (?) and **\x3f**, the URL is **http://www.***.com\x3fpage1\\x3f**.

Example

Clear the OCSP server DOWN information of the specified URL.

```
<Huawei> reset pki ocsp server down-information
```

19.17.116 rsa local-key-pair

Function

The **rsa local-key-pair** command configures the RSA key pair used to request a certificate using the SCEP or in an offline mode.

The **undo rsa local-key-pair** command deletes the RSA key pair used to request a certificate using the SCEP or in an offline mode.

By default, the system does not configure the RSA key pair used to request a certificate using the SCEP or in an offline mode.

Format

rsa local-key-pair *key-name*

undo rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the RSA key pair.	The value must be an existing RSA key pair name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PKI entity that requests a certificate from the CA using the SCEP or in offline PKCS#10 mode must contain a public key. Run this command to configure the RSA key pair.

Prerequisites

The RSA key pair for certificate application has been created using the **19.17.106 pki rsa local-key-pair create** command or the RSA key pair has been imported to the memory using the **19.17.95 pki import rsa-key-pair** command.

Precautions

An RSA key pair can be specified to only one PKI.

Example

Configure the RSA key pair that is referenced by the PKI realm **test**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] pki rsa local-key-pair create test
 Info: The name of the new key-pair will be: test
 The size of the public key ranges from 512 to 4096.
 Input the bits in the modules:2048
 Generating key-pairs...
.......................+++
.......................................................................
........+++
[Huawei] pki realm test
[Huawei-pki-realm-test] rsa local-key-pair test
```

Related Topics

19.17.106 pki rsa local-key-pair create
19.17.95 pki import rsa-key-pair

19.17.117 serial-number

Function

The **serial-number** command adds the serial number of a device to the PKI entity.

The **undo serial-number** command restores the default setting.

By default, the serial number of a device is not added to the PKI entity.

Format

serial-number

undo serial-number

Parameters

None

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity include the identity information of the PKI entity. The CA identifies a certificate applicant based on identity information provided by a PKI entity. To further identify the applicant, add the serial number of the device to the PKI entity.

After the serial number of the device is added to a PKI entity, the certificate request packet sent by the device to the CA server carries this serial number. After receiving the certificate request packet, the CA server verifies the packet. For each valid packet, the CA server generates a digital certificate carrying the device serial number.

 Copyright © Huawei Technologies Co., Ltd.

Example

Add the serial number of the device to a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] serial-number
```

Related Topics

19.17.35 display pki entity

19.17.118 sm2 local-key-pair

Function

The **sm2 local-key-pair** command configures the SM2 key pair used to request a certificate in an offline mode.

The **undo sm2 local-key-pair** command deletes the SM2 key pair used to request a certificate in an offline mode.

By default, the system does not configure the SM2 key pair used to request a certificate in an offline mode.

Format

sm2 local-key-pair *key-name*

undo rsa local-key-pair

Parameters

Parameter	Description	Value
key-name	Specifies the name of the SM2 key pair.	The value must be an existing SM2 key pair name.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The PKI entity that requests a certificate from the CA in offline PKCS#10 mode must contain a public key. Run this command to configure the SM2 key pair.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The SM2 key pair for certificate application has been created using the **19.17.109 pki sm2 local-key-pair create** command or the SM2 key pair has been imported to the memory using the **19.17.96 pki import sm2-key-pair** command.

Precautions

An SM2 key pair can be specified to only one PKI.

Example

Configure the SM2 key pair that is referenced by the PKI realm **test**.

```
<Huawei> system-view
[Huawei] pki sm2 local-key-pair create test
 Info: The name of the new key-pair will be: test
 Generating key-pairs...
[Huawei] pki realm test
[Huawei-pki-realm-test] sm2 local-key-pair test
```

Related Topics

19.17.109 pki sm2 local-key-pair create

19.17.96 pki import sm2-key-pair

19.17.40 display pki realm

19.17.119 source interface

Function

The **source interface** command configures the source interface used in TCP connection setup.

The **undo source interface** command restores the default source interface used in TCP connection setup.

By default, the device uses the outbound interface as the source interface for TCP connection setup.

Format

source interface *interface-type interface-number*

undo source interface

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies an interface's IP address as the source IP address used in TCP connection setup. ● *interface-type* indicates the type of the interface. ● *interface-number* indicates the number of the interface.	-

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **source interface** command specifies the source interface for establishing a connection between the device and the Simple Certificate Enrollment Protocol (SCEP) or Online Certificate Status Protocol (OCSP) server. This interface IP address is the source IP address of the TCP connection.

In the multi-output scenario, if the interfaces for sending and receiving a TCP packet are different, the IP address in the received TCP packet is different from the IP address of the receiving interface. Then the TCP packet is dropped, and the TCP connection is torn down. In this situation, you can run this command to specify the loopback interface address.

Precautions

Ensure that the interface is at Layer 3 and has an IP address configured.

Example

Configure the source interface used in TCP connection setup to Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip address 10.136.2.25 24
[Huawei-Ethernet2/0/0] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] source interface ethernet 2/0/0
```

19.17.120 state (PKI entity view)

Function

The **state** command configures a state or province name for an entity.

The **undo state** command deletes the configuration.

By default, no state or province name is configured for a PKI entity.

Format

state *state-name*

undo state

Parameters

Parameter	Description	Value
state-name	Specifies the state or province name of an entity.	The value is a string of 1 to 32 case-sensitive characters, including letters, numerals, apostrophes ('), equal signs (=), parentheses (), plus signs (+), commas (,), minus signs (-), periods (.), slashes (/), colons (:), and spaces.

Views

PKI entity view

Default Level

2: Configuration level

Usage Guidelines

The parameters of a PKI entity contain the identity information of the entity. The CA identifies a certificate applicant based on identity information provided by the entity. To facilitate applicant identification, configure a state or province name for a PKI entity.

After the state or province name is configured for a PKI entity, the certificate request packet sent by the device to the CA server contains this province name. The CA server verifies every received certificate request packet. For each valid packet, the CA server generates a digital certificate carrying the state or provision name of the PKI entity.

Example

Configure the province name to **Jiangsu** for a PKI entity.

```
<Huawei> system-view
[Huawei] pki entity entity1
[Huawei-pki-entity-entity1] state Jiangsu
```

Related Topics

19.17.35 display pki entity

19.17.121 undo pki cmp poll-request session

Function

The **undo pki cmp poll-request session** command cancels CMP polling requests.

Format

undo pki cmp poll-request session *session-name*

Parameters

Parameter	Description	Value
session-name	Specifies the name of the CMP session.	The value must be an existing CMP session name.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the server cannot deliver the results immediately after the client initiates certificate-related requests, the server requires the client to send the requests in polling mode until the server deliver the final result. The process duration varies with the actual situation. To cancel the process, run the command. In that, the certificate-related request is also canceled.

Prerequisites

A CMP session has been created using the **19.17.73 pki cmp session** command.

Example

Cancel CMP polling requests.

```
<Huawei> system-view
[Huawei] pki cmp session test
[Huawei-pki-cmp-session-test] quit
[Huawei] undo pki cmp poll-request session test
```

Related Topics

19.17.73 pki cmp session

 Copyright © Huawei Technologies Co., Ltd.

19.17.122 validate time disable

Function

The **validate time disable** command ignores time check in PKI certificate authentication.

The **undo validate time disable** command restores the default configuration.

By default, time is checked in PKI certificate authentication.

NOTE

Only AR100&AR120&AR150 series, AR161, AR161W, AR161G-L, AR161G-Lc, AR161G-U, AR169, AR169G-L, AR169CVW, AR169CVW-4B4S among the AR160 series support this command.

Format

validate time disable

undo validate time disable

Parameters

None

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device verifies the time during PKI certificate verification. If the time does not match, the PKI certificate verification fails. If the device does not support the clock synchronization function and restarts due to causes such as power-off, the system time is restored to the factory setting and an error occurs in PKI certificate verification. To avoid this problem, the administrator can run this command to disable the device from verifying the time during PKI certificate verification.

Precautions

After the **validate time disable** is run, the device will not generate certificate expiration logs.

Example

Ignore time check in PKI certificate authentication.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] PKI realm test
[Huawei-pki-realm-test] validate time disable
```

19.17.123 vpn-instance

Function

The **vpn-instance** command adds a PKI to a specified VPN.

The **undo vpn-instance** command unbinds a PKI from a specified VPN.

By default, a PKI does not belong to any VPN.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance *vpn-instance-name*

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the name of a VPN instance.	The value must be the name of an existing VPN instance.

Views

PKI realm view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To obtain and verify certificates, the device needs to communicate with the CA or SCEP server. When the CA or SECP server is in a VPN, add the PKI to the specified VPN.

Prerequisites

1. A VPN instance has been created using the **12.9.35 ip vpn-instance** command.
2. The RD has been configured using the **12.9.50 route-distinguisher** command.

Example

Add the PKI to the VPN named **vrf1**.

```
<Huawei> system-view
[Huawei] ip vpn-instance vrf1
[Huawei-vpn-instance-vrf1] route-distinguisher 22:1
[Huawei-vpn-instance-vrf1-af-ipv4] quit
[Huawei-vpn-instance-vrf1] quit
[Huawei] pki realm abc
[Huawei-pki-realm-abc] vpn-instance vrf1
```

Related Topics

12.9.35 ip vpn-instance

12.9.50 route-distinguisher

19.18 SSL Configuration Commands

19.18.1 ciphersuite

Function

The **ciphersuite** command configures cipher suites in a server SSL policy.

The **undo ciphersuite** command restores the default configuration.

By default, a server SSL policy supports the cipher suites: **ecdhe_rsa_aes128_gcm_sha256**, **ecdhe_rsa_aes256_gcm_sha384**, **rsa_aes_128_sha256**, and **rsa_aes_256_sha256**.

Format

ciphersuite { **rsa_3des_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_sha256** | **rsa_aes_256_sha256** | **rsa_aes128_ccm** | **rsa_aes128_gcm_sha256** | **rsa_aes256_ccm** | **rsa_aes256_gcm_sha384** | **ecdhe_rsa_aes128_gcm_sha256** | **ecdhe_rsa_aes256_gcm_sha384** } *

undo ciphersuite

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
rsa_3des_cbc_sha	Indicates the **rsa_3des_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 3DES_CBC algorithm to encrypt data, and the SHA algorithm to compute the MAC. **NOTE** RSA: Rivest-Shamir-Adleman DES: Data Encryption Standard CBC: Cipher Block Chaining SHA: Secure Hash Algorithm	-
rsa_aes_128_cbc_sha	Indicates the **rsa_aes_128_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA algorithm to compute the message authentication code (MAC). **NOTE** AES: Advanced Encryption Standard	-
rsa_aes_128_sha256	Indicates the **rsa_aes_128_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes_256_sha256	Indicates the **rsa_aes_256_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
rsa_aes128_ccm	Indicates the **rsa_aes128_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 128-bit AES_CCM to encrypt data. **NOTE** CCM: Counter with CBC-MAC	-
rsa_aes128_gcm_sha256	Indicates the **rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC. **NOTE** GCM: Galois/Counter Mode	-
rsa_aes256_ccm	Indicates the **rsa_aes256_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 256-bit AES_CCM to encrypt data.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes256_gcm_sha384	Indicates the **rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-
ecdhe_rsa_aes128_gcm_sha256	Indicates the **ecdhe_rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC. **NOTE** GCM: Galois/Counter Mode ECDHE: Elliptic Curve Diffie-Hellman with Ephemeral keys	-
ecdhe_rsa_aes256_gcm_sha384	Indicates the **ecdhe_rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-

Views

Server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A cipher suite consists of a data encryption algorithm, a key exchange algorithm, and a MAC algorithm. During an SSL handshake, an SSL client sends a Client Hello message to notify an SSL server of the SSL protocol version and cipher suites that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to notify the client.

The **ciphersuite** command configures the cipher suite that the Router can use when it functions as an SSL server.

Configuration Impact

To ensure high security, you are not advised to configure the cipher suite supported by the server SSL policy to **rsa_3des_cbc_sha** and **rsa_aes_128_cbc_sha**.

Using the **ecdhe_rsa_aes128_gcm_sha256** or **ecdhe_rsa_aes256_gcm_sha384** algorithm will affect the SSL server performance.

Example

Configure a server SSL policy to use the **rsa_aes_256_sha256** cipher suite.

```
<Huawei> system-view
[Huawei] ssl policy users type server
[Huawei-ssl-policy-users] ciphersuite rsa_aes_256_sha256
```

Related Topics

19.18.10 ssl policy

19.18.2 display ssl connection statistics

Function

The **display ssl connection statistics** command displays statistics on SSL connections.

Format

display ssl connection statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a device sets up a connection with an SSL server or client, the device automatically counts and records the SSL connection.

This command displays the maximum number of SSL connections within a certain period so that the administrator can perform SSL fault diagnosis and troubleshooting quickly.

Example

View statistics on SSL connections.

```
<Huawei> display ssl connection statistics
-------------------------------------------------------------------------------
Maximum of total connections in history          :   100
Begin time of total connections                  :  2013-09-26 12:19:11
Maximum time of total connections                :   2013-09-26 12:19:11
-------------------------------------------------------------------------------
```

Table 19-175 Description of the display ssl connection statistics command output

Item	Description
Maximum of total connections in history	Maximum number of SSL connections in history.
Begin time of total connections	Time when the system starts to count SSL connections.
Maximum time of total connections	Time when the system records the maximum number of SSL connections.

Related Topics

19.18.7 reset ssl connection statistics

19.18.3 display ssl policy

Function

Using the **display ssl policy** command, you can view information about an SSL policy.

Format

display ssl policy [*policy-name*]

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy. If this parameter is not specified, the system displays information about all SSL policies.	The SSL policy name must already exist.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays information about all SSL policies or a specified SSL policy.

Example

Display information about all SSL policies.

```
<Huawei> display ssl policy
Policy number: 2
  ---------------------------------------------------------------------------
  policy ID   policy name                    policy type     bind number
  ---------------------------------------------------------------------------
  1           client-users                   Client         0
  2           server-users                    Server         0
  ---------------------------------------------------------------------------
```

Display information about the client SSL policy **client-users**.

```
<Huawei> display ssl policy client-users
  ---------------------------------------------------------------------------
  Policy name                        :   client-users
  Policy ID                        :   2
  Policy type                        :   Client
  Cipher suite                       :   rsa_aes128_sha256
                                     rsa_aes256_sha256
  PKI realm                          :   -
  Version                          :   tls1.2
  Server verify                      :   1
  CA certificate chain load status       :   unloaded
  CA certificate num                 :   0
  Local certificate load status          :   unloaded
  SSL renegotiation status               :   enable
  Bind number                      :   0
  SSL connection number                  :   0
---------------------------------------------------------------------------
```

Display information about server SSL policy **server-users**.

```
<Huawei> display ssl policy server-users
  ---------------------------------------------------------------------------
  Policy name                        :   server-users
```

```
Policy ID                        :  3
Policy type                       :  Server
Cipher suite                      :  rsa_aes128_sha256
                                 rsa_aes256_sha256
PKI realm                         :  -
Version                          :  tls1.2
Cache number                        :  128
Time out(second)                    :  3600
Local certificate load status        :  unloaded
CA certificate chain load status      :  unloaded
SSL renegotiation status             :  enable
Bind number                       :  0
SSL connection number                :  0
--------------------------------------------------------------------------------
```

Table 19-176 Description of the display ssl policy command output

Item	Description
Policy name	Name of an SSL policy. To configure an SSL policy, run the **ssl policy** command.
Policy ID	ID of an SSL policy.
Policy type	Type of an SSL policy: client SSL policy or server SSL policy. To configure an SSL policy, run the **ssl policy** command.
Cipher suite	Cipher suite used by the SSL policy. • To configure a client SSL policy, run the **19.18.5 prefer-ciphersuite** command. • To configure a server SSL policy, run the **19.18.1 ciphersuite** command.
PKI realm	PKI domain used by the SSL policy. To configure the PKI domain, run the **19.18.4 pki-realm** command.
Version	Version of the SSL protocol used by the client SSL policy. • ssl3.0 • tls1.0 • tls1.1 • tls1.12 To specify the SSL version, run the **19.18.12 version (Client SSL policy view)** command.
Server verify	Whether the SSL client is enabled to authenticate an SSL server. • 1: enabled • 0: disabled

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CA certificate chain load status	Whether the CA certificate chain has been loaded to the SSL client. • loaded: The certificate chain has been loaded to the SSL client. • unloaded: The certificate has not been loaded to the SSL client. • got but unloaded: The SSL client has obtained the certificate chain but has not loaded it.
CA certificate num	Number of CA certificates in the certificate chain.
Local certificate load status	Local certificate loading status. **loaded** indicates that the certificate has been loaded. **unloaded** indicates that the certificate is not loaded. **pending** indicates that the certificate is being generated.
SSL renegotiation status	SSL renegotiation status. • enable • disable
Bind number	Whether an SSL policy has been applied to an application layer protocol such as HTTP. • 1: yes • 0: no To apply an SSL policy to HTTP, run the **19.19.4 http secure-server ssl-policy** command.
SSL connection number	Number of SSL connections established by using an SSL policy.
Cache number	Maximum number of sessions that can be saved on the SSL server. To configure a session, run the **session** command.
Time out(second)	Timeout period of a saved session. To configure a session, run the **session** command.

19.18.4 pki-realm

Function

Using the **pki-realm** command, you can specify a public key infrastructure (PKI) domain in an SSL policy.

Using the **undo pki-realm** command, you can delete the PKI domain from the SSL policy.

By default, the PKI domain **default** exists on the device. This domain can be modified, but cannot be deleted.

Format

pki-realm *realm-name*

undo pki-realm

Parameters

Parameter	Description	Value
realm-name	Specifies the name of a PKI domain.	The PKI domain name must already exist.

Views

Client SSL policy view, server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command specifies a PKI domain in an SSL policy. A PKI domain has different functions when it is specified in a server SSL policy and a client SSL policy:

- After a PKI domain is specified in the server SSL policy view, the Router functioning as an SSL server obtains a digital certificate from the certificate authority (CA) specified in the PKI domain. Then SSL clients authenticate the Router by checking the digital certificate.
- After a PKI domain is specified in the client SSL policy view, the Router functioning as an SSL client obtains a CA certificate chain from the CA specified in the PKI domain. If SSL server authentication is enabled by using the **server-verify enable** command, the Router authenticates the SSL server using the CA certificate chain.

Prerequisites

A PKI domain has been created.

Precautions

When the SSL policy is referenced by another configuration, you cannot modify the configuration using the **pki-realm** command.

When functioning as an SSL server, the Router is authenticated by SSL clients, but it cannot authenticate SSL clients.

When functioning as an SSL client, the Router does not allow SSL servers to authenticate it, but it can authenticate SSL servers.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a client SSL policy to use the PKI domain **client-realm**.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] pki-realm client-realm
```

Related Topics

19.18.10 ssl policy

19.18.8 server-verify enable

19.17.103 pki realm (system view)

19.18.5 prefer-ciphersuite

Function

The **prefer-ciphersuite** command configures cipher suites in a client SSL policy.

The **undo prefer-ciphersuite** command restores the default configuration.

By default, a client SSL policy uses the cipher suites: **ecdhe_rsa_aes128_gcm_sha256**, **ecdhe_rsa_aes256_gcm_sha384**, **rsa_aes_128_sha256**, and **rsa_aes_256_sha256**.

Format

prefer-ciphersuite { **rsa_3des_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_128_sha256** | **rsa_aes_256_sha256** | **rsa_aes128_ccm** | **rsa_aes128_gcm_sha256** | **rsa_aes256_ccm** | **rsa_aes256_gcm_sha384** | **ecdhe_rsa_aes128_gcm_sha256** | **ecdhe_rsa_aes256_gcm_sha384** } *

undo prefer-ciphersuite

Parameters

Parameter	Description	Value
rsa_3des_cbc_sha	Indicates the **rsa_3des_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 3DES_CBC algorithm to encrypt data, and the SHA algorithm to compute the MAC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes_128_cbc_sha	Indicates the **rsa_aes_128_cbc_sha** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA algorithm to compute the message authentication code (MAC).	-
rsa_aes_128_sha256	Indicates the **rsa_aes_128_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
rsa_aes_256_sha256	Indicates the **rsa_aes_256_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_CBC to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
rsa_aes128_ccm	Indicates the **rsa_aes128_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 128-bit AES_CCM to encrypt data.	-
rsa_aes128_gcm_sha256	Indicates the **rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rsa_aes256_ccm	Indicates the **rsa_aes256_ccm** cipher suite. This cipher suite uses the RSA algorithm to compute the key and the 256-bit AES_CCM to encrypt data.	-
rsa_aes256_gcm_sha384	Indicates the **rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-
ecdhe_rsa_aes128_gcm_sha256	Indicates the **ecdhe_rsa_aes128_gcm_sha256** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 128-bit AES_GCM to encrypt data, and the SHA2-256 algorithm to compute the MAC.	-
ecdhe_rsa_aes256_gcm_sha384	Indicates the **ecdhe_rsa_aes256_gcm_sha384** cipher suite. This cipher suite uses the ECDHE RSA algorithm to compute the key, the 256-bit AES_GCM to encrypt data, and the SHA2-384 algorithm to compute the MAC.	-

Views

Client SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A cipher suite consists of a data encryption algorithm, a key exchange algorithm, and a MAC algorithm. During an SSL handshake, an SSL client sends a Client Hello message to notify an SSL server of the SSL protocol version and cipher suites that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to notify the client.

The **prefer-ciphersuite** command configures the cipher suite that the Router can use when it functions as an SSL client.

Configuration Impact

If you run the **prefer-ciphersuite** command multiple times in the same client SSL policy view, only the latest configuration takes effect.

Precautions

To ensure high security, you are not advised to configure the cipher suite used by the client SSL policy to **rsa_3des_cbc_sha** and **rsa_aes_128_cbc_sha**.

Ensure that the cipher suite specified in this command is supported by the SSL server. Before running this command, check the cipher suites that the SSL server supports.

Example

Configure a client SSL policy to use the **rsa_aes_256_sha256** cipher suite.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] prefer-ciphersuite rsa_aes_256_sha256
```

Related Topics

19.18.10 ssl policy
19.18.8 server-verify enable
19.18.1 ciphersuite

19.18.6 renegotiation enable

Function

The **renegotiation enable** command enables re-negotiation of an SSL connection.

The **undo renegotiation enable** command disables re-negotiation of an SSL connection.

By default, re-negotiation of an SSL connection is enabled.

Format

renegotiation enable

undo renegotiation enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A client and a server negotiate session parameters by using the SSL handshake protocol to verify the identities of the two parties and negotiate the private key and cipher suite. Asymmetric cryptography is used to encrypt keys and authenticate peer identities when session parameters are being negotiated during the handshake. The computation workload is heavy, consuming a lot of system resources.

If an attacker sends re-negotiation requests continuously, the device consumes a lot of system resources processing these requests. To process re-negotiation requests, a server consumes 15 times the resources that is consumed by a client. This prevents the server from receiving requests from authorized users or suspends the server, affecting normal service operations.

You can run this command to disable re-negotiation of an SSL connection. The device then rejects re-negotiation requests, preventing the preceding problem.

Precautions

After re-negotiation of an SSL connection is disabled, the re-negotiation session will be interrupted.

Example

Disable re-negotiation of an SSL connection on the server.

```
<Huawei> system-view
[Huawei] ssl policy server-users type server
[Huawei-ssl-policy-server-users] undo renegotiation enable
```

Disable re-negotiation of an SSL connection on the client.

```
<Huawei> system-view
[Huawei] ssl policy client-users type client
[Huawei-ssl-policy-client-users] undo renegotiation enable
```

Related Topics

19.18.3 display ssl policy

 Copyright © Huawei Technologies Co., Ltd.

19.18.7 reset ssl connection statistics

Function

The **reset ssl connection statistics** command deletes statistics on SSL connections.

Format

reset ssl connection statistics

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before counting the maximum number of SSL connections within a certain period of time, delete the existing SSL statistics first.

Precautions

SSL statistics cannot be restored after you delete them. So, confirm the action before you use the command.

Example

Delete statistics on SSL connections.

```
<Huawei> reset ssl connection statistics
```

Related Topics

19.18.2 display ssl connection statistics

19.18.8 server-verify enable

Function

Using the **server-verify enable** command, you can enable SSL server authentication in a client SSL policy.

Using the **undo server-verify enable** command, you can disable SSL server authentication in a client SSL policy.

 Copyright © Huawei Technologies Co., Ltd.

By default, SSL server authentication is enabled in a client SSL policy.

Format

server-verify enable

undo server-verify enable

Parameters

None

Views

Client SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL server and an SSL client perform a handshake to negotiate session parameters and establish a session. During the handshake, the SSL client authenticates the SSL server by checking its digital certificate.

The **server-verify enable** command enables the Router to authenticate SSL servers when it functions as an SSL client.

Precautions

Exercise caution when running the **undo server-verify enable** command because communication becomes insecure after this command is executed.

Example

Enable SSL server authentication.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] server-verify enable
```

Related Topics

19.18.10 ssl policy

19.18.4 pki-realm

19.18.9 session

Function

Using the **session** command, you can set the maximum number of sessions that can be saved and the timeout period of a saved session.

 Copyright © Huawei Technologies Co., Ltd.

Using the **undo session** command, you can restore the default configuration.

By default, a maximum of 3600 sessions can be saved, and the timeout period of a saved session is as follows:

- AR100&AR120&AR150&AR160&AR200 series: 32
- AR1200 series: 128
- AR2200 series: 128
- AR3200 series: 256
- AR3600 series: 256

Format

session { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

Parameters

Parameter	Description	Value
cachesize *size*	Sets the maximum number of sessions that can be saved on the SSL server.	The value is an integer that varies according to different devices.
timeout *time*	Sets the timeout period of a saved session.	The value is an integer that ranges from 1800 to 72000, in seconds.

Views

Server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL server and an SSL client carry out a complex SSL handshake to establish a session. To streamline the SSL handshake process, the SSL protocol allows the server and client to use the previously negotiated parameters to establish new sessions. Therefore, the SSL server must store session information. The **session** command configures the maximum number of sessions that can be saved and the timeout period of a saved session.

- If the number of saved sessions reaches the maximum number, the SSL client stops saving new sessions.

- When the timeout period of a session expires, the SSL server deletes the session.

Precautions

If you run the **session** command multiple times in the same server SSL policy view, only the latest configuration takes effect.

Example

Set the maximum number of sessions that can be saved to 50, and the timeout period of a saved session to 7200s.

```
<Huawei> system-view
[Huawei] ssl policy users type server
[Huawei-ssl-policy-users] session cachesize 50 timeout 7200
```

Related Topics

19.18.10 ssl policy

19.18.10 ssl policy

Function

Using the **ssl policy** command, you can create an SSL policy and enter its view, or enter the view of an existing SSL policy.

Using the **undo ssl policy** command, you can delete an SSL policy.

By default, no SSL policy is created.

Format

ssl policy *policy-name* [**type** { **client** | **server** }]

undo ssl policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL policy.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain any space or question mark (?).
type { **client** | **server** }	Specifies the type of an SSL policy: client SSL policy or server SSL policy.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The Secure Sockets Layer (SSL) protocol protects data privacy on the Internet. It allows a client and a server to communicate in a way designed to prevent eavesdropping.

You can use the **ssl policy** command to create a client or server SSL policy, and configure SSL parameters in the SSL policy view.

Precautions

You must set the SSL policy type when creating an SSL policy. To enter the SSL policy view, you only need to specify the policy name.

The device supports a maximum of 16 SSL policies.

To ensure that the functions referencing SSL policy, such as HTTPS, are available by default, a default server SSL policy exists on the Router. The default policy is bound to a default PKI domain.

Example

Create a client SSL policy **users**.

```
<Huawei> system-view
[Huawei] ssl policy users type client
```

Related Topics

19.18.4 pki-realm

19.18.3 display ssl policy

19.18.11 ssl renegotiation-rate

Function

The **ssl renegotiation-rate** command sets the SSL renegotiation rate.

The **undo ssl renegotiation-rate** command restores the SSL renegotiation rate to default value.

By default, the SSL renegotiation is performed once per second.

Format

ssl renegotiation-rate *rate*

 Copyright © Huawei Technologies Co., Ltd.

undo ssl renegotiation-rate

Parameters

Parameter	Description	Value
rate	Specifies how many times SSL renegotiation is performed per second.	The value is an integer that ranges from 0 to 65535. By default, the SSL renegotiation is performed once per second. The value 0 indicates that the SSL renegotiation rate is not limited.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Disabling the renegotiation function on the device can protect the device against renegotiation attacks, but will interrupt services. Therefore, you can keep the renegotiation function enabled, and set the SSL renegotiation rate to minimize the impact of renegotiation attacks on services.

You can set the SSL renegotiation rate according to the CPU capability of the device.

Example

Set the SSL renegotiation rate to 2.

```
<Huawei> system-view
[Huawei] ssl renegotiation-rate 2
```

19.18.12 version (Client SSL policy view)

Function

The **version** command specifies an SSL protocol version in a client SSL policy.

The **undo version** command restores the default SSL protocol version.

By default, a client SSL policy uses Transport Layer Security (TLS) version 1.2.

Format

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** }

undo version

Parameters

Parameter	Description	Value
ssl3.0	Indicates that the SSL client uses SSL3.0 to communicate with the SSL server.	-
tls1.0	Indicates that the SSL client uses TLS1.0 to communicate with the SSL server.	-
tls1.1	Indicates that the SSL client uses TLS1.1 to communicate with the SSL server.	-
tls1.2	Indicates that the SSL client uses TLS1.2 to communicate with the SSL server. **NOTE** TLS1.2 version is recommended, other protocol version has potential security risks.	-

Views

Client SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL server and an SSL client perform a handshake to negotiate session parameters and establish a session. During an SSL handshake, the SSL client sends a Client Hello message to notify the SSL server of the SSL protocol version and cipher suites that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to notify the client.

The **version** command configures the SSL version used by the SSL client. The SSL client sends a Client Hello message to the SSL server to notify the server of the configured SSL version, and the SSL server determines the SSL version used for this communication.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If you run the **version** command multiple times in the same client SSL policy view, only the latest configuration takes effect.

Ensure that the SSL protocol version specified in this command is supported by the SSL server. Before running this command, check the SSL protocol versions that the SSL server supports.

Example

Configure a client SSL policy to use TLS1.1.

```
<Huawei> system-view
[Huawei] ssl policy users type client
[Huawei-ssl-policy-users] version tls1.1
```

Related Topics

19.18.10 ssl policy

19.18.13 version (server SSL policy view)

Function

The **version** command specifies an SSL protocol version in a server SSL policy.

The **undo version** command restores the default SSL protocol versions of the server SSL policy.

By default, a server SSL policy uses Transport Layer Security (TLS) versions 1.2.

Format

version { **ssl3.0** | **tls1.0** | **tls1.1** | **tls1.2** } *

undo version

Parameters

Parameter	Description	Value
ssl3.0	Indicates that the SSL server uses SSL3.0 to communicate with the SSL client.	-
tls1.0	Indicates that the SSL server uses TLS1.0 to communicate with the SSL client.	-
tls1.1	Indicates that the SSL server uses TLS1.1 to communicate with the SSL client.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
tls1.2	Indicates that the SSL server uses TLS1.2 to communicate with the SSL client. **NOTE** TLS1.2 version is recommended, other protocol version has potential security risks.	-

Views

Server SSL policy view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An SSL client and an SSL server perform a handshake to negotiate session parameters and establish a session. During an SSL handshake, an SSL client sends a Client Hello message to notify an SSL server of the SSL protocol version, encryption algorithm, key exchanging algorithm, and MAC algorithm that it supports. The SSL server determines the SSL protocol version and cipher suite used for this communication and sends a Server Hello message to the client.

The **version** command specifies the SSL protocol version used in the server SSL policy. Then a Server Hello message containing the configured SSL protocol version to the SSL client, and the SSL server determines the SSL protocol version used for this communication.

Precautions

If you run the **version** command multiple times in the same server SSL policy view, only the latest configuration takes effect.

Example

Configure a server SSL policy to use TLS1.1.

```
<Huawei> system-view
[Huawei] ssl policy users type server
[Huawei-ssl-policy-users] version tls1.1
```

Related Topics

19.18.10 ssl policy

19.19 HTTPS Configuration Commands

19.19.1 http secure-client ssl-policy

Function

The **http secure-client ssl-policy** command associates a client SSL policy to an HTTPS client.

The **undo http secure-client ssl-policy** command disassociates a client SSL policy from an HTTPS client.

By default, an HTTPS client is not associated with any client SSL policy.

Format

http secure-client ssl-policy *policy-name*

undo http secure-client ssl-policy

Parameters

Message	Description	Value
policy-name	Specifies the name of the client SSL policy to be associated with an HTTPS client.	The value is a string of 1 to 31 case-sensitive characters without spaces or question mark (?).

Views

System view

Default Level

3: Management level

Usage Guidelines

Use Scenario

When the web proxy service of SSL VPN is configured on the device, if the web server only provides HTTPS service, this command is mandatory. The device functioning as the HTTPS client can use the data encryption, identity authentication, and message integrity check mechanisms provided by the SSL protocol to securely transmit data with the web server.

Prerequisites

A client SSL policy has been created using the **ssl policy** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Associate the client SSL policy **users** to the HTTPS client.

```
<Huawei> system-view
[Huawei] http secure-client ssl-policy users
```

Related Topics

19.18.10 ssl policy

19.19.2 http secure-server enable

Function

The **http secure-server enable** command enables the HTTPS server function on the device.

The **undo http secure-server enable** command disables the HTTPS server function on the device.

By default, the HTTPS server function is enabled on the device.

Format

http secure-server enable

undo http secure-server enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When users use the web page to access a remote device functioning as an HTTP server, the following problems exist:

- Users cannot authenticate the device.
- Privacy and integrity of data transmitted between users and the device cannot be ensured.

This command enables the device to function as an HTTPS server. The device uses the SSL protocol's data encryption, identity authentication, and message integrity check mechanisms to protect security of data transmitted between users and the

 Copyright © Huawei Technologies Co., Ltd.

device. These mechanisms ensure that users securely access a remote device on web pages.

Precautions

An SSL policy must have been associated with the HTTPS server using the **http secure-server ssl-policy** command. Otherwise, the **http secure-server ssl-policy** command does not take effect.

Example

Enable the HTTPS server function on the device.

```
<Huawei> system-view
[Huawei] http secure-server enable
```

Related Topics

19.19.4 http secure-server ssl-policy

19.19.3 http secure-server manager-port

Function

The **http secure-server manager-port** command enables the management port of the HTTPS server and sets the management port number.

The **undo http secure-server manager-port** command restores the default setting of the HTTPS server's management port.

By default, the management port of the HTTPS server is disabled.

NOTE

Only users at level 3 and higher levels can log in to the web platform through the management port.

Format

http secure-server manager-port *port-number*

undo http secure-server manager-port

Parameters

Parameter	Description	Value
port-number	Specifies the management port number of the HTTPS server.	The value is 443 or an integer that ranges from 1025 to 51200.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run this command to enable the management port of the HTTPS server and set the management port number, and then can manage the router.

Precautions

Changing the management port number of the HTTPS server forces all online users to go offline. Therefore, exercise caution when performing this operation.

Example

Set the management port number of the HTTPS server to 1066.

```
<Huawei> system-view
[Huawei] http secure-server manager-port 1066
```

19.19.4 http secure-server ssl-policy

Function

The **http secure-server ssl-policy** command applies a server SSL policy to the HTTPS service.

The **undo http secure-server ssl-policy** command cancels the configuration.

By default, the server SSL policy applied to the HTTPS service on the device is default_policy.

Format

http secure-server ssl-policy *policy-name*

undo http secure-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a server SSL policy.	The value is a string of 1 to 31 case-sensitive characters. It cannot contain any space or question mark (?).

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

This command applies a server SSL policy to the HTTPS service. The device functioning as the HTTPS server uses the SSL protocol's data encryption, identity authentication, and message integrity check mechanisms to ensure the security of data transmitted between users and the device.

Prerequisites

A server SSL policy has been created using the **ssl policy** command.

Precautions

After the HTTPS server function is enabled using the **http secure-server enable** command, you cannot change or delete the server SSL policy associated with the HTTPS server. Before changing or deleting the server SSL policy associated with the HTTPS server, run the **undo http secure-server enable** command to disable the HTTPS server function.

Example

Apply a server SSL policy to the HTTPS service.

```
<Huawei> system-view
[Huawei] http secure-server ssl-policy users
```

Related Topics

19.18.10 ssl policy

19.19.5 http secure-server port

Function

Using the **http secure-server port** command, you can set the port number for the HTTPS service.

Using the **undo http secure-server port** command, you can restore the default port number of the HTTPS service.

By default, the port number of the HTTPS service is 443.

Format

http secure-server port *port-number*

undo http secure-server port

Parameters

Parameter	Description	Value
port-number	Specifies the port number of the HTTPS service.	The value is an integer that ranges from 1025 to 51200. The default value is 443.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By default, the port number of the HTTPS service is 443. Attackers may use the default port to attack an HTTPS server, reducing the bandwidth and deteriorating the performance of the HTTPS server. As a result, authorized users cannot access the HTTPS server.

This command allows you to set another port number for the HTTPS service to avoid such attacks.

Precautions

Changing the port number of the HTTPS service forces all online users to go offline. Therefore, exercise caution when performing this operation.

Example

Set the port number of the HTTPS service to 1278.

```
<Huawei> system-view
[Huawei] http secure-server port 1278
```

Related Topics

19.19.4 http secure-server ssl-policy

19.20 Keychain Configuration Commands

19.20.1 algorithm

Function

The **algorithm** command configures a key authentication algorithm.

The **undo algorithm** command deletes a key authentication algorithm.

By default, no algorithm is configured.

Format

algorithm { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** | **simple** }

undo algorithm

Parameters

Parameter	Description	Value
hmac-md5	Indicates that HMAC (Keyed-Hashing for Message Authentication)-Message Digest 5 (MD5) is used for packet encryption and authentication. **NOTE** HMAC-MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
hmac-sha-256	Indicates that HMAC-Secure Hash Algorithm 256 (SHA-256) is used for packet encryption and authentication.	-
hmac-sha1-12	Indicates that HMAC-Secure Hash Algorithm 1-12 (SHA1-12) is used for packet encryption and authentication.	-
hmac-sha1-20	Indicates that HMAC-SHA1-20 is used for packet encryption and authentication.	-
md5	Indicates that MD5 is used for packet encryption and authentication. **NOTE** MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
sha-1	Indicates that SHA-1 is used for packet encryption and authentication. **NOTE** To ensure high security, do not use the SHA-1 algorithm.	-
sha-256	Indicates that SHA-256 is used for packet encryption and authentication.	-
simple	Indicates that the configured key is used for packet authentication. **NOTE** The authentication algorithm specified by **simple** is not secure. HMAC-SHA-256 or SHA-256 is recommended.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. A keychain consists of multiple keys, each of which needs to be configured with an authentication algorithm. Different keys are valid within different time periods, ensuring dynamic change of keychain authentication algorithms.

Packets are authenticated and encrypted based on the authentication algorithm and key string associated with a specified key. This improves the packet transmission security.

The characteristics of each authentication algorithm are as follows:

- MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length.
- SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message.
- HMAC-SHA-256: The 128-bit SHA-1 message digest.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.
- SHA-256: The 128-bit SHA-1 message digest.

The MD5 algorithm provides faster calculation speed than the SHA-1 algorithm; the SHA-1 algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA-1, HMAC is more secure, but slower in calculation speed. The HMAC algorithm is recommended to improve data transmission security.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Keys configured on the sender and receiver of packets must correspond to the same authentication and encryption algorithms. Otherwise, packet transmission fails for not passing the authentication.

If algorithm is not configured, key will never be active.

Example

Configure algorithm sha-256 on key-id 1.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] algorithm sha-256
```

Related Topics

19.20.5 key-id

19.20.6 key-string

19.20.2 default send-key-id

Function

The **default send-key-id** command configures a particular key as the default send key for that keychain.

The **undo default send-key-id** command deletes default send key.

By default, no key is configured as default send key.

Format

default send-key-id

undo default send-key-id

Parameters

None

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key-sting dynamically. This can reduce the workload of changing the algorithm and key manually. A keychain

consists of multiple authentication keys, each of which is valid within different time periods. When a key becomes valid, the authentication algorithm corresponding to the key is used, and packets passing the authentication will be sent or received.

If a key for packet sending is not configured in a keychain or no key for packet sending is valid within a certain period, protocol packets cannot be authenticated and encrypted. As a result, protocol packet transmission fails. To address such a problem, configure a default key for packet sending. If no key is valid, the default key for packet sending is used.

Precautions

Each keychain can have only one default key for packet sending.

- If the default key for packet sending is an existing key, the authentication and encryption algorithms, and key corresponding to the key are used.
- If the default key for packet sending is a newly created key, configure the authentication and encryption algorithms.

Example

Configure the key-1 as default send key in keychain huawei.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] default send-key-id
```

Related Topics

19.20.5 key-id

19.20.3 display keychain

Function

The **display keychain** command displays the configuration of a specified keychain.

Format

display keychain *keychain-name* [**key-id** *key-id*]

Parameters

Parameter	Description	Value
keychain-name	Displays the configuration of a keychain with a specified name.	The keychain must already exist.
key-id *key-id*	Displays the configuration of a specified key in the keychain.	The key must already exist.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

To troubleshoot a keychain authentication failure or collect required information before configuration, run the **display keychain** command to view configurations of a specified keychain.

Example

Display the configuration of the keychain **huawei**.

```
<Huawei> display keychain huawei
 Keychain Information:
 ---------------------
 Keychain Name            : huawei
   Timer Mode             : Absolute
   Time Type              : Utc
   Receive Tolerance(min)  : 100
   TCP Kind               : 182
   TCP Algorithm IDs      :
     HMAC-MD5             : 5
     HMAC-SHA1-12         : 2
     HMAC-SHA1-20         : 6
     HMAC-SHA-256         : 7
     SHA-256              : 8
     MD5                  : 3
     SHA1                 : 4
 Number of Key IDs        : 1
 Active Send Key ID       : 1
 Active Receive Key IDs   : 01
 Default send Key ID      : 1
 Default send Key Status  : Inactive

 Key ID Information:
 -------------------
 Key ID                   : 1
   Key string             : ******
   Algorithm              : MD5
   SEND TIMER             :
     Start time           : 2012-03-14 00:00
     End time             : 2012-08-08 23:59
     Status               : Active
   RECEIVE TIMER          :
     Start time           : 2012-03-14 00:00
     End time             : 2012-08-08 23:59
     Status               : Active

 Key ID                   : 2
   Key string             : -
   Algorithm              : -
   SEND TIMER             :
     Status               : Inactive
   RECEIVE TIMER          :
     Status               : Inactive
```

Display the configuration of key-id 1 in the keychain **huawei**.

```
<Huawei> display keychain huawei key-id 1
 Keychain Information:
 ---------------------
 Keychain Name            : huawei
   Timer Mode             : Absolute
```

```
  Time Type              : Utc
  Receive Tolerance(min)  : 100
  TCP Kind               : 182
  TCP Algorithm IDs       :
    HMAC-MD5              : 5
    HMAC-SHA1-12          : 2
    HMAC-SHA1-20          : 6
    HMAC-SHA-256          : 7
    SHA-256               : 8
    MD5                   : 3
    SHA1                  : 4

Key ID Information:
-------------------
Key ID                   : 1
  Key string             : ******
  Algorithm              : MD5
  SEND TIMER             :
    Start time           : 2012-03-14 00:00
    End time             : 2012-08-08 23:59
    Status               : Active
  RECEIVE TIMER          :
    Start time           : 2012-03-14 00:00
    End time             : 2012-08-08 23:59
    Status               : Active
  DEFAULT SEND KEY ID INFORMATION
    Default              : Configured
    Status               : Inactive
```

Table 19-177 Description of the display keychain command output

Item	Description
Keychain Name	Name of a keychain. To set the keychain name, run the **keychain** command.
Timer Mode	Time mode of a keychain. ● Absolute: The keychain takes effect in an absolute time range. ● Daily periodic: The keychain is valid on a daily basis. ● Weekly periodic: The keychain is valid on a weekly basis. ● Monthly periodic: The keychain is valid on a monthly basis. ● Yearly periodic: The keychain is valid on a yearly basis. To set the time mode, run the **keychain** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Time Type	Time type of a keychain. ● Lmt: The time type of Keychain is Local Mean Time (LMT). ● Utc: The time type of Keychain is Universal Time Coordinated (UTC). To set the time type, run the **time mode** command.
Receive Tolerance(min)	Receive tolerance time configured for a keychain. To set the receive tolerance time, run the **receive-tolerance** command.
TCP Kind	TCP kind value configured for a keychain. To set the TCP kind value, run the **tcp-kind** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
TCP Algorithm IDs	TCP algorithm ID configured for a keychain. The characteristics of each authentication algorithm are as follows: ● MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length. ● SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message. ● HMAC-SHA-256: The 128-bit SHA-1 message digest. ● HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. ● HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. ● SHA-256: The 128-bit SHA-1 message digest. The MD5 algorithm provides faster calculation speed than the SHA-1 algorithm; the SHA-1 algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA-1, HMAC is more secure, but slower in calculation speed. The HMAC algorithm is recommended to improve data transmission security. To set the TCP algorithm ID, run the **tcp-algorithm-id** command.
Number of Key IDs	Number of key IDs.
Active Send Key ID	ID of the active send key.
Active Receive Key IDs	ID of the active receive key.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Default send Key ID	ID of the default send key.
Default send Key Status	Status of the default send key: ● Active ● Inactive
Key ID	Key configured in a keychain. To set the key ID, run the **key-id** command.
Key string	Key string configured for the key. To set the key string, run the **key-string** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Algorithm	Algorithm configured for the key. The characteristics of each authentication algorithm are as follows: ● MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length. ● SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2. ● HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. **NOTE** If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message. ● HMAC-SHA-256: The 128-bit SHA-1 message digest. ● HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code. ● HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code. ● SHA-256: The 128-bit SHA-1 message digest. The MD5 algorithm provides faster calculation speed than the SHA-1 algorithm; the SHA-1 algorithm is more secure than the MD5 algorithm. Compared with MD5 and SHA-1, HMAC is more secure, but slower in calculation speed. The HMAC algorithm is recommended to improve data transmission security.
SEND TIMER	Send time of a key. To set the send time of a key, run the **send-time** command.
Start time	Time when a key becomes valid.
End time	Time when a key becomes invalid.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Status	Status of send/receive keys: ● Active ● Inactive
RECEIVE TIMER	Receive time of a key. To set the receive time of a key, run the **receive-time** command.
DEFAULT SEND KEY ID INFORMATION	Information about the default send key.
Default	Configuration of the default send key: ● Not configured ● Configured
Status	Status of the default send key: ● Active ● Inactive

19.20.4 keychain

Function

The **keychain** command creates a new set of keychain rules or displays the keychain view.

The **undo keychain** command deletes the keychain configuration.

By default, no keychain is configured.

Format

keychain *keychain-name* **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } }

undo keychain *keychain-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
keychain-name	Specifies the keychain name. All the applications identify the set of keychain rules by keychain name.	The value is a string of 1 to 47 case-insensitive characters. Except the question mark (?) and space. However, when double quotation marks (") are used around the string, spaces are allowed in the string.
mode	Indicates the time mode of a keychain. **NOTE** ● The time mode of a keychain must be specified when a keychain is created. ● You do not need to specify the time mode for a created keychain.	-
absolute	Indicates that the given keychain is non-periodic.	-
periodic	Indicates that the given keychain is periodic.	-
daily	Indicates that the given keychain is day-periodic.	-
weekly	Indicates that the given keychain is week-periodic.	-
monthly	Indicates that the given keychain is month-periodic.	-
yearly	Indicates that the given keychain is year-periodic.	-

Views

System view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

 Copyright © Huawei Technologies Co., Ltd.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

There are two keychain time modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

Follow-up Procedure

Run the **key-id** command to configure a key. If the key is not configured, the keychain cannot authenticate and encrypt protocol packets.

The time mode of a key must be the same as the time mode of the keychain.

Precautions

A keychain supports a maximum of 64 keys.

The **keychain** *keychain-name* command displays a specific keychain view. If the keychain specified by *keychain-name* does not exist, the **keychain** *keychain-name* command cannot be executed. To create a keychain, run the **keychain** *keychain-name* **mode** { **absolute** | **periodic** { **daily** | **weekly** | **monthly** | **yearly** } } command.

Example

Configure the keychain **huawei** and enter keychain view.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei]
```

Related Topics

19.20.5 key-id

19.20.5 key-id

Function

The **key-id** command creates a new set of key-ids or displays the key-id view.

The **undo key-id** command deletes the key-id configuration.

By default, no key-id is configured.

Format

key-id *key-id*

undo key-id *key-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
key-id	Specifies the key identification number of a keychain.	The integer value ranges from 0 to 63.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key dynamically. This can reduce the workload of manually changing the algorithm and key.

The dynamic change of the keychain authentication algorithm is implemented based on the keys. Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Follow-up Procedure

After key-id is specified, perform the following operations:

- Run the **algorithm** command to configure an algorithm used by the key.
- Run the **key-string** command to specify a key string.
- Run the **send-time** command to specify the send time of the key.
- Run the **receive-time** command to specify the receive time of the key.

Precautions

A **key-id** represents a key on the device.

A keychain supports 64 keys, but only one key takes effect during one period.

No active key can be used to authenticate and encrypt protocol packets at the intervals of keys. Therefore, run the **default send-key-id** command to specify a default key.

The time mode of the key must be the same as the time mode of Keychain.

Example

Configure key-id 1.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1]
```

Related Topics

19.20.6 key-string
19.20.1 algorithm
19.20.9 send-time
19.20.7 receive-time

19.20.6 key-string

Function

The **key-string** command specifies a key used for keychain authentication.

The **undo key-string** command deletes a key used for keychain authentication.

By default, no key is configured for keychain authentication.

Format

key-string { **plain** *plain-text* | [**cipher**] *cipher-text* }

undo key-string

Parameters

Parameter	Description	Value
plain *plain-text*	Indicates the plain text used for authentication. The configured text will be stored as unencrypted text and displayed as unencrypted text. **NOTE** When configuring an authentication password, select the ciphertext mode because the password is saved in the configuration file as a simple text if you select the plaintext mode, which has a high risk. To ensure device security, change the password periodically.	The value is a string of case-sensitive characters that can be letters or digits. The value is a string of case-sensitive characters ranging from 1 to 255. **NOTE** If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.
cipher	Specifies the cipher key string used for encryption and decryption.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher-text	Indicates the cipher text used for authentication.	The value is a string of case-sensitive characters that can be letters or digits. The authentication password can be a string of 1 to 255 characters in plaintext or a string of 20 to 392 characters in ciphertext. **NOTE** If a password contains a space, the password must be placed into a pair of double quotation marks. Only one pair of double quotation marks can be used for each user name.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by dynamically changing the authentication algorithm and key string. This can prevent unauthorized users from obtaining the key string, and authentication and encryption algorithms, and reduce the workload of manually changing the algorithm and key string.

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm. When a key becomes valid, the corresponding authentication algorithm is used.

Precautions

An authentication key configured in cipher text mode will be also displayed in cipher text mode. Therefore, remember the plaintext key string when configuring the key in cipher text mode.

If the authentication key is not configured, the corresponding key remains in inactive state.

Example

Configure the key string **Huawei@1234**.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] key-id 1
[Huawei-keychain-huawei-keyid-1] key-string cipher Huawei@1234
```

Related Topics

19.20.5 key-id

19.20.1 algorithm

19.20.7 receive-time

Function

The **receive-time** command configures a key as a receive key for the specified interval of time.

The **undo receive-time** command deletes the receive time configuration.

By default, no receive time is configured.

Format

receive-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

receive-time daily *start-time* **to** *end-time*

receive-time day { *start-day-name* **to** *end-day-name* | *day-name &<1-7>* }

receive-time date { *start-date-value* **to** *end-date-value* | *date-value &<1-31>* }

receive-time month { *start-month-name* **to** *end-month-name* | *month-name &<1-12>* }

undo receive-time

Parameters

Parameter	Description	Value
start-time	Specifies the start receive time.	In HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specifies the start date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the receive time in minutes.	The value ranges from 1 to 26280000.
infinite	Indicates that the key will be acting as an active receive key forever from the configured start time.	-
to	Indicates a separator.	-
end-time	Specifies the end receive time.	In HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start start.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-date	Specifies the end date.	In YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily receive time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end receive day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the receive day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end receive date of the month.	The value ranges from 2 to 31. The end date must be later than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the receive date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-
start-month-name	Specifies the month of the year to be configured as the start receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.
end-month-name	Specifies the end receive month. The end month must be greater than the start month.	The end month must be later than the start month. It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
month-name &<1-12>	Specifies the month of the year to be configured as the receive month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different keys for packet sending and receiving to be valid within different time periods.

When the system time is within the specified interval, the receive key is in active state.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which receive keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys can be active at the same time. The device will select a key for decryption based on the received packet.

Example

Configure the receive time with the time mode as absolute and range as infinite.

```
<Huawei> system-view
[Huawei] keychain huawei1 mode absolute
[Huawei-keychain-huawei1] key-id 1
[Huawei-keychain-huawei1-keyid-1] receive-time 14:52 2008-10-1 duration infinite
```

Configure the receive time with the time mode as daily.

```
<Huawei> system-view
[Huawei] keychain huawei2 mode periodic daily
[Huawei-keychain-huawei2] key-id 1
[Huawei-keychain-huawei2-keyid-1] receive-time daily 14:52 to 18:10
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.20.9 send-time

19.20.8 receive-tolerance

Function

The **receive-tolerance** command sets receive tolerance for all the receive keys in the keychain.

The **undo receive-tolerance** command deletes the receive tolerance configuration.

By default, no receive tolerance is configured.

Format

receive-tolerance { *value* | **infinite** }

undo receive-tolerance

Parameters

Parameter	Description	Value
value	Specifies the receive tolerance value for a keychain.	The integer value ranges from 1 to 14400 in minutes.
infinite	Indicates that the receive tolerance is infinite. That is, the receive key is always valid.	-

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

In keychain authentication mode, secure protocol packet transmission is provided by changing the authentication algorithm and key string dynamically. Each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm is used.

Due to the networking environment or clock asynchronization on the packet sender and receiver, packets may be delayed. The receiver may receive a packet sent from the sender after its key for packet receiving becomes invalid. As a result, the receiver discards the packet and packet transmission is interrupted. To address this problem, set a tolerance time to ensure that the validity period of the receive

 Copyright © Huawei Technologies Co., Ltd.

key on the receiver expires after all packets sent from the sender reach the receiver.

Precautions

A tolerance time is required for each keychain. The configured tolerance time takes effect for all keys in the keychain.

Example

Configure the receive tolerance time as 570 minutes.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] receive-tolerance 570
```

19.20.9 send-time

Function

The **send-time** command configures a key as a send key at a specified interval.

The **undo send-time** command deletes the send time configuration.

By default, no send-time is configured.

Format

send-time *start-time start-date* { **duration** { *duration-value* | **infinite** } | **to** *end-time end-date* }

send-time daily *start-time* **to** *end-time*

send-time day { *start-day-name* **to** *end-day-name* | *day-name &<1-7>* }

send-time date { *start-date-value* **to** *end-date-value* | *date-value &<1-31>* }

send-time month { *start-month-name* **to** *end-month-name* | *month-name &<1-12>* }

undo send-time

Parameters

Parameter	Description	Value
start-time	Specifies the start send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59.
start-date	Specify the start date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
duration *duration-value*	Specifies the duration of the send time, in minutes.	The value ranges from 1 to 26280000.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
infinite	Indicates that the key will act as a send key forever from the configured start time.	-
to	Indicates a separator.	-
end-time	Specifies the end send time.	The value is in HH:MM format. The value ranges from 00:00 to 23:59. The end time must be later than the start time.
end-date	Specifies the end date.	The value is in YYYY-MM-DD format. The value ranges from 1970-01-01 to 2050-12-31.
daily	Specifies the daily send time for the given key.	-
day	Specifies the days of the week.	-
start-day-name	Specifies the day of the week to be configured as the start send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun.
end-day-name	Specifies the end send day for the given key.	It can be Tue, Wed, Thur, Fri, Sat, and Sun. The end day must be later than the start day.
day-name &<1-7>	Specifies the day of the week to be configured as the send day for the given key.	It can be Mon, Tue, Wed, Thur, Fri, Sat, and Sun. One or more days can be configured.
date	Specifies the date of the month.	-
start-date-value	Specifies the start date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31.
end-date-value	Specifies the end date of the month to be configured as the send date for the given key.	the The value ranges from 2 to 31. The end date must be greater than the start date.
date-value &<1-31>	Specifies the date of the month to be configured as the send date for the given key.	The value ranges from 1 to 31. One or more dates can be configured.
month	Specifies the months of the year.	-
start-month-name	Specifies the month of the year to be configured as the start send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end-month-name	Specifies the end send month. The end month must be greater than the start month.	It can be Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. The end month must be later than the start month.
month-name &<1-12>	Specifies the month of the year to be configured as the send month for the given key.	It can be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, and Dec. One or more months can be configured.

Views

Key-ID view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

Each keychain consists of multiple keys that are valid within different time periods and each key is configured with an authentication algorithm and a key string. When a key becomes valid, the corresponding authentication algorithm and the key string are used. Configure different send and receive keys to be valid within different time periods.

When the system is within the send time range of the key, the device will use the algorithm and key of the configured key to encrypt the packet.

There are two keychain validity modes:

- Absolute time range: In this mode, keychains are valid within a certain period.
- Periodic time range: In this mode, keychains are valid periodically.

The mode in which send keys become valid must be the same as that configured for the keychain.

Precautions

Multiple receive keys cannot be active at the same time. Only one key takes effect during a period in a keychain.

Example

Configure the send time with the time mode as absolute.

```
<Huawei> system-view
```

```
[Huawei] keychain huawei1 mode absolute
[Huawei-keychain-huawei1] key-id 1
[Huawei-keychain-huawei1-keyid-1] send-time 14:52 2008-10-1 to 14:52 2040-10-1
```

Configure the send time with the time mode as daily.

```
<Huawei> system-view
[Huawei] keychain huawei2 mode periodic daily
[Huawei-keychain-huawei2] key-id 1
[Huawei-keychain-huawei2-keyid-1] send-time daily 14:52 to 18:10
```

Related Topics

19.20.7 receive-time

19.20.10 tcp-algorithm-id

Function

The **tcp-algorithm-id** command specifies a TCP algorithm ID to represent an algorithm supported by the keychain.

The **undo tcp-algorithm-id** command restores the default settings.

By default, mapping between the TCP algorithm and algorithm ID supported by IANA is used.

Format

tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** } *algorithm-id*

undo tcp-algorithm-id { **hmac-md5** | **hmac-sha-256** | **hmac-sha1-12** | **hmac-sha1-20** | **md5** | **sha-1** | **sha-256** }

Parameters

Parameter	Description	Value
hmac-md5	Specifies that message authentication algorithm used is HMAC-MD5. **NOTE** HMAC-MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
hmac-sha-256	Specifies that message authentication algorithm used is HMAC-SHA-256.	-
hmac-sha1-12	Specifies that message authentication algorithm used is HMAC-SHA1-12.	-
hmac-sha1-20	Specifies that message authentication algorithm used is HMAC-SHA1-20.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
md5	Specifies that message authentication algorithm used is MD5. **NOTE** MD5 has potential security risks. HMAC-SHA-256 or SHA-256 is recommended.	-
sha-1	Specifies that message authentication algorithm used is SHA-1. **NOTE** To ensure high security, do not use the SHA-1 algorithm.	-
sha-256	Specifies that message authentication algorithm used is SHA-256.	-
algorithm-id	Specifies the TCP algorithm ID to represent the algorithm.	The value ranges from 1 to 63. Default algorithm id for algorithm types are: **md5** is 3, **hmac-sha-256** is 7, **sha-1** is 4, **hmac-md5** is 5, **hmac-sha1-12** is 2, **hmac-sha1-20** is 6 and **sha-256** is 8.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

The TCP connection is authenticated using the authentication algorithm specified by the algorithm ID. The algorithm ID is not defined by IANA. Different vendors use different algorithm IDs to identify authentication algorithms. When two devices of different vendors are connected, ensure that algorithm IDs configured on the two devices are the same.

The characteristics of each authentication algorithm are as follows:

- MD5: The 128-bit MD5 message digest is calculated based on the entered message of any length.

 Copyright © Huawei Technologies Co., Ltd.

- SHA-1: The 160-bit SHA-1 message digest is calculated based on the entered message with the length shorter than the 64th power of 2.
- HMAC-MD5: The 128-bit HMAC-MD5 message digest is calculated based on the 512-bit message that is converted from the entered message of any length.

  NOTE

  If the length of an entered message is less than 512 bits, 0s are added to make up a 512-bit message. If the length of an entered message is greater than 512 bits, the message is converted into a 128-bit message based on the MD5 algorithm. After that, 0s are added to make up a 512-bit message.
- HMAC-SHA1-12: The 160-bit HMAC-SHA1-12 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. The leftmost 96 bits (12 x 8) are used as the authentication code.
- HMAC-SHA1-20: The 160-bit HMAC-SHA1-20 message digest is calculated based on the 512-bit message that is converted from the entered message of any length. All the 160 bits are used as the authentication code.

Follow-up Procedure

After configuring algorithm IDs for the communicating parties, run the **tcp-kind** command to configure TCP types for the communicating parties.

Precautions

Each algorithm has a unique algorithm ID.

Example

Configure the TCP algorithm ID of **hmac-sha-256** as 1.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] tcp-algorithm-id hmac-sha-256 1
```

Related Topics

19.20.11 tcp-kind

19.20.11 tcp-kind

Function

The **tcp-kind** command specifies the option type in the TCP enhanced authentication option.

The **undo tcp-kind** command restores the default TCP kind value.

By default, the default kind value is 254.

Format

tcp-kind *kind-value*

undo tcp-kind

Parameters

Parameter	Description	Value
kind-value	Specifies the TCP kind value to be used for that keychain.	The value ranges from 28 to 255.

Views

Keychain view

Default Level

2: Configuration Level

Usage Guidelines

Usage Scenario

A keychain ensures secure protocol packet transmission by dynamically changing the authentication algorithm and key string. Packets to be transmitted over non-TCP and TCP connections are authenticated using authentication and encryption algorithms and key string corresponding to a key. The TCP connection needs to be authenticated to enhance security.

TCP connection request packets carry enhanced authentication options and are authenticated by a specified authentication algorithm. Different vendors use different kind values to specify the enhanced authentication option. Kind values configured for the communicating parties must be the same.

Follow-up Procedure

After configuring the same TCP kind value for the communicating parties, run the **tcp-algorithm-id** command to specify TCP algorithm IDs for the communicating parties.

Precautions

Communicating parties using the keychain authentication must establish a TCP connection when configuring the kind value. Otherwise, the TCP authentication does not take effect.

Example

Configure the TCP kind value as 252 for the keychain **huawei**.

```
<Huawei> system-view
[Huawei] keychain huawei mode absolute
[Huawei-keychain-huawei] tcp-kind 252
```

Related Topics

19.20.4 keychain

19.20.10 tcp-algorithm-id

 Copyright © Huawei Technologies Co., Ltd.

19.20.12 time mode

Function

The **time mode** command configures the time mode for Keychain.

The **undo time mode** command restores the default time mode for Keychain.

By default, the time mode of Keychain is Local Mean Time (LMT).

Format

time mode { **utc** | **lmt** }

undo time mode

Parameters

Parameter	Description	Value
utc	Specifies that the configured time is in Universal Time Coordinated (UTC) format.	-
lmt	Specifies that the configured time is in LMT format.	-

Views

Keychain view

Default Level

2: Configuration level

Usage Guidelines

Each keychain consists of multiple key IDs that are valid within different time periods and each key ID is configured with an authentication algorithm. When a key ID becomes valid, the corresponding authentication algorithm is used, ensuring the dynamic change of authentication algorithms. Configure different key IDs for packet sending and receiving to be valid within different time periods.

To configure the time mode for Keychain, run the **time mode** command. You can configure UTC or LMT for Keychain based on the network planning. Ensure that the time mode remains the same on the entire network.

Example

Configure the time mode for Keychain as UTC.

```
<Huawei> system-view
[Huawei] keychain huawei1 mode absolute
[Huawei-keychain-huawei1] time mode utc
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

19.20.4 keychain

20 QoS Commands

About This Chapter

NOTE

4GE-2S boards do not support QoS.

20.1 MQC Configuration Commands
20.2 Priority Mapping Commands
20.3 Traffic Policing and Traffic Shaping Commands
20.4 Congestion Avoidance and Congestion Management Commands
20.5 Filtering Configuration Commands
20.6 Statistics Configuration Commands
20.7 ACL-based Simplified Traffic Policy Commands
20.8 Bandwidth Management Configuration Commands
20.9 Application Control Management Commands
20.10 SAC Configuration Commands

20.1 MQC Configuration Commands

NOTE

The 4GE-2S, 4ES2G-S, 4ES2GP-S, 9ES2 and 24ES2GP cards do not support MQC.

20.1.1 classifier behavior

Function

The **classifier behavior** command binds a traffic behavior to a traffic classifier in a traffic policy.

 Copyright © Huawei Technologies Co., Ltd.

The **undo classifier** command unbinds a traffic behavior from a traffic classifier in a traffic policy.

By default, no traffic classifier or traffic behavior is bound to a traffic policy.

Format

classifier *classifier-name* **behavior** *behavior-name* [**precedence** *precedence-value*]

undo classifier *classifier-name*

Parameters

Parameter	Description	Value
classifier-name	Specifies the name of a traffic classifier.	The value is a string of 1 to 31 case-sensitive characters without spaces.
behavior-name	Specifies the name of a traffic behavior.	The value is a string of 1 to 31 case-sensitive characters without spaces.
precedence *precedence-value*	Specifies the priority of a pair of a traffic classifier and a traffic behavior. ● If another pair of a traffic classifier and a traffic behavior in the same traffic policy is specified with the same priority, the priority setting takes effect on the first configured pair. ● If no priority is specified for a pair of a traffic classifier and a traffic behavior, the device automatically allocates a priority, which is a multiple of 5 and larger than the current largest priority value, to the pair.	The value is an integer that ranges from 0 to 65535. A smaller value indicates a higher priority.

Views

Traffic policy view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To take an action for packets of a certain type, use a traffic classifier to group the packets into one class and use a traffic behavior to define an action. Then associate the traffic classifier with the traffic behavior and bind them to a traffic policy. You can run the **precedence** *precedence-value* command to specify the priority of the bound traffic classifier and traffic behavior. A smaller value of *precedence-value* indicates a higher priority.

Prerequisites

- A traffic classifier has been created using the **traffic classifier** command.
- A traffic behavior has been created using the **traffic behavior** command.
- A traffic policy has been created using the **traffic policy** command.

Precautions

When a traffic policy that is bound to a traffic classifier and a traffic behavior is applied to an interface, you can directly change the binding between the traffic classifier and the traffic behavior.

The device supports a maximum of 1024 traffic classifiers, traffic behaviors, or traffic policies. In a traffic policy, one traffic classifier can be bound to only one traffic behavior; each traffic policy supports a maximum of 1024 pairs of traffic classifiers and traffic behaviors.

Example

Bind the traffic classifier **c1** to the traffic behavior **b1** in the traffic policy **p1**, and apply the traffic policy to Eth2/0/0 in the inbound direction.

```
<Huawei> system-view
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match any
[Huawei-classifier-c1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark 8021p 2
[Huawei-behavior-b1] quit
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] traffic-policy p1 inbound
[Huawei-Ethernet2/0/0] quit
```

In policy b, bind traffic classifier c to traffic behavior b, and set the priority of the bound traffic classifier and traffic behavior to 3.

```
<Huawei> system-view
[Huawei] traffic classifier c
[Huawei-classifier-c] if-match any
[Huawei-classifier-c] quit
[Huawei] traffic behavior b
[Huawei-behavior-b] remark 8021p 2
[Huawei-behavior-b] quit
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei] traffic policy p
[Huawei-trafficpolicy-p] classifier c behavior b precedence 3
```

Bind the traffic classifier **c1** to the new traffic behavior **newb1** in the traffic policy **p1** that has been applied to Eth2/0/0 in the inbound direction.

```
<Huawei> system-view
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior newb1
[Huawei-trafficpolicy-p1] quit
```

Related Topics

20.1.2 display traffic behavior
20.1.3 display traffic classifier
20.1.4 display traffic policy
20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy

20.1.2 display traffic behavior

Function

The **display traffic behavior** command displays the traffic behavior configuration on the device.

Format

display traffic behavior { **system-defined** | **user-defined** } [*behavior-name*]

Parameters

Parameter	Description	Value
system-defined	Displays the configuration of the system-defined traffic behavior.	-
user-defined	Displays the configuration of a user-defined traffic behavior.	-
behavior-name	Specifies the name of a traffic behavior. If this parameter is not specified, the configuration of all traffic behaviors is displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic behavior** command displays the configuration of a specified traffic behavior or all traffic behaviors. The command output helps you check the traffic behavior configuration and locate faults.

Precautions

If no traffic behavior is created, the system displays the following information after this command is executed:

```
Info: There is no behavior exists.
```

If the specified traffic behavior name is incorrect, the system displays an error message after this command is executed:

```
Error: The behavior does not exist.
```

Example

Display configurations of all traffic behaviors on the device.

```
<Huawei> display traffic behavior user-defined
  User Defined Behavior Information:
    Behavior: b1
      Committed Access Rate:
        CIR 256 (Kbps), PIR 0 (Kbps), CBS 48128 (byte), PBS 80128 (byte)
        Color Mode: color Blind
        Conform Action: pass
        Yellow  Action: pass
        Exceed  Action: discard
      statistic: enable
      Marking:
        Remark DSCP 15
```

Table 20-1 Description of the **display traffic behavior user-defined** command output

Item	Description
Behavior	Traffic behavior name. To create a traffic behavior, run the **traffic behavior** command.
Committed Access Rate	CAR. To configure an action taken for packets whose rate exceeds the CIR, run the **car (traffic behavior view)** command.
CIR	Committed information rate (CIR). To set the CIR, run the **car (traffic behavior view)** command.
PIR	Peak information rate (PIR). To set the PIR, run the **car (traffic behavior view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
CBS	Committed burst size (CBS). To set the CBS, run the **car (traffic behavior view)** command.
PBS	Peak burst size (PBS). To set the PBS, run the **car (traffic behavior view)** command.
Color Mode	Color mode, which can be color-aware or color-blind. To set the color mode, run the **car (traffic behavior view)** command.
Conform Action	Action taken for packets whose rate is within the CIR. To configure an action taken for packets whose rate is within the CIR, run the **car (traffic behavior view)** command.
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.
Exceed Action	Action taken for packets whose rate exceeds the CIR. To configure an action taken for packets whose rate exceeds the CIR, run the **car (traffic behavior view)** command.
Marking	Re-marking action. To configure re-marking, run the **remark** command.

Related Topics

20.3.2 car (traffic behavior view)

20.1.44 traffic behavior

20.6.1 statistic enable (traffic behavior view)

20.1.3 display traffic classifier

Function

The **display traffic classifier** command displays the traffic classifier configuration on the device.

Format

display traffic classifier { **system-defined** | **user-defined** } [*classifier-name*]

Parameters

Parameter	Description	Value
system-defined	Displays the configuration of the system-defined traffic classifier.	-
user-defined	Displays the configuration of a user-defined traffic classifier.	-
classifier-name	Displays the configuration of a specified traffic classifier. If the name of a traffic classifier is not specified, the configuration of the system-defined traffic classifier or all user-defined traffic classifiers is displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic classifier** command displays the configuration of a specified traffic classifier or all traffic classifiers. The command output helps you check the traffic classifier configuration and locate faults.

Precautions

If no traffic classifier is created, the system displays the following information after this command is executed:

```
Info: There is no classifier exists.
```

If the specified traffic classifier name is incorrect, the system displays an error message after this command is executed:

```
Error: The classifier does not exist.
```

Example

Display the configuration of all traffic classifiers on the device.

```
<Huawei> display traffic classifier user-defined
  User Defined Classifier Information:
   Classifier: c2
```

```
 Operator: AND
 Rule (s) :
  if-match vlan-id 110

Classifier: c3
 Operator: AND
 Rule (s) :
  if-match vlan-id 100

Classifier: c1
 Operator: AND
 Rule (s) :
  if-match vlan-id 120
```

Table 20-2 Description of the **display traffic classifier user-defined** command output

Item	Description
Classifier	Traffic classifier name. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Rule(s)	Rule in a traffic classifier.

Related Topics

20.1.45 traffic classifier

20.1.4 display traffic policy

Function

The **display traffic policy** command displays the traffic policy configuration on the device.

Format

display traffic policy user-defined [*policy-name* [**classifier** *classifier-name*]]

Parameters

Parameter	Description	Value
user-defined	Displays the user-defined traffic policy configuration.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy. If this parameter is not specified, the configuration of all traffic policies is displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.
classifier *classifier-name*	Specifies the name of a traffic classifier. If the name of a traffic policy is specified but this parameter is not specified, only the traffic policy configuration is displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy** command displays the configuration of a specified traffic policy or all traffic policies. The command output helps you check the traffic policy configuration and locate faults.

Precautions

If no traffic policy is created, the system displays an error message after this command is executed:

```
Info: There is no policy exists.
```

If the specified traffic policy name is incorrect, the system displays an error message after this command is executed:

```
Error: The policy does not exist.
```

Example

Display the configuration of the traffic behavior bound to the traffic classifier **c1** in the traffic policy **p1**.

```
<Huawei> display traffic policy user-defined p1 classifier c1
 User Defined Traffic Policy Information:
     Classifier: c1
      Operator: OR
     Behavior: b1
       statistic: enable
```

```
    Committed Access Rate:
      CIR 1000 (Kbps), PIR 2000 (Kbps), CBS 125000 (byte), PBS 250000 (byte)
      Color Mode: color Blind
      Conform Action: pass
      Yellow  Action: pass
      Exceed  Action: discard
```

Table 20-3 Description of the **display traffic policy user-defined** command output

Item	Description
Classifier	Traffic classifier in a traffic policy. To create a traffic classifier, run the **traffic classifier** command.
Operator	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior bound to the traffic classifier. To create a traffic behavior, run the **traffic behavior** command.
statistic	Whether the traffic statistics function is enabled. To enable the traffic statistics function, run the **statistic enable (traffic behavior view)** command.
Committed Access Rate	CAR. To configure CAR, run the **car (traffic behavior view)** command.
CIR 1000 (Kbps), PIR 2000 (Kbps), CBS 125000 (byte), PBS 250000 (byte)	Parameters in the QoS CAR profile, including the CIR, PIR, CBS, and PBS. To configure CAR parameters, run the **car (traffic behavior view)** command.
Color Mode	Color mode, which can be color-aware or color-blind. To configure a color mode, run the **car (traffic behavior view)** command.
Conform Action	Action taken for packets whose rate is within the CIR. To configure an action taken for packets whose rate is within the CIR, run the **car (traffic behavior view)** command.
Yellow Action	Action taken for yellow packets. To configure an action taken for yellow packets, run the **car (traffic behavior view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Exceed Action	Action taken for packets whose rate exceeds the CIR. To configure an action taken for packets whose rate exceeds the CIR, run the **car (traffic behavior view)** command.

Related Topics

20.3.2 car (traffic behavior view)
20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy
20.1.49 traffic-policy (interface view)

20.1.5 display traffic policy statistics

Function

The **display traffic policy statistics** command displays statistics on packets matching a traffic policy that is applied to an interface.

Format

display traffic policy statistics interface *interface-type interface-number* [**pvc** *vpi-number*/*vci-number* | **dlci** *dlic-number*] { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name* [**son-class** *son-class-name*]]]

display traffic policy statistics interface virtual-template *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name* [**son-class** *son-class-name*]]]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays packet statistics on a specified interface to which a traffic policy has been applied. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Parameter	Description	Value
pvc *vpi-number*|*vci-number*	Specifies the Virtual Path Identifier (VPI)/Virtual Channel Identifier (VCI) pair. The VPI/VCI pair can be specified on only ATM interfaces.	• *vpi-number* is an integer that ranges from 0 to 255. • *vci-number* is an integer that can be 0-2, or 5-255.
dlci *dlic-number*	Specifies the DLCI number. The DLCI number can be specified on only serial or MFR interfaces.	The value is an integer that ranges from 16 to 1022.
virtual-template *vt-number* **virtual-access** *va-number*	Displays packet statistics on a specified virtual interface to which a traffic policy has been applied. • **virtual-template** *vt-number* specifies the number of a virtual template interface. • **virtual-access** *va-number* specifies the number of a virtual access interface.	*vt-number* is an integer that ranges from 0 to 1023. *va-number* is an integer that ranges from 0 to 1023.
inbound	Displays packet statistics in the inbound direction to which a traffic policy has been applied.	-
outbound	Displays packet statistics in the outbound direction to which a traffic policy has been applied.	-
verbose	Displays detailed packet statistics.	-
classifier-base	Displays statistics on packets matching a specified traffic classifier. If this parameter is specified, statistics on packets matching all traffic classifiers in the traffic policy are displayed.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
rule-base	Displays statistics on packets matching a rule. If this parameter is specified, statistics on packets matching all rules are displayed. **NOTE** Matching rules cannot be used to query packet statistics about the nested traffic policy.	-
class *classifier-name*	Specifies the name of a traffic classifier. If this parameter is specified, statistics on packets matching the specified traffic classifier or rules in the specified traffic classifier are displayed. If this parameter is not specified, statistics on packets matching all traffic classifiers are displayed. Displays statistics on packets matching a specified traffic classifier in HQoS.	The value is a string of 1 to 31 case-sensitive characters without spaces.
son-class *son-class-name*	Displays statistics on packets matching a traffic classifier of a sub traffic policy bound to the traffic classifier specified by *classifier-name*.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy statistics** command displays statistics on forwarded packets and discarded packets on an interface to which a traffic policy has been applied. The command output helps you locate faults.

Precautions

If no traffic policy is applied, the system displays the following error message after this command is executed:

```
Info: The Policy is not applied in this view.
```

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays the following information after this command is executed:

```
Info: Statistic has not been enabled.
```

Example

Display packet statistics on Eth2/0/0 in the inbound direction to which a traffic policy has been applied.

```
<Huawei> display traffic policy statistics interface ethernet 2/0/0 inbound

 Interface: Ethernet2/0/0
 Traffic policy inbound: p1
 Rule number: 1
 Current status: OK!
Item                  Sum(Packets/Bytes)            Rate(pps/bps)
-------------------------------------------------------------------------------
Matched                 585,859/72,646,516              999/991,976
  Passed                296,554/36,772,696              504/499,976
  Dropped               289,305/35,873,820              495/491,992
    Filter                0/0                       0/0
    CAR                 289,305/35,873,820              495/491,992
  Queue Matched               0/0                       0/0
    Enqueued                0/0                       0/0
    Discarded               0/0                       0/0
  CAR                   585,859/72,646,516            1,000/992,000
    Green packets         296,050/36,710,200              504/500,000
    Yellow packets          504/62,496                    0/0
    Red packets           289,305/35,873,820              495/491,992
```

Display statistics on incoming packets matching a traffic classifier in the traffic policy that has been applied to Eth2/0/0.

```
<Huawei> display traffic policy statistics interface ethernet 2/0/0 inbound verbose classifier-base class
c1
 Interface: Ethernet2/0/0
 Traffic policy inbound: p1
 Rule number: 1
 Current status: OK!
 Classifier: c1 operator or
 Behavior: b1
Item                  Sum(Packets/Bytes)            Rate(pps/bps)
-------------------------------------------------------------------------------
Matched                 640,466/79,417,784            1,000/992,168
  Passed                324,078/40,185,672              504/500,096
  Dropped               316,388/39,232,112              496/492,072
    Filter                0/0                       0/0
    CAR                 316,388/39,232,112              496/492,072
  Queue Matched               0/0                       0/0
    Enqueued                0/0                       0/0
    Discarded               0/0                       0/0
  CAR                   640,466/79,417,784            1,000/992,168
    Green packets         323,574/40,123,176              504/500,096
    Yellow packets          504/62,496                    0/0
    Red packets           316,388/39,232,112              496/492,072
Behavior:Be
```

```
Item                    Sum(Packets/Bytes)          Rate(pps/bps)
-----------------------------------------------------------------------------
  Queue Matched                 0/0                       0/0
    Enqueued                  0/0                       0/0
    Discarded                 0/0                       0/0
```

Display statistics on incoming packets matching the traffic classifier **c0** in a sub traffic policy bound to the traffic classifier **c1** in the traffic policy that has been applied to Eth2/0/0.1.

```
<Huawei> display traffic policy statistics interface ethernet 2/0/0.1 inbound verbose classifier-base
class son-class c0

 Interface: Ethernet2/0/0.1
 Traffic policy inbound: p1
 Rule number: 1
 Current status: OK!
-----------------------------------------------------------------------------
 Classifier: c1
   Behavior: b1
     Nest Policy: p0
-----------------------------------------------------------------------------
 Classifier: c0 operator or
 Behavior: b0
Item                        Sum(Packets/Bytes)          Rate(pps/bps)
-----------------------------------------------------------------------------
Matched                          2,575,767/                  2,000/
                               319,395,108                1,984,880
  +--Passed                        130,327/                    100/
                                16,160,548                  100,040
  +--Dropped                     2,445,440/                  1,900/
                               303,234,560                1,884,840
    +--Filter                          0/                      0/
                                       0                       0
    +--CAR                       2,445,440/                  1,900/
                               303,234,560                1,884,840
  +--Queue Matched                     0/                      0/
                                       0                       0
    +--Enqueued                        0/                      0/
                                       0                       0
    +--Discarded                       0/                      0/
                                       0                       0
  +--Car                         2,575,767/                  2,000/
                               319,395,108                1,984,880
    +--Green packets               130,127/                    100/
                                16,135,748                  100,040
    +--Yellow packets                  200/                      0/
                                   24,800                        0
    +--Red packets                 2,445,440/                  1,900/
                               303,234,560                1,884,840
```

Table 20-4 Description of the **display traffic policy statistics** command output

Item	Description
Interface	Interface to which the traffic policy is applied.
Traffic policy inbound	Applied traffic policy.
Rule number	Number of valid rules in the traffic classifier.
Current status	Traffic policy status.

Item	Description
Classifier	Relationship between rules in the traffic classifier. To configure the relationship between rules in a traffic classifier, run the **traffic classifier** command.
Behavior	Traffic behavior name. To create a traffic behavior, run the **traffic behavior** command.
Item	Statistical item.
Sum(Packets/Bytes)	Number of packets or bytes. If the information is displayed as -, the statistics on this item cannot be collected.
Rate(pps/bps)	Rate, in pps or bit/s. If the information is displayed as -, the statistics on this item cannot be collected.
Matched	Numbers of packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Passed	Numbers of forwarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Dropped	Numbers of discarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. The discarded packets include the filtered packets and packets dropped by CAR.
Filter	Numbers of filtered packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
CAR	Numbers of packets and bytes that match traffic classification rules and are discarded by CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. To configure CAR, run the **car (traffic behavior view)** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Queue Matched	Numbers of packets and bytes that match rules in AF, LLQ, EF, and BE queues. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Enqueued	Numbers of forwarded packets and bytes that match rules in AF, LLQ, EF, and BE queues. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Discarded	Numbers of discarded packets and bytes that match rules in AF, LLQ, EF, and BE queues. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Car	Numbers of packets and bytes that match the traffic classifier. The traffic classifier is bound to the traffic behavior that containing the CAR action. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Green packets	Number of green packets, including the number of bytes in green packets. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Yellow packets	Number of yellow packets, including the number of bytes in yellow packets. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Red packets	Number of red packets, including the number of bytes in red packets. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.

Related Topics

20.3.2 car (traffic behavior view)
20.1.41 reset traffic policy statistics
20.6.1 statistic enable (traffic behavior view)
20.1.44 traffic behavior
20.1.45 traffic classifier

 Copyright © Huawei Technologies Co., Ltd.

20.1.6 display traffic policy statistics bridge-domain

Function

The **display traffic policy statistics bridge-domain** command displays statistics on packets matching a traffic policy that is applied to a BD.

NOTE

Only AR100&AR120&AR150&AR160&AR200&AR1200 series and AR2220E support this command.

Format

display traffic policy statistics bridge-domain *bd-id* { **inbound** | **outbound** } [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name* [**son-class** *son-class-name*]]]

Parameters

Parameter	Description	Value
bd-id	Displays statistics on packets matching a traffic policy that is applied to a specified BD.	The value is an integer. The value ranges are as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-64 ● AR1200 series: 1-128 ● AR2220E: 1-256
inbound	Displays statistics on packets matching a traffic policy that is applied to a BD in the inbound direction.	-
outbound	Displays statistics on packets matching a traffic policy that is applied to a BD in the outbound direction.	-
verbose	Displays detailed packet statistics.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
classifier-base	Displays statistics on packets matching a specified traffic classifier. If this parameter is specified, statistics on packets matching all traffic classifiers in the traffic policy are displayed.	-
rule-base	Displays statistics on packets matching a rule. If this parameter is specified, statistics on packets matching all rules are displayed. **NOTE** Matching rules cannot be used to query packet statistics about the nested traffic policy.	-
class *classifier-name*	Specifies the name of a traffic classifier. If this parameter is specified, statistics on packets matching the specified traffic classifier or rules in the specified traffic classifier are displayed. If this parameter is not specified, statistics on packets matching all traffic classifiers are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.
son-class *son-class-name*	Displays statistics on packets matching a traffic classifier of a sub traffic policy bound to the traffic classifier specified by *classifier-name*. **NOTE** Currently, the device does not support the function of this parameter.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic policy statistics bridge-domain** command displays statistics on forwarded and discarded packets in a BD to which a traffic policy has been applied. You can determine whether the traffic policy is applied correctly, and the command output helps you locate faults.

Configuration Notes

If you do not run the **statistics enable (traffic behavior view)** command in the view of the traffic behavior bound to the traffic policy, the system displays an error message after the **display traffic policy statistics bridge-domain** command is executed:

```
Info: Statistic has not been enabled!
```

NOTE

When packets successfully match the traffic policy that is applied to a BD in the inbound or outbound direction, the statistics queried through the **display traffic policy statistics bridge-domain** command are twice the actual statistics.

Example

Display statistics on packets matching a traffic policy that is applied to BD 1 in the outbound direction.

```
<Huawei> display traffic policy statistics bridge-domain 1 outbound

bridge-domain: 1
Traffic policy outbound: p1
 Rule number: 1
 Current status: OK!
 Item                    Sum(Packets/Bytes)              Rate(pps/bps)
 -------------------------------------------------------------------------------
 Matched                      0/0                             0/0
   Passed                     0/0                             0/0
   Dropped                    0/0                             0/0
     Filter                   0/0                             0/0
     CAR                      0/0                             0/0
   CAR                        0/0                             0/0
     Green packets              0/0                             0/0
     Yellow packets             0/0                             0/0
     Red packets                0/0                             0/0
```

Table 20-5 Description of the **display traffic policy statistics bridge-domain** command output

Item	Description
bridge-domain	BD to which the traffic policy is applied.
Traffic policy outbound	Traffic policy that is applied.
Rule number	Number of valid rules in the traffic classifier.

Item	Description
Current status	Status of the traffic policy.
Item	Statistical item.
Sum(Packets/Bytes)	Number of packets or bytes. If the information is displayed as -, the statistics on this item cannot be collected.
Rate(pps/bps)	Rate, in pps or bit/s. If the information is displayed as -, the statistics on this item cannot be collected.
Matched	Numbers of packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Passed	Numbers of forwarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Dropped	Numbers of discarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. The number of dropped packets includes the number of packets dropped by filtering and CAR.
Filter	Numbers of filtered packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
CAR	Numbers of packets and bytes that match traffic classification rules and are discarded by CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. To configure CAR, run the **car (traffic behavior view)** command.
CAR	Numbers of discarded packets and bytes that match the traffic classifier. The traffic classifier is bound to the traffic behavior that defines CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Green packets	Numbers of green packets and bytes in green packets that match the traffic classifier. The traffic classifier is bound to the traffic behavior that defines CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Yellow packets	Numbers of yellow packets and bytes in yellow packets that match the traffic classifier. The traffic classifier is bound to the traffic behavior that defines CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Red packets	Numbers of red packets and bytes in red packets that match the traffic classifier. The traffic classifier is bound to the traffic behavior that defines CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.

Related Topics

20.3.2 car (traffic behavior view)
20.1.42 reset traffic policy statistics bridge-domain
20.6.1 statistic enable (traffic behavior view)
20.1.44 traffic behavior
20.1.45 traffic classifier

20.1.7 display traffic policy statistics global

Function

The **display traffic policy statistics global** command displays statistics on packets matching a global traffic policy.

Format

display traffic policy statistics global [**verbose** { **classifier-base** | **rule-base** } [**class** *classifier-name* [**son-class** *son-class-name*]]]

Parameters

Parameter	Description	Value
verbose	Displays detailed packet statistics.	-
classifier-base	Displays statistics on packets matching a specified traffic classifier. If this parameter is specified, statistics on packets matching all traffic classifiers in the traffic policy are displayed.	-
rule-base	Displays statistics on packets matching a rule. If this parameter is specified, statistics on packets matching all rules are displayed. **NOTE** Matching rules cannot be used to query packet statistics about the nested traffic policy.	-
class *classifier-name*	Specifies the name of a traffic classifier. If this parameter is specified, statistics on packets matching the specified traffic classifier or rules in the specified traffic classifier are displayed. If this parameter is not specified, statistics on packets matching all traffic classifiers are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.
son-class *son-class-name*	Displays statistics on packets matching a traffic classifier of a sub traffic policy bound to the traffic classifier specified by *classifier-name*. **NOTE** The device does not support the function of this parameter.	The value is a string of 1 to 31 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display traffic policy statistics global** command to check statistics on packets that are forwarded and discarded after a global traffic policy has been applied. The command output helps you check the global policy configuration and locate faults.

Precautions

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays the following information after this command is executed:

```
Info: Statistic has not been enabled.
```

Example

Check statistics on packets matching a global traffic policy.

```
<Huawei> display traffic policy statistics global

global
Traffic policy inbound: a
 Rule number: 1
 Current status: OK!
 Item                  Sum(Packets/Bytes)              Rate(pps/bps)
 -----------------------------------------------------------------------------
 Matched                 89,181/25,711,702                 1/528
   Passed                89,181/25,711,702                 1/528
   Dropped                     0/0                       0/0
     Filter                  0/0                       0/0
     CAR                     0/0                       0/0
   Queue Matched                 0/0                       0/0
     Enqueued                  0/0                       0/0
     Discarded                 0/0                       0/0
   CAR                         0/0                       0/0
     Green packets               0/0                       0/0
     Yellow packets              0/0                       0/0
     Red packets                 0/0                       0/0
```

Table 20-6 Description of the **display traffic policy statistics global** command output

Item	Description
global	Global traffic policy.
Traffic policy inbound	Applied traffic policy.
Rule number	Number of valid rules in the traffic classifier.

Item	Description
Current status	Traffic policy status.
Item	Statistical item.
Sum(Packets/Bytes)	Number of packets or bytes. If the information is displayed as -, the statistics on this item cannot be collected.
Rate(pps/bps)	Rate, in pps or bit/s. If the information is displayed as -, the statistics on this item cannot be collected.
Matched	Numbers of packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Passed	Numbers of forwarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Dropped	Numbers of discarded packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. The discarded packets include the filtered packets and packets dropped by CAR.
Filter	Numbers of filtered packets and bytes that match traffic classification rules. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
CAR	Numbers of packets and bytes that match traffic classification rules and are discarded by CAR. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time. To configure CAR, run the **car (traffic behavior view)** command.
Queue Matched	Numbers of packets and bytes that match rules in AF, LLQ, EF, and BE queues. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Enqueued	Numbers of forwarded packets and bytes that match rules in AF, LLQ, EF, and BE queues. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Discarded	Numbers of discarded packets and bytes that match rules in AF, LLQ, EF, and BE queues. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
CAR	Numbers of packets and bytes that match the traffic classifier. The traffic classifier is bound to the traffic behavior that containing the CAR action. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Green packets	Number of green packets, including the number of bytes in green packets. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Yellow packets	Number of yellow packets, including the number of bytes in yellow packets. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.
Red packets	Number of red packets, including the number of bytes in red packets. The data is originated from the packet statistics that have been collected since the original statistics were cleared last time.

20.1.8 display traffic-policy applied-record

Function

The **display traffic-policy applied-record** command displays traffic policy records.

Format

display traffic-policy applied-record [*policy-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
policy-name	Displays the record of a specified traffic policy. If this parameter is not specified, records of all the applied traffic policies are displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display traffic-policy applied-record** command displays a record of an applied traffic policy or records of all applied traffic policies, including the view, interface number, and direction that the traffic policy/policies is/are applied to, and number of times the traffic policy/policies is/are applied. The command output helps you check traffic policy records and locate faults.

Precautions

If no traffic policy is created or the specified traffic policy name is incorrect, the system displays an error message after this command is executed:

```
Error: Traffic policy does not exist.
```

Example

Display the record of the traffic policy.

```
<Huawei> display traffic-policy applied-record p1
-----------------------------------------------
  Policy Name:   p1
  Policy Index:  2
     Classifier:c1      Behavior:b1     Precedence:5
-----------------------------------------------
 *interface GigabitEthernet2/0/0
    traffic-policy p1 inbound
      slot 0    :  success
      slot 2    :  success
   Classifier: c1
    Operator: OR
    Rule(s) :
     if-match 8021p 4
     Behavior: b1
      Marking:
        Remark DSCP cs2
   Behavior: Be
      Assured Forwarding:
```

```
      Bandwidth 0 (Kbps)
-----------------------------------------------
 Policy total applied times: 1.
<Huawei> display traffic-policy applied-record p
-----------------------------------------------
 Policy Name:   p
 Policy Index:  1
    Classifier:c     Behavior:b    Precedence:5
-----------------------------------------------
 *global
   traffic-policy p inbound
     slot 11   :  success
  Classifier: c
   Operator: OR
   Rule(s) :
    if-match any
    Behavior: b
     statistic: enable
-----------------------------------------------
 Policy total applied times: 1.
```

Table 20-7 Description of the **display traffic-policy applied-record** command output

Item	Description
Policy Name	Traffic policy name.
Policy Index	Traffic policy index.
Classifier	Traffic classifier name.
Behavior	Traffic behavior name.
Precedence	Priority of a pair of a traffic classifier and a traffic behavior.
interface GigabitEthernet2/0/0	Interface to which the traffic policy is applied.
global	System to which the traffic policy is applied.
traffic-policy p1 inbound	Inbound direction to which the traffic policy **p1** is applied.
slot	Status of the traffic policy applied to the specified card. ● success: The traffic policy is applied successfully. ● fail: The traffic policy fails to be applied.
Operator	Relationship between rules in the traffic classifier.
Rule(s)	Rules in the traffic classifier.
Marking	Re-marking action.
Policy total applied times	Number of times the traffic policy is applied.

Related Topics

20.1.45 traffic classifier
20.1.44 traffic behavior
20.1.46 traffic policy

20.1.9 if-match 8021p

Function

The **if-match 8021p** command configures a matching rule based on the 802.1p priority of VLAN packets in a traffic classifier.

The **undo if-match 8021p** command deletes a matching rule based on the 802.1p priority of VLAN packets in a traffic classifier.

By default, a matching rule based on the 802.1p priority of VLAN packets is not configured in a traffic classifier.

Format

if-match 8021p *8021p-value* &<1-8>

undo if-match 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority in VLAN packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match 8021p** command to classify traffic based on the 802.1p priority in VLAN packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

Regardless of whether the relationship between traffic classification rules is AND or OR, if you enter multiple values of 802.1p priorities, the packet that matches one 802.1p priority matches a rule.

If you run the **if-match 8021p** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configures a matching rule based on the 802.1p priority of 1 in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match 8021p 1
```

Related Topics

20.1.45 traffic classifier

20.1.10 if-match acl

Function

The **if-match acl** command configures a matching rule based on an Access Control List (ACL) in a traffic classifier.

The **undo if-match acl** command deletes a matching rule based on an ACL.

By default, a matching rule based on an ACL is not configured in a traffic classifier.

Format

if-match [**ipv6**] **acl** { *acl-number* | *acl-name* }

undo if-match [**ipv6**] **acl** { *acl-number* | *acl-name* }

Parameters

Parameter	Description	Value
ipv6	Indicates that IPv6 ACLs are matched. If this parameter is not specified, IPv4 ACLs are matched.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The value is an integer that ranges from 2000 to 4999. The number of an ACL6 ranges from 2000 to 3999. ● ACLs numbered 2000 to 2999 are basic ACLs, which are used to classify all packets. ● ACLs numbered 3000 to 3999 are advanced ACLs, which are used to classify packets based on Layer 3 information. ● ACLs numbered 4000 to 4999 are Layer 2 ACLs, which are used to classify packets based on the source MAC address, destination MAC address, and packet type.
acl-name	Specifies the name of an ACL.	The value is a string of 1 to 32 case-sensitive characters without spaces. The value must start with a letter (case sensitive).

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To classify packets based on the interface that receives packets, source IP address, destination IP address, protocol over IP, source and destination TCP port numbers, ICMP type and code, and source and destination MAC addresses, ARP packets, reference an ACL in a traffic classifier. You must first define an ACL and configure rules in the ACL, and then run the **if-match acl** command to configure a matching

rule based on the ACL so that the device processes packets matching the same rule in the same manner.

Prerequisites

The following operations must have been performed:

- Create an ACL and configure rules in the ACL.
- Create a traffic classifier using the **traffic classifier** command.

Precautions

Regardless of whether the relationship between rules in a traffic classifier is AND or OR, if an ACL contains multiple rules, the packet that matches one ACL rule matches the ACL.

You can configure multiple ACL rules in a traffic classifier to match different types of packets. A traffic classifier allows a maximum of 1024 if-match rules.

If a traffic policy containing **if-match acl** is applied to a Layer 2 interface on the device, it does not take effect for traffic forwarded at Layer 2.

NOTE

A traffic policy containing **if-match ipv6 acl** can be applied to only WAN-side interfaces.

Example

Configure a matching rule based on ACL 2046 in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] acl 2046
[Huawei-acl-basic-2046] rule permit source any
[Huawei-acl-basic-2046] quit
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match acl 2046
```

Related Topics

19.7.4 acl (system view)

20.1.18 if-match inbound-interface

20.1.30 if-match vlan-id

20.1.45 traffic classifier

20.1.11 if-match any

Function

The **if-match any** command configures a matching rule based on all data packets in a traffic classifier.

The **undo if-match any** command deletes a matching rule based on all data packets in a traffic classifier.

By default, a matching rule based on all data packets is not configured in a traffic classifier.

 Copyright © Huawei Technologies Co., Ltd.

Format

if-match any

undo if-match any

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To process all the data packets in the same manner, run the **if-match any** command.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The **if-match any** command is valid for all data packets but is invalid for the control packets sent to the CPU, such as Bridge Protocol Data Units (BPDUs) of the Spanning Tree Protocol (STP).

NOTE

A traffic policy containing **if-match any** that is applied to a LAN-side interface takes effect for only IPv4 packets.

If **if-match any** and other Layer 3 rules exist in a traffic classifier, **if-match any** matches only Layer 3 packets.

Example

Configure a matching rule based on all data packets in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match any
```

Related Topics

20.1.45 traffic classifier

20.1.12 if-match cvlan-8021p

 Copyright © Huawei Technologies Co., Ltd.

Function

The **if-match cvlan-8021p** command configures a matching rule based on the 802.1p priority in the inner tag of QinQ packets in a traffic classifier.

The **undo if-match cvlan-8021p** command deletes a matching rule based on the 802.1p priority in the inner tag of QinQ packets in a traffic classifier.

By default, a matching rule based on the 802.1p priority in the inner tag of QinQ packets is not configured in a traffic classifier.

Format

if-match cvlan-8021p *8021p-value* &<1-8>

undo if-match cvlan-8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in the inner tag of QinQ packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of QinQ packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match cvlan-8021p** command to classify packets based on the 802.1p priority in the inner tag of QinQ packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The **if-match cvlan-8021p** command is valid for only the double-tagged packets.

If you enter multiple 802.1p priorities in the inner tags of packets in the command, a packet matches a rule as long as it matches one of the 802.1p

 Copyright © Huawei Technologies Co., Ltd.

priorities in the inner tags of packets, regardless of whether the relationship between traffic classification rules is AND or OR.

If you run the **if-match cvlan-8021p** command multiple times in the same traffic classifier view, only the latest configuration takes effect.

Example

Configure a matching rule based on the inner 802.1p priority of 1 in QinQ packets in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match cvlan-8021p 1
```

Related Topics

20.1.45 traffic classifier

20.1.13 if-match cvlan-id

Function

The **if-match cvlan-id** command configures a matching rule based on the VLAN ID in the inner tag of QinQ packets in a traffic classifier. You can specify the VLAN ID range in the inner tag.

The **undo if-match cvlan-id** command deletes a matching rule based on the VLAN ID in the inner tag of QinQ packets in a traffic classifier.

By default, a matching rule based on the VLAN ID in the inner tag of QinQ packets is not configured in a traffic classifier.

Format

if-match cvlan-id *start-cvlan-id* [**to** *end-cvlan-id*]

undo if-match cvlan-id *start-cvlan-id* [**to** *end-cvlan-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start-cvlan-id [**to** *end-cvlan-id*]	Specifies the VLAN ID in the inner tag of a QinQ packet.	• *start-cvlan-id* specifies the start VLAN ID in the inner tag. The value is an integer that ranges from 1 to 4094. • *end-cvlan-id* specifies the end VLAN ID in the inner tag. The value is an integer that ranges from 1 to 4094. The value of *end-cvlan-id* must be larger than the value of *start-cvlan-id*. If **to** *end-cvlan-id* is not specified, only the VLAN ID specified by *start-cvlan-id* is matched.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match cvlan-id** command to classify packets based on the VLAN ID in the inner tag of QinQ packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

The **if-match cvlan-id** command is valid for only the double-tagged packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a matching rule based on the VLAN ID of 100 in the inner tag of QinQ packets in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match cvlan-id 100
```

Related Topics

20.1.45 traffic classifier

20.1.14 if-match destination-mac

Function

The **if-match destination-mac** command configures a matching rule based on the destination MAC address in a traffic classifier.

The **undo if-match destination-mac** command deletes a matching rule based on the destination MAC address in a traffic classifier.

By default, a matching rule based on the destination MAC address is not configured in a traffic classifier.

Format

if-match destination-mac *mac-address* [**mac-address-mask** *mac-address-mask*]

undo if-match destination-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-address-mask *mac-address-mask*	Specifies the mask of the destination MAC address. Similar to the mask of the IP address, the value F indicates that the destination MAC address is matched and the value 0 indicates that the destination MAC address is not matched. The mask of the MAC address determines a group of MAC addresses. The device can accurately match certain bits in the destination MAC address using the mask of the MAC address. In practice, you can set these bits to F in the mask of the destination MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits. The value cannot be 0-0-0.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match destination-mac** command to configure a matching rule based on the destination MAC address in a traffic classifier so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match destination-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a matching rule based on the destination MAC address of 0050-ba27-bed3 in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match destination-mac 0050-ba27-bed3
```

Configure a matching rule based on the destination MAC address of XX50-bXX7-bed3 in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match destination-mac 0050-b007-bed3 mac-address-mask 00ff-f00f-ffff
```

Related Topics

20.1.27 if-match source-mac

20.1.45 traffic classifier

20.1.15 if-match dlci

Function

The **if-match dlci** command configures a matching rule based on the data line connection identifier (DLCI) value of Frame Relay (FR) packets in a traffic classifier.

The **undo if-match dlci** command deletes a matching rule based on the DLCI value of FR packets in a traffic classifier.

By default, a matching rule based on the DLCI value of FR packets is not configured in a traffic classifier.

Format

if-match dlci *start-dlci-number* [**to** *end-dlci-number*]

undo if-match dlci *start-dlci-number* [**to** *end-dlci-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start-dlci-number [**to** *end-dlci-number*]	Specifies the DLCI value in FR packets. • *start-dlci-number* specifies the start DLCI value. • *end-dlci-number* specifies the end DLCI value. *end-dlci-number* must be larger than *start-dlci-number*. If *end-dlci-number* is not specified, only the start DLCI value is matched.	The values of *start-dlci-number* and *end-dlci-number* are integers in the range of 16 to 1022.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match dlci** command to classify FR packets based on the DLCI number so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match dlci** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on DLCI number 16 of FR packets in the traffic classifier **database**.

```
<Huawei> system-view
[Huawei] traffic classifier database
[Huawei-classifier-database] if-match dlci 16
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.1.1 classifier behavior
20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy

20.1.16 if-match dscp

Function

The **if-match dscp** command configures a matching rule based on the Differentiated Services Code Point (DSCP) priority of packets in a traffic classifier.

The **undo if-match dscp** command deletes a matching rule based on the DSCP priority of packets in a traffic classifier.

By default, a matching rule based on the DSCP priority of packets is not configured in a traffic classifier.

Format

if-match [**ipv6**] **dscp** *dscp-value* &<1-8>

undo if-match [**ipv6**] **dscp**

Parameters

Parameter	Description	Value
ipv6	Indicates that IPv6 packets are matched. If this parameter is not specified, IPv4 packets are matched.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dscp *dscp-value*	Specifies the DSCP priority.	The value can be a DiffServ code, an integer ranging from 0 to 63, or the name of the DSCP service type such as af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1-cs7, default, and ef. The values corresponding to service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match dscp** command to classify packets based on the DSCP priority of packets so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you enter multiple DSCP priorities in the command, a packet matches a rule as longs as it matches one of the DSCP priorities, regardless of whether the relationship between traffic classification rules is AND or OR.

In a traffic classifier where the relationship between rules is AND, the **if-match dscp** and **if-match ip-precedence** commands cannot be used simultaneously.

NOTE

A traffic policy containing **if-match ipv6 dscp** can be applied to only WAN-side interfaces.

If you run the **if-match dscp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the DSCP priority of 1 in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match dscp 1
```

Related Topics

20.1.19 if-match ip-precedence

20.1.45 traffic classifier

20.1.17 if-match fr-de

Function

The **if-match fr-de** command configures a matching rule based on the Discard Eligibility (DE) value of Frame Relay (FR) packets in a traffic classifier.

The **undo if-match fr-de** command deletes a matching rule based on the DE value of FR packets in a traffic classifier.

By default, a matching rule based on the DE value of FR packets is not configured in a traffic classifier.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR160 series does not support this command.

Format

if-match fr-de

undo if-match fr-de

Parameters

None

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The DE value of FR packets is set by the DTE such as a router or the FR network. On the FR network where congestion occurs, FR packets with the DE value of 1 are discarded without any notification, and FR packets with the DE value of 0 are not discarded.

You can run the **if-match fr-de** command to classify FR packets based on the DE value. The FR packets with the DE value of 1 are matched.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Example

Configure a matching rule based on the DE value of 1 in FR packets in the traffic classifier **database**.

```
<Huawei> system-view
[Huawei] traffic classifier database
[Huawei-classifier-database] if-match fr-de
```

Related Topics

20.1.1 classifier behavior

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

 Copyright © Huawei Technologies Co., Ltd.

20.1.18 if-match inbound-interface

Function

The **if-match inbound-interface** command configures a matching rule based on an inbound interface in a traffic classifier.

The **undo if-match inbound-interface** command deletes a matching rule based on an inbound interface in a traffic classifier.

By default, a matching rule based on an inbound interface is not configured in a traffic classifier.

Format

if-match inbound-interface *interface-type interface-number*

undo if-match inbound-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an inbound interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match inbound-interface** command to classify traffic based on an inbound interface so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- A traffic policy containing **if-match inbound-interface** can only be configured on WAN-side interfaces of the device.
- If you run the **if-match inbound-interface** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the inbound interface of Eth2/0/0 in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match inbound-interface ethernet 2/0/0
```

Related Topics

20.1.45 traffic classifier

20.1.19 if-match ip-precedence

Function

The **if-match ip-precedence** command configures a matching rule based on the IP precedence of packets in a traffic classifier.

The **undo if-match ip-precedence** command deletes a matching rule based on the IP precedence of packets in a traffic classifier.

By default, a matching rule based on the IP precedence of packets is not configured in a traffic classifier.

Format

if-match ip-precedence *ip-precedence-value* &<1-8>

undo if-match ip-precedence

Parameters

Parameter	Description	Value
ip-precedence-value	Specifies the IP precedence.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match ip-precedence** command to classify packets based on the IP precedence so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

After the **if-match ip-precedence** command is run, IP precedences are listed in ascending order.

If you enter multiple IP precedences in the **if-match ip-precedence** command, a packet matches a rule as long as it matches one of the IP precedence, regardless of whether the relationship between traffic classification rules is AND or OR.

In a traffic classifier where the relationship between rules is AND, the **if-match dscp** and **if-match ip-precedence** commands cannot be used simultaneously.

If you run the **if-match ip-precedence** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the IP precedence of 1 in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match ip-precedence 1
```

Related Topics

20.1.16 if-match dscp

20.1.19 if-match ip-precedence

20.1.45 traffic classifier

20.1.20 if-match l2-protocol

Function

The **if-match l2-protocol** command configures a matching rule based on the Layer 2 protocol type in a traffic classifier.

The **undo if-match l2-protocol** command deletes a matching rule based on the Layer 2 protocol type in a traffic classifier.

 Copyright © Huawei Technologies Co., Ltd.

By default, a matching rule based on the Layer 2 protocol type is not configured in a traffic classifier.

Format

if-match l2-protocol { **arp** | **ip** | **mpls** | **rarp** | *protocol-value* }

undo if-match l2-protocol

Parameters

Parameter	Description	Value
arp	Indicates that ARP packets are classified.	The value of **arp** corresponds to 0x0806.
ip	Indicates that IP packets are classified.	The value of **ip** corresponds to 0x0800.
mpls	Indicates that MPLS packets are classified.	The value of **mpls** corresponds to 0x8847.
rarp	Indicates that RARP packets are classified.	The value of **rarp** corresponds to 0x8035.
protocol-value	Specifies the value of a protocol type.	The value ranges from 0x0600 to 0xFFFF in hexadecimal notation and must start with 0x. The value of *protocol-value* must be larger than 0x600.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match l2-protocol** command to classify packets based on the Layer 2 protocol type so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The device supports Layer 2 protocols including ARP, IP, MPLS, and RARP.

NOTE

A traffic policy containing **if-match l2-protocol** that is applied to a LAN-side interface takes effect for only IPv4 packets.

If you run the **if-match l2-protocol** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Define a matching rule based on the protocol type of ARP in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match l2-protocol arp
```

Related Topics

20.1.45 traffic classifier

20.1.21 if-match mpls-exp

Function

The **if-match mpls-exp** command configures a matching rule based on the EXP priority of MPLS packets in a traffic classifier.

The **undo if-match mpls-exp** command deletes a matching rule based on the EXP priority of MPLS packets in a traffic classifier.

By default, a matching rule based on the EXP priority of MPLS packets is not configured in a traffic classifier.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support the **if-match mpls-exp** command.

Format

if-match mpls-exp *exp-value* &<1-8>

undo if-match mpls-exp

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
exp-value	Specifies the EXP priority of MPLS packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of MPLS packets.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match mpls-exp** command to classify MPLS packets based on the EXP priority so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you enter multiple values of EXP priorities in the command, a packet matches the traffic classifier as long as it matches one of the EXP priorities, regardless of whether the relationship between traffic classification rules is AND or OR.

A traffic policy containing **if-match mpls-exp** that is applied to the outbound direction does not take effect.

If you run the **if-match mpls-exp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the EXP priority of 1 or 4 in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match mpls-exp 1 4
```

Related Topics

20.1.45 traffic classifier

20.1.22 if-match outbound-interface

Function

The **if-match outbound-interface** command configures a matching rule based on an outbound cellular interface in a traffic classifier.

The **undo if-match outbound-interface** command deletes a matching rule based on an outbound cellular interface in a traffic classifier.

By default, no matching rule based on an outbound cellular interface is configured in a traffic classifier.

Format

if-match outbound-interface Cellular *interface-number:channel*

undo if-match outbound-interface

Parameters

Parameter	Description	Value
Cellular *interface-number*	Specifies the number of a cellular interface.	-
channel	Specifies the channel ID of a cellular interface.	The value is 1 or 2.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match outbound-interface** command to classify packets based on an outbound cellular interface so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

- The traffic policy that is bound to the traffic classifier based on the outbound interface can be only applied to the cellular interface in the outbound direction.
- If you run the **if-match outbound-interface** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the outbound interface of Cellular3/0/0:1 in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match outbound-interface Cellular 3/0/0:1
```

Related Topics

20.1.45 traffic classifier

20.1.23 if-match packet-length

Function

The **if-match packet-length** command configures a matching rule based on the IPv4 packet length in a traffic classifier.

The **undo if-match packet-length** command deletes a matching rule based on the IPv4 packet length in a traffic classifier.

By default, no matching rule based on the IPv4 packet length is configured in a traffic classifier.

Format

if-match packet-length *min-length* [**to** *max-length*]

undo if-match packet-length

Parameters

Parameter	Description	Value
min-length	Specifies the minimum value in the IPv4 packet length range if *max-length* is specified, or the IPv4 packet length if *max-length* is not specified.	The value is an integer that ranges from 1 to 16000, in bytes.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
to *max-length*	Specifies the maximum value in the IPv4 packet length range. If this parameter is not specified, the IPv4 packet length is matched.	The value is an integer that ranges from 1 to 16000, in bytes. The value of *max-length* must be larger than or equal to the value of *min-length*.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match packet-length** command to classify packets based on the IPv4 packet length so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

In the **if-match packet-length** command, the matched packet length is the IP packet header plus the data length, excluding the Ethernet packet header.

The **if-match packet-length** command cannot be used to match the IPv6 packet length.

If you run the **if-match packet-length** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the IPv4 packet length of 1000 bytes in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match packet-length 1000
```

Related Topics

20.1.45 traffic classifier

20.1.24 if-match protocol

Function

The **if-match protocol** command configures a matching rule based on a protocol in a traffic classifier.

The **undo if-match protocol** command deletes a matching rule based on a protocol in a traffic classifier.

By default, a matching rule based on a protocol is not configured in a traffic classifier.

Format

if-match protocol { **ip** | **ipv6** }

undo if-match protocol

Parameters

Parameter	Description	Value
ip	Indicates an IP protocol.	-
ipv6	Indicates an IPv6 protocol.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match protocol** command to classify packets based on a protocol so that the device processes packets of the same protocol in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

Currently, the device supports IPv4 and IPv6.

If you run the **if-match protocol** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a matching rule based on the IP protocol in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match protocol ip
```

Related Topics

20.1.45 traffic classifier

20.1.25 if-match qos-group

Function

The **if-match qos-group** command configures a matching rule for traffic classification based on the QoS group index in a traffic classifier.

The **undo if-match qos-group** command deletes a matching rule based on the QoS group index in a traffic classifier.

By default, no matching rule based on the QoS group index is configured in a traffic classifier.

Format

if-match qos-group *min-value* [**to** *max-value*]

undo if-match qos-group *min-value* [**to** *max-value*]

Parameters

Parameter	Description	Value
min-value [**to** *max-value*]	Specifies the QoS group ID ranges. • *min-value* specifies the ID of the first QoS group. • **to** *max-value* specifies the ID of the last QoS group. The value of *max-value* must be greater than the value of *min-value*. *max-value* and *min-value* identify a range of QoS groups. If **to** *max-value* is not specified, only the QoS group specified by *min-value* is displayed.	• The value of *min-value* is an integer that ranges from 1 to 99. • The value of *max-value* is an integer that ranges from 1 to 99.

 Copyright © Huawei Technologies Co., Ltd.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a QoS group of packets is specified, run the **if-match qos-group** command to configure a matching rule based on the QoS group index of packets in a traffic classifier so that the device can provide differentiated services.

Prerequisites

- Run the **remark qos-group** command in the traffic behavior view to configure the QoS group that packets belong to.

  NOTE

  A QoS group that packets belong to has been configured using the **qos group** command in the view of the IPSec policy in manual mode, view of the IPSec policy in ISAKMP mode, IPSec policy template view, IPSec profile view, or Efficient VPN policy view.

- A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If a QoS group is modified in an IPSec policy and the traffic policy matches the modified QoS group, run the **reset ipsec sa** or **reset ike sa** command to clear SAs and establish new SAs through re-negotiation.

The **if-match qos-group** and **if-match packet-length** commands cannot be configured in the same traffic classifier.

Example

Configure the device to match packets with QoS group 2 to 10 in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] traffic behavior b
[Huawei-behavior-b] remark qos-group 3
[Huawei-behavior-b] traffic classifier class1
[Huawei-classifier-class1] if-match qos-group 2 to 10
```

Related Topics

20.1.45 traffic classifier

20.1.40 remark qos-group

20.1.26 if-match rtp

Function

The **if-match rtp** command configures a matching rule based on the Real-time Transport Protocol (RTP) port number in a traffic classifier.

The **undo if-match rtp** command deletes a matching rule based on the RTP port number in a traffic classifier.

By default, a matching rule based on the RTP port number is not configured in a traffic classifier.

Format

if-match rtp start-port *start-port-number* **end-port** *end-port-number*

undo if-match rtp

Parameters

Parameter	Description	Value
start-port *start-port-number*	Specifies the start RTP port number.	The value is an integer that ranges from 2000 to 65535.
end-port *end-port-number*	Specifies the end RTP port number.	The value is an integer that ranges from 2000 to 65535. *end-port-number* must be larger than *start-port-number*.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match rtp** command to classify packets based on the RTP port number so that the device processes packets with even port numbers in the range of *start-port-number* and *end-port-number* matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

A traffic policy containing **if-match rtp** can only be configured on WAN-side interfaces of the device.

If you run the **if-match rtp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on even port numbers in the range of 2222 to 2666 in the traffic classifier **database**.

```
<Huawei> system-view
[Huawei] traffic classifier database
[Huawei-classifier-database] if-match rtp start-port 2222 end-port 2666
```

Related Topics

20.1.1 classifier behavior

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.1.27 if-match source-mac

Function

The **if-match source-mac** command configures a matching rule based on the source MAC address in a traffic classifier.

The **undo if-match source-mac** command deletes a matching rule based on the source MAC address in a traffic classifier.

By default, a matching rule based on the source MAC address is not configured in a traffic classifier.

Format

if-match source-mac *mac-address* [**mac-address-mask** *mac-address-mask*]

undo if-match source-mac

Parameters

Parameter	Description	Value
mac-address	Specifies the source MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mac-address-mask *mac-address-mask*	Specifies the mask of the source MAC address. Similar to the mask of the IP address, the mask of the MAC address determines a group of MAC addresses. The device can accurately match certain bits in the source MAC address using the mask of the MAC address. In practice, you can set these bits to F in the mask of the source MAC address.	The value is in H-H-H format. An H is a hexadecimal number of 4 digits. The value cannot be 0-0-0.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match source-mac** command to classify packets based on the source MAC address so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match source-mac** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the source MAC address of 0050-ba27-bed2 in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match source-mac 0050-ba27-bed2
```

 Copyright © Huawei Technologies Co., Ltd.

Configure a matching rule based on the source MAC address of XX50-bXX7-bed3 in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match source-mac 0050-ba27-bed3 mac-address-mask 00ff-f00f-ffff
```

Related Topics

20.1.14 if-match destination-mac

20.1.45 traffic classifier

20.1.28 if-match tcp

Function

The **if-match tcp** command configures a matching rule based on the SYN Flag in the TCP packet header in a traffic classifier.

The **undo if-match tcp** command deletes a matching rule based on the SYN Flag in the TCP packet header in a traffic classifier.

By default, a matching rule based on the SYN Flag in the TCP packet header is not configured in a traffic classifier.

Format

if-match tcp syn-flag { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }*

undo if-match tcp syn-flag

Parameters

Parameter	Description	Value
syn-flag	Specifies the SYN Flag in the TCP packet header.	-
ack	Indicates that the SYN Flag type in the TCP packet header is ACK.	-
fin	Indicates that the SYN Flag type in the TCP packet header is FIN.	-
psh	Indicates that the SYN Flag type in the TCP packet header is PSH.	-
rst	Indicates that the SYN Flag type in the TCP packet header is RST.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
syn	Indicates that the SYN Flag type in the TCP packet header is SYN.	-
urg	Indicates that the SYN Flag type in the TCP packet header is URG.	-

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match tcp** command to classify packets based on the SYN Flag in the TCP packet header so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

A traffic policy containing **if-match tcp** that is applied to a LAN-side interface takes effect for only IPv4 packets.

If you run the **if-match tcp** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the SYN Flag of psh in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match tcp syn-flag psh
```

Related Topics

20.1.45 traffic classifier

20.1.29 if-match user-set

Function

The **if-match user-set** command configures a matching rule based on the user group in a traffic classifier.

The **undo if-match user-set** command deletes a matching rule based on the user group in a traffic classifier.

By default, no matching rule based on the user group is configured in a traffic classifier.

NOTE

Only the AR100&AR120&AR150&AR160&AR200 series supports this command.

Format

if-match user-set *user-set-name* [**time-range** *time-range-name*]

undo if-match user-set

Parameters

Parameter	Description	Value
user-set-name	Specifies the name of a user group.	The value is a string of 1 to 32 case-sensitive characters without spaces.
time-range *time-range-name*	Specifies the time range during which traffic from a user group is limited. The time range must have been configured using the **time-range** command; otherwise, the time range does not take effect after the **if-match user-set** command is used.	The value is a string of 1 to 32 case-sensitive characters without spaces, starting with an upper-case or lower-case letter.

Views

Traffic classifier view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

You can run the **if-match user-set** command to configure a matching rule based on the user group in a traffic classifier so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A user group has been created using the **user-set** command.

Example

Define a matching rule to match packets from the user group **vip** in the traffic classifier **class1**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set vip
[Huawei-web-user-set-vip] quit
[Huawei-web] quit
[Huawei] traffic classifier class1 operator or
[Huawei-classifier-class1] if-match user-set vip
```

Related Topics

20.1.45 traffic classifier

19.7.24 time-range

20.8.6 user-set

20.1.30 if-match vlan-id

Function

The **if-match vlan-id** command configures a matching rule based on the VLAN ID of packets in a traffic classifier.

The **undo if-match vlan-id** command deletes a matching rule based on the VLAN ID of packets in a traffic classifier.

By default, a matching rule based on the VLAN ID of packets is not configured in a traffic classifier.

Format

if-match vlan-id *start-vlan-id* [**to** *end-vlan-id*]

undo if-match vlan-id *start-vlan-id* [**to** *end-vlan-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start-vlan-id [**to** *end-vlan-id*]	Specifies the outer VLAN ID.	• *start-vlan-id* specifies the start outer VLAN ID. The value of *start-vlan-id* is an integer that ranges from 1 to 4094. • *end-vlan-id* specifies the end outer VLAN ID. The value of *end-vlan-id* is an integer that ranges from 1 to 4094. *end-vlan-id* must be larger than *start-vlan-id*. If **to** *end-vlan-id* is not specified, only the VLAN ID specified by *start-vlan-id* is matched.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match vlan-id** command to classify packets based on the VLAN ID so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

A traffic classifier has been created using the **traffic classifier** command in the system view.

Example

Configure a matching rule based on VLAN 2 in the traffic classifier **c1**.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1] if-match vlan-id 2
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.1.45 traffic classifier

20.1.31 if-match pvc

Function

The **if-match pvc** command configures a matching rule based on the Permanent Virtual Circuit (PVC) of ATM packets in a traffic classifier.

The **undo if-match pvc** command deletes a matching rule based on the PVC of ATM packets in a traffic classifier.

By default, a matching rule based on the PVC of ATM packets is not configured in a traffic classifier.

Format

if-match pvc *vpi-number|vci-number*

undo if-match pvc *vpi-number|vci-number*

Parameters

Parameter	Description	Value
vpi-number|vci-number	Specifies the Virtual Path Identifier (VPI) or Virtual Channel Identifier (VCI) number.	• The VPI number is an integer that ranges from 0 to 255. • The VCI number is an integer that can be 0-2, or 5-65534.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match pvc** command to classify ATM packets based on the PVC so that the device processes packets matching the same traffic classifier in the same manner.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A traffic classifier has been created using the **traffic classifier** command in the system view.

Precautions

If you run the **if-match pvc** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure a matching rule based on the VPI/VCI pair of 1/101 in the traffic classifier **database**.

```
<Huawei> system-view
[Huawei] traffic classifier database
[Huawei-classifier-database] if-match pvc 1/101
```

Related Topics

20.1.1 classifier behavior

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.1.32 ip netstream sampler (traffic behavior view)

Function

The **ip netstream sampler** command configures an action of sampling IPv4 packets in a traffic behavior.

The **undo ip netstream** command deletes an action of sampling IPv4 packets in a traffic behavior.

By default, an action of sampling IPv4 packets is not configured in a traffic behavior.

Format

ip netstream sampler { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **multicast** | **rpf-failure** | **unicast** }*

undo ip netstream

Parameters

Parameter	Description	Value
fix-packets *packet-interval*	Specifies the number of packets between two sampled packets in the packet-based regular sampling.	The value is an integer that ranges from 1 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
fix-time *time-interval*	Specifies the sampling interval in time-based regular sampling.	The value is an integer that ranges from 5 to 30000, in milliseconds.
random-packets *packet-interval*	Specifies the number of packets between two sampled packets in the packet-based random sampling.	The value is an integer that ranges from 1 to 65535.
random-time *time-interval*	Specifies the sampling interval in time-based random sampling.	The value is as follows: ● 3.0 ● 6.0 ● 12.0 ● 24.0 ● 48.0 ● 96.0 ● 192.0 ● 383.5 ● 767.0 ● 1534.0 ● 3068.0 ● 6136.0 The unit is millisecond.
multicast	Enables sampling of multicast packets.	-
rpf-failure	Enables sampling of packets that fail the RPF check in a traffic behavior.	-
unicast	Enables sampling of unicast packets.	-

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can configure NetStream for packets matching a traffic classifier, and set a sampling mode and the sampling interval so that the device only analyzes statistics on packets matching the traffic classifier.

If you run the **ip netstream sampler** command multiple times in the same view, only the latest configuration takes effect.

Example

Configure sampling of multicast packets at intervals of 100 packets in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] ip netstream sampler fix-packets 100 multicast
```

Related Topics

21.12.13 ip netstream

20.1.33 qos pre-nat

Function

The **qos pre-nat** command enables NAT pre-classification.

The **undo qos pre-nat** command disables NAT pre-classification.

By default, NAT pre-classification is disabled.

Format

qos pre-nat

undo qos pre-nat

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the NAT-enabled device translates the private IP address of IP packets into the public IP address, the NAT-enabled device cannot identify the private IP address before translation on the outbound interface and cannot classify IP packets based on private IP addresses. NAT pre-classification enables the NAT-

enabled device to carry the private IP address before translation on the outbound interface so that the NAT-enabled device can classify IP packets based on private IP addresses and provide differentiated services.

Follow-up Procedure

Configure a traffic classifier, configure a matching rule based on private IP addresses, configure a traffic behavior for packets matching the traffic classifier, associate the traffic classifier with the traffic behavior in a traffic policy, and apply the traffic policy to the outbound interface of the NAT-enabled device.

Example

Enable NAT pre-classification on GE1/0/0 and configure traffic policing for packets matching private IP addresses.

```
<Huawei> system-view
[Huawei] acl 2001
[Huawei-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Huawei-acl-basic-2001] quit
[Huawei] nat address-group 1 10.2.2.2 10.2.2.3
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] qos pre-nat
[Huawei-GigabitEthernet1/0/0] quit
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match acl 2001
[Huawei-classifier-c1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] car cir 10000
[Huawei-behavior-b1] quit
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] traffic-policy p1 outbound
```

Related Topics

8.5.24 nat outbound

20.1.34 remark 8021p

Function

The **remark 8021p** command configures an action of re-marking the 802.1p priority in VLAN packets in a traffic behavior.

The **undo remark 8021p** command deletes the configuration.

By default, an action of re-marking the 802.1p priority in VLAN packets is not configured in a traffic behavior.

Format

remark 8021p *8021p-value*

undo remark 8021p

Parameters

Parameter	Description	Value
8021p-value	Specifies the 802.1p priority in VLAN packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority in VLAN packets.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the inner 802.1p priority in VLAN packets, run the **remark 8021p** command to configure the device to re-mark the inner 802.1p priority in VLAN packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing 8021.p priority re-marking.

Precautions

If a traffic policy containing **remark 8021p** is applied to the outbound direction on an interface, the device still processes outgoing packets based on the original priority but the downstream Layer 2 device processes the packets based on the re-marked priority.

If the **trust** command and a traffic policy containing **remark 8021p** are used on the same interface, **remark 8021p** in the traffic policy takes precedence over the **trust** command. Packet priorities are not affected by the **trust** command.

If you run the **remark 8021p** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark 802.1p priorities of VLAN packets with 4 in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark 8021p 4
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.1.9 if-match 8021p

20.1.44 traffic behavior

20.1.35 remark cvlan-8021p

Function

The **remark cvlan-8021p** command configures an action of re-marking the inner 802.1p priority in QinQ packets in a traffic behavior.

The **undo remark cvlan-8021p** command deletes the configuration.

By default, an action of re-marking the inner 802.1p priority in QinQ packets is not configured in a traffic behavior.

Format

remark cvlan-8021p *8021p-value*

undo remark cvlan-8021p

Parameters

Parameter	Description	Value
8021p-value	Re-marks the inner 802.1p priority in QinQ packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the inner 802.1p priority in QinQ packets, run the **remark cvlan-8021p** command to configure the upstream device to re-mark the inner 802.1p priority in QinQ packets in a traffic behavior.

Precautions

The **remark cvlan-8021p** command is valid only for QinQ packets that carry two or more layers of tags.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **remark cvlan-8021p** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the inner 802.1p priority in QinQ packets with 5 in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark cvlan-8021p 5
```

Related Topics

20.1.44 traffic behavior

20.1.36 remark dscp

Function

The **remark dscp** command configures an action of re-marking the DSCP priority in IP packets in a traffic behavior.

The **undo remark dscp** command deletes the configuration.

By default, an action of re-marking the DSCP priority in IP packets is not configured in a traffic behavior.

Format

remark dscp { *dscp-name* | *dscp-value* }

undo remark dscp

Parameters

Parameter	Description	Value
dscp-name	Specifies the DSCP priority name in IP packets.	The value can be **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.
dscp-value	Specifies the DSCP priority in IP packets.	The value is an integer that ranges from 0 to 63. A larger value indicates a higher priority.

Views

Traffic behavior view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the DSCP priority, run the **remark dscp** command to configure the device to re-mark the DSCP priority in IP packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing DSCP priority re-marking.

Precautions

If a traffic policy containing **remark dscp** is applied to the outbound direction on an interface, the device still processes outgoing packets based on the original priority but the downstream Layer 3 device or above processes the packets based on the re-marked priority.

If the **trust** command and a traffic policy containing **remark dscp** are used on the same interface, **remark dscp** in the traffic policy takes precedence over the **trust** command. Packet priorities are not affected by the **trust** command.

If you run the **remark dscp** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the DSCP priority in IP packets with 56 in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark dscp 56
```

Related Topics

20.1.44 traffic behavior

20.1.37 remark fr-de

Function

The **remark fr-de** command configures an action of re-marking the DE value in FR packets in a traffic behavior.

The **undo remark fr-de** command deletes the configuration.

By default, an action of re-marking the DE value in FR packets is not configured in a traffic behavior.

 Copyright © Huawei Technologies Co., Ltd.

Format

remark fr-de *fr-de-value*

undo remark fr-de

Parameters

Parameter	Description	Value
fr-de-value	Specifies the DE value in FR packets.	The value is 0 or 1.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **remark fr-de** command takes effect for FR packets with the DE value. The device replaces the DE value in FR packets sent on an interface by using the **remark fr-de** command. When FR packets with the DE value reach a downstream device through the device, you can run the **remark fr-de** command to re-mark the DE value in FR packets so that the downstream device can identify the packets.

Precautions

If you run the **remark fr-de** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Re-mark the DE value in FR packets to 1 in the traffic behavior **database**.

```
<Huawei> system-view
[Huawei] traffic behavior database
[Huawei-behavior-database] remark fr-de 1
```

Related Topics

20.1.1 classifier behavior

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

 Copyright © Huawei Technologies Co., Ltd.

20.1.38 remark local-precedence

Function

The **remark local-precedence** command configures an action of re-marking the internal priority in packets in a traffic behavior.

The **undo remark local-precedence** command deletes the configuration.

By default, an action of re-marking the internal priority in packets is not configured in a traffic behavior.

Format

remark local-precedence *local-precedence-value*

undo remark local-precedence

Parameters

Parameter	Description	Value
local-precedence-value	Specifies the internal priority value.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority. The value can be **af1**, **af2**, **af3**, **af4**, **be**, **cs6**, **cs7**, or **ef**. The values corresponding to internal priority names are as follows: ● af1: 1 ● af2: 2 ● af3: 3 ● af4: 4 ● be: 0 ● cs6: 6 ● cs7: 7 ● ef: 5

Views

Traffic behavior view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To provide differentiated services based on the internal priority of packets, run the **remark local-precedence** command to configure the device to re-mark the internal priority of packets so that the device can provide QoS based on the re-marked priority.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing internal priority re-marking.

Precautions

Re-marking the internal priority only affects QoS processing of packets on the device.

When **remark local-precedence** is defined in the traffic behavior, you are advised to apply the traffic policy containing the traffic behavior to the inbound direction of the interface.

If you run the **remark local-precedence** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the internal priority of packets with 2 in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark local-precedence 2
```

Related Topics

20.1.44 traffic behavior

20.1.39 remark mpls-exp

Function

The **remark mpls-exp** command configures an action of re-marking the EXP priority in MPLS packets in a traffic behavior.

The **undo remark mpls-exp** command deletes the configuration.

By default, an action of re-marking the EXP priority in MPLS packets is not configured in a traffic behavior.

NOTE

The AR100&AR120&AR150&AR160&AR200 series do not support this command.

Format

remark mpls-exp *exp-value*

undo remark mpls-exp

Parameters

Parameter	Description	Value
exp-value	Specifies the EXP priority of MPLS packets.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of MPLS packets.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To provide differentiated services based on the DSCP priority, run the **remark mpls-exp** command to configure the device to re-mark the EXP priority in MPLS packets in a traffic behavior.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing internal priority re-marking.

Precautions

If a traffic policy containing **remark mpls-exp** is applied to the outbound direction on an interface, the device still processes outgoing packets based on the original priority but the downstream device processes the packets based on the re-marked priority.

If the **trust** command and a traffic policy containing **remark mpls-exp** are used on the same interface, **remark mpls-exp** in the traffic policy takes precedence over the **trust** command. Packet priorities are not affected by the **trust** command.

If you run the **remark mpls-exp** command in the same traffic behavior view multiple times, only the latest configuration takes effect.

Example

Re-mark the EXP priority in MPLS packets with 4 in the traffic behavior **b1**.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark mpls-exp 4
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.1.21 if-match mpls-exp
20.1.44 traffic behavior

20.1.40 remark qos-group

Function

The **remark qos-group** command configures a QoS group that packets belong to.

The **undo remark qos-group** command deletes a QoS group that packets belong to.

By default, the QoS group that packets belong to is not configured.

Format

remark qos-group *qos-group-value*

undo remark qos-group

Parameters

Parameter	Description	Value
qos-group-value	Specifies the ID of a QoS group.	The value is an integer that ranges from 1 to 99.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the QoS group that packets belong to is specified, the device classifies packets to implement QoS management.

Follow-up Procedure

After the QoS group that packets belong to is configured, run the **if-match qos-group** command in the traffic classifier view to create a matching rule based on the QoS group.

Precautions

After the QoS group that packets belong to is configured, packets are not modified and the configuration is not delivered to the downstream device.

 Copyright © Huawei Technologies Co., Ltd.

A QoS group that IPSec packets belong to has been configured using the **qos group** command in the view of the IPSec policy in manual mode, view of the IPSec policy in ISAKMP mode, IPSec policy template view, IPSec profile view, or Efficient VPN policy view.

Example

Configure QoS group 2 that packets belong to in the traffic behavior view.

```
<Huawei> system-view
[Huawei] traffic behavior b
[Huawei-behavior-b] remark qos-group 2
```

Related Topics

20.1.44 traffic behavior

20.1.25 if-match qos-group

20.1.41 reset traffic policy statistics

Function

The **reset traffic policy statistics** command clears traffic statistics on an interface to which a traffic policy has been applied.

Format

reset traffic policy statistics interface *interface-type interface-number* [**pvc** *vpi-number/vci-number* | **dlci** *dlic-number*] { **inbound** | **outbound** }

reset traffic policy statistics interface virtual-template *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears traffic statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
pvc *vpi-number/vci-number*	Specifies the Virtual Path Identifier (VPI)/Virtual Channel Identifier (VCI) pair. The VPI/VCI pair can be specified on only ATM interfaces.	• *vpi-number* is an integer that ranges from 0 to 255. • *vci-number* is an integer that can be 0-2, or 5-255.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dlci *dlic-number*	Specifies the DLCI number. The DLCI number can be specified on only serial or MFR interfaces.	The value is an integer that ranges from 16 to 1022.
virtual-template *vt-number* **virtual-access** *va-number*	Clears traffic statistics on a specified virtual interface. • **virtual-template** *vt-number* specifies the number of a virtual template interface. • **virtual-access** *va-number* specifies the number of a virtual access interface.	The value of *vt-number* is an integer that ranges from 0 to 1023. The value of *va-number* is an integer that ranges from 0 to 1023.
inbound	Clears traffic statistics in the inbound direction.	-
outbound	Clears traffic statistics in the outbound direction.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before recollecting statistics on packets matching a traffic policy on an interface, run the **reset traffic policy statistics** command to clear existing packet statistics. Then run the **display traffic policy statistics** command to view packet statistics.

Precautions

The cleared traffic statistics cannot be restored. Exercise caution when you use the command.

If no traffic policy is applied, the system displays an error message after the **reset traffic policy statistics** command is executed:

```
Error: The Policy is not applied in this view.
```

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays an error message after the **reset traffic policy statistics** command is executed:

```
Info: Statistic has not been enabled.
```

Example

Clear traffic statistics on Eth2/0/0 in the inbound direction to which a traffic policy has been applied.

```
<Huawei> reset traffic policy statistics interface ethernet 2/0/0 inbound
```

Related Topics

20.1.5 display traffic policy statistics

20.6.1 statistic enable (traffic behavior view)

20.1.46 traffic policy

20.1.42 reset traffic policy statistics bridge-domain

Function

The **reset traffic policy statistics bridge-domain** command clears statistics on packets matching a traffic policy that is applied to a BD.

NOTE

Only AR100&AR120&AR150&AR160&AR200&AR1200 series and AR2220E support this command.

Format

reset traffic policy statistics bridge-domain *bd-id* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
bd-id	Clears statistics on packets matching a traffic policy that is applied to a specified BD.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256
inbound	Clears statistics on packets matching a traffic policy that is applied to a BD in the inbound direction.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
outbound	Clears statistics on packets matching a traffic policy that is applied to a BD in the outbound direction.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To re-collect statistics on packets matching a traffic policy that is applied to a BD, run the **display traffic policy statistics bridge-domain** command to check packet statistics and run the **reset traffic policy statistics bridge-domain** command to clear existing packet statistics.

Configuration Notes

After the **reset traffic policy statistics bridge-domain** command is executed, packet statistics are cleared and cannot be restored. Exercise caution when you use this command.

If you do not run the **statistics enable (traffic behavior view)** command in the view of the traffic behavior bound to the traffic policy, the system displays an error message after the **reset traffic policy statistics bridge-domain** command is executed:

```
Info: Statistic has not been enabled!
```

Example

Clear statistics on packets matching a traffic policy that is applied to BD 1 in the outbound direction.

```
<Huawei> reset traffic policy statistics bridge-domain 1 outbound
```

Related Topics

20.1.6 display traffic policy statistics bridge-domain

20.6.1 statistic enable (traffic behavior view)

20.1.47 traffic-policy (BD view)

 Copyright © Huawei Technologies Co., Ltd.

20.1.43 reset traffic policy statistics global

Function

The **reset traffic policy statistics global** command clears statistics on packets matching a global traffic policy.

Format

reset traffic policy statistics global

Parameters

None

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before recollecting statistics on packets matching a global traffic policy, run the **reset traffic policy statistics global** command to clear existing packet statistics. Then run the **display traffic policy statistics global** command to view packet statistics.

Precautions

The cleared traffic statistics cannot be restored. Exercise caution when you use this command.

If you do not run the **statistic enable (traffic behavior view)** command in the view of the traffic behavior in a traffic policy, the system displays an error message after the **reset traffic policy statistics** command is executed:

```
Info: Statistic has not been enabled.
```

Example

Clear statistics on packets matching a global traffic policy.

```
<Huawei> reset traffic policy statistics global
```

Related Topics

20.1.7 display traffic policy statistics global

 Copyright © Huawei Technologies Co., Ltd.

20.1.44 traffic behavior

Function

The **traffic behavior** command creates a traffic behavior and displays the traffic behavior view, or directly displays the view of an existing traffic behavior.

The **undo traffic behavior** command deletes a traffic behavior.

By default, the traffic behavior **be** exists in the system.

Format

traffic behavior *behavior-name*

undo traffic behavior *behavior-name*

Parameters

Parameter	Description	Value
behavior-name	Specifies the name of a traffic behavior.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A traffic classifier is used to differentiate services and must be associated with a flow control or resource allocation action such as packet filtering, traffic policing, and re-marking. The actions constitute a traffic behavior. The **traffic behavior** command creates a traffic behavior.

Follow-up Procedure

Configure an action in the traffic behavior view. For example, run the **car (traffic behavior view)** command to configure the traffic policing action.

Precautions

The default traffic behavior **be** exists in the system. This traffic behavior cannot be deleted or modified.

To delete a traffic behavior, unbind the traffic policy containing the traffic behavior from an interface and unbind the traffic behavior from a traffic classifier in the

 Copyright © Huawei Technologies Co., Ltd.

traffic policy. To modify only actions in a traffic behavior, you do not need to unbind the traffic policy containing the traffic behavior from an interface.

On the device, a maximum of 1024 traffic behaviors can be created and multiple traffic actions can be configured in a traffic behavior.

Example

Create the traffic behavior **b1** and enter the traffic behavior view.

```
<Huawei> system-view
[Huawei] traffic behavior b1
[Huawei-behavior-b1]
```

Related Topics

20.1.1 classifier behavior
20.1.2 display traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy

20.1.45 traffic classifier

Function

The **traffic classifier** command creates a traffic classifier and displays the traffic classifier view, or directly displays the view of an existing traffic classifier.

The **undo traffic classifier** command deletes a traffic classifier.

By default, the traffic classifier **default-class** exists in the system.

Format

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

undo traffic classifier *classifier-name*

Parameters

Parameter	Description	Value
classifier-name	Specifies the name of a user-defined traffic classifier.	The value is a string of 1 to 31 case-sensitive characters without spaces.
operator	Specifies the relationship between rules in a traffic classifier. If this parameter is not specified, the relationship between rules is OR by default.	-

Parameter	Description	Value
and	Indicates that the relationship between rules is AND. After this parameter is specified, the following situations occur: ● If a traffic classifier contains ACL rules, packets match the traffic classifier only when the packets match one ACL rule and all the non-ACL rules. ● If a traffic classifier does not contain ACL rules, packets match the traffic classifier only when the packets match all the non-ACL rules.	-
or	Indicates that the relationship between rules is OR. After this parameter is specified, packets match a traffic classifier if the packets match one or more rules.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A traffic classifier classifies traffic of a certain type using matching rules. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior (see **traffic behavior**) to a traffic policy and apply the traffic policy.

A traffic classifier can be created based on Layer 2 information such as the 802.1p priority in the VLAN ID, 802.1p priority in the C-VLAN ID, VLAN ID, or Layer 2

protocol type, and Layer 3 information such as the DSCP priority or IP priority, or ACLs.

Follow-up Procedure

Define rules in the traffic classifier. For example, run the **if-match 8021p** command to define rules based on the 802.1p priority in the VLAN tag.

Precautions

The default traffic classifier **default-class** exists in the system. This traffic classifier cannot be deleted or modified.

To delete a traffic classifier, unbind the traffic policy containing the traffic classifier from an interface and unbind the traffic classifier from a traffic behavior in the traffic policy. To modify a traffic classifier, you do not need to unbind the traffic policy containing the traffic classifier from an interface.

A maximum of 1024 traffic classifiers can be created on the device.

NOTE

After the relationship between rules in a traffic classifier is changed, the system checks whether rules conflict. When the relationship between rules is changed from OR to AND and multiple rules are configured, for example, matching rules based on the 802.1p priority in the inner tag, DSCP priority, IP precedence, and VLAN ID, the rules may conflict and the system displays a message indicating that the relationship cannot be changed. The relationship between rules can be changed from AND to OR but services may be affected because more packets are matched. Exercise caution when you change the relationship between rules.

Example

Create a traffic classifier **c1** and enter the traffic classifier view.

```
<Huawei> system-view
[Huawei] traffic classifier c1 operator and
[Huawei-classifier-c1]
```

Related Topics

20.1.1 classifier behavior
20.1.3 display traffic classifier
20.1.44 traffic behavior
20.1.46 traffic policy

20.1.46 traffic policy

Function

The **traffic policy** command creates a traffic policy and displays the traffic policy view, or displays the view of an existing traffic policy.

The **undo traffic policy** command deletes a traffic policy.

By default, no traffic policy is created in the system.

Format

traffic policy *policy-name* [**match-extended**]

undo traffic policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value is a string of 1 to 31 case-sensitive characters without spaces
match-extended	Set the matching mode of traffic classifiers in a traffic policy to extended.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are obtained based on Layer 2 information, Layer 3 information, or ACLs. To implement differentiated services for service flows of packets, bind a traffic classifier and a traffic behavior to the created traffic policy and apply the traffic policy. You can use the **traffic policy** command to create a traffic policy. A maximum of 1024 traffic policies can be created on the device.

When a traffic policy is bound to two or more than two pairs of traffic classifiers and traffic behaviors, packets first match the deny rule in a traffic classifier, and **match-extended** is specified, packets are not discarded. The device continues to match packets with rules in the subsequent traffic classifier. If packets do not match any rule, packets are forwarded based on the original forwarding path. If the permit rule is defined, packets are processed based on the action in a traffic behavior.

Pre-configuration Tasks

A traffic classifier and a traffic behavior have been created.

Follow-up Procedure

- Run the **classifier behavior** command in the traffic policy view to associate the traffic policy with a traffic classifier and a traffic behavior.
- Run the **traffic-policy (interface view)** command to apply the traffic policy to an interface to make the created traffic policy take effect.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

If the traffic policy that you want to delete has been applied to an interface, run the **undo traffic-policy** command to unbind the traffic policy from the interface. Then run the **undo traffic policy** command in the system view to delete the traffic policy. If the traffic policy is not applied, delete it directly.

Example

Create a traffic policy **p1**, and associate the traffic classifier **c1** with the traffic behavior **b1** in the traffic policy.

```
<Huawei> system-view
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match any
[Huawei-classifier-c1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark 8021p 2
[Huawei-behavior-b1] quit
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
```

Delete the traffic policy **p1** that has been applied to the inbound indirection on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo traffic-policy inbound
[Huawei-Ethernet2/0/0] quit
[Huawei] undo traffic policy p1
```

After the traffic policy p is applied to Ethernet2/0/0 in the outbound direction, the packets that match the traffic classifier **c1** are not denied. The device continues to match packets with the traffic classifier **c2** and processes the packets based on the action defined in the traffic behavior **b2**.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule deny ip source 10.10.1.1 0
[Huawei-acl-adv-3000] quit
[Huawei] acl 3001
[Huawei-acl-adv-3001] rule permit ip source 10.10.1.2 0
[Huawei-acl-adv-3001] quit
[Huawei] traffic classifier c1 operator or
[Huawei-classifier-c1] if-match acl 3000
[Huawei-classifier-c1] quit
[Huawei] traffic classifier c2 operator or
[Huawei-classifier-c2] if-match acl 3001
[Huawei-classifier-c2] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] statistic enable
[Huawei-behavior-b1] quit
[Huawei] traffic behavior b2
[Huawei-behavior-b2] statistic enable
[Huawei-behavior-b2] quit
[Huawei] traffic policy p match-extended
[Huawei-trafficpolicy-p] classifier c1 behavior b1
[Huawei-trafficpolicy-p] classifier c2 behavior b2
[Huawei-trafficpolicy-p] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] traffic-policy p outbound
```

Related Topics

20.1.1 classifier behavior

20.1.4 display traffic policy
20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.49 traffic-policy (interface view)

20.1.47 traffic-policy (BD view)

Function

The **traffic-policy** command applies a traffic policy to a BD.

The **undo traffic-policy** command unbinds a traffic policy from a BD.

By default, no traffic policy is applied to a BD.

NOTE

Only AR100&AR120&AR150&AR160&AR200&AR1200 series and AR2220E support this command.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

undo traffic-policy { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value is an integer. The value ranges are as follows: • AR100&AR120&AR150&AR160&AR200 series: 1-64 • AR1200 series: 1-128 • AR2220E: 1-256
inbound	Applies a traffic policy to a BD in the inbound direction.	-
outbound	Applies a traffic policy to a BD in the outbound direction.	-

Views

BD view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACL rules. To implement differentiated services for service flows, bind a traffic classifier and a traffic behavior to the created traffic policy and apply the traffic policy. The **traffic-policy** command applies a traffic policy to a BD.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

NOTE

The traffic behavior of the traffic policy that is applied to the BD can only define the following actions: packet filtering, priority re-marking, traffic policing, NetStream sampling, and traffic statistics.

Configuration Notes

Only one traffic policy can be applied to each direction in a BD, but a traffic policy can be applied to different directions in different BDs.

After a traffic policy is applied, you cannot directly delete the traffic policy or traffic classifiers or traffic behaviors in the traffic policy. If the traffic policy that you want to delete has been applied to a BD, run the **undo traffic-policy** command to unbind the traffic policy. Then run the **undo traffic policy** command in the system view to delete the traffic policy.

Example

Create a traffic policy named **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to BD 10 in the inbound direction.

```
<Huawei> system-view
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match any
[Huawei-classifier-c1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] remark 8021p 2
[Huawei-behavior-b1] quit
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] bridge-domain 10
[Huawei-bd10] traffic-policy p1 inbound
```

Related Topics

20.1.1 classifier behavior
20.1.4 display traffic policy
20.1.44 traffic behavior

20.1.45 traffic classifier
20.1.46 traffic policy

20.1.48 traffic-policy (interzone view)

Function

The **traffic-policy** command binds a traffic policy to an interzone.

The **undo traffic-policy** command unbinds a traffic policy from an interzone.

By default, no traffic policy is bound to an interzone.

NOTE

Only AR100&AR120&AR150&AR160&AR200 series support this command.

Format

traffic-policy *policy-name*

undo traffic-policy *policy-name*

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy to be bound to an interzone.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Interzone view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After a traffic policy is created, the traffic policy must be bound to an interzone so that the bound traffic classifiers and traffic behaviors in the traffic policy take effect and differentiated services are implemented.

Prerequisites

The **firewall interzone** command has been executed to create an interzone and enter the interzone view.

 Copyright © Huawei Technologies Co., Ltd.

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Example

Bind the traffic policy **security** to an interzone.

```
<Huawei> system-view
[Huawei] firewall zone zone1
[Huawei-zone-zone1] priority 10
[Huawei-zone-zone1] quit
[Huawei] firewall zone zone2
[Huawei-zone-zone2] priority 13
[Huawei-zone-zone2] quit
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match dscp 0
[Huawei-classifier-c1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] statistic enable
[Huawei-behavior-b1] quit
[Huawei] traffic policy security
[Huawei-trafficpolicy-security] classifier c1 behavior b1
[Huawei-trafficpolicy-security] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone2-zone1] traffic-policy security
```

Related Topics

19.8.51 firewall interzone

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.1.49 traffic-policy (interface view)

Function

The **traffic-policy** command applies a traffic policy to an interface.

The **undo traffic-policy** command deletes a traffic policy from an interface.

By default, no traffic policy is applied to an interface.

Format

traffic-policy *policy-name* { **inbound** | **outbound** }

undo traffic-policy { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
inbound	Applies a traffic policy to the inbound direction.	-
outbound	Applies a traffic policy to the outbound direction.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets are classified based on Layer 2 information, Layer 3 information, or ACLs. To provide differentiated services for service flows, bind a traffic classifier and a traffic behavior to a traffic policy and apply the traffic policy. You can use the **traffic-policy** command to apply a created traffic policy to an interface.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

- Only one traffic policy can be applied to each direction on an interface, but a traffic policy can be applied to different directions on different interfaces.
- When traffic policy nesting is applied to a sub-interface, the traffic policy that is bound to sub traffic policies can be bound to only one pair of the traffic classifier and traffic behavior and only the default traffic classifier **default-class** can be used.
- If the traffic policy that you want to delete has been applied to an interface, run the **undo traffic-policy** command to unbind the traffic policy from the interface. Then run the **undo traffic policy** command in the system view to delete the traffic policy.
- Except for the 8FE1GE and 24GE, the configuration is invalid during LAN-side data switching.

Example

Create a traffic policy **p1**, bind the created traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and apply the traffic policy to the inbound direction on Eth2/0/0.

```
<Huawei> system-view
[Huawei] traffic policy p1
```

```
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] traffic-policy p1 inbound
```

Related Topics

20.1.1 classifier behavior

20.1.4 display traffic policy

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.1.50 traffic-policy (traffic behavior view)

Function

The **traffic-policy** command configures an action of binding a sub traffic policy in a traffic behavior.

The **undo traffic-policy** command deletes the action of binding a sub traffic policy from a traffic behavior.

By default, an action of binding a sub traffic policy is not configured in a traffic behavior.

Format

traffic-policy *policy-name*

undo traffic-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a user-defined traffic policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

On the WAN-side interface, a traffic behavior in a traffic policy can be bound to a sub traffic policy. The sub traffic policy is used to configure queue scheduling and traffic shaping. The **traffic-policy** command binds a sub traffic policy to a traffic behavior so that the device can provide differentiated services.

Prerequisites

A sub traffic policy has been configured.

Precautions

The traffic policy whose sub traffic policy is bound to a traffic behavior can be applied to only the WAN interface.

To apply traffic policy nesting to the inbound direction of an interface or a sub-interface, the traffic behavior of a traffic policy only can be statistic and sub traffic policy.

Example

Bind the sub traffic policy **tp-son** to the traffic behavior **tb1**.

```
<Huawei> system-view
[Huawei] traffic behavior tb1
[Huawei-behavior-tb1] traffic-policy tp-son
```

Related Topics

20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy

20.1.51 traffic-policy global bind interface

Function

The **traffic-policy global bind interface** command applies a traffic policy to the system of an AR and binds this traffic policy to an interface.

The **undo traffic-policy global bind interface** command unbinds the globally applied traffic policy from an interface.

By default, no traffic policy is applied to the system or bound to any interface of an AR.

Format

traffic-policy *policy-name* **global bind interface** { *interface-type interface-number* }&<1-16>

undo traffic-policy global bind interface [*interface-type interface-number*]&<1-16>

Parameters

Parameter	Description	Value
policy-name	Specifies the name of a traffic policy.	The value is a string of 1 to 31 case-sensitive characters without spaces.
interface-type interface-number	Specifies the interface to which the traffic policy is bound. • *interface-type*: Specifies the interface type. • *interface-number*: Specifies the interface number.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic classifiers can be used to classify traffic and traffic behaviors to implement refined traffic processing. If the traffic policy is bound to interfaces of the AR, these interfaces process all entering traffic based on this traffic policy in the same manner.

Prerequisites

A traffic policy has been created using the **traffic policy** command, and traffic classifiers and traffic behaviors have been bound to the traffic policy.

Precautions

Only one traffic policy can apply to the system of an AR, and the traffic policy takes effect only for inbound traffic.

If you run the **traffic-policy global bind interface** command multiple times to bind the traffic policy to multiple interfaces, the traffic policy takes effect on all these interfaces.

If you run the **undo traffic-policy global bind interface** command without setting the *interface-type* and *interface-number* parameters, the global traffic policy will be unbound from all bound interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Classifiers in a global traffic policy cannot be used to match the EXP field of MPLS packets or applied to IPv6 packets. The **remark mpls-exp** action cannot be configured in a global traffic policy.

If an interface-based traffic policy is applied to the interface where a global traffic policy is applied, the traffic policies take effect according to the following rules:

- If the redirecting action is configured in both traffic policies, only the redirecting behavior in the interface-based traffic policy is valid.
- In other cases, the device executes the traffic behavior in the interface-based traffic policy and then the traffic behavior in the global traffic policy.

The globally applied traffic policy can be bound only to GE, Ethernet, and VLANIF interfaces.

NOTE

- After a traffic policy is applied to an AR, this traffic policy as well as bound traffic classifiers or traffic behaviors cannot be directly deleted. To delete a traffic policy applied to an AR, run the **undo traffic-policy global bind interface** command in the system view to cancel the application of the traffic policy and then run the **undo traffic policy** command.
- This configuration does not take effect when the AR transfers LAN-side data.

Example

Create a traffic policy named **p1**, and bind the traffic classifier **c1** and traffic behavior **b1** to the traffic policy, and bind it to an interface of the AR.

```
<Huawei> system-view
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] traffic-policy p1 global bind interface GigabitEthernet0/0/1
```

Related Topics

20.1.46 traffic policy

20.1.52 url-filter-profile

Function

The **url-filter-profile** command binds a URL filtering profile to a traffic behavior.

The **undo url-filter-profile** command unbinds a URL filtering profile from a traffic behavior.

By default, no URL filtering profile is bound to a traffic behavior.

NOTE

Only AR100&AR120&AR150&AR160&AR200 series support this command.

Format

url-filter-profile *profile-name*

undo url-filter-profile

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a URL filtering profile.	The value is a string of case-sensitive characters. The value cannot contain question marks (?), commas (,), double quotation marks ("), and hyphens (-). ● The value contains 1 to 32 characters if the value does not contain spaces. ● If the value contains spaces, you must enclose the value with double quotation marks (""), for example, "user for test". The value is a string of 3 to 34 characters.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

With rapid development of Internet applications and popularity of computer networks, acquisition, sharing, and dissemination of information have become more widespread than ever, which brings unprecedented threats to enterprises.

- Employees visit non-work-related websites during working hours, reducing the working efficiency.
- Visiting illegal or malicious websites may result in threats such as worms, viruses, and Trojan horses.

After a URL filtering profile is bound to a traffic behavior, bind the traffic behavior and traffic classifier to a traffic policy and apply the traffic policy to the interzone so that URL filtering takes effect. URL filtering regulates online behaviors by controlling which URLs users can access.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A URL filtering profile has been created using the **profile type url-filter name** command.

Follow-up Procedure

1. Create a traffic policy and run the **classifier behavior** command in the traffic policy view to associate the traffic policy with traffic classifiers and traffic behaviors.
2. Run the **traffic-policy (interzone view)** command in the interzone view to apply the traffic policy.

   NOTE

   If the traffic policy is applied to an interface, URL filtering is unavailable.

Precautions

When a traffic behavior is bound to multiple URL filtering profiles, only the URL filtering profile that is first bound to the traffic behavior takes effect.

Example

Bind the traffic behavior **b1** to the URL filtering profile **abc**, bind the traffic behavior **b1** and traffic classifier **c1** to the traffic policy **p1**, and apply the traffic policy **p1** to the interzone.

```
<Huawei> system-view
[Huawei] profile type url-filter name abc
[Huawei-profile-url-filter-abc] quit
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match 8021p 2
[Huawei-classifier-c1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] url-filter-profile abc
[Huawei-behavior-b1] quit
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] firewall interzone zone1 zone2
[Huawei-interzone-zone2-zone1] traffic-policy p1
```

Related Topics

19.9.3.19 profile type url-filter name

20.1.1 classifier behavior

20.1.48 traffic-policy (interzone view)

20.2 Priority Mapping Commands

20.2.1 display qos map-table

Function

The **display qos map-table** command displays the mapping between priorities.

Format

display qos map-table [**dot1p-dot1p** | **dot1p-dscp** | **dscp-lp** | **dscp-dot1p** | **dscp-dscp**] (AR100&AR120&AR150&AR160&AR200 series)

display qos map-table [**dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp** | **exp-exp**] (AR1200 series, AR2220E, AR2204, AR2220L and AR2240C)

display qos map-table [**dot1p-dot1p** | **dot1p-dscp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** | **dscp-lp** | **exp-exp** | **exp-lp**] (AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2204-24GE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2220, AR2240, AR3200&AR3600 series)

Parameters

Parameter	Description	Value
dot1p-dot1p	Specifies the name of the mapping table. That is, the mapping between 802.1p priorities.	-
dot1p-dscp	Specifies the name of the mapping table. That is, the mapping from 802.1p priorities to Differentiated Services Code Point (DSCP) priorities.	-
dot1p-lp	Specifies the name of the mapping table. That is, the mapping from 802.1p priorities to local priorities.	-
dscp-dot1p	Specifies the name of the mapping table. That is, the mapping from DSCP priorities to 802.1p priorities.	-
dscp-dscp	Specifies the name of the mapping table. That is, the mapping between DSCP priorities.	-
dscp-lp	Specifies the name of the mapping table. That is, the mapping from DSCP priorities to local priorities.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
exp-exp	Specifies the name of the mapping table. That is, the mapping between MPLS EXP priorities.	-
exp-lp	Specifies the name of the mapping table. That is, the mapping from MPLS EXP priorities to local priorities.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before and after configuring the mapping between priorities, you can use the **display qos map-table** command to check whether the priority mapping is correct.

Example

Display the mapping between the current DSCP priorities and Dot1p priorities.

```
<Huawei> display qos map-table dscp-dot1p
Input DSCP       Dot1P
------------------------
0                0
1                0
2                0
3                0
4                0
5                0
6                0
7                0
......
```

Display all the mappings between the current priorities on AR3200&AR3600 series.

```
<Huawei> display qos map-table
Input Dot1p      LP
-------------------
 0               0
 1               1
 2               2
 3               3
 4               4
 5               5
 6               6
 7               7
```

 Copyright © Huawei Technologies Co., Ltd.

```
Input Dot1p      Dot1p
-------------------
 0               0
 1               1
 2               2
 3               3
 4               4
 5               5
 6               6
 7               7
Input Dot1p      DSCP
-------------------
 0               0
 1               8
 2               16
 3               24
 4               32
 5               40
 6               48
 7               56
Input DSCP      LP
-------------------
 0               0
 1               0
 2               0
 3               0
 4               0
 5               0
 6               0
 7               0
......
Input DSCP      Dot1p
-------------------
 0               0
 1               0
 2               0
 3               0
 4               0
 5               0
 6               0
 7               0
......
Input DSCP      DSCP
-------------------
 0               0
 1               1
 2               2
 3               3
 4               4
 5               5
 6               6
 7               7
......
Input EXP     LP
-------------------
 0               0
 1               1
 2               2
 3               3
 4               4
 5               5
 6               6
 7               7
Input EXP      EXP
-------------------
 0               0
 1               1
 2               2
 3               3
```

```
4          4
5          5
6          6
7          7
```

Table 20-8 Description of the display qos map-table command output

Item	Description
Input Dot1p	Input 802.1p priority. The value is an integer that ranges from 0 to 7. To set the input 802.1p priority, run the **input** command.
Input DSCP	Input DSCP priority. The value is an integer that ranges from 0 to 63. To set the input DSCP priority, run the **input** command.
Dot1p	Output 802.1p priority. The value is an integer that ranges from 0 to 7. To set the output 802.1p priority, run the **input** command.
DSCP	Output DSCP priority. The value is an integer that ranges from 0 to 63. To set the output DSCP priority, run the **input** command.
LP	Output local priority. The value is an integer that ranges from 0 to 7. To set the output local priority, run the **input** command.
Input EXP	Input MPLS EXP priority. The value is an integer that ranges from 0 to 7. To set the input MPLS EXP priority, run the **input** command.
EXP	Output MPLS EXP priority. The value is an integer that ranges from 0 to 7. To set the output MPLS EXP priority, run the **input** command.

NOTE

A larger value indicates a higher priority.

Related Topics

20.2.2 input

20.2.4 qos map-table

20.2.2 input

Function

The **input** command configures the mapping between priorities.

The **undo input** command restores the default mapping between priorities.

The default setting is as follows:

- **Table 20-9** lists the mapping from Dot1p priorities to DSCP priorities supported by the AR120&AR150&AR160&AR200 series, AR1200 series, AR2240C, AR2220E, and AR2204. The mapping from Dot1p priorities to Dot1p priorities remains unchanged. **Table 20-11** lists the mapping from DSCP priorities to Dot1p priorities. The mapping from DSCP priorities to DSCP priorities remains unchanged. The mapping from MPLS EXP priorities to MPLS EXP priorities remains unchanged.
- **Table 20-10** lists the mapping from Dot1p priorities to DSCP priorities and from Dot1p priorities to local priorities supported by the AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series. The mapping from Dot1p priorities to Dot1p priorities remains unchanged. **Table 20-12** lists the mapping from DSCP priorities to Dot1p priorities and from DSCP priorities to local priorities. The mapping from DSCP priorities to DSCP priorities remains unchanged. **Table 20-13** lists the mapping from MPLS EXP priorities to local priorities. The mapping from MPLS EXP priorities to MPLS EXP priorities remains unchanged.

Table 20-9 Mapping from 802.1p priorities to DSCP priorities (AR120&AR150&AR160&AR200 series, AR1200 series, AR2220E, AR2240C, and AR2204)

Input Dot1p	Output DSCP
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

Table 20-10 Mapping from 802.1p priorities to DSCP priorities, and local priorities (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series)

Input Dot1p	Output DSCP	Output LP
0	0	0
1	8	1
2	16	2

 Copyright © Huawei Technologies Co., Ltd.

Input Dot1p	Output DSCP	Output LP
3	24	3
4	32	4
5	40	5
6	48	6
7	56	7

Table 20-11 Mapping from DSCP priorities to 802.1p priorities (AR120&AR150&AR160&AR200 series,AR1200 series, AR2220E, AR2240C, and AR2204)

Input DSCP	Output Dot1p
0-7	0
8-15	1
16-23	2
24-31	3
32-39	4
40-47	5
48-55	6
56-63	7

Table 20-12 Mapping from DSCP priorities to 802.1p priorities, and local priorities (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series)

Input DSCP	Output Dot1p	Output LP
0-7	0	0
8-15	1	1
16-23	2	2
24-31	3	3
32-39	4	4
40-47	5	5
48-55	6	6

 Copyright © Huawei Technologies Co., Ltd.

Input DSCP	Output Dot1p	Output LP
56-63	7	7

Table 20-13 Mapping from MPLS EXP priorities to local priorities, and local priorities (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series)

Input MPLS EXP	Output LP
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Format

input { *input-value1* [**to** *input-value2*] } &<1-10> **output** *output-value*

undo input { **all** | { *input-value1* [**to** *input-value2*] } &<1-10> }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

NOTE

802.1p priority mapping table views include:

- dot1p-dot1p view and dot1p-dscp view (AR120&AR150&AR160&AR200 series, AR2240C, AR1200 series, AR2204, AR2220E)
- dot1p-dot1p view, dot1p-dscp view, and dot1p-lp view (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200, AR3600 series)

DSCP priority mapping table views include:

- dscp-dot1p view and dscp-dscp view (AR120&AR150&AR160&AR200 series, AR2240C, AR1200 series, AR2204, AR2220E)
- dscp-dot1p view, dscp-dscp view, and dscp-lp view (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200, AR3600 series)

MPLS EXPpriority mapping table views include:

- exp-exp view (AR1200 series, AR2204, AR2220E, AR2240C)
- exp-exp view, exp-lp view (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200, AR3600 series)

Parameter	Description	Value
input-value1	• Specifies the start input 802.1p priority in the 802.1p priority mapping table view. • Specifies the start input DSCP priority in the DSCP priority mapping table view. • Specifies the start input EXP priority in the MPLS EXP priority mapping table view.	• In the 802.1p priority mapping table view, the value is an integer that ranges from 0 to 7. • In the DSCP priority mapping table view, the value is an integer that ranges from 0 to 63. • In the MPLS EXP priority mapping table view, the value is an integer that ranges from 0 to 7. A greater value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
to *input-value2*	• Specifies the end input 802.1p priority in the 802.1p priority mapping table view. • Specifies the end input DSCP priority in the DSCP priority mapping table view. • Specifies the end input EXP priority in the MPLS EXP priority mapping table view.	The value of *input-value2* and the value of *input-value1* determine the priority range. • In the 802.1p priority mapping table view, the value is an integer that ranges from 0 to 7. • In the DSCP priority mapping table view, the value is an integer that ranges from 0 to 63. • In the MPLS EXP priority mapping table view, the value is an integer that ranges from 0 to 7. A greater value indicates a higher priority.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
output-value	• 802.1p priority mapping table views: – Specifies the output 802.1p or DSCP priority. (AR120&AR150&AR160&AR200 series, AR1200 series, AR2204, AR2240C, AR2220E) – Specifies the output 802.1p, DSCP, or local priority. (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200&AR3600 series) • DSCP priority mapping table views: – Specifies the output 802.1p or DSCP priority. (AR120&AR150&AR160&AR200 series, AR1200 series, AR2240C, AR2204, AR2220E) – Specifies the output 802.1p, DSCP, or local priority. (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E,	• 802.1p priority mapping table views: – In the dot1p-dot1p view, the value is an integer that ranges from 0 to 7. – In the dot1p-dscp view, the value is an integer that ranges from 0 to 63. – In the dot1p-lp view, the value is an integer that ranges from 0 to 7. (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200&AR3600 series) • DSCP priority mapping table views: – In the dscp-dot1p view, the value is an integer that ranges from 0 to 7. – In the dscp-dscp view, the value is an integer that ranges from 0 to 63. – In the dscp-lp view, the value is an integer that ranges from 0 to 7. (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P,

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
	AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200&AR3600 series) ● MPLS EXP priority mapping table views: – Specifies the output MPLS EXP priority. (AR1200 series, AR2240C, AR2204, AR2220E) – Specifies the output MPLS EXP or local priority. (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200&AR3600 series)	AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200&AR3600 series) ● MPLS EXP priority mapping table views: – In the exp-exp view, the value is an integer that ranges from 0 to 7. – In the exp-lp view, the value is an integer that ranges from 0 to 7. (AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2220, AR2240, AR3200&AR3600 series) A greater value indicates a higher priority.
all	● Specifies all the 802.1p priority mapping in the 802.1p priority mapping table view. ● Specifies all the DSCP priority mapping in the DSCP priority mapping table view. ● Specifies all the MPLS EXP priority mapping in the MPLS EXP priority mapping table view.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

Priority mapping table view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Different packets carry different priorities. For example, VLAN packets carry 802.1p priorities, IP packets carry DSCP priorities.

- When packets enter a device, the device sends packets to queues based on the mapping between packet priorities and local priorities.
- When packets go out of a device, the connected downstream device guarantees QoS based on the mapping.

When a data packet is sent from a Layer 3 network to a Layer 2 network, the DSCP priority of the data packet is mapped to the 802.1p priority. When a data packet is sent from a Layer 2 network to a Layer 3 network, the 802.1p priority of the data packet is mapped to the DSCP priority.

You can use the **input** command to configure the mapping between priorities so that packets enter queues based on packet priorities. Differentiated services can be provided.

Precautions

If you run the **input** command multiple times in the same priority mapping table view, only the latest configuration takes effect.

Example

Configure the mapping in the DSCP priority mapping table: DSCP priorities 0 to 15 are mapped to 802.1p priority 0 and the mapping between DSCP priorities 16 to 63 and 802.1p priorities remains unchanged.

```
<Huawei> system-view
[Huawei] qos map-table dscp-dot1p
[Huawei-maptbl-dscp-dot1p] input 0 to 15 output 0
```

Related Topics

20.2.1 display qos map-table
20.2.4 qos map-table

20.2.3 port priority

Function

The **port priority** command configures the priority for an interface.

The **undo port priority** command restores the default priority of an interface.

By default, the priority of an interface is 0.

Format

port priority *priority-value*

undo port priority

Parameters

Parameter	Description	Value
priority-value	Specifies the priority of an interface.	The value is an integer that ranges from 0 to 7. A larger value indicates a higher priority of an interface.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Scenario

The 802.1p priority is determined by the 3-bit priority 802.1p field contained in a VLAN tag. The 802.1p priority is used to ensure QoS in the DiffServ model.

If this command is not used, packets enter queue 0. When this command is used, packets are processed as follows.

 Copyright © Huawei Technologies Co., Ltd.

Interface Configuration	Whether a Received Packet Carries a VLAN Tag	Processing Method
Setting the interface priority	No	The AR100&AR120&AR150&AR160&AR200&AR1200&AR2200 (except the AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220 and AR2240) series searches for an entry mapping the 802.1p priority, modifies the packet priority, and sends the packet to a queue. The AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series searches for an entry mapping the 802.1p priority and sends the packet to a queue.

 Copyright © Huawei Technologies Co., Ltd.

Interface Configuration	Whether a Received Packet Carries a VLAN Tag	Processing Method
Setting the interface priority	Yes	The AR100&AR120&AR150&AR160&AR200&AR1200&AR2200 (except the AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220 and AR2240) series searches for an entry mapping the 802.1p priority, modifies the packet priority, and sends the packet to a queue. The AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series searches for an entry mapping the 802.1p priority and sends the packet to a queue.
trust 8021p override	No	The device searches for an entry mapping the default 802.1p priority, modifies the packet priority, and sends the packet to a queue.

 Copyright © Huawei Technologies Co., Ltd.

Interface Configuration	Whether a Received Packet Carries a VLAN Tag	Processing Method
trust 8021p	No	The AR100&AR120&AR150&AR160&AR200&AR1200&AR2200 (except the AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220 and AR2240) series searches for an entry mapping the 802.1p priority, modifies the packet priority, and sends the packet to a queue. The AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series searches for an entry mapping the 802.1p priority and sends the packet to a queue.

Precautions

If you run the **port priority** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Set the priority of Eth2/0/0 to 1.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port priority 1
```

20.2.4 qos map-table

Function

The **qos map-table** command displays the Dot1p, MPLS EXP, or DSCP priority mapping table view.

Format

qos map-table { **dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp** } (AR100&AR120&AR150&AR160&AR200 series)

qos map-table { **dot1p-dot1p** | **dot1p-dscp** | **dscp-dot1p** | **dscp-dscp** | **exp-exp** } (AR1200 series, AR2204, AR2220E, AR2240C)

qos map-table { **dot1p-dot1p** | **dot1p-dscp** | **dot1p-lp** | **dscp-dot1p** | **dscp-dscp** | **dscp-lp** | **exp-exp** | **exp-lp** } (AR2201-48FE, AR2202-48FE, AR2220, AR2240, AR3200&AR3600 series)

qos map-table { **dot1p-dot1p** | **dscp-dot1p** }(AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R, AR2204-51GE, AR2204E, AR2204E-D)

Parameters

Parameter	Description	Value
dot1p-dot1p	Displays the dot1p-dot1p view. The dot1p-dot1p table contains the mapping between 802.1p priorities.	-
dot1p-dscp	Displays the dot1p-dscp view. The dot1p-dscp table contains the mapping between 802.1p priorities and DSCP priorities.	-
dot1p-lp	Displays the dot1p-lp view. The dot1p-lp table contains the mapping between 802.1p priorities and local priorities.	-
dscp-dot1p	Displays the dscp-dot1p view. The dscp-dot1p table contains the mapping between DSCP priorities and 802.1p priorities.	-
dscp-dscp	Displays the dscp-dscp view. The dscp-dscp table contains the mapping between DSCP priorities and DSCP priorities.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dscp-lp	Displays the dscp-lp view. The dot1p-lp table contains the mapping between DSCP priorities and local priorities.	-
exp-exp	Displays the exp-exp view. The exp-exp table contains the mapping between MPLS EXP priorities and MPLS EXP priorities.	-
exp-lp	Displays the exp-lp view. The exp-exp table contains the mapping between MPLS EXP priorities and local priorities.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before mapping received packets based on the DSCP priority, MPLS EXP priority, or Dot1p priority, run the **qos map-table** command to enter the priority mapping table view.

Follow-up Procedure

Run the **input** command to configure the mapping.

Example

Enter the dscp-dot1p view.

```
<Huawei> system-view
[Huawei] qos map-table dscp-dot1p
[Huawei-maptbl-dscp-dot1p]
```

Related Topics

20.2.1 display qos map-table
20.2.2 input

20.2.5 trust

20.2.5 trust

Function

The **trust** command specifies the priority to be mapped for packets.

The **undo trust** command cancels the configuration.

By default, the interface priority is used and packet priorities are not trusted.

Format

trust { **8021p** [**override**] | **dscp** [**override**] | **exp** }

NOTE

AR100&AR120&AR150&AR160&AR200 series do not support **exp**.

undo trust

Parameters

Parameter	Description	Value
8021p	Maps packets based on the 802.1p priority.	-
dscp	Maps packets based on the DSCP priority.	-
override	Allows the packet priority to be changed to the mapped priority.	-
exp	Maps packets based on the MPLS EXP priority.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device sends packets to different queues based on packet priorities. By default, the interface does not trust packet priorities. Packets enter queues according to the port priority.

 Copyright © Huawei Technologies Co., Ltd.

If all the packets enter queues according to the interface priority, all the packets on an interface enter the same queue. Differentiated services cannot be provided. The **trust** command specifies the priority to be mapped for packets so that packets with different priorities enter different queues. The device provides differentiated services using queue scheduling.

- The AR100&AR120&AR150&AR160&AR200&AR1200&AR2200 (except the AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220, AR2240) series sends packets to queues based on the mapped 802.1p priority.
- The AR2204XE, AR2204XE-DC, AR2201-48FE, AR2202-48FE, AR2220, AR2240 and AR3200&AR3600 series sends packets to queues based on the mapped local priority.

Precautions

Different interfaces support different parameters in the **trust** command. For example, only GE interfaces and its sub-interfaces, FE interfaces and its sub-interfaces, and PON interfaces and its sub-interfaces support **8021p**. Only WAN interfaces including Layer 3 XGE interfaces and its sub-interfaces, GE interfaces and its sub-interfaces, Layer 3 FE interfaces and its sub-interfaces, and IMA-Group interfaces support **exp**. The supported parameters depend on device models.

If a sub-interface is not configured to trust a type of the priority, packets are mapped according to the priority trusted by the main interface. If a sub-interface is also configured to trust a type of the priority, packets are mapped according to the priority trusted by the sub-interface.

- On the AR100&AR120&AR150&AR160&AR200&AR1200 series, AR2204-27GE, AR2204-27GE-P, AR2204E-D-27GE, AR2204-51GE-P, AR2204-51GE-R or AR2204, if **override** is not specified, the 8021.p priority of packets is changed to the mapped value and the DSCP priority of packets remains unchanged after the packets are mapped based on the specified priority. If **override** is specified, 802.1p priorities and DSCP priorities in packets are changed to mapped values after the packets are mapped based on the specified priority.
- On the AR2201-48FE, AR2204E, AR2204E-D, AR2202-48FE, AR2220E, AR2220, AR2240, AR2240C, or AR3200&AR3600 series, if **override** is not specified, packet priorities are not changed after the packets are mapped based on the specified priority. If **override** is specified, 802.1p priorities and DSCP priorities in packets are changed to mapped values after the packets are mapped based on the specified priority.

If the **trust** command and a traffic policy containing **remark 8021p** or **remark dscp** are used on the same interface, **remark 8021p** or **remark dscp** in the traffic policy takes precedence over the **trust** command. Packet priorities are not affected by the **trust** command.

If you run the **trust** command multiple times on the same interface, only the latest configuration takes effect.

Example

Configure Eth2/0/0 to trust DSCP priorities.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] trust dscp
```

Related Topics

20.1.36 remark dscp
20.1.34 remark 8021p

20.3 Traffic Policing and Traffic Shaping Commands

20.3.1 bandwidth

Function

The **bandwidth** command sets the base value for the percentage of the CIR to the interface bandwidth in MQC-based traffic policing.

The **undo bandwidth** command cancels the base value for the percentage of the CIR to the interface bandwidth in MQC-based traffic policing.

By default, the base value for the percentage of the CIR to the interface bandwidth is not set in MQC-based traffic policing.

Format

bandwidth *bandwidth-value* [**kbps**]

undo bandwidth

Parameters

Parameter	Description	Value
bandwidth-value	Specifies the base value for the percentage of the CIR to the interface bandwidth in MQC-based traffic policing.	The value is an integer that ranges from 1 to 1000000, and the default unit is Mbit/s.
kbps	Indicates the unit of an interface bandwidth is kbit/s. If **kbps** is not specified, the unit of an interface bandwidth is Mbit/s.	-

Views

Dialer interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

In MQC-based traffic policing, you can specify the percentage of the CIR. By default, the actual interface bandwidth is used as the base value for the percentage of the CIR. You can run the **bandwidth** *bandwidth-value* command to set the base value for the percentage of the CIR. For example, when *cir-percentage* in the **car cir pct** *cir-percentage* command is set to 10 and *bandwidth-value* in the **bandwidth** *bandwidth-value* command is set to 20 Mbit/s, the rate limit is 2 Mbit/s (20 Mbit/s x 10%).

Example

Set the base value for the percentage of the CIR to the interface bandwidth in MQC-based traffic policing to 20 Mbit/s.

```
<Huawei> system-view
[Huawei] interface dialer 0
[Huawei-Dialer0] bandwidth 20
```

Related Topics

20.3.2 car (traffic behavior view)

20.3.2 car (traffic behavior view)

Function

The **car** command configures traffic policing in a traffic behavior.

The **undo car** command deletes traffic policing from a traffic behavior.

By default, traffic policing is not configured in a traffic behavior.

Format

car cir { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (AR100&AR120&AR150&AR160&AR200)

car cir { *cir-value* | **pct** *cir-percentage* } [**pir** { *pir-value* | **pct** *pir-percentage* }] [**cbs** *cbs-value* **pbs** *pbs-value*] [**share**] [**mode** { **color-blind** | **color-aware** }] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] (AR1200, AR2200, AR3200, AR3600)

undo car

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cir	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	-
cir-value	Specifies the absolute value of the CIR.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
pct *cir-percentage*	Specifies the percentage of the CIR to the interface bandwidth.	The value is an integer that ranges from 1 to 100.
pir	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	-
pir-value	Specifies the absolute value of the PIR.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be higher than or equal to the CIR. The default PIR is equal to the CIR.
pct *pir-percentage*	Specifies the percentage of the PIR to the interface bandwidth.	The value is an integer that ranges from 1 to 100.
share	Indicates that all the rules in a traffic classifier bound to a traffic behavior share CAR parameters.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. The default setting is as follows: ● If the PIR is not set or the PIR and CIR are the same, the CBS is 188 times the CIR. ● If the PIR is set and the PIR and CIR are different, the CBS is 125 times the CIR.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. The default setting is as follows: ● If the PIR is not set or the PIR and CIR are the same, the PBS is 313 times the CIR. ● If the PIR is set and the PIR and CIR are different, the PBS is 125 times the PIR.
mode	Indicates the color mode for a traffic behavior in the traffic policy. This parameter is valid for only the traffic behavior in the traffic policy.	-
color-blind	Indicates the color-blind mode. In color-blind mode, a traffic behavior in the sub traffic policy does not affect the traffic policing action.	-
color-aware	Indicates the color-aware mode. In color-aware mode, a traffic behavior in the sub traffic policy affects the traffic policing action.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
yellow **green** **red**	Specifies the packet color. By default, green packets and yellow packets are allowed to pass through, and red packets are discarded.	-
discard	Discards packets of a color.	-
pass	Permits packets of a color to pass through.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remark-dscp *dscp-value*	Re-marks the DSCP priority of packets of a color.	The value can be the DiffServ code, an integer ranging from 0 to 63; the value can also be the name of the DSCP service type, such as af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1-cs7, default, and ef. The values corresponding to names of DSCP service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46
remark-8021p *8021p-value*	Re-marks the 802.1p priorities of packets.	The value is an integer that ranges from 0 to 7.
remark-mpls-exp *exp-value*	Re-marks the EXP priorities of packets.	The value is an integer that ranges from 0 to 7.

 Copyright © Huawei Technologies Co., Ltd.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Flow-based traffic policing controls traffic that matches traffic classification rules and discards the excess traffic to limit traffic within a proper range and to protect network resources.

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate so that the outgoing traffic rate is limited within a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

Traffic policing based on traffic policies controls rates of packets of different types.

Traffic policing actions include permit, deny, and forward based on the changed priority. By default, green packets and yellow packets are allowed to pass through, and red packets are discarded.

- You can change the methods for processing packets in different colors received on WAN interfaces. For example, if you change the DSCP priority, EXP priority, or 802.1p priority of green packets before forwarding them, the connected device can provide QoS services based on the changed priority.
- The device cannot discard the green packets received on LAN interfaces or change priorities of these packets.
- The device cannot discard the green or yellow packets sent from LAN interfaces.

Prerequisites

A traffic behavior has been created using the **traffic behavior** command.

Precautions

When traffic policing is performed for the packets received on LAN interfaces, CAR is separately performed for packets forwarded to LAN and WAN interfaces. The configured rate limit may be twice the actual CAR value.

When the CBS is smaller than the number of bytes in a packet, packets of this type are discarded.

To prevent a device failure to identify the packet color, you are advised to set the PBS to be larger than the CBS.

 Copyright © Huawei Technologies Co., Ltd.

When the minimum granularity of traffic policing is larger than the maximum rate of an interface, traffic policing does not take effect on the interface. You need to set the CIR or PIR to be smaller than the maximum rate of the interface.

On LAN interfaces of devices:

- On the Layer 2 FE interface of the AR121, AR121W, AR121GW-L, AR129GW-L and AR150&AR200 series, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s.
- On the Layer 2 GE interface of the AR129CV, AR129CVW, AR129CVW-L, AR100&AR160 series, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s. When the traffic policing rate is in the range of 100 Mbit/s to 1 Gbit/s, the traffic policing rate is a multiple of 10 Mbit/s.
- On the FE interface of the SRU of the AR1220, ARAR1220F, AR1220V, AR1220W and AR1220VW, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s.
- On the GE interface of the SRU of the AR1220-8GE, AR1220C, AR1220E, AR1220EV and AR1220EVW, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s. When the traffic policing rate is in the range of 100 Mbit/s to 1 Gbit/s, the traffic policing rate is a multiple of 10 Mbit/s.
- On LAN interfaces of the AR2200&AR3200&AR3600 series, the traffic policing rate is a multiple of 64 kbit/s. If the CIR is set to 64 x *n* kbit/s, the traffic policing rate is 64 x *n* kbit/s. If the CIR is larger than 64 x *n* kbit/s and is smaller than 64 x (*n* + 1) kbit/s, the traffic policing rate is 64 x *n* kbit/s.
- On other LAN interfaces, the traffic policing rate is a multiple of 64 kbit/s. If the CIR is set to 64 x *n* kbit/s, the traffic policing rate is 64 x *n* kbit/s. If the CIR is larger than 64 x *n* kbit/s and is smaller than 64 x (*n* + 1) kbit/s, the traffic policing rate is 64 x *n* kbit/s.

Only WAN-side interfaces support the percentage of the CIR to the interface bandwidth and the percentage of the PIR to the interface bandwidth. You must use either absolute values of the CIR and PIR or the percentages of the CIR and PIR to the interface bandwidth.

When you use the bandwidth percentage for setting the CIR and PIR, the bandwidth varies depending on the interface type:

- The bandwidth is the actual physical bandwidth of a physical interface.
- The bandwidth of a tunnel interface or virtual Ethernet interface is 1 Gbit/s.
- The bandwidth of a logical interface such as the Eth-Trunk, MP-Group interface or MFR interface, that is bundled by multiple interfaces or sub-interfaces is the total bandwidth of all bundled interfaces or sub-interfaces.
- The bandwidth of a dialer interface is the actual bandwidth of a physical interface bound to the dialer interface or the bandwidth sum of multiple physical interfaces.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

When a virtual template interface is bound to L2TP services, the percentage of the CIR or PIR to the interface bandwidth cannot be set on the virtual template interface.

The traffic policing action in the traffic policy configured for outbound traffic on the LAN-side interface of the device is invalid for replicated multicast packets.

Example

Configure traffic policing in the traffic behavior **tb1**: Set the CIR to 384 kbit/s and the PIR to 768 kbit/s, permit green packets to be sent, forward yellow packets after the DSCP priority of yellow packets is re-marked with 0, and discard red packets.

```
<Huawei> system-view
[Huawei] traffic behavior tb1
[Huawei-behavior-tb1] car cir 384 pir 768 green pass yellow pass remark-dscp 0 red discard
```

Related Topics

20.1.5 display traffic policy statistics

20.1.44 traffic behavior

20.1.46 traffic policy

20.3.3 car (QoS profile view)

Function

The **car** command configures traffic policing in a QoS profile.

The **undo car** command deletes the traffic policing configuration from the QoS profile.

By default, traffic policing is not configured in a QoS profile.

Format

car cir *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] { **inbound** | **outbound** }

undo car { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the guaranteed average transmission rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate of traffic that can pass through an interface.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be higher than or equal to the CIR. The default PIR is equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in Bytes. If the PIR is not set, the default CBS is 188 times the CIR. If the PIR is set, the default CBS is 125 times the CIR.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in Bytes. If the PIR is not set, the default PBS is 313 times the CIR. If the PIR is set, the default PBS is 125 times the PIR.
inbound	Indicates inbound traffic policing.	-
outbound	Indicates outbound traffic policing.	-

Views

QoS profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing discards excess traffic to limit traffic within a proper range and to protect network resources.

The **car** command configures traffic policing in a QoS profile.

Follow-up Procedure

Apply the QoS profile in the AAA service scheme view.

Precautions

When the traffic policing rate is larger than the maximum bandwidth of an interface, traffic policing does not take effect on the interface. Set the CIR and PIR to be smaller than the rate of an interface.

When the CBS is smaller than the number of bytes in a packet, the device directly discards the packet.

Example

Create a QoS profile named **huawei** in which the CIR is set to 10000 kbit/s, the CBS is set to 10240 bytes, and the PBS is set to 10240 bytes.

```
<Huawei> system-view
[Huawei] qos-profile huawei
[Huawei-qos-profile-huawei] car cir 10000 cbs 10240 pbs 10240 inbound
```

Related Topics

20.3.18 qos-profile

20.3.4 display qos-profile

Function

The **display qos-profile** command displays the configured QoS profile information.

Format

display qos-profile [*profile-name*]

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a QoS profile.	The value must the name of an existing QoS profile.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display qos-profile** command displays the configuration of a specified QoS profile or all QoS profiles. The command output helps you check the QoS profile configuration and locate QoS faults.

Example

Display the summary configurations of all QoS profiles.

```
<Huawei> display qos-profile
qos-profile a1:
  car cir 1000 cbs 188000 pbs 313000 inbound

qos-profile a2:
  statistics enable
```

Table 20-14 Description of the **display qos-profile** command output

Item	Description
qos-profile a1	Name of the QoS profile.
car cir 1000 cbs 188000 pbs 313000 inbound	CAR in the inbound direction.
statistics enable	Whether the traffic statistics function is configured.

Related Topics

20.3.18 qos-profile

20.3.3 car (QoS profile view)

20.3.5 display qos adaptation-profile

Function

The **display qos adaptation-profile** command displays the adaptive traffic profile configuration.

Format

display qos adaptation-profile [*adaptation-profile-name*]

Parameters

Parameter	Description	Value
adaptation-profile-name	Specifies the name of an adaptive traffic profile.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

A maximum of 4 adaptive traffic profiles can be configured on the AR150&AR200 series.

A maximum of 8 adaptive traffic profiles can be configured on theAR100&AR120&AR160 series.

A maximum of 16 adaptive traffic profiles can be configured on the AR1200 series.

A maximum of 64 adaptive traffic profiles can be configured on the AR2200 series.

A maximum of 256 adaptive traffic profiles can be configured on the AR3200&AR3600 series.

You can use the **display qos adaptation-profile** command to view the number of configured adaptive traffic profiles and the detailed configuration of a specified adaptive traffic profile.

If the adaptive traffic profile name is not specified, the **display qos adaptation-profile** command displays the indexes and names of all the configured adaptive traffic profiles, maximum number of adaptive traffic profiles in the system, and number of configured adaptive traffic profiles. If the adaptive traffic profile name is specified, the **display qos adaptation-profile** command displays the detailed configuration of the adaptive traffic profile.

Example

Display the indexes and names of all the configured adaptive traffic profiles.

```
<Huawei> display qos adaptation-profile
     Index                Adaptation-profile name
-----------------------------------------------------------------
     0                    gts1
```

```
     1                    gts2
-----------------------------------------------------------------
 Total   256     Used   2
```

Display the detailed configuration of the adaptive traffic profile **gts1**.

```
<Huawei> dis qos adaptation-profile gts1
Adaptation-profile: gts1
-----------------------------------------------------------------
Rate lower threshold: 2048(Kbps)
Rate upper threshold: 3072(Kbps)
Low rate adjustment threshold on packet loss: 20(%)
High rate adjustment threshold on packet loss: 30(%)
Rate step: 128(Kbps)
Rate increase interval: 50(s)
NQA admin Name: admin
NQA test Name: jitter
-----------------------------------------------------------------
```

Table 20-15 Description of the **display qos adaptation-profile** command output

Item	Description
Index	Adaptive traffic profile index.
Adaptation-profile name	Adaptive traffic profile name.
Total	Maximum number of adaptive traffic profiles in the system.
Used	Number of configured adaptive traffic profiles.
Adaptation-profile	Adaptive traffic profile name.
Rate lower threshold	Lower threshold for the traffic shaping rate. To set the lower threshold for the traffic shaping rate, run the **rate-range** command.
Rate upper threshold	Upper threshold for the traffic shaping rate. To set the upper threshold for the traffic shaping rate, run the **rate-range** command.
Low rate adjustment threshold on packet loss	Lower threshold for the packet loss ratio. To set the lower threshold for the packet loss ratio, run the **rate-adjust loss** command.
High rate adjustment threshold on packet loss	Upper threshold for the packet loss ratio. To set the upper threshold for the packet loss ratio, run the **rate-adjust loss** command.
Rate step	Traffic shaping rate adaptation step. To set the traffic shaping rate adaptation step, run the **rate-adjust step** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Rate increase interval	Interval at which the traffic shaping rate increases. To set the interval at which the traffic shaping rate increases, run the **rate-adjust increase interval** command.
NQA admin Name	Administrator name for the NQA test instance bound to the adaptive traffic profile. To set the administrator name for the NQA test instance bound to the adaptive traffic profile, run the **track nqa** command.
NQA test Name	Name of the NQA test instance bound to the adaptive traffic profile. To set the name of the NQA test instance bound to the adaptive traffic profile, run the **track nqa** command.

Related Topics

20.3.11 qos adaptation-profile
20.3.19 rate-adjust increase interval
20.3.20 rate-adjust loss
20.3.21 rate-adjust step
20.3.22 rate-range
20.3.24 track nqa

20.3.6 display qos adaptation-profile applied-record

Function

The **display qos adaptation-profile applied-record** command displays the record of a specified adaptive traffic profile.

Format

display qos adaptation-profile *adaptation-profile-name* [**interface** *interface-type interface-number*] **applied-record**

display qos adaptation-profile *adaptation-profile-name* **interface virtual-template** *vt-number* **virtual-access** *va-number* **applied-record**

Parameters

Parameter	Description	Value
adaptation-profile-name	Displays the record of a specified adaptive traffic profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.
interface *interface-type interface-number*	Displays the record of a specified adaptive traffic profile on a specified interface: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
virtual-template *vt-number*	Displays the queue-based traffic statistics on a specified virtual template interface. *vt-number* specifies the number of the virtual template interface.	The value is an integer that ranges from 0 to 1023.
virtual-access *va-number*	Displays the queue-based traffic statistics on a specified virtual access interface. *va-number* specifies the number of the virtual access interface.	The value is an integer that ranges from 0 to 1023.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display qos adaptation-profile applied-record** command displays the record of a specified adaptive traffic profile, including information about the interface, traffic profile, and NQA test instance bound to the adaptive traffic profile, traffic shaping rate, and latest packet loss ratio detected by the NQA test instance. The command output helps you locate faults.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the record of the adaptive traffic profile **gts1** on all interfaces.

```
<Huawei> display qos adaptation-profile gts1 applied-record
Interface: GigabitEthernet1/0/0
-----------------------------------------------------------------
 Policy: p1
  Classifier: c1
   Behavior: b1
    gts adaptation-profile gts1
-----------------------------------------------------------------
```

Display the record of the adaptive traffic profile **gts1** on the GE1/0/0.

```
<Huawei> display qos adaptation-profile gts1 interface gigabitethernet 1/0/0 applied-record
Interface: GigabitEthernet1/0/0
-----------------------------------------------------------------
QoS gts adaptation-profile: gts1
-----------------------------------------------------------------
NQA admin Name: admin
NQA test Name: jitter
Current Rate: 3072(Kbps)
Last packet loss: 20(%)
The latest traffic shaping rate fails to be updated because the packet loss ratio is within the allowed range.
```

Table 20-16 Description of the **display qos adaptation-profile applied-record** command output

Item	Description
Interface: GigabitEthernet1/0/0	Interface to which the adaptive traffic profile is applied.
QoS gts adaptation-profile: gts1	Adaptive traffic profile that is applied to the interface. To bind an adaptive traffic profile to an interface, run the **qos gts adaptation-profile** command.
Policy: p1	Traffic policy **p1** bound to the adaptive traffic profile.
Classifier: c1	Traffic classifier bound to the traffic policy.
Behavior: b1	Traffic behavior bound to the traffic policy.
gts adaptation-profile gts1	Adaptive traffic profile bound to the traffic behavior. To bind an adaptive traffic profile to a traffic behavior, run the **gts adaptation-profile** command.
NQA admin Name	Administrator name for the NQA test instance bound to the adaptive traffic profile. To set the administrator name for the NQA test instance bound to the adaptive traffic profile, run the **track nqa** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
NQA test Name	Name of the NQA test instance bound to the adaptive traffic profile. To set the name of the NQA test instance bound to the adaptive traffic profile, run the **track nqa** command.
Current Rate	Current traffic shaping rate.
Last packet loss	Latest packet loss ratio detected by the NQA test instance.
The latest traffic shaping rate fails to be updated because the packet loss ratio is within the allowed range.	Result of the update on the latest traffic shaping. One of the following results may be displayed: • The latest traffic shaping rate is updated successfully. • The latest traffic shaping rate fails to be updated because the packet loss ratio is not greater than the upper threshold for three consecutive times. • The latest traffic shaping rate fails to be updated because the packet loss ratio is not smaller than the upper threshold for three consecutive times. • The latest traffic shaping rate fails to be updated because the packet loss ratio is within the allowed range. • The latest traffic shaping rate fails to be updated because NQA detection fails. • The latest traffic shaping rate fails to be updated because bandwidth is sufficient to carry traffic. • The latest traffic shaping rate fails to be updated because the traffic shaping rate reaches the rate limit.

Related Topics

20.3.11 qos adaptation-profile
20.3.19 rate-adjust increase interval
20.3.20 rate-adjust loss
20.3.21 rate-adjust step
20.3.22 rate-range

20.3.24 track nqa

20.3.7 display qos car statistics

Function

The **display qos car statistics** command displays statistics on forwarded and discarded packets in the inbound direction to a specified interface where a QoS CAR profile is applied.

Format

display qos car statistics interface *interface-type interface-number* { **inbound** | **outbound** }

display qos car statistics interface { **virtual-template** *vt-number* **virtual-access** *va-number* } { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics on forwarded and discarded packets on a specified interface.	-
virtual-template *vt-number*	Displays statistics on forwarded and discarded packets on a specified virtual template interface.	The value is an integer that ranges from 0 to 1023.
virtual-access *va-number*	Displays statistics on forwarded and discarded packets on a specified virtual access interface.	The value is an integer that ranges from 0 to 1023.
inbound	Displays statistics on forwarded and discarded packets and statistics on packets in different colors after traffic policing is performed in the inbound direction.	-
outbound	Displays statistics on forwarded and discarded packets and statistics on packets in different colors after traffic policing is performed in the outbound direction.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run the **display qos car statistics** command to check statistics on forwarded and discarded packets in the inbound direction of an interface where a QoS CAR profile is applied. The command output helps you locate faults.

Example

Display statistics on forwarded and discarded packets after traffic policing is performed in the outbound direction on the GE1/0/0.

```
<Huawei> display qos car statistics interface gigabitethernet 1/0/0 outbound
 Interface : GigabitEthernet1/0/0
 Direction : Outbound
-----------------------------------------------------------------------------
Type            Packets/Bytes                Rate(pps/bps)
-----------------------------------------------------------------------------
Drop                 0/0                          0/0
Pass                0/0                          0/0
Green                 0/0                          0/0
Yellow                0/0                          0/0
Red                 0/0                          0/0
```

Table 20-17 Description of the **display qos car statistics** command output

Item	Description
Interface	Number of the interface where traffic policing is configured.
Direction	Direction in which traffic policing is performed on the interface: ● Inbound ● Outbound
Drop	Number of discarded packets on the interface after traffic policing is applied.
Pass	Number of forwarded packets on the interface after traffic policing is applied.
Green	Number of green packets on the interface after traffic policing is applied.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Yellow	Number of yellow packets on the interface after traffic policing is applied.
Red	Number of red packets on the interface after traffic policing is applied.
Type	Packet processing mode after traffic policing is applied to an interface.
Packets/Bytes	Number of packets or bytes.
Rate(pps/bps)	Rates, in pps or bit/s.

Related Topics

20.3.12 qos car

20.3.8 gts (traffic behavior view)

Function

The **gts** command configures traffic shaping in a traffic behavior.

The **undo gts** command deletes traffic shaping from a traffic behavior.

By default, traffic shaping is not configured in a traffic behavior.

Format

gts cir { *cir-value* [**cbs** *cbs-value*] | **pct** *pct-value* } [**queue-length** *queue-length*]

undo gts

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. By default, the CBS value is 25 times the CIR value. If the value 25 times the CIR value is smaller than 1500, the CBS value is 1500.
pct *pct-value*	Specifies the percentage of the available bandwidth.	The value is an integer that ranges from 1 to 100. **NOTE** After the PCT is configured, the CBS cannot be configured manually. The device automatically calculates the default CBS based on the configured PCT.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
queue-length *queue-length*	Specifies the maximum number of packets buffered in a queue.	The value is an integer. The value range is as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-1024 ● AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2204, AR2220E, AR2220, AR2240C, AR2240 (SRU40/60), AR3260&AR3670 (SRU40/60): 1-2048 ● AR2204XE, AR2204XE-DC, AR2240 (SRU80/SRU100/SRU100E/SRU200/SRU200E/SRU400), AR3260 (SRU80/SRU100/SRU100E/SRU200/SRU200E/SRU400) and AR3670: 1-1023 The default value is 64.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the rate of the downstream device interface is smaller than the rate of the upstream device interface, congestion may occur on the downstream device interface. To prevent packet loss and congestion, configure traffic shaping for queues on the upstream device interface to control the rate of outgoing packets so that packets can be sent at an even rate.

 Copyright © Huawei Technologies Co., Ltd.

After configuring traffic shaping in a traffic behavior bound to a traffic policy, you can set different rates for packets matching different traffic classifiers on an interface so that differentiated services are implemented.

NOTE

- If **gts (traffic behavior view)** is configured in a traffic behavior of a traffic policy, the queue bandwidth of the sub traffic policy is the queue bandwidth of the traffic policy multiplied by *pct-value*.
- If a traffic policy is applied to the interface where **qos gts** is configured, the queue bandwidth of the interface is the CIR multiplied by *pct-value*.
- In other situations, the queue bandwidth is the interface bandwidth multiplied by *pct-value*.

Follow-up Procedure

Create a traffic classifier and a traffic policy, bind the traffic classifier to the traffic behavior in the traffic policy, and apply the traffic policy.

Precautions

You cannot configure **gts (traffic behavior view)** and **gts adaptation-profile** commands in the same traffic behavior.

Traffic shaping can only be configured in a traffic behavior of a traffic policy on the outbound WAN interface of the device.

If you run the **gts** command multiple times, only the latest configuration takes effect.

Example

Configure traffic shaping in the traffic behavior **tb1**: Set the CIR to 38400 kbit/s, the CBS to 960000 bytes, and the maximum number of packets buffered in a queue to 100.

```
<Huawei> system-view
[Huawei] traffic behavior tb1
[Huawei-behavior-tb1] gts cir 38400 cbs 960000 queue-length 100
```

Related Topics

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.3.9 gts adaptation-profile

Function

The **gts adaptation-profile** command binds an adaptive traffic profile to a traffic behavior.

The **undo gts** command unbinds an adaptive traffic profile from a traffic behavior.

By default, no adaptive traffic profile is bound to a traffic behavior.

 Copyright © Huawei Technologies Co., Ltd.

Format

gts adaptation-profile *adaptation-profile-name*

undo gts

Parameters

Parameter	Description	Value
adaptation-profile-name	Specifies the name of an adaptive traffic profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic shaping solves the packet loss problem on the inbound interface of the downstream device when the rate of the inbound interface on the downstream device is smaller than the rate of the outbound interface on the upstream device. In some scenarios, the interface rate of the downstream device is variable, so the upstream device cannot determine the traffic shaping parameters.

Adaptive traffic shaping associates an NQA test instance with an adaptive traffic profile so that the upstream device can dynamically adjust traffic shaping parameters based on the packet loss ratio of the downstream device detected by the NQA test instance. The **gts adaptation-profile** command binds an adaptive traffic profile to a traffic behavior.

Follow-up Procedure

Create a traffic classifier and a traffic policy, bind the traffic classifier to the traffic behavior in the traffic policy, and apply the traffic policy.

Precautions

You cannot configure **gts (traffic behavior view)** and **gts adaptation-profile** in the same traffic behavior.

An adaptive traffic profile can only be bound to a traffic behavior in a traffic policy on the outbound WAN interface of the device.

If an adaptive traffic profile is used in the traffic behavior bound to a traffic policy, the traffic shaping rate in the adaptive traffic profile must be higher than the bandwidth defined in the sub traffic policy.

 Copyright © Huawei Technologies Co., Ltd.

Example

Bind the adaptive traffic profile **gts1** to the traffic behavior **tb1**.

```
<Huawei> system-view
[Huawei] traffic behavior tb1
[Huawei-behavior-tb1] gts adaptation-profile gts1
```

Related Topics

20.3.8 gts (traffic behavior view)

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.3.10 port-schedule high

Function

The **port-schedule high** command sets the high priority for an interface.

The **undo port-schedule high** command restores the default priority of an interface to Normal.

By default, the interface priority is Normal.

Format

port-schedule high

undo port-schedule high

NOTE

This command takes effect for only interfaces on the 4GEW-T and 4GEW-S cards.

Parameters

None

Views

GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the total service traffic volume on four interfaces of the 4GEW-T or 4GEW-S card exceeds 1 Gbit/s, the device discards packets randomly. If important services are transmitted on an interface, the services cannot be preferentially forwarded.

 Copyright © Huawei Technologies Co., Ltd.

You can run this command to set a high priority for the interface so that packets on the interface can be preferentially forwarded.

For example, if the high priority is set for interface 1, traffic entering interface 1 is sent to the high-priority queue. Then the device preferentially forwards traffic on interface 1. Traffic entering interfaces 2, 3, and 4 preempts the remaining bandwidth. Here, the remaining bandwidth is calculated as follows:

- Remaining bandwidth = 1 Gbit/s - Bandwidth used by interface 1

If the bandwidth is insufficient, the device randomly discards traffic on interfaces 2, 3, and 4. If the high priority is set for interfaces 1 and 2, the device preferentially forwards traffic on interfaces 1 and 2. If the sum of traffic on interfaces 1 and 2 exceeds 1 Gbit/s, the device randomly discards traffic on interfaces 1 and 2.

Precautions

If the high priority is set for the four interfaces and the sum of traffic on the four interfaces exceeds 1 Gbit/s, the device randomly discards traffic.

Example

Set a high priority for GE1/0/1.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/1
[Huawei-GigabitEthernet1/0/1] port-schedule high
```

20.3.11 qos adaptation-profile

Function

The **qos adaptation-profile** command creates an adaptive traffic profile and displays the adaptive traffic profile view.

The **undo qos adaptation-profile** command deletes an adaptive traffic profile.

By default, no adaptive traffic profile is created.

Format

qos adaptation-profile *adaptation-profile-name*

undo qos adaptation-profile *adaptation-profile-name*

Parameters

Parameter	Description	Value
adaptation-profile-name	Specifies the name of an adaptive traffic profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic shaping solves the packet loss problem on the inbound interface of the downstream device when the rate of the inbound interface on the downstream device is smaller than the rate of the outbound interface on the upstream device. In some scenarios, the interface rate of the downstream device is variable, so the upstream device cannot determine the traffic shaping parameters.

Adaptive traffic shaping associates an NQA test instance with an adaptive traffic profile so that the upstream device can dynamically adjust traffic shaping parameters based on the packet loss ratio of the downstream device detected by the NQA test instance. The **qos adaptation-profile** command creates an adaptive traffic profile and displays the adaptive traffic profile view.

Follow-up Procedure

1. Set parameters in the adaptive traffic profile.

   Run **track nqa**, **rate-range**, **rate-adjust step**, **rate-adjust loss**, or **rate-adjust increase interval** in the adaptive traffic profile view or manually set parameters.
2. Apply the adaptive traffic profile.
   - Bind the adaptive traffic profile to an interface.

     Run the **qos gts adaptation-profile** command to bind the adaptive traffic profile to an interface.
   - Reference the adaptive traffic profile in a traffic policy.

     Run the **gts adaptation-profile** command to bind the adaptive traffic profile to a traffic behavior, bind the traffic behavior and traffic classifier to the traffic policy, and apply the traffic policy to an interface.

Precautions

A maximum of 4 adaptive traffic profiles can be configured on the AR150 series.

A maximum of 8 adaptive traffic profiles can be configured on the AR100&AR120&AR160&AR200 series.

A maximum of 16 adaptive traffic profiles can be configured on the AR1200 series.

A maximum of 64 adaptive traffic profiles can be configured on the AR2200 series.

A maximum of 256 adaptive traffic profiles can be configured on the AR3200&AR3600 series.

The traffic policy bound to an adaptive traffic profile can be configured only on WAN interfaces of the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an adaptive traffic profile named **gts1**.

```
<Huawei> system-view
[Huawei] qos adaptation-profile gts1
[Huawei-qos-adaptation-profile-gts1]
```

Related Topics

20.3.9 gts adaptation-profile

20.3.14 qos gts adaptation-profile

20.3.19 rate-adjust increase interval

20.3.20 rate-adjust loss

20.3.21 rate-adjust step

20.3.22 rate-range

20.3.24 track nqa

20.3.12 qos car

Function

The **qos car** command configures traffic policing.

The **undo qos car** command deletes traffic policing.

By default, traffic policing is not configured.

Format

On the WAN side:

qos car { **inbound** | **outbound** } [**acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*]] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (AR100 series, AR120 series, AR150 series, AR160 series, AR200 series)

qos car { **inbound** | **outbound** } **user-set** *user-set-name* **cir** *cir-value* [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] (AR100, AR120, AR150, AR160, and AR200 series)

qos car { **inbound** | **outbound** } [**acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*]] **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass**

 Copyright © Huawei Technologies Co., Ltd.

[**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] (AR1200, AR2200, AR3200, AR3600 series)

undo qos car { **inbound** | **outbound** } [**acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address*]

undo qos car { **inbound** | **outbound** } **user-set** *user-set-name* (AR100 series, AR120 series, AR150 series, AR160 series, AR200 series)

On the LAN side:

qos car inbound cir *cir-value*

undo qos car inbound

qos car { **inbound** | **outbound** } { **acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*] } **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value*] }] (AR100 series, AR120 series, AR150 series, AR160 series, AR200 series)

qos car { **inbound** | **outbound** } { **acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* [**per-address**] [**time-range** *time-range-name*] } **cir** *cir-value* [**pir** *pir-value*] [**cbs** *cbs-value* **pbs** *pbs-value*] [**green** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**yellow** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] [**red** { **discard** | **pass** [**remark-8021p** *8021p-value* | **remark-dscp** *dscp-value* | **remark-mpls-exp** *exp-value*] }] (AR1200, AR2200, AR3200, AR3600 series)

undo qos car { **inbound** | **outbound** } { **acl** *acl-number* | { **destination-ip-address** | **source-ip-address** } **range** *start-ip-address* **to** *end-ip-address* }

NOTE

LAN interfaces of the AR100 series, AR120 series, AR150 series, AR160 series, AR200 series, AR1220E, AR1220EV, and AR1220EVW do not support interface-based traffic policing.

The 4GE-2S and 4ES2GP-S cards do not support interface-based traffic policing.

The WAN-side traffic policing command can be configured on Layer 2 VE interfaces.

The 4ES2G-S card does not support Layer 2 traffic policing.

Parameters

Parameter	Description	Value
inbound	Performs traffic policing in the inbound direction on an interface.	-

Parameter	Description	Value
outbound	Performs traffic policing in the outbound direction on an interface.	-
user-set *user-set-name*	Specifies the name of a user group to which bandwidth limiting is applied.	The value is a string of 1 to 32 case-sensitive characters without spaces.
acl *acl-number*	Performs traffic policing for packets matching a specified ACL.	The value is an integer that ranges from 2000 to 3999. ● The number of a basic ACL ranges from 2000 to 2999. ● The number of an advanced ACL ranges from 3000 to 3999.
destination-ip-address	Performs traffic policing for packets whose destination IP addresses are in a specified range.	-
source-ip-address	Performs traffic policing for packets whose source IP addresses are in a specified range.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
range *start-ip-address* **to** *end-ip-address*	Specifies an IP address range.	The value is in dotted decimal notation. ● The AR100 series, AR120 series, AR150 series, AR160 series, AR200 series, A1200 series allow a maximum of 2048 IP addresses. ● The AR2200, AR3600, and AR3200 series allow a maximum of 4096 IP addresses. **NOTE** When the device applies QoS CAR to packets within the matched IP address range, one ACL resource is occupied for each IP address. The preceding IP address range takes effective only when ACL resources are sufficient. You can run the **display acl resource** command to view information about ACL resources. The **Remaining** parameter indicates the number of remaining resources.
per-address	Performs traffic policing for packets from each IP address. If this parameter is not specified, the system aggregates all the flows and uses CAR to limit the flows.	-
time-range *time-range-name*	Specifies the time range during which CAR is performed for each IP address. The time range must have been configured using the **time-range** command.	The value is a string of case-sensitive characters without spaces and must begin with a letter. The value ranges from 1 to 32.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed average rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. **NOTE** On LAN interfaces of the device, if the CIR is smaller than 64 kbit/s, the rate limit is 64 kbit/s.
pir *pir-value*	Specifies the peak information rate (PIR), which is the maximum rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The PIR must be greater than or equal to the CIR.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. The default setting is as follows: ● If the PIR is not set or the PIR and CIR are the same, the CBS is 188 times the CIR. ● If the PIR is set and the PIR and CIR are different, the CBS is 125 times the CIR.
pbs *pbs-value*	Specifies the peak burst size (PBS), which is the maximum volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. The default setting is as follows: ● If the PIR is not set or the PIR and CIR are the same, the PBS is 313 times the CIR. ● If the PIR is set and the PIR and CIR are different, the PBS is 125 times the PIR.
green **yellow** **red**	Specifies the packet color. By default, green packets and yellow packets are allowed to pass through, and red packets are discarded.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
discard	Discards packets of a color.	-
pass	Permits packets of a color to pass through.	-
remark-dscp *dscp-value*	Re-marks the DSCP priority of packets when they are transmitted on a Layer 3 network.	The value can be the DiffServ code, an integer ranging from 0 to 63; the value can also be the name of the DSCP service type, such as af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1-cs7, default, and ef. The values corresponding to names of DSCP service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46
remark-8021p *8021p-value*	Re-marks the 802.1p priority of VLAN packets.	The value is an integer that ranges from 0 to 7.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
remark-mpls-exp *exp-value*	Re-marks the MPLS EXP priority of packets.	The value is an integer that ranges from 0 to 7.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic policing controls traffic by monitoring the rate of traffic, and discards excess traffic to limit traffic within a proper range and to protect network resources.

When data is sent from a high-speed link to a low-speed link, the bandwidth on the interface of the low-speed link is insufficient. As a result, a large number of packets are discarded. To solve this problem, configure traffic policing for outgoing traffic on the interface of the high-speed link. The interface then discards the packets whose rate exceeds the traffic policing rate so that the outgoing traffic rate is limited within a proper range. You can also configure traffic policing for incoming traffic on the interface of the low-speed link. The interface then discards the received packets whose rate exceeds the traffic policing rate.

Interface-based traffic policing provides the following functions:

- Limits all the service traffic on an interface.

  (LAN interfaces of the AR100&AR120&AR150&AR160&AR200 series, AR1220E, AR1220EV and AR1220EVW do not support interface-based traffic policing)
- Limits the service traffic matching a specified ACL rule.
- Limits the service traffic whose source and destination IP addresses are within a specified range.

Traffic policing actions include permit, deny, and forward after priority change. By default, green packets and yellow packets are allowed to pass through, and red packets are discarded.

After bandwidth limiting based on user groups is configured, the device limits traffic from all IP addresses of the user group.

Prerequisites

A user group has been created using the **user-set** command when bandwidth limiting is enabled based on the user group.

Precautions

When the traffic shaping rate is greater than the maximum rate of an interface, traffic policing is not performed on the interface. You need to set the CIR or PIR to be smaller than the maximum rate of the interface.

 Copyright © Huawei Technologies Co., Ltd.

When the CBS is smaller than the number of bytes in a packet, packets of this type are discarded.

To prevent a device failure to identify the packet color, you are advised to set the PBS to be larger than the CBS.

On LAN interfaces of devices:

- On the Layer 2 FE interface of the AR121, AR121W, AR121GW-L, AR129GW-L and AR150&AR200 series, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s.
- On the Layer 2 GE interface of the AR129CV, AR129CVW, AR129CVW-L, AR100&AR160 series, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s. When the traffic policing rate is in the range of 100 Mbit/s to 1 Gbit/s, the traffic policing rate is a multiple of 10 Mbit/s.
- On the FE interface of the SRU of the AR1220, ARAR1220F, AR1220V, AR1220W and AR1220VW, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s.
- On the GE interface of the SRU of the AR1220-8GE, AR1220C, AR1220E, AR1220EV and AR1220EVW, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s. When the traffic policing rate is in the range of 100 Mbit/s to 1 Gbit/s, the traffic policing rate is a multiple of 10 Mbit/s.
- On LAN interfaces of the AR2200&AR3200&AR3600 series, the traffic policing rate is a multiple of 64 kbit/s. If the CIR is set to 64 x *n* kbit/s, the traffic policing rate is 64 x *n* kbit/s. If the CIR is larger than 64 x *n* kbit/s and is smaller than 64 x (*n* + 1) kbit/s, the traffic policing rate is 64 x *n* kbit/s.
- On other LAN interfaces, the traffic policing rate is a multiple of 64 kbit/s. If the CIR is set to 64 x *n* kbit/s, the traffic policing rate is 64 x *n* kbit/s. If the CIR is larger than 64 x *n* kbit/s and is smaller than 64 x (*n* + 1) kbit/s, the traffic policing rate is 64 x *n* kbit/s.

The **qos car** command can be executed in the interface or sub-interface view. If the **qos car** command is used on the interface and its sub-interfaces simultaneously:

- If a GE interface or an XGE interface is used, data flows passing from its sub-interface are limited by the CAR on the sub-interface and the GE or XGE interface.
- On an ATM or serial interface, data flows passing from its sub-interface are only limited by CAR on the sub-interface. Only data flows passing from the ATM or serial interface are limited by CAR on the ATM or serial interface.

If the ACL number, destination IP address range, or source IP address range is configured in the **qos car** command on WAN interfaces, you can run the **qos car** command repeatedly on a WAN interface or sub-interface to configure at most 16 times.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the CIR for incoming traffic to 2000 kbit/s on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] qos car inbound cir 2000
```

On the GE0/0/1, set the CIR to 3000 kbit/s, CBS to 564000 bytes, and PBS to 939000 bytes for a user group in the inbound direction.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set huawei
[Huawei-web-user-set-huawei] quit
[Huawei-web] quit
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] qos car inbound user-set huawei cir 3000 cbs 564000 pbs 939000 green pass yellow pass red discard
```

Related Topics

20.3.7 display qos car statistics
19.7.24 time-range
20.8.6 user-set

20.3.13 qos gts

Function

The **qos gts** command configures traffic shaping on an interface.

The **undo qos gts** command cancels traffic shaping on an interface.

By default, traffic shaping is not performed on an interface.

Format

qos gts cir *cir-value* [**cbs** *cbs-value*]

undo qos gts

NOTE

- Layer 2 interfaces on AR100 series, AR120 series, AR150 series, AR160 series, AR200 series, AR1200 series do not support the **qos gts** command.
- The 9ES2, 4GE-2S, 4ES2G-S, and 4ES2GP-S cards do not support the **qos gts** command.

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. **NOTE** On LAN interfaces of the device, if the CIR is smaller than 64 kbit/s, the rate limit is 64 kbit/s.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. By default, the CBS is 25 times the CIR. If the value 25 times the CIR is smaller than 1500, the CBS is 1500.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If data traffic sent from the upstream device is heavy, the downstream network may be congested or a large number of packets are directly discarded. To prevent this problem, you can use the **qos gts** command to configure traffic shaping on the outbound interface of the upstream device to limit the traffic on a network connection so that packets can be transmitted at an even rate.

The differences between traffic policing and traffic shaping are as follows:

- Traffic policing directly discards the packets whose rate exceeds the rate limit. Traffic shaping, however, buffers the packets whose rate is larger than the traffic shaping rate. When there are sufficient tokens in the token bucket, the buffered packets are forwarded at an even rate.
- Traffic shaping increases the delay, whereas traffic policing does not.

Precautions

If you run the **qos gts** command multiple times in the same interface view, only the latest configuration takes effect.

The **qos gts** and **qos gts adaptation-profile** commands cannot be configured on the same interface.

 Copyright © Huawei Technologies Co., Ltd.

When the traffic shaping rate is larger than the maximum rate of an interface, traffic is not shaped on the interface. It is recommended that the CIR be smaller than the rate of an interface.

On LAN interfaces of devices:

- On the Layer 2 FE interface of the AR121, AR121W, AR121GW-L, AR129GW-L AR150, and AR200 series, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s.
- On the Layer 2 GE interface of the AR129CV, AR129CVW, AR129CVW-L, AR100 series, AR160 series, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s. When the traffic policing rate is in the range of 100 Mbit/s to 1 Gbit/s, the traffic policing rate is a multiple of 10 Mbit/s.
- On the FE interface of the SRU of the AR1220, ARAR1220F, AR1220V, AR1220W, and AR1220VW, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s.
- On the GE interface of the SRU of the AR1220-8GE, AR1220C, AR1220E, AR1220EV, and AR1220EVW, when the traffic policing rate is in the range of 64 kbit/s to 1 Mbit/s, the traffic policing rate is a multiple of 64 kbit/s. When the traffic policing rate is in the range of 1 Mbit/s to 100 Mbit/s, the traffic policing rate is a multiple of 1 Mbit/s. When the traffic policing rate is in the range of 100 Mbit/s to 1 Gbit/s, the traffic policing rate is a multiple of 10 Mbit/s.
- On LAN interfaces of the AR2200, &AR3200&AR3600 series, the traffic policing rate is a multiple of 64 kbit/s. If the CIR is set to 64 x *n* kbit/s, the traffic policing rate is 64 x *n* kbit/s. If the CIR is larger than 64 x *n* kbit/s and is smaller than 64 x (*n* + 1) kbit/s, the traffic policing rate is 64 x *n* kbit/s.
- On other LAN interfaces, the traffic policing rate is a multiple of 64 kbit/s. If the CIR is set to 64 x *n* kbit/s, the traffic policing rate is 64 x *n* kbit/s. If the CIR is larger than 64 x *n* kbit/s and is smaller than 64 x (*n* + 1) kbit/s, the traffic policing rate is 64 x *n* kbit/s.

The **qos gts** command shapes traffic of all queues on an interface, whereas the **queue gts** command shapes traffic of a specified queue on an interface. If both queue-based traffic shaping and interface-based traffic shaping are configured on an interface, the CIR of interface-based traffic shaping cannot be lower than the sum of CIR values of all the queues on the interface; otherwise, the traffic shaping result may be incorrect. For example, packets in the queue with a higher priority may be not scheduled in a timely manner.

After a physical interface is bound to a virtual template interface to form an MP-link, the **qos gts** command is invalid on the physical interface. For details about MP binding, see Implementing MP.

For logical interfaces (excluding Layer 2 Eth-Trunk interfaces), run the **qos gts** command on the interface to configure interface-based traffic shaping. It is recommended that the CIR be set to 90% of the logical interface bandwidth. The

 Copyright © Huawei Technologies Co., Ltd.

remaining 10% bandwidth is reserved for protocol packets. If the logical interface has sub-interfaces, run the **qos gts** command on the main interface.

Example

Set the CIR of data packets to be sent from the Eth2/0/0 to 2000 kbit/s and CBS to 375000 bytes.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] qos gts cir 2000 cbs 375000
```

Related Topics

20.3.17 queue gts

20.3.14 qos gts adaptation-profile

Function

The **qos gts adaptation-profile** command binds an adaptive traffic profile to an interface.

The **undo qos gts** command unbinds an adaptive traffic profile from an interface.

By default, no adaptive traffic profile is bound to an interface.

Format

qos gts adaptation-profile *adaptation-profile-name*

undo qos gts

Parameters

Parameter	Description	Value
adaptation-profile-name	Specifies the name of an adaptive traffic profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traffic shaping solves the packet loss problem on the inbound interface of the downstream device when the rate of the inbound interface on the downstream device is smaller than the rate of the outbound interface on the upstream device. In some scenarios, the interface rate of the downstream device is variable, so the upstream device cannot determine the traffic shaping parameters.

Adaptive traffic shaping associates an NQA test instance with an adaptive traffic profile so that the upstream device can dynamically adjust traffic shaping parameters based on the NQA result. The **qos gts adaptation-profile** command binds an adaptive traffic profile to an interface.

Precautions

The **qos gts** and **qos gts adaptation-profile** commands cannot be configured on the same interface.

An adaptive traffic profile can be bound to only a WAN interface on the device.

The traffic shaping rate configured using the **qos gts adaptation-profile** command applies to all queues on an interface, and the traffic shaping rate configured using the **queue gts** command applies to a specified queue on an interface. If both **qos gts adaptation-profile** and **queue gts** are used on an interface, the lower threshold for the traffic shaping rate in the adaptive traffic profile must be larger than or equal to the sum of traffic shaping rates of all the queues on the interface; otherwise, the traffic shaping result may be incorrect. For example, packets in queues with higher priorities are not scheduled in a timely manner.

If you run the **qos gts adaptation-profile** command multiple times in the same interface view, only the latest configuration takes effect.

Example

Bind the adaptive traffic profile **gts1** to GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] qos gts adaptation-profile gts1
```

Related Topics

20.3.11 qos adaptation-profile

20.3.13 qos gts

20.3.15 qos lr (interface view)

Function

The **qos lr** command sets the percentage of the rate for sending packets to the interface bandwidth.

The **undo qos lr** command restores the default percentage of the rate for sending packets to the interface bandwidth.

By default, the percentage of the rate for sending packets to the interface bandwidth is 100.

 Copyright © Huawei Technologies Co., Ltd.

Format

qos lr pct *pct-value* [**cbs** *cbs-value*]

undo qos lr

Parameters

Parameter	Description	Value
pct *pct-value*	Specifies the percentage of the rate for sending packets to the interface bandwidth.	The value is an integer that ranges from 1 to 100.
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer that ranges from 1500 to 4294967295, in bytes. The default value is three times the interface bandwidth.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To limit the rate of sending packets on an interface, run the **qos lr** command to set the percentage of the rate for sending packets to the interface bandwidth.

Precautions

Only WAN-side physical interfaces support the **qos lr** command.

If you run the **qos lr** command multiple times on the same interface, only the latest configuration takes effect.

Rate limiting will not take effect until queue scheduling is configured.

Example

On the GE1/0/0, set the percentage of the rate for sending packets to the interface bandwidth to 50% and CBS to 375000 bytes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] qos lr pct 50 cbs 375000
[Huawei-GigabitEthernet1/0/0] quit
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.3.13 qos gts

20.3.16 qos overhead

Function

The **qos overhead** command configures the mode for calculating the packet length during traffic policing or traffic shaping.

By default, physical-layer and link-layer compensation information is included in packet length calculation during traffic policing or traffic shaping.

Format

qos overhead layer { **link** | **physics** }

Parameters

Parameter	Description	Value
layer	Indicates whether physical-layer or link-layer compensation information is included in packet length calculation during traffic policing or traffic shaping.	-
link	Indicates that link-layer compensation information is included in packet length calculation during traffic policing or traffic shaping.	-
physics	Indicates that physical-layer and link-layer compensation information is included in packet length calculation during traffic policing or traffic shaping.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

During traffic policing or traffic shaping, run the **qos overhead** command to configure the mode for calculating the packet length. When the same CIR is used, the number of forwarded packets when the **qos overhead layer link** command is used is larger than that when the **qos overhead layer physics** command is used. The **qos overhead** command takes effect only when it is used with one of the following commands:

- **car**
- **qos car**
- **qos gts**
- **qos adaptation-profile**
- **queue gts**
- **gts**
- **qos lr**

Precautions

Only Ethernet, PPP, and FR links support the **qos overhead** command.

Example

Configure the device to use only link-layer compensation information in packet length calculation during traffic policing or traffic shaping.

```
<Huawei> system-view
[Huawei] qos overhead layer link
```

Related Topics

20.3.2 car (traffic behavior view)
20.3.12 qos car
20.3.13 qos gts
20.3.11 qos adaptation-profile
20.3.17 queue gts
20.3.8 gts (traffic behavior view)
20.3.15 qos lr (interface view)

20.3.17 queue gts

Function

The **queue gts** command configures traffic shaping for queues.

The **undo queue gts** command cancels traffic shaping for queues.

 Copyright © Huawei Technologies Co., Ltd.

By default, traffic shaping is not performed for queues.

Format

queue { *start-queue-index* [**to** *end-queue-index*] } &<1–10> **gts cir** *cir-value* [**cbs** *cbs-value*]

undo queue { *start-queue-index* [**to** *end-queue-index*] } &<1–10> **gts**

Parameters

Parameter	Description	Values
start-queue-index [**to** *end-queue-index*]	Specifies the indexes of the queues for which traffic shaping is configured. ● *start-queue-index* specifies the index of the first queue for which traffic shaping is configured. ● *end-queue-index* specifies the index of the last queue for which traffic shaping is configured. If **to** *end-queue-index* is not specified, traffic shaping is configured for only the queue specified by *start-queue-index*.	The value of *start-queue-index* is an integer that ranges from 0 to 7. The value of *end-queue-index* is an integer that ranges from 0 to 7.
cir *cir-value*	Specifies the committed information rate (CIR), which is the allowed rate at which traffic can pass through.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. **NOTE** When you bind a queue profile to a LAN interface on the device and the CIR is smaller than 64 kbit/s, the rate limit is 64 kbit/s.
cbs *cbs-value*	Specifies the committed burst size (CBS), which is the average volume of burst traffic that can pass through an interface.	The value is an integer that ranges from 1500 to 4294967295, in bytes. By default, the CBS is 25 times the CIR. If the value 25 times the CIR is smaller than 1500, the CBS is 1500.

 Copyright © Huawei Technologies Co., Ltd.

Views

Queue profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the rate of the downstream device interface is smaller than the rate of the upstream device interface, congestion may occur on the downstream device interface. To prevent packet loss and congestion, configure traffic shaping for queues on the upstream device interface to control the rate of outgoing packets so that packets can be sent at an even rate.

Service packets enter queues on an interface based on priorities. Different from interface-based traffic shaping, queue-based traffic shaping applies different rates to packets in queues with different priorities to implement differentiated services for queues.

Follow-up Procedure

Run the **qos queue-profile (interface view)** command to bind the queue profile to an interface.

Precautions

NOTE

Interfaces on the 4ES2G-S, 4ES2GP-S and 9ES2 cards do not support the **queue gts** command.

Layer 2 FE interfaces on the AR150&200 series do not support the **queue gts** command.

Layer 2 GE interfaces on the AR120&AR160 series do not support the **queue gts** command.

FE interfaces on the SRU of the AR1200 series do not support the **queue gts** command.

en

When the traffic shaping rate is larger than the maximum rate of an interface, traffic in queues is not shaped. It is recommended that the CIR be lower than the rate of an interface.

On the device's LAN interface, the traffic shaping rate is a multiple of is 64 kbit/s. If the CIR is set to 64 x *n* kbit/s, the rate limit is 64 x *n* kbit/s. If the CIR is larger than 64 x *n* kbit/s and is smaller than 64 x (*n* + 1) kbit/s, the rate limit is 64 x *n* kbit/s.

If queue-based traffic shaping is configured on an interface, the traffic shaping rate on the interface must be larger than the bandwidth required by all queues on the interface; otherwise, the traffic shaping result may be incorrect. For example, packets in queues with higher priorities are not scheduled in a timely manner.

If you run the **queue gts** command multiple times in the same queue profile view, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

When you change the queue shaping configuration in the view of the queue profile bound to an interface, the device synchronizes the change to the interface that supports **queue gts**. If the interface does not support **queue gts**, the system displays a configuration failure message.

Example

Create a queue profile named **hello-world** and set the CIR and CBS of queue 0 to queue 3 to 2000 kbit/s and 375000 bytes respectively.

```
<Huawei> system-view
[Huawei] qos queue-profile hello-world
[Huawei-qos-queue-profile-hello-world] queue 0 to 3 gts cir 2000 cbs 375000
```

Related Topics

20.4.3 display qos queue-profile
20.4.8 qos queue-profile (interface view)
20.4.9 qos queue-profile (system view)
20.4.13 queue length
20.4.16 queue weight
20.4.19 schedule

20.3.18 qos-profile

Function

The **qos-profile** command creates a QoS profile and displays its view, or directly displays the view of an existing QoS profile.

The **undo qos-profile** command deletes a QoS profile.

By default, no QoS profile is configured on the device.

Format

qos-profile *profile-name*

undo qos-profile *profile-name*

Parameters

Parameter	Description	Value
profile-name	Specifies the name of a QoS profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can define QoS configurations in a QoS profile to implement such functions as traffic policing and traffic statistics.

Follow-up Procedure

- Define parameters in the QoS profile, including parameters of traffic policing and traffic statistics.
- Apply the QoS profile in the specified view.

Example

Create a QoS profile named **huawei** and enter the QoS profile view.

```
<Huawei> system-view
[Huawei] qos-profile huawei
[Huawei-qos-profile-huawei]
```

Related Topics

20.3.3 car (QoS profile view)

20.3.19 rate-adjust increase interval

Function

The **rate-adjust increase interval** command sets the interval at which the traffic shaping rate increases.

The **undo rate-adjust increase interval** command restores the default interval at which the traffic shaping rate increases.

By default, the traffic shaping rate increases at intervals of 30s.

Format

rate-adjust increase interval *interval-value*

undo rate-adjust increase interval

Parameters

Parameter	Description	Value
interval-value	Specifies the interval at which the traffic shaping rate increases.	The value is an integer that ranges from 10 to 65535, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Views

Adaptive traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Adaptive traffic shaping associates an NQA test instance with an adaptive traffic profile so that the upstream device can dynamically adjust traffic shaping parameters based on the packet loss ratio of the downstream device detected by the NQA test instance. The upstream device increases the traffic shaping rate when the NQA test instance detects that the packet loss ratio is smaller than the lower threshold for the packet loss ratio in the adaptive traffic profile for three consecutive times and congestion occurs on the outbound interface of the upstream device. You can run this command to set the interval to prevent frequent traffic shaping rate change.

Precautions

If you run the **rate-adjust increase interval** command multiple times in the same adaptive traffic profile view, only the latest configuration takes effect.

Example

Set the interval at which the traffic shaping rate increases in the adaptive traffic profile **gts1** to 50s.

```
<Huawei> system-view
[Huawei] qos adaptation-profile gts1
[Huawei-qos-adaptation-profile-gts1] rate-adjust increase interval 50
```

Related Topics

20.3.9 gts adaptation-profile

20.3.11 qos adaptation-profile

20.3.14 qos gts adaptation-profile

20.3.20 rate-adjust loss

20.3.21 rate-adjust step

20.3.22 rate-range

20.3.24 track nqa

20.3.20 rate-adjust loss

Function

The **rate-adjust loss** command sets the packet loss ratio range in an adaptive traffic profile.

The **undo rate-adjust loss** command restores the default packet loss ratio range in an adaptive traffic profile.

By default, the packet loss ratio ranges from 10% to 20%.

Format

rate-adjust loss low-threshold *low-threshold-percentage* **high-threshold** *high-threshold-percentage*

undo rate-adjust loss

Parameters

Parameter	Description	Value
low-threshold *low-threshold-percentage*	Specifies the lower threshold for the packet loss ratio.	The value is an integer that ranges from 0 to 100.
high-threshold *high-threshold-percentage*	Specifies the upper threshold for the packet loss ratio.	The value is an integer that ranges from 0 to 100. The value of *high-threshold-percentage* cannot be smaller than the value of *low-threshold-percentage*.

Views

Adaptive traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Adaptive traffic shaping associates an NQA test instance with an adaptive traffic profile so that the upstream device can dynamically adjust traffic shaping parameters based on the packet loss ratio of the downstream device detected by the NQA test instance. The **rate-adjust loss** command sets the packet loss ratio range in an adaptive traffic profile:

- The upstream device reduces the traffic shaping rate when the NQA test instance detects that the packet loss ratio is larger than the upper threshold in the adaptive traffic profile.
- The upstream device increases the traffic shaping rate when all the following conditions are met:
  - The NQA test instance detects that the packet loss ratio is lower than the lower threshold in the adaptive traffic profile.

  - Congestion occurs on the outbound interface of the upstream device.
  - The interval at which the traffic shaping rate increases is reached.
- The upstream device retains the traffic shaping rate in one of the following scenarios:
  - The NQA test instance detects that the packet loss ratio is smaller than the lower threshold in the adaptive traffic profile and no congestion occurs on the outbound interface of the upstream device.
  - The detected packet loss ratio is within the packet loss ratio range in the adaptive traffic profile.
- The upstream device uses the upper threshold for the traffic shaping rate in the adaptive traffic profile when the NQA test fails.
- The upstream device uses the upper threshold for the traffic shaping rate in the adaptive traffic profile when the adaptive traffic profile is not bound to the NQA test instance.

Precautions

If you run the **rate-adjust loss** command multiple times in the same adaptive traffic profile view, only the latest configuration takes effect.

Example

Set the packet loss ratio range in the adaptive traffic profile **gts1** to 20% to 30%.

```
<Huawei> system-view
[Huawei] qos adaptation-profile gts1
[Huawei-qos-adaptation-profile-gts1] rate-adjust loss low-threshold 20 high-threshold 30
```

Related Topics

20.3.9 gts adaptation-profile

20.3.11 qos adaptation-profile

20.3.14 qos gts adaptation-profile

20.3.19 rate-adjust increase interval

20.3.21 rate-adjust step

20.3.22 rate-range

20.3.24 track nqa

20.3.21 rate-adjust step

Function

The **rate-adjust step** command sets the traffic shaping rate adaptation step in an adaptive traffic profile.

The **undo rate-adjust step** command restores the default traffic shaping rate adaptation step in an adaptive traffic profile.

By default, the traffic shaping rate adaptation step is 64 kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Format

rate-adjust step *step*

undo rate-adjust step

Parameters

Parameter	Description	Value
step	Specifies the traffic shaping rate adaptation step.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.

Views

Adaptive traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Adaptive traffic shaping associates an NQA test instance with an adaptive traffic profile so that the upstream device can dynamically adjust traffic shaping parameters based on the packet loss ratio of the downstream device detected by the NQA test instance. The **rate-adjust step** command sets the traffic shaping rate adaptation step in an adaptive traffic profile.

Precautions

If you run the **rate-adjust step** command multiple times in the same adaptive traffic profile view, only the latest configuration takes effect.

Example

Set the traffic shaping rate adaptation step in an adaptive traffic profile **gts1** to 32 kbit/s.

```
<Huawei> system-view
[Huawei] qos adaptation-profile gts1
[Huawei-qos-adaptation-profile-gts1] rate-adjust step 32
```

Related Topics

20.3.9 gts adaptation-profile
20.3.11 qos adaptation-profile
20.3.14 qos gts adaptation-profile
20.3.19 rate-adjust increase interval
20.3.20 rate-adjust loss

 Copyright © Huawei Technologies Co., Ltd.

20.3.22 rate-range
20.3.24 track nqa

20.3.22 rate-range

Function

The **rate-range** command sets the traffic shaping rate range in an adaptive traffic profile.

Format

rate-range low-threshold *low-threshold-value* **high-threshold** *high-threshold-value*

Parameters

Parameter	Description	Value
low-threshold *low-threshold-value*	Specifies the lower threshold for the traffic shaping rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
high-threshold *high-threshold-value*	Specifies the upper threshold for the traffic shaping rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s. The value of *high-threshold-value* cannot be smaller than the value of *low-threshold-value*.

Views

Adaptive traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Adaptive traffic shaping adjusts the traffic shaping rate based on the packet loss ratio of the downstream device detected by the NQA test instance. The **rate-range** command sets the traffic shaping rate range in an adaptive traffic profile.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

If an adaptive traffic profile is used in the traffic behavior bound to a traffic policy, the traffic shaping rate in the adaptive traffic profile must be larger than the bandwidth defined in the sub traffic policy.

If both an adaptive traffic profile and queue-based traffic shaping are configured on the same interface, the traffic shaping rate in the adaptive traffic profile must be larger than the bandwidth required by queues on the interface.

If you run the **rate-range** command multiple times in the same adaptive traffic profile view, only the latest configuration takes effect.

Example

Set the traffic shaping rate range in the adaptive traffic profile **gts1** to 500 kbit/s to 800 kbit/s.

```
<Huawei> system-view
[Huawei] qos adaptation-profile gts1
[Huawei-qos-adaptation-profile-gts1] rate-range low-threshold 500 high-threshold 800
```

Related Topics

20.3.9 gts adaptation-profile
20.3.11 qos adaptation-profile
20.3.14 qos gts adaptation-profile
20.3.19 rate-adjust increase interval
20.3.20 rate-adjust loss
20.3.21 rate-adjust step
20.3.24 track nqa

20.3.23 reset qos car statistics

Function

The **reset qos car statistics** command clears packet statistics on an interface to which a QoS CAR profile is applied.

Format

reset qos car statistics interface *interface-type interface-number* { **inbound** | **outbound** }

reset qos car statistics interface virtual-template *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears packet statistics on a specified interface.	-

Parameter	Description	Value
inbound	Clears statistics in the inbound direction on an interface.	-
outbound	Clears statistics in the outbound direction on an interface.	-
virtual-template *vt-number*	Displays queue-based traffic statistics on a specified virtual template interface. *vt-number* specifies the number of the virtual template interface.	The value is an integer that ranges from 0 to 1023.
virtual-access *va-number*	Displays queue-based traffic statistics on a specified virtual access interface. *va-number* specifies the number of the virtual access interface. You can run the **display virtual-access** command to display the state of the virtual access interface status.	The value is an integer that ranges from 0 to 1023.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before recollecting statistics on forwarded and discarded packets on an interface to which a QoS CAR profile is applied, run the **reset qos car statistics** command to clear existing statistics. Then run the **display qos car statistics** command to view the packet statistics.

Precautions

The cleared statistics on forwarded and discarded packets on an interface cannot be restored. Exercise caution when you use this command.

Example

Clear statistics in the inbound direction on the Eth2/0/0.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> reset qos car statistics interface ethernet 2/0/0 inbound
```

Related Topics

20.3.12 qos car

20.3.7 display qos car statistics

20.3.24 track nqa

Function

The **track nqa** command binds an NQA test instance to an adaptive traffic profile.

The **undo track nqa** command unbinds an NQA test instance from an adaptive traffic profile.

By default, no NQA test instance is bound an adaptive traffic profile.

Format

track nqa *admin-name test-name*

undo track nqa

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator name for an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters without spaces.

Views

Adaptive traffic profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Adaptive traffic shaping associates an NQA test instance with an adaptive traffic profile so that the upstream device can dynamically adjust traffic shaping

parameters based on the packet loss ratio of the downstream device detected by the NQA test instance. The **track nqa** command binds an NQA test instance to an adaptive traffic profile.

- The upstream device reduces the traffic shaping rate when the NQA test instance detects that the packet loss ratio is larger than the upper threshold in the adaptive traffic profile.
- The upstream device increases the traffic shaping rate when all the following conditions are met:
  - The NQA test instance detects that the packet loss ratio is lower than the lower threshold in the adaptive traffic profile.
  - Congestion occurs on the outbound interface of the upstream device.
  - The interval at which the traffic shaping rate increases is reached.
- The upstream device retains the traffic shaping rate in one of the following scenarios:
  - The NQA test instance detects that the packet loss ratio is smaller than the lower threshold in the adaptive traffic profile and no congestion occurs on the outbound interface of the upstream device.
  - The detected packet loss ratio is within the packet loss ratio range in the adaptive traffic profile.
- The upstream device uses the upper threshold for the traffic shaping rate in the adaptive traffic profile when the NQA test fails.
- The upstream device uses the upper threshold for the traffic shaping rate in the adaptive traffic profile when the adaptive traffic profile is not bound to the NQA test instance.

Precautions

If you run the **track nqa** command multiple times in the same adaptive traffic profile view, only the latest configuration takes effect.

After the **undo track nqa** command is used, the traffic shaping rate is restored to the upper threshold for the traffic shaping rate in the adaptive traffic profile by the **rate range** command.

Example

Bind the NQA test instance **jitter1** with the administration name **admin** to the adaptive traffic profile **gts1**.

```
<Huawei> system-view
[Huawei] qos adaptation-profile gts1
[Huawei-qos-adaptation-profile-gts1] track nqa admin jitter1
```

Related Topics

20.3.9 gts adaptation-profile
20.3.11 qos adaptation-profile
20.3.14 qos gts adaptation-profile
20.3.19 rate-adjust increase interval
20.3.20 rate-adjust loss
20.3.21 rate-adjust step

 Copyright © Huawei Technologies Co., Ltd.

20.3.22 rate-range

20.4 Congestion Avoidance and Congestion Management Commands

20.4.1 display drop-profile

Function

The **display drop-profile** command displays the configuration of a WRED drop profile.

Format

display drop-profile [*drop-profile-name*]

Parameters

Parameter	Description	Value
drop-profile-name	Displays detailed information about a WRED drop profile with the specified name. If the parameter is not specified, brief information about all drop profiles is displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can use the **display drop-profile** command to view the number of configured drop profiles and all configuration of a specified drop profile.

Precautions

In addition to the default drop profile, a maximum of 63 drop profiles can be configured on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display brief information about all drop profiles on the device.

```
<Huawei> display drop-profile
      Index                  Drop-profile name
-----------------------------------------------------------------
      1                      drop-profile1
      2                      drop-profile2
-----------------------------------------------------------------
 Total   63     Used   2
```

Display detailed information about the drop profile named **drop-profile1**.

```
<Huawei> display drop-profile drop-profile1
Drop-profile[1]: drop-profile1
IP-Precedence      Low-limit   High-limit  Discard-percentage
-----------------------------------------------------------------
0(routine)          30          100         10
1(priority)         30          100         10
2(immediate)        30          100         10
3(flash)            30          80          50
4(flash-override)   30          100         10
5(critical)         30          100         10
6(internet)         30          100         10
7(network)          30          100         10
-----------------------------------------------------------------
```

Table 20-18 Description of the display drop-profile command output

Item	Description
Index	Drop profile index.
Drop-profile name	Drop profile name. To configure a drop profile, run the **drop-profile (system view)** command.
Total	Total number of drop profiles that can be configured on the device.
Used	Number of configured drop profiles.
Drop-profile[1]	Drop profile name in which 1 indicates the drop profile index.
IP-Precedence	WRED drop profile based on IP priorities of packets. If the WRED drop profile is based on DSCP priorities of packets, DSCP is displayed.
Low-limit	Lower drop threshold, in percentage.
High-limit	Upper drop threshold, in percentage.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Discard-percentage	Maximum drop probability, in percentage. To set the maximum drop probability, run the **ip-precedence discard-percentage** or **dscp discard-percentage** command.

Related Topics

20.4.6 drop-profile (system view)

20.4.5 ip-precedence discard-percentage

20.4.4 dscp discard-percentage

20.4.2 display qos queue statistics

Function

The **display qos queue statistics** command displays queue-based traffic statistics on an interface.

Format

display qos queue statistics interface *interface-type interface-number* [**queue** *queue-index*]

display qos queue statistics interface virtual-template *vt-number* **virtual-access** *va-number* [**queue** *queue-index*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays queue-based traffic statistics on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
virtual-template *vt-number*	Displays queue-based traffic statistics on a specified virtual template interface. *vt-number* specifies the number of the virtual template interface.	The value is an integer that ranges from 0 to 1023.
virtual-access *va-number*	Displays queue-based traffic statistics on a specified virtual access interface. *va-number* specifies the number of the virtual access interface. You can run the **display virtual-access** command to view the virtual access interface status.	The value is an integer that ranges from 0 to 1023.
queue *queue-index*	Displays statistics on the queue with a specified index.	The value is an integer that ranges from 0 to 7.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check whether packets in each queue on an interface are forwarded or discarded because of congestion, view the statistics on each queue on the interface.

Precautions

Each WAN-side interface on the device has a protocol queue named **protocol**, which cannot be modified or deleted. Protocol queues are responsible for forwarding all protocol packets such as ARP packets, and ICMP packets on the control plane. Packets in a protocol queue are scheduled in Strict Priority (SP) mode. Packets in other queues can be scheduled only after packets in protocol queues are scheduled.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- The Layer 2 FE interface and Layer 2 GE interface on the AR100&AR120&AR150&AR160&AR200 series does not support the **display qos queue statistics** command.
- The FE interface on the main control board of the AR1200 series does not support the **display qos queue statistics** command.
- The 4GE-2S, 4ES2G-S, 4ES2GP-S, and 9ES2 cards do not support the **display qos queue statistics** command.

The GE interfaces on the main control board of the device do not support the **display qos queue statistics** command.

Example

Display traffic statistics on queues on GE1/0/0.

```
<Huawei> display qos queue statistics interface gigabitethernet 1/0/0
-------------------------------------------------------------------------------
Queue          Passed          Pass Rate       Dropped         Drop Rate
          (Packets/Bytes)     (pps/bps)    (Packets/Bytes)     (pps/bps)
-------------------------------------------------------------------------------
0                 0/            0/            -/            -/
                  -             -             -             -
1                 0/            0/            -/            -/
                  -             -             -             -
2                 0/            0/            -/            -/
                  -             -             -             -
3                 0/            0/            -/            -/
                  -             -             -             -
4                 0/            0/            -/            -/
                  -             -             -             -
5                 0/            0/            -/            -/
                  -             -             -             -
6              1850/            0/            -/            -/
                  -             -             -             -
7                 0/            0/            -/            -/
                  -             -             -             -
-------------------------------------------------------------------------------
```

Table 20-19 Description of the **display qos queue statistics** command output

Item	Description
Queue	Queue index.
Passed(Packets/Bytes)	Statistics on forwarded packet or bytes. If the information is displayed as -, the statistics on this item cannot be collected.
Pass Rate(pps/bps)	Rate of forwarded packets, in pps or bit/s. This item indicates the average rate of packets that are forwarded since the last time the **display qos queue statistics** command is run to query traffic statistics. If the information is displayed as -, the statistics on this item cannot be collected.

Item	Description
Dropped(Packets/Bytes)	Statistics on discarded packets or bytes. If the information is displayed as -, the statistics on this item cannot be collected.
Drop Rate(pps/bps)	Rate of discarded packets, in pps or bit/s. This item indicates the average rate of packets that are discarded since the last time the **display qos queue statistics** command is run to query traffic statistics. If the information is displayed as -, the statistics on this item cannot be collected.

Related Topics

20.4.18 reset qos queue statistics

20.4.3 display qos queue-profile

Function

The **display qos queue-profile** command displays information about queue profiles.

Format

display qos queue-profile [*queue-profile-name*]

Parameters

Parameter	Description	Value
queue-profile-name	Specifies the name of a queue profile. If this parameter is not specified, brief information about all queue profiles is displayed.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

On the device, a maximum of 32 queue profiles can be configured. Before or after configuring queue profiles, you can use the **display qos queue-profile** command to view the number of configured queue profiles and all the configuration of the specified queue profile.

Example

Display all the queue profile indexes and names.

```
<Huawei> display qos queue-profile
Index                    Queue-profile name
-----------------------------------------------------------------
0                         qp1
1                         qp2
2                         qp3
-----------------------------------------------------------------
  Total  32  Used  3
```

Display the detailed configuration of the queue profile **qp1**.

```
<Huawei> display qos queue-profile qp1
Queue-profile:qp1
Queue   Schedule   Weight  Length(Bytes/Packets)  GTS(CIR/CBS)
-----------------------------------------------------------------------------------------------------
0       DRR       10       -/-                    -/-
1       DRR       10       -/-                    -/-
2       DRR       10       -/-                    -/-
3       DRR       10       -/-                    -/-
4       DRR       10       -/-                    -/-
5       PQ        -        -/-                    -/-
6       PQ        -        -/-                    -/-
7       PQ        -        -/-                    64/10000
```

Table 20-20 Description of the display qos queue-profile command output

Item	Description
Index	Queue profile index.
Queue-profile name	Queue profile name.
Total	Maximum number of queue profiles that can be configured on the device.
Used	Number of configured queue profiles.
Queue	Queue index.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Schedule	Scheduling mode: ● DRR ● PQ ● WFQ ● WRR To set the scheduling mode, run the **schedule** command.
Weight	Queue weight.
Length(Bytes/Packets)	Queue length, which can be the number of bytes or the number of packets.
GTS(CIR/CBS)	Traffic shaping rate, which can be the CIR or CBS value. To configure GTS, run the **queue gts** command.

Related Topics

20.4.8 qos queue-profile (interface view)
20.4.9 qos queue-profile (system view)
20.3.17 queue gts
20.4.13 queue length
20.4.16 queue weight
20.4.19 schedule

20.4.4 dscp discard-percentage

Function

The **dscp discard-percentage** command sets WRED parameters for packets with a specified DSCP priority, including the upper and lower drop thresholds and the maximum drop probability.

The **undo dscp** command restores the default values of WRED parameters for packets with a specified DSCP priority.

By default, the lower drop threshold is 30%, the upper drop threshold is 100%, and the maximum drop probability is 10%.

Format

dscp { *dscp-value1* [**to** *dscp-value2*] } &<1-10> **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*

undo dscp [*dscp-value1* [**to** *dscp-value2*]] &<1-10>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
dscp-value1	Specifies the start DSCP priority.	The value can be the DiffServ code, ranging from 0 to 63; the value can also be the name of the DSCP service type, such as af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1-cs7, default, and ef. The service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dscp-value2	Specifies the end DSCP priority.	The value can be the DiffServ code, ranging from 0 to 63; the value can also be the name of the DSCP service type, such as af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1-cs7, default, and ef. The service types are as follows: ● af11: 10 ● af12: 12 ● af13: 14 ● af21: 18 ● af22: 20 ● af23: 22 ● af31: 26 ● af32: 28 ● af33: 30 ● af41: 34 ● af42: 36 ● af43: 38 ● cs1: 8 ● cs2: 16 ● cs3: 24 ● cs4: 32 ● cs5: 40 ● cs6: 48 ● cs7: 56 ● default: 0 ● ef: 46
low-limit-percentage	Specifies the lower drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, packets start to be discarded.	The value is an integer that ranges from 0 to 100. The default value is 30.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
high-limit-percentage	Specifies the upper drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, all the packets are discarded.	The value is an integer that ranges from *low-limit-percentage* to 100. The default value is 100.
discard-percentage	Specifies the maximum drop probability.	The value is an integer that ranges from 1 to 100. The default value is 10.

Views

Drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device uses the tail drop method and discards data packets at the end of a queue when congestion occurs. The tail drop method causes global Transmission Control Protocol (TCP) synchronization and reduces link usage.

WRED is a random drop method based on packet priorities. It has the following advantages:

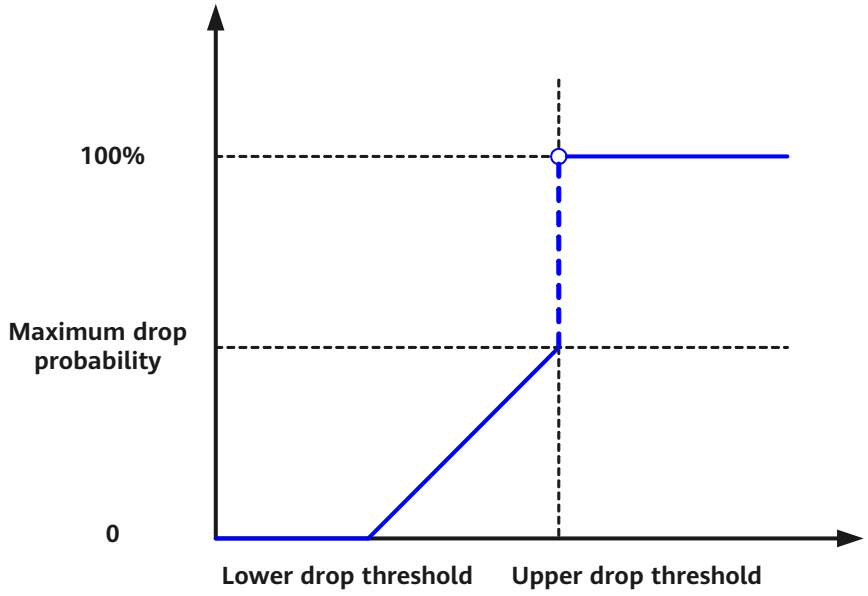
- WRED discards packets based on packet priorities, so the drop probability of packets with higher priorities is low.
- WRED sets the upper and lower drop thresholds and the maximum drop probability and discards packets randomly, which prevents global TCP synchronization.

The drop probability varies according to the queue length, as shown in **Figure 20-1**.

- When the queue length is smaller than the lower drop threshold, no packet is discarded.
- When the queue length is greater than the upper drop threshold, all packets are discarded.
- When the queue length is between the lower drop threshold and the upper drop threshold, incoming packets are discarded randomly. The drop probability cannot be greater than the maximum drop probability.

 Copyright © Huawei Technologies Co., Ltd.

Figure 20-1 WRED drop probability



Follow-up Procedure

Perform either of the following operations as required:

- Apply the drop profile to a queue profile.

  Run the **queue drop-profile** command in the queue profile view to bind the drop profile to each queue, and then run the **qos queue-profile (interface view)** command to bind the queue profile to an interface.
- Apply the drop profile to a traffic policy.

  Run the **drop-profile (traffic behavior view)** command to bind the drop profile to a traffic behavior, bind the traffic behavior and traffic classifier to the traffic policy, and then apply the traffic policy to an interface.

Precautions

When congestion occurs, packets with the maximum drop probability are discarded first.

The **dscp discard-percentage** and **ip-precedence discard-percentage** command cannot be used in the same drop profile view. If the drop profile based on IP priorities is used, you must run the **wred dscp** command.

If you run the **dscp discard-percentage** command with the same DSCP priority in the same drop profile view, only the latest configuration takes effect.

Example

In the drop profile **drop-profile1**, set the upper and lower drop thresholds to 80% and 50% and the maximum drop probability to 30% for packets with DSCP priority 3.

```
<Huawei> system-view
[Huawei] drop-profile drop-profile1
```

```
[Huawei-drop-profile-drop-profile1] wred dscp
[Huawei-drop-profile-drop-profile1] dscp 3 low-limit 50 high-limit 80 discard-percentage 30
```

Related Topics

20.4.1 display drop-profile

20.4.6 drop-profile (system view)

20.4.7 drop-profile (traffic behavior view)

20.4.5 ip-precedence discard-percentage

20.4.11 queue drop-profile

20.4.20 wred

20.4.5 ip-precedence discard-percentage

Function

The **ip-precedence discard-percentage** command sets WRED parameters for packets with a specified IP precedence, including the upper and lower drop thresholds and the maximum drop probability.

The **undo ip-precedence** command restores the default values of WRED parameters for packets with a specified IP precedence.

By default, the lower drop threshold is 30%, the upper drop threshold is 100%, and the maximum drop probability is 10%.

Format

ip-precedence { *ip-precedence-value1* [**to** *ip-precedence-value2*] } &<1-10> **low-limit** *low-limit-percentage* **high-limit** *high-limit-percentage* **discard-percentage** *discard-percentage*

undo ip-precedence [*ip-precedence-value1* [**to** *ip-precedence-value2*]] &<1-10>

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-precedence-value1	Specifies the start IP precedence.	The value can be an integer or a name. The integer ranges from 0 to 7. The mappings between names and numbers are as follows: ● network: 7 ● internet: 6 ● critical: 5 ● flash-override: 4 ● flash: 3 ● immediate: 2 ● priority: 1 ● routine: 0
ip-precedence-value2	Specifies the end IP precedence.	The value can be an integer or a name. The integer ranges from 0 to 7. The mappings between names and numbers are as follows: ● network: 7 ● internet: 6 ● critical: 5 ● flash-override: 4 ● flash: 3 ● immediate: 2 ● priority: 1 ● routine: 0
low-limit-percentage	Specifies the lower drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, packets start to be discarded.	The value is an integer that ranges from 0 to 100. The default value is 30.
high-limit-percentage	Specifies the upper drop threshold. When the percentage of the packet count in a queue to the queue length reaches this value, all the packets are discarded.	The value is an integer that ranges from *low-limit-percentage* to 100. The default value is 100.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
discard-percentage	Specifies the maximum drop probability.	The value is an integer that ranges from 1 to 100. The default value is 10.

Views

Drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device uses the tail drop method and discards data packets at the end of a queue when congestion occurs. The tail drop method causes global Transmission Control Protocol (TCP) synchronization and reduces link usage.

WRED is a random drop method based on packet priorities. It has the following advantages:

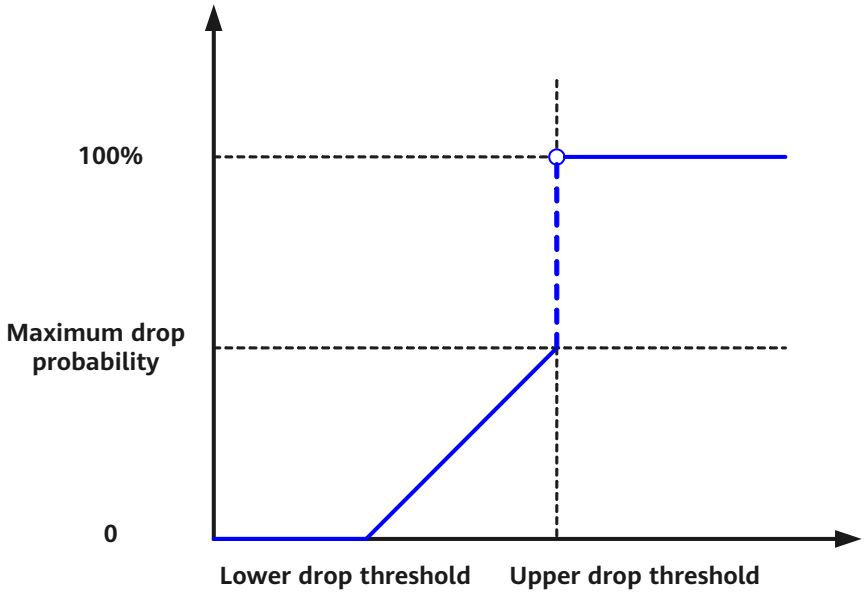
- WRED discards packets based on packet priorities, so the drop probability of packets with higher priorities is low.
- WRED sets the upper and lower drop thresholds and the maximum drop probability and discards packets randomly, which prevents global TCP synchronization.

The drop probability varies according to the queue length, as shown in **Figure 20-2**.

- When the queue length is smaller than the lower drop threshold, no packet is discarded.
- When the queue length is greater than the upper drop threshold, all packets are discarded.
- When the queue length is between the lower drop threshold and the upper drop threshold, incoming packets are discarded randomly. The drop probability cannot be greater than the maximum drop probability.

 Copyright © Huawei Technologies Co., Ltd.

Figure 20-2 WRED drop probability



Follow-up Procedure

Apply the drop profile to a queue profile or traffic policy:

- Apply the drop profile to a queue profile.

  Run the **queue drop-profile** command in the queue profile view to bind the drop profile to each queue, and then run the **qos queue-profile (interface view)** command to bind the queue profile to an interface.
- Apply the drop profile to a traffic policy.

  Run the **drop-profile (traffic behavior view)** command to bind the drop profile to a traffic behavior, bind the traffic behavior and traffic classifier to the traffic policy, and then apply the traffic policy to an interface.

Precautions

When congestion occurs, packets with the maximum drop probability are discarded first.

The **dscp discard-percentage** and **ip-precedence discard-percentage** command cannot be used in the same drop profile view. If the drop profile based on DSCP priorities is used, you must run the **wred ip-precedence** command.

If you run the **ip-precedence discard-percentage** command with the same precedence in the same drop profile view, only the latest configuration takes effect.

Example

In the drop profile **drop-profile1**, set the upper and lower drop thresholds to 80% and 50% and the maximum drop probability to 30% for packets with IP precedence 3.

```
<Huawei> system-view
[Huawei] drop-profile drop-profile1
[Huawei-drop-profile-drop-profile1] wred ip-precedence
[Huawei-drop-profile-drop-profile1] ip-precedence 3 low-limit 50 high-limit 80 discard-percentage 30
```

Related Topics

20.4.1 display drop-profile

20.4.6 drop-profile (system view)

20.4.7 drop-profile (traffic behavior view)

20.4.4 dscp discard-percentage

20.4.11 queue drop-profile

20.4.20 wred

20.4.6 drop-profile (system view)

Function

The **drop-profile** command creates a drop profile and enters the drop profile view, or enters the existing drop profile view.

The **undo drop-profile** command deletes a drop profile.

By default, the drop profile **default** exists.

Format

drop-profile *drop-profile-name*

undo drop-profile *drop-profile-name*

Parameters

Parameter	Description	Value
drop-profile-name	Specifies the name of a drop profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device uses the tail drop method and discards data packets at the end of a queue when congestion occurs. The tail drop method causes global Transmission Control Protocol (TCP) synchronization and reduces link usage. The Weighted Random Early Detection (WRED) can solve the problem.

A drop profile defines WRED parameters for queues and is used to implement congestion avoidance for queues bound to the drop profile. The **drop-profile** command creates a drop profile and displays the drop profile view.

Follow-up Procedure

1. Set WRED parameters in the drop profile.

   Run the **dscp discard-percentage** or **ip-precedence discard-percentage** command in the drop profile view to set WRED parameters for packets with a specified DSCP priority or IP precedence.

2. Apply the drop profile.
   - Apply the drop profile to a queue profile.

     Run the **queue drop-profile** command in the queue profile view to bind the drop profile to each queue, and then run the **qos queue-profile (interface view)** command to bind the queue profile to an interface.
   - Apply the drop profile to a traffic policy.

     Run the **drop-profile (traffic behavior view)** command to bind the drop profile to a traffic behavior, bind the traffic behavior and traffic classifier to the traffic policy, and then apply the traffic policy to an interface.

Precautions

In addition to one reserved drop profile, a maximum of 63 drop profiles can be configured on the device.

A drop profile can be bound to queue profiles on WAN-side interfaces and layer 2 VE interfaces.

If a drop profile is not applied to an interface, you can directly modify or delete the drop profile. If a drop profile has been applied to an interface:

- When you modify the configuration of the drop profile, the modification is synchronized to the interface and takes effect immediately if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.
- If the drop profile has been bound to a queue profile, to delete the drop profile, run the **undo qos queue-profile** command in the interface view to unbind the queue profile from the interface, run the **undo queue drop-profile** command in the queue profile view to unbind the drop profile from the queue profile, and run the **undo drop-profile** command to delete the drop profile.
- If the drop profile has been bound to a traffic behavior, to delete the drop profile, run the **undo traffic-policy** command in the interface view to unbind the traffic policy containing the traffic behavior from the interface, run the **undo drop-profile** command in the traffic behavior view to unbind the drop profile from the traffic behavior, and run the **undo drop-profile** command to delete the drop profile.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create a drop profile named **hello-world**.

```
<Huawei> system-view
[Huawei] drop-profile hello-world
[Huawei-drop-profile-hello-world]
```

Related Topics

20.4.1 display drop-profile
20.4.4 dscp discard-percentage
20.4.5 ip-precedence discard-percentage
20.4.11 queue drop-profile
20.4.7 drop-profile (traffic behavior view)
20.4.20 wred

20.4.7 drop-profile (traffic behavior view)

Function

The **drop-profile** command binds a drop profile to a traffic behavior for Assured Forwarding (AF) queues or Best-Effort (BE) queues in Weighted Fair Queuing (WFQ) mode.

The **undo drop-profile** command unbinds a drop profile from a traffic behavior for AF queues or BE queues in WFQ mode.

By default, no traffic behavior is bound to a drop profile. All queues use tail drop.

Format

drop-profile *drop-profile-name*

undo drop-profile

Parameters

Parameter	Description	Value
drop-profile-name	Specifies the name of a drop profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Traffic behavior view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After a drop profile is bound to a traffic behavior, bind the traffic behavior and traffic classifier to a traffic policy and apply the traffic policy to an interface so that WRED parameters in the drop profile take effect on the interface.

Prerequisites

A drop profile has been created by using the **drop-profile (system view)** command.

Precautions

A queue profile can be bound to a traffic behavior in a traffic policy on the outbound WAN-side interface and layer 2 VE interface of the device.

When a traffic behavior is bound to a drop profile, the default queue length is 64 packets and cannot be set.

On the device, a traffic behavior can be bound to a drop profile for only AF queues and BE queues in WFQ mode. Tail drop is supported for only EF and LLQ queues.

When you bind a drop profile to or unbind a drop profile from a traffic behavior in a traffic policy that has been applied to an interface, the modification is synchronized to the interface and takes effect immediately if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

If you run the **drop-profile** command multiple times in the same traffic behavior view, only the latest configuration takes effect.

Example

Bind the drop profile **dp1** to the traffic behavior **database** where the WFQ mode is used and the number of queues is 16.

```
<Huawei> system-view
[Huawei] traffic behavior database
[Huawei-behavior-database] queue wfq queue-number 16
[Huawei-behavior-database] drop-profile dp1
```

Related Topics

20.1.1 classifier behavior

20.4.1 display drop-profile

20.4.6 drop-profile (system view)

20.4.4 dscp discard-percentage

20.4.5 ip-precedence discard-percentage

20.4.10 queue af

20.4.14 queue-length

20.4.17 queue wfq

20.1.44 traffic behavior

20.1.45 traffic classifier

 Copyright © Huawei Technologies Co., Ltd.

20.1.46 traffic policy
20.4.20 wred

20.4.8 qos queue-profile (interface view)

Function

The **qos queue-profile** command applies a queue profile to an interface.

The **undo qos queue-profile** command deletes a queue profile from an interface.

By default, an interface is not bound to any queue profile.

Format

qos queue-profile *queue-profile-name*

undo qos queue-profile

NOTE

- Layer 2 interfaces on the AR100&AR120serise, AR161, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161G-U, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR169G-L, AR169-P-M9, AR169RW-P-M9, AR169W-P-M9, AR1220C, AR1220F, AR1220E, AR1220EV, AR1220EVW and AR1220-8GE do not support the **qos queue-profile (interface view)** command.
- The 9ES2, 4GE-2S, 4ES2G-S, and 4ES2GP-S cards do not support the **qos queue-profile (interface view)** command.

Parameters

Parameter	Description	Value
queue-profile-name	Specifies the name of a queue profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A queue profile is a set of queue parameters that determine the scheduling mode between queues, length, weight, and traffic shaping rate of queues. After an

interface is bound to a queue profile, different services can be provided for queues on the interface.

After a queue profile is created, bind the queue profile to an interface so that the scheduling modes, lengths, weights, and traffic shaping rates of queues take effect on the interface.

Prerequisites

A queue profile has been created by using the **qos queue-profile (system view)** command.

Precautions

WAN interfaces and LAN interfaces of the device support different scheduling modes.

When you modify the configuration of the queue profile bound to an interface, the modification is synchronized to the interface and takes effect immediately if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

After a physical interface is bound to a virtual template interface to form an MP-link, the **qos queue-profile (system view)** command is invalid on the physical interface. For details about MP binding, see Implementing MP.

Example

Create a queue profile named **hello-world**, set the length of queue 0 to 4096 bytes, retain default values for other parameters, and apply the queue profile to Eth2/0/0.

```
<Huawei> system-view
[Huawei] qos queue-profile hello-world
[Huawei-qos-queue-profile-hello-world] queue 0 length bytes 4096
[Huawei-qos-queue-profile-hello-world] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] qos queue-profile hello-world
[Huawei-Ethernet2/0/0] quit
```

Related Topics

20.4.3 display qos queue-profile

20.4.9 qos queue-profile (system view)

20.3.17 queue gts

20.4.13 queue length

20.4.16 queue weight

20.4.19 schedule

20.4.9 qos queue-profile (system view)

Function

The **qos queue-profile** command creates a queue profile and displays its view, or directly displays the view of the existing queue profile.

The **undo qos queue-profile** command deletes a queue profile.

By default, no queue profile is configured.

Format

qos queue-profile *queue-profile-name*

undo qos queue-profile *queue-profile-name*

Parameters

Parameter	Description	Value
queue-profile-name	Specifies the name of a queue profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **qos queue-profile (system view)** command is used to create a queue profile. The queue profile is a set of queue parameters that determine the scheduling mode, lengths, weights, and traffic shaping rates of queues. After a queue profile is bound to an interface, different services can be provided for queues on the interface.

Follow-up Procedure

The **qos queue-profile (interface view)** command binds a queue profile to an interface.

Precautions

A maximum of 32 queue profiles can be configured on the device.

When you modify the configuration of the queue profile bound to an interface, the modification is synchronized to the interface and takes effect immediately if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

To delete the queue profile bound to an interface, run the **undo qos queue-profile** command in the interface view to unbind the queue profile from the interface. Then run the **undo qos queue-profile** *queue-profile-name* command in the system view to delete the queue profile.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

Only the scheduling mode can be set in a queue profile bound to a Layer 2 interface on the SRU of the AR150&AR200 series, AR161F, AR161F-DGP, AR161FG-L, AR161FG-Lc, AR161FGW-L, AR161FGW-La, AR161FGW-Lc, AR161FV-1P, AR161FW, AR161FW-P-M5, AR162F, AR168F, AR168F-4P, AR169F, AR169FVW, AR169FVW-8S, AR169JFVW-4B4S, AR169JFVW-2S, AR169FGW-L, AR169FGVW-L, AR1220, AR1220V, AR1220W and AR1220VW.

Example

Create a queue profile named **hello-world**.

```
<Huawei> system-view
[Huawei] qos queue-profile hello-world
[Huawei-qos-queue-profile-hello-world]
```

Related Topics

20.4.3 display qos queue-profile

20.4.8 qos queue-profile (interface view)

20.3.17 queue gts

20.4.13 queue length

20.4.16 queue weight

20.4.19 schedule

20.4.10 queue af

Function

The **queue af** command configures Assured Forwarding (AF) for packets of a certain type and sets the assured minimum bandwidth.

The **undo queue af** command cancels AF for packets of a certain type.

By default, AF is not configured for packets of a certain type.

Format

queue af bandwidth { *bandwidth* | [**remaining**] **pct** *percentage* }

undo queue af

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
remaining	Specifies the remaining bandwidth of an interface. If this parameter is specified: **pct** = AF queue bandwidth/(Actual available bandwidth of the interface - EF queue bandwidth) If this parameter is not specified: **pct** = AF queue bandwidth/Actual available bandwidth of the interface	-
bandwidth	Specifies the assured minimum bandwidth.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
pct *percentage*	Specifies the percentage of the minimum bandwidth to the available bandwidth on an interface.	The value is an integer that ranges from 1 to 100.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device provides the following types of queues for packets matching user-defined traffic classifiers:

- Assured Forwarding (AF) queues
- Expedited Forwarding (EF) queues
- Best Effort (BE) queues
- Low-latency (LLQ) queues

 Copyright © Huawei Technologies Co., Ltd.

AF ensures a low drop probability of packets when the rate of outgoing service traffic does not exceed the minimum bandwidth. It is applied to services of heavy traffic whose bandwidth needs to be ensured.

You can specify **remaining** to configure the percentage of the remaining available bandwidth to provide fine-grained bandwidth allocation. For example, an EF queue is configured and assigned 95% of the actual available bandwidth of the interface. The remaining 5% bandwidth needs to be allocated to two AF queues. One AF queue occupies 10% of the remaining bandwidth, and the other occupies 90% of the remaining bandwidth. You can specify **remaining**.

Follow-up Procedure

Create a traffic classifier and a traffic policy, bind the traffic classifier to the traffic behavior in the traffic policy, and then apply the traffic policy.

Precautions

AF can only be configured in a traffic behavior of a traffic policy on the outbound WAN-side interface and Layer 2 VE interface of the device.

An interface can be bound to only a traffic policy containing **queue af** or a queue profile.

A maximum of 64 AF queues are allowed in a traffic behavior of a traffic policy.

If multiple traffic behaviors in a traffic policy all define **queue af**, configure the percentage of the actual available bandwidth of the interface or percentage of the remaining bandwidth. If the percentage of the remaining bandwidth is configured, the sum of the percentages cannot exceed 100%.

If AF, EF, LLQ are configured in traffic behaviors bound to a traffic policy, the sum of bandwidth values for AF, EF, LLQ queues must be less than or equal to the available bandwidth of the interface to which the traffic policy is applied. The available bandwidth is as follows:

- If the **qos gts** or **qos gts adaptation-profile** command is not used on an interface:
  - The available bandwidth of a physical interface is the actual bandwidth of the physical interface. If the **qos lr** command is used on the physical interface, the available bandwidth is the actual bandwidth of the interface multiplied by the configured percentage of the rate for sending packets to the interface bandwidth.
  - The available bandwidth of a tunnel interface or a virtual Ethernet interface is 1 Gbit/s.
  - The available bandwidth of a logical interface such as the Eth-Trunk, MFR, and MP-Group formed by binding multiple interfaces or sub-interfaces is the total bandwidth of bound interfaces or sub-interfaces.
  - The available bandwidth of the dialer interface is the actual bandwidth of a bound physical interface or the sum of bandwidth of multiple bound physical interfaces.
- If the **qos gts** or **qos gts adaptation-profile** command is used on an interface, the available bandwidth is the CIR value.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the **queue af** command has been used in a traffic behavior, you cannot use the **queue ef**, **queue llq**, or **queue wfq** command in the traffic behavior.
- When a virtual template interface is bound to L2TP services, the percentage of the minimum bandwidth to the available bandwidth cannot be set on the virtual template interface.
- If a traffic policy containing the traffic behavior is applied to an interface, the **trust** command does not take effect on the interface.

If you run the **queue af** command multiple times in the same traffic behavior view, only the latest configuration takes effect.

Example

Configure AF for the traffic behavior **database** and set the minimum bandwidth to 20000 kbit/s.

```
<Huawei> system-view
[Huawei] traffic behavior database
[Huawei-behavior-database] queue af bandwidth 20000
```

Related Topics

20.1.1 classifier behavior

20.4.7 drop-profile (traffic behavior view)

20.3.8 gts (traffic behavior view)

20.4.12 queue ef

20.4.15 queue llq

20.4.17 queue wfq

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.4.11 queue drop-profile

Function

The **queue drop-profile** command binds a drop profile to a queue in a queue profile.

The **undo queue drop-profile** command unbinds a drop profile from a queue in a queue profile.

By default, a drop profile is not bound to any queue. All queues use tail drop.

Format

queue { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **drop-profile** *drop-profile-name*

undo queue { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **drop-profile**

Parameters

Parameter	Description	Value
start-queue-index [**to** *end-queue-index*]	Specifies the index of a queue bound to a drop profile. ● *start-queue-index* specifies the index of the first queue bound to a drop profile. The value is an integer that ranges from 0 to 7. ● *end-queue-index* specifies the index of the last queue bound to a drop profile. The value is an integer that ranges from 0 to 7. *end-queue-index* must be greater than *start-queue-index*. If **to** *end-queue-index* is not specified, only the queue specified by *start-queue-index* is bound to a drop profile.	-
drop-profile-name	Specifies the name of a drop profile.	The value is a string of 1 to 31 case-sensitive characters without spaces.

Views

Queue profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the device uses the tail drop method and discards data packets at the end of a queue when congestion occurs. The tail drop method causes global Transmission Control Protocol (TCP) synchronization and reduces link usage. The Weighted Random Early Detection (WRED) can solve the problem.

 Copyright © Huawei Technologies Co., Ltd.

A drop profile defines WRED parameters. The **queue drop-profile** command binds a queue to a drop profile. You can bind the drop profile to a queue profile and apply the queue profile to the interface to implement congestion avoidance for queues bound to the drop profile.

Prerequisites

A drop profile has been created by using the **drop-profile (system view)** command.

WFQ has been configured by using the **schedule** command.

Precautions

Drop profiles can be bound to only queues using WFQ on WAN-side interfaces and layer 2 VE interfaces of the device.

When you bind a drop profile to or unbind a drop profile from a queue in a queue profile that has been applied to an interface, the modification is synchronized to the interface and takes effect immediately if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

When running the **schedule** command to modify or delete the scheduling mode of a queue, you must delete the drop profile bound to the queue.

If you run the **queue drop-profile** command multiple times in the same queue profile view, only the latest configuration takes effect.

Example

Bind the drop profile **dp1** to queues 2 and 3 in the queue profile **qp1**.

```
<Huawei> system-view
[Huawei] qos queue-profile qp1
[Huawei-qos-queue-profile-qp1] schedule wfq 2 to 3
[Huawei-qos-queue-profile-qp1] queue 2 to 3 drop-profile dp1
```

Related Topics

20.4.1 display drop-profile

20.4.6 drop-profile (system view)

20.4.4 dscp discard-percentage

20.4.5 ip-precedence discard-percentage

20.4.20 wred

20.4.12 queue ef

Function

The **queue ef** command configures Expedited Forwarding (EF) for packets of a certain type and sets the minimum bandwidth.

The **undo queue ef** command cancels EF for packets of a certain type.

By default, EF is not configured for packets of a certain type.

 Copyright © Huawei Technologies Co., Ltd.

Format

queue ef bandwidth { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] }

undo queue ef

Parameters

Parameter	Description	Value
bandwidth	Specifies the minimum bandwidth for EF queues.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer that ranges from 32 to 4294967295, in bytes. By default, the CBS value is 25 times the value of *bandwidth*.
pct *percentage*	Specifies the percentage of the minimum bandwidth to the available bandwidth on an interface.	The value is an integer that ranges from 1 to 100.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device provides the following types of queues for packets matching user-defined traffic classifiers:

- Assured Forwarding (AF) queues
- Expedited Forwarding (EF) queues
- Best Effort (BE) queues
- Low-latency (LLQ) queues

After packets matching a rule enter EF queues, they are scheduled in Strict Priority (SP) mode. Packets in other queues are scheduled only after all the packets in EF queues are scheduled.

 Copyright © Huawei Technologies Co., Ltd.

EF is applied to the services requiring the low delay, low drop probability, assured bandwidth, and occupying low bandwidth, for example, voice packets.

NOTE

After the minimum bandwidth of EF queues is set, if there is traffic in other queues, EF queues can obtain the minimum bandwidth specified by *bandwidth*. If there is no traffic in other queues, EF queues can obtain the maximum bandwidth of the interface to ensure that high-priority packets are forwarded.

Follow-up Procedure

Create a traffic classifier and a traffic policy, bind the traffic classifier to the traffic behavior in the traffic policy, and then apply the traffic policy.

Precautions

EF can be configured in a traffic behavior of a traffic policy on the outbound WAN-side interface and Layer 2 VE interface of the device.

An interface can be bound to only a traffic policy containing **queue ef** or a queue profile.

If AF, EF, LLQ are configured in traffic behaviors bound to a traffic policy, the sum of bandwidth values for AF, EF, LLQ queues must be less than or equal to the available bandwidth of the interface to which the traffic policy is applied. When you use the bandwidth percentage to set the minimum bandwidth, the available bandwidth is as follows:

- If the **qos gts** or **qos gts adaptation-profile** command is not used on an interface:
  - The available bandwidth of a physical interface is the actual bandwidth of the physical interface. If the **qos lr** command is used on the physical interface, the available bandwidth is the actual bandwidth of the interface multiplied by the configured percentage of the rate for sending packets to the interface bandwidth.
  - The available bandwidth of a tunnel interface or a virtual Ethernet interface is 1 Gbit/s.
  - The available bandwidth of a logical interface such as the Eth-Trunk, MFR, and MP-Group formed by binding multiple interfaces or sub-interfaces is the total bandwidth of bound interfaces or sub-interfaces.
  - The available bandwidth of the dialer interface is the actual bandwidth of a bound physical interface or the sum of bandwidth of multiple bound physical interfaces.
- If the **qos gts** or **qos gts adaptation-profile** command is used on an interface, the available bandwidth is the CIR value.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- If the **queue ef** command has been used in a traffic behavior, you cannot use the **queue af**, **queue llq**, **queue wfq**, **gts (traffic behavior view)**, or **gts adaptation-profile** command in the traffic behavior.
- When a virtual template interface is bound to L2TP services, the percentage of the minimum bandwidth to the available bandwidth cannot be set on the virtual template interface.
- If a traffic policy containing the traffic behavior is applied to an interface, the **trust** command does not take effect on the interface.
- A minimum of four EF and LLQ queues are allowed in a traffic behavior of a traffic policy. Packets in EF or LLQ queues are scheduled in SP mode. Packets in AF queues and BE queues are scheduled only after packets in EF or LLQ queues are scheduled. Packets in EF or LLQ queues are scheduled in SP mode according to the sequence in which queues were configured. Packets in the queue that was configured first are scheduled first.

If you run the **queue ef** command multiple times in the same traffic behavior view, only the latest configuration takes effect.

Example

Configure EF for the traffic behavior **database**, and set the minimum bandwidth to 200 kbit/s and CBS value to 5000 bytes.

```
<Huawei> system-view
[Huawei] traffic behavior database
[Huawei-behavior-database] queue ef bandwidth 200 cbs 5000
```

Related Topics

20.1.1 classifier behavior
20.3.8 gts (traffic behavior view)
20.4.10 queue af
20.4.15 queue llq
20.4.17 queue wfq
20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy

20.4.13 queue length

Function

The **queue length** command sets the length of a queue.

The **undo queue length** command restores the default length of a queue.

Table 20-21 lists the default lengths of queues.

Table 20-21 Default lengths of queues in different scheduling modes

Scheduling Mode	Default Queue length
PQ	● AR100&AR120&AR150&AR160&AR200&AR1200&AR2200 (except the AR2240) series – WAN-side interfaces: 128000 bytes or 64 packets – LAN-side interfaces: 5120 bytes or 20 packets ● AR2240 (SRU40/SRU60/SRU100/SRU100E) and AR3260 (SRU40/SRU60/SRU100/SRU100E) – WAN-side interfaces: 128000 bytes or 64 packets – LAN-side interfaces: 5120 bytes or 20 packets ● AR2240 (SRU80/SRU200/SRU200E/SRU400), AR3200 (SRU80/SRU200/SRU200E/SRU400) and AR3600 series – WAN-side interfaces: 16384 bytes or 64 packets – LAN-side interfaces: 5120 bytes or 20 packets
DRR	LAN-side interfaces: 5120 bytes or 20 packets
WRR	LAN-side interfaces: 5120 bytes or 20 packets
WFQ	● AR100&AR120&AR150&AR160&AR200&AR1200&AR2200 (except the AR2240) series: 131072 bytes or 64 packets ● AR2240 (SRU40/SRU60/SRU100/SRU100E) and AR3260 (SRU40/SRU60/SRU100/SRU100E) series: 131072 bytes or 64 packets ● AR2240 (SRU80/SRU200/SRU200E/SRU400), AR3200 (SRU80/SRU200/SRU200E/SRU400) and AR3600 series: 16384 bytes or 64 packets ● WAN-side interfaces: 131072 bytes or 64 packets ● LAN-side interfaces (VE interface): 128000 bytes or 64 packets

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The default lengths of queues of layer 2 VE interfaces are the default lengths of queues of WAN-side-interfaces.

Format

queue { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **length** { **bytes** *bytes-value* | **packets** *packets-value* }*

undo queue { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **length** [**bytes** | **packets**]*

Parameters

Parameter	Description	Value
start-queue-index [**to** *end-queue-index*]	Specifies the index of a queue. ● *start-queue-index* specifies the index of the first queue. The value is an integer that ranges from 0 to 7. ● *end-queue-index* specifies the index of the last queue. The value is an integer that ranges from 0 to 7. If **to** *end-queue-index* is not specified, the queue length is configured for only the queue specified by *start-queue-index*.	-
bytes *bytes-value*	Specifies the maximum number of bytes that can be buffered in a queue.	The value is an integer that ranges from 2048 to 2097152.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
packets *packets-value*	Specifies the maximum number of packets that can be buffered in a queue.	The value is an integer. The value range is as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-1024 ● AR1200&AR2200 (except the AR2240) series: 1-2048 ● AR2240 (SRU40/SRU60/SRU100/SRU100E) and AR3260 (SRU40/SRU60/SRU100/SRU100E): 1-2048 ● AR2240 (SRU80/SRU200/SRU200E/SRU400), AR3260 (SRU80/SRU200/SRU200E/SRU400) and AR3670: 1-1023

Views

Queue profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The queue length affects queue traffic shaping, congestion management, and congestion avoidance. When the number of packets in a queue reaches the maximum value or the total number of bytes in a queue reaches the maximum value, the queue does not receive packets. Instead, the queue discards the excess packets.

A longer queue buffers more packets but introduces a longer delay. If congestion occurs on a network intermittently, a longer queue prevents unnecessary packet loss. If congestion always occurs on a network, increasing the queue length cannot solve the problem. To solve this problem, increase the bandwidth.

Follow-up Procedure

Run the **qos queue-profile (interface view)** command to bind the queue profile to an interface.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

When you modify the queue length in the queue profile bound to an interface, the modification is synchronized to the interface automatically if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

NOTE

- A queue profile that defines the queue length using the **queue length** command cannot be applied to an interface of the 4ES2G-S, 4ES2GP-S, or 9ES2 card.
- A queue profile that defines the queue length using the **queue length** command cannot be applied to AR100&AR120&AR150&AR160&AR200 series Layer 2 FE interfaces and Layer 2 GE interfaces.
- A queue profile that defines the queue length using the **queue length** command cannot be applied to FE interfaces on the AR1200 series SRU.
- When a queue profile is applied to a LAN-side interface, the queue length can be set to an integer in the range of 1 to 25. If the queue length on the device is set to be larger than 25, the system displays the following error message:
  Error: The queue length of this profile exceeds the upper limit.

If you run the **queue length** command multiple times in the same queue profile view, only the latest configuration takes effect.

Example

Create a queue profile named **hello-world** and set the length of queues 0 and 1 to 4096 bytes.

```
<Huawei> system-view
[Huawei] qos queue-profile hello-world
[Huawei-qos-queue-profile-hello-world] queue 0 to 1 length bytes 4096
```

Related Topics

20.4.3 display qos queue-profile
20.4.8 qos queue-profile (interface view)
20.4.9 qos queue-profile (system view)
20.4.19 schedule

20.4.14 queue-length

Function

The **queue-length** command sets the maximum length of a queue in a traffic behavior.

The **undo queue-length** command restores the default length of a queue.

By default, a queue can store a maximum of 131072 bytes or 64 packets.

Format

queue-length { **bytes** *bytes-value* | **packets** *packets-value* }*

undo queue-length

Parameters

Parameter	Description	Value
bytes *bytes-value*	Specifies the maximum number of bytes buffered in a queue.	The value is an integer that ranges from 2048 to 2097152.
packets *packets-value*	Specifies the maximum number of packets buffered in a queue.	The value is an integer. The value range is as follows: ● AR100&AR120&AR150&AR160&AR200 series: 1-1024 ● AR1200 series, AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2204E-D, AR2202-48FE, AR2204, AR2220E, AR2220, AR2240C, AR2240 (SRU40/SRU60/SRU100/SRU100E), AR3260 (SRU40/SRU60/SRU100/SRU100E): 1-2048 ● AR2240 (SRU80/SRU200/SRU200E/SRU400), AR3260 (SRU80/SRU200/SRU200E/SRU400), AR3670: 1-1023

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **queue-length** command is used to set the maximum length of a queue. The queue length affects queue traffic shaping, congestion management, and

 Copyright © Huawei Technologies Co., Ltd.

congestion avoidance. If the number of packets in a queue reaches the maximum value, the queue directly discards the packets. A longer queue buffers more packets but introduces a longer delay. If congestion occurs on a network intermittently, buffering more packets prevents unnecessary packet loss. If congestion always occurs on a network, increasing the queue length cannot solve the problem. You need to increase the bandwidth.

Prerequisites

The queue scheduling mode has been configured using the **queue ef**, **queue af** or **queue wfq** command.

Precautions

The queue length and drop method can be configured in a traffic behavior of a traffic policy on the outbound WAN or layer 2 VE interface of the device.

If you run the **queue-length** command multiple times in the same traffic behavior view, only the latest configuration takes effect.

Example

Configure AF in the traffic behavior **database**, set the minimum assured bandwidth to 200 kbit/s, and set the queue length to 16 packets.

```
<Huawei> system-view
[Huawei] traffic behavior database
[Huawei-behavior-database] queue af bandwidth 200
[Huawei-behavior-database] queue-length packets 16
```

Related Topics

20.1.1 classifier behavior

20.4.7 drop-profile (traffic behavior view)

20.4.10 queue af

20.4.12 queue ef

20.4.17 queue wfq

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.4.15 queue llq

Function

The **queue llq** command configures low latency queuing (LLQ) for packets of a certain type and set the maximum bandwidth.

The **undo queue llq** command cancels the configuration.

By default, LLQ is not configured for packets of a certain type.

 Copyright © Huawei Technologies Co., Ltd.

Format

queue llq bandwidth { *bandwidth* [**cbs** *cbs-value*] | **pct** *percentage* [**cbs** *cbs-value*] }

undo queue llq

Parameters

Parameter	Description	Value
bandwidth	Specifies the maximum bandwidth for LLQ queues.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
cbs *cbs-value*	Specifies the committed burst size (CBS).	The value is an integer that ranges from 32 to 4294967295, in bytes. By default, the CBS value is 25 times the value of *bandwidth*.
pct *percentage*	Specifies the percentage of the maximum bandwidth to the available bandwidth on an interface.	The value is an integer that ranges from 1 to 100.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device provides the following types of queues for user-defined traffic classifiers:

- Assured Forwarding (AF) queues
- Expedited Forwarding (EF) queues
- Best Effort (BE) queues
- Low Latency queuing (LLQ) queues

LLQ queues are special type of EF queues and have shorter delay.

Follow-up Procedure

Create a traffic classifier and a traffic policy, bind the traffic classifier to the traffic behavior in the traffic policy, and then apply the traffic policy.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

LLQ can be configured in a traffic behavior of a traffic policy on the outbound WAN-side interface and Layer 2 VE interface of the device.

A traffic policy containing a traffic behavior and a drop profile cannot be used on an interface.

You cannot use the **queue-length** command to set the length for LLQ queues.

A low drop probability is ensured only when the traffic rate of LLQ queues falls below the maximum bandwidth.

If AF, EF, LLQ are configured in traffic behaviors bound to a traffic policy, the sum of bandwidth values for AF, EF, LLQ queues must be less than or equal to the available bandwidth of the interface to which the traffic policy is applied. When you use the bandwidth percentage to set the maximum bandwidth, the available bandwidth is as follows:

- If the **qos gts** or **qos gts adaptation-profile** command is not used on an interface:
  - The available bandwidth is the actual physical bandwidth of a physical interface. If the **qos lr** command is used on the physical interface, the available bandwidth is the actual bandwidth of the interface multiplied by the configured percentage of the rate for sending packets to the interface bandwidth.
  - The available bandwidth of a tunnel interface or a virtual Ethernet interface is 1 Gbit/s.
  - The available bandwidth of a logical interface such as the Eth-Trunk, MFR interface, or MP-Group interface that is bundled by multiple interfaces or sub-interfaces is the total bandwidth of all bundled interfaces or sub-interfaces.
  - The available bandwidth of the dialer interface is the actual bandwidth of a bound physical interface or the sum of bandwidth of multiple bound physical interfaces.
- If the **qos gts** or **qos gts adaptation-profile** command is used on an interface, the available bandwidth is the CIR value.

NOTE

- If the **queue llq** command has been used in a traffic behavior, you cannot use the **queue ef**, **queue af**, **queue wfq**, **gts (traffic behavior view)**, or **gts adaptation-profile** command in the traffic behavior.
- When a virtual template interface is bound to L2TP services, the percentage of the maximum bandwidth to the available bandwidth cannot be set on the virtual template interface.
- If a traffic policy containing the traffic behavior is applied to an interface, the **trust** command does not take effect on the interface.
- A maximum of four EF and LLQ queues are allowed in a traffic behavior of a traffic policy. Packets in EF or LLQ queues are scheduled in SP mode. Packets in AF queues and Weighted Fair Queuing (WFQ) queues are scheduled only after packets in EF or LLQ queues are scheduled. Packets in EF or LLQ queues are scheduled in SP mode according to the sequence in which queues were configured. Packets in the queue that was configured first are scheduled first.

 Copyright © Huawei Technologies Co., Ltd.

If you run the **queue llq** command multiple times in the same traffic behavior view, only the latest configuration takes effect.

Example

Configure LLQ for the traffic behavior **database** and set the maximum bandwidth to 1000 kbit/s.

```
<Huawei> system-view
[Huawei] traffic behavior database
[Huawei-behavior-database] queue llq bandwidth 1000
```

Related Topics

20.1.1 classifier behavior

20.3.8 gts (traffic behavior view)

20.4.10 queue af

20.4.12 queue ef

20.4.17 queue wfq

20.1.44 traffic behavior

20.1.45 traffic classifier

20.1.46 traffic policy

20.4.16 queue weight

Function

The **queue weight** command sets the weight of a queue.

The **undo queue weight** command restores the default weight of a queue.

By default, the weight of a queue is 10.

Format

queue { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **weight** *weight-value*

undo queue { *start-queue-index* [**to** *end-queue-index*] } &<1-10> **weight**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start-queue-index [**to** *end-queue-index*]	Specifies the index of a queue. ● *start-queue-index* specifies the index of the first queue. The value is an integer that ranges from 0 to 7. ● *end-queue-index* specifies the index of the last queue. The value is an integer that ranges from 0 to 7. If **to** *end-queue-index* is not specified, the weight is configured for only the queue specified by *start-queue-index*.	-
weight *weight-value*	Specifies the queue weight.	The value is an integer that ranges from 1 to 100.

Views

Queue profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packets in queues are scheduled unevenly according to different service requirements. When Deficit Round Robin (DRR), Weighted Round Robin (WRR), or Weighted Fair Queuing (WFQ) scheduling is used, packets in queues are scheduled based on queue weights. Packets in queues with a greater weight are scheduled more times.

Prerequisites

A scheduling mode has been configured by using the **schedule** command.

Follow-up Procedure

Run the **qos queue-profile (interface view)** command to bind the queue profile to an interface.

Precautions

If PQ scheduling is used, packets in queues with lower priorities are processed only after all the packets in queues with higher priority are processed. Therefore, the weight cannot be set for these queues.

When you modify the weight in the queue profile bound to an interface, the modification is synchronized to the interface automatically if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

NOTE

- A queue profile that defines the queue weight using the **queue weight** command cannot be applied to an interface of the 4ES2G-S, 4ES2GP-S, or 9ES2 card.
- A queue profile that defines the queue weight using the **queue weight** command cannot be applied to AR100&AR120&AR150&AR160&AR200 series Layer 2 FE interfaces and Layer 2 GE interfaces.
- A queue profile that defines the queue weight using the **queue weight** command cannot be applied to FE interfaces on the AR1200 series SRU.

If you run the **queue weight** command multiple times in the same queue profile view, only the latest configuration takes effect.

Example

Create a queue profile named **hello-world** and set the scheduling mode of queues 0 to 3 to WRR, the weight of queues 0 and 1 to 20, and the weight of queues 2 and 3 to 30.

```
<Huawei> system-view
[Huawei] qos queue-profile hello-world
[Huawei-qos-queue-profile-hello-world] schedule wrr 0 to 3
[Huawei-qos-queue-profile-hello-world] queue 0 to 1 weight 20
[Huawei-qos-queue-profile-hello-world] queue 2 to 3 weight 30
```

Related Topics

20.4.3 display qos queue-profile

20.4.8 qos queue-profile (interface view)

20.4.9 qos queue-profile (system view)

20.3.17 queue gts

20.4.13 queue length

20.4.19 schedule

20.4.17 queue wfq

Function

The **queue wfq** command configures the device to send packets matching the default traffic classifier to BE queues in WFQ mode and sets the number of queues.

 Copyright © Huawei Technologies Co., Ltd.

The **undo queue wfq** command cancels the configuration.

By default, the device is not configured to send packets matching the default traffic classifier to BE queues in WFQ mode.

Format

queue wfq [**queue-number** *total-queue-number*]

undo queue wfq

Parameters

Parameter	Description	Value
queue-number *total-queue-number*	Specifies the number of BE queues in WFQ mode. If this parameter is not specified, one BE queue is used.	The value is 8, 16, 32, or 64. **NOTE** Currently, the actual value that takes effect on the device is 1.

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device provides the following types of queues for user-defined traffic classifiers:

- AF queues
- EF queues
- BE queues
- LLQ queues

After a traffic policy containing AF and EF is applied to an interface, AF, LLQ, and EF queues occupy some bandwidth of the interface and other packets enter BE queues. The device schedules packets in BE queues in WFQ mode and evenly allocates bandwidth to BE queues according to the IP precedence, and source and destination IP addresses. When a greater number of queues are set, WFQ allocates bandwidth more evenly but more resources are occupied.

WFQ is applied to the services insensitive to the delay and packet loss, for example, Internet access services.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Create a traffic policy, and bind the traffic classifier and the traffic behavior to the traffic policy, and apply the traffic policy to the interface.

Precautions

A traffic policy containing BE can be applied to the outbound direction on a WAN-side interface and layer 2 VE interface.

If the traffic policy bound to the traffic behavior containing **queue wfq** is applied to an interface:

- On the AR100&AR120&AR150&AR160&AR200 series, AR1200 series, AR2220E,, and AR2204:
  - If the **trust** command is not used (the interface priority is trusted), priorities of packets entering the same interface are changed to the same value. Packets still enter queues according to the WFQ algorithm, but the packets are scheduled evenly.
  - If the **trust** command is used, packet priorities are changed. Packets still enter queues, but are scheduled based on changed priorities because the WFQ algorithm allocates bandwidth based on packet priorities.
- On the AR2201-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E, AR2202-48FE, AR2220, AR2240C, AR2240 or AR3200&AR3600 series:
  - If the **trust** command is not used (the interface priority is trusted), priorities of packets entering the same interface are changed to the same value. Packets still enter queues according to the WFQ algorithm, but the packets are scheduled evenly.
  - If the **trust** command without **override** specified is used, the **trust** command on the interface does not take effect.
  - If the **trust** command with **override** specified is used, priorities in packets entering the interface are changed. Packets still enter queues, but are scheduled based on changed priorities because the WFQ algorithm allocates bandwidth based on packet priorities.

NOTE

- If the **queue wfq** command has been used in a traffic behavior, you cannot use the **queue ef**, **queue af**, or **queue llq** command in the traffic behavior.
- BE queues in WFQ mode use the remaining bandwidth of AF, LLQ, and EF queues; therefore, the traffic behavior must be bound to the default traffic classifier defined by the system. The remaining bandwidth is obtained by subtracting the minimum bandwidth and the maximum bandwidth from the interface bandwidth. In addition, the binding between the default traffic classifier and the traffic behavior must be configured last in the traffic policy so that all the packets in BE queues match this traffic classifier.

If you run the **queue wfq** command in the same traffic classifier view multiple times, only the latest configuration takes effect.

Example

Configure WFQ for the default traffic classifier bound to the traffic behavior **database** and set the number of queues to 16.

```
<Huawei> system-view
[Huawei] traffic behavior database
[Huawei-behavior-database] queue wfq queue-number 16
```

Related Topics

20.1.1 classifier behavior
20.4.7 drop-profile (traffic behavior view)
20.3.8 gts (traffic behavior view)
20.4.10 queue af
20.4.12 queue ef
20.4.15 queue llq
20.1.44 traffic behavior
20.1.45 traffic classifier
20.1.46 traffic policy

20.4.18 reset qos queue statistics

Function

The **reset qos queue statistics** command clears queue-based traffic statistics on an interface.

Format

reset qos queue statistics interface *interface-type interface-number* [**queue** *queue-index*]

reset qos queue statistics interface virtual-template *vt-number* **virtual-access** *va-number* [**queue** *queue-index*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears queue-based traffic statistics on a specified interface. • *interface-type* specifies the type of the interface. • *interface-number* specifies the number of the interface.	-
virtual-template *vt-number*	Displays queue-based traffic statistics on a specified virtual template interface. *vt-number* specifies the number of the virtual template interface.	The value is an integer that ranges from 0 to 1023.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
virtual-access *va-number*	Displays queue-based traffic statistics on a specified virtual access interface. *va-number* specifies the number of the virtual access interface.	The value is an integer that ranges from 0 to 1023.
queue *queue-index*	Displays statistics on the queue with a specified index.	The value is an integer that ranges from 0 to 7.

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect queue-based statistics within a certain period, run the **reset qos queue statistics** command to clear the existing statistics first.

Precautions

Queue-based statistics cannot be restored after you clear them. Therefore, exercise caution when you run the command.

Example

Clear queue-based traffic statistics on Eth2/0/0.

```
<Huawei> reset qos queue statistics interface ethernet 2/0/0
```

Related Topics

20.4.2 display qos queue statistics

20.4.19 schedule

Function

The **schedule** command configures a scheduling mode between queues in a queue profile.

The **undo schedule** command restores the default scheduling mode between queues in a queue profile.

By default, an interface is not bound to any queue profile; all the queues on LAN-side interfaces (except Layer 2 VE interfaces) use WRR, and all the queues on WAN-side interfaces and Layer 2 VE interfaces use WFQ.

Format

In the queue profile bound to WAN-side interfaces:

schedule { **pq** *start-queue-index* [**to** *end-queue-index*] | **wfq** *start-queue-index* [**to** *end-queue-index*] }*

undo schedule

In the queue profile bound to LAN-side interfaces:

schedule { **pq** *start-queue-index* [**to** *end-queue-index*] | **drr** *start-queue-index* [**to** *end-queue-index*] | **wrr** *start-queue-index* [**to** *end-queue-index*] }*

undo schedule

Parameters

Parameter	Description	Value
pq	Indicates PQ scheduling.	-
drr	Indicates Deficit Round Robin (DRR) scheduling.	-
wrr	Indicates Weighted Round Robin (WRR) scheduling.	-
wfq	Indicates Weighted Fair Queuing (WFQ) scheduling.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
start-queue-index [**to** *end-queue-index*]	Specifies the index of a queue. ● *start-queue-index* specifies the index of the first queue. ● *end-queue-index* specifies the index of the last queue. If **to** *end-queue-index* is not specified, the scheduling mode is configured for only the queue specified by *start-queue-index*.	*start-queue-index* and *end-queue-index* are integers that range from 0 to 7. A larger value indicates a higher priority of a queue. **NOTE** ● When a queue profile applies to a Layer 2 interface of the AR150, AR160 (except the AR161, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR169G-L, AR169-P-M9, AR169RW-P-M9 and AR169W-P-M9) and AR200 series, *start-queue-index* is an integer that ranges from 0 to 3. A larger value indicates a higher priority of a queue. ● When a queue profile applies to a Layer 2 interface of the SPU on the AR1200 (except the AR1220C, AR1220F, AR1220E, AR1220EV, AR1220EVW and AR1220-8GE) series, *start-queue-index* is an integer that ranges from 0 to 3. A larger value indicates a higher priority of a queue.

Views

Queue profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs on a network intermittently, congestion management needs to be performed to provide high QoS for delay-sensitive services. Congestion management is implemented by using queue scheduling technologies.

When the network is congested, you can configure a scheduling mode for a queue so that the delay and jitter of various service packets can be adjusted in the following manners: The packets of delay-sensitive services, such as the video service and the voice service, can be processed preferentially. Among the delay-insensitive services, such as the email service, the packets with the same priority are processed equally and the packets with different priorities are processed based on their weights.

Follow-up Procedure

Run the **qos queue-profile (interface view)** command to bind the queue profile to an interface.

Precautions

When you modify the scheduling mode in the queue profile bound to an interface, the modification is synchronized to the interface automatically if the interface supports this configuration. If the interface does not support this configuration, the system displays a configuration failure message.

WAN-side and LAN-side interfaces of the device support different scheduling modes. When the **schedule** command used in the queue profile view is not bound to any interface, all scheduling modes can be configured. If the **schedule** command is used in the queue profile bound to an interface, the system displays an error message when you configure a scheduling mode denied by the interface. Table 1 shows the scheduling modes supported by LAN-side interfaces and WAN-side interfaces.

 Copyright © Huawei Technologies Co., Ltd.

Table 20-22 Scheduling modes supported by each interface

Interface	Scheduling Mode
LAN interface	● PQ ● DRR ● WRR ● PQ+DRR ● PQ+WRR **NOTE** ● Layer 2 interfaces on the AR150&AR160 (except the AR161, AR161EW, AR161EW-M1, AR161G-L, AR161G-Lc, AR161W, AR169, AR169CVW, AR169CVW-4B4S, AR169JFVW-4B4S, AR169JFVW-2S, AR169EGW-L, AR169EW, AR169G-L, AR169-P-M9, AR169RW-P-M9 and AR169W-P-M9)&AR200 series support only PQ, WRR, and PQ+WRR, but do not support DRR. ● Layer 2 interfaces on the AR1200 (except the AR1220C, AR1220F, AR1220E, AR1220EV, AR1220EVW and AR1220-8GE) series SRU support only PQ, WRR, and PQ+WRR, but do not support DRR. ● Layer 2 VE interfaces only support PQ, WFQ and PQ+WFQ.
WAN interface	● PQ ● WFQ ● PQ+WFQ

The mixed scheduling mode indicates that some queues use PQ scheduling and some queues use other scheduling modes. PQ scheduling can be configured for one queue with the highest priority or multiple queues with consecutive higher priorities.

- When a queue uses PQ scheduling, other queues whose priorities are higher than the priority of this queue also use PQ scheduling.
- When a queue uses non-PQ scheduling, other queues whose priorities are lower than the priority of this queue also use this scheduling mode.

A queue can use only one scheduling mode. If you set multiple scheduling modes for a queue, only the latest configuration takes effect.

Example

Create a queue profile named **hello-world** and set the scheduling mode of queues 0 to 3 to WRR.

```
<Huawei> system-view
[Huawei] qos queue-profile hello-world
[Huawei-qos-queue-profile-hello-world] schedule wrr 0 to 3
```

Related Topics

20.4.3 display qos queue-profile
20.4.8 qos queue-profile (interface view)
20.4.9 qos queue-profile (system view)
20.3.17 queue gts
20.4.13 queue length
20.4.16 queue weight

20.4.20 wred

Function

The **wred** command configures a WRED drop profile based on DSCP or IP priorities.

By default, a WRED drop profile based on IP priorities is used.

NOTE

LAN-side subcards do not support WRED.

Format

wred { **dscp** | **ip-precedence** }

Parameters

Parameter	Description	Value
dscp	Indicates that a WRED drop profile based on DSCP priorities is used.	-
ip-precedence	Indicates that a WRED drop profile based on IP precedences is used.	-

Views

Drop profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A drop profile defines WRED parameters for queues and is used to implement congestion avoidance for queues bound to the drop profile.

The device supports a WRED drop profile based on DSCP or IP priorities:

- The value of an IP priority ranges from 0 to 7.
- The value of a DSCP priority ranges from 0 to 63.
- Eight DSCP priorities correspond to one IP priority.

WRED based on DSCP priorities differentiates services more refinedly.

Follow-up Procedure

Run the **dscp discard-percentage** or **ip-precedence discard-percentage** command to configure a WRED drop profile based on DSCP priorities or IP precedences.

Precautions

If WRED parameters have been configured in the drop profile:

- If the priority specified by the **wred** command is different from the priority used by the WRED drop profile, the WRED drop profile uses the priority specified by the **wred** command and default values of WRED parameters are restored: The lower drop threshold is 30%, the upper drop threshold is 100%, and the maximum drop probability is 10%.
- If the priority specified by the **wred** command is the same as the priority used by the WRED drop profile, default values of WRED parameters are not restored.

Example

Configure a WRED drop profile based on DSCP priorities and set default WRED parameters.

```
<Huawei> system-view
[Huawei] drop-profile drop-profile1
[Huawei-drop-profile-drop-profile1] wred dscp
```

Related Topics

20.4.1 display drop-profile
20.4.4 dscp discard-percentage
20.4.6 drop-profile (system view)
20.4.7 drop-profile (traffic behavior view)
20.4.5 ip-precedence discard-percentage
20.4.11 queue drop-profile

20.5 Filtering Configuration Commands

 Copyright © Huawei Technologies Co., Ltd.

20.5.1 deny | permit

Function

The **deny** | **permit** command configures access control for service packets based on traffic classifiers.

- The **deny** command prevents service flows that match a specified rule from passing through.
- The **permit** command forwards packets matching traffic classification rules according to the original policy.

By default, the **permit** command is used to forward packets matching traffic classification rules according to the original policy.

Format

deny | **permit**

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device implements access control using a traffic policy. That is, you can use a traffic policy containing **deny** | **permit** on the device so that the device provides the firewall function to filter out specified types of packets. The **deny** | **permit** command only filters data packets, but does not process control packets such as STP BPDUs sent to the CPU.

Precautions

When you specify a packet filtering action for packets matching an ACL, if the ACL rule defines **permit**, the device processes packets according to the action (**deny** or **permit**) in the traffic behavior. If the ACL rule defines **deny**, the device discards packets regardless of whether **deny** or **permit** is configured in the traffic behavior.

If the **deny** action is configured together with other actions in the same traffic behavior, the other actions (except traffic statistics) do not take effect. For this reason, before adding another traffic action that is not traffic statistics to a traffic behavior, ensure that the traffic behavior does not contain the **deny** action or run the **permit** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a traffic policy **p1** to prevent the packets from VLAN 2 to pass through Eth2/0/0.

```
<Huawei> system-view
[Huawei] traffic classifier c1
[Huawei-classifier-c1] if-match vlan-id 2
[Huawei-classifier-c1] quit
[Huawei] traffic behavior b1
[Huawei-behavior-b1] deny
[Huawei-behavior-b1] quit
[Huawei] traffic policy p1
[Huawei-trafficpolicy-p1] classifier c1 behavior b1
[Huawei-trafficpolicy-p1] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] traffic-policy p1 inbound
```

Related Topics

20.1.44 traffic behavior

20.6 Statistics Configuration Commands

20.6.1 statistic enable (traffic behavior view)

Function

The **statistic enable** command enables the traffic statistics function in a traffic behavior.

The **undo statistic enable** command disables the traffic statistics function in a traffic behavior.

By default, the traffic statistics function in a traffic behavior is disabled.

Format

statistic enable

undo statistic enable

Parameters

None

Views

Traffic behavior view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To view the statistics on a traffic policy, you can use the **statistic enable** command to enable the statistics function. After the statistics function is enabled, you can use the **display traffic policy statistics** command to view the statistics.

Follow-up Procedure

Run the **traffic policy** command to create a traffic policy and run the **classifier behavior** command in the traffic policy view to bind the traffic classifier to the traffic behavior containing the traffic statistics collection function.

Example

Enable the statistics function in a traffic behavior **test**.

```
<Huawei> system-view
[Huawei] traffic behavior test
[Huawei-behavior-test] statistic enable
```

Related Topics

20.1.5 display traffic policy statistics

20.1.41 reset traffic policy statistics

20.1.44 traffic behavior

20.6.2 statistics enable (QoS profile view)

Function

The **statistics enable** command enables traffic statistics in a QoS profile.

The **undo statistics enable** command disables traffic statistics in a QoS profile.

By default, the traffic statistics function is disabled in a QoS profile.

Format

statistics enable

undo statistics enable

Parameters

None

Views

QoS profile view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

This command collects traffic statistics of successfully authenticated online users. Then the device sends the statistics result to the accounting server, and the accounting server performs accounting based on the statistics result.

Follow-up Procedure

Apply the QoS profile in the AAA service scheme view.

Example

Enable traffic statistics in the QoS profile **huawei**.

```
<Huawei> system-view
[Huawei] qos-profile huawei
[Huawei-qos-profile-huawei] statistics enable
```

Related Topics

20.3.18 qos-profile

20.7 ACL-based Simplified Traffic Policy Commands

20.7.1 acl forward-algorithm hash

Function

The **acl forward-algorithm hash enable** command changes the algorithm used to search for ACL entries to the hash algorithm for simplified ACLs on an interface.

The **acl forward-algorithm hash disable** command disables the function of changing the algorithm used to search for ACL entries for simplified ACLs on an interface.

By default, the function of changing the algorithm used to search for ACL entries is enabled for simplified ACLs.

NOTE

Only V200R010C10 and later versions support this command.

Format

acl forward-algorithm hash { **enable** | **disable** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
enable	Changes the algorithm used to search for ACL entries to the hash algorithm for simplified ACLs on an interface.	-
disable	Disables the function of changing the algorithm used to search for ACL entries for simplified ACLs on an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In scenarios where there are a large number of flow entries, if simplified ACL services are configured on an interface, you can use this command to change the algorithm used to search for ACL entries to the hash algorithm for simplified ACLs. This improves the forwarding performance of the device.

Configuration Impact

If this command is run for scenarios where there are only a small number of flow entries, the forwarding performance of simplified ACL services will be affected. Therefore, use this command under the guidance of Huawei engineers.

Example

Change the algorithm used to search for ACL entries to the hash algorithm for simplified ACLs on an interface.

```
<Huawei> system-view
[Huawei] acl forward-algorithm hash enable
```

20.7.2 display traffic-filter applied-record

Function

The **display traffic-filter applied-record** command displays the record about ACL-based packet filtering.

Format

display traffic-filter applied-record

Parameters

None

Views

All views

Default Level

2: Configuration level

Usage Guidelines

The **display traffic-filter applied-record** command displays the record about ACL-based packet filtering. The command output helps you check the ACL-based packet filtering configuration and locate faults.

Example

Display the record about ACL-based packet filtering.

Table 20-23 Description of the display traffic-filter applied-record command output

Item	Description
Interface	Interface to which ACL-based packet filtering is applied.
Direction	Direction in which ACL-based packet filtering is configured: ● inbound: ACL-based packet filtering is configured in the inbound direction. ● outbound: ACL-based packet filtering is configured in the outbound direction.
AppliedRecord	Record about ACL-based packet filtering.

Related Topics

20.7.3 display traffic-filter statistics
20.7.4 reset traffic-filter statistics
20.1.49 traffic-policy (interface view)

20.7.3 display traffic-filter statistics

Function

The **display traffic-filter statistics** command displays statistics on ACL-based packet filtering on an interface.

Format

display traffic-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** } [**verbose rule-base**]

display traffic-filter statistics interface virtual-template *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** } [**verbose rule-base**]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics on packet filtering on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
virtual-template *vt-number* **virtual-access** *va-number*	Specifies the number of a virtual template interface. Displays statistics on packet filtering on a specified virtual interface. ● **virtual-template** *vt-number* specifies the number of a virtual template interface. The value is an integer that ranges from 0 to 1023. ● **virtual-access** *va-number* specifies the number of a virtual access interface. The value is an integer that ranges from 0 to 1023.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
inbound	Displays statistics on packet filtering in the inbound direction.	-
outbound	Displays statistics on packet filtering in the outbound direction.	-
verbose rule-base	Displays statistics on packets that are filtered based on ACL rules.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To view statistics on ACL-based packet filtering, run the **display traffic-filter statistics** command.

Prerequisites

ACL-based packet filtering has been configured using the **traffic-filter (interface view)** command.

Example

Display statistics on outgoing packets that are filtered based on ACL on GE1/0/0.

```
<Huawei> display traffic-filter statistics interface gigabitethernet 1/0/0 outbound
-----------------------------------------------------------
  *interface GigabitEthernet1/0/0 outbound
  Matched: 5,617(Packets)  Passed: 0(Packets)   Dropped: 5,617(Packets)
```

Display statistics on outgoing packets that are filtered based on ACL rules on GE1/0/0.

```
<Huawei> display traffic-filter statistics interface gigabitethernet 1/0/0 outbound verbose rule-base
-----------------------------------------------------------
  *interface GigabitEthernet1/0/0 outbound
 rule 5 permit icmp
  Passed Packet                    0,Passed Bytes                    0
  Dropped Packet                     0,Dropped Bytes                     0
```

Table 20-24 Description of the display traffic-filter statistics command output

Item	Description
interface GigabitEthernet1/0/0 outbound	Packets matching the ACL rule are filtered in the outbound direction on GigabitEthernet1/0/0. To filter packets based on an ACL, run the **traffic-filter (interface view)** command.
Matched	Number of packets matching ACL rules.
Passed	Number of forwarded packets matching ACL rules.
Dropped	Number of discarded packets matching ACL rules.
rule 5 permit icmp	Matched ACL rules.
Passed Packet	Number of forwarded packets matching ACL rules.
Passed Bytes	Number of forwarded bytes matching ACL rules.
Dropped Packet	Number of discarded packets matching ACL rules.
Dropped Bytes	Number of discarded bytes matching ACL rules.

Related Topics

20.7.5 traffic-filter (interface view)
20.7.4 reset traffic-filter statistics

20.7.4 reset traffic-filter statistics

Function

The **reset traffic-filter statistics** command clears statistics on ACL-based packet filtering on an interface.

Format

reset traffic-filter statistics interface *interface-type interface-number* { **inbound** | **outbound** }

reset traffic-filter statistics interface virtual-template *vt-number* **virtual-access** *va-number* { **inbound** | **outbound** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Clears statistics on packet filtering on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
virtual-template *vt-number* **virtual-access** *va-number*	Clears statistics on packet filtering on a specified virtual interface. ● **virtual-template** *vt-number* specifies the number of a virtual template interface. The value is an integer that ranges from 0 to 1023. ● **virtual-access** *va-number* specifies the number of a virtual access interface. The value is an integer that ranges from 0 to 1023.	-
inbound	Clears statistics on packet filtering in the inbound direction.	-
outbound	Clears statistics on packet filtering in the outbound direction.	-

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Before recollecting statistics on ACL-based packet filtering on an interface, run the **reset traffic-filter statistics** command to clear the existing statistics. Wait for a

period, and run the **display traffic-filter statistics** command to view the statistics on ACL-based packet filtering.

Example

Clear statistics on ACL-based packet filtering on GE1/0/0.

```
<Huawei> reset traffic-filter statistics interface gigabitethernet 1/0/0 inbound
```

Related Topics

20.7.5 traffic-filter (interface view)

20.7.3 display traffic-filter statistics

20.7.5 traffic-filter (interface view)

Function

The **traffic-filter** command applies an ACL to an interface to filter packets on the interface.

The **undo traffic-filter** command cancels the configuration.

By default, no ACL is applied to an interface to filter packets on the interface.

Format

traffic-filter { **inbound** | **outbound** } { **acl** | **ipv6 acl** } { *acl-number* | **name** *acl-name* }

undo traffic-filter { **inbound** | **outbound** } [**ipv6 acl**]

Parameters

Parameter	Description	Value
inbound	Configures ACL-based packet filtering in the inbound direction on an interface.	-
outbound	Configures ACL-based packet filtering in the outbound direction on an interface.	-
acl	Filters packets based on the IPv4 ACL.	-
ipv6 acl	Filters packets based on the IPv6 ACL.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
acl-number	Specifies the number of an ACL.	The IPv4 ACL number ranges from 2000 to 4999, and the IPv6 ACL number ranges from 2000 to 3999. ● The value of a basic ACL/ACL6 ranges from 2000 to 2999. ● The value of an advanced ACL/ACL6 ranges from 3000 to 3999. ● The value of a Layer 2 ACL ranges from 4000 to 4999.
name *acl-name*	Filters packets based on a specified named ACL. *acl-name* specifies the name of the ACL.	The value must be the name of an existing ACL.

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **traffic-filter** command is executed on an interface, the device filters packets matching ACL rules:

- If the action in an ACL rule is **deny**, the device discards packets matching the rule.
- If the action in an ACL rule is **permit**, the device forwards packets matching the rule.
- If no rule is matched, packets are allowed to pass through.

Precautions

ACL-based packet filtering can be configured on the WAN interface and logical interface that provides Layer 3 functions.

Loopback interfaces of the device support **traffic-filter inbound acl** { *acl-number* | **name** *acl-name* } and **undo traffic-filter inbound**. That is, **traffic-filter** can be

configured on a loopback interface in the inbound direction, but IPv6 ACLs are not supported.

NOTE

When **traffic-filter** command is used on loopback interface, there has the following limitations:

- Layer 2 ACLs cannot be used.
- If the basic ACL based on the fragment flag is used, **traffic-filter** does not take effect.
- If the advanced ACL based on gre, igmp, ipinip, and ospf is used, **traffic-filter** does not take effect.

If packets match an ACL rule with the **deny** action and a traffic policy (configured using the **traffic-policy (interface view)**) command simultaneously on an interface, the traffic policy does not take effect for the packets.

You can specify an empty ACL (ACL number) in this command, and configure this ACL later.

You can apply only one ACL in one direction on an interface to filter packets. Before modifying the ACL referenced by the **traffic-filter** command, run the **undo traffic-filter** command to cancel packet filtering based on this ACL.

On a device equipped with 8FE1GE and 24GE cards that support forwarding at Layer 3, if ACL-based traffic policies and ACL-based simplified traffic policies are configured on VLANIF interfaces, the device processes traffic traversing the 8FE1GE and 24GE cards in the following ways:

- For packets sent from LAN ports on the SRU panel and other LAN cards (cards excluding 8FE1GE and 24GE) to LAN ports of 8FE1GE and 24GE cards, the device forwards the packets to the sub-core CPU for forwarding. In this case, ACL-based traffic policies and ACL-based simplified traffic policies can be configured.
- For packets transmitted between LAN ports of 8FE1GE and 24GE cards, the device directly forwards the packets at Layer 3, without the need of sending packets to the sub-core CPU. To configure ACL-based traffic policies and ACL-based simplified traffic policies on an interface, run the **set workmode lan-card l3centralize** command to disable the routing and forwarding function on 8FE1GE and 24GE cards first so that ACL-based traffic policies can take effect.
- For packets sent from LAN ports on 8FE1GE and 24GE cards to LAN ports on the SRU panel and other LAN cards (cards excluding 8FE1GE and 24GE), the device directly forwards the packets at Layer 3, without the need of sending packets to the sub-core CPU. To make ACL-based traffic policies configured on interfaces effective, you need to run the **set workmode lan-card l3centralize** command to disable the routing and forwarding function on 8FE1GE and 24GE cards first.

Example

On the Eth2/0/0, configure packet filtering based on the ACL that permits packets with source IP address 192.168.0.2/32.

```
<Huawei> system-view
[Huawei] acl 3000
[Huawei-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[Huawei-acl-adv-3000] quit
```

```
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] traffic-filter inbound acl 3000
```

Related Topics

19.7.4 acl (system view)
19.7.18 rule (basic ACL view)
19.7.16 rule (advanced ACL view)
19.7.20 rule (layer 2 ACL view)
20.7.3 display traffic-filter statistics
20.7.4 reset traffic-filter statistics
20.7.2 display traffic-filter applied-record

20.8 Bandwidth Management Configuration Commands

NOTE

Only AR100&AR120&AR150&AR160&AR200 series support bandwidth management.

20.8.1 bandlimit

Function

The **bandlimit** command enables user bandwidth limiting and sets user bandwidth limiting parameters.

The **undo bandlimit** command disables user bandwidth limiting and deletes user bandwidth limiting parameters.

By default, user bandwidth limiting is not enabled and user bandwidth limiting parameters are not configured.

Format

bandlimit interface { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* { { **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } * } | **user-set** *user-set-name* { { **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } * [**share**] } } [**time-range** *time-range-name*] [**description** *description*]

undo bandlimit interface { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* [**share**] }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	The value depends on the interface type and slot ID.

Parameter	Description	Value
interface *interface-name*	Specifies the name of an interface.	The value depends on the interface type and slot ID.
type	Specifies the bandwidth limiting type.	-
ip *ip-address*	Specifies the IP address to which bandwidth limiting is applied.	The value is in dotted decimal notation.
inbound cir *in-cir-value*	Specifies the inbound committed information rate (CIR), that is, guaranteed average transmission rate in the inbound direction.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
outbound cir *out-cir-value*	Specifies the outbound CIR, that is, guaranteed average transmission rate in the outbound direction.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
user-set *user-set-name*	Specifies the name of a user group to which bandwidth limiting is applied.	The value is a string of 1 to 31 case-sensitive characters without spaces.
share	Specifies the bandwidth limiting mode. **NOTE** When this parameter is specified, rate limiting is applied to all IP addresses of a user group. If this parameter is not specified, rate limiting is applied to each IP address of a user group.	-
time-range *time-range-name*	Specifies the time range during which bandwidth limiting is applied. The time range must have been configured using the **time-range** command; otherwise, the time range does not take effect after the **bandlimit** command is used.	The value is a string of 1 to 32 case-sensitive characters without spaces, starting with an upper-case or lower-case letter.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
description *description*	Specifies the description of a function.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters excluding question marks (?) and spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Network resources are limited. When non-key services occupy much bandwidth, packets of core services may be discarded. To address this issue, perform bandwidth limiting for the non-key services. This command limits the maximum bandwidth for some IP addresses or user groups on a WAN interface and ensures the bandwidth of core services.

Prerequisites

A user group has been created using the **user-set** command when bandwidth limiting is enabled based on the user group.

Precautions

If you run the **bandlimit** command multiple times in the web view, only the latest configuration takes effect.

When the **bandlimit** command is executed in the web view, the device delivers the **qos car** command configuration to the interface. If bandwidth limiting is based on IP addresses in the inbound direction, the IP address in the web view is mapped to the destination IP address in the **qos car** command. If bandwidth limiting is based on IP addresses in the outbound direction, the IP address in the web view is mapped to the source IP address in the **qos car** command.

When **time-range** is configured and the current time is out of the range specified by **time-range**, the device deletes the **qos car** command configuration from the interface. However, the **bandlimit** command in the web view remains unchanged. If the current time is in the range specified by **time-range**, the device delivers the **qos car** command configuration to the interface.

Example

On the GE1/0/0 in the inbound direction, set the CIR of packets with the IP address of 10.10.0.5 to 3000 kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] bandlimit interface GigabitEthernet 1/0/0 type ip 10.10.0.5 inbound cir 3000
```

On the GE1/0/0 in the inbound direction, set the CIR of packets of the user group **huawei** to 3000 kbit/s.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set huawei
[Huawei-web-user-set-huawei] quit
[Huawei-web] bandlimit interface GigabitEthernet 1/0/0 type user-set huawei inbound cir 3000
```

Related Topics

20.8.6 user-set

20.3.12 qos car

19.7.24 time-range

20.8.2 bandguarantee

Function

The **bandguarantee** command enables user bandwidth guarantee and sets user bandwidth guarantee parameters.

The **undo bandguarantee** command disables user bandwidth guarantee and deletes user bandwidth guarantee parameters.

By default, user bandwidth guarantee is not enabled and user bandwidth guarantee parameters are not configured.

Format

bandguarantee interface { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* } **cir** *cir-value* [**time-range** *time-range-name*] [**description** *description*]

undo bandguarantee interface { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* }

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of an interface.	The value depends on the interface type and slot ID.
interface *interface-name*	Specifies the name of an interface.	The value depends on the interface type and slot ID.
type	Specifies the bandwidth guarantee mode.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip *ip-address*	Specifies the IP address to which guaranteed bandwidth is applied.	The value is in dotted decimal notation.
user-set *user-set-name*	Specifies the name of a user group to which bandwidth guarantee is applied.	The value is a string of 1 to 32 case-sensitive characters without spaces.
cir *cir-value*	Specifies the committed information rate (CIR), that is, guaranteed average transmission rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
time-range *time-range-name*	Specifies the time range during which bandwidth guarantee is applied. The time range must have been configured using the **time-range** command; otherwise, the time range does not take effect after the **bandguarantee** command is used.	The value is a string of 1 to 32 case-sensitive characters without spaces, starting with an upper-case or lower-case letter.
description *description*	Specifies the description of a function.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters excluding question marks (?) and spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When congestion occurs on a network, to prevent packet loss of core services due to insufficient bandwidth, enable bandwidth guarantee for core services. This command guarantees the minimum bandwidth for some IP addresses or user groups on a WAN interface and ensures that core services are processed preferentially when congestion occurs.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

A user group has been created using the **user-set** command when bandwidth guarantee is enabled based on the user group.

Precautions

If you run the **bandguarantee** command multiple times in the web view, only the latest configuration takes effect.

When the **bandguarantee** command is executed in the web view, the device delivers the configuration of a traffic classifier and a traffic behavior and applies a traffic policy to an interface. If bandwidth guarantee is performed based on IP addresses, **if-match acl** is delivered in the traffic classifier view and the **queue af** and **statistic enable** are delivered in the traffic behavior view. If bandwidth guarantee is performed based on user groups, **if-match user-set** is delivered in the traffic classifier view and the **queue af** and **statistic enable** are delivered in the traffic behavior view.

Example

On the GE1/0/0, set the CIR of packets with the IP address of 10.10.0.5 to 1000 kbit/s and configure the description as **huawei**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] bandguarantee interface GigabitEthernet 1/0/0 type ip 10.10.0.5 cir 1000 description
huawei
```

On the GE1/0/0, set the CIR of packets of the user group **vip** to 1000 kbit/s and configure the description as **huawei**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set vip
[Huawei-web-user-set-vip] quit
[Huawei-web] bandguarantee interface GigabitEthernet 1/0/0 type user-set vip cir 1000 description
huawei
```

Related Topics

19.7.24 time-range

20.8.6 user-set

20.8.3 enable bandlimit

Function

The **enable bandlimit** command enables user bandwidth limiting.

The **disable bandlimit** command disables user bandwidth limiting.

By default, user bandwidth limiting is enabled.

Format

enable bandlimit interface { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* [**share**] }

disable bandlimit interface { *interface-type interface-number* | *interface-name* } **type ip** *ip-address* [{ **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } * [**time-range** *time-range-name*] [**description** *description*]]

disable bandlimit interface { *interface-type interface-number* | *interface-name* } **type user-set** *user-set-name* [{ **inbound cir** *in-cir-value* | **outbound cir** *out-cir-value* } * [**share**] [**time-range** *time-range-name*] [**description** *description*]]

Parameters

Parameter	Description	Value
enable	Enables user bandwidth limiting.	-
disable	Disables user bandwidth limiting.	-
interface-type interface-number	Specifies the type and number of an interface.	The value depends on the interface type and slot ID.
interface-name	Specifies the name of an interface.	The value depends on the interface type and slot ID.
type	Specifies the bandwidth limiting type.	-
ip *ip-address*	Specifies the IP address to which bandwidth limiting is applied.	The value is in dotted decimal notation.
inbound	Enables bandwidth limiting in the inbound direction.	-
outbound	Enables bandwidth limiting in the outbound direction.	-
cir *in-cir-value*	Specifies the inbound committed information rate (CIR), that is, guaranteed average transmission rate in the inbound direction.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
cir *out-cir-value*	Specifies the outbound CIR, that is, guaranteed average transmission rate in the outbound direction.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
user-set *user-set-name*	Specifies the name of a user group to which bandwidth limiting is applied.	The value is a string of 1 to 31 case-sensitive characters without spaces.
share	Specifies the bandwidth limiting mode. **NOTE** When this parameter is specified, bandwidth limiting is applied to all IP addresses of a user group. If this parameter is not specified, bandwidth limiting is applied to each IP address of a user group.	-
time-range *time-range-name*	Specifies the time range during which bandwidth limiting is applied. The time range must have been configured using the **time-range** command; otherwise, the time range does not take effect after the **enable bandlimit** command is used.	The value is a string of 1 to 32 case-sensitive characters without spaces, starting with an upper-case or lower-case letter.
description *description*	Specifies the description of a function.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters excluding question marks (?) and spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After maximum bandwidth guarantee is configured on a WAN interface, you can use the **enable bandlimit** or **disable bandlimit** command to enable or disable user bandwidth limiting.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

User bandwidth limiting has been enabled and user bandwidth limiting parameters have been configured using the **bandlimit** command.

Follow-up Procedure

After the **disable bandlimit** command is used to disable user bandwidth limiting, run the **enable bandlimit** command to enable bandwidth limiting configured by the **bandlimit** command.

Precautions

When the **enable bandlimit** command is executed in the web view, the device delivers the **qos car** command configuration to the interface. If bandwidth limiting is based on IP addresses in the inbound direction, the IP address in the web view is mapped to the destination IP address in the **qos car** command. If bandwidth limiting is based on IP addresses in the outbound direction, the IP address in the web view is mapped to the source IP address in the **qos car** command.

When the **disable bandlimit** command is executed in the web view, the device deletes the **qos car** command configuration from the interface.

When **enable bandlimit** is configured and **time-range** is specified, if the current time is out of the range specified by **time-range**, the device does not deliver the **qos car** command configuration to the interface. If the current time is in the range specified by **time-range**, the device delivers the **qos car** command configuration to the interface.

Example

Disable bandwidth limiting based on IP addresses on the GE1/0/0.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] bandlimit interface GigabitEthernet 1/0/0 type ip 10.10.0.5 inbound cir 3000
[Huawei-web] disable bandlimit interface GigabitEthernet 1/0/0 type ip 10.10.0.5 inbound cir 3000
```

Disable bandwidth limiting based on user groups on the GE1/0/0.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set huawei
[Huawei-web-user-set-huawei] quit
[Huawei-web] bandlimit interface GigabitEthernet 1/0/0 type user-set huawei inbound cir 3000
[Huawei-web] disable bandlimit interface GigabitEthernet 1/0/0 type user-set huawei inbound cir 3000
```

Related Topics

20.8.6 user-set
20.3.12 qos car
19.7.24 time-range

20.8.4 enable bandguarantee

Function

The **enable bandguarantee** command enables user bandwidth guarantee.

The **disable bandguarantee** command disables user bandwidth guarantee.

By default, user bandwidth guarantee is enabled.

Format

enable bandguarantee interface { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* } **cir** *cir-value* [**time-range** *time-range-name*] [**description** *description*]

disable bandguarantee interface { *interface-type interface-number* | *interface-name* } **type** { **ip** *ip-address* | **user-set** *user-set-name* } **cir** *cir-value* [**time-range** *time-range-name*] [**description** *description*]

Parameters

Parameter	Description	Value
enable	Enables user bandwidth guarantee.	-
disable	Disables user bandwidth guarantee.	-
interface-type interface-number	Specifies the type and number of an interface.	The value depends on the interface type and slot ID.
interface-name	Specifies the name of an interface.	The value depends on the interface type and slot ID.
type	Specifies the bandwidth guarantee mode.	-
ip *ip-address*	Specifies the IP address to which bandwidth guarantee is applied.	The value is in dotted decimal notation.
user-set *user-set-name*	Specifies the name of a user group to which bandwidth guarantee is applied.	The value is a string of 1 to 32 case-sensitive characters without spaces.
cir *cir-value*	Specifies the committed information rate (CIR), that is, guaranteed average transmission rate.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-range *time-range-name*	Specifies the time range during which bandwidth guarantee is applied. The time range must have been configured using the **time-range** command; otherwise, the time range does not take effect after the **enable bandguarantee** command is used.	The value is a string of 1 to 32 case-sensitive characters without spaces, starting with an upper-case or lower-case letter.
description *description*	Specifies the description of a function.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters excluding question marks (?) and spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After minimum bandwidth guarantee is configured on a WAN interface, you can use the **enable bandguarantee** or **disable bandguarantee** command to enable or disable user bandwidth guarantee.

Prerequisites

The **bandguarantee** command has been executed before you use the **disable bandguarantee** command.

Follow-up Procedure

After the **disable bandguarantee** command is used to disable user bandwidth guarantee, run the **enable bandguarantee** command to enable bandwidth guarantee configured by the **bandguarantee** command.

Precautions

When the **enable bandguarantee** command is executed in the web view, the device delivers the configuration of a traffic classifier and a traffic behavior and applies a traffic policy to an interface. If bandwidth guarantee is performed based on IP addresses, **if-match acl** is delivered in the traffic classifier view and the

 Copyright © Huawei Technologies Co., Ltd.

queue af and **statistic enable** are delivered in the traffic behavior view. If bandwidth guarantee is performed based on user groups, **if-match user-set** is delivered in the traffic classifier view and the **queue af** and **statistic enable** are delivered in the traffic behavior view.

When the **disable bandguarantee** command is executed in the web view, the configuration of the traffic classifier, traffic behavior, and traffic policy will be deleted.

Example

Disable bandwidth guarantee based on IP addresses on the GE1/0/0.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] bandguarantee interface GigabitEthernet 1/0/0 type ip 10.10.0.5 cir 1000 description
huawei
[Huawei-web] disable bandguarantee interface GigabitEthernet 1/0/0 type ip 10.10.0.5 cir 1000
description huawei
```

Disable bandwidth guarantee based on user groups on the GE1/0/0.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set vip
[Huawei-web-user-set-vip] quit
[Huawei-web] bandguarantee interface GigabitEthernet 1/0/0 type user-set vip cir 1000 description
huawei
[Huawei-web] disable bandguarantee interface GigabitEthernet 1/0/0 type user-set vip cir 1000
description huawei
```

Related Topics

19.7.24 time-range

20.8.6 user-set

20.8.5 user-ip

Function

The **user-ip** command configures an IP network segment for users in a web user group.

The **undo user-ip** command deletes an IP network segment configured for users in a web user group.

By default, no IP network segment is configured for users in a web user group.

Format

user-ip from *ip_addr1* **to** *ip_addr2* [**description** *description*]

undo user-ip from *ip_addr1* **to** *ip_addr2*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
from *ip_addr1*	Specifies the start IP address of the IP network segment for users in a web user group.	The value is in dotted decimal notation.
to *ip_addr2*	Specifies the end IP address of the IP network segment for users in a web user group.	The value is in dotted decimal notation.
description *description*	Specifies description of the IP network segment for users in a web user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters excluding question marks (?) and spaces.

Views

user-set view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The web system allows you to manage the bandwidth, application, website visit, and file type based on user groups, facilitating management. You can run the **user-ip** command to configure an IP address for a user in a web user group or an IP address segment for users in the web user group, and add description for the IP address or IP address segment.

Precautions

If the values of *ip_addr1* and *ip_addr2* are the same, an IP address is configured for a user in a web user group.

A web user group supports a maximum of 30 IP address segments and 12K IP addresses.

Example

Configure the IP address segment from 10.1.1.1 to 10.1.1.10 for users in the web user group **leader** and set the description to **develop-leader**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set leader
[Huawei-web-user-set-leader] user-ip from 10.1.1.1 to 10.1.1.10 description develop-leader
```

Related Topics

20.8.6 user-set

20.8.6 user-set

Function

The **user-set** command creates a web user group and displays the web user group view, or displays the view of an existing web user group.

The **undo user-set** command deletes a created web user group.

By default, the device contains two web user groups named **VIP** and **Default**.

Format

user-set *user-set-name*

undo user-set *user-set-name*

Parameters

Parameter	Description	Value
user-set-name	Specifies the name of a web user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters excluding question marks (?) and spaces.

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

The web system allows you to manage the bandwidth, application, website visit, and file type based on user groups. You can run the **user-set** command to create a web user group and enter the web user group view, or enter the view of an existing web user group.

Example

Configure a web user group named **leader**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set leader
[Huawei-web-user-set-leader]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.8.5 user-ip

20.8.7 web

Function

The **web** command displays the web view.

Format

web

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To perform configurations related to the web system, enter the web view first. You can run this command in the system view to enter the web view.

Example

Display the web view.

```
<Huawei> system-view
[Huawei] web
[Huawei-web]
```

20.9 Application Control Management Commands

NOTE

Only AR100&AR120&AR150&AR160&AR200 series support application control management.

20.9.1 app-profile

Function

The **app-profile** command configures the name of an application control profile.

The **undo app-profile** command deletes the name of an application control profile.

 Copyright © Huawei Technologies Co., Ltd.

By default, the name of an application control profile is not configured.

Format

app-profile *app-profile-name*

undo app-profile *app-profile-name*

Parameters

Parameter	Description	Value
app-profile-name	Specifies the name of an application control profile.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces, for example, "a b CD".

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you want to manage a large number of applications of different types, run the **app-profile** command to configure an application control profile. You can bind the application control profile to one or more user groups to implement the same application control management.

Configuration Impact

An application control profile applies to all members in the selected user group.

Follow-up Procedure

Run the **application-control** command in the web view to bind the profile to a user group. Otherwise, the profile does not take effect.

Example

Create application control profile **research**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] app-profile research
```

Related Topics

20.9.4 application-control

20.9.3 application

20.9.2 category

20.9.2 category

Function

The **category** command configures the application protocol type.

The **undo category** command deletes an existing application protocol type.

By default, application protocol types are not added to the SA signature file.

Format

category *category-name*

undo category *category-name*

Parameters

Parameter	Description	Value
category-name	Specifies the type of application protocols.	The value is a character string without spaces. The value range depends on the applications supported in the signature database.

Views

Application control profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a large number of application protocols of the same type are configured, you can run the **category** command to specify the application protocol type. By doing so, you do not need to configure application protocol names of the same type one by one.

Prerequisites

You have entered the application control profile view by running the **app-profile** command. If you configure application protocol names in other views, the configuration does not take effect.

Configuration Impact

After an application protocol type is configured, it applies to all members in the selected user group.

Follow-up Procedure

Run the **application-control** command in the web view to bind the profile to a user group. Otherwise, the profile does not take effect.

Example

Configure application protocol type **Email** in application control profile **test**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] app-profile test
[Huawei-web-app-profile-test] category Email
```

Related Topics

20.9.4 application-control

20.9.1 app-profile

20.9.3 application

20.9.3 application

Function

The **application** command configures the application protocol name.

The **undo application** command deletes an existing application name.

By default, application protocol names are not added to the SA signature file.

Format

application *application-name*

undo application *application-name*

Parameters

Parameter	Description	Value
application-name	Specifies the name of an application protocol.	The value is a character string without spaces. The value range depends on the applications supported in the signature database.

 Copyright © Huawei Technologies Co., Ltd.

Views

Application control profile view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After you run this command to configure detailed application protocol names in the application control profile, the router filters applications based on the application protocol name. If application protocol names are not configured, the router does not filter applications.

Prerequisites

You have entered the application control profile view by running the **app-profile** command. If you configure application protocol names in other views, the configuration does not take effect.

Configuration Impact

After an application protocol name is configured, it applies to all members in the selected user group.

Follow-up Procedure

Run the **application-control** command in the web view to bind the profile to a user group. Otherwise, the profile does not take effect.

Example

Configure application protocol name **dns** in application control profile **test**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] app-profile test
[Huawei-web-app-profile-test] application dns
```

Related Topics

20.9.4 application-control

20.9.1 app-profile

20.9.2 category

20.9.4 application-control

Function

The **application-control** command binds an application control profile to a user group.

The **undo application-control** command unbinds an application control profile from a user group.

 Copyright © Huawei Technologies Co., Ltd.

By default, application control management is not configured for a user group.

Format

application-control user-set *user-set-name* **app-profile** *app-profile-name* **type** { **cir** *cir-value* | **application-deny** } [**time-range** *time-range-name*] [**description** *description-text*]

undo application-control user-set *user-set-name* **app-profile** *app-profile-name*

Parameters

Parameter	Description	Value
user-set *user-set-name*	Specifies the name of a user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces, for example, "a b CD".
app-profile *app-profile-name*	Specifies the name of an application control profile.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces, for example, "a b CD".
type	Specifies the type of application to be controlled.	-
cir *cir-value*	Sets a rate limit for an application.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
application-deny	Prohibits users in the user group from accessing an application.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-range *time-range-name*	Specifies the time range during which application control is applied.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. It cannot contain question marks (?) or spaces. In addition, the word **all** cannot be specified as a time range name.
description *description-text*	Indicates description of the function.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces, for example, "a b CD".

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run this command to carry out application control management on members in a user group. For example, you can limit the rate of Thunder or prohibit access to Kugou.

Prerequisites

A user group has been created by running the **user-set** command. An application control profile has been created by running the **app-profile** command.

Configuration Impact

An application control profile applies to all members in the selected user group.

Example

Prohibit members in user group **owner** from accessing applications in application control profile **research**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set owner
[Huawei-web-user-set-owner] quit
[Huawei-web] app-profile research
[Huawei-web-app-profile-research] quit
[Huawei-web] application-control user-set owner app-profile research type application-deny
```

Related Topics

20.9.3 application

20.9.1 app-profile

20.9.2 category

20.9.5 enable application-control

Function

The **enable application-control** command enables the application control management function for a user group.

The **disable application-control** command disables the application control management function for a user group.

By default, the application control management function is disabled for a user group.

Format

enable application-control user-set *user-set-name* **app-profile** *app-profile-name*

disable application-control user-set *user-set-name* **app-profile** *app-profile-name* [**type** { **cir** *cir-value* | **application-deny** } [**time-range** *time-range-name*] [**description** *description-text*]]

Parameters

Parameter	Description	Value
user-set *user-set-name*	Specifies the name of a user group.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces, for example, "a b CD".

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
app-profile *app-profile-name*	Specifies the name of an application control profile.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces, for example, "a b CD".
type	Specifies the type of application to be controlled.	-
cir *cir-value*	Sets a rate limit for an application.	The value is an integer that ranges from 8 to 4294967295, in kbit/s.
application-deny	Prohibits users in the user group from accessing an application.	-
time-range *time-range-name*	Specifies the time range during which application control is applied.	The value is a string of 1 to 32 case-sensitive characters and must begin with a letter. It cannot contain question marks (?) or spaces. In addition, the word **all** cannot be specified as a time range name.
description *description-text*	Indicates description of the function.	The value is a string of 1 to 31 case-sensitive characters. It can contain special characters, but cannot contain question marks (?) or spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces, for example, "a b CD".

Views

Web view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An administrator can run the **enable application-control** command to enable the application control management function for a user group. With this function, the administrator can manage applications in the user group, for example, denying access to an application or rate-limiting the traffic of an application for a user.

Prerequisites

A user group and application control profile have been created and bound. To create a user group, run the **user-set** command; to create an application control profile, run the **app-profile** command; to bind an application control profile to a user group, run the **application-control** command.

Example

Enable application control management for the user group **owner**.

```
<Huawei> system-view
[Huawei] web
[Huawei-web] user-set owner
[Huawei-web-user-set-owner] quit
[Huawei-web] app-profile research
[Huawei-web-app-profile-research] quit
[Huawei-web] application-control user-set owner app-profile research type application-deny
[Huawei-web] enable application-control user-set owner app-profile research
```

20.10 SAC Configuration Commands

NOTE

SAC configuration commands take effect only after the deep security defense function is enabled on the device.

20.10.1 application name cache type aging-time

Function

The **application name cache type aging-time** command sets the aging time of the entry associated with pre-defined application identification.

The **undo application name cache type aging-time** command restores the default setting.

By default, the value of the aging time of the entry generated upon multi-channel application identification for ftp is 180 seconds and for other applications is 300 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Format

application name *name* **cache type multi-channel aging-time** *aging-time*

undo application name *name* **cache type multi-channel aging-time**

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a predefined application.	The value must be the name of an existing application.
multi-channel aging-time *aging-time*	Specifies the aging time of the entry generated upon multi-channel application identification.	The value is an integer ranging from 1 to 60,000, in seconds. The default value of FTP is 180 seconds, The default value of other applications is 300 seconds.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

The **application name cache type aging-time** command sets the aging time of the entry associated with the identification of predefined applications. The entry associated with the identification of user-defined applications never ages.

Example

Set the aging time of the entry associated with FTP data channel application identification to 100 seconds.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] application name FTP cache type multi-channel aging-time 100
```

20.10.2 category sub-category

Function

The **category sub-category** command configures a category and a subcategory for a user-defined application.

The **undo category** command restores the default category and sub-category of a user-defined application.

By default, the category and sub-category of a user-defined application are **General** and **Other**, respectively.

 Copyright © Huawei Technologies Co., Ltd.

Format

category *category* **sub-category** *sub-category*

undo category

Parameters

Parameter	Description	Value
category	Specifies the category of a user-defined application.	See **Category and subcategory of applications**.
sub-category	Specifies the sub-category of a user-defined application.	See **Category and subcategory of applications**.

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, the category and sub-category of a user-defined application are **General** and **Other**, respectively. To add the user-defined application to another category and sub-category, you can run this command so that user-defined applications are classified based on the category.

Table 20-25 describes the categories and sub-categories of applications supported by the AR.

Table 20-25 Category and subcategory of applications

Category	Subcategory	Description
Business_Systems	Auth_Service	Authentication service **NOTE** This subcategory is no longer used but is retained for backward compatibility. Do not add user-defined applications to this subcategory.
	Data_Backup	Data backup software, such as Rsync
	Database	Database, such as MySQL
	Electronic_Business	Electronic business, such as eBay

 Copyright © Huawei Technologies Co., Ltd.

Category	Subcategory	Description
	Email	Email, such as Gmail
	Enterprise_Application	Enterprise application software, such as the Concurrent Versions System (CVS), Outlook Web Access
	File_Access	File access **NOTE** This subcategory is no longer used but is retained for backward compatibility. Do not add user-defined applications to this subcategory.
	Finance	Finance, such as Scottrade
	Internet_Conferencing	Internet conferencing applications, such as live-meeting
	Remote_Access	Remote access control software, such as Radmin, RSH
	WebMail	Web mail **NOTE** This subcategory is no longer used but is retained for backward compatibility. Do not add user-defined applications to this subcategory.
Entertainment	Game	Game software, such as Warcraft
	Instant_Messaging	IM software, such as QQ, MSN
	Media_Sharing	Applications for online videos, music, or radio, and music download and upload, such as Youtube, PPfilm, HTTP-audio, and iTunes
	MicroBlog	Microblog **NOTE** This subcategory is no longer used but is retained for backward compatibility. Do not add user-defined applications to this subcategory.
	PeerCasting	P2P web video, such as Livestation
	Social_Networking	Social networking websites, such as Facebook

 Copyright © Huawei Technologies Co., Ltd.

Category	Subcategory	Description
	VoIP	VoIP software, such as MSN, Skype
	Web_Video	Web video, such as YouTube
	WireLess	Wireless terminal application **NOTE** This subcategory is no longer used but is retained for backward compatibility. Do not add user-defined applications to this subcategory.
General_Internet	AppDownload	APP download, such as APP Store and Google Play Store
	Browser_Plugin	Website plug-ins, such as LastPass
	FileShare_P2P	P2P file sharing, such as BT and eDonkey
	File_Sharing	Fire sharing software, such as Mozy, XDCC
	IM_File_Transfer	Applications for IM file transfer, such as file transfer in Yahoo Messenger
	Network_Storage	Network storage, such as Huawei network disk and SkyDrive
	Search_Engines	Search engines, such as Google and Yahoo
	Software_Update	Applications for software update, such as Windowsupdate
	Utility	Small tools, such as Google Translate
	Web_Browsing	Applications for web browsing, such as Sougo browser
	Web_Content_Aggregate	Information gathering software, such as EventBox
	Web_Desktop	Web desktop system, such as Windows Live, cloudo

 Copyright © Huawei Technologies Co., Ltd.

Category	Subcategory	Description
	Web_Posting	Web forum **NOTE** This subcategory is no longer used but is retained for backward compatibility. Do not add user-defined applications to this subcategory.
	Web_Spider	Web crawler software, such as WebReaper
Network	Attack	Network attacks, such as worms
	CloudService	Cloud service, such as Huawei HiSpace and Google_App_Engine
	Encrypted_Tunnel	Tunneling applications, such as GRE, L2TP
	Infrastructure	Basic network protocols, such as HTTP and HTTPS
	Ip_Protocol	IP-layer protocols, such as ICMP and IPv6
	Network_Admin	Network administration, such as Corba and Syslog
	News_Group	News group, such as Sohu_News
	Proxy	Proxy software, such as CCproxy
General	General_UDP	General UDP applications
	General_TCP	General TCP applications
	Other	Other general applications

Precautions

If you run the **category sub-category** command in the same user-defined application view multiple times, only the latest configuration takes effect.

Example

Configure the category **Business_Systems** and subcategory **Database** for the user-defined application **abc**.

```
<Huawei> system-view
[Huawei] sa
```

```
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] category Business_Systems sub-category Database
```

20.10.3 data-model

Function

The **data-model** command specifies a data model for a user-defined application.

The **undo data-model** command restores the default data model of a user-defined application.

By default, the data model of a user-defined application is **unassigned**.

Format

data-model { **browser-based** | **client-server** | **networking** | **peer-to-peer** | **unassigned** }

undo data-model

Parameters

Parameter	Description	Value
browser-based	Indicates that the data model depends on the running mode of the web browser, for example, web games.	-
client-server	Indicates that the data model is the client/server model, such as client games.	-
networking	Indicates that the data model is of common network and is often used for communication between systems so that network operations can be performed, for example, HTTP and HTTPS.	-
peer-to-peer	Indicates that the data model is P2P, for example, Thunder and BT.	-
unassigned	Non-specified data model.	-

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The default data model of a user-defined application is **unassigned**. To specify another data model for a user-defined application, you can run this command so that user-defined applications are classified based on the data model.

Precautions

If you run the **data-model** command in the same user-defined application view multiple times, only the latest configuration takes effect.

Example

Configure the data model for the user-defined application **UD_abc** as **client-server**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] data-model client-server
```

20.10.4 description (user-defined application view)

Function

The **description** command configures a description for a user-defined application.

The **undo description** command deletes a description of a user-defined application.

By default, no description is configured for a user-defined application.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined application.	The value is a string of 1 to 128 case-sensitive characters with spaces.

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

The **description** command configures a description for a user-defined application, which helps memorize and distinguish user-defined applications.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the description **test** for the user-defined application **UD_abc**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] description test
```

20.10.5 description (user-defined application rule view)

Function

The **description** command configures a description for a user-defined application rule.

The **undo description** command deletes a description of a user-defined application rule.

By default, no description is configured for a user-defined application rule.

Format

description *description*

undo description

Parameters

Parameter	Description	Value
description	Specifies the description of a user-defined application rule.	The value is a string of 1 to 128 case-sensitive characters with spaces.

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

The **description** command configures a description for a user-defined application rule, which helps memorize and distinguish user-defined application rules.

Example

Configure the description **test** for the user-defined application rule **rule1**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-sa-user-defined-app-UD_abc] rule name rule1
[Huawei-sa-user-defined-app-UD_abc-rule-rule1] description test
```

20.10.6 detect max-bytes

Function

The **detect max-bytes** command specifies the maximum number of bytes to be detected by the SA module.

The **undo detect max-bytes** command restores the default maximum number of bytes to be detected by the SA module.

By default, the maximum number of bytes to be detected by the SA module is 2048.

Format

detect max-bytes *max-bytes*

undo detect max-bytes

Parameters

Parameter	Description	Value
max-bytes	Specifies the maximum number of bytes to be detected.	The value is an integer ranging from 1 to 10240.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

This command is used to specify the maximum number of bytes detected by the SA module to prevent certain applications from evading the detection by using small packets.

In common cases, the default maximum value can meet the requirement. If the value is too large, the device performance may deteriorate. If the value is too small, the device may fail to detect certain applications.

Example

Set the maximum number of bytes to be detected by the SA module to 4096.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] detect max-bytes 4096
```

 Copyright © Huawei Technologies Co., Ltd.

20.10.7 detect max-packets

Function

The **detect max-packets** command specifies the maximum number of packets to be detected by the SA module.

The **undo detect max-packets** command restores the maximum number of packets detected by the SA module to the default value.

By default, the maximum number of packets to be detected by the SA module is 16.

Format

detect max-packets *max-packets*

undo detect max-packets

Parameters

Parameter	Description	Value
max-packets	Specifies the maximum number of packets in a session.	The value is an integer ranging from 1 to 64.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

The specified maximum number of packets to be detected covers both directions in a session.

Example

Set the maximum number of packets to be detected by the SA module to **20**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] detect max-packets 20
```

20.10.8 detect max-time

Function

The **detect max-time** command sets the maximum duration in which the SA module detects sessions.

The **undo detect max-time** command restores the maximum duration to the default value.

Format

detect max-time *max-time*

undo detect max-time

Parameters

Parameter	Description	Value
max-time	Specifies the maximum session detection duration.	The value is an integer ranging from 0 to 60, in minutes. The default value is 1.

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Set the maximum duration in which the SA module detects sessions to 5 minutes.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] detect max-time 5
```

20.10.9 detect uni-direction

Function

The **detect uni-direction** command configures the unidirectional detection on the SA module.

The **undo detect uni-direction** command cancels the unidirectional detection and restores the bidirectional detection.

By default, the SA module works in bidirectional detection mode.

Format

detect uni-direction

 Copyright © Huawei Technologies Co., Ltd.

undo detect uni-direction

Parameters

None

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

SA detection falls into unidirectional detection and bidirectional detection. By default, the SA module works in bidirectional detection mode. If the device is deployed in unidirectional mode, use the **detect uni-direction** command to configure the unidirectional detection mode of the SA module.

Example

Configure the unidirectional detection mode of the SA module.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] detect uni-direction
```

20.10.10 display application

Function

The **display application** command displays information about applications in the system.

Format

display application [**pre-defined** | **user-defined** | **name** *name*]

Parameters

Parameter	Description	Value
pre-defined	Indicates predefined applications.	-
user-defined	Indicates user-defined applications.	-
name *name*	Specifies the name of an application.	The value must be the name of an existing application.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the information about all applications.

```
<Huawei> display application
Service Awareness Signature Database Information:
Total Applications: 1603
-------------------------------------------------------------------------------
---------------------------------------------
 AppID Name                          Category                 Sub-category
                 RiskLevel State
 1     BT                            General_Internet         FileShare_P2
P                 4        activated
 2     PPLive                        Entertainment            Peercasting
                 5        activated
 3     Thunder                       General_Internet         FileShare_P2
P                 5        activated
 5     FTP                           Network                  Infrastructu
re                3        activated
 6     FTPS                          Network                  Infrastructu
re                4        activated
 7     eDonkey_eMule                 General_Internet         FileShare_P2
P                 5        activated
 9     QQLive                        Entertainment            Peercasting
                 5        activated
 11    Fasttrack                     General_Internet         FileShare_P2
P                 5        activated
 12    PPStream                      Entertainment            Peercasting
                 5        activated
 14    DirectConnect                 General_Internet         FileShare_P2
P                 3        activated
 15    KuGoo                         Entertainment            Peercasting
                 5        activated
 18    POCO                          General_Internet         Photo_Sharin
g                 5        activated
 20    Maze                          General_Internet         FileShare_P2
P                 3        activated
 22    UUSee                         Entertainment            Peercasting
                 4        activated
 23    Vagaa                         General_Internet         FileShare_P2
P                 4        activated
 25    QQDownLoad                    General_Internet         FileShare_P2
P                 4        activated
 27    Filetopia                     General_Internet         FileShare_P2
P                 5        activated
 28    Soulseek                      General_Internet         FileShare_P2
P                 5        activated
 29    Sopcast                       Entertainment            Peercasting
                 5        activated
 31    KooWo                         Entertainment            Peercasting
                 5        activated
  ---- More ----
```

Table 20-26 Description of the **display application** command output

Item	Description
Total Applications	Total number of applications
AppID	Application ID
Name	Name of an application
Category	Category of an application. For details, see **Category and subcategory of applications**.
Sub-category	Subcategory of an application. For details, see **Category and subcategory of applications**.
RiskLevel	Risk level of an application
State	State of an application A predefined application can be in either of the following states: ● activated: indicates that an application takes effect. ● disabled: indicates that an application does not take effect. A user-defined application can be in either of the following states: ● committed: indicates that an application is configured and committed. ● not committed: indicates that an application is created or modified but not committed.

Display information on predefined application **BT**.

```
<Huawei> display application name BT
Application BT Information:
-----------------------------------------------------------------------------------------
  Application ID      : 1
  Application Name    : BT
  Category            : General_Internet
  Sub-category        : FileShare_P2P
  Software            : Other
  Risk Level          : 4
  Label               : "Productivity-Loss", "Data-Loss", "Bandwidth-
Consuming",
                      "Evasive", "Tunneling", "P2P-Based"
  State               : activated
  DataModel           : peer-to-peer
  Description         : BitTorrent (BT) is a P2P protocol for multi-point downloading
an
                      d can be used for many different kinds of applications. The
clie
                      nt downloads and uploads data at the same time. Example:
BitTorr
                      ent, BitSpirit and BitComet.

  Total Rule Number   : 0
```

```
-----------------------------------------------------------------------------------------
```

Display information on user-defined application **UD_123**.

```
<Huawei> display application name UD_123
Application UD_123 Information:
-----------------------------------------------------------------------------------------
  Application ID      : 60001
  Application Name    : UD_123
  Category            : General
  Sub-category        : Other
  Risk Level          : 1
  Label               :
  State               : committed
  DataModel           : unassigned
  Description         : -
  Total Rule Number   : 1

  -----------------------------------------------------------------------------------------
    Rule Name         : rule_123
    IP Address        : -
    IPv6 Address      : -
    Protocol          : TCP
    Port              : -
    Context           : flow
    Direction         : both
    Type              : plain string
    Field             : General-Payload
    Signature         : inout1
  -----------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------
```

Table 20-27 Description of the **display application name** *name* command output

Item	Description
Application *name* Information	Application *name* information
Application ID	Application ID
Application Name	Application name
Category	Category of the application
Sub-category	Subcategory of the application
Software	Software name to which the application corresponds This item is displayed only for predefined applications.
Risk Level	Risk level of the application
Label	Label of the application

Item	Description
State	Status of the application A predefined application has two states: ● activated: indicates that the application takes effect. ● disabled: indicates the application is disabled. A user-defined application has two states: ● committed: indicates that the application configuration is committed. ● not committed: indicates that the application is newly created or modified but its configuration is not committed.
DataModel	Data transmission mode: ● unassigned ● client-server ● browser-based ● networking ● peer-to-peer
Description	Description of the application
Total Rule Number	Number of rules For a predefined application, the parameter value is fixed to 0. For a user-defined application, the parameter is displayed only after rules are configured.
Rule Name	Rule name
IP Address	IPv4 destination address
IPv6 Address	IPv6 destination address
Protocol	Protocol type ● TCP ● UDP ● any
Port	Destination port
Context	Detection scope: ● flow ● packet

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Direction	Detection direction: ● both: any direction ● request: request data ● response: response data
Type	Match mode
Field	Protocol field
Signature	Keyword

20.10.11 display application name aging-time

Function

The **display application name aging-time** command displays the aging time of the entry associated with application identification.

Format

display application name *name* **aging-time**

Parameters

Parameter	Description	Value
name *name*	Specifies the name of an application.	The value must be the name of an existing application.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

The **display application name aging-time** command displays the aging time of the entry associated with the identification of predefined applications. The entry associated with the identification of user-defined applications never ages.

Example

Display the aging time of the entry associated with FTP identification.

```
<Huawei> display application name FTP aging-time
Aging Time:
```

```
-------------------------------------------------------------------------------
 Application Name                  : FTP
 Acceleration Aging-time(sec)       : 300
 Multi-channel Aging-time(sec)      : 180
-------------------------------------------------------------------------------
```

Table 20-28 Description of the **display application name aging-time** command output

Item	Description
Application Name	Name of an application
Acceleration Aging-time(sec)	Aging time of the entry generated upon application identification acceleration
Multi-channel Aging-time(sec)	Aging time of the entry generated upon multi-channel application identification If the queried application is not a multi-channel application, **-** is displayed.

20.10.12 display sa application-list

Function

The **display sa application-list** command displays applications in the SA signature file.

Format

display sa application-list

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The SA signature file contains different application protocols. After a signature file is loaded successfully, run the **display sa application-list** command to view application protocols in the signature file.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display SA application protocols in the system.

```
<Huawei> display sa application-list
  SA application list
-------------------------------------------------------------------------------

  Index    Protocol Name                Description
  1        BT                             BitTorrent (BT) is a P2P protocol
                                        for multi-point downloading and can
                                        be used for many different kinds of
                                        applications. The client downloads
                                        and uploads data at the same time.
                                        Example: BitTorrent, BitSpirit, and
                                        BitComet.
  2        PPLive                          PPLive is a kind of software for
                                        watching online videos. It supports
                                        the live and on-demand functions.
                                        Example: PPLive, TTver, PPTV,
                                        Wanneng TV.
  3        Thunder                          Thunder is a kind of P2P-based
                                        software for downloading. Example:
                                        Thunder, Thunder movie, Web
                                        Thunder, Diandian, Thunder Kankan,
                                        and Thunder Tingting.
  4        FTP                            FTP is the abbreviation of File
                                        Transfer Protocol  which also has a
                                        specific software can be applied to
                                        various applications to control
                                        file' s two-way transmission on the
                                        Internet. Example: CuteFTP.
  5        eDonkey_eMule                       eMule is a kind of P2P client
                                        software which supports files
                                        sharing through the Internet.
                                        Example: eMule Xtreme, easyMule.
  6        QQLive                           QQLive is a kind of software for
                                        watching online videos developed by
                                        Tencent. Example: QQLive Web TV,
                                        Wanneng Web TV, and TTver Web TV.
  7        Fasttrack                       FastTrack is a protocol used in P2P
                                        softwares such as Kazaa, Grokster,
                                        iMesh, and Morpheus. It is called
                                        the second generation P2P protocol.
                                        Example: Fasttrack.
  8        PPStream                         PPStream is a kind of software for
                                        watching Web videos which supports
                                        multiple channels. It is quite
                                        popular all over China. Example:
                                        PPS Web TV, PPStream VOD, TTver,
                                        Wanneng Web TV.
  9        DirectConnect                         DirectConnect, developed by
                                        Neo-Modus, is a kind of free P2P
                                        client software with the open
                                        source code which supports file
                                        exchange and chat. Example:
                                        DirectConnect++, StrongDC++.
  10       KuGoo                           KuGou/KuGoo is a kind of P2P music
                                        sharing software in China which
                                        supports downloading and online
                                        listening. Example: KuGoo music.
  11       Fring_VoIP                       Fring is a kind of free VoIP
                                        software and is used for a mobile
                                        phone to connect to the Internet
                                        for communication and IM. Fring for
                                        Android does not supporting flow
                                        blocking in text chat. Example:
                                        Fring
  12       PPGou                           PPGou is a kind of downloading
```

```
                                 software which supports  HTTP and
                                 P2P downloading. Example: PPGou.
13       POCO                        POCO, developed by PoCo, is a kind
                                 of P2P-based software for resources
                                 sharing, albums management, and
                                 electronic magazine online reading.
                                 Example: POCO multimedia sharing
                                 platform.
---- More ----
-------------------------------------------------------------------------------
Total: 945
```

Table 20-29 Description of the display sa application-list command output

Item	Description
SA application list	SA application protocol list.
Index	Index of an application protocol in the SA signature file.
Protocol Name	Application protocol name in the SA signature file, for example, QQLive.
Description	Description of the application protocol, for example, QQLive, an online video player software developed by Tencent.
Total	Total number of application protocols in the SA signature file.

Related Topics

19.9.1.26 update local

19.9.1.31 update restore sdb-default

20.10.13 display sa application-statistic

Function

The **display sa application-statistic** command displays statistics on packets of different SA application protocols on an interface.

Format

display sa application-statistic { **application** *application-name* | **top-n** *number* | **all** } **interface** { *interface-type interface-number* | **virtual-template** *vt-number* **virtual-access** *va-number* } [**inbound** | **outbound**]

Parameters

Parameter	Description	Value
application *application-name*	Displays statistics on packets of a specified application.	The value is a string of 1 to 34 case-sensitive characters without spaces.
top-n *number*	Displays statistics on packets with the largest number of bytes of the first *N*th SA application protocols.	The value is an integer that ranges from 1 to 20.
all	Displays statistics on packets of all SA application protocols.	-
interface *interface-type interface-number*	Displays statistics on packets of an SA application protocol on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
virtual-template *vt-number* **virtual-access** *va-number*	Displays statistics on packets of an SA application protocol on a specified virtual interface. ● **virtual-template** *vt-number* specifies the number of a virtual template interface. The value is an integer that ranges from 0 to 1023. ● **virtual-access** *va-number* specifies the number of a virtual access interface. The value is an integer that ranges from 0 to 1023.	-
inbound	Displays packet statistics on the inbound interface.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
outbound	Displays packet statistics on the outbound interface.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the SA statistics function is enabled on an interface, run the **display sa application-statistic** command to view statistics on packets of different SA application protocols.

Precautions

If there is no packet of an SA application protocol on an interface, statistics are empty.

Example

Display statistics on packets of SA applications.

```
<Huawei> display sa application-statistic all interface GigabitEthernet 0/0/0
Protocol        Direction        Packets              Bytes       Rate(bps)
-------------------------------------------------------------------------------
DNS             Inbound          34,883,510           2,999,981,860   6,443,200
-------------------------------------------------------------------------------
```

Table 20-30 Description of the display sa application-statistic command output

Item	Description
Protocol	SA application protocol.
Direction	• Inbound: indicates the statistics on incoming packets. • Outbound: indicates the statistics on outgoing packets.
Packets	Number of forwarded packets on an SA-enabled interface.
Bytes	Number of forwarded bytes on an SA-enabled interface.

Item	Description
Rate(bps)	Rate of forwarded packets on an SA-enabled interface, in bps.

Related Topics

19.9.1.31 update restore sdb-default
20.10.28 sa application-statistic enable

20.10.14 display sa category

Function

The **display sa category** command displays SA group information in the system.

Format

display sa category [*category-name*]

Parameters

Parameter	Description	Value
category-name	Displays names of SA groups supported by the device. If this parameter is not specified, the command displays information about all the SA groups.	The value is a string of 1 to 31 case-insensitive characters without spaces.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command displays SA groups supported by the device and application protocols in the SA groups.

Before and after configuring an SA group and application protocols, you can run the **display sa category** command to check whether application protocols in the SA group meet service requirements.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the configuration of the SA group **Email**.

```
<Huawei> display sa category Email
  SA Category
  Name: Email
-------------------------------------------------------------------------------

  Index    Application Name                Description
  1        MAPI_OETP_Exchange                Mail or Messaging Application
                                   Programming Interface (MAPI) is a
                                   kind of open interface that
                                   programmers used to create mail
                                   writing and workgroup programs (for
                                   example, Email, plan, agenda, and
                                   file management). Example:
                                   OETP_MAPI_ExchangeMapiCdo and
  2        Mail.ru                     Mail.Ru is the most popular Russian
                                   Internet portal. This portal
                                   provides some kinds of services
                                   including e-mail, on-line diaries,
                                   social networking, video and photo
                                   hosting and so on.
  3        Kuikoo                       kuikoo is a website which provides
                                   easy-to-use mail services, allowing
                                   you to send and receive emails
                                   anytime anywhere conveniently and
                                   quickly . This service can be
                                   applied to computer or mobile phone
                                   platform freely.
  4        In_Mail                      In.com is an Indian website
                                   providing easy-to-use mail
                                   services, allowing you to
                                   conveniently and quickly send and
                                   receive emails anytime anywhere.
                                   This service can be applied on
                                   computers or mobile phone platforms
                                   freely.
  5        ShangMail                     ShangMail is a professional mobile
                                   mail service provided based on the
                                   leading push technology.
-------------------------------------------------------------------------------
  Total: 5
```

Table 20-31 Description of the display sa category command output

Item	Description
Name	SA group name.
Index	Index of an application protocol in the SA group.
Description	Description of the application protocol.
Total	Total number of application protocols in the SA group.

Related Topics

19.9.1.9 engine enable

19.9.1.31 update restore sdb-default

20.10.15 display sa information

Function

The **display sa information** command displays the SA configuration.

Format

display sa information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display sa information** command displays the SA configuration, including the SA status, number of protocols, and signature file status, and name.

Before and after configuring SA, run the **display sa information** command to check whether the SA configuration is correct.

Example

Display the SA configuration.

```
<Huawei> display sa information
-------------------------------------------------------------------------------
  SA status: enabled
  App protocol num       : 1622
  SA signature status    : loaded
  SA signature name      : sd1:/update/sa-sdb/sa_h30071000_2015030601.zip
-------------------------------------------------------------------------------
```

Table 20-32 Description of the display sa information command output

Item	Description
SA status	Whether SA is enabled: ● enabled: SA is enabled. ● disabled: SA is disabled. **NOTE** If SA is disabled, the information is not displayed. To enable SA, run the **update restore sdb-default** command.
App protocol num	Number of application protocols.
SA signature status	Whether the signature file is loaded: ● loaded: The signature file has been loaded. ● not loaded: The signature file is not loaded.
SA signature name	SA signature file name. To enable SA and load a signature file, run the **update restore sdb-default** command.

Related Topics

19.9.1.26 update local

19.9.1.31 update restore sdb-default

20.10.16 if-match application

Function

The **if-match application** command configures a matching rule in a traffic classifier based on application protocols.

The **undo if-match app-protocolundo if-match application** command deletes a matching rule in a traffic classifier based on application protocols.

By default, a matching rule based on application protocols is not configured in a traffic classifier.

Format

if-match application *application-name* [**user-set** *user-set-name*] [**time-range** *time-name*]

NOTE

Only AR100&AR120&AR150&AR160&AR200 series support **user-set**.

undo if-match application *application-name*

Parameters

Parameter	Description	Value
application-name	Specifies the name of an application protocol.	The value is a character string. The value depends on the applications supported in the signature database. You can run the **display sa application-list** command to check the value.
user-set *user-set-name*	Specifies the name of a user group to which ACL rules take effect.	The value is a string of 1 to 32 case-sensitive characters without spaces.
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules are always valid.	The value is a string of 1 to 32 case-sensitive characters without spaces, starting with an uppercase or a lowercase letter. In addition, the word **all** cannot be specified as a time range name.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match application** command to classify traffic based on the application protocol. The device implements the same traffic policy for the packets of the same application protocol.

You can flexibly configure the time range during which a matching rule takes effect. If the specified time range does not exist, the matching rule does not take effect.

Prerequisites

The deep security function has been enabled and a SAC signature file has been loaded using the **engine enable** command.

Precautions

If you run the **if-match application** command multiple times in the same traffic classifier view, multiple matching rules are configured.

 Copyright © Huawei Technologies Co., Ltd.

If a traffic policy contains a matching rule configured using the **if-match application** and the traffic policy needs to be applied to packets encapsulated by multiple link layer protocols, apply the traffic policy to a Layer 3 interface that has an IP address. For example, PPPoA packets are generated by encapsulating ATM cells in a PPP header, while PPP packets are encapsulated by IP or other protocols. You must create a virtual template (VT) interface and map the VT interface to the ATM interface. In this case, apply the traffic policy to the VT interface. **if-match application** in the traffic policy does not take effect if the traffic policy is applied to the ATM interface.

If a traffic policy contains a matching rule configured using the **if-match app-protocol** command and the traffic policy needs to be applied to packets on a sub-interface, apply the traffic policy to the sub-interface. **if-match application** in the traffic policy does not take effect if the traffic policy is applied to the main interface.

A user group has been created using the **user-set** command when the ACL rules take effect based on the user group.

Example

Define the traffic classifier **class1** to match packets of the SA application protocol **91farm**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match application 91farm
```

Related Topics

19.9.1.26 update local

19.9.1.31 update restore sdb-default

20.1.45 traffic classifier

20.10.17 if-match category

Function

The **if-match category** command configures a matching rule in a traffic classifier based on an SA group.

The **undo if-match category** command deletes a matching rule in a traffic classifier based on an SA group.

By default, a matching rule based on an SA group is not configured in a traffic classifier.

Format

if-match category *category-name* [**user-set** *user-set-name*] [**time-range** *time-name*]

NOTE

Only AR100&AR120&AR150&AR160&AR200 series support **user-set**.

undo if-match category *category-name*

Parameters

Parameter	Description	Value
category-name	Specifies the name of an SA group.	The value is a character string without spaces. You can run the **display sa category** command to check the value.
user-set *user-set-name*	Specifies the name of a user group to which ACL rules take effect.	The value is a string of 1 to 32 case-sensitive characters without spaces.
time-range *time-name*	Specifies the name of a time range during which ACL rules take effect. If this parameter is not specified, ACL rules are always valid.	The value is a string of 1 to 32 case-sensitive characters without spaces, starting with an uppercase or a lowercase letter. The value cannot be **all**.

Views

Traffic classifier view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **if-match category** command to configure a matching rule in a traffic classifier based on an SA group so that the device processes packets matching the same traffic classifier in the same manner.

The **if-match category** command defines a time range during which ACL rules take effect. You can flexibly configure the time range during which a matching rule takes effect. If the specified time range does not exist, the matching rule does not take effect.

Prerequisites

The SA application group specified by *category-name* already exists in the signature database. You can run the **display sa category** command to check whether the application group exists in the signature database.

Precautions

When a traffic classifier contains **if-match category**, the relationship between rules in the traffic classifier must be **or**.

If you run the **if-match category** command multiple times in the same traffic classifier view, multiple matching rules are configured.

 Copyright © Huawei Technologies Co., Ltd.

If a traffic policy contains a matching rule configured using the **if-match category** and needs to be applied to packets encapsulated by multiple link-layer protocols, apply it to a Layer 3 interface that has an IP address.

NOTE

For example, PPPoA packets are generated by encapsulating ATM cells in a PPP header, while PPP packets are encapsulated by IP or other protocols. You must create a virtual template (VT) interface and apply the VT interface to the ATM interface. In this case, apply the traffic policy to the VT interface. **if-match protocol-group** in the traffic policy that applies to an ATM interface does not take effect.

If a traffic policy contains a matching rule configured using the **if-match category** command and needs to be applied to packets on a sub-interface, apply it to the sub-interface. **if-match category** in the traffic policy that applies to a main interface does not take effect.

A user group has been created using the **user-set** command when the ACL rules take effect based on the user group.

Example

Define the traffic classifier **class1** to match the SA group **Email**.

```
<Huawei> system-view
[Huawei] traffic classifier class1
[Huawei-classifier-class1] if-match category Email
```

Related Topics

19.9.1.31 update restore sdb-default
19.9.1.26 update local
20.1.45 traffic classifier

20.10.18 ip-address (user-defined application rule view)

Function

The **ip-address** command configures an IPv4 address for a user-defined application rule.

The **undo ip-address** command deletes an IPv4 address of a user-defined application rule.

By default, no IPv4 address is configured for a user-defined application rule.

Format

ip-address *ip-address* [*mask* | *mask-length*]

undo ip-address { *ip-address* [*mask* | *mask-length*] | **all** }

Parameters

Parameter	Description	Value
ip-address	Specifies an IPv4 address.	The value is in dotted decimal notation.
mask	Specifies a subnet mask.	The value is in dotted decimal notation.
mask-length	Specifies the mask length.	The value is an integer that ranges from 1 to 32.
all	Indicates all IPv4 addresses.	-

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

After an IPv4 address is configured, the service detection engine can match network packets based on the configured IPv4 address, transport layer protocol, and port (triplet). When the triplet of traffic to be identified is determined, configure a user-defined triplet so that the device can rapidly identify traffic. For example, a user has a server. You can configure a user-defined triplet rule based on the server address, port, and transport layer protocol so that the rule can be used to identify all access traffic of the server. A user-defined application rule based on the triplet contains at least one IP address or one port number. The configured IPv4 address is the destination IPv4 address.

Precautions

You can configure a single IPv4 address or specify the subnet mask or mask length to configure a network segment in a user-defined application rule.

A user-defined application rule allows a maximum of four IPv4 addresses.

Example

Configure the IPv4 address of 10.1.1.1 for the user-defined application rule **rule1**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] rule name rule1
[Huawei-sa-user-defined-app-UD_abc-rule-rule1] ip-address 10.1.1.1
```

20.10.19 label (user-defined application view)

Function

The **label** command configures a label for a user-defined application.

The **undo label** command deletes a label of a user-defined application.

By default, no label is configured for a user-defined application.

Format

label *label-name* &<1-8>

undo label [*label-name*]

Parameters

Parameter	Description	Value
label-name	Specifies the label of a user-defined application.	For details about the label value and category, see **Table 20-33**.

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

No label is configured for a user-defined application by default. You can run the **label** command to configure a label for a user-defined application so that user-defined applications are classified based on labels.

Table 20-33 describes label classification.

Table 20-33 Label classification

Dimension	Label Name
Technology	• **Mobile-Supported**: mobile phone-supported applications • **Cloud-Based**: cloud-based applications • **Encrypted-Communications**: applications with encrypted communication • **P2P-Based**: P2P-based applications • **HTTP-Based**: HTTP-based applications • **Tunneling**: tunneling protocol-based applications

 Copyright © Huawei Technologies Co., Ltd.

Dimension	Label Name
Function	• **Network-Storage**: network disk applications • **Social-Applications**: social applications • **Plays-Game**: game applications • **Browses-Web**: applications for web page browsing • **Speech**: applications for giving opinions • **Sends-Mail**: email sending applications • **Supports-IM**: IM applications • **Supports-Video**: video transfer applications • **Supports-VoIP**: voice communication applications • **Supports-File-Transfer**: file transfer applications
Risk	The system automatically calculates the risk level (1-5) of an application based on configured risk characteristics. A higher risk level indicates a higher risk of an application. • **Exploitable**: The application has known vulnerabilities. • **Malware-Vehicle**: The malware can run on this application. The application can be used by the known malware to initiate attacks or intercept data, and is spread with this malware. • **Productivity-Loss**: The application reduces the working efficiency. Entertainment applications and news and video websites affect working of enterprise employees. • **Bandwidth-Consuming**: The application consumes network bandwidth. Applications such as Thunder and BT occupy much network bandwidth. • **Evasive**: The application has evasive characteristics. The application uses a port or protocol to traverse the firewall, proxy, or rejected webpages. • **Data-Loss**: The application causes data leakage, and provides functions such as file transmission and text upload. Using this application may cause enterprise data leakage.
Others	• **Database**: database-based applications • **Business-Applications**: enterprise applications

Follow-up Procedure

After adding labels to the user-defined application, you must run **engine configuration commit** to commit it.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a label for the user-defined application **UD_abc**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] label P2P-Based Encrypted-Communications Business-Applications
```

Related Topics

19.9.1.8 engine configuration commit

20.10.20 port (user-defined application rule view)

Function

The **port** command configures a port number for a user-defined application rule.

The **undo port** command deletes a port number of a user-defined application rule.

By default, no port number is configured for a user-defined application rule.

Format

port *port*

undo port { *port* | **all** }

Parameters

Parameter	Description	Value
port	Specifies the port number of a user-defined application rule.	The value is an integer that ranges from 1 to 65535.
all	Indicates all port numbers.	-

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

A maximum of four port numbers can be configured in a user-defined application rule.

After a port is configured, the service detection engine can match network packets based on the configured port, transport layer protocol, and IP address (triplet). When the triplet of traffic to be identified is determined, configure a user-defined

 Copyright © Huawei Technologies Co., Ltd.

triplet so that the device can rapidly identify traffic. For example, a user has a server. You can configure a user-defined triplet rule based on the server address, port, and transport layer protocol so that the rule can be used to identify all access traffic of the server. A user-defined application rule based on the triplet contains at least one IP address or one port number. The configured port is the destination port.

Example

Configure port 80 for the user-defined application rule **rule1**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] rule name rule1
[Huawei-sa-user-defined-app-UD_abc-rule-rule1] port 80
```

20.10.21 port-identification packet-number-threshold

Function

The **port-identification packet-number-threshold** command sets the threshold of packet quantity for port identification in the SA module.

The **undo port-identification packet-number-threshold** command restores the default threshold of packet quantity for port identification in the SA module.

The default threshold of packet quantity for port identification in the SA module is 16.

Format

port-identification packet-number-threshold *packets*

undo port-identification packet-number-threshold

Parameters

Parameter	Description	Value
packets	Specifies the number of packets.	The value is an integer ranging from 1 to 64.

Views

SA view

Level

2: Configuration level

Usage Guidelines

If packets exceeding the threshold are sent to the IAE and their applications cannot be identified, the SA module identifies the application by port. A high

threshold compromises the application identification performance while a low threshold increases the false positive rate. The default value (16) is recommended.

Example

Set the threshold of packet quantity for port identification in the SA module to 32.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] port-identification packet-number-threshold 32
```

20.10.22 protocol (user-defined application rule view)

Function

The **protocol** command configures the transport layer protocol type.

The **undo protocol** command restores the default transport layer protocol type.

By default, a user-defined application rule uses any type of a transport layer protocol, that is, the rule is valid for both TCP and UDP packets.

Format

protocol { **tcp** | **udp** }

undo protocol

Parameters

Parameter	Description	Value
tcp	Indicates TCP.	-
udp	Indicates UDP.	-

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

When a user-defined application rule is created based on the triplet, the default protocol types are TCP and UDP. If only one protocol type needs to be matched, run this command.

Precautions

If you run the **protocol** multiple times in the same user-defined application rule view, only the latest configuration takes effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the transport layer protocol type as TCP in a user-defined application rule.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] rule name rule1
[Huawei-sa-user-defined-app-UD_abc-rule-rule1] protocol tcp
```

20.10.23 rename (user-defined application rule view)

Function

The **rename** command renames a user-defined application rule.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the name of a user-defined application rule.	The value is a string of case-sensitive characters. When the name does not contain spaces, the value is a string of 1 to 32 characters. When the name contains spaces, the value is a string of 3 to 34 characters, and you need to put the string in double quotation marks ("), for example, "user for test". The name cannot contain question marks (?), commas (,), and hyphens (-). If the name does not contain spaces, double quotation marks ("") are not included. The name cannot be any or all.

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

You can run the **rename** command to rename a user-defined application rule to facilitate memorizing and management.

Example

Rename **rule1** to **rule2** for the user-defined application **UD_abc**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] rule name rule1
[Huawei-sa-user-defined-app-UD_abc-rule-rule1] rename rule2
[Huawei-sa-user-defined-app-UD_abc-rule-rule2]
```

20.10.24 rename (user-defined application view)

Function

The **rename** command renames a user-defined application.

Format

rename *new-name*

Parameters

Parameter	Description	Value
new-name	Specifies the name of a user-defined application.	The value is a string of case-sensitive characters and must start with UD_. When the name does not contain spaces, the value is a string of 4 to 32 characters. When the name contains spaces, the value is a string of 6 to 34 characters, and you need to put the string in double quotation marks (""), for example, "user for test". The name cannot contain question marks (?), commas (,), and hyphens (-). If the name does not contain spaces, double quotation marks ("") are not included.

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

You can run the **rename** command to rename a user-defined application to facilitate memorizing and management.

Example

Rename the user-defined application **UD_abc** to **UD_hello**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
```

```
[Huawei-sa-user-defined-app-UD_abc] rename UD_hello
[Huawei-sa-user-defined-app-UD_hello]
```

20.10.25 reset sa application-statistic

Function

The reset sa application-statistic command deletes statistics on SA application protocol packets.

Format

reset sa application-statistic { **application** *application-name* | **all** } **interface** { *interface-type interface-number* | **virtual-template** *vt-number* **virtual-access** *va-number* }

Parameters

Parameter	Description	Value
application *application-name*	Clears statistics on packets of a specified application.	The value is a string of 1 to 31 case-sensitive characters without spaces.
all	Clear statistics on packets of all SA application protocols.	-
interface *interface-type interface-number*	Clears statistics on packets on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
virtual-template *vt-number* **virtual-access** *va-number*	Clears statistics on packets on a specified virtual interface. ● **virtual-template** *vt-number* specifies the number of a virtual template interface. ● **virtual-access** *va-number* specifies the number of a virtual access interface.	The value of *vt-number* is an integer that ranges from 0 to 1023. The value of *va-number* is an integer that ranges from 0 to 1023.

 Copyright © Huawei Technologies Co., Ltd.

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **display sa application-statistic** command displays all the previous statistics on SA application protocol packets. Before recollecting statistics, run the **reset sa application-statistic** command to delete the original statistics.

Precautions

The cleared packet statistics cannot be restored. Exercise caution when you use the command.

Example

Delete statistics on packets of all SA application protocols on GE2/0/0.

```
<Huawei> reset sa application-statistic all interface gigabitethernet 2/0/0
```

Related Topics

20.10.28 sa application-statistic enable

20.10.13 display sa application-statistic

20.10.26 rule (user-defined application view)

Function

The **rule** command configures a rule for a user-defined application and displays the user-defined application rule view.

The **undo rule** command deletes a rule of a user-defined application.

By default, no rule is configured for a user-defined application.

Format

rule name *name*

undo rule { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a user-defined application rule.	The value is a string of case-sensitive characters. When the name does not contain spaces, the value is a string of 1 to 32 characters. When the name contains spaces, the value is a string of 3 to 34 characters, and you need to put the string in double quotation marks ("""), for example, "user for test". The name cannot contain question marks (?), commas (,), and hyphens (-). If the name does not contain spaces, double quotation marks ("") are not included. The name cannot be any or all.
all	Indicates all user-defined application rules.	-

Views

User-defined application view

Default Level

2: Configuration level

Usage Guidelines

The AR supports rule creation based on the triplet, keyword, or the combination of the triplet and keyword. The triplet falls into the destination triplet (server address, protocol type, and destination port number) and source triplet (user source address, protocol type, and source port number). The keyword refers to the signature of an application, and the signature identifies the application.

- You can run **20.10.18 ip-address (user-defined application rule view)**, **20.10.20 port (user-defined application rule view)**, and **20.10.22 protocol (user-defined application rule view)** to specify the triplet of an application. After the configuration is complete and submitted, the AR first uses the destination triplet of the first packet of a session to match traffic. If the traffic matches the destination triplet, the traffic is originated from this application. If the traffic does not match the destination triplet, the AR uses the source triplet of the first packet of a session to match traffic. If the traffic matches the source triplet, the traffic is originated from this application. If no match is found, the application of the traffic is not the application specified in the triplet.

  A user-defined application rule based on the triplet contains at least one IP address or one port number.
- You can run **20.10.29 signature (user-defined application rule view)** to specify the keyword of an application.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- Multiple rules can be configured for a user-defined application simultaneously. The relationship between rules is OR, that is, the traffic matches one rule is originated from an application.
- When the maximum number of user-defined application rules is reached but the maximum number of user-defined applications is not reached, you can continue to configure user-defined applications but cannot configure user-defined application rules.
- When configuring rules for user-defined applications, ensure that one flow will not match two or more rules. Otherwise, the flow may be identified to belong to multiple applications. For example, for a flow, the source IP address is SIP, the source port number is SPort, the destination IP address is DIP, the destination port number is DPort, and the protocol type is Pro. If DIP or DPort is defined in the rule for user-defined application A, and SIP or SPort is defined in the rule for user-defined application B, the flow matches the destination triplet of application A and the source triplet of application B. Therefore, the flow is identified to belong to both application A and application B. In the SD-WAN dual-gateway scenario, if the identification results of the same flow are different on the two gateways, packets of the flow may be sent and received along different paths, causing a forwarding failure.

Example

Create **rule1** for the user-defined application **UD_abc** and enter the rule view.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] rule name rule1
[Huawei-sa-user-defined-app-UD_abc-rule-rule1]
```

Related Topics

20.10.18 ip-address (user-defined application rule view)
20.10.20 port (user-defined application rule view)
20.10.22 protocol (user-defined application rule view)
20.10.29 signature (user-defined application rule view)

20.10.27 sa

Function

The **sa** command displays the SA view.

Format

sa

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

None

Example

Access the SA view.

```
<Huawei> system-view
[Huawei] sa
```

20.10.28 sa application-statistic enable

Function

The **sa application-statistic enable** command enables the SA statistics function on an interface.

The **undo sa application-statistic enable** command disables the SA statistics function on an interface.

By default, the SA statistics function is disabled on an interface.

Format

sa application-statistic enable

undo sa application-statistic enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect statistics on Layer 4 to Layer 7 traffic on an interface, run the **sa application-statistic enable** command to enable the SA statistics function.

 Copyright © Huawei Technologies Co., Ltd.

After the SA statistics function is enabled on an interface, you can use the **display sa application-statistic** command to view SA statistics.

Precautions

Only Layer 3 interfaces support SA traffic statistics.

Example

Enable the SA statistics function on GE1/0/0.

```
<Huawei> system view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] sa application-statistic enable
```

Related Topics

20.10.13 display sa application-statistic

6.11.6 bridge (interface view)

20.10.29 signature (user-defined application rule view)

Function

The **signature** command configures a signature for a user-defined application.

The **undo signature** command deletes a signature of a user-defined application.

By default, no signature is configured for a user-defined application.

Format

signature context { **flow** | **packet** } **direction** { **request** | **response** | **both** } **plain-string** *plain-string* [**field** *field*]

undo signature

Parameters

Parameter	Description	Value
context	Indicates the context matching a signature.	-
flow	Indicates flow-based matching.	-
packet	Indicates packet-based matching.	-
direction	Indicates the detection direction.	-
request	Indicates the request direction.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
response	Indicates the response direction.	-
both	Indicates bidirectional detection.	-
plain-string *plain-string*	Specifies a common character string.	The value is a string of 3 to 128 case-sensitive characters. When the value contains spaces and question marks (?), you must put the string in double quotation marks ("""), for example, "GET w?". In this case, the value contains 5 to 130 characters. When the keyword contains double quotation marks, the double quotation marks need to be converted into \x22. For example, the common character string abc"d is converted into abc\x22d.
field *field*	Specifies a signature field.	When TCP or UDP is used, you can search for **General-payload**.

Views

User-defined application rule view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In practice, data packets of some applications contain the same character string, which is equivalent to a signature. To find traffic of a required application, you can run the **signature context** command to configure the character string and direction to be matched so that the AR can block or permit data traffic from this application or take other actions.

Precautions

A user-defined application rule can be configured with only one signature.

Example

Configure the signature of the user-defined application rule **rule1** as **abcde**, and configure packet-based matching and the request direction.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc] rule name rule1
```

```
[Huawei-sa-user-defined-app-UD_abc-rule-rule1] signature context flow direction request plain-string abcde field General-Payload
```

20.10.30 user-defined-application

Function

The **user-defined-application** command creates a user-defined application and displays its view.

The **undo user-defined-application** command deletes a user-defined application.

By default, no user-defined application is configured.

Format

user-defined-application name *name*

undo user-defined-application { **name** *name* | **all** }

Parameters

Parameter	Description	Value
name *name*	Specifies the name of a user-defined application.	The value is a string of case-sensitive characters and must start with **UD_**. When the name does not contain spaces, the value is a string of 4 to 32 characters. When the name contains spaces, the value is a string of 6 to 34 characters, and you need to put the string in double quotation marks (""), for example, "UD_user for test". The name cannot contain question marks (?), commas (,), and hyphens (-). If the name does not contain spaces, double quotation marks ("") are not included.
all	Indicates all user-defined applications.	-

Views

SA view

Default Level

2: Configuration level

Usage Guidelines

Generally, the AR with the built-in signature file can easily identify common applications. For the applications that are not predefined in the signature file, you can define an application based on the application signature.

Example

Create a user-defined application named **UD_abc**.

```
<Huawei> system-view
[Huawei] sa
[Huawei-sa] user-defined-application name UD_abc
[Huawei-sa-user-defined-app-UD_abc]
```

 Copyright © Huawei Technologies Co., Ltd.

21 Network Management and Monitoring Commands

About This Chapter

21.1 SNMP Configuration Commands
21.2 RMON and RMON2 Configuration Commands
21.3 TCP FPM Configuration Commands
21.4 IP FPM Configuration Commands
21.5 CWMP Configuration Commands
21.6 LLDP Configuration Commands
21.7 NQA Configuration Commands
21.8 LSDP Configuration Commands
21.9 Service Diagnosis Configuration Commands
21.10 Mirroring Configuration Commands
21.11 Packet Capture Configuration Command
21.12 NetStream Configuration Commands
21.13 IP Accounting Configuration Commands
21.14 TWAMP Light Configuration Commands
21.15 Ping and Tracert Configuration Commands

21.1 SNMP Configuration Commands

NOTE

AR100&AR120 series (except AR129CV&AR129CVW&AR129CGVW-L) do not support SNMP.

 Copyright © Huawei Technologies Co., Ltd.

21.1.1 display snmp-agent community

Function

The **display snmp-agent community** command displays the configured community name.

Format

display snmp-agent community { **read** | **write** }

Parameters

Parameter	Description	Value
read	Displays the name of a read-only community. The parameter is specified using the **snmp-agent community** command.	-
write	Displays the name of a read-write community. The parameter is specified using the **snmp-agent community** command.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

When configuring a management entity, you can use the **display snmp-agent community** command to check the community name configured on the current agent.

You have to configure the community name using the **snmp-agent community** command before you run the **display snmp-agent community** command.

Example

Display the current community name.

```
<Huawei> display snmp-agent community read
  Community name: %@%@$X!5#d+t+OJOXL1[{O2!&Fe&0UZv'@a;R/`Y+kK$4BUGFe)&2YLuM/kMF!
HPG5Mzz3DXe2&F%@%@
  Storage type: nonVolatile
  View name: ViewDefault
  Acl: 2001

  Total number is 1
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-1 Description of the display snmp-agent community read command output

Item	Description
Community name	Name of a community.
Storage type	Data storage type. The system supports the following five storage types: ● volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. Objects with storage type **volatile** cannot be changed to **readOnly** or **permanent**. ● nonVolatile: Lines are saved in the nonvolatile storage medium such as Non Volatile Random Access Memory (NVRAM) and can be restored after the device restarts. Objects with storage type **nonVolatile** cannot be changed to **readOnly** or **permanent**. ● permanent: Permanent lines are saved in the nonvolatile storage medium such as Read-only Memory (ROM). They can be modified but cannot be deleted. Rowstatus objects with storage type **permanent** cannot be modified. ● readOnly: Read-only lines are saved in the nonvolatile storage medium such as ROM. They cannot be modified or deleted. Rowstatus objects with storage type **readOnly** cannot be modified. ● other: other storage types. In practice, the device generally uses only the **nonVolatile** type.
View name	Name of a view.
Acl	Number of the ACL configured for the community.

Related Topics

21.1.17 snmp-agent community

 Copyright © Huawei Technologies Co., Ltd.

21.1.2 display snmp-agent extend error-code status

Function

The **display snmp-agent extend error-code status** command allows you to check whether the function of sending extended error codes to the NMS is enabled on the device.

Format

display snmp-agent extend error-code status

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

If the NMS does not receive the extended error codes sent from the device, you can run the **display snmp-agent extend error-code status** command to check whether the function of sending extended error codes is enabled on the device.

Example

Display whether the function of sending extended error codes is enabled on the device.

```
<Huawei> display snmp-agent extend error-code status
Extend error-code status: enabled
```

Table 21-2 Description of the display snmp-agent extend error-code status command output

Item	Description
Extend error-code status	Whether the function of sending extended error codes is enabled. ● enabled: The function of sending extended error codes is enabled. ● disabled: The function of sending extended error codes is disabled.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.20 snmp-agent extend error-code enable

21.1.3 display snmp-agent group

Function

The **display snmp-agent group** command displays information about an SNMP agent group.

Format

display snmp-agent group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Displays the name of an SNMP agent group.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When configuring a management object according to the SNMPv3 group information, you can run the **display snmp-agent group** command to view information about the SNMP agent group.

If the command contains no parameter, information about all groups is displayed, such as the group name, security model, and storage type.

Precautions

You can run the **display snmp-agent group** command to view information about an SNMP agent group only after the SNMP agent group is created through the **snmp-agent group** command.

Example

Display information about all SNMPv3 working groups.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display snmp-agent group

  Group name: testgroup
  Security model: v3 AuthPriv
  Readview: ViewDefault
  Writeview: dnsmib
  Notifyview: dnsmib
  Storage type: nonVolatile
  Acl: 2001

  Total number is 1
```

Table 21-3 Table 1 Description of the display snmp-agent group command output

Item	Description
Group name	Indicates the name of an SNMP agent group.
Security model	Security mode. The options are as follows: ● v3 AuthPriv: authenticated and encrypted. ● v3 noAuthPriv: encrypted but not authenticated. ● v3 AuthnoPriv: authenticated but not encrypted. ● v3 noAuthnoPriv: neither authenticated nor encrypted.
Readview	Indicates the view of the read-only MIB of the group. This parameter can be set using the **snmp-agent group** command.
Writeview	Indicates the view of the read-write MIB of the group. This parameter can be set using the **snmp-agent group** command.
Notifyview	Indicates the view of the notify MIB of the group. This parameter can be set using the **snmp-agent group** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Storage type	Data storage type. The system supports the following five storage types: ● readOnly: Readonly lines are saved in the nonvolatile storage medium. They cannot be modified or deleted. Rowstatus objects with storage type **readOnly** cannot be modified. ● permanent: Permanent lines are saved in the nonvolatile storage medium. They can be modified but cannot be deleted. Rowstatus objects with storage type **permanent** cannot be modified. ● nonVolatile: Lines are saved in the nonvolatile storage medium and are restored after the device restarts. Objects with storage type **nonVolatile** cannot be changed to **readOnly** or **permanent**. ● volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. Objects with storage type **volatile** cannot be changed to **readOnly** or **permanent**. ● other: other storage types. In practice, the device generally uses only the **nonVolatile** type.
Acl	Indicates the number of the ACL configured for the group.

Related Topics

21.1.21 snmp-agent group

21.1.4 display snmp-agent local-engineid

Function

The **display snmp-agent local-engineid** command displays the engine ID of the local SNMP entity.

Format

display snmp-agent local-engineid

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The engine ID of the SNMP is the unique identity of the SNMP management feature. The engine ID uniquely identifies an SNMP entity in a management domain. The engine ID of the SNMP is one of the important components of the SNMP entity, enabling multiple functions such as message scheduling, message processing, security authentication, and access control.

After the SNMP agent function is enabled, you can run the **display snmp-agent local-engineid** command to display the default or configured local SNMP entity.

Example

Display the engine ID of the local SNMP entity.

```
<Huawei> display snmp-agent local-engineid
  SNMP local EngineID: 800007DB030819A6CDA894
```

Table 21-4 Description of the display snmp-agent local-engineid command output

Item	Description
SNMP local EngineID	The engine ID of the local SNMP entity is manually specified by an administrator using the **snmp-agent local-engineid** command or automatically generated by the system using certain algorithms.

Related Topics

21.1.22 snmp-agent local-engineid

21.1.5 display snmp-agent mib-view

Function

The **display snmp-agent mib-view** command displays the current MIB view.

Format

display snmp-agent mib-view [*view-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
view-name	Specifies the view to be displayed. This parameter can be set using the **snmp-agent mib-view** command.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **snmp-agent mib-view** command creates or updates a MIB view. To check the default and configured MIB view, you can run the **display snmp-agent mib-view** command.

By default, the view ViewDefault is adopted.

Precautions

Before running the **display snmp-agent mib-view** command, ensure that the SNMP agent has been enabled.

Example

Display the current MIB view.

```
<Huawei> display snmp-agent mib-view
  View name: ViewDefault
  MIB subtree: internet
  Subtree mask:
  Storage type: nonVolatile
  View type: included
  View status: active

  View name: ViewDefault
  MIB subtree: lagMIB
  Subtree mask:
  Storage type: nonVolatile
  View type: included
  View status: active

  View name: ViewDefault
  MIB subtree: snmpUsmMIB
  Subtree mask:
  Storage type: nonVolatile
  View type: excluded
  View status: active
```

 Copyright © Huawei Technologies Co., Ltd.

```
View name: ViewDefault
MIB subtree: snmpVacmMIB
Subtree mask:
Storage type: nonVolatile
View type: excluded
View status: active

Total number is 1
```

Table 21-5 Description of the display snmp-agent mib-view command output

Item	Description
View name	View name.
MIB subtree	MIB subtree.
Subtree mask	Subtree mask.
Storage type	Data storage type. ● volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. ● nonVolatile: Lines are saved in the nonvolatile storage medium and are restored after the device restarts. ● permanent: Permanent lines are saved in the nonvolatile storage medium. They can be modified but cannot be deleted. ● readOnly: Readonly lines are saved in the nonvolatile storage medium. They cannot be modified or deleted. ● other: other storage types.
View type	Type of a view. The options are as follows: ● included: The view includes the subtree. ● excluded: The view excludes the subtree.
View status	Indicates the status of the MIB view.
Total number	Total number of views whose information is queried.

Related Topics

21.1.23 snmp-agent mib-view

 Copyright © Huawei Technologies Co., Ltd.

21.1.6 display snmp-agent notify-filter-profile

Function

The **display snmp-agent notify-filter-profile** command displays information about a specified trap filter profile or all trap filter profiles.

Format

display snmp-agent notify-filter-profile

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display snmp-agent notify-filter-profile** command to view information about configured trap filter profiles. The command can display all the configured trap filter profiles or a specified trap file profile.

Example

Display information about configured trap filter profiles.

```
<Huawei> display snmp-agent notify-filter-profile
  Trap filter profile list:
  notify-filter name: 1
  notify-filter type: included
  notify-filter subtree: iso
  notify-filter storage-type: nonVolatile
  notify-filter status: active
```

Table 21-6 Description of the display snmp-agent notify-filter-profile command output

Item	Description
notify-filter name	Name of a trap filter profile.
notify-filter type	Whether to filter out the trap object.
notify-filter subtree	Trap filter subtree.
notify-filter storage-type	Storage mode of the trap filter profile.
notify-filter status	Status of a row.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.24 snmp-agent notify-filter-profile

21.1.7 display snmp-agent statistics

Function

The **display snmp-agent statistics** command displays statistics about SNMP messages.

Format

display snmp-agent statistics

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

The **display snmp-agent statistics** command analyzes the statistics about SNMP messages and obtains information about the communication between the SNMP agent and the NMS for fault location.

In an SNMP management system, the NMS and the SNMP agent exchange SNMP messages as follows:

- The NMS acts as a manager to send an SNMP Request message to the SNMP agent.
- The SNMP agent searches the MIB on the device for the required information and sends an SNMP Response message to the NMS.
- When the trap triggering conditions are met, the SNMP agent sends a trap to the NMS to report the event occurring on the device. In this manner, the network administrator can process the event occurring on the network in time.

NOTE

If large number of messages are received in short period, a great number of CPU resources are occupied. The number of received messages depends on the frequency at which the NMS sends the Request messages.

Example

Display the statistics about the SNMP messages.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display snmp-agent statistics
  The PDU process average time ( second ): 2
  0 Messages delivered to the SNMP entity
  0 Messages which were for an unsupported version
  0 Messages which used an unknown community name
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  0 MIB objects retrieved successfully
  0 MIB objects altered successfully
  0 Get-request PDUs accepted and processed
  0 Get-next PDUs accepted and processed
  0 Set-request PDUs accepted and processed
  0 Messages passed from the SNMP entity
  0 Messages which were discarded, because the message queue is full
  0 SNMP PDUs which had a tooBig error (Maximum packet size 12000)
  0 SNMP PDUs which had a noSuchName error
  0 SNMP PDUs which had a had badValue error
  0 SNMP PDUs which had a general error
  0 Response PDUs accepted and processed
  0 Trap PDUs accepted and processed
  Top 10 nodes which take the longest time:
   0:PerSwitchCosttime=219ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=219ms
SwitchCnt=1
   1:PerSwitchCosttime=72ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=72ms
SwitchCnt=1
   2:PerSwitchCosttime=60ms OpType=0 OID=1.3.6.1.2.1.2.1 CallBack=0x32a3f6c CostTime=60ms
SwitchCnt=1
   3:PerSwitchCosttime=39ms OpType=0 OID=1.3.6.1.2.1.1.1 CallBack=0x32a3f6c CostTime=39ms
SwitchCnt=1
   4:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
   5:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
   6:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.1 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
   7:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.2 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
   8:PerSwitchCosttime=2ms OpType=2 OID=1.3.6.1.2.1.2.2.1.2 CallBack=0x32a51a0 CostTime=2ms
SwitchCnt=1
   9:PerSwitchCosttime=1ms OpType=0 OID=1.3.6.1.2.1.1.2 CallBack=0x32a3f6c CostTime=1ms SwitchCnt=1
```

Table 21-7 Description of the display snmp-agent statistics command output

Item	Description
Messages delivered to the SNMP entity	Total number of received SNMP messages.
Messages which were for an unsupported version	Number of messages with incorrect version information.
Messages which used an unknown community name	Number of messages with incorrect community names.
Messages which represented an illegal operation for the community supplied	Number of messages whose community names have incorrect access rights.
ASN.1 or BER errors in the process of decoding	Number of SNMP messages with encoding errors.
MIB objects retrieved successfully	Number of variables requested by the NMS.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
MIB objects altered successfully	Number of variables set by the NMS.
Get-request PDUs accepted and processed	Number of received GetRequest messages.
Get-next PDUs accepted and processed	Number of received GetNextRequest messages.
Set-request PDUs accepted and processed	Number of received SetRequest messages.
Messages passed from the SNMP entity	Total number of outgoing SNMP messages.
Messages which were discarded, because the message queue is full	Total number of discarded SNMP messages resulting in an outbound message queue being full.
SNMP PDUs which had a tooBig error (Maximum packet size 12000)	Number of SNMP messages with Too_big errors.
SNMP PDUs which had a noSuchName error	Number of messages with noSuchName errors.
SNMP PDUs which had a had badValue error	Number of SNMP messages with Bad_values errors.
SNMP PDUs which had a general error	Number of SNMP messages with General_errors.
Response PDUs accepted and processed	Number of received response messages.
Trap PDUs accepted and processed	Number of sent traps.
NOTE V200R010C10 and later versions support the following parameters.	
Top 10 nodes which take the longest time	Top 10 objects that take the longest time to complete.
PerSwitchCosttime	Time consumed before a single handover.
OpType	Operation type.
OID	OID.
CallBack	Callback address.
CostTime	Total time consumed.
SwitchCnt	Number of switchovers.

Copyright © Huawei Technologies Co., Ltd.

21.1.8 display snmp-agent sys-info

Function

The **display snmp-agent sys-info** command displays the system information of the current SNMP device, including the contact information about the system maintenance, physical location of the device, and SNMP version.

Format

display snmp-agent sys-info [**contact** | **location** | **version**] *

Parameters

Parameter	Description	Value
contact	Displays the contact information of the current SNMP device.	-
location	Displays the physical location information of the current SNMP device.	-
version	Displays the SNMP version running in the current system.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

You can use the **display snmp-agent sys-info** command to check the system maintenance information of the current SNMP device. The information includes:

- Contact information of the device administrator
- Physical location of the device
- SNMP version

If the parameter is not specified, all information is displayed.

The **snmp-agent sys-info** command can be used to set the output of the **display snmp-agent sys-info** command

Example

Display the system information of the SNMP agent.

```
<Huawei> display snmp-agent sys-info
 The contact person for this managed node:
        R&D Beijing, Huawei Technologies Co.,Ltd.
  The physical location of this node:
        Beijing China
  SNMP version running in the system:
        SNMPv2c
```

 Copyright © Huawei Technologies Co., Ltd.

Display the SNMP version running in the current system.

```
<Huawei> display snmp-agent sys-info version
  SNMP version running in the system:
        SNMPv2c
```

Display the contact information of the current SNMP device.

```
<Huawei> display snmp-agent sys-info contact
 The contact person for this managed node:
        R&D Beijing, Huawei Technologies Co.,Ltd.
```

Display the physical location information of the current SNMP device.

```
<Huawei> display snmp-agent sys-info location
 The physical location of this node:
        Beijing China
```

Table 21-8 Description of the display snmp-agent sys-info command output

Item	Description
The contact person for this managed node:	Contact person of the managed device. By specifying this parameter, you can store the important information to the router for convenient query.
The physical location of this node:	Location of the managed device.
SNMP version running in the system:	SNMP version running in the current system. The value can be: ● SNMPv1 ● SNMPv2c ● SNMPv3

Related Topics

21.1.26 snmp-agent sys-info

21.1.9 display snmp-agent target-host

Function

The **display snmp-agent target-host** command displays the list of destination hosts that receive traps.

Format

display snmp-agent target-host

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can use this command to query the IP addresses of all valid destination hosts that are configured to receive traps. The command output consists of the following two parts:

- List of the destination hosts that receive traps.
- Parameter list of the destination hosts and hosts that are not bound to the parameters.

Precautions

Host parameters must have been configured for the destination host. Otherwise, the destination host cannot receive traps, and parameters are not displayed.

Example

Display the configurations of all destination hosts in the system.

```
<Huawei> display snmp-agent target-host
  Traphost list:
  Target host name: nms2
  Traphost address: 10.1.1.2
  Traphost portnumber: 162
  Target host parameter: trapnms2

  Total number is 1

  Parameter list trap target host:
  Parameter name of the target host: trapnms2
  Message mode of the target host: SNMPV3
  Trap version of the target host: v3
  Security name of the target host:  %@%@_=XqAFC_94uCS,3'<gYC*ZU6%@%@
  Security level of the target host: privacy

  Total number is 1
```

Table 21-9 Description of the display snmp-agent target-host command output

Item	Description
Traphost list	List of the destination hosts that receive traps.
Target host name	Name of a destination host that receives traps.
Traphost address	IP address of a destination host that receives traps.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Traphost portnumber	Number of the port on a destination host for receiving traps.
Target host parameter	Parameter name of a destination host that receives traps.
Parameter list trap target host	Parameter list of destination hosts that receive traps.
Parameter name of the target host	Parameter name of destination hosts that receive traps.
Message mode of the target host	Protocol used by destination hosts that receive traps.
Trap version of the target host	Version of the protocol for transmitting traps.
Security name of the target host	Security name of destination hosts that receive traps.
Security level of the target host	Authentication mode of traps.
Total number	Total number of views whose information is queried.

Related Topics

21.1.30 snmp-agent trap enable

21.1.10 display snmp-agent trap all

Function

The **display snmp-agent trap all** command checks current and default status of all traps in all features.

Format

display snmp-agent trap [**feature-name** *feature-name*] **all**

Parameters

Parameter	Description	Value
feature-name *feature-name*	Specifies a feature that generates traps.	-

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

After the device is enabled to send traps to the NMS:

- You can run the **display snmp-agent trap all** command to check the status of all traps in all features.
- You can run the **display snmp-agent trap feature-name** *feature-name* **all** command to check the status of all traps in a specified feature.

Example

Check the default status of all traps in all features.

```
<Huawei> display snmp-agent trap all
-------------------------------------------------------------------------------
Feature name: SSH
Trap number : 1
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwSSHSftpUserNumExceedMax       off                     off
-------------------------------------------------------------------------------
Feature name: VFS
Trap number : 3
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwFlhOperNotification           off                     off
hwFlhSyncSuccessNotification    off                     off
hwFlhSyncFailNotification       off                     off
-------------------------------------------------------------------------------
  ---- More ----
```

Table 21-10 Description of the display snmp-agent trap all command output

Item	Description
Feature name	Name of the feature that generates traps.
Trap number	Number of traps generated by this feature.
Trap name	Trap name.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Current switch status	Current status of the trap function: • on: indicates that the trap function is enabled. • off: indicates that the trap function is disabled.

Related Topics

21.1.29 snmp-agent trap disable

21.1.30 snmp-agent trap enable

21.1.31 snmp-agent trap enable feature-name

21.1.11 display snmp-agent trap feature-name snmp all

Function

The **display snmp-agent trap feature-name snmp all** command displays whether all SNMP traps are enabled.

Format

display snmp-agent trap feature-name snmp all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent trap feature-name snmp all** command to check status of all SNMP traps. This status can be configured using the **snmp-agent trap enable feature-name snmp** command.

Example

View whether all SNMP traps are enabled.

```
<Huawei>display snmp-agent trap feature-name snmp all
-----------------------------------------------------------------------------
Feature name: SNMP
Trap number : 3
```

 Copyright © Huawei Technologies Co., Ltd.

```
-----------------------------------------------------------------------------
Trap name                  Default switch status   Current switch status
coldStart                 on                      on
warmStart                  on                      on
authenticationFailure        off                     off
```

Table 21-11 Description of the display snmp-agent trap feature-name snmp all command output

Item	Description
Feature name	Name of the module where the trap is generated
Trap number	Number of traps.
Trap name	Name of trap, including ● authenticationFailure: This trap is generated when a user uses an incorrect community name and is unable to log in to the device. ● coldStart: This trap is generated when the device is powered off and restarted. ● warmStart: This trap is generated when the status of SNMP agent is changed from disable to enable.
Default switch status	Default status of a trap ● on: The trap function is enabled. ● off: The trap function is disabled.
Current switch status	Current status of a trap ● on: The trap function is enabled. ● off: The trap function is disabled. This status can be configured using the **snmp-agent trap enable feature-name snmp** command.

Related Topics

21.1.32 snmp-agent trap enable feature-name snmp

21.1.12 display snmp-agent trap-source

Function

The **display snmp-agent trap-source** command displays the source interface that sends trap messages.

Format

display snmp-agent trap-source

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

3: Management level

Usage Guidelines

After users run the **snmp-agent trap source** command to configure the source interface that sends trap messages, you can run the **display snmp-agent trap-source** command to display the configured source interface.

Example

Display the source interface that sends trap messages.

```
<Huawei> display snmp-agent trap-source
  Trap source interface name: GigabitEthernet1/0/0
```

Table 21-12 Description of the display snmp-agent trap-source output

Item	Description
Trap source interface name	Source interface that sends trap messages.

Related Topics

21.1.36 snmp-agent trap source

21.1.13 display snmp-agent usm-user

Function

The **display snmp-agent usm-user** command displays information about an SNMPv3 user.

Format

display snmp-agent usm-user [*user-name*]

Parameters

Parameter	Description	Value
user-name	Specifies an SNMPv3 user. This parameter is specified using the **snmp-agent usm-user** command.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The displayed information about an SNMPv3 user includes:

- User name.
- Local engine ID of the user. The SNMPv3 engine ID uniquely identifies an SNMPv3 agent in a management domain. The SNMPv3 engine ID is an important component of the SNMPv3 agent. It schedules and processes SNMPv3 messages, and implements security authentication and access control.

Precautions

The **display snmp-agent usm-user** command is applicable only to SNMPv3 users.

Example

Display information about all current SNMPv3 users.

```
<Huawei> display snmp-agent usm-user
  User name: testuser
  Engine ID: 800007DB03548998F3A458
  Group name: testgroup
  Authentication mode: md5, Privacy mode: des56
  Storage type: nonVolatile
  User status: active

  Total number is 1
```

Table 21-13 Description of the display snmp-agent usm-user command output

Item	Description
User name	SNMPv3 user name, which identifies a user.
Engine ID	Engine ID corresponding to the SNMPv3 user.
Group name	SNMPv3 group name corresponding to the SNMPv3 user.
Authentication mode	Authentication mode for the SNMPv3 user: ● md5 ● No authentication mode

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Privacy mode	Encryption mode for the SNMPv3 user: ● des56 ● aes128
Storage type	Data storage type. ● volatile: Lines are saved in the volatile storage medium and are lost after the device restarts. ● nonVolatile: Lines are saved in the nonvolatile storage medium and are restored after the device restarts. ● permanent: Permanent lines are saved in the nonvolatile storage medium. They can be modified but cannot be deleted. ● readOnly: Readonly lines are saved in the nonvolatile storage medium. They cannot be modified or deleted. ● other: other storage types.
User status	Status of the SNMPv3 user: ● active ● inactive
Total number	Number of SNMPv3 users.

Related Topics

21.1.21 snmp-agent group
21.1.22 snmp-agent local-engineid
21.1.37 snmp-agent usm-user

21.1.14 enable snmp trap updown

Function

The **enable snmp trap updown** command enables an interface to send a trap to the NMS when the protocol status of the interface changes.

The **undo enable snmp trap updown** command disables an interface from sending a trap to the NMS when the protocol status of the interface changes.

By default, an interface sends a Trap message to the NMS when the protocol status of the interface changes.

 Copyright © Huawei Technologies Co., Ltd.

Format

enable snmp trap updown

undo enable snmp trap updown

Parameters

None

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **enable snmp trap updown** command is used to enable an interface to send a Trap message to the NMS when the protocol status of the interface changes, which helps the NMS monitor the interface status in real time.

Precautions

By default, the function of sending a Trap message to the NMS when the protocol status of the interface changes is enabled. If an interface alternates between Up and Down, it will frequently send Trap messages to the NMS, causing the NMS to be busy processing these Trap messages. In this case, you can run the **undo enable snmp trap updown** command to disable the interface from sending trap messages to the NMS.

Example

Enable an interface to send a trap to the NMS when the protocol status of the interface changes.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] enable snmp trap updown
```

21.1.15 snmp-agent

Function

The **snmp-agent** command enables the SNMP agent function.

The **undo snmp-agent** command disables the SNMP agent function.

By default, the SNMP agent function is disabled.

Format

snmp-agent

 Copyright © Huawei Technologies Co., Ltd.

undo snmp-agent

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

By executing the **snmp-agent** command with any parameter enables the SNMP agent function. For example, if you execute the **snmp-agent community** command, the community name gets created and also SNMP agent function is enabled.

Precautions

- To configure SNMP functions using the command, you do not need to run the **snmp-agent** command to enable the SNMP agent function.
- To configure SNMP functions using the configuration file, you need to run the **snmp-agent** command in the configuration file; otherwise, you cannot enable SNMP functions.

Example

Enable the SNMP agent function.

```
<Huawei> system-view
[Huawei] snmp-agent
```

Disable the SNMP agent function.

```
<Huawei> system-view
[Huawei] undo snmp-agent
```

21.1.16 snmp-agent bulk-fast enable

Function

The **snmp-agent bulk-fast enable** command enables the function of accelerating the SNMP GetBulk operation.

The **undo snmp-agent bulk-fast enable** command disables the function of accelerating the SNMP GetBulk operation.

By default, the function of accelerating the SNMP GetBulk operation is disabled.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

This function is supported in V200R010C10 and later versions.

Format

snmp-agent bulk-fast enable

undo snmp-agent bulk-fast enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

The GetBulk operation is slow when only some SNMP views are configured. You can run the **snmp-agent bulk-fast enable** command to enable the function of accelerating the SNMP GetBulk operation.

Example

Enable the function of accelerating the SNMP GetBulk operation.

```
<Huawei> system-view
[Huawei] snmp-agent bulk-fast enable
```

21.1.17 snmp-agent community

Function

The **snmp-agent community** command configures the SNMPv1 or SNMPv2c read-write community name.

The **undo snmp-agent community** command is used to delete the configuration of the community name.

By default, the community name is not configured.

Format

snmp-agent community { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*] *

undo snmp-agent community *community-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
read	Indicates that the community with a specified name has the read-only rights in the specified view.	-
write	Indicates that the community with a specified name has the read-write rights in the specified view.	-
community-name	Specifies the name of a community. The community name is displayed in cipher text in the configuration file.	The value is a string of 6 to 32 characters or 88 characters case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string. ● When the community name is a string of 6 to 32 characters, the string is processed as plain text by default and will be encrypted. ● When the community name is a string of 88 characters, the string is processed as cipher text by default, and the system will determine whether the string can be parsed. By default, the complexity check is enabled for a community name. If a community name fails the complexity check, the community name cannot be configured. **NOTE** The device has the following requirements for community name complexity: ● The default minimum length of a community name is six characters. ● A community name includes at least two kinds of characters, which can be uppercase letters, lowercase letters, digits, and special characters.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
mib-view *view-name*	Specifies a MIB view that the community name can access. ● If no MIB view that the community name can access is specified, the community name can access only the default MIB view, that is, ViewDefault. ● If a MIB view that the community name can access is specified, the community name can access the specified MIB view.	It is a string of 1 to 32 case-sensitive characters without spaces. When double quotation marks are used around the string, spaces are allowed in the string.
acl *acl-number*	Specifies the ACL corresponding to the community name. **NOTE** Currently, SNMP supports only basic ACLs.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When running the **snmp-agent community** command, you can select parameters based on the networking requirements.

- To grant the NMS read-only permission in the specified view, configure **read**.
- To grant the NMS read-write permission in the specified view, configure **write**.
- To allow specified NMSs using this community name have the rights of ViewDefault, omit **mib-view** *view-name*.
- To allow all NMSs using this community name to manage specified objects on a managed device, omit **acl** *acl-number*.
- To allow specified NMSs using this community name to manage specified objects on a managed device, configure **mib-view** and **acl**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

When both community name and ACL are configured, the NMS verifies the community name before accessing the device, and then checks the ACL rules. If the community name does not exist, the packet is discarded and a log indicating that the community name is wrong is printed. The ACL rule is not checked. That is, the ACL rule is checked only when the community name exists.

You can run the **display snmp-agent community** command to view the current community name.

Precautions

When you configure a community name in cipher text that starts and ends with %@%@ (the community name can be decrypted by the device), the community name is displayed in the same manner as the configured one in the configuration file. Do not use this setting.

If you specify the parameter **mib-view** or **acl** when running the **snmp-agent community** command, configure the MIB view and ACL rule. If the default MIB view is deleted, the NMS using this community name cannot communicate with managed devices. To continue to use this community name, specify an existing MIB view.

Example

Set the name of a community to **comaccess1** and configure the read-only rights for the community.

```
<Huawei> system-view
[Huawei] snmp-agent community read comaccess1
```

Set the name of a community to **comaccess2** and configure the read-write rights for the community.

```
<Huawei> system-view
[Huawei] snmp-agent community write comaccess2
```

Related Topics

21.1.1 display snmp-agent community

21.1.18 snmp-agent complexity-check disable

Function

The **snmp-agent complexity-check disable** command disables complexity check for community names and SNMPv3 authentication and encryption passwords.

The **undo snmp-agent complexity-check disable** command enables complexity check for community names and SNMPv3 authentication and encryption passwords.

By default, complexity check for community names and SNMPv3 authentication and encryption passwords is enabled.

 Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent complexity-check disable

undo snmp-agent complexity-check disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To improve maintenance efficiency in secure environment, disable complexity check for community names and SNMPv3 passwords by running the **snmp-agent complexity-check disable** command. After complexity check is disabled, the minimum length of a community name or SNMPv3 password is 1, and the community name or password must contain at least one type of characters.

If a community name or SNMPv3 password does not meet complexity requirements, the system is prone to attacks from malicious users, affecting system security. Therefore, you are advised to run the **undo snmp-agent complexity-check disable** command to enable complexity check for community names and SNMPv3 passwords. After complexity check is enabled, the community names or SNMPv3 authentication and encryption passwords must meet the following requirements:

- A community name contains at least six characters. An SNMPv3 authentication or encryption password contains at least eight characters.
- A community name or password must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters (excluding spaces).
- An SNMPv3 authentication password cannot be the same as an SNMPv3 encryption password.

Example

Disable complexity check for community names or SNMPv3 authentication and encryption passwords.

```
<Huawei> system-view
[Huawei] snmp-agent complexity-check disable
```

Related Topics

21.1.17 snmp-agent community

 Copyright © Huawei Technologies Co., Ltd.

21.1.19 snmp-agent community simple

Function

The **snmp-agent community simple** command enables plain text mode for the community names of SNMPv1 and SNMPv2c.

The **undo snmp-agent community simple** command disables plain text mode for the community names.

By default, community names are not transmitted in plain text.

Format

snmp-agent community simple { **read** | **write** } *community-name* [**mib-view** *view-name* | **acl** *acl-number*] *

undo snmp-agent community simple

Parameters

Parameter	Description	Value
read	Indicates that a community name has the read permission in the specified MIB view.	-
write	Indicates that a community name has the read and write permission in the specified MIB view.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
community-name	Specifies a community name, which is displayed in plain text in the configuration file.	The value is a string of 6 to 32 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces. **NOTE** The community name must meet the following requirements: ● The community name contains at least six characters. ● The community name must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters. ● By default, the system checks the community name complexity. The community name that fails the check is not allowed.
mib-view *view-name*	Specifies the MIB view that a community name can access. ● If no MIB view is specified for a community name, this community name can access only the default MIB view, ViewDefault. ● If a MIB view is specified for a community name, this community name can access only the specified MIB view.	The value is a string of 1 to 32 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
acl *acl-number*	Specifies the ACL number matching the community name. **NOTE** SNMP supports only the basic ACL, but does not support advanced or MPLS-based ACL. The specified ACL takes effect for both IPv4 and IPv6 networks.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When running the **snmp-agent community simple** command to enable plain text mode for SNMPv1 and SNMPv2c read-write community names, select the parameters as required:

- To grant only the read right to the NMS in the specified view (for example, for an administrator with a low level), use the **read** parameter.
- To grant the read and write rights to the NMS in the specified view (for example, for an administrator with a high level), use the **write** parameter.
- To allow some NMSs using a community name to access the MIB view Viewdefault, do not specify the **mib-view** *view-name* parameter.
- To allow some NMSs using a community name to manage certain objects, specify both **mib-view** and **acl**.

NOTE

When both community name and ACL are configured, the NMS checks the community name and then the ACL before accessing the device. If a community name does not exist, packets are discarded and the system prints a community name error log. In addition, the system does not check ACL. That is, the system checks ACL only when the community name exists.

To view the current community name, run the **display snmp-agent community** command.

Precautions

If the **mib-view** or **acl** parameter is specified in the **snmp-agent community** command, configure the MIB view and ACL rules. Do not delete the default MIB view. If it is deleted, the NMS and managed device using this community name cannot set up a connection. To use this community name again, specify an existing MIB view.

Example

Enable plain text mode for the community name **comaccess1** and grant only the read right to the community name.

```
<Huawei> system-view
[Huawei] snmp-agent community simple read comaccess1
```

Enable plain text mode for the community name **comaccess2** and grant the read and write rights to the community name.

```
<Huawei> system-view
[Huawei] snmp-agent community simple write comaccess2
```

Related Topics

21.1.1 display snmp-agent community

 Copyright © Huawei Technologies Co., Ltd.

21.1.20 snmp-agent extend error-code enable

Function

The **snmp-agent extend error-code enable** command enables the function of sending extended error codes to the NMS on the device.

The **undo snmp-agent extend error-code enable** command disables the function of sending extended error codes to the NMS.

By default, the function of sending extended error codes to the NMS is disabled.

Format

snmp-agent extend error-code enable

undo snmp-agent extend error-code enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

If the NMS and managed device are Huawei devices, error codes are extended and more scenarios are defined after the function of sending extended error codes is enabled. As a result, users are enabled to locate and troubleshoot faults quickly and accurately.

Support of the MIB for the extended error code:

- For the MIB that supports the extended error code, you can enable the SNMP extended error code function and use Huawei NMS to provide the NMS with various error codes.
- For the MIB that does not support the extended error code, after the SNMP extended error code function is enabled, NMS of either Huawei or other vendors can obtain only the standard error code.

Example

Enable the function of sending extended error codes to the NMS on the device.

```
<Huawei> system-view
[Huawei] snmp-agent extend error-code enable
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.2 display snmp-agent extend error-code status

21.1.21 snmp-agent group

Function

The **snmp-agent group** command creates an SNMP group by mapping SNMP users to SNMP views.

The **undo snmp-agent group** command deletes a specified SNMP user group.

By default, no SNMP group is configured.

Format

snmp-agent group v3 *group-name* { **authentication** | **noauth** | **privacy** } [**read-view** *read-view* | **write-view** *write-view* | **notify-view** *notify-view* | **acl** *acl-number*] *

undo snmp-agent group v3 *group-name* { **authentication** | **noauth** | **privacy** }

Parameters

Parameter	Description	Value
v3	Indicates that the SNMP group uses the security mode in SNMPv3.	-
group-name	Specifies the name of an SNMP group.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
authentication | **noauth** | **privacy**	Indicates the security level of the SNMP group. • **authentication**: indicates that SNMP messages are authenticated but not encrypted. • **noauth**: indicates that SNMP messages are neither authenticated nor encrypted. • **privacy**: indicates that SNMP messages are authenticated and encrypted.	For security purposes, it is recommended that you set the security level of the SNMP group to **privacy**.
read-view *read-view*	Specifies a read-only view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *read-view* specified by the **snmp-agent mib-view** command.
write-view *write-view*	Specifies a read-write view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *write-view* is specified by the **snmp-agent mib-view** command.
notify-view *notify-view*	Specifies a notify view.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. *notify-view* is specified by the **snmp-agent mib-view** command.
acl *acl-number*	Specifies a basic ACL.	The value is an integer that ranges from 2000 to 2999.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

SNMPv1 and SNMPv2c have serious defects in terms of security. The security authentication mechanism used by SNMPv1 and SNMPv2c is based on the community name. In this mechanism, the community name is transmitted in plain text. You are not advised to use SNMPv1 and SNMPv2c on untrusted networks.

By adopting the user-based security model, SNMPv3 eradicates the security defects in SNMPv1 and SNMPv2c and provides two services, authentication and privacy. The SNMP group name and security name determine an SNMP group. SNMPv3 defines the following security levels:

- noAuthNoPriv
- AuthNoPriv
- AuthPriv

NOTE

The security authentication level noAuthPriv does not exist. This is because the generation of a key is based on the authentication information and product information.

The **snmp-agent group** command can be used to configure the following:

- Authentication
- Privacy
- Access rights for users of SNMP group
- Bind the SNMP group to a MIB view

Parameters are selected based on the following rules:

- To enhance security, configure the parameter **authentication** or **privacy**.
  - If neither **authentication** nor **privacy** are configured, SNMP messages are not authenticated or encrypted. This applies to the environment that is secure and has a fixed administrator.
  - To authenticate SNMP messages without encryption, configure the parameter **authentication**. This mode is applicable to secure networks managed by many administrators who may frequently perform operations on the same device. Authentication allows only the administrators with permission to access the device.
  - To authenticate and encrypt SNMP messages, configure the parameter **privacy**. This mode is applicable to insecure networks managed by many administrators who may frequently perform operations on the same device. Authentication and encryption allow only specified administrators to access the device and encrypts data before the transmission. This prevents data from being tampered or leaked.

 Copyright © Huawei Technologies Co., Ltd.

- To grant the NMS read-only permission in the specified view, configure **read-view**. To grant the NMS read-write permission in the specified view, configure **write-view**.

  To filter unnecessary alarms, configure **notify-view**. After this parameter is configured, only alarms generated on MIB objects specified by **notify-view** are delivered to the NMS.

  By default, the read-only view of an SNMP group is the ViewDefault view, and the names of the read-write view and inform view are not specified.
- To allow specified NMSs in the same SNMPv3 group to access the device, configure **acl**.

Configuration Impact

When you run the **undo snmp-agent group** command to delete an SNMP user group, you delete all SNMP users in the SNMP user group.

Precautions

To receive trap messages specified in *notify-view*, you need to ensure the target host for receiving SNMP traps is specified through the **snmp-agent target-host trap-hostname** command.

User access can be encrypted and authenticated, authenticated but not encrypted, or neither authenticated nor encrypted. If the access level of a user is lower than the security level of the specified group, the access fails. When the groups that a user can access have multiple security levels, the user can select the group with the highest security level among the groups that can be accessed, and access the view of the group.

Example

Create an SNMPv3 group named **Johngroup**, authenticate and encrypt SNMP messages, and configure the view that the SNMPv3 group can read only to public.

```
<Huawei> system-view
[Huawei] snmp-agent
[Huawei] snmp-agent mib-view excluded public 1.3.6.1.2.1
[Huawei] snmp-agent group v3 Johngroup privacy read-view public
```

Create an SNMPv3 group named **Johngroup**, authenticate and encrypt SNMP messages, and configure the view that the SNMPv3 group write-view to private.

```
<Huawei> system-view
[Huawei] snmp-agent
[Huawei] snmp-agent mib-view included private 1.3.6.1.2.1
[Huawei] snmp-agent group v3 Johngroup privacy write-view private
```

Related Topics

21.1.23 snmp-agent mib-view

21.1.37 snmp-agent usm-user

21.1.3 display snmp-agent group

 Copyright © Huawei Technologies Co., Ltd.

21.1.22 snmp-agent local-engineid

Function

The **snmp-agent local-engineid** command sets an engine ID for the local SNMP agent.

The **undo snmp-agent local-engineid** command restores the engine ID of the local SNMP agent to the default value.

By default, the device uses an internal algorithm to automatically generate an engine ID for a device. The engine ID consists of the enterprise number and the device information.

Format

snmp-agent local-engineid { *engineid* | **sysname** }

undo snmp-agent local-engineid

Parameters

Parameter	Description	Value
engineid	Specifies the engine ID of the local SNMP agent.	The value is string of 10 to 64 hexadecimal digits.
sysname	Indicates the engine ID generated based on the system name.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **snmp-agent local-engineid** command to set an engine ID for the local SNMP agent for identification.

The SNMP engine ID uniquely identifies an SNMP agent in a management domain. The SNMP engine ID is an important component of the SNMP agent. It schedules and processes SNMP messages, and implements security authentication and access control. You can use the **display snmp-agent local-engineid** command to check the engine ID of the local SNMP entity.

When setting an engine ID, you need to comply with the following rules:

- The length of the octet strings varies. The first four octets are set to the binary equivalent of the agent, which is SNMP management private

 Copyright © Huawei Technologies Co., Ltd.

enterprise number and is assigned by the Internet Assigned Numbers Authority (IANA). The engine ID of Huawei devices is 2011 in decimal notation. The first digit is in binary format, and has a fixed value 1. Therefore, the engine ID in hexadecimal format is 800007DB.

- The device information can be configured manually. It is recommended that the IP address or MAC address of the device be used as the device information to uniquely identify the device.

Precautions

If the local engine ID is set or changed, the existing SNMPv3 user with this engine ID is deleted. If the original engine ID is restored, the corresponding user configuration is restored.

After the SNMP agent function is enabled using the **snmp-agent** command, the system automatically adopts the default engine ID for the local SNMP agent.

The password summary used by SNMPv3 users is calculated using MD5 or SHA based on the user password and engine ID of the local SNMP agent. If the engine ID of the local SNMP agent is changed, the generated password summary becomes invalid. As a result, a new password summary needs to be generated for SNMPv3 users.

Example

Set the engine ID of the local SNMP agent to 800007DB03360102101100.

```
<Huawei> system-view
[Huawei] snmp-agent local-engineid 800007DB03360102101100
Info: Modify the local-engineid will disable the configured SNMPv3 user, all
users must be reconfigured, proceed? (y/n)[n]:y
```

Related Topics

21.1.4 display snmp-agent local-engineid

21.1.37 snmp-agent usm-user

21.1.23 snmp-agent mib-view

Function

The **snmp-agent mib-view** command creates or updates a MIB view.

The **undo snmp-agent mib-view** command cancels the configuration of the current MIB view.

By default, the MIB view name is ViewDefault, and the MIB subtree includes lagMIB nodes and all internet subnodes except for snmpVacmMIB and snmpUsmMIB.

Format

snmp-agent mib-view *view-name* { **exclude** | **include** } *subtree-name* [**mask** *mask*]

undo snmp-agent mib-view *view-name* [*subtree-name*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
view-name	Specifies the MIB view name.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
exclude	Excludes the MIB subtree.	-
include	Includes the MIB subtree.	-
subtree-name	Specifies the name of the subtree, which identifies a subtree uniquely. *subtree-name* can be the OID (such as 1.4.5.3.1) or the name (such as system) of the subtree.	It is a string of 1 to 128 characters, which are case sensitive and cannot be blank spaces. **NOTE** It must be a valid MIB subtree.
mask	Indicates the subtree mask, which specifies the access range of the view.	-
mask	Specifies the value of the subtree mask. This parameter specifies the mode and length of the matching between the user operation node and the subtree included by the view.	The value is a hexadecimal string of 1 to 32 characters.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

A MIB view is an abstract set of all managed objects. The NMS manages the device by reading and writing the managed objects in the MIB. A MIB view defines management information included and excluded in this MIB view.

If you forget which information you have configured for a MIB view, you can run the **display snmp-agent mib-view** command to check it.

Precautions

If both the **include** and **exclude** parameters are configured for MIB objects that have an inclusion relationship, whether to include or exclude the lowest MIB

 Copyright © Huawei Technologies Co., Ltd.

object will be determined by the parameter configured for the lowest MIB object. For example, the snmpV2, snmpModules, and snmpUsmMIB objects are from top down in the MIB table. If the **exclude** parameter is configured for snmpUsmMIB objects and **include** is configured for snmpV2, snmpUsmMIB objects will still be excluded.

When using the **snmp-agent mib-view** command, note the following:

- A view name uniquely identifies a view. Configuring the same view name repeatedly is equivalent to adding the subtree to the view. The system displays prompt information when a subtree is overwritten due to the repeated subtree configuration. The default view cannot be deleted.
- The system checks the subtree name. The configured subtree must be the one existing in the MIB tree. The subtree name is configurable.
- The rule of smallest range is adopted for the access rights of the leaf node. That is, the MIB subtree configured with the include/exclude rights at the most internal layer determines the authority of the leaves inside the subtree.
- Only an existing view can be deleted regardless of whether the view is referenced or not.
- The total number of subtrees in all views cannot exceed 20.
- A leaf node of the MIB tree defines the managed object of the device, such as the routing table. The leaf node with a unique value is called a scalar, and the leaf node with multiple values is called a variable.
- To set the security level to privacy or authentication, you must run the **snmp-agent mib-view** *view-name* **include** *subtree-name* command to configure the MIB view information and the included MIB subtree.

An input mask must meet the following requirements:

- The mask is a hexadecimal string.
- The bit converted to 1 (a binary number) indicates that the subtree matches the corresponding sub IDs exactly. The bit converted to 0 (a binary number) indicates that the subtree matches the sub IDs universally.
- After the mask is converted to a binary string, the length of the string should not less than the number of the sub IDs of the subtree. In addition, 0 must exist before 1.
- A view record without a mask indicates that the view matches the subtrees completely.

Example

Configure MIB view **a1** that includes the internet subtree.

```
<Huawei> system-view
[Huawei] snmp-agent mib-view a1 include internet
```

Related Topics

21.1.5 display snmp-agent mib-view

21.1.17 snmp-agent community

21.1.21 snmp-agent group

 Copyright © Huawei Technologies Co., Ltd.

21.1.24 snmp-agent notify-filter-profile

Function

The **snmp-agent notify-filter-profile** command creates or updates a trap filter profile.

The **undo snmp-agent notify-filter-profile** command deletes a trap filter profile.

By default, no trap is filtered.

Format

snmp-agent notify-filter-profile { **include** | **exclude** } *profile-name oid-tree*

undo snmp-agent notify-filter-profile *profile-name* [*oid-tree*]

Parameters

Parameter	Description	Value
include	Includes the specified MIB subtree. **NOTE** The **include** parameter is configured to filter traps of a certain type that are sent to the destination host. In addition to configuring the trap object, you need to configure all the objects of the parameter bound to the trap object.	-
exclude	Excludes the specified MIB subtree. **NOTE** The **exclude** parameter is configured to filter traps of a certain type that are not sent to the destination host.	-
profile-name	Specifies the name of a trap filter profile.	The value is a string of 1 to 32 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
oid-tree	Specifies the OID for the MIB subtree. *oid-tree* can be the OID (such as 1.4.5.3.1) or the name (such as system) of the subtree.	The value is a string of 1 to 128 case-sensitive characters without spaces. **NOTE** It must be a valid MIB subtree.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

To filter the traps sent to a destination host, run the **snmp-agent notify-filter-profile** command to configure a trap filter profile and specify the MIB object to be filtered in the profile.

Before sending a trap message to a target host, the device checks whether the alarm object and parameter binding object are within the filtering range of the target host. If this trap is within the filtering range, the device does not send the trap message; otherwise, the device sends the trap message.

NOTE

If no trap filter profile is configured, all traps are sent to the destination host.

Example

Configure a trap filter profile named **tmp**.

```
<Huawei> system-view
[Huawei] snmp-agent notify-filter-profile include tmp linkDown
```

Related Topics

21.1.6 display snmp-agent notify-filter-profile

21.1.25 snmp-agent permit interface

Function

The **snmp-agent permit interface** command specifies physical interfaces on the device to which the NMS can connect.

The **undo snmp-agent permit interface** command restores the default physical interfaces on the device to which the NMS can connect.

By default, the NMS can connect to all the physical interfaces on the device.

Format

snmp-agent permit interface { *interface-type interface-number* } &<1-5>

undo snmp-agent permit interface

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type*: specifies the interface type. *interface-number*: specifies the interface number. *interface-number* and *interface-type* specify an interface.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent the NMS from connecting to the device through an unauthorized physical interface, you can run the **snmp-agent permit interface** command to specify physical interfaces on the device to which the NMS can connect.

Precautions

- By default, the NMS can connect to all the physical interfaces on the device. When you run this command to specify one physical interface on the device, the NMS cannot connect to the other physical interfaces on the device.
- You can specify a maximum of five interfaces each time you run the **snmp-agent permit interface** command. The latest configuration overrides the previous one. For example, before you run the command, the NMS can connect to three physical interfaces GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 on the device. After you run the command to specify the interface GigabitEthernet 1/0/0, the NMS can only connect to the interface GigabitEthernet 1/0/0.

Example

Specify physical interfaces on the device to which the NMS can connect.

```
<Huawei> system-view
[Huawei] snmp-agent permit interface gigabitethernet 1/0/0 gigabitethernet 2/0/0
  Info: Succeeded in setting snmp permit interface.
```

Restore the default physical interfaces on the device to which the NMS can connect.

```
<Huawei> system-view
[Huawei] undo snmp-agent permit interface
```

 Copyright © Huawei Technologies Co., Ltd.

21.1.26 snmp-agent sys-info

Function

The **snmp-agent sys-info** command sets the SNMP system information.

The **undo snmp-agent sys-info** command restores the default setting.

By default, the system maintenance information is " R&D Shenzhen, Huawei Technologies Co.,Ltd.": the system location is Shenzhen China" and the version is SNMPv3.

Format

snmp-agent sys-info { **contact** *contact* | **location** *location* | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

undo snmp-agent sys-info { **contact** | **location** | **version** { { **v1** | **v2c** | **v3** } * | **all** } }

Parameters

Parameter	Description	Value
contact *contact*	Indicates contact information of system maintenance.	The value is a string of 1 to 225 case-sensitive characters that can contain spaces.
location *location*	Indicates the location of a device.	The value is a string of 1 to 255 case-sensitive characters that can contain spaces.
version { { **v1** | **v2c** | **v3** } * | **all** }	Indicates the SNMP version. ● **v1**: SNMPv1 is enabled. ● **v2c**: SNMPv2c is enabled. ● **v3**: SNMPv3 is enabled. ● **all**: SNMPv1, SNMPv2c, and SNMPv3 are enabled.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

To configure the contact information for the managed node, you can run the **snmp-agent sys-info contact** command in the system. If a device fails, maintenance personnel can contact the vendor for device maintenance.

To configure the physical location of the node, you can run the **snmp-agent sys-info location** command in the system.

To configure features in a specified version, you can run the **snmp-agent sys-info version** command to set the corresponding SNMP version in the system. SNMPv1 or SNMPv2c is not secure enough. Using SNMPv3 is recommended.

SNMPv1:

- Community-name-based access control
- MIB-view-based access control

SNMPv2c:

- Community-name-based access control
- MIB-view-based access control

Besides inheriting basic SNMPv2c operations, SNMPv3 defines a management architecture, which introduces a User-based Security Model (USM) to provide users with a more secure access mechanism.

- User group
- Group-based access control
- User-based access control
- Authentication and encryption mechanisms

NOTE

Use **display snmp-agent sys-info** command to view the information of the system maintenance, the physical location of the node and the SNMP version.

Precautions

A lack of authentication capabilities in SNMPv1 and SNMPv2c results in vulnerability to security threats, so SNMPv3 is recommended.

Example

Set the contact information of the system maintenance as "call Operator at 010-12345678".

```
<Huawei> system-view
[Huawei] snmp-agent sys-info contact call Operator at 010-12345678
```

Set the location of a device as "shanghai China".

```
<Huawei> system-view
[Huawei] snmp-agent sys-info location shanghai China
```

Set the current SNMP version used by the system to SNMPv2c.

```
<Huawei> system-view
[Huawei] snmp-agent sys-info version v2c
```

Related Topics

21.1.8 display snmp-agent sys-info

 Copyright © Huawei Technologies Co., Ltd.

21.1.27 snmp-agent target-host trap-hostname

Function

The **snmp-agent target-host trap-hostname** configures the target host of trap messages.

The **undo snmp-agent target-host trap-hostname** deletes the target host of trap messages.

By default, no target host of trap messages is configured.

Format

snmp-agent target-host trap-hostname *hostname* **address** { *ipv4-addr* [**udp-port** *udp-portid*] [**public-net** | **vpn-instance** *vpn-instance-name*] | **ipv6** *ipv6-addr* [**udp-port** *udp-portid*] } **trap-paramsname** *paramsname* [**notify-filter-profile** *profile-name*]

undo snmp-agent target-host trap-hostname *hostname*

Parameters

Parameter	Description	Value
hostname	Specifies the name of the target host.	The name a string of 1 to 32 case-sensitive characters without spaces.
address *ipv4-addr*	Indicates the IP address of the target host.	The value is in dotted decimal notation.
udp-port *udp-portid*	Indicates the ID of the port on the target host for receiving trap messages.	The value is an integer that ranges from 1 to 65535. The default value is 162.
public-net	Indicates that the target host connects the alarm host on the public network.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Indicates the name of a VPN instance.	The name a string of 1 to 31 case-sensitive characters without spaces.
ipv6-address *ipv6-address*	Specifies the IPv6 address of the target host.	The value is a hexadecimal number that ranges from 0 to FFFF (0::0 to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, "::" indicates that the value of the field between the two colons is 0).
udp-port *udp-portid*	Indicates that the target host receives port numbers of trap messages.	The value is an integer that ranges from 1 to 65535.
trap-paramsname *paramsname*	Indicates the name of the trap sending parameter list used by the target host.	The name a string of 1 to 32 case-sensitive characters without spaces.
notify-filter-profile *profile-name*	Specifies the name of a trap filter profile.	The name a string of 1 to 32 case-sensitive characters without spaces.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Only the terminal configured as the target host of trap messages can receive traps. The NMS is generally configured as the target host of trap messages. Currently, the system supports a maximum of 20 target hosts.

Example

Set the IP address of the target host to 10.1.1.1, the host name to aaa, and the trap sending parameter list name to abc.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] snmp-agent target-host trap-hostname aaa address 10.1.1.1 trap-paramsnam abc
```

21.1.28 snmp-agent target-host trap-paramsname

Function

The **snmp-agent target-host trap-paramsname** command configures parameters for sending trap messages. The trap sending parameter list is composed of these parameters.

The **undo snmp-agent target-host trap-paramsname** command deletes a trap sending parameter list.

Format

snmp-agent target-host trap-paramsname *paramsname* { { **v1** | **v2c** } **securityname** *securityname* | **v3 securityname** *securityname* { **authentication** | **noauthnopriv** | **privacy** } } [**binding-private-value**] [**private-netmanager**]

undo snmp-agent target-host trap-paramsname *paramsname*

Parameters

Parameter	Description	Value
paramsname	Specifies the name of a trap sending parameter list.	The value is a string of 1 to 32 characters.
v1	Indicates SNMPv1. This parameter specifies SNMPv1 as the trap message sending protocol.	-
v2c	Indicates SNMPv2c. This parameter specifies SNMPv2c as the trap message sending protocol.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
v3	Indicates SNMPv3. SNMPv3 protocol contains the basic functions of SNMPv1 and SNMPv2 and defines a series of management functions for network security and access control. This parameter specifies SNMPv3 as the trap message sending protocol.	-
securityname *securityname*	Indicates the host name in the trap message. When the trap sending protocol is the SNMPv3 protocol, this parameter is the user name in the SNMPv3 group.	The value is a string. The string length range is ● 1 to 32 characters in plain text. ● 48 to 68 characters in cipher text.
authentication	Authenticates but not encrypts trap messages. When the trap sending protocol is SNMPv3, this parameter can authenticate (the receiver) but not encrypt (the sender) trap messages.	-
noauthnopriv	Authenticates and encrypts no trap message. When the trap sending protocol is SNMPv3, this parameter is used as if no trap message needs to be authenticated (the receiver) or encrypted (the sender).	-
privacy	Authenticates and encrypts trap messages. When the trap sending protocol is SNMPv3, this parameter can authenticate (the receiver) and encrypt (the sender) trap messages.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
binding-private-value	Indicates that trap messages sent to a target host carry extended bound variables. If alarm objects defined in public MIBs are extended on a Huawei data communication device, you can use the **binding-private-value** parameter to determine whether the corresponding trap messages sent from the device to an NMS carry extended bound variables. ● If the **binding-private-value** parameter is not specified, the trap message does not carry extended bound variables. The **binding-private-value** parameter is not recommended when the NMS is a third-party NMS. This ensures that the third-party NMS can receive trap messages from Huawei data communication devices. By default, a trap message sent from a Huawei data communication device does not carry extended bound variables. ● If the **binding-private-value** parameter is specified, the trap message carries extended bound variables. The **binding-private-value** parameter is recommended when the NMS is a Huawei NMS. This allows more abundant information in trap messages.	-
private-netmanager	# Configure the Huawei NMS as the target host to receive trap messages. After the Huawei NMS is used, the alarm message sent to the Huawei NMS can contain more detailed information, such as the alarm type, alarm ID, and send time of the alarm message.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Currently, the system supports a maximum of 20 trap sending parameter lists.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the trap sending parameter list: set the list name to aaa, set SNMPv3 as the trap sending protocol, set the host name in the SNMP trap as bbb, and authenticate but do not encrypt the trap messages.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] snmp-agent target-host trap-paramsname aaa v3 securityname bbb authentication
```

Related Topics

21.1.9 display snmp-agent target-host
21.1.27 snmp-agent target-host trap-hostname

21.1.29 snmp-agent trap disable

Function

The **snmp-agent trap disable** command disables the trap function for all features.

The **undo snmp-agent trap disable** command restores the trap function for all features to the default status.

By default, the **display snmp-agent trap all** command can be used to view the status of the trap function for all features.

Format

snmp-agent trap disable

undo snmp-agent trap disable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for all modules, run the **snmp-agent trap enable** command. To enable the trap function for a specified module, run the **snmp-agent trap enable feature-name** command.

- To disable the trap function for all modules, run the **snmp-agent trap disable** command.
- To restore the trap function for all features to the default status, run the **undo snmp-agent trap disable** or **undo snmp-agent trap enable** command.

 Copyright © Huawei Technologies Co., Ltd.

NOTE

To disable the trap function for a specified module, run the **undo snmp-agent trap enable feature-name** command.

Example

Disable the trap function for all features.

```
<Huawei> system-view
[Huawei] snmp-agent trap disable
```

Related Topics

21.1.10 display snmp-agent trap all

21.1.30 snmp-agent trap enable

Function

The **snmp-agent trap enable** command enables the router to send traps.

The **undo snmp-agent trap enable** command restores the default setting.

The default configuration of the **snmp-agent trap enable** command can be checked by the **display snmp-agent trap all** command.

Format

snmp-agent trap enable

undo snmp-agent trap enable

Parameters

None.

Views

System view

Default Level

3: Management level

Usage Guidelines

To enable the trap function for all modules, run the **snmp-agent trap enable** command.

Example

Enable the router to send traps.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable
```


Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.10 display snmp-agent trap all

21.1.31 snmp-agent trap enable feature-name

Function

The **snmp-agent trap enable feature-name** command enables a specified trap for a specified feature.

The **undo snmp-agent trap enable feature-name** command disables a specified trap for a specified feature.

The default configuration of the **snmp-agent trap enable feature-name** command can be checked using the **display snmp-agent trap all** command.

Format

snmp-agent trap enable feature-name *feature-name* [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name *feature-name* [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
feature-name	Specifies the name of the feature that generates traps.	-
trap-name *trap-name*	Specifies the name of a trap.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

If **trap-name** *trap-name* is not specified, the router enables all traps about a specified feature after the **snmp-agent trap enable feature-name** *feature-name* command is used.

You can run the **display snmp-agent trap all** command to check the configuration result.

Example

Enable the router to send the vrrptrapauthfailure trap about VRRP to the NMS.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name vrrp trap-name vrrptrapauthfailure
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.10 display snmp-agent trap all

21.1.32 snmp-agent trap enable feature-name snmp

Function

The **snmp-agent trap enable feature-name snmp** command enables an SNMP trap.

The **undo snmp-agent trap enable feature-name snmp** command disables an SNMP trap.

By default, the coldStart and warmStart traps are enabled and the authenticationFailure trap is disabled.

Format

snmp-agent trap enable feature-name snmp [**trap-name** *trap-name*]

undo snmp-agent trap enable feature-name snmp [**trap-name** *trap-name*]

Parameters

Parameter	Description	Value
trap-name *trap-name*	Specifies the name of a trap.	The traps are as follows: ● authenticationFailure ● coldstart ● warmstart

Views

System view

Default Level

3: Management level

Usage Guidelines

The **snmp-agent trap enable feature-name snmp** command is used to enable an SNMP trap. After that, the trap generated during the device running will be sent to the NMS. At present, the following SNMP traps are supported:

- coldStart: This trap is generated when the device is powered off and restarted.
- warmStart: This trap is generated when the status of SNMP agent is changed from disable to enable.
- authenticationFailure: This trap is generated when a user uses an incorrect community name and is unable to log in to the device.

 Copyright © Huawei Technologies Co., Ltd.

You can run the **display snmp-agent trap feature-name snmp all** command to check the configuration result.

Example

Enable the SNMP authenticationFailure trap.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name snmp trap-name authenticationFailure
```

Related Topics

21.1.11 display snmp-agent trap feature-name snmp all

21.1.33 snmp-agent trap enable syslog

Function

The **snmp-agent trap enable syslog** command enables the function of converting logs to trap messages when syslog is triggered.

The **undo snmp-agent trap enable syslog** command disables the function of converting logs to trap messages when syslog is triggered.

By default, the function of converting logs to trap messages is disabled when syslog is triggered.

Format

snmp-agent trap enable syslog

undo snmp-agent trap enable syslog

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To enable the function of converting logs to trap messages when syslog is triggered, run the **snmp-agent trap enable syslog** command.

Precautions

To make the command take effect, you need to run the **snmp-agent trap enable** command to enable the router to send trap packets.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the function of converting logs to trap messages when syslog is triggered.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable syslog
```

Related Topics

21.1.30 snmp-agent trap enable

21.1.34 snmp-agent trap life

Function

The **snmp-agent trap life** command sets the lifetime of trap messages. When the lifetime expires, the trap messages are discarded.

The **undo snmp-agent trap life** command cancels the current settings.

By default, the lifetime of trap messages is 120 seconds.

Format

snmp-agent trap life *seconds*

undo snmp-agent trap life

Parameters

Parameter	Description	Value
seconds	Specifies the lifetime of trap messages.	The value is an integer that ranges from 1 to 2592000, in seconds. The default value is 120.

Views

System view

Default Level

3: Management level

Usage Guidelines

When the lifetime expires, the trap messages are discarded.

Example

Set the lifetime of trap messages to 60 seconds.

```
<Huawei> system-view
[Huawei] snmp-agent trap life 60
```


Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.30 snmp-agent trap enable

21.1.35 snmp-agent trap queue-size

Function

The **snmp-agent trap queue-size** command sets the queue length of the trap messages sent to a target host.

The **undo snmp-agent trap queue-size** command cancels the current settings.

The default value is 100.

Format

snmp-agent trap queue-size *size*

undo snmp-agent trap queue-size

Parameters

Parameter	Description	Value
size	Specifies the queue length of trap messages.	The value is an integer that ranges from 1 to 1000. The default value is 100.

Views

System view

Default Level

3: Management level

Usage Guidelines

When a large number of trap messages need to be sent in a certain period of time, packets will be lost if the queue length of trap messages is insufficient. The queue length can be adjusted to reduce the packet loss ratio.

When the lifetime of trap messages is long, the queue length of trap messages needs to be lengthened. If the queue length is not lengthened, packet loss will occur.

Example

Set the queue length of the trap messages sent to the target host to 200.

```
<Huawei> system-view
[Huawei] snmp-agent trap queue-size 200
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.30 snmp-agent trap enable
21.1.34 snmp-agent trap life

21.1.36 snmp-agent trap source

Function

The **snmp-agent trap source** command sets the source interface from which traps are sent.

The **undo snmp-agent trap source** command removes the set source interface configuration.

By default, source interface is not set.

Format

snmp-agent trap source *interface-type interface-number*

undo snmp-agent trap source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface that sends traps.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **snmp-agent trap source** command to specify the type and number of the interface on the device from which traps are sent. The system specifies the IP address of this interface as the source IP address of traps. In this way, the trap source can be identified on the NMS.

Precautions

The source interface that sends traps must have an IP address; otherwise, the commands will fail to take effect. To ensure device security, it is recommended that you set the source IP address to the local loopback address.

 Copyright © Huawei Technologies Co., Ltd.

The source interface in traps on the device must be the same as the source interface specified on the NM station. Otherwise, the NM station cannot receive traps.

Example

Specify the IP address of GE1/0/0 as the source address of traps.

```
<Huawei> system-view
[Huawei] snmp-agent trap source gigabitethernet 1/0/0
```

Related Topics

21.1.30 snmp-agent trap enable

21.1.37 snmp-agent usm-user

Function

The **snmp-agent usm-user** command adds a user to an SNMP user group.

The **undo snmp-agent usm-user** command deletes a user from an SNMP user group.

By default, the SNMP user group has no users added.

Format

snmp-agent usm-user v3 *user-name* [**group** *group-name* | **acl** *acl-number*] *

snmp-agent usm-user v3 *user-name* **authentication-mode** { **md5** | **sha** }

snmp-agent usm-user v3 *user-name* **privacy-mode** { **aes128** | **des56** }

undo snmp-agent usm-user v3 *user-name* [**acl** | **authentication-mode** | **group** | **privacy-mode**]

Parameters

Parameter	Description	Value
v3	Indicates that the SNMP user group uses the SNMPv3 security mode.	-
user-name	Specifies a user name.	The value is a string of 1 to 32 case-sensitive characters without spaces.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
group *group-name*	Specifies the name of the SNMP group that the user belongs to.	The value is a string of 1 to 32 case-sensitive characters without spaces.
authentication-mode	Sets the authentication mode. **NOTE** Authentication is a process in which the SNMP agent (or the NMS) confirms that the message is received from an authorized NMS (or SNMP agent) and the message is not changed during transmission. RFC 2104 defines Keyed-Hashing for Message Authentication Code (HMAC), an effective tool that uses the security hash function and key to generate the message authentication code. This tool is widely used in the Internet. HMAC used in SNMP includes HMAC-MD5-96 and HMAC-SHA-96. The hash function of HMAC-MD5-96 is MD5 that uses 128-bit authKey to generate the key. The hash function of HMAC-SHA-96 is SHA-1 that uses 160-bit authKey to generate the key.	-
md5	Uses the HMAC MD5 algorithm for user authentication. Two communication parties share a private key. The sending party uses this key to create a message authentication code (MAC), and the receiving party uses this key to calculate the MAC. If the calculated MAC matches the MAC created by the sending party, the authentication succeeds.	-
sha	Uses the HMAC SHA algorithm for user authentication. The working principle of the HMAC SHA algorithm is similar to that of the HMAC MD5 algorithm. The only difference lies in the methods for generating the MAC. **NOTE** The calculation speed of the HMAC-MD5-96 algorithm is faster than that of the HMAC-SHA-96 algorithm; the HMAC-SHA-96 algorithm is more secure than the HMAC-MD5-96 algorithm. To ensure high security, please use the HMAC-SHA-96 algorithm.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
privacy-mode	Specifies the authentication with encryption. The system adopts the cipher block chaining (CBC) code of the data encryption standard (DES) and uses 128-bit privKey to generate the key. The NMS uses the key to calculate the CBC code and then adds the CBC code to the message while the SNMP agent fetches the authentication code through the same key and then obtains the actual information. Like the identification authentication, the encryption requires the NMS and the SNMP agent to share the same key to encrypt and decrypt the message.	-
aes128	The 128-bit AES encryption algorithm is used to encrypt the PDU of packets. Each user has a key and uses this key to encrypt data using the AES algorithm and sends the encrypted data together with user information to the receiving party. After receiving the data, the receiving party obtains the key from the user information, and calculates the encrypted data based on the AES algorithm to obtain the plain text.	-
des56	The 56-bit DES encryption algorithm is used to encrypt the PDU of packets. Each user has a key and uses this key to encrypt data using the DES algorithm and sends the encrypted data together with user information to the receiving party. After receiving the data, the receiving party obtains the key from the user information, and calculates the encrypted data based on the DES algorithm to obtain the plain text.	-
acl *acl-number*	Specifies the ACL number.	The value is an integer that ranges from 2000 to 2999.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

SNMPv1 and SNMPv2c have serious defects in terms of security. The security authentication mechanism used by SNMPv1 and SNMPv2c is based on the community name. In this mechanism, the community name is transmitted in plain text. You are not advised to use SNMPv1 and SNMPv2c on untrusted networks.

By adopting the user-based security model, SNMPv3 eradicates the security defects in SNMPv1 and SNMPv2c and provides two services, authentication and encryption. The user-based security model defines three security authentication levels: noAuthNoPriv, AuthNoPriv, and AuthPriv.

NOTE

The security authentication level noAuthPriv does not exist. This is because the generation of a key is based on the authentication information and product information.

Different from SNMPv1 and SNMPv2c, SNMPv3 can implement access control, identity authentication, and data encryption through the local processing model and user security model. SNMPv3 can provide higher security and confidentiality than SNMPv1 and SNMPv2c. The following table lists the difference between SNMPv1, SNMPv2c, and SNMPv3:

Table 21-14 Comparison in the security of SNMP of different versions

Protocol version	User Checksum	Encryption	Authentication
v1	Adopts the community name.	None	None
v2c	Adopts the community name.	None	None
v3	Adopts user name-based encryption/ decryption.	Yes	Yes

The **snmp-agent group** command can be used to configure the authentication, encryption, and access rights for an SNMP group. The **snmp-agent group** command can be used to configure the rights for users in a specified SNMP group and bind the SNMP group to a MIB view. The MIB view is created through the **snmp-agent mib-view** command. For details, see the usage guideline of this command. After an SNMP user group is configured, the MIB-view-based access control is configured for the SNMP user group. Users cannot access objects in the MIB view through the SNMP user group. The purpose of adding SNMP users to an SNMP user group is to ensure that SNMP users in an SNMP user group have the same security level and access control list. When you run the **snmp-agent usm-user** command to configure a user in an SNMP user group, you configure the MIB-view-based access rights for the user. If an SNMP user group is configured with the AuthPriv access rights, you can configure the authentication mode and encryption mode when configuring SNMP users. Note that the authentication keys

 Copyright © Huawei Technologies Co., Ltd.

and encryption passwords configured on the NMS and the SNMP agent should be the same; otherwise, authentication fails.

When the NMS and device are in an insecure network environment, for example, a network prone to attacks, it is recommended that you configure different authentication password and encryption password to improve security.

Configuration Impact

If an SNMP agent is configured with a remote user, the engine ID is required during the authentication. If the engine ID changes after the remote user is configured, the remote user becomes invalid.

Precautions

The user security level must be higher than or equal to the security level of the SNMP user group to which the user is added.

The security level of an SNMP user group can be (in descending order):

- Level 1: privacy (authentication and encryption)
- Level 2: authentication (without encryption)
- Level 3: none (neither authentication nor encryption)

The user security level must be higher than the user group level. For example, if the security level of an SNMP user group is level 1, the security level of the user that is added to the group must be level 1; if the security level of an SNMP user group is level 2, the security level of the user that is added to the group can be level 1 or level 2.

To add an SNMP user to an SNMP group, ensure that the SNMP user group is valid.

If you run the **snmp-agent usm-user** command multiple times, only the latest configuration takes effect.

Keep your user name and plain-text password well when creating the user. The plain-text password is required when the NMS accesses the device.

Note that MD5 and DES56 encryption algorithm cannot ensure security. SHA and AES128 encryption algorithm is recommended.

Example

Configure an SNMPv3 user with user name **u1**, group name **g1**, authentication mode **SHA**, authentication password **8937561bc**, encryption mode **AES128**, and encryption password **68283asd**

```
<Huawei> system-view
[Huawei] snmp-agent usm-user v3 u1 group g1
[Huawei] snmp-agent usm-user v3 u1 authentication-mode sha
Please configure the authentication password (<8-64>)
Enter Password:
Confirm Password:
[Huawei] snmp-agent usm-user v3 u1 privacy-mode aes128
Please configure the privacy password (<8-64>)
Enter Password:
Confirm Password:
[Huawei]
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.1.21 snmp-agent group

21.1.38 snmp-agent source loopback

Function

The **snmp-agent source loopback** command configures a Loopback interface as the source interface for sending packets.

The **undo snmp-agent source** command restores the default source interface for sending packets.

By default, the source interface for sending packets is a physical outbound interface.

Format

snmp-agent source loopback *loopback-number*

undo snmp-agent source

Parameters

Parameter	Description	Value
loopback-number	Specifies the number of a Loopback interface.	The value is an integer, and the value range varies depending on the device model.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the NMS sends a get operation request to the device, the device replies with a response packet. The response packet carries source interface information. The device uses the IP address of this interface as the source address of packets. When an ACL is configured on the NMS to filter the packets sent from the device, the ACL rules vary according to source interface IP addresses, and communication may be affected by interface status. After a Loopback interface is configured as the source interface for response packets using the **snmp-agent source loopback** command, the impact of source address difference and interface status can be avoided by specifying the source address in an ACL rule as this Loopback interface address. This configuration allows the device to filter outgoing packets and protect security. In addition, the configurations of ACL rules and security policies are simplified.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

Loopback interface that will be configured as the source interface must exist on the device and has an IPv6 address. Otherwise, command execution will fail.

Example

Set Loopback0 as the source interface for sending packets.

```
<Huawei> system-view
[Huawei] snmp-agent source loopback 0
```

21.1.39 snmp-agent server-source

Function

The **snmp-agent server-source** command sets the source IP address used by an SNMP server to send packets.

The **undo snmp-agent server-source** command restores the default source IP address used by an SNMP server to send packets.

By default, the SNMP server uses source IP address 0.0.0.0 to send packets.

Format

snmp-agent server-source { **-a** [**ipv6**] *source-ip-address* | **-i** [**ipv6**] *interface-type interface-number* }

undo snmp-agent [**ipv6**] **server-source**

Parameters

Parameter	Description	Value
ipv6	Specifies that the source IP address used by an SNMP server to send packets is an IPv6 address.	-
-a *source-ip-address*	Specifies the source IP address on the local device. A loopback interface address is recommended.	-
-i *interface-type interface-number*	Sets the loopback interface on the local device as the source interface. If no loopback interface exists on the device or the loopback interface does not have an IP address, the command fails.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the default source IP address 0.0.0.0 is not changed, the device selects a source IP address according to routing entries to send packets. When an ACL is configured to filter incoming and outgoing packets on a device, the ACL rules are configured based on interface IP addresses, and packet filtering is affected by interface status. You can select a stable interface as the source interface, for example, the loopback interface. Setting the source or destination address in an ACL rule as a stable interface's address can simplify the configurations of ACL rules and security policies. In addition, packet filtering will not be affected by interface IP addresses and interface status, and device security is improved.

Precautions

- After the source IP address is specified for the SNMP server, the server address you entered when logging in to the server must be the same as that specified in this command; otherwise, you cannot log in to the server.
- If the SNMP service has been started, running this command will restart the SNMP service.

Example

Set LoopBack0 as the source interface of an SNMP server.

```
<Huawei> system-view
[Huawei] snmp-agent server-source -i loopback 0
Info: Succeeded in setting the source interface of the snmp-agent to LoopBack0
```

21.2 RMON and RMON2 Configuration Commands

21.2.1 display rmon alarm

Function

The **display rmon alarm** command displays information about RMON alarm function.

Format

display rmon alarm [*entry-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
entry-number	Displays information about the RMON alarm entry with the specified index. If no index is specified, information about all alarms is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring the RMON alarm thresholds using the **rmon alarm** command, you can run this command to view the configured alarm variables, sampling interval, thresholds, alarm triggering condition, and last sampled value.

Example

Display the RMON alarm configurations.

```
<Huawei> display rmon alarm
Alarm table 1 owned by creator is VALID.
  Samples delta value       : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
  Sampling interval         : 5(sec)
  Rising threshold          : 1000 (linked with event 1)
  Falling threshold         : 100(linked with event 1)
  When startup enables      : risingOrFallingAlarm
  Latest value              : 0
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-15 Description of the display rmon alarm command output

Item	Description
Alarm table *entry-number* owned by *owner* is *status*.	The current status of the alarm entry *entry-number* created by *owner* is *status*. ● entry-number: alarm entry index, corresponding to the alarmIndex object in alarmTable. ● owner: creator of the entry, corresponding to the alarmOwner object in alarmTable. ● status: row status of the alarm entry with the specified index, corresponding to the alarmStatus in alarmTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Samples delta value	Alarm variable, namely, monitored MIB object, corresponding to the alarmVariable object in alarmTable.
Sampling interval	Sampling interval, in seconds, corresponding to the alarmInterval object in alarmTable.
Rising threshold	Rising threshold of the alarm table, corresponding to the alarmRisingThreshold object in alarmTable. When the sampled value reaches or exceeds the rising threshold, an alarm is generated.
Falling threshold	Falling threshold of the alarm table, corresponding to the alarmFallingThreshold object in alarmTable. When the sampled value reaches or falls below the falling threshold, an alarm is generated.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
When startup enables	Condition that triggers alarms, corresponding to the alarmStartupAlarm object in alarmTable. When the sampled value exceeds the rising threshold or falls below the falling threshold, an alarm is generated. The values are: ● risingOrFallingAlarm: generating an alarm when the sampled value exceeds the rising threshold or falls below the falling threshold ● risingAlarm: generating an alarm when the sampled value exceeds the rising threshold ● fallingAlarm: generating an alarm when the sampled value falls below the falling threshold
Latest value	Latest sampled value, corresponding to the alarmValue object in alarmTable.

Related Topics

21.2.11 rmon alarm

21.2.2 display rmon event

Function

The **display rmon event** command displays information about RMON events.

Format

display rmon event [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays the configuration of the RMON event with the specified index. If no index is specified, information about all events is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

After configuring the trap or log function for RMON events, you can run this command to view the configured event description, whether events trigger traps and logs, and latest event.

Example

Display the RMON event configurations.

```
<Huawei> display rmon event
Event table 1 owned by Huawei is VALID.
  Description: null.
  Will cause log  when triggered, last triggered at 0days 00h:24m:10s.69th.
```

Table 21-16 Description of the display rmon event command output

Item	Description
Event table *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. ● entry-number: event entry index, corresponding to the eventIndex object in eventTable. ● owner: creator of the entry, corresponding to the eventOwner object in eventTable. ● status: row status of the event entry with the specified index, corresponding to the eventStatus in eventTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Description	Event description, corresponding to the eventDescription object in eventTable.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Will cause log when triggered	Whether events trigger traps or logs, corresponding to the eventType object in eventTable. The actions associated with events are as follows: ● none: no action is taken. ● log: a log is recorded when an event is triggered. ● trap: a trap is sent to the NMS when an event is triggered. ● log-trap: a log is recorded and a trap is sent to the NMS when an event is triggered.
last triggered at	Latest event time, corresponding to the eventLastTimeSent object in eventTable.

Related Topics

21.2.12 rmon event

21.2.3 display rmon eventlog

Function

The **display rmon eventlog** command displays details about RMON event logs.

Format

display rmon eventlog [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays the log with the specified index. If no index is specified, information about all event logs is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

If you use the **rmon event** command to specify that a log is recorded for a certain event, the event record is stored in the LogTable. The command output includes event index, current event status, time the event triggers a log (calculated based on the number of seconds elapsed since system initialization or startup), and event description.

Example

Display the log of RMON event 1.

```
<Huawei> display rmon eventlog 1
Event table 1 owned by User is VALID.
  Generates eventLog 1.1 at 0days 00h:00m:07s.43th.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1, less than or equal to 100 with alarm
value 0. Alarm sample type is delta.
  Generates eventLog 1.2 at 0days 00h:02m:26s.43th.
  Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1, greater than or equal to 1000 with alarm
value 10443. Alarm sample type is delta.
```

Table 21-17 Description of the display rmon eventlog command output

Item	Description
Event table *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. • entry-number: event log entry index, corresponding to the logEventIndex object in LogTable. • owner: creator of the entry, corresponding to the eventOwner object in eventTable. • status: row status of the event entry with the specified index, corresponding to the eventStatus in eventTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Generates eventLog at	Log creation time (time elapsed since system startup), corresponding to the logTime object in LogTable.
Description	Event description, corresponding to the logDescription object in LogTable.

Related Topics

21.2.2 display rmon event

21.2.12 rmon event

 Copyright © Huawei Technologies Co., Ltd.

21.2.4 display rmon history

Function

The **display rmon history** command displays RMON history sampling information.

Format

display rmon history [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RMON history sampling information on the specified Ethernet interface. If this parameter is not specified, RMON history sampling information on all interfaces is displayed.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring RMON history statistics on an interface using the **rmon history** command, the system samples packets on the interface periodically. The **display rmon history** command can display history sampling information, including the number of sampled packets, history sampling interval, latest sampling information, Ethernet interface usage, number of CRC error packets, and total number of packets.

Example

Display RMON history sampling information.

```
<Huawei> display rmon history
History control entry 1 owned by Creator is VALID
  Samples interface     : Ethernet2/0/0<ifEntry.402653698>
  Sampling interval     : 30(sec) with 10 buckets max
  Last Sampling time    : 0days 00h:09m:43s.00th
  Latest sampled values :
  octets              :645       , packets           :7
  broadcast packets    :7         , multicast packets :0
  undersize packets    :6         , oversize packets  :0
  fragments packets    :0         , jabbers packets   :0
  CRC alignment errors :0         , collisions        :0
  Dropped packet:      :0         , utilization       :0
```

Display RMON history sampling information on the specified interface.

```
<Huawei> display rmon history ethernet 2/0/0
History control entry 1 owned by Creator is VALID
```

 Copyright © Huawei Technologies Co., Ltd.

```
Samples interface     : Ethernet2/0/0<ifEntry.402653698>
Sampling interval     : 30(sec) with 10 buckets max
Last Sampling time    : 0days 00h:09m:43s.00th
Latest sampled values :
octets              :645       , packets           :7
broadcast packets    :7         , multicast packets :0
undersize packets    :6         , oversize packets  :0
fragments packets    :0         , jabbers packets   :0
CRC alignment errors :0         , collisions        :0
Dropped packet:      :0         , utilization       :0
History record:
Record No.1 (Sample time: 0days 00h:02m:30s.01th)
octets              :0         , packets           :0
broadcast packets    :0         , multicast packets :0
undersize packets    :0         , oversize packets  :0
fragments packets    :0         , jabbers packets   :0
CRC alignment errors :0         , collisions        :0
Dropped packet:      :0         , utilization       :0
```

Table 21-18 Description of the display rmon history command output

Item	Description
History control entry *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. ● entry-number: history control table entry index, corresponding to the historyControlIndex object in historyControlTable. ● owner: creator of the entry, corresponding to the historyControlOwner object in historyControlTable. ● status: row status of the history control table entry with the specified index, corresponding to the historyControlStatus in historyControlTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Samples interface	Sampled interface.
Sampling interval	Sampling interval, in seconds, corresponding to the historyControlInterval object in historyControlTable. The system samples packets on the interface at this interval.
Last Sampling time	Latest sampling time, corresponding to the etherHistoryIntervalStart object in etherHistoryTable.
Latest sampled values	Latest sampling result.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
octets	Number of bytes received in a sampling interval, corresponding to the etherHistoryOctets object in etherHistoryTable.
packets	Number of packets received in a sampling interval, corresponding to the etherHistoryPkts object in etherHistoryTable.
broadcast packets	Number of broadcast packets received in a sampling interval, corresponding to the etherHistoryBroadcastPkts object in etherHistoryTable.
multicast packets	Number of multicast packets received in a sampling interval, corresponding to the etherHistoryMulticastPkts object in etherHistoryTable.
undersize packets	Number of undersize packets received in a sampling interval, corresponding to the etherHistoryUndersizePkts object in etherHistoryTable.
oversize packets	Number of large packets received in a sampling interval, corresponding to the etherHistoryOversizePkts object in etherHistoryTable.
fragments packets	Number of undersize and CRC error packets received in a sampling interval, corresponding to the etherHistoryFrag-ments object in etherHistoryTable.
jabbers packets	Number of large and CRC error packets received in a sampling interval, corresponding to the etherHistoryJabbers object in etherHistoryTable.
CRC alignment errors	Number of CRC error packets received in a sampling interval, corresponding to the etherHistoryCRCAlignErrors object in etherHistoryTable.
collisions	Number of collision packets received in a sampling interval, corresponding to the etherHistoryCollisions object in etherHistoryTable.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dropped packet	Number of packets discarded in a sampling interval, corresponding to the etherHistoryDropEvents object in etherHistoryTable.
utilization	Bandwidth usage in a sampling interval, corresponding to the etherHistoryUtilization object in etherHistoryTable.
History record	History sampling result.

Related Topics

21.2.13 rmon history

21.2.5 display rmon prialarm

Function

The **display rmon prialarm** command displays information about RMON extended alarm function.

Format

display rmon prialarm [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Displays information about the RMON extended alarm entry with the specified index. If this parameter is not specified, all RMON extended alarm information is displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring RMON extended alarm function using the **rmon prialarm** command, you can run this command to view sampling interval, rising and falling thresholds, alarm triggering condition, and latest sampled value.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the RMON extended alarm configurations.

```
<Huawei> display rmon prialarm
Prialarm table 1 owned by Huawei is VALID.
  Samples absolute value    : .1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1
  Sampling interval         : 30(sec)
  Rising threshold          : 1000(linked with event 3)
  Falling threshold         : 100(linked with event 3)
  When startup enables      : risingOrFallingAlarm
  This entry will exist     : forever
  Latest value              : 557
```

Table 21-19 Description of the display rmon prialarm command output

Item	Description
Prialarm table *entry-number* owned by *owner* is *status*.	The current status of the extended alarm entry *entry-number* created by *owner* is *status*. ● entry-number: extended alarm entry. ● owner: creator of the entry. ● status: row status of the extended alarm entry with the specified index. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Samples *type* value	The sampling type is *type*. The value of *type* can be: ● absolute: absolute value sampling ● delta: variable value sampling ● changeratio: change rate of sampled values (Change rate = Value change/Sampling interval) This field is followed by an alarm variable.
Sampling interval	Interval at which traffic is sampled.
Rising threshold	Alarm rising threshold.
Falling threshold	Alarm falling threshold.
linked with event *entry-number*	Associate with the row with index *entry-number*.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
When startup enables	Condition that triggers alarms (exceed the rising threshold or falls below the falling threshold). The values are: • risingOrFallingAlarm: generating an alarm when the sampled value exceeds the rising threshold or falls below the falling threshold • risingAlarm: generating an alarm when the sampled value exceeds the rising threshold • fallingAlarm: generating an alarm when the sampled value falls below the falling threshold
This entry will exist	Aging time of the extended alarm entry. An entry may be valid permanently or in a certain period.
Latest value	Latest sampling result.

Related Topics

21.2.14 rmon prialarm

21.2.6 display rmon statistics

Function

The **display rmon statistics** command displays RMON Ethernet statistics.

Format

display rmon statistics [*interface-type interface-number*]

Parameters

Parameter	Description	Value
interface-type interface-number	Displays RMON Ethernet statistics on the specified Ethernet interface. If this parameter is not specified, RMON Ethernet statistics on all interfaces are displayed.	-

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you configure Ethernet statistics using the **rmon statistics** command, the system collects packet statistics on Ethernet interfaces. The command output includes communication information generated since statistics function is enabled. The command output helps you locate faults.

When the device restarts, all statistics are cleared.

Example

Display RMON Ethernet statistics.

```
<Huawei> display rmon statistics
Statistics entry 1 owned by Creator is VALID.
  Interface : Ethernet2/0/0<ifEntry.402653698>
  Received  :
  octets              :142915224 , packets          :1749151
  broadcast packets   :11603     , multicast packets:756252
  undersize packets   :0         , oversize packets :0
  fragments packets   :0         , jabbers packets  :0
  CRC alignment errors:0         , collisions       :0
  Dropped packet (insufficient resources):1795
  Packets received according to length (octets):
  64     :150183    ,  65-127  :150183    ,  128-255  :1383
  256-511:3698      ,  512-1023:0         ,  1024-1518:0
```

Table 21-20 Description of the display rmon statistics command output

Item	Description
Statistics entry *entry-number* owned by *owner* is *status*.	The current status of the event entry *entry-number* created by *owner* is *status*. ● entry-number: Ethernet statistics entry, corresponding to the etherStatsIndex object in etherStatsTable. ● owner: creator of the entry, corresponding to the etherStatsOwner object in etherStatsTable. ● status: row status of the Ethernet statistics entry with the specified index, corresponding to the etherStatsStatus in etherStatsTable. – UNDERCREATION: invalid – VALID: valid – INVALID: invalid due to hot swapping of the LPU
Interface	Interface where statistics are collected, corresponding to the etherStatsDataSource object in etherStatsTable, followed by the interface OID.
Received	Number of received packets.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
octets	Number of received octets.
packets	Number of received packets, corresponding to the etherStatsPkts object in etherStatsTable.
broadcast packets	Number of received broadcast packets, corresponding to the etherStatsBroadcastPkts object in etherStatsTable.
multicast packets	Number of received multicast packets, corresponding to the etherStatsMulticastPkts object in etherStatsTable.
undersize packets	Number of received undersize packets, corresponding to the etherStatsUndersizePkts object in etherStatsTable.
oversize packets	Number of received large packets, corresponding to the etherStatsOversizePkts object in etherStatsTable.
fragments packets	Number of received undersize and CRC error packets, corresponding to the etherStatsFragments object in etherStatsTable.
jabbers packets	Number of received large and CRC error packets, corresponding to the etherStatsJabbers object in etherStatsTable.
CRC alignment errors	Number of received CRC error packets, corresponding to the etherStatsCRCAlignErrors object in etherStatsTable.
collisions	Number of received collision packets, corresponding to the etherStatsCollisions object in etherStatsTable.
Dropped packet	Number of discarded packets, corresponding to the etherStatsDropEvents object in etherStatsTable.
Packets received according to length	Number of received packets with different lengths, corresponding to the etherStatsPkts64Octets, etherStatsPkts65to127Octets, etherStatsPkts128to255Octets, etherStatsPkts256to511Octets, etherStatsPkts512to1023Octets, and etherStatsPkts1024to1518Octets objects in etherStatsTable.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.2.15 rmon statistics

21.2.7 display rmon2 hlhostcontroltable

Function

The **display rmon2 hlhostcontroltable** command displays information about entries in hlHostControlTable.

Format

display rmon2 hlhostcontroltable [**index** *ctrl-index*] [**verbose**]

Parameters

Parameter	Description	Value
index *ctrl-index*	Indicates the entry index, which uniquely identifies an entry in the host control table.	The value is an integer that ranges from 1 to 65535.
verbose	Displays details about the host control table.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After you use the **rmon2 hlhostcontroltable** command to create a protocol directory table, you can run the **display rmon2 hlhostcontroltable** command to view the configurations.

If no entry index is specified, the configuration of the entire table is displayed.

Example

Display information about the entry with index 123 in the host control table.

```
<Huawei> display rmon2 hlhostcontroltable index 123
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
```

 Copyright © Huawei Technologies Co., Ltd.

```
maxentries - hlhostcontrolnlmaxdesiredentries
status - hlhostcontrolstatus

index datasource              droppedfrm inserts    Deletes    maxentries      status
123   GE2/0/0                 0          0          0          50              active
```

Display detailed information about the entry with index 123 in the host control table.

```
<Huawei> display rmon2 hlhostcontroltable index 123 verbose
Abbreviation:
index - hlhostcontrolindex
datasource - hlhostcontroldatasource
droppedfrm - hlhostcontrolnldroppedframes
inserts - hlhostcontrolnlinserts
Deletes - hlHostControlNlDeletes
maxentries - hlhostcontrolnlmaxdesiredentries
owner - hlhostcontrolowner
status - hlhostcontrolstatus

index      :   123
datasource  :   GigabitEthernet2/0/0
droppedfrm  :   0
inserts     :   7
Deletes     :   0
maxentries  :   100
owner       :   china
status      :   active
```

Table 21-21 Description of the **display rmon2 hlhostcontroltable** command output

Item	Description
index	Index of hlHostControlTable.
datasource	Source interface of data.
droppedfrm	Number of the frames that are received on the statistics interface but not added into nlHost entries.
inserts	Times add nlHost entries are added to nlHostTable.
Deletes	Times nlHost entries are deleted from nlHostTable.
maxentries	Maximum number of entries that nlHostTable contains.
owner	Owner of entries.
status	Status of entries in the hlHostControlTable. ● active: running normally ● notinservice: invalid

Related Topics

21.2.16 rmon2 hlhostcontroltable

 Copyright © Huawei Technologies Co., Ltd.

21.2.8 display rmon2 nlhosttable

Function

The **display rmon2 nlhosttable** command displays information about entries in the nlHostTable.

Format

display rmon2 nlhosttable [**hostcontrolindex** *ctrl-index*] [**hostaddress** *ip-address*]

Parameters

Parameter	Description	Value
hostcontrolindex *ctrl-index*	Specifies the index number. A *ctrl-index* uniquely identifies an entry in the hlHostControlTable.	It is an integer ranging from 1 to 65535.
hostaddress *ip-address*	Checks the traffic on a specified host.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After statistics function is configured on an interface, you can view traffic statistics using this command. A maximum of 5000 rows can be displayed for each protocol on an interface.

Example

Display information about the entry with index 1 in the host table.

```
<Huawei> display rmon2 nlhosttable hostcontrolindex 1 hostaddress 10.110.94.177
Abbreviation:
HIdx - hlHostControlIndex
Addr - nlHostAddress
InPkts - nlHostInPkts
OutPkts - nlHostOutPkts
InOctes - nlHostInOctets
OutOctes - nlHostOutOctets
OutMac - nlHostOutMacNonUnicastPkts
HIdx   Addr            InPkts    OutPkts   InOctes   OutOctes   OutMac
1      10.110.94.177   4         5         216       483
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-22 Description of the display rmon2 nlhosttable command output

Item	Description
HIdx	Index of the host control table.
Addr	Host address. It is the source address of the incoming IP packets on the monitored interface and destination address of the outgoing IP packets on the interface.
InPkts	Number of incoming packets on the monitored interface.
OutPkts	Number of outgoing packets on the monitored interface.
InOctes	Number of incoming bytes on the monitored interface.
OutOctes	Number of outgoing bytes on the monitored interface.
OutMac	Number of outgoing non-unicast packets on the monitored interface.

21.2.9 display rmon2 protocoldirtable

Function

The **display rmon2 protocoldirtable** command displays all entries in the protocolDirTable.

Format

display rmon2 protocoldirtable

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

After you use the **rmon2 protocoldirtable** command to configure statistics on IP packets, you can run the **display rmon2 protocoldirtable** command to view the configurations.

Example

Display entries in the protocolDirTable.

```
<Huawei> display rmon2 protocoldirtable
protocolDirId              :   8.0.0.0.1.0.0.8.0
protocolDirParameters      :   2.0.0
protocolDirLocalIndex      :   2
protocolDirDescr           :   IP
protocolDirAddressMapConfig:   notsupported
protocolDirHostConfig      :   supportedon
protocolDirMatrixConfig    :   notsupported
protocolDirOwner           :   china
protocolDirStatus          :   active
```

Table 21-23 Description of the display rmon2 protocoldirtable command output

Item	Description
protocolDirId	Protocol directory ID. Currently, RMON2 only supports IP protocol, so the protocol directory ID is fixed at 8.0.0.0.1.0.0.8.0.
protocolDirParameters	Protocol directory parameter. The value is fixed at 2.0.0.
protocolDirLocalIndex	Local protocol directory index.
protocolDirDescr	Protocol directory description.
protocolDirAddressMapConfig	Whether protocol directory address mapping is supported. This function is not supported currently.
protocolDirHostConfig	• notsupported: The device does not monitor the network-layer host table of the protocol, and this value cannot be changed. • supportedon: The device can monitor the network-layer host table of the protocol, and the monitoring function is enabled. • supportedoff: The device can monitor the network-layer host table of the protocol, but the monitoring function is disabled.
protocolDirMatrixConfig	Whether protocol directory matrix is supported. This function is not supported currently.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
protocolDirOwner	Protocol directory owner.
protocolDirStatus	Protocol directory status. ● active: running normally ● not in service: invalid

Related Topics

21.2.17 rmon2 protocoldirtable

21.2.10 display snmp-agent trap feature-name rmon all

Function

The **display snmp-agent trap feature-name rmon all** command displays the status of all traps about the RMON module.

Format

display snmp-agent trap feature-name rmon all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None.

Example

Display the status of all traps about the RMON module.

```
<Huawei> display snmp-agent trap feature-name rmon all
-----------------------------------------------------------------------------
Feature name: RMON
Trap number : 4
-----------------------------------------------------------------------------
Trap name                Default switch status   Current switch status
risingalarm              on                      on
fallingalarm             on                      on
rmon_pri_risingalarm     on                      on
rmon_pri_fallingalarm    on                      on
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-24 Description of the display snmp-agent trap feature-name rmon all command output

Item	Description
Feature name	Name of the module to which a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap message of the RMON module.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Current status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
risingalarm	Indicates that the current sampled value is greater than or equal to the set threshold specified by the alarm table.
fallingalarm	Indicates that the current sampled value is less than or equal to the set threshold specified by the alarm table.
rmon_pri_risingalarm	Indicates that the current sampled value is greater than or equal to the set threshold specified by the pri_alarm table.
rmon_pri_fallingalarm	Indicates that the current sampled value is less than or equal to the set threshold specified by the pri_alarm table.

Related Topics

21.2.19 snmp-agent trap enable feature-name rmon

21.2.11 rmon alarm

Function

The **rmon alarm** command adds an entry to the alarm table.

The **undo rmon alarm** command deletes an entry from the alarm table.

Format

rmon alarm *entry-number alarm-OID sampling-time* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *owner-name*]

 Copyright © Huawei Technologies Co., Ltd.

undo rmon alarm *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
alarm-OID	Specifies the alarm OID.	The name is a string of 1 to 256 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
sampling-time	Specifies the sampling interval.	The value is an integer that ranges from 5 to 65535, in seconds.
absolute	Indicates that the sample type is absolute. The value is the sampled value at the end of the period.	-
changeratio	Indicates that the sample type is changeratio. The value is Changing value/Sampling interval.	-
delta	Indicates that the sample type is delta. The value is the difference between the samples at the beginning and end of the period.	-
rising-threshold *threshold-value1*	Specifies the rising threshold of sampled value.	The value is an integer that ranges from 1 to 2147483647.
event-entry1	Indicates the event index corresponding to the rising threshold.	The value is an integer that ranges from 1 to 65535.
falling-threshold *threshold-value2*	Specifies the falling threshold of sampled value.	The value is an integer that ranges from 0 to 2147483646.
event-entry2	Indicates the event index corresponding to the falling threshold.	The value is an integer that ranges from 1 to 65535.
owner *owner-name*	Indicates the owner of the alarm.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor system running status, run the **rmon alarm** command to configure an alarm table and add an entry to the alarm table. After the command is executed, the RMON alarm function is enabled. The system obtains information about the monitored object at the specified interval, and compares the obtained value with the configured threshold. Then the system triggers the event according to the following table, and records log or sends a trap to the NMS.

Situation	Action
The sampled value is larger than or equal to the configured rising threshold *threshold-value1*.	Trigger *event-entry1*.
The sampled value is smaller than or equal to the configured falling threshold *threshold-value2*.	Trigger *event-entry2*.

Prerequisites

Before configuring alarm function for the specified object, run the **rmon event** command to define the associated events.

If the alarm variables configured in RMON alarm function are MIB variables defined in the statistics group or history group, the Ethernet statistics function or history statistics function must be configured on the monitored Ethernet interface first. Otherwise, alarm entries cannot be created.

Example

Monitor alarm thresholds for etherStatsBroadcastPkts (alarm OID is 1.3.6.1.2.1.16.1.1.1.6.1): Set the sampling interval to 30 seconds and sample type to absolute. When the sampled value reaches or exceeds 500, event 1 is triggered. When the sampled value reaches or falls below 100, event 2 is triggered. The owner is **creator**.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon statistics 1 owner creator
[Huawei-Ethernet2/0/0] quit
[Huawei] rmon event 1 log
[Huawei] rmon event 2 trap public
[Huawei] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.6.1 30 absolute rising-threshold 500 1 falling-threshold 100
2 owner creator
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.2.1 display rmon alarm

21.2.12 rmon event

Function

The **rmon event** command adds an entry to the event table.

The **undo rmon event** command deletes an entry from the event table.

Format

rmon event *entry-number* [**description** *string*] { **log** | **trap** *object* | **log-trap** *object* | **none** } [**owner** *owner-name*]

undo rmon event *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
description *string*	Specifies the event description.	The value is a string of 1 to 127 characters.
log	Records a log for the event.	-
trap	Sends a trap to the NMS.	-
object	Specifies the community name of the NMS receiving the trap.	The value is a string of 1 to 127 characters.
log-trap	Records a log and sends a trap to the NMS for the event.	-
none	Indicates that no action is taken for the event.	-
owner *owner-name*	Indicates the creator of the event entry.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

This command specifies whether to record a log or send a trap for events. When an error occurs in the system, the RMON alarm function triggers the corresponding event. You can run the **rmon event** command to configure an event table and add an entry to the table. The entry specifies whether to record a log or send a trap to the NMS for the event.

Prerequisites

The **rmon alarm** command is executed to configure the alarm objects. Otherwise, no alarm will trigger the event.

Example

Send a trap to the NMS for event 10.

```
<Huawei> system-view
[Huawei] rmon event 10 trap public
```

Related Topics

21.2.2 display rmon event

21.2.13 rmon history

Function

The **rmon history** command adds an entry to the history control table.

The **undo rmon history** command deletes an entry from the history control table.

Format

rmon history *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *owner-name*]

undo rmon history *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
buckets *number*	Indicates the maximum number of records in the history control table.	The value is an integer that ranges from 1 to 10.
interval *sampling-interval*	Specifies the sampling interval.	The value is an integer that ranges from 5 to 3600, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
owner *owner-name*	Indicates the owner of the entry in the history control table.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

Ethernet interface view, GE interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect statistics on the specified interface at an interval and save the statistics for future retrieval, run the **rmon history** command to configure a history control table and add an entry to the table. The system can periodically collect statistics on each type of traffic, including bandwidth usage, number of error packets, and total number of packets.

Precautions

The number of stored records is determined by the **buckets** *number* parameter. When the number of records in the table reaches the maximum, the system overwrites the old records with new ones. Statistics include the number of packets, broadcast packets, and multicast packets received by the interface within a sampling interval. You can run the **display rmon history** command to view history sampling results.

Example

Configure a history control table and add an entry with index 1 to the table. Set the maximum number of entries in the table to 10, sampling interval to 5 seconds, and creator to **user1**.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon history 1 buckets 10 interval 5 owner user1
```

Related Topics

21.2.4 display rmon history

21.2.14 rmon prialarm

Function

The **rmon prialarm** command adds an entry to the extended alarm table.

Copyright © Huawei Technologies Co., Ltd.

The **undo rmon prialarm** command deletes an entry from the extended alarm table.

Format

rmon prialarm *entry-number prialarm-formula description-string sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **cycle** *entry-period* | **forever** } [**owner** *owner-name*]

undo rmon prialarm *entry-number*

Parameters

Parameter	Description	Value
entry-number	Specifies the index of the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
prialarm-formula	Specifies the formula for calculating an alarm variable. The alarm variable in the formula is identified by an OID. The OID value starts with a dot, for example, (.1.3.6.1.2.1.2.1.10.1)*8. The calculation formula is defined by user. The calculation result is a long integer. Ensure that the length of calculation result in each step cannot exceed the limit; otherwise, the calculation result is incorrect.	The value is a string of 1 to 256 characters.
description-string	Specifies the alarm description.	The value is a string of 1 to 256 characters.
sampling-interval	Specifies the sampling interval.	The value is an integer that ranges from 10 to 65535, in seconds.
absolute	Indicates that the sample type is absolute. The value is the sampled value at the end of the period.	-
changeratio	Indicates that the sample type is changeratio. The value is Changing value/Sampling interval.	-
delta	Indicates that the sample type is delta. The value is the difference between the samples at the beginning and end of the period.	-
rising-threshold *threshold-value1*	Specifies the alarm rising threshold.	The value is an integer that ranges from 1 to 2147483647.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
event-entry1	Indicates the entry number of the event corresponding to the rising threshold in the event table.	The value is an integer that ranges from 1 to 65535.
falling-threshold *threshold-value2*	Specifies the alarm falling threshold.	The value is an integer that ranges from 0 to 2147483646.
event-entry2	Indicates the entry number of the event corresponding to the falling threshold in the event table.	The value is an integer that ranges from 1 to 65535.
entrytype	Indicates the lifetime type of an alarm entry.	-
cycle *entry-period*	Indicates the lifetime of an alarm entry.	The value is an integer that ranges from 11 to 2147483646.
forever	Indicates that the alarm entry is valid permanently.	-
owner *owner-name*	Indicates the owner of the extended alarm variable.	The value is a string of 1 to 127 case-sensitive characters without spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The extended alarm function can compute the alarm variables and compare the result with the specified threshold.

After the extended alarm function is enabled, the system performs the following operations:

1. Samples the alarm variables in the extended alarm formula at the specified sampling interval.
2. Calculates the sampled value using the defined formula.
3. Compares the calculation result with the thresholds and takes actions according to the following table.

 Copyright © Huawei Technologies Co., Ltd.

Situation	Action
The sampled value is larger than or equal to the configured rising threshold *threshold-value1*.	Trigger *event-entry1*.
The sampled value is smaller than or equal to the configured falling threshold *threshold-value2*.	Trigger *event-entry2*.

To use more alarm functions, run the **rmon prialarm** command to configure the extended alarm table and add an entry to the table.

Prerequisites

Before configuring extended alarm function for the specified object, run the **rmon event** command to define the associated events. Otherwise, events cannot be triggered even if alarms are generated. When the sampled value exceeds the rising threshold or falls below the falling threshold, whether to record a log or send a trap to the NMS is determined by the **rmon event** command.

Example

Monitor broadcast and multicast packets: Set the sampling interval to 10 seconds and sample type to absolute. Trigger event 3 when the sample value reaches or exceeds 100000 and when the sample value reaches or falls below 100. Set the lifetime of the entry to forever and the owner to **Huawei**.

```
<Huawei> system-view
[Huawei] rmon prialarm 1 .1.1.3.6.1.2.1.16.1.1.1.6.1+.1.3.6.1.2.1.16.1.1.1.7.1 sumofbroadandmulti 10
absolute rising-threshold 100000 3 falling-threshold 100 3 entrytype forever owner Huawei
```

Related Topics

21.2.5 display rmon prialarm

21.2.15 rmon statistics

Function

The **rmon statistics** command adds an entry to the statistics table.

The **undo rmon statistics** command deletes an entry from the statistics table.

Format

rmon statistics *entry-number* [**owner** *owner-name*]

undo rmon statistics *entry-number*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
entry-number	Indicates the row index corresponding to the entry to be added or deleted.	The value is an integer that ranges from 1 to 65535.
owner *owner-name*	Indicates the owner name.	The name is a string of 1 to 127 case-sensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.

Views

Ethernet interface view, GE interface view, XGE sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To keep collecting statistics on the current interface, run the **rmon statistics** command to configure a statistics table and add an entry to the table. This command monitors usage of Ethernet interfaces and collects statistics on errors, including the number of collision packets, CRC error packets, undersize and large packets, timeout packets, fragments, broadcast packets, multicast packets, and unicast packets.

Prerequisites

The **rmon-statistics enable** command is executed to enable RMON statistics function on the interface. If the command is not executed, the statistics result is 0.

Example

Configure a statistics table on Ethernet2/0/0 and add an entry with index 20 to the table.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon statistics 20 owner creater
```

Related Topics

21.2.6 display rmon statistics
21.2.18 rmon-statistics enable

 Copyright © Huawei Technologies Co., Ltd.

21.2.16 rmon2 hlhostcontroltable

Function

The **rmon2 hlhostcontroltable** command creates or changes an entry in the hlHostControlTable.

The **undo rmon2 hlhostcontroltable** command deletes an entry from the hlHostControlTable or from the whole table.

Format

rmon2 hlhostcontroltable index *ctrl-index* [**datasource interface** *interface-type interface-number*] [**maxentry** *maxentry-value*] [**owner** *owner-name*] [**status** { **active** | **inactive** }]

undo rmon2 hlhostcontroltable [**index** *ctrl-index*]

Parameters

Parameter	Description	Value
ctrl-index	Indicates the entry index, which uniquely identifies an entry in the host control table.	The value is an integer that ranges from 1 to 65535.
datasource interface *interface-type interface-number*	Identifies an interface and a subnet, corresponding to hlHostControlDataSource. The parameter value, namely, the interface index, is the data source defining the entry. In this command, the data source is represented by interface type and number.	-
maxentry *maxentry-value*	Indicates the maximum number of entries in the host table.	The value is an integer that ranges from 1 to 100000. The default value is 50. If the host table contains too many entries, system performance is degraded. The default settings of host table are recommended.
owner *owner-name*	Indicates the owner.	The value is a string of 1 to 127 characters and cannot be empty.
status	Indicates the status of an entry in the host control table, corresponding to hlHostControlStatus.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
active	Indicates that the hlHostControlStatus value in the host control table is active and this entry is available.	-
inactive	Indicates that the hlHostControlStatus value in the host control table is not in service and this entry is inactive and unavailable.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor traffic on the subnet connected to an interface of the managed device, run the **rmon2 hlhostcontroltable** command and specify the interface.

Precautions

When creating an entry, specify the **datasource interface** parameter to identify the interface, which specifies the subnet. The parameter value, namely, the interface index, is the data source defining the entry. Enter the interface type and number in the command. Only one entry can be created for each interface in the host control table.

The parameter **status** in the **display rmon2 hlhostcontroltable** command output matches the hlhostcontrolstatus value, which indicates the entry status.

- When the hlhostcontrolstatus value is set to **inactive**, all related entries in the host table are deleted automatically.
- When the hlhostcontrolstatus value is set to **active**, you cannot change the hlhostcontroldatasource and hlhostcontrolnlmaxdesiredentries values.
- If an interface that corresponds to the hlhostcontroldatasource in an entry is deleted, the entry is deleted at the same time.

Example

Create an entry in the host control table.

```
<Huawei> system-view
[Huawei] rmon2 hlhostcontroltable index 1 datasource interface ethernet 2/0/0 maxentry 100 owner
huawei status active
```

Set the hlHostControlStatus value in the host control table to **not in service**.

```
<Huawei> system-view
[Huawei] rmon2 hlhostcontroltable index 1 status inactive
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.2.7 display rmon2 hlhostcontroltable

21.2.17 rmon2 protocoldirtable

Function

The **rmon2 protocoldirtable** command creates or modifies an entry in the protocolDirTable.

The **undo rmon2 protocoldirtable** command deletes an entry from the protocolDirTable. If optional parameters are not specified, the entire table is deleted.

Format

rmon2 protocoldirtable protocoldirid *protocol-id* **parameter** *parameter-value* [**descr** *description-string*] [**host** { **notsupported** | **supportedon** | **supportedoff** }] [**owner** *owner-name*] [**status** { **active** | **inactive** }]

undo rmon2 protocoldirtable [**protocoldirid** *protocol-id* **parameter** *parameter-value*]

Parameters

Parameter	Description	Value
protocol-id	Indicates the protocol ID. Only IP protocol is supported currently.	The value is fixed at 8.0.0.0.1.0.0.8.0.
parameter *parameter-value*	Indicates the protocol parameter.	The value is fixed at 2.0.0.
descr *description-string*	Indicates the description of the protocol directory table.	The value is a string of 1 to 64 characters.
host	Indicates the configuration of protocol directory host, corresponding to protocolDirHostConfig in the **display rmon2 protocoldirtable** command output.	-
notsupported	Indicates that the device does not monitor the network-layer host table of the protocol, and this value cannot be changed.	-
supportedon	Indicates that the device can monitor the network-layer host table of the protocol, and the monitoring function is enabled.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
supportedoff	Indicates that the device can monitor the network-layer host table of the protocol, but the monitoring function is disabled.	-
owner *owner-name*	Indicates the owner.	The value is a string of 1 to 127 characters.
status	Indicates the entry status, corresponding to the protocolDirStatus value in the **display rmon2 protocoldirtable** command output.	-
active	Indicates that the protocolDirStatus value in the host control table is active and this entry is available.	-
inactive	Indicates that the protocolDirStatus value in the host control table is not in service and this entry is inactive and unavailable.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To monitor statistics on IP packets, run this command.

RMON2 supports only statistics on IP packets on an Ethernet interface. A protocol occupies an entry, so there is only one entry in the table.

Precautions

When running the **rmon2 protocoldirtable** command, you must set the description and protocols supported by the host. That is, the **descr** and **host** parameters are mandatory.

The parameter **status** in the **display rmon2 protocoldirtable** command output matches the protocoldirStatus value, which indicates the entry status.

- When the **status** parameter is set to **active**, the **descr** value cannot be modified. The value of **host** (corresponding to the protocolDirHostConfig value, indicating the protocol directory host configuration) can be modified. This parameter indicates whether to monitor the network-layer host table of the protocol.

 Copyright © Huawei Technologies Co., Ltd.

  - If the **host** value is set to **notsupported**, the **host** value cannot be modified.
  - If the **host** value is not **notsupported**, the value can be switched between **supportedon** and **supportedoff**.
  - When the **host** value is changed from **supportedon** to **supportedoff**, the corresponding entry in the host control table is deleted.
- When the status is **inactive**, all related entries in the host table are deleted.

Example

Create an entry in the protocol directory table.

```
<Huawei> system-view
[Huawei] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 descr huawei host
supportedon owner huawei status active
```

Set the protocolDirStatus value in the protocol directory table to not in service.

```
<Huawei> system-view
[Huawei] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 status inactive
```

Set the protocolDirHostConfig value in the protocol directory table to supportedon.

```
<Huawei> system-view
[Huawei] rmon2 protocoldirtable protocoldirid 8.0.0.0.1.0.0.8.0 parameter 2.0.0 host supportedon
```

Related Topics

21.2.9 display rmon2 protocoldirtable

21.2.18 rmon-statistics enable

Function

The **rmon-statistics enable** command enables RMON statistics function on an interface.

The **undo rmon-statistics** command disables RMON statistics function on an interface.

By default, RMON statistics function is disabled on interfaces.

Format

rmon-statistics enable

undo rmon-statistics

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

If the statistics function is not enabled on an interface, statistics in the statistics table and history table are 0.

Example

Enable RMON statistics function on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] rmon-statistics enable
```

Related Topics

21.2.15 rmon statistics

21.2.19 snmp-agent trap enable feature-name rmon

Function

The **snmp-agent trap enable feature-name rmon** command enables the alarm function for the RMON module.

The **undo snmp-agent trap enable feature-name rmon** command disables the alarm function for the RMON module.

By default, the alarm function is enabled for the RMON module.

Format

snmp-agent trap enable feature-name rmon [**trap-name** { **fallingalarm** | **risingalarm** | **rmon_pri_fallingalarm** | **rmon_pri_risingalarm** }]

undo snmp-agent trap enable feature-name rmon [**trap-name** { **fallingalarm** | **risingalarm** | **rmon_pri_fallingalarm** | **rmon_pri_risingalarm** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the alarm function for the specified event. If no event type is specified using the **trap-name** parameter, all types of alarms are enabled or disabled for the RMON module.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
fallingalarm	Indicates that the current sampled value is smaller than or equal to the threshold configured in the alarmTable.	-
risingalarm	Indicates that the current sampled value is larger than or equal to the threshold configured in the alarmTable.	-
rmon_pri_fallingalarm	Indicates that the current sampled value is smaller than or equal to the threshold configured in the prialarmTable.	-
rmon_pri_risingalarm	Indicates that the current sampled value is larger than or equal to the threshold configured in the prialarmTable.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

A device managed by the NMS can send traps to the NMS if the alarm function is enabled for the RMON module on the device. By default, all alarms for the RMON module are enabled. If only one or some event alarms need to be enabled, run the **snmp-agent trap enable feature-name rmon trap-name** command.

Example

Enable the fallingalarm for the RMON module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name rmon trap-name fallingalarm
```

21.3 TCP FPM Configuration Commands

21.3.1 display tcp fpm session

Function

The **display tcp fpm session** command displays TCP FPM statistics.

 Copyright © Huawei Technologies Co., Ltd.

Format

display tcp fpm session { **all** | **number** }

Parameters

Parameter	Description	Value
all	Displays all TCP FPM statistics.	-
number	Indicates the number of sessions involved in TCP FPM statistics collection.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

This command can display TCP FPM statistics, including network delay and packet loss rate, which are the reference for network optimization.

Example

Display all TCP FPM statistics.

```
<Huawei> display tcp fpm session all
Index DstIP(Port)          SrcIP(Port)          Loss(%)  SND  CND  RT   Application
1 10.1.1.3(2053)           10.1.3.2(3351)         0       12   4    0     FTP
```

Display the number of entries of which the TCP FPM statistics are displayed.

```
<Huawei> display tcp fpm session number
 TCP fpm session number : 2
```

Table 21-25 Description of the **display tcp fpm session** command output

Item	Description
Index	Index of a session involved in TCP FPM statistics collection.
DstIP(Port)	IP address and port number of the application server.
SrcIP(Port)	IP address and port number of the application client.
Loss(%)	Packet loss rate.
CND	Network time on the client.
SND	Network time on the server.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
RT	Response time of the router.
Application	Application type.
TCP fpm session number	Number of sessions involved in TCP FPM statistics collection.

21.3.2 reset tcp fpm session all

Function

The **reset tcp fpm session all** command clears TCP FPM statistics.

Format

reset tcp fpm session all

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To understand the quality of the network running TCP applications, clear existing TCP FPM statistics first, and then collect new statistics. From the latest statistics, you can know the network status in real time.

Precautions

Statistics cannot be restored after being cleared. Exercise caution when you run the following commands.

Example

Clear TCP FPM statistics.

```
<Huawei> system-view
[Huawei] reset tcp fpm session all
 Reset tcp fpm session success .
```

 Copyright © Huawei Technologies Co., Ltd.

21.3.3 pm report tcp fpm enable

Function

The **pm report tcp fpm enable** command enables the function of reporting TCP FPM statistics to the controller.

The **undo pm report tcp fpm enable** command disables the function of reporting TCP FPM statistics to the controller.

By default, TCP FPM statistics are not reported to the controller.

Format

pm report tcp fpm enable

undo pm report tcp fpm enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

TCP FPM statistics can be displayed in two methods:

- CLI: Run the
  display tcp fpm session
  command to view TCP FPM statistics.
- Controller: Display TCP FPM statistics on the GUI.

If you want to view statistics on the controller, enable the function of reporting TCP FPM statistics to the controller.

Precautions

This method can be used only in the SD-WAN solution, in which a controller is deployed.

Example

Enable the function of reporting TCP FPM statistics to the controller.

```
<Huawei> system-view
[Huawei] pm report tcp fpm enable
```

 Copyright © Huawei Technologies Co., Ltd.

21.3.4 tcp fpm enable

Function

The **tcp fpm enable** command enables the TCP FPM function.

The **undo tcp fpm enable** command disables the TCP FPM function.

By default, the TCP FPM function is disabled.

Format

tcp fpm enable

undo tcp fpm enable

Parameters

None

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the TCP FPM function is enabled, the router can collect network performance statistics of TCP applications, such as delay and packet loss rate. You can optimize the network based on the network performance.

Precautions

Ethernet interfaces do not support this command when working as Layer 2 interfaces. Therefore, the interfaces must be added to VLANIF interfaces or the interface mode must be switched to Layer 3.

Example

Enable the TCP FPM function.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] tcp fpm enable
```

21.3.5 tcp fpm report time

 Copyright © Huawei Technologies Co., Ltd.

Function

The **tcp fpm report time** command sets the interval for reporting TCP FPM statistics to the controller.

The **undo tcp fpm report time** command sets the interval for reporting TCP FPM statistics to the controller to the default value.

By default, the interval for reporting TCP FPM statistics to the controller is 60s.

Format

tcp fpm report time *time*

undo tcp fpm report time

Parameters

Parameter	Description	Value
time	Specifies the interval for reporting TCP FPM statistics to the controller.	The value is an integer that ranges from 5 to 86400, in seconds.

Views

System view

Default Level

3: Management level

Usage Guidelines

By default, the router sends statistics on TCP applications, such as delay and packet loss rate, to the controller at an interval of 60s. You can change the interval if needed.

Example

Set the interval for reporting TCP FPM statistics to the controller to 100s.

```
<Huawei> system-view
[Huawei] tcp fpm report time 100
```

21.4 IP FPM Configuration Commands

21.4.1 authentication-mode (IPFPM-DCP view)

Function

The **authentication-mode** command configures the authentication mode and password for a Data Collecting Point (DCP).

 Copyright © Huawei Technologies Co., Ltd.

The **undo authentication-mode** command deletes the authentication mode and password of a DCP.

By default, no authentication mode or password is configured for a DCP.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Indicates the HMAC-SHA256 authentication algorithm to be used for packets sent from a DCP to an MCP.	-
key-id *key-id*	Specifies the key ID for the authentication password of a DCP.	The value is an integer ranging from 1 to 64.
cipher	Indicates that the authentication password is displayed in ciphertext.	-
password	Specifies the authentication password of a DCP.	The value is a string of characters. ● The value ranges from 1 to 255 for simple passwords. ● The value ranges from 32 to 392 for ciphertext passwords.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security and performance statistics reliability, run the **authentication-mode** command so that authentication is performed during IP FPM performance statistics. An MCP and its associated DCPs must have the same

 Copyright © Huawei Technologies Co., Ltd.

authentication mode and password configured. The MCP processes packets only from the authenticated DCPs.

Prerequisites

The **nqa ipfpm dcp** command has been run to enable DCP globally.

Precautions

IP FPM supports only the HMAC-SHA256 authentication algorithm.

Example

Configure the authentication mode and password for a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-ipfpm-dcp] authentication-mode hmac-sha256 key-id 1 cipher Huawei-123
```

21.4.2 authentication-mode (IPFPM-MCP view)

Function

The **authentication-mode** command configures the authentication mode and password for a Measurement Control Point (MCP) in the IP Flow Performance Measurement (IP FPM) model.

The **undo authentication-mode** command deletes the authentication mode and password of an MCP in the IP FPM model.

By default, no authentication mode or password is configured for an MCP in the IP FPM model.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256 key-id *key-id*

Parameters

Parameter	Description	Value
hmac-sha256	Indicates the HMAC-SHA256 authentication algorithm to be used for packets sent from a DCP to an MCP.	-
key-id *key-id*	Specifies the key ID for the authentication password of an MCP.	The value is an integer ranging from 1 to 64.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher	Indicates that the authentication password is displayed in ciphertext.	-
password	Specifies the authentication password of an MCP.	The value is a string of case-sensitive characters without spaces. ● The value ranges from 1 to 255 for simple passwords. ● The value ranges from 32 to 392 for ciphertext passwords.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security and performance statistics reliability, run the **authentication-mode** command so that authentication is performed during IP FPM performance statistics. An MCP and its associated DCPs must have the same authentication mode and password configured. The MCP processes packets only from the authenticated DCPs.

Precautions

IP FPM supports only the HMAC-SHA256 authentication algorithm.

The authentication mode and password configured on an MCP must be the same as those configured on the DCPs associated with this MCP. Otherwise, the MCP cannot process the statistics reported by the DCPs.

Example

Configure the authentication mode and password for an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] authentication-mode hmac-sha256 key-id 1 Huawei-123
```

 Copyright © Huawei Technologies Co., Ltd.

21.4.3 authentication-mode (IPFPM-DCP instance view)

Function

The **authentication-mode** command configures the authentication mode and password for an IP FPM instance.

The **undo authentication-mode** command deletes the authentication mode and password of an IP FPM instance.

By default, no authentication mode or password is configured for an IP FPM instance.

Format

authentication-mode hmac-sha256 key-id *key-id* [**cipher**] *password*

undo authentication-mode hmac-sha256

Parameters

Parameter	Description	Value
hmac-sha256	Indicates the HMAC-SHA256 authentication algorithm to be used for packets sent from a DCP to an MCP.	-
key-id *key-id*	Specifies the key ID for the authentication password of an IP FPM instance.	The value is an integer ranging from 1 to 64.
cipher	Indicates that the authentication password is displayed in ciphertext.	-
password	Specifies the authentication password of an IP FPM instance.	The value is a string of case-sensitive characters without spaces. ● The value ranges from 1 to 255 for simple passwords. ● The value ranges from 32 to 392 for ciphertext passwords.

Views

IPFPM-DCP instance view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enhance network security and performance statistics reliability, run the **authentication-mode** command so that authentication is performed during IP FPM performance statistics. An MCP and its associated DCPs must have the same authentication mode and password configured. The MCP processes packets only from the authenticated DCPs.

Precautions

IP FPM supports only the HMAC-SHA256 authentication algorithm.

If no authentication mode or password is configured for an IP FPM instance on a DCP, the authentication mode and password configured for the DCP takes effect. If the authentication mode and password are configured in both the DCP view and IP FPM instance view, the configuration in the IP FPM instance view takes effect.

Example

Configure the authentication mode and password for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] authentication-mode hmac-sha256 key-id 1 cipher Huawei-123
```

Related Topics

21.4.17 instance (IPFPM-DCP view)

21.4.2 authentication-mode (IPFPM-MCP view)

21.4.4 color-flag

Function

The **color-flag** command configures color bits.

The **undo color-flag** command restores the default color bits.

By default, the sixth bit in the ToS field of the IPv4 packet header is used as the loss color bit; the seventh bit in the ToS field of the IPv4 packet header is used as the delay color bit; Bit 0 in the Flags field of the IPv4 packet header is used as the multicast color bit. Using the default configurations is recommended.

Format

color-flag loss-measure { **tos-bit** *tos-bit* | **flags-bit0** } **delay-measure** { **tos-bit** *tos-bit* | **flags-bit0** }

undo color-flag

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
loss-measure	Indicates IP Flow Performance Measurement (IP FPM) packet loss measurement.	-
tos-bit *tos-bit*	Specifies a bit from the third to seventh bits in the ToS field of the IPv4 packet header as a color bit.	The value is an integer ranging from 3 to 7.
flags-bit0	Specifies Bit 0 in the Flags field of the IPv4 packet header as a color bit.	-
delay-measure	Indicates IP FPM delay measurement.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using IP FPM to measure network performance, run the **color-flag** command to specify a bit as a color bit based on network planning.

Precautions

All DCPs associated with an MCP must have the same multicast color bit configured.

The loss, delay, and multicast color bits cannot use the same bit, and the bits used for loss, and delay must not have been used in other measurement tasks.

Example

Configure IP FPM color bits.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] color-flag loss-measure tos-bit 3 delay-measure tos-bit 4
```

Related Topics

21.4.25 nqa ipfpm dcp

 Copyright © Huawei Technologies Co., Ltd.

21.4.5 dcp

Function

The **dcp** command specifies a Data Collecting Point (DCP) ID for an IP Flow Performance Measurement (IP FPM) instance on a MCP.

The **undo dcp** command deletes a DCP ID from an IP FPM instance on an MCP.

By default, no DCP ID is specified for an IP FPM instance on an MCP.

Format

dcp *dcp-id*

undo dcp [*dcp-id*]

Parameters

Parameter	Description	Value
dcp-id	Specifies the DCP ID of an IP FPM instance on an MCP. **NOTE** If *dcp-id* is not specified, the **undo dcp** command deletes all DCP IDs from a specified IP FPM instance on an MCP.	This value is in dotted decimal notation.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An IP FPM instance contains one or more DCPs. To specify DCP IDs for an IP FPM instance after it is created on an MCP, run the **dcp** command so that the MCP can determine whether the statistics are reported from authenticated DCPs.

Prerequisites

The **instance** command has been run to configure an IP FPM instance on an MCP.

Precautions

The DCP ID specified for an IP FPM instance on an MCP must be the same as that configured in the **dcp id** command on a DCP.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify a DCP ID for IP FPM instance 1 on an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
[Huawei-nqa-ipfpm-mcp-instance-1] dcp 10.1.1.1
```

Related Topics

21.4.26 nqa ipfpm mcp
21.4.16 instance (IPFPM-MCP view)

21.4.6 dcp id

Function

The **dcp id** command configures a DCP ID.

The **undo dcp id** command deletes a DCP ID.

By default, no DCP ID is configured.

Format

dcp id *dcp-id*

undo dcp id

Parameters

Parameter	Description	Value
dcp-id	ID of a DCP in the IP Flow Performance Measurement (IP FPM) model. Using the Router ID of a device that is configured as a DCP as its DCP ID is recommended.	This value is in dotted decimal notation.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow communication between an MCP and a DCP, run the **dcp id** command to configure a DCP ID. After the DCP receives the statistics for an IP FPM instance from TLPs, the DCP encapsulates the statistics and the DCP ID to packets and

 Copyright © Huawei Technologies Co., Ltd.

sends the packets with the DCP ID as the source IP address. After the MCP receives the packets, it compares the DCP ID carried in the packets with that configured in the **dcp** command run on itself.

- If the two DCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.
- If the two DCP IDs are different, the MCP considers the packets invalid and discards them.

Precautions

The DCP ID configured in an IP FPM instance must be the same as that specified in the **dcp** command run on an MCP. Otherwise, the MCP associated with this DCP cannot process the statistics reported by the DCP.

Example

Configure a DCP ID.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] dcp id 10.1.1.1
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.23 mcp id

21.4.5 dcp

21.4.7 delay-measure enable two-way

Function

The **delay-measure enable two-way** command enables on-demand two-way delay measurement for an IP FPM instance.

The **undo delay-measure enable two-way** command disables on-demand two-way delay measurement for an IP FPM instance.

By default, on-demand two-way delay measurement of an IP FPM instance is disabled.

Format

delay-measure enable two-way tlp *tlp-id1* [*tlp-id2*] [**continual** | **time-range** { **5** | **10** | **15** | **30** }]

undo delay-measure enable two-way

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
tlp *tlp-id1*	Specifies the TLP in-point for on-demand two-way delay measurement.	The value is an integer ranging from 1 to 16777215.
tlp-id2	Specifies the TLP out-point for on-demand two-way delay measurement. **NOTE** Currently, delay measurement is enabled by default for TLP out-points on the AR. Therefore, when enabling delay measurement, you must specify *tlp-id1*. *tlp-id2* can be specified as needed.	The value is an integer ranging from 1 to 16777215.
continual	Enables the continuous packet loss measurement function.	-
time-range { **5** | **10** | **15** | **30** }	Specifies the statistical period for on-demand two-way delay measurement. The value is an integer that can be 5, 10, 15, or 30, in minutes. The default value is 10 min.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IP FPM performance statistics serve as a reliable reference for assessing IP network performance and therefore are useful for fault diagnosis and service statistics. To monitor two-way delay performance in a specified period or diagnose network faults and locate faulty nodes when network performance deteriorates, run the **delay-measure enable two-way** command.

Prerequisites

An IP FPM model has been established, including configuring a DCP and MCP, binding a TLP to a physical interface, and creating a target flow and IP FPM instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Before implementing two-way delay measurement, ensure that the target flow in the IP FPM instance is bidirectional.

After a device restart, on-demand two-way delay measurement does not take effect any more.

After a master/slave main control board switchover, the measurement can be properly performed only when clock synchronization is complete. Clock synchronization takes a long time. Therefore, you are advised to reconfigure on-demand two-way delay measurement.

Example

Enable on-demand two-way delay measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 200 out-point egress
[Huawei-nqa-ipfpm-dcp-instance-1] delay-measure enable two-way tlp 100 200 time-range 15
```

Enable proactive two-way delay measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 200 out-point egress
[Huawei-nqa-ipfpm-dcp-instance-1] delay-measure enable two-way tlp 100 200 continual
```

Related Topics

21.4.25 nqa ipfpm dcp
21.4.17 instance (IPFPM-DCP view)

21.4.8 description (IPFPM-DCP instance view)

Function

The **description** command configures the description for an IP FPM instance.

The **undo description** command deletes the description of an IP FPM instance.

By default, no description is configured for an IP FPM instance.

Format

description *text*

undo description

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
text	Specifies the description of an IP FPM instance.	The value is a string of 1 to 64 case-sensitive characters, spaces supported.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help understand the services monitored by an IP FPM instance and the functions of the instance, run the **description** command to configure the description that shows detailed functions of the instance.

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. Configuring the description for an IP FPM instance is recommended in the following situations:

- Many IP FPM instances are configured, and their functions cannot be clearly identified.
- An IP FPM instance is used at a long interval, and its function may be left forgotten.

Precautions

If an IP FPM instance is configured but does not have a description, it may be misused.

Example

Configure the description for IP FPM instance 1.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] description NanJinToHeFei
```

Related Topics

21.4.9 description (IPFPM-MCP instance view)

 Copyright © Huawei Technologies Co., Ltd.

21.4.9 description (IPFPM-MCP instance view)

Function

The **description** command configures the description for an IP FPM instance.

The **undo description** command deletes the description of an IP FPM instance.

By default, no description is configured for an IP FPM instance.

Format

description *text*

undo description

Parameters

Parameter	Description	Value
text	Specifies the description of an IP FPM instance.	The value is a string of 1 to 64 case-sensitive characters, spaces supported.

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To help understand the services monitored by an IP FPM instance and the functions of the instance, run the **description** command to configure the description that shows detailed functions of the instance.

An IP FPM instance is identified by an integer ID, and therefore its functions are not easy to understand. Configuring the description for an IP FPM instance is recommended in the following situations:

- Many IP FPM instances are configured, and their functions cannot be clearly identified.
- An IP FPM instance is used at a long interval, and its function may be left forgotten.

Precautions

If an IP FPM instance is configured but does not have a description, it may be misused.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure the description for IP FPM instance 1.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
[Huawei-nqa-ipfpm-mcp-instance-1] description NanJinToHeFei
```

Related Topics

21.4.8 description (IPFPM-DCP instance view)

21.4.10 display ipfpm dcp

Function

The **display ipfpm dcp** command displays DCP configurations.

Format

display ipfpm dcp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether DCP configurations are correct, run the **display ipfpm dcp** command.

Example

Display DCP configurations.

```
<Huawei> display ipfpm dcp
Specification Information(Main Board):
 Max Instance Number                    :521
 Max 10s Instance Number                :521
 Max TLP Number                         :521
 Max TLP Number Per Instance            :8

Configuration Information:
 DCP ID                          : --
 Loss-measure Flag               : tos-bit6(default)
 Delay-measure Flag              : tos-bit7(default)
 Authentication Mode             : hmac-sha256
 Test Instances MCP ID           : --
```


Copyright © Huawei Technologies Co., Ltd.

```
Test Instances MCP Port          :  65030(default)
Current Instance Number           : 1
```

Table 21-26 Description of the **display ipfpm dcp** command output

Item	Description
Specification Information(Main Board)	Specifications for the main control board
Max Instance Number	Maximum number of IP FPM instances supported by the main control board
Max 10s Instance Number	Maximum number of IP FPM instances with the period of 10 seconds supported by the main control board
Max TLP Number	Maximum number of TLPs supported by the main control board
Max TLP Number Per Instance	Maximum number of TLPs supported by each IP FPM instance on the main control board
Configuration Information	DCP configurations
DCP ID	Data Collecting Point ID
Loss-measure Flag	Packet loss color bit: ● tos-bit3: third bit in the ToS field of the IPv4 packet header ● tos-bit4: fourth bit in the ToS field of the IPv4 packet header ● tos-bit5: fifth bit in the ToS field of the IPv4 packet header ● tos-bit6: sixth bit in the ToS field of the IPv4 packet header ● tos-bit7: seventh bit in the ToS field of the IPv4 packet header ● flag-bit0: Bit 0 in the Flags field of the IPv4 packet header

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Delay-measure Flag	Delay color bit: ● tos-bit3: third bit in the ToS field of the IPv4 packet header ● tos-bit4: fourth bit in the ToS field of the IPv4 packet header ● tos-bit5: fifth bit in the ToS field of the IPv4 packet header ● tos-bit6: sixth bit in the ToS field of the IPv4 packet header ● tos-bit7: seventh bit in the ToS field of the IPv4 packet header ● flag-bit0: Bit 0 in the Flags field of the IPv4 packet header
Authentication Mode	Authentication mode for the DCP: ● hmac-sha256: HMAC-SHA256 authentication ● --: non-authentication
Test Instances MCP ID	Measurement Control Point ID in the IP FPM instance
Test Instances MCP Port	User Datagram Protocol port number used by the DCP to communicate with the MCP in the IP FPM instance
Current Instance Number	Number of IP FPM instances

Related Topics

21.4.11 display ipfpm mcp

21.4.11 display ipfpm mcp

Function

The **display ipfpm mcp** command displays MCP configurations.

Format

display ipfpm mcp

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether MCP configurations are correct, run the **display ipfpm mcp** command.

Example

Display MCP configurations.

```
<Huawei> display ipfpm mcp
Specification Information:
 Max Instance Number                    :128
 Max DCP Number Per Instance            :128

Configuration Information:
 MCP ID                                 :--
 Status                                 :Active
 Protocol Port                          :65030(default)
 Current Instance Number                :2
```

Table 21-27 Description of the **display ipfpm mcp** command output

Item	Description
Specification Information	Specifications for the MCP
Max Instance Number	Maximum number of IP FPM instances supported by the MCP
Max DCP Number Per Instance	Maximum number of DCPs supported by each IP FPM instance on the MCP
Configuration Information	MCP configurations
MCP ID	Measurement Control Point ID
Status	MCP status: ● Active ● Deleting
Protocol Port	UDP port number used for the MCP to communicate with DCPs
Total Instances	Number of IP FPM instances

Related Topics

21.4.10 display ipfpm dcp

Copyright © Huawei Technologies Co., Ltd.

21.4.12 display ipfpm instance application

Function

The **display ipfpm instance application** command displays the relationship between IP FPM instances and applications.

Format

display ipfpm instance application

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

You can run this command to view the relationship between IP FPM instances and applications.

Precautions

Before running the **display ipfpm instance application** command, you need to run the **flow application** *application-name* command first to configure application matching information of the target flow.

Example

Display the relationship between IP FPM instances and applications.

```
<Huawei> display ipfpm instance application
-----------------------------------------------------------------------------
 Index          InstanceId          APPid            APPName
-----------------------------------------------------------------------------
  1               1                3559             DBank
  2               2                101             QQHuaXia
  3               3                3560             DBankSync
-----------------------------------------------------------------------------
```

Table 21-28 Description of the **display ipfpm instance application** command output

Item	Description
Index	Index of a test record.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
InstanceId	ID of an instance.
APPid	ID of an application.
APPName	Name of an application.

Related Topics

21.4.15 flow (IPFPM-DCP instance view)

21.4.13 display ipfpm statistic-type

Function

The **display ipfpm statistic-type** command displays performance statistics for an IP FPM instance.

Format

display ipfpm statistic-type { **loss** | **twoway-delay** } **instance** *instance-id*

Parameters

Parameter	Description	Value
loss	Displays packet loss statistics.	-
twoway-delay	Displays two-way delay statistics.	-
instance *instance-id*	Specifies an IP FPM instance ID.	The value is an integer ranging from 1 to 16777214.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To check the number of discarded packets, packet loss rate, one-way and two-way delay statistics, and jitter of an IP FPM instance, run the **display ipfpm statistic-**

 Copyright © Huawei Technologies Co., Ltd.

type command. To locate and diagnose network faults when network performance deteriorates, run the **display ipfpm statistic-type** command with **ach** configured to check statistics for a specified ACH.

Precautions

This command is valid only on MCPs.

The first statistics collected may not be accurate, therefore, using subsequent statistics as a reference for network performance is recommended.

The precision of NTP clock synchronization is different from that of IP FPM measurement. As a result, the data reported by IP FPM may be inaccurate and a negative number may be generated.

Example

Display the packet loss statistics for IP FPM instance 1 on an MCP.

```
<Huawei> display ipfpm statistic-type loss instance 1
Latest loss statistics of forward flow:
Unit: p - packet, b - byte
-----------------------------------------------------------------------------------------
 Period          Loss(p)          LossRatio(p)  Loss(b)          LossRatio(b)
-----------------------------------------------------------------------------------------
 136118757         20                20.000000% 2000               20.000000%
 136118756         20                20.000000% 2000               20.000000%
 136118755         20                20.000000% 2000               20.000000%
 136118753         20                20.000000% 2000               20.000000%
 136118752         20                20.000000% 2000               20.000000%
 136118751         20                20.000000% 2000               20.000000%
 136118750         20                20.000000% 2000               20.000000%
 136118749         20                20.000000% 2000               20.000000%
 136118748         20                20.000000% 2000               20.000000%
 136118747         20                20.000000% 2000               20.000000%
 136118746         20                20.000000% 2000               20.000000%
 136118745         20                20.000000% 2000               20.000000%

Latest loss statistics of backward flow:
Unit: p - packet, b - byte
-----------------------------------------------------------------------------------------
 Period          Loss(p)          LossRatio(p)  Loss(b)          LossRatio(b)
-----------------------------------------------------------------------------------------
 136118757         20                20.000000% 2000               20.000000%
 136118756         20                20.000000% 2000               20.000000%
 136118755         20                20.000000% 2000               20.000000%
 136118753         20                20.000000% 2000               20.000000%
 136118752         20                20.000000% 2000               20.000000%
 136118751         20                20.000000% 2000               20.000000%
 136118750         20                20.000000% 2000               20.000000%
 136118749         20                20.000000% 2000               20.000000%
 136118748         20                20.000000% 2000               20.000000%
 136118747         20                20.000000% 2000               20.000000%
 136118746         20                20.000000% 2000               20.000000%
 136118745         20                20.000000% 2000               20.000000%
```

Display the two-way delay statistics for IP FPM instance 1 on an MCP.

```
<Huawei> display ipfpm statistic-type twoway-delay instance 1
Latest two-way delay statistics:
-------------------------------------------------
 Period          Delay(usec) Delay
                             Variation(usec)
-------------------------------------------------
 136118757         800         0
 136118756         800         0
```

 Copyright © Huawei Technologies Co., Ltd.

```
 136118755          800        0
 136118753          800        0
 136118752          800        0
 136118751          800        0
 136118750          800        0
 136118749          800        0
 136118748          800        0
 136118747          800        0
 136118746          800        0
 136118745          800        0

Latest one-way delay statistics of bidirectional flow:
-------------------------------------------------------------------------------
 Period             Forward     ForwardDelay    Backward    BackwardDelay
                  Delay(usec) Variation(usec) Delay(usec) Variation(usec)
-------------------------------------------------------------------------------
 136118757          400        0            400        0
 136118756          400        0            400        0
 136118755          400        0            400        0
 136118753          400        0            400        0
 136118752          400        0            400        0
 136118751          400        0            400        0
 136118750          400        0            400        0
 136118749          400        0            400        0
 136118748          400        0            400        0
 136118747          400        0            400        0
 136118746          400        0            400        0
 136118745          400        0            400        0
```

Table 21-29 Description of the **display ipfpm statistic-type** command output

Item	Description
Period	Statistical period ID
Loss(p)	Number of discarded packets
LossRatio(p)	Packet loss rate
Loss(b)	Number of discarded bytes
LossRatio(b)	Byte loss rate
Delay(usec)	Delay, in microseconds
DelayVariation(usec)	Jitter, in microseconds
ForwardDelay(usec)	Delay for the forward delay, in microseconds
ForwardDelayVariation(usec)	Jitter for the forward delay, in microseconds
BackwardDelay(usec)	Delay for the backward delay, in microseconds
BackwardDelayVariation(usec)	Jitter for the backward delay, in microseconds

Copyright © Huawei Technologies Co., Ltd.

21.4.14 display snmp-agent trap feature-name ipfpm all

Function

The **display snmp-agent trap feature-name ipfpm all** command displays configurations of all alarm functions of the IP FPM module.

Format

display snmp-agent trap feature-name ipfpm all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To check whether the alarm functions of the IP FPM module are enabled, run the **display snmp-agent trap feature-name ipfpm all** command.

Example

Display configurations of all alarm functions of the IP FPM module.

```
<Huawei> display snmp-agent trap feature-name ipfpm all
-------------------------------------------------------------------------------
Feature name: IPFPM
Trap number : 8
-------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
hwIpfpmLossRatioExceed          off                     off
hwIpfpmLossRatioRecovery        off                     off
hwIpfpmOneDelayExceed           off                     off
hwIpfpmOneDelayRecovery         off                     off
hwIpfpmTwoDelayExceed           off                     off
hwIpfpmTwoDelayRecovery         off                     off
hwIpfpmTlpExceed                off                     off
hwIpfpmTlpRecovery              off                     off
```

Table 21-30 Description of the **display snmp-agent trap feature-name ipfpm all** command output

Item	Description
Feature name	Name of the module to which the alarms are related
Trap number	Number of alarms

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trap name	Names of alarms related to the IP FPM module: • hwIpfpmLossRatioExceed: packet loss alarm • hwIpfpmLossRatioRecovery: packet loss clear alarm • hwIpfpmOneDelayExceed: one-way delay alarm • hwIpfpmOneDelayRecovery: one-way delay clear alarm • hwIpfpmTwoDelayExceed: two-way delay alarm • hwIpfpmTwoDelayRecovery: two-way delay clear alarm • hwIpfpmTlpExceed: TLPs threshold-crossing alarm • hwIpfpmTlpRecovery: TLPs threshold-crossing clear alarm
Default switch status	Default alarm status • on: The alarm function is enabled. • off: The alarm function is disabled.
Current switch status	Current alarm status • on: The alarm function is enabled. • off: The alarm function is disabled.

Related Topics

21.4.28 snmp-agent trap enable feature-name ipfpm

21.4.15 flow (IPFPM-DCP instance view)

Function

The **flow** command configures the target flow characteristics for an IP FPM instance.

The **undo flow** command deletes the target flow characteristics of an IP FPM instance.

By default, no characteristics are configured for the target flow of an IP FPM instance.

Format

flow forward { **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] | **protocol** { { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | *protocol-number* } } *

flow backward { **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] | **protocol** { { **tcp** | **udp** }

 Copyright © Huawei Technologies Co., Ltd.

{ **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | *protocol-number* } } *

flow bidirectional { **dscp** *dscp-value* | **source** *src-ip-address* [*src-mask-length*] | **destination** *dest-ip-address* [*dest-mask-length*] | **protocol** { { **tcp** | **udp** } { **source-port** *src-port-number1* [**to** *src-port-number2*] | **destination-port** *dest-port-number1* [**to** *dest-port-number2*] } * | *protocol-number* } } *

flow application *application-name*

undo flow { **forward** | **backward** | **bidirectional** | **application** }

Parameters

Parameter	Description	Value
forward	Indicates the forward target flow.	-
backward	Indicates the backward target flow.	-
bidirectional	Indicates the symmetrical bidirectional target flow. **NOTE** If the target flow is symmetrical bidirectional, set *src-ip-address* to specify a source IP address and *dest-ip-address* to specify a destination IP address for the target flow.	-
application	Specifies the application protocol of the target flow.	-
dscp *dscp-value*	Specifies the DSCP value of the target flow.	The value is an integer ranging from 0 to 63.
source *src-ip-address*	Specifies the source IP address of the target flow.	This value is in dotted decimal notation.
src-mask-length	Specifies the mask length of the source IP address of the target flow.	The value is an integer ranging from 1 to 32.
destination *dest-ip-address*	Specifies the destination IP address of the target flow.	This value is in dotted decimal notation.
dest-mask-length	Specifies the mask length of the destination IP address of the target flow.	The value is an integer ranging from 1 to 32.
protocol	Indicates the protocol type of the target flow.	-
tcp	Indicates that the protocol type of the target flow is TCP.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
udp	Indicates that the protocol type of the target flow is UDP.	-
source-port *src-port-number1*	Specifies the start source port number of the target flow.	The value is an integer ranging from 1 to 65535.
src-port-number2	Specifies the end source port number of the target flow.	The value is an integer ranging from 1 to 65535. *src-port-number2* must be greater than *src-port-number1*.
destination-port *dest-port-number1*	Specifies the start destination port number of the target flow.	The value is an integer ranging from 1 to 65535.
dest-port-number2	Specifies the end destination port number of the target flow.	The value is an integer ranging from 1 to 65535. *dest-port-number2* must be greater than *dest-port-number1*.
protocol-number	Indicates the protocol number of the target flow.	The value is an integer ranging from 1 to 5, 7 to 16, or 18 to 255. **NOTE** The value 6 indicates TCP, and the value 17 indicates UDP.
application-name	Specifies the name of the application protocol.	The value is a string of characters without spaces. The value depends on application protocols in the signature database.

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

One or more fields in IP headers can be specified to identify target flows. The field can be the source IP address or prefix, destination IP address or prefix, protocol type, source port number, destination port number, or ToS. The more fields specified, the more accurately flows can be identified. Specifying as many fields as possible is recommended to maximize the measurement accuracy.

 Copyright © Huawei Technologies Co., Ltd.

To define target flows and ensure measurement accuracy, run the **flow** command to configure target flow characteristics.

Configuration Impact

An IP FPM instance can have only one target flow configured, either unidirectional or bidirectional. A bidirectional target flow is logically two unidirectional flows in opposite directions.

- If the target flow in an IP FPM instance is bidirectional, two situations are available:
  - If the bidirectional target flow is symmetrical, you can specify **bidirectional** to configure the bidirectional target flow characteristics. By default, the characteristics specified are used for the forward flow, and the reverse of those are used for the backward flow. Specifically, the source and destination IP addresses and port numbers specified for the forward flow are used respectively as the destination and source IP addresses and port numbers for the backward flow.
  - If the bidirectional target flow is asymmetrical, you must configure **forward** and **backward** in two command instances to configure the forward and backward flow characteristics.

Precautions

Target flows in different IP FPM instances cannot have the same characteristics. The forward and backward target flows in an IP FPM instance cannot have the same characteristics neither.

To make the application protocol of the target flow configured for a specified **application** in an IP FPM instance take effect, you need to specify **bidirectional**, **forward**, or **backward** to configure any flow characteristic of bidirectional target flow, forward target flow, and backward target flow. In addition, you need to run the **sa application-statistic enable** command on the interface to enable SAC before using the IP FPM function.

Example

Configure the target flow characteristics for IP FPM instance 1.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] flow bidirectional source 1.1.1.1 destination 2.2.2.2
```

Related Topics

21.4.25 nqa ipfpm dcp
21.4.17 instance (IPFPM-DCP view)

21.4.16 instance (IPFPM-MCP view)

Function

The **instance** command creates an IP FPM instance on a Measurement Control Point (MCP) and displays the instance view.

The **undo instance** command deletes an IP FPM instance of an MCP.

 Copyright © Huawei Technologies Co., Ltd.

By default, no IP FPM instance is created on MCPs.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IP FPM instance.	The value is an integer ranging from 1 to 8355838.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement IP FPM performance statistics on a specified service flow, run the **instance** command to create an IP FPM instance. Each IP FPM instance is composed of a target flow, TLPs, and a statistical period.

Precautions

The IP FPM instance ID must be unique on an MCP and all its associated DCPs.

An MCP and all its associated DCPs must have the same IP FPM instance configured. Otherwise, statistics collection does not take effect.

Example

Create an IP FPM instance on an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
```

Related Topics

21.4.26 nqa ipfpm mcp

21.4.9 description (IPFPM-MCP instance view)

21.4.17 instance (IPFPM-DCP view)

 Copyright © Huawei Technologies Co., Ltd.

21.4.17 instance (IPFPM-DCP view)

Function

The **instance** command creates an IP FPM instance on a DCP and displays the instance view.

The **undo instance** command deletes an IP FPM instance of a DCP.

By default, no IP FPM instance is created on DCPs.

Format

instance *instance-id*

undo instance *instance-id*

Parameters

Parameter	Description	Value
instance-id	Specifies the ID of an IP FPM instance.	The value is an integer ranging from 1 to 8355838.

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To implement IP FPM performance statistics on a specified service flow, run the **instance** command to create an IP FPM instance. Each IP FPM instance is composed of a target flow, TLPs, and a statistical period.

Follow-up Procedure

Run the following commands to configure parameters for the configured IP FPM instance.

- Run the **flow** command to configure target flow characteristics.
- Run the **tlp** command to configure a TLP.
- Run the **interval** command to configure the statistical period.

Precautions

The IP FPM instance ID must be unique on an MCP and all its associated DCPs.

An MCP and all its associated DCPs must have the same IP FPM instance configured. Otherwise, statistics collection does not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Create an IP FPM instance on a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.8 description (IPFPM-DCP instance view)

21.4.16 instance (IPFPM-MCP view)

21.4.15 flow (IPFPM-DCP instance view)

21.4.29 tlp

21.4.18 interval

21.4.18 interval

Function

The **interval** command configures the statistical period for an IP FPM instance.

The **undo interval** command restores the default statistical period of an IP FPM instance.

By default, the statistical period is 10s.

Format

interval { **10** | **60** | **600** }

undo interval

Parameters

Parameter	Description	Value
10	Specifies the statistical period for an IP FPM instance as 10s.	-
60	Specifies the statistical period for an IP FPM instance as 60s.	-
600	Specifies the statistical period for an IP FPM instance as 600s.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To implement IP FPM performance statistics and ensure measurement accuracy, run the **interval** command to configure a statistical period based on the clock offset, maximum transmission delay, and system performance.

The statistical period of an IP FPM instance is a period of time from when TLPs measure the number of packets or bytes to when DCPs report the statistics to an MCP and the MCP calculates the measurement result.

The shorter the statistical period, the more frequent DCPs report the statistics to the MCP, and the more statistics the DCPs and MCP will process. Therefore, the statistical period change will affect the system performance of the DCPs and MCP.

Configuration Impact

If the statistical period of an IP FPM instance is changed, it must be changed for all DCPs of this IP FPM instance. Otherwise, statistics collection does not take effect.

Precautions

To ensure statistics accuracy, before you change the statistical period of an IP FPM instance, disabling packet loss or delay measurement in the instance view is recommended.

Example

Configure the statistical period for IP FPM instance 1 as 60s.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] interval 60
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.17 instance (IPFPM-DCP view)

21.4.15 flow (IPFPM-DCP instance view)

21.4.7 delay-measure enable two-way

21.4.19 ipfpm tlp (layer 3 interface)

Function

The **ipfpm tlp** command binds a Target Logical Port (TLP) to an interface.

The **undo ipfpm tlp** command unbinds a TLP from an interface.

By default, a TLP is not bound to any interface.

Format

ipfpm tlp *tlp-id*

 Copyright © Huawei Technologies Co., Ltd.

undo ipfpm tlp { *tlp-id* | **all** }

Parameters

Parameter	Description	Value
tlp-id	Specifies a TLP ID.	The value is an integer ranging from 1 to 16777215.
all	Unbinds TLP from all interfaces in the IP FPM statistical system.	-

Views

interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before implementing IP FPM performance statistics, ensure that TLPs are bound to interfaces.

Precautions

A TLP can be bound to only one interface on the DCPs associated with an MCP.

Example

Bind the interface GigabitEthernet0/0/0 to TLP 100.

```
<Huawei> system-view
[Huawei] interface Gigabitethernet0/0/0
[Huawei-GigabitEthernet0/0/0] ipfpm tlp 100
```

Related Topics

21.4.29 tlp

21.4.20 loss-measure enable

Function

The **loss-measure enable** command enables on-demand packet loss measurement for an IP FPM instance.

The **undo loss-measure enable** command disables on-demand packet loss measurement for an IP FPM instance.

By default, on-demand packet loss measurement is disabled for an IP FPM instance.

 Copyright © Huawei Technologies Co., Ltd.

Format

loss-measure enable [**continual** | **time-range** { **5** | **10** | **15** | **30** }]

undo loss-measure enable [**continual** | **time-range** { **5** | **10** | **15** | **30** }]

Parameters

Parameter	Description	Value
continual	Enables the continuous packet loss measurement function.	-
time-range { **5** | **10** | **15** | **30** }	Specifies the statistical period for on-demand packet loss measurement. The value is an integer that can be 5, 10, 15, or 30, in minutes. The default value is 10min.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The IP FPM performance statistics serve as a reliable reference for assessing IP network performance and therefore are useful for fault diagnosis and service statistics. To monitor on-demand packet loss performance in a specified period or diagnose network faults and locate faulty nodes when network performance deteriorates, run the **loss-measure enable** command.

Prerequisites

An IP FPM model has been established, including configuring a DCP and MCP, binding a TLP to a physical interface, and creating a target flow and IP FPM instance.

Precautions

After a device restart, on-demand packet loss measurement does not take effect any more.

After a master/slave main control board switchover, the measurement can be properly performed only when clock synchronization is complete. Clock synchronization takes a long time. Therefore, you are advised to reconfigure on-demand packet loss measurement.

On-demand packet loss measurement cannot be enabled together with continuous packet loss measurement. If the continuous packet loss measurement

 Copyright © Huawei Technologies Co., Ltd.

function is enabled first, on-demand packet loss measurement can be enabled successfully only when the **undo loss-measure enable continual** command is run.

Example

Enable on-demand packet loss measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] loss-measure enable time-range 30
```

Enable proactive packet loss measurement for an IP FPM instance.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] loss-measure enable continual
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.17 instance (IPFPM-DCP view)

21.4.21 mcp (IPFPM-DCP instance view)

Function

The **mcp** command specifies a Measurement Control Point (MCP) ID for an IP Flow Performance Measurement (IP FPM) instance on a Data Collecting Point (DCP).

The **undo mcp** command deletes the MCP ID of an IP FPM instance on a DCP.

By default, no MCP ID is specified for an IP FPM instance on a DCP.

Format

mcp *mcp-id* [**port** *port-number*] [**vpn-instance** *vpn-instance-name* | **net-manager-vpn**]

undo mcp

Parameters

Parameter	Description	Value
mcp-id	Specifies an MCP ID for an IP FPM instance on a DCP. Using the Router ID of a device that is configured as an MCP as its MCP ID is recommended.	This value is in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port *port-number*	Specifies a UDP port number for a DCP to communicate with an MCP.	The value is an integer ranging from 1024 to 65535. The default value is 65030 and is recommended.
vpn-instance *vpn-instance-name*	Specifies a VPN instance for a DCP to communicate with an MCP.	The name is a string of 1 to 31 case-sensitive characters without any spaces.
net-manager-vpn	Specifies a management VPN for a DCP to communicate with an MCP.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a DCP in an IP FPM instance to report the statistics collected by TLPs to an MCP, run the **mcp** command to specify the MCP ID for the DCP in this instance.

Prerequisites

The **instance** command has been run to configure an IP FPM instance.

NOTE

The VPN instance has been created on the DCP before you configure **vpn-instance** *vpn-instance-name* or **net-manager-vpn** to allow the DCP to report the statistics to the MCP through the specified VPN or management VPN.

Implementation

After receiving the statistics for an IP FPM instance from TLPs, a DCP encapsulates the statistics and the MCP ID in the IP FPM instance to packets and sends the packets to the destination IP address identified by the MCP ID. After the MCP receives the packets, it compares the MCP ID carried in the packets with that configured in the **mcp id** command run on itself.

- If the two MCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.
- If the two MCP IDs are different, the MCP considers the packets invalid and discards them.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

The MCP ID must be an IP address reachable to the DCPs. The MCP ID specified for an IP FPM instance on a DCP must be the same as that specified in the **mcp id** command run on the MCP associated with this DCP.

The UDP port number configured on the DCP must be the same as that configured in the **protocol udp port** command run on the MCP associated with this DCP. Otherwise, the DCP cannot report the statistics to the MCP.

Example

Specify the MCP ID for IP FPM instance 1 on a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] mcp 10.1.1.1
```

Specify the MCP ID for IP FPM instance 1 on a DCP and configure the DCP to send statistics to the MCP through the VPN instance **vpnforipfpm**.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] mcp 10.1.1.1 vpn-instance vpnforipfpm
```

21.4.22 mcp (IPFPM-DCP view)

Function

The **mcp** command specifies a MCP ID for all IP FPM instances on a DCP.

The **undo mcp** command deletes the MCP ID of all IP FPM instances on a DCP.

By default, no MCP ID is specified for IP FPM instances on a DCP.

Format

mcp *mcp-id* [**port** *port-number*] [**vpn-instance** *vpn-instance-name* | **net-manager-vpn**]

undo mcp

Parameters

Parameter	Description	Value
mcp-id	Specifies an MCP ID for all IP FPM instances on a DCP. Using the Router ID of a device that is configured as an MCP as its MCP ID is recommended.	This value is in dotted decimal notation.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port *port-number*	Specifies a UDP port number for a DCP to communicate with an MCP.	The value is an integer ranging from 1024 to 65535. The default value is 65030 and is recommended.
vpn-instance *vpn-instance-name*	Specifies a VPN instance for a DCP to communicate with an MCP.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
net-manager-vpn	Specifies a management VPN for a DCP to communicate with an MCP.	-

Views

IPFPM-DCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a DCP in an IP FPM instance to report the statistics collected by TLPs to an MCP, run the **mcp** command to specify the MCP ID for all IP FPM instances on the DCP.

Prerequisites

The **nqa ipfpm dcp** command has been run to enable DCP globally.

NOTE

The VPN instance has been created on the DCP before you configure **vpn-instance** *vpn-instance-name* or **net-manager-vpn** to allow the DCP to report the statistics to the MCP through the specified VPN or management VPN.

Implementation

After receiving the statistics for all IP FPM instances from TLPs, a DCP encapsulates the statistics and the MCP ID in the IP FPM instances to packets and sends the packets to the destination IP address identified by the MCP ID. After the MCP receives the packets, it compares the MCP ID carried in the packets with that configured in the **mcp id** command run on itself.

- If the two MCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.

 Copyright © Huawei Technologies Co., Ltd.

- If the two MCP IDs are different, the MCP considers the packets invalid and discards them.

Precautions

The MCP ID must be an IP address reachable to DCPs. The MCP ID specified for all IP FPM instances on a DCP must be the same as that specified in the **mcp id** command run on the MCP associated with this DCP.

The UDP port number configured on the DCP must be the same as that configured in the **protocol udp port** command run on the MCP associated with this DCP. Otherwise, the DCP cannot report the statistics to the MCP.

If the **mcp** command has been run in the IP FPM instance view for some instances on a DCP and an MCP ID is specified for all IP FPM instances on the DCP, the MCP ID specified in the IP FPM instance view takes effect.

Example

Specify the MCP ID for all IP FPM instances on a DCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] mcp 10.1.1.1
```

Specify the MCP ID for IP FPM instance 1 on a DCP and configure the DCP to send statistics to the MCP through the VPN instance **vpnforipfpm**.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] mcp 10.1.1.1 vpn-instance vpnforipfpm
```

Related Topics

21.4.25 nqa ipfpm dcp

21.4.27 protocol udp port

21.4.23 mcp id

21.4.23 mcp id

Function

The **mcp id** command configures an MCP ID.

The **undo mcp id** command deletes an MCP ID.

By default, no MCP ID is configured.

Format

mcp id *mcp-id*

undo mcp id

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mcp-id	Specifies an MCP ID. Using the Router ID of a device that is configured as an MCP as its MCP ID is recommended.	This value is in dotted decimal notation.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow communication between an MCP and a DCP, run the **mcp id** command to configure an MCP ID. After the DCP receives the statistics for an IP FPM instance from TLPs, the DCP encapsulates the statistics and the MCP ID specified by the **mcp** command run in the IP FPM instance to packets and sends the packets to the destination IP address identified by the MCP ID. After the MCP receives the packets, it compares the MCP ID carried in the packets with that configured in the **mcp id** command run on itself.

- If the two MCP IDs are the same, the MCP accepts the packets and summarizes and calculates the statistics.
- If the two MCP IDs are different, the MCP considers the packets invalid and discards them.

Precautions

The MCP ID must be an IP address reachable to DCPs. The MCP ID configured on an MCP must be the same as that specified in the **mcp** command run in the IP FPM instance view of all DCPs associated with this MCP. If an MCP ID is changed on an MCP, it must be changed for all DCPs associated with this MCP in an IP FPM instance. Otherwise, the MCP cannot process the statistics reported by the DCPs.

Example

Configure an MCP ID.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] mcp id 10.1.1.1
```

21.4.24 measure disable (IPFPM-MCP instance view)

 Copyright © Huawei Technologies Co., Ltd.

Function

The **measure disable** command disables IP FPM performance statistics collection of a specified instance on a MCP.

The **undo measure disable** and **measure enable** commands function the same to enable IP FPM performance statistics collection for a specified instance on an MCP.

By default, IP FPM performance statistics collection is enabled for instances on an MCP.

Format

measure disable

measure enable

undo measure disable

Parameters

None

Views

IPFPM-MCP instance view

Default Level

2: Configuration level

Usage Guidelines

When DCP configurations are being changed, the MCP may receive incorrect statistics from the DCP. To prevent this, run the **measure disable** command to disable IP FPM performance statistics collection of a specified instance on the MCP. After the DCP configuration change is complete, run the **undo measure disable** or **measure enable** command to enable IP FPM performance statistics collection for the specified instance on the MCP. This ensures accurate measurement.

Example

Disable IP FPM performance statistics collection of a specified instance on an MCP.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] instance 1
[Huawei-nqa-ipfpm-mcp-instance-1] measure disable
```

Related Topics

21.4.26 nqa ipfpm mcp

 Copyright © Huawei Technologies Co., Ltd.

21.4.25 nqa ipfpm dcp

Function

The **nqa ipfpm dcp** command enables DCP globally and displays the IPFPM-DCP view.

The **undo nqa ipfpm dcp** command disables DCP globally.

By default, DCP is disabled globally.

Format

nqa ipfpm dcp

undo nqa ipfpm dcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable DCP globally so that IP FPM performance statistics can be implemented, run the **nqa ipfpm dcp** command. A DCP manages and controls TLPs, collects statistics generated by TLPs, and reports the statistics to an MCP.

Follow-up Procedure

Run the **dcp id** command to configure a DCP ID.

Precautions

DCP and MCP functionalities can be configured on the same device.

Example

Enable DCP globally and display the IPFPM-DCP view.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
```

Related Topics

21.4.6 dcp id

21.4.26 nqa ipfpm mcp

 Copyright © Huawei Technologies Co., Ltd.

21.4.26 nqa ipfpm mcp

Function

The **nqa ipfpm mcp** command enables Measurement Control Point (MCP) globally and displays the IPFPM-MCP view.

The **undo nqa ipfpm mcp** command disables MCP globally.

By default, MCP is enabled globally.

Format

nqa ipfpm mcp

undo nqa ipfpm mcp

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable MCP globally so that IP FPM performance statistics can be implemented, run the **nqa ipfpm mcp** command. An MCP collects statistics reported by DCPs, summarizes and calculates the statistics, and reports measurement results to user terminals or the NMS.

Follow-up Procedure

Run the **mcp id** command to configure an MCP ID.

Precautions

MCP and DCP functionalities can be configured on the same device.

Example

Enable MCP globally and display the IPFPM-MCP view.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
```

Related Topics

21.4.23 mcp id

 Copyright © Huawei Technologies Co., Ltd.

21.4.25 nqa ipfpm dcp

21.4.27 protocol udp port

Function

The **protocol udp port** command configures an User Datagram Protocol (UDP) port number for a MCP to communicate with DCPs.

The **undo protocol udp port** command restores the default UDP port number for an MCP to communicate with DCPs.

By default, an MCP uses UDP port 65030 to communicate with DCPs.

Format

protocol udp port *port-number*

undo protocol udp port

Parameters

Parameter	Description	Value
port-number	Specifies the UDP port number for an MCP to communicate with DCPs.	The value is an integer ranging from 1024 to 65535.

Views

IPFPM-MCP view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, an MCP uses UDP port 65030 to communicate with DCPs. To change the default UDP port number for an MCP to communicate with DCPs, run the **protocol udp port** command.

Precautions

The UDP port number configured on an MCP must be the same as that specified in the **mcp** command run in the IP FPM instance view of all DCPs associated with this MCP. If a UDP port number is changed on an MCP, it must be changed for all DCPs associated with this MCP in an IP FPM instance. Otherwise, the MCP cannot process the statistics reported by the DCPs.

 Copyright © Huawei Technologies Co., Ltd.

Example

Specify UDP port 1024 for an MCP to communicate with DCPs.

```
<Huawei> system-view
[Huawei] nqa ipfpm mcp
[Huawei-nqa-ipfpm-mcp] protocol udp port 1024
```

Related Topics

21.4.23 mcp id

21.4.26 nqa ipfpm mcp

21.4.25 nqa ipfpm dcp

21.4.28 snmp-agent trap enable feature-name ipfpm

Function

The **snmp-agent trap enable feature-name ipfpm** command enables the alarm function for the IP FPM module.

The **undo snmp-agent trap enable feature-name ipfpm** command disables the alarm function of the IP FPM module.

By default, the alarm function of the IP FPM module is disabled.

Format

snmp-agent trap enable feature-name ipfpm [**trap-name** { **hwipfpmlossratioexceed** | **hwipfpmlossratiorecovery** | **hwipfpmonedelayexceed** | **hwipfpmonedelayrecovery** | **hwipfpmtwodelayexceed** | **hwipfpmtwodelayrecovery** | **hwipfpmtlpexceed** | **hwipfpmtlprecovery**}]

undo snmp-agent trap enable feature-name ipfpm [**trap-name** { **hwipfpmlossratioexceed** | **hwipfpmlossratiorecovery** | **hwipfpmonedelayexceed** | **hwipfpmonedelayrecovery** | **hwipfpmtwodelayexceed** | **hwipfpmtwodelayrecovery** | **hwipfpmtlpexceed** | **hwipfpmtlprecovery**}]

Parameters

Parameter	Description	Value
trap-name	Indicates the alarm function for a specific type of event.	-
hwipfpmlossratioexceed	Indicates the packet loss alarm function.	-
hwipfpmlossratiorecovery	Indicates the packet loss clear alarm function.	-
hwipfpmonedelayexceed	Indicates the one-way delay alarm.	-
hwipfpmonedelayrecovery	Indicates the one-way delay clear alarm.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwipfpmtwodelayexceed	Indicates the two-way delay alarm.	-
hwipfpmtwodelayrecovery	Indicates the two-way delay clear alarm.	-
hwipfpmtlpexceed	Indicates the TLPs threshold-crossing alarm.	-
hwipfpmtlprecovery	Indicates the TLPs threshold-crossing clear alarm.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To allow a device to use SNMP to report IP FPM alarms to the NMS, run the **snmp-agent trap enable feature-name ipfpm** command to enable the alarm function. SNMP is a widely used network management protocol that collects network communication statistics using agent software embedded in managed devices.

Precautions

If you do not configure **trap-name** in the **snmp-agent trap enable feature-name ipfpm** command, the command enables all alarm functions for the IP FPM module. If **trap-name** is configured, a specific alarm function is enabled.

Example

Enable the two-way delay alarm.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name ipfpm trap-name hwipfpmtwodelayexceed
```

Related Topics

21.4.14 display snmp-agent trap feature-name ipfpm all

21.4.29 tlp

Function

The **tlp** command configures a Target Logical Port (TLP) for an IP FPM instance and specifies the TLP role.

The **undo tlp** command deletes a TLP of an IP FPM instance.

By default, no TLP is configured for an IP FPM instance.

 Copyright © Huawei Technologies Co., Ltd.

Format

tlp *tlp-id* { **in-point** | **out-point** } { **ingress** | **egress** }

undo tlp *tlp-id*

Parameters

Parameter	Description	Value
tlp-id	Specifies a TLP ID.	The value is an integer ranging from 1 to 16777215.
in-point	Specifies a TLP as an in-point. The system sets the measurement flags of target flows on an in-point.	-
ingress	Indicates the upstream target flow.	-
out-point	Specifies a TLP as an out-point. The system clears the measurement flags of target flows on an out-point.	-
egress	Indicates the downstream target flow.	-

Views

IPFPM-DCP instance view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To locate faults in IP FPM performance statistics scenarios, run the **tlp** command to configure TLPs in an IP FPM instance. TLPs are measurement points along the path of the target flow and compile and output the statistics. TLPs can be in-points, mid-points, or out-points.

Precautions

A TLP that functions as the in-point for the forward target flow is the out-point for the backward target flow. The TLP role specified in the **tlp** *tlp-id* { **in-point ingress** | **out-point egress** } command applies only to the forward target flow, and the reverse of the specified role is used for the backward target flow.

A TLP cannot function as both the in-point and out-point for the same unidirectional target flow.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a TLP for IP FPM instance 1 and specify the TLP role.

```
<Huawei> system-view
[Huawei] nqa ipfpm dcp
[Huawei-nqa-ipfpm-dcp] instance 1
[Huawei-nqa-ipfpm-dcp-instance-1] tlp 100 in-point ingress
```

Related Topics

21.4.25 nqa ipfpm dcp
21.4.17 instance (IPFPM-DCP view)
21.4.19 ipfpm tlp (layer 3 interface)

21.5 CWMP Configuration Commands

NOTE

The AR120 series (except AR129CV, AR129CVW and AR129CGVW-L) do not support CWMP.

21.5.1 cwmp

Function

The **cwmp** command displays the CWMP view.

Format

cwmp

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

On networks, too many devices are scattered on the user side and are hard to manage and maintain. To solve the preceding problems, CWMP defines a mechanism to manage the CPE by an ACS. This facilitates CPE management, reduces maintenance and operation costs, and improves troubleshooting efficiency.

The router functions as a CPE.

 Copyright © Huawei Technologies Co., Ltd.

Follow-up Procedure

Configure the CWMP function of the CPE.

Example

Enter the CWMP view.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp]
```

Related Topics

21.5.15 cwmp enable

21.5.2 cwmp acs password

Function

The **cwmp acs password** command configures the password used to connect the CPE to the ACS.

The **undo cwmp acs password** command deletes the password.

By default, no password is available.

Format

cwmp acs password cipher

undo cwmp acs password

Parameters

Parameter	Description	Value
cipher	Displays the password in cipher text.	-

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp acs password**

 Copyright © Huawei Technologies Co., Ltd.

command is used to configure the authentication password used to connect the CPE to the ACS.

After the CPE sends an Inform message containing a URL to the ACS, the ACS authenticates the CPE using the user name and password. After being authenticated, the CPE can set up a connection with the ACS.

Precautions

The passwords must meet the following requirements:

- The password is a string of 6 to 255 case-sensitive characters.
- The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character.

  The special characters include spaces and the following:

  `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Password entered in interactive mode is not displayed on the screen.

After an active/standby switchover on the AR3200 routers, you need to run this command again to set a password.

Example

Set the password to abc123456.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp acs password cipher
Enter Password(<6-255>):
Confirm password:
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

21.5.3 cwmp acs url

Function

The **cwmp acs url** command configures the URL used to connect the CPE to the ACS.

The **undo cwmp acs url** command deletes the URL.

By default, no URL is available.

Format

cwmp acs url *url*

undo cwmp acs url

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
url	Specifies the URL used to connect the CPE to the ACS.	The value is a string of 8 to 400 characters, in the format http://host[:port]/path or https://host[:port]/path. ● host: IP address or domain name. ● port: port number. The default value is **80**. Generally, the port number is added to the IP address or domain name only after the port number is changed. ● path: working path of the HTTP server. The URL in the HTTPS format can ensure the communication security and data integrity between the ACS and CPE.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Before setting up a connection with the ACS, the CPE needs to obtain the ACS URL. The **cwmp acs url** command configures the URL used to connect the CPE to the ACS.

After the CPE sends an Inform message containing the IP address of the CPE to the URL of the ACS, the ACS authenticates the CPE using the user name and password. After being authenticated, the CPE can set up a connection with the ACS.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the URL to http://www.acs.com/acs.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp acs url http://www.acs.com/acs
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

21.5.4 cwmp acs username

Function

The **cwmp acs username** command configures the user name used to connect the CPE to the ACS.

The **undo cwmp acs username** command deletes the user name.

By default, no user name is available.

Format

cwmp acs username *username*

undo cwmp acs username

Parameters

Parameter	Description	Value
username	Specifies the user name used to connect the CPE to the ACS.	The value is a string of 1 to 255 case-sensitive characters. It cannot contain the following special characters: \ ? " #.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp acs username** command is used to configure the authentication user name used to connect the CPE to the ACS.

After the CPE sends an Inform message containing a URL to the ACS, the ACS authenticates the CPE using the user name and password. After being authenticated, the CPE can set up a connection with the ACS.

Example

Set the user name to newname.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp acs username newname
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

21.5.5 cwmp cpe connect interface

Function

The **cwmp cpe connect interface** command configures the interface that a CPE uses to connect to an ACS.

The **undo cwmp cpe connect interface** command cancels the interface.

By default, the CPE automatically selects an interface from interfaces with reachable routes to the ACS to set up a CWMP connection with the ACS.

Format

cwmp cpe connect interface *interface-type interface-number*

undo cwmp cpe connect interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the interface connecting to an ACS.	-

Views

CWMP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The Inform message sent by a CPE to an ACS contains the IP address of the specified interface. After authenticating the CPE, the ACS connects to this IP address and saves the IP address in its own address list. When the ACS initiates a connection with the CPE, the ACS sends an HTTP packet containing this IP address.

Generally, a CPE obtains a CWMP connection interface from all the interfaces to which the ACS have reachable routes. If the obtained interface does not connect the CPE to the ACS, CWMP connection fails to be set up. Therefore, a CWMP connection interface needs to be specified manually. You can use the **cwmp cpe connect interface** command to configure the interface.

After the CWMP connection interface is configured, the IP address of this interface is used as the source IP address of the CWMP connection.

Example

Specify GE 1/0/0 on the CPE to connect to the ACS.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe connect interface gigabitethernet 1/0/0
```

Related Topics

21.5.6 cwmp cpe connect retry

21.5.6 cwmp cpe connect retry

Function

The **cwmp cpe connect retry** command sets the number of attempts the CPE can make to retry a connection.

The **undo cwmp cpe connect retry** command restores the default number of attempts.

By default, the maximum number of attempts is 3.

Format

cwmp cpe connect retry *times*

undo cwmp cpe connect retry

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
times	Specifies the maximum number of attempts the CPE can make to retry a connection.	The value is an integer that ranges from 0 to 100. The value 0 indicates that the CPE does not retry a connection if the connection attempt fails.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the CPE fails to set up a connection with the ACS or a connection is interrupted unexpectedly, the CPE can be configured to automatically re-set up the connection. If the number of CPE auto-connection reattempts reaches the upper limit, the connection between the CPE and the ACS fails.

For the unstable link, you can increase the number of connection reattempts, which can be configured by the **cwmp cpe connect retry** command.

Example

Set the number of attempts the CPE can make to retry a connection to 5.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe connect retry 5
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.7 cwmp cpe inform interval

Function

The **cwmp cpe inform interval** command sets the interval at which the CPE sends Inform messages.

The **undo cwmp cpe inform interval** command restores the default interval.

 Copyright © Huawei Technologies Co., Ltd.

By default, a CPE sends an Inform message every 600 seconds.

Format

cwmp cpe inform interval *seconds*

undo cwmp cpe inform interval

Parameters

Parameter	Description	Value
seconds	Specifies the interval at which a CPE sends Inform messages.	V200R010C00: The value is an integer that ranges from 30 to 86400, in seconds. V200R010C10 and later versions: The value is an integer that ranges from 30 to 172800, in seconds.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To set up a connection with an ACS, a CPE needs to send Inform messages. After an interval for sending the Inform messages is set by the **cwmp cpe inform interval** command, the CPE can automatically send Inform messages to the ACS at the interval.

Set a proper interval. If the interval is too short, the CPE frequently sends Inform messages to occupy network resources.

Prerequisites

The **cwmp cpe inform interval** command takes effect only after the **cwmp cpe inform interval enable** command is executed to enable periodic sending of Inform messages.

Example

Set the interval at which the CPE sends Inform messages to 800 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform interval 800
```

Related Topics

21.5.1 cwmp

21.5.8 cwmp cpe inform interval enable

21.5.22 display cwmp configuration

21.5.8 cwmp cpe inform interval enable

Function

The **cwmp cpe inform interval enable** command enables the CPE to periodically send Inform messages.

The **undo cwmp cpe inform interval enable** command disables the CPE from periodically sending Inform messages.

By default, the CPE does not periodically send Inform messages.

Format

cwmp cpe inform interval enable

undo cwmp cpe inform interval enable

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To set up a connection with an ACS, a CPE needs to send Inform messages. After the function for the CPE to periodically send Inform messages is enabled by the **cwmp cpe inform interval enable** command, the CPE automatically sends Inform messages to the ACS.

After the CPE is enabled to periodically send Inform messages, set the interval using the **cwmp cpe inform interval** command. By default, a CPE sends an Inform message every 600 seconds.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable the CPE to periodically send Inform messages.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform interval enable
```

Related Topics

21.5.1 cwmp

21.5.7 cwmp cpe inform interval

21.5.22 display cwmp configuration

21.5.9 cwmp cpe inform product-class device-type

Function

The **cwmp cpe inform product-class device-type** command adds the actual product type of the CPE to the session initiated by the CPE to the ACS.

The **undo cwmp cpe inform product-class device-type** command restores the default configuration.

By default, the session initiated by the CPE to the ACS contains the product type AccessRouter.

Format

cwmp cpe inform product-class device-type

undo cwmp cpe inform product-class device-type

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

When the ACS needs to manage CPEs based on the product types of CPEs, use the **cwmp cpe inform product-class device-type** command to add the actual product types of CPEs to the sessions sent to the ACS. For example, the actual product types of CPEs include AR2220, AR2240C and AR2240.

 Copyright © Huawei Technologies Co., Ltd.

Example

Add the actual product type of the CPE to the session initiated by the CPE to the ACS.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform product-class device-type
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.10 cwmp cpe inform time

Function

The **cwmp cpe inform time** command sets the time when a CPE sends an inform message.

The **undo cwmp cpe inform time** command cancels the time setting.

By default, no time is specified for the CPE to send an inform message.

Format

cwmp cpe inform time *time*

undo cwmp cpe inform time

Parameters

Parameter	Description	Value
time	Specifies the date and time when a CPE sends an inform message.	The value ranges from 1970-01-01T00:00:00 to 2105-12-31T23:59:59, in the format yyyy-mm-ddThh:mm:ss. The specified time must be later than the system time.

Views

CWMP view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To set up a connection with an ACS, a CPE needs to send inform messages. After the time is set by the **cwmp cpe inform time** command, the CPE automatically sends an inform message to the ACS at the specified time.

Example

Configure the CPE to send an inform message at 2012-07-01 20:00:00.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe inform time 2012-07-01T20:00:00
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.11 cwmp cpe password

Function

The **cwmp cpe password** command configures the password used to connect an ACS to a CPE.

The **undo cwmp cpe password** command deletes the password.

By default, no password is available.

Format

cwmp cpe password cipher

undo cwmp cpe password

Parameters

Parameter	Description	Value
cipher	Displays the password in cipher text.	-

Views

CWMP view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp cpe password** command is used to configure the authentication password used to connect the ACS to the CPE.

An ACS can send connection requests to a CPE at any time. After the ACS sends an HTTP packet containing the IP address of the CPE, the CPE authenticates the ACS using the user name and password. After being authenticated, the ACS can set up a connection with the CPE.

Precautions

The passwords must meet the following requirements:

- The password is a string of 6 to 255 case-sensitive characters.
- The password must contain at least two of the following characters: upper-case character, lower-case character, digit, and special character.

  The special characters include spaces and the following:

  `~!@#$%^&*()-_=+\|[{}];:'",<.>/?
- Password entered in interactive mode is not displayed on the screen.
- The password cannot be the same as the username.

After an active/standby switchover on the AR3200 routers, you need to run this command again to set a password.

Example

Set the password to abc123456.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe password cipher
Enter Password(<6-255>):
Confirm password:
```

Related Topics

21.5.12 cwmp cpe username

21.5.12 cwmp cpe username

Function

The **cwmp cpe username** command configures the user name used to connect the ACS to the CPE.

The **undo cwmp cpe username** command deletes the user name.

By default, no user name is available.

Format

cwmp cpe username *username*

 Copyright © Huawei Technologies Co., Ltd.

undo cwmp cpe username

Parameters

Parameter	Description	Value
username	Specifies the user name used to connect the ACS to the CPE.	The value is a string of 1 to 255 case-sensitive characters, and cannot include invalid character \ ?.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

To prevent the transaction processing between CPEs and ACSs from being falsified and ensure the transaction processing confidentiality, the **cwmp cpe username** command is used to configure the authentication user name used to connect the ACS to the CPE.

An ACS can send connection requests to a CPE at any time. After the ACS sends an HTTP packet containing the IP address of the CPE, the CPE authenticates the ACS using the user name and password. After being authenticated, the ACS can set up a connection with the CPE.

Example

Set the user name to newname.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe username newname
```

Related Topics

21.5.11 cwmp cpe password

21.5.13 cwmp cpe wait timeout

Function

The **cwmp cpe wait timeout** command configures the connection timeout interval of the CPE. If no data is transmitted within the timeout interval, the connection between the CPE and ACS is torn down.

 Copyright © Huawei Technologies Co., Ltd.

The **undo cwmp cpe wait timeout** command restores the default connection timeout interval.

By default, the connection timeout interval is 30 seconds.

Format

cwmp cpe wait timeout *seconds*

undo cwmp cpe wait timeout

Parameters

Parameter	Description	Value
seconds	Specifies the connection timeout interval.	The value is integer that ranges from 30 to 1800, in seconds.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The connection timeout interval is used in either of the following scenarios:

- After sending an Inform message to the ACS, if the CPE does not receive a response within the connection timeout interval, the CPE considers that the connection fails.
- After a connection is set up, if the CPE and the ACS do not exchange any messages within the connection timeout interval, the CPE considers that the connection is invalid and tears down the connection.

Example

Set the connection timeout interval of the CPE to 60 seconds.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp cpe wait timeout 60
```

Related Topics

21.5.1 cwmp
21.5.22 display cwmp configuration

 Copyright © Huawei Technologies Co., Ltd.

21.5.14 cwmp device-info serial-number system-mac

Function

The **cwmp device-info serial-number system-mac** command sets the serial number of a CPE to the system MAC address of the device.

The **undo cwmp device-info serial-number** command restores the default settings.

By default, the serial number of a CPE is the device ESN.

Format

cwmp device-info serial-number system-mac

undo cwmp device-info serial-number

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The ACS can monitor various parameters of the CPE connected to the ACS. To ensure that the system MAC address is the serial number of the CPE, run the **cwmp device-info serial-number system-mac** command.

Precautions

If the CWMP session has been established, run the **cwmp device-info serial-number system-mac** or **undo cwmp device-info serial-number** command to re-establish a new CWMP session.

Example

Set the serial number of the CPE to the system MAC address of the device.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp device-info serial-number system-mac
```

 Copyright © Huawei Technologies Co., Ltd.

21.5.15 cwmp enable

Function

The **cwmp enable** command enables the CWMP function on a CPE.

The **undo cwmp enable** command disables the CWMP function on a CPE.

By default, the CWMP function is disabled on a CPE.

Format

cwmp enable

undo cwmp enable

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

After the CWMP function is enabled for a CPE by the **cwmp enable** command, the CPE can be remotely managed by an ACS. The CWMP function facilitates CPE management, saves maintenance costs, and improves troubleshooting efficiency.

When a CPE is uploading or downloading files, the CWMP function on the CPE cannot be disabled.

Example

Disable the CWMP function on a CPE.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] undo cwmp enable
```

Related Topics

21.5.1 cwmp

21.5.22 display cwmp configuration

21.5.25 display cwmp status

 Copyright © Huawei Technologies Co., Ltd.

21.5.16 cwmp escape-character

Function

The **cwmp escape-character** command adds a character to be translated.

The **undo cwmp escape-character** command deletes a character to be translated.

Format

cwmp escape-character *character characters*

undo cwmp escape-character *character*

Parameters

Parameter	Description	Value
character	Specifies a character to be translated.	The value is a case-sensitive character. It cannot be a space. **NOTE** The letter *e* or single quotation mark (") cannot be translated.
characters	Specifies a character (string) after translation.	The value is a string of 1 to 6 case-sensitive characters without any space. **NOTE** ● The translated content cannot be double quotation marks (" ") or single quotation mark ("), but can be a character string containing double quotation marks, for example, "@". ● However, translating a character into a character string containing double quotation marks may cause device exceptions; therefore, it is not recommended.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If a configuration file contains special characters that are not supported by the ACS, the upload fails. To solve this problem, you can configure these characters to be translated into characters supported by the ACS on the CPE. The CPE then can upload the configuration file to the ACS successfully. You can run the **cwmp escape-character** command to add a character to be translated.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- Currently, only 30 characters to be translated are supported. If more than 30 characters to be translated are configured, an error message is displayed.
- To make character translation take effect, run the **cwmp escape-character enable** command.

Example

Translate > into @.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] cwmp
[Huawei-cwmp] cwmp escape-character > @
```

Delete > to be translated.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] cwmp
[Huawei-cwmp] undo cwmp escape-character >
```

Related Topics

21.5.1 cwmp

21.5.17 cwmp escape-character enable

21.5.17 cwmp escape-character enable

Function

The **cwmp escape-character enable** command enables the character translation function.

The **undo cwmp escape-character enable** command disables the character translation function.

By default, character translation is disabled.

Format

cwmp escape-character enable

undo cwmp escape-character enable

Parameters

None

Views

CWMP view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

If you want to add or delete translated characters, first run the **cwmp escape-character enable** command to enable the character translation function.

Precautions

You can run the **cwmp escape-character** command to add or delete a translated character. New or deleted translation characters will not take effect until the **cwmp escape-character enable** command is used.

Example

Enable the character translation function.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] cwmp
[Huawei-cwmp] cwmp escape-character enable
```

Related Topics

21.5.1 cwmp

21.5.16 cwmp escape-character

21.5.18 cwmp password complexity-check disable

Function

The **cwmp password complexity-check disable** command disables complexity check on the passwords used for authentication between ACS and CPE.

The **undo cwmp password complexity-check disable** command enables complexity check on the passwords used for authentication between ACS and CPE.

By default, the complexity check on the passwords used for authentication between ACS and CPE is enabled.

Format

cwmp password complexity-check disable

undo cwmp password complexity-check disable

Parameters

None

Views

CWMP view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When the complexity check function is enabled, the passwords entered in interactive mode for authentication between CPE and ACS must meet the following requirements:

- A password is a string of 6 to 255 case-sensitive characters.
- The password must be a combination of at least two of the following: uppercase letters, lowercase letters, digits, and special characters.

  Special characters include `~ ! @ # $ % ^ & * ( ) - _ = + \ | [{ }] ; : ' " , < . > /.

If you want to use simple passwords for CPE and ACS authentication, run the **cwmp password complexity-check disable** command to disable password complexity check. After the command is executed, the passwords configured using the **cwmp acs password cipher** and **cwmp cpe password cipher** commands do not need to meet complexity check requirements.

Precautions

To ensure security, do not disable complexity check on the passwords used for authentication between ACS and CPE.

Example

Disable complexity check on the passwords used for authentication between ACS and CPE.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp password complexity-check disable
```

21.5.19 cwmp permit interface

Function

The **cwmp permit interface** command specifies physical interfaces on the CPE to which the ACS can connect.

The **undo cwmp permit interface** command restores the default physical interfaces on the CPE to which the ACS can connect.

By default, the ACS can connect to all the physical interfaces on the CPE.

Format

cwmp permit interface { *interface-type interface-number* } &<1-5>

undo cwmp permit interface

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	*interface-type*: specifies the interface type. *interface-number*: specifies the interface number. *interface-number* and *interface-type* specify an interface.	-

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To prevent the ACS from connecting to the CPE through an unauthorized physical interface, you can run the **cwmp permit interface** command to specify physical interfaces on the CPE to which the ACS can connect.

Precautions

- By default, the ACS can connect to all the physical interfaces on the CPE. When you run this command to specify one physical interface on the CPE, the ACS cannot connect to the other physical interfaces on the CPE.
- You can specify a maximum of five interfaces each time you run the **cwmp permit interface** command. The latest configuration overrides the previous one. For example, before you run the command, the ACS can connect to three physical interfaces GigabitEthernet 1/0/0, GigabitEthernet 2/0/0, and GigabitEthernet 3/0/0 on the CPE. After you run the command to specify the interface GigabitEthernet 1/0/0, the ACS can only connect to the interface GigabitEthernet 1/0/0.

Example

Specify physical interfaces on the CPE to which the ACS can connect.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp permit interface gigabitethernet 1/0/0 gigabitethernet 2/0/0
  Info: Succeeded in setting cwmp permit interface.
```

Restore the default physical interfaces on the CPE to which the ACS can connect.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] undo cwmp permit interface
```

 Copyright © Huawei Technologies Co., Ltd.

21.5.20 cwmp request upload current-configuration

Function

The **cwmp request upload current-configuration** command configures a CPE to upload the currently loaded configuration file to an ACS.

Format

cwmp request upload current-configuration

Parameters

None

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

After the connection between a CPE and an ACS is set up, the CPE needs to upload the currently loaded configuration file to the ACS. This function is configured by the **cwmp request upload current-configuration** command.

Example

Configure a CPE to upload the currently loaded configuration file to an ACS.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp request upload current-configuration
```

Related Topics

21.5.24 display cwmp request upload status

21.5.21 cwmp ssl-client

Function

The **cwmp ssl-client** command configures a certificate or policy for the HTTPS client.

The **undo cwmp ssl-client** command deletes the configured certificate or policy.

By default, no certificate or policy is configured for the HTTPS client.

 Copyright © Huawei Technologies Co., Ltd.

Format

cwmp ssl-client { **client-root-cert** *rootcert-path1* [*rootcert-path2*] | **ssl-policy** *policy-name* }

undo cwmp ssl-client { **client-root-cert** | **ssl-policy** }

Parameters

Parameter	Description	Value
client-root-cert *rootcert-path1 rootcert-path2*	Configures the CPE to validate the certificate from the ACS. ● *rootcert-path1*: Specifies the absolute path of the level-1 root certificate. The level-1 root certificate is issued by the certification association (CA). ● *rootcert-path2*: Specifies the absolute path of the level-2 root certificate. The Level-2 root certificate is used for communication between devices.	The value is a string of 1 to 64 case-sensitive characters. It cannot contain any space or question mark (?).
ssl-policy *policy-name*	Configures the CPE to validate the SSL policy from the ACS.	The value is a string of 1 to 31 case-insensitive characters. It cannot contain any space or question mark (?).

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Security Socket Layer (SSL) ensures communication security and data integrity between the ACS and CPE.

 Copyright © Huawei Technologies Co., Ltd.

When the ACS URL is in the HTTPS format, the CPE and ACS must authenticate each other, and the SSL connection is set up only after the CPE and ACS are authenticated. It ensures the confidentiality of communication between the ACS and the CPE and data integrity.

NOTE

Before configuring a CPE to authenticate the ACS using an SSL policy, run the **ssl policy** *policy-name* command to configure the SSL policy on the CPE.

Precautions

The system time must be correctly set; otherwise, certificate validation may fail. To use a new certificate, uninstall the existing certificate first.

Example

Load the root certificate Interop_CA.cer.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp ssl-client client-root-cert flash:/Interop_CA.cer
Info: Succeed to load the trusted CA certificate.
[Huawei-cwmp]
```

21.5.22 display cwmp configuration

Function

The **display cwmp configuration** command displays the CWMP configurations on a CPE.

Format

display cwmp configuration

Parameters

None

Views

All view

Default Level

3: Management level

Usage Guidelines

None

Example

Display the CWMP configurations on a CPE.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display cwmp configuration
  CWMP is enabled
  ACS URL:                    http://www.acs.com:80/acs
  ACS username:                 hwcpe
  ACS password:                 %@%@x:J6T3+\>-7JE_7mDOKM,v`c%@%@
  Inform enable status:           disabled
  Inform interval:             600s
  Inform time:                 -
  Wait timeout:                 30s
  Reconnection times:             3
```

Table 21-31 Description of the **display cwmp configuration** command output

Item	Description
CWMP is enabled	CWMP (TR-069) is enabled. ● enable: CWMP is enabled. ● disabled: CWMP is disabled. This item can be configured by the **cwmp enable** command.
ACS URL	ACS's URL to which the CPE connects. If no URL is configured, the system displays -. This item can be configured by the **cwmp acs url** command.
ACS username	Authentication user name of the ACS. If no user name is configured, the system displays -. This item can be configured by the **cwmp acs username** command.
ACS password	Authentication password of the ACS. If no password is configured, the system displays -. This item can be configured by the **cwmp acs password** command.
Inform enable status	Whether the CPE is configured to periodically send Inform messages. This item can be configured by the **cwmp cpe inform interval enable** command.
Inform interval	Interval at which the CPE sends Inform messages. This item can be configured by the **cwmp cpe inform interval** command.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Inform time	Time when the CPE sends an Inform message. If no time is specified, the system displays -. This item can be configured by the **cwmp cpe inform time** command.
Wait timeout	Close-wait timer of the CPE. This item can be configured by the **cwmp cpe wait timeout** command.
Reconnection times	Maximum number of attempts the CPE can make to retry a connection. This item can be configured by the **cwmp cpe connect retry** command.

Related Topics

21.5.2 cwmp acs password
21.5.3 cwmp acs url
21.5.4 cwmp acs username
21.5.7 cwmp cpe inform interval
21.5.8 cwmp cpe inform interval enable
21.5.10 cwmp cpe inform time
21.5.13 cwmp cpe wait timeout
21.5.6 cwmp cpe connect retry
21.5.15 cwmp enable

21.5.23 display cwmp password

Function

The **display cwmp password** command displays the password that the CPE uses to connect to the ACS, and the password that the ACS uses to connect to the CPE.

Format

display cwmp password

Parameters

None

Views

CWMP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command is used to view the password that the CPE uses to connect to the ACS and the password that the ACS uses to connect to the CPE.

Example

Display the passwords that the CPE and the ACS use to connect to each other.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] display cwmp password
 cwmp cpe password %@%@=;fNL1~b)Z:v/&#DBe^0$y7!%@%@
 cwmp acs password %@%@H6^EXz:*EP-!'->Apla@$xZK%@%@
```

Table 21-32 Description of the display cwmp password command output

Item	Description
cwmp cpe password	Password that the ACS uses to connect to the CPE.
cwmp acs password	Password that the CPE uses to connect to the ACS.

Related Topics

21.5.2 cwmp acs password

21.5.11 cwmp cpe password

21.5.24 display cwmp request upload status

Function

The **display cwmp request upload status** command displays the status of the configuration file uploaded from a CPE to an ACS.

Format

display cwmp request upload status

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

This command is used to view the status of the configuration file uploaded from a CPE to an ACS. The command output and description are as follows:

- **Success to upload the current configuration file**: indicates that the configuration file has been uploaded to the ACS.
- **The current configuration file is uploading**: indicates that the configuration file is being uploaded to the ACS.
- **Failed to upload the current configuration file**: indicates that the configuration file fails to be uploaded to the ACS.

Example

Display the status of the configuration file uploaded from a CPE to an ACS.

```
<Huawei> display cwmp request upload status
Success to upload the current configuration file.
```

Related Topics

21.5.20 cwmp request upload current-configuration

21.5.25 display cwmp status

Function

The **display cwmp status** command displays the CWMP status on a CPE.

Format

display cwmp status

Parameters

None

Views

All view

Default Level

3: Management level

Usage Guidelines

None

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the CWMP status on a CPE.

```
<Huawei> display cwmp status
 CWMP is enabled
 ACS URL:                          -
 ACS information is set by:          user
 ACS username:                       -
 ACS password:                       -
 Connection status:                  disconnected
 Time of last successful connection:   -
```

Table 21-33 Description of the **display cwmp status** command output

Item	Description
CWMP is enabled	CWMP (TR-069) is enabled. ● enable: CWMP is enabled. ● disabled: CWMP is disabled. This item can be configured by the **cwmp enable** command.
ACS URL	ACS's URL to which the CPE connects. If no URL is configured, the system displays -. This item can be configured by the **cwmp acs url** command.
ACS information is set by	How the CPE obtains the ACS's URL. ● user: The ACS's URL is configured using a command. ● acs: The URL is sent by the ACS to the CPE. ● dhcp: The URL is sent by the ACS to a DHCP server.
ACS username	Authentication user name of the ACS. If no user name is configured, the system displays -. This item can be configured by the **cwmp acs username** command.
ACS password	Authentication password of the ACS. If no password is configured, the system displays -. This item can be configured by the **cwmp acs password** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Connection status	Status of a connection between the CPE and the ACS: • connected: The connection has been set up successfully. • disconnected: The connection has not been set up. • waiting response: The CPE is waiting for the response packet from the ACS.
Time of last successful connection	Time when the last connection is set up. If no connection has been set up, the system displays -.

Related Topics

21.5.2 cwmp acs password
21.5.3 cwmp acs url
21.5.4 cwmp acs username
21.5.15 cwmp enable

21.5.26 cwmp ip-change inform disable

Function

The **cwmp ip-change inform disable** command disables the device from informing the ACS of an IP address change event.

The **undo cwmp ip-change inform disable** command enables the device to inform the ACS of an IP address change event.

By default, when the IP address of a device changes, the device does not inform the ACS of this event.

Format

cwmp ip-change inform disable

undo cwmp ip-change inform disable

Parameters

None

Views

CWMP view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **cwmp ip-change inform disable** command to disable the device from informing the ACS of an IP address change event.

Precautions

This command takes effect only on IP addresses reachable to the ACS.

Example

Disable the device from informing the ACS of an IP address change event.

```
<Huawei> system-view
Enter system view, return user view with Ctrl+Z.
[Huawei] cwmp
[Huawei-cwmp] cwmp ip-change inform disable
```

Related Topics

21.5.1 cwmp

21.5.27 cwmp ssl-server ssl-policy

Function

The **cwmp ssl-server ssl-policy** command binds an SSL server policy to CWMP.

The **undo cwmp ssl-ser ssl-policy** command unbinds an SSL server policy from CWMP.

By default, no SSL server policy is bound to CWMP.

Format

cwmp ssl-server ssl-policy *policy-name*

undo cwmp ssl-server ssl-policy

Parameters

Parameter	Description	Value
policy-name	Specifies the name of an SSL server policy.	The value is a string of 1 to 31 case-insensitive characters. It cannot contain spaces or question marks (?).

Copyright © Huawei Technologies Co., Ltd.

Views

CWMP view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When an ACS initiates a connection with a CPE, you can configure a transport-layer security protocol to ensure communication data security and integrity. Hypertext Transfer Protocol Secure (HTTPS) supports the Secure Sockets Layer (SSL) protocol. Run the **cwmp ssl-server ssl-policy** *policy-name* command to bind an SSL policy to CWMP, so that the ACS can set up HTTPS connections. After this command is executed, run the **display ssl ssl-policy** command to view the binding information of SSL server policy.

Precautions

1. The connection is initiated by the server, so the SSL policy type must be server; otherwise, the SSL connection cannot be set up. Run the **ssl policy** *policy-name* [**type** { **client** | **server** }] command to configure the SSL server policy.
2. Before binding an SSL server policy to CWMP, run the **pki-realm** *realm-name* command to specify the PKI realm for the SSL policy.

Example

Bind the SSL server policy to CWMP.

```
<Huawei> system-view
[Huawei] cwmp
[Huawei-cwmp] cwmp ssl-server ssl-policy Test3Server
Info:Succeed to bind ssl policy.
```

21.6 LLDP Configuration Commands

21.6.1 display lldp local

Function

The **display lldp local** command displays global LLDP information or the LLDP information on a specified interface.

Format

display lldp local [**interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays the LLDP information on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the command displays LLDP information on all the interfaces with LLDP enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp local** command displays the global LLDP information or the LLDP information on an interface.

- The global LLDP information includes system information, MED system information, system configuration, and data statistics on the peer device.
- The LLDP information on the Ethernet interface, and port group include the interface information and MED interface information, The LLDP information on the Serial interface includes the interface information.

To verify the LLDP information and Layer 2 information of the system and interfaces, run this command.

Prerequisites

The LLDP function has been enabled globally and on the specified interface.

Example

Display the global LLDP information.

```
<Huawei> display lldp local
System information
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
System name    :Huawei
System description  :Huawei AR2240 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.120 (AR2240 V200R010 ) Copyright (C) 2011-2013 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
LLDP Up time   :2012/05/10 11:40:49
```


Copyright © Huawei Technologies Co., Ltd.

```
MED system information
Device class   :Network Connectivity
(MED inventory information of master board)
HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :404
SoftwareRev       :V200R010
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

System configuration
LLDP Status                    :enabled            (default is disabled)
LLDP Message Tx Interval       :30                 (default is 30s)
LLDP Message Tx Hold Multiplier :4                 (default is 4)
LLDP Refresh Delay             :2                  (default is 2s)
LLDP Tx Delay                  :2                  (default is 2s)
LLDP Notification Interval     :5                  (default is 5s)
LLDP Notification Enable       :enabled            (default is enabled)
Management Address             :IP: 10.10.10.1  MAC: 00e0-11fc-1710

Remote Table Statistics:
Remote Table Last Change Time   :0 days, 5 hours, 57 minutes, 32 seconds

Remote Neighbors Added          :15

Remote Neighbors Deleted        :13

Remote Neighbors Dropped        :0

Remote Neighbors Aged           :0

Total Neighbors                 :2


Port information:
Interface GigabitEthernet1/0/0:
LLDP Enable Status       :enabled            (default is disabled)
Total Neighbors          :0

Port ID subtype     :interfaceName
Port ID             :GigabitEthernet1/0/0
Port description    :HUAWEI, AR Series, GigabitEthernet1/0/0 Interface

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:0

Interface Ethernet2/0/0:
LLDP Enable Status       :enabled            (default is disabled)
```


Copyright © Huawei Technologies Co., Ltd.

```
Total Neighbors          :1

Port ID subtype     :interfaceName
Port ID             :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface

Port And Protocol VLAN ID(PPVID) don't supported
Port VLAN ID(PVID)  :1
VLAN name of VLAN 1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP GVRP

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED port information

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID          :0
Media policy L2 priority     :6
Media policy Dscp            :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
  ---- More ----
```

Table 21-34 Description of the display lldp local command output.

Item	Description
System information	
Chassis type	Device ID sub-type: ● chassisComponent: chassis alias ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● InterfaceName: name of the interface ● local: name of the local device
Chassis ID	Device ID.
System name	Name of the device.
System description	Device description.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
System capabilities supported	Capabilities of the local device, including: • repeater: repeater • bridge: bridge device • wlanAccessPoint: wireless access point • router: router • telephone: wireless device • docsisCableDevice: management station • stationOnly: base station • other: other capabilities
System capabilities enabled	Capabilities enabled on the local device, including: • repeater: repeater • bridge: bridge device • wlanAccessPoint: wireless access point • router: router • telephone: wireless device • docsisCableDevice: management station • stationOnly: base station • other: other capabilities
LLDP Up time	Time when LLDP is enabled.
MED system information	
Device class	Type of the MED device.
HardwareRev	Hardware version of the device.
FirmwareRev	Firmware version of the product.
SoftwareRev	Software version of the device.
SerialNum	Serial number.
Manufacturer name	Name of the manufacturer
Model name	Name of a model.
Asset tracking identifier	Asset tracking ID.
System configuration	
LLDP Status	LLDP status: • Enabled • Disabled This parameter is configured using the **lldp enable (system view)** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
LLDP Message Tx Interval	Interval for sending LLDP packets. This parameter is configured using the **lldp message-transmission interval** command.
LLDP Message Tx Hold Multiplier	Multiplier of the period in which the message is held. This parameter is configured using the **lldp message-transmission hold-multiplier** command.
LLDP Refresh Delay	Delay in re-initializing the LLDP module. This parameter is configured using the **lldp restart-delay** command.
LLDP Tx Delay	Delay in sending the LLDP packets. This parameter is configured using the **lldp message-transmission delay** command.
LLDP Notification Interval	Delay in sending the notification after the remote information changes. This parameter is configured using the **lldp trap-interval** command.
LLDP Notification Enable	Status of the notification function. • Enabled • Disabled
Management Address	Management address. This parameter is configured using the **lldp management-address** command.
Remote Table Statistics	
Remote Table Last Change Time	Time that elapsed since the latest modification of remote data.
Remote Neighbors Added	Number of added remote neighbors.
Remote Neighbors Deleted	Number of deleted remote neighbors.
Remote Neighbors Dropped	Number of remote neighbors discarded after the buffer is used up.
Remote Neighbors Aged	Number of neighbors that are aged out and deleted.
Total Neighbors	Number of remote neighbors.
Port information	

Copyright © Huawei Technologies Co., Ltd.

Item	Description
LLDP Enable Status	LLDP status: ● Enabled ● Disabled
Total Neighbors	Number of remote neighbors.
Port ID subtype	Subtypes of a port ID. ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● InterfaceName: name of the interface ● agentCircuitId: circuit ID of the DHCP agent ● local: name of the local device
Port ID	Interface ID.
Port description	Interface description.
Port VLAN ID(PVID)	VLAN ID of the interface.
VLAN name of VLAN 1	Name of VLAN 1.
Protocol identity	Protocol ID.
Auto-negotiation supported	Whether the interface supports auto-negotiation: ● Yes ● No
Auto-negotiation enabled	Whether the interface is enabled with auto-negotiation: ● Yes ● No
OperMau	Auto-sensing rate and duplex mode of the interface.
Power port class	PoE type: ● PSE: power-sourcing equipment ● PD: powered device
PSE power supported	Whether the PSE power is supported. ● Yes: PSE power is supported. ● No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. ● Yes: enabled. ● No: disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSE pairs control ability	Whether the PSE twisted pair control is supported. ● Yes: PSE twisted pair control is supported. ● No: PSE twisted pair control is not supported.
Power pairs	PoE remote power supply mode. ● Signal: power supply mode of signal lines ● Spare: power supply mode of spare signal lines ● Unknown: an unknown remote power supply mode
Port power classification	PD power control level on the interface: ● Class0: indicates level 1. ● Class1: indicates level 2. ● Class2: indicates level 3. ● Class3: indicates level 4. ● Class4: indicates level 5. ● Unknown: indicates an unknown level.
Link aggregation supported	Whether the interface supports link aggregation. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Link aggregation enabled	Whether link aggregation is enabled on the interface. ● Yes: enabled ● No: disabled
Aggregation port ID	ID of an aggregated interface, If link aggregation is disabled, the value of this field is 0.
Maximum frame Size	Maximum size of a frame supported by the interface.
MED port information	
Media policy type	Type of the media policy: ● voice: indicates that the device supports voice. ● unknown: indicates that the type of the media policy is unknown.
Unknown Policy	Whether the type of the media policy is unknown: ● Yes: unknown ● Defined: known

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
VLAN tagged	Whether to add tag to the packets of the voice VLAN. ● Yes: Adds a VLAN tag to packets of the voice VLAN. ● No: Not to add a VLAN tag to packets of the voice VLAN.
Media policy VlanID	ID of the voice VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type.
PoE PSE power source	Type of the PSE: ● Primary: indicates primary power supply. ● Backup: indicates backup power supply. ● Unknown: indicates power supply of an unknown type.
Port PSE Priority	PSE priority of an interface: ● Unknown: indicates an unknown priority. ● Critical: indicates the highest priority. ● High: indicates the medium priority. ● Low: indicates the lowest priority.
Port Available power value	Port power supply.

Related Topics

21.6.10 lldp enable (system view)

21.6.2 display lldp neighbor

Function

The **display lldp neighbor** command displays information about neighboring device of all interfaces or a specified interface.

Format

display lldp neighbor [**interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays information about neighboring devices of a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the command displays information about neighboring devices of all interfaces with LLDP enabled.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Using this command, you can know which neighboring devices are connected to the local device, to which interfaces the neighboring devices are connected, layer 2 information about the neighbors, and whether LLDP configuration is correct.

Prerequisites

The LLDP function has been enabled globally and on the specified interface.

Example

Display information about neighbor devices of interfaces Ethernet2/0/0.

```
<Huawei> display lldp neighbor interface ethernet 2/0/0
Ethernet2/0/0 has 1 neighbors:

Neighbor index : 1
Chassis type   :macAddress
Chassis ID     :00e0-11fc-1710
Port ID type   :interfaceName
Port ID        :Ethernet2/0/0
Port description    :HUAWEI, AR Series, Ethernet2/0/0 Interface
```

 Copyright © Huawei Technologies Co., Ltd.

```
System name         :Huawei
System description  :Huawei AR2240 Huawei Versatile Routing Platform Software  V
RP (R) software,Version 5.120 (AR2240 V200R010) Copyright (C) 2011-2013 Huawei
 Technologies Co., Ltd
System capabilities supported   :bridge
System capabilities enabled     :bridge
Management address type  :ipV4
Management address       : 10.0.0.1
Expired time   :104s


Port VLAN ID(PVID)  :1
VLAN name of VLAN  1: VLAN1
Protocol identity   :STP RSTP/MSTP LACP GVRP

Auto-negotiation supported    :Yes
Auto-negotiation enabled      :Yes
OperMau   :speed(100)/duplex(Full)

Power port class         :PD
PSE power supported      :No
PSE power enabled        :No
PSE pairs control ability:No
Power pairs              :Unknown
Port power classification:Unknown

Link aggregation supported:Yes
Link aggregation enabled :No
Aggregation port ID      :0
Maximum frame Size       :9216

MED Device information
Device class   :Network Connectivity

HardwareRev       :AR01SRU1A VER.A
FirmwareRev       :100
SoftwareRev       :V200R010
SerialNum         :NA
Manufacturer name :HUAWEI TECH CO., LTD
Model name        :NA
Asset tracking identifier :NA

Media policy type   :Voice
Unknown Policy      :Defined
VLAN tagged         :Yes
Media policy VlanID      :0
Media policy L2 priority :6
Media policy Dscp        :46

Power Type               :Unknown
PoE PSE power source     :Unknown
Port PSE Priority        :Unknown
Port Available power value:2
```

Table 21-35 Description of the display lldp neighbor command output

Item	Description
Neighbor index	Index of a neighbor.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Chassis type	ID sub-types of a neighboring device: ● chassisComponent: chassis alias ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● InterfaceName: name of the interface ● local: name of the local device
Chassis Id	ID of a neighboring device.
Port ID type	ID sub-type of a neighboring interface: ● interfaceAlias: interface alias ● portComponent: interface or backplane alias ● macAddress: MAC address ● networkAddress: network address ● InterfaceName: name of the interface ● agentCircuitId: circuit ID of the DHCP agent ● local: name of the local device
Port Id	ID of a neighbor interface.
Port description	Description of a neighboring interface.
System name	System name of a neighboring device.
System description	Description of a neighboring device.
System capabilities supported	Capabilities of a neighboring device (at least one capability is supported): ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
System capabilities enabled	Capabilities enabled on a neighboring device (This field is a subset of the system capabilities supported field, and at least one capability must be enabled). ● other: other capabilities ● repeater: repeater ● bridge: bridge device ● wlanAccessPoint: wireless access point (AP) ● router: router ● telephone: wireless device ● docsisCableDevice: management station ● stationOnly: base station
Management address type	Type of the management address.
Management address	Management address of a neighbor.
Expired time	Aging time of a neighbor.
Port VLAN ID(PVID)	VLAN ID of an interface.
Protocol identity	Protocol ID.
VLAN name of VLAN 1	Name of VLAN 1.
Auto-negotiation supported	Whether the interface supports auto-negotiation: ● Yes: Auto-negotiation is supported. ● No: Auto-negotiation is not supported.
Auto-negotiation enabled	Whether the interface is enabled with auto-negotiation: ● Yes: enabled. ● No: disabled.
OperMau	Transmission rate and duplex mode of the interface.
Power port class	PoE type: ● PSE: power-sourcing equipment. ● PD: powered device.
PSE power supported	Whether the PSE power is supported. ● Yes: PSE power is supported. ● No: PSE power is not supported.
PSE power enabled	Whether the PSE power is enabled. ● Yes: enabled. ● No: disabled.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
PSE pairs control ability	Whether the PSE control is supported. ● Yes: PSE control is supported. ● No: PSE control is not supported.
Power pairs	PoE remote power supply mode. ● Signal: power supply mode of signal lines. ● Spare: power supply mode of spare signal lines. ● Unknown: an unknown remote power supply mode.
Port power classification	PD power control level on the interface: ● Class0: indicates level 1. ● Class1: indicates level 2. ● Class2: indicates level 3. ● Class3: indicates level 4. ● Class4: indicates level 5. ● Unknown: indicates an unknown control level.
Link aggregation supported	Whether link aggregation is supported on the interface. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Link aggregation enabled	Whether link aggregation is enabled on an interface. ● Yes: The interface supports link aggregation. ● No: The interface does not support link aggregation.
Aggregation port ID	ID of an aggregated interface, If link aggregation is disabled, the value of this field is 0.
Maximum frame Size	Maximum size of a frame supported by the interface.
Device class	Type of the MED device.
HardwareRev	Hardware version of the product.
FirmwareRev	Firmware version of the product.
SoftwareRev	Software version of the product.
SerialNum	Serial number.
Manufacturer name	Name of the manufacturer.
Model name	Name of a model.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Asset tracking identifier	Asset tracking ID.
Media policy type	Type of the media policy: ● voice: indicates that the device supports voice. ● unknown: indicates that the type of the media policy is unknown.
Unknown Policy	Whether the type of the media policy is unknown. Yes indicates that the media policy type is unknown. No indicates that the media policy type is known.
VLAN tagged	Whether to add tag to the packets of the voice VLAN.
Media policy VlanID	ID of the voice VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy Dscp	DSCP value.
Power Type	Power supply type: ● PSE: power-sourcing equipment. ● PD: powered device.
PoE PSE power source	Type of the PSE: ● Primary: indicates primary power supply. ● Backup: indicates backup power supply. ● Unknown: indicates power supply of an unknown type.
Port PSE Priority	PSE priority of an interface: ● Unknown: indicates an unknown priority. ● Critical: indicates the highest priority. ● High: indicates the medium priority. ● Low: indicates the lowest priority.
Port Available power value	Port power supply

Related Topics

21.6.10 lldp enable (system view)

 Copyright © Huawei Technologies Co., Ltd.

21.6.3 display lldp neighbor brief

Function

The **display lldp neighbor brief** command displays brief information about neighbors of the device.

Format

display lldp neighbor brief

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

To quickly view the neighbors of the local device and the interfaces connected to neighbors, run this command.

Prerequisites

The LLDP function has been enabled globally.

Example

Display information about neighbor devices.

```
<Huawei> display lldp neighbor brief
Local Intf   Neighbor Dev          Neighbor Intf          Exptime
Eth2/0/0     Huawei                Eth0/0/2               103
```

Table 21-36 Description of the display lldp neighbor brief command output

Item	Description
Local Intf	Local interface.
Neighbor Dev	Name of neighbor device.
Neighbor Intf	Neighboring interface.
Exptime	Aging time of a neighbor, in seconds.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.6.2 display lldp neighbor

21.6.10 lldp enable (system view)

21.6.4 display lldp statistics

Function

The **display lldp statistics** command displays statistics about LLDP packets sent and received by all or a specified interface.

Format

display lldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays statistics about LLDP packet sent and received by a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, the command displays statistics about LLDP packets on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp statistics** command displays the statistics about sent and received LLDP packets.

Copyright © Huawei Technologies Co., Ltd.

To display the LLDP packet statistics within a specified period of time, run the **reset lldp statistics** command to clear the existing statistics first, and then run the **display lldp statistics** command to display the new statistics.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Precautions

If the LLDP function is enabled globally but disabled on an interface, the packet statistics on the interface are 0.

Example

Display the statistics about sent and received LLDP packets on all interfaces.

```
<Huawei> display lldp statistics
LLDP statistics global Information:
Statistics for Ethernet2/0/0:
Transmitted Frames Total: 2839
Received Frames Total:    2728      Frames Discarded Total:  0
Frames Error Total:       0         TLVs Discarded Total:    0
TLVs Unrecognized Total:  0         Neighbors Expired Total: 0
```

Table 21-37 Description of the display lldp statistics command output

Item	Description
Transmitted Frames Total	Number of sent LLDP packets.
Received Frames Total	Number of received LLDP packets.
Frames Discarded Total	Number of discarded LLDP packets.
Frames Error Total	Number of received errored LLDP packets.
TLVs Discarded Total	Number of discarded TLVs.
TLVs Unrecognized Total	Number of unknown TLVs.
Neighbors Expired Total	Number of aged-out neighbors.

Related Topics

21.6.10 lldp enable (system view)
21.6.19 reset lldp statistics

21.6.5 display lldp tlv-config

Function

The **display lldp tlv-config** command displays optional TLVs that can be sent with LLDP packets on all or a specified interface.

Format

display lldp tlv-config [**interface** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Displays optional TLVs supported by a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, the command displays optional TLVs on all interfaces.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

The **display lldp tlv-config** command displays the TLVs supported by the specified interface or all interfaces, and thus you can know whether the required TLVs are enabled and unneeded TLVs are disabled.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Example

Display Optional TLVs that can be sent with LLDP packets on Ethernet2/0/0.

```
<Huawei> display lldp tlv-config interface ethernet 2/0/0
LLDP tlv-config of port [Ethernet2/0/0]:
Name                          Status    Default
Basic optional TLV:
Port Description TLV              Yes       Yes
System Name TLV                   Yes       Yes
System Description TLV            Yes       Yes
System Capabilities TLV           Yes       Yes
Management Address TLV            Yes       Yes
IEEE 802.1 extend TLV:
Port VLAN ID TLV                  Yes       Yes
Port And Protocol VLAN ID TLV     Yes       Yes
VLAN Name TLV                     Yes       Yes
```

 Copyright © Huawei Technologies Co., Ltd.

```
Protocol identity TLV            Yes       Yes
IEEE 802.3 extend TLV:
MAC-Physic TLV                   Yes       Yes
Power via MDI TLV                Yes       Yes
Link Aggregation TLV             Yes       Yes
Maximum Frame Size TLV           Yes       Yes
LLDP-MED extend TLV:
Capabilities TLV                 Yes       Yes
Network Policy TLV               Yes       Yes
Extended Power via MDI TLV       Yes       Yes
Inventory TLV                    Yes       Yes
Location Identification TLV      No        No
```

Table 21-38 Description of the display lldp tlv-config command output

Item	Description
Name	Type of TLV.
Status	Whether the interface is configured to send the TLVs of the specified type.
Default	Whether the TLVs of the specified types are sent on an interface by default.
Basic optional TLV	Basic TLVs that can be sent on an interface.
Port Description TLV	Interface description TLV.
System Name TLV	System name TLV.
System Description TLV	System description TLV.
System Capabilities TLV	TLV indicating the system capability set.
Management Address TLV	Management address TLV.
IEEE 802.1 extend TLV	Type of the IEEE 802.1 organizational-specific TLVs that can be sent on an interface.
Port VLAN ID TLV	PVID TLV.
Port And Protocol VLAN ID TLV	Port and protocol VLAN ID TLV.
VLAN Name TLV	VLAN name TLV.
Protocol identity TLV	Protocol ID TLV.
IEEE 802.3 extend TLV	IEEE 802.3 organizational-specific TLVs that can be sent on an interface.
MAC-Physic TLV	TLV indicating physical attributes of an interface.
Power via MDI TLV	Power capability TLV.
Link Aggregation TLV	Link aggregation TLV.
Maximum Frame Size TLV	Maximum frame length TLV.
LLDP-MED extend TLV	LLDP MED TLV.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Capabilities TLV	TLV indicating MED capability sets.
Extended Power via MDI TLV	TLV indicating the extended power supply capabilities.
Inventory TLV	Inventory information, including Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model name TLV, and Asset id TLV.
Network Policy TLV	Network policy TLV.
Location Identification TLV	Location ID TLV.

21.6.6 display snmp-agent trap feature-name lldptrap all

Function

The **display snmp-agent trap feature-name lldptrap all** command displays the status of all traps on the LLDP module.

Format

display snmp-agent trap feature-name lldptrap all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Before running the **display snmp-agent trap feature-name lldptrap all** command, run the **snmp-agent** command to enable the SNMP Agent function.

Example

Display the status of all traps on the LLDP module.

```
<Huawei> display snmp-agent trap feature-name lldptrap all
-----------------------------------------------------------------------------
Feature name: LLDPTRAP
Trap number : 4
```

 Copyright © Huawei Technologies Co., Ltd.

```
-------------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
lldpRemTablesChange            on                      on
hwLldpEnabled                 on                    on
hwLldpDisabled                on                    on
hwLldpLocManIPAddrChange       on                      on
```

Table 21-39 Description of the **display snmp-agent trap feature-name lldptrap all** command output

Item	Description
Feature name	Name of the module to which a trap belongs.
Trap number	Number of traps.
Trap name	Names of a trap, traps of the LLDP module include: ● lldpRemTablesChange: Sends a trap when LLDP neighbor information changes. ● hwLldpEnabled: Sends a Huawei proprietary trap when the LLDP function is enabled globally. ● hwLldpDisabled: Sends a Huawei proprietary trap when the LLDP function is disabled globally. ● hwLldpLocManIPAddrChange: Sends a Huawei proprietary trap when the LLDP management address of the device changes.
Default switch status	Default status of a trap: ● on: The trap is enabled. ● off: The trap is disabled.
Current switch status	Status of a trap: ● on: The trap is enabled. ● off: The trap is disabled.

Related Topics

21.6.20 snmp-agent trap enable feature-name lldptrap

21.6.7 lldp clear neighbor

Function

The **lldp clear neighbor** command clears neighbor information in the system or on an interface.

Format

lldp clear neighbor [**interface** *interface-type interface-number*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Indicates the type and number of the interface whose neighbor information to be cleared. In the command: ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number. If no interface is specified, neighbor information of all interfaces is cleared.	-

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

If you want to obtain the latest neighbor information of interfaces, use the **lldp clear neighbor** command to clear existing neighbor information. When an interface receives new packets, new neighbor information is generated.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Example

Clear neighbor information of all interfaces.

```
<Huawei> lldp clear neighbor
Warning: This command will clear the neighbor information of all the ports. Continue? [Y/N]y
```

Related Topics

21.6.1 display lldp local
21.6.2 display lldp neighbor
21.6.3 display lldp neighbor brief

 Copyright © Huawei Technologies Co., Ltd.

21.6.9 lldp enable (interface view)
21.6.10 lldp enable (system view)

21.6.8 lldp dot3-tlv power

Function

The **lldp dot3-tlv power** command sets the standard to which the 802.3 Power via MDI TLV sent by an interface conforms.

By default, the 802.3 Power via MDI TLV conforms to 802.1 ab.

Format

lldp dot3-tlv power { **802.1ab** | **802.3at** }

Parameters

Parameter	Description	Value
802.1ab	Indicates that the 802.3 Power via MDI TLV sent by the interface conforms to 802.1 ab.	-
802.3at	Indicates that the 802.3 Power via MDI TLV sent by the interface conforms to 802.3 at.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The 802.3 Power via MDI TLV has the following formats:

- 802.1 ab format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class]
- 802.3 at format: [TLV type | TLV information string length | 802.3 OUI | MDI power support | PSE power pair | power class | type/source/priority | PD requested power value | PSE allocated power value]

Based on 802.1 ab, 802.3 at extends three fields: type/source/priority, PD requested power value, and PSE allocated power value.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The LLDP function has been enabled globally and on interfaces.

Precautions

After the global LLDP is disabled, the LLDP configuration is deleted from all interfaces.

Before selecting a format of the 802.3 Power via MDI TLV, you must know the TLV format supported by the neighbors. The TLV format on the local device must be the same as that on the neighbors.

Member interfaces of the Eth-Trunk do not support this command.

Example

Configure the interface to send the 802.3 Power via MDI TLV conforming to 802.3 at.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] lldp dot3-tlv power 802.3at
```

Related Topics

21.6.1 display lldp local
21.6.10 lldp enable (system view)
21.6.9 lldp enable (interface view)

21.6.9 lldp enable (interface view)

Function

The **lldp enable** command enables LLDP on an interface.

The **undo lldp enable** command disables LLDP on an interface.

After LLDP is enabled in the system view, all interfaces are enabled with LLDP.

Format

lldp enable

undo lldp enable

Parameters

None

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Serial interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After LLDP is enabled on an interface, the interface exchanges LLDP packets with LLDP-enabled neighbors. The interface receives status information from the neighbors and sends the local status information to the neighbors. The NMS then obtains the status information for topology discovery.

Prerequisites

The LLDP function has been enabled globally.

Precautions

LLDP can be enabled in the system view and the interface view.

- After LLDP is enabled in the system view, all interfaces are enabled with LLDP.
- After LLDP is disabled in the system view, all LLDP settings are restored to the default settings except the setting of LLDP trap. Therefore, LLDP is also disabled on all interfaces.
- An interface can send and receive LLDP packets only after LLDP is enabled in both the system view and the interface view.
- After LLDP is disabled globally, the commands for enabling and disabling LLDP on an interface do not take effect.
- If LLDP needs to be disabled on some interfaces, enable LLDP globally first, and run the **undo lldp enable** command on these interfaces. To re-enable LLDP on these interfaces, run the **lldp enable** command in the views of these interfaces.

NOTE

- LLDP can be enabled and disabled only on the physical interfaces, but cannot be used on logical interfaces such as VLANIF interface and Eth-Trunk.
- On an Eth-Trunk, LLDP can only be enabled on member interfaces. The interfaces enabled with LLDP and not enabled with LLDP can exist in the same Eth-Trunk.
- Only serial interfaces enabled with PPP and HDLC support LLDP.

Example

Disable LLDP on Ethernet2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] undo lldp enable
Info: The LLDP is disable on the port successfully.
```

Related Topics

21.6.1 display lldp local
21.6.10 lldp enable (system view)

 Copyright © Huawei Technologies Co., Ltd.

21.6.10 lldp enable (system view)

Function

The **lldp enable** command enables LLDP globally.

The **undo lldp enable** command disables LLDP globally.

By default, LLDP is disabled globally.

Format

lldp enable

undo lldp enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To view the Layer 2 link status or analyze network topology, run the **lldp enable** command.

Configuration Impact

After LLDP is enabled globally, the device sends its own status information to LLDP-enabled neighbors and receives the status information from the neighbors.

Precautions

The interval between enabling LLDP globally and disabling LLDP cannot be shorter than 10 seconds; otherwise, an error message is displayed.

LLDP can be enabled in the system view and the interface view.

- After LLDP is enabled in the system view, all interfaces are enabled with LLDP.
- After LLDP is disabled in the system view, all LLDP settings are restored to the default settings except the setting of LLDP trap. Therefore, LLDP is also disabled on all interfaces.
- An interface can send and receive LLDP packets only after LLDP is enabled in both the system view and the interface view.
- After LLDP is disabled globally, the commands for enabling and disabling LLDP on an interface do not take effect.

 Copyright © Huawei Technologies Co., Ltd.

Example

Enable LLDP globally.

```
<Huawei> system-view
[Huawei] lldp enable
Info: Global LLDP is enabled successfully.
```

Disable LLDP globally.

```
<Huawei> system-view
[Huawei] undo lldp enable
Warning: This command will delete the configurations of LLDP on all the ports.Continue?[Y/N]y
Info: Global LLDP is disabled successfully.
```

21.6.11 lldp management-address

Function

The **lldp management-address** command configures the LLDP management IP address.

The **undo lldp management-address** command restores the default setting.

By default, the system automatically obtains the management IP address.

Format

lldp management-address *ip-address*

undo lldp management-address

Parameters

Parameter	Description	Value
ip-address	Specifies the management IP address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The management IP address is carried in the management address TLV field of the LLDP packet. It is used by the NMS to identify and manage devices. A management address identifies a device, facilitating the layout of the network topology and network management. To allocate a management address to a neighbor, run the **lldp management-address** command.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The LLDP function has been enabled globally.

The management IP address to be allocated must be a valid IP address existing on the device.

Configuration Impact

After the configuration, the management IP address is added to the management address TLV field of the LLDP packet. The NMS then identifies the device according to the management IP address.

Precautions

This command cannot be used to configure an IP address for an interface board.

If the configured management IP address is invalid or no management IP address is configured, the system sets an IP address in the address list as the management IP address. The system selects the IP address in the following sequence: loopback interface address, VLANIF interface address, and Layer 3 interface address. Among the IP addresses of the same type, the system selects the smallest one. If the system does not find a management IP address, the bridge MAC address is used as the management IP address.

Example

Set the LLDP management IP address to 10.10.10.1.

```
<Huawei> system-view
[Huawei] lldp management-address 10.10.10.1
```

Related Topics

21.6.1 display lldp local
21.6.10 lldp enable (system view)

21.6.12 lldp message-transmission delay

Function

The **lldp message-transmission delay** command sets the LLDP packet transmission delay.

The **undo lldp message-transmission delay** command restores the default LLDP packet transmission delay.

By default, the LLDP packet transmission delay is 2 seconds.

Format

lldp message-transmission delay *delay*

undo lldp message-transmission delay

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
delay	Specifies the LLDP packet transmission delay.	The value is an integer ranging from 1 to 8192, in seconds. The default value is 2 seconds. The *delay* value depends on the *interval* value in **lldp message-transmission interval**. The *delay* value must be equal to or smaller than a quarter of the *interval* value.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the interface sends an LLDP packet to the neighbor when the device status changes frequently. After the LLDP packet transmission delay is set on the device, the LLDP-enabled interfaces send LLDP packets to neighbors after a delay (the delay is the same as or longer than the delay you specified). The interfaces may send LLDP packets at different time points.

If the device status changes frequently, extend the delay in preventing the device from frequently sending packets to the neighbors. A delay suppresses the network topology flapping.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

The LLDP packet transmission delay must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency when the local device status frequently changes. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.

 Copyright © Huawei Technologies Co., Ltd.

- A small value increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time when the local device status frequently changes. However, if the value is too small, LLDP packets are exchanged frequently, increasing the system load.
- The default value is recommended.

Precautions

Consider the value of *interval* when adjusting the value of *delay* because it is restricted by the value of *interval*.

- The value of *delay* ranges from 1 to 8192.
- The value of *delay* must be smaller than or equal to a quarter of *interval*. Therefore, if you want to set *delay* to be greater than a quarter of *interval*, first increase the *interval* value to four times the new *delay* value, and then increase the *delay* value.

NOTE

If the *interval* value is smaller than four times the *delay* value, the system displays an error message when you run the **undo lldp message-transmission delay** command. To run the **undo lldp message-transmission delay** command in this case, increase the *interval* value to at least four times the *delay* value first.

Example

Set the LLDP packet transmission delay to 5 second.

```
<Huawei> system-view
[Huawei] lldp message-transmission delay 5
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.14 lldp message-transmission interval

21.6.13 lldp message-transmission hold-multiplier

Function

The **lldp message-transmission hold-multiplier** command sets the hold time multiplier of device information stored on neighbors.

The **undo lldp message-transmission hold-multiplier** command restores the default hold time multiplier of device information stored on neighbors.

The default hold time multiplier is 4.

Format

lldp message-transmission hold-multiplier *hold*

undo lldp message-transmission hold-multiplier

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
hold	Specifies the hold time multiplier of device information on neighbors.	The value is an integer ranging from 2 to 10. The default value is 4.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The time multiplier is used to calculate how long a packet can be saved on a neighboring node. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the TTL.

The storage time calculation formula is: TTL = Min (65535, (*interval* x *hold*)).

TTL is the device information storage time. It is the smaller value between 65535 and (*interval* x *hold*).

interval indicates the interval at which the device sends LLDP packets to neighbors. This parameter is set by **lldp message-transmission interval**. *hold* indicates the hold time multiplier of device information on neighbors.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

The hold time multiplier of device information on neighbors must be set to a proper value.

- A large value of *hold* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *hold* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the hold time multiplier of device information on neighbors to 5.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] lldp message-transmission hold-multiplier 5
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.14 lldp message-transmission interval

21.6.14 lldp message-transmission interval

Function

The **lldp message-transmission interval** command sets the LLDP transmission interval.

The **undo lldp message-transmission interval** command restores the default LLDP transmission interval.

The default LLDP transmission interval is 30 seconds.

Format

lldp message-transmission interval *interval*

undo lldp message-transmission interval

Parameters

Parameter	Description	Value
interval	Specifies the LLDP transmission interval.	The value is an integer ranging from 5 to 32768, in seconds. The default value is 30 seconds. The *interval* value depends on the *delay* value in **lldp message-transmission delay**. The value of *interval* must be equal to or greater than four times the value of *delay*. Otherwise, an error occurs in the configuration.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the LLDP status of the device keeps unchanged or the device does not discover new neighbors, the interface sends LLDP packets to the neighbors at a certain interval. After the LLDP transmission interval is set on the device, the LLDP enabled interfaces send LLDP packets to neighbors at this interval. The interfaces may send LLDP packets at different time points.

If you want to change the network topology detection frequency, run the **lldp message-transmission interval** command to change the LLDP transmission interval.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

The LLDP transmission interval must be set properly and adjusted according to network loads.

- A large value reduces the LLDP packet transmission frequency. This helps save system resources. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A short interval increases the LLDP packet transmission frequency and enables the NMS to discover network topology changes in real time. However, if the interval is too short, LLDP packets are exchanged frequently, increasing the system load.
- The default value is recommended.

Precautions

Consider the value of *delay* when adjusting the value of *interval* because it is restricted by the value of *delay*.

- The value of *interval* ranges from 5 to 32768.
- The value of *interval* must be equal to or greater than four times the value of *delay*. Therefore, if you want to set *interval* to be smaller than four times the value of *delay*, first reduce the *delay* value to be equal to or smaller than a quarter of the new *interval* value, and then reduce the *interval* value.

NOTE

If the *delay* value is greater than a quarter of the *interval* value, the system displays an error message when you run the **undo lldp message-transmission interval** command. To run the **undo lldp message-transmission interval** command in this case, reduce the *delay* value to be equal to or smaller than a quarter of *interval* first.

Example

Set the LLDP transmission interval to 35 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] lldp message-transmission interval 35
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.12 lldp message-transmission delay

21.6.15 lldp restart-delay

Function

The **lldp restart-delay** command sets the delay in re-enabling the LLDP function on an interface.

The **undo lldp restart-delay** command restores the default delay in re-enabling the LLDP function on an interface.

The default delay is 2 seconds.

Format

lldp restart-delay *delay*

undo lldp restart-delay

Parameters

Parameter	Description	Value
delay	Specifies the delay in re-enabling the LLDP function on an interface.	The value is an integer ranging from 1 to 10, in seconds. The default value is 2 seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before LLDP is re-enabled on an interface. The delay suppresses the topology flapping caused by the frequent LLDP status changes.

Prerequisites

The LLDP function has been enabled globally.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

The delay in re-enabling the LLDP function on an interface must be set properly.

- A large value of *delay* prevents network topology flapping. However, if the value is too large, the device cannot notify neighbors of its status in a timely manner, and the NMS cannot discover the network topology changes in real time.
- A small value of *delay* enables the NMS to discover topology change in time. However, if the value is too small, the neighbors update device information too frequently. This increases the load on the system and wastes resources.
- The default value is recommended.

Example

Set the delay in re-enabling the LLDP function on an interface to 3 second.

```
<Huawei> system-view
[Huawei] lldp restart-delay 3
```

Related Topics

21.6.1 display lldp local

21.6.10 lldp enable (system view)

21.6.16 lldp tlv-enable

Function

The **lldp tlv-enable** command sets the type of the TLVs that can be sent by an interface.

The **undo lldp tlv-enable** command sets the type of the TLVs disabled on an interface.

By default, an interface advertises all types of TLVs except the Location Identification TLV.

Format

lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** [*vlan-id*] | **vlan-name** [*vlan-id*] | **protocol-identity** }

lldp tlv-enable dot3-tlv { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** { **civic-address** *device-type country-code* { *ca-type ca-value* } & <1-10> | **elin-address** *Tel-Number* } | **network-policy** | **power-over-ethernet** }

undo lldp tlv-enable basic-tlv { **all** | **management-address** | **port-description** | **system-capability** | **system-description** | **system-name** }

 Copyright © Huawei Technologies Co., Ltd.

undo lldp tlv-enable dot1-tlv { **all** | **port-vlan-id** | **protocol-vlan-id** | **vlan-name** | **protocol-identity** }

undo lldp tlv-enable dot3-tlv { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }

undo lldp tlv-enable med-tlv { **all** | **capability** | **inventory** | **location-id** [**civic-address** | **elin-address**] | **network-policy** | **power-over-ethernet** }

Parameters

Parameter	Description	Value
all	• Indicates to advertise all types of TLVs when the device advertises basic TLVs, TLVs in the IEEE 802.1 format, and TLVs in the IEEE 802.3 format. • After the **all** parameter is specified, all MED TLVs except the Location Identification TLV are advertised.	-
basic-tlv	Indicates to advertise basic TLVs that include: • Management-address TLV • Port Description TLV • System Capabilities TLV • System Description TLV • System Name TLV	-
management-address	Indicates to advertise Management-address TLV.	-
port-description	Indicates to advertise Port Description TLV.	-
system-capability	Indicates to advertise System Capabilities TLV.	-
system-description	Indicates to advertise System Description TLV.	-
system-name	Indicates to advertise System Name TLV.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
dot1-tlv	Indicates to advertise the TLVs in the IEEE 802.1 format that include: ● Port VLAN TLV ● Port protocol VLAN TLV ● VLAN Name TLV ● Protocol identity TLV **NOTE** Only Layer 2 physical interfaces such as Ethernet and GE interfaces support **dot1-tlv** and related parameters.	-
port-vlan-id	Indicates to advertise port VLAN TLV. The VLAN ID is the default VLAN ID on the interface.	-
protocol-vlan-id [*vlan-id*]	Indicates to advertise port protocol VLAN TLV. If *vlan-id* is not specified, the interface does not support protocol VLAN TLVs.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
vlan-name [*vlan-id*]	Indicates to advertise VLAN Name TLV. If *vlan-id* is not specified, the default VLAN ID is used.	The value of *vlan-id* is an integer that ranges from 1 to 4094.
protocol-identity	Indicates to advertise protocol identity TLV.	-
dot3-tlv	Indicates to advertise the TLVs in the IEEE 802.3 format that include: ● Link Aggregation TLV ● MAC/PHY Configuration/Status TLV ● Maximum Frame Size TLV ● Power Via MDI TLV	-
link-aggregation	Indicates to advertise Link Aggregation TLV.	-
mac-physic	Indicates to advertise MAC/PHY Configuration/Status TLV.	-
max-frame-size	Indicates to advertise Maximum Frame Size TLV.	-
power	Indicates to advertise Power Via MDI TLV.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
med-tlv	Indicates to advertise MED TLVs that include: ● LLDP-MED Capabilities TLV ● Inventory TLV ● Location Identification TLV ● Network Policy TLV ● Extended Power-via-MDI TLV	-
capability	Indicates to advertise MED Capabilities TLV.	-
inventory	Indicates to advertise Hardware Revision TLV, Firmware Revision TLV, Software Revision TLV, Serial Number TLV, Manufacturer Name TLV, Model Name TLV, and Asset ID TLV.	-
location-id	Indicates to advertise Location Identification TLV.	-
civic-address *device-type country-code* { *ca-type ca-value* } & <1-10>	Indicates to advertise the common address information of the network devices encapsulated in Location Identification TLV. ● *device-type* specifies the type of the device. The value is an integer that ranges from 0 to 2. 0 indicates that the device is a DHCP server. 1 indicates that the device is a switch. 2 indicates that the device is an MED endpoint. ● *country-code* specifies the country code. For the value range, see ISO 3166. ● { *ca-type ca-value* }&<1-10> specifies the address information. *ca-type* specifies the type of address information. The value is an integer that ranges from 0 to 255. *ca-value* specifies the content of the address information. The value is a string of 1-250 characters. **<1-10>** indicates that the preceding parameters can be entered 10 times.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
elin-address *Tel-Number*	Advertises the emergency phone number encapsulated in Location Identification TLV.	The value is a string of 10 to 25 numerals. Each numeral ranges from 0 to 9.
network-policy	Advertises Network Policy TLV. Network Policy TLV is used to exchange VLAN configurations between network devices and terminal devices. A switch uses the TLV to advertise voice VLAN ID and voice stream priority to an IP phone. Then the IP phone forwards packets according to the received voice VLAN ID and priority, ensuring the voice quality.	-
power-over-ethernet	Advertises Extended Power via MDI TLV.	-

Views

Ethernet interface view, GE interface view, XGE interface view, port group view, Serial interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In LLDP, all device information is encapsulated in Link Layer Discovery Protocol data units (LLDPDUs), which are then sent to neighbors. An LLDPDU contains a variety of TLVs. In a TLV, T indicates the information type, L indicates the information length, and V indicates the value or the content to be sent.

Devices exchange LLDPDUs carrying TLVs to obtain neighbor information. The TLVs that can be encapsulated in an LLDP packet include basic TLVs, TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Basic TLVs are essential for managing network devices. The TLVs in the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs are defined by standardization organizations and other organizations, which are used to enhance the network device management. You can determine whether to advertise the IEEE 802.1 format, TLVs in the IEEE 802.3 format, and MED TLVs.

Devices on both ends can have different TLV types configured. You only need to configure TLV types according to networking requirements.

 Copyright © Huawei Technologies Co., Ltd.

Prerequisites

The LLDP function is enabled globally and on interfaces.

Precautions

- When the supported TLVs are basic TLVs, TLVs in the IEEE 802.1 format, and TLVs in the IEEE 802.3 format, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs. When the supported TLVs are MED TLVs, the **lldp tlv-enable** command with the **all** parameter advertises all TLVs except Location Identification TLV.

  If the **all** parameter is not specified, only one type of TLV can be advertised. To advertise multiple types of TLVs, run this command multiple times.
- You can specify the other types of MED TLVs only after specifying the MED Capabilities TLV.

  To disable the MED Capabilities TLV, first disable the other types of MED TLVs.

  To disable the MAC/PHY Configuration/Status TLVs, first disable the MED Capabilities TLV.
- The 802.3 MAC/PHY Configuration/Status TLVs are automatically advertised after the MED Capabilities TLV is advertised.
- If you disable the MED TLVs using the command with the **all** parameter, the 802.3 MAC/PHY Configuration/Status TLVs are not disabled automatically.
- A serial interface can advertise only basic TLVs.

Example

Configure Ethernet2/0/0 to advertise the Link Aggregation TLV in the IEEE 802.3 format.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] lldp tlv-enable dot3-tlv link-aggregation
```

Related Topics

21.6.10 lldp enable (system view)
21.6.5 display lldp tlv-config

21.6.17 lldp tlv-enable private-tlv authentication

Function

The **lldp tlv-enable private-tlv authentication** command enables LLDP packet authentication.

The **undo lldp tlv-enable private-tlv authentication** command disables LLDP packet authentication.

By default, LLDP packet authentication is disabled.

Format

lldp tlv-enable private-tlv authentication password { **simple** | **cipher** } *password*

 Copyright © Huawei Technologies Co., Ltd.

undo lldp tlv-enable private-tlv authentication

Parameters

Value	Description	Value
simple	Indicates the password in plain text. **NOTICE** If **simple** is selected, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text.	-
cipher	Indicates the password in cipher text. The password is displayed in cipher text.	-
password	Specifies the password for LLDP packet authentication.	The value is a string of case-sensitive characters without command line characters such as spaces and question marks (?). ● When **simple** is specified, the password is in plaintext and contains 1 to 32 characters. ● When **cipher** is specified, the password can be either in ciphertext or plaintext, depending on what is entered. The password in plaintext contains 1 to 32 characters, such as **huawei123**. The password in ciphertext must be a string of 48 characters, for example, **%^%#/}pb(9>!)4@plQ<Z]@UG2WH45|y/DE=%p<5K,ZJU%^%#**.

Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, GE interface view, XGE interface view, port group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the **lldp tlv-enable private-tlv authentication** command is run an interface, the interface is blocked immediately and can be connected only when the password in LLDP packets sent from the peer end is the same as that configured on the interface.

Prerequisites

The LLDP function has been enabled globally.

Precaution

This command only supports configuration on Layer 2 interface.

Example

Enable LLDP packet authentication on Ethernet2/0/0 and set the password in plaintext to **huawei123**.

```
<Huawei> system-view
[Huawei] interface Ethernet 2/0/0
[Huawei-Ethernet2/0/0] lldp tlv-enable private-tlv authentication password simple huawei123
```

Related Topics

21.6.10 lldp enable (system view)

21.6.18 lldp trap-interval

Function

The **lldp trap-interval** command sets the delay in sending neighbor change traps to the NMS.

The **undo lldp trap-interval** command restores the default delay in sending neighbor change traps to the NMS.

By default, the device sends a neighbor change trap to the NMS after a 5-second delay.

Format

lldp trap-interval *interval*

undo lldp trap-interval

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interval	Specifies the delay in sending traps.	The value is an integer ranging from 5 to 3600, in seconds. The default value is 5 seconds. The default value is recommended.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

There is a delay before the device sends LLDP traps about neighbor information changes to the NMS. When neighbor information changes frequently, you can prolong the delay. In this way, the device will not frequently send traps to the NMS, and the network topology flapping is suppressed.

Prerequisites

The LLDP function has been enabled globally.

Configuration Impact

After the delay is set on the device, LLDP-enabled interfaces send LLDP traps to neighbors after a delay (the delay is the same as or longer than the delay you specified). The interfaces may send LLDP traps at different time points.

Precautions

The configured delay applies only to the trap, which reports changes in neighbor information, including the number of added neighbors, number of deleted neighbors, number of neighbors that are aged out, and number of neighbors of which the information is deleted.

Example

Set the delay in sending neighbor change traps to 6 seconds.

```
<Huawei> system-view
[Huawei] lldp trap-interval 6
```

Related Topics

21.6.1 display lldp local

 Copyright © Huawei Technologies Co., Ltd.

21.6.10 lldp enable (system view)

21.6.19 reset lldp statistics

Function

The **reset lldp statistics** command clears LLDP packet statistics on all interfaces or on a specified interface.

Format

reset lldp statistics [**interface** *interface-type interface-number*]

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Specifies the type and number of the interface where the LLDP statistics you want to reset. In the command: • *interface-type* specifies the interface type. • *interface-number* specifies the interface number. If no interface is specified, LLDP packet statistics of all interfaces are cleared.	-

Views

User view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To troubleshoot LLDP faults, you may need to view LLDP packet statistics within a certain period of time. In this case, you must run the **reset lldp statistics** command to clear existing LLDP packet statistics, and run the **display lldp statistics** command to view the new LLDP packet statistics.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The LLDP function has been enabled globally and on interfaces.

Example

Clear LLDP packet statistics on all interfaces.

```
<Huawei> reset lldp statistics
Warning: This Command will clear LLDP statistics of all the ports. Continue? [Y/N]:y
```

Clear LLDP packet statistics of Ethernet2/0/0.

```
<Huawei> reset lldp statistics interface ethernet 2/0/0
```

Related Topics

21.6.4 display lldp statistics
21.6.10 lldp enable (system view)

21.6.20 snmp-agent trap enable feature-name lldptrap

Function

The **snmp-agent trap enable feature-name lldptrap** command enables the LLDP trap function on the device.

The **undo snmp-agent trap enable feature-name lldptrap** command disables the LLDP trap function on the device.

By default, the LLDP trap function is enabled.

Format

snmp-agent trap enable feature-name lldptrap [**trap-name** { **hwlldpdisabled** | **hwlldpenabled** | **hwlldplocmanipaddrchange** | **lldpremtableschange** }]

undo snmp-agent trap enable feature-name lldptrap [**trap-name** { **hwlldpdisabled** | **hwlldpenabled** | **hwlldplocmanipaddrchange** | **lldpremtableschange** }]

Parameters

Parameter	Description	Value
trap-name	Enables or disables the trap function for the specified event.	-
hwlldpdisabled	Sends a Huawei proprietary trap when the LLDP function is disabled globally.	-
hwlldpenabled	Sends a Huawei proprietary trap when the LLDP function is enabled globally.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
hwlldplocmanipaddrch-ange	Sends a Huawei proprietary trap when the LLDP management address of the device changes.	-
lldpremtableschange	Sends a trap when LLDP neighbor information changes.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To enable the device to send traps when the LLDP status changes, run the **snmp-agent trap enable feature-name lldptrap** command.

Prerequisites

A reachable route exists between the device and the NMS, and the SNMP parameters are set.

Configuration Impact

After the LLDP trap function is enabled, the device sends traps to the NMS in one of the following cases:

- The LLDP function is enabled or disabled globally.
- The local management address changes.
- A neighbor is added, deleted, discarded, or aged out.

Precautions

The LLDP trap function applies to all interfaces.

If the network topology is unstable, disable the LLDP trap function to prevent frequent trap sending.

To set the interval between sending neighbor change traps to the NMS, run the **lldp trap-interval** command. If neighbor information changes frequently, extend the interval to reduce the number of traps.

Example

Enable the LLDP trap function on the device.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name lldptrap
```

Related Topics

21.6.6 display snmp-agent trap feature-name lldptrap all

21.7 NQA Configuration Commands

21.7.1 adv-factor

Function

The **adv-factor** command configures an advantage factor for simulated voice calculation in an NQA jitter test.

The **undo adv-factor** command restores the default setting.

By default, the advantage factor for simulated voice test calculation is 0.

Format

adv-factor *factor-value*

undo adv-factor

Parameters

Parameter	Description	Value
factor-value	Specifies the advantage factor for simulated voice test calculation.	The value is an integer that ranges from 0 to 20. The default value is 0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

On a network bearing VoIP services, a jitter test is used to test VoIP service quality. The **adv-factor** command is used to configure the advantage factor for voice test calculation to simulate packet jitter generated by actual voice packets.

When calculating the quality parameter R value of the voice transmission network, a test engineer needs to specify an advantage factor according to the transmission distance and media. The value shows the expected compensation for voice quality

 Copyright © Huawei Technologies Co., Ltd.

degradation during network transmission. The user-defined value is determined by the type of the network to be tested. The higher the expected level of service quality degradation, the greater the value. The *factor-value* parameter shows tolerance over a certain level of voice quality degradation during network transmission.

For example:

- Set the advantage factor to 0 in testing a common wire communication system.
- Set the advantage factor to 20 in testing a multi-hop FR network connected to the satellite.

Prerequisites

The **adv-factor** command can be used only after the following conditions are met:

- The UDP jitter test is used.
- The code type for the simulated voice test of a jitter test instance has been set using the **jitter-codec** command. The code types of g711a, g711u, and g729a are applied to the VoIP applications of conversion between simulated voice signals and digital signals.
- The **nqa-server udpecho** command has been run on the remote device to respond to the jitter test.

Configuration Impact

If the advantage factor has been configured, running the **adv-factor** command will override the previous configuration.

If the code type is changed after the **jitter-codec** command is run, the configured advantage factor does not take effect and you need to configure a new advantage factor.

Precautions

The advantage factor of a running test instance cannot be changed.

Example

Set the advantage factor for a simulated voice test calculation to 20.

```
<Huawei> system-view
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] jitter-codec g711a
[Huawei-nqa-admin-jitter] adv-factor 20
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.46 jitter-codec

 Copyright © Huawei Technologies Co., Ltd.

21.7.2 agetime

Function

The **agetime** command sets the aging time of an NQA test instance.

The **undo agetime** command restores the default aging time of an NQA test instance.

The default aging time of an NQA test instance is 0, indicating that the test instance is not aged.

Format

agetime *hh:mm:ss*

undo agetime

Parameters

Parameter	Description	Value
hh:mm:ss	Specifies the aging time.	*hh* ranges from 0 to 23; *mm* ranges from 0 to 59; *ss* ranges from 0 to 59.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent endless running of a test instance, you need to age the test instance periodically. The **agetime** command can be used to configure the aging time to change the survival time of a test instance in the system.

- The aging time is started when the NQA test instance is in the inactive state. When the aging time expires, the system deletes the NQA test instance automatically.
- The aging time is reset when the NQA test instance is in the active state.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

The aging time of a running test instance cannot be changed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the aging time of NQA test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] agetime 1:0:0
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.3 alarm

Function

The **alarm** command sets an alarm threshold for the monitored item of an NQA test result.

The **undo alarm** command deletes an alarm threshold for the monitored item of an NQA test result.

By default, no alarm threshold is configured for the monitored item of an NQA test result.

Format

alarm *entry-number* { **jitter-average** | **jitter-ds-average** | **jitter-sd-average** | **lost-packet-ratio** | **packet-loss-ds** | **packet-loss-sd** | **rtt-average** } { **absolute** | **delta** } { **falling-threshold** *threshold-value1 event-entry1* | **rising-threshold** *threshold-value2 event-entry2* } * [**description** *description*]

undo alarm [*entry-number*]

Parameters

Parameter	Description	Value
entry-number	Specifies the index of an entry.	The value is an integer that ranges from 1 to 65535.
jitter-average	Indicates the average jitter value. This value is available only for jitter test instances.	-
jitter-ds-average	Indicates the average jitter value of packets from the destination to the source. This value is available only for jitter test instances.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
jitter-sd-average	Indicates the average jitter value of packets from the source to the destination. This value is available only for jitter test instances.	-
lost-packet-ratio	Indicates the packet loss ratio. This value is available for all test instances.	-
packet-loss-ds	Indicates the number of lost packets sent from the destination to the source. This value is available only for jitter test instances.	-
packet-loss-sd	Indicates the number of lost packets sent from the source to the destination. This value is available only for jitter test instances.	-
rtt-average	Indicates the average round trip time (RTT). This value is available for all test instances.	-
absolute	Indicates an absolute sampled value, which refers to the sampled value obtained this time.	-
delta	Indicates a relative sampled value, which refers to a changed value comparing with the last sampled value	-
falling-threshold *threshold-value1*	Specifies the lower threshold.	The value is an integer that ranges from 0 to 2147483647.
event-entry1	Specifies the index of the entry corresponding to the lower threshold in the event table.	The value is an integer that ranges from 1 to 65535.
rising-threshold *threshold-value2*	Specifies the upper threshold.	The value is an integer that ranges from 0 to 2147483647.
event-entry2	Specifies the index of the entry corresponding to the upper threshold in the event table.	The value is an integer that ranges from 1 to 65535.
description	Indicates the description of this alarm.	The value is a string of 1 to 127 case-sensitive characters with spaces supported.

Views

NQA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the monitored item of an NQA test result exceeds the threshold, the system sends an alarm to the NMS.

According to the NQA alarm mechanism, an alarm is generated when the monitored item exceeds the threshold only after an alarm threshold and an alarm event are both configured. The system will generate an alarm if the monitored item exceeds the upper or lower threshold configured in the event table. If an incorrect alarm variable is specified, for example, an inexistent OID is specified, no alarm will be generated.

You can run the **alarm** command to add or delete an alarm entry in the NQA alarm table. If an alarm variable is specified, an alarm is generated when the system becomes abnormal. If the monitored item exceeds the threshold, an alarm is generated.

Prerequisites

An event has been associated with the NQA alarm using the **nqa event** command. An alarm table is determined by an event table. The entry number in an event table and the event number specified by an alarm must be consistent. Otherwise, if you run the **alarm** command, the system will display a message indicating that the alarm event does not exist.

The trap function has been enabled for the NQA module using the **snmp-agent trap enable feature-name nqa** command and the route between the device and NMS is reachable. In this way, NQA alarms can be sent to the network management system (NMS).

Configuration Impact

Ensure that the alarm entry to be entered is unique. If an alarm entry number exists and you enter the same entry number, the new entry number will override the configuration to which the original alarm corresponds.

Example

Configure alarms to be sent when the packet loss ratio exceeds the threshold.

```
<Huawei> system-view
[Huawei] nqa event 10 trap
[Huawei] nqa event 100 trap
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] alarm 10 lost-packet-ratio absolute falling-threshold 10 10 rising-threshold 100 100
```

Related Topics

21.7.58 nqa event

21.7.56 nqa

 Copyright © Huawei Technologies Co., Ltd.

21.7.4 clear-records

Function

The **clear-records** command clears statistics on NQA test instances.

Format

clear-records

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Clearing statistics on the ongoing test is forbidden.

Before running the command, ensure that the test type specified by the **test-type** command exists.

Example

Clear all statistics on NQA test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] clear-records
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.18 display nqa history

21.7.20 display nqa results

21.7.5 community read cipher

Function

The **community read cipher** command configures the community name for SNMP test.

The **undo community** command deletes the community name of SNMP test.

 Copyright © Huawei Technologies Co., Ltd.

By default, the community name for SNMP test is public.

Format

community read cipher *community-name*

undo community

Parameters

Parameter	Description	Value
community-name	Specifies the community name for SNMP test.	The value is a string of case-sensitive characters without command line characters such as spaces and question marks. The length ranges from 1 to 32 for plain text and ranges from 32 to 68 for cipher text. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A community, uniquely identified by a community name, defines administrative relationships between NMSs and SNMP agents. The community name acts like a password to regulate access to an SNMP agent. An NMS can access an SNMP agent only if the community name carried in the SNMP request sent by the NMS is the same as the community name configured on the SNMP agent.

When the SNMP versions on agents are SNMPv1 or SNMPv2c, the community name must be configured using the **community read cipher** command, and the community name must be a read-only community name on SNMP agents. When the SNMP versions on agents are SNMPv3, the community name does not need to be configured because SNMPv3 does not support community names.

Prerequisites

The NQA test instance has been configured using the **nqa** command, and the test instance type has been set to SNMP using the **test-type** command.

Example

Set the community name for SNMP test.

```
<Huawei> system-view
[Huawei] nqa test-instance user test1
```

 Copyright © Huawei Technologies Co., Ltd.

```
[Huawei-nqa-user-test1] test-type snmp
[Huawei-nqa-user-test1] community read cipher Huawei-123
```

21.7.6 datafill

Function

The **datafill** command configures pad characters in an NQA test instance.

The **undo datafill** command deletes the pad characters in an NQA test instance.

By default, there are no padding characters in an NQA test instance.

Format

datafill *fillstring*

undo datafill

Parameters

Parameter	Description	Value
fillstring	Specifies the pad characters for NQA test packets.	The value is a string of 1 to 230 case-sensitive characters with spaces supported. The question mark (?) is not supported. The default value is 0 (an empty pad character).

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test, you need to simulate actual datagrams to obtain more accurate statistics. The **datasize** command can be used to set the size of the Data field. To differentiate packets sent from different test instances, add the specified characters to identify the test packets.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type can be one of the following:

- UDP
- Jitter
- ICMP

 Copyright © Huawei Technologies Co., Ltd.

- Trace
- LSP Ping

Configuration Impact

After the **datafill** command is run, the following situations may occur:

- If the length of the data packet sent from the test instance is shorter than the configured pad character, only the forepart of the pad character can be used.
- If the length of the data packet sent from the test instance is larger than the configured pad character, the pad character is repeated in sequence until the data packet is successfully padded.

For example, the pad character is set to **abcd**. If the length of the test packet is 3, only **abc** is used to pad the test packet. If the length of the test packet is 6, **abcdab** is used to pad the test packet.

Precautions

The pad character of a running test instance cannot be changed.

Example

Set the pad characters of the test named **user test** to **abcd**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] datafill abcd
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.7 datasize

21.7.7 datasize

Function

The **datasize** command sets the size of the NQA test packet.

The **undo datasize** command restores the size of the NQA test packet.

The default size is 0, which indicates that the test packet does not carry data information.

Format

datasize *size*

undo datasize

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
size	Specifies the size of the NQA test packet.	The value is an integer that ranges from 0 to 8100, in bytes. If the configured size of a packet is smaller than the default size of a packet, the configured size is invalid and the packet is forwarded based on its default size. **NOTE** When you run the **hardware-based enable** command for a Jitter test instance, the value ranges from 0 to 1472, in bytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **datasize** command to set the size of the data field of a test packet. This ensures that the size of the test packet is closer to the size of the actual data packet and the obtained statistics are more accurate.

For example, if a UDP jitter test instance is used to detect voice over IP (VoIP) services, you can run the **datasize** command to set the size of the NQA test packet to the same size as the actual voice packet. This enables a simulation of the actual traffic that occurs in a period of time.

To simulate a voice data flow with the transmission rate of 64 kbit/s, you can set the size of the voice packet to 172 bytes (160-byte payload + 12-byte RTP header + 28-byte IP header and UDP header) and set the interval for sending the voice packet to 20 ms. In this manner, 3000 packets can be sent in one minute.

Prerequisites

The test type has been specified using the **test-type** command.

The **datasize** command is applicable only to the ICMP, UDP, trace, LSP ping, and jitter test instances.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

You cannot change the size of the running test packets.

Example

Set the size of the packets to 100 bytes in the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] datasize 100
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.41 interval (NQA view)

21.7.6 datafill

21.7.8 description (NQA view)

Function

The **description** command configures description of an NQA test instance.

The **undo description** command deletes the description of an NQA test instance.

By default, no description is configured for an NQA test instance.

Format

description *string*

undo description

Parameters

Parameter	Description	Value
string	Specifies the description of an NQA test instance.	The value is a string of 1 to 230 case-sensitive characters with spaces.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The **description** command can be used to briefly describe the test instance to help maintenance. Generally, the test item or the test objective of a test instance is described.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Configuration Impact

If the description of a test instance has been configured, running the **description** command will override the previous configuration.

Precautions

The description of a running test instance cannot be changed.

Example

Set the description of the test named **user test** to fortest.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] description fortest
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.9 destination-address

Function

The **destination-address** command specifies the destination address of an NQA test instance.

The **undo destination-address** command deletes the destination address of an NQA test instance.

By default, destination address is not configured for an NQA test instance.

Format

destination-address { **ipv4** *ipv4-address* [**lsp-masklen** *masklen* [**lsp-loopback** *loopback-address*] [**vpn-frr-path**] | **lsp-loopback** *loopback-address* [**lsp-masklen** *masklen*] [**vpn-frr-path**] | **vpn-frr-path**] | **ipv6** *ipv6-address* | **url** *urlstring* }

destination-address mac *mac-address*

undo destination-address

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4 *ipv4-address*	Specifies an IPv4 destination address.	The IPv4 address is in dotted decimal notation.
lsp-masklen *masklen*	Specifies the mask length of an LSP's IPv4 address prefix.	The value is an integer that ranges from 0 to 32.
lsp-loopback *loopback-address*	Specifies a 127/8 IP address in the MPLS echo request packet header.	-
vpn-frr-path	Indicates that the connectivity of the backup VPN FRR LSP will be checked.	-
ipv6 *ipv6-address*	Specifies an IPv6 destination address.	The value is a 32-digit hexadecimal number, in the format X:X:X:X:X:X:X:X.
url *urlstring*	Specifies a destination URL address.	The value is a string of 1 to 230 case-insensitive characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
mac *mac-address*	Indicates the unicast MAC address.	A MAC address in the format of H-H-H. Each H stands for one to four hexadecimal characters.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **destination-address** command to specify the destination address of an NQA test instance.

Precautions

- The Label Switched Path (LSP) parameters can be configured only for the LSP test instances.
- You cannot configure destination IP address for DHCP test instances.
- You can specify the destination address as a URL address only for the HTTP, trace, and DNS test instances.

 Copyright © Huawei Technologies Co., Ltd.

- The destination addresses of DNS test instances must be URL addresses but cannot be IPv4 addresses, and the destination URL addresses must contain dots (.); otherwise, the test may fail.
- You cannot change the destination address of a running test instance.

Example

Configure the destination address for test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] destination-address ipv4 10.1.1.1
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.10 destination-port

Function

The **destination-port** command configures the destination port number for an NQA test.

The **undo destination-port** command restores the default setting.

By default, no destination port number is specified for an NQA test.

Format

destination-port *port-number*

undo destination-port

Parameters

Parameter	Description	Value
port-number	Specifies the destination port number.	The value is integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

NQA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies to only the FTP, HTTP, Jitter, TCP, UDP, and Trace test instances.

Precautions

You cannot change the destination port number of the test that is being performed.

Example

Set the destination port number to 2020 for the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] destination-port 2020
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.11 display ip nqa-compatible responder statistics

Function

The **display ip nqa-compatible responder statistics** command displays statistics on the NQA handshake packets sent from the third-party device or NMS software.

Format

display ip nqa-compatible responder statistics

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

When a device works with a third-party device or NMS software to perform UDP-Echo or UDP-Jitter packets, this command displays statistics about NQA handshake packets sent from the third-party device or NMS software.

Prerequisites

The device is configured to respond to the UDP tests initiated by the third-party device or NMS software.

Example

Display statistics on NQA handshake packets sent from the third-party device or NMS software.

```
<Huawei> display ip nqa-compatible responder statistics
IP NQA-COMPATIBLEs Responder is: Enabled
Number of control message received:4
Recent success sources:
Number of successes:2
SIP            DIP            Sport  Dport  Tos  Time
-------------------------------------------------------------------------------
10.10.10.26    10.10.10.14    30000  40000  36   [21:13:02.028 UTC 20 06 2013]
10.10.10.26    10.10.10.14    30000  40000  36   [21:13:12.008 UTC 20 06 2013]
Recent fail sources:
Fail reason: IP,PortNum or Tos matching failure.
Number of failures:2
SIP            DIP            Sport  Dport  Tos  Time
-------------------------------------------------------------------------------
10.10.10.28    10.10.10.14    30001  40001  38   [21:13:06.358 UTC 20 06 2013]
10.10.10.28    10.10.10.14    30001  40001  38   [21:13:11.368 UTC 20 06 2013]
```

Table 21-40 Description of the display ip nqa-compatible responder statistics command output

Item	Description
IP NQA-COMPATIBLEs Responder is	Whether the device is enabled to respond to UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software.
Number of control message received	Number of received handshake packets.
Recent success sources	The third-party packets that are successfully received.
Number of successes	Number of packets that are successfully received.
SIP	Source IP address of packets.
DIP	Destination IP address of packets.
Sport	Source port of packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Dport	Destination port of packets.
Tos	Packet priority.
Time	Packet receiving time.
Recent fail sources	The third-party packets that are failed to be received.
Fail reason	Reason of packet receiving failure.
Number of failures	Number of packets that are failed to be received.

21.7.12 display nqa application

Function

The **display nqa application** command displays the type of the NQA test instance that corresponds to the service.

Format

display nqa application

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You need to choose a proper NQA test instance type based on the service to be tested. You can run the **display nqa application** command to view the type of the NQA test instance that corresponds to the service.

NOTE

You can run this command to view the type of the NQA test instance corresponding to the service. However, the test instance that can be configured on the device uses the test instanced configured in the **test-type** command as an example.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display the type of the NQA test instance corresponding to the service.

```
<Huawei> display nqa application
Application: The area that you test.
Subclasss  : The subclass of application.
NQA type   : The type of NQA test-instance.
Application            Subclass              NQA type
--------------------------------------------------------------------------------
internet               ---                   http
                                             ftp
                                             dns
                                             dhcp

streaming media        ---                   jitter

network performance    ---                   jitter

trouble-shooting       application           http
                                             ftp
                                             dns
                                             dhcp
                                             snmp

                       network               udp
                                             tcp
                                             icmp
                                             trace

                       link

                       mpls                  lspping
                                             lsptrace
```

Table 21-41 Description of the display nqa application command output

Item	Description
Application	Service type.
Subclasss	Service sub-type.
NQA type	Type of the corresponding NQA test instance.

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.13 display nqa alarm

Function

The **display nqa alarm** command displays alarms of an NQA test instance.

Format

display nqa alarm [**test-instance** *admin-name test-name*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
test-instance *admin-name*	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 characters.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 characters.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display nqa alarm** command to display current alarms of a specified test instance or all test instances.

NOTE

To display alarms of a single test instance, ensure that the specified test instance exists.

Example

Display alarms of a single NQA test instance.

```
<Huawei> display nqa alarm test-instance admin jitter
NQA Alarm Information:
-------------------------------------------------------------------
Admin-Name   Operation-Tag   Alarm-Entry   AlarmType   Event-Entry
-------------------------------------------------------------------
admin        jitter          10            Rising      10
admin        jitter          10            Falling     10
```

Table 21-42 Description of the display nqa alarm test-instance admin jitter command output

Item	Description
Admin-Name	Administrator of an NQA test instance.
Operation-Tag	Name of the test instance.
Alarm-Entry	Alarm number.
AlarmType	Alarm type.
Event-Entry	Associated event number.

Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.3 alarm

21.7.14 display nqa-alarm

Function

The **display nqa-alarm** command displays the maximum number of NQA alarms that the system allows and the number of current NQA alarms.

Format

display nqa-alarm

Parameters

None

Views

NQA view

Default Level

1: Monitoring level

Usage Guidelines

After you run the **display nqa-alarm** command, the maximum number of NQA alarms that the system allows and the number of current NQA alarms are displayed.

Example

Display the number of NQA alarms.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] display nqa-alarm
NQA alarm information:
-----------------------------------------------------
NQA Alarm Max: 5                NQA Alarm Number: 0
-----------------------------------------------------
```

Table 21-43 Description of the display nqa-alarm command output

Item	Description
NQA Alarm Max	Maximum number of NQA alarms that the system allows.
NQA Alarm Number	Number of current NQA alarms.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.56 nqa
21.7.3 alarm

21.7.15 display nqa event

Function

The **display nqa event** command displays the event associated with the alarm.

Format

display nqa event [*event-entry*]

Parameters

Parameter	Description	Value
event-entry	Specifies the index of the entry that is associated with the alarm in the event table. If this parameter is not specified, all events associated with alarms are displayed.	The value is an integer that ranges from 1 to 65535.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display nqa event** command to view the event associated with the NQA alarm.

Example

Display event 10.

```
<Huawei> display nqa event 10
NQA Event Information:
-----------------------------------------------------------------------------
Event-Entry     Event-type     Description     Admin-Name     Operation-Tag
-----------------------------------------------------------------------------
10              linkage        None            admin          icmp
```

Table 21-44 Description of the display nqa event command output

Item	Description
Event-Entry	Number of the entry in the event table.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Event-type	Event type.
Description	Event description.
Admin-Name	Name of the administrator.
Operation-Tag	Name of linkage test instance.

Related Topics

21.7.58 nqa event

21.7.16 display nqa-event

Function

The **display nqa-event** command displays the maximum number of NQA events that the system allows and the number of configured NQA events.

Format

display nqa-event

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

The **display nqa-event** command displays the maximum number of NQA events that the system allows and the number of NQA events that have been configured.

Example

Display information about NQA events.

```
<Huawei> display nqa-event
NQA event information:
-----------------------------------------------------
NQA Event Max: 100              NQA Event Number: 0
-----------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-45 Description of the display nqa-event command output

Item	Description
NQA Event Max	Maximum number of NQA events that the system allows.
NQA Event Number	Number of configured NQA events.

Related Topics

21.7.58 nqa event

21.7.17 display nqa-group

Function

The **display nqa-group** command displays NQA group status.

Format

display nqa-group [*group-name*]

Parameters

Parameter	Description	Value
group-name	Specifies the name of an NQA group.	The value is a string of 1 to 32 case-sensitive characters without spaces or question marks. If the character string is quoted by double quotation marks, the character string can contain spaces and question marks.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view NQA group status, run the **display nqa-group** command. By viewing NQA group status, you can know whether the probe of an NQA group is successful and the probe result of each NQA test instance, facilitating fault location.

If the *group-name* parameter is not specified, status of all NQA groups is displayed.

 Copyright © Huawei Technologies Co., Ltd.

Example

View NQA group status.

```
<Huawei> display nqa-group
NQA-group information:
--------------------------------------------------------------------------------
 NQA-group group1
      Admin-name                  Test-name                   State
  NQA  admin1                     test1                     NA
  NQA  admin2                     test2                     NA
  NQA  admin3                     test3                     NA
 NQA-group group2
      Admin-name                  Test-name                   State
  NQA  admin4                     test4                     NA
  NQA  admin5                     test5                     NA
--------------------------------------------------------------------------------
```

Table 21-46 Description of the **display nqa-group** command output

Item	Description
NQA-group	Name of an NQA group.
Admin-name	Administrator of an NQA test instance.
Test-name	Name of an NQA test instance.
State	NQA group status: • UP: The probe of the NQA test instance is successful. • DOWN: The probe of the NQA test instance fails. • NA: The NQA test instance does not exist or the NQA test instance type is not ICMP. The probe of an NQA group is considered to be successful as long as the probe of one NQA test instance in the group is successful. If the probes of all NQA test instances fail, the probe of the NQA group fails.
NQA	NQA test instance information, including the administrator, name, and status of an NQA test instance.

Related Topics

21.7.69 nqa-group
21.7.57 nqa (NQA group view)

21.7.18 display nqa history

Function

The **display nqa history** command displays the history records about an NQA test.

 Copyright © Huawei Technologies Co., Ltd.

Format

display nqa history [**test-instance** *admin-name test-name*] [**from** *start-date start-time* **to** *end-date end-time*]

Parameters

Parameter	Description	Value
test-instance	Indicates NQA test instances.	-
admin-name	Specifies the name of the administrator for an NQA test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
test-name	Specifies the name of an NQA test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
start-date	Specifies the start date, in the format of YYYY/MM/DD.	YYYY specifies a year that ranges from 2000 to 2099; MM specifies a month that ranges from 1 to 12; DD specifies a day that ranges from 1 to 31.
start-time	Specifies the start time, in the format of HH:MM:SS.	HH specifies an hour that ranges from 0 to 23; MM specifies a minute that ranges from 0 to 59; SS specifies a second that ranges from 0 to 59.
end-date	Specifies the end date, in the format of YYYY/MM/DD.	YYYY specifies a year that ranges from 2000 to 2099; MM specifies a month that ranges from 1 to 12; DD specifies a day that ranges from 1 to 31.
end-time	Specifies the end time, in the format of HH:MM:SS.	HH specifies an hour that ranges from 0 to 23; MM specifies a minute that ranges from 0 to 59; SS specifies a second that ranges from 0 to 59.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

NQA provides NQA test instances to test network operation conditions, to export statistics, and to effectively cut costs. NQA measures the performance of different protocols running on the network.

The **display nqa history** command helps you understand the network status by displaying the operation statistics about each test packet, including the status and round-trip delay.

NOTE

No history record about the failed jitter test instances exist.

To filter out information about failed tests in a historical table related to ICMP test instances, run the **records history-filter failures** command before viewing historical statistics.

Precautions

If no optional parameter is specified, all history records of an NQA test instance are displayed.

When NQA test result table and historical table are displayed in a split screen, latest results are displayed to improve user experience.

Example

Display the history records about an NQA test.

```
<Huawei> display nqa history
 NQA entry(admin, ftp) history:
 Index  T/H/P     Response Status       Address       Time
 1      1/1/1     1157ms   success      10.2.1.2      2012-07-15 10:16:38.188
 2      2/1/1     3000ms   timeout      UnKnow        2012-07-15 10:18:2.922
 NQA entry(admin, http) history:
 Index  T/H/P     Response Status       Address       Time
 1      1/1/1     0ms      busy         UnKnow        2012-07-15 11:16:39.915
 2      1/1/2     0ms      busy         UnKnow        2012-07-15 11:16:39.978
 3      1/1/3     0ms      busy         UnKnow        2012-07-15 11:16:39.40
```

Table 21-47 Description of the display nqa history command output

Item	Description
NQA entry(admin, ftp)	NQA test items: • admin: indicates the name of the administrator for an NQA test instance. • ftp: indicates the name of the NQA test instance.
Index	Index of a test record.
T/H/P	• T: Times, which indicates the sequence of the test for a test instance. • H: Hop, which indicates the sequence of the hop. • P: Probe, which indicates the sequence of the probe.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Response	Period from the time when a probe packet is sent to the time when a response packet is received.
Status	Probe status: • success: indicates that the probe succeeds. • timeout: indicates that the probe times out and no response packet is received. • busy: indicates that the resources are insufficient and the probe packet fails to be sent. When Status is busy, the value of the Response field is 0 ms. • drop: indicates that the probe packet is discarded because of no link is available. When Status is busy, the value of the Response field is 0 ms.
Address	Destination IP address of an NQA test instance.
Time	Time when the response packet is received.

Related Topics

21.7.4 clear-records

21.7.79 records

21.7.19 display nqa-parameter

Function

The **display nqa-parameter** command displays parameters for the current NQA test instance.

Format

display nqa-parameter

Parameters

None

Views

NQA view

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **display nqa-parameter** command to view parameters available for the current NQA test instance.

Differences between the **display nqa-parameter** and **display this** commands are as follows:

- The **display this** command is used to display commands that have been configured for the test instance. It shows the configuration records.
- The **display nqa-parameter** command is used to display parameters available for the current NQA test instance and prompt which parameter is mandatory for the start of the test instance. Before running the **display nqa-parameter** command, ensure that the type of the test instance is configured.

Example

Display parameters available for the NQA test instance in the NQA view.

```
<Huawei> system-view
[Huawei] nqa test-instance admin icmp
[Huawei-nqa-admin-icmp] test-type icmp
[Huawei-nqa-admin-icmp] description huawei nqa
[Huawei-nqa-admin-icmp] destination-address ipv4 10.1.1.1
[Huawei-nqa-admin-icmp] timeout 5
[Huawei-nqa-admin-icmp] display nqa-parameter
 *: the parameter must be configured before starting the test-instance.
 #: the parameter is undecided.
 <blank>: the parameter is optional.
*test-type                      :icmp
 description                     :huawei nqa
 frequency                       :
 timeout                         :5(default:3)
 threshold rtd                   :
*destination-address type        :ipv4
*destination-address             :10.1.1.1
 source-address type             :
 source-address                  :
 ttl                             :---(default:30)
 datasize                        :
 datafill                        :
 source-interface                :
 sendpacket passroute            :---(default:no)
 probe-count                     :---(default:3)
 send-trap                       :---(default:none)
  test-failtimes                 :---(default:1)
 tos                             :---(default:0)
 fail-percent                    :---(default:100)
 interval                        :---(default:4000)
 vpn-instance                    :
 records history                 :---(default:50)
 records result                  :---(default:5)
 records history-filter          :---(default:all)
 agetime                         :---(default:0:0:0)
 ip-forwarding                   :---(default:no)
 nexthop-address type            :
 nexthop-address                 :
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-48 Description of the display nqa-parameter command output

Item	Description
test-type	Type of the NQA test instance, which is set using the **test-type** command.
description	Description of the NQA test instance, which is configured using the **description** command.
frequency	Interval at which the NQA test instance is automatically performed, which is set using the **frequency** command.
timeout	timeout period for a probe of an NQA test instance, which is set using the **timeout** command.
threshold rtd	RTD of the NQA test instance, which is set using the **threshold** command.
destination-address type	Destination IP address type of the NQA test instance, which is set using the **destination-address** command.
destination-address	Destination IP address of the NQA test instance, which is set using the **destination-address** command.
source-address type	Source IP address type of the NQA test instance, which is set using the **source-address** command.
source-address	Source IP address of the NQA test instance, which is set using the **source-address** command.
ttl	TTL of the NQA test packet, which is set using the **ttl** command.
datasize	Size of the NQA test packet, which is set using the **datasize** command.
datafill	Pad characters in the NQA test packet, which is set using the **datafill** command.
source-interface	Source interface of the NQA test instance, which is set using the **source-interface** command.
sendpacket passroute	Whether the test instance is configured to send packets without searching the routing table, which is set using the **sendpacket passroute** command.
probe-count	Number of probes for the NQA test instance, which is set using the **probe-count** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
send-trap	Conditions for sending traps for the NQA test instance, which are configured using the **send-trap** command.
test-failtimes	Number of continuous test failures in the NQA test instance, which is set using the **test-failtimes** command.
tos	Type of service (TOS) of the test package in the NQA test instance, which is set using the **tos** command.
fail-percent	Percentage of failed NQA test instances, which is set using the **fail-percent** command.
interval	Interval for sending NQA test packets, which is set using the **interval** command.
vpn-instance	VPN instance name of the NQA test instance, which is set using the **vpn-instance** command.
records history	Maximum number of history records allowed for the NQA test instance, which is set using the **records** command.
records result	Maximum number of test result records allowed for the NQA test instance, which is set using the **records** command.
records history-filter	Filtering records from a historical table for an NQA test instance, referring to the **records history-filter** command.
agetime	Aging time of the NQA test instance, which is set using the **agetime** command.
ip-forwarding	Forwarding IP packets forcibly, which is set using the **ip-forwarding** command.
nexthop-address type	The type of the next hop address, which is set using the **nexthop** command.
nexthop-address	The next hop address, which is set using the **nexthop** command.

Related Topics

21.7.56 nqa
21.7.95 test-type

 Copyright © Huawei Technologies Co., Ltd.

21.7.20 display nqa results

Function

The **display nqa results** command displays NQA test results.

Format

display nqa results [**collection** | **success** | **failed**] [**test-instance** *admin-name test-name*] [**verbose**]

Parameters

Parameter	Description	Value
collection	Indicates the total NQA test results.	-
success	Indicates the results of successful tests.	-
failed	Indicates the results of failed tests.	-
test-instance	Indicates an NQA test instance.	-
admin-name	Specifies the name of the administrator for an NQA test instance.	The value must be the name of an existing NQA test instance administrator.
test-name	Specifies the name of an NQA test instance.	The value must be the name of an existing NQA test instance.
verbose	Displays detailed information.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

NQA test results cannot be displayed automatically on the terminal. To view NQA test results, run the **display nqa results** command.

If no test instance is specified, the test result of the test instance is displayed in the corresponding test instance view, and the test result of all test instances is displayed in the system view or other views irrelevant to test instances. If a test instance is specified, the test result of only this test instance is displayed.

The **display nqa results** command displays the results of a test instance that has been complete.

 Copyright © Huawei Technologies Co., Ltd.

The output of the **display nqa results** command contains the following two parts:

- Universal test results: This part does not vary according to the test instance type.
- Detailed statistics of each test: Statistics items in this part vary according to the test instance type.

The **display nqa results collection** command is used to display the statistics on accumulative results. At present, only the jitter test supports the query of accumulated results.

Precautions

If no optional parameter is specified, all NQA test results are displayed.

When you run the **display nqa results** command to check the results of a single jitter or ICMP jitter test instance:

- If the value of **SendProbe** is 0, no test packet has been sent, and **Packet Loss Ratio** is displayed as 100% (default value).
- If the value of **SendProbe** is not 0 and the value of **Packet Loss Ratio** is 100%, all test packets have been lost.

When you run the **display nqa results collection** command to check the accumulative results of multiple jitter or ICMP jitter test instances:

- If the value of **SendProbe** is 0, no test packet has been sent in these tests, and **Packet Loss Ratio** is displayed as 0% (default value).
- If the value of **SendProbe** is not 0 but the value of **Packet Loss Ratio** is 0%, no test packet has been lost.

Formula used to calculate the accumulative packet loss ratio: Accumulative packet loss ratio = (Accumulative number of sent packets – Accumulative number of received packets)/Accumulative number of sent packets x 100%. If the value of **SendProbe** in the results of a single test is 0, it is not considered during the calculation of the accumulative packet loss ratio.

Example

Display the results of an NQA ICMP test.

```
<Huawei> display nqa results test-instance admin icmp
  NQA entry(admin, icmp) :testflag is inactive ,testtype is icmp
  1 . Test 1 result   The test is finished
   Send operation times: 3              Receive response times: 3
   Completion:success                   RTD OverThresholds number: 0
   Attempts number:1                    Drop operation number:0
   Disconnect operation number:0        Operation timeout number:0
   System busy operation number:0       Connection fail number:0
   Operation sequence errors number:0   RTT Status errors number:0
   Destination ip address:10.138.77.21
   Min/Max/Average Completion Time: 2/2/2
   Sum/Square-Sum  Completion Time: 6/12
   Last Good Probe Time: 2012-07-02 17:09:18.1
   Lost packet ratio: 0 %
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-49 Description of the display nqa results test-instance admin icmp command output

Item	Description
NQA entry(admin, icmp)	NQA test items: ● admin: indicates the administrator or creator of the NQA test instance. ● icmp: indicates the name of the NQA test instance.
testflag	Test flag. ● active: indicates that the test is running. Checking the result of a running test is invalid. ● inactive: indicates that the test is complete. At this time, the actual test result is displayed.
testtype	Test type.
1 . Test 1 result	Sequence number of test results. Test results are numbered based on the time when the tests are complete.
The test is finished	Test status: ● finished: indicates that the test is complete. ● running: indicates that the test is running.
Send operation times	Number of sent packets.
Receive response times	Number of received response packets.
Completion	Completing status of the test: ● success: indicates that the test is complete successfully. ● no result: indicates that the test is running, and no test result is obtained or no test result is obtained after the test. ● failed: indicates that the test fails. ● negotiate failed: indicates that the negotiation fails.
RTD OverThresholds number	Number of times that the round-trip delay (RTD) threshold is exceeded.
Attempts number	Test times.
Drop operation number	Number of system resource allocation failures.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Disconnect operation number	Number of forcible disconnections.
Operation timeout number	Number of timeout operations during the test.
System busy operation number	Number of conflict operations.
Connection fail number	Number of times that the local end fails to establish connections with the peer.
Operation sequence errors number	Number of received disordered packets.
RTT Status errors number	Number of RTT status errors.
Destination ip address	Destination IP address of the test.
Min/Max/Average Completion Time	Minimum/Maximum/Average time taken to complete the test.
Sum/Square-Sum Completion Time	Sum and square sum of the time taken to complete the test.
Last Good Probe Time	Time at which the last probe is complete.
Lost packet ratio	Packet loss ratio.

Display the result of an NQA jitter test.

```
<Huawei> display nqa results test-instance admin jitter
 NQA entry(admin, jitter) :testflag is inactive ,testtype is jitter
  1 . Test 1 result   The test is finished
   SendProbe:60                          ResponseProbe:0
   Completion:failed                     RTD OverThresholds number:0
   OWD OverThresholds SD number:0        OWD OverThresholds DS number:0
   Min/Max/Avg/Sum RTT:0/0/0/0           RTT Square Sum:0
   NumOfRTT:0                            Drop operation number:0
   Operation sequence errors number:0    RTT Stats errors number:0
   System busy operation number:0        Operation timeout number:60
   Min Positive SD:0                     Min Positive DS:0
   Max Positive SD:0                     Max Positive DS:0
   Positive SD Number:0                  Positive DS Number:0
   Positive SD Sum:0                     Positive DS Sum:0
   Positive SD Square Sum:0              Positive DS Square Sum:0
   Min Negative SD:0                     Min Negative DS:0
   Max Negative SD:0                     Max Negative DS:0
   Negative SD Number:0                  Negative DS Number:0
   Negative SD Sum:0                     Negative DS Sum:0
   Negative SD Square Sum:0              Negative DS Square Sum:0
   Min Delay SD:0                        Min Delay DS:0
   Avg Delay SD:0                        Avg Delay DS:0
   Max Delay SD:0                        Max Delay DS:0
   Delay SD Square Sum:0                 Delay DS Square Sum:0
   Packet Loss SD:0                      Packet Loss DS:0
   Packet Loss Unknown:0                 Average of Jitter:0
   Average of Jitter SD:0                Average of Jitter DS:0
   Jitter out value:0.0000000            Jitter in value:0.0000000
   NumberOfOWD:0                         Packet Loss Ratio: 100%
   OWD SD Sum:0                          OWD DS Sum:0
   ICPIF value: 0                        MOS-CQ value: 0
   TimeStamp unit: ms                    Packet Rewrite Number: 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
  Packet Rewrite Ratio: 0%            Packet Disorder Number: 0
  Packet Disorder Ratio: 0%           Fragment-disorder Number: 0
  Fragment-disorder Ratio: 0%          Jitter OverThresholds SD number:0
  Jitter OverThresholds DS number:0    OverallOverThresholds number:0
Start time: 2014-06-25 18:47:05+08:00
End time: 2014-06-25 18:47:05+08:00
```

Table 21-50 Description of the display nqa results test-instance admin jitter command output

Item	Description
NQA entry(admin, jitter)	NQA test items: ● admin: indicates the name of the administrator for an NQA test instance. ● jitter: indicates the name of the NQA test instance.
testflag	Test flag: ● active: indicates that the test is running. Checking the test result during the operation is invalid. ● inactive: indicates that the test is complete. At this time, the actual test result is displayed.
testtype	Test type.
SendProbe	Number of sent probes.
ResponseProbe	Number of received response probes.
Completion	Completing status of the test: ● success: indicates that the test is complete successfully. ● no result: indicates that the test is running, so no result is obtained. ● failed: indicates that the test fails. ● negotiate failed: indicates that negotiation fails. This parameter is displayed only for hardware-based UDP Jitter test instances.
RTD OverThresholds number	Number of times that the RTD threshold is exceeded.
OWD OverThresholds SD number	Number of times that the one-way delay (OWD) threshold (from the source to the destination) is exceeded.
OWD OverThresholds DS number	Number of times that the OWD threshold (from the destination to the source) is exceeded.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Min/Max/Avg/Sum RTT	Minimum/Maximum/Average/Sum of the RTT.
RTT Square Sum	RTT square sum of the probes.
NumOfRTT	Number of RTTs.
Drop operation number	Number of system resource allocation failures.
Operation sequence errors number	Serial number of the error packets received by the client.
RTT Stats errors number	Number of RTT status errors.
System busy operation number	Number of conflict operations.
Operation timeout number	Number of timeout operations during the test.
Min Positive SD	Minimum positive jitter from the source to the destination.
Min Positive DS	Minimum positive jitter from the destination to the source.
Max Positive SD	Maximum positive jitter from the source to the destination.
Max Positive DS	Maximum positive jitter from the destination to the source.
Positive SD Number	Number of the positive jitter from the source to the destination.
Positive DS Number	Number of the positive jitter from the destination to the source.
Positive SD Sum	Sum of the positive jitter from the source to the destination.
Positive DS Sum	Sum of the positive jitter from the destination to the source.
Positive SD Square Sum	Square sum of the positive jitter from the source to the destination.
Positive DS Square Sum	Square sum of the positive jitter from the destination to the source.
Min Negative SD	Minimum negative jitter from the source to the destination.
Min Negative DS	Minimum negative jitter from the destination to the source.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Max Negative SD	Maximum negative jitter from the source to the destination.
Max Negative DS	Maximum negative jitter from the destination to the source.
Negative SD Number	Number of the negative jitter from the source to the destination.
Negative DS Number	Number of the negative jitter from the destination to the source.
Negative SD Sum	Sum of the negative jitter from the source to the destination.
Negative DS Sum	Sum of the negative jitter from the destination to the source.
Negative SD Square Sum	Square sum of the negative jitter from the source to the destination.
Negative DS Square Sum	Square sum of the negative jitter from the destination to the source.
Min Delay SD	Minimum delay from the source to the destination.
Min Delay DS	Minimum delay from the destination to the source.
Avg Delay SD	Average delay from the source to the destination.
Avg Delay DS	Average delay from the destination to the source.
Max Delay SD	Maximum delay from the source to the destination.
Max Delay DS	Maximum delay from the destination to the source.
Delay SD Square Sum	Square sum of the delay jitter from the source to the destination.
Delay DS Square Sum	Square sum of the delay jitter from the destination to the source.
Packet Loss SD	Maximum number of lost packets from the source to the destination.
Packet Loss DS	Maximum number of lost packets from the destination to the source.
Packet Loss Unknown	Number of packets lost at an unknown direction.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Average of Jitter	Average jitter.
Average of Jitter SD	Average jitter from the source to the destination.
Average of Jitter DS	Average jitter from the destination to the source.
Jitter out value	Jitter in sending packets.
Jitter in value	Jitter in receiving packets.
NumberOfOWD	Number of OWD packets.
Packet Loss Ratio	Packet loss ratio.
OWD SD Sum	Sum of OWD from the source to the destination.
OWD DS Sum	Sum of OWD from the destination to the source.
MOS-CQ value	Average estimate of VoIP performance.
ICPIF value	Advantage factor.
TimeStamp unit	Unit of the timestamp.
Packet Rewrite Number	Number of rewritten packets.
Packet Rewrite Ratio	Percentage of rewritten packets to total packets.
Packet Disorder Number	Number of out-of-order packets.
Packet Disorder Ratio	Percentage of out-of-order packets to total packets.
Fragment-disorder Ratio	Percentage of out-of-order fragmented packets to total packets.
Jitter OverThresholds SD number	Number of times that a test instance is successfully performed with the jitter exceeding the specified threshold from the source to the destination.
Jitter OverThresholds DS number	Number of times that a test instance is successfully performed with the jitter exceeding the specified threshold from the destination to the source.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
OverallOverThresholds number	Number of times that a test instance is successfully performed with any of the delays from the source to the destination or from the destination to the source, the bi-directional delay, the jitters from the source to the destination or from the destination to the source exceeding the set threshold.

Display the statistics on the total NQA test results after the packet rewrite check function is configured.

```
<Huawei> display nqa results collection
NQA entry(admin, jitter) :testtype is jitter
  1 . Test 1 collect result
    SendProbe:60                        ResponseProbe:47
    Completion:1                        RTD OverThresholds number:0
    OWD OverThresholds SD number:0      OWD OverThresholds DS number:0
    Min/Max/Avg/Sum RTT:30/1130/296/13910 RTT Square Sum:10840100
    NumOfRTT:47                         Drop operation number:0
    Operation sequence errors number:0  RTT Stats errors number:0
    System busy operation number:0      Operation timeout number:13
    Min Positive SD:10                  Min Positive DS:10
    Max Positive SD:260                 Max Positive DS:160
    Positive SD Number:9                Positive DS Number:4
    Positive SD Sum:690                 Positive DS Sum:230
    Positive SD Square Sum:122900       Positive DS Square Sum:27700
    Min Negative SD:20                  Min Negative DS:30
    Max Negative SD:60                  Max Negative DS:290
    Negative SD Number:31               Negative DS Number:5
    Negative SD Sum:1010                Negative DS Sum:530
    Negative SD Square Sum:34300        Negative DS Square Sum:105100
    Min Delay SD:15                     Min Delay DS:14
    Avg Delay SD:147                    Avg Delay DS:146
    Max Delay SD:565                    Max Delay DS:564
    Delay SD Square Sum:2710025         Delay DS Square Sum:2696162
    Packet Loss SD:0                    Packet Loss DS:0
    Packet Loss Unknown:0               Average of Jitter:50
    Average of Jitter SD:42             Average of Jitter DS:84
    Jitter out value:0.0000000          Jitter in value:0.0000000
    NumberOfOWD:47                      Packet Loss Ratio: 21%
    OWD SD Sum:6955                     OWD DS Sum:6908
    ICPIF value: 0                      MOS-CQ value: 0
    TimeStamp unit: ms                  Packet Rewrite Number: 0
    Packet Rewrite Ratio: 0%            Packet Disorder Number: 0
    Packet Disorder Ratio: 0%           Fragment-disorder Number: 0
    Fragment-disorder Ratio: 0%         Jitter OverThresholds SD number:0
    Jitter OverThresholds DS number:0   OverallOverThresholds number:0
```

Table 21-51 Description of the display nqa results collection command output

Item	Description
SendProbe	Number of sent probes.
ResponseProbe	Number of received response probes.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Completion	Number of times that the test is performed.
RTD OverThresholds number	Number of times that the RTD threshold is exceeded.
OWD OverThresholds SD number	Number of times that the OWD threshold (from the source to the destination) is exceeded.
OWD OverThresholds DS number	Number of times that the OWD threshold (from the destination to the source) is exceeded.
Min/Max/Avg/Sum RTT	Minimum/Maximum/Average/Sum of the RTT.
RTT Square Sum	RTT square sum of the probes.
NumOfRTT	Number of RTTs.
Drop operation number	Number of system resource allocation failures.
Operation sequence errors number	Serial number of the error packets received by the client.
RTT Stats errors number	Number of RTT status errors.
System busy operation number	Number of conflict operations.
Operation timeout number	Number of timeout operations during the test.
Min Positive SD	Minimum positive jitter from the source to the destination.
Min Positive DS	Minimum positive jitter from the destination to the source.
Max Positive SD	Maximum positive jitter from the source to the destination.
Max Positive DS	Maximum positive jitter from the destination to the source.
Positive SD Number	Number of the positive jitter from the source to the destination.
Positive DS Number	Number of the positive jitter from the destination to the source.
Positive SD Sum	Sum of the positive jitter from the source to the destination.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Positive DS Sum	Sum of the positive jitter from the destination to the source.
Positive SD Square Sum	Square sum of the positive jitter from the source to the destination.
Positive DS Square Sum	Square sum of the positive jitter from the destination to the source.
Min Negative SD	Minimum negative jitter from the source to the destination.
Min Negative DS	Minimum negative jitter from the destination to the source.
Max Negative SD	Maximum negative jitter from the source to the destination.
Max Negative DS	Maximum negative jitter from the destination to the source.
Negative SD Number	Number of the negative jitter from the source to the destination.
Negative DS Number	Number of the negative jitter from the destination to the source.
Negative SD Sum	Sum of the negative jitter from the source to the destination.
Negative DS Sum	Sum of the negative jitter from the destination to the source.
Negative SD Square Sum	Square sum of the negative jitter from the source to the destination.
Negative DS Square Sum	Square sum of the negative jitter from the destination to the source.
Min Delay SD	Minimum delay from the source to the destination.
Min Delay DS	Minimum delay from the destination to the source.
Avg Delay SD	Average delay from the source to the destination.
Avg Delay DS	Average delay from the destination to the source.
Max Delay SD	Maximum delay from the source to the destination.
Max Delay DS	Maximum delay from the destination to the source.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Delay SD Square Sum	Square sum of the delay jitter from the source to the destination.
Delay DS Square Sum	Square sum of the delay jitter from the destination to the source.
Packet Loss SD	Maximum number of lost packets from the source to the destination.
Packet Loss DS	Maximum number of lost packets from the destination to the source.
Packet Loss Unknown	Number of packets lost at an unknown direction.
Average of Jitter	Average jitter.
Average of Jitter SD	Average jitter from the source to the destination.
Average of Jitter DS	Average jitter from the destination to the source.
Jitter out value	Jitter in sending packets.
Jitter in value	Jitter in receiving packets.
NumberOfOWD	Number of OWD packets.
Packet Loss Ratio	Packet loss ratio.
OWD SD Sum	Sum of OWD from the source to the destination.
OWD DS Sum	Sum of OWD from the destination to the source.
MOS-CQ value	Average estimate of VoIP performance.
ICPIF value	Advantage factor.
TimeStamp unit	Unit of the timestamp.

Related Topics

21.7.4 clear-records

21.7.21 display nqa support-server-type

Function

The **display nqa support-server-type** command displays the server types supported by NQA.

 Copyright © Huawei Technologies Co., Ltd.

Format

display nqa support-server-type

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the server types supported by NQA.

```
<Huawei> display nqa support-server-type
NQA support server type information:

-----------------------------------------------------
  Type            Description
  tcp server       NQA TCP server
  udp server       NQA UDP server
  rtp server      NQA RTP server

-----------------------------------------------------
```

Table 21-52 Description of the display nqa support-server-type command output

Item	Description
Type	Server types supported by NQA.
Description	Description of the server types supported by NQA

Related Topics

21.7.73 nqa-server tcpconnect
21.7.74 nqa-server udpecho

21.7.22 display nqa support-test-type

Function

The **display nqa support-test-type** command displays the test instance types supported by NQA.

 Copyright © Huawei Technologies Co., Ltd.

Format

display nqa support-test-type

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can run the **display nqa support-test-type** command to view all test instances supported by the device.

NOTE

You can run this command to view all test instances supported on the device. However, the test instance that can be configured on the device uses the test instanced configured in the **test-type** command as an example.

- If the **display nqa support-test-type** command is run on the NQA server, the test instances supported by the server are displayed.
- If the **display nqa support-test-type** command is run on the NQA client, the test instances supported by the client are displayed.

Example

Display the test instance types supported by NQA.

```
<Huawei> display nqa support-test-type
NQA support test type information:

-------------------------------------------------
 Type          Description
 tcp          TCP type NQA test
 udp           UDP type NQA test
 http         HTTP type NQA test
 ftp         FTP type NQA test
 jitter      JITTER type NQA test
 icmp          ICMP type NQA test
 snmp           SNMP type NQA test
 trace        TRACE type NQA test
 lspping       LSPPING type NQA test
 lsptrace      LSPTRACE type NQA test
 dns         DNS type NQA test
 dhcp          DHCP type NQA test


-------------------------------------------------
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-53 Description of the display nqa support-test-type command output

Item	Description
Type	Test instance types supported by NQA.
Description	Description of the test instance types supported by NQA.

Related Topics

21.7.95 test-type

21.7.23 display nqa-agent

Function

The **display nqa-agent** command displays test status and configuration on an NQA client.

Format

display nqa-agent [*admin-name test-name*] [**verbose**]

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 characters.
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 characters.
verbose	Indicates detailed information about the client status of an NQA test.	-

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the client status of an NQA test.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display nqa-agent
  NQA Tests Max:256          NQA Tests  Number:   1
  NQA Flow  Max:256          NQA Flow Remained:256
nqa test-instance admin icmp
 test-type icmp
 destination-address ipv4 192.168.1.2
```

Table 21-54 Description of the display nqa-agent command output

Item	Description
NQA Tests Max	Maximum number of supported NQA test instances.
NQA Tests Number	Number of current NQA test instances.
NQA Flow Max	Maximum number of concurrent NQA test instances.
NQA Flow Remained	Maximum number of concurrent and performable NQA test instances.
test-type	Test type.
destination-address	destination address of a test.

Related Topics

21.7.56 nqa
21.7.95 test-type
21.7.92 start

21.7.24 display nqa-ftp-record configuration

Function

The **display nqa-ftp-record configuration** command displays the configuration of NQA test result sent to the FTP server using FTP.

Format

display nqa-ftp-record configuration

Parameters

None

Views

All views

Default Level

1: Monitoring level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To check the configuration of NQA test result upload to the FTP server through FTP, run the **display nqa-ftp-record configuration** command.

Example

Display the configuration of NQA test result sending to the FTP server using FTP.

```
<Huawei> display nqa-ftp-record configuration
---------------NQA FTP SAVE RECORD CONFIGURATION---------------
  FUNCTION: ENABLE    TRAP: ENABLE
  IP-ADDRESS:10.1.2.8
    SOURCE-ADDRESS:10.1.2.1
  VPN-INSTANCE:
  USERNAME:ftp
  PASSWORD:
  FILENAME:icmp
  ITEM-NUM:100000
  TIME:60
    DATETIMETYPE:UTC
  LAST FINISHED FILENAME:icmp20131214-163628.txt
```

Table 21-55 Description of the display nqa-ftp-record configuration command output

Item	Description
FUNCTION	Whether enable the NQA test results to be sent to the FTP server using FTP. ● ENABLE: enabled. ● DISABLE: disabled. To set this field, run the **nqa-ftp-record enable** command.
TRAP	Whether send a trap when the NQA test result is saved to the FTP server using FTP. ● ENABLE: enabled. ● DISABLE: disabled. To set this field, run the **nqa-ftp-record trap-enable** command.
IP-ADDRESS	FTP server address. To set this field, run the **nqa-ftp-record ip-address** command.
SOURCE-ADDRESS	FTP client address. To set this field, run the **nqa-ftp-record source-address** command.
VPN-INSTANCE	VPN instance name.
USERNAME	User name for logging in to the FTP server. To set this field, run the **nqa-ftp-record username** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
PASSWORD	Password for logging in to the FTP server. To set this field, run the **nqa-ftp-record password** command.
FILENAME	Name of a file created at the FTP server. To set this field, run the **nqa-ftp-record filename** command.
ITEM-NUM	Number of NQA test results that are saved to a file using FTP. To set this field, run the **nqa-ftp-record item-num** command.
TIME	Duration of saving NQA test results to a file using FTP. To set this field, run the **nqa-ftp-record time** command.
DATETIMETYPE	Type of time based on which test results are saved to a file on the FTP server: ● UTC: worldwide standard time type. ● LOCAL: local time type (recommended). To set this field, run the **nqa upload statistics datetime-type** command.
LAST FINISHED FILENAME	Name of a file created at the FTP server last time.

Related Topics

21.7.59 nqa-ftp-record enable
21.7.60 nqa-ftp-record filename
21.7.61 nqa-ftp-record ip-address
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.66 nqa-ftp-record source-address
21.7.64 nqa-ftp-record time
21.7.65 nqa-ftp-record trap-enable
21.7.67 nqa-ftp-record username
21.7.75 nqa upload statistics datetime-type

21.7.25 display nqa-server

Function

The **display nqa-server** command displays information about NQA servers.

 Copyright © Huawei Technologies Co., Ltd.

Format

display nqa-server

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Both the server and the client need to be configured before starting a TCP, jitter or UDP test instance. Otherwise, the test instances cannot be started.

- In the case of a TCP test instance, the **nqa-server tcpconnect** command needs to be run to enable a TCP server.
- In the case of a jitter or a UDP test instance, the **nqa-server udpecho** command needs to be run to enable a UDP server.

Example

Display the information about NQA servers.

```
<Huawei> display nqa-server

 NQA Server Max: 128              NQA Server Num: 1
 NQA Concurrent TCP Server: 0     NQA Concurrent UDP Server: 1
 NQA Concurrent RTP-UDP Server: 0
nqa-server udpecho 10.1.1.1 6000    ACTIVE    Hardware-based
```

Table 21-56 Description of the display nqa-server command output

Item	Description
NQA Server Max	Maximum number of NQA servers that can be configured.
NQA Server Num	Number of current NQA servers.
NQA Concurrent TCP Server	Number of the configured TCP servers.
NQA Concurrent UDP Server	Number of the configured UDP servers.
NQA Concurrent RTP-UDP Server	Number of the configured RTP-UDP servers.
nqa-server	Running servers.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
ACTIVE	Status of the NQA server.

Related Topics

21.7.73 nqa-server tcpconnect
21.7.74 nqa-server udpecho

21.7.26 display nqa-server session

Function

The **display nqa-server session** command displays the NQA client information on the NQA server.

Format

display nqa-server session

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

After the **nqa-server session-record enable** command is executed on the NQA server to enable NQA client information display, run the **display nqa-server session** command to view information about all NQA clients connected to the NQA server. The NQA client information includes the IP address of NQA server, IP address of NQA client, source port of NQA client, and VPN.

Precautions

This command is valid for only hardware-based UDP jitter test.

Example

Display NQA client information on the NQA server.

```
<Huawei> display nqa-server session
Total NQA Jitter items = 2
-----------------------------------------------------------
```

 Copyright © Huawei Technologies Co., Ltd.

```
Server-IP Client-IP Client-Port VPN-INSTANCE
------------------------------------------------------------
192.168.0.1 192.168.0.255 63081
192.168.0.1 192.168.0.255 53779
------------------------------------------------------------
```

Table 21-57 Description of the display nqa-server session command output

Item	Description
Total NQA Jitter items	Number of UDP jitter test instances.
Server-IP	IP address of the NQA server.
Client-IP	IP address of the NQA client.
Client-Port	Source port of the NQA client.
VPN-INSTANCE	VPN instance that the server belongs to.

Related Topics

21.7.72 nqa-server session-record enable

21.7.27 display snmp-agent trap feature-name nqa all

Function

The **display snmp-agent trap feature-name nqa all** command displays the status of all traps of the NQA module.

Format

display snmp-agent trap feature-name nqa all

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

None

Example

Display the status of all traps of the NQA module.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> display snmp-agent trap feature-name nqa all
-------------------------------------------------------------------------------
Feature name: NQA
Trap number : 29
-------------------------------------------------------------------------------
Trap name                      Default switch status   Current switch status
nqaResultsProbeFailed           on                      on
nqaHTTPStatsProbeFailed         on                      on
pingProbeFailed                 on                      on
nqaFTPStatsProbeFailed          on                      on
pingTestFailed                  on                      on
pingTestCompleted               on                      on
traceRouteTestFailed            on                      on
traceRouteTestCompleted         on                      on
nqaResultsTestFailed            on                      on
nqaResultsTestCompleted         on                      on
nqaResultsThresholdNotification
                                on                      on
nqaHTTPStatsTestFailed          on                      on
nqaHTTPStatsTestCompleted       on                      on
nqaHTTPStatsThresholdNotification
                                on                      on
nqaFTPStatsTestFailed           on                      on
nqaFTPStatsTestCompleted        on                      on
nqaFTPStatsThresholdNotification
                                on                      on
nqaJitterStatsTestFailed        on                      on
nqaJitterStatsTestCompleted     on                      on
nqaJitterStatsRTDThresholdNotification
                                on                      on
nqaJitterStatsOWDThresholdNotificationSD
                                on                      on
nqaJitterStatsOWDThresholdNotificationDS
                                on                      on
nqaRisingAlarmNotification      on                      on
nqaFaillingAlarmNotification    on                      on
nqaFtpSaveRecordNotification    on                      on
nqaJitterStatsJitterThresholdNotificationSD
                                on                      on
nqaJitterStatsJitterThresholdNotificationDS
                                on                      on
nqaReflectorStateChangeNotification
                                on                      on
nqaResultsTestResultChange      on                      on
```

Table 21-58 Description of the display snmp-agent trap feature-name nqa all command output

Item	Description
Feature name	Name of the module that a trap belongs to.
Trap number	Number of traps.
Trap name	Name of a trap.
Default switch status	Default status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.
Current switch status	Status of the trap function: ● on: indicates that the trap function is enabled. ● off: indicates that the trap function is disabled.

 Copyright © Huawei Technologies Co., Ltd.

21.7.28 dns-server

Function

The **dns-server** command configures the IP address of the domain name service (DNS) server in the NQA test.

The **undo dns-server** command deletes the configured IP address of the DNS server.

By default, the IP address of the DNS server is not configured.

Format

dns-server ipv4 *ip-address*

undo dns-server

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies an IPv4 address for the DNS server.	The value is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Before using a DNS test instance to detect the rate of resolving a given DNS name to an IP address, configure a DNS server first.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The test instance can only be a DNS or HTTP test instance.

Precautions

The DNS server configuration of a running test instance cannot be changed.

Example

Set the IP address of the DNS server to 10.1.1.1 in the test named **user test**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type dns
[Huawei-nqa-user-test] dns-server ipv4 10.1.1.1
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.9 destination-address

21.7.29 fail-percent

Function

The **fail-percent** command sets the failure percentage for the NQA test instance.

The **undo fail-percent** command deletes the configured failure percentage for the NQA test instance.

By default, the failure percentage is 100%. That is, the test is regarded as a failure only when all the probes fail.

Format

fail-percent *percent*

undo fail-percent

Parameters

Parameter	Description	Value
percent	Specifies the percentage of failed probes.	The value is an integer that ranges from 1 to 100.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, multiple probes are sent to test probe packets. Statistics obtained from multiple probe tests show the network quality.

In actual scenarios, however, a probe test may fail because of interference in the network. In addition, a failure in a probe test does not mean that the NQA test fails. The **fail-percent** command can be used to set failure percentage to check whether an NQA test fails or not. If the number of failure probe packets to the

 Copyright © Huawei Technologies Co., Ltd.

total number of probe packets reaches a specified percentage, the NQA test is considered as a failure.

For example, the number of sent packets set in the **probe-count** command is 10, but seven of them are lost during the probe test, the following situations occur:

- If the failure percentage is set to 80, the probe test is considered a success.
- If the failure percentage is set to 60, the probe test is considered a failure.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The failure percentage cannot be set for an FTP, a trace, a LSP Trace, and a DNS test instance.

Precautions

The failure percentage of a running test instance cannot be changed.

Example

Set the percentage of the failed probes to 10% in the test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] fail-percent 10
```

Related Topics

21.7.76 probe-count

21.7.30 forwarding-simulation inbound-interface

Function

The **forwarding-simulation inbound-interface** command configures a simulated inbound interface.

The **undo forwarding-simulation inbound-interface** command deletes a simulated inbound interface.

By default, no simulated inbound interfaces are configured.

Format

forwarding-simulation inbound-interface *interface-type interface-number*

undo forwarding-simulation inbound-interface

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of a simulated inbound interface.	–

 Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

By default, NQA test packets are regarded as host packets. The host packets are processed differently with the forwarded packets in that the former is preferably forwarded.

The **forwarding-simulation inbound-interface** command configures a simulated interface through which the NQA test packets, same as the forwarded packets, are forwarded to the product forwarding channel.

In a generalflow test instance, to allow the initiator and reflector to support the lossless mode, run the **forwarding-simulation inbound-interface** *interface-type interface-number* command. This allows the initiator and reflector interfaces to transmit both RFC 2544 and non-RFC 2544 traffic.

Prerequisites

Before configuring a DHCP test instance, configure a DHCP server or DHCP Relay, and ensure reachable routes between the DHCP client and the DHCP server or the DHCP Relay.

Precautions

The type of the test instance must be DHCP test instances.

In the DHCP test instance case, **source-interface** *interface-type interface-number* command and **forwarding-simulation inbound-interface** *interface-type interface-number* command are mutually exclusive. In addition, the DHCP client and NQA DHCP test instance cannot be configured on the same device. Otherwise, the NQA DHCP test instance may fail.

Example

Configure a simulated inbound interface in lossless mode for a DHCP test instance.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type dhcp
[Huawei-nqa-user-test] forwarding-simulation inbound-interface gigabitethernet 1/0/0
```

Related Topics

21.7.90 source-interface

 Copyright © Huawei Technologies Co., Ltd.

21.7.31 frequency

Function

The **frequency** command sets the interval at which an NQA test instance is automatically performed.

The **undo frequency** command deletes the configured interval at which an NQA test instance is automatically performed.

By default, the interval at which an NQA test instance is automatically performed is not configured. That is, the test is performed for one time.

Format

frequency *interval*

undo frequency

Parameters

Parameter	Description	Value
interval	Specifies the interval at which an NQA test instance is automatically performed.	The value is an integer that ranges from 1 to 604800, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **start** command to set the start time and end time of an NQA test. If you need to perform period test from the start time to the end time in a test instance, run the **frequency** command to set the interval at which an NQA test instance is automatically performed. After that, the NQA test is automatically performed one time at each configured interval.

Configuring the interval of periodic NQA test avoid time-consuming manual operations.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

The **frequency** value must comply with the following rules:

 Copyright © Huawei Technologies Co., Ltd.

- In the DHCP, DNS, FTP, HTTP, or Trace test instance, the **frequency** value must be larger than the product of **timeout** and **probe-count**.
- In the ICMP, SNMP, TCP, or UDP test instance, the **frequency** value must be larger than the product of **interval**and **probe-count**.
- In the Jitter test instance:

  frequency > **probe-count** × **jitter-packetnum** × **interval** + **timeout**
- In the hardware-based Jitter test instance:

  frequency > **probe-count** × **jitter-packetnum** × **interval** + 6200 + (5 × **timeout**/3)

  The unit of 6200 is ms.
- may be returned if the following condition is true: Interval at which the NQA test is automatically performed ≤ (Number of sent packets -1) x Interval + Timeout period + 1. For a test instance with jitter-packetnum configured, the number of sent packets is Probe-count x jitter-packetnum.

For trace and LSP trace test instances, the interval must be larger than or equal to 60 seconds.

If no end time is configured, the test cannot stop automatically. You need to stop it manually. The frequency of a running test instance cannot be changed.

Example

Set the interval at which test instance **user test** is automatically performed to 20 seconds.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] frequency 20
```

21.7.32 ftp-filename

Function

The **ftp-filename** command configures the file name and file path for an NQA FTP test instance.

The **undo ftp-filename** command deletes the file name and file path for an NQA FTP test instance.

By default, no file name and file path are configured.

Format

ftp-filename *file-name*

undo ftp-filename

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
file-name	Specifies the name and path of the operation file in an FTP test instance.	The value is a string of 1 to 230 characters.

Views

NQA view

Default Level

3: Management level

Usage Guidelines

The **ftp-filename** command is valid only for FTP test instances.

You cannot change the file path and file name of a running test instance.

If no file path is specified, the system searches for the file in the current path.

The file name cannot end with any forward slashes (/) or backward slashes (\).

The file name includes but is not limited to the extension name, such as .txt.

NOTE

Various FTP servers may support files with the file name in different length ranges. Before you configure this command, ensure that the target FTP server supports the length of the specified file name. Otherwise, NQA test results may fail to be transmitted using FTP.

Example

Set the FTP path and file name of test instance **user test** to **D:\abc** and **abc.txt** respectively.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-filename D:\abc\abc.txt
```

Related Topics

21.7.56 nqa

21.7.34 ftp-operation

21.7.95 test-type

21.7.33 ftp-filesize

Function

The **ftp-filesize** command sets the size of the file used in an NQA FTP test instance.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ftp-filesize** command restores the default size of the file used in an NQA FTP test instance.

By default, the size of the file used in the FTP test is 1000 Kbytes.

Format

ftp-filesize *size*

undo ftp-filesize

Parameters

Parameter	Description	Value
size	Specifies the size of the file used in the FTP test.	The value is an integer that ranges from 1 to 10000, in Kbytes.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You cannot change the configured size of the file when the test is running.

If specifying the size of the upload file is adopted, the FTP client automatically generates the file name **nqa-ftp-test.txt**. If the test is performed several times, the newly uploaded file replaces the previous one.

The type of the test instance has been set to **ftp** using the **test-type** command.

Example

Set the size of the file to 1024 bytes in the FTP upload test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-filesize 1024
```

Related Topics

21.7.34 ftp-operation

21.7.95 test-type

 Copyright © Huawei Technologies Co., Ltd.

21.7.34 ftp-operation

Function

The **ftp-operation** command sets the operation mode for an NQA FTP test instance.

The **undo ftp-operation** command restores the default operation mode of an NQA FTP test instance.

By default, the operation mode of an FTP test instance is **get**.

Format

ftp-operation { **get** | **put** }

undo ftp-operation put

Parameters

Parameter	Description	Value
get	Indicates that the client downloads a file from the server and the download speed is recorded.	-
put	Indicates that the client uploads a local file or a created file to the server and the upload speed is recorded.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP download test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

The **ftp-operation** command can be used to specify the FTP operation mode as **put** or **get**. A connection with the FTP server is set up using the IP address, the user name, and the password of the FTP server, and the time to set up FTP connection is recorded.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The operation mode of a running test instance cannot be changed.

Example

Perform a test named **user test** to obtain the FTP download speed.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-operation get
```

Related Topics

21.7.33 ftp-filesize

21.7.32 ftp-filename

21.7.95 test-type

21.7.35 ftp-password

Function

The **ftp-password** command sets a password for logging in to the FTP server in an NQA FTP test instance.

The **undo ftp-password** command deletes the configured password for logging in to the FTP server.

By default, no password is set for FTP test instances.

Format

ftp-password { *password* | **cipher** *cipher-password* }

undo ftp-password

Parameters

Parameter	Description	Value
password	Specifies the password for logging in to the FTP server in an FTP test instance.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. • The length of a plaintext password ranges from 1 to 32. • The length of a ciphertext password ranges from 32 to 68. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-password*	Specifies the password for logging in to the FTP server in an FTP test instance.	The value is a string of 1 to 32 or 32 to 68case-sensitive characters without spaces. ● The length of a plaintext password ranges from 1 to 32. ● The length of a ciphertext password ranges from 32 to 68. ● If the password length is 32 and the configured ciphertext password can be decrypted successfully, the configured ciphertext password takes effect. If the configured ciphertext password cannot be decrypted, the plaintext password is used after passing the validity check. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **ftp-password** command

 Copyright © Huawei Technologies Co., Ltd.

can be used to set the specified user and password. Only the user who enters the authorized user name and password is authorized to access the network.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

The password of a running test instance cannot be changed.

Example

Set the password for logging in to the FTP server to **Huawei-123**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-password Huawei-123
```

Related Topics

21.7.36 ftp-username

21.7.95 test-type

21.7.36 ftp-username

Function

The **ftp-username** command sets the user name for logging in to the FTP server in an FTP test instance.

The **undo ftp-username** command deletes the configured user name for logging in to the FTP server.

By default, no user name is set for FTP test instances.

Format

ftp-username *name*

undo ftp-username

Parameters

Parameter	Description	Value
name	Specifies the user name for logging in to the FTP server.	The value is a string of 1 to 255 case-sensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the FTP test, the local device functions as an FTP client to download/upload the specified file from/to the FTP server. Statistics about each FTP phase are displayed, including the time to set up an FTP control connection and the time to transmit data.

To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **ftp-username** command can be used to set the specified user in an FTP test. Only the user who enters the authorized user name and password is authorized to access the network.

Prerequisites

The type of the test instance has been set to **ftp** using the **test-type** command.

Precautions

The user name of a running test instance cannot be changed.

Example

Set the user name for logging in to the FTP server to **user1**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type ftp
[Huawei-nqa-user-test] ftp-username user1
```

Related Topics

21.7.35 ftp-password
21.7.95 test-type

21.7.37 hardware-based enable

Function

The **hardware-based enable** command enables the hardware forwarding engine on the LPU to send packets and add timestamps to the packets during the jitter test.

The **undo hardware-based** command disables the hardware forwarding engine on the LPU from sending packets and adding timestamps to the packets during the jitter test.

By default, the hardware forwarding engine on the LPU is not enabled to send packets and add timestamps to the packets.

Format

hardware-based enable

 Copyright © Huawei Technologies Co., Ltd.

undo hardware-based

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **hardware-based enable** command can only be used in the jitter test to enable the hardware forwarding engine on the LPU to send packets and add timestamps to the packets.

After the **hardware-based enable** command is configured, the **sendpacket passroute** can be configured, but does not take effect.

Example

Enable the hardware forwarding engine on the LPU to send packets and add timestamps to the packets.

```
<Huawei> system-view
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] hardware-based enable
```

Related Topics

21.7.95 test-type

21.7.38 http-operation

Function

The **http-operation** command sets the operation mode for an NQA HTTP test instance.

By default, the operation mode of the HTTP test instance is GET.

Format

http-operation get

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
get	Obtains data from the HTTP server.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

This command applies only to the HTTP test.

You cannot change the operation mode of a running HTTP test instance.

Example

Set the operation mode of HTTP test instance **user test** to **get**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type http
[Huawei-nqa-user-test] http-operation get
```

Related Topics

21.7.39 http-url

21.7.95 test-type

21.7.39 http-url

Function

The **http-url** command configures the uniform resource locator (URL) and version information for an HTTP test instance.

The **undo http-url** command deletes the configured URL and version information.

By default, no URL or version information is configured for an HTTP test instance.

Format

http-url *deststring* [*verstring*]

undo http-url

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
deststring	Specifies the name of the web page used for an HTTP test.	The value is a string of 1 to 230 case-insensitive characters without spaces. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.
verstring	Specifies the HTTP version.	It can be set to v1.0 or 1.1. The default HTTP version is v1.0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

HTTP1.0 and HTTP1.1 are supported in this test instance.

Precautions

The **http-url** command applies only to HTTP test instances. You cannot change the URL of a running HTTP test instance.

The URL of a HTTP test instance must be a URL that is displayed in a browser.

Example

Set the URL of HTTP test instance **user test** to **http://www.example.com**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type http
[Huawei-nqa-user-test] http-url http://www.example.com
```

Related Topics

21.7.38 http-operation

21.7.95 test-type

21.7.40 icmp-jitter-mode

Function

The **icmp-jitter-mode** command sets the type of ICMP jitter test instance.

The **undo icmp-jitter-mode** command restores the default type of ICMP jitter test instance.

 Copyright © Huawei Technologies Co., Ltd.

By default, the ICMP jitter test type is icmp-timestamp.

Format

icmp-jitter-mode { **icmp-echo** | **icmp-timestamp** }

undo icmp-jitter-mode

Parameters

Parameter	Description	Value
icmp-echo	Configures the ICMP jitter test instance to use ICMP echo packets.	-
icmp-timestamp	Configures the ICMP jitter test instance to use ICMP timestamp packets.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

In an ICMP jitter test, icmp-timestamp has a higher calculation precision of jitter parameters (such as delay and jitter) than icmp-echo. Therefore, icmp-timestamp is recommended.

NOTE

If the remote device does not support icmp-timestamp or requires ICMP echo packets, configure icmp-echo.

Example

Configure the ICMP jitter test instance to use ICMP echo packets.

```
<Huawei> system-view
[Huawei] nqa test-instance admin icmpjitter
[Huawei-nqa-admin-icmpjitter] test-type icmpjitter
[Huawei-nqa-admin-icmpjitter] icmp-jitter-mode icmp-echo
```

Related Topics

21.7.95 test-type

21.7.41 interval (NQA view)

Function

The **interval** command sets the interval at which NQA test packets are sent.

 Copyright © Huawei Technologies Co., Ltd.

The **undo interval** command restores the default setting.

- The interval is 20 milliseconds for a jitter test instance.
- The interval is 4 seconds for other test instances.

Format

interval { **milliseconds** *interval* | **seconds** *interval* }

undo interval

Parameters

Parameter	Description	Value
milliseconds *interval*	Sets the interval at which packets are sent, in milliseconds. **NOTE** If the configured interval is a multiple of 1000 milliseconds, the system will automatically convert milliseconds into seconds.	The value is an integer that ranges from 10 to 60000.
seconds *interval*	Sets the interval at which packets are sent, in seconds.	The value is an integer that ranges from 1 to 60, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, multiple probes are sent. Statistics obtained from multiple probe tests show the network quality. Probe packets (or probes) are sent at a specified interval.

- If the network quality is poor, the interval at which packets are sent must be increased. Otherwise, the network performance may deteriorate.
- If the network quality is good, the interval at which are sent can be decreased to shorten the waiting time.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The type of a test instance has been specified using the **test-type** command. The **interval** command is valid only for the jitter, ICMP, SNMP, LSP Ping, TCP, and UDP test instances.

Configuration Impact

- If the configured interval is a multiple of 1000 milliseconds, the system will automatically convert milliseconds into seconds.
- Packets can be sent at interval of milliseconds only in jitter test instances. The interval at which packets are sent must be greater than the timeout period set using the **timeout** command in all test instances except the jitter test instance.
- If the interval for sending packets has been configured, running the **interval** command will override the previous configuration.

Precautions

- The interval for sending packets of a running test instance cannot be changed.
- The interval for sending UDP jitter test packets must be less than 1 second.

Example

Set the interval for sending test packets to 1000 milliseconds.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] interval milliseconds 1000
```

21.7.42 ip nqa-compatible responder enable

Function

The **ip nqa-compatible responder enable** command enables the device to respond to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

The **undo ip nqa-compatible responder enable** command disables the device from responding to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

By default, the device is disabled from responding to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

Format

ip nqa-compatible responder [**vpn-instance** *vpn-instance-name*] **enable**

undo ip nqa-compatible responder [**vpn-instance** *vpn-instance-name*] **enable**

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the third-party device or NMS software.	The VPN instance has been created on the device.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

When the device connects a third-party device or NMS software, run the **ip nqa-compatible responder enable** command to enable the device to respond to UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software.

Example

Enable the device to respond to UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

```
<Huawei> system-view
[Huawei] ip nqa-compatible responder enable
```

Related Topics

21.7.44 ip nqa-compatible udp

21.7.43 ip nqa-compatible auto

21.7.43 ip nqa-compatible auto

Function

The **ip nqa-compatible auto** command configures the device to respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

The **undo ip nqa-compatible auto** command configures the device not to respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

By default, the device does not respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

Format

ip nqa-compatible auto

undo ip nqa-compatible auto

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device works with a third-party device or software to perform UDP-Echo or UDP-Jitter tests, this command allows the device to respond to UDP-Echo or UDP-Jitter packets sent from the third-party device or NMS software.

Prerequisites

The **ip nqa-compatible responder enable** command has been executed in the device view to enable the capability to respond to the UDP-Echo or UDP-Jitter packets sent from the a third-party device or NMS software.

Precautions

If the **ip nqa-compatible udp** command has been configured, the **ip nqa-compatible auto** command does not take effect. Run the **undo ip nqa-compatible udp** first.

Example

Configure the device to respond to UDP-Echo or UDP-Jitter packets sent from a third-party device or NMS software.

```
<Huawei> system-view
[Huawei] ip nqa-compatible auto
```

Related Topics

21.7.44 ip nqa-compatible udp

21.7.42 ip nqa-compatible responder enable

21.7.44 ip nqa-compatible udp

Function

The **ip nqa-compatible udp** command configures the IP address, port number, and service type of the response to the UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

The **undo ip nqa-compatible udp** command deletes the IP address, port number, and service type of the response to the UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software.

 Copyright © Huawei Technologies Co., Ltd.

By default, the IP address, port number, and service type of the response to the UDP-Echo or UDP-Jitter packets sent by a third-party device or NMS software are not configured.

Format

ip nqa-compatible { **device** | **network-management** } **udp** *ip-address* [**vpn-instance** *vpn-instance-name*] *port-number* [*tos-value*]

undo ip nqa-compatible { **device** | **network-management** } **udp** *ip-address* [**vpn-instance** *vpn-instance-name*] *port-number* [*tos-value*]

Parameters

Parameter	Description	Value
device	Specifies a third-party device.	-
network-management	Specifies a third-party NMS software.	-
ip-address	Specifies the IP address of the third-party device or NMS software.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the third-party device or NMS software.	The VPN instance has been created on the device.
port-number	Specifies the port number of the third-party device or NMS software.	The value is an integer that ranges from 0 to 65535.
tos-value	Specifies the service type of the third-party device or NMS software.	The value is an integer that ranges from 0 to 255.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device connects to the third-party device or NMS software and needs to respond to the UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software, run this command to specify the IP address, port number, and service type of the response. This command helps improving the accuracy and security of NQA tests.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **ip nqa-compatible responder** [**vpn-instance** *vpn-instance-name*] **enable** command has been executed in the system view to enable the device to respond to the UDP-Echo or UDP-Jitter packets sent by the third-party device or NMS software.

Precaution

If the configured port number is 7, 13, or 19, run the **undo anti-attack udp-flood enable** command to disable UDP Flood attack defense before running the **ip nqa-compatible udp** command. Otherwise, the device discards UDP-Echo or UDP-Jitter packets. If the configured port number is occupied by another process, the **ip nqa-compatible udp** command fails to take effect.

If the **ip nqa-compatible auto** command has been configured, the **ip nqa-compatible udp** command does not take effect. Run the **undo ip nqa-compatible auto** first.

Example

Set the IP address to 10.1.1.1, port number to 2000, and service type to 10 for the response to the UDP-Echo or UDP-Jitter packets sent by the third-party.

```
<Huawei> system-view
[Huawei] ip nqa-compatible device udp 10.1.1.1 2000 10
```

Related Topics

21.7.43 ip nqa-compatible auto

21.7.42 ip nqa-compatible responder enable

21.7.45 ip-forwarding

Function

The **ip-forwarding** command configures packets to be forcibly forwarded using IP on the first node.

The **undo ip-forwarding** command disables packets from being forcibly forwarded using IP on the first node.

Format

ip-forwarding

undo ip-forwarding

Parameters

None

Views

NQA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

When a fault occurs on the network, you can first run the **ping** command to check network connectivity. On an MPLS network, if a fault occurs but the control layer fails to detect the fault, the ping operation fails. To fast identify whether the fault occurs on the MPLS network or on the IP network, you can configure IP packets to be forcibly forwarded using IP on the first node. This can help you fast locate the fault.

NOTE

Currently, only NQA ICMP test instances support this configuration.

Example

Configure packets to be forwarded using IP.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] ip-forwarding
```

Related Topics

21.7.95 test-type

21.7.46 jitter-codec

Function

The **jitter-codec** command configures a code type for an NQA jitter simulated voice test.

The **undo jitter-codec** command deletes the configured code type of an NQA jitter simulated voice test.

By default, an NQA jitter test is not a simulated voice test.

Format

jitter-codec { **g711a** | **g711u** | **g729a** }

undo jitter-codec

Parameters

Parameter	Description	Value
g711a	Sets the code type of a simulated voice test to g711alaw. The transmission rate of g711alaw is 64 kbit/s.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
g711u	Sets the code type of a simulated voice test to g711ulaw. The transmission rate of g711ulaw is 64 kbit/s.	-
g729a	Sets the code type of a simulated voice test to g729a. The transmission rate of g729a is 8 kbit/s.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **jitter-codec** command can be used to configure the code types of conversion between simulated voice signals and digital signals to detect VoIP services in jitter test instances. You can specify different code types for VoIP services in actual situations.

The size of a jitter test packet varies with the code type.

- If the code type is **g711a**, the packet size configured using the **datasize** *size* command is 172 bytes.
- If the code type is **g711u**, the packet size configured using the **datasize** *size* command is 172 bytes.
- If the code type is **g729a**, the packet size configured using the **datasize** *size* command is 32 bytes.

The differences between g711a, g711u, and g729a of a jitter test instance are as follows:

Table 21-59 Differences between the code types

Code Type	Length of Data Area	Number of the Sent Packets	Interval at Which Packets Are Sent
g711a	172 bytes	1000	20 ms
g711u	172 bytes	1000	20 ms
g729a	32 bytes	1000	20 ms

After configuring the code type, run the **adv-factor** command to configure an advantage factor to simulate the jitter of actual voice packets.

After configuring the **jitter-codec** and **adv-factor** commands in a jitter test instance, you can adjust test packets to simulate the sending of VoIP traffic. This simulation helps to detect VoIP network and analyze service traffic.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

- The actual code types of the VoIP services to be tested have been set to the same.
- The test instance type has been set to jitter using the **test-type jitter** command.
- The remote device has been enabled to respond to the jitter test using the **nqa-server udpecho** command.

Configuration Impact

- If a code type has been configured, running the **jitter-codec** command will override the previous configuration.
- If a code type is changed, the configured advantage factor does not take effect and you need to configure a new advantage factor.

Precautions

The code type of a running test instance cannot be changed.

Example

Set the code type of a simulated voice test case to g711a.

```
<Huawei> system-view
[Huawei] nqa test-instance admin jitter
[Huawei-nqa-admin-jitter] test-type jitter
[Huawei-nqa-admin-jitter] jitter-codec g711a
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.7.1 adv-factor

21.7.47 jitter-packetnum

Function

The **jitter-packetnum** command sets the number of packets sent in each probe test instance.

The **undo jitter-packetnum** command restores the default number of packets sent in each probe test instance.

By default, 20 test packets are sent in each probe.

Format

jitter-packetnum *number*

undo jitter-packetnum

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
number	Specifies the number of test packets sent in each probe in the jitter test (**probe-count**).	The value is an integer that ranges from 1 to 3000. The default value is 20.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In an NQA test instance, the **jitter-packetnum** command can be used to set the number of consecutive packets to simulate the actual traffic of a data in a specified period of time. This helps simulate services more accurately.

For example, the **jitter-packetnum** command can be used to set the number of consecutive packets to 3000 and an interval of 20 ms to send packets. In this way, G.711 traffic can be simulated within one minute to detect VoIP services in UDP jitter test instances.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The number of sent packets can be configured only for jitter test instances.

Configuration Impact

- In jitter test instances, the number of sent packets = **jitter-packetnum** x **probe-count**, but the product cannot exceed 3000.
- If the number of probe packets has been set, running the **jitter-packetnum** command will override the previous configuration.

Precautions

The number of probe packets of a running test instance cannot be changed.

Example

Perform 3 probes in the test named **user test** and send 1000 packets in each probe.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] probe-count 3
[Huawei-nqa-user-test] jitter-packetnum 1000
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.41 interval (NQA view)
21.7.76 probe-count

21.7.48 lsp-exp

Function

The **lsp-exp** command configures the LSP EXP value of MPLS Echo Request packets in an NQA test instance.

Using the **undo lsp-exp** command, you can restore the default setting.

By default, LSP EXP is 0.

Format

lsp-exp *exp*

undo lsp-exp

Parameters

Parameter	Description	Value
exp	Specifies the LSP EXP value of an NQA test instance.	The value is an integer that ranges from 0 to 7. The default value is 0.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-exp** command.

The MPLS experimental bits (EXP) field is a 3-bit field in the MPLS header used to mark the precedence of MPLS packets.

Test packets are added to different queues according to their LSP EXP values, so that

- Congestion on the link can be avoided.
- Specified queue can be detected.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

This command applies to only the LSP test.

You cannot change the configured LSP EXP value when the test is performed.

Example

Set the LSP EXP value to 5.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-exp 5
```

Related Topics

21.7.95 test-type

21.7.49 lsp-path full-display

Function

Using the **lsp-path full-display** command, you can view all devices, including Ps, along an LSP in the NQA test result.

Using the **undo lsp-path full-display** command, you can view all devices, except for Ps, along an LSP in the NQA test result.

By default, you can view only PEs, not Ps, along an LSP in the NQA test result.

Format

lsp-path full-display

undo lsp-path full-display

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **lsp-path full-display** command can be used to display all devices, including Ps, along an LSP in the NQA test result. At present, this command is available only for VPLS PW trace test instances.

After the **lsp-path full-display** command is run, you can view all devices, including Ps, along an LSP in the result of a VPLS PW trace test instance. Otherwise, you can view only PEs along an LSP.

 Copyright © Huawei Technologies Co., Ltd.

Example

Display all devices, including Ps, along an LSP in the result of a VPLS PW trace test instance.

```
<Huawei> system-view
[Huawei] nqa test-instance vplspw trace
[Huawei-nqa-vplspw-trace] test-type vplspwtrace
[Huawei-nqa-vplspw-trace] lsp-path full-display
```

Related Topics

21.7.95 test-type

21.7.50 lsp-nexthop

Function

The **lsp-nexthop** command is used to configure the IP address of the next hop in the case that load balancing is enabled.

Using the **undo lsp-nexthop** command, you can cancel the current setting.

By default, the next-hop IP address of any link that participates in load balancing.

Format

lsp-nexthop *nexthop-ip-address*

undo lsp-nexthop

Parameters

Parameter	Description	Value
nexthop-ip-address	Specifies the next hop address.	It is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-nexthop** command.

Two conditions must be meet before you use the command:

 Copyright © Huawei Technologies Co., Ltd.

- **lsp-type** is IPv4
- **lsp-version** is RFC4379

You can use the **lsp-nexthop** command to configure the IP address of the next hop. Test instance type supported as following:

- LSP Ping
- LSP Trace

Precautions

A running test instance cannot be configured with the next hop address.

Example

Specify the next hop address for the LSP Ping test instance whose LSP type is IPv4 and lsp-version is rfc4379.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type ipv4
[Huawei-nqa-user-test] lsp-version rfc4379
[Huawei-nqa-user-test] lsp-nexthop 10.1.2.20
```

Related Topics

21.7.95 test-type

21.7.53 lsp-type

21.7.51 lsp-replymode

Function

Using the **lsp-replymode** command, you can set the reply mode for the LSP test.

Using the **undo lsp-replymode** command, you can restore the default setting.

By default, UDP packets are used.

Format

lsp-replymode { **no-reply** | **udp** | **udp-via-vpls** | **udp-router-alert** | **level-control-channel** }

undo lsp-replymode

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
no-reply	Indicates that the LSP test is not responded.	If the **no-reply** parameter is specified in the command, the destination does not respond to NQA probe packets. This configuration is used to collect the statistics on or process received probe packets on the destination host, and no response packets need to be sent. The NQA test instance fails because the client does not receive response packets.
udp	Indicates that IPv4 UDP packets are used to respond to the LSP test.	-
udp-via-vpls	Indicates that VPLS UDP packets are used to respond to the LSP test.	-
udp-router-alert	Indicates that VPLS UDP packets are used to respond to the LSP test.	-
level-control-channel	Indicates that the reply packets are sent through the application-level control channel.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-replymode** command.

Using the **lsp-replymode** command, you can set the reply mode for the LSP test. The following test instances are supported:

- LSP Ping
- LSP Trace

 Copyright © Huawei Technologies Co., Ltd.

Precautions

lsp-replymode no-reply indicates the unidirectional test. If the client displays timeout, it indicates that the test succeeds.

You cannot change the reply mode of the currently performed LSP test.

Example

Set the reply mode of the test named **user test** to sending UDP packets.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-replymode udp
```

Related Topics

21.7.95 test-type

21.7.52 lsp-tetunnel

Function

The **lsp-tetunnel** command configures the TE tunnel used in an NQA LSP test.

The **undo lsp-tetunnel** command deletes the configured TE tunnel.

By default, no TE tunnel is configured for an LSP test instance.

Format

lsp-tetunnel tunnel *interface-number* [**hot-standby** | **primary**]

undo lsp-tetunnel

Parameters

Parameter	Description	Value
tunnel *interface-number*	Specifies the tunnel interface number.	-
hot-standby	Indicates the hot-standby tunnel of the TE tunnel.	-
primary	Indicates the primary tunnel of the TE tunnel.	-

Views

NQA view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Prerequisites

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-tetunnel** command.

Before using the **lsp-tetunnel** command to configure the TE tunnel in an NQA LSP test instance, run the **lsp-type te** command to specify the NQA LSP test type to TE.

You cannot change the TE tunnel when the LSP test is performed.

Example

Configure the TE tunnel of the test named **user test**.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] quit
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type te
[Huawei-nqa-user-test] lsp-tetunnel tunnel 0/0/1
```

Configure the CR-LSP hot-standby tunnel of the test named **user test**.

```
<Huawei> system-view
[Huawei] interface tunnel 0/0/1
[Huawei-Tunnel0/0/1] quit
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type te
[Huawei-nqa-user-test] lsp-tetunnel tunnel 0/0/1 hot-standby
```

Related Topics

21.7.95 test-type
21.7.53 lsp-type

21.7.53 lsp-type

Function

Using the **lsp-type** command, you can configure the LSP test type.

Using the **undo lsp-type** command, you can cancel configuring the LSP test type.

By the default, the value of lsp-type is ipv4.

Format

lsp-type { **ipv4** | **te** | **ipv4-vpn** }

undo lsp-type

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4	Sets the test type to Ipv4 LSP ping/trace.	-
te	Sets the type to LSP ping/trace of the TE tunnel.	-
ipv4-vpn	Sets the LSP test type to IPv4 L3VPN.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

NOTE

The AR100&AR120&AR150&160&200 does not support the **lsp-type** command.

The **lsp-type** command can be used to configure the LSP test type of an NQA test instance to detect an LDP or a TE tunnel.

- If **ipv4** is configured, the NQA test instance is used to detect the connectivity of a specified LDP LSP. The destination address of the test instance is configured using the **destination-address** command.
- If **te** is configured, the NQA test instance is used to detect the connectivity of a specified TE tunnel. The destination address of the test instance is configured using the **lsp-tetunnel** command.
- If the **ipv4-vpn** parameter is set, the NQA test case is used to test LSPs on a BGP-based L3VPN network.
  - To test a primary LSP on a BGP-based L3VPN network, specify the destination address using the **destination-address lsp-masklen** *masklen* command.
  - To test a primary LSP on a BGP-based L3VPN network, specify the destination address using the **destination-address lsp-masklen** *masklen* **vpn-frr-path** command.

Prerequisites

- If the LSP test type is set to IPv4, the NQA test instance type must be set to LSP ping or LSP trace.
- If the LSP test type is set to TE, the NQA test instance type must be set to LSP ping or LSP trace.
- If the LSP test type is set to IPv4 L3VPN, the NQA test instance type must be set to LSP ping.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The type of an LSP test that is running cannot be changed.

Example

Set the type of the test named **user test** to Ipv4 LSP ping.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-type ipv4
```

Related Topics

21.7.95 test-type

21.7.54 lsp-version

Function

Using the **lsp-version** command, you can configure the protocol that is used by the LSP test instance.

Using the **undo lsp-version** command, you can restore the default setting.

By default, draft6 is adopted.

Format

lsp-version { **rfc4379** | **draft6** | **ptn-mode** }

undo lsp-version

Parameters

Parameter	Description	Value
rfc4379	Indicates that the protocol defined in RFC 4379 is adopted.	-
draft6	Indicates that Draft-ietf-mpls-lsp-ping-06 is adopted.	-
ptn-mode	Indicates that trace VC packets are replied in a multi-segment PW scenario.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

NOTE

The AR100&AR120&AR150&AR160&200 does not support the **lsp-version** command.

The **lsp-version** command can be used to specify the protocol that is used by the LSP test instance.

Prerequisites

If **draft6** or **rfc4379** is specified in the **lsp-version** command, specify **lspping** or **lsptrace** in the **test-type** command.

NOTE

The protocol adopted by a running LSP test instance cannot be changed.

Example

Configure the LSP test instance to use the protocol defined in RFC 4379.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type lspping
[Huawei-nqa-user-test] lsp-version rfc4379
```

Related Topics

21.7.95 test-type

21.7.55 nexthop

Function

The **nexthop** configures a next hop address for NQA test packets.

The **undo nexthop** deletes the configured next hop address for the NQA test packets.

By default, the next hop address for the NQA test packets is obtained by searching the routing table.

Format

nexthop { **ipv4** *ip-address* }

undo nexthop

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ipv4 *ip-address*	Specifies a next hop address for NQA test packets.	The value is in dotted decimal notation. **NOTE** The specified next hop must be the physical interface directly connected to the device that sends the NQA test packets.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the scenario that an NQA test instance is associated with static routes, if a link becomes faulty, the NQA test instance detects this fault and then the static routes associated with the NQA test instance become Down. After the link recovers, the NQA test instance attempts to send ICMP test packets over the static routes. Because these static routes are still Down, the NQA test instance still fails to detect link connectivity. Traffic fails to be forwarded.

The **nexthop** command configures a next hop address for the NQA test packets, which ensures that the packets are forwarded when the link recovers from the fault, and the static routes associated with the NQA test instance are Up.

Prerequisites

Only the NQA ICMP test instance allows you to specify a next hop address for NQA test packets.

Precautions

After you specify the next hop address, you can also run the **source-interface** command to specify an outbound interface.

NOTE

If the next hop address is allocated dynamically using DHCP, the **source-interface** command must be run to specify the outbound interface.

In this case, the test must meet the following conditions. Otherwise, the test fails.

- The specified next hop address matches the outbound interface.
- The specified outbound interface cannot be the member interface of a logical interface.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure a next hop address for NQA ICMP test packets.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test]  test-type icmp
[Huawei-nqa-user-test] nexthop ipv4 10.1.1.1
```

21.7.56 nqa

Function

The **nqa** command creates an NQA test instance and enters the NQA view.

The **undo nqa** command deletes an NQA test instance.

Format

nqa test-instance *admin-name test-name*

undo nqa { **test-instance** *admin-name test-name* | **all-test-instance** }

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks ('').
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks ('').
all-test-instance	Specifies all NQA test instances.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The NQA is an integrated network test function. NQA test instances can accurately detect network running status, collect test statistics, and reduce costs.

NQA measures the performance of different protocols running on the network. NQA allows enterprise users to collect network operation indexes in real time, such as total delay of the HTTP, TCP connection delay, DNS resolution delay, file transmission delay, FTP connection delay, and DNS resolution error ratio.

To check these performance indexes, you can create NQA test instances. The two ends of an NQA test are called the NQA client and NQA server. The NQA client is responsible for initiating an NQA test. After receiving packets, the NQA server sends response messages to the NQA client. You can learn about the running status of a corresponding network according to the returned packets.

Configuration Impact

After the **undo nqa all-test-instance** command is run, all NQA test instances including the running test instance will be deleted. In this scenario, you cannot perform any operation on each test instance.

Precautions

The **undo nqa test-instance** *admin-name test-name* command cannot delete a running NQA test instance.

The **undo nqa all-test-instance** command deletes all NQA test instances (including the running test instances).

Example

Create a test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test]
```

Related Topics

21.7.95 test-type

21.7.57 nqa (NQA group view)

Function

The **nqa** command adds the specified NQA test instance to an NQA group.

The **undo nqa** command deletes the specified NQA test instance from an NQA group.

Format

nqa *admin-name test-name*

undo nqa *admin-name test-name*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
admin-name	Specifies the administrator of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks ('').
test-name	Specifies the name of an NQA test instance.	The value is a string of 1 to 32 case-sensitive characters, excluding question marks (?), en dashes (-), a single or consecutive quotation marks ('').

Views

NQA group view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To add the specified NQA test instance to an NQA group, run the **nqa (NQA group view)** command. When an NQA group contains multiple NQA test instances, you can monitor multiple links at the same time by managing this NQA group.

The detection of an NQA group succeeds when at least one NQA test instance in the group succeeds. If no NQA test instance in an NQA group succeeds, the detection of this NQA group fails.

Precautions

If you delete an NQA test instance that belongs to an NQA group, this test instance is also deleted from this group.

Example

Add the NQA test instances **admin1 test1** and **admin2 test2** to the NQA group **group1**.

```
<Huawei> system-view
[Huawei] nqa-group group1
[Huawei-nqa-group-group1] nqa admin1 test1
[Huawei-nqa-group-group1] nqa admin2 test2
```


Copyright © Huawei Technologies Co., Ltd.

21.7.58 nqa event

Function

The **nqa event** command associates an event with the NQA alarm.

The **undo nqa event** command deletes the configured event.

By default, no event is associated with the NQA alarm.

Format

nqa event *event-entry* { **log** | **trap** | **log-trap** | **linkage** *admin-name test-name* | **none** } [*description*]

undo nqa event [*event-entry*]

Parameters

Parameter	Description	Value
event-entry	Specifies the index of the entry in the event table.	The value is an integer that ranges from 1 to 65535.
log	Records a log for the event.	-
trap	Sends a trap to the NMS.	-
log-trap	Records a log and sends a trap to the NMS for the event.	-
linkage	Triggers a linkage test instance for the event.	-
admin-name	Specifies the administrator of the linkage test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
test-name	Specifies the name of the linkage test instance.	It is a string of 1 to 32 characters, spaces not supported. When quotation marks are used around the string, spaces are allowed in the string.
none	Marks as no event for the event.	-
description	Indicates the description of the event.	The value is a string of 1 to 127 characters with spaces supported.

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If the monitored item of an NQA test result exceeds the threshold, the system sends an alarm. The **nqa event** command can be used to associate an event with the alarm.

When an event occurs, you can process the event associated with the NQA alarm in the following ways:

- Record a log.
- Send a trap to the NMS.
- Record a log and send a trap to the NMS.
- Trigger a linkage test instance.
- Mark as no event.

Prerequisites

A test instance has been configured before associating it with an event. Creating other types of events requires no prerequisites.

Configuration Impact

After the **undo nqa event** command is run, all alarm events will be deleted if no event entry number is specified. If an event entry number is specified, the corresponding alarm event will be deleted.

Precautions

After running the **nqa event** command, run the **alarm** command to configure the alarm threshold for the monitored item of an NQA test result. In this case, an alarm is generated when the system becomes abnormal.

During configuration, check whether the event entry exists. If an event entry number to be entered exists, and the original event is not associated with an alarm, the original event which the event entry number corresponds to is overwritten after the event number is entered.

The event being associated with an alarm cannot be deleted.

Example

Associate event table 1 with linkage test instance **icmp**.

```
<Huawei> system-view
[Huawei] nqa event 1 linkage admin icmp
```

Related Topics

21.7.3 alarm

Copyright © Huawei Technologies Co., Ltd.

21.7.15 display nqa event
21.7.16 display nqa-event

21.7.59 nqa-ftp-record enable

Function

The **nqa-ftp-record enable** command enables the device to send the NQA test result to the FTP server using FTP.

The **undo nqa-ftp-record enable** command disables the device from sending the NQA test result to the FTP server using FTP.

By default, the test result is not sent to the FTP server using FTP.

Format

nqa-ftp-record enable

undo nqa-ftp-record enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The latest test result overrides the previous ones, because only a few NQA test results can be saved on the device. By default, the system stores the latest five test results. If you do not query the test results in a timely manner, some of them will be lost.

To solve this problem, you can save NQA test results to the FTP server using FTP. The NQA client sends test results to the specified FTP server using FTP. The FTP server then saves the test results to a text file.

Prerequisites

Parameters for the FTP connection have been set using the **nqa-ftp-record ip-address**, **nqa-ftp-record username**, **nqa-ftp-record password**, and **nqa-ftp-record filename** commands.

Precautions

During the FTP transmission, ensure the connectivity of the FTP connection.

 Copyright © Huawei Technologies Co., Ltd.

It is recommended that you use the FTP protocol in the secure network environment.

Example

Enable the device to send test results to the FTP server using FTP.

```
<Huawei> system-view
[Huawei] nqa-ftp-record enable
```

Related Topics

21.7.60 nqa-ftp-record filename
21.7.61 nqa-ftp-record ip-address
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.65 nqa-ftp-record trap-enable
21.7.64 nqa-ftp-record time

21.7.60 nqa-ftp-record filename

Function

The **nqa-ftp-record filename** command configures a file name for NQA test results when the test results are saved to the FTP server.

The **undo nqa-ftp-record filename** command deletes the file name configured for NQA test results.

Format

nqa-ftp-record filename *filename*

undo nqa-ftp-record filename

Parameters

Parameter	Description	Value
filename	Specifies the file name.	The value is a string of 1 to 200 characters. The file name cannot end with any forward slashes (/) or backward slashes (\). **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

The file to be saved is named in the format of file name-year-month-day-hour-minute-second.txt. If the number of sent results reaches the configured maximum value or the storage time of results expires, the system creates a file to save these results.

NOTE

Various FTP servers may support files with the file name in different length ranges. Before you configure this command, ensure that the target FTP server supports the length of the specified file name. Otherwise, NQA test results may fail to be transmitted using FTP.

Example

Save test results to the file named **a**.

```
<Huawei> system-view
[Huawei] nqa-ftp-record filename a
```

Related Topics

21.7.59 nqa-ftp-record enable
21.7.61 nqa-ftp-record ip-address
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.64 nqa-ftp-record time

21.7.61 nqa-ftp-record ip-address

Function

The **nqa-ftp-record ip-address** command configures an IP address for the FTP server where NQA test results are saved.

The **undo nqa-ftp-record ip-address** command deletes the IP address of the FTP server where NQA test results are saved.

By default, no IP address is configured for the FTP server.

Format

nqa-ftp-record ip-address *ip-address*

undo nqa-ftp-record ip-address

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Specifies an IP address for the FTP server.	The IP address is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

During the FTP transmission, ensure the connectivity of the FTP connection. If the FTP connection fails and the buffer of the test result is full, the test result that is saved for the longest time in the buffer is deleted.

Example

Configure NQA test results to be sent to 10.1.1.8 using FTP.

```
<Huawei> system-view
[Huawei] nqa-ftp-record ip-address 10.1.1.8
```

Related Topics

21.7.59 nqa-ftp-record enable
21.7.60 nqa-ftp-record filename
21.7.62 nqa-ftp-record item-num
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.65 nqa-ftp-record trap-enable
21.7.64 nqa-ftp-record time

21.7.62 nqa-ftp-record item-num

Function

The **nqa-ftp-record item-num** command sets the number of test results that can be saved to a file on the FTP server.

The **undo nqa-ftp-record item-num** command restores the default number of test results that can be saved to a file on the FTP server.

By default, 100000 test results can be saved to a file on the FTP server.

Format

nqa-ftp-record item-num *item-number*

 Copyright © Huawei Technologies Co., Ltd.

undo nqa-ftp-record item-num

Parameters

Parameter	Description	Value
item-number	Specifies the number of test results that can be saved to a file on the FTP server.	The value is an integer that ranges from 10000 to 2147483647.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When NQA test results are sent to the specified FTP server using FTP and the FTP server stores NQA test results to a text file, you need to set the maximum number of NQA test results that can be saved in each text file. If the number of test results exceeds the configured number, a new text file is created on the FTP server by the sequence number to store the subsequent NQA test results.

In addition, if the interval at which a test result is saved expires, a new file is also created on the FTP server by the sequence number to store NQA test results. If both the **nqa-ftp-record time** and **nqa-ftp-record item-num** commands are executed, a new file is created and the subsequent test results are saved to the new file when either of the interval at which a test result is saved or the number of test results reaches the configured value.

Configuration Impact

The system can send two test results to the FTP server each time. If the FTP server cannot resume the process of file writing after the process is interrupted, a new file is created on the FTP server to store NQA test results.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Set the number of NQA test results that can be saved to a file on the FTP server to 10010.

```
<Huawei> system-view
[Huawei] nqa-ftp-record item-num 10010
```

Related Topics

21.7.59 nqa-ftp-record enable

 Copyright © Huawei Technologies Co., Ltd.

21.7.61 nqa-ftp-record ip-address
21.7.60 nqa-ftp-record filename
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username
21.7.64 nqa-ftp-record time

21.7.63 nqa-ftp-record password

Function

The **nqa-ftp-record password** command configures a password for logging in to the FTP server where NQA test results are saved.

The **undo nqa-ftp-record password** command deletes the password for logging in to the FTP server where NQA test results are saved.

Format

nqa-ftp-record password { *password* | **cipher** *cipher-password* }

undo nqa-ftp-record password

Parameters

Parameter	Description	Value
password	Specifies a password for logging in to the FTP server where NQA test results are saved.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. ● The length of a plaintext password ranges from 1 to 32. ● The length of a ciphertext password ranges from 32 to 68. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
cipher *cipher-password*	Specifies a password for logging in to the FTP server where NQA test results are saved.	The value is a string of 1 to 32 or 32 to 68 case-sensitive characters without spaces. ● The length of a plaintext password ranges from 1 to 32. ● The length of a ciphertext password ranges from 32 to 68. ● If the password length is 32 and the configured ciphertext password can be decrypted successfully, the configured ciphertext password takes effect. If the configured ciphertext password cannot be decrypted, the plaintext password is used after passing the validity check. **NOTE** When quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used when the system sends NQA test results to the specified FTP server using FTP. To ensure test security and prevent unauthorized users from accessing the network, you need to enable identity authentication. The **nqa-ftp-record password** command can be used to set the specified user and password. Only the user who enters the authorized user name and password is authorized to access the network.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

Ensure that the **nqa-ftp-record password** command has been run before running the **nqa-ftp-record enable** command. Otherwise, FTP record (FTPR) cannot be enabled.

Precautions

The configured password and the user name configured by the **nqa-ftp-record username** command must be consistent.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Set the password for logging in to the FTP server to **Huawei-123**.

```
<Huawei> system-view
[Huawei] nqa-ftp-record password Huawei-123
```

Related Topics

21.7.59 nqa-ftp-record enable

21.7.60 nqa-ftp-record filename

21.7.62 nqa-ftp-record item-num

21.7.61 nqa-ftp-record ip-address

21.7.67 nqa-ftp-record username

21.7.64 nqa-ftp-record time

21.7.64 nqa-ftp-record time

Function

The **nqa-ftp-record time** command sets the interval at which test results are saved to a file on the FTP server.

The **undo nqa-ftp-record time** command restores the default interval at which test results are saved to a file on the FTP server.

By default, the interval at which NQA test results are saved to a file on the FTP server is 60 minutes.

Format

nqa-ftp-record time *time*

undo nqa-ftp-record time

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
time	Specifies the interval at which test results are stored to a text file using FTP.	The value is an integer that ranges from 1 to 43200, in minutes. The default value is 60.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When NQA test results are sent to a specified FTP server using FTP and the FTP server stores NQA test results to a text file, you need to set the interval at which test results are stored to a text file. A text file can store the test results in a specified period of time. If the interval exceeds the configured time, a new text file is created on the FTP server by the sequence number to store the subsequent NQA test results.

In addition, if the number of test results stored in a file on the FTP server reaches the configured number, a new file is also created on the FTP server by the sequence number to store the NQA test results. If both the **nqa-ftp-record time** and **nqa-ftp-record item-num** commands are configured, the following situations occur:

- If the number of test results stored in a file on the FTP server reaches the configured number, a new file is created and the subsequent test results is stored to the new file.
- If the number of test results stored in a file on the FTP server does not reach the configured number, but the interval at which a test result is stored reaches the configured interval, a new file is created and the subsequent test results are stored to the new file.

Precautions

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Set the interval at which NQA test results are saved to 10 minutes.

```
<Huawei> system-view
[Huawei] nqa-ftp-record time 10
```

Related Topics

21.7.59 nqa-ftp-record enable

 Copyright © Huawei Technologies Co., Ltd.

21.7.60 nqa-ftp-record filename
21.7.62 nqa-ftp-record item-num
21.7.61 nqa-ftp-record ip-address
21.7.63 nqa-ftp-record password
21.7.67 nqa-ftp-record username

21.7.65 nqa-ftp-record trap-enable

Function

The **nqa-ftp-record trap-enable** command generates traps after NQA test results are saved using FTP.

The **undo nqa-ftp-record trap-enable** command disables the generation of traps after NQA test results are saved using FTP.

By default, no trap is generated when the NQA test result is saved using FTP.

Format

nqa-ftp-record trap-enable

undo nqa-ftp-record trap-enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used when the system sends NQA test results to the specified FTP server using FTP. After the NQA test results are saved using FTP, the system sends a trap to the NMS.

Configuration Impact

If the test result is saved successfully at the first time, no trap is generated. If the test result is saved successfully at the second time, a trap is generated.

A trap is generated only after each text file is saved successfully. That is, when the number of saved test results reaches the configured number, or the interval at which a test result is saved reaches the configured time, the current text file can be saved successfully and a trap is generated.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Configure traps to be sent to the NMS using FTP after the NQA test result is saved.

```
<Huawei> system-view
[Huawei] nqa-ftp-record trap-enable
```

Related Topics

21.7.59 nqa-ftp-record enable

21.7.66 nqa-ftp-record source-address

Function

The **nqa-ftp-record source-address** command configures the address of the FTP client from which NQA test results are uploaded to the FTP server.

The **nqa-ftp-record source-address** restores the default FTP client address from which NQA test results are uploaded to the FTP server.

By default, the address of the FTP client from which NQA test results are uploaded to the FTP server is not configured.

Format

nqa-ftp-record source-address *ip-address*

undo nqa-ftp-record source-address

Parameters

Parameter	Description	Value
ip-address	Specifies an FTP client address.	The value is in dotted decimal notation.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

To specify the address of the FTP client from which NQA test results are uploaded to the FTP server in a scenario that has client address restrictions, run the **nqa-ftp-record source-address** command.

 Copyright © Huawei Technologies Co., Ltd.

Example

Configure 10.2.2.8 as the address of the FTP client from which NQA test results are uploaded to the FTP server.

```
<Huawei> system-view
[Huawei] nqa-ftp-record source-address 10.2.2.8
```

21.7.67 nqa-ftp-record username

Function

The **nqa-ftp-record username** command configures a user name for logging in to the FTP server where NQA test results are saved.

The **undo nqa-ftp-record username** command deletes the user name for logging in to the FTP server where NQA test results are saved.

By default, no user name is configured.

Format

nqa-ftp-record username *username*

undo nqa-ftp-record username

Parameters

Parameter	Description	Value
username	Specifies a user name for logging in to the FTP server where NQA test results are saved.	The value is a string of 1 to 255 characters.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

The user name configured for logging in to the FTP server where NQA test results are saved must be an existing user name on the FTP server.

Example

Set the user name for logging in to the FTP server to **ftp**.

```
<Huawei> system-view
[Huawei] nqa-ftp-record username ftp
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.59 nqa-ftp-record enable
21.7.60 nqa-ftp-record filename
21.7.62 nqa-ftp-record item-num
21.7.61 nqa-ftp-record ip-address
21.7.63 nqa-ftp-record password

21.7.68 nqa-ftp-record vpn-instance

Function

The **nqa-ftp-record vpn-instance** command configures a VPN instance for the FTP server where NQA test results are saved.

The **undo nqa-ftp-record vpn-instance** command deletes the VPN instance configured for the FTP server where NQA test results are saved.

By default, the name of a VPN instance is not configured on the system.

Format

nqa-ftp-record vpn-instance *vpn-instance*

undo nqa-ftp-record vpn-instance

Parameters

Parameter	Description	Value
vpn-instance	Specifies the name of the VPN instance to which the FTP server belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The command can be used when the system sends NQA test results to the specified FTP server using FTP. When the NQA client is connected to the FTP server through a VPN, the **nqa-ftp-record vpn-instance** command can be used to specify the name of the VPN instance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

Before test results are sent to the FTP server using FTP, ensure that the FTP connection works properly.

Example

Configure VPN instance **v1** to send NQA test results.

```
<Huawei> system-view
[Huawei] nqa-ftp-record vpn-instance v1
```

Related Topics

21.7.59 nqa-ftp-record enable

21.7.60 nqa-ftp-record filename

21.7.62 nqa-ftp-record item-num

21.7.63 nqa-ftp-record password

21.7.67 nqa-ftp-record username

21.7.69 nqa-group

Function

The **nqa-group** command creates an NQA group and displays the NQA group view, or displays an existing NQA group view.

The **undo nqa-group** command deletes an NQA group.

Format

nqa-group *group-name*

undo nqa-group *group-name*

Parameters

Parameter	Description	Value
group-name	Specifies the name of an NQA group.	It is a string of 1 to 32 case-sensitive characters without any space.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

After an NQA group is created using the **nqa-group** command, you can add NQA test instances to the NQA group using the **nqa (NQA group view)** command, and then manage the NQA group to monitor multiple links at the same time.

Example

Create the NQA group **group1** and add the NQA test instances **admin1 test1** and **admin2 test2** to the NQA group.

```
<Huawei> system-view
[Huawei] nqa-group group1
[Huawei-nqa-group-group1] nqa admin1 test1
[Huawei-nqa-group-group1] nqa admin2 test2
```

21.7.70 nqa-jitter tag-version

Function

The **nqa-jitter tag-version** command sets the packet version for a jitter test instance.

The **undo nqa-jitter tag-version** command restores the default packet version for a jitter test instance.

By default, the packet version of a jitter test instance is 1.

Format

nqa-jitter tag-version *version-number*

undo nqa-jitter tag-version

Parameters

Parameter	Description	Value
version-number	Specifies the packet version for a jitter test instance.	The value can be 1 or 2.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Version 1 does not support unidirectional packet loss statistics.

Version 2 produces more accurate packet statistics, which helps network administrators to locate network faults and detect malicious attacks towards the

 Copyright © Huawei Technologies Co., Ltd.

network. After version 2 and collecting the packet loss across a unidirectional link are enabled, you can view the packet loss across the link from the source end to the destination end, from the destination end to the source end, or in an unknown direction in the test results.

Therefore, configuring version 2 is recommended.

Configuration Impact

If the packet version of a jitter test instance has been configured, running the **nqa-jitter tag-version** command will override the previous configuration.

Precautions

- If the packet version for the jitter test is 1, configuring the UDP server is optional.
- If the packet version of the jitter test is 2, configuring UDP server is mandatory. You need to run the **nqa-server udpecho** command to configure the UDP server. If the command is not configured, the UDP jitter test instance on the ingress will fail due to timeout.

Example

Set the packet version of a jitter test instance to 2.

```
<Huawei> system-view
[Huawei] nqa-jitter tag-version 2
```

21.7.71 nqa-server rtp-udp

Function

The **nqa-server rtp-udp** command configures an RTP server for an NQA test.

The **undo nqa-server rtp-udp** command deletes the RTP server for an NQA test.

By default, no RTP server is configured.

Format

nqa-server rtp-udp [**vpn-instance** *vpn-instance-name*] *ip-address port-number*

undo nqa-server rtp-udp { [**vpn-instance** *vpn-instance-name*] *ip-address port-number* | **all** }

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the RTP server belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
ip-address	Specifies the IP address of the RTP server for monitoring RTP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the RTP server for monitoring RTP services.	The value is an integer that can be any value in the range of 1025 to 65535.
all	Specifies RTP servers for all NQA tests.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Incomplete or unclear pictures may occur during a Telepresence conference because of the unstable network. You can deploy an RTP test instance at the source node, and run the **nqa-server rtp-udp** command at the transit mode and destination node to deploy RTP servers to perform a jitter test. This method helps you easily locate faults, facilitates network maintenance, and improves Telepresence conference experience.

Example

Configure an RTP UDP server for an NQA test instance.

```
<Huawei> system-view
[Huawei] nqa-server rtp-udp 10.10.10.2 2500
```

21.7.72 nqa-server session-record enable

Function

The **nqa-server session-record enable** command enables NQA client information display on the NQA server.

The **undo nqa-server session-record enable** command disables NQA client information display on the NQA server.

By default, NQA client information display is disabled on the NQA server.

Format

nqa-server session-record enable

undo nqa-server session-record enable

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **nqa-server session-record enable** command is executed on the NQA server to enable NQA client information display, run the **display nqa-server session** command to view information about all NQA clients connected to the NQA server. The NQA client information includes the IP address of NQA server, IP address of NQA client, source port of NQA client, and VPN.

Precautions

This command is valid for only hardware-based UDP jitter test.

Example

Enable NQA client information display on the NQA server.

```
<Huawei> system-view
[Huawei] nqa-server session-record enable
```

Related Topics

21.7.26 display nqa-server session

21.7.73 nqa-server tcpconnect

Function

The **nqa-server tcpconnect** command configures the IP address and port number for the TCP server in an NQA TCP test instance.

The **undo nqa-server tcpconnect** command deletes the IP address and port number configured for the TCP server in an NQA TCP test instance.

By default, no IP address or port number is configured for the TCP server in an NQA TCP test instance.

Format

nqa-server tcpconnect [**vpn-instance** *vpn-instance-name*] *ip-address port-number*

undo nqa-server tcpconnect { **all** | [**vpn-instance** *vpn-instance-name*] *ip-address port-number* }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the TCP server belongs. **NOTE** This parameter is invalid when a loopback address is specified as the TCP server address.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
all	Indicates all TCP listening addresses and port numbers.	-
ip-address	Specifies the IP address of the TCP server for monitoring TCP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the TCP server for monitoring TCP services.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NQA TCP test is used to detect the rate at which a TCP connection is set up between an NQA client and a TCP server through the three-way handshake. In a TCP test instance, a TCP server needs to be configured on the server end to respond to probe packets.

Perform the following steps on the client to configure TCP server parameters:

- Run the **destination-address** command to configure the destination address of an NQA test instance or the IP address of the TCP server.

 Copyright © Huawei Technologies Co., Ltd.

- Run the **destination-port** command to configure the destination port number of an NQA test instance, or the port number of the TCP server.

If the client and the server are connected through a VPN, you need to specify the VPN instance name.

Configuration Impact

Running the **undo nqa-server tcpconnect all** command will delete the IP address and port number of the TCP server.

Precautions

A TCP server is configured only in a TCP test instance.

Example

Create a TCP server for an NQA test instance with the IP address as 10.10.10.1 and the port number as 5000.

```
<Huawei> system-view
[Huawei] nqa-server tcpconnect 10.10.10.1 5000
```

Related Topics

21.7.9 destination-address

21.7.10 destination-port

21.7.74 nqa-server udpecho

Function

The **nqa-server udpecho** command configures the IP address and port number for the UDP server in an NQA test.

The **undo nqa-server udpecho** command deletes the IP address and port number configured for the UDP server in an NQA test.

By default, no IP address or port number is configured for the UDP server in an NQA test.

Format

nqa-server udpecho [**vpn-instance** *vpn-instance-name*] { **auto-address** | *ip-address* | **ipv6** *ipv6-address* } *port-number*

undo nqa-server udpecho { [**vpn-instance** *vpn-instance-name*] { **auto-address** | *ip-address* | **ipv6** *ipv6-address* } *port-number* | **all** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the server belongs. **NOTE** This parameter is invalid when a loopback address is specified as the UDP server address.	The value is a string of 1 to 31 characters.
all	Specifies a server for all NQA test instances.	-
ip-address	Specifies the IP address of the server for monitoring UDP services.	The value is in dotted decimal notation.
port-number	Specifies the port number of the server for monitoring UDP services.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.
ipv6 *ipv6-address*	Specifies the IPv6 address of the server for monitoring UDP services.	-
auto-address	Configures the UDP service on the NQA server to automatically monitor all IPv4 addresses.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command is used on a UDP server.

UDP packets are transmitted in a jitter test. The test is used to obtain the packet delay, jitter, and packet loss ratio by comparing timestamps in the request and response packets. A UDP server needs to be configured for an NQA test to respond to probe packets.

If the client and the server are connected through a VPN, you need to specify the VPN instance name.

If the local IPv4 address cannot be predicted because of dynamic address allocation by DHCP, specify the **auto-address** keyword to configure the UDP service on the NQA server to automatically monitor all IPv4 addresses.

 Copyright © Huawei Technologies Co., Ltd.

Configuration Impact

Running the **undo nqa-server udpecho all** command will delete the IP address and port number of the UDP server for all NQA UDP test instances.

Precautions

- If the version number of the jitter test packets is 1, the command is optional.
- If the version number of the jitter test packets is 2, the command is mandatory. If the command is not configured, the jitter test instance on the ingress will fail due to timeout.

Example

Create an NQA UDP monitoring server with the IP address 10.10.10.2 and the port number 6000.

```
<Huawei> system-view
[Huawei] nqa-server udpecho 10.10.10.2 6000
```

21.7.75 nqa upload statistics datetime-type

Function

The **nqa upload statistics datetime-type** command configures the time type based on which NQA test results are uploaded to the server.

The **undo nqa upload statistics datetime-type** command restores the default time type based on which NQA test results are uploaded to the server.

The default time type based on which NQA test results are uploaded to the server is Coordinated Universal Time (UTC).

Format

nqa upload statistics datetime-type { **utc** | **local** }

undo nqa upload statistics datetime-type

Parameters

Parameter	Description	Value
utc	Indicates that NQA test results are uploaded to the server based on UTC.	-
local	Indicates that NQA test results are uploaded to the server based on local time.	-

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

UTC is the default time type based on which NQA test results are uploaded to the server. This time type causes difficulties in time understanding. To change the time type to local time, run the **nqa upload statistics datetime-type local** command.

NOTE

- UTC: Coordinated Universal Time, which is the standard time used globally.
- Local time: If the local time is faster than UTC, for example, Beijing Time is 8 hours faster than UTC, the time zone of China is UTC+8. If the local time is slower than UTC, for example, Hawaii Time is 10 hours slower than UTC, the time zone of Hawaii is UTC-10.

Example

Change the time type based on which NQA test results are uploaded to the server to local time.

```
<Huawei> system-view
[Huawei] nqa upload statistics datetime-type local
```

21.7.76 probe-count

Function

The **probe-count** command sets the number of probes for an NQA test instance.

The **undo probe-count** command restores the default number of probes for an NQA test instance.

By default, the number of probes for an NQA test instance is 3.

Format

probe-count *number*

undo probe-count

Parameters

Parameter	Description	Value
number	Specifies the number of probes in an NQA test instance.	The value is an integer that ranges from 1 to 15. The default value is 3. **NOTE** The number of probes in a trace test instance cannot be more than 10.

Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NQA test consists of multiple probes. By default, if one or more probes are successful in an NQA test, the test is considered successful. If all probes fail, the test is considered a failure. The number of probes in an NQA test is based on the network quality.

- If the network to be tested is a reliable network, the number of probes can be set relatively small because the probe can be successful after a small number of probe packets are sent.
- If the network to be tested is an unreliable network, the number of probes can be set relatively large because the probe can be successful only after a large number of probe packets are sent.

You can also detect the network quality based on statistics obtained from multiple probes. For example,

- If the probe test is successful after a small number of probes packets are sent, the network quality is good.
- If the probe test is successful after a large number of probes packets are sent, the network quality is poor.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Configuration Impact

- In jitter test instances, the number of sent packets = **probe-count** x **jitter-packetnum**, but the product cannot exceed 3000.
- If the number of probes has been configured, running the **probe-count** command will override the previous configuration.

Precautions

The number of probes cannot be set for an FTP or a DNS test.

The number of probes of a running test instance cannot be changed.

Example

Set the number of probes to 6 in NQA test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] probe-count 6
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.47 jitter-packetnum
21.7.77 probe-failtimes

21.7.77 probe-failtimes

Function

The **probe-failtimes** command sets the threshold for the number of traps to be sent when the NQA test fails. That is, test packet fragmentation is not allowed.

The **undo probe-failtimes** command restores the default threshold for the number of traps to be sent when the NQA test fails.

By default, one trap is sent for each probe failure.

Format

probe-failtimes *times*

undo probe-failtimes

Parameters

Parameter	Description	Value
times	Specifies the threshold for the number of traps to be sent when the NQA test fails, that is, the number of continuous probe failures.	The value is an integer that ranges from 1 to 15. The default value is 1.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NQA probe test is used to check whether response packets are received in a probe. If the number of continuous probe failures reaches the specified value, the system sends a trap to the specified NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Follow-up Procedure

 Copyright © Huawei Technologies Co., Ltd.

Run the **send-trap probefailure** command to enable the system to send a trap to the NMS after a probe fails. Otherwise, the trap cannot be sent to the NMS after a probe fails.

Precautions

- This configuration of a running test instance cannot be changed.
- If the test instance does not support **probe-count** *number*, you are advised to set **probe-failtimes** to 1; otherwise, traps cannot be sent.
- If the test instance supports **probe-count** *number*, you are advised to set **probe-failtimes** to be smaller or equivalent to probe-count; otherwise, traps cannot be sent.

Example

Set the number of continuous probe failures to 10 in the test named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type tcp
[Huawei-nqa-user-test] probe-failtimes 10
```

Related Topics

21.7.95 test-type

21.7.86 send-trap

21.7.78 packet-rewrite-check

Function

The **packet-rewrite-check** command configures the NQA packet rewrite check function by padding NQA packets.

The **undo packet-rewrite-check** command cancels NQA packet padding.

By default, NQA packet padding is not configured.

Format

packet-rewrite-check { **alternant-binary** | **same-binary** }

undo packet-rewrite-check

Parameters

Parameter	Description	Value
alternant-binary	Pads bits 0101 and 1010 alternatively into test packets.	-
same-binary	Pads bits 0000 and 1111 alternatively into test packets.	-

Views

NQA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Packet rewrite frequently occurs on the live network. The NQA packet rewrite check function can locate the device where the packet rewrite occurs by dividing the network into different parts and checking these parts one by one. The NQA packet rewrite check function uses test packets padded with specified bits for rewrite checking. Bit transition may occur on any bit of the packet, for example, it may occur on one bit in bits 1010, 0000, or 1111. To locate where the bit transition or whether packet rewrite occurs, configuring both **alternant-binary** and **same-binary** is recommended. In this manner, the length and contents of the bits can be changed as required. For example, bits 1010 can be padded into the first test packet and 0101 into the second one. After receiving the response packet, the device checks contents of the packet and determines whether the packet is rewritten.

Configuration Impact

Packet contents will be changed because bit characters are padded into the packet.

Precautions

If the **packet-rewrite-check** command has been configured, the **datafill** command cannot be used. In addition, you cannot configure the **hardware-based enable** command, because the LPU does not support the NQA packet rewrite check function.

Example

Pad bits 0000 and 1111 alternatively into test packets to be sent in the test instance named **user city1**.

```
<Huawei> system-view
[Huawei] nqa test-instance user city1
[Huawei-nqa-user-city1] test-type jitter
[Huawei-nqa-user-city1] packet-rewrite-check same-binary
```

21.7.79 records

Function

The **records** command sets the maximum number of history records and the maximum number of test results for NQA test instances.

The **undo records** command restores the default maximum number of history records and the default maximum number of test results for NQA test instances.

By default, the number of history records is 50, and the number of test results is 5.

 Copyright © Huawei Technologies Co., Ltd.

Format

records { **history** *number* | **result** *number* }

undo records { **history** | **result** }

Parameters

Parameter	Description	Value
history *number*	Specifies the maximum number of history records.	The value is an integer that ranges from 0 to 50. The default value is 50.
result *number*	Specifies the maximum number of test results.	The value is an integer that ranges from 1 to 10. The default value is 5.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

You can run the **records** command to set the maximum number of history records and the maximum number of test results for NQA test instances.

By default, a test instance supports 50 history records. You need to limit the number of history records on the device. In addition, you need to set the number of allowed remaining history records that can be added. The configured maximum number of history records cannot exceed the sum of the total default number of history records and the remaining number of history records.

Precautions

The type of a test instance has been specified using the **test-type** command.

This configuration of a running test instance cannot be changed.

Example

Set the maximum number of history records to 30 for test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] records history 30
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.18 display nqa history

21.7.20 display nqa results

21.7.80 records history-filter

Function

The **records history-filter** command enables a device to filter out records in a historical NQA test instance table.

The **undo records history-filter** command disables a device from filtering records in historical NQA test instance tables.

By default, a device does not filter records in historical NQA test instance tables.

Format

records history-filter { **all** | **failures** }

undo records history-filter

Parameters

Parameter	Description	Value
all	Indicates all records.	-
failures	Indicates records about failed test instances.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Before running the **records history-filter** command, you must run the **test-type** command to specify the test instance type.

To filter records about failed NQA test instances, configure the **failures** parameter in the **records history-filter** command.

NOTE

The **records history-filter** command only takes effect on ICMP test instances.

Example

Enable a device to filter records about failed NQA test instances in a test named **user test**.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] records history-filter failures
```

Related Topics

21.7.18 display nqa history

21.7.20 display nqa results

21.7.81 remote-pw-id

Function

Using the **remote-pw-id** command, you can configure the ID of the remote end of a PW or a VC.

Using the **undo remote-pw-id** command, you can remove the configured ID of the remote end of a PW or a VC.

When the VC type is LDP, **remote-pw-id** defaults to be 0.

Format

remote-pw-id *remote-pw-id*

undo remote-pw-id

Parameters

Parameter	Description	Value
remote-pw-id	Specifies the ID of the remote end of a PW or a VC.	The value is a decimal integer. ● In the case of a PWE3 ping test instance, the value of *remote-pw-id* is an integer that ranges from 1 to 4294967295, and only the VC type of LDP is supported. The default value is 0, indicating that the ID of the remote end of a PW is not configured. ● In the case of a PWE3 trace, – if the VC type is LDP, the value of *remote-pw-id* is an integer that ranges from 1 to 4294967295. The default value is 0. – if the VC type is BGP, the value of *remote-pw-id* is an integer that ranges from 0 to 65534.

Views

NQA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Before running the **remote-pw-id** command, you must set the test type to PWE3 Trace or PWE3 Ping in the NQA view.

Example

In the NQA view, configure the ID of the remote end of a PW to 100, the administrator to admin, and the test type to PWE3 trace.

```
<Huawei> system-view
[Huawei] nqa test-instance admin pwe3
[Huawei-nqa-admin-pwe3] test-type pwe3trace
[Huawei-nqa-admin-pwe3] remote-pw-id 100
```

21.7.82 remote-address (NQA view)

Function

Using the **remote-address** command, you can configure the remote address.

Using the **undo remote-address** command, you can delete a remote address.

By default, no remote address is configured.

Format

remote-address ipv4 *remote-ip-address*

undo remote-address

Parameters

Parameter	Description	Value
ipv4 *remote-ip-address*	Specifies the remotely assigned IP address.	It is in dotted decimal notation.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Use the **remote-address** command, you can specify a remote ip address.

 Copyright © Huawei Technologies Co., Ltd.

The supported test instance are:

- vplsmtrace
- vplspwping

Example

Configure an IP address 1.1.1.1 for VPLS multicast trace test.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type vplsmtrace
[Huawei-nqa-user-test] remote-address ipv4 1.1.1.1
```

21.7.83 reset ip nqa-compatible responder statistics

Function

The **reset ip nqa-compatible responder statistics** command deletes statistics on the NQA handshake packets sent from the third-party device or NMS software.

Format

reset ip nqa-compatible responder statistics

Parameters

None

Views

User view

Default Level

1: Monitoring level

Usage Guidelines

Usage Scenario

Before checking the latest status of communication between the device and third-party device or NMS software, use this command to delete old statistics first.

Precautions

Once statistics on the NQA handshake packets sent from the third-party device or NMS software are deleted, they cannot be restored. Confirm the action before you perform it.

Example

Delete statistics on NQA handshake packets sent from the third-party device or NMS software.

```
<Huawei> reset ip nqa-compatible responder statistics
```

 Copyright © Huawei Technologies Co., Ltd.

21.7.84 restart (NQA view)

Function

The **restart** command restarts the current running test instance.

Format

restart

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Function of the **restart** command is the same as that of the **start now** command.

Example

Restart the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] destination-port 8000
[Huawei-nqa-user-test] destination-address ipv4 10.1.1.1
[Huawei-nqa-user-test] restart
```

Related Topics

21.7.92 start
21.7.93 stop

21.7.85 sendpacket passroute

Function

The **sendpacket passroute** command enables test packets to be sent without searching the routing table.

The **undo sendpacket passroute** command restores the default setting.

By default, the test packet is sent according to the routing table.

 Copyright © Huawei Technologies Co., Ltd.

Format

sendpacket passroute

undo sendpacket passroute

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The type of a test instance has been specified using the **test-type** command. The type of test instances that are supported is as follows:

- ICMP
- TCP
- UDP
- HTTP
- Jitter
- FTP
- SNMP
- Trace

You cannot change this configuration of a running test instance.

After the **sendpacket passroute** command is executed, the device sends test packets without searching the routing table. However, the configurations of **ttl** and **ip-forwarding** become invalid.

Example

Enable test packets to be sent without searching the routing table.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] sendpacket passroute
```

Related Topics

21.7.95 test-type

21.7.56 nqa

 Copyright © Huawei Technologies Co., Ltd.

21.7.86 send-trap

Function

The **send-trap** command configures conditions for sending traps.

The **undo send-trap** command deletes the previous configuration.

By default, the device is disabled from sending traps.

Format

send-trap { **all** | { **owd-ds** | **owd-sd** | **probefailure** | **rtd** | **testcomplete** | **testfailure** | **jitter-sd** | **jitter-ds** | **testresult-change** } * }

undo send-trap { **all** | { **owd-ds** | **owd-sd** | **probefailure** | **rtd** | **testcomplete** | **testfailure** | **jitter-sd** | **jitter-ds** | **testresult-change** } * }

Parameters

Parameter	Description	Value
all	Indicates that a trap is sent in any of the following situations: ● The one-way delay (OWD) exceeds the threshold. ● The RTD exceeds the threshold. ● NQA probes fail. ● An NQA test succeeds. ● NQA tests fail. ● NQA probe result changes.	-
owd-ds	Indicates that a trap is sent when the OWD from the destination to the source exceeds the threshold. **NOTE** This parameter applies only to jitter test instances.	-
owd-sd	Indicates that a trap is sent when the OWD from the source to the destination exceeds the threshold. **NOTE** This parameter applies only to jitter test instances.	-
probefailure	Indicates that a trap is sent when the number of probe failures reaches the threshold. **NOTE** This parameter does not apply to Jitter test instances.	-
rtd	Indicates that a trap is sent when the RTD exceeds the threshold.	-
testcomplete	Indicates that a trap is sent when a test succeeds.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
testfailure	Indicates that a trap is sent when the number of test failures reaches the threshold.	-
jitter-sd	Indicates that a trap is sent when the jitter from the source to the destination exceeds the threshold.	-
jitter-ds	Indicates that a trap is sent when the jitter from the destination to the source exceeds the threshold.	-
testresult-change	Indicates that a trap is sent when the probe result changes. **NOTE** This function supports only ICMP test instances.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Traps are generated no matter whether the NQA test succeeds or fails. You can determine whether traps are sent to the NMS by enabling or disabling the trap function.

The device sends traps to the NMS in any of the following situations:

- The OWD exceeds the threshold.

  If the OWD from the source to the destination or from the destination to the source exceeds the threshold, the device sends a trap to the NMS using the configured NMS address.
- The RTD exceeds the threshold.

  If the RTD exceeds the threshold, the device sends a trap to the NMS using the configured address.
- NQA probes fail.

  When no response packet is received after a specified number of continuous test packets are sent, the device sends a trap to the NMS using the configured address.
- An NQA test succeeds.

  When the device receives a response packet from a destination address, the device sends a trap to the NMS using the configured address.
- NQA tests fail.

  When the number of continuous test failures reaches the maximum number, the device sends a trap to the NMS using the configured address.
- NQA probe result changes.

 Copyright © Huawei Technologies Co., Ltd.

When the NQA probe result changes, the device sends a trap to the NMS using the configured address.

You can run the **send-trap** command to configure conditions for sending traps. When a condition is met, the device sends a trap to the NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

The route between the device and NMS is reachable, and related configurations are complete. The trap function has been enabled for the NQA module using the **snmp-agent trap enable feature-name nqa** command, and the host where traps are sent is configured using the **snmp-agent target-host trap-hostname** command; otherwise, traps cannot be sent to the NMS.

Precautions

You cannot change this configuration of a running test instance.

Example

Configure the test instance **user test** to send a trap when the test fails.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] send-trap testfailure
```

Related Topics

21.7.95 test-type

21.7.88 snmp-agent trap enable feature-name nqa

21.1.27 snmp-agent target-host trap-hostname

21.7.77 probe-failtimes

21.7.94 test-failtimes

21.7.87 set-df

Function

The **set-df** command configures the DF (Don't Fragment) field of the test packet. This field prevents packets from being fragmented.

The **undo set-df** command restores the default setting.

By default, packet fragmentation is allowed.

Format

set-df

undo set-df

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If two hosts need to communicate with each other over multiple networks, the smallest MTU value of the networks is the path MTU value. Packets can be transmitted normally over multiple networks only after the path MTU value is obtained.

If the DF bit of a packet is not configured, and the length of the packet is longer than the MTU value, the packet will be fragmented into several fragments that are shorter than the path MTU value. As a result, the path MTU cannot be detected by sending packets with increasing lengths. To detect the path MTU value, run the **set-df** command to prohibit packet fragmentation. Then, increase the length of packets sent along the path to find the path MTU value.

Prerequisites

The type of a test instance has been set to Trace using the **test-type trace** command.

Precautions

The configuration of the DF bit for packets in a running test instance cannot be changed.

Example

Set the test packet sent without being fragmented.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type trace
[Huawei-nqa-user-test] set-df
```

Related Topics

21.7.95 test-type

21.7.88 snmp-agent trap enable feature-name nqa

Function

The **snmp-agent trap enable feature-name nqa** command enables the trap function for the NQA module.

The **undo snmp-agent trap enable feature-name nqa** command disables the trap function for the NQA module.

By default, the trap function is enabled for the NQA module.

 Copyright © Huawei Technologies Co., Ltd.

Format

snmp-agent trap enable feature-name nqa [**trap-name** { **nqaresultsprobefailed** | **nqahttpstatsprobefailed** | **pingprobefailed** | **nqaftpstatsprobefailed** | **pingtestfailed** | **pingtestcompleted** | **traceroutetestfailed** | **traceroutetestcompleted** | **nqaresultstestfailed** | **nqaresultstestcompleted** | **nqaresultsthresholdnotification** | **nqahttpstatstestfailed** | **nqahttpstatstestcompleted** | **nqahttpstatsthresholdnotification** | **nqaftpstatstestfailed** | **nqaftpstatstestcompleted** | **nqaftpstatsthresholdnotification** | **nqajitterstatstestfailed** | **nqajitterstatstestcompleted** | **nqajitterstatsrtdthresholdnotification** | **nqajitterstatsowdthresholdnotificationsd** | **nqajitterstatsowdthresholdnotificationds** | **nqarisingalarmnotification** | **nqafaillingalarmnotification** | **nqaftpsaverecordnotification** | **nqajitterstatsjitterthresholdnotificationsd** | **nqajitterstatsjitterthresholdnotificationds** | **nqareflectorstatechangenotification** | **nqaResultsTestResultChange** }]

undo snmp-agent trap enable feature-name nqa [**trap-name** { **nqaresultsprobefailed** | **nqahttpstatsprobefailed** | **pingprobefailed** | **nqaftpstatsprobefailed** | **pingtestfailed** | **pingtestcompleted** | **traceroutetestfailed** | **traceroutetestcompleted** | **nqaresultstestfailed** | **nqaresultstestcompleted** | **nqaresultsthresholdnotification** | **nqahttpstatstestfailed** | **nqahttpstatstestcompleted** | **nqahttpstatsthresholdnotification** | **nqaftpstatstestfailed** | **nqaftpstatstestcompleted** | **nqaftpstatsthresholdnotification** | **nqajitterstatstestfailed** | **nqajitterstatstestcompleted** | **nqajitterstatsrtdthresholdnotification** | **nqajitterstatsowdthresholdnotificationsd** | **nqajitterstatsowdthresholdnotificationds** | **nqarisingalarmnotification** | **nqafaillingalarmnotification** | **nqaftpsaverecordnotification** | **nqajitterstatsjitterthresholdnotificationsd** | **nqajitterstatsjitterthresholdnotificationds** | **nqareflectorstatechangenotification** | **nqaResultsTestResultChange** }]

Parameters

Parameter	Description	Value
trap-name	Enables the trap function for the specified event for the NQA module.	-
nqaresultsprobefailed	Sends a trap when the number of continuous probe failures exceeds the threshold.	-
nqahttpstatsprobefailed	Sends a trap when the number of continuous probe failures exceeds the threshold in an HTTP test instance.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pingprobefailed	Sends a trap when the number of continuous ping failures exceeds the threshold.	-
nqaftpstatsprobefailed	Sends a trap when a test result fails to be saved to the FTP server.	-
pingtestfailed	Sends a trap when a ping test fails.	-
pingtestcompleted	Sends a trap when a ping test is complete.	-
traceroutetestfailed	Sends a trap when no destination path is obtained in a traceroute test.	-
traceroutetestcompleted	Sends a trap when a destination path is obtained in a traceroute test.	-
nqaresultstestfailed	Sends a trap when a common test fails.	-
nqaresultstestcompleted	Sends a trap when a common test is complete.	-
nqaresultsthresholdnotification	Sends a trap when the completing time of a test instance expires.	-
nqahttpstatstestfailed	Sends a trap when an HTTP test fails.	-
nqahttpstatstestcompleted	Sends a trap when an HTTP test is complete.	-
nqahttpstatsthresholdnotification	Sends a trap when the completing time of an HTTP test instance expires.	-
nqaftpstatstestfailed	Sends a trap when an FTP test fails.	-
nqaftpstatstestcompleted	Sends a trap when an FTP test is complete.	-
nqaftpstatsthresholdnotification	Sends a trap when the completing time of an FTP test instance expires.	-
nqajitterstatstestfailed	Sends a trap when a jitter test fails.	-
nqajitterstatstestcompleted	Sends a trap when a jitter test is complete.	-

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
nqajitterstatsrtdthresholdnotification	Sends a trap when the completing time of a jitter test instance expires.	-
nqajitterstatsowdthresholdnotificationsd	Sends a trap when the time from the source to the destination expires in a jitter test instance.	-
nqajitterstatsowdthresholdnotificationds	Sends a trap when the time from the destination to the source expires in a jitter test instance.	-
nqarisingalarmnotification	Sends a traps when the value of the monitored node exceeds the threshold.	-
nqafaillingalarmnotification	Sends a traps when the value of the monitored node is smaller than the threshold.	-
nqaftpsaverecordnotification	Sends a trap when a test result is saved to the FTP server.	-
nqajitterstatsjitterthresholdnotificationsd	Sends a trap when the jitter time from the source to the destination expires in a jitter test instance.	-
nqajitterstatsjitterthresholdnotificationds	Sends a trap when the jitter time from the destination to the source expires in a jitter test instance.	-
nqareflectorstatechangenotification	Trap generated when the reflector status in the general flow test instance changes.	-
nqaResultsTestResultChange	Trap generated when the probe result of an ICMP test instance changes.	-

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

To enable the trap function for one or more specific events, specify **trap-name**.

Example

Enable the trap function for the NQA nqaftpstatsprobefailed module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name nqa trap-name nqaftpstatsprobefailed
```

Related Topics

21.7.27 display snmp-agent trap feature-name nqa all

21.7.89 source-address

Function

The **source-address** command sets the source IP address for a test instance.

The **undo source-address** command restores the default setting.

By default, the IP address of the interface where packets are sent functions as the source IP address of a test instance.

Format

source-address { **ipv4** *ipv4-address* | **ipv6** *ipv6-address* }

undo source-address

Parameters

Parameter	Description	Value
ipv4 *ipv4-address*	Specifies the IPv4 source address for the NQA test instance.	The value is in dotted decimal notation.
ipv6 *ipv6-address*	Specifies the IPv6 source address for the NQA test instance. **NOTE** Only DNS, ICMP, trace, and jitter tests support IPv6 source addresses.	The value consists of 128 octets, which are classified into 8 groups. Each group contains 4 hexadecimal numbers in the format X:X:X:X:X:X:X:X.

Views

NQA view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The **source-address** command is used to configure the source IP address for the NQA test. After the test packets reach the destination, a packet is returned, with the configured source IP address as the destination address. If no source IP address is configured, the system specifies the IP address that sends test packets as the source IP address.

Prerequisites

The type of a test instance has been specified using the **test-type** command. However, the test type cannot be DHCP.

Precautions

The configuration of the source IP address of the running test instance cannot be changed.

Example

Set the source IP address to 10.1.1.1 for test instance **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] source-address ipv4 10.1.1.1
```

Related Topics

21.7.95 test-type

21.7.90 source-interface

21.7.91 source-port

21.7.90 source-interface

Function

The **source-interface** command configures the source interface for an NQA test instance.

The **undo source-interface** command cancels the configuration.

By default, no source interface is configured for an NQA test instance.

Format

source-interface *interface-type interface-number*

undo source-interface

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the source interface for an NQA test instance.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After test packets reach the destination address, the destination end sends response packets to the client end. After the **source-interface** command is used to configure the source interface for an NQA test instance, there are the following scenarios:

- If the **source-address** command is run to specify the source IP address, the test packets are sent from the specified source interface, but the response packets are received from the configured source IP address.
- If no source IP address is specified for an NQA test instance, the IP address of the source interface will be used as the source IP address of the NQA test instance. In this scenario, the initiated and responded packets are both transmitted over the outbound interface specified by the **source-interface** command.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The source interface can be configured only for DHCP, ICMP, and Jitter test instances.

Precautions

The configuration of the source interface of a running test instance cannot be changed.

Use an interface with an IP address as the source interface of the NQA test instance; otherwise, the command does not take effect.

In the load balancing scenario, trunks and their member interfaces do not support tests.

Example

Set the source interface of test instance **user test** to gigabitethernet 1/0/0.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] source-interface gigabitethernet 1/0/0
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.95 test-type
21.7.91 source-port
21.7.89 source-address

21.7.91 source-port

Function

The **source-port** command configures the source port for an NQA test instance.

The **undo source-port** command restores the default setting.

No default source port number is specified, port numbers are randomly allocated by the system.

Format

source-port *port-number*

undo source-port

Parameters

Parameter	Description	Value
port-number	Specifies the source port number for an NQA test instance.	The value is an integer that ranges from 1 to 65535. The configured port cannot be a well-known port or used by other modules.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a source port number is specified in an NQA test instance, NQA test packets can be regulated more accurately, which prevents the probe packets from being filtered by rules such ACL. The **source-port** command can be used to configure the source port for this NQA test instance:

- If no source port number is specified for an NQA test instance, a port number is selected at random to receive or send NQA test packets.
- If source port number is specified for an NQA test instance, the specified port number is used to receive and send NQA test packets.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The test instance type has been specified using the **test-type** command. The source port number can be configured only for TCP, FTP, HTTP, UDP, jitter (including jitter test instances based on the mechanism that the LPU sends packets), and SNMP test instances.

Precautions

The port specified in the **source-port** command must be available; otherwise, the probe fails.

Port numbers 61442 to 65535 are reserved. Do not use the port numbers; otherwise, the probe fails.

You cannot change this configuration of a running test instance.

Example

Set the source port number of test instance **user test** to 3000.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type tcp
[Huawei-nqa-user-test] source-port 3000
```

Related Topics

21.7.95 test-type

21.7.90 source-interface

21.7.89 source-address

21.7.92 start

Function

The **start** command sets the start mode and end mode for an NQA test instance.

The **undo start** command stops a running NQA test instance or restores the configuration of start mode and end mode of an unperformed NQA test instance.

By default, the test instance stops automatically after test packets are sent.

Format

start at [*yyyy*|*mm*|*dd*] *hh:mm:ss* [**end** { **at** [*yyyy*|*mm*|*dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }]

start delay { **seconds** *second* | *hh:mm:ss* } [**end** { **at** [*yyyy*|*mm*|*dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }]

start now [**end** { **at** [*yyyy*|*mm*|*dd*] *hh:mm:ss* | **delay** { **seconds** *second* | *hh:mm:ss* } | **lifetime** { **seconds** *second* | *hh:mm:ss* } }]

undo start

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
start at [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss*	Performs a test instance at a specified time. **NOTE** The configured time must be later than the time on the device.	-
start delay { **seconds** *second* | *hh*:*mm*:*ss* }	Specifies a delay in performing a test instance.	• **seconds** *second*: specifies a delay in performing a test instance. The value is an integer ranging from 1 to 86399, in seconds. • *hh*:*mm*:*ss*: specifies a delay in performing a test instance. If *hh*:*mm*:*ss* is specified, the system automatically sets the moment in seconds. For example, 1:0:0 indicates that a test instance starts in one hour (3600 seconds).
start now	Performs a test instance immediately.	-
end at [*yyyy*/*mm*/*dd*] *hh*:*mm*:*ss*	Stops a test instance at a specified time.	-
end delay { **seconds** *second* | *hh*:*mm*:*ss* }	Specifies a delay in stopping a test instance. This delay is set based on the current system time. For example: If **start at 9:00:00 end delay seconds 60** is run at 8:59:40, then, a test instance starts at 9:00:00 and ends at 9:00:40.	• **seconds** *second*: specifies a delay in stopping a test instance. The value is an integer ranging from 6 to 86399 in seconds. • *hh*:*mm*:*ss*: specifies a delay in stopping a test instance. For example, 1:0:0 stands for a 3600-second delay from the current system time till the time that the test instance stops.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
end lifetime { **seconds** *second* | *hh:mm:ss* }	Specifies the lifetime of an NQA test instance (starting from the moment that the NQA test instance starts). For example: If **start delay seconds 60 end lifetime seconds 120** is run at 9:00:00, then, a test instance lasts for 120s as it starts at 09:01:00 and ends at 09:03:00.	• **seconds** *second*: sets the life time of a test instance in seconds. The value is an integer ranging from 6 to 86399 in seconds. • *hh:mm:ss*: sets the lifetime of a test instance. For example, 1:0:0 indicates that the lifetime of a test instance is 3600s starting from the moment a test instance starts.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After configuring test instances and relevant attributes, you need to manually set the start and end modes for the test instances. The types of start and end modes are as follows:

- Start modes:
  - Starting a test instance at a specified time
  - Starting a test instance immediately
  - Starting a test instance after a certain delay
- End modes:
  - Ending a test instance at a specified time
  - Ending a test instance immediately
  - Ending a test instance after a certain delay
  - Ending a test instance after all test packets are sent

You can set the start and end modes as required.

Precautions

If the number of the running test instances reaches the maximum value defined by the system, the **start** command is invalid.

For the same test instance, the **start now** command can be used again only when the previous configuration is complete.

When starting a test instance at a specified time, the time must be later than the current time on the device.

 Copyright © Huawei Technologies Co., Ltd.

Example

Perform the test 10 hours later.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] destination-address ipv4 10.1.1.1
[Huawei-nqa-user-test] destination-port 4000
[Huawei-nqa-user-test] start delay 10:00:00
```

Related Topics

21.7.95 test-type

21.7.23 display nqa-agent

21.7.93 stop

Function

The **stop** command stops an NQA test instance.

Format

stop

Parameters

None

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

You can run this command to stop only the running NQA test instances, that is, test instances in active state.

Example

Stop the test instance named **user test**.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] stop
```

Related Topics

21.7.92 start

21.7.31 frequency

 Copyright © Huawei Technologies Co., Ltd.

21.7.94 test-failtimes

Function

The **test-failtimes** command sets the number of consecutive test failures in an NQA test.

The **undo test-failtimes** command restores the default setting.

By default, a trap message is sent for each test failure.

Format

test-failtimes *times*

undo test-failtimes

Parameters

Parameter	Description	Value
times	Specifies the number of consecutive test failures in an NQA test.	The value is an integer that ranges from 1 to 15. The default value is 1.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

An NQA test consists of multiple probe tests. By default, if one or more probe tests are successful in an NQA test, the test is considered successful. If all probe tests fail, the test is considered failed. If the number of consecutive test failures reaches the specified value, the system will send a trap to the specified NMS.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Follow-up Procedure

Run the **send-trap testfailure** command to send a trap to the NMS after an NQA test fails. Otherwise, the trap cannot be sent to the NMS after an NQA test fails.

Precautions

This configuration of a running test instance cannot be changed.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the number of consecutive test failures to 10.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] test-failtimes 10
```

Related Topics

21.7.29 fail-percent

21.7.86 send-trap

21.7.95 test-type

Function

The **test-type** command configures the test type for an NQA test instance.

The **undo test-type** command cancels the test type configured for an NQA test instance.

By default, no test type is configured.

Format

test-type { **dhcp** | **dns** | **ftp** | **http** | **icmp** | **icmpjitter** | **jitter** | **lspping** | **lsptrace** | **snmp** | **tcp** | **trace** | **udp** | **vplsping** | **vplstrace** | **vplspwping** | **vplspwtrace** }

undo test-type

Parameters

Parameter	Description	Value
dhcp	Specifies a DHCP test.	-
dns	Specifies a DNS test.	-
ftp	Specifies an FTP service test.	-
http	Specifies an HTTP service test.	-
icmp	Specifies an ICMP test.	-
icmpjitter	Specifies an ICMP jitter test, which can detect the jitter on the network by using ICMP packets.	-
jitter	Specifies a jitter test, which can detect the jitter during UDP packet transmission.	-
lspping	Specifies an LSP ping test.	-
lsptrace	Specifies an LSP trace route test.	-
snmp	Specifies an SNMP test.	-
tcp	Specifies a TCP test.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
trace	Specifies a trace test.	-
udp	Specifies a UDP test.	-
vplsping	Specifies a VPLS MAC ping test.	-
vplstrace	Specifies a VPLS MAC trace test.	-
vplspwping	Specifies a VPLS PW ping test.	-
vplspwtrace	Specifies a VPLS PW trace test.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The type of a running test instance cannot be changed.

Example

Configure the test type of an NQA test instance as TCP.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type tcp
```

Related Topics

21.7.56 nqa

21.7.96 timestamp-unit

Function

The **timestamp-unit** command sets the unit of timestamp for an NQA test instance.

The **undo timestamp-unit** command restores the default setting.

By default, the unit of timestamp for an NQA test instance is millisecond.

Format

timestamp-unit { **millisecond** | **microsecond** }

undo timestamp-unit microsecond

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
millisecond	Sets the unit of timestamp for an NQA test instance to millisecond.	-
microsecond	Sets the unit of timestamp for an NQA test instance to microsecond.	-

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The **timestamp-unit millisecond** command sets the unit of timestamp for an NQA test instance to millisecond.

The **timestamp-unit microsecond** command sets the unit of timestamp for an NQA test instance to microsecond.

Prerequisites

Hardware forwarding has been enabled using the **hardware-based enable** command.

Precautions

The **timestamp-unit** command takes effect for only jitter test instances.

Example

Set the unit of timestamp for an NQA test instance to microsecond.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] hardware-based enable
[Huawei-nqa-user-test] timestamp-unit microsecond
```

Related Topics

21.7.56 nqa

21.7.97 threshold

Function

The **threshold** command sets the OWD and RTD threshold.

The **undo threshold** command deletes the OWD threshold and the RTD threshold.

 Copyright © Huawei Technologies Co., Ltd.

By default, no threshold is set.

Format

threshold { **owd-ds** *owd-ds-value* | **owd-sd** *owd-sd-value* | **rtd** *rtd-value* }

undo threshold { **owd-ds** | **owd-sd** | **rtd** }

Parameters

Parameter	Description	Value
owd-ds *owd-ds-value*	Sets the OWD threshold of packets sent from the destination to the source.	The value is an integer that ranges from 1 to 60000. The unit of this value is the same as that of the timestamp set using the **timestamp-unit** command.
owd-sd *owd-sd-value*	Sets the OWD threshold of packets sent from the source to the destination.	The value is an integer that ranges from 1 to 60000. The unit of this value is the same as that of the timestamp set using the **timestamp-unit** command.
rtd *rtd-value*	Sets the RTD threshold.	The value is an integer that ranges from 1 to 60000. The unit of this value is the same as that of the timestamp set using the **timestamp-unit** command.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The OWD threshold is applied only to jitter test instances.

Example

Set the RTD threshold to 2 ms.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] threshold rtd 2
```

Related Topics

21.7.86 send-trap

 Copyright © Huawei Technologies Co., Ltd.

21.7.98 timeout

Function

The **timeout** command sets the timeout period for a probe of an NQA test instance.

The **undo timeout** command restores the default timeout period for a probe of an NQA test instance.

By default, the timeout period for DHCP and FTP test instances is 15 seconds and that for other test instances is 3 seconds.

Format

timeout *time*

undo timeout

Parameters

Parameter	Description	Value
time	Specifies the timeout period for a probe.	The value is an integer that ranges from 1 to 60, in seconds.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The timeout period refers to the waiting time after a probe is sent. If no response packet is received when the timeout period expires, the probe fails. The timeout period is set based on the actual networking. If the value is too small, the NQA test instance fails.

On an unstable network with a low transmission rate, you need to prolong the timeout period for sending probe packets to ensure that response packets can be received.

Prerequisites

The type of a test instance has been specified using the **test-type** command.

Precautions

- You are advised to set the timeout period based on the round-trip time (RTT) value. Ensure that the timeout period set by the **timeout** command is longer than the RTT value.

 Copyright © Huawei Technologies Co., Ltd.

- In all test instances except jitter test instance, the timeout period set by the **timeout** command must be smaller than or equal to the interval of automatic tests set by the **interval** command. Otherwise, the tests fail due to timeout of test packets.
- In a DHCP test, packets are sent at random within 10 seconds. If the timeout period is shorter than 10 seconds, some or all packets may time out. Therefore, in a DHCP test, the timeout period must be longer than 10 seconds. The default timeout period is 15 seconds.

Precautions

You cannot change this configuration of a running test instance.

In an ICMP test instance, if the following conditions are met, the Completion field in the test results will be displayed as **no result**:

- The system CPU usage exceeds 90% and the configured timeout period is less than 6s.
- **frequency** configured ≤ (**probe-count** - 1) × **interval** + 6.

Example

Set the timeout period of the test instance named **user test** to 20 seconds.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type jitter
[Huawei-nqa-user-test] timeout 20
```

Related Topics

21.7.31 frequency

21.7.41 interval (NQA view)

21.7.99 tos

Function

The **tos** command sets the ToS value for an NQA test packet.

The **undo tos** command restores the default ToS value of an NQA test packet.

By default, the ToS value is 0.

Format

tos *value*

undo tos

Parameters

Parameter	Description	Value
value	Specifies the ToS value of a packet.	The value is an integer that ranges from 0 to 255. The default value is 0.

 Copyright © Huawei Technologies Co., Ltd.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The ToS field contains a precedence sub-field and a ToS sub-field. The precedence sub-field indicates the priority of a packet and the ToS sub-field is seldom used. All the bits in the ToS sub-field must be set to 0. You can set the priority of probe packets by setting the ToS value. When a large number of packets are received, packets of high priorities are processed preferentially.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The following types of test instances are not supported:

- DNS
- DHCP
- Trace
- LSP Ping
- LSP Trace

Configuration Impact

If you run the **tos** command multiple times, only the latest configuration takes effect.

Precautions

The ToS value of a running test instance cannot be changed.

Example

Set the ToS value for the test instance named **user test** to 10.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] tos 10
```

Related Topics

21.7.95 test-type

21.7.56 nqa

Copyright © Huawei Technologies Co., Ltd.

21.7.100 tracert-hopfailtimes

Function

The **tracert-hopfailtimes** command sets the number of consecutive failed hops indicating a failed trace test instance.

The **undo tracert-hopfailtimes** command restores the default number of consecutive failed hops indicating a failed trace test instance.

By default, five consecutive failed hops indicates a failed trace test instance.

Format

tracert-hopfailtimes *times*

undo tracert-hopfailtimes

Parameters

Parameter	Description	Value
times	Specifies the number of consecutive failed hops indicating a failed trace test instance.	The value is an integer that ranges from 1 to 255.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **tracert-hopfailtimes** command only takes effect for trace and LSP trace test instances.

You cannot change this configuration of a running test instance.

Example

Set the number of consecutive failed hops indicating a failed trace test instance to 6.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type trace
[Huawei-nqa-user-test] tracert-hopfailtimes 6
```

Related Topics

21.7.95 test-type

 Copyright © Huawei Technologies Co., Ltd.

21.7.101 tracert-livetime

Function

The **tracert-livetime** command sets the time to live (TTL) value for trace test instances in an NQA test.

The **undo tracert-livetime** command restores the default TTL value for trace test instances in an NQA test.

By default, the initial TTL value is 1 and the maximum TTL value is 30.

Format

tracert-livetime first-ttl *first-ttl* **max-ttl** *max-ttl*

undo tracert-livetime

Parameters

Parameter	Description	Value
first-ttl *first-ttl*	Specifies the initial TTL value of a packet.	The value is an integer that ranges from 1 to 255. The default value is 1.
max-ttl *max-ttl*	Specifies the maximum TTL value of a packet.	The value is an integer that ranges from 1 to 255. The value of *max-ttl* must be greater than the value of *first-ttl*. By default, the maximum TTL value is 30.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **tracert-livetime** command takes effect only for trace and LSP trace test instances.

You cannot change this configuration of a running test instance.

Example

Set the initial TTL value of the test instance named **user test** to 5 and the maximum TTL value to 20.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type trace
[Huawei-nqa-user-test] tracert-livetime first-ttl 5 max-ttl 20
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.7.95 test-type

21.7.102 ttl

Function

The **ttl** command sets the TTL value for the test packets of an NQA test instance.

The **undo ttl** command restores the default setting.

The default TTL value is 30.

Format

ttl *number*

undo ttl

Parameters

Parameter	Description	Value
number	Specifies the TTL value.	The value is an integer that ranges from 1 to 255. The default TTL value is 30.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To prevent test packets from being transmitted endlessly, the test instance must be performed within certain hops.

When a test packet is created, you can run the **ttl** command to set the TTL value. When the test packet is transmitted along Layer 3 routing devices, each Layer 3 routing device decrements the TTL value by one when the packet arrives. When the TTL value is 0, the Layer 3 routing device discards the test packet and sends an error message to the sending end. This prevents test packets from being transmitted endlessly.

Prerequisites

The type of a test instance has been specified using the **test-type** command. The type of test instances that are not supported is as follows:

- DNS

 Copyright © Huawei Technologies Co., Ltd.

- DHCP
- Trace
- LSP Trace

Configuration Impact

If you run the **ttl** command multiple times, only the latest configuration takes effect.

Precautions

The type of a running test instance cannot be changed.

Example

Set the TTL value for the test packets of a test instance named **user test** to 10.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] ttl 10
```

Related Topics

21.7.95 test-type

21.7.103 ttl-copymode

Function

Using the **ttl-copymode** command, you can specify the TTL propagation mode (pipe or uniform) for a multi-hop PW detection.

Using the **undo ttl-copymode** command, you can cancel the TTL propagation mode configured in the NQA view.

By default, the TTL propagation mode varies with products.

Format

ttl-copymode { **pipe** | **uniform** }

undo ttl-copymode

Parameters

Parameter	Description	Value
pipe	Sets the TTL propagation mode to pipe.	-
uniform	Sets the TTL propagation mode to uniform.	-

Views

NQA view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

During the detection of a multi-hop PW, if the default TTL propagation mode on different devices is different, you need to specify the TTL propagation mode on the first hop of the PW. This command is used to detect BGP/MPLS IP VPN networks.

The TTL propagated in pipe and uniform modes is processed in different manners:

- When receiving a packet carrying the TTL propagated in pipe mode, the system strips the outer tag of the packet, decreases the TTL in the inner tag by 1, and then sets the TTL in the outer tag to 255.
- When receiving a packet carrying the TTL propagated in uniform mode, the system maps the TTL in the outer tag to the inner tag, decreases the TTL in the inner tag by 1, and then sets the TTL in the outer tag to the value of the TTL in the inner tag.

NOTE

The **ttl-copymode** command makes sense only in the trace test instances. In the case of an trace test instance, you need to first run the **vpn-instance** *vpn-instance-name* command to bind the NQA trace test instance with a VPN instance.

Example

Configure the TTL propagation mode of packets in the NQA trace test instance as pipe.

```
<Huawei> system-view
[Huawei] nqa test-instance admin trace
[Huawei-nqa-admin-trace] test-type trace
[Huawei-nqa-admin-trace] vpn-instance voice
[Huawei-nqa-admin-trace] ttl-copymode pipe
```

Related Topics

21.7.95 test-type

21.7.104 vlan (NQA view)

Function

Using the **vlan** command, you can configure a VLAN ID for the NQA test instance.

Using the **undo vlan** command, you can delete a specified VLAN.

By default, no VLAN ID is configured.

Format

vlan *vlan-id*

undo vlan

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
vlan *vlan-id*	Indicates a VLAN. *vlan-id* specifies the VLAN ID.	*vlan-id* is an integer that ranges from 1 to 4094.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

If both the destination MAC address and the specified VLAN need to be matched, you need to set a VLAN ID.

The test instances that can be configured with a VLAN ID include:

- vplsping
- vplstrace
- vplspwping
- vplspwtrace
- vplsmping
- vplsmtrace
- gmacping
- gmactrace
- generalflow

Example

Set the VLAN ID of the test instance to 1.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type vplsping
[Huawei-nqa-user-test] vlan 1
```

Related Topics

6.3.43 vlan

21.7.105 vpn-instance

Function

The **vpn-instance** command configures the VPN instance that an NQA test instance belongs to.

The **undo vpn-instance** command deletes the configured VPN instance.

 Copyright © Huawei Technologies Co., Ltd.

By default, no VPN instance is configured.

Format

vpn-instance *vpn-instance-name*

undo vpn-instance

Parameters

Parameter	Description	Value
vpn-instance-name	Specifies the VPN instance that an NQA test instance belongs to.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Views

NQA view

Default Level

2: Configuration level

Usage Guidelines

The **vpn-instance** command does not take effect for DNS, LSP ping, LSP trace, and DHCP test instances.

Example

Set the VPN instance for an NQA test instance named **user test** to vrf1.

```
<Huawei> system-view
[Huawei] nqa test-instance user test
[Huawei-nqa-user-test] test-type icmp
[Huawei-nqa-user-test] vpn-instance vrf1
```

Related Topics

21.7.56 nqa

21.7.95 test-type

21.8 LSDP Configuration Commands

NOTE

An AR3200 has active/standby MPUs installed. An active/standby switchover between the MPUs will also cause the interface status to alternate between Down and Up. It is difficult to determine whether the interface status change is caused by MPU switchover or LSDP. Therefore, you are not advised to configure LSDP on an AR3200.

Copyright © Huawei Technologies Co., Ltd.

21.8.1 lsdp

Function

The **lsdp** command configures LSDP on a device.

The **undo lsdp** command disables LSDP on a device.

By default, the LSDP function is disabled on a device.

Format

lsdp *ip-address* [*nexthop-address*] [**interval** *interval-number*] [**probe-count** *count-number*]

undo lsdp

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IP address of probe packets.	The value is in dotted decimal notation.
nexthop-address	Specifies the next-hop IP address of probe packets.	The value is in dotted decimal notation.
interval *interval-number*	Specifies the interval for sending probe packets.	The value is an integer that ranges from 100 to 10000, in milliseconds. The default value is 1000. That is, the device sends a probe packet every second.
probe-count *count-number*	Specifies the maximum number of probe counts upon probe failures.	The value is an integer that ranges from 3 to 10. The default value is 3. That is, the device considers a probe failed if the device does not receive a reply packet after three ARP or ICMP request packets are sent. Then the device sets the interface status to Down.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

After the **lsdp** command is executed on an interface, the interface sends probe packets (ARP and ICMP packets) to the destination address to detect link connectivity. If the interface receives a reply packet within a probe interval, LSDP considers the destination address reachable. In this situation, the probe is successful and LSDP sets the interface status to Up. If the interface does not receive a reply packet within a probe interval, LSDP considers the destination address unreachable. In this situation, the probe fails, LSDP sets the interface status to Down, and services on this interface become invalid.

The probe intervals are calculated as follows:

- Interval for sending ARP packets: *interval-number***count-number*
- Interval for sending ICMP packets: *interval-number**(*count-number*+n)

  n is the number of sent ARP packets. The value ranges from 1 to *count-number*.

The default value of *interval-number* is 1000. That is, the device sends a probe packet every second. The default value of *count-number* is 3. That is, an LSDP probe fails if the interface does not receive an ARP reply packet within 3x1 seconds or an ICMP reply packet within (3+n)x1 seconds. Then LSDP sets the interface status to Down. When the default value of *count-number* is used, n can be 1, 2, or 3, indicating that the interface receives an ARP reply packet after sending 1, 2, or 3 ARP request packets.

After LSDP sets the status of an interface to Down, the device continuously sends ARP and ICMP packets for probing. When the link is recovered, LSDP sets the interface to Up.

Configuration Impact

The interface with LSDP configured periodically sends ARP and ICMP packets. When LSDP detects that the link to a destination address fails, it sets the interface status to Down.

Example

Configure an interface to send one LSDP probe packet to destination address 10.1.1.1 through next-hop address 10.10.1.1 every 100 milliseconds and set the maximum number of probe counts to 5.

```
<Huawei> system-view
[Huawei] interface gigabitethernet1/0/0
[Huawei-GigabitEthernet1/0/0] lsdp 10.1.1.1 10.10.1.1 interval 100 probe-count 5
```

Related Topics

21.8.3 display lsdp

 Copyright © Huawei Technologies Co., Ltd.

21.8.2 lsdp trigger protocol ospf delay-up

Function

The **lsdp trigger protocol ospf delay-up** command configures a delay in sending OSPF packets after LSDP detects that a link goes Up.

The **undo lsdp trigger protocol** command restores the default configuration.

By default, no delay is configured for the device to send OSPF packets after LSDP detects that a link goes Up.

Format

lsdp trigger protocol ospf delay-up *delay-time*

undo lsdp trigger protocol

Parameters

Parameter	Description	Value
delay-time	Specifies a delay.	The value is an integer that ranges from 1 to 3600, in seconds.

Views

Ethernet interface view, GE interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When LSDP detects that a link goes Down, OSPF packets will be blocked. You can run the **lsdp trigger protocol ospf delay-up** command to configure a delay in sending OSPF packets after LSDP detects that a link goes Up.

Prerequisites

The destination IP address to which probe packets are sent has been configured using the **lsdp** command.

Example

Set the delay in sending OSPF packets after LSDP detects that the link goes Up to 10 seconds.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/1
[Huawei-GigabitEthernet0/0/1] lsdp trigger protocol ospf delay-up 10
```

21.8.3 display lsdp

Function

The **display lsdp** command displays the LSDP information.

Format

display lsdp

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

You can use this command to view LSDP configuration, running status, and running results.

Example

View the LSDP information.

```
<Huawei> display lsdp
======LSDP INFO=========
LSDP Instance Index : 1
LSDP Test : success
LSDP Interface Name : GigabitEthernet0/0/0
LSDP Interface Status : UP
LSDP Interface Ip : 10.1.2.1
LSDP Destination Ip : 10.1.4.2
LSDP Next-hop Ip : 10.1.2.2
LSDP Interval : 1000
LSDP Probe-count : 3
LSDP UpTimes : 0
LSDP DownTimes : 0
========================
```

Table 21-60 Description of the **display lsdp** command output

Item	Description
LSDP Instance Index	LSDP table index.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
LSDP Test	Current LSDP probe result. ● success: Probe is successful. ● fail: Probe fails. ● --: No result.
LSDP Interface Name	Types and numbers of the interface where LSDP is configured.
LSDP Interface Status	Status of the interface where LSDP is configured.
LSDP Interface Ip	IP address of the interface where LSDP is configured.
LSDP Destination Ip	Destination IP address of probe packets. To configure the destination IP address of probe packets, run the **lsdp** command.
LSDP Next-hop Ip	Next-hop IP address of probe packets. To configure the next-hop IP address of probe packets, run the **lsdp** command.
LSDP Interval	Interval for sending probe packets. To configure the interval for sending probe packets, run the **lsdp** command.
LSDP Probe-count	Maximum number of probe counts upon probe failures. To configure the maximum number of probe counts, run the **lsdp** command.
LSDP UpTimes	Maximum number of times an interface goes Up after LSDP is configured.
LSDP DownTimes	Maximum number of times an interface goes Down after LSDP is configured.

Related Topics

21.8.1 lsdp

21.9 Service Diagnosis Configuration Commands

21.9.1 display trace information

 Copyright © Huawei Technologies Co., Ltd.

Function

The **display trace information** command displays information about service diagnosis.

Format

display trace information

Parameters

None

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After configuring service diagnosis, you can run this command to view global information about service diagnosis, for example, the counts of diagnosis instances and objects created on the device.

Example

Display information about service diagnosis.

```
<Huawei> display trace information
Trace Information:
-----------------------------------------------------------
Trace Enable                        : Enable
Debug info level                    : Brief
Debug fill-instance                 : Off
Debug quit-instance                 : Off
Debug output information            : Off
Syslog Source IP Address            : -

The sum of all the instances        : 0
The startID of the instance table   : -
Alloc instance times                : 9
Free instance times                 : 9
The sum of all the objects          : 2
-----------------------------------------------------------
```

Table 21-61 Description of the display trace information command output

Item	Description
Trace Information	Information about service diagnosis.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Trace Enable	Status of service diagnosis. ● Disable: Service diagnosis is disabled. ● Enable: Service diagnosis is enabled. This field can be modified using the **trace enable** command.
Debug info level	Output level of service diagnosis information. ● Brief: brief service diagnosis information. ● Detail: detailed service diagnosis information. This field can be modified using the **trace enable** command.
Debug fill-instance	Debugging status of the **fill-instance** module. ● Off: disabled ● On: enabled
Debug quit-instance	Debugging status of the **quit-instance** module. ● Off: disabled ● On: enabled
Debug output information	Debugging status of the **output information** module. ● Off: disabled ● On: enabled
Syslog Source IP Address	IP address of the interface for exporting diagnosis information to the log server. To set the IP address of the interface for exporting diagnosis information to a log server, run the **trace syslog source** command.
The sum of all the instances	Total number of diagnosis instances.
The startID of the instance table	Start ID of the instance table.
Alloc instance times	Number of the allocated diagnosis instances.
Free instance times	Number of the release diagnosis instances.
The sum of all the objects	Total number of diagnosis objects.

Related Topics

21.9.6 trace enable
21.9.8 trace syslog source

 Copyright © Huawei Technologies Co., Ltd.

21.9.2 display trace instance

Function

The **display trace instance** command displays diagnosis instances on a device.

Format

display trace instance [*instance-start-id* [*instance-end-id*] | **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **cid** *cid*] [**slot** *slot-id*]

Parameters

Parameter	Description	Value
instance-start-id	Specifies the ID of the first instance whose information is displayed, that is, start ID.	The value varies according to different devices.
instance-end-id	Specifies the ID of the last instance whose information is displayed, that is, end ID.	The value varies according to different devices. **NOTE** The *instance-end-id* value must be larger than the *instance-start-id* value.
mac-address *mac-address*	Specifies a MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 4 digits.
ip-address *ip-address*	Specifies an IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces.
interface *interface-type interface-number*	Specifies the type and number of an interface.	-
cid *cid*	Specifies the diagnosis instance CID.	The value varies according to different devices.
slot *slot-id*	Specifies the slot ID of an interface card.	The value varies according to different devices.

 Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you specify no parameter, all diagnosis instances are displayed in sequence. Each time you run this command, 10 diagnosis instances are displayed. For example, all diagnosis instances have been created on the device. When you run the **display trace instance** command for the first time, information about diagnosis instances 0 to 9 is displayed. When you run this command again, information about instances 10 to 19 is displayed. This process is repeated until information about all the diagnosis instances is displayed. If you specify the value of *instance-start-id*, information about 10 diagnosis instances from this ID is displayed.

To view information about diagnosis instances within a specified range, run the **display trace instance** *instance-start-id instance-end-id* command to specify the start and end IDs of diagnosis instances.

Example

Display information about diagnosis instances on the interface with the IP address of 10.10.10.1.

```
<Huawei> display trace instance ip-address 10.10.10.1
Trace Instance:
-------------------------------------------------------------
  ID             : 0
  MAC Address    : 00e0-fc03-0203
  IP Flag        : -
  Session ID     : 4
  IP Address     : 10.10.10.1
  VRF Index      : -
  CID            : -
  Calling Number : -
  SubCallingNum  : NO
  User Name      : -
  Interface      : -
  QinQ VLAN ID   : -
  User VLAN ID   : -
  Access Mode    : pppoe
  User Tunnel ID : -
  Modules online : EAPoL  :0    WEBS   :0    WEB    :0    AAA    :0
                   CM     :0    TM     :0    SAM    :0    RADIUS :0
                   DHCPS  :0    DHCPC  :0    DHCPR  :0    DHCPP  :0
                   TACACS :0    AM     :0    SAVI   :0    WLAN_AC:0
                   L2TP   :0    LNS    :0    PPP    :0    PPPOE  :1
                   PPPOLNS:0
 -------------------------------------------------------------
  Total 1, 1 printed
```

Table 21-62 Description of the display trace instance command output

Item	Description
ID	ID of the diagnosis instance.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
MAC Address	MAC address of the interface.
IP Flag	Flag of the IP address.
Session ID	ID of the session, only valid for PPPoX users.
IP Address	IP address of the interface.
VRF Index	User VRF index.
CID	User connect ID.
Calling Number	User calling number.
SubCallingNum	Whether fuzzy matching is supported.
User Name	User name.
Interface	Interface index.
QinQ VLAN ID	QinQ VLAN ID.
User VLAN ID	User VLAN ID.
Access Mode	User access mode.
User Tunnel ID	User tunnel ID.
Modules online	User status on a module. User status can be: ● 0: The user is offline on the module. ● 1: The user is online on the module.

Related Topics

21.9.7 trace object

21.9.3 display trace object

Function

The **display trace object** command displays the configuration about a service diagnosis object.

Format

display trace object [*service-object-id*] [**slot** *slot-id*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
service-object-id	Specifies the ID of a diagnosis object.	The value is an integer that ranges from 0 to 3.
slot *slot-id*	Specifies the slot ID of an interface card.	The value varies according to different devices.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

If you do not specify the parameters *service-object-id* and **slot**, configurations about all diagnosis objects are displayed.

Example

Display configurations about all diagnosis objects.

```
<Huawei> display trace object
Trace Object:
-------------------------------------------------------------
  Object ID      : 0
  Slot           : -
  MAC Address    : -
  IP Flag        : -
  Session ID     : -
  IP Address     : 1.1.1.1
  VRF Index      : -
  CID            : -
  Calling Number : -
  SubCallingNum  : NO
  User Name      : -
  Interface      : -
  QinQ VLAN ID   : -
  User VLAN ID   : -
  Access Mode    : -
  User Tunnel ID : -
  Output         : command line ( User-Intf 131 )

  Object ID      : 1
  Slot           : -
  MAC Address    : -
  IP Flag        : -
  Session ID     : -
  IP Address     : -
  VRF Index      : -
  CID            : -
  Calling Number : -
  SubCallingNum  : NO
  User Name      : huawei
  Interface      : -
```

 Copyright © Huawei Technologies Co., Ltd.

```
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : -
User Tunnel ID : -
Output         : command line ( User-Intf 131 )

Object ID      : 2
Slot           : -
MAC Address    : 0101-0101-0101
IP Flag        : -
Session ID     : -
IP Address     : -
VRF Index      : -
CID            : -
Calling Number : -
SubCallingNum  : NO
User Name      : -
Interface      : -
QinQ VLAN ID   : -
User VLAN ID   : -
Access Mode    : -
User Tunnel ID : -
Output         : command line ( User-Intf 131 )

-------------------------------------------------------------
Total 3, 3 printed
```

Table 21-63 Description of the display trace object command output

Item	Description
Object ID	ID of the diagnosis object. This parameter is automatically generated from 0 in sequence of creation time.
Slot	Slot ID of the interface board.
MAC Address	MAC address of the interface. To set the MAC address of an interface, run the **trace object** command.
IP Flag	Flag of the IP address.
Session ID	ID of the session, only valid for PPPoX users.
IP Address	IP address of the interface. To set the IP address of an interface, run the **trace object** command.
VRF Index	User VRF index.
CID	User connect ID.
Calling Number	User calling number. To set the calling number, run the **trace object** command.
SubCallingNum	Whether fuzzy matching is supported. To set the SubCallingNum, run the **trace object** command.
User Name	User name. To set the user name, run the **trace object** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Interface	Interface index. To set the interface index, run the **trace object** command.
QinQ VLAN ID	QinQ VLAN ID. To set the QinQ VLAN ID, run the **trace object** command.
User VLAN ID	User VLAN ID. To set the user VLAN ID, run the **trace object** command.
Access Mode	User access mode, including dot1x, mac-authen, portal, wlan, pppoe, and pppolns. To set the user access mode, run the **trace object** command.
User Tunnel ID	User tunnel ID. To set the user tunnel ID, run the **trace object** command.
Output	Direction in which the device exports diagnosis information. To set the direction, run the **trace object** command. ● Command line (User-Intf X): Diagnosis information is displayed on the screen of a configuration terminal. **NOTE** When the configuration terminal is online, X displays the absolute number of the user interface (the absolute number can be checked using the **display users** command). When the configuration terminal is offline, X displays offline. ● file: Diagnosis information is exported to files. ● server: Diagnosis information is exported to a log server.
Total 3, 3 printed	Total number of created diagnosis objects and count of displayed objects.

Related Topics

21.9.7 trace object

21.9.4 reset trace instance

Function

The **reset trace instance** command clears all the diagnosis instances on a device.

Format

reset trace instance

 Copyright © Huawei Technologies Co., Ltd.

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

After service diagnosis is enabled and a diagnosis object is created on a device, the device creates a diagnosis instance when a user matching the attributes of the diagnosis object gets online. If the device diagnoses services of multiple users, it creates a diagnosis instance for each user, which occupies a large amount of system resources. Therefore, the device needs to delete the diagnosis instance of a user when the user goes online successfully or fails to go online. Additionally, the device provides an aging mechanism for service diagnosis. When the aging time is reached, the device automatically deletes diagnosis instances to reclaim resources.

In addition to the preceding two methods for automatically clearing diagnosis instances, you can run the **reset trace instance** command to clear all the diagnosis instances.

NOTICE

After all the diagnosis instances are cleared using the **reset trace instance** command, properly running diagnosis instances are also deleted. Exercise caution when you run the **reset trace instance** command.

Example

Clear all diagnosis instances on the device.

```
<Huawei> system-view
[Huawei] reset trace instance
```

Related Topics

21.9.2 display trace instance

21.9.5 save trace information

Function

The **save trace information** command saves diagnosis information in the buffer area as a file.

 Copyright © Huawei Technologies Co., Ltd.

Format

save trace information

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After you specify the parameter **file** *file-name* in the **trace object** command to save diagnosis information as files to the default root directory on the storage device, the system saves diagnosis information in the buffer area until the buffer is full. To prevent data loss, the system automatically saves diagnosis information in the buffer area as the file *file-name*. Before the buffer becomes full, to view real-time diagnosis information, run the **save trace information** command to save diagnosis information in the buffer area as a file.

Prerequisites

The device has been configured to export diagnosis information as a file using the **trace object** command.

Example

Save diagnosis information as a file.

```
<Huawei> system-view
[Huawei] save trace information
```

Related Topics

21.9.7 trace object

21.9.6 trace enable

Function

The **trace enable** command enables service diagnosis.

The **undo trace enable** command disables service diagnosis.

By default, service diagnosis is disabled.

Copyright © Huawei Technologies Co., Ltd.

Format

trace enable [**brief**]

undo trace enable

Parameters

Parameter	Description	Value
brief	Configures the device to output brief service diagnosis information.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

It is difficult to locate problems during user access based on debugging information on existing networks because multiple users may get online or offline simultaneously and debugging information about a specified user cannot be displayed. Service diagnosis provided by the router allows maintenance personnel to customize attributes and create diagnosis objects to diagnose information about services of specified users. To enable service diagnosis, run the **trace enable** command.

Service diagnosis information can be displayed in two methods:

- The **trace enable brief** command configures the device to output brief service diagnosis information.
- The **trace enable** command configures the device to output detailed service diagnosis information.

Follow-up Procedure

After service diagnosis is enabled, run the **trace object** command to create a diagnosis object. After an ID is generated for the diagnosis object, the system starts diagnosis services.

Precautions

Service diagnosis affects system performance. Therefore, enable service diagnosis only when fault locating is required. After locating faults, immediately run the **undo trace enable** command to disable service diagnosis.

 Copyright © Huawei Technologies Co., Ltd.

The **trace enable** command is not recorded in the configuration file. Therefore, run the **trace enable** command again after the device restarts to make service diagnosis take effect.

Example

Enable the service diagnosis function and configure the device to output brief service diagnosis information.

```
<Huawei> system-view
[Huawei] trace enable brief
```

Related Topics

21.9.7 trace object

21.9.7 trace object

Function

The **trace object** command creates a diagnosis object.

The **undo trace object** command deletes a diagnosis object.

By default, no diagnosis object is created. If you do not specify the direction at which information is exported, the default direction is the CLI.

Format

trace object { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** | **pppoe** | **pppolns** } } * [**slot** *slot-id*] [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }]

trace object calling-number [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }] [**slot** *slot-id*] [| **include**] **calling-number-content** *text*

trace object tunnel-id *tunnel-id* [**slot** *slot-id*] [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }]

undo trace object { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** | **pppoe** | **pppolns** } } * [**slot** *slot-id*] [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }]

undo trace object { *service-object-id* | **all** }

undo trace object { **calling-number** [| **include**] **calling-number-content** *text* | **tunnel-id** *tunnel-id* }

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
mac-address *mac-address*	Creates a diagnosis object based on the MAC address.	The value is in the format of H-H-H, in which H is a hexadecimal number of 4 digits.
ip-address *ip-address*	Creates a diagnosis object based on the IP address.	The value is in dotted decimal notation.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces.
interface *interface-type interface-number*	Creates a diagnosis object based on the interface.	-
user-vlan *user-vlan-id*	Creates a diagnosis object based on the user VLAN.	The value is an integer that ranges from 1 to 4094.
qinq-vlan *qinq-vlan-id*	Creates a diagnosis object based on the QinQ VLAN ID.	The value is an integer that ranges from 1 to 4094.
user-name *user-name*	Creates a diagnosis object based on the user name.	The value is a string of 1 to 253 case-insensitive characters without spaces.
access-mode	Creates a diagnosis object based on the access mode.	-
dot1x	Creates a diagnosis object based on the dot1x access mode.	-
mac-authen	Creates a diagnosis object based on the mac-authen access mode.	-
portal	Creates a diagnosis object based on the portal access mode.	-
wlan	Creates a diagnosis object based on the wlan access mode.	-
pppoe	Creates a diagnosis object based on the pppoe access mode.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
pppolns	Creates a diagnosis object based on the pppolns access mode.	-
| **include**	Whether fuzzy matching is supported.	-
calling-number-content *text*	Creates a diagnosis object based on the calling number.	The value varies according to different devices.
tunnel-id *tunnel-id*	Creates a diagnosis object based on the tunnel ID.	The value varies according to different devices.
slot *slot-id*	Specifies the slot ID of an interface card.	The value varies according to different devices.
output	Specifies the direction in which the device exports diagnosis information.	-
command-line	Exports diagnosis information to the CLI.	-
file *file-name*	Exports diagnosis information as a file. **NOTE** It is recommended that you export the diagnosis information to a specified file.	The value of *file-name* is a string of 1 to 63 case-insensitive characters without spaces.
syslog-server *syslog-server-ip*	Exports diagnosis information to a log server.	*syslog-server-ip* specifies the IP address of the log server, in dotted decimal notation.
service-object-id	Specifies the ID of a diagnosis object to be deleted. **NOTE** Diagnosis object IDs are generated based on sequence in which the diagnosis objects are created. The ID starts from 0. To view all created diagnosis objects, run the **display trace object** command.	The value is an integer that ranges from 0 to 3.
all	Deletes all diagnosis objects.	-

Copyright © Huawei Technologies Co., Ltd.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

When locating faults of DHCP, L2TP, AAA, or NAC service during user access, maintenance personnel can create diagnosis objects to trace services and locate the faults.

Users with different services have different attributes. Create diagnosis objects for different services based on different attributes.

- DHCP service: based on the MAC address.
- L2TP service: based on the calling number and tunnel ID.
- AAA and NAC services: based on the MAC address, IP address, user name, user VLAN ID, access mode, or interface number.

NOTE

To ensure that you can diagnose the entire DHCP service process, create a diagnosis object based on the MAC address. You can run the **trace object mac-address** *mac-address* [**output** { **command-line** | **file** *file-name* | **syslog-server** *syslog-server-ip* }] command to create a diagnosis object for the DHCP service.

Service diagnosis supports only common AAA users.

Prerequisites

Service diagnosis has been enabled using the **trace enable** command.

Precautions

The diagnosis output file cannot exceeds 1 MB. The excessive diagnosis information is not recorded.

You can run the **undo trace object** command to delete diagnosis objects in any of the following modes:

- Delete diagnosis objects based on the object attributes. Run the **undo trace object** { **mac-address** *mac-address* | **ip-address** *ip-address* [**vpn-instance** *vpn-instance-name*] | **interface** *interface-type interface-number* | **user-vlan** *user-vlan-id* [**qinq-vlan** *qinq-vlan-id*] | **user-name** *user-name* | **access-mode** { **dot1x** | **mac-authen** | **portal** | **wlan** | **pppoe** | **pppolns** } } * or **undo trace object** { **calling-number** [| **include**] **calling-number-content** *text* | **tunnel-id** *tunnel-id* } command. For example, diagnosis objects 1 (10.10.10.1) and 2 (10.10.10.1+0025-9efb-be78) have been created. To delete diagnosis objects based on the IP address, run the **undo trace object ip-address 10.10.10.1** command. Diagnosis objects 1 and 2 are deleted.
- Delete diagnosis objects based on the object ID. Run the **undo trace object** *service-object-id* command to delete a specified diagnosis object. You can view the object ID using the **display trace object** command

 Copyright © Huawei Technologies Co., Ltd.

- Delete all diagnosis objects using the **undo trace object all** command.

Example

Create a diagnosis instance on the interface with the IP address of 10.10.10.1.

```
<Huawei> system-view
[Huawei] trace object ip-address 10.10.10.1
```

Related Topics

21.9.3 display trace object
21.9.6 trace enable

21.9.8 trace syslog source

Function

The **trace syslog source** command sets the source interface from which the device exports diagnosis information to a log server.

The **undo trace syslog source** command cancels the configuration of the source interface from which the device exports diagnosis information to a log server.

By default, no interface is specified to export diagnosis information to the log server.

Format

trace syslog source *interface-type interface-number*

undo trace syslog source

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of an interface.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage scenario

After you specify an interface for exporting diagnosis information to a log server, the system specifies the IP address of this interface as the source IP address of

 Copyright © Huawei Technologies Co., Ltd.

service diagnosis packets. In this way, the log server can identify the source of diagnosis information.

Prerequisites

The device has been configured to export diagnosis information to a log server using the **trace object** command.

Precautions

The **trace syslog source** command is not recorded in the configuration file. After the device restarts, the configured source interface for exporting diagnosis information is invalid. To set the source interface, run the **trace syslog source** command again.

Example

Set GE1/0/0 as the source interface for exporting diagnosis information to the log server.

```
<Huawei> system-view
[Huawei] trace syslog source gigabitethernet 1/0/0
```

Related Topics

21.9.7 trace object

21.10 Mirroring Configuration Commands

NOTE

The device supports mirroring. The mirroring function is used for network detection and fault management, and may involve personal communication information. Huawei cannot collect or store user communication information without permission. It is recommended that relevant functions used to collect or store user communication information be enabled under applicable laws and regulations. During user communication information usage and storage, measures must be taken to protect user communication information.

21.10.1 display mirror-port

Function

The **display mirror-port** command displays the port mirroring configuration.

Format

display mirror-port

Parameters

None

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Display the port mirroring configuration.

```
<Huawei> display mirror-port
 ------------------------------------------------------------------------------
  Mirror-port              Direction  Observe-dest
 ------------------------------------------------------------------------------
 1 Ethernet2/0/0            Inbound    Ethernet2/0/1
 2 GigabitEthernet1/0/0     Inbound    DIP:2.1.1.2 SIP:1.1.1.2 DSCP:0
 ------------------------------------------------------------------------------
```

Table 21-64 Description of the display mirror-port command output

Item	Description
Mirror-port	Mirrored ports. You can run the **21.10.3 mirror (interface view)** command to set this parameter.
Direction	Direction of packets on a mirrored port. The value can be: ● both: indicates incoming and outgoing packets. ● inbound: indicates incoming packets. ● outbound: indicates outgoing packets. You can run the **21.10.3 mirror (interface view)** command to set this parameter.
Observe-dest	Local observing port. You can run the **21.10.5 observe-port** command to set local observing port.

Related Topics

21.10.3 mirror (interface view)

21.10.5 observe-port

Copyright © Huawei Technologies Co., Ltd.

21.10.2 display observe-port

Function

The **display observe-port** command displays the observing port configuration.

Format

display observe-port

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

None

Example

Display the observing port configuration.

```
<Huawei> display observe-port
  ----------------------------------------------------------------------
  Index     : 1
  Interface: Ethernet1/0/1
  Used      : 1
  ----------------------------------------------------------------------
```

Table 21-65 Description of the display observe-port command output

Item	Description
Index	Index of the observing port.
Interface	Observing port. You can run the **21.10.5 observe-port** command to set this parameter.
Used	Number of times that the observing port is used.

Related Topics

21.10.5 observe-port

 Copyright © Huawei Technologies Co., Ltd.

21.10.3 mirror (interface view)

Function

The **mirror** command enables port mirroring.

The **undo mirror** command disables port mirroring.

By default, port mirroring is disabled.

Format

mirror to observe-port { **both** | **inbound** | **outbound** } [**exclude-link-head**]

undo mirror { **both** | **inbound** | **outbound** }

Parameters

Parameter	Description	Value
observe-port	Indicates local port mirroring.	-
both	Mirrors both the incoming and outgoing packets on a port.	-
inbound	Mirrors only incoming packets on a port.	-
outbound	Mirrors only outgoing packets on a port.	-
exclude-link-head	Removes non-Ethernet link layer information before mirroring packets on a port.	-

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The device supports mirroring incoming packets, outgoing packets, and both incoming and outgoing packets.

The device may fail to analyze some IP packets that carry non-Ethernet link layer information, such as IPOA packets during port mirroring. In this case, specify the

 Copyright © Huawei Technologies Co., Ltd.

exclude-link-layer parameter to remove non-Ethernet link layer information from the packets, so that the device can correctly analyze the packets.

Prerequisites

In local port mirroring, the local observing port has been configured using the **21.10.5 observe-port** command.

Precautions

- An observing port or server can be applied to port mirroring and traffic mirroring simultaneously. However, you cannot identify the source of mirrored packets by using the **5.1.4 display interface** command.
- Port mirroring does not affect system security but affects system performance. To ensure system performance, disable port mirroring when you do not need to monitor traffic.
- To configure mirroring on a port again, run the **undo mirror** { **both** | **inbound** | **outbound** } command to delete the existing configuration first.
- To ensure that all mirrored packets are transmitted to the observing port, configure the same link type and bandwidth for the mirrored and observing ports.

Example

Mirror all incoming packets on Eth2/0/0 to the observing port.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mirror to observe-port inbound
```

Related Topics

21.10.5 observe-port

21.10.4 mirror (traffic behavior view)

Function

The **mirror** command used in the traffic behavior view enables traffic mirroring to mirror packets matching certain rules to the observing port.

The **undo mirror** command disables traffic mirroring.

By default, traffic mirroring is disabled.

Format

mirror to observe-port

undo mirror

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
observe-port	Indicates the observing port used for traffic mirroring.	-

Views

Traffic behavior view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a traffic policy containing a traffic behavior is configured on a port, the device mirrors the packets that match the traffic policy to the local observing port or remote observing server. The local observing port must be a LAN-side port.

Prerequisites

- A traffic behavior has been created using the **20.1.44 traffic behavior** command.
- In local traffic mirroring, the local observing port has been configured using the **21.10.5 observe-port** command.

Follow-up Procedure

Create a traffic classifier and a traffic policy, bind the traffic classifier and traffic behavior to the traffic policy, and apply the traffic policy to the mirrored port.

Precautions

- An observing port or server can be applied to port mirroring and traffic mirroring simultaneously. However, you cannot identify the source of mirrored packets by using the **5.1.4 display interface** command.
- Traffic mirroring does not affect system security but affects system performance. To ensure system performance, disable traffic mirroring when you do not need to monitor traffic.

Example

Mirror the packets matching certain rules to the observing port.

```
<Huawei> system-view
[Huawei] traffic behavior tb1
[Huawei-behavior-tb1] mirror to observe-port
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

20.1.44 traffic behavior
21.10.5 observe-port

21.10.5 observe-port

Function

The **observe-port** command configures a local observing port.

The **undo observe-port** command deletes a local observing port.

By default, no local observing port is configured.

NOTE

In PPPoEoA and IPoEoA scenarios, only WAN-side interfaces can be used as observing interfaces.

Format

observe-port interface *interface-type interface-number*

undo observe-port

Parameters

Parameter	Description	Value
interface-type interface-number	Specifies the type and number of the observing port. • *interface-type* specifies the type of the port. • *interface-number* specifies the number of the port.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If the monitoring device and monitored device are connected to the same router, run the **observe-port** command to configure a local observing port to monitor

 Copyright © Huawei Technologies Co., Ltd.

ports on the monitored device or traffic passing through the ports on the monitored device.

Precautions

- Do not configure other functions on an observing port; otherwise, the mirroring function is affected.
- If an observing port configured with the mirroring function needs to be deleted, delete the mirrored port first.
- The management port cannot be configured as a local observing port.
- Only LAN-side and WAN-side ports can be configured as local observing ports.

Example

Configure Eth2/0/0 as the local observing port.

```
<Huawei> system-view
[Huawei] observe-port interface ethernet 2/0/0
```

Related Topics

21.10.2 display observe-port

21.11 Packet Capture Configuration Command

NOTE

Based on your requirements to detect failures in telecom transmission, this feature may collect or store some communication information about specific customers. Huawei cannot offer services to collect or store this information unilaterally. Before enabling the function, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.

21.11.1 capture-packet

Function

The **capture-packet** command captures service packets matching specified rules, displays captured packet information on the terminal, or saves the captured packets on the local device.

By default, the captured packets on the device are not configured.

Format

capture-packet { **interface** *interface-type interface-number* | **dsp** } [**acl** *acl-number*] **destination** { **terminal** | **file** *file-name* } * [**car cir** *car-value* | **time-out** *time* | **packet-num** *number* | **packet-len** *length* }] *

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Captures packets on a specified interface. ● *interface-type* specifies the interface type. ● *interface-number* specifies the interface number.	-
dsp	Specifies the captured DSP voice packets.	-
acl	Configures an ACL.	-
acl-number	Captures packets matching a specified ACL.	The value is an integer that ranges from 2000 to 4999.
destination	Indicates the destination to which captured packet information is sent.	-
terminal	Displays captured packet information on a terminal.	-
file *file-name*	Saves captured packet information to a file. *file-name* is in the format of [drive][file-name] (such as flash:/test.cap), in which [file-name] is in the format of *.cap.	The value is a string of 5 to 63 characters without spaces. When quotation marks are used around the string, spaces are allowed in the string.
car cir *car-value*	Specifies the rate at which packets are captured.	The value is an integer that ranges from 1 to 256, in pps. The default value is 64 pps.
time-out *time*	Specifies the timeout period for capturing packets. The system stops capturing packets after the specified timeout period expires.	The value is an integer that ranges from 1 to 300, in seconds. By default, the timeout period is 60s.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
packet-num *number*	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	The value is an integer that ranges from 1 to 2000. The default value is 100.
packet-len *length*	Specifies the length of captured packets that can be displayed on the terminal or stored on the storage medium.	The value is an integer that ranges from 20 to 64, in bytes. The default value is 64 bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

If an error occurs in service traffic forwarding (for example, the traffic status does not match the traffic model), it is recommended that you configure the device to capture service packets for analysis so that the device can quickly identify invalid packets. This function ensures correct data transmission on the network.

Precautions

When packets are received by a LAN port and sent to a LAN port, the packets cannot be captured.

When the 8FE1GE or 24GE board is installed on an AR1220, Layer 2 packets cannot be captured, and Layer 3 packets can be captured. When the 8FE1GE or 24GE board is installed on a model except AR1220 and the inbound interface is on 8FE1GE or 24GE, both Layer 2 and Layer 3 packets are forwarded by LSW, and the packets cannot be mirrored. When the inbound interface is on another LAN board, Layer 2 packets cannot be mirrored and Layer 3 packets can be mirrored.

The device can capture incoming and outgoing packets.

Before using the **capture-packet** command again, wait until the last command execution is complete.

The system limits the rate of captured packets. If the rate of packets exceeds the limit, some packets may be discarded.

You can set the timeout period specified by *time* and the number of packets to be captured specified by *number* for a capture instance. If the timeout period expires

 Copyright © Huawei Technologies Co., Ltd.

or the specified number of packets are captured, the system stops capturing packets.

The **capture-packet** and **voice-monitor** commands cannot be configured simultaneously.

Example

Capture packets on the interface GE1/0/0 and display them on the terminal.

```
<Huawei> system-view
[Huawei] capture-packet interface gigabitethernet 1/0/0 destination terminal time-out 10
[Huawei]
  Packet: 1
  ---------------------------------------------------------
  ff ff ff ff ff ff 00 e0 fc 01 00 08 08 06 00 01
  08 00 06 04 00 01 00 e0 fc 01 00 08 02 01 01 03
  00 00 00 00 00 00 0a 01 01 01 00 00 00 00 00 00
  00 00 00 00 00 00 00 00 00 00 00 00
  ---------------------------------------------------------

  ------------------capture report-----------------------
  file: NULL
  interface: GigabitEthernet1/0/0
  acl: -
  car: 64pps timeout: 10s
  packets: 100 (expected) 1 (actual)
  length: 48 (expected)
  ---------------------------------------------------------
```

Table 21-66 Description of the capture-packet command output

Item	Description
file	Local path that stores captured packets. NULL marking for empty.
interface	Interface where packets are captured.
acl	ACL number.
car	Rate of captured packets.
timeout	Timeout interval of packet capture. The system stops capturing packets after the specified time interval.
packets	Expected number and actual number of captured packets.
length	Length of captured packets.

21.11.2 display voice-monitor

Function

The **display voice-monitor** command displays information about voice packets passing the device.

 Copyright © Huawei Technologies Co., Ltd.

Format

display voice-monitor

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To view information about voice packets passing the device, run the **display voice-monitor** command.

Prerequisites

The device is configured to capture voice packets using the **voice-monitor** command.

Example

Display information about voice packets passing the device.

```
<Huawei> display voice-monitor
-----------------------------------------------------------------------------
TelNo                IPAddr        Port      Direction RuleIndex
-----------------------------------------------------------------------------
20000                 10.0.0.1      51201     Inbound   0
10000                 10.0.0.2      61945     Outbound  1
```

Table 21-67 Description of the display voice-monitor command output

Item	Description
TelNo	Phone number in the captured voice packets.
IPAddr	IP address of voice packets.
Port	Port number of voice packets.
Direction	Direction of voice packets: ● Inbound: incoming voice packets. ● Outbound: outgoing voice packets.
RuleIndex	ID of the resource occupied by voice packets.

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.11.3 voice-monitor

21.11.3 voice-monitor

Function

The **voice-monitor** command configures the device to capture voice packets passing the device and save them.

By default, the device is not configured to capture voice packets passing the device.

Format

voice-monitor interface *interface-type interface-number* **destination file** *file-name* * **telno** *telephone-number* &<1-8> [**car cir** *cir-value* | **time-out** *time* | **packet-num** *number*] | **packet-len** *length* } *

Parameters

Parameter	Description	Value
interface *interface-type interface-number*	Captures packets on a specified interface. • *interface-type* specifies the interface type. • *interface-number* specifies the interface number.	-
destination	Specifies the destination where captured packets are saved.	-
file *file-name*	Specifies the name of the file for storing captured packets.	The value is a string of 5 to 63 characters without spaces. The value must end with *.cap.
telno *telephone-number* &<1-8>	Specifies the phone number in captured packets.	The value is a string of 1 to 24 numerals. Each numeral ranges from 0 to 9. A maximum of 8 telephone numbers can be entered.
car cir *cir-value*	Specifies the rate at which packets are captured.	The value is an integer that ranges from 1 to 256, in pps. The default rate is 64 pps.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
time-out *time*	Specifies the timeout interval of packet capture. The system stops capturing packets after the specified timeout interval.	The value is an integer that ranges from 1 to 300, in seconds. The default timeout interval is 60s.
packet-num *number*	Specifies the number of packets to be captured. The system stops capturing packets after the specified number of packets are captured.	The value is an integer that ranges from 1 to 2000. The default value is 100.
packet-len *length*	Specifies the length of captured packets that can be displayed on the terminal or stored on the storage medium.	The value is an integer that ranges from 20 to 64, in bytes. The default value is 64 bytes.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When unexpected voice traffic occurs, for example, the traffic status does not match the traffic model, run the **voice-monitor** command to configure the device to capture voice packets for analysis. Then the device can process invalid packets in a timely manner, and data services can be correctly transmitted and voice communication quality is ensured.

When configuring packet capture, you can set parameters according to the number of packets on an interface. If there are many packets on the interface, set a small value of *time* and a large value of *number*. If there are less packets on an interface, set a large value of *time* and a small value of *number*.

Precautions

- The packet capture configuration is not saved in the configuration file, and becomes invalid when packet capture is complete.
- Before using the **voice-monitor** command again, wait until the last command execution is complete.
- The system limits the rate of captured packets. If the rate of packets exceeds the limit, some packets may be discarded.

 Copyright © Huawei Technologies Co., Ltd.

- You can set the timeout interval of packet capture and number of packets to be captured. The system stops capturing packets after the timeout interval or the number of packets to be captured is reached.
- The **voice-monitor** and **capture-packet** commands cannot be configured simultaneously.

Example

Configure the device to capture voice packets on GE1/0/0 and save them in the **capture.cap** file.

```
<Huawei> system-view
[Huawei] voice-monitor interface gigabitethernet 1/0/0 destination file capture.cap telno 10000 20000
Warning: The packet capture function has been enabled and packets are stored in flash:/capture.cap .
[Huawei]
  ------------------capture report-----------------------
  file: flash:/capture.cap
  interface: GigabitEthernet1/0/0
  acl: -
  car: 64pps timeout: 60s
  packets: 100 (expected) 0 (actual)
  length: whole (expected)
  -------------------------------------------------------
```

Table 21-68 Description of the voice-monitor command output

Item	Description
file	File name and path for storing captured packets.
interface	Interface where packets are captured.
acl	ACL number.
car	Rate at which packets are captured.
timeout	Timeout interval of packet capture. The system stops capturing packets after the specified timeout interval.
packets	Expected and actual numbers of captured packets.
length	Length of captured packets.

21.12 NetStream Configuration Commands

NOTE

- The NetStream function conforms to IETF RFC3954. For security risks, see IETF RFC3954. This function involves analyzing the communications information of terminal customers. Before enabling the function, ensure that it is performed within the boundaries permitted by applicable laws and regulations. Effective measures must be taken to ensure that information is securely protected.
- NetStream supports sampling of IPv4 unicast, multicast packets, and IPv4 packets encapsulated with MPLS labels.

 Copyright © Huawei Technologies Co., Ltd.

21.12.1 collect application

Function

The **collect application** command configures the application name or description of traffic to be added to the flexible flow statistics exported to the NSC.

The **undo collect application** command restores the default configuration.

By default, the flexible flow statistics that are exported to the NSC do not contain the application name and description.

Format

collect application { **name** | **description** }

undo collect application { **name** | **description** }

Parameters

Parameter	Description	Value
name	Specifies the traffic application name to be added to the flexible flow statistics exported to the NSC.	-
description	Specifies the traffic description to be added to the flexible flow statistics exported to the NSC.	-

Views

Flexible flow template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain more information from flexible flow statistics, you can specify that the statistics contain the application name or description of traffic and set the application names and description according to your needs.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **engine enable** command has been run to enable deep security defense, and the **sa application-statistic enable** command has been run to enable SA statistics collection on a NetStream interface.

After the deep security function is enabled, if SAC is used for the first time, run the **update restore sdb-default** command to manually load the SA signature file.

Example

Specify the traffic application name to be added to the flexible flow statistics exported to the NSC.

```
<Huawei> system-view
[Huawei] ip netstream record huawei_record
[Huawei-record-huawei_record] collect application name
```

21.12.2 collect category name

Function

The **collect category name** command configures the application category and subcategory of traffic to be added to the flexible flow statistics exported to the NSC.

The **undo collect category name** command restores the default configuration.

By default, the flexible flow statistics that are exported to the NSC do not contain the application category and subcategory.

Format

collect category name

undo collect category name

Parameters

None

Views

Flexible flow template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain more information from flexible flow statistics, you can specify that the statistics contain the application name or description of traffic and set the application names and description according to your needs.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

The **engine enable** command has been run to enable deep security defense, and the **sa application-statistic enable** command has been run to enable SA statistics collection on a NetStream interface.

After the deep security function is enabled, if SAC is used for the first time, run the **update restore sdb-default** command to manually load the SA signature file.

Example

Specify that the flexible flow statistics that are exported to the NSC contain the application category and subcategory of traffic.

```
<Huawei> system-view
[Huawei] ip netstream record huawei_record
[Huawei-record-huawei_record] collect category name
```

21.12.3 collect counter

Function

The **collect counter** command allows the flexible flow statistics exported to the NetStream Collector (NSC) to contain the number of bytes and packets.

The **undo collect counter** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the number of bytes or packets.

Format

collect counter { **bytes** | **packets** }

undo collect counter { **bytes** | **packets** }

Parameters

Parameter	Description	Value
bytes	Indicates that the flexible flow statistics exported to NSC contain the number of bytes.	-
packets	Indicates that the flexible flow statistics exported to NSC contain the number of packets.	-

Views

Flexible flow statistics template view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether flexible flow statistics contain the number of bytes and packets.

Prerequisites

A flexible flow statistics template has been created using the **ip netstream record** command.

Precaution

If a flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

Example

Configure the flexible flow statistics template **record1** to export the flexible flow statistics containing the number of packets to the NSC.

```
<Huawei> system-view
[Huawei] ip netstream record record1
[Huawei-record-record1] collect counter packets
```

Related Topics

21.12.29 ip netstream record

21.12.4 collect interface

Function

The **collect interface** command allows the flexible flow statistics exported to the NSC to contain the indexes of inbound and outbound interfaces.

The **undo collect interface** command restores the default setting.

By default, the flexible flow statistics exported to the NSC do not contain the index of inbound or outbound interface.

Format

collect interface { **input** | **output** }

undo collect interface { **input** | **output** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
input	Indicates that the flexible flow statistics exported to the NSC contain the index of inbound interface.	-
output	Indicates that the flexible flow statistics exported to the NSC contain the index of outbound interface.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To obtain richer flow statistics, configure whether flexible flow statistics exported to the NSC contain indexes of inbound and outbound interfaces.

Prerequisites

A flexible flow statistics template has been created using the **ip netstream record** command.

Precaution

If a flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

Example

Configure the flexible flow statistics template **record1** to export the flexible flow statistics containing the inbound interface index to the NSC.

```
<Huawei> system-view
[Huawei] ip netstream record record1
[Huawei-record-record1] collect interface input
```

Related Topics

21.12.29 ip netstream record

 Copyright © Huawei Technologies Co., Ltd.

21.12.5 display ip netstream

Function

The **display ip netstream** command displays the NetStream configurations.

Format

display ip netstream { **all** | **global** }

Parameters

Parameter	Description	Value
all	Displays all the NetStream configurations, including: ● NetStream configurations in the system view ● NetStream configurations in the aggregation view ● NetStream configurations in the flexible flow statistics view ● NetStream configurations in the interface view	-
global	Displays the NetStream configurations in a specified view, for example: ● NetStream configurations in the system view ● NetStream configurations in the aggregation view ● NetStream configurations in the flexible flow statistics view	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Display NetStream configurations in the system view and aggregation view.

```
<Huawei> display ip netstream global
ip netstream export host 10.0.0.2 255 vpn-instance vpna
ip netstream aggregation destination-prefix
 enable
 export version 9
 ip netstream export host 10.5.5.5 3 vpn-instance vpna
```

Table 21-69 Description of the display ip netstream global command output

Item	Description
ip netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The field *ip-address* indicates the destination address of the exported packets, and *port-number* is the UDP port. The field *vpn-instance-name* indicates the VPN instance to which the destination address belongs. This field is displayed only when the **ip netstream export host** command has been executed in the system view.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
ip netstream aggregation destination-prefix	Destination-prefix aggregation method. This field is displayed only when the **ip netstream aggregation** command has been executed to set the aggregation method. Currently, the following aggregation modes are supported: ● as: AS aggregation ● as-tos: AS-ToS aggregation ● destination-prefix: destination-prefix aggregation ● destination-prefix-tos: destination-prefix-ToS aggregation ● prefix: prefix aggregation ● prefix-tos: prefix-ToS aggregation ● protocol-port: protocol-port aggregation ● protocol-port-tos: protocol-port-ToS aggregation ● source-prefix: source-prefix aggregation ● source-prefix-tos: source-prefix-ToS aggregation
enable	The destination-prefix aggregation mode is enabled. This field is displayed only when the **enable** command has been executed in the aggregation view.
export version *version*	The field *version* indicates the version format of the exported packets carrying aggregation flow statistics. If the version retains the default setting, this field is not displayed. This field is displayed only when the **export version** command has been executed.
ip netstream export host *ip-address port-number* vpn-instance *vpn-instance-name*	The field *ip-address* indicates the destination address of the exported packets, and *port-number* is the UDP port. The field *vpn-instance-name* indicates the VPN instance to which the destination address belongs. This field is displayed only when the **ip netstream export host** command has been executed in the NetStream aggregation view.

Related Topics

21.12.14 ip netstream aggregation
21.12.21 ip netstream export host
21.12.26 ip netstream export version

 Copyright © Huawei Technologies Co., Ltd.

21.12.11 enable

21.12.6 display ip netstream cache

Function

The **display ip netstream cache** command displays flow information in the NetStream cache.

Format

display ip netstream cache [**classify** [**source-ip** *source-ip* | **destination-ip** *destination-ip* | **source-port** *source-port* | **destination-port** *destination-port* | **protocol** *protocol-id* | **start-time** *start-time* | **end-time** *end-time*] * | [**verbose**] | **top** [*top-value*] [**sort-by** { **bytes** | **packets** }] | **verbose**]

Parameters

Parameter	Description	Value
classify	Searches for the saved flow entries.	-
source-ip *source-ip*	Specifies the source IP address used for search.	The value is in dotted decimal notation.
destination-ip *destination-ip*	Specifies the destination IP address used for search.	The value is in dotted decimal notation.
source-port *source-port*	Specifies the source port number used for search.	The value is an integer that ranges from 0 to 65535.
destination-port *destination-port*	Specifies the destination port number used for search.	The value is an integer that ranges from 0 to 65535.
protocol *protocol-id*	Specifies the protocol number used for search.	The value is an integer that ranges from 0 to 65535.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
start-time *start-time*	Specifies the start time used for search.	The value is in hh:mm:ss YYYY/MM/DD formats. The time is in 24-hour format and displayed as hh:mm:ss. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59. The date is in YYYY/MM/DD format. YYYY specifies the year, MM specifies the month, and DD specifies the day. The value is an integer that ranges from 1970-01-01 to 2099-12-31.
end-time *end-time*	Specifies the end time used for search.	The value is in hh:mm:ss YYYY/MM/DD formats. The time is in 24-hour format and displayed as hh:mm:ss. hh indicates the hour that is an integer ranging from 0 to 23. mm indicates the minute that is an integer ranging from 0 to 59. ss indicates the second that is an integer ranging from 0 to 59. The date is in YYYY/MM/DD format. YYYY specifies the year, MM specifies the month, and DD specifies the day. The value is an integer that ranges from 1970-01-01 to 2099-12-31.
top	Displays the flows in the descending order of flow volume. By default, flows are displayed in the descending order of the number of packets.	-
top-value	Specifies the number of flows that need to be displayed in a certain order.	The value is an integer that ranges from 1 to 200. The default value is 10.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sort-by	Specifies the order in which flows are displayed.	-
bytes	Indicates that the flows are displayed in the order of bytes.	-
packets	Indicates that the flows are displayed in the order of packets.	-
verbose	Displays detailed information about flows in the NetStream cache.	-

Views

All views

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After the NetStream sampling function is enabled, run the **display ip netstream cache** command to view information about flows in NetStream cache.

To view the cached flows in the order of flow volume, run the **display ip netstream cache top** command. The **display ip netstream cache** command can display the flows in the descending order of the number of **bytes** or **packets**.

To search for the saved flow entries based on the seven attributes (including the source IP address, destination IP address, source port number, destination port number, protocol number, start time, and end time), run the **display ip netstream cache classify** command.

NOTE

Only AR2204E, AR2240, AR2240C, and AR3200 series routers support flow entry search based on the seven attributes.

Precaution

This command cannot display the aged flows, so you must run this command before the flows age in the cache.

The flow table information is based on seven-tuple to retrieve sequential dependent relationships. For example, after retrieval based on the destination IP

 Copyright © Huawei Technologies Co., Ltd.

address, the source port number, destination port number, protocol number, and start or end time can also be retrieved, but the source IP address cannot be retrieved.

When the number of data flows on the network exceeds the upper limit, an accelerated aging mechanism can be used so that statistics about all data flows can be collected.

- When the number of remaining flow tables is between 25% and 30% of the upper limit, the actual inactive aging period is two thirds of the configured inactive aging period.
- When the number of remaining flow tables is greater than 5% of the upper limit and less than or equal to 25% of the upper limit, the actual inactive aging period is half of the configured inactive aging period.
- When the number of remaining flow tables is less than or equal to 5% of the upper limit, the flow tables are aged after the aging timer expires.

Example

Display information about flows in the NetStream cache.

```
<Huawei> display ip netstream cache
 IP netstream cache information :
   Active stream timeout ( in minutes )   : 30
   Inactive stream timeout ( in seconds ) : 30
   IP active stream number                : 2
   IP inactive stream number              : 0
   Last statistics reset time             : Never

IP packet size distribution (41100 total packets) :
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448
 .000 .000 .148 .000 .850 .000 .000 .000 .000 .000 .000 .000 .000 .000

  480  512  544  576 1024 1536 2048 2506 3072 3584 4096 4608 >4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

 Protocol          Total   Packets    Stream    Packets  Active(sec)  Idle(sec)
                 Streams      /sec      /sec    /stream    /stream     /stream
-----------------------------------------------------------------------------------
 IP-other              1       928         0       6500          7           0
 UDP-other             1       300         0      35100        117           0

Type  DstIP(Port)            SrcIP(Port)           Pro  ToS  Packets      If(Direc)
-----------------------------------------------------------------------------------
IP    192.168.1.2(80)          192.168.2.2(0)          17   0    353
GigabitEthernet0/0/0(I)
IP    192.168.2.2(0)           192.168.1.2(0)          114  68   70     GigabitEthernet0/0/0(O)
```

Table 21-70 Description of the display ip NetStream cache command output

Item	Description
IP netstream cache information	Information about the NetStream cache.
Active stream timeout (in minutes)	Active aging time, in minutes.
Inactive stream timeout (in seconds)	Inactive aging time, in seconds.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
IP active stream number	Number of active IP flows in the NetStream cache.
IP inactive stream number	Number of inactive IP flows in the NetStream cache.
Last statistics reset time	Last time the statistics are cleared. This time does not change with the system time. This field is displayed only when the **reset ip netstream statistic** command is executed; otherwise, the message "Last statistics reset time : Never" is displayed.
IP packet size distribution (41100 total packets)	Distribution of IP packets based on the packet size. Bracketed information indicates the total number of IP packets. The distribution value is displayed as a three-bit decimal based on the ratio to the total number of IP packets. For example, ".027" indicates that the IP packets in the NetStream cache are 0.027 of the total number of IP packets.
1-32 64 96 128 160 192 224 256 288 320 352 384 416 448 480 512 544 576 1024 1536 2048 2506 3072 3584 4096 4608 >4608	Interval between IP packet size. The packet length does not contain the link layer header. When the packet length does not exceed 576 bytes, the packet length increases by 32 bytes. For example, "1-32" maps the number of packets whose lengths range from 1 byte to 32 bytes, and "64" maps the number of packets whose lengths range from 33 bytes to 64 bytes. When the packet length exceeds 1024 bytes, the packet length increases by 512 bytes. For example, "1536" maps the number of packets whose lengths range from 1025 bytes to 1536 bytes. The number of packets whose lengths range from 577 bytes to 1024 bytes is recorded mapping "1024".
Protocol	Protocol number.
Total Streams	Total number of flows.
Packets/sec	Number of packets per second.
Stream/sec	Number of flows per second.
Packets /stream	Average number of packets in each flow.
Active(sec) /stream	Average active time of each flow. Unit is seconds.
Idle(sec) /stream	Average inactive time of each flow. Unit is seconds.
Type	Flow type.
DstIP(Port)	Destination IP address (destination port number) of flows.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
SrcIP(Port)	Source IP address (source port number) of flows.
Pro	Protocol type of flows.
ToS	Service type of flows.
Pkts	Number of packets in a flow.
If(Direc)	Interface name (flow direction). ● (I): inbound direction ● (O): outbound direction

21.12.7 display ip netstream record

Function

The **display ip netstream record** command displays the configuration of a flexible flow statistics template.

Format

display ip netstream record { **all** | **name** *record-name* }

Parameters

Parameter	Description	Value
all	Displays configurations of all flexible flow statistics templates.	-
name *record-name*	Displays the configuration of a flexible flow statistics template specified by *record-name*.	**NOTE** The parameter *record-name* is determined by the template name configured using the **ip netstream record** command.

Views

All views

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

None

Example

Display the configuration of the flexible flow statistics template **test0**.

```
<Huawei> display ip netstream record name test0
ip netstream record test0
 match ipv4 source-address
 match ipv4 destination-address
```

Table 21-71 Description of the display ip netstream record command output

Item	Description
ip netstream record test0	The flexible flow statistics template is **test0**.
match ipv4 source-address	According to the template **test0**, flows are aggregated based on the source IP address. This field is configured using the **match ipv4** command.
match ipv4 destination-address	According to the template **test0**, flows are aggregated based on the destination IP address. This field is configured using the **match ipv4** command.

Related Topics

21.12.29 ip netstream record

21.12.8 display ip netstream statistic

Function

The **display ip netstream statistic** command displays the NetStream flow statistics.

Format

display ip netstream statistic

Parameters

None

Views

All views

Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

None

Example

Display the NetStream statistics.

```
<Huawei> display ip netstream statistic
 Origin ingress entries           : 30000
 Origin ingress packets           : 30000
 Origin ingress octets            : 1380000
 Origin egress entries            : 0
 Origin egress packets            : 0
 Origin egress octets             : 0
 Origin total entries             : 30000
 Agility ingress entries          : 30000
 Agility ingress packets          : 30000
 Agility ingress octets           : 3960000
 Agility egress entries           : 0
 Agility egress packets           : 0
 Agility egress octets            : 0
 Agility total entries            : 30000
 Handle origin entries            : 29035
 Handle agility entries           : 29050
 Handle As aggre entries          : 1
 Handle ProtPort aggre entries    : 1
 Handle SrcPrefix aggre entries   : 118
 Handle DstPrefix aggre entries   : 1
 Handle Prefix aggre entries      : 118
 Handle AsTos aggre entries       : 1
 Handle ProtPortTos aggre entries : 1
 Handle SrcPreTos aggre entries   : 118
 Handle DstPreTos aggre entries   : 1
 Handle PreTos aggre entries      : 118
```

Table 21-72 Description of the display ip netstream statistic command output

Item	Description
Origin ingress entries	Total number of incoming original flows.
Origin ingress packets	Total number of incoming original packets.
Origin ingress octets	Total number of incoming original bytes.
Origin egress entries	Total number of outgoing original flows.
Origin egress packets	Total number of outgoing original packets.
Origin egress octets	Total number of outgoing original bytes.
Origin total entries	Total number of original flows.
Agility ingress entries	Number of incoming flexible flows.
Agility ingress packets	Number of incoming flexible packets.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Agility ingress octets	Number of incoming flexible bytes.
Agility egress entries	Number of outgoing flexible flows.
Agility egress packets	Number of outgoing flexible packets.
Agility egress octets	Number of outgoing flexible bytes.
Agility total entries	Total number of flexible flows.
Handle origin entries	Number of processed incoming and outgoing original flows.
Handle agility entries	Number of processed incoming and outgoing flexible flows.
Handle As aggre entries	Number of processed incoming and outgoing AS aggregation flows.
Handle ProtPort aggre entries	Number of processed incoming and outgoing protocol-port aggregation flows.
Handle SrcPrefix aggre entries	Number of processed incoming and outgoing source-prefix aggregation flows.
Handle DstPrefix aggre entries	Number of processed incoming and outgoing destination-prefix aggregation flows.
Handle Prefix aggre entries	Number of processed incoming and outgoing prefix aggregation flows.
Handle AsTos aggre entries	Number of processed incoming and outgoing AS-ToS aggregation flows.
Handle ProtPortTos aggre entries	Number of processed incoming and outgoing protocol-port-ToS aggregation flows.
Handle SrcPreTos aggre entries	Number of processed incoming and outgoing source-prefix-ToS aggregation flows.
Handle DstPreTos aggre entries	Number of processed incoming and outgoing destination-prefix-ToS aggregation flows.
Handle PreTos aggre entries	Number of processed incoming and outgoing prefix-ToS aggregation flows.

21.12.9 display snmp-agent trap feature-name netstream all

Function

The **display snmp-agent trap feature-name netstream all** command displays the status of all traps on the NetStream module.

 Copyright © Huawei Technologies Co., Ltd.

Format

display snmp-agent trap feature-name netstream all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent trap feature-name netstream all** command to check the status of all traps on the NetStream module. This status can be configured using the **snmp-agent trap enable feature-name netstream** command.

Example

Display the status of all traps on the NetStream module.

```
<Huawei> display snmp-agent trap feature-name netstream all
-----------------------------------------------------------------------------
Feature name: netstream
Trap number : 1
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwNetStreamSessionFull          off                     off
```

Table 21-73 Description of the display snmp-agent trap feature-name netstream all command output

Item	Description
Feature name	Name of the module that a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap.
Default switch status	Default status of a trap: ● on: The trap is enabled. ● off: The trap is disabled.
Current switch status	Status of a trap: ● on: The trap is enabled. ● off: The trap is disabled. This status can be configured using the **snmp-agent trap enable feature-name netstream** command.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
hwNetStreamSessionFull	The NetStream session table is full.

Related Topics

21.12.44 snmp-agent trap enable feature-name netstream

21.12.10 display snmp-agent trap feature-name sindex all

Function

The **display snmp-agent trap feature-name sindex all** command displays the status of all traps on the SINDEX module.

Format

display snmp-agent trap feature-name sindex all

Parameters

None

Views

All views

Default Level

3: Management level

Usage Guidelines

You can run the **display snmp-agent trap feature-name sindex all** command to check the status of all traps on the SINDEX module. This status can be configured using the **snmp-agent trap enable feature-name sindex** command.

Example

Display the status of all traps on the SINDEX module.

```
<Huawei> display snmp-agent trap feature-name sindex all
-----------------------------------------------------------------------------
Feature name: SINDEX
Trap number : 1
-----------------------------------------------------------------------------
Trap name                    Default switch status   Current switch status
hwNetStreamIndexUsedUp          on                      on
```


Copyright © Huawei Technologies Co., Ltd.

Table 21-74 Description of the display snmp-agent trap feature-name sindex all command output

Item	Description
Feature name	Name of the module that a trap message belongs.
Trap number	Number of trap messages.
Trap name	Name of a trap.
Default switch status	Default status of a trap: ● on: The trap is enabled. ● off: The trap is disabled.
Current switch status	Status of a trap: ● on: The trap is enabled. ● off: The trap is disabled. This status can be configured using the **snmp-agent trap enable feature-name sindex** command.
hwNetStreamIndexUsed-Up	The NetStream interface indexes are all allocated.

Related Topics

21.12.45 snmp-agent trap enable feature-name sindex

21.12.11 enable

Function

The **enable** command enables the aggregation function in the aggregation view.

The **undo enable** command disables the aggregation function in the aggregation view.

By default, the aggregation function is disabled.

Format

enable

undo enable

Parameters

None

Views

NetStream aggregation view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The **enable** command takes effect only in the NetStream aggregation view. Flow statistics are exported according to the configured aggregation method only after you run the **enable** command in the aggregation view.

Precautions

When this command is executed, the device will send an aggregation template to the server.

Example

Enable destination address prefix aggregation.

```
<Huawei> system-view
[Huawei] ip netstream aggregation destination-prefix
[Huawei-aggregation-dstpre] enable
```

Related Topics

21.12.14 ip netstream aggregation

21.12.12 export version

Function

The **export version** command configures the versions of exported packets carrying aggregation flow statistics and flexible flow statistics.

The **undo export version** command restores the default setting.

By default, the version of exported packets carrying aggregation flow statistics is V8 and the version of exported packets carrying flexible flow statistics is V9.

Format

export version *version*

undo export version

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
version	Specifies the version numbers of exported packets carrying aggregation flow statistics and flexible flow statistics.	The value of *version* is as follows: • The value is 8, 9, or 10 in the NetStream aggregation view. The default is 8. • The value is 9 or 10 in the flexible flow statistics template view. The default is 9.

Views

NetStream aggregation view, flexible flow statistics template view

Default Level

3: Management level

Usage Guidelines

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

The format of exported packets in V8 is fixed and is not easy to expand. The format of exported packets in V9 or V10 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

Example

Set the version number of exported packets carrying aggregation flow statistics to V9.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as] export version 9
```

Set the version number of exported packets carrying flexible flow statistics to V10.

```
<Huawei> system-view
[Huawei] ip netstream record test
[Huawei-record-test] export version 10
```

Related Topics

21.12.14 ip netstream aggregation
21.12.29 ip netstream record

 Copyright © Huawei Technologies Co., Ltd.

21.12.13 ip netstream

Function

The **ip netstream** command enables IPv4 flow statistics collection on the inbound and outbound interfaces.

The **undo ip netstream** command restores the default setting.

By default, statistics collection for IPv4 flows is disabled on the inbound and outbound interfaces.

Format

ip netstream { **inbound** | **outbound** }

undo ip netstream { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables flow statistics collection on the inbound interface.	-
outbound	Enables flow statistics collection on the outbound interface.	-

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To export IPv4 flow statistics, you must run the **ip netstream** command to enable the IPv4 flow statistics collection function on the interface.

Precautions

When you enable the IPv4 flow statistics collection function on the inbound interface, enable the statistics collection function on unicast and multicast packets.

If the NetStream function is enabled on the main interface but you do not set a sampling ratio using the **21.12.31 ip netstream sampler (interface view)** command, the main interface uses the sampling ratio of 1:100. If you set the sampling ratio, the interface uses this sampling ratio.

 Copyright © Huawei Technologies Co., Ltd.

When this command is executed, the device will send a template to the server.

Example

Enable the flow statistics collection function for the incoming IPv4 packets on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream inbound
```

Related Topics

21.12.31 ip netstream sampler (interface view)

21.12.14 ip netstream aggregation

Function

The **ip netstream aggregation** command configures the aggregation method and displays the aggregation view.

Format

ip netstream aggregation { **as** | **as-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos** }

Parameters

Parameter	Description	Value
as	Specifies the AS aggregation. It classifies flows based on: • Source AS number • Destination AS number • Inbound interface index • Outbound interface index	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
as-tos	Specifies the AS-ToS aggregation. It classifies flows based on: ● Source AS number ● Destination AS number ● Inbound interface index ● Outbound interface index ● ToS	-
destination-prefix	Specifies the destination-prefix aggregation. It classifies flows based on: ● Destination AS number ● Destination mask length ● Outbound interface index ● Destination prefix	-
destination-prefix-tos	Specifies the destination-prefix-ToS aggregation. It classifies flows based on: ● Destination AS number ● Destination mask length ● Destination prefix ● ToS ● Outbound interface index	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
prefix	Specifies the prefix aggregation. It classifies flows based on: ● Source and destination AS numbers ● Source and destination mask lengths ● Source and destination prefixes ● Inbound interface index ● Outbound interface index	-
prefix-tos	Specifies the prefix-ToS aggregation. It classifies flows based on: ● Source and destination AS numbers ● Source and destination mask lengths ● Source and destination prefixes ● ToS ● Inbound interface index ● Outbound interface index	-
protocol-port	Specifies the protocol-port aggregation. It classifies flows based on: ● Protocol number ● Source port number ● Destination port number	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
protocol-port-tos	Specifies the protocol-port-ToS aggregation. It classifies flows based on: ● Protocol number ● Source port number ● Destination port number ● ToS ● Inbound interface index ● Outbound interface index	-
source-prefix	Specifies the source-prefix aggregation. It classifies flows based on: ● Source AS number ● Source mask length ● Source prefix ● Inbound interface index	-
source-prefix-tos	Specifies the source-prefix-ToS aggregation. It classifies flows based on: ● Source AS number ● Source mask length ● Source prefix ● ToS ● Inbound interface index	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

NetStream aggregation groups the original flows with the same attributes together. The aggregation flow statistics collection and original flow statistics

 Copyright © Huawei Technologies Co., Ltd.

collection are different. The original flow statistics collection is on the basis of sampled packets, while the aggregation flow statistics collection is on the basis of original flows. Therefore, the aggregation flow statistics collection generates less data.

Follow-up Procedure

Run the **enable** command in the aggregation view to enable the device to export flow statistics according to the configured aggregation method.

Example

Configure the NetStream AS aggregation method.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as]
```

Configure the NetStream destination-prefix aggregation method.

```
<Huawei> system-view
[Huawei] ip netstream aggregation destination-prefix
[Huawei-aggregation-dstpre]
```

Related Topics

21.12.11 enable

21.12.15 ip netstream aggregation enable

Function

The **ip netstream aggregation enable** command enables the function of aggregating site visitor traffic on an interface.

The **undo ip netstream aggregation enable** command disables the function of aggregating site visitor traffic on an interface.

By default, the function of aggregating site visitor traffic is disabled on an interface.

Format

ip netstream aggregation enable

undo ip netstream aggregation enable

Parameters

None

Views

Interface view

Default Level

2: Configuration level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You can run the **ip netstream aggregation enable** command to enable the function of aggregating site visitor traffic on an interface and report uplink and downlink data on the interface to the Agile Controller.

Example

Enable the function of aggregating site visitor traffic on an interface.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 0/0/0
[Huawei-Gigabitethernet0/0/0] ip netstream aggregation enable
```

21.12.16 ip netstream aggregation timeout active

Function

The **ip netstream aggregation timeout active** command sets the active aging time of aggregation flows.

The **undo ip netstream aggregation timeout active** command restores the default setting.

By default, the active aging time of aggregation flows is 30 minutes.

Format

ip netstream aggregation timeout active *active-interval*

undo ip netstream aggregation timeout active

Parameters

Parameter	Description	Value
active-interval	Specifies the active aging time of aggregation flows.	The value is an integer that ranges from 1 to 60, in minutes. The default value is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the

 Copyright © Huawei Technologies Co., Ltd.

new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the active time (from flow creation time to the current time) of an aggregation flow exceeds the specified active aging time, the flow is exported to the destination.

To quickly detect the status of an active flow, set the active time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the active time to a large value.

Precaution

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the active aging time of aggregation flows to 20 minutes.

```
<Huawei> system-view
[Huawei] ip netstream aggregation timeout active 20
```

21.12.17 ip netstream aggregation timeout inactive

Function

The **ip netstream aggregation timeout inactive** command sets the inactive aging time of aggregation flows.

The **undo ip netstream aggregation timeout inactive** command restores the default setting.

By default, the inactive aging time of aggregation flows is 30 seconds.

Format

ip netstream aggregation timeout inactive *inactive-interval*

undo ip netstream aggregation timeout inactive

Parameters

Parameter	Description	Value
inactive-interval	Specifies the inactive aging time of aggregation flows.	The value is an integer that ranges from 10 to 600, in seconds. The default value is 30.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the inactive time (from the last packet receiving time to the current time) of an aggregation flow exceeds the specified inactive aging time, the flow is exported to the destination.

To quickly detect the status of an inactive flow, set the inactive time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the inactive time to a large value.

Precaution

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the inactive aging time of aggregation flows to 40 seconds.

```
<Huawei> system-view
[Huawei] ip netstream aggregation timeout inactive 40
```

21.12.18 ip netstream as extend enable

Function

The **ip netstream as extend enable** command sets the BGP AS number range.

The **undo ip netstream as extend enable** command restores the default setting.

By default, the BGP AS numbers range from 1 to 65535.

Format

ip netstream as extend enable

undo ip netstream as extend enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Management level

Usage Guidelines

Usage Scenario

By default, the BGP AS numbers range from 1 to 65535. A BGP AS number supports 32 bits; therefore, the BGP AS numbers ranging from 65536 to 4294967295 are not supported. After the **ip netstream as extend enable** command is executed, the BGP AS numbers ranging from 1 to 4294967295 can be supported.

Precautions

Only the output packets of V9 or V10 support the 32-bit BGP AS numbers.

Example

Set the supported BGP AS number range.

```
<Huawei> system-view
[Huawei] ip netstream as extend enable
```

21.12.19 ip netstream cache log enable

Function

The **ip netstream cache log enable** command enables the function of recording logs in NetStream traffic statistics globally.

The **undo ip netstream cache log enable** command disables the function of recording logs in NetStream traffic statistics globally.

By default, the function of recording logs is disabled.

NOTE

Only AR2204E&AR2240&AR2240C, and AR3200 Series do support the command.

Format

ip netstream cache log enable

undo ip netstream cache log enable

Parameters

None

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ip netstream cache log enable** command to enable the function of recording logs in NetStream traffic statistics.

Prerequisites

Before running this command, you need to ensure that the valid path for storing logs in NetStream traffic statistics has been configured using the **ip netstream cache log log-directory** command.

Precautions

The device has a rate limit on recording flows, and a maximum of 8000 aging flows are supported in the aging period. If the number of aged flows exceeds 8000, the device may discard some flow records to protect CPU resources. You are advised to set a long aging time (the default value is recommended) to reduce the probability of flow record loss.

Example

Enable the function of recording logs in NetStream traffic statistics.

```
<Huawei> system-view
[Huawei] ip netstream cache log log-directory usb0:
[Huawei] ip netstream cache log enable
```

Related Topics

21.12.20 ip netstream cache log log-directory

21.12.20 ip netstream cache log log-directory

Function

The **ip netstream cache log log-directory** command sets the path for storing logs in NetStream traffic statistics.

The **undo ip netstream cache log log-directory** command deletes the path for storing logs in NetStream traffic statistics.

By default, the path for storing logs is not configured.

NOTE

Only AR2204E&AR2240&AR2240C, and AR3200 series support the command.

Format

ip netstream cache log log-directory *log-directory*

undo ip netstream cache log log-directory *log-directory*

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
log-directory	Indicates the path for storing logs.	The value is a string of 1 to 63 case-insensitive characters without spaces. **NOTE** Logs can be saved to either a USB flash drive or an external SD card, but not the flash directory. The name of the currently used folder and data file in the root directory of the USB flash drive is NetStreamLog/netstreamdata.db. The logs in NetStream traffic statistics should be stored in the folder using this name. If a folder with the same name exists, the data may fail to be saved or the original file may be overwritten.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ip netstream cache log log-directory** command to set the path for storing logs in NetStream traffic statistics.

Precautions

If the function of recording logs is enabled globally by running the **ip netstream cache log enable** command, you want to delete the configured path for storing logs in NetStream traffic statistics, you must first run the **undo ip netstream cache log enable** command to disable the function of recording logs globally, and then run the **undo ip netstream cache log log-directory** command.

If the function of recording logs is enabled globally by running the **ip netstream cache log enable** command, you cannot run the **ip netstream cache log log-directory** command to set a new path for storing logs. To change the configured path for storing logs, you need to run the **undo ip netstream cache log enable** command to disable the function of recording logs first.

 Copyright © Huawei Technologies Co., Ltd.

Multiple data files can be saved to the fixed folder in the root directory of the USB flash drive, and the size of each data file is 10 MB. For example, if the first data file is netstreamdata.db, the system automatically creates the second data file netstreamdata2.db when the size of the data file exceeds 10 MB. In this manner, the third data file is netstreamdata3.db and the Xth data file is netstreamdatax.db.

Example

Set the path for storing logs in NetStream traffic statistics to usb0.

```
<Huawei> system-view
[Huawei] ip netstream cache log log-directory usb0:
```

Related Topics

21.12.19 ip netstream cache log enable

21.12.21 ip netstream export host

Function

The **ip netstream export host** command configures the destination IP address and destination UDP port number for the exported packets carrying IPv4 flow statistics.

The **undo ip netstream export host** command deletes the configured destination IP address and destination UDP port number for the exported packets carrying IPv4 flow statistics.

By default, no destination IP address and destination UDP port number are configured in the system view or aggregation view for the exported packets carrying IPv4 flow statistics.

Format

ip netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

undo ip netstream export host *ip-address port-number* [**vpn-instance** *vpn-instance-name*]

Parameters

Parameter	Description	Value
ip-address	Specifies the destination IPv4 address of the exported packets carrying IPv4 flow statistics.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
port-number	Specifies the destination UDP port number of the exported packets carrying IPv4 flow statistics.	The value is an integer that ranges from 0 to 65535.
vpn-instance *vpn-instance-name*	Specifies the VPN instance of the exported packets carrying IPv4 flow statistics.	The VPN instance has been created on the device.

Views

System view, NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After finishing data collection, the NDE sends the collected data to the NSC. This command specifies the destination address of the collected data, that is, the NSC IP address.

Precautions

When you run the **ip netstream export host** command in the system view, this command configures the destination address for the exported packets carrying IPv4 original flow statistics and IPv4 flexible flow statistics; when you run this command in the aggregation view, this command configures the destination address for the exported packets carrying IPv4 aggregation flows. The exported packets carrying aggregation flow statistics preferentially use the destination address configured in the aggregation view. If the destination address is not configured in the aggregation view, the exported packets carrying aggregation flow statistics use the destination address configured in the system view.

You can configure two destination addresses in the system view or aggregation view to implement NSC backup. To configure a third destination IP address, run the **undo netstream export ip host** command to delete an existing one first; otherwise, the system displays a message indicating that the maximum number of addresses is exceeded and the configuration fails.

Example

Set the destination IP address for the exported packets carrying original flow statistics to 10.1.1.1, and UDP port number to 222.

```
<Huawei> system-view
[Huawei] ip netstream export host 10.1.1.1 222
```

 Copyright © Huawei Technologies Co., Ltd.

Set the destination IP address for the exported packets carrying aggregation flow statistics to 10.2.2.1, and UDP port number to 255.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as] ip netstream export host 10.2.2.1 255
```

21.12.22 ip netstream export index-switch

Function

The **ip netstream export index-switch** command sets the number of digits in the interface indexes contained in an exported NetStream packet.

By default, the number of digits in interface indexes is 16.

Format

ip netstream export index-switch *index-switch*

Parameters

Parameter	Description	Value
index-switch	Specifies the number of digits in the index of a specified interface.	The value is 16 or 32. The default value is 16.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can run the **ip netstream export index-switch** command to set the number of digits in the interface index to 16 or 32.

The number of digits in an interface index contained in exported packets must be the same as the number of digits in an interface index that can be parsed by the NMS. For example, if the NMS can parse the 32-digit interface index, set the number of digits in an interface index contained in exported packets to 32.

Precautions

The number of digits in the interface index can be changed to 32 only when the NMS supports 32-digit interface index. If the number of digits in an interface index contained in exported packets is different from the number of digits in an

 Copyright © Huawei Technologies Co., Ltd.

interface index supported by the NMS, the NMS cannot identify NetStream packets sent by the device.

Example

Change the number of digits in the interface index contained in an exported NetStream packet from 16 to 32.

```
<Huawei> system-view
[Huawei] ip netstream export index-switch 32
```

21.12.23 ip netstream export source

Function

The **ip netstream export source** command configures the source address for the exported packets carrying IPv4 flow statistics and source UDP port number.

The **undo ip netstream export source** command restores the default source address and source UDP port number of the exported packets carrying IPv4 flow statistics.

By default, the source IP address of the exported packets carrying IPv4 flow statistics is not configured.

Format

ip netstream export source *ip-address* [*portnumber*]

undo ip netstream export source

Parameters

Parameter	Description	Value
ip-address	Specifies the source IPv4 address of the exported packets carrying IPv4 flow statistics.	-
portnumber	Specifies the source port of the exported packets carrying IPv4 flow statistics.	The value is an integer that ranges from 0 to 65535.

Views

System view, NetStream aggregation view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The NMS working with the NetStream system may need to identify the data source based on the source address in NetStream packets. You can run the **ip netstream export source** command to configure the source address of exported packets carrying IPv4 flow statistics.

Precautions

NetStream prefers the source IP and source UDP port number address configured in the aggregation view. If no source address is specified in an aggregation method, the source address configured in the system view is used.

Example

In the system view, set the source address for the exported packets carrying IPv4 flow statistics to 10.1.1.1.

```
<Huawei> system-view
[Huawei] ip netstream export source 10.1.1.1
```

In the aggregation view, set the source address for the exported packets carrying IPv4 flow statistics to 10.2.2.2.

```
<Huawei> system-view
[Huawei] ip netstream aggregation as
[Huawei-aggregation-as] ip netstream export source 10.2.2.2
```

21.12.24 ip netstream export source interface

Function

The **ip netstream export source interface** command configures the outbound interface for the exported packets carrying original flow statistics.

The **undo ip netstream export source** command deletes the outbound interface for the exported packets carrying original flow statistics.

By default, no outbound interface is configured for the exported packets carrying original flow statistics.

Format

ip netstream export source interface *interface-type interface-number* [*port-number*]

undo ip netstream export source

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
interface-type	Specifies the type of the outbound interface.	The value can be Ethernet interface, VLANIF interface, dialer interface, and Cellular interface.
interface-number	Specifies the number of the outbound interface.	-
port-number	Specifies the source UDP port of the exported NetStream packet.	The value is an integer that ranges from 0 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The NMS identifies the data source according to the outbound interface in NetStream packets, so you need to run the **ip netstream export source interface** command to set the outbound interface for NetStream packets. When the IP address of the outbound interface changes, NetStream packets can be sent from the outbound interface.

Precautions

The **ip netstream export source interface** command can be used only on Layer 3 interfaces.

Example

Set the outbound interface for the exported packets carrying original flow statistics to GE0/0/1.

```
<Huawei> system-view
[Huawei] ip netstream export source interface gigabitethernet 0/0/1
```

21.12.25 ip netstream export template timeout-rate

Function

The **ip netstream export template timeout-rate** command sets the interval for sending the NetStream export template.

 Copyright © Huawei Technologies Co., Ltd.

The **undo ip netstream export template timeout-rate** command restores the default interval.

By default, the interval for sending the NetStream export template is 30 minutes.

Format

ip netstream export template timeout-rate *timeout-interval*

undo ip netstream export template timeout-rate

Parameters

Parameter	Description	Value
timeout-interval	Specifies the interval for sending the NetStream export template.	The value is an integer in the range from 1 to 3600, in minutes. The default value is 30.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If network traffic is heavy, the template refresh interval should be set to a small value; however, more traffic is generated for sending the template. Therefore, you need to select a proper interval for sending the NetStream export template. In this case, you can run the **ip netstream export template timeout-rate** command to adjust the interval.

Example

Set the interval for sending the NetStream export template to 50 minutes.

```
<Huawei> system-view
[Huawei] ip netstream export template timeout-rate 50
```

21.12.26 ip netstream export version

Function

The **ip netstream export version** command configures the version number of the exported packets carrying original flow statistics.

The **undo ip netstream export version** command restores the default setting.

 Copyright © Huawei Technologies Co., Ltd.

By default, the version number of the exported packets carrying IPv4 original flow statistics is 5. Packets of V5 have no AS option and do not carry BGP next hop information.

Format

ip netstream export version *version* [**origin-as** | **peer-as**] [**bgp-nexthop**]

undo ip netstream export version

Parameters

Parameter	Description	Value
version	Specifies the version number of exported packets carrying IPv4 flow statistics.	The value of *version* is set to 5, 9 or 10. The default is 5.
origin-as	Specifies the AS number recorded in the statistics as the original AS number.	-
peer-as	Specifies the AS number recorded in the statistics as the peer AS number.	-
bgp-nexthop	Configures the statistics to carry BGP next hop information. Currently, V9 and V10 support the exported packets carrying BGP next hop information.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The NDE exports NetStream flow statistics to the NSC. The version of exported packets must be the same as that configured on the NSC so that the NSC can parse the exported packets.

 Copyright © Huawei Technologies Co., Ltd.

The format of exported packets in V5 is fixed and is not easy to expand. The format of exported packets in V9 or V10 is defined in templates and is easy to combine or expand. The statistics are exported more flexibly.

Precautions

Only one version can be specified on a device. The versions configured on all the devices on the network must be the same as the version configured on the NMS.

The AS option is used according to the actual situation of the AS configured on each device. The AS option affects only the packet statistics result, but does not affect the flows. The AS option is encapsulated in the AS option field carried in the NetStream packets sent to the NMS. The exported packets of V5 do not support BGP next hop information.

Example

Set the version of the exported packets carrying IPv4 flow statistics to V9 and AS option to **peer-as**.

```
<Huawei> system-view
[Huawei] ip netstream export version 9 peer-as
```

21.12.27 ip netstream multicast

Function

The **ip netstream multicast** command enables the flow statistics collection function for incoming and outgoing IPv4 multicast flows.

The **undo ip netstream multicast** command disables the flow statistics collection function for incoming and outgoing IPv4 multicast flows.

By default, the flow statistics collection function is disabled for incoming and outgoing IPv4 multicast flows.

Format

ip netstream multicast { **inbound** | **outbound** }

undo ip netstream multicast { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Indicates the incoming packets.	-
outbound	Indicates the outgoing packets.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

The **ip netstream multicast** command allows the device to collect statistics about incoming and outgoing IPv4 multicast packets and export the statistics to the NMS.

Example

Enable the flow statistics collection function for incoming IPv4 multicast packets on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream multicast inbound
```

21.12.28 ip netstream pre-classify enable

Function

The **ip netstream pre-classify enable** command enables the NetStream pre-classify function globally.

The **undo ip netstream pre-classify enable** command disables the NetStream pre-classify function globally.

By default, the pre-classify function is disabled globally.

Format

ip netstream pre-classify enable

undo ip netstream pre-classify enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

If you need to collect statistics on original packets when the IPSec, NAT, and VXLAN services are configured together, run the **ip netstream pre-classify enable** command to enable the pre-classify function globally and configure the pre-classify function for original packets.

 Copyright © Huawei Technologies Co., Ltd.

The pre-classify function for original packets is configured using the **qos pre-classify** command.

When multiple services are configured, NetStream extracts the template content in the pre-classify configuration order. For example, if VXLAN is configured and then IPSec is configured, and pre-classify is configured for both services, NetStream extracts the original packets from the VXLAN encapsulation first. If pre-classify is configured for only IPSec, NetStream extracts VXLAN encapsulated packets.

Example

Enable NetStream pre-classify globally.

```
<Huawei> system-view
[Huawei] ip netstream pre-classify enable
```

21.12.29 ip netstream record

Function

The **ip netstream record** command creates a new flexible flow statistics template or displays the view of an existing flexible statistics template.

The **undo ip netstream record** command deletes a specified flexible flow statistics template.

By default, no flexible flow statistics template exists.

Format

ip netstream record *record-name*

undo ip netstream record *record-name*

Parameters

Parameter	Description	Value
record-name	Specifies the name of the flexible flow statistics template.	The value is a string of 1 to 20 case-sensitive characters without spaces. The name of the flexible flow statistics template cannot contain special characters such as @, %, or *.

Views

System view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You need to create the flexible flow statistics template before exporting flexible flow statistics.

Precautions

A maximum of 16 flexible flow statistics templates can be configured on one device. To configure a third flexible flow statistics template, run the **undo ip netstream record** command to delete an existing one first.

The flexible flow statistics template that has been applied to an interface cannot be modified or deleted. To delete this flexible flow statistics template, run the **undo port ip netstream record** command on the interface and then modify or delete the template.

Example

Create the flexible flow statistics template named **abc**.

```
<Huawei> system-view
[Huawei] ip netstream record abc
[Huawei-record-abc]
```

Related Topics

21.12.41 port ip netstream record

21.12.7 display ip netstream record

21.12.30 ip netstream rpf-failure

Function

The **ip netstream rpf-failure** command enables NetStream functions for collecting statistics about flows that fail the RPF check.

The **undo ip netstream rpf-failure** command disables NetStream functions from collecting statistics about flows that fail the RPF check.

By default, NetStream functions are disabled from collecting statistics about flows that fail the RPF check.

Format

ip netstream rpf-failure inbound

undo ip netstream rpf-failure inbound

Parameters

None

 Copyright © Huawei Technologies Co., Ltd.

Views

Interface view

Default Level

3: Management level

Usage Guidelines

You need to enable the RPF check before configuring NetStream functions for collecting statistics about flows that fail the RPF check.

Example

Enable RPF statistics function on Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream rpf-failure inbound
```

21.12.31 ip netstream sampler (interface view)

Function

The **ip netstream sampler** command configures the packet sampling function for IPv4 packets on an interface.

The **undo ip netstream sampler** command restores the default setting.

By default, the packet-based regular sampling is used. The default packet sampling ratio is 100.

Format

ip netstream sampler { **fix-packets** *packet-interval* | **fix-time** *time-interval* | **random-packets** *packet-interval* | **random-time** *time-interval* } { **inbound** | **outbound** }

undo ip netstream sampler { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
fix-packets *packet-interval*	Indicates the number of packets between two sampled packets in the packet-based regular sampling.	The value is an integer that ranges from 1 to 65535.
fix-time *time-interval*	Indicates the interval of time-based regular sampling.	The value is an integer that ranges from 5 to 30000, in milliseconds.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
random-packets *packet-interval*	Indicates the number of packets between two sampled packets in the packet-based random sampling.	The value is an integer that ranges from 1 to 65535.
random-time *time-interval*	Indicates the interval of time-based random sampling.	The value can be the following: ● 3.0 ● 6.0 ● 12.0 ● 24.0 ● 48.0 ● 96.0 ● 192.0 ● 383.5 ● 767.0 ● 1534.0 ● 3068.0 ● 6136.0 The unit is millisecond.
inbound	Samples incoming traffic on an interface.	-
outbound	Samples outgoing traffic on an interface.	-

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

You can set an interval for sampling packets so that only statistics about sampled packets are collected. The statistics show the flow status on the entire network. The sampling function reduces NetStream impact on device performance.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

You must run the **ip netstream sampler** command together with the **21.12.13 ip netstream** command. If you run only the **ip netstream sampler** command, the command does not take effect.

If you run the **ip netstream sampler** command multiple times in the same view, only the latest configuration takes effect.

Example

Set the packet-based regular sampling ratio for the incoming packets on Eth2/0/0 to 1200.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip netstream sampler fix-packets 1200 inbound
[Huawei-Ethernet2/0/0] ip netstream inbound
```

Related Topics

21.12.13 ip netstream

21.12.32 ip netstream tcp-flag enable

Function

The **ip netstream tcp-flag enable** command configures the aging of NetStream traffic according to the FIN flag or the RST flag in the TCP packet header.

The **undo ip netstream tcp-flag enable** command restores the default setting.

By default, NetStream flows are not aged according to the FIN or RST flag in the TCP packet header.

Format

ip netstream tcp-flag enable

undo ip netstream tcp-flag enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

The FIN or RST flag in a TCP packet indicates that the TCP connection is terminated. When receiving a packet with the FIN or RST flag, the device immediately ages the corresponding NetStream flow. If the **ip netstream tcp-flag enable** command is not run, NetStream flows are aged by following other criteria, for example, inactive aging time or bytes overflow.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Only original flows can be aged according to the FIN or RST flag in the TCP packet header.

Example

Configure the aging of original flows according to the FIN or RST flag in the TCP packet header.

```
<Huawei> system-view
[Huawei] ip netstream tcp-flag enable
```

21.12.33 ip netstream tm-after enable

Function

The **ip netstream tm-after enable** command enables the NetStream sampling function after queue scheduling.

The **undo ip netstream tm-after enable** command restores the default setting.

By default, NetStream sampling is performed before queue scheduling.

Format

ip netstream tm-after enable

undo ip netstream tm-after enable

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

 Copyright © Huawei Technologies Co., Ltd.

By default, NetStream sampling is performed before queue scheduling. If a local device discards packets, the bandwidth calculated based on sampling data is greater than the bandwidth configured on the interface. To resolve this problem, run the **ip netstream tm-after enable** command to enable the NetStream sampling function after queue scheduling.

Example

Enable the NetStream sampling function after queue scheduling.

```
<Huawei> system-view
[Huawei] ip netstream tm-after enable
```

21.12.34 ip netstream timeout active

Function

The **ip netstream timeout active** command configures the active flow aging time.

The **undo ip netstream timeout active** command restores the default setting.

By default, the active flow aging time is 30 minutes.

Format

ip netstream timeout active *active-interval*

undo ip netstream timeout active

Parameters

Parameter	Description	Value
active-interval	Specifies the active aging time.	The value is an integer that ranges from 1 to 60, in minutes. The default is 30.

Views

System view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

 Copyright © Huawei Technologies Co., Ltd.

When the active time (from flow creation time to the current time) of a flow exceeds the specified active aging time, the flow is exported to the destination.

To quickly detect the status of an active flow, set the active time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the active time to a large value.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the active aging time to 20 minutes.

```
<Huawei> system-view
[Huawei] ip netstream timeout active 20
```

21.12.35 ip netstream timeout inactive

Function

The **ip netstream timeout inactive** command configures the inactive aging time.

The **undo ip netstream timeout inactive** command restores the default setting.

By default, the inactive aging time is 30 seconds.

Format

ip netstream timeout inactive *inactive-interval*

undo ip netstream timeout inactive

Parameters

Parameter	Description	Value
inactive-interval	Specifies the inactive aging time.	The value is an integer that ranges from 10 to 600, in seconds. The default is 30.

Views

System view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

Network traffic may burst intermittently, while the memory capacity of the NDE is limited. Earlier flows in the memory need to be exported to release space for the new flows. The process of exporting old flows is called aging. All flows in the NDE memory will be exported to the NSC for analysis.

When the inactive time (from the last packet receiving time to the current time) of an original or flexible flow exceeds the specified inactive aging time, the flow is exported to the destination.

To quickly detect the status of an inactive flow, set the inactive time to a small value; however, this setting increases the frequency at which NetStream packets are sent. To reduce the frequency at which NetStream packets are exported and improve statistics collecting efficiency, set the inactive time to a large value.

Precautions

If you set multiple aging modes on the device, a flow is aged when it matches any criterion.

Example

Set the inactive aging time to 20 seconds.

```
<Huawei> system-view
[Huawei] ip netstream timeout inactive 20
```

21.12.36 ip-mpls netstream

Function

The **ip-mpls netstream** command enables the function of collecting statistics about IPv4 and MPLS flows in the inbound and outbound directions of an interface.

The **undo ip-mpls netstream** command restores the default configuration.

By default, the function of collecting statistics about IPv4 and MPLS flows in the inbound and outbound directions of an interface is disabled.

NOTE

This command is supported only by the AR1200, AR2200, AR3200, and AR3600 series routers.

Format

ip-mpls netstream { **inbound** | **outbound** }

undo ip-mpls netstream { **inbound** | **outbound** }

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
inbound	Enables the function of collecting statistics about IPv4 and MPLS flows in the inbound direction of an interface.	-
outbound	Enables the function of collecting statistics about IPv4 and MPLS flows in the outbound direction of an interface.	-

Views

Ethernet interface view, Ethernet sub-interface view, GigabitEthernet interface view, GigabitEthernet sub-interface view, XGigabitEthernet interface view, XGigabitEthernet sub-interface view, serial interface view, or serial sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

In the NetStream implementation, you must run this command to enable the flow statistics collection function on an interface so that the statistics about IPv4 and MPLS flows can be displayed.

Precautions

The **ip netstream**, **mpls netstream**, and **ip-mpls netstream** commands are mutually exclusive. Only one of these commands can be enabled on an interface.

If NetStream is configured on a main interface but the sampling ratio is not configured using the **21.12.31 ip netstream sampler (interface view)** command, the main interface samples packets based on the fixed sampling ratio of 1/100. Otherwise, the main interface samples packets based on the configured sampling ratio.

If the **port ip netstream record** command is configured on an interface, the **ip-mpls netstream** command cannot be configured.

When the **ip-mpls netstream** command is run and the version of the exported packets is 9, the device sends the original flow template with ID 1317 to the server.

 Copyright © Huawei Technologies Co., Ltd.

MPLS traffic in MPLS over GRE and L2VPN scenarios is not supported. Statistics about aggregation flows and flexible flows of MPLS traffic cannot be collected. MPLS traffic statistics collection based on MQC is not supported.

Example

Enable the function of collecting statistics about IPv4 and MPLS flows in the inbound direction of Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] ip-mpls netstream inbound
```

Related Topics

21.12.31 ip netstream sampler (interface view)

21.12.37 mpls netstream

Function

The **mpls netstream** command enables the function of collecting statistics about MPLS flows in the inbound and outbound directions of an interface.

The **undo mpls netstream** command restores the default configuration.

By default, the function of collecting statistics about MPLS flows in the inbound and outbound directions of an interface is disabled.

NOTE

This command is supported only by the AR1200, AR2200, AR3200, and AR3600 series routers.

Format

mpls netstream { **inbound** | **outbound** }

undo mpls netstream { **inbound** | **outbound** }

Parameters

Parameter	Description	Value
inbound	Enables the function of collecting statistics about MPLS flows in the inbound direction of an interface.	-
outbound	Enables the function of collecting statistics about MPLS flows in the outbound direction of an interface.	-

Copyright © Huawei Technologies Co., Ltd.

Views

Ethernet interface view, Ethernet sub-interface view, GigabitEthernet interface view, GigabitEthernet sub-interface view, XGigabitEthernet interface view, XGigabitEthernet sub-interface view, serial interface view, or serial sub-interface view

Default Level

2: Configuration level

Usage Guidelines

Application Scenario

In the NetStream implementation, you must run this command to enable the flow statistics collection function on an interface so that the statistics about MPLS flows can be displayed.

Precautions

The **ip netstream**, **mpls netstream**, and **ip-mpls netstream** commands are mutually exclusive. Only one of these commands can be enabled on an interface.

If NetStream is configured on a main interface but the sampling ratio is not configured using the **21.12.31 ip netstream sampler (interface view)** command, the main interface samples packets based on the fixed sampling ratio of 1/100. Otherwise, the main interface samples packets based on the configured sampling ratio.

If the **port ip netstream record** command is configured on an interface, the **mpls netstream** command cannot be configured.

When the **mpls netstream** command is run and the version of the exported packets is 9, the device sends the original flow template with ID 1317 to the server.

MPLS traffic in MPLS over GRE and L2VPN scenarios is not supported. Statistics about aggregation flows and flexible flows of MPLS traffic cannot be collected. MPLS traffic statistics collection based on MQC is not supported.

Example

Enable the function of collecting statistics about MPLS flows in the inbound direction of Eth2/0/0.

```
<Huawei> system-view
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] mpls netstream inbound
```

Related Topics

21.12.31 ip netstream sampler (interface view)

21.12.38 mask

Copyright © Huawei Technologies Co., Ltd.

Function

The **mask** command sets the aggregation mask length.

The **undo mask** command restores the default setting.

By default, no aggregation mask is configured.

Format

mask { **source** | **destination** } **minimum** *mask-length*

undo mask { **source** | **destination** }

Parameters

Parameter	Description	Value
source	Indicates the aggregation mask of the source address. It is used in the following aggregation methods: prefix, prefix-ToS, source-prefix, and source-prefix-ToS.	-
destination	Indicates the aggregation mask of the destination address. It is used in the following aggregation methods: prefix, prefix-ToS, destination-prefix, or destination-prefix-ToS.	-
mask-length	Specifies the aggregation mask length.	The value is an integer that ranges from 1 to 32.

Views

NetStream aggregation view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

The system uses the larger value between the set mask and the largest mask in the FIB table. If the aggregation mask is not configured, the system uses the mask in the FIB table for aggregation.

Precaution

Aggregation masks are applied to six aggregation methods: **destination-prefix**, **destination-prefix-tos**, **prefix**, **prefix-tos**, **source-prefix**, and **source-prefix-tos**.

 Copyright © Huawei Technologies Co., Ltd.

Example

Set the aggregation mask length in the source-prefix aggregation method to 24.

```
<Huawei> system-view
[Huawei] ip netstream aggregation source-prefix
[Huawei-aggregation-srcpre] mask source minimum 24
```

21.12.39 match ipv4

Function

The **match ipv4** command configures aggregation keywords in an IPv4 flexible flow statistics template.

The **undo match ipv4** command deletes aggregation keywords from an IPv4 flexible flow statistics template.

Format

match ipv4 { **protocol** | **tos** | **source-address** | **destination-address** | **source-port** | **destination-port** }

undo match ipv4 { **protocol** | **tos** | **source-address** | **destination-address** | **source-port** | **destination-port** }

Parameters

Parameter	Description	Value
protocol	Indicates the IP protocol aggregation.	-
tos	Indicates the ToS priority aggregation.	-
source-address	Indicates the source IP address aggregation.	-
destination-address	Indicates the destination IP address aggregation.	-
source-port	Indicates the source port number aggregation.	-
destination-port	Indicates the destination port aggregation.	-

Views

Flexible flow statistics template view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

You need to create a flexible flow statistics template using the **21.12.29 ip netstream record** command before running the **match ipv4** command.

When you run the **match ipv4** command to configure the aggregation keywords, only one keyword can be configured each time. If you run this command multiple times in the same view, a set of multiple aggregation keywords is configured. If a template has been applied to an interface, you cannot modify or delete aggregation keywords from the template.

Example

Set the flexible flow statistics template **abc1** to aggregate flows based on the source port number.

```
<Huawei> system-view
[Huawei] ip netstream record abc1
[Huawei-record-abc1] match ipv4 source-port
```

Related Topics

21.12.29 ip netstream record

21.12.40 match vxlan vni

Function

The **match vxlan vni** command configures the VXLAN VNI aggregation keyword for record.

The **undo match vxlan vni** command deletes the VXLAN VNI aggregation keyword.

By default, no VXLAN VNI aggregation keyword is configured in a flexible flow statistics template.

Format

match vxlan vni

undo match vxlan vni

Parameters

None

Views

Flexible flow template view

Default Level

3: Management level

 Copyright © Huawei Technologies Co., Ltd.

Usage Guidelines

Usage Scenario

The VXLAN Network Identifier (VNI) is similar to a VLAN ID. It is used to divide VXLAN segments. When you configure VNI in the flexible flow statistics template, run this command to set the aggregation keyword.

Prerequisites

A flexible flow statistics template has been created or the flexible flow statistics template view is displayed using the **ip netstream record** command.

Precautions

When you run the **match vxlan vni** command to configure the VXLAN VNI aggregation keyword for record, if the record view has been applied to an interface, the aggregation keyword cannot be modified or deleted.

Only a VXLAN-capable device supports this command.

NOTE

Only the AR100, AR120, AR150, AR160, AR200, AR1200 series, AR2220E, AR2240, and AR3260 support VXLAN. AR2220E, AR2240, and AR3260 need to run the **portswitch** command to change the working mode of all interfaces on the SRU200, SRU400, 4GECS, and 2X10GL from Layer 3 mode to Layer 2 mode. The interfaces that change the working mode to layer 2 only support VXLAN. Only the 8FE1GE, 24GE, and 24ES2GP ethernet LAN card support VXLAN.

Only the AR100, AR120, AR150, AR160 (except AR161EW, AR161EW-M1, AR169EW, AR169EGW-L), AR200, AR1200series, AR2220E support EVPN.

Example

Configure the **abc1** record to aggregate flows based on the VNI type.

```
<Huawei> system-view
[Huawei] ip netstream record abc1
[Huawei-record-abc1] match vxlan vni
```

Related Topics

21.12.29 ip netstream record

21.12.41 port ip netstream record

Function

The **port ip netstream record** command applies the flexible flow statistics template to an interface.

The **undo port ip netstream record** command deletes a specified flexible flow statistics template on an interface.

By default, no flexible flow statistics template is applied to an interface.

Format

port ip netstream record *record-name*

 Copyright © Huawei Technologies Co., Ltd.

undo port ip netstream record

Parameters

Parameter	Description	Value
record-name	Specifies the name of a flexible flow statistics template.	The value is a string of 1 to 20 case-sensitive characters without spaces. The name of the flexible flow statistics template cannot contain special characters such as \, /, :, <, >, |, @, ', % or *. The value is the same as the IPv4 flexible flow statistics template name configured using the **ip netstream record** command.

Views

Interface view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

After a flexible flow statistics template is configured, run the **port ip netstream record** command to apply the template to an interface.

The interface then aggregates flows based on the configured aggregation keywords, collects flow statistics, and exports aged flows to the NSC.

Prerequisites

The flexible flow statistics template has been created and at least one aggregation keyword has been configured using the **match ip4** command.

Precautions

Each interface can be configured with only one flexible flow statistics template. Before modifying the flexible flow statistics template in the same interface view, run the **undo port ip netstream record** command to delete the existing configuration.

If the flexible flow statistics template has been applied to an interface, the template configuration cannot be modified or deleted.

 Copyright © Huawei Technologies Co., Ltd.

When flow statistics collection is enabled both on the inbound and outbound interfaces, the **port ip netstream record** command does not take effect.

Example

Configure the flexible flow statistics template **abc1** (aggregating flows based on the source and destination IP addresses, collecting statistics about the number of packets, and exporting the inbound interface index). Apply such configurations to Eth2/0/0.

```
<Huawei> system-view
[Huawei] ip netstream record abc1
[Huawei-record-abc1] match ipv4 source-address
[Huawei-record-abc1] match ipv4 destination-address
[Huawei-record-abc1] collect counter packets
[Huawei-record-abc1] collect interface input
[Huawei-record-abc1] quit
[Huawei] interface ethernet 2/0/0
[Huawei-Ethernet2/0/0] port ip netstream record abc1
 Info: Interface got a record config succeed.
```

Related Topics

21.12.29 ip netstream record

21.12.13 ip netstream

21.12.42 reset ip netstream cache

Function

The **reset ip netstream cache** command forcibly ages all the flows in the cache.

Format

reset ip netstream cache

Parameters

None

Views

System view

Default Level

3: Management level

Usage Guidelines

Forced aging is used when you require the latest statistics, but you do not satisfy with the existing aging conditions or some flows fail to age out due to an anomaly. You can forcibly age out all the original flows in the cache and export the flow statistics.

 Copyright © Huawei Technologies Co., Ltd.

Example

Age all the flows in the cache forcibly.

```
<Huawei> system-view
[Huawei] reset ip netstream cache
```

21.12.43 reset ip netstream statistic

Function

The **reset ip netstream statistic** command deletes NetStream flow statistics.

Format

reset ip netstream statistic

Parameters

None

Views

User view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

When diagnosing and locating network faults, collect flow statistics in a specified period. Before statistics collection starts, you can run this command to delete historical statistics.

Precautions

The **reset ip netstream statistic** command deletes all NetStream statistics. The statistics cannot be restored after being deleted. Therefore, confirm the action before running this command.

You can run this command multiple times at any interval.

Example

Delete NetStream statistics.

```
<Huawei> reset ip netstream statistic
```

 Copyright © Huawei Technologies Co., Ltd.

21.12.44 snmp-agent trap enable feature-name netstream

Function

The **snmp-agent trap enable feature-name netstream** command enables the NetStream trap function on the device.

The **undo snmp-agent trap enable feature-name netstream** command disables the NetStream trap function on the device.

By default, the NetStream trap function is disabled.

Format

snmp-agent trap enable feature-name netstream [**trap-name hwnetstreamsessionfull**]

undo snmp-agent trap enable feature-name netstream [**trap-name hwnetstreamsessionfull**]

Parameters

Parameter	Description	Value
trap-name	Specifies the name of the trap for a specified event.	-
hwnetstreamsessionfull	Sends Huawei-proprietary trap messages when the NetStream session table is full.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the NetStream trap function on the device.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name netstream
```

 Copyright © Huawei Technologies Co., Ltd.

21.12.45 snmp-agent trap enable feature-name sindex

Function

The **snmp-agent trap enable feature-name sindex** command enables the trap function for the SINDEX module.

The **undo snmp-agent trap enable feature-name sindex** command disables the trap function for the SINDEX module.

By default, the trap function is enabled for the SINDEX module.

Format

snmp-agent trap enable feature-name sindex [**trap-name hwnetstreamindexusedup**]

undo snmp-agent trap enable feature-name sindex [**trap-name hwnetstreamindexusedup**]

Parameters

Parameter	Description	Value
trap-name	Specifies the name of the trap for a specified event on the SINDEX module.	-
hwnetstreamindexu-sedup	Sends Huawei-proprietary trap messages when all interface indexes are allocated.	-

Views

System view

Default Level

3: Management level

Usage Guidelines

None

Example

Enable the trap function for the SINDEX module.

```
<Huawei> system-view
[Huawei] snmp-agent trap enable feature-name sindex
```

 Copyright © Huawei Technologies Co., Ltd.

21.13 IP Accounting Configuration Commands

21.13.1 display ip accounting input-packets

Function

The **display ip accounting input-packets** command displays statistics about incoming IP packets.

Format

display ip accounting input-packets { **matched** | **mismatched** } [**top**]

Parameters

Parameter	Description	Value
matched	Displays incoming packet statistics records in the matched table. **NOTE** The matched table stores statistics about the packets matching the IP accounting rules.	-
mismatched	Displays incoming packet statistics records in the mismatched table. **NOTE** The mismatched table stores: ● Statistics about the packets not matching the IP accounting rules. ● Common IP accounting statistics if no IP accounting rule is configured.	-
top	Displays the top 32 records with the most packets in a statistics table. If the table contains less than 32 records, all records will be displayed. **NOTE** If the **top** parameter is not specified, all records in the table are displayed.	-

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Background

The **display ip accounting input-packets** command displays statistics about incoming IP packets. These statistics help you monitor network traffic.

Precautions

The default upper threshold of the mismatched table is 0. To store records into the mismatched table, change the upper threshold; otherwise, no information is displayed for the mismatched table.

Example

Display incoming packet statistics in the matched table.

```
<Huawei> display ip accounting input-packets matched
The matched list contains 2 incoming streams.
Source          Destination     Protocol Packets     Bytes       Age(Unit:Min)
10.138.78.120   192.168.200.155 6        104         4821        0
10.138.78.119   192.168.200.155 6        17          782         0
```

Table 21-75 Description of the display ip accounting input-packets command output

Item	Description
Source	Source address of IP packets.
Destination	Destination addresses of IP packets.
Protocol	Packet protocol.
Packets	Number of packets.
Bytes	Number of bytes.
Age(Unit:Min)	Update time of date flows, in minutes.

Related Topics

21.13.2 display ip accounting output-packets

21.13.3 display ip accounting precedence

21.13.5 ip accounting

 Copyright © Huawei Technologies Co., Ltd.

21.13.2 display ip accounting output-packets

Function

The **display ip accounting output-packets** command displays statistics about outgoing IP packets.

Format

display ip accounting output-packets { **matched** | **mismatched** } [**top**]

Parameters

Parameter	Description	Value
matched	Displays outgoing packet statistics records in the matched table. **NOTE** The matched table stores statistics about the packets matching the IP accounting rules.	-
mismatched	Displays outgoing packet statistics records in the mismatched table. **NOTE** The mismatched table stores: ● Statistics about the packets not matching the IP accounting rules. ● Common IP accounting statistics if no IP accounting rule is configured.	-
top	Displays the top 32 records with the most packets in a statistics table. If the table contains less than 32 records, all records will be displayed. **NOTE** If the **top** parameter is not specified, all records in the table are displayed.	-

Views

All views

 Copyright © Huawei Technologies Co., Ltd.

Default Level

1: Monitoring level

Usage Guidelines

Background

The **display ip accounting output-packets** command displays statistics about outgoing IP packets. These statistics help you monitor network traffic.

Precautions

The default upper threshold of the mismatched table is 0. To store records into the mismatched table, change the upper threshold; otherwise, no information is displayed for the mismatched table.

Example

Display outgoing packet statistics in the matched table.

```
<Huawei> display ip accounting output-packets matched
The matched list contains 1 outgoing streams.
Source          Destination     Protocol Packets     Bytes       Age(Unit:Min)
192.168.1.112   192.168.1.255   17       5           1145        2
```

Table 21-76 Description of the display ip accounting output-packets command output

Item	Description
Source	Source address of IP packets.
Destination	Destination addresses of IP packets.
Protocol	Packet protocol.
Packets	Number of packets.
Bytes	Number of bytes.
Age(Unit:Min)	Update time of date flows, in minutes.

Related Topics

21.13.1 display ip accounting input-packets
21.13.3 display ip accounting precedence
21.13.5 ip accounting

21.13.3 display ip accounting precedence

Function

The **display ip accounting precedence** command displays statistics about IP precedence accounting.

 Copyright © Huawei Technologies Co., Ltd.

Format

display ip accounting precedence

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Precautions

The statistics about IP precedence accounting are stored in a dedicated statistics table.

Example

Display statistics about IP precedence accounting.

```
<Huawei> display ip accounting precedence
Precedence Packets          Bytes
Input
0          11920            1480947
Output
0          200              32889
```

Table 21-77 Description of the display ip accounting precedence command output

Item	Description
Precedence	IP packet precedence, ranging from 0 to 7.
Packets	Number of packets.
Bytes	Number of bytes.
Input	Statistics about incoming packets.
Output	Statistics about outgoing packets.

Related Topics

21.13.1 display ip accounting input-packets
21.13.2 display ip accounting output-packets
21.13.8 ip accounting precedence

 Copyright © Huawei Technologies Co., Ltd.

21.13.4 display ip accounting rule

Function

The **display ip accounting rule** command displays IP accounting rules.

Format

display ip accounting rule

Parameters

None.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

Background

The **display ip accounting rule** command displays all configured IP accounting rules for you to manage the rules.

Example

Display IP accounting rules.

```
<Huawei> display ip accounting rule
 IP Accounting rule list:
 IP address:            address mask:
 192.168.0.1             255.255.255.255
 192.168.0.2             255.255.255.255
 ---------------------------------------
 Total: 2 rules
```

Table 21-78 Description of the display ip accounting rule command output

Item	Description
IP address	IP address in an IP accounting rule.
address mask	Subnet mask in an IP accounting rule.

Related Topics

21.13.9 ip accounting rule

 Copyright © Huawei Technologies Co., Ltd.

21.13.5 ip accounting

Function

The **ip accounting** command enables IP accounting for the incoming or outgoing packets on an interface.

The **undo ip accounting** command disables IP accounting on an interface.

By default, IP accounting is disabled on all interfaces.

Format

ip accounting { **input-packets** | **output-packets** }

undo ip accounting { **input-packets** | **output-packets** }

Parameters

Parameter	Description	Value
input-packets	Enables IP accounting for the incoming packets on an interface.	-
output-packets	Enables IP accounting for the outgoing packets on an interface.	-

Views

Interface view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To collect statistics on the incoming or outgoing packets on an interface, run the **ip accounting** command to enable IP accounting on the interface.

Example

Enable IP accounting for the incoming packets on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip accounting input-packets
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.13.1 display ip accounting input-packets
21.13.2 display ip accounting output-packets

21.13.6 ip accounting matched-threshold

Function

The **ip accounting matched-threshold** command sets the upper threshold for a matched table.

The **undo ip accounting matched-threshold** command restores the default upper threshold of a matched table.

By default, the upper threshold of a matched table is 512.

Format

ip accounting matched-threshold *thresh-value*

undo ip accounting matched-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
thresh-value	Indicates the upper threshold of a matched table.	The value is an integer and the value range differs in various product series. On the AR100&AR120&AR150&AR160&200 series, the value ranges from 0 to 1024. On the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, and AR2204, the value ranges from 0 to 4096. On the AR2220L, AR2220E, AR2240C, AR2220, and AR2240, the value ranges from 0 to 8192. On the AR3200&AR3600 series, the value ranges from 0 to 16384. The default value is 512.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

A matched table stores statistics about the packets matching the IP accounting rules. The **ip accounting matched-threshold** command specifies the maximum number of records stored in the matched table. When the number of stored records reaches the upper threshold, new records cannot be added to the matched table.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The matched table does not store the statistics records of IP precedence accounting.

Example

Set the upper threshold for a matched table to 1000.

```
<Huawei> system-view
[Huawei] ip accounting matched-threshold 1000
```

Related Topics

21.13.7 ip accounting mismatched-threshold

21.13.7 ip accounting mismatched-threshold

Function

The **ip accounting mismatched-threshold** command sets the upper threshold for a mismatched table.

The **undo ip accounting mismatched-threshold** command restores the default upper threshold of a mismatched table.

By default, the upper threshold of a mismatched table is 0.

Format

ip accounting mismatched-threshold *thresh-value*

undo ip accounting mismatched-threshold

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
thresh-value	Indicates the upper threshold of a mismatched table.	The value is an integer and the value range differs in various product series. On the AR100&AR120&AR150&160&200 series, the value ranges from 0 to 1024. On the AR1200 series, AR2201-48FE, AR2202-48FE, AR2204-27GE, AR2204-27GE-P, AR2204-51GE-P, AR2204-51GE-R, AR2204E-D, AR2204E, and AR2204, the value ranges from 0 to 4096. On the AR2220L, AR2220E, AR2240C, AR2220, and AR2240, the value ranges from 0 to 8192. On the AR3200&AR3600 series, the value ranges from 0 to 16384. The default value is 0.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When common IP accounting is enabled without IP accounting rules configured, all statistics are recorded in the mismatched table. When common IP accounting is enabled with IP accounting rules configured, statistics about the packets that do not match the IP accounting rules are recorded in the mismatched table. The **ip accounting mismatched-threshold** command specifies the maximum number of records stored in the mismatched table. When the number of stored records reaches the upper threshold, new records cannot be added to the mismatched table.

Precautions

 Copyright © Huawei Technologies Co., Ltd.

The default upper threshold of a mismatched table is 0. To store records into the mismatched table, change the upper threshold; otherwise, the mismatched table does not store records.

The mismatched table does not store the statistics records of IP precedence accounting.

Example

Set the upper threshold for a mismatched table to 1000.

```
<Huawei> system-view
[Huawei] ip accounting mismatched-threshold 1000
```

Related Topics

21.13.6 ip accounting matched-threshold

21.13.8 ip accounting precedence

Function

The **ip accounting precedence** command enables IP precedence accounting for the incoming or outgoing packets on an interface.

The **undo ip accounting precedence** command disables IP precedence accounting for the incoming or outgoing packets on an interface.

By default, IP precedence accounting is disabled on interfaces.

Format

ip accounting precedence { **input-packets** | **output-packets** }

undo ip accounting precedence { **input-packets** | **output-packets** }

Parameters

Parameter	Description	Value
input-packets	Enables IP precedence accounting for the incoming packets on an interface.	-
output-packets	Enables IP precedence accounting for the outgoing packets on an interface.	-

Views

Interface view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

IP precedence ranges from 0 to 7. The **ip accounting precedence** command collects statistics about the packets with each IP precedence.

Prerequisite

The **ip accounting** { **input-packets** | **output-packets** } command has been executed to enable common IP accounting for the incoming or outgoing packets on the interface.

NOTE

For example, to use IP precedence accounting on the packets received by an interface, first enable common IP accounting for the incoming packets on the interface. The directions to which common IP accounting and IP precedence accounting apply must be the same.

Example

Enable IP precedence accounting for the incoming packets on GE1/0/0.

```
<Huawei> system-view
[Huawei] interface gigabitethernet 1/0/0
[Huawei-GigabitEthernet1/0/0] ip accounting input-packets
[Huawei-GigabitEthernet1/0/0] ip accounting precedence input-packets
```

Related Topics

21.13.3 display ip accounting precedence

21.13.9 ip accounting rule

Function

The **ip accounting rule** command creates IP accounting rules.

The **undo ip accounting rule** command deletes IP accounting rules.

By default, no IP accounting rule is configured.

Format

ip accounting rule *ip-address* { *mask* | *mask-length* }

undo ip accounting rule [*ip-address* { *mask* | *mask-length* }]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
ip-address	Indicates the IP address in an IP accounting rule.	The value is in dotted decimal notation.
mask	Indicates the subnet mask in an IP accounting rule.	The value is in dotted decimal notation.
mask-length	Indicates the mask length.	The value is an integer that ranges from 0 to 32.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

After the **ip accounting rule** command is executed, statistics about the packets with source or destination addresses matching the IP accounting rule are recorded in the matched table. Statistics about the packets not matching the IP accounting rule are recorded in the mismatched table.

Precautions

IP accounting contains a maximum of 32 rules. When an IP packet matches any IP accounting rule, statistics about the packet are recorded in the matched table.

NOTE

IP precedence accounting does not have rules.

Example

Collect statistics about the packets with source or destination address 192.168.0.1/32.

```
<Huawei> system-view
[Huawei] ip accounting rule 192.168.0.1 255.255.255.255
```

Related Topics

21.13.4 display ip accounting rule

 Copyright © Huawei Technologies Co., Ltd.

21.13.10 ip accounting timeout

Function

The **ip accounting timeout** command sets the aging time for IP accounting statistics records.

The **undo ip accounting timeout** command restores the default aging time of IP accounting statistics records.

By default, the aging time of IP accounting statistics records is 720 minutes (12 hours).

Format

ip accounting timeout *time-value*

undo ip accounting timeout

Parameters

Parameter	Description	Value
time-value	Indicates the aging time of IP accounting statistics records.	The value is an integer that ranges from 60 to 10080, in minutes. The default value is 720.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

If a statistics record is not updated within the aging time, the record is aged out and deleted.

Precautions

The aging time does not apply to IP precedence accounting. The records in the statistics table of IP precedence accounting can only be deleted manually using the **reset ip accounting precedence** command.

Example

Set the aging time of IP accounting statistics records to 60 minutes.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> system-view
[Huawei] ip accounting timeout 60
```

21.13.11 reset ip accounting

Function

The **reset ip accounting** command clears IP accounting statistics.

Format

reset ip accounting { **all** | **matched** | **mismatched** | **precedence** }

Parameters

Parameter	Description	Value
all	Clears all statistics tables.	-
matched	Clears the matched table. **NOTE** The matched table stores statistics about the packets matching the IP accounting rules.	-
mismatched	Clears the mismatched table. **NOTE** The mismatched table stores: ● Statistics about the packets not matching the IP accounting rules. ● Common IP accounting statistics if no IP accounting rule is configured.	-
precedence	Clears the statistics table of IP precedence accounting. **NOTE** This table stores the statistics records of IP precedence accounting.	-

Views

User view

Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Precautions

Before collecting packet statistics, you should clear existing statistics records; otherwise, statistics are inaccurate. If you do not clear them, the records will not be deleted until the aging time expires.

Example

Clear all statistics tables.

```
<Huawei> reset ip accounting all
```

Related Topics

21.13.1 display ip accounting input-packets

21.13.2 display ip accounting output-packets

21.14 TWAMP Light Configuration Commands

NOTE

AR3670 do not support TWAMP Light.

21.14.1 client

Function

The **client** command enables the TWAMP Light Client function and displays the Client view. If the Client function has been enabled, this command directly displays the Client view.

The **undo client** command disables the TWAMP Light Client function.

By default, the TWAMP Light Client function is disabled.

Format

client

undo client

Parameters

None

Views

TWAMP-Light view

 Copyright © Huawei Technologies Co., Ltd.

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the TWAMP Light service, run the **client** command to display the Client view and create a TWAMP Light session. The measurement service is started based on the session configuration.

Precautions

When the TWAMP Light Client function is disabled, all TWAMP Light sessions are deleted and the measurement service is stopped.

Example

Enable the TWAMP Light Client function.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] client
[Huawei-twamp-light-client]
```

21.14.2 display twamp-light responder test-session

Function

The **display twamp-light responder test-session** command displays real-time measurement session information on the TWAMP Light reflector.

Format

display twamp-light responder test-session [**verbose** | *session-id*]

Parameters

Parameter	Description	Value
verbose	Displays details about a measurement session on the TWAMP Light reflector.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
session-id	Displays real-time information about the specified measurement session on the TWAMP Light reflector.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

After the continual or on-demand performance measurement function is enabled, you can run this command to view real-time measurement session information on the TWAMP Light reflector if you want to check the measurement session configuration or locate the fault in measurement.

Example

Display the summary of all measurement sessions.

```
<Huawei> display twamp-light responder test-session
Total number  : 5
--------------------------------------------------------------------------------
 ID    Local-IP       Local-Port    Remote-IP      Remote-Port
--------------------------------------------------------------------------------
  2    192.168.1.1        10000     192.168.1.6        20000
  3    192.168.1.2        10000     192.168.1.6        20000
  4    192.168.1.3        10000     192.168.1.6        20000
  5    192.168.1.4        10000     192.168.1.6        20000
  6    192.168.1.5        10000     192.168.1.6        20000
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-79 Description of the **display twamp-light responder test-session** command output

Item	Description
Total number	Total number of sessions.
ID	Measurement session ID.
Local-IP	IP address of the session reflector.
Local-Port	UDP port number of the session reflector.
Remote-IP	IP address of the session sender.
Remote-Port	UDP port number of the session sender.

Display details about all measurement sessions.

```
<Huawei> display twamp-light responder test-session verbose
Session ID                  : 1
Local IP                    : 192.168.1.1
Local Port                  : 10000
Remote IP                   : 192.168.1.6
Remote Port                 : 20000
Mode                        : unauthenticated
VPN Instance                :
Description                 : test

Session ID                  : 2
Local IP                    : 192.168.1.2
Local Port                  : 10000
Remote IP                   : 192.168.1.6
Remote Port                 : 20000
Mode                        : unauthenticated
VPN Instance                :
Description                 : test
```

Table 21-80 Description of the **display twamp-light responder test-session verbose** command output

Item	Description
Session ID	Measurement session ID.
Local IP	IP address of the session reflector.
Local Port	UDP port number of the session reflector.
Remote IP	IP address of the session sender.
Remote Port	UDP port number of the session sender.

 Copyright © Huawei Technologies Co., Ltd.

Item	Description
Mode	Authentication mode. The value **unauthenticated** indicates that authentication is disabled.
VPN Instance	L3VPN instance name.
Description	Measurement session description.

21.14.3 display twamp-light statistic-type

Function

The **display twamp-light statistic-type** command displays bidirectional delay or packet loss statistics of the TWAMP Light sessions.

Format

display twamp-light statistic-type { **twoway-delay** | **twoway-loss** } **test-session** *session-id*

Parameters

Parameter	Description	Value
twoway-delay	Displays statistics about bidirectional delay measurement.	–
twoway-loss	Displays statistics about bidirectional packet loss measurement.	–

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
test-session *session-id*	Displays statistics about the specified session.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

To view statistics on a measurement session, run this command. The command output contains bidirectional delay or packet loss statistics on the TWAMP Light session.

Example

Display bidirectional delay statistics on the specified measurement session.

```
<Huawei> display twamp-light statistic-type twoway-delay test-session 1
Latest two-way delay statistics(usec):
--------------------------------------------------------------------------------
    Index      Delay(Avg)     Jitter(Avg)        Tx-Jitter(Avg)    Rx-Jitter(Avg)
--------------------------------------------------------------------------------
    11027          0              0                 0                 0
    11028          0              0                 0                 0
    11029          4              4                 4                 4
    11030          1              1                 1                 1
    11031          1              1                 1                 1
    11032          1              1                 1                 1
    11033          0              0                 0                 0
    11034          1              1                 1                 1
    11035          2              2                 2                 2
```

 Copyright © Huawei Technologies Co., Ltd.

```
    11036        2          2              2              2
    11037        0          0              0              0
    11038        2          2              2              2
    11039        1          1              1              1
    11040        0          0              0              0
    11041        0          0              0              0
    11042        0          0              0              0
    11043        0          0              0              0
    11044        1          1              1              1
    11045        3          3              3              3
    11046        0          0              0              0
    11047        1          1              1              1
    11048        0          0              0              0
    11049        0          0              0              0
    11050        0          0              0              0
    11051        1          1              1              1
    11052        0          0              0              0
    11053        5          5              5              5
    11054        7          7              7              7
    11055        0          0              0              0
    11056        1          1              1              1
--------------------------------------------------------------------------------
Average Delay    :          1    Average Jitter   :          1
Maximum Delay    :          7    Maximum Jitter   :          7
Minimum Delay    :          0    Minimum Jitter   :          0
Average TxJitter :          1    Average RxJitter :          1
Maximum TxJitter :          7    Maximum RxJitter :          7
Minimum TxJitter :          0    Minimum RxJitter :          0
```

Table 21-81 Description of the **display twamp-light statistic-type twoway-delay** command output

Item	Description
Latest two-way delay statistics(usec)	Bidirectional delay measurement statistics, in microsecond.
Index	Statistics sequence number.
Delay(Avg)	Average delay.
Jitter(Avg)	Average jitter.
Tx-Jitter(Avg)	Average jitter on the sender.
Rx-Jitter(Avg)	Average jitter on the receiver.
Average Delay	Average delay.
Average Jitter	Average jitter.
Maximum Delay	Maximum delay.
Maximum Jitter	Maximum jitter.
Minimum Delay	Minimum delay.
Minimum Jitter	Minimum jitter.
Average TxJitter	Average jitter on the sender.
Average RxJitter	Average jitter on the receiver.
Maximum TxJitter	Maximum jitter on the sender.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Maximum RxJitter	Maximum jitter on the receiver.
Minimum TxJitter	Minimum jitter on the sender.
Minimum RxJitter	Minimum jitter on the receiver.

NOTE

- The statistics includes the packet sampling point and accumulative statistics. On-demand statistics includes the recent 100 sampling points and continual statistics includes the recent 30 sampling points.
- The delay, jitter, and unidirectional jitter are the average values of the sampling point.
- The maximum, minimum, and average values in on-demand and continual measurement are accumulative values, so it is a normal situation that the values exceed the acceptable range of the sampling point.
- The interval for displaying sampling result is relevant to the configured packet sending interval. If the sending interval is set to 100 ms, the sampling result is displayed every second. If the sending interval is set to 1000 ms, the sampling result is displayed every 10s.

Display bidirectional packet loss statistics on the specified measurement session.

```
<Huawei> display twamp-light statistic-type twoway-loss test-session 1
Latest two-way loss statistics:
--------------------------------------------------------------------------------
    Index      Loss count      Loss ratio
--------------------------------------------------------------------------------
    11006            5        50.0000%
    11007            3        30.0000%
    11008            4        40.0000%
    11009            8        80.0000%
    11010           10       100.0000%
    11011            1        10.0000%
    11012           10       100.0000%
    11013            2        20.0000%
    11014           10       100.0000%
    11015            9        90.0000%
    11016            6        60.0000%
    11017            2        20.0000%
    11018            8        80.0000%
    11019            2        20.0000%
    11020            8        80.0000%
    11021            2        20.0000%
    11022            2        20.0000%
    11023            7        70.0000%
    11024            4        40.0000%
    11025            4        40.0000%
    11026            7        70.0000%
    11027            7        70.0000%
    11028            8        80.0000%
    11029            1        10.0000%
    11030            2        20.0000%
    11031            8        80.0000%
    11032            7        70.0000%
    11033            7        70.0000%
    11034            8        80.0000%
    11035            4        40.0000%
--------------------------------------------------------------------------------
Average Loss Count :         5    Average Loss Ratio :  55.3333%
```

 Copyright © Huawei Technologies Co., Ltd.

```
Maximum Loss Count :        10    Maximum Loss Ratio : 100.0000%
Minimum Loss Count :         1    Minimum Loss Ratio :  10.0000%
```

Table 21-82 Description of the **display twamp-light statistic-type twoway-loss** command output

Item	Description
Latest two-way loss statistics	Bidirectional packet loss statistics.
Loss count	Number of dropped packets.
Loss ratio	Packet loss rate.
Average Loss Count	Average number of dropped packets.
Average Loss Ratio	Average packet loss rate.
Maximum Loss Count	Maximum number of dropped packets.
Maximum Loss Ratio	Maximum packet loss rate.
Minimum Loss Count	Minimum number of dropped packets.
Minimum Loss Ratio	Minimum packet loss rate.

NOTE

- The statistics includes the packet sampling point and accumulative statistics. On-demand statistics includes the recent 100 sampling points and continual statistics includes the recent 30 sampling points.
- The delay, jitter, and unidirectional jitter are the average values of the sampling point.
- The maximum, minimum, and average values in on-demand and continual measurement are accumulative values, so it is a normal situation that the values exceed the acceptable range of the sampling point.
- The interval for displaying sampling result is relevant to the configured packet sending interval. If the sending interval is set to 100 ms, the sampling result is displayed every second. If the sending interval is set to 1000 ms, the sampling result is displayed every 10s.

21.14.4 display twamp-light test-session

Function

The **display twamp-light test-session** command displays real-time information about TWAMP Light sessions.

Format

display twamp-light test-session [**verbose** | *session-id*]

Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
verbose	Displays details about a TWAMP Light session.	-
session-id	Displays real-time information about the specified TWAMP Light session.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.

Views

All views

Default Level

1: Monitoring level

Usage Guidelines

When a fault occurs in continual measurement, on-demand measurement, or measurement session, run this command to view real-time information about the TWAMP Light sessions.

Example

Display the summary of all measurement sessions.

```
<Huawei> display twamp-light test-session
Total number  : 2
Active number : 1
--------------------------------------------------------------------------------
  ID       Sender-IP   Sender-Port     Reflector-IP    Reflector-Port  State
--------------------------------------------------------------------------------
   1        1.1.1.1        2001        2.2.2.2            2010   active
   2        1.1.1.1        2001        3.3.3.3            2020   inactive
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-83 Description of the **display twamp-light test-session** command output

Item	Description
Total number	Total number of sessions.
Active number	Number of sessions in continual or on-demand measurement.
ID	Measurement session ID.
Sender-IP	IP address of the session sender.
Sender-Port	UDP port number of the session sender.
Reflector-IP	IP address of the session reflector.
Reflector-Port	UDP port number of the session reflector.
State	The states of measurement sessions include: ● active: indicates that continual or on-demand measurement is enabled. ● inactive: indicates that continual or on-demand measurement is not enabled or not normally enabled. – not startup: indicates that measurement is not enabled. – absence of resource: indicates that there is a lack of resources such as boards. – board fault: indicates a board failure. **NOTE** If the **State** value is active, the number of sent and received packets is the real-time result. If the **State** value is inactive, the number of sent and received packets is the last query result when the state is active.

Display details about all measurement sessions.

```
<Huawei> display twamp-light test-session verbose
Session ID                  : 1
State                       : active
Type                        : continual
Sender IP                   : 1.1.1.1
Sender Port                 : 2001
Reflector IP                : 2.2.2.2
Reflector Port              : 2010
Mode                        : unauthenticated
DSCP                        : 0
```

 Copyright © Huawei Technologies Co., Ltd.

```
Padding Length                  : 128
VPN Instance                    :
Last Start Time                 : 2014-08-05 16:41:05-08:00
Last Stop Time                  : never
Period Time(in millisecond)     : 100
Time Out(in second)             : 5
Duration Time(in second)        : -
Packet Count                    : -
Sequence Number                 : 0
Test Tx Number                  : 0
Test Rx Number                  : 0
Test Discard Number             : 0

Session ID                      : 2
State                           : inactive(absence of resource)
Type                            : on-demand
Sender IP                       : 1.1.1.1
Sender Port                     : 2001
Reflector IP                    : 3.3.3.3
Reflector Port                  : 2020
Mode                            : unauthenticated
DSCP                            : 0
Padding Length                  : 128
VPN Instance                    :
Last Start Time                 : never
Last Stop Time                  : never
Period Time(in millisecond)     : 100
Time Out(in second)             : 8
Duration Time(in second)        : 300
Packet Count                    : 0
Sequence Number                 : 0
Test Tx Number                  : 0
Test Rx Number                  : 0
Test Discard Number             : 0
```

Table 21-84 Description of the **display twamp-light test-session verbose** command output

Item	Description
Session ID	Measurement session ID.
Type	Measurement session type: ● on-demand ● continual
Sender IP	IP address of the session sender.
Sender Port	UDP port number of the session sender.
Reflector IP	IP address of the session reflector.
Reflector Port	UDP port number of the session reflector.
Mode	Authentication mode. The value **unauthenticated** indicates that authentication is disabled.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
DSCP	Differentiated Services Code Point (DSCP) value of the measurement session.
Padding Length	Padding length of the measurement session.
VPN Instance	L3VPN instance name.
Last Start Time	Latest activation time.
Last Stop Time	Latest stop time.
Period Time(in millisecond)	Measurement interval of a session, in millisecond.
Time Out(in second)	Timeout interval, in seconds.
Duration Time(in second)	Packet sending duration, displayed only for on-demand measurement, in seconds.
Packet Count	Number of sent packets, displayed only for on-demand measurement.
Sequence Number	Latest sequence number.
Test Tx Number	Accumulative number of sent packets.
Test Rx Number	Accumulative number of received packets.
Test Discard Number	Accumulative number of dropped invalid packets.

Display details about the specified measurement session.

```
<Huawei> display twamp-light test-session 1
Session ID                      : 1
State                           : active
Type                            : continual
Sender IP                       : 1.1.1.1
Sender Port                     : 2001
Reflector IP                    : 2.2.2.2
Reflector Port                  : 2010
Mode                            : unauthenticated
DSCP                            : 0
Padding Length                  : 128
VPN Instance                    :
Last Start Time                 : 2014-08-05 16:41:05-08:00
Last Stop Time                  : never
Period Time(in millisecond)     : 100
Time Out(in second)             : 5
Duration Time(in second)        : -
Packet Count                    : -
Sequence Number                 : 0
Test Tx Number                  : 0
Test Rx Number                  : 0
Test Discard Number             : 0
```

 Copyright © Huawei Technologies Co., Ltd.

Related Topics

21.14.8 test start

21.14.9 test start-continual

21.14.5 nqa twamp-light

Function

The **nqa twamp-light** command creates the TWAMP Light service and displays the TWAMP-Light view. If the TWAMP-Light service already exists, the TWAMP-Light view is directly displayed.

The **undo nqa twamp-light** command deletes the TWAMP Light service.

By default, the TWAMP Light service is not created.

Format

nqa twamp-light

undo nqa twamp-light

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TWAMP Light uses a light structure to simplify the protocol used to set up performance measurement sessions. It measures bidirectional IP performance between any network nodes. When the TWAMP Light service is required, run the **nqa twamp-light** command to create the TWAMP Light service.

Precautions

After you run the **undo nqa twamp-light** command, the device automatically deletes all measurement sessions and services on client and sender.

Example

Create the TWAMP Light service.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light]
```

 Copyright © Huawei Technologies Co., Ltd.

21.14.6 responder

Function

The **responder** command enables the TWAMP Light Responder function and displays the Responder view. If the Responder function has been enabled, this command directly displays the Responder view.

The **undo responder** command disables the TWAMP Light Responder function.

By default, the TWAMP Light Responder function is disabled.

Format

responder

undo responder

Parameters

None

Views

TWAMP-Light view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the TWAMP Light service, run the **responder** command on the responder to display the responder view and create a measurement session. Then the controller starts the measurement service based on the session configuration.

Precautions

After the TWAMP Light responder is deleted, the packet loss rate is displayed as 100%, which is inaccurate.

Example

Enable the TWAMP Light responder function.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] responder
[Huawei-twamp-light-responder]
```

 Copyright © Huawei Technologies Co., Ltd.

21.14.7 sender

Function

The **sender** command enables the TWAMP Light Sender function and displays the Sender view. If the Sender function has been enabled, this command directly displays the Sender view.

The **undo sender** command disables the TWAMP Light Sender function.

By default, the TWAMP Light Sender function is disabled.

Format

sender

undo sender

Parameters

None

Views

TWAMP-Light view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To use the TWAMP Light service, create the TWAMP Light Sender using the **sender** command, and then start the measurement service on Sender.

Precautions

- When starting the measurement service, ensure that the TWAMP Light session has been created on the Client.
- When you delete the Sender, only the continual measurement service is stopped, but the on-demand measurement service will not be stopped. The on-demand measurement stops only when the specified interval is expired or a certain number of packets are sent.

Example

Display the Sender view.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender]
```

 Copyright © Huawei Technologies Co., Ltd.

21.14.8 test start

Function

The **test start** command sets the time range or number of packets for the on-demand measurement service.

Format

test start test-session *session-id* { **duration** *duration* | **packet-count** *packet-count* } [**period** { **10** | **100** | **1000** | **30000** }] [**time-out** *time-out*]

Parameters

Parameter	Description	Value
test-session *session-id*	Specifies the ID of the measurement session.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.
duration *duration*	Specifies the packet sending duration of the measurement session.	The value is an integer that ranges from 60 to 300, in seconds.
packet-count *packet-count*	Specifies the number of packets sent in the measurement session.	The value is an integer that ranges from 100 to 30000.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
period	Specifies the interval for sending packets.	The value is an integer, in millisecond. The default value is 100 ms.
10	Sets the interval for sending packets to 10 ms.	-
100	Sets the interval for sending packets to 100 ms.	-
1000	Sets the interval for sending packets to 1s.	-
30000	Sets the interval for sending packets to 30s.	-
time-out *time-out*	Specifies the timeout interval for response packets within the sampling interval.	The value is an integer that ranges from 1 to 10, in seconds. By default, the value is 5s.

Views

TWAMP-Light-Sender view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TWAMP Light includes two modes: on-demand and continual. On-demand measurement indicates that performance measurement is started manually within the specified time range aiming at network fault diagnosis. It is a one-off measurement in the diagnosis period. Continual measurement indicates the measurement is performed continuously.

- To measure performance only once, enable on-demand measurement by running the **test start** command. The measurement stops when the specified interval is expired or a certain number of packets are sent.
- To measure performance continuously, enable continual measurement by running the **test start-continual** command.

Prerequisites

 Copyright © Huawei Technologies Co., Ltd.

A session has been created on Client.

Precautions

On-demand measurement fails in the following situations:

- More than 64 measurement sessions are configured.
- On-demand measurement is started during continual measurement.
- The measurement command is successfully executed, but the measurement fails to start due to a lack of resource, such as boards. In this situation, the **display twamp-light test-session** command displays the **State** value as inactive.

Example

Set the number of sent packets to 30000 to enable on-demand measurement.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender] test start test-session 1 packet-count 30000
```

Related Topics

21.14.9 test start-continual

21.14.4 display twamp-light test-session

21.14.9 test start-continual

Function

The **test start-continual** command configures continual measurement.

The **undo test start-continual** command stops continual measurement.

Format

test start-continual test-session *session-id* [**period** { **10** | **100** | **1000** | **30000** } [**sample-interval** *interval-value*]] [**time-out** *time-out*]

undo test start-continual test-session *session-id*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
test-session *session-id*	Specifies the ID of the measurement session.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.
period	Specifies the interval for sending packets.	The value is an integer, in millisecond. The default value is 100 ms.
10	Sets the interval for sending packets to 10 ms.	-
100	Sets the interval for sending packets to 100 ms.	-
1000	Sets the interval for sending packets to 1s.	-
30000	Sets the interval for sending packets to 30s.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
sample-interval *interval-value*	Specifies a sampling interval.	The value is an integer, in seconds. **NOTE** The sampling interval varies according to the interval at which packets are sent over a test session. ● If the packet sending interval is 10 ms, the sampling interval is 1s. ● If the packet sending interval is 100 ms, the sampling interval ranges from 1s to 10s, with the default value being 1s. ● If the packet sending interval is 1s, the sampling interval ranges from 10s to 100s, with the default value being 10s. ● If the packet sending interval is 30s, the sampling interval ranges from 60s to 300s, with the default value being 60s. **sample-interval** *interval-value* must be less than or equal to **duration** *duration*.
time-out *time-out*	Specifies the timeout interval for response packets within the sampling interval.	The value is an integer that ranges from 1 to 10, in seconds. By default, the value is 5s.

Views

TWAMP-Light-Sender view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

TWAMP Light includes two modes: on-demand and continual. On-demand measurement indicates that performance measurement is started manually within the specified time range aiming at network fault diagnosis. It is a one-off measurement in the diagnosis period. Continual measurement indicates the measurement is performed continuously.

- To measure performance only once, enable on-demand measurement by running the **test start** command. The measurement stops when the specified interval is expired or a certain number of packets are sent.
- To measure performance continuously, enable continual measurement by running the **test start-continual** command.

Prerequisites

A session has been created on Client.

 Copyright © Huawei Technologies Co., Ltd.

Precautions

- When a measurement session is deleted, the continual measurement configuration of this session is also deleted.
- After the Sender is deleted, all continual measurement configurations are deleted.
- If you enable continual measurement during an on-demand measurement, the on-demand measurement immediately stops and the continual measurement starts.
- The measurement command is successfully executed, but the measurement fails to start due to a lack of resource, such as boards. In this situation, the **display twamp-light test-session** command displays the **State** value as inactive.

Example

Start continual measurement for a session.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender] test start-continual test-session 1
```

Related Topics

21.14.8 test start

21.14.4 display twamp-light test-session

21.14.10 test stop

Function

The **test stop** command stops on-demand measurement of the TWAMP Light service.

Format

test stop { **all** | **test-session** *session-id* }

Parameters

Parameter	Description	Value
all	Stops on-demand measurement for all sessions.	–

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
test-session *session-id*	Specifies the ID of the measurement session to be stopped.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.

Views

TWAMP-Light-Sender view

Default Level

2: Configuration level

Usage Guidelines

To stop on-demand measurement for the specified session or all sessions, you can run the **test stop** command.

Example

Stop on-demand measurement for session 1.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] sender
[Huawei-twamp-light-sender] test stop test-session 1
```

21.14.11 test-session

Function

The **test-session** command creates a session in the TWAMP Light service.

The **undo test-session** command deletes a session in the TWAMP Light service.

By default, no measurement session is created.

 Copyright © Huawei Technologies Co., Ltd.

Format

test-session *session-id* **sender-ip** *sender-ip-address* **reflector-ip** *reflector-ip-address* **sender-port** *sender-port* **reflector-port** *reflector-port* [**vpn-instance** *vpn-instance-name*] [**dscp** *dscp-value* | **padding** *padding-length* | **description** *description*] *

undo test-session *session-id*

Parameters

Parameter	Description	Value
session-id	Specifies the ID of the measurement session.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.
sender-ip *sender-ip-address*	Specifies the IP address of the sender.	The value is in dotted decimal notation.
reflector-ip *reflector-ip-address*	Specifies the IP address of the reflector.	The value is in dotted decimal notation.
sender-port *sender-port*	Specifies the UDP port number of the sender.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
reflector-port *reflector-port*	Specifies the UDP port number of the reflector.	The value is 862, 863, or an integer that ranges from 1025 to 65535.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.
dscp *dscp-value*	Specifies the DSCP value of sent packets.	The value is an integer that ranges from 0 to 63. The default value is 0.
padding *padding-length*	Specifies the padding length of the measurement session.	The value is an integer that ranges from 32 to 8500. The default value is 128.
description *description*	Indicates the description of the specified measurement session. To configure description for a measurement session, specify the **description** parameter. The description facilitates session management and operation.	The value is a string of 3 to 32 characters without spaces. **NOTE** If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

TWAMP-Light-Client view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you need to use the TWAMP Light service, create a TWAMP Light session, including the sender's IP address, reflector's IP address, sender's UDP port number, reflector's UDP port number, and VPN instance name. The created session starts measurement only when the start command is run.

Precautions

- After a session is created, its parameters cannot be modified. To modify the session parameters, delete the session and create it again.

 Copyright © Huawei Technologies Co., Ltd.

- The IP address must be a unicast address.
- The UDP port of the sender must be a port that is not occupied.
- All the parameters related to the VPN instance must exist. When the VPN instance is deleted, the related measurement instance is also deleted.
- To configure a session with multiple DSCP values, you can specify different UDP port numbers for sender. The following are two examples:
  - Session 1: **test-session** 1 **sender-ip** 1.1.1.1 **reflector-ip** 2.2.2.2 **sender-port** 1025 **reflector-port** 1025 **dscp** 3
  - Session 2: **test-session** 2 **sender-ip** 1.1.1.1 **reflector-ip** 2.2.2.2 **sender-port** 1026 **reflector-port** 1025 **dscp** 6

Example

Create a TWAMP Light session.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] client
[Huawei-twamp-light-client] test-session 1 sender-ip 1.1.1.1 reflector-ip 2.2.2.2 sender-port 3000
reflector-port 3000
```

21.14.12 test-session (TWAMP-Light-Responder view)

Function

The **test-session** command creates a session on the TWAMP Light reflector.

The **undo test-session** command deletes a session on the TWAMP Light reflector.

By default, no measurement session is created on the reflector.

Format

test-session *session-id* **local-ip** *local-ip-address* **remote-ip** *remote-ip-address* **local-port** *local-port* **remote-port** *remote-port* [**vpn-instance** *vpn-instance-name*] [**description** *description*]

undo test-session *session-id* [**local-ip** *local-ip-address* **remote-ip** *remote-ip-address* **local-port** *local-port* **remote-port** *remote-port* [**vpn-instance** *vpn-instance-name*] [**description** *description*]]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
session-id	Specifies the ID of the measurement session.	The value is an integer. ● For AR100&AR120&AR150&AR160&AR200, the value ranges from 1 to 64. ● For AR1200 series, the value ranges from 1 to 128. ● For AR2200 series (except AR2240 and AR2240C), the value ranges from 1 to 1024. ● For AR2240C, the value ranges from 1 to 256. ● AR2240, AR3200 series: – For the AR3200 with SRU40, SRU80, SRU100, or SRU100E, the value ranges from 1 to 512. – For the AR3200 with SRU200E or SRU200, the value ranges from 1 to 1024. – For the AR3200 with SRU400, the value ranges from 1 to 2048. ● For AR3600 series, the value ranges from 1 to 1024.
local-ip *local-ip-address*	Specifies the IP address of the reflector.	The value is in dotted decimal notation.
remote-ip *remote-ip-address*	Specifies the IP address of the sender.	The value is in dotted decimal notation.
local-port *local-port*	Specifies the UDP port number of the reflector.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
remote-port *remote-port*	Specifies the UDP port number of the sender.	The value is 862, 863, or an integer that ranges from 1025 to 65535.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
description *description*	Indicates the description of the specified measurement session. To configure description for a measurement session, specify the **description** parameter. The description facilitates session management and operation.	The value is a string of 3 to 32 case-sensitive characters without spaces. If the string is enclosed in double quotation marks (" "), the string can contain spaces.

Views

TWAMP-Light-Responder view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When you need to use the TWAMP Light service, create a TWAMP Light session on the reflector, including the sender's IP address, reflector's IP address, sender's UDP port number, reflector's UDP port number, and VPN instance name.

Precautions

- The created session starts measurement only when the start command is run.
- After a measurement session is created, its parameters cannot be modified.
- The IP address must be a unicast address.
- The UDP port of the sender must be a port that is not occupied.
- The VPN instance parameters must already exist.

Example

Create a TWAMP Light session on the reflector.

```
<Huawei> system-view
[Huawei] nqa twamp-light
[Huawei-twamp-light] responder
[Huawei-twamp-light-responder] test-session 1 local-ip 1.1.1.1 remote-ip 2.2.2.2 local-port 3000 remote-port 3000 vpn-instance vpn1
```

 Copyright © Huawei Technologies Co., Ltd.

21.15 Ping and Tracert Configuration Commands

21.15.1 ping

Function

The **ping** command checks whether a specified IPv4 address is reachable and exports corresponding statistics.

Format

ping [**ip**] [**-a** *source-ip-address* | **-c** *count* | **-d** | **-h** *ttl-value* | { **-nexthop** *nexthop-ip-address* | **-i** *interface-type interface-number* } * | **-m** *time* | **-n** | **-name** | **-p** *pattern* | **-q** | **-r** | { **-s** *packetsize* | **-range** [**min** *min-size* | **max** *max-size* | **step** *step-size*] * } | **-system-time** | **-t** *timeout* | **-tos** *tos-value* | **-v** | **-vpn-instance** *vpn-instance-name* | [**-f** | **ignore-mtu**]] * *host* [**ip-forwarding**]

Parameters

Parameter	Description	Value
ip	Indicates the IPv4 protocol. If **ip** is not specified, the IPv4 protocol is used.	-
-a *source-ip-address*	Specifies the source IP address of the ICMP Echo Request message. If the source IP address is not specified, the IP address of the outbound interface is used as the source IP address of the ICMP Echo Request message.	The value is in dotted decimal notation. The IP address must be a valid A, B, or C class address.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-c *count*	Specifies the number of times for sending ICMP Echo Request messages. The **ping** command labels each ICMP Echo Request message with a sequence ID that starts from 1 and is increased by 1. By default, five ICMP Echo Request messages are sent. You can set the number of ICMP Echo Request messages to send by specifying the parameter *count*. In the case of poor network quality, you can set this parameter to a comparatively large value to check the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-d	Indicates that the socket works in debug mode.	By default, the socket works in non-debug mode.
-f	Indicates that packets are not fragmented during transmission. **NOTE** After this parameter is specified, ICMP packets are not fragmented. If the ICMP packet size exceeds the link MTU, the ICMP packet is discarded. If you do not want ICMP packets to be discarded, do not specify this parameter or increase the link MTU.	-
-h *ttl-value*	Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 device that the message reaches sends an ICMP timeout message to the source host, indicating that the destination host is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 255.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value

-nexthop *nexthop-ip-address*	Specifies an IP address for the next hop.
	If you have specified this parameter, the device no longer searches the routing table before sending ICMP Echo Request packets. This process prevents ping failures caused by incorrect routing entries.
		The value is in dotted decimal notation.
		NOTE
		• The specified next hop address must be the next hop address of a directly connected physical interface.
		• When you specify a next hop address, you can configure **-i** *interface-type interface-number* to specify an outbound interface. The following conditions must be met to ensure a test success:
		  • The specified next hop address must match the outbound interface.
		  • The specified outbound interface cannot be a logical interface's member interface.
		• If you have specified a next hop address, you cannot specify a VPN.

-i *interface-type interface-number*	Specifies the outbound interface for sending ICMP Echo Request messages.	**NOTE** • In load balancing scenarios, if an interface is specified to send ICMP Echo Request packets, all packets are sent from the interface and load balancing is not performed. • The interface specified to send ICMP Echo Request packets must be a Layer 3 interface, such as a VLANIF interface, Eth-trunk interface, or a Layer 3 Eth-trunk member interface.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-m *time*	Specifies the time to wait before sending the next ICMP Echo Request message. Each time the source sends an ICMP Echo Request message using the **ping** command, the source waits a period of time (500 ms by default) before sending the next ICMP Echo Request message. You can set the time to wait before sending the next ICMP Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 500, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 500.
-n	Uses the value of *host* as the IP address to spare domain name resolution.	-
-name	Displays the name of the destination host.	-
-p *pattern*	Specifies pad characters for ICMP Echo Request messages. By configuring pad characters for ICMP Echo Request messages, you can identify a specific message among the large number of received ICMP Echo Reply messages.	The value is a hexadecimal integer that ranges from 0 to FFFFFFFF. By default, the padding starts from 0x01, and continues in ascending order.
-q	Displays only the statistics. If the **ping** command carries this parameter, the system displays only the statistics information such as the number of sent and received packets, packet loss rate, and minimum, average, and maximum RTTs of the packet.	By default, the system displays all statistics information.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-r	Records the route along which an IP packet is forwarded. When **-r** is specified, during the transmission of an IP packet, the IP address of each Layer 3 device that the IP packet passes through is added to the Options field. When the IP packet reaches the destination, all IP addresses recorded in the Options field are copied to the ICMP Echo Reply message. In addition, the IP address of each Layer 3 device that the returned IP packet passes through is added to the message. When the ping program receives the ICMP Echo Reply message, IP addresses of the passed Layer 3 devices are displayed.	By default, the route along which an IP packet is forwarded is not recorded.
-s *packetsize*	Specifies the length of an ICMP Echo Request message, excluding the IP header and ICMP header.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-range	Enables the device to send ICMP Echo Request messages with variable payload lengths.	• If the **-range** parameter is not specified, the payload length of an ICMP Echo Request message is equal to the length specified by the **-s** *packetsize* parameter. The default value is 56, in bytes. • If the **-range** parameter is specified, the payload length of the first ICMP Echo Request message is **min** *min-size*, and that of the second ICMP Echo Request message is **min** *min-size* plus **step** *step-size*. The payload length increases incrementally by **step** *step-size* for subsequent ICMP Echo Request messages until **max** *max-size* is reached. After that, the device will not send ICMP Echo Request messages any more. By default, the payload length of an ICMP Echo Request message ranges from 56 to 9600 bytes, and the step length is 1 byte.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
		NOTE • The command execution takes a long period if a large number of ICMP Echo Request messages need to be sent. If you want to terminate the command execution, press **Ctrl+C**. • To change the number of ICMP Echo Request messages to be sent, change the values of **min** *min-size* and **max** *max-size*. The value of **min** *min-size* must be smaller than that of **max** *max-size*. • If both the **-range** and **-c** *count* parameters are specified, the device sends ICMP Echo Request messages of the same payload length for the number of times specified by the **-c** *count* parameter.
min *min-size*	Specifies the minimum payload length of an ICMP Echo Request message.	The value is an integer ranging from 20 to 9600, in bytes. The default value is 56.
max *max-size*	Specifies the maximum payload length of an ICMP Echo Request message.	The value is an integer ranging from 20 to 9600, in bytes. The default value is 9600.
step *step-size*	Specifies the step length of an ICMP Echo Request message.	The value is an integer ranging from 1 to 1000, in bytes. The default value is 1.
-system-time	Displays the system time when the ping packet is sent.	-

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-t *timeout*	Specifies the timeout period to wait for an ICMP Echo Reply message after an ICMP Echo Request message is sent. After the **ping** command is run, the source sends an ICMP Echo Request message to a destination and waits for an ICMP Echo Reply message. If the destination, after receiving the ICMP Echo Request message, returns an ICMP Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMP Echo Reply message within the specified period, the source displays information indicating that the message times out. Normally, the source receives an ICMP Echo Reply message within 1 to 10 seconds after sending an ICMP Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-tos *tos-value*	Specifies the ToS value of the sent ICMP Echo Request messages. The ToS value is used to set the packet priority.	The value is an integer that ranges from 0 to 255. The default value is 0.
-v	Displays all received ICMP Echo Reply messages. ● If **-v** is not specified, the system displays only the ICMP Echo Reply messages received by the local user. ● If **-v** is specified, the system displays all received ICMP Echo Reply messages.	By default, only ICMP Echo Reply messages for the local user are displayed.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
ignore-mtu	Indicates that the system does not check the interface MTU when a packet is sent.	-
host	Specifies the domain name or IP address of the destination host.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation.
ip-forwarding	Indicates that the ping packets are forcibly forwarded through IP on the first node.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping** command is a common debugging tool for testing the network connectivity by transmitting ICMP Echo messages. It can detect the following items:

- Availability of the remote device
- Round-trip delay in communication between the local and remote devices
- Packet loss rate

You can run the **ping** command to check the network connectivity or line quality in the following scenarios:

- Check the protocol stack on the local device. You can run the **ping** *loopback-address* command to check whether the TCP/IP protocol stack works properly on the local device.

 Copyright © Huawei Technologies Co., Ltd.

- Check whether the destination host is reachable on an IP network. You can run the **ping** *host* command to send an ICMP Echo Request message to the destination host. If a reply is received, the destination host is reachable.
- Check whether the peer is reachable on a Layer 3 VPN. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **ping** *host* command to check whether the peer is reachable. When a VPN instance name is specified, you can run the **ping -vpn-instance** *vpn-instance-name host* command to send an ICMP Echo Request message to the peer. If the peer returns an ICMP Echo Reply message, the peer is reachable.
- In the case of an unstable network, you can run the **ping -c** *count* **-t** *timeout host* command to check the quality of the network between the local device and the peer. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.
- Check the path. You can run the **ping -r** *host* command to obtain information about nodes along the path from the local device to the peer.
- When you want to locate a fault or collect traffic statistics, specify the **-m** and **-t** parameters to allow the device to quickly send **ping** request packets.
- When the packet size is large, specify the **-s** and **-f** parameters to detect the MTU on the intermediate link.
- When IPSec or NAT is used, specify the **-a** parameter to configure the source address as the private network address to check the network connectivity. In addition, to check whether NAT translation succeeds using the ping test with the source address specified, you must run the **ip soft-forward enhance enable** command first to enable the enhanced forwarding function for control packets generated by the device.

Prerequisite

- Before running the **ping** command, ensure that the ICMP module is working properly.
- If **-vpn-instance** is specified, ensure that the VPN module is working properly.

Precautions

- When you use the **ping** command on a third-party device to check the connectivity between the third-party device and the router, set the ping packet size to a value smaller than 64000 bytes to ensure a better test result.
- If an intermediate device is disabled from responding to ICMP messages, detection on this node fails.
- If a fault occurs in the ping process, you can press **Ctrl+C** to terminate the ping operation.
- For security purposes, do not **ping** the broadcast address, such as XX.XX.XX.255.
- When the destination host is unreachable, the system displays "Request time out", which indicates that the ICMP Echo Request message times out.

Example

Check whether the host at 10.1.1.2 is reachable.

 Copyright © Huawei Technologies Co., Ltd.

```
<Huawei> ping 10.1.1.2
  PING 10.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.2: bytes=56 Sequence=1 ttl=255 time=2 ms
    Reply from 10.1.1.2: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 10.1.1.2: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 10.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/1/2 ms
```

Check whether the device at 10.1.1.3 in vpn1 is reachable

```
<Huawei> ping -vpn-instance vpn1 10.1.1.3
  PING 10.1.1.3: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.3: bytes=56 Sequence=1 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=2 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=3 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=4 ttl=255 time=31 ms
    Reply from 10.1.1.3: bytes=56 Sequence=5 ttl=255 time=31 ms
  --- 10.1.1.3 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 31/31/31 ms
```

Check whether the host at 10.1.1.4 is reachable, set the transmission count to 8, and set the period for waiting for an ICMP Echo Reply message to 4000 ms.

```
<Huawei> ping -c 8 -t 4000 10.1.1.4
  PING 10.1.1.4: 56  data bytes, press CTRL_C to break
    Reply from 10.1.1.4: bytes=56 Sequence=1 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=2 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=3 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=4 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=5 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=6 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=7 ttl=255 time=32 ms
    Reply from 10.1.1.4: bytes=56 Sequence=8 ttl=255 time=32 ms
  --- 10.1.1.4 ping statistics ---
    8 packet(s) transmitted
    8 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 32/32/32 ms
```

Table 21-85 Description of the ping command output

Item	Description
PING x.x.x.x	Reachability of the destination host with the IP address as *x.x.x.x* is tested.
x data bytes	Length of a sent ICMP Echo Request message.
press CTRL_C to break	The ongoing ping test is terminated after you press **Ctrl +C**.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
Reply from x.x.x.x	The destination host responds to the ICMP Echo Request message with an ICMP Echo Reply message that contains the following items: • bytes: indicates the length of the ICMP Echo Reply message. • Sequence: indicates the sequence number of the ICMP Echo Reply message. • ttl: indicate the TTL value of the ICMP Echo Reply message. • time: indicates the RTT, in milliseconds. If no ICMP Echo Reply message is received after the timeout period, the system displays "Request time out".
x.x.x.x ping statistics	Statistics collected after the ping test on the destination host. The statistics include the following information: • packet(s) transmitted: indicates the number of sent ICMP Echo Request messages. • packet(s) received: indicates the number of received ICMP Echo Reply messages. • % packet loss: indicates the percentage of unresponded messages to total sent messages. • round-trip min/avg/max: indicates the minimum, average, and maximum RTTs. The unit is ms. (On an IPv4 network, round-trip min/avg/max is not displayed if the ping fails. On an IPv6 network, round-trip min/avg/max = 0/0/0 ms is displayed if the ping fails.)

Related Topics

21.15.2 ping ipv6
21.15.3 tracert
21.15.4 tracert ipv6

21.15.2 ping ipv6

Function

The **ping ipv6** command checks whether a specified IPv6 address is reachable and exports corresponding statistics.

Format

ping ipv6 [**-a** *source-ipv6-address* | **-c** *count* | **-h** *ttl-value* | **-m** *time* | **-name** | **-s** *packetsize* | **-t** *timeout* | **-tc** *traffic-class-value* | **vpn-instance** *vpn-instance-name*] * *host* [**-i** *interface-type interface-number*]

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
-a *source-ipv6-address*	Specifies a source IPv6 address for sending ICMPv6 Echo Request messages. The specified source IPv6 address cannot be the virtual IPv6 address configured for VRRP6. If no source IPv6 address is specified, the IPv6 address of the outbound interface is used as the source address for sending ICMPv6 Echo Request messages.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
-c *count*	Specifies the number of times for sending ICMPv6 Echo Request messages. You can increase the number of outgoing packets to detect the network quality based on the packet loss rate.	The value is an integer that ranges from 1 to 4294967295. The default value is 5.
-h *ttl-value*	Specifies the TTL value. If the TTL field is reduced to 0 during message forwarding, the Layer 3 router that the message reaches sends an ICMPv6 timeout message to the source host, indicating that the destination host is unreachable.	The value is an integer that ranges from 1 to 255. The default value is 255.
-m *time*	Specifies the time to wait before sending the next ICMPv6 Echo Request message. Each time the source sends an ICMPv6 Echo Request message using the **ping ipv6** command, the source waits a period of time (2000 ms by default) before sending the next ICMPv6 Echo Request message. You can set the time to wait before sending the next ICMPv6 Echo Request message using the parameter *time*. In the case of poor network condition, the value should be equal to or larger than 2000, in milliseconds.	The value is an integer that ranges from 1 to 10000, in milliseconds. The default value is 2000.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-name	Displays the name of the destination host.	-
-s *packetsize*	Specifies the length of an ICMPv6 Echo Request message, excluding the IP header and ICMPv6 header.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.
-t *timeout*	Specifies the timeout period to wait for an ICMPv6 Echo Reply message after an ICMPv6 Echo Request message is sent. After the **ping ipv6** command is run, the source sends an ICMPv6 Echo Request message to a destination and waits for an ICMPv6 Echo Reply message. If the destination, after receiving the ICMPv6 Echo Request message, returns an ICMPv6 Echo Reply message to the source within the period specified by the parameter *timeout*, the destination is reachable. If the destination does not return an ICMPv6 Echo Reply message within the specified period, the source displays information indicating that the message times out. Normally, the source receives an ICMPv6 Echo Reply message within 1 to 10 seconds after sending an ICMPv6 Echo Request message. If the transmission speed is low, properly prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 2000.
-tc *traffic-class-value*	Specifies the traffic classification in the ICMPv6 Echo Request message. To configure traffic control for ICMPv6 packets, set the parameter *traffic-class-value*.	The value is an integer that ranges from 0 to 255. The default value is 0.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance for the IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host	Specifies the host name or IPv6 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The IPv6 address is a 32–bit string in hexadecimal format, namely, the format X:X:X:X:X:X:X:X.
-i *interface-type interface-number*	Specifies the outbound interface for sending ICMPv6 Echo Request messages.	-

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

The **ping ipv6** command is a widely used debugging tool for checking network connectivity and host reachability on an IPv6 network by transmitting ICMPv6 messages. It can detect the following items:

- Availability of the remote device
- Round-trip delay in communication between the local and remote devices
- Packet loss rate

You can run the **ping ipv6** command to check the IPv6 network connectivity or line quality in the following scenarios:

- Check the protocol stack on the local device. You can run the **ping ipv6** *IPv6-loopback-address* command to check whether the TCP/IP protocol stack works properly on the local device.
- Check whether the destination IPv6 host is reachable on an IPv6 network. You can run the **ping ipv6** *host* command to send an ICMPv6 Echo Request message to the destination host. If a reply is received, the destination host is reachable.
- Check whether the peer is reachable on a Layer 3 VPN. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **ping ipv6** *host* command to check whether the peer is reachable. When a VPN instance name is specified, you can run the **ping ipv6 vpn-instance** *vpn-instance-name host* command to send an ICMPv6 Echo

 Copyright © Huawei Technologies Co., Ltd.

Request message to the peer. If the peer returns an ICMPv6 Echo Reply message, the peer is reachable.

- In the case of an unstable network, you can run the **ping ipv6 -c** *count* **-t** *timeout host* command to check the quality of the network between the local device and the peer. By analyzing the packet loss rate and average delay in the command output, you can evaluate the network quality. If the network is unreliable, set the packet transmission count (**-c**) and timeout (**-t**) to the upper limits. This makes the test result accurate.

Prerequisites

- Before running the **ping ipv6** command, ensure that the ICMPv6 module is working properly.
- If **-vpn-instance** is specified, ensure that the VPN module is working properly.

Precautions

- If an intermediate device is disabled from responding to ICMPv6 messages, detection on this node fails.
- If the IPv6 address of the destination host maps the local address, specify the name of the local outbound interface through which the ICMPv6 Echo Request message is sent. Otherwise, reply to the **ping ipv6** command times out.
- When the destination host is unreachable, the system displays "Request time out" indicating that the ICMPv6 Echo Request message times out and displays statistics collected by the IPv6 ping test.
- If a fault occurs in the IPv6 ping process, you can press **Ctrl+C** to terminate the IPv6 ping operation.

Example

Check whether the host with the IPv6 address as FC00::1 is reachable.

```
<Huawei> ping ipv6 FC00::1
 PING FC00::1 : 56  data bytes, press CTRL_C to break
    Reply from FC00::1
    bytes=56 Sequence=1 hop limit=64 time=115 ms
    Reply from FC00::1
    bytes=56 Sequence=2 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=3 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=4 hop limit=64 time=1 ms
    Reply from FC00::1
    bytes=56 Sequence=5 hop limit=64 time=1 ms
  ---FC00::1 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max=1/23/115 ms
```

Table 21-86 Description of the ping ipv6 command output

Item	Description
PING HH:HH::HH:H	IPv6 address of the destination host.

Copyright © Huawei Technologies Co., Ltd.

Item	Description
x data bytes	Length of a sent ICMPv6 Echo Request message.
press CTRL_C to break	The ongoing IPv6 ping test is terminated after you press **Ctrl+C**.
Reply from HH:HH::HH:H	The destination host responds to the ICMPv6 Echo Request message with an ICMPv6 Echo Reply message that contains the following items: • bytes: indicates the length of the ICMPv6 Echo Reply message. • sequence: indicates the sequence number of the ICMPv6 Echo Reply message. • hop limit: indicates the TTL of the ICMPv6 Echo Reply message. • time: indicates the RTT, in milliseconds. If no ICMPv6 Echo Reply message is received after the timeout period, the system displays "Request time out".
HH:HH::HH:H ping statistics	Statistics collected after the IPv6 ping test on the destination host. The statistics include the following information: • packet(s) transmitted: indicates the number of sent ICMPv6 Echo Request messages. • packet(s) received: indicates the number of received ICMPv6 Echo Reply messages. • % packet loss: indicates the percentage of unresponded messages to total sent messages. • round-trip min/avg/max: indicates the minimum, average, and maximum RTTs.

Related Topics

21.15.4 tracert ipv6

21.15.3 tracert

Function

The **tracert** command checks the path of packets from the source to the destination, checks network connectivity, and locates a network fault.

Format

tracert [**-a** *source-ip-address* | **-f** *first-ttl* | **-m** *max-ttl* | **-name** | **-p** *port* | **-q** *nqueries* | **-s** *packetsize* | **-v** | **-vpn-instance** *vpn-instance-name* [**pipe**] | **-w** *timeout*] * *host*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
-a *source-ip-address*	Specifies the source address of a probe packet. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address for sending tracert packets.	The value is in dotted decimal notation.
-f *first-ttl*	Specifies the initial TTL. The TTL field is carried in the IP header. It indicates the lifetime of packets and specifies the maximum hops that packets can pass through. The TTL value is set on the source and reduced by 1 each time the packet passes through a hop. When the TTL value is reduced to 0, the packet is discarded. At the same time, an ICMP Timeout message is sent to notify the source host. If *first-ttl* is specified and the number of hops is smaller than the value of *first-ttl*, no ICMP Timeout packet is sent to the source host when the packet passes through these hops. If *max-ttl* is specified, the value of *first-ttl* must be smaller than the value of *max-ttl*.	The value is an integer that ranges from 1 to 255. The default value is 1.
-m *max-ttl*	Specifies the maximum TTL. Usually, the maximum TTL is set to the number of hops the packet passes through. You need to use this parameter to change the TTL. If *first-ttl* is specified, the value of *max-ttl* must be greater than the value of *first-ttl*.	The value is an integer that ranges from 1 to 255. The default value is 30.
-name	Displays the host name of each hop.	-
-p *port*	Specifies the UDP port number of the destination. Before specifying the UDP port number for the destination, ensure that the port is not in use; otherwise, the tracert fails.	The value is an integer that ranges from 0 to 65535. The default value is 33434.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-q *nqueries*	Specifies the number of probe packets to be sent each time. In the case of poor network quality, you can set this parameter to a comparatively large value to ensure that the probe packet can reach the destination.	The value is an integer that ranges from 1 to 65535. The default value is 3.
-v	Displays the MPLS label carried in the ICMP Time Exceeded packet. This parameter is used to show the public label in the tracert initiated by PE.	By default, the MPLS label carried in the ICMP Time Exceeded is not displayed. Instead, only the path information carried in the ICMP Time Exceeded and Port-Unreachable packets is displayed.
-vpn-instance *vpn-instance-name*	Specifies the name of the VPN instance to which the destination address belongs.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.
pipe	Indicates that the TTL of a VPN instance is in pipe mode.	-
-w *timeout*	Specifies the timeout period to wait for a reply. If a tracert packet times out when reaching a gateway, an asterisk (*) is displayed. In the case of poor network quality and a low network transmission rate, you are advised to prolong the timeout period.	The value is an integer that ranges from 0 to 65535, in milliseconds. The default value is 5000.
-s *packetsize*	Specifies the length of an ICMP Echo Request message, excluding the IP header and ICMP header.	The value is an integer that ranges from 12 to 9600, in bytes. The default value is 12.
host	Indicates the domain name or IPv4 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters with spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. Alternatively, the value can be a valid IPv4 address in dotted decimal notation.

Copyright © Huawei Technologies Co., Ltd.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

During routine system maintenance, you can run the **ping** command to check network connectivity. If the ping fails, run the **tracert** command to locate the fault on the network.

You can specify different parameters in the **tracert** command for different scenarios:

- To check information about nodes between the source and the destination, run the **tracert** *host* command.
- To check information about nodes between the source and the destination on a Layer 3 VPN, run the **tracert -vpn-instance** *vpn-instance-name host* command. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **tracert** *host* command to check whether the peer is reachable. To check information about nodes between the source and the destination in a specified VPN instance, run the **tracert -vpn-instance** *vpn-instance-name host* command.
- On an unstable network, you can run the **tracert -q** *nqueries* **-w** *timeout host* command to check information about nodes between the source and the destination. If the network is unreliable, set the packet transmission count (**-q**) and timeout (**-w**) to the upper limits. This makes the test result accurate.
- To check information about nodes along a segment of a path, run the **tracert -f** *first-ttl* **-m** *max-ttl host* command that has initial TTL and maximum TTL specified.

Prerequisite

- The UDP module of each node is working properly; otherwise, the tracert operation fails.
- If **-vpn-instance** is specified, ensure that the VPN module of each node is working properly.
- The ICMP module of each node is working properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert** command is as follows:

1. The source sends a packet with the TTL being 1. After the TTL times out, the first hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.
2. The source sends a packet with the TTL being 2. After the TTL times out, the second hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.

 Copyright © Huawei Technologies Co., Ltd.

3. The source sends a packet with the TTL being 3. After the TTL times out, the third hop sends an ICMP Error message to the source, indicating that the packet cannot be forwarded.
4. The preceding process proceeds until the packet reaches the destination.

When receiving a packet, each destination hop cannot find the port specified in the packet, and returns an ICMP Port Unreachable message, indicating that the destination port is unreachable and the tracert ends. In this manner, the result of each probe is displayed on the source, according to which you can find the path from the source to the destination.

Configuration Impact

If a fault occurs when you run the **tracert** command, the following information may be displayed:

- !H: The host is unreachable.
- !N: The network is unreachable.
- !: The port is unreachable.
- !P: The protocol type is incorrect.
- !F: The packet is incorrectly fragmented.
- !S: The source route is incorrect.

Precautions

To ensure that the router properly responds to a Tracert request initiated by a source device when the router is the destination device to be tested, you must run the **icmp port-unreachable send** command to enable the device to send ICMP port-unreachable packets.

Once **-r** is specified, the outputs of both the **tracert** and **ping** commands show information about nodes between the source and the destination. Differences between the outputs of the **tracert** and **ping** commands are as follows:

- If the **ping** command times out on a transit node, a timeout packet is returned and the command output displays no path information.
- If the **tracert** command times out on a transit node, the command output displays " * * * " indicating that the tracert times out on the node but the tracert is not interrupted.

Example

Tracert the gateways from the source host to the destination host with the IP address being 10.1.1.11.

```
<Huawei> tracert 10.1.1.11
traceroute to 10.1.1.11 (10.1.1.11), max hops: 30, packet length: 40, press CTRL_C to break
1 10.3.112.1   10 ms 10 ms 10 ms
2 10.32.216.1  19 ms 19 ms 19 ms
3 * * *
4 * * *
5 * * *
6 * * *
7 10.1.1.11   339 ms 279 ms 279 ms
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-87 Description of the tracert command output

Item	Description
traceroute to	Tracert to a destination IP address.
max hops	Maximum TTL value.
packet length	Length of a sent packet.
10.3.112.1 10 ms 10 ms 10 ms	The integer 1 indicates the first hop gateway. Each hop increments the hop count. By default, the maximum hop count is 30. "10.3.112.1" is the gateway address of the first hop. The IPv4 address following the serial number of each hop is the gateway address of the hop. "10 ms 10 ms 10 ms" indicates the difference between the time when the three UDP packets are sent and when corresponding ICMP Time Exceeded or ICMP Port Unreachable messages are received. By default, each hop sends three UDP probe packets.
* * *	No ICMP Time Exceeded message or ICMP Port Unreachable message is returned within a specified period on the Nth hop. By default, an ICMP Time Exceeded message or ICMP Port-unreachable message should be returned within 5000 ms.

Related Topics

21.15.1 ping
21.15.2 ping ipv6
21.15.4 tracert ipv6

21.15.4 tracert ipv6

Function

The **tracert ipv6** command checks the path of packets from the source to the destination, checks IPv6 network connectivity, and locates a network fault.

Format

tracert ipv6 [**-a** *source-ipv6-address* | **-f** *first-hop-limit* | **-m** *max-hop-limit* | **-name** | **-p** *port-number* | **-q** *probes* | **-s** *packetsize* | **-w** *timeout* | **vpn-instance** *vpn-instance-name*] * *host*

 Copyright © Huawei Technologies Co., Ltd.

Parameters

Parameter	Description	Value
-a *source-ipv6-address*	Specifies the source address of a tracert packet. If this parameter is not specified, the IP address of the outbound interface is used as the source IP address for sending tracert packets.	The value is a 32-digit hexadecimal number, in the format of X:X:X:X:X:X:X:X.
-f *first-hop-limit*	Specifies the initial hop-limit. Carried in the IPv6 header, the hop-limit (time to live) indicates the lifetime of IPv6 packets and specifies the maximum number of hops that the IPv6 packets can pass through. The hop-limit field in IPv6 packets is similar to the TTL field in the IPv4 packets. The hop-limit value is set on the source and reduced by 1 each time the packet passes through a Layer 3 device. When the hop-limit value is reduced to 0 on a Layer 3 device, the Layer 3 device discards the packet and sends an ICMPv6 Timeout message to the source. If *first-hop-limit* is specified and the number of hops is smaller than the specified value, the hop-limit value will be greater than 0 after the packet passes through all the nodes. Therefore, no ICMPv6 Timeout message is sent to the source. If *max-hop-limit* is specified, the value of *first-hop-limit* must be smaller than the value of *max-hop-limit*.	The value is an integer that ranges from 1 to 255. The default value is 1.
-m *max-hop-limit*	Specifies the maximum hop-limit. Usually, the maximum hop-limit is set to the number of hops that a packet passes through. To change the hop-limit value, you need to use this parameter. If *first-hop-limit* is specified, the value of *max-hop-limit* must be greater than the value of *first-hop-limit*.	The value is an integer that ranges from 1 to 255. The default value is 30.

 Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
-name	Displays the name of the destination host.	-
-p *port-number*	Specifies the UDP port number of the destination. ● If no UDP port number is specified for the destination, when you run the **tracert ipv6** command, a port with the port number greater than 32768 is randomly chosen for the destination to receive tracert packets. ● Before specifying the UDP port number for the destination, ensure that the port is not in use; otherwise, the tracert fails.	The value is an integer that ranges from 1 to 65535. The default value is 33434.
-q *probes*	Specifies the number of tracert packets sent each time. In the case of poor network quality, you can set *probes* to a comparatively large value to ensure that tracert packets can reach the destination.	The value is an integer that ranges from 1 to 65535. The default value is 3.
-s *packetsize*	Specifies the length of an ICMPv6 Echo Request message, excluding the IP header and ICMPv6 header.	The value is an integer that ranges from 20 to 9600, in bytes. The default value is 56.
-w *timeout*	Sets the timeout period to wait for a reply. If a tracert packet times out when reaching a gateway, an asterisk (*) is displayed. In the case of poor network quality and a low network transmission rate, you are advised to prolong the timeout period.	The value is an integer that ranges from 1 to 65535, in milliseconds. The default value is 5000.
vpn-instance *vpn-instance-name*	Specifies the name of a VPN instance for the IPv6 address family.	The value is a string of 1 to 31 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string.

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
host	Specifies the host name or IPv6 address of the destination host.	The value is a string of 1 to 255 case-sensitive characters, spaces not supported. When double quotation marks are used around the string, spaces are allowed in the string. The IPv6 address is a 32–bit string in hexadecimal format, namely, the format X:X:X:X:X:X:X:X.

Views

All views

Default Level

0: Visit level

Usage Guidelines

Usage Scenario

When a fault occurs on the network and the peer is an IPv6 device, you can run the **ping ipv6** command to check network connectivity based on the reply message, and then run the **tracert ipv6** command to locate the fault.

You can specify different parameters in the **tracert ipv6** command for different scenarios:

- To check information about nodes between the source and the IPv6 destination, run the **tracert ipv6** *host* command.
- To check information about nodes between the source and the IPv6 destination on a Layer 3 VPN, run the **tracert ipv6 vpn-instance** *vpn-instance-name host* command. On a Layer 3 VPN, devices may not have routing information about each other. Therefore, you cannot use the **tracert ipv6** *host* command to check whether the peer is reachable. To check information about nodes between the source and the IPv6 destination in a specified VPN instance, run the **tracert ipv6 vpn-instance** *vpn-instance-name host* command.
- On an unstable network, you can run the **tracert ipv6 -q** *probes* **-w** *timeout host* command to check information about nodes between the source and the IPv6 destination. If the network is unreliable, set the packet transmission count (**-q**) and timeout (**-w**) to the upper limits. This makes the test result accurate.
- To check information about nodes along a segment of a path, run the **tracert ipv6 -f** *first-hop-limit* **-m** *max-hop-limit host* command that has initial hop-limit and maximum hop-limit specified.

Prerequisites

Copyright © Huawei Technologies Co., Ltd.

- The UDP module of each node is working properly; otherwise, the IPv6 tracert operation fails.
- The VPN module of each node is working properly if **vpn-instance** is specified.
- The ICMPv6 module of each node is working properly; otherwise, " * * * " is displayed.

Procedure

The execution process of the **tracert ipv6** command is as follows:

- The source sends a packet with the hop-limit being 1. After the hop-limit times out, the first hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The source sends a packet with the hop-limit being 2. After the hop-limit times out, the second hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The source sends a packet with the hop-limit being 3. After the hop-limit times out, the third hop sends an ICMPv6 Error message to the source, indicating that the packet cannot be forwarded.
- The preceding process proceeds until the packet reaches the destination.

When receiving an IPv6 packet, each destination hop cannot find the port specified in the IPv6 packet, and therefore returns an ICMPv6 Port Unreachable message, indicating that the destination port is unreachable and the IPv6 tracert ends. In this manner, the result of each probe is displayed on the source, according to which you can find the path from the source to the destination.

Configuration Impact

If a fault occurs when you run the **tracert ipv6** command, the following information may be displayed:

- !H: The host is unreachable.
- !N: The network is unreachable.
- !: The port is unreachable.
- !P: The protocol type is incorrect.
- !F: The packet is incorrectly fragmented.
- !S: The source route is incorrect.

Precautions

By default, the ICMPv6 module is automatically enabled after you enable the IPv6 module.

Example

Set the number of packets to be sent to 5 and timeout period to 8000 ms, and tracert the gateways from the source to the destination at FC00::3.

```
<Huawei> tracert ipv6 -q 5 -w 8000 FC00::3
traceroute to FC00::3 30 hops max,60 bytes packet
1 FC00:1::3 26 ms 23 ms 26 ms 30 ms 29 ms
2 FC00::3 3020 ms 3024 ms 4040 ms 6820 ms 5584 ms
```

 Copyright © Huawei Technologies Co., Ltd.

Table 21-88 Description of the tracert ipv6 command output

Item	Description
traceroute to HH:HH::HH:H	IPv6 address of the destination host.
x hops max	Maximum hop-limit value.
x bytes packet	Length of a tracert packet.
1 2	Sequence number of the received ICMPv6 Echo Reply message.
HH:HH::HH:H	Address of the IPCMPv6 Echo Reply message.
26 ms 23 ms 26 ms	RTT, in milliseconds.

Related Topics

21.15.2 ping ipv6

Copyright © Huawei Technologies Co., Ltd.